株式会社シマンテック
認証業務運用規程
（Certification Practice Statement）

Version 3.8.14

Effective Date: 2014/3/28

株式会社シマンテック
東京都港区赤坂 1-11-44
TEL: 03-5114-4794
https://www.symantec.com/ja/jp/

株式会社シマンテック認証業務運用規程

認証事業の譲渡完了に伴う親会社名の表記について

2010 年 8 月 9 日をもちまして、米国ベリサインから米国シマンテック・コーポレーション（以下、「米国シマンテック」）への認証事業の譲渡が完了しました。これに伴い、本文書に記載されている、米国ベリサインが有していたルート証明書など PKI サービスの一部は米国シマンテックが所有者となります。

ブランド名の変更完了までの間、「ベリサイン」と「シマンテック」の記載が並存いたしますが、本文書において、会社名につきましては「米国シマンテック」を、ブランド名や認証局名の一部といったブランド名につきましては「ベリサイン」を使用いたします。

謝辞
本文書の作成および検討に際して、各界の専門家の方々から頂戴したご支援に対し、ここに深く感謝の意を表します。

Table of Contents

1. はじめに

本書は、シマンテックの認証業務運用規程（Certification Practice Statement, 以下「本 CPS」という）である。本 CPS は、シマンテック認証機関が Symantec Trust Network（以下「STN」という） に関する証明書ポリシー（Certificate Policies, 以下「CP」という）に定める要件に従い、証明書の発行、管理、失効および更新を含む一連のサービスを提供する際に採用する手続きを記載したものである。

CP は、STN を統治するポリシーの最上位文書である。ビジネス、法的および STN 内での技術的要求(承認、発行、管理、証明書の使用、失効、更新)を確立することで、関連する信頼されたサービスを提供する。STN スタンダードと呼ばれるこれらの要求事項は、STN のセキュリティと完全性を維持し、全 STN 参加者に適用され、それゆえ、STN 全体に一定の信頼という保証を提供する。STN と STN スタンダードに関する詳細な情報は、CP に記載されている。

シマンテックは、サブドメインと呼ばれる STN の一部について権限を有している。シマンテック・サブドメインは、カスタマ、利用者および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む。

CP は STN 参加者が充足すべき要件を規定する一方、本 CPS は、シマンテック・サブドメイン内で当該要件をどのようにシマンテックが充足するかを定めるものである。特に、本 CPS は、CP および STN スタンダードの要件に従い、STN のシマンテック・サブドメイン内において、シマンテックが採用する次の実務について記載する。

- STN をサポートする重要なインフラの安全な運用
- STN 証明書の発行、管理、失効および更新

STN 内のシマンテック・サブドメインは、CP と STN スタンダードを満たすことが求められる。

本 CPS は、CP および本 CPS の構成について Internet Engineering Task Force (IETF) RFC 3647 に従う。STN に属する認証機関は、CA/ブラウザフォーラム（www.cabforum.org）による以下のガイドラインに含まれる、最新の要件に準拠する。

- EV SSL 証明書の発行と管理に関するガイドライン
- EV 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
- パブリック証明書の発行と管理に関する基本要件（Baseline Requirements）

本 CPS とこれらのガイドラインの要件の間に不一致が生ずる場合は、ガイドラインの要件が本書よりも優先される。

すなわち、CPに従ってシマンテック認証機関から発行されるEV SSL証明書、EV コード・サイニング証明書ならびにドメイン認証および組織認証のSSL 証明書 [1] は、CA/ブラウザフォーラムの定める要件に適合する。これらのドメイン認証および組織認証の証明書は、これらの要件を支持し適合するために、CP セクション 1.2 に規定されるポリシー修飾子を含んで発行される。これらのポリシー修飾子を含んで発行される全ての証明書は、CA/ブラウザフォーラムが定める要件に適合して発行され管理されていることを、シマンテック認証機関は明言する。

1.1 概要

シマンテックは、CP セクション 1.1 に定めるプロセッシング・センタであり、証明書の発行に使用される秘密鍵を格納する暗号モジュール等の、認証機関システムを収容する安全な施設を有している。シマンテックは、STN 内で認証機関となり、証明書のライフサイクル（発行、管理、失効および更新）に関するサービスを提供する。また、シマンテックは、自らのエンタープライズ・カスタマまたはシマン

[1] さらに、シマンテックは CA/ブラウザフォーラム Baseline Requirements の対象外である企業向け（SSL 用途でない）クライアント証明書を発行している。さらに、CA/ブラウザフォーラム要件において（組織認証 SSL 証明書など）限定された運用に加え、本 CPS では組織向けに発行された、その組織の情報を含む Class 2 または Class 3 証明書についても述べる。
これらの証明書を、本 CPS では「組織向け証明書」と記載する。

テックに従属するサービス・センタのエンタープライズ・カスタマの代わりに、認証機関の鍵管理および証明書のライフサイクルに関するサービスを提供する。さらに、シマンテックは、コンシューマー向け（Class 1、2 リテール証明書）、ウェブ・サイト向け（セキュア・サーバ ID、グローバル・サーバ ID など）およびエンタープライズ向け（マネージド PKI サービス）の各サービスにおいて証明書を提供する。シマンテックの提供する上記以外のサービスまたは米国シマンテックがシマンテックに提供するサービスに関しては、本 CPS の対象外である。

本 CPS は、具体的に、以下の事項に適用される。

- 米国シマンテックの第一次認証機関
- STN をサポートする、シマンテックのインフラストラクチャ認証機関およびシマンテックの管理認証機関
- シマンテックのパブリック認証機関および 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・カスタマの認証機関

より一般的には、本 CPS はシマンテック・サブドメイン内における全ての個人および組織（以下総称して「サブドメイン参加者」という）による当該サブドメイン内の STN サービスの利用にも適用される。また、本 CPS に特に記載がない場合において、シマンテックの管理するプライベート認証機関は、本 CPS の適用範囲外である。シマンテック以外のアフィリエートが管理する認証機関も、本 CPS の対象外である。

STN では、Class 1～4 の 4 種類の証明書が発行される。CP は、これらの証明書のポリシー（Class 毎に一つのポリシーがある）を定義し、Class 毎に STN スタンダードを設定する文書である。

シマンテックは、STN のサブドメイン内で 3 種類(Class 1,2,3)の Class の証明書を提供する。本 CPS は、シマンテックがそのサブドメイン内で各 Class の CP の要件をどのように充足するかを規定する。従って、本 CPS は、3 種類の Class の証明書に対する発行および管理に関する実務と手続きを対象とする文書である。

シマンテックは、政府の要求事項または業界の標準および要件に従うために、本 CPS を補足する文書を公開することができる。

上記の補足文書は、補足事項に基づき発行された証明書の利用者および依拠当事者に適用されるものとする。

本 CPS は、シマンテック・サブドメインに関係する一連の文書の一つである。本 CPS 以外の文書としては、以下のものが含まれる。

- より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機密文書で、以下のものを含む。
  - STN インフラストラクチャに適用されるセキュリティの原則を規定する、“Physical Security Policy”
  - 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、米国シマンテックおよびアフィリエートに適用される詳細な要件を記載する“Security and Audit Requirements Guide”
  - 詳細なキーマネージメントの運用要件を示す、”KeyCeremony Reference Guide”

- シマンテックが制定する付属契約。当該付属契約は、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する。特に、STN スタンダードからこれらの STN 参加者に至る契約がある場合において、STN 参加者がどのようにして STN スタンダードを充足しなければならないかについての具体的な手続きを規定する。

多くの場合、本 CPS 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を記述した上記の付属文書を参照する。

1.2 文書名と識別

この文書は、シマンテックの CPS である。STN 証明書は、各 STN 証明書の Class に対応するオブジェクト識別子を含む。従って、シマンテックは、本 CPS にオブジェクト識別子を割り当てていない。ポリシー・オブジェクト識別子は、本 CPS セクション 7.1.6 に従い使用される。

ドメイン認証と組織認証の SSL 証明書は CP セクション 1.2 に規定されるオブジェクト修飾子を含む。これは CA/ブラウザフォーラムが定める Baseline Requirements を支持し順守していることを示す。

1.3 PKI 参加者

1.3.1 認証機関

認証機関という用語は、STN内で公開鍵証明書を発行する全ての組織に適用される包括的な用語である。認証機関は、第一次認証機関と呼ばれるカテゴリの発行者を包含する。第一次認証機関は、4 つのドメインのルート[2]となり、一つの第一次認証機関が各Classの証明書のために存在する。各第一次認証機関は、米国シマンテックのエンティティである。第一次認証機関の下位に属するシマンテックの認証機関は、利用者または他の認証機関に証明書を発行する。

また、米国シマンテックは、内部的な管理のための階層である「 Symantec Class 3 Internal Administrator CA 」階層を管理する。

また、米国シマンテックは「 Symantec Universal Root Certification Authority 」および「Symantec ECC Universal Root Certification Authority」を管理する。「 Symantec Universal Root Certification Authority 」は、Class 3 および特定のClass 2 の下位認証機関証明書を発行する。

シマンテックのエンタープライズ・カスタマは、米国シマンテックの第一次認証機関の下位に属する認証機関として、自らの認証機関を運営することができる。当該カスタマは、STN CPおよびシマンテックの本CPSの全要件を順守するために、シマンテックと契約を締結する。しかしながら、これらの下位認証機関はそれぞれ内部要件に基づき、より限定的な運用を行うことができる。

1.3.2 登録機関

登録機関は、STN 認証機関の代わりに、エンドユーザ証明書の申請者の本人確認と認証を行い、エンドユーザ証明書の失効要求を行い、証明書のリニューアルまたはリキーの申請を承認する。シマンテックは、自らが発行する証明書の登録機関になることができる。

シマンテックと契約を締結する第三者は、自らの登録機関となり、シマンテック認証機関が発行する証明書の認証を行うことができる。第三者登録機関は、STN のCP、本CPSおよびシマンテックと締

[2] STN では現在 Class 4 証明書の発行は行われていない。

結する契約に定める全ての要件を順守しなければならない。しかしながら、登録機関は、内部要件に基づき、より限定的な運用を行うことができる。[3]

1.3.3 エンド・エンティティ

STN のエンド・エンティティは、STN 認証機関により発行される証明書の全てのエンドユーザ（エンティティを含む）を含む。エンド・エンティティは、証明書のエンドユーザ利用者とされるエンティティである。エンドユーザ利用者としては、個人、組織、またはファイアウォール、ルーター、信頼されるサーバもしくは組織内で通信を安全に行うためのその他の機器でインフラストラクチャを構成するものがありうる。

ある場合において、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。しかしながら、証明書を要求する者と信用される Subject が異なる場合がある。例えば、ある組織は、従業員に、当該組織を代表して電子取引やビジネスを行わせるために証明書を要求することができる。このような場合、証明書の発行を申込むエンティティ（すなわち、ある特定のサービスの申込みを通じて、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 Subject（一般的には、信用される者）とは異なる。この二つの役割を区別するために、本 CPS では以下の二つの異なる用語を使用する。すなわち、「利用者」は証明書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、「Subject」は証明書と紐づけられる者である。利用者は証明書の利用に関する最終的な責任を負う者であるが、Subject は証明書が提示されるときに認証される個人である。

