■■■ SSL-API／グローバルパートナーセンターをご利用中の　■■■

■■■ パートナー様に該当する可能性のある重要なお知らせです　■■■

2017 年 10 月 26 日

SSL-API パートナー各位

合同会社シマンテック・ウェブサイトセキュリティ

【重要】マネージド CA 対応に伴う SSL サーバ証明書製品ならびに申請システム等における仕様変更などのご案内

平素は弊社製品の販売支援をいただき、誠にありがとうございます。

このたび弊社では、SSL サーバ証明書製品の認証業務を DigiCert 社とのパートナーシップに基づいて統合し認証レベルをより一層強化すると共に、SSL サーバ証明書を発行するための PKI インフラを刷新し、ブラウザーコミュニティによる要求を満たすことで Google Chrome 等の警告表示によるお客様への影響を回避することを目的とする SSL サーバ証明書ならびに申請システムの仕様変更を実施させていただくこととなりましたので、ご案内申し上げます。

詳細につきましては下記をご覧ください。

弊社では引き続きサービスの向上に努めてまいりますので、今後ともご愛顧を賜りますよう、お願い申し上げます。

記

1. 変更適用予定日

2017 年 11 月下旬

※ 日程を確定次第、別途ご案内いたします。

2. 変更の背景

(補足資料の page3-6 を併せてご参照ください)

さる 2017 年 6 月 5 日付けのレター「Symantec Website Security からの重要なお知らせ」等でご案内の通り、弊社ではブラウザーコミュニティによる提案への対応の検討を行ってまいりました。この中で示唆された oogle Chrome による警告表示などの問題によるお客様のウェブサイトの継続性への影響を回避する目的で、DigiCert 社とのパートナーシップに基づく認証業務の統合、ならびに新しい PKI インフラへの移行を行うことを決定いたしました。

(以下、統合後の認証業務モデルならびに移行後の新しいインフラを総称し「Managed CA」と呼びます)

以下にご案内する証明書製品ならびに申請システムの各種仕様変更は、この一連の Managed CA への移行の取組みの一環として実施させていただくものです。

Managed CA への移行ならびに各種仕様変更の概要については以下の補足資料を合わせてご参照・ご活用ください。

[補足資料] 「Managed CA 対応」における製品仕様変更点について

https://www.jp.websecurity.symantec.com/sid-partner/ssl-api/doc/20171025_symcsslapi.pdf

Google Chrome による警告表示と回避方法の詳細についてはこちらをご参照ください。

[シマンテック ブログ]Symantec SSL/TLS サーバ証明書の入れ替えに関する情報について

https://www.symantec.com/connect/blogs/symantec-ssltls

3. 証明書製品仕様の変更について

(補足資料の page7-14 を併せてご参照ください)

3-1. 対象システム

シマンテック グローバルパートナーセンター

シマンテック SSL-API

3-2. 対象製品

対象システムから発行する全ての SSL サーバ証明書製品 ※ セーフサイト、コードサイニング証明書を除きます

3-3. 変更内容

3-3-1. ルート証明書ならびに中間 CA 証明書の変更

Managed CA への移行後の新しいインフラでは、新たなルート認証局ならびに 中間認証局を構築いたします。ここから発行される SSL サーバ証明書は、この 新しいルート証明書ならびに中間証明書によって検証されます。

また、各種ブラウザ、スマートフォンや携帯端末などとの接続性を維持する 目的で、従来より普及するルート証明書にチェーンするクロスルート証明書を 提供します。

Managed CA への移行後の新しい SSL サーバ証明書をサーバにインストールする 際には、新しい中間証明書ならびにクロスルート証明書の両方をインストール ください。

新しいルートおよび中間 CA 証明書の階層構造につきましては以下をご参照ください。

[ルート／中間の階層構造について - Part1]

https://knowledge.symantec.com/jp/support/ssl-certificates-support/index?page=content&id=INFO4596

[ルート／中間の階層構造について - Part2 (詳細)]

https://knowledge.symantec.com/jp/support/ssl-certificates-support/index?page=content&id=INFO4597

※すでに発行済みのサーバ証明書をご利用中は、従来の中間 CA 証明書をご利用ください。

3-3-2. SSL サーバ証明書のプロファイル変更

Managed CA への移行後の新しい SSL サーバ証明書では、証明書プロファイルに 以下の変更が適用されます。

・Subject Key Identifier (サブジェクトキー識別子) : フィールドを追加 ・Certificate Policies (証明書ポリシー) : ポリシー参照 URL 変更、他 ・Signed Certificate Timestamp : 「登録なし」の場合に SCT を含まない

変更内容の詳細につきましてはこちらをご覧下さい。

[12 月 1 日 Managed CA 対応リリース後の証明書階層構造における証明書プロファイルの変更について]

https://knowledge.symantec.com/jp/support/ssl-certificates-support/index?page=content&id=INFO4648

3-3-3. OCSP および CDP の変更

Managed CA への移行後の新しい SSL サーバ証明書では、OCSP(オンライン証明書 ステータスプロトコル)レスポンダならびに CDP(CRL(証明書失効リスト)配布 ポイント)が変更されます。

