2026 年 11 月 9 日

お客様各位

セイコーソリューションズ株式会社

PHP の脆弱性（CVE-2026-109618、CVE-2026-109619）に関するお知らせ

（第 3 報）

平素より当社製品をご利用いただき、誠にありがとうございます。

2026 年 10 月 21 日に、PHP の開発元から、PHP の脆弱性 2 件（CVE-2026-109618、CVE-2026-109619）が公表されました。
当社製品のうち、Web 管理画面または REST API に PHP を使用している製品が、本脆弱性の影響を受けます。
本脆弱性は、ログインなどの認証を経ることなく、ネットワーク経由で攻撃を受けるおそれがあるものです。

対象製品をお使いのお客様におかれましては、修正版のシステムソフトウェアをご提供するまでの間、本書の「回避策」に記載の設定をお願いいたします。
本書は、新しい情報が判明次第、改訂してお知らせいたします。

改版履歴

版	発行日	改版内容
第 1 報	2026 年 10 月 22 日	初版
第 2 報	2026 年 10 月 23 日	4 項「影響を受けない製品」に、TS-2335 シリーズを追加（第 1 報では調査中）
第 3 報	2026 年 11 月 9 日	10 項「当社の対応」に、修正版のシステムソフトウェアのリリース予定日を追加

第 3 報　(発行日：2026/11/09)

第 3 報では、以下の内容をお知らせいたします。

1　脆弱性の概要

PHP の開発元が公表した脆弱性は、以下の 2 件です。
いずれも、攻撃者が本装置の Web 管理画面または REST API に通信できる場合、細工したリクエストによって本装置内で任意のコードを実行されるおそれがあります。

CVE 番号	内容	深刻度（CVSS）
CVE-2026-109618	PHP がメモリー不足を処理する際の不具合	v3.1：9.8（緊急） v4.0：9.2
CVE-2026-109619	PHP が前のリクエストで解放したメモリーを、次のリクエストの処理で誤って使用する不具合	v3.1：9.8（緊急） v4.0：9.2

詳細は、以下をご参照ください。
・NVD：https://nvd.nist.gov/vuln/detail/CVE-2026-109618
・NVD：https://nvd.nist.gov/vuln/detail/CVE-2026-109619
・PHP の開発元のセキュリティー情報：https://github.com/php/php-src/security/advisories

2　影響を受ける条件

以下の条件をすべて満たす場合に、本脆弱性の影響を受けます。
・「影響を受ける製品」に記載の製品を、対象のシステムソフトウェアで使用している
・HTTP サーバーまたは HTTPS サーバー（Web 管理画面、REST API）を有効にしている
・攻撃者が本装置の HTTP サーバーまたは HTTPS サーバーに通信できる

本脆弱性は、Web 管理画面や REST API がログインの認証を行う前の処理で発生します。
そのため、ユーザーのパスワードを変更しても、本脆弱性による攻撃を防ぐことはできません。
「回避策」に記載の設定により、HTTP サーバー、HTTPS サーバーに通信できる接続元をなくすか、限定してください。

3　影響を受ける製品

以下の製品が、本脆弱性の影響を受けます。

製品	対象のシステムソフトウェア	影響を受ける機能
TS-2560 シリーズ	すべての Version	Web 管理画面（HTTP、HTTPS）
TS-2220 シリーズ	すべての Version	Web 管理画面（HTTP）
TS-2950 シリーズ	すべての Version	Web 管理画面（HTTP、HTTPS）
TS-1550	すべての Version	Web 管理画面（HTTP、HTTPS）
NS-2260 シリーズ	すべての Version	REST API（HTTP サーバー、HTTPS サーバー）
NS-2250 シリーズ	Version 3.0～Version 3.3	REST API（HTTP サーバー、HTTPS サーバー）

いずれの製品も、工場出荷時の設定では、HTTP サーバー、HTTPS サーバー（Web 管理画面、REST API）は無効になっています。
そのため、本脆弱性の影響を受けるのは、お客様がこれらを有効にして使用している場合に限られます。
なお、有効にしている場合でも接続元を限定していないと、すべての接続元から Web 管理画面や REST API に通信できる状態となりますので、ご注意ください。

