TANDBERG DATA
Securing your Information

RDX QuikStation セキュリティパッチ 2026-10

ご案内と適用手順（QuikStation 4 / QuikStation 8 共通）

本件脆弱性の根本修正は最新ファームウェア 3.3.0.5 にのみ適用可能です。そのため、本パッチは FW3.3.0.5 への更新も含みます。(パッチは全てのバージョンに実行できます)

1. はじめに

本書は、RDX QuikStation 4 および QuikStation 8/QuikStation8_10G の Web 管理画面（Apache / PHP）に関するセキュリティパッチのご案内です。

緊急対策：PHP の脆弱性「php2shell」（CVE-2026-109618、CVE-2026-109619／CVSS 9.2）
2026 年 10 月 21 日に公開された PHP の重大な脆弱性です。認証不要で、Web 管理画面の任意の URL に細工した HTTP リクエストを 1 回送るだけで、Web サーバー権限での任意コード実行につながります。QuikStation の Web 管理画面は Apache の mod_php で動作しているため該当します。
本パッチはファームウェアを最新化した上で、PHP セキュリティチームが公開した公式の修正（PHP 7.4 向けバックポート）を組み込んだ PHP に置き換え、この脆弱性を根本的に解消します。現在お使いのファームウェアが 3.3.0.5 でも本パッチを適用しないと脆弱性の問題は解消されませんので、必ず適用をお願いいたします。一部古いファームウェアでは緩和策のみの適用となりますが、**2026 年 10 月 22 日時点で公開・観測されている攻撃手法は、いずれも緩和設定で無効化される経路を用いており、緩和設定のみの装置でも成立しません。**ただし緩和設定は PHP プロジェクト自身が「一時的・部分的な緩和」と位置付けているものですので、本パッチの案内に従い、ファームウェアを最新化した上で再度本パッチを適用することを強く推奨いたします。

本パッチは 2 つの層で構成されます：**（1）緩和設定**（Apache／PHP／TLS の設定変更。全ファームウェアに適用可）と、**（2）PHP 修正**（PHP 7.4.33 ＋ PHP セキュリティチーム公式の修正を組み込んだ PHP モジュール。ファームウェア 3.3.0.5 専用）。実行するパッチは 1 つで、装置のファームウェアに応じて自動的に必要な層を適用します。ファームウェア 3.3.0.5 への更新や、すでにファームウェア 3.3.0.5 の装置の予備の起動スロットの更新も本パッチが行い、装置が再起動します。SSH 経由で適用し、適用後は装置の Web 管理画面が数秒間再起動します。**ファームウェア更新による再起動中を除き、バックアップ動作・**

iSCSI 接続・ネットワークリンクには影響しません。パッチの実行中は装置の Web 管理画面を操作しないでください。

対象：市場で稼働する全ての QuikStation 4 / QuikStation 8 / QuikStation8_10G。特定号機以降などの条件はありません。ファームウェアによる動作の違いは次のとおりです。

装置のファームウェア	本パッチの動作
1.x 系（1.3.6〜1.5.1.26）	緩和設定を適用し、**保存確認のため装置を 1 回再起動**します（下記※）。PHP 修正を適用するには FW 2.5.2 以降への更新（4 章のリンクの手順）後に本パッチを再実行する必要があります
2.5.2〜3.2.x	緩和設定を適用した後、**同梱のファームウェア 3.3.0.5 への更新を実行**（装置が再起動。1 回あたり数分、機種により 10 分程度）。復帰後、もう一方の起動領域にも 3.3.0.5 を書き込むため**再起動は通常 2 回**になります。Windows／Mac／Linux のツールは再起動を待って自動で続行し、PHP 修正まで適用します（装置上で直接実行した場合のみ、復帰後に本パッチをもう一度実行してください）
3.3.0.5	PHP 修正と緩和設定（未適用の場合）を適用。もう一方の起動領域が 3.3.0.5 より古い場合は、そこにも 3.3.0.5 を書き込み（**装置が再起動 1 回**）、復帰後に両方の起動領域へ PHP 修正を適用。両方の起動領域が既に 3.3.0.5 の場合は、適用後に**保存確認のため 1 回再起動**します（下記※）

