Junos®基本シリーズ

This Week：Junosデバイスのセキュリティ強化

著者：ジョン・ウィードリー

JUNIPER NETWORKS®

発行者：Juniper Networks Books
著者：ジョン・ウィードリー
技術校閲者：トム・ヴァン・メーター、ティム・ブラウン、リチャード・ウッドマン
主編集者：パトリック・エイムズ
原稿整理・校正編集者：ナンシー・ケルベル
J-Net コミュニティ管理者：ジュリー・ワイダー

著者の紹介
ジョン・ウィードリーは、ジュニパーネットワークスのレジデントエンジニアです。ジュニパーネットワークスの JNCIS-SEC、JNCIS-SSL、JNCIA-FWV、および JNCIA-EX の有資格者であり、過去 15 年間に渡って米国政府機関をサポートしてきました。

著者の謝辞
私を辛抱強く支え、理解してくれた家族に感謝します。また、多大なる尽力、指導、激励をくれたパトリック・エイムズ氏、指導および技術校閲を担当してくれたトム・ヴァン・メーター氏、技術校閲および付録 B の執筆にあたってくれたリチャード・ウッドマン氏、土台となる全体像および技術的指導をくれたティム・ブラウン氏にも感謝します。

ISBN：978-1-936779-40-6（書籍）
印刷：Vervante Corporation（米国）

ISBN：978-1-936779-41-3（電子書籍）

改訂：初版、2011 年 12 月
2 3 4 5 6 7 8 9 10 #7100145-en

本書は、さまざまな形式で www.juniper.net/dayone から入手できます。

本書についてのご意見・ご感想は電子メールで dayone@juniper.net 宛にお寄せください。

Juniper Networks Books は、ネットワークの生産性および効率に特に重点を置いた書籍を扱っています。完全なライブラリについては、www.juniper.net/books を参照してください。

本書を読む前に

本書を読む前に、Junos OSの基本的な管理機能について理解しておいてください。例えば、オペレーションコマンド、Junosの設定を確認し、変更できるスキルが必要です。
このような基本的スキルがない場合、本書に記載されてる内容を理解できず、設定例を実際のデバイスやテスト環境にスムーズに展開できない可能性があります。

Junos CLIのスキル向上に役立つ参考資料をお探しの場合は、http://www.juniper.net/dayoneからDay Oneシリーズのブックレットをダウンロードしてください。*『Day One：JUNOS CLIの探求』*および*『Day One: Junosの基本設定』*は特にお奨めです。

*『This Week：Junosデバイスのセキュリティ強化』*は、読者に以下のネットワーキングの知識があることを前提に執筆されています。

- TCP/IPに関する知識と経験があること。
- Junos OSに関する中級レベルの知識と設定経験があること。本書では、セキュリティを強化するために、基本的な設定概念をさらに発展させています。
- ネットワーク攻撃およびセキュリティに関する基礎知識があること。
- 必須ではありませんが、Junosデバイスを使用しながら本書を読み進めると、記載されている例の設定を練習することができます。

本書の学習目標

- 組織のセキュリティ体制にとって不可欠な、デバイス管理の非技術的側面を理解する
- デバイス展開に際し、物理的セキュリティの対策が重要であること、またソフトウェア機能がデバイスのセキュリティ強化に役立つことを理解する
- ジュニパーネットワークスのデバイスに共通のOS、すなわち「One Junos」によってもたらされるメリットと、それがいかにデバイスの保護に役立つかを理解する
- Junosのセキュリティ機能とデフォルト設定が強固なセキュリティの基盤となっていることを理解する
- 必要なサービスと適切なセキュリティ対策を認識し、その対策を施すことによりどのような影響があるかを論理的に理解する
- デバイスアクセスの最適化やユーザー権限の制限といった、重要なマネジメント機能について理解する
- ルーティングプロトコルおよびシグナリングプロトコルにおいて認証を適切に設定する
- ルーティングエンジンを保護する適切なファイアウォールフィルタを作成し、適用する

はじめに

最初に、『*This Week：Junos デバイスのセキュリティ強化*』内で登場するいくつかのトピックについて明確にしておきましょう。

セキュリティポリシー

CERT.org によると、セキュリティポリシーは、どのような防御メカニズムを使用するか、サービスをどのように設定するかなど、具体策を決定するための枠組みとなるもので、セキュアプログラミングガイドラインや、ユーザーおよびシステム管理者向け手順を策定するためのベースとなります。セキュリティポリシーが明確になっていれば、それを基に、それぞれの環境に合ったセキュリティ要件を盛り込んだチェックリストを作成することができます。

言うまでもなく、セキュリティポリシーが定義され、そのポリシーに従ってデバイスの管理およびセキュリティ強化に必要な施策が定義されていれば、ネットワークデバイスの保護は大変容易になります。セキュリティポリシーがまだ策定されていない場合は、本書を読み進める前に、以下の各ポリシーで定義すべき課題について検討してください。

- パスワード複雑性ポリシー：安全だと考えられるパスワードの最小長と最大長は？また、パスワードをセキュアにするためには、数字、大文字、小文字、および特殊文字を組み合わせることが必要です。この最も基本的なレベルを軽視しないでください。
- 認証ポリシー：ローカル認証と集中認証のどちらを使用しますか？また、RADIUS と TACACS+ のどちらを使用しますか？
- アクセスポリシー：デバイスを管理するためにどのようなアクセスサービスを使用しますか（SSH、J-Web など）？すべてのアクセスサービスに暗号化は必要ですか？
- 管理ポリシー：ネットワークデバイスでサポートする必要のある管理サービスは（NTP、SNMPv1/2/3、Syslog、SSH など）？

冗長性と耐障害性

機密性、完全性および可用性の確保は情報セキュリティの中核となります。ネットワークの安定性を高め、常に状態変化に対応できる体制を整えておくことが、可用性向上につながるのです。これらの基本的な要件を満たすうえで、冗長性を備えたシステムと耐障害性を持たせた設計が大きな役割を果たします。

ですから、本書を読み終えて実際に設計を行うときは、2 台の Syslog サーバー、2 台の認証サーバー、2 台の NTP サーバーというように、常にペアで構成することで、信頼性が大幅に向上することを意識しておいてください。また、プライマリサーバーとバックアップサーバーを別々のネットワークサブネット上、別々の建物内、または別々の地理的位置に配置することにより、可用性を最大限に高めることができます。

さらに詳しくは　ネットワークを設計するときは、可用性が最大限になるよう設計してください。デバイスのクラスタリング、VRRP、LAG（Link Aggregation Group）、JSRP（Junos OS Services Redundancy Protocol）などハイアベイラビリティを提供するテクノロジーが多数あります。ハイアベイラビリティの詳細については、http://www.juniper.net/books で紹介されている、ジェイムズ・ソンデレガー、オリン・ブロムバーグ、キーラン・ミルネ、およびセナド・パリスラモビック著『*Junos High Availability*』（O’Reilly Media 発行、2009 年）を参照してください。

ジュニパーネットワークスのナレッジベース（KB）

本書では、ジュニパーネットワークスのナレッジベース（KB）がいくつか取り上げられています。多くのナレッジベースは、アクセスするためにジュニパーネットワークスのカスタマーサポートセンターのアカウントが必要です。

第1章では、ジュニパーネットワークスのカスタマーサポートセンターへのアカウント登録により得られるその他のメリットも紹介しています。

アカウントがなくても、本書を読んで知識を身に付けることができますが、セキュリティ全般およびセキュリティ強化に関するすべてを本書で説明することはできません。そのため、ナレッジベースおよびその他の関連情報を紹介し、別の機会に確認できるようにしています。

『This Week：Junos デバイスのセキュリティ強化』について

ジュニパーネットワークスは、同社製品のセキュリティを非常に重大なものとして捉えており、業界のベストプラクティスに沿った実証あるプロセスと手順を提供します。*『This Week：Junos デバイスのセキュリティ強化』*では、これらのプロセスと手順を以下のトピックに分け、4 章構成で説明します。

- ノンテクニカル情報：セキュリティを検討する以前にエンジニアが知っておくべき情報があります。第1章では、ジュニパーネットワークスの SIRT（Security Incident Response Team）およびカスタマーサポートセンター（CSC）の他、ソフトウェアのダウンロードおよび脆弱性の開示について、セキュリティ関連の重要な情報を提供します。
- 物理的セキュリティ：悪意のあるユーザーがネットワークデバイスに物理的にアクセスできる場合、そのユーザーによって引き起こされる被害に対し、ソフトウェア機能によるセキュリティ強化はまったく役に立ちません。第 2 章では、デバイスの基本的な物理的アクセスからの保護について説明します。
- OS のセキュリティ：セキュアな Junos とセキュリティを考慮したデフォルト設定は、デバイス全体のセキュリティ強化のベースになります。第 3 章では、セキュリティに関連する、Junos のデフォルトの管理、およびカーネルとネットワーク動作について説明します。
- セキュリティ強化のための設定：第 4 章では、様々な側面からデバイスを保護するための、Junos OS の機能の設定方法を説明します。

これらの 4 つの章に加え、付録では、セキュリティ体制に役立つ情報を記載しています。

- 付録 A：この付録には、本書の重要ポイントが簡易チェックリストとしてまとめられています。このチェックリストでは、やるべき項目の完了時にチェックマークを付け、実施状況を確認することができます。
- 付録 B：米国政府の APL（Approved Products List）の認定要件を満たすためにジュニパーネットワークスが取り組んでいる認定のリストです。
- 付録 C：Junos デバイスの中レベルのセキュリティ設定例を掲載します。

This Week へようこそ

This Week シリーズは、Juniper Networks Books より発行され、非常に高い評価を得ている Day One シリーズから発展した書籍です。Day One シリーズは、読者が 1 日で習得できる量の情報を提供することに重点を置いています。一方、This Week シリーズでは、ネットワーキングテクノロジーについて、講習形式であれば数日かけて習得する内容を、演習を用いながら解説するものです。どのライブラリも複数のフォーマットで形式で入手できます。

- 無料の PDF 版を http://www.juniper.net/dayone からダウンロードできます。
- iPhone および iPad 用の電子書籍版を iTunes ストア >Books から入手できます。Juniper Networks Books を検索してください。
- Kindle アプリが稼働するデバイス（Android、Kindle、iPad、PC、または Mac）用に電子書籍版があり、デバイスの Kindle アプリを起動して Kindle Store にアクセスして入手できます。Juniper Networks Books を検索してください。
- 印刷版を Vervante Corporation（www.vervante.com）または Amazon（www.amazon.com）から、ページ数に応じて $12 ～ 28 で購入することもできます。
- Nook、iPad、およびさまざまな Android アプリで、PDF ファイルを表示できます。
- ご使用のデバイスが Apple 製品でなく、電子書籍アプリが .epub ファイルを使用している場合は、iTunes を起動し、iTunes ストアから .epub ファイルをダウンロードしてください。これにより、iTunes からデスクトップにこのファイルをドラッグアンドドロップし、.epub デバイスと同期させることができます。

第1章

ノンテクニカル情報

ルーター、スイッチ、およびファイアウォールは、ネットワークにおいてそれぞれ重要な目的や役割を担っており、いずれも不可欠です。そのため、これらのデバイスは、プローブ（事前調査）、スキャン、および攻撃を受けないよう対策を施す必要があります。デバイスを保護するときは、そのネットワークが持つ目的や機能、外部からのアクセスを可能にしているサービスはどれか、エンジニアはどのようにそのデバイスにアクセスしているか、そのためにどのような権限が必要かなど、そのデバイスをあらゆる側面から捉える必要があります。

Junos デバイスのセキュリティを強化するのに、正当な接続のみを許可するファイアウォールフィルタを設定し、一部のプロトコルにレートリミットを適用し、その他すべてのトラフィックをドロップするということだけでは不十分です。確かに、ファイアウォールフィルタはセキュリティ上重要な要素ですが、破られた場合に備えて措置を講じておかなければなりません。包括的なセキュリティを実現するには、多重に防御する必要があります。

セキュリティ要件は環境によって異なるため、本書では、ネットワークに具体的にどのようなセキュリティ機能を実装すべきかについて言及しません。代わりに、Junosに組み込まれているさまざまなセキュリティ機能と設定の実装方法をご紹介し、これらの導入に関する注意点と影響について説明します。

最終的に、Junos が企業のセキュリティポリシーに準拠するようセキュリティ機能を実装するのは皆さん自身です。それでは始めましょう。

One Junos

Junos OS は、ジュニパーネットワークスのルーター、スイッチ、およびセキュリティデバイスに渡って共通の CLI を提供します。Junos は単一のソースコードとなっていますが、これは極めてユニークな特徴です。すなわち、図 1.1 に示すように、ジュニパーネットワークスのエンジニアが開発した新機能のコードは、必要に応じて、Junos OS が稼働する多数のプラットフォームで共有されます。このように単一の OS によって一貫したユーザーエクスペリエンスが提供されるため、設計が容易になり、直感的に操作することができます。さらに、デバイスのセキュリティにも一貫性を持たせることができ、変更をより迅速に反映させることができます。また、管理者は、基本的なシャーシ管理から複雑なルーティング機能まで、ネットワーク全体を監視、管理、および最適化していく中ですべてのデバイスにわたって同じツールを使うことができます。

ほとんどのデフォルト動作は、ジュニパーネットワークスの多くのプラットフォーム（J、M、MX、EX、SRX）に渡って共通です。また、本書で紹介する機能の多くは Junos のベースコードの一部であるため、Junos ベースのすべてのプラットフォームで利用することができます。ただし、掲載されている一部のコマンドは、特定のプラットフォームおよびハードウェアモジュールでのみ有効です。特定のプラットフォームで動作が異なる場合は、その旨を記載しています。

注 本書に掲載されている設定例では、さまざまなプラットフォームが使用されています。これは、One Junos であることの証明になっています。なお、設定例はすべて、Junos 10.4 でテストされています。

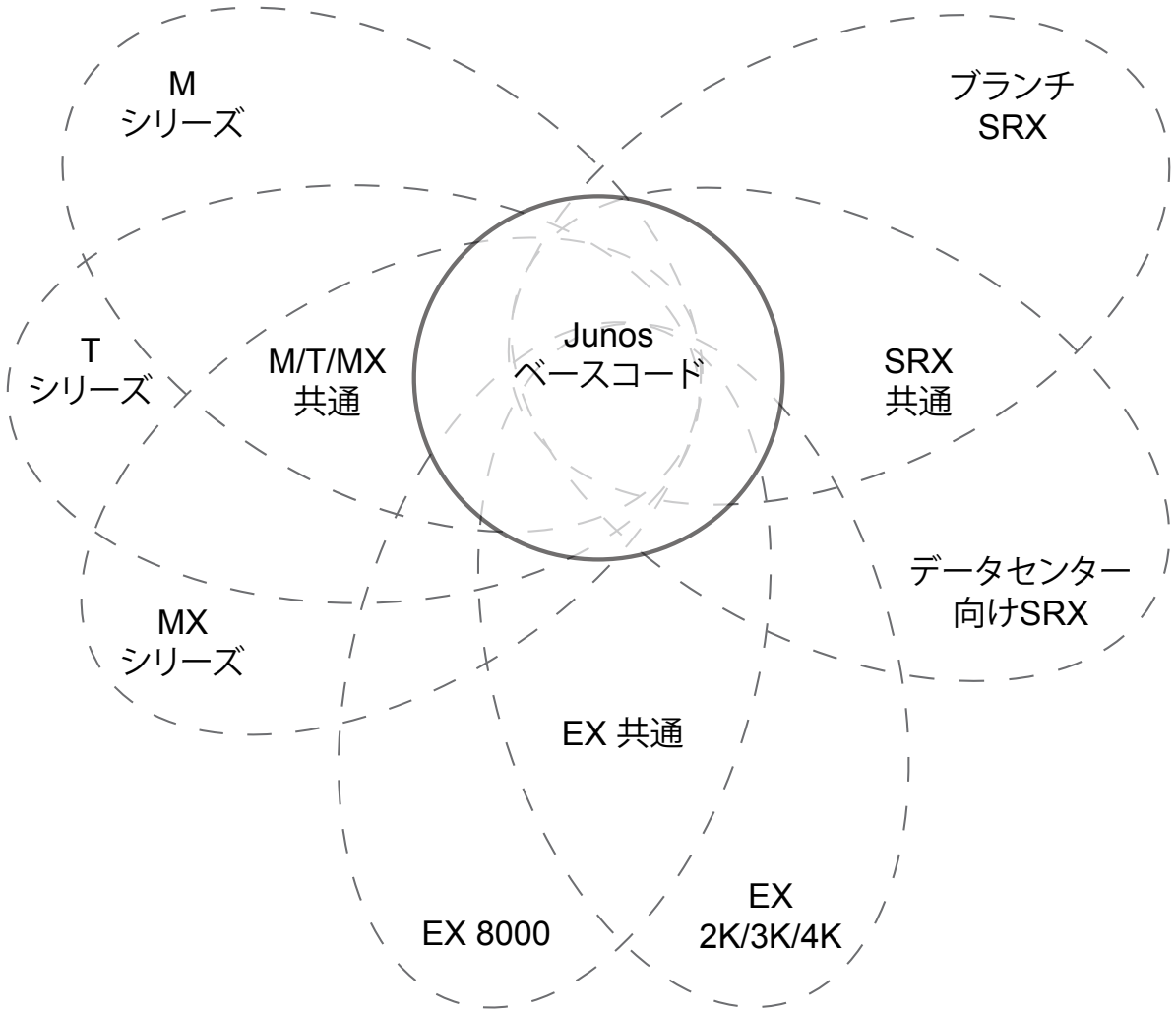

図 1.1 Junos のコードベースと各プラットフォームの関係

ジュニパーネットワークスの SIRT（Security Incident Response Team）

ジュニパーネットワークスの SIRT（Security Incident Response Team）は、ジュニパーネットワークスの製品、サービス、またはそれに関連するあらゆるセキュリティ脆弱性の対処にあたるチームです。SIRT の役割は、報告された脆弱性の対応と管理を一貫して行うことです。また、DDoS（Distributed Denial of Service）やネットワーク侵入といった問題についてもユーザーをサポートします。

SIRT は、ジュニパーネットワークスの製品、サービス、セキュリティリスクを常に正しく認識するために、運用セキュリティコミュニティ、その他の CSIRT（Computer Security Incident Response Team）、ジュニパーネットワークスのユーザーコミュニティ、およびその他メディアと連携しています。

このように各方面から得られたセキュリティ情報は精査され、より大規模な SIRT チーム、ジュニパーネットワークスの他部門、そして最終的にジュニパーネットワークスのユーザーに伝えられます。また、SIRT は、新たなベストプラクティスを作成し、ネットワーク業界のセキュリティ関連コミュニティをリードしてユーザーのネットワーク安定稼働に努めています。

セキュリティ情報の概要

ジュニパーネットワークスの SIRT は、セキュリティに関する最新情報をユーザーにお届けするために、セキュリティ情報を定期的に発行しています。SIRT セキュリティ情報は 2009 年に開始され、以下の 2 つに分類されています。

- Security Advisory には、ジュニパーネットワークス側の要因によるものか、プロトコルそのものの不備のような一般的要因によるものかに関わらず、ジュニパーネットワークスの製品またはサービスに内在する脆弱性についての情報が記載されています。
- Security Notice には、ジュニパーネットワークスの製品またはサービスの脆弱性には直接関連していなくとも、ユーザー、パートナー、および場合によっては一般の方でも注意すべき問題について記載されています。

いずれのセキュリティ情報にも、脆弱性による影響を軽減する手法についての記述が含まれる場合があります。

ヒント 脆弱性が疑われる場合、または脆弱性の影響で発生した事象が確認された場合は、http://www.juniper.net/us/en/security/report-vulnerability/ から報告してください。

権限に基づく開示

ジュニパーネットワークスは、権限に基づく開示ポリシーを実施しています。すなわち、ジュニパーネットワークスのセキュリティ情報は、ジュニパーネットワークスのカスタマーサポートウェブサイトへのアクセス権限を持つユーザーおよびパートナーのみがアクセスすることができます。ジュニパーネットワークスでは、セキュリティに関する一般向けアナウンスを行うことはなく、セキュリティ情報を一般公開することもありません。権限に基づく開示ポリシーは、セキュリティ情報をユーザーおよびパートナーに限定し、報道機関や一般の方、特に悪意のあるユーザーから遠ざけることを目的としています。

ただし、このようなプロセスが実施されているからと言って、これらの情報が機密事項であるとか、機密保持契約（NDA）の対象であるとか、または企業秘密に該当するかというと、そうではありません。むしろ、ジュニパーネットワークスの SIRT は、これらの情報が必要に応じてアクセス権限を持たない個人やグループにも広がることも想定しています。

例えば、Security Advisory の「Response to "TCP Split Handshake Attack" Vulnerability in Juniper SRX Firewalls」というタイトルのものや、PSN 番号「PSN-2011-04-229」、またセキュリティ勧告が存在するという事実そのものは、アクセス権限のあるユーザーに限定された情報ではありません。実際、National CSIRT およびその他同様のセキュリティ機関では、メンバー間のセキュリティ情報共有のために Security Advisory の再配布を定期的に行っています。このように Security Advisory が再配布される場合、ジュニパーネットワークスの SIRT は、ジュニパーネットワークスの Security Advisory へのハイパーリンクを含めるよう求めています。これは詳細情報の情報源を一元化することで、重大情報の混同や伝達ミスを低減するためです。

開示スケジュール

ジュニパーネットワークスは、定期および不定期の 2 種類の情報開示を行っています。定期開示は、権限に基づく開示プロセスに従い、毎月第 2 水曜日に行われます。製品は 3 つのカテゴリーに分類され、以下のスケジュールに従って公開されます。

- 1 月、4 月、7 月、10 月：ルーティング、スイッチング
- 2 月、5 月、8 月、11 月：ネットワーク管理
- 3 月、6 月、9 月、12 月：セキュリティ、アクセス、アクセラレーション

不定期のセキュリティ情報は、脆弱性を悪用した攻撃が発生しうる場合や、業界全体に影響するセキュリティインシデント、またはマルチベンダー間で発生しうる問題に対しサードパーティが修正を行った場合のみ発行されます。

定期的に発行されるセキュリティ情報は、エンジニアが Junos を導入しようとしている場合に、よりセキュアなバージョンを選択するうえで役立ちます。Security Advisory の発行後にすぐアップグレードが必要となるバージョンをインストールしてしまうより、修正されたコードがすでに組み込まれているバージョンで展開する方が既知の脆弱性に当たることなく安全だからです。

脆弱性の深刻度

First.org は、CVSS（Common Vulnerability Scoring System）を、以下のように定義しています。" CVSS とは脆弱性を引き起こす設計になっていた、ベンダー依存ではなく業界標準の該当箇所、および緊急度と対策の重要性を判断するためのツールである。これにより脆弱性スコアリングシステムが乱立して整合性がなかったという問題が解決されており、共通の基準として誰もが積極的に採用すべきものだ。"

実際、CVSS は多くのネットワークベンダーに利用されています。これは、米国 National Vulnerability Database イニシアチブの一環として作成されたものであり、現在は Study Group 17 で国際電気通信連合規格として検討されています。CVSS は、異なる組織同士が脆弱性の深刻度について認識を一致させることができるツールとして考えればよいでしょう。両者が共通の理解に達することで、適切なアクションを取ることができます。

ジュニパーネットワークスは、報告された同社のすべての脆弱性に対して CVSS を利用しており、CVSS スコアに従って深刻度を評価し、その修正および対策の優先度を設定しています。SIRT は、2010 年 1 月に、すべての Security Advisory で CVSS スコアの提供を開始しました。これにより、ユーザーはスコアを基に完全な CVSS 評価を実施できるようになりました。ジュニパーネットワークスのユーザーは、CVSS トータルスコアから、各自のネットワークに関連する脆弱性の深刻度をより正確に把握することができます。

さらに詳しくは CVSS の詳細については、ジュニパーネットワークスのナレッジベース KB16446「Common Vulnerabilities Scoring System (CVSS) and Juniper' s Security Advisories」（kb.juniper.net）を参照してください。

ジュニパーネットワークスのカスタマーサポートセンター（CSC）

カスタマーサポートセンター（CSC）は、ジュニパーネットワークスのユーザーおよびパートナー向け情報ポータルとして、受賞実績もあります。CSC では、役立つ情報（不具合情報の検索、ライセンス管理、ナレッジベース、アプリケーションノートなど）が多数提供されていますが、このセクションでは、特に、セキュリティ関連機能について取り上げます。

さらに詳しくは 各自のアカウントを使用して http://www.juniper.net/customers/support/ にログインする必要があります。

ソフトウェアダウンロード

CSC のソフトウェアダウンロードセクションでは、最新バージョンの Junos OS を入手することができます。一般的にソフトウェア配布サイトでは、セキュリティが侵害され、改ざんされたコードがアップロードされて広範囲に配布される恐れがあります。そのため、CSC では、暗号化チェックサムによって Junos ソフトウェアの完全性を確保しています。

暗号化チェックサムは、偶発的または意図的に変えられたことを検出する目的で、デジタルデータブロック（この場合は Junos OS のインストールパッケージ）から計算される固定サイズの文字列です。

最も一般的なチェックサムアルゴリズムに MD5 と SHA1 の 2 つがあります。図 1.2 に示すように、ジュニパーネットワークスは、CSC で提供されるすべてのバージョンの Junos OS に MD5 および SHA1 両方のチェックサムを組み込んでいます。

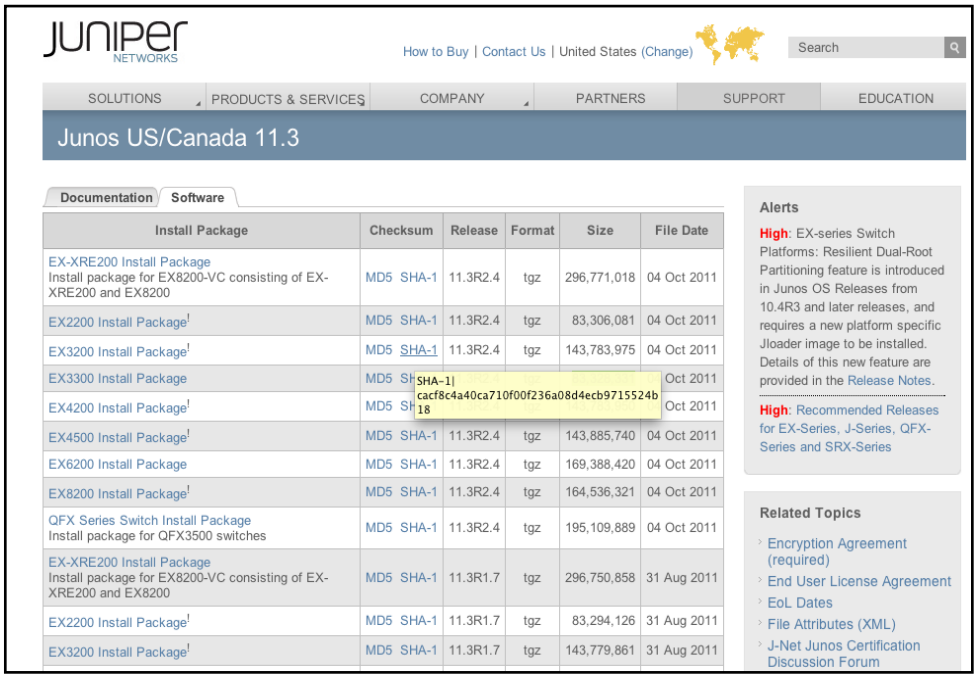

図 1.2　ソフトウェアの SHA1 チェックサム

インストールパッケージをデバイスにコピーしたら、インストール前に、組み込まれている Junos チェックサムユーティリティを使用してパッケージの完全性を確認してください（チェックサムが一致した場合は、ジュニパーネットワークス提供の本物のインストールパッケージがダウンロードされ、改ざんされることなくデバイスに転送されたことを示しています）。

```
jweidley@ex3200> file checksum sha1 /var/tmp/jinstall-ex-3200-10.4R2.6-domestic-signed.tgz
SHA1 (/var/tmp/jinstall-ex-3200-10.4R2.6-domestic-signed.tgz) = cacf8c4a40ca710f00f236a08d4ecb971
5524b18
```

インターネットでは、無料のチェックサムユーティリティが多数提供されていますが、このようなユーティリティを利用する場合は、その入手元が信頼されたソースかどうかを十分に検討してください。

さらに詳しくは　チェックサムの一致については、『*Day One：Junos Tips, Techniques, and Templates 2011*』を参照してください（http://www.juniper.net/dayone）。

テクニカルブリテン

サポートされていないバージョンの Junos OS ソフトウェア（非常に古いためサポートが終了している、または生産終了している）をデバイスで実行すると、セキュリティリスクにさらされる危険性があります。なぜなら、そのバージョンのサポート終了以降に発見されたソフトウェアの脆弱性に対しては未対策ということになるからです。

逆に、サポートされている Junos ソフトウェアを、サポートされているハードウェアで実行すれば、セキュリティの脆弱性が発見された場合も簡単にアップグレードでき、安定したネットワークを維持できるということです。

ジュニパーネットワークスは、運用およびプランニングに役立つ最新情報をユーザーにお届けするために、同社製品に関するテクニカルブリテンを定期的に発行しています。テクニカルブリテンには、ハードウェアおよびソフトウェアの生産終了（EOL）のお知らせや前述の SIRT セキュリティ情報などがあります。

注意　ジュニパーネットワークスでは、基本的に、エンジニアリング終了（EOE）または生産終了（EOL）になったリリースに対するセキュリティ修正の適用は行っていません。脆弱性の修正対象のリリースに関する詳細については、ジュニパーネットワークスのナレッジベース KB16765（kb.juniper.net）を参照してください。

さらに詳しくは　ハードウェアおよびソフトウェアの全バージョンのエンジニアリング終了（EOE）、サポート終了（EOS）、および生産終了（EOL）の日付については、http://www.juniper.net/support/eol/ を参照してください。

少なくとも生産終了のお知らせおよび SIRT ブリテンに登録しておくことを強くお奨めします。

EOL のお知らせおよび SIRT ブリテンへの登録方法

1. まず、https://www.juniper.net/alerts/subscribe.jsp?actionBtn=Modify にアクセスします。

2. 各自の CSC ユーザー名とパスワードを使用してログインします。

3. カテゴリーごとに分類されたジュニパーネットワークスブリテンの表が表示されます。

4. （少なくとも）すべての SIRT セキュリティ情報に登録してください。図 1.3 に示すように、[Security Notice – SIRT] および [Security Bulletins – SIRT] を選択します。

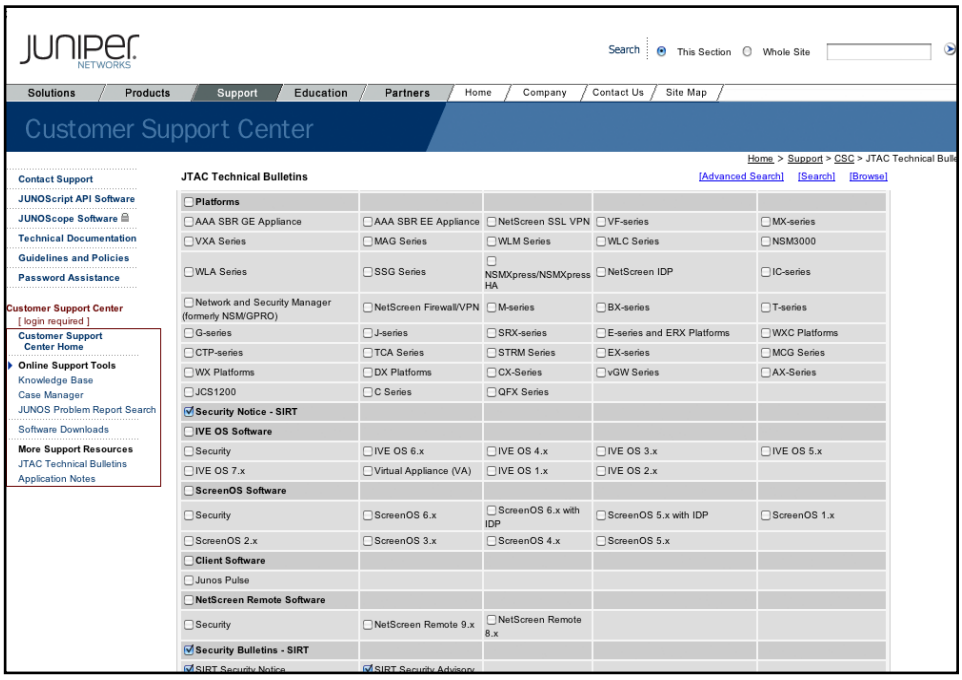

図 1.3　SIRT セキュリティ情報 / 通知を選択したときの画面

5. 図 1.4 に示すように、[End-of-Life (EOL) Product Announcement] セクションで、各自の環境に該当するすべての関連ソフトウェアおよびハードウェアプラットフォームを選択します。

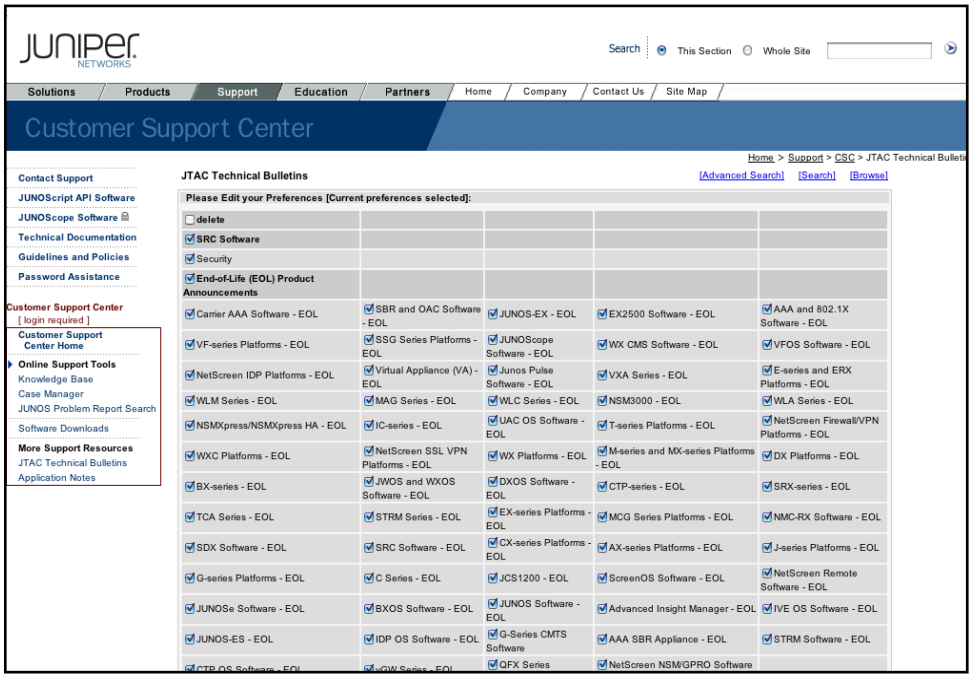

図 1.4 **[End-of-Life] セクションで選択したときの画面**

6. ページの下までスクロールして [Update Now] ボタンをクリックし、選択を保存します。

さらに詳しくは CSC で提供されているその他のサービスに関する詳細については、CSC メインページ（http://www.juniper.net/customers/support/）からアクセス可能な『*JTAC User Guide*』を参照してください。

第2章

物理的セキュリティ

物理的セキュリティについてはその他の手段ではカバーできません。ドライバーやハンマーを手にした悪意ある者からデバイスを保護するソフトウェア機能はないのです。重要なネットワークデバイスは、十分な物理的セキュリティ対策が講じられた安全な場所に設置することを強くお奨めします。これは単純なことのようですが、必ずしも、セキュリティの整備されたデータセンターやワイヤリングクローゼット内の、鍵のかかったラックにネットワークデバイスを設置できるわけではありません。それでも、ネットワークやデータを保護するためにできることはあります。この章では、データセンターやラボのラックに設置されたデバイスを、物理的にアクセス可能な者から保護するための Junos 機能を紹介します。

