Cisco Group Encrypted Transport VPN コンフィギュレーションガイド

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries.To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks.Third-party trademarks mentioned are the property of their respective owners.The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1110R)

© 2017 Cisco Systems, Inc. All rights reserved.

目 次

最初にお読みください 1

Cisco Group Encrypted Transport VPN 3

機能情報の確認 4

Cisco Group Encrypted Transport VPN の前提条件 4

Cisco Group Encrypted Transport VPN の制約事項 5

Cisco Group Encrypted Transport VPN に関する情報 6

Cisco Group Encrypted Transport VPN の概要 6

Cisco Group Encrypted Transport VPN のアーキテクチャ 7

キー配布グループ ドメイン オブ インタープリテーション（GDOI） 7

GDOI 7

グループ メンバー 8

キー サーバ 8

Cisco ソフトウェアでのプロトコル メッセージの動作 9

IPSec 10

IPsec SA を更新するためのキー サーバとグループ メンバー間の通信フロー 10

IPsec と ISAKMP タイマー 11

アドレス保存 12

セキュア データ プレーン マルチキャスト 13

セキュア データ プレーン ユニキャスト 14

Cisco Group Encrypted Transport VPN の機能 14

キー再生成 14

キー再生成シーケンス番号のチェック 15

マルチキャスト キー再生成 15

マルチキャスト キー再生成の設定要件 16

ユニキャスト キー再生成と SA 16

ポリシー変更後のキー再生成の動作 18

グループ メンバーにおけるIPsec SA の使用 20
設定変更によってキー サーバごとのキー再生成のトリガーが可能 21
キー再生成をトリガーするコマンド 22
キー再生成の再送信 28
グループ メンバー アクセス コントロール リスト 28
セキュリティ ポリシー変更時におけるグループ メンバーの動作 29
時間ベースのアンチリプレイ 30
クロック同期 31
インターバル期間 31
アンチ リプレイ設定 32
コントロール プレーンの時間ベースのアンチリプレイ 32
連携キー サーバ 35
通知メッセージ 36
キー サーバのロールの変更 37
受信専用 SA 38
グローバル変換 38
パッシブ SA 39
拡張ソリューションの管理性 39
VRF-Lite インターフェイスによるサポート 39
GM 登録の認証ポリシー 39
GET VPN GM 認証 40
Protocol Independent Multicast-Sparse Mode でのキー再生成機能 41
Fail-Close モード 41
Fail-Close 機能の使用上の注意事項 42
GDOI 登録成功を追跡する MIB オブジェクトの作成 43
BGP の GET VPN ルーティング認識 43
Cisco Group Encrypted Transport VPN システム ロギング メッセージ 46
Cisco Group Encrypted Transport VPN の設定方法 51
キー サーバの設定 51
前提条件 51
キー再生成メッセージに署名するための RSA キーの設定 52
次の作業 52

グループ ID、サーバ タイプ、および SA タイプの設定 53
次の作業 54
キー再生成の設定 54
前提条件 55
ユニキャスト キー再生成の設定 55
マルチキャスト キー再生成の設定 58
グループ メンバー ACL の設定 61
次の作業 62
IPsec ライフタイム タイマーの設定 62
次の作業 63
ISAKMP ライフタイム タイマーの設定 63
IPsec SA の設定 64
次の作業 67
GDOI グループ用の時間ベースのアンチリプレイの設定 67
パッシブ SA の設定 70
キー サーバのロールのリセット 71
グループ メンバーの設定 71
グループ名、ID、キー サーバ IP アドレス、およびグループ メンバー登録の設定 71
次の作業 73
暗号マップ エントリの作成 73
次の作業 74
トラフィックを暗号化する必要があるインターフェイスへの暗号マップの適用 74
Fail-Close モードのアクティブ化 75
KEK の許容可能な暗号化アルゴリズムまたはハッシュ アルゴリズムの設定 76
TEK の受け入れ可能トランスフォーム セットの設定 78
グループ メンバーの暗号状態の追跡 80
GET VPN GM 認証の設定 81
事前共有キーを使用する GM 認証の設定 82
PKI を使用する GM 認証の設定 83
Cisco Group Encrypted Transport VPN 設定の確認とトラブルシューティング 87

キー サーバ上のアクティブなグループ メンバーの確認 87
キー再生成関連統計情報の確認 88
グループ メンバー上で GDOI によって作成された IPsec SA の確認 89
キー サーバ上で GDOI によって作成された IPsec SA の確認 90
グループ メンバーが最後にキー サーバから受信した TEK の確認 91
連携キー サーバの状態と統計情報の確認 91
アンチリプレイ疑似時間関連の統計情報の確認 92
暗号マップの Fail-Close モードの状態の確認 93
Cisco Group Encrypted Transport VPN の設定例 94
例：キー サーバとグループ メンバーのケース スタディ 94
キー サーバ 1 の例 95
キー サーバ 2 の例 96
例：グループ メンバー 1 の設定 97
例：グループ メンバー 2 の設定 98
例：グループ メンバー 3 の設定 98
例：グループ メンバー 4 の設定 99
例：グループ メンバー 5 の設定 100
例：グループ メンバーが最後にキー サーバから受信した TEK の確認 100
パッシブ SA の例 101
Fail-Close モードの例 102
Cisco Group Encrypted Transport VPN の追加の制約事項 102
関連資料 102
標準 103
MIB 103
RFC 103
シスコのテクニカル サポート 104
Cisco Group Encrypted Transport VPN の機能情報 104
用語集 112
GET VPN GM の削除とポリシー トリガー 115
機能情報の確認 115
GM の削除とポリシー トリガーに関する情報 116
GET VPN のソフトウェア バージョン 116
GM の削除 116

他の GET VPN ソフトウェア バージョンとの GM 削除の互換性 117

一時的な IPsec SA による GM の削除 117

即時の IPsec SA 削除による GM の削除 117

ポリシーの交換とキー再生成のトリガー 117

キー再生成をトリガーする TEK および KEK ポリシー変更に関する不整合 118

ポリシーの交換およびキー再生成のトリガーの他の GET VPN ソフトウェア バージョンとの互換性 121

GET VPN GM 削除およびポリシー トリガーの設定方法 121

GM の削除をサポートするソフトウェア バージョンを GM が実行していることを確認する 121

一時的な IPsec SA による GM の削除 122

GM の削除と IPSec SA の即時削除 124

GM がポリシーの交換をサポートするソフトウェア バージョンを実行していることを確認する 125

キー再生成のトリガー 126

GET VPN GM の削除とポリシーのトリガーの設定例 127

例：GET VPN ネットワークからの GM の削除 127

例：グループ メンバーのキー再生成のトリガー 128

GET VPN GM の削除とポリシーのトリガーのその他の参考資料 130

GET VPN GM の削除とポリシーのトリガーの機能情報 130

GET VPN の GDOI MIB サポート 133

機能情報の確認 133

GET VPN の GDOI MIB サポートに関する情報 134

他の GET VPN ソフトウェア バージョンとの GDOI MIB の互換性 134

GDOI MIB テーブル階層 135

GDOI MIB テーブル オブジェクト 135

GDOI MIB 通知 139

GDOI MIB の制限 140

GET VPN の GDOI MIB サポートの設定方法 140

GDOI MIB をサポートするソフトウェア バージョンを GM が実行していることを確認する 140

SNMP コミュニティのアクセス コントロールの作成 141

SNMP マネージャとの通信の有効化 142
GDOI MIB 通知の有効化 143
GET VPN 用の GDOI MIB サポートの設定例 145
例：GDOI MIB をサポートするソフトウェア バージョンを GM が実行していることを確認する 145
例：SNMP コミュニティのアクセス コントロールの作成 146
例：SNMP マネージャとの通信の有効化 146
例：GDOI MIB 通知の有効化 146
GET VPN 用の GDOI MIB サポートのその他の参考資料 146
GET VPN 用の GDOI MIB サポートの機能情報 147
GET VPN の復元力 149
機能情報の確認 149
GET VPN の復元力の前提条件 150
GET VPN の復元力の制約事項 150
GET VPN の復元力に関する情報 150
長い SA ライフタイム 150
クロック スキューの軽減 151
更新のキー再生成 151
新しい発信 IPsec SA へのロールオーバー 151
定期的なリマインダ同期キー再生成 152
事前配置されたキー再生成 152
GET VPN の復元力の設定方法 152
GM が長い SA ライフタイムをサポートするソフトウェア バージョンを実行していることを確認する 152
長い SA ライフタイムの設定 153
TEK の長い SA ライフタイムの設定 153
KEK の長い SA ライフタイムの設定 154
定期的なリマインダ同期キー再生成の設定 155
GET VPN の復元力の確認とトラブルシューティング 156
キー サーバの GET VPN の復元力の確認とトラブルシューティング 156
グループ メンバーの GET VPN の復元力の確認とトラブルシューティング 157
GET VPN 復元力の設定例 158

例：GMが長いSAライフタイムをサポートするソフトウェアバージョンを実行していることを確認する 158
例：長い SA ライフタイムの設定 159
例：定期的なリマインダ同期キー再生成の設定 159
GET VPN の復元力のその他の参考資料 159
GET VPN の復元力の機能情報 161
GETVPN 復元力 GM - エラー検出 163
機能情報の確認 163
GETVPN の復元力：GM のエラー検出に関する情報 164
エラー処理 164
GETVPN の復元力：GM のエラー検出の設定方法 165
GETVPN の復元力：GM のエラー検出の設定 165
GETVPN の復元力：GM のエラー検出の設定例 166
例：GETVPN の復元力：GM のエラー検出の設定 166
GETVPN の復元力：GM のエラー検出その他の参考資料 166
GETVPN の復元力：GM のエラー検出の機能情報 167
GETVPN CRL チェック 169
機能情報の確認 169
GETVPN CRL チェックに関する情報 170
連携キー サーバのプロトコル統合 170
GETVPN CRL チェックの設定方法 171
GETVPN CRL チェックのためのキー サーバの設定 171
グループ メンバーでの CRL チェックの無効化 174
証明書の IKE 認証の設定 175
キー サーバでの GETVPN CRL チェックの有効化 176
GETVPN CRL チェックの設定例 177
例：GETVPN CRL チェックの有効化 177
GETVPN CRL チェックに関する追加情報 178
GETVPN CRL チェックに関する機能情報 179
スイート B での GET VPN のサポート 181
機能情報の確認 181
スイート B での GET VPN のサポートの前提条件 182

スイート B での GET VPN のサポートの制約事項 182
スイート B での GET VPN のサポートに関する情報 182
スイート B 182
SHA-2 および HMAC-SHA-2 183
AES-GCM と AEC-GMAC 183
スイート B に準拠する暗号化アルゴリズムのセット 183
SID 管理 184
グループ サイズ 185
連携キー サーバへの KSSID 割り当て 186
グループの再初期化 188
スイート B の Cisco GET VPN システム ロギング メッセージ 188
スイート B での GET VPN のサポートの設定方法 191
GM がスイート B をサポートするソフトウェア バージョンを実行していることを確認する 191
GET VPN スイート B でのキー サーバの設定 192
KEK の署名ハッシュ アルゴリズムの設定 192
グループ サイズの設定 194
キー サーバ識別子の設定 195
スイート B の IPsec SA の設定 198
GET VPN スイート B でのグループ メンバーの設定 201
スイート B の KEK の許容可能な暗号化アルゴリズムまたはハッシュ アルゴリズムの設定 201
スイート B の TEK の受け入れ可能トランスフォーム セットの設定 203
スイート B での GET VPN のサポートの確認とトラブルシューティング 205
キーサーバ上のスイートBでのGETVPNのサポートの確認とトラブルシューティング 205
GM 上のスイート B での GET VPN のサポートの確認とトラブルシューティング 208
スイート B での GET VPN のサポートの設定例 211
例：GM がスイート B をサポートするソフトウェア バージョンを実行していることを確認する 211
例：GET VPN スイート B のキー サーバの設定 211

例：GET VPN スイート B のグループ メンバーの設定 212
その他の参考資料 213
スイート B での GET VPN のサポートの機能情報 214
Cisco TrustSec の IPsec インライン タギングの GET VPN サポート 217
機能情報の確認 218
Cisco TrustSec 用の IPsec インライン タギングの GET VPN のサポートの前提条件 218
Cisco TrustSec 用の IPsec インライン タギングの GET VPN のサポートの制約事項 218
Cisco TrustSec の IPsec インライン タギングの GET VPN サポートに関する情報 219
セキュリティ グループ タギング機能のグループ メンバー登録 219
セキュリティ グループ タギングが有効な SA の作成 219
グループ メンバー データ プレーンのセキュリティ グループ タグの処理 219
セキュリティ グループ タギング使用時のパケットのオーバーヘッドとフラグメンテーション 220
Cisco TrustSec の IPsec インライン タギングの GET VPN サポートの設定方法 221
GM が Cisco TrustSec の IPsec インライン タギングをサポートするソフトウェア バージョンを実行していることを確認する 221
Cisco TrustSec の IPsec インライン タギングの設定 222
キー再生成のトリガー 223
Cisco TrustSec 用の IPsec インライン タギングの GET VPN のサポートの確認とトラブルシューティング 224
Cisco TrustSec の IPsec インライン タギングの GET VPN サポートの設定例 225
例：GM が Cisco TrustSec の IPsec インライン タギングをサポートするソフトウェア バージョンを実行していることを確認する 225
例：Cisco TrustSec の IPsec インライン タギングの設定 226
例：グループ メンバーのキー再生成のトリガー 227
Cisco TrustSec 用の IPsec インライン タギングの GET VPN のサポートのその他の参考資料 228
Cisco TrustSec 用の IPsec インライン タギングの GET VPN のサポートの機能情報 229
GETVPN GDOI バイパス 233
機能情報の確認 233
GETVPN GDOI バイパスの制約事項 234
GETVPN GDOI バイパスに関する情報 234

GDOI バイパス暗号化ポリシー 234
デフォルト GDOI バイパス暗号化ポリシーの有効化と無効化 234
デフォルト GDOI バイパス暗号化ポリシーの強化 234
GETVPN GDOI バイパスの設定方法 235
デフォルト GDOI バイパス暗号化ポリシーの有効化 235
デフォルト GDOI バイパス暗号化ポリシーの無効化 236
デフォルト GDOI バイパス暗号化ポリシーの有効性と無効性の確認 237
GETVPN GDOI バイパスの設定例 238
例：デフォルト GDOI バイパス暗号化ポリシーの有効化 238
例：デフォルト GDOI バイパス暗号化ポリシーの無効化 238
GETVPN GDOI バイパスのその他の参考資料 239
GETVPN GDOI バイパスの機能情報 240
GETVPN G-IKEv2 241
機能情報の確認 241
GETVPN G-IKEv2 の前提条件 242
GETVPN G-IKEv2 の制約事項 242
GETVPN G-IKEv2 に関する情報 242
GETVPN G-IKEv2 の概要 242
インターネット キー エクスチェンジ バージョン 2（IKEv2） 243
GETVPN G-IKEv2 の交換 244
サポートされている機能および構成 246
GDOI から G-IKEv2 への移行 247
GETVPN G-IKEv2 の設定方法 249
GETVPN G-IKEv2 の設定 249
GETVPN G-IKEv2 のその他の参考資料 250
GETVPN G-IKEv2 の機能情報 251
8K GM スケールの改善 253
機能情報の確認 253
8K GM スケールの改善 の前提条件 254
8K GM スケールの改善に関する情報 254
8K GM スケールの改善 254
8K GM スケールの改善の設定方法 254

グループ メンバー ヘッダーのプロトコル バージョンのアップグレードとダウングレード 254
8K GM スケールの改善の設定例 256
例：グループ メンバー ヘッダーのプロトコル バージョンのアップグレード 256
例：グループ メンバー ヘッダーのプロトコル バージョンのダウングレード 256
8K GM スケールの改善のその他の参考資料 256
8K GM スケールの改善 の機能情報 257

第 1 章

最初にお読みください

Cisco IOS XE 16 についての重要事項

Cisco IOS XE Release 3.7.0E（Catalyst スイッチ）と Cisco IOS XE Release 3.17S（アクセスおよびエッジ ルーティング）という有効な 2 つのリリースが統合され、スイッチングおよびルーティング ポートフォリオ内のアクセスおよびエッジ製品を幅広く網羅する 1 つの統合リリース バージョン（Cisco IOS XE 16）へと進化しました。

（注） 機能が導入されると、技術構成ガイドの [Feature Information] テーブルで通知されます。その機能に対応している他のプラットフォームについては、通知される場合と通知されない場合があります。特定の機能がプラットフォームでサポートされているかどうかを確認するには、製品のランディングページに表示される技術構成ガイドをご覧ください。製品のランディングページに技術構成ガイドが表示された場合、そのプラットフォームでは機能がサポートされています。

第 2 章

Cisco Group Encrypted Transport VPN

Cisco Group Encrypted Transport VPN（GET VPN）は、Cisco IOS デバイス上で発生する、または Cisco IOS デバイス を経由するプライベート WAN 上の IP マルチキャスト トラフィック グループまたはユニキャスト トラフィックの安全を守るために必要な一連の機能です。GET VPN では、キーイング プロトコルであるグループ ドメイン オブ インタープリテーション（GDOI）と、IP セキュリティ（IPsec）暗号化が組み合されており、ユーザは、IP マルチキャスト トラフィックやユニキャスト トラフィックをセキュリティ保護するための効果的な方式を利用できます。GET VPN では、ルータによって、トンネル化されていない（つまり「ネイティブな」）IP マルチキャストおよびユニキャスト パケットに対して暗号化を適用できるので、マルチキャストおよびユニキャスト トラフィックを保護するためにトンネルを設定する必要がありません。

（注） セキュリティに対する脅威とそれに対抗するための暗号化技術は絶えず変化しています。暗号化に関するシスコの最新の推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

ここでは、Cisco GET VPN の設定、確認、およびトラブルシューティングの方法を説明します。

Cisco Group Encrypted Transport VPN には、次のような利点があります。

- データ セキュリティおよびトランスポート認証が利用可能で、すべての WAN トラフィックを暗号化することによって、セキュリティ適合性および内部規則を満たすことが可能。
- 大規模なネットワーク メッシュが可能であり、グループ暗号キーを使用した、複雑なピアツーピアのキー管理が不要。
- マルチプロトコル ラベル スイッチング（MPLS）ネットワークの場合でも、ネットワーク インテリジェンス（フルメッシュ接続、ナチュラル ルーティング パス、Quality of Service（QoS）など）を維持。
- 一元化されたキー サーバを使用してメンバーシップを簡単に管理可能。
- 中央集中型ハブを介した転送が不要な、サイト間におけるフルタイムの直接通信を実現することによって遅延とジッタの低減が可能。

- マルチキャスト トラフィックの複製にコア ネットワークを使用し、個々のピア サイトごとにおけるパケットの複製を不要にすることによって、宅内装置（CPE）およびプロバイダー エッジ（PE）暗号化デバイスの負荷を削減。

- 機能情報の確認，4 ページ
- Cisco Group Encrypted Transport VPN の前提条件，4 ページ
- Cisco Group Encrypted Transport VPN の制約事項，5 ページ
- Cisco Group Encrypted Transport VPN に関する情報，6 ページ
- Cisco Group Encrypted Transport VPN の設定方法，51 ページ
- Cisco Group Encrypted Transport VPN の設定例，94 ページ
- Cisco Group Encrypted Transport VPN の追加の制約事項，102 ページ
- Cisco Group Encrypted Transport VPN の機能情報，104 ページ
- 用語集，112 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、『Bug Search Tool』およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

Cisco Group Encrypted Transport VPN の前提条件

- Cisco IOS XE リリース 2.3 以降を使用している必要があります。
- IPsec およびインターネット キー交換（IKE）に関する知識が必要です。
- Cisco IOS XE グローバル ルータにおけるマルチキャストおよびユニキャスト ルーティングの設定方法を知っている必要があります。
- IKE ポリシーを設定する際、IKE ライフタイムを最小値の 5 分に設定する必要があります。その結果、不要なリソースが、IKE セキュリティ アソシエーション（SA）のメンテナンスで無駄に使用されなくなります。登録 IKE SA が確立したら、キー再生成 SA が作成済みとなり、将来のキー再生成を受け入れるために使用されるので、登録 SA を維持する必要はなくなります。

Cisco Group Encrypted Transport VPN の制約事項

- カウンタ ベースのアンチ リプレイ用に高パケット レートを暗号化する場合、ライフタイムを長く設定し過ぎないようにしてください。長く設定し過ぎると、シーケンス番号のラップに数時間かかってしまう可能性があります。たとえば、パケット レートが毎秒 100 キロパケットである場合、ライフタイムは、SA がシーケンス番号のラップ前に使用されるように 11.93 時間より短く設定する必要があります。
- Cisco IOS XE ソフトウェアでは、ネットワークにアクセスするユーザの包含ポート範囲を **permit** コマンドを使用して拡張 ACL と照合することはできません。
- ユニキャスト トラフィックおよびカウンタベースのアンチリプレイでは、グループ メンバーの 1 つが停止してから復帰した場合、シーケンス番号がグループ メンバー間で同期されていない状態になる可能性があります。たとえば、グループ メンバー 1 からグループ メンバー 2 へのトラフィックが存在し、最後のシーケンス番号が *n* になる場合です。Group Member 1 が停止してから復帰します。グループ メンバー 1 における SA のシーケンス番号は現在 1 で始まっていますが、グループ メンバー 2 では、前のシーケンス番号から連続する番号（*n* + 1）と予測しています。このような状況の結果、Group Member 1 のシーケンス番号が *n* になるか、次のキー再生成まで、Group Member 1 からの後続のトラフィックは停止します。
- 転送モード トラフィック セレクタを設定する際、転送モードを SA にすることが可能です。パケット サイズが MTU を超え、パケットが転送できなくなると、SA が発生します。
- 転送モードは、Group Encrypted Transport VPN Mode（GM）から GM へのトラフィックだけに使用してください。
- カプセル化されたパケットの IP ヘッダー内の don't fragment bit（df-bit）設定を上書きする場合、グローバル コンフィギュレーション モードで上書きコマンドを設定する必要があります。GET VPN では、インターフェイス コンフィギュレーションは受け入れられません。この制限事項は、GET VPN にだけ当てはまります。IPsec では、グローバル コンフィギュレーション専用上書きコマンドおよびインターフェイス専用上書きコマンドの両方が受け入れられます。
- カウンタベースのアンチ リプレイは推奨できません。カウンタベースのアンチ リプレイは、1 つのグループ内に 2 つのグループ メンバーが存在している時にだけ動作します。
- GET VPN 時間ベースのアンチリプレイ機能では、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータと Cisco 4330 サービス統合型ルータの Encapsulating Security Payload（ESP）転送モードがサポートされていません。
- Path MTU Discovery（PMTUD）は、GET VPN に対しては動作しないので、df-bit が設定されており、中間リンクの MTU がカプセル化されたパケットのサイズより小さい場合に、カプセル化されたパケットが廃棄される可能性があります。このようなイベントが発生した場合、パケットを廃棄するルータによってパケット上の発信元 IP アドレスに対して通知が送信され、df-bit の設定のためにルータによるパケットのフラグメント化ができなかったために、パケットが廃棄されたことが通知されます。GET VPN ではヘッダー保存機能があるため、このメッセージはカプセル化を行うエンドポイントを経由しないで、直接データの発信元に送信されます。そのため、カプセル化を行うルータは、カプセル化の後で df-bit を設定する前

により小さいサイズにパケットをフラグメント化しなければならないと判断できません。パケット上の df-bit 設定は継続され、中間ルータにおいて、それらのパケットは引き続き廃棄されます（これはトラフィックのブラックホール化と呼ばれています）。

- Cisco IOS XE リリース 3.5S 以前のリリースでは、Cisco IOS XE イメージを使用してキー サーバを設定することはできません。これらは Cisco IOS T ベースまたはメインラインベース イメージを使用して設定する必要があります。これは、Cisco IOS XE リリース 3.6S 以降のリリースの制約ではありません。
- 暗号化エンジンの最適化のために、時間ベースのアンチリプレイ（TBAR）のオーバーヘッドは 12 バイトではなく 16 バイトです。
- Cisco ASR 1000 シリーズ アグリゲーション サービス ルータの GET VPN 設定で正常なトラフィック フローを保証するため、Cisco IOS XE リリース 3.12S 以前のリリース、Cisco IOS XE リリース 3.14S および Cisco IOS XE リリース 3.15S では 20 秒を超える TBAR ウィンドウ サイズが推奨されます。Cisco IOS XE リリース 3.13S、Cisco IOS XE リリース 3.16S 以降のリリースでは、20 秒以内の TBAR ウィンドウ サイズが許可されます。
- トンネル インターフェイスとポートチャネル インターフェイスでは暗号マップはサポートされていません。

Cisco Group Encrypted Transport VPN に関する情報

Cisco Group Encrypted Transport VPN の概要

音声やビデオなどのネットワークを利用するアプリケーションによって、即時に通信可能で各ブランチが相互接続された、QoS 対応 WAN の必要性が増しています。これらのアプリケーションは分散して配置されるため、スケーラビリティに対する要求も高まります。同時に、企業の WAN テクノロジーにおいては、QoS 対応ブランチ間相互接続と転送のセキュリティとの間でトレードオフが発生します。ネットワーク セキュリティのリスクが増大し、適合認定が重要になりつつある中、次世代の WAN 暗号化テクノロジーである GET VPN を利用すれば、ネットワークのインテリジェント化とデータ プライバシとの間で折り合いをつける必要性を低下させることができます。

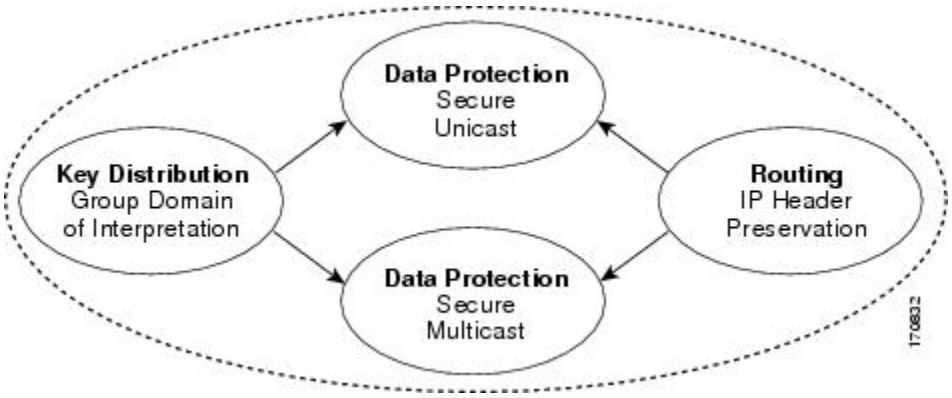
シスコでは、GET の導入に伴い、トンネルレス VPN を提供しており、これによりトンネルが不要になります。ポイントツーポイント トンネルの必要性をなくすことで、メッシュ ネットワークを大規模化すると同時に、音声やビデオの品質にとって重要なネットワークインテリジェンス機能を維持することが可能となっています。GET では、「信頼できる」グループ メンバーというコンセプトを基にした、各種の標準規格に準拠準拠したセキュリティ モデルが用意されています。信頼できるメンバーのルータでは、ポイントツーポイント IPsec トンネル関係とは独立した共通のセキュリティ方式が使用されます。ポイントツーポイント トンネルではなく信頼できるグループを使用することによって、「any-any」ネットワークを大規模化すると同時に、音声やビデオの品質にとって重要なネットワークインテリジェンス機能（QoS、ルーティング、マルチキャストなど）を維持することが可能となっています。

GET ベースのネットワークは、IP や MPLS などを含む、さまざまな WAN 環境で使用できます。この暗号化テクノロジーを使用する MPLS VPN はスケーラビリティ、管理性、コストに優れており、政府によって義務付けられている暗号化要件が満たされます。GET は柔軟であるため、セキュリティを必要とする企業では、サービス プロバイダー WAN サービスにおいて独自のネットワーク セキュリティを管理することも、暗号化サービスをプロバイダーに委託することもできます。GET によって、部分メッシュ接続または完全メッシュ接続を必要とする大規模なレイヤ 2 または MPLS ネットワークの保護が簡易化されます。

Cisco Group Encrypted Transport VPN のアーキテクチャ

GET VPN は、マルチキャスト キー再生、「ネイティブの」マルチキャスト パケットの暗号化を可能にする手段、およびプライベート WAN を介したユニキャスト キー再生成を網羅するソリューションです。マルチキャスト キー再生と GET VPN は、インターネット技術特別調査委員会（IETF）の RFC 3547 で定義されている GDOI を基盤としています。また、ヘッダー保存および SA 検索の領域においては、IPsec と各種の共通点が存在します。IPsec SA の動的配信が追加され、IPsec のトンネルが重複する特性が削除されています。次の図に、GET VPN の各概念と、概念間の関係を示します。

図 *1*：*GET VPN* の概念と関係



キー配布グループ ドメイン オブ インタープリテーション（GDOI）

GDOI

GDOI は、グループ キー管理のための、Internet Security Association Key Management Protocol（ISAKMP）ドメイン オブ インタープリテーション（DOI）として定義されています。グループ管理モデルでは、GDOI プロトコルが、グループ メンバーと、グループ コントローラまたはキーサーバ（GCKS）との間で動作し、その結果、認証されているグループ メンバー間での SA が確立されます。ISAKMP では、ネゴシエーションの 2 つのフェーズが定義されています。GDOI は、フェーズ 1 の ISAKMP セキュリティ アソシエーションによって保護されます。フェーズ 2 の交換は、RFC 6407 によって定義されています。次の図に示したトポロジとそれに続く説明は、このプロトコルのしくみを説明したものです。

グループ メンバー

グループ メンバーは、グループと通信するために必要な IPsec SA または SA を取得するためのキー サーバに登録します。グループ メンバーによって、そのグループの個別のポリシーおよびキーを取得するためのキー サーバにグループ ID が提供されます。これらのキーは、現在の IPsec SA が期限切れになる前に、定期的に更新されます。その結果、トラフィックのロスがなくなります。

showcryptoisakmpsadetail コマンドの出力では、GET VPN の Key Encryption Key（KEK）キー再生成認証に RSA 署名が使用されるため、セキュリティ アソシエーション（SA）認証を「rsig」として表示します。

キー サーバ

キー サーバの役割には、ポリシーの維持や、グループのキーの作成および維持などがあります。グループ メンバーが登録されると、キー サーバによってこのポリシーおよびキーが、グループ メンバーに対してダウンロードされます。また、キー サーバは、既存のキーの期限が切れる前にグループに対してキーの再生成を実行します。

（注） Cisco IOS XE リリース 3.5S 以前のリリースでは、キー サーバは Cisco ASR 1000 シリーズ ルータではサポートされていません。これらは Cisco IOS T ベースまたはメインラインベース イメージを使用して設定する必要があります。これは、Cisco IOS XE リリース 3.6S 以降のリリースの制限ではありません。

キー サーバには、登録要求の処理およびキーの再生成の送信という 2 つの機能があります。グループ メンバーはいつでも登録可能で、最新のポリシーおよびキーを受信できます。グループ メンバーがキー サーバに登録する場合、キー サーバによって、グループ メンバーが参加を試みているグループ ID が確認されます。この ID が有効なグループ ID だった場合、キー サーバによって、SA ポリシーがグループ メンバーに対して送信されます。ダウンロードされたポリシーを処理できることがグループ メンバーによって確認されると、キーサーバから各キーがダウンロードされます。

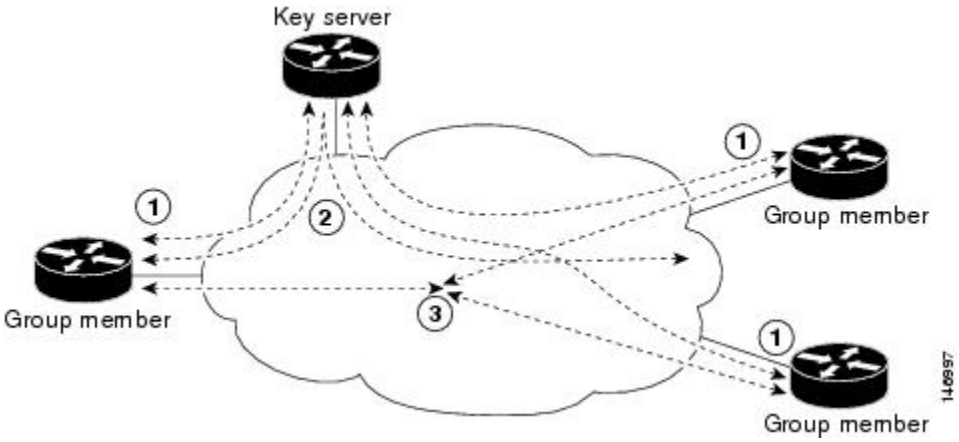
キー サーバからダウンロードされるキーには、キー暗号キー（KEK）とトラフィック暗号キー（TEK）の 2 種類があります。TEK は、同じグループ内のグループ メンバーどうしの通信で使用される IPsec SA になります。KEK は、キー再生成メッセージを暗号化します。

IPsec SA の期限切れが近づいた場合、またはキー サーバ上のポリシーが変更（コマンドライン インターフェイス [CLI] を使用）された場合、GDOI サーバによってキー再生成メッセージが送信されます。CSCti89255 では、KEK タイマーが期限切れになる前に KEK のキー再生成が行われます。グループ メンバーもタイマーを開始し、タイマーの期限が切れる前に更新されたキーを受け取ることを期待します。これらを受け取らない場合、グループ メンバーは KEK の期限切れの前にジッタが生じた再登録を開始します。KEK ライフタイムが期限切れになると、KEK は削除されます。

パケット損失に備えて、キー再生成メッセージが定期的に送信される場合もあります。パケット損失が発生する原因としては、信頼できる転送を使用することなくキー再生成メッセージが送信されることなどが考えられます。キーの再生成メカニズムがマルチキャストである場合は、受信

者がキーの再生成メッセージを受信できなかったことを示す有効なフィードバック メカニズムがないため、定期的に再送信することによってすべての受信者が最新の情報を受信できるようにします。キー再生成メカニズムがユニキャストである場合、受信元によって確認応答メッセージが送信されます。

図 *2*：グループ メンバーがグループに参加するうえで必要なプロトコル フロー



上記のトポロジは、次のようにグループ メンバーがグループに参加するうえで必要なプロトコル フローを示しています。

1. グループ メンバーがキー サーバに登録されます。キー サーバによってグループ メンバーが認証および許可され、グループ メンバーが IP マルチキャスト パケットを暗号化および復号化するうえで必要な IPsec ポリシーおよびキーがダウンロードされます。
2. 必要に応じて、キー サーバからグループ メンバーに対してキーの再生成メッセージが「プッシュ」されます。キー再生成メッセージには、古い IPsec SA の期限が切れた際に使用される新しい IPsec ポリシーおよびキーが格納されています。常に有効なグループ キーが使用できるように、キーの再生成メッセージは SA の期限が切れる前に送信されます。
3. 各グループ メンバーは、キー サーバによって認証を受けてから、キー サーバから受信した IPsec SA を使用して、同じグループ内の他の認証済みグループ メンバーと通信します。

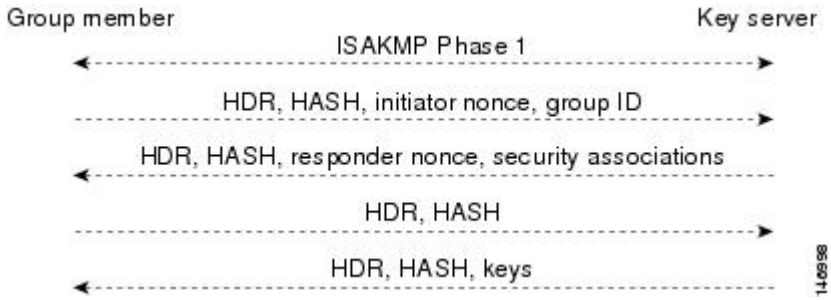
Cisco ソフトウェアでのプロトコル メッセージの動作

マルチキャスト キー再生では、グループのポリシーおよびキーを配信するために GDOI プロトコル（RFC 6407）が使用されます。GDOI プロトコルは、キー サーバとグループ メンバーの間で使用されます。キー サーバによってポリシーとキーが作成および維持され、さらに、認証された各グループ メンバーにダウンロードされます。

GDOI プロトコルは、ISAKMP フェーズ 1 交換によって保護されます。GDOI キー サーバと GDOI グループ メンバーの ISAKMP ポリシーは同じである必要があります。このフェーズ 1 ISAKMP ポリシーは、そのポリシーに従う GDOI プロトコルを保護できる程度に強力なものである必要があります。GDOI プロトコルは、フェーズ 1 ISAKMP ポリシーに従う 4 メッセージ交換です。フェーズ 1 ISAKMP 交換は、メイン モードまたはアグレッシブ モードで発生する可能性があります。

次の図は、ISAKMP フェーズ 1 交換を示しています。

図 *3*：*ISAKMP* フェーズ *1* 交換と *GDOI* 登録



上記メッセージ（ISAKMP フェーズ 1 メッセージと 4 つの GDOI プロトコル メッセージ）を GDOI 登録と呼びます。上に示した交換全体は、グループ メンバーとキー サーバ間のユニキャスト交換です。

キー再生成メカニズムがマルチキャストである場合、登録中、グループ メンバーによってマルチキャスト グループのアドレスが受信され、そのグループ メンバーが、マルチキャスト キー再生成を受信するうえで必要なマルチキャスト グループに登録されます。

GDOI プロトコルでは、ユーザ データグラム プロトコル（UDP）ポート 848 が使用されます（Network Address Translation-Traversal（NAT-T）が使用されている場合、ポートは 4500 まで変化します）。

IPSec

IPsec は、IP レイヤのトラフィックのための各種セキュリティ サービスを提供するためのアーキテクチャが定義された、よく知られた RFC です。IETF RFC 2401 には、各種コンポーネントおよびそれらがどのように互いに組み合されて IP 環境を形成しているかが記述されています。

IPsec SA を更新するためのキー サーバとグループ メンバー間の通信フロー

キー サーバとグループ メンバーは、GET VPN アーキテクチャを構成する 2 つのコンポーネントです。キー サーバには、グループ認証キーと IPsec SA が保存され、グループ メンバーに対して提供されます。

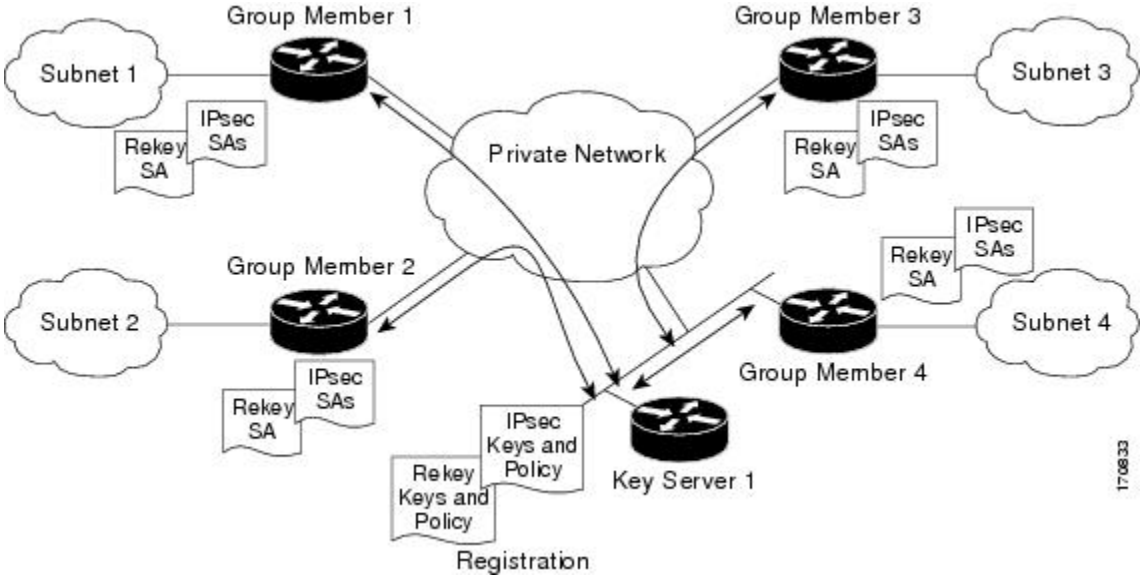
グループ メンバーでは、対象となるトラフィック（暗号化するに値し、IPsec によってセキュリティ保護されるトラフィック）に対して暗号化サービスが提供されます。

キー サーバとグループ メンバー間における通信は暗号化およびセキュリティ保護されます。GDOI には、TEK と KEK という 2 つのキーがサポートされています。TEK は、キー サーバからすべてのグループ メンバーにダウンロードされます。ダウンロードされた TEK は、グループ メンバー間で安全に通信するためにすべてのグループ メンバーで使用されます。このキーは、実質的には、すべてのグループ メンバーによって共有されるグループ キーとなります。グループ ポリシーおよび IPsec SA は、グループ メンバーへの定期的なキーの再生成メッセージを使用して、キー サーバによってリフレッシュされます。KEK もキー サーバによってダウンロードされ、グループ メンバーによって、キー サーバから受信するキーの再生成メッセージの復号化に使用されます。

キー サーバによって、GDOI グループのグループ ポリシーと IPsec SA が生成されます。キー サーバによって生成される情報には、複数の TEK 属性、トラフィック暗号化ポリシー、ライフタイム、送信元と宛先、各 TEK に関連付けられるセキュリティ パラメータ インデックス（SPI）ID、キーの再生成ポリシー（1 つの KEK）などがあります。

次の図に、グループ メンバーおよびキー サーバ間の通信フローを示します。キー サーバは、グループ メンバーからの登録メッセージを受信したあと、グループ ポリシーと新しい IPsec SA を含む情報を生成します。次に、新しい IPsec SA がグループ メンバーにダウンロードされます。キー サーバでは、グループごとに、各グループ メンバーの IP アドレスを含むテーブルが保持されます。グループ メンバーが登録されると、キー サーバはメンバーの IP アドレスを関連するグループのテーブルに追加します。これにより、キーサーバは、アクティブなグループ メンバーをモニタできるようになります。1 つのキー サーバで複数のグループをサポートできます。また、1 つのグループ メンバーは、複数のグループに属することができます。

図 *4*：グループ メンバーおよびキー サーバ間の通信フロー



IPsec と ISAKMP タイマー

IPsec と ISAKMP SA は、次のタイマーによって維持されます。

- TEK ライフタイム：IPsec SA のライフタイムを決定します。TEK ライフタイムが終了する前に、キー サーバによってキー再生成メッセージが送信されます。このメッセージには、新しい TEK 暗号キーと変換、および既存の KEK 暗号キーと変換が格納されています。TEK ライフタイムはキー サーバ上でだけ設定します。ライフタイムは、GDOI プロトコルによって各グループ メンバーに対して「プッシュ ダウン」されます。TEK ライフタイムの値はネットワークのセキュリティ ポリシーによって異なります。**setsecurity-associationlifetime** コマンドが設定されていない場合、デフォルト値である 86,400 秒が有効になります。TEK ライフタイムを設定するには、「IPsec ライフタイム タイマーの設定」セクションを参照してください。

- KEK ライフタイム：GET VPN キー再生成 SA のライフタイムを決定します。ライフタイムが終了する前に、キー サーバによってキー再生成メッセージが送信されます。このメッセージには、新しい KEK 暗号キーと変換、および新しい TEK 暗号キーと変換が格納されています。TEK ライフタイムはキー サーバ上でだけ設定します。ライフタイムは、GDOI プロトコルによって各グループ メンバーに対して動的にプッシュ ダウンされます。KEK ライフタイム値は、TEK ライフタイム値よりも大きい必要があります（KEK ライフタイム値は、TEK ライフタイム値の少なくとも 3 倍以上にすることが推奨されます）。**rekeylifetime** コマンドが設定されていない場合、デフォルト値である 86,400 秒が有効になります。KEK ライフタイムを設定するには、「マルチキャスト キー再生成の設定」セクションを参照してください。
- ISAKMP SA ライフタイム：ISAKMP SA が期限切れになる前にどれだけの期間存在するべきかを定義します。ISAKMP SA ライフタイムは、グループ メンバーおよびキー サーバ上で設定します。グループ メンバーとキー サーバに連携可能なキー サーバがない場合、グループ メンバーの登録が終了しても ISAKMP SA は使用されません。このような（連携可能なキー サーバがない）場合、ISAKMP SA のライフタイムを短く設定できます（最小 60 秒）。連携可能なキー サーバが存在する場合は、連携可能なキー サーバの通信中に ISAKMP SA を「アップ」の状態に保つため、すべてのキー サーバのライフタイムを長く設定する必要があります。**lifetime** コマンドが設定されていない場合、デフォルト値である 86,400 秒が有効になります。ISAKMP SA ライフタイムを設定するには、「ISAKMP ライフタイム タイマーの設定」セクションを参照してください。

アドレス保存

ここでは、GET VPN でのアドレス保存について説明します。

以下の図に示すように、IPsec で保護されたデータ パケットでは、外側の IP ヘッダーで元の送信元と宛先が伝送されます。トンネル エンドポイントのアドレスには置換されません。この技術は、IPsec Tunnel Mode with Address Preservation と呼ばれています。

図 *5*：ヘッダー保存

GET VPN では、アドレスが維持されるため、コア ネットワーク内のルーティング機能を使用できます。アドレスの維持によって、ネットワーク内の、宛先アドレスへのルートをアドバタイズする任意のカスタマー エッジ（CE）デバイスにパケットを配送するルーティングが可能となります。グループのポリシーに一致するすべての送信元および宛先は、同様に処理されます。アドレスの維持は、IPsec ピア間のリンクが利用できない状況では、トラフィックの「ブラックホール」状況に対処するのに役立ちます。

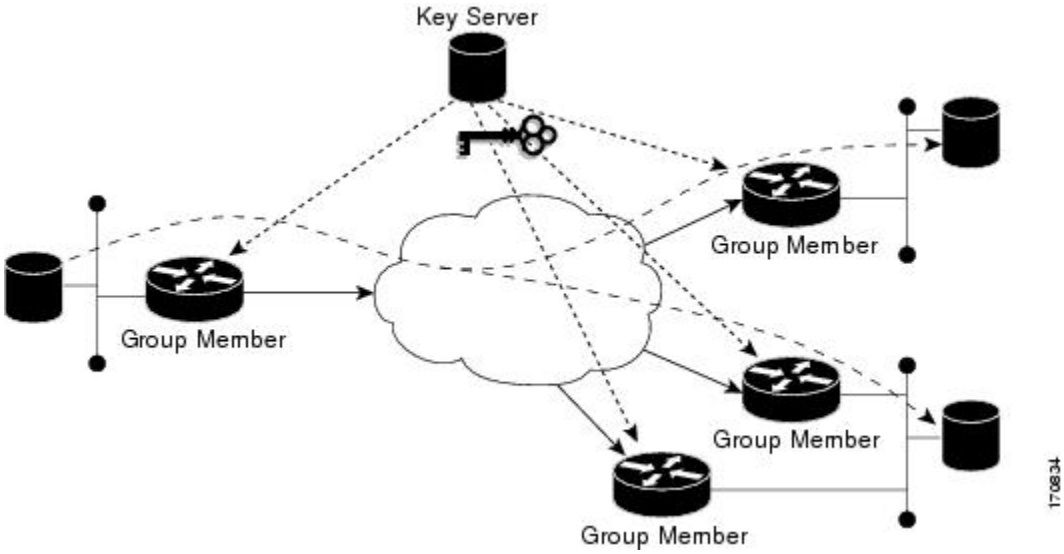
また、ヘッダーが維持されることによって、企業のアドレス空間全体および WAN においてルーティングの継続性が維持されます。その結果、キャンパスのエンド ホスト アドレスは WAN に公開されます（MPLS では、これは WAN のエッジに適用されます）。このため、GET VPN は、

WAN ネットワークが「プライベート」ネットワークとして動作する場合にだけ適用できます（MPLS ネットワークなど）。

セキュア データ プレーン マルチキャスト

マルチキャストの送信元では、キーサーバから取得される TEK が使用され、ヘッダーが保存されたマルチキャストデータパケットが、スイッチングされる前に暗号化されます。マルチキャストパケットのレプリケーションが、マルチキャスト パケット内に保持されている（S,G）ステートに基づいてコア内で実行されます。次の図に、このプロセスを示します。

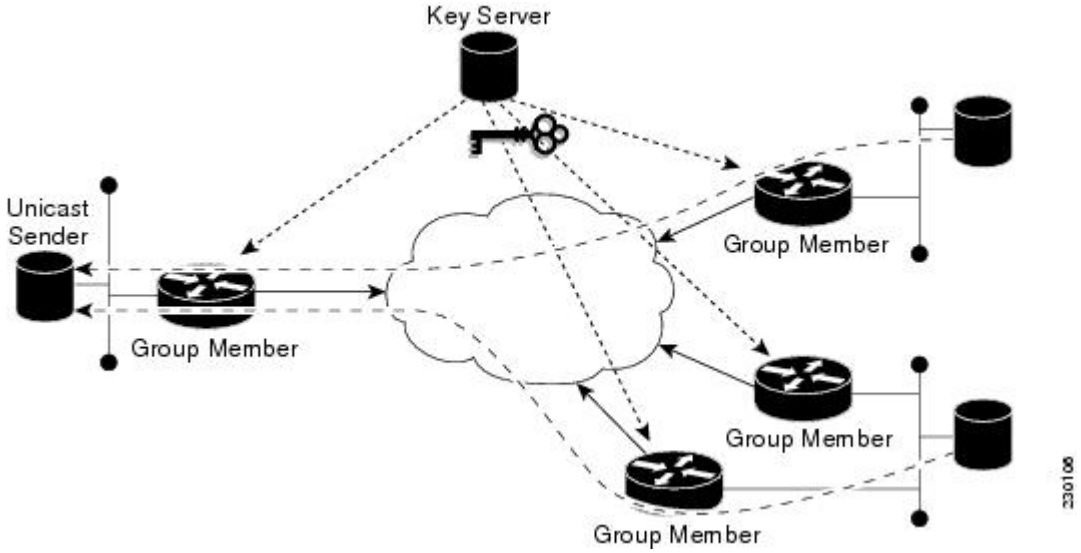
図 *6*：セキュア データ プレーン マルチキャスト プロセス



セキュア データ プレーン ユニキャスト

ユニキャストの送信元では、キー サーバから取得される TEK が使用され、ヘッダーが保存されたユニキャストデータパケットが、宛先にスイッチングされる前に暗号化されます。次の図に、このプロセスを示します。