※ 一部の装置では内蔵ストレージが書込みを保持しなくなる故障が知られており、その場合は再起動で変更が失われます。ファームウェア更新を伴う装置では更新後の再起動で保存を確認できますが、1.x および両方の起動領域が 3.3.0.5 の装置では他に再起動が無いため、本パッチが適用後に 1 回だけ再起動し、復帰後の再実行で `PERSIST: VERIFIED`（保存を確認）と表示します。保存されていなかった場合は `STORAGE FAULT` として案内し、サポートへの連絡をお願いします。

2. 本パッチで対処する項目

本表は本パッチ（ファームウェア 3.3.0.5 ＋ PHP 修正）を適用した状態での結果です。凡例：**解消**＝指摘が解消／緩和＝攻撃の成立条件を除去または影響を限定。FW 1.5.1.26 以前の装置で緩和策のみしか適用されない場合に結果が異なる項目には、その旨を（※）で記載しています。

項目／CVE	本パッチの内容	区分
CVE-2026-109618 PHP メモリ不足処理時のメモリ破壊（RCE）	PHP セキュリティチーム公式の修正を組み込んだ PHP 7.4.33 に置き換え（ただし FW1.5.1.26 以前の装置で緩和策のみしか適用されない場合は、PHP `memory_limit = -1` と Apache `LimitRequestBody` による緩和設定のみ）	**解消** ※緩和策のみの場合は緩和
CVE-2026-109619 PHP リクエスト間の状態保持による use-after-free（RCE）	同上。修正済み PHP ではセッションのアップロード進捗機能自体が削除されています（ただし FW1.5.1.26 以前の装置で緩和策のみしか適用されない場合は、PHP `session.upload_progress.enabled = 0` による緩和設定のみ）	**解消** ※緩和策のみの場合は緩和
Obsolete Version of PHP（PHP 7.4.5）	PHP を 7.4 系の最終版 7.4.33 に更新（上記公式修正を含み、7.4.33 までの修正を全て含みます）。PHP 7.4 系自体はサポート終了のため、スキャナーによっては引き続き「古い PHP」として検出されることがあります（ただし FW1.5.1.26 以前の装置で緩和策のみしか適用されない場合は、7.4.5 のまま）	7.4.33 に更新 ※緩和策のみの場合は未対応
PHP：CVE-2019-11048、CVE-2020-7068、CVE-2020-7069、CVE-2020-7070、CVE-2020-7071、CVE-2021-21702、CVE-2021-21703、CVE-2021-21704、CVE-2021-21705、CVE-2021-21707、CVE-2021-21708、CVE-2022-31625、CVE-2022-31626、CVE-2022-31628、CVE-2022-31629、CVE-2022-31630、CVE-2022-37454	PHP 7.4.33 で修正済み（ただし FW1.5.1.26 以前の装置で緩和策のみしか適用されない場合は、未対応。うち CVE-2021-21702（SOAP）、21703（FPM）、21704（Firebird）、2022-31625（pgsql）、31626（mysqlnd）、31630（GD）は該当する拡張を読み込んでいないため該当せず、CVE-2019-11048 は DoS に限られ、その他は管理画面が使用しない関数か影響が軽微）	**解消** ※緩和策のみの場合は未対応
CVE-2024-40725 / CVE-2024-39884 Apache：AddType によるハンドラ設定でのソース開示	PHP ハンドラを `AddType` から `SetHandler`（FilesMatch）方式に変更	**解消**
CVE-2026-79768 Apache	未使用の mod_userdir を無効化	**解消**

