[補足資料]
「Managed CA対応」における製品仕様変更点について

最終更新日：2017年11月16日

[パートナー様用]

目次

1. Managed CA対応とは
2. 証明書製品仕様および利用上の注意点
3. ストアフロント機能の変更点

1. Managed CA対応とは

「Managed CA対応」とは

- シマンテックグループのSSLサーバ証明書の**発行を担うPKIのコアインフラ**、ならびにCA/ブラウザフォーラムが定める業界標準に沿った**認証業務**を第三者の認証局事業者によって実施するモデル(通称**「Managed CA」モデル**)へ移行する一連の対応を指します。

- 目的：シマンテックグループのSSLサーバ証明書、申請システムやAPI等の管理サービスを、今後もお客様に継続的に、支障なくご利用いただくことを目的とする取り組みです。

- 背景：シマンテックによる過去の一部の不適切な発行に対する再発防止策の提案に対して、これに対する多くのパートナ様／お客様、Google社／Mozilla社等のブラウザベンダや業界関係者からのフィードバックなどを踏まえて立案された取り組みです。

- スケジュール(“Managed CA対応”リリース日時)：**2017年12月1日(金) 10時(日本時間)**
  - メンテナンス予定日時 2017年 11月 30日(木)20:00 ～ 12月 1日(金) 10:00 (日本時間)
  - 弊社都合により変更する場合、改めてご案内申し上げます。

- 対象製品：パブリックのSSLサーバ証明書
  - 全ての認証カテゴリ(EV/OV/DV)、全てのブランド(Symantec/GeoTrust)を含む
  - 対象外：コードサイニング証明書、セキュア・メールIDなどのS/MIME証明書
    その他、証明書以外の製品(セーフサイト、WAF、セキュリティ診断等)

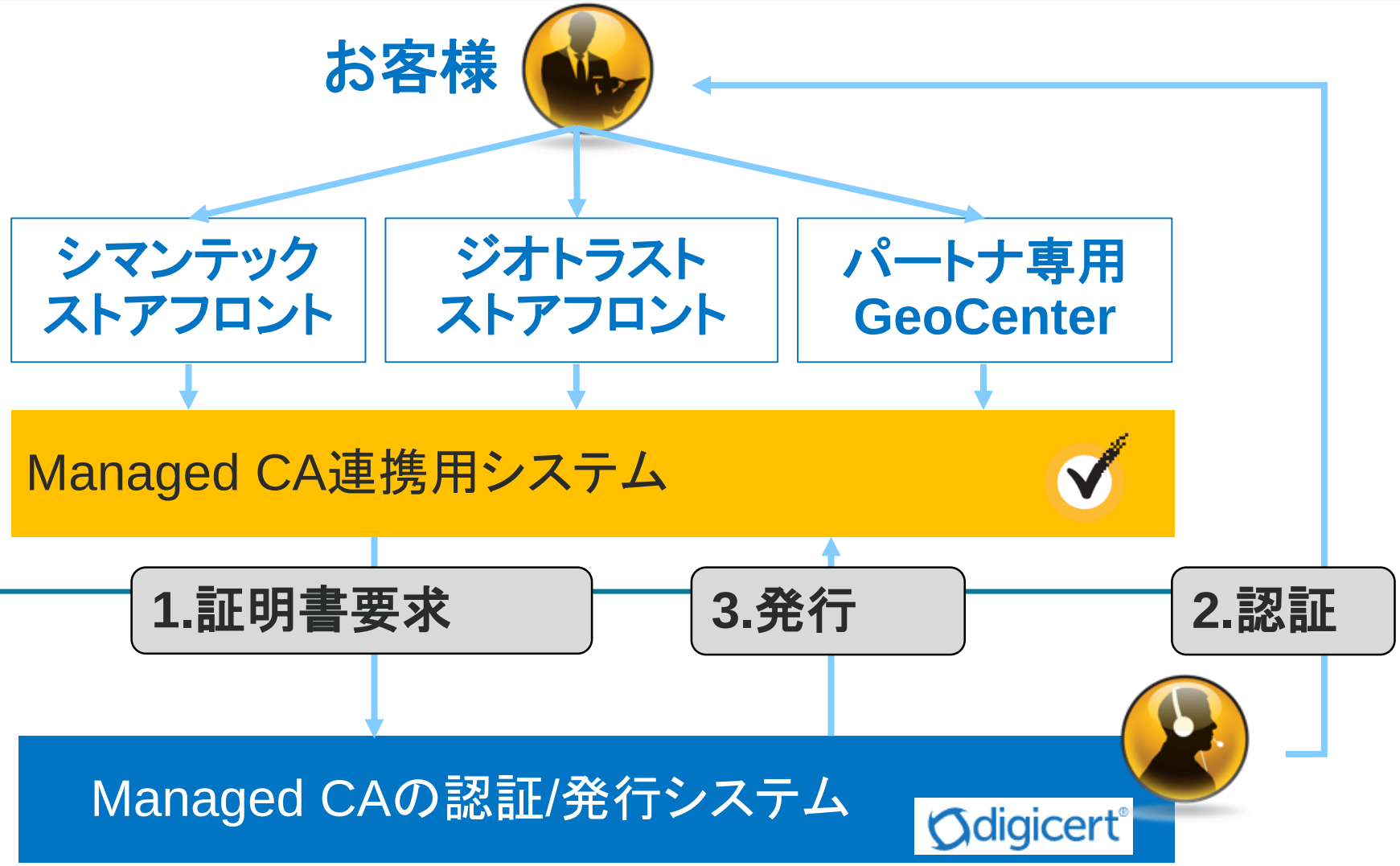
「Managed CA対応」は「バックエンドの変更」であり、原則として(*1)デジサート・ジャパン合同会社(旧シマンテック・ウェブサイトセキュリティ合同会社)のお客様がご利用いただく申請システム（ストアフロント等）の操作等の変更はございません。