図 7: セキュア データ プレーン ユニキャスト プロセス



Cisco Group Encrypted Transport VPN の機能

キー再生成

キー再生成は IPsec SA を更新するために使用されます。IPsec SA またはキー再生成 SA の期限切れが近づくと、特定のグループの単一のキー再生成メッセージがキー サーバ上で生成されます。キー再生成の配信のために新しいIKEセッションが生成されることはありません。キー再生成メッセージは、キー サーバによって、既存の IKE SA を介して配信されます。

キー再生成では、マルチキャスト メッセージまたはユニキャスト メッセージを使用できます。GET VPN では、ユニキャスト キー再生成とマルチキャスト キー再生成の両方がサポートされています。

CSCti89255 では、KEK タイマーが期限切れになる前に KEK のキー再生成が行われます。グループ メンバーもタイマーを開始し、タイマーの期限が切れる前に更新されたキーを受け取ることを期待します。これらを受け取らない場合、グループ メンバーは KEK の期限切れの前にジッタが生じた再登録を開始します。KEK ライフタイムが期限切れになると、KEK は削除されます。これにより以下が確保されます。

- より安全な KEK の有効期限確認メカニズム

- より安全な KEK の再登録メカニズム
- 設定されたライフタイムを超える KEK の使用の回避

次のサブセクションではキー再生成の詳細情報を提供します。

キー再生成シーケンス番号のチェック

キーサーバとグループメンバー間のキー再生成シーケンス番号のチェックは次のように行われます。

1. GROUPKEY-PUSH メッセージのアンチリプレーは RFC 6407 で規定されているように復元されます。
   - グループ メンバーは、最後に受信したキー再生成メッセージのシーケンス番号以下の番号のキー再生成メッセージをすべてドロップします。
   - グループ メンバーは、最後に受信したキー再生成メッセージのシーケンス番号より大きい番号のキー再生成メッセージをすべて（差がどれだけ大きくても）承認します。
2. シーケンス番号は、KEK 再生成メッセージ時ではなく、KEK 再生成キーの後の最初のキー再生成メッセージ時に 1 にリセットされます。

マルチキャスト キー再生成

マルチキャストキー再生成は、有効なマルチキャストキー再生成が使用されて送信されます。登録が成功すると、グループメンバーが特定のマルチキャストグループに登録されます。グループに登録されているすべてのグループメンバーによって、このマルチキャストキー再生成が受信されます。マルチキャストキー再生成は、キーサーバに設定されているライフタイムに基づいて定期的に送信されます。IPsec またはキー再生成ポリシーがキーサーバ上で変更された場合もマルチキャスト キー再生成が送信されます。設定の変更によってトリガーされると、キー再生成によって、新しく更新されたポリシーが有効なマルチキャストキー再生成を持つすべてのグループメンバーに送信されます。

キー サーバによって、キー再生成の時間が次のようにプッシュ バックされます。

1.TEK のタイムアウトが 300 秒の場合：

tek_rekey_offset = 90（300 < 900 のため）

再送信が設定されている場合、キー再生成タイマーがさらに戻されます。

3 つの再送信がすべて 10 秒の場合：3 * 10

その結果、キー再生成が実際に発生するのは (300 - 90 - 30) = 180 秒

2.TEK のタイムアウトが 3600 秒の場合：

tek_rekey_offset = 3600 * 10% = 360 秒

再送信が設定されている場合、キー再生成タイマーがさらに戻されます。

3 つの再送信がすべて 10 秒の場合：3 * 10

その結果、キー再生成が実際に発生するのは (3600 - 360 - 30) = 3210 秒

KEK の期限が切れ、転送モードがマルチキャストである場合、マルチキャスト KEK キー再生成が送信されます。マルチキャスト KEK が送信されると、グループ メンバーによって古い KEK が新しい KEK に置き換えられます。これはマルチキャスト キー再生成であり、再送信が送信されるので、古いKEKは引き続き暗号化に使用されます。このような状況が発生するのは、グループ メンバーによって新しいKEKキー再生成が受信されていないためです。そのため、マルチキャスト キー再生成を受信したグループ メンバーには古い KEK は存在せず、それらの再送信は廃棄されます。

最初に KEK キーを受信せず、現在は KEK 再送信を受信して古い KEK を新しい KEK に置き換えているグループ メンバーの場合、後の再送信は廃棄されます。たとえば、5 つの再送信が設定されており、シーケンス番号が 1 のマルチキャスト KEK キー再生成がグループ メンバー 1 で受信される場合、グループ メンバーに古い KEK がないため、シーケンス番号が 2、3、4、5、6 である他のすべての再送信は廃棄されます。

グループ メンバー 2 によってシーケンス番号が 1 の KEK キー再生成が取得されず、シーケンス番号が 2 である再送信が受信された場合、他の再送信 3、4、5、6 は廃棄されます。

マルチキャスト キー再生成の設定要件

グループ メンバーがキー サーバに登録するときは、データベースに KEK SA をインストールします。キー再生成の転送がマルチキャストのとき、グループ メンバーは IGMP を使用して、キー サーバによって定義されたマルチキャスト ストリームに参加します。IGMP 参加は、暗号マップを含むインターフェイスから送信されます。

（注） IGMP トラフィックは、キー サーバで定義された ACL またはグループ メンバーのローカル拒否 ACL による暗号化から除外する必要があります。

暗号マップを使用して設定されたものと同じインターフェイス経由でキー サーバに到達できないときは、ストリームに手動で参加する必要があります。

ユニキャスト キー再生成と SA

大型のユニキャストグループでは、遅延問題を軽減するため、キーサーバによって一度にごく少数のグループメンバーのキー再生成メッセージだけが生成されます。すべてのグループメンバーによって、古いSAの期限が切れる前に新しいSAの同じキー再生成メッセージが受信されることが、キー サーバには保証されています。さらに、ユニキャスト グループでは、キー サーバからのキー再生成メッセージが受信された後、グループ メンバーによって、暗号化された確認応答（ACK）メッセージが、キー再生成メッセージの一部として受信されたキーが使用されて、キー サーバに送信されます。キー サーバによって ACK メッセージが受信されると、その受信が関連するグループのテーブルに書き込まれ、次のことが実行されます。

- キー サーバにアクティブなグループ メンバーの最新リストが保管されます。
- キー サーバによって、アクティブなメンバーにだけキー再生成メッセージが送信されます。

さらに、ユニキャストグループでは、3 回連続したキー再生成が行われて ACK メッセージが 1 つもキー サーバによって受信されなかった場合、キー サーバによってアクティブ リストからグループ メンバーが削除され、その特定のグループ メンバーに対するキー再生成メッセージの送信が停止されます。3 回連続したキー再生成が行われて ACK メッセージが 1 つも受信されなくても、グループ メンバーがキー再生成メッセージを受信する必要がある場合には、現在の SA が期限切れになった後には、グループ メンバーはキー サーバに完全に再登録される必要があります。非応答グループ メンバーのイジェクトは、キー サーバがユニキャスト キー再生成モードで動作している場合にだけ行われます。マルチキャスト キー再生成モードでは、キー サーバによるグループ メンバーの排出は行われません。そのモードでは、グループ メンバーが ACK メッセージを送信できないからです。

マルチキャスト キー再生成におけるのと同様、再送信が設定されている場合、各キー再生成は、設定された回数再送信されます。

キー再生成転送モードおよび認証は、GDOI グループ下で設定できます。

ユニキャスト キー再生成転送モードが定義されていない場合、デフォルトでマルチキャストが適用されます。

TEK キー再生成が受信されなかった場合、現在の IPsec SA が期限切れになる 60 秒前にグループ メンバーがキー サーバに再登録されます。グループ メンバーの再登録が発生する前に、キー サーバによってキー再生成が送信される必要があります。再送信が設定されていない場合、SA が期限切れになる前に、キー サーバによってキー再生成 tek_rekey_offse が送信されます。tek_rekey_offset は、設定されているキー再生成ライフタイムに基づいて算出されます。TEK キー再生成のライフタイムが 900 秒より短い場合、tek_rekey_offset は 90 秒に設定されます。TEK キー再生成のライフタイムが 900 秒を超えるように設定されている場合、rekey_offset = (設定されている TEK キー再生成のライフタイム)/10 となります。再送信が設定されている場合、SA が期限切れになる 90 秒前に最新の再送信が送信されるように、tek_rekey_offset よりも前にキー再生成が発生します。

キー サーバでは、すべてのユニキャスト グループ メンバーに対するキー再生成の送信をいつ開始するか計算するために、次の例に示す数式が使用されます。キー サーバにおけるユニキャスト キー再生成処理によって、1 回のループで 50 のグループにおけるユニキャスト グループ メンバーに対してキー再生成が送信されます。このループ内でかかる時間は推定 5 秒です。

キー サーバによって、50 のグループのグループ メンバーのキー再生成が行われます。これは 2 回のループに相当します。たとえば、グループ メンバーの数が 100 の場合：

キー再生成ループの数 = (100 グループ メンバー)/50 = 2 ループ：

- 1 回のループでのキー再生成にかかる時間（推定）= 5 秒
- 50 の 2 回ループにおける 100 グループ メンバーに対するキー再生成にかかる時間：2 * 5 秒 = 10 秒

そのため、キー サーバによって、キー再生成の時間が次のようにプッシュ バックされます。

- TEK のタイムアウトが 300 の場合：300 - 10 = 290

ただし、開始は TEK が期限切れになるよりも前である必要があります（マルチキャストの場合と同じです）。

- 300 < 900 であるため、tek_rekey_offset = 90

- そのため、実際の TEK 時間から 90 秒を引いて、290 - tek_rekey_offset = 200 秒

再送信が設定されている場合、キー再生成タイマーがさらに戻されます。

- 3 つの再送信がすべて 10 秒の場合：200 - (3 * 10) = 170
- TEK のタイムアウトが 3600 秒である場合：3600 - 10 = 3590

ただし、開始はTEKが期限切れになるよりも前である必要があります（マルチキャストの場合と同じです）。

- 3600 > 900 であるため、tek_rekey_offset = 3600 * 10% = 360
- そのため、実際の TEK 時間から 360 秒を引いて、3590 - tek_rekey_offset = 3230 秒

再送信が設定されている場合、キー再生成タイマーがさらに戻されます。

- 3 つの再送信がすべて 10 秒の場合：3230 - (3 * 10) = 3200 秒

数式 tek_rekey_offset は、ユニキャストおよびマルチキャスト キー再生成に適用されます。

ポリシー変更後のキー再生成の動作

次の表に、セキュリティ ポリシーの変更に対応したキー再生成の動作の一覧を示します。

表 *1*：セキュリティ ポリシー変更後のキー再生成の動作

ポリシーの変更	キー再生成を送信するか	ポリシー変更後のキー再生成の動作
TEK：SA ライフタイム	No	古い SA は、そのライフタイムが期限切れになるまでアクティブのままになります。新しいライフタイムは、次にスケジュールされたキー再生成の後に有効になります。
TEK：IPSEC トランスフォーム セット	Yes	古いトランスフォーム セットの SA は、そのライフタイムが期限切れになるまでアクティブのままになります。
TEK：IPSEC プロファイル	Yes	古いプロファイルの SA は、そのライフタイムが期限切れになるまでアクティブのままになります。

ポリシーの変更	キー再生成を送信するか	ポリシー変更後のキー再生成の動作
TEK：一致する ACL	Yes	発信パケット分類では、即座に新しいアクセス コントロール リスト（ACL）が使用されます。古い SA は SA データベース内に保存されたままになります。
TEK：リプレイ カウンタのイネーブル化	Yes	カウンタ リプレイがない古い SA は、そのライフタイムが期限切れになるまでアクティブのままになります。
TEK：リプレイ カウンタの変更	No	新しいリプレイ カウンタがある SA は、次にスケジュールされたキー再生成時に送信されます。
TEK：リプレイカウンタのディセーブル化	Yes	カウンタ リプレイがイネーブルになっている古い SA は、そのライフタイムが期限切れになるまでアクティブのままになります。
TEK：受信専用のイネーブル	Yes	受信専用モードは、キー再生成後ただちにアクティブになります。
TEK：受信専用のディセーブル	Yes	受信専用モードは、キー再生成後ただちに非アクティブになります。
KEK：SA ライフタイムの動作	No	変更は次のキー再生成時に適用されます。
KEK：認証キーの変更	Yes	変更は次のキー再生成時に適用されます。
KEK：暗号アルゴリズムの変更	Yes	変更は即時に適用されます。

ポリシーの変更を即時に有効にするには、次の手順に従います。

- キー サーバで **clearcryptogdoi [group]** コマンドを使用します。

- すべてのグループ メンバーで **clearcryptogdoi** [**group**] コマンドを使用します。

（注） キー サーバは管理者がコンフィギュレーション モードを終了するとポリシーの更新のためのキー再生成を送信し、適切な場合にキー再生成が送信されるようにします。

（注） グループ メンバーで双方向モードに変更する前のパッシブ モードの動作は次のとおりです。

キー サーバの SA モードを「no sa receive-only」に変更し、コンフィギュレーション モードを終了する場合、キー再生成はグループ メンバーに送信され、「受信専用」から「発信オプション」にグループ メンバーの状態が変化するのを確認できます。組み込みタイマーによって設定されたインターバル（約 5 分）の後は「両方」に状態が変化します。

キー サーバはこの状態をすぐに「両方」として示します。すべてのグループ メンバーが更新される過程である可能性があるため、これは意図的に行われます。

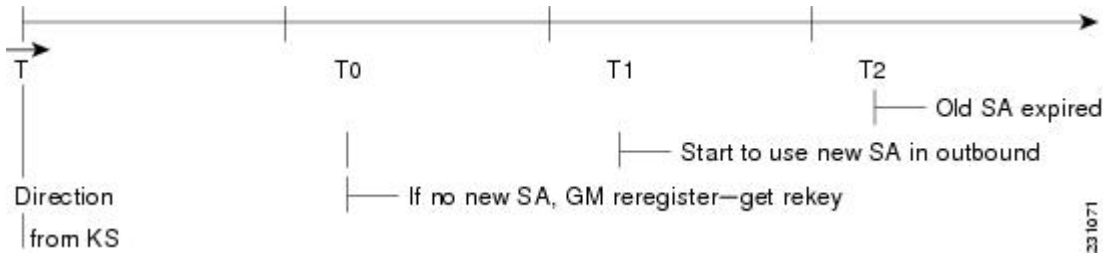
グループ メンバーにおける**IPsec SA** の使用

グループ メンバー上でキー再生成が受信され、処理されると、新しい IPsec SA（SPI）がインストールされます。古い IPsec SA と新しい IPsec SA が共に使用される期間が存在します。指定された一定期間の経過後に、古い IPsec SA は削除されます。この重複によって、すべてのグループ メンバーが現在のキー再生成を受信し、新しい IPsec SA を追加できます。この動作は、キー サーバからのキー再生成のための転送モード（マルチキャストまたはユニキャスト キー再生成転送）とは無関係です。

グループ メンバー上では、古い SA が期限切れになる約 30 秒前に、グループ メンバーによって、パケットを暗号化するために発信方向で新しい SA が使用されます。古い SA が期限切れになる約 60 秒前にキー サーバからのキー再生成を介して新しい SA がグループ メンバー側で受信されていない場合、グループ メンバーが登録されます。

次の図では、時間 T2 が古い SA が期限切れになる時間です。T1 が T2 の 30 秒前で、これは、グループ メンバー（GM）によって発信方向で新しい SA の使用が開始される時間です。T0 は、T2 の 30 秒前です。T0 の時点で新しい SA が受信されない場合、グループ メンバーが登録される必要があります。T は、T0 の 30 秒前です。T の時点でキー サーバによってキー再生成が送信される必要があります。

図 *8* : グループ メンバーにおける ***IPsec SA*** の使用



設定変更によってキー サーバごとのキー再生成のトリガーが可能

（注） セキュリティに対する脅威とそれに対抗するための暗号化技術は絶えず変化しています。暗号化に関するシスコの最新の推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

キーサーバ上の設定変更によって、キーサーバごとの再生成のトリガーが可能です。次のサンプル設定を参照し、サンプルに記述されたもののうち、キー再生成が発生する変更と発生しない変更を確認してください。

```
crypto ipsec transform-set gdoi-p esp-aes esp-sha-hmac
!
crypto ipsec profile gdoi-p
 set security-association lifetime seconds 900
set transform-set gdoi-p
!
crypto gdoi group diffint
 identity number 3333
 server local
  rekey algorithm aes 128
  rekey address ipv4 121
  rekey lifetime seconds 3600
  no rekey retransmit
  rekey authentication mypubkey rsa mykeys
  sa ipsec 1
   profile gdoi-p
   match address ipv4 120
   replay counter window-size 3
```

次に示すキー サーバ上での設定変更では、キー サーバからのキー再生成がトリガーされます。

- TEK 設定におけるすべての変更（例の「sa ipsec 1」）。
  - ACL（上記例の「match address ipv4 120」）が変更された場合。ACL におけるすべての追加、削除、または変更がキー再生成の原因となります。
  - TEK リプレイがキーサーバ上でイネーブルまたはディセーブルになっている場合、キー再生成が送信されます。
  - TEK 内の IPsec プロファイルの削除または追加（例の「profile gdoi-p」）。
  - マルチキャストからユニキャスト転送への変更。
  - ユニキャストからマルチキャスト転送への変更。

次に示すキー サーバ上での設定変更は、キー サーバからのキー再生成のトリガーとはなりません。

- TEK 下におけるリプレイ カウンタ ウィンドウ サイズの変更（例の「sa ipsec 1」）。
- キー再生成再送信の設定または削除。
- キー再生成 ACL の削除または設定。

- TEK ライフタイムの変更（上記例の「set security-association lifetime seconds 300」）または KEK ライフタイムの変更（例の「rekey lifetime seconds 500」）。
- キー再生成アルゴリズムの追加、削除、または変更（例の「rekey algorithm aes 128」）。

キー再生成をトリガーするコマンド

次の表は、GET VPN コマンドによる変更の包括的な一覧です。どのコマンドがキー再生成のトリガーとなり、どのコマンドがならないのかを示しています。各コマンドは、それらのコマンドが入力されるコンフィギュレーション モードに基づいて分類しています。表には、キー再生成のトリガーになるか否かを問わず、コマンドが有効になるタイミングも示しています。

表 *2*：キー再生成をトリガーするコマンド

説明	コマンド	キー再生成のトリガーとなるか	トリガーするタイミング	変更が有効になるタイミング
Mode = (config)	**configureterminal**	—	—	—
GDOI グループ内で使用される ACL の変更または削除（例：**deny ip** *access-number* [*options*]）	[**no**] **access-list** *access-number* [*options*]	No	—	即時

説明	コマンド	キー再生成のトリガーとなるか	トリガーするタイミング	変更が有効になるタイミング
IPsec プロファイルで使用される ACL の変更または削除（例：**match address ipv4** *access-list-id* | *name*[*options*]）	[**no**] **access-list** *access-list-number*[*options*]	Yes	コンフィギュレーションモードの終了時	キーサーバ上での **show running-config** コマンドの出力は、ポリシーが不完全である、パケットがまだ既存の SA によって暗号化または復号化されている、ダウンロードされた ACL は消去されたが mtree エントリがまだ存在している（**show crypto ruleset** コマンドの出力を表示することによる）、および、新しい SA がダウンロードされず、古い SA が暗号化または復号化でまだアクティブであることを示します。
ISAKMP 事前共有キー（任意のキー）の追加または削除	**crypto isakmp key** *keyadd address*	No	—	即時
ISAKMP 事前共有キー（グループメンバーのキー）の追加または削除	**crypto isakmp key** *keyadd address*	No	—	Key Encryption Key（KEK）SA が期限切れになった後（再登録）
IPsec プロファイルの追加	**crypto ipsec profile**	No	—	即時
ISAKMP ポリシーの追加または削除	**crypto isakmp policy** *priority*	No	—	即時

説明	コマンド	キー再生成のトリガーとなるか	トリガーするタイミング	変更が有効になるタイミング
Mode = (ipsec-profile)	**crypto ipsec profile** *name*	—	—	—
（IPsec プロファイル内の）SA ライフタイムの変更	**set security-association lifetime seconds**	No	—	次のキー再生成
トランスフォームセットの変更	**set transform-set** *transform-set-name*	Yes	コンフィギュレーションモードの終了時	古いトランスフォームセットの SA は、ライフタイムが期限切れになるまでアクティブのままになります。
Mode = (config-gdoi-group)	**crypto gdoi group** *group-name*	—	—	—
ID 番号の変更	**identity number** *number*	No	—	グループメンバー上でただちに設定する必要があります。他のグループメンバーでは、古いグループ ID の TEK および KEK が引き続き使用されます。
Mode = (gdoi-local-server)	**server local**	—	—	—
ユニキャストからマルチキャスト転送への変更	**rekey transport unicast**	Yes	即時	キー再生成がトリガーされた後
マルチキャストからユニキャスト転送への変更	**[no] rekey transport unicast**	Yes	コンフィギュレーションモードの終了時	キー再生成がトリガーされた後

説明	コマンド	キー再生成のトリガーとなるか	トリガーするタイミング	変更が有効になるタイミング
キー再生成アドレスの変更	**rekeyaddressipv4** {*access-list-number* | *access-list-name*}	Yes	コンフィギュレーションモードの終了時	キー再生成がトリガーされた後（ただし、ACL 自体を変更してもマルチキャストキー再生成はトリガーされません)
キー再生成ライフタイムの変更	**rekeylifetimeseconds** *number-of-seconds*	No	—	次のキー再生成。ただし、コマンドが発行される（現在のライフタイムがキー再生成と共に送信される）と、ライフタイムは減少を開始します。
キー再生成再送信のイネーブル化またはディセーブル化	**rekeytransmit** *number-of-seconds* [**number** *number-of-transmissions*]	No	—	次のキー再生成
キー再生成認証のイネーブル化	**rekeyauthentication** [**primary** | **secondary**]	Yes	コンフィギュレーションモードの終了時	キー再生成がトリガーされた後
キー再生成認証のディセーブル化	[**no**] **rekeyauthentication**	No	—	即時
キー再生成認証キーの変更	**rekeyauthentication** [**primary** | **secondary**]	Yes	コンフィギュレーションモードの終了時	キー再生成がトリガーされた後
キー再生成暗号化の変更	**rekeycipher** *type-for-rekey-cipher*	Yes	コンフィギュレーションモードの終了時	新しいアルゴリズムは即座に有効になります。
Mode = (gdoi-sa-ipsec)	**saipsec** *sequence-number*	—	—	—

説明	コマンド	キー再生成のトリガーとなるか	トリガーするタイミング	変更が有効になるタイミング
プロファイルの変更	**profile** *ipsec-profile-name*	Yes	コンフィギュレーションモードの終了時	ライフタイムが期限切れになるまで古いプロファイルの SA は有効のままです。
ACL の一致の変更	**matchaddress** [options]	Yes	コンフィギュレーションモードの終了時	キー再生成がトリガーされた後
カウンタリプレイのイネーブル化	**replaycounterwindowsize** *seconds*	Yes	コンフィギュレーションモードの終了時	ライフタイムが期限切れになるまでカウンタリプレイなしの古い SA は非アクティブになります。
リプレイカウンタ値の変更	**replaycounterwindowsize** *seconds*	No	—	次のキー再生成
時間ベースのアンチ リプレイのイネーブル化	**replaytimewindowsize** *seconds*	Yes	コンフィギュレーションモードの終了時	時間ベースのアンチ リプレイがイネーブルになった新しい SA が送信されますが、時間ベースのアンチリプレイがディセーブルになった古い SA は、ライフタイムが期限切れになるまでアクティブのままになります。

説明	コマンド	キー再生成のトリガーとなるか	トリガーするタイミング	変更が有効になるタイミング
時間ベースのアンチ リプレイ ウィンドウの変更	**replay time window-size** *seconds*	No	—	新しい時間ベースのアンチリプレイウィンドウが有効になるのは、キーサーバとグループメンバーの両方で **clearcryptogdoi** コマンドが入力された後だけです。
Mode = (gdoi-coop-ks-config)	**冗長性**	—	—	—
冗長性のイネーブル化	**冗長性**	No	—	他の各キーサーバ上でただちに設定する必要があります。
ローカルプライオリティの変更	**localpriority** *number*	No	—	即時にですが、キーサーバに選択は強要しません。
ピアアドレスの追加または削除	[**no**]**peer address ipv4** *ip-address*	No	—	次の連携可能な（COOP）メッセージ
冗長性のディセーブル化	[**no**]**redundancy**	No	—	他の各キーサーバ上でただちに設定する必要があります。

疑似時間同期によってタイムアウトが発生した場合、KEK タイマーまたは TEK タイマーのどちらかが次の 60 秒間に期限切れになるようにスケジュールされているかどうかがキーサーバによって確認されます。そのようにスケジュールされている場合、そのタイムアウトと疑似時間同期タイムアウトが結合されます。つまり、そのキー再生成は TEK キー再生成または KEK キー再生成と、疑似時間同期タイムアウト キー再生成の両方として動作します。疑似時間同期の詳細については、「時間ベースのアンチ リプレイ」セクションを参照してください。

キー再生成の再送信

マルチキャスト キー再生成は、デフォルトで再送信されます。ユニキャスト キー再生成では、キー サーバが ACK を受信しない場合にキー再生成が再送信されます。どちらの場合も、キー再生成の再送信前に、次の 120 秒間にスケジュールされている TEK キー再生成または KEK キー再生成があるかどうかがキー サーバによって確認されます。ある場合、現在の再送信は停止され、スケジュールされたキー再生成が発生するまで待機します。

グループ メンバー アクセス コントロール リスト

GET VPN の場合、保護する必要があるトラフィックは、ACL によってキー サーバ上にスタティックに定義されます。グループ メンバーによって、キー サーバから保護対象に関する情報が取得されます。この構造によって、キー サーバによる必要に応じたポリシーの動的な選択および変更が可能となっています。Secure Multicast では、キー サーバの ACL が包括的に定義されます。ACL には、暗号化する必要があるトラフィックだけが厳密に定義されているだけでなく、暗黙の拒否によって、他のすべてのトラフィックは暗号化されない状態で許可されるようになっています（つまり、許可がない場合、他のすべてのトラフィックは許可されます）。

GET VPN では、異なる考え方が採用されています。つまり、暗号化する必要のあるパケットの定義が独立して配信されます。GET VPN でサポートしているのはスタティックに定義されたトラフィック セレクタだけです。キー サーバ上で、拒否 ACL と許可 ACL の両方を使用してポリシーを定義できます。グループ メンバー上で、手動で設定できるのは拒否 ACL だけです。キー サーバからダウンロードされるポリシーと、グループ メンバー上で設定されるポリシーは結合されます。グループ メンバー上で設定された ACL はすべて、キー サーバからダウンロードされたものよりも優先されます。

グループ メンバーによってキー サーバから ACL が取得されると、グループ メンバーによって、一時的な ACL が作成され、それがデータベースに挿入されます。何らかの理由によりグループ メンバーが GDOI グループから削除されると、この ACL は削除されます。パケットが ACL に一致しているが、そのパケット用に IPsec SA が存在していない場合、インターフェイスから出ていくパケットは、グループ メンバーによって廃棄されます。

キー サーバによって一連のトラフィック セレクタが送信され、それらがグループ メンバー上のグループ メンバー ACL と正確には一致していない場合があります。このような違いが発生した場合、その違いを結合して解決する必要があります。グループ メンバーは、キーサーバよりもトポロジを認識するので、ダウンロードされた ACL は、グループ メンバー ACL の末尾に追加されます。グループ メンバー ACL（暗黙の拒否を除く）が最初にデータベースに挿入され、次に、ダウンロードされたキー サーバ ACL が挿入されます。このデータベースは優先化され、一致したエントリが検出された時はいつでも、データベース検索は終了します。

グループ メンバー ACL の設定方法については、「グループ メンバー ACL の設定」セクションを参照してください。

セキュリティ ポリシー変更時におけるグループ メンバーの動作

キー サーバでACLまたは他のポリシーが変更されると、グループ メンバーの動作が変わります。次の 3 種類のシナリオで、グループ メンバーの動作に対するポリシーの各種変更の影響を説明します。

シナリオ 1

次の例では、ホスト A とホスト B を許可するように ACL が最初に設定されています。

```
ip access-list extended get-acl
permit ip host A host B
permit ip host B host A
```

次に、キー サーバで、ホスト C とホスト D を許可するように ACL が変更されます。

```
ip access-list extended get-acl
permit ip host C host D
permit ip host D host C
```

ACL の変更は、次の方法でグループ メンバーの動作に影響を与えます。

- キー サーバによって、ただちに、すべてのグループ メンバーに対してキー再生成が送信されます。
- キー再生成後ただちに、グループ メンバーによって、ホスト A とホスト B 間のトラフィックが暗号化されていないテキストで送信されます。
- キー再生成後ただちに、グループ メンバーによって、ホスト C とホスト D 間のトラフィックが暗号化されたテキストで送信されます。

シナリオ 2

ポリシーによってトランスフォーム セットが更新され、時間ベースのアンチ リプレイ（TBAR）の変更がキー サーバに対して行われると、グループ メンバーの動作が変わります。

このシナリオでは、次のことが想定されています。

- トランスフォーム セットが、ESP-3DES から ESP-AES へ変更されている。
- ポリシーの変更は、現在の TEK ライフタイムが期限切れになる 1000 秒前に発生する。

これらのポリシーの変更は、次のようにグループ メンバーの動作に影響を与えます。

- キー サーバによって、古い SA（3DES）と新しい SA（AES）の両方のキー再生成が送信されます。
- グループ メンバーでは、期限切れになるまでの 1000 秒間、古い SA（3DES）の使用が継続されます。
- 古いSAが期限切れになると、グループ メンバーによって、新しいSA（AES）に自動的に切り替えられます。

シナリオ 3

キー サーバで、ACL の変更と、トランスフォーム セットや TBAR など他の変更の両方を含むその他のポリシーの更新が行われると、グループ メンバーの動作が変わります。

このシナリオでは、次のことが想定されています。

- ACL がシナリオ 1 で指定されたとおりに更新されている。
- トランスフォーム セットが、ESP-3DES から ESP-AES へ変更されている。
- ポリシーの変更は、現在の TEK ライフタイムが期限切れになる 1000 秒前に発生する。

ACL の変更とその他のポリシーの更新は、次のようにグループ メンバーの動作に影響を与えます。

- キー サーバによって、古い SA（3DES）と新しい SA（AES）の両方で構成されているキー再生成が送信されます。
- キー再生成後ただちに、グループ メンバーによって、ホスト A とホスト B 間のトラフィックが暗号化されていないテキストで送信されます。
- グループ メンバーによって、TEK のライフタイムが期限切れにならない限り 1000 秒間、古い SA（3DES）を使用した、ホスト C とホスト D 間の暗号化されたトラフィックが送信されます。
- 古い SA（3DES）が期限切れになると、グループ メンバーによる新しい SA への切り替えが自動的に行われ、AES におけるホスト C とホスト D 間のトラフィックが暗号化されます。

時間ベースのアンチリプレイ

アンチ リプレイは、IPSec（RFC 2401）のようなデータ暗号化プロトコルにおいて重要な機能の 1 つです。アンチ リプレイによって、第三者が IPsec カンバセーションを盗聴したり、パケットを盗んだり、さらにはそれらのパケットを後でセッションに挿入したりすることを防ぐことが可能です。時間ベースのアンチ リプレイ メカニズムを利用すれば、過去にすでに到着しているはずのリプレイ パケットを検出することによって、無効なパケットを廃棄できます。

GET VPN では、マルチセンダ トラフィック用のアンチ リプレイ保護を提供するために、同期アンチ リプレイ（SAR）が使用されています。SAR は、実社会のネットワーク タイム プロトコル（NTP）クロックや、シーケンシャル カウンタ メカニズム（パケットが送信順に受信されて処理されることを保証するメカニズム）とは独立しています。SAR クロックは、ルール正しく進みます。このクロックによって追跡される時間は、疑似時間と呼ばれます。疑似時間はキー サーバ上で維持され、キー再生成メッセージ内で指定されているグループ メンバーに対して、pseudoTimeStamp というタイムスタンプ フィールドとして定期的に送信されます。GET VPN では、Metadata というシスコ独自のプロトコルによって、psuedoTimeStamp をカプセル化しています。グループ メンバーは、定期的にキー サーバの疑似時間に再同期される必要があります。キー サーバの疑似時間は、最初のグループ メンバーが登録されたときから進み始めます。最初は、登録プロセス中に、キー サーバからグループ メンバーに対して、キー サーバの現在の疑似時間の値およびウィンドウ サイズが送信されます。時間ベースのリプレイ対応情報、ウィンドウ サイズ、キー サーバの疑似時間などの新しい属性は、SA ペイロード（TEK）で送信されます。

グループ メンバーは、疑似時間を使用して次のようにリプレイを防止します。pseudoTimeStamp には、送信者がパケットを作成したときの疑似時間の値が含まれています。受信者は、送信者の疑似時間の値と自身の疑似時間の値を比較して、パケットが再送されたパケットであるかどうかを判断します。受信元では、時間ベースのアンチ リプレイ「ウィンドウ」を利用して、そのウィンドウ内のタイプスタンプ値が格納されたパケットを受信します。ウィンドウ サイズは、キー サーバで設定されて、すべてのグループ メンバーに送信されます。

（注） グループ メンバーとして Cisco VSA を使用している場合、時間ベースのアンチ リプレイは使用しないでください。

次の図は、アンチリプレイ ウィンドウを示しています。値 PTr は受信者のローカルの疑似時間を、W はウィンドウ サイズを示しています。

図 *9*：アンチリプレイ ウィンドウ

クロック同期

グループ メンバーのクロックとキーサーバとの同期は、ずれたり失われたりする可能性があります。クロックの同期を維持するため、キー サーバの最新の疑似時間値が格納されたキー再生成メッセージ（マルチキャストがユニキャストかは状況に応じます）が（キー再生成メッセージで、あるいは、グループ メンバーに対して最小で 30 分ごとに）定期的に送信されます。このアンチ リプレイ チェックでパケットにエラーが発生した場合、送信元および受信元の両方の疑似時間がプリントされ、エラー メッセージが生成され、カウントの値が増分されます。

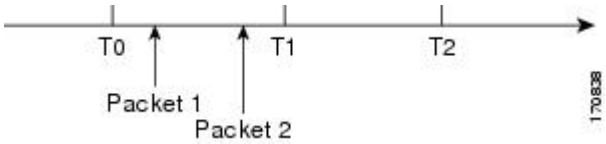
アンチ リプレイの統計情報を表示するには、送信元および受信元デバイスの両方で **show crypto gdoi group** *group-name* **gm replay** コマンドを使用します。管理者がサイズ設定のリプレイ方法に影響を与えるような設定変更を行った場合、キー サーバによってキー再生成メッセージが発信されます。

インターバル期間

ティックは、SAR クロックのインターバル期間です。この期間に送信された各パケットの pseudoTimeStamp は同じものになります。またティックは、キー サーバからの疑似時間と共にグループ メンバーにダウンロードされます。たとえば、インターバル期間 に示すように、T0 と T1 の間に送信されたパケットの pseudoTimeStamp は 同じ T0 になります。SAR には、ルーズなアンチ リプレイ保護が用意されています。リプレイされたパケットは、それらがウィンドウ内にリプ

レイされている場合は、受信されます。デフォルトのウィンドウ サイズは 100 秒です。パケットのリプレイを最小限に抑えるため、ウィンドウ サイズを小さく保つことを推奨します。

図 *10*：*SAR* クロックのインターバル期間



アンチ リプレイ設定

アンチ リプレイ機能をキー サーバ上の IPsec SA 下でイネーブルにするには、次のコマンドを使用します。

- **replaytimewindow-size**：非シーケンシャルまたは時間ベース モードがサポートされるリプレイ時間オプションをイネーブルにします。ウィンドウ サイズは秒単位です。このモードは、1 つのグループ内に 3 つ以上のグループ メンバーが存在している場合にだけ使用します。
- **replaycounterwindow-size**：シーケンシャル モードをイネーブルにします。このモードは、1 つのグループ内に 2 つのグループ メンバーだけが存在している場合に便利です。
- **noreplaycounterwindow-size**：アンチ リプレイをディセーブルにします。

コントロール プレーンの時間ベースのアンチリプレイ

キー再生成疑似時間のチェック

キー サーバとグループ メンバー間のキー再生成疑似時間のチェックは次のように行われます。

- グループ メンバーがキー サーバと自身との疑似時間の許容差を計算します。データ プレーンで設定された TBAR ウィンドウ サイズ、または 30 秒の小さい方となります。
- グループ メンバーは自身より疑似時間が大きいすべてのキー再生成を受け入れ、自身の疑似時間をより大きい値に更新します。計算された疑似時間の許容差よりも差が大きい場合は、次の syslog メッセージも生成されます。

```
*Jul 28 22:56:37.503: %GDOI-3-PSEUDO_TIME_LARGE: Pseudotime difference between key server
(20008 sec) and GM (10057 sec) is larger than expected in group GET. Adjust to new pseudotime
```

- グループ メンバーが自身よりも疑似時間が小さいが許容差以内のキー再生成を受信した場合、グループ メンバーはキー再生成を受け入れ、疑似時間値をそのキー再生成疑似時間値に更新します。

- グループ メンバーが自身よりも疑似時間が小さいが許容差を超えているキー再生成を受信した場合、グループ メンバーはキー再生成メッセージをドロップし、次の syslog メッセージを生成します。

```
*Jul 28 23:37:59.699: %GDOI-3-PSEUDO_TIME_TOO_OLD: Rekey received in group GET is too old
and fail PST check: my_pst is 22490 sec, peer_pst is 10026 sec, allowable_skew is 30 sec
```

セカンダリ キー サーバでの ANN メッセージ疑似時間の処理

連携キー サーバ間のポリシーおよびグループメンバー情報の同期には、連携キー サーバ通知（ANN）メッセージが使用されます。

セカンダリ サーバ キーは次のように ANN メッセージを処理します。

- セカンダリ キー サーバが ANN メッセージの許容疑似時間を計算します。データ プレーンで設定された TBAR ウィンドウ サイズの値、または 30 秒の小さい方となります。
- セカンダリ キー サーバが疑似時間がより大きいプライマリ キー サーバから ANN メッセージを受信した場合、次が行われます。
- 疑似時間をプライマリ キー サーバの値に更新します。
- 疑似時間の差が許容差よりも大きい場合は、次の syslog メッセージが生成されます。

```
*Jul 28 23:48:56.871: %GDOI-4-GDOI_ANN_TIMESTAMP_LARGE: COOP_KS ANN received from KS 10.0.8.1
 in group GET has pseudotime bigger than myself. Adjust to new pseudotime:
my_old_pst is 23147 sec, peer_pst is 30005 sec
```

- セカンダリ キー サーバが疑似時間がより小さいプライマリ キー サーバから ANN メッセージを受信した場合、次のようになります。
  - 差が許容範囲内の場合、セカンダリ キー サーバはそれを受け入れ、疑似時間をプライマリ キー サーバの値に更新します。
  - 差が許容範囲を超える場合は、次の syslog メッセージが生成されます。

```
*Jul 28 23:42:12.603: %GDOI-4-GDOI_ANN_TIMESTAMP_TOO_OLD: COOP_KS ANN from KS 10.0.8.1 in
group GET is too old and fail PST check:
my_pst is 22743 sec, peer_pst is 103 sec, allowable_skew is 10 sec
```

3 つの再送信要求の後、セカンダリ キー サーバが有効な疑似時間の ANN メッセージを受信していない場合は、次のように、新しいグループメンバー登録のブロックが開始されます。

```
*Jul 28 23:38:57.859: %GDOI-5-COOP_KS_VALID_ANN_TIMER_EXPIRED: This sec-KS has NOT received
 an ANN with valid pseudotime for an extended period in group GET. It will block new group
 members registration temporarily until a valid ANN is received
*Jul 29 00:08:47.775: %GDOI-5-COOP_KS_BLOCK_NEW_GM_REGISTER: This key server temporarily
blocks group member with ip-addr 10.0.0.2 from registering in group GET as it has not
received an ANN with valid pseudotime for prolonged period
```

セカンダリ キー サーバは、次のいずれかが発生するとグループ メンバー登録機能を再開します。

- プライマリ キー サーバから有効な疑似時間の ANN を受け取る。
- プライマリ キー サーバになる。
- **clearcryptogdoigroup** コマンドはセカンダリ キー サーバで実行されます。

プライマリ キー サーバでの ANN メッセージ疑似時間の処理

プライマリ サーバ キーは次のように ANN メッセージを処理します。

- ANN メッセージの許容疑似時間を計算します。データ プレーンで設定された TBAR ウィンドウ サイズの値、または 30 秒の小さい方となります。
- 疑似時間が小さいが許容差以内のセカンダリ キー サーバ ANN メッセージは受け入れられます。
- 疑似時間が小さいが許容差を超えている ANN メッセージは拒否されます。

ネットワークのマージ中は、次の条件が適用されます。

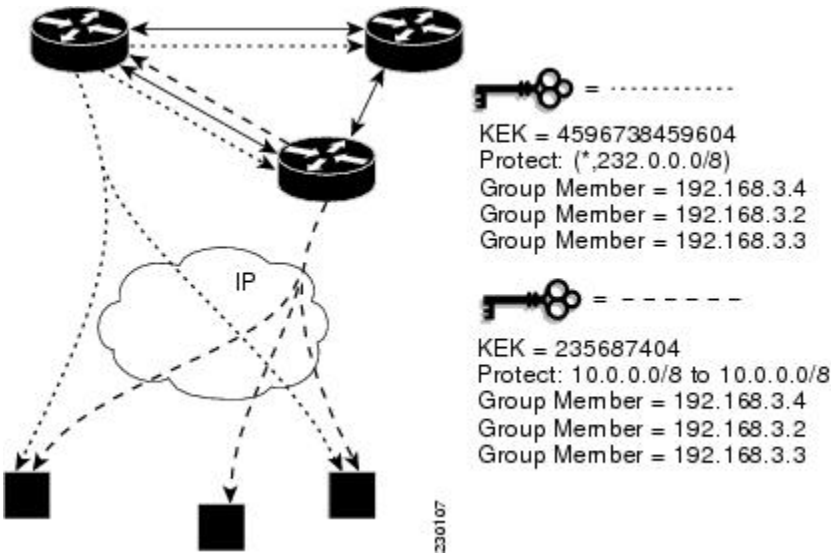
- 新しいプライマリ キー サーバは 2 つのキー サーバ間で大きい方の疑似時間を常に選択します。
- 差が計算された疑似時間の許容差よりも大きい場合、新しいプライマリ キー サーバはキー再生成をすべてのグループ メンバーに対して送信し、疑似時間を更新します。また、次の syslog メッセージも生成されます。

```
*Jul 28 23:42:41.311: %GDOI-5-COOP_KS_ELECTION: KS entering election mode in group GET
(Previous Primary = NONE)
*Jul 28 23:42:41.311: %GDOI-4-GDOI_ANN_TIMESTAMP_LARGE: COOP_KS ANN received from KS 10.0.9.1
 in group GET has PST bigger than myself. Adjust to new pseudotime:
my_old_pst is 0 sec, peer_pst is 22772 sec
*Jul 28 23:43:16.335: %GDOI-5-COOP_KS_TRANS_TO_PRI: KS 10.0.8.1 in group GET transitioned
to Primary (Previous Primary = NONE)
*Jul 28 23:43:16.347: %GDOI-5-KS_SEND_UNICAST_REKEY: Sending Unicast Rekey for group GET
from address 10.0.8.1 with seq # 1
```

連携キー サーバ

次の図は、連携キーサーバのキー配布を示したものです。図の下のテキストで、連携キーサーバ機能について説明します。

図 *11*：連携キー サーバのキー配布



連携キーサーバを利用すると、GET VPNに冗長性が与えられます。冗長性、高可用性、およびプライマリ キーサーバに障害が発生した場合の素早いリカバリを確保するために、複数のキーサーバがGET VPNによってサポートされます。複数の連携GDOIキーサーバによって、共同でグループの GDOI 登録が管理されます。各キー サーバはアクティブなキー サーバであり、各グループメンバーからの GDOI 登録要求を処理します。キー サーバどうしで連携しているので、各キーサーバから、そのキーサーバに登録するグループメンバーに対して同じ状態が配信されます。それぞれの GDOI キー サーバによって、GDOI 登録の一部を処理できるので、ロードバランスが実現します。

プライマリ キーの役割は、グループ ポリシーの作成と配信です。連携キー サーバのキー配布が発生すると、1 つのキー サーバが自身をプライマリとして宣言し、ポリシーを作成し、そのほかのセカンダリ キー サーバにポリシーを送信します。セカンダリ キー サーバは、ポリシーを取得して選択モードを終了すると、プライマリ キー サーバをプライマリ キー サーバとして宣言します。また、セカンダリ キーサーバは、連携キーサーバのキー配布が進行している間、GM 登録をブロックします。この変更により時間が短縮されるため、連携キー サーバの配布はより効率的になります。たとえば、配布時には次のような syslog の警告メッセージが表示されます。

```
00:00:16: %GDOI-5-COOP_KS_BLOCK_NEW_GM_REGISTER_ELECTION: This KS temporarily blocks GM
with ip-addr 10.0.4.1 from registering in group diffint as the KS election is underway
```

プライマリ キー サーバによってグループ情報のアップデートが他のすべてのキー サーバに定期的に送信（またはブロードキャスト）され、その結果、これらのサーバどうしの同期が維持されます。何らかの理由によりセカンダリ キーサーバがアップデートの受信に失敗した場合、そのセカンダリ キー サーバは、プライマリ キー サーバにアクセスして、直接情報のアップデートを要

求します。延長期間にアップデートが受信されない場合、セカンダリ キーサーバによって、プライマリ サーバが到達不能（つまり「dead」）としてマーキングされます。

新しいポリシーがプライマリ キー サーバで作成されると、グループ メンバーが登録されるキーサーバがどのサーバかにかかわらず、プライマリ キー サーバの役割は、GDOI グループ メンバーに対するキー再生成メッセージの配信となります。

連携キー サーバ設定では、キー再生成のシーケンス番号がプライマリおよびセカンダリ キー サーバ間で同期されます。

ネットワーク マージでは、キーサーバは両者の大きい方のキー再生成シーケンス番号が選択されます。

連携キー サーバの設定で 300 を超えるグループ メンバーをサポートしている場合、**buffers huge size** コマンドを使用してバッファ サイズを増やす必要があります。

連携キー サーバのアドレスのインターフェイスが閉じているとき、ネットワークは分割されます。インターフェイスが推奨設定である転送インターフェイスでない場合、キー再生成はグループ内のすべてのキー サーバからグループ メンバーに送信されます。このシナリオでは、**no crypto gdoi group***group name* コマンドを使用します。

通知メッセージ

通知メッセージは IKE フェーズ 1 によってセキュリティ保護され、IKE 通知メッセージとして送信されます。IKEによって提供される認証および機密保持は、キーサーバ間のメッセージをセキュリティ保護するために使用されます。通知メッセージ内のシーケンス番号によって、アンチ リプレイ保護が提供されます。通知メッセージは定期的にプライマリ キー サーバからセカンダリ キーサーバに送信されます。

通知メッセージには、現在の状態を維持するための次のコンポーネントが含まれます。

キー サーバの送信元プライオリティ

この値は送信元のプライオリティを示します。CLI によって設定可能です。最も高いプライオリティを持つキー サーバがプライマリ キー サーバとなります。プライオリティの値が同じ場合、最も高い IP アドレスを持つキー サーバがプライマリ キー サーバになります。

送信元のロールの維持

同期期間中、各キー サーバが地理的に分散した場所にある場合、それらのキー サーバにネットワーク分割イベントが発生する可能性があります。ネットワーク分割イベントが発生した場合、一定の期間中、複数のキーサーバがプライマリ キーサーバになる可能性があります。ネットワークが再び正常に動作し、すべてのキーサーバが互いに検知したら、各キーサーバがそれぞれの正しいロールを維持できるように、それらのサーバに対して、送信元の現在のロールを通知する必要があります。

リターン パケット フラグの要求

すべてのメッセージは一方向のメッセージとして定義されています。必要に応じて、キー サーバによってピアから現在の状態を要求し、そのロールを検出するか、グループの現在の状態を要求するかを行うことができます。

グループ ポリシー

グループ ポリシーは、任意のグループのために維持されるポリシーです。グループ メンバーの情報、IPsec SA、およびキーなどがあります。

アンチ リプレイ機能および組み込まれた連携通知メッセージがサポートされています。プライマリ キー サーバによって疑似時間値が更新され、その値がグループ内のすべてのセカンダリ キー サーバに送信されます。セカンダリ キー サーバによって、それらのサーバの SAR クロックとこの更新された値とが同期されます。

連携キー サーバ間の ANN メッセージ シーケンス番号のチェック

次に、連携キー サーバ間のシーケンス番号のチェックについて説明します。

- 連携キー サーバは、最後に受信した ANN メッセージのシーケンス番号以下の番号の ANN メッセージをすべてドロップします。
- ANN メッセージは、その差が大きくても、最後に受信したキー再生成メッセージよりシーケンス番号が大きい場合に承認されます。
- キーサーバがリロードされると、新しいIKEセッションがピア間に作成され、リロードされたキー サーバの ANN シーケンス番号はゼロから開始します。この場合、もう一方ではどのシーケンス番号の ANN メッセージも受け入れます。

キー サーバのロールの変更

連携キーサーバのネットワークでは、プライマリ サーバが、選択時における最も高いプライオリティに基づいて選択されます。他のキー サーバのステータスはセカンダリになります。プライマリ キー サーバが停止状態として検知されたり、そのロールが変更されたりした場合、**clearcryptogdoikscooprole** コマンドを使用すれば、プライマリ キー サーバの連携ロールをリセットできます。

clearcryptogdoikscooprole コマンドがセカンダリ キー サーバ上で実行されると、選択がそのセカンダリ キー サーバ上でトリガーされますが、すでに選択されているプライマリ キー サーバが存在しているため、たいての場合そのサーバはセカンダリ キーサーバのままとなります。しかし、**clearcryptogdoikscooprole** コマンドがプライマリ キー サーバ上で実行された場合、そのプライマリ キー サーバはセカンダリ ロールに再割り当てされ、その結果、すべてのキー サーバが関わる新しい選択がトリガーされます。前のプライマリ サーバのプライオリティが（すべてのキーサーバの中で）最も高い場合、そのサーバが再びプライマリ サーバになります。前のプライマリ サーバがプライオリティの最も高いサーバではない場合、プライオリティが最も高いサーバが新しいプライマリ サーバとして選択されます。

