2015.08.31 KDDI 株式会社

暗号化通信プロトコル「SSL 3.0」脆弱性の対応について

先般、インターネットで通信内容の保護に使用されている暗号化方式「SSL 3.0」において、 暗号化通信が解読される恐れがあるなどの深刻な脆弱性が見つかったと報じられました。

現在、弊社 Web サイトの一部でこの SSL3.0 を使用している為、セキュリティ保護対策と して、9月1日より SSL3.0 による通信を無効化し、SSL を基に強化・開発された暗号化方 式「TLS」通信に切替させて頂きます。

本対策により一部の古い Web ブラウザ(InterntExplorer・Google Chrome など)や通信設定 によっては、弊社 Web サイトが閲覧できなくなる可能性があります。

そのような場合には、以下の手順に沿ってお客さまが利用されている Web ブラウザの設定 を変更して頂くことで、安全な通信の暗号化(TLS1.0 以降)を使用して弊社 Web サイト を引き続きご利用頂くことが可能となります。

■Internet Explorer の設定確認と変更手順

ウィンドウ上部のメニュー「ツール」から「インターネットオプション」を選択します。
 ※メニューバーがない場合はウィンドウ右上の歯車マークから(下図)

		<u> </u>
	印刷(P) フライル(C)	Č.
	ンアイル(F) 拡大(Z) (100%)	
	セーフティ(S)	•
	ダウンロードの表示(N)	Ctrl+J
	F12 開発者ツール(L)	
_	ピンで固定されたサイト(G)	
	インターネット オプション(0)	
_	バージョン情報(A)	

- 2. インターネットオプションのダイアログボックス上部の「詳細設定」タブをクリックし ます。
- 3. 「セキュリティ」カテゴリにある「SSL3.0を使用する」のチェックを外します。
- 4. 「TLS1.0 を使用する」「TLS1.1 の使用」「TLS1.2 の使用」のチェックボックスにチェ ックが入っていない場合はチェックを入れます。
- 5. インターネットオプションダイアログの「OK」ボタンをクリックします。

インターネット オプション ? 2					
全般 セキュリティ ブライバシー コンテンツ 接続 ブログラム 詳細設定 2					
 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 マ DOM ストレージを有効にする マ 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 マ 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 マ TLS 1.0 を使用する マ TLS 1.0 の使用 マ TLS 1.1 の使用 マ TLS 1.2 の使用 マ 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* マ サーバーの証明書失効を確認する* マ ボッカードト・ホウログラムの署名を確認する 					
*Internet Explorer の再開版に有効になりより。 詳細設定を復元(R)					
Internet Explorer の設定をリセット Internet Explorer の設定を既定の状態にリセットします。 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 適用(<u>A</u>)					
nternet Explorer を再起動します。					

6. Internet Explorer を再起動します。

■Google Chrome の設定確認と変更手順

1.ウィンドウ右上「三」マークから「設定」を選択します。

	<u> </u>	×			
		☆=			
新しいタブ(T)	(Ctrl+T			
新しいウィンドウ(N)	(Ctrl+N			
シークレット ウィンドウを開く(I)	Ctrl+Shift+N				
履歴(H)	Ctrl+H				
ダウンロード(D)	Ctrl+J				
最近使ったタブ		+			
ブックマーク(B)					
拡大/縮小	- 100% +	53			
印刷(P)		Ctrl+P			
名前を付けてページを保存(A) Ctrl-		Ctrl+S			
検索(F)	(Ctrl+F			
その他のツール(L)					
編集 切り取り(T)	⊐ピー(C) 貼	O付け(P)			
設定(S)					
Google Chrome について(Google Chrome について(G)				
ヘルプ(H)	∧J <i>L</i> Ĵ(H)				
Windows 8 モードで Chrome を再起動					
終了(X)	終了(X) Ctrl+Shift+Q				

2.「詳細設定を表示」をクリックします。

☆ 設定	×		
← → C 🗋 c	hrome://settings		☆ =
Chrome	設定	設定項目を検索	-
履歴 拡張機能	 ホームホッンで表示する ブックマークバーを常に表示する 		
設定	検索		
概要	アドレスバー から検索するときに使用する検索エンジンを設定します。 Google 検索エンジンの管理 「OK Google」による音声検索の開始を有効にする 詳しく見る 新しいタブで google.com を開き、「OK Google」と発声します		
	ユーザー		
	 ダストのブラウジングを許可する だれでも Chrome にユーザーを追加できるようにする ユーザーを追加…」 福集…」 剤除…」 ブックマークと設定をインボート… 		
	既定のブラウザ Google Chrome を既定のブラウザにする 現在、Google Chrome は既定のブラウザに設定されていません。 詳細設定を表示。		

3.「ネットワーク」の「プロキシ設定の変更」ボタンをクリックします。

◆ 設定	×	≛ _ □ ×
← → C	C chrome://settings	☆ =
Chrome 國際	設定 調査 - 調査 - コー -	•
拡張機能	パスワードとフォーム	
設定	🕢 ワンクリックでのウェブ フォームへの自動入力を有効にする 自動入力設定の管理	
柳亜	🕢 パスワードの保存を確認する パスワードを管理	
104.54	ウェブ コンテンツ	
	フォントサイズ: 中 ▼ ページのズーム: 100%	
	ネットワーク Google Chrome は、コンピュータのシステムプロキシ設定を使用してネットワークに接続しています。 プロキシ設定の変更… 言語	
	これの時にとなる当時の久生となりの方面とまたすの <u>年にくれな</u> ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	
	ダウンロード保存先: ChUsershtanaka_2Downloads 変更	

4.Internet Explorer の手順2から手順5と同様の手順で設定します。

5.GoogleChrome を再起動します。

■注意事項

SSL3.0の設定を外した後は、TLSをサポートしないWebサイトに接続できなくなります。 また、一部の携帯電話(フィーチャーフォン)からはセキュリティの問題でアクセスでき なくなる場合があります。機種ごとの対応詳細につきましては、書く携帯電話事業者へご 確認ください。

以上