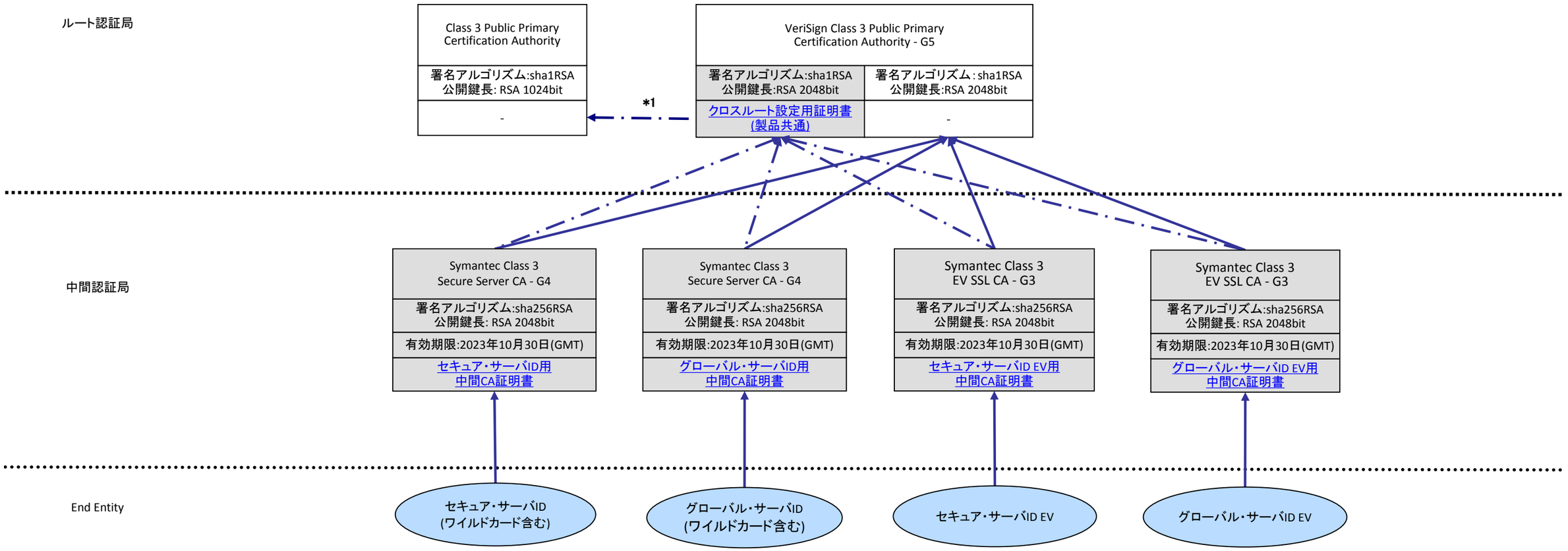
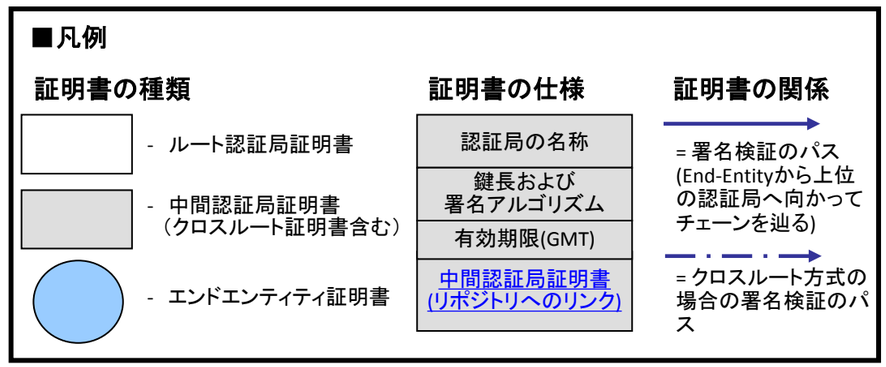
シマンテック RSA SHA-2対応版SSLサーバ証明書製品の階層構造

