インフラストラクチャの復元力Cisco IOS XR

内容

はじめに

このドキュメントでは、Cisco IOS® XRの強化機能の1つである、安全でない機能と暗号を体系的にフェーズアウトする方法について説明します。

Cisco IOS XRインフラストラクチャの復元力

シスコデバイスのセキュリティポスチャを向上させるために、シスコはデフォルト設定を変更し、安全でない機能を廃止して最終的に削除し、新しいセキュリティ機能を導入しています。これらの変更は、ネットワークインフラストラクチャを強化し、脅威主体のアクティビティの可視性を向上させることを目的としています。

「Resilient Infrastructure」ページを参照してください。インフラストラクチャの強化、Cisco IOS XRソフトウェアの強化ガイド、機能の廃止プロセス、および機能の廃止と削除の詳細について説

明しています。推奨される代替案は、機能の削除と推奨される代替案について説明します。

Cisco IOS XRは、安全でない機能と暗号を段階的に廃止しています。これには、Cisco IOS XRでの設定コマンドと実行コマンドの両方が含まれます。

影響を受ける機能

- Telnet
- TFTP
- FTP
- HTTP
- SNMP v1/v2c
- SNMP v3（authPrivなし）
- IPソースルート
- TCP/UDPスモールサーバ
- 事前共有キー（タイプ7）とMD5を使用するTACACS+およびRADIUS
- SSH v1
- TLS 1.0/1.1
- NTPv2/3およびMD5
- GRPC、TLSなし、TLSv1.0/1.1
- TFTP/FTPでのcopy、utility、およびinstallを使用したexecコマンド

グループ化

コンフィギュレーションコマンドがありますが、実行コマンド（「copy」コマンドなど）もあります。

廃止されたコマンドは次のようにグループ化できます。

- SSHv1、Telnet（サーバおよびクライアント）、TFTP（クライアント）、FTP
- DSAホストキー、TACACS/RADIUSタイプ7、TLS 1.0/1.1
- その他：TCP/UDPスモールサーバ、IPソースルーティング（IPv4およびIPv6）

フェーズ

このプロジェクトは、通常の機能の廃止アプローチであるwarn -> restrict -> removeに従います。

- Cisco IOS XRリリース25.4.1での警告
- 制限フェーズ
- 機能の削除

警告フェーズ

警告とは何ですか。

1. CLI（コマンドラインインターフェイス）ヘルプ機能
2. syslog警告
3. yangモジュールの説明警告

設定された安全でないオプションに対して警告が表示されます。これらは、**30日**の頻度で表示されるsyslogメッセージです。

安全でない機能が使用されると、次のログ警告（レベル4または警告）が表示されます。

*%**INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN***：機能'<*feature-name*>'が使用されているか、設定されています。この機能はセキュリティで保護されていないことがわかっています。この機能の使用を中止することを検討してください。**<推奨事項>**

推奨されるのは、insecureオプションの代わりに何を使用するかです。

FTPの警告例：

%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN：機能「*FTP*」が使用されているか設定されている。この機能はセキュリティで保護されていないことがわかっています。この機能の使用を中止することを検討してください。*SFTP*の使用を推奨します。

使用されている単語または設定されている単語に注目してください。「utilized」は実行コマンドを指し、「configured」は設定コマンドを指します。

insecureオプション(レベル6またはinformational)が削除されると、警告メッセージが表示される場合があります。 例：

RP/0/RP0/CPU0:Oct 22 06:43:43.967 UTC: tacacsd[1155]: %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED ：安全でない機能「*TACACS+ over TCP with shared secret (default mode)*」設定が削除されました。

非推奨の安全でないオプションのリスト

これは、Cisco IOS XRリリースの警告フェーズで警告をトリガーする、安全でないオプションのリストです。

リストには、安全でないオプション、設定または実行コマンド、警告メッセージ、および関連するYangモデルが表示されます。

IPソースルーティング(RFC 791)

CLI を使う場合：

<#root>

```
RP/0/RP0/CPU0:Router(config)#
ip ?

  source-route       Process packets with source routing header options (This is deprecated sin

RP/0/RP0/CPU0:Router(config)#
ipv4 ?

  source-route     Process packets with source routing header options (This is deprecated since

RP/0/RP0/CPU0:Router(config)#
```

ipv6 ?

```
  source-route     Process packets with source routing header options (This is deprecated since
```

IPソースルート

ipv6ソースルート

ipv4ソースルート

warning

RP/0/RP0/CPU0:Oct 17 19:01:48.806 UTC:ipv4_ma[254]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN：機能「IPV4 SOURCE ROUTE」が使用または設定されています。この機能はセキュリティで保護されていないことがわかっています。この機能の使用を中止することを検討してください。セキュリティリスクがあるため、IPv4ソースルーティングは有効にしないでください。

