# シマンテック　トラスト　ネットワーク（STN)
# 認証業務運用規程
# (Certification Practice Statement)

## バージョン 3.8.27

## 2016 年 12 月 19 日

本ドキュメントは Symantec Corporation が発行する Symantec Trust Network(STN) Certification Practice Statement を株式会社シマンテックで翻訳を行ったものです。
原本と本ドキュメントで内容に差異がある場合、原本が優先されます。

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043 USA
+1 650.527.8000
*www.symantec.com*

**シマンテック トラスト ネットワーク (STN)**
**認証業務運用規程 (Certification Practice Statement)**



発行日:2016 年 1 月 14 日

**重要 – 買収に関するお知らせ**

2010 年 8 月 9 日をもって、Symantec Corporation (以下、「シマンテック」) による VeriSign Inc (以下、「ベリサイン」) の認証事業の買収が完了しました。これに伴い、シマンテックが本認証業務運用規程文書および本書に記載されている PKI Service の登録所有者となりました。

ただし、運用上実際に認証機関およびサービスのブランド名の変更が完了するまで、本書においては「ベリサイン」と「シマンテック」の記載が並存するものとします。会社名として「ベリサイン」と記載されているものはすべて、厳密には過去の所有者を示す言葉が残されているだけとお考えください。

**商標に関する注意**

**目次**

# 1. はじめに

本書は、シマンテック トラスト ネットワーク (STN) 認証業務運用規程 (Certification Practice Statement、以下「CPS」) です。本 CPS は、シマンテック認証機関 (Certification Authority、以下「CA」) がシマンテック トラスト ネットワークに関する証明書ポリシー (Certificate Policy、以下「CP」) の特定の要件に従い、証明書の発行、管理、失効、および更新を含む (ただし、これらに限定されない) 認証サービスを提供する際に採用する手続きについて記載したものです。

CP は、STN を統制するポリシーの最上位文書です。STN 内で電子証明書の承認、発行、管理、使用、失効、および更新し、信頼される関連サービスを提供するためのビジネス、法的、および技術的な要件を確立します。「STN スタンダード」と呼ばれるこれらの要件は、STN のセキュリティと完全性を保護し、STN 参加者すべてに適用され、結果として、STN 全体にわたって統一された信頼を保証します。STN と STN スタンダードに関する詳細な情報は、CP に記載されています。

シマンテックは、STN のシマンテック「サブドメイン」と呼ばれる STN の一部について権限を有します。シマンテック サブドメインは、カスタマ、利用者、依拠当事者などのシマンテックの下位に位置するエンティティを含みます。

CP は STN 参加者が満たさなければならない要件を規定しますが、本 CPS は、STN の シマンテック サブドメイン内でシマンテックがどのように当該要件を満たすかを説明するものです。具体的には、本 CPS では、以下の業務についてシマンテックが採用する手続きについて説明します。

- STN をサポートするコア インフラストラクチャの安全な管理
- STN 証明書の発行、管理、失効、および更新

いずれも、STN のシマンテック サブドメイン内において、CP とその STN スタンダードの要件に従って行うものとします。

本 CPS は、CP および CPS の構成について Internet Engineering Task Force (IETF) RFC 3647 に従います。STN 層に属する CA は、CA/ブラウザ フォーラム (CABF) の最新の要件に準拠します。CA/ブラウザ フォーラムの要件には、以下のものがあります。

- EV (Extended Validation) 証明書の発行と管理に関するガイドライン
- EV (Extended Validation) コードサイニング証明書の発行と管理に関するガイドライン
- 公的に信頼された証明書 (パブリック証明書) の発行と管理に関する基本要件

これらは、www.cabforum.org で公開されています。本文書とこれら要件の間に何らかの不一致が生ずる場合は、これら要件が本文書よりも優先されます。

現時点では、本 CP に従ってシマンテック CA から発行されるシマンテックの EV (Extended Validation) SSL 証明書、EV (Extended Validation) コードサイニング証明書、およびドメイン認証 (DV)/組織認証 (OV) SSL 証明書[1]は、CA/ブラウザ フォーラムの要件に準拠します。かかる DV/OV 証明書は、CP のセクション 1.2 に規定される対応ポリシー識別子を含めて発行され、これらの要件に対応し適合していることを示します。シマンテック CA は、これらポリシー識別子を含めて発行される証明書はすべて、CA/ブラウザ フォーラムの要件に適合して発行および管理されていることを表明します。

[1] さらにシマンテックは CA/ブラウザ フォーラム基本要件の対象外である組織向け (SSL 用途でない) クライアント証明書を発行します。また、CA/ブラウザ フォーラムのみに関連する手続き (OV SSL 証明書用) に加え、本 CPS では組織向けに発行され、その組織の情報を含む Class 2 または Class 3 証明書についての手続きも説明します。本 CPS では、かかる証明書を「組織向け証明書」と呼びます。

シマンテック トラスト ネットワークは、シマンテックの中の専門の事業部門が管理し、会社が提供する他のセキュリティ製品の責任を持つ事業部門から独立して運用します。STN はネットワークの一部であるルートから SSL 監査目的の中間 CA を発行することはありません。アプリケーション ソフトウェア提供者の製品(プライベート ルート)の中の現在または過去に信頼されたことがないルートは SSL 監視に使用する中間 CA を作成するために使われることがあります。

2017 年 2 月 1 日以降、STN は、https://aka.ms/csbr に掲載されている現行バージョンの the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates を適用します。本ドキュメントと当該要件に差異がある場合、当該要件が優先されます。
2017 年 2 月 1 日以降に発行されたコードサイニング証明書で、マイクロソフト オーセンティコードおよび付随する技術で使用する証明書には、ポリシー識別子に 2.23.140.1.4.1 を含み the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates に適合していることを示します。

**相互認証**
STN の Non-Federal Shared Service Provider (SSP) シマンテック サブドメインは、米連邦ブリッジ CA と相互認証され、連邦ブリッジ認証局 (FBCA) 向けの X.509 証明書ポリシーおよびシマンテックの Non-Federal Shared Service Provider (SSP) 認証業務運用規程の要件に従って運用されます。

### *1.1 概要*

本 CPS は特に以下の事項に適用されます。

- シマンテックのパブリック プライマリ認証機関 (PCA)
- シマンテック トラスト ネットワークをサポートする、シマンテック インフラストラクチャ CA およびシマンテック管理 CA[2]
- STN のシマンテック サブドメイン内で証明書を発行する、シマンテックのパブリック CA およびエンタープライズ カスタマの CA。

注記:以下の日付をもって、以下のルート証明書を本文書の適用範囲から除外します。

- 2015 年 12 月 1 日
  **VeriSign Class 3 Public Primary Certification Authority**
  Country = US
  Organization = VeriSign, Inc.
  Organizational Unit = Class 3 Public Primary Certification Authority
- 2015 年 3 月 27 日
  **VeriSign Class 3 Public Primary Certification Authority – G2**
  Country = US
  Organization = VeriSign, Inc.
  Organizational Unit = Class 3 Public Primary Certification Authority - G2
  Organizational Unit = (c) 1998 VeriSign, Inc. - For authorized use only
  Organizational Unit = VeriSign Trust Network

PCA または Class 3 PCA への参照は、これらのルート証明書には適用されません。これらのルート証明書は私的な目的だけに利用されることだけを意図しており、ブラウザの信頼されるルートリストから除外されるべきです。シマンテック トラスト ネットワーク CPS および CP はこのルート証明書の使用ならびに、いかなる付随サービスについて規定しません。

より一般的には、本 CPS は、株式会社シマンテックによって管理される STN CA を含むシマンテックのサブドメイン内におけるすべての個人およびエンティティ (以下総称して「シマンテック サブドメイン参加

[2] シマンテックは、本 CPS の範囲内で、パブリックおよびプライベート/内部的 Class 3 階層の両方を運用します。Class 3 内部 CA 階層は、プライベート PCA、および CP のセクション 1.2 で規定されている指定 OID 値で識別されます。プライベート PCA 証明書は、証明書の使用目的から「サーバー認証」と「コードサイニング」が明示的に除外されるよう構成されます。

者」) による STN のシマンテック サブドメイン内の STN サービスの利用についても規定します。また、本 CPS に特に記載がない場合、シマンテックが管理するプライベート CA および階層は、本 CPS の適用範囲外です[3]。関連会社が管理する CA も、本 CPS の対象外です。

STN には、Class 1～4 の 4 クラスの証明書があります。CP は、これらの証明書ポリシー (クラスごとに 1 つのポリシーがある) を定義し、クラスごとの STN スタンダードを定める文書です。

シマンテックは現在、STN のシマンテック サブドメイン内で 3 クラスの証明書を提供しています。本 CPS は、シマンテックがそのサブドメイン内でどのように各クラスの CP の要件に対応するかを説明します。従って、本 CPS は、3 つの証明書クラスすべてについて、発行および管理に関する業務と手続きを記載している文書です。

シマンテックは、政府の特定のポリシー要件、またはその他の業界の標準および要件に対応するために、本 CPS を補足する認証業務運用規程を公開できます。

上記の補足証明書ポリシーは、当該補足ポリシーに基づき発行された証明書の利用者およびこれらの依拠当事者が利用できるものとします。

本 CPS は、STN のシマンテック サブドメインに関係する一連の文書の 1 つに過ぎません。本 CPS 以外の文書には、以下のものがあります。

- 詳細な要件を規定することで CP および本 CPS を補足するセキュリティおよび運用に関する付属の機密文書。以下のものが該当します。[4]
  - *『Symantec Physical Security Policy』*: STN インフラストラクチャを統制するセキュリティの原則を規定しています。
  - *『Symantec Security and Audit Requirements (SAR) Guide』*: 人的、物理的、電気通信、論理的、および暗号鍵管理のセキュリティに関する、シマンテックおよび関連会社に適用される詳細な要件を記載しています。
  - *『Key Ceremony Reference Guide』*: 鍵管理についての詳細な運用要件を記載しています。

- シマンテックが制定する付属契約。これらの契約は、シマンテックのカスタマ、利用者、および依拠当事者を拘束します。特に、当該契約は STN スタンダードをこれらの STN 参加者に伝えるものであり、場合によっては、STN スタンダードへの対応方法について具体的な手続きを規定します。

多くの場合、本 CPS では、STN のシマンテック サブドメインのセキュリティを危殆化する可能性がある場合 (本 CPS で記載する事項を含む) に、STN スタンダードを実施するための具体的かつ詳細な手続きについて上記の付属文書を参照します。

### *1.2 文書名と識別*

本書は、シマンテック トラスト ネットワーク (STN) 認証業務運用規程 (CPS) です。STN 証明書は、STN CP の セクション 1.2 に規定されている、適用される STN 証明書クラスに対応するオブジェクト識別子の値を含みます。従って、シマンテックは、本 CPS でオブジェクト識別子の値を割り当てません。証明書ポリシーのオブジェクト識別子は、セクション 7.1.6 に従って使用されます。

---

3 Authenticated Content Signing (ACS) 証明書は、STN 以外の CA によって発行されます。ただし、ACS 利用者が ACS 証明書で使用される所定の手続きの違いを理解できるように、本 CPS の一部のセクションで ACS 証明書について言及しています。

4 これらの文書は公開されていませんが、文書の仕様はシマンテックの年 1 回の WebTrust for CA 監査に含まれており、特別な契約を締結しているカスタマに提供される可能性があります。

ドメイン認証と組織認証の SSL 証明書は、STN CP のセクション 1.2 に規定されている、対応する OID の値を含みます。これは CA/ブラウザ フォーラムの基本要件に対応し準拠していることを示します。

## *1.3 PKI 参加者*

### 1.3.1 認証機関

認証機関 (CA) という用語は、STN 内で公開鍵証明書を発行する権限が付与されているすべてのエンティティに適用される包括的な用語です。CA は、プライマリ認証機関 (PCA) と呼ばれる発行元のサブカテゴリを包含します。PCA は、4 つのドメインのルートの役割を果たし[5]、証明書の各クラスに 1 つの PCA が存在します。各 PCA は、シマンテックのエンティティです。PCA の下位の CA は、エンドユーザー利用者や他の CA に証明書を発行します。

シマンテックは、シマンテックの内部的な管理に限定して使用される「Symantec Class 3 Internal Administrator CA」階層も運用しています。

また、シマンテックは「Symantec Universal Root Certification Authority」および「Symantec ECC Universal Root Certification Authority」も運用しています。Universal Root CA は、Class 3 および特定の Class 2 の下位 CA 証明書を発行します。

シマンテックのエンタープライズ カスタマは、パブリック STN PCA の下位に属する CA として、独自の CA を運用できます。かかるカスタマは、STN CP および STN CPS のすべての要件を遵守するための契約関係をシマンテックと結びます。ただし、これらの下位 CA はそれぞれの内部要件に基づき、限定的な運用を行うことができます。

### 1.3.2 登録機関

登録機関は、STN CA の代わりに、エンドユーザー証明書の申請者の識別と認証を行い、エンドユーザー証明書の失効要求の開始または転送を行い、証明書の更新またはリキーの申請を承認します。シマンテックは、自らが発行する証明書の RA になることができます。

シマンテックと契約関係を結ぶ第三者は、自らの RA となり、STN CA による証明書の発行を承認できます。第三者の RA は、STN CP、STN CPS、およびシマンテックと締結するエンタープライズ サービス契約の条項に定められているすべての要件を遵守する必要があります。ただし、RA はそれぞれの内部要件に基づき、限定的な運用を行うことができます。[6]

### 1.3.3 利用者

STN における利用者は、STN CA により発行される証明書のすべてのエンドユーザー (エンティティを含む) を含みます。利用者とは、証明書のエンドユーザー利用者として指定されたエンティティです。エンドユーザー利用者としては、個人、組織、またはインフラストラクチャを構成するもの (ファイアウォール、ルーター、信頼性の高いサーバー、組織内で通信を保護するために使用されるその他のデバイスなど) が考えられます。

証明書は、自己使用のために個人またはエンティティへ直接発行される場合があります。ただし、通常の場合、証明書を要求する当事者と、認証情報の適用先 (サブジェクト) は異なります。たとえば、組織では、組織を代表して従業員が電子取引やビジネスを行うことができるように従業員の証明書を要求す

[5] Class 4 証明書は、現在 STN では発行されていません。
[6] 第三者の RA の例としては、Managed PKI Service カスタマが挙げられます。

ることがあります。このような場合、証明書発行を申し込むエンティティ (すなわち、特定のサービスの申し込みを通じて、または発行者として、証明書の支払いを行う者) は、証明書のサブジェクトであるエンティティ (通常は、認証情報の所持者) とは異なります。これら 2 つの役割を区別するために、本 CPS では「利用者」と「サブジェクト」という、異なる 2 つの用語を使用します。「利用者」は認証情報の提供を受けるためにシマンテックと契約を締結するエンティティであり、「サブジェクト」は認証情報が紐付けられている者です。利用者は認証情報の使用に関する最終的な責任を負いますが、サブジェクトは認証情報が提示されたときに認証される個人です。

「サブジェクト」が使用される場合、それは「利用者」と区別することを示しています。「利用者」が使用される場合、他とは別のエンティティとして単なる利用者を意味する場合もあれば、サブジェクトの意味を含む場合もあります。本 CPS ではその用語の使われ方により、正しく理解できるようになっています。

CA も、自己署名した証明書を発行する PCA として、または上位 CA によって証明書が発行される CA として、技術的には STN 内の証明書の利用者です。ただし、この CPS における「エンドエンティティ」および「利用者」への言及は、エンドユーザー利用者のみに当てはまります。

### 1.3.4 依拠当事者

依拠当事者は、STN で発行される証明書や電子署名に依拠して行動する個人またはエンティティです。依拠当事者は、STN 内において利用者である場合も、利用者でない場合もあります。

### 1.3.5 他の参加者

規定されません。

## *1.4 証明書の用途*

### 1.4.1 適切な証明書の用途

#### 1.4.1.1 個人に発行される証明書

個人向け証明書は、通常、電子メールの署名および暗号化、ならびに申請の認証 (クライアント認証) を行う個人により使用されます。個人向け証明書の最も一般的な用途は、以下の表 1 に記載されていますが、これら以外の目的に利用することもできます。ただし、依拠当事者がその証明書に合理的に依拠することができ、かつその用途が法律、STN CP、発行された証明書の根拠となる CPS、および利用者との契約によって禁止されていないものに限ります。

| 証明書クラス | 保証レベル | | | 用途 | | |
|---|---|---|---|---|---|---|
| | 保証レベル: 低 | 保証レベル: 中 | 保証レベル: 高 | 署名 | 暗号化 | クライアント認証 |
| Class 1 証明書 | ✓ | | | ✓ | ✓ | ✓ |
| Class 2 証明書 | | ✓ | | ✓ | ✓ | ✓ |
| Class 3 証明書 | | | ✓ | ✓ | ✓ | ✓ |

**表 1. 個人向け証明書の用途**

#### 1.4.1.2 組織に発行される証明書

組織向け証明書が組織に発行されるのは、組織が法的に存在すること、および証明書に含まれる組織の他の属性 (インターネットや電子メールのドメインの所有権など。ただし、検証されていない利用者情報を除く) が認証された後になります。本 CPS では、組織向け証明書の用途を制限することは意図していません。組織向け証明書の最も一般的な用途は、以下の表 2 に示されていますが、これら以外の目的に利用することもできます。ただし、依拠当事者がその証明書に合理的に依拠することができ、かつその用途が法律、STN CP、発行された証明書の根拠となる CPS、および利用者との契約によって禁止されていないものに限ります。

| | 保証レベル | | | | 用途 | | | |
|---|---|---|---|---|---|---|---|---|
| 証明書 クラス | 中 | 高 (EV) | 高 (CA/BF 組織認証) | 高 | コード/コンテンツの署名 | Secure SSL/TLS セッション | 認証 | 署名/暗号化 |
| Class 3 証明書 | | | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Class 3 EV SSL 証明書 | ✓ | ✓ | | ✓ | | ✓ | ✓ | ✓ |
| Class 3 EV コードサイニング証明書 | ✓ | ✓ | | ✓ | ✓ | | ✓ | ✓ |
| Class 3 組織認証 (OV) 証明書 | | | ✓ | ✓ | | ✓ | ✓ | ✓ |
| Class 3 ドメイン認証 (DV) 証明書 | ✓ | | | | | ✓ | ✓ (ドメインのみ) | ✓ |

**表 2. 組織向け証明書の用途**[7]

#### 1.4.1.3 保証レベル

**保証のレベルが低の証明書**は、認証目的または否認防止を裏付ける目的として利用してはならない証明書です。電子署名は、特定の電子メール アドレスを持つ送信者から電子メールが発信されたという低レベルの保証を提供します。一方で、証明書は利用者の識別情報を証明することはありません。暗号化を適用することで、依拠当事者は利用者の証明書を使用して利用者向けのメッセージを暗号化できるようになりますが、送信者の依拠当事者は、受信者が実際に証明書で指定された人物であることを確信することはできません。

**保証のレベルが中の証明書**は、Class 1 および 3 と比較して、利用者の識別情報を中程度で保証することを必要とする組織間、組織内、商業用、および個人用の電子メールを保護するのに適している証明書です。
シマンテック ベーシック ドメイン認証(DV)証明書は、暗号化を提供するためにドメインに対して発行された証明書です。シマンテックは、証明書を申請した人物がドメイン認証または申請者が FQDN に対して実質的な管理権を有することを示すことでドメインを管理していることを確認します。ドメインを所有する組織の認証は行いません。

**保証のレベルが高の証明書**は、Class 1 および 2 と比較して、利用者の識別情報について高い保証を提供する個人および組織向けの Class 3 証明書です。

[7]「限られた状況において、Class 2 証明書が Managed PKI カスタマから関連組織に発行されることがあります (組織内の個人には発行されません)。そのような証明書は、組織の認証および申請の署名に限って使用できます。本 CPS のセキュリティ基準に適合している認証および手続きの要件を定めたエンタープライズ サービス契約を通じてシマンテックより明示的に認められている場合を除き、利用者は、コードおよびコンテンツの署名、SSL 暗号化、および S/MIME 署名のためにこの証明書を使用することは禁止されており、そのような鍵の用途はこれら証明書では無効になります。」

**保証のレベルが高の証明書 (EV 証明書)** は、『Guidelines for Extended Validation Certificates』に従ってシマンテックが発行する Class 3 証明書です。

### 1.4.2 禁止される証明書の用途

証明書は、適用される法律、特に輸出入に関して適用される法律で認められる範囲でのみ利用されるものとします。

シマンテック証明書は、危険な環境における制御装置として利用または再販するため、あるいは、システム障害が死亡、身体障害、または深刻な環境被害を直接もたらすような核施設、航空・通信システム、航空管制、兵器管理システムの運用など、フェイル セーフ機能を必要とする用途のために設計されているものでも、意図されているものでも、また認められているものでもありません。また、Class 1 証明書は、識別情報の証明、または識別情報もしくは権限の否認防止を裏付けるものとして利用されないものとします。クライアント証明書は、クライアント アプリケーションでの使用を意図しており、サーバーまたは組織向け証明書として使用されないものとします。

CA 証明書は、CA の役割以外の目的で利用することはできません。さらに、エンドユーザー利用者証明書は、CA 証明書として利用されないものとします。

STN とその参加者は、証明書保持者が合理的に所有または管理しないドメイン名または IP アドレスに対して中間者またはトラフィック管理のために使うことができるいかなる証明書も発行しません。

シマンテックは、定期的に中間 CA のリキーを行います。中間 CA 証明書をルート証明書として組み込んでいるサード パーティ製のアプリケーションまたはプラットフォームは、中間 CA のリキーが行われた後では指定どおりに動作しない可能性があります。従って、シマンテックは、中間 CA 証明書をルート証明書として利用することを保証しておらず、これをアプリケーションやプラットフォームのルート証明書として組み込まないことを推奨します。ルート証明書として、シマンテックでは PCA ルート証明書を利用することを推奨します。

## *1.5 ポリシーの管理*

### 1.5.1 文書の管理組織

Symantec Corporation
350 Ellis Street
Mountain View CA 94043
USA

### 1.5.2 連絡先

PKI Policy Manager,
Symantec Trust Network Policy Management Authority
c/o Symantec Corporation
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527-8000 (voice)
+1 (650) 527-8050 (fax)
*practices@symantec.com*

CA/ブラウザ フォーラム (CABF)の連絡先は以下にあります。
https://cabforum.org/leadership/

### 1.5.3 CP へのポリシーの適合性の決定者

STN Policy Management Authority (PMA) は、本 CPS の適合性および適用性を決定します。

### 1.5.4 CPS の承認手続き

本 CPS および以後の改定の承認は、PMA により行われるものとします。改定は、CPS の改定部分を含めた文書の形式か、更新通知のいずれかの方法で行われるものとします。改定版または更新通知は、シマンテック リポジトリの [Practices Updates and Notices] セクション (*www.symantec.com/about/profile/policies/repository.jsp*) に掲載されるものとします。更新事項は、参照バージョンの CPS の指定された条項または矛盾する条項に優先します。PMA は、CPS に変更を加えることで、証明書の各クラスに対応している証明書ポリシーのオブジェクト識別子にも変更が必要かどうかを判断するものとします。

## *1.6 定義と頭字語*

頭字語と定義の一覧については、付録 A を参照してください。

# 2. 公開およびリポジトリに関する責任

## *2.1 リポジトリ*

シマンテックは、自身の CA およびエンタープライズ カスタマ (Managed PKI カスタマ) の CA のために、リポジトリの役割を果たす責任があります。シマンテックは CPS セクション 2.2 に従って、エンドユーザー利用者に発行した証明書をリポジトリで公開します。

エンドユーザー利用者の証明書が失効した場合、シマンテックはその失効通知をリポジトリで公開します。シマンテックは、本 CPS の規定に従い、自身の CA の CRL、およびシマンテック サブドメイン内のサービス センターならびにエンタープライズ カスタマの CA の CRL を発行します。これに加え、Online Certificate Status Protocol (以下「OCSP」) サービスの契約を締結しているエンタープライズ カスタマ向けに、シマンテックは本 CPS の規定に従って OCSP サービスを提供します。

## *2.2 証明書情報の公開*

シマンテックは、依拠当事者が失効およびその他の証明書ステータス情報をオンラインで照会することを可能にする Web ベースのリポジトリを保持します。シマンテックは、依拠当事者に対し、証明書のステータスを確認するための適切なリポジトリの探し方、および OCSP (Online Certificate Status Protocol) が利用可能な場合に適切な OCSP レスポンダの探し方について情報を提供します。

シマンテックは、自身の CA、およびそれらのサブドメイン内のクライアント サービス センターの CA の代わりに発行する証明書を公開します。エンドユーザー利用者の証明書が失効した場合、シマンテックはその失効通知をリポジトリで公開するものとします。さらに、シマンテックは証明書失効リスト (CRL) を発行し、利用可能な場合には、自身の CA およびそのサブドメイン内のサービス センターの CA のために OCSP (Online Certificate Status Protocol) サービスを提供します。

シマンテックは、常に以下の文書の最新バージョンを公開します。

- STN CP
- 本 STN CPS
- 利用規約
- 依拠当事者規約

シマンテックは、以下に関して、リポジトリの役割を果たす責任を負います。

- シマンテックのパブリック プライマリ認証機関 (PCA)、および STN をサポートするシマンテック インフラストラクチャ/管理 CA
- シマンテックの CA、および STN のシマンテック サブドメイン内で証明書を発行するエンタープライズ カスタマの CA

シマンテックは、特定の CA 情報をシマンテックの Web サイトのリポジトリ セクション (*www.symantec.com/about/profile/policies/repository.jsp*) で公開します。詳細は以下のとおりです。

シマンテックは、STN CP、本 CPS、利用規約、および依拠当事者規約をシマンテックの Web サイトのリポジトリ セクションで公開します。

シマンテックは、以下の表 3 に従って証明書を公開します。

| ***証明書タイプ*** | ***公開の要件*** |
|---|---|
| STN PCA および STN 発行のルート CA 証明書 | 最新のブラウザ ソフトウェアに含めることで、および以下のクエリー機能を通じてエンドユーザー利用者証明書で取得可能な証明書チェーンの一部として、依拠当事者が利用可能になります。 |
| STN 発行の CA 証明書 | 以下のクエリー機能を通じてエンドユーザー利用者証明書で取得可能な証明書チェーンの一部として、依拠当事者が利用可能になります。 |
| Managed PKI ライト証明書および Managed PKI カスタマの CA 証明書をサポートする STN CA の証明書 | LDAP ディレクトリ サーバー (*directory.verisign.com*) のクエリーを通じて利用可能になります。 |
| シマンテック OCSP レスポンダ証明書 | LDAP ディレクトリ サーバー (*directory.verisign.com*) のクエリーを通じて利用可能になります。 |
| エンドユーザー利用者証明書 (用途に応じて、特定の Class 3 証明書を除く) | シマンテック リポジトリ (https://pki-search.symauth.com/pki-search/index.html) のクエリー機能、および LDAP ディレクトリ サーバー (*directory.verisign.com*) のクエリーを通じて任意で公開され、依拠当事者が利用可能になります。ただし、Class 3 SSL およびコードサイニング証明書は除きます。 |
| Managed PKI カスタマを通じて発行されたエンドユーザー利用者証明書 | 上記のクエリー機能を通じて利用可能になります。ただし、Managed PKI カスタマの判断により、証明書にアクセスできるのは証明書のシリアル番号を使用して検索する場合に限定されます。 |
| 「Symantec Class 3 Organizational VIP Device CA」によって発行されたエンドユーザー利用者証明書 | パブリック クエリーを使用して利用できません |

**表 3 – 証明書の公開要件**

### *2.3 公開の時期または頻度*

本 CPS の改定は、セクション 9.12 に従って公開されます。利用規約および依拠当事者規約の改定は、必要に応じて公開されます。証明書は、発行と同時に公開されます。証明書ステータス情報は、本 CPS の規定に従い公開されます。

### *2.4 リポジトリへのアクセス制御*

シマンテックの Web サイトのリポジトリ部分で公開される情報は、公的にアクセス可能なものです。かかる情報への閲覧のみのアクセスは制限されません。シマンテックは、証明書、証明書ステータス情報、または CRL にアクセスする条件として、それらにアクセスする者に対し、依拠当事者規約または CRL 利用規約への同意を要求します。シマンテックは、リポジトリの記載事項について、権限のない者による追加、削除、または変更を防止するための論理的および物理的なセキュリティ対策を講じています。

シマンテックと関連会社はリポジトリを読み取り専用で公開します。また、セクション 1.5.4 に記載のリンクまたは関連会社の CPS で定義された場所となります。

# 3. 識別と認証

## *3.1 名称*

STN CP、本 CPS、または電子証明書の記載内容に別段の定めがある場合を除き、STN に基づいて発行された証明書に記載されている名称は認証されたものです。

### 3.1.1 名称のタイプ

*現在、STN はシマンテック所有となっていますが、以前発行された証明書は当時の所有者の名前で発行されています。該当する証明書の組織名 (O) 行に "VeriSign, Inc." 、部門名 (OU) に "VeriSign Trust Network" が記載されていますが、それぞれ「Symantec Corporation」および「Symantec Trust Network」を意味するものとします。該当する証明書の組織名 (O) 行に "VeriSign Japan K.K." が記載されていますが、「Symantec Japan, Inc.」を意味するものとします。該当する証明書の組織名 (O) 行に "VeriSign Australia." が記載されていますが、「Symantec Corporation」を意味するものとします。*

STN CA 証明書は、発行者 (Issuer) およびサブジェクト (Subject) フィールドに X.501 識別名 (DN) を含みます。STN CA 識別名は、以下の表 4 に定めるもので構成されます。

| *属性* | *値* |
|---|---|
| 国名:<br>Country (C) = | 2 文字の ISO 国コード。または使用されません。 |
| 組織名:<br>Organization (O) = | "Symantec Corporation" または <組織名>[8] |
| 部門名:<br>Organizational Unit (OU) = | シマンテック CA 証明書には、複数の OU 属性を含めることができます。さらに、この属性には、以下の項目を 1 つまたは複数含めることができます。<br>• CA 名<br>• Symantec Trust Network<br>• 証明書の使用条件を規定する依拠当事者規約を参照する旨の記載<br>• 著作権に関する通知<br>• 証明書のタイプを説明する記載 |
| 州または都道府県名:<br>State or Province (S) = | 使用されません。 |
| 市区町村名:<br>Locality (L) = | 使用されません。ただし、「Symantec Commercial Software Publishers CA」では、"Internet" を使用します。 |
| コモンネーム:<br>Common Name (CN) = | (CA 名が OU 属性で特定されていない場合) この属性は CA 名を含みます。または使用されません。 |

**表 4 – CA 証明書に含まれる識別名の属性**

エンドユーザー利用者証明書は、SubjectName フィールドに X.501 DN を含み、表 5 で示されている要素で構成されます。

| *属性* | *値* |
|---|---|
| 国名:<br>Country (C) = | 2 文字の ISO 国コード。または使用されません。 |
| 組織名:<br>Organization (O) = | 組織属性は、次のように使用されます。<br>• "Symantec Corporation" (OCSP レスポンダの場合、およびオプションで組織と関連のない個人向け証明書の場合)[9] |

[8] カスタマ組織専用の CA の場合、「O=」の記載事項は正式な組織名になるものとします。

| *属性* | *値* |
|---|---|
| | • 利用者の組織名 (Web サーバー証明書の場合、および組織と関連のある個人向け証明書の場合)<br>• ベーシック ドメイン認証(DV)証明書では使用しません |
| 部門名:<br>Organizational Unit (OU) = | シマンテック エンドユーザー利用者証明書には、複数の OU 属性を含めることができます。さらに、この属性には、以下の項目を 1 つまたは複数含めることができます。<br>• 利用者の部門名 (組織向け証明書の場合、および組織と関連のある個人向け証明書の場合)<br>• Symantec Trust Network<br>• 証明書の使用条件を規定する依拠当事者規約を参照する旨の記載<br>• 著作権に関する通知<br>• “Authenticated by Symantec[10]” および “Member, Symantec Trust Network” (シマンテックにより申請が認証された証明書の場合)<br>• “Domain Validated” (適用される場合)<br>• 証明書のタイプを説明する記載 [11]<br>• “No organization affiliation” (個人に発行されるコードサイニング証明書の場合) |
| 州または都道府県名:<br>State or Province (S) = | 利用者の州または都道府県名を示します (個人に発行される証明書の場合、州または都道府県名(S) フィールドは必須ではありません)。 |
| 市区町村:<br>Locality (L) = | 利用者の市区町村を示します (個人に発行される証明書の場合、市区町村 (L) は必須フィールドではありません)。 |
| コモンネーム:<br>Common Name (CN) = | この属性は、次のものを含みます。<br>• OCSP レスポンダ名 (OCSP レスポンダ証明書の場合)<br>• ドメイン名 またはパブリック IP アドレス(Web サーバー証明書の場合)<br>• 組織名 (コード/オブジェクト サイニング証明書の場合)<br>• 個人の名前 (個人向け証明書、または個人に発行されるコードサイニング証明書の場合)<br>• “Persona Not Validated” (Class 1 個人向け証明書の場合) [12]<br>• Class1 個人向け証明書は本属性を含めない可能性がある |
| 電子メール アドレス:<br>E-Mail Address (E) = | 電子メール アドレスは、Class 1 個人向け証明書と MPKI 加入者証明書に含まれる可能性があります。<br>Class3 組織向け電子メール署名証明書のための電子メールアドレス |

**表 5 – エンドユーザー利用者証明書に含まれる識別名の属性**

エンドユーザー利用者証明書のサブジェクト識別名のコモンネーム (CN=) 要素は、Class 2 および 3 証明書の場合に認証されます。 Class 1 証明書のコモンネームは、含まれないか、過去に、“Persona Not Validated”が含まれていたことがあります。

- 組織向け証明書のサブジェクト DN に含まれる認証されたコモンネームの値は、ドメイン名、または組織もしくは組織内の部署の正式な名称です。
- ただし、Class 3 組織向け ASB 証明書のサブジェクト DN に含まれる認証済みコモンネームの値は、組織の秘密鍵を使用する権限が付与された組織の代表者の一般に認められている個人名であり、Organization (O=) 要素が組織の正式名となります。

---

[9] シマンテックの場合、Class 2 証明書の承認された特定の場合において、内部用途のための内部情報を含む接尾語が O の値に追加されることがあります。シマンテックは、“Symantec Corporation – “ <接尾語> (例: Symantec Corporation – Build 5315) という形式で記載された組織名について、正式なエンティティとしてシマンテックを正確に表すことを証明します。

[10] RA サービスを実行する契約を締結している関連会社またはカスタマは、利用者認証を行う組織名を示すものとします。

[11] 承認された特定の状況において、内部用途のための Class 2 証明書が発行される場合があります。かかる証明書では、DN および OU の値にシマンテックの組織名が含まれますが、意図された内部用途以外で証明書を使用する場合に特有の信頼性に欠ける値になるものとします。

[12] 2014/7/11 までにシマンテックによって承認された"Class1 Managed PKI"顧客は、OU に” Persona Not Validated”の記載がある限り、CN に仮名を記載することができます。

- 個人向け証明書のサブジェクト DN に含まれるコモンネームの値は、当該個人の一般に認められている個人名です。
- 全てのWebサーバー証明書において、subjectAltNameエクステンションには、サブジェクトDNのコモンネームの認証された値を含みます。(ドメイン名またはパブリック IP アドレス) subjectAltName エクステンションには、コモンネームと同等の認証を行った追加のドメイン名やパブリック IP アドレスを含むことがあります。

EV SSL 証明書の項目とプロファイル要件については、本 CPS の付録 B3 のセクション 6 に記載されています。

ベーシック ドメイン認証(DV)証明書は、SubjectName フィールドに X.501 DN を含み、表 5A で示されている要素で構成されます。

| *属性* | *値* |
|---|---|
| 国名:<br>Country (C) = | 使用されません。 |
| 州または都道府県名:<br>State or Province (P) = | 使用されません。 |
| 市区町村名:<br>Locality (L) = | 使用されません。 |
| 組織名:<br>Organization (O) = | 使用されません。 |
| 部門名:<br>Organizational Unit (OU) = | ベーシック ドメイン認証(DV)証明書には、以下の OU 属性を含みます。<br>• Symantec Trust Network<br>• “Domain Validated” |
| コモンネーム:<br>Common Name (CN) = | 登録されたドメイン名 |
| 電子メール アドレス:<br>E-Mail(E)= | 使用されません。 |

**表 5A – ベーシック ドメイン認証(DV) エンドユーザー利用者証明書に含まれる識別名の属性**

#### 3.1.1.1 CA/ブラウザ フォーラムの名称の要件

EV SSL 証明書、EV コードサイニング証明書、およびドメイン認証/組織認証の SSL 証明書は、STNの追加手続きとして、付録 B1、付録 C、および付録 Dで規定されている CA/ブラウザ フォーラムの要件に準拠します。

### 3.1.2 意味のある名称にすることの必要性

Class 2 および 3 のエンドユーザー利用者証明書は、証明書のサブジェクトである個人または組織の識別を可能にする、一般に理解される意味のある名称を含みます。

STN CA 証明書は、証明書のサブジェクトである CA の識別を可能にする、一般に理解される意味のある名称を含みます。

### 3.1.3 利用者の匿名または仮名

Class 1 の個人利用者の識別情報は認証されません。Class 1 の利用者は仮名を使用できます。特定のエンドユーザー利用者の識別情報 (未成年者や機密事項を扱う政府関係者に関する情報など) を秘匿することが法律によって義務付けられている場合や州/政府機関によって要求されている場合を除き、Class 2 および 3 の利用者は仮名 (利用者の正式な個人名または組織名以外の名前) を使用することは許可されません。証明書での匿名使用の申請があると、その必要性について PMA が審査し、許可された場合には、識別情報の認証は行われているが秘匿されている旨が証明書に記載されます。

### 3.1.4 多様な名称形式を解釈するための規則

規定されません。

### 3.1.5 名称の一意性

シマンテックは、利用者の申請手続きにおいて自動化された機能により、利用者のサブジェクト識別名 (DN) が、特定の CA のドメイン内で一意であることを保証します。利用者は、サブジェクト DN が同一の証明書を複数所有できます。

### 3.1.6 商標の認識、認証、および役割

証明書申請者は、証明書申請において、他者の知的財産権を侵害するような名称を使用してはなりません。ただし、シマンテックは、証明書申請者が証明書申請に記載の名称の知的財産権を有しているかどうかを検証しません。また、ドメイン ネーム、商号、商標、サービス マークに関する紛争を仲裁、調停、その他の方法で解決することもしません。シマンテックは、証明書申請者に何ら責任を負うことなく、かかる紛争を理由としてあらゆる証明書申請を否認または保留する権利を有します。

## *3.2 初回の識別情報確認*

### 3.2.1 秘密鍵の所持を証明する方法

証明書申請者は、証明書に記載されている公開鍵に対応する秘密鍵を正当に所有していることを証明しなければなりません。秘密鍵の所持を証明する場合は、PKCS #10 を使用する方法、暗号化を使用する同等の別の方法、またはシマンテックが承認した別の方法を利用するものとします。この要件は、事前に生成された鍵がスマートカードに格納されている場合など、利用者の代わりに CA によって鍵ペアが生成される場合には適用されません。

### 3.2.2 組織の識別情報確認

証明書に組織名が含まれる場合は常に、組織の識別情報および証明書申請者から提供されたその他の申請情報 (確認されない利用者情報を除く) は、文書化されたシマンテックの検証手続きに従って確認されます。

シマンテックは少なくとも以下の確認を行うものとします。

- 最低 1 種類の第三者による識別情報証明サービスまたはデータベース、あるいは適切な政府機関/所管官庁によって発行されたか登録されている組織の存在を裏付ける文書を使用して、組織が存在していること。

- 証明書の申請者に対し、電話、郵便、またはこれらに相当する手段により、組織についての特定の情報、つまり組織が証明書の申請を承認していること、および証明書の申請者の代わりに証明書申請が提出されている場合は、その提出者に権限が与えられていること。

  承認された組織代表者として個人名が証明書に含まれている場合は、その個人が雇用されていること、および組織に代わって行動する権限が与えられていることも確認されるものとします。

ドメイン名または電子メール アドレスが証明書に含まれる場合、シマンテックは完全修飾ドメイン名または電子メール ドメインとしてドメイン名を使用する権限が組織にあることを認証します。組織認証(OV)とExtended Validation(EV)のドメインの認証は、全てにおいて組織の認証と一緒に完了させます。

米輸出規制および米商務省産業安全保障局 (BIS) 発行のライセンスを遵守するために必要な追加調査は、必要に応じてシマンテックおよび関連会社が行います。

特定のタイプの証明書については、表 6 で説明している追加手続きを実施します。

| *証明書タイプ* | *追加手続き* |
|---|---|
| **Extended Validation (EV) 証明書** | シマンテックにおける EV SSL 証明書の発行手続きは、本 CPS の付録 B1 に記載されています。<br>シマンテックにおける EV コードサイニング証明書の発行手続きは、本 CPS の付録 C に記載されています。 |
| **組織認証 (OV)/ドメイン認証 (DV) 証明書** | シマンテックによる OV/DV 証明書の発行手続きは、本 CPS の補足 D に記載している「OV/DV 証明書に関する CA/ブラウザ フォーラム要件」として区別して記載されています。 |
| **OFX サーバー ID** | シマンテックは、組織名が空白または金融機関であること、もしくは以下の SIC コードのいずれかで分類されていることを確認します。<br>• 60xx 預金受け入れ金融機関<br>• 61xx 預金を受け入れない金融機関 (信販機関)<br>• 62xx 証券および商品相場の仲介業者<br>• 63xx 保険業者<br>• 64xx 保険代理店、保険仲介業者、保険業務<br>• 67xx ホールディング オフィスおよびその他の投資事務所<br>• 7372 パッケージ済みソフトウェア<br>• 7373 コンピュータ統合システム設計<br>• 7374 データの処理および準備<br>• 3661 電話機および電信機<br>• 8721 会計、監査、経理 |
| **Hardware Protected SSL 証明書および Hardware Protected EV コードサイニング証明書** | シマンテックは、鍵ペアが FIPS 140 認定ハードウェアで生成されていることを確認します。 |
| **Managed PKI for Intranet SSL 証明書** | シマンテックは、デバイスに割り当てられたホスト名または IP アドレスがインターネット (一般公開サイト) からアクセスできないこと、そして証明書利用者によって所有されていることを確認します。*<br>*subjectAlternativeName エクステンションやサブジェクトのコモンネームに予約済み IP アドレスか内部的な名前を持つ証明書の利用は、CA/ブラウザ フォーラムによって禁止され、2016 年 10 月までに排除されます。施行日の後に発行されたそのような証明書は、2015 年 11 月 1 日より前に有効期限を迎えなければなりません。2016 年 10 月 1 日以降の有効期限を持つ発行済みの証明書は、2016 年 10 月 1 日で失効されます。 |
| **ACS (Authenticated Content Signing) 証明書** | シマンテックは、ACS を使用して何らかのコンテンツに電子署名を行う場合、事前にそのコンテンツは当該組織がそのコードサイニング証明書を使用して署名したオリジナルの内容そのものであることを認証します。 |
| **電子メール署名用組織向けクラス 3 証明書** | シマンテックは、電子メールのドメイン名の所有権が当該組織にあることを確認します。 |

