

## GLBB GS3SFP-232-GE ユーザーガイド

ファームウェアバージョン 2.0

2026年4月1日

## 目次

<b>1</b>	<b>はじめに</b>	<b>3</b>
<b>2</b>	<b>製品仕様</b>	<b>5</b>
<b>3</b>	<b>設置手順</b>	<b>7</b>
	デバイスの開封.....	7
	GS3をネットワークに接続する.....	7
	GS3への接続.....	7
	IPアドレスの設定.....	7
	マルチキャストによるリンクローカルIPv6アドレスの特定.....	8
<b>4</b>	<b>GS3へのログイン</b>	<b>9</b>
	SSH アクセス.....	9
<b>5</b>	<b>使用方法</b>	<b>10</b>
	メニューの操作と表示.....	10
<b>6</b>	<b>シリアルコマンド</b>	<b>11</b>
	シリアル接続.....	11
	シリアル表示.....	11
	シリアル遅延-CRLF <0000>.....	11
	シリアルボーレート.....	11
	シリアルデータサイズ <ビット>.....	12
	シリアルパリティ <なし/奇数/偶数>.....	12
	シリアルストップビット <ビット数>.....	12
	シリアル終了キー.....	13
<b>7</b>	<b>GS3をシリアルコンソールに接続する</b>	<b>14</b>
<b>8</b>	<b>ネットワークコマンド</b>	<b>15</b>
	network show.....	15
	network ipv4 <manual/dhcp/disable>.....	15
	network ipv6 <auto/random/manual/linklocal/disable>.....	16
	network port cli <ポート>.....	17
	network reverse-ssh <ポート>.....	17
	network timeout <timeout>.....	17
	network hostname <ホスト名>.....	18
	ネットワーク NTP <リモート NTP アドレス>.....	18
	network syslog <リモート-syslog-アドレス>.....	18
<b>9</b>	<b>セキュリティ管理コマンド</b>	<b>19</b>
	ユーザー一覧.....	19
	user add <ユーザー名> <パスワード> <管理者/一般>.....	19
	ユーザー変更 <ユーザー名> <新しいパスワード>.....	19
	ユーザー削除 <ユーザー名>.....	19

user publickey <ユーザー名> .....	19
セッション一覧 .....	20
セッション終了 <セッションID> .....	20
ssh config <kex/ホストキー> .....	20
ssh publickeyonly <有効/無効> .....	21
acl set <ipv4/ipv6> <ip> .....	21
acl del <ipv4/ipv6> <リスト番号> .....	21
acl list <ipv4/ipv6> .....	22
<b>10 ファームウェアコマンド</b> .....	<b>23</b>
ファームウェアのバージョン .....	23
ファームウェアのアップグレード .....	23
ファームウェアサーバー <set/get> .....	23
リセット <デフォルト/再起動> .....	24
<b>11 シリアル・フレーズ・ロケータ</b> .....	<b>25</b>
キーフレーズ追加 <キーフレーズ> .....	25
キーフレーズ一覧 .....	25
keyphrase del <リスト番号> .....	25
<b>SSH セキュリティ監査の出力</b> .....	<b>26</b>
<b>B 導入例：ウォームリロードの検出</b> .....	<b>27</b>
<b>C 導入例：ホストの復旧の検出</b> .....	<b>28</b>
<b>D ファームウェアのリリースとSHA256ハッシュ値</b> .....	<b>29</b>

# 1 はじめに

GLBB Secure Smart Serial (GS3) は、シリアルデバイス (TIA-232/RS-232) への安全なリモートアクセス専用に設計された、小型フォームファクタのコンソールサーバーです。GS3 は、ポスト量子鍵交換を含む最新の SSH セキュリティプロトコルを採用しています。

## 主な機能

### 1. 多彩な接続性

GS3は、100Mbps、1G、および10GイーサネットSFP/SFP+ポートに挿入することで動作し、イーサネットネットワークからシリアルポートを制御するための柔軟な導入オプションを提供します。

### 2. 統合管理

GS3は、イーサネットとシリアルポートの管理を同一スイッチ上で統合することで、ネットワーク管理を簡素化するように設計されています。シリアルポートを動的に追加できるため、固定構成において別途コンソール管理デバイスを用意する必要がなくなります。これにより、ハードウェアコストを削減し、より環境に優しいソリューションを提供します。

### 3. RJ-45経由のシリアル通信

GS3のRJ-45コネクタは、デバイスのシリアルコンソールポートに接続するためのシリアル通信専用です。標準的なストレートイーサネットケーブルを使用しますが、管理対象デバイスとGS3間の接続に必要なのは、ピン3、4、5、6のみです。<sup>1</sup>

### 4. 簡素化されたIPベースのシリアル管理

各GS3デバイスには固有のIPアドレスが割り当てられるため、複数のTCPポートを追跡する手間を省き、IPベースのシリアル通信管理を直接行うことができます。これにより、統合イーサネットIPネットワーク上でのシリアルデバイスの管理が簡素化されます。

### 5. セキュリティと安定性の強化<sup>2</sup>

GS3は、以下の堅牢なセキュリティ機能を提供します：

- ポスト量子鍵交換 ML-KEM-768 に対応
- ローカル設定可能なユーザーを5人までサポート
- 公開鍵を使用したSSHログインのサポート
- ユーザーログインおよびセッションタイムアウトのSyslogレポート
- 管理者用アカウントは5つありますが、管理用および切断用の通常ログインは4つだけです
- 許可されたSSHクライアントのアクセス制御リスト (ACL)
- IPv4/IPv6を完全に設定可能、ランダムなIPv6アドレスに対応
- アップグレードに60秒未満
- 管理対象デバイスからSSHを廃止することでリスクを排除
- SSH鍵交換アルゴリズムおよび鍵の詳細な設定
- アクティブなコンソールセッションを優先し、新規接続は後回し
- JumpServerはセッションを録画し、コマンドを制限可能
- 1つのIPアドレスにつき1つのシリアルコンソールを割り当て、きめ細かなセキュリティ制御を実現

<sup>1</sup> RJ-45 間の接続には、標準的なストレートイーサネットケーブルが適しています。特注ケーブルが必要な場合は、弊社ウェブサイトをご覧ください：<https://www.glbb.jp/en/hardware/g3/>

<sup>2</sup> GS3のSSHセキュリティ態勢を独自に検証するために、ssh-auditの出力例を付録Aに、SSHセキュリティ態勢の独立した検証例としてssh-auditの出力例を掲載しています。