RP/0/RP0/CPU0:Oct 17 19:01:48.806 UTC:ipv6_io[310]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN：機能「IPV6 SOURCE ROUTE」が使用または設定されています。この機能はセキュリティで保護されていないことがわかっています。この機能の使用を中止することを検討してください。セキュリティリスクがあるため、IPv6ソースルーティングは有効にしないでください。

Yangモデル

Cisco-IOS-XR-ipv4-ma-cfg

Cisco-IOS-XR-ipv6-io-cfg

Cisco-IOS-XR-um-ipv4-cfg

Cisco-IOS-XR-um-ipv6-cfg

推奨事項

insecureオプションを削除します。

完全な代替案はありません。送信元アドレスに基づいてネットワークを通過するトラフィックを制御したい顧客は、ポリシーベースルーティング(PBR)または、ルーティングの決定をエンドユーザに任せないで管理者が制御するその他の送信元ルーティングメカニズムを使用して、これを行うことができます。

SSH v1

CLIを使う場合：

```
<#root>
RP/0/RP0/CPU0:Router(config)#
```

```
ssh client ?

  v1                Set ssh client to use version 1. This is deprecated and will be removed in 2

RP/0/RP0/CPU0:Router(config)#
ssh server ?

  v1                          Cisco sshd protocol version 1. This is deprecated in 25.3.1.
```

sshクライアントv1

sshサーバv1

warning

RP/0/RP0/CPU0:11月19日15:20:42.814 UTC:ssh_conf_proxy[1210]: %SECURITY-SSHD_CONF_PRX-4-WARNING_GENERAL：バックアップサーバ、netconf-portコンフィギュレーション、ssh v1、sshポートはこのプラットフォームおよびリリースではサポートされておらず、有効になりません

Yangモデル

Cisco-IOS-XR-um-ssh-cfg

推奨事項

SSH v2を使用します。

設定SSHv2:セキュアシェルの実装

事前共有キー（タイプ7）を使用するTACACS+およびRADIUS

CLIを使う場合：

<#root>

```
RP/0/RP0/CPU0:Router(config)#
tacacs-server host 10.0.0.1

RP/0/RP0/CPU0:Router(config-tacacs-host)#
key ?

  clear      Config deprecated from 7.4.1. Use '0' instead.
  encrypted  Config deprecated from 7.4.1. Use '7' instead.

RP/0/RP0/CPU0:Router(config)#
tacacs-server key ?
```

```
  clear      Config deprecated from 7.4.1. Use '0' instead.
  encrypted  Config deprecated from 7.4.1. Use '7' instead.
```

tacacsサーバキー7 135445410615102B28252B203E270A

tacacs-server host 10.1.1.1ポート49

キー7 1513090F007B7977

radius-server host 10.0.0.1 auth-port 9999 acct-port 8888

キー7 1513090F007B7977

aaaサーバradius dynamic-author

クライアント10.10.10.2 vrfデフォルト

サーバキー7 05080F1C2243

RADIUSサーバキー7 130415110F

aaaグループサーバradius RAD

server-private 10.2.4.5 auth-port 12344 acct-port 12345

キー7 1304464058

warning

RP/0/RP0/CPU0:Oct 18 18:00:42.505 UTC:tacacsd[1155]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN ：機能「TACACS+共有秘密（タイプ7エンコーディング）」が使用または設定されます。この機能はセキュリティで保護されていないことがわかっています。この機能の使用を中止することを検討してください。代わりにType 6（AESベース）暗号化を使用します。

RP/0/RP0/CPU0:Oct 18 18:00:42.505 UTC:tacacsd[1155]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN：機能「TACACS+ over TCP with shared secret (default mode)」が使用または設定されている。この機能はセキュリティで保護されていないことがわかっています。この機能の使用を中止することを検討してください。セキュリティを強化するには、TACACS+ over TLS(Secure TACACS+)を使用します。

RP/0/RP0/CPU0:Oct 18 18:18:19.460 UTC:radiusd[1149]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN：機能「RADIUS共有秘密（タイプ7エンコーディング）」が使用または設定されています。この機能はセキュリティで保護されていないことがわかっています。この機能の使用を中止することを検討してください。代わりにType 6（AESベース）暗号化を使用します。