コンソールポートと AUX ポート

適切なセキュリティ対策を講じないと、コンソールポートや AUX（Auxiliary）ポートからデバイスへの不正アクセスが許可されてしまう可能性があります。この章では、このような状況を想定して説明を進めていきます。

コンソールポートは、デバイスの初期設定および緊急アクセス用に使用され、AUX ポートは、主にモデムを介したリモートアクセスのために使用されます。

コンソールポートのセキュリティ強化

多くの Junos デバイスでは、コンソールポートは、デフォルトで有効になっている唯一のアクセス手段です。コンソールポートアクセスに関するセキュリティ上の課題として、主に無認証セッションとパスワードリカバリーの 2 つがあります。

このセクションを読むことで、これらのセキュリティ問題にアプローチする機能や、さらにセキュリティを強化する機能について理解できるでしょう。

注意 ローカルユーザーアカウントを設定し、セキュアなリモートシステムへ設定をバックアップする環境が整うまで、コンソールアクセスへのセキュリティ対策は必要最小限にしてください。

基本的なコンソールセキュリティの設定方法

ここでは、前述のセキュリティ上の課題を解決するための基本的なコンソールポートセキュリティの実装方法を説明します。

無認証セッションは、権限のあるエンジニアがコンソール経由でログインし、適切にログアウトせずにうっかりケーブルを外してしまった場合に発生します。この場合、次回コンソールに接続した者は、認証を受けなくても CLI にアクセスできてしまいます。

log-out-on-disconnect オプションは、その名前が示すとおり、ケーブル切断時にログアウトを実行します。コンソールポートに接続されたケーブルがデバイスから物理的に取り外されると、そのユーザーセッションは終了します。このオプションは以下のように設定します。

```
[edit system ports]
jweidley@ex3200# set console log-out-on-disconnect
```

無認証セッションは、コンソールセッションの終了後も接続がアイドル状態のまま放置された場合にも発生します。この状況は、ターミナルサーバーを使用している場合に起こりがちです。

ログインクラスにはアイドルタイマーが設定され、すべてのユーザーアカウントには、ログインクラスを定義する必要があります（詳細については、第 4 章の「ログイン許可」セクションを参照してください）。ただし、root アカウントは例外です。root アカウントにはログインクラスは設定できないため、操作が行われていないことを理由に自動的にログアウトすることはありません。

アイドル状態のコンソールセッションを防ぐには、コンソールポートを insecure に設定します。これにより、root ユーザーはコンソールから直接ログインできなくなります。従ってコンソールに接続していたユーザーは通常のユーザーアカウントを使って（ローカルまたは RADIUS/TACACS+ の）認証を行うことになりますが、この通常ユーザーのアカウントには少なくともログインクラスが、できればアイドルタイムアウトが設定されていることが望ましいです。

```
[edit system ports]
jweidley@ex3200# set console insecure
```

コンソールセキュリティに関するもう 1 つの課題は、パスワードリカバリーです。ジュニパーネットワークスが公開している、Junos ベースのデバイスのパスワードリカバリーに関するすべての参考資料には、認証情報の入力なしに root パスワードをリセットする方法が示されています。この方法は、root パスワードをなくしてしまった場合には役立ちますが、デバイスに物理的にアクセスできる者に不正アクセスを許すことにもなります。

2 番目のステップで説明したようにコンソールポートを insecure に設定すると、リカバリープロセスで root パスワードの入力を求められるため、不正なデバイスリカバリーから保護することもできます。以下に示すように、root パスワードを入力しないと、recovery または shell オプションは表示されません。

```
Enter root password, or ^D to go multi-user
Password:
Enter full pathname of shell or 'recovery' for root password recovery or RETURN for /bin/sh:
```

それでは、設定を見てみましょう。

```
[edit system ports]
jweidley@ex3200# show
console {
    log-out-on-disconnect;
    insecure;
}
```

注意 コンソールポートを insecure に設定し、root アカウントのパスワードを忘れてしまった場合は、デバイスのクリーンインストールで復旧させることができます。ただし、これによってすべての設定とログデータが失われます。

注 コンソールポートが insecure に設定されている場合、誰かが root でログインしようとすると、Junos により以下のような Syslog メッセージが生成され、不正なアクティビティとして通知されます。

```
Sep 17 05:08:11.550 2011  ex3200 login:LOGIN_REFUSED:Login of user root from host [unknown] on
device ttyu0 was refused:NOROOT
```

ヒント 緊急状態でもデバイスにアクセスできるようにするために、システムで少なくとも 1 つのローカルアカウントに最高の権限を設定してください。

パスワードリカバリーの無効化方法

セキュリティに不安のある場所やセキュリティの非常に厳しい環境に Junos デバイスが設置されている場合など、パスワードリカバリーができることがリスクと見なされることもあります。

前のセクションで説明した機能を使っても、root パスワードが分かってさえいれば、パスワードリカバリーは可能です。そのため、パスワードリカバリー機能を完全に無効化するには、root アカウントの認証機能を無効化する必要があります。これには、パスワード設定コマンドで encrypted-password オプションを使用し、パスワード部分に二重引用符で囲んだスペースを指定します。

```
[edit system]
jweidley@ex3200# set root-authentication encrypted-pass word " "

[edit]
jweidley@ex3200# show system
host-name ex3200;
authentication-order radius;
root-authentication {
    encrypted-password " "; ## SECRET-DATA
}
```

こうすると encrypted-password が" < スペース >" に見えますが、root パスワードがスペースになっているわけではありません。encrypted-password で見える値は、ハッシュ計算（MD5 または SHA1）された結果です。ログイン時、入力されたパスワードはハッシュ計算され、保存されている暗号化値と比較されますが、これがスペースに一致することはないため、root アカウント認証を無効化することになるのです。

root アカウントは、システムで最も強力なユーザーアカウントであり、システムレベルのデバッグのほとんどで必要になります。上記の設定を行うと、シェルから su - root コマンドも実行できなくなることに注意してください。この設定は絶対に必要な場合を除き、使用しないでください。

注意 コンソールポートが insecure に設定され、root アカウント認証が無効になっている場合、デバイスのクリーンインストールによりデバイスを復旧させることができます。ただし、これによってすべての設定とログデータが失われます。

コンソールポートの無効化方法

一部の環境では、すべてのコンソールアクセスが許容できないリスクと見なされることがあるかもしれません。このような場合、コンソールポートを完全に無効にすることもできます。

```
[edit system ports]
jweidley@ex3200# set console disable

[edit system ports]
jweidley@ex3200# show
console disable;
```

警告！ コンソールポートを無効にすることはお奨めしません。コンソールポートを無効にすると、緊急アクセスやデバイスのリカバリーに支障をきたします。コンソールポートの無効化は、厳格な物理的セキュリティ要件を満たすために絶対に必要、という場合のみ行ってください。

ヒント ソフトウェアでコンソールポートを無効にする代わりに、ポートロックデバイスを使用することもできます。このようなデバイスは複数のメーカーから提供されており、コストパフォーマンスに優れています。これにより機能を犠牲にすることなく、ある程度の物理的セキュリティを確保することができます。

AUX ポートのセキュリティ強化

AUX ポートは、リモートデバイスにダイヤルインアクセスを提供するために、モデムと組み合わせて使用します。AUX ポートは、セカンダリコンソールポートとしても使用できます。この場合、コンソールポートが抱えるセキュリティ上の問題は AUX ポートにも共通します。

ただし、すべての Junos デバイスに AUX ポートが実装されているわけではありません。AUX ポートはデフォルトで無効になっていますが、通常コンフィグレーションには表示されません。この場合、以下のコマンドで、明示的に設定するとよいでしょう。

```
[edit system ports]
jweidley@MX240# set auxiliary disable

[edit system ports]
jweidley@MX240# show
auxiliary disable;
```

AUX ポートを使用する正当な用途がある場合、CLI で、コンソールポートと同様に insecure オプションを使用して直接 root アクセスを制限することができます。

```
[edit system ports]
jweidley@MX240# set auxiliary insecure

[edit system ports]
jweidley@MX240# show
auxiliary insecure;
```

コンソールポートと AUX ポートのアクセスおよび機能を制限する際に必要な注意点について、ここでは十分に取り上げることができません。これらの機能を実装する前に、通常の使用状況、保守手順、緊急時対応などのあらゆるシナリオについて時間をかけて調査し、テストしてください。

ダイアグポートのセキュリティ強化

SCB（System Control Board）、SSB（System and Switch Board）、SFM（Switching and Forwarding Module）、FEB（Forwarding Engine Board） などの一部のハードウェアモジュールには、詳細な解析のために使う特殊ポートが実装されています。デフォルトでは、ダイアグポートにはパスワードが設定されていないため、不正なユーザーがこのポートを通してシステムにアクセスしたり、そのネットワーク固有の機密情報を入手できる可能性があります。

ダイアグポートをパスワードで保護するには、以下のコマンドを使用します。

```
[edit system]
jweidley@ex3200# set diag-port-authentication plain-text-password
New password:<password>
Retype new password:<password>

[edit system]
jweidley@ex3200# set pic-console-authentication plain-text-password
New password:<password>
Retype new password:<password>

[edit system]
jweidley@ex3200#
```

注 これらのコマンドは、特定のハードウェアプラットフォームでのみ有効です。ご使用のデバイスでこのコマンドがサポートされているかどうかは Junos CLI でご確認ください。

実践：サポートされていないデバイスでのダイアグポートパスワードの設定

まずデバイスにログインします。この例では、SCB、SSB、SFM、または FEB が搭載されていない EX3200 を使用しています。

`edit system` と入力し、Enter を押します。

`set ?` と入力し、diag-port-authentication オプションを探します。

しかし、このコマンドは表示されません。そこで、コマンド全体 set diag-port-authentication plain-text-password を入力し、Enter を押します。

パスワードプロンプトに従ってパスワードを設定します。

show と入力して設定を表示すると、設定が無視されたことを示す警告が表示されます。

```
[edit system]
jweidley@ex3200# show
host-name ex3200;
##
## Warning: configuration block ignored: unsupported platform (ex3200-24t)
##
diag-port-authentication {
    encrypted-password "$1$2PbSMm6p$/0YXC//1EE7ttuxOY8LaR."; ## SECRET-DATA
}
...
```

ヒント Junos OS は、実際には何の処理も実行されなくても、サポートされていないコマンドが入力可能で、コミットもできます。ただし、このようなコマンドを使用すると、設定が分かりにくくなり、他のエンジニアの判断を誤らせる可能性があるため、使用しないことをお奨めします。ネットワークに導入されている各 Junos プラットフォームごとにテンプレートを作成することを検討してください。

クラフトインタフェースと LCD メニュー

多くのジュニパーネットワークスの製品には、クラフトインタフェースまたは LCD があります。クラフトインタフェースと LCD メニューは、システムステータスやトラブルシューティング情報を表示することのできるユーザーインタフェースで、フロントパネルに実装されています。また、FPC をオフラインまたはオンラインにしたり、工場出荷時の設定に戻すなど、システムの制御および保守機能を実行するための操作ボタンがあり、メニューオプションも選択できます。

このセクションでは、クラフトインタフェースと LCD メニューで提供されるいくつかの機能と、物理的アクセスが可能な者から保護するためのオプションについて説明します。

クラフトインタフェースのセキュリティ強化

EX シリーズを除くすべてのハイエンド Junos プラットフォームは、必ずクラフトインタフェースを実装しています。ラックを別のユーザーと共有している場合など、状況によっては、クラフトインタフェースのセキュリティについて検討する必要があります。クラフトインタフェースからの操作を無効にすると、FPC または PIC のオンライン化 / オフライン化、アラーム確認などの機能が使用できなくなります。

```
[edit]
jweidley@MX240# set chassis craft-lockout
```

注意 この機能は、エンジニアによる日常的な保守作業に影響する可能性があります。そのため、この機能を有効にする前に、保守およびサポートモデルについて考慮してください。

[Reset Config] ボタンのセキュリティ強化方法

J シリーズやブランチ SRX など小型のデバイスには、クラフトインタフェースや LCD メニューはありませんが、代わりに便利なオプションを備えた [Reset Config] ボタンがあります。

図 2.1 に示すように、[Reset Config] ボタンは、誤って押すことがないよう凹状になっています。[Reset Config] ボタンを押すときは、伸ばしたクリップなどを差し込みます。

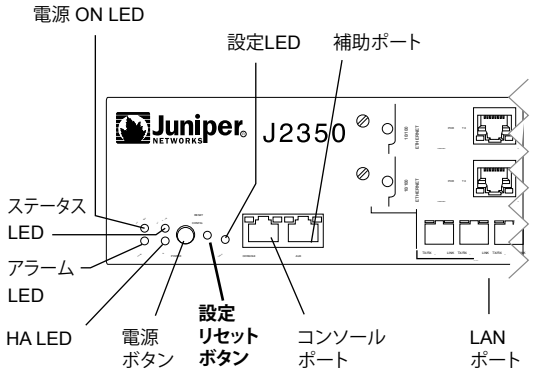

図 2.1 **[Reset Config] ボタンの例**

[Reset Config] ボタンを押下した時のデフォルトの挙動は以下のとおりです。

- このボタンを押してすぐに放すと、rescue config が保存されている場合は、それがロードされてコミットされます。
- ステータス LED が赤く点滅するまでこのボタンを押し続けると（約 15 秒）、バックアップおよび rescue config を含むすべてのデバイス上の設定が削除され、工場出荷時の設定がロードされてコミットされます。

rescue config の復旧機能はそのままに、[Reset Config] ボタンによってルーターが工場出荷時の設定にリセットされないようにするには、以下のコマンドを使用します。

```
[edit chassis]
jweidley@j6350# set config-button no-clear
```

逆にルーターを工場出荷時の設定にリセットする機能はそのままで、[Reset Config] ボタンによってルーターに rescue config が反映されないようにするには、以下のコマンドを使用します。

```
[edit chassis]
jweidley@j6350# set config-button no-rescue
```

どちらのオプションも必要なく、[Reset Config] ボタンを完全に無効にする場合は、以下のコマンドを使用します。

```
[edit chassis]
jweidley@j6350# set config-button no-clear no-rescue
```

さらに詳しくは 詳細については、http://www.juniper.net/techpubs/en_US/junos/topics/reference/configuration-statement/config-button-edit-chassis.html を参照してください。

LCD メニューのセキュリティ

ジュニパーネットワークスのスイッチには、LCD が実装されています。LCD では、ステータス確認やいくつかの機能の設定ができますが、適切にセキュリティ設定をしておかないと、システムがセキュリティリスクにさらされる可能性があります。

Junos OS バージョン 10.2 には、LCD の表示内容やオプションについて、新たなコマンドが追加され、より詳細な確認が可能になっています。

デフォルトで利用可能なメニューオプションを確認するには、以下のコマンドを使用します。

```
jweidley@ex3200> show chassis lcd menu
status-menu
status-menu power-status
status-menu environ-menu
status-menu show-version
maintenance-menu
maintenance-menu halt-menu
maintenance-menu system-reboot
maintenance-menu rescue-config
maintenance-menu factory-default
```

このデバイスがリモートサイトに設置されており、作業を行う Tier-1 エンジニアがいない場合はどうすればよいのでしょうか。また、何らかの理由で、デバイスで動作している OS のバージョンを非表示にしたり、アクティブな設定を工場出荷時の設定で上書きされないようにする場合はどうでしょうか。以下は、LCD メニューのオプションを無効にするコマンドです。

```
[edit]
jweidley@ex3200# edit chassis lcd-menu

[edit chassis lcd-menu]
jweidley@ex3200# set fpc 0 menu-item "status-menu show-version" disable

[edit chassis lcd-menu]
jweidley@ex3200# set fpc 0 menu-item "maintenance-menu factory-default" disable

[edit chassis lcd-menu]
jweidley@ex3200# commit and-quit comment "disabled LCD ver & load default"
commit complete
Exiting configuration mode

jweidley@ex3200> show chassis lcd menu
status-menu
status-menu power-status
status-menu environ-menu
maintenance-menu
maintenance-menu halt-menu
maintenance-menu system-reboot
maintenance-menu rescue-config
```

例えばセキュリティに不安のある場所にデバイスが設置されている場合など、LCD オプションをそのままにすべきでない場合は、以下のコマンドで LCD メニューを完全に無効にし、その設定変更を確認することができます。

```
[edit]
jweidley@ex3200# edit chassis lcd-menu
[edit chassis lcd-menu]
```

```
jweidley@ex3200# set fpc 0 menu-item maintenance-menu disable

[edit chassis lcd-menu]
jweidley@ex3200# set fpc 0 menu-item status-menu disable

[edit chassis lcd-menu]
jweidley@ex3200# commit and-quit comment "disabled LCD menus"
commit complete
Exiting configuration mode

jweidley@ex3200> show chassis lcd menu

jweidley@ex3200>
```

注 EX シリーズでは、バーチャルシャーシの場合、コマンドが若干異なります。上記のコマンドは単体で動作している時のものです。EX でバーチャルシャーシを構成している場合は、追加設定が必要になります。

さらに詳しくは LCD メニューの詳細なリストおよび各プラットフォームのサポート状況については、http://www.juniper.net/techpubs/en_US/junos/topics/reference/configuration-statement/menu-item-edit-chassis.html を参照してください。

未使用のネットワークポートのセキュリティ強化

セキュリティ上の観点から、未使用のネットワークポートを disable にするか、少なくとも使用不可またはケーブルが接続されても影響が出ない状態に設定することをお奨めします。このような対策を取ることで、物理的にアクセスできる者がそのデバイスを経由して他のデバイスまたはネットワーク内の情報にアクセスする可能性を低減することができます。

インタフェースを無効にするには、disable コマンドを使用します。また、インタフェースの description オプションを使うことで設定情報の量は増えますが、デバイスを管理する上で必要な情報を入力でき、非常に有益です。

```
[edit interfaces]
jweidley@MX80# set ge-1/0/1 description "---unused---" disable

[edit interfaces]
jweidley@MX80# commit and-quit comment "disabled ge-1/0/1"
commit complete
Exiting configuration mode

jweidley@MX80> show interfaces descriptions
Interface    Admin Link Description
ge-1/0/0     up    up   ex4500-201;ge-0/0/0;192.168.46.2
ge-1/0/1     down  down ---unused---
ge-1/0/2     up    up   srx5600;ge-0/0/0;192.168.46.54
fxp0         up    up   Out-of-band mgt net
```

EX スイッチでは未使用のポートはデフォルトでは以下のような設定になっています。

- デフォルトでは、すべてのポートがアクセスポートとして定義され、default という名前のタグなし VLAN に配置されます。
- ポートは、デフォルトでアクセスモードに設定され、他のスイッチに接続されても自動的にトランクのネゴシエーションは行われません。

- さらに、デフォルトではトランクには default VLAN は含まれません。以下に示すように、default VLAN に 802.1q タグが割り当てられていません。

```
jweidley@ex3200> show vlans default
Name            Tag     Interfaces
default
                        ge-0/0/5.0, ge-0/0/6.0, ge-0/0/9.0,
                        ge-0/0/18.0, ge-0/0/19.0
dmz             200
                        ge-0/0/7.0*, ge-0/0/8.0*
```

さらに詳しくは ジュニパーネットワークスのスイッチ製品におけるデフォルト VLAN およびネイティブ VLAN の動作については、http://www.juniper.net/books で紹介されている『*Junos Enterprise Switching*』（レイノルドおよびマーシュキー著、O' Reilly Media 発行、2009 年）を参照してください。

設定情報の消去

設定情報は知的財産であるため、作業対象のデバイスが企業のものか政府機関のものかに関わらず、保護する必要があります。運用していく中で、デバイスを移動したり、一時的に保管場所に置いたり、あるいは製品交換のためジュニパーネットワークスに返送することもあるでしょう。このような場合に、ルーティングエンジンからユーザー固有のデータが削除されるように、必要なステップを踏む必要があります。

以下の方法から選択できます。

- 手動で重要なデータを削除：これは最も間違いが起こりやすく、また時間のかかる方法です。Junos ソフトウェアでは、さまざまな場所にデータが保存されるため、すべての機密情報を確実に削除するのは容易ではありません。
- メディアフォーマット：この方法では、リカバリープロセスをセキュリティ目的のために実行します。通常は、ストレージが再パーティション化され、Junos OS が完全に再インストールされるため、すべての情報が失われます。
- すべてのメディアを物理的に取り外す：この方法は最もコストがかかります。まずセキュリティ強化パッケージが適用されるようにアカウントチームと調整する必要があります。

注 設定情報消去の手段として、load factory-default configuration コマンドは含まれません。これは、このコマンドがユーザーの機密情報を安全に削除するための方法ではないためです。あくまで、工場出荷時の設定に素早く戻すための方法に過ぎません。

このセクションでは、2 つ目の方法である、メディアを使った再フォーマットについて取り上げます。メディアインストールの実行手順は Junos プラットフォームによって異なるため、ここでは、このプロセスの基本情報を提供し、実際の手順を示したリンクを記載します。

まず、現在提供されている Junos OS パッケージのタイプについて理解しておくことが重要です。

- インストールバンドル：インストールバンドルでは、Junos OS をマイナーリビジョン間で（例えば、リリース 9.1 からリリース 9.2 へ）ダウングレードまたはアップグレードすることができます。インストールバンドルを使用すると、バージョン間のアップグレードまたはダウングレードに必要なファイルのみが変更されます。

- インストールパッケージ：インストールパッケージでは、メジャーリリース間で（例えば、リリース 9.2 からリリース 10.1 へ）アップグレードおよびダウングレードすることができます。インストールパッケージをインストールすると、ソフトウェアが完全に再インストールされ、Junos ファイルシステムが再構築されます。このとき、過去のシステムログなどが削除されることがあります。ただし、インストール前の設定ファイルは保持されます。
- インストールメディア：インストールメディアでは、ルーターをソフトウェア障害から復旧させることができます。インストールメディアにより、メディアが再パーティション化され、Junos OS が完全に再インストールされます。このインストール中、インストール前の情報は何も維持されません。

インストールメディアは、PCMCIA、コンパクトフラッシュ、または USB ドライブを使って Junos ディスクイメージを作成するためのパッケージです。このディスクイメージを使用することで、ルーティングエンジンを再フォーマットし、すべてのデータを消去することができます。

ヒント メディアインストールによって、ある程度企業固有のデータがルーティングエンジンから消去されることは保証されますが、あらゆるデータ解析技術を駆使することで、データを復旧できる場合があることを認識しておいてください。高度なセキュリティが要求される環境では、メディアの物理的な取り外しが唯一の選択肢となる場合があります。

インストールメディアの入手

インストールメディアは、ジュニパーネットワークスのソフトウェアダウンロードサイトから入手できます。図 2.2 に示す、一般的なインストールパッケージ専用のセクションにアクセスしてください。

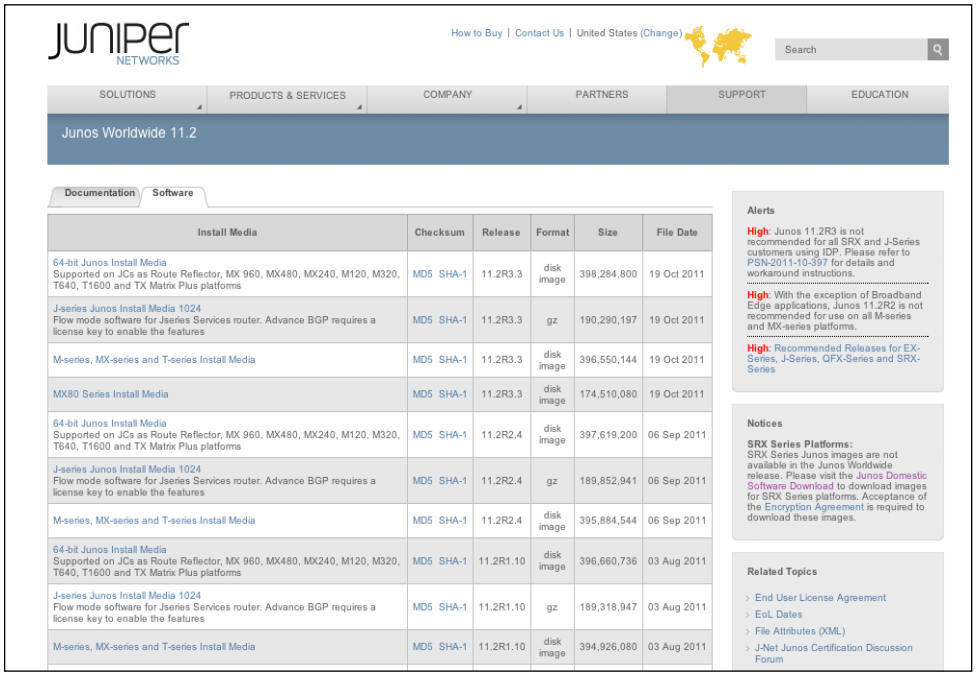

図 2.2 **CSC：インストールメディアのダウンロード**

図 2.2 より、Junos デバイスプラットフォームごとに異なるインストールメディアがあることが分かります。ご使用のデバイス用に正しいパッケージをダウンロードしてください。

さらに詳しくは さまざまな Junos OS メディア、または緊急リカバリーディスクの作成とリカバリーインストールの実行に関する詳細については、『*Junos OS Software Installation and Upgrade Guide*』（http://www.juniper.net/techpubs/en_US/junos10.4/information-products/pathway-pages/software-installation-and-upgrade/software-installation-and-upgrade.html）を参照してください。

ヒント ルーティングエンジン上のすべてのデータをセキュアに消去し、すべてのキー値をリセットする `a request system zeroize` Junos CLI コマンドがありますが、その機能とサポートは Junos デバイスプラットフォームによって異なります。そのため、このコマンドを使用する場合は、事前に、ご使用のプラットフォームにおける影響とサポート状況について確認してください。

第3章

OSのセキュリティ

Junos OS は、安定性とセキュリティが不可欠で、機能停止が数十万ものユーザーに影響してしまうサービスプロバイダ環境でスタートしました。サービスプロバイダ環境では、すべての機能に合理的で仕様通りの挙動が求められます。例として、ダイレクテッドブロードキャストおよび IP ソースルーティング動作について考えてみましょう。これらは、場合によっては便利な機能ですが、デフォルトで有効にすると、十分な安定性、他デバイスとの整合性、およびセキュリティが確保されません。使用する場合は、これらの機能を必要とするインタフェースにのみ設定されるべきです。

OS 自体が持つセキュリティ機能は、デバイスの全体的なセキュリティと安定性の基盤になります。OS がセキュアでなければ、設定に関係なく、デバイスがセキュリティ被害を被る可能性があります。

Junos OS のベースコードには、セキュアなデフォルト値、合理的なネットワーク機能の仕様、カーネルの保護など、セキュリティと安定性を強化する多数の機能が組み込まれています。この章では、Junos 自体が備えるセキュリティ機能と、デバイスの全体的なセキュリティ対策のベースとなるデフォルト設定について説明します。

工場出荷時の設定

残念ながら、ネットワークデバイスはポートリッスンをしているサービスがある以上、ある程度のリスクにさらされていることになります。ネットワーク環境はユーザーごとに異なるため、ジュニパーネットワークスでは、ユーザーが Junos デバイスでどのサービスを有効にすべきかについて言及しません。また、これらすべての機能を無効にするために多くの設定変更を行わなければならない場合、1 つの間違いがネットワークのセキュリティをさらに低下させ、攻撃を受けやすくなる可能性があります。

そのため、ジュニパーネットワークスは、デフォルト設定を必要最小限にしており、必要に応じてエンジニアが機能を追加しなければならないようにしています。これにより、初期導入時に必要な設定が増える可能性がありますが、セキュリティ上のメリットは、そのわずかなデメリットをはるかに上回ります。

工場出荷時の設定は、プラットフォームによって多少異なりますが、デバイスがネットワーク機器としての役割を果たすために、必要最小限の機能のみ有効になっていることを覚えておいてください。

実践：工場出荷時の設定の表示

対象の Junos デバイスによって異なりますが、ここで注目すべき事項は、デフォルトのアカウントとアクセスサービスです。

1. Junos デバイスにログインし、設定モードに切り替えます。

2. `load factory-default` コマンドを入力します。

```
[edit]
jweidley@MX80# load factory-default
warning: activating factory configuration

[edit]
jweidley@MX80#
```

3. `show` コマンドを入力し、工場出荷時の設定を表示します。

```
[edit]
jweidley@MX80# show
## Last changed:2011-03-14 08:25:13 UTC
system {
```

```
    syslog {
        user * {
            any emergency;
        }
        file messages {
            any notice;
            authorization info;
        }
        file interactive-commands {
            interactive-commands any;
        }
    }
    ## Warning: missing mandatory statement(s):'root-authentication'
}

[edit]
jweidley@MX80#
```

工場出荷時の設定には、アクセスサービス（telnet、SSH など）やユーザーアカウントが含まれていません。また、root ユーザーにパスワードが設定されていないことにも留意してください。これについては、次のセクションで説明します。

4. これらの変更をコミットしない場合は、`rollback` コマンドを入力し、アクティブな設定と候補設定を同期させます。

```
[edit]
jweidley@MX80# rollback
load complete

[edit]
jweidley@MX80#
```

5. 設定が変更されていないことを確認します。

```
[edit]
jweidley@MX80# show | compare

[edit]
jweidley@MX80#
```

6. デバイスからログアウトします。

root アカウントのパスワード

root アカウントは、Junos デバイスで最も強力なアカウントであるため、パスワードで保護する必要があります。root アカウントにはデフォルトのパスワードはなく、すべての Junos デバイスは、root アカウントのパスワードが設定されていない状態で出荷されます。これにより、エンジニアがデフォルトパスワードを変更せずにそのまま使い続ける、ということが起こらないようになっています。

root パスワードは、デバイスの初期設定時に設定する必要があります。実際、Junos OS の通常の動作では、以下に示すように、root パスワードを設定しないと、初期設定はコミットされません。

```
[edit]
jweidley@MX80# commit
[edit]
  'system'
    Missing mandatory statement:'root-authentication'
error: commit failed:(missing statements)

[edit]
jweidley@MX80#
```

サポートアカウント

Unix ベースの OS を使う一部ベンダーは、ユーザーによるトラブルシューティングを支援するため、root と同じレベルの権限を持つサポートアカウントを追加している場合があります。通常、このアカウントは、/etc/passwd にアカウントを作成し、そのユーザー ID（uid）またはグループ ID（gid）を 0 に設定することにより作成されます。しかし、そもそも外部の者がデバイスのログイン名とパスワードを持つべきではなく、このようなアカウントにより、セキュリティ上大きなリスクが生じることになります。Junos OS には、こういったサポートアカウントやバックドアサポートアカウントはありません。root レベルのアカウントは 1 つのみであることは、shell から以下のコマンドを実行することで確認できます。

```
jweidley@ex3200> start shell
% cat /etc/passwd | egrep ':0:'
root:*:0:0:Charlie &:/root:/bin/csh
%
```

出力には、root アカウントが 1 つのみ表示されています。

パスワード

システムへの攻撃の多くは、アクセス可能な者、不満や恨みを抱えている従業員、またはその他状況により、ネットワーク内から仕掛けられます。このような攻撃を防ぐためには、すべてのネットワークデバイスパスワードを暗号化し、デバイスの設定またはコンソールに表示できないようにすることが不可欠です。

セキュアなパスワード保持

Junos OS は、複数の暗号化およびハッシュアルゴリズムによりパスワードのセキュリティを強化するいくつかの手法をサポートしています。デフォルトのハッシュアルゴリズムは MD5 ですが、さらに強固なセキュリティが求められる環境では、SHA1 に変更することもできます。

CLI でプレーンテキストのパスワードを設定すると、Enter キーを押した直後に、Junos OS によりそのパスワードが暗号化されます。プレーンテキストのパスワードは、アーカイブされた設定のバックアップを含むすべての設定ファイルに、常にセキュアな方法で保存されます。

これは、パスワードを保護するためよく用いられる重要なセキュリティ機能ですが、同時に、機密情報を秘匿するうえでも役立ちます。例えば、Tier-3 エンジニアが Tier-1 のエンジニアに設定情報を渡す際、次のように暗号化された情報で提示することにより、実際のパスワードを知らせることなく、すべてのルーターにアカウントを作成することができます。

```
set system login user EMERGENCY full-name "Emergency Account"
set system login user EMERGENCY class super-user
set system login user EMERGENCY authentication encrypted-password "$1$zEj/6q97$r8GfPUOfRqGhNaSa7f
Jg//"
```

デフォルトパスワードポリシー

容易に推測できるパスワードが設定されることがないよう、Junos には、プレーンテキストパスワードに対してデフォルトで以下の要件があります。

- 長さ：パスワードは、6 ～ 128 文字でなければなりません。
- 文字：パスワードには、ほとんどの文字クラス（大文字、小文字、数字、句読文字、およびその他の特殊文字）を含めることができます。制御文字は使用しないでください。
- 複雑性：パスワードは、少なくとも大文字と小文字または複数の文字クラスを組み合わせる必要があります。

このデフォルトポリシーにより、ある程度の保護は可能ですが、このデフォルトポリシーがユーザーのパスワード複雑性要件を満たしていない場合は、第 4 章の「ローカル認証」を参照し、これらのパラメータのカスタマイズ方法を確認してください。

さらに詳しくは Junos のプレーンテキストパスワードに関する詳細については、http://www.juniper.net/techpubs/en_US/junos10.4/topics/concept/authentication-plain-text-password-requirements.html を参照してください。

SNMP による設定

Junos OS の誕生当初は、使用可能な SNMP バージョンはバージョン 1 および 2 のみで、これらのバージョンでは、SNMP マネージャとデバイス間の通信の暗号化および認証がどちらも行われなかったことから、SNMP はセキュアでないと考えられていました。誰かが SNMP トラフィックをキャプチャし、同じコミュニティストリングを使用することにより、デバイスに対して不正な変更を行う可能性がありました。

Junos デバイスは、SNMP で設定を追加・変更・削除することはできません。これは、書き換え可能な MIB（Management Information Base）がほとんどないためです。SNMPv3 では、プロトコルに認証および暗号化が追加されており、Junos は SNMPv3 をサポートしていますが、SNMP による設定の追加・変更・削除は引き続き許可されていません。

CLI、J-Web、Junoscript など、Junos デバイスを設定する方法はいくつかありますが、SNMP はこれに含まれません。

注 ping および traceroute 関連の MIB など、トラブルシューティングに使用される書き換え可能な MIB もいくつかあります。

リモートアクセス

ネットワークデバイスでサービスを有効にするたびに、悪意のあるユーザーにデバイス侵入の機会を与えることになり、攻撃を受けるポイントが増えます。

多くの Junos デバイスでは、工場出荷時の設定に telnet、SSH、J-Web などのリモートアクセスサービスは含まれていません。このようにセキュアなデフォルト設定を採用し、エンジニアが必要なリモートアクセスサービスのみを有効にしなければならないようにすることで、攻撃に使われる要素を極力排除しています。

注 ブランチ SRX や J シリーズ デバイスなどローエンドのプラットフォームのような例外もあります。これらのプラットフォームのデフォルト設定には、十分な経験のないエンジニアでも円滑に作業できるよう、いくつかのマネジメントサービスが含まれています。これらのデバイスでは、セキュリティ上の課題を低減するために、マネジメントサービスはグローバルではなく、特定のインタフェースまたはセキュリティゾーンでのみ有効になっています。詳細については、各プラットフォームの参考資料を参照してください。

さらに詳しくは セキュアでないアクセスサービスの無効化およびアクセスサービスのセキュリティ強化方法については、第 4 章の「アクセスセキュリティ」セクションを参照してください。

カーネル

Junos が FreeBSD をベースとしており、Junos CLI から Unix シェルにアクセスできることは周知の事実です。従って、別のシステムでコンパイルされたプログラムが Junos デバイスで実行されるという可能性が考えられます。しかし、ジュニパーネットワークスはこのリスクに対し、ジュニパーネットワークスが正式にコンパイルしたプログラムのみインストールでき、ルーティングエンジン上で実行できる仕組みを導入しています。