**表 6 – 特別な認証手続き**

#### 3.2.2.1 組織の申請者に関する CA/ブラウザ フォーラムの審査の要件

EV SSL 証明書、EV コードサイニング証明書、およびドメイン認証/組織認証の SSL 証明書は、STN の追加手続きとして、付録 B1、付録 C、および付録 Dで規定されている CA/ブラウザ フォーラムの要件に準拠します。

#### 3.2.2.2 組織の申請者に関する Mozilla 社の審査の要件

証明書内の国際化ドメイン名 (IDN) の申請において、シマンテックは IDN の同形異義語攻撃に備え、ドメイン名所有者の検証を行います。シマンテックでは、複数の Whois サービスの検索を実行して特定ドメインの所有者を自動的に検出するプロセスを採用しています。検索が失敗した場合、手動による再検索が実行され、RA は手動でその証明書申請を否認することができます。さらに、RA は 1 つのホストネーム ラベル内で複数のスクリプトで作成されているように表示されるドメイン名はすべて否認します。

シマンテックは、CA/ブラウザ フォーラムに積極的に参加し、IDN 証明書のスタンダード確立に寄与します。また、フォーラム本体で承認されたスタンダードを遵守します。

#### 3.2.2.3 ドメインの認証

シマンテックは、ドメイン名の審査において以下の手法を用います。また、選択肢の1番目を最初に実施します。

1. Whois検索を実施し、申請者がドメインのレジストラにおいてドメインの登録者であるか確認する。

2. ドメインのレジストラによって提供される住所、電子メール アドレスまたは電話番号を使って直接ドメイン登録者へ連絡する。

3. ドメイン利用許可証に依拠する。

4. Whoisに登録されている登録者名、技術連絡担当者、登録担当者に記載されている連絡先情報を使って直接ドメイン登録者へ連絡する。

5. ”admin”、”administrator”、”webmaster”、”hostmaster”、または”postmaster”とアットマーク(”@”)と要求されたFQDNから0などその他を削除し成形されたドメインとによって生成された電子メール アドレスを使ってドメインの管理者へ連絡する。

6. FQDNを含むURIで識別可能なオンラインwebページ上の情報を合意した変更がされたことをを確認することでFQDNを申請者が実質的に管理していることを確認する。

### 3.2.3 個人の識別情報の認証

個人の識別情報の認証は、証明書の Class によって異なります。STN 証明書の各クラス別の最低限の認証基準について、表 7 で説明します。

| 証明書クラス | 識別情報の認証 |
|---|---|
| **Class 1** | 識別情報は認証されません。証明書利用者が当該電子メール アドレスにアクセスできるか限定的な確認を行います。シマンテックは以下の方法に則って実施します。申請者から登録申請を受け取ると、シマンテックはセキュリティの観点から2通の電子メールを申請者へ送ります。1通目の電子メールはセルフサービスのwebページにアクセスするためのURLを含み、もう1通の電子メールにはセルフサービスのwebページにアクセスし申請者の電子メール アドレスのためにランダムで生成されたパスワードが含まれます。証明書申請者はシマンテック セルフサービスwebページから要求した証明書を受け取るためにこのパスワードを使わなければなりません。申請者は提供した電子メール アドレスにシマンテックが送る電子メールを実際に受信し、提供されたパスワードを使って証明書を受領することで確認します。 |

| 証明書クラス | 識別情報の認証 |
|---|---|
| **Class 2** | 以下により、識別情報を認証します。<br>▪ エンタープライズ管理者顧客が証明書申請を手動で確認を実施する。申請者は申請時に提供するe-mailアドレスを通じて証明書を受け取る。ランダムに生成されたパスコードをエンタープライズ管理者が申請する権限を持つ申請者に別手段で提供し、申請者が当該パスコードを利用するパスコードを使った認証<br>▪ 申請者から提供された情報と業務記録またはデータベース(アクティブ ディレクトリやLDAPなどの顧客ディレクトリ)に含まれる情報の照合 |
| **Class 3** | Class 3 個人向け証明書の認証は、CA または RA の代理人、もしくは証明書申請者の所在地で公証人またはこれと同等の権限を有する当局者の面前に、証明書申請者本人が出頭することにより行います。代理人、公証人、またはその他の当局者が証明書申請者の識別情報を確認する際には、パスポートや運転免許証など広く認識された様式の政府発行の写真付き身分証明書と、これ以外の身元を識別する認証情報を照合するものとします。<br><br>Class 3 の管理者証明書の認証は、組織の認証、組織からの識別情報の確認、および管理者として行動する者の承認に基づきます。<br><br>シマンテックは、自身の管理者の証明書申請を承認する場合もあります。管理者は組織内の「信頼される人物」です。この場合、シマンテックの証明書申請の認証は、雇用関係(請負業者の場合は定着率) および経歴調査手続きを関連させた識別情報の確認に基づくものとします。[13]<br><br>e-mail アドレス確認<br>Class 3 組織向け e-mail 証明書。シマンテックは申請者がドメインを所有していることを 3.2.2.3 の 1 から 3 番目の手段で確認する。申請者は確認されたドメインを含む任意のメールアドレスを証明書に入れることができる。 |
| **米国連邦政府を除くエンティティ向けの Shared Service Provider (SSP) 証明書** | 証明書利用者の識別情報は、実質上、連邦ブリッジ認証局 (FBCA) 向けの X.509 証明書ポリシーおよびシマンテックの Non-Federal Shared Service Provider (SSP) 認証業務運用規程の要件に従って検証されます。 |

**表 7. 個人の識別情報の認証**

### 3.2.4 確認されない利用者情報

確認されない利用者情報は、以下のとおりです。

- 一定の例外を除く部門名 (OU) [14]
- Class 1 証明書の利用者名
- 証明書において確認を行わないと明示されているその他の情報

### 3.2.5 権限の確認

証明書において、個人名が組織名と関連付けられており、個人の所属または組織に代わって行動する権限があることが示されている場合は常に、シマンテックまたは RA は、以下の確認を行います。

13シマンテックは、デバイスやサーバーなど、人間以外の受取人に関連付けられる管理者証明書を承認できます。人間以外の受取人向けの Class 3 管理者証明書の申請を認証する際には、以下が行われるものとします。

- 証明書申請において管理者として指定されたサービスの存在および識別情報の認証
- 管理機能を実行しているサービスと一貫した方法でサービスが安全に実装されていることの認証
- 証明書申請において管理者として指定されたサービスの管理者証明書を申請している者の識別情報と承認の確認

14 CA/ブラウザ フォーラムのガイドラインに準拠することが証明されたドメイン認証/組織認証証明書は、確認された部門名 (OU) の値を含むことがあります。

- 最低 1 種類の第三者による識別情報証明サービスまたはデータベース、あるいは適切な政府機関によって発行されたか登録されている組織の存在を裏付ける文書を使用して、組織が存在していること。
- 関連する個人向けの証明書を承認する RA の業務記録または業務情報データベース (従業員や顧客のリストなど) に含まれる情報を使用する。または、組織に対し、電話、郵便、またはこれらに相当する手段により、証明書申請を提出している個人が組織に雇用されていること、そして該当する場合は組織の代わりに行動する権限が与えられていること。

### 3.2.6 相互運用の基準

表明しません。

## *3.3 リキー要求時の識別と認証*

証明書を継続して使用するには、既存の利用者証明書の有効期間内に、利用者は新しい証明書を入手する必要があります。シマンテックは、通常、有効期間が満了する鍵ペアを取り替えるために、新しい鍵ペアを生成することを利用者に要求します (技術的に「リキー (reKey)」と定義されます)。ただし、特定の場合においては (Web サーバー証明書の場合など)、利用者は、既存の鍵ペア用に新しい証明書を要求できます (技術的に「更新 (renewal)」と定義されます)。

通常、「リキー」と「更新」はどちらも「証明書の更新」と表現されますが、これは、古い証明書を新しい証明書に置き換えるという事実に着目しており、新しい鍵ペアが生成されるかどうかについては重視していません。Class 3 サーバー証明書を除く STN 証明書のすべてのクラスとタイプでは、シマンテックのエンドユーザー利用者証明書の更新プロセスの一部として新しい鍵ペアが常に生成されるため、この区別は重要ではありません。ただし、Class 3 サーバー証明書の場合、利用者の鍵ペアは Web サーバー上で生成され、ほとんどの Web サーバーの鍵生成ツールにおいて既存の鍵ペアで新しい証明書要求を作成することが許可されているため、「リキー」と「更新」が区別されます。

### 3.3.1 定期的なリキーの識別と認証

リキーの手続きにおいては、エンドユーザー利用者証明書のリキーを要求する個人または組織が証明書の実際の利用者であるか確認されます。

実施可能な手続きとして、チャレンジ フレーズ (またはこれと同等なもの) を使用する方法や、秘密鍵の所持を証明する方法が挙げられます。利用者は申請情報とともに、チャレンジ フレーズを選択し、提示します。証明書の更新では、利用者が自身の再申請情報とともにチャレンジ フレーズ (またはこれと同等なもの) を正しく提示し、申請情報 (企業担当者および技術担当者の情報を含む) が変更されていなければ、更新された証明書が自動的に発行されます。チャレンジ フレーズ (またはこれと同等なもの) の代用として、シマンテックは更新される証明書について、確認された企業連絡先に関連付いている電子メール アドレスに電子メール メッセージを送信し、証明書の更新依頼の確認と、証明書発行の承認を要求できます。シマンテックは証明書発行の承認確認を受け取ったら、申請情報 (企業担当者および技術担当者の連絡先情報を含む[15]) が変更されていない場合に証明書を発行します。

この方法でリキーまたは更新が行われてから、それ以降のリキーまたは更新において別の状況であった場合、シマンテックまたは RA は、最初の証明書申請時の識別および認証の要件に従って利用者の識別情報の再確認を行います。[16]

---

[15] 承認された正式な連絡先変更手続きにより連絡先情報が変更されていれば、証明書の自動更新は有効なままとします。

[16] ただし、Class 3 組織向け ASB 証明書のリキー/更新要求の認証の場合は、最初の証明書申請時と同じ識別と認証に加え、チャレンジ フレーズの使用が要求されます。

特に、リテール Class 3 組織向け SSL 証明書の場合、シマンテックは、証明書に含まれる組織名およびドメイン名の再認証をセクション 6.3.2 に記載の間隔で行います。この場合、以下の確認が行われます。

- 以降の証明書更新時にチャレンジ フレーズが正しく使用されている、または確認の返信が企業担当者向けの電子メールで得られる
- 証明書の識別名が変更されていない
- 企業担当者および技術担当者の情報が前回確認したものから変更されていない

シマンテックは、証明書の申請者に対し、電話、郵便、またはこれらに相当する手段により、組織についての特定の情報、つまり組織が証明書の申請を承認していること、および証明書の申請者の代わりに証明書申請が提出されている場合は、その提出者に権限が与えられていることを再確認する必要はありません。

証明書の有効期間満了から 30 日を経た後のリキーについては、最初の証明書申請と同様に再認証が行われ、証明書は自動的に発行されません。

### 3.3.2 失効後のリキーの識別と認証

失効後のリキー/更新は、失効の理由が以下の場合は許可されません。

- 証明書 (Class 1 証明書を除く) が、その証明書のサブジェクトとして指定されている個人以外に発行された場合
- 証明書 (Class 1 証明書を除く) が、その証明書のサブジェクトとして指定されている個人またはエンティティの承認なく発行された場合
- 利用者の証明書申請を承認しているエンティティが、証明書申請における重大な事実が虚偽であることを発見した場合、またはそのように確信する理由がある場合
- STN を保全するためにシマンテックが必要と認める何らかの理由がある場合

上記の定めに従うことを条件として、組織向けまたは CA 証明書の失効後の更新については、更新手続きによって、更新を必要としている組織または CA が証明書の実際の利用者であると確認される場合にのみ許可されます。更新後の組織向け証明書は、更新前の組織向け証明書と同じサブジェクト DN を含むものとします。

個人向け証明書の失効後の更新については、更新を必要としている個人が実際の利用者であることを確認する必要があります。実施可能な手続きとして、チャレンジ フレーズ (またはこれと同等なもの) を使用する方法が挙げられます。この手続きまたはシマンテックが承認したその他の手続き以外に、最初の証明書申請における識別と認証の要件が、失効後の証明書の更新で使用されるものとします。

## *3.4 失効要求の識別と認証*

証明書を失効させる前に、シマンテックは失効要求を行ったのが証明書の利用者または証明書申請を承認したエンティティであることを確認します。

利用者の失効要求を認証する際に実施可能な手続きは、次のとおりです。

- 特定の証明書タイプの利用者に自身のチャレンジ フレーズ (またはこれと同等なもの) を提示してもらい、記録されているチャレンジ フレーズ (またはこれと同等なもの) と一致した場合には、自動的に証明書が失効する (注: このオプションは必ずしもすべてのカスタマが利用できるとは限りません)。
- 失効を要求していること、および失効の対象となる証明書を参照することで検証できる電子署名が含まれたメッセージを利用者から受信する。

- 失効を要求している個人または組織が実際の利用者であることを、証明書のクラスに合わせて保証する利用者に連絡する。かかる連絡には、状況に応じて、電話、ファクシミリ、電子メール、郵便、宅配便のいずれか 1 つ以上を含みます。

シマンテックの管理者は、シマンテック サブドメイン内のエンドユーザー利用者証明書の失効を要求できます。管理者による失効処理の実行を許可する前に、シマンテックは SSL およびクライアント認証を使用したアクセス制御を通じて、または STN で承認されたその他の手続きを使用して、管理者の識別情報を認証します。

自動承認ソフトウェア モジュールを使用する RA は、シマンテックに失効要求を一括して提出できます。かかる要求は、RA の自動承認ハードウェア トークンの秘密鍵で署名された電子署名入りの要求にすることで認証されるものとします。

CA 証明書の失効要求は、その失効が実際に当該 CA によって要求されていることをシマンテックが確認することによって、認証されるものとします。

# 4. 証明書ライフサイクルに関する運用要件

## *4.1 証明書申請*

### 4.1.1 証明書申請を提出できる者

証明書申請を提出できる者は、以下のとおりです。

- 証明書のサブジェクトに記載されている個人
- 組織またはエンティティの正式な代表者
- CA の正式な代表者
- RA の正式な代表者

### 4.1.2 申請手続きおよび責任

#### 4.1.2.1 エンドユーザー証明書の利用者

エンドユーザー証明書のすべての利用者は、セクション 9.6.3 に記載される説明と保証が含まれた関連のある利用規約に同意することを明らかにし、以下の項目からなる申請手続きを履行するものとします。

- 証明書申請の必要事項を記載し、正しい情報を提供する
- 鍵ペアを生成する、または生成されるよう手配する
- 自身の公開鍵を直接または RA 経由でシマンテックに提示する
- シマンテックに提示した公開鍵に対応する秘密鍵を所有していること、または排他的に制御していることを証明する

#### 4.1.2.2 CA/ブラウザ フォーラムの証明書申請の要件

EV SSL 証明書、EV コードサイニング証明書、およびドメイン認証/組織認証の SSL 証明書は、STN の追加手続きとして、付録 B1、付録 C、および付録 Dで規定されている CA/ブラウザ フォーラムの要件に準拠します。

#### 4.1.2.3 CA および RA の証明書

CA および RA 証明書の利用者は、シマンテックと契約を締結します。CA および RA 申請者は、契約の過程において、自身の識別情報を示す証明書と連絡先情報を提供するものとします。この契約過程において、または遅くとも CA または RA の鍵ペアを作成する鍵生成セレモニーよりも前に、申請者はシマンテックと協力して、適切な識別名および当該申請者によって発行される証明書の記載内容を決定するものとします。[17]

## *4.2 証明書申請の処理*

### 4.2.1 識別と認証機能の実行

シマンテックまたは RA は、セクション 3.2 の規定で要求されているすべての利用者情報について、識別と認証を実行するものとします。

### 4.2.2 証明書申請の承認または否認

シマンテックまたは RA は、以下の基準が満たされている場合、証明書の申請を承認します。

- セクション 3.2 の規定で要求されているすべての利用者情報について、識別および認証が問題なく完了した
- 支払いが完了している

シマンテックまたは RA は、以下の場合に証明書の申請を否認します。

- セクション 3.2 の規定で要求されているすべての利用者情報について、識別および認証を完了できない
- 利用者が、要求された関係書類を提供しない
- 利用者が、指定時間内に通知への返答をしない
- 支払いが完了していない
- RA が、利用者への証明書発行によって、STN の信用が失墜する可能性があると確信している

### 4.2.3 証明書申請の処理時間

シマンテックは、受領から妥当な時間内に証明書申請の処理を開始します。関連する利用規約、CPS、または STN 参加者間のその他の契約に別段の定めがない限り、申請処理を完了するまでの時間に関する規定はありません。証明書申請は、否認されるまで有効なままです。

### 4.2.4 証明書認証局権限(Certification Authority Authorization CAA)

2015 年 10 月 1 日時点において、シマンテックは、証明書認証局権限(Certificate Authority Authorization CAA)レコードをパブリック SSL 証明書の認証と確認プロセスの一環として記録します。その日より前は、シマンテックは全てのパブリック SSL 証明書の申請について CAA レコードを確認しない可能性があります。パブリック SSL 証明書とは、公開しているルート証明書につながり、CA/ブラウザ フォーラムの基本要件と EV 要件を満たすものを意味します。

[17] 例外として、利用者証明書がルートから直接発行される場合があります。この例外は、鍵ペアのサイズと長さが 2048 ビット以下の利用者証明書の場合にのみ適用されるものとします。

## *4.3 証明書の発行*

### 4.3.1 証明書の発行過程における CA の役割

証明書は、シマンテックによって証明書申請が承認された後、または RA からの証明書発行要求を受領した後に、作成され発行されます。シマンテックは、証明書申請者に対し、証明書申請に記載の情報に基づき、当該証明書申請を承認してから、証明書を作成し発行します。

### 4.3.2 利用者に対する CA による証明書発行通知

シマンテックは、直接または RA を介して、当該証明書を作成したことを利用者に通知し、その証明書が利用可能になった旨を通知することにより、利用者が証明書にアクセスできるようにするものとします。Web サイトから証明書をダウンロードするのを許可するか、証明書を含むメッセージを送信することで、エンドユーザー利用者が証明書を利用できるようになるものとします。

### 4.3.3 ルート CA による証明書発行に関する CA/ブラウザ フォーラム要件

EV SSL 証明書、EV コードサイニング証明書、およびドメイン認証/組織認証の SSL 証明書は、STN の追加手続きとして、付録 B1、付録 C、および付録 Dで規定されている CA/ブラウザ フォーラムの要件に準拠します。

## *4.4 証明書の受領*

### 4.4.1 証明書の受領となる行為

以下の行為により、証明書を受領したことになります。

- 証明書をダウンロードする、または電子メールに添付されたメッセージから証明書をインストールする
- 利用者が、証明書またはその中身に異議を唱えない

### 4.4.2 CA による証明書の公開

シマンテックは、一般にアクセス可能なリポジトリにおいて、発行した証明書を公開します。

### 4.4.3 他のエンティティへの CA による証明書発行通知

RA は、自身が承認した証明書発行に関する通知を受け取ることができます。

## *4.5 鍵ペアと証明書の使用*

### 4.5.1 利用者の秘密鍵および証明書の使用

証明書において公開鍵に対応する秘密鍵の使用は、利用者が利用規約に同意し、証明書を受領した場合にのみ許可されるものとします。その証明書は、シマンテックの利用規約、ならびに STN CP および本 CPS の規定に従って合法的に使用されるものとします。証明書の使用は、証明書に含まれる *KeyUsage* エクステンションと一致している必要があります (たとえば、Digital Signature が有効になっていない場合には、署名に使用してはいけません)。

利用者は、自身の秘密鍵が不正に使用されないよう保護するものとし、さらに証明書の有効期間が満了した場合または証明書が失効した場合は、秘密鍵の使用を中止するものとします。利用者以外の当事者は、セクション 4.12 に規定されている場合を除き、利用者の秘密鍵をアーカイブしないものとします。

### 4.5.2 依拠当事者の公開鍵および証明書の使用

依拠当事者は、証明書に依拠する条件として、適用される依拠当事者規約の条件に同意するものとします。

証明書の依拠は、この状況下において妥当なものでなければなりません。さらなる保証が必要な状況の場合、依拠当事者は、かかる依拠が妥当なものであるとみなされるような保証を取得しなければなりません。

依拠する行為の前に、依拠当事者は、独自に以下の項目を実施するものとします。

- 特定の何らかの目的のために証明書を使用することが適切であるか否かを評価し、証明書が本 CPS で禁止もしくは制限されていない適切な目的のために実際に使用されるか判断する。シマンテックは、証明書の使用が適切であるか否かの評価について責任を負いません。
- 証明書に含まれる *KeyUsage* エクステンションに従って、証明書が使用されているか否かを評価する (たとえば、Digital Signature が有効になっていない証明書は、利用者の署名の有効性を検証するために依拠することはできません)。
- 証明書のステータスおよび証明書を発行したチェーン内のすべての CA を評価する。依拠当事者は、証明書チェーン内の証明書が 1 つでも失効している場合、証明書チェーン内の証明書が失効される前にエンドユーザー利用者証明書によって実行された電子署名への依拠が妥当なものかどうかを調査する全責任を負います。かかる依拠はすべて、依拠当事者のみのリスクで行われます。

証明書の使用が適切であることを前提として、依拠当事者は、実施したい電子署名の検証や他の暗号処理のために、それら各処理に関連する証明書に依拠する条件として、適切なソフトウェアとハードウェアの両方またはいずれかを使用するものとします。かかる処理には、証明書チェーンの識別、および証明書チェーン内のすべての証明書での電子署名の検証が含まれます。

## *4.6 証明書の更新*

証明書の更新とは、公開鍵やその他の証明書情報を変更することなく、利用者に新しい証明書を発行することです。ほとんどの Web サーバー鍵生成ツールでは既存の鍵ペアで新しい証明書要求を作成できるため、証明書の更新は、鍵ペアが Web サーバーで生成される Class 3証明書でサポートされています。

### 4.6.1 証明書の更新が行われる場合

証明書を継続して使用するには、既存の利用者証明書の有効期間内に、利用者は新しい証明書を更新する必要があります。証明書は、有効期間満了後に更新することもできます。

### 4.6.2 更新を要求できる者

個人向け証明書の場合はその利用者のみ、組織向け証明書の場合は正式な代表者のみが証明書の更新を要求できます。

### 4.6.3 証明書の更新要求の処理

更新手続きにおいては、エンドユーザー利用者証明書の更新を要求する個人または組織が証明書の実際の利用者であること (または利用者から許可を得ていること) が確認されます。

実施可能な手続きとして、チャレンジ フレーズ (またはこれと同等なもの) を使用する方法や、秘密鍵の所持を証明する方法が挙げられます。利用者は申請情報とともに、チャレンジ フレーズ (またはこれと同等なもの) を選択し、提示します。証明書の更新では、利用者が自身の再申請情報とともにチャレン

ジ フレーズ (またはこれと同等なもの) を正しく提示し、申請情報 (企業情報および技術担当者情報を含む[18]) が変更されていなければ、更新された証明書が自動的に発行されます。チャレンジ フレーズ (またはこれと同等なもの) の代用として、シマンテックは更新される証明書について、確認された企業連絡先に関連付いている電子メール アドレスに電子メール メッセージを送信し、証明書の更新依頼の確認と、証明書発行の承認を要求できます。シマンテックは証明書発行の承認確認を受け取ったら、申請情報 (企業担当者および技術担当者の連絡先情報を含む[19]) が変更されていない場合に証明書を発行します。

上記の方法で更新が行われた後、再度更新する場合に別の状況であった場合、シマンテックまたは RA は、本 CPS で最初の証明書申請の認証として規定されている要件に従って、利用者の識別情報を再確認するものとします。

特に、リテール Class 3 組織向け SSL 証明書の場合、シマンテックは、証明書に含まれる組織名およびドメイン名の再認証をセクション 6.3.2 に記載の間隔で行います。

この場合、以下の確認が行われます。

- 以降の証明書更新時にチャレンジ フレーズが正しく使用されている、または確認の返信が企業担当者向けの電子メールで得られる
- 証明書の識別名が変更されていない
- 企業担当者および技術担当者の情報が前回確認したものから変更されていない

シマンテックは、証明書の申請者に対し、電話、郵便、またはこれらに相当する手段により、組織についての特定の情報、つまり組織が証明書の申請を承認していること、および証明書の申請者の代わりに証明書申請が提出されている場合は、その提出者に権限が与えられていることを再確認する必要はありません。

上記の手続きまたはシマンテックが承認したその他の手続きの他に、最初の証明書申請における認証の要件がエンドユーザー利用者証明書の更新に使用されるものとします。

### 4.6.4 利用者への新しい証明書の発行通知

更新された証明書の利用者への発行通知は、セクション 4.3.2 に従って行われます。

### 4.6.5 更新された証明書の受領確認となる行為

更新された証明書を受領したこととされる行為は、セクション 4.4.1 に従います。

### 4.6.6 更新された証明書の CA による公開

更新された証明書は、一般にアクセス可能なシマンテックのリポジトリで公開されます。

### 4.6.7 他のエンティティへの CA による証明書発行通知

RA は、自身が承認した証明書発行に関する通知を受け取ることができます。

## *4.7 証明書のリキー*

証明書のリキーとは、新しい公開鍵を認定する新しい証明書の発行を申請することです。証明書のリキーは、証明書のすべてのクラスでサポートされます。

---

[18] 承認された正式な連絡先変更手続きにより連絡先情報が変更されていれば、証明書の自動更新は有効なままとします。

[19] 承認された正式な連絡先変更手続きにより連絡先情報が変更されていれば、証明書の自動更新は有効なままとします。

### 4.7.1 証明書がリキーされる場合

証明書を継続して使用するには、既存の利用者証明書の有効期間内に、利用者は証明書のリキーを行う必要があります。証明書は、有効期間満了後にリキーすることもできます。

### 4.7.2 新しい公開鍵の証明書を要求できる者

個人向け証明書の場合はその利用者のみ、組織向け証明書の場合は正式な代表者のみが証明書の更新を要求できます。

### 4.7.3 証明書のリキー要求の処理

リキーの手続きにおいては、エンドユーザー利用者証明書の更新を要求する個人または組織が証明書の実際の利用者であること (または利用者から許可を得ていること) が確認されます。

実施可能な手続きとして、チャレンジ フレーズ (またはこれと同等なもの) を使用する方法や、秘密鍵の所持を証明する方法が挙げられます。利用者は申請情報とともに、チャレンジ フレーズ (またはこれと同等なもの) を選択し、提示します。証明書の更新では、利用者が自身の再申請情報とともにチャレンジ フレーズ (またはこれと同等なもの) を正しく提示し、申請情報 (連絡先情報を含む[20]) が変更されていなければ、更新された証明書が自動的に発行されます。セクション 3.3.1 の規定に従うことを条件として、この方法でリキーが行われてから、それ以降のリキーにおいて別の状況であった場合、シマンテックまたは RA は、本 CPS で最初の証明書申請の認証として規定されている要件に従って、利用者の識別情報を再確認するものとします。

上記の手続きまたはシマンテックが承認したその他の手続きの他に、最初の証明書申請における認証の要件がエンドユーザー利用者証明書のリキーに使用されるものとします。

### 4.7.4 利用者への新しい証明書の発行通知

リキーされた証明書の利用者への発行通知は、セクション 4.3.2 に従って行われます。

### 4.7.5 リキーされた証明書の受領確認となる行為

リキーされた証明書を受領したこととされる行為は、セクション 4.4.1 に従います。

### 4.7.6 リキーされた証明書の CA による公開

リキーされた証明書は、一般にアクセス可能なシマンテックのリポジトリで公開されます。

### 4.7.7 他のエンティティへの CA による証明書発行通知

RA は、自身が承認した証明書発行に関する通知を受け取ることができます。

## *4.8 証明書の変更*

### 4.8.1 証明書の変更が行われる場合

証明書を変更するとは、既存の証明書に記載された情報 (利用者の公開鍵を除く) に変更があるために、新しい証明書の発行を申請するということです。

証明書の変更は、セクション 4.1 に規定される証明書申請として見なされます。

[20] 承認された正式な連絡先変更手続きにより連絡先情報が変更されていれば、証明書の自動更新は有効なままとします。

### 4.8.2 証明書の変更を要求できる者

セクション 4.1.1 を参照してください。

### 4.8.3 証明書の変更要求の処理

シマンテックまたは RA は、セクション 3.2 の規定に従い、必要とされるすべての利用者情報について、識別と認証を実行するものとします。

### 4.8.4 利用者への新しい証明書の発行通知

セクション 4.3.2 を参照してください。

### 4.8.5 変更された証明書の受領確認となる行為

セクション 4.4.1 を参照してください。

### 4.8.6 変更された証明書の CA による公開

セクション 4.4.2 を参照してください。

### 4.8.7 他のエンティティへの CA による証明書発行通知

セクション 4.4.3 を参照してください。

## *4.9 証明書の失効および効力停止*

### 4.9.1 失効が行われる場合

以下に挙げた場合にのみ、エンドユーザー利用者証明書は、シマンテック (または利用者) によって失効され、CRL で公開されます。以下に挙げた場合以外の事由によって証明書の使用ができない (または、使用を望まない) 利用者から要求があった場合、シマンテックは、そのデータベース内で有効でないものとして証明書にフラグを設定しますが、CRL 上では公開しません。

エンドユーザー利用者証明書は、次のいずれかの事由が生じた場合に失効されます。

- シマンテック、カスタマ、または利用者において、利用者の秘密鍵が危殆化したと確信できる理由がある、またはそのことが強く疑われる場合
- シマンテックまたはカスタマにおいて、適用される利用規約に定める重要な義務、表明、または保証に関して利用者が重大な違反を行ったと確信できる理由がある場合
- 利用者との利用規約が解除された場合
- エンタープライズ カスタマと利用者の関係が解消された場合、または終了した場合
- Class 3 組織向け ASB 証明書の利用者である組織と、利用者の秘密鍵を制御している組織代表者の関係が解消された場合、または終了した場合
- シマンテックまたはカスタマにおいて、「適用される CPS で求められる手続きに厳密に従わずに証明書が発行された」、「証明書 (Class 1 証明書を除く) が証明書のサブジェクトとして指定されている者以外に対して発行された」、「証明書 (Class 1 証明書を除く) が当該証明書のサブジェクトとして指定されている者の許可を得ずに発行された」のいずれかの状況であると確信できる理由がある場合
- シマンテックまたはカスタマにおいて、証明書申請内の重要情報が虚偽であると確信できる理由がある場合
- シマンテックまたはカスタマにおいて、証明書発行に関する重大な前提条件が満たされておらず、免除もできないと判断する場合
- Class 3 組織向け証明書の場合において、利用者の組織名が変更される場合

- 確認されない利用者情報を除き、証明書内の情報に誤りがある場合、または変更が生じた場合
- セクション 6.3.2 に規定された方法で、利用者の識別情報が再確認できなかった場合
- コードサイニング証明書の場合で、
    - o アプリケーション ソフトウェア提供者が CA の失効と証明書がマルウェアまたは不必要なソフトウェアの署名に使われたことの可能性について調査を要求した場合
    - o STN 関係者に証明書がマルウェアの署名に使用されたことを示す報告書が提出された場合
- 利用者が期限までに利用料を支払わなかった場合
- 証明書の使用を継続すると、STN に悪影響が及ぶ場合

証明書を使用することで STN に悪影響が及ぶかどうかを検討する場合、シマンテックでは特に以下のことを考慮します。

- 受け取った苦情の特徴と回数
- 苦情を申し立てた者の識別情報
- 効力を有する関連法規
- 悪影響を及ぼすと申し立てられた使用に対する利用者からの回答

コードサイニング証明書を使用することで STN に悪影響が及ぶかどうかを検討する場合、さらにシマンテックでは以下のことを特に考慮します。

- 署名されているコードの名前
- コードの動作
- コードの配布方法
- コードの受領者への開示
- コードについての追加の申し立て
- 2017 年 2 月 1 日以降、コードサイニング証明書は、マイクロソフトによって採択された the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates のセクション 13.1.5 に記載されている全ての加入者証明書の失効理由に適合します

シマンテックは、管理者として行動するための管理者権限が解除された場合、または終了した場合、管理者証明書を失効させることもできます。

シマンテックの利用規約では、エンドユーザー利用者に対し、その秘密鍵の危殆化を把握したか疑いが生じた時点で直ちにシマンテックに通知するよう規定しています。

#### 4.9.1.1 失効理由に関する CA/ブラウザ フォーラム要件

EV SSL 証明書、EV コードサイニング証明書、およびドメイン認証/組織認証の SSL 証明書は、STN の追加手続きとして、付録 B1、付録 C、および付録 Dで規定されている CA/ブラウザ フォーラムの要件に準拠します。

### 4.9.2 失効を要求できる者

個人の利用者は、自身の個人向け証明書の失効について、シマンテックまたは RA の正式な代表者を通じて要求できます。組織向け証明書の場合は、当該組織の正当な権限が与えられた代表者が、当該組織に対して発行された証明書の失効を要求できるものとします。シマンテックまたは RA の正当に権限が与えられた代表者は、RA 管理者の証明書の失効を要求できるものとします。利用者の証明書申請を承認したエンティティも、利用者証明書を失効させるか、失効を要求できるものとします。

コードサイニング証明書について、シマンテックと関連会社は、コードサイニング証明書の提供先であるアンチ・マルウェア組織、加入者、依拠当事者、アプリケーション ソフトウェア提供者およびその他に対して、秘密鍵漏洩の疑い、証明書の誤った利用、証明書の疑わしいコードに対する署名、乗っ取り攻撃、その他の詐欺行為への利用、漏洩、誤利用、不適切な管理、その他証明書に関連する事項についてどのように報告するかについて明確な指示を提供します。シマンテックと関連会社はウェブサイトに説明書を一般公開します。

シマンテックとその関連会社は、コードサインニング証明書の発行と、以下の４つの事象による失効権限を有します。(1) アプリケーション ソフトウェア提供者が失効の要求をしシマンテックまたはその関連会社がその他の行動を採る意図がない場合、(2) 認証された加入者が失効の要求をした場合、(3) CA が証明書の漏洩もしくは疑いがあるコードに対して使用したと信じるに足りる情報が、第三者より提供された場合、(4) CA が当該証明書は失効すべきであると判断した場合。シマンテックと関連会社は、the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates のセクション 13.1.5 に記載の失効要求の対応手順に沿ったコードサイニング証明書を発行します。

シマンテックのみ、自身の CA に対して発行された証明書の失効を要求または開始できます。RA は、正当に権限が与えられた自身の代表者を通じて、自身の証明書の失効を要求できます。また、RA の上位エンティティは、自身の証明書の失効を要求または開始できるものとします。

いかなる人物も証明書の誤使用、証明書に関する不適切な管理、詐欺または鍵の漏洩の目撃をシマンテック ウェブサイト https://www.symantec.com/contact/authentication/ssl-certificate-complaint.jsp からオンラインフォームを使って証明書問題報告を提出することによって要求でき、CABF 基本要件に記載の時間以内に行動が取られます。

### 4.9.3 失効を要求する手続き

#### 4.9.3.1 エンドユーザー利用者証明書の失効を要求する手続き

失効を要求するエンドユーザー利用者は、シマンテックまたは当該利用者の証明書申請を承認したカスタマに対しその要求について伝えなければならず、連絡を受けた側は速やかに証明書の失効を開始します。エンタープライズ カスタマの場合、利用者はエンタープライズ管理者に対し要求について伝えなければならず、連絡を受けた管理者は失効要求について処理するためにシマンテックに連絡します。この失効要求の連絡については、CPS のセクション 3.4 の規定に従うものとします。エンタープライズ以外のカスタマの場合も、CPS のセクション 3.4 の規定に従って失効要求を連絡するものとします。

エンタープライズ カスタマが、自らの判断で、エンドユーザー利用者証明書の失効を開始する場合、Managed PKI カスタマまたは ASB カスタマは、当該証明書を失効するようシマンテックに指示します。

#### 4.9.3.2 証明書失効プロセスに関する CA/ブラウザ フォーラム要件

EV SSL 証明書、EV コードサイニング証明書、およびドメイン認証/組織認証の SSL 証明書は、STN の追加手続きとして、付録 B1 および付録 C、ならびに付録 Dで規定されている CA/ブラウザ フォーラムの要件に準拠します。

#### 4.9.3.3 CA/RA 証明書の失効を要求する手続き

自身の CA/RA 証明書の失効を要求する CA または RA は、かかる要求についてシマンテックに連絡する必要があります。シマンテックは、それを受けて当該証明書を失効させます。シマンテックは、CA/RA 証明書の失効を開始することもできます。

### 4.9.4 失効要求の猶予期間

失効要求は、商業上合理的な時間内に、可能な限り速やかに提出されるものとします。

### 4.9.5 CA による失効要求処理の期限

シマンテックは、遅滞なく失効要求を処理するために、商業上合理的な対策を講じます。
2017 年 2 月 1 日以降、シマンテックは、コードサイニング証明書について、the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates のセクション 13.1.5.3 のマルウェアとして定義されている失効時間に従います。

### 4.9.6 依拠当事者の失効調査の要件

依拠当事者は、依拠しようとする証明書のステータスを調査するものとします。依拠当事者が証明書ステータスを調査する方法の 1 つとして、依拠当事者が依拠しようとする証明書を発行した CA が公表した最新の CRL の調査が挙げられます。また、依拠当事者は、適切な Web ベースのリポジトリを使用して証明書ステータスを調査するか、OCSP (利用可能な場合) を使用することで、この要件に対応することも可能です。CA は、失効のステータスを調査するために、依拠当事者に対して、適切な CRL、Web ベースのリポジトリ、または OCSP レスポンダ (利用可能な場合) の所在場所についての情報を提供するものとします。

CRL リポジトリは多数かつ色々な場所にあるため、依拠当事者は証明書に含まれる CRL Distribution Points エクステンションの URL を使って CRL にアクセスすることが推奨されます。適切な OCSP レスポンダは、証明書に含まれる Authority Information Access エクステンションにあります。

### 4.9.7 CRL の発行頻度

エンドユーザー利用者証明書の CRL は、少なくとも 1 日 1 回発行されます。CA 証明書の CRL は、少なくとも年 1 回発行され、さらに CA 証明書が失効するたびに発行されるものとします。[21]

Authenticated Content Signing (ACS) のルート CA の CRL は、年に 1 回公開されますが、CA 証明書が失効したときも、その都度公開されます。

CRL に記載されている証明書の有効期間が切れると、証明書の有効期間以降に発行される CRL から証明書が削除される場合があります。

#### 4.9.7.1 CRL 発行に関する CA/ブラウザ フォーラム要件

EV SSL 証明書、EV コードサイニング証明書、およびドメイン認証/組織認証の SSL 証明書の CRL の発行については、STN の追加手続きとして、付録 B1 および付録 C、ならびに付録 Dで規定されている CA/ブラウザ フォーラムの要件に準拠します。

[21]「Symantec Class 3 Organizational VIP Device CA」の CRL は、CA が発行した証明書が失効したときにのみ、その都度発行されます。

#### 4.9.7.2 CRL 発行に関する マイクロソフト要件

コードサイニングとタイムスタンプ証明書のCRL発行頻度は、本CPSに記載されており、https://aka.ms/csbr に掲載されている the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificatesのセクション13.2.2に従います。

### 4.9.8 CRL の最大遅延時間

CRL は、作成されてから商業上合理的な時間内にリポジトリに掲載されます。通常、作成から数分以内に自動的に行われます。

### 4.9.9 利用可能なオンラインでの失効/ステータス調査

オンラインでの失効およびその他の証明書ステータスの情報は、Web ベース リポジトリ、そして提供されている場合は OCSP を通じて入手できます。シマンテックは、CRL の公開に加え、シマンテック リポジトリにおけるクエリー機能により、証明書ステータス情報を提供します。

個人向け証明書ステータス情報を確認できる Web ベースのクエリー機能には、以下のシマンテック リポジトリからアクセスできます。

- https://pki-search.symauth.com/pki-search/index.html

シマンテックは、OCSP による証明書ステータス情報も提供しています。OCSP サービスに関する契約を締結しているエンタープライズ カスタマは、OCSP を利用することにより証明書ステータスを調査できます。関係する OCSP レスポンダの URL は、エンタープライズ カスタマに伝えられます。

シマンテックは、コードサイニングとタイムスタンプ証明書の OCPS レスポンスを証明書の有効期限が切れた後、少なくとも10 年間提供します。失効された証明書のシリアル番号は、証明書の有効期限が切れた後、少なくとも 10 年間 CRL に残ります。

#### 4.9.9.1 OCSP の利用に関する CA/ブラウザ フォーラム要件

EV SSL 証明書、EV コードサイニング証明書、およびドメイン認証/組織認証の SSL 証明書での OCSP の利用については、STN の追加手続きとして、付録 B1 および付録 C、ならびに付録 Dで規定されている CA/ブラウザ フォーラムの要件に準拠します。

### 4.9.10 オンラインでの失効調査の要件

依拠当事者は、依拠しようとする証明書のステータスを調査しなければなりません。依拠当事者が依拠しようとしている証明書のステータスについて、関連する最新の CRL を参照するという方法で調査しない場合、当該依拠当事者は、適切なリポジトリを参照するか、(OCSP のサービスが利用できる場合は) 適切な OCSP レスポンダを使用して証明書ステータスを要求することにより、証明書のステータスを調査するものとします。

### 4.9.11 その他の利用可能な失効通知の形式

規定されません。

### 4.9.12 鍵の危殆化についての特別な要件

シマンテックは、自身の CA のいずれか、またはサブドメイン内のいずれかの CA の秘密鍵が危殆化したことを発見した場合、またはそう確信する理由がある場合には、商業上合理的な努力を尽くして、潜在的な依拠当事者に通知します。

### 4.9.13 効力を停止する場合

規定されません。

### 4.9.14 効力停止を要求できる者

規定されません。

### 4.9.15 効力停止を要求する手続き

規定されません。

### 4.9.16 効力停止期間の制限

規定されません。

## *4.10 証明書のステータス サービス*

### 4.10.1 運用上の特性

パブリック証明書のステータスは、シマンテックの Web サイトに掲載されている CRL、LDAP ディレクトリ、および (利用できる場合は) OCSP レスポンダを通じて確認できます。

### 4.10.2 サービスの可用性

証明書ステータス サービスは、計画的な停止を除き、24 時間 365 日利用できます。

EV SSL 証明書、EV コードサイニング証明書、およびドメイン認証/組織認証の SSL 証明書の証明書ステータス サービスについては、STN の追加手続きとして、付録 B1 および付録 C、ならびに付録 D で規定されている CA/ブラウザ フォーラムの要件に準拠します。

