

Cisco Firepower Management Center バージョン 7.0 から収集される Cisco Success Network テレメトリデータ

初版 : 2022 年 5 月 31 日

最終更新 : 2023 年 8 月 16 日

Cisco Secure Firewall Management Center から収集される Cisco Success Network テレメトリデータ

Cisco Success Network では、登録済み FMC はリアルタイムの設定と動作の状態に関する情報を Cisco Success Network Cloud に継続的にストリーミングすることができます。このドキュメントでは、収集およびモニターされるデータのリストを示します。

登録済みデバイス データ

Cisco Success Network に FMC を登録したら、登録済みの FMC デバイスに関する選択したテレメトリデータが Cisco Cloud へストリーミングされます。次の表に、登録済みのデバイスに関して収集し、監視しているデータを示します。このデータには、侵入ポリシー（システムが提供するポリシーとカスタムポリシーの両方）および登録済みの FMC のマルウェア検出に関する機能に固有の情報が含まれます。

表 1: 登録済みデバイスのテレメトリ データ

データ ポイント	値の例
デバイス名 (Device Name)	Management Center East
デバイス UUID	24fd0ccf-1464- 491f-a503- d241317bb327
デバイス モデル	Cisco Firepower Management Center for VMWare
シリアル番号 (Serial Number)	9AMDESQP6UN
システム稼働時間 (System Uptime)	99700000
製品 ID (Product Identifier)	FS-VMW-SW-K9
スマート ライセンス PIID	24fd0ccf-1464- 491f-a503- d241317bb327

データ ポイント	値の例
仮想アカウント識別子	CiscoSVStemp
スマートライセンスバーチャルアカウント名	FTD-ENG-SJC
有効な SSO の数。	1
SSO ユーザーの数。	2
SSO アイデンティティプロバイダー。	okta
FMC の SecureX 機能が有効かどうか。	1
SSE プロキシ (LocalAPIApplication) を介してアクセスされる FMC API URL はどれか。	/api/local/fmc_config/v1/domain/{domainUUID}/object/networks
SSE プロキシ (LocalAPIApplication) 経由でアクセスされた FMC API の数。	4

ソフトウェアバージョンデータ

Cisco Success Network は、ソフトウェアのバージョン、ルールの更新バージョン、地理位置情報データベースのバージョン、脆弱性データベースのバージョン情報など、登録済みの FMC デバイスに関連するソフトウェア情報を収集します。次の表に、登録済みのデバイスに関して収集し、監視しているソフトウェア情報を示します。

表 2: ソフトウェアバージョンのテレメトリ データ

データ ポイント	値の例
FMC ソフトウェアバージョン	{ type: "SOFTWARE", version: "x.x.x.x" }
ルールの更新バージョン	{ version: "2016-11-29-001-vrt", lastUpdated: 1468606837000 }
脆弱性データベース (VDB) のバージョン	{ version: "271", lastUpdated: 1468606837000 }
地理的位置情報データベースのバージョン	{ version: "850" }

管理対象デバイス データ

Cisco Success Network は、登録済み FMC に関連付けられているすべての管理対象デバイスに関する情報を収集します。次の表に、管理対象デバイスに関して収集し、監視している情報を示します。これには、管理対象デバイスの URL フィルタリング、侵略防御、およびマルウェア検出など、機能に固有のポリシーおよびライセンス情報が含まれます。

表 3: 管理対象デバイスのテレメトリ データ

データ ポイント	値の例
管理対象デバイス名。	firepower
管理対象デバイスバージョン。	6.2.3-10616
管理対象デバイスマネージャ。	FMC
管理対象デバイスモデル。	Cisco Firepower 2130 NGFW アプライアンス Cisco FTD VMware
管理対象デバイスのシリアル番号。	9AMDESQP6UN
管理対象デバイスの PID。	FPR2130-NGFW-K9 NGFWv
Snort エンジン。	SNORT3
データの取得に失敗した場合の localUrlCount プラグインのエラー。	"errors": ["Ping DB trial no. 1 ", "SF::SFDBI::ping", "Ping returned 1", "Can't call method \"getPayload\" on an undefined value at /usr/local/sf/lib/perl/5.10.1/SF/CSMAgent.pm line 1906.", "", "Printing stack trace:", " called from /usr/local/sf/lib/perl/5.10.1/SF/CSMAgent. pm (1906)", " called from /usr/local/sf/lib/perl/5.10.1/SF/SSE/devices _plug.pm (409)", " called from /usr/local/sf/bin/devices_plug.pl (76)", " called from /usr/local/sf/bin/devices_plug.pl (93)"]
デバイスに URL フィルタリング ライセンスを使用しているか	True

データ ポイント	値の例
デバイスごとにURLフィルタリングを使用する AC ルール。	10
URL フィルタリングライセンスを使用する URL フィルタリングでの AC ルールの数。	3
脅威ライセンスを使用する URL フィルタリングでの AC ルールの数。	3
デバイスに脅威ライセンスを使用しているか	True
AC ポリシーに侵略ルールを追加しているか	True
侵入ポリシーを使用する AC ルールの数。	10
デバイスにマルウェア ライセンスを使用しているか	True
マルウェアポリシーを使用する AC ルールの数。	10
マルウェアライセンスを使用するマルウェアポリシーでの AC ルールの数。	5
デバイスに Threat Intelligence Director (TID) を使用しているか	True
静的ルートの数。	4
VRF 数。	0
デバイスでの HA のリモート展開が試行されているかどうか。	いいえ (False)
デバイス証明書が表示されるかどうか。	いいえ (False)
管理対象デバイスに nsz 値が設定されているかどうか。	いいえ (False)
管理対象デバイスに ogs 値が設定されているかどうか。	いいえ (False)
ローカル URL 項目の数。	{ "url": "/api/local/fmc_config/v1/domain/{domainUUID}/object/networks", "count": 10}, {"url": "/api/local/fmc_platform/v1/info/serverversion", "count": 2}

