マーチャントセキュリティ

システムアップグレードガイド

SHA-256 準拠に関する情報はこちらをクリックしてください。

ご使用の実装環境を今後も安全にご利用いただくために

セキュリティ上の脅威は絶えず変化しています。お客さまのセキュリティは常に PayPal の最優先事項です。現在だけではなく将来の脅威にも備えるため、PayPal では、お客さまの実装環境において、以下のアップグレードを推奨しています。

1. VeriSign G2 ルート証明書の使用の中止
2. SHA-256 アルゴリズムを使用した証明書に対応するための実装環境の更新

変更理由

公的認証局(CA)の業界は、SSL 証明書のセキュリティ改善に常に取り組んでいます。2016 年から SHA-256 署名アルゴリズムの使用が必須になることを控え、VeriSign G2 ルート証明書のサポートは終了します。VeriSign G2 ルート証明書は、PayPal API および IPN (Instant Payment Notification)のエンドポイントへの接続に長く使用されてきました。

対応が必要な時期

これら変更に備えてできるかぎり早急に対応されることをお勧めします。本番環境および Sandbox の API エンドポイントのアップグレード日を含む詳しいスケジュールは、PayPal の 2015-2016 SSL Certificate Change Microsite(2015-2016 SSL 証明書変更のマイクロサイト)をご覧ください。

NOTE: これらの変更は、業界全体のセキュリティの問題に対応するもので、PayPal に限った変更ではありません。アップグレードが完了すると、PayPal 実装環境のプライバシーと信頼性が向上します。これらの変更の詳細はシステムによって異なりますので、システム管理者のサポートを受けながら変更されることをおすすめします。

1. VeriSign G2 ルート証明書の使用の中止

問題: VeriSign では以前、1024 bit G2 ルート証明書によって署名された信頼チェーンを含む SSL 証明書を発行していました。ここ数年は、米国政府および公的な認証局の業界が、より安全な 2048 bit の証明書に移行してきたため、現在 VeriSign は、2006 年に発行された 2048 bit G5 ルート証明書によって署名された信頼チェーンを含む SSL 証明書を発行しています。

PayPal の対応: 業界標準にしたがい、G2 ルート証明書によって署名される PayPal の証明書/信頼チェーンが求められる API/IPN エンドポイントへのセキュアな接続の対応を終了します。セキュアな接続ができるのは、G5 ルート証明書によって署名される証明書/信頼チェーンが求められるセキュアな接続リクエストのみです。

必要な対応

現在システムからの要求により VeriSign ルート証明書が使用されている場合、G2 識別子の付与された証明書に依存する SSL 接続の使用を中止する必要があります。業界では、年内に 1024 bit のルート証明書の使用を順次中止するよう積極的に取り組んでいます。

- G2 ルート証明書によって署名された証明書チェーンに依存するセキュアな接続はサポートされません。

組織単位	Class 3 Public Primary Certification Authority - **G2**
シリアル番号	7d d9 fe 07 cf a8 1e b7 10 79 67 fb a7 89 34 c6
証明書のフィンガープリント (SHA1)	85 37 1c a6 e5 50 14 3d ce 28 03 47 1b de 3a 09 e8 f8 77 0f

- G5 ルート証明書によって署名された証明書チェーンに依存するセキュアな接続はサポートされます。

コモンネーム	VeriSign Class 3 Public Primary Certification Authority - **G5**
シリアル番号	18 da d1 9e 26 7d e8 bb 4a 21 58 cd cc 6b 3b 4a
証明書のフィンガープリント (SHA1)	4e b6 d5 78 49 9b 1c cf 5f 58 1e ad 56 be 3d 9b 67 44 a5 e5