## 6. ファームウェアのアップグレードが可能で、ユーザーフレンドリーなリセット機能

GS3はSFTP経由でファームウェアのアップグレードが可能であり、最新の機能やセキュリティ更新を常に利用できます。最新のファームウェアは、GS3のサイト (<https://glbb-japan-odoo-b2c-up.odoo.com/hardware/g3>) から入手できます。デバイスのパスワードを忘れた場合、アクティブなシリアルコンソールに接続した状態で、10秒間に4回以上RJ-45インターフェースの抜き差しを行うことで、GS3をデフォルト設定にリセットできます。これにより、デフォルト設定へのシンプルなフェイルセーフ復旧メカニズムが作動します。

## 7. 動作機能

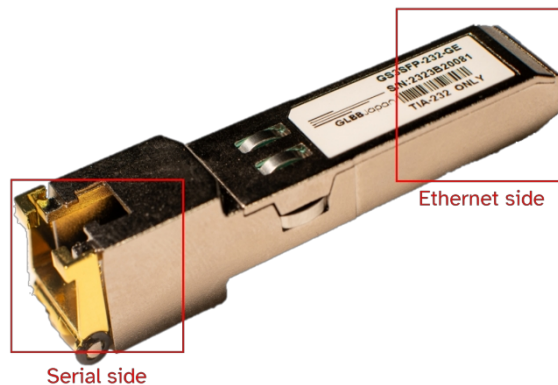
GS3は複数のシリアル通信速度に対応しており、CR/LF送信遅延機能を備えています。この送信遅延機能により、SSH経由で管理インターフェースにコピー&ペーストを行う際に遅延が必要な場合など、テキストが文字化けするのを防ぐことができます。一部のターミナルエミュレーションクライアントには遅延設定機能がありますが、コマンドラインでのSSHなど、すべてのクライアントにその機能があるわけではありません。GS3では、必要に応じて遅延を追加することができます。

## 8. 24時間365日の監視とアラート

GS3は、接続されたデバイスの継続的な監視を可能にし、特定のキーワード、ログインイベント、およびリロードが検出された際に、設定された1つまたは2つのSyslogサーバーへアラートを送信できます。例えば、「SYSLOG」というキーワードが設定されている場合、コンソールに報告されたすべてのSyslogメッセージが、行の終わりまたは100文字のいずれか早い方まで、Syslogサーバーへ送信されます。

## 2 製品仕様

GLBB Secure Smart Serial (GS3) は、企業環境およびサービスプロバイダー環境の両方において、イーサネットおよびシリアル通信を管理するために設計された、汎用性が高く安全なネットワーク機器です。大規模な導入やミッションクリティカルなアプリケーションの複雑な要件を満たす高度な機能を備えています。



### イーサネット通信

- **SFP および SFP+ 互換性**：SFP/SFP+ ポートを介して 100Mbps、1G、および 10G イーサネットをサポートします。
- **レセプタクル**：小型フォームファクタ・プラグブル・モジュールに関する SFF-8432 仕様<sup>3</sup>に準拠しています。
- **インターフェース**：20 ピン INF-8074i 準拠、SFP ポート経由の高速イーサネット通信に対応。

### シリアル通信

- **コネクタ**：シリアル通信用 RJ-45 コネクタ。
- **シリアル機能**：シリアルデバイスの安全なリモート管理のためのリバース SSH をサポート。
- **シリアル規格**：TIA-232 (RS-232)。
- **対応ボーレート**：標準の9600および115200 bpsに加え、GS3は幅広いボーレートに対応しており、さまざまなサービスプロバイダーや企業環境において柔軟な運用が可能です。

### 消費電力

- **最大消費電力**：0.65W - 消費電力が懸念される環境において、エネルギー効率に優れた選択肢です。

### セキュリティと管理

- 安全なリモート管理のための SSHv2 をサポートしています。
- セキュリティ強化のための SSH クライアント ACL を許可。

<sup>3</sup> SFF-8432: 拡張小型フォームファクタ・プラグブル・モジュール (SFP+) およびケージの仕様

- ファームウェアは SFTP 経由でアップグレード可能であり、更新の失敗から保護する堅牢なブートローダーが搭載されています。
- DNSおよびNTPのサポート：GS3はDNSとNTPの両方をサポートしており、NTPプールと連携することで、正確なタイムスタンプとログの記録を保証します。これらは、イベントの正確な追跡やネットワークのトラブルシューティングにおいて不可欠な要素です。

## 認証

- RoHS、FCC、CE、およびVCCIの認証を取得しており、環境および安全基準への準拠を保証します。

## その他の機能

- デバイスごとに固有の IP アドレスが割り当てられるため、イーサネット経由でのシリアルポートの管理が容易です。
- 最大 5 人のローカル設定ユーザーをサポート。
- IPv4 および IPv6 に対応し、復旧用の IPv6 リンクローカルアドレスも含まれています。
- Syslog による継続的な監視およびアラートシステム。
- CR/LF送信遅延：この機能は、SSH管理セッション中、特にシリアルコンソールに大量のデータを貼り付ける際に、テキストが文字化けするのを防ぐのに役立ちます。イーサネットベースのSSHセッションでもデータ破損が発生する可能性があり、一部のターミナルエミュレータでは、このような問題を軽減するためにCR/LF遅延を実装しています。
- リバースSSH（デフォルトTCPポート922）経由でのシリアルコンソールへの直接アクセスをサポートしており、GS3をインバウンド接続にさらすことなく、安全なインバウンド接続を可能にします。<sup>4</sup>

---

<sup>4</sup> リバースSSHアクセスはデフォルトで有効になっていますが、CLIへのアクセスのみに制限するために無効にすることも可能です。

## 3 インストール手順

### デバイスの開梱

パッケージからGS3を慎重に取り出し、以下のものが含まれていることを確認してください：

- GS3 本体
- クイックスタートガイド

### GS3をネットワークに接続する

- GS3モジュールを挿入します。
- GS3を、メディアコンバータ、ルータ、スイッチ、またはその他の互換性のあるデバイスのSFPまたはSFP+ポートに接続します。<sup>5</sup>一部の10G SFP+ポートでは、自動ネゴシエーションが成功しない場合、速度を1Gに設定するために手動での設定が必要になることがあります。
- リンクステータスの確認：GS3を挿入してから数秒以内に、リンクライトが点灯するはずですが、10秒以内にライトが点灯しない場合は、問題が発生している可能性があるため、接続を確認してください。

### GS3への接続

GS3と通信するには、GS3が接続されているデバイス（メディアコンバータやスイッチなど）にノートパソコンを接続してください。同じネットワーク／ブロードキャストドメイン内にあることを確認してください。<sup>6</sup>

