[補足資料]
2016年4月(予定)のマイクロソフト社のルート証明書情報更新の影響と対策に関するご案内について

最終更新日：2016年4月1日
合同会社シマンテック・ウェブサイトセキュリティ

※ 本資料は上記の最終更新日時点での情報に基づいて可能な限り正確かつ最新の情報が記載されるよう細心の注意を払っておりますが、今後変更される可能性がございますので、ご了承ください。

※ 最新の情報は以下のウェブサイトを併せてご参照ください。
Knowlege Base [2016年4月(予定)のマイクロソフト社のルート証明書情報更新の影響と対策に関するご案内]
https://knowledge.symantec.com/jp/support/ssl-certificates-support/index?page=content&id=ALERT2009

はじめに：ご案内の対象のお客様

- お客様が管理されるサーバについて、本件のご案内の対象となり影響の有無ならびに対策をご検討いただく必要があるか否かを、以下の2点を踏まえてご確認ください。
  1) サポート対象クライアント、ならびに
  2)「クロスルート設定」(*1)の有無

サポート対象クライアント / クロスルート設定の有無	Windows OS上で動作するブラウザ等(*2)を含む (不特定多数のユーザによる、PCブラウザを含む不特定のクライアント環境からのアクセスを想定している場合を含みます)	Windows OS上で動作するブラウザ等(*2)を含まない (例:POSやATMなどの業務端末や機器、OA機器や家電、従来型の携帯電話のみをサポート対象とする場合)
「あり」の場合	本件のご案内の対象です。 ご案内の内容をご確認の上、「クロスルート設定」を解除いただく等の対策をいただくことを推奨します。	本件のご案内の対象外です。 (セキュリティへの考慮から、可能な限り早期にクロスルート設定を解除いただくことを推奨します)
「なし」の場合	本件のご案内の対象外です。	
不明の場合	以下の記事をご参照いただきクロスルート設定の有無を判別してください。 FAQ：インストールした証明書の確認方法(チェックサイトでの確認方法)] https://knowledge.symantec.com/jp/support/ssl-certificates-support/index?page=content&id=SO22875	

*1：詳細はp5参照

*2：詳細はp4参照。ブラウザ以外にも、サーバ間通信を行うWindows Server、Windows Phone等のモバイル機器や業務端末等、Windows OS上のルート証明書ストアを利用する各種ミドルウェア/ソフトウェアも対象となる可能性があります

(ご参考) Windows OS上のブラウザでの警告/エラー表示イメージ

シマンテック SSLサーバ証明書を利用してSSL/TLS通信を行った際に、次ページの条件に全て該当する場合、Windows OS上で動作するInternet ExplorerやGoogle Chrome等、一部のブラウザにて「このWebサイトのセキュリティ証明書には問題があります」等のエラー画面が表示され、正しくHTTPS接続ができない事象が発生します。

＜図1:エラー表示例1＞

OS : Windows 7
ブラウザ : Internet Explorer

＜図2:エラー表示例2＞

OS : Windows 7
ブラウザ : Google Chrome

警告/エラー事象の発生条件ならびに範囲

本日時点までの再現試験ならびにマイクロソフト社への照会の結果、当該事象が発生することが判明している条件ならびに範囲は以下の通りです。

条件①：ウェブサーバ環境にて、シマンテックの下記SSLサーバ証明書のいずれかの製品を
クロスルート設定あり(*1, p5参照)で導入・設定している場合
・シマンテック EV SSL証明書
・シマンテック グローバル・サーバID、シマンテック セキュア・サーバID

条件②：クライアント環境が以下表1のいずれかのOSとブラウザの組み合わせであること
(表1への補記「※注1」も併せてご確認ください))

条件③：クライアント環境のルート証明書ストア(Windows Trusted Root Store)に、G5ルート証明書(*2)が含まれていないこと

条件④：マイクロソフト社のルート証明書更新情報が配信されることによりクライアント環境のルート証明書ストアに搭載されているG1ルート証明書(*3)のWindows上のプロパティ「サーバー認証」がOFF(信頼停止)とされた状態となること

＜表1：当該事象が発生することが判明しているOSとブラウザの組み合わせ＞

OS	ブラウザ
Windows Vista, Windows 7, Windows 8.1, Windows 10	Internet Explorer
	Google Chrome
	Opera
	Microsoft Edge Browser