次の表に、ポリシーレベルごとのすべての情報を示します。

データ ポイント	値の例
Snort2 に割り当てられたアクセスポリシーデバイスの数	1
Snort3 に割り当てられたアクセスポリシーデバイスの数	0
アクセスポリシーのカスタム IPS ポリシーの数	1
アクセスポリシーのカスタム NAP ポリシーの数	1
IPS syslog が有効かどうか。	いいえ (False)
syslog の接続先がオーバーライドされるかどうか。	いいえ (False)
親ポリシー UUID	4294967319
ポリシー UUID	4294977323
アクセスポリシーのシステム IPS ポリシーの数	0
アクセスポリシーのシステム NAP ポリシーの数	0
移行された Snort3 侵入ポリシーの数	1
失敗したポリシーの数	0
ポリシーが失敗した理由の数	該当なし
部分的に失敗したポリシーの数	0
ポリシーの部分的な失敗の理由の数	該当なし
成功したポリシーの数	1
Snort2 IPS に割り当てられたデバイスの数	0
有効なカスタムルールの数	0
設定されたダイナミックルールの数	0
Firepower 推奨事項を使用するかどうか	いいえ (False)
グローバルしきい値が無効かどうか	いいえ (False)

データ ポイント	値の例
グローバルしきい値が更新されているかどうか	いいえ (False)
Snort2 IPS 親ポリシー UUID	abba00a0-cf29-425c-9d75-49699aac898
Snort2 IPS ポリシー UUID	0e6aa778-69f2-11eb-8e9e-6475e0e0131b
機密データ検出が有効かどうか	いいえ (False)
SNMP 対応ルールの数	0
設定された抑制ルールの数	0
設定されたしきい値ルールの数	0
合格した Snort2 IPS カスタムルールの数	1
置換を伴う Snort2 IPS カスタムルールの数	1
Snort2 IPS カスタムルールの数	9
割り当て済みの Snort2 ネットワーク分析ポリシーデバイスの数	0
追加された Snort2 ネットワーク分析ポリシーカスタム インスタンスの数	該当なし
最後に変更されたタイムスタンプ	2021-02-15 14:15:50
Snort2 ネットワーク分析親ポリシー UUID	abba00a0-cf29-425c-9d75-49699aac898
Snort2 ネットワーク分析ポリシー UUID	e889a48c-6f96-11eb-969d-7075e0e0131b
Snort2 ネットワーク分析のポリシーユーザー無効インスペクタ	dns
Snort2 ネットワーク分析のポリシーユーザー編集インスペクタ	dce_rpc
Snort2 ネットワーク分析のポリシーユーザー有効インスペクタ	http_inspect、dce_rpc
Snort3 IPS に割り当てられたデバイスの数	0
有効なカスタムルールのグループの数	0
除外されたカスタムルールのグループの数	0
追加されたカスタムルールのグループの数	0

データ ポイント	値の例
Snort3 IPS ルールオーバーライドの数	0
Snort3 IPS 親ポリシー UUID	7003
Snort3 IPS ポリシー UUID	4294973084
Snort3 IPS カスタムルールのグループの数	2
Snort3 IPS カスタムルールの数	1
抑制された Snort3 IPS ルールの数	0
しきい値を持つ Snort3 IPS ルールの数	0
割り当て済みの Snort3 ネットワーク分析ポリシーデバイスの数	0
追加された Snort3 ネットワーク分析ポリシーカスタム インスタンスの数	該当なし
編集された Snort3 ネットワーク分析ポリシーデフォルト インスタンスの数	該当なし
Snort3 ネットワーク分析親ポリシー UUID	7303
Snort3 ネットワーク分析ポリシー UUID	4294978428
Snort3 ネットワーク分析のポリシーユーザー無効インスペクタ	該当なし
Snort3 ネットワーク分析のポリシーユーザー編集インスペクタ	該当なし
Snort3 ネットワーク分析のポリシーユーザー有効インスペクタ	該当なし

導入情報

展開を設定した後、影響を受けるデバイスにその変更を展開する必要があります。次の表に、影響を受けるデバイスの数と成功か失敗かの情報を含む展開のステータスなど、設定の展開に関して収集し、モニターするデータを示します。

表 4: 導入情報

データ ポイント	値の例
ジョブ ID (Job ID)	8589936079

データ ポイント	値の例
展開用に選択したデバイスの数	3
展開に失敗したデバイスの数	1
展開に成功したデバイスの数	2
終了時間 (End Time)	1523993913001
開始時間(Start Time)	1523993840445
ステータス	SUCCEEDED
ターゲット デバイスの UUID	4f14f644-41e0 -11e8-9354- cf32315d7095
展開したポリシー タイプ	NetworkDiscovery NGFWPolicy DeviceConfiguration
現在の実行で収集した最後の展開ジョブの ID	8589936079
コンテナ タイプ (スタンドアロンまたは HA ペア)	STANDALONE HAPAIR
コンテナの UUID	5e006633-30fe-11e9-8a70-cd88086eeac0
デバイス モデル	Cisco FTD for VMWare
デバイスバージョン	6.4.0
ポリシー バンドルのサイズ	3588153

TLS/SSL インспекション イベント データ

Firepower システムは、デフォルトではセキュア ソケット レイヤ (SSL) プロトコルまたはその後継である Transport Layer Security (TLS) プロトコルで暗号化されたトラフィックを検査できません。TLS/SSL インспекションを使用すると、暗号化トラフィックをインспекションを実行せずにブロックしたり、暗号化または復号されたトラフィックをアクセスコントロールを使用して検査したりできます。次の各表では、暗号化されたトラフィックについて Cisco Success Network と共有する統計情報について説明します。

ハンドシェイク プロセス

システムで TCP 接続での TLS/SSL ハンドシェイクが検出された場合、その検出されたトラフィックを復号できるかどうか判定されます。システムは、暗号化されたセッションを処理する際にトラフィックに関する詳細をログに記録します。

表 5: TLS/SSL インスペクション：ハンドシェイクのテレメトリ データ

データ ポイント	値の例
<p>システムは、トラフィックが復号できず次の状態となった場合、適用されたアクションを報告します。</p> <ul style="list-style-type: none"> • ブロック • TCP リセットによるブロック • 復号されない 	0 以上の整数値
<p>システムは、トラフィックが次の方法で復号できた場合、適用されたアクションを報告します。</p> <ul style="list-style-type: none"> • 既知の秘密キーを使用する。 • 置換キーのみを使用する。 • 自己署名証明書へ再署名する。 • サーバー証明書へ再署名する。 	0 以上の整数値
暗号化されたトラフィックをブロックするように設定された SSL ルールの数。	0 以上の整数値
暗号化されたトラフィックをブロックし、接続をリセットするように設定された SSL ルールの数。	0 以上の整数値
着信トラフィックを復号するように設定された SSL ルールの数。	0 以上の整数値
発信トラフィックを復号するように設定された SSL ルールの数。	0 以上の整数値
暗号化されたトラフィックを復号しないように設定された SSL ルールの数。	0 以上の整数値
暗号化されたトラフィックをログに記録するように設定された SSL ルールの数。	0 以上の整数値
AC ポリシーに侵入が設定されているかどうか。	いいえ (False)
侵入が設定された AC ルールの数。	0 以上の整数値