### IPアドレスの設定

GS3のデフォルトのIPv4アドレスは192.168.11.11/24で、ゲートウェイアドレスは192.168.11.1です。GS3と通信するには、ノートパソコンのIPアドレスを192.168.11.0/24サブネット内に設定してください。IPv6リンクローカルアドレスを使用して接続することも可能です。デフォルトのIPv6リンクローカルアドレスは、EUI-64形式（例：fe80::8e12:c2ff:fexx:xxxx）で、ここで「xx:xxxx」はシリアル番号です。

### 接続のテスト

ノートパソコンのIPを設定した後、GS3にping<sup>7</sup>を実行して接続をテストしてください。

#### IPv4 ping の例:

```
ping 192.168.11.11
```

#### IPv6 pingの例:<sup>8</sup>

```
ping -6 fe80 ::8 e12: c2ff: fexx: xxxx% インターフェイス
```

<sup>5</sup> 現時点では、SFP28ポートはサポートされていないことにご注意ください。

<sup>6</sup> GS3がルータに接続されている場合、ルータのインターフェイスがブリッジされていない限り、まずルータにSSHで接続し、次にルータからGS3にSSHで接続して実行する必要がある場合があります。

<sup>7</sup> macOSでは、ping6コマンドを使用してIPv6アドレスにpingを実行してください。

<sup>8</sup> IPv6ではリンクローカルアドレスに使用するインターフェイスを指定する必要があるため、%interfaceを実際のネットワークインターフェイス（例：20）に置き換えてください。

## マルチキャストによるリンクローカル IPv6 アドレスの特定

デバイスから直接シリアル番号を取得したくない場合は、IPv6の全ノードマルチキャストアドレスにpingを送信することで、ネットワーク上のGS3の位置を特定できます：

例：

```
ping -6 ff02 ::1%20
```

```
32バイトのデータで ff02 ::1%20 に ping を実行中：
リクエストのタイムアウトが発生しました。
```

Windows では、ping の応答が表示されない場合がありますが、次のコマンドを使用して近隣ホストを確認できます：<sup>9</sup>

```
netsh interface ipv6 show neighbors
```

インターネットアドレス	物理アドレス	タイプ
fe80 ::8 e12: c2ff: fe00 :253	8c-12-c2-00-02-53	到達可能
ff02 ::1	33 -33 -00 -00 -00 -01	永続
ff02 ::2	33 -33 -00 -00 -00 -02	永続
ff02 ::16	33 -33 -00 -00 -00 -16	永続
ff02 :: fb	33 -33 -00 -00 -00 - fb	永続
ff02 ::1:2	33 -33 -00 -01 -00 -02	永続
ff02 ::1:3	33 -33 -00 -01 -00 -03	永続

<sup>9</sup> IPv6 リンクローカルアドレスは EUI-64 形式を使用します。この形式では、2 番目の 16 進文字「C」が「E」に変更され、変更後の OUI とデバイスのシリアル番号の間に FFFE が挿入されます。

## 4 GS3 へのログイン

### SSH アクセス

GS3へのpingが通ることを確認したら、SSH経由でログインする準備が整いました。ターミナルエミュレータ（例：PuTTY）またはコマンドラインインターフェースを使用してください。

デフォルトのログイン情報は、ユーザー名「admin」、パスワード「password」です。

#### 例：IPv4 SSH

```
ssh admin@192.168.11.11

admin@192.168.11.11 のパスワード:
GS-3 SFP モジュールに接続しました。コンソールのエスケープキーは CTRL+] です。[ admin@ssh -to- serial]>
```

#### 例: IPv6 SSH

```
ssh admin@fe80 ::8 e12: c2ff: fe00 :253%20

admin@fe80 ::8 e12: c2ff: fe00 :253%20 ' s パスワード:
GS-3 SFP モジュールに接続しました。コンソールのエスケープキーは CTRL+] です。[ admin@ssh -to- serial]>
```

## 5 使用方法

### メニューの移動と表示

? コマンドを使用してメニューを表示します (Tab キーによる補完がサポートされています)。

メニューは、シリアルコマンド、ネットワークコマンド、セキュリティ管理、ファームウェアコマンド、およびシリアルフリーズロケータコマンドのセクションに分かれています。

例：

```
GS-3 SFPモジュールのCLIに接続しています。   コンソール
escape key は CTRL+] [ admin@ssh -to- serial]>?
### シリアルコマンド serial
  connect serial show
  serial delay - crlf <0000 > serial
  baudrate <レート > serial datasize <
  ビット数 >
  serial parity <none/ odd/even > serial
  stopbits <bits >
  serial exitkey
### ネットワークコマンド
  network show
  network ipv4 <手動/DHCP/無効>
  network ipv6 <auto/ random/ manual/ linklocal/ disable >network port cli/
  reverse - ssh <port >
  network timeout <タイムアウト時間> network
  hostname <ホスト名> network ntp <リモート -
  ntp-addr>
  network <syslog1 / syslog2> <remote - syslog -addr> network reverse - ssh
  <enable/ disable>
### セキュリティ管理ユーザー一覧
  user add <admin/ regular > <username > <password > user change
  <username > <new_password >
  user delete <ユーザー名> user
  publickey <ユーザー名> session list
  session kill <セッションID> ssh
  config <鍵/ ホストキー>
  ssh publickeyonly <有効/無効> acl set <ipv4/ipv6>
  <IPアドレス>
  acl del <ipv4/ipv6> <リスト番号> acl list
  <ipv4/ipv6>
### ファームウェアコマンド フ
  ファームウェアバージョン ファ
  ムウェアアップグレード
  ファームウェアサーバー <設定/取得>
  リセット <デフォルト/再起動>
### シリアルフリーズロケータコマンド keyphrase add
  <キーフレーズ> keyphrase del <リスト番号>
  keyphrase list
```

## 6 シリアルコマンド

「シリアルコマンド」セクションでは、GS3のシリアル通信設定を管理および構成するために必要なツールを提供します。これらのコマンドを使用すると、現在の設定を表示したり、ボーレート、データサイズ、パリティ、ストップビット、送信遅延などの設定を調整したりすることができます。

### serial connect

シリアルコンソールへの接続を確立します。

例:

```
[ admin@ssh -to- serial]>serial connect シリアルセッションを
開始しています...
コンソールのエスケープキーは CTRL+] です
Z
```

### serial show

現在のシリアル設定を表示します。

例:

```
[ admin@ssh -to- serial]>serial show UART
Config - ベース: 0 x4000D000 クロック: 120000000
Hz
ボーレート: 115200
データサイズ: 8 バ
リティ: N ストップ
ビット: 1
フロー制御: N 送信遅延: 100 ms
現在の設定が表示されました。
Z
```