※注1：＜ご注意ください＞:左記の組み合わせ以外にも、サーバ間通信を行うWindows Server、Windows Phone等のモバイル機器や業務端末等、Windows OS上のルート証明書ストアを利用する各種ミドルウェア/ソフトウェアも対象となる可能性があります。お客様にてご利用中のプラットフォームが対象となるか否かの詳細についてはマイクロソフト社へお問合せください。
当社にてより詳細かつ網羅的な情報が入手でき次第、弊社ウェブサイトならびに当補足資料等に追加掲載させていただきます。

*1：現在のウェブサーバの設定は以下のチェックサイトでもご確認いただけます。
FAQ：インストールした証明書の確認方法(チェックサイトでの確認方法)
https://knowledge.symantec.com/jp/support/ssl-certificates-support/index?page=content&id=SO22875

*2：「VeriSign Class 3 Public Primary Certification Authority - G5」、通称「G5ルート」、詳細はp5-6参照

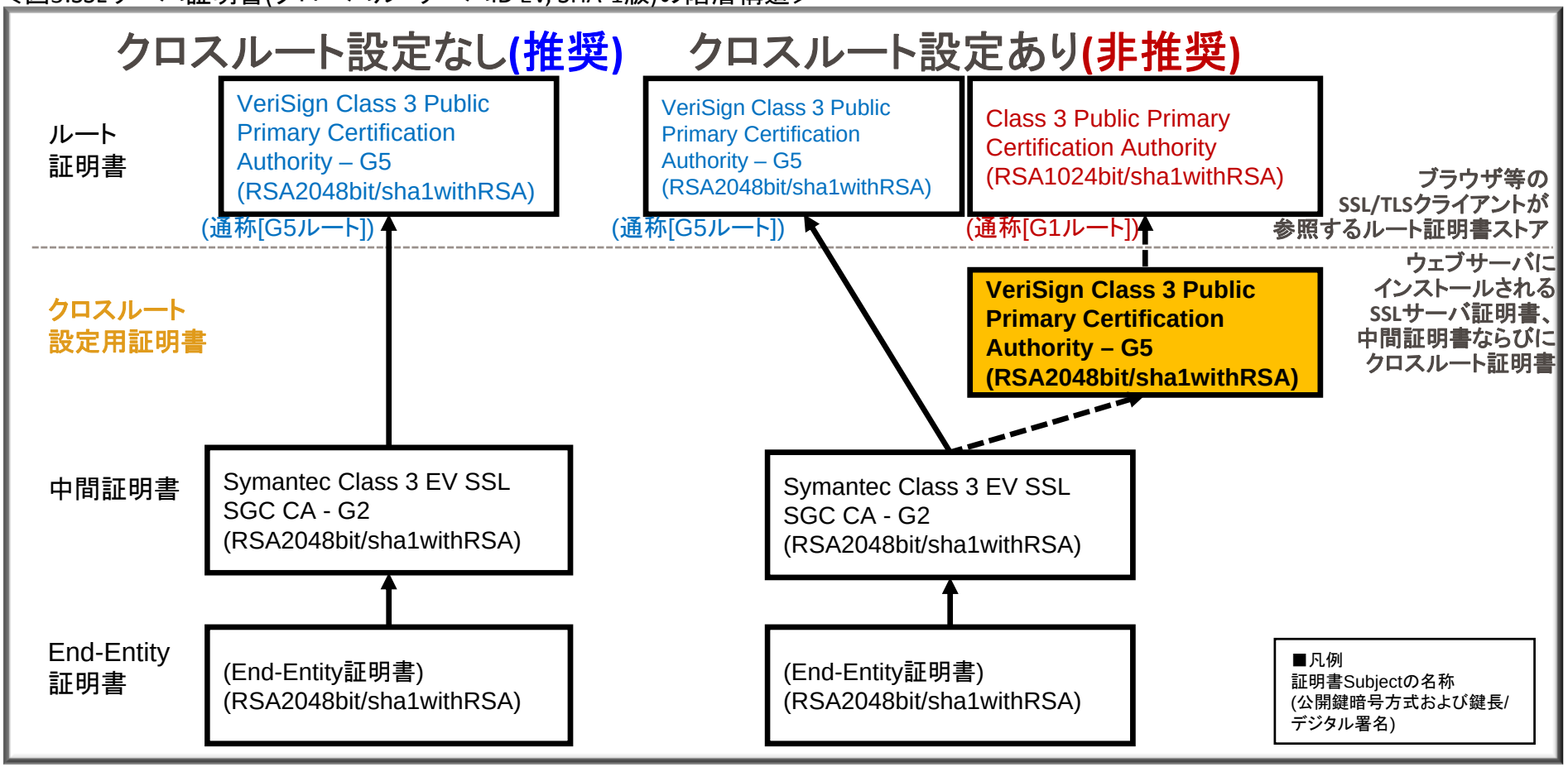
*3：「Class 3 Public Primary Certification Authority」、通称[G1ルート]、詳細はp5-6参照