ソフトウェアのインテグリティチェック

各 Junos OS ソフトウェアイメージには、デジタル署名された実行可能ファイルのマニフェストが含まれ、このシグネチャーの正当性が確認された場合にのみ、その実行可能ファイルをシステムに登録することができます。Junos ソフトウェアでは、シグネチャーが登録されていないバイナリーは実行されません。この機能により、Junos デバイスのインテグリティを侵害する可能性のある不正なソフトウェアやアクティビティからシステムを保護しています。

Junos 7.5 以降では、SHA1 フィンガープリントマニフェストが一致しているバイナリーのみカーネルで実行されるようにするために、デジタルシグネチャーが使用されています。Junos では、これらのフィンガープリントが、デジタル署名されたマニフェストからロードされますが、ローダーは、そのシグネチャーの正当性が確認できた場合のみこの処理を実行します。Junos では、そのシグネチャーに、RSA で暗号化された SHA1 ダイジェストが使用されます。

また、すべての Junos ソフトウェアモジュールは、SHA-1（Secure Hash Algorithm 1）または MD5（Message Digest 5）の結果として生成されたデジタルシグネチャーを含んでおり、署名されたパッケージとして提供されます。このパッケージは、内部計算の結果が、対応するファイルに記録された結果と一致する場合のみインストールされます。

この仕様は、Junos デバイスの再起動時に確認できます。

```
Mounted jbase package on /dev/md0...
Verified manifest signed by PackageProduction_10_4_0
Verified jboot signed by PackageProduction_10_4_0
Verified jbase-10.4R3.4 signed by PackageProduction_10_4_0
Mounted jcrypto-ex package on /dev/md1...
Verified manifest signed by PackageProduction_10_4_0
Verified jcrypto-ex-10.4R3.4 signed by PackageProduction_10_4_0
Mounted jdocs-ex package on /dev/md2...
Verified manifest signed by PackageProduction_10_4_0
Verified jdocs-ex-10.4R3.4 signed by PackageProduction_10_4_0
Mounted jkernel-ex package on /dev/md3...
Verified manifest signed by PackageProduction_10_4_0
Verified jkernel-ex-10.4R3.4 signed by PackageProduction_10_4_0
Mounted jpfe-ex42x package on /dev/md4...
Verified manifest signed by PackageProduction_10_4_0
Verified jpfe-ex42x-10.4R3.4 signed by PackageProduction_10_4_0
Mounted jroute-ex package on /dev/md5...
Verified manifest signed by PackageProduction_10_4_0
Verified jroute-ex-10.4R3.4 signed by PackageProduction_10_4_0
Mounted jswitch-ex package on /dev/md6...
Verified manifest signed by PackageProduction_10_4_0
Verified jswitch-ex-10.4R3.4 signed by PackageProduction_10_4_0
Mounted jweb-ex package on /dev/md7...
Verified manifest signed by PackageProduction_10_4_0
Verified jweb-ex-10.4R3.4 signed by PackageProduction_10_4_0
```

さらに詳しくは　詳細については、ジュニパーネットワークスのナレッジベース KB12831「Verification of Junos Software Images」を参照してください。

ネットワーク

過去に、あまり使われない機能が有効化されており、インターネットおよびユーザーネットワークを不安定にしたり、パフォーマンスを劣化させる原因となっていたケースがありました。このセクションでは、これらの機能に関連する Junos OS の仕様について説明し、アウトオブバンドマネジメントのメリットを示します。

アウトオブバンドマネジメント

ネットワークデバイスは、基本的に In-Band および OOB（Out-of-Band）の 2 つの方法で管理できます。インバンドマネジメントでは、マネジメントトラフィックは、ユーザートラフィックと物理インタフェースおよびケーブルを共有します。一方、OOB マネジメントでは、マネジメント専用に別のインタフェースとリンクを使います。OOB マネジメントのためにコストはかかりますが、図 3.1 に示すように、ユーザートラフィックとマネジメントトラフィックを明確に分離することができます。

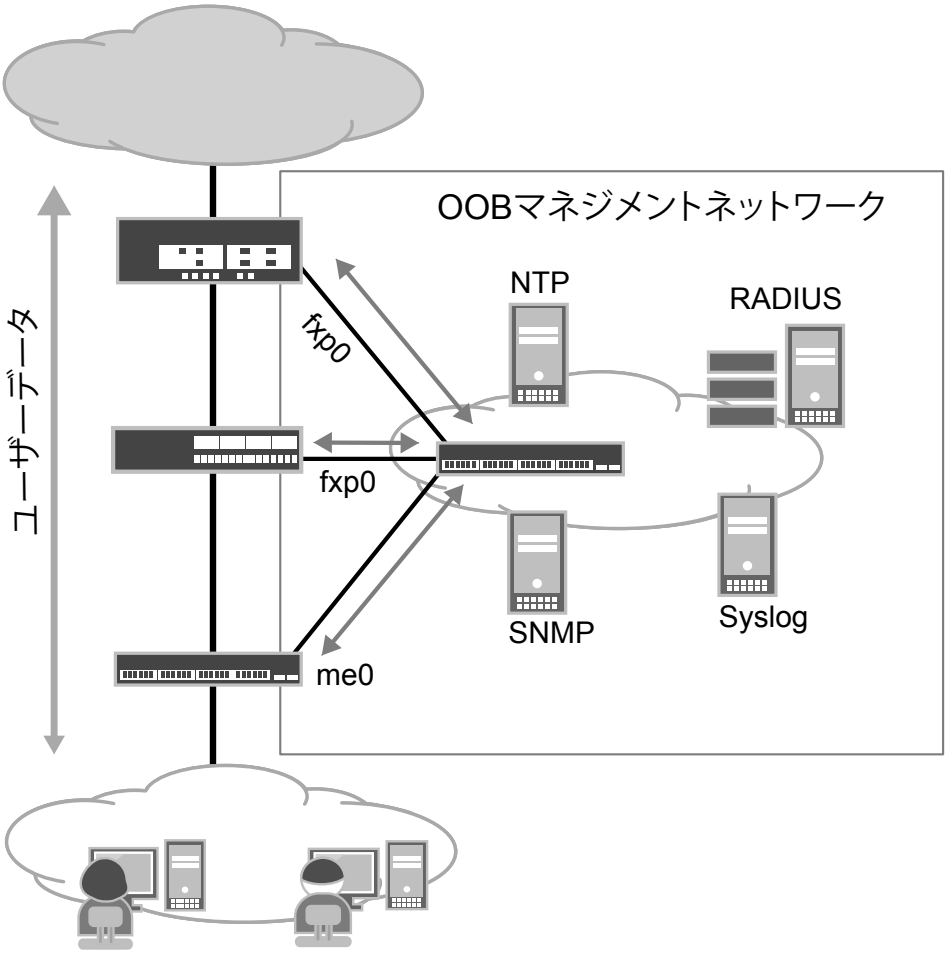

図 3.1 **OOB マネジメントネットワーク**

多くの Junos OS プラットフォームには、専用の OOB マネジメントインタフェースが実装されています。このインタフェースは、ルーターおよびセキュリティプラットフォームでは fxp0、スイッチでは me0 または vme0 と呼ばれます。J シリーズ ルーターおよびブランチ SRX は小型製品のため、専用のマネジメントインタフェースはありません（ただし、任意のイーサネットインタフェースをマネジメント目的で使用できます）。

専用の OOB マネジメントポートは非トランジットインタフェースとも呼ばれます。これは、マネジメントインタフェースから入ったトラフィックが他のインタフェースから出ることはできず、また他のインタフェースから入ったトラフィックがマネジメントインタフェースから出ることができないためです。

図 3.1 は、OOB マネジメントポートを使うことで、マネジメントデータ（NTP、SNMP、認証、Syslog など）がユーザートラフィックから物理的に分離され、ネットワーク全体でセキュリティ体制が強化される様子を示しています。悪意のあるユーザーを管理トラフィックから物理的に分離すれば、マネジメントトラフィックをスニフィングされたり妨害されたりすることはありません。

IP ソースルーティング

ルーターは、ルーティングプロトコルを使用して通信し、特定のネットワークまでのルート情報を交換します。パケットは、宛先アドレスに基づいてネットワーク上でルーティングされます。ルーターは宛先までの最適パスを認識しているため、宛先アドレスを元にルーティングするのは当然のことです。

IP RFC（RFC 791）には当初、ストリクトおよびルーズソースルーティングのための IP ヘッダーオプションが含まれていました。ソースルーティングでは、送信側が、パケットが宛先に到達するまでに経由するパスのすべて（ストリクト）または一つのゲートウェイ（ルーズ）を指定することができます。

このオプションはネットワークのトラブルシューティングのためにありましたが、悪意のあるユーザーがソースルーティングを使用して、特定のネットワークセグメントにパケットを向かわせ、ネットワークトポロジー情報を収集し、場合によってはセキュリティを無効にする可能性があるということにもなります。

古いバージョンの Junos では、ソースルーティングがデフォルトで有効になっていましたが、無効にすることも可能でした。

```
[edit]
jweidley@MX240# set chassis no-source-route
```

Junos 8.5 以降では、IPv4 ソースルーティングはデフォルトで無効です。ネットワークでソースルーティングが必要な場合は、`[edit routing-options source-routing]` 階層で有効にすることができます。このような仕様変更が行われたため、Junos CLI では、前述の CLI コマンドに、廃止予定であることを示すフラグが付けられます。

```
[edit]
jweidley@mx240# show chassis
no-source-route; ## Warning:'source-route' is deprecated
```

ヒント パケットルーティングにおける最適のパスの決定は、ジュニパーネットワークスのルーターに任せ、ユーザーによるソースルーティングは許可しないでください。

IP ダイレクテッドブロードキャスト

ダイレクテッドブロードキャストは、パケットが特定のサブネットのブロードキャストアドレスに送信された場合に発生します。IP ダイレクテッドブロードキャストパケットは、宛先サブネットに到達するまでは、ユニキャスト IP パケットと同じようにネットワークを通過します。宛先サブネットに到達し、パス上の最後のデバイスで IP ダイレクテッドブロードキャストが有効になっている場合、そのルーターまたはスイッチは、IP ダイレクテッドブロードキャストパケットを、ターゲットサブネット向けのブロードキャストに変換し、送出します。これにより、ターゲットサブネット上のすべてのホストが IP ダイレクテッドブロードキャストパケットを受信します。ただし、この処理によってルーターまたはスイッチに負荷がかかります。さらに、IP スプーフィングが使われている環境では、ダイレクテッドブロードキャストがさらに致命的な状況を招く可能性があります。また、特定ホストに対する DoS（Denial of Service）攻撃や、ネットワークの全体的なパフォーマンスを低下させる手段として悪用される可能性もあります。

ただし、ダイレクテッドブロードキャストそのものが必ずしも悪質なわけではありません。バックアップなどのリモートマネジメントツールや WOL（Wake on LAN）アプリケーションには、IP ダイレクテッドブロードキャストを必要とするものもあります。

Junos ソフトウェアでは、ダイレクテッドブロードキャストはデフォルトで必ず無効になっています。ジュニパーネットワークスは、ダイレクテッドブロードキャストの妥当なユースケースを認識しており、ターゲッテッドブロードキャストと呼ばれる機能を導入しました。この機能は、インタフェース単位で明示的に設定する必要があります。

プロキシ ARP

プロキシ ARP（Address Resolution Protocol）は、ネットワークデバイス（通常はルーター）が別のデバイス宛ての ARP 要求に代理で応答する機能です。応答したルーターがその宛先までのルーティングを行います。

プロキシ ARP は、ルーティングエンジンに不要な負荷をかけようとする悪意のあるユーザーに悪用される可能性があります。また、プロキシ ARP を有効化する際に、間違ったサブネットマスクを設定するなどのミスが考えられ、それによりネットワーク障害が起こる可能性もあります。

Junos ソフトウェアはデフォルトではプロキシ ARP は無効になっており、自身の持つ IP アドレスに対する ARP 要求にのみ応答します。これにより、シンプルで把握しやすいネットワーク設定になっています。

プロキシ ARP は、その機能を必要とする状況では非常に有益な機能です。Junos OS では、インタフェース単位でプロキシ ARP を設定できますが、あくまで必要になった時のみ使う機能として理解してください。極力余分な機能を使わずに適切にネットワークを設計し、展開することがベストなのです。

デフォルト ARP ポリサー

ジュニパーネットワークス EX シリーズを除き、Junos OS ではデフォルトで、ルーティングエンジンで処理される ARP パケットに対して、レートリミットが適用されます。これにより、設定不備によるものか悪意のある行為によるものかを問わず、ARP ストーム攻撃によってルーティングエンジンのリソースがすべて枯渇する状況を防ぎます。

```
jweidley@MX240> show policer
Policers:
Name                                                Packets
__default_arp_policer__                             0
```

デフォルトポリサーがユーザーの要件を満たしていない場合は、カスタムポリサーを作成して、必要なインタフェースに適用することもできます。ポリサーの作成および適用の詳細については、第 4 章の「ルーティングエンジンの保護」を参照してください。

第4章

セキュリティ強化のための設定

この章ではデバイスのセキュリティを強化するための機能を実装するプロセスについて解説します。Junos のデフォルト設定では、あらゆる状況に適応するセキュリティが提供されています。ただし、いかにセキュアなデバイスであっても、不適切なコンフィグレーションではセキュリティレベルが低下してしまいます。この章では、Junos デバイスをさまざまな側面から強化するセキュリティオプションの適切な設定について説明します。

ネットワークの強化

最初に、Junos デバイスのサービスの基本的な動作と、これらのサービスをどのように強化すれば不確定要素がなく、信頼性・安全性の高いネットワークにできるかを理解しましょう。

アドレス選択

デフォルトでは、ルーティングエンジンで生成されるトラフィック（cflowd、syslog、NTP など）の送信元アドレスは、宛先に最も近いインタフェースの IP アドレスになります。

デフォルトのままでは、大規模で、高密度に接続されたネットワークでは、障害時に送信元アドレスが変わってしまう可能性があります。ルーティングエンジンで生成されるトラフィックの送信元アドレスを固定化するために、ループバック（lo0）アドレスを使用することをお奨めします。

パケットがルーテッドインタフェースから送信されるときに、ローカルで生成されるすべての IP パケットの送信元アドレスとしてループバックインタフェース（lo0）の IP アドレスを使用する場合は、CLI で `default-address-selection` オプションを使用します。この設定は、OOB マネジメントインタフェース（fxp0 または me0）から送信されるトラフィックには適用されないことに注意してください。

```
[edit]
jweidley@ex3200# set system default-address-selection
```

ヒント 送信元アドレスとしてループバックを使用すると、すべてのネットワークデバイスのループバックインタフェースの IP アドレスが特定のサブネット内にある場合、デバイスから送信される管理トラフィックを指定して許可するファイアウォールルールを簡単に作成できるというメリットもあります。

注意 このコマンドを使用する場合は、Junos デバイスの初期設定の段階で追加しておくことをお奨めします。このコマンドを稼働中のデバイスに追加するときは、十分注意し、コマンド追加後も、ルーティングエンジンで生成されるすべてのトラフィックが引き続き期待どおり動作することを確認してください。

ICMP リダイレクト

ICMP リダイレクトとは、ルータからパケットの送信元に送られる notification で、特定のホストまたはネットワークへのベターなパスが存在することを通知する際に使用されるものです。送信元デバイスは ICMP リダイレクトを受信すると、自身のルーティングテーブルを変更し、以降送信するすべてのパケットを ICMP リダイレクトで通知されたルーター経由でルーティングします。

ヒント ICMP リダイレクトはオプションであり、必須ではありません。適切に設計されたネットワークであれば、ICMP に頼らなくても正常に機能するはずです。

ICMP リダイレクトを使う時の最大の脅威は、DoS 攻撃です。最適ではないパスでルーティングされた何千 pps ものパケットを受けることで、ルーターがそれらに応答せざるを得なくなり、これによりルーターのリソースが枯渇してしまいます。

Junos OS のデフォルト動作では、ICMP リダイレクトが送信されますが、以下のコマンドを使用することにより、ICMP リダイレクトをグローバルで無効にすることができます。

```
[edit]
jweidley@ex3200# set system no-redirects
```

初期インストール後、最終的な設定に落ち着くまでの間、一時的に ICMP リダイレクトを有効にしなければならないような状況もあります。このような場合、エンジニアは、ICMP リダイレクトを必要なインタフェースのみで有効なままにし、不要なインターフェースで無効にすることができます。インタフェース単位でリダイレクトを無効にするには、以下のコマンドを使用します。

```
[edit interfaces ge-0/0/3 unit 50]
jweidley@ex3200# set family inet no-redirects
```

SYN-FIN TCP フラグ

OS のタイプとバージョンを特定する方法の 1 つとして、標準外のパケットタイプを送信し、ターゲットの応答を分析するという方法があります。この手法は、TCP/IP スタックフィンガープリンティングと呼ばれます。このプロセスで一般的に使用されるパケットタイプの 1 つに、SYN および FIN フラグが両方設定された TCP パケットがあります。SYN フラグは接続の初期確立時に使用され、FIN フラグはセッションを終了させるときに使用されるものであるため、これは明らかに無効なパケットです。

このように SYN フラグと FIN フラグが両方セットされた TCP パケットは、その他の不正な目的に使用される可能性もあるため、ドロップする必要があります。この無効な TCP フラグの組み合わせは、ファイアウォールフィルタでブロックすることもできますが、Junos では、`[system internet-options]` 階層に、これらのパケットをカーネルレベルでドロップするためのオプションが用意されています。

```
{master:0}[edit]
jweidley@EX4500# set system internet-options tcp-drop-synfin-set
```

TCP リセット（RST）パケット

閉じられているポートに対してサービス要求があると、通常 RST または RST/ACK が返送されます。ポートスキャンを行うツールは、ネットワークデバイスに対して一定の範囲のポートを指定してパケットを送信し、その応答をリスニングすることで、そのポートで実行されているサービスがあるかどうかを判断します。

ところが、大量のポートスキャンはルーティングエンジンに不要な負荷をかけ、パフォーマンスに悪影響をおよぼしたり、サービス停止を引き起こす可能性もあります。Junos がリスニングを行っていないポートへの接続要求に対し、TCP リセット（RST）パケットを送信しないようにするには、`no-tcp-reset` オプションを使用します。ここで、この CLI を使用して、どのような結果が得られるかを見てみましょう。

```
[edit]
jweidley@mx240# edit system internet-options

[edit system internet-options]
jweidley@mx240# set no-tcp-reset ?
Possible completions:
  drop-all-tcp         Drop all TCP Packets
  drop-tcp-with-syn-only  Drop only those TCP Packets with SYN bit
```

このコマンドには 2 つのオプションがあります。

- drop-all-tcp：FIN/RST、ACK/RST など、標準外の TCP フラグの組み合わせになっているパケットを検出してドロップします。
- drop-tcp-with-syn-only：SYN フラグのみが設定されているか、SYN フラグを含むフラグの組み合わせが設定されている TCP パケットを検出してドロップします。

ping タイムスタンプとレコードルート

実網では外部送信元からの ping をブロックすることをお奨めしますが、ping は内部ホストにとって非常に役立つトラブルシューティングツールです。そのため、一般には、ルーティングエンジンに送信される ping にレートリミットを適用することにより、ルーティングエンジンを危険にさらすことなく、この機能をトラブルシューティングに利用できるようにしています（詳細については、この章の「ルーティングエンジンの保護」セクションを参照してください）。

タイムスタンプオプションを使用すると、宛先ホストまでの往復時間を測定できます。また、レコードルートオプションは、traceroute コマンドとは異なり、宛先までのパスだけでなく復路のルートも示されるため、ネットワークパスの問題のトラブルシューティングに役立ちます。

ただし、タイムスタンプおよびレコードルートオプションの応答にはルーティングエンジンのループバックアドレスが使用されますが、これは通常ユーザーと共有すべき情報ではありません。ルーティングエンジンの存在を隠しながら、これらの便利なサービスを提供するには、以下のコマンドを使用します。

```
[edit]
jweidley@ex3200# set system no-ping-record-route

[edit]
jweidley@ex3200# set system no-ping-time-stamp
```

LLDP（Link Layer Discover Protocol）

LLDP（Link Layer Discover Protocol）は、ベンダーに依存しない標準レイヤー 2 プロトコルで、ネットワークデバイスが LAN 上に自身の情報と LLDP のケイパビリティをアドバタイズすることができます。LLDP 対応デバイスは、TLV（Type Length Value）の形式で情報を送信します。これらのメッセージには、シャーシおよびポート情報、システム名、デバイスの機能など、デバイス固有の情報を含めることができます。

LLDP-MED（LLDP-Media Endpoint Discovery）は、LLDP 標準を拡張したもので、VoIP（Voice Over IP）エンドポイントデバイスと他のネットワーキングデバイス間でのインターオペラビリティをサポートします。LLDP-MED では、ネットワークポリシーの検出や PoE（Power over Ethernet）マネジメントなど、追加の TLV 情報が使用されます。

Junos OS では、LLDP と LLDP-MED の設定コマンドは異なりますが、このセクションでは、この 2 つをまとめて LLDP と呼ぶことにします。

LLDP に伴うセキュリティリスクとして、パケットが認証または暗号化されないことが挙げられます。すなわち、悪意のあるユーザーが LLDP パケットのキャプチャを行い、ネットワークに関する情報を入手する可能性があります。また、攻撃者が脆弱性を見つけるために、またはデバイスをクラッシュさせて DoS 攻撃を仕掛けるために、不正な LLDP パケットを送り込む可能性もあります。

EX シリーズでは、デフォルトですべてのインタフェースで LLDP が有効です。LLDP のセキュリティを強化するため、この機能を必要とするインタフェース（ルーター側インタフェース、スイッチ側インタフェース、VoIP 電話など）でのみこの機能を有効にしてください。図 4.1 は、必要なインタフェースに LLDP が制限されたネットワークトポロジーの例です。

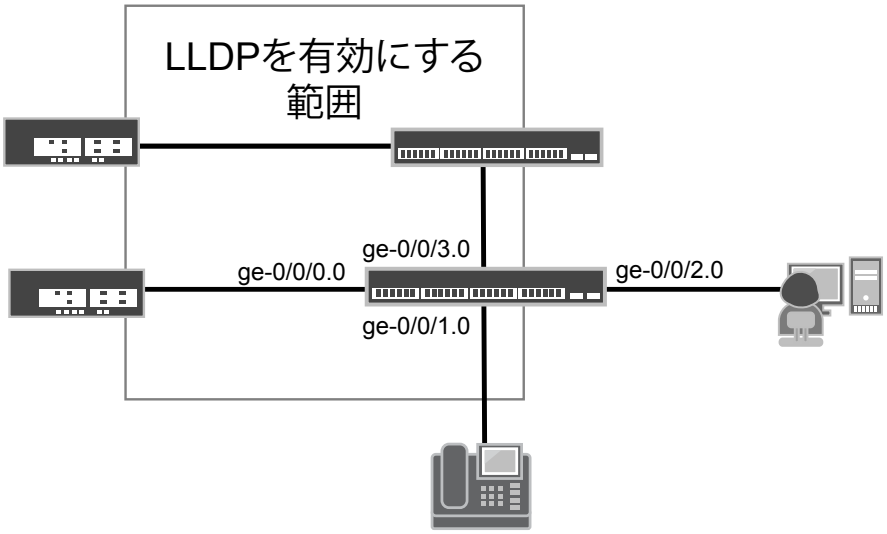

図 4.1　**推奨される LLDP の導入**

図 4.1 のトポロジーを参考に、まず、すべてのインタフェースで LLDP を無効にします。次に LLDP を有効にする必要のあるインタフェースを、明示的に定義します。

```
[edit]
jweidley@ex3200# edit protocols lldp
[edit protocols lldp]
jweidley@ex3200# set interface all disable
[edit protocols lldp]
jweidley@ex3200# set interface ge-0/0/0.0
[edit protocols lldp]
jweidley@ex3200# set interface ge-0/0/3.0
[edit protocols lldp]
jweidley@ex3200# top edit protocols lldp-med
[edit protocols lldp-med]
jweidley@ex3200# set interface ge-0/0/1.0
```

ここで、LLDP の完全な設定を確認してみましょう。

```
[edit protocols]
jweidley@ex3200# show
lldp {
    interface all {
        disable;
    }
    interface ge-0/0/0.0;
    interface ge-0/0/3.0;
}
lldp-med {
    interface all {
        disable;
    }
    interface ge-0/0/1.0;
}
```

注　LLDP および LLDP-MED は、EX シリーズで導入された機能ですが、現在は MX およびブランチ SRX プラットフォームにも実装されています。ご使用のプラットフォームでの LLDP および LLDP-MED のサポート状況については、ジュニパーネットワークスのオンライン参考資料で確認してください。

実践：LLDP で共有される情報

show lldp neighbors interface <interface> コマンドを使用して、LLDP によってどのような情報を取得できるかを見てみましょう。このコマンドを実際のデバイスで試してみます。

```
jweidley@srx210> show lldp neighbors interface fe-0/0/7.0
LLDP Neighbor Information:
Local Information:
Index:1 Time to live:120 Time mark:Tue Mar  1 22:59:37 2011 Age:0 secs
Local Interface    : fe-0/0/7.0
Parent Interface   :-
Local Port ID      :531
Ageout Count       :0
Neighbour Information:
Chassis type       :Mac address
Chassis ID         :00:23:9c:01:96:80
Port type          :Locally assigned
Port ID            :531
Port description   :Connection to SRX210 DMZ Port
System name        : ex3200

System Description :Juniper Networks, Inc. ex3200-24t , version 10.4R3.4 Build date:2010-08-13
12:56:38 UTC
System capabilities
        Supported  :Bridge Router
        Enabled    :Bridge Router
Management Info
        Type               :IPv4
        Address            :192.168.5.1
Port ID           :0
        Subtype            :1
        Interface Subtype :Unknown(1)
        OID                :1.3.6.1.2.1.31.1.1.1.1.0
```

出力の太字部分から、この SRX210 が EX3200 に接続されていること、この EX3200 が 24 の RJ-45 ポートを持つモデルであること、この EX3200 で Junos 10.4R3.4 が実行されていること、およびこの EX3200 の管理アドレスが 192.168.5.1 であることが分かります。

マネジメントサービス

ネットワークデバイスは、ネットワークの使用状況、エラー、およびトラフィックパターンに関する豊富な情報を提供することができます。ネットワークデバイスから取得した情報は、キャパシティプランニング、インシデントへの対応、障害の切り分け、および詳細解析にも利用できます。この情報は、正確かつタイムリーでなければならず、またセキュアな方法で取得する必要があります。

このセクションでは、情報の収集およびデバイスの設定ファイルのバックアップをセキュアに行う方法と、正確な時刻を保持するセキュアな方法について説明します。

NTP（Network Time Protocol）

セキュリティ監査の観点では、エンジニアがシステムイベントを相互に関連付け、問題の原因を収集できるように、時刻を正確に保つことが不可欠です。NTP（Network Time Protocol）は、複数のデバイスを共通のクロックに同期させるための業界標準です。NTP では UDP によって通信が行われるため、悪意のあるユーザーが NTP サーバーの IP アドレスになりすまして不正確なタイムスタンプを挿入しようとするなどのセキュリティリスクが考えられます。このようなリスクを低減するために、認証を利用して NTP のセキュリティを強化する必要があります。

Junos では、デフォルトで NTP は有効ではありません。以下の手順では、ハッシュメカニズムとして MD5 を使用した認証を実装して NTP を有効にする方法を示します。

さらに詳しくは NTP の詳細については、『*Junos OS Basic System Configuration Guide*』（http://www.juniper.net/techpubs/en_US/junos10.4/information-products/pathway-pages/system-basics/time-management.html）を参照してください。

MD5 認証を実装して NTP を有効にする方法

1. 基本的な NTP 設定を行います。

```
[edit]
jweidley@ex3200# set system time-zone America/New_York
[edit]
jweidley@ex3200# edit system ntp
[edit system ntp]
jweidley@ex3200# set boot-server 192.168.3.2
```

2. 認証キーを設定します。認証キーの ID と値は、NTP クライアントおよびサーバー間で一致させる必要があります。パスワード複雑性ポリシーに適合した共有秘密パスワードを選択します。

```
[edit system ntp]
jweidley@ex3200# set authentication-key 1 type md5 value Z3l>L8@w
```

3. 設定した認証キー ID を「trusted（信頼された）」キーとして設定します。

```
[edit system ntp]
jweidley@ex3200# set trusted-key 1
```

4. 正確な時間が不可欠であるため、プライマリおよびセカンダリ NTP サーバーを設定し、trusted キー ID を指定します。耐障害性を高めるために、セカンダリ NTP サーバーは、プライマリ NTP サーバーとは別のネットワーク上に配置します。

```
[edit system ntp]
jweidley@ex3200# set server 192.168.3.2 key 1 prefer
[edit system ntp]
jweidley@ex3200# set server 192.168.33.2 key 1
```

5.（オプション）set system default-address-selection が設定されていない場合、以下のコマンドを使用して、強制的にすべての NTP 通信がループバックアドレスを使用するようにします。

```
[edit system ntp]
jweidley@ex3200# set source-address 172.24.3.1
```

6. 設定を確認します。

```
[edit system ntp]
jweidley@ex3200# show
boot-server 192.168.3.2;
authentication-key 1 type md5 value " $9$-kboZjHqKvMWLNs4"; ## SECRET-DATA
server 192.168.3.2 key 1 prefer; ## SECRET-DATA
server 192.168.33.2 key 1; ## SECRET-DATA
trusted-key 1;
source-address 172.24.3.1;
```

7. 設定をコミットしてコメントします。

```
[edit system ntp]
jweidley@ex3200# commit and-quit comment "Configured NTP Auth"
commit complete
Exiting configuration mode
jweidley@ex3200>
```

8. NTP で時刻を更新し、適切に NTP が動作することを確認します。

```
jweidley@ex3200> set date ntp
10 Mar 17:30:34 ntpdate[27784]: step time server 192.168.3.2 offset 0.000603 sec
```

9. これで、NTP が設定され、動作可能な状態になりました。次のステップでは、NTP トラフィックのソースを信頼されたもののみに制限するために、ファイアウォールフィルタを設定して、NTP のセキュリティをさらに強化します。詳細については、この章の「ルーティングエンジンの保護」セクションを参照してください。

注意 Junos デバイスを他のネットワークデバイスの NTP ソースとして設定することも可能ですが、暗号化処理によりリソースが大量に消費される可能性があります。そのため、ベストセキュリティプラクティスとして、専用の NTP サーバーを導入することが推奨されます。

注 ベストセキュリティプラクティスとして、さらに、OOB 管理ネットワークに配置された NTP サーバーを使用して、マネジメントトラフィックとユーザートラフィックを分離することをお奨めします。

SNMPv2（Simple Network Management Protocol Version 2）

SNMP は、ネットワークデバイスをリモートから監視および管理するための標準プロトコルとして広く使用されています。SNMP には、ネットワークのトポロジーおよび使用状況に関するデータを収集する機能があるため、これをトラブルシューティングやプランニングに役立てることができます。SNMP は非常に便利なツールですが、旧バージョンの SNMP では単純なコミュニティベースのアクセスコントロールとなるため、本質的にセキュアではありません。SNMP のアクセスには、コミュニティストリングと呼ばれる単純なパスワードが用いられます。コミュニティストリングは暗号化されずにデバイス間で送信されるため、スヌーピング攻撃に対して脆弱になります。また、このプロトコルで標準または容易に推測可能なコミュニティストリングをデフォルトで有効にするベンダーがいたため、SNMP のセキュリティに対する評価はさらに低下しました。

セキュリティは、OOB（Out-of-Band）管理ネットワークを使用して、すべての SNMP 通信をユーザートラフィックと分離することにより、大幅に向上させることができます。

Junos OS では、SNMP はデフォルトで有効になっておらず、デフォルトのコミュニティストリングもありません。また、Junos には SNMP アクセスを分離・制限する、様々な機能が実装されています。このセクションでは、これらの機能の設定をご説明します。

ヒント コミュニティストリングはプレーンテキストで送信されるため、容易に読み取られる可能性があります。そのため、ベストセキュリティプラクティスとしては、複雑なコミュニティストリングを使用し、定期的に変更することが推奨されます。

さらに詳しくは SNMP の詳細および SNMP の例については、http://www.juniper.net/books で紹介されている『*Junos Cookbook*』（アビバ・ギャレット著、O’Reilly Media 発行、2006 年）を参照してください。

注 この SNMP セクションの設定例では、特定の MIB 名が使用されていますが、MIB は Junos のバージョンによっては異なる場合があります。Junos 10.4 の MIB 名の完全なリストについては、http://www.juniper.net/techpubs/en_US/junos10.4/topics/concept/juniper-specific-mibs-junos-nm.html または http://www.juniper.net/techpubs/en_US/junos10.4/information-products/topic-collections/reference-mibs-and-traps/ref-snmp-mibs-and-traps.pdf を参照してください。

SNMPv2 を有効にする方法

1. システムのロケーション情報として、そのデバイスを見つけやすい記述にします。

```
[edit snmp]
jweidley@ex3200# set location "DC1-Rack:8-Row:2"
```

2. システムのコンタクト先として、NOC がこのデバイスの緊急時または問題発生時に誰に連絡すればよいかが分かる記述にします。

```
[edit snmp]
jweidley@ex3200# set contact "CompanyName NOC:123.456.7890"
```

3. コミュニティストリングを定義します。コミュニティストリングは基本的にはパスワードであるため、通常は、パスワード複雑性ポリシーに適合したコミュニティストリングにします。

```
[edit snmp]
jweidley@ex3200# edit community S8M!y:4b
```

4. いくつかの書き換え可能な MIB によって設定が変更される可能性を排除するために、read-only モードのみを許可します。

```
[edit snmp community "S8M!y:4b"]
jweidley@ex3200# set authorization read-only
```

5. クエリーの送信を許可するプライマリおよびセカンダリ SNMPv2 サーバーを定義します。耐障害性を高めるために、セカンダリ SNMPv2 サーバーは、プライマリサーバーとは別のネットワーク上に配置します。

```
[edit snmp community "S8M!y:4b"]
jweidley@ex3200# set clients 192.168.3.3/32

[edit snmp community "S8M!y:4b"]
jweidley@ex3200# set clients 192.168.33.3/32
```

6. 設定を確認します。

```
[edit snmp]
jweidley@ex3200# show
location DC1-Rack:8-Row:2;
contact CompanyName NOC:123.456.7890;
community S8M!y:4b {
    authorization read-only;
    clients {
        192.168.3.3/32;
        192.168.33.3/32;
    }
 }
```

7. 設定をコミットしてコメントします。

```
[edit snmp]
jweidley@ex3200# commit and-quit comment "Configured SNMPv2"
commit complete
Exiting configuration mode

jweidley@ex3200>
```

8. これで、SNMP が設定されました。次のステップでは、SNMP トラフィックのソースを信頼されたもののみに制限するためにファイアウォールフィルタを設定して、SNMP 設定のセキュリティをさらに強化します。詳細については、この章の「ルーティングエンジンの保護」セクションを参照してください。

9.（オプション）SNMP クエリーを OOB（Out-of-Band）管理ネットワークで受信しない場合、SNMP クエリーを特定のインタフェースに制限することで、全体的なセキュリティを強化することができます。

```
[edit snmp]
jweidley@ex3200# set interface ge-0/0/1.0
```

SNMP ビューの使用方法

前述の設定では、定義された管理ステーションがネットワークデバイスの全ての MIB にアクセスすることができます。ただし、権限のある管理ステーションがすべての MIB オブジェクトに対し、繰り返しクエリを行った場合に、パフォーマンスに影響をおよぼす可能性があります。

このような意図していない事象を回避する 1 つの方法として、管理ステーションごとにアクセスできる MIB を制限することができます。これを行うには、View を作成します。View を作成するために、管理ステーションがアクセスする必要のある MIB を正確に特定しておく必要があります。

この例では、管理ステーションがシャーシインベントリ情報のみを取得する必要があると仮定しましょう。以下は、前述の SNMPv2 設定に View を追加する方法です。

1. 目的の MIB のみが含まれるビューを作成します。

```
[edit snmp]
jweidley@ex3200# set view inventory-only oid jnxBoxAnatomy include
[edit snmp]
jweidley@ex3200# set view inventory-only oid system include
```

