WHITE PAPER:

White Paper

いまさら聞けない、SSLサーバ証明書とルート証明書の関係

暗号アルゴリズム2010年問題対応されるサイト運営者　必見!

Symantec

Norton SECURED
powered by Symantec

CONTENTS

概要 4

第1章　暗号化通信で必須となる、SSLサーバ証明書とルート証明書 5

HTTPS通信の開始方法 5

SSLサーバ証明書とルート証明書の関係 5

第2章　暗号化通信における信頼の要、ルート証明書 6

クライアントに登録されるルート証明書 6

認証局（ルート証明書）を登録する基準 7

第3章　登録された認証局（ルート証明書）のメンテナンス 8

PCブラウザにおける認証局（ルート証明書）のメンテナンス 8

携帯電話や家電・組み込み機器における認証局（ルート証明書）のメンテナンス 8

携帯電話（NTT docomo）を例に見る登録された認証局（ルート証明書） 8

第4章　最後に 10

付録　シマンテックSSLサーバ証明書 11

シマンテック グローバル・サーバID EV（サーバタイプ:すべて共通） 12

シマンテック セキュア・サーバID EV（サーバタイプ:すべて共通） 13

シマンテック グローバル・サーバID（サーバタイプ:新仕様※1） 14

シマンテック グローバル・サーバID（サーバタイプ:旧来仕様※2） 15

シマンテック セキュア・サーバID（サーバタイプ:新仕様※3） 16

シマンテック セキュア・サーバID（プラットフォーム:旧来仕様※4） 17

概要

不景気を反映した消費スタイルの価格・ポイントサービス志向などにより、今までホームセンターで買っていたような日用品まで E コマースで購入されるようになってきました。とくに、昨今では、携帯電話やスマートフォンなどのモバイル EC 市場が全体を牽引する形となり、景気の低迷にもかかわらず消費者向け E コマース市場が依然として急成長しています。

この市場の成長スピードと連動してウェブサイト構築に求められるのが、開発スピードです。最近のウェブサイトの開発期間は 2 ヶ月、3 ヶ月という短いサイクルが求められ、一つのトラブルがスケジュール全体の致命的な遅延に繋がりかねません。また、そうした短期間で開発されたシステムに対しては、十分なテスト時間が設けられず、いざサイトをオープンしたとたんに、トラブルが発生するのです。

「ウェブサイトに接続しようとすると、セキュリティの警告がでるのはなぜ?」

「新しい携帯電話からは通信できるけど、古い携帯電話だと接続できないはなぜ?」

最近のウェブサイトは、外部システムとの連携が前提で構築され、こうした複雑化したシステムで発生するトラブルの原因は、ネットワークからアプリケーション、システム連携など様々な要因が考えられます。ウェブサイト構築にとって一つでもその要因を排除することが理想です。このホワイトペーパでは、前述のようなトラブルが発生する原因について、SSL（Secure Sockets Layer）暗号化通信の技術的な仕組みを通して解説していきます。この仕組みを理解することによって、トラブル発生時に何が原因であるのか、より具体的にイメージしながら対応することができ、また、事前に問題回避することもできるようになるでしょう。

第 1 章　暗号化通信で必須となる、SSL サーバ証明書とルート証明書

HTTPS 通信の開始方法

HTTPS 通信を開始する際に、クライアント（ウェブブラウザや携帯電話など）とウェブサーバ間では、どのような処理が行われているのでしょうか?

クライアントとウェブサーバの間では、下記の手順①～④および図 1 のようなやり取りが行われます。

① クライアントがセキュアなウェブサイト（https:// ～）へアクセスし、SSL 暗号化通信で接続を要求します。このときクライアントは、自身が使用可能な暗号化の仕様（暗号方式、鍵長、圧縮方式）をウェブサーバへ伝えます。ウェブサーバは、クライアントから提示された暗号化使用から実際に利用するものを選択して、クライアントへ通知します。

② ウェブサーバは、自分の身分を証明する SSL サーバ証明書をクライアントへ送ります。クライアントは SSL サーバ証明書を受け取り、クライアントに「信頼される認証局」としてあらかじめ登録されている認証局（CA）の証明書（これをルート証明書と呼ぶ）を用いて SSL サーバ証明書の署名検証を行います。またクライアントは、SSL サーバ証明書からウェブサーバの公開鍵を取得します。

③ 正しくルート証明書へのチェーンを辿って署名検証が完了すると、クライアントはウェブサーバの公開鍵を用いてプリマスタシークレット（共通鍵を生成する基となる乱数データ）を暗号化し、ウェブサーバへ送付します。ウェブサーバは自分の秘密鍵を用いて、プリマスタシークレットを復号します。

④ ③で共有されたプリマスタシークレットを基にクライアントとウェブサーバで同じ共通鍵を生成および共有し、以降のセッションではこの共通鍵を用いて暗号化・復号して通信を行います。

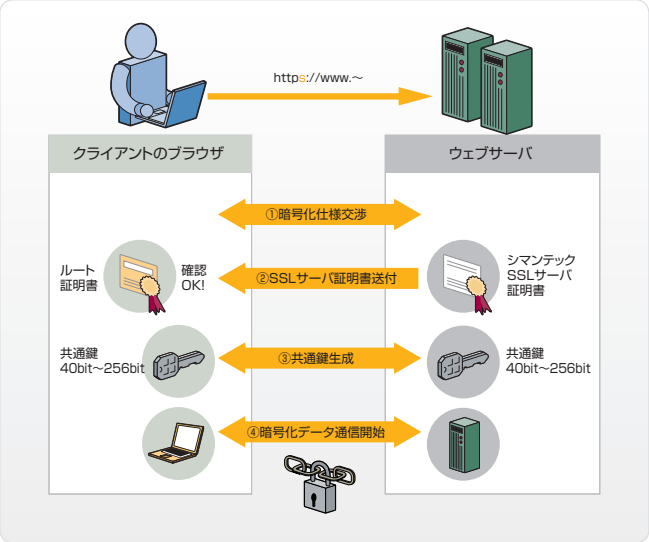


図 1.　SSL 暗号化通信開始時のウェブサーバとクライアントのやり取りのイメージ

HTTPS 通信が開始される短い時間の中で、ルート証明書は、ウェブサーバから送られてくる SSL サーバ証明書の信頼性を判断する重要な役割を果たしていることがわかるでしょう。