### serial delay-crlf <0000>

送信遅延を設定します。設定範囲は 0 から 86,400,000 ミリ秒（最大 24 時間）です。

例:

```
[ admin@ssh -to- serial]>serial delay - crlf 300 UART設定 - ベー
ス: 0 x4000D000
クロック: 120000000 Hz
ボーレート: 115200
データ長: 8 パリテ
ィ: N ストップビッ
ト: 1
フロー制御: N 送信遅延: 300 ms
送信遅延を300ミリ秒に設定しました。
Z
```

### シリアルボーレート <rate>

ボーレートを設定します。デフォルト設定は 115200 です。最小値は 1200、最大値は 115200 ビット/秒です。

例: 次の例では、シリアルボーレートを 9600 に設定しています。

```
[ admin@ssh -to- serial]>serial baudrate 9600UART設定 - ベ  
ース: 0 x4000D000  
クロック: 120000000 Hz  
ボーレート: 9600  
データ長: 8 パリテ  
ィ: N ストップビッ  
ト: 1  
フロー制御: N 送信遅延: 300 ms  
シリアルボーレートを 9600 に設定しました。
```

### シリアルデータサイズ <ビット数>

送信するデータのサイズを設定します。範囲は5~8ビットです。

**例:** 次の例では、シリアルデータサイズを5ビットに設定しています。

```
[ admin@ssh -to- serial]>serial datasize 5 UART 設定 -  
ベース: 0 x4000D000  
クロック: 120000000 Hz  
ボーレート: 9600  
データサイズ: 5 パ  
リティ: N ストップ  
ビット: 1  
フロー制御: N 送信遅延: 100 ms  
シリアルデータサイズを 5 ビットに設定しました。
```

### シリアルパリティ <なし/奇数/偶数>

パリティモードを「なし」、「奇数」、「偶数」のいずれかに設定します。

**例:** 次の例では、送信パリティモードを「Odd」に設定しています。

```
[ admin@ssh -to- serial]>serial parity oddUART 設定 -  
ベース: 0 x4000D000  
クロック: 120000000 Hz  
ボーレート: 9600  
データ長: 5 パリテ  
ィ: 0 ストップビッ  
ト: 1  
フロー制御: N 送信遅延: 100 ms シ  
リアルパリティは 0 に設定されていま  
す。
```

### serial stopbits <bits>

ストップビット数 (1 または 2) を設定します。

**例:** 次の例は、シリアルストップビットを 2 に設定しています。

```
[ admin@ssh -to- serial]>serial stopbits 2 UART Config  
- Base: 0 x4000D000  
クロック: 120000000 Hz  
ボーレート: 115200  
データ長: 8 パリテ  
ィ: N ストップビッ  
ト: 2  
フロー制御: N 送信遅延: 300 ms  
シリアルストップビットは 2 に設定されています。
```

**serial exitkey**

コンソールセッションを終了するために使用されるキーの組み合わせを変更します。

**例:** 次の例では、終了キーを CTRL + A に設定しています。

```
[ admin@ssh -to- serial]>serial exitkey
終了キーとして使用するキーを押してください...

終了キーが設定されました: CTRL+A
```

## 7 GS3をシリアルコンソールに接続する

GS3はDCE（データ通信機器）として機能します。GS3をDTE（データ端末機器）に適合する設定で構成し、そのケーブルをシリアルコンソールのコネクタに接続してください。<sup>10</sup>

### シリアルケーブル

RJ-45 to RJ-45				
GS3	Pin	Color	Pin	Console
Rx	3	White/Green	3	Tx
Tx	6	Green	6	Rx
GND	5	White/Blue	5	GND
GND	4	Blue	4	GND

RJ-45 to Mini-B				
GS3	Pin	Color	Pin	Console
Rx	3	White/Green	3	Tx
Tx	6	Green	2	Rx
GND	4	Blue	5	GND

RJ-45 to DB-9				
GS3	Pin	Color	Pin	Console
Rx	3	White/Green	3	Tx
Tx	6	Green	2	Rx
GND	4	Blue	5	GND

ケーブルを接続してもデバイスにアクセスできない場合は、正しいポート（イーサネットポートやCTS/RTS対応のRS-232ポートではない）に接続されているか確認してください。通常のイーサネットケーブルを使用してイーサネットポートに接続してしまうと、GS3は直ちに動作を停止します。イーサネットポートからケーブルを抜くと、GS3モジュールは復旧します。

<sup>10</sup> ごくまれに、Brocade/Extreme MLXe-4などのDTEデバイスがDCEとして配線される場合がありますが、MLXe-8およびMLXe-16はDTEとして配線されています。

## 8 ネットワークコマンド

ネットワークコマンドのセクションでは、GS3のネットワーク設定を構成および管理するためのツールを提供します。これらのコマンドを使用すると、ユーザーは現在のネットワーク構成の表示、IPv4およびIPv6設定の変更、DHCPの有効化または無効化、NTPサーバーとの時刻同期の設定を行うことができます。また、システムホスト名の設定、ネットワークポートの管理、Syslogサーバー経由のリモートロギングの設定も可能です。セキュリティ強化のため、GS3はSSHクライアントへのアクセスを制限するホストごとのアクセス制御リスト（ACL）もサポートしています。

### network show

GS3の現在のネットワーク構成を表示します。これには、IPv4およびIPv6設定、DNSサーバー、MACアドレス、インターフェース名、ホスト名、リバースSSH設定、およびNTPやSyslogなどのリモートサービスが含まれます。

例：以下の出力は、GS3のデフォルトのネットワーク設定を示しています。

```
[ admin@ssh -to- serial]>network show コンパイル
日時: 2025年12月23日 04:34:08

静的IPv4アドレス: 192.168.11.11 IPv4サブネットマ
スク: 255.255.255.0 IPv4デフォルトゲートウェイ:
IPv4 プライマリ DNS:
IPv4 セカンダリ DNS:
IPv6 リンクローカルアドレス: fe80 ::8 e12: c2ff: fe00 :16d IPv6 グローバルア
ドレス: ::
IPv6 デフォルトルーター: ::
IPv6 プライマリ DNS:
IPv6 セカンダリ DNS:
リバースSSHポート: 65535CLI SSHポ
ート: 22
SSHリバース接続タイムアウト: 300秒インターフェース名: eth0
ホスト名: ssh-to-serial
MACアドレス: 8C-12-C2-00-01-6D
DHCP: 無効SLAAC: 有効
固定アドレス: EUI -64 を使用して有効IPv4: 有効
リモート NTP サーバー: 0.0.0.0
リモート Syslog サーバー 1: 192.168.11.11
リモート Syslog サーバー 2: 0.0.0.0

現在の設定が表示されています。
```