受信専用 SA

マルチキャストトラフィックでGDOIプロトコルが使用されている場合、双方向SAがインストールされます。受信専用機能を利用すれば、段階的な導入が可能となり、ネットワーク全体を稼働させる前にごく少数のサイトを確認できます。サイトをテストするには、グループ メンバーの 1 つが他のすべてのグループ メンバーに暗号化されたトラフィックを送信し、トラフィックを復号化してトラフィックを「暗号化せずに」転送させる必要があります。受信専用 SA モードでは、期間の受信方向のみで暗号化できます。（受信専用 SA プロセスの手順を参照してください）。キー サーバで **sareceive-only** コマンドを設定する場合、ステップ 2 および 3 は自動的に発生します。

1 GDOI キー サーバ上で IPsec SA を「受信専用」としてマーキングします。

これにより、グループ メンバーによる着信方向だけの SA のインストールが可能となります。受信専用 SA は、暗号グループの下で設定できます（「グループ ID、サーバ タイプ、および SA タイプの設定」セクションを参照してください）。

1 GDOI TEK ペイロードを「受信専用」としてマーキングします。

sareceive-only コマンドが設定されている場合、このグループ下のすべての TEK は、グループ メンバーへの送信時に、キー サーバによって「受信専用」としてマーキングされます。

1 一方向の IPsec フローのインストール

GDOI グループ メンバーによって、「受信専用」としてマーキングされているキー サーバからの IPsec SA が受信される度に、グループ メンバーによって、着信方向と発信方向の両方ではなく、着信方向だけでこの IPsec SA がインストールされます。

1 次のローカル変換コマンドを使用して個々のグループ メンバーをテストします。

2 **cryptogdoigmipsecdirectioninboundoptional**

3 **cryptogdoigmipsecdirectionboth**

最初に、個々のグループ メンバーを個別にpassiveモード（この変換により、発信チェックに対して有効な SA が存在することが通知されます）に変換してから、次に、双方向モードに変換します。

1 「受信専用」から「受信および送信」にグローバルに変換します。

テスト フェーズが終了し「受信専用」SA を双方向 SA に変換しなければならない時には、次の方式を使用できます。

グローバル変換

グループ下の **sa receive-only** コマンドを削除します。**sa receive-only** コマンドを削除すると、このグループの新しい IPsec SA が作成され、キー再生成が開始されます。受信と同時に、グループ メンバーによって、双方向で SA が再インストールされ、その SA の passive モードでの使用が開始されます。SA が永続的に passive モードでいることはできないので、5 分間キー再生成がなかっ

た場合、グループ メンバーによって、これらの SA が受信モードまたは送信モードに変更されます。passive モードから双方向暗号化モードへの変換は自動で行われるので、管理者は何もする必要はありません。

パッシブ SA

パッシブ SA 機能によって、グループ メンバーを、永続的に passive モードにするように設定できます。パッシブ SA 機能を使用すれば、**cryptogdoigmipsecdirectioninboundoptional** 特権 EXEC コマンドを使用する必要はなくなります。ただし、ルータのリロード後にこれが永続するわけではなく、キー再生成からのキー サーバ設定によって無効にできます。passive モードのグループ メンバーがあると、GET VPN への移行中におけるネットワーク テストやデバッグに利点があります。移行中に完全な暗号化保護を利用できるからです。グループ メンバーの passive モード設定は、キー サーバ設定よりも高いプライオリティを持ちます。**cryptogdoigmipsecdirectioninboundoptional** 特権 EXEC コマンドは、グループ メンバーとキー サーバの設定を元に戻す次のキー再生成まで設定を無効にすることができます。

パッシブ SA 機能を設定するには、「パッシブ SA の設定」セクションを参照してください。

拡張ソリューションの管理性

機能の確認を支援するために、複数の **show** コマンドおよび **debug** コマンドがサポートされています。詳細については、「Fail-Close モードのアクティブ化」セクションを参照してください。

VRF-Lite インターフェイスによるサポート

VRF-Lite アプリケーションでは、ルーティング テーブルをユーザ グループ（または VPN）ごとに分離することによって、コントロールプレーンおよびフォワーディングプレーンでのトラフィックのセグメンテーションがサポートされています。また、各ユーザ グループの関連インターフェイスまたは専用インターフェイス上のトラフィックが転送されます。

MPLS VPN ネットワークに接続されているリモート サイトによって、セグメンテーションをキャンパスから WAN へ拡張する導入シナリオがあります。このような拡張されたセグメンテーションの場合、CE（グループ メンバーまたはキー サーバ）デバイス上の CE-PE インターフェイスが、関連する Virtual Routing and Forwarding（VRF）に「バインド」されます。この VRF インターフェイスは、MPLS PE デバイスに接続されます。MPLS PE デバイスでは、VRF インターフェイスが関連するボーダーゲートウェイ プロトコル（BGP）VRF プロセスにマッピングされています。このような場合、クリプトマップが VRF インターフェイスに適用されます。他の設定変更は必要ありません。

GM 登録の認証ポリシー

GM は、事前共有キーまたは公開キーインフラストラクチャ（PKI）を使用して登録時にキー サーバに認証できます。事前共有キーは、展開が容易ですが、プロアクティブに管理する必要があります。シスコはネットワーク内のすべてのデバイスに対してデフォルト キー（0.0.0.0 のアドレス

で定義されるキー）を定義するのではなく、ピアベースの事前共有キーを展開することをお勧めします。事前共有キーは定期的に更新する必要があります（数ヵ月ごと）。

（注） キー再生成は KEK を使用してセキュリティが確保されるため、事前共有キーは暗号化データ プレーンまたはコントロール プレーンに影響を与えずにキー サーバ グループ メンバー（KS-GM）ピアごとに更新できます。新しく割り当てられた事前共有キーを使用して、発注済みの一連のキー サーバごとに GM を再登録できるようにすることが重要です。

PKI では、事前共有キーを使用するときに直面するキー管理の困難を克服するためにインフラストラクチャを使用します。PKI インフラストラクチャは認証局（CA）として機能し、ここでルータ証明書が発行され、維持されます。ただし、IKE 認証中に PKI を使用することは計算負荷が集中します。PKI の展開では、キー サーバのキャパシティ、設計、および配置が重要になります。

セキュリティを強化するため、GET VPN では事前共有キーまたは PKI を使用する GM 認証もサポートします。詳細については、「GET VPN 認証」セクションを参照してください。

GET VPN GM 認証

GET VPN GM 認証は、事前共有キーまたは PKI を使用して実行できます。GET VPN 認証をオンにすることはベスト プラクティスです。キー サーバが複数の GDOI グループに使用される際、あるグループの GM が別のグループからキーとポリシーを要求するのを防ぐには、キー サーバ認証が必要です。ISAKMP 認証では GM がキー サーバから GDOI 属性を要求できることが確認され、GDOI 認証では GM がキー サーバに設定された特定のグループから GDOI 属性を要求できることが確認されます。

GDOI 認証は、GM から送信された ISAKMP ID に基づきます。GM が ID として IP アドレスを送信すると、認証アドレスのみが認証に使用されます。GM が識別名（DN）またはホスト名を送信すると、認証 ID が使用されます。ID として IP アドレスを使用すると、DN またはホスト名と照合する認証がバイパスされます。逆も同様です。特定の DN の GM だけが接続できる（別の ID を使用する GM が接続できない）ようにするには、認証アドレスで **denyany** を指定する必要があります。

事前共有キーを使用する GM 認証

事前共有キーを使用するとき、GET VPN では IP アドレスを使用する GM 認証がサポートされます。GM の WAN アドレス（またはサブネット）を照合する ACL は、GET VPN グループ設定に定義し、適用することができます。ACL と一致する IP アドレスを持つ GM は認証が成功し、キー サーバに登録できます。GM IP アドレスが ACL と一致しない場合、キー サーバは GM の登録要求を拒否します。

認証失敗の場合、次の syslog メッセージが生成されます。

```
%GDOI-1-UNAUTHORIZED_IPADDR: Group getvpn received registration from
unauthorized ip address: 10.1.1.9
```

PKI を使用する GM 認証

PKI を使用する場合、GET VPN では一般的に使用される DN または完全修飾ドメイン名（FQDN）を使用する GM 認証がサポートされます。GM 認証をアクティブにするには、**authorizationidentity** コマンドを使用します。GM 証明書の特定のフィールド（通常、組織ユニット（OU））と一致する暗号 ID は、GET VPN グループ設定に定義し、適用することができます。暗号 ID を定義するには、**cryptoidentity** コマンドを使用します。

証明書クレデンシャルが ISAKMP ID と一致する GM は認証され、キー サーバに登録できます。たとえば、すべての GM 証明書に OU=GETVPN が発行される場合、すべての GM が OU=GETVPN を持つ証明書を提示することをチェック（認証）するようにキー サーバを設定できます。GM が提示する証明書の OU がそれ以外に設定されている場合、GM のキー サーバへの登録は認証されません。

認証が失敗した場合、次の syslog メッセージが生成されます。

```
%GDOI-1-UNAUTHORIZED_IDENTITY: Group getvpn received registration from
unauthorized identity: Dist.name: hostname=GroupMember-1, ou=TEST
```

Protocol Independent Multicast-Sparse Mode でのキー再生成機能

マルチキャスト キー再生成は、マルチキャストのすべてのモードで使用できます。継続するトラフィックが受信されないと PIM-SM Shortest Path Tree（SPT）が廃棄される可能性があるため、Protocol Independent Multicast-Sparse Mode（PIM-SM）を設定するときは必ず、**rekey retransmit** コマンドを使用する必要があります。トラフィックが再開すると、PIM-SM によって SPT が必ず確立されます。キー再生成パケットを再送信すると、PIM-SM による SPT の設定時にグループ メンバーによってキー再生成が受信される可能性が高くなります。

Fail-Close モード

グループ メンバーがキー サーバに登録されないと、そのグループ メンバーを通過するトラフィックが暗号化されません。この状態は「フェールオープン」と呼ばれます。グループ メンバーが登録される前に暗号化されていないトラフィックがそのグループ メンバーを通過することを防ぐには、Fail-Close 機能を設定します。この機能を設定すると、暗黙的な「permit ip any any」ポリシーがインストールされ、そのグループ メンバーを通過する暗号化されていないトラフィックはすべて廃棄されます（この状態を Fail-Close モードと呼びます）。

Fail-Close 機能は、インターフェイス ACL を設定することによっても実現可能です。ただし、Fail-Close 機能は、ACL リストよりも管理しやすく、実装も簡単です。

Fail-Close 機能を設定している場合でも、**match address** コマンド（**match address** {*access-list-number* | *access-list-name*}）を設定することによって、特定の暗号化されていないトラフィックがグループ メンバーを通過することを許可することが可能です。この明示的な「deny」ACL は、暗黙的な「permit ip any any」によって、拒否された（暗号化されていない）トラフィックがグループ メンバーの通過を許可される前に追加されます。

グループ メンバーの登録が正常終了したら、Fail-Close ポリシーが明示的であるか暗黙的であるかを問わず削除され、グループ メンバーの動作が、Fail-Close 機能が設定される以前のものと同じになります。

Fail-Close 機能の使用上の注意事項

Fail-Closeモードで作業するためにクリプトマップを設定する場合、注意しなければならないことがあります。Fail-Close ACLを正しく定義しないと、自分自身をロックアウトしてしまう可能性があります。たとえば、セキュア シェル（SSH）を使用して暗号マップが適用されたインターフェイス経由でルータにログインする場合、**denytcpanyeq***port***host***address* コマンド ラインを Fail-Close ACL 下に含める必要があります。キーサーバへのパスを検索する場合は、ルータが使用しているルーティング プロトコル（**denyospfanyany** など）も含める必要がある場合もあります。最初に Fail-Close とその ACL を設定し、次に **showcryptomapgdoifail-close***map-name* コマンドを使用して Fail-Close ACL を確認します。Fail-Close ACL を確認し、それが正しいと確信したら、**activate** コマンドを設定して、Fail-Close モードで暗号マップを動作させることができます。**activate** コマンドを設定しない限り、Fail-Close はアクティブになりません。

Fail-Close ACL はグループ メンバーの視点で設定します。Fail-Close ACL は、グループ メンバー上で次のように設定されます。

access-list125denyiphost*host1-ip-addrhost2-ip-addr*

Fail-Close モードでは、host1 から host2 へのすべての IP トラフィックが、Group Member 1 によって、暗号化されていないテキストで送信されます。さらに、着信ミラー トラフィック（つまり、host2 から host1 への IP トラフィック）も、GM1 によって暗号化されていないテキストで受信されます。

（注） deny エントリに一致するすべての IP トラフィックは、グループ メンバーによって、暗号化されていないテキストで送信されます。

着信トラフィックは、ミラー アクセス リストに対応付けられます。

Fail-Close アクセス リストは、グループ メンバー アクセス リストと同じルールに従います。詳細は、「グループ メンバー アクセス コントロール リスト」のセクションを参照してください。

GDOI 再登録を行うために **denyudpanyeq848anyeq848** コマンドを設定する必要はありません。コード自体によって、そのコードの設定対象となっているキー サーバからの、特定のグループ メンバーの GDOI パケットであるかどうかが判断されます。そのグループ メンバーの GDOI パケットだった場合、そのパケットは処理されます。ただし、キー サーバがグループ メンバー 1 の後になるシナリオでは、グループ メンバー 1 がキー サーバに正常に登録できない場合、グループ メンバー 1 に対して明示的に **denyudpanyeq848anyeq848** コマンド ラインが設定されていない限り、他のグループ メンバーも登録できなくなります。しかし、Fail-Close機能が正しく設定されている場合は、グループ メンバーがキーサーバへの登録に失敗しても、望まないトラフィックが「暗号化されずに」出ていくことがないようにすることができます。ただし、他のグループ メンバーからの登録パケットが、登録に失敗した場合でもグループ メンバー 1 経由でキー サーバに到達できる場合、指定されたトラフィックが暗号化されずに出ていくことを許可することができます。

Fail-Close モードの設定の詳細については、「Fail-Close モードのアクティブ化」セクションを参照してください。

Fail-Close モードがアクティブになっているか確認するには、**showcryptomapgdoifail-close** コマンドを使用します。

GDOI 登録成功を追跡する MIB オブジェクトの作成

ルーティング ブラックホールを回避するため、GET VPN のルーティング プレーンと暗号プレーンは同期する必要があります。GET VPN ルーティング ブラックホールは次の状況で発生します。

- アクティブな TEK がない KS に GM が登録できず、トラフィックを暗号化または復号化できない。
- GM TEK SA の期限が切れたがキー再生成または再登録によって KS から新しいキーを受け取っていない。
- GM は KS からキー再生成を受け取ったが、SA を暗号エンジンにインストールするときにエラーが発生する。

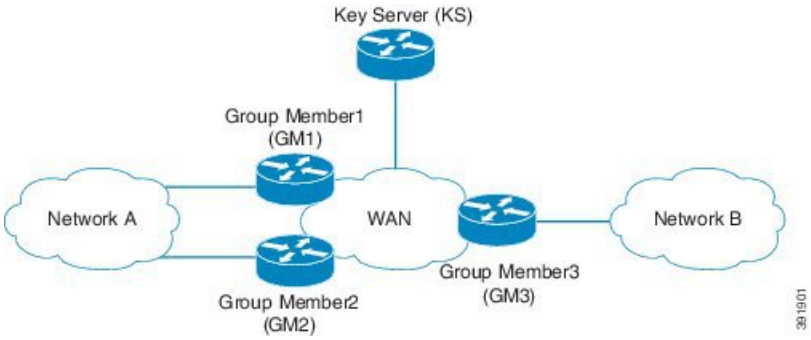
GDOI 登録成功を追跡する MIB オブジェクトの作成機能では、グループ内のアクティブな TEK 数を示すため、GDOI MIB に新しい MIB オブジェクトが導入されています。

BGP の GET VPN ルーティング認識

ルーティング ブラックホールを回避するため、GET VPN のルーティング プレーンと暗号プレーンは同期する必要があります。グループ メンバー（GM）がキー サーバ（KS）に正常に登録される場合、セキュリティ ポリシーまたはキーは GM にインストールされません。ただし、GM は他の GM に対して保護されたネットワークのルートをアドバタイズできます。

次の図は、ブラック ホールの生成について説明しています。

図 *12*：ルーティング ブラックホールの生成



1. グループ メンバー 1、グループ メンバー 2、グループ メンバー 3 が起動し、WAN とルーティング アジャセンシー関係を確立します。
2. グループ メンバー 1 およびグループ メンバー 2 は、ネットワーク A のプレフィックスを WAN にアドバタイズします。ネットワーク B からネットワーク A へのトラフィックの優先パスは、グループ メンバー 1 経由です。
3. グループ メンバー 3 はネットワーク B を WAN にアドバタイズします。トラフィック ネットワーク A からネットワーク B への優先パスは、グループ メンバー 1 経由です。

4. KS は、ネットワーク A とネットワーク B の間のすべてのトラフィックを保護するためのセキュリティを定義します。
5. グループ メンバー 1 とグループ メンバー 3（およびグループ メンバー 2）は正常に KS からセキュリティ キーを取得し、ネットワーク A とネットワーク B 間のすべてのトラフィックを保護します。
6. グループ メンバー 2 およびグループ メンバー 3 が正常にキーを取得する一方、グループ メンバー 1 は更新されたキーまたはポリシーの受信に失敗し、KS への再登録に失敗します。
7. ルーティング プロトコルは、ネットワーク A とネットワーク B 間のすべてのトラフィックに対してグループ メンバー 1 経由のパスを優先し続けます。
8. グループ メンバー 1 は、ポリシーまたはキーが無効なため、ネットワーク A とネットワーク B の間に流れるトラフィックすべてをドロップします。

ネットワーク B のホストがネットワーク A のホストにトラフィックを送信する際、トラフィックはグループ メンバー 3 によって暗号化され、グループ メンバー 1 経由（優先パス）でネットワーク A に送信されます。ただし、グループ メンバー 1 はトラフィックを復号するためのポリシーまたは現在のキーを持たないため、パケットをドロップします。その結果、トラフィックはドロップされ、ブラック ホールが生成されます。同様に、ネットワーク A のホストがネットワーク B のホストにトラフィックを送信する際、トラフィックはグループ メンバー 1（優先パス）に転送され、グループ メンバー 1 にポリシーまたは現在のキーがないためにドロップされます。グループ メンバー 1 にポリシーまたはキーがない場合、適切な動作としてトラフィックはグループ メンバー 2 経由で転送および再ルーティングされます。

BGP の GET VPN ルーティング認識機能では、GETVPN GM の暗号化状態を追跡し、追跡情報を適用して GM で双方向条件付きルート フィルタリングを実行することにより、ルーティング ブラック ホールを防ぎます。

GM ステータスの追跡のための GDOI MIB

新しい GDOI MIB では、トラフィックの暗号化または復号に関する GM のステータスを表示します。GM がトラフィックを暗号化して復号できる場合はこの MIB が *true* に設定され、復号できず、次のことが発生する場合は、GM が false に設定されます。

- GM が KS に正常に登録されない。
- GM TEK キーの有効期限が切れ、正しいキー再生成または再登録がない。
- キー再生成セキュリティ アソシエーション（SA）のインストールと HW 暗号エンジンのエラー。

スタブオブジェクトを作成し、このオブジェクトにトラッキング ID を割り当てて GDOI MIB をモニタすることにより、拡張オブジェクト トラッキング（EOT）を設定する必要があります。次に、トラッキング ID 99 をスタブオブジェクトに割り当てる設定例を示します。

```
event manager applet test1
 event snmp oid <new GDOI MIB object> .....
 action 2.0 track set 99 state up

track 99 stub-object
 delay up 60
```

GM の設定時に GM 暗号化の状態を追跡するには、**client status** コマンドを実行します。コマンドでは、スタブオブジェクトに割り当てられたトラッキング ID を指定する必要があります。

双方向条件付きルート フィルタリング

双方向条件付きルート フィルタリングでは、BGP、OSPF、EIGRP、RIPv2 などのさまざまなルーティング プロトコルをサポートしています。EOT は GET VPN GM 暗号化状態を追跡し、EOT 値に基づいて条件により特定のルートマップエントリを有効または無効にします。次に、GET VPN GM 暗号化状態をモニタする設定例を示します。

```
route-map bgp-policy-out permit 10
 match ip address register-int-Only
route-map bgp-policy-out permit 20
 match track 99
 match ip address orig_route_map_acl_out
route-map bgp-policy-out deny 30

route-map bgp-policy-in permit 10
 match ip address noc
route-map bgp-policy-in permit 20
 match track 99
 match ip address orig_route_map_acl_in
route-map bgp-policy-in deny 30

ip access-list standard noc
 permit 1.1.1.0                                    <---- NOC subnet with Keyserver (KS)
ip access-list standard register-int-Only
 permit 2.2.2.2                                    <---- registration interface ip of the
GM itself
ip access-list standard orig_route_map_acl_in       <---- original inbound route-map ACL
 permit a.b.c.d
 permit .......
ip access-list standard orig_route_map_acl_out      <---- original outbound route-map ACL
 permit e.f.g.h
 permit .......

router bgp 64600
 no synchronization
 bgp router-id xxxxxxxx
 bgp log-neighbor-changes
 network xxxxxxxxxx mask 255.255.255.255
 network xxxxxxxxxx mask 255.255.255.252
 neighbor xxxxxxxxxx remote-as 65000
 neighbor xxxxxxxxxx description PE
 neighbor xxxxxxxxxx route-map bgp-policy-in in
 neighbor xxxxxxxxxx route-map bgp-policy-out out
```

上記の例では、GET VPN GM 暗号化状態をモニタするために **match track 99** コマンドが指定されています。 GM が適切に機能する場合、**match track 99** コマンドは値 *true* を返し、GM は次のルートをアドバタイズまたは受信します。

- 発信：GM 登録インターフェイスに到達するルート、および着信ルートマップのアクセスコントロール リスト（ACL）「orig_route_map_acl_out」によって許可されたルート。
- 着信：NOC に到達するルート、およびルーティングは、ピアから受信した発信ルート マップ ACL「orig_route_map_acl_in」によって許可されたルート。

一方、GM が正しく機能しない場合、**match track 99** コマンドは値 *false* を返し、GM は次のルートのみをアドバタイズまたは受信します。

- 発信：GM 登録インターフェイスに到達するルート。
- 着信：NOC サブネットに到達するルート。

Cisco Group Encrypted Transport VPN システム ロギング メッセージ

次の表に、GET VPN システム ロギング（syslog とも呼ばれます）メッセージと説明を示します。

表 *3*：***GET VPN*** システム ロギング メッセージ

メッセージ	説明
COOP_CONFIG_MISMATCH	プライマリ KS とセカンダリ KS 間の設定が一致しません。
COOP_KS_ADD	グループ内の連携 KS のリストに KS が追加されました。
COOP_KS_ELECTION	ローカル KS によってグループ内の選択プロセスが開始されました。
COOP_KS_REACH	設定済み連携 KS 間の到達可能性は回復しています。
COOP_KS_REMOVE	グループ内の連携 KS のリストから KS が削除されました。
COOP_KS_TRANS_TO_PRI	ローカル KS が、グループ内のセカンダリ サーバからプライマリ ロールに移行しました。
COOP_KS_UNAUTH	認証されたリモートサーバによって、グループ内のローカル KS へのアクセスが試行されました。敵対的なイベントの可能性があります。
COOP_KS_UNREACH	設定済み連携 KS 間の到達可能性が失われています。敵対的なイベントの可能性があります。
COOP_KS_VER_MISMATCH	各 KS が、異なるバージョンの Cisco IOS コードを実行しています。
COOP_PACKET_DROPPED	ドライバ バッファ サイズに設定されたハード制限によって、このサイズ以上のパケットの送信はできません。
GDOI-3-GDOI_REKEY_SEQ_FAILURE	シーケンス番号のアンチ リプレイ チェックが失敗したため、キー再生成メッセージが拒否されています。

メッセージ	説明
GDOI-3-GM_NO_CRYPTO_ENGINE	リソースが不足しているかサポートされていない機能が要求されたために暗号化エンジンが検出できません。
GDOI-3-PSEUDO_TIME_LARGE	キー再生成に、計算された許容される疑似時間の差を超える大きな疑似時間があります。
GDOI-3-PSEUDO_TIME_TOO_OLD	キー再生成に、計算された許容される疑似時間の差を超える小さな疑似時間があります。
GDOI-4-GDOI_ANN_TIMESTAMP_ LARGE	セカンダリ KS が、プライマリ KS から計算された許容される疑似時間の差を超える大きな疑似時間がある ANN を受信しています。
GDOI-4-GDOI_ANN_TIMESTAMP_ TOO_OLD	セカンダリ KS が、プライマリ KS から計算された許容される疑似時間の差を超える小さな疑似時間がある ANN を受信しています。
GDOI-5-COOP_KS_BLOCK_NEW_GM_REGISTER	セカンダリ KS がプライマリ KS から有効な疑似時間を受信していないため、GM のグループへの登録を一時的にブロックしています。
GDOI-5-COOP_KS_VALID_ANN_ TIMER_EXPIRED	セカンダリ KS が 3 つの再送信後に無効な疑似時間のある ANN を受信し続けています。セカンダリ KS は有効な ANN が受信されるまで一時的に新しいグループ メンバー登録をブロックします。
GDOI_ACL_NUM	ACL のエントリが多すぎます。GDOI は、指定された最初の 100 個の ACL エントリだけを受け入れます。
GDOI_REKEY_FAILURE	GDOI キー再生成中に、KS からのペイロード構文解析が、この GM 上で失敗しました。
GM_ACL_MERGE	GM と KS 間における ACL の違いは解決され、結合が実行されました。
GM_ACL_PERMIT	GM は「拒否」の ACL のみをサポートできます。「許可」エントリと一致するすべてのトラフィックがドロップされます。
GM_CLEAR_REGISTER	ローカル GM によって、**clearcryptogdoi** コマンドが実行されました。

メッセージ	説明
GM_CM_ATTACH	このローカルGM用の暗号マップが追加されました。
GM_CM_DETACH	このローカルGM用の暗号マップが削除されました。
GM_CONV_SA_DUPLEX	IPsec SA が、GM 上のグループ内で双方向モードに変換されました。
GM_CONV_SA_DUPLEX_LOCAL	CLI コマンドによって、GM上のグループ内で、IPsec SA が双方向モードに変換されました。
GM_DELETE	グループ内の GM が KS から削除されました。
GM_ENABLE_GDOI_CM	GMに、KSを持つグループ内のGDOI暗号マップ上のイネーブルにされた ACL があります。
GM_HASH_FAIL	GDOI 登録プロトコル中に KS によって送信されたメッセージに不具合があるか、ハッシュがありません。
GM_INCOMPLETE_CFG	GDOI グループ設定で、グループ ID、サーバ ID、またはその両方が見つからないために、登録が完了できません。
GM_NO_IPSEC_FLOWS	IPsec フロー 制限に関するハードウェアの制限に達しました。IPsec SA をこれ以上作成できません。
GM_RE_REGISTER	あるグループのために作成された IPsec SA が期限切れか、消去された可能性があります。KS に再登録する必要があります。
GM_RECV_DELETE	GM を削除するために KS によって送信されたメッセージを受信しました。
GM_RECV_REKEY	キー再生成を受信しました。
GM_REGS_COMPL	Registration complete.
GM_REJECTING_SA_PAYLOAD	GDOI登録プロトコル中に、KSによって送信された提案が、ローカルGMによって拒否されました。

メッセージ	説明
GM_REKEY_NOT_RECD	GM によって、グループ内の KS からのキー再生成メッセージが受信されませんでした。現在実装されていません。
GM_REKEY_TRANS_2_MULTI	GM が、ユニキャストキー再生成メカニズムの使用から、マルチキャストメカニズムの使用へと移行しました。
GM_REKEY_TRANS_2_UNI	GM が、マルチキャストキー再生成メカニズムの使用から、ユニキャストメカニズムの使用へと移行しました。
GM_SA_INGRESS	グループ内の KS からの受信専用 ACL が、GM によって受信されました。
GM_UNREGISTER	GM がグループから去りました。
KS_BAD_ID	GDOI 登録プロトコル中に、ローカル KS と GM との間で設定の不一致が発生しました。
KS_BLACKHOLE_ACK	KS が、GM からのメッセージに対してブラックホール化の状態になりました。敵対的なイベントの可能性があります。
KS_CLEAR_REGISTER	ローカル KS によって、**clearcryptogdoi** コマンドが実行されました。
KS_CONV_SAS_DUPLEX	IPsec SA が、グループ内で双方向モードに変換されました。
KS_CONV_SAS_INGRESS	IPsec SA が、グループ内で受信専用モードに変換されました。
KS_FIRST_GM, GDOI, LOG_INFO	ローカル KS がグループに参加している最初の GM を受信しました。
KS_GM_REJECTS_SA_PAYLOAD	GDOI 登録プロトコル中に、KS によって送信された提案が、GM によって拒否されました。
KS_GM_REVOKED	キー再生成プロトコル中に、認証されていないメンバーによるグループへの加入が試行されました。敵対的なイベントの可能性があります。

メッセージ	説明
KS_GROUP_ADD	コンフィギュレーション コマンドが実行され、グループ内に KS が追加されました。
KS_GROUP_DELETE	コンフィギュレーション コマンドが実行され、グループから KS が削除されました。
KS_HASH_FAIL	GDOI 登録プロトコル中に GM によって送信されたメッセージに不具合があるか、ハッシュがありません。
KS_LAST_GM	最後の GM がローカル KS でグループを去りました。
KS_NACK_GM_EJECT	KS が、GM からの ACK メッセージを受信しない状態になり、イジェクトされました。
KS_NO_RSA_KEYS	RSA キーが作成されなかったか、失われています。
KS_REGS_COMPL	KS による、グループ内における登録が正常終了しました。
KS_REKEY_TRANS_2_MULTI	グループが、ユニキャスト キー再生成メカニズムの使用から、マルチキャスト メカニズムへと移行しました。
KS_REKEY_TRANS_2_UNI	グループが、マルチキャスト キー再生成メカニズムの使用から、ユニキャスト メカニズムの使用へと移行しました。
KS_SEND_MCAST_REKEY	マルチキャスト キー再生成を送信中です。
KS_SEND_UNICAST_REKEY	ユニキャスト キー再生成を送信中です。
KS_UNAUTHORIZED	GDOI 登録プロトコル中に、認証されていないメンバーによるグループへの加入が試行されました。敵対的なイベントの可能性があります。
KS_UNSOL_ACK	KS によって、過去の GM からの非送信請求 ACK メッセージが受信されたか、DoS 攻撃を受けています。敵対的なイベントの可能性があります。

メッセージ	説明
PSEUDO_TIME_LARGE	GM によって、その GM の疑似時間とは大きく異なる値を持つ疑似時間が受信されました。
REPLAY_FAILED	GM または KS のアンチ リプレイ チェックが失敗しました。
UNAUTHORIZED_IDENTITY	登録要求が、要求を行っているデバイスがグループの参加を許可されなかったために廃棄されました。
UNAUTHORIZED_IPADDR	登録要求が、要求を行っているデバイスがグループの参加を許可されなかったために廃棄されました。
UNEXPECTED_SIGKEY	予期しないシグニチャ キーが検出されました。このシグニチャ キーを解除します。
UNREGISTERED_INTERFACE	未登録のインターフェイスからの登録を受信中です。処理を停止してください。
UNSUPPORTED_TEK_PROTO	予期しない TEK プロトコルです。

Cisco Group Encrypted Transport VPN の設定方法

キー サーバの設定

前提条件

GDOI グループを作成する前に、最初に IKE および IPsec トランスフォーム セットを設定してから、IPsec プロファイルを作成する必要があります。IKE と IPsec トランスフォーム セットの設定方法、および IPsec プロファイルの作成方法については、「その他の関連資料」セクションの「関連資料」の項を参照してください。

キー再生成メッセージに署名するための RSA キーの設定

（注） セキュリティに対する脅威とそれに対抗するための暗号化技術は絶えず変化しています。暗号化に関するシスコの最新の推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

キー再生成メッセージに署名するために使用される RSA キーを設定するには、次の手順を実行します。キー再生成が使用中でない場合、このサブ作業はスキップしてください。

手順の概要

1. **enable**
2. **configureterminal**
3. **cryptokeygeneratersageneral-keyslabel***name-of-key*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cryptokeygeneratersageneral-keyslabel***name-of-key* 例： `Router(config)# crypto key generate rsa general-keys label mykeys`	キー再生成メッセージに署名するために使用される RSA キーを生成します。生成されるキーの長さ（ビット単位）を確認するプロンプトが表示されます。2048 未満の長さを指定することは推奨されません。

次の作業

グループ ID、サーバ タイプ、および SA タイプを設定します（「グループ ID、サーバ タイプ、および SA タイプの設定」セクションを参照してください）。

グループ ID、サーバ タイプ、および SA タイプの設定

サイトが大量にある場合、特にあるサイトがDual Multipoint VPN（DMVPN）のような他の暗号化ソリューションから移行する場合は、予防措置を取り、段階的に機能を追加する必要があります。たとえば、すべてのCPEデバイスを、トラフィックが双方向で暗号化されるように設定するのではなく、1つまたは少数のグループだけが暗号化されたトラフィックの送信を許可されるように、一方向の暗号化を設定することが可能です。その他のデバイスは暗号化されたトラフィックだけを受信することが許可されます。1 つまたは少数のメンバーに関する一方向の暗号化の検証が終わったら、すべてのメンバーに対して双方向の暗号化をオンにできます。この「着信専用」トラフィックは、暗号グループ下で **sareceiveonly** コマンドを使用して制御可能です。

グループ ID、サーバ タイプ、および SA タイプを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **cryptogdoigroup***group-name*
4. 次のいずれかのコマンドを入力します。
   - **identitynumber***number*
   - **identityaddressipv4***address*
5. **serverlocal**
6. **sareceive-only**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cryptogdoigroup***group-name* 例： `Router(config)# crypto gdoi group gdoigroupname`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 4	次のいずれかのコマンドを入力します。
	• **identitynumber***number*
	• **identityaddressipv4***address*
	
	例：
	`Router(config-gdoi-group)# identity number 3333`
	
	例：
	`Router(config-gdoi-group)# identity address ipv4 209.165.200.225`
		GDOI グループ番号またはアドレスを指定します。

ステップ 5	**serverlocal** 例： `Router(config-gdoi-group)# server local`	デバイスを GDOI キー サーバとして指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 6	**sareceive-only** 例： `Router(config-local-server)# sa receive-only`	IPsec SA がグループ メンバーによって「着信専用」としてインストールされるように指定します。

次の作業

グループ メンバーが双方向の受信および送信モードで動作するように、キーサーバ上の受信専用設定を削除します。

キー再生成の設定

ここでは、次のオプションの作業について説明します。

キー再生成は、グループのポリシーと IPsec SA を定期的に更新するために、キー サーバによってコントロールプレーンで使用されます。グループ メンバー側では、他の何らかの理由によりタイマーが満了するときに完全に登録するのではないので、キー再生成への登録の更新がより効率的になります。最初の登録は常にユニキャスト登録です。

キーサーバは、ユニキャストまたはマルチキャストモードでキー再生成を送信するように設定できます。キー再生成の転送モードは、キーサーバによってIPマルチキャストが使用されてキー再生成が配信できるかどうかによって決まります。マルチキャスト機能がカスタマーのネットワー

ク内に存在しない場合、キーサーバを、ユニキャストメッセージを使用してキー再生成を送信するように設定する必要があります。

キー再生成の追加オプションでは、**rekeyauthentication**、**rekeyretransmit**、および **rekeyaddressipv4** コマンドを使用します。ユニキャスト転送モードが設定されている場合、このユニキャスト キー再生成メッセージの送信元アドレスが指定されるように **sourceaddress** コマンドを指定する必要があります。

マルチキャストは、キー再生成メッセージのデフォルトの転送タイプです。次の箇条書きでは、キー再生成転送タイプにどのような場合にマルチキャストにするか、あるいはユニキャストにするかを説明します。

- グループ内のすべてのメンバーがマルチキャストに対応している場合は、**rekeytransportunicast** コマンドを設定しません。マルチキャスト キー再生成はデフォルトでオンになっているので、このグループ下でキー再生成転送タイプ「ユニキャスト」が過去に設定されていない場合、**norekeytransportunicast** コマンドは必要ありません。
- グループ内のすべてのメンバーがユニキャストである場合、**rekeytransportunicast** コマンドを使用します。
- グループ内に混合されたメンバーがある場合（つまり、大多数がマルチキャストで、少数がユニキャスト）、**rekeytransportunicast** コマンドは設定しません。キー再生成は、グループ メンバーの大多数に対して、マルチキャストで配信されます。マルチキャスト メッセージを受信しない残りのグループ メンバー（ユニキャスト グループ メンバー）は、そのポリシーが期限切れになった時にキー サーバに再登録する必要があります。混合モード（つまり、ユニキャストとマルチキャスト キー再生成モード）は現在サポートされていません。

norekeytransportunicast コマンドが使用されている場合、マルチキャスト キー再生成メッセージを受信できない GDOI グループ内のメンバーを、最新のグループ ポリシーを取得するようにキー サーバに登録する必要があります。再登録すると、デフォルトの転送タイプが強制的にマルチキャストになります。過去に転送タイプが設定されていない場合、マルチキャスト転送タイプがデフォルトで適用されます。

前提条件

rekey authentication コマンドを設定する前に、**crypto key generate rsa** コマンドおよび **general-keys** キーワードと **label** キーワードを使用して RSA キーが生成されるようにルータを設定しておく必要があります（例：「crypto key generate rsa general-key label my keys」）。

ユニキャスト キー再生成の設定

次の設定作業表では、アドレス「ipv4 10.0.5.2」は、ユニキャストまたはマルチキャスト キー再生成メッセージを送信するキー サーバ上のインターフェイスを示しています。このアドレスは、ユニキャスト キー再生成では必須ですが、マルチキャスト キー再生成では任意です。マルチキャスト キー再生成の場合、キー サーバの送信元アドレスを、キー再生成 ACL から取得できます。

ユニキャスト キー再生成を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **cryptogdoigroup***group-name*
4. 次のいずれかのコマンドを入力します。
   - **identitynumber***number*
   - **identityaddressipv4***address*
5. **serverlocal**
6. **rekeytransportunicast**
7. **rekeylifetimeseconds***number-of-seconds*
8. **rekeyretransmit***number-of-seconds***number***number-of-retransmissions*
9. **rekeyauthenticationmypubkeyrsa***key-name*
10. **addressipv4***ipv4-address*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cryptogdoigroup***group-name* 例： `Router(config)# crypto gdoi group gdoigroupname`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。
ステップ 4	次のいずれかのコマンドを入力します。 • **identitynumber***number* • **identityaddressipv4***address*	GDOI グループ番号またはアドレスを指定します。

	コマンドまたはアクション	目的

	例：
	`Router(config-gdoi-group)# identity number 3333`
	例：
	`Router(config-gdoi-group)# identity address ipv4 209.165.200.225`	

ステップ 5	**serverlocal** 例： `Router(config-gdoi-group)# server local`	デバイスを GDOI キー サーバとして指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 6	**rekeytransportunicast** 例： `Router(config-local-server)# rekey transport unicast`	グループ メンバーに対するキー再生成メッセージのユニキャスト配信を設定します。
ステップ 7	**rekeylifetimeseconds***number-of-seconds* 例： `Router(gdoi-local-server)# rekey lifetime seconds 300`	（任意）任意の暗号キーが使用される秒数を制限します。 • このコマンドが設定されていない場合、デフォルト値の 86,400 秒が有効になります。
ステップ 8	**rekeyretransmit***number-of-seconds***number***number-of-retransmissions* 例： `Router(gdoi-local-server)# rekey retransmit 10 number 3`	（任意）キー再生成メッセージが再送信される回数を指定します。 • このコマンドが設定されていない場合、再送信は行われません。
ステップ 9	**rekeyauthenticationmypubkeyrsa***key-name* 例： `Router(gdoi-local-server)# rekey authentication mypubkey rsa mykeys`	（任意）GDOI グループ メンバーに対するキー再生成に使用されるキーを指定します。 • キー再生成が不要な場合、このコマンドは任意です。キー再生成が必須の場合、このコマンドは必須です。

	コマンドまたはアクション	目的
ステップ 10	**addressipv4***ipv4-address* 例： `Router(gdoi-local-server)# address ipv4 209.165.200.225`	（任意）ユニキャスト キー再生成メッセージの送信元情報を指定します。 • キー再生成が不要な場合、このコマンドは任意です。キー再生成が必須の場合、このコマンドは必須です。

マルチキャスト キー再生成の設定

マルチキャスト キー再生成を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **cryptogdoigroup***group-name*
4. 次のいずれかのコマンドを入力します。
   - **identitynumber***number*
   - **identityaddressipv4***address*
5. **serverlocal**
6. **rekeyaddressipv4** {*access-list-name* | *access-list-number*}
7. **rekeylifetimeseconds***number-of-seconds*
8. **rekeyretransmit***number-of-seconds***number***number-of-retransmissions*
9. **rekeyauthentication** {**mypubkey** | **pubkey**} **rsa***key-name*
10. **exit**
11. **exit**
12. **access-list***access-list-number* {**deny** | **permit**} **udphost***source* [*operator*[*port*]] **host***source* [*operator*[*port*]]
13. **interface***typeslot/ port*
14. **ip igmp join-group** *group-address* [**source***source-address*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cryptogdoigroup***group-name* 例： `Router(config)# crypto gdoi group gdoigroupname`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。

ステップ 4	次のいずれかのコマンドを入力します。
	• **identitynumber***number*
	• **identityaddressipv4***address*
	
	例：
	`Router(config-gdoi-group)# identity number 3333`
	
	例：
	`Router(config-gdoi-group)# identity address ipv4 209.165.200.225`
		GDOI グループ番号またはアドレスを指定します。

ステップ 5	**serverlocal** 例： `Router(config-gdoi-group)# server local`	デバイスを GDOI キー サーバとして指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 6	**rekeyaddressipv4** {*access-list-name* | *access-list-number*} 例： `Router(gdoi-local-server)# rekey address ipv4 121`	登録するマルチキャスト サブアドレス範囲グループ メンバーを定義します。

	コマンドまたはアクション	目的
ステップ 7	**rekeylifetimeseconds***number-of-seconds* 例： `Router(gdoi-local-server)# rekey lifetime seconds 300`	（任意）任意の暗号キーが使用される秒数を制限します。 • このコマンドが設定されていない場合、デフォルト値の 86,400 秒が有効になります。
ステップ 8	**rekeyretransmit***number-of-seconds***number***number-of-retransmissions* 例： `Router(gdoi-local-server)# rekey retransmit 10 number 3`	（任意）キー再生成メッセージが再送信される回数を指定します。 • このコマンドが設定されていない場合、再送信は行われません。
ステップ 9	**rekeyauthentication** {**mypubkey** | **pubkey**} **rsa***key-name* 例： `Router(gdoi-local-server)# rekey authentication mypubkey rsa mykeys`	（任意）GDOI グループ メンバーに対するキー再生成に使用されるキーを指定します。 • キー再生成が不要な場合、このコマンドは任意です。キー再生成が必須の場合、このコマンドは必須です。
ステップ 10	**exit** 例： `Router(gdoi-local-server)# exit`	GDOI サーバ ローカル コンフィギュレーション モードを終了します。
ステップ 11	**exit** 例： `Router(config-gdoi-group)# exit`	GDOI グループ コンフィギュレーション モードを終了します。
ステップ 12	**access-list***access-list-number* {**deny** | **permit**} **udphost***source* [*operator*[*port*]] **host***source* [*operator*[*port*]] 例： `Router(config)# access-list 121 permit udp host 10.0.5.2 eq 848 host 239.0.1.2 eq 848`	拡張 IP アクセス リストを定義します。
ステップ 13	**interface***typeslot*/ *port* 例： `Router(config)# interface gigabitethernet 0/0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 14	**ip igmp join-group** *group-address* [**source***source-address*] 例： `Router(config-if)# ip igmp join-group 232.2.2.2 source 10.1.1.1`	指定したグループまたはチャネルに参加するようにルータのインターフェイスを設定します。 （注） 暗号マップが設定されているものと同じインターフェイスでキー サーバに到達できない場合に手動でストリームに参加するには、このコマンドを使用します。

グループ メンバー ACL の設定

deny エントリに一致するすべての IP トラフィックは、グループ メンバーによって、暗号化されていないテキストで送信されます。着信トラフィックは、ミラーアクセスリストに対応付けられます。

（注） グループ メンバー ACL にエントリを追加または削除するために推奨の方法として、最初に既存のグループ メンバー ACL のコピーを異なる名前で作成してから、この新しい ACL のエントリに追加または削除します。その後 GDOI 暗号マップ下の既存のグループ メンバー ACL を新しく作成したグループ メンバー ACL で置き換える必要があります。

グループ メンバー ACL を設定するには、このタスクを実行します（グループ メンバーのアクセス リストに拒否ステートメントが含まれている場合があることに注意してください）。

手順の概要

1. **enable**
2. **configureterminal**
3. **access-list***access-list-number***denyiphost***source***host***source*
4. **access-list***access-list-number***permitip***source*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**access-list***access-list-number***denyiphost***source***host***source* 例： `Router(config)# access-list 101 deny ip host 10.0.0.1 host 10.0.0.2`	拒否される IP アクセス リストを定義します。
ステップ 4	**access-list***access-list-number***permitip***source* 例： `Router(config)# access-list 103 permit ip 209.165.200.225 0.255.255.255 10.20.0.0 0.255.255.255`	許可される IP アクセス リストを定義します。

次の作業

手順 4 で定義したアクセス リストは、SA の設定に使用する必要があるものと同じです。「IPsec SA の設定」のセクションを参照してください。

IPsec ライフタイム タイマーの設定

プロファイルの IPsec ライフタイム タイマーを設定するには、次の手順を実行します。この設定作業を実行しない場合、デフォルトは最大 IPsec SA ライフタイムの 3600 秒になります。TEK ライフタイム値は 900 秒を超える値にする必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **cryptoipsecprofile***name*
4. **setsecurity-associationlifetimeseconds***seconds*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cryptoipsecprofile***name* 例： `Router(config)# crypto ipsec profile profile1`	2 つの IPsec ルータ間における IPsec 暗号化で使用される IPsec パラメータを定義し、暗号化 IPsec プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**setsecurity-associationlifetimeseconds***seconds* 例： `Router(ipsec-profile)# set security-association lifetime seconds 2700`	IPsec SA をネゴシエーションするときに使用されるグローバル ライフタイム値を上書きします（特定のクリプト マップ エントリの場合）。

次の作業

IPsec SA を設定します。「IPsec SA の設定」のセクションを参照してください。

ISAKMP ライフタイム タイマーの設定

ISAKMP ライフタイム タイマーを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **cryptoisakmppolicy***priority*
4. **lifetime***seconds*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cryptoisakmppolicy***priority* 例： `Router(config)# crypto isakmp policy 1`	IKE ポリシーを定義し、ISAKMP ポリシー コンフィギュレーション モードを開始します。
ステップ 4	**lifetime***seconds* 例： `Router(config-isakmp-policy)# lifetime 86400`	IKE SA のライフタイムを指定します。

IPsec SA の設定

時間ベースのアンチリプレイがキーサーバ上で設定されているが、それに対応する機能がグループ メンバーにない場合、GDOI-3-GM_NO_CRYPTO_ENGINE syslog メッセージがグループ メンバーに記録されます。システム エラー メッセージの一覧については、「Cisco Group Encrypted Transport VPN システム ロギング メッセージ」セクションを参照してください。

（注） セキュリティに対する脅威とそれに対抗するための暗号化技術は絶えず変化しています。暗号化に関するシスコの最新の推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

IPsec SA を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **cryptoipsectransform-set***transform-set-nametransform*[*transform2...transform4*]
4. **cryptoipsecprofile***ipsec-profile-name*
5. **settransform-set***transform-set-name*
6. **exit**
7. **cryptogdoigroup***group-name*
8. 次のいずれかのコマンドを入力します。
   - **identitynumber***number*
   - **identityaddressipv4***address*
9. **serverlocal**
10. **saipsec***sequence-number*
11. **profile***ipsec-profile-name*
12. **matchaddressipv4** {*access-list-number* | *access-list-name*}
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権EXECモードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**cryptoipsectransform-set***transform-set-nametransform*[*transform2...transform4*] 例： `Router(config)# crypto ipsec transform-set gdoi-trans esp-aes esp-sha-hmac`	トランスフォーム セット（セキュリティプロトコルとセキュリティアルゴリズムの受け入れ可能な組み合わせ）を定義します。
ステップ 4	**cryptoipsecprofile***ipsec-profile-name* 例： `Router(config)# crypto ipsec profile profile1`	IPsec プロファイルを定義し、暗号 ipsec プロファイル コンフィギュレーションモードを開始します。
ステップ 5	**settransform-set***transform-set-name* 例： `Router(ipsec-profile)# set transform-set transformset1`	クリプト マップ エントリで使用可能なトランスフォームセットを指定します。
ステップ 6	**exit** 例： `Router(ipsec-profile)# exit`	IPSec プロファイル コンフィギュレーションモードを終了します。
ステップ 7	**cryptogdoigroup***group-name* 例： `Router(config)# crypto gdoi group gdoigroupname`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。

ステップ 8	次のいずれかのコマンドを入力します。
	• **identitynumber***number*
	• **identityaddressipv4***address*
	
	例：
	`Router(config-gdoi-group)# identity number 3333`
	
	例：
	`Router(config-gdoi-group)# identity address ipv4 209.165.200.225`
		GDOI グループ番号またはアドレスを指定します。

ステップ 9	**serverlocal** 例： `Router(config-gdoi-group)# server local`	デバイスを GDOI キー サーバとして指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 10	**saipsec***sequence-number* 例： `Router(gdoi-local-server)# sa ipsec 1`	GDOI グループに使用される IPsec SA ポリシー情報を指定し、GDOI SA IPsec コンフィギュレーションモードを開始する。
ステップ 11	**profile***ipsec-profile-name* 例： `Router(gdoi-sa-ipsec)# profile gdoi-p`	GDOI グループ用の IPsec SA ポリシーを定義します。
ステップ 12	**matchaddressipv4** {*access-list-number* | *access-list-name*} 例： `Router(gdoi-sa-ipsec)# match address ipv4 102`	GDOI 登録の IP 拡張アクセスリストを指定します。
ステップ 13	**end** 例： `Router(gdoi-sa-ipsec)# end`	GDOI SA IPsec コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