「Subject」が使用される場合、「利用者」と区別することを示している。「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と、Subject の意味も包含する場合とがある。この二つの使い分けが、本 CPS の正確な理解のために必要である。

認証機関は、自己署名した証明書を発行する第一次認証機関として、または上位の認証機関による証明書を発行される認証機関として、技術的には STN 内の証明書の利用者でもある。本CPSにおける「エンド・エンティティ」および「利用者」という場合は、エンドユーザ利用者にのみ適用される。

1.3.4 依拠当事者

依拠当事者は STN 下で発行される証明書またはデジタル署名に依拠して行為する個人またはエンティティである。依拠当事者は STN 内において利用者である場合もあるし、利用者でない場合もある。

1.3.5 他の参加者

適用せず。

1.4 証明書の利用

1.4.1 適切な証明書の利用

1.4.1.1 個人に発行される証明書

個人向け証明書は、電子メールに署名を付与するためおよび電子メールを暗号化するため、および申請を認証するため（クライアント認証）に、通常個人により使用される。最も一般的な個人向け証明

[3] 第三者登録機関の一例として、マネージドPKIサービスのカスタマがある。

書の利用形態は、以下の Table 1 に記載されているが、これ以外の目的にも利用することができる。但し、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るものでなければならず、その利用が法律、STN CP、発行された証明書の根拠となる本 CPS および利用者との間の契約によって禁止されていないものに限る。

証明書の Class	保証のレベル			使用用途		
	低	中	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			✓	✓	✓	✓

Table 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

組織向け証明書は、組織が法的に存在することおよび証明書内に含まれる組織の他の属性（例えば、インターネットまたは電子メールのドメインの所有権など。但し、検証されていない利用者情報を除く）が認証された後、組織向けに発行される。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ない。最も一般的な組織向け証明書の利用形態は、以下の Table 2 に記載されているが、これ以外の目的にも利用することができる。但し、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るものでなければならず、その利用が法律、STN CP、発行された証明書の根拠となる本 CPS および利用者との間の契約によって禁止されていないものに限る。

証明書の Class	保証のレベル			使用用途			
	高 (EV 証明書)	高 (CA/BF 組織認証証明書)	高	コード/オブジェクト・サイニング	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 組織認証証明書		✓	✓		✓	✓	✓

Table 2 – 組織向け証明書の用途

1.4.1.3 保証のレベル

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。デジタル署名は、送信者がある電子メールアドレスから電子メールを発信したという低レベルの保証を提供する。しかしながら、証明書は利用者の同一性の証明を提供するものではない。暗号化アプリケーションは、依拠当事者が利用者へメッセージを暗号化するために利用者の証明書を使用することを可能にする。しかしながら、発信者である依拠当事者は、受信者が実際に証明書で指定された者であることを確信することはできない。

保証のレベルが中の証明書は、Class 1 および 3 と比較して、利用者の同一性を中程度で保証することが必要な組織内外、商業用および個人用の電子メールの安全性を確保するのに適している。

保証のレベルが高の証明書は、Class 1 および 2 に比較し、利用者の同一性について高い保証を提供する個人向けおよび企業向けの Class 3 証明書である。

保証のレベルが高(EV証明書)の証明書は、"Guidelines for Extended Validation Certificates"に従ったシマンテック発行のClass 3 証明書である。

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、特に輸出入に係る法律の認める範囲でのみ利用されなければならない。

STN 証明書は、危険な環境下における制御装置での利用または再販のため、あるいは、機能停止が直接に死亡、身体障害、または深刻な環境被害をもたらすようなフェイル・セーフ機能を必要とする核施設、航空・通信システム、航空管制、兵器管理システム等での利用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ない。また、Class 1 証明書は、実在性の証明または実在性もしくは権限の否認防止を裏付けるものとして利用することはできない。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用途を意図しており、サーバまたは組織向け証明書として使用することはできない。

認証機関証明書は、認証機関の役割を果たす目的以外の目的で利用することはできない。さらに、エンドユーザ証明書は、認証機関証明書として利用することはできない。

シマンテックは定期的に中間認証機関証明書の鍵ペアを変更する。中間認証機関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のアプリケーションまたはプラットフォームは、中間認証機関証明書の鍵ペアが変更された後では指定されたとおり動作しない可能性がある。従って、シマンテックは、中間認証機関証明書をルート証明書として利用することを保証せず、これをアプリケーションまたは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する。シマンテックは、ルート証明書として、第一次認証機関を利用することを推奨する。

1.5 ポリシー管理

1.5.1 本文書の管理組織

株式会社シマンテック
〒107－0052 東京都港区赤坂 1-11-44
電話 03-5114-4778
FAX 03-5114-4186
dl-vsj-practice@symantec.com

1.5.2 連絡先

株式会社シマンテック
〒107－0052 東京都港区赤坂 1-11-44
電話 03-5114-4778
FAX 03-5114-4186
dl-vsj-practice@symantec.com

1.5.3 CP への適合性の決定者

シマンテックは、本 CPS および本 CPS を補充しまたはこれに従属する文書が、CP または本 CPS に適合するかどうかの決定をする責任を有する。

1.5.4 承認手続き

本 CPS および修正の承認はシマンテックによりなされるものとする。変更は、本 CPS の改定部分を含む文書の形式によるか、改定通知によるかのいずれかの方法でなされる。改定版の本 CPS あるいは改定通知は、シマンテックのリポジトリの「プラクティス・アップデート」（https://www.symantec.com/about/profile/policies/repository.jsp）にリンクされる。改定部分として記載されている事項は、本 CPS の参照されたバージョンの指定されたまたは矛盾する条項に優先する。

1.6　定義

別表 A を参照のこと。

2. 公表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、自己の認証機関およびエンタープライズ・カスタマの認証機関のため、リポジトリの機能を果たす。シマンテックは本 CPS セクション 2.2 の定めるところに従いリポジトリで、利用者に発行した証明書を公表する。

利用者証明書が失効された場合、シマンテックはこれをリポジトリにおいて公表する。シマンテックは、シマンテック・サブドメイン内の自己の認証機関、サービス・センタおよびエンタープライズ・カスタマの認証機関に関する CRL を本 CPS に従い発行する。これに加え、オンライン証明書ステータス・プロトコールサービス（以下「OCSP」という）の契約をしているエンタープライズ・カスタマのために、シマンテックは本 CPS に従い、OCSP サービスを提供する。

2.2 証明書情報の公表

シマンテックは、依拠当事者が証明書の失効その他のステータスをオンラインで問い合わせるための LDAP ベースのリポジトリを管理する。シマンテックは、依拠当事者に証明書のステータスを調べるための適切なリポジトリの探し方、および OCSP が利用可能な場合、適切な OCSP レスポンダーの探し方に関する情報を提供する。

シマンテックは、自己の認証機関およびサブドメイン内におけるサービス・センタの認証機関の代わりに、発行された証明書を公表する。利用者証明書が失効された場合、シマンテックはこれをリポジトリで公表する。さらに、シマンテックは CRL を発行し、利用可能な場合には、自己の認証機関およびサブドメイン内のサービス・センタ認証機関のために OCSP を提供する。

シマンテックは、以下の文書の最新バージョンを公表する。

- STN CP
- 本 CPS
- 利用規約
- 依拠当事者規約

シマンテックは、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認証機関およびエンタープライズ・カスタマの認証機関に対して、リポジトリの機能を果たす。

シマンテックは、認証機関に関する情報をリポジトリ
（https://www.symantec.com/about/profile/policies/repository.jsp）で公表する。

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ウェブ・サイト内のリポジトリで公表する。

シマンテックは、Table 3 に従い、証明書を公表する。

証明書の種類	公表の要件
STN 第一次認証機関および STN ルート認証機関証明書	最新のブラウザに含まれ、依拠当事者に利用可能
シマンテック中間認証機関証明書	下記のクエリーを通じて利用者証明書とともに取得可能な証明書チェーンの一部として、依拠当事者に利用可能

シマンテック認証機関証明書で、マネージド PKI ライト証明書およびマネージド PKI カスタマの認証機関証明書をサポートするもの	directory.verisign.co.jp にあるシマンテック LDAP ディレクトリ・サーバにおけるクエリーを通じて利用可能
シマンテック OCSP レスポンダー証明書	directory.verisign.co.jp にあるシマンテック LDAP ディレクトリ・サーバにおけるクエリーを通じて利用可能
Class 3 SSL サーバ証明書およびコード・サイニング証明書	シマンテックのリポジトリにある証明書ステータス確認のリンク先で検索が可能
Class 3 SSL サーバ証明書およびコード・サイニング証明書を除く利用者証明書	directory.verisign.co.jp にあるシマンテックのリポジトリにおけるクエリーを通じて依拠当事者に利用可能
マネージド PKI カスタマを通じて発行された利用者証明書	上記のクエリーを通じて利用可能なものとするが、マネージド PKI カスタマの判断により、証明書は当該証明書のシリアル・ナンバーを通じた検索を通してのみアクセスすることができる

Table 3 – 証明書の公表の要件

2.3 公表の頻度

本 CPS の改定は、本 CPS セクション 9.12 に従い、公表される。利用規約および依拠当事者規約の改定は必要に応じ公表される。証明書は、発行時に公表される。証明書ステータス情報は本 CPS の定めに従い公表される。

2.4 リポジトリへのアクセス制限

シマンテックのウェブ・サイトのリポジトリ部分に公表される情報は、公的にアクセス可能なものである当該情報に対する閲覧のみのアクセスは制限されないものとする。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、依拠当事者規約への同意を要求する。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、抹消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の手段を講じている。

3. 確認と認証

3.1 名称

STN 下で発行された証明書に記載されている名称は、STN CP、本 CPS もしくは証明書中に別段の定めがある場合を除き、認証されたものである。

3.1.1 識別名の種類

現在、STN は米国シマンテックの所有となっているが、以前発行された証明書には買収前の社名およびブランド名が記載されている場合がある。該当する証明書には Organization(O)行に“VeriSign, Inc.”、Organizational Unit(OU)に“VeriSign Trust Network”が記載されているが、これはそれぞれ「米国シマンテック」および「シマンテック・トラスト・ネットワーク」を意味する。

シマンテック認証機関証明書は、Issuer および Subject フィールドに X.501 識別名を含む。
シマンテック認証機関識別名は、Table 4 に定めるものから構成される。

属性	値
Country (C) =	“US”、“JP”もしくは使用せず。
Organization (O) =	“Symantec Corporation”、“Symantec Japan, Inc.”、“VeriSign Japan K.K.”、もしくは組織名 [4]
Organizational Unit (OU) =	シマンテック認証機関証明書は以下に定める一つ以上の OU 属性を含むことができる。 ・ 認証機関名 ・ Symantec Trust Network ・ 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 ・ 著作権に関する通知 ・ 証明書の種類に関する記載
State or Province (S) =	使用せず。
Locality (L) =	使用せず。ただし、「 Symantec Commercial Software Publishers CA 」は、”Internet”を使用。
CommonName (CN) =	認証機関名が OU 属性で特定されない場合、この属性は認証機関名を含む、もしくは使用せず。

