



ファームウェアバージョン:	R2.10.B006	
ハードウェアバージョン:	DGS-1250-28X	A1
	DGS-1250-28XMP	A1
	DGS-1250-52X	A1
	DGS-1250-52XMP	A1
発行日:	2025/6/16	

本リリースノートには、D-Link 製スイッチのファームウェア更新に関する重要な情報が含まれています。ご使用のスイッチに対応するリリースノートであることを確認してください。

- 新しいスイッチにインストールを行う際には、デバイス上のハードウェアバージョンの表示を確認し、ご使用のスイッチがファームウェアのシステム要件を満たしていることを確認してください。ファームウェアとハードウェアの互換性についての詳細情報は、“変更履歴とシステム要件”の項を参照してください。
- 新しくリリースされたファームウェアへのアップグレードを行う場合は、“アップグレード手順”の項を参照しながら正しい手順でファームウェアのアップグレードを行ってください。

スイッチ本体に関する詳細な情報が必要な場合は“ユーザマニュアル”を参照してください。

目次：

変更履歴とシステム要件：	2
アップグレード手順：	2
CLI（シリアルポート）を使用したアップグレード	2
Web GUI を使用したアップグレード	5
追加機能：	8
MIB および D-View モジュールの変更点：	8
コマンドラインインタフェースの変更点：	8
修正した問題点：	11
既知の問題：	11

変更履歴とシステム要件：

ファームウェアバージョン	リリース日付	モデル	ハードウェアバージョン
ランタイム：R2.10.B006	2025/6/16	DGS-1250-28X	A1
		DGS-1250-28XMP	A1
		DGS-1250-52X	A1
		DGS-1250-52XMP	A1

※R2.10.B006へのアップグレード後、SSLがデフォルトで有効になります。https://<IPアドレス>で管理画面に接続してください。

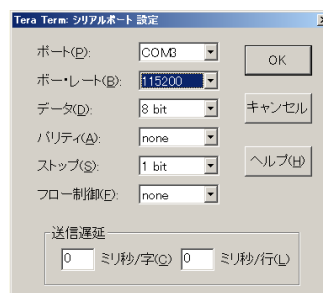
アップグレード手順：

アップグレードは、CLI(シリアルポート)もしくは Web GUI から実施することができます。

CLI (シリアルポート) を使用したアップグレード

1. スイッチの RS-232C シリアルポート (コンソールポート) と PC を接続し、ターミナルソフトウェアを起動します。ターミナルソフトウェアの設定は下記の通りです。(本手順書ではターミナルソフトウェアは Tera Term を使用しています。)

- ボーレート：115200
- データビット：8
- パリティ：none
- ストップビット：1
- フロー制御：none



2. ターミナルコンソール上でキーボード上のいずれかのキーを押します。
3. ユーザ名とパスワードの入力を求められますので、アカウント情報を入力し「Enter」を押します。初期値のアカウントおよびパスワードは「admin」です。
4. ログイン後は下記のコマンドを使用し、ファームウェアのアップデートを行います。

コマンド	説明
show boot	現在のブートイメージと設定ファイル名を表示します。
copy tftp://location/filename flash: {Image1 Image2}	TFTP サーバからスイッチにファームウェアをダウンロードします。
configure terminal	グローバルコンフィグモードに入ります。
boot image	次回の起動時にイメージファイルとして使用されるファイルを指定します。
end	現在のコンフィグモードを終了し、EXEC モードに戻ります。
reboot	スイッチをリブートします。
show version	スイッチのバージョンを表示します。

以下の例を参考にファームウェアのアップデートを行ってください。

例)

(1) スイッチのユーザ名とパスワードを入力してログインします。

ユーザ名とパスワードの初期値は「admin」です。

(2) 現在のブートイメージを確認します。

※以降の例では、現在のブートイメージとは別のイメージIDに対しファームウェアの更新を行います。

Switch#**show boot**

Unit 1

Boot image: /c:/Image1

Boot config: /c:/Config1

(3) スイッチにファームウェアをダウンロードします。

Switch#**copy tftp: //10.90.90.100/DGS1250_Ax_FW2_10_B006.had flash: Image2**

Address of remote host [10.90.90.100]?