(条件① 補足説明) クロスルート証明書とは

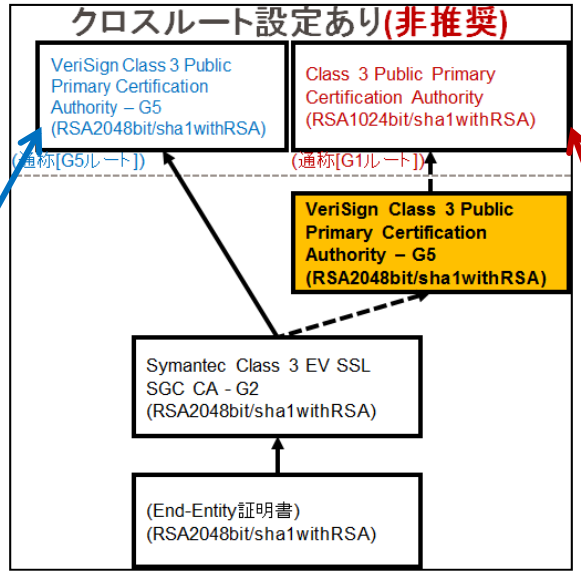
POSやATMなどの業務端末や機器、OA機器や家電、従来型の携帯電話では新しい暗号技術(*1)に対応したルート証明書(*2)が搭載されていない場合があります。新しいルート証明書は搭載されていないが、古くから普及するルート証明書(*2)は搭載されている場合、サーバ側に併せてクロスルート証明書を設定することによって、こうしたクライアント環境での証明書の検証が可能(*3)となります。

*1:公開鍵暗号におけるRSA2048bit、デジタル署名におけるSHA-2アルゴリズム等を指します。
*2:シマンテックのSSLサーバ証明書製品(全製品共通)における「新しい暗号技術に対応したルート証明書」ならびに「古くから普及するルート証明書」とは、以下のルート証明書を指します。
新しい暗号技術に対応したルート証明書「VeriSign Class 3 Public Primary Certification Authority - G5」(通称[G5ルート])
古くから普及するルート証明書:「Class 3 Public Primary Certification Authority」(通称[G1ルート])
*3:不特定多数のユーザから、PCブラウザを含む不特定のクライアント環境からのアクセスを想定している場合は、クロスルート証明書の設定は推奨されません。
https://knowledge.symantec.com/jp/support/ssl-certificates-support/index?page=content&id=SO28069

＜図3:SSLサーバ証明書(グローバル・サーバID EV, SHA-1版)の階層構造＞



(条件③、④ 補足説明)
G5ルート、G1ルートとは



VeriSign Class 3 Public Primary Certification Authority – G5 (通称G5ルート)		
Windows OS 搭載状況	Windows 2000/ME以前	未搭載
	Windows XP以降	オンライン自動配信プログラムで配信
公開鍵	**RSA2048bit**	
識別情報	発行者: VeriSign Class 3 Public Primary Certification Authority – G5 発行先: VeriSign Class 3 Public Primary Certification Authority – G5 有効期限 : 2036年7月17日(日本時間) シリアル番号 : 18 da d1 9e 26 7d e8 bb 4a 21 58 cd cc 6b 3b 4a SHA-1 fingerprint : 4e b6 d5 78 49 9b 1c cf 5f 58 1e ad 56 be 3d 9b 67 44 a5 e5	