Table 4 – 認証機関証明書に含まれる識別名の属性

利用者向け証明書は、SubjectName フィールドに X.501 識別名を含み、Table 5 に定めるものから構成される。

属性	値
Country (C) =	JP もしくは使用せず。
Organization (O) =	この属性は、次のように使用される。 ・ シマンテックのOCSP レスポンダーおよび任意の記載として組織と関連を有さない個人向け証明書の場合、

[4] エンタープライズ・カスタマの認証機関の場合、「o=」の記載事項はカスタマの組織名を法的に示す値となる。

属性	値
	“Symantec Corporation”、“Symantec Japan, Inc.” または“VeriSign Japan K.K.”[5] ・ SSL サーバ証明書および組織と関連を有する個人向け証明書の場合、利用者の組織名
Organizational Unit (OU) =	シマンテックのエンドユーザ利用者向け証明書は以下のような OU 属性を一つないし複数含む。 ・ 組織向け証明書および組織と関連を有する個人向け証明書の場合、利用者組織単位 ・ Symantec Trust Network ・ 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 ・ 著作権に関する通知 ・ シマンテックにより認証された証明書(SSL サーバ証明書とコード・サイニング証明書を除く)中に、“Authenticated by VeriSign Japan K.K.”および“Member, Symantec Trust Network” ・ シマンテックにより認証された証明書(SSL サーバ証明書とコード・サイニング証明書)中に、“Authenticated by Symantec”および“Member, Symantec Trust Network” ・ “Persona Not Validated”(Class 1 個人向け証明書) ・ 証明書の種類を説明する記載[6] ・ “No organization affiliation”(個人向けコード・サイニング証明書)
State or Province (S) =	都道府県もしくは使用せず。
Locality (L) =	市区町村もしくは使用せず。
CommonName (CN) =	この属性は、次のものを含む。 ・ OCSP レスポンダー名(OCSP レスポンダー証明書) ・ 完全修飾ドメイン名(SSL サーバ証明書) ・ 組織名(コード/オブジェクト・サイニング証明書) ・ “Persona Not Validated”(Class 1 個人向け証明書)[7] ・ 個人の名前(個人向け証明書または個人向けコード・サイニング証明書)
E-Mail Address (E) =	Class 1 個人向け証明書および一般的なマネージド PKI 利用者証明書の場合、電子メールアドレス Class 3 組織向けメール署名証明書の場合、電子メールアドレス

Table 5 –利用者証明書中の識別名属性

利用者証明書の Subject 識別名の CommonName (= CN)の記載事項は、Class 2 および 3 証明書の場合、認証される。

- 組織向け証明書の Subject 識別名に含まれる認証された CommonName 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当な名称である。
- 個人向け証明書の Subject 識別名に含まれる CommonName の値は、一般に受入られている個人名である。

[5] シマンテックの場合、Class 2 証明書の社内用途において O 行の値に社内用の接尾節を追加することがある。"Symentec Corporation –[xxxx] (例: Symantec Corporation – Build 5315)"のような形式の記載は法的にもシマンテックを表すものであると保証する。

[6] 認可された特定の条件において、シマンテックの内部用途のための Class 2 証明書が発行される。該当する証明書の識別名や OU として、内部用途以外での証明書の使用するうえでは信頼性に欠ける値を含む。

[7] Xxxx 年 xx 月 xx 日現在、既存のシマンテックが承認した Symantec Class1 Managed PKI 顧客が発行する Class1 個人用証明書にについては、OU に“Persona Not Validated”が表記されていることを条件に通称名を CN に使用する場合がある

EV 証明書の項目とプロファイルの要求項目については、本 CPS Appendix B3 のセクション 6 に記載される。

3.1.1.1 CA/ブラウザフォーラム識別名の要件

EV SSL 証明書、EV コード・サイニング証明書ならびにドメイン認証および組織認証の SSL サーバ証明書は、STN の補足として本 CPS の Appendix B1、Appendix C、および、Appendix D それぞれのセクション 9 に定める手続きにより、CA/ブラウザフォーラムの定める要件に準拠する。

3.1.2 意味のある名称であることの必要性

Class 2 および3の利用者証明書は、証明書のSubjectである個人または組織の同一性を特定することが可能な一般に理解されている意味のある名称を含む。

シマンテック認証機関証明書は、証明書の対象(Subject)である認証機関の同一性を特定することが可能な、一般に理解されている意味のある名称を含む。

3.1.3 匿名またはペンネームの使用

Class 1 証明書の利用者の本人確認は行われない。Class 1 証明書の利用者は匿名またはペンネームを使用することができる。法律または政府機関により、未成年者や機密事項を扱う政府関係者に関する情報等の利用者を秘匿することが要求される場合を除き、Class 2 および 3 証明書の利用者は利用者の正式な個人名または組織名以外のものを使用することができない。証明書中の匿名使用申請については、シマンテックがその必要性を認めた場合に許可され、この場合利用者の本人確認は行われているが利用者名は匿名である旨が証明書に記載される。

3.1.4 識別名を解釈するための指針

適用せず。

3.1.5 唯一の名称

シマンテックは利用者の申込手続きを通じて、Subject 識別名が、ある特定の認証機関のドメイン内で唯一のものであることを保証する。一人の利用者が複数の同一の Subject 識別名を持つ証明書を所持することは可能である。

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らない。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の検証を行わない。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ものではない。シマンテックは、証明書申請者に何等の責任を負うことなく、上記の紛争を理由として証明書申請を拒絶する権利を有する。

3.2 初回の本人確認

3.2.1 秘密鍵を所有していることの証明方法

証明書申請者は証明書に含まれる公開鍵と対になる秘密鍵を正当に所有していることを PKCS#10、暗号学的にこれと同等の方法またはシマンテックが承認したその他の方法のいずれかにより証明しなければならない。鍵ペアが認証機関により利用者の代理として生成される場合(予め生成された鍵をスマートカードに格納する場合など)には、上記の要件は適用されない。

3.2.2 組織の実在性確認

証明書に組織名が含まれる場合、組織の実在性および証明書申請者から提供されたその他の申請情報(確認を実施しない利用者情報を除く)は、シマンテックが規定する認証手順に従い確認される。

シマンテックは少なくとも以下の確認を行う。

- 当該組織が存在していることを最低一種類の第三者の証明サービス、データベースまたは当該組織の存在を確認する政府機関または所管官庁が発行もしくは保持する文書によって確認する。
- 証明書の申請が組織を代表して行われたことならびに申請者に申請の権限があることを電話、郵便またはこれらに相当する方法により確認する。証明書に組織を代理する個人名が記載される場合、その者の雇用の確認と組織を代理する権限があることも確認する。

証明書にドメインまたは電子メールアドレスが含まれる場合、シマンテックは当該組織が当該ドメインをFQDNまたは電子メールに含まれるドメインとしての使用権を保持しているかを確認する。

必要に応じて米国輸出規制および米国商務省産業安全保障局発行のライセンスを充足するための追加的な調査をシマンテックが行う。

特定の種類の証明書については、Table 6 に記載されている手続きを行う。

証明書の種類	追加となる手続き
Extended Validation Certificates	シマンテックにおける EV 証明書の発行手続きは、本 CPS の Appendix B1 に記載される。EV コード・サイニング証明書の発行手続きは、本 CPS の Appendix C に記載される。
組織認証およびドメイン認証証明書	シマンテックが組織認証およびドメイン認証証明書を発行する際の手続きは、本 CPS 上では「組織認証およびドメイン認証証明書に関する CA/ブラウザフォーラム要件」に従って区別される。
Authenticated Content Signing Certificate (ACS)	シマンテックにより ACS 証明書を用いたデジタル署名が施される場合、署名対象は当該組織がそのコード・サイニング証明書を用いて署名した元の内容そのものであることを事前に確認する。
Secure Mail ID	Class 3 組織向けメール署名用証明書の手続きはコード・サイニング証明書に順ずる。ただし、E-Mail Address (E)に含まれるメールアドレス内のドメインについては追加で所有確認を行う。

Table 6 –特別な認証手続き

3.2.2.1 組織名の申請に関する 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・サイニング証明書ならびにドメイン認証および組織認証の SSL 証明書は、STN の補足として本 CPS の Appendix B1、Appendix C および Appendix D それぞれのセクション 11 に定める手続きにより、CA/ブラウザフォーラムの定める要件に準拠する。

3.2.2.2 組織名の申請に関する Mozilla 社の審査の要件

証明書内の国際化ドメイン名(IDNs)の申請において、シマンテックは同形異義語攻撃に備え、ドメイン名所有者の検証を行う。シマンテックは自動化されたシステムにより複数の Whois 検索を実行してドメインの所有者を特定する。検索が失敗した場合、手動による再検索が実行され、登録局は証明書発行要求を却下する。さらに、登録局は、その特定のホストネーム・ラベルの検索結果として確認されたいかなるドメイン名も却下する。

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する。また、スタンダードを満たすよう注力する。

3.2.3 個人の実在性確認

個人の実在性の確認に関しては証明書の Class によって異なる。Table 7 に Class 別の STN 証明書の標準的な確認方法を説明する。

証明書の Class	同一性の確認
Class 1	同一性の確認を行わない。利用者の電子メールアドレスについて、当該アドレスにメールを送り、利用者が応答することができるかの限定的な確認のみを行う。
Class 2	申請者からの申請情報と以下のいずれかの情報を照合することで、存在確認を行う。 ・ シマンテックが承認した存在確認のためのサービス(主要な信用機関またはその他の信用できる情報提供サービス) ・ 証明書を承認する登録機関の従業員または顧客リストなどの業務上の記録またはデータベースに含まれる情報
Class 3	Class 3 個人向け証明書の認証は、証明書申請者が認証機関もしくは登録機関の代理人また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出頭すること、またはこれと同程度のレベルで本人であることを確認できるという証拠となる文書により行う。代理人、公証人またはその他の当局者は証明書申請者をパスポート、運転免許証など政府が発行する写真付きの身分証明書ともう一種類の身分証明書とを照合することにより確認する。 Class 3 の管理者証明書の認証は、組織の確認、実在性の確認および管理者の権限の確認に基づき行う。 シマンテックは、自らの管理者の証明書申請も承認する。管理者は組織内の「信頼される人物」である。この場合、当該証明書申請の認証は、雇用または請負業者としての関係、および経歴調査との関係における実在性の確認に基づき行われる。

Table 7 –利用者の同一性の確認

3.2.4 確認を行わない申請情報

確認を行わない申請情報は以下の通り。

- 一定の例外を除く部門名（OU）[8]
- 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係付けられており、個人が組織と関連することまたは組織の代理人であることを示す場合、シマンテックまたは登録機関は、以下の確認を行う。