**警告：** ネットワーク設定コマンドを実行すると、GS3がネットワークスタックを再起動するため、すべてのSSHセッションが切断されます。

### network ipv4 <manual/dhcp/disable>

GS3のIPv4設定を構成します。静的IPアドレスを手動で割り当てる（manual）、DHCPによる動的IP割り当てを有効にする（dhcp）、またはIPv4を完全に無効にする（disable）のいずれかを選択できます。<sup>11</sup>

<sup>11</sup> 引数が指定されていない場合、network ipv4 を実行すると、デフォルトで手動設定モードに入ります。

**例:**

```
[ admin@ssh -to- serial]>network ipv4 manual ホストアドレス
を入力してください:
192.168.11.11

ホストアドレスは 192.168.11.11 に設定されました。サブネ
ットマスクを入力してください:
255.255.255.0

サブネットマスクは 255.255.255.0 に設定されました
。デフォルトゲートウェイを入力してください:
192.168.11.1

デフォルトゲートウェイは 192.168.11.1 に設定されています
。プライマリ DNS を入力してください:
8.8.8.8

プライマリ DNS は 8.8.8.8 に設定されました。セ
カンダリ DNS を入力してください:
1.1.1.1

セカンダリ DNS は 1.1.1.1 に設定されました。すべて
の IPv4 設定が完了しました。
```

**例:**

```
[ admin@ssh -to- serial]>network ipv4 dhcp DHCPが有効
になっています
システムの再起 動 中...
```

**例:**

```
[ admin@ssh -to- serial]>network ipv4 disable IPv4が無効に
なりました
```

**network ipv6 <auto/random/manual/linklocal/disable>**

GS3のIPv6設定を構成します。グローバルアドレスを手動で割り当てる、SLAACを使用して自動的に生成する（auto）、ランダムなアドレスを生成する（random）、リンクローカルアドレスのみを使用する（linklocal）、またはIPv6を完全に無効にする（disable）ことができます。

**例:**

```
[ admin@ssh -to- serial]>network ipv6 manual Enter
Global IPv6 Address: 2001:db8:abcd:0012::1
グローバルアドレスは 2001:db8:abcd:0012::1 に設定されています

プレフィックス長を入力してください:
64
プレフィックス長は 64 に設定されました

デフォルトルーター（ゲートウェイ）を入力してく
ださい: 2001:db8:abcd:0012::fffe
デフォルトルーターは 2001:db8:abcd:0012::fffe に設定されました

IPv6プレフィックスを入力してく
ださい: 2001:db8:abcd:0012::
IPv6プレフィックスが 2001:db8:abcd:0012:: に設定されました

プライマリ DNS を入力してください:
2001:4860:4860::8888

プライマリ DNS が 2001:4860:4860::8888 に設定されました
```

```

セカンダリ DNS を入力してください:
2001:4860:4860::8844

セカンダリ DNS は 2001:4860:4860::8844 に設定されました

グローバルアドレスは 2001:db8:abcd:0012::1 に設定されましたプレフィック
ス長は 64 に設定されました
デフォルトルーターは 2001:db8:abcd:0012::ffff に設定されています
EUIを使用して設定されたリンクローカルアドレス: 64:fe80::8e12:c2ff:fe00:c9

```

```

[ admin@ssh -to- serial]>network ipv4 disable IPv6は無効化
されました

```

### network port cli <port>

GS3へのコマンドラインインターフェース管理用SSH接続で使用するTCPポートを設定します。ポート値は1から65,535の範囲で指定する必要があります。デフォルトのポートは22です。

#### 例:

```

[ admin@ssh -to- serial]>network port cli 22 CLIポートは22
に設定されました
システムの再起 動 中...

```

### network reverse-ssh <ポート>

GS3への着信リバースSSH接続に使用するTCPポートを設定します。ポートの値は1~65,535の範囲で指定する必要があります。デフォルトのポートは922です。

#### 例:

```

[ admin@ssh -to- serial]>network port reverse - ssh 922リバースSSHポート
は922に設定されました
システムの再起 動 中...

```

### ネットワークタイムアウト <timeout>

SSHのタイムアウト時間を秒単位で設定します。設定可能な範囲は60秒から86,400秒（1分から24時間）です。デフォルトのタイムアウト時間は300秒です。この設定は、GS3がCLIおよび/またはリバースSSHセッションを、非アクティブ状態による切断までどのくらいの間アクティブに維持するかを制御します<sup>(12)</sup>

#### 例:

```

[ admin@ssh -to- serial]>network timeout 60リバースSSHのタ
イムアウトが60秒に設定されました。

```

<sup>12</sup> GS3には内部クロックが搭載されていないため、すべてのタイムアウト時間は目安であることをご了承ください。

**network hostname <ホスト名>**

GS3のシステムホスト名を設定します。ホスト名は最大32文字で、先頭は英字でなければなりません。

例：

```
[ admin@ssh -to- serial]>network hostname example - host ホスト名が
example - host に設定されました
[ admin@example - host]>
```

**network ntp <remote-ntp-addr>**

時刻同期用のリモート NTP サーバーを設定します（IP アドレスまたはホスト名のいずれかを指定できます）。現在、IPv4 のみがサポートされています。

例:

```
[ admin@example - host]>network ntp time.example.com NTPサーバーは
time.example.comに設定されています
```

**network syslog <remote-syslog-addr>**

GS3 がシステムログメッセージを送信するリモート syslog サーバーの IP アドレスを設定します。これにより、監視、監査、およびトラブルシューティングを目的とした一元的なログ収集が可能になります。

GS3 は、冗長化またはマルチ宛先ロギングのために、最大 2 台のリモート syslog サーバーの設定をサポートしています。

IPv4 および IPv6 の両方がサポートされています。syslog サーバーは、GS3 から到達可能である必要があります。ログメッセージは、標準の syslog UDP ポート 514 を使用して送信されます。

syslogが設定されている場合、GS3は以下を含むセキュリティ関連のSSHイベントを報告します：

- SSHセッションの確立（ログイン成功）
- SSH認証の失敗
- SSHセッションの終了（ログアウトまたは切断）

これらのイベントは、一元的な監査、アクセス監視、およびセキュリティ分析をサポートします。

例 (IPv4)：

```
[ admin@example - host]>network syslog 192.0.2.15 Syslog サーバーは
192.0.2.15 に設定されています
```