（2015年6月4日時点）



ご注意ください:
シマンテック ストアフロントで2014/9/15以前に申請した方、マネージドPKI for SSL にて2014/4/8以前に申請した方は中間CA証明書の署名アルゴリズムはRSA SHA-1となります、上記階層とは異なりますのでご注意ください。

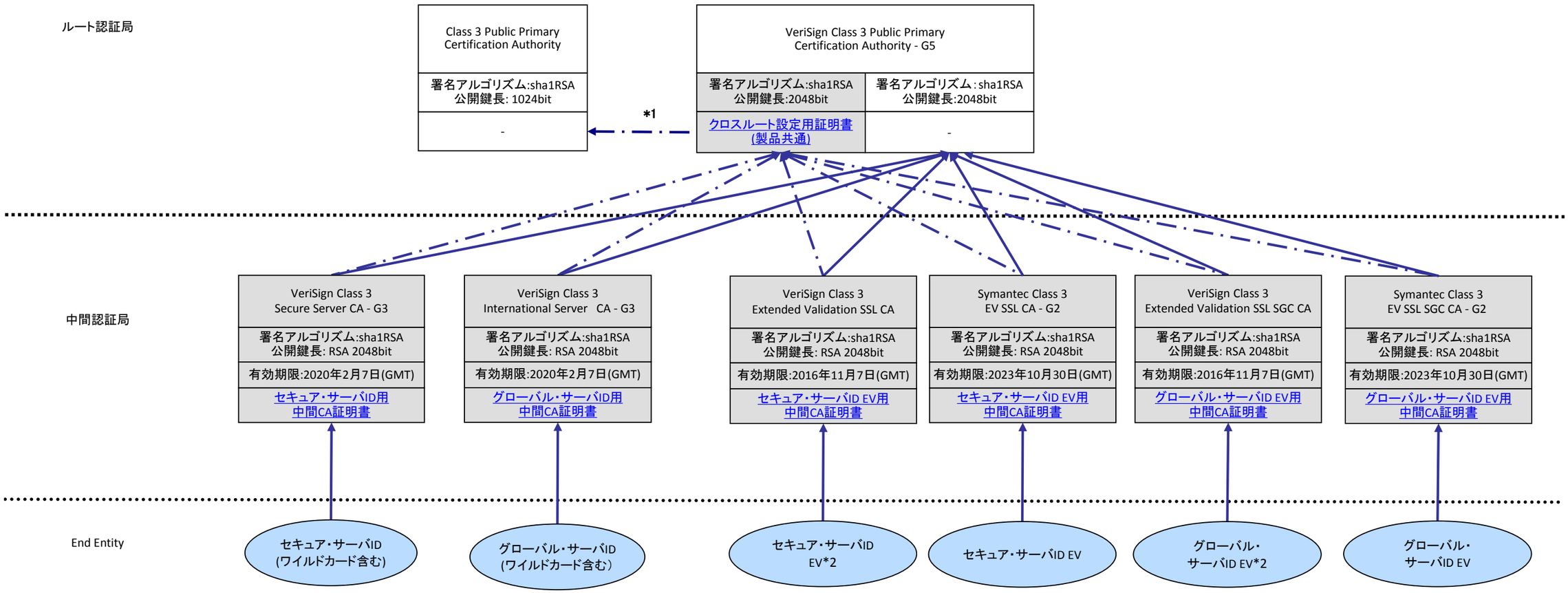
*1 : シマンテックのサーバID製品は、VeriSign Class3 Public Primary Certification Authority - G5 (通称:Class3PCA G5)に3階層でチェーンします。Class3PCA - G5ルート認証局証明書が搭載されていないレガシープラットフォームとの後方互換性を確保する目的でのみ、Class3 Public Primary Certification Authority (通称 Class3PCA G1)に4階層でチェーンさせることを当面の間許容します。(クロスルート方式と呼ばれます)