SSL サーバ証明書とルート証明書の関係

SSL サーバ証明書は、ウェブサイトを運営している団体のいわゆる「電子的な身分証明書」です。これを確認することで、認証済みの安全なサイトなのか、それとも身元の確認が取れない危険なサイトなのかを見極めることができます。

SSL サーバ証明書は、シマンテックのような「認証局事業者」に申請し、その事業者が設定する認証を受けて発行してもらう必要があります。SSL サーバ証明書には、サーバの運営者である組織名、証明書を発行した認証局の名前、ウェブサーバの公開鍵や証明書の有効期間が明記されており、さらに認証局事業者の署名が付いています。

認証局事業者の署名とは、SSL サーバ証明書のハッシュ値を認証局の秘密鍵で暗号化したデータです。クライアントは、SSL サーバ証明書を受け取ると、クライアントに登録されている認証局の証明書（ルート証明書）を用いて、この認証局の署名を復号します。復号したデータが、SSL サーバ証明書のハッシュ値と一致すれば、第三者によって改ざんされたものでない、正しく認証局事業者が発行した SSL サーバ証明書であることが確認できます。

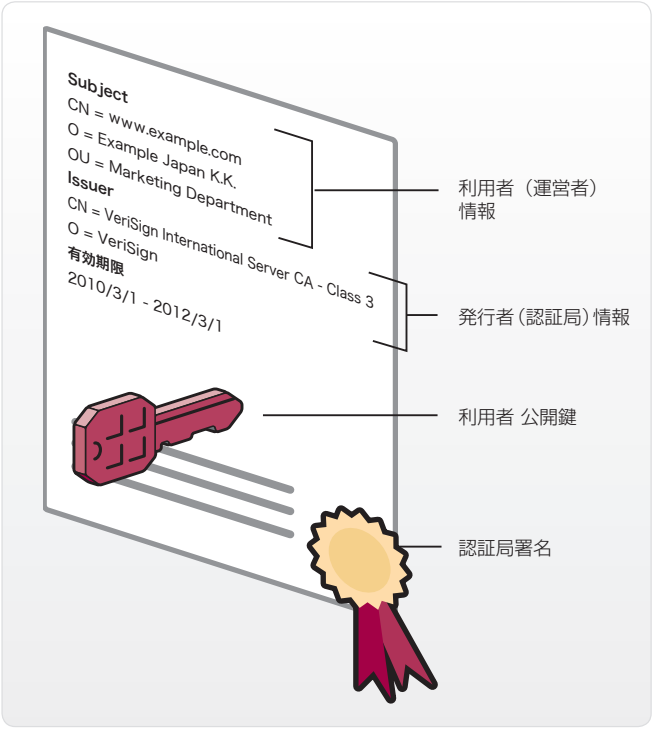


図 2.　SSL サーバ証明書の概略

このようにウェブサーバから送られてくる SSL サーバ証明書が、信頼できる証明書かを署名検証するキーポイントとなるのがクライアントに登録されている認証局の証明書（ルート証明書）であることがわかるでしょう。

認証局の証明書（ルート証明書）が存在しないと、ウェブサーバから送られてくる SSL サーバ証明書の認証局の署名が検証できずに、下記のようなエラーが発生します。

ウェブサイトに接続しようとすると、セキュリティの警告がでる

新しい携帯電話からは通信できるけど、古い携帯電話だと接続できない

次の章では、クライアントに登録されているルート証明書に関する概説と、上記エラーの原因であるクライアントがルート証明書を登録する基準について解説します。

第 2 章　暗号化通信における信頼の要、ルート証明書

クライアントに登録されるルート証明書

クライアントに登録されているルート証明書のリストは、PC の場合は簡単に確認することができます。Microsoft Internet Explorer の場合、メニューの「ツール」から、「インターネットオプション（O）」、「コンテンツ」、「証明書」、「信頼されたルート証明書機関」を辿ることで、登録された認証局（ルート証明書）の一覧を確認することができます。

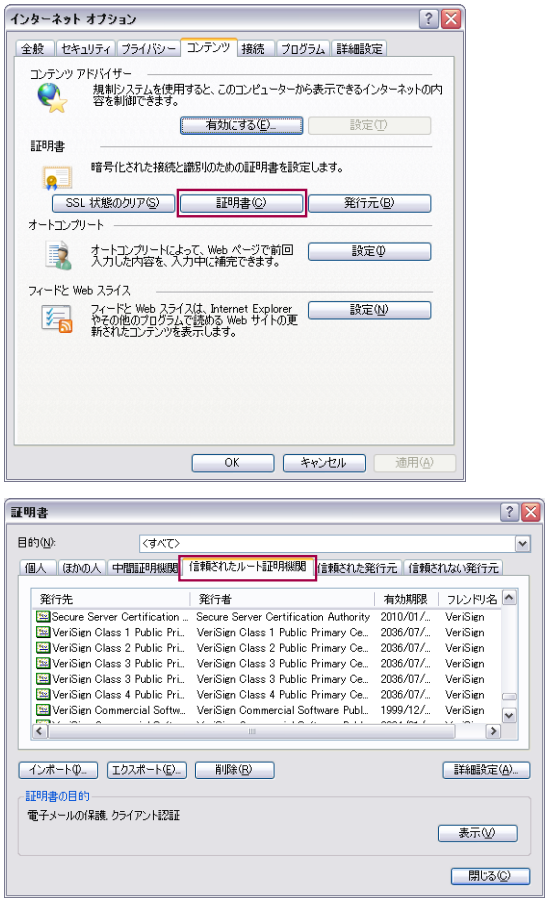


図 3.　Internet Explorer に登録されたルート証明書の確認方法

ルート証明書は、自分自身で電子署名をした電子証明書を発行しているという特徴があります。図 3. の例で言うと、発行先と発行者が同じであることで確認することができます。ブラウザベンダーや携帯電話の提供者であるキャリア、家電・組み込み機器メーカなどが、このようなルート証明書を組込むにあたっては、独自に厳密な審査を行っています。このプロセスに合格して初めて「信頼できるルート認証局」として登録されるというルールが採用されているので、私たちはこれを用いた SSL 通信を「信頼」できると言えます。