*1：バックエンドの変更に伴う一部機能への影響に伴って、サービス機能や操作などに変更がある場合があります。
当資料の以下のページではこの背景から予定されている変更点を挙げます。

Managed CA対応後の申請～発行までの流れ

ご利用中の
プラットフォーム
(フロントエンド)

DigiCert社の
プラットフォーム
(バックエンド)



SSLサーバ証明書取得プロセス 変更点まとめ

取得プロセス

大項目	中項目	現在	Managed CAモデル移行後
申請	証明書申請	シマンテック(*1)のフロントエンドシステム/APよりご申請	変更なし
	お見積・注文書	シマンテック(*1)より発行	変更なし
認証	セキュリティチェック	シマンテック(*1)にて実施	変更なし
	DV認証(whois/file/DNS)	シマンテック(*1)のシステムによるDV認証(メール／Polling)	**Managed CAパートナ(DigiCert社)のシステムによるDV認証(メール／Polling)**
	EV/OV製品ドメイン名確認	シマンテック(*1)によるドメイン名利用権の確認(メール)	**Managed CAパートナ(DigiCert社)によるドメイン名利用権の確認(メール)**
	EV/OV製品申請意思確認	シマンテック(*1)による申請団体への意思確認(電話／メール)	**Managed CAパートナ(DigiCert社)による申請団体への意思確認(電話／メール)**
発行・納品	発行処理	シマンテック(*1)のバックエンドにて発行処理	**Managed CAパートナ(DigiCert社)のバックエンドにて発行処理**
	納品	シマンテック(*1)のフロントエンドシステム(メール／Download)	変更なし
請求	請求書	シマンテック(*1)より発行	変更なし
サポート	技術サポート	シマンテック(*1)にてサポート提供	変更なし

*1 : シマンテック・ウェブサイトセキュリティ合同会社は、2017年11月1日を以てデジサート・ジャパン合同会社へ社名を変更いたしました。
詳しくはこちら : https://www.websecurity.symantec.com/ja/jp/digicert-and-symantec-faq