次の作業

リプレイを設定する必要があります。リプレイを設定しない場合、デフォルトはカウンタ モードになります。

GDOI グループ用の時間ベースのアンチリプレイの設定

GDOI グループ用の時間ベースのアンチ リプレイを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **cryptogdoigroup***group-name*
4. **identitynumber***policy-name*
5. **serverlocal**
6. **address***ip-address*
7. **saipsec***sequence-number*
8. **profile***ipsec-profile-name*
9. **matchaddress** {**ipv4** *access-list-number* | *access-list-name*}
10. **replaycounterwindow-size***seconds*
11. **replaytimewindow-size***seconds*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cryptogdoigroup***group-name* 例： `Router(config)# crypto gdoi group gdoigroup1`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。
ステップ 4	**identitynumber***policy-name* 例： `Router(config-gdoi-group)# identity number 1234`	GDOI グループ番号を指定します。
ステップ 5	**serverlocal** 例： `Router(config-gdoi-group)# server local`	デバイスを GDOI キー サーバとして指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 6	**address***ip-address* 例： `Router(config-server-local)# address 209.165.200.225`	送信元アドレスを設定します。このアドレスは、ローカル キー サーバによって送信されるパケットの送信元として使用されます。
ステップ 7	**saipsec***sequence-number* 例： `Router(config-server-local)# sa ipsec 1`	IPsec SA を指定し、GDOI SA IPsec コンフィギュレーション モードを開始します。
ステップ 8	**profile***ipsec-profile-name* 例： `Router(gdoi-sa-ipsec)# profile test1`	GDOI グループ用の IPsec SA ポリシーを定義します。
ステップ 9	**matchaddress** {**ipv4** *access-list-number* | *access-list-name*} 例： `Router(gdoi-sa-ipsec)# match address ipv4 101`	GDOI 登録の IP 拡張アクセス リストを指定します。
ステップ 10	**replaycounterwindow-size***seconds* 例： `Router(gdoi-sa-ipsec)# replay counter window-size 512`	1 つのグループ内に 2 つのグループ メンバーだけが存在している場合、GDOI を使用して、アクセス リスト内に定義されたトラフィックのカウンタ ベースのアンチ リプレイ保護をオンにします。 （注） このコマンドによる動作と **replay time window-size** コマンドによる動作は、相互に排他的な関係にあります。設定できるのはどちらか一方だけです。
ステップ 11	**replaytimewindow-size***seconds* 例： `Router(gdoi-sa-ipsec)# replay time window-size 1`	1 つのグループ内に 3 つ以上のグループ メンバーが存在している場合、GDOI を使用して、アンチ リプレイ保護のウィンドウ サイズを設定します。 （注） このコマンドによる動作と **replay counter window-size** コマンドによる動作は、相互に排他的な関係にあります。設定できるのはどちらか一方だけです。

パッシブ SA の設定

（グループ メンバーを passive モードにするために）パッシブ SA を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **cryptogdoigroup***group-name*
4. **identity***name*
5. **passive**
6. **serveraddressipv4**{*address* | *hostname*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cryptogdoigroup***group-name* 例： `Router(config)# crypto gdoi group group1`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。
ステップ 4	**identity***name* 例： `Router(config-gdoi-group)# identity 2345`	クリプト マップに対して ID を設定します。
ステップ 5	**passive** 例： `Router(config-gdoi-group)# passive`	グループ メンバーを passive モードにします。

	コマンドまたはアクション	目的
ステップ 6	**serveraddressipv4**{*address* | *hostname*} 例： `Router(config-gdoi-group)# server address ipv4 209.165.200.225`	GDOI グループが到達しようとするサーバのアドレスを指定します。

キー サーバのロールのリセット

プライマリ サーバの連係可能なロールをリセットするには、次の手順を実行します。

手順の概要

1. **enable**
2. **clearcryptogdoikscooprole**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clearcryptogdoikscooprole** 例： `Router# clear crypto gdoi ks coop role`	キー サーバの連携ロールをリセットします。

グループ メンバーの設定

グループ メンバーを設定するには、次のサブ作業を実行します。

グループ名、ID、キー サーバ IP アドレス、およびグループ メンバー登録の設定

グループ名、ID、キー サーバ IP アドレス、およびグループ メンバー登録を設定するには、次の手順を実行します。キー サーバ アドレスは 8 個まで設定できます。

手順の概要

1. **enable**
2. **configureterminal**
3. **cryptogdoigroup***group-name*
4. 次のいずれかを実行します。
   - **identitynumber***number*
   - **identityaddressipv4***address*
5. **serveraddressipv4***address*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cryptogdoigroup***group-name* 例： `Router(config)# crypto gdoi group gdoigroupone`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。

ステップ 4	次のいずれかを実行します。
	• **identitynumber***number*
	• **identityaddressipv4***address*
	
	例：
	
	`Router(config-gdoi-group)# identity number 3333`
	
	例：
	
	`Router(config-gdoi-group)# identity address ipv4 209.165.200.225`
		GDOI グループ番号またはアドレスを指定します。

	コマンドまたはアクション	目的
ステップ 5	**serveraddressipv4***address* 例： `Router(config-gdoi-group)# server address ipv4 209.165.200.225`	GDOI グループが到達しようとするサーバのアドレスを指定します。 • アドレスを無効にするには、このコマンドの **no** 形式を使用します。

次の作業

クリプトマップを設定します。「暗号マップエントリの作成」セクションを参照してください。

暗号マップ エントリの作成

クリプト マップ エントリを作成し、それに GDOI グループを関連付けるには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **cryptomap***map-nameseq-num***gdoi**
4. **setgroup***group-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cryptomap***map-nameseq-num***gdoi** 例： `Router(config)# crypto map mymap 10 gdoi`	クリプト マップ コンフィギュレーション モードを開始して、クリプト マップ エントリを作成または変更します。

	コマンドまたはアクション	目的
ステップ 4	**setgroup***group-name* 例： `Router(config-crypto-map)# set group group1`	GDOI グループをクリプト マップに関連付けます。

次の作業

トラフィックを暗号化する必要があるインターフェイスにクリプト マップを適用します。「トラフィックを暗号化する必要があるインターフェイスへの暗号マップの適用」セクションを参照してください。

トラフィックを暗号化する必要があるインターフェイスへの暗号マップの適用

トラフィックを暗号化する必要があるインターフェイスに暗号マップを適用するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***typeslot*/*port*
4. **cryptomap***map-name***redundancy***standby-group-name***stateful**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface***typeslot/port* 例： `Router(config)# interface gigabitethernet 0/0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**cryptomap***map-name***redundancy***standby-group-name***stateful** 例： `Router(config-if)# crypto map map1`	クリプトマップをインターフェイスに適用します。

Fail-Close モードのアクティブ化

Fail-Close モードは、グループ メンバーがキー サーバに登録される前に暗号されていないトラフィックがそのグループ メンバーを通過しないようにします。

クリプト マップを Fail-Close モードで動作するように設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **cryptomap***map-name***gdoifail-close**
4. **matchaddress** {*access-list-number* |*access-list-name*}
5. **activate**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**cryptomap***map-name***gdoifail-close** 例： `Router(config)# crypto map map1 gdoi fail-close`	暗号マップが Fail-Close モードで動作するように指定して暗号マップ Fail-Close コンフィギュレーション モードを開始します。
ステップ 4	**matchaddress** {*access-list-number* |*access-list-name*} 例： `Router(crypto-map-fail-close)# match address 133`	（オプション）GDOI 登録用の ACL を指定します。
ステップ 5	**activate** 例： `Router(crypto-map-fail-close)# activate`	Fail-Close モードをアクティブ化します。

KEK の許容可能な暗号化アルゴリズムまたはハッシュ アルゴリズムの設定

（注） セキュリティに対する脅威とそれに対抗するための暗号化技術は絶えず変化しています。暗号化に関するシスコの最新の推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

GM によって許可される KEK の暗号化およびハッシュ アルゴリズムを設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **cryptogdoigroup***group-name*
4. 次のいずれかのコマンドを入力します。
   - **identitynumber***number*
   - **identityaddressipv4***address*
5. **serveraddressipv4***address*
6. **clientrekeyencryption***cipher*[...[*cipher*]]
7. **clientrekeyhash***hash*
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cryptogdoigroup***group-name* 例： `Router(config)# crypto gdoi group gdoigroupone`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。
ステップ 4	次のいずれかのコマンドを入力します。 • **identitynumber***number* • **identityaddressipv4***address* 例： `Router(config-gdoi-group)# identity number 3333`	GDOI グループ番号またはアドレスを指定します。

	コマンドまたはアクション	目的
	例： `Router(config-gdoi-group)# identity address ipv4 10.2.2.2`	
ステップ 5	**serveraddressipv4***address* 例： `Router(config-gdoi-group)# server address ipv4 10.0.5.2`	GDOI グループが到達しようとするサーバのアドレスを指定します。 • アドレスを無効にするには、このコマンドの **no** 形式を使用します。
ステップ 6	**clientrekeyencryption***cipher*[...[*cipher*]] 例： `Router(config-gdoi-group)# client rekey encryption aes 128 aes 192 aes 256`	KEK のクライアント受け入れ可能キー再生成暗号化を設定します。
ステップ 7	**clientrekeyhash***hash* 例： `Router(config-gdoi-group)# client rekey hash sha`	KEK のクライアント受け入れ可能ハッシュを設定します。
ステップ 8	**end** 例： `Router(config-gdoi-group)# end`	GDOI グループ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

TEK の受け入れ可能トランスフォーム セットの設定

GM によって許可されるデータ暗号化または認証のために TEK が使用するトランスフォーム セットを設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **cryptoipsectransform-set***transform-set-nametransform* [*transform2...transform4*]
4. **exit**
5. **cryptogdoigroup***group-name*
6. **clienttransform-sets***transform-set-name1* [...[*transform-set-name6*]]
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cryptoipsectransform-set***transform-set-nametransform* [*transform2...transform4*] 例： `Router(config)# crypto ipsec transform-set g1 esp-aes 192 esp-sha-hmac`	トランフォーム セット（セキュリティ プロトコルおよびアルゴリズムの受け入れ可能な組み合わせ）を定義し、暗号化トランスフォーム コンフィギュレーション モードを開始します。
ステップ 4	**exit** 例： `Router(cfg-crypto-trans)# exit`	暗号化トランスフォーム コンフィギュレーション モードを終了します。
ステップ 5	**cryptogdoigroup***group-name* 例： `Router(config)# crypto gdoi group gdoigroupone`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 6	**clienttransform-sets***transform-set-name1* [...[*transform-set-name6*]] 例： `Router(config-gdoi-group)# client transform-sets g1`	データの暗号化および認証のためにTEKによって使用される受け入れ可能トランスフォームタグを指定します。 • トランスフォーム セット タグは 6 個まで指定できます。
ステップ 7	**end** 例： `Router(config-gdoi-group)# end`	GDOI グループ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

グループ メンバーの暗号状態の追跡

設定済みの拡張オブジェクト トラッカー（EOT）のスタブオブジェクト ID を使用してグループ メンバー（GM）の暗号化状態を追跡するには、この作業を実行します。

はじめる前に

スタブオブジェクトを作成し、このオブジェクトにトラッキング ID を割り当てて GDOI MIB をモニタすることにより、拡張オブジェクトトラッキング（EOT）を設定する必要があります。次に、トラッキング ID 99 をスタブオブジェクトに割り当てる設定例を示します。

```
event manager applet test1
 event snmp oid <new GDOI MIB object> .....
 action 2.0 track set 99 state up

track 99 stub-object
 delay up 60
```

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group***group-name*
4. **client status active-sa track***tracking-number*
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gdoi group***group-name* 例： `Device(config)# crypto gdoi group gdoigroupone`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。
ステップ 4	**client status active-sa track***tracking-number* 例： `Device(config-gdoi-group)# client status active-sa track 99`	スタブオブジェクトの追跡を有効化します。この例では、GM がキー サーバ（KS）から有効なトラフィック暗号キー（TEK）を受信すると、スタブオブジェクト 99 の状態を「UP」に設定します。一方、登録失敗やキー再生成の前に TEK の期限が切れた場合などのエラーのために有効な TEK がない場合、GM はスタブオブジェクト 99 の状態を「DOWN」に設定します。
ステップ 5	**exit** 例： `Device(config-gdoi-group)# exit`	GDOI グループ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

GET VPN GM 認証の設定

GET VPN GM 認証は、事前共有キーまたは PKI を使用して実行できます。GET VPN 認証をオンにすることはベスト プラクティスです。キー サーバが複数の GDOI グループに使用される際、あるグループの GM が別のグループからキーとポリシーを要求するのを防ぐには、キー サーバ認証が必要です。ISAKMP 認証では GM がキー サーバから GDOI 属性を要求できることが確認され、GDOI 認証では GM がキー サーバに設定された特定のグループから GDOI 属性を要求できることが確認されます。

GET VPN GM 認証を設定するには、次のいずれかのタスクを実行します。

事前共有キーを使用する GM 認証の設定

事前共有キーを使用する GM の認証を設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **cryptogdoigroup***group-name*
4. **serverlocal**
5. **authorizationaddressipv4**{*access-list-name*|*access-list-number*}
6. **exit**
7. **exit**
8. **access-list***access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**time-range** *time-range-name*] [**fragments**] [**log** [*word*] | **log-input** [*word*]]
9. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cryptogdoigroup***group-name* 例： `Router(config)# crypto gdoi group getvpn`	GDOI を指定し、GDOI グループ コンフィギュレーション モードを開始します。
ステップ 4	**serverlocal** 例： `Router(config-gdoi-group)# server local`	デバイスを GDOI キー サーバとして指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**authorizationaddressipv4**{*access-list-name*|*access-list-number*} 例： `Router(gdoi-local-server)# authorization address ipv4 50`	GDOI のアドレスのリストを指定します。
ステップ 6	**exit** 例： `Router(gdoi-local-server)# exit`	GDOI ローカル コンフィギュレーション モードを終了して GDOI グループ コンフィギュレーション モードに戻ります。
ステップ 7	**exit** 例： `Router(config-gdoi-group)# exit`	GDOI グループ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**access-list***access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**time-range** *time-range-name*] [**fragments**] [**log** [*word*] | **log-input** [*word*]] 例： `Router(config)# access-list 50 permit ip 209.165.200.225 0.0.0.0 209.165.200.254 0.0.0.0`	許可される IP アクセス リストを定義します。 • この例では、アクセス リスト番号 50 のアクセスリストが定義され、送信元 IP アドレス 209.165.200.225 から宛先 IP アドレス 209.165.200.254 に送信されるパケットが許可されます。
ステップ 9	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

PKI を使用する GM 認証の設定

PKI を使用する GM の認証を設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **cryptoisakmpidentity** {**address** | **dn** | **hostname**}
4. **cryptopkitrustpoint***name*
5. **subject-name** [*x.500-name*]
6. **exit**
7. **cryptogdoigroup***group-name*
8. **serverlocal**
9. **authorizationidentity***name*
10. **exit**
11. **exit**
12. **cryptoidentity***name*
13. **dn***name=string* [, *name=string*]
14. **exit**
15. **cryptoisakmpidentity** {**address** | **dn** | **hostname**}
16. **cryptopkitrustpoint***name*
17. **subject-name** [*x.500-name*]
18. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cryptoisakmpidentity** {**address** | **dn** | **hostname**} 例： `Router(config)# crypto isakmp identity dn`	ルータがインターネットキー交換（IKE）プロトコルに参加する際にルータが使用するアイデンティティを定義します。

	コマンドまたはアクション	目的
ステップ 4	**cryptopkitrustpoint***name* 例： `Router(config)# crypto pki trustpoint GETVPN`	ルータで使用するトラストポイントを宣言し、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 5	**subject-name** [*x.500-name*] 例： `Router(ca-trustpoint)# subject-name OU=GETVPN`	証明書要求の所有者名を指定します。
ステップ 6	**exit** 例： `Router(ca-trustpoint)# exit`	CA トラストポイント コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**cryptogdoigroup***group-name* 例： `Router(config)# crypto gdoi group getvpn`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。
ステップ 8	**serverlocal** 例： `Router(config-gdoi-group)# server local`	デバイスを GDOI キー サーバとして指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 9	**authorizationidentity***name* 例： `Router(gdoi-local-server)# authorization identity GETVPN_FILTER`	GDOI グループのアイデンティティを指定します。
ステップ 10	**exit** 例： `Router(gdoi-local-server)# exit`	GDOI ローカル サーバ コンフィギュレーション モードを終了して GDOI グループ コンフィギュレーション モードに戻ります。
ステップ 11	**exit** 例： `Router(config-gdoi-group)# exit`	GDOI グループ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 12	**cryptoidentity***name* 例： `Router(config)# crypto identity GETVPN_FILTER`	ルータの証明書内にある指定 DN リストを使用してルータのアイデンティティを設定し、暗号アイデンティティ コンフィギュレーション モードを開始します。
ステップ 13	**dn***name*=*string* [, *name*=*string*] 例： `Router(config-crypto-identity)# dn ou=GETVPN`	ルータの証明書内にある DN に、ルータのアイデンティティを関連付けます。
ステップ 14	**exit** 例： `Router(config-crypto-identity)# exit`	GDOI グループ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 15	**cryptoisakmpidentity** {**address** | **dn** | **hostname**} 例： `Router(config)# crypto isakmp identity dn`	IKE プロトコルに参加する際にルータが使用するアイデンティティを定義します。
ステップ 16	**cryptopkitrustpoint***name* 例： `Router(config)# crypto pki trustpoint GETVPN`	ルータで使用するトラストポイントを宣言し、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 17	**subject-name** [*x.500-name*] 例： `Router(ca-trustpoint)# subject-name ou=getvpn`	証明書要求の所有者名を指定します。
ステップ 18	**end** 例： `Router(ca-trustpoint)# exit`	GDOI グループ コンフィギュレーション モードを終了し、設定を保存して、特権 EXEC モードに戻ります。

Cisco Group Encrypted Transport VPN 設定の確認とトラブルシューティング

GET VPN の設定を確認およびトラブルシューティングするには、次の作業を行います。これらの作業は任意であり、トラブルシューティング中に情報を収集するために行います。

（注） CSCsi82594 では、時間ベースのアンチリプレイ（TBAR）を有効にした場合、キー再生成の期間は 2 時間（7200 秒）に設定されます。このシナリオでは、キー サーバは 2 時間（7200 秒）ごとにグループ メンバーに定期的にキー再生成を送信します。次の例では、トラフィック暗号キー（TEK）のライフタイムが 28800 秒（8 時間）に設定されていますが、キー再生成タイマーは依然として 2 時間です。TBAR 情報を表示する show の出力には、**show crypto gdoi gm replay** および **show crypto gdoi ks replay** コマンドを使用します。

```
crypto ipsec profile atm-profile
set security-association lifetime seconds 28800
!
crypto gdoi group ATM-DSL
server local
   sa ipsec 1
      !
      replay time window-size 100
```

キー サーバ上のアクティブなグループ メンバーの確認

キー サーバ上のアクティブなグループ メンバーを確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **showcryptogdoiksmembers**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showcryptogdoiksmembers** 例： `Router# show crypto gdoi ks members`	キー サーバ メンバーに関する情報を表示します。

キー再生成関連統計情報の確認

キー再生成関連統計情報を確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **showcryptogdoiksrekey**
3. **showcryptogdoi [gm]**

手順の詳細

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードをイネーブルにします。

- パスワードを入力します（要求された場合）。

ステップ 2 **showcryptogdoiksrekey**

例：

```
Device# show crypto gdoi ks rekey

For group diffint (handle: 2147483650) server 10.0.8.1 (handle: 2147483650):

# of teks : 1 Seq num : 0
KEK POLICY (transport type : Unicast)
spi : 0xA8110DE7CC8B0FB201F2A8BFAA0F2D90
management alg : disabled encrypt alg : 3DES
crypto iv length : 8 key size : 24
orig life(sec): 300 remaining life(sec): 296 <------- ticking down
sig hash algorithm : enabled sig key length : 94
sig size : 64
sig key name : mykeys
```

キー サーバ上でこのコマンドを実行すると、キー サーバから送信されるキー再生成に関する情報が表示されます。出力は、KEK の残りのライフタイムの経過を表示します。

ステップ 3 **showcryptogdoi [gm]**

例：

```
Device# show crypto gdoi
GROUP INFORMATION

Group Name : diffint
Group Identity : 3333
```

```
Rekeys received : 0
IPSec SA Direction : Both

Group Server list : 10.0.8.1

Group member : 10.0.3.1 vrf: None
Version : 1.0.2
Registration status : Registered
Registered with : 10.0.8.1
Re-registers in : 93 sec <-----------re-registration time for TEK or KEK
Succeeded registration: 1
Attempted registration: 1
Last rekey from : 0.0.0.0
Last rekey seq num : 0
Unicast rekey received: 0
Rekey ACKs sent : 0
Rekey Received : never
allowable rekey cipher: any
allowable rekey hash : any
allowable transformtag: any ESP

Rekeys cumulative
Total received : 0
After latest register : 0
Rekey Acks sents : 0

ACL Downloaded From KS 10.0.8.1:
access-list permit ip host 10.0.1.1 host 239.0.1.1
access-list permit ip host 10.0.100.2 host 238.0.1.1

KEK POLICY:
Rekey Transport Type : Unicast
Lifetime (secs) : 255 <-----------lifetime ticking
Encrypt Algorithm : 3DES
Key Size : 192
Sig Hash Algorithm : HMAC_AUTH_SHA
Sig Key Length (bits) : 512
```

グループ メンバー上でこのコマンドを実行すると、キー サーバから送信されるキー再生成に関する情報が表示されます。出力の「re-registers in」フィールドは、その後にグループ メンバーが TEK または KEK に再登録する、より短い方の期間を表示します。

グループ メンバー上で GDOI によって作成された IPsec SA の確認

グループ メンバー上で GDOI によって作成された IPsec SA を確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **showcryptogdoigroup***group-name***ipsecsa**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showcryptogdoigroup***group-name***ipsecsa** 例： `Router# show crypto gdoi group diffint ipsec sa`	グループ メンバー上で GDOI によって作成された IPsec SA に関する情報を表示します。 • この場合、表示されるのは、グループ「diffint」に関する情報だけです。 • すべてのグループの IPsec SA に関する情報を表示するには、**group** キーワードおよび *group-name* 引数を省略します。

キー サーバ上で GDOI によって作成された IPsec SA の確認

キー サーバ上で GDOI によって作成された IPsec SA を確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **showcryptoipsecsa**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showcryptoipsecsa** 例： `Device# show crypto ipsec sa`	現在のSAによって使用されている設定を表示します。

グループ メンバーが最後にキー サーバから受信した TEK の確認

GM が最後に KS から受信した TEK を確認するには、GM で次のステップを実行します。

手順の概要

1. **enable**
2. **showcryptogdoi**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showcryptogdoi** 例： `Router# show crypto gdoi`	現在の GDOI 構成、および KS からダウンロードされたポリシーを表示します。TEK は TEK POLICY セクションに表示されます。デバッグを有効にせずに、次のコマンドを使用することで、TEK が実際に最後に受信した GM を KS から IPsec コントロール プレーンにダウンロードした TEK（**show crypto ipsec sa** コマンドを使用して表示可能）と比較できます。

連携キー サーバの状態と統計情報の確認

連携キー サーバの状態と統計情報を確認するには、**debug** および **show** コマンドのうち 1 つまたは両方を使用して、次の手順を実行します。

手順の概要

1. **enable**
2. **debugcryptogdoikscoop**
3. **showcryptogdoigroup***group-name***kscoop**[**version**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debugcryptogdoikscoop** 例： `Router# debug crypto gdoi ks coop`	連携キー サーバに関する情報を表示します。
ステップ 3	**showcryptogdoigroup***group-name***kscoop**[**version**] 例： `Router# show crypto gdoi group diffint ks coop version`	グループ「diffint」に関する情報と、連携キー サーバに関するバージョン情報を表示します。

アンチリプレイ疑似時間関連の統計情報の確認

アンチリプレイ疑似時間関連の統計情報を確認するには、**clear**、**debug**、および **show** コマンドのうち 1 つまたはすべてを使用して、次の手順を実行します。

手順の概要

1. **enable**
2. **clearcryptogdoigroup***group-name***replay**
3. **debugcryptogdoireplay**
4. **showcryptogdoigroup***group-name*
5. **showcryptogdoigroup***group-name***ksreplay**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**clearcryptogdoigroup***group-name***replay** 例： `Router# clear crypto gdoi group diffint replay`	リプレイ カウンタを消去します。
ステップ 3	**debugcryptogdoireplay** 例： `Router# debug crypto gdoi replay`	パケット内に格納されている疑似時間スタンプに関する情報を表示します。
ステップ 4	**showcryptogdoigroup***group-name* 例： `Router# show crypto gdoi group diffint`	グループ メンバーの現在の疑似時間に関する情報を表示します。 • このグループのアンチリプレイに関連する各種カウントも表示します。
ステップ 5	**showcryptogdoigroup***group-name***ksreplay** 例： `Router# show crypto gdoi group diffint ks replay`	キー サーバの現在の疑似時間に関する情報を表示します。

暗号マップの Fail-Close モードの状態の確認

クリプト マップの Fail-Close モードの状態を確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **showcryptomapgdoifail-close**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**showcryptomapgdoifail-close** 例： `Router# show crypto map gdoi fail-close`	Fail-Close モードの状態に関する情報を表示します。

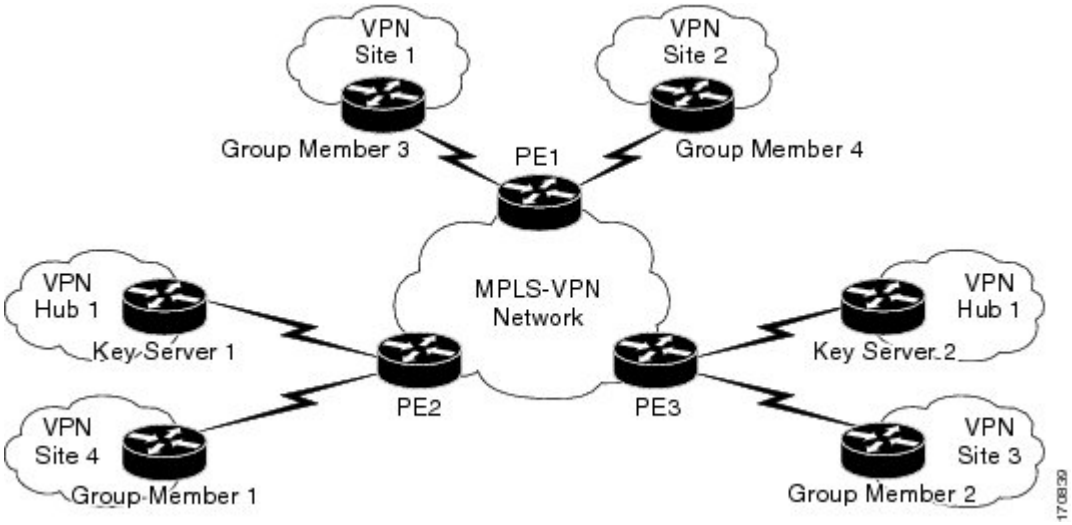
Cisco Group Encrypted Transport VPN の設定例

例：キー サーバとグループ メンバーのケース スタディ

次のケース スタディでは、MPLS VPN 環境における CE 間のトラフィックを暗号化します。

MPLS VPN コアによって、下図に示すとおりに各 VPN サイトを相互接続します。Group Member 1 から Group Member 4 までの VPN サイト CPE を、これらのサイトがその一部となっている VPN と関連付けられた単一の GDOI グループにグループ化します。このシナリオは、インターネット VPN のシナリオです。すべてのキー サーバおよびグループ メンバーは同じ VPN の一部です。Key Server 1 と Key Server 2 は連携キー サーバであり、VPN メンバーである Group Member 1 から Group Member 4 までがサポートされています。Key Server 1 はプライマリ キー サーバであり、Key Server 2 はセカンダリ キー サーバです。

図 *13*：キー サーバとグループ メンバーのシナリオ



次の設定例は上図のケース スタディに基づいています。

キー サーバ 1 の例

Key server 1 はプライマリ キー サーバです。

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname KS1
!
logging buffered 100000 debugging
no logging console
!
no aaa new-model
!
resource policy
!
clock timezone EST 0
ip subnet-zero
no ip domain lookup
ip domain name cisco.com
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
 lifetime 400
crypto isakmp key cisco address 10.1.1.13
crypto isakmp key cisco address 10.1.1.9
crypto isakmp key cisco address 10.1.1.1
crypto isakmp key cisco address 10.1.1.5
crypto isakmp key cisco address 10.1.1.21
!
crypto ipsec transform-set gdoi-trans-group1 esp-3des esp-sha-hmac
!
crypto ipsec profile gdoi-profile-group1
 set security-association lifetime seconds 1800
 set transform-set gdoi-trans-group1
!
crypto gdoi group group1
 identity number 1
 server local
  rekey lifetime seconds 86400
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa group1-export-general
  rekey transport unicast
  sa ipsec 1
   profile gdoi-profile-group1
   match address ipv4 101
   replay counter window-size 64
  address ipv4 209.165.200.225
  redundancy
   local priority 10
   peer address ipv4 209.165.200.225
   !
interface Ethernet0/0
 ip address 209.165.200.225 255.255.255.252
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.18
!
access-list 101 permit ip 10.1.0.0 0.0.255.255 10.1.0.0 0.0.255.255
!
end
```

キー サーバ 2 の例

Key Server 2はセカンダリ キー サーバです。

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname KS2
!
logging buffered 100000 debugging
no logging console
!
no aaa new-model
!
resource policy
!
clock timezone EST 0
ip subnet-zero
no ip domain lookup
ip domain name cisco
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
 lifetime 400
crypto isakmp key cisco address 10.1.1.9
crypto isakmp key cisco address 10.1.1.1
crypto isakmp key cisco address 10.1.1.5
crypto isakmp key cisco address 10.1.1.17
crypto isakmp key cisco address 10.1.1.13
!
crypto ipsec transform-set gdoi-trans-group1 esp-3des esp-sha-hmac
!
crypto ipsec profile gdoi-profile-group1
 set security-association lifetime seconds 1800
 set transform-set gdoi-trans-group1
!
crypto gdoi group group1
 identity number 1
 server local

  rekey lifetime seconds 86400
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa group1-export-general
  rekey transport unicast
  sa ipsec 1
   profile gdoi-profile-group1
   match address ipv4 101
   replay counter window-size 64
  address ipv4 10.1.1.21
  redundancy
   local priority 1
   peer address ipv4 10.1.1.17
   !
interface Ethernet0/0
 ip address 209.165.200.225 255.255.255.252
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.22
!
access-list 101 permit ip 10.1.0.0 0.0.255.255 10.1.0.0 0.0.255.255
!
end
```

例：グループ メンバー 1 の設定

Group Member 1 は、これらのサイトがその一部となっている VPN と関連付けられた GDOI グループの一部です。

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname GM1
!
resource policy
!
clock timezone EST 0
ip subnet-zero
!
crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 14
 lifetime 3600
crypto isakmp key cisco address 209.165.200.225
crypto isakmp key cisco address 209.165.201.1
!
crypto gdoi group group1
 identity number 1
 server address ipv4 209.165.200.225
 server address ipv4 209.165.201.1
!
crypto map map-group1 10 gdoi
 set group group1
!
interface Ethernet0/0
 ip address 209.165.200.225 255.255.255.252
 crypto map map-group1
!
router bgp 1000
 no synchronization
 bgp log-neighbor-changes
 network 10.1.1.0 mask 255.255.255.0
 neighbor 10.1.1.2 remote-as 5000
 no auto-summary
!
ip classless
!
End
The same GDOI group cannot be applied to multiple interfaces. The following examples show
unsupported cases:
```

例 1

```
crypto map map-group1
  group g1
 interface ethernet 1/0
  crypto map map-group1
 interface ethernet 2/0
  crypto map map-group1
```

例 2

```
crypto map map-group1 10 gdoi
  set group group1
crypto map map-group2 10 gdoi
  set group group1
```

```
 interface ethernet 1/0
  crypto map map-group1
 interface ethernet 2/0
```

例：グループ メンバー 2 の設定

Group Member 2 は、これらのサイトがその一部となっている VPN と関連付けられた GDOI グループの一部です。

```
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname GM2
!
resource policy
!
clock timezone EST 0
ip subnet-zero
!
crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 14
 lifetime 3600
crypto isakmp key cisco address 209.165.200.225
crypto isakmp key cisco address 209.165.201.1
!
crypto gdoi group group1
 identity number 1
 server address ipv4 209.165.201.1
 server address ipv4 209.165.200.225
!
crypto map map-group1 10 gdoi
 set group group1
!
interface Ethernet0/0
 ip address 209.165.200.225 255.255.255.252
 crypto map map-group1
!
router bgp 2000
 no synchronization
 bgp log-neighbor-changes
 network 10.1.2.0 mask 255.255.255.0
 neighbor 10.1.1.6 remote-as 5000
 no auto-summary
!
ip classless
!
end
```

例：グループ メンバー 3 の設定

Group Member 3 は、これらのサイトがその一部となっている VPN と関連付けられた GDOI グループの一部です。

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname GM3
!
resource policy
!
```

```
clock timezone EST 0
ip subnet-zero
!
crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 14
 lifetime 3600
crypto isakmp key cisco address 209.165.200.225
crypto isakmp key cisco address 209.165.201.1
!
crypto ipsec transform-set gdoi-trans-group1 esp-aes esp-sha-hmac
crypto gdoi group group1
 identity number 1
 server address ipv4 209.165.200.225
 server address ipv4 209.165.201.1
!
crypto map map-group1 10 gdoi
 set group group1
!
interface Ethernet0/0
 ip address 209.165.201.1 255.255.255.252
 crypto map map-group1
!
router bgp 3000
 no synchronization
 bgp log-neighbor-changes
 network 10.1.3.0 mask 255.255.255.0
 neighbor 10.1.1.10 remote-as 5000
 no auto-summary
!
ip classless
!
end
```

例：グループ メンバー 4 の設定

Group Member 4 は、これらのサイトがその一部となっている VPN と関連付けられた GDOI グループの一部です。

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname GM4
!
clock timezone EST 0
ip subnet-zero
!
crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 14
 lifetime 3600
crypto isakmp key cisco address 209.165.200.225
crypto isakmp key cisco address 209.165.201.1
!
crypto gdoi group group1
 identity number 1
 server address ipv4 209.165.200.225
 server address ipv4 209.165.201.1
!
crypto map map-group1 10 gdoi
 set group group1
!
interface Ethernet0/0
 ip address 209.165.201.1 255.255.255.252
 crypto map map-group1
```

```
!
router bgp 4000
 no synchronization
 bgp log-neighbor-changes
 network 10.1.4.0 mask 255.255.255.0
 neighbor 10.1.1.14 remote-as 5000
 no auto-summary
!
ip classless
!
end
```

例：グループ メンバー 5 の設定

グループ メンバーの複数のインターフェイスが同じ GDOI グループの一部である場合、ループバック インターフェイスを使用して暗号化を行う必要があります。ループバック インターフェイスを使用しない場合、暗号化されたトラフィックが処理される各インターフェイスを個別にキー サーバに登録する必要があります。

キー サーバではこれらが別個の要求と判断されるので、同一のグループ メンバーの複数のレコードが保管されます。これは、複数のキー再生成が送信されることも意味します。暗号化がループバック インターフェイスから行われる場合は、グループ メンバーを一度だけキー サーバに登録します。

次の設定は、どのようにグループ メンバーを一度だけキー サーバに登録するのかを示しています。

```
!

interface GigabitEthernet0/1
 description *** To AGG-1 ***
 crypto map dgvpn
!
interface GigabitEthernet0/2
 description *** To AGG-2 ***
 crypto map dgvpn
!
interface Loopback0
 ip address 209.165.201.1 255.255.255.255
!
 crypto map dgvpn local-address Loopback0
!
```

例：グループ メンバーが最後にキー サーバから受信した TEK の確認

次の例は、現在の GDOI 構成、および KS からダウンロードされたポリシーを表示する方法を示します。

```
Device# show crypto gdoi

GROUP INFORMATION

    Group Name               : GETV6
.
.
.
KEK POLICY:
.
.
```

```
.
TEK POLICY for the current KS-Policy ACEs Downloaded:
  Ethernet2/0:
    IPsec SA:
        spi: 0x627E4B84(1652444036)
        transform: esp-aes
        sa timing:remaining key lifetime (sec): (3214)
        Anti-Replay(Time Based) : 10 sec interval
        tag method : cts sgt
        alg key size: 24 (bytes)
        sig key size: 20 (bytes)
        encaps: ENCAPS_TUNNEL


GROUP INFORMATION

    Group Name               : GETV4
.
.
.
KEK POLICY:
.
.
.
TEK POLICY for the current KS-Policy ACEs Downloaded:
  Ethernet2/0:
    IPsec SA:
        spi: 0xF6E6B597(4142314903)
        transform: esp-aes
        sa timing:remaining key lifetime (sec): (3214)
        Anti-Replay : Disabled
        tag method : cts sgt
        alg key size: 24 (bytes)
        sig key size: 20 (bytes)
        encaps: ENCAPS_TUNNEL
```

TEK は TEK POLICY セクションに表示されます。デバッグを有効にせずに、次のコマンドを使用することで、TEK が実際に最後に受信した GM を KS から IPsec コントロール プレーンにダウンロードした TEK（**show crypto ipsec sa** コマンドを使用して表示可能）と比較できます。

タグ メソッド フィールドは、GET VPN インライン タギングに使用するメソッドを示します。可能な値は cts sgt（Cisco TrustSec セキュリティ グループ タグ用）または無効です。alg キー サイズ フィールドは、TEK ポリシーで設定されている暗号化アルゴリズムのキーの長さを示します。sig キー サイズ フィールドは、TEK ポリシーで設定されている署名のキーの長さを示します。encaps フィールドは、TEK ポリシーで設定されている IPsec カプセル化のタイプ（トンネルまたはトランスポート）を示します。

このコマンドの出力は、TEK が KS から受け取った時刻から期限切れになったことを示す場合があります。

パッシブ SA の例

次の例は、発信パケットに関する暗号化ルールに関する情報を示しています。

```
Router# show crypto ruleset
Ethernet0/0:
  59 ANY ANY DENY
  11 ANY/848 ANY/848 DENY
 IP ANY ANY IPSec SA Passive
 IP ANY ANY IPSec Cryptomap
```

次の例は、IPsec SA の方向モードを示しています。

```
Router# show crypto ruleset detail
Ethernet0/0:
 20000001000019  59 ANY ANY DENY -> 20000001999999
20000001000029  11 ANY/848 ANY/848 DENY -> 20000001999999
 20000001000035 IP ANY ANY IPSec SA Passive
 20000001000039 IP ANY ANY IPSec Cryptomap
```

Fail-Close モードの例

次の例は、Fail-Close モードがすでにアクティブになっていて、グループ メンバーが登録される前のアクセス リスト 102 からの暗号化されていないトラフィックが許可されていることを示しています。

```
crypto map map1 gdoi fail-close
 match address 102
 activate
crypto map map1 10 gdoi
 set group ks1_group
 match address 101
!
access-list 101 deny ip 10.0.1.0 0.0.0.255 10.0.1.0 0.0.0.255
access-list 102 deny tcp any eq telnet any
```

次の **show crypto map gdoi fail-close** コマンドの出力は、Fail-Close モードがすでにアクティブになっていることを示しています。