次節では、ブラウザベンダーなどが実施する厳密な審査とは、どのような基準に基づくものなのかについて、マイクロソフトが公開している内容を例に説明します。

認証局（ルート証明書）を登録する基準

シマンテックのような認証局は、業務を適切に行うために、CP（Certificate Policy：証明書ポリシー）とCPS（Certification Practice Statement：認証局運用規程）を作成し、この文書に従って業務を遂行しています。CP/CPSは、認証サービスにおける認証局の義務と責任、運用方法、電子証明書の適用範囲などを電子証明書の利用者や検証者へ告知することで認証局の社会的信頼性を向上させると共に、係争発生時の責任の明確化するための重要な文書です。一般的に、このような文章は公開されていますが、実際に認証局が業務を適切に行っているか、また発行される電子証明書を信頼してよいかを、電子証明書の利用者を含む外部の利害関係者が判断することはできません。そこで登場するのが「監査」というキーワードです。

外部の利害関係者が、認証局や発行された電子証明書を信頼できるかどうかを判断するうえで、認証局の業務に精通し、認証局から独立した第三者による監査が行われているかどうかが、ブラウザベンダーなどが「信頼できるルート認証局」として登録する重要な基準となっています。たとえば、マイクロソフトでは、登録基準として、どのような監査を満たす必要があるかをウェブで公開しています。

マイクロソフト ルート証明書プログラム

http://technet.microsoft.com/ja-jp/library/cc751157.aspx

一般要件（抜粋）
CA は監査を完了し、監査結果をマイクロソフトに 12 か月ごとに提出する必要があります。監査は、拡張キー使用法 (EKU) の割り当てで、マイクロソフトにより有効とされる PKI 階層を対象とする必要があります。マイクロソフトが有効にするすべての証明書の使用は定期的に監査される必要があります。監査レポートは監査の対象となっている特定の種類の証明書を発行するサブ CA を含むすべての範囲の PKI 階層を文書化する必要があります。適格な監査には次が含まれます。

- CA監査者（監査機関）について認可されているWebTrustにより完了されたWebTrust for Certificate Authorities v1.0またはそれ以降（英語情報）。
- ETSI TS 101 456 v1.2.1またはそれ以降（英語情報）
- ETSI TS 102 042 v1.1.1またはそれ以降（英語情報）、または
- CA監査者（監査機関）について認可されているWebTrustか、CAと同じ管轄の査定人についての法律やポリシーにより運営されている監査機関のいずれかにより完了されたISO 21188:2006（英語情報） “Public key infrastructure for financial services - Practices and policy framework”。

※ CA：Certificate Authority　認証局

ここで紹介されている監査基準の一つであるWebTrustについて、もう少し詳しく解説します。米国公認会計士協会（AICPA）及びカナダ勅許会計士協会（CICA）が定めた、オンラインにおける電子商取引を対象とした保証サービスをWebTrustのサービスとして定義されています。その中でも、認証局の信頼性を保証するサービスとしてWebTrust for CAというものがあり、認証局がその原則と規準に準拠しているかどうかを監査法人が検証し、準拠が確認された認証局に対して検証報告書が発行します。また、ブラウザベンダーやキャリア、家電・組み込み機器メーカなどは、このような監査結果を確認することによって、各認証局を「信頼できるルート認証局」として登録しています。

次の章では、クライアントに組み込まれたルート証明書が、どのような形でメンテナンスされるのか、そしてメンテナンスができない場合には、どのような状況がもたらされるのかについて解説します。

第3章　登録された認証局（ルート証明書）のメンテナンス

クライアントの出荷時に組み込まれた認証局（ルート証明書）は、定期的にメンテナンス（更新）をする必要があります。その理由としては、新しい暗号アルゴリズムを採用したルート証明書の追加や、危殆化した暗号アルゴリズムを使用しているルート証明書の削除を行うことを目的としてメンテナンスが実行されます。

PC ブラウザにおける認証局（ルート証明書）のメンテナンス

PC ブラウザなどでは出荷時に組み込まれた認証局（ルート証明書）に対して、定期的にオンラインでメンテナンス（更新）が実行することができます。

（参考）代表的なブラウザベンダーのルート証明書の更新方法

（1）マイクロソフト　ルート証明書の更新プログラムが提供されています。

（2）Mozilla Firefox ブラウザのバージョンアップにより自動的にルート証明書が更新されます。

携帯電話や家電・組み込み機器における認証局（ルート証明書）のメンテナンス

PC に比べて、携帯電話や家電・組み込み機器には、場合によっては、以下のような制限があるので、SSL サーバ証明書の選択には注意が必要です。

（1）ルート証明書のオンラインアップデート機能が提供されていない

（2）デバイスのメモリー容量の関係で限られたルート証明書のみしか登録できない

（3）最新の暗号アルゴリズムは取り扱えない

つまり出荷時に組み込まれた認証局（ルート証明書）のみが、「信頼できるルート認証局」として登録され、SSL 暗号化通信を実現することができます。以下では、NTT docomo が公開しているルート証明書の一覧を例にして、SSL サーバ証明書の選択の注意点を詳細に解説します。

携帯電話（NTT docomo）を例に見る登録された認証局（ルート証明書）

携帯電話において、どのようなルート証明書がリストに登録されているかは、携帯電話の提供者である各キャリアのホームページで公開されています。

（参考）各キャリアの SSL/TLS 通信に関する携帯電話仕様について

（1）NTT docomo

http://www.nttdocomo.co.jp/service/imode/make/content/ssl/spec/index.html#taiou

（2）au by KDDI

http://www.au.kddi.com/ezfactory/tec/spec/ssl.html

（3）SoftBank Mobile

http://creation.mb.softbank.jp/web/web_ssl.html

NTT docomo で公開されている各携帯端末に登録されているルート証明書の一覧から抜粋した内容を表 2 に示します。これを見ると分かるように、発売時期などによって登録されているルート証明書の種類や登録数が異なっていることが確認できます。