### 4.10.3 オプション機能

OCSP は、オプションのステータス確認サービス機能です。すべての製品で利用できるわけではなく、製品によっては有効に設定しなければならない場合があります。

## *4.11 利用の終了*

利用者は、以下の事由によりシマンテック証明書の利用を終了できます。

- 利用者の証明書を、更新またはリキーを行うことなく有効期間満了とする場合
- 利用者の証明書を、証明書の取り替えを行うことなく、有効期間内に失効させた場合

## *4.12 鍵の預託と復元*

Managed PKI Key Management Service を導入している企業を除き、STN 参加者は、CA、RA、エンドユーザー利用者の秘密鍵を預託できません。

Symantec Managed PKI Service で鍵預託オプションを使用するエンタープライズ カスタマは、自身が承認する証明書申請を行った利用者の秘密鍵のコピーを預託できます。エンタープライズ カスタマは、企業施設内またはシマンテックの安全なデータ センター内で鍵を預託できます。企業施設外で運用される場合、シマンテックは、利用者の秘密鍵のコピーを保管しませんが、利用者の鍵復元処理において重要な役割を果たします。

### 4.12.1 鍵の預託/復元のポリシーと実施方法

Symantec Managed PKI Service (またはシマンテックが承認した同等のサービス) で鍵預託オプションを使用するエンタープライズ カスタマは、エンドユーザー利用者の秘密鍵を預託することが許可されています。預託された秘密鍵は、Managed PKI Key Manager ソフトウェアを使用して暗号化された形式で保管されるものとします。Managed PKI Key Manager Service (またはシマンテックが承認した同等のサービス) を使用するエンタープライズ カスタマを除き、CA またはエンドユーザー利用者の秘密鍵は預託されないものとします。

エンドユーザー利用者の秘密鍵は、Managed PKI Key Management Service の管理者ガイド内で許可されている状況においてのみ復元されるものとします。当該ガイドにおいては以下のことが求められます。

- Managed PKI Key Manager を使用しているエンタープライズ カスタマは、利用者を主張する者からの利用者の秘密鍵の要求が実際にその利用者からであり、不正によるものではないことを確認するため、利用者になると主張している者の識別情報を確認するものとします。
- エンタープライズ カスタマは、違法、詐欺、またはその他の不正な目的のためではなく、司法または行政上の手続きもしくは捜索令状に従うなど、正当かつ合法的な目的がある場合においてのみ、利用者の許可なく、利用者の秘密鍵を復元するものとします。
- かかるエンタープライズ カスタマは、Key Management Service 管理者およびその他の者が秘密鍵に不正アクセスするのを防ぐため、要員管理を取り入れるものとします。

Symantec Managed PKI Service で鍵預託オプションを使用するエンタープライズ カスタマには、以下の事項を実施することが推奨されています。

- 利用者に対して、当該利用者の秘密鍵が預託されていることを通知する
- 預託された利用者の鍵を不法な開示から保護する
- 預託された利用者の鍵の復元に使用される可能性がある管理者自身の鍵を含む、すべての情報を保護する
- 適切に認証および承認された復元要求に対してのみ、預託された利用者の鍵を引き渡す
- 紛失した証明書の使用を中止するなどの特定の状況においては、暗号化鍵を復元する前に、利用者の鍵ペアを失効させる
- 利用者自身が復元を要求した場合を除き、鍵復元に関する情報を利用者に伝えない
- 法律、政府の定める規則、規制、エンタープライズ カスタマの内規、または所轄裁判所からの命令により要求されない限り、預託された鍵または預託された鍵に関連する情報を第三者に開示しない、または開示を許可しない

### 4.12.2 セッション キーのカプセル化、および復元のポリシーと実施方法

秘密鍵は、暗号化された形式にて Key Manager データベースで保管されます。各利用者の秘密鍵は、独自のトリプル DES 対称鍵で個別に暗号化されます。Key Escrow Record (KER) が生成され、次にトリプル DES 鍵がランダム セッション キーと結合され、セッション キー マスク (MSK) を形成します。結果として生じた MSK は、証明書要求情報とともに、シマンテックの Managed PKI データベースに安全な方法で送信され、保管されます。KER (エンドユーザーの秘密鍵を含む) と個々のセッション キーは、Key Manager データベースに保管され、それ以外の鍵関連データはすべて破棄されます。

Managed PKI データベースは、シマンテックの安全なデータ センターから運用されます。エンタープライズ カスタマは、Key Manager データベースの運用場所として、自社内またはシマンテックの安全なデータ センターのいずれかを選択できます。

秘密鍵および電子証明書を復元する際には、Managed PKI 管理者が安全な方法で Managed PKI Control Center にログインし、復元する鍵ペアを適切に選択して、[Recover] のハイパーリンクをクリックする必要があります。承認された管理者が [Recover] リンクをクリックした場合にのみ、当該鍵ペア

の MSK が Managed PKI データベースから返されます。Key Manager では、KMD からセッションキーを取り出して MSK と結合させ、最初に秘密鍵を暗号化するのに使用されたトリプル DES 鍵を再生成し、エンドユーザーの秘密鍵の復元を可能にします。最後に、暗号化された PKCS#12 ファイルが管理者へ返され、最終的にエンドユーザーに配布されます。

# 5. 施設、管理、運用における制御

## *5.1 物理的制御*

シマンテックは、本 CPS のセキュリティ要件に対応するシマンテック物理的セキュリティ ポリシーを実装しています。このポリシーへの準拠は、セクション 8 に記載されているシマンテックの独自の監査要件に含まれます。シマンテック物理的セキュリティ ポリシーにはセキュリティに関する機密情報が含まれており、シマンテックの合意がある場合にのみ参照できます。要件の概要については、以下のサブセクションで説明されています。

### 5.1.1 施設の所在地および構造

STN CA および RA の運用は、内密か公然かに関係なく、機密情報とシステムの不正な使用、アクセス、または開示を防止、予防、および検知するよう物理的に保護された環境において行われます。

また、シマンテックは CA の運用のために、災害復旧施設も維持します。シマンテックの災害復旧施設は、複数の物理的セキュリティ階層により保護されており、シマンテックの主要施設に匹敵します。

### 5.1.2 物理的アクセス

STN CA システムは、最低でも 4 階層の物理的セキュリティによって保護されており、上位の階層にアクセスする前に、下位の階層にアクセスする必要があります。

各階層へのアクセスは、段階的に制限される物理的アクセス権により制御されます。機密を要する CA 運用業務や、認証、検証、発行などの証明書プロセスのライフサイクルに関連するすべての業務は、高度に制限された物理的階層内で行われます。各階層にアクセスする際には、近接型カードと従業員バッジを使用する必要があります。物理的アクセスは、ログおよび映像により自動的に記録されます。追加階層では、生体認証を含む二要素認証を利用して、個別のアクセス制御が行われます。付き添いのない者 (信頼できない従業員や訪問者など) は、そのような保護された場所への入室は許可されません。

物理的セキュリティ システムには、鍵管理セキュリティを目的とした追加階層が含まれており、CSU および鍵情報のオンラインおよびオフラインでの保管を保護します。暗号化情報の作成および保管に使用されるエリアは、それぞれ生体認証を含む二要素認証を利用したデュアル コントロールが必須となります。オンラインの CSU はロックされたキャビネットを利用して保護され、オフラインの CSU は施錠された金庫、キャビネット、およびコンテナを利用して保護されます。CSU および鍵情報へのアクセスは、シマンテックの職務分離に関する要件に従って制限されます。これらの階層におけるキャビネットまたはコンテナの開閉は、監査を目的として記録されます。

### 5.1.3 電源および空調

シマンテックの安全性の高い施設は、一次施設および予備施設として、以下の設備を備えています。

- 電力の継続的供給を確保する電源システム
- 温度および相対湿度を制御するための暖房/換気/空調システム

### 5.1.4 水害

シマンテックでは、シマンテックのシステムへの水害の影響を最小限に抑えるための合理的な対策を講じています。

### 5.1.5 火災予防および火災保護対策

シマンテックでは、火災の予防および消火、炎または煙によるその他の損害を防ぐための合理的な対策を講じています。シマンテックの火災予防および火災保護対策は、国内の火災安全規則に従って設計されています。

### 5.1.6 媒体の保管

商用ソフトウェアおよびデータ、監査資料、アーカイブ、またはバックアップ資料を格納する各種媒体は、シマンテックの施設内に保管されるか、または許可された者だけにアクセスを限定する適切な物理的/論理的アクセス制御機能を有し、かかる媒体を不測の損傷（水害、火事、電磁気など）から保護するよう設計されているオフサイトの安全な保管施設で保管されます。

### 5.1.7 廃棄処理

機密文書および資料は、廃棄前にシュレッダーにより処分されます。機密情報を収集または伝達するために利用された媒体は、廃棄前に読み取り不可の状態にします。暗号化デバイスは、廃棄前に、物理的に破壊されるか、製造業者のガイドラインに従い初期化されます。その他の廃棄物は、シマンテックの通常の廃棄物処理要件に従って廃棄されます。

### 5.1.8 オフサイトでのバックアップ

シマンテックは、重要なシステム データ、監査ログ データ、その他の機密情報のバックアップを定期的に行います。オフサイトのバックアップ媒体は、保証付きの第三者の保管施設およびシマンテックの災害復旧施設を使用して、物理的に安全な方法で保管されます。

## *5.2 手続きの制御*

### 5.2.1 信頼される役割

信頼される者とは、認証または暗号化業務を行うか制御する全従業員、請負業者、およびコンサルタントなどであり、以下の作業に大きくかかわる可能性があります。

- 証明書申請における情報の検証
- 証明書の申請、失効要求、更新要求、または申請情報に対する承認、否認、またはその他の処理
- 証明書の発行または失効 (リポジトリの制限された部分へアクセスできる者を含む)
- 利用者の情報または要求への対処

信頼される者の職務には、以下のものが含まれますが、これらに限定されません。

- カスタマ サービス要員
- 暗号化業務要員
- セキュリティ要員
- システム管理者
- 特定の技術要員
- 基盤の信頼性を管理するために指定された経営陣

シマンテックは、本セクションで特定された要員の区分を、信頼される地位を有する信頼される者とみなします。信頼される地位を取得して信頼される者になろうとする者は、本 CPS に規定されている資格要件を満たさなければなりません。

### 5.2.2 職務ごとに必要とされる人数

シマンテックは、業務内容に基づいて職務を分離すること、および機密を要する職務が複数の信頼される者により実施されることを確実にするための厳格な制御手続きを定め、維持し、実施しています。

業務内容に基づく職務の分離を確実に行うために、方針と制御手続きが定められています。CA 用暗号化ハードウェア (暗号化署名ユニットまたは CSU) および関連する鍵情報へのアクセスや管理など、最も機密性の高い職務には、複数の信頼される者が要求されます。

このような内部統制手続きは、物理的または論理的にデバイスにアクセスするために最低 2 名の信頼される要員が必要となるよう設計されています。CA 用暗号化ハードウェアへのアクセスは、その受け入れと審査から最終的な論理的/物理的破壊までのライフサイクル全体において、複数の信頼される者により厳格に実施されます。運用鍵を使用してモジュールがアクティベーションされると、さらに厳格なアクセス制御機能が呼び出され、デバイスへの物理的および論理的アクセスにおける分割制御が維持されます。モジュールに対して物理的にアクセスできる者は「シークレット シェア」を保有しておらず、「シークレット シェア」を保有する者はモジュールに対して物理的にアクセスできません。

Class 3 証明書の検証および発行など、自動的な検証/発行システムの対象外となるその他の手動での業務は、2 名以上の信頼される者によって、または 1 名以上の信頼される者と自動的な検証/発行プロセスを組み合わせることによって行われます。鍵復元を手動で行う場合は、任意で、許可された 2 名の管理者による検証を必須にすることができます。

### 5.2.3 各役割の識別と認証

信頼される者になろうとするすべての者について、シマンテックの HR またはセキュリティ部門への面前出頭および広く認識されている身分証明書 (パスポート、運転免許証など) の調査により、識別情報の確認が行われます。識別情報については、本 CPS セクション 5.3.1 の経歴調査手続きによってさらに確認されます。

シマンテックは、当該人物が信頼される地位を獲得していること、および部署の承認を得ていることを確認してから、当該人物に対して以下を実施します。

- アクセス用デバイスを支給し、必要な施設へのアクセスを許可する
- STN CA、RA、またはその他の IT システムにアクセスして特定業務を実行するための電子的なクレデンシャルを発行する

### 5.2.4 職務の分離を必要とする役割

職務の分離を要求する役割には以下のものがあります (ただし、これらに限定されません)。

- 証明書申請における情報の検証
- 証明書の申請、失効要求、鍵復元要求、更新要求、または申請情報に対する承認、否認、またはその他の処理
- 証明書の発行または失効 (リポジトリの制限された部分へアクセスできる者を含む)
- 利用者の情報または要求への対処
- CA 証明書の生成、発行、または破棄
- プロダクション環境への CA のロード作業

## *5.3 人事的管理*

信頼される者になろうとする者は、想定される業務を問題なく遂行するために必要な経歴、資格、および経験を有している証拠を提出しなければなりません。さらに必要な場合、政府機関との契約に基づく証明サービスを履行するために必要な政府の許可書も提出しなければなりません。経歴調査は、信頼される地位を有する要員について、少なくとも 5 年ごとに実施されます。

### 5.3.1 資格、経験、および許可書の要件

シマンテックは、信頼される者になろうとする者に対し、想定される業務を問題なく十分に遂行するために必要な経歴、資格、および経験を有している証拠を提出することを要求します。さらに必要な場合、政府機関との契約に基づく証明サービスを履行するために必要な政府の許可書の提出も要求します。

### 5.3.2 経歴調査手続き

信頼される役割の雇用を開始する前に、シマンテックは以下の項目を含む経歴調査を行います。

- 過去の就業状況の確認
- 職歴の照会
- 最高位の学歴、または最も関連の深い学歴の確認
- 犯罪歴の調査 (地区、地方、全国区)
- 信用情報/財務記録の調査
- 運転免許経歴証明書の調査
- 社会保障局の記録の調査

地域に適用される法律またはその他の状況より、本セクションで規定されたいずれかの要件を満たすことができない場合、シマンテックは、法律で許可されている代替調査手段を活用して、極めて類似の情報が提供されるようにします。これは、関係する政府機関によって実施された経歴調査の取得を含みますがこれに限定されません。

経歴調査により明らかになった事項で、信頼される地位の候補者として否認される理由になる可能性があるもの、または既存の信頼される者に対して何らかの措置を講じる理由になる可能性があるものとしては、通常、以下のものがあります (ただしこれらに限定されません)。

- 候補者または信頼される者の不実表示
- 極めて好ましくない、または信頼できない職歴の照会
- 犯罪の有罪判決
- 財務面の無責任さを裏付けるもの

上記の情報を含む報告書は、人事およびセキュリティの要員が査定し、経歴調査で明らかになった事項の種類、影響の大きさ、および行動の頻度を考慮して、適切な方針を決定します。決定された措置として、信頼される地位の候補者としての採用中止や、既存の信頼される地位の剥奪などが実施される場合があります。

経歴調査で明らかにされた情報を使用してかかる措置を実施する場合は、関連する連邦、州、および地域の法律に従います。

### 5.3.3 トレーニング要件

シマンテックは、採用した要員に対し、問題なく十分に業務を遂行するために必要とされるトレーニング (オンザジョブ トレーニングを含む) を行います。かかるトレーニングの記録は、シマンテックが保持します。シマンテックは、必要に応じて、トレーニング プログラムを定期的に見直し、向上させます。

シマンテックのトレーニング プログラムは、個人の業務に合わせて用意され、関連する内容として以下の項目が盛り込まれます。

- PKI の基本的な概念
- 業務責任
- シマンテックのセキュリティ/運用におけるポリシーおよび手続き
- 導入するハードウェアおよびソフトウェアの利用と運用
- 事故および危殆化が発生した場合の報告と対処方法
- 災害復旧および業務継続の手続き

#### 5.3.3.1 トレーニングとスキル レベルに関する CA/ブラウザ フォーラム要件

EV SSL 証明書、EV コードサイニング証明書、およびドメイン認証/組織認証の SSL 証明書の場合、STN の追加手続きとして、付録 B1、付録 C、および付録 D で規定されている要員トレーニングが行われます。

### 5.3.4 再トレーニングの頻度および要件

シマンテックは要員に対し、かかる要員が業務を問題なく十分に遂行するためのスキル レベルを確実に維持するために必要な範囲および頻度で、再トレーニングおよび最新情報を提供します。

### 5.3.5 人事異動の頻度および順序

規定されません。

### 5.3.6 無許可の行為に対する制裁

無許可の行為またはシマンテックのポリシーと手続きに違反するその他の行為に対しては、適切な懲戒処分が下されます。懲戒処分は解雇にまで及ぶ場合もあり、無許可の行為の頻度および程度に応じた措置が取られます。

### 5.3.7 請負事業者の要件

限られた状況において、請負事業者またはコンサルタントが、信頼される地位を占めることがあります。そのような請負業者またはコンサルタントのいずれに対しても、同様の地位にあるシマンテックの従業員に適用されるものと同一の職務上およびセキュリティ上の基準が適用されます。

本 CPS セクション 5.3.2 で規定されている経歴調査手続きを完了していない、または通過していない請負事業者およびコンサルタントは、信頼される者に付き添われ、常に直接監督される場合においてのみ、シマンテックの安全に管理された施設内に入室できます。

### 5.3.8 要員に提供される資料

シマンテックは、従業員に対し、業務を問題なく十分に遂行するために必要なトレーニングおよびその他の資料を提供します。

## *5.4 監査ログの手続き*

### 5.4.1 記録されるイベントの種類

シマンテックは、手動または自動により、以下の重要なイベントについて記録します。

- 以下の事項を含む、CA の鍵のライフサイクル管理に関するイベント
    - o 鍵の生成、バックアップ、保管、復元、アーカイブ、および破壊

    - CA の詳細または鍵の変更
    - 暗号化デバイスのライフサイクル管理に関するイベント
- 以下の事項を含む、CA および利用者証明書のライフサイクル管理に関するイベント
    - 証明書の申請、発行、更新、リキー、および失効
    - 要求の処理 (成功したものおよび不成功に終わったものを含む)
    - 証明書作成ポリシーの変更
    - 証明書および CRL の生成と発行
- 信頼される従業員イベント、以下
    - ログオン、ログオフの実施
    - 全ての権限者の作成、削除、パスワード設定、システム権限変更の実施
    - 人員変更
- セキュリティに関連する以下のイベント:
    - PKI システムへのアクセスの試み (成功したものおよび不成功に終わったものを含む)
    - システムおよびアプリケーションの開始と終了
    - CA 秘密鍵の運用のためのアクティベーション データの保有
    - システム構成変更とメンテナンス
    - シマンテックの要員によって実行された PKI およびセキュリティのシステムに対する行為
    - セキュリティへの配慮が必要なファイルまたは記録に対する読み取り、書き込み、削除、または破壊
    - セキュリティ プロファイルの変更
    - システム故障、ハードウェア障害、およびその他の異常
    - ファイアウォールおよびルーターの動作
    - CA 施設への訪問者の入退室

ログには以下の項目が記録されます。

- 記録された日時
- 自動的に書き込まれる日常的な記録の場合は、そのシリアル番号またはシーケンス番号
- 日常的な記録を書き込むエンティティの識別情報
- 記録の説明/種別

シマンテックの RA とエンタープライズの管理者は、次の事項を含む、証明書申請に関する情報を記録します。

- 証明書申請者により提出された身分証明書の種類
- 該当する場合は、身分証明書に記載されている一意の識別データ、番号、またはそれらの組み合わせ (証明書申請者の運転免許証番号など)
- 申請書および身分証明書のコピーの保管場所
- 申請を受領したエンティティの識別情報
- 身分証明書を検証するために使用された方法 (ある場合)
- 証明書申請を受領した CA または発行指示を行った RA の名称 (該当する場合)

EV SSL 証明書、EV コードサイニング証明書、およびドメイン認証/組織認証の SSL 証明書は、STN の追加手続きとして、付録 B1、付録 C、および付録 D で規定されている CA/ブラウザ フォーラムの要件に準拠します。

### 5.4.2 ログを処理する頻度

CA システムは継続的に監視され、セキュリティおよび運用に関して重大なイベントが発生した場合には即時に警告が発せられ、任命されたシステム セキュリティ要員による確認が行われます。月次の監査ログ レビューでは、当該ログが改ざんされていないか検証され、さらにログで検出されたあらゆる警告または異常イベントが精査されます。監査ログ レビューに基づいて取られた措置についても文書化されます。

### 5.4.3 監査ログを保持する期間

監査ログは、少なくとも処理後 2 か月間はオンサイトで保管され、その後はセクション 5.5.2 に従ってアーカイブされるものとします。

### 5.4.4 監査ログの保護

監査ログは、ログ ファイルに対して不正な参照、改変、削除、またはその他の改ざん行為が行われないよう保護する仕組みが備わっている電子的な監査ログ システムにより保護されます。

### 5.4.5 監査ログのバックアップ手続き

監査ログの増加分のバックアップは 1 日 1 回、全体のバックアップは週に 1 回の頻度で実行されます。

### 5.4.6 監査データ収集システム (内部と外部)

自動生成される監査データは、アプリケーション、ネットワーク、およびオペレーティング システムのレベルで記録されます。手動作成される監査データは、シマンテックの要員によって記録されます。

### 5.4.7 イベントを起こしたサブジェクトへの通知

監査データ収集システムでイベントがログに記録される際に、当該イベントを起こした個人、組織、デバイス、またはアプリケーションに対して通知することは要求されません。

### 5.4.8 脆弱性の評価

監査プロセスでイベントが記録されるのは、システムの脆弱性を監視するためでもあります。このように監視されたイベントが調査されてから、論理的なセキュリティ脆弱性評価 (LSVA) が実行され、レビューされて、修正されます。LSVA はリアルタイムで自動収集されるログ データを基盤として、日次、月次、および年次ベースで実行されます。年次の LSVA は、エンティティの年次のコンプライアンス監査の資料として利用されます。

## *5.5 記録のアーカイブ*

### 5.5.1 アーカイブされる記録の種類

シマンテックは以下の記録をアーカイブします。

- セクション 5.4 の規定により収集されたすべての監査データ
- 証明書申請情報
- 証明書申請に添付された書類
- 証明書ライフサイクルに関連する情報 (失効、リキー、更新の申請情報など)

### 5.5.2 アーカイブの保管期間

記録は、証明書の有効期間満了日または失効日から少なくとも以下の期間にわたって保管されるものとします。

- Class 1 証明書については 5 年間
- Class 2 および Class 3 証明書については 10 年 6 か月間

### 5.5.3 アーカイブの保護

シマンテックはアーカイブを保護して、許可された信頼される者だけがアーカイブにアクセスできるようにします。アーカイブは、信頼性の高いシステムに保存することにより、不正な参照、改変、削除、またはその他の改ざんが行われないよう保護されます。アーカイブ データを格納する媒体、およびアーカイブ データを処理するのに必要とされるアプリケーションは、本 CPS で規定された期間にわたってアーカイブデータにアクセスできるよう維持されるものとします。

### 5.5.4 アーカイブのバックアップ手続き

シマンテックは、発行された証明書情報の電子アーカイブについて、増加分のバックアップは 1 日 1 回、全体のバックアップは週に 1 回の頻度で行います。紙媒体による記録のコピーは、オフサイトの安全性の高い施設において維持されるものとします。

### 5.5.5 記録にタイムスタンプをつける要件

証明書、CRL、およびその他の失効に関するデータベース エントリは、日時の情報を含むものとします。かかる時間情報については、暗号技術に基づく処理は必要とされません。

### 5.5.6 アーカイブ収集システム (内部または外部)

エンタープライズ RA カスタマを除き、シマンテックのアーカイブ収集システムは、内部に存在するシステムになります。エンタープライズ RA については、シマンテックが監査証跡の保存に関する支援を行います。従って、かかるアーカイブ収集システムは、そのエンタープライズ RA にとっては外部に存在するシステムとなります。

### 5.5.7 アーカイブ情報の取得および検証の手続き

許可された信頼される者だけがアーカイブにアクセスできます。情報が復元される際には、その整合性が検証されます。

## *5.6 鍵の切り替え*

STN CA の鍵ペアは、本 CPS で規定されたそれぞれの最大ライフタイム終了でその役割が終わります。STN CA 証明書は、CA 鍵ペアの認定された累計ライフタイムがその CA 鍵ペアの最大ライフタイムを超えない限りにおいて、更新できます。新規の CA 鍵ペアは、必要に応じて生成されます。たとえば、役割を終えようとしている CA 鍵ペアを交換する場合、使用中の鍵ペアを補完する場合、新しいサービスをサポートする場合などです。

上位 CA の CA 証明書の有効期間が満了になる前に、上位 CA の階層内において、古い上位 CA 鍵ペアから新しい CA 鍵ペアにエンティティが円滑に移行できるように、鍵の切り替え手続きが定められます。シマンテックの CA 鍵の切り替えプロセスでは、以下のことが要求されます。

- 上位 CA は、自身の鍵ペアの残存ライフタイムが、自身の階層内の下位 CA により発行された特定タイプの証明書の有効期間と等しくなる時点の 60 日以上前の日 (以下「発行停止日」) に下位 CA 証明書の新規発行を停止すること。

- 「発行停止日」後に受領した下位 CA (またはエンドユーザー利用者) 証明書要求が有効性検証で合格すると、証明書は新しい CA 鍵ペアで署名されること。

上位 CA は、元の鍵ペアを使用して発行された最後の証明書の有効期間満了日に達するまでは、元の上位 CA 秘密鍵で署名された CRL を発行し続けます。

## *5.7 危殆化および災害からの復旧*

### 5.7.1 事故および危殆化への対処手続き

CA に関する特定情報 (証明書申請データ、監査データ、発行されたすべての証明書に関するデータベース レコード) のバックアップは、オフサイト ストレージで保管され、危殆化または災害が発生した場合に利用可能になるものとします。CA 秘密鍵のバックアップは、CP セクション 6.2.4 に従って生成され、維持されるものとします。シマンテックは、シマンテック所有の CA に加え、シマンテック サブドメイン内のエンタープライズ カスタマの CA についても、前述の CA 情報のバックアップを維持します。

### 5.7.2 コンピュータ リソース、ソフトウェア、またはデータが破損した場合

コンピュータ リソース、ソフトウェア、またはデータについて破損が生じた場合、そのような問題が発生したことについてシマンテックのセキュリティ担当部署に報告され、シマンテックの事故対処手続きが定められます。かかる手続きでは、上位者に対する適切な報告、事故調査、および事故対応が要求されます。必要であれば、シマンテックの鍵の危殆化または災害復旧の手続きが定められます。

### 5.7.3 エンティティの秘密鍵が危殆化した場合の手続き

STN CA、シマンテック インフラストラクチャ、またはカスタマの CA 秘密鍵の危殆化が疑われた場合、もしくは認知された場合、シマンテックの鍵危殆化対応手続きが、シマンテック セキュリティ インシデント レスポンス チーム (SSIRT) により定められます。このチームは、セキュリティ、暗号化業務運用、プロダクション サービスの要員、およびその他のシマンテック経営陣の代表者で編成されており、状況を見極め、アクション プランを策定し、シマンテック経営陣の承認を得た上でアクション プランを実施します。

CA 証明書の失効が要求される場合は、以下の手続きが遂行されます。

- 証明書が失効された状態であることを、本 CPS セクション 4.9.7 に従って、シマンテック リポジトリを通じて依拠当事者に連絡する。
- 商業上合理的な努力を尽くして、影響を受けるすべての STN 参加者に失効の追加通知を提供する。
- CA は、本 CPS セクション 5.8 に従って CA が終了している場合を除き、本 CPS セクション 5.6 に従って新しい鍵ペアを生成する。

### 5.7.4 災害後の業務継続能力

シマンテックは、業務を中断しなければならないような状況下で、重要な業務機能を回復できるように業務継続プランを作成し維持します。シマンテックは主要なプロダクション施設から地理的に離れた場所で、災害復旧拠点 (Disaster Recovery Facility、以下「DRF」) を維持します。DRF は連邦政府と軍規格で設計された頑丈な施設であり、シマンテックのセキュリティ基準を満たすよう特に設備も整っています。[22]

[22] 株式会社シマンテックおよびシマンテック オーストラリアの施設は主要施設から地理的に離れた場所に DRF を維持しています。両方の DRF はシマンテックのセキュリティ標準を明確に満たすように作られています。

シマンテックの主要施設が永久に利用できなくなるほどの自然災害または人為的災害が発生した場合、シマンテック業務継続チームとシマンテック認証業務事故管理チームは、部門横断型の管理チームと協力して、災害状況を公式発表する判断を下し、事故を管理します。災害状況を公表してから、DRF でのシマンテックのプロダクション サービス機能の復旧に着手します。

シマンテックは、STN PKI Service を含む Managed PKI Service のための災害復旧プラン (Disaster Recovery Plan、以下「DRP」) を策定しています。DRP では、プランを実行に移す条件、および許容可能なシステム停止と復旧時間について特定します。DRP では、バックアップ データと STN 鍵のバックアップ コピーを使用してシマンテック STN 運用環境を再構成するチーム向けの手続きを定義します。

さらに、EV SSL 証明書、EV コードサイニング証明書、およびドメイン認証/組織認証の SSL 証明書の場合、シマンテックの DRP には、STN の追加手続きとして、付録 B1 および付録 C、ならびに付録 D で規定されている CA/ブラウザ フォーラムの要件が含まれます。

主要なプロダクション サービス機能の目標復旧時間は、24 時間以内です。

シマンテックは、DRF のサービス機能を確認するために災害復旧テストを少なくとも年に 1回 実施します。全社的な業務継続訓練もシマンテック業務継続チームにより、追加シナリオ (流行病、地震、洪水、停電など) の手続きをテストし評価するために毎年実施します。

シマンテックは業務復旧プランの策定、維持、テストに十分な措置を講じ、シマンテックの災害または重大な業務中断に備えたプランは業界で確立されているベスト プラクティスの多くと合致しています。

シマンテックは、その災害復旧施設において、冗長構成のハードウェアを装備し、CA およびインフラストラクチャ システム ソフトウェアのバックアップを維持します。さらに、CA の秘密鍵は本 CPS セクション 6.2.4 に従って災害復旧を目的としてバックアップされ、維持されます。

シマンテックは、STN CA に加え、シマンテック サブドメイン内のサービス センターおよびエンタープライズ カスタマの CA についても、重要な CA 情報のバックアップをオフサイトで維持します。かかる情報には、証明書申請データ、監査データ (本 CPS セクション 4.5 による)、および発行されたすべての証明書のデータベース レコードを含みますが、これらに限定されません。

### *5.8 CA または RA の終了*

STN CA またはエンタープライズ カスタマの CA が、その運用を停止する必要がある場合、シマンテックは、CA の終了に先立ち、商業上合理的な努力を尽くして、利用者、依拠当事者、および影響を受ける他のエンティティに対し、かかる終了について通知します。CA の終了が要求される場合、シマンテック、およびカスタマ CA の場合は該当カスタマが、カスタマ、利用者、および依拠当事者の混乱を最小限に抑えるための終了プランを策定します。この終了プランでは、適宜以下の事項に言及します。

- 利用者、依拠当事者、カスタマなど、終了によって影響を受ける当事者に対し、CA の状況を知らせる通知を提供すること
- 上記の通知にかかる費用に対処すること
- シマンテックにより CA に発行された証明書を失効させること
- 本 CPS で要求されている期間にわたって CA のアーカイブおよび記録を保存すること
- 利用者およびカスタマへのサポート サービスを継続すること
- CRL の発行やオンライン ステータス チェック サービスなど、失効サービスを継続すること
- 必要に応じて、エンドユーザー利用者および下位 CA の、有効期限内かつ未失効の証明書を失効させること

- 終了プランまたは規定に基づいて、有効期限内かつ未失効の証明書が失効した利用者については、必要に応じて払い戻しを行うこと。または、業務を引き継ぐ CA によって代替証明書が発行されること
- CA の秘密鍵およびその秘密鍵を含むハードウェア トークンを処分すること
- 業務を引き継ぐ CA に 当該 CA のサービスを移行するために必要な規定を定めること

### *5.9 データ セキュリティ*

EV SSL 証明書、EV コードサイニング証明書、およびドメイン認証/組織認証の SSL 証明書の発行について、シマンテックは、STN の追加手続きとして、付録 B1、付録 C、および付録 D で規定されている CA/ブラウザ フォーラムのデータ セキュリティに関する要件に準拠します。

# 6. 技術的セキュリティ制御

## *6.1 鍵ペアの生成およびインストール*

### 6.1.1 鍵ペアの生成

CA 鍵ペアの生成は、事前に選考され訓練を受けた複数の信頼される個人により、生成される鍵にセキュリティと要求される暗号強度を提供する信頼できるシステムとプロセスを使用して実行されます。PCA および発行元ルート CA の場合、鍵生成に使用される暗号化モジュールは、FIPS 140-1 レベル 3 の要件を満たします。それら以外の CA (STN CA および Managed PKI カスタマの CA を含む) の場合、使用される暗号化モジュールは最低限 FIPS 140-1 レベル 2 の要件を満たします。

CA の鍵ペアはすべて、『Key Ceremony Reference Guide』、『CA Key Management Tool User's Guide』、および『Symantec SAR Guide』の要件に従い、事前に計画された鍵生成セレモニーにおいて生成されます。それぞれの鍵生成セレモニーにおいて実行された作業は記録され、日付が付され、関わったすべての個人により署名されます。これらの記録は、シマンテックの経営陣が適当であるとみなす期間にわたって、監査および追跡調査の目的で保持されます。

RA 鍵ペアの生成は、通常、ブラウザ ソフトウェアとともに提供される FIPS 140-1 レベル 1 認定の暗号化モジュールを使用して RA により実行されます。

エンタープライズ カスタマは、自身の自動承認サーバーで使用される鍵ペアを生成します。シマンテックでは、自動承認サーバーの鍵ペアの生成については、FIPS 140-1 レベル 2 認定の暗号化モジュールを使用して実行することを推奨しています。

エンドユーザー利用者の鍵ペアの生成は、通常、当該利用者によって実行されます。Class 1 証明書、Class 2 証明書、および Class 3 コード/オブジェクト サイニング証明書の場合、利用者は通常、ブラウザ ソフトウェアとともに鍵生成のために提供される FIPS140-1 レベル 1 認定の暗号化モジュールを使用します。サーバー証明書の場合、利用者は通常、Web サーバー ソフトウェアとともに提供される鍵生成ユーティリティを使用します。

ACS アプリケーション ID の場合、シマンテックは、少なくとも FIPS 140-1 レベル 3 の要件を満たす暗号化モジュールで生成される乱数シードを使用して、利用者の代わりに鍵ペアを生成します。

付録 B および 付録 C に記載されている追加手続きでは、CA/ブラウザ フォーラムの要件に準拠する証明書についての追加要件を特定しています。

### 6.1.2 利用者への秘密鍵の交付

エンドユーザー利用者の鍵ペアがエンドユーザー利用者により生成される場合、利用者への秘密鍵の交付は生じません。ACS アプリケーション ID の場合も、利用者への秘密鍵の交付は生じません。

RA またはエンドユーザー利用者の鍵ペアが、シマンテックによりハードウェア トークンまたはスマートカードで事前に生成されている場合、それらデバイスは RA またはエンドユーザー利用者に対し、商用配送サービスを使用して不正開封防止機能を施した上で配布されます。デバイスをアクティベーションするために必要なデータは、そのデバイスの配布とは別の方法により、RA またはエンドユーザー利用者に渡されます。デバイスの配布については、シマンテックによってログに記録されます。

エンドユーザー利用者の鍵ペアが、エンタープライズ カスタマによりハードウェア トークンまたはスマートカードで事前に生成されている場合、それらデバイスはエンドユーザー利用者に対し、商用配送サービスを使用して不正開封防止機能を施した上で配布されます。デバイスをアクティベーションするために必要なデータは、そのデバイスの配布とは別の方法により、RA またはエンドユーザー利用者に渡されます。デバイスの配布については、エンタープライズ カスタマによってログに記録されます。

鍵復元サービスのために Managed PKI Key Manager を使用するエンタープライズ カスタマの場合、かかるカスタマは (自らが承認する証明書申請を行った利用者に代わり) 暗号用鍵ペアを生成し、パスワードで保護された PKCS #12 ファイルを使用して当該鍵ペアを利用者に送信できます。

### 6.1.3 証明書発行者への公開鍵の交付

エンドユーザー利用者および RA は、PKCS#10 の証明書署名要求 (CSR) を使用するか、それ以外の Secure Sockets Layer (SSL) によって保護されたセッションで電子署名されたパッケージを使用して、自身の公開鍵を電子的にシマンテックに提供して認証を受けます。CA、RA、またはエンドユーザー利用者の鍵ペアがシマンテックにより生成される場合、本要件は適用されません。

### 6.1.4 依拠当事者への CA 公開鍵の交付

シマンテックは、その PCA およびルート CA の CA 証明書を、Web ブラウザ ソフトウェアに組み込むことにより、利用者および依拠当事者が利用できるようにします。新規の PCA およびルート CA の証明書が生成される場合、シマンテックは、ブラウザの最新のリリース版およびアップデート版に組み込んでもらうために、その新規証明書をブラウザの製造業者に提供します。

シマンテックは、通常、証明書チェーン全体 (発行 CA およびチェーン内のすべての CA を含む) を、証明書の発行時にエンドユーザー利用者に提供します。STN CA 証明書は、LDAP ディレクトリ (*directory.verisign.com*[23]) からもダウンロードできます。

### 6.1.5 鍵サイズ

鍵ペアは、予定使用期間においては、暗号解読技術を使用して鍵ペアの秘密鍵が他者に解かれないように十分な長さにするものとします。最小鍵サイズについてのシマンテック標準は、PCA と CA の場合、2048 ビットの RSA と同等の強度を持つ鍵ペアを使用することです[24]。以下の表では、シマンテックのルート鍵ペアと強度を示しています。

---

[23] Symantec Japan, Inc. または VeriSign Japan K.K. が発行する STN CA の証明書は LDAP ディレクトリ (directory.verisign.co.jp)からダウンロードできます。

[24] シマンテックは、標準の Web ブラウザ以外のクライアント ソフトウェアで使用されることが意図された、最小数 (未公表) の SSL サーバー証明書を発行する権利を有します。これらの証明書には、クリティカル EKU エクステンションが含まれますが、それには serverAuth フラグは設定されず、標準 Web ブラウザにおいて使用されるべきでないことを示す 2.16.840.1.113733.1.8.54.1 の特別なフラグが設定されます。

| 公開鍵アルゴリズム | 署名<br>アルゴリズム | クラス | 世代 |
|---|---|---|---|
| 2048 ビット RSA | SHA1 | Class 1、2、3 PCA | G3 PCA |
| | | Class 3 PCA | G5 PCA |
| | SHA256 | Class 1、2、および Class 3 Universal Root PCA | G6 PCA |
| 384 ビット ECC | SHA384 | Class 1、2、3* PCA | G4 PCA |
| 4096 ビット RSA | SHA384 | Class 3 PCA | G6 PCA |
| 2048_256 ビット DSA | SHA256 | Class 1、2、3 PCA | G7 PCA |
| * Class 3 の第四世代 (G4) ルートには、ベリサイン ブランドのもの (旧) と シマンテック ブランドのものの 2 つが存在します。 | | | |

**表:シマンテックのルート CA と鍵サイズ**

STN PCA と CA のすべてのクラス、RA、およびエンドエンティティ証明書では、電子署名ハッシュ アルゴリズムに SHA-2 が使用されます。また、特定バージョンのシマンテック プロセッシング センターでは、エンドエンティティ利用者証明書においてハッシュ アルゴリズムとして SHA-256 と SHA-384 の使用をサポートしています。 SHA-1 は、SSL と EV コードサイニング証明書を除いた古いアプリケーションまたはユースケースで使われる可能性があります。これらの利用は CA/ブラウザ フォーラムや関連するアプリケーションソフトウェア提供者の定める手順およびポリシーに反しません。

#### 6.1.5.1 鍵サイズに関する CA/ブラウザ フォーラム要件

EV SSL 証明書、EV コードサイニング証明書、およびドメイン認証/組織認証の SSL 証明書は、STN の追加手続きとして、付録 B1、付録 C、および付録 D で規定されている CA/ブラウザ フォーラムの要件に準拠します。[25]

シマンテックのルート CA 証明書は、アルゴリズム タイプと鍵サイズに関する以下の要件を満たします。

| | 有効期間の始まりが<br>2010 年 12 月 31 日<br>またはそれ以前の場合 | 有効期間の始まりが<br>2010 年 12 月 31 日よりも後の場合 |
|---|---|---|
| ダイジェスト アルゴリズム | MD5 (非推奨)<br>SHA-1 、SHA-256 、SHA-384 、または SHA-512 | SHA-1* 、SHA-256 、SHA-384 、または SHA-512 |
| 最小 RSA 係数サイズ (ビット) | 2048** | 2048 |
| 最小 DSA 係数サイズ (ビット) | 適用外 | 2048 |
| ECC 曲線 | NIST P-256、P-384、または P-521 | NIST P-256、P-384、または P-521 |

**表 4A – ルート CA 証明書のアルゴリズムと鍵サイズ**

[25] 非標準の鍵ペアと 2048 ビット未満の鍵サイズを使用する STN 証明書は、特定のグループまたは閉鎖的なエコ システム内で使用される場合に承認されます。

シマンテックの下位 CA 証明書は、アルゴリズム タイプと鍵サイズに関する以下の要件を満たします。

| | 有効期間の始まりが<br>2010 年 12 月 31 日<br>またはそれ以前で、<br>終わりが 2013 年 12 月 31 日<br>またはそれ以前の場合 | 有効期間の始まりが<br>2010 年 12 月 31 日よりも後で<br>終わりが 2013 年 12 月 31 日よりも<br>後の場合 |
|---|---|---|
| ダイジェスト アルゴリズム | SHA-1、SHA-256、SHA-384、または SHA-512 | SHA-1*、SHA-256、SHA-384、または SHA-512 |
| 最小 RSA 係数サイズ (ビット) | 1024 | 2048 |
| 最小 DSA 係数サイズ (ビット) | 2048 | 2048 |
| ECC 曲線 | NIST P-256、P-384、または P-521 | NIST P-256、P-384、または P-521 |

**表 4B – 下位 CA 証明書のアルゴリズムと鍵サイズ**

シマンテック CA は、以下のアルゴリズム タイプと鍵サイズの鍵を使用する利用者証明書のみを発行するものとします。

| | 有効期間の終わりが<br>2013 年 12 月 31 日<br>またはそれ以前の場合 | 有効期間の終わりが<br>2013 年 12 月 31 日よりも後の場合 |
|---|---|---|
| ダイジェスト アルゴリズム | SHA-1*、SHA-256、SHA-384、または SHA-512 | SHA-1*、SHA-256、SHA-384、または SHA-512 |
| 最小 RSA 係数サイズ (ビット) | 1024 | 2048 |
| 最小 DSA 係数サイズ (ビット) | 2048 | 2048 |
| ECC 曲線 | NIST P-256、P-384、または P-521 | NIST P-256、P-384、または P-521 |

