

# Cisco 8000およびNCS5500プラットフォームでの新しいパスワード回復手順

## 内容

[概要](#)

[背景説明](#)

[問題](#)

[解決方法](#)

[新しいパスワード回復手順](#)

[要約](#)

## 概要

このドキュメントでは、Cisco 8000およびNCS5500プラットフォーム用のCisco IOS®-XRの新しいパスワード回復プロセスについて説明します。

## 背景説明

ユーザがXR7 LNTプラットフォーム(Cisco 8000、NCS-540L)またはeXRプラットフォーム ( ASR9K 64ビット、NCS5K、NCS5500、NCS 540、NCS )ですべてのユーザのルートパスワードを忘場合560)では、ユーザに対してルータがアクセス不能になります。ユーザ名とパスワードが正しく組み合わせられていないと、ログインは不可能になります。現在、このようなルータのパスワード回復は、USBブート方式または外部サーバからのiPXEブートを使用したルータの再イメージ化によってのみ可能です。ルータの再イメージ化には、ルータソフトウェアを再インストールし、デバイス設定をロードする必要があります。ソフトウェアの再インストールは、時間のかかるプロセスです。

Cisco 8000シリーズプラットフォーム用の7.3.16リリースとNCS5500シリーズプラットフォーム用の7.3.3を開始し、ルータの再イメージ化を行わずに新しいパスワード回復方法を開発しました。このようなパスワード回復方法では、ソフトウェアを再インストールする必要がないため、時間が節約され、パスワードのリセット後にルータにアクセスできます。この新しいパスワード回復方法は、古いユーザ情報とユーザのランタイムデータがパスワード回復処理の開始前に消去されるため、セキュリティ標準に準拠しています。

## 問題

現在、XR7 LNTプラットフォーム(Cisco 8000、NCS-540L)またはeXRプラットフォーム ( ASR9K 64ビット、NCS5K、NCS5500、NCS 540、NCS 560 )でのパスワード回復はできません。パスワードをリセットする唯一の方法は、USBブート方式または外部サーバからのiPXEブートを使用してルータを再イメージ化することです。ルータのソフトウェアを再インストールしてデバイス設定をロードするため、これは時間のかかるプロセスです。

Cisco XR7およびeXRプラットフォームのパスワード回復には、より高速で安全な方法が必要です。

# 解決方法

Cisco 8000シリーズプラットフォーム用の7.3.16リリースとNCS5500シリーズプラットフォーム用の7.3.3を開始し、ルータの再イメージ化を行わずに新しいパスワード回復方法を開発しました。ルートプロセッサ(RP)ブートアップ画面のGrand Unified Bootloader(GRUB)メニューに、パスワード回復手順のために明示的に作成された新しいオプション「IOS-XR-Recovery」が追加されます。ルータ設定では、新しいパスワード回復機能を有効にするために、新しいコマンドsystem recoveryが作成されます。これは現在オプションの機能であり、デフォルトでは有効になっていません。

## 警告:

- RP BIOSブートアップGRUB画面メニューオプションIOS-XR-recoveryは、ルータ設定で設定されたコマンドシステム回復または未設定に関係なく表示されます。ルータ設定にsystem recoveryコマンドが存在せず、bios GRUB画面メニューオプションIOS-XR-recoveryを選択して新しいパスワード回復方法を試みた場合は、ルータはパスワード回復処理を中止し、古い設定でブートします。したがって、パスワード回復方法が機能するようにルータでsystem recoveryコマンドを設定する必要があります。
- パスワード回復機能は、デフォルトでは無効になっています。
- パスワード回復機能は、コマンドラインインターフェイス(CLI)を使用して明示的に有効にする必要があります。RP/0/RP0/CPU0:HOSTNAME(config)#system recovery。
- ルータがパスワード回復手順を実行すると、ルータのブートアップ後にsystem recoveryコマンドが無効になり、パスワード回復手順の一部としてすべてのルータ設定が消去されます。デバイス設定に含まれていない場合は、デバイス設定を再度ロードし、system recoveryコマンドを設定する必要があります。
- ルータ設定の削除とは別に、ユーザが作成したすべてのファイル、show tech files、dumper filesは、パスワード回復中のクリーンアップ手順の一環として、disk0とハードディスクの両方から消去されます。
- この機能は現在、Cisco 8000、7.3.3以降のNCS5500、および他のXR7 LNTおよびeXRプラットフォームで7.3.16以降でサポートされており、今後のリリースでこの機能を使用できるようになります。
- 両方のRPカードがシャーシに取り付けられているプラットフォームでは、所定の手順を使用します。両方のRPカードをBIOS GRUBメニューに表示します。次に、各RPカードでパスワード回復手順を1つずつ実行する必要があります。これはデュアルRPプラットフォームでは必須のステップであり、そうでない場合は、設定とファイルクリーンアップの不一致が発生します。

## 新しいパスワード回復手順

前提条件：新しいパスワード回復機能は、CLIがデバイス設定の一部である場合にのみ機能します。CLIが設定されていない場合、設定CLIが欠落しているため、新しいパスワード回復メカニズムは機能しません。

パスワード回復機能を有効にする：

```
RP/0/RP0/CPU0:HOSTNAME(config)#system recovery
```

パスワード回復機能を無効にする :

```
RP/0/RP0/CPU0:HOSTNAME(config)#no system recovery
```

パスワード回復手順は、RPコンソールからのみ実行する必要があります。

ステップ1:RPカードをbios GRUBメニューに表示します。両方のRPカードがシャーシに取り付けられているプラットフォームでは、パスワード回復手順を開始する前に、両方のRPカードをBIOS GRUBメニューにダウンさせる必要があります。これは必須ステップです。これは、デバイスの電源を再投入して、両方のRPコンソールのESCキーを押してbios GRUBメニューに入るか、各RPを1つずつ物理的に取り付け直してから、RPコンソールのESCキーを押してbiosメニューに入ります。

