

BACREX

自動送受信パックユーザーの皆様へ



**SSL3.0の脆弱性に対する弊社製品及び関連サービスへの影響と対策について**

謹啓、平素は弊社製品並びに弊社業務に格別のご高配を賜り厚く御礼申し上げます。

さて、米国のGoogleのセキュリティチームが、現地時間10月14日(火)にSSL 3.0の脆弱性「POODLE」(Padding Oracle On Downgraded Legacy Encryptionの略：プードル)を発表したことにより、国内のニュース等でも大きく報道されておりますが、情報処理推進機構(IPA)が10月17日に「ただちに悪用可能な脆弱性ではない」としたうえで注意喚起情報を掲載しました。(詳細については下記のURLをご参照ください。)

弊社では、安心・安全にお使いいただくために本事象に対する弊社製品及び関連サービスに対して対策を進めておりますのでご案内いたします。一部、対応策に未確定な部分があるため、中間報告としてのご提示がありますが、何とぞご理解とご協力をお願い申し上げます。

尚、最新情報については、弊社HPなどで随時更新してご提供いたします。

本件について、ご不明の点などございましたら、担当窓口にお問い合わせください。

敬具

記

○情報処理推進機構(IPA)の注意喚起：

SSL 3.0の脆弱性対策について (CVE-2014-3566)

<https://www.ipa.go.jp/security/announce/20141017-ssl.html>

1. 弊社製品及び関連サービスへの影響について

(1) この脆弱性を悪用するには、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複雑な条件が必要になります。弊社製品及びサービスにおいて、ただちに、深刻な脅威となる可能性は低いと考えます。

(2) 現時点では、SSL3.0を使用しないプロトコル抑止設定を行わないでください。

弊社製品に限らず、インターネットなど通信を利用する場合、サーバ側とクライアント側とでは利用するプロトコルのバージョンに双方が対応している必要があります。本脆弱性に対する一般的な対策方法として、WEBサーバ側やクライアント側でSSL 3.0プロトコルを使用せず、TLSを利用可と設定を変更する方法が公開されていますが、どちらか一方がこのような設定を行った場合、クライアント製品やブラウザ(インターネットエクスプローラ：以下IE)での接続ができなくなる可能性があります。

## 2. クライアント側弊社製品の今後の対応について

今後は、より安全・安心にご利用いただくため、SSL3.0 を使用しない設定を推奨する予定ですが、現時点ではサーバ側の対応の可否により接続できなくなる可能性があります。

(1) ブラウザ (IE) のオプション設定によって抑止が可能です。

(2) 自動送受信パックパックご利用の場合

### a. Ver.4 シリーズの場合

SSL3.0 での通信を基本としているため、現在、TLS 通信を可能とするパッチを準備中です。このパッチを適用することにより TLS 最新バージョンから順に接続するようになるため、サーバ側が TLS に対応している場合、SSL3.0 での通信は行われません。

準備ができ次第、弊社 HP などで公開、提供いたします。

### b. Ver.3 シリーズの場合

ブラウザ (IE) のオプション設定に準拠した動作となります。

SSL3.0 を不可とし、TLS を可とした場合、TLS での通信となります。

現時点でもオプション設定による抑止は設定可能ですが、サーバ側が対応できない場合、接続できなくなる可能性があります。

## <参考情報>

### ■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>

### ■JVN 脆弱性対策情報データベース

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>

以上

□本件に関するお問い合わせ先

#### 1. 株式会社ニュートラル札幌本社

BACREX サポート E-mail : bacrex-support@neutral.co.jp

TEL : 011-290-5688 FAX : 011-290-5687 担当 : 岩木・山岸

#### 2. 株式会社ニュートラル東京オフィス

BACREX 販売パートナー事務局 E-mail : partner@neutral.co.jp

TEL : 03-5575-3655 FAX : 03-5575-3654 担当 : 北岡