**表 4C – 利用者証明書のアルゴリズムと鍵サイズ**

* SHA-1 は、CA/ブラウザ フォーラム パブリック証明書の発行および管理に関する基本要件のセクション 7.1.3 で定義されている基準に従った RSA 鍵で使われる可能性があります。

** 2010 年 12 月 31 日よりも前に 2048 ビット未満の RSA 鍵長で発行されたルート CA 証明書は、本要件に従って発行される利用者証明書のトラスト アンカーとして引き続き機能できます。

シマンテック CA は、要求されている公開鍵が本セクションで規定されている最小アルゴリズム鍵サイズに対応していない場合に証明書要求を否認する権利があります。

### 6.1.6 公開鍵のパラメータ生成と品質検査

規定されません。

### 6.1.7 鍵用途の目的 (X.509 v3 鍵用途フィールドによる)

セクション 7.1.2.1 を参照してください。

## *6.2 秘密鍵の保護および暗号化モジュールの技術制御*

シマンテックは、シマンテックとエンタープライズ カスタマの CA 秘密鍵のセキュリティを確保するため、物理的な制御、論理的な制御、および手続き上の制御を組み合わせて実装しています。利用者は契約により、秘密鍵の紛失、漏えい、改変、または不正使用を防止するために必要な対策を講じることが要求されます。

### 6.2.1 暗号化モジュールの基準と制御

PCA および発行元ルート CA の鍵ペア生成ならびに CA 秘密鍵の保管について、シマンテックは FIPS 140-1 レベル 3 の認定を取得しているか、その要件を満たすハードウェア暗号化モジュールを使用します。 シマンテックはエンタープライズ RA 顧客が全ての RA 自動承認暗号化オペレーションを FIPS 140-1 レベル 2 以上の暗号化モジュール上で実施することを推奨します。

### 6.2.2 秘密鍵の複数人管理 (m out of n 方式)

シマンテックは、機密性の高い CA 暗号化操作において複数の信頼される個人の関与を要求する技術的/手続的な仕組みを実装しています。シマンテックは「シークレット シェアリング」という手法を使用して、CA 秘密鍵を利用するために必要とされるアクティベーション データを「シークレット シェア」と呼ばれる別々のパーツに分割し、「シェアホルダー」と呼ばれる訓練を受けた信頼される個人が保有するようにします。特定のハードウェア暗号化モジュールに関して作成/分配されたシークレット シェアの総数 (n) のうち、シークレット シェアの基準数 (m) が、当該モジュールに保管されている CA 秘密鍵をアクティベーションするために必要となります。

CA 証明書への署名に必要なシェアの基準数は、3 です。要求されるシェアの基準数に変わりはなくても、災害復旧トークンのための分配されるシェアの数は、運用トークンのために分配される数よりも少ない場合があります、シークレット シェアは、本 CPS に従って保護されます。

### 6.2.3 秘密鍵の預託

CA 秘密鍵は、預託されません。エンドユーザー利用者の秘密鍵の預託については、セクション 4.12 で詳しく説明されています。

### 6.2.4 秘密鍵のバックアップ

シマンテックは、CA 秘密鍵のバックアップ コピーを、通常の復旧および災害復旧の目的で作成します。かかる鍵は、暗号化された形式で、ハードウェア暗号化モジュール内と、関連する鍵保管デバイスに格納されます。CA 秘密鍵の保管に使用される暗号化モジュールは、本 CPS の要件を満たします。CA 秘密鍵は、本 CPS に従い、バックアップ用のハードウェア暗号化モジュールにコピーされます。

CA 秘密鍵のオンサイト バックアップ コピーを含むモジュールは、本 CPS の要件に従います。CA 秘密鍵の災害復旧用コピーを含むモジュールは、本 CPS の要件に従います。

シマンテックは、RA 秘密鍵のコピーは保管しません。エンドユーザー利用者の秘密鍵のバックアップについては、セクション 6.2.3 とセクション 4.12 を参照してください。ACS アプリケーション ID の場合、シマンテックは利用者の秘密鍵のコピーを保管しません。

### 6.2.5 秘密鍵のアーカイブ

STN CA 証明書の有効期間が満了すると、その証明書に関連付いている鍵ペアは、本 CPS の要件を満たすハードウェア暗号化モジュールを使用して、最低 5 年間は安全に保持されます。これら CA 鍵ペアは、対応する CA 証明書が本 CPS に従って更新されなければ、かかる CA 証明書の有効期間の満了に伴い、署名に使用されなくなるものとします。

シマンテックは、RA および利用者の秘密鍵のコピーはアーカイブしません。

### 6.2.6 秘密鍵の暗号化モジュールへの転送または暗号化モジュールからの転送

シマンテックは、CA 鍵ペアを、その鍵が使用されるハードウェア暗号化モジュールにおいて生成します。さらにシマンテックは、通常の復旧および災害復旧を目的としてかかる鍵ペアのコピーを作成します。CA

鍵ペアが別のハードウェア暗号モジュールにバックアップされる際には、かかる鍵ペアは暗号化された形式でモジュール間を移動します。

### 6.2.7 暗号化モジュールへの秘密鍵の格納

ハードウェア暗号化モジュールに保存される CA または RA の秘密鍵は、暗号化された形式で格納されるものとします。

### 6.2.8 秘密鍵をアクティベーションする方法

シマンテック サブドメインのすべての参加者は、自身の秘密鍵のアクティベーション データについて、紛失、盗難、改変、不法な開示、または不正使用から保護するものとします。

#### 6.2.8.1 Class 1 証明書

Class 1 秘密鍵の保護基準は、利用者が自身のワークステーションを物理的に保護するための商業上合理的な対策を講じて、利用者の承認を得ずにワークステーションおよびそれに関連付けられている秘密鍵が使用されないようにすることです。さらにシマンテックは、利用者がセクション 6.4.1 で規定されているパスワードまたはそれと同等の強度のセキュリティ対策を使用して、秘密鍵をアクティベーションする前に利用者認証を行うことを推奨しています。たとえば、秘密鍵を操作するためのパスワード、Windows ログオンまたはスクリーン セーバーのパスワード、ネットワーク ログオンのパスワードなどが該当します。

#### 6.2.8.2 Class 2 証明書

Class 2 秘密鍵の保護基準は、利用者に対して、以下の対策を施すことです。

- セクション 6.4.1 で規定されているパスワードまたはそれと同等の強度のセキュリティ対策を使用して、秘密鍵をアクティベーションする前に利用者認証を行う。たとえば、秘密鍵を操作するためのパスワード、Windows ログオンまたはスクリーン セーバーのパスワードなどが該当します。
- 利用者のワークステーションを物理的に保護するための商業上合理的な対策を施して、利用者の承認を得ずにワークステーションおよびそれに関連付けられている秘密鍵が使用されないようにする。

秘密鍵のアクティベーションを解除したときは、暗号化された形式でのみ保持されるものとします。

#### 6.2.8.3 Class 3 証明書 (管理者証明書を除く)

Class 3 秘密鍵の保護基準 (管理者を除く) は、利用者に対して、以下の対策を施すことです。

- スマートカード、生体認証アクセス対応デバイス、またはそれらと同等の強度のセキュリティ対策を使用して、秘密鍵をアクティベーションする前に利用者認証を行う。
- 利用者のワークステーションを物理的に保護するための商業上合理的な対策を施して、利用者の承認を得ずにワークステーションおよびそれに関連付けられている秘密鍵が使用されないようにする。

セクション 6.4.1 に従って、スマートカードまたは生体認証アクセス対応デバイスとともにパスワードを使用することが推奨されます。秘密鍵のアクティベーションを解除したときは、暗号化された形式でのみ保持されるものとします。

#### 6.2.8.4 管理者の秘密鍵 (Class 3)

管理者の秘密鍵の保護基準では、管理者に以下のことを要求します。

- スマートカード、生体認証アクセス対応デバイス、セクション 6.4.1 で規定されているパスワード、またはそれらと同等の強度のセキュリティ対策を使用して、秘密鍵をアクティベーションする前に管理者認証を行う。たとえば、秘密鍵を操作するためのパスワード、Windows ログオンまたはスクリーン セーバーのパスワード、ネットワーク ログオンのパスワードなどが該当します。
- 管理者のワークステーションを物理的に保護するための商業上合理的な対策を施して、管理者の承認を得ずにワークステーションおよびそれに関連付けられている秘密鍵が使用されないようにする。

技術的な制御によって事前承認されたドメインへの発行には限られない場合、シマンテックでは、アプリケーション ソフトウェア提供者がルート証明書の配布により信頼を得る証明書の発行ができる秘密鍵をアクティベーションする前に管理者認証を行い、管理者がスマートカード、生体認証アクセス対応デバイス、またはこれらと同等の強度のセキュリティをセクション 6.4.1 で規定されているパスワードとともに使用することを要求します。

秘密鍵のアクティベーションを解除したときは、暗号化された形式でのみ保持されるものとします。

#### 6.2.8.5 暗号化モジュールを使用するエンタープライズ RA (自動承認または Managed PKI Key Manager Service を使用)

暗号化モジュールを使用する管理者の秘密鍵の保護基準では、管理者に対し以下のことを要求します。

- 暗号化モジュールは、セクション 6.4.1 で規定されているパスワードとともに使用し、秘密鍵をアクティベーションする前に管理者認証を行う。
- 暗号化モジュール リーダーが備わっているワークステーションを物理的に保護するための商業上合理的な対策を施して、管理者の承認を得ずにワークステーションおよび暗号化モジュールに関連付けられている秘密鍵が使用されないようにする。

#### 6.2.8.6 プロセッシング センターに保管される秘密鍵 (Class 1 ～ 3)

オンライン CA の秘密鍵は、セクション 6.2.2 で規定されているように、そのアクティベーション データ (安全な媒体に格納される) を供給する基準数のシェアホルダーによってアクティベーションされるものとします。秘密鍵がアクティベーションされると、その秘密鍵は CA がオフラインになってアクティベーションが解除されるまでの不特定期間にわたってアクティブな状態になります。同様に、オフラインの CA の秘密鍵をアクティベーションさせるためには、アクティベーション データを供給する基準数のシェアホルダーが要求されるものとします。秘密鍵がアクティベーションされてから、その秘密鍵がアクティブになるのは 1 回限りとします。

### 6.2.9 秘密鍵のアクティベーションを解除する方法

STN CA 秘密鍵は、トークン リーダーから取り出されるとアクティベーションが解除されます。RA 秘密鍵 (RA 申請を認証するために使用されたもの) は、システムをログオフするとアクティベーションが解除されます。RA は、作業場所を離れる際に自身のワークステーションをログオフすることが要求されます。

クライアント管理者、RA、およびエンドユーザー利用者の秘密鍵は、ユーザーが採用した認証方式に応じて、操作が終わるたび、システムのログオフ時、またはスマートカード リーダーからスマートカードを取り外すときにアクティベーションを解除できます。すべての場合において、エンドユーザー利用者は、本

CPS に従って自身の秘密鍵を適切に保護する義務があります。ACS アプリケーション ID に関連付けられている秘密鍵は、コード署名で使用された後、速やかに削除されます。

### 6.2.10 秘密鍵を破壊する方法

シマンテックは、必要な場合、鍵の再生につながる残留データが残らないことを合理的に確認できる方法で CA 秘密鍵を破壊します。シマンテックは、CA 秘密鍵を完全に破壊するように、ハードウェア暗号化モジュールの初期化機能およびその他の適切な方法を活用します。CA の鍵の破壊に関する操作をする場合は立会人を置きます。ACS アプリケーション ID に関連付けられている秘密鍵は、コード署名で使用された後、速やかに削除されます。

### 6.2.11 暗号化モジュールの評価

セクション 6.2.1 を参照してください。

## *6.3 鍵ペアの管理に関するその他の事項*

### 6.3.1 公開鍵のアーカイブ

STN CA、RA、およびエンドユーザー利用者の証明書はバックアップされ、シマンテックの定期的なバックアップ手続きの一環としてアーカイブされます。

### 6.3.2 証明書の運用期間および鍵ペアの使用期間

証明書の運用期間は、その有効期間が満了になるか、失効になることで終了します。鍵ペアの運用期間は、それに関連付けられている証明書の運用期間と同じです。ただし、復号化および署名検証には鍵ペアの使用を継続できます。本 CPS の発効日以降に発行された証明書の場合、シマンテック証明書の最長運用期間は表 8 に定めるとおりです[26]。既存の利用者証明書の更新によって得られたエンドユーザー利用者証明書は、有効期間が長い場合があります (最長 3 か月)。

さらに、STN CA は、いずれかの上位 CA 証明書の有効期間が満了になった後に下位 CA が発行した証明書の有効期間が満了になる事態が起こらないように、CA の証明書の有効期間が満了になる前の適当な日(60 日に加え発行された証明書の最大有効期間)に、新規証明書の発行を停止します。

| *証明書の発行者* | *有効期間* |
|---|---|
| PCA 自己署名 (1024 ビット RSA) | 最長 30 年間 |
| PCA 自己署名 (2048 ビット RSA) | 最長 37 年間 |
| PCA 自己署名 (256 ビット ECC) | 最長 30 年間 |
| PCA 自己署名 (384 ビット ECC) | 最長 30 年間 |
| PCA からオフラインの中間 CA へ | 通常 10 年間。ただし、更新後は最長 15 年間 |
| PCA からオンラインの CA へ | 通常 5 年間。ただし、更新後は最長 10 年間[27] |
| オフラインの中間 CA から | 通常 5 年間。ただし、更新後は最長 10 年間[28] |

[26] セクション 6.3.2 で規定されている上限値を超える証明書有効期間に関する個別の例外については、シマンテックによる承認が必要です。またそのような例外は、SHA 2 または ECC アルゴリズムや 4096 ビット以上の鍵サイズなど、より強固な暗号化アルゴリズムや鍵サイズを使用する証明書に厳しく限定されています。承認制を考慮して、ハードウェア デバイスでの生成や保管など、秘密鍵の保護に関する追加要件が課せられる場合があります。

[27] Symantec Onsite Administrator CA-Class 3、Class 3 Secure Server Operational Administrator CA、および Class 3 OnSite Enterprise Administrator CA – G2 は、旧式システムのサポートのために 10 年を超える有効期間がありますが、適切な時期に失効されるものとします。

| *証明書の発行者* | *有効期間* |
|---|---|
| オンラインの CA へ | |
| オンラインの CA から<br>エンドユーザー個人利用者へ | 通常は最長 3 年間。ただし、以下の条件の下で、証明書は一回更新でき、その期間は最長 6 年間[29]。6 年経過後は新規申請が必要になります。 |
| オンラインの CA から<br>エンドエンティティ組織利用者へ | セクション 6.3.2.1 の制約の下で、通常最長 6 年間[30]。この場合、更新やリキーは選択できません。6 年経過後は新規申請が必要になります。 |

**表 8 – 証明書の運用期間**

本セクションに別段の記載がある場合を除き、シマンテック サブドメインの参加者は、鍵ペアの使用期間が終了した後は、すべての使用を中止するものとします。

エンドユーザー利用者に対して CA が発行した証明書は、以下の要件を満たす場合、3 年を越える運用期間 (最長 6 年) を有することができます。

- 組織向け証明書の運用環境に関係する利用者鍵ペアが保護され、データ センターの高度な保護が適用された中で運用されること。個人向けの証明書は、利用者の鍵ペアがスマートカードなどのハードウェア トークンに格納されること。
- セクション 3.2.3 の規定に従い、利用者は最低 3 年ごとに再認証を受けること。
- 利用者が再認証手続きを完了できない場合、または上記の要求が行われた場合にかかる秘密鍵の所持を証明できない場合、CA は利用者の証明書を失効させること。

シマンテックは、PCA によって署名されるオンライン CA である「Symantec Class 3 International Server CA」、「Thawte SGC CA」、および「Class 3 Open Financial Exchange CA」も運用します。これら CA の有効期間は、SGC および OFX の機能を提供する証明書の継続的な相互運用性を確保するため、表 8 に記載した有効期間を延長させることができます。

#### 6.3.2.1 有効期間に関する CA/ブラウザ フォーラム要件

EV SSL 証明書、EV コードサイニング証明書、およびドメイン認証/組織認証の SSL 証明書は、STN の追加手続きとして、付録 B1、付録 C、および付録 Dで規定されている CA/ブラウザ フォーラムの要件に準拠します。

### *6.4 アクティベーション データ*

### 6.4.1 アクティベーション データの生成およびインストール

STN CA 秘密鍵を含むトークンを保護するために使用されるアクティベーション データ (シークレット シェア) は、本 CPS のセクション 6.2.2 および『Key Ceremony Reference Guide』に定める要件に従って生成されます。シークレット シェアの生成および分配はログに記録されます。

---

[28] 有効期間が 6 年のエンドユーザー利用者証明書が発行される場合、オンライン CA 証明書の運用期間は、更新オプションなしで 10 年になります。5 年経過後に CA のリキーが要求されます。

[29] 有効期間が 6 年のエンドユーザー利用者証明書が発行される場合、オンライン CA 証明書の運用期間は、更新オプションなしで 10 年になります。5 年経過後に CA のリキーが要求されます。

[30]少なくとも、有効期間が 3 年を超える証明書の識別名は、証明書の発行日から 3 年経過後に再確認されます。シマンテック自動承認証明書を除き、STN の一部の運用をサポートするためだけに使用される組織用エンドエンティティ証明書に関しては、有効期間が 5 年のものを発行でき、更新後は最長 10 年とすることができます。

RA は自身の秘密鍵を保護するために強固なパスワードを選択することが要求されます。シマンテックのパスワード選択に関するガイドラインでは、パスワードに関して以下の要件を定めています。

- ユーザーが生成すること
- 15 字以上であること
- アルファベットと数字を 1 文字以上ずつ含むこと
- 小文字を 1 文字以上含むこと
- 同じ文字が多く含まれないこと
- オペレータのプロファイル名と同一でないこと
- ユーザーのプロファイル名の長い文字列が含まれないこと

シマンテックは、エンタープライズ管理者、RA、およびエンドユーザー利用者に対しても、同様の要件を満たすパスワードを選択することを強く推奨します。また、シマンテックは、秘密鍵のアクティベーションにおいて二要素認証の仕組み (トークンとパスフレーズ、生体認証とトークン、生体認証とパスフレーズなど) を使用することも推奨します。

### 6.4.2 アクティベーション データの保護

シマンテックのシェアホルダーは、所有するシークレット シェアを保護すること、およびシェアホルダーとしての責任を認識する合意書に署名することが要求されます。

RA は、その管理者/RA の秘密鍵を、パスワード保護とブラウザの「高セキュリティ」オプションを使用して、暗号化された形式で格納することが要求されます。

シマンテックは、クライアント管理者、RA、およびエンドユーザー利用者に対して、暗号化された形式で秘密鍵を格納し、ハードウェア トークンと強固なパスフレーズのいずれかまたは両方を使用して秘密鍵を保護することを強く推奨します。トークンとパスフレーズ、生体認証とトークン、生体認証とパスフレーズなど、二要素認証の仕組みを使用することが推奨されます。

### 6.4.3 アクティベーション データに関するその他の事項

#### 6.4.3.1 アクティベーション データの転送

秘密鍵のアクティベーション データが転送される場合、STN 参加者は、かかる秘密鍵の紛失、盗難、改変、不正な開示、不正な使用から保護する対策を講じて、転送を保護するものとします。エンドユーザー利用者のアクティベーション データとして、Windows またはネットワークへのログイン時のユーザー名/パスワードの組み合わせが使用される場合、ネットワーク経由で転送されるパスワードは、不正なユーザーによるアクセスから保護されるものとします。

#### 6.4.3.2 アクティベーション データの破壊

CA 秘密鍵のアクティベーション データは、かかるアクティベーション データによって保護される秘密鍵の紛失、盗難、改変、不正な開示、不正な使用から保護する対策を講じて、使用停止されるものとします。セクション 5.5.2 で規定された記録の保管期間の経過後に、シマンテックは、上書きするか物理的に破壊することで、アクティベーション データを使用停止するものとします。

## *6.5 コンピュータ セキュリティの制御*

シマンテックは、CA および RA のすべての機能を、シマンテックの『SAR Guide』の要件を満たす信頼できるシステムで遂行します。エンタープライズ カスタマは、信頼できるシステムを使用しなければなりません。

### 6.5.1 特定のコンピュータ セキュリティの技術要件

シマンテックは、CA ソフトウェアおよびデータ ファイルを保持するシステムとして、不正なアクセスから保護される「信頼できるシステム」を確保します。さらにシマンテックは、プロダクション サーバーへのアクセスを、業務上正当な理由がある個人に限定します。一般的なアプリケーション ユーザーは、プロダクション サーバーのアカウントを有しません。

シマンテックのプロダクション ネットワークは、論理的に他の部分から切り離されています。このように切り離すことで、指定のアプリケーション プロセス以外からのネットワーク アクセスを防止します。シマンテックは、ファイアウォールを使用して、内外から侵入されないようプロダクション ネットワークを保護し、プロダクション システムにアクセスするネットワーク処理の機能および発信元を制限します。

シマンテックでは、必要最低限の文字数からなる英数字と特殊文字で組み合わされたパスワードを使用するよう要求します。このパスワードを定期的に変更することもシマンテックでは要求します。

シマンテックの CA 運用をサポートしているシマンテック データベースへの直接アクセスは、シマンテックのプロダクション運用グループに属し、かかるアクセスについて業務上の正当な理由を有する信頼される者に限定されます。

#### 6.5.1.1 システム セキュリティに関する CA/ブラウザ フォーラム要件

EV SSL 証明書、EV コードサイニング証明書、およびドメイン認証/組織認証の SSL 証明書は、STN の追加手続きとして、付録 B1、付録 C、および付録 D で規定されている CA/ブラウザ フォーラムの要件に準拠します。

### 6.5.2 コンピュータ セキュリティの評価

規定されません。

## *6.6 ライフサイクルの技術的制御*

### 6.6.1 システム開発の制御

アプリケーションは、シマンテックのシステム開発および変更管理基準に従って、シマンテックが開発し、実装します。シマンテックは、エンタープライズ カスタマに対し、RA および特定の CA 機能を遂行するためのソフトウェアも提供します。かかるソフトウェアは、シマンテックのシステム開発基準に従って開発されます。

シマンテックが開発したソフトウェアは、初回ロード時に、シマンテックから提供されているシステム上の当該ソフトウェアについて、インストール前に改変されていないか、および使用予定のバージョンであるか検証する手段を提供します。

### 6.6.2 セキュリティ管理の制御

シマンテックは、その CA システムの構成を制御および監視するためのメカニズムとポリシーのいずれかまたは両方を有しています。シマンテックは、すべてのソフトウェア パッケージおよびシマンテック ソフトウェアのアップデートについて、ハッシュを作成します。このハッシュは、かかるソフトウェアの完全性を手動で検証するために使用されます。インストール時と、その後は日次で、シマンテックはその CA システムの完全性を確認します。

### 6.6.3 ライフサイクル セキュリティの制御

規定されません。

### *6.7 ネットワーク セキュリティの制御*

シマンテックは、不正なアクセスおよびその他の悪意ある活動を防止するため、『Security and Audit Requirements (SAR) Guide』に従って保護されたネットワークを使用して、シマンテックの CA および RA のすべての機能を遂行します。シマンテックは、暗号化および電子署名を使用することで、機密情報の通信を保護します。

### *6.8 タイムスタンプ*

証明書、CRL、およびその他の失効に関するデータベース エントリは、日時の情報を含むものとします。かかる時間情報については、暗号技術に基づく処理は必要とされません。

## 7. 証明書、CRL、および OCSP のプロファイル

### *7.1 証明書プロファイル*

シマンテックの証明書は、通常、(a) ITU-T (国際電気通信連合･電気通信標準化部門) による X.509 勧告 (1997 年):「Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997」、および (b) RFC 5280:「Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002」に準拠します[31]。証明書タイプに適用されるように、STN 証明書は、公的に信頼された証明書 (パブリック証明書) の発行と管理について、最新バージョンの CA/ブラウザ フォーラムの基本要件に準拠します。[32]

少なくとも X.509 証明書は、以下の表 9 に示すように、基本フィールド、および所定の規定値や値の制約事項を含みます。

| *フィールド* | *値/値の制約事項* |
|---|---|
| シリアル番号<br>(Serial Number) | CSPRNG から出力される 64 ビット以上のエントロピーを示す発行者識別名 (Issuer DN) ごとの一意の値 |
| 署名アルゴリズム<br>(Signature Algorithm) | 証明書への署名に使用されるアルゴリズムのオブジェクト識別子 (CP セクション 7.1.3 を参照) |
| 発行者識別名<br>(Issuer DN) | セクション 7.1.4 を参照 |
| 有効期間の開始<br>(Valid From) | 万国標準時を基準とする。米海軍天文台のマスター クロックに同期。RFC 5280 に従いエンコードされる |
| 有効期間の終了<br>(Valid To) | 万国標準時を基準とする。米海軍天文台のマスター クロックに同期。RFC 5280 に従いエンコードされる |
| サブジェクト識別名<br>(Subject DN) | CP セクション 7.1.4 を参照 |
| サブジェクト公開鍵 | RFC 5280 に従いエンコードされる |

[31] STN 証明書は、通常 RFC 5280 に準拠しますが、限られた特定の規定に対応しない場合があります。

[32] 鍵ペアを持ち、鍵サイズが 2048 ビット未満で、最新バージョンの CA/ブラウザ フォーラムの基本要件に準拠しない STN 証明書は、serverAuth フラグが除去されたか指定 ID (2.16.840.1.113733.1.8.54.1) を含むかのいずれかまたは両方の設定がなされています。

| *フィールド* | *値/値の制約事項* |
|---|---|
| (Subject Public Key) | |
| 署名<br>(Signature) | RFC 5280 に従い生成されエンコードされる |

**表 9 – 証明書プロファイルの基本フィールド**

### 7.1.1 バージョン番号

シマンテックの証明書は X.509 バージョン 3 の証明書ですが、特定のルート証明書については旧式のシステムをサポートするために X.509 バージョン 1 の証明書が許可されます。CA 証明書は X.509 バージョン 1 またはバージョン 3 の CA 証明書にし、エンドユーザー利用者証明書は X.509 バージョン 3 にするものとします。

### 7.1.2 証明書エクステンション

シマンテックは、X.509 バージョン 3 の STN 証明書に、セクション 7.1.2.1 ～ 7.1.2.8 で要求されるエクステンションを設定します。プライベート エクステンションは許容されますが、プライベート エクステンションの使用は、本 CPS および適用される CP において、参照という形式で明確に含まれない限り、保証の対象外です。

EV SSL 証明書のエクステンションについての要件は、本 CPS の付録 B3 に記載されています。

#### 7.1.2.1 KeyUsage

X.509 バージョン 3 証明書は、通常、RFC 5280:「Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002」に従って設定されます。KeyUsage エクステンションの重大度 (Criticality) フィールドは、通常 CA 証明書の場合は「TRUE」に設定され、エンドエンティティ利用者証明書の場合も同様です。

注:これらの証明書における nonRepudiation ビット[33]の設定は必須ではありません。PKI 業界において nonRepudiation ビットが意味するところについて意見がまだ一致していないためです。そのような意見統一がなされるまで、nonRepudiation ビットは依拠当事者になる者にとって意味あるものにならない可能性があります。さらに、一般に使用されている大分部のアプリケーションでは、必ずしも常に nonRepudiation ビットを適切に扱っているとは言えません。このため、ビットを設定することは、依拠当事者が信頼性に関して判断を下す際の助けにならないことがあります。従って、本 CPS では nonRepudiation ビットの設定は要求されません。設定されるケースとしては、Managed PKI Key Manager を使用して発行されるデュアル鍵ペアの署名証明書や、要求された場合が考えられます。電子証明書の使用に起因する否認防止に関連する争議については、利用者と依拠当事者間のみの問題となります。シマンテックは当該争議に関する一切の責任を負わないものとします。

#### 7.1.2.2 Certificate Policies エクステンション

X.509 バージョン 3 証明書の *CertificatePolicies* エクステンションは、CP セクション 7.1.6 に従って STN CP のオブジェクト識別子を含み、CP セクション 7.1.8 に規定されているポリシー修飾子が設定されます。このエクステンションの重大度 (Criticality) フィールドは、「FALSE」に設定されるものとします。

---

[33] nonRepudiation ビットは、X.509 規格に従って、電子証明書において ContentCommitment として参照される場合があります。

#### 7.1.2.2.1 Certificate Policies エクステンションに関する CA/ブラウザ フォーラム要件

EV SSL 証明書、EV コードサイニング証明書、およびドメイン認証/組織認証の SSL 証明書は、STN の追加手続きとして、付録 B1、付録 C、および付録 Dで規定されている CA/ブラウザ フォーラムの要件に準拠します。

### 7.1.2.3 Subject Alternative Names

X.509 バージョン 3 証明書の *subjectAltName* エクステンションは、RFC 5280 に従って設定されます。ただし、Public Lite アカウントで発行される証明書については、任意で *SubjectAltName* に電子メール アドレスが含まれないことがあります。このエクステンションの重大度 (Criticality) フィールドは、「FALSE」に設定されるものとします。
全ての Web サーバー証明書において、subjectAltName エクステンションには、サブジェクト DN のコモンネームの認証された値を含みます。(ドメイン名またはパブリック IP アドレス) subjectAltName エクステンションには、コモンネームと同等の認証を行った追加のドメイン名やパブリック IP アドレスを含むことがあります。

### 7.1.2.4 Basic Constraints

シマンテックの X.509 バージョン 3 の CA 証明書における *BasicConstraints* エクステンションは、CA フィールドが「TRUE」に設定されるものとします。エンドユーザー利用者証明書における *BasicConstraints* エクステンションは、CA フィールドが「FALSE」に設定されるものとします。このエクステンションの重大度 (Criticality) フィールドは、CA 証明書の場合は「TRUE」に設定されますが、エンドユーザー利用者証明書の場合は「TRUE」と「FALSE」のいずれかに設定できます。

シマンテックの X.509 バージョン 3 CA 証明書には、*BasicConstraints* エクステンションに *pathLenConstraint* フィールドがあり、認証パスにおいてこの証明書に続く中間の CA 証明書の最大数が設定されます。エンドユーザー利用者証明書を発行するオンラインのエンタープライズ カスタマに発行される CA 証明書では、「*pathLenConstraint*」フィールドがあり、認証パスにおいてエンドユーザー利用者証明書だけが続くことができることを示す「0」の値に設定されるものとします。

### 7.1.2.5 Extended Key Usage

デフォルトでは、*ExtendedKeyUsage* は重要ではないエクステンションとして設定されます。STN CA 証明書には *ExtendedKeyUsage* エクステンションは含まれません。シマンテック証明書は、アプリケーション ソフトウェア提供者がトラスト ビットを許可し、プライベート PKI ユースケースにおいて ExtendedKeyUsage エクステンションを含む可能性があります。

### 7.1.2.6 CRL Distribution Points

シマンテックのほとんどの X.509 バージョン 3 エンドユーザー利用者証明書および中間 CA 証明書には、*cRLDistributionPoints* エクステンションが含まれており、このエクステンションには依拠当事者が CA 証明書のステータスを確認するための CRL を入手できる URL が格納されます。このエクステンションの重大度 (Criticality) フィールドは、「FALSE」に設定されます。 URL は、LDAP プロトコルを除き Mozilla 要件に適合します。URL は cRLDistributionPoints エクステンションに複数含まれる可能性があります。

#### 7.1.2.7 Authority Key Identifier

シマンテックは、通常、X.509 バージョン 3 エンドユーザー利用者証明書と中間 CA 証明書の Authority Key Identifier エクステンションを設定します。証明書の発行者が Subject Key Identifier エクステンションを持つ場合、Authority Key Identifier には、当該証明書を発行する CA の公開鍵の 160 ビット SHA-1 のハッシュ値が設定されます。
それ以外の場合、Authority Key Identifier エクステンションには、発行 CA のサブジェクト識別名とシリアル番号が含まれます。このエクステンションの重大度 (Criticality) フィールドは、「FALSE」に設定されます。

#### 7.1.2.8 Subject Key Identifier

シマンテックが *subjectKeyIdentifier* エクステンションを有する X.509 バージョン 3 STN 証明書を発行する場合、当該証明書のサブジェクトの公開鍵をベースとする *keyIdentifier* は、RFC 5280 に記述されているいずれかの手法に従って生成されます。このエクステンションが使用される場合、エクステンションの重大度 (Criticality) フィールドは「FALSE」に設定されます。

### 7.1.3 アルゴリズムのオブジェクト識別子

シマンテックの証明書は、以下のいずれかのアルゴリズムを使用して署名されます。

- ***sha256withRSAEncryption*** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
- ***ecdsa-with-Sha256*** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2}
- ***ecdsa-with-Sha384*** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 3}
- ***sha-1WithRSAEncryption*** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

これらのアルゴリズムを使用して生成された証明書の署名は、RFC 3279 に準拠するものとします。*sha256WithRSAEncryption* が、*sha-1WithRSAEncryption*[34] に代わって使用されます。

### 7.1.4 名前の形式

シマンテックは、セクション 3.1.1 に従って、発行者名 (Issuer Name) およびサブジェクト識別名 (Subject Distinguished Name) を含む STN 証明書を発行します。発行される各証明書の発行者名には、発行 CA の国名 (Country)、組織名 (Organization Name)、およびコモンネーム (Common Name) が含まれます。

さらに、シマンテックは、エンドユーザー利用者証明書内に部門名 (OU) フィールドを追加し、適用される依拠当事者規約へのポインターとなる URL において証明書の使用条件が規定されていることを伝える記述を含めることができます。適用される依拠当事者規約へのポインターが、証明書の policy エクステンションに含まれない場合は、この OU が表示されなければなりません。

[34] *sha-1WithRSAEncryption* が使用されるのは、旧式アプリケーションによる業務継続を維持する目的であると事前に承認を得た場合のみです。

### 7.1.5 名前の制約

規定されません。

### 7.1.6 証明書ポリシーのオブジェクト識別子

CertificatePolicies エクステンションが使用される場合、証明書には、STN CP セクション 1.2 で規定されているように、適切な証明書クラスに対応する CertificatePolicy のオブジェクト識別子が含まれます。CertificatePolicies エクステンションを含み、STN CP の公開前に発行された古い証明書の場合、証明書は STN CPS を参照します。

#### 7.1.6.1 証明書ポリシーのオブジェクト識別子に関する CA/ブラウザ フォーラム要件

EV SSL 証明書、EV コードサイニング証明書、およびドメイン認証/組織認証の SSL 証明書は、STN の追加手続きとして、付録 B1、付録 C、および付録 D で規定されている CA/ブラウザ フォーラムの要件に準拠します。

### 7.1.7 Policy Constraints エクステンションの使用

規定されません。

### 7.1.8 ポリシー修飾子の構文と意味

シマンテックは、通常、Certificate Policies エクステンション内にポリシー修飾子を含む X.509 バージョン 3 STN 証明書を発行します。一般に、かかる証明書は、適用される依拠当事者規約または STN CPS を指定する CPS ポインター修飾子を含みます。さらに、一部の証明書は、適用される依拠当事者規約を指定する User Notice 修飾子を含みます。

### 7.1.9 クリティカルな Certificate Policies エクステンションに対する解釈方法

規定されません。

## *7.2 CRL のプロファイル*

該当する証明書タイプに対応する CRL は CA/ブラウザ フォーラム パブリック証明書の発行および管理に関する基本要件の現行バージョンに適合します。

バージョン 2 の CRL は、RFC 5280 に準拠し、以下の表 13 で規定される基本フィールドと内容を含みます。

| フィールド | 値/値の制約事項 |
|---|---|
| バージョン<br>(Version) | セクション 7.2.1 を参照。 |
| 署名アルゴリズム<br>(Signature Algorithm) | RFC 3279 に従って、CRL に署名するために使用されるアルゴリズム (CPS セクション 7.1.3 を参照)。 |
| 発行者<br>(Issuer) | CRL の署名および発行を行ったエンティティ。 |
| 発効日<br>(Effective Date) | CRL の発効日。CRL は発行と同時に有効となる。 |
| 次回更新日<br>(Next Update) | 次回の CRL の発行期限日。CRL の発行頻度は、セクション 4.9.7 の要件に従います。 |
| 失効した証明書<br>(Revoked Certificates) | 失効した証明書のリスト。失効した証明書のシリアル番号と失効日も記載されます。 |

**表 13 – CRL プロファイルの基本フィールド**

### 7.2.1 バージョン番号

シマンテックは、X.509 バージョン 1 とバージョン 2 の両方の CRL をサポートします。バージョン 2 の CRL は、RFC 5280 の要件に準拠します。

### 7.2.2 CRL および CRL エントリ エクステンション

規定されません。

## *7.3 OCSP プロファイル*

OCSP (Online Certificate Status Protocol) は、特定の証明書の失効情報を速やかに取得する手段の 1 つです。シマンテックで確認する証明書は、以下のとおりです。

- Class 2 エンタープライズ向け証明書 (RFC 2560 に準拠する エンタープライズ OCSP を使用)
- Class 2 エンタープライズ向け証明書および RFC 6960 に準拠するシマンテック TGV (Trusted Global Validation) サービスを使用する Class 3 組織向け証明書

**OCSP 署名に関する CA/ブラウザ フォーラム要件**
EV SSL 証明書、EV コードサイニング証明書、およびドメイン認証/組織認証の SSL 証明書の場合、シマンテックは STN の追加手続きとして、付録 B1 および付録 C、ならびに付録 D で規定されている OCSP 応答を提供します。

### 7.3.1 バージョン番号

RFC 2560、RFC 5019 で規定されているバージョン 1 の OCSP 仕様、および RFC 6960 がサポートされます。

### 7.3.2 OCSP エクステンション

シマンテックの TGV サービスでは、各 OCSP 応答の最新性を確立するために、セキュリティで保護されたタイムスタンプと有効期限を使用します。シマンテックでは、各 OCSP 応答の最新性の確立のために Nonce を使用しません。クライアントは Nonce を含む要求に対する応答に Nonce を含めるよう求めることはできません。クライアントはその代わりに、ローカル時刻を使用して応答の最新性を確認する必要があります。

# 8. 準拠性監査とその他の評価

セクション 1.3.1 で規定されている STN ルート CA、Class 3 組織向け CA、Class 2 組織向けおよび個人向け CA、および Class 1 個人向け CA を含む、シマンテックのパブリックおよび Managed PKI Service をサポートしているシマンテックのデータ センター運用/鍵管理運用に関しては、WebTrust for Certification Authorities v2.0 以降による調査が年 1 回行われます。Symantec Japan Inc.のパブリック CA の外部監査は WebTrust for Certification Authorities ではなく ISAE3402/SSAE16 で実施します。シマンテックは、エンタープライズ カスタマに対し、本 CPS に基づく準拠性監査およびこれらのカスタマ タイプに応じた監査プログラムを受けることを要求する権利があるものとします。

準拠性監査に加えて、シマンテックは、STN のシマンテック サブドメインの信頼性を確保するために、それ以外の審査および調査も実施できる権利があるものとします。これには、以下の項目を含みますが、これらに限定されません。

- 関連会社のセキュリティおよびプラクティス レビューによってオペレーションの開始を許可します。セキュリティおよびプラクティス レビューは関連会社がSTN標準に適合することを保証するために関連会社施設のセキュリティ、セキュリティ文書、CPS、STN 関連の合意、プライバシーポリシー、認証計画のレビューを含みます。
- シマンテックは、監査対象エンティティについて、「STN スタンダードを満たしていない」、「事故または危殆化が生じた」、もしくは「STN のセキュリティ/完全性を現実的または潜在的に脅かすような作為または不作為があった」と確信できる理由がある場合には、自らの判断により、いつでも自分自身、関連会社またはエンタープライズ カスタマに「緊急監査/調査」を実施する権利があるものとします。
- シマンテックは、準拠性監査において不完全または例外的な結果が発見された場合、または通常業務の過程での全体的リスク管理プロセスの一環として、カスタマについて「追加リスク マネジメント レビュー」を行う権利があるものとします。

シマンテックは、これらの監査、審査、および調査を第三者の監査法人に対し委任する権利があるものとします。監査/審査/調査の対象であるエンティティは、シマンテックおよび監査/審査/調査を行う要員に対し、相応の協力を行うものとします。

**内部監査に関する CA/ブラウザ フォーラム要件**

EV SSL 証明書、EV コードサイニング証明書、およびドメイン認証/組織認証の SSL 証明書の場合、シマンテックは、STN の追加手続きとして、付録 B1 および付録 C、ならびに付録 D で規定されている内部監査を実施するものとします。

### *8.1 評価の頻度と状況*

準拠性監査は、監査対象エンティティの費用負担により、少なくとも年 1 回実施されます。1 回の監査期間は 1 年未満とし、監査の空白期間が生じないように実施されます。

### *8.2 評価人の識別情報/資格*

シマンテックの CA の準拠性監査は、以下のような会計事務所により実施されます。

- WebTrust for Certification Authorities v2.0 以降を実施できる能力を証明すること。
- 公開鍵インフラストラクチャ技術、情報セキュリティに関するツールと技術、セキュリティ監査、および第三者証明の職務に深い知識を有すること。
- 米国公認会計士協会 (AICPA) から認定されていること。この認定を受けるには、特定技術の保有、専門家同士の審査などの品質保証対策、能力テスト、業務に対する適正なスタッフの配置に関する基準、および継続的な専門教育が要求されます。
- 法律、政府による規制、または職業倫理に拘束されること。
- 補償限度額が最低 100 万米ドル以上の業務上過失損害賠償保険/過失怠慢賠償責任保険を維持していること。

### *8.3 評価者と評価対象エンティティの関係*

シマンテックの運用についての準拠性監査は、シマンテックとは無関係の会計事務所によって実施されます。

### *8.4 評価対象項目*

シマンテックが実施する年 1 回の WebTrust for Certification Authorities (またはこれと同等のもの)の監査範囲は、CA の環境統制、鍵管理の運用、インフラストラクチャ/管理 CA の制御、証明書ライフサイクル管理、および CA 業務に関する情報開示を含みます。

**登録局の監査(Class 1-2)**
エンタープライズ カスタマが承認する Class1 と 2 の証明書は年次監査を受ける可能性があります。シマンテックおよび、または上位組織(上位組織がシマンテックでない場合)の要請によって、エンタープライズ カスタマは STN ポリシーに対するいかなる例外や違反行為は記録し、違反行為の改善をする可能性があります。

**登録局の監査(Class 3)**
エンタープライズ カスタマが発行を認証する Class 3 SSL 証明書は STN の責務のもと年次監査を受けます。シマンテックおよび、または上位組織(上位組織がシマンテックでない場合)の要請によって、エンタープライズ カスタマは STN ポリシーに対するいかなる例外や違反行為は記録し、違反行為の改善をします。