mod_userdir 情報開示		
CVE-2026-33007 Apache mod_authn_socache クラッシュ	未使用の mod_authn_socache を無効化	**解消**
CVE-2021-3449 OpenSSL TLS 再ネゴシエーション時の NULL 参照（DoS）	TLS 1.2 以下の再ネゴシエーションを無効化（NoRenegotiation）。※ファームウェア 1.x（OpenSSL 1.0.2）はこの脆弱性の対象外	緩和
CVE-2012-4929 CRIME（TLS 圧縮）	SSLCompression off を明示	**解消**
TLS 1.0 / TLS 1.1 のサポート（RFC 8996）	TLS 1.2 および 1.3 のみ許可	**解消**
BEAST（CVE-2011-3389）、Lucky13（CVE-2013-0169）、SWEET32（CVE-2016-2183）、Logjam／一般的な素数の使用（CVE-2015-4000）、静的鍵交換（RSA）暗号、弱い MAC（SHA-1）暗号スイート、DES/IDEA 暗号スイート、強い暗号の欠如	暗号スイートを ECDHE＋AEAD（AES-GCM／ChaCha20）のみに限定、サーバー側優先順位を強制、セッションチケット無効化	**解消**
Slowloris 型の低速リクエスト攻撃（CVE-2007-6750）	RequestReadTimeout を設定	緩和
Cross-Site Tracing（TRACE メソッド）	TraceEnable off を明示	**解消**
クリックジャッキング	X-Frame-Options: SAMEORIGIN を付与	**解消**
Cookie の HttpOnly フラグ欠如／Secure フラグ欠如	セッション Cookie に HttpOnly、HTTPS 応答の全 Cookie に Secure を付与、session.use_strict_mode 有効化	**解消**
サーバーバージョン情報の開示（Server ヘッダ、X-Powered-By、ETag）	ServerTokens Prod、ServerSignature Off、expose_php Off、FileETag None、X-Content-Type-Options、Referrer-Policy	**解消**
PHP リモートラッパー経由の SSRF 面（CVE-2020-7071、CVE-2021-	Web 管理画面は URL を開かないため allow_url_fopen Off、allow_url_include Off、enable_dl Off	緩和(攻撃面の除去)

21705 関連）		

3. 本パッチの対応外の項目（OpenSSL／Apache の更新が必要なもの）

以下は OpenSSL／Apache 自体の更新が必要であり、本パッチでは対処できません。ただし備考欄に記載のとおり、QuikStation においては攻撃経路が存在しないか、影響が DoS（Web 管理画面の一時的な応答停止）程度にとどまり、認証不要の侵入につながるものはありません。これらは今後、パッチまたはファームウェア更新の形で対処する予定です。それでもこれらの指摘について直ちに対処が必要なお客様は、従来どおり **2023 年 11 月公開の「Security Patch Instructions」に含まれる Web 管理画面の無効化スクリプト（**`QS-security-patch.sh`／`webinterface.sh`**）**をご利用ください。（案内書（英語）：https://pub-4f6f0f4e63894238a2e6d96abbaa1645.r2.dev/RDX_QuikStation_Security_Patch_Information_and_Instructions_2023-11.pdf、スクリプト（QS-Patch.tar）：https://pub-4f6f0f4e63894238a2e6d96abbaa1645.r2.dev/QS-Patch.tar。案内書に記載の Overland-Tandberg 社のダウンロード先は現在アクセスできないため、同じファイルをここに置いています）Web 管理画面を停止した状態では、以下の項目（および上記 2 章の項目）は到達不能となります。設定が必要な時だけ `webinterface.sh enable` で一時的に有効化し、作業後に `disable` で停止してください。

備考の区分：（a）＝構成上、脆弱なコードが動作していない／攻撃経路が無い　（b）＝該当するが影響は DoS 等に限定　（c）＝該当するが QuikStation に無い構成（リバースプロキシ等）が前提

項目	備考
OpenSSL：CVE-2020-1971、CVE-2021-3449（緩和のみ）、CVE-2021-3711、CVE-2021-3712、CVE-2021-4160、CVE-2021-23840、CVE-2021-23841、CVE-2022-0778、CVE-2022-1292、CVE-2022-2068、CVE-2022-2097、CVE-2022-4304、	OpenSSL 1.1.1w 以降で修正。（a）CVE-2022-1292／2022-2068（c_rehash スクリプト）、2021-4160（MIPS のみ）、2022-2097（32 ビット x86 のみ）、2021-3711（SM2）は該当しません。（a）証明書解析に関する CVE-2020-1971、2021-3712、2021-23841、2022-0778、2022-4450、2023-0215、2023-0286 は攻撃者の証明書を受け取る経路（クライアント証明書認証）が無いため到達しません。（a）CVE-2022-4304（RSA 鍵交換）は本パッチの暗号スイート制限により到達しません。（b）CVE-2021-23840