Class 3 Public Primary Certification Authority (通称G1ルート)		
Windows OS 搭載状況	Windows 2000/ME以前	プレインストール
	Windows XP以降	プレインストール
公開鍵	**RSA1024bit**	
識別情報1	発行者 : Class 3 Public Primary Certification Authority 発行先 : Class 3 Public Primary Certification Authority 有効期限 : 2028年8月2日(日本時間) シリアル番号 : 70 ba e4 1d 10 d9 29 34 b6 38 ca 7b 03 cc ba bf SHA-1 fingerprint : 74 2c 31 92 e6 07 e4 24 eb 45 49 54 2b e1 bb c5 3e 61 74 e2	
識別情報2	発行者 : Class 3 Public Primary Certification Authority 発行先 : Class 3 Public Primary Certification Authority 有効期限 : 2028年8月3日(日本時間) シリアル番号 : 3c 91 31 cb 1f f6 d0 1b 0e 9a b8 d0 44 bf 12 be SHA-1 fingerprint : a1 db 63 93 91 6f 17 e4 18 55 09 40 04 15 c7 02 40 b0 ae 6b	

(条件④ 補足説明)
マイクロソフト社Windows OS上のルート証明書プロパティ

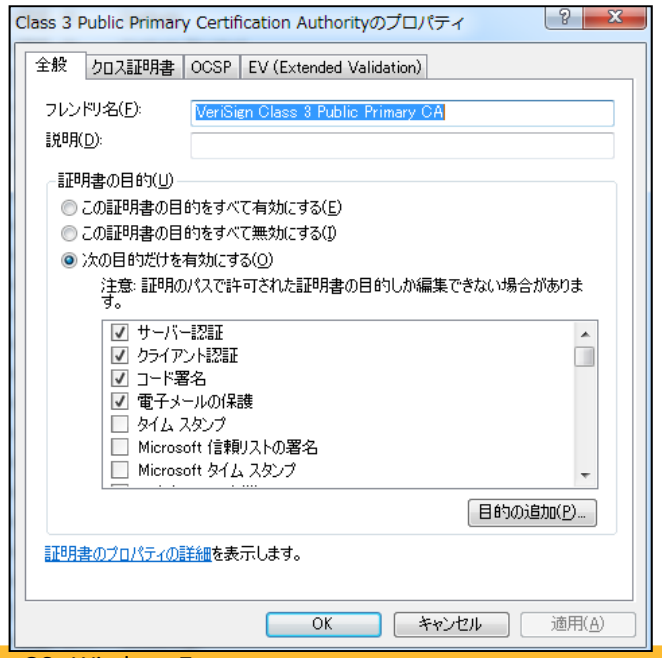
- マイクロソフト社のWindows OS上では、各認証局が提供するルート証明書に対して、追加でプロパティ情報(ルート証明書の用途に応じて複数存在する)を付与しております。

  (参考:英語)Microsoft Trusted Root Certificate Program Updates
  http://social.technet.microsoft.com/wiki/contents/articles/31680.microsoft-trusted-root-certificate-program-updates.aspx

- このたびマイクロソフト社より、以下の日程でWindows OSに対するルート証明書更新情報を配信しシマンテックのG1ルート(詳細後述)における「サーバー認証」プロパティをOFF (信頼停止)とする予定である旨の通知を受領しました。

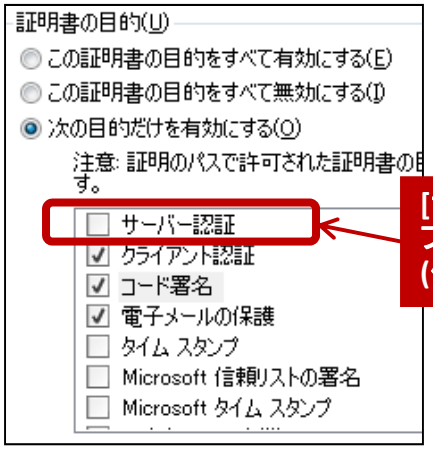
  – 配信日時(予定) : 2016年4月19日(火)または20日(水)(日本時間) (米国時間2016年4月19日(火))

本日時点(2016年4月19/20日(予定)まで)の
Windows OS上の「G1ルートのプロパティ」



OS : Windows 7

2016年4月19/20日(予定)以降の
Windows OS上の「G1ルートのプロパティ」



**[サーバー認証]
プロパティ情報をOFF
(信頼停止)にした状態**

(条件③ 補足説明)
Windows OSのルート証明書ストアにG5ルートが搭載される条件

Windows XP以降のOSではG5ルート(VeriSign Class 3 Public Primary Certification Authority - G5)は出荷時点ではプレインストールされていませんが、以下の4つの方法(タイミング)で追加されます。

