OPENTEXT™

SHA-2 証明書への移行

よくある質問（FAQ）

この文書の使用方法

この FAQ では、当社の SHA-1 から SHA-2 証明書への移行予定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 http://www.opentext.com/campaigns/sha2 で公表される予定です。

SHA-2 とは何ですか?

SHA-2 は暗号ハッシュアルゴリズムの一種で、2001 年に米国の国家安全保障局（National Security Agency）が発表しました。SHA は「安全なハッシュアルゴリズム」（Secure Hash Algorithm）の略です。SHA のハッシュ機能は、TLS や SSL のようなセキュリティアプリケーションやプロトコルで、公開鍵アルゴリズムと組み合わせて暗号化とデジタル署名の両方で使用されています。

OpenText が SHA-1 から SHA-2 証明書へ移行するのはなぜですか?

近年の暗号攻撃法の進歩に伴い、SHA-1 証明書を使用していると、攻撃者によるコンテンツのなりすまし、フィッシング攻撃、中間者攻撃などが可能になってしまうと、ネットワークセキュリティの専門家は警告しています。この潜在的な脆弱性は OpenText™ Trading Grid™、OpenText Information Exchange, OpenText EasyLink GMS、または OpenText EasyLink ICC.Net に存在するものではありませんが、最高レベルのデータの完全性およびお客様のセキュリティを維持するための当社の継続的な取り組みの一環として、SHA-2 証明書に移行します。

SHA-2 が使用する暗号ハッシュは格段に強力であり、SHA-1 と同様の脆弱性は存在しません。

お客様の社内システムが SHA-2 をサポートするかどうかを確認するには、https://www.digicert.com/sha-2-compatibility.htm を参照してください。

SHA-2 に移行するために、OpenText は何をしていますか?

OpenText は、現在の証明書の失効に合わせて、すべての証明書を SHA-2 に一新します。当社は、SHA-1 から SHA-2 証明書への移行を **2017 年 1 月 1 日**までに完了することを予定しています。この日は、Microsoft®が、同社の SHA-1 証明書のサポートを打ち切ると発表している日でもあります。SHA-2 証明書は、現在の当社の認証局である Comodo によって発行される予定です。

注：当社は、お客様と取引先がテストする時間を確保できるように、運用前環境の証明書を失効以前にアップグレードすることがあります。

どういった影響があるのですか?

お客様またはお客様のお取引先様が FTPS、AS2、RosettaNet、OFTP、MQ、AS3 等の、Trading Grid™、Information Exchange, EasyLink GMS、または EasyLink ICC.Net との間でデジタル署名または暗号化されたメッセージ交換接続を確立するプロトコルを使用している場合は、お客様の SHA-1 証明書を SHA-2 証明書に置き換え、セキュリティ保護を強化する準備を始めることが推奨されます。

私は何をする必要がありますか?

この変更の準備として、またスムーズな証明書の更新を確実なものとするため、以下を実施してください。

1. お客様の通信ソフトウェアが Comodo が発行する SHA-2 証明書をサポートすることを、お客様のサービスやソフトウェアプロバイダーに確認します。
    a. サポートしている場合は、お客様の現在の OpenText 公開鍵証明書が失効した時点でより安全な SHA-2 証明書に移行するための調整の準備はできています。
    b. サポートしておらず、お客様の現在の通信ソフトウェアプロバイダーの援助を受けられない場合は、お客様を担当する OpenText のカスタマーマネージャーにご相談ください。お客様がご利用できる選択肢を検討いたします。
2. お客様の取引先に連絡し、取引先の通信ソフトウェアが Comodo が発行する SHA-2 証明書をサポートすることを、取引先のソフトウェアプロバイダーに同様に確認してもらいます。

証明書の更新手順に変更がありますか?

証明書の更新手順には変更がありません。ただし、OpenText は証明書の失効日以前に証明書を SHA-2 に更新し、2017 年 1 月 1 日という期日よりも前にコンプライアンスを確実にすることがあります。

現在の OpenText 公開鍵証明書が 2016 年 12 月 31 日よりも後に失効する場合はどうなりますか?