2. この View を目的のコミュニティストリングに関連付けます。

```
[edit snmp]
jweidley@ex3200# set community S8M!y:4b view inventory-only
```

3. 設定を確認します。

```
[edit snmp]
jweidley@ex3200# show
location DC1-Rack:8-Row:2;
contact CompanyName NOC:123.456.7890;
view inventory-only {
    oid jnxBoxAnatomy include;
    oid system include;
}
community S8M!y:4b {
    view inventory-only;
    authorization read-only;
    clients {
        192.168.3.3/32;
        192.168.33.3/32;
    }
 }
```

複数の SNMP コミュニティの使用

単一のコミュニティでは、すべての管理ステーションが同じコミュニティストリングを使用して同じ情報にアクセスします。場合によっては、このような状況が望ましくないこともあります。そこで、複数の SNMP View と複数のコミュニティを使用することにより、特定の MIB へのアクセスをそれぞれ異なるコミュニティストリング（パスワード）によって分離することができます。

次の設定例では、`client-list` CLI オプションを使用して、組織ごとに SNMP 管理ステーションをグループ化します。”performance”という client-list はサービスプロバイダの SNMP ステーション用で、Anatomy、Interface、OSPF、BGP の各 MIB にアクセスできます。一方、”partner”という client-list は、パートナーの SNMP ステーションを定義し、インタフェース MIB のみに制限されます。

1. サービスプロバイダの管理サーバー用の View を作成します。

```
[edit snmp]
jweidley@MX80# set view system-level oid jnxBoxAnatomy include

[edit snmp]
jweidley@MX80# set view system-level oid 1.3.6.1.2.1.2 include

[edit snmp]
jweidley@MX80# set view system-level oid 1.3.6.1.2.1.14 include

[edit snmp]
jweidley@MX80# set view system-level oid 1.3.6.1.2.1.15 include
```

2. パートナーの管理サーバーの View を作成します。

```
[edit snmp]
jweidley@MX80# set view limited oid 1.3.6.1.2.1.2 include
```

3. サービスプロバイダのサーバー用の client-list を作成します。

```
[edit snmp]
jweidley@MX80# set client-list performance 192.168.10.0/28

[edit snmp]
jweidley@MX80# set client-list performance 192.168.20.0/28
```

4. パートナーのサーバーの client-list を作成します。

```
[edit snmp]
jweidley@MX80# set client-list partner 172.16.1.0/28

[edit snmp]
jweidley@MX80# set client-list partner 172.16.10.0/28
```

5. 1 つ目のコミュニティストリングを作成し、読み取り専用アクセスに設定して、サービスプロバイダの client-list および View を関連付けます。

```
[edit snmp]
jweidley@MX80# set community CfL!d4#2 authorization read-only

[edit snmp]
jweidley@MX80# set community CfL!d4#2 client-list-name performance

[edit snmp]
jweidley@MX80# set community CfL!d4#2 view system-level
```

6. 2 つ目のコミュニティストリングを作成し、読み取り専用アクセスに設定して、パートナーの client-list および View を関連付けます。

```
[edit snmp]
jweidley@MX80# set community xH#5^Gp9 authorization read-only

[edit snmp]
jweidley@MX80# set community xH#5^Gp9 client-list-name partner

[edit snmp]
jweidley@MX80# set community xH#5^Gp9 view limited
```

7. 設定全体を確認します。

```
[edit snmp]
jweidley@MX80# show
location DC1-Rack:5-Row:2;
contact "CompanyName NOC:123.456.7890";
view system-level {
    oid jnxBoxAnatomy include;
    oid 1.3.6.1.2.1.2 include;
    oid 1.3.6.1.2.1.14 include;
    oid 1.3.6.1.2.1.15 include;
}
view limited {
    oid 1.3.6.1.2.1.2 include;
}
client-list performance {
    192.168.10.0/28;
    192.168.20.0/28;
}
client-list partner {
    172.16.1.0/28;
    172.16.10.0/28;
}
community "CfL!d4#2" {
    view system-level;
    authorization read-only;
    client-list-name performance;
}
community "xH#5^Gp9" {
    view limited;
    authorization read-only;
    client-list-name partner;
}
```

8. 設定の変更をコミットしてコメントします。

```
[edit]
jweidley@MX80# commit and-quit comment "enabled multiple snmp communities"
commit complete
Exiting configuration mode

jweidley@MX80>
```

SNMPv3（Simple Network Management Protocol Version 3）

前述のとおり、SNMP v1 および v2 の主な欠点は、すべての通信に対して暗号化も認証も行われないことです。すなわち、ネットワーク経由でデバイスにアクセスできさえすれば、クエリーを送信し、コミュニティストリングを推測することができます。また、パケットをキャプチャしてネットワークに関する詳細情報を入手することも可能です。

SNMPv3 では、USM（User Security Module）を使用して SNMP 通信を認証および暗号化することにより、セキュリティを強化できます。Junos における SNMPv3 の実装では、さまざまなハッシュおよび暗号化アルゴリズムがサポートされています。最も強力な手法では最高レベルのセキュリティが実現されるのは当然ですが、現実的にはご使用の管理ステーションでサポートされているアルゴリズムと暗号化を選択しなければなりません。

設定例に入る前に、SNMPv3 エンジン ID について理解しておくことが必要です。エンジン ID は、SNMP マネージャに対してデバイスを識別するために使用され、一意の値でなければなりません。デフォルトでは、ローカルエンジン ID として、デバイスのデフォルト IP アドレスが使用されます。ただし、SNMP 管理ステーションまたは個別の環境に適応させるために、別の値を利用したい場合もあるでしょう。

注意 SNMPv3 の認証キーおよび暗号化キーは、関連付けられているパスワードとエンジン ID に基づいて生成されます。エンジン ID を変更する場合、SNMPv3 ユーザーパスワードも変更する必要があります。これは、このパスワードが以前のエンジン ID に基づいているためで、設定をコミットするときに警告が表示されます。そのため、最初にエンジン ID を設定してから、SNMPv3 ユーザーを設定するのがよいでしょう。

さらに詳しくは エンジン ID の詳細については、ジュニパーネットワークスの技術資料（http://www.juniper.net/techpubs/en_US/junos10.4/topics/task/configuration/local-engine-id-configuring-junos-nm.html）を参照してください。

さらに詳しくは SNMP の詳細および SNMP の設定例については、http://www.juniper.net/books で紹介されている『*Junos Cookbook*』（アビバ・ギャレット著、O' Reilly Media 発行、2006 年）を参照してください。

SNMPv3 通信のための USM の設定方法

1. エンジン ID を管理インタフェースの MAC アドレスに設定します。

```
[edit snmp]
jweidley@srx210# set engine-id use-mac-address
```

2. この SNMPv3 ユーザーがアクセス可能な MIB を制限するため、限定的な View を作成します。

```
[edit snmp]
jweidley@srx210# set view inventory-view oid jnxBoxAnatomy include

[edit snmp]
jweidley@srx210# set view inventory-view oid system include
```

3. SNMPv3 ユーザーアカウントを作成し、認証およびプライバシーアルゴリズムを選択して、パスワードを選択します。この例では、最大限のセキュリティを提供するために、最もセキュアなハッシュおよび暗号化手法を使用します。認証およびプライバシーパスワードは、組織のパスワード複雑性ポリシーに適合した、それぞれ異なる一意の値にすることに注意してください。

```
[edit snmp]
jweidley@srx210# edit v3

[edit snmp v3]
jweidley@srx210# set usm local-engine user nms-user authentication-sha authentication-password
S8M!y:4b

[edit snmp v3]
jweidley@srx210# set usm local-engine user nms-user privacy-aes128 privacy-password $Y5wIm@4
```

4. VACM は、View-based Access Control Model（ビューベースのアクセスコントロールモデル）の略で、手順 1 ～ 3 の設定を関連付けることによりアクセスを制御します。

```
[edit snmp v3]
jweidley@srx210# edit vacm

[edit snmp v3 vacm]
jweidley@srx210# set security-to-group security-model usm security-name nms-user group
inventory-view

[edit snmp v3 vacm]
jweidley@srx210# set access group inventory default-context-prefix security-model usm security-
level privacy read-view inventory-view
```

```
[edit snmp v3 vacm]
jweidley@srx210# set access group inventory default-context-prefix security-model usm security-
level privacy notify-view inventory-view
```

5. 設定を確認します。

```
[edit snmp v3 vacm]
jweidley@srx210# up 2

[edit snmp]
jweidley@srx210# show
v3 {
    usm {
        local-engine {
            user nms-user {
                authentication-sha {
                    authentication-key "$9$BcnEreMWxws48Lk.P5F39ApOBEcylvMXn/u1IEyrvWLxbsUjH.mTJZ
9AtpB1X7Nb4aiHmf5FmP39CAOONdVsYojHqzn/goDk.mTQcyrlWLs24aJD4oUHmfzFn/CABIylK8xN69OIESeKoJZUDkmPQF3
9HkIEhSMWaZGUqm69ABRhOO1hSyW8-VwY2a"; ## SECRET-DATA
                }
                privacy-aes128 {
                    privacy-key "$9$yg6eK87NbY4aSrWxN-wsz3nCOBcylKvLREgoaGiHfTz3nCOORSyKuOhrKMN-.
Pfz9AOBEeK836KMLxdV24aZGik.PTQnVwz369OBSreMWxws4GUHaJ36AtIRlKMW7-s24aGDre24oJHkIEhrM8-Vwsgo8Lik.
mF3hSyKvLxNdb24LXHq.fzF69AuIE"; ## SECRET-DATA
                }
            }
        }
    }
    vacm {
        security-to-group {
            security-model usm {
                security-name nms-user {
                    group inventory-view;
                }
            }
        }
        access {
            group inventory {
                default-context-prefix {
                    security-model usm {
                        security-level privacy {
                            read-view inventory-view;
                            notify-view inventory-view;
                        }
                    }
                }
            }
        }
    }
}
engine-id {
    use-mac-address;
}
view inventory-view {
    oid jnxBoxAnatomy include;
    oid system include;
}
```

6. これで、SNMPv3 が設定されました。次のステップでは、SNMP トラフィックを信頼されたソースのみに制限するためにファイアウォールフィルタを設定して、SNMP 設定のセキュリティをさらに強化します。詳細については、この章の「ルーティングエンジンの保護」セクションを参照してください。

SNMPv3 トラップ

SNMP トラップは、管理ステーションに重要なイベントを通知するためにネットワークデバイスから送信されるメッセージです。前のセクションでは、SNMP トラップについて説明しませんでしたが、これは、セキュリティ機能を設定するうえで、強力なコミュニティストリングと OOB 管理ネットワークを使用すること以外にそれ程重要なことはないためです。

前述の暗号化セキュリティと USM（User Security Model）は、SNMPv3 トラップの生成にも適用されますが、以下の例では、Junos デバイスが SNMPv3 管理ステーションに SNMPv3 トラップを送信できるようにするために必要な設定を行います。

SNMPv3 の設定は多少分かりにくいため、前の SNMPv3 設定を削除し、SNMPv3 トラップを最初から設定しましょう。

注意 SNMPv3 の認証キーおよび暗号化キーは、関連付けられているパスワードとエンジン ID に基づいて生成されます。エンジン ID を変更する場合、SNMPv3 ユーザーパスワードも変更する必要があります。これは、このパスワードが以前のエンジン ID に基づいているためで、設定をコミットするときに警告が表示されます。そのため、最初にエンジン ID を設定してから、SNMPv3 ユーザーを設定するのがよいでしょう。

1. エンジン ID を管理インタフェースの MAC アドレスに設定します。

```
[edit snmp]
jweidley@srx210# set engine-id use-mac-address
```

2. SNMPv3 ユーザーアカウントを作成し、認証および暗号化アルゴリズムを選択して、パスワードを選択します。この例では、最高レベルのセキュリティを設定するために、最もセキュアなハッシュおよび暗号化手法を使用します。認証パスワードとプライバシーパスワードは、組織のパスワード複雑性ポリシーに適合した、それぞれ異なるユニークな値にするよう注意してください。

```
[edit snmp]
jweidley@srx210# edit v3

[edit snmp v3]
jweidley@srx210# set usm local-engine user nms-user authentication-sha authentication-password
S8M!y:4b

[edit snmp v3]
jweidley@srx210# set usm local-engine user nms-user privacy-aes128 privacy-password $Y5wIm@4
```

3. SNMP では、複数のタイプの通知がサポートされます。この例では、通知方法として trap を指定し、chassis-trap-receivers という名前の参照タグを作成します。この参照タグは手順 5 で使用します。

```
 [edit snmp v3]
jweidley@srx210# set notify chassis-trap-list type trap

[edit snmp v3]
jweidley@srx210# set notify chassis-trap-list tag chassis-trap-receivers
```

4. マネージャに送信するトラップ MIB を定義します。

```
[edit snmp v3]
jweidley@srx210# set notify-filter chassis-traps oid jnxChassisTraps include

[edit snmp v3]
jweidley@srx210# set notify-filter chassis-traps oid jnxChassisOKTraps include
```

5. トラップを受信する SNMP マネージャ（ターゲット）の IP アドレスを指定します。手順 3 のタグリストおよび手順 6 の特定の SNMPv3 パラメータにサーバーをリンクすることもできます。

```
[edit snmp v3]
jweidley@srx210# edit target-address nms1

[edit snmp v3 target-address nms1]
jweidley@srx210# set address 192.168.3.2

[edit snmp v3 target-address nms1]
jweidley@srx210# set tag-list chassis-trap-receivers

[edit snmp v3 target-address nms1]
jweidley@srx210# set target-parameters noc-snmpv3-settings
```

6. ネットワーク管理サーバーに通知するときの SNMPv3 パラメータを設定します。

```
[edit snmp v3 target-address nms1]
jweidley@srx210# up

[edit snmp v3]
jweidley@srx210# edit target-parameters noc-snmpv3-settings

[edit snmp v3 target-parameters noc-snmpv3-settings] jweidley@srx210# set parameters message-
processing-model v3

[edit snmp v3 target-parameters noc-snmpv3-settings]
jweidley@srx210# set parameters security-model usm

[edit snmp v3 target-parameters noc-snmpv3-settings]
jweidley@srx210# set parameters security-level privacy

[edit snmp v3 target-parameters noc-snmpv3-settings]
jweidley@srx210# set parameters security-name nms-user

[edit snmp v3 target-parameters noc-snmpv3-settings]
jweidley@srx210# set notify-filter chassis-traps
```

7. 設定を確認します。

```
[edit snmp v3 target-parameters noc-snmpv3-settings]
jweidley@srx210# up 2

[edit snmp]
jweidley@srx210# show
v3 {
    usm {
        local-engine {
            user nms-user {
                authentication-sha {
                    authentication-key "$9$jQq5Q3nCB1h6/8X7-ws4aZUjqmfTF39YgGiHqf5Fn/
CO1evWXxdyr4aJZji9AtOhSMWxN-wx7s4oaUDtuO1IcvWLbYgEcK8XxdVmf5Tn/1RhSyKhceWxNbwYgoajHfTz6Ct24UHqPQz
cyreK8x7Vws4W8Hq.P3nSrleLx24ajk.UDi.Pfn6pOBIRS"; ## SECRET-DATA
                }
                privacy-aes128 {
                    privacy-key "$9$gnaJDkqfQ3624UHq.5TyleW7-YgoJZjbwFn6CuOEcyleW7Nb2gJx7s4JGq.1R
EyM8N-waJDlKJGjHmPz369CuO1RcSeP5ylKMN-24aGUH5T3CAO6/lK8LVboJGUk.Tz36Ct4az3n/OOVws4GD.P5TFnDjuO1Ir
ls2gJZjHqmfz3jiOB1EyrKM8xVw"; ## SECRET-DATA
                }
            }
        }
    }
```

```
    target-address nms1 {
        address 192.168.3.2;
        tag-list chassis-trap-receivers;
        target-parameters noc-snmpv3-settings;
    }
    target-parameters noc-snmpv3-settings {
        parameters {
            message-processing-model v3;
            security-model usm;
            security-level privacy;
            security-name nms-user;
        }
        notify-filter chassis-traps;
    }
    notify chassis-trap-list {
        type trap;
        tag chassis-trap-receivers;
    }
    notify-filter chassis-traps {
        oid jnxChassisTraps include;
        oid jnxChassisOKTraps include;
    }
}
engine-id {
    use-mac-address;
}
```

ここでは分かりやすくするために、トラップレシーバーを 1 つのみ設定していますが、実際の環境では、耐障害性を高めるために、Junos OS の target-address コマンドで複数のレシーバーを設定してください。

Syslog

Syslog は、システム情報をローカルに、または指定のリモートサーバーに記録する業界標準です。ロギングはシステムアクティビティのオーディットトレイルを作成するもので、コンフィグレーションエラーの特定、デバイスへの侵入確認、サービスダウン時のトラブルシューティング、プローブやスキャンへの対応といったことに役立ちます。ロギングはデバイスのセキュリティの強化に不可欠なのです。

注 Junos デバイスプラットフォームには、ローカルログを保存できる十分な容量のドライブスペースがあります。Syslog サーバーを使用できない場合や Syslog パケットがネットワーク上でドロップされた場合に備えて、ローカルにログを保存できるため、セキュリティが向上します。

一般的には、リモートログは監査用途に使用され、ローカルログはトラブルシューティングに使用されます。ログメッセージタイプごとにログファイルを分け、ローカルに保存することも可能です。これは、ユーザーにより実行されたコマンドなど特定のメッセージタイプは監査人などの特定のユーザーのみが表示できるようにし、一般ユーザーはこれらのログを表示できないようにする、といった場合に便利です。

以下では、ローカルおよびリモート Syslog を設定し、各ログファイルに別々のメッセージタイプを保存する設定をします。

1. デバイスにログインしているユーザーに対して emergency レベルのメッセージが表示されるようにします。

```
[edit]
```

```
jweidley@EX3200# edit system syslog

[edit system syslog]
jweidley@EX3200# set user * any emergency
```

2. すべての info レベルのメッセージがデバイスの messages ファイルにローカルでロギングされるようにします。

```
[edit system syslog]
jweidley@EX3200# set file messages any info

[edit system syslog]
jweidley@EX3200# set file messages authorization info
```

3. User-Auth という名前の別ファイルを作成します。このファイルには、すべての認証情報と、ログインしているユーザーが実行したすべてのコマンドが保持されます。

```
[edit system syslog]
jweidley@EX3200# set file User-Auth authorization any

[edit system syslog]
jweidley@EX3200# set file User-Auth interactive-commands any
```

4. 次に、audit という名前のファイルを作成します。このファイルには、ログインしているユーザーが実行したすべてのコマンドが保持されます。

```
[edit system syslog]
jweidley@EX3200# set file audit interactive-commands any
```

5. 次に、processes という名前のファイルを作成します。このファイルには、システムデーモンで生成されたログメッセージが保持されます。

```
[edit system syslog]
jweidley@EX3200# set file processes daemon any
```

6. コンソールへの接続時に、デバイスの現在のステータスを通知するシステムメッセージが表示されると便利です。コンソールに接続しているときに、この情報が表示されるようにします。

```
[edit system syslog]
jweidley@EX3200# set console any any
```

7. 高度なセキュリティが要求される環境では、監査および障害対応のため、すべてのメッセージをリモートの Syslog サーバーに送信することをお奨めします。耐障害性を高めるために、2 台の Syslog サーバーを設定してください。

```
[edit system syslog]
jweidley@EX3200# set host 192.168.3.2 any any

[edit system syslog]
jweidley@EX3200# set host 192.168.4.2 any any
```

8. デフォルトでは、リモートサーバーに送信される Syslog メッセージにはホスト名が含まれません。混乱を避けるために、log-prefix オプションを使用し、ホスト名などのユニークな識別子を全ての Syslog メッセージに含めることをお奨めします。

```
[edit system syslog]
jweidley@EX3200# set host 192.168.3.2 log-prefix EX3200

[edit system syslog]
jweidley@EX3200# set host 192.168.4.2 log-prefix EX3200
```

9.（オプション）ネットワーク内の一貫性と耐障害性を確保するために、Syslog トラフィックの送信元をループバックアドレスにしてください。set system default-address selection が設定されていない場合は、以下のコマンドを使用します。

```
[edit system syslog]
jweidley@EX3200# set source-address 192.168.5.1
```

10. 場合によっては、デフォルトの時間形式では、セキュリティ監査や障害時の詳細解析には精度が不十分な場合があります。タイムスタンプの精度をできる限り高めるには、millisecond および year オプションを使用します。

```
[edit system syslog]
jweidley@EX3200# set time-format millisecond year
```

11. 設定を確認します。

```
[edit system syslog]
jweidley@EX3200# show
user * {
    any emergency;
}
host 192.168.3.2 {
    any any;
    log-prefix EX3200;
}
host 192.168.4.2 {
    any any;
    log-prefix EX3200;
}
file messages {
    any info;
    authorization info;
}
file User-Auth {
    authorization any;
    interactive-commands any;
}
file audit {
    interactive-commands any;
}
file processes {
    daemon any;
}
console {
    any any;
}
time-format year millisecond;
```

ロギング要件は、企業によって大きく異なります。幸い、Junos における Syslog の実装には多くの機能が用意されているため、多様な要件に対応することができます。

さらに詳しくは リモート Syslog メッセージへのホスト名の追加に関する詳細については、ナレッジベース KB12679 を参照してください（http://kb.juniper.net/InfoCenter/index?page=content&id=KB12679&cat=SRX_SERIES&actp=LIST）。

さらに詳しくは 本書の範囲外ですが、ログファイルの管理も重要なトピックです。内部ストレージに保持できるデータ量には限りがあるため、デバイスに保存する必要のあるログの量とスペースの容量のバランスを取る必要があります。ログファイルのサイズと数を制限する設定例については、http://www.juniper.net/books で紹介されている『*Junos Cookbook*』（アビバ・ギャレット著、O’ Reilly Media 発行、2006 年）を参照してください。

さらに詳しくは Syslog のプランニングおよび実装の詳細については、http://www.juniper.net/books で紹介されている『*Junos High Availability*』（ジェイムズ・ソンデレガー、オリン・ブロムバーグ、キーラン・ミルネ、およびセナド・パリスラモビック著、O'Reilly Media 発行、2009 年）を参照してください。

コンフィグレーションのバックアップ

コンフィグレーションのバックアップは、障害復旧に不可欠です。また、デバイスの管理においても、おそらく最も重要であるにも関わらず、最も軽視されがちな要素の 1 つです。

Junos OS では、デフォルトで過去のコンフィグレーションのコピーがデバイスに保存されます（その数はプラットフォームによって異なります）。この機能により、設定不備から素早く復旧したり（`rollback` 機能を使用）、コミットの前後で何が変わったかを確認する作業（`compare` 機能を使用）が簡単に行えます。この機能に加え、致命的なデバイス障害が発生した場合やデバイスの復旧が必要になった場合に設定を読み込めるよう、コンフィグレーションを外部システムにアーカイブすることもお奨めします。このアーカイブ用のサーバーは、必要な担当者にのみにアクセスを制限した、セキュリティが強化されたサーバーでなければなりません。

デバイス設定をバックアップするオープンソースまたは市販ソフトウェアパッケージがいくつかありますが、このセクションでは、コンフィグレーションをアーカイブする Junos の機能とその設定について取り上げます。

設定は、手動でローカルに保存することも、リモートサーバーに保存することもできます。ここでは、信頼性と一貫性を確保するために、デバイス設定を自動的にアーカイブする 2 つの方法を設定します。

さらに詳しくは このセクションで説明するバックアップ情報の詳細については、http://www.juniper.net/techpubs/en_US/junos/topics/task/configuration/junos-software-system-management-router-configuration-archiving.html を参照してください。

コンフィグレーションの定期的バックアップの設定

設定を頻繁に変更する必要のないデバイスでは、定期的に自動でバックアップしておくとよいでしょう。

このセクションでは、Junos の `transfer-interval` 機能を設定して、設定が 24 時間（1440 分）おきにアーカイブされるようにします。Junos はいくつかの転送プロトコルをサポートしていますが、ここでは、転送時の機密性と完全性を確保するために SCP（Secure Copy）を使用します。

1. `transfer-interval` オプションを設定します。設定のバックアップ間隔を分単位で定義します（15 ～ 2880 の範囲で指定可能です）。

```
[edit]
jweidley@EX3200# edit system archival configuration

[edit system archival configuration]
jweidley@EX3200# set transfer-interval 1440
```

2. アーカイブサーバーのサーバーユーザー名、ホスト名、ディレクトリ、パスワードを入力します。入力形式が非常に特殊なため、正しく入力してください。

```
[edit system archival configuration]
jweidley@EX3200# set archive-sites scp://jweidley@192.168.3.2:/Configs password 3zP%a9@E
```

3. Enter キーを押すと、アーカイブサーバーとの間で SSH 接続を確立し、アーカイブサーバの公開鍵を入手します。yes と入力して処理を続行します。

```
The authenticity of host /192.168.3.2 (192.168.3.2)/ can/t be established.
RSA key fingerprint is 84:da:22:78:d2:26:df:86:e5:1f:c0:33:41:db:35:02.
Are you sure you want to continue connecting (yes/no)?yes
Warning:Permanently added /192.168.3.2/ (RSA) to the list of known hosts.

[edit system archival configuration]
jweidley@EX3200#
```

4. 設定を確認します。

```
[edit system archival configuration]
jweidley@EX3200# show
transfer-interval 1440;
archive-sites {
    "scp://jweidley@192.168.3.2:/Configs" password "$9$EGCyMCVb1JGnev2aajPf359AO1"; ## SECRET-
DATA
}
```

アーカイブサーバーの公開鍵は、Junos の [security ssh-known-hosts] 階層下の設定に自動的に保存されます。

このファイルがアーカイブサーバーに転送されるときには、デバイスのホスト名と転送日時から成るユニークなファイル名が付けられます。

```
<device-name>_juniper.conf[.gz]_YYYYMMDD_HHMMSS
```

注意 手順 2 のコマンドでは、コマンドの一部としてアーカイブサーバーのパスワードを入力する必要があります。パスワードをのぞき見られたりコンソールのログから取得されないよう、必要なセキュリティ対策を講じてください。また、手順 4 では、Junos により、実際のパスワードではなくパスワードのハッシュ計算値が保存され、セキュリティが維持されていることが分かります。

ヒント コンフィグレーションのアーカイブを設定したら、ログで確認してください（show log messages）。Junos では、転送の成功および失敗を示すメッセージが生成されます。

コンフィグレーションのオンデマンドバックアップの設定

コンフィグレーションの変更が頻繁に行われるデバイスでは、24 時間おきでは最新の設定情報がバックアップされていない状況が発生しうるため、定期バックアップが最適ではない場合があります。

そこで、transfer-on-commit コマンドを設定し、コミットの完了後に Junos OS により設定がアーカイブサーバーに転送されるようにしましょう。これにより、定期バックアップに加え、設定を変更するたびに自動的にバックアップが行われます。Junos では複数の転送プロトコルを使用できますが、ここでは、転送時の機密性と完全性を確保するために SCP(Secure Copy) を使用します。

1. 最初に、transfer-on-commit オプションを有効にします。

```
[edit]
jweidley@EX3200# edit system archival configuration
```

```
[edit system archival configuration]
jweidley@EX3200# set transfer-on-commit
```

2. アーカイブサーバーのユーザー名、ホスト名、ディレクトリ、パスワードを入力します。入力形式が非常に特殊なため、正しく入力してください。

```
[edit system archival configuration]
jweidley@EX3200# set archive-sites scp://jweidley@192.168.3.2:/Configs password 3zP%a9@E
```

3. Enter キーを押すと、アーカイブサーバーとの間で SSH 接続を確立し、アーカイブサーバの公開鍵を入手します。yes と入力して処理を続行します。

```
The authenticity of host /192.168.3.2 (192.168.3.2)/ can/t be established.
RSA key fingerprint is 84:da:22:78:d2:26:df:86:e5:1f:c0:33:41:db:35:02.
Are you sure you want to continue connecting (yes/no)?yes
Warning:Permanently added /192.168.3.2/ (RSA) to the list of known hosts.

[edit system archival configuration]
jweidley@EX3200#
```

4. 設定を確認します。

```
[edit system archival configuration]
jweidley@EX3200# show
transfer-on-commit;
archive-sites {
    "scp://jweidley@192.168.3.2:/Configs" password "$9$EGCyMCVb1JGnev2aajPf359AO1"; ## SECRET-DATA
}
```

アーカイブサーバーの公開鍵は、Junos の [security ssh-known-hosts] 階層下の設定に自動的に保存されます。

このファイルがアーカイブサーバーに転送されるときには、デバイスのホスト名と転送日時から成るユニークなファイル名が付けられます。

```
<device-name>_juniper.conf[.gz]_YYYYMMDD_HHMMSS
```

注意 手順 2 のコマンドでは、コマンドの一部としてアーカイブサーバーのパスワードを入力する必要があります。パスワードをのぞき見られたりコンソールのログから取得されないよう必要なセキュリティ対策を講じてください。また、手順 4 では、Junos により、実際のパスワードではなくパスワードのハッシュ計算値が保存され、セキュリティが維持されていることが分かります。

ヒント コンフィグレーションのアーカイブを設定したら、ログで確認してください（show log messages）。Junos では、転送の成功および失敗を示すメッセージが生成されます。

アクセスセキュリティ

Junos デバイスは、さまざまな方法で管理することができます。このセクションでは、セキュアではないアクセスサービスを無効にする方法、セキュアなアクセスサービスを有効にする方法、および警告バナーを設定する方法を説明します。

デフォルトでは、すべてのアクセスサービスが無効になっているため、必要なサービスを個別に有効化する必要があります。ただし、ブランチ SRX プラットフォームと一部の J シリーズ ルーターは例外で、一部のサービスが「trust」ゾーンでデフォルトで有効になっています。

注 このセクションで説明するサービス以外にも、Junos OS でサポートされるセキュアなアクセスサービスがあります。これらのサービスについても、以下に説明するサービスと同様にセキュリティを強化することができます。

警告バナー

組織のセキュリティを強化するためにできる最も簡単なことの１つが、電子的な「立ち入り禁止」標識である警告バナーを設定することです。これによって技術的にデバイスが保護されるわけではありませんが、警告バナーで使用上の注意事項を示し、リマインダーとして、また法的免責事項として機能させることで、役に立つこともあります。

最も効果的なのは、ユーザーがログインアカウント情報を入力する前に警告バナーを提示することです。

Junos では警告バナーの文字数は最大 2048 文字まで入力可能です。これは、デバイスを操作する上でユーザが期待されることを詳細に記述するのに十分な文字数です。

警告バナーの設定は簡単に行えます。以下に例を示します。

```
[edit]
jweidley@MX80# set system login message "\n\tUNAUTHORIZED USE OF THIS SYSTEM\n\tIS STRICTLY
PROHIBITED!\n\tPlease contact \/company-noc@company.com\/ to gain\access to this equipment if
you need authorization.\n"
```

このログインメッセージの設定例により、以下のようなログインメッセージが生成されます。

```
server% ssh router1
Trying 1.1.1.1...
Connected to router1.
Escape character is /^]/.

   UNAUTHORIZED USE OF THIS SYSTEM
   IS STRICTLY PROHIBITED!

   Please contact /company-noc@company.com/ to gain
   access to this equipment if you need authorization.

MX80 (ttyp0)
login:
```

さらに詳しくは ログインメッセージの形式の詳細については、http://www.juniper.net/techpubs/en_US/junos10.4/topics/task/configuration/authentication-router-login-message.html を参照してください。

セキュアではないアクセスサービスの無効化

デバイスとの通信が暗号化されていない場合、アクセスサービスはセキュアではないと考えるべきです。クリアテキストによる通信は、のぞき見やパケットキャプチャー攻撃を受けやすくなります。また、IP スプーフィングのように、攻撃者がコマンドを実行する目的で信頼された IP アドレスのなりすましを行う可能性もあります。

多くの Junos デバイスプラットフォームでは、デフォルトでリモートアクセスサービスは有効になっていませんが、このセクションで説明するコマンドを使用することにより、展開済みのデバイス上でセキュアではないアクセスサービスを無効にすることができます。

注意 さまざまな理由（Junos イメージの転送、トラブルシューティング、管理など) で、セキュアではないアクセスサービスが実稼働環境で有効になっている可能性があります。これらのサービスを無効にする前に、実際の環境でこれらのサービスがどのように利用されているかを確認してください。

セキュアではないアクセスサービスの無効化方法

1. Berkeley r コマンドを無効にします。r コマンドは、利便性のためパスワードを入力しなくても使用できます。以下のコマンドはどちらも hidden でドキュメント化されていません。これらのサービスを有効にする方法は、パブリックソースから入手できます。

```
[edit system services]
jweidley@ex3200# delete rsh

[edit system services]
jweidley@ex3200# delete rlogin
```

2. FTP を無効にします。

```
[edit system services]
jweidley@ex3200# delete ftp
```

3. Finger を無効にします。

```
[edit system services]
jweidley@ex3200# delete finger
```

4. Telnet を無効にします。

```
[edit system services]
jweidley@ex3200# delete telnet
```

5. HTTP による J-Web を無効にします。

```
[edit system services]
jweidley@ex3200# delete web-management http
```

注 有効になっていないアクセスサービスを無効にしようとすると、Junos により以下のエラーメッセージが表示されます。

```
[edit system services]
jweidley@ex3200# delete finger
warning: statement not found
```

これは警告メッセージですが、重要な問題を示すものではありません。複数のデバイスにセキュリティ強化テンプレートを適用するときに、このことを覚えておくとよいでしょう。

さらに詳しくは 当然ながら、セキュアではないアクセスサービスを無効にしても、権限のあるエンジニアがこれらのアクセスサービスを再度有効化するのを阻止することはできません。ただし、Junos オートメーションスクリプティングを使用して、デバイスのアクセスサービスの設定を監視することは可能です。また、これらのセキュアではないサービスをチェックして警告を表示するスクリプトや、これらの設定のコミットを許可しないスクリプトを作成し、インストールすることができます。このようなスクリプトを作成する際に参考にできるスクリプト例については、ジュニパーネットワークスの Configuration Automation ライブラリ（http://www.juniper.net/us/en/community/junos/script-automation/library/configuration/）を参照してください。

セキュアなアクセスサービスの有効化

通信が暗号化され、スヌーピングから保護されている場合、アクセスサービスはセキュアと考えられます。このセクションでは、セキュアなアクセスサービスを有効にする方法を説明し、さらにセキュリティを強化するオプションについて紹介します。

Secure Shell

SSH（Secure Shell）は、セキュアチャネルを使用してデバイス間でデータを交換するためのネットワークプロトコルです。SSH は、Telnet やその他セキュアではないアクセスプロトコルに代わるものとして設計されました。

SSH のセキュリティ強化方法

1. SSHv1 には、マン・イン・ザ・ミドル攻撃に対して脆弱であるため、SSHv2 のみを使用します。

```
[edit system services]
jweidley@ex3200# set ssh protocol-version v2
```

2. root アカウントでの SSH アクセスを拒否します。SSH を有効にすると、root アカウントも含め、設定されているすべてのユーザーがデバイスにアクセスできるようになります。

```
[edit system services]
jweidley@ex3200# set ssh root-login deny
```

root アカウントの SSH アクセスを無効にしないと、以下の 2 つの問題が生じます。

- root アカウントは、Junos デバイスで最も強力なアカウントであり、すべての Junos デバイスに存在します。総当たり方式でデバイスにアクセスしようとする者は、有効なユーザー名とパスワードを両方推測しなければなりません。しかし SSH によるルートアクセスを無効にしない場合、パスワードのみを推測すればよいため、作業が半分で済むことになります。
- 前述のとおり、root アカウントにはログインクラスが関連付けられないため、操作が行われていないことを理由に自動的にログアウトすることはありません。

3. リソースを保護し、DoS（Denial of Service）の可能性を低減するために、総接続数を制限します。

```
[edit system services]
jweidley@ex3200# set ssh connection-limit 10
```