作成者 : 合同会社シマンテック・ウェブサイトセキュリティ
作成日 : 2016年2月16日

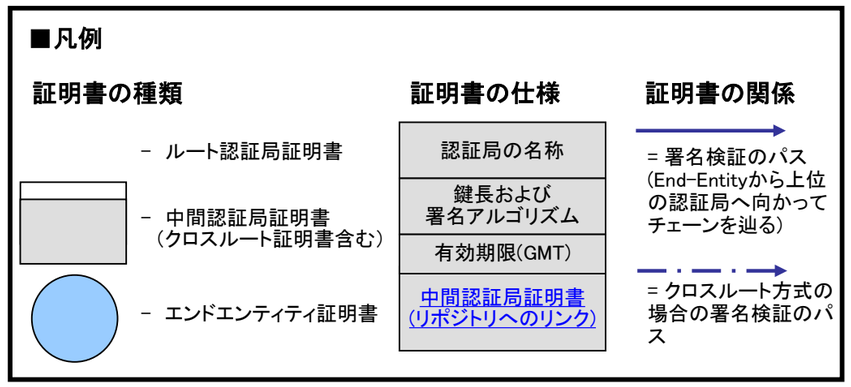
シマンテック　RSA SHA-1版SSLサーバ証明書製品の階層構造

（2015年6月4日時点）



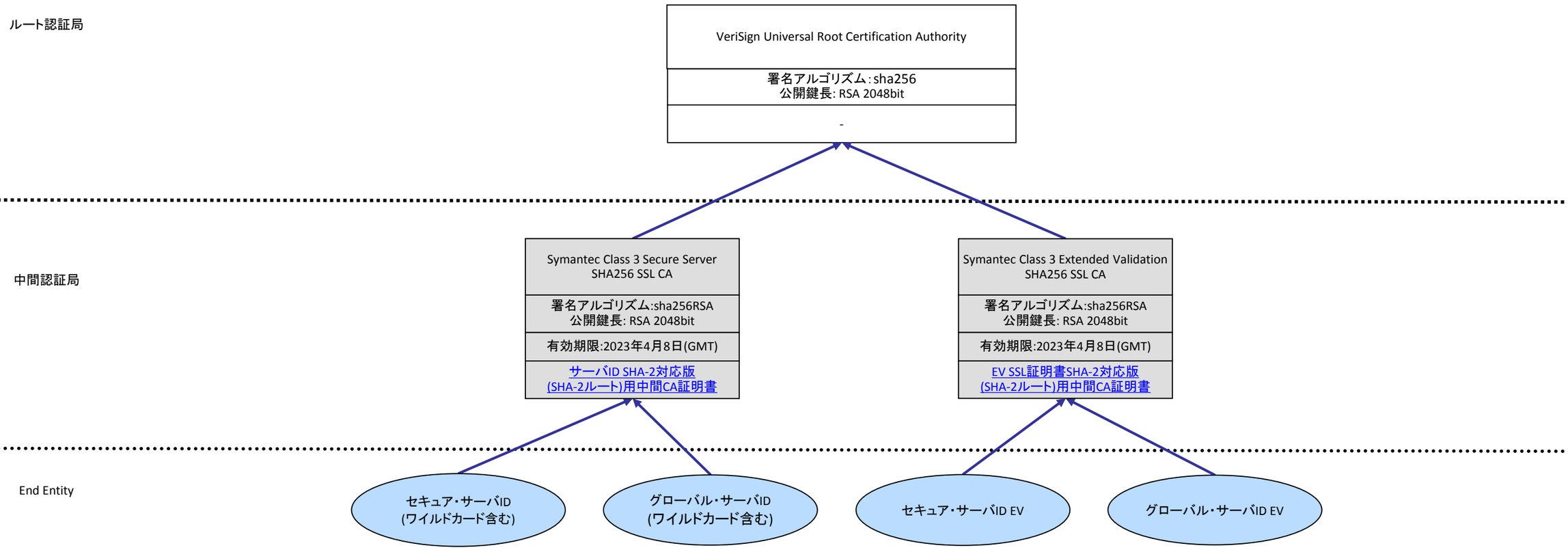
*1 : シマンテックのサーバID製品は、VeriSign Class3 Public Primary Certification Authority - G5 (通称:Class3PCA G5)に3階層でチェーンします。Class3PCA - G5ルート認証局証明書が搭載されていないレガシープラットフォームとの後方互換性を確保する目的でのみ、Class3 Public Primary Certification Authority (通称 Class3PCA G1)に4階層でチェーンさせることを当面の間許容します。(クロスルート方式と呼ばれます)