OpenText は現在の OpenText 公開鍵 SHA-1 証明書を使っているお客様に積極的に連絡し、2017 年 1 月 1 日という期限までに SHA-2 へ移行するようお手伝いします。

この変更でどのサービスが影響を受けますか?

この変更は、SSL ブラウザー証明書すべてと、一部の通信プロトコルに影響があります。最近のウェブブラウザーを使って OpenText に接続しているのであれば、この証明書のアップグレードによる悪影響はありません。

注：現状では、*SSH*、*PGP*、または *GPG* の暗号鍵には影響ありません。

この変更でどのプロトコルが影響を受けますか?

SHA-2 証明書への移行によって、以下のプロトコルに影響があります。

- AS2
- AS3
- HTTPS
- SSL-FTP（FTPS）
- RosettaNet
- MQ
- Sterling/IBM – Connect:Direct Secure Plus

現在、OpenText はどの SHA-2 ハッシュ関数をサポートしますか?

現時点では、OpenText は以下の SHA-2 のバージョンによって署名された証明書をサポートします。

- SHA256
- SHA384
- SHA512

将来は、OpenText はこれ以外のタイプの SHA-2 証明書もサポートすることを予定しています。詳細は、利用可能になる時点でお知らせします。

私の通信ソフトウェアは SHA-2 証明書をサポートしません。どうしたらよいのですか?

OpenText は、データの完全性とセキュリティを維持するための最も効果的な方法として SHA-2 証明書へ移行することをお勧めしますが、すべてのお客様が SHA-2 証明書をサポートできるわけではないことも理解しています。

お客様のソフトウェアが SHA-2 または自己署名証明書をサポートしない場合は、証明書交換チームがお客様と協力し、最大 1 年間代替策を提供する予定です。2015 年 12 月 31 日以降は、OpenText は代替証明書発行オプションを提供しません。2016 年からは、証明書交換チームは SHA-1 証明書を発行するオプションをすべて無効にします。お客

様は SHA-2 証明書または自己署名証明書に移行する必要があります。その時点でも、お客様が SHA-2 証明書をサポートできない場合は、証明書交換チームが自己署名の SHA-1 証明書を実装するよう、お客様に協力します。

証明書交換チーム

E メール：CertificateExchange@opentext.com
電話：米国 1-800-334-2255 内線 2378

Comodo とは何ですか?

Comodo は OpenText の主要な認証局です。認証局とは、デジタル証明書を発行し管理する組織です。詳しくは、www.comodo.com を参照してください。

OpenText が Comodo を採用したのはなぜですか?

Comodo は最高レベルの暗号技術を利用したデジタル証明書の完全なラインアップを提供しているうえ、エンタープライズ用途に適した技術力と柔軟性を備えているので、OpenText は Comodo を採用しました。Comodo は WebTrust 認証を取得した認証局（CA）であり、機密性、システムの信頼性、および適正な業務手順に関する最高レベルの規準を満たしていることが、権限のある独立した監査によって認められています。

Comodo に切り替えることによって私のサービスに影響がありますか?

Comodo が発行する証明書への切り替えによって、新しいファイル交換製品にはほとんど影響がないはずです。Comodo は比較的新しい認証局であるため、古いファイル交換製品（概ね 10 年以上前の製品）を使い続けているお客様は、その製品の証明書ストアへのルート証明書と中間証明書の読み込みの際に問題が起きるかもしれません。詳しくは、Comodo のウェブサイト www.comodo.com を参照してください。

注：お客様が古いファイル交換製品または自社開発したソフトウェアを使っている場合は、証明書チェーン（*.p7b* ファイル）に含まれるすべての証明書を読み込む必要があります。*.cer* 形式を使う場合は、*Comodo* の三つの証明書のすべてが証明書ストアに読み込まれていることを確認してください。

詳細についての連絡先はどこですか?

詳細については、OpenText Trading Grid/Information Exchange のお客様はクラウドサポートサービスまでご連絡ください。

OpenText EasyLink GMS および ICC.Net のお客様は OpenText EasyLink カスタマーサポートまでご連絡ください。

Sterling Connect:Direct のユーザーのみ

私が使っている Sterling Connect:Direct のバージョンが SHA-2 に対応しているかどうか、どうすればわかりますか?