Source filename [DGS1250_Ax_FW2_10_B006.had]?

Accessing tftp://10.90.90.100/DGS1250_Ax_FW2_10_B006.had...

Transmission start...

Transmission finished, file length 9433360 bytes.

Please wait, programming flash..... 100 %

Please wait, programming flash for language filesDone.

(4) ブートイメージを指定します。

Switch#**configure terminal**

Switch(config)#**boot image Image2**

Switch(config)#**end**

Switch#**show boot**

Unit 1

Boot image: /c:/Image2

Boot config: /c:/Config1

(5) スイッチを再起動します。

Switch#**reboot**

Are you sure you want to proceed with the system reboot?(y/n) **y**

Please wait, the switch is rebooting...

注意：

スイッチのアップグレード中及び再起動中に、電源を切らないでください。電源を切ると、起動に失敗し、起動できなくなることがあります。故障の原因となりますので、ご注意ください。

注意：

PoE 対応モデルにおいて、R2.03.B010 から R2.04.B012/R2.10.B006 へのアップグレードを行う場合、PoE コントローラのアップグレードも行われるため、5 分程度の時間を要します。

(6) バージョンがアップグレードされていることを確認します。

Switch#**show version**

System MAC Address: xx-xx-xx-xx-xx-xx

Module Name DGS-1250-52XMP

H/W A1

Runtime 2.10.B006

※R2.10.B006 へのアップグレード後、SSL がデフォルトで有効になります。

※SSL 機能には v2.10.B006 において既知の脆弱性が存在します。SSL 機能を無効にするか、本リリースノートの [「既知の問題」](#) をご確認ください、対応策を実施してください。

Web GUI を使用したアップグレード

1. Java SE runtime environment をダウンロードして、お客様の PC にインストールします。
2. TFTP サーバ経由でアップグレードを行う場合は、PC 上で TFTP サーバを有効にします。(必ずご使用の PC に TFTP サーバのインストールを行っておいてください。)
3. お客様の PC とスイッチを R-45 ネットワークケーブルで接続します。
PC とスイッチの IP アドレスは同じサブネット内に設定してください。
(例：スイッチの IP アドレスが 10.90.90.90 の場合、PC は 10.90.90.100 など)
4. スwitchの IP アドレス（初期値：10.90.90.90）をブラウザのアドレスバーに入力し、Web GUI にアクセスします。
5. Web GUI にログインします。
「User Name」（管理者のユーザ名）と「Password」（パスワード）の初期値は「admin」です。
6. **Management > File System** を選択し、「Boot File」をクリックします。

The screenshot shows the 'File System' web interface. At the top, there is a 'Path' input field containing 'C:' and a 'Go' button. Below this are 'Copy' and 'Boot File' buttons. A table lists available drives:

Drive	Media Type	Size (MB)	File System Type	Label
C:	Flash	44	swfs	

7. 現在のブートイメージ（「Image1」または「Image2」）を確認します。

The screenshot shows the 'File System' web interface with the 'Boot File' section expanded. The 'Path' field now contains 'c/'. The 'Boot Image' dropdown is set to 'Image 1' and the 'Boot Configuration' dropdown is set to 'Configuration 1'. There are 'Apply' and 'Cancel' buttons. Below these are two columns: 'Boot Image' and 'Boot Configuration', each with a table listing the selected items.