データ ポイント	値の例
Threat Intelligence Director (TID) が有効かどうか。	はい (True)
トラフィック侵入の検出と防御を実行するために脅威ライセンスが必要だった AC ルールの数。	0 以上の整数値
脅威ライセンスがトラフィック侵入の検知と防御に使用されるかどうか。	はい (True)
URL フィルタリングが設定された AC ルールの数。	0 以上の整数値
脅威ライセンスが必要な AC ルールの数。	0 以上の整数値
URL ライセンスが必要な AC ルールの数	0 以上の整数値
脅威ライセンスが URL フィルタリングに使用されるかどうか。	はい (True)
SSL ハンドシェイクメッセージを処理するように設定されたアクションの数。	0 以上の整数値

キャッシュ データ

TLS/SSL ハンドシェイクが完了すると、管理対象デバイスは暗号化セッションデータをキャッシュに保存し、それによりフルハンドシェイクを必要とせずにセッションを再開できます。管理対象デバイスもサーバー証明書データをキャッシュに保存し、それにより後続のセッションでのより速いハンドシェイクの処理が可能になります。

表 6: TLS/SSL インспекション : キャッシュのテレメトリ データ

データ ポイント	値の例
	0 以上の整数値

データ ポイント	値の例
<p>システムは暗号化されたセッションデータおよびサーバ証明書データをキャッシュし、キャッシュについて SSL 接続ごとにレポートします。具体的な内容は次のとおりです。</p> <ul style="list-style-type: none"> • SSLセッション情報がキャッシュされた回数。 • SSL証明書検証キャッシュがヒットした回数。 • SSL 証明書検証キャッシュのルックアップが失敗した回数。 • SSL 元証明書キャッシュがヒットした回数。 • SSL 元証明書キャッシュのルックアップが失敗した回数。 • SSL 再署名証明書キャッシュがヒットした回数。 • SSL 再署名証明書キャッシュのルックアップが失敗した回数。 • Client Hello ダイジェストキャッシュエントリの回数。 • Client Hello ダイジェストキャッシュが削除された回数。 • Client Hello ダイジェストキャッシュがヒットした回数。 • Client Hello ダイジェストキャッシュメモリが使用された回数。 • Client Hello ダイジェストキャッシュがヒットしなかった回数。 • エンドポイント証明書キャッシュエントリの回数。 • エンドポイント証明書キャッシュメモリが使用された回数。 • 外部証明書キャッシュエントリの回数。 • 外部証明書キャッシュメモリが使用された回数。 • 内部 CA キャッシュエントリ。 • 内部CA キャッシュメモリが使用された回数。 	

データ ポイント	値の例
<ul style="list-style-type: none"> • オブジェクト リスト キャッシュ エントリの回数。 • オブジェクト リスト キャッシュ メモリが使用された回数。 • 元の証明書キャッシュ エントリの回数。 • 元の証明書キャッシュ エントリのメモリが使用された回数。 • 元の証明書キャッシュ が削除された回数。 • 元の証明書キャッシュ がヒットした回数。 • 元の証明書キャッシュ メモリが使用された回数。 • 元の証明書キャッシュ がヒットしなかった回数。 • 再署名された証明書キャッシュ エントリの回数。 • 再署名された証明書キャッシュ エントリのメモリが使用された回数。 • 再署名された証明書キャッシュ が削除された回数。 • 再署名された証明書キャッシュ がヒットした回数。 • 再署名された証明書キャッシュ メモリが使用された回数。 • 再署名された証明書キャッシュ がヒットしなかった回数。 • サーバー名キャッシュ エントリの回数。 • サーバー名キャッシュ が削除された回数。 • サーバー名キャッシュ がヒットした回数。 • サーバー名キャッシュ メモリが使用された回数。 • サーバー名キャッシュ がヒットしなかった回数。 • セッション ID キャッシュ エントリの回数。 	

データ ポイント	値の例
<ul style="list-style-type: none"> • セッション ID キャッシュが削除された回数。 • セッション ID キャッシュがヒットした回数。 • セッション ID キャッシュメモリが使用された回数。 • セッション ID キャッシュがヒットしなかった回数 • セッション チケット キャッシュ エントリの回数。 • セッション チケット キャッシュが削除された回数。 • セッション チケット キャッシュがヒットした回数。 • セッション チケット キャッシュ メモリが使用された回数。 • セッション チケット キャッシュがヒットしなかった回数。 • SSL キャッシュ合計メモリの回数。 • SSL キャッシュ合計メモリが使用された回数。 • URL 再試行キャッシュエントリの回数。 • URL 再試行キャッシュが削除された回数。 • URL 再試行キャッシュがヒットした回数。 • URL 再試行キャッシュメモリが使用された回数。 • URL 再試行キャッシュがヒットしなかった回数。 	
<p>FMC で SSL の使用が有効になっているかどうか。</p>	<p>はい (True)</p>

証明書のステータス

システムは暗号化されたトラフィックを評価し、暗号化サーバーの証明書のステータスを報告します。

表 7: TLS/SSL インспекション : 証明書ステータスのテレメトリ データ

データ ポイント	値の例
<p>システムは暗号化されたトラフィックを暗号化サーバーの証明書ステータスに基づいて評価し、報告します。</p> <ul style="list-style-type: none"> • SSL 証明書が有効な接続の数。 • SSL 証明書の有効期限が切れている接続の数。 • SSL 証明書の発行者が無効な接続の数。 • SSL 証明書に無効な署名が含まれている接続の数。 • SSL 証明書がチェックされない接続の数。 • SSL 証明書がまだ有効になっていない接続の数。 • SSL 証明書が取り消された接続の数。 • SSL 証明書が自己署名されている接続の数。 • SSL 証明書が不明な接続の数。 	<p>0 以上の整数値</p>