```
Router# show crypto map gdoi fail-close

Crypto Map: "svn"
        Activate: yes
        Fail-Close Access-List: (Deny = Forward In Clear, Permit = Drop)
            access-list 105 deny tcp any port = 23 any
            access-list 105 deny ospf any any
```

Cisco Group Encrypted Transport VPN の追加の制約事項

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command References*』
IKE および IKE ポリシーの設定	『*Internet Key Exchange for IPsec VPNs Configuration Guide*』の「Configuring Internet Key Exchange for IPsec VPNs」モジュール

関連項目	マニュアル タイトル
IPsec トランスフォームの設定	『*Internet Key Exchange for IPsec VPNs Configuration Guide*』の「Configuring Internet Key Exchange for IPsec VPNs」モジュール
エンタープライズ ネットワークの GET VPN の有効化のための基本的な導入ガイドライン	『Cisco IOS GET VPN Solutions Deployment Guide』
別の VRF（専用の管理 VRF など）によるコントロールプレーン トラフィック（GDOI 登録およびキー再生成）のルーティング	『Cisco IOS GETVPN VRF-Aware GDOI GM Solution Deployment Guide』
推奨される暗号化アルゴリズム	『Next Generation Encryption』

標準

規格	タイトル
新しい標準または変更された標準はサポートされていません。また、既存の標準に対するサポートに変更はありません。	—

MIB

MIB	MIB のリンク
CISCO-GDOI-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2401	『*Security Architecture for the Internet Protocol*』

RFC	タイトル
RFC 6407	『*The Group Domain of Interpretation*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Cisco Group Encrypted Transport VPN の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *4*：*Cisco Group Encrypted Transport VPN* の機能情報

機能名	リリース	機能情報
Cisco Group Encrypted Transport VPN	Cisco IOS XE Release 2.3	Cisco Group Encrypted Transport VPN は、any-to-any の接続を必要とする大規模な IP または MPLS サイトに対する最適な暗号化ソリューションであり、コンバージェンスに要する時間が最短に抑えられ、処理、プロビジョニング、管理、トラブルシューティングの低いオーバヘッドを実現しています。 次のコマンドが導入または変更されました：**addressipv4(GDOI)**、**clearcryptogdoi**、**cryptogdoigm**、**debugcryptogdoi**、**localpriority**、**peeraddressipv4**、**redundancy**、**rekeyaddressipv4**、**rekeytransportunicast**、**replaycounterwindow-size**、**replaytimewindow-size**、**sareceive-only**、**showcryptogdoi**。
GDOI 登録成功を追跡する MIB オブジェクトの作成	Cisco IOS XE リリース 3.12S	GDOI 登録成功を追跡する MIB オブジェクトの作成機能では、グループ内のアクティブな TEK 数を示すため、GDOI MIB に新しい MIB オブジェクトが導入されています。

機能名	リリース	機能情報
GET VPN の強化	Cisco IOS XE Release 3.9S	この機能は GET VPN の復元力を改善します。復元力を強化することで、次のいずれかの方法を使用してデータ トラフィックの中断を防止または最小化します。 • トラフィックの中断の原因となる状態が検出された場合に修正を行います。 • 障害が検出された場合に迅速に回復機能を実行します。 次のコマンドが変更されました：**show crypto gdoi**、**show crypto ipsec sa**、**show tech-support**。

機能名	リリース	機能情報
GET VPN フェーズ 1.2	Cisco IOS XE Release 2.3	これらの機能拡張には、次の機能があります。 • キー サーバのロールの変更 この機能を使用すれば、キー サーバのロールをプライマリからセカンダリに変更できます。 次のコマンドはこの機能のために追加または変更されました：**clear crypto gdoi ks coop role** • Fail-Close モード この機能によって、グループ メンバーが登録される前に、暗号化されていないトラフィックがそのグループ メンバーを通過することを防止できます。 次のコマンドはこの機能のために追加または変更されました：**activate**、**cryptomap**、**matchaddress**、および **showcryptomap**。 • パッシブ SA この機能を使用すれば、グループ メンバーを passive モードに永続的に設定できます。 次のコマンドはこの機能のために導入されました：**passive**。

機能名	リリース	機能情報
BGP 向けの GETVPN ルーティング対応	Cisco IOS XE リリース 3.13S	BGP の GET VPN ルーティング認識機能では、GETVPN GM の暗号化状態を追跡し、追跡情報を適用して GM で双方向条件付きルート フィルタリングを実行することにより、ルーティング ブラック ホールを防ぎます。 次のコマンドが導入または変更されました：**client status active-sa track**。

機能名	リリース	機能情報
GET VPN の復元力	Cisco IOS XE Release 3.9S	この機能は、エラーが発生したときのデータ トラフィックの中断が防止または最小化されるように GET VPN の復元力を向上します。 この機能は、長い SA ライフタイムの機能を導入しています。これにより、キー暗号キーとトラフィック暗号キーのライフタイムを最大 24 時間から 30 日に延長して設定できます。また、この機能により、最後にスケジュールされたキー再生成の確認応答で応答しなかったグループ メンバーに、定期的にリマインダ キー再生成を送信し続けるようにキー サーバを設定することができます。 長い SA ライフタイムを定期的なリマインダ キー再生成と組み合わせて使用することで、キーがロールオーバーする前にグループ メンバーがスケジュールされたキー再生成を行わない場合、キー サーバがグループ メンバーを効果的に同期できます。 次のコマンドが変更されました：**rekey lifetime**、**rekey retransmit**、**set security-association lifetime**、**show crypto gdoi**。

機能名	リリース	機能情報
Cisco TrustSec の IPsec インライン タギングの GET VPN サポート	Cisco IOS XE Release 3.9S	Cisco TrustSec（CTS）は、認証時に取得したユーザとデバイスの ID 情報を使用して、ネットワークに進入するパケットを分類します。CTS では、CTS ネットワークへの進入時にセキュリティ グループ タグ（SGT）でパケットにタグを付けることで各パケットの分類が維持されます。これにより、パケットはデータ パス全体を通じて識別され、セキュリティおよびその他のポリシー基準が適用されます。タグにより、スイッチやファイアウォールなどの中継ネットワークは分類に基づいてアクセス コントロール ポリシーを適用することができます。Cisco TrustSec の IPsec インライン タギングの GET VPN サポート機能では、GET VPN インライン タギングを使用してプライベート WAN 経由で SGT 情報を伝送します。 次のコマンドが導入または変更されました：**show crypto gdoi**、**show crypto ipsec sa**、**tag cts sgt**。
GET VPN 時間ベースのアンチリプレイ	Cisco IOS XE Release 2.3	時間ベースのアンチリプレイのサポートが Cisco VSA に追加されました。

機能名	リリース	機能情報
GET VPN のトラブルシューティング	Cisco IOS XE Release 3.8S	この機能では、エラー状態のログとそのトレースバック、および条件付きデバッグを保存（これはキー サーバから個々のグループ メンバーをデバッグする機能を提供します）するために、デバッグ レベル（これによりデバッグ メッセージを機能ごとに有効にできます）、イベント ロギング、トレース終了の機能の向上を提供します。条件付きデバッグ機能は、GM またはそのほかの連携キー サーバに基づいてフィルタリングできるように、キー サーバの条件付きデバッグを実行する能力を提供します。イベント ロギング機能は、イベントの最後のセットを記録する機能を提供します。 次のコマンドが導入または変更されました：**clear crypto gdoi**、**debug crypto condition unmatched**、**debug crypto gdoi**、**debug crypto gdoi condition**、**monitor event-trace gdoi**、**show crypto gdoi**、および **show monitor event-trace gdoi**。
Group Encrypted Transport VPN キー サーバ	Cisco IOS XE Release 3.6S	キー サーバとして Cisco IOS XE を実行するデバイスを設定するためのサポートが追加されました。 この機能は、Cisco IOS XE リリース 3.6S で Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 Cisco IOS XE リリース 3.13S では、シスコ クラウド サービス ルータ（CSR）1000V シリーズのサポートが追加されました。

機能名	リリース	機能情報
GET VPN の VSA サポート	Cisco IOS XE Release 2.3	Cisco VSA（高性能暗号化エンジン）サポートが、GDOI および GET VPN に対して追加されました。 （注） このプラットフォームは、このリリースでは時間ベースのアンチリプレイをサポートしていません。
GET VPN IKEv1 の分離	Cisco IOS XE Release 3.11S	この機能は、メンテナンスやトラブルシューティングに役立ちます。 次のコマンドが変更されました：**show tech-support**、**show crypto gdoi** および **show crypto ipsec sa**。

用語集

DOI：Domain of Interpretation（ドメイン オブ インタープリテーション）。Internet Security Association Key Management Protocol（ISAKMP）の場合、キー管理メッセージが送信されるコンテキスト内に記述されるセキュリティ アソシエーション（SA）のペイロード内の値です（IPsec または グループ ドメイン オブ インタープリテーション）。

GDOI：Group Domain of Interpretation（グループ ドメイン オブ インタープリテーション）。ISAKMP の場合、相互に信頼し合うシステムのグループのキーを配信および管理する手段です。

グループ メンバー：グループに登録されるデバイス（Cisco IOS ルータ）。他のグループ メンバーと通信するためにキー サーバによって制御されます。

グループ セキュリティ アソシエーション：グループ内のすべてのグループ メンバーによって共有される SA。

IPsec：IP セキュリティ。一連の RFC（IETF RFC 2401 を参照）で定義されている IP パケット用データ暗号化プロトコル。

ISAKMP：Internet Security Association and Key Management Protocol（インターネット セキュリティ アソシエーションおよびキー管理プロトコル）。暗号キー管理プロトコルのためのフレームワークを提供するプロトコルです。

KEK：Key Encryption Key。キー サーバとグループ メンバー間のキー再生成を保護するために使用されるキーです。

キーサーバ：グループメンバーに対してキーおよびポリシーを配信するデバイス（Cisco IOS ルータ）。

MTU：最大伝送ユニット。通信プロトコルの特定のレイヤによって宛先に渡すことが可能な最大パケットまたはフレーム サイズ（バイト単位）です。

SA：セキュリティ アソシエーション（SA）。グループ内のすべてのグループ メンバーによって共有される SA です。

シンプル ネットワーク管理プロトコル（SNMP）：SNMP エージェントからの管理対象デバイスの外部モニタリングを可能にする、相互運用可能な標準ベースのプロトコルです。

TEK：トラフィック暗号キー。グループ メンバー間のキー再生成を保護するために使用されるキーです。

第 3 章

GET VPN GM の削除とポリシー トリガー

GET VPN GM の削除とポリシー トリガー機能では、グループ暗号化トランスポート（GET）VPN ネットワークから不要なグループメンバー（GM）を簡単に削除できます。新しいセキュリティアソシエーション（SA）をインストールし、古い SA を削除するキー再生成トリガーの方法を提供します。また、デバイスがこれらの機能をサポートする GET VPN ソフトウェアのバージョンを実行しているかどうかを確認することができます。

- 機能情報の確認，115 ページ
- GM の削除とポリシー トリガーに関する情報，116 ページ
- GET VPN GM 削除およびポリシー トリガーの設定方法，121 ページ
- GET VPN GM の削除とポリシーのトリガーの設定例，127 ページ
- GET VPN GM の削除とポリシーのトリガーのその他の参考資料，130 ページ
- GET VPN GM の削除とポリシーのトリガーの機能情報，130 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、『Bug Search Tool』およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

GM の削除とポリシー トリガーに関する情報

GET VPN のソフトウェア バージョン

GET VPN のソフトウェア バージョンは次の形式です。

major-version.minor-version.mini-version

値は次のとおりです。

- *major-version* は、すべての GET VPN デバイスの互換性を定義します。
- *minor-version* は、キー サーバ（KS）/KS 間（連携キー サーバ）の関係と GM/GM 間の相互運用性に関する互換性を定義します。
- *mini-version* は、互換性に影響しない機能変更を追跡します。

たとえば、基本バージョン（以前のすべての GET VPN 機能）は 1.0.1 です。また、たとえば GM の削除機能とポリシー交換機能が含まれるバージョンは 1.0.2 である場合、これらの機能は（トリガーされるキー再生成でのこれらの機能の動作導入に関係なく）基本バージョンと完全な後方互換性があることを意味します。

GM はインターネット キー エクスチェンジ（IKE）フェーズ 1 ネゴシエーション（RFC 2408、『*Internet Security Association and Key Management Protocol [ISAKMP]*』で定義されています）の間にベンダー ID ペイロードで KS に GET VPN ソフトウェア バージョンを送信します。KS は、連携 KS 通知（ANN）メッセージのバージョン フィールドで他の連携 KS にソフトウェア バージョンを送信します。連携 KS も、各 GM が使用しているバージョンのリストを同期します。

GM 削除機能とポリシー交換機能はそれぞれ、その機能をサポートしていないグループのデバイスを検出するために KS（またはプライマリ KS）で実行するコマンドを提供しています。

GM の削除

GM の削除とポリシー交換機能がないとき、グループから不要な GM を削除するには、次の手順を実行する必要があります。

1. フェーズ 1 のクレデンシャル（たとえば、事前共有キーまたは 1 つ以上の PKI 証明書）を失効にします。
2. KS のトラフィック暗号キー（TEK）および Key Encryption Key（KEK）データベースをクリアします。
3. 各 GM で TEK および KEK データベースを個別にクリアし、強制的に各 GM を再登録します。

GET VPN グループが数千の GM にサービスを提供しているとき、機能させるとき、3 番目のステップには時間がかかります。また、実稼動ネットワークのグループ全体をクリアすると、ネットワーク中断を引き起こす可能性があります。GET VPN GM 削除機能とポリシー トリガー機能で

は、KS（またはプライマリ KS）で入力したコマンドを使用して新たな一連の TEK および KEK キーを作成し、それらを GM に伝播することによって、このプロセスを自動化します。

他の GET VPN ソフトウェア バージョンとの GM 削除の互換性

GET VPN の GM 削除およびポリシー トリガー機能は、GET VPN ネットワークのすべてのデバイスがこの機能をサポートする GET VPN ソフトウェア バージョンにアップグレードされた後にのみ使用する必要があります。そうしないと、古いソフトウェアを実行しているセカンダリ KS または GM が GM の削除メッセージを無視し、古い SA を使用してトラフィックの暗号化と復号化を続行します。この動作により、ネットワーク トラフィックの中断が発生します。

この機能には、ネットワークのすべてのデバイスが GM の削除をサポートするバージョンを実行しているかどうかを確認するために KS（またはプライマリ KS）で使用するコマンドが用意されています。プライマリ KS が GM の削除をサポートしていないデバイスを含むネットワークの GM を削除しようとすると、警告メッセージが表示されます。詳細については、「GM の削除をサポートするソフトウェア バージョンを GM が実行していることを確認する」セクションを参照してください。

一時的な IPsec SA による GM の削除

GET VPN GM の削除とポリシー トリガー機能には、一時的な IPsec SA により GM の削除をトリガーするために KS（またはプライマリ KS）で使用するコマンドが用意されています。この動作により、すべての GM のキーのライフタイムが短縮され、キーの有効期限が切れる前に再登録します。GM の削除の間、ライフタイムが期限切れになるまで一時的な IPsec SA を使用してトラフィックの暗号化と復号化が継続されるため、ネットワーク中断は発生しません。詳細については、「一時的な IPsec SA による GM の削除」セクションを参照してください。

即時の IPsec SA 削除による GM の削除

GET VPN GM の削除とポリシー トリガー機能では、GM が強制的に古い TEK と KEK を（一時的な SA を使用せず）即座に削除し、再登録するために KS（またはプライマリ KS）で使用できるオプションのキーワードを提供します。ただし、この動作により、データ プレーンに中断が引き起こされる可能性があります。そのため、重大なセキュリティ上の理由がある場合のみこの方式を使用する必要があります。詳細については、「GM の削除と IPSec SA の即座の削除」セクションを参照してください。

ポリシーの交換とキー再生成のトリガー

GET VPN GM 削除およびポリシー トリガー機能では、古い SA を削除し、新しい SA をインストールするための新しいキー再生成トリガー方法を提供します。

キー再生成をトリガーする TEK および KEK ポリシー変更に関する不整合

この機能なしでは、キー再生成をトリガーする TEK および KEK ポリシー変更に関して不整合があります。

- セキュリティ ポリシーの更新中に複数のキー再生成が送信される可能性があります。
- 一部のポリシー変更は（たとえば、トランスフォーム セット、プロファイル、ライフタイム、およびアンチリプレイ）新しい SA を GM にインストールしますが、既存のポリシーからの SA はライフタイムが期限切れになるまでアクティブのままになります。
- 一部のポリシー変更（たとえば、TEK のアクセス コントロール エントリ/アクセス コントロール リスト（ACE/ACL）の変更）は新しい SA を GM にインストールし、即座に有効になります。ただし、古い SA は各 GM のデータベースで維持されます（ライフタイムが期限切れになるまで **show crypto ipsec sa** コマンドを使用して表示できます）。

たとえば、KS が Data Encryption Standard（DES）から Advanced Encryption Standard（AES）にポリシーを変更する場合、GM がこのトリガーされたキー再生成を受け取ると、新しい SA（例：AES）がインストールされ、古い SA（例：DES）のライフタイムは短縮されます。GM は短縮されたライフタイムが期限切れになるまで古い SA を使用してトラフィックの暗号化と復号化を継続します。

次に、短縮されたライフタイムを計算する式を示します。

TEK_SLT = MIN(TEK_RLT, MAX(90s, MIN(5%(TEK_CLT), 3600s)))

値は次のとおりです。

- TEK_SLT は TEK の短縮されたライフタイムです。
- TEK_RLT は TEK の残りのライフタイムです。
- TEK_CLT は TEK の設定されたライフタイムです。

次の表は、キー再生成に関する不整合をまとめたものです。

表 *5*：セキュリティ ポリシー変更後のキー再生成の動作

ポリシーの変更	キー再生成を送信するか	ポリシー変更後のキー再生成の動作
TEK：SA ライフタイム	No	古い SA は、そのライフタイムが期限切れになるまでアクティブのままになります。新しいライフタイムは、次にスケジュールされたキー再生成の後に有効になります。**clear crypto sa** コマンドを入力しても、再度古いライフタイムを使用して再登録され、古い SA がダウンロードされます。
TEK：IPSEC トランスフォーム セット	Yes	古いトランスフォーム セットの SA は、そのライフタイムが期限切れになるまでアクティブのままになります。
TEK：IPSEC プロファイル	Yes	古いプロファイルの SA は、そのライフタイムが期限切れになるまでアクティブのままになります。
TEK：一致する ACL	Yes	発信パケット分類ですぐに ACL が使用されます。ただし、古い SA は SA データベースに残ります（**show crypto ipsec sa** コマンドを使用して表示できます）。
TEK：リプレイ カウンタのイネーブル化	Yes	ただし、カウンタ リプレイがない古い SA は、そのライフタイムが期限切れになるまでアクティブのままになります。
TEK：リプレイ カウンタ値の変更	No	新しいリプレイ カウンタがある SA は、次にスケジュールされたキー再生成時に送信されます。

ポリシーの変更	キー再生成を送信するか	ポリシー変更後のキー再生成の動作
TEK：リプレイ カウンタのディセーブル化	Yes	ただし、カウンタ リプレイがイネーブルになっている古い SA は、そのライフタイムが期限切れになるまでアクティブのままになります。
TEK：TBAR の有効化	Yes	ただし、時間ベースのアンチリプレイ（TBAR）が無効になった古い SA は、そのライフタイムが期限切れになるまでアクティブのままになります。
TEK：TBAR ウィンドウの変更	No	新しい TBAR ウィンドウがある SA は、次にスケジュールされたキー再生成時に送信されます。
TEK：TBAR の無効化	Yes	ただし、TBAR がイネーブルになっている古い SA は、そのライフタイムが期限切れになるまでアクティブのままになります。
TEK：受信専用のイネーブル	Yes	受信専用モードは、キー再生成後ただちにアクティブになります。
TEK：受信専用のディセーブル	Yes	受信専用モードは、キー再生成後ただちに非アクティブになります。
KEK：SA ライフタイムの動作	No	変更は次のキー再生成時に適用されます。
KEK：認証キーの変更	Yes	変更は即時に適用されます。
KEK：暗号アルゴリズムの変更	Yes	変更は即時に適用されます。

この機能では、一貫性を確保することで、これらの問題を解決します。この機能によって、GET VPN ポリシーの変更単独ではキー再生成がトリガーされなくなります。ポリシー（およびグローバルコンフィギュレーションモードの終了）を変更すると、ポリシーが変更され、キー再生成が必要であることを示す syslog メッセージがプライマリ KS に表示されます。この機能には、（実

行コンフィギュレーションの最新のセキュリティ ポリシーに基づく）キー再生成を送信するために KS（またはプライマリ KS）で入力する新しいコマンドが用意されています。

この機能ではまた、古い TEK および KEK を即座に削除し、新しい TEK および KEK をインストールするようにキー再生成を受信する GM に強制する追加のキーワードを新しいコマンドに用意しています。そのため、新しいポリシーは古い SA ポリシーが期限切れになるのを待たずにただちに反映されます。（ただし、すべての GM が同時にキー再生成メッセージを受信しない場合があるため、このキーワードを使用すると、一時的なトラフィックの切断が発生する可能性があります）。

ポリシーの交換およびキー再生成のトリガーの他の GET VPN ソフトウェア バージョンとの互換性

キー再生成のトリガーは、GET VPN ネットワーク内のすべてのデバイスをこの機能をサポートする GET VPN ソフトウェア バージョンにアップグレードしてから使用する必要があります。**crypto gdoi ks** コマンドをまだサポートしていない古いバージョンを実行している GM では、プライマリ KS はソフトウェア バージョン管理機能を使用してこれらのバージョンを検出し、ポリシー交換のための命令を送信せずにキー再生成のトリガーのみ実行します。したがって、GM がキー再生成を受信すると、新しい SA をインストールしますが、古い SA の有効期間は短縮しません。（この動作は以前のキー再生成メソッドと同様であり、ポリシーの交換をサポートしないデバイスの後方互換性が確保されます。）

この機能は、ネットワークのすべてのデバイスがポリシーの交換をサポートするバージョンを実行しているかどうかを確認するために KS（またはプライマリ KS）で使用するコマンドを提供します。詳細については「GM がポリシーの交換をサポートするソフトウェア バージョンを実行していることを確認する」セクションを参照してください。

GET VPN GM 削除およびポリシー トリガーの設定方法

GM の削除をサポートするソフトウェア バージョンを GM が実行していることを確認する

GET VPN の GM 削除およびポリシー トリガー機能は、GET VPN ネットワークのすべてのデバイスがこの機能をサポートする GET VPN ソフトウェア バージョンにアップグレードされた後にのみ使用する必要があります。そうしないと、古いソフトウェアを実行しているセカンダリ KS または GM が GM 削除メッセージを無視して、古い SA を使用するトラフィックの暗号化および復号化を継続します。この動作により、ネットワーク トラフィックの中断が発生します。

ネットワーク内のすべてのデバイスが GM 削除をサポートすることを確認するには、KS（またはプライマリ KS）でこの作業を実行します。

手順の概要

1. **enable**
2. **showcryptogdoifeaturegm-removal**
3. **showcryptogdoifeaturegm-removal|includeNo**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showcryptogdoifeaturegm-removal** 例： `Device# show crypto gdoi feature gm-removal`	GET VPN ネットワーク内の各 KS および GM で実行されている GET VPN ソフトウェアのバージョンを表示し、そのデバイスが GM 削除をサポートしているかどうかを表示します。
ステップ 3	**showcryptogdoifeaturegm-removal|includeNo** 例： `Device# show crypto gdoi feature gm-removal | include No`	（オプション）GM削除をサポートしないデバイスのみ表示します。

一時的な IPsec SA による GM の削除

一時的な IPsec SA の GM の削除をトリガーするには、KS（またはプライマリ KS）でこの作業を実行します。

手順の概要

1. **enable**
2. **clearcryptogdoi** [**group***group-name*] **ksmembers**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clearcryptogdoi** [**group***group-name*] **ksmembers** 例： `Device# clear crypto gdoi ks members`	新しい TEK および KEK キーのセットを作成します。またこのコマンドは、すべての GM に古い TEK および KEK データベースをクリーンアップするための GM 削除メッセージも送信します。

例

KS に次のようにメッセージが表示されます。

```
Device# clear crypto gdoi ks members

% This GM-Removal message will shorten all GMs' key lifetimes and cause them to
re-register before keys expiry.
Are you sure you want to proceed? ? [yes/no]: yes
Sending GM-Removal message to group GET...
```

各 GM が GM 削除メッセージを受信すると、次の syslog メッセージが各 GM に表示されます。

```
*Jan 28 08:37:03.103: %GDOI-4-GM_RECV_DELETE: GM received delete-msg from KS in group GET.

TEKs lifetime are reduced and re-registration will start before SA expiry
```

各 GM は KEK を即時削除し、次のように古い TEK のライフタイムを短縮します。

```
TEK_SLT = MIN(TEK_RLT, MAX(90s, MIN(5%(TEK_CLT), 3600s)))
TEK_SLT: TEK shortened lifetime
TEK_RLT: TEK Remaining LIfeTime
TEK_CLT: TEK Configured LIfeTime
```

また GM は、従来の再登録タイマーに従いジッター（ランダムな遅延）が適用された新しい TEK と KEK を取得するために KS への再登録を開始します。ジッターは、すべての GM が同時に再登録してキー サーバの CPU に過負荷を与えることを防ぎます。KS にインストールされた新しいクレデンシャルに基づいて認証を通す GM だけが新しい TEK と KEK を受信します。

トラフィックはライフタイムが期限切れになるまで一時的な IPsec SA を使用して暗号化と復号化を続けるため、GM 削除によってネットワークの中断が発生することはありません。

セカンダリ KS でこのコマンドを使用しようとすると、次のように拒否されます。

```
Device# clear crypto gdoi ks members

ERROR for group GET: can only execute this command on Primary KS
```

GM の削除と IPSec SA の即時削除

古い TEK と KEK を即時削除して再登録するように GM に強制するには KS（またはプライマリ KS）でこの作業を実行します。

手順の概要

1. **enable**
2. **clearcryptogdoi** [**group***group-name*] **ksmembersnow**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clearcryptogdoi** [**group***group-name*] **ksmembersnow** 例： `Device# clear crypto gdoi ks members now`	新しい TEK および KEK キーのセットを作成します。またこのコマンドは、すべての GM に古い TEK および KEK データベースをクリーンアップするための GM 削除メッセージも送信します。 （注） **now** キーワードの使用により、データ プレーンにネットワーク中断が発生することがあります。セキュリティに関する問題が中断よりも重要である場合にのみ、GM 削除を進めます。

例

KS に次のようにメッセージが表示されます。

```
Device# clear crypto gdoi ks members now

% This GM-Removal immediate message will cleanup all GMs downloaded policies
% This will cause all GMs to re-register.
Are you sure you want to proceed? ? [yes/no]: yes
Sending GM-Removal message to group GET...
```

上記のコマンドの入力後、KS は、各 GM の次のアクションをトリガーするために「remove now」メッセージを各 GM に送信します。

1. ダウンロードされた TEK および KEK ならびにそのポリシーがすぐにクリーンアップされ、（明示的にフェールクローズ モードが設定されていない限り）フェールオープン モードに戻ります。
2. 設定されている TEK ライフタイムの 2 パーセント以内のランダムに選択された期間でタイマーを設定します。

3 ステップ 2 のタイマーの期限が切れると、GM は新しい TEK および KEK をダウンロードするために KS への再登録を開始します。

各 GM では、GM がランダムな期間内に再登録されることを示すために次の syslog メッセージが表示されます。

```
*Jan 28 08:27:05.627: %GDOI-4-GM_RECV_DELETE_IMMEDIATE: GM receive REMOVAL-NOW in group
GET to cleanup downloaded policy now. Re-registration will start in a randomly chosen
period of 34 sec
```

GM 削除をサポートしていないデバイスを含むネットワークの GM を削除しようとすると、警告メッセージが表示されます。

```
Device# clear crypto gdoi ks members now

% This GM-Removal immediate message will cleanup all GMs downloaded policies
% This will cause all GMs to re-register.
Are you sure you want to proceed? ? [yes/no]: yes
WARNING for group GET: some devices cannot support GM-REMOVAL and can cause network
disruption. Please check 'show crypto gdoi feature'.
Are you sure you want to proceed ? [yes/no]: no
```

GM がポリシーの交換をサポートするソフトウェア バージョンを実行していることを確認する

ネットワーク内のすべてのデバイスがポリシーの交換をサポートするかどうかを確認するには、KS（またはプライマリ KS）でこの作業を実行します。

手順の概要

1. **enable**
2. **showcryptogdoifeaturepolicy-replace**
3. **showcryptogdoifeaturepolicy-replace|includeNo**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showcryptogdoifeaturepolicy-replace** 例： `Device# show crypto gdoi feature policy-replace`	GET VPN ネットワーク内の各 KS および GM で実行されている GET VPN ソフトウェアのバージョンを表示し、そのデバイスがポリシーの交換をサポートしているかどうかを表示します。

	コマンドまたはアクション	目的
ステップ 3	**showcryptogdoifeaturepolicy-replace|includeNo** 例： `Device# show crypto gdoi feature policy-replace | include No`	（オプション）ポリシーの交換をサポートしないデバイスのみ検索します。これらのデバイスでは、プライマリ KS はポリシー交換に関する手順なしでトリガーされるキー再生成のみを送信します。したがって、GM がキー再生成を受信すると、新しいSAをインストールしますが、古いSAの有効期間は短縮しません。この動作は既存のキー再生成メソッドと同じであり後方互換性があります。

キー再生成のトリガー

KS（またはプライマリ KS）でセキュリティ ポリシーを変更し（たとえば、DES から AES）、グローバルコンフィギュレーションモードを終了すると、ポリシーが変更され、キー再生成が必要であることを示す syslog メッセージが KS に表示されます。実行コンフィギュレーションの最新のポリシーに基づくキー再生成を送信するために、次のようにキー再生成をトリガーするコマンドを入力します。

キー再生成をトリガーするには KS（プライマリ KS）でこの作業を実行します。

手順の概要

1. **enable**
2. **cryptogdoiks** [**group***group-name*] **rekey** [**replace-now**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**cryptogdoiks** [**group***group-name*] **rekey** [**replace-now**] 例： `Device# crypto gdoi ks group mygroup rekey`	すべての GM のキー再生成をトリガーします。 オプションの **replace-now** キーワードは、各 GM の古い TEK および KEK を即時に置き換え、SA が期限切れになる前に新しいポリシーを有効にします。 （注） **replace-now** キーワードを使用すると、一時的なトラフィックの不連続を引き起こすことがあります。

例

KS に次のようにメッセージが表示されます。

```
Device# crypto gdoi ks rekey
Device#
*Jan 28 09:17:44.363: %GDOI-5-KS_SEND_UNICAST_REKEY: Sending Unicast Rekey with
policy-replace for group GET from address 10.0.8.1 with seq # 2
```

ポリシーの変更後、各 GM がこのトリガーされたキー再生成を受信すると、新しい SA（たとえば、AES 用）をインストールして、古い SA（たとえば、DES 用）のライフタイムを短縮します。各 GM はこの短縮されたライフタイムが期限切れになるまで古い SA を使用してトラフィックの暗号化および復号化を続けます。

セカンダリ KS のキー再生成をトリガーしようとすると、次のようにコマンドが拒否されます。

```
Device# crypto gdoi ks rekey
ERROR for group GET: This command must be executed on Pri-KS
```

GET VPN GM の削除とポリシーのトリガーの設定例

例：GET VPN ネットワークからの GM の削除

GM の削除をサポートするソフトウェア バージョンを GM が実行していることを確認する

次の例は、ネットワーク内のすべてのデバイスが GM 削除機能をサポートしているかどうかを確認するために KS（またはプライマリ KS）で GET VPN ソフトウェア バージョン管理コマンドを使用する方法を示します。

```
Device# show crypto gdoi feature gm-removal

Group Name: GET
 Key Server ID       Version   Feature Supported
    10.0.8.1         1.0.2          Yes
    10.0.9.1         1.0.2          Yes
    10.0.10.1        1.0.2          Yes
    10.0.11.1        1.0.2          Yes
 Group Member ID     Version   Feature Supported
    10.0.0.2         1.0.2          Yes
    10.0.0.3         1.0.1          No
```

次の例は、GM の削除をサポートしていないデバイスのみを検索する方法を示します。

```
Device# show crypto gdoi feature gm-removal | include No

       10.0.0.3          1.0.1          No
```

上記の例では、IP アドレス 10.0.0.3 の GM は（GM の削除をサポートしない）古いソフトウェア バージョン 1.0.1 を実行中であり、アップグレードする必要があることを示しています。

一時的な IPsec SA による GM の削除

次の例では、一時的な IPsec SA を使用する GM の削除をトリガーする方法を示します。KS（またはプライマリ KS）でこのコマンドを使用します。

```
Device# clear crypto gdoi ks members
```

```
% This GM-Removal message will shorten all GMs' key lifetimes and cause them to
re-register before keys expiry.
Are you sure you want to proceed? ? [yes/no]: yes
Sending GM-Removal message to group GET...
```

GM の削除と IPSec SA の即時削除

次の例は、古い TEK と KEK を即座に削除して再登録するために GM を強制適用する方法を示しています。KS（またはプライマリ KS）でこのコマンドを使用します。

```
Device# clear crypto gdoi ks members now

% This GM-Removal immediate message will cleanup all GMs downloaded policies
% This will cause all GMs to re-register.
Are you sure you want to proceed? ? [yes/no]: yes
Sending GM-Removal message to group GET...
```

例：グループ メンバーのキー再生成のトリガー

GM がキー再生成のトリガーをサポートするソフトウェア バージョンを実行していることを確認する

次の例は、GET VPN ネットワークのデバイスのソフトウェアのバージョンを表示し、またポリシー変更後のキー再生成のトリガーをサポートするかどうかを表示するために、KS（またはプライマリ KS）で GET VPN ソフトウェア バージョン管理コマンドを使用する方法を示します。

```
Device# show crypto gdoi feature policy-replace

Key Server ID       Version  Feature Supported
  10.0.8.1         1.0.2          Yes
  10.0.9.1         1.0.2          Yes
  10.0.10.1        1.0.2          Yes
  10.0.11.1        1.0.2          Yes
 Group Member ID     Version  Feature Supported
  5.0.0.2          1.0.2          Yes
  9.0.0.2          1.0.1          No
```

次の例は、ポリシー交換後のキー再生成のトリガーをサポートしていないデバイスのみを検索する方法を示します。

```
Device# show crypto gdoi feature policy-replace  | include No

       9.0.0.2          1.0.1          No
```

これらのデバイスでは、プライマリ KS はポリシー交換に関する手順なしでトリガーされるキー再生成のみを送信します。したがって、GMがキー再生成を受信すると、新しいSAをインストールしますが、古い SA の有効期間は短縮しません。

キー再生成のトリガー

次の例では、ポリシー変更の実行後にキー再生成をトリガーする方法を示します。この例では、**profile gdoi-p2** コマンドで IPSec ポリシーの変更（たとえば、DES から AES）が発生します。

```
Device# configure terminal
Device(config)# crypto gdoi group GET
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# sa ipsec 1
Device(gdoi-sa-ipsec)# no profile gdoi-p
Device(gdoi-sa-ipsec)# profile gdoi-p2
Device(gdoi-sa-ipsec)# end
Device#

*Jan 28 09:15:15.527: %SYS-5-CONFIG_I: Configured from console by console
*Jan 28 09:15:15.527: %GDOI-5-POLICY_CHANGE: GDOI group GET policy has changed. Use
'crypto gdoi ks rekey' to send a rekey, or the changes will be send in the next scheduled
rekey
Device# crypto gdoi ks rekey
Device#
*Jan 28 09:17:44.363: %GDOI-5-KS_SEND_UNICAST_REKEY: Sending Unicast Rekey with
policy-replace for group GET from address 10.0.8.1 with seq # 2
```

次の例では、セカンダリ KS のキー再生成をトリガーしようとすると表示されるエラー メッセージを示します。

```
Device# crypto gdoi ks rekey

ERROR for group GET: This command must be executed on Pri-KS
```

（注） 時間ベースのアンチリプレイ（TBAR）が設定されると、キーサーバは2時間（7200秒）ごとに定期的にキー再生成をグループ メンバーに送信します。次の例では、有効期間が 8 時間（28800 秒）に設定されていますが、キー再生成タイマーは 2 時間に設定されています。

```
Device(config)# crypto ipsec profile atm-profile
Device(ipsec-profile)# set security-association lifetime seconds 28800
!
Device(ipsec-profile)# exit
Device(config)# crypto gdoi group ATM-DSL
Device(config-gdoi-group)# server local
Device(gdoi-sa-ipsec)# sa ipsec 1
!
Device(gdoi-sa-ipsec)# replay time window-size 100
```

show crypto gdoi gm replay および **show crypto gdoi ks replay** コマンドは、TBAR の情報を表示します。

GETVPNGMの削除とポリシーのトリガーのその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command References*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

GET VPN GM の削除とポリシーのトリガーの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *6*：***GET VPN GM*** の削除とポリシーのトリガーの機能情報

機能名	リリース	機能情報
GET VPN GM の削除とポリシー トリガー	Cisco IOS XE Release 3.8S	この機能は、GET VPN ネットワークから不要な GM を効率的に削除するコマンド、新しい SA をインストールして古い SA を削除するためにキー再生成をトリガーするコマンド、およびネットワーク デバイスがこれらの機能をサポートする GET VPN ソフトウェアのバージョンを実行しているかどうかを表示するコマンドを提供します。 次のコマンドが導入または変更されました：**clear crypto gdoi**、**crypto gdoi ks**、**show crypto gdoi**。

第 4 章

GET VPN の GDOI MIB サポート

暗号化された既存のMIBはインターネットキーエクスチェンジ（IKE）およびIP Security（IPsec）MIB であり、Group Domain of Interpretation（GDOI）には不十分です。GET VPN の GDOI MIB サポート機能では、RFC 6407、『The Group Domain of Interpretation』に MIB のサポートが追加されます。GDOI MIB IETF 標準規格に関連するオブジェクトのみがサポートされます。GDOI MIB .my ファイルは SNMP 管理ステーションにインポートして解析することにより、テーブル オブジェクトと階層情報を取得することができます。

GDOI MIB は、（トラップと呼ばれていた）オブジェクトおよび通知で構成されます。これには、GDOIグループ、グループメンバー（GM）とキーサーバ（KS）のピア、および作成またはダウンロードされるポリシーに関する情報が含まれます。「get」操作のみが GDOI でサポートされます。

GET VPN の GDOI MIB のサポートを設定するには、「GET VPN の GDOI MIB サポートの設定」セクションを参照してください。

- 機能情報の確認，133 ページ
- GET VPN の GDOI MIB サポートに関する情報，134 ページ
- GET VPN の GDOI MIB サポートの設定方法，140 ページ
- GET VPN 用の GDOI MIB サポートの設定例，145 ページ
- GET VPN 用の GDOI MIB サポートのその他の参考資料，146 ページ
- GET VPN 用の GDOI MIB サポートの機能情報，147 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、『Bug Search Tool』およびご使用のプラットフォームおよびソフトウェアリリースのリリースノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

GET VPN の GDOI MIB サポートに関する情報

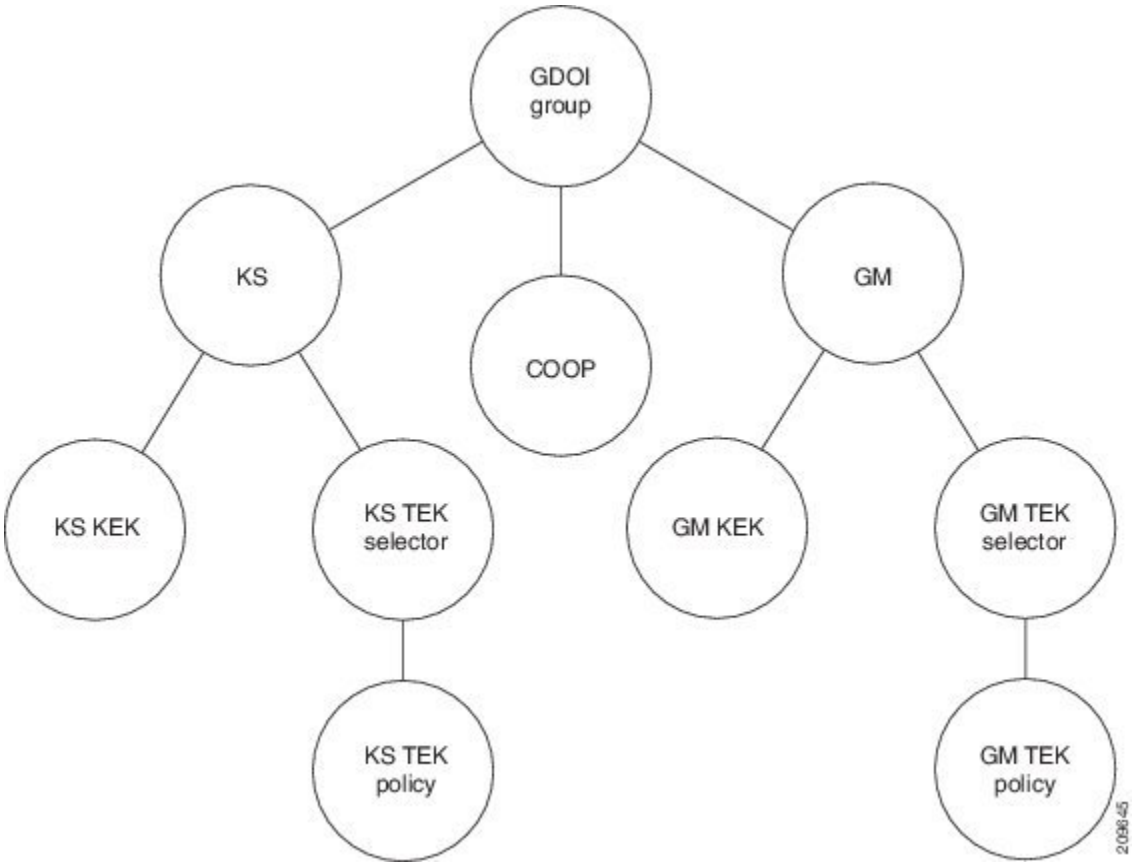
他の GET VPN ソフトウェア バージョンとの GDOI MIB の互換性

GET VPN の GDOI MIB サポート機能には、ネットワークのすべてのデバイスが GDOI MIB をサポートするバージョンを実行しているかどうかを確認するために KS（プライマリ KS）で使用するコマンドが用意されています。詳細については、「GDOI MIB をサポートするソフトウェア バージョンを GM が実行していることを確認する」セクションを参照してください。

GDOI MIB テーブル階層

GDOI MIB オブジェクトは次の GDOI MIB テーブルで構成されます。次に、テーブル間の関係（階層）を示します。

図 *14*：*GDOI MIB* テーブル階層



GDOI MIB テーブル オブジェクト

次は、MIB テーブル オブジェクトのリストです（グループごとにリスト）。

グループ テーブル オブジェクト：

- Group ID type：グループ ID が IP アドレス、グループ番号、ホスト名などのいずれであるかを指定します。
- Group ID length：グループ ID 値のオクテット数。
- Group ID value：グループ番号、IP アドレス、またはホスト名。
- Group name：文字列の値。

- Group member count：このグループに登録済みの KS 数を指定します。
- Group active peer KS count：このグループに対するアクティブな KS 数を指定します。
- Group last rekey retransmits：最後のキー再生成操作の一部として送信されたキー再生成メッセージと再送信メッセージの累積数を指定します。
- Group last rekey time taken：最後のキー再生成操作の完了に KS が費やした時間を指定します。

KS テーブル オブジェクト：

- KS ID type
- KS ID length
- KS ID value
- Active KEK：キー再生成メッセージを暗号化するために KS によって現在使用されている Key Encryption Key（KEK）の SPI。
- Last rekey sequence number：グループに KS から送信された最後のキー再生成番号。
- KS Role：プライマリまたはセカンダリ。
- Number of registered GMs：この KS に登録された GM の数。

COOP テーブル オブジェクト：

- COOP peer ID type
- COOP peer ID length
- COOP peer ID value
- COOP peer ID role：プライマリまたはセカンダリ
- COOP peer status：アライブ、デッド、または不明
- Number of registered GMs：この COOP ピアに登録された GM の数

GM テーブル：

- GM ID type
- GM ID length
- GM ID value
- Registered KS ID type：GM が登録されている KS の ID タイプ。
- Registered KS ID length
- Registered KS ID value
- Active KEK：キー再生成メッセージの復号化に GM が現在使用している KEK の SPI。
- Last rekey seq number：GM が受信した最後のキー再生成番号。
- Count of active TEKs：データプレーン トラフィックの暗号化/復号化/認証のために GM によって使用されるアクティブな TEK の数。

KS KEK テーブル：

- KEK index
- KEK SPI
- KEK source ID information：送信元 ID のタイプ、ID の長さ、および ID の値。
- KEK source ID port：送信元 ID に関連付けられたポート。
- KEK destination ID information：宛先 ID のタイプ、ID の長さ、および ID の値。
- KEK destination ID port：宛先 ID に関連付けられたポート。
- IP protocol ID：UDP または TCP。
- キー管理アルゴリズム（未使用）。
- 暗号化アルゴリズムとキーの長さ（ビット）
- SIG ペイロード ハッシュ アルゴリズム、SIG ペイロード署名アルゴリズム、および SIG ペイロード キーの長さ（ビット）。
- ハッシュ アルゴリズム（IPsec MIB から再利用されます）
- Diffie-Hellman グループ
- KEK original lifetime (seconds)：KEK が有効である最長時間。
- KEK remaining lifetime (seconds)

KS TEK セレクタ テーブル（KS で GDOI グループ設定の IPsec SA の一部として設定された ACL に対応）：

- TEK selector index：トラフィック暗号キー（TEK）の整数のインデックス。
- TEK source ID information：送信元 ID のタイプ、ID の長さ、および ID の値。
- TEK source ID port：送信元 ID に関連付けられたポート。
- TEK destination ID information：宛先 ID のタイプ、ID の長さ、および ID の値。
- TEK destination ID port：宛先 ID に関連付けられたポート。
- TEK Security protocol：SA TEK ペイロードの GDOI_PROTO_IPSEC_ESP プロトコル ID 値（RFC 6407 を参照）。

KS TEK ポリシー テーブル：

- TEK policy index：整数のインデックス。
- TEK SPI：4 つのオクテット
- Encapsulation mode：トンネルまたは転送。
- 暗号化アルゴリズムとキーの長さ（ビット）
- 整合性および認証アルゴリズムとキーの長さ（ビット）

- TBAR window size (seconds)
- TEK original lifetime (seconds)：TEK が有効である最長時間。
- TEK remaining lifetime (seconds)
- TEK Status：着信、発信、または不使用。

GM KEK テーブル：

- KEK index：整数のインデックス。
- KEK SPI
- KEK source ID information：送信元 ID のタイプ、ID の長さ、および ID の値。
- KEK source ID port：送信元 ID に関連付けられたポート。
- KEK destination ID information：宛先 ID のタイプ、ID の長さ、および ID の値。
- KEK destination ID port：宛先 ID に関連付けられたポート。
- IP protocol ID：UDP または TCP。
- Key Management アルゴリズム（未使用）
- 暗号化アルゴリズムとキーの長さ（ビット）
- SIG ペイロード ハッシュ アルゴリズム、SIG ペイロード署名アルゴリズム、および SIG ペイロード キーの長さ（ビット）
- Hash algorithm
- Diffie-Hellman グループ
- KEK original lifetime (seconds)：KEK が有効である最長時間。
- KEK remaining lifetime (seconds)

GM TEK セレクタ テーブル（KS から TEK ポリシーの一部として GM にダウンロードされる ACL に対応）：

- TEK selector index：整数のインデックス。
- TEK source ID information：送信元 ID のタイプ、ID の長さ、および ID の値。
- TEK source ID port：送信元 ID に関連付けられたポート。
- TEK destination ID information：宛先 ID のタイプ、ID の長さ、および ID の値。
- TEK destination ID port：宛先 ID に関連付けられたポート。
- TEK Security protocol：SA TEK ペイロードの GDOI_PROTO_IPSEC_ESP プロトコル ID 値（RFC 6407 を参照）。

GM TEK ポリシー テーブル：

- TEK policy index：整数のインデックス。

- TEK SPI：4 つのオクテット。
- Encapsulation mode：トンネルまたは転送。
- 暗号化アルゴリズムとキーの長さ（ビット）
- 整合性および認証アルゴリズムとキーの長さ（ビット）
- TBAR window size (seconds)
- TEK original lifetime (seconds)：TEK が有効である最長時間。
- TEK remaining lifetime (seconds)
- TEK Status：着信、発信、または不使用。

GDOI MIB 通知

GDOI MIB は次の表の Simple Network Management Protocol（SNMP）通知をサポートしています。GDOI MIB には、KS によって生成された通知と各 GM によって生成された通知の 2 種類の通知があります。任意の組み合わせの通知（またはすべての通知）を有効にできます。

表 *7*：***GDOI MIB*** にサポートされる ***SNMP*** 通知

通知	説明
KS New Registration	KS が GM から最初に登録要求を受信した。
KS Registration Complete	GM が KS への登録を完了した。
KS Rekey Pushed	キー再生成メッセージが KS によって送信された。
KS No RSA Keys	RSA キーが見つからないために KS からエラー通知が受信された。
GM Register	GM が KS に最初の登録要求を送信した。
GM Registration Complete	GM が KS への登録を完了した。
GM Re-Register	GM が KS への登録プロセスを開始した。
GM Rekey Received	キー再生成メッセージが GM で受信された。
GM Incomplete Config	GMが設定の不足によるエラー通知を送信した。
GM Rekey Failure	GM がキー再生成の処理とインストールができないため、エラー通知を送信した。

通知	説明
KS Role Change	KS がプライマリとセカンダリ ロールを切り替えた。
KS GM Deleted	GM が KS から削除されると生成されます。
KS Peer Reachable	到達不能な COOP ピアが到達可能になると KS によって生成されます。
KS Peer Unreachable	到達可能な COOP ピアが到達不能になると KS によって生成されます。

詳細については、「GDOI MIB 通知の有効化」セクションを参照してください。

GDOI MIB の制限

GDOI MIB には RFC 6407 にリストされているオブジェクトのみが含まれ、GDOI のシスコ実装に固有の機能のためのオブェクトは含まれません。リストでは次の演算を使用します。

- 連携キー サーバ
- GM ACL
- 受信専用 SA
- Fail-Close またはフェール オープン
- 暗号マップ オブジェクト
- 他の Cisco GET VPN 固有の機能

GET VPN の GDOI MIB サポートの設定方法

GDOI MIB をサポートするソフトウェア バージョンを GM が実行していることを確認する

GET VPN ネットワーク内のすべてのデバイスが GDOI MIB をサポートすることを確認するには、KS（またはプライマリ KS）でこの作業を実行します。

手順の概要

1. **enable**
2. **showcryptogdoifeaturegdoi-mib**
3. **showcryptogdoifeaturegdoi-mib|includeNo**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showcryptogdoifeaturegdoi-mib** 例： `Device# show crypto gdoi feature gdoi-mib`	ネットワーク内の各 KS および GM で実行されている GET VPN ソフトウェアのバージョンを表示し、そのデバイスが GDOI MIB をサポートしているかどうかを表示します。
ステップ 3	**showcryptogdoifeaturegdoi-mib|includeNo** 例： `Device# show crypto gdoi feature gdoi-mib | include No`	（オプション）GDOI MIB をサポートしないデバイスのみ検索します。

SNMP コミュニティのアクセス コントロールの作成

SNMP へのアクセスを許可するために、KS または GM 上の SNMP マネージャと SNMP エージェント間の関係を定義する SNMP コミュニティ アクセス文字列を指定します。このコミュニティ アクセス文字列は、デバイス上のエージェントへのアクセスを制御するパスワードのように機能します。

コミュニティ アクセス文字列を指定するにはこの作業を行います。

手順の概要

1. **enable**
2. **configureterminal**
3. **snmp-servercommunity***community-string* [**view***view-name*] [**ro** | **rw**] [**ipv6***nacl*] [*access-list-number* | *extended-access-list-number* | *access-list-name*]
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**snmp-servercommunity***community-string* [**view***view-name*] [**ro** | **rw**] [**ipv6***nacl*] [*access-list-number* | *extended-access-list-number* | *access-list-name*] 例： `Device(config)# snmp-server community mycommunity`	コミュニティ アクセス文字列を指定します。
ステップ 4	**end** 例： `Device(config)# end`	グローバルコンフィギュレーションモードを終了し、設定を保存して、特権 EXEC モードに戻ります。

コミュニティ アクセス文字列の指定に関する詳細については、『*SNMP Configuration Guide*』の「Configuring SNMP Support」モジュールを参照してください。**snmp-servercommunity** コマンドに関する詳細（構文と使用法に関するガイドラインを含む）については、『Cisco IOS SNMP Support Command Reference』を参照してください。

SNMP マネージャとの通信の有効化

KS の SNMP エージェントまたは GM と SNMP マネージャ間の通信を有効にするには、このタスクを実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **snmp-serverhost** {*hostname* | *ip-address*} **version** {**1** | **2c** | **3**} *community-string*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**snmp-serverhost** {*hostname* | *ip-address*} **version** {**1** | **2c** | **3**} *community-string* 例： `Device(config)# snmp-server host 209.165.200.225 version 2c mycommunity`	ホストが SNMP 通知を受信するように指定します。 • 2c は通常 SNMP バージョンとして使用されます。
ステップ 4	**end** 例： `Device(config)# end`	グローバルコンフィギュレーションモードを終了し、設定を保存して、特権 EXEC モードに戻ります。

SNMP マネージャとの通信を有効にする方法についての詳細は、『*SNMP Configuration Guide*』の「Configuring SNMP Support」モジュールを参照してください。**snmp-serverhost** コマンドに関する詳細（構文と使用法に関するガイドラインを含む）については、『Cisco IOS SNMP Support Command Reference』を参照してください。

GDOI MIB 通知の有効化

KS または GM の GDOI MIB 通知を有効にするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **snmp-serverenabletrapsgdoi** [*notification-type*]
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-serverenabletrapsgdoi** [*notification-type*] 例： `Device(config)# snmp-server enable traps gdoi gm-registration-complete gm-rekey-rcvd ks-new-registration ks-reg-complete`	有効にする特定の SNMP 通知を指定します。任意の順序で次の種類を組み合わせて指定できます。次のキーワードなしでコマンドを入力すると、すべての GDOI MIB 通知が有効になります。 • **gm-incomplete-cfg**：設定が見つからないため GM がエラー通知を送信しました。 • **gm-re-register**：GM が KS で登録プロセスを開始しました。 • **gm-registration-complete**：GM が KS への登録を完了しました。 • **gm-rekey-fail**：キー再生成を正常に処理およびインストールできないため、GM がエラー通知を送信しました。 • **gm-rekey-rcvd**：GM がキー再生成メッセージを受信しました。 • **gm-start-registration**：GM が最初の登録要求を KS に送信しました。 • **ks-new-registration**：KS が最初の登録要求を GM から受信しました。 • **ks-no-rsa-keys**：RSA キーが見つからないため KS からのエラー通知を受信しました。 • **ks-reg-complete**：GM が KS への登録を完了しました。 • **ks-rekey-pushed**：KS からキー再生成メッセージが送信されました。 • **ks-gm-deleted**：GM が KS によって削除されます。 • **ks-peer-reachable**：到達不能な COOP ピアが到達可能になります。

	コマンドまたはアクション	目的
		• **ks-peer-unreachable**：到達可能な COOP ピアが到達不能になります。 • **ks-role-change**：KS の役割がプライマリからセカンダリ（またはその逆）に変更されます。
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、設定を保存して、特権 EXEC モードに戻ります。

GET VPN 用の GDOI MIB サポートの設定例

例：GDOI MIB をサポートするソフトウェア バージョンを GM が実行していることを確認する

次の例は、ネットワーク内のすべてのデバイスが GDOI MIB をサポートしているかどうかを確認するために KS（またはプライマリ KS）で GET VPN ソフトウェア バージョン管理コマンドを使用する方法を示します。

```
Device# show crypto gdoi feature gdoi-mib

Group Name: GET
 Key Server ID       Version   Feature Supported
    10.0.8.1         1.0.2          Yes
    10.0.9.1         1.0.2          Yes
    10.0.10.1        1.0.2          Yes
    10.0.11.1        1.0.2          Yes
 Group Member ID     Version   Feature Supported
    10.0.11.2          1.0.2          Yes
    10.0.11.3          1.0.1          No
```

次の例は、GDOI MIB をサポートしていないデバイスのみを検索する方法を示します。

```
Device# show crypto gdoi feature gdoi-mib | include No

       10.0.11.3          1.0.1          No
```

例：SNMP コミュニティのアクセス コントロールの作成

次の例では、SNMP へのアクセスを許可するために、KS または GM 上の SNMP マネージャと SNMP エージェント間の関係を定義するために mycommunity という名前の SNMP コミュニティ文字列を指定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# snmp-server community mycommunity
Device(config)# end
```

例：SNMP マネージャとの通信の有効化

次に、SNMP マネージャとの通信を有効化する例を示します。この例では、すでに作成されている mycommunity という名前のコミュニティ文字列を使用します。

```
Device> enable
Device# configure terminal
Device(config)# snmp-server host 209.165.200.225 version 2c mycommunity
Device(config)# end
```