**シマンテックまたは関連会社の監査(Class 1-3)**
シマンテックおよびそれぞれの関連会社は、受託会社の持つリスクに関して米国公認会計士協会の Statement on Service Organizations Control (SOC)報告書により提供されるガイドラインに従い鑑査されます。適合監査は認証局のための WebTrust 監査またはシマンテックが承認した同等の監査標準です。承認した監査には運用ポリシーと手順および運用有効性のテストに関する報告書が含まれます。

### *8.5 不備の結果として取られる処置*

シマンテックの運用に関する準拠性監査に関して、準拠性監査時に重大な例外または不備が指摘された場合は、取るべき処置が判断されることになります。この判断は、監査人から指摘を受けて、シマンテック経営陣が行います。シマンテック経営陣は、是正措置の策定および実施について責任を負います。シマンテックが、かかる例外または不備により STN のセキュリティもしくは完全性に対して直接的な脅威がもたらされると判断した場合には、是正措置が 30 日以内に策定され、商業上合理的な期間内に実施されます。これよりも深刻度の低い例外または不備の場合、シマンテックの経営陣は、当該事項の重要性を評価し、適切な措置を判断します。

### *8.6 結果の連絡*

シマンテックは、年次の監査報告書を、監査期間終了後 3 か月以内に公表します。3 か月を超える遅れが生じる場合には、認定監査人の署名入りの説明文書が提示されるものとします。シマンテックの WebTrust for CA 監査報告書は、 *www.symantec.com/about/profile/policies/repository.jsp* で確認できます。

## 9. 業務および法律に関するその他の事項

### *9.1 料金*

#### 9.1.1 証明書の発行または更新の手数料

シマンテックは、エンドユーザー利用者に対し、証明書の発行、管理、および更新に関する手数料を請求する権利を有します。

### 9.1.2 証明書アクセスの手数料

シマンテックは、証明書をリポジトリで利用できるようにするか、または他の方法によって依拠当事者が証明書を利用できるようにする対価としての手数料を請求しません。

### 9.1.3 失効またはステータス情報へのアクセスの手数料

シマンテックは、CP で要求されている CRL をリポジトリで利用できるようにするか、または他の方法によって依拠当事者が利用できるようにする対価としての手数料を請求しません。ただし、シマンテックは、カスタマイズされた CRL、OCSP サービス、またはその他の付加価値のある失効およびステータス情報サービスを提供する場合については手数料を請求する権利を有します。シマンテックは、シマンテックの書面による事前の明示的な同意なしで、証明書ステータス情報を利用した製品またはサービスを提供する第三者に対し、失効情報、証明書ステータス情報、リポジトリ内のタイムスタンプへのアクセスを許可しません。

### 9.1.4 その他のサービスの手数料

シマンテックは、本 CPS へのアクセスに関する手数料を請求しません。複製、再配布、変更、派生的文書の作成など、文書の単純な閲覧以外を目的とした利用については、当該文書の著作権を有するエンティティと使用許諾契約を締結するものとします。

### 9.1.5 返金に関するポリシー

シマンテック サブドメイン内では、以下の返金ポリシー (掲載先: *www.symantec.com/about/profile/policies/repository.jsp*) が適用されます。

シマンテックは、証明書の業務運用および証明書の発行において、厳格な手続きとポリシーを厳守し、これを支持します。しかしながら、いかなる理由でも、利用者が自身に発行された証明書について十分な満足を得られない場合、利用者はシマンテックに対して、発行から 30 日以内に証明書を失効させること、および利用者に返金することを要求できます。当初の 30 日間が過ぎた後でも、利用者または利用者の証明書に関して本 CPS または NetSure (sm) プロテクション プランに基づく保証またはその他の重大な義務にシマンテックが違反した場合には、利用者はシマンテックに対して、証明書を失効させ、返金するよう要求できます。シマンテックは、利用者の証明書を失効させた後、速やかに、証明書に支払われた該当料金の全額を、証明書の料金がクレジット カードで支払われた場合は利用者のクレジット カードに返金し、そうでなければ小切手で利用者に返金します。返金を要求する場合は、カスタマ サービス (+1 650 426-3400) に問い合わせてください。この返金ポリシーは、唯一の救済方法ではなく、利用者が利用できる他の救済方法を制限するものでもありません。

## *9.2 財務上の責任*

### 9.2.1 保険の範囲

エンタープライズ カスタマは、保険会社の過失および怠慢に関する賠償責任保険プログラム、または自家保険を利用して、商業上合理的な水準の過失怠慢賠償責任保険を維持することが推奨されます。シマンテックは、かかる過失怠慢賠償責任保険を維持します。

### 9.2.2 その他の資産

エンタープライズ カスタマは、業務継続と任務遂行をまかなうための十分な財源を有するものとし、利用者および依拠当事者に対して合理的な範囲で賠償責任のリスクを負うことができなければなりません。シマンテックの財務状況は、*http://investor.symantec.com/phoenix.zhtml?c=89422&p=irol-irhome* で公開されている開示情報に記載されています。

### 9.2.3 拡張される保証範囲

NetSure プロテクション プランは、シマンテック SSL 証明書およびコードサイニング証明書の利用者に向けて、シマンテックの証明書発行時の不備が原因で生じる紛失/損害、またはシマンテックの過失もしくは契約上の義務違反によって引き起こされるその他の不正行為に対する保護を提供するための、拡張された保証プログラムです。ただし、証明書の利用者が、適用されるサービス規約の義務を果たしている場合に限ります。NetSure プロテクション プランに関する一般情報、および対象となる証明書については、*www.symantec.com/about/profile/policies/repository.jsp* を参照してください。

## *9.3 業務情報の機密保持*

### 9.3.1 機密情報の範囲

利用者の以下の記録については、セクション 9.3.2 に従い、機密性およびプライバシーを保持するものとします (以下、「機密/個人情報」)。

- CA 申請記録 (承認、不承認を問わない)
- 証明書申請記録
- Managed PKI Key Manager を使用してエンタープライズ カスタマが保有する秘密鍵、およびかかる秘密鍵の復元に必要な情報
- 処理記録 (処理の全記録および監査証跡の両方を含む)
- シマンテックまたはカスタマにより生成または保有される監査証跡の記録
- シマンテックまたはカスタマ、もしくはそれぞれの監査人 (内部監査人か外部監査人かを問わない) により作成された監査報告書 (かかる報告書が保持されている場合)
- 緊急時対応プランおよび災害復旧プラン
- シマンテックのハードウェア/ソフトウェアの運用、および証明書サービス/所定の申請サービスの管理を制御するセキュリティ対策

### 9.3.2 機密情報の範囲に含まれない情報

証明書、証明書の失効およびその他のステータス情報、シマンテックのリポジトリおよびそれに含まれている情報は、機密/個人情報とはみなされません。セクション 9.3.1 に基づいて明示的に機密/個人情報にみなされる情報以外は、機密情報でも個人情報でもないものとします。このセクションは、適用される個人情報保護法規に従います。

### 9.3.3 機密情報の保護責任

シマンテックは、第三者に漏えいおよび開示されないよう機密情報を保護します。

## *9.4 個人情報のプライバシー保護*

### 9.4.1 プライバシー プラン

シマンテックは、CP セクション 9.4.1 に従って、プライバシー ポリシーを導入し、*www.symantec.com/about/profile/privacypolicy/index.jsp*[35] で公開しています。

### 9.4.2 個人情報として取り扱う情報

発行された証明書の記載内容、証明書ディレクトリ、およびオンラインの CRL で公開されていない利用者に関する情報はすべて、個人情報として取り扱われます。

---

[35] 日本語版のプライバシー プランは以下で公開しています。
http://www.symantec.com/ja/jp/about/profile/policies/privacy.jsp.

### 9.4.3 個人情報としてみなされない情報

現地の法律に従うことを条件として、証明書で公開される情報はすべて個人情報とはみなされません。

### 9.4.4 個人情報の保護責任

シマンテックと関連会社は、個人情報が第三者に漏えいおよび開示されないよう保護するとともに、自身の所在地の個人情報保護法規に全面的に従うものとします。

### 9.4.5 個人情報の利用に関する通知および同意

本 CPS、適用されるプライバシー ポリシー、または規約に別段の定めがない限り、個人情報はその情報が該当する当事者の同意がなければ利用されません。
このセクションは、適用される個人情報保護法規に従います。

### 9.4.6 司法手続きまたは行政手続きによる開示

シマンテックは、シマンテックが以下に相当すると誠意を持って確信する場合、機密/個人情報を開示する権限を有するものとします。

- 召喚令状および捜索令状に対して、情報開示が必要な場合
- 召喚令状、質問書、事実認否要求、文書提出要求など、民事および行政上の措置における開示制度 (ディカバリー プロセス) に際し、司法、行政、その他の法的な手続きに対して、情報開示が必要な場合

このセクションは、適用される個人情報保護法規に従います。

### 9.4.7 その他の情報開示に関する状況

規定されません。

## *9.5 知的財産権*

利用者および依拠当事者を除く、シマンテック サブドメイン参加者間での知的財産権の帰属は、そのシマンテック サブドメイン参加者間で適用される契約に準拠します。セクション 9.5 の以下のサブセクションは、利用者と依拠当事者に関係する知的財産権に適用されます。

### 9.5.1 証明書および失効情報に関する財産権

CA は、自身が発行する証明書および失効情報に付帯するすべての知的財産権を留保します。シマンテックおよびカスタマは、完全な複製が行われ、かつ証明書で参照される依拠当事者規約に従って証明書が使用される場合に限り、非独占的かつ無償という条件で証明書の複製および配布を許可します。シマンテックおよびカスタマは、適用される CRL 利用規約、依拠当事者規約、およびその他適用されるあらゆる規約に従い、依拠当事者の役割を果たすために失効情報を使用することを許可するものとします。

### 9.5.2 CPS に関する財産権

STN 参加者は、シマンテックが本 CPS に付帯するすべての知的財産権を留保することを認めます。

### 9.5.3 名称に関する財産権

証明書申請者は、証明書申請に含まれる商標、サービス マーク、または商号に関する権利 (ある場合)、およびかかる証明書申請者に発行される証明書内の識別名に関する権利をすべて留保します。

### 9.5.4 鍵および鍵情報に関する財産権

CA およびエンドユーザー利用者の証明書に対応する鍵ペアは、これらの証明書それぞれのサブジェクトとなっている CA およびエンドユーザー利用者に帰属し、Managed PKI Key Manager を使用するエンタープライズ カスタマの権利に従い、それらが保管および保護されている物理的媒体に関係なく、かかる者がこれらの鍵ペアに付帯するすべての知的財産権を留保します。上記の一般性を制限することなく、シマンテックのルート公開鍵およびそれを含むルート証明書については、すべての PCA 公開鍵および自己署名証明書を含めて、シマンテックに帰属します。シマンテックは、ソフトウェアおよびハードウェアのメーカーに対し、当該ルート証明書を複製し、信頼できるハードウェア デバイスまたはソフトウェアにコピーを置く権利を付与します。最終的に、CA の秘密鍵のシークレット シェアは CA に帰属し、CA は、シマンテックからシークレット シェアまたは CA を物理的に所持することができない場合でも、かかるシークレット シェアに付帯するすべての知的財産権を留保します。

## *9.6 表明と保証*

### 9.6.1 CA の表明と保証

シマンテックは、以下の事項を保証します。

- 証明書には、証明書申請の承認または証明書の発行を行うエンティティに知られている、またはエンティティに起因する重大な不実表示がないこと
- 証明書内の情報には、証明書申請の承認または証明書の発行を行うエンティティが、証明書申請の管理または証明書の作成を実行する際に相応の注意を払わなかったことが原因で生じた誤りがないこと
- 証明書が 本 CPS の重大なすべての要件を満たしていること
- 失効サービスおよびリポジトリの使用が、重大なすべての面において、適用される CPS に準拠していること

利用規約でさらなる表明と保証を定めることができます。

#### 9.6.1.1 保証と義務に関する CA/ブラウザ フォーラム要件

EV SSL 証明書、EV コードサイニング証明書、およびドメイン認証/組織認証の SSL 証明書は、STN の追加手続きとして、付録 B1 および付録 C、ならびに付録 Dに記載されている CA/ブラウザ フォーラムの要件に準拠します。

### 9.6.2 RA の表明と保証

RA は、以下の事項を保証します。

- 証明書には、証明書申請の承認または証明書の発行を行うエンティティに知られている、またはエンティティに起因する重大な不実表示がないこと
- 証明書内の情報には、証明書申請の承認を行うエンティティが、証明書申請の管理を実行する際に相応の注意を払わなかったことが原因で生じた誤りがないこと
- 証明書が 本 CPS の重大なすべての要件を満たしていること
- 失効サービス (該当する場合) およびリポジトリの使用が、重大なすべての面において、適用される CPS に準拠していること

利用規約でさらなる表明と保証を定めることができます。

### 9.6.3 利用者の表明と保証

利用者は、以下の事項を保証します。

- 証明書に記載される公開鍵に対応する秘密鍵を使用して生成される各電子署名が、利用者の電子署名であり、電子署名が生成される時点で証明書が受領され、運用可能である (有効期限内であり、かつ失効されていない) こと
- 利用者の秘密鍵は保護されており、権限を付与された者以外から利用者の秘密鍵にアクセスしたことがないこと
- 利用者が提出した証明書申請において、利用者が表明したことがすべて真実であること
- 利用者が提供し、証明書に記載されたすべての情報が真実であること
- 証明書が正当で合法的な目的のためにのみ使用されており、かつ本 CPS に従っていること
- 利用者がエンドユーザー利用者であって CA ではないこと。また、証明書に記載された公開鍵に対応する秘密鍵を、CA であるかどうかを問わず、いかなる証明書 (または公開鍵を証明するその他の形式) または CRL に電子署名する目的で使用していないこと

利用規約でさらなる表明と保証を定めることができます。

### 9.6.4 依拠当事者の表明と保証

依拠当事者規約では依拠当事者に対して、証明書内の情報で依拠すべき範囲を決定するために依拠当事者が必要十分な情報を得ていること、かかる情報を依拠するかどうかを決定することに関して依拠当事者のみが責任を負うこと、および本 CPS で規定されている依拠当事者の義務の履行を怠った結果についての法的責任を依拠当事者が負うものとすることを認めることを要求します。

依拠当事者規約でさらなる表明と保証を定めることができます。

### 9.6.5 その他の参加者の表明と保証

規定されません。

## *9.7 保証の否認*

適用される法律で許可される限り、利用規約および依拠当事者規約は、商品性または特定目的への適合性に関するあらゆる保証を含め、NetSure プロテクション プランの対象範囲外では、シマンテックの一切の保証を否認するものとします。

## *9.8 責任の制限*

シマンテックが証明書ポリシーおよび認証業務運用規程に準拠して証明書を発行し、発行管理する限り、シマンテックは利用者、いかなる依拠当事者、あるいはその他いかなる第三者機関がかかる証明書を利用または依拠することで生じた損害や損失に関して、一切の賠償責任を負わないものとします。適用される法律で許可される限り、利用規約および依拠当事者規約は、NetSure プロテクション プランの対象範囲外で、シマンテックの賠償責任を制限するものとします。賠償責任の制限には、間接的、特別、付随的、および派生的に生じた損害の免責が含まれるものとします。また、利用規約および依拠当事者規約は、特定の証明書についてシマンテックが負担する損害賠償額の上限が以下のとおりであることを含むものとします。

| クラス | 損害賠償額の上限 |
|---|---|
| **Class 1** | 100 米ドル ($ 100.00 US) |
| **Class 2** | 5,000 米ドル ($ 5,000.00 US) |
| **Class 3** | 100,000 米ドル ($ 100,000.00 US) |

**表 14 – 損害賠償額の上限**

表 14 に定める損害賠償額の上限は、NetSure プロテクション プランの対象範囲外で回収可能な損害額に制限します。NetSure プロテクション プランに基づく支払額は、当該プランの損害賠償額の上限が適用されます。各種証明書に関する NetSure プロテクション プランに基づく損害賠償額の上限は、10,000 米ドルから 1,750,000 米ドルの範囲にわたります。 NetSure プロテクション プランの詳細については、www.symantec.com/about/profile/policies/repository.jsp を参照してください。

利用者の賠償責任 (とその制限の両方またはいずれか) は、適用される利用規約で規定されるものとします。

エンタープライズ RA および該当する CA の賠償責任 (とその制限の両方またはいずれか) は、両者間の契約で定められるものとします。

依拠当事者の賠償責任 (とその制限の両方またはいずれか) は、適用される依拠当事規約で規定されるものとします。

EV 証明書に対するシマンテックの賠償責任の制限は、本 CPS の付録 B1 にも記述されています。

## *9.9 補償*

### 9.9.1 利用者による補償

適用される法律で許可される限り、利用者は以下の事由による損害について、シマンテックに補償することを要求されます。

- 利用者の証明書申請において利用者が虚偽または不実の表明を行った場合
- 利用者が証明書申請において重大な事実を開示することを怠った場合で、不実の表明または怠慢が過失でなされたか、当事者を欺く意図を持ってなされたとき
- 利用者が利用者の秘密鍵の保護、信頼できるシステムの使用、またはその他利用者の秘密鍵の危殆化、紛失、開示、改変、または不正使用を防ぐために必要な予防策を講じることを怠った場合
- 利用者が第三者の知的財産権を侵害するような名称 (コモンネーム、ドメイン名、または電子メール アドレスを含むがこれらに限定されない) を使用した場合

適用される利用規約には、追加の補償義務を含めることができます。

### 9.9.2 依拠当事者による補償

適用される法律で許可される限り、依拠当事者規約では依拠当事者に対し、以下の事由による損害について、シマンテックに補償することを要求されます。

- 依拠当事者が依拠当事者としての義務の履行を怠った場合
- 依拠当事者による証明書の依拠が特定の状況において合理的でない場合
- 依拠当事者が、証明書について有効期限が満了しているか失効されているかどうかを判断するために証明書のステータスを確認することを怠った場合

適用される依拠当事者規約には、追加の補償義務を含めることができます。

### 9.9.3 アプリケーション ソフトウェア サプライヤの補償

利用者および依拠当事者への賠償責任のいかなる制限にもかかわらず、シマンテック ルート CA との間でルート証明書配布契約を締結しているアプリケーション ソフトウェア サプライヤが、本要件に基づく、または証明書の発行/保守、あるいは依拠当事者またはその他の者による依拠を理由として存在する可能性がある、CA のいかなる義務または潜在的賠償責任を負わないことを CA は理解し、同意します。

したがって、CA は、CA によって発行された証明書に関連してかかるアプリケーション ソフトウェア サプライヤが被るいかなる申し立て、損害、および損失について、その訴因または法的根拠にかかわらず、かかるアプリケーション ソフトウェア サプライヤを擁護し、補償し、免責するものとします。ただし、アプリケーション ソフトウェア サプライヤのソフトウェアで、有効期限を過ぎていない証明書を信頼できないものとして表示したことによって、または (1) 有効期限を過ぎた証明書、あるいは (2) 失効した証明書 (ただし、失効ステータスを現在 CA がオンラインで公開しており、アプリケーション ソフトウェアがかかるステータスをチェックしなかったか、失効ステータスの表示を無視した場合のみ) を信頼できると表示したことによって申し立て、損害、または損失が直接引き起こされた場合には、CA によって発行された証明書に関連してかかるアプリケーション ソフト ウェアサプライヤが被った申し立て、損害、または損失に関して、上記は適用されません。

## *9.10 有効期間と終了*

### 9.10.1 有効期間

本 CPS は、シマンテックのリポジトリに公開されたときに有効になります。本 CPS の改定も、シマンテックのリポジトリに公開されたときに有効になります。

### 9.10.2 終了

本 CPS は随時改定されますが、新しいバージョンの CPS に差し替えられるまで、効力を有するものとします。

### 9.10.3 終了の効果と効力の残存

本 CPS が終了した場合においても、シマンテック サブドメインの参加者は、発行されたすべての証明書について、当該証明書の残存有効期間中は本 CPS の条項に拘束されます。

## *9.11 参加者への個別の通知と連絡*

当事者間の契約による別段の指定がない限り、シマンテック サブドメインの参加者は、連絡事項の重大性と内容に配慮しながら、相互に連絡を取り合うために商業上合理的な方法を使用するものとします。

## *9.12 改定*

### 9.12.1 改定手続き

本 CPS の改定は、シマンテック PMA (Policy Management Authority) が行うことができます。改定は、CPS の改定部分を含めた文書の形式か、更新部分を示す形式のいずれかの方法で行われるものとします。改定版または更新通知は、シマンテック リポジトリの [Practices Updates and Notices] セクション (www.symantec.com/about/profile/policies/repository.jsp) に掲載されるものとします。更新事項は、参照バージョンの CPS の指定された条項または矛盾する条項に優先します。PMA は、CPS に変更を加えることで、証明書の各クラスに対応している証明書ポリシーのオブジェクト識別子にも変更が必要かどうかを判断するものとします。

### 9.12.2 通知方法と期間

シマンテックおよび PMA は、誤植の訂正、URL の変更、および連絡先の変更を含むがこれらに限定されない重大ではない改定については、改定に関する通知を行わずに、本 CPS を改定する権利を留保します。改定内容が重大かどうかを指定する PMA の決定は、PMA の単独の判断によるものとします。

CPS の改定案は、シマンテック リポジトリの [Practices Updates and Notices] セクション (www.symantec.com/about/profile/policies/repository.jsp) に掲載されるものとします。

PMA は、他のシマンテック サブドメイン参加者に対して CPS の改定案を求めます。提案された改定が望ましいことを PMA が認め、改定の実施を提案する場合、PMA はこのセクションに従って、かかる改定の通知を提供するものとします。

それとは反対に、本 CPS の定めにかかわらず、PMA が STN またはその一部のセキュリティ侵害を停止または防止するために、直ちに本 CPS の重大な改定を行うことが必要であると確信する場合には、シマンテックおよび PMA はシマンテック リポジトリに公開することにより、かかる改定を行う権限を有するものとします。かかる改定は、公開と同時に直ちに効力を有します。シマンテックは、公開してから妥当な時間内に、かかる改定について関連会社に通知するものとします。

シマンテックと PMA は、CA/ブラウザ フォーラムのガイドラインに従い、本 CPS を少なくとも年次で更新します。

#### 9.12.2.1 意見期間

他に定められた場合を除き、本 CPS の重大なあらゆる改定について意見を求める期間は、かかる改定案がシマンテック リポジトリに掲載された日から 15 日間に設定するものとします。シマンテック サブドメイン参加者は誰でも、意見期間が終わるまで、PMA に意見を提出できるものとします。

#### 9.12.2.2 意見の取り扱い方

PMA は、改定案に対するすべての意見について検討するものとします。PMA は、(a) 改定案を修正なしで有効にする、(b) 改定案を修正し、必要な場合は、新たな改定案として再公開する、(c) 改定案を撤回する、のいずれかの対応をとるものとします。PMA は、関連会社に通知し、さらにシマンテック リポジトリの [Practices Updates and Notices] セクションに通知を掲載することで、改定案を撤回する権限を有します。改定案が修正または撤回されない限り、かかる改定案は意見期間の満了をもって有効になるものとします。

### 9.12.3 OID の変更が必要な場合

PMA が証明書ポリシーに対応するオブジェクト識別子において変更が必要であると判断する場合は、改定内容に、証明書の各クラスに対応する証明書ポリシーの新しいオブジェクト識別子を含めるものとします。そうでない場合は、改定内容として、証明書ポリシーのオブジェクト識別子の変更を要求しないものとします。

## *9.13 紛争の解決*

### 9.13.1 シマンテック、関連会社、カスタマ間の紛争

シマンテック サブドメイン参加者間の紛争は、当事者間に適用される契約の規定に従って解決されるものとします。

### 9.13.2 エンドユーザー利用者または依拠当事者との紛争

適用される法律で許可される限り、利用規約および依拠当事者規約には、紛争解決に関する条項を含めるものとします。シマンテックが関与する紛争では、最初に 60 日間の交渉期間を経てから、米国居住者が原告の場合は、カリフォルニア州サンタクララ郡を管轄する連邦裁判所または州立裁判所で訴訟が行われることが要求されます。また、原告が米国居住者ではない場合は、シマンテックによって別途承

認されたものがない限り、国際商工会議所 (ICC) による調停および仲裁の規則に従って、ICC が仲裁を行うことが要求されます。

### *9.14 準拠法*

適用される法律で定められている制限に従い、本 CPS の執行力、構造、解釈、および有効性については、契約またはその他の法選択の規定にかかわらず、また米国カリフォルニア州における商業的な関連を確立する必要なく、米国カリフォルニア州法に準拠するものとします。この法選択は、STN 参加者すべての手続きおよび解釈を確実に統一させるために、当該参加者の居住地に関係なく行われます。

上記の準拠法規定は、本 CPS のみに適用されます。本 CPS を参照という形式で組み込んでいる契約は、独自の準拠法に関する規定を定めることができます。ただし、かかる契約のその他の規定とは別に、適用される法律上の制限に従い、本 CPS の条項の執行力、構造、解釈、および有効性は、本セクション 9.14 に準拠します。

本 CPS は、ソフトウェア、ハードウェア、または技術情報の輸出入における制約を含むがこれに限定されない、適用される国内/州/地域/外国法、規則、規定、条例、法令、および命令に従います。

### *9.15 適用される法の遵守*

本 CPS は、ソフトウェア、ハードウェア、または技術情報の輸出入における制約を含むがこれに限定されない、適用される国内/州/地域/外国法、規則、規定、条例、法令、および命令に従います。証明書の発行に関して、該当管轄地の法律によって認可が要求される場合、シマンテックは、CA に対し、業務を行う各管轄地において CA として認可します。

### *9.16 雑則*

#### 9.16.1 完全合意

規定されません。

#### 9.16.2 権利譲渡

規定されません。

#### 9.16.3 分離可能性

本 CPS の条項または規定が裁判所またはその他権限のある行政機関によって執行不可能であると判断された場合でも、その他の条項または規定は有効なままとします。

#### 9.16.4 強制執行 (弁護士費用と権利放棄)

規定されません。

#### 9.16.5 不可抗力

適用される法律で許可される限り、利用規約および依拠当事者規約には、シマンテックを保護する不可抗力条項を含むものとします。

### *9.17 その他の条項*

規定されません。

# 付録 A: 頭字語･定義表

## *頭字語表*

| 用語 | 定義 |
|---|---|
| ***AICPA*** | American Institute of Certified Public Accountants (米国公認会計士協会) |
| ***ANSI*** | The American National Standards Institute (米国規格協会) |
| ***ACS*** | Authenticated Content Signing (認証コンテンツ署名) |
| ***BIS*** | The United States Bureau of Industry and Science of the United States Department of Commerce (米国商務省産業安全保障局) |
| ***CA*** | Certification Authority (認証機関) |
| ***ccTLD*** | Country Code Top-Level Domain (国別コード トップレベル ドメイン) |
| ***CICA*** | Canadian Instituted of Chartered Accountants (カナダ公認会計士協会) |
| ***CP*** | Certificate Policy (証明書ポリシー) |
| ***CPS*** | Certification Practice Statement (認証業務運用規程) |
| ***CRL*** | Certificate Revocation List (証明書失効リスト) |
| ***CSPRNG*** | Cryptographically Secure Pseudo-Random Number Generator(暗号論的擬似乱数生成器) |
| ***DBA*** | Doing Business As (事業名) |
| ***DNS*** | Domain Name System (ドメイン ネーム システム) |
| ***EV*** | Extended Validation (拡張認証) |
| ***FIPS*** | United State Federal Information Processing Standards (連邦情報処理規格) |
| ***FQDN*** | Fully Qualified Domain Name (完全修飾ドメイン名) |
| ***ICC*** | International Chamber of Commerce (国際商工会議所) |
| ***IM*** | Instant Messaging (インスタント メッセージ) |
| ***IANA*** | Internet Assigned Numbers Authority (インターネット番号割当て機関) |
| ***ICANN*** | Internet Corporation for Assigned Names and Numbers (インターネットの名前および数値割り当てのための機関) |
| ***ISO*** | International Organization for Standardization (国際標準化機構) |
| ***KRB*** | Key Recovery Block (キー リカバリ ブロック) |
| ***LSVA*** | Logical security vulnerability assessment (論理的なセキ ュリティ脆弱性評価) |
| ***NIST*** | (US Government) National Institute of Standards and Technology (米国立標準技術研究所) |
| ***OCSP*** | Online Certificate Status Protocol |
| ***OID*** | Object Identifier (オブジェクト識別子) |
| ***PCA*** | Primary Certification Authority (プライマリ認証機関) |
| ***PIN*** | Personal identification number (個人識別番号) |
| ***PKCS*** | Public-Key Cryptography Standard (公開鍵暗号標準) |
| ***PKI*** | Public Key Infrastructure (公開鍵基盤) |
| ***PMA*** | Policy Management Authority (ポリシー管理機関) |
| ***QGIS*** | Qualified Government Information Source (行政機関の信頼情報源) |
| ***QIIS*** | Qualified Independent Information Source (第三者機関の信頼情報源) |
| ***RA*** | Registration Authority (登録機関) |
| ***RFC*** | Request for comment (意見募集) |
| ***SAR*** | Security Audit Requirements (セキュリティ監査要件) |
| ***S/MIME*** | Secure multipurpose Internet mail extensions (セキュリティで保護された多目的インターネット メール拡張子) |
| ***SSL*** | Secure Sockets Layer (セキュア ソケット レイヤー) |
| ***STN*** | Symantec Trust Network (シマンテック トラスト ネットワーク) |
| ***TLD*** | Top-Level Domain (トップレベル ドメイン) |
| ***TLS*** | Transport Layer Security (トランスポート レイヤー セキュリティ) |

## *定義*

| 用語 | 定義 |
|---|---|
| ***管理者*** ***(Administrator)*** | プロセッシング センター、サービス センター、Managed PKI カスタマ、または Gateway カスタマの組織内で、検証その他 CA または RA の役割を果たす信頼される者。 |
| ***管理者証明書*** ***(Administrator Certificate)*** | 管理者に発行される証明書で、CA または RA としての機能を果たすためにのみ利用できるもの。 |
| ***関連会社*** ***(Affiliate)*** | 技術、通信、金融サービスなどの業界において、ある特定の地域において STN の配布およびサービス チャネルになるためにシマンテックと契約を締結している一流の信頼される第三者。<br>CA/ブラウザ フォーラムの文書では、「*関連会社 (Affiliate)*」という用語について、次のように定義しています。別のエンティティを支配する、別のエンティティによって支配される、または別のエンティティと共通の支配権の下にある企業、共同経営会社、共同事業、またはその他のエンティティ、あるいは行政機関の直接的な支配権の下で運営されている機関、部署、下位行政機関、または任意のエンティティ。 |
| ***Affiliate Practices Legal Requirements Guidebook*** | 関連会社の CPS、規約、認証手続き、およびプライバシー ポリシーの要件について、関連会社が満たさなければならない他の要件とともに規定されたシマンテックの文書。 |
| ***関連する個人*** ***(Affiliated Individual)*** | Managed PKI カスタマ、Managed PKI ライト カスタマ、Gateway カスタマのエンティティとして関連する個人。(i) 役員、取締役、従業員、パートナー、業務請負人、インターンまたは、当該エンティティ内部の者、(ii) 利害関係のあるシマンテック登録コミュニティ メンバー、(iii) 当該エンティティと関係があり、当該エンティティがその者の識別情報について適切な保証をすることができる取引その他の記録がある者。 |
| ***申請者*** ***(Applicant)*** | それをサブジェクトとして指定する EV 証明書の申請 (または更新要求) を行う民間組織または政府機関。 |
| ***申請権限者*** ***(Applicant Representative)*** | EV 証明書の申請者が雇用した個人で、(i) 申請者に代わって EV 証明書要求に署名して提出する、または承認する、または (ii) 申請者に代わって利用規約に署名して提出する者。 |
| ***アプリケーション ソフトウェア ベンダー*** ***(Application Software Vendor)*** | 証明書を表示または使用し、ルート証明書を配布するインターネット ブラウザ ソフトウェアまたはその他のソフトウェアの開発元 (KDE、Microsoft Corporation、Mozilla Corporation、Opera Software ASA、Red Hat, Inc. など)。 |
| ***申請者*** ***(Applicant)*** | 証明書を申請 (またはその更新を要求) する自然人または法人。証明書が発行されると、申請者は利用者と呼ばれるようになります。デバイスに発行される証明書の場合、実際の証明書要求を送信しているのがデバイスである場合でも、申請者は証明書に指定されたデバイスを管理または運用するエンティティとなります。 |
| ***申請権限者*** ***(Applicant Representative)*** | 申請者本人、申請者に雇用された者、または承認を受けて申請者の代理となる権限があると表明する代理人であり、(i) 申請者に代わって証明書要求に署名して提出する、または承認する、(ii) 申請者に代わって利用規約に署名して提出する、または (iii) 申請者が CA の関連会社である場合に、申請者に代わって証明書使用条件を認めて同意する自然人または保証人。 |
| ***アプリケーション ソフトウェア サプライヤ*** ***(Application Software Supplier)*** | 証明書を表示または使用し、ルート証明書を組み込むインターネット ブラウザ ソフトウェアまたはその他の依拠当事者のアプリケーション ソフトウェアのサプライヤ。 |
| ***証明書*** ***(Attestation Letter)*** | 会計士、弁護士、政府職員、または当該情報について習慣的に依拠されるその他の信頼できる第三者によって記述された、サブジェクト情報が正しいものであることを証明する証書。 |
| ***監査報告書*** ***(Audit Report)*** | エンティティのプロセスおよび管理が、本要件の必須条項に従っているかどうかについての公認監査人の意見を述べた、公認監査人からの報告書。 |
| ***自動承認*** ***(Automated Administration)*** | 申請情報がデータベースにある情報と一致する場合、証明書の申請が自動的に承認される手続き。 |
| ***自動承認ソフトウェア モジュール*** ***(Automated Administration Software Module)*** | 自動承認を行うシマンテック提供ソフトウェア。 |
| ***証明書*** ***(Certificate)*** | 少なくとも、CA の名称を記載するか CA を識別し、利用者を識別し、利用者の公開鍵を含み、証明書の運用期間を識別し、証明書のシリアル番号を含み、そして CA によって電子署名されたメッセージ。 |
| ***証明書申請者*** ***(Certificate Applicant)*** | CA による証明書発行を要求する個人または組織。 |
| ***証明書申請*** ***(Certificate Application)*** | 証明書申請者 (または証明書申請者の委任代理人) から CA に対して証明書の発行を求める要求。 |
| ***証明書承認者*** ***(Certificate Approver)*** | □申請者に雇われた自然人、または EV 証明書申請者を代表して (i) 証明書要求者として行動し、他の従業員または第三者に証明書要求者としての権限を与え、(ii) 他の申請書要求者が提出する EV 証明書要求を承認するための明示的な権限を有する代理人である自然人。 |
| ***証明書チェーン*** ***(Certificate Chain)*** | エンドユーザー利用者証明書および CA 証明書を含む、一連の証明書リストのこと。ルート証明書で終了となります。 |
| ***証明書データ*** | CA の所有または管理下にある、あるいは CA がアクセスできる証明書要求およびそれに関連するデータ |

| 用語 | 定義 |
|---|---|
| ***(Certificate Data)*** | (申請者から取得したかどうかを問いません)。 |
| ***証明書管理の統制対象 (Certificate Management Control Objectives)*** | 準拠性監査に対応するために、エンティティが満たさなければならない基準。 |
| ***証明書管理プロセス (Certificate Management Process)*** | 鍵、ソフトウェア、およびハードウェアの使用に関連付けられるプロセス、運用、および手順。これに基づいて、CA は証明書データの検証、証明書の発行、リポジトリの保持、証明書の失効を行います。 |
| ***証明書ポリシー (Certificate Policies、CP)*** | 「シマンテック トラスト ネットワーク証明書ポリシー」と呼ばれる、STN を統制する主要な方針を記載している文書。 |
| ***証明書問題の報告 (Certificate Problem Report)*** | 鍵の危殆化、証明書の不正使用、または証明書に関連するその他の種類の詐欺、危殆化、不正使用、あるいは不適切な行為の疑いの申し立て。 |
| ***証明書要求者 (Certificate Requester)*** | 申請者に雇われて権限を与えられた自然人、または申請者を代表するための明示的な権限を有する代理人、または申請者の代理として EV 証明書要求を作成および提出する第三者 (ISP、ホスティング会社など)。 |
| ***証明書失効リスト (Certificate Revocation List、CRL)*** | CP セクション 3.4 に従って、有効期間満了前に失効した証明書を特定する目的で、CA によって電子署名され、定期的に (または緊急に) 発行されるリスト。このリストは、通常、CRL 発行者の名前、発行日、次回 CRL 発行予定日、失効した証明書のシリアル番号、具体的な時刻、および失効理由を示します。 |
| ***証明書署名要求 (Certificate Signing Request)*** | 証明書を発行させるための要求を伝えるメッセージ。 |
| ***認証機関 (Certification Authority、CA)*** | STN において、証明書を発行、管理、失効、および更新する権限を付与されたエンティティ。 |
| ***認証業務運用規程 (Certification Practice Statement、CPS)*** | シマンテックまたは関連会社が証明書申請の承認/否認、および証明書の発行/管理/失効を行う際に採用する運用手続きを規定した文書。Managed PKI カスタマおよび Gateway カスタマは、採用するよう要求されます。 |
| ***チャレンジ フレーズ (Challenge Phrase)*** | 証明書申請の際に、証明書申請者が選択する秘密のフレーズ。証明書が発行されると、証明書申請者は利用者になり、利用者が利用者証明書の失効または更新を求めるときに、CA または RA はその利用者を認証するためにチャレンジ フレーズを使用できます。 |
| ***クラス (Class)*** | CP 内で定義されているように、保証レベルを特定するもの。CP セクション 1.1.1 を参照。 |
| ***クライアント サービス センター (Client Service Center)*** | コンシューマー、または企業の事業部門で、クライアント証明書を提供している関連会社 (サービス センター)。 |
| ***準拠性監査 (Compliance Audit)*** | プロセッシング センター、サービス センター、Managed PKI カスタマ、または Gateway カスタマがそれぞれに適用される STN スタンダードに適合しているかどうかを判断するために受ける定期的な監査。 |
| ***危殆化 (Compromise)*** | セキュリティ ポリシーに違反した (またはその疑いのある) 行為で、機密情報の不正開示または制御不能が生じた可能性があること。秘密鍵における危殆化は、紛失、盗難、開示、改変、不正使用、または当該秘密鍵のその他のセキュリティが危険にさらされることを意味する。 |
| ***機密/個人情報 (Confidential/Private Information)*** | CP セクション 2.8.1 に従って、機密および秘密にすることを要求される情報。 |
| ***契約書署名者 (Contract Signer)*** | 申請者に雇われた自然人、または申請者を代表するための明示的な権限を有し、EV 証明書の申請者の代理として利用規約に署名する権限を与えられた代理人。 |
| ***国 (Country)*** | 本ガイドラインで定義される主権国家を意味します。 |
| ***CRL 利用規約 (CRL Usage Agreement)*** | CRL または CRL に記載の情報を使用するための諸条件を定めている規約。 |
| ***クロス証明書 (Cross Certificate)*** | 2 つのルート CA 間の信頼関係を確立するために使用される証明書。 |
| ***カスタマ (Customer)*** | Managed PKI カスタマまたは Gateway カスタマである組織。 |
| ***暗号論的擬似乱数生成器 (Cryptographically Secure Pseudo-Random Number Generator)*** | 暗号技術で利用するための擬似乱数を発生させるための機器。 |
| ***委譲先の第三者 (Delegated Third Party)*** | CA ではないが、本書に定められた 1 つ以上の CA 要件を履行または充足することにより証明書管理プロセスを支援することを、CA によって承認されている自然人または法人。 |
| ***要求払い預金口座 (Demand Deposit Account)*** | 銀行その他の金融機関の預金口座。この口座に預け入れた資金は、要求に応じて払い戻されます。要求払い預金口座は、小切手、銀行為替手形、自動引き落とし、電子送金などの手段による現金不要の支払いの推進を主たる目的とします。利用状況は国により異なりますが、要求払い預金口座は、当座預金勘定、シェアドラフト勘定、または経常勘定として一般的に知られています。 |

| 用語 | 定義 |
|---|---|
| | |
| ***ドメイン認証*** ***(Domain Authorization)*** | 特定のドメイン ネームスペースに関する証明書を要求する権限を申請者が有することを証明するために、ドメイン名登録者によって提供される信書または他の文書。 |
| ***ドメイン名*** ***(Domain Name)*** | ドメイン ネーム システムでノードに割り当てられるラベル。 |
| ***ドメイン ネームスペース*** ***(Domain Namespace)*** | ドメイン ネーム システム内の単一ノードに従属することが可能なすべてのドメイン名のセット。 |
| ***ドメイン名登録者*** ***(Domain Name Registrant)*** | ドメイン名の「所有者」を表すこともあるが、正しくは、ドメイン名の使用方法を管理する権利を有するとしてドメイン名登録機関に登録された人物またはエンティティ (WHOIS またはドメイン名登録機関によって「登録者」として掲載されている自然人や法人など)。 |
| ***ドメイン名登録機関*** ***(Domain Name Registrar)*** | (i) Internet Corporation for Assigned Names and Numbers (ICANN)、(ii) 国内のドメイン名機関/レジストリ、または (iii) Network Information Center (その関連会社、下請業者、代理人、後継者、譲受人を含む) の援助または合意によって、ドメイン名を登録する者またはエンティティ。 |
| ***エンタープライズ サービス センターとしての事業*** ***(Enterprise, as in Enterprise Service Center)*** | 関連会社が Managed PKI カスタマに対して Managed PKI Service を提供するために開始する事業。 |
| ***エンタープライズ EV 証明書*** ***(Enterprise EV Certificate)*** | Managed PKI for SSL カスタマがシマンテックに対して、シマンテックによる審査済みのドメインを含む第 3 以上のドメイン レベルで発行することを許可する EV 証明書。 |
| ***エンタープライズ*** ***(Enterprise RA)*** | CA/ブラウザ フォーラムのガイドラインの要件に従い、最初の EV 証明書に記載されているシマンテック認証済みのドメインを含む第 3 以上のドメインレベルのドメインに関して、シマンテック認証済みのドメインおよび組織の有効な EV 証明書を複数要求できる Managed PKI for SSL カスタマ。 |
| ***有効期限日*** ***(Expiry Date)*** | 証明書の有効期間の最終日を定義する、証明書内の「有効期間の終了」の日付。 |
| ***EV 証明書*** ***(EV Certificate)*** | EV ガイドラインに指定される情報を含み、そのガイドラインに従って検証される電子証明書。 |
| ***EV OID*** | 「オブジェクト識別子」と呼ばれる識別番号であり、EV 証明書の *certificatePolicies* フィールドに含まれている。この識別子により、(i) その証明書に関連する CA ポリシー ステートメントが示され、また (ii) 1 社以上のアプリケーション ソフトウェア ベンダーとの事前合意により、証明書が EV 証明書としてマーク付けされます。 |
| ***緊急監査/調査*** ***(Exigent Audit/Investigation)*** | エンティティが STN スタンダードに従っていない、エンティティに関係する事故または危殆化が発生した、またはエンティティによって STN のセキュリティが実際に脅威にさらされたもしくはその可能性があると確信できる理由がある場合に、シマンテックが行う監査または調査。 |
| ***拡張認証*** ***(Extended Validation)*** | 主要認証機関とブラウザ ベンダーにより構成されているフォーラムで公開された EV 証明書に関するガイドラインで定義された審査手続き。 |
| ***完全修飾ドメイン名*** ***(Fully-Qualified Domain Name)*** | インターネット ドメイン ネーム システム内のすべての上位ノードのラベルを含むドメイン名。 |
| ***行政機関*** ***(Government Entity)*** | 国またはかかる国における下位の行政区分 (州、市、郡など) の政府が運営する法人、機関、部署、省庁、支部、または同様の要素。 |
| ***知的財産権*** ***(Intellectual Property Rights)*** | 著作権、特許権、企業秘密、商標、およびその他の知的財産権に基づく権利。 |
| ***中間 CA*** ***(Intermediate Certification Authority、Intermediate CA)*** | 証明書チェーン内で、ルート CA の証明書と、エンドユーザー利用者証明書を発行した認証機関の証明書の間に位置する証明書を発行する認証機関。 |
| ***内部名*** ***(Internal Name)*** | 証明書のコモンネームまたは SubjectAlternativeName フィールドに含まれる文字列(IP アドレスではない)で、IANA の Root Zone データベースにトップレベルドメインとして登録されているもので終わっていないため、証明書の発行時点においてパブリック DNS で世界で唯一のものと確認できないもの。 |
| ***国際組織*** ***(International Organization)*** | 2 か国以上の政府またはその代理により署名された制定文書 (憲章、条約、協定、または同等の文書) により設立される組織。 |
| ***発行 CA*** ***(Issuing CA)*** | 特定の証明書に関連して、証明書を発行した CA。ルート CA または下位 CA の場合もあります。 |
| ***鍵の危殆化*** ***(Key Compromise)*** | 秘密鍵は、その値が権限のない人物に開示された場合、権限のない人物がアクセスした場合、または権限のない人物がその値を検出できる実用的な手法が存在する場合に、危殆化したと見なされます。 |
| ***鍵ペア生成セレモニー*** ***(Key Generation Ceremony)*** | CA または RA の鍵ペアの生成、秘密鍵の暗号モジュールへの転送、秘密鍵のバックアップ、公開鍵の認証を組み合わせた手続き、またはいずれかの手続き。 |
| ***鍵生成スクリプト*** | CA 鍵ペアの生成の手続きが記述された計画書。 |