#	ルート証明書ストア追加方法	対象OS	自動/手動	説明
1	ウェブサイトへのアクセスによる自動インストール 条件:シマンテックのSSLサーバ証明書(クロスルート証明書設定なし)を利用いただいているウェブサイト	XP以降	自動	・httpsサイト(認証局を問わず)初回接続時に、マイクロソフト社のオンラインストアからルート証明書リスト(キャッシュファイル)をダウンロードします。 ・その後httpsサイト接続都度、キャッシュファイルから必要なルート証明書を「信頼されたルート証明機関」に自動的に追加し、利用可能な状態とします。 **(参考)マイクロソフト社による自動インストール機能の説明** http://blogs.technet.com/b/jpntsblog/archive/2009/12/24/windows-pki-2.aspx
2	ノートンセキュアドシール(旧ベリサイン シール)の「EV Upgrader」機能	XP以降	自動	ノートンセキュアドシールが掲載されたウェブサイトに接続時に、シールに含まれるスクリプト機能により、G5ルートストアを自動的に「信頼されたルート証明機関」へ登録します。
3	「ルート証明書の更新プログラム」を適用	XP以降	手動	個別クライアントOS環境毎にexeをダウンロードして実行することで、MSFTが利用可能とする全てのルート証明書が「信頼されたルート証明機関」に展開され、利用可能な状態になります。
4	Windows Updateにて「カスタム」の「ルート証明書更新プログラム」を選択し実行	XPのみ	(半)自動	上記#4をWindows Updateメニューから実行するものです (Windows Vista以降では対象外です)

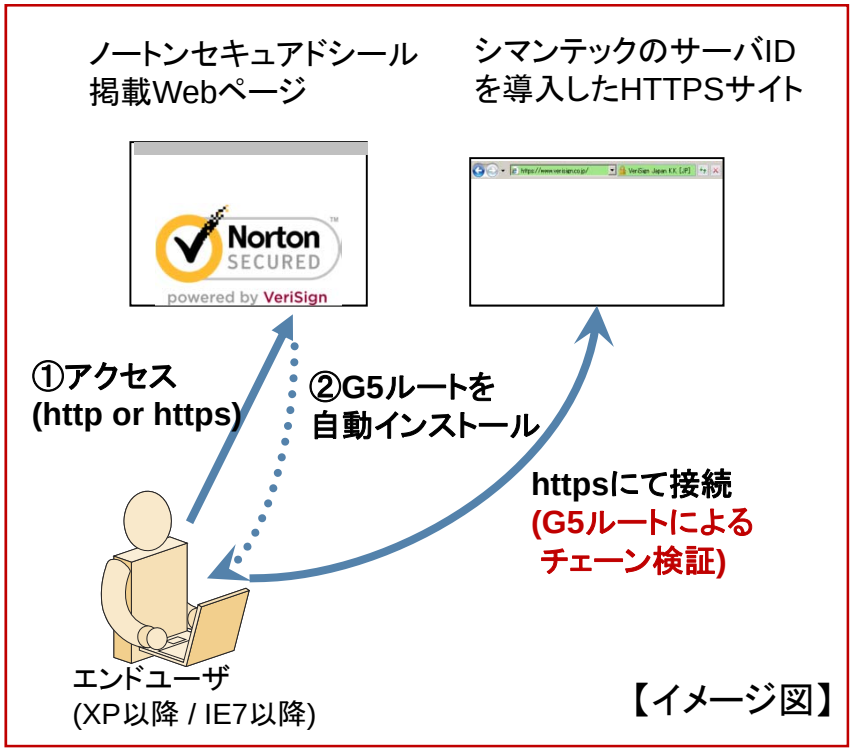
(条件③ 補足説明)
(ご参考)EV Upgraderとは

- EV Upgraderとは、Windows XP以降 & IE7以降を利用しているクライアントが、ノートンセキュアドシール(旧ベリサイン シール)を掲載するウェブページにアクセスした際に、G5ルート証明書を自動インストールさせる仕組みです
- EV Upgraderは2007年から今日まで提供を継続しております。
- ノートンセキュアドシールは1日あたり6億5千万回表示されており、G5ルートは大多数のWindows PCに既に搭載されていると考えられます。

EV Upgraderの仕組み

① クライアントがノートンセキュアドシールの掲載されたウェブページにアクセスします。

② G5ルート証明書がクライアントに自動インストールされます。インストールはバックグラウンドで自動的に行われるため、ユーザが意識することはありません。



■シールデザインの変遷(2007年以降)

