情報セキュリティ

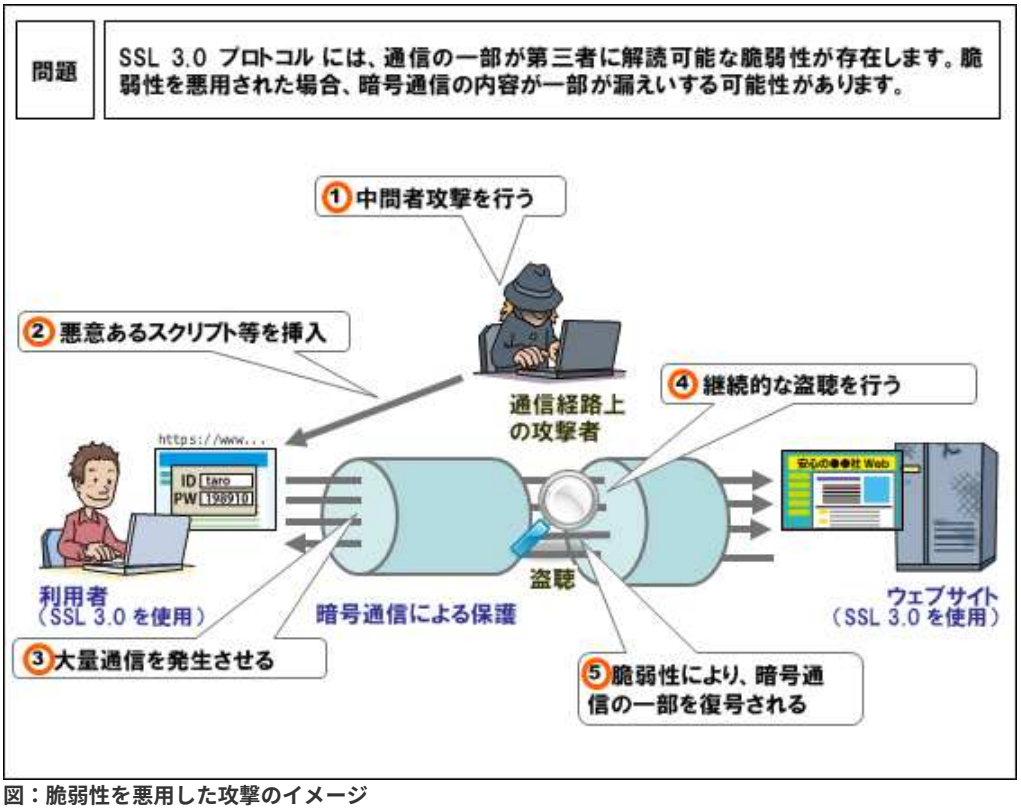
更新：SSL 3.0 の脆弱性対策について(CVE-2014-3566)

最終更新日：2014年10月30日

※追記すべき情報がある場合には、その都度このページを更新する予定です。

概要

SSL 3.0 プロトコルには、通信の一部が第三者に解読可能な脆弱性が存在します。サーバ、クライアント間の通信において、SSL 3.0 を使用している場合、通信の一部が第三者に漏えいする可能性があります。
ただし、攻撃には複数の条件が必要で、例えば、中間者攻撃や、攻撃対象に大量の通信を発生させるなど一定の条件が必要になります。そのためただちに悪用可能な脆弱性ではありません。
サーバ管理者および利用者は対策の要否を検討し、必要に応じて後述の対策を実施してください。



図：脆弱性を悪用した攻撃のイメージ

対策

サーバもしくはクライアントのどちらか一方で、SSL 3.0 を無効化することで対策できます。
なお、SSL 3.0 を無効化することで次の影響を受ける可能性があります。

サーバ側で SSL 3.0 を無効にした場合
一部のクライアントから接続ができなくなる可能性があります。
クライアント側で SSL 3.0 を無効にした場合
一部のサーバに接続できなくなる可能性があります。

サーバ管理者向け対策

Windows における SSL 3.0 の無効化
マイクロソフトから Windows で SSL 3.0 を無効化する方法が公開されています。
下記 URL に記載されている回避策の 「サーバー ソフトウェア用」 を実施してください。

https://technet.microsoft.com/ja-jp/library/security/3009008.aspx

Apache Http Server における SSL 3.0 の無効化
レッドハットから Apache Http Server で SSL 3.0 を無効化する方法が公開されています。
下記 URL に記載されている設定変更を実施してください。

https://access.redhat.com/ja/solutions/1232613

利用者向け対策

ブラウザごとの対策情報を参照し、SSL 3.0 を無効化してください。

- Internet Explorer
  Internet Explorerは、設定を変更することにより、SSL3.0を無効化することができます。詳しくは、下記URLのマイクロソフト セキュリティアドバイザリを参照してください。
  マイクロソフト セキュリティ アドバイザリ 3009008
  https://technet.microsoft.com/ja-jp/library/security/3009008.aspx

  2014年10月30日追記
  Microsoft 社から、回避策として新たに「Fix it」が公開されました。 下記 URL に記載されている回避策の 「Fix it ツールを利用する」 を実施してください。
  http://blogs.technet.com/b/jpsecurity/archive/2014/10/30/3009008-ssl3-rev.aspx

- Firefox
  Firefox は、次期バージョンからデフォルトで SSL 3.0 を無効化すると発表しています。
  Mozilla Security Blog(English)
  https://blog.mozilla.org/security/2014/10/14/the-poodle-attack-and-the-end-of-ssl-3-0/

  2014年10月30日追記
  現行バージョンの Firefox で SSL 3.0 を無効化するアドオンが公開されています。
  Mozilla Japan ブログ
  http://www.mozilla.jp/blog/entry/10433/

- Chrome
  現時点で Google 社からは SSL 3.0 を無効化する方法は公開されていませんが、数ヵ月後には SSL 3.0 のサポートを完全に打ち切る予定であると発表しています。

This POODLE bites: exploiting the SSL 3.0 fallback(English)
http://googleonlinesecurity.blogspot.jp/2014/10/this-poodle-bites-exploiting-ssl-30.html

参考情報

- CVE-2014-3566
  http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566
- OpenSSL およびその他の製品で使用される SSL プロトコルにおける平文データを取得される脆弱性
  http://jvndb.jvn.jp/ja/contents/2014/JVNDB-2014-004670.html
- SSLv3 プロトコルに暗号化データを解読される脆弱性(POODLE 攻撃)
  https://jvn.jp/vu/JVNVU98283300/index.html

本件に関するお問い合わせ先

IPA　技術本部　セキュリティセンター

E-mail： vuln-inq@ipa.go.jp

更新履歴

2014年10月30日　　対策：追記

2014年10月17日　　掲載