BEEP による設定への NETCONF アクセス

ネットワーク設定プロトコル（NETCONF）overブロック拡張可能交換プロトコル（BEEP）機能を使用して、NETCONF 上で設定変更の通知を送信できます。 通知は、設定変更が行われたことを示すイベントです。 変更には、設定の追加、削除、または修正があります。 通知は、設定操作の正常終了後に、一連の変更を示す1つのメッセージとして送信されます。変更された設定ごとに個別にメッセージを送信するわけではありません。

BEEP は、Simple Authentication and Security Layer（SASL）プロファイルを使用して既存のセキュリティ モデルに単純な直接マッピングを提供します。 また、NETCONF over BEEP は、トランスポート層セキュリティ（TLS）を使用して、サーバ認証、またはサーバ側とクライアント側での認証のうち、いずれかの認証を行う強力な暗号化メカニズムを提供することもできます。

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。 最新の警告および機能情報については、『Bug Search Tool』およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある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。

BEEP による設定への NETCONF アクセスの前提条件

NETCONF over BEEP リスナーには、Simple Authentication and Security layer（SASL）を設定する必要があります。

BEEP による設定への NETCONF アクセスの制約事項

Transport Layer Security（TLS）を使用する BEEP を設定するには、暗号イメージを実行する必要があります。

BEEP による設定への NETCONF アクセスについて

NETCONF over BEEP の概要

BEEP による設定への NETCONF アクセス機能は、BEEP を転送プロトコルとしてイネーブルにして、NETCONF セッションで使用できるようにします。 NETCONF over BEEP を使用すると、NETCONF サーバまたは NETCONF クライアントのいずれかが接続を開始するように設定できます。これによって、デバイスが断続的に接続された大規模ネットワークや、ファイアウォールおよびネットワーク アドレス変換（NAT）があるために管理接続を反転する必要のあるデバイスをサポートできます。

BEEP は、コネクション型非同期相互作用のための汎用アプリケーション プロトコル フレームワークです。 これは、従来さまざまなプロトコルの実装で何度も利用されてきた機能を提供することを目的としています。 BEEP は一般的に Transmission Control Protocol（TCP）上で動作し、メッセージの交換が可能です。 HTTP および同様のプロトコルとは異なり、接続の両端でいつでもメッセージを送信できます。 BEEP には暗号化と認証のファシリティも含まれており、高い拡張性があります。

BEEP プロトコルには、ピア同士が同時に独立してメッセージを交換できるフレーミング メカニズムが含まれています。 通常これらのメッセージは XML を使用して構成されます。 すべての交換は、転送セキュリティ、ユーザ認証、またはデータ交換などの明確に定義されたアプリケーション特性にバインドされたコンテキストで実行されます。 このバインディングによってチャネルが形成されます。各チャネルには交換されるメッセージの構文およびセマンティクスを定義する関連付けられたプロファイルがあります。

BEEP セッションは NETCONF サービスにマップされます。 セッションが確立されると、各 BEEP ピアは自身がサポートするプロファイルをアドバタイズします。 チャネルの作成中に、クライアント（BEEP イニシエータ）はそのチャネルの 1 つまたは複数のプロファイルを提示します。 サーバ（BEEP リスナー）がチャネルを作成する場合、サーバはいずれかのプロファイルを選択し、そ

のプロファイルを応答で送信します。 サーバは、どのプロファイルも受け入れできないことを示し、チャネルの作成を断る場合もあります。

BEEP では、同時に複数のデータ交換チャネルを使用できます。

BEEP はピアツーピア プロトコルですが、特定のタイミングで実行している役割に応じて、各ピアにラベルが付けられます。 BEEP セッションの確立時に、新規接続を待ち受けるピアが BEEP リスナーです。 リスナーへの接続を確立するもう一方のピアが BEEP イニシエータになります。 交換を開始する BEEP ピアがクライアントで、もう一方の BEEP ピアがサーバです。 通常、サーバの役割を実行する BEEP ピアは、リッスンする役割も実行します。 ただし、BEEP はピアツーピア プロトコルであるからといって、サーバの役割を実行する BEEP ピアが、リッスンする役割も実行する必要はありません。

NETCONF over BEEP と SASL

SASL は、接続ベースのプロトコルに認証サポートを追加するためのインターネット標準方式です。 SASL をセキュリティ アプライアンスと Lightweight Directory Access Protocol（LDAP）サーバとの間で使用してユーザ認証を保護できます。

BEEP リスナーには、SASL を設定する必要があります。

NETCONF over BEEP と TLS

TLS は、相互認証、完全性のためのハッシュの使用、プライバシー保護のための暗号化を可能にすることで、クライアントとサーバとの間にセキュアな通信を提供するアプリケーション レベルのプロトコルです。 TLS では、証明書、公開キー、および秘密キーを使用します。