*2 : シマンテックストアフロントにて、2014/7/10以前にご申請、またはマネージドPKI for SSL にて、2014/7/24以前にご申請いただいた証明書が対象です。



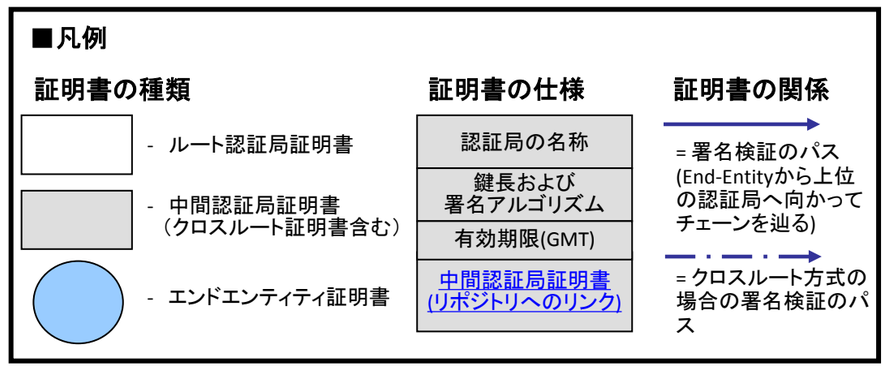
作成者 : 合同会社シマンテック・ウェブサイトセキュリティ
作成日 : 2016年2月16日

シマンテック RSA SHA-2対応版（SHA-2ルート）SSLサーバ証明書製品の階層構造



ご注意ください：
シマンテック ストアフロントで2014/9/15以前に申請した方、マネージドPKI for SSL にて2014/4/8以前に申請した方は中間CA証明書の署名アルゴリズムはRSA SHA-1となります、上記階層とは異なりますのでご注意ください。