2. 証明書製品仕様の変更点および利用上の注意点

SSLサーバ証明書 製品仕様 変更点まとめ

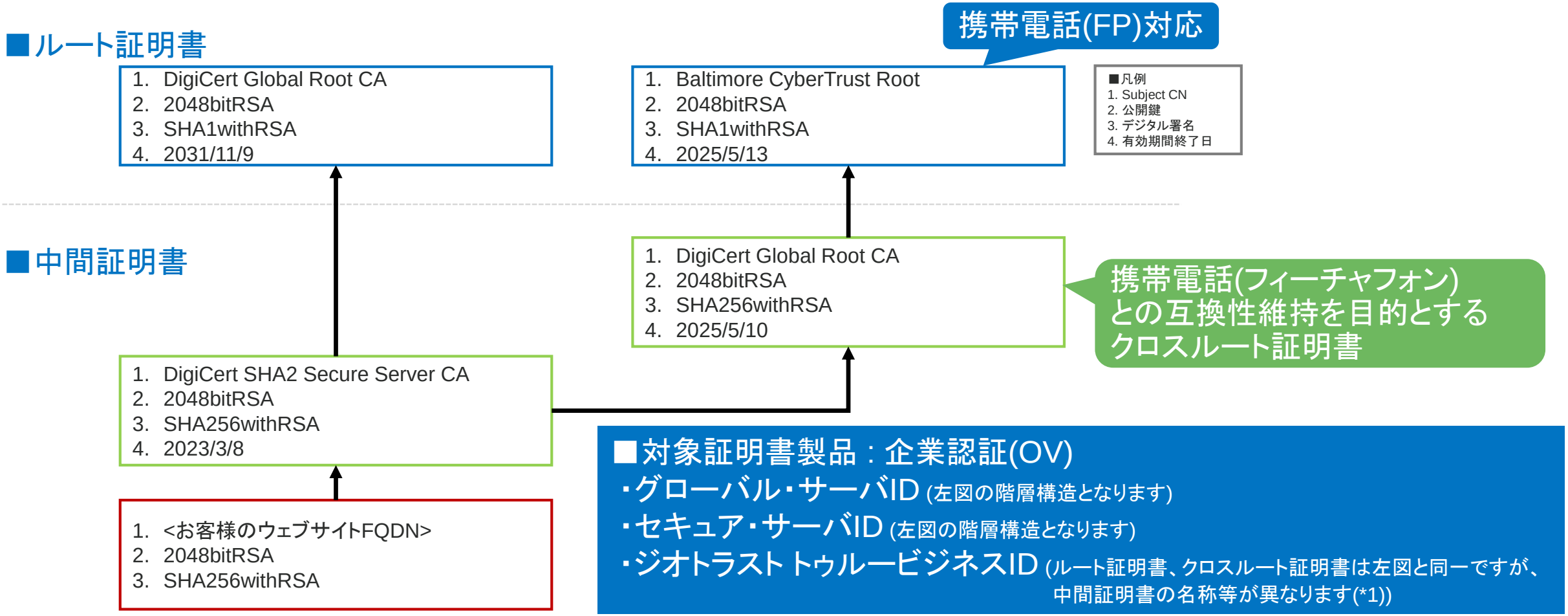
■ブランド/申請システム/製品共通(一部注記ある場合を除く)

大項目	中項目	現在	Managed CAモデル移行後
証明書	ルート	<製品ごとに異なる>	変更あり (詳細後述)
	中間証明書	<製品ごとに異なる>	変更あり (詳細後述)
	End Entity	<製品ごとに異なる>	変更あり (詳細後述)
端末対応率(標準(推奨)階層構造)	PC	SHA-2対応環境(WinXP SP3以降など)	変更なし
	フィーチャフォン	SHA-2対応環境(Android1.5以降など)	変更なし
	スマートフォン	SHA-2対応環境(アクセスシェア約9割)	変更なし
階層構造オプション	RSA	標準(推奨) / フルSHA-2チェーンオプションから選択可	変更なし
	ECC	Full-ECC / Hybrid(RSAルート)オプションから選択可	引き続き取得いただけますが、申請プロセスが一部変更となります(*1)
	DSA	選択可	ご提供を終了させていただきます。
その他の製品仕様	CT	登録/一部非公開/登録なし から選択	「一部非公開」オプションを削除 ⇒ 今後「登録あり」および「登録なし」の2つの選択肢からご選択いただきます。
	OCSP/CRL	-	CDP/OCSPレスポンダURL変更
無償バンドル(シマンテックブランド製品のみ)	マルウェアスキャン	EV SSL、グローバル・サーバID、セキュア・サーバIDで利用可能	変更なし
	脆弱性アセスメント	EV SSL、グローバル・サーバIDで利用可能	変更なし
	シールインサーチ	ノートンセキュリティ/iLunascape/Sleipnir上で表示	一部変更あり ※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。(*2)

*1 : 変更後のECC証明書の取得方法は以下の弊社Knowledge Baseでご案内いたします。
https://knowledge.symantec.com/jp/support/ssl-certificates-support/index?page=content&id=SO23461
*2 : iLunascape/Sleipnir提供事業者との契約満了に伴うサービスの提供終了となります。

Managed CA対応後の証明書階層構造 – 企業認証(OV)

