Rev. 1 2014.11.11



Express5800 シリーズ iStorageNS シリーズ SSL3.0 脆弱性問題回避 設定手順書

■ はじめに

ブラウザおよび Java アプレットならびに Java Web Start から起動される Java アプリケーションなどから SSL 3.0 プロトコルを利用しているとき、CVE-2014-3566 POODLE(Padding Oracle On Downgraded Legacy Encryption)と呼ばれる脆弱性を利用した攻撃により、暗号化された通信内容の一部を解読される可能性があります。この脆弱性につきましては、クライアントのブラウザおよび Java で SSL3.0を無効化し、TLS1.0 以降のプロトコルを有効にすることで対策することができます。

本手順書は、クライアントのブラウザおよび Java の SSL3.0 無効化の設定手順について記載しています。

【対象コンピュータ】

SSL3.0 をサポートする Web ブラウザおよび Java Runtime Environment がインスト ールされているコンピュータ。

【改版履歴】

Rev.	日付	主な改版内容
1	2014/11/11	• 初版制定

<u>目 次</u>

🔳 (a	よじめに	2
1	Web ブラウザ設定	4
2	Java 設定1	0

1 Web ブラウザ設定

以下、Web ブラウザを通じて操作を行うコンピュータ上での手順になります。

【Internet Explorer の場合】

Internet Explorer の[ツール]-[インターネットオプション]-[詳細設定]から[セキュリ ティ]メニュー内の SSL/TLS に関する項目を下記のように TLS1.0 以上のみが有効に なるように変更してください。

インターネット オプション [? 🗙
全般 セキュリティ プライバシー コンテンツ 接続 プログラム 詳細設定	
設定	
 エンコードされたアドレスを常に表示する セキュリティ DOM ストレージを有効にする POST の送信が POST を許可しないゾーンにリダイレクトされた場合に SmartScreen フィルター機能を有効にする SSL 2.0 を使用する 	
 SSL 3.0 を使用する TLS 1.0 を使用する TLS 1.1 の使用 TLS 1.2 の使用 オンラインからの攻撃の緩和に役立てるため、メモリ保護を有効にする* サーバーの証明書失効を確認する* ダウンロードしたプログラムの署名を確認する 	Ŧ
*Internet Explorer の再開後に有効になります。	
「新聞記でになっている」の「新聞」を定ちます。 「「「新聞」であります。 「「「新聞」であります。	
Internet Explorer の設定を明定の状態にリセットします。 リセット(S)	
ブラウザーが不安定な状態になった場合にのみ、この設定を使ってください。	
OK キャンセル 道	適用(A)

■●
重要
以下の製品については、Internet Explorer 9 以外の Internet Explorer をご使用ください。

 EXPRESSSCOPE エンジン3 搭載製品 以下の製品が対象です。

R110e-1E、R110d-1E、R110e-1M、R110d-1M、R110g-1E、R110f-1E

R120e-1M, R120d-1M, R120e-2M, R120d-2M, R120e-1E, R120d-1E, R120e-2E, R120d-2E

T110e-M、T110d、T110g-E、T110f-E、T110g-S、T110f-S、T120d、 T120e

E110d-1, E110d-M, E120d-1, E120d-M, E120e-M

GT110g、GT110f、GT110g-S、GT110f-S、GT110e、GT110d、GT110e-S、GT110d-S

B120d、B120d-h、B120e、B120e-h

NS300Rd, NS100Td, NS300Te, NS300Rb, NS100Tb, NS500Rc, NS500Rd, NS500Re, NS300Tc

MW400h2、CS400h2、LB400h2

V608-L/H[N8610-1011/1012] 、 V608-L/H[N8610-1021/1022] 、 V618-L 、 V618-H 、 V628-L 、 V628-H[N8610-1023 ~ 1028] 、 V608-L/H[N8610-1031/1032]、V628-H[N8610-1033~1038]