CVE-2022-4450、CVE-2023-0215、CVE-2023-0286	は巨大入力時の整数オーバーフローで影響は軽微です
Apache HTTP Server：CVE-2021-34798、CVE-2023-38709、CVE-2024-42516、CVE-2024-38476 ほか core の修正	Apache 2.4.6x 以降で修正。（a）mod_proxy／mod_http2／mod_lua／mod_dav／CGI 系の CVE はモジュールを読み込んでいないため、mod_rewrite 系の CVE は書き換えルールが無いため該当しません。（b）CVE-2021-34798 は細工したヘッダで子プロセスが停止する DoS です（自動再起動）。（c）CVE-2022-22720 はリバースプロキシ配下、CVE-2023-38709／2024-24795／2024-38476／2024-42516 は利用者入力を応答ヘッダに反映するアプリが前提で、管理画面では成立しません
自己署名の TLS/SSL 証明書、証明書の Subject CN 不一致、信頼されない証明書	装置固有の自己署名証明書を使用しているため。同一ネットワーク内での中間者攻撃の余地は残るため、管理画面へのアクセスを管理用端末に限定することで対処してください
ICMP timestamp response	2023 年の案内と同様、対応外です
TCP timestamp response	TCP タイムスタンプは高速（10GbE）iSCSI 転送の信頼性（PAWS）に必要なため、本パッチでは意図的に無効化していません

4. ファームウェア更新とパッチ適用の順序

本パッチにはファームウェア 3.3.0.5 が同梱されており、**PHP 修正に必要なファームウェア更新は本パッチ自身が行います**。お客様が手動でファームウェアを更新する必要があるのは 1.x 系（1.5.1.26 以前）の装置だけです。現在のファームウェア別の流れは次のとおりです。

現在のファームウェア	流れ
3.3.0.5	そのまま本パッチを適用してください。もう一方の起動領域に 3.3.0.5 より古いファームウェアが残っている場合は、本パッチが PHP 修正と緩和設定を適用した後にそこにも 3.3.0.5 を書き込み（装置が再起動、数分〜10 分程度）、復帰後に両方の起動領域へ PHP 修正を入れます。
2.5.2〜3.2.x	そのまま本パッチを適用してください。緩和設定 → 3.3.0.5 への更新（装置が再起動、数分〜10 分程度） → PHP 修正 → もう一方の起動領域にも 3.3.0.5 を書き込み（再起動 2 回目） → 両方の起動領域へ PHP 修正、までを Windows／Mac／Linux のツールが自動で行います（装置上で直接実行した場合は、復帰後に本パッチをもう一度実行してください）。**再起動中はバックアップと iSCSI 接続が中断されますので、バックアップが動作していない時間帯に実行してください。**先に手動で 3.3.0.5 へ更新してから適用しても構いません。
1.5.1.26 以前（1.x 系）	1.x 系から 2.x 系への更新は本パッチでは行えません（3 段階の更新作業が必要です。手順は本表の下のリンク）。**まず本パッチを適用**して緩和設定で保護し、その後に下記手順で 2.5.2 以降へ更新してください。**この更新でパッチは完全に消えますので、更新後に本パッチをもう一度実行してください。**再実行時は 3.3.0.5 への更新と PHP 修正まで自動で行われます。

1.x 系からの更新手順（3 段階）の詳細：
https://drive.google.com/file/d/1C4yG0U92Van-UYk4u5ptwxw-rBgTesYe/view?usp=drive_link

ファームウェア 3.3.0.5 は本パッチに同梱されています。単体で必要な場合はこちらから：
https://overlandtandberg.co.jp/downloads

将来ファームウェアを再度更新・再書き込み・ダウングレードした場合は、**更新後に本パッチをもう一度実行してください**。2.x／3.x 系の間の更新では緩和設定は有効なまま残りますが、PHP 修正は書き換わった

起動領域から消えます（ファームウェア更新は起動領域を丸ごと書き換えるためです）。本パッチ（第３版以降）は修正済み PHP の控えを装置内に保管しており、書き換わった起動領域の PHP が対応ファームウェア（2.8.0.8〜3.3.0.5）の標準 PHP であれば、次の起動時に自動で修正を入れ直します。ただし確実を期すため、更新後は本パッチの再実行を推奨します（数秒〜数分。緩和設定の控えも補修されます）。適用状態は 8 章の `_phpsec` 表示で確認できます。本パッチ（`qs-patch.sh`）はファームウェアの状態を自動判別するため、どの状態からでも同じファイル・同じ手順で実行できます。

5. 適用前の準備（共通）

1. QuikStation の Web 管理画面にログインし、**System Settings > Options > Diagnostics** タブで **Allow Remote Access (SSH)** を有効にします。
2. 同じ画面で**鍵ファイルをダウンロード**します（装置ごとに異なります）。
3. パッチ一式をダウンロードし、1 つのフォルダに展開します。