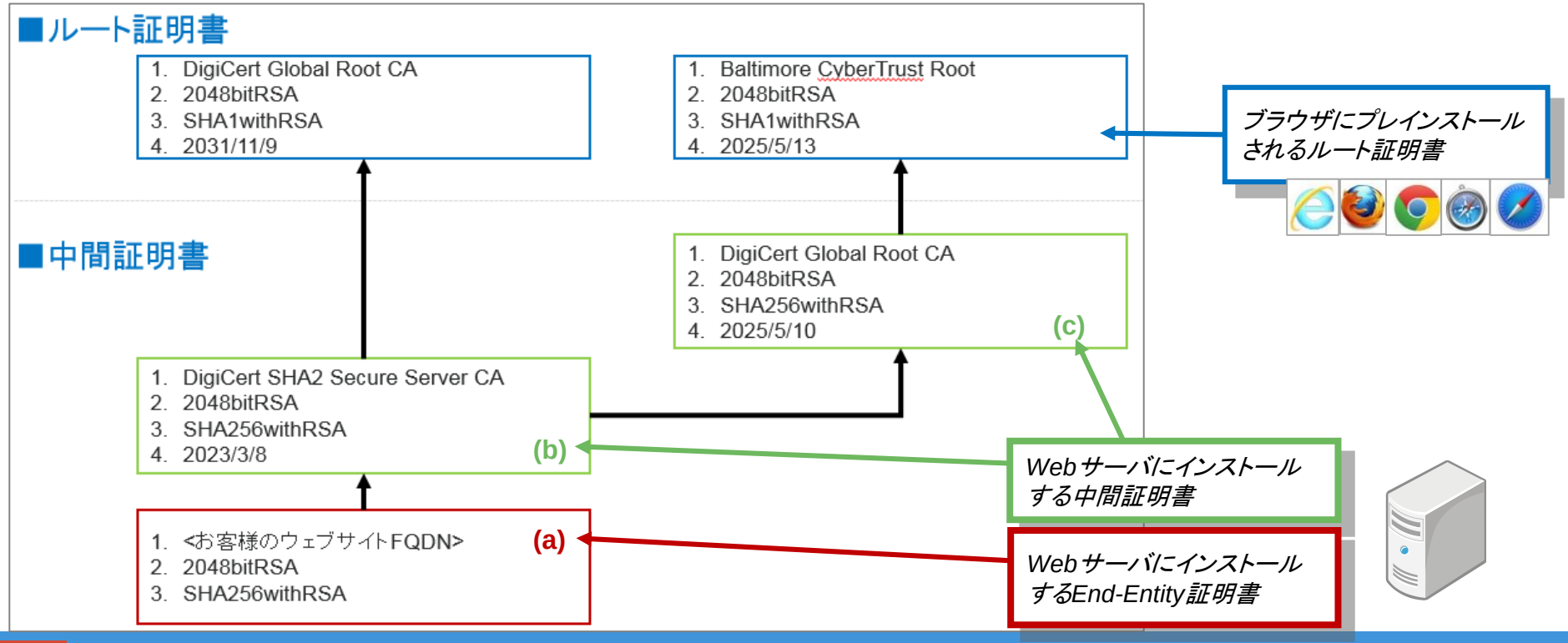
- 次世代の**シマンテック 企業認証(OV)SSLサーバ証明書**は、以下のような階層構造(ルート／中間証明書)を採用します。
- 携帯電話(フィーチャフォン、以下FP)との互換性維持を目的とするクロスルート証明書を併せて提供します。



*1：各製品ごとの階層構造詳細は以下を併せて参照ください。
[シマンテックブランド製品] https://knowledge.symantec.com/jp/support/ssl-certificates-support/index?page=content&id=INFO4697
[ジオトラストブランド製品] https://knowledge.geotrust.com/jp/support/knowledge-base/index?page=content&id=INFO4698