失敗の理由

システムは暗号化されたトラフィックを評価し、システムがトラフィックの復号化に失敗している場合は失敗の理由を報告します。

表 8: TLS/SSL インспекション : 失敗のテレメトリデータ

データ ポイント	値の例
<p>システムは暗号化されたトラフィックを評価し、システムが次の理由のためにトラフィックの復号化に失敗している場合は失敗の理由を報告します。</p> <ul style="list-style-type: none"> • 復号エラー。 • ハンドシェイク中のポリシー判定の実行。 • ハンドシェイク前のポリシー判定の実行。 • 圧縮がネゴシエートされている。 • キャッシュされていないセッション。 • インターフェイスがパッシブモード。 • 不明な暗号スイート。 • サポートされていない暗号スイート。 	0 以上の整数値

バージョン (Version)

システムは暗号化されたトラフィックを評価し、ネゴシエートされた TLS/SSL バージョンを接続ごとに報告します。

表 9: TLS/SSL インспекション : バージョンのテレメトリ データ

データ ポイント	値の例
<p>システムは暗号化されたトラフィックを評価し、次のようなネゴシエートされたバージョンを SSL 接続ごとに報告します。</p> <ul style="list-style-type: none"> • SSLv2 のネゴシエート。 • SSLv3 のネゴシエート。 • 不明なバージョンのネゴシエート。 • TLSv1.0 のネゴシエート。 • TLSv1.1 のネゴシエート。 • TLSv1.2 のネゴシエート。 • TLSv1.3 のネゴシエート。 	0 以上の整数値

Snort 再起動データ

管理対象デバイス上の Snort プロセスと呼ばれるトラフィック インспекション エンジンが再起動すると、プロセスが再開されるまでインспекションが中断されます。ユーザー定義のアプリケーションの作成/削除を行うか、システムまたはカスタム アプリケーション デテクタを有効化/無効化すると、展開プロセスを経由することなく、ただちに Snort プロセスが再起動します。Snort プロセスの再起動が続行されていることが警告され、キャンセルが可能になります。再起動は、現在のドメインまたはそのいずれかの子ドメイン内の任意の管理対象デバイスで発生します。

表 10: Snort 再起動のテレメトリ データ

データ ポイント	値の例
カスタムアプリケーションデテクタを有効または無効にした場合の Snort 再起動の数。	0 以上の整数値
カスタムアプリケーションデテクタを作成または変更した場合の Snort 再起動の数。	0 以上の整数値

Snort3 データ

次の表に、Snort3 プロセスに関する収集およびモニター対象のデータを示します。これには、TCP/IP およびその他のネットワークプロトコルのパケット パフォーマンス モニタリングに関するセッション固有の情報が含まれます。

表 11: Snort3 テレメトリデータ

データ ポイント	値の例
キャッシュまたはフローメモリの容量がいっぱいになったためにプルーニングされたセッションの数。	0 以上の整数値
Snort がフローの開始を認識しなかったセッションの数。	0 以上の整数値
ミッドストリームを検出するセッションの数。	0 以上の整数値

データ ポイント	値の例
<p>システムは、遅延の基本レベルを決定するために使用されるパケットパフォーマンスモニタリングに関連する次のカウントを報告します。</p> <ul style="list-style-type: none"> • 合計検出時間のしきい値を超えたパケットの数。 • ルールのしきい値を超えたパケットの数。 • SSL パケットタイムアウトの数。 • 合計パケット数がモニターされる。 • 検出にかかった合計時間。 • パケットによる検出にかかった最大時間。 • ルールのしきい値を超えたルールツリーの数。 • 評価済みルールの合計数。 • 一時停止後に再度有効になったルールの数。 	0 以上の整数値
TCP セッションの最大数。	0 以上の整数値
処理された TCP データのバイト数。	0 以上の整数値
UDP セッションの最大数。	0 以上の整数値
処理された UDP データのバイト数。	0 以上の整数値
IP セッションの最大数 (ICMP/UDP/TCP 以外)。	0 以上の整数値
処理された IP データのバイト数 (ICMP/UDP/TCP 以外)。	0 以上の整数値
FTP セッションの最大数。	0 以上の整数値
処理された FTP データのバイト数	0 以上の整数値
HTTP セッションの最大数。	0 以上の整数値
SMTP セッションの最大数。	0 以上の整数値
処理された SMTP データのバイト数。	0 以上の整数値
POP セッションの最大数。	0 以上の整数値

データ ポイント	値の例
処理された POP データのバイト数	0 以上の整数値
SSH セッションの最大数。	0 以上の整数値
処理された SSH データのバイト数。	0 以上の整数値
処理された SSL パケットの数。	0 以上の整数値
無視された SSL パケットの数。	0 以上の整数値
無視された SSL セッションの数。	0 以上の整数値
SSL セッションの最大数。	0 以上の整数値
HTTP/2 セッションの最大数。	0 以上の整数値
処理された HTTP/2 データの最大バイト数 (total_bytes)。	0 以上の整数値
処理された HTTP データの最大バイト数 (total_bytes)。	0 以上の整数値
データ収集の開始時刻 (Unix エポック形式)。	整数文字列
Snort のクリーン終了リストの数。	0 以上の整数値
Snort の予期しない終了リストの数。	0 以上の整数値
Snort3 侵入ポリシーに Firepower 推奨事項が使用されるかどうか。	いいえ (False)
無効になっているルールが Snort3 侵入ポリシー推奨設定で受け入れられるかどうか。	いいえ (False)
Snort3 侵入ポリシー推奨設定が最後に更新された時刻。	1625032449791
Snort3 侵入ポリシーの推奨事項の数。	12