例：GDOI MIB 通知の有効化

次に、GDOI MIB 通知を有効化する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# snmp-server enable traps gdoi gm-registration-complete gm-rekey-rcvd
ks-new-registration ks-reg-complete
Device(config)# end
```

GET VPN 用の GDOI MIB サポートのその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command References*』

関連項目	マニュアル タイトル
SNMP の設定	• 『SNMP Configuration Guide, Cisco IOS Release 15.2M&T』の「Configuring SNMP Support」モジュール • 『Cisco IOS SNMP Support Command Reference』

MIB

MIB	MIB のリンク
CISCO-GDOI-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

GET VPN 用の GDOI MIB サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *8*：*GET VPN* 用の *GDOI MIB* サポートの機能情報

機能名	リリース	機能情報
GET VPN の GDOI MIB サポート	Cisco IOS XE Release 3.8S	この機能は、IETF RFC 6407『The Group Domain of Interpretation』用の MIB サポートを追加します。この機能は、GDOI MIB の IETF 標準に関連したオブジェクトのみをサポートします。またこの機能は、ネットワーク上のデバイスが GDOI MIB をサポートする GET VPN ソフトウェアのバージョンを実行しているかどうかを表示するコマンドも提供します。 GDOI MIB は、GDOI グループ、GM と KS ピア、および作成またはダウンロードされたポリシーに関する情報が含まれるオブジェクトと通知から構成されます。 次のコマンドが導入されました：**snmp-server enable traps gdoi**。
XE 3.16 GETVPN GDOI/COOP MIBS	Cisco IOS XE リリース 3.16S	XE 3.16 GETVPN GDOI/COOP MIBS 機能では、キー サーバ パラメータ用の追加の SNMP MIB オブジェクトとキー サーバ イベント用のトラップを使用して既存の CISCO-GDOI-MIB を強化します。 次のコマンドが変更されました：**snmp-server enable traps gdoi**。

第 5 章

GET VPN の復元力

GET VPN の復元力機能では、Cisco Group Encrypted Transport（GET）VPN の復元力を改善し、エラーが発生したときのデータ トラフィックの中断を防止したり最小化したりします。

- 機能情報の確認，149 ページ
- GET VPN の復元力の前提条件，150 ページ
- GET VPN の復元力の制約事項，150 ページ
- GET VPN の復元力に関する情報，150 ページ
- GET VPN の復元力の設定方法，152 ページ
- GET VPN 復元力の設定例，158 ページ
- GET VPN の復元力のその他の参考資料，159 ページ
- GET VPN の復元力の機能情報，161 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、『Bug Search Tool』およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

GET VPN の復元力の前提条件

この機能を有効にするすべてのキーサーバ（KS）およびグループメンバー（GM）で、GET VPN ソフトウェア バージョン 1.0.4 以降を実行している必要があります。この機能は、GET VPN ネットワーク内のすべてのデバイスをこの機能をサポートする GET VPN ソフトウェア バージョンにアップグレードしてから使用する必要があります。この機能は、ネットワークのすべてのデバイスがこの機能をサポートするバージョンを実行しているかどうかを確認するためにKS（またはプライマリ KS）で使用するコマンドを提供します。詳細については「*GM* が長い *SA* ライフタイムをサポートするソフトウェア バージョンを実行していることを確認する」セクションを参照してください。

GET VPN の復元力の制約事項

- すべてキー サーバ（KS）およびグループ メンバー（GM）は、長い SA ライフタイム向けにアップグレードする必要があります。

GET VPN の復元力に関する情報

長い SA ライフタイム

長いセキュリティ アソシエーション（SA）ライフタイム機能では、Key Encryption Key（KEK）およびトラフィック暗号キー（TEK）の最大ライフタイムを 24 時間から 30 日に延長します。この機能により、スケジュールされた最後のキー再生成時に確認応答に応答しないグループ メンバー（GM）に対して定期的なリマインダ キー再生成を送信し続けるようにキー サーバ（KS）を設定することもできます。

定期的なリマインダ キー再生成と長いSAライフタイムを組み合わせて使用することにより、キーがロールオーバーする前にスケジュールされたキー再生成に失敗した場合、KSが効果的にGMを同期することができます。

（注） 24 時間より長いライフタイムでは、暗号化アルゴリズムを、128 ビット以上の AES キーを使用する Advanced Encryption Standard-Cipher Block Chaining（AES-CBC）または Advanced Encryption Standard-Galois/Counter Mode（AES-GCM）にする必要があります。

長い SA ライフタイム機能は GETVPN スイート B 機能とともに使用すると、GCM-AES と GMAC-AES でカプセル化されたパケットのグループでトラフィック暗号キー（TEK）ポリシーがトランスフォームされるときに AES-GSM および Galois Message Authentication Code-Advanced Encryption Standard（GMAC-AES）を使用できます。

長い SA ライフタイムへの移行

長い SA ライフタイム機能（1 日以上）に移行するときには、次のルールが適用されます。

- 長い SA ライフタイムが暗号 IPsec プロファイルに設定されているとき、GETVPN は非 Group Domain of Interpretation（GDOI）グループに対して IPsec プロファイルを使用しないように警告メッセージを表示します。
- グループ メンバーが短い SA ライフタイムでキー サーバに登録され、キー サーバがポリシーを長い SA ライフタイムに変更する場合、GETVPN は **crypto gdoi ks rekey** コマンドを設定してポリシー変更を開始するときにすべての GM のソフトウェア バージョンをチェックします。KS に登録されている GM が長い SA ライフタイムをサポートしていない場合、すべての GM がアップグレードされるまでポリシーの変更を推奨しないというメッセージが表示されます。
- 長い SA 機能が KS で有効になると、この機能をサポートしていない古い Cisco IOS リリースを実行している GM からの登録がブロックされます。

クロック スキューの軽減

セキュリティ アソシエーション（SA）のライフタイムが長いとき、グループ メンバー（GM）は長期間、キー サーバから更新を受信しないことがあります。これにより、グループ メンバーは Key Encryption Key（KEK）ライフタイム、トラフィック暗号キー（TEK）ライフタイム、および時間ベースアンチリプレイ（TBAR）疑似時間の間クロック スキューを経験することがあります。更新のキー再生成と新しい発信 IPsec SA へのロールオーバーによって GM はクロック スキューの問題を軽減することができます。

更新のキー再生成

トラフィック暗号キー（TEK）のライフタイムが 2 日以上の期間に設定され、時間ベースのアンチリプレイ（TBAR）が無効である場合、キー サーバは 24 時間ごとに更新のキー再生成を送信し、すべてのグループ メンバー（GM）の Key Encryption Key（KEK）ライフタイム、TEK ライフタイム、および TBAR 疑似時間を更新します。簡単に言うと、更新のキー再生成は、最後のユニキャスト確認応答（ACK）の受信状態に関係ない、すべての GM への現在の KEK ポリシー、TEK ポリシー、および TBAR 疑似時間（有効な場合）の再送信です。TBAR が有効な場合、更新のキー再生成は疑似時間を同期するために 2 時間ごとに送信され、追加の更新のキー再生成は必要ありません。

新しい発信 IPsec SA へのロールオーバー

長い SA ライフタイム（1 日以上）が設定されている場合、トラフィック暗号キー（TEK）の残りのライフタイムが、下限が 30 秒のライフタイムに設定された古い TEK の 1 % に達し、古い TEK の残りのライフタイムの 30 秒でないとき、ロールオーバーが発生します。これにより、（他の GM が古い TEK を削除してから）1 つの GM から新しい TEK 遅延にロールオーバーされるトラフィックが破棄されるまで、グループ メンバー（GM）間のより大きなクロック スキューが可能になります。これによって、長期間 GM が「オフライン」（KS からの切断）になり、クロック スキューを軽減するための更新のキー再生成を受信できない問題が緩和されます。

定期的なリマインダ同期キー再生成

キー サーバ（KS）の定期的なリマインダ同期キー再生成機能を使用すると、スケジュールされている直前のキー再生成時に確認応答（ACK）に応答しないグループ メンバー（GM）に対して定期的なリマインダ キー再生成を送信できます。長い SA ライフタイム機能とこの機能の組み合わせは、キーのロールオーバーの前にスケジュールされたキー再生成に失敗した GM と KS が同期するために有効です。KS グループ設定で、キー再生成の再送信を設定するときの **rekey retransmit** コマンドに新しいキーワード **periodic** が追加されています。

キー再生成の再送信と同様に、定期的な再送信はそれぞれシーケンス番号を増加させます。スケジュールされた 3 回のキー再生成（再送信ではない）で GM が ACK を送信しないと、GM は KS のデータベースから削除されます。

事前配置されたキー再生成

長い SA ライフタイム（1 日以上）が設定されているとき、事前配置されたキー再生成機能を使用すると、キー サーバ（KS）は SA ライフタイムの半分の期間より先にキー再生成を送信できます。キー再生成の送信の通常な動作は短い SA ライフタイムに使用されます。グループ メンバー（GM）はこの早いキー再生成を受信すると、新しい TEK が発信としてロールオーバーされるまで、引き続き古い TEK を発信として使用します。事前配置されたキー再生成機能と長い SA ライフタイム機能の組み合わせはキーのロールオーバーの安定性を向上させます。この機能により、定期的なリマインダ キー再生成や同期キー再生成などのキー再生成エラーを回復するための十分な時間（KS）が確保されます。

GET VPN の復元力の設定方法

GM が長い SA ライフタイムをサポートするソフトウェア バージョンを実行していることを確認する

長い SA ライフタイムは、GET VPN ネットワーク内のすべてのデバイスをこの機能をサポートする GET VPN ソフトウェア バージョンにアップグレードしてから使用する必要があります。

ネットワーク内のすべてのデバイスが長い SA ライフタイムをサポートしていることを確認するには、キー サーバ（またはプライマリ キー サーバ）でこの作業を実行します。

手順の概要

1. **enable**
2. **show crypto gdoi feature long-sa-lifetime**
3. **show crypto gdoi feature long-sa-lifetime | include No**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show crypto gdoi feature long-sa-lifetime** 例： `Device# show crypto gdoi feature long-sa-lifetime`	GET VPN ネットワーク内の各 KS および GM で実行されている GET VPN ソフトウェアのバージョンを表示し、そのデバイスが長い SA ライフタイムをサポートしているかどうかを表示します。
ステップ 3	**show crypto gdoi feature long-sa-lifetime | include No** 例： `Device# show crypto gdoi feature long-sa-lifetime | include No`	（オプション）長い SA ライフタイムをサポートしないデバイスのみ表示します。

長い SA ライフタイムの設定

TEK の長い SA ライフタイムの設定

トラフィック暗号キー（TEK）の長い SA ライフタイムを設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec profile***name*
4. **set security-association lifetime days** *days*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ipsec profile***name* 例： `Device(config)# crypto ipsec profile gdoi-p`	2 つの IPsec デバイス間における IPsec 暗号化で使用される IPsec パラメータを定義し、暗号化 IPsec プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**set security-association lifetime days** *days* 例： `Device(ipsec-profile)# set security-association lifetime days 15`	セキュリティ アソシエーション（SA）のライフタイムを 1 日に設定します。 • 最大日数は 30 日です。
ステップ 5	**end** 例： `Device(ipsec-profile)# end`	暗号 IPsec プロファイル ピア コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

KEK の長い SA ライフタイムの設定

キー暗号キー（TEK）の長い SA ライフタイムを設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group***group-name*
4. **identity number** *number*
5. **server local**
6. **rekey lifetime days** *days*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gdoi group***group-name* 例： `Device(config)# crypto gdoi group GET`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。
ステップ 4	**identity number** *number* 例： `Device(config-gdoi-group)# identity number 3333`	GDOI グループ番号を指定します。
ステップ 5	**server local** 例： `Device(config-gdoi-group)# server local`	デバイスを GDOI キー サーバとして指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 6	**rekey lifetime days** *days* 例： `Device(gdoi-local-server)# rekey lifetime days 20`	KEK の日数または秒数を制限します。
ステップ 7	**end** 例： `Device(gdoi-local-server)# end`	GDOI ローカル サーバ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

定期的なリマインダ同期キー再生成の設定

定期的なリマインダ同期キー再生成を設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. **identity number** *number*
5. **server local**
6. **rekey retransmit** *number-of-seconds* **periodic**
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gdoi group** *group-name* 例： `Device(config)# crypto gdoi group group1`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。
ステップ 4	**identity number** *number* 例： `Device(config-gdoi-group)# identity number 3333`	GDOI グループ番号を指定します。
ステップ 5	**server local** 例： `Device(config-gdoi-group)# server local`	デバイスを GDOI キー サーバとして指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 6	**rekey retransmit** *number-of-seconds* **periodic** 例： `Device(gdoi-local-server)# rekey retransmit 10 periodic`	キー再生成メッセージが定期的に再送信される回数を指定します。 • このコマンドが設定されていない場合、再送信は行われません。
ステップ 7	**end** 例： `Device(gdoi-local-server)# end`	GDOI ローカル サーバ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

GET VPN の復元力の確認とトラブルシューティング

キー サーバの GET VPN の復元力の確認とトラブルシューティング

キー サーバ（KS）で実行されている設定を表示するには、**show running-config** コマンドと次のコマンドを使用します。

手順の概要

1. **enable**
2. **show crypto gdoi**
3. **show crypto gdoi ks rekey**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show crypto gdoi** 例： `Device# show crypto gdoi`	現在の GDOI 構成、および KS からダウンロードされたポリシーを表示します。
ステップ 3	**show crypto gdoi ks rekey** 例： `Device# show crypto gdoi ks rekey`	KS から送信されるキー再生成に関する情報を表示します。

グループ メンバーの GET VPN の復元力の確認とトラブルシューティング

グループ メンバー（GM）で実行されている設定を表示するには、**show running-config** コマンドと次のコマンドを使用します。

手順の概要

1. **enable**
2. **show crypto gdoi ks rekey**
3. **show crypto gdoi ks policy**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**show crypto gdoi ks rekey** 例： `Device# show crypto gdoi ks rekey`	KS から送信されるキー再生成に関する情報を表示します。
ステップ 3	**show crypto gdoi ks policy** 例： `Device# show crypto gdoi ks policy`	次のキー再生成までの時間を表示します。

GET VPN 復元力の設定例

例：GMが長いSAライフタイムをサポートするソフトウェアバージョンを実行していることを確認する

次の例は、各グループ内のすべてのデバイスが長い SA ライフタイムをサポートしているかどうかを確認するために KS（またはプライマリ KS）で GET VPN ソフトウェア バージョン管理コマンドを使用する方法を示します。

```
Device# show crypto gdoi feature long-sa-lifetime

Group Name: GETVPN
    Key Server ID       Version   Feature Supported
        10.0.5.2         1.0.4          Yes
        10.0.6.2         1.0.4          Yes
        10.0.7.2         1.0.3          No
        10.0.8.2         1.0.2          No

    Group Member ID     Version   Feature Supported
        10.0.1.2         1.0.2          No
        10.0.2.5         1.0.3          No
        10.0.3.1         1.0.4          Yes
        10.0.3.2         1.0.4          Yes
```

また、上記のコマンドは GM でも入力できます（その GM の情報を表示します。KS や他の GM には使用できません）。

次の例は、KS（プライマリ KS）で長い SA ライフタイムをサポートしていない GET VPN ネットワークのデバイスのみ検索するコマンドを入力する方法を示しています。

```
Device# show crypto gdoi feature long-sa-lifetime | include No

        10.0.7.2         1.0.3          No
        10.0.8.2         1.0.2          No
        10.0.1.2         1.0.2          No
        10.0.2.5         1.0.3          No
```

例：長い SA ライフタイムの設定

例：TEK の長い SA ライフタイムの設定

次に、トラフィック暗号キー（TEK）の長い SA ライフタイムの設定方法の例を示します。

```
Device> enable
Device# configure terminal
Device(config)# crypto ipsec profile gdoi-p
Device(ipsec-profile)# set security-association lifetime days 15
Device(ipsec-profile)# end
```

例：KEK の長い SA ライフタイムの設定

次に、キー暗号キー（KEK）の長い SA ライフタイムの設定方法の例を示します。

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group GET
Device(config-gdoi-group)# identity number 3333
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# rekey lifetime days 20
Device(gdoi-local-server)# end
```

例：定期的なリマインダ同期キー再生成の設定

次に、定期的なリマインダ同期キー再生成の設定方法の例を示します。

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group group1
Device(config-gdoi-group)# identity number 3333
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# rekey retransmit 10 periodic
Device(gdoi-local-server)# end
```

GET VPN の復元力のその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
Cisco IOS セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』
エンタープライズ ネットワークの GET VPN の有効化のための基本的な導入ガイドライン	『Cisco IOS GET VPN Solutions Deployment Guide』
GET VPN ネットワークの設計と実装	『Group Encrypted Transport VPN (GETVPN) Design and Implementation Guide』

標準および RFC

標準/RFC	タイトル
RFC 2401	『*Security Architecture for the Internet Protocol*』
RFC 6407	『*The Group Domain of Interpretation*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

GET VPN の復元力の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *9*：*GET VPN* の復元力の機能情報

機能名	リリース	機能情報
GET VPN の復元力	Cisco IOS XE Release 3.9S	GET VPN の復元力機能では、Cisco Group Encrypted Transport（GET）VPN の復元力を改善し、エラーが発生したときのデータ トラフィックの中断を防止したり最小化したりします。 次のコマンドが導入または変更されました：**rekey lifetime**、**rekey retransmit**、**set security-association lifetime**、**show crypto gdoi**。

第 6 章

GETVPN 復元力 GM - エラー検出

GETVPN 復元力 - GM エラー検出機能では、無効なステートフル パケット インスペクション（SPI）または時間ベースのアンチリプレイ（TBAR）エラーなど、各グループ ドメイン オブ インタープリテーション（GDOI）のデータ プレーンで異常なパケットを検出します。これらのエラーは追跡され、パケットの外部送信元 IP アドレスが記録されます。

- 機能情報の確認，163 ページ
- GETVPN の復元力：GM のエラー検出に関する情報，164 ページ
- GETVPN の復元力：GM のエラー検出の設定方法，165 ページ
- GETVPN の復元力：GM のエラー検出の設定例，166 ページ
- GETVPN の復元力：GM のエラー検出その他の参考資料，166 ページ
- GETVPN の復元力：GM のエラー検出の機能情報，167 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、『Bug Search Tool』およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

GETVPN の復元力：GM のエラー検出に関する情報

エラー処理

GETVPN 復元力 - GM エラー検出機能によって障害が検出されると、異常なパケットの送信元 IP アドレスを示す syslog メッセージが生成されます。

```
 *Feb 10 21:01:56.043:
%GDOI-4-TIMEBASED_REPLAY_FAILED: An anti replay check has failed in
group GETVPN from sourceip-address
100.0.0.9.
 my_pseudotime is 600006.78 secs,
peer_pseudotime is 500033.34 secs, replay_window is 100
(second)
 *Feb 10 21:01:56.043:
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed
 connection id=29, sequence
number=11
```

show crypto gdoi gm replay コマンドは、直近の 50 個の時間ベースのアンチリプレイ（TBAR）エラーの履歴を表示します。これらの送信元 IP アドレス レコードを使用すると、送信者グループ メンバー（GM）を突き止め、既存のハードウェアまたはソフトウェアの問題を調査することができます。次の統計情報もコマンドで利用できます。

- GM リカバリ機能のオン/オフ
- リカバリの間隔
- 適用される GM リカバリの再登録の数

エラーが発生すると、GM は次に使用可能なキー サーバ（KS）に再登録し、最新のポリシーとキーを取得し、登録が完了するまで以前にダウンロードされたすべてのグループ ポリシーとキーを維持します。

たとえば、連携キー サーバ（COOP KS）の分割が発生すると、レベルを上げられた各 KS が独自の Key Encryption Key（KEK）とトラフィック暗号化キー（TEK）を生成します。GM が復号できない無効な SPI パケットを受信すると、リスト内の次のキー サーバ（KS）へのリカバリ登録が実行されます。このリカバリ登録は、リスト内の次の KS への各クライアント リカバリ間隔で、無効なステートフル パケット インスペクション（SPI）パケットまたは TBAR エラーごとに繰り返されます。リスト内のすべての KS が回復され、無効な SPI が含まれなくなると、その SPI は誤検出としてマークされ、それ以上のリカバリ登録は実行されません。KS は TBAR エラーに対して常にリカバリ登録を実行します。ただし、無効な SPI のために GM がリストのすべての KS を回復し、SPI がある KS がなくなると、その SPI は誤検出としてマークされ、その SPI のためにさらにリカバリ登録が実行されることはなくなります。

この GM リカバリの再登録機能がトリガーされたことを通知するため、syslog メッセージが生成されます。たとえば、GM が 300 秒ごとにコントロール プレーンのエラーをモニタするように設定している場合、リカバリ登録が発生すると、次の syslog が生成されます。

```
*Feb 23 19:06:28.600: %GDOI-5-GM_RECOVERY_REGISTER: received invalid GDOI packets; register
 to KS to refresh policy, keys, and PST.
```

GETVPN の復元力：GM のエラー検出の設定方法

GETVPN の復元力：GM のエラー検出の設定

手順の概要

1. **cryptogdoigroup***group-name*
2. **identitynumber** *number*
3. **serveraddressipv4** *address*
4. **client recovery-check interval** *interval*
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**cryptogdoigroup***group-name* 例： `Device(config)# crypto gdoi group GETVPN`	グループ ドメイン オブ インタープリテーション（GDOI）グループを作成し、GDOI グループ コンフィギュレーション モードを開始します。
ステップ 2	**identitynumber** *number* 例： `Device(config-gdoi-group)# identity number 1111`	GDOI グループ番号を指定します。
ステップ 3	**serveraddressipv4** *address* 例： `Device(config-gdoi-group)# server address ipv4 1.0.0.2`	GDOI グループが到達しようとするサーバの IP アドレスを指定します。
ステップ 4	**client recovery-check interval** *interval* 例： `Device(config-gdoi-group)# client recovery-check interval 300`	コントロールプレーンを監視するクライアント グループ メンバー（GM）の時間間隔を設定します。
ステップ 5	**exit** 例： `Device(config-gdoi-group)# exit`	GDOI グループ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

GETVPN の復元力：GM のエラー検出の設定例

例：GETVPN の復元力：GM のエラー検出の設定

次の例は、グループ メンバー（GM）が 300 秒ごとにコントロール プレーンのエラーを監視できるようにする方法を示します。

```
crypto gdoi group GETVPN
 identity number 1111
 server address ipv4 1.0.0.2
 client recovery-check interval 300
```

GETVPN の復元力：GM のエラー検出その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command References*』
エンタープライズ ネットワークの GET VPN の有効化のための基本的な導入ガイドライン	『*Cisco IOS GET VPN Solutions Deployment Guide*』
GET VPN ネットワークの設計と実装	『*Group Encrypted Transport VPN (GETVPN) Design and Implementation Guide*』

標準および RFC

標準/RFC	タイトル
RFC 6407	『*The Group Domain of Interpretation*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

GETVPN の復元力：GM のエラー検出の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *10*：*GETVPN* の復元力：*GM* のエラー検出の機能情報

機能名	リリース	機能情報
GETVPN の復元力：GM のエラー検出	Cisco IOS XE Release 3.10S	各 GDOI グループのデータ プレーンのエラー パケットを検出します。 次のコマンドが導入されました：**client recovery-check interval**。

第 7 章

GETVPN CRL チェック

Group Encrypted Transport VPN（GET VPN）プロセスの間、証明書は認証局（CA）から受信され、アイデンティティの証明として使用されます。証明書は、キーのセキュリティ侵害や証明書の喪失など、さまざまな理由により失効する可能性があります。失効した証明書はリポジトリに定期的に発行される証明書失効リスト（CRL）に配置されます。このリストは設定済みの CRL ライフタイムで指定された期間、リポジトリに格納されます。数時間から数日の任意の期間にすることができます。

- 機能情報の確認，169 ページ
- GETVPN CRL チェックに関する情報，170 ページ
- GETVPN CRL チェックの設定方法，171 ページ
- GETVPN CRL チェックの設定例，177 ページ
- GETVPN CRL チェックに関する追加情報，178 ページ
- GETVPN CRL チェックに関する機能情報，179 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、『Bug Search Tool』およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

GETVPN CRL チェックに関する情報

インターネット キー エクスチェンジ（IKE）では、証明書は 2 台のピア間でセッションが確立されるときに検証されます。現在のセッションは証明書失効の影響を受けません。ただし、新しいセッションを確立することはできず、グループ メンバーがキー サーバ（KS）に再登録しない限り証明書は再検証されません。

GETVPN CRL チェック機能では、設定されたトラストポイントで新しい CRL が利用可能なときに公開キー インフラストラクチャ（PKI）がグループ ドメイン オブ インタープリテーション（GDOI）KS に通知することができます。その後 KS は新しい Key Encryption Key（KEK）を作成し、グループ メンバー デバイスに再認証メッセージを送信します。これにより、syslog メッセージが出力され、現在の KEK が削除され、KS に再登録されます。

連携キー サーバのプロトコル統合

連携キーサーバのプロトコル（COOP）は、VPN ネットワークに複数のキー サーバ（KS）を設定できるようにする GET VPN の機能です。KS 冗長性のために使用されます。

すべての KS でグループ メンバー（GM）の再認証を有効にすることで、GETVPN CRL チェックは COOP と統合されます。ただし、連携 KS 間で一時的に接続が失われる場合、COOP 分割が発生する可能性は常にあります。

再認証がトリガーされたときの COOP 分割なし

COOP 分割が発生しない場合、プライマリ GM デバイスはセカンダリ KS の Key Encryption Key（KEK）を削除し、GM に再認証メッセージを送信します。セカンダリ KS は GM が再登録を開始する前に現在のポリシーをプライマリ ポリシーと同期させます。すべての GM が使用可能な KS に再登録して再認証され、新しい KEK を受信します。

再認証がトリガーされたときの COOP 分割

再認証がトリガーされる前に COOP 分割が発生し、2 つのプライマリ KS しかない場合、両者が再認証メッセージを送信します。それぞれのプライマリ KS は異なる新しい KEK を作成します。GM は、メッセージを受信するとすぐに既存の KEK をすべて削除するため、受信する最初の再認証メッセージだけを理解します。GM は使用可能な KS に再登録し、CRL チェックが行われます。再登録のとき、GM が登録した KS に応じて GM は最初のプライマリの KEK または 2 番目のプライマリの KEK のいずれかを受け取ります。GM はその KEK をインストールし、そのプライマリ KS からのみ今後のキー再生成を受信します。COOP マージが発生すると、KS はポリシーを同期し、キー再生成を送信して、すべての GM が最新の KEK とトラフィック暗号キー（TEK）を持つようにします。

異なる KEK の作成の回避

COOP 分割中に再認証がトリガーされる場合も、再認証と CRL チェックは依然として発生します。ただし、KS での異なる KEK の作成をトリガーすることは、再認証を遅らすことによって回避できます。プライマリ KS はすべての COOP KS に到達可能な（分割されない）場合にのみ、再

認証を開始します。1 つの COOP KS に到達できない場合、プライマリ KS はすべての COOP KS が到達可能になるまで再認証メッセージの送信を遅らせます。

GETVPN CRL チェックの設定方法

GETVPN CRL チェック機能を有効にする前に、複数のコンポーネントを設定する必要があります。次の作業を行います。

- グループ メンバーとキー サーバが PKI クライアントとなるために定義された公開キー インフラストラクチャ（PKI）認証局（CA）（証明書を取得するように登録する必要があります）。
- PKI での証明書失効リスト（CRL）チェックを有効にするように設定されたキー サーバ（KS）。
- CA で利用可能であり、最初に必要なときに CRL をダウンロードするように設定された KS。これは、新しい CRL が利用可能になった後に最初のグループ メンバー（GM）登録に続いて KS が CRL をダウンロードすることを意味します。「GETVPN CRL チェックのためのキー サーバの設定」セクションを参照してください。
- PKI のグループ メンバー デバイスで無効化された CRL チェック。「グループ メンバーでの CRL チェックの無効化」セクションを参照してください。
- 証明書に対して設定されたインターネット キー エクスチェンジ（IKE）認証。「証明書の IKE 認証の設定」セクションを参照してください。

GETVPN CRL チェックのためのキー サーバの設定

新しい CRL が認証局（CA）で利用可能になった後に最初のグループ メンバー（GM）登録が発生した場合にキー サーバ（KS）が証明書失効リスト（CRL）をダウンロードするように設定するには、次のステップを実行します。

手順の概要

1. **ipdomainname***name*
2. **iphttp server**
3. **cryptopkitrustpoint** *name*
4. **enrollmenturl***url*
5. **revocation-check***method*
6. **exit**
7. **cryptoidentity** *method*
8. **fqdn***domain*
9. **fqdn***domain*
10. **exit**
11. **cryptogdoigroup** *group-name*
12. **serverlocal**
13. **authorizationidentity** *name*
14. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ipdomainname***name* 例： `Device(config)# ip domain name cisco.com`	Cisco IOS ソフトウェアが未修飾ホスト名（ドット付き 10 進ドメイン名を含まない名前）を作成するときに使用するデフォルトのドメイン名を定義します。
ステップ 2	**iphttp server** 例： `Device(config)# ip http server`	IP または IPv6 システム上の HTTP サーバを有効化します。
ステップ 3	**cryptopkitrustpoint** *name* 例： `Device(config)# crypto pki trustpoint mycert`	デバイスで使用するトラストポイントを定義し、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 4	**enrollmenturl***url* 例： `Device(config-ca-trustpoint)# enrollment url http://10.1.3.1:80`	CA の登録 URL を指定します。

	コマンドまたはアクション	目的
ステップ 5	**revocation-check***method* 例： `Device(config-ca-trustpoint)# revocation-check crl`	CRL による証明書チェックが行われることを確認します。
ステップ 6	**exit** 例： `Device(config-ca-trustpoint)# exit`	CA トラストポイント コンフィギュレーションモードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**cryptoidentity** *method* 例： `Device(config)# crypto identity abcd`	デバイスの証明書内にある指定の識別名（DN）リストを使用してデバイスのアイデンティティを設定し、暗号アイデンティティ コンフィギュレーション モードを開始します。 （注） 特定の証明書、特に特定の DN の証明書を使用して、ピアが指定された暗号化インターフェイスにアクセスしないようにするデバイス構成の制限を設定できます。
ステップ 8	**fqdn***domain* 例： `Device(config-crypto-identity)# fqdn ut01-unix5.cisco.com`	GM の完全修飾ドメイン名（FQDN）のリモート アイデンティティからネーム マングラーを取得します。
ステップ 9	**fqdn***domain* 例： `Device(config-crypto-identity)# fqdn ut01-unix6.cisco.com`	次の GM の FQDN のリモート アイデンティティからネーム マングラーを取得します。
ステップ 10	**exit** 例： `Device(config-crypto-identity)# exit`	暗号アイデンティティ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**cryptogdoigroup** *group-name* 例： `Device(config)# crypto gdoi group gdoi-group1`	グループ ドメイン オブ インタープリテーション（GDOI）グループを作成し、GDOI グループ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 12	**serverlocal** 例： `Device(config-gdoi-group)# server local`	デバイスを GDOI キー サーバとして指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 13	**authorizationidentity** *name* 例： `Device(config-gdoi-local-server)# authorization identity abcd`	識別名（DN）または FQDN に基づいて GDOI グループの認証アイデンティティを指定します。
ステップ 14	**end** 例： `Device(config-gdoi-local-server)# end`	GDOI ローカル サーバ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

グループ メンバーでの CRL チェックの無効化

Public Key Infrastructure（PKI）のグループ メンバー（GM）をチェックする証明書失効リスト（CRL）を無効にするには、次のステップを実行してください。

手順の概要

1. **ipdomainname***name*
2. **iphttp server**
3. **cryptopkitrustpoint** *name*
4. **enrollmenturl***url*
5. **revocation-check***method*
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ipdomainname***name* 例： `Device(config)# ip domain name cisco.com`	Cisco IOS ソフトウェアが未修飾ホスト名（ドット付き 10 進ドメイン名を含まない名前）を作成するときに使用するデフォルトのドメイン名を定義します。

	コマンドまたはアクション	目的
ステップ 2	**iphttp server** 例： `Device(config)# ip http server`	IP または IPv6 システム上の HTTP サーバを有効化します。
ステップ 3	**cryptopkitrustpoint** *name* 例： `Device(config)# crypto pki trustpoint mycert`	デバイスで使用するトラストポイントを定義し、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 4	**enrollmenturl***url* 例： `Device(config-ca-trustpoint)# enrollment url http://10.1.3.1:80`	認証局（CA）の登録 URL を指定します。
ステップ 5	**revocation-check***method* 例： `Device(config-ca-trustpoint)# revocation-check none`	GM の証明書チェックを無効にします。
ステップ 6	**exit** 例： `Device(config-ca-trustpoint)# exit`	CA トラストポイント モードを終了し、グローバル コンフィギュレーション モードに戻ります。

証明書の IKE 認証の設定

手順の概要

1. **cryptoisakmppolicy***priority*
2. **noauthenticationpre-share**
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**cryptoisakmppolicy***priority* 例： `Router(config)# crypto isakmp policy 1`	インターネット キー エクスチェンジ（IKE）ポリシーを定義して、ISAKMP ポリシー コンフィギュレーション モードを開始します。
ステップ 2	**noauthenticationpre-share** 例： `Router(config-isakmp)# no authentication pre-share`	IKE ポリシー内の認証方式をデフォルト値にリセットします。
ステップ 3	**end** 例： `Router(config)# end`	特権 EXEC モードに戻ります。

キー サーバでの GETVPN CRL チェックの有効化

新しい証明書失効リスト（CRL）が設定されているトラストポイント認証局（CA）で利用可能になったときに Public Key Infrastructure（PKI）がドメイン オブ インタープリテーション（GDOI）キー サーバ（KS）に通知するように設定するには、次のステップを実行します。

手順の概要

1. **cryptogdoigroup** *group-name*
2. **serverlocal**
3. **registrationperiodic crl trustpoint** *trustpoint-name*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**cryptogdoigroup** *group-name* 例： `Device(config)# crypto gdoi group gdoi_group1`	GDOI グループを作成し、GDOI グループ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**serverlocal** 例： `Device(config-gdoi-group)# server local`	デバイスをGDOIキーサーバとして指定し、GDOIローカル サーバ コンフィギュレーション モードを開始します。
ステップ 3	**registrationperiodic crl trustpoint** *trustpoint-name* 例： `Device(config-gdoi-local-server)# registration periodic crl trustpoint mycert`	設定されている PKI トラストポイント認証局で新しい CRL が使用可能になったときに GDOI KS の定期的な登録を有効にします。
ステップ 4	**end** 例： `Device(config-gdoi-local-server)# end`	GDOI ローカル サーバ モードを終了し、特権 EXEC モードに戻ります。

GETVPN CRL チェックの設定例

例：GETVPN CRL チェックの有効化

次の例は、すべての必須の事前設定を含めた、GETVPN CRL チェック機能を有効にする方法を示します。

例：GETVPN CRL チェックのためのキー サーバの設定

次の例では、新しい CRL が mycert という名前のトラストポイントの認証局（CA）で利用可能になった後に最初のグループ メンバー登録が発生すると、キー サーバ（KS）が証明書失効リスト（CRL）をダウンロードするように設定されます。

```
ip domain name cisco.com
ip http server
crypto pki trustpoint mycert
 enrollment url http://10.1.3.1:80
 revocation-check crl

crypto identity abcd
 fqdn ut01-unix5.cisco.com
 fqdn ut01-unix6.cisco.com

crypto gdoi group gdoi-group1
 server local
 authorization identity abcd
```

例：グループ メンバーでの CRL チェックの無効化

次の例では、Public Key Infrastructure（PKI）のグループ メンバー（GM）の CRL チェックが無効化されます。

```
ip domain name cisco.com
ip http server
crypto pki trustpoint mycert
 enrollment url http://10.1.3.1:80
 revocation-check none
```

例：証明書の IKE 認証の設定

```
crypto isakmp policy 1
 no authentication pre-share
```

例：キー サーバの GETVPN CRL チェックの有効化

次の例では、新しい CRL が mycert という名前のトラストポイント CA で利用可能になると、PKI が group1 という名前の GDOI KS に通知するように設定されます。

```
Crypto gdoi group gdoi_group1
 Server local
  registration periodic crl trustpoint mycert
```

GETVPN CRL チェックに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command References*』
エンタープライズ ネットワークの GET VPN の有効化のための基本的な導入ガイドライン	『*Cisco IOS GETVPN Solution Deployment Guide*』
GET VPN ネットワークの設計と実装	『*Group Encrypted Transport VPN (GETVPN) Design and Implementation Guide*』

標準および RFC

標準/RFC	タイトル
RFC 2401	『*Security Architecture for the Internet Protocol*』
RFC 6407	『*The Group Domain of Interpretation*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

GETVPN CRL チェックに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *11*：*GETVPN CRL* チェックに関する機能情報

機能名	リリース	機能情報
GETVPN CRL チェック	Cisco IOS XE Release 3.10S	新しい証明書失効リスト（CRL）が設定されているトラストポイントで利用可能になったときに Public Key Infrastructure（PKI）がドメイン オブ インタープリテーション（GDOI）キー サーバ（KS）に通知できるようにします。 次のコマンドが導入されました：**registration periodic crl trustpoint**。

第 8 章

スイート B での GET VPN のサポート

スイート B での GET VPN のサポート機能では、Cisco Group Encrypted Transport（GET）VPN に対してスイート B の暗号方式セットのサポートが追加されます。スイート B は、Galois Counter Mode Advanced Encryption Standard（GCM-AES）を含む暗号化アルゴリズムとハッシュ、デジタル署名、キー交換用のアルゴリズムのセットです。

IP Security（IPsec）VPN のスイート B は、RFC 4869、『Suite B Cryptographic Suites for IPsec』でその使用が定義されている標準規格です。スイート B は Cisco IPsec VPN に包括的なセキュリティ拡張機能を提供し、大規模な展開に対して追加のセキュリティを有効にします。スイート B は、リモート サイト間のワイドエリア ネットワーク（WAN）に高度な暗号化セキュリティを必要とする組織に対して推奨されるソリューションです。

- 機能情報の確認，181 ページ
- スイート B での GET VPN のサポートの前提条件，182 ページ
- スイート B での GET VPN のサポートの制約事項，182 ページ
- スイート B での GET VPN のサポートに関する情報，182 ページ
- スイート B での GET VPN のサポートの設定方法，191 ページ
- スイート B での GET VPN のサポートの設定例，211 ページ
- その他の参考資料，213 ページ
- スイート B での GET VPN のサポートの機能情報，214 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、『Bug Search Tool』およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

スイート B での GET VPN のサポートの前提条件

この機能を有効にするすべてのキーサーバ（KS）およびグループメンバー（GM）で、GET VPN ソフトウェア バージョン 1.0.4 以降を実行している必要があります。この機能は、GET VPN ネットワーク内のすべてのデバイスをこの機能をサポートする GET VPN ソフトウェア バージョンにアップグレードしてから使用する必要があります。この機能は、ネットワークのすべてのデバイスがスイート B をサポートするバージョンであるかどうかを確認するために KS（またはプライマリ KS）で使用するコマンドを提供します。詳細については「GM がスイート B をサポートするソフトウェア バージョンを実行していることを確認する」セクションを参照してください。

スイート B での GET VPN のサポートの制約事項

これらが GCM ポリシーまたはガロア メッセージ認証コード（GMAC）トラフィック暗号キー（TEK）ポリシーを使用している場合、グループのすべての連携 KS で同一順序の同一の ACL エントリ（ACE）を持つアクセスコントロールリスト（ACL）を使用する必要があります。そうでない場合、別の KS に登録する GM は、ポリシーのダウンロード後は正しく暗号化および復号化することができません。これは、スイート B では、SPI（TEK に関連付けられているセキュリティ パラメータ インデックス ID）が各 ACL エントリに対して生成され、各 ACL エントリに対して一意であるためです。

既存の ACL のエントリの順序を変更することはできません。したがって、GCM または GMAC TEK ポリシーを使用していて、各 KS に同一順序の同一エントリを持つように各 KS の ACL を更新する必要がある場合は、各セカンダリ KS から ACL を削除し、プライマリ KS で新しい ACL を作成し、セカンダリ KS にそれをコピーしてから、プライマリ KS で **crypto gdoi ks rekey** コマンドを入力して GET VPN ネットワーク全体のキー再生成をトリガーする必要があります。

ip access-list コマンドの **no** 形式（IPv6 を使用している場合は **ipv6 access-list** コマンドの **no** 形式）を使用して ACL を削除します。

スイート B での GET VPN のサポートに関する情報

スイート B

スイート B は国家安全保障局（NSA）と国立標準技術研究所（NIST）によって標準化されています。スイート B での GET VPN のサポート機能では、これらの暗号化アルゴリズムが GDOI および GET VPN とさまざまな方法（SHA-2/HMAC-SHA-2 と AEC-GCM/AES-GMAC の使用など）で使用できるようにします。

セキュア ハッシュ アルゴリズム 2（SHA-2）は、米国の連邦情報処理標準（FIPS）として NSA により設計され、NIST によって公開された一連の暗号ハッシュ関数（SHA-224、SHA-256、SHA-384、および SHA-512）です。SHA-2 には旧モデル SHA-1 からの多数の変更が含まれます。SHA-2 は 224、256、384、または 512 ビットのダイジェストを含む 4 つのハッシュ関数のセットで構成されます。

HMAC は反復暗号ハッシュ関数を使用するメッセージ認証のメカニズムです。HMAC-SHA-2 は、IPsec の秘密共有キーと組み合わせた SHA-2 バージョン（SHA-224、SHA-256、SHA-384 および SHA-512）反復暗号ハッシュ関数と組み合わせて使用される HMAC です。これらの組み合わせにより、HMAC-SHA-224、HMAC-SHA-256、HMAC-SHA-384、HMAC-SHA-512 と呼ばれます。これらのアルゴリズムは、認証ヘッダー（AH）（ただし GET VPN でサポートされていません）、Encapsulating Security Payload（ESP）、IKE、および IKEv2 プロトコルのデータ発信元の認証および整合性の基礎として、および IKE および IKEv2 の Pseudo-Random Function（PRF）としても使用できます。

GCM を使用する AES（AES-GCM）は、IPsec の暗号化アルゴリズムです。Galois メッセージ認証コードを使用する AES（AES-GMAC）もまた、IPsec に使用されるメッセージの整合性アルゴリズムです。

SHA-2 および HMAC-SHA-2

スイート B での GET VPN のサポート機能では、ハッシュおよび署名アルゴリズムとして SHA-2 および HMAC-SHA-2（HMAC-SHA-256、384、および 512）を使用することができます。256、384、および 512 ビット キーによる SHA-2 および HMAC-SHA-2 は次に使用されます。

- RFC 6407、『The Group Domain of Interpretation』の Section 3.2（KS と GM 間の認証）で説明されているハッシュ アルゴリズムとして IKEv1 を使用する GDOI 登録。
- KS からのキー再生成メッセージの認証および GM からの確認応答メッセージの認証のためのキー再生成メッセージをハッシュ化する Key Encryption Key（KEK）キー再生成ポリシー。
- IPsec SA 整合性チェックのための HMAC-SHA-2 の TEK IPsec ポリシー。

AES-GCM と AEC-GMAC

256、384、および 512 ビット キーによる AES-GCM（AES-GCM-128、192、および 256）および AES-GMAC（AES-GMAC-128、192、および 256）暗号化アルゴリズムは、IPsec SA 暗号化および整合性アルゴリズムとして TEK IPsec ポリシーで使用されます。GCM は暗号化および整合性に使用され、GMAC は整合性のみに使用されます。

スイート B に準拠する暗号化アルゴリズムのセット

RFC 4869 には IKE および IPsec を使用する 4 セットの暗号化アルゴリズムが定義されています。設定すると、これらのいずれかのセットがスイート B に準拠します。各セットは、暗号化アルゴリズム、デジタル署名アルゴリズム、キーアグリーメントアルゴリズム、およびハッシュまたはメッセージ ダイジェスト アルゴリズムで構成されます。

- Suite-B-GCM-128：128 ビット AES-GCM を使用する ESP の整合性の保護と機密性を提供します（RFC 4106、『The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)』を参照してください）。ESP の整合性の保護および暗号化が両方必要な場合はこのスイートまたは Suite-B-GCM-256 を使用します。
- Suite-B-GCM-256：256 ビット AES-GCM を使用する ESP の整合性の保護と機密性を提供します（RFC 4106、『The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)』を参照してください）。ESP の整合性の保護および暗号化が両方必要な場合はこのスイートまたは Suite-B-GCM-128 を使用します。
- Suite-B-GMAC-128：128 ビット AES-GMAC を使用して ESP の整合性の保護を提供します（RFC 4543、『The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH』を参照してください）が、機密性は提供しません。ESP 暗号化の必要がない場合にのみこのスイートまたは Suite-B-GMAC-256 を使用します。
- Suite-B-GMAC-256：256 ビット AES-GMAC を使用して ESP の整合性の保護を提供します（RFC 4543、『The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH』を参照してください）が、機密性は提供しません。ESP 暗号化の必要がない場合にのみこのスイートまたは Suite-B-GMAC-128 を使用します。

シスコのソフトウェアでは、これらのどのアルゴリズムも設定できます。スイート B での GET VPN のサポート機能では、GET VPN でこれらのアルゴリズムを使用できます。

SID 管理

GET VPN のカウンタ ベースの動作モード（ESP-GCM-AES など）では、初期化ベクトル（IV）をグループ キーで再利用しない必要があります。そのため、この機能では KS が IV 作成のための一意の送信者 ID（SID）を各 GM（インターフェイスごと）に割り当てることができる方法が提供されています。

スイート B の IPsec SA 暗号化および整合性アルゴリズムとして使用される TEK IPsec ポリシーには、GM にこれらの一意の SID 値（GMSID）を配布するため、KS で一意の SID 値のプールの管理が必要です。それぞれの連携 KS には割り当てる GMSID の個別のプールが必要です。各 KS はこれらの SID プールを設定するために一意の KS SID（KSSID）を設定します。

SID の領域は、KSSID 部と GMSID 部の 2 部に分けられます。したがって、SID は KSSID と GMSID の連結であり、KSSID は SID の KS 部、GMSID は SID の GM 部です。SID は次のビットによって形成されます。

```
 0                   1                   2
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3  (bits)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    KSSID    |             GMSID               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

この例では、各 KSSID（0 ～ 127）に 2^{17}（131,072）の GMSID があり、登録する各 GM に動的に割り当てられます。

GM は GMSID を使用して、AES-GCM または AES-GMAC を使用するときに指定したキーで送信される各パケットに対して一意の 64 ビット IV を形成します。IV は次のバイトで形成されます。

```
  0   1   2   3   4   5   6   7   (bytes)
+---+---+---+---+---+---+---+---+
|    SID    |       SSIV        |
+---+---+---+---+---+---+---+---+
```

送信者固有の IV（SSIV）は、パケット カウンタです。

グループ サイズ

グループ サイズは、GM への配布のため KS に予約されている KSSID および GMSID の SID スペース割り当ての長さです。使用可能なグループ サイズには、小（8、12、または 16 ビット）、中（24 ビット、デフォルト）、大（32 ビット）があります。中は、ほぼすべてのネットワークに適しています。

大のグループ サイズは、マニュアル『Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program』のセクション A.5「Key/IV Pair Uniqueness Requirements from SP 800-38D」の要件（スイート B と組み合わせて使用される GET VPN に 2^{32} 以上の使用可能な固有の「モジュール名」（SID）がある必要がある）に厳密に準拠する必要がある場合にのみ使用する必要があります。このマニュアルは、NIST および Communications Security Establishment Canada（CSEC）によって発行および管理されています。

たとえば、KS 1 台の大のグループ サイズで SID は 32 ビットであり、512 個の KSSID 値（0 ～ 511 の範囲）があり、それぞれに GM の登録に配布する GMSID が 8,388,607 個あります。大のグループ サイズでは、次の KSSID 割り当てのガイドラインを使用して、KSSID の範囲を設定します。

表 *12*：グループ サイズ大に推奨される *KSSID* 範囲

KS	1 台の KS（連携 KS なし）	2 台の連携 KS	3 台の連携 KS	4 台の連携 KS
KS1	0 - 511	0 - 255	0 - 127	0 - 63
KS2	—	256 - 511	128 - 255	64 - 127
KS3	—	—	256 - 383	128 - 191
KS4	—	—	384 - 511	192 - 255
KS5	—	—	—	256 - 319
KS6	—	—	—	320 - 383
KS7	—	—	—	384 - 447
KS8	—	—	—	448 - 511

最初に元の KS を設定し、より多くの KS を含めるように連携 KS ネットワークを拡張する予定の場合、上の表の列にはネットワークで予想される KS の数を使用し、後で新しい KS を追加できるようにします。

小（8、12、または 16 ビット）のグループ サイズは、RFC 6054、『Using Counter Modes with Encapsulating Security Payload (ESP) and Authentication Header (AH) to Protect Group Traffic』に従って、8、12、および 16 ビットの SID 長さで厳格な相互運用性が要求される、よく理解されている状況でのみ使用する必要があります。このような相互運用性が必要な場合、グループごとの SID の数が厳しく制限される（これにより KS および GM の数が厳しく制限される）ため、ネットワークの設計時は注意が必要です。小グループ サイズの制限を次に示します。

表 *13*：グループ サイズ小の制限

SID 長さ	KSSID（合計 KS）	KSSID ごとの GMSID	GMSID（合計 GM）	KS 1 台に可能な GM 登録数（すべての KS に KSSID を均等に割り当てた後）			
—	—	—	—	**1 KS**	**2 KS**	**4 KS**	**8 KS**
8 ビット	2	128	255	320	96	—	—
12 ビット	4	1,024	4,095	3,840	1,792	768	—
16 ビット	16	4,096	65,535	64,512	31,744	15,360	7,168

連携キー サーバへの KSSID 割り当て

設定されたグループ サイズ、KS の数、GM の数、KS ごとの GM の数、および KS または GM（または両方）の将来の拡張に基づいて、最初の GDOI KS ID（KSSID）の数を各 KS に割り当てるよう前もって計画する必要があります。

GDOI グループに複数の連携 KS があるときは、各 KS が固有の KSSID 値のセットを持つようにして、登録する GM が、グループ内の登録する別の GM と同じ SID を受け取らないようにする必要があります。このため、連携 KS の数と、連携 KS を後で追加するかどうかを考慮しつつ、連携 KS 全体に KSSID をどのように割り当てるのかを前もって計画する必要があります。何も追加しない場合、すべての KS で利用可能なすべての KSSID を割り当てることができます。連携 KS を追加する場合、一部の KSSID を予約し、それらの KS をネットワークに追加するときに割り当てる必要があります。

KSSID は再割り当てできます。ただし、GMSID を配布するために KS によってすでに使用されている KSSID を KS から削除する場合、グループはトラフィックを損失することなく再初期化されます（つまり、すべての GM が強制的に再登録を行い、TEK IPsec SA のキー再生成が行われて使用済みの KSSID がリセットされます）。このグループの再初期化を回避するには、（中のデフォルト グループ サイズを使用する）次の表のガイドラインを使用します。

表 *14*：連携 *KS*（グループ サイズ中）の推奨される *KSSID* 割り当て範囲

	1 台の KS（連携 KS なし）	2 台の連携 KS	3 台の連携 KS	4 台の連携 KS
KS1	0 - 127	0 - 63	0 - 31	0 - 15
KS2	—	64 - 127	32 - 63	16 - 31
KS3	—	—	64 - 95	32 - 47
KS4	—	—	96 - 127	48 - 64
KS5	—	—	—	65 - 80
KS6	—	—	—	81 - 95
KS7	—	—	—	96 - 112
KS8	—	—	—	113 - 127

より多くの KS を含めるように連携 KS ネットワークを拡張する予定の場合、最初に元の KS を設定するときは、上の表の列には拡張したネットワークで予定される KS の数を使用し、後で新しい KS を追加できるようにします。

次に、KS に KSSID を割り当てるための追加のガイドラインを示します。

- KS 全体の KSSID の連続するブロックのみを設定します（例：KS1 = 0-9 + 40-49、KS2 = 10-19 + 50-59、KS3 = 20-29、KS4 = 30-39 など）。
- 任意の 1 台の KS には、（他の KS が GM 登録をすべて失敗した場合）グループからすべての GM 登録を受信するために十分な KSSID のスペースがある必要があります。
- グループの再初期化を回避するには、新しいKSSIDの値または範囲だけを追加します。必要な場合を除き、これらは削除しないでください。
- ネットワーク分割（連携 KS 間の接続の損失）の間は、KSSID の割り当てを変更しないでください。これにより、マージ時（連携 KS 間の接続の回復時）に再初期化を引き起こす可能性がある KSSID の重複を防ぎます。
- グループが *n* とおりの分割（セカンダリ KS が計画されるがまだ設定されていないという意味）を開始する場合は、すべてのKSSIDをグループが分割されていないかのように設定します。

使用可能な KSSID の数は、次の表のように、グループ サイズの設定に依存します。

表 *15*：グループ サイズに基づく使用可能な *KSSID* の範囲

設定されたグループ サイズ	使用可能な KSSID の数
小（8 ビット）	0 ～ 1
小（12 ビット）	0 ～ 3
小（16 ビット）	0 ～ 15
中	0 ～ 127
大	0 ～ 511

グループの再初期化

グループの再初期化は、KSSID を廃棄するプロセスです。グループの再初期化は、すべての KS にわたって発生します（プライマリおよびセカンダリ）。どの KS もグループの再初期化をトリガーでき、次のときに発生します。

- 非 GCM から GCM に TEK ポリシーを変更する。
- グループ サイズを変更する。
- 以前に使用した KSSID を削除する。
- グループの KS が KSSID と GMSID の両方を使い果たした。
- 連携 KS によって検出された KSSID の重複が解決された。

再初期化では、すべての KS が使用済みの KSSID を古い（使用済みの）KSSID に移動します（それにより廃棄されます）。次に、再初期化によって新しい KEK と新しい TEK が作成され、既存の TEK ライフタイムが短くなり、既存の TEK が削除され、すべての GM が再登録します（**clear crypto gdoi ks members** コマンドによって決定される期間内）。この期間は残りのライフタイムの 5 % であり、90 秒から 1 時間の間です。既存の TEK のライフタイムが期限切れになると、各 KS は古い（使用済み）KSSID をリセットするため、すべての KSSID が再度使用可能になります。