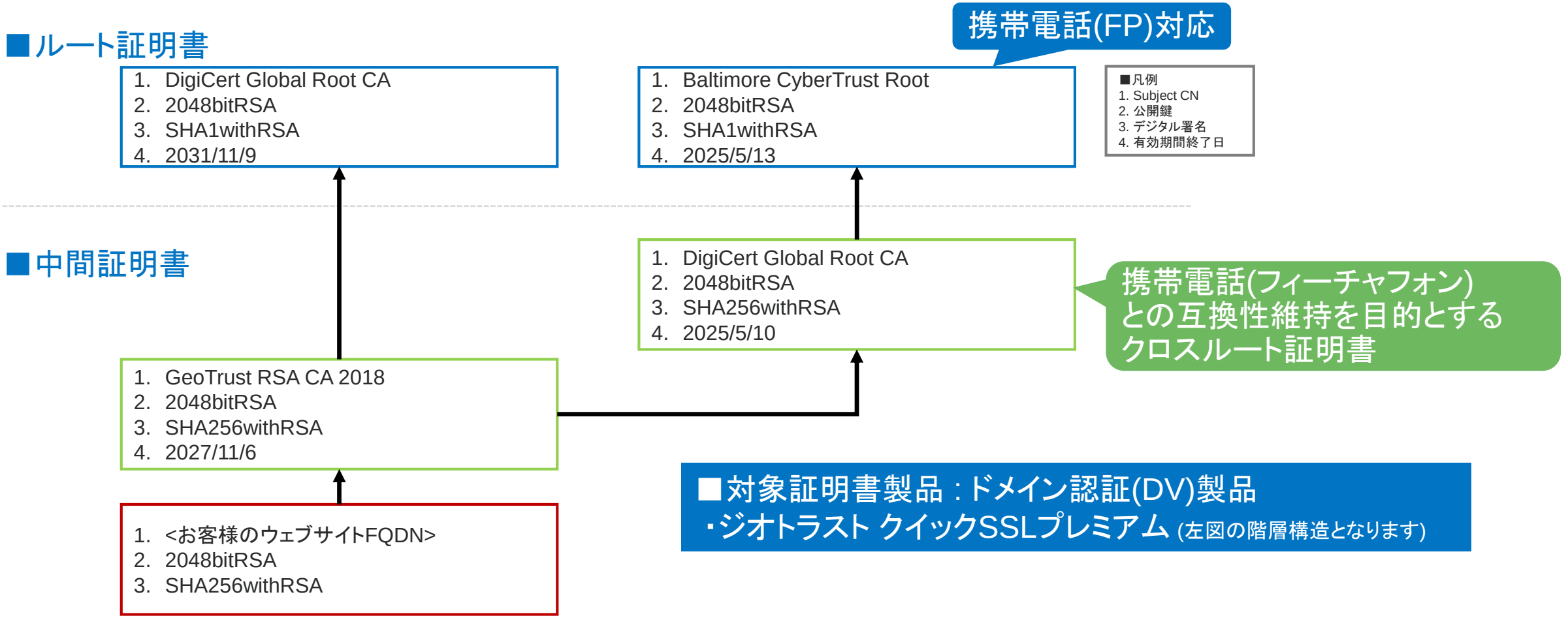
(参考) クロスルートとは？ - インストール時の注意点

- 「クロスルート」とは、ルート証明書普及に関する下位互換性を確保する仕組みです。
  - 新しいルート認証局に対して、旧来から普及するルート証明書を持つ認証局から署名を行い、クロスルート証明書(中間証明書として利用される)としてWebサーバにインストールすることで、新しいルート証明書が普及していない端末上でのサーバ認証を可能とします。
  - お客様のSubjectコモンネーム(FQDN)に対してEnd-Entity証明書(a)と併せて、追加で2階層分の中間証明書((b)および(c))の計3枚の証明書をお客様のサーバへインストールする必要があります(*1) 。
  - ブラウザからの通信要求時には3枚の証明書がダウンロードされて、TLSハンドシェイク(CertificateVerify)に用いられます。



Managed CA対応後の証明書階層構造 – ドメイン認証(DV)