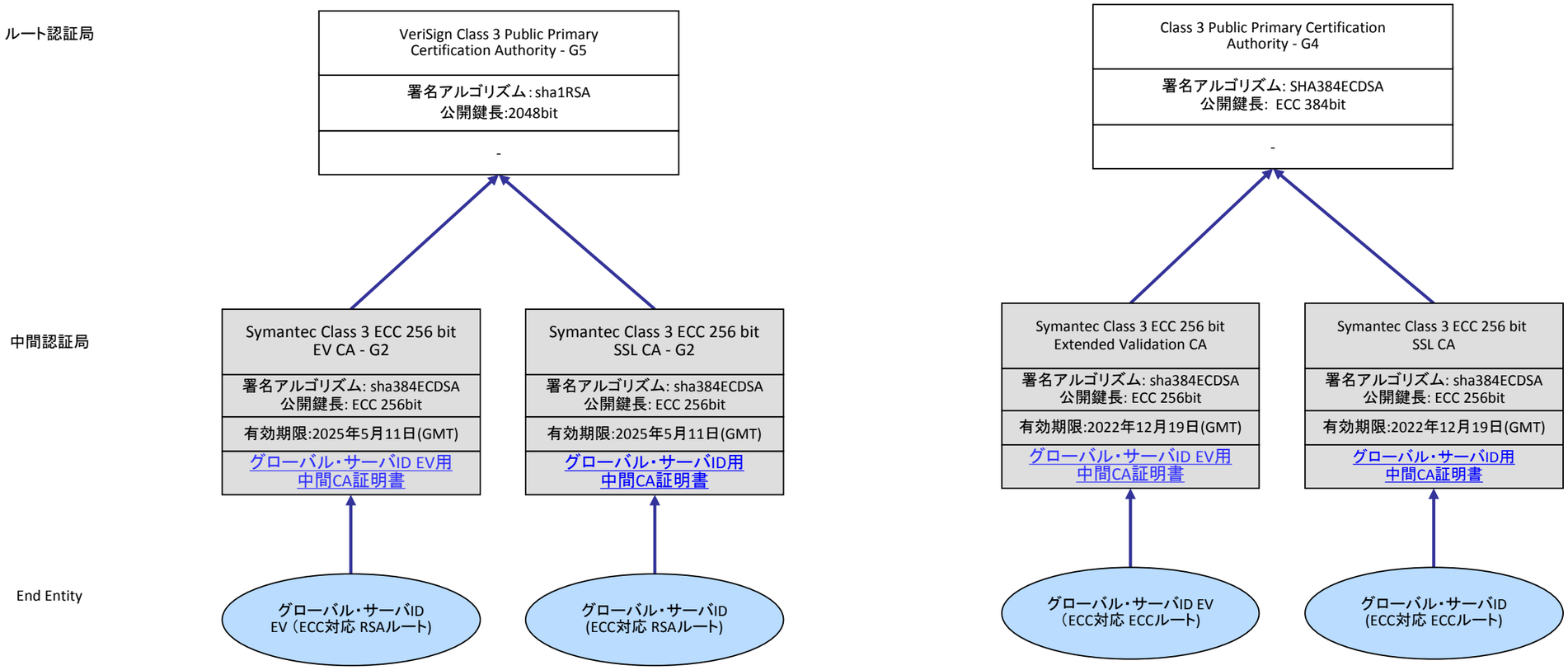
*1 : シマンテックのサーバID製品は、VeriSign Class3 Public Primary Certification Authority - G5 (通称:Class3PCA G5)に3階層でチェーンします。Class3PCA - G5ルート認証局証明書が搭載されていないレガシープラットフォームとの後方互換性を確保する目的でのみ、Class3 Public Primary Certification Authority (通称 Class3PCA G1)に4階層でチェーンさせることを当面の間許容します。(クロスルート方式と呼ばれます)