例 (IPv6):

```
[ admin@example - host]>network syslog 2001:db8::15 Syslogサーバーは
2001:db8::15に設定されました
```

## 9 セキュリティ管理コマンド

「セキュリティ管理コマンド」セクションでは、GS3 上のユーザーアカウント、アクセス制御リスト (ACL)、および SSH セッションを管理するためのツールを提供します。

### user list

GS3に設定されているすべてのユーザーアカウントの一覧を表示します。これには、ユーザー名と役割（管理者または一般ユーザー）が含まれます。

例：

```
[ admin@ssh -to- serial]>user list User 1:  
admin ( admin)
```

### user add <admin/regular> <username> <password>

指定されたロールを持つ新しいユーザーアカウントをGS3に追加します。ユーザー名とパスワードは最大33文字まで指定できます。

例:

```
[ admin@ssh -to- serial]>user add regular regular password ユーザー regular の追加  
成功しました。
```

### user change <ユーザー名> <新しいパスワード>

既存のユーザーアカウントのパスワードを変更します。

例：

```
[ admin@ssh -to- serial]>user change regular password ユーザー regular のパ  
スワードが正常に変更されました。
```

### user delete <username>

指定したユーザーアカウントを削除します。

例:

```
[ admin@ssh -to- serial]>user delete regular  
一般ユーザー「regular」を削除しようとしています。  
削除を確認してください (1/3回目)。確認する場合は「y」を、中止する場合は「n」を入力してください：削除を  
確認してください (2/3回目)。確認する場合は「y」を、中止する場合は「n」を入力してください：削除を確認し  
てください (3/3回目)。確認する場合は「y」を、中止する場合は「n」を入力してください：ユーザー「regular」  
の削除に成功しました。
```

### user publickey <username>

指定されたユーザーアカウントに SSH 公開鍵を関連付けます。設定された公開鍵は、SSH 公開鍵認証が有効になっている場合に、ユーザーの認証に使用されます。

例:

```
[ admin@ssh -to- serial]>user publickey admin ユーザー admin
の公開鍵を入力してください:
ssh- ed25519 AAAAC3NzaC11ZDI1NTE5AAAAI... user@example - host ユーザー admin の公開鍵の
設定に成功しました。
```

## セッション一覧

セッション ID および関連するユーザーを含む、すべてのアクティブな SSH セッションのリストを表示します。一般ユーザーは合計 4 つのアクティブなセッションを持つことができ、管理者ユーザーはさらに 1 つのセッションを持つことができ、必要に応じて一般ユーザーのセッションを強制終了することができます。セッション ID は 1 から始まり、1024 まで続き、その後 1 にリセットされます。

### 例：

```
[ admin@ssh -to- serial]>session list アクティブ
なセッション:
セッションID: 5, ユーザー: admin , 送信元IP: 192.168.17.8 , セッション時間: 10秒
```

## session kill <sessionId>

セッション ID に基づいて特定の SSH セッションを終了します。

セキュリティ強化のため、GS3では、新規のSSH接続の試行を1秒あたり最大5回に制限しています。

### 例：

```
[ admin@ssh -to- serial]>session list アクティブ
なセッション:
セッションID: 1, ユーザー: admin , 送信元IP: 192.168.17.8 , セッション時間: 19 セッションID: 2, ユーザー:
regular , 送信元IP: 192.168.11.18 , セッション時間: 10 [ admin@ssh -to- serial]>session kill 2
セッションID: 2 を終了しました。
```

## ssh config <kex/host-key>

GS3で使用されるSSH暗号化アルゴリズムを対話形式で設定します。このコマンドを使用すると、管理者はセキュリティポリシーの要件を満たすため、またはレガシーなSSHクライアントとの互換性を維持するために、特定の鍵交換（KEX）アルゴリズムやSSHホスト鍵の種類を有効または無効にすることができます。

kex を指定すると、GS3 はサポートされている各鍵交換アルゴリズムについて確認を求めます。host-key を指定すると、GS3 はサポートされている各 SSH ホスト鍵アルゴリズムについて確認を求めます。鍵に対して適切な kex アルゴリズムを有効にするよう注意してください。例えば、ssh-rsa を有効にする場合は、hostkey として diffie-hellman-group14-sha1 および/または diffie-hellman-group1-sha1 も有効にしてください。

### 例：

```
[ admin@ssh -to- serial]>ssh config kex kex ecdh -sha2
- nistp256 [Y]:
kex ecdh -sha2 - nistp384 [Y]:
kex diffie - hellman - group14 - sha256 [Y]:
KEX Diffie-Hellman - グループ14 - SHA1 [n]:
KEX Diffie-Hellman - グループ14 - SHA256 [Y]:
KEXアルゴリズムの設定が保存されました。システムを再起動します...
```

```
[ admin@ssh -to- serial]>ssh config host - key key ssh-
ed25519 [Y]:
鍵 ecdsa -sha2 - nistp256 [Y]:
鍵: ssh-rsa [n]:
ホストキーアルゴリズムの設定が保存されました。システムを再起動します...
```

### ssh publickeyonly <有効/無効>

公開鍵認証のみを使用するSSH認証を有効または無効にします。有効にするには、まず user publickey <username> コマンドを使用して、対象のユーザーアカウントに公開鍵を関連付ける必要があります。

#### 例:

```
[ admin@ssh -to- serial]>user publickey admin ユーザー admin
の公開鍵を入力してください:
ssh- ed25519 AAAAC3NzaC1lZDI1NTE5AAAAI... user@example - host ユーザー admin の公開鍵の
設定に成功しました。
[ admin@ssh -to- serial]>ssh publickeyonly enable
公開鍵のみによる認証が有効になりました。システムを再起動します...
```

公開鍵のみの認証が有効になっている場合、パスワードベースのSSHログインは拒否されます。有効な秘密鍵なしで接続を試みるクライアントには、アクセス拒否エラーが表示されます。

#### 例:

```
% ssh admin@192.168.11.11
admin@192.168.11.11: アクセス拒否 (公開鍵)。
```

### acl set <ipv4/ipv6> <ip>

IPv4 または IPv6 のアクセス制御リスト (ACL) に IP アドレスを追加します。ACL に含まれているアドレスのみ、GS3 への SSH 接続を開始することが許可されます。ACL は、再ログインするまで、現在ログインしているユーザーには影響しません。

#### 例:

```
[ admin@ssh -to- serial]>acl set ipv4 192.0.2.100 IPアドレス
192.0.2.100 がACLに追加されました
[ admin@ssh -to- serial]>acl set ipv4 192.0.2.100 IPアドレス 192.0.2.100 がACLに追加
されました
```