証明書はデジタル ID カードに似ています。 この証明書は、クライアントに対してサーバの ID を証明します。 各証明書には、発行した機関の名前、証明書の発行先エンティティの名前、エンティティの公開キー、および証明書の有効期限を示すタイム スタンプが含まれます。

公開キーおよび秘密キーは、情報の暗号化および復号化に使用される暗号キーです。 公開キーは共有されますが、秘密キーは公開されることはありません。 公開キーと秘密キーの各ペアは一緒に動作します。 公開キーを使用して暗号化されたデータは、その秘密キーでのみ復号化できます。

NETCONF over BEEP とアクセス リスト

オプションで、NETCONF over SSHv2 セッション用のアクセス リストを設定できます。 アクセス リストは、IP アドレスに対する許可および拒否の条件を順番に並べたものです。 シスコ ソフトウェアは、アクセス リストの条件に対して、アドレスを 1 つずつテストします。 最初の一致によって、ソフトウェアがアドレスを受け入れるか、拒否するかが決まります。 最初に一致が見つかった後は条件のテストが終了するため、条件の順序は重要です。 条件が一致しなければ、アドレスは拒否されます。

アクセス リストの使用に関連する 2 つの主要な作業は次のとおりです。

1. アクセス リストの番号または名前とアクセス条件を指定して、アクセス リストを作成する。
2. アクセス リストをインターフェイスまたは端末回線に適用する。

アクセス リストの設定の詳細については、『*Security Configuration Guide: Securing the Data Plane*』の「IP Access List Overview」および「Creating an IP Access List and Applying It to an Interface」モジュールを参照してください。

BEEP による設定への NETCONF アクセスの設定方法

SASL プロファイルの設定

SASL を使用して NETCONF over BEEP をイネーブルにするには、まず SASL プロファイルを設定する必要があります。SASL プロファイルは、デバイスへのアクセスが許可されるユーザを指定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **sasl profile** *profile-name*
4. **mechanism di gest-md5**
5. **server** *user-name* **password** *password*
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	**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	**sasl profile** *profile-name* 例： `Device(config)# sasl profile beep`	SASL プロファイルを設定し、SASL 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。

	コマンドまたはアクション	目的
ステップ 4	**mechanism di gest-md5** 例： `Device(config-SASL-profile)# mechanism digest-md5`	SASL プロファイル メカニズムを設定します。
ステップ 5	**server** *user-name* **password** *password* 例： `Device(config-SASL-profile)# server user1 password password1`	SASL サーバを設定します。
ステップ 6	**exit** 例： `Device(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。

NETCONF over BEEP のイネーブル化

はじめる前に

- 同時 NETCONF セッションと同じ数以上の vty 行が設定されている必要があります。
- SASL を使用する NETCONF over BEEP を設定するには、まず SASL プロファイルを設定する必要があります。

（注）
- 4 個以上の同時 NETCONF セッションを設定する必要があります。
- 最大 16 個の同時 NETCONF セッションを設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto key generate rsa general-keys**
4. **crypto pki trustpoint** *name*
5. **enrollment url** *url*
6. **subject-name** *name*
7. **revocation-check** *method1* [*method2* [*method3*]]
8. **exit**
9. **crypto pki authenticate** *name*
10. **crypto pki enroll** *name*
11. **netconf lock-time** *seconds*
12. **line vty** line-number [*ending-line-number*]
13. **netconf max-sessions** *session*
14. **netconf beep initiator** {*hostname* | *ip-address*} *port-number* **user** *sasl-user* **password** *sasl-password*[**encrypt** *trustpoint*] [**reconnect-time** *seconds*]
15. **netconf beep listener** [*port-number*] [**acl** *access-list-number*] [**sasl** *sasl-profile*] [**encrypt** *trustpoint*]
16. **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 key generate rsa general-keys** 例： `Device(config)# crypto key generate rsa general-keys`	Rivest, Shamir, and Adelman（RSA）キー ペアを生成し、汎用のキー ペアを生成するように指定します。 この手順は一度だけ実行してください。

	コマンドまたはアクション	目的
ステップ 4	**crypto pki trustpoint** *name* 例： `Device(config)# crypto pki trustpoint my_trustpoint`	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	**enrollment url** *url* 例： `Device(ca-trustpoint)# enrollment url http://10.2.3.3:80`	認証局（CA）の登録パラメータを指定します。
ステップ 6	**subject-name** *name* 例： `Device(ca-trustpoint)# subject-name CN=dns_name_of_host.com`	証明書要求の所有者名を指定します。 （注） サブジェクト名は、デバイスのドメイン ネーム システム（DNS）名にする必要があります。
ステップ 7	**revocation-check** *method1* [*method2* [*method3*]] 例： `Device(ca-trustpoint)# revocation-check none`	証明書の失効ステータスをチェックします。
ステップ 8	**exit** 例： `Device(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 9	**crypto pki authenticate** *name* 例： `Device(config)# crypto pki authenticate my_trustpoint`	CA の証明書を取得して、認証局を認証します。
ステップ 10	**crypto pki enroll** *name* 例： `Device(config)# crypto pki enroll my_trustpoint`	ルータの証明書を CA から取得します。
ステップ 11	**netconf lock-time** *seconds* 例： `Device(config)# netconf lock-time 60`	（任意）NETCONF 設定を中間操作が行われないようにロックする最長時間を指定します。 seconds 引数の有効な値の範囲は 1 ～ 300 秒です。 デフォルト値は 10 秒です。