一貫してEV Upgrader機能を提供中

警告/エラー事象の回避方法 (1/3)

	ケース1	ケース2	ケース3	ケース4
[ウェブサーバ側] クロスルート証明書設定の有無	あり	あり → なし(方法1)	なし	なし
[クライアント側] Windows OSのルートストア におけるG5ルート証明書の有無	あり	なし → あり(方法2)	あり	なし
クライアント側での 警告/エラー表示	警告/エラー画面は表示されません	上記方法1または方法2のいずれかを実施することで、警告/エラー画面が表示されなくなります。	警告/エラー画面は表示されません	警告/エラー画面は表示されません (*1)

■方法1 :ウェブサーバ側での回避方法

- ウェブサーバ管理者の操作によって回避する方法です。
  (サポート対象クライアントにWindows 2000, Windows MEあるいはこれ以前のレガシープラットフォーム、または従来型の携帯電話等、新しい暗号技術に対応したG5ルート証明書が搭載されていない環境が含まれる場合、こうした環境で警告/エラー表示される場合がありますので ご注意ください)
- 詳細は次頁以降を参照ください。

■方法2 : クライアント環境での回避方法

- 各クライアントPC(端末)での操作によって回避する方法です。
  (対象となる全てのクライアント環境での対応が必要となる点にご注意ください)
- 詳細は次頁以降を参照ください。

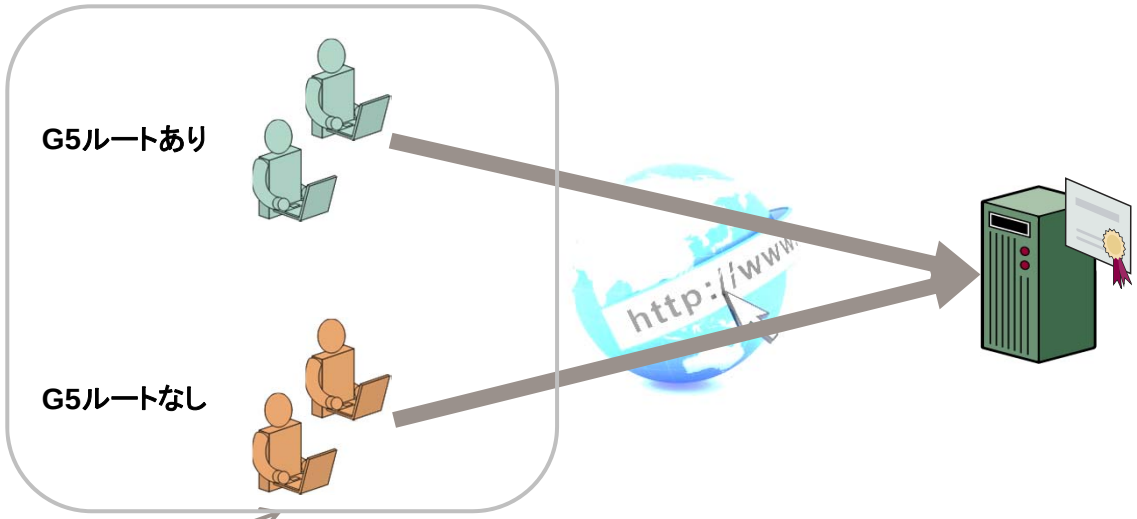
*1 : Windows OSでは、httpsサイト(認証局を問わず)初回接続時に、マイクロソフト社のオンラインストアからルート証明書リスト(キャッシュファイル)をダウンロードし、都度、キャッシュファイルから必要なルート証明書を「信頼されたルート証明機関」に自動的に追加し、利用可能な状態とします。
(参考)マイクロソフト社による自動インストール機能の説明 http://blogs.technet.com/b/jpntsblog/archive/2009/12/24/windows-pki-2.aspx

警告/エラー事象の回避方法 (2/3)
方法1 : ウェブサーバ側での回避方法

※ サポート対象クライアントにWindows 2000, Windows MEあるいはこれ以前のレガシープラットフォーム、または従来型の携帯電話等、新しい暗号技術に対応したG5ルート証明書が搭載されていない環境が含まれる場合、こうした環境で警告/エラー表示される場合がありますのでご注意ください。

<クライアント環境>
Windows OSユーザ

<ウェブサーバ環境>



クロスルート設定なし(推奨)