表2.各携帯端末(抜粋)に登録されているルート証明書の一覧

機種名	発売日	登録されているルート証明書
L-04B	2010年6月25日	VeriSignクラス3 Primary CAルート証明書 VeriSignクラス 3 Primary CA ルート証明書G2 Equifax Secure Certificate Authority Equifax Secure eBusiness CA-1 GeoTrust Global CA GTE CyberTrust Global Root Baltimore CyberTrust Root GlobalSign Root CA GlobalSign Root CA-R2 Valicert Class 3 Policy Validation Authority
L-03B	2010年3月12日	
L-02B	2009年12月18日	
L-01B	2010年3月26日	VeriSignクラス3 Primary CAルート証明書 VeriSignクラス 3 Primary CA ルート証明書G2 Equifax Secure Certificate Authority Equifax Secure eBusiness CA-1 GeoTrust Global CA GTE CyberTrust Global Root Baltimore CyberTrust Root GlobalSign Root CA GlobalSign Root CA-R2 Valicert Class 3 Policy Validation Authority RSA Security 2048 V3 Security Communication RootCA1 AddTrust External CA Root AAA Certificate Services COMODO Certificate Authority
FOMA 901i	2004年12月24日	VeriSignクラス3 Primary CAルート証明書 VeriSignクラス 3 Primary CA ルート証明書G2 Equifax Secure Certificate Authority Equifax Secure eBusiness CA-1 GeoTrust Global CA GTE CyberTrust Global Root Baltimore CyberTrust Root
FOMA 900i	2004年2月29日	VeriSignクラス3 Primary CAルート証明書 VeriSignクラス 3 Primary CA ルート証明書G2 GTE CyberTrust Global Root

前述のように、携帯電話や家電・組み込み機器においては、場合によっては「信頼できるルート認証局」としてルート証明書が登録されるのは出荷されるタイミングのみです。シマンテックのルート証明書（VeriSign クラス 3 Primary CA ルート証明書と VeriSign クラス 3 Primary CA ルート証明書 G2）は、古くは 2001 年の携帯電話から「信頼できるルート認証局」として登録されています。ここに、シマンテックが SSL 暗号化通信の対応率として業界 No.1 を維持している理由があります。例えば、携帯電話におけるルート証明書搭載率を表した資料に株式会社ケータイラボラトリー『第三世代携帯端末 ルート証明書搭載状況 調査結果と分析』（2010 年 3 月 1 日、参考 URL : http://www.ktai-labo.com/pdf/ssl_free_report.pdf）があります。この資料によるとシマンテックのルート証明書（VeriSign クラス 3 Primary CA ルート証明書と VeriSign クラス 3 Primary CA ルート証明書 G2）は搭載率 100% に達していることが分かり、この高いルート証明書の普及率が、携帯電話対応率業界 No.1 を維持しているゆえんです。

第4章　最後に

ウェブサイト構築作業において SSL サーバ証明書の導入は、つい片手間に考えてしまうかもしれません。そのため、SSL サーバ証明書の選定では、価格や発行スピードで選んでしまいがちですが、その結果としてサービス運用中に思わぬトラブルが発生する可能性があります。

こういったトラブルを避けるためにも、今回ご紹介した認証局（ルート証明書）の役割について理解したうえで、SSLサーバ証明書を選定、導入することで、予期しないトラブルを未然に防ぐことができるでしょう。

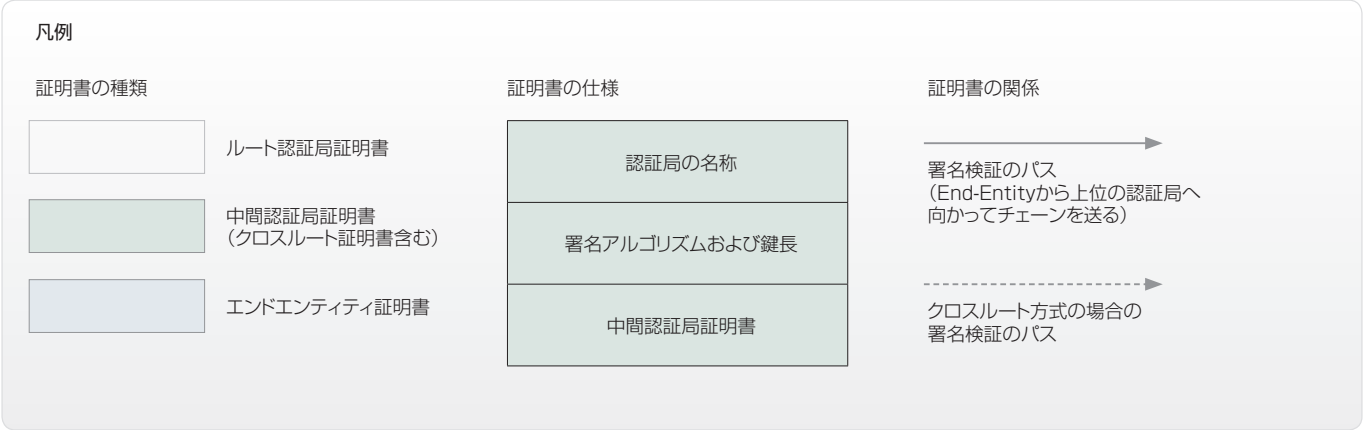
付録　シマンテック SSL サーバ証明書

本稿が想定する読者にあたるウェブサイト運営者の SSL サーバ証明書の選定業務の中で、シマンテック SSL サーバ証明書が、どのルート証明書から発行されているかを正しく把握し、自社のサービス要件にあった証明書を選択いただくために、それぞれの SSL サーバ証明書とルート証明書の関係を解説します。