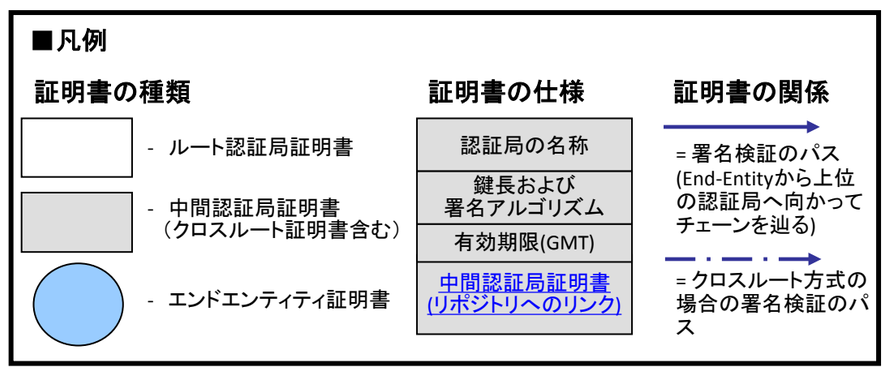


作成者：合同会社シマンテック・ウェブサイトセキュリティ
作成日：2016年2月16日

シマンテック ECC対応版SSLサーバ証明書の階層構造

（2015年8月31日時点）

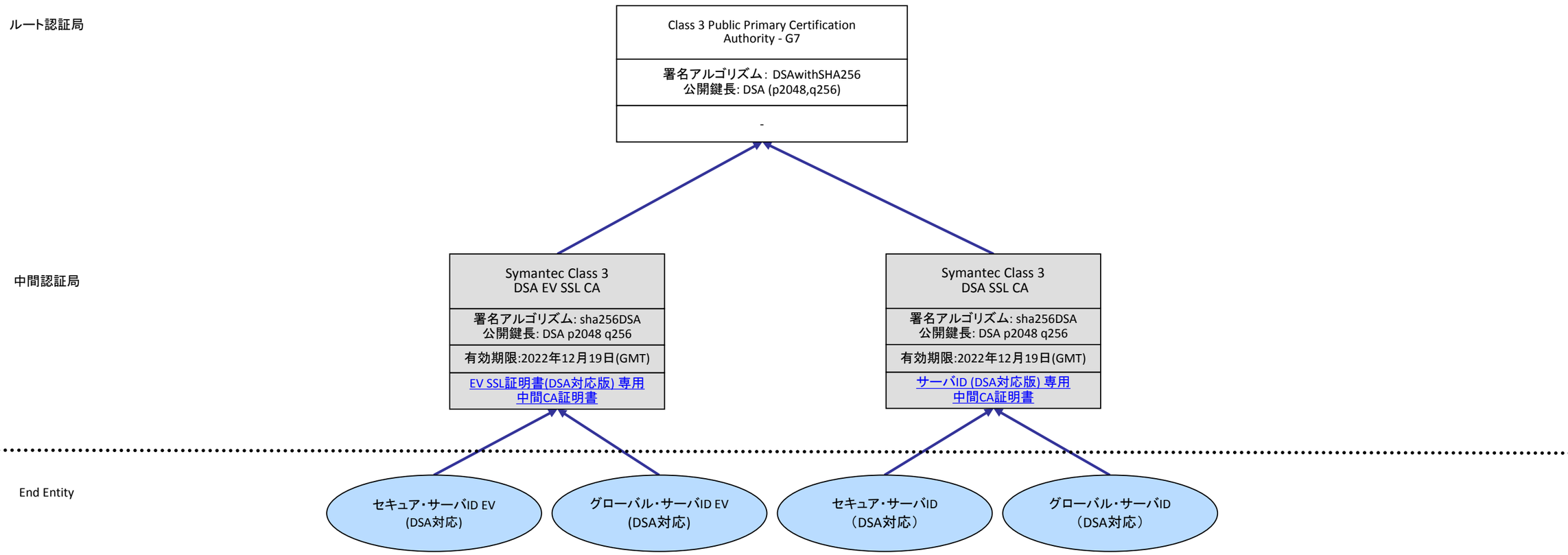




作成者：合同会社シマンテック・ウェブサイトセキュリティ
作成日：2016年2月16日

シマンテック DSA対応版SSLサーバ証明書の階層構造

（2014年12月1日時点）



作成者：合同会社シマンテック・ウェブサイトセキュリティ
作成日：2015年6月4日

シマンテック RSA SHA-2対応版コードサイニング証明書の階層構造

（2015年6月4日時点）

ルート認証局

Class 3 Public Primary Certification Authority	
署名アルゴリズム:sha1RSA 公開鍵長: 1024bit	
－	

*1

VeriSign Class 3 Public Primary Certification Authority - G5	
署名アルゴリズム:sha1RSA 公開鍵長:2048bit	署名アルゴリズム：sha1RSA 公開鍵長:2048bit
クロスルート設定用証明書 （製品共通）	－

中間認証局

Symantec Class 3 SHA256 Code Signing CA
署名アルゴリズム:sha256RSA 公開鍵長: RSA 2048bit
有効期限:2023年12月9日(GMT)
コードサイニング証明書用 中間CA証明書

End Entity

- コードサイニング証明書 for Adobe AIR
- コードサイニング証明書 for Microsoft Authenticode
- コードサイニング証明書 for Java
- コードサイニング証明書for ドキュメントサイニング
- コードサイニング証明書 for Microsoft Office and VBA