再初期化により GM でトラフィックが中断されることはありません。すべての GM は登録時に新しい TEK を含む新しい GMSID を受信します。

スイート B の Cisco GET VPN システム ロギング メッセージ

次の表では、スイート B に関連する GET VPN システム ロギング（syslog とも呼ばれます）メッセージについて説明します。

表 *16* : ***KS*** および連携 ***KS*** メッセージ

メッセージ	説明
%GDOI-5-KS_REINIT_GROUP: *reason* for group *group-name* and will re-initialize the group.	KS はグループを再初期化します。表示される可能性のある *reason* の文字列は、次のとおりです。 • KS configured Suite-B transform requiring SIDs • KS configured Suite-B transform requiring SIDs during scheduled rekey • KS is running out of SIDs • KS changed Group Size • KS removed used KSSIDs • KS issued ’clear crypto gdoi ks members’ • KS issued re-init test cmd • KSSID overlap was resolved • Pri KS peer changed used Group Size • Pri KS peer sent re-init request • Sec KS peer sent re-init request
%GDOI-5-KS_REINIT_FINISH: Re-initialization of group *group-name* completed.	グループの再初期化が完了しました。一部の操作は再初期化中（グループサイズの変更時や使用する KSSID の削除時など）にブロックされるため、再初期化がいつ完了したのかを確認するのに役立ちます。再初期化は、古い（使用した）TEK がクリアされるまで終了しません。これは、再初期化が再度チェックされるか（**show** コマンドの実行時、グループ サイズまたは KSSID の設定時、または連携 KS の更新時など）、次の GM が登録するまで発生しないことがあります。
%GDOI-3-KS_NO_SID_AVAILABLE: GMs for group *group-name* need SIDs but this KS has no KS SIDs configured or no more SIDs available.	（GCM の使用時と GM が登録を開始した後）グループの GM は SID を必要としますが、KS に設定された KSSID がないか、それ以上使用可能な SID がありません。

メッセージ	説明
%GDOI-3-COOP_KS_KSSID_OVERLAP: Overlapping KS Sender Identifier(s) (KSSID) {*KSSID*|*KSSID-Range*} with COOP-KS peer *ip-address* in group *group-name* blocking GM registration (MISCONFIG).	別のグループの連携 KS ピアと重複する KSSID または KSSID 範囲が GM 登録をブロックしています。重複する KSSID 設定は CLI によって連携 KS でブロックされますが、GET VPN ネットワークの分割シナリオ（1 つ以上の連携 KS が一時的に使用できなかったがオンラインに戻った場合）や保存済みの設定を使用するとこれが生じることがあります。
%GDOI-5-COOP_KS_KSSID_OVERLAP_RESOLVED: Resolved overlapping KS Sender Identifier(s) (KSSID) with COOP-KS peer allowing GM registrations once again.	連携 KS ピアと重複する KSSID が解決されました（GM 登録を再開できます）。

表 *17* : ***GM*** メッセージ

メッセージ	説明
%GDOI-5-GM_IV_EXHAUSTED: GM for group *group-name* exhausted its IV space for interface *interface-name* and will re-register.	グループの GM が特定の SA の IV スペース（固有の IV のセットの意味）を使い尽くしたため、再登録します。
%GDOI-5-GM_REJECTING_SA_PAYLOAD: Registration: Policy in SA payload sent by KS *ip-address* rejected by GM in the group *group-name* reason: client rekey hash algorithm (*kek-policy*) is unacceptable by this GM.	クライアントのキー再生成ハッシュアルゴリズム（指定された KEK ポリシー）が指定されたグループの GM によって承認されませんでした。登録時に GM が KEK ポリシーを拒否しました。
%GDOI-5-GM_REJECTING_SA_PAYLOAD: Registration: Policy in SA payload sent by KS *ip-address* rejected by GM in the group *group-name* reason : client rekey transform-sets (*tek-policy*) for data-protection are unacceptable by this GM.	データ保護のクライアントのキー再生成トランスフォームセット（指定された TEK ポリシー）が GM によって承認されませんでした。登録時に GM が TEK ポリシーを拒否しました。
%GDOI-5-GM_REKEY_TRANSFORMSET_CHECK_FAIL: The transform set (*transform-set*) for data protection in group *group-name* is unacceptable by this client.	グループのデータ保護のトランスフォームセットがクライアントによって承認されませんでした。GM がキー再生成を受け取り、TEK ポリシーを拒否しました。

メッセージ	説明
%GDOI-3-KS_REKEY_AUTH_KEY_LENGTH_INSUFFICIENT: Rejected rekey sig-hash algorithm change: using sig-hash algorithm HMAC_AUTH_SHA*bits* requires an authentication key length of at least *number-of-bits* bits (*number-of-blocks* blocks in bytes) - current RSA key "360-bit" is only 45 blocks in bytes.	RSA キーのモジュラス長が十分にないため、キー再生成のシグニチャ ハッシュ アルゴリズムの設定が拒否されました。HMAC-SHA-384 は少なくとも 465 ビット（バイトの 59 ブロック）のモジュラスを必要とし、HMAC-SHA-512 は 593 ビット（バイトの 75 ブロック）のモジュラスを必要とします。

スイート B での GET VPN のサポートの設定方法

スイート B での GET VPN のサポート機能セットの各機能は個別に設定可能です。しかし、スイート B の標準に準拠するため、特定の組み合わせでこれらの機能を設定する必要があります。これらの組み合わせの詳細は、RFC 4869、『Suite B Cryptographic Suites for IPsec』を参照してください。

GM がスイート B をサポートするソフトウェア バージョンを実行していることを確認する

GET VPN はグループに基づいた技術であるため、（プライマリ KS、連携 KS、および GM を含めた）同じグループ内のすべてのデバイスは、機能を有効化するためにスイート B の機能をサポートする必要があります。グループの機能を有効にするには、グループ内のすべてのデバイスが GET VPN ソフトウェアの互換性のあるバージョンを実行していることを確認する必要があります。

GET VPN ネットワークのすべてのデバイスがスイート B をサポートしていることを確認するには、KS（またはプライマリ KS）で次のステップを実行します。

手順の概要

1. **enable**
2. **showcryptogdoifeaturesuite-b**
3. **showcryptogdoifeaturesuite-b|includeNo**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showcryptogdoifeaturesuite-b** 例： `Device# show crypto gdoi feature suite-b`	ネットワーク内の各 KS および GM で実行されている GET VPN ソフトウェアのバージョンを表示し、そのデバイスがスイート B をサポートしているかどうかを表示します。
ステップ 3	**showcryptogdoifeaturesuite-b|includeNo** 例： `Device# show crypto gdoi feature suite-b | include No`	（オプション）スイート B をサポートしないデバイスのみ検索します。

GET VPN スイート B でのキー サーバの設定

KEK の署名ハッシュ アルゴリズムの設定

KEK の署名ハッシュ アルゴリズムを設定するにはこの作業を行います。

はじめる前に

この作業には次の前提条件があります。

- デバイスに関連付けられている RSA キー ペアを使用するキー再生成認証が有効になっていることを確認します。これを行うには、**rekey authentication** コマンドを **mypubkey rsa***key-name* キーワードと引数で使用します。
- RSA キー ペアに十分な長さのモジュラスがあることを確認します。HMAC-SHA-384 は少なくとも 465 ビット（バイトの 59 ブロック）のモジュラスを必要とし、HMAC-SHA-512 は 593 ビット（バイトの 75 ブロック）のモジュラスを必要とします。キー再生成の署名ハッシュ アルゴリズムが不十分なモジュラス長のキー ペアを使用する SHA-384 または SHA-512 に変更されると、設定拒否メッセージがコンソールに表示され、システム ログ メッセージが生成されます。同様に、キー再生成の署名ハッシュ アルゴリズムがすでに SHA-384 または SHA-512 であり、キーペアが不十分なモジュラス長の 1 つに変更されると、同様のメッセージがコンソールに表示され、同じシステム ログ メッセージが生成されます。

- キー再生成メッセージを受信した後の GM から KS への確認応答の認証に SHA-2/HMAC-SHA-2 を使用するには、GM へのキー再生成メッセージのユニキャスト配信を有効にする必要があります。これを実行するには、**rekey transport unicast** コマンドを使用します。

手順の概要

1. **enable**
2. **configureterminal**
3. **cryptogdoigroup** [**ipv6**]*group-name*
4. **serverlocal**
5. **rekey sig-hash algorithm** *algorithm*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cryptogdoigroup** [**ipv6**]*group-name* 例： `Device(config)# crypto gdoi group mygroup`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。 • データ プレーン内で IPv6 で GET VPN を使用する場合、**ipv6** キーワードを使用する必要があります。
ステップ 4	**serverlocal** 例： `Device(config-gdoi-group)# server local`	デバイスを GDOI KS として指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 5	**rekey sig-hash algorithm** *algorithm* 例： `Device(gdoi-local-server)# rekey sig-hash algorithm sha512`	KEK の署名ハッシュ アルゴリズムを設定します。スイート B では、**sha256**、**sha384**、または **sha512** を指定する必要があります。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Device(gdoi-local-server)# end`	GDOI ローカル サーバ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

グループ サイズの設定

このタスクはオプションです。ほぼすべての展開で、メディアのデフォルトグループサイズ（送信者識別子の長さ）が推奨されます。スイート B のグループ サイズを設定するにはこの作業を行います。

スイート B（つまり ESP-GCM または ESP-GMAC）が設定され、スイート B のポリシーが生成された後で、連携 KS を使用するグループのグループ サイズを変更する場合、プライマリ KS で変更する前にすべてのセカンダリ KS でグループ サイズを変更する必要があります。

グループ サイズを変更すると（新しい SID 長が使用できるように）グループが初期化されます。KS 全体で競合するグループ サイズ設定があると GM 登録がブロックされます。

手順の概要

1. **enable**
2. **configureterminal**
3. **cryptogdoigroup** [**ipv6**]*group-name*
4. **serverlocal**
5. **groupsize** {**small** {**8** | **12** | **16**} | **medium** | **large**}
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**cryptogdoigroup** [**ipv6**]*group-name* 例： `Device(config)# crypto gdoi group mygroup`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。 • データ プレーン内で IPv6 で GET VPN を使用する場合、**ipv6** キーワードを使用する必要があります。
ステップ 4	**serverlocal** 例： `Device(config-gdoi-group)# server local`	デバイスを GDOI KS として指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 5	**groupsize** {**small** {**8** | **12** | **16**} | **medium** | **large**} 例： `Device(gdoi-local-server)# group size small 16`	グループ サイズを設定します。
ステップ 6	**end** 例： `Device(gdoi-local-server)# end`	GDOI ローカル サーバ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

キー サーバ識別子の設定

スイート B では、それぞれの GM に固有の GMSID の割り当てが必要です。これは GM が以前同じキーに（その GM または別の GM が）使用した SID を再利用できないことを意味します。したがって、GET VPN が重複する SID 値を許可しないように設計されていても、KS ごとに固有のセットを持つように KS 間の KSSID 値を正しく設定する必要があります。（KS 間の KSSID が重複すると再初期化されます。）

KS に SID のプールを割り当てるには少なくとも 1 つの KSSID を設定する必要があります。TEK IPSec ポリシーとして GCM または GMAC を設定する前に KS でこれを行います。

この作業を行って KS に KSSID または KSSID の範囲を割り当てます。各 KS は、GCM または GMAC を使用する際には少なくとも 1 つの KSSID を割り当てる必要があります。単一の KSSID、KSSID の範囲、またはその両方を設定できます。メディアのデフォルト グループ サイズとして、0 ～ 127 の範囲の 128 個の利用可能な KSSID 値があります。

KSSID 値は、GDOI ローカル サーバ ID コンフィギュレーション モードを終了するまで KS に割り当てられません（KS から使用もできません）。

手順の概要

1. **enable**
2. **configureterminal**
3. **cryptogdoigroup** [**ipv6**]*group-name*
4. **serverlocal**
5. **identifier**
6. **range***lowest-kssid-highest-kssid*
7. **value***kssid*
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cryptogdoigroup** [**ipv6**]*group-name* 例： `Device(config)# crypto gdoi group mygroup`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。 • データ プレーン内で IPv6 で GET VPN を使用する場合、**ipv6** キーワードを使用する必要があります。
ステップ 4	**serverlocal** 例： `Device(config-gdoi-group)# server local`	デバイスを GDOI KS として指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 5	**identifier** 例： `Device(gdoi-local-server)# identifier`	GDOI ローカル サーバ ID コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 6	**range***lowest-kssid-highest-kssid* 例： `Device(gdoi-local-server-id)# range 10 - 20`	KSSID の範囲を割り当てます。 • この範囲は、グループ全体で一意である必要があります。
ステップ 7	**value***kssid* 例： `Device(gdoi-local-server-id)# value 0`	KSSID を割り当てます。 • この KSSID は、グループ全体で一意である必要があります。 • **value 0** コマンドは、KSSID 値 0 で始まる SID のプールを KS に割り当てます（つまり 0x0 で始まり 0x1FFFF で終わる SID 値のプールが割り当てられます）。
ステップ 8	**end** 例： `Device(gdoi-local-server-id)# end`	GDOI ローカル サーバ ID コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

すでに別の KSSID が割り当てられている KS に 1 つ以上の KS を設定しようとすると（かつ連携 KS ネットワークが分割されていないと）、設定は拒否され、GDOI ローカル サーバ ID コンフィギュレーション モードを終了すると次のメッセージが表示されます。

```
% Key Server SID Configuration Denied:
%   The following Key Server SIDs being added overlap:
%   2, 200-250  (COOP-KS Peer: 10.0.9.1)
```

連携 KS ネットワークが分割されている場合、重複する KSSID を設定する必要はありません。ネットワークのマージで KSSID の重複が検出されると、GM の登録は重複が解決するまでブロックされます。次のシステム ログ メッセージが両方の KS に表示されます。

```
%GDOI-3-COOP_KSSID_OVERLAP: Overlapping KS Sender Identifier(s) (KSSID) {2, 200-250} with
COOP-KS peer 10.0.9.1 in group diffint blocking GM registration (MISCONFIG)
```

KS が重複する KSSID を構成解除すると、グループはトラフィックを損失することなく再初期化します（つまり、すべての GM が再登録を強制され、TEK IPSec SA は使用された KSSID をリセットするためにキー再生成されます）。次のシステム ログ メッセージが KS に表示されます。

```
%SYS-5-CONFIG_I: Configured from console by console
%GDOI-5-COOP_KSSID_OVERLAP_RESOLVED: Resolved overlapping KS Sender Identifier(s) (KSSID)
with COOP-KS peer allowing GM registrations once again
%GDOI-5-KS_REINIT_GROUP: KSSID overlap was resolved for group diffint and will re-initialize
 the group.
%GDOI-5-KS_SEND_UNICAST_REKEY: Sending Unicast Rekey for group diffint from address 10.0.8.1
 with seq # 11
%GDOI-4-GM_DELETE: GM 10.0.3.1 deleted from group diffint.
%GDOI-4-GM_DELETE: GM 10.65.9.2 deleted from group diffint.
```

%GDOI-5-KS_SEND_UNICAST_REKEY システム ログ メッセージは、これがプライマリ KS である場合にのみ表示されます。KSSID が重複しているピア KS でも %GDOI-5-COOP_KSSID_OVERLAP_RESOLVED システム ログ メッセージが表示されます。

スイート B の IPsec SA の設定

スイート B の IPsec SA を設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **cryptoipsectransform-set***transform-set-name* {**esp-gcm** | **esp-gmac**} [**128** | **192** | **256**]
4. **cryptoipsecprofile***ipsec-profile-name*
5. **settransform-set***transform-set-name*
6. **exit**
7. **cryptogdoigroup** [**ipv6**]*group-name*
8. 次のいずれかのコマンドを入力します。
   - **identitynumber***number*
   - **identityaddressipv4***address*
9. **serverlocal**
10. **saipsec***sequence-number*
11. **profile***ipsec-profile-name*
12. **matchaddress** {**ipv4** | **ipv6**} {*access-list-number* | *access-list-name*}
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**cryptoipsectransform-set***transform-set-name* {**esp-gcm** | **esp-gmac**} [**128** | **192** | **256**] 例： `Device(config)# crypto ipsec transform-set g1 esp-gcm 192`	トランフォーム セット（セキュリティ プロトコルおよびアルゴリズムの受け入れ可能な組み合わせ）を定義し、暗号化トランスフォーム コンフィギュレーション モードを開始します。 • スイート B では、ESP-GCM または ESP-GMAC を使用するトランスフォーム セットを指定する必要があります。（別のコマンドラインにコマンドをもう一度入力して、複数のトランスフォーム セットを定義できます。） • オプションで 128、192、または 256 のキー サイズを指定できます。デフォルトのキーのサイズは 128 です。
ステップ 4	**cryptoipsecprofile***ipsec-profile-name* 例： `Device(config)# crypto ipsec profile profile1`	IPsec プロファイル（2 つの IPsec ルータ間の IPsec 暗号化に使用されるパラメータ）を定義して、IPsec プロファイル コンフィギュレーション モードを開始します。
ステップ 5	**settransform-set***transform-set-name* 例： `Device(ipsec-profile)# set transform-set transformset1`	クリプト マップ エントリで使用可能なトランスフォーム セットを指定します。
ステップ 6	**exit** 例： `Device(ipsec-profile)# exit`	IPSec プロファイル コンフィギュレーション モードを終了します。
ステップ 7	**cryptogdoigroup** [**ipv6**]*group-name* 例： `Device(config)# crypto gdoi group gdoigroupname`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。 • データ プレーン内で IPv6 で GET VPN を使用する場合、**ipv6** キーワードを使用する必要があります。
ステップ 8	次のいずれかのコマンドを入力します。 • **identitynumber***number* • **identityaddressipv4***address*	GDOI グループ番号またはアドレスを指定します。 • **identitynumber***number* コマンドは IPv4 および IPv6 の構成に適用されます。 • **identityaddressipv4***address* コマンドは、IPv4 構成のみに適用されます。

	コマンドまたはアクション	目的

	例：
	`Device(config-gdoi-group)# identity number 3333`
	
	例：
	`Device(config-gdoi-group)# identity address ipv4 209.165.200.225`	

ステップ 9	**serverlocal** 例： `Device(config-gdoi-group)# server local`	デバイスを GDOI KS として指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 10	**saipsec***sequence-number* 例： `Device(gdoi-local-server)# sa ipsec 1`	GDOI グループに使用される IPsec SA ポリシー情報を指定し、GDOI SA IPsec コンフィギュレーション モードを開始する。
ステップ 11	**profile***ipsec-profile-name* 例： `Device(gdoi-sa-ipsec)# profile gdoi-p`	GDOI グループ用の IPsec SA ポリシーを定義します。
ステップ 12	**matchaddress** {**ipv4** | **ipv6**} {*access-list-number* | *access-list-name*} 例： `Device(gdoi-sa-ipsec)# match address ipv4 102`	GDOI 登録の IP 拡張アクセス リスト（ACL）を選択します。 • IPv4 グループに対しては **ipv4** キーワード、IPv6 グループに対しては **ipv6** キーワードを使用する必要があります。 • IPv6 構成には（番号付きではなく）名前付きアクセス リストを使用する必要があります。 （注） 必ずグループのすべての連携 KS の中で同一順序で同一エントリを持つ ACL を選択してください。そうでない場合、別の KS に登録する GM は、ポリシーのダウンロード後は正しく暗号化および復号化することができません。

	コマンドまたはアクション	目的

		（注） IPv6 グループに IPv4 のポリシーを割り当てようとすると、アクセス リスト名が無効であるか、リストはすでに存在するが誤った種類であることを示すエラー メッセージが表示されます。
		`Access-list type conflicts with prior definition`
		`% ERROR: access-list-name is either an invalid name or the list already exists but is the wrong type.`

ステップ 13	**end** 例： `Device(gdoi-sa-ipsec)# end`	GDOI SA IPsec コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

GET VPN スイート B でのグループ メンバーの設定

スイート B の KEK の許容可能な暗号化アルゴリズムまたはハッシュ アルゴリズムの設定

GM によって許可される KEK 用の スイート B 暗号化およびハッシュ アルゴリズムを設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **cryptogdoigroup** [**ipv6**]*group-name*
4. 次のいずれかのコマンドを入力します。
   - **identitynumber***number*
   - **identityaddressipv4***address*
5. **serveraddressipv4***address*
6. **clientrekeyencryption***cipher*[...[*cipher*]]
7. **clientrekeyhash***hash*
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cryptogdoigroup** [**ipv6**]*group-name* 例： `Device(config)# crypto gdoi group gdoigroupone`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。 • データ プレーン内で IPv6 で GET VPN を使用する場合、**ipv6** キーワードを使用する必要があります。

ステップ 4	次のいずれかのコマンドを入力します。
	
	• **identitynumber***number*
	
	• **identityaddressipv4***address*
	
	例：
	
	`Device(config-gdoi-group)# identity number 3333`
	
	例：
	
	`Device(config-gdoi-group)# identity address ipv4 10.2.2.2`
		GDOI グループ番号またはアドレスを指定します。

ステップ 5	**serveraddressipv4***address* 例： `Device(config-gdoi-group)# server address ipv4 10.0.5.2`	GDOI グループが到達しようとするサーバのアドレスを指定します。 • アドレスを無効にするには、このコマンドの **no** 形式を使用します。
ステップ 6	**clientrekeyencryption***cipher*[...[*cipher*]] 例： `Device(config-gdoi-group)# client rekey encryption 3des-cbc aes 192 aes 256`	KEK のクライアント受け入れ可能キー再生成暗号化を設定します。

	コマンドまたはアクション	目的
ステップ 7	**clientrekeyhash***hash* 例： `Device(config-gdoi-group)# client rekey hash sha384`	KEK のクライアント受け入れ可能ハッシュを設定します。 • スイート B では、**sha256**、**sha384**、または **sha512** を指定する必要があります。
ステップ 8	**end** 例： `Device(config-gdoi-group)# end`	GDOI グループ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

スイート B の TEK の受け入れ可能トランスフォーム セットの設定

GM によって許可されるデータ暗号化または認証のために TEK が使用するトランスフォーム セットを設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **cryptoipsectransform-set***transform-set-name* {**esp-gcm** | **esp-gmac**} [**128** | **192** | **256**]
4. **exit**
5. **cryptogdoigroup** [**ipv6**]*group-name*
6. **clienttransform-sets***transform-set-name1* [...[*transform-set-name6*]]
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**cryptoipsectransform-set***transform-set-name* {**esp-gcm** | **esp-gmac**} [**128** | **192** | **256**] 例： `Device(config)# crypto ipsec transform-set g1 esp-gcm 192`	トランフォーム セット（セキュリティ プロトコルおよびアルゴリズムの受け入れ可能な組み合わせ）を定義し、暗号化トランスフォーム コンフィギュレーション モードを開始します。 • スイート B では、ESP-GCM または ESP-GMAC を使用するトランスフォーム セットを指定する必要があります。 • 別のコマンドラインにコマンドをもう一度入力して、複数のトランスフォーム セットを定義できます。 • オプションで 128、192、または 256 のキー サイズを指定できます。デフォルトのキーのサイズは 128 です。
ステップ 4	**exit** 例： `Device(cfg-crypto-trans)# exit`	暗号化トランスフォーム コンフィギュレーション モードを終了します。
ステップ 5	**cryptogdoigroup** [**ipv6**]*group-name* 例： `Device(config)# crypto gdoi group gdoigroupone`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。 • データ プレーン内で IPv6 で GET VPN を使用する場合、**ipv6** キーワードを使用する必要があります。
ステップ 6	**clienttransform-sets***transform-set-name1* [...[*transform-set-name6*]] 例： `Device(config-gdoi-group)# client transform-sets g1`	データの暗号化および認証のために TEK によって使用される受け入れ可能トランスフォームセットタグを指定します。 • トランスフォーム セット タグは 6 個まで指定できます。
ステップ 7	**end** 例： `Device(config-gdoi-group)# end`	GDOI グループ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

スイート B での GET VPN のサポートの確認とトラブルシューティング

キー サーバ上のスイート B での GET VPN のサポートの確認とトラブルシューティング

KS で実行されている設定を表示するには、**show running-config** コマンドを使用します。

手順の概要

1. **show crypto gdoi ks identifier** [**detail**]
2. **show crypto gdoi ks coop identifier** [**detail**]
3. **show crypto gdoi feature suite-b**
4. **show crypto gdoi ks policy**

手順の詳細

ステップ 1 **show crypto gdoi ks identifier** [**detail**]

例：

```
Device# show crypto gdoi ks identifier detail

KS Sender ID (KSSID) Information for Group diffint:

    Transform Mode           : Counter (Suite B)
    reinitializing          : No
    SID Length (Group Size)  : 24 bits (medium)
    Current KSSID In-Use     : 0
    Last GMSID Used          : 1

    KSSID (or SIDS)Assigned        : 0-15
    KSSID (or SIDS)Used            : 0
    KSSID (or SIDS) Used  (Old)      : none
    Available KSSID (or SIDS): 1-15

    REMAINING SIDs:
      KSSID to reinitialize at         : 15
      GMSID to reinitialize at         : 6291456
      # of SIDs Remaining for Cur KSSID : 8388606
      # of SIDs Remaining until Re-init : 132120575
```

このコマンドは、スイート B の SID 管理の状態を表示します。Transform Mode フィールドは SID 管理およびスイート B のポリシーがグループ内で現在使用されているかどうかを確認するために非カウンタ（非スイート B）またはカウンタ（スイート B）のいずれかにできます。グループが現在再初期化（つまり、すべての GM が再登録を強制され、TEK IPsec SA がキー再生成されて使用済みの KSSID をリセットする）を行っている場合は、reinitializing フィールドに Yes が表示されます。SID Length (Group Size) フィールドは、グループで現在使用されているグループ サイズを決定します。デフォルトは 24 ビット（中）です。

Current KSSID In-Use フィールドおよび Last GMSID Used フィールドは、次の登録 GM に分配される SID（または SIDS）に対応します。KSSID (or SIDS) Assigned フィールドは、連携 KS と同期した、ローカル

に設定されている KSSID に対応します。Available KSSID (or SIDS) フィールドは、最後の再初期化以降まだ使用されていない KSSID に対応します。新しい KSSID を使用するたびに KSSID (or SIDS) Used フィールドに追加され、再初期化時に、これらの使用された KSSID が KSSID (or SIDS) Used (Old) フィールドに移動されます。再初期化期間の終わりに、古い使用済みの KSSID がクリアされて再び Available KSSID プールに加えられます。

（注） # of SIDs Remaining until Re-init フィールドの値が 0 に近づくと、GM が再登録を継続している場合はすぐに再初期化が発生します。再初期化によってトラフィックの中断やネットワークの問題が発生することはありませんが、すべての GM がの再登録が発生します。

ステップ 2 **show crypto gdoi ks coop identifier [detail]**

例：

```
Device# show crypto gdoi ks coop identifier detail

COOP-KS Sender ID (SID) Information for Group diffint:

    Local KS Role: Primary   , Local KS Status: Alive
        Local Address                : 10.0.8.1
        Next SID Client Operation    : NOTIFY
        reinitializing              : No
        KSSID Overlap                : No
        SID Length (Group Size) Cfg  : 24 bits (medium)
        SID Length (Group Size) Used : 24 bits (medium)
        Current KSSID In-Use         : 0
        KSSID (or SIDS)Assigned            : 0-15
        KSSID (or SIDS)Used                : 0
        Old KSSID (or SIDS)Used            : none

    Peer KS Role:  Secondary , Peer KS Status:  Alive
        Peer Address                 : 10.0.9.1
        Next SID Client Operation    : NOTIFY
        reinitializing              : No
        KSSID Overlap                : No
        SID Length (Group Size) Cfg  : 24 bits (medium)
        SID Length (Group Size) Used : 24 bits (medium)
        Current KSSID In-Use         : 16
        KSSID (or SIDS)Assigned            : 16-31
        KSSID (or SIDS)Used                : 16
        Old KSSID (or SIDS)Used            : none
```

このコマンドは、連携 KS 全体で同期化された SID のステータス情報を表示します。

KSSID Overlap フィールドに Yes が表示されると、KSSID の重複（ネットワークの分割時に発生することがあります）が解決するまで GM 登録がブロックされます。GM 登録を再開するには、1 つの連携 KS またはほかの KS から重複している KSSID を構成解除する必要があります。重複する KSSID が解決すると、再初期化が発生します。

グループ サイズを変更すると（ほとんどの導入では推奨されません）、すべてのセカンダリ KS で最初に新しいグループ サイズを設定する必要があります。次にプライマリ KS で、SID Length (Group Size) Cfg フィールドに、すべての連携 KS ピアの新しいグループ サイズが表示されます。プライマリ KS で新しいグループ サイズを設定したときのみ、すべての KS が新しいグループ サイズの使用を開始し、SID Length (Group Size) Used フィールドを更新して新しいグループ サイズを表示します。

ステップ 3 **show crypto gdoi feature suite-b**

例：

```
Device# show crypto gdoi feature suite-b

Group Name: diffint
    Key Server ID       Version   Feature Supported
        10.0.8.1         1.0.4          Yes
        10.0.9.1         1.0.4          Yes

    Group Member ID     Version   Feature Supported
        10.0.3.1         1.0.4          Yes
        10.0.4.1         1.0.4          Yes
```

このコマンドは、KS および GM が スイート B 機能セット（つまり、AES-GCM、AES-GMAC、SHA-2、および HMAC-SHA2）を使用できるかどうかを表示します。Version フィールドが 1.0.4 またはそれ以上を表示し、Feature Supported フィールドが連携 KS グループ内のすべての KS、および登録されている GM について Yes を表示する必要があります。

ステップ 4 **show crypto gdoi ks policy**

例：

```
Device# show crypto gdoi ks policy

Key Server Policy:
For group diffint (handle: 2147483650) server 10.0.8.1 (handle: 2147483650):

  # of teks : 4  Seq num : 0
  KEK POLICY (transport type : Unicast)
    spi : 0x80474E999FE8F60364B7F51809E28C84
    management alg     : disabled    encrypt alg       : 3DES
    crypto iv length   : 8           key size          : 24
    orig life(sec): 86400       remaining life(sec): 85586
    sig hash algorithm : enabled     sig key length    : 162
    sig size           : 128
    sig key name       : mykeys

  TEK POLICY (encaps : ENCAPS_TUNNEL)
    spi                : 0x9C666FA7
    access-list        : gcm-acl
    Selector           : permit ip host 10.0.1.1 host 239.0.1.1
    transform          : esp-gcm
    alg key size       : 20            sig key size          : 0
    orig life(sec)     : 900           remaining life(sec)   : 87
    tek life(sec)      : 900           elapsed time(sec)     : 813
    override life (sec): 0             antireplay window size: 64


  TEK POLICY (encaps : ENCAPS_TUNNEL)
    spi                : 0x54E8D5D3
    access-list        : gcm-acl
    Selector           : permit ip host 10.0.100.2 host 238.0.1.1
    transform          : esp-gcm
    alg key size       : 20            sig key size          : 0
    orig life(sec)     : 900           remaining life(sec)   : 87
    tek life(sec)      : 900           elapsed time(sec)     : 813
    override life (sec): 0             antireplay window size: 64



  TEK POLICY (encaps : ENCAPS_TUNNEL)
    spi                : 0xC8B4DE6D
    access-list        : gcm-acl
```

```
    Selector           : permit ip host 10.0.1.1 host 10.0.100.2
    transform          : esp-gcm
    alg key size       : 20            sig key size          : 0
    orig life(sec)     : 900           remaining life(sec)   : 87
    tek life(sec)      : 900           elapsed time(sec)     : 813
    override life (sec): 0             antireplay window size: 64


  TEK POLICY (encaps : ENCAPS_TUNNEL)
    spi                : 0x1C908AF3
    access-list        : gcm-acl
    Selector           : permit ip host 10.0.100.2 host 10.0.1.1
    transform          : esp-gcm
    alg key size       : 20            sig key size          : 0
    orig life(sec)     : 900           remaining life(sec)   : 87
    tek life(sec)      : 900           elapsed time(sec)     : 813
```

このコマンドは、TEK および IPSec SA が ESP-GCM または ESP-GMAC の TEK ポリシーの access-list フィールド内の ACL から（Selector フィールドに表示される）ACE ごとに生成されているかどうかを表示します。またこのコマンドは、KEK ポリシーが署名ハッシュ アルゴリズムとして SHA-2/HMAC-SHA-2 を使用しているかどうかも表示します。

GM 上のスイート B での GET VPN のサポートの確認とトラブルシューティング

GM で実行されている設定を表示するには、**show running-config** コマンドを使用します。

手順の概要

1. **show crypto gdoi gm identifier** [**detail**]
2. **show crypto gdoi feature suite-b**
3. **show crypto gdoi**

手順の詳細

ステップ 1 **show crypto gdoi gm identifier** [**detail**]

例：

```
Device# show crypto gdoi gm identifier detail

GM Sender ID (SID) Information for Group diffint:

  Group Member: 10.65.9.2        vrf: None
    Transform Mode                 : Counter (Suite B)
    # of SIDs Last Requested       : 3

    CURRENT SIDs:
      Shared Across Interfaces?    : Yes
      SID Length (Group Size)      : 24 bits (medium)
      # of SIDs Downloaded          : 3
      First SID Downloaded         : 0x08000007
      Last SID Downloaded          : 0x08000009
```

```
  CM Interface   B/W (Kbps) MTU (B)  # Req # Rx  Installed SID Range
  ============== ========== ======== ===== ===== =======================
  Et2/0          10000      1500     1     3     0x08000007 - 0x08000009
  Et3/0          10000      1500     1     3     0x08000007 - 0x08000009
  Et4/0          10000      1500     1     3     0x08000007 - 0x08000009

NEXT SID REQUEST:
  TEK Lifetime                  : 900 sec
  SID Length (Group Size)       : 32 bits (LARGE)
```

このコマンドは、GM が GCM-AES または GMAC-AES を TEK IPsec SA ポリシーとして使用しているときに受信してインストールされた SID のステータスを表示します。Transform Mode フィールドでは、SID がダウンロードされ、インストールされているかどうか、およびスイート B のポリシーがグループで使用されているかどうかを確認するために、非カウンタ（非スイート B）またはカウンタ（スイート B）を表示できます。# of SIDs Last Requested フィールドは、主にこの登録されている（つまり、ローカル アドレスまたはクライアント登録インターフェイスを使用している）GM のために暗号マップが適用されるインターフェイスの数に依存します。SID は、ローカルアドレスを使用している場合は Shared Across Interfaces フィールドであり、各 CM の Installed SID Range フィールドも同じになります。このコマンドは、主に各 CM インターフェイスにインストールされている SID があることを確認するために使用します。

ステップ 2 **show crypto gdoi feature suite-b**

例：

```
Device# show crypto gdoi feature Suite B

       Version    Feature Supported
        1.0.4           Yes
```

このコマンドは、この GM がスイート B 機能セット（つまり、GCM-AES、GMAC-AES、SHA-2、および HMAC-SHA-2）を使用できるかどうかを表示します。Version フィールドが 1.0.4 またはそれ以上を表示し、Feature Supported フィールドが Yes を表示する必要があります。

ステップ 3 **show crypto gdoi**

例：

```
Device# show crypto gdoi

GROUP INFORMATION

    Group Name               : diffint
    Group Identity           : 1234
    Crypto Path              : ipv4
    Key Management Path      : ipv4
    Rekeys received          : 0
    IPSec SA Direction       : Both

     Group Server list       : 10.0.8.1

    Group member             : 10.0.3.1         vrf: None
       Version               : 1.0.4
       Registration status   : Registered
       Registered with       : 10.0.8.1
.
.
```

```
.
ACL Downloaded From KS 10.0.8.1:
   access-list   permit ip host 10.0.1.1 host 239.0.1.1
   access-list   permit ip host 10.0.100.2 host 238.0.1.1
   access-list   permit ip host 10.0.1.1 host 10.0.100.2
   access-list   permit ip host 10.0.100.2 host 10.0.1.1

KEK POLICY:
    Rekey Transport Type     : Unicast
    Lifetime (secs)          : 85740
    Encrypt Algorithm        : 3DES
    Key Size                 : 192
    Sig Hash Algorithm       : HMAC_AUTH_SHA256
    Sig Key Length (bits)    : 1024

TEK POLICY for the current KS-Policy ACEs Downloaded:
  Ethernet3/0:
    IPsec SA:
        spi: 0x318846DE(831014622)
        transform: esp-gcm
        sa timing:remaining key lifetime (sec): (86350)
        Anti-Replay(Counter Based) : 64

    IPsec SA:
        spi: 0xF367AEA0(4083658400)
        transform: esp-gcm
        sa timing:remaining key lifetime (sec): (86350)
        Anti-Replay(Counter Based) : 64

    IPsec SA:
        spi: 0xE583A3F5(3850609653)
        transform: esp-gcm
        sa timing:remaining key lifetime (sec): (86350)
        Anti-Replay(Counter Based) : 64

    IPsec SA:
        spi: 0xE9AC04C(245022796)
        transform: esp-gcm
        sa timing:remaining key lifetime (sec): (86350)
        Anti-Replay(Counter Based) : 64
```

複数の IPsec SA のプレゼンスは、GCM または GMAC が設定されていることを示します（各 IPSec SA にはダウンロードした各 ACE の固有の SPI があることに注意してください）。TEK POLICY for the current KS-Policy ACEs Downloaded セクションの TEK POLICY に記載されている各 ACE に関して、このコマンドは、TEK ポリシーおよび IPsec SA が ACL Downloaded From KS に記載されている ACL からダウンロード（およびインストール）されているかどうかを表示します。またこのコマンドは、KEK ポリシーが署名ハッシュ アルゴリズム（たとえば、HMAC_AUTH_SHA256）に SHA-2/HMAC-SHA-2 を使用しているかどうかも表示します。

スイート B での GET VPN のサポートの設定例

例：GM がスイート B をサポートするソフトウェア バージョンを実行していることを確認する

次の例は、各グループ内のすべてのデバイスがスイート B 暗号化をサポートしているかどうかを確認するために KS（またはプライマリ KS）で GET VPN ソフトウェア バージョン管理コマンドを使用する方法を示します。

```
Device# show crypto gdoi feature suite-b

Group Name: GETVPN
    Key Server ID       Version   Feature Supported
        10.0.5.2         1.0.4          Yes
        10.0.6.2         1.0.4          Yes
        10.0.7.2         1.0.3          No
        10.0.8.2         1.0.2          No

    Group Member ID     Version   Feature Supported
        10.0.1.2         1.0.2          No
        10.0.2.5         1.0.3          No
        10.0.3.1         1.0.4          Yes
        10.0.3.2         1.0.4          Yes
```

また、上記のコマンドは GM でも入力できます（その GM の情報を表示します。KS や他の GM には使用できません）。

次の例は、KS（プライマリ KS）でスイート B をサポートしていない GET VPN ネットワークのデバイスのみ検索するコマンドを入力する方法を示しています。

```
Device# show crypto gdoi feature suite-b | include No

        10.0.7.2         1.0.3          No
        10.0.8.2         1.0.2          No
        10.0.1.2         1.0.2          No
        10.0.2.5         1.0.3          No
```

例：GET VPN スイート B のキー サーバの設定

KEK の署名ハッシュ アルゴリズムの設定

次に、KEK の署名ハッシュ アルゴリズムを設定する方法の例を示します。

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group mygroup
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# rekey sig-hash algorithm sha512
Device(gdoi-local-server)# end
```

スイート B のグループ サイズの設定

メディアのデフォルトのグループ サイズはほとんどの導入に十分であるため、スイート B のグループ サイズの設定はオプションです。次の例は、スイート B にグループ サイズを設定する方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group mygroup
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# group size small 16
Device(gdoi-local-server)# end
```

キー サーバ識別子の設定

次の例では、KS に KSSID および KSSID の範囲を割り当てる方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group mygroup
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# identifier
Device(gdoi-local-server-id)# range 10 - 20
Device(gdoi-local-server-id)# value 0
Device(gdoi-local-server-id)# end
```

スイート B の IPsec SA の設定

次の例では、スイート B の IPsec SA を設定する方法を示します。この例では、アイデンティティ アドレスではなくアイデンティティ番号を使用します。

```
Device> enable
Device# configure terminal
Device(config)# crypto ipsec transform-set g1 esp-gcm 192
Device(config)# crypto ipsec profile profile1
Device(ipsec-profile)# set transform-set transformset1
Device(ipsec-profile)# exit
Device(config)# crypto gdoi group gdoigroupname
Device(config-gdoi-group)# identity number 3333
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# sa ipsec 1
Device(gdoi-sa-ipsec)# profile gdoi-p
Device(gdoi-sa-ipsec)# match address ipv4 102
Device(gdoi-sa-ipsec)# end
```

例：GET VPN スイート B のグループ メンバーの設定

スイート B の KEK の暗号化アルゴリズムまたはハッシュ アルゴリズムの設定

次の例は、GM によって許可される KEK のスイート B 暗号化およびハッシュ アルゴリズムの設定方法について説明します。この例では、アイデンティティ アドレスを使用します（IPv4 データ

プレーン構成とのみ互換性）。代わりにアイデンティティ番号を使用できます（IPv4 および IPv6 データ プレーン構成と互換性）。

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group gdoigroupone
Device(config-gdoi-group)# identity address ipv4 10.2.2.2
Device(config-gdoi-group)# server address ipv4 10.0.5.2
Device(config-gdoi-group)# client rekey encryption 3des-cbc aes 192 aes 256
Device(config-gdoi-group)# client rekey hash sha384
Device(config-gdoi-group)# end
```

スイート B の TEK の受け入れ可能トランスフォーム セットの設定

次の例は、データ暗号化または認証のために TEK が使用する受け入れ可能トランスフォーム セットを設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# crypto ipsec transform-set g1 esp-gcm 192
Device(cfg-crypto-trans)# exit
Device(config)# crypto gdoi group gdoigroupone
Device(config-gdoi-group)# client transform-sets g1
Device(config-gdoi-group)# end
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command References*』
IKE および IKE ポリシーの設定作業 IPsec トランスフォームの設定作業	『Internet Key Exchange for IPsec VPNs Configuration Guide, Cisco IOS Release 15.2M&T』の「Configuring Internet Key Exchange for IPsec VPNs」モジュール
エンタープライズ ネットワークの GET VPN の有効化のための基本的な導入ガイドライン	『Cisco IOS GET VPN Solutions Deployment Guide』

標準および RFC

標準/RFC	タイトル
連邦情報処理標準（FIPS）パブリケーション 140-2	『Security Requirements for Cryptographic Modules』
RFC 2401	『Security Architecture for the Internet Protocol』
RFC 4106	『The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)』
RFC 4543	『The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH』
RFC 4869	『Suite B Cryptographic Suites for IPsec』
RFC 6054	『Using Counter Modes with Encapsulating Security Payload (ESP) and Authentication Header (AH) to Protect Group Traffic』
RFC 6407	『The Group Domain of Interpretation』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

スイート B での GET VPN のサポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *18*：スイート *B* での *GET VPN* のサポートの機能情報

機能名	リリース	機能情報
スイート B での GET VPN のサポート	Cisco IOS XE Release 3.10S	スイート B での GET VPN のサポート機能では、Cisco Group Encrypted Transport（GET）VPN に対してスイート B の暗号方式セットのサポートが追加されます。スイート B は、Galois Counter Mode Advanced Encryption Standard（GCM-AES）を含む暗号化アルゴリズムとハッシュ、デジタル署名、キー交換用のアルゴリズムのセットです。IP Security（IPsec）VPN 用のスイート B は、RFC 4869 で使用法が定義されている標準です。スイート B は Cisco IPsec VPN に包括的なセキュリティ拡張機能を提供し、大規模な展開に対して追加のセキュリティを有効にします。スイート B は、リモートサイト間のワイドエリア ネットワーク（WAN）に高度な暗号化セキュリティを必要とする組織に対して推奨されるソリューションです。 次のコマンドが導入または変更されました：**client rekey hash**、**crypto key export ec**、**crypto key generate ec keysize**、**crypto key import ec**、**group size**、**identifier**、**rekey sig-hash algorithm**、**show crypto gdoi**。

第 9 章

Cisco TrustSec の IPsec インライン タギングの GET VPN サポート

Cisco TrustSec（CTS）アーキテクチャは、信頼できるネットワークデバイスのドメインを確立することによってネットワークを保護します。ネットワーク デバイスがネットワークに認証されると、クラウド内のデバイス間のリンクを使用する通信は、暗号化、メッセージ整合性チェック、およびリプレイ保護メカニズムを組み合わせることで保護されます。

CTS は認証時に取得したユーザとデバイスの ID 情報を使用して、ネットワークに進入するパケットを分類します。CTS では、ネットワークへの進入時にセキュリティ グループ タグ（SGT）を付けることで各パケットまたはフレームの分類が維持されます。これにより、パケットまたはフレームがデータ パス全体を通じて正しく識別され、セキュリティおよびその他のポリシー基準が適用されます。タグにより、スイッチやファイアウォールなどの中継ネットワークは分類に基づいてアクセス コントロール ポリシーを適用することができます。

Cisco TrustSec の IPsec インライン タギングの GET VPN サポート機能では、GET VPN インライン タギングを使用してプライベート WAN 経由で SGT 情報を伝送します。

- 機能情報の確認，218 ページ
- Cisco TrustSec 用の IPsec インライン タギングの GET VPN のサポートの前提条件，218 ページ
- Cisco TrustSec 用の IPsec インライン タギングの GET VPN のサポートの制約事項，218 ページ
- Cisco TrustSec の IPsec インライン タギングの GET VPN サポートに関する情報，219 ページ
- Cisco TrustSec の IPsec インライン タギングの GET VPN サポートの設定方法，221 ページ
- Cisco TrustSec の IPsec インライン タギングの GET VPN サポートの設定例，225 ページ
- Cisco TrustSec 用の IPsec インライン タギングの GET VPN のサポートのその他の参考資料，228 ページ
- Cisco TrustSec 用の IPsec インライン タギングの GET VPN のサポートの機能情報，229 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、『Bug Search Tool』およびご使用のプラットフォームおよびソフトウェアリリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

Cisco TrustSec 用の IPsec インライン タギングの GET VPN のサポートの前提条件

この機能を有効にするすべてのキーサーバ（KS）およびグループ メンバー（GM）で、GET VPN ソフトウェア バージョン 1.0.5 以降を実行している必要があります。この機能は、GET VPN ネットワーク内のすべてのデバイスをこの機能をサポートする GET VPN ソフトウェア バージョンにアップグレードしてから使用する必要があります。

この機能は、ネットワークのすべてのデバイスが Cisco TrustSec の IPsec インライン タギングをサポートするバージョンを実行しているかどうかを確認するために KS（またはプライマリ KS）で使用するコマンドを提供します。詳細については「GM が Cisco TrustSec の IPsec インライン タギングをサポートするソフトウェア バージョンを実行していることを確認する」セクションを参照してください。

Cisco TrustSec 用の IPsec インライン タギングの GET VPN のサポートの制約事項

- この機能は、IPv6 トラフィックをサポートしません。
- この機能は、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ、または第 2 世代シスコ サービス統合型ルータ（ISR G2）用の Cisco VPN 内部サービス モジュールのトランスポート モードをサポートしません。

Cisco TrustSec の IPsec インライン タギングの GET VPN サポートに関する情報

セキュリティ グループ タギング機能のグループ メンバー登録

KS はグループ メンバー（GM）からセキュリティ アソシエーション（SA）登録要求を受信するか、連携 KS から接続確立要求を受信すると、グループ SA が SGT インライン タギングを有効にしているかどうかを確認します。有効にしている場合、承認を得るためには、すべての GM と連携 KS が GET VPN ソフトウェア バージョン 1.0.5 以降を使用して登録する必要があります。そうでない場合、登録要求または確立要求は拒否され、KS はネットワーク管理者に通知する syslog メッセージを生成します。

セキュリティ グループ タギングが有効な SA の作成

（**tag cts sgt** コマンドを使用して）グループ SA で IPsec インライン タギングの GET VPN サポートを有効にして、（**crypto gdoi ks rekey** コマンドを使用して）キー再生成をトリガーすると、KS は互換性のあるソフトウェア バージョンを使用しないグループ内の GM および連携 KS をチェックします。見つかると、警告メッセージが表示されます。

```
WARNING for group GETVPN: some devices cannot support SGT inline tagging. Rekey can cause
traffic disruption and GM registration failures. Please check 'show crypto gdoi feature
sgt'.
Are you sure you want to proceed ? [yes/no]:
```

グループ メンバー データ プレーンのセキュリティ グループ タグの処理

出力トラフィックとは、GM の GDOI 保護インターフェイスから送信されるトラフィックです。次の表は、出力パスにおける GM の動作を示したものです。

表 *19* : セキュリティ グループ タグの出力処理

セキュリティ グループ タギングが SA で有効	CTS が SGT を提供	GM データ プレーンの動作
Yes	Yes	SGT を Cisco メタデータに追加し、暗号化
Yes	No	SGT なしで暗号化
No	Yes	SGT なしで暗号化

セキュリティ グループ タギングが SA で有効	CTS が SGT を提供	GM データ プレーンの動作
No	No	SGT なしで暗号化

入力トラフィックとは、GM の GDOI 保護インターフェイスが受信するトラフィックです。次の表は、入力パスにおける GM の動作を示したものです。

表 *20*：セキュリティ グループ タグの入力処理

セキュリティ グループ タギングが SA で有効	CTS が SGT を提供	GM データ プレーンの動作
Yes	Yes	CTS の SGT を復号して抽出
Yes	No	SGT の処理なしで復号
No	Yes	復号して SGT を無視
No	No	SGT の処理なしで復号

セキュリティ グループ タギング使用時のパケットのオーバーヘッドとフラグメンテーション

各 GDOI パケットに SGT 情報を含む Cisco メタデータが追加されるため、SGT インライン タギングではパケットのオーバーヘッドが 8 バイト（または、時間ベースのアンチリプレイを有効にすると 16 バイト）増加します。

パケットが GDOI の暗号化の前に分割される場合、各フラグメントはそれに応じた SGT 情報とともにインライン タギングされます。パケットが GDOI 暗号化の後で分割される場合、最初のフラグメントのみが SGT 情報とともにインライン タギングされます。

2 つの方法を使用してフラグメンテーションを処理できます。1 つ目の方法は、Cisco メタデータを介した SGT 情報の伝達に使用される追加分のバイトを収容して暗号化を処理しているインターフェイスで **ip mtu** コマンドを使用することです。2 つ目の方法は、GM の LAN インターフェイスで **ip tcp adjst-mss 1352** コマンドを使用することです。このコマンドにより、LAN セグメントの最終的な IP パケットは 1392 バイト未満となり、それによって SGT を伝送するための任意のオーバーヘッドと Cisco メタデータに対して 108 バイトが提供されます。