次の表に、Snort3 ランタイム XTLS トラフィック情報を示します。

データ ポイント	値の例
証明書 DND 判定数。	1
証明書 DR 判定数。	1
証明書 DRK 判定数。	2
証明書 DKK 判定数。	3

データ ポイント	値の例
証明書 DP 判定数。	4
Client Hello Definitive DND エントリの回数。	5
フロー オーバー サブスクリプションの数。	6
SSLv3 のネゴシエート。	7
TLSv1.0 のネゴシエート。	8
TLSv1.1 のネゴシエート。	9
TLSv1.2 のネゴシエート。	10
TLSv1.3 のネゴシエート。	11
復号された TLSv1.3 フロー。	12
esni の要求。	13
暗号のネゴシエート。	{ "TLS_RSA_WITH_AES_128_CBC_SHA": 3 }, { "TLS_RSA_WITH_AES_256_CBC_SHA": 1 }
サポートされていない暗号スイート。	{ "DHE-DSS-AES256-GCM-SHA384" }
ドロップされた暗号。	{ }
不正な証明書。	{ "www.gmail.com": 4 }, { "www.reddit.com": 3 }
不明な証明書。	{ "www.youtube.com": 4 }
不明な認証局。	{ "www.youtube.com": 4 }

次の表に、Snort3 クラッシュ情報を示します。

データ ポイント	値の例
カスタムアプリケーションディテクタのバージョン。	0 以上の整数値
データ収集ライブラリ (DAQ) のパケットトレース。	0 以上の整数値
データ収集ライブラリ (DAQ) のデータメッセージ。	0 以上の整数値
データ収集ライブラリ (DAQ) のヘッダーメッセージ。	0 以上の整数値

データ ポイント	値の例
データ収集ライブラリ (DAQ) のタイプ。	0 以上の整数値
IMS ビルド	1403
IMS バージョン	6.7.0
ISP バージョン	lsp-dev-20200710-1754
モデル	Cisco Firepower 2120 Threat Defense
モデル番号	72
NAVL バージョン	98
プロセス ID 番号 (PID)	12368
Signal	6
Snort ビルド	4.116
Snort バージョン	3.0.1
SSP ビルド	99.15.1.245
タイム スタンプ (Time Stamp)	15991116699.963031
VDB ビルド	336
VDBバージョン (VDB Version)	4.5.0

コンテキストクロス起動データ

コンテキストクロス起動機能を使用すると、FMC の外部の Web ベースのリソースにおける潜在的な脅威に関する詳細情報をすばやく検索できます。FMC のイベントビューアまたはダッシュボードのイベントから、外部リソースの関連情報を直接クリックできます。これにより、その IP アドレス、ポート、プロトコル、ドメイン、または SHA 256 ハッシュに基づいて、特定のイベントに関連するコンテキストを迅速に収集できます。

表 12: コンテキストクロス起動のテレメトリ データ

データ ポイント	値の例
FMC 上に設定されているコンテキストクロス起動リソースの数。	0 以上の整数値
FMC 上で有効になっているコンテキストクロス起動リソースの数。	0 以上の整数値

データ ポイント	値の例
ドメイン変数を含むコンテキストクロス起動インスタンスの数。	0 以上の整数値
IP 変数を含むコンテキストクロス起動インスタンスの数。	0 以上の整数値
SHA 256 変数を含むコンテキストクロス起動インスタンスの数。	0 以上の整数値
FMC 上で有効になっている Stealthwatch 設定リソースの数。	0 以上の整数値
ログホストがある Stealthwatch 設定の数。	0 以上の整数値
FMC 上のストアイベントの Stealthwatch 設定の数。	0 以上の整数値
SAL 統合ウィザードで使用されるセットアップのタイプは One Box。	0 以上の整数値
テーマのレガシーの数。	0 以上の整数値

VPN データ

次の表では、FTD デバイスに登録されているさまざまな証明書オブジェクトに関して Cisco Success Network に報告されるデータについて説明します。

表 13: VPN テレメトリデータ

データ ポイント	値の例
EST オブジェクトの証明書登録。	0 以上の整数値
手動オブジェクトの証明書登録。	
PKCS12 オブジェクトの証明書登録。	
SCEP オブジェクトの証明書登録。	
自己署名オブジェクトの証明書登録。	
証明書登録。	
証明書が登録されているデバイスの数。	

次の表に、FTD デバイスで設定されたリモートアクセス VPN ポリシーに関して Cisco Success Network と共有されるデータ（接続プロファイルやダイナミックアクセスポリシーの数など）を示します。

データ ポイント	値の例
ローカルにフォールバックする接続プロファイル。	2
ローカル認証を使用する接続プロファイル。	2
RADIUS を使用する接続プロファイル。	0 以上の整数値
レルムを使用する接続プロファイル。	1403
SAML を使用する接続プロファイル。	6.7.0
RAVPN が設定されたデバイス。	lsp-dev-20200710-1754
ロードバランシングが有効になっているデバイス。	Cisco Firepower 2120 Threat Defense
ダイナミック アクセス ポリシー。	72
ダイナミック アクセス ポリシー レコード。	98
RAVPN 接続プロファイル。	12368
RAVPN ポリシー。	6
IKEv2 を使用する RAVPN ポリシー。	4.116
SSL を使用する RAVPN ポリシー。	3.0.1

次の表に、脅威防御デバイスのさまざまなサイト間 VPN トポロジ設定に関して Cisco Success Network と共有されるデータを示します。

データ ポイント	値の例
S2S VPN が設定されたデバイス。	0 以上の整数値
証明書認証を使用する S2S IKEv1 VPN。	
証明書認証を使用する S2S IKEv2 VPN。	
S2S VPN エクストラネットエンドポイント。	
S2S VPN フルメッシュトポロジ。	
S2S VPN ハブおよびスポークトポロジ。	
S2S VPN IKEv1 トポロジ。	
S2S VPN IKEv2 トポロジ。	
S2S VPN ポイントツーポイント トポロジ。	
S2S VPN VTI トポロジ。	