4. リソースを保護し、DoS（Denial of Service）の可能性を低減するために、1 分あたりのログイン数を制限します。

```
[edit system services]
jweidley@ex3200# set ssh rate-limit 2
```

5. 設定を確認します。

```
[edit system services]
jweidley@ex3200# show
ssh {
    root-login deny;
    protocol-version v2;
    connection-limit 10;
    rate-limit 2;
}
```

6. これで、SSH が設定されました、次のステップでは、接続を信頼されたソースに限定することでセキュリティを強化します。詳細については、この章の「ルーティングエンジンの保護」セクションを参照してください。

注 一部の Junos プラットフォームでは、同時 SSH 接続数に制限があることにも注意してください。そのため、これらの値を変更する前に、該当するプラットフォームの参考資料を確認してください。また、環境にとって妥当な「connection-limit」および「rate-limit」値を調べてください。実際のネットワークについてこれらの値を決定するときは、通常のオペレーションや緊急時の状況を考慮する必要があります。

HTTPS による J-Web のセキュリティ強化

J-Web は、Junos デバイスの設定および監視に使用される、ジュニパーネットワークスの Web ユーザーインタフェースの名称です。HTTPS を有効にすることにより、デバイスへの接続において機密性と完全性を確保することができます。

注 証明書の生成方法については、本書では言及しません。そのため、以下の手順では、信頼された認証局によって署名された X.509 SSL 証明書をすでに入手していることを前提としています。

J-Web のセキュリティ強化方法

1. 信頼された CA（Certificate Authority）によってデジタル署名された有効な X.509 証明書を取得し、Junos デバイスのホームディレクトリにコピーします。

2. 証明書をロードします。

```
[edit]
jweidley@ex3200# edit security certificates

[edit security certificates]
jweidley@ex3200# set local ex3200-ssl-cert load-key-file ?
Possible completions:
  <load-key-file>      File (URL) containing an SSL certificate and
                       private key in PEM format
  ex3200cert.pem       Size:2278, Last changed:May 19 20:39:04

[edit security certificates]
jweidley@ex3200# set local ex3200-ssl-cert load-key-file ex3200cert.pem
```

3. HTTPS を有効にし、この X.509 証明書を使用するように設定します。

```
 [edit security certificates]
jweidley@ex3200# top edit system services web-management

[edit system services web-management]
jweidley@ex3200# set https local-certificate ex3200-ssl-cert
```

4. セキュリティプラクティスとして、不正ユーザーが無認証でアクセスする可能性を低減するために、常にセッションのアイドルタイムアウトを有効にすることをお奨めします。

```
 [edit system services web-management]
jweidley@ex3200# set session idle-timeout 30
```

5. 権限のあるユーザーのみ使用するように、J-Web セッション数を制限します。また、システムリソースが節約でき、DoS 攻撃の可能性も低減されます。

```
 [edit system services web-management]
jweidley@ex3200# set session session-limit 4
```

6.（オプション）OOB 管理インターフェースを使用しない場合、管理ネットワークに接続するインタフェースなど特定インタフェースでのみ J-Web 接続を受け入れるようにすることができます。

```
 [edit system services web-management]
jweidley@ex3200# set https interface ge-0/0/0
```

7. 設定を確認します。

```
[edit system services web-management]
jweidley@ex3200# show
https {
    local-certificate ex3200-ssl-cert;
    interface ge-0/0/0.0;
}
session {
    idle-timeout 30;
    session-limit 4;
}

[edit system services web-management]
jweidley@ex3200# top show security
certificates {
    local {
        ex3200-ssl-cert {
            "-----BEGIN RSA PRIVATE KEY-----\nMIICXAIBAAKBgQDDqlL96hg0393M6r68qqzNFoFRUdubqI+k9j
QMyeOmS1ibT26j\nh6g+Ep
..... [ removed ] .....
vgohYImwYNlmvddX9YrqBDI=\n-----END RSA PRIVATE KEY-----\n-----BEGIN CERTIFICATE-----\nMIID1zCCA0
CgAwIBAgIJAKGSmTVk+487MA0GCSqGSIb3DQEBBQUAMIGkMQswCQYD\nVQQGEw
..... [ removed ] .....
y8sLLs5xMPO3TUHlBxTH97UOuJ\n-----END CERTIFICATE-----\n"; ## SECRET-DATA
        }
    }
}
```

8. これで、J-Web が設定されました。次のステップでは、接続元を信頼されたソースに限定することでセキュリティを強化します。詳細については、この章の「ルーティングエンジンの保護」セクションを参照してください。

ヒント ベストセキュリティプラクティスとして、自己署名された証明書ではなく、信頼された認証局によって署名された有効な SSL 証明書を使用することをお奨めします。自己署名された証明書でも機密性は提供されますが、証明書のルートを検証できず、証明書検証エラーが表示されるため、毎回証明書の警告を無視しなければならなくなります。

ユーザー認証

この他、ネットワークデバイスのセキュリティ強化において重要なポイントとして、ユーザー認証、コマンド権限、およびアクセス許可があります。すべてのユーザーアクセス要求には、何らかの認証が必要になります。ユーザー認証要求は、ローカル、あるいは RADIUS や TACACS+ によってリモートで処理することができます。

比較的大規模なネットワークでは、一貫したパスワードポリシーの適用およびユーザーアカウントの管理を行うために、認証を集中化させることもよくあります。ただし、ネットワークの規模に関わらず、緊急時に備えて、ネットワークデバイスに必ず 1 つ以上のローカルユーザーアカウントを設定する必要があります。

次のセクションでは、カスタムログインクラス、RADIUS、RADIUS アカウンティング、TACACS+、TACACS+ アカウンティング、およびローカルユーザーアカウントを使用してユーザー許可を設定する方法を説明し、パスワード複雑性ポリシーを適用するために必要な機能を紹介します。

ログイン許可

情報セキュリティの原則は「最小権限」です。これは、ユーザー、プロセス、サービスおよびデバイスはその機能やアサインされた役割に見合ったアクセスと操作権限のみ与えられるべきであるという考え方です。

Junos ソフトウェアでは、ユーザー権限はログインクラスで定義されます。Junos デバイスにログインするすべてのユーザーに、ログインクラスを割り当てる必要があります。ログインクラスでは、以下のことを定義できます。

- ユーザーがデバイスにログインしたときのアクセス権限
- ユーザーが実行できる、または実行できないコマンドおよびステートメント
- 時間ベースのアクセス制御、アイドルタイムアウト、ログイン時のシステムアラームの表示など、その他の便利なオプション

Junos ソフトウェアには、以下の 4 つのログインクラスが組み込まれています。

ログインクラス	アクセス許可	説明
operator	clear、network、reset、trace、view	オペレーションモードで、これらのカテゴリで使用可能なすべてのアクションを実行できます。operator は、設定を表示または変更したり、デバイスをシャットダウンまたは再起動したりすることはできません。
read-only	view	オペレーションモードで、view アクセス許可で使用可能なすべてのアクションを実行できます。
super-user	すべて	デバイスに対してすべての操作を実行できます。
unauthorized	なし	デバイスへのログインは可能ですが、ログアウト以外の操作を実行することはできません。

これらの予め用意されたログインクラスが実際の環境に適していない場合も考えられます。幸い、Junos OS では、管理ユーザーが使用できるコマンドをクラスごとに詳細に設定できるため、柔軟なアクセスコントロールが可能です。

さらに詳しくは ログインクラスの設定の詳細については、Junos の技術資料『*Junos OS Basic System Configuration Guide*』（http://www.juniper.net/techpubs/en_US/junos10.4/information-products/pathway-pages/system-basics/user-access.html）を参照してください。

カスタムログインクラスの作成方法

オペレータのアクセスに「最小権限」の考え方を適用する場合は、ファイアウォールを設定する時と同じ手法をとります。すなわち、デフォルトですべて拒否するところから始め、次に組織における各役割の責任範囲を確認し、対応する Junos CLI 階層へのアクセスを許可します。

デバイスへのアクセスを必要とするエンジニアまたはグループの役割について考えてみてください。ログイン要件はおそらくサイトによってそれぞれ異なりますが、このセクションでは、標準的な Tier-1、Tier-2 および Tier-3 エンジニアの例を用いて、各レベルに対して特定の機能を許可および拒否する方法を説明します。この例では各レベルのエンジニアの要件を以下のように想定します。

- Tier-1：基本的なトラブルシューティングのために show コマンドを実行したり、到達可否を確認するためにネットワークツール（ping、traceroute など）を実行できなければなりません。また、設定を確認できなければなりませんが、秘密文字列は見えないようにする必要があります。

- Tier-2：Tier-1 エンジニアが利用できる機能に加え、デバイスのカウンターおよび統計のクリアや、インタフェースおよびルーティング設定変更ができなければなりません。
- Tier-3：運用業務をサポートするためにデバイスに対してあらゆる機能を実行できるだけでなく、詳細なデバッグやコードのアップグレードなど高度なトラブルシューティングを行えなければなりません。

Tier-1

Tier-1 ネットワークオペレータ用に、必要なパーミッションのみを与える新しいログインクラスを作成します。

1. ログインクラス名を定義します。

```
{master:0}[edit]
jweidley@EX4500# edit system login class tier1
```

2. アイドルタイムアウトを、環境に適した値に設定します。この期間が経過すると、ユーザーは自動的にシステムからログオフします。ユーザーには、セッションがタイムアウトになることを通知する警告メッセージが表示されます。

```
{master:0}[edit system login class tier1]
jweidley@EX4500# set idle-timeout 10
```

3. Junos の操作に慣れていないエンジニアには、ログイン時のヒントが役立ちます。また、コマンドに関する役立つ情報を表示することもできます。

```
{master:0}[edit system login class tier1]
jweidley@EX4500# set login-tip
```

4. その時点で発生しているシステムアラームについて確認できるように、アラートを出すことができます。

```
{master:0}[edit system login class tier1]
jweidley@EX4500# set login-alarms
```

5. maintenance パーミッションは、デバイスのシャットダウンや再起動など、保守に関連するタスクを許可します。

```
{master:0}[edit system login class tier1]
jweidley@EX4500# set permissions maintenance
```

6. view パーミッションは、ルーティングテーブル、スパニングツリー、インタフェース統計などの確認に役立つ show コマンドの使用を許可します。

```
{master:0}[edit system login class tier1]
jweidley@EX4500# set permissions view
```

7. network パーミッションは、接続およびルーティングを確認するための ping、traceroute、telnet、および SSH の使用を許可します。

```
{master:0}[edit system login class tier1]
jweidley@EX4500# set permissions network
```

8. view-configuration パーミッションは、コンフィグレーションの表示を許可します。設定全体を表示できますが、暗号化された文字列は見えません。

```
{master:0}[edit system login class tier1]
jweidley@EX4500# set permissions view-configuration
```

9. 一部のパーミッションにより、Tier-1 ユーザーが使用してはならないコマンドも実行可能になります。deny-commands オプションでは、正規表現を使用して、Tier-1 エンジニアが実行してはならないコマンドを明示的に定義できます。そのほとんどはコマンドどおりの意味ですが、ここでいくつか取り上げて説明しておきましょう。

- (start *) は、Unix シェルへのアクセスを取得するために使用できるすべての start コマンドを制限します。
- (set cli idle-timeout) は、ログインクラスのアイドルタイムアウト値を再設定する機能を制限します。

```
{master:0}[edit system login class tier1]
jweidley@EX4500# set deny-commands "(start *)|(set cli idle-timeout)|(request system
software)|(request system zeroize)|(request chassis)"
```

10. 設定を確認します。

```
{master:0}[edit system login class tier1]
jweidley@EX4500# show
idle-timeout 10;
login-alarms;
login-tip;
permissions [ maintenance network view view-configuration ];
deny-commands "(start *)|(set cli idle-timeout)|(request system software)|(request system
zeroize)|(request chassis)";
```

さらに詳しくは 正規表現の詳細および例については、Junos の技術資料『*Junos OS Access Privilege Configuration Guide*』（http://www.juniperpodcast.com/techpubs/en_US/junos10.4/information-products/topic-collections/config-guide-access-privilege/swconfig-access-privilege.pdf）を参照してください。

Tier-2

次に、Tier-2 エンジニア用に、さらに高度な機能を実行できる、別のログインクラスを作成しましょう。

1. ログインクラスの名前を定義します。

```
{master:0}[edit system login]
jweidley@EX4500# edit class tier2
```

2. アイドルタイムアウトを、環境に適した値に設定します。この期間が経過すると、ユーザーは自動的にシステムからログオフします。ユーザーには、セッションがタイムアウトになることを通知する警告メッセージが表示されます。

```
{master:0}[edit system login class tier2]
jweidley@EX4500# set idle-timeout 15
```

3. その時点で発生しているシステムアラームについて確認できるように、アラートを出すことができます。

```
{master:0}[edit system login class tier2]
jweidley@EX4500# set login-alarms
```

4. Tier-2 エンジニアには、少なくとも Tier-1 エンジニアと同じ範囲の実行権限が必要なため、同じパーミッションを設定します。

```
{master:0}[edit system login class tier2]
jweidley@EX4500# set permissions maintenance
```

```
{master:0}[edit system login class tier2]
jweidley@EX4500# set permissions network

{master:0}[edit system login class tier2]
jweidley@EX4500# set permissions view

{master:0}[edit system login class tier2]
jweidley@EX4500# set permissions view-configuration
```

5. clear パーミッションは、カウンターおよび統計情報のクリアを許可します。これは、いくつかのトラブルシューティングシナリオで役立ちます。

```
{master:0}[edit system login class tier2]
jweidley@EX4500# set permissions clear
```

6. configure パーミッションにより、コンフィグレーションモードへ切り替えができるようになりますが、デフォルトでは、実際に設定する権限は与えられません。そのため、Tier-2 エンジニアに、プロビジョニングをサポートするためのインタフェースおよびルーティング関連情報の設定を許可します。

```
{master:0}[edit system login class tier2]
jweidley@EX4500# set permissions configure

{master:0}[edit system login class tier2]
jweidley@EX4500# set permissions interface-control

{master:0}[edit system login class tier2]
jweidley@EX4500# set permissions routing-control
```

7. rollback パーミッションは、エラーが発生した場合に設定の変更を元に戻すことを許可します。

```
{master:0}[edit system login class tier2]
jweidley@EX4500# set permissions rollback
```

8. deny-commands オプションを使用して、特定のコマンドを制限します。

```
{master:0}[edit system login class tier2]
jweidley@EX4500# set deny-commands "(start *)|(set cli idle-timeout)|(request system
software)|(request system zeroize)"
```

9. deny-configuration オプションを使用して、パーミッションが与えられた中の特定の階層について、設定変更を制限します。

```
{master:0}[edit system login class tier2]
jweidley@EX4500# set deny-configuration "(groups)"
```

10. それでは、設定を確認してみましょう。

```
{master:0}[edit system login class tier2]
jweidley@EX4500# show
idle-timeout 15;
login-alarms;
permissions [ clear configure interface-control maintenance network rollback routing-control
view view-configuration ];
deny-commands "(start *)|(set cli idle-timeout)|(request system software)|(request system
zeroize)";
deny-configuration "(groups)";
```

Tier-3

Tier-3 エンジニアには、予め定義されている super-user ログインクラスをそのまま使用することもできますが、ここでは、アイドルタイムアウトとその他の項目をカスタマイズします。

1. ログインクラス名を定義します。

```
{master:0}[edit system login]
lab@EX4500# edit class tier3
```

2. アイドルタイムアウトを、環境に適した値に設定します。この期間が経過すると、ユーザーは自動的にシステムからログオフします。ユーザーには、セッションがタイムアウトになることを通知する警告メッセージが表示されます。

```
{master:0}[edit system login class tier3]
lab@EX4500# set idle-timeout 20
```

3. その時点で発生しているシステムアラームについて確認できるように、アラートを出すことができます。

```
{master:0}[edit system login class tier3]
jweidley@EX4500# set login-alarms
```

4. all キーワードを使用して、すべての項目についてパーミッションを与えます。

```
{master:0}[edit system login class tier3]
lab@EX4500# set permissions all
```

5. それでは、設定を確認してみましょう。

```
{master:0}[edit system login class tier3]
lab@EX4500# show
idle-timeout 20;
login-alarms;
permissions all;
```

ログインクラスの設定は、それを使用する組織によってそれぞれ異なります。Junos OS には、ニーズに合わせてポリシーを設計できるオプションが多数用意されています。実際のオペレーションに合致するまで、何パターンか試す必要があるかも知れません。

ヒント [system login class] では、アクセス可能な時刻や曜日など、ログインポリシーの強化に役立つその他のオプションを利用できます。これらのオプションは、組織のセキュリティポリシーに応じて、必要であれば使用してください。

さらに詳しくは さまざまなログインクラスのパーミッションについては、http://www.juniper.net/techpubs/software/junos-security/junos-security10.4/junos-security-admin-guide/index.html?user-auth-ov-section.html を参照してください。

さらに詳しくは ログインクラスの例については、http://www.juniper.net/books で紹介されている『*Junos Cookbook*』（アビバ・ギャレット著、O’Reilly Media 発行、2006 年）を参照してください。

RADIUS と RADIUS アカウンティング

RADIUS（Remote Authentication Dial-in User Service）は、ネットワークデバイスの認証・認可・アカウンティング（AAA）を集中的に行う業界標準のプロトコルです。

RADIUS プロトコルでは、ネットワーク上でプレーンテキストのパスワードがやり取りされることはありません。クライアントとサーバー間で取り決められた共有の秘密パスワードとハッシュアルゴリズムを使用してパスワードのセキュリティを強化しています。また、セキュリティは、OOB 管理ネットワークを使用してユーザーデータと管理データを分離することによりさらに強化できます（RADIUS メッセージを見ることができなければ、悪意のあるユーザーがその情報をのぞき見たり、クラッキングしたり、なりすまし攻撃をすることはできません）。

注 Junos OS の RADIUS クライアント機能および RADIUS サーバーソフトウェアパッケージでは、ある程度柔軟な設定ができますが、これについては本書では触れません。このセクションでは、ネットワークデバイスの観点からセキュアな通信および適切なアカウンティングの設定について説明します。

さらに詳しくは RADIUS の設定およびベンダー固有の属性（VSA）の詳細については、Junos の技術資料『*Junos OS Basic System Configuration Guide*』（http://www.juniper.net/techpubs/en_US/junos/information-products/topic-collections/config-guide-system-basics/config-guide-system-basics.pdf）を参照してください。

RADIUS 認証の設定方法

1. 最初に、RADIUS サーバーの IP アドレスを定義します。

```
[edit]
jweidley@ex3200# edit system radius-server 192.168.3.20
```

2. 共有秘密パスワードを設定します。これは、パスワード複雑性ポリシーに適合した、容易に推測できない強力なパスワードにする必要があります。

```
[edit system radius-server 192.168.3.20]
jweidley@ex3200# set secret $2rK-nh%Aj4WQ=}
```

3. RADIUS サーバーがリクエストをリスニングするポートを定義します。UDP 1812 がデフォルトポートですが、これを明示的に設定することにより、分かりやすくなります。

```
 [edit system radius-server 192.168.3.20]
jweidley@ex3200# set port 1812
```

4.（オプション）`set system default-address-selection` が設定されていない場合、特定のアドレスから RADIUS リクエストが送出されるようにするために、送信元アドレスを設定します。通常は、lo0 インタフェースの IP アドレスを使用します。

```
 [edit system radius-server 192.168.3.20]
jweidley@ex3200# set source-address 192.168.70.1
```

5. 設定を確認します。

```
 [edit system radius-server 192.168.3.20]
jweidley@ex3200# show
port 1812;
secret "$9$oIJjH.P5F69mPRhylMWjHkqQF"; ## SECRET-DATA
source-address 192.168.70.1;
```

Junos における RADIUS の実装では、アカウントが期限切れになった場合、リセットされた場合、またはアカウントに次回ログイン時にパスワードを変更するよう設定されている場合、パスワード変更がサポートされています。これを行うには、MS-CHAP（Microsoft version of the Challenge Handshake Authentication Protocol）を設定します。

```
[edit]
jweidley@ex3200# edit system radius-options

[edit system radius-options]
jweidley@ex3200# set password-protocol mschap-v2

[edit system radius-options]
jweidley@ex3200# show
password-protocol mschap-v2;
```

注 分かりやすくするために、この例では、1 台の RADIUS サーバーの設定のみ示していますが、実際の環境では耐障害性を高めるために、複数の RADIUS サーバーを別々のサブネットに設置することをお奨めします。

RADIUS アカウンティングの設定方法

1. アカウンティングメッセージを送出するイベントを設定します。この設定例では、完全な監査を行えるように、すべてのオプションを設定します。

```
[edit]
jweidley@ex3200# edit system accounting

[edit system accounting]
jweidley@ex3200# set events login

[edit system accounting]
jweidley@ex3200# set events change-log

[edit system accounting]
jweidley@ex3200# set events interactive-commands
```

2. RADIUS サーバーの IP アドレスを設定し、アカウンティングに使うポートを設定します（UDP 1813 がデフォルトの RADIUS アカウンティングポートですが、これを明示的に設定することにより、分かりやすくなります）。

```
 [edit system accounting]
jweidley@ex3200# edit destination radius server 192.168.3.20

[edit system accounting destination radius server 192.168.3.20]
jweidley@ex3200# set accounting-port 1813
```

3. 共有秘密パスワードを設定します。これは、パスワード複雑性ポリシーに適合した、容易に推測できない強力なパスワードにする必要があります。

```
 [edit system accounting destination radius server 192.168.3.20]
jweidley@ex3200# set secret M1zoVg2NRa8:r#r
```

4.（オプション）set system default-address-selection が設定されていない場合、特定のアドレスから RADIUS リクエストが送出されるようにするために、送信元アドレスを設定します。通常は、lo0 インタフェースの IP アドレスを使用します。

```
 [edit system accounting destination radius server 192.168.3.20]
jweidley@ex3200# set source-address 192.168.70.1
```

5. 設定を確認します。

```
[edit system accounting destination radius server 192.168.3.20]
jweidley@ex3200# show
accounting-port 1813;
secret "$9$cxFyvWX7-w24x7k.fT3nvW8LVw"; ## SECRET-DATA
source-address 192.168.70.1;
```

注 分かりやすくするために、この例では、1台の RADIUS アカウンティングサーバーの設定のみ示していますが、実際の環境では耐障害性を高めるために、複数の RADIUS サーバーを別々のサブネットに設置することをお奨めします。

TACACS+ と TACACS+ アカウンティング

TACACS+（Terminal Access Controller Access-Control System Plus）は、従来の TACACS 認証ソフトウェアの最新バージョンです。TACACS+ は、認証、権限付与、およびアカウンティング（AAA）のためのプロトコルで、ネットワークデバイスへのアクセスを制御します。

注 Junos OS の TACACS+ クライアント機能および TACACS+ サーバーソフトウェアパッケージでは、ある程度柔軟な設定ができますが、これについては本書では触れません。このセクションでは、ネットワークデバイスの観点からセキュアな通信および適切なアカウンティングの設定について説明します。

さらに詳しくは TACACS+ 設定およびベンダー固有の属性（VSA）の詳細については、Junos の技術資料『*Junos OS Basic System Configuration Guide*』（http://www.juniper.net/techpubs/en_US/junos10.4/information-products/pathway-pages/system-basics/user-access.html）を参照してください。

TACACS+ 認証の設定方法

1. TACACS+ サーバーの IP アドレスを定義します。

```
[edit]
jweidley@ex8208# edit system tacplus-server 192.168.3.40
```

2. 共有秘密パスワードを設定します。これは、パスワード複雑性ポリシーに適合した、容易に推測できない強力なパスワードにする必要があります。

```
[edit system tacplus-server 192.168.3.40]
jweidley@ex8208# set secret $2rK-nh%Aj4WQ=}
```

3. TACACS+ ポートを TCP 49 に設定します。これはデフォルトポートですが、これを明示的に設定することにより、分かりやすくなります。

```
[edit system tacplus-server 192.168.3.40]
jweidley@ex8208# set port 49
```

4.（オプション）set system default-address-selection が設定されていない場合、特定のアドレスから TACACS+ リクエストが送出されるようにするために、送信元アドレスを設定します。通常は、lo0 インタフェースの IP アドレスを使用します。

```
[edit system tacplus-server 192.168.3.40]
jweidley@ex8208# set source-address 192.168.70.1
```

5. 設定を確認します。

```
[edit system tacplus-server 192.168.3.40]
jweidley@ex8208# show
port 49;
secret "$9$RywhlKWLxdwY8LjH.PQzlKvMNd"; ## SECRET-DATA
source-address 192.168.70.1;
```

注 分かりやすくするために、この例では、1 台の TACACS+ サーバーの設定のみ示していますが、実際の環境では耐障害性を高めるために、複数の TACACS+ サーバーを別々のサブネットに設置することをお奨めします。

TACACS+ アカウンティングの設定方法

1. アカウンティングによってトラックするイベントを設定します。この設定例では、完全な監査を行えるように、すべてのオプションを設定しましょう。

```
[edit system tacplus-server 192.168.3.40]
jweidley@ex8208# top edit system accounting

[edit system accounting]
jweidley@ex8208# set events login

[edit system accounting]
jweidley@ex8208# set events change-log

[edit system accounting]
jweidley@ex8208# set events interactive-commands
```

2. TACACS+ アカウンティングサーバーの IP アドレスを定義します。

```
[edit system accounting]
jweidley@ex8208# edit destination tacplus server 192.168.3.40
```

3. 共有秘密パスワードを設定します。これは、パスワード複雑性ポリシーに適合した、容易に推測できない強力なパスワードにする必要があります。

```
[edit system accounting destination tacplus server 192.168.3.40]
jweidley@ex8208# set secret M1zoVg2NRa8:r#r
```

4. TACACS+ アカウンティングポートを TCP 49 に設定します。これはデフォルトポートですが、これを明示的に設定することにより、分かりやすくなります。

```
[edit system accounting destination tacplus server 192.168.3.40]
jweidley@ex8208# set port 49
```

5. （オプション）set system default-address-selection が設定されていない場合、特定のアドレスから TACACS+ 要求が送出されるようにするために、送信元アドレスを設定します。通常は、lo0 インタフェースの IP アドレスを使用します。

```
[edit system accounting destination tacplus server 192.168.3.40]
jweidley@ex8208# set source-address 192.168.70.1
```

6. 設定を確認します。

```
[edit system accounting destination tacplus server 192.168.3.40]
jweidley@ex8208# show
port 49;
secret "$9$ZsUk.fTz6Ct5TcyevLXk.mP36"; ## SECRET-DATA
source-address 192.168.70.1;
```

注 分かりやすくするために、この例では、1台の TACACS+ アカウンティングサーバーの設定のみ示していますが、実際の環境では耐障害性を高めるために、複数の TACACS+ サーバーを別々のサブネットに設置することをお奨めします。

パスワード複雑性

集中認証が常に可能なわけではないため、エンジニアは一定の強度のパスワードを使用する必要があります。単純なパスワードではネットワークデバイスがセキュリティリスクにさらされる可能性があります。

パスワードの強化方法

1. 必要最小限のパスワード文字数を 6 ～ 20 文字の間で設定します。(以下の例では 15 文字に設定しています。)

```
[edit]
jweidley@ex4200# edit system login password

[edit system login password]
jweidley@ex4200# set minimum-length 15
```

2. change-type コマンドで character-sets を定義します。これにより、Junos は、使用された文字セット（大文字、小文字、数字、および特殊文字）の種類をカウントします。

```
[edit system login]
jweidley@ex4200# set change-type character-sets
```

3. 文字列の中で、文字の種類を変えさせる場合、その最低変更回数を設定します。

```
[edit system login password]
jweidley@ex4200# set minimum-changes 4
```

4. 最も強度が高く、最もセキュアなパスワード保存形式である SHA-1 を設定します。

```
[edit system login password]
jweidley@ex4200# set format sha1
```

5. 設定を確認します。

```
[edit system login password]
jweidley@ex4200# show
minimum-length 15;
change-type character-sets;
minimum-changes 4;
format sha1;
```

さらに詳しくは 環境に最適な設定を判断するための change-types および set-transitions の説明については、Junos の技術資料『*Junos OS Basic System Configuration Guide*』（http://www.juniper.net/techpubs/en_US/junos10.4/information-products/pathway-pages/system-basics/user-access.html）を参照してください。

注意 上記のパスワード複雑性オプションは、コミット後にのみユーザーアカウントに適用されます。複雑性オプションの設定前に作成されたアカウントは、これらの新しいパスワード要件の影響を受けません。

ローカルログインアカウントとテンプレート

多くのネットワークOSと同様に、Junos OSでは、ローカルユーザーアカウントを作成することができます。Junosデバイスのユーザーアカウントには、rootユーザーと非rootユーザーの2種類があります。第3章で説明したとおり、rootアカウントは唯一のデフォルトアカウントで、システムで最も強力なアカウントです。このセクションでは、ユーザーアカウントについて取り上げます。

Junosでは、テンプレートを使用して、RADIUS/TACACS+で認証を受けるユーザーにパーミッションを設定することもできます。各テンプレートでは、そのテンプレートを使用するユーザーグループに適した、異なるパーミッションを定義できます。これらのテンプレートは、ルーターのローカルで定義し、TACACS+およびRADIUS認証サーバーによって参照されます。

さらに詳しくは ローカルユーザーアカウントおよびテンプレートの詳細については、Junosの技術資料『*Junos OS Basic System Configuration Guide*』（http://www.juniper.net/techpubs/en_US/junos/information-products/topic-collections/config-guide-system-basics/config-guide-system-basics.pdf）を参照してください。

ローカルユーザーアカウントの作成方法

集中認証を使用する場合も、常に、システムに少なくとも1つはローカルユーザーアカウントを設定することをお奨めします。これは、RADIUS/TACACS+がダウンした場合、ローカルアカウントが、デバイスにログインするための代替手段になるからです。

1. ローカルユーザー名を定義します。このアカウントの目的を記述するために、`full-name`オプションを使用します。

```
[edit system login]
admin@j6350# set user emergency full-name "Emergency Only Local Account"
```

2. デバイスでこのユーザーに与えるパーミッションを割り当てます。これを行うには、デフォルトまたはカスタム`login class`を割り当てます。

```
[edit system login]
admin@j6350# set user emergency class tier3
```

3. オプションで、ファイルの転送時にファイル所有権の問題が生じないようにするために、Junosデバイスおよび Unixシステムで共通のユーザーID（uid）を設定します（ユーザーIDを指定しない場合、Junosにより自動的に割り当てられます）。

```
[edit system login]
admin@j6350# set user emergency uid 2010
```

4. 最後に、アカウントにパスワードを割り当てます。

```
[edit system login]
admin@j6350# set user emergency authentication plain-text-password
New password:
Retype new password:
```

ヒント `full-name`オプションでは、電話番号やエンジニアの所属部署など、そのユーザーアカウントの連絡先情報を指定することもできます。

ユーザーテンプレートを作成するための設定は、パスワードの設定を除き、ログインアカウントを設定する場合とほとんど同じです。パスワードチェックは、外部認証サーバー（RADIUS/TACACS+）によって処理されるため、パスワードは必要ありません。

ログインテンプレートの作成方法

前の章の「ログイン許可」セクションで設定したログインクラスによってパーミッションが割り当てられるエンジニア用のログインテンプレートを作成します。

1. ローカルユーザー名を定義します。このとき、full-name オプションを使用して、アカウントの目的を記述することができます。

```
[edit system login]
admin@j6350# set user tier1 full-name "Login template for Tier1 Users"
```

2. デバイスでこのユーザーに与えるパーミッションレベルを割り当てます。これを行うには、適切なデフォルトまたはカスタムログインクラスを割り当てます。

```
[edit system login]
admin@j6350# set user tier1 class tier1
```

3. オプションで、ファイルの転送時にファイル所有権の問題が生じないようにするために、Junos デバイスおよび Unix システム共通のユーザー ID（uid）を設定します（ユーザー ID を指定しない場合、Junos により自動的に割り当てられます）。

```
[edit system login]
admin@j6350# set user tier1 uid 2001
```

4. tier2 および tier3 テンプレートを追加して、設定は完了です。

```
[edit system login]
admin@j6350# set user tier2 full-name "Login template for Tier2 Users"

[edit system login]
admin@j6350# set user tier2 class tier2

[edit system login]
admin@j6350# set user tier2 uid 2002

[edit system login]
admin@j6350# set user tier3 full-name "Login template for Tier3 Users"

[edit system login]
admin@j6350# set user tier3 class tier3

[edit system login]
admin@j6350# set user tier3 uid 2003
```

5. 設定を確認します。

```
[edit system login]
user tier1 {
    full-name "Login template for Tier1 Users";
    uid 2001;
    class tier1;
}
user tier2 {
    full-name "Login template for Tier2 Users";
    uid 2002;
    class tier2;
}
user tier3 {
    full-name "Login template for Tier3 Users";
    uid 2003;
    class tier3;
}
```

ヒント セキュリティエンジニアの立場では、グループアカウントに対しては否定的です。これは、監査の観点からすると、誰がログインしたかの証跡が無いことになるからです。集中認証を使用する場合、ローカルログインテンプレートを使ったとしても、各ユーザーのログインおよび実行されたコマンドの情報についてきめ細かくアカウンティングできます。

実践：アカウンティング情報の確認

RADIUS 認証が設定され、ユーザーがユーザーテンプレートにマッピングされています。それでは、パーミッション、適用されているユーザーテンプレート、そしてユーザーのアカウンティング情報を確認する方法を説明しましょう。ユーザー認証情報は、`show cli authorization` コマンドにより表示できます。

```
jweidley@mx960> show cli authorization
Current user:/tier3/ login:/jweidley/ class /tier3/
Permissions:
    admin       -- Can view user accounts
    admin-control-- Can modify user accounts
    clear       -- Can clear learned network information
    configure   -- Can enter configuration mode
    control     -- Can modify any configuration
```

出力の最初の行にある `current user` は、ログインテンプレート名（tier3）です。`login` フィールドは、デバイスに対して認証されるユーザー名（jweidley）で、`class` は、ログインテンプレートによって割り当てられたログインクラス（tier3）です。

interactive-commands ログファイルを調べると、Junos により、完全なアカウンティング情報を維持するために、すべてのログに、ログインテンプレート名ではなくユーザーのログイン名でタグ付けされていることが確認できます。

```
Jun 15 14:08:54.439 2011  mx960-1 mgd[88155]:%INTERACT-6-UI_CMDLINE_READ_LINE:User /jweidley/,
command /show configuration /
Jun 15 14:09:18.783 2011  mx960-1 mgd[88155]:%INTERACT-6-UI_CMDLINE_READ_LINE:User /jweidley/,
command /show log messages /
Jun 15 14:09:36.352 2011  mx960-1 mgd[88155]:%INTERACT-6-UI_CMDLINE_READ_LINE:User /jweidley/,
command /show log security /
```

ログイン試行回数の制限

パスワード推測攻撃は、ユーザーのパスワード入力を繰り返し試行することにより、デバイスに不正アクセスしようとするものです。統計的に、この攻撃の成功率は、ログイン試行回数にしきい値を設定することによって低減できます。

パスワード推測攻撃を阻止する方法

ログインセキュリティに関する Junos のデフォルト設定により、パスワード推測攻撃からある程度保護することはできますが、それがすべての環境に適しているとは限りません。ここでは、不正なログインアクセス試行に対する保護を強化するための 4 つのオプションについて説明します。

1. 接続が切断されるまでに、ユーザーが連続してログインのためのパスワードを入力できる最大試行回数を設定します。この値の範囲は 1 ～ 10 で、デフォルト値は 10 です。

```
{master:0}[edit system login retry-options]
jweidley@EX4500# set tries-before-disconnect 3
```

2. ユーザーがログインに失敗した際、次のログインを試行できるようになるまでの待ち時間を作ることができますが、何回失敗した後にこの待ち時間を発動させるかを設定します。この値の範囲は 1 ～ 3 で、デフォルト値は 2 です。

```
{master:0}[edit system login retry-options]
jweidley@EX4500# set backoff-threshold 1
```

