セキュリティ強化のガイドライン

この付録では、次の項について説明します。

セキュリティ強化のガイドライン

システムのセキュリティ強化を検討する場合は、次のセキュリティ強化ガイドラインを考慮する必要があります。

- ホストプラットフォームのセキュリティ強化ガイドを参照してください。次に例を示します。
  - Red Hat 6：

    https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/pdf/Security_Guide/Red_Hat_Enterprise_Linux-6-Security_Guide-en-US.pdf
  - RHEL/CentOS 7.x：

    https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/pdf/Security_Guide/Red_Hat_Enterprise_Linux-7-Security_Guide-en-US.pdf

    https://www.cisecurity.org/benchmark/red_hat_linux/

    https://www.cisecurity.org/benchmark/centos_linux/
  - Windows Server 2012：

    https://www.cisecurity.org/wp-content/uploads/2017/04/CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0.pdf
  - NSA セキュリティ強化ガイド集：

    https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml

セキュリティ強化のガイドライン

注 上記のリンクは外部 Web サイトを参照しており、シスコはそれらを最新の状態に保つ責任を負いません。これらは参照のためだけに提供されています。コンテンツが古い場合やリンクにアクセスできない場合は、Web サイトの所有者に連絡して最新情報を入手してください。

- Cisco Prime Network Registrar で使用されていないポートを無効化またはブロックします。Cisco Prime Network Registrar のマニュアルには、ポートの使用法と、接続追跡などのファイアウォール項目の使用に関する問題の概要が記載されています。
  - Cisco Prime Network Registrar で使用されるポートのリストについては、『*Cisco Prime Network Registrar 10.1* アドミニストレーション ガイド』の「*Cisco Prime Network Registrar* サービスのデフォルトポート（*Default Ports for Cisco Prime Network Registrar Services*）」の項を参照してください。一部はデフォルトであり、インストール中または構成中に変更されている可能性があることに注意してください。
  - 接続トラッキング関連の問題については、『*Cisco Prime Network Registrar 10.1* アドミニストレーション ガイド』の「*DNS* パフォーマンスとファイアウォールの接続追跡（*DNS Performance and Firewall Connection Tracking*）」の項を参照してください。
- 非 root アカウントを使用して Cisco Prime Network Registrar をインストールし、セキュリティ機能を使用します（つまり、https で、セキュアな SCP セッションが必要です）。
- 製品ディレクトリ（主に /opt/nwreg2/* および /var/nwreg2/*）が適切にロックされていることを確認します。必要に応じて保護を調整する必要がある場合があることに注意してください（オフラインバックアップの実行やログの表示など）。
- DNS 固有の考慮事項には、次のようなものがあります。
  - DNS セキュリティ拡張機能（DNSSEC）の使用：

    DNSSECにより、データ出自の認証、データの完全性の確認、および認証による存在否定が可能になります。DNSSEC を使用すると、DNS プロトコルが特定のタイプの攻撃（特に DNS スプーフィング攻撃）の影響を受けにくくなります。DNSSEC は、デジタル署名を DNS データに追加することによって、悪意のある応答や偽造された応答を防ぎ、各 DNS 応答の完全性と真正性を検証できます。

    Cisco Prime Network Registrar 9.0 以前の権威 DNS サーバは、ゾーンの署名をサポートしていません。Cisco Prime Network Registrar 10.0 から権威 DNSSEC のサポートにより、DNS ゾーンに認証と完全性が付加されます。このサポートにより、Cisco Prime Network Registrar DNS サーバはセキュアゾーンと非セキュアゾーンの両方をサポートできます。詳細については、『*Cisco Prime Network Registrar 10.1* 権威およびキャッシング *DNS* ユーザ ガイド』の「権威 *DNSSEC* の管理（*Managing Authoritative DNSSEC*）」の項を参照してください。
  - ACL を使用したセキュアな DNS サーバアクティビティ：

- ゾーンクエリの制限：DNS サーバ上の *restrict-query-acl* 属性は、*restrict-query-acl* が明示的に設定されていないゾーンのデフォルト値として機能します。
- ゾーン転送要求の制限：*restrict-xfer-acl* 属性を使用して、既知のセカンダリサーバへのゾーン転送要求をフィルタリングします。
- DDNS 更新の制限：*update-acl* 属性を使用して、既知の DHCP サーバからの DDNS パケットをフィルタリングします。

- TSIG または GSS-TSIG を使用したセキュアゾーン転送および DNS 更新：

  セキュア モードでのゾーン転送は、HMAC MD5 ベースの TSIG と GSS-TSIG の両方をサポートします。オプションの TSIG キーまたは GSS-TSIG キー（の「トランザクション セキュリティ（*Transaction Security*）」の項または「*GSS-TSIG*」の項 *Cisco Prime Network Registrar 10.1 DHCP* ユーザ ガイドを参照）をマスターサーバアドレスに追加することができます。それには、形式 *addresskey* を使用してエントリをハイフンでつなぎます。エントリごとに、[IP キーの追加（Add IP Key]）] をクリックします。

  詳細については、『*Cisco Prime Network Registrar 10.1* 権威およびキャッシング *DNS* ユーザ ガイド』の「ゾーン分散の作成（*Creating a Zone Distribution*）」の項を参照してください。

- クエリ ID と送信元ポートをランダム化。
- DNS レートの制限：『*Cisco Prime Network Registrar 10.1* 権威およびキャッシング *DNS* ユーザ ガイド』の「キャッシングレート制限の管理（*Managing Caching Rate Limiting*）」の項を参照してください。
- 再帰サーバと権威サーバの役割分担。

- DHCP 固有の考慮事項には、次のようなものがあります。
  - 「外部」の送信元からの DHCPv4 トラフィックと DHCPv6 トラフィックがルータでブロックされ、有効なリレーエージェントだけが DHCP サーバにパケットを転送できることを確認します。
  - スイッチで DHCP ガードおよび同様のサービスを使用します。

    https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_1/nx-os/security/configuration/guide/sec_nx-os-cfg/sec_dhcpsnoop.htmlを参照してください

    https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-sy/dhcp-15-sy-book/ip6-dhcpv6-guard.pdfを参照してください
  - おしゃべりクライアントフィルタの使用：『*Cisco Prime Network Registrar 10.1 DHCP* ユーザ ガイド』の「拡張機能を使用したおしゃべりクライアントの防止（*Preventing Chatty Clients by Using an Extension*）」の項を参照してください。

- 通常、Active Directory（LDAP）および RADIUS ユーザに導入できるパスワードのルール（つまり、変更頻度、長さ、および難易度のチェック）として、外部ユーザ認証の使用を

セキュリティ強化のガイドライン

検討してください。『*Cisco Prime Network Registrar 10.1* アドミニストレーション ガイド』の「外部認証サーバ（*External Authentication Servers*）」の項を参照してください。