RP/0/RP0/CPU0:Oct 18 18:18:19.460 UTC:radiusd[1149]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN：機能「共有秘密（デフォルトモード）を使用したRADIUS over UDP」が使用または設定されています。この機能はセキュリティで保護されていないことがわかっています。この機能の使用を中止することを検討してください。セキュリティを強化するには、RADIUS over TLS(RadSec)またはDTLSを使用します。

Yangモデル

-

推奨事項

TACACS+またはRADIUS over TLS 1.3またはDTLSを使用します。クレデンシャルにはタイプ6を使用します。

TACACS+またはRADIUS over TLS 1.3またはDTLSの設定:AAAサービスの設定

TLS 1.0/1.1、弱い暗号は廃止

CLI を使う場合：

<#root>

RP/0/RP0/CPU0:Router(config)#

http client ssl version ?

```
  tls1.0  Force TLSv1.0 to be used for HTTPS requests, TLSv1.0 is deprecated from 25.3.1
  tls1.1  Force TLSv1.1 to be used for HTTPS requests, TLSv1.1 is deprecated from 25.3.1
```

RP/0/RP0/CPU0:Router(config)#

logging tls-server server-name min-version ?

```
  tls1.0  Set TLSv1.0 to be used as min version for syslog, TLSv1.0 is deprecated from 25.3.1
  tls1.1  Set TLSv1.1 to be used as min version for syslog, TLSv1.1 is deprecated from 25.3.1
```

RP/0/RP0/CPU0:Router(config)#

logging tls-server server-name max-version ?

```
  tls1.0  Set TLSv1.0 to be used as max version for syslog, TLSv1.0 is deprecated from 25.3.1
  tls1.1  Set TLSv1.1 to be used as max version for syslog, TLSv1.1 is deprecated from 25.3.1
```

logging tls-server server server-name <> max-version tls1.0|tls1.1

warning

-

Yangモデル

Cisco-IOS-XR-um-logging-cfg

Cisco-IOS-XR-um-http-client-cfg.yang（登録ユーザ専用）

推奨事項

TLS1.2またはTLS1.3を使用します。

設定のセキュアロギング：セキュアロギングの実装

Telnet（サーバおよびクライアント）

CLI を使う場合：

<#root>

```
RP/0/RP0/CPU0:Router(config)#
telnet ?

  ipv4  IPv4 configuration. (Telnet is deprecated since 25.4.1. SSH is recommended instead.)
  ipv6  IPv6 configuration. (Telnet is deprecated since 25.4.1. SSH is recommended instead.)
  vrf   VRF name for telnet server. (Telnet is deprecated since 25.4.1. SSH is recommended inste

RP/0/RP0/CPU0:Router(config)#
telnet ipv4 ?

  client  Telnet client configuration commands. (Telnet is deprecated since 25.4.1. SSH is recon
  server  Telnet server configuration commands. (Telnet is deprecated since 25.4.1. SSH is recon

RP/0/RP0/CPU0:Router(config)#
telnet ipv6 ?

  client  Telnet client configuration commands. (Telnet is deprecated since 25.4.1. SSH is recon
  server  Telnet server configuration commands. (Telnet is deprecated since 25.4.1. SSH is recon

RP/0/RP0/CPU0:Router(config)#
telnet vrf default ?

  ipv4  IPv4 configuration. (Telnet is deprecated since 25.4.1. SSH is recommended instead.)
  ipv6  IPv6 configuration. (Telnet is deprecated since 25.4.1. SSH is recommended instead.)

RP/0/RP0/CPU0:Router(config)#
telnet vrf test ?

  ipv4  IPv4 configuration. (Telnet is deprecated since 25.4.1. SSH is recommended instead.)
  ipv6  IPv6 configuration. (Telnet is deprecated since 25.4.1. SSH is recommended instead.)

RP/0/RP0/CPU0:Router#
telnet ?

  A.B.C.D          IPv4 address. (Telnet is deprecated since 25.4.1. SSH is recommended instead
  WORD             Hostname of the remote node. (Telnet is deprecated since 25.4.1. SSH is recon
```

```
  X:X::X           IPv6 address. (Telnet is deprecated since 25.4.1. SSH is recommended instead
  disconnect-char  telnet client disconnect char. (Telnet is deprecated since 25.4.1. SSH is re
  vrf              vrf table for the route lookup. (Telnet is deprecated since 25.4.1. SSH is r
```

telnet

telnet ipv4

telnet ipv6

Telnet VRF

warning

RP/0/RP0/CPU0:Jun 27 10:59:52.226 UTC: cinetd[145]: %IP-CINETD-4-TELNET_WARNING:Telnetのサポートは、25.4.1以降では廃止されています。代わりにSSHを使用してください。