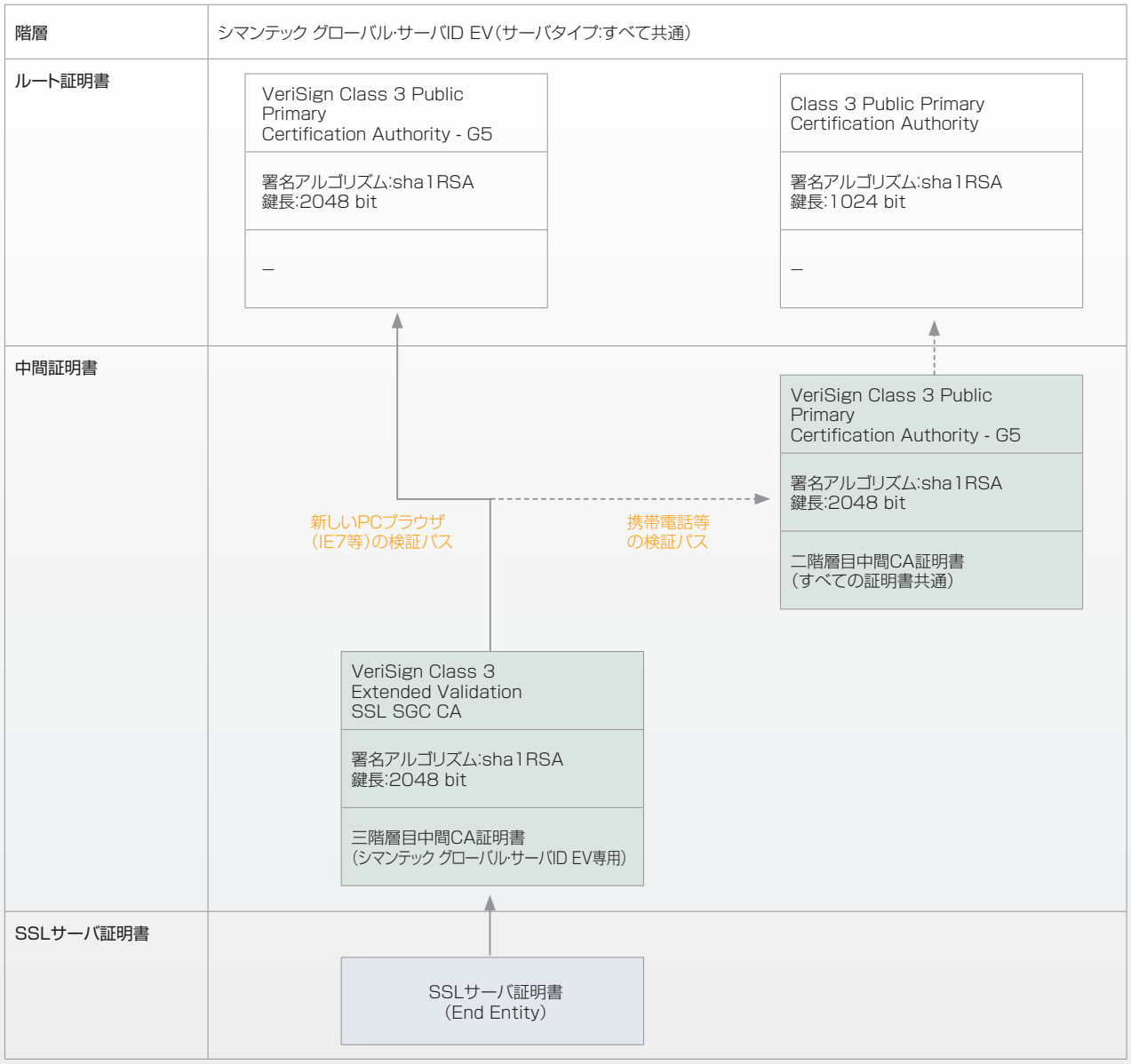
シマンテック SSL サーバ証明書には、以下の 4 種類があります。しかしながら、暗号アルゴリズム 2010 年問題の対応によりシマンテック グローバル・サーバ ID とシマンテック セキュア・サーバ ID に対して、2010 年 10 月に仕様変更いたしました。さらに、申請者が選択する「サーバタイプ」によって、発行される SSL サーバ証明書に対応する認証局（ルート証明書）が異なります。

以下では、それぞれの SSL サーバ証明書に対応する認証局（ルート認証局）を図解します。

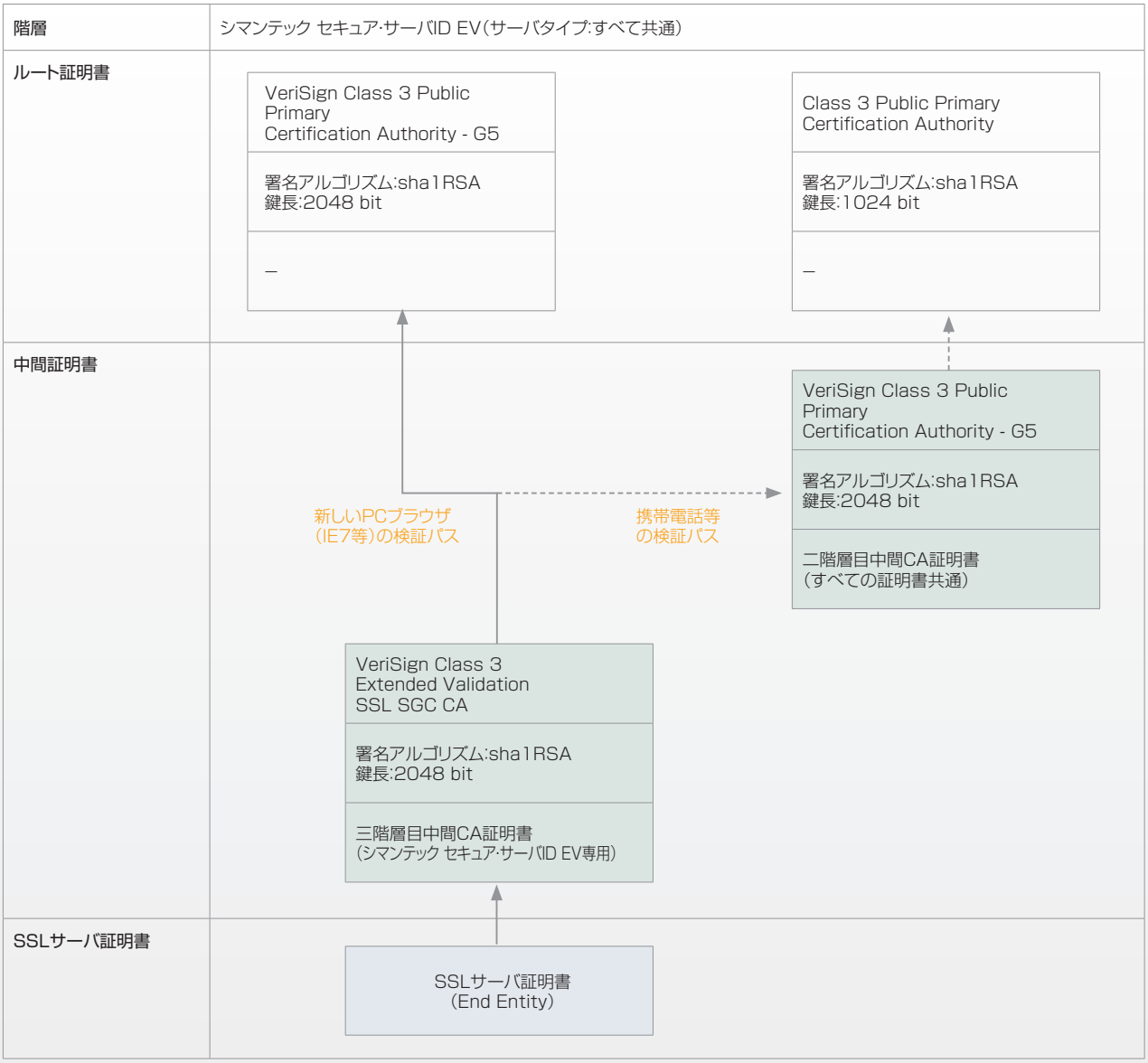
（1）シマンテック グローバル・サーバ ID EV
（2）シマンテック セキュア・サーバ ID EV
（3）シマンテック グローバル・サーバ ID
（4）シマンテック セキュア・サーバ ID