- 当該組織が存在していることを最低一種類の第三者の証明サービス、データベースまたは当該組織の存在を確認する政府機関または所管官庁が発行または保持する文書によって存在を確認する。
- 証明書を承認する登録機関の従業員または顧客リストなどの業務上の記録またはデータベースに含まれる情報を使用し、または証明書の申請が組織を代表して行われたことならびに申請者に申請の権限があることを、電話、郵便またはこれらに相当する方法により確認する。

3.2.6 共同運営の条件

適用せず。

3.3 リキー申請の確認と認証

証明書を継続して使用するためには、証明書の有効期限内に新しい証明書を入手する必要がある。シマンテックは、一般的に、有効期限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要求する（技術的に「リキー(reKey)」と定義される）。しかし、ある場合においては（例えばウェブ・サーバ用証明書の場合）、シマンテックは、既存の鍵ペアで新しい証明書を利用者が要求することを認める（技術的に「リニューアル(renewal)」と定義される）。

一般的には、「リキー」および「リニューアル」ともに、「証明書の更新」と表現されるが、これは、古い証明書を新しい証明書に置換える事実に着目して、新しい鍵ペアが生成されるかどうかを重要視しないことによる。Class 3　サーバ用証明書を除き、全 Class とタイプの証明書について、シマンテック利用者向け証明書更新手続きの一部として、新しい鍵ペアが常に生成されるので、この区別は重要でない。しかし、Class 3　サーバ用証明書については、利用者の鍵ペアはウェブ・サーバ上で生成され、ほとんどのウェブ・サーバの鍵生成ツールが既存の鍵ペアで新しい証明書のリクエストの作成を許容しているので、「リキー」と「リニューアル」の区別は意味をもつ。

3.3.1 定期的なリキーに関する確認と認証

リキーの手続きにおいては、利用者証明書のリキーを要求する者または組織が証明書の実際の利用者であることが確認される。

[8] CA/ブラウザフォーラムガイドラインに準拠することを証明されたドメイン認証および組織認証証明書は、認証された組織単位（OU）の値を含むことがある

チャレンジフレーズ(またはこれと同等なもの)の使用または秘密鍵の保有を証明することが上記手続きの条件を満たす一つの方法である。利用者は申請情報と共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、提示する。証明書のリキーの際、利用者の再登録情報とともに、チャレンジフレーズ(またはこれと同等なもの)が正しく提示され、申請責任者および技術担当者情報を含む申請者情報が変更されていなければ、リキーされた証明書は自動的に発行される。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、シマンテックは証明書の更新に際し、認証された企業連絡先のメールアドレスに電子メールを送信し、証明書更新の要求確認と、証明書発行の承認を要求する。証明書発行を承認する確認が取れた場合、シマンテックは申請時の情報[9]が変更されていないことを確認し、証明書を発行する[10]。

この方法によるリキー後、そしてそれ以降リキーが行われる際に、シマンテックまたは登録機関は証明書申請の認証要件に従い申請者の実在性の再確認を行う。

特に、Class 3 組織向け SSL サーバ証明書の場合、シマンテックは、証明書に含まれる組織名称、ドメイン名の再認証を本 CPS セクション 6.3.2 に記載の間隔で行う。
要件

- チャレンジフレーズがリキーされる証明書に対して正しく使用されているか、または、申請責任者から電子メールにより確認の返信を得られたこと
- 証明書の識別名が変更されていないこと
- 申請責任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こと

シマンテックは、証明書のリキーの申請に際し、組織が申請を許可し、申請者に組織を代表して証明書の申請の権限があることについて、電話、郵便またはこれらに相当する方法による再確認は行わない。

証明書の有効期間満了から 30 日以降のリキーについては再度認証を行い、証明書は自動的に発行されない。

3.3.2 証明書失効後のリキーに関する確認と認証

証明書失効後のリキーまたはリニューアルは、失効の理由が以下の場合、許可されない。

- 証明書(Class 1 証明書を除く)Subject に記載されている以外の者に発行された場合
- 証明書(Class 1 証明書を除く)が、当該証明書の Subject に記載されている者または機関の許可無く発行された場合
- 利用者の証明書申請を承認した機関が、証明書申請中の重要な事実が虚偽であることを発見した場合、またはそう信じる理由がある場合
- STN を保全するために米国シマンテックまたはシマンテックが必要と認める場合

上記の定めに従うことを条件として、組織向けまたは認証機関証明書の失効後のリニューアルについては、更新手続きによって、組織向けまたは認証機関証明書の更新を要求する者が証明書の利用者であると確認される場合にのみ許可される。更新後の組織向け証明書は更新前の証明書に含まれる Subject 識別名 と同じものを含む。

個人向け証明書の失効後の更新については、更新を要求する者が利用者であることを確認しなければならない。チャレンジフレーズ(またはこれと同等なもの)を使用することが一つの方法である。上記の方法またはシマンテックが認めるその他の方法以外に、最初の証明書申請に対して行った確認および認証の要件が失効後の証明書の更新に適用される。

---

[9] 所定の変更手続きにより連絡先情報が変更されている場合、証明書は自動更新可能である。
[10] 製品によってはこの手続きを実施しない場合がある。

3.4 失効申請に関する確認と認証

証明書の失効前に、シマンテックは失効申請が証明書の利用者または証明書申請を承認した者によってなされたものであることを検証する。

利用者の失効申請を認証するための手続きには、以下のものを含む。

- 利用者に自己のチャレンジフレーズ（またはこれと同等なもの）を提出させ、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こと。（注意:本オプションは全ての利用者で利用できるとは限らない）
- 失効申請をする利用者からの、失効の対象となる証明書を参照することで検証できるデジタル署名を含むメッセージを受領すること。
- 証明書の Class を考慮して、失効を申請する者または組織が、実際に利用者であるという合理的な保証を提供する利用者と連絡すること。この連絡には、状況に応じて、電話、ファクシミリ、電子メール、郵便または宅配便の何れか一つ以上を含む。

シマンテックの管理者は、シマンテック・サブドメイン内で利用者証明書の失効を申請することができる。シマンテックは、管理者が失効に関する行為を遂行することを許可する前に、管理者の同一性を SSL/TLS およびクライアント認証を利用するアクセス・コントロールを通じて、または STN が認めるその他の手段を用いて認証する。

自動承認モジュールを利用するマネージド PKI カスタマは、シマンテックに失効申請を一括して提出することができる。当該申請は、マネージド PKI カスタマの自動承認用の秘密鍵でデジタル署名された申請によって認証される。

マネージド PKI カスタマの認証機関証明書の失効申請は、その失効が当該認証機関によって申請されているものであることをシマンテックが確認することにより、認証される。

4. 証明書のライフサイクルに対する運用要件

4.1 証明書申請

4.1.1 証明書申請を行うことができる者

証明書申請を行うことができる者は、以下のとおりである。

- 証明書の Subject に表示される個人
- 組織もしくはエンティティから権限を受けた代理人,
- 認証機関から権限を受けた代理人
- 登録機関から権限を受けた代理人

4.1.2 登録手続きおよび責任

4.1.2.1 エンドユーザ証明書の利用者

全エンドユーザ証明書の利用者は、セクション 9.6.3 に記載される事項を含んだ関連する利用規約に同意することを明らかにし、次の各項目からなる申請手続きを履行するものとする。

- 証明書申請の必要事項を記載し、真正な情報を提供すること
- 鍵ペアを生成もしくは生成させる手配をすること
- 自己の公開鍵を直接もしくは登録機関を通じてシマンテックに引き渡すこと
- シマンテックに提示された公開鍵に対する秘密鍵の所有および排他制御が証明できること

4.1.2.2 CA/ブラウザフォーラムの証明書申請要件

EV SSL 証明書、EV コード・サイニング証明書ならびにドメイン認証および組織認証の SSL 証明書は、STN の補足として本 CPS の Appendix B1、Appendix C および Appendix D それぞれのセクション 10 に定める手続きにより、CA/ブラウザフォーラムの定める要件に準拠する。

4.1.2.3 認証機関と登録機関の証明書

認証機関と登録機関証明書の利用者は、シマンテックと契約を締結する。契約の過程において、認証機関と登録機関の申請者は、資格を証する書面と連絡先に関する情報を提供する。当該契約過程において、もしくは、遅くとも認証機関や登録機関の鍵ペアを鍵ペア生成のセレモニー前に、申請者は、シマンテックに協力して、適切な識別名および申請者に対して発行されるべき証明書に記載される内容を決定する。

4.2 証明書申請手続

4.2.1 本人性確認と認証機能の実施

シマンテックもしくは登録機関は、セクション 3.2 において要求される利用者の全情報の確認および認証を行う。

4.2.2 証明書申請の承認もしくは拒絶

シマンテックもしくは登録機関は、以下の基準が満たされている場合、証明書申請を承認する。

- セクション 3.2 において要求される利用者の全情報の確認および認証が問題なく完了する

こと
- 支払いが完了していること

以下の場合、シマンテックもしくは登録機関は、証明書申請を拒絶する。
- セクション 3.2 において要求される利用者の全情報の確認および認証を完了することができないとき
- 利用者が、要求されたサポートのための資料提供をしないとき
- 利用者が、指定された時間内に返答をしないとき
- 支払いの完了を確認できないとき
- 登録機関が、利用者へ証明書を発行することが STN の不信に繋がると信ずるとき

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手続きを開始する。関連する利用規約、本 CPS もしくは他の STN 参加者間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定めない。その証明書申請は、拒絶されるまで有効である。

4.3 証明書発行

4.3.1 証明書の発行過程における認証機関の行為

証明書は、証明書申請の承認後、登録機関からの証明書発行申請を受領した後に、生成され発行される。シマンテックは、証明書申請者に対し、証明書申請に含まれていた情報に基づき、当該証明書申請の承認後に、証明書を生成し発行する。

4.3.2 認証機関の利用者に対する証明書発行通知

シマンテックは、直接もしくは登録機関を通じて、その証明書を生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、利用者に証明書へのアクセス手段を提供する。証明書は、エンドユーザ利用者がウェブ・サイトからダウンロードするか、もしくは、当該利用者に対する証明書を含んで送信されたメッセージによるか、いずれかの方法により利用者が利用することができるようになる。

4.3.3 ルート認証局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・サイニング証明書ならびにドメイン認証および組織認証の SSL 証明書は、STN の補足として本 CPS の Appendix B1、Appendix C および Appendix D それぞれのセクション 12 に定める手続きにより、CA/ブラウザフォーラムの定める要件に準拠する。

4.4 証明書の受領

4.4.1 証明書の受領となる行為

次の場合、利用者は、証明書を受領したこととなる。
- 証明書のダウンロードまたは電子メールに添付されたメッセージからの証明書のインストール
- 利用者が、証明書、もしくは、その構成に異議を唱えない場合

4.4.2　認証機関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公開されたリポジトリを用いて発行した証明書を公開する。

4.4.3　他のエンティティに対する認証機関の証明書発行通知

登録機関は、自らの承認した証明書発行に関する通知を受け取る場合がある。

4.5　鍵ペアと証明書の用途

4.5.1　利用者の秘密鍵および証明書の使用

証明書における公開鍵に対応した秘密鍵の使用は、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。その証明書は、シマンテックの利用規約ならびに STN の CP および本 CPS の条件に従って合法的に使用されなければならない。証明書の使用は、証明書に含まれる keyUsage エクステンションに一致していなければならない(例えば、もし Digital Signature が有効となっていない場合には、署名に使用されてはならない)。