MTU の問題に関する設計の詳細については、『Group Encrypted Transport VPN (GETVPN) Design and Implementation Guide』の「Designing Around MTU Issues」のセクションを参照してください。

Cisco TrustSec の IPsec インライン タギングの GET VPN サポートの設定方法

GM が Cisco TrustSec の IPsec インライン タギングをサポートするソフトウェア バージョンを実行していることを確認する

Cisco TrustSec の IPsec インライン タギング機能は、GET VPN ネットワーク内のすべてのデバイスをこの機能をサポートする GET VPN ソフトウェア バージョンにアップグレードしてから使用する必要があります。

ネットワーク内のすべてのデバイスが Cisco TrustSec の IPsec インライン タギングをサポートすることを確認するには、KS（またはプライマリ KS）でこの作業を実行します。

手順の概要

1. **enable**
2. **showcryptogdoifeaturects-sgt**
3. **showcryptogdoifeaturects-sgt|includeNo**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showcryptogdoifeaturects-sgt** 例： `Device# show crypto gdoi feature cts-sgt`	GET VPN ネットワーク内の各 KS および GM で実行されている GET VPN ソフトウェアのバージョンを表示し、そのデバイスが Cisco TrustSec の IPsec インライン タギングをサポートしているかどうかを表示します。
ステップ 3	**showcryptogdoifeaturects-sgt|includeNo** 例： `Device# show crypto gdoi feature cts-sgt | include No`	（オプション）Cisco TrustSec の IPsec インライン タギングをサポートしていないデバイスのみ表示します。

Cisco TrustSec の IPsec インライン タギングの設定

Cisco TrustSec の IPsec インライン タギングを設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **crypto gdoi group***group-name*
4. 次のいずれかのコマンドを入力します。
   - **identitynumber***number*
   - **identityaddressipv4***address*
5. **server local**
6. **sa ipsec** *sequence-number*
7. **tag cts sgt**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gdoi group***group-name* 例： `Device(config)# crypto gdoi group GET-SGT`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。
ステップ 4	次のいずれかのコマンドを入力します。 • **identitynumber***number* • **identityaddressipv4***address*	GDOI グループ番号またはアドレスを指定します。

	コマンドまたはアクション	目的

	例：
	`Device(config-gdoi-group)# identity number 3333`
	例：
	`Device(config-gdoi-group)# identity address ipv4 10.2.2.2`	

ステップ 5	**server local** 例： `Device(config-gdoi-group)# server local`	デバイスを GDOI KS として指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 6	**sa ipsec** *sequence-number* 例： `Device(gdoi-local-server)# sa ipsec 1`	GDOI グループに使用される IPsec SA ポリシー情報を指定し、GDOI SA IPsec コンフィギュレーション モードを開始する。
ステップ 7	**tag cts sgt** 例： `Device(gdoi-sa-ipsec)# tag cts sgt`	Cisco TrustSec の IPSec インライン タギングを有効化します。
ステップ 8	**end** 例： `Device(gdoi-sa-ipsec)# end`	GDOI SA IPsec コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IPsecインラインタギングを有効にした後、キー再生成をトリガーする必要があります。詳細については「キー再生成のトリガー」セクションを参照してください。

キー再生成のトリガー

KS（またはプライマリ KS）でセキュリティ ポリシーを変更し（たとえば、DES から AES）、グローバルコンフィギュレーションモードを終了すると、ポリシーが変更され、キー再生成が必要であることを示す syslog メッセージが KS に表示されます。実行コンフィギュレーションの最新のポリシーに基づくキー再生成を送信するために、次のようにキー再生成をトリガーするコマンドを入力します。

キー再生成をトリガーするには KS（プライマリ KS）でこの作業を実行します。

手順の概要

1. **enable**
2. **cryptogdoiks** [**group***group-name*] **rekey** [**replace-now**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**cryptogdoiks** [**group***group-name*] **rekey** [**replace-now**] 例： `Device# crypto gdoi ks group mygroup rekey`	すべての GM のキー再生成をトリガーします。 オプションの **replace-now** キーワードは、各 GM の古い TEK および KEK を即時に置き換え、SA が期限切れになる前に新しいポリシーを有効にします。 （注） **replace-now** キーワードを使用すると、一時的なトラフィックの不連続を引き起こすことがあります。

例

KS に次のようにメッセージが表示されます。

```
Device# crypto gdoi ks rekey
Device#
*Jan 28 09:17:44.363: %GDOI-5-KS_SEND_UNICAST_REKEY: Sending Unicast Rekey with
policy-replace for group GET from address 10.0.8.1 with seq # 2
```

ポリシーの変更後、各 GM がこのトリガーされたキー再生成を受信すると、新しい SA（たとえば、AES 用）をインストールして、古い SA（たとえば、DES 用）のライフタイムを短縮します。各 GM はこの短縮されたライフタイムが期限切れになるまで古い SA を使用してトラフィックの暗号化および復号化を続けます。

セカンダリ KS のキー再生成をトリガーしようとすると、次のようにコマンドが拒否されます。

```
Device# crypto gdoi ks rekey
ERROR for group GET: This command must be executed on Pri-KS
```

Cisco TrustSec 用の IPsec インライン タギングの GET VPN のサポートの確認とトラブルシューティング

GM で実行されている設定を表示するには、**show running-config** コマンドを使用します。

SGT でタグ付けされたパケットの数を表示するには、次のコマンドを入力します。

```
Device# show crypto ipsec sa detail

interface: Ethernet0/0
   Crypto map tag: GET, local addr 5.0.0.2
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   Group: GET-SGT
.
.
.
#pkts tagged (send): 0, #pkts untagged (rcv): 5
```

pkts tagged (send) フィールドは、アウトバウンド方向の SGT でタグ付けされたパケットを表示します。pkts untagged (rcv) フィールドは、インバウンド方向の SGT でタグ付けされていないパケットを表示します。

Cisco TrustSec の IPsec インライン タギングの GET VPN サポートの設定例

例：GM が Cisco TrustSec の IPsec インライン タギングをサポートするソフトウェア バージョンを実行していることを確認する

次の例は、各グループ内のすべてのデバイスが Cisco TrustSec の IPsec インライン タギングをサポートしているかどうかを確認するために KS（またはプライマリ KS）で GET VPN ソフトウェア バージョン管理コマンドを使用する方法を示します。

```
Device# show crypto gdoi feature cts-sgt

Group Name: GETVPN
    Key Server ID       Version   Feature Supported
        10.0.5.2         1.0.5          Yes
        10.0.6.2         1.0.5          Yes
        10.0.7.2         1.0.3          No
        10.0.8.2         1.0.2          No

    Group Member ID     Version   Feature Supported
        10.0.1.2         1.0.2          No
        10.0.2.5         1.0.3          No
        10.0.3.1         1.0.5          Yes
        10.0.3.2         1.0.5          Yes
```

また、上記のコマンドは GM でも入力できます（その GM の情報を表示します。KS や他の GM には使用できません）。

次の例は、KS（プライマリ KS）で Cisco TrustSec の IPsec インライン タギングをサポートしていない GET VPN ネットワークのデバイスのみ検索するコマンドを入力する方法を示しています。

```
Device# show crypto gdoi feature cts-sgt | include No

        10.0.7.2         1.0.3          No
        10.0.8.2         1.0.2          No
```

```
10.0.1.2         1.0.2          No
10.0.2.5         1.0.3          No
```

例：Cisco TrustSec の IPsec インライン タギングの設定

次に、単一の GDOI グループを提供する KS 用の IPsec SA の CTS SGT インライン タギングを設定する方法の例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip access-list extended ACL-SGT
Device(config-ext-nacl)# permit ip any any
Device(config-ext-nacl)# exit
Device(config)# crypto gdoi group GET-SGT
Device(config-gdoi-group)# identity number 1
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# sa ipsec 1
Device(gdoi-sa-ipsec)# tag cts sgt
Device(gdoi-sa-ipsec)# profile gdoi-p2
Device(gdoi-sa-ipsec)# match address ipv4 ACL-SGT
Device(gdoi-sa-ipsec)# replay time window-size 100
Device(gdoi-sa-ipsec)# end
```

次に、GET VPN バージョン 1.0.5 以降 にアップグレードした GM を使用する（したがって CTS SGT インライン タギングをサポートしている）グループと、まだアップグレードしていない GM を使用するグループの、2 つのグループを設定する方法の例を示します。アップグレード済みの GM は、グループ番号 1111（小さい暗号マップ シーケンス番号）にグループ番号 2222（大きい暗号マップ シーケンス番号）とともに登録します。アップグレードしていない GM はグループ番号 2222 にのみ登録します。

この例では、2 つのサイト間のトラフィックに対して SGT タギングを設定します。**permit ip** コマンドは、2 つのサイト間の通信を許可するアクセス コントロール リスト（ACL）にアクセス コントロール エントリ（ACE）を追加します。

```
Device> enable
Device# configure terminal
Device(config)# ip access-list extended ACL_NET_AB
Device(config-ext-nacl)# permit ip 10.1.0.0 0.0.255.255 10.2.0.0 0.0.255.255
Device(config-ext-nacl)# permit ip 10.2.0.0 0.0.255.255 10.1.0.0 0.0.255.255
Device(config-ext-nacl)# exit
Device(config)# ip access-list extended ACL_ALL
Device(config-ext-nacl)# permit ip any any
Device(config-ext-nacl)# exit
Device(config)# crypto gdoi group GET1
Device(config-gdoi-group)# identity number 1111
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# rekey authentication mypubkey rsa mykey
Device(gdoi-local-server)# rekey transport unicast
Device(gdoi-local-server)# sa ipsec 1
Device(gdoi-sa-ipsec)# tag cts sgt
Device(gdoi-sa-ipsec)# profile gdoi-p2
Device(gdoi-sa-ipsec)# match address ipv4 ACL_NET_AB
Device(gdoi-sa-ipsec)# replay time window-size 100
Device(gdoi-sa-ipsec)# exit
Device(gdoi-local-server)# exit
Device(config-gdoi-group)# exit
Device(config)# crypto gdoi group GET2
Device(config-gdoi-group)# crypto gdoi group GET2
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# rekey authentication mypubkey rsa mykey
Device(gdoi-local-server)# rekey transport unicast
```

```
Device(gdoi-local-server)# sa ipsec 1
Device(gdoi-sa-ipsec)# profile gdoi-p2
Device(gdoi-sa-ipsec)# match address ipv4 ACL_ALL
Device(gdoi-sa-ipsec)# replay time window-size 100
Device(gdoi-sa-ipsec)# end
```

（注） GET VPN は、ACL あたり最大 100 の ACE をサポートします。

例：グループ メンバーのキー再生成のトリガー

GM がキー再生成のトリガーをサポートするソフトウェア バージョンを実行していることを確認する

次の例は、GET VPN ネットワークのデバイスのソフトウェアのバージョンを表示し、またポリシー変更後のキー再生成のトリガーをサポートするかどうかを表示するために、KS（またはプライマリ KS）で GET VPN ソフトウェア バージョン管理コマンドを使用する方法を示します。

```
Device# show crypto gdoi feature policy-replace

Key Server ID       Version  Feature Supported
  10.0.8.1         1.0.2          Yes
  10.0.9.1         1.0.2          Yes
  10.0.10.1        1.0.2          Yes
  10.0.11.1        1.0.2          Yes
 Group Member ID     Version  Feature Supported
  5.0.0.2          1.0.2          Yes
  9.0.0.2          1.0.1          No
```

次の例は、ポリシー交換後のキー再生成のトリガーをサポートしていないデバイスのみを検索する方法を示します。

```
Device# show crypto gdoi feature policy-replace  | include No

       9.0.0.2          1.0.1          No
```

これらのデバイスでは、プライマリ KS はポリシー交換に関する手順なしでトリガーされるキー再生成のみを送信します。したがって、GM がキー再生成を受信すると、新しい SA をインストールしますが、古い SA の有効期間は短縮しません。

キー再生成のトリガー

次の例では、ポリシー変更の実行後にキー再生成をトリガーする方法を示します。この例では、**profile gdoi-p2** コマンドで IPSec ポリシーの変更（たとえば、DES から AES）が発生します。

```
Device# configure terminal
Device(config)# crypto gdoi group GET
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# sa ipsec 1
Device(gdoi-sa-ipsec)# no profile gdoi-p
Device(gdoi-sa-ipsec)# profile gdoi-p2
Device(gdoi-sa-ipsec)# end
Device#
```

```
*Jan 28 09:15:15.527: %SYS-5-CONFIG_I: Configured from console by console
*Jan 28 09:15:15.527: %GDOI-5-POLICY_CHANGE: GDOI group GET policy has changed. Use
'crypto gdoi ks rekey' to send a rekey, or the changes will be send in the next scheduled
rekey
Device# crypto gdoi ks rekey
Device#
*Jan 28 09:17:44.363: %GDOI-5-KS_SEND_UNICAST_REKEY: Sending Unicast Rekey with
policy-replace for group GET from address 10.0.8.1 with seq # 2
```

次の例では、セカンダリ KS のキー再生成をトリガーしようとすると表示されるエラー メッセージを示します。

```
Device# crypto gdoi ks rekey

ERROR for group GET: This command must be executed on Pri-KS
```

（注） 時間ベースのアンチリプレイ（TBAR）が設定されると、キー サーバは2時間（7200秒）ごとに定期的にキー再生成をグループ メンバーに送信します。次の例では、有効期間が 8 時間（28800 秒）に設定されていますが、キー再生成タイマーは 2 時間に設定されています。

```
Device(config)# crypto ipsec profile atm-profile
Device(ipsec-profile)# set security-association lifetime seconds 28800
!
Device(ipsec-profile)# exit
Device(config)# crypto gdoi group ATM-DSL
Device(config-gdoi-group)# server local
Device(gdoi-sa-ipsec)# sa ipsec 1
!
Device(gdoi-sa-ipsec)# replay time window-size 100
```

show crypto gdoi gm replay および **show crypto gdoi ks replay** コマンドは、TBAR の情報を表示します。

Cisco TrustSec 用の IPsec インライン タギングの GET VPN のサポートのその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command References*』
エンタープライズ ネットワークの GET VPN の有効化のための基本的な導入ガイドライン	『Cisco IOS GET VPN Solutions Deployment Guide』
Cisco TrustSec の設定	『Cisco TrustSec Configuration Guide, Cisco IOS Release 15M&T』

関連項目	マニュアル タイトル
MTU の問題の迂回設計	『Group Encrypted Transport VPN (GETVPN) Design and Implementation Guide』

標準および RFC

標準/RFC	タイトル
RFC 2401	『Security Architecture for the Internet Protocol』
RFC 6407	『The Group Domain of Interpretation』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Cisco TrustSec 用の IPsec インライン タギングの GET VPN のサポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *21*：*Cisco TrustSec* 用の *IPsec* インライン タギングの *GET VPN* のサポートの機能情報

機能名	リリース	機能情報
Cisco TrustSec の IPsec インライン タギングの GET VPN サポート	Cisco IOS XE Release 3.9S	

機能名	リリース	機能情報
		Cisco TrustSec（CTS）アーキテクチャは、信頼できるネットワーク デバイスのドメインを確立することによってネットワークを保護します。ネットワーク デバイスがネットワークに認証されると、クラウド内のデバイス間のリンクを使用する通信は、暗号化、メッセージ整合性チェック、およびリプレイ保護メカニズムを組み合わせることで保護されます。 CTS は認証時に取得したユーザとデバイスの ID 情報を使用して、ネットワークに進入するパケットを分類します。CTS では、ネットワークへの進入時にセキュリティ グループ タグ（SGT）でパケットまたはフレームにタグを付けることで各パケットまたはフレームの分類が維持されます。これにより、パケットはデータ パス全体を通じて識別され、セキュリティおよびその他のポリシー基準が適用されます。タグにより、スイッチやファイアウォールなどの中継ネットワークは分類に基づいてアクセス コントロール ポリシーを適用することができます。 Cisco TrustSec の IPsec インライン タギングの GET VPN サポート機能では、GET VPN インライン タギングを使用してプライベート WAN 経由で SGT 情報を伝送します。 次のコマンドが導入または変更されました：**show crypto gdoi**、**show crypto ipsec sa**、**tag cts sgt**。

第 10 章

GETVPN GDOI バイパス

GETVPN GDOI バイパス機能では、デフォルトのグループ ドメイン オブ インタープリテーション（GDOI）バイパス暗号化ポリシーの有効化と無効化をサポートします。また、有効にすると、デフォルト GDOI バイパス暗号化ポリシーの強化もサポートされます。

- 機能情報の確認，233 ページ
- GETVPN GDOI バイパスの制約事項，234 ページ
- GETVPN GDOI バイパスに関する情報，234 ページ
- GETVPN GDOI バイパスの設定方法，235 ページ
- GETVPN GDOI バイパスの設定例，238 ページ
- GETVPN GDOI バイパスのその他の参考資料，239 ページ
- GETVPN GDOI バイパスの機能情報，240 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、『Bug Search Tool』およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

GETVPN GDOI バイパスの制約事項

キー サーバ（KS）がグループ メンバー（GM）の後ろに配置されるときは、ローカルの拒否アクセス コントロール リスト（ACL）を明示的に設定し、トランスポート プロトコルとして UDP を、送信元または宛先のいずれかとしてポート 848 を使用するトラフィック（UDP 848 トラフィック）が通過できるようにする必要があります。

GETVPN GDOI バイパスに関する情報

GDOI バイパス暗号化ポリシー

Cisco IOS の Group Encrypted Transport VPN（GETVPN）は、グループはキー管理プロトコルとしてグループ ドメイン オブ インタープリテーション（GDOI）を使用します。

グループ メンバー（GM）は暗号化と復号を担当するデバイスです。つまり、GET VPN データ プレーンを処理するデバイスです。

キー サーバ（KS）は、GET VPN コントロール プレーンを作成し、維持するデバイスです。トラフィック、暗号化プロトコル、セキュリティ アソシエーション、キー再生成タイマーなどのすべての暗号化ポリシーは KS で一元的に定義され、登録時にすべての GM にプッシュされます。

デフォルト GDOI バイパス暗号化ポリシーの有効化と無効化

新しいグループ メンバー（GM）設定では、GM ローカル アクセス コントロール リスト（ACL）を明示的に設定することによって、ユーザはグループ ドメイン オブ インタープリテーション（GDOI）バイパス暗号化ポリシーを無効にし、トラフィックの例外を制御することができます。

デフォルト GDOI バイパス暗号化ポリシーの強化

セキュリティを強化するため、デフォルトのグループ ドメイン オブ インタープリテーション（GDOI）バイパス暗号化ポリシーを適用する一方、次の変更が実施されています。

- デフォルト GDOI バイパス暗号化ポリシーは、Group Encrypted Transport VPN（GETVPN）保護インターフェイス（GDOI 暗号マップが適用されるインターフェイス）にのみインストールされます。登録またはキー再生成に使用するグループ メンバー（GM）のアドレス宛ての UDP848 トラフィックのみが許可されます。
- GM VRF 認識型機能を使用して GDOI データ プレーンとコントロール プレーンが異なる VRF にあることを指定する場合、デフォルト GDOI バイパス暗号化ポリシーの自動挿入は GDOI 保護インターフェイスに適用されません。

- UDP をトランスポート プロトコルとして、ポート 848 を送信元または宛先（UDP 848 トラフィック）として使用するトラフィックが他の非 GDOI 保護インターフェイスに着信すると予想される場合は、非 GDOI 暗号マップの例外を明示的に設定する必要があります。
- 複数グループの暗号マップ セットを設定する場合、インストールされる全体の GDOI バイパス暗号化ポリシーは、セキュリティ アソシエーション データベース（SADB）内の各グループの GDOI バイパス暗号化ポリシーすべての統合です。

以下に説明する条件のいずれかにより、GETVPN 保護インターフェイスに適用されるデフォルト GDOI バイパス暗号化ポリシーの再計算がトリガーされます。

- **no client bypass-policy** コマンドを使用した **client bypass-policy** 設定の削除。
- インターフェイスの GDOI バイパス暗号マップの適用または削除。
- 暗号マップ セットの GDOI バイパス暗号マップの適用または削除。
- GDOI 保護インターフェイスの IP アドレスの変更（**no client registration interface** が使用される場合）。
  - **client registration interface** が使用される場合、次の場合に GETVPN 保護インターフェイスに適用されるデフォルト GDOI バイパス暗号化ポリシーの再計算がトリガーされます。
    - **no client registration interface** から **client registration interface** への変更
    - クライアント登録インターフェイスに対する変更（たとえば、ループバック 0 からループバック 1）
    - クライアント登録インターフェイス アドレスの変更

GETVPN GDOI バイパスの設定方法

デフォルト GDOI バイパス暗号化ポリシーの有効化

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group***group-name*
4. **client bypass-policy**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gdoi group***group-name* 例： `Device(config)# crypto gdoi group GETVPN`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。
ステップ 4	**client bypass-policy** 例： `Device(config-gdoi-group)# client bypass-policy`	デフォルト GDOI バイパス暗号化ポリシーを有効化します。
ステップ 5	**end** 例： `Device(config-gdoi-group)# end`	GDOI グループ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

デフォルト GDOI バイパス暗号化ポリシーの無効化

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group***group-name*
4. **no client bypass-policy**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gdoi group***group-name* 例： `Device(config)# crypto gdoi group GETVPN`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。
ステップ 4	**no client bypass-policy** 例： `Device(config-gdoi-group)# no client bypass-policy`	デフォルト GDOI バイパス暗号化ポリシーを無効にします。
ステップ 5	**end** 例： `Device(config-gdoi-group)# end`	GDOI グループ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

デフォルト GDOI バイパス暗号化ポリシーの有効性と無効性の確認

手順の概要

1. **enable**
2. **show crypto gdoi gm acl**
3. **show crypto gdoi gm acl**

手順の詳細

ステップ 1 **enable**

特権 EXEC モードをイネーブルにします。

• パスワードを入力します（要求された場合）。

例：

```
Device> enable
```

ステップ 2 **show crypto gdoi gm acl**

デフォルト GDOI バイパス暗号化ポリシーの有効性を確認します。

（注） VRF は、非グローバルである場合にのみ表示されます。

例：

```
Device# show crypto gdoi gm acl

Group Name: GETVPN
 ACL Downloaded From KS 10.0.0.2:
   access-list   deny eigrp any any
   access-list   permit ip any any
 ACL Configured Locally:
 ACL of default GDOI bypass policy:
   Ethernet1/0: deny udp host 10.0.0.9 eq 848 any eq 848 vrf RED*
```

ステップ 3 **show crypto gdoi gm acl**

デフォルト GDOI バイパス暗号化ポリシーの無効性を確認します。

例：

```
Device# show crypto gdoi gm acl

Group Name: GETVPN
 ACL Downloaded From KS 10.0.0.2:
   access-list   deny eigrp any any
   access-list   permit ip any any
 ACL Configured Locally:
 ACL of default GDOI bypass policy: Disabled
```

GETVPN GDOI バイパスの設定例

例：デフォルト GDOI バイパス暗号化ポリシーの有効化

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group getvpn
Device(config-gdoi-group)# client bypass-policy
Device(config-gdoi-group)# end
```

例：デフォルト GDOI バイパス暗号化ポリシーの無効化

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group getvpn
```

```
Device(config-gdoi-group)# no client bypass-policy
Device(config-gdoi-group)# end
```

GETVPN GDOI バイパスのその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command References*』
エンタープライズ ネットワークの GET VPN の有効化のための基本的な導入ガイドライン	『*Cisco IOS GET VPN Solutions Deployment Guide*』
GET VPN ネットワークの設計と実装	『*Group Encrypted Transport VPN (GETVPN) Design and Implementation Guide*』

標準および RFC

標準/RFC	タイトル
RFC 6407	『*The Group Domain of Interpretation*』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

GETVPN GDOI バイパスの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *22*：***GETVPN GDOI*** バイパスの機能情報

機能名	リリース	機能情報
GETVPN GDOI バイパス	Cisco IOS XE リリース 3.13S	GETVPN GDOI バイパス機能では、デフォルトのグループ ドメイン オブ インタープリテーション（GDOI）バイパス暗号化ポリシーの有効化と無効化をサポートします。また、有効にすると、デフォルト GDOI バイパス暗号化ポリシーの強化もサポートされます。 次のコマンドが導入されました：**client bypass-policy** および **show crypto gdoi gm acl**。

第 11 章

GETVPN G-IKEv2

Cisco Group Encrypted Transport VPN（GET VPN）には、シスコ デバイス上で発生する、またはシスコ デバイスを経由するエンタープライズ プライベート WAN 上の IP マルチキャスト トラフィック グループまたはユニキャスト トラフィックの安全を守るために必要な一連の機能が含まれます。GETVPN G-IKEv2 機能は GETVPN にインターネット キー エクスチェンジ バージョン 2（IKEv2）プロトコルを実装するため、GETVPN は IKEv2 のメリットを享受できます。

- 機能情報の確認，241 ページ
- GETVPN G-IKEv2 の前提条件，242 ページ
- GETVPN G-IKEv2 の制約事項，242 ページ
- GETVPN G-IKEv2 に関する情報，242 ページ
- GETVPN G-IKEv2 の設定方法，249 ページ
- GETVPN G-IKEv2 のその他の参考資料，250 ページ
- GETVPN G-IKEv2 の機能情報，251 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、『Bug Search Tool』およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

GETVPN G-IKEv2 の前提条件

- インターネット キー エクスチェンジ バージョン 2 をデバイスで設定する必要があります。詳細については、『*FlexVPN and Internet Key Exchange Version 2 Configuration Guide*』を参照してください。

GETVPN G-IKEv2 の制約事項

- キー サーバ（KS）には Group Key Management（GKM）と Group Domain of Interpretation（GDOI）の両方を設定できますが、グループ メンバー（GM）には GKM と GDOI のいずれかを設定できます。

GETVPN G-IKEv2 に関する情報

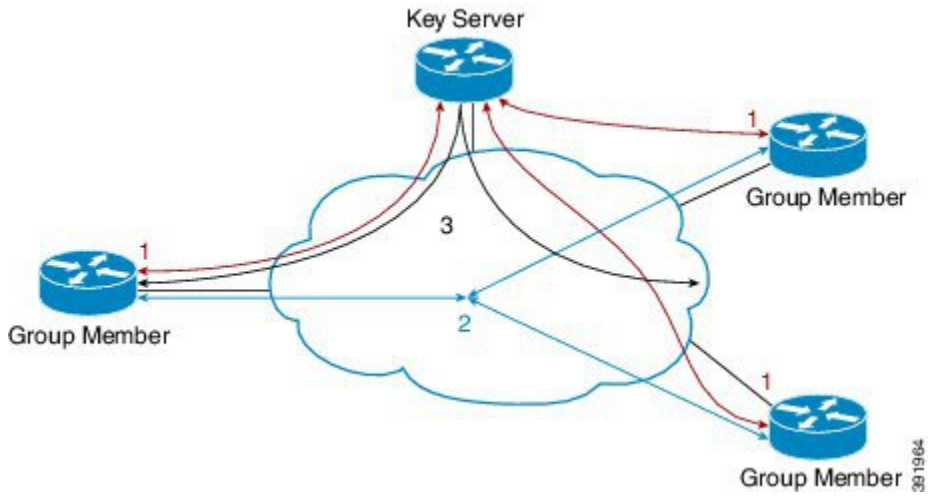
GETVPN G-IKEv2 の概要

Cisco Group Encrypted Transport バーチャル プライベート ネットワーク（GETVPN）アーキテクチャは、Group Domain of Interpretation（GDOI）プロトコルに基づいています。GETVPN では、Internet Security Exchange and Key Management Protocol（ISAKMP）を使用して、新しいグループ メンバーの認証、暗号化ポリシーのダウンロード、およびグループ メンバーへのトラフィック暗号キー（TEK）と Key Encryption Key（KEK）の配信を行います。ただし、インターネット キー エクスチェンジ バージョン 2（IKEv2）は置き換えられます。IKEv2 は、ネットワーク遅延を軽減し、メッセージ交換の複雑さを軽減し、相互運用性と信頼性を向上させ、ハッシュ認証の暗号化の問題を修正します。GET VPN は IKEv2 プロトコルと IPsec を組み合わせ、GETVPN G-IKEv2 機能によって IP マルチキャスト トラフィックまたはユニキャスト トラフィックを保護する効果的な方法を提供します。この機能では、シスコのすべての VPN Technologies を利用して完全な IKEv2 ソリューションを提供します。

G-IKEv2 プロトコルは、グループ メンバー（GM）に対し、キー サーバ（KS）からポリシーおよびキーをダウンロードするメカニズムを提供します。これらのポリシーおよびキーは、グループ内の GM 間の通信を保護するために使用されます。G-IKEv2 は、企業のプライベート WAN におけるリモート ロケーション間のグループ通信を保護する新しいモデルです。次の図は、G-IKEv2

を使用して GM を KS に登録し、KS から GM にキーおよびポリシーをダウンロードする GETVPN の基本システム アーキテクチャを示しています。

図 *15*：*G-IKEv2* プロトコルを使用する *GETVPN* アーキテクチャ



インターネット キー エクスチェンジ バージョン 2（IKEv2）

RFC 4306 に基づく次世代のキー管理プロトコルであるインターネット キー エクスチェンジ バージョン 2（IKEv2）は、IKE プロトコルの機能拡張です。IKEv2 は、相互認証の実行およびセキュリティ アソシエーション（SA）の確立および維持のために使用されます。IKEv2 の詳細については、『*FlexVPN and Internet Key Exchange Version 2 Configuration Guide*』を参照してください。

次の表では、IKE と IKEv2 間のトンネル パフォーマンスを比較します。

プロトコル	1 秒あたりのトンネル数	最大同時トンネル数
IKE	45	60
IKEv2	89	200

IKEv2 の利点は次のとおりです。

デッド ピア検出とネットワーク アドレス変換トラバーサル

インターネット キー エクスチェンジ バージョン 2（IKEv2）にはデッド ピア検出（DPD）とネットワーク アドレス変換トラバーサル（NAT-T）のサポートが組み込まれています。

証明書の URL

証明書は IKEv2 パケット内で送信されるのではなく URL とハッシュを通じて参照できるため、フラグメンテーションを回避できます。

DoS 攻撃の復元力

IKEv2 は、要求者を確認するまで要求を処理しません。これにより、偽の場所から大量の暗号化（高コスト）処理を実行するようにスプーフィングされる可能性がある IKEv1 でのサービス妨害（DoS）の問題にある程度対処しています。

EAP のサポート

IKEv2 では認証に Extensible Authentication Protocol（EAP）を使用できます。

複数の暗号エンジン

ネットワークに IPv4 と IPv6 の両方のトラフィックがあり、複数の暗号エンジンがある場合、次のいずれかの設定オプションを選択します。

- 1 つのエンジンで IPv4 トラフィックを処理し、他方のエンジンで IPv6 トラフィックを処理する。
- 1 つのエンジンで IPv4 と IPv6 の両方のトラフィックを処理する。

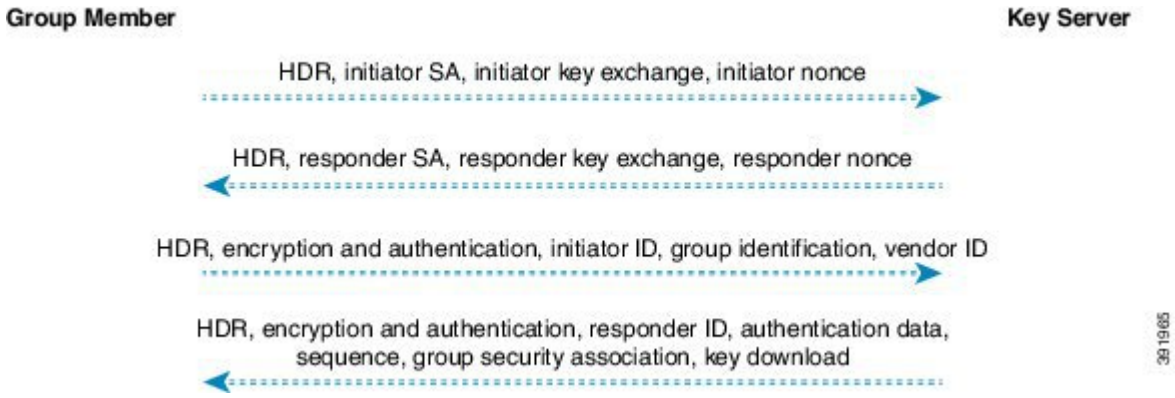
信頼性と状態管理（ウィンドウイング）

IKEv2 では、信頼性を提供するためにシーケンス番号と確認が使用され、エラー処理ロジスティックと共有状態管理が要求されます。

GETVPN G-IKEv2 の交換

GM と KS 間のメッセージ交換は、IKEv2 の標準ドラフトを使用する Internet Engineering Task Force（IETF）のグループ キー管理に準拠しています。

図 *16*：*G-IKEv2* メッセージ交換



1 グループ メンバーは、優先される暗号化アルゴリズム（SAiペイロード）、発信側のキー交換（KE）フェーズ 1 ペイロードの Diffie-Hellman 公開番号、および発信側のナンス ペイロードの存在を保証するための乱数であるナンスを送信することによってキー サーバへの登録要求を開始します。

2 キー サーバはネゴシエート済みの暗号化アルゴリズム（応答側の SA フェーズ 1 ペイロード）、Diffie-Hellman 公開番号（応答側の KE ペイロード）、ナンス（応答側のナンス ペイロード）を使用して応答します。オプションで、認証方式として Rivest、Shamir、Adleman（RSA）デジタル署名を使用するようにキー サーバが設定されている場合、キー サーバも証明書要求を送信します。

3 登録要求に対するキー サーバの応答を受信すると、グループ メンバーは SAr1 ペイロードの暗号化アルゴリズムと Diffie-Hellman 値を使用してキーを作成し、キー サーバに送信されるメッセージを暗号化します。RSA デジタル署名が認証方式として使用される場合、暗号化されたメッセージには、発信側の ID と、オプションで証明書および証明書要求が含まれます。スイート B の実装の場合、Galois/Counter Mode（GCM）–Advanced Encryption Standard（AES）または Galois Message Authentication Code（GMAC）–Advanced Encryption Standard（AES）トランスフォームとともに使用される送信者 ID を要求するために通知ペイロードが送信されます。

（注） グループ メンバーは、1 日のライフタイムの間、インターフェイスに適用可能な一連の送信元 ID を要求します。登録（長い SA ライフタイムの場合）またはキー再生成（短い SA ライフタイムの場合）のメッセージでライフタイムを受け取ると、グループ メンバーは将来の登録のため送信者 ID の数を計算するためにライフタイムを保存します。

4 グループ マネージャの認証後、キー サーバはグループ マネージャを登録する前にグループ メンバーを承認します。登録後、キー サーバはグループ マネージャにグループ ポリシー（GSA ペイロード）およびグループのキーイング マテリアル（KD ペイロード）を送信します。SEQ ペイロードはオプションであり、キー サーバでキー再生成メッセージの現在のシーケンス番号をグループ マネージャに通知する場合に送信されます。これらのペイロードは、GSA_AUTH 応答メッセージに含められます。

グループ メンバーの通信

グループ メンバーは相互に IPsec トンネルを確立するのではなく、IPsec ポリシーおよびキーを使用してグループ内のグループ メンバー間の通信を保護します。

将来の登録

セキュアな登録チャネルがグループマネージャとキーサーバとの間に確立されると、そのほかのグループの追加のグループ メンバー登録は、確立されたセキュアな登録チャネルを通じて行われます。そのようなシナリオでは、グループ メンバーはグループ ID（IDg）を含む GSA_CLIENT_SERVER 交換を使用して、キー サーバから Key Encryption Key（KEK）またはトラフィック暗号キー（TEK）のいずれかを要求します。

キー サーバのキー再生成

キー サーバはユニキャストまたはマルチキャスト通信を介して G-IKEv2 グループ メンテナンス チャネルを使用するグループ メンバーに新しいグループ キーを配布します。キー再生成は G-IKEv2 のオプションです。キー再生成を使用すると、KS はグループ メンバーにキー再生成メッセージを送信します。このメッセージはキー サーバの設定に応じてユニキャストまたはマルチキャストにできます。キー サーバでは、登録時にグループ メンバーに送信される KEK を使用してキー再

生成メッセージを暗号化します。キー再生成メッセージを受信したら、グループ メンバーは、キー再生成メッセージの SEQ 番号が最後に受信した SEQ 番号より大きいことを確認する必要があります。グループ メンバーは、どちらが後でも、登録メッセージまたはキー再生成メッセージのいずれかから SEQ 番号を受け取っているはずです。GDOI（IKEv1）と G-IKEv2 の両方のグループとしてキー サーバ グループが設定されている場合、マルチキャスト キー再生成のため、2 つのキー再生成メッセージ（GDOI 用に 1 つと G-IKEv2 用に 1 つ）が送信されます。ユニキャスト キー再生成の場合、キー サーバはグループ メンバーのモードまたはタイプに応じて GDOI または G-IKEv2 のキー再生成のみを送信します。

（注） キー再生成がユニキャストの場合、グループ メンバーはキー サーバに確認応答を送信する必要があります。

サポートされている機能および構成

GETVPN G-IKEv2 機能では、次のような既存の GETVPN 機能がサポートされています。

- キー再生成と再送信
- GM アクセス コントロール リスト（ACL）
- Fail-Close モード
- 受信専用モード
- アンチリプレイ
- グループ メンバー登録の認証ポリシー
- GDOI MIB
- VRF 認識型グループ メンバー
- グループ メンバーの削除とポリシー交換
- 連携キー サーバ
- GETVPN IPv6 データプレーン
- IPsec インライン タギングのサポート
- GETVPN の復元力のフェーズ 1 とフェーズ 2
- 連携通知メッセージの最適化

すべての GETVPN GDOI コマンド（EXEC およびグローバル コンフィギュレーション コマンド）にはキーワード **gdoi** が含まれます。G-IKEv2 には「Domain of Interpretation」が含まれないため、「グループ キー管理」を指すキーワード **gkm** を使用して、登録およびキー再生成に GDOI または GKM プロトコルを使用するグループを示します。**crypto gdoi** と **crypto gkm** の両方が、このリリースでサポートされます。ただし、**crypto gdoi** コマンドは今後廃止されます。

GDOI から G-IKEv2 への移行

長期にわたって、キー サーバとグループ メンバーを G-IKEv2 にアップグレードして移行することを希望している場合があります。GETVPN グループ全体の GDOI から G-IKEv2 への移行には、慎重な計画が必要です。すべてのグループ メンバーを同時に移行することはできません。移行では、GDOI グループ メンバーと G-IKEv2 グループ メンバーが、GDOI と G-IKEv2 の異なるコントロールプレーンプロトコルを使用する一方で、同じトラフィック暗号キー（TEK）を使用した通信を可能にする必要があります。GDOI から G-IKEv2 への移行の順番は次のとおりです。

- 後方互換性：GETVPN G-IKEv2 機能を含む新しい Cisco IOS ソフトウェア イメージでは既存の GDOI 機能をサポートしている必要があり、Cisco IOS ソフトウェアの以前のリリースの GDOI 機能との互換性が必要です。
- サービス アップグレード：Cisco IOS ソフトウェア イメージを変更する推奨順序は、セカンダリ キー サーバ、プライマリ キー サーバ、およびグループ メンバーです。
- サービス ダウングレード：Cisco IOS ソフトウェア イメージを変更する推奨順序は、グループ メンバー、セカンダリ キー サーバ、プライマリ キー サーバです。

サービス アップグレード手順

1. 既存のキーサーバとグループメンバーのGDOI設定を保存します。詳細については、『*Managing Configuration Files Configuration Guide*』の「Configuration Replace and Configuration Rollback」機能モジュールを参照してください。
2. キー サーバの移行中のネットワーク分割およびマージを防ぐため、すべてのキー サーバで Key Encryption Key（KEK）とトラフィック暗号キー（TEK）のライフタイムを設定します。新しいライフタイムを設定するには、crypto gdoi ks rekey コマンドを使用します。
3. 新しい Cisco IOS ソフトウェア イメージにキー サーバをアップグレードします。上記の順序に従います。セカンダリ キー サーバから開始し、プライマリ キー サーバに続きます。キーワード **gdoi** を使用するすべての既存の設定がキーワード **gkm** に変換されます。たとえば、グローバル コンフィギュレーション コマンド **crypto gdoi group** は **crypto gkm group** コマンドに変換されます。ただし、再登録とキー再生成にはグループは引き続き GDOI を使用します。
4. キー サーバで、GDOI および G-IKEv2 グループ メンバーをサポートするグループに対してサーバ ローカル コマンドの **gikev2** コマンドを実行します。
5. 新しい Cisco IOS ソフトウェア イメージにグループ メンバーをアップグレードします。キーワード「**gdoi**」を使用するすべての既存の設定がキーワード **gkm** に変換されます。たとえば、グローバル設定コマンド **crypto gdoi group** および **crypto map gdoi** は「**crypto gkm group**」および **crypto map gkm** にそれぞれ変換されます。これらのグループは再登録とキー再生成には GDOI を引き続き使用し、**client protocol gdoi** コマンドを含めます。
6. グループ メンバーで G-IKEv2 を使用するには、**client protocol gikev2** コマンドを設定します。
7. GDOI グループ メンバーへのサービスを停止するには、サーバのローカル コマンドの **no gdoi** コマンドを設定します。

G-IKEv2 へのアップグレード後に GDOI を使用するグループ メンバーに対して、グループ メンバー グループ設定の **client protocol gdoi** コマンドを設定します。グループ メンバーは G-IKEv2 の代わりに GDOI を使用してキー サーバに再度登録します。

（注） グループ メンバーを変換する前に、グループ メンバーの登録先のキー サーバが GDOI ローカル サーバ コンフィギュレーション モードの gdoi コマンドで設定されていることを確認します。

サービス ダウングレード手順

以前に保存（アップグレード手順の前に保存）した GDOI 設定を使用し、各グループ メンバーの Cisco IOS ソフトウェアをダウングレードします。次に、キー サーバをダウングレードします。セカンダリ キーサーバから開始し、プライマリ キーサーバに続きます。詳細については、『*Managing Configuration Files Configuration Guide*』の「Configuration Replace and Configuration Rollback」機能モジュールを参照してください。

移行例

このセクションでは、GDOI から G-IKEv2 への移行の例を示します。次に、G-IKEv2 Cisco IOS ソフトウェア イメージにアップグレードした後に GDOI グループ g1 を GKM グループに変換する例を示します。Cisco IOS ソフトウェアのアップグレードの前のキー サーバ設定の例を次に示します。

```
crypto gdoi group g1
 identity 1111
 server local
  .
  .
  .
  sa ipsec 1
   profile getvpn_profile
   match address getvpn_acl
   .
   .
   .
   redundancy
   .
   .
   .
```

Cisco IOS ソフトウェアのアップグレードの後のキー サーバ設定の例を次に示します。この例では、コマンド **gdoi**、**no gikev2**、および **gikev2** が自動的に追加されます。**gikev2** コマンドは G-IKEv2 登録の受け入れを開始します。

```
crypto gkm group g1
 identity 1111
 server local
  gdoi
  no gikev2
  gikev2 ikev2_profile1
  .
  .
  .
  sa ipsec 1
   profile getvpn_profile
   match address getvpn_acl
   .
   .
```

```
 .
 redundancy
 .
 .
 .
```

Cisco IOS ソフトウェアのアップグレードの前のグループ メンバー設定の例を次に示します。

```
crypto gdoi group g1
 identity 1111
 server address ipv4 ks1
 server address ipv4 ks2

crypto map GETVPN_CM 10 gdoi
 set group g1

interface g0/0/0
 crypto map GETVPN_CM
```

Cisco IOS ソフトウェアのアップグレードの後のグループ メンバー設定の例を次に示します。この例で、コマンド **client protocol gdoi** および **client protocol gikev2** は自動的に追加されます。**client protocol gikev2** コマンドは G-IKEv2 の使用を開始します。

```
crypto gkm group g1
 identity 1111
 server address ipv4 ks1
 server address ipv4 ks2
 client protocol gdoi
 client protocol gikev2 ikev2_profile1 ] - Configure this to start using G-IKEv2

crypto map GETVPN_CM 10 gkm
 set group g1

interface g0/0/0
 crypto map GETVPN_CM
```

GETVPN G-IKEv2 の設定方法

GETVPN G-IKEv2 の設定

すべての GETVPN コマンドにキーワード **gdoi** が含まれています。G-IKEv2 にはドメイン オブ インタープリテーションが含まれていないため、登録およびキー再生成に GDOI と G-IKEv2 のいずれかのプロトコルを使用できるグループではグループ キー管理を指す全般的な短縮形 **gkm** が使用されます。このフェーズでは、**crypto gdoi** と **crypto gkm** の両方のコマンドが使用できます。ただし、**GDOI** キーワードは廃止されるため、今後は **gkm** キーワードに置き換わります。キー サーバ、グループ メンバーの設定の詳細については、『*Cisco Group Encrypted Transport VPN Configuration Guide*』の「How to Configure Cisco Group Encrypted Transport VPN」セクションを参照し、**gdoi** キーワードを **gkm** キーワードに置き換えてください。

GETVPN G-IKEv2 のその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

標準および RFC

標準/RFC	タイトル
RFC 4306	『*Internet Key Exchange (IKEv2) Protocol*』
IKEv2 を使用したグループ キー管理	『*draft-yeung-g-ikev2-07*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

GETVPN G-IKEv2 の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *23*：*GETVPN G-IKEv2* の機能情報

機能名	リリース	機能情報
GETVPN G-IKEv2	Cisco IOS XE リリース 3.14S	Cisco Group Encrypted Transport VPN（GET VPN）には、シスコ デバイス上で発生する、またはシスコ デバイスを経由するエンタープライズプライベート WAN 上の IP マルチキャスト トラフィック グループまたはユニキャスト トラフィックの安全を守るために必要な一連の機能が含まれます。GETVPN G-IKEv2 機能は GETVPN にインターネット キー エクスチェンジ バージョン 2（IKEv2）プロトコルを実装するため、GETVPN は IKEv2 のメリットを享受できます。 Cisco IOS XE 3.14S では、この機能は Cisco ASR 1000 シリーズ アグリゲーション サービス ルータおよび Cisco 4400 シリーズ サービス統合型ルータで導入されました。 **GDOI** キーワードを使用してサポートされるすべてのコマンドは、**gkm** キーワードを使用してサポートされます。

第 12 章

8K GM スケールの改善

8K GM スケールの改善機能では、グループ メンバー（GM）の数を 8000 まで増やすことにより、Cooperative Protocol（COOP）通知メッセージの最適化をサポートします。

- 機能情報の確認，253 ページ
- 8K GM スケールの改善 の前提条件，254 ページ
- 8K GM スケールの改善に関する情報，254 ページ
- 8K GM スケールの改善の設定方法，254 ページ
- 8K GM スケールの改善の設定例，256 ページ
- 8K GM スケールの改善のその他の参考資料，256 ページ
- 8K GM スケールの改善 の機能情報，257 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、『Bug Search Tool』およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

8K GM スケールの改善 の前提条件

特定のプロトコル バージョンをアップグレードまたはダウングレードするには、グループ メンバー（GM）間で中断のない通信を確保するため、同じポリシー、キー、および GM データベースを維持します。

8K GM スケールの改善に関する情報

8K GM スケールの改善

Cooperative Protocol Announcement（COOP ANN）メッセージには複数のクライアントがあり、各クライアントはプロトコル バージョンに関連付けられます。COOP ANN メッセージは、最大 8000 のグループ メンバー（GM）を保留にし、続いて GM ヘッダーのプロトコル バージョンが上がるように最適化されています。

この機能はまた、GM ヘッダー プロトコル バージョンのアップグレードとダウングレードもサポートします。

8K GM スケールの改善の設定方法

グループ メンバー ヘッダーのプロトコル バージョンのアップグレードとダウングレード

はじめる前に

- すべてのキー サーバ（KS）が、ネットワークを 4000 GM 以上に拡張する前に「最適化」プロトコル バージョンにアップグレードされることを確認します。
- すべてのアップグレードされた KS が、最大で 4000 GM をサポートするネットワークに縮小する前に「基本」プロトコルバージョンにダウングレードされる必要があることを確認します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group***group-name*
4. **server local**
5. 冗長性
6. **protocol version** {**base** | **optimize**}
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gdoi group***group-name* 例： `Device(config)# crypto gdoi group GETVPN`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。
ステップ 4	**server local** 例： `Device(config-gdoi-group)# server local`	ローカルに定義されているグループ サーバを特定し、GDOI のローカル サーバのコンフィギュレーション モードを開始します。
ステップ 5	冗長性 例： `Device(gdoi-local-server)# redundancy`	GDOI COOP KS コンフィギュレーション モードを開始します。 （注） ローカル サーバの送信元アドレスが定義されていることを確認します。
ステップ 6	**protocol version** {**base**	**optimize**} 例： `Device(gdoi-coop-ks-config)# protocol version optimize`	GM ヘッダーのプロトコル バージョンをアップグレードまたはダウングレードします。 • **基本**：4000 GM までの COOP ANN メッセージをサポートします。 • **最適化**：8000 GM までの COOP ANN メッセージをサポートします。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： `Device(gdoi-coop-ks-config)# end`	COOP KS コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

8K GM スケールの改善の設定例

例：グループ メンバー ヘッダーのプロトコル バージョンのアップグレード

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group getvpn
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# redundancy
Device(gdoi-coop-ks-config)# protocol version optimize
Device(gdoi-coop-ks-config)# end
```

例：グループ メンバー ヘッダーのプロトコル バージョンのダウングレード

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group getvpn
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# redundancy
Device(gdoi-coop-ks-config)# protocol version base
Device(gdoi-coop-ks-config)# end
```

8K GM スケールの改善のその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command References*』
エンタープライズ ネットワークの GET VPN の有効化のための基本的な導入ガイドライン	『*Cisco IOS GET VPN Solutions Deployment Guide*』

関連項目	マニュアル タイトル
GET VPN ネットワークの設計と実装	『*Group Encrypted Transport VPN (GETVPN) Design and Implementation Guide*』

標準および RFC

標準/RFC	タイトル
RFC 6407	『*The Group Domain of Interpretation*』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

8K GM スケールの改善 の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *24*：*8K GM* スケールの改善 の機能情報

機能名	リリース	機能情報
8K GM スケールの改善	Cisco IOS XE リリース 3.14S	8K GM スケールの改善機能では、グループメンバー（GM）の数を 8000 まで増やすことにより、Cooperative Protocol（COOP）通知メッセージの最適化をサポートします。 次のコマンドが変更されました：**protocol**。