3. ログイン失敗後、次のログインを試行できるようになるまでの待ち時間を秒単位で定義します。backoff-threshold オプションで指定した値を超えると、以降、ログインに失敗するたびにこの値の秒数分、待ち時間が長くなっていきます。この値の範囲は 5 ～ 10 で、デフォルト値は 5 です。

```
{master:0}[edit system login retry-options]
jweidley@EX4500# set backoff-factor 6
```

4. ユーザーがログイン時にパスワードを入力しようとしている間、接続を維持しておく最小時間を秒単位で設定します。この値の範囲は 20 ～ 60、デフォルトは 20 です。

```
{master:0}[edit system login retry-options]
jweidley@EX4500# set minimum-time 30
```

5. それでは、設定を確認してみましょう。

```
{master:0}[edit system login retry-options]
jweidley@EX4500# show
tries-before-disconnect 3;
backoff-threshold 1;
backoff-factor 6;
minimum-time 30;
```

認証順序

ローカルパスワードデータベース以外の認証方法を有効にするには、authentication-order 設定が必要です。認証順序を設定するときは、いくつかの概念について考慮する必要があります。authentication-order コマンドでローカルパスワードデータベースが指定されているかどうかに関わらず、ローカルパスワードデータベースは常に参照先に含まれます。ここで重要になるのは、ローカルパスワードデータベースがいつ使用されるのかを理解することです。

ログイン試行が行われるたびに、Junos OS は、パスワードが受け入れられるまで、設定されている認証方法を設定されている順序で試そうとします。ユーザー名とパスワードが合致すると、ログインが成功し、他の認証方法は使用されません。ある認証方法で応答が得られなかった場合、またはユーザー名またはパスワードが不正なため拒否の応答が返された場合、次の認証方法が試されます。

設定されているどの認証方法でもログイン資格情報が受け入れられなかった場合や拒否の応答が返された場合、ログインは失敗します。設定されているどの認証方法からも応答が返されなかった場合、Junos ソフトウェアは、最後の手段としてローカルパスワード認証を使用します。

以下の例について考えてみましょう。

```
[edit system]
jweidley@ex4200# show authentication-order
authentication-order [ radius password ];
```

ユーザーが認証を試行すると、まず RADIUS サーバーへの問い合わせが行われます。パスワードが正しく入力されなかったり、アカウントが設定されていないなどの理由で、RADIUS サーバーが拒否の応答を返すと、次にローカルパスワードデータベースへの問い合わせが行われます。

つまり、RADIUS サーバーが使用可能なときでも、RADIUS にないローカルアカウントが設定されていれば、ユーザーはそのアカウントでログインできるということです。

ユーザー認証に必ず RADIUS を使用し、RADIUS サーバーにアクセスできない場合にのみローカルパスワードデータベースへの問い合わせを行う場合は、以下の設定をしてください。

```
[edit system]
jweidley@ex4200# show authentication-order
authentication-order radius;
```

この例の設定で、集中認証によるセキュリティ強化というメリットはそのままにサーバーが使用できなくなるという不測の事態にも対応できるため、多くの状況に適しています。

さらに詳しくは Junos における認証順序の詳細については、http://www.juniper.net/books で紹介されている『*Junos Enterprise Routing, 2nd Edition*』（サウスウィック、マーシュキー、およびレイノルド著、O'Reilly Media 発行、2011 年）を参照してください。

ルーティングプロトコルとルート認証

ルーティングプロトコルのセキュリティ強化には多くの側面がありますが、残念ながら、そのほとんどはこのコンパクトにまとめられた This Week で取り上げることはできません。このセクションでは、信頼された隣接機器とのルーティング更新における認証のみ説明します。

どのネットワークにおいても、ネットワーク全体を正常に運用するためには、安定したルーティングが非常に重要になります。セキュリティプラクティスとして、すべてのルーティングプロトコルトラフィックを認証することにより、信頼されたルーターのみがルーティング情報を交換できるようにすることをお奨めします。

このような環境で脅威となるのは、不正なルーターが、網内のルーターに偽のルーティングアドバタイズメントを送り付け、トラフィックフローを変えたり混乱させたりする可能性があることです。悪意のあるユーザーや組織は、トラフィックを分析したり、DoS（Denial of Service）攻撃を仕掛けるために、トラフィックのルートを変更させることがあります。

このようなリスクを確実に防ぐためには、ルーティングドメイン全体に渡ってすべてのピアルーターとの間にルート認証を設定する必要があります。Junos では、認証キーはすべて暗号化された形式で保存されるため、エンジニアは、実際のパスワードを明かすことなく、暗号化された文字列を共有することができます。

注意 ステートフルファイアウォールを通してルーティングプロトコルを実行している状況でルート認証を有効にする場合は、ファイアウォールベンダーのマニュアルで、TCP シーケンス番号のランダム化について確認してください。これは重要なことです。ファイアウォールによってシーケンス番号がランダム化される場合、異なる暗号化チェックサム値が生成され、隣接関係を確立できなくなります。

ベストプラクティス ベストプラクティスとして、ファイアウォールフィルタによって、ルーティングプロトコルの更新を信頼されたソースに制限することをお奨めします。詳細については、「ルーティングエンジンの保護」セクションを参照してください。

注 多くのルーティングプロトコルでは、何らかの認証がサポートされています。このセクションでは、最も一般的な IGP および EGP プロトコルと、2 つの MPLS シグナリングプロトコルの設定例を示します。

RIP 認証

ルート認証を実装するには、RIP バージョン 2（RIPv2）を使用する必要があります。RIPv2 では、シンプルおよび MD5 の 2 つのタイプのルート認証手法がサポートされます。シンプルルート認証では、最小限のセキュリティが提供されますが、プロトコル更新パケットをスニッフィングすることにより「秘密」キーが復元される可能性があるため、当然ながらルート認証の効果は低くなります。そのため、認証タイプとして MD5 を設定するほうがよいでしょう。

MD5 は、広く利用されている暗号化ハッシュアルゴリズムで、128 ビットのハッシュ値を生成します。送信側ルーターは、隣接機器に送信するすべての RIP パケットに、設定済みの MD5 ハッシュ値を挿入します。受信側ルーターは RIP パケットを受信すると、パケットの内容を処理する前に、このチェックサム値を確認します。

すべての RIP グループに対して認証を有効にするか、特定の RIP グループに対してのみ有効にするのか考慮する必要があります。ここでは、その両方の方法で設定しましょう。

すべてのグループに対して RIP ルート認証を有効にする方法

この例では、すべての RIP グループに対してルート認証を設定します。直接管理しているデバイスとのみ通信を行う場合は、認証をグローバルに有効にすることをお奨めします。この場合、キーを一度指定すれば済むため、設定が少なくなります。

1. 以下のシンプルな RIP 設定から開始します。

```
[edit protocols rip]
jweidley@mx80# show
group eng-group {
    export advertise-static;
    neighbor ge-0/0/1.0;
}
```

2. 認証タイプを MD5 に設定します。

```
[edit protocols rip]
jweidley@mx80# set authentication-type md5
```

3. 認証キーを設定します。組織のパスワード複雑性ポリシーに適合した、容易に推測できないキーを使用することをお奨めします。

```
[edit protocols rip]
jweidley@mx80# set authentication-key D5vw~\H,[bIOaG4
```

4. それでは、設定を確認してみましょう。

```
[edit protocols rip]
jweidley@mx80# show
authentication-type md5;
authentication-key "$9$XVy-VY4aUH.PaJT3n/puO1RhK8"; ## SECRET-DATA
group eng-group {
    export advertise-static;
    neighbor ge-0/0/1.0;
}
```

個々のグループに対して RIP ルート認証を有効にする方法

認証タイプとキーは、グループレベルで設定することもできます。この場合、組織や部門ごとに異なる認証キーを使用することができます。

1. 以下の単純な RIP 設定から開始します。

```
[edit protocols rip]
jweidley@mx80# show
group eng-group {
    export advertise-static;
    neighbor ge-0/0/1.0;
}
```

2. グループレベルで、認証タイプを MD5 に設定します。

```
[edit protocols rip]
jweidley@mx80# edit group eng-group

[edit protocols rip group eng-group]
jweidley@mx80# set neighbor ge-0/0/1.0 authentication-type md5
```

3. 認証キーを設定します。組織のパスワード複雑性ポリシーに適合した、容易に推測できないキーを使用することをお奨めします。

```
[edit protocols rip group eng-group]
jweidley@mx80# set neighbor ge-0/0/1.0 authentication-key D5vw~\H,[bI0aG4
```

4. 設定を確認します。

```
[edit protocols rip group eng-group]
jweidley@mx80# up

[edit protocols rip]
jweidley@mx80# show
group eng-group {
    export advertise-static;
    neighbor ge-0/0/1.0 {
        authentication-type md5;
        authentication-key "$9$sv4aUikPQ36kqCu0BhcylKMNb"; ## SECRET-DATA
    }
}
```

さらに詳しくは RIP の詳細については、http://www.juniper.net/books で紹介されている『*Junos Cookbook*』（アビバ・ギャレット著、O' Reilly Media 発行、2006 年）を参照してください。

OSPF ルート認証

RIP と同様に、OSPF でも、シンプルおよび MD5 ルート認証タイプがサポートされます。シンプルルート認証では、最小限のセキュリティが提供されますが、プロトコル更新パケットをスニッフィングすることにより「秘密」キーが復元される可能性があるため、RIP の場合と同様にルート認証の効果は低くなります。認証タイプとして MD5 を設定するほうがよいでしょう。

MD5 は、広く利用されている暗号化ハッシュアルゴリズムで、128 ビットのハッシュ値を生成します。送信側ルーターは、隣接機器に送信するすべての OSPF パケットに、設定済みの MD5 ハッシュ値を挿入します。受信側ルーターは OSPF パケットを受信すると、パケットの内容を処理する前に、このチェックサム値を確認します。

OSPF 認証を有効にする方法

1. 基本的な OSPF 設定から開始します。

```
[edit protocols ospf]
jweidley@mx240# show
export advertise-static;
area 0.0.0.0 {
    interface ge-0/0/1.0;
}
```

2. 認証タイプを MD5 に設定します。0 ～ 255 の範囲のキー ID を選択します。ここでは、1 を使用します。次に、キー値、すなわちパスワードを設定します。組織のパスワード複雑性ポリシーに適合した、容易に推測できないキーを使用することをお奨めします。

```
[edit protocols ospf]
jweidley@mx240# edit area 0.0.0.0

[edit protocols ospf area 0.0.0.0]
jweidley@mx240# set interface ge-0/0/1.0 authentication md5 1 key D5vw~\H,[bIOaG4
```

3. 設定を確認します。

```
[edit protocols ospf]
jweidley@mx240# show
export advertise-static;
area 0.0.0.0 {
    interface ge-0/0/1.0 {
        authentication {
            md5 1 key "$9$N4bs4JGi.fTGUF"; ## SECRET-DATA
        }
    }
}
```

自動キーロールオーバーを使用した OSPF 認証を有効にする方法

セキュリティプラクティスとして、静的に設定されたパスワードは定期的に変更する方がよいでしょう。これには、ルート認証キーも含まれます。大規模なネットワークでは、このタスクは大変な作業になり、場合によっては管理できなくなる可能性があります。

このセクションでは、start-time オプションを設定します。このオプションにより、特定の日時から自動的に異なるキーに変えることができます。そのためにも、信頼されたクロックソースを用意すべきなのです。

1. 前の例を基に、2 つ目の認証キーを設定し、その認証キーを使用し始める日時を設定します。

```
[edit protocols ospf area 0.0.0.0]
jweidley@mx240# set interface ge-0/0/1.0 authentication md5 2 key 4}QYWwR+^@V7^uf start-time
2011-03-31.16:32
```

2. それでは、設定を確認してみましょう。

```
[edit protocols ospf area 0.0.0.0]
jweidley@mx240# show
interface ge-0/0/1.0 {
    authentication {
        md5 1 key "$9$N4bs4JGi.fTGUF"; ## SECRET-DATA
        md5 2 key "$9$v4DM7Vg4ZjkPJG" start-time "2011-3-31.16:32:00 -0700"; ## SECRET-DATA
    }
}
```

注 キーローテーションは日時に基づくため、安定した、信頼できる NTP ソースが不可欠です。

さらに詳しくは OSPF の詳細については、http://www.juniper.net/books で紹介されている『*Junos Cookbook*』（アビバ・ギャレット著、O’ Reilly Media 発行、2006 年）を参照してください。

OSPFv3 ルート認証

OSPFv3 は、IPv6 ネットワークでのルーティング情報交換をサポートする OSPF バージョンです。OSPFv3 では、設計上、プロトコル認証が削除されています。これは、ルーティングプロトコルと IPv6 スタックの両方に認証メカニズムを実装する必要はないためです。そのため、OSPFv3 ルート認証では、IPSEC を使用します。

OSPFv3 ルート認証の設定方法

この例では、OSPFv3 と、セキュリティ強化のための IPSEC セキュリティアソシエーション（SA）を設定します。Junos では、複数のハッシュおよび暗号化アルゴリズムがサポートされます。この例では MD5 を使用しますが、実際に実装するときは、ネットワークに最適なアルゴリズムを選択してください。

1. 実際に動作するシンプルな OSPFv3 設定から開始します。

```
[edit protocols ospf3]
jweidley@MX480# show
area 0.0.0.0 {
    interface lo0.0 {
        passive;
    }
    interface ge-0/0/1;
}
```

2. IPSEC セキュリティアソシエーションを設定します。

```
[edit]
jweidley@MX480# edit security ipsec security-association ospf3-auth-core

[edit security ipsec security-association ospf3-auth-core]
jweidley@MX480# set description ospf3-neighbor-auth-core

[edit security ipsec security-association ospf3-auth-core]
jweidley@MX480# set mode transport

[edit security ipsec security-association ospf3-auth-core]
jweidley@MX480# set manual direction bidirectional protocol ah

[edit security ipsec security-association ospf3-auth-core]
jweidley@MX480# set manual direction bidirectional spi 256
```

3. 実際の環境で使用する認証アルゴリズムを設定します。ここでは MD5 を使用します。

```
[edit security ipsec security-association ospf3-auth-core]
jweidley@MX480# set manual direction bidirectional authentication algorithm hmac-md5-96
```

4. 次に、キー値、すなわちパスワードを設定します。組織のパスワード複雑性ポリシーに適合した、容易に推測できないキーを使用することをお奨めします。

```
 [edit security ipsec security-association ospf3-auth-core]
jweidley@MX480# set manual direction bidirectional authentication key ascii-text D5vw~\H,[bIOaG4j
```

5. 認証に IPSEC SA を使用するよう OSPFv3 を設定します。

```
[edit security ipsec security-association ospf3-auth-core]
jweidley@MX480# top edit protocols ospf3 area 0.0.0.0

[edit protocols ospf3 area 0.0.0.0]
jweidley@MX480# set interface ge-0/0/1 ipsec-sa ospf3-auth-core
```

6. それでは、設定を確認してみましょう。

```
[edit protocols ospf3 area 0.0.0.0]
jweidley@MX480# up

[edit protocols ospf3]
jweidley@MX480# show
area 0.0.0.0 {
    interface lo0.0 {
        passive;
    }
```

```
    interface ge-0/0/1 {
        ipsec-sa ospf3-auth-core;
    }
}

[edit protocols ospf3]
jweidley@MX480# top show security ipsec security-association ospf3-auth-core
description ospf3-neighbor-auth-core;
mode transport;
manual {
    direction bidirectional {
        protocol ah;
        spi 256;
        authentication {
            algorithm hmac-md5-96;
            key ascii-text "$9$W5I8XNs24DHmGDEyrvx72goaUjz3/AtOreYgoaiHTQF3ApSyK"; ## SECRET-DATA
        }
    }
}
```

IS-IS 認証

Junos OS でサポートされる認証では、すべての IGP がサポートされますが、各 IGP 自体のセキュリティ強度には差があります。多くのサービスプロバイダでは、OSPF か IS-IS が使われますが、これにより高速なコンバージェンスとスケーラビリティを実現できるだけでなく、MPLS（Multiprotocol Label Switching）でトラフィックエンジニアリング機能を利用することができます。IP 内にカプセル化されるためリモートからのなりすましや DoS 攻撃に対して脆弱な OSPF と比べ、IS-IS はネットワークレイヤーで動作しないことから、なりすまし行為が難しくなります。

Junos における IS-IS 認証の実装では、リンクステート PDU（LSP）、IIH PDU、完全および部分シーケンス番号 PDU（CSNP および PSNP）を含むすべての PDU タイプに、デフォルトで MD5 チェックサム値が挿入されます。

また、IS-IS では、レベル 1 およびレベル 2 でシンプルおよび MD5 認証が両方サポートされています。シンプル認証では、プロトコル更新のスニッフィングによってキーを容易に復元できることから、本書の前セクションと同様に、MD5 を使用します。

レベル 1 の IS-IS 認証を有効にする方法

1. 実際に動作するシンプルな ISIS 設定から開始します。

```
[edit protocols isis]
jweidley@mx80# show
interface ge-0/0/1.0 {
    level 2 disable;
}
interface lo0.0 {
    passive;
}
```

2. 認証タイプを MD5 に設定します。

```
[edit protocols isis]
jweidley@mx80# set level 1 authentication-type md5
```

3. 認証キーを設定します。組織のパスワード複雑性ポリシーに適合した、容易に推測できないキーを使用することをお奨めします。

```
[edit protocols isis]
jweidley@mx80# set level 1 authentication-key D5vw~\H,[bIOaG4
```

4. 設定を確認します。

```
[edit protocols isis]
jweidley@mx80# show
level 1 {
    authentication-key "$9$wHgoGjHmTFnHk9puOEhSrev7V"; ## SECRET-DATA
    authentication-type md5;
}
interface ge-0/0/1.0 {
    level 2 disable;
}
interface lo0.0 {
    passive;
}
```

Hello パケット交換に対して IS-IS 認証を有効にする方法

セキュリティをさらに強化するために、IS-IS Hello 交換の認証でインタフェースごとに別の認証キーを設定することもできます。

1. 前述の例を基に、特定のインタフェースで認証タイプを設定します。

```
[edit protocols isis]
jweidley@mx80# edit interface ge-0/0/1.0

[edit protocols isis interface ge-0/0/1.0]
jweidley@mx80# set level 1 hello-authentication-type md5
```

2. 認証キーを設定します。組織のパスワード複雑性ポリシーに適合した、容易に推測できないキーを使用することをお奨めします。

```
[edit protocols isis interface ge-0/0/1.0]
jweidley@mx80# set level 1 hello-authentication-key 4}QYWwR+^@V7^uf
```

3. 設定全体を確認します。

```
[edit protocols isis interface ge-0/0/1.0]
jweidley@mx80# up

[edit protocols isis]
jweidley@mx80# show
level 1 {
    authentication-key "$9$wHgoGjHmTFnHk9puOEhSrev7V"; ## SECRET-DATA
    authentication-type md5;
}
interface ge-0/0/1.0 {
    level 2 disable;
    level 1 {
        hello-authentication-key "$9$yDcKMXNds4JGdVjq.PzFn/CtIc"; ## SECRET-DATA
        hello-authentication-type md5;
    }
}
interface lo0.0 {
    passive;
}
```

注 M、MX、およびTシリーズ デバイスのJunos 11.2では、IS-ISのヒットレス認証キーロールオーバーを使用できます。詳細については、http://www.juniper.net/techpubs/en_US/junos11.2/topics/example/authentication-keychain-hitless-isis.html を参照してください。

BGP 認証

BGP は、AS（Autonomous System）に接続するための EGP（External Gateway Protocol）です。これまでの例の IGP と同様に、BGP でも MD5 認証がサポートされます。Junos は、高度なセキュリティ要件に対応するために、MD5 よりさらに強力なアルゴリズムをサポートしていますが、以下の例では MD5 を使用します。

MD5 は、広く利用されている暗号化ハッシュアルゴリズムで、128 ビットのハッシュ値を生成します。送信側ルーターは、隣接機器に送信するすべての BGP パケットに、設定済みの MD5 ハッシュ値を挿入します。受信側ルーターは BGP パケットを受信すると、パケットの内容を処理する前に、このチェックサム値を確認します。

BGP のルート認証を実装する際は、認証をグローバルに有効にするか、グループごとに有効にするか、またはピアごとに有効にするかを考慮する必要があります。このような柔軟性により、大規模な環境において、設定を合理化し、認証設定およびキー変更を管理しやすくすることができます。

ヒント セキュリティプラクティスとして、External BGP ネイバーの認証はピアレベルで設定することをお奨めします。これにより、サービスプロバイダごとに個別のキーを使用し、これらのキーが共有されないようにすることができます。

MD5 による BGP 認証を有効にする方法

セキュリティプラクティスとして、外部ピアに対してピアごとの認証を使用し、各ネイバーに対して個別のキーを使用することが推奨されます。以下の例でもこれに従います。

1. 実際に動作するシンプルな BGP 設定から開始します。

```
[edit protocols bgp]
jweidley@MX960# show
group session-to-isp1 {
    type external;
    peer-as 65000;
    neighbor 192.168.11.1;
}
```

2. ピアルーターへの認証を有効にします。組織のパスワード複雑性ポリシーに適合した、容易に推測できない認証キーを使用することをお奨めします。

```
[edit protocols bgp]
jweidley@MX960# edit group session-to-isp1

[edit protocols bgp group session-to-isp1]
jweidley@MX960# set neighbor 192.168.11.1 authentication-key 4}QYWwR+^@V7^uf
```

3. 設定全体を確認します。

```
[edit protocols bgp group session-to-isp1]
jweidley@MX960# up

[edit protocols bgp]
jweidley@MX960# show
group session-to-isp1 {
    type external;
    peer-as 65000;
    neighbor 192.168.11.1 {
        authentication-key "$9$y8grWL4aUjkmcyoZjHTQEhSeM84aGUDHO1bsgJiHOBIhSe"; ## SECRET-DATA
    }
}
```

ヒットレス認証キーロールオーバーを使用した BGP 認証を有効にする方法

セキュリティプラクティスとして、静的なパスワードは定期的に変更するのがよいでしょう。これには、ルート認証キーも含まれますが、大規模なネットワークでは大変な作業になり、場合によっては管理できなくなる可能性があります。

認証キーは、BGP ピアリングセッションをリセットせずに変更することが可能です。これは、ヒットレス認証キーロールオーバーと呼ばれます。

ヒットレス認証キーロールオーバーでは、複数のキー ID、共有秘密パスワード、および実装日時から成る認証キーチェーンが使用されます。このキーチェーンは、このアルゴリズムが設定されている BGP ネイバーとのセッションに関連付けられます。

1. 実際に動作するシンプルな BGP 設定から開始します。

```
[edit protocols bgp]
jweidley@MX960# show
group session-to-core {
    type internal;
    local-address 10.10.10.170;
    neighbor 10.10.10.86;
}
```

2. キーチェーンに最初のキーを設定します。キー ID の範囲は 0 ～ 63 です。組織のパスワード複雑性ポリシーに適合した、容易に推測できない認証キーを使用することをお奨めします。

```
[edit protocols bgp]
jweidley@MX960# top edit security authentication-key-chains key-chain core-bgp-keychain

[edit security authentication-key-chains key-chain core-bgp-keychain]
jweidley@MX960# set key 0 secret D5vw~\H,[bIOaG4

[edit security authentication-key-chains key-chain core-bgp-keychain]
jweidley@m10# set key 0 start-time 2011-04-01.00:01
```

3. キーチェーンに 2 つ目のキーを設定します。この手順を必要な数だけ繰り返します。

```
 [edit security authentication-key-chains key-chain core-bgp-keychain]
jweidley@MX960# set key 1 secret 4}QYWwR+^@V7^uf

[edit security authentication-key-chains key-chain core-bgp-keychain]
jweidley@MX960# set key 1 start-time 2011-07-01.00:01
```

4. BGP ネイバーの認証に MD5 アルゴリズムを使用するよう設定します。

```
[edit security authentication-key-chains key-chain core-bgp-keychain]
jweidley@MX960# top edit protocols bgp group session-to-core

[edit protocols bgp group session-to-core]
jweidley@MX960# set neighbor 10.10.10.86 authentication-algorithm md5
```

5. 先ほど設定したキーチェーンとネイバーをマッピングします。

```
 [edit protocols bgp group session-to-core]
jweidley@MX960# set neighbor 10.10.10.86 authentication-key-chain core-bgp-keychain
```

6. それでは、設定を確認してみましょう。

```
[edit protocols bgp group session-to-core]
jweidley@MX960# show
type internal;
local-address 10.10.10.170;
neighbor 10.10.10.86{
    authentication-algorithm md5;
    authentication-key-chain core-bgp-keychain;
}

[edit protocols bgp group session-to-core]
jweidley@MX960# top show security authentication-key-chains
key-chain core-bgp-keychain {
    description "automatic key management for BGP with core";
    key 0 {
        secret "$9$bp24ZDi.5z3iH/tpOREcylKxd"; ## SECRET-DATA
        start-time "2011-4-3.00:01:00 -0700";
    }
    key 1 {
        secret "$9$s9YJGQF//9tX7.PT3AtLxNVwg"; ## SECRET-DATA
        start-time "2011-7-1.00:01:00 -0700";
    }
}
```

注　キーローテーションは日時に基づくため、安定した、信頼できる NTP ソースを設定することが不可欠です。

さらに詳しくは　ヒットレス認証キーロールオーバーの詳細については、http://www.juniper.net/techpubs/en_US/junos10.4/topics/usage-guidelines/routing-configuring-authentication-for-bgp.html?searchid=1265747436637 を参照してください。

MPLS（Multi-Protocol Label Switching）

ネットワークの論理的分割を促進し、セキュリティを強化する適切な MPLS（Multi-Protocol Label Switching）設定には、多数の機能が含まれていますが、本書ですべてを網羅することはできません。ただし、信頼されていないソースとの間でラベル付きパケットの送受信を行わなければ、多くの MPLS の脆弱性と攻撃は、回避することができます。そこで、このセクションでは、MPLS のやり取りを信頼されたソースにのみ限定する方法を説明します。

MPLS の設定の中では、インタフェースで `family mpls` を有効にする必要があります。この設定は、そのインタフェースで受信した MPLS プロトコルパケットをドロップしないようシステムに指示するものです。デバイスが、想定されたルーターからのみ MPLS パケットを受信するよう、必要なインタフェースにのみ family-mpls を設定してください。

また、どのインタフェースがどのプロトコルに参加しているかを RPD（Routing Protocol Daemon）に通知するには、Junos の `protocols` 階層で MPLS を有効にする必要があります。公開されている参考資料の中には、`interface all` を紹介しているものもあります。このコマンドで MPLS は動作しますが、一部の MPLS 攻撃に対してデバイスが脆弱なままになる可能性があります。

図 4.2 に、必要なインタフェースで必要なプロトコルのみを有効にした、推奨される MPLS の設定を示します。CE（Customer Edge）側のインタフェースは、MPLS に直接参加しないため、設定しないでください。

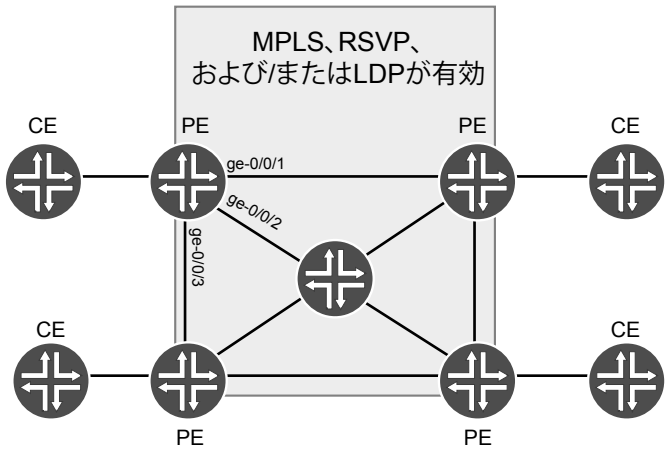

図 4.2　**必要なインタフェースで MPLS、RSVP、LDP を有効にした状態**

図 4.2 のように MPLS インタフェースを設定する方法

図 4.2 の PE1 の P 側および PE 側インタフェースの MPLS を設定します。

1. 最初に、インタフェースレベルで family MPLS を有効にする必要があります。

```
[edit interfaces]
jweidley@PE1# set ge-0/0/1 unit 0 family mpls

[edit interfaces]
jweidley@PE1# set ge-0/0/2 unit 0 family mpls

[edit interfaces]
jweidley@PE1# set ge-0/0/3 unit 0 family mpls
```

2. 次に、protocols MPLS で、P 向けおよび PE 向けインタフェースのみを定義します。

```
[edit]
jweidley@PE1# edit protocols mpls

[edit protocols mpls]
jweidley@PE1# set interface ge-0/0/1.0

[edit protocols mpls]
jweidley@PE1# set interface ge-0/0/2.0

[edit protocols mpls]
jweidley@PE1# set interface ge-0/0/3.0

[edit protocols mpls]
jweidley@PE1# show
interface ge-0/0/1.0;
interface ge-0/0/2.0;
interface ge-0/0/3.0;
```

さらに詳しくは　MPLS の概念の詳細および実際の設定例については、ティム・フィオラおよびジェイミー・パナゴス著『*This Week：MPLS の導入*』（http://www.juniper.net/dayone）を参照してください。

RSVP 認証

RSVP プロトコルのやり取りでも、認証することによって、信頼されたデバイスのみがリザベーションのセットアップに参加するようにできます。

Junos では、RSVP 認証で MD5 がサポートされます。偽装、メッセージ改ざん、およびリプレイ攻撃を防御するために、メッセージダイジェストが特定のインタフェースからすべてのネイバーに送信されます。組織のパスワード複雑性ポリシーに適合した、容易に推測できない認証キーを使用してください。

RSVP を有効にするインターフェースでは認証を設定しておくことをおすすめします。以下の設定で全てです。

```
[edit]
jweidley@PE1# edit protocols rsvp

[edit protocols rsvp]
jweidley@PE1# set interface ge-0/0/2.0 authentication-key 4{QYBxwR+$@V7!uf

[edit protocols rsvp]
jweidley@PE1# show
interface ge-0/0/2.0 {
    authentication-key "$9$d7V2aZGi.fzDi"; ## SECRET-DATA
}
```

注 この機能では機密性が提供されないことに注意してください。すなわち、信頼されたネイバーの認証のみが行われ、パケットの内容は暗号化されません。

ヒント また、RSVP メッセージの交換を信頼された IP アドレスのみに制限する設定をファイアウォールフィルタに追加することをお奨めします。

さらに詳しくは RSVP 認証の詳細については、http://www.juniper.net/books で紹介されている『*Junos Cookbook*』（アビバ・ギャレット著、O’ Reilly Media 発行、2006 年）を参照してください。

LDP 認証

LDP 認証は、LDP セッションのコネクションストリームに入り込む可能性のある、なりすましの TCP パケットからの保護に役立ちます。

LDP 通信は必要なインタフェースにのみ有効にし、認証によってなりすまし攻撃から保護することをお奨めします。組織のパスワード複雑性ポリシーに適合した、容易に推測できない認証キーを使用してください。

以下、設定です。

```
[edit]
jweidley@PE1# edit protocols ldp session 10.10.10.85

[edit protocols ldp session 10.10.10.85]
jweidley@PE1# set authentication-key 4{QYBxwR+$@V7!uf

[edit protocols ldp session 10.10.10.85]
jweidley@PE1# show
authentication-key "$9$pJpguIcyrvL7Vev"; ## SECRET-DATA
```

注 LDPでは、より強力な認証アルゴリズムと自動キーローテーションのためのキーチェーン（http://www.juniper.net/techpubs/en_US/junos11.2/topics/reference/configuration-statement/authentication-key-chains-edit-security.html で説明）もサポートされています。ご使用のプラットフォームとJunosのバージョンの参考資料も確認してください。

ヒント また、LDP メッセージの交換を信頼された IP アドレスのみに制限する設定をファイアウォールフィルタに追加することをお奨めします。

さらに詳しくは LDP 認証の詳細については、http://www.juniper.net/books で紹介されている『*Junos Cookbook*』（アビバ・ギャレット著、O' Reilly Media 発行、2006 年）を参照してください。

ルーティングエンジンの保護

RE（Routing Engine）は、ルーティング情報更新の処理から CLI（Command Line Interface）の提供まで、さまざまな機能を実行します。他のデバイスと同様に、そのリソースには限りがあるため、デバイスの安定性と可用性が確保されるよう、RE のリソースを保護する必要があります。

本書のこれまでのセクションでは、セキュアではないサービスを無効にする方法、セキュアなサービスを有効にする方法、管理サービスのセキュリティを強化する方法、ログインするユーザーに必要最低限の権限を適用する方法、およびルーティングプロトコルで認証を有効にする方法を説明してきました。最後のステップでは、許可されたソースアドレスとプロトコルのみを許可するファイアウォールフィルタを適用して、ルーティングエンジンを保護します。

RE に到達するすべてのトラフィックに注意を向け、どういったセキュリティリスクの可能性があるかを認識しておくことが重要です。直前のセクションでは、認証機能により、ルーターが信頼されたピアとのみルーティング関係を形成できることを説明しました。これはルーティングプロトコルの保護には役立ちますが、悪意のあるパケットや信頼されていないパケットが RE（Routing Engine）の特定のプロセスにアプローチするのを完全に防ぐことはできません。例えば、攻撃者が特定のプロトコルで偽のパケットを用いて、ルーターに攻撃を仕掛ける可能性もあります。このようなパケットは認証チェックで失敗しますが、攻撃によって RE のルーターリソース（CPU サイクルおよびキュー）が消費される可能性があるため、ある程度のインパクトは受けることになります。この状況を防ぐには、信頼されたソースからのプロトコルとコントロールパケットのみがファイアウォールフィルタを通過し、RE に到達できるようにする必要があります。

各環境およびデバイスによって考慮すべきことはそれぞれ異なるため、どの環境にも適用できる包括的なファイアウォールフィルタを提示するのは困難です。しかし、Junos は、機能と細分性を提供する独自の用語と多彩なオプションを備えているため、あらゆる状況に対応できます。ルーティングエンジンのセキュリティ強化というトピックで Day One ブックレット 1 冊を割いているのはそのためです（このページ下部の参考資料を参照してください）。ここで同じ概念の説明を繰り返すつもりはありません。代わりに、ルーティングエンジン保護およびそれに必要な概念を説明し、実装する上でのちょっとしたテクニックを紹介します。

注意 ファイアウォールフィルタ構文はすべての Junos プラットフォームで共通ですが、ハードウェア（チップセット、ASIC など）の違いにより、機能によっては特定プラットフォームのみのサポートになっているものもあります。フィルタを設計する前に、ご使用のプラットフォームのファイアウォールフィルタに関する参考資料を確認することを強くお奨めします。

さらに詳しくは ファイアウォールフィルタによるルーティングエンジンのセキュリティ強化に関する詳細な基本情報および優れたチュートリアルについては、ダグラス・ハンクス・ジュニア著『*Day One:Securing the Routing Engine on M, MX, and T Series*』（http://www.juniper.net/dayone）を参照してください。

ファイアウォールフィルタの設計

ファイアウォールフィルタを作成する基本的な方法は 2 通りあります。

- デフォルトで許可：このようなフィルタでは、望ましくないホスト、ネットワーク、またはポートとプロトコルを指定し、これらを拒否します。このフィルタの最後の条件で、その他すべてのトラフィックを許可します。
- デフォルトで拒否：信頼されたソースから、デバイスに設定されているサービスおよび機能へのトラフィックを許可するファイアウォールフィルタを作成します。このフィルタの最後の条件で、その他すべてのトラフィックを拒否します。

デフォルトで拒否の方法は、最もセキュアで、ルーティングエンジンの保護に最適です。このセクションでは、デフォルトで拒否の方法を使用します。

デフォルトで拒否のフィルタの場合、必要なすべてのサービスを期待どおりに動作させるために、デフォルト許可のフィルタに比べ、多くの考慮とテストが必要になります。ファイアウォールを作成し、RE に対して何を許可するかを考慮するときには、出発点として以下のリストを参考にするとよいでしょう。

- ルーティングプロトコル（BGP、OSPF など）
- アクセスサービス（SSH、J-Web、NETCONF など）
- 管理サービス（SNMP、NTP、DNS など）
- 診断およびトラブルシューティングプロトコル（ICMP、traceroute など）