4　影響を受けない製品

以下の製品は、本脆弱性の影響を受けません。

製品	理由
TS-291x シリーズ、TS-292x シリーズ	Web 管理画面を持っていません
TS-2335 シリーズ ※	PHP を使用していません
TD-450、TD-210	PHP を使用していません
NS-2250 シリーズ Version 2.2 以前	PHP を使用していません（REST API は Version 3.0 で追加した機能です）
NS-2236	PHP を使用していません
SmartJumper	PHP を使用していません

※ 第 2 報で追加いたしました（第 1 報では調査中としておりました）。

5　サポート終了製品

サポート終了製品については、本脆弱性の対象は以下のとおりです。

製品	対象	補足
TS-2550 シリーズ	対象	Web 管理画面（HTTP、HTTPS）。回避策の設定をお願いいたします。設定方法は TS-2950 シリーズと同じです。
TS-2850 シリーズ	対象	Web 管理画面（HTTP、HTTPS）。回避策の設定をお願いいたします。設定方法は TS-2950 シリーズと同じです。
TS-2210 シリーズ	対象外	Web 管理画面に PHP を使用していません
NS-2240 シリーズ	対象外	

6　回避策

修正版のシステムソフトウェアをご提供するまでの間、お使いの状況に応じて以下の設定をお願いいたします。

Web 管理画面、REST API の使用状況	お願いする設定
使用していない	HTTP サーバー、HTTPS サーバーを無効にしてください。無効にすると、本脆弱性の影響を受けません。
使用している	通信できる接続元を、管理に使用する端末の IP アドレスに限定してください。

あわせて、インターネットなどの信頼できないネットワークから本装置に直接通信できないよう、設置場所にもご配慮ください。
製品ごとの設定方法は、以降の項目をご参照ください。

7　回避策の設定方法（TS-2560 シリーズ、TS-2220 シリーズ、TS-1550）

使用していない場合

コンソール、Telnet、または SSH で本装置にログインし、以下のコマンドで HTTP サーバー、HTTPS サーバーを無効にして、設定を保存してください。

```
enable
configure
no http
no https
end
write memory
```

TS-2220 シリーズは HTTPS の機能を持たないため、no https と https allow-host は不要です。
前面パネルから無効にすることもできます。

・TS-2560 シリーズ、TS-2220 シリーズ：設定メニューの「4. Web Access」で Disable を選択し、「7. Config / Log」で Save を選択します。
・TS-1550：設定メニューの「8. CLI / Web Access」で HTTP、HTTPS をそれぞれ Disable にし、「11. Config」で Save を選択します。

使用している場合

Web アクセスを許可するホストを、管理に使用する端末に限定します。
以下は、管理に使用する端末の IP アドレスが 192.0.2.10 の場合の設定例です。

```
enable
configure
http allow-host 192.0.2.10
https allow-host 192.0.2.10
end
write memory
```

許可するホストを設定していない場合は、すべてのホストからの Web アクセスを許可する状態になっています（工場出荷時の設定）。
TS-2560 シリーズ、TS-2220 シリーズを IPv6 アドレスでも使用している場合は、http allow-host6、https allow-host6 コマンドで同様に設定してください。
前面パネルの設定メニュー（TS-2560 シリーズ、TS-2220 シリーズは「4. Web Access」、TS-1550 は「8. CLI / Web Access」）からも、許可する IP アドレスを設定できます。

操作の詳細については、各製品の「導入・運用の手引き」をご参照ください。

8　回避策の設定方法（TS-2950 シリーズ、TS-2550 シリーズ、TS-2850 シリーズ）

使用していない場合

コンソール、Telnet、または SSH で本装置にログインし、以下のコマンドで HTTP サーバー、HTTPS サーバーを無効にして、設定を保存してください。

```
enable
configure
no http
no https
end
write memory
```

TS-2950 シリーズでは、前面パネルの設定メニューの「Web Access」で Disable を選択し、「Config / Log」で Save を選択することでも無効にできます。