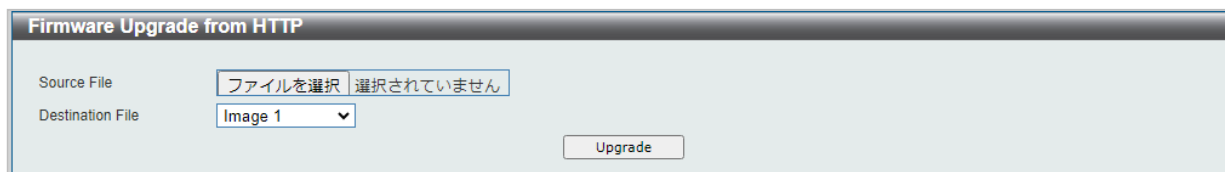
Boot Image	Boot Configuration
/c:/Image1	/c:/Config1

※この後のアップグレード作業で、現在のイメージ ID か別のイメージ ID を指定する必要があります。

8. ファームウェアアップグレードは、**Tools > Firmware Upgrade & Backup** から実行します。アップグレードの方法は「HTTP」「TFTP」から選択します。

HTTP 経由でアップグレードを行う場合

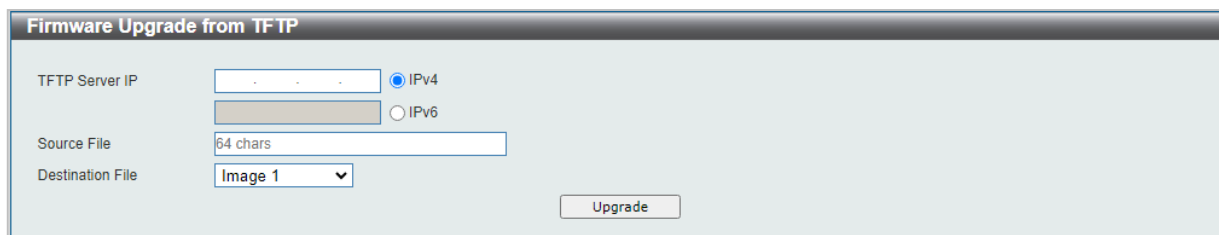
Tools > Firmware Upgrade & Backup > Firmware Upgrade from HTTP を選択します。



- Source File : 「ファイルを選択」をクリックし、ファームウェアファイルを選択します
- Destination File : ファームウェアの保存先として、「Image 1」または「Image 2」を指定します。

TFTP サーバ経由でアップグレードを行う場合

Tools > Firmware Upgrade & Backup > Firmware Upgrade from TFTP を選択します。



- TFTP Server IP: IPv4 もしくは IPv6 を選択し、TFTP サーバの IP アドレスを入力します。
- Source File : TFTP サーバ上に保存したファームウェアファイル名を入力します
- Destination File : ファームウェアの保存先として、「Image 1」または「Image 2」を指定します。

9. 「Upgrade」をクリックします。
10. ステータス画面が表示されます。
アップロード完了後に「Done.」と表示されるまで待機します。

注意：ファームウェアのダウンロード中およびアップグレード中に、電源を切らないでください。電源を切ると、起動に失敗し、起動できなくなることがあります。故障の原因となりますので、ご注意ください。

※TFTP によるアップグレードの場合はポップアップ画面が表示されますので、「Done.」メッセージ表示後に右上の「×」をクリックして画面を閉じます。

11. 次回のスイッチリブート時にブートアップを行うイメージが選択するために、**Management > File System** の順にクリックします。

※現在のブートイメージ ID をアップグレード先として指定した場合、ブートイメージの変更は不要です。手順 11～14 をスキップし、手順 15 のシステム再起動に進んでください。

Drive	Media Type	Size (MB)	File System Type	Label
C:	Flash	44	swfs	

12. 「Boot File」をクリックします。
13. 「Boot Image」で新しいイメージ ID を指定し、「Apply」をクリックします。

Boot Image	Boot Configuration
/c:/image1	/c:/Config1

14. ブートファイルの指定に成功すると「Success.」メッセージが表示されます。画面の「OK」をクリックします。
15. **Tools > Reboot System** をクリックし、スイッチをリブートします。

16. 以下の画面で「Yes」を選択し「Reboot」をクリックします。
「Are you sure you want to reboot?」と表示されるので「OK」ボタンをクリックし、スイッチを再起動してください。

Do you want to save the settings? ☒ Yes ☐ No

If you do not save the settings, all changes made in this session will be lost.