この他、以下の考慮すべきポイントを覚えておいてください。

- ファイアウォールフィルタはステートレスです。すなわち、それより前にデバイスで許可または拒否されたパケットについて考慮しません。
- ファイアウォールフィルタは、上から下へ順番に処理されます。多くの Junos プラットフォームでは、ファイアウォールフィルタはハードウェアでラインレートで処理されますが、ベストプラクティスとして、複数のフィルタを設定するときは、常に、ルーティングプロトコルなど時間的な制約があるプロトコルをフィルタの先頭近くに配置することをお奨めします。
- サービスごとに term を分けることをお奨めします。こうすることにより、設定が分かりやすくなり、変更およびトラブルシューティングが容易になります。
- プロトコルおよびサービスについては先頭に deny の term を配置します。これにより、ログが、不要な情報で煩雑にならないようにすることができます。

ファイアウォールフィルタのビルディングブロック

ファイアウォールフィルタ構文は詳細を記述するため、容易に理解できない場合があります。このセクションでは、ファイアウォールフィルタを分かりやすく、また管理しやすくするための機能をいくつか紹介します。詳細については、*『Day One:Securing the Routing Engine』*をダウンロードしてください。

prefix-list によるホストまたはネットワークのグループ化

多くのファイアウォールでは、ホストやネットワークなどをグループ化して一つのオブジェクトにし、ファイアウォールルールでこのオブジェクトを参照するようにしています。これにより、オブジェクト名によってホスト / ネットワークのグループを参照することができ、設定がわかりやすくなります。

ここで紹介する最初の例では、ネットワーク管理サブネットが含まれるプレフィックスを作成しましょう。

1. mgmt-nets という名前の prefix-list を作成します。

```
[edit]
jweidley@MX240# edit policy-options prefix-list mgmt-nets
```

2. この prefix-list に管理サブネットの IP サブネットを追加します。

```
[edit policy-options prefix-list mgmt-nets]
jweidley@MX240# set 192.168.2.0/24

[edit policy-options prefix-list mgmt-nets]
jweidley@MX240# set 192.168.4.0/24
```

3. 設定を確認します。

```
[edit policy-options prefix-list mgmt-nets]
jweidley@MX240# show
192.168.2.0/24;
192.168.4.0/24;
```

注 J シリーズや SRX デバイスなどフローベースでトラフィックを処理するプラットフォームでは、prefix-list と address-set を混同しないよう注意してください。どちらもサポートしていますが、その使用目的が異なります。address-set がセキュリティポリシーで使用されるのに対し、prefix-list はパケットベースのフィルタリング機能に使用されます。

apply-path による動的 prefix-list の作成

デフォルトで拒否のファイアウォールフィルタでは、特定のホストとプロトコルを許可し、その他すべてを拒否するため、管理が煩雑になる可能性があります。NTP サーバーを変更したり新しい BGP ピアを追加した場合はどうなるのでしょうか。お分かりのとおり、必ずファイアウォールフィルタを更新する必要があり、そうしないとファイアウォールフィルタが正しく機能しなくなります。

Junos の apply-path 機能を使用すると、コンフィグレーションの特定箇所で一致したパターンを基に prefix-list を動的に作成することができます。これにより、同じ情報を繰り返し記述する必要がなくなるため、設定が分かりやすくなり、見落とす可能性が低減されます。

例として、本書の NTP 階層の設定を使用して、ntp-servers という名前の prefix-list を作成してみましょう。NTP 設定は以下のようになります。

```
[edit]
jweidley@MX240# show system ntp
boot-server 192.168.3.2;
authentication-key 1 type md5 value "$9$-kboZjHqKvMWLNs4"; ## SECRET-DATA
server 192.168.3.2 key 1 prefer; ## SECRET-DATA
server 192.168.33.2 key 1; ## SECRET-DATA
trusted-key 1;
source-address 172.25.44.132;
```

ここで、apply-path を使用して prefix-list を設定します。これにより、NTP 設定が変更されると、prefix-list が自動的に更新されるようになります。

1. ntp-servers という名前の prefix-list を作成します。

```
[edit]
lab@MX240# edit policy-options prefix-list ntp-servers
```

2. apply-path 機能を使用して、設定内の NTP サーバーを照合します。

```
[edit]
lab@MX240# set apply-path "system ntp server <*>"
```

3. 設定を確認します。

```
[edit policy-options prefix-list ntp-servers]
lab@MX240# show
apply-path "system ntp server <*>";
```

手順 3 から、この prefix-list の値が、[system ntp] 階層で設定されている NTP server コマンドから取り出されることが分かります。実際の IP アドレスを確認するには、以下のように show | display inheritance コマンドを使用します。

```
[edit policy-options prefix-list ntp-servers]
lab@MX240-RE0# show | display inheritance
##
## apply-path was expanded to:
##     192.168.3.2;
##     192.168.33.2;
##
apply-path "system ntp server <*>";
```

apply-path を使用する最大のメリットは、Junos によって自動的に動的 prefix-list が作成され、維持されることです。

トラフィックにレートリミットを適用するポリサーの作成

ポリサーを使用してトラフィックにレートリミットを適用することができます。ポリサーはファイアウォールフィルタと連携し、フィルタまたは条件に一致したトラフィックに対して帯域を制限します。

ポリサーの設定は非常に簡単ですが、帯域幅の定義は少々トリッキーです。

注 ポリサーの動作、使用されるアルゴリズム、その監視方法については本書では扱いません。詳細については、この簡潔なチュートリアルの後の参考資料を参照してください。このセクションでは、ポリサーによってルーティングエンジンを保護する方法のみ説明します。

それでは、3Mbps の制限を適用するポリサーを設定しましょう。

1. ポリサーの名前を定義します。簡潔な記述名を使用すると、ファイアウォールフィルタの設定が分かりやすくなるため便利です。この例では、limit という名前を使用し、最大帯域幅「3m」を挿入しましょう。

```
[edit firewall]
jweidley@MX240# edit policer limit-3m
```

2. 最大帯域幅を設定します。bandwidth-limit コマンドは、bps で定義しますが、幸い Junos CLI では、より分かりやすい値（g（1,000,000,000）、m（1,000,000）、および k（1,000））を使用できます。

```
[edit firewall policer limit-3m]
jweidley@MX240# set if-exceeding bandwidth-limit 3m
```

3. burst-size-limit コマンドは必須です。このコマンドで指定した最大値までトラフィックがバーストすると、ポリシングによる平均帯域幅の適用が開始されます。この値は、バイト単位で指定してください。

```
[edit firewall policer limit-3m]
jweidley@MX240# set if-exceeding burst-size-limit 625k
```

4. 次に、設定したしきい値を超えたトラフィックに対してどのような処理を実行するかを定義します。この例では、このようなトラフィックをドロップします。

```
[edit firewall policer limit-3m]
jweidley@MX240 # set then discard
```

5. 設定を確認します。

```
[edit firewall policer limit-3m]
jweidley@MX240# up

[edit firewall]
jweidley@MX240# show policer limit-3m
if-exceeding {
    bandwidth-limit 3m;
    burst-size-limit 625k;
}
then discard;
```

ポリシングについてさらに深く調べ、実機確認しておくとよいでしょう。そうすることで、その動作や `burst-size-limit` コマンドの影響についての理解を深めることができます。このコマンドの設定値が小さすぎると、過剰なポリシングにつながります。また、大きすぎると、十分にポリシングが行われない可能性があります。

さらに詳しくは ポリサーの詳細については、ダグラス・ハンクス・ジュニア著『*Day One:Securing the Routing Engine on M, MX, and T Series*』（http://www.juniper.net/dayone）または http://www.juniper.net/books で紹介されている『*Junos Enterprise Routing, 2nd Edition*』（サウスウィック、マーシュキー、およびレイノルド著、O’ Reilly Media 発行、2008 年）を参照してください。

ファイアウォールフィルタの作成

前述の概念を利用して、必要なサービスとトラフィックのみを許可し、ルーティングエンジンへのその他すべてのトラフィックを拒否する、基本的なファイアウォールフィルタを作成しましょう。

1. 最初に、必要な prefix-list を作成します。

```
[edit]
jweidley@MX240# edit policy-options prefix-list bgp-neighbors

[edit policy-options prefix-list bgp-neighbors]
jweidley@MX240# set apply-path "protocols bgp group <*> neighbor <*>"

[edit policy-options prefix-list bgp-neighbors]
jweidley@MX240# up

[edit policy-options]
jweidley@MX240# edit prefix-list ipv4-interfaces

[edit policy-options prefix-list ipv4-interfaces]
jweidley@MX240# set apply-path "interfaces <*> unit <*> family inet address <*>"

[edit policy-options prefix-list ipv4-interfaces]
jweidley@MX240# up

[edit policy-options]
jweidley@MX240# edit prefix-list ospf-all-routers

[edit policy-options prefix-list ospf-all-routers]
jweidley@MX240# set 224.0.0.5/32
```

```
[edit policy-options prefix-list ospf-all-routers]
jweidley@MX240# set 224.0.0.6/32

[edit policy-options prefix-list ospf-all-routers]
jweidley@MX240# up

[edit policy-options]
jweidley@MX240# edit prefix-list ntp-servers

[edit policy-options prefix-list ntp-servers]
jweidley@MX240# set apply-path "system ntp server <*>"

[edit policy-options prefix-list ntp-servers]
jweidley@MX240# up

[edit policy-options]
jweidley@MX240# edit prefix-list snmp-servers

[edit policy-options prefix-list snmp-servers]
jweidley@MX240# set apply-path "snmp community <*> clients <*>"

[edit policy-options prefix-list snmp-servers]
jweidley@MX240# up

[edit policy-options]
jweidley@MX240# edit prefix-list mgmt-nets

[edit policy-options prefix-list mgmt-nets]
jweidley@MX240# set 192.168.3.0/24

[edit policy-options prefix-list mgmt-nets]
jweidley@MX240# set 192.168.33.0/24

[edit policy-options prefix-list mgmt-nets]
jweidley@MX240# up

[edit policy-options]
jweidley@MX240# edit prefix-list radius-servers

[edit policy-options prefix-list radius-servers]
jweidley@MX240# set apply-path "system radius-server <*>"

[edit policy-options prefix-list radius-servers]
jweidley@MX240# up

[edit policy-options]
jweidley@MX240# edit prefix-list localhost

[edit policy-options prefix-list localhost]
jweidley@MX240# set 127.0.0.0/8

[edit policy-options prefix-list localhost]
jweidley@MX240# top
```

2. 使用するダイナミックルーティングプロトコルを許可する term を作成します。この例では、BGP および OSPF を許可します。

```
[edit]
jweidley@MX240# edit firewall family inet filter protect-re

[edit firewall family inet filter protect-re]
jweidley@MX240# edit term allow-bgp
```

```
[edit firewall family inet filter protect-re term allow-bgp]
jweidley@MX240# set from prefix-list bgp-neighbors

[edit firewall family inet filter protect-re term allow-bgp]
jweidley@MX240# set from protocol tcp

[edit firewall family inet filter protect-re term allow-bgp]
jweidley@MX240# set from destination-port bgp

[edit firewall family inet filter protect-re term allow-bgp]
jweidley@MX240# set then accept

[edit firewall family inet filter protect-re term allow-bgp]
jweidley@MX240# up

[edit firewall family inet filter protect-re]
jweidley@MX240# edit term allow-ospf

[edit firewall family inet filter protect-re term allow-ospf]
jweidley@MX240# set from source-prefix-list ipv4-interfaces

[edit firewall family inet filter protect-re term allow-ospf]
jweidley@MX240# set from destination-prefix-list ospf-all-routers

[edit firewall family inet filter protect-re term allow-ospf]
jweidley@MX240# set from destination-prefix-list ipv4-interfaces

[edit firewall family inet filter protect-re term allow-ospf]
jweidley@MX240# set from protocol ospf

[edit firewall family inet filter protect-re term allow-ospf]
jweidley@MX240# set then accept

[edit firewall family inet filter protect-re term allow-ospf]
jweidley@MX240# up
```

3. 次に、信頼された管理ネットワークからの SSH（Secure Shell）によるセキュアなリモートアクセスを許可するための term を作成します。

```
[edit firewall family inet filter protect-re]
jweidley@MX240# edit term allow-ssh

[edit firewall family inet filter protect-re term allow-ssh]
jweidley@MX240# set from prefix-list mgmt-nets

[edit firewall family inet filter protect-re term allow-ssh]
jweidley@MX240# set from protocol tcp

[edit firewall family inet filter protect-re term allow-ssh]
jweidley@MX240# set from destination-port ssh

[edit firewall family inet filter protect-re term allow-ssh]
jweidley@MX240# set then accept

[edit firewall family inet filter protect-re term allow-ssh]
jweidley@MX240# up
```

4. ネットワークを監視するため、管理サーバーからの SNMP アクセスを許可します。

```
[edit firewall family inet filter protect-re]
jweidley@MX240# edit term allow-snmp

[edit firewall family inet filter protect-re term allow-snmp]
```

```
jweidley@MX240# set from prefix-list snmp-servers

[edit firewall family inet filter protect-re term allow-snmp]
jweidley@MX240# set from protocol udp

[edit firewall family inet filter protect-re term allow-snmp]
jweidley@MX240# set from destination-port 161

[edit firewall family inet filter protect-re term allow-snmp]
jweidley@MX240# set then accept

[edit firewall family inet filter protect-re term allow-snmp]
jweidley@MX240# up
```

5. NTP サーバとの同期を許可します。

```
[edit firewall family inet filter protect-re]
jweidley@MX240# edit term allow-ntp

[edit firewall family inet filter protect-re term allow-ntp]
jweidley@MX240# set from prefix-list ntp-servers

[edit firewall family inet filter protect-re term allow-ntp]
jweidley@MX240# set from prefix-list localhost

[edit firewall family inet filter protect-re term allow-ntp]
jweidley@MX240# set from protocol udp

[edit firewall family inet filter protect-re term allow-ntp]
jweidley@MX240# set from destination-port ntp

[edit firewall family inet filter protect-re term allow-ntp]
jweidley@MX240# set then accept

[edit firewall family inet filter protect-re term allow-ntp]
jweidley@MX240# up
```

6. RADIUS サーバーからの RADIUS レスポンスのみを許可します。このフィルタでは RADIUS サーバーのポートを送信元ポートとして定義しており、入力フィルタであるため RADIUS レスポンスにマッチするものになっています。

```
[edit firewall family inet filter protect-re]
jweidley@MX240# edit term allow-radius

[edit firewall family inet filter protect-re term allow-radius]
jweidley@MX240# set from prefix-list radius-servers

[edit firewall family inet filter protect-re term allow-radius]
jweidley@MX240# set from protocol udp

[edit firewall family inet filter protect-re term allow-radius]
jweidley@MX240# set from source-port 1812

[edit firewall family inet filter protect-re term allow-radius]
jweidley@MX240# set from source-port 1813

[edit firewall family inet filter protect-re term allow-radius]
jweidley@MX240# set from source-port 1645

[edit firewall family inet filter protect-re term allow-radius]
jweidley@MX240# set then accept

[edit firewall family inet filter protect-re term allow-radius]
jweidley@MX240# up
```

7. トラブルシューティングに役立つ ICMP タイプと traceroute で使う UDP ポートを許可します。ただし、フラグメント ICMP パケットはすべてブロックします。

```
[edit firewall family inet filter protect-re]
jweidley@MX240# edit term icmp-frags

[edit firewall family inet filter protect-re term icmp-frags]
jweidley@MX240# set from protocol icmp

[edit firewall family inet filter protect-re term icmp-frags]
jweidley@MX240# set from is-fragment

[edit firewall family inet filter protect-re term icmp-frags]
jweidley@MX240# set then syslog discard

[edit firewall family inet filter protect-re term icmp-frags]
jweidley@MX240# up

[edit firewall family inet filter protect-re]
jweidley@MX240# edit term allow-icmp

[edit firewall family inet filter protect-re term allow-icmp]
jweidley@MX240# set from protocol icmp

[edit firewall family inet filter protect-re term allow-icmp]
jweidley@MX240# set from icmp-type echo-request

[edit firewall family inet filter protect-re term allow-icmp]
jweidley@MX240# set from icmp-type echo-reply

[edit firewall family inet filter protect-re term allow-icmp]
jweidley@MX240# set from icmp-type unreachable

[edit firewall family inet filter protect-re term allow-icmp]
jweidley@MX240# set from icmp-type time-exceeded

[edit firewall family inet filter protect-re term allow-icmp]
jweidley@MX240# set then accept

[edit firewall family inet filter protect-re term allow-icmp]
jweidley@MX240# up

[edit firewall family inet filter protect-re]
jweidley@MX240# edit term allow-traceroute

[edit firewall family inet filter protect-re term allow-traceroute]
jweidley@MX240# set from protocol udp

[edit firewall family inet filter protect-re term allow-traceroute]
jweidley@MX240# set from destination-port 33434-33523

[edit firewall family inet filter protect-re term allow-traceroute]
jweidley@MX240# set then accept

[edit firewall family inet filter protect-re term allow-traceroute]
jweidley@MX240# up
```

8. 確立されたすべてのセッションを許可する term を作成します。tcp-established キーワードは、ACK または RST ビットが設定された TCP パケットに一致します。

```
[edit firewall family inet filter protect-re]
jweidley@MX240# edit term tcp-established

[edit firewall family inet filter protect-re term tcp-established]
jweidley@MX240# set from protocol tcp

[edit firewall family inet filter protect-re term tcp-established]
jweidley@MX240# set from source-port ssh

[edit firewall family inet filter protect-re term tcp-established]
jweidley@MX240# set from source-port bgp

[edit firewall family inet filter protect-re term tcp-established]
jweidley@MX240# set from tcp-established

[edit firewall family inet filter protect-re term tcp-established]
jweidley@MX240# set then accept

[edit firewall family inet filter protect-re term tcp-established]
jweidley@MX240# up
```

9. 最後に、デフォルトで拒否のtermを設定して、すべてのトラフィックをドロップし、ログ記録します。log オプションにより、PFE（Packet Forwarding Engine）のバッファにパケットヘッダー情報が保存され、Syslog オプションにより、ルーティングエンジンにパケットヘッダー情報が保存されます。

```
[edit firewall family inet filter protect-re]
jweidley@MX240# edit term default-deny

[edit firewall family inet filter protect-re term default-deny]
jweidley@MX240# set then syslog log discard

[edit firewall family inet filter protect-re term default-deny]
jweidley@MX240# top
```

10. それでは、ファイアウォール設定を確認してみましょう。

```
[edit]
jweidley@MX240# show policy-options
prefix-list bgp-neighbors {
    apply-path "protocols bgp group <*> neighbor <*>";
}
prefix-list ipv4-interfaces {
    apply-path "interfaces <*> unit <*> family inet address <*>";
}
prefix-list ospf-all-routers {
    224.0.0.5/32;
    224.0.0.6/32;
}
prefix-list ntp-servers {
    apply-path "system ntp server <*>";
}
prefix-list snmp-servers {
    apply-path "snmp community <*> clients <*>";
}
prefix-list mgmt-nets {
    192.168.3.0/24;
    192.168.33.0/24;
}
prefix-list radius-servers {
    apply-path "system radius-server <*>";
}
prefix-list localhost {
```

```
    127.0.0.0/8;
}

[edit]
jweidley@MX240# show firewall | no-more
family inet {
    filter protect-re {
        term allow-bgp {
            from {
                prefix-list {
                    bgp-neighbors;
                }
                protocol tcp;
                destination-port bgp;
            }
            then accept;
        }
        term allow-ospf {
            from {
                source-prefix-list {
                    ipv4-interfaces;
                }
                destination-prefix-list {
                    ospf-all-routers;
                    ipv4-interfaces;
                }
                protocol ospf;
            }
            then accept;
        }
        term allow-ssh {
            from {
                prefix-list {
                    mgmt-nets;
                }
                protocol tcp;
                destination-port ssh;
            }
            then accept;
        }
        term allow-snmp {
            from {
                prefix-list {
                    snmp-servers;
                }
                protocol udp;
                destination-port 161;
            }
            then accept;
        }
        term allow-ntp {
            from {
                prefix-list {
                    ntp-servers;
                    localhost;
                }
                protocol udp;
                destination-port ntp;
            }
            then accept;
        }
        term allow-radius {
            from {
```

```
                prefix-list {
                    radius-servers;
                }
                protocol udp;
                source-port [ 1812 1813 1645 ];
            }
            then accept;
        }
        term icmp-frags {
            from {
                is-fragment;
                protocol icmp;
            }
            then {
                syslog;
                discard;
            }
        }
        term allow-icmp {
            from {
                protocol icmp;
                icmp-type [ echo-request echo-reply unreachable time-exceeded ];
            }
            then accept;
        }
        term allow-traceroute {
            from {
                protocol udp;
                destination-port 33434-33523;
            }
            then accept;
        }
        term tcp-established {
            from {
                protocol tcp;
                source-port [ ssh bgp ];
                tcp-established;
            }
            then accept;
        }
        term default-deny {
            then {
                log;
                syslog;
                discard;
            }
        }
    }
}
```

レートリミット付きファイアウォールフィルタの作成

レートリミットにより、フィルタにもう1つの防御機能が提供されます。特定ホストからの特定プロトコルのみを許可することに加え、レートリミットによって、許可されたトラフィックの量を許容範囲内に制限することで、許可されたホストであってもルーティングエンジンに大量のトラフィックを送信できないようにします。

重複を避けるため、前のセクションのファイアウォールフィルタをベースに、特定タイプのトラフィックにレートリミットを適用するポリサーを追加していきます。また、ルーティングエンジンを TCP SYN フラッド攻撃から保護する新しい term も追加します。

1. 最初に、それぞれ異なるレートでトラフィックを制限するポリサーをいくつか設定しましょう。

```
[edit firewall]
jweidley@MX240#edit policer limit-10m

[edit firewall policer limit-10m]
jweidley@MX240#set if-exceeding bandwidth-limit 10m

[edit firewall policer limit-10m]
jweidley@MX240#set if-exceeding burst-size-limit 625k

[edit firewall policer limit-10m]
jweidley@MX240#set then discard

[edit firewall policer limit-10m]
jweidley@MX240#up

[edit firewall]
jweidley@MX240#edit policer limit-3m

[edit firewall policer limit-3m]
jweidley@MX240#set if-exceeding bandwidth-limit 3m

[edit firewall policer limit-3m]
jweidley@MX240#set if-exceeding burst-size-limit 15k

[edit firewall policer limit-3m]
jweidley@MX240#set then discard

[edit firewall policer limit-3m]
jweidley@MX240#up


[edit firewall]
jweidley@MX240#edit policer limit-1m

[edit firewall policer limit-1m]
jweidley@MX240#set if-exceeding bandwidth-limit 1m

[edit firewall policer limit-1m]
jweidley@MX240#set if-exceeding burst-size-limit 15k

[edit firewall policer limit-1m]
jweidley@MX240#set then discard

[edit firewall policer limit-1m]
jweidley@MX240#up

[edit firewall]
jweidley@MX240#edit policer limit-100k

[edit firewall policer limit-100k]
jweidley@MX240#set if-exceeding bandwidth-limit 100k

[edit firewall policer limit-100k]
jweidley@MX240#set if-exceeding burst-size-limit 15k

[edit firewall policer limit-100k]
jweidley@MX240#set then discard

[edit firewall policer limit-100k]
jweidley@MX240#up
```

```
[edit firewall]
jweidley@MX240#edit policer limit-32k

[edit firewall policer limit-32k]
jweidley@MX240#set if-exceeding bandwidth-limit 32k

[edit firewall policer limit-32k]
jweidley@MX240#set if-exceeding burst-size-limit 15k

[edit firewall policer limit-32k]
jweidley@MX240#set then discard

[edit firewall policer limit-32k]
jweidley@MX240#top
```

2. セキュリティ強化の対策はやりすぎて問題になる、ということはありません。ルーティングエンジンをさらに保護するために、管理プロトコルにポリサーを追加して、このプロトコルが適切に動作するようにしましょう。SSH トラフィックは、10Mbps に制限します。この値は、環境によっては高すぎると感じるかもしれませんが、新しい Junos イメージなどの大容量ファイルを SCP（Secure Copy）によって RE に転送することを想定しています。

```
[edit firewall family inet filter protect-re]
jweidley@MX240#set term allow-ssh then policer limit-10m
```

3. SNMP トラフィックを 1Mbps に制限しましょう。この値であれば、ネットワーク管理プロトコルがルーティングエンジンに影響を与えることなく、多数の OID を安全に取り出すことができます。

```
[edit firewall family inet filter protect-re]
jweidley@MX240#set term allow-snmp then policer limit-1m
```

3. NTP トラフィックに含まれるパケットは毎時数個のみであるため、32Kbps に制限します。

```
[edit firewall family inet filter protect-re]
jweidley@MX240#set term allow-ntp then policer limit-32k
```

4. そして、RADIUS トラフィックでは大量の帯域幅を消費すべきではないため、この例では、トラフィックを 32Kbps に制限します。

```
[edit firewall family inet filter protect-re]
jweidley@MX240#set term allow-radius then policer limit-32k
```

フラッド攻撃から保護する方法

フラッド攻撃は、すべてのシステムリソースを枯渇させることを目的に、ターゲットデバイスに大量のパケットを送りつけるものです。これまでに報告された一般的なフラッド攻撃では、ICMP および TCP SYN パケットが使用されてきましたが、それ以外のパケットタイプでも不可能ではありません。このセクションでは、フラッド攻撃でよく使われるプロトコルにポリサーを適用します。

1. 最初に記述するポリサーは、`tcp-established` に対するものです。基本的に、ファイアウォールフィルタの `tcp-established` キーワードは、ACK または RST ビットが設定されたすべてのパケットを照合するため、ルーティングエンジンがフラッド攻撃に対して脆弱になる可能性があります。そのため、この条件に 10Mbps のポリサーを適用します。

```
[edit firewall family inet filter protect-re]
jweidley@MX240#set term tcp-established then policer limit-10m
```

2. 障害切り分けのために、トラブルシューティングプロトコルを許可しなければなりませんが、過剰なシステムリソースが消費されないよう、帯域を制限する必要があります。トラブルシューティングおよびパフォーマンス監視の多くの状況で、ICMP トラフィックを 1Mbps に制限するのが妥当ではないでしょうか。

```
[edit firewall family inet filter protect-re]
jweidley@MX240#set term allow-icmp then policer limit-1m
```

3. traceroute トラフィックを 1Mbps に制限します。

```
[edit firewall family inet filter protect-re]
jweidley@MX240#set term allow-traceroute then policer limit-1m
```

4. TCP フラッド攻撃として、SYN 攻撃が最もよく知られていますが、その他の TCP コントロールフラグが使用される可能性もあります。そこで、RST、FIN、および SYN（同時に ACK フラグも設定されていない場合）フラグが設定された TCP コントロールパケットにポリサーを適用しましょう。

```
[edit firewall family inet filter protect-re]
jweidley@MX240#edit term synflood-protect

[edit firewall family inet filter protect-re term synflood-protect]
jweidley@MX240#set from source-prefix-list bgp-neighbors

[edit firewall family inet filter protect-re term synflood-protect]
jweidley@MX240#set from source-prefix-list mgmt-nets

[edit firewall family inet filter protect-re term synflood-protect]
jweidley@MX240#set from protocol tcp

[edit firewall family inet filter protect-re term synflood-protect]
jweidley@MX240#set from tcp-flags "(syn & !ack) | fin | rst"

[edit firewall family inet filter protect-re term synflood-protect]
jweidley@MX240#set then policer limit-100k

[edit firewall family inet filter protect-re term synflood-protect]
jweidley@MX240#set then accept
```

5. SYN フラッド攻撃を効果的に防御するには、この term をフィルタの先頭に配置する必要があります。

```
[edit firewall family inet filter protect-re term synflood-protect]
jweidley@MX240#up

[edit firewall family inet filter protect-re]
jweidley@MX240#insert term synflood-protect before term allow-bgp
```

6. それでは、ファイアウォールフィルタとポリサーの設定を確認してみましょう。

```
[edit firewall family inet filter protect-re]
jweidley@MX240#up 2

[edit firewall]
jweidley@MX240#show | no-more
family inet {
    filter protect-re {
        term synflood-protect {
            from {
                source-prefix-list {
                    bgp-neighbors;
                    mgmt-nets;
                }
                protocol tcp;
                tcp-flags "(syn & !ack) | fin | rst";
            }
            then {
                policer limit-100k;
                accept;
            }
```

```
}
term allow-bgp {
    from {
        prefix-list {
            bgp-neighbors;
        }
        protocol tcp;
        destination-port bgp;
    }
    then accept;
}
term allow-ospf {
    from {
        source-prefix-list {
            ipv4-interfaces;
        }
        destination-prefix-list {
            ospf-all-routers;
            ipv4-interfaces;
        }
        protocol ospf;
    }
    then accept;
}
term allow-ssh {
    from {
        prefix-list {
            mgmt-nets;
        }
        protocol tcp;
        destination-port ssh;
    }
    then {
        policer limit-10m;
        accept;
    }
}
term allow-snmp {
    from {
        prefix-list {
            snmp-servers;
        }
        protocol udp;
        destination-port 161;
    }
    then {
        policer limit-1m;
        accept;
    }
}
term allow-ntp {
    from {
        prefix-list {
            ntp-servers;
            localhost;
        }
        protocol udp;
        destination-port ntp;
    }
    then {
        policer limit-32k;
        accept;
    }
```

```
        }
        term allow-radius {
            from {
                prefix-list {
                    radius-servers;
                }
                protocol udp;
                source-port [ 1812 1813 1645 ];
            }
            then {
                policer limit-32k;
                accept;
            }
        }
        term icmp-frags {
            from {
                is-fragment;
                protocol icmp;
            }
            then {
                syslog;
                discard;
            }
        }
        term allow-icmp {
            from {
                protocol icmp;
                icmp-type [ echo-request echo-reply unreachable time-exceeded ];
            }
            then {
                policer limit-1m;
                accept;
            }
        }
        term allow-traceroute {
            from {
                protocol udp;
                destination-port 33434-33523;
            }
            then {
                policer limit-1m;
                accept;
            }
        }
        term tcp-established {
            from {
                protocol tcp;
                source-port [ ssh bgp ];
                tcp-established;
            }
            then {
                policer limit-10m;
                accept;
            }
        }
        term default-deny {
            then {
                log;
                syslog;
                discard;
            }
        }
    }
```

```
}
policer limit-10m {
    if-exceeding {
        bandwidth-limit 10m;
        burst-size-limit 625k;
    }
    then discard;
}
policer limit-1m {
    if-exceeding {
        bandwidth-limit 1m;
        burst-size-limit 15k;
    }
    then discard;
}
policer limit-100k {
    if-exceeding {
        bandwidth-limit 100k;
        burst-size-limit 15k;
    }
    then discard;
}
policer limit-32k {
    if-exceeding {
        bandwidth-limit 32k;
        burst-size-limit 15k;
    }
    then discard;
}
```

ファイアウォールフィルタの実装

ファイアウォールフィルタは、2 ステップのプロセスで使用することができます。すなわち、まずフィルタを作成し、次にそれらをインタフェースのどちらかの方向に適用します。

ここでの目的は、ルーティングエンジンのセキュリティを強化することであるため、作成したファイアウォールフィルタをループバックインタフェース（lo0）に適用しましょう。ループバックインタフェースは、RE に関連付けられた論理インタフェースです。そのため、ルーティングエンジンを保護するには、図 4.3 に示すように、ファイアウォールフィルタをすべてのインタフェースに適用するのではなく、ループバックインタフェースにのみ適用することになります。

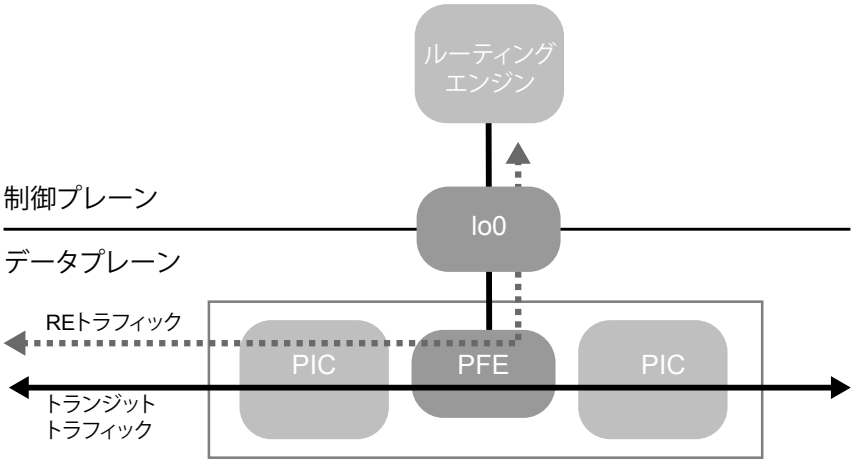

図 4.3　トランジットトラフィックと RE トラフィック

ファイアウォールフィルタには、どの方向のトラフィックを対象にするかを指示する必要があります。フィルタを適用する方向には、以下の 2 つがあります。

- 入力：パケットがネットワークからインタフェースに入るときに、ファイアウォールフィルタと照合されます。
- 出力：パケットがインタフェースから出て行くときに、ファイアウォールフィルタと照合されます。

ここでは、ルーティングエンジンを保護するために、図 4.4 に示すように、lo0 インタフェース（入力）に入ってくるトラフィックを対象としたファイアウォールフィルタを実装しましょう。

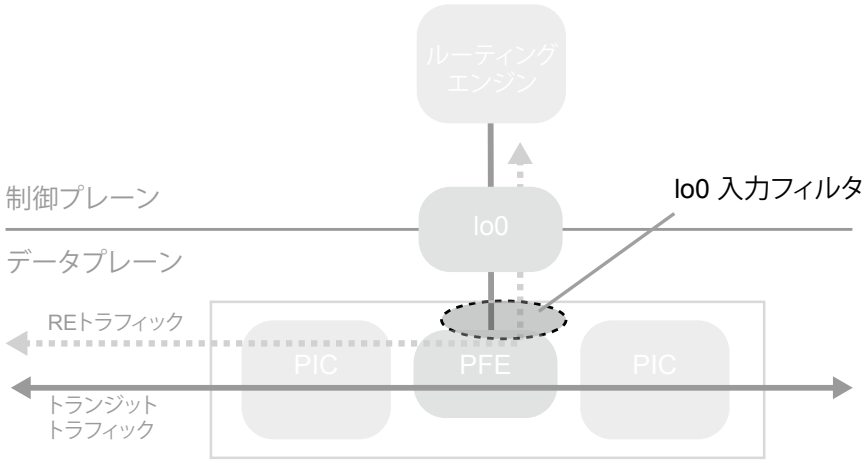

図 4.4 **トランジットトラフィックと RE トラフィック（lo0 入力フィルタあり）**

ここで紹介する例では、protect-re フィルタを lo0.0 インタフェースに適用します。

```
[edit interfaces lo0]
jweidley@MX240# show
unit 0 {
    family inet {
        filter {
            input protect-re;
        }
        address 10.10.10.170/32;
    }
}
```

ヒントと自己防衛手法

ファイアウォールフィルタについてどの程度理解を深め、テストを行ったかに関係なく、実際にコンフィグレーションをコミットするときには、慎重になり、さらに多少ナーバスになるのは当然のことです。幸い、Junos には、このような心配を和らげるために役立ついくつかの機能が組み込まれています。また、成功率を上げるためのテクニックもいくつかあります。

明らかに最初に考えるべきことは、設定を反映させる際、ファイアウォールフィルタをコンソールポートからコミットすることです。これにより、デバイスから閉め出されてアクセスできなくなる可能性を低減できます。

ただし、常にコンソールアクセスを使用できるわけではありません。その場合、2 ステップのコミットプロセスを提供する `commit confirmed <min>` コマンドを使用することです。このコマンドの入力後、変更は反映されますが、指定時間内に 2 回目の `commit` を発行するまで、その変更は継続されません。つまり 2 回目の `commit` を入力しないまま指定時間が経過すると、設定は自動的にロールバックされます。これは、

