OPENTEXT™

POODLE の脆弱性

よくある質問（FAQ）

このドキュメントの使用方法

この FAQ では、POODLE の脆弱性に関してお客様からもっともよく寄せられる質問への回答を一部紹介したものです。この文書は変更されることがあり、http://techsupport.gxs.com/で定期的にアップデートされます。

POODLE とは

POODLE は、**P**adding **O**racle **O**n **D**owngraded **L**egacy **E**ncryption（ダウングレードしたレガシー暗号通信でのパディングオラクル）の略です。セキュリティの問題は、その名前が示すとおり、古い形式の暗号を悪用できるプロトコルのダウングレードにあります。この問題は、Google が This POODLE Bites:Exploiting The SSL 3.0 Fallback（プードルにかまれる：SSL3.0 フォールバックの悪用）と呼ばれる論文を発表して以来、世界の注目を集めるようになりました。

POODLE の仕組み

POODLE では、接続をセキュアソケットレイヤー（SSL）バージョン 3.0 に強制的に「フォールバック」する**中間者攻撃（man-in-the-middle attack）**を実行して、ユーザーの機密情報を手に入れることが可能になります。情報漏えいの危機にさらされるデータは、有効な SSL 接続の種類によって異なります。

脆弱性は、中と評価されています。つまり、この問題によりデータ要素の機密性、統合性および可用性は危険にさらされる可能性がありますが、これが実行されるには 1 つ以上の前提条件が必要となります。POODLE 攻撃は、実行するのが非常に困難で、1 バイトのデータを入手するのに 250 回以上のトランザクションを試行する必要があります。

お客様を守るために OpenText が行っていること

OpenText のセキュリティ専門家は、現在 POODLE に関連するリスクを分析しています。必要に応じて、OpenText は SSL バージョン 3 以前を無効にして、GXS 通信ゲートウェイへのアクセスを禁止します。その代わりに OpenText は、POODLE 攻撃から保護するための推奨プロトコルであるトランスポート層セキュリティ（TLS）を使用します。

どういった影響があるか

セキュアソケットレイヤー（SSL）バージョン 3（SSLv3）をサポートするすべてのサービスは悪用される可能性があり、攻撃者がセキュアなセッションの暗号を解読したり、場合によってはユーザーデータを入手することができるようになります。

接続が POODLE 攻撃に脆弱になるのは、送信側と受信側が両方とも SSLv3 をサポートする場合のみです。SSLv3 をすでに無効にしている場合、上記の問題の影響は受けません。OpenText では、お客様が社内アプリケーション管理者またはソフトウェアプロバイダーに問い合わせて、サービスの接続に TLS 1.0 以降（SSLv3 を無効にした状態で）を使用していることを確認するよう推奨します。

お客様がしなくてはならないこと

OpenText は、段階的に影響を受けた通信ゲートウェイのプロトコルを更新します。修復計画はまだ検討中で、切り替えの日程の詳細については後ほどご連絡します。お客様は、計画された切り替え日時の前に相応な変更通知を受け取ります。

その間、お客様は通信ソフトウェアがフォールバックモードの TLS（TLS 1.2、1.1、および 1.0）をサポートすることを確認してください。可能である場合は、直ちに SSL を無効にすることを推奨します。SSL を無効にする方法に関して質問がある場合は、担当のソフトウェアプロバイダーにお問い合わせください。

POODLE の攻撃を受けるブラウザ

ブラウザベースのアプリケーションの場合、SSLv3 を使う Web ブラウザはすべて危険にさらされます。最新のウェブブラウザ（Chrome、Firefox、Safari、および Internet Explorer 9 以降）のほとんどは、TLS1.0 以降を使用していますが、Internet Explorer 6 などのレガシーブラウザは SSLv3 しかサポートしません。つまり、旧型の PC やブラウザバージョンを使用するユーザーは、POODLE による脆弱性の影響を受ける可能性があります。