	コマンドまたはアクション	目的
ステップ 12	**line vty** line-number [*ending-line-number*] 例： `Device(config)# line vty 0 15`	リモート コンソール アクセスの仮想端末回線を識別します。 NETCONF セッションの最大数と同じ数の vty 回線を設定する必要があります。
ステップ 13	**netconf max-sessions** *session* 例： `Device(config)# netconf max-sessions 16`	（任意）許容される同時NETCONFセッションの最大数を指定します。
ステップ 14	**netconf beep initiator** {*hostname* | *ip-address*} *port-number* **user** *sasl-user* **password** *sasl-password*[**encrypt** *trustpoint*] [**reconnect-time** *seconds*] 例： `Device(config)# netconf beep initiator host1 23 user user1 password password1 encrypt 23 reconnect-time 60`	（任意）BEEP を NETCONF セッションの転送プロトコルとして指定し、ピアをBEEPイニシエータとして設定します。 （注） この手順は、NETCONF BEEP のイニシエータ セッションを設定する場合に実行します。 任意で、BEEP リスナー セッションを設定することもできます。
ステップ 15	**netconf beep listener** [*port-number*] [**acl** *access-list-number*] [**sasl** *sasl-profile*] [**encrypt** *trustpoint*] 例： `Device(config)# netconf beep listener 26 acl 101 sasl profile1 encrypt 25`	（任意）BEEP を NETCONF の転送プロトコルとして指定し、ピアを BEEP リスナーとして設定します。 （注） この手順は、NETCONF BEEP のリスナーセッションを設定する場合に実行します。 任意で、BEEP イニシエータ セッションを設定することもできます。
ステップ 16	**exit** 例： `Device(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。

BEEP による設定への NETCONF アクセスの設定例

例：NETCONF over BEEP のイネーブル化

```
Device# configure terminal
Device(config)# crypto key generate rsa general-keys
```

```
Device(ca-trustpoint)# crypto pki trustpoint my_trustpoint

Device(ca-trustpoint)# enrollment url http://10.2.3.3:80
Device(ca-trustpoint)# subject-name CN=dns_name_of_host.com
Device(ca-trustpoint)# revocation-check none
Device(ca-trustpoint)# crypto pki authenticate my_trustpoint

Device(ca-trustpoint)# crypto pki enroll my_trustpoint

Device(ca-trustpoint)# line vty 0 15

Device(ca-trustpoint)# exit
Device(config)# netconf lock-time 60

Device(config)# netconf max-sessions 16

Device(config)# netconf beep initiator host1 23 user my_user password my_password encrypt
my_trustpoint reconnect-time 60

Device(config)# netconf beep listener 23 sasl user1 encrypt my_trustpoint
```

BEEP による設定への NETCONF アクセスに関する追加情報

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 Commands List, All Releases』
NETCONF コマンド：コマンド構文、コマンドモード、コマンド履歴、デフォルト、使用に関する注意事項、および例	『*Cisco IOS Cisco Networking Services Command Reference*』

標準および RFC

標準/RFC	タイトル
RFC 2222	『*Simple Authentication and Security Layer (SASL)*』
RFC 3080	『*The Blocks Extensible Exchange Protocol Core*』
RFC 4741	『*NETCONF Configuration Protocol*』
RFC 4744	『*Using the NETCONF Protocol over the Blocks Extensible Exchange Protocol (BEEP)*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 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。 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

BEEP による設定への NETCONF アクセスの機能情報

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 *1*：***BEEP*** による設定への ***NETCONF*** アクセスの機能情報

機能名	リリース	機能情報
BEEP による設定への NETCONF アクセス	Cisco IOS XE Release 2.1 12.2(33)SB 12.2(33)SRB 12.2(33)SXI 12.4(9)T	NETCONF over BEEP 機能を使用すると、NETCONF サーバまたはNETCONF クライアントのどちらかが接続を開始するように設定できます。これによって、デバイスが断続的に接続された大規模ネットワークや、ファイアウォールおよび Network Address Translators（NAT）があるために管理接続を反転する必要のあるデバイスをサポートできます。 この機能により、**netconf beep initiator**、**netconf beep listener** の各コマンドが導入または変更されました。