   ダウンロード：https://pub-4f6f0f4e63894238a2e6d96abbaa1645.r2.dev/QS-SecurityFix-2026-10-v13.zip

   （ファイル名：`QS-SecurityFix-2026-10-v13.zip`。約 100 MB。SHA-256 チェックサム `SHA256SUMS.txt` と本書の PDF は https://quikstation-patch.pages.dev/ にあります）

6. 適用手順 ― Windows（クリック 1 つで完了）

1. 展開したフォルダ（`QS-SecurityFix.bat`、`qs-patch.sh`、`qs-secfix.sh`、`qs-phpfix.sh`、`libphp7.so`、`php`、`quikstation_3.3.0.5.swu`、`plink.exe`、`pscp.exe`、`qs-keyconv.ps1` が入っています）に、5 章でダウンロードした**鍵ファイルを保存**します。ファイル名はそのままで構いません。
2. `QS-SecurityFix.bat` **をダブルクリック**します。鍵ファイルは自動的に検出されます。
3. QuikStation の IP アドレス（Web 管理画面を開く時のアドレス）を入力し、Enter を押します。
4. 現在の状態が表示された後、`Type YES to apply the patch:` と表示されたら `YES` と入力します。

5. 最後に `RESULT: PROTECTED` と表示されれば完了です。（次の手順 6 で SSH を無効に戻すのも忘れないでください）1.x および両方の起動領域が 3.3.0.5 の装置では、適用後に保存確認の再起動が 1 回入り、復帰後に `PERSIST: VERIFIED` を確認して完了します。ファームウェアの更新が必要な装置（2.5.2〜3.2.x、または 3.3.0.5 でもう一方の起動領域が古い場合）では途中で 3.3.0.5 の書き込みと再起動が入り（2.5.2〜3.2.x では通常 2 回。1 回あたり数分、機種により 10 分程度）、バッチが装置の停止と復帰を確認して自動で続行します。実行中は装置の Web 管理画面を操作しないでください。**再起動中はバックアップと iSCSI 接続が中断されますので、バックアップが動作していない時間帯に実行してください。**1.x の装置では緩和設定のみ適用され、`RESULT: MITIGATED` とその旨の案内が表示されます。実行記録は同じフォルダの `QS-SecurityFix-log.txt` に保存されます。
6. **最後に必ず管理画面で SSH を無効に戻します（System Settings > Options > Diagnostics > Allow Remote Access (SSH) をオフ）。ダウンロードした鍵ファイルも削除してください。**

> 確認のみ：QS-SecurityFix.bat <IP アドレス> /STATUS　　元に戻す：QS-SecurityFix.bat <IP アドレス> /RESTORE
> Windows 7 以降で動作します。PC へのインストールやレジストリの変更は行いません。複数台に適用する場合は、各装置の鍵ファイルを同じフォルダに入れておくと、実行時にどの装置かを選択できます。

7. 適用手順 — macOS／Linux

標準の OpenSSH クライアント（`ssh`、`scp`、`ssh-keygen`）を使用します。同梱の `qs-patch-apply.sh` を使うのが簡単です。装置が提示するホスト鍵を 5 章でダウンロードした鍵ファイルと照合し、一致しない場合は中止します。ファームウェア更新の再起動も待って自動で続行します。

```
chmod +x qs-patch-apply.sh
./qs-patch-apply.sh <IP アドレス> <鍵ファイル>              # 適用
./qs-patch-apply.sh <IP アドレス> <鍵ファイル> --status     # 確認のみ
./qs-patch-apply.sh <IP アドレス> <鍵ファイル> --restore    # 元に戻す
```

最後に忘れずに管理画面から SSH を無効に戻してください。

手動で行う場合：

```
# 新しい OpenSSH では scp に -O を付けてください（装置に SFTP がありません）
chmod 600 <鍵ファイル>
ssh -i <鍵ファイル> vtx@<IP アドレス> "mkdir -p /tmp/qsfix"
scp -O -i <鍵ファイル> qs-patch.sh qs-secfix.sh qs-phpfix.sh libphp7.so php vtx@<IP アドレス>:/tmp/qsfix/
scp -O -i <鍵ファイル> quikstation_3.3.0.5.swu vtx@<IP アドレス>:/srv/www/tmp/   # FW 更新が必要な装置のみ
ssh -t -i <鍵ファイル> vtx@<IP アドレス> "sh /tmp/qsfix/qs-patch.sh"        # yes と入力
ssh -i <鍵ファイル> vtx@<IP アドレス> "sh /tmp/qsfix/qs-patch.sh --status"
```