利用者は、自らの秘密鍵を不正に使用されないよう保護し、証明書の有効期間が満了しまたは証明書が失効した場合は、秘密鍵の使用を中止しなくてはならない。利用者以外の者は、本 CPS セクション 4.12 に規定する場合を除き、利用者の秘密鍵を保管してはならない。

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。

証明書の依拠は、特定の状況下において、合理的でなければならない。具体的状況により追加の確認が必要であることを示している場合、依拠当事者は、そのような依拠が合理的であるとみなされるために、当該確認を行わなければならない。

依拠する行為を行う前に、依拠当事者は、独自に次のことを行う。

- 与えられた目的のために証明書を使用することが適当であるか否かを評価し、証明書が実際に、本 CPS で禁止されまたは制限されていない適切な目的に使用されるものであるか否かを決定する。シマンテックは、証明書使用の適切さの評価について責任を負わない。
- 証明書は、証明書中に含まれる KeyUsage エクステンションに従って使用されるか否かを独自に評価する(例えば、Digital Signature が有効でない場合には、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ない)。
- 証明書および証明書を発行したチェーン内の全認証機関ステータスを評価する。証明書チェーン中の証明書が一つでも失効されている場合、依拠当事者は、エンドユーザ利用者の電子証明書によって、証明書チェーンの中の証明書が失効される前に署名された電子署名が信頼できるかどうかを調査する単独の責任がある。当該依拠は、依拠当事者の単独のリスクで行われるものとする。

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操作のために適切なソフトウェアやハードウェアを使用しなければならず、これがこれらの操作に関連する電子証明書に依拠する条件となる。当該操作は、証明書チェーンを識別すること、証明書チェーン内の全証明書の電子署名を検証することを含む。

4.6 証明書のリニューアル

証明書のリニューアルは、公開鍵その他の証明書情報に変更を伴わない、利用者への新しい証明書の発行を意味する。証明書のリニューアルは、殆どのウェブ・サーバの鍵生成ツールが既存の鍵ペアで新しい証明書のリクエストファイルの作成を行うことができるので、鍵ペアがウェブ・サーバ上で生成されるClass 3証明書に対応している。

4.6.1 証明書がリニューアルされる場合

既存の利用者証明書の有効期間が満了する前に、利用者は、証明書を継続して使用するために、新しい証明書にリニューアルする必要がある。証明書は、有効期間満了後に、リニューアルすることもできる。

4.6.2 リニューアルを申請することができる者

個人向け証明書についてはその利用者、組織向け証明書についてはその権限のある者のみが、証明書のリニューアルを依頼できる。

4.6.3 証明書のリニューアル申請の手続

リニューアルの手続きにおいては、エンドユーザ利用者証明書を更新しようとしている者または組織が、実際にその証明書の利用者(または利用者によって承認されている者)であることが確認される。

チャレンジフレーズ(またはこれと同等なもの)の使用または秘密鍵の保有を証明することが上記手続きの条件を満たす一つの方法である。利用者は申請情報と共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、提示する。証明書のリニューアルの際、利用者の再登録情報とともに、チャレンジフレーズ(またはこれと同等なもの)が正しく提示され、申請責任者および技術担当者情報を含む申請者情報が変更されていなければ、リニューアルされた証明書は自動的に発行される。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、シマンテックは証明書の更新に際し、認証された企業連絡先のメールアドレスに電子メールを送信し、証明書更新の要求確認と、証明書発行の承認を要求する。証明書発行を承認する確認が取れた場合、シマンテックは申請時の情報[11]が変更されていないことを確認し、証明書を発行する[12]。

この方法によるリニューアル後、そしてそれ以降リニューアルが行われる際に、シマンテックまたは登録機関は本 CPS に記載される証明書申請の認証要件に従い申請者の実在性の再確認を行う。

特に、Class 3 組織向け SSL サーバ証明書の場合、シマンテックは、証明書に含まれる組織名称、ドメイン名の再認証を本 CPS セクション 6.3.2 に記載の間隔で行う。

要件

- チャレンジフレーズがリニューアルされる証明書に対して正しく使用されているか、または、申請責任者から電子メールにより確認の返信を得られたこと
- 証明書の識別名が変更されていないこと
- 申請責任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こと

[11] 所定の変更手続きにより連絡先情報が変更されている場合、証明書は自動更新可能である。
[12] 製品によってはこの手続きを実施しない場合がある。

シマンテックは、証明書のリニューアルの申請に際し、組織が申請を許可し、申請者に組織を代表して証明書の申請の権限があることについて、電話、郵便またはこれらに相当する方法による再確認は行わない。

上記の方法またはシマンテックが認めるその他の方法以外に、最初の証明書申請に対して行った確認および認証の要件がエンドユーザ証明書のリニューアルに適用される。

4.6.4 利用者に対する新しい証明書発行通知

利用者に対するリニューアルされた証明書の発行通知は、セクション 4.3.2 に従う。

4.6.5 リニューアルされた証明書の受領確認の行為

リニューアル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 に従う。

4.6.6 認証機関によるリニューアルされた証明書の公開

リニューアルされた証明書は、シマンテックのリポジトリで公開される。

4.6.7 他のエンティティに対する認証機関の証明書発行通知

登録機関は、自らの承認した証明書発行に関する通知を受け取る場合がある。

4.7 証明書のリキー

証明書のリキーは、新しい公開鍵を認証する新しい証明書の発行の申請である。証明書のリキーは、全証明書 Class に対応している。

4.7.1 証明書がリキーされる場合

既存の利用者証明書の有効期間が満了する前に、利用者は、証明書を継続して使用するために証明書をリキーする必要がある。証明書は、有効期間満了後に、リキーすることもできる。

4.7.2 新しい公開鍵の証明書を申請することができる者

個人向け証明書についてはその利用者、組織向け証明書についてはその権限のある者のみが、証明書のリキーを申請できる。

4.7.3 証明書のリキー申請の手続

リキー手続きにおいては、エンドユーザ利用者証明書を更新しようとしている者または組織が、実際にその証明書の利用者(または利用者によって承認されている者)であることが確認される。

チャレンジフレーズ(またはこれと同等なもの)の使用または秘密鍵の保有を証明することが上記手続きの条件を満たす一つの方法である。利用者は申請情報と共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、提示する。証明書のリキーの際、利用者の再登録情報とともに、チャレンジフレーズ(またはこれと同等なもの)が正しく提示され、連絡先情報を含む申請者情報が変更されていない場合、更新された証明書は自動的に発行される。この方法によるリキー後、そしてそれ以降リキーが行われる機会に、シマンテックまたは登録機関は最初の証明書申請の認証要件に従い申請者の実在性の再確認を行う。

上記の方法またはシマンテックが認めるその他の方法以外に、最初の証明書申請に対して行った確認および認証の要件がエンドユーザ証明書のリキーに適用される。

4.7.4 利用者に対する新しい証明書発行通知

利用者に対するリキーされた証明書の発行通知は、セクション 4.3.2 に従う。

4.7.5 リキーされた証明書の受領確認の行為

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 に従う。

4.7.6 認証機関によるリキーされた証明書の公開

リキーされた証明書は、シマンテックのリポジトリで公開される。

4.7.7 他のエンティティに対する認証機関の証明書発行通知

登録機関は、自らの承認した証明書発行に関して通知を受け取ることがある。

4.8 証明書の変更

4.8.1 証明書が変更される場合

証明書の変更は、利用者の公開鍵の変更を除く、既存の証明書の情報に変更であり、新しい証明書の発行の申請を参照することとなるがあった場合に行われる。

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取り扱われる。

4.8.2 証明書の変更を申請することができる者

本 CPS セクション 4.1.1 を参照のこと。

4.8.3 証明書の変更申請の手続

シマンテック、もしくは、登録機関は、セクション 3.2 に規定される全利用者情報の確認と認証を行う。

4.8.4 利用者に対する新しい証明書発行通知

本 CPS セクション 4.3.2 を参照のこと。

4.8.5 変更された証明書の受領確認の行為

本 CPS セクション 4.4.1 を参照のこと。

4.8.6 認証機関による変更された証明書の公開

本 CPS セクション 4.4.2 を参照のこと。

4.8.7 他のエンティティに対する認証機関の証明書発行通知

本 CPS セクション 4.4.3 を参照のこと。

4.9 証明書の失効および効力の停止

4.9.1 失効が行われる場合

以下に記載された場合にのみ、エンドユーザ利用者証明書は、シマンテックまたは利用者によって失効され、CRL 上に記載される。以下に示される以外の理由によって証明書を使用できない(または、もはや利用を望まない)利用者から申請を受けた場合には、シマンテックは、そのデータベース中に有効でないものとしてのフラグを設定するが、CRL 上で公表はしない。

利用者証明書は、次のいずれかの事由が生じた場合には失効される。

- シマンテック、カスタマまたは利用者において、利用者の秘密鍵の危殆化が生じたものと信ずべき理由があり、またはそのことが強く推測される場合
- シマンテックまたはカスタマにおいて、利用者が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重大な違反を行ったと信ずべき理由がある場合
- 利用者との利用規約が終了した場合
- エンタープライズ・カスタマと利用者との関係が終了した場合
- シマンテックまたはカスタマにおいて、証明書が本 CPS によって要求される手続に重要な点において従っていないか、証明書(Class 1 証明書を除く)が証明書上に Subject として記載されている者以外の者に対して発行されたか、または証明書(Class 1 証明書を除く)が当該証明書上に Subject として記載されている者の許可を受けずに発行されたかのいずれかの事由があると信ずべき理由がある場合
- シマンテックまたはカスタマにおいて、証明書申請中の重要な事実が虚偽であると信ずべき理由がある場合
- シマンテックまたはカスタマが、証明書発行に関する重要な前提条件が満たされておらずかつ当該条件を満たすよう請求することがないと、決定した場合
- 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となった場合
- 証明書中に含まれる情報(ただし、確認を実施しない利用者情報を除く)が正しくないかまたは変更された場合
- 本 CPS セクション 6.3.2 に定める間隔で利用者の実在性が再確認できなかった場合
- 利用者が期限までに利用料を支払わなかった場合
- その証明書の継続的な使用が、STN に悪影響を与える場合

シマンテックは、証明書の使用が、STN に悪影響を与えると考える場合、特に、以下のことを考慮する。

- 受領した苦情の質と回数
- 苦情を申し立てた者に対する本人確認

- 効力を有する関連法規
- 申し立てられた有害な使用に対する利用者からの回答

コード・サイニング証明書の使用が、STN に悪影響を与えると考える場合、シマンテックは、上記に加えて、特に以下のことを考慮する。

- 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公開
- そのコードになされた追加の申し立て

シマンテックは、また、管理者として行為するための管理者権限が終了した場合、管理者証明書を失効させることができる。

シマンテックの利用規約において、利用者に対し、その秘密鍵の危殆化を知りまたはその疑いがある場合に、直ちにその旨をシマンテックに通知する義務があることを規定する。

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・サイニング証明書ならびにドメイン認証および組織認証の SSL 証明書は、STN の補足として本 CPS の Appendix B1、Appendix C および Appendix D それぞれのセクション 13 に定める手続きにより、CA/ブラウザフォーラムの定める要件に準拠する。