Reboot

注意：スイッチの再起動中に、電源を切らないでください。再起動中に電源を切ると、起動に失敗し、起動できなくなることがあります。故障の原因となりますので、ご注意ください。

注意：PoE 対応モデルにおいて、R2.03.B010 から R2.04.B012/R2.10.B006 へのアップグレードを行う場合、PoE コントローラのアップグレードも行われるため、5 分程度の時間を要します。

17. システムの再起動後にログインし、デバイス情報画面でファームウェアのバージョンがアップグレードされていることを確認します。

※R2.10.B006 へのアップグレード後、SSL がデフォルトで有効になります。https://<IP アドレス>で管理画面に接続してください。

※SSL 機能には v2.10.B006 において既知の脆弱性が存在します。SSL 機能を無効にするか、本リリースノートの[「既知の問題」](#)をご確認いただき、対応策を実施してください。

追加機能：

ファームウェアバージョン	変更点
R2.10.B006	<ol style="list-style-type: none"> 1. DGS-712/G1 をサポート致しました。 2. GBIC 情報の表示をサポート致しました。 3. 再起動スケジュール設定をサポート致しました。 4. non-WAC Radius CoA/DM をサポート致しました。(CLI) 5. SSH でアルゴリズムの設定をサポート致しました。 6. jQuery v3.5.0 以降をサポート致しました。 7. OpenSSL を更新致しました。

MIB および D-View モジュールの変更点：

ファームウェアバージョン	更新ファイル
R2.10.B006	DGS-1250_R2.10_MIB_Files_20240417.zip

コマンドラインインタフェースの変更点：

ファームウェアバージョン	変更点
R2.10.B006	<ol style="list-style-type: none"> 1. Non-WAC 機能 <ol style="list-style-type: none"> (1) RADIUS CoA&DM (RFC5176)のコマンドを追加致しました。 <pre> aaa server radius dynamic-author no aaa server radius dynamic-author client { IP-ADDRESS HOSTNAME } server-key [0 7] STRING no client { HOSTNAME IP-ADDRESS } port PORT-NUMBER no port radius-server attribute 55 include-in-acct-req no radius-server attribute 55 include-in-acct-req </pre> (2) NAS-Identifier (RADIUS Attribute 32)のコマンドを追加致しました。 <pre> radius-server attribute 32 include-in-access-req STRING no radius-server attribute 32 include-in-access-req </pre> (3) NAS-IP-Address (RADIUS Attribute 4)のコマンドを追加致しました。 <pre> radius-server attribute 4 IP-ADDRESS no radius-server attribute 4 IP-ADDRESS </pre>

- (4) Tunnel-Private-Group-ID (RADIUS Attribute 81)
UIなし

- (5) RADIUS送信元インタフェースのコマンドを追加致しました。

```
ip radius source-interface INTERFACE-ID

no ip radius source-interface

ip tacacs source-interface INTERFACE-ID

no ip tacacs source-interface

ipv6 radius source-interface INTERFACE-ID

no ipv6 radius source-interface

ipv6 tacacs source-interface INTERFACE-ID

no ipv6 tacacs source-interface
```

- (6) Network Accountingのコマンドを追加・更新致しました。
以下のコマンドを追加致しました。

```
aaa accounting network default {start-stop METHOD1 [METHOD2...] | none}

no aaa accounting network default
```

以下のコマンドを更新致しました。

```
radius-server host {IP-ADDRESS | IPV6-ADDRESS } [auth-port PORT] [acct-port PORT] [timeout SECONDS ] [retransmit COUNT ] key [0 | 7] KEY-STRING
```

2. GBIC 情報の表示コマンドを追加致しました。

```
show interfaces [INTERFACE-ID [, | -]] gbic
```

3. 再起動スケジュールのコマンドを追加致しました。

```
reboot schedule {in MINUTES | at HH:MM [DDMTHYYYY]} [save_before_reboot]

no reboot schedule

show reboot schedule
```