A1020a, A1020b

 EXPRESSSCOPE エンジン SP 3 搭載製品 以下の製品が対象です(*)。

A1040b、A2040b、A2020b、A2010b、R140e-4

(*) ただし、EXPRESSSCOPE エンジン SP 3 のファームウェアリビジョンが 1.14 より以前のリビジョンを適用の場合に限ります。

 EXPRESSSCOPE エンジン3 ft 搭載製品 以下の製品が対象です。

R320c-E4、R320c-M4、R320d-M4

 EXPRESSSCOPE エンジン SP 2 搭載製品 以下の製品が対象です。

A1080a-S, A1080a-D, A1080a-E, A1040a

【Firefox ESR の場合】

アドレスバーに「about:config」と入力してください。



「最新の注意を払って使用する」ボタンを押すと検索画面が表示されます。

 about:config - Mozilla Firefox ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) 	ツール(T) ヘルブ	^г (Н)		
about:config +				
Firefox about: config			☆ マ C 🛛 🕄 → Google	۹ 🖡
検索(R):				٩
設定名	▲ 状態	型	循	R
accessibility accessive visus esactivation	初期設定値	古偽庙	true	
accessibility blockautorefresh	初期設定値	百傷値	false	
accessibility browsewithcaret	初期設定値	百傷値	false	
accessibility browsewithcaret shortcut enabled	初期設定値	直傷値	true	
accessibility delay plugin time	初期設定値	整数值	10000	
accessibility delay plugins	初期設定値	真偽値	false	
accessibility force disabled	初期設定値	整数値	0	
accessibility mouse focuses formcontrol	初期設定値	真偽値	false	
accessibility tabfocus	初期設定値	整数値	7	
accessibility.tabfocus_applies_to_xul	初期設定値	真偽値	false	
accessibility.typeaheadfind	初期設定値	真偽値	false	
accessibility.typeaheadfind.autostart	初期設定値	真偽値	true	
accessibility.typeaheadfind.casesensitive	初期設定値	整数値	0	
accessibility.typeaheadfind.enablesound	初期設定値	真偽値	true	
accessibility.typeaheadfind.enabletimeout	初期設定値	真偽値	true	
accessibility.typeaheadfind.flashBar	初期設定値	整数値	1	
accessibility.typeaheadfind.linksonly	初期設定値	真偽値	false	
accessibility.typeaheadfind.prefillwithselection	初期設定値	真偽値	true	
accessibility.typeaheadfind.soundURL	初期設定値	文字列	beep	
accessibility.typeaheadfind.startlink.sonly	初期設定値	真偽値	false	
accessibility.typeaheadfind.timeout	初期設定値	整数値	5000	
accessibility.usebrailledisplay	初期設定値	文字列		
accessibility.usetexttospeech	初期設定値	文字列		
accessibility.warn_on_browsewithcaret	初期設定値	真偽値	true	-
	5m Hn 2n, -5 /	= ~~ ~+	· · ·	

ESR17 の場合

「検索」に"security.enable_ssl3"を入力して値を確認してください。

about: config - Mozilla Firefox ファイル(F) 編集(E) 表示(V) 風感(S) ブックマーク(B) ツール(T)) ヘルプ(H)				
about:config +					
♦ ⇒ ⊗ about:config				☆ マ C 🛃 - Google	₽ ♣ ♠ #-
🙆 よく見るページ 🔅 Firefox を使いこなそう <u>参</u> 最新ニュース 📈 B	3MC Web Console	190	ESMPRO/ServerMan		
検索(<u>R</u>): security.enable_ssl3		I			×
設定名	▲ 状態	型	値		Ę
security.enable_ssl3	初期設定値	真偽値	true		
services.sync.prefs.sync.security.enable_ssl3	初期設定値	真偽値	true		
x					

"true"の場合、「security.enable_ssl3」をダブルクリックすると"false"に切り替わります。

i about:config - Mozilla Firefox				÷	
ファイル(E) 編集(E) 表示(Y) 履歴(S) フックマーク(B) ツール	(日) ヘルプ(日)				
about:config +					
< 🔶 🌏 about:config				☆ ▼ C Google	₽ ♣ ♠ ₩-
🕗 よく見るページ 🗍 Firefox を使いこなそう 🔜 最新ニュース 属	BMC Web Console	190	ESMPRO/ServerMan		
検索(<u>R</u>): security.enable_ssl3					×
設定名	∧ 状態	型	値		Ę
security.enable_ssl3	ユーザ設定	真偽値	false		
services.sync.prefs.sync.security.enable_ssl3	初期設定値	真偽値	true		
X					

Web ブラウザを再起動してください。

ESR24.以降の場合

「検索」に"security.tls.version.min"を入力して値を確認してください。

about:config - Mozilla Firefox ファイル(E) 編集(E) 表示(Y) 履歴(S) ブックマーク(E) about:config +) ツール(I) ヘルフ	*(日)						×
O Firefox about: config				☆ ≂ e	🞖 + Google	Q	÷	⋒
検索(R): sequrity.tls.version.min								×
設定名	▲ 状態	型	値					
security, tils, version, min , services, sync, prefs, sync, security, tils, version, min	初期設定値 初期設定値	整数値 真偽値	0 true					

0の場合、「security.tls.version.min」をダブルクリックして表示されるウインドウから 1を入力して「OK」ボタンをクリックしてください。

整数値を	ミスカしてください
?	security.tls.version.min
	1
	OK キャンセル
	OK キャンセル

Web ブラウザを再起動してください。

2 Java 設定

Java がインストールされたコンピュータのコントロールパネルより Java を選択し、Java コントロールパネルを開きます。

🍰 Javaコントロール・パネル 📃 📼 🔜
一般 更新 Java セキュリティ 詳細
バージョン情報
Javaコントロール・パネルについてのバージョン情報を表示します。
バージョン情報(8)
ネットワーク設定
ネットワーク設定は接続時に使用されます。デフォルトでは、JavaはWebブラウザのネットワーク設定を使 用します。これらの設定を変更できるのは上級ユーザーのみです。
ネットワーク設定(N)
インターネット一時ファイル
Javaアプリケーションで使用されたファイルは、次回すばやく実行できるように特別なフォルダ内に格納されます。ファイルの削除や設定の変更を行えるのは上級ユーザーのみです。
表示(V)
ブラウザのJavaが有効になっています。 「セキュリティ」タブを参照
OK 取消 適用(A)

[詳細]-[高度なセキュリティ設定]から"SSL 3.0 を使用する"のチェックを外し、TLS1.0 以上のプロトコルにチェックを入れます。



保護紙

(このページは意図的に空白にしています)