Symantec Class 3 EV SSL SGC CA - G2
(RSA2048bit/sha1withRSA)

(End-Entity証明書)
(RSA2048bit/sha1withRSA)

※ クライアント環境はG5ルートあり/なし、いずれの場合も回避可能となります。
注)ウェブサーバ側がクロスルート設定なしの場合、クライアント環境にG5ルート証明書がない場合Windowsルート証明書プログラムによって、自動的に必要なG5ルート証明書がダウンロードされ、インストールされます。

方法1 : ウェブサーバ側でクロスルート設定用証明書を削除していただくことで、当事象を回避することができることが確認されております。

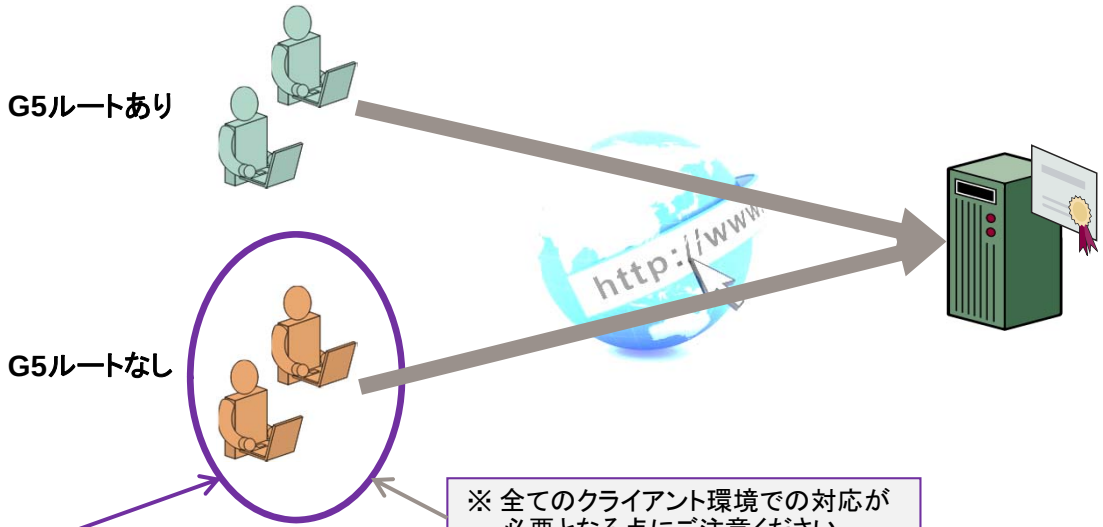
■クロスルート設定用証明書の削除方法
https://knowledge.symantec.com/jp/support/ssl-certificates-support/index?page=content&id=SO28077

警告/エラー事象の回避方法 (3/3)
方法2 : クライアント環境での回避方法

※ サーバ側はクロスルート設定あり/なし、いずれの場合も回避可能となります。
注) クライアント環境にG5ルート証明書がある場合、ウェブサーバにクロスルート設定ありの場合も、Windowsクライアントはクロスルート設定用証明書を無視して、G5ルートでのチェーン検証を行います。

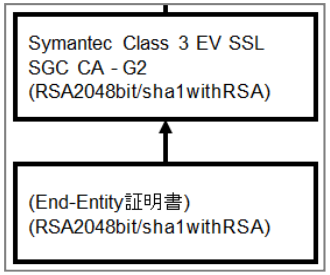
<クライアント環境>
Windows OSユーザ

<ウェブサーバ環境>

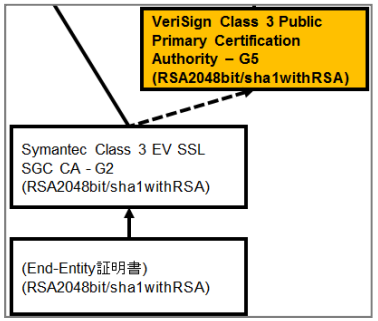


※ 全てのクライアント環境での対応が必要となる点にご注意ください。

クロスルート設定なし(推奨)



クロスルート設定あり(非推奨)



方法2 : クライアント環境で下記のサイトの手順を実施いただき、
G5ルートをルート証明書ストアにインストールいただくことで、
当該警告/エラー事象を回避できることが確認されております。

■SSL接続エラーの回避方法について
http://www.symantec.com/ja/jp/page.jsp?id=ssl-connection-avoidance