Yangモデル

Cisco-IOS-XR-ipv4-telnet-cfg

Cisco-IOS-XR-ipv4-telnet-mgmt-cfg

Cisco-IOS-XR-um-telnet-cfg

推奨事項

SSHv2を使用します。

設定SSHv2:セキュアシェルの実装

TFTP（サーバおよびクライアント）

CLIを使う場合：

<#root>

```
RP/0/RP0/CPU0:Router(config)#
ip tftp ?

  client  TFTP client configuration commands (This is deprecated since 25.4.1)
```

TFTP

IP TFTP

TFTPクライアント

warning

RP/0/RP0/CPU0:Oct 17 19:03:29.475 UTC:tftp_fs[414]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN：機能「TFTPクライアント」が使用または設定されています。この機能はセキュリティで保護されていないことがわかっています。この機能の使用を中止することを検討してください。代わりにSFTPを使用します。

Yangモデル

-

推奨事項

sFTPまたはHTTPSを使用します。

設定sFTP:セキュアシェルの実装

TCP/UDPスモールサーバ

CLIを使う場合：

<#root>

```
RP/0/RP0/CPU0:Router(config)#
service ?

  ipv4                    Ipv4 small servers (This is deprecated)
  ipv6                    Ipv6 small servers (This is deprecated)

RP/0/RP0/CPU0:Router(config)#
service ipv4 ?

  tcp-small-servers  Enable small TCP servers (e.g., ECHO)(This is deprecated)
  udp-small-servers  Enable small UDP servers (e.g., ECHO)(This is deprecated)
```

サービスipv4

サービスipv6

warning

-

Yangモデル

Cisco-IOS-XR-ip-tcp-cfg

Cisco-IOS-XR-ip-udp-cfg

推奨事項

TCP/UDPスモールサーバを無効にします。

FTP

CLI を使う場合：

```
<#root>
RP/0/RP0/CPU0:Router(config)#
ftp ?

  client  FTP client config commands.This is deprecated since 25.4.1.SFTP is recommended instea
RP/0/RP0/CPU0:Router(config)#
ip ftp ?

  client  FTP client config commands.This is deprecated since 25.4.1.SFTP is recommended instea
```

IP FTP

FTP

warning

RP/0/RP0/CPU0:Oct 16 21:42:42.897 UTC:ftp_fs[1190]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN：機能「FTPクライアント」が使用または設定されています。この機能はセキュリティで保護されていないことがわかっています。この機能の使用を中止することを検討してください。代わりにSFTPを使用します。