手動の場合、ファームウェア更新で装置が再起動したら、復帰後に上記の転送と実行をもう一度行ってください（RESULT: PROTECTED、1.x の装置では RESULT: MITIGATED になるまで）。--status の出力の PLAN: 行が FWUPDATE で始まる装置だけ、quikstation_3.3.0.5.swu の転送が必要です。

最後に忘れずに管理画面から SSH を無効に戻してください。

8. 適用後の確認と注意事項

- --status（Windows では /STATUS）で RESULT: PROTECTED（1.x の装置では RESULT: MITIGATED）と表示されることを確認してください。
- PHP 修正が稼働している装置では、Web 管理画面のバージョン情報（About ダイアログ、システム画面のバージョン欄）に表示されるファームウェアバージョンの末尾に _phpsec が付きます（例：03.003.00.5_phpsec）。ツールを使わずに適用状態を確認する目安としてご利用ください。この表示は修正済み PHP が稼働している間だけ付き、ファームウェア更新などで修正が外れると自動的に消えます（--restore で元に戻した場合も消えます）。
- 適用中、Web 管理画面は数秒間再起動します。ログイン中の場合は再度ログインしてください。**ファームウェア更新が行われる場合の再起動中を除き、バックアップ・iSCSI・ネットワークには影響しません。**
- 適用後、Web 管理画面への接続には **TLS 1.2 以上**が必要です（ファームウェア 2.x/3.x では TLS 1.2 と 1.3、1.x では TLS 1.2 のみ）（TLS 1.0/1.1 のみの古いブラウザからは接続できなくなります）。Windows 8.1／Server 2012 R2 以降の標準ブラウザ、および現行の Chrome／Edge／Firefox／Safari は対応しています。

- 設定変更で Web サーバーが起動できなかった場合、パッチは**自動的に元の設定へ巻き戻し**、その旨を表示します。修正済み PHP で Web サーバーが起動できなかった場合も、このパッチで入れ替えた分だけを自動的に元の PHP に戻します（起動時のフックも、モジュールが読み込めない場合は元に戻し、`--status` にその旨を表示します）。元の PHP は装置内に保管されており、`--restore` で戻せます。
- 本パッチは再起動後も有効です。ファームウェア更新との関係は 4 章のとおりです。更新後は必ず本パッチをもう一度実行してください（対応ファームウェアの範囲では起動時に PHP 修正が自動で入り直りますが、再実行で確実になります）。
- QuikStation 8 は起動時にシステムを RAM に展開して動作するため、本パッチはディスク上の起動領域と稼働中の RAM 上の両方を更新します。まれに RAM 側の更新ができない場合は `RESULT: INSTALLED - RESTART THE UNIT` と表示されます。その場合は Web 管理画面から装置を再起動し、復帰後に本パッチをもう一度実行してください。
- 本パッチの実行中にファームウェア更新が進行中（更新受理から再起動まで）の場合、パッチは何もせず `RESULT: FIRMWARE UPDATE IN PROGRESS` と表示します。再起動が終わってから再実行してください。更新は長くて 15 分程度かかることがあります。その間は再実行しないでください。
- 内蔵ストレージが読み取り専用になった装置（まれに発生します。再起動後に設定やログが消えます）では、パッチは `RESULT: STORAGE FAULT` と表示し、再起動を伴うファームウェア更新は行いません。緩和設定と PHP 修正は次の再起動まで有効です。この表示が出た場合は、ツールの記録ファイルと Web 管理画面からダウンロードしたログをサポートまでお送りください。
- 作業後は Web 管理画面で **SSH を無効**に戻し、ダウンロードした**鍵ファイルを削除**してください（鍵ファイルは装置への管理者権限のログインに使えます）。
- 元に戻す場合は `--restore`（Windows では `/RESTORE`）を実行してください。

TANDBERG DATA
Securing your Information

©2026 Tandberg Data

初版 20261023　第 2 版 20261026　第 3 版 20261028