■凡例

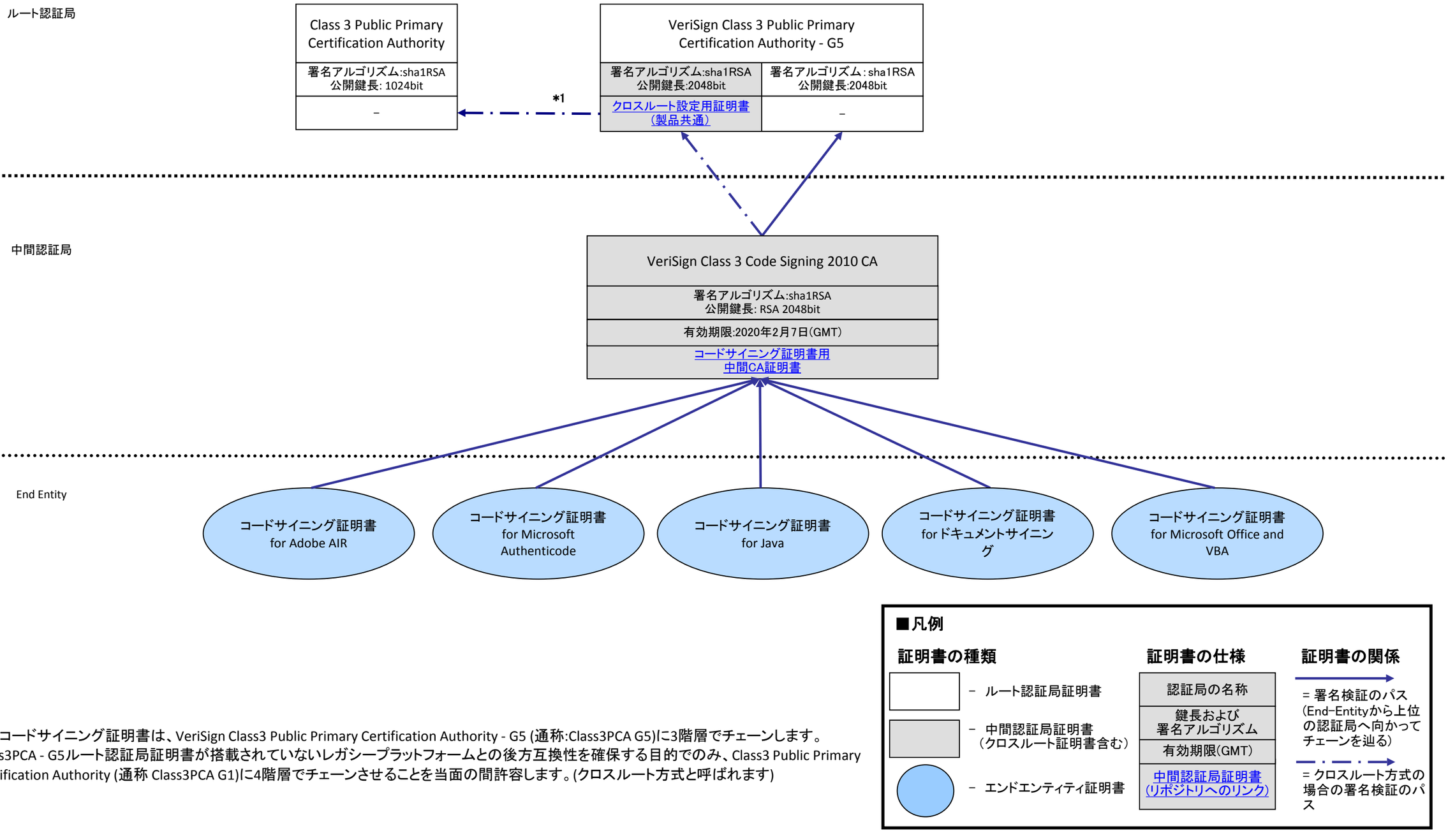
証明書の種類	証明書の仕様	証明書の関係
－ ルート認証局証明書	認証局の名称	= 署名検証のパス（End-Entityから上位の認証局へ向かってチェーンを辿る）
－ 中間認証局証明書（クロスルート証明書含む）	鍵長および署名アルゴリズム 有効期限(GMT)	= クロスルート方式の場合の署名検証のパス
－ エンドエンティティ証明書	中間認証局証明書（リポジトリへのリンク）	

*1 : コードサイニング証明書は、VeriSign Class3 Public Primary Certification Authority - G5 (通称:Class3PCA G5)に3階層でチェーンします。Class3PCA - G5ルート認証局証明書が搭載されていないレガシープラットフォームとの後方互換性を確保する目的でのみ、Class3 Public Primary Certification Authority (通称 Class3PCA G1)に4階層でチェーンさせることを当面の間許容します。(クロスルート方式と呼ばれます)