Yangモデル

Cisco-IOS-XR-um-ftp-tftp-cfg

推奨事項

sFTPまたはHTTPSを使用します。

設定sFTP:セキュアシェルの実装

SNMP v1/2c

CLI を使う場合：

<#root>

```
RP/0/RP0/CPU0:Router(config)#
snmp-server ?

  chassis-id            String to uniquely identify this chassis
  community             Enable SNMP;  set community string and access privileges. (This is depr

RP/0/RP0/CPU0:Router(config)#
snmp-server ?

  community             Enable SNMP;  set community string and access privileges. (This is depr

RP/0/RP0/CPU0:Router(config)#
snmp-server user test test ?

  v1      user using the v1 security model (This is deprecated since 25.4.1)
  v2c     user using the v2c security model (This is deprecated since 25.4.1)
  v3      user using the v3 security model

RP/0/RP0/CPU0:Router(config)#
snmp-server host 10.0.0.1 version ?

  1   Use 1 for SNMPv1. (This is deprecated since 25.4.1)
  2c  Use 2c for SNMPv2c. (This is deprecated since 25.4.1)
  3   Use 3 for SNMPv3

RP/0/RP0/CPU0:Router(config)#
snmp-server group test ?

  v1   group using the v1 security model (This is deprecated since 25.4.1)
  v2c  group using the v2c security model (This is deprecated since 25.4.1)
  v3   group using the User Security Model (SNMPv3)

RP/0/RP0/CPU0:Router(config)#
snmp-server ?

  community             Enable SNMP;  set community string and access privileges. (This is depr
  community-map         Community Mapping as per RFC-2576. (This is deprecated since 25.4.1)

RP/0/RP0/CPU0:Router(config)#
snmp-server user user1 group1 ?

  v1      user using the v1 security model (This is deprecated since 25.4.1)
  v2c     user using the v2c security model (This is deprecated since 25.4.1)

RP/0/RP0/CPU0:Router(config)#
```

```
snmp-server user user1 group1 v3 auth md5 test priv ?


  3des    Use 168 bit 3DES algorithm for encryption (This is deprecated since 25.4.1)
  des56   Use 56 bit DES algorithm for encryption (This is deprecated since 25.4.1)

RP/0/RP0/CPU0:Router(config)#

snmp ?


  community             Enable SNMP;  set community string and access privileges. (This is depr

RP/0/RP0/CPU0:Router(config)#

snmp user user test ?


  remote  Specify a remote SNMP entity to which the user belongs
  v1      user using the v1 security model (This is deprecated since 25.4.1)
  v2c     user using the v2c security model (This is deprecated since 25.4.1)

RP/0/RP0/CPU0:Router(config)#

snmp-server user user1 group1 v3 auth ?


  md5      Use HMAC MD5 algorithm for authentication (This is deprecated since 25.4.1)
  sha      Use HMAC SHA algorithm for authentication (This is deprecated since 25.4.1)

RP/0/RP0/CPU0:Router(config)#

snmp user user1 group1 v3 auth ?


  md5      Use HMAC MD5 algorithm for authentication (This is deprecated since 25.4.1)
  sha      Use HMAC SHA algorithm for authentication (This is deprecated since 25.4.1)

RP/0/RP0/CPU0:Router(config)#

snmp user user1 group1 v3 auth md5 test priv ?


  3des    Use 168 bit 3DES algorithm for encryption (This is deprecated since 25.4.1)
  des56   Use 56 bit DES algorithm for encryption (This is deprecated since 25.4.1)

RP/0/RP0/CPU0:Router(config)#

snmp host 10.1.1.1 version ?


  1   Use 1 for SNMPv1. (This is deprecated since 25.4.1)
  2c  Use 2c for SNMPv2c. (This is deprecated since 25.4.1)

RP/0/RP0/CPU0:Router(config)#

snmp-server host 10.1.1.1 version ?


  1   Use 1 for SNMPv1. (This is deprecated since 25.4.1)
  2c  Use 2c for SNMPv2c. (This is deprecated since 25.4.1)

RP/0/RP0/CPU0:Router(config)#

snmp ?
```

```
  community-map          Community Mapping as per RFC-2576. (This is deprecated since 25.4.1)
```

SNMPサーバコミュニティ

snmp-server user <> <> v1 | v2c

snmp-server user <> <> v3 auth md5 | sha

snmp-server user <> <> v3 auth md5|sha <> priv 3des|des56

snmp-server host <> version 1|v2c

snmp-server group <> v1|v2c

SNMPサーバコミュニティマップ

snmp コミュニティ

snmpユーザー<> <> v1|v2c

snmpユーザー<> <> v3 auth md5|sha

snmpユーザー<> <> v3 auth md5/sha <> priv 3des|des56

snmp host <> version 1|v2c

snmpグループ<> v1|v2c

SNMPコミュニティマップ

warning

-

Yangモデル

Cisco-IOS-XR-um-snmp-server-cfg

推奨事項

SNMPv3と認証および暗号化(authPriv)を使用します。

認証およびauthPrivを使用したSNMPv3の設定:簡易ネットワーク管理プロトコルの設定

NTPバージョン2および3とMD5認証

CLIを使う場合：

<#root>

```
RP/0/RP0/CPU0:Router(config)#
ntp server 10.1.1.1 version ?

  <2-4>  NTP version number. Values 2-3 are DEPRECATED from 25.4.1 onwards; use 4 instead.

RP/0/RP0/CPU0:Router(config)#
ntp peer 10.1.1.1 version ?

  <2-4>  NTP version number. Values 2-3 are DEPRECATED from 25.4.1 onwards; use 4 instead.

RP/0/RP0/CPU0:Router(config)#
ntp server admin-plane version ?

  <1-4>  NTP version number. Values 1-3 are DEPRECATED from 25.4.1 onwards; use 4 instead.

RP/0/RP0/CPU0:Router(config)#
ntp interface gigabitEthernet 0/0/0/0 broadcast version ?

  <2-4>  NTP version number. Values 2-3 are DEPRECATED from 25.4.1 onwards; use 4 instead.

RP/0/RP0/CPU0:Router(config)#
ntp interface gigabitEthernet 0/0/0/0 multicast version ?

  <2-4>  NTP version number. Values 2-3 are DEPRECATED from 25.4.1 onwards; use 4 instead.

RP/0/RP0/CPU0:Router(config)#
ntp authentication-key 1 md5 clear 1234
```

ntpサーバ<>バージョン2|3

ntp peer <> version 2/3

ntpサーバ管理プレーンバージョン1/2/3

ntpインターフェイス<>ブロードキャストバージョン2|3

ntpインターフェイス<>マルチキャストバージョン2|3

ntp authentication-key <> md5 <> <>

warning

RP/0/RP0/CPU0:11月25日16:09:15.422 UTC: ntpd[159]: %IP-IP_NTP-5-CONFIG_NOT_RECOMMENDED:NTPv2およびNTPv3は、25.4.1以降では廃止されています。NTPv4を使用してください。