### acl del <ipv4/ipv6> <listnum>

インデックス番号に基づいて、アクセス制御リスト (ACL) から IP アドレスを削除します。このコマンドを使用して、以前に許可されていた IPv4 または IPv6 アドレスへのアクセス権を無効にします。

#### 例:

```
[ admin@ssh -to- serial]>acl del ipv4 0 インデックス 0 の
IP アドレスが ACL から削除されました [ admin@ssh -to-
serial]>acl del ipv6 0 インデックス 0 の IP アドレスが
ACL から削除されました
```

**acl list <ipv4/ipv6>**

IPv4 または IPv6 のアクセス制御リスト (ACL) の現在のエントリを表示します。各エントリは、対応するインデックス番号とともに一覧表示されます。

**例:**

```
[ admin@ssh -to- serial]>acl list ipv4
0. 192.10.2.100
[ admin@ssh -to- serial]>acl list ipv6
0. 2001:db8:abcd:0012::10
```

## 10 ファームウェアコマンド

ファームウェアコマンドのセクションでは、GS3のファームウェアを管理および保守するためのツールを提供します。これらのコマンドを使用すると、ユーザーは現在のファームウェアを確認したり、アップグレードを実行したり、SFTP経由でのアップグレードに必要なサーバー設定や認証情報を設定したりできます。GS3管理者は、CLIを使用してファームウェア関連の設定をデフォルト状態にリセットしたり、GS3を再起動してGS3の高速な再起動時間をテストしたりすることができます。

### firmware version

現在のファームウェアのバージョンとビルド情報を表示します。

例:

```
[ admin@ssh -to- serial]>firmware version Version: 2.0  
コンパイル日時: 2025年12月23日 04:34:07
```

### ファームウェアのアップグレード

ファームウェアのアップグレードを開始します。<sup>13</sup>

例:

```
[ admin@ssh -to- serial]>firmware upgrade ファームウェアの更新を開始しました...  
ファームウェアの更新に成功しました。ブートローダーを起動します...  
リモートホスト 192.168.11.11 からの読み取り: 接続が相手側によってリセットされました。  
192.168.11.11 への接続が閉じられました。  
client_loop: send disconnect: パイプが切断されました
```

### ファームウェアサーバー <set/get>

ファームウェアファイルが保存されている SFTP サーバーの認証情報と設定を設定または取得します。

例:

```
[ admin@ssh -to- serial]>firmware server set SFTPサーバー名  
を入力してください:  
192.0.2.10  
SFTPサーバーのポートを入力してください:  
22  
SFTPユーザー名を入力してください:  
sftpuser  
SFTP パスワードを入力してください:  
*****  
SFTP ファイル名を入力してください:  
firmware.bin  
SFTPサーバーの認証情報が正常に更新されました! [ admin@ssh -to-  
serial]>firmware server get SFTPサーバー名: 192.0.2.10  
SFTPサーバーポート: 22 SFTPユーザ  
ー名: sftpuser  
SFTP パスワード: [ 削除済み] SFTP ファ  
イル名: gs3_2_0.bin 信頼済みホストキー:
```

<sup>13</sup> 「firmware upgrade」コマンドの実行中に別の管理者レベルのユーザーがログインしている場合、ファームウェアの更新はタイムアウトし、220 エラーが発生することに注意してください。

```
[ admin@ssh -to- serial]>firmware server get SFTP サーバー  
名: 192.168.11.12  
SFTP サーバーポート: 22 SFTP ユ  
ーザー名: jbolton  
SFTP パスワード: [ 削除済み] SFTP ファ  
イル名: gs3_2_0.bin 信頼済みホストキー:  
ssh- ed25519 AAAAC3NzaC11ZDI1NTE5AAAAIBRZb2N1bWVudGF0aW9uT25seUtleTAwMDAwMDAw
```

## リセット <デフォルト/再起動>

### reset defaults

デバイスの設定を工場出荷時のデフォルト設定にリセットします。ユーザー定義の設定パラメータはすべて消去され、システムは初期状態に復元されます。

### リセット 再起動

現在の設定を変更せずにデバイスを再起動します。

### 例:

```
[ admin@ssh -to- serial]>reset defaults  
システム設定が工場出荷時のデフォルト値にリセットされました。
```

```
[ admin@ssh -to- serial]>reset reboot システムの  
再起動中...
```

### 物理リセット:

GS3の電源が入っている状態で、10秒以内に5回以上コンソールケーブルを素早く抜き差しすることで、ハードウェアによる工場出荷時設定へのリセットを実行できます。この操作は、「リセットデフォルト」を実行することと同等です。

## 11 シリアルフレーズロケータ

この機能は、シリアルコンソールポートの出力を監視し、特定のキーワードを検出します。最大10個のキーワードを設定できます。一致が検出されると、GS3はSyslogメッセージを生成し、設定されたリモートサーバーに送信します。

### keyphrase add <キーフレーズ>

シリアルコンソールの出力で監視するフレーズの一覧に、キーフレーズを追加します。システムでは最大10個のキーフレーズをサポートしています。設定されたフレーズがシリアル出力で検出されると、GS3は適切なリモートサーバーに対してsyslogメッセージを送信します。

例：

```
[ admin@ssh -to- serial]>keyphrase add ERROR: Link Down 0: ERROR: Link Down
[ admin@ssh -to- serial]>keyphrase add CPU Overheat Warning 0: ERROR: Link Down
1: CPU過熱警告
```

### keyphrase list

シリアルコンソールの出力で、現在設定され監視対象となっているすべてのキーワードを表示します。

例：

```
[ admin@ssh -to- serial]>keyphrase list 0: ERROR:
リンクダウン
1: CPU過熱警告
```

### keyphrase del <リスト番号>

keyphrase list コマンドで表示されるインデックス番号を使用して、監視リストからキーフレーズを削除します。削除されると、システムはそのフレーズに基づいて監視を行ったり、アラートを発動したりしなくなります。

例:

```
[ admin@ssh -to- serial]>keyphrase list 0: ERROR:
Link Down
1: CPU過熱警告
[ admin@ssh -to- serial]>keyphrase del 0 0: CPU過熱
警告
[ admin@ssh -to- serial]>keyphrase list 0: CPU過熱警
告
```

## A SSHセキュリティ監査の結果

本付録では、業界標準の ssh-audit ツールを使用して GS3 に対して実施された独立した SSH セキュリティ評価の例を示します。この出力は、透明性を確保し、セキュリティチームが GS3 SSH サービスの暗号化態勢を評価するのに支援するために掲載されています。<sup>14</sup>