デバイスから閉め出されるのを防ぐことができる素晴らしいコマンドです。

デフォルトの commit confirm の値は 10 分です。誤ってデバイスから閉め出され、ルーティング更新がブロックされてしまった場合には、この時間が長すぎるかもしれません。幸い、commit confirm の値は変更可能です。ロールバック時間としては 2 分が妥当でしょう。この時間があれば、リモートアクセス、ルーティング隣接関係などを確認することができます。それでは設定してみましょう。

```
[edit interfaces lo0 unit 0]
jweidley@MX240# commit confirmed 2
commit confirmed will be automatically rolled back in 2 minutes unless confirmed
commit complete

# commit confirmed will be rolled back in 2 minutes
[edit interfaces lo0 unit 0]
jweidley@MX240#

Broadcast Message from root@MX240
        (no tty) at 1:47 EDT...

Commit was not confirmed; automatic rollback complete.

[edit interfaces lo0 unit 0]
jweidley@MX240#
```

もう一つのテクニックは、ログ記録を有効にして一時的に Default Permit 条件を Default Deny 条件の上に挿入することです。この方法では、デフォルトで許可のログを監視して、ファイアウォールフィルタに含め忘れたものがないかを確認することができます。それでは設定してみましょう。

```
[edit firewall family inet filter protect-RE]
lab@MX240# show
....
term temp-default-permit {
    then {
        log;
        accept;
    }
}
term default-deny {
    then {
        log;
        syslog;
        reject;
    }
}
```

次に、show firewall log コマンドを使用して、重要なトラフィックが欠落していないか確認できます。ファイアウォールログの出力が見にくい場合がありますが、出力をよく調べてみましょう。

```
jweidley@MX240> show firewall log
Log :
Time      Filter    Action Interface  Protocol Src Addr      Dest Addr
20:09:26  protect-re A     fxp0.0     IGMP     172.25.46.190 224.0.0.1
20:09:26  protect-re A     fxp0.0     UDP      172.25.46.6   172.25.46.255
20:09:19  protect-re A     fxp0.0     IGMP     172.25.45.140 224.0.0.1
20:09:17  protect-re A     fxp0.0     IGMP     172.25.46.96  224.0.0.1
20:09:11  protect-re A     fxp0.0     IGMP     172.25.46.180 224.0.0.1
20:09:07  protect-re A     fxp0.0     IGMP     172.25.46.182 224.0.0.1
20:09:05  protect-re A     fxp0.0     UDP      172.25.46.15  172.25.46.255
```

show firewall log detail コマンドを使用して、送信元ポートと宛先ポートを表示させることもできます。重要なトラフィックが拒否されていないことを確認したら、一時的に追加したデフォルトで許可の条件は削除して結構です。

最後に紹介するテクニックは、カウンターを使用してデバイスが受信している特定トラフィックの量を調べることです。内部ログバッファに保存できるデータ量は限られているため、show firewall log コマンドを実行したときに、デバイスがトラフィックで「あふれている」ように思えることもあります。カウンターと clear および show firewall counters コマンドを組み合わせて使用することで、どの程度のデータが拒否されているかをより正確に知ることができます。

```
jweidley@MX240> show firewall

Filter: protect-re
Counters:
Name                        Bytes              Packets
count-syn                   4840069            55160
count-ping                  69624648           229862
default-deny                4805044704         28671684
```

本書では、さまざまな側面から Junos デバイスのセキュリティ強化について説明してきました。フレキシビリティ、単一の OS によってもたらされるメリット、そして特に、必要な機能を有効にしながら Junos デバイスのセキュリティを強化する機能など、Junos 自体に組み込まれているセキュリティ機能の素晴らしさを十分理解できたことでしょう。

セキュリティ強化テンプレートを作成するときは、実際のネットワーク固有のセキュリティ要件に応じてこれらの手法を活用してください。ガイダンスおよび指示については、各自のセキュリティポリシーを参照してください。また、設定の変更が、他のチーム、通常の運用、および緊急時の対応にどのように影響しうるかを調査してください。変更後の設定をラボでテストし、すべてのエンジニアに、設定の変更内容および挙動が変わる点について伝えてください。そして何より、ルールに従い、注意深く、また継続的に監視することが重要です。

そうして、デバイスのセキュリティ体制を強化することができるのです。

付録

付録 A：Junos のセキュリティ強化チェックリスト

管理（第 1 章を参照）

- ■ 最新のジュニパーネットワークスセキュリティ勧告を調べる
- ■ 最新のサポート / 推奨バージョンの Junos をインストールする
- ■ インストール前に、必ず暗号化チェックサムを確認する

物理的セキュリティ（第 2 章を参照）

- ■ 以前設置されていたデバイスを再導入する場合は、メディアインストールを実行して、以前の設定およびその他データをすべて確実に削除する
- ■ コンソールポート
  - □ logout-on-disconnect 機能を設定する
  - □ insecure 機能を設定する
- ■ AUX ポート
  - □ 正当な用途がない場合は、補助ポートを無効にする
  - □ insecure 機能を設定する
- ■ ダイアグポート
  - □ 診断ポートに強力なパスワードを設定する
- ■ クラフトインタフェース /LCD メニュー
  - □ 環境に不要な機能を無効にする
- ■ 未使用のネットワークポートを無効にする

ネットワークセキュリティ（第 3 章および第 4 章を参照）

- ■ すべてのマネジメント関連トラフィックに OOB（Out-of-Band）インタフェースを使用する（第 3 章を参照）
- ■ default-address-selection オプションを有効にする（第 4 章を参照）
  - □ または、ルーティングエンジンで生成されるすべてのトラフィックの送信元アドレスを設定する（NTP、SNMP、Syslog など）
- ■ ICMP リダイレクトをグローバルで無効にする（第 4 章を参照）
- ■ ソースルーティングが設定されていないことを確認する（第 3 章を参照）
- ■ IP ダイレクテッドブロードキャストが設定されていないことを確認する（第 3 章を参照）
- ■ プロキシ ARP が設定されていないこと、またはプロキシ ARP が特定のインタフェースに制限されていることを確認する（第 3 章を参照）
- ■ SYN および FIN フラグの組み合わせが設定された TCP パケットを RE（Routing Engine）でドロップするよう設定する（第 4 章を参照）
- ■ ICMP タイムスタンプおよびレコードルートリクエストで RE が lo0 IP アドレスを隠すよう設定する（第 4 章を参照）
- ■ 必要なネットワークポートにのみ LLDP を設定する（第 4 章を参照）

マネジメントサービスのセキュリティ（第 4 章を参照）

- 複数の信頼されたサーバーとの NTP 通信に認証を設定する
- 最もセキュアな方法を使用して、複数の信頼されたサーバーとの SNMP 通信を設定する
  - コミュニティストリングと USM パスワードは、パスワード複雑性ポリシーに適合した、容易に推測できないものにする
  - read-only に設定する。read-write は絶対に必要な場合にのみ使用する
  - 複数の信頼されたサーバーへのクエリー / トラップ送信を許可する
- 拡張タイムスタンプを使用して複数の信頼されたサーバーに Syslog メッセージを送信する
- 複数の信頼されたサーバーへのセキュアな自動設定バックアップを設定する

アクセスセキュリティ（第 4 章を参照）

- ログイン情報の入力前に表示される警告バナーを設定する
- セキュアではないアクセスサービス、または不要なアクセスサービスを無効にする（telnet、HTTP による J-Web、FTP など）
- 必要となるセキュアなアクセスサービスを有効にする
  - SSH
    - SSH バージョン 2 を使用する
    - root アカウントでのログインを拒否する
    - 環境に適した connection-limit および rate-limit を設定する
  - J-Web
    - 信頼された CA により署名された有効な証明書を使用して、HTTPS を使用する
    - 許可された特定のインタフェースからのみアクセスが行われるよう制限する
    - idle-time 値を設定してアイドル状態の接続を終了する
    - 環境に適した session-limit を設定する

ユーザー認証のセキュリティ（第 4 章を参照）

- パスワード複雑性ポリシーを設定する
  - 最小パスワード長、文字セット、および最小変更回数
  - SHA1 でパスワードを保存する
- root アカウントに、組織のパスワード複雑性ポリシーに適合した強力なパスワードが設定されていることを確認する
- パスワード推測攻撃から防御するために、ログインセキュリティオプションを設定する

- 権限を必要最小限にする原則に従って、アクセスレベルが異なるエンジニアのために、それぞれのカスタムログインクラスを設定する
  - □ 職務ごとにコマンドを制限する
  - □ すべてのログインクラスに適切なアイドルタイムアウトを設定する
- 集中認証
  - □ 組織のパスワード複雑性ポリシーに適合した強力な共有秘密パスワードを使用する
  - □ 耐障害性を高めるために複数のサーバーを設定する
  - □ アクティビティおよび使用状況をトレースするためのアカウンティングを設定する
  - □ 認証サーバーが使用できない場合に備えて、緊急用のローカルアカウントを作成する
- ローカル認証
  - □ 組織のパスワード複雑性ポリシーに適合した強力なパスワードを使用する
  - □ ローカルアカウントを、必要なユーザーに限定する
  - □ 設定されているすべてのローカルアカウントの作成理由および使用目的を把握する
- ログインセキュリティポリシーに従って authentication-order を適切に設定する

ルーティングプロトコルのセキュリティ（第 4 章を参照）

- 必要なインタフェースでのみルーティングプロトコルを使用する
- BGP トラフィックの送信元をループバックインタフェースにする
- 内部および外部の信頼されたソースとのルート認証を設定する
  - □ ご使用の機器および隣接機器でサポートされている最も強力なアルゴリズムを選択する
  - □ 組織のパスワード複雑性ポリシーに適合した強力な認証キーを使用する
  - □ 組織ごとに異なる認証キーを使用してキーの使用範囲を制限する
- 組織のセキュリティポリシーに従って、ルート認証キーを定期的に変更する（ルーティングプロトコルでサポートされている場合は、ヒットレスキーロールオーバーの使用を検討する）

ファイアウォールフィルタ（第 4 章を参照）

- ファイアウォールフィルタでデフォルトで拒否のポリシーを使用してルーティングエンジンを保護する
  - □ 必要な ICMP タイプのみを許可し、その他すべての ICMP タイプおよびコードを拒否する
  - □ 最後の条件 default-deny に syslog オプションを含め、拒否されたすべてのトラフィックを中央で監視できるようにする
- フラッド攻撃で一般的に使用されているプロトコルにレートリミットを適用する
- ポリサーを使用して、（適切な範囲内で）許可されたプロトコルにレートリミットを適用する

付録 B：ジュニパーネットワークスにおける米国政府認定への取り組み

ジュニパーネットワークスは、デバイスが必要な米国政府認定を取得できるよう、多大な労力とリソースを注いでいます。ここでは、そのプロセスについて概説しますが、最初にジュニパーネットワークスの主な 2 つのお問い合わせ先を示しておきます。

- 認定関連の情報については、Federal Strategic Initiatives 部門ディレクター（UCAPL@juniper.net）に問い合わせください。
- 技術情報については、レジデントテストエンジニア（jitc-test-engineers@juniper.net）に問い合わせることができます。ただし、エンジニアに直接お送りいただいたお問い合わせは、回答前に Federal Strategic Initiatives 部門の審査を通過する必要があります。

認定製品リスト登録までの過程

米国政府は、APL（Approved Products List）への登録を米国政府機関への販売の前提条件としており、ネットワーキングデバイスを該当 APL に登録する前に、いくつかの認定を取得することを要求しています。DoD（Department of Defense）では、DoD 内の APL 数を低減するために、UC-APL（Unified Capabilities Approved Products List）という単一の APL への登録を義務付けています。また、各軍において、UCR（Unified Capabilities Requirements）ドキュメントの内容に加え、必要に応じて軍固有の要件が追加されることがあります。これらの追加要件は、該当する軍のテストラボから提示され、政府機関とジュニパーネットワークスとの間で交渉が行われます。

UCR には、非常に多数の要件が詳述されており、これらの要件はテクノロジーごとに分類されています（一般ネットワーク機器 -NA、ルーター -R、レイヤー 3 スイッチ -LS）。そのため、ルーターについて指定された要件が一般ネットワーク機器に該当しない場合もあります。両方に該当する要件については、両方のデバイスが対象となります。JITC（Joint Interoperability Test Command）によって作成される UC テスト計画では、テスト対象の機器に関わらず、再現性を確保するために、これらの要件と詳細な手順が組み合わされます。すべての UC ドキュメントには、UCCO（Uniform Capabilities Certification Office）ホームページからアクセスできます（[Policies and Procedures]、[Key Documents and Requirements] の順にページをたどります）。

UCR リストでは、テストを受ける前に、デバイスが FIPS（Federal Information Processing Standard）および NIAP（National Information Assurance Partnership）の認定を取得することを要求しています。FIPS の認定は、NIST（National Institute of Standards and Technology）認定ラボで実施され、暗号化アルゴリズムの検証が行われます。一方、NIAP では、Protection Profile（保護プロファイル）に従って、デバイスが IA（Information Assurance）規格に適合していることが確認されます。NIAP 認定審理中でも、UC テストを開始する資格は十分ありますが、FIPS 140-2 認定は完了していなければなりません。NIST では、証明書および Security Policy（セキュリティポリシー）ドキュメントが作成され、NIAP では、Security Target（セキュリティターゲット）および Validation Report（検証レポート）ドキュメントと Common Criteria Certificates（共通基準証明書）が作成されます。

UC テストは、アリゾナ州フォートフアチュカの DISA（Defense Information Systems Agency）JITC（Joint Interoperability Test Command）、アリゾナ州フォートフアチュカの陸軍 TIC（Technology Integration Center）、メリーランド州インディアンヘッドの JITC、米国内のその他研究所など、さまざまな政府研究所で実施されます。ジュニパーネットワークスにおける連邦政府認定への取り組みは、カスタマーサービス部門に所属するレジデントテストエンジニアによって支えられています。ジュニパーネットワークス製品のスケジュールは、政府スポンサー、該当するテスト施設、デバイスの必要数およびタイプ（ファームウェアのバージョンを含む）、出荷スケジュール、輸送要件、およびデモプールのサポートの交渉後に Federal Strategic Initiatives 部門で決定されます。テストエンジニアは、どの研究所が選択された場合も、その研究所での政府による評価を支援します。

評価が完了すると、欠陥があった場合は TDR（Test Deficiency Report）として通知されます。TDR は、判定のため DISA に提出されます。TDR がクローズしない場合、ジュニパーネットワークスは、テスト対象デバイス（DUT）でいつ要件が満たされるか、また規格への完全準拠に先立って必要な軽減措置について詳述した POAM（Plan of Action and Milestones）の提出を求められます。軽減措置は、承認された方法で DUT を導入するために実装する必要のある導入条件として追加されます。

評価に合格すると、認定文書、DIACAP（DoD Information Assurance Certification and Accreditation Process）スコアカードが作成され、UC-APL に登録されます。DIACAP スコアカードは、政府および軍関係者が利用できますが、その際、CAC（Common Access Card）署名の電子メールを ucco@disa.mil に送信する必要があります。DIACAP スコアカードは、DUT 導入時にネットワーク認定のために必要になります。導入を行う組織は、テスト時に使用されたセキュリティ設定を適用することにより、完成された DIACAP スコアカードを使用して認定プロセスを短縮することができます。

設定、また最終的にはネットワーク認定を支援するために、ジュニパーネットワークスは、各テスト対象デバイスの『*Secure Deployment Guide*』を提供しています。このガイドでは、テストされた設定についての説明と、例、テストされた設定、および使用されたスクリプトがすべて 1 冊のドキュメントとしてまとめられています。このガイドは、ファイルサイズを削減し、クロスプラットフォームの互換性を確保するために、PDF 形式で提供されます。詳細については、Federal Strategic Initiatives 部門ディレクターにお問い合わせください。

以下の Web サイトでは、これらの情報をさらに深く調べることができます。

- UCCO ホームページ：
  http://www.disa.mil/ucco/index.html
- DISA APL プロセスガイド：
  http://www.disa.mil/ucco/apl_process.html?panel=1#A_Services
- UC APL のテストセンター：
  http://www.disa.mil/ucco/testing_facilities/
- FIPS ホームページ：
  http://csrc.nist.gov/groups/STM/cmvp/index.html
- FIPS モジュール検証リスト：
  http://csrc.nist.gov/groups/STM/cmvp/validation.html#02
- NIAP ホームページ：
  http://www.niap-ccevs.org/
- NIAP 米国政府承認済み保護プロファイル：
  http://www.niap-ccevs.org/pp/
- NIAP 評価製品リスト：
  http://www.niap-ccevs.org/vpl/
- 共通基準ポータル（CCEVS の管理外）：
  http://www.commoncriteriaportal.org/
- DISA STIG：
  http://iase.disa.mil/stigs/

付録 C：中レベルのセキュリティ設定例

注 以下の設定は、本書の Web ページ（http://www.juniper.net/dayone）から .rtf 形式の独立したファイルとして入手できます。

```
set version 10.4R6.5
set system host-name MX240
set system time-zone America/New_York
set system default-address-selection
set system no-redirects
set system no-ping-record-route
set system no-ping-time-stamp
set system internet-options tcp-drop-synfin-set
set system authentication-order [ radius tacplus ]
set system ports console log-out-on-disconnect
set system ports console insecure
set system ports auxiliary disable
set system ports auxiliary insecure
set system diag-port-authentication encrypted-password <PASSWORD>
set system pic-console-authentication encrypted-password <PASSWORD>
set system root-authentication encrypted-password <PASSWORD>
set system radius-server 192.168.3.20 port 1812
set system radius-server 192.168.3.20 secret <PASSWORD>
set system radius-server 192.168.4.20 port 1812
set system radius-server 192.168.4.20 secret <PASSWORD>
set system tacplus-server 192.168.3.40 port 49
set system tacplus-server 192.168.3.40 secret <PASSWORD>
set system tacplus-server 192.168.4.40 port 49
set system tacplus-server 192.168.4.40 secret <PASSWORD>
set system radius-options password-protocol mschap-v2
set system accounting events login
set system accounting events change-log
set system accounting events interactive-commands
```

```
set system accounting destination radius server 192.168.3.20 accounting-port 1813

set system accounting destination radius server 192.168.3.20 secret <PASSWORD>

set system accounting destination radius server 192.168.4.20 accounting-port 1813

set system accounting destination radius server 192.168.4.20 secret <PASSWORD>

set system accounting destination tacplus server 192.168.3.40 port 49

set system accounting destination tacplus server 192.168.3.40 secret <PASSWORD>

set system accounting destination tacplus server 192.168.4.40 port 49

set system accounting destination tacplus server 192.168.4.40 secret <PASSWORD>

set system login message .\n\tUNAUTHORIZED USE OF THIS SYSTEM\n\tIS STRICTLY PROHIBITED!\n\tPlease
contact \/company-noc@company.com\/ to gain\access to this equipment if you need authorization.\n"

set system login retry-options tries-before-disconnect 3

set system login retry-options backoff-threshold 1

set system login retry-options backoff-factor 6

set system login retry-options minimum-time 30

set system login class tier1 idle-timeout 10

set system login class tier1 login-alarms

set system login class tier1 login-tip

set system login class tier1 permissions maintenance

set system login class tier1 permissions network

set system login class tier1 permissions view

set system login class tier1 permissions view-configuration

set system login class tier1 deny-commands .(start *)|(set cli idle-timeout)|(request system
software)|(request system zeroize)|(request chassis)"

set system login class tier2 idle-timeout 15

set system login class tier2 login-alarms

set system login class tier2 permissions clear

set system login class tier2 permissions configure

set system login class tier2 permissions interface-control

set system login class tier2 permissions maintenance

set system login class tier2 permissions network

set system login class tier2 permissions rollback

set system login class tier2 permissions routing-control

set system login class tier2 permissions view
```

```
set system login class tier2 permissions view-configuration

set system login class tier2 deny-commands .(start *)|(set cli idle-timeout)|(request system
software)|(request system zeroize)"

set system login class tier2 deny-configuration .(groups)"

set system login class tier3 idle-timeout 20

set system login class tier3 login-alarms

set system login class tier3 permissions all

set system login user emergency full-name .Emergency Only Local Account"

set system login user emergency uid 2010

set system login user emergency class tier3

set system login user emergency authentication encrypted-password <PASSWORD>

set system login user tier1 full-name .Login template for Tier1 Users"

set system login user tier1 uid 2001

set system login user tier1 class tier1

set system login user tier2 full-name .Login template for Tier2 Users"

set system login user tier2 uid 2002

set system login user tier2 class tier2

set system login user tier3 full-name .Login template for Tier3 Users"

set system login user tier3 uid 2003

set system login user tier3 class tier3

set system login password minimum-length 15

set system login password change-type character-sets

set system login password minimum-changes 4

set system login password format sha1

set system services ssh root-login deny

set system services ssh protocol-version v2

set system services ssh connection-limit 10

set system services ssh rate-limit 2

set system services web-management https local-certificate ssl-cert

set system services web-management session idle-timeout 30

set system services web-management session session-limit 4

set system syslog user * any emergency
```

```
set system syslog host 192.168.3.2 any any

set system syslog host 192.168.3.2 log-prefix MX240

set system syslog host 192.168.4.2 any any

set system syslog host 192.168.4.2 log-prefix MX240

set system syslog file messages any info

set system syslog file messages authorization info

set system syslog file User-Auth authorization any

set system syslog file User-Auth interactive-commands any

set system syslog file audit interactive-commands any

set system syslog file processes daemon any

set system syslog console any any

set system syslog time-format year

set system syslog time-format millisecond

set system archival configuration transfer-on-commit

set system archival configuration archive-sites .scp://jweidley@192.168.3.2:/Configs" password
<PASSWORD>

set system ntp boot-server 192.168.3.2

set system ntp authentication-key 1 type md5

set system ntp authentication-key 1 value <PASSWORD>

set system ntp server 192.168.3.2 key 1

set system ntp server 192.168.3.2 prefer

set system ntp server 192.168.33.2 key 1

set system ntp trusted-key 1

set interfaces ge-0/0/4 description ---unused---

set interfaces ge-0/0/4 disable

set interfaces fxp0 unit 0 description .OOB Management"

set interfaces fxp0 unit 0 family inet address 172.25.46.170/24

set interfaces lo0 unit 0 family inet filter input protect-re

set snmp location DC1-Rack:8-Row:2

set snmp contact .CompanyName NOC:123.456.7890"

set snmp v3 usm local-engine user nms-user authentication-sha authentication-key <PASSWORD>

set snmp v3 usm local-engine user nms-user privacy-aes128 privacy-key <PASSWORD>
```

```
set snmp v3 vacm security-to-group security-model usm security-name nms-user group inventory-view

set snmp v3 vacm access group inventory default-context-prefix security-model usm security-level
privacy read-view inventory-view

set snmp v3 vacm access group inventory default-context-prefix security-model usm security-level
privacy notify-view inventory-view

set snmp v3 target-address nms1 address 192.168.3.2

set snmp v3 target-address nms1 tag-list chassis-trap-receivers

set snmp v3 target-address nms1 target-parameters noc-snmpv3-settings

set snmp v3 target-parameters noc-snmpv3-settings parameters message-processing-model v3

set snmp v3 target-parameters noc-snmpv3-settings parameters security-model usm

set snmp v3 target-parameters noc-snmpv3-settings parameters security-level privacy

set snmp v3 target-parameters noc-snmpv3-settings parameters security-name nms-user

set snmp v3 target-parameters noc-snmpv3-settings notify-filter chassis-traps

set snmp v3 notify chassis-trap-list type trap

set snmp v3 notify chassis-trap-list tag chassis-trap-receivers

set snmp v3 notify-filter chassis-traps oid jnxChassisOKTraps include

set snmp engine-id use-mac-address

set snmp view inventory-only oid jnxBoxAnatomy include

set snmp view inventory-only oid system include

set snmp view system-level oid jnxBoxAnatomy include

set snmp view system-level oid 1.3.6.1.2.1.2 include

set snmp view system-level oid 1.3.6.1.2.1.14 include

set snmp view system-level oid 1.3.6.1.2.1.15 include

set snmp view limited oid 1.3.6.1.2.1.2 include

set snmp client-list performance 192.168.10.0/28

set snmp client-list performance 192.168.20.0/28

set snmp client-list partner 172.16.1.0/28

set snmp client-list partner 172.16.10.0/28

set snmp community .S8M!y:4b" view inventory-only

set snmp community .S8M!y:4b" authorization read-only

set snmp community .S8M!y:4b" clients 192.168.3.3/32

set snmp community .S8M!y:4b" clients 192.168.33.3/32

set snmp community .CfL!d4#2" view system-level
```

```
set snmp community .CfL!d4#2" authorization read-only

set snmp community .CfL!d4#2" client-list-name performance

set snmp community .xH#5^Gp9" view limited

set snmp community .xH#5^Gp9" authorization read-only

set snmp community .xH#5^Gp9" client-list-name partner

set routing-options static route 0.0.0.0/0 next-hop 172.25.46.1

set routing-options router-id 10.10.10.170

set routing-options autonomous-system 65501

set protocols rsvp interface ge-0/0/2.0 authentication-key <PASSWORD>

set protocols bgp group session-to-isp1 type external

set protocols bgp group session-to-isp1 peer-as 65000

set protocols bgp group session-to-isp1 neighbor 192.168.11.1 authentication-key <PASSWORD>

set protocols bgp group session-to-core type internal

set protocols bgp group session-to-core local-address 10.10.10.170

set protocols bgp group session-to-core neighbor 10.10.10.86 authentication-algorithm md5

set protocols bgp group session-to-core neighbor 10.10.10.86 authentication-key-chain core-bgp-
keychain

set protocols isis level 1 authentication-key <PASSWORD>

set protocols isis level 1 authentication-type md5

set protocols isis interface ge-0/0/1.0 level 2 disable

set protocols isis interface ge-0/0/1.0 level 1 hello-authentication-key <PASSWORD>

set protocols isis interface ge-0/0/1.0 level 1 hello-authentication-type md5

set protocols isis interface lo0.0 passive

set protocols ospf export advertise-static

set protocols ospf area 0.0.0.0 interface ge-0/0/1.0 authentication md5 1 key <PASSWORD>

set protocols ospf area 0.0.0.0 interface ge-0/0/1.0 authentication md5 2 key <PASSWORD>

set protocols ospf area 0.0.0.0 interface ge-0/0/1.0 authentication md5 2 start-time .2011-3-
31.16:32:00 -0400"

set protocols ospf3 export advertise-static

set protocols ospf3 area 0.0.0.0 interface lo0.0 passive

set protocols ospf3 area 0.0.0.0 interface ge-0/0/1.0 ipsec-sa ospf3-auth-core

set protocols ldp session 10.10.10.85 authentication-key <PASSWORD>

set protocols rip authentication-type md5
```

```
set protocols rip authentication-key <PASSWORD>

set protocols rip group eng-group export advertise-static

set protocols rip group eng-group neighbor ge-0/0/1.0 authentication-type md5

set protocols rip group eng-group neighbor ge-0/0/1.0 authentication-key <PASSWORD>

set protocols lldp interface all disable

set protocols lldp interface ge-0/0/0

set protocols lldp interface ge-0/0/3

set policy-options prefix-list bgp-neighbors apply-path .protocols bgp group <*> neighbor <*>"

set policy-options prefix-list ipv4-interfaces apply-path .interfaces <*> unit <*> family inet
address <*>"

set policy-options prefix-list ospf-all-routers 224.0.0.5/32

set policy-options prefix-list ospf-all-routers 224.0.0.6/32

set policy-options prefix-list ntp-servers apply-path .system ntp server <*>"

set policy-options prefix-list snmp-servers apply-path .snmp community <*> clients <*>"

set policy-options prefix-list mgmt-nets 192.168.3.0/24

set policy-options prefix-list mgmt-nets 192.168.33.0/24

set policy-options prefix-list radius-servers apply-path .system radius-server <*>"

set policy-options prefix-list localhost 127.0.0.0/8

set policy-options policy-statement advertise-static from protocol static

set policy-options policy-statement advertise-static then accept

set security certificates local ssl-cert <CERTIFICATE>

set security ipsec security-association ospf3-auth-core description ospf3-neighbor-auth-core

set security ipsec security-association ospf3-auth-core mode transport

set security ipsec security-association ospf3-auth-core manual direction bidirectional protocol ah

set security ipsec security-association ospf3-auth-core manual direction bidirectional spi 256

set security ipsec security-association ospf3-auth-core manual direction bidirectional
authentication algorithm hmac-md5-96

set security ipsec security-association ospf3-auth-core manual direction bidirectional
authentication key ascii-text <PASSWORD>

set security authentication-key-chains key-chain core-bgp-keychain key 0 secret <PASSWORD>

set security authentication-key-chains key-chain core-bgp-keychain key 0 start-time .2011-4-
1.00:01:00 -0400"

set security authentication-key-chains key-chain core-bgp-keychain key 1 secret <PASSWORD>
```

```
set security authentication-key-chains key-chain core-bgp-keychain key 1 start-time .2011-7-
1.00:01:00 -0400"

set firewall family inet filter protect-re term synflood-protect from source-prefix-list bgp-
neighbors

set firewall family inet filter protect-re term synflood-protect from source-prefix-list mgmt-
nets

set firewall family inet filter protect-re term synflood-protect from protocol tcp

set firewall family inet filter protect-re term synflood-protect from tcp-flags .(syn & !ack) |
fin | rst"

set firewall family inet filter protect-re term synflood-protect then policer limit-100k

set firewall family inet filter protect-re term synflood-protect then accept

set firewall family inet filter protect-re term allow-bgp from prefix-list bgp-neighbors

set firewall family inet filter protect-re term allow-bgp from protocol tcp

set firewall family inet filter protect-re term allow-bgp from destination-port bgp

set firewall family inet filter protect-re term allow-bgp then accept

set firewall family inet filter protect-re term allow-ospf from source-prefix-list ipv4-
interfaces

set firewall family inet filter protect-re term allow-ospf from destination-prefix-list ospf-
all-routers

set firewall family inet filter protect-re term allow-ospf from destination-prefix-list ipv4-
interfaces

set firewall family inet filter protect-re term allow-ospf from protocol ospf

set firewall family inet filter protect-re term allow-ospf then accept

set firewall family inet filter protect-re term allow-ssh from prefix-list mgmt-nets

set firewall family inet filter protect-re term allow-ssh from protocol tcp

set firewall family inet filter protect-re term allow-ssh from destination-port ssh

set firewall family inet filter protect-re term allow-ssh then policer limit-10m

set firewall family inet filter protect-re term allow-ssh then accept

set firewall family inet filter protect-re term allow-snmp from prefix-list snmp-servers

set firewall family inet filter protect-re term allow-snmp from protocol udp

set firewall family inet filter protect-re term allow-snmp from destination-port 161

set firewall family inet filter protect-re term allow-snmp then policer limit-1m

set firewall family inet filter protect-re term allow-snmp then accept

set firewall family inet filter protect-re term allow-ntp from prefix-list ntp-servers

set firewall family inet filter protect-re term allow-ntp from prefix-list localhost

set firewall family inet filter protect-re term allow-ntp from protocol udp

set firewall family inet filter protect-re term allow-ntp from destination-port ntp
```

```
set firewall family inet filter protect-re term allow-ntp then policer limit-32k
set firewall family inet filter protect-re term allow-ntp then accept
set firewall family inet filter protect-re term allow-radius from prefix-list radius-servers
set firewall family inet filter protect-re term allow-radius from protocol udp
set firewall family inet filter protect-re term allow-radius from source-port 1812
set firewall family inet filter protect-re term allow-radius from source-port 1813
set firewall family inet filter protect-re term allow-radius from source-port 1645
set firewall family inet filter protect-re term allow-radius then policer limit-32k
set firewall family inet filter protect-re term allow-radius then accept
set firewall family inet filter protect-re term icmp-frags from is-fragment
set firewall family inet filter protect-re term icmp-frags from protocol icmp
set firewall family inet filter protect-re term icmp-frags then syslog
set firewall family inet filter protect-re term icmp-frags then discard
set firewall family inet filter protect-re term allow-icmp from protocol icmp
set firewall family inet filter protect-re term allow-icmp from icmp-type echo-request
set firewall family inet filter protect-re term allow-icmp from icmp-type echo-reply
set firewall family inet filter protect-re term allow-icmp from icmp-type unreachable
set firewall family inet filter protect-re term allow-icmp from icmp-type time-exceeded
set firewall family inet filter protect-re term allow-icmp then policer limit-1m
set firewall family inet filter protect-re term allow-icmp then accept
set firewall family inet filter protect-re term allow-traceroute from protocol udp
set firewall family inet filter protect-re term allow-traceroute from destination-port 33434-
33523
set firewall family inet filter protect-re term allow-traceroute then policer limit-1m
set firewall family inet filter protect-re term allow-traceroute then accept
set firewall family inet filter protect-re term tcp-established from protocol tcp
set firewall family inet filter protect-re term tcp-established from source-port ssh
set firewall family inet filter protect-re term tcp-established from source-port bgp
set firewall family inet filter protect-re term tcp-established from tcp-established
set firewall family inet filter protect-re term tcp-established then policer limit-10m
set firewall family inet filter protect-re term tcp-established then accept
set firewall family inet filter protect-re term default-deny then log
set firewall family inet filter protect-re term default-deny then syslog
```

```
set firewall family inet filter protect-re term default-deny then discard
set firewall policer limit-10m if-exceeding bandwidth-limit 10m
set firewall policer limit-10m if-exceeding burst-size-limit 625k
set firewall policer limit-10m then discard
set firewall policer limit-3m if-exceeding bandwidth-limit 3m
set firewall policer limit-3m if-exceeding burst-size-limit 15k
set firewall policer limit-3m then discard
set firewall policer limit-1m if-exceeding bandwidth-limit 1m
set firewall policer limit-1m if-exceeding burst-size-limit 15k
set firewall policer limit-1m then discard
set firewall policer limit-100k if-exceeding bandwidth-limit 100k
set firewall policer limit-100k if-exceeding burst-size-limit 15k
set firewall policer limit-100k then discard
set firewall policer limit-32k if-exceeding bandwidth-limit 32k
set firewall policer limit-32k if-exceeding burst-size-limit 15k
set firewall policer limit-32k then discard
```

次に参照すべき資料およびサイト

http://www.juniper.net/dayone

Day One シリーズは、PDF 形式で無料でダウンロードできます。また、一部のタイトルには、Junos の設定にそのまま組み込むことのできるコピーアンドペースト版が含まれています（ライブラリは、iTunes>Books から iPad および iPhone 用の eBook 形式のデータ、または Kindle Store から Kindle、Android、Blackberry、Mac、および PC 版のデータをそれぞれ入手できます。また、印刷版を Amazon または www.vervante.com で購入可能）。

http://www.juniper.net/books

完全な Juniper Networks Books ライブラリと、これらの書籍に関与している多くの書籍発行者を確認できます。本書で紹介した多くの書籍は、このジュニパーネットワークスのリソースで紹介されています。

http://forums.juniper.net/jnet

ジュニパーネットワークスがスポンサーとなっている J-Net コミュニケーションフォーラムは、ジュニパーネットワークスの製品、テクノロジー、およびソリューションに関する情報、ベストプラクティス、および疑問点を共有するための場です。この無料のフォーラムに参加するには、登録が必要です。

www.juniper.net/techpubs/

ジュニパーネットワークスのテクニカルマニュアルには、MPLS を含む、Junos のあらゆる部分を理解して設定する上で必要なすべての情報が含まれています。一連のマニュアルはあらゆる情報を網羅しているとともに、ジュニパーネットワークスのエンジニアリング担当者によって徹底的なレビューが行われています。

www.juniper.net/training/fasttrack

オンライン、オンサイト、または世界中のパートナートレーニングセンターで受講できるコースをご用意しています。JNTCP（ジュニパーネットワークス技術認定資格プログラム）では、ジュニパーネットワークス製品の設定およびトラブルシューティングに関する能力認定を行っています。短期間でエンタープライズ向けルーティング、スイッチング、またはセキュリティでの認定を受けるには、提供されているオンラインコース、受講ガイド、およびラボガイドをご利用ください。