テレメトリ ファイルの例

次に、FMC とその管理対象デバイスに関してポリシーと展開の情報をストリーミングするための Cisco Success Network テレメトリファイルの例を示します。

```
{
  "version" : "1.0",
  "metadata" : {
    "topic" : "fmc.telemetry",
    "contentType" : "application/json"
  },
  "payload" : {
    "recordType" : "CST_FMC",
    "recordVersion" : "7.0.0",
    "recordedAt" : 1568961395861,
    "fmc" : {
      "deviceInfo" : {
        "deviceModel" : "Cisco Firepower Management Center for VMWare",
        "deviceName" : "liverpool",
        "deviceUuid" : "c9a7877c-da65-11e9-956f-cc1767fe73df",
        "isSsoEnabled" : 1,
        "numberOfSsoUsers" : 2,
        "ssoIdentityProvider" : "okta",
        "serialNumber" : "None",
        "smartLicenseProductInstanceIdentifier" : "1077ac5d-619f-49eb-a6a9-6ad61c30a481",

        "smartLicenseVirtualAccountName" : "FTD-ENG-SJC",
        "systemUptime" : 114808000,
        "udiProductIdentifier" : "FS-VMW-SW-K9",
        "SecureX": {
          "isSecureXEnabled": 1
        }
      },
      "versions" : {
        "items" : [
```



```

    {
      "type" : "SOFTWARE",
      "version" : "6.6.0-1034"
    },
    {
      "lastUpdated" : 0,
      "type" : "SNORT_RULES_DB",
      "version" : "2019-08-12-001-vrt"
    },
    {
      "lastUpdated" : 1568847127000,
      "type" : "VULNERABILITY_DB",
      "version" : "309"
    },
    {
      "type" : "GEOLOCATION_DB",
      "version" : "None"
    }
  ]
},
"managedDevices" : {
  "items" : [
    {
      "deviceInfo" : {
        "deviceManager" : "FMC",
        "deviceModel" : "Cisco Firepower 4125 Threat Defense",
        "deviceName" : "192.168.1.165",
        "deviceVersion" : "6.6.0-1034",
        "serialNumber" : "FCH22197RU0"
      },
      "malware" : {
        "malwareLicenseUsed" : true,
        "numberOfACRulesNeedMalwareLicense" : 0,
        "numberOfACRulesWithMalware" : 0
      },
      "sslCacheStats" : {
        "clientHelloDigestCacheEntries" : 3,
        "clientHelloDigestCacheEvicted" : 0,
        "clientHelloDigestCacheHit" : 7,
        "clientHelloDigestCacheMemoryUsed" : 720460,
        "clientHelloDigestCacheMiss" : 7,
        "endpointCertCacheEntries" : 0,
        "endpointCertCacheMemoryUsed" : 960,
        "externalCertCacheEntries" : 0,
        "externalCertCacheMemoryUsed" : 960,
        "internalCACacheEntries" : 1,
        "internalCACacheMemoryUsed" : 1049,
        "objectListCacheEntries" : 2,
        "objectListCacheMemoryUsed" : 1278,
        "originalCertCacheEntries" : 3,
        "originalCertCacheEntriesMemoryUsed" : 9120,
        "originalCertCacheEvicted" : 0,
        "originalCertCacheHit" : 7,
        "originalCertCacheMemoryUsed" : 80460,
        "originalCertCacheMiss" : 0,
        "resignedCertCacheEntries" : 3,
        "resignedCertCacheEntriesMemoryUsed" : 4270,
        "resignedCertCacheEvicted" : 0,
        "resignedCertCacheHit" : 14,
        "resignedCertCacheMemoryUsed" : 720484,
        "resignedCertCacheMiss" : 2,
        "serverNameCacheEntries" : 6,
        "serverNameCacheEvicted" : 0,

```

```

"serverNameCacheHit" : 14,
"serverNameCacheMemoryUsed" : 16731,
"serverNameCacheMiss" : 0,
"sessionIDCacheEntries" : 1,
"sessionIDCacheEvicted" : 0,
"sessionIDCacheHit" : 0,
"sessionIDCacheMemoryUsed" : 720428,
"sessionIDCacheMiss" : 14,
"sessionTicketCacheEntries" : 1,
"sessionTicketCacheEvicted" : 0,
"sessionTicketCacheHit" : 0,
"sessionTicketCacheMemoryUsed" : 720393,
"sessionTicketCacheMiss" : 0,
"sslCachesTotalMemory" : 14000000,
"sslCachesTotalMemoryUsed" : 2999399,
"urlRetryCacheEntries" : 0,
"urlRetryCacheEvicted" : 0,
"urlRetryCacheHit" : 0,
"urlRetryCacheMemoryUsed" : 16176,
"urlRetryCacheMiss" : 0
},

snort3RuntimeStatistics: {
  "sessionStatistics": {
    "midStreamSessions": 2,
    "prunedSessions": 9,
    "maxTCPSessions": 1045,
    "tcpDataBytesProcessed": 2558555,
    "maxUDPSessions": 450,
    "udpDataBytesProcessed": 332458,
    "maxIPSessions": 227,
    "ipDataBytesProcessed": 221084
  },
  "snortLatency": {
    "packetTimeout": 4,
    "totalPacketsMonitored": 4009872,
    "totalTimeSpentInDetection": 322456620,
    "maximumTimeSpent": 3345,
    "totalNumberRulesEvaluated": 2047,
    "rulesExceededLatency": 2,
    "rulesReenabled": 2
  },
  "ftpStatistics": {
    "maxFTPSessions": 422,
    "ftpDataBytesProcessed": 399212
  },
  "httpStatistics": {
    "maxHTTPSessions": 536
  },
  "smtpStatistics": {
    "maxSMTPSessions": 215,
    "smtpDataBytesProcessed": 23342
  },
  "popStatistics": {
    "maxPOPSessions": 205,
    "popDataBytesProcessed": 22311
  },
  "sshStatistics": {
    "maxSshSessions": 57,
    "sshDataBytesProcessed": 108715
  },
  "sslStatistics": {
    "packetsProcessed": 20312,