| 用語 | 定義 |
|---|---|
| ***(Key Generation Script)*** | |
| ***Key Manager 管理者 (Key Manager Administrator)*** | Managed PKI Key Manager を使用する Managed PKI カスタマにおいて、鍵の生成と復元の職務を負う管理者。 |
| ***鍵ペア (Key Pair)*** | 秘密鍵とそれに関連付けられた公開鍵。 |
| ***キー リカバリ ブロック (Key Recovery Block、KRB)*** | 暗号鍵を利用して暗号化された利用者秘密鍵を含むデータ構造。KRB は PKI Key Manager ソフトウェアを使用して生成される。 |
| ***鍵復元サービス (Key Recovery Service)*** | Managed PKI カスタマが Managed PKI Key Manager を使用して利用者の秘密鍵を復元する際に、キーリカバリ ブロックの復元に必要な暗号鍵を提供するシマンテックのサービス。 |
| ***法人 (Legal Entity)*** | 国の法律制度に則った組織、企業、共同経営会社、事業体、トラスト、行政機関、またはその他のエンティティ。 |
| ***Managed PKI*** | シマンテックのエンタープライズ カスタマおよび関連会社が、個人（従業員、パートナー、サプライヤー、カスタマなど）およびデバイス（サーバー、ルーター、ファイアウォールなど）に証明書を配布できるようにするシマンテックの完全統合型マネージド PKI サービス。Managed PKI により、エンタープライズ カスタマは、メッセージ、イントラネット[36]、エクストラネット、仮想プライベート ネットワーク、および電子商取引のアプリケーションを保護できるようになります。 |
| ***Managed PKI 管理者 (Managed PKI Administrator)*** | Managed PKI カスタマのために認証その他 RA の役割を果たす管理者。 |
| ***Managed PKI コントロール センター (Managed PKI Control Center )*** | Managed PKI 管理者が証明書申請を手動認証できるようにする Web ベースのインターフェース。 |
| ***Managed PKI Key Manager*** | 特別な Managed PKI 契約に基づき、鍵復旧機能の実装を選択した Managed PKI カスタマのための鍵復元ソリューション。 |
| ***Managed PKI Key Management Service 管理者ガイド (Managed PKI Key Management Service Administrator's Guide)*** | Managed PKI Key Manager を使用する Managed PKI カスタマのため運用要件および手続きを規定する文書。 |
| ***手動承認 (Manual Authentication)*** | 管理者が Web ベースのインターフェイスを使用して証明書申請を 1 件ずつ手動で審査し、承認する手続き。 |
| ***NetSure プロテクション プラン (NetSure Protection Plan)*** | CP セクション 9.2.3 に規定されている拡張保証プログラム。 |
| ***確認を実施しない利用者情報 (Nonverified Subscriber Information)*** | 証明書申請者から CA または RA に送信された情報で、証明書に含まれるが、当該 CA または RA が確認していないもの。当該 CA および RA は、情報が証明書申請者から送信されたものであるという事実以外は何ら保証しない。 |
| ***否認防止 (Non-repudiation)*** | 通信の発信元、通信が送信されたこと、および通信が到達したことを不当に否認された場合に、主体に対する防護策を提供する通信属性。通信の発信元の否認には、過去の 1 件以上の連続メッセージと同じ送信元からの通信を否認することも含みます。これは、送信者に関連付いている認証情報が不明な場合でも同様です。注:最終的には、裁判所による裁定、仲裁、または他の裁決機関のみが否認を防止できます。たとえば、STN 証明書を参照して認証される電子署名は、裁判所による否認防止かどうかの判断をサポートする証拠を提供できますが、電子署名自体が否認防止をもたらすわけではありません。 |
| ***オブジェクト識別子 (Object Identifier) (オブジェクト識別子)*** | 特定のオブジェクトまたはオブジェクト クラスに適用される国際標準化機構 (ISO) の標準に従って登録された一意の英数字または数字の識別子。 |
| ***OCSP (Online Certificate Status Protocol)*** | オンラインの証明書チェック プロトコルであり、依拠当事者に対してリアルタイムで証明書ステータス情報を提供する。 |
| ***OCSP レスポンダ (OCSP Responder)*** | CA の権限の下で運用され、証明書のステータス要求の処理のためにリポジトリに接続されているオンライン サーバー。<br>「Online Certificate Status Protocol」も参照してください。 |
| ***オフライン CA (Offline CA)*** | ネットワーク経由の侵入者による予期される攻撃から保護するために、セキュリティ上の理由でオフラインにて保全される STN PCA、発行元ルート CA、および他の特定の中間 CA。これらの CA はエンドユーザー利用者証明書を直接署名しません。 |
| ***オンライン CA*** | エンドユーザー利用者証明書を署名する CA であり、署名サービスを継続して提供するためにオンラインに |

[36] subjectAlternativeName エクステンションやサブジェクトのコモンネームに予約済み IP アドレスか内部的な名前を持つ SSL/コードサイニング証明書の利用は、CA/ブラウザ フォーラムによって禁止され、2016 年 10 月までに排除されます。施行日の後に発行されたそのような証明書は、2015 年 11 月 1 日より前に有効期限を迎えなければなりません。2016 年 10 月 1 日以降の有効期限を持つ発行済みの証明書は、2016 年 10 月 1 日で失効されます。

| 用語 | 定義 |
|---|---|
| ***(Online CA)*** | て保全される。 |
| ***OCSP (Online Certificate Status Protocol)*** | 依拠当事者に対してリアルタイムで証明書ステータス情報を提供するためのプロトコル。 |
| ***運用期間 (Operational Period)*** | 証明書が発行された日時 (証明書にそれより後の日時の記載がある場合にはその記載された日時) に始まり、当該証明書の有効期間が終了する日時 (それ以前に失効した場合にはその失効日時) に終了する期間。 |
| ***親会社 (Parent Company)*** | 子会社の過半数を所有する会社。QIIS の参照よって、または登録されている Chartered Professional Accountant (CPA) あるいは米国外では同様の組織によって提供された財務報告によって確認できます。 |
| ***PKCS #10*** | RSA Security Inc. により開発された公開鍵暗号基準 (Public-Key Cryptography Standard) #10 であり、証明書署名要求の構造について定義している。 |
| ***PKCS #12*** | RSA Security Inc. により開発された公開鍵暗号基準 (Public-Key Cryptography Standard) #12 であり、秘密鍵の安全な転送方法について定義している。 |
| ***ポリシー管理機関 (Policy Management Authority、PMA)*** | STN 全体に本ポリシーを公表することを担当しているシマンテック内の組織。 |
| ***プライマリ認証機関 (Primary Certification Authority、PCA)*** | 特定クラスの証明書のルート CA として活動する CA。下位の CA に対して証明書を発行します。 |
| ***代表者 (Principal Individual)*** | 民間組織、行政機関、または事業体における所有者、共同経営者、経営メンバー、取締役、または役員であり、雇用の役職により識別される個人。または、かかるエンティティまたは組織により EV 証明書の要求、発行、および使用に関連する事業を許可された従業員、下請業者、または代理人。 |
| ***秘密鍵 (Private Key)*** | 鍵ペアの一方の鍵。所有者によって秘匿性が保たれ、電子署名の作成、および対応する公開鍵を使用して暗号化された電子記録またはファイルの復号の、両方またはいずれかのために使用されます。 |
| ***プロセッシング センター (Processing Center)*** | 特に証明書発行に使用される暗号化モジュールを収容するセキュアな施設を構築する組織 (シマンテックまたは特定の関連会社)。コンシューマーおよび Web サイト事業部門において、プロセッシング センターは、STN 内で CA として活動し、証明書の発行、管理、失効、および更新といった包括的な証明書ライフサイクル サービスを提供します。企業の事業部門において、プロセッシング センターは、企業自身の Managed PKI カスタマ、または下位のサービス センターの Managed PKI カスタマに代わり、証明書ライフサイクル サービスを提供します。 |
| ***公開鍵 (Public Key)*** | 鍵ペアの一方の鍵。対応する秘密鍵の所有者によって公開され、依拠当事者が使用して、所有者の対応する秘密鍵を用いて作成された電子署名を検証し、メッセージを暗号化して所有者の対応する秘密鍵を用いてのみ復号できるようにするか、そのいずれかを行います。 |
| ***公開鍵基盤 (Public Key Infrastructure、PKI)*** | 証明書ベースの公開鍵暗号システムの実施および運用を集約的にサポートするアーキテクチャ、機構、技術、業務、および手続きのこと。STN PKI は、STN の提供および実装を連携させる複数のシステムで構成されます。 |
| ***パブリック証明書 (Publicly-Trusted Certificate)*** | 広く利用可能なアプリケーション ソフトウェアで対応するルート証明書がトラスト アンカーとして配布されている事実により信頼されている証明書。 |
| ***公認監査人 (Qualified Auditor)*** | セクション 17.6 (監査人の資格) の要件を満たす自然人または法人。 |
| ***登録ドメイン名 (Registered Domain Name)*** | ドメイン名登録機関に登録されているドメイン名。 |
| ***登録機関 (Registration Agency)*** | エンティティの事業形態、または免許、設立許可、その他の認証による事業認可に関連する事業情報を登録する行政機関。登録機関には、(i) 州企業局あるいは州務長官、(ii) 認可機関 (州保険局など)、(iii) 所管機関 (金融規制、銀行業務、金融取引を監督する州政府事務所または局) あるいは連邦機関 (通貨監査局 (OCC) や貯蓄金融機関監督局 (OTC) など) を含めることができますが、これらに限定されません。 |
| ***登録機関 (Registration Authority、RA)*** | CA から承認されたエンティティであり、証明書申請者による証明書の申請をサポートするとともに、証明書申請の承認または否認、証明書の失効、証明書の更新を実行する。 |
| ***統制された金融機関 (Regulated Financial Institution)*** | 金融機関の構築および認可について定めている政府、国、州、地方自治体の法律に基づき、政府、国、州、地方自治体により規制当局の統制、監督、検査を受けている金融機関。 |
| ***信頼できる連絡手段 (Reliable Method of Communication)*** | 申請権限者以外の情報源を使用して検証された、郵便/宅配便の配送先住所、電話番号、電子メール アドレスなどの連絡方法。 |
| ***依拠当事者 (Relying Party)*** | 証明書または電子署名に依拠して行動する個人または組織。 |
| ***依拠当事者規約 (Relying Party Agreement)*** | CA により使用される規約で、個人または組織が依拠当事者として活動するための諸条件を規定するもの。 |

| 用語 | 定義 |
|---|---|
| ***リポジトリ (Repository)*** | 公開された PKI 管理文書 (証明書ポリシーや認証業務運用規程など)、および証明書ステータス情報を、CRL または OCSP レスポンスの形で含むオンライン データベース。 |
| ***リセラー (Reseller)*** | 特定の市場に対し、シマンテックまたは関連会社に代わり、サービスを販売するエンティティ。 |
| ***予約 IP アドレス (Reserved IP Address)*** | IANA が予約済みとしている IPv4 または IPv6 アドレス。<br>http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml<br>http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml |
| ***リテール証明書 (Retail Certificate)*** | CA の機能を果たすシマンテックまたは関連会社によって、Web サイトでシマンテックまたは関連会社に 1 件ずつ申請した個人または組織に対して発行される証明書。 |
| ***ルート CA (Root CA)*** | アプリケーション ソフトウェア サプライヤからルート証明書が配布され、下位 CA 証明書を発行する、最高位の認証機関。 |
| ***ルート証明書 (Root Certificate)*** | 自身を識別し、下位 CA に発行される証明書の検証を推進するために、ルート CA によって発行される自己署名証明書。 |
| ***RSA*** | Rivest 氏、Shamir 氏、Adelman 氏によって発明された公開鍵暗号方式。 |
| ***シークレット シェア (Secret Share)*** | シークレット シェアリング契約に基づく、CA 秘密鍵の一部または CA 秘密鍵を運用するために必要なアクティベーション データの一部。 |
| ***シークレット シェアリング (Secret Sharing)*** | CA 秘密鍵、または CA 秘密鍵を運用するためのアクティベーション データを分割する手続き。CP セクション 6.2.2 に基づいて CA 秘密鍵の運用を複数人の管理下に置くために行われます。 |
| ***Secure Sockets Layer (SSL)*** | Netscape Communications Corporation によって開発された Web 通信を保護するための業界標準方式。SSL セキュリティ プロトコルは、TCP/IP 接続において、データの暗号化、サーバー認証、メッセージの完全性、およびクライアント認証 (任意) を可能にします。 |
| ***Security and Audit Requirements (SAR) Guide*** | プロセッシング センターおよびサービス センターのセキュリティ/監査要件および業務を規定するシマンテックの文書。 |
| ***セキュリティおよび業務のレビュー (Security and Practices Review)*** | 関連会社が運用許可を得る際に、シマンテックが関連会社に対して行うレビュー。 |
| ***サービス センター (Service Center)*** | 特定のクラスまたはタイプの証明書発行を目的とした証明書の発行に対する証明書署名ユニットは保有せずに、プロセッシング センターに依拠しそのような証明書の発行、管理、失効、および更新を行う関連会社。 |
| ***主権国家 (Sovereign State)*** | 自らの政府を運営し、他の権力に依存したり、その支配を受けたりしない国家。 |
| ***サブドメイン (Sub-domain)*** | STN 階層内において、あるエンティティとそれより下位のすべてのエンティティの制御を受ける STN の一部。 |
| ***サブジェクト (Subject)*** | 証明書においてサブジェクトとして識別される自然人、デバイス、システム、ユニット、または法人であり、公開鍵に対応する秘密鍵の保持者。サブジェクトは、利用者、または利用者の管理および運用下にあるデバイスです。組織向け証明書の場合の「サブジェクト」は、秘密鍵を保持する機器またはデバイスを指します。サブジェクトには識別可能な名称が割り当てられ、そのサブジェクトの証明書に含まれる公開鍵と結び付けられます。 |
| ***サブジェクト識別情報 (Subject Identity Information)*** | 証明書のサブジェクトを識別する情報。サブジェクト識別情報は、subjectAltName エクステンションまたはサブジェクト コモンネーム フィールドに指定されるドメイン名を含みません。 |
| ***下位 CA (Subordinate CA)*** | その証明書がルート CA または別の下位 CA によって署名される認証機関。 |
| ***利用者 (Subscriber)*** | 個人向け証明書の場合は、証明書のサブジェクトであり、証明書が発行される者のこと。組織向け証明書の場合は、証明書のサブジェクトである機器またはデバイスを所有し、証明書が発行される組織のこと。利用者は、証明書に記載されている公開鍵に対応する秘密鍵を使用でき、使用する権限を有しています。 |
| ***利用規約 (Subscriber Agreement)*** | CA または RA により使用される規約で、個人または組織が利用者として活動するための諸条件を規定するもの。 |
| ***子会社 (Subsidiary Company)*** | 申請者が過半数を所有する会社。QIIS の参照、または登録されている Chartered Professional Accountant (CPA) か米国外では同様の組織によって提供された財務報告によって確認できます。 |
| ***上位エンティティ (Superior Entity)*** | Class 1、2、3 のいずれかの STN 階層における特定のエンティティ以上のエンティティ。 |
| ***追加リスク マネジメント レビュー (Supplemental Risk Management Review)*** | 準拠性監査において不完全または例外的な結果が発見された場合、または通常業務の過程での全体的リスク管理プロセスの一環として、シマンテックが実施するエンティティの審査。 |
| ***シマンテック (Symantec)*** | 本 CPS で関連のある各記述に関して、シマンテックとその子会社は、問題となる特定の業務に対し、責任を負うということ。 |
| ***シマンテック電子公証サービス (Symantec Digital Notarization*** | 特定の文書またはデータ セットが特定の時点で存在したことを電子署名付きで表明するサービス。 |

| 用語 | 定義 |
|---|---|
| ***Service)*** | Managed PKI カスタマ向けのサービスです。 |
| ***使用条件 (Terms of Use)*** | 申請者/利用者が CA の関連会社である場合の、本要件に従って発行される証明書の保管および容認される使用に関する条件。 |
| ***信頼される者 (Trusted Person)*** | STN 内のエンティティの従業員、請負業者、またはコンサルタントであり、かかるエンティティ、その製品、サービス、施設、または手続きに関する基盤となる信頼性を管理する責任を負う者。本 CPS セクション 5.2.1 で詳細に規定されています。 |
| ***信頼される地位 (Trusted Position)*** | STN のエンティティにおける地位であり、信頼される者がその地位を占める必要がある |
| ***信頼できるシステム (Trustworthy System)*** | 侵入や不正使用から合理的に保護されており、合理的なレベルの可用性、信頼性、および正しい運用をもたらし、意図される機能の履行に合理的に適しており、かつ適用されるセキュリティ ポリシーを施行する、コンピュータ ハードウェア、ソフトウェア、および手続き。「信頼できるシステムは」、政府が定めた用語体系における「信頼されるシステム (Trusted system)」と必ずしも一致するわけではありません。 |
| ***シマンテック レポジトリ (Symantec Repository)*** | 証明書およびその他関連するシマンテック トラスト ネットワークの情報について、オンラインでアクセス可能なシマンテックのデータベース。 |
| ***シマンテック トラスト ネットワーク (Symantec Trust Network、STN)*** | シマンテック トラスト ネットワーク証明書ポリシーによって統制される証明書ベースの公開鍵基盤。シマンテックとその関連会社、およびそれぞれのカスタマ、利用者、ならびに依拠当事者が、証明書を世界レベルで展開し使用できるようにします。 |
| ***STN 参加者 (STN Participant)*** | STN 内において、シマンテック、関連会社、カスタマ、ユニバーサル サービス センター、リセラー、利用者、または依拠当事者の 1 つ以上に該当する個人または組織。 |
| ***STN スタンダード (STN Standards)*** | STN 内で、証明書の発行、管理、失効、更新、使用に関する事業上、法的、および技術的な要件。 |
| ***未登録ドメイン名 (Unregistered Domain Name)*** | 登録ドメイン名ではないドメイン名。 |
| ***有効な証明書 (Valid Certificate)*** | RFC 5280 で規定される検証手続きに合格した証明書。 |
| ***認証スペシャリスト (Validation Specialists)*** | 本要件により規定される情報検証職責を履行する人物。 |
| ***有効期間 (Validity Period)*** | 証明書が発行された日から有効期限日までの期間。 |
| ***ワイルドカード証明書 (Wildcard Certificate)*** | 証明書に含まれるサブジェクトの FQDN の左端にアスタリスク (*) を含む証明書。 |

# 付録 B1: EV SSL 証明書の追加認証手続き

EV 証明書の発行と管理のための CA/ブラウザ フォーラム ガイドラインの最新バーションは、http://cabforum.org/extended-validation で見ることができます。

# 付録 B2: EV 証明書の最低限の暗号化アルゴリズムと鍵のサイズ

### *1. ルート CA 証明書*

| | **アルゴリズムの最低強度** |
|---|---|
| **ダイジェスト アルゴリズム** | SHA-1*、SHA-256、SHA-384、または SHA-512 |
| **RSA** | 2048 ビット |
| **ECC** | 256 または 384 ビット |

### *2. 下位 CA 証明書*

| | **アルゴリズムの最低強度** |
|---|---|
| **ダイジェスト アルゴリズム** | SHA-1*、SHA-256、SHA-384、または SHA-512 |
| **RSA** | 2048 ビット |
| **ECC** | 256 または 384 ビット |

### *3. 利用者証明書*

| | **アルゴリズムの最低強度** |
|---|---|
| **ダイジェスト アルゴリズム** | SHA-1*、SHA-256、SHA-384、または SHA-512 |
| **RSA** | 2048 ビット |
| **ECC** | 256 または 384 ビット |

*SHA-1 は、SHA-2 が依拠当事者の大多数が使用するブラウザで広くサポートされるようになるまで、使用されるものとします。

# 付録 B3: EV 証明書で要求される証明書エクステンション

### *1. ルート CA 証明書*

2006 年 10 月以後に生成されるルート証明書は、X.509 v3 でなければなりません (MUST)。

**(a) *basicConstraints***

証明書が v3 であり、かつ 2006 年 10 月以降に生成されている場合、証明書の電子署名の認証に使用される公開鍵を含むすべての CA 証明書で、このエクステンションは Critical に指定されなければなりません (MUST)。CA フィールドは、True に設定されなければなりません (MUST)。*pathLenConstraint* フィールドは、存在すべきではありません (SHOULD NOT)。

**(b) *keyUsage***

証明書が v3 であり、かつ 2006 年 10 月以降に生成されている場合、このエクステンションが存在していなければならず (MUST)、また Critical に指定されなければなりません (MUST)。*CertSign* および *cRLSign* のビット位置は、設定されなければなりません (MUST)。その他すべてのビット位置は、設定されるべきではありません (SHOULD NOT)。

**(c) *certificatePolicies***

このエクステンションは、存在すべきではありません (SHOULD NOT)。

**(d) *extendedKeyUsage***

このエクステンションは、存在しません。

他のすべてのフィールドとエクステンションは、RFC 5280 に従って設定されます。

### *2. 下位 CA 証明書*

**(a) *certificatePolicies***

存在しなければならず (MUST)、Critical に指定されるべきではありません (SHOULD NOT)。ポリシー識別子のセットは、シマンテックの EV ポリシーの識別子を含まなければなりません (MUST)。

certificatePolicies:policyIdentifier (必須)

- ***anyPolicy*** 識別子 (下位 CA がシマンテックにより管理される場合)

**(b) *cRLDistributionPoint***

常に存在し、かつ、Critical に指定されません。シマンテックの CRL サービスの HTTP URL を含みます。

**(c) *authorityInformationAccess***

存在しなければならず (MUST)、かつ、Critical に指定されてはなりません (MUST NOT)。
発行する CA の OCSP レスポンダの HTTP URL を含むものとします (accessMethod = 1.3.6.1.5.5.7.48.1) (SHALL)。HTTP accessMethod は、シマンテックの証明書に含まれるべきです (accessMethod = 1.3.6.1.5.5.7.48.2) (SHOULD)。

**(d) *basicConstraints***

このエクステンションは、証明書の電子署名の認証に使用される公開鍵を含むすべての CA 証明書で存在しなければならず (MUST)、また Critical に指定されなければなりません (MUST)。CA

フィールドは、True に設定されなければなりません (MUST)。*pathLenConstraint* フィールドは、存在できます (MAY)。

**(e)** ***keyUsage***

このエクステンションは存在しなければならず (MUST)、かつ、Critical に指定されなければなりません (MUST)。*CertSign* および *cRLSign* のビット位置は、設定されなければなりません (MUST)。その他すべてのビット位置は、設定されてはなりません (MUST NOT)。

他のすべてのフィールドとエクステンションは、RFC 5280 に従って設定されなければなりません (MUST)。

### *3. 利用者証明書*

**(a)** ***certificatePolicies***

存在しなければならず (MUST)、Critical に指定されるべきではありません (SHOULD NOT)。ポリシー識別子のセットは、シマンテックの EV ポリシーの識別子を含まなければなりません (MUST)。

certificatePolicies:policyIdentifier (必須)
- o EV ポリシー OID

certificatePolicies:policyQualifiers:policyQualifierId (必須)
- o id-qt 2 [RFC 5280]

certificatePolicies:policyQualifiers:qualifier (必須)
- o 認証業務運用規程 (CPS) の URI

**(b)** ***cRLDistributionPoint***

常に存在し、かつ、Critical に指定されません。シマンテックの CRL サービスの HTTP URL を含みます。

**(c)** ***authorityInformationAccess***

常に存在し、かつ、Critical に指定されません。国シマンテックの OCSP レスポンダの HTTP URL を含むものとします (accessMethod = 1.3.6.1.5.5.7.48.1) (SHALL)。HTTP accessMethod は、シマンテックの証明書に含めることができます (accessMethod = 1.3.6.1.5.5.7.48.2) (MAY)。

**(d)** ***basicConstraints*** (任意)

存在する場合、CA フィールドは false に設定されなければなりません (MUST)。

**(e)** ***keyUsage*** (任意)

存在する場合、*CertSign* および *cRLSign* のビット位置は、設定されてはなりません (MUST NOT)。

**(f)** ***extKeyUsage***

値 *id-kp-serverAuth* [RFC5280] または *id-kp-clientAuth* [RFC5280] のいずれか、もしくは両方が存在しなければなりません (MUST)。その他の値は、存在すべきではありません (SHOULD NOT)。

**(f)** ***SubjectAltName***

RFC5280 に従って設定され、重要度が FALSE に設定されます。

他のすべてのフィールドとエクステンションは、RFC 5280 に従って設定されます。

# 付録 B4: 外国の組織名称ガイドライン

*注:この付録の記述は、ラテン文字での組織名の登録が行われていない国からの EV 申請にのみ関連します。特定の国々に関するより詳細な情報が、この付録に将来追加される可能性があります。*

EV 申請者の組織名が QGIS にラテン文字で登録されず、申請者の国の文字による組織名と登録が本ガイドラインに従って QGIS で検証済みである場合、シマンテックはラテン文字の組織名を EV 証明書に入れることができます (MAY)。この様な場合、シマンテックはこの付録に示す以下の手続きに従います。

**ローマ字名称**
登録名の翻字/ローマ字名を含める場合、ローマ字名は申請者の法人設立管轄地の行政機関によって正式に認められた体系を使用して、シマンテックにより検証されます。

シマンテックが、申請者の法人設立管轄地の行政機関によって正式に認められた体系を使用して、登録名の翻字/ローマ字名に依拠できない場合は、以下のいずれかの方法 (優先度順に記載) に依拠しなければなりません (MUST)。

- 国際標準化機構 (ISO) により認められる体系。
- 国連により認められる体系、または
- 弁護士意見書による登録名のローマ字名称の確認。

**英語名**
登録名のローマ字名ではないラテン文字名を含める場合、シマンテックはラテン文字名について以下の事項を検証します。

- 組織登録の一部として届出された定款 (または同等の文書) に含まれている、または
- 納税申告の際に申請者を認識する名称として、申請者の法人設立管轄地の QGTIS により認識されている。または
- 登録されている組織に関連付けられている名称であることが、QIIS で確認されている。または
- 登録されている組織に関連付けられる商号であることが、弁護士意見書により確認されている。

**<u>国ごとの手続き</u>**

**F-1. 日本**
前述の手続きに加えて、以下の手続きが適用されます。

- ヘボン式ローマ字名は、日本式ローマ字名として容認される。
- シマンテックは、申請者の正式名称のローマ字翻字を、QIIS または弁護士意見書のいずれかにより検証できます (MAY)。
- シマンテックは、金融庁で英語名を検証できます (MAY)。シマンテックはこの場合、金融庁に提出された監査済みの財務諸表に記録されている英語名を検証します。
- 定款で英語名を検証する場合、定款には、定款が真正かつ最新であることを証明する元の日本語の社印が押印された文書、または弁護士意見書のいずれかが付随していなければなりません (MUST)。シマンテックは、社印の真正性を検証します。

## 付録 C: EV コードサイニング証明書の追加認証手続き

*EV コードサイニング証明書の発行と管理のための CA/ブラウザ フォーラム ガイドライン*の最新バージョンは、https://cabforum.org/ev-code-signing-certificate-guidelines/で見ることができます。

## 付録 D: 補足 -『パブリック証明書の発行および管理に関する基本要件』

CA/ブラウザ フォーラムのパブリック証明書の発行および管理に関する基本要件 の最新バーションは、https://cabforum.org/baseline-requirements-documents/で見ることができます。

# 付録 E:変更履歴

**変更履歴:バージョン 3.8.27 (2016 年 12 月)**

| 説明 | セクション & 変更内容 |
|---|---|
| 多方面 | 文章全体に対して事務・管理的な変更を実施 |
| 1.はじめに | シマンテック トラスト ネットワークは、シマンテックの中の専門の事業部門が管理し、会社が提供する他のセキュリティ製品の責任を持つ事業部門から独立して運用します。STNはネットワークの一部であるルートからSSL監査目的の中間CAを発行することはありません。アプリケーション ソフトウェア提供者の製品(プライベート ルート)の中の現在または過去に信頼されたことがないルートはSSL監視に使用する中間CAを作成するために使われることがあります。 |
| 1.4.2 禁止される証明書の用途 | STNとその参加者は、証明書保持者が合理的に所有または管理しないドメイン名またはIPアドレスに対して中間者またはトラフィック管理のために使うことができるいかなる証明書も発行しません。 |
| 3.1.1 名称のタイプ | 部門名から削除<br>·“Persona Not Validated” (Class 1 個人向け証明書の場合)<br>(本件に関連した脚注)<br><br>コモンネームに追加<br>Class 1 個人向け証明書は本属性を含めない可能性があります。<br><br>電子メール アドレスを変更<br>電子メール アドレスは、Class 1 個人向け証明書とMPKI加入者証明書に含まれる可能性があります。<br><br>表5の下に追加<br>Class 1証明書のコモンネームは、含まれないか、過去に、“Persona Not Validated”が含まれていたことがあります。 |
| 4.9.2 失効を要求できる者 | 追加<br>いかなる人物も証明書の誤使用、証明書に関する不適切な管理、詐欺または鍵の漏洩の目撃をシマンテック ウェブサイト https://www.symantec.com/contact/authentication/ssl-certificate-complaint.jspからオンラインフォームを使って証明書問題報告を提出することによって要求でき、CABF基本要件に記載の時間以内に行動が取られます。 |
| バージョン 3.8.26 変更履歴 | 削除<br>4.9 証明書の失効および効力停止 (追加: STN参加者(関連会社、プロセッシングセンター、サービスセンター)がコードサイニング証明書を発行し、証明書の破棄のための独立した認証局を持つ場合、コードサイニング証明書の破棄とステータス確認のための手順はSTN参加者のCPSで文書化されなければならなず、aka.ms/csbrに掲載されている該当するMicrosoft Minimum Requirementsのセクション13に適合しなければならない。 |

**変更履歴:バージョン 3.8.26 (2016 年 9 月)**

| 説明 | セクション & 変更内容 |
|---|---|
| 多方面 | 文章全体に対して事務・管理的な変更を実施 |
| 1.はじめに | 追加<br>2017年2月1日以降、STNは、https://aka.ms/csbrに掲載されている現行バージョンのthe Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificatesを適用します。本ドキュメントと当該要件に差異がある場合、当該要件が優先されます。<br>2017年2月1日以降に発行されたコードサイニング証明書で、マイクロソフト オーセンティコードおよび付随する技術で使用する証明書には、ポリシー識別子に2.23.140.1.4.1を含みthe Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificatesに適合していることを示します。 |
| 1.5.2 連絡先 | 追加<br>CA/ブラウザ フォーラム (CABF)の連絡先は以下にあります。<br>https://cabforum.org/leadership/ |

| 説明 | セクション & 変更内容 |
|---|---|
| 2.4 リポジトリへのアクセス制御 | 追加<br>シマンテックと関連会社はリポジトリを読み取り専用で公開します。また、セクション1.5.4に記載のリンクまたは関連会社のCPSで定義された場所となります。 |
| 3.2.6 相互運用の基準 | STN CPを重複する以下の文を削除し、表明しません。に変更。<br>シマンテックは、STN 以外の CA に対し、一方的に当該 CA を認定することで STN との相互運用を可能にする相互運用サービスを提供することがあります。このようにして相互運用が可能になった CA は、必要に応じて、追加ポリシーで補足された STN CP に準拠します。<br><br>シマンテックが STN 以外の CA との STN の相互運用を可能にするのは、少なくとも以下の状況にある CA の場合のみとします。<br>·シマンテックと契約関係を結んでいる<br>·発行する証明書のクラスについて、STN 要件を満たす CPS を遵守して運用している<br>·相互運用が許可されるまでにコンプライアンス評価に合格している<br>·相互運用する継続的な権利についての年 1 回のコンプライアンス評価に合格している |
| 4.9.1 失効が行われる場合 | 追加<br>·コードサイニング証明書の場合で、<br>oアプリケーション ソフトウェア提供者がCAの失効と証明書がマルウェアまたは不必要なソフトウェアの署名に使われたことの可能性について調査を要求した場合<br>oSTN関係者に証明書がマルウェアの署名に使用されたことを示す報告書が提出された場合<br><br>·2017年2月1日以降、コードサイニング証明書は、マイクロソフトによって採択されたthe Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificatesのセクション13.1.5に記載されている全ての加入者証明書の失効理由に適合します |
| 4.9.2 失効を要求できる者 | 追加<br>コードサイニング証明書について、シマンテックと関連会社は、コードサイニング証明書の提供先であるアンチ・マルウェア組織、加入者、依拠当事者、アプリケーション ソフトウェア提供者およびその他に対して、秘密鍵漏洩の疑い、証明書の誤った利用、証明書の疑わしいコードに対する署名、乗っ取り攻撃、その他の詐欺行為への利用、漏洩、誤利用、不適切な管理、その他証明書に関連する事項についてどのように報告するかについて明確な指示を提供します。シマンテックと関連会社はウェブサイトに説明書を一般公開します。<br><br>シマンテックとその関連会社は、コードサインニング証明書の発行と、以下の4つの事象による失効権限を有します。(1) アプリケーション ソフトウェア提供者が失効の要求をしシマンテックまたはその関連会社がその他の行動を採る意図がない場合、(2) 認証された加入者が失効の要求をした場合、(3) CAが証明書の漏洩もしくは疑いがあるコードに対して使用したと信じるに足りる情報が、第三者より提供された場合、(4) CAが当該証明書は失効すべきであると判断した場合。シマンテックと関連会社は、the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificatesのセクション13.1.5に記載の失効要求の対応手順に沿ったコードサイニング証明書を発行します。 |
| 4.9.5 CA による失効要求処理の期限 | 追加<br>2017年2月1日以降、シマンテックは、コードサイニング証明書について、the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificatesのセクション13.1.5.3のマルウェアとして定義されている失効時間に従います。 |
| 4.9.6 依拠当事者の失効調査の要件 | 追加<br>CRLリポジトリは多数かつ色々な場所にあるため、依拠当事者は証明書に含まれるCRL Distribution PointsエクステンションのURLを使ってCRLにアクセスすることが推奨されます。適切なOCSPレスポンダは、証明書に含まれるAuthority Information Accessエクステンションにあります。 |
| 4.9.7.2 CRL 発行に関する マイクロソフト要件 | 追加<br>コードサイニングとタイムスタンプ証明書のCRL発行頻度は、本CPSに記載されており、https://aka.ms/csbr に掲載されているthe Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificatesのセクション13.2.2に従います。 |
| 4.9.9 利用可能なオンラインでの失効/ステータス調査 | 追加<br>シマンテックは、コードサイニングとタイムスタンプ証明書のOCPSレスポンスを証明書の有効期限が切れた後、少なくとも10年間提供します。失効された証明書のシリアル番号は、証明書の有効期限が切れた後、少なくとも10年間CRLに残ります。 |
| 5.4.1 記録されるイベントの種類 | 追加<br>o CAの詳細または鍵の変更<br>o 証明書の発行 |

| 説明 | セクション & 変更内容 |
|---|---|
| | o 証明書作成ポリシーの変更<br>· 信頼される従業員イベント、以下<br>o ログオン、ログオフの実施<br>o 全ての権限者の作成、削除、パスワード設定、システム権限変更の実施<br>o 人員変更<br>o システムおよびアプリケーションの開始と終了<br>o CA秘密鍵の運用のためのアクティベーション データの保有<br>o システム構成変更とメンテナンス<br>o 記録に対する破壊 |
| 6.1.5 鍵サイズ | 最初の文からSHA-1の記述を削除、以下を文を追加。<br>STN PCA と CA のすべてのクラス、RA、およびエンドエンティティ証明書では、電子署名ハッシュアルゴリズムに SHA-2が使用されます。また、特定バージョンのシマンテック プロセッシング センターでは、エンドエンティティ利用者証明書においてハッシュ アルゴリズムとして SHA-256 と SHA-384 の使用をサポートしています。 SHA-1は、SSLとEVコードサイニング証明書を除いた古いアプリケーションまたはユースケースで使われる可能性があります。これらの利用はCA/ブラウザフォーラムや関連するアプリケーションソフトウェア提供者の定める手順およびポリシーに反しません。 |
| 6.1.5.1 鍵サイズに関する CA/ブラウザ フォーラム要件 | 追加<br>SHA-1は、CA/ブラウザ フォーラム パブリック証明書の発行および管理に関する基本要件のセクション7.1.3で定義されている基準に従ったRSA鍵で使われる可能性があります。<br>削除<br>SHA-1 は、世界中の大多数の依拠当事者が使用するブラウザにおいて SHA-256 が広くサポートされるようになるまで使用できます。 |
| 6.2.1 暗号化モジュールの基準と制御 | 追加<br>シマンテックはエンタープライズRA顧客が全てのRA自動承認暗号化オペレーションをFIPS 140-1 レベル 2以上の暗号化モジュール上で実施することを推奨します。 |
| 6.2.8.4 管理者の秘密鍵 (Class 3) | 推奨を要求に変更。技術的な制御の事項、最後の事項を追加。<br>技術的な制御によって事前承認されたドメインへの発行には限られない場合、シマンテックでは、アプリケーション ソフトウェア提供者がルート証明書の配布により信頼を得る証明書の発行ができる秘密鍵をアクティベーションする前に管理者認証を行い、管理者がスマートカード、生体認証アクセス対応デバイス、またはこれらと同等の強度のセキュリティをセクション 6.4.1 で規定されているパスワードとともに使用することを要求します。 |
| 6.2.10 秘密鍵を破壊する方法 | 記録するから立会人を置くへ変更。<br>CA の鍵の破壊に関する操作をする場合は立会人を置きます。 |
| 6.3.2 証明書の運用期間および鍵ペアの使用期間 | カカッコ内に詳細を追加<br>さらに、STN CA は、いずれかの上位 CA 証明書の有効期間が満了になった後に下位 CA が発行した証明書の有効期間が満了になる事態が起こらないように、CA の証明書の有効期間が満了になる前の適当な日(60日に加え発行された証明書の最大有効期間)に、新規証明書の発行を停止します。<br><br>表 8 – 証明書の運用期間のオンラインの CA からエンドユーザー個人利用者へを以下へ変更<br>通常は最長 3 年間。ただし、以下の条件の下で、証明書は一回更新でき、その期間は最長 6 年間 。6 年経過後は新規申請が必要になります。<br><br>表 8 – 証明書の運用期間のオンラインの CA からエンドエンティティ組織利用者へを以下へ変更<br>セクション6.3.2.1の制約の下で、通常最長 6 年間 。この場合、更新やリキーは選択できません。6年経過後は新規申請が必要になります。<br><br>削除<br>STN CP のセクション 6.3.2 の規定に関して、シマンテック PMA は、CA 鍵ペアの移行中に PKI Service が中断しないように、例外措置として、限定数の CA において規定上限を超える有効期間の適用を承認します。この例外措置は、SSL 証明書を発行する CA に関与していないカスタマ、インフラストラクチャ、管理用 CA に対してのみプロセッシング センターのソフトウェア機能を運用しているシマンテックの関連会社に適用できます。ただし、この例外措置は、最長で 2014 年 8 月 31 日までとし、CA の有効期間を延長して合計で 14 年を超えてしまう場合は適用できず、さらに 2013 年 12 月 31 日以降は使用できないものとします。 |
| 6.6.2 セキュリティ管理の制御 | 定期的から日次へ変更<br>インストール時と、その後は日次で、シマンテックはその CA システムの完全性を確認します。 |

| 説明 | セクション & 変更内容 |
|---|---|
| 7.1 証明書プロファイル | 表 9のシリアル番号に関する記述を変更<br>CSPRNGから出力される64 ビット以上のエントロピーを示す発行者識別名 (Issuer DN) ごとの一意の値 |
| 7.1.2.1 KeyUsage | 値は通常TRUEに設定される記述に変更 |
| 7.1.2.5 Extended Key Usage | 追加<br>シマンテック証明書は、アプリケーション ソフトウェア提供者がトラスト ビットを許可し、プライベート PKIユースケースにおいてExtendedKeyUsageエクステンションを含む可能性があります。 |
| 7.1.2.6 CRL Distribution Points | 追加<br>URLは、LDAPプロトコルを除きMozilla要件に適合します。URLはcRLDistributionPointsエクステンションに複数含まれる可能性があります。 |
| 7.1.3 アルゴリズムのオブジェクト識別子 | 削除<br>· md5WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 4}<br><br>SHA-1に代わってSHA256が使用されることへの変更、MD5の記述を削除<br>これらのアルゴリズムを使用して生成された証明書の署名は、RFC 3279 に準拠するものとします。sha256WithRSAEncryption が、sha-1WithRSAEncryption に代わって使用されます。 |
| 7.2 CRL のプロファイル | 追加<br>該当する証明書タイプに対応するCRLはCA/ブラウザ フォーラム パブリック証明書の発行および管理に関する基本要件の現行バージョンに適合します。 |
| 7.3 OCSP プロファイル | RFC 6960への準拠へ変更<br>·Class 2 エンタープライズ向け証明書および RFC 6960 に準拠するシマンテック TGV (Trusted Global Validation) サービスを使用するClass 3 組織向け証明書 |
| 7.3.1 バージョン番号 | RFC 6960への準拠へ変更<br>RFC 2560、RFC 5019で規定されているバージョン 1 の OCSP 仕様、および RFC 6960がサポートされます。 |
| 8. 準拠性監査とその他の評価 | 削除<br>カスタマ固有の CA の場合は、カスタマが要求しない限り、シマンテックの運用における監査の一部として特に監査されることはありません。<br><br>追加<br>·関連会社のセキュリティおよびプラクティス レビューによってオペレーションの開始を許可します。セキュリティおよびプラクティス レビューは関連会社がSTN標準に適合することを保証するために関連会社施設のセキュリティ、セキュリティ文書、CPS、STN関連の合意、プライバシーポリシー、認証計画のレビューを含みます。<br><br>変更<br>エンタープライズ カスタマーの記述を、自分自身、関連会社へ変更<br>·シマンテックは、監査対象エンティティについて、「STN スタンダードを満たしていない」、「事故または危殆化が生じた」、もしくは「STN のセキュリティ/完全性を現実的または潜在的に脅かすような作為または不作為があった」と確信できる理由がある場合には、自らの判断により、いつでも自分自身、関連会社またはエンタープライズ カスタマに「緊急監査/調査」を実施する権利があるものとします。 |
| 8.4 評価対象項目 | 追加<br>登録局の監査(Class 1-2)<br>エンタープライズ カスタマが承認するClass1と2の証明書は年次監査を受ける可能性があります。シマンテックおよび、または上位組織(上位組織がシマンテックでない場合)の要請によって、エンタープライズ カスタマはSTNポリシーに対するいかなる例外や違反行為は記録し、違反行為の改善をする可能性があります。<br><br>登録局の監査(Class 3)<br>エンタープライズ カスタマが発行を認証するClass 3 SSL証明書はSTNの責務のもと年次監査を受けます。シマンテックおよび、または上位組織(上位組織がシマンテックでない場合)の要請によって、エンタープライズ カスタマはSTNポリシーに対するいかなる例外や違反行為は記録し、違反行為の改善をします。<br><br>シマンテックまたは関連会社の監査(Class 1-3)<br>シマンテックおよびそれぞれの関連会社は、受託会社の持つリスクに関して米国公認会計士協会の |

| 説明 | セクション & 変更内容 |
|---|---|
| | Statement on Service Organizations Control (SOC)報告書により提供されるガイドラインに従い鑑査されます。適合監査は認証局のためのWebTrust監査またはシマンテックが承認した同等の監査標準です。承認した監査には運用ポリシーと手順および運用有効性のテストに関する報告書が含まれます。 |
| 9.4.4 個人情報の保護責任 | 以下へ変更<br>シマンテックと関連会社は、個人情報が第三者に漏えいおよび開示されないよう保護するとともに、自身の所在地の個人情報保護法規に全面的に従うものとします。 |
| 9.12.2 通知方法と期間 | 追加<br>シマンテックとPMAは、CA/ブラウザ フォーラムのガイドラインに従い、本CPSを少なくとも年次で更新します。 |
| 付録 A: 頭字語・定義表 | 追加 頭字語<br>CSPRNG Cryptographically Secure Pseudo-Random Number Generator(暗号論的擬似乱数生成器)<br><br>追加 定義表<br>暗号論的擬似乱数生成器 (Cryptographically Secure Pseudo-Random Number Generator) 暗号技術で利用するための擬似乱数を発生させるための機器。 |