RP/0/RP0/CPU0:11月25日16:09:15.422 UTC:ntpd[159]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN：機能「認証なしのNTP」が使用または設定されています。この機能はセキュリティで保護されていないことがわかっています。この機能の使用を中止することを検討してください。

Yangモデル

Cisco-IOS-XR-um-ntp-cfg.yang（オプション）

推奨事項

NTPバージョン4またはMD5以外の認証を使用します。

NTPの設定：Network Time Protocolの設定

GRPC

CLIを使う場合：

<#root>

```
RP/0/RP0/CPU0:Router(config)#
```

grpc ?

```
  aaa                          AAA authorization and authentication for gRPC
  address-family               DEPRECATED. Removing in 26.3.1: Address family identifier type
  apply-group                  Apply configuration from a group
  certificate                  DEPRECATED. Removing in 26.3.1: gRPC server certificate
  certificate-authentication   DEPRECATED. Removing in 26.3.1: Enables Certificate based Authentication
  certificate-id               DEPRECATED. Removing in 26.3.1: Active Certificate
  default-server-disable       Configuration to disable the default gRPC server
  dscp                         DEPRECATED. Removing in 26.3.1: QoS marking DSCP to be set on transmitted
  exclude-group                Exclude apply-group configuration from a group
  gnmi                         gNMI service configuration
  gnpsi                        gnpsi configuration
  gnsi                         gNSI
  gribi                        gRIBI service configuration
  keepalive                    DEPRECATED. Removing in 26.3.1: Server keepalive time and timeout
  listen-addresses             DEPRECATED. Removing in 26.3.1: gRPC server listening addresses
  local-connection             DEPRECATED. Removing in 26.3.1: Enable gRPC server over Unix socket
  max-concurrent-streams       gRPC server maximum concurrent streams per connection
  max-request-per-user         Maximum concurrent requests per user
  max-request-total            Maximum concurrent requests in total
  max-streams                  Maximum number of streaming gRPCs (Default: 32)
  max-streams-per-user         Maximum number of streaming gRPCs per user (Default: 32)
  memory                       EMSd-Go soft memory limit in MB
  min-keepalive-interval       DEPRECATED. Removing in 26.3.1: Minimum client keepalive interval
  name                         DEPRECATED. Removing in 26.3.1: gRPC server name
  no-tls                       DEPRECATED. Removing in 26.3.1: No TLS
  p4rt                         p4 runtime configuration
  port                         DEPRECATED. Removing in 26.3.1: Server listening port
  remote-connection            DEPRECATED. Removing in 26.3.1: Configuration to toggle TCP support on th
  segment-routing              gRPC segment-routing configuration
```

```
  server                    gRPC server configuration
  service-layer             grpc service layer configuration
  tls-cipher                DEPRECATED. Removing in 26.3.1: gRPC TLS 1.0-1.2 cipher suites
  tls-max-version           DEPRECATED. Removing in 26.3.1: gRPC maximum TLS version
  tls-min-version           DEPRECATED. Removing in 26.3.1: gRPC minimum TLS version
  tls-mutual                DEPRECATED. Removing in 26.3.1: Mutual Authentication
  tls-trustpoint            DEPRECATED. Removing in 26.3.1: Configure trustpoint
  tlsV1-disable             Disable support for TLS version 1.0
                            tlsv1-disable CLI is deprecated.
                            Use tls-min-version CLI to set minimum TLS version.
  ttl                       DEPRECATED. Removing in 26.3.1: gRPC packets TTL value
  tunnel                    DEPRECATED. Removing in 26.3.1: grpc tunnel service
  vrf                       DEPRECATED. Removing in 26.3.1: Server vrf
  <cr>
```

grpc非tls
grpc tls-max|最小 – バージョン1.0|1.1
grpc tls-ciper default|enable|disable（TLS 1.2では、3つの設定を評価した後で安全でない暗号スイートが使用された場合、安全ではありません）

warning

RP/0/RP0/CPU0:11月29日19:38:30.833 UTC:emsd[1122]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN：機能「gRPC insecure configuration」が使用または設定されています。この機能は安全でないことが分かっているため非推奨です。将来のリリースでは削除される予定です。 server=DEFAULT（TLSバージョンは1.2より古く、安全でない暗号スイートが設定されています）