```

```

        "sessionsIgnored": 5,
        "maxSslSessions": 35
    }
    "snortExitStatistics": {
        "cleanExits": 0,
        "unexpectedExits": 3
    },
    "snortCrashInfoStatistics": [
        {
            "appid_version": "75",
            "backtrace": [
                "#0 0x14c2b7c206d0 in nanosleep+0x40 (/lib64/libpthread.so.0
@0x14c2b7c0f000)",
                "#1 0x55f2d78079f9
(/ngfw/var/sf/detection_engines/c976095a-d89c-11ea-a29b-d7a1e06ce5bc/snort3
@0x55f2d772c000)",
                "#2 0x14c2b72940ab in __libc_start_main+0xeb (/lib64/libc.so.6
@0x14c2b7270000)",
                "#3 0x55f2d781caaa in _start+0x2a
(/ngfw/var/sf/detection_engines/c976095a-d89c-11ea-a29b-d7a1e06ce5bc/snort3
@0x55f2d772c000)"
            ],
            "daq_msg_data_len": 0,
            "daq_msg_header_len": 0,
            "daq_msg_type": 0,
            "ims_build": "1973",
            "ims_version": "6.7.0",
            "lsp_version": "lsp-dev-20200807-1948",
            "model": "Cisco Firepower Threat Defense for VMWare",
            "model_number": "75",
            "navl_version": "99",
            "pid": 32070,
            "signal": 6,
            "snort_build": "4.107",
            "snort_version": "3.0.1",
            "ssp_build": "99.15.1.222",
            "timestamp": "1597033269.500086",
            "vdb_build": "337",
            "vdb_version": "4.5.0"
        }
    ]
},
"sslUsage" : {
    "isSslEnabled" : true
},
"ssl_rules_counter" : {
    "block" : {
        "apps" : 0,
        "cert_statuses" : 0,
        "cipher_suites" : 0,
        "decryption_certs" : 0,
        "dst_networks" : 0,
        "dst_services" : 0,
        "dst_zones" : 0,
        "external_certs" : 0,
        "issuer_dns" : 0,
        "logging" : 1,
        "replace_public_key" : 0,
        "src_networks" : 0,
        "src_services" : 0,
        "src_zones" : 0,
        "ssl_versions" : 0,
        "subject_dns" : 0,
        "urls" : 0,
    }
}

```

```

        "users" : 0,
        "vlan_tags" : 0
    },
    "block_with_reset" : {
        "apps" : 0,
        "cert_statuses" : 0,
        "cipher_suites" : 0,
        "decryption_certs" : 0,
        "dst_networks" : 0,
        "dst_services" : 0,
        "dst_zones" : 0,
        "external_certs" : 0,
        "issuer_dns" : 0,
        "logging" : 0,
        "replace_public_key" : 0,
        "src_networks" : 0,
        "src_services" : 0,
        "src_zones" : 0,
        "ssl_versions" : 0,
        "subject_dns" : 0,
        "urls" : 0,
        "users" : 0,
        "vlan_tags" : 0
    },
    "decrypt_known_key" : {
        "apps" : 0,
        "cert_statuses" : 0,
        "cipher_suites" : 0,
        "decryption_certs" : 0,
        "dst_networks" : 0,
        "dst_services" : 0,
        "dst_zones" : 0,
        "external_certs" : 0,
        "issuer_dns" : 0,
        "logging" : 0,
        "replace_public_key" : 0,
        "src_networks" : 0,
        "src_services" : 0,
        "src_zones" : 0,
        "ssl_versions" : 0,
        "subject_dns" : 0,
        "urls" : 0,
        "users" : 0,
        "vlan_tags" : 0
    },
    "decrypt_resign" : {
        "apps" : 0,
        "cert_statuses" : 0,
        "cipher_suites" : 0,
        "decryption_certs" : 0,
        "dst_networks" : 0,
        "dst_services" : 0,
        "dst_zones" : 0,
        "external_certs" : 0,
        "issuer_dns" : 0,
        "logging" : 0,
        "replace_public_key" : 0,
        "src_networks" : 0,
        "src_services" : 0,
        "src_zones" : 0,
        "ssl_versions" : 0,
        "subject_dns" : 0,
        "urls" : 0,
        "users" : 0,
    }
}

```

```

        "vlan_tags" : 0
    },
    "do_not_decrypt" : {
        "apps" : 0,
        "cert_statuses" : 0,
        "cipher_suites" : 0,
        "decryption_certs" : 0,
        "dst_networks" : 0,
        "dst_services" : 0,
        "dst_zones" : 0,
        "external_certs" : 0,
        "issuer_dns" : 0,
        "logging" : 0,
        "replace_public_key" : 0,
        "src_networks" : 0,
        "src_services" : 0,
        "src_zones" : 0,
        "ssl_versions" : 0,
        "subject_dns" : 0,
        "urls" : 0,
        "users" : 0,
        "vlan_tags" : 0
    },
    "monitor" : {
        "apps" : 0,
        "cert_statuses" : 0,
        "cipher_suites" : 0,
        "decryption_certs" : 0,
        "dst_networks" : 0,
        "dst_services" : 0,
        "dst_zones" : 0,
        "external_certs" : 0,
        "issuer_dns" : 0,
        "logging" : 0,
        "replace_public_key" : 0,
        "src_networks" : 0,
        "src_services" : 0,
        "src_zones" : 0,
        "ssl_versions" : 0,
        "subject_dns" : 0,
        "urls" : 0,
        "users" : 0,
        "vlan_tags" : 0
    }
},
"threat" : {
    "acPolicyHasIntrusion" : false,
    "acRulesWithIntrusion" : 0,
    "isTIDEnabled" : true,
    "numberOfACRulesNeedThreatLicense" : 0,
    "threatLicenseUsed" : true
},
"urlFiltering" : {
    "acRulesWithURLFiltering" : 0,
    "numberOfACRulesNeedThreatLicense" : 0,
    "numberOfACRulesNeedURLLicense" : 0,
    "urlFilteringLicenseUsed" : true
}
}
]
},
"deploymentData" : { },
"analysis" : {
    "crossLaunchInfo" : {

```

```

    "count" : 28,
    "enabledCount" : 28,
    "iocInfo" : [
      {
        "domain" : 10,
        "ip" : 9,
        "sha256" : 9
      }
    ]
  },
  "stealthwatchConfig" : {
    "crossLaunchEnabled" : 1
  }
},
"theme" : {
  "legacy" : 1
},
"SSLStats" : {
  "action" : {
    "block" : 0,
    "block_with_reset" : 0,
    "decrypt_resign_self_signed" : 0,
    "decrypt_resign_self_signed_replace_key_only" : 0,
    "decrypt_resign_signed_cert" : 887,
    "decrypt_with_known_key" : 0,
    "do_not_decrypt" : 0
  },
  "cache_status" : {
    "cached_session" : 60,
    "cert_validation_cache_hit" : 0,
    "cert_validation_cache_miss" : 887,
    "orig_cert_cache_hit" : 771,
    "orig_cert_cache_miss" : 0,
    "resigned_cert_cache_hit" : 887,
    "resigned_cert_cache_miss" : 17,
    "session_cache_hit" : 0,
    "session_cache_miss" : 700
  },
  "cert_status" : {
    "cert_expired" : 0,
    "cert_invalid_issuer" : 1,
    "cert_invalid_signature" : 0,
    "cert_not_checked" : 0,
    "cert_not_yet_valid" : 0,
    "cert_revoked" : 0,
    "cert_self_signed" : 0,
    "cert_unknown" : 0,
    "cert_valid" : 886
  },
  "failure_reason" : {
    "decryption_error" : 0,
    "handshake_error_before_verdict" : 0,
    "handshake_error_during_verdict" : 0,
    "ssl_compression" : 0,
    "uncached_session" : 0,
    "undecryptable_in_passive_mode" : 0,
    "unknown_cipher_suite" : 0,
    "unsupported_cipher_suite" : 0
  },
  "version" : {
    "ssl_v20" : 0,
    "ssl_v30" : 0,
    "ssl_version_unknown" : 0,
    "tls_v10" : 0,