**変更履歴:バージョン 3.8.25 (2016 年 8 月)**

| 説明 | セクション & 変更内容 |
|---|---|
| 表 2 - 組織向け証明書の用途 | 保証レベル"中"列と"Class 3 ドメイン認証(DV) 証明書"行を追加。 |
| セクション 1.4.1.3 保証レベル | 保証レベル"中"の段落を追加。 |
| 表 5 – エンドユーザー利用者証明書に含まれる識別名の属性 | 属性Oの値リストに以下を追加。<br>·ベーシック ドメイン認証(DV)証明書では使用しません<br>属性OUの値リストにに以下を追加。<br>·“Domain Validated”(適用される場合) |
| セクション 3.1.1 | 以下の文の後に、表 5A – ベーシック ドメイン認証(DV) エンドユーザー利用者証明書に含まれる識別名の属性を追加。<br><br>ベーシック ドメイン認証(DV)証明書は、SubjectName フィールドに X.501 DN を含み、表 5A で示されている要素で構成されます。 |

**変更履歴:バージョン 3.8.24 (2016 年 5 月)**

| 説明 | セクション & 変更内容 |
|---|---|
| 表 8 – 証明書の運用期間 | 以下のPCAについて運用期間の記述を変更<br>PCA 自己署名 (2048 ビット RSA) 最長50年から37年 |

**変更履歴:バージョン 3.8.23 (2016 年 1 月)**

| 説明 | セクション & 変更内容 |
|---|---|
| 表 6 – 特別な認証手続き | Managed PKI for Intranet SSL証明書のために既存の記述を変更<br><br>subjectAlternativeNameエクステンションやサブジェクトのコモンネームに予約済みIPアドレスか内部的な名前を持つ証明書の利用は、CA/ブラウザ フォーラムによって禁止され、2016年10月までに排除されます。~~2016年10月より前~~施行日の後に発行されたそのような証明書は、2015年11月1日より前に有効期限を迎えなければなりません。~~2015~~2016年~~11~~10月1日以降の有効期限を持つ発行済みの証明書は、2016年10月1日で失効されます。 |
| 定義 | 既存の注記36を変更<br><br>subjectAlternativeNameエクステンションやサブジェクトのコモンネームに予約済みIPアドレスか内部的な名前を持つSSL/コードサイニング証明書の利用は、CA/ブラウザ フォーラムによって禁止され、2016年10月までに排除されます。~~2016年10月より前~~施行日の後に発行されたそのような証明書は、2015年11月1日より前に有効期限を迎えなければなりません。~~2015~~2016年~~11~~10月1日以降の有効期限を持つ発行済みの証明書は、2016年10月1日で失効されます。 |

| 説明 | セクション & 変更内容 |
|---|---|
| 定義 | 内部サーバー名 (Internal Server Name)の定義を削除<br><br>内部名(Internal name)の定義を追加<br><br>証明書のコモンネームまたはSubjectAlternativeNameフィールドに含まれる文字列(IPアドレスではない)で、IANAのRoot Zoneデータベースにトップレベルドメインとして登録されているもので終わっていないため、証明書の発行時点においてパブリックDNSで世界で唯一のものと確認できないもの。 |

**変更履歴:バージョン 3.8.22 (2015 年 12 月)**

| 説明 | セクション & 変更内容 |
|---|---|
| 1.1 概要 | 既存の注記を変更<br><br>~~注記: 2015 年 3 月 27 日をもって、Symantec Class 3 Public Primary Certification Authority - G2 は本文書の適用範囲から除外します。すなわち、PCA または Class 3 PCA への参照は Symantec Class3 PCA-G2 には適用されません。このルート証明書はブラウザの信頼されるルートリストから除外され私的な目的だけに利用されます。シマンテック トラスト ネットワーク CPS および CP はこのルート証明書の使用ならびに、いかなる付随サービスについて規定しません。~~<br><br>注記:以下の日付をもって、以下のルート証明書を本文書の適用範囲から除外します。<br>• 2015 年 12 月 1 日<br>**VeriSign Class 3 Public Primary Certification Authority**<br>Country = US<br>Organization = VeriSign, Inc.<br>Organizational Unit = Class 3 Public Primary Certification Authority<br>• 2015 年 3 月 27 日<br>**VeriSign Class 3 Public Primary Certification Authority – G2**<br>Country = US<br>Organization = VeriSign, Inc.<br>Organizational Unit = Class 3 Public Primary Certification Authority - G2<br>Organizational Unit = (c) 1998 VeriSign, Inc. - For authorized use only<br>Organizational Unit = VeriSign Trust Network<br>PCA または Class 3 PCA への参照は、これらのルート証明書には適用されません。これらのルート証明書は私的な目的だけに利用されることだけを意図しており、ブラウザの信頼されるルートリストから除外されるべきです。シマンテック トラスト ネットワーク CPS および CP はこのルート証明書の使用ならびに、いかなる付随サービスについて規定しません。 |

**変更履歴:バージョン 3.8.21 (2015 年 11 月)**

| 説明 | セクション & 変更内容 |
|---|---|
| 表 5 – エンドユーザー利用者証明書に含まれる識別名の属性 | Web サーバー証明書の項目に“またはパブリック IP アドレス”を追加<br><br>この属性は、次のものを含みます。<br>• OCSP レスポンダ名 (OCSP レスポンダ証明書の場合)<br>• ドメイン名 **またはパブリック IP アドレス**(Web サーバー証明書の場合)<br>• 組織名 (コード/オブジェクト サイニング証明書の場合)<br>• 個人の名前 (個人向け証明書、または個人に発行されるコードサイニング証明書の場合)<br>• “Persona Not Validated” (Class 1 個人向け証明書の場合) |
| 3.1.1 名前のタイプ | “表 5 – エンドユーザー利用者証明書に含まれる識別名の属性”の下のリストの最後に以下を追加<br><br>• 全てのWebサーバー証明書において、subjectAltNameエクステンションには、サブジェクトDNのコモンネームの認証された値を含みます。(ドメイン名またはパブリックIPアドレス) subjectAltNameエクステンションには、コモンネームと同等の認証を行った追加のドメイン名やパブリックIPアドレスを含むことがあります。 |
| 7.1.2.3 Subject Altanative Names | 以下を最後に追加<br><br>全ての Web サーバー証明書において、subjectAltName エクステンションには、サブジェクト DN のコ |

| 説明 | セクション & 変更内容 |
|---|---|
| | モンネームの認証された値を含みます。(ドメイン名またはパブリック IP アドレス) subjectAltName エクステンションには、コモンネームと同等の認証を行った追加のドメイン名やパブリック IP アドレスを含むことがあります。 |

**変更履歴:バージョン 3.8.20 (2015 年 6 月)**

| 説明 | セクション & 変更内容 |
|---|---|
| 3.2.2 組織の識別情報確認 | 最後の一文を追加<br>ドメイン名または電子メール アドレスが証明書に含まれる場合、シマンテックは完全修飾ドメイン名または電子メール ドメインとしてドメイン名を使用する権限が組織にあることを認証します。組織認証(OV)とExtended Validation(EV)のドメインの認証は、全てにおいて組織の認証と一緒に完了させます。 |
| 3.2.2.2 組織の申請者に関する Mozilla 社の審査の要件 | 以下の修正を実施<br>証明書内の国際化ドメイン名 (IDN) の申請において、シマンテックは IDN の同形異義語攻撃に備え、ドメイン名所有者の検証を行います。シマンテックでは、複数の Whois サービスの検索を実行して特定ドメインの所有者を自動的に検出するプロセスを採用しています。検索が失敗した場合、手動による再検索が実行され、RA は手動でその証明書申請を否認~~します~~することができます。さらに、RA は 1 つのホストネーム ラベル内で複数のスクリプトで作成されているように表示されるドメイン名はすべて否認します。<br>シマンテックは、CA/ブラウザ フォーラムに積極的に参加し、IDN 証明書のスタンダード確立に寄与します。また、フォーラム本体で~~策定~~承認されたスタンダードを遵守~~するよう注力~~します。 |
| 3.2.2.3 ドメインの認証 | 本セクションを追加<br>シマンテックは、ドメイン名の審査において以下の手法を用います。また、選択肢の1番目を最初に実施します。<br>1. Whois検索を実施し、申請者がドメインのレジストラにおいてドメインの登録者であるか確認する。<br>2. ドメインのレジストラによって提供される住所、電子メール アドレスまたは電話番号を使って直接ドメイン登録者へ連絡する。<br>3. ドメイン利用許可証に依拠する。<br>4. Whoisに登録されている登録者名、技術連絡担当者、登録担当者に記載されている連絡先情報を使って直接ドメイン登録者へ連絡する。<br>5. ”admin”、”administrator”、”webmaster”、”hostmaster”、または”postmaster”とアットマーク(”@”)と要求されたFQDNから0などその他を削除し成形されたドメインとによって生成された電子メール アドレスを使ってドメインの管理者へ連絡する。<br>6. FQDNを含むURIで識別可能なオンラインwebページ上の情報を合意した変更がされたことをを確認することでFQDNを申請者が実質的に管理していることを確認する。 |
| 3.2.3 個人の識別情報の認証 | 表7のClass1の識別情報の認証を修正<br>識別情報は認証されません。~~利用者の電子メール アドレスについて、当該アドレスに電子メールを送り、利用者が応答できるかという限定的な確認を行います。~~証明書利用者が当該電子メール アドレスにアクセスできるか限定的な確認を行います。シマンテックは以下の方法に則って実施します。申請者から登録申請を受け取ると、シマンテックはセキュリティの観点から2通の電子メールを申請者へ送ります。1通目の電子メールはセルフサービスのwebページにアクセスするためのURLを含み、もう1通の電子メールにはセルフサービスのwebページにアクセスし申請者の電子メール アドレスのためにランダムで生成されたパスワードが含まれます。証明書申請者はシマンテック セルフサービスwebページから要求した証明書を受け取るためにこのパスワードを使わなければなりません。申請者は提供した電子メール アドレスにシマンテックが送る電子メールを実際に受信し、提供されたパスワードを使って証明書を受領することで確認します。 |
| 3.2.3 個人の識別情報の認証 | 表7のClass2の識別情報の認証を修正 |
| 3.2.3 個人の識別情報の認証 | 表7のClass3の識別情報の認証を修正 |

**変更履歴:バージョン 3.8.19 (2015 年 3 月)**

| 説明 | セクション & 変更内容 |
|---|---|
| 1.1 概要 | 本セクションに以下の注記を追加<br>注記: 2015年3月27日をもって、Symantec Class 3 Public Primary Certification Authority . G2は本文書の適用範囲から除外します。すなわち。PCAまたはClass 3 PCAはへの参照はSymantec Class3 PCA-G2には適用されません。このルート証明書はブラウザの信頼されるルートリストから除外され私的な目的にのみ利用されます。シマンテック トラスト ネットワーク CPSおよびCPはこのルート証明書の使用ならびに、いかなる付随サービスについて規定しません。 |
| 6.1.5 鍵サイズ | 注釈の一部を削除（＃24）<br>~~旧式のプラットフォームを使用するカスタマをサポートするため、CA の信頼性は 1024 ビットの RSA 鍵ペアを使用するシマンテックの第 1世代 (G1) および第 2 世代 (G2) の旧式の信頼されるルートまで拡張されています。1024 ビットの RSA 鍵ペアを使用するエンドエンティティ証明書は、有効期間が 2014 年 1 月 31 日までのものであれば発行できます。 また、2013年以降も旧式アプリケーションを使用した業務継続を保持することについて事前承認を受けた上で、セクション 6.3.2 に従って、プロセッシング センターのソフトウェア機能を操作するシマンテックの関連会社に対しても個別に例外として許可できます。~~<br>シマンテックは、標準の Web ブラウザ以外のクライアント ソフトウェアで使用されることが意図された、最小数 (未公表) の SSL サーバー証明書を発行する権利を有します。これらの証明書には、クリティカル EKU エクステンションが含まれますが、それには serverAuth フラグは設定されず、標準 Web ブラウザにおいて使用されるべきでないことを示す 2.16.840.1.113733.1.8.54.1 の特別なフラグが設定されます。 |

**変更履歴:バージョン 3.8.18 (2015 年 2 月)**

| 説明 | セクション & 変更内容 |
|---|---|
| 表 3 – 証明書の公開要件 | リポジトリURLの変更とSSL/コードサイニング証明書リポジトリの参照URLの削除<br>シマンテック リポジトリ (https://pki-search.symauth.com/pki-search/index.htm~~https://digitalid.verisign.com/services/client/index.html~~) のクエリー機能、および LDAP ディレクトリ サーバー (*directory.verisign.com*) のクエリーを通じて任意で公開され、依拠当事者が利用可能になります。ただし、~~シマンテック リポジトリ (https://digitalid.verisign.com/services/server/search.htm) のクエリー機能を通じて利用できる~~ Class 3 SSL およびコードサイニング証明書は除きます。 |
| 3.1.1 名前のタイプ | VeriSign Japan Inc.をVeriSign Japan K.K.へ変更 |
| 表 6 – 特別な認証手続き | “US”を”2 文字の ISO 国コード”に変更<br><br>Managed PKI for Intranet SSL 証明書に追記<br>subjectAlternativeNameエクステンションやサブジェクトのコモンネームに予約済みIPアドレスか内部的な名前を持つ証明書の利用は、CA/ブラウザ フォーラムによって禁止され、2016年10月までに排除されます。2016年10月より前に発行されたそのような証明書は、2015年11月1日より前に有効期限を迎えなければなりません。2015年11月1日以降の有効期限を持つ発行済みの証明書は、2016年10月1日で失効されます。<br><br>電子メール署名用組織向けクラス3証明書を追加<br>シマンテックは、電子メールのドメイン名の所有権が当該組織にあることを確認します。 |
| 4.9.9 利用可能なオンラインでの失効/ステータス調査 | リポジトリのURL変更とSSL/コードサイニング証明書リポジトリのURL削除<br><br>オンラインでの失効およびその他の証明書ステータスの情報は、Web ベース リポジトリ、そして提供されている場合は OCSP を通じて入手できます。シマンテックは、CRL の公開に加え、シマンテック リポジトリにおけるクエリー機能により、証明書ステータス情報を提供します。<br><br>個人向け証明書ステータス情報を確認できる Web ベースのクエリー機能には、以下のシマンテック リポジトリからアクセスできます。<br>.<br>https://pki-search.symauth.com/pki-search/index.html~~https://digitalid.verisign.com/services/client/index.html (個人向け証明書の場合)~~<br>~~. https://digitalid.verisign.com/services/server/search.htm (SSL およびコードサイニング証明書の場合)~~<br><br>シマンテックは、OCSP による証明書ステータス情報も提供しています。OCSP サービスに関する契約を締結しているエンタープライズ カスタマは、OCSP を利用することにより証明書ステータスを調査できます。関係する OCSP レスポンダの |

| 説明 | セクション & 変更内容 |
|---|---|
| | URL は、エンタープライズ カスタマに伝えられます。 |
| 付録 A: 頭字語・定義表 | MPKIの定義に注記を追加<br>subjectAlternativeNameエクステンションやサブジェクトのコモンネームに予約済みIPアドレスか内部的な名前を持つ証明書の利用は、CA/ブラウザ フォーラムによって禁止され、2016年10月までに排除されます。2016年10月より前に発行されたそのような証明書は、2015年11月1日より前に有効期限を迎えなければなりません。2015年11月1日以降の有効期限を持つ発行済みの証明書は、2016年10月1日で失効されます。 |
| 付録 B2 EV 証明書の最低限の暗号化アルゴリズムと鍵のサイズ | 追記変更<br><br>SHA-1 は、SHA-2~~56~~ が依拠当事者の大多数が使用するブラウザで広くサポートされるようになるまで、使用できるものとします。 |

**変更履歴:バージョン 3.8.17 (2015 年 1 月)**

| 説明 | セクション & 変更内容 |
|---|---|
| セクション 4.2.4 証明書認証局権限 (Certificate Authority Authorization CAA)を追加 | セクション 4.2.4 証明書認証局権限(Certificate Authority Authorization CAA)<br>2015 年 10 月 日 1 時 点 において、シマンテックは、証 明 書 認 証 局 権 限 (Certificate Authority Authorization CAA)レコードをパブリックSSL証明書の認証と確認プロセスの一環として記録します。その日より前は、シマンテックは全てのパブリックSSL証明書の申請についてCAAレコードを確認しない可能性があります。パブリックSSL証明書とは、公開しているルート証明書につながり、CA/ブラウザフォーラムの基本要件とEV要件を満たすものを意味します。 |

**変更履歴:バージョン 3.8.16 (2014 年 5 月)**

| 説明 | セクション & 変更内容 |
|---|---|
| シマンテック サブドメインの定義の中に株式会社シマンテックが管理している STN CA に関する記述を追加 | 1.1 概要<br>より一般的には、本 CPS は、株式会社シマンテックによって管理されるSTN CA を含むシマンテックのサブドメイン内におけるすべての個人およびエンティティ (以下総称して「シマンテック サブドメイン参加者」) による STN のシマンテック サブドメイン内の STN サービスの利用についても規定します。 |
| 古い証明書の組織名の記載を追加 | 3.1.1 名称のタイプ<br>*該当する証明書の組織名 (O) 行に “VeriSign Japan K.K.” が記載されていますが、「Symantec Japan, Inc.」を意味するものとします。該当する証明書の組織名 (O) 行に “VeriSign Australia.” が記載されていますが、「Symantec Corporation」を意味するものとします。* |
| Symantec Japan CPS で承認されていた Class1 個人向け証明書及び Class3 組織向け証明書のための追記(現在は本 CPS へ統合) | 表 6 – エンドユーザー利用者証明書に含まれる識別名の属性<br>コモンネームに追加<br>・“Persona Not Validated”(Class 1 個人向け証明書の場合)<br>注釈を追加<br>2014/7/11までにシマンテックによって承認された"Class1 Managed PKI"顧客は、OUに”Persona Not Validated”の記載がある限り、CNに仮名を記載することができます。<br>電子メールアドレスに追加<br>Class3組織向け電子メール署名証明書のための電子メールアドレス |
| 付録 D のリファレンスを追加 | 表 6 – 特別な認証手続き<br>組織認証 (OV)/ドメイン認証 (DV) 証明書<br>シマンテックによる OV/DV 証明書の発行手続きは、本 CPS ではの補足Dに記載している「OV/DV 証明書に関する CA/ブラウザ フォーラム要件」として区別して記載されています。 |
| シマンテック所有を削除、株式会社シマンテック及びシマンテック オーストラリアの DRF の注記を追加 | 5.7.4 災害後の業務継続能力<br>シマンテックは主要なプロダクション施設から地理的に離れた場所で、~~シマンテック所有~~の災害復旧拠点 (Disaster Recovery Facility、以下「DRF」) を維持します。<br>注記 |

| 説明 | セクション & 変更内容 |
|---|---|
| | 株式会社シマンテックおよびシマンテック オーストラリアの施設は主要施設から地理的に離れた場所にDRFを維持しています。両方のDRFはシマンテックのセキュリティ標準を明確に満たすように作られています。 |
| LDAP ディレクトリについて注記を追加 | 6.1.4 依拠当事者への CA 公開鍵の交付<br>Symantec Japan Inc.またはVeriSign Japan K.K.が発行するSTN CAの証明書はLDAP ディレクトリ（directory.verisign.co.jp））からダウンロードできます。 |
| 株式会社シマンテックの外部監査手法を追加 | 8. 準拠性監査とその他の監査<br>Symantec Japan Inc. のパブリックCA の外部監査は WebTrust for Certification AuthoritiesではなくISAE3402/SSAE16で実施する。 |
| 日本語のプライバシーポリシーの URL を追加 | 9.4.1 プライバシー プラン<br>日本語版のプライバシー プランは以下で公開しています。<br>http://www.symantec.com/ja/jp/about/profile/privacypolicy/index.jsp |
| 文書を外部ウェブサイトの URL を参照するよう変更 | Appendix B1<br>EV 証明書の発行と管理のための CA/ブラウザ フォーラム ガイドラインの最新バージョンは、http://cabforum.org/extended-validationで見ることができます。 |
| 文書を外部ウェブサイトの URL を参照するよう変更 | Appendix C<br>EV コードサイニング証明書の発行と管理のための CA/ブラウザ フォーラム ガイドラインの最新バージョンは、https://cabforum.org/ev-code-signing-certificate-guidelines/で見ることができます。 |
| 文書を外部ウェブサイトの URL を参照するよう変更 | Appendix D<br>CA/ブラウザ フォーラムのパブリック証明書の発行および管理に関する基本要件(CA/ブラウザ フォーラム）の最新バージョンは、https://cabforum.org/baseline-requirements-documents/で見ることができます。 |

**変更履歴:バージョン 3.8.15 (2014 年 3 月)**

| 説明 | セクション & 変更内容 |
|---|---|
| NetSure プロテクション プランに基づく損害賠償額の変更 | セクション 9.8 – NetSure プロテクション プランに基づく損害賠償額を10,000米ドルから1,750,000米ドルへ変更(50,000米ドルから250,000米ドルから) |

**変更履歴:バージョン 3.8.14 (2013 年 12 月)**

| 説明 | セクション & 変更内容 |
|---|---|
| 1024 ビット証明書の有効期限の変更 | セクション 6.1.5 – 日付を 2014 年 1 月 31 日に変更 |
| 関連会社 PC CA の例外言語の更新 | セクション 6.3.2 – カスタマ CA を追加、および例外適用最終日を 2013 年 12 月 31 日に変更。 |

**変更履歴:バージョン 3.8.13 (2013 年 11 月)**

| 説明 | セクション & 変更内容 |
|---|---|
| セクション 1 概要 | CA/ブラウザ フォーラム基本要件への準拠を明確化 |
| 6.1.5 鍵サイズ | 2048 ビット未満の利用者証明書が、サーバー認証フラグと指定 OID が設定されない EKU を含むことについて明確化 |
| 7.1 証明書プロファイル | 2048 ビット未満の利用者証明書が、サーバー認証フラグと指定 OID が設定されない EKU を含むことについて明確化 |
| 7.1.2.1 鍵用途 | 閉鎖的なエコ システム内で使用される 2048 ビット以下のサイズの証明書に対する承認 |
| 付録 B1 | EV ガイドラインをバージョン 1.4.3 に更新。 |
| 付録 D | 基本要件をバージョン 1.1.6 に更新 |

**変更履歴:バージョン 3.8.12 (2013 年 2 月)**

| 説明 | セクション & 変更内容 |
|---|---|
| 新しいルートを追加 | セクション 6.1.5 – G4、G6、および G7 の PCA を追加 |
| 監査ログの処理手続きを明確化。 | セクション 5.4.2 – 監査ログの処理手続きを明確化 |
| Mozilla IDN 検証要件を追加 | セクション 3.2.2 – IDN の同形異義語攻撃に備えるための IDN の検証手続きを追加 |

**変更履歴:バージョン 3.8.11 (2013 年 1 月)**

| 説明 | セクション & 変更内容 |
|---|---|
| CA/ブラウザ フォーラム EV v1.4 ガイドラインに関する調整 | • 構成変更された CA/ブラウザ フォーラム ガイドラインに一致するように、付録 B1 のすべてのセクションを更新<br>• 付録 B1 との相互参照のために付録 C (EV コードサイニング) を更新<br>•付録 B1 との相互参照のために付録 D (OV および DV 証明書の要件) を作成<br>•CA/ブラウザ フォーラムの手続きにおいて必要とされる、CPS の付録 B1、C、および D への参照を更新 |

**変更履歴:バージョン 3.8.10**

| 説明 | セクション & 変更内容 |
|---|---|
| 2048 DSA ルートの追加 | **6.1.5 鍵サイズ**<br>シマンテックの第 7 世代 (G7) PCA で 2048 ビットの DSA 鍵ペアを使用 |
| プライベート Class 3 管理階層の追加 | **1.1 概要**<br>• シマンテック トラスト ネットワークをサポートする、シマンテック インフラストラクチャ CA およびシマンテック管理 CA[1]<br>また、本 CPS に特に記載がない場合、シマンテックが管理するプライベート CA および階層は、本 CPS の適用範囲外です。[2] 関連会社が管理する CA も、本 CPS の対象外です。<br>脚注:<br>[1]シマンテックは、本 CPS の範囲内で、パブリックおよびプライベート/内部的 Class 3 階層の両方を運用します。Class 3 内部 CA 階層は、プライベート PCA、および CP のセクション 1.2 で規定されている指定 OID 値で識別されます。プライベート PCA 証明書は、証明書の使用目的から「サーバー認証」と「コードサイニング」が明示的に除外されるよう構成されます。<br>**1.3.1 認証機関**<br>シマンテックは、シマンテックの内部的な管理に限定して使用される「Symantec Class 3 Internal Administrator CA」階層も運用しています。<br>シマンテックは「Symantec Universal Root Certification Authority」および「Symantec ECC Universal Root Certification Authority」も運用しています。Universal Root CA は、Class 3 および特定の Class 2 の下位 CA 証明書を発行します。<br>シマンテックのエンタープライズ カスタマは、パブリック STN PCA の下位に属する CA として、独自の CA を運用できます。 |
| CN 属性値 (Class 1 個人向け証明書の場合) | 3.1.1 名称<br>CN = “Persona Not Validated” (Class 1 個人向け証明書の場合) |
| エンタープライズ以外のカスタマについての失効要求がエンタープライズ管理者により伝達されない | 4.9.3.1 失効要求<br>エンタープライズ以外のカスタマの場合も、CPS のセクション 3.4 の規定に従って失効要求を連絡するものとします。 |

**変更履歴:バージョン 3.8.9**

| 説明 | セクション & 変更内容 |
|---|---|
| **EV コードサイニング証明書の CA/ブラウザ フォーラム要件** (バージョン v1.4) への準拠を反映するすべての更新。 | 付録 C。<br>セクション 1.4.1.2、表 2 – Class 3 EV 証明書のカテゴリに CS 証明書を追加<br>セクション 3.2.2、表 6 – EV-CS 証明書および H/W が保護された EV-CS 証明書に手続きを追加 |
| 通常の保守 | セクション 1、1 ページ、「組織向け証明書」を明確化/定義する脚注を追加 |
| | 「セキュア・サーバ CA」および「セキュア・サーバID」を削除 – セクション 1.3.1、3.1.1、6.3.2.1、付録 A の定義 |

| 説明 | セクション & 変更内容 |
|---|---|
| | 「ASB 証明書」を削除 – セクション 2.1、3.1.1、4.9.1、4.9.3.1、付録 A の定義 |
| | TGV プロトコルを TGV サービスに修正 – セクション 7.3 |
| | ブランド名変更によるシマンテック リポジトリ URL の全面変更 – www.symantec.com/about/profile/policies/repository.jsp |
| | 断定的な記述に変更:「シマンテックは確認するものとします」を「シマンテックは確認します」に変更 – セクション 3.2.2.1、4.1.2.2、4.9.3.2、4.9.7.1、4.9.9.1、6.1.5.1、6.3.2.1、6.5.1.1、7.1.2.2.1 |
| | ポリシー OID への参照を明確化:「STN CP のセクション 1.2 に記載されている対応するポリシー識別子」 – セクション 7.1.6.1 |

**変更履歴:バージョン 3.8.8**

| 説明 | セクション & 変更内容 |
|---|---|
| 2012 年 7 月 1 日に発効する DV および OV 証明書に関して CA/ブラウザ フォーラム要件に準拠することを反映。 | 文書全体。詳細な変更内容は、STN CP & CPS 向けの PWG 承認マッピング マトリクスを参照。 |

**変更履歴:バージョン 3.8.7**

| 説明 | セクション & 変更内容 |
|---|---|
| Universal Root の明確化 – Class 3 および特定の Class 2 証明書のみに制限。 | **1.3.1**<br>シマンテックは「Symantec Universal Root Certification Authority」および「Symantec ECC Universal Root Certification Authority」も運用しています。Universal Root CA は、~~特定の証明書クラスでは定義されておらず、~~Class 3 および特定の Class 2 の~~すべてのクラスの~~下位 CA の証明書を発行します。 |
| 自らの RA サービスを実行するカスタマ向けのカスタマイズの要件を明確化。 | **3.1.1** 脚注の追加:<br>OU= “Authenticated by Symantec[1]”<br>[1] サービスを実行する契約を締結している関連会社またはカスタマは、利用者認証を行う組織名を示すものとします。 |
| ログ処理の改善の追加。 | **5.4.2**<br>CA システムおよび監査ログは、セキュリティおよび運用に関連する顕著なイベントについて、リアル タイムのアラートを提供するために継続的に監視されます~~少なくとも毎週確認されます~~。 |
| シマンテックへの移行に関して BCP を更新 | **5.7.4**<br>以前のベリサイン BCP の説明をシマンテック BCP の説明に置き換え。 |
| 更新/リキーが必要になるまでの s/w 認証の有効期間を 2 年から 3 年に延長。 | **6.3.2**<br>**証明書の発行者:** / **有効期間**<br>オンラインの CA からエンドユーザー個人利用者へ / 通常は最長 ~~2~~3 年間。[1]ただし、以下の場合には最長 6 年間。この場合、更新やリキーは選択できません。6 年経過後は新規申請が必要になります。<br><br>エンドユーザー利用者に対して CA が発行した証明書は、以下の要件を満たす場合、~~2~~3 年を越える運用期間 (最長 6 年) を有することができます。<br>• 組織向け証明書の運用環境に関係する利用者鍵ペアが保護され、データ センターの高度な保護が適用された中で運用されること。個人向けの証明書は、利用者の鍵ペアがスマートカードなどのハードウェア トークンに格納されること。 |

**変更履歴:バージョン 3.8.6**

| 説明 | セクション & 変更内容 |
|---|---|
| 古い 1024 ビット CA 鍵の有効期限を 14 年以上に延長し、最長有効期間の 2012 年 8 月 31 日までに制限し、2011 年 12 月 31 日までに限って利用可能とする | **6.1.5**<br>最小鍵サイズについてのシマンテック標準は、PCA と CA の場合、2048 ビットの RSA と同等の強度を持つ鍵ペアを使用することです。<br>[1] 旧式のプラットフォームを使用するカスタマをサポートするため、CA の信頼性は 1024 ビットの RSA 鍵ペアを使用するシマンテックの第 1 世代 (G1) および第 2 世代 (G2) の旧式の信頼されるルートまで拡張されています。1024 ビットの RSA 鍵ペアを使用するエンドエンティティ証明書は、有効期間が 2011 年 12 |

[1] 有効期間が 6 年のエンドユーザー利用者証明書が発行される場合、オンライン CA 証明書の運用期間は、更新オプションなしで 10 年になります。5 年経過後に CA のリキーが要求されます。

| 説明 | セクション & 変更内容 |
|---|---|
| 例外。 | 月 31 日までのものであれば発行できます。また、2011 年以降も旧式アプリケーションを使用した業務継続を保持することについて事前承認を受けた上で、セクション 6.3.2 に従って、プロセッシング センターのソフトウェア機能を操作するシマンテックの関連会社に対しても個別に例外として許可できます。<br><br>**6.3.2**<br>STN CP のセクション 6.3.2 の規定に関して、シマンテック PMA は、CA 鍵ペアの移行中に PKI Service が中断しないように、例外措置として、限定数の CA において規定上限を超える有効期間の適用を承認します。この例外措置は、SSL 証明書を発行する CA に関与していないインフラストラクチャ、管理用 CA に対してのみプロセッシング センターのソフトウェア機能を運用しているシマンテックの関連会社に適用できます。ただし、この例外措置は、最長で ~~2014 年 4 月 30 日~~ 2014 年 8 月 31 日までとし、CA の有効期間を延長して合計で ~~13~~14 年を超えてしまう場合は適用できず、さらに ~~2011 年 4 月 30 日~~ 2011 年 12 月 31 日以降は使用できないものとします。 |

**変更履歴:バージョン 3.8.5**

| 説明 | セクション & 変更内容 |
|---|---|
| ベリサインからシマンテックへの移行 (名称、URL、電子メール アドレスを含む) | 文書全体、<br>名称:ベリサインをシマンテック に変更<br>ベリサイン トラスト ネットワーク (VeriSign Trust Network、VTN) を シマンテック トラスト ネットワーク (Symantec Trust Network、STN) に変更<br>URL:verisign.com を symantec.com に変更<br>電子メール アドレス:verisign.com を symantec.com に変更 |
| 古い証明書に記載されている DN 名は、現在は新しい所有者を表します。 | **セクション 3.1.1**<br>*現在、STN はシマンテック所有となっていますが (ii ページの「買収に関するお知らせ」を参照)、以前発行された証明書は当時の所有者の名前とブランドで発行されています。該当する証明書には組織名 (O) 行に "VeriSign, Inc."、部門名 (OU) に "VeriSign Trust Network" が記載されていますが、それぞれ「Symantec Corporation」および「Symantec Trust Network」を意味するものとします。* |
| 個人向けコードサイニング証明書の許可権限の変更 | **セクション 3.1.1**<br>OU = "No organization affiliation" (個人に発行されるコードサイニング証明書)<br>CN = 個人の名前 (個人向け証明書、または個人に発行されるコードサイニング証明書の場合)。 |
| シマンテック内部の目的で発行される Class 2 証明書の DN 名 | **セクション 3.1.1** 脚注の追加。<br>組織 (O) = "Symantec Corporation" (OCSP レスポンダの場合、およびオプションで組織と関連のない個人向け証明書 [8]の場合)<br>[8] シマンテックの場合、Class 2 証明書の承認された特定の場合において、内部用途のための内部情報を含む接尾語が O の値に追加されることがあります。シマンテックは、"Symantec Corporation – " <接尾語> (例: Symantec Corporation – Build 5315) という形式で記載された組織名について、正式なエンティティとしてシマンテックを正確に表すことを証明します。<br><br>部門名 (OU) = 証明書のタイプを説明する記載 [9]<br>[9] 承認された特定の状況において、内部用途のための Class 2 証明書が発行される場合があります。かかる証明書では、DN および OU の値にシマンテックの組織名が含まれますが、意図された内部用途以外で証明書を使用する場合に特有の信頼性に欠ける値になるものとします。 |
| Magnum リリースでの自己失効の中止。 | **セクション 3.4**<br>特定の証明書タイプの利用者に自身のチャレンジ フレーズ (またはこれと同等なもの) を提示してもらい、記録されているチャレンジ フレーズ (またはこれと同等なもの) と一致した場合には、自動的に証明書が失効します (注: このオプションは必ずしもすべてのカスタマが利用できるとは限りません)。<br>**セクション 4.9.2**<br>個人の利用者は、自身の個人向け証明書の失効について、シマンテックまたは RA の正式な代表者を通じて要求できます。 |
| 復元された鍵を失効する条件の明確化。 | **セクション 4.12.1**<br>紛失した証明書の使用を中止するなどの特定の状況においては、暗号化鍵を復元する前に、利用者の鍵ペアを失効させる。 |
| 「シマンテック」の RA のみに対する制限の削除。要件を全体に適用。 | **セクション 6.2.9**<br>~~シマンテック~~ RA 秘密鍵 (RA 申請を認証するために使用されたもの) は、システムをログオフするとアクティベーションが解除されます。~~シマンテック~~ RA は、作業場所を離れる際に自身のワークステーションをログオフすることが要求されます。 |

| 説明 | セクション & 変更内容 |
|---|---|
| | **セクション 6.4.2:**<br>~~シマンテック~~ RA は、その管理者/RA の秘密鍵を、パスワード保護とブラウザの「高セキュリティ」オプションを使用して、暗号化された形式で格納することが要求されます。 |
| CA の有効期間を 13 年以上に延長する例外を、最長で 2014 年 4 月 30 日までに制限。 | **セクション 6.3.2**<br>シマンテック PMA は、CA 鍵ペアの移行中に PKI Service が中断しないように、例外措置として、限定数の CA において規定上限を超える有効期間の適用を承認します。ただし、この例外措置は、最長で 2014 年 4 月 30 日までとし、CA の有効期間を延長して合計で 13 年を超えてしまう場合は適用できず、さらに 2011 年 4 月 30 日以降は使用できないものとします。 |
| PC ソフトウェアの EAL-4 証明書の文書の削除。 | **セクション 6.5.2**<br>~~シマンテックの中核的ソフトウェアであるプロセッシング センターの 1 バージョンは、プロセッシング センターのセキュリティ ターゲットに対して独立研究所が実施したコモン クライテリアの評価に基づき、ISO/IEC 15408-3:1999, *情報技術 – セキュリティ技法 – IT セキュリティのための評価基準 – パート 3: セキュリティ保証要件*の EAL 4 の保証の要件を満たしました。シマンテックは、プロセッシング センター ソフトウェアの新リリースを、コモン クライテリアに従って随時評価することがあります。~~規定されません。 |
| EKU および対応する重大度 (Criticality) の更新。 | **セクション 7.1.2.1**<br>表 6、および表の説明文を削除。<br>**セクション 7.1.2.5**<br>表 7、および表の説明文を削除。 |
| 利用者証明書について BasicConstraints 設定に変更。 | **セクション 7.1.2.4。**<br>エンドユーザー利用者証明書における BasicConstraints エクステンションは、CA フィールドが「FALSE」に設定されるものとします~~空のシーケンスの値に設定されるものとします。~~。このエクステンションの重大度 (Criticality) フィールドは、CA 証明書の場合は「TRUE」に設定されますが、~~そうでない場合は「FALSE」に設定されます~~エンドユーザー利用者証明書の場合は「TRUE」と「FALSE」のいずれかに設定できます。 |
| | |

**変更履歴:バージョン 3.8.4**

| 説明 | セクション & 変更内容 |
|---|---|
| 用途に応じた Class 3 証明書の公開の修正。 | **セクション 2.2、表 3:**<br>***証明書タイプ*** / ***公開の要件***<br>エンドユーザー利用者証明書 (用途に応じて、特定の Class 3 証明書を除く)。 / ベリサイン® リポジトリ (*https://digitalid.verisign.com/services/client/index.html*) のクエリー機能、および LDAP ディレクトリ サーバー (*directory.Symantec.com*) のクエリーを通じて、任意で公開され、依拠当事者が利用可能になります。ただし、ベリサイン® リポジトリ (*https://digitalid.verisign.com/services/server/search.htm*) のクエリー機能を通じて利用できる Class 3 SSL およびコードサイニング証明書は除きます。<br>**セクション 4.9.9:**<br>証明書ステータス情報を確認できる Web ベースのクエリー機能には、以下のベリサイン® リポジトリからアクセスできます。<br>• *https://digitalid.verisign.com/services/client/index.html* (個人向け証明書の場合)<br>*https://digitalid.verisign.com/services/server/search.htm* (SSL およびコードサイニング~~サーバーおよび開発者~~証明書の場合)。 |
| Public Lite アカウントの subjAltName における電子メール アドレス除外の例外 | **セクション 7.1.2.3**<br>X.509 バージョン 3 証明書の subjectAltName エクステンションは、RFC 5280 に従って設定されます。ただし、Public Lite アカウントで発行される証明書については、オプションで *SubjAltName* に電子メール アドレスが含まれないことがあります。このエクステンションの重大度 (Criticality) フィールドは、「FALSE」に設定されるものとします。 |
| 2010 年 12 月 31 日以前に計画される移行のすべての説明を削除するポリシーの更新。<br>識別された個別の例外を脚注に追加。 | **6.1.5 鍵サイズ**<br>最小鍵サイズについてのシマンテック標準は、PCA と CA の場合、2048 ビットの RSA と同等の強度を持つ鍵ペアを使用することです。[15]<br>~~シマンテックの第 1 世代および第 2 世代 (G1 および G2) の PCA と CA は、1024 ビットの RSA 鍵ペアを含み、~~シマンテックの第 3 および第 4 世代 (G3 および G5) の PCA は、2048 ビットの RSA 鍵ペアを含みます。~~RSA 鍵ペアを使用するすべてのクラスのシマンテック証明書に対する署名は、2013 年 12 月 31 日までに少なくとも 2048 ビット (または同等) の鍵サイズを使用するルートに移行するものとしま~~ |