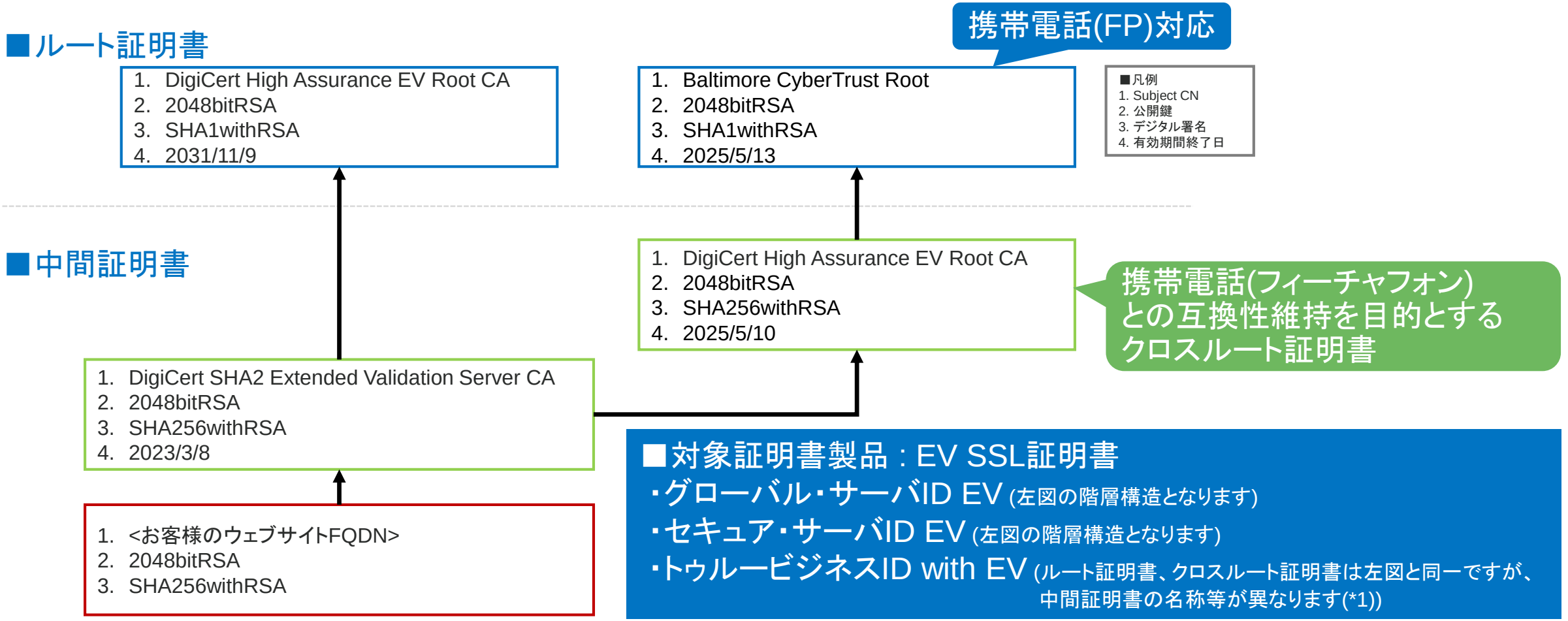
- 次世代の**ドメイン認証(DV)SSLサーバ証明書**は、以下のような階層構造(ルート／中間証明書)を採用します。
- 携帯電話(フィーチャフォン、以下FP)との互換性維持を目的とするクロスルート証明書を併せて提供します。



*1：各製品ごとの階層構造詳細は以下を併せて参照ください。
[シマンテックブランド製品] https://knowledge.symantec.com/jp/support/ssl-certificates-support/index?page=content&id=INFO4697
[ジオトラストブランド製品] https://knowledge.geotrust.com/jp/support/knowledge-base/index?page=content&id=INFO4698

Managed CA対応後の証明書階層構造 – EV SSL証明書

- 次世代のシマンテック **EV SSL証明書**は、以下のような階層構造(ルート／中間証明書)を採用します。
- 携帯電話(FP)との互換性維持を目的とするクロスルート証明書を併せてご提供します。



*1：各製品ごとの階層構造詳細は以下を併せて参照ください。
[シマンテックブランド製品] https://knowledge.symantec.com/jp/support/ssl-certificates-support/index?page=content&id=INFO4697
[ジオトラストブランド製品] https://knowledge.geotrust.com/jp/support/knowledge-base/index?page=content&id=INFO4698

各ルート証明書の概要ならびにクライアント対応状況

		DigiCert Global Root CA	DigiCert High Assurance EV Root CA	Baltimore CyberTrust Root	(参考) VeriSign Class 3 Public Primary Certification Authority - G5
用途		OV/DV証明書用のルート証明書 （推奨階層構造オプション）	EV SSL証明書用のルート証明書 （推奨階層構造オプション）	携帯電話(FP)に対応したルート証明書 **（クロスルート証明書の追加設定により利用可）**	2017年11月以前発行分のシマンテック製品のルート証明書
暗号アルゴリズム (鍵長、自己署名アルゴリズム)		RSA2048bit / sha1withRSA	RSA2048bit / sha1withRSA	RSA2048bit / sha1withRSA	RSA2048bit / sha1withRSA
有効期間開始日（≠配布開始）		2006年	2006年	2000年	2006年
普及率 総合評価		○	○	◎	◎
PC	Internet Explorer	◎	◎	◎	◎
	Google Chrome				
	Firefox	◎	◎	◎	◎
	Safari	◎	◎	◎	◎
スマホ	Android	◎	◎	◎	◎
	iOS	◎	◎	◎	◎
FP	携帯電話(FP)	×	×	○ (SHA-2対応の全機種、約9割)	○ (SHA-2対応の全機種、約9割)

※ 詳細な携帯クライアント対応状況は、11月下旬を目処に以下ウェブページへ公開予定
https://www.symantec.com/ja/jp/page.jsp?id=ssl-eligibility
https://www.geotrust.co.jp/products/resources/compatibility_listing/