ブラウザを更新せずに OpenText サービスにアクセスしようとすると、アカウントはどうなりますか。

お客様のアカウントはシャットダウンされませんが、接続が拒否され OpenText サービスにアクセスできなくなります。

POODLE 攻撃に脆弱な接続方法はどれですか。

OpenText 情報セキュリティは、OpenText サービスへの接続に使用されるさまざまな通信プロトコルに POODLE が示すリスクを判断する分析を行っています。SSL のセキュリティ機能を使用する通信プロトコルのリストには、次が含まれます。

- HTTPs
- FTPs
- AS2
- RosettaNet

- OFTP
- MQ
- AS3

お客様またはお客様の取引先が上記の通信プロトコルのいずれかを使用する場合、すぐに何か対策を取る必要はありません。OpenText は、SSL を無効にする必要があるプロトコルを判断するため、各プロトコルのリスク分析を行っています。影響を受けたお客様は、計画された切り替え日時の前に相応な変更通知を受け取ります（通常 60 日前）。

SSLv3 を無効にする方法

ブラウザ：
ブラウザで SSLv3 サポートを無効にする方法については、インターネット上でさまざまなリソースを入手することができます。たとえば、https://zmap.io/sslv3/browsers.html などがあります。

接続ソフトウェア：
サードパーティのソフトウェアパッケージを使って当社のサービスに接続しているお客様は、担当のソフトウェアプロバイダーにすぐに連絡して、TLS がサポートされており、SSL を安全に無効化できることを確認されることを推奨します。

自分のサービスが修復計画によって影響を受けるかどうか、どのようにわかるのですか。

各通信プロトコルについてのお客様への通知には、SSL のセキュリティ機能を使用し、修復計画の対象となるゲートウェイの URL が含まれています。ゲートウェイの URL の一覧をご覧になるには、当社のウェブサイトを訪問し、お使いの通信プロトコルについての通知をダウンロードしてください。

私の通信ゲートウェイの SSL がオフになるのはいつですか。

OpenText は、段階的に影響を受けた通信ゲートウェイのプロトコルを更新します。修復計画はまだ検討中で、切り替えの日程の詳細については後ほどご連絡します。すでに修復された通信プロトコル用の日程を確認するには、当社のウェブサイトをご覧ください。

私のシステムは、トランスポート層セキュリティ（TLS）をサポートできません。どうしたらよいのですか。

OpenText は、POODLE の脅威に対処するための最も効果的な方法として SSL を無効にすることをお勧めしますが、当社はすべてのお客様がトランスポート層セキュリティ（TLS）をサポートできるわけで

はないことを理解しております。お客様が TLS をサポートできない場合には、お客様が SSL を使用して GXS ネットワークへのアクセスを継続することができる例外リストを OpenText GXS が確立しております。SSL の使用を継続するためには、お客様の会社を当社の例外リストに追加するために当社のウェブサイトを訪問していただく必要があります。

私の取引先についてはどうですか。

通信ゲートウェイの修正が行われたため、お客様と取引先には、OpenText GXS 通信ゲートウェイとのメッセージ交換接続を確立するために、TLS を使用していただく必要があります。お客様は、今後の POODLE 修復の準備をするために必要な活動について、取引先に通知する責任があります。

OpenText サービスに直接接続する取引先がおらず、トランスポート層セキュリティ（TLS）をサポートできず、例外リストに追加されることをお望みの場合には、ご自分の IP アドレスを OpenText に提供していただく必要があります。

詳細についての連絡先

質問がある場合やその他のサポートを必要とする場合は、指定の問い合わせ先情報を使って担当のサポート機関に連絡するか、各国の問い合わせ先情報を **OpenText ウェブサイト**で参照してください。

About OpenText

OpenText provides Enterprise Information Management software that helps companies of all sizes and industries to manage, secure and leverage their unstructured business information, either in their data center or in the cloud. Over 50,000 companies already use OpenText solutions to unleash the power of their information. To learn more about OpenText (NASDAQ: OTEX; TSX: OTC), please visit www.opentext.com.

www.opentext.com

NORTH AMERICA +800 499 6544 • UNITED STATES +1 847 267 9330 • GERMANY +49 89 4629 0

UNITED KINGDOM +44 0 1189 848 000 • AUSTRALIA +61 2 9026 3400