### 監査方法

- ツール：ssh-audit
- 対象：GS3 SSHサービス
- プロトコル：SSHv2
- 実行環境：外部クライアントホスト

### 実行したコマンド

```
ssh-audit <GS3 -IP-アドレス>
```

### 監査出力

```
# 一般
( gen) バナー: SSH -2.0 - CycloneSSH_2 .5.2
( gen) 互換性: OpenSSH 9.9 以降、Dropbear SSH 2020.79 以降 ( gen) 圧縮: 無効

# 鍵交換アルゴリズム ( kex)
mlkem768x25519 - sha256 ( kex)
curve25519 - sha256
( kex) curve25519 -sha256@libssh.org ( kex)
ext-info -s
( kex) kex-strict -s-v00@openssh.com

# ホスト - 鍵アルゴリズム (key)
ssh-ed25519

# 暗号化アルゴリズム (ciphers) (enc) aes128 - gcm
(enc) aes128 -gcm@openssh.com (enc)
aes256 - gcm
(enc) aes256 -gcm@openssh.com (enc)
aes128 - ctr
(enc) aes192 - ctr
(enc) aes256 - ctr

# メッセージ認証コード (MAC) アルゴリズム hmac -sha2 -
256-etm@openssh.com (mac) hmac -sha2 -512-
etm@openssh.com
```

<sup>14</sup> 結果は、テスト時点での GS3 のデフォルトの SSH 設定を反映しており、ファームウェアのバージョンによって異なる場合があります。

## B 導入例：ウォームリロードの検出

Cisco Catalyst 2950 でのウォームリロードを検出するには、次の起動シーケンスを確認してください。

```
C2950 ブートローダー (C2950 -HB00T -M) バージョン 12.1(11 r)EA1、リリースソフトウェア (fc1)
2002年7月22日(月) 17:18、antonino によりコンパイルされました。
WS-C2950 -12 起動中...
ベースイーサネット MAC アドレス: 00:12:7 f:38: a4 :40 Xmodem ファイルシ
ステムが利用可能です。
フラッシュの初期化...
flashfs[0]: 87 ファイル、3 ディレクトリ
flashfs[0]: 孤立ファイル 0 個、孤立ディレクトリ 0 個 flashfs[0]: 合計バイト数:
7741440
flashfs[0]: 使用バイト数: 6511104 flashfs[0]: 空きバイト数:
1230336 flashfs[0]: flashfs fsck に 8 秒かかりました。
... フラッシュの初期化が完了しました。
ブートセクタファイルシステム (bs:) がインストールされました、fsid: 3 パラメータブ
ロックファイルシステム (pb:) がインストールされました、fsid: 4 「flash:/ c2950 -
i6q412 -mz.121 -22. EA1. bin」を読み込んでいます...###
```

このイベントを追跡するには、次のコマンドを使用して最初の行をキーフレーズとして追加してください:

```
[ admin@ssh -to- serial]>keyphrase add C2950 ブートローダー (C2950 -HB00T -M) バージョン 12.1(11 r)EA1 , リリースソフトウェア ( fc1)
0. C2950 ブートローダー (C2950 -HB00T -M) バージョン 12.1(11 r)EA1、リリースソフトウェア (fc1)
```

キーフレーズが正常に追加されたことを確認してください:

```
[ admin@ssh -to- serial]>keyphrase list
0. C2950 ブートローダー (C2950 -HB00T -M) バージョン 12.1(11 r)EA1 , リリースソフトウェア ( fc1)
```

ウォームリロードが発生すると、GS3はこのキーフレーズと照合し、設定されたsyslogサーバーにアラートを送信します:

```
10月10日 15:33:37 192.0.2.15 ssh-to-serial 一致が見つかりました: C2950 ブートローダー (C2950 -HB00T -M) バージョン 12.1(11 r)EA1 , リリ
ソフトウェア ( fc1)
```

## C 導入例：ホストリカバリの検出

Cisco Catalyst 2950 でホストリカバリを検出するには、次の手順に従います。

```
00:00:15: % SPANTREE -5- EXTENDED_SYSID: タイプ vlan に対して拡張 SysId が有効化されました00:00:17: %SYS-5-
CONFIG_I: コンソールからメモリ経由で設定されました
00:00:18: %SYS-5- RESTART: システムが再起動しました --Cisco
Internetwork Operating System Software
IOS (tm) C2950 ソフトウェア (C2950 - I6Q4L2 -M)、バージョン 12.1(22) EA1、リリースソフトウェア (fc1)
Copyright (c) 1986 -2004 by Cisco Systems, Inc. 2004年7月12日(月)
08:18 に madison によってコンパイル
00:00:18: %SNMP -5- COLDSTART: ホスト Switch 上の SNMP エージェントがコールドスタートを実行中です 00:00:18: %LINK -5- CHANGED: インターフ
ェース Vlan1 の状態が管理ダウンに変更されました 00:00:19: %LINK -5- CHANGED: インターフェース Vlan2 の状態が管理ダウンに変更されました
00:00:19: % LINEPROTO -5- UPDOWN: インターフェース Vlan1 のラインプロトコルの状態がダウンに変更されました 00:00:20: % LINEPROTO -5-
UPDOWN: インターフェース Vlan2 のラインプロトコルの状態がダウンに変更されました Switch >
```

このイベントを追跡するには、以下のキーフレーズを使用して、次の行を追加してください：

```
[ admin@ssh -to- serial]>keyphrase add %SYS-5- RESTART:
0: %SYS-5- RESTART:
```

キーフレーズが正常に追加されたことを確認してください：

```
[ admin@ssh -to- serial]>keyphrase list
0. %SYS-5- RESTART:
```

ホストが復旧すると、GS3はこのキーフレーズと照合し、設定されたsyslogサーバーにアラートを送信します：

```
10月10日 15:35:38 192.0.2.15 ssh-to-serial 一致が見つかりました: 0. %SYS -5- RESTART:
```

## D ファームウェアのリリースとSHA256ハッシュ値

以下は、GS3でサポートされているファームウェアのリリースとSHA256ハッシュ値の一覧です:

バージョン 2.0 ファイル名 GS3_2_0.bin SHA256 ハッシュ: E7DD92333F1FB389E80DE73B3A26AC657AC846A09EDA9081FAAFEBFFD14C0E5A
--

GLBB Japanのウェブサイト <https://www.glbb.ne.jp/hardware/g3> を確認し、このPDFを検証してください。また、このPDFを使用して、上記のSHA256ハッシュとバイナリを照合してください。