SSLサーバ証明書 End-Entity プロファイル変更

- Managed CA対応後の新しい証明書(End-Entity証明書)のプロファイルは、以下のように変更されます。

■ブランド/製品共通

変更対象 証明書フィールド	変更内容	注意点
Issuer (発行者)	・新しい中間CA証明書のSubject DN	特になし
Certificate Policy (証明書ポリシー)	・ポリシー・規約の参照URLを新URL(*1)へ移動 ・Policy OID (SYMC No Auth Data Reuse)を追加	特になし
CRL Distribution Points (CRL配布ポイント)	CRL配布ポイントのURLを新URL(*2)へ移動	Firewall設定等に注意(*3)
Authority Information Access (機関情報アクセス)	OCSPレスポンダおよびIssuer証明書ダウンロードURLを 新URL(*2)へ移動	Firewall設定等に注意(*3)
Subject Key Identifier (サブジェクトキー識別子)	フィールドを追加	特になし
SCT (Signed Certificate Timestamp)	「登録する」を選択した場合、SCTを含む(変更なし) 「登録しない」を選択した場合、SCTは含まれない (「一部非公開」は今後選択できなくなります)	特になし

*1 : 新しい証明書プロファイルにおけるポリシー・規約の参照URLは以下の当社Knowledge Base(FAQ)に順次公開予定
[シマンテックブランド製品] https://knowledge.symantec.com/jp/support/ssl-certificates-support/index?page=content&id=INFO4703
[ジオトラストブランド製品] https://knowledge.geotrust.com/jp/support/knowledge-base/index?page=content&id=INFO4704

*2 : CRLならびにOCSPの新URLは以下の当社Knowledge Base(FAQ)に順次公開予定
[シマンテックブランド製品] https://knowledge.symantec.com/jp/support/ssl-certificates-support/index?page=content&id=INFO4706
[ジオトラストブランド製品] https://knowledge.geotrust.com/jp/support/knowledge-base/index?page=content&id=INFO4707

*3 : エンドユーザ様の環境によって、例えばグループ内ITポリシーとして外部アクセス可能ドメイン名のホワイトリストを運用し、
これ以外のドメインへの通信をFirewall等で遮断するような設定をされている場合、新しいドメイン名を設定追加いただく必要がございます。

3. ストアフロント機能の変更点

シマンテック ストアフロント 扱い製品/コンソール機能など変更点まとめ

大項目	中項目		現在	Managed CA移行後
扱い製品	・グローバル・サーバID EV ・セキュア・サーバID EV		(新規/更新/乗換/再発行を問わず) 現行製品仕様にて発行	(新規/更新/乗換/再発行を問わず) 新製品仕様にて発行
	・グローバル・サーバID (Wildcardを含む) ・セキュア・サーバID (Wildcardを含む)		(新規/更新/乗換/再発行を問わず) 現行製品仕様にて発行	(新規/更新/乗換/再発行を問わず) 新製品仕様にて発行
	・マルチドメイン(SANs)対応		利用可能	引き続き取得いただけますが、申請プロセスが一部変更となります(*2)
	日本独自 バンドル 機能/製品	・エクスプレスオプション (*1)	利用可能	ご提供を終了させていただきます(*1)
		・グローバル・サーバID エクスプレスプレミアム (*1)	利用可能	ご提供を終了させていただきます(*1)
	・コードサイニング証明書 ・セキュアメールID (S/MIME) ・セーフサイト		現行製品仕様にて発行	変更なし
コンソール機能	・新規 / 更新(いつでも更新) / 乗換申請		利用可能	変更なし ※ 発行される証明書は[新仕様]となります。
	・再発行申請		利用可能	一部変更あり ※ エンドユーザーポータルにおける再発行時のアルゴリズム オプション変更(例：RSA⇒ECC)がご利用いただけなくなります ※ 同一アルゴリズムオプションでの再発行は可能。 ※ 発行される証明書は[新仕様]となります。
	・無償バンドル機能管理機能		利用可能	変更なし
お支払方式	・銀行振込		利用可能	変更なし
	・クーポン		利用可能	変更なし

*1：「エクスプレスオプション」「グローバル・サーバID エクスプレスプレミアム」に付帯されるエクスプレスサービスとは、サーバID（EV SSL証明書を除く）を緊急で取得する必要があるお客様向けの有償オプションサービスとしてご提供して参りました。今回、認証業務の第三者認証局事業者による実施を軸とするバックエンドプロセスの見直しに伴い提供を終了させていただきます。