```

```

        "tls_v11" : 0,
        "tls_v12" : 887,
        "tls_v13" : 0
    }
},
"snortRestart" : {
    "appDetectorSnortRestartCnt" : 0,
    "appSnortRestartCnt" : 0
}
},
"localUrlCount" : {
    "items": [
        {
            "url": "/api/local/fmc_config/v1/domain/{domainUUID}/object/networks",
            "count": 10
        },
        {
            "url": "/api/local/fmc_platform/v1/info/serverversion",
            "count": 2
        }
    ]
}
},
"policyData" : {
    "AccessPolicyInfo" : [
        {
            "assignedSnort2Devices" : 0,
            "assignedSnort3Devices" : 2,
            "customIpsPolicyCount" : 0,
            "customNapPolicyCount" : 0,
            "enabledIpsSyslog" : false,
            "overrideSyslogDestination" : false,
            "systemIpsPolicyCount" : 1,
            "systemNapPolicyCount" : 1
        },
        {
            "assignedSnort2Devices" : 0,
            "assignedSnort3Devices" : 0,
            "customIpsPolicyCount" : 0,
            "customNapPolicyCount" : 0,
            "enabledIpsSyslog" : false,
            "overrideSyslogDestination" : false,
            "systemIpsPolicyCount" : 1,
            "systemNapPolicyCount" : 1
        },
        {
            "assignedSnort2Devices" : 0,
            "assignedSnort3Devices" : 0,
            "customIpsPolicyCount" : 0,
            "customNapPolicyCount" : 0,
            "enabledIpsSyslog" : false,
            "overrideSyslogDestination" : false,
            "systemIpsPolicyCount" : 1,
            "systemNapPolicyCount" : 1
        },
        {
            "assignedSnort2Devices" : 0,
            "assignedSnort3Devices" : 0,
            "customIpsPolicyCount" : 0,
            "customNapPolicyCount" : 0,
            "enabledIpsSyslog" : false,
            "overrideSyslogDestination" : false,
            "systemIpsPolicyCount" : 1,
            "systemNapPolicyCount" : 1
        }
    ]
}
}

```

```

],
"MigratedSnort3IntrusionPolicyInfo" : {
  "migratedPolicies" : 0,
  "policiesFailureCount" : 0,
  "policiesFailureReason" : [
    "N/A"
  ],
  "policiesPartialFailureCount" : 0,
  "policiesPartialFailureReason" : [
    "N/A"
  ],
  "policiesSuccessCount" : 0
},
"Snort3IntrusionPolicyInfo" : {
  "Snort3IpsList" : [
    {
      "assignedSnort3Devices" : 0,
      "enabledCustomRuleGroupCount" : 0,
      "excludedRuleGroupsCount" : 0,
      "includedRuleGroupsCount" : 0,
      "overridenRules" : 2
    },
    {
      "assignedSnort3Devices" : 0,
      "enabledCustomRuleGroupCount" : 0,
      "excludedRuleGroupsCount" : 0,
      "includedRuleGroupsCount" : 0,
      "overridenRules" : 0
    }
  ],
  "customRuleGroups" : 2,
  "customRules" : 1,
  "rulesWithSuppression" : 0,
  "rulesWithThreshold" : 0
},
"Snort3NetworkAnalysisPolicyInfo" : [
  {
    "assignedSnort3Devices" : 0,
    "customInstancesAdded" : [
      "N/A"
    ],
    "defaultInstancesEdited" : [
      "N/A"
    ],
    "userDisabledInspectors" : [
      "N/A"
    ],
    "userEditedInspectors" : [
      "N/A"
    ],
    "userEnabledInspectors" : [
      "N/A"
    ]
  }
]
},
"vpnData" : {
  "certificate" : {
    "certificateEnrollmentESTObjects" : 2,
    "certificateEnrollmentManualObjects" : 0,
    "certificateEnrollmentPKCS12Objects" : 3,
    "certificateEnrollmentSCEPObjects" : 2,
    "certificateEnrollmentSelfSignedObjects" : 3,
    "certificateEnrollments" : 17,

```



```
    "devicesWithCertificateEnrollments" : 4
  },
  "remoteAccessVpn" : {
    "connectionProfilesWithFallbackToLocal" : 2,
    "connectionProfilesWithLocalAuthentication" : 2,
    "connectionProfilesWithRADIUS" : 6,
    "connectionProfilesWithRealm" : 1,
    "connectionProfilesWithSAML" : 0,
    "devicesConfiguredWithRAVPN" : 3,
    "devicesEnabledWithLoadBalancing" : 2,
    "dynamicAccessPolicies" : 2,
    "dynamicAccessPolicyRecords" : 7,
    "ravpnConnectionProfiles" : 9,
    "ravpnPolicies" : 2,
    "ravpnPoliciesWithIKEv2" : 2,
    "ravpnPoliciesWithSSL" : 2
  },
  "siteToSiteVpn" : {
    "devicesConfiguredWithS2SVpn" : 3,
    "s2sIKEv1VpnWithCertificateAuthentication" : 1,
    "s2sIKEv2VpnWithCertificateAuthentication" : 1,
    "s2sVpnExtranetEndpoints" : 6,
    "s2sVpnFullMeshTopologies" : 1,
    "s2sVpnHubAndSpokeTopologies" : 2,
    "s2sVpnIKEv1Topologies" : 4,
    "s2sVpnIKEv2Topologies" : 7,
    "s2sVpnPointToPointTopologies" : 6,
    "s2sVpnVTITopologies" : 2
  }
}
```

【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。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. 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. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.

翻訳について

このドキュメントは、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。