Yangモデル

Cisco-IOS-XR-um-grpc-cfg.yang（登録ユーザ専用）

Cisco-IOS-XR-man-ems-oper.yang（登録ユーザ専用）

Cisco-IOS-XR-man-ems-grpc-tls-credentials-rotate-act.yang

Cisco-IOS-XR-man-ems-cfg.yang（登録ユーザ専用）

推奨事項

強力な暗号を使用して、TLS 1.2以降（TLS 1.3が望ましい）を使用します。

設定：gRPCプロトコルを使用してデータモデルのネットワーク操作を定義する

安全でない実行コマンドのリスト

Copyコマンド

CLIを使う場合：

<#root>

RP/0/RP0/CPU0:Router#

copy ?

```
  ftp:            Copy from ftp: file system (Deprecated since 25.4.1)
  tftp:           Copy from tftp: file system (Deprecated since 25.4.1)
```

copy <src as tftp/ftp> <dst as tftp/ftp>

copy running-config ?」というエラーメッセージが

warning

RP/0/RP0/CPU0:11月26日15:05:57.666 UTC:filesys_cli[66940]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN：機能「copy ftp」が使用されたか設定されています。この機能は安全でないことが判明しているため廃止されます。将来のリリースで削除される予定です。代わりにSFTPまたはSCPを使用してください。

RP/0/RP0/CPU0:11月26日15:09:06.181 UTC:filesys_cli[67445]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN：機能「copy tftp」が使用されたか、設定されています。この機能は安全でないことが判明しているため廃止されます。将来のリリースで削除される予定です。代わりにSFTPまたはSCPを使用してください。

Yangモデル

-

推奨事項

sFTPまたはSCPを使用します。

設定：セキュアシェルの実装

インストールコマンド

CLIを使う場合：

```
install source

install add source

install replace
```

"

warning

-

Yangモデル

Cisco-IOS-XR-sysadmin-instmgr-oper.yang

推奨事項

sFTPまたはSCPを使用します。

設定：セキュアシェルの実装

ユーティリティコマンド

CLI を使う場合：

```
utility mv source
```

Yangモデル

Yangモデルの変更点が多すぎるため、それらをすべて一覧に表示できません。

これは、ソースルーティングの削除に関するYang *modelCisco-IOS-XR-ipv4-ma-cfg.yanger*のコメントの例です。

```
revision "2025-09-01" {
    description
      "Deprecated IPv4 Source Route Configuration.

leaf source-route {
      type boolean;
      default "true";
      status deprecated;
      description
        "The flag for enabling whether to process packets
        with source routing header options (This is
        deprecated since 25.4.1)";
```

これは、FTPおよびTFTPを削除するためのYang *modelCisco-IOS-XR-um-ftp-tftp-cfg*.yangのコメントの例です。

```
revision 2025-08-29 {
    description
      "TFTP config commands are deprecated.
       2025-08-20
         FTP config commands are deprecated.";

container ftp {
    status deprecated;
    description
      "Global FTP configuration commands.This is deprecated since 25.4.1.
       SFTP is recommended instead.";
    container client {
      status deprecated;
      description
        "FTP client configuration commands.This is deprecated since 25.4.1.
         SFTP is recommended instead.";

       container ipv4 {
          status "deprecated";
          description
            "Ipv4 (This is deprecated since 25.4.1)";

container ipv6 {
          status "deprecated";
          description
            "Ipv6  (This is deprecated since 25.4.1)";

container tftp-fs {
    status deprecated;
    description
      "Global TFTP configuration commands (This is deprecated since 25.4.1)";
    container client {
      status deprecated;
      description
        "TFTP client configuration commands (This is deprecated since 25.4.1)";
      container vrfs {
        status "deprecated";
        description
          "VRF name for TFTP service (This is deprecated since 25.4.1)";
```

IOS XR強化ガイド

このガイド『Cisco IOS XRソフトウェア強化ガイド』は、ネットワーク管理者とセキュリティ担当者が、Cisco IOS XRベースのルータを保護してネットワークの全体的なセキュリティポスチャを向上させるのに役立ちます。

このドキュメントは、ネットワークデバイスの機能を分類する3つのプレーンを中心に構成されています。

ルータの3つの機能プレーンとは、管理プレーン、コントロールプレーン、およびデータプレーンです。それぞれ異なる機能を提供するため、保護する必要があります。

- **管理プレーン**：管理プレーンには、Cisco IOS XRデバイスおよびネットワークのプロビジョニング、メンテナンス

、およびモニタリング機能をサポートするすべてのトラフィックの論理グループが含まれます。このグループのトラフィックには、Secure Shell(SSH)、Secure Copy Protocol(SCP)、Simple Network Management Protocol(SNMP)、Syslog、TACACS+、RADIUS、DNS、NetFlow、およびCisco Discovery Protocolが含まれます。管理プレーントラフィックは常にローカルのCisco IOS XRデバイス宛てです。