*2：変更後のマルチドメイン(SANs)対応SSLサーバ証明書の取得方法は以下の弊社Knowledge Baseでご案内いたします。
https://knowledge.symantec.com/jp/support/ssl-certificates-support/index?page=content&id=SO23158

ジオトラスト ストアフロント 扱い製品/コンソール機能など変更点まとめ

大項目	中項目	現在	Managed CA移行後
扱い製品	・トゥルービジネスID with EV (SANsを含む)	(新規/更新/乗換/再発行を問わず) 現行製品仕様にて発行	(新規/更新/乗換/再発行を問わず) 新製品仕様にて発行
	・トゥルービジネスID (Wildcard/SANsを含む)	(新規/更新/乗換/再発行を問わず) 現行製品仕様にて発行	(新規/更新/乗換/再発行を問わず) 新製品仕様にて発行
	・クイックSSLプレミアム (Wildcard/SANsを含む)	(新規/更新/乗換/再発行を問わず) 現行製品仕様にて発行	(新規/更新/乗換/再発行を問わず) 新製品仕様にて発行
コンソール機能	・新規 / 更新 / 乗換申請	利用可能	変更なし ※ 発行される証明書は[新仕様]となります。
	・再発行申請	利用可能	変更なし ※ 発行される証明書は[新仕様]となります。
支払方式	・銀行振込	利用可能	変更なし
	・クレジットカード	利用可能	変更なし
	・クーポン	利用可能	変更なし

パートナ専用GeoCenter 扱い製品/コンソール機能など変更点まとめ

大項目	中項目	現在	Managed CA移行後
扱い製品	・トゥルービジネスID with EV (SANsを含む)	(新規/更新/乗換/再発行を問わず) 現行製品仕様にて発行	(新規/更新/乗換/再発行を問わず) 新製品仕様にて発行
	・トゥルービジネスID (Wildcard/SANsを含む)	(新規/更新/乗換/再発行を問わず) 現行製品仕様にて発行	(新規/更新/乗換/再発行を問わず) 新製品仕様にて発行
	・クイックSSLプレミアム (Wildcard/SANsを含む)	(新規/更新/乗換/再発行を問わず) 現行製品仕様にて発行	(新規/更新/乗換/再発行を問わず) 新製品仕様にて発行
コンソール機能	・新規 / 更新 / 乗換申請	利用可能	変更なし ※ 発行される証明書は[新仕様]となります。
	・再発行申請	利用可能	変更なし ※ 発行される証明書は[新仕様]となります。
	・パートナ情報/個人アカウント管理	利用可能	変更なし
支払方式	・トークン	利用可能	変更なし

「またぎオーダ」の扱いについて

- リリース時点でPENDING（申請受付済かつ未発行）ステータスにあるオーダ（通称「またぎオーダ」）は、リリース時点から順次、ManagedCA対応後の新インフラ(現DigiCertインフラ)に情報が引き渡され、これと同時に、DigiCertの認証プロセスならびにツール類を使った認証作業が実施されます。
- この時点までに現シマンテックインフラ上で「部分的に」認証作業が完了されていたとしても、発行が完了していない場合、現シマンテックインフラ上の認証記録は無効となり、DigiCertインフラ上での認証が最初から実施される運びとなります。
- ドメイン認証 - メール(WHOIS)認証方式の場合、
  - PENDINGの状態でリリース時点を迎えた場合、旧インフラで生成されたPIN情報を含む承認申請メール(Approver Email)は、その時点で無効となります。新インフラにて再生成されたPIN情報を含む承認申請メールが、WHOIS掲載のメールアドレスならびに5種類の規定のアドレス(例:admin@)に配信されます。結果的に、該当のお客様は、旧と新、両インフラから2通の承認申請メール(Approver Email)を受信することとなりますが、リリース以後は、新インフラから配信された承認申請メールから承認(Approve)をいただくことで、証明書を発行することが可能となります。
- ドメイン認証 -ファイル認証方式の場合、
  - PENDINGの状態でリリース時点を迎えた場合、旧インフラで生成されたファイル認証用のトークン情報はその時点で無効となります。新インフラにて再生成されたファイル認証用のトークン情報を再度配置いただく必要がございます。この時点移行、新インフラのPolling機能にて、対象のウェブサーバに対して認証用トークンの確認を行います。この場合に、新インフラにて再生成されたファイル認証用のトークン情報は、リリース以降にジオトラスト ストアフロント/パートナ専用GeoCenter上で、該当オーダの申請情報詳細画面からダウンロードいただくことが可能です。