4.9.2 証明書の失効を申請することができる者

個人の利用者は、自己の証明書につき失効をシマンテックまたは登録機関を通じて申請することができる。組織向け証明書の場合においては、当該組織の正当な権限のある者のみが当該組織に対して発行された証明書の失効を申請することができる。シマンテックもしくは登録機関の正当な権限のある者は、登録機関の管理者証明書の失効を申請することができる。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、または失効を申請することができる。

シマンテックは、自己の認証機関に対して発行された証明書の失効を申請し、または失効させることができる。登録機関は、自己の正当な権限のある者を通じて、自己の証明書の失効依頼を申請することができる。

4.9.3 失効申請要求の手続

4.9.3.1 エンドユーザ利用者の証明書の失効申請手続

証明書の失効を申請しようとする利用者は、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てその旨知らせるものとし、申請を受けた者は速やかに証明書の失効に着手する。エンタープライズ・カスタマに関しては、利用者は当該エンタープライズの管理者に対して証明書の失効申請を知らせるものとし、当該管理者は失効申請をその処理のためシマンテックに知らせるものとする。失効申請の連絡については、本 CPS セクション 3.4 に定めるところに従う。非エンタープライズ・カスタマに関しても、証明書の失効を申請する場合は、本 CPS セクション 3.4 に従う。

エンタープライズ・カスタマが、自らの判断で、エンドユーザ利用者証明書の失効を申請する場合、マネージド PKI カスタマは、当該証明書の失効をシマンテックに指示するものとする。

4.9.3.2 証明書の失効に関する CA/ブラウザフォーラム要件

EV SSL 証明書、EV コード・サイニング証明書ならびにドメイン認証および組織認証の SSL 証明書は、STN の補足として本 CPS の Appendix B1 および Appendix C それぞれのセクション 13 ならびに Appendix D セクション 13.1 にそれぞれ定める手続きにより、CA/ブラウザフォーラムの定める要件に準拠する。

4.9.3.3 認証機関もしくは登録機関証明書の失効申請手続

自らの認証機関または登録機関の証明書の失効申請を行う認証機関または登録機関は、シマンテックに対しその旨知らせるものとする。シマンテックは、それを受けて当該証明書の失効を行う。シマンテックは、認証機関または登録機関の証明書の失効に自ら着手することもできる。

4.9.4 失効申請の猶予期間

証明書の失効申請は、商業上合理的な期間内に、可能な限り速やかに提出されるものとする。

4.9.5 認証機関が失効申請を処理しなければならない期間

シマンテックは、遅滞なく失効申請を処理するよう、商業上合理的な方策を講じる。

4.9.6 依拠当事者に要求される CRL の調査

依拠当事者は、自己が依拠しようとする証明書のステータスについて調査しなければならない。依拠当事者が証明書ステータスを調査するための一つの方法は、依拠当事者が依拠しようとする証明書を発行する認証機関が公表した最新の CRL を調査することである。または、依拠当事者は、適切な LDAP ベースのリポジトリや OCSP(利用可能である場合)を用いて、証明書ステータスを調査することによって当該要求を満たすことができる。認証機関は、失効のステータスを調査するために、依拠当事者に、適切な CRL、LDAP ベースのリポジトリまたは OCSP(利用可能である場合)の所在場所についての情報を提供する。

4.9.7 CRL の発行頻度

エンドユーザ利用者証明書についての CRL は、少なくとも一日一回発行される。認証機関証明書に対する CRL は、少なくとも年一回発行されるが、認証機関証明書が失効した場合は、その都度発行される。

Authenticated Content Signing (ACS)のルート認証機関についての CRL は、毎年発行されるが、認証機関証明書が失効した場合は、その都度発行される。CRL に記載されている証明書の有効期間が満了した場合、その証明書の期間満了後に発行される CRL から削除される場合がある。

4.9.7.1 CRL の発行に関する CA/ブラウザフォーラム要件

EV SSL 証明書、EV コード・サイニング証明書ならびにドメイン認証および組織認証の SSL 証明書に関する CRL の発行は、STN の補足として本 CPS の Appendix B1 および Appendix C それぞれのセクション 13 ならびに Appendix D セクション 13.2.2 にそれぞれ定める手続きにより、CA/ブラウザフォーラムの定める要件に準拠する。

4.9.8 CRL の最大発行所要時間

CRL は、作成後、商業的に合理的な時間内にリポジトリに掲載される。これは、通常は、作成から数分以内に自動的に実行される。

4.9.9 利用可能なオンラインによる失効/ステータス調査

オンラインによる失効および他の証明書のステータス情報は、ウェブベース、LDAP ベースのリポジトリ、および（提供されている場合は）OCSP を通じて提供される。シマンテックは、CRL の公表に加え、シマンテックのリポジトリのクエリー機能を通じて、証明書ステータス情報を提供する。

SSL サーバ証明書およびコード・サイニング証明書のステータス情報は、シマンテックのリポジトリにある証明書ステータス確認のリンク先のクエリー機能を通じて利用することができる。

シマンテックは、OCSP の証明書ステータス情報を提供している。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することができる。関係する OCSP レスポンダーの URL は、エンタープライズ・カスタマに連絡される。

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・サイニング証明書ならびにドメイン認証および組織認証の SSL 証明書での OCSP の利用については、STN の補足として本 CPS の Appendix B1 および Appendix C それぞれのセクション 13 ならびに Appendix D セクション 13.2.2 にそれぞれ定める手続きにより、CA/ブラウザフォーラムの定める要件に準拠する。

4.9.10 オンラインによる失効調査要件

依拠当事者は、依拠しようとする証明書のステータスをチェックしなくてはならない。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を関連する最新の CRL を参照することにより調査しなかった場合には、当該依拠当事者は、適用されるリポジトリを参照するか、または(OCSP のサービスが利用できる場合は)適用される OCSP レスポンダーを使い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チェックしなければならない。

4.9.11 利用可能な失効の公表についての他の形式

適用せず。

4.9.12 鍵の危殆化に関する特別な要件

シマンテックは、シマンテック認証機関またはサブドメイン下の認証機関の秘密鍵につき危殆化が生じたことを発見したか、そう信ずるに足る理由がある場合には、その旨を潜在的な依拠当事者に対し通知するよう商業上合理的な努力をする。

4.9.13 効力を停止する場合

適用せず。

4.9.14 効力停止申請をすることができる者

適用せず。

4.9.15 効力停止申請の手続

適用せず。

4.9.16 効力停止の制限

適用せず。

4.10 証明書のステータス・サービス

4.10.1 運用上の特徴

公開された証明書ステータスは、シマンテックのウェブ・サイトの CRL、LDAP ディレクトリ、および(利用できる場合)OCSP レスポンダーを通じて確認することができる。

4.10.2 サービスの可用性

証明書ステータス・サービスは、計画停止を除き 24 時間 365 日利用可能である。

EV SSL 証明書、EV コード・サイニング証明書ならびにドメイン認証および組織認証の SSL 証明書での証明書ステータス・サービスについては、STN の補足として本 CPS の Appendix B1 および Appendix C それぞれのセクション 13 ならびに Appendix D セクション 13.2.3 にそれぞれ定める手続きにより、CA/ブラウザフォーラムの定める要件に準拠する。

4.10.3 オプション機能

OCSP は、証明書のステータスを調査するためのオプション・サービスであり、全製品に使用できるものではなく、ある特定の製品に対してのみ利用可能である。

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することができる:

- 利用者の証明書を、リニューアルやリキーすることなく有効期限満了とした場合
- 利用者の証明書を、証明書を取り替えることなく有効期限前に失効させた場合

4.12 鍵の預託と復旧

キーマネージメントサービスを利用している場合を除き、STN 参加者は、認証機関、登録機関、エンドユーザ利用者の秘密鍵を預託しない。

キーマネージメントサービス(またはシマンテックが承認した同等のサービス)を用いるエンタープライズ・カスタマは、自己が承認した証明書申請を行った利用者の秘密鍵のコピーを預託することできる。キーマネージメントサービス(またはシマンテックが承認した同等のサービス)はシマンテックの安全な

データ・センタ施設内もしくは施設外で運用される。シマンテックは、利用者の秘密鍵の保管は行わないものの、当該利用者の鍵の復旧手順に関し、重要な役割を果たす。

4.12.1 鍵の預託ならびに復旧時のポリシーおよび実施

キーマネージメントサービス(またはシマンテックが承認した同等のサービス)を利用するエンタープライズ・カスタマは、エンドユーザ利用者の秘密鍵を預託することが許される。預託された秘密鍵は、マネージド PKI キーマネージャー・ソフトウェアを用いて暗号化され保管される。キーマネージメントサービス(またはシマンテックが承認した同等のサービス)を利用するエンタープライズ・カスタマを除き、認証機関またはエンドユーザ利用者の秘密鍵は預託されることはない。

エンドユーザ利用者の秘密鍵は、キーマネージメントサービスの管理者ガイドによって認められる場合のみ復旧し得る。当該ガイドにおいては以下のことが求められる。

- キーマネージメントサービスを使用しているエンタープライズ・カスタマは、その秘密鍵の利用者だと主張している者からの当該秘密鍵の要求が実際にその利用者からの要求であり、不正によるものではないことを確認するため、当該利用者だと主張する者の本人確認を行う。
- エンタープライズ・カスタマは、違法、詐欺その他の不正な目的のためではなく、司法または行政手続もしくは捜索令状に従う場合のような合法的な目的の場合のみ、利用者の許可なしに、利用者の秘密鍵を復旧する。
- このようなエンタープライズ・カスタマは、キーマネージメントサービス管理者およびその他の者が秘密鍵へ許可なくアクセスすることを防ぐため、要員管理を行う。

キーマネージメントサービスを利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る。

- 利用者に対する当該利用者の秘密鍵が預託されたことの通知
- 利用者の預託された秘密鍵の不正な開示からの保護
- 利用者の預託された秘密鍵の復旧に使用される管理者自身の鍵を含む全情報の保護
- 適切に認証され承認された要求に対してのみ預託された秘密鍵を引き渡すこと
- 利用者自身が管理する秘密鍵の紛失により証明書の利用を終了する事象が発生した場合に、暗号化され預託された秘密鍵を復旧する前に利用者鍵ペアを失効させること
- 利用者自身が復旧要求をした場合以外は、鍵復旧に関する情報を利用者へ提供しないこと
- 法律、政府の定める規則、当該エンタープライズ・カスタマの内規または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こと