変更内容の詳細につきましてはこちらをご覧下さい。

[12 月 1 日 Managed CA 対応リリース後の TLS/SSL 証明書の OCSP および CRL について]

https://knowledge.symantec.com/jp/support/ssl-certificates-support/index?page=content&id=INFO4647

3-3-4. その他の変更

Managed CA への移行後の新しい SSL サーバ証明書製品では、上記の点と併せて 以下の変更が適用されます。

・アルゴリズムオプション「DSA」の提供終了：

SSL サーバ証明書のマルチアルゴリズム機能のうち、署名アルゴリズム DSA を用いたオプションの提供を終了いたします。

・CT(Certificate Transparency)における「CT へ登録する情報の一部を非公開 (Name Redaction)とする」オプションの提供終了： Managed CA への移行後は、「登録する」選択時のみ CT ログサーバへ登録いたします。

・シールインサーチの一部サービスの終了（シマンテック製品)： iLunascape および Sleipnir 各ブラウザ上でのシールインサーチ表示を終了 させていただきます。

※ iLunascape および Sleipnir 各提供事業者との契約満了に伴うサービス終了となります。

4. SSL-API 機能の仕様変更について

(補足資料の page16-17 を併せてご参照ください)

4-1. ファイル認証用トークンの生成にかかる変更点

(対象: ジオトラスト クイック SSL プレミアム、ラピッド SSL) Managed CA への移行後、セキュリティチェック(*1)該当時に、ファイル 認証用トークンが QuickOrder 機能の Response に含まれない場合があります。

ファイル認証用トークンを入手いただくためには、シマンテック認証 サポートチームによる確認作業完了後に、GetOrderByPartnerOrderID 機能 でオーダ情報を照会いただくことで、トークン情報を取得いただけます。

*1 : セキュリティチェックとは

https://knowledge.geotrust.com/jp/support/knowledge-base/index?page=content&id=SO24216

4-2. WHOIS 認証用メールアドレス変更機能

Managed CA への移行後、WHOIS 認証による発行の完了前に認証用メール アドレスを変更する機能 (ChangeApproverEmail)はご利用いただけなく なります。

4-3. ドメイン認証(DV)認証方式変更機能

Managed CA への移行後、ファイル認証または DNS 認証を選択し申請後に、 発行の完了前に認証方式を WHOIS 認証に変更する機能 (ModifyOrder:UPDATE_DV_AUTH_METHOD)はご利用いただけなくなります。

4-4. テスト用(Pilot)環境限定 機能検証補助機能

Managed CA への移行後、テスト用(Pilot)環境における機能検証を補助する 目的でご提供している ModifyOrder:PUSH_ORDER_STATE 機能はご利用いただけ なくなります。

その他、上記以外の詳細につきましては上述の「補足資料」をご覧下さい。

5. パートナーポータルならびにエンドユーザーポータル機能の仕様変更について (補足資料の page18 を併せてご参照ください)

5-1. 一部メールテンプレート編集機能の変更

(対象: ジオトラスト クイック SSL プレミアム、ラピッド SSL)

Managed CA への移行後、WHOIS 認証における承認依頼メールのテンプレートを 編集(カスタマイズ)いただけるパートナーポータルの機能はご利用いただけ なくなります。

5-2. 再発行時のアルゴリズムオプション変更機能について

(対象: シマンテック グローバル・サーバ ID EV、グローバル・サーバ ID) これまでエンドユーザーポータルにおける再発行機能を用いて、有効な対象 製品をご利用中のお客様はアルゴリズムオプションを変更(例:RSA⇒ECC)いた だくことが可能でした。 この度、新しい PKI インフラへの移行に伴い、エンドユーザポータル上で

アルゴリズムオプションを変更して再発行いただく機能はご利用いただけ なくなります。

※アルゴリズムオプションの変更を伴わない再発行は引き続きご利用いただけます。

6. 今後の予定について

Managed CA への移行に関する本番(Production)環境のリリースに先立って、テスト用(Pilot)環境でのリリースを 2017 年 11 月中旬に予定しております。

※ 日程を確定次第、別途ご案内いたします。

テスト用(Pilot)環境をご利用中のパートナー様におかれましては、万が一にも本番稼働中の SSL-API 統合済みのシステムにおける業務上の影響を避けていただくために、念のための事前動作確認をご検討、実施いただけますよう、何卒ご協力をお願い申し上げます。

テスト用(Pilot)環境の開設につきましては、営業担当者または下記のサポート窓口にご相談ください。

7. 本件に関するお問合せ先

合同会社シマンテック・ウェブサイトセキュリティ

認証に関するお問い合わせ

Email：auth_support_japan@symantec.com

電話：03-5114-4135（自動音声ガイダンス 1）

受付時間：土日祝日および年末年始を除く平日 9:30 - 17:30

テクニカルサポート

Email：sslapi_info_jp@symantec.com

電話：03-5114-4135（自動音声ガイダンス 2）

受付時間：土日祝日および年末年始を除く平日 9:30 - 17:30

営業窓口

パートナープログラム事務局

電話番号： 03-5114-4796

メールアドレス： ssl-partner@symantec.com

以上

合同会社シマンテック・ウェブサイトセキュリティ パートナー営業部

パートナープログラム事務局

電話番号　　: 03-5114-4796　FAX 番号 : 03-6368-9578

メールアドレス : ssl-partner@symantec.com