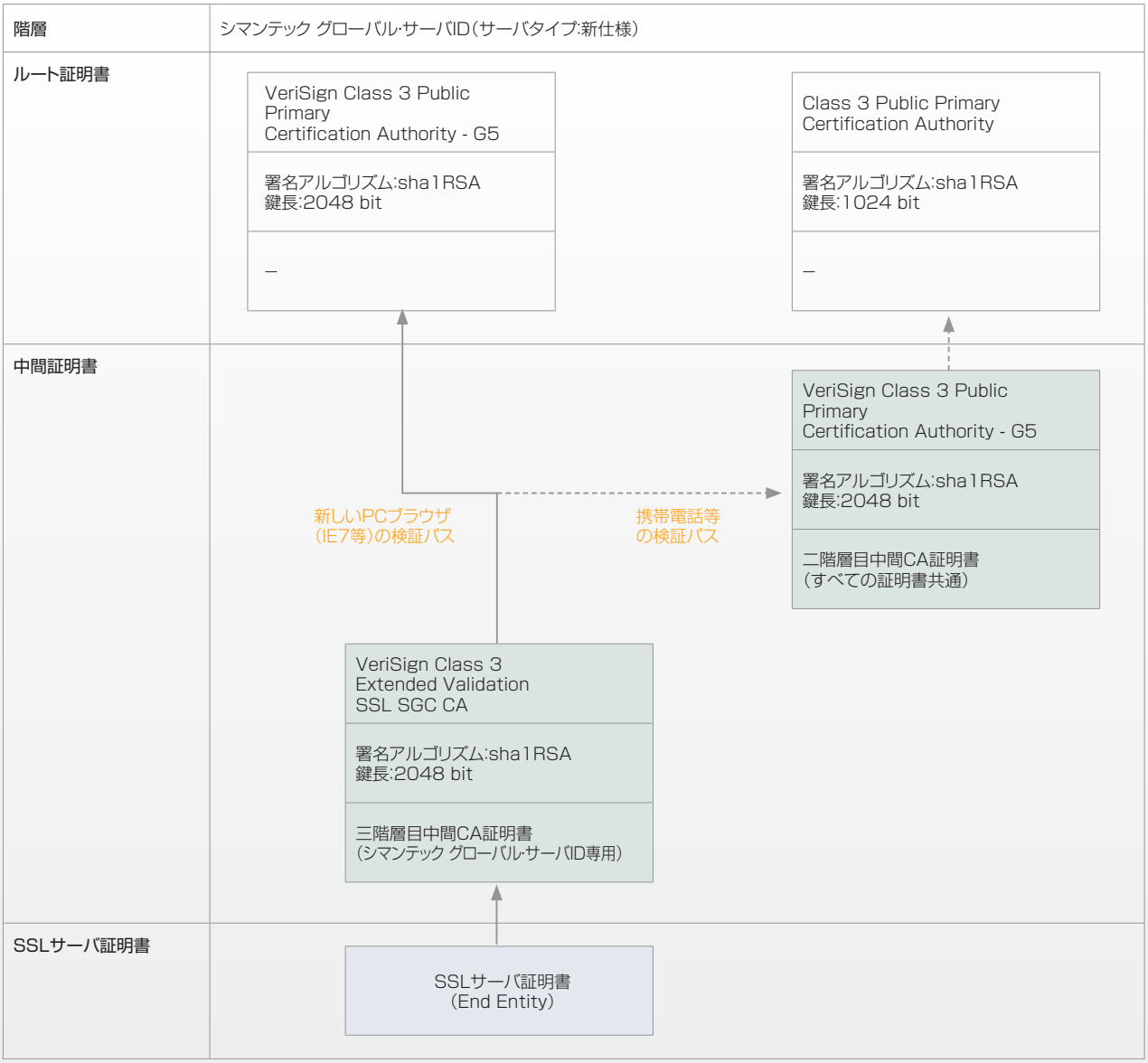
シマンテック グローバル・サーバID EV（サーバタイプ:すべて共通）



シマンテック セキュア・サーバID EV（サーバタイプ:すべて共通）

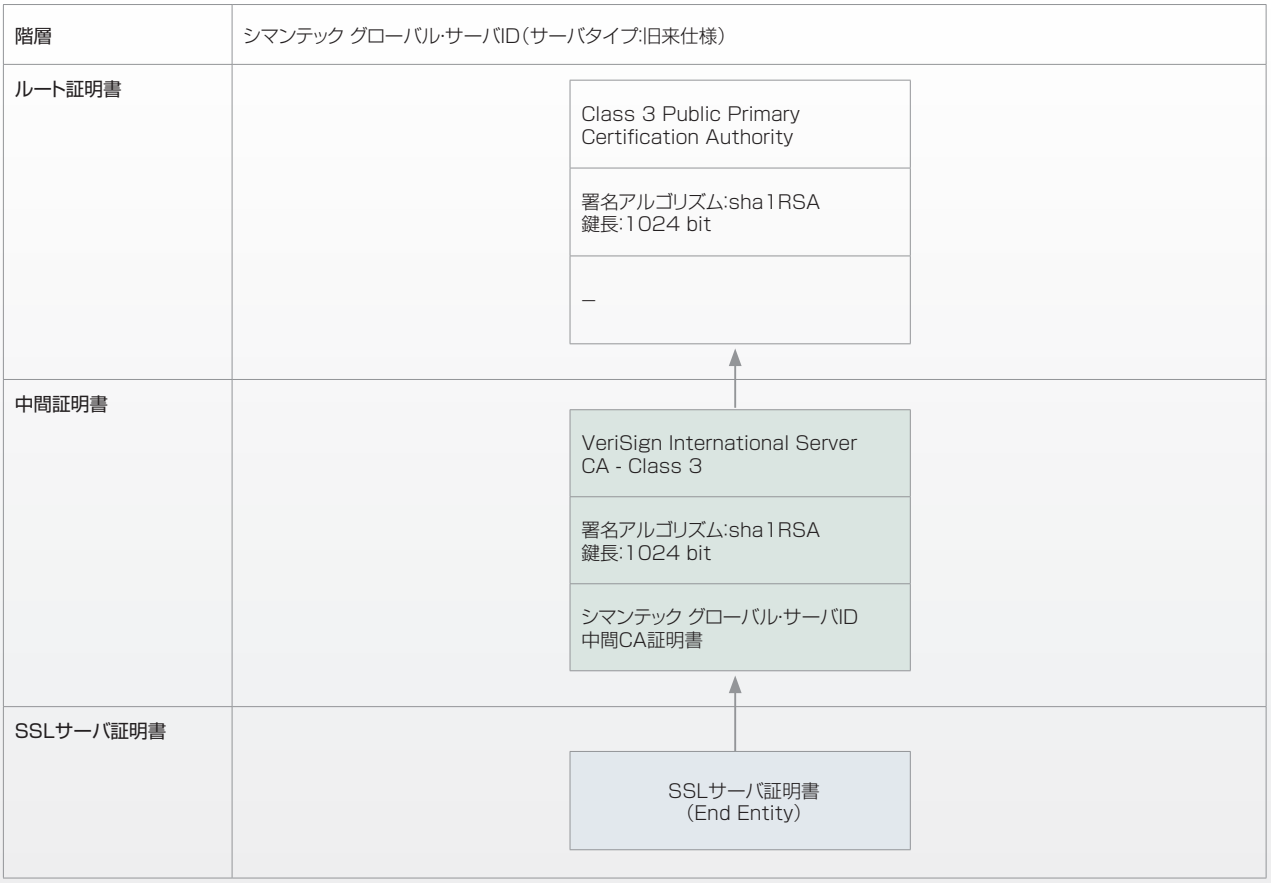


シマンテック グローバル・サーバID（サーバタイプ:新仕様※1）