4.12.2 セッションキーのカプセル化ならびに復旧時のポリシーおよび実施

秘密鍵は、キーマネージャー・データベース内で暗号化され保管される。それぞれの利用者秘密鍵は、個々にtriple-DESで暗号化される。Key Escrow Record (KER) が生成され、次に、triple-DESの鍵が、ハードウェアの中で生成されたランダムセッションキーマスクと結合される。結果として生じたマスクドセッションキー(MSK)のみが、シマンテックのマネージドPKIデータベースに安全に送られ、保管される。KER(エンドユーザの秘密鍵を含む) と個々のセッションキーは、キーマネージャー・データベースに保管され、その他の鍵関連データは破棄される。

マネージドPKIデータベースはシマンテックのデータ・センタ施設外から安全に操作することができる。エンタープライズ・カスタマはキーマネージャー・データベースをシマンテックの安全なデータ・センタ施設内もしくは施設外で運用することができる。

秘密鍵および電子証明書の復旧の場合、マネージドPKI管理者が安全にマネージドPKI コントロール・センタにログインし、復旧のための適切な鍵ペアの選択し、“recover”のハイパーリンクをクリックすることを要求される。承認された管理者が“recover”のリンクをクリックした後にのみ、鍵ペアに対するMSKは、マネージドPKIデータベースから返却される。キーマネージャーは、キーマネージャー・データベースからセッションキーを取り出しMSKと結合させ、最初に秘密鍵を暗号化するのに使われたtriple-DES の鍵を再生成し、エンドユーザの秘密鍵を復旧させる。最後に、暗号化されたPKCS#12ファイルが、管理者へ返却され、最終的にエンドユーザへ配布される。

5. 設備、管理および運用統制

5.1 物理的管理

シマンテックは、本CPSに対応する「Physical Security Policy」を作成し、実施している。セクション8に記載されている独立監査人による監査の要求基準は、このポリシーへの準拠性も含む。「Physical Security Policy」は、非公開のセキュリティ情報を含んでおり、シマンテックの合意の下にのみ参照することができる。要求基準に関する概要は以下で説明される。

5.1.1 立地場所および構造

シマンテックの認証機関と登録機関業務は、公然または非公然の不正侵入および機密情報とこれを扱う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下で行われる。

また、シマンテックは認証機関業務のために災害復旧施設を維持している。シマンテックの災害復旧施設はシマンテックの主施設に相当する複数の物理的セキュリティ階層により保護されている。

5.1.2 物理的アクセス

シマンテック認証機関システムは最低4階層の物理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へのアクセスが要求される。

各階層へのアクセスは、累進的に制限される物理的アクセス特権により管理される。機密を要する認証機関業務、認証、検証、および発行の証明手続きのライフサイクルに関連する全ての業務は、高度に制限された物理セキュリティ階層の中で行われる。各階層へのアクセスには近接型の入退室カードが要求される。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る。付加的な階層では、生体認証を含む二要素認証を必須とする。従業員および訪問者によるこれらの保護された階層へ入室においては、信頼された者の立会いを必須とする。

物理セキュリティシステムは、オンラインおよびオフラインのハードウェア暗号モジュールの保管場所、および鍵管理上必要となる重要資料の保護を目的とした追加のセキュリティ階層を含む。鍵生成および保管に用いられる区画は、デュアルコントロールと、生体認証を含む二要素認証を必須とする。オンラインに配置されたハードウェア暗号モジュールは施錠されたキャビネットにより保護され、オフラインに保管されるハードウェア暗号モジュールは施錠された金庫、キャビネットおよびコンテナにより保護される。ハードウェア暗号モジュールおよび鍵管理上必要となる重要資料へのアクセスは、シマンテックの職務分離に関する要件に従い制限される。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目的のために記録される。

5.1.3 電源および空調

シマンテックのセキュアな施設は、一次および予備の以下の設備を備えている。

- 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管理するための暖房、換気、空調システム

5.1.4 水による被害

シマンテックは、シマンテックのシステムへの水による被害の影響を最小にするための合理的な漏水対策を講じている。

5.1.5　火災予防および保護対策

シマンテックは、火災の予防および消火その他炎もしくは煙による影響を防ぐための合理的な予防策を講じている。シマンテックの火災予防および保護対策は、国内の火災安全規則に則って設計されている。

5.1.6　メディアの保管

商用ソフトウェアおよびデータ、監査資料、保存記録またはバックアップ資料を格納するメディアは、シマンテックの施設内に保管されるか、または、権限ある者だけがアクセスできる適切な物理的・論理的アクセス管理機能を有し、水害、火事および電磁気等による当該メディアの不測の損傷を防止するように設計された、上記施設外の安全な保管施設で保管される。

5.1.7　廃棄物処理

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るものとする。機密情報を収集または伝達するために利用されたメディアは、廃棄前に読取不可能となるようにするものとする。暗号化デバイスは、廃棄前に、物理的に破壊されるか、または製造業者のガイドラインに従い初期化されるものとする。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い、廃棄される。

5.1.8　オフサイト・バックアップ

シマンテックは、重要なシステム・データ、監査記録その他の機密情報のバックアップを定期的に行う。オフサイト・バックアップ・メディアは、保障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する物理的に安全な方法で保管される。

5.2　手続的管理

5.2.1　信頼される役割

信頼される者には、以下の事項に重大な影響を及ぼしうる、認証または暗号作業にアクセスしもしくはこれを管理する全ての従業員、独立請負業者およびコンサルタントを含む。

- 証明書申請中の情報の検証
- 証明書申請、失効要求、更新要求または申込情報の承認、拒絶その他の処理
- 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する人を含む）
- 利用者の情報または要求の取扱

信頼される者には、以下の者を含むが、これに限定されない。

- カスタマ・サービス要員
- キーマネージャー
- セキュリティ要員
- システム管理者
- 技術要員のうち指定された者
- 認証基盤の信頼性を管理するために指名された経営陣

シマンテックは、本セクションで明らかにされる要員の区分を、信頼される地位を有する信頼される者と考える。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 に定める資格要件を完全に満たさなければならない。

5.2.2 職務ごとに必要とされる人数

シマンテックは、業務内容に基づく職務の分離、および機密を要する業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管理手続きを定め、維持し、実施している。

職務上の責任に基づき、職務の分離を確実にするために、方針と管理手続きが制定される。認証機関用ハードウェア暗号モジュールおよび関連する鍵関係資料へのアクセスおよび管理等の最も機密を要する業務は、複数の信頼される者により行われる。

これらの内部統制手続きは、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 名の信頼される者が必要となるよう設計されている。認証機関用ハードウェア暗号モジュールへのアクセスは、その受入から最終の論理的または物理的破壊の検査までのライフサイクルを通じて、複数の信頼される者により厳格に実施される。モジュールが活性化されサービスに供されると、当該モジュールに関する一切の操作は、物理的および論理的にも複数の権限により管理される。モジュールへの物理的なアクセスができる者は、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、モジュールへの物理的なアクセスができない。

自動化された検証および発行システムによって発行されるもの以外の Class 3 証明書の検証および発行などの業務は、少なくとも 2 人の信頼される者によって、または少なくとも 1 人の信頼された者と自動化された検証および発行プロセスの組み合わせによって行われる。

5.2.3 それぞれの任務に必要な身元の確認

全ての信頼される者になろうとする者について、シマンテック担当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、運転免許証等）の調査により、本人確認作業が行われる。身元については、更に本 CPS セクション 5.3.1 に従い、身元調査が行われる。

シマンテックは、ある人物に対して以下を実施する前に、当該人物が信頼される地位を獲得していることおよび必要な部署の許可が取得されていることを保証する。

- アクセス用のデバイスが発行され、特定の必要とされた施設へのアクセスが許諾される
- シマンテック認証機関、登録機関その他情報技術システムへアクセスし特定の業務を行うための電子的な資格証明書の発行を行う

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は以下を含むが、これに限定されない。

- 証明書申請における情報の検証
- 証明書申請、失効要求、復旧要求、更新要求または申込情報の承認、拒絶その他の処理
- 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する者を含む）
- 利用者の情報または要求の取扱
- 認証機関証明書の生成、発行または破棄
- 認証機関のロード作業

5.3　人事的管理

信頼される者になろうとする者は、想定される業務を十分に遂行するために必要な経歴、資格および経験を有することの証拠を提出しなければならない。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許可も提出しなければならない。経歴調査は、信頼される地位を有する人員について少なくとも 5 年毎に繰返されるものとする。

5.3.1　経歴、資格、経験および許可要件

シマンテックは、信頼される者になろうとする者が、想定される業務を十分に遂行するために必要な経歴、資格および経験を有することの証拠を提出することを要求する。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許可も提出しなければならない。

5.3.2　経歴調査手続き

信頼される職務への雇用を行う前に、シマンテックは以下の事項を含む経歴調査を行う。

- 過去の雇用の確認
- 職歴の照会
- 最高学歴もしくは適切な学歴の確認

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拒絶される理由となりうるもの、或いは既存の信頼される者に対する何らかの措置を取る理由となりうるものは、一般的に以下のものを含む。

- 候補者または信頼される人物の不実表示
- 極めて芳しくないまた信頼できない身元照会結果

上記の情報を含む報告書は、シマンテック担当部門が査定を行い、経歴調査で明らかになった事項の種類、影響度および行動の頻度に照らし、適切な方針を決定する。この決定事項には、信頼されうる地位の候補者としての採用の中止、または既存の信頼されうる地位の剥奪を含む。

経歴調査、およびこれにより収集された情報の取扱は、日本の法律に従う。

5.3.3　トレーニング要件

シマンテックは、採用後、十分に業務を遂行できるよう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）を従業員に対し行い、受講の記録を保管する。シマンテックは、トレーニング・プログラムを必要に応じ定期的に見直し、改善する。

シマンテックのトレーニング・プログラムは、個々の業務に応じ策定され、関係するものとして次の事項を含む。

- PKI 基礎概念
- 業務責任
- シマンテックセキュリティならびに運用上のポリシーおよび手順
- 採用されるハードウェアおよびソフトウェアの利用と運用
- 事件および危殆化が発生した場合の報告ならびにその取扱
- 災害復旧および事業継続の手順

5.3.3.1 トレーニングとスキルに関する CA/ブラウザフォーラム要件

EV SSL 証明書、EV コード・サイニング証明書ならびにドメイン認証および組織認証の SSL 証明書のために行われる要員のトレーニングは、STN の補足として本 CPS の Appendix B1、Appendix C および Appendix D それぞれのセクション 14.1 に定める手続きにより、CA/ブラウザフォーラムの定める要件に準拠する。

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、従業員が業務を十分に遂行するための技能を維持することを確実にするために必要な範囲および頻度で、再教育を行う。

5.3.5 人事異動の頻度および順序

適用せず。

5.3.6 無権限の行為に対する制裁

無権限の行為またはシマンテックのポリシーおよび手順に対するその他の違反に対しては、適切な懲戒処分が取られる。懲戒処分には解雇を含み、無権限の行為の頻度および重大性に応じた措置が取られる。

5.3.7 請負事業者の要件

限定された環境下で、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る。これらの請負業者またはコンサルタントに対しては、同種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または同等の業務上およびセキュリティ上の基準が適用される。