4. SSH コマンドを追加致しました。

```
ip ssh server algorithm encryption { [aes128-cbc]
[aes192-cbc][aes256-cbc] [3des-cbc] [blowfish-cbc] [twofish128-cbc]
[twofish192-cbc] [twofish256-cbc] [arcfour] [cast128-cbc] [aes128-ctr]
[aes192-ctr][aes256-ctr] [aes128-gcm@openssh.com] [aes256-gcm@openssh.com] [chacha20-poly1305@openssh.com] }

no ip ssh server algorithm encryption { aes128-cbc | aes192-cbc | aes256-cbc
| 3des-cbc | blowfish-cbc | twofish128-cbc | twofish192-cbc |
twofish256-cbc | arcfour | cast128-cbc | aes128-ctr | aes192-ctr |
aes256-ctr | aes128-gcm@openssh.com | aes256-gcm@openssh.com |
chacha20-poly1305@openssh.com}
```

```
ip ssh server algorithm key-exchange
[{{diffie-hellman-group1-sha1}}][{{diffie-hellman-group14-sha1}}
[{{diffie-hellman-group14-sha256}}][{{diffie-hellman-group16-sha512}}
[{{diffie-hellman-group18-sha512}}][{{diffie-hellman-group-exchange-sha1
}} [{{diffie-hellmangroup-exchange-sha256}}
[{{ecdh-sha2-nistp256}}][{{ecdh-sha2-nistp384}} [{{ecdh-sha2-nistp521}}
[{{curve25519-sha256}}]]

no ip ssh server algorithm key-exchange {diffie-hellman-group1-sha1 |
diffie-hellman-group14-sha1 | diffie-hellman-group14-sha256 |
diffiehellman-group16-sha512 | diffie-hellman-group18-sha512 |
diffiehellman-group-exchange-sha1 |
diffie-hellman-group-exchange-sha256 | ecdh-sha2-nistp256 |
ecdh-sha2-nistp384 |ecdh-sha2-nistp521 |curve25519-sha256}

ip ssh server algorithm mac { [hmac-sha1] [hmac-sha1-96]
[hmac-md5] [hmac-md5-96] [hmac-sha2-256]}

no ip ssh server algorithm mac {hmac-sha1| hmac-sha1-96 | hmac-md5 |
hmac-md5-96 | hmac-sha2-256}

ip ssh server algorithm hostkey {ssh-dss| ssh-rsa}

no ip ssh server algorithm hostkey {ssh-dss| ssh-rsa}
```

5. SSL コマンドを追加致しました。

```
no ssl-service-policy <string 1-32> [ { version [ { tls1.0 } ] [ { tls1.1 } ]
[ { tls1.2 } ] | ciphersuite [ { dhe-dss-3des-ede-cbc-sha } ]
[ { rsa-3des-ede-cbc-sha } ] [ { rsa-rc4-128-sha } ] [ { rsa-rc4-128-md5 } ]
[ { rsa-export-rc4-40-md5 } ] [ { rsa-aes-128-cbc-sha } ]
[ { rsa-aes-256-cbc-sha } ] [ { rsa-aes-128-cbc-sha256 } ]
[ { rsa-aes-256-cbc-sha256 } ] [ { dhe-dss-aes-256-cbc-sha } ]
[ { dhe-rsa-aes-256-cbc-sha } ] [ { ecdhe-rsa-aes-128-gcm-sha256 } ]
[ { ecdhe-rsaaes-256-gcm-sha384 } ] | secure-trustpoint |
session-cache-timeout } ]

ssl-service-policy <string 1-32> [ { version [ { tls1.0 } ] [ { tls1.1 } ]
[ { tls1.2 } ] | ciphersuite [ { dhe-dss-3des-ede-cbc-sha } ]
[ { rsa-3des-ede-cbc-sha } ] [ { rsa-rc4-128-sha } ] [ { rsa-rc4-128-md5 } ]
[ { rsa-export-rc4-40-md5 } ] [ { rsa-aes-128-cbc-sha } ]
[ { rsa-aes-256-cbc-sha } ] [ { rsa-aes-128-cbc-sha256 } ]
[ { rsa-aes-256-cbcsha256 } ] [ { dhe-dss-aes-256-cbc-sha } ]
[ { dhe-rsa-aes-256-cbcsha } ] [ { ecdhe-rsa-aes-128-gcm-sha256 } ]
[ { ecdhe-rsa-aes-256-gcm-sha384 } ] | secure-trustpoint <string 1-32> |
session-cachetimeout <value 60-86400> } ]
```

