

SSL3.0の脆弱性に対する対応について

愛知県共済生活協同組合

インターネット通信で使用する暗号化方式「SSL 3.0」において脆弱性が発見され、暗号化されている通信の内容が第三者に漏えいする可能性があるとして報じられたことを受け、当組合サイトにおいてもSSL3.0の利用を停止いたしました。当組合のサイトは、この脆弱性の影響を受けない暗号化方式「TLS」に対応しておりますので、「SSL 3.0」を無効化することをおすすめします。

「SSL 3.0」の脆弱性対策について、詳しくは独立行政法人 情報処理推進機構 (IPA) のサイトでご覧いただけます。

[SSL 3.0 の脆弱性対策について\(CVE-2014-3566\)](#)

[推奨する対処方法]

Internet Explorerでは、設定を変更することにより、「SSL 3.0」を無効化することができます。

1. Internet Explorer の [ツール] メニューの [インターネット オプション] をクリックします。
2. [インターネット オプション] ダイアログ ボックスの [詳細設定] タブをクリックします。
3. [セキュリティ] カテゴリで、[SSL 3.0 を使用する]のチェック ボックスをオフにし、[TLS 1.0 を使用する]、[TLS 1.1 の使用]、および [TLS 1.2 の使用]のチェック ボックスをオンにします。
4. [OK] をクリックします。
5. 終了し、Internet Explorer を再起動します。

※SSL3.0を無効としても、TLSを有効としていただくことで、セキュリティが低下することはありません。