使用している場合

アクセス制御リストで、HTTP、HTTPS に通信できる接続元を管理に使用する端末に限定します（最後の行で許可した通信以外をすべて拒否するため、ほかの通信を透過する行もあわせて登録します）。
以下は、管理に使用する端末の IP アドレスが 192.0.2.10、アクセス制御リスト名が webonly、適用先が LAN1 の場合の設定例です。

```
enable
configure
ip access-list webonly
line 10 permit tcp 192.0.2.10/32 0.0.0.0/0 eq 80
line 20 permit tcp 192.0.2.10/32 0.0.0.0/0 eq 443
line 30 deny tcp 0.0.0.0/0 0.0.0.0/0 eq 80
line 40 deny tcp 0.0.0.0/0 0.0.0.0/0 eq 443
line 50 permit tcp 0.0.0.0/0 0.0.0.0/0
line 60 permit udp 0.0.0.0/0 0.0.0.0/0
line 70 permit icmp 0.0.0.0/0 0.0.0.0/0
exit
interface ethernet 1
ip traffic-filter webonly
end
show running-config
write memory
```

line 10〜40 で、HTTP、HTTPS の通信を管理に使用する端末からのものだけ透過し、line 50〜70 で、NTP などほかの通信をこれまでどおり透過します。
設定は、本装置を再起動することなく反映されます。

- 192.0.2.10、webonly、ethernet 1 は、お使いの環境に合わせて変更してください。アクセス制御リスト名に使用できる文字は英小文字と数字で、1〜15 文字です。
- LAN1 以外の LAN にも IP アドレスを設定している場合はそのインターフェースにも、IPv6 アドレスでも使用している場合は IPv6 のアクセス制御リストも、同様に設定してください。

TS-2950 シリーズでは、Web ユーティリティからも同じ設定ができます（「導入・運用の手引き」の 3.5.3、3.5.5）。

9　回避策の設定方法（NS-2260 シリーズ、NS-2250 シリーズ）

まず、show service コマンドで<http>および<https>の status を確認してください。
どちらも disable の場合、設定は不要です。

使用していない場合

以下のコマンドで HTTP サーバー、HTTPS サーバーを無効にして、設定を保存してください。

```
disable http
disable https
write
```

使用している場合

IP フィルター機能で、HTTPS サーバー（標準のポート番号は 10443）に通信できる接続元を管理に使用する端末に限定します。
以下は、管理に使用する端末の IP アドレスが 192.0.2.10 の場合の設定例です。

```
create ipfilter input line 1 accept any any 192.0.2.10/32 tcp 10443
create ipfilter input line 2 drop any any any tcp 10443
enable ipfilter
write
```

1 行目で管理に使用する端末からの通信を透過し、2 行目でそれ以外の接続元からの通信を破棄します。
どちらの条件にも一致しない通信（ほかのサービスへの通信）は、これまでどおり透過します。

・HTTP サーバーも使用している場合は、ポート番号 10080 についても同じ 2 行を登録してください。
・set http port、set https port コマンドでポート番号を変更している場合は、変更後のポート番号を指定してください。
・すでにほかのフィルター条件を登録している場合は、この 2 行が先に評価されるよう、行番号を調整してください。
・IPv6 アドレスでも使用している場合は、create ip6filter、enable ip6filter コマンドで同様に設定してください。

コマンドの詳細については、「コマンドリファレンス」をご参照ください。

10 当社の対応

当社では、本脆弱性を修正したシステムソフトウェアを、以下の予定でご提供いたします ※。
修正版では、Web 管理画面、REST API で使用している PHP を、Version 8.5.12 に更新します。

製品	修正版のシステムソフトウェア	ご提供の予定日
TS-2560 シリーズ、TS-2220 シリーズ	Version 8.1.0	2026 年 11 月 17 日
NS-2260 シリーズ	Version 2.0.2	2026 年 11 月 17 日
NS-2250 シリーズ	Version 3.3.1	2026 年 11 月 17 日
TS-2950 シリーズ	Version 6.9.30	2026 年 11 月 25 日
TS-1550	Version 3.1.0	2026 年 11 月 25 日

予定日が変わる場合は、改めてお知らせいたします。
修正版を適用するまでの間は、「回避策」に記載の設定を継続してください。

※ 第 3 報で追加いたしました（第 2 報までは、ご提供の時期は決まり次第お知らせするとしておりました）。

11 お問い合わせ

本件に関するお問い合わせは、製品に応じて以下の窓口までお願いいたします。

製品	お問い合わせ先
タイムサーバー（型番が TS で始まる製品）、TD-450、TD-210	time.ce@seiko-sol.co.jp
コンソールサーバー（型番が NS で始まる製品）、SmartJumper	ns-support@seiko-sol.co.jp

以上