RP0およびRP1カード :

```
Press Esc for boot options

Cisco 8000(R) Series BIOS Ver 1.22 Primary
Intel(R) Xeon(R) CPU D-1530 @ 2.40GHz
Board Type 0x220 PID 8812 Serial FOX2422PC5N
X86FPGA 1.5.0 TamLib 3.04.12
```

RP0およびRP1カード :

```
Press Esc for boot options
                                GNU GRUB  version 2.02 (LOCKED)

C+-----+-----+-----+-----+-----+-----+-----+-----+-----+
I| *IOS-XR-latest
B|  IOS-XR-fallback
X|  IOS-XR-recovery
|
W|
|
V|
(|
|
+-----+-----+-----+-----+-----+-----+-----+-----+-----+

Use the ^ and v keys to select which entry is highlighted.
Press enter to boot the selected OS.
```

ステップ2:RP0カードコンソールで、GRUBメニューからIOS-XR-recoveryオプションを選択し、Enterキーを押します。

RP0カード :

```
Press Esc for boot options
GNU GRUB version 2.02 (LOCKED)

C+-----+
I| IOS-XR-latest
B| IOS-XR-fallback
X| *IOS-XR-recovery
V|
(|
+-----+

Use the ^ and v keys to select which entry is highlighted.
Press enter to boot the selected OS.
```

ステップ3:GRUBメニューから**IOS-XR-recovery**オプションを選択して、RP0カードコンソールに「Initiating IOS-XR System Recovery...」というメッセージが表示されたら、RP1カードコンソールで**Enter**を押します。RP0カードが「Enter root-system username:」プロンプトに到達するまで待つことはできません。そうしないと、RP1カードが自動リロードされ、BIOS GRUBメニューが終了します。RP0カードはアクティブとして起動し、RP1カードはリカバリプロセス後にスタンバイカードとして起動します。

RP0カード :

```
Execute: cryptsetup luksOpen /dev/main-xr-vg/install-data-encrypted_in encrypted -d '-'
#####
# Initiating IOS-XR System Recovery... #
# This will erase all user & system configuration! #
# *** System will reboot upon completion *** #
#####

Checking if system recovery is enabled
WARNING: Failed to connect to lvmtool. Falling back to device scanning.
System Recovery enabled by user
Start System Recovery
```

RP1カード :

```
Press Esc for boot options
GNU GRUB version 2.02 (LOCKED)

C+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
I| IOS-XR-latest
B| IOS-XR-fallback
X| *IOS-XR-recovery
V|
(
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

Use the ^ and v keys to select which entry is highlighted.
Press enter to boot the selected OS.
```

ステップ4:RP0カードで、新しいルートユーザとパスワードを作成します。新しいルートユーザ名とパスワードを使用して、デバイスへのログインを試みます。

RP0カード :

```
RP/0/RP0/CPU0:Jul 8 04:52:06.169 CEST: ifmgr[361]: %PKT_INFRA-LINK-3-UPDOWN : Interface MgmtEth0/RP0/CPU0/0, changed state to Down
RP/0/RP0/CPU0:Jul 8 04:52:06.170 CEST: ifmgr[361]: %PKT_INFRA-LINK-3-UPDOWN : Interface MgmtEth0/RP0/CPU0/0, changed state to Up
!!!!!!!!!!!!!!!!!!!!!! NO root-system username is configured. Need to configure root-system username. !!!!!!!!!!!!!!!!!!!!!!!

--- Administrative User Dialog ---

Enter root-system username: █
```

ステップ5 : この時点で、パスワード回復手順が完了します。

これで、ルータは空の設定で起動し、手順4で作成したルートユーザ名パスワードで起動します。通常のルータ設定に進むか、バックアップファイルから設定をロードします (パスワード回復手順の一部としてdisk0またはハードディスクに保存された設定は失われます)。RP0とRP1の両方のRP0コンソールログに、パスワード回復を確認する確認手順として、また、両方のRPのすべての古いユーザデータのクリーンアップが正常に完了したことを確認するために、このメッセージが表示されることを確認します。そうでない場合は、RP0コンソールログに次のメッセージが表示されるまで、「Prerequisite Step」と「Step 1. ~ 4.」を繰り返します。スタンバイRPに対してこのメッセージが表示されない場合は、スタンバイRPに対してのみ、前提条件のステップとステップ1. ~ 4.を繰り返す必要があります。

```
RP/0/RP0/CPU0:Jul 8 06:13:24.551 CEST: sys_rec[1188]: %SECURITY-SYSTEM_RECOVERY-1-REPORT :
System Recovery at 06:10:19 CEST Thu Jul 08 2021 was successful
```

```
RP/0/RP1/CPU0:Jul 8 06:15:13.967 CEST: sys_rec[1188]: %SECURITY-SYSTEM_RECOVERY-1-REPORT :
System Recovery at 06:11:23 CEST Thu Jul 08 2021 was successful
```

## 要約

この新しいパスワード回復手順を使用すると、Cisco 8000シリーズプラットフォームおよびNCS5500シリーズプラットフォームで失われたパスワードを10分以内に安全にリセットできます。