<table>
<tr><th>説明</th><th>セクション ＆ 変更内容</th></tr>
<tr><td></td><td>~~す。~~<br>シマンテックは、RA および利用者証明書の鍵ペアに最低でも 2048 ビット の RSA と同等の強度の鍵サイズ~~を使用することを推奨しますを~~発行します。~~シマンテックは、すべての 1024 ビット RSA を 2013 年 12 月 31 日までに廃止します。~~<br>例外に関する脚注の追加:<br>[15] 旧式のプラットフォームを使用するカスタマをサポートするため、CA の信頼性は 1024 ビットの RSA 鍵ペアを使用するシマンテックの第 1 世代 (G1) および第 2 世代 (G2) の旧式の信頼されるルートまで拡張されています。1024 ビットの RSA 鍵ペアを使用するエンドエンティティ証明書は、有効期間が 2011 年 12 月 31 日までのものであれば発行できます。旧式アプリケーションによる業務継続を維持する目的であると事前に承認を得た場合に、さらなる個別の例外が許可されます。<br><br>付属 B2 (EV 証明書)<br>ルート、下位 CA、および利用者証明書は、次の事項を反映。<br><table><tr><th></th><th>~~2010 年 12 月 31 日以前に発行された証明書~~</th><th></th></tr><tr><td>ダイジェスト アルゴリズム</td><td>~~SHA-1~~</td><td>SHA-1* 、SHA-256 、SHA-384 、または SHA-512</td></tr><tr><td>RSA</td><td>~~2048 または 2048 ビット~~</td><td>2048 ビット</td></tr><tr><td>ECC</td><td>~~256 または 384 ビット~~</td><td>256 または 384 ビット</td></tr></table>*SHA-1 は、SHA-256 が依拠当事者の大多数が使用するブラウザで広くサポートされるようになるまで、使用される~~べきです~~ものとします。</td></tr>
<tr><td>例外に特定された CA についての更新</td><td>セクション 6.3.2<br>サービスが終了している「CL3 Organizational VIP Device CA」を削除。<br>~~シマンテックは「Symantec® Class 3 Organizational VIP Device CA」を運用します。この CA が発行した組織利用者証明書については、以下の状況に該当する場合に、3 年を超えて最大 5 年の有効期間を設定できます。~~<br>~~• 証明書の鍵ペアがハードウェアに格納される、および~~<br>~~• シマンテックが本 CPS の規定に従って組織を認証した、および~~<br>~~SSL/TLS を使用するサーバーの保護に使用される場合に、サーバーへのアクセス経路がプライベートネットワークまたはイントラネットに限られる。~~<br>10 年を超える有効期間の例外として、「CL 3 Onsite Enterprise Admin CA – G2」を追加 (脚注 17)<br>ベリサイン® Onsite Administrator CA-Class 3、Class 3 Secure Server Operational Administrator CA、および Class 3 OnSite Enterprise Administrator CA – G2 は、旧式システムのサポートのために 10 年を超える有効期間がありますが、適切な時期に失効されるものとします。</td></tr>
<tr><td colspan="2">自動更新される 6 年の証明書有効期間、およびエンタープライズおよびクライアント PKI の 6 年の証明書有効期間の変更</td></tr>
<tr><td>DN の再認証は「証明書のリキー」イベントを伴わずに周期的に発生。</td><td>セクション 3.3.1<br>特に、リテール Class 3 組織向け SSL 証明書~~についての後続のリキー要求~~の場合、シマンテックは、証明書に含まれる組織名およびドメイン名の再認証をセクション 6.3.2 に記載の間隔で行います。</td></tr>
<tr><td>DN の再認証は「証明書の更新」イベントを伴わずに周期的に発生。</td><td>セクション 4.6.3<br>特に、リテール Class 3 組織向け SSL 証明書~~についての後続の更新要求~~の場合、シマンテックは、証明書に含まれる組織名およびドメイン名の再認証をセクション 6.3.2 に記載の間隔で行います。</td></tr>
<tr><td>自動更新プロセスのための証明書失効の新しい条件を 2 つ追加。</td><td>セクション 4.9.1<br>エンドユーザー利用者証明書は、次のいずれかの事由が生じた場合に失効されます。(2 項目を追加)<br>• セクション 6.3.2 に規定された方法で、利用者の識別情報が再確認できなかった場合<br>• 利用者が期限までに利用料を支払わなかった場合</td></tr>
<tr><td>オンライン CA の 6 年有効の証明書は、10 年の有効期間を設定する必要がある。<br>有効期間が 10 年の CA は 5 年後にリキーが必要。</td><td>セクション 6.3.2、表 8 および脚注 18<br><table><tr><th>証明書の発行者</th><th>有効期間</th></tr><tr><td>オフラインの中間 CA からオンラインの CA へ</td><td>通常 5 年間。ただし、更新後は最長 10 年間 [18]</td></tr></table>[18]~~6~~5 年のエンドユーザー利用者証明書が発行される場合、オンライン CA 証明書の運用期間は、更新オプションなしで 10 年になります。5 年経過後に CA のリキーが要求されます。</td></tr>
<tr><td>証明書の 6 年の有効期間終了時に利用者証明書の再申請が必要。<br>有効期間が 10 年の CA</td><td>表 8 および脚注 19<br><table><tr><th>証明書の発行者</th><th>有効期間</th></tr><tr><td>オンラインの CA からエ</td><td>ただし、以下の場合には最長 ~~6~~5 年間。[19] この場合、</td></tr></table></td></tr>
</table>

| 説明 | セクション & 変更内容 |
|---|---|
| は 5 年後にリキーが必要。 | ンドユーザー個人利用者へ: 更新やリキーは選択できません。6 年経過後は新規申請が必要になります。<br>[19]~~65~~ 年のエンドユーザー利用者証明書が発行される場合、オンライン CA 証明書の運用期間は、更新オプションなしで 10 年になります。5 年経過後に CA のリキーが要求されます。 |
| 有効期間が 6 年の証明書は 3 年後に再確認が必要。 | **セクション 6.3.2、表 8 および脚注 20**<br>証明書の発行者: オンラインの CA からエンドユーザー組織利用者へ<br>有効期間: 通常最長 ~~65~~ 年間。[20] この場合、更新やリキーは選択できません。6 年経過後は新規申請が必要になります。<br>[20] 少なくとも、~~4 年または 5 年の有効期間を持つ SSL~~ 有効期間が 3 年を超える証明書の識別名は、証明書の発行日から 3 年経過後に再確認されます。ベリサイン® 自動承認証明書を除き、VTN の一部の運用をサポートするためだけに使用される組織用エンドエンティティ証明書に関しては、有効期間が 5 年のものを発行でき、更新後は最長 10 年とすることができます。 |
| 有効期間が 6 年の証明書に適用される制限の明確化 | **セクション 6.3.2**<br>エンドユーザー利用者に対して CA が発行した証明書は、以下の要件を満たす場合、2 年を越える運用期間 (最長 ~~5~~6 年) を有することができます。<br>• ~~証明書が個人向け証明書である。~~<br>• 組織向け証明書の運用環境に関係する利用者鍵ペアが保護され、データ センターの高度な保護が適用されて運用されること。個人向けの証明書は、利用者の鍵ペアがスマート カードなどのハードウェア トークンに格納されること。<br>• セクション 3.2.3 の規定に従い、利用者は最低 3 年 ~~25 か月~~ごとに再認証を受けること。<br>• セクション 3.2.3 の規定に従い、利用者は、証明書に含まれる公開鍵に対応する秘密鍵の所有を最低 25 か月ごとに証明するものとする。<br>• 利用者が再認証手続きを完了できない場合、または上記の要求が行われた場合にかかる秘密鍵の所持を証明できない場合、CA は利用者の証明書を失効させるものとします。 |

**変更履歴:バージョン 3.8.3**

| 説明 | セクション & 変更内容 |
|---|---|
| 商標表示の更新、および買収に関するお知らせの追加。 | ii ページ。 |
| シマンテックの買収および VTN CA サービスに対する所有権を明確にするよう変更。 | ドキュメント全体:<br>• 企業の所有者および連絡先方法をシマンテックに変更。<br>• CA 名と VTN ブランドは、ブランド名変更が可能となるまでは引き続きベリサインの名称を反映。 |
| 準拠法および資産およびプライバシー プランをシマンテックの所有に対応させて変更。 | セクション 9.2.2、9.14、9.13.2、および 9.4.1 |
| ベリサインのローミング サービス (販売中止)について削除 | セクション 6.2.8.2、6.2.8.3、および付録 A |
| Certificate Interoperability Service (CIS) (販売中止) への参照について削除 | セクション 3.2.6、脚注 |
| TGV サービスの明確化 | セクション 7.3 |
| 証明書有効期間の例外に必要なシマンテックの承認の明確化 | セクション 6.3.2、脚注 16 |

**変更履歴:バージョン 3.8.2**

| 説明 | セクション & 変更内容 |
|---|---|
| CA の移行、鍵サイズ、および Universal Root の記述の変更 | **1.3.1 認証機関**<br>ベリサインは「VeriSign Universal Root Certification Authority」および「VeriSign ECC Universal Root Certification Authority」も運用しています。VeriSign Universal Root CA は、特定の証明書クラスで定義されるのではなく、下位 CA の任意のクラスの証明書を発行できる認証機関です。 |
| RSA:<br>• ルートと CA は 2013 年 12 月 31 日付で 2048 ビットに | **6.1.5 鍵サイズ**<br>鍵ペアは、予定使用期間においては、暗号解読技術を使用して鍵ペアの秘密鍵が他者に解かれないように十分な長さにするものとします。最小鍵サイズについてのベリサイン標準は、PCA と CA の場合、1000 ビット RSA の鍵ペアを使用する古い Secure Server CA を除いて、10242048 ビットの RSA と同等の |

| 説明 | セクション & 変更内容 |
|---|---|
| 移行。<br>• EV 証明書は 2010 年 12 月 31 日付で 2048 ビットに移行。<br>• RA と EE は 2048 ビットの生成を推奨されるが、1024 ビットも引き続き承認される。ただし、すべての 1024 ビット RSA は 2013 年 12 月 31 日までに終了。<br><br>ECC:<br>• 384 ビット ECC CL3PCA-G4 は Universal Root。<br><br>アルゴリズム:<br>-SHA-1&256 (RSA を使用)<br>-SHA-256&384 (ECC を使用)<br>- MD5 は事前合意がある場合のみ<br>-MD2 は使用しない | 強度を持つ鍵ペアを使用することです。<br><br>ベリサインの第 1 および第 2 世代 (G1 および G2) の PCA と CA は、1024 ビットの RSA 鍵ペアを含み、シマンテックの第 3 および第 4 世代(G3 および G5) の PCA は、2048 ビットの RSA 鍵ペアを含みます。RSA 鍵ペアを使用するすべてのクラスのベリサイン証明書に対する署名は、2013 年 12 月 31 日までに少なくとも 2048 ビット (または同等) の鍵サイズを使用するルートに移行するものとします。<br><br>ベリサインは、RA および利用者証明書の鍵ペアに最低でも 2048 ビット の RSA と同等の強度の鍵サイズを使用することを推奨します。ベリサインは、2048 ビット未満の鍵ペアの RSA を使用して生成される利用者証明書の一部を引き続き承認しますが、すべての 1024 ビット RSA の使用を 2013 年 12 月 31 日までに終了します。ベリサインは、登録機関およびエンドユーザー利用者が 1024 ビットの RSA 鍵ペアを生成することを推奨します。ベリサインは、512 ビット未満の鍵ペアを使用して生成される利用者証明書の一部を承認しません。<br><br>ベリサインの ECC Universal Root CA および第 4 世代 (G4) の Class 3 PCA は、384 ビット ECC を使用します。<br><br>PCA と CA のすべてのクラス、RA、およびエンドエンティティ証明書では、電子署名ハッシュ アルゴリズムに SHA-1 と SHA-2 のいずれかが使用されます。また、特定バージョンのベリサイン プロセッシング センターでは、エンドエンティティ利用者証明書において SHA-256、SHA-384、および SHA-512 の暗号化アルゴリズムの使用をサポートしています。 |
| | **6.3.2 証明書の運用期間および鍵ペアの使用期間**<br>*表 4:*<br>PCA 自己署名 (1024 ビット RSA) - 最長 30 年<br>PCA 自己署名 (1024 ビット RSA) - 最長 30 年<br>PCA 自己署名 (256 ビット ECC) - 最長 30 年<br>PCA 自己署名 (384 ビット ECC) - 最長 30 年<br><br>および:<br>ベリサインは、PCA によって署名されるオンライン CA である「VeriSign Class 3 International Server CA」、「Thawte SGC CA」、および「Class 3 Open Financial Exchange CA-G2」も運用します。これら CA の有効期間は、SGC および OFX の機能を提供する証明書の継続的な相互運用性を確保するため、表 8 に記載した有効期間を延長させることができます。 |
| | **7.1.3 アルゴリズムのオブジェクト識別子**<br>• ***sha256withRSAEncryption*** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}<br>• ***ecdsa-with-Sha256*** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2}<br>• ***ecdsa-with-Sha384*** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 3}<br>• ***sha-1WithRSAEncryption*** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}<br>• ***md5WithRSAEncryption*** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 4}<br>• ***md2WithRSAEncryption*** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 2}<br>***md5WithRSAEncryption*** よりも、***sha-1WithRSAEncryption*** または ***sha-256WithRSAEncryption*** のいずれかが優先的に使用されます**が使用されます** ***md2WithRSAEncryption*** は、利用者証明書の署名には使用されなくなりましたが、一部の古い CA およびエンドユーザー利用者証明書の CRL については署名に使用されます。<br>脚注の追加:<br>*****md5WithRSAEncryption*** が使用されるのは、旧式アプリケーションによる業務継続を維持する目的であると事前に承認を得た場合のみです。 |
| | **7.2 CRL のプロファイル**<br>署名アルゴリズム - CRL の署名に使用されるアルゴリズム。ベリサイン CRL は、RFC 3279 に従い、sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) または md5WithRSAEncryption (OID: 1.2.840.113549.1.1.4) を使用して署名されます。(CP セクション 7.1.3 を参照) |
| | **付録 B2**<br>ECC 224、233、256、または 283 384 ビット |
| リモートからホストされる | **4.12 鍵の預託と復元**<br>Managed PKI Key Management Service (KMS) を使用するエンタープライズ カスタマは、自身が承認す |

| 説明 | セクション & 変更内容 |
|---|---|
| KMS KMS – カスタマが自らの施設でリモートからKMS および KMD をホストするオプションを提供します。 | る証明書申請を行った利用者の秘密鍵のコピーを預託できます。エンタープライズ カスタマは、企業施設内またはベリサインの安全なデータ センター内で運用される KMS を使用できます。企業施設外で運用される場合、ベリサインは、利用者の秘密鍵のコピーを保管しませんが、利用者の鍵復元処理において重要な役割を果たします。 |
| | **4.12.2 セッション キーのカプセル化、および復元のポリシー実施方法**<br>秘密鍵は、企業施設内で暗号化された形式にて Key Manager データベースで保管されます。各利用者の秘密鍵は、独自のトリプル DES 対称鍵で個別に暗号化されます。Key Escrow Record (KER) が生成され、次にトリプル DES 鍵がランダム セッション キーと結合され、ハードウェアで生成され破棄されたセッション キー マスク (MSK) を形成します。結果として生じた MSK は、証明書要求情報と共に、ベリサインの Managed PKI データベースに安全な方法で送信され、保管されます。KER (エンドユーザーの秘密鍵を含む) と個々のセッション キーは、Key Manager データベースに保管され、それ以外の鍵関連データはすべて破棄されます。<br><br>Managed PKI データベースは、ベリサインの安全なデータ センターから運用されます。エンタープライズ カスタマは、Key Manager データベースの運用場所として、自社内またはベリサインの安全なデータ センターのいずれかを選択できます。<br><br>秘密鍵および電子証明書を復元する際には、Managed PKI 管理者が安全な方法で Managed PKI Control Center にログインし、復元する鍵ペアを適切に選択して、[Recover] のハイパーリンクをクリックする必要があります。承認された管理者が [Recover] リンクをクリックした場合にのみ、当該鍵ペアの MSK が、ベリサインの安全なデータ センターから運用される Managed PKI データベースから返されます。Key Manager は、KMD からセッション キーを取り出して MSK と結合させ、MSK とランダム セッション キー マスクを結合させて、最初に秘密鍵を暗号化するのに使用されたトリプル DES 鍵を再生成し、エンドユーザーの秘密鍵の復元を可能にします。最後に、暗号化された PKCS#12 ファイルが管理者へ返され、最終的にエンドユーザーに配布されます。<br><br>脚注 15 の削除:<br>限られた状況において、またエンタープライズ サービス契約に明確に許可されている場合にのみ、ベリサインは企業の Key Management Service、および関連する預託された秘密鍵をホストできます。 |
| | **5.2.2 職務ごとに必要とされる人数**<br>Class 3 証明書の検証および発行など、自動的な検証/発行システムの対象外となるその他の手動での業務は、2 名以上の信頼される者によって、または 1 名以上の信頼される者と自動的な検証/発行プロセスを組み合わせることによって行われます。鍵復元を手動で行う場合は、オプションで、許可された 2 名の管理者による検証を必須にすることができます。 |
| | **5.2.4 職務の分離を必要とする役割**<br>職務の分離を要求する役割には以下のものがあります (ただし、これらに限定されません)。<br>• 証明書申請における情報の検証<br>• 証明書の申請、失効要求、鍵復元要求、更新要求、または申請情報に対する承認、否認、またはその他の処理 |
| Class 3 管理者 (従業員である必要はない) の ID 証明の修正 | **3.2.3 個人の識別情報**<br>Class 3 の管理者証明書は、組織の認証、および管理者として行動する個人の識別情報雇用についての組織からの確認を含むものとします。<br><br>脚注 5:<br>証明書申請において管理者として指定された、サービスの管理者証明書を申請している人物の識別情報雇用の承認の確認 |
| 付録 B3 | 利用者証明書のエクステンションのリストに SAN を明確に追加:<br>SubjectAltName:存在する場合は、RFC5280 に従って設定され、重要度 (Criticality) が FALSE に設定されます。 |
| セクション 3.2.3 | NF SSP CA のポリシー機関名を修正。 |

**変更履歴:バージョン 3.8.1**

| セクション | 説明 |
|---|---|
| セクション 6.3.2、脚注 20 | 追加:「ベリサイン自動承認証明書を除き…」 |
| 付録 B1、セクション 8 | 最長有効期間を 1 年から 13 か月に更新 |
| 付録 B1、セクション 22(d)(3) | セクション 22(d)(3) を作成 |

| | |
|---|---|
| 付録 B1、セクション 25 | 削除:「EV 証明書を更新する前に、更新要求が申請者により適切に承認され、EV 証明書に表示される情報が現在でも正確かつ有効であることを保証するため、ベリサインはガイドラインおよび本手続きで求められるすべての認証および確認のタスクを実行します。」<br>この項を、発行されている EV 証明書の正誤表に沿う内容に置き換え。また、ガイドラインに沿う更新の定義を挿入。 |
| 付録 B3、セクション 3 | 追加:「(f) extKeyUsage」 |
| 付録 B1-B4、およびドキュメント全体 | RFC 3280 への参照をすべて RFC 5280 に置き換え |

**変更履歴:バージョン 3.8**

| セクション | 説明 |
|---|---|
| セクション 6.3.2、表 8 | エンドエンティティ組織利用者向けオンライン CA の有効期間を 3 年から 5 年に更新。<br><br>脚注 17。脚注を更新して「Class 3 Secure Server Operational Administrator CA」を追加<br><br>脚注 20。少なくとも、有効期間が 3 年を超える証明書の識別名は、証明書の発行日から 3 年経過後に再確認されます。 |

**変更履歴:バージョン 3.7**

| セクション | 説明 |
|---|---|
| セクション 1.3.1 | 追加:「ベリサインは「VeriSign Universal Root Certification Authority」も運用しています。VeriSign Universal Root Certification Authority は特定の認証クラスで定義されず、任意のクラスの下位 CA を発行できます。」 |
| セクション 6.3.2 | 削除:「ベリサインは VeriSign Class 3 International Server CA も運用しています。これは、PCA によって署名されたオンライン CA です。この CA の有効期間は、SGC/セットアップ技術に関するブラウザ ベンダーとの契約上の義務を満たし、この機能を提供する証明書の継続的な相互運用性を保証するために、表 8 に記載した有効期間を超えることがあります。」<br><br>追加:「ベリサインは、PCA によって署名されるオンライン CA である「VeriSign Class 3 International Server CA」、および「Class 3 Open Financial Exchange CA - G2」も運用します。これら CA の有効期間は、SGC および OFX の機能を提供する証明書の継続的な相互運用性を確保するため、表 8 に記載した有効期間を延長させることができます。 |
| セクション 6.3.2 | 削除:「この例外について、影響を受ける CA は 2010 年 12 月 31 日以降まで延長しないものとします。」<br>追加:「この例外措置は、CA の有効期間を延長して合計で 13 年を超えてしまう場合は適用できず、さらに 2011 年 4 月 30 日以降は使用できないものとします。 |
| セクション 6.3.2 | 脚注の追加:「証明書の有効期間は、より強固な暗号化アルゴリズムや鍵サイズを使用する証明書については、セクション 6.3.2 で規定されている上限を超えて延長できます (SHA 2 または ECC アルゴリズムや 2048 ビット以上の鍵サイズなど)。 |
| セクション 7.1.3 | 2 個のアルゴリズムを追加:<br>1. sha256withRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}<br><br>2. ecdsa-with-Sha384 OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 3} |
| 付録 B1、セクション 16 (a) | 親会社/子会社の住所確認のために更新 |
| 付録 B1、セクション 5 | 非営利団体のサブジェクトを追加 |
| 付録 B1、セクション 6(a)3 – 表 1 | 追加:非営利団体:V1.0、5.(3) 項 |
| 付録 B1、セクション 14 | 追加:行政機関と非営利団体 |
| 付録 B1、セクション 19 | 事前同等権限を追加 |
| 付録 B4 | 発行されている EV ガイドラインの正誤表に沿って付録 A4 を更新 |
| 定義 | 追加:<br>「国」:<br>「主権国家」: |

| | |
|---|---|
| | 「国際組織」:<br>「親会社」<br>「子会社」を過半数所有会社であり、完全所有会社ではないという定義に更新。 |

**変更履歴:バージョン 3.6**

| セクション | 説明 |
|---|---|
| セクション 4.1.2.1 | 「ベリサインに提供される公開鍵に対応する秘密鍵の所有を示す」から<br>「ベリサインに提示した公開鍵に対応する秘密鍵を所有していること、**または排他的に制御**していることを証明する」に変更。 |
| セクション 6.1.1 | 「ACS アプリケーション ID の場合、シマンテックは、FIPS 140-1 レベル 3 の要件を満たす暗号化モジュールで生成される乱数シードを使用して、利用者の代わりに鍵ペアを生成します。」<br>から<br>「ACS アプリケーション ID の場合、シマンテックは、**少なくとも** FIPS 140-1 レベル 3 の要件を満たす暗号化モジュールで生成される乱数シードを使用して、利用者の代わりに鍵ペアを生成します。」<br>に変更。 |
| セクション 6.2.5 | 削除:「ベリサイン CA 鍵ペアの有効期間が終了すると、このような CA 鍵ペアは少なくとも 5 年間はアーカイブされます。アーカイブされた CA 鍵ペアは、本 CPS の要件を満たすハードウェアの暗号化モジュールを使用して、安全に格納されます。手続きの管理により、アーカイブされた CA 鍵ペアが実稼動環境での使用に戻されないように防止されます。アーカイブ期間が終了すると、アーカイブされた CA 秘密鍵は本 CPS に従って安全に破棄されます。」 |
| セクション 6.3.2 | 追加:「VTN CP のセクション 6.3.2 の規定に関して、ベリサイン PMA は、CA 鍵ペアの移行中に PKI Service が中断しないように、例外措置として、限定数の CA において規定上限を超える有効期間の適用を承認します。この例外について、影響を受ける CA は 2010 年 12 月 31 日以降まで延長しないものとします。」 |
| セクション 7.1 | 「ベリサインの証明書は、(a) ITU-T (国際電気通信連合･電気通信標準化部門) による X.509 勧告 (1997 年): 「Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997」、および (b) RFC 5280: 「Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002」に準拠します。」<br>から<br>「ベリサインの証明書は、**通常、**(a) ITU-T (国際電気通信連合･電気通信標準化部門) による X.509 勧告 (1997 年): 「Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997」、および (b) RFC 5280: 「Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002」に準拠します。」に変更 |
| セクション 7.1.2.1 | 削除:「注: KeyUsage エクステンションに nonRepudiation ビットは設定されていませんが、ベリサインはこれらの証明書向けに否認防止サービスをサポートしています。これらの証明書における nonRepudiation ビットの設定は必須ではありません。PKI 業界において nonRepudiation ビットが意味するところについて意見がまだ一致していないためです。そのような意見統一がなされるまで、nonRepudiation ビットは依拠当事者になる者にとって意味あるものにならない可能性があります。さらに、一般に使用されている大分部のアプリケーションでは、nonRepudiation ビットを適切に扱っているとは言えません。このため、ビットを設定することは、依拠当事者が信頼性に関して判断を下す際の助けになりません。結果的に、本 CPS では nonRepudiation ビットの消去が必要になります。ただし、設定されるケースとしては、Managed PKI Key Manager を使用して発行されるデュアル鍵ペアの署名証明書が考えられます。<br><br>追加:「注: これらの証明書における nonRepudiation ビットの設定は必須ではありません。PKI 業界において nonRepudiation ビットが意味するところについて意見が一致していないためです。そのような意見統一がなされるまで、nonRepudiation ビットは依拠当事者になる者にとって意味あるものにならない可能性があります。さらに、一般に使用されている大分部のアプリケーションでは、必ずしも nonRepudiation ビットを適切に扱っているとは言えません。このため、ビットを設定することは、依拠当事者が信頼性に関して判断を下す際の助けにならないことがあります。従って、本 CPS では nonRepudiation ビットの設定は要求されません。設定されるケースとしては、Managed PKI Key Manager を使用して発行されるデュアル鍵ペアの署名証明書や、要求された場合が考えられます。電子証明書の使用に起因する否認防止に関連する争議については、利用者と依拠当事者間のみの問題となります。ベリサインは当該争議に関する一切の責任を負わないものとします。<br><br>脚注の追加:「nonRepudiation ビットは、X.509 規格に従って、電子証明書において ContentCommitment として参照される場合があります。」 |
| セクション 9.13.2 | 管轄地をカリフォルニア州サンタ クララ郡からバージニア州フェアファックス郡に更新 |
| セクション 9.14 | 準拠法をカリフォルニア州からバージニア州に更新 |

**変更履歴:バージョン 3.5**

| | |
|---|---|
| セクション 6.2.5 | 削除:「ベリサイン CA 鍵ペアの有効期間が終了すると、このような CA 鍵ペアは少なくとも 5 年間はアーカイブされます。アーカイブされた CA 鍵ペアは、本 CPS の要件を満たすハードウェアの暗号化モジュールを使用して、安全に |

| | |
|---|---|
| | 格納されます。手続きの管理により、アーカイブされた CA 鍵ペアが実稼動環境での使用に戻されないように防止されます。アーカイブ期間が終了すると、アーカイブされた CA 秘密鍵は本 CPS に従って安全に破棄されます。」<br><br>追加:「ベリサイン CA 証明書の有効期間が満了すると、その証明書に関連付いている鍵ペアは、本 CPS の要件を満たすハードウェア暗号化モジュールを使用して、最低 5 年間は安全に保持されます。これら CA 鍵ペアは、CA 証明書が本 CPS に従って更新されなければ、有効期間の満了に伴い、署名に使用されなくなるものとします。」 |
| セクション 6.2.10 | 削除:「ベリサイン CA の運用期間終了時には、CA 秘密鍵の 1 つ以上のコピーが CPS §6.2.5 に沿ってアーカイブされます。CA 秘密鍵の残りのコピーは安全に破棄されます。さらに、アーカイブされた CA 秘密鍵はアーカイブ期間終了時に安全に破棄されます。CA の鍵の破壊を実施する際には、複数の信頼できる個人の参加が必要とされます。」 |
| セクション 6.3.2 | 追加:「既存の利用者証明書の更新によって得られたエンドユーザー利用者証明書は、有効期間が長い場合があります (最長 3 か月)。」 |
| セクション 6.3.2、表 8 | 「エンドエンティティ組織利用者向けオンライン CA」を更新し、「通常は最長 3 年」の有効期間を反映。 |
| セクション 7.1.4 | 依拠当事者規約が policy エクステンションからリンクされている限りにおいて、依拠当事者規約のサブジェクト名へのポインターとなる OU は任意であることを明確化。 |
| セクション 9.8 | Netsure の損害賠償額の上限を 50,000 米ドルから 250,000 米ドルに更新。1,000 米ドルから 1,000,000.00 米ドルに |
| 定義 | 「NetSure プロテクション プラン」:CPS セクションへの参照を修正して定義を更新。<br>追加:「代表者」、「子会社」、「登録機関」 |
| 付録 B1-B4 | CA/ブラウザ フォーラムが発行する EV ガイドラインのバージョン 1.0 に沿って EV 手続きを更新。 |

**変更履歴:バージョン 3.4**

| | |
|---|---|
| セクション 1.1 | 脚注の追加:「Authenticated Content Signing (ACS) 証明書は、VTN 以外の CA によって発行されます。ただし、ACS 利用者が ACS 証明書で使用される所定の手続きの違いを理解できるように、このベリサイン CPS の一部のセクションで ACS 証明書について言及しています。」 |
| セクション 3.2.3、表 7 | 非連邦エンティティ向けの Shared Service Provider 証明書の確認要件を追加:「証明書利用者の識別情報は、実質上、米国国土安全保障省 PKI (Public Key Infrastructure) 向けの X.509 証明書ポリシーに従って行われます。」 |
| セクション 3.3.1 | チャレンジ フレーズの代替として、企業担当者の確認された電子メール アドレスからの応答を追加 |
| セクション 4.6.3 | チャレンジ フレーズの代替として、企業担当者の確認された電子メール アドレスからの応答を追加 |
| セクション 4.9.7 | 削除:「CA 証明書の CRL は少なくとも四半期ごとに発行するものとします。」<br>追加:「CA 証明書の CRL は少なくとも毎年発行するものとします。」 |
| セクション 6.3.2 | 追加:「ベリサインは VeriSign Class 3 International Server CA も運用しています。これは、PCA によって署名されたオンライン CA です。この CA の有効期間は、SGC/セットアップ技術に関するブラウザ ベンダーとの契約上の義務を満たし、この機能を提供する証明書の継続的な相互運用性を保証するために、表 8 に記載した有効期間を超えることがあります。」 |
| セクション 7.1.2.1 | 更新して指定:「KeyUsage エクステンションの重大度 (Criticality) フィールドは、通常 CA 証明書の場合は「TRUE」に設定され、エンドエンティティ利用者証明書の場合は「TRUE」と「FALSE」のいずれかに設定できます。」 |
| セクション 7.1.2.1 - 表 10 | CA の重大度 (Criticality) を「FALSE」から「TRUE」に更新 |
| セクション 9.3.3 | 追加:「ベリサインは、第三者に漏えいおよび開示されないよう機密情報を保護します。」 |
| 定義 | 削除:「関連会社監査プログラム ガイド」 |

**変更履歴:バージョン 3.3**

| | |
|---|---|
| セクション 1 | 追加:「本 CPS は、CP および CPS の構成について Internet Engineering Task Force (IETF) RFC 3647 に従います。」 |
| セクション 1.4.1.2 - 表 2 | 追加:保証のレベルが高の |
| セクション 1.4.1.3 | 追加:「**保証のレベルが高の証明書 (EV 証明書)** は、『Guidelines for Extended Validation Certificates』に従ってベリサインが発行する Class 3 証明書です。」 |
| セクション 2.2 - 表 3 | 追加:「VeriSign Class 3 Organizational VIP Device CA」によって発行されたエンドユーザー利用者証明書は、パブリック クエリーを使用して利用できません。 |
| セクション 3.1.1 | 追加:「EV SSL 証明書の項目とプロファイル要件については、本 CPS の付録 B3 のセクション 6 に記載されています。」 |
| セクション 3.2.2 – 表 6 | 追加:「ベリサインにおける EV SSL 証明書の発行手続きは、本 CPS の付録 B1 に記載されています。」 |
| セクション 3.2.6 | 脚注の追加:「ベリサインの Certificate Interoperability Service (CIS) は、Certificate Interoperability Service (CIS) CP の補足に従って、自らの CPS を持つことを奨励されますが、これは必須ではありません。ただし、いかなる場合も、ベリサインのリポジトリで発効されるベリサインの Certificate Interoperability Service (CIS) CP の補足に準 |

| | |
|---|---|
| | 拠しなければなりません。」 |
| セクション 3.3.1 | 削除:「特に、リテール Class 3 組織向け証明書についての後続の更新要求の場合、ベリサインは、証明書に含まれる組織名およびドメイン名の再認証を行います。次の状況では…」<br><br>追加:「特に、リテール Class 3 組織向け証明書についての、www.verisign.com からの後続のリキー要求の場合、ベリサインは、証明書に含まれる組織名およびドメイン名の再認証を行います。次の状況では…」 |
| セクション 4.6.3 | 削除:「特に、Class 3 組織向け証明書についての後続の更新要求の場合、ベリサインは、証明書に含まれる組織名およびドメイン名の再認証を行います。次の状況では…」<br><br>追加:「特に、リテール Class 3 組織向け証明書についての、www.verisign.com からの後続の更新要求の場合、ベリサインは、証明書に含まれる組織名およびドメイン名の再認証を行います。次の状況では…」 |
| セクション 4.9.7 | 脚注の追加:「「VeriSign Class 3 Organizational VIP Device CA」の CRL は、CA が発行した証明書が失効したときにのみ、その都度発行されます」。 |
| セクション 6.3.2 | 追加:「ベリサインは「VeriSign Class 3 Organizational VIP Device CA」を運用します。この CA が発行した組織利用者証明書については、以下の状況に該当する場合に、3 年を超えて最大 5 年の有効期間を設定できます。<br>o 証明書の鍵ペアがハードウェアに格納される、および<br>o ベリサインが本 CPS について組織体を認証した、および<br>o SSL/TLS を使用するサーバーの保護に使用される場合に、サーバーへのアクセス経路がプライベート ネットワークまたはイントラネットに限られる。 “ |
| セクション 6.3.2 - 脚注 16 | 削除:「これらの証明書の識別名は、少なくとも 25 か月ごとにベリサインによって再認証されるものとします」 |
| セクション 7.1.2 | 追加:「EV SSL 証明書のエクステンションについての要件は、本 CPS の付録 B3 に記載されています。」 |
| セクション 7.1.8 | 削除:「CertificatePolicies エクステンションが使用される場合、証明書には、VTN CP のセクション 1.2 で規定されているように、適切な証明書クラスに対応する CertificatePolicy のオブジェクト識別子が含まれます。CertificatePolicies エクステンションを含み、VTN CP の公開前に発行された古い証明書の場合、証明書はベリサイン CPS や依拠当事者規約を参照します。<br><br>追加:「ベリサインは、通常、Certificate Policies エクステンション内にポリシー修飾子を含む X.509 バージョン 3 VTN 証明書を発行します。一般に、かかる証明書は、適用される依拠当事者規約またはベリサイン CPS を指定する CPS ポインター修飾子を含みます。さらに、一部の証明書は、適用される依拠当事者規約を指定する User Notice 修飾子を含みます。」 |
| セクション 9.8 | 追加:「EV 証明書に対するベリサインの賠償責任の制限は、本 CPS の付録 B1 のセクション 37 にも記述されています。」 |
| セクション 9.8 | 削除:「また、利用規約および依拠当事者規約は、特定の証明書についてベリサインおよび関連会社が負担する損害賠償額の上限が以下のとおりであることを含むものとします…<br>追加:「また、利用規約および依拠当事者規約は、特定の証明書についてベリサインが負担する損害賠償額の上限が以下のとおりであることを含むものとします…」 |
| 定義 | 「拡張認証」の定義を追加 |
| 付録 B | 付録 B の追加:「EV SSL 証明書の追加認証手続き」 |
| 付録 C | 付録 C の追加: EV 証明書の最低限の暗号化アルゴリズムと鍵のサイズ |
| 付録 D | 付録 D の追加:EV 証明書で要求される証明書エクステンション |

**変更履歴:バージョン 3.2 (2006 年 5 月 1 日発効)**

| | |
|---|---|
| 全体 | 誤字を修正 |
| セクション 1.4.1.2 (表 2) | 組織証明書向けの適切な用途として TLS を追加。 |
| セクション 3.2.3 | 修正:「Class 3 の管理者証明書は、組織の認証、および管理者として行動する個人の雇用についての組織からの確認を含むものとします。」から<br>「Class 3 の管理者証明書の認証は、組織の認証、組織からの雇用の確認、および管理者として行動する個人の承認に基づきます。」に変更 |
| セクション 3.3.1 およびセクション 4.6.3 | 自動発行の更新のために、企業担当者および技術担当者の情報が変更されてはならないことを指定。 |
| セクション 3.3.1 およびセクション 4.6.3 | 追加:<br>「特に、Class 3 組織向け証明書についての後続の更新要求の場合、ベリサインは、証明書に含まれる組織名およびドメイン名の再認証を行います。次の状況では…」<br>• 以降の証明書更新時にチャレンジ フレーズが正しく使用されている、および<br>• 証明書の識別名が変更されていない<br>• 企業担当者および技術担当者の情報が前回確認したものから変更されていない |

| | |
|---|---|
| | ベリサインは、証明書の申請者に対し、電話、郵便、またはこれらに相当する手段により、組織についての特定の情報、つまり組織が証明書の申請を承認していること、および証明書の申請者の代わりに証明書申請が提出されている場合は、その提出者に権限が与えられていることを再確認する必要はありません。 |
| セクション 7.2 | RFC 5280 への参照の削除 |
| セクション 7.2.1 | 追加:「バージョン 2 の CRL は、RFC 5280 の要件に準拠します。」 |
| セクション 9.2.1 | 更新:<br>「エンタープライズ カスタマは、保険会社の過失および怠慢に関する賠償責任保険プログラム、または自家保険を利用して、商業上合理的な水準の過失怠慢賠償責任保険を維持するものとします。この保険の要件は行政機関には適用されません。ベリサインは、かかる過失怠慢賠償責任保険を維持します。」<br>から<br>「エンタープライズ カスタマは、保険会社の過失および怠慢に関する賠償責任保険プログラム、または自家保険を利用して、商業上合理的な水準の過失怠慢賠償責任保険を維持することが推奨されます。ベリサインは、かかる過失怠慢賠償責任保険を維持します。」に変更 |
| セクション 9.2.3 | セクションの表題を「エンドエンティティ向けの保険または保証範囲」から「拡張される保証範囲」に更新 |
| セクション 9.2.3 | 以下の内容を置き換え:<br>「NetSure プロテクション プランは、ベリサインの VTN のサブドメイン内に適用される拡張保証プログラムです。NetSure プロテクション プランの適用を受ける利用者には、証明書の公開鍵に対応する利用者秘密鍵の盗難、破損、喪失、または意図しない開示、あるいはなりすまし、利用者証明書の使用における特定の喪失といった、予期しない出来事に対する保護が提供されます。NetSure プロテクション プランは、依拠当事者がプランの対象となる証明書に依拠する場合にも保護を提供します。NetSure はベリサインが提供するプログラムであり、民間保険会社から取得した保険により支援されます。プロテクション プランに関する一般情報、および対象となる証明書については、http://www.verisign.com/netsure を参照してください。」<br><br>NetSure プロテクション プランの保護は、ベリサインのエンタープライズ カスタマに対しても無償で提供されます。エンタープライズ カスタマは、このサービスの適切な合意に従い、 NetSure プロテクション プランの保護を取得できます。このサービスは、証明書申請がエンタープライズ カスタマにより承認された利用者に NetSure プロテクション プランの保護を拡張するだけでなく、このような保護をエンタープライズ カスタマ自体にも拡張します。たとえば、Managed PKI カスタマの従業員が、Managed PKI カスタマの事業で使用するために証明書を申請して、これを Managed PKI カスタマが承認し、さらに、利用者のアクションにより損害が発生する場合、実際に損害を被る当事者は、利用者の雇用者としての役割を担う Managed PKI カスタマである可能性があります。NetSure プロテクション プランの対象となることで、Managed PKI カスタマは利用者のアクションが原因で被った損害について賠償を請求できます。」<br>変更後:<br>「NetSure プロテクション プランは、ベリサイン SSL 証明書およびコードサイニング証明書の利用者に向けて、ベリサインの証明書発行時の不備が原因で生じる紛失/損害、またはベリサインの過失もしくは契約上の義務違反によって引き起こされるその他の不正行為に対する保護を提供するための、拡張された保証プログラムです。ただし、証明書の利用者が、適用されるサービス規約の義務を果たしている場合に限ります。プロテクション プランに関する一般情報、および対象となる証明書については、http://www.verisign.com/netsure を参照してください。」 |

**変更履歴:バージョン 3.1 (2005 年 12 月 1 日追加)**

| | |
|---|---|
| セクション 2.3 | セクション 8 への参照をセクション 9.12 に変更 |
| セクション 4.5.2 | 次の記述を含むように更新:「依拠当事者は、証明書チェーン内の証明書が失効される前にエンドユーザー利用者証明書によって実行された電子署名への依拠が妥当なものかどうかを調査する全責任を負います。かかる依拠はすべて、依拠当事者のみのリスクで行われます。」 |
| セクション 4.12.1 | 鍵復元の要件リストをベリサインの推奨事項に変更 |
| セクション 6.2.1 | 削除:「他の CA について、ベリサインは、認証された、または少なくとも FIPS 140-1 レベル 2 の要件を満たすハードウェア暗号化モジュールを使用しています。」 |
| セクション 9.2.2 | ベリサインの SEC への届出に関する URL の更新:http://www.verisign.com/verisign-inc/vrsn-investors/sec-filings/index.html |