Sterling Connect:Direct の SHA-2 サポートについての詳細は、IBM のウェブサイトにある SHA-2 Support というガイドを参照してください。このガイドには、以下のリンクからアクセスできます。

ftp://ftp.software.ibm.com/software/commerce/doc/mft/cdcommon/secplus_SHA2SupportForCD_Book.pdf

「***Table 2. SHA-2 Compatible Software***」（表 2. SHA-2 と互換のあるソフトウェア）を参照して、お使いの Connect:Direct のバージョンが SHA-2 をサポートするかどうかを確認します。お使いのバージョンが SHA-2 と互換がない場合、いくつかの選択肢が考えられます。例えば、以下のような対策があります。

1. Connect:Direct ソフトウェアを、SHA-2 をサポートするバージョンにアップグレードします。
2. OpenText の担当者に連絡し、データ転送用に他のプロトコルをインストール/設定します。

注：お客様が OpenText を使って**インバウンド**ファイルを送信するのみであれば、何も問題が起きないかもしれません。しかし、お使いのシステムが SHA-2 証明書をサポートできなければ、OpenText はデータファイルを送信することができなくなります。

Connect:Direct を使って OpenText に接続するための一般的な前提条件はどのようなものですか?

一般的な前提条件には以下のようなものがあります。

- OpenText はお客様が用意したルート認証局および/または中間証明書を当社の信頼されたストアにインストール/追加することしか行いません。

- OpenText に送信する証明書は自己署名にしません。OpenText は自己署名証明書を受け付けません。
- クライアント認証は無効にします。
- OpenText は、証明書が base64 エンコード形式になっていることを推奨します。
- すべての暗号スイートを Secure Plus のセットアップに追加します。
- OpenText を TLSv1 用に設定します。

OpenText との接続を有効にするために Connect:Direct システムにインストールする必要のある証明書はどれですか?

お客様は、以下の新しい証明書を個別のファイルとしてインストールすることが必要になります。

- 公開証明書（チェーンに含まれる証明書を含んでいる必要があります。）
- 中間証明書（チェーンにルート CA を含んでいる必要があります。）
- ルート CA 証明書

新しい証明書をどうすればいいのですか?

お客様は該当する証明書を、お使いの Secure Plus の OpenText の Connect:Direct ノード用セットアップにインストール/追加する必要があります。お客様の社内の技術担当者および/または IBM のサポートにご相談ください。

OpenText の以前の証明書は削除するのですか?

以前の証明書を削除する必要があるかどうかは、個々の Connect:Direct Secure Plus のセットアップによって異なります。お客様の社内の技術担当者および/または IBM のサポートにご相談ください。

SHA-2 証明書のサポートには、他にも Secure Plus の設定が必要ですか?

必要ありません。しかし、お客様の方針により、以下の変更を行うこともできます。

- すべての暗号スイートを Secure Plus のセットアップに追加します。
- 安全性が低い、またはすでに破られている暗号スイートを削除します。

SHA-2 証明書を使ったテストを行う必要がありますか?

OpenText は、お客様が新しい証明書を使ってテストを行い、それが正しく機能することを確認するようお勧めします。何か問題が起きた場合は、クラウドサポートサービスに製品サービスリクエストを出してください。

私の証明書が失効するとどうなりますか?

証明書の失効とは、通常は、公開証明書の失効を意味し、中間証明書やルート CA 証明書は失効していない状態です。多くの場合、お客様は実際の証明書に関して何もする必要はありません。それは、中間証明書および/またはルート CA 証明書には変更がないからです。中間証明書および/またはルート CA 証明書が新しくなった場合は、それを信頼されたストアに追加してください。

About OpenText

OpenText enables the digital world by simplifying, transforming, and accelerating enterprise information needs, on premises or in the cloud. For more information about OpenText Cloud Services (NASDAQ: OTEX, TSX: OTC) visit www.gxs.com.

Connect with us:

- OpenText CEO Mark Barrenechea's blog
- Twitter | LinkedIn | Facebook