これらのガイドラインにしたがって、サポートされている VeriSign G5 ルート証明書を使用してセキュアに接続していることを確認します。

1. **証明書ストアを確認します。**サイト管理者またはシステム管理者に、検証ロジックのコードによって使用されているルートストアに VeriSign G5 ルート証明書が含まれていることを確認してください。含まれている場合、対応は不要です。
    - 以下のリンクを参照し、Java、Linux、または Windows を使用している G5 ルート証明書がキーストアに存在することを確認してください。
2. **エラーログを確認します。**VeriSign G5 ルート証明書をダウンロードして G2 ルート証明書と置き換えていない場合、以下のようなエラーメッセージが表示される可能性があります。
    - SSL handshake error, “No trusted certificate found” (SSL ハンドシェイクエラー、「信用できる証明書がありません」)
    - Result code -31, “The certificate chain did not validate, no local certificate found” (結果コード-31、「証明書チェーンが有効ではありませんでした。ローカルの証明書がありません」)
    - Result code -8, “SSL connection failed” (結果コード-8、「SSL 接続に失敗しました」)
    - -1 error (-1 エラー)

    これらの問題を解決するには、以下のいずれかを行ってください。

    - ソフトウェアを、SHA-256 に対応した最新バージョンに更新します。または
    - 証明書の検証/認証にキーストアが使用されている場合は、VeriSign G5 ルート証明書をキーストアにインストールします。

3. **VeriSign G5 ルート証明書を入手します。**証明書ストアまたは Java クライアントに VeriSign G5 ルート証明書が含まれていない場合は、システム管理者に依頼して VeriSign からダウンロードし、ほかの SSL 接続認証パッケージとともに証明書ストアに保存してください。
    - Symantec の VeriSign G5 ルート証明書をダウンロードしてください Symantec の VeriSign G5 ルート証明書をダウンロードしてください
    - お使いのサーバーで要求される場合は特定のサーバーSSL 証明書をダウンロードしてください

2. SHA-256 署名アルゴリズムへの更新

問題: SHA-1 は、22 年前から使用されている暗号アルゴリズムですが、コンピュータの性能向上によりインターネット攻撃による脅威にさらされています。SHA-256 は、256 bit のハッシュ値によるより強力なアルゴリズムを使用しています。

PayPal の対応: 2016 年半ばに、すべての本番環境および Sandbox のエンドポイントの SSL 証明書を、SHA-1 からより強力で堅牢な SHA-256 にアップグレードします。

必要な対応

以下のガイドラインにしたがって、SHA-1 署名アルゴリズムを使用する SSL 証明書から、より強力な SHA-256 署名アルゴリズムに移行してください。

1. **お客さま側の環境を確認します。**SHA-256 証明書に対応していることを確認してください。
    - サポートされているハードウェアおよびソフトウェアの一覧を、DigiCert の SHA-2 互換性ガイドや Symantec のサポート対象ブラウザ・サーバーリストなどのページでご覧ください。
    - お使いの環境の一部が SHA-256 に対応していない場合は、新しい証明書をインストールする前に、その部分を置き換えるかアップグレードする必要があります。
    - Windows 2000 Server および Windows XP の一部のバージョンは、SHA-2 との互換性がない可能性があります。SHA2 と Windows に関する Windows PKI ブログでは、お使いの環境をアップグレードするためのパッチや推奨情報を確認できます。
2. **証明書を確認します。**お使いの環境が SHA-256 に対応している場合は、キーストアに VeriSign G5 ルート証明書があることを確認してください。

ご質問がある場合

その他の詳細情報およびよくある質問は、PayPal の 2015-2016 SSL Certificate Change Microsite(2015-2016 SSL 証明書変更のマイクロサイト)をご覧ください。

ありがとうございます

この問題に関するお客さまの早急なご対応および弊社の取り組みへのご理解、ありがとうございます。これらの作業により互換性の問題が発生する可能性があることを理解しております。短い間ですがご迷惑をおかけすることになり誠に申し訳ございませんが、お客さまのアカウントおよび財務情報をより安全に保護するため、何卒ご理解の程よろしくお願い申し上げます。