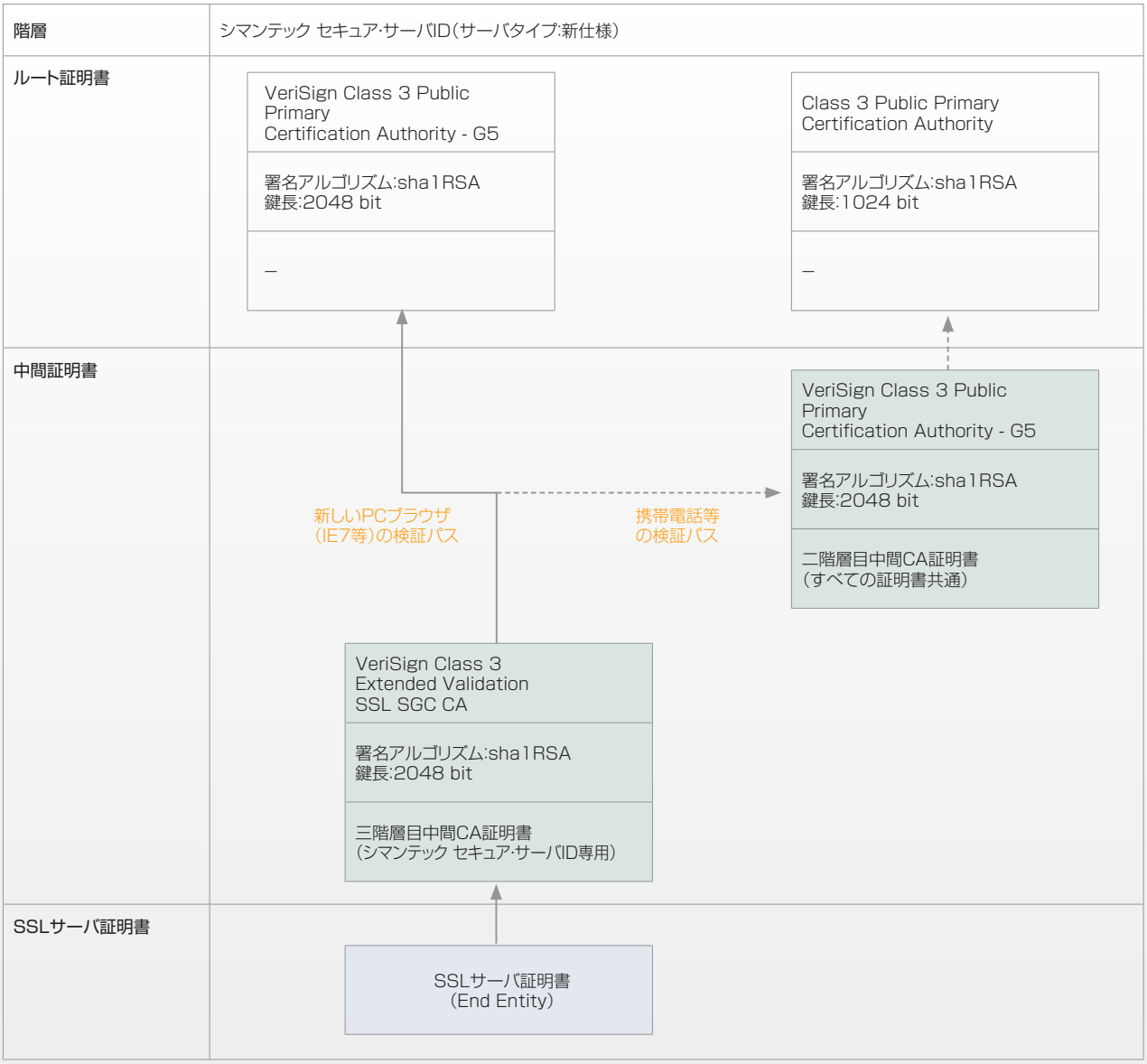
※ 1 : ストアフロントをご利用のお客様は、「マイクロソフト」と「マイクロソフト以外のサーバ」の 2 種類を選択した場合に発行されます。
シマンテック マネージド PKI for SSL をご利用のお客様は、「Old Premium SSL」以外を選択した場合に発行されます。