- コントロールプレーン：コントロールプレーンには、ネットワークとそのインターフェイスの状態を作成および維持するために使用される、すべてのルーティング、シグナリング、リンクステート、およびその他のコントロールプロトコルの論理グループが含まれます。これには、Border Gateway Protocol(BGP)、Open Shortest Path First(OSPF)、Label Distribution Protocol(LDP)、Intermediate System to Intermediate System(IS-IS)、Network Time Protocol(NTP)、Address Resolution Protocol(ARP)、およびレイヤ2キープアライブが含まれます。コントロールプレーントラフィックは常にローカルCisco IOS XRデバイス宛てに送信されます。
- データプレーン：データプレーンには、ホスト、クライアント、サーバ、およびアプリケーションによって生成された「お客様」のアプリケーショントラフィックの論理グループが含まれています。トラフィックの送信元および宛先は、ネットワークでサポートされている他の同様のデバイスです。データプレーン機能には、IPソースルーティング、IPダイレクトブロードキャスト、ICMPリダイレクト、ICMP到達不能、プロキシARPなどがあります。データプレーントラフィックは主に高速パスで転送され、ローカルのCisco IOS XRデバイス宛てになることはありません。

Config Resilient Infrastructureテスター

ルータの設定をテストし、安全であるかどうかを確認できます。このツールは、IOS XR:Cisco Config Resilient Infrastructure Testerなどの複数のオペレーティングシステムで機能します。

質問と回答

1. コマンドを2回設定した場合、または同じコマンドを再度設定した場合、同じsyslog警告メッセージが再度表示されますか。

A：いいえ。

2. 2つの異なる機能に対する2つの設定コマンドが同じコミットで実行されると、2つのsyslog警告が発生しますか。

A：はい。

例：

RP/0/RP0/CPU0:Oct 17 19:01:48.806 UTC:ipv6_io[310]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN：機能「IPV6 SOURCE ROUTE」が使用または設定されています。この機能はセキュリティで保護されていないことがわかっています。この機能の使用を中止することを検討してください。セキュリティリスクがあるため、IPv6ソースルーティングは有効にしないでください。

RP/0/RP0/CPU0:Oct 17 19:01:48.806 UTC:ipv4_ma[254]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN：機能「IPV4 SOURCE ROUTE」が使用または設定されています。この機能はセキュリティで保護されていないことがわかっています。この機能の使用を中止することを検討してください。セキュリティリスクがあるため、IPv4ソースルーティングは有効にしないでください。

3. 新しいコミットで新しく安全でない設定コマンドを実行すると、新しい警告が表示されますか。

A：はい。

4. 安全でない機能が設定から削除されたとき、syslog警告はありますか。

A：はい

例:

RP/0/RP0/CPU0:Oct 18 08:16:24.410 UTC: ssh_conf_proxy[1210]: %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED ：安全でない機能「SSH host-key DSA algorithm」の設定が削除されました。

RP/0/RP0/CPU0:Oct 22 06:37:21.960 UTC:tacacsd[1155]: %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED：安全でない機能「TACACS+共有秘密（タイプ7エンコーディング）」の設定を削除。

RP/0/RP0/CPU0:Oct 22 06:42:21.805 UTC:tacacsd[1155]: %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED：安全でない機能「共有秘密（デフォルトモード）を使用したTCP上のTACACS+」の設定を削除。

5. ルータ上でTelnetが使用できることが表示されません。

A：オプションのTelnet RPMをロードした場合にのみTelnetを使用できるIOS XR7/LNTを実行することができます。

6. XR7/LNTでは、コマンド「install source」に対してsFTPまたはSCPオプションは表示されません。

A：現時点では、XR7/LNTは「install source」コマンドに対してsFTPまたはSCPをサポートしていません。

7. 変更はIOS XR eXRとIOS XR7/LNTに等しく適用されますか。

A：はい。

8. ルータがIOS XR eXRまたはIOS XR XR7/LNTを実行しているかどうかを確認する方法

A:「show version」を使用して「LNT」を探します。8000ルータといくつかのNCS540バリアントでは、IOS XR7/LNTが稼働しています。

例：

<#root>

```
RP/0/RP0/CPU0:Router#
```

show version

Cisco IOS XR Software, Version 25.2.2

LNT

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。