作成者：合同会社シマンテック・ウェブサイトセキュリティ
作成日：2016年2月16日

シマンテック RSA SHA-1版コードサイニング証明書の階層構造

（2015年6月4日時点）

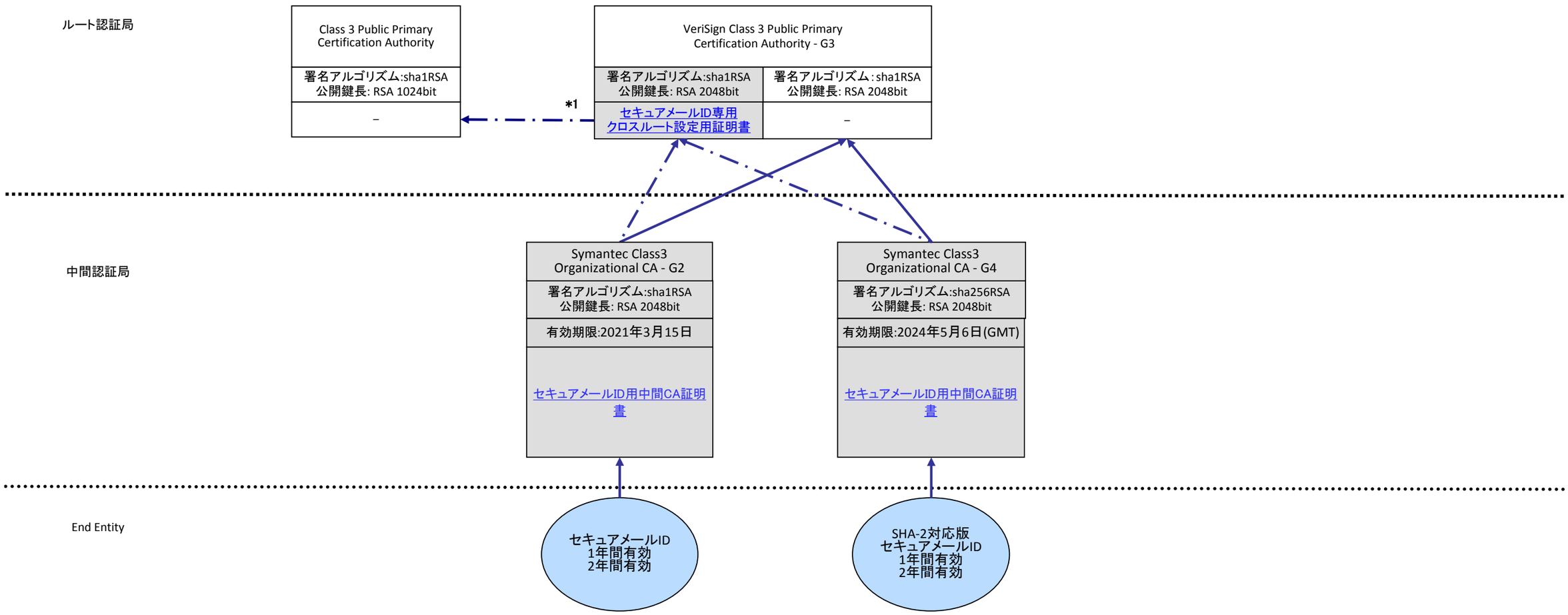


*1 : コードサイニング証明書は、VeriSign Class3 Public Primary Certification Authority - G5 (通称:Class3PCA G5)に3階層でチェーンします。Class3PCA - G5ルート認証局証明書が搭載されていないレガシープラットフォームとの後方互換性を確保する目的でのみ、Class3 Public Primary Certification Authority (通称 Class3PCA G1)に4階層でチェーンさせることを当面の間許容します。(クロスルート方式と呼ばれます)

作成者 : 合同会社シマンテック・ウェブサイトセキュリティ
作成日 : 2016年2月16日

シマンテック セキュアメールIDの階層構造

（2014年12月1日時点）



■凡例

証明書の種類	証明書の仕様	証明書の関係
– ルート認証局証明書	認証局の名称	= 署名検証のパス（End-Entityから上位の認証局へ向かってチェーンを辿る）
– 中間認証局証明書（クロスルート証明書含む）	鍵長および署名アルゴリズム	
– エンドエンティティ証明書	有効期限(GMT)	= クロスルート方式の場合の署名検証のパス
	中間認証局証明書（リポジトリへのリンク）	

*1 : シマンテックのセキュアメールIDは、通常VeriSign Class3 Public Primary Certification Authority - G3 (通称:Class3PCA G3)に3階層でチェーンしますが、Class3PCA - G3ルート認証局証明書が搭載されていないレガシープラットフォームとの通信をカバーするために、Class3 Public Primary Certification Authority (通称 Class3PCA G1)に4階層でチェーンします。(クロスルート方式と呼ばれます)

作成者 : 合同会社シマンテック・ウェブサイトセキュリティ
作成日 : 2016年2月16日