修正した問題点：

ファームウェアバージョン	修正した問題点
R2.10.B006	<ol style="list-style-type: none"> IPSG (IP Source Guard) + IMPB (IP-MAC-Port Binding) を有効化した後、トラフィックが転送されない問題を修正致しました。 AAA 機能において、セッションが異なる場合でも Acct-session ID が常に同じ ID 番号となる問題を修正致しました。 IP アドレスを除く工場出荷時設定へのリセットを選択した場合でも、IPv6 アドレスがリセットされてしまう問題を修正致しました。 SSL 機能において、パスワード保護された証明書およびプライベートキーのファイルインポートに対応していなかった問題を修正致しました。 コンソール経由で IPv6 ソースガード設定を行い、show running-config を実行した際にクラッシュする場合がある問題を修正致しました。 DSCP CoS マッピングで優先制御が適切に動作しない問題を修正致しました。

既知の問題：

ファームウェアバージョン	既知の問題
R2.10.B006	<ol style="list-style-type: none"> マルチキャストフィルタリング機能の Filter Unregistered モードにおいて、予約済み IP アドレス (239.*.*、224.0.0.*、224.0.1.*、FF0*::*、FF0*::DB8:0:0) がフィルタされない問題。 SSL 機能及び SSH 機能には既知の脆弱性が存在します。これらの機能を使用する場合は、以下の対応策を実施してください。 <ul style="list-style-type: none"> 以下の SSH アルゴリズム設定を無効化します。 <p>暗号化アルゴリズム：</p> <pre>[aes128-ctr] [aes192-ctr] [aes256-ctr] [3des-cbc] [blowfish-cbc] [twofish128-cbc] [twofish192-cbc] [twofish256-cbc] [twofish-cbc] [arcfour] [cast128-cbc] [aes128-ctr] [aes192-ctr] [aes256-ctr]</pre> <p>MAC アルゴリズム：</p> <pre>[hmac-sha1] [hmac-sha1-96] [hmac-md5]</pre>

	<p>[hmac-md5-96]</p> <p>ホスト鍵設定アルゴリズム :</p> <p>[ssh-dss]</p> <p>鍵交換アルゴリズム :</p> <p>[diffie-hellman-group14-sha1]</p> <p>[diffie-hellman-group1-sha1]</p> <p>[diffie-hellman-group-exchange-sha1]</p> <p>[ecdh-sha2-nistp256]</p> <p>[ecdh-sha2-nistp384]</p> <p>[ecdh-sha2-nistp521]</p> <p>[curve25519-sha256]</p> <p>● 以下の TLS オプションを無効化します。</p> <p>TLS バージョン</p> <p>[TLS 1.0]</p> <p>[TLS 1.1]</p> <p>暗号化スイート</p> <p>[DHE_DSS_WITH_3DES_EDE_CBC_SHA]</p> <p>[RSA_WITH_3DES_EDE_CBC_SHA]</p> <p>[RSA_EXPORT_WITH_RC4_40_MD5]</p> <p>[RSA_WITH_RC4_128_MD5]</p> <p>[RSA_WITH_AES_128_CBC_SHA]</p> <p>[RSA_WITH_AES_256_CBC_SHA]</p> <p>[DHE_DSS_WITH_AES_256_CBC_SHA]</p> <p>[DHE_RSA_WITH_AES_256_CBC_SHA]</p>
--	---

Copyright 2025 D-Link Japan K.K.