シマンテック グローバル・サーバID（サーバタイプ:旧来仕様※2）



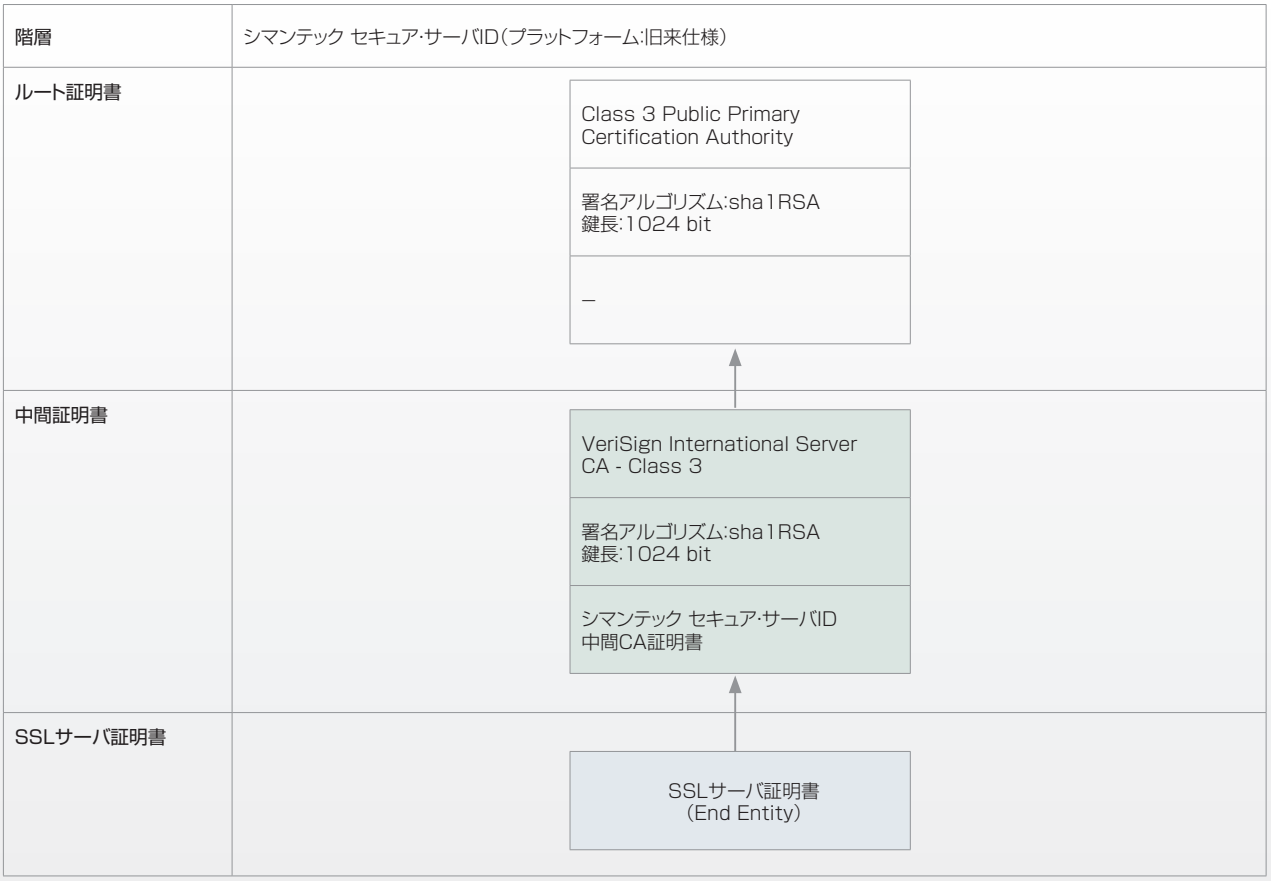
※ 2 : ストアフロントをご利用のお客様は、「旧来仕様（1024bit）- マイクロソフト」と「旧来仕様（1024bit）- マイクロソフト以外」の 2 種類を選択した場合に発行されます。
シマンテック マネージド PKI for SSL をご利用のお客様は、「Old Premium SSL」を選択した場合に発行されます。

シマンテック セキュア・サーバID（サーバタイプ:新仕様※3）



※ 3 : ストアフロントをご利用のお客様は、「マイクロソフト」と「マイクロソフト以外のサーバ」の 2 種類を選択した場合に発行されます。
シマンテック マネージド PKI for SSL をご利用のお客様は、「3 階層 中間 CA 1024bit（IIS 用）」と「3 階層 中間 CA 1024bit（IIS 以外）」の 2 種類を選択した場合に発行されます。

シマンテック セキュア・サーバID（プラットフォーム:旧来仕様※4）



※ 4 : ストアフロントをご利用のお客様の場合、「旧来仕様（1024bit）- マイクロソフト」と「旧来仕様（1024bit）- マイクロソフト以外」の 2 種類があります。シマンテック マネージド PKI for SSL をご利用のお客様の場合、「3 階層 中間 CA 1024bit（IIS 用）」と「3 階層 中間 CA 1024bit（IIS 以外）」の 2 種類があります。

WPROOT2010_1308

合同会社シマンテック・ウェブサイトセキュリティ
https://www.jp.websecurity.symantec.com/
〒104-0028　東京都港区赤坂1-11-44赤坂インターシティ
Tel : 0120-707-637
E-mail : websales_jp@symantec.com