本 CPS セクション 5.3.2 に記載する経歴調査を経ない請負事業者またはコンサルタントは、信頼される者に付添われ、直接に監督される範囲でのみシマンテックの安全に管理された施設内にアクセスすることができる。

5.3.8 要員に提供される資料

シマンテックは、業務を十分に遂行するために必要となるトレーニングおよび資料の提供を従業員に対し行う。

5.4 監査記録の手続き

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、次の重要なイベントについて記録する。

- 次の事項を含む、認証機関鍵のライフサイクル管理イベント
  - 鍵の生成、バックアップ、保管、復旧、および破壊
  - 暗号モジュールのライフサイクル管理イベント
- 次の事項を含む、認証機関証明書および利用者証明書のライフサイクル管理イベント
  - 証明書申請、リニューアル、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）

－証明書および CRL の生成と発行
・ 次の事項を含む、セキュリティに関連するイベント
－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を含む）
－シマンテックの要員によってなされた PKI およびセキュリティのシステムに対する行為
－セキュリティ上、取扱に慎重を要するファイルまたは記録に関する読み込み、書き込みまたは削除

－セキュリティ・プロファイルの変更
－システムの故障、ハードウェアの異常および他の異変
－ファイアウォールおよびルーターの動作
－認証機関の設備への来訪者の入退室

記録の記入事項は次の項目を含む
- 記録の日時
- 自動的な日々の記録に関しては、そのシリアルまたはシーケンスナンバー
- 日々の記録をなすエンティティの身元
- 記録の種別

シマンテックの登録機関とエンタープライズの管理者は、次の事項を含む、証明書申請情報に関する記録をとる。
- 証明書申請者により提出された身元確認の書類の種類
- 申請者の同一性確認のための書類がある場合、これに関するデータ、番号またはその組み合わせ（例えば、証明書申請者の運転免許証番号）
- 申請書および同一性確認のための書類写しの保管場所
- 申請を受領したエンティティの身元
- 同一性確認のための書類を検証するために用いられた方法があれば、その方法
- 証明書申請を受領した認証機関または発行指示を行った登録機関がある場合、その名称

EV SSL 証明書、EV コード・サイニング証明書ならびにドメイン認証および組織認証の SSL 証明書については、STN の補足として本 CPS の Appendix B1、Appendix C および Appendix D それぞれのセクション 15 に定める手続きにより、CA/ブラウザフォーラムの定める要件に準拠する。

5.4.2 記録を処理する頻度

認証機関システムは、常時監視される。重要なセキュリティおよび操作イベントが発生した場合即時に検知され、任命された要員によるレビューがなされる。

月次の監査ログレビューには、当該ログが改ざんされていないことの確認および記録された全ての警告もしくは異常における精査が含まれている。監査ログレビューに基づいて実施した対応についても、記録されるものとする。

5.4.3 監査記録を保持する期間

監査記録は、少なくとも処理後 2 ヶ月間は記録を行った場所で保管され、その後はセクション 5.5.2 に従い保管されなければならない。

5.4.4 監査記録の保護

監査記録は、無権限者による参照、変更、削除、または他の改ざん行為から記録ファイルを保護するための仕組みを含む電子的な監査記録システムにより保護される。

5.4.5 監査記録のバックアップ手続

監査記録の増加分のバックアップは毎日生成され、全体のバックアップは週に一度の頻度でなされる。

5.4.6 監査ログ集計システム（内部対外部）

自動で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る。手動で作成される監査データはシマンテックの要員により記録される。

5.4.7 イベントを生ぜしめた Subject に対する通知

監査ログ集計システムによりイベントが記録される場合、当該イベントを生ぜしめた個人、機関、デバイスまたはアプリケーションに対しては、何らの通知をすることも要求されない。

5.4.8 脆弱性の評価

システムの脆弱性を監視するため、監査プロセスの対象となるイベントが記録される。論理的なセキュリティ脆弱性評価（LSVA）は、これらの記録されたイベントの調査後、実行され、調査され、変更される。LSVA はリアルタイムの自動的な記録データに基づきなされ、“Security and Audit Requirements Guide”の要件に従い、日次、月次および年次ベースで実行される。年次の LSVA は、年次の準拠性監査の資料として利用される。

5.5 記録の保管

5.5.1 保管される記録の種類

シマンテックは次の記録を保管する。

- セクション 5.4 により集められた全監査データ
- 証明書申請情報
- 証明書申請に関連する書類
- 失効、リキー、リニューアル申請情報などの証明書ライフサイクルに関連する情報

5.5.2 記録保管の期間

記録は、証明書の有効期間満了または失効の日から少なくとも次の期間保管されなければならない。

- Class 1 証明書については 5 年の間
- Class 2 および 3 証明書については 10 年 6 ヶ月の間

5.5.3 保管記録の保護

シマンテックは、権限のある信頼される者のみがアクセスすることができるよう、保管された記録の保護を行う。保管された記録は、無権限者による閲覧、変更、削除その他改ざんができないよう、信頼されるシステムにより保護される。保管データを格納するメディアおよび保管データを処理するた

めに必要なアプリケーションは、本 CPS にて定められた期間、保管データにアクセスできることを確実にするために維持管理されなければならない。

5.5.4 保管記録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的な記録について、増加分のバックアップは毎日これを行い、全体のバックアップは週に一度の頻度でこれを行う。紙媒体による記録のコピーは、オフサイトのセキュアな施設において保管されなければならない。

5.5.5 記録のタイム・スタンプに関する要件

証明書、CRL、および他の失効に関するデータベースのエントリは、日時の情報を含まなければならない。当該時間情報については暗号技術による処理が必要とされない。

5.5.6 保管記録収集システム（内部または外部）

エンタープライズ登録機関のカスタマのものを除き、保管記録収集システムは、シマンテック内部に存在する。エンタープライズ登録機関については、シマンテックは当該顧客の監査証跡の保存について支援をおこなう。したがって、このような保管記録収集システムは、そのエンタープライズ登録機関にとっては外部となる。

5.5.7 保管記録情報の取得および検証の手続

許可された信頼される者だけが保管記録へアクセスすることができる。保管された情報の復旧の際には、その整合性の検証を行う。

5.6 鍵の切り替え

シマンテック認証機関の鍵ペアは、本 CPS に定められたそれぞれの最大ライフタイムの満了時にその役割を終了する。シマンテック認証機関証明書は、その累計した認証機関鍵ペアのライフタイムがその最大ライフタイムとして定められた期間を超えない限りにおいて、更新することができる。新規の認証機関鍵ペアは、例えば、役割が終了する認証機関鍵ペアの交換を行う場合、実際に使用されている鍵ペアを補完する場合および新しいサービスをサポートする場合など、必要に応じ生成される。

上位認証機関の認証機関証明書の有効期間満了に先立ち、上位認証機関階層の内部において、古い上位認証機関鍵ペアから新しい上位認証機関鍵ペアへの円滑な移行を可能にするために、鍵の切り替え手続が定められる。シマンテック認証機関の鍵切り替え手続は、次のことを要求する。

- 上位認証機関は、自己の鍵ペアの残存ライフタイムが、自らの階層内の下位認証機関により発行された証明書の有効期間と等しくなる日の遅くとも 60 日以上前の日（以下「発行停止日」という）に新たな下位認証機関の証明書の発行を停止する。
- 有効性検証に合格した下位認証機関（または利用者）証明書の発行申請で発行停止日の後に受領されたものに関しては、当該証明書は新しい認証機関の鍵ペアを用いて署名されるものとする。

上位認証機関は、元の鍵ペアを用いて発行された最後の証明書の有効期間満了日までは、元の上位認証機関の秘密鍵を用いて、CRL の発行を継続するものとする。

5.7 危殆化および災害からの復旧

5.7.1 事故および危殆化の取扱手続

認証機関に関する特定の情報（証明書申請データ、監査データ、発行された全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保管が行われ、危殆化または災害が発生した場合に利用可能でなければならない。認証機関の秘密鍵のバックアップは CP セクション 6.2.4 に従い生成され維持されなければならない。シマンテックは、自身、および自身のサブドメインに属するエンタープライズ・カスタマの認証機関に関する前記の認証機関情報のバックアップを維持管理する。

5.7.2 コンピューターの資源、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、当該事象の発生についてはシマンテックのセキュリティ担当部署に報告されるものとし、シマンテックの事故取扱手続が規定される。当該手続は、適切な上位者に対する報告、事故調査および事故対応を含む。もし必要であれば、シマンテックの鍵の危殆化または災害復旧手続が規定される。

5.7.3 エンティティの秘密鍵が危殆化した場合の手続

シマンテック認証機関、シマンテックのインフラストラクチャまたはカスタマ認証機関の秘密鍵についての危殆化が認知されるか、その疑いが生じた場合、シマンテックの鍵危殆化対応手続が、インシデントレスポンスチームにより制定される。このチームは、セキュリティ、キーマネージャー、システム運用部門の要員および他のシマンテック管理者の代表者を含むものであるが、状況を評価し、アクションプランを作成し、シマンテックの経営陣の承認を得て当該アクションプランを実施する。

認証機関証明書の失効が必要な場合、次の手続が実施される。

- 証明書が失効された状態にあることを、依拠当事者に対し、本 CPS セクション 4.9.7 に従い、シマンテックのリポジトリを通じて、連絡する。
- 影響を受ける全ての STN 参加者に対して、失効の追加通知がなされるべき商業上合理的な努力がなされる。
- 認証機関が本 CPS セクション 5.8 に従い終了していない限り、本 CPS セクション 5.6 に従い新しい鍵ペアを生成する。

5.7.4 災害後の事業継続能力

5.7.4.1 米国シマンテック

米国シマンテックは、事業を中断しなければならないような状況下で、重要な事業機能を回復させるための事業継続計画を作成し維持している。米国シマンテックは主要施設から地理的に離れた米国シマンテックが所有する障害復旧拠点(Disaster Recovery Facility、以下「DRF」)を維持している。DRF は連邦政府と軍規格で設計された強固な施設で、特に米国シマンテックのセキュリティ基準を満たしている。

自然または人為的災害が発生した状況により米国シマンテックの主要施設が永久に利用できない場合、シマンテック事業継続チームとシマンテック認証業務インシデント管理チームは機能横断的な管理チームを調整し、災害状況を公式に明らかにするための判断を行い、インシデントを管理する。災害状況を明らかにした後、DRF での米国シマンテックのサービス機能の復旧に着手する。

米国シマンテックは、STN PKI サービスを含むマネージド PKI サービスのための災害復旧計画（Disaster Recovery Plan、以下「DRP」）を策定している。DRP はバックアップ データとバックアップされた STN 認証機関の鍵ペア複製を利用して行うシマンテック STN 運用の再構成期間における手順を定義する。

EV SSL 証明書、EV コード・サイニング証明書ならびにドメイン認証および組織認証の SSL 証明書での DRP については、STN の補足として本 CPS の Appendix B1 および Appendix C それぞれのセクション 16 ならびに Appendix D セクション 16.4 にそれぞれ定める手続きにより、CA/ブラウザフォーラムの定める要件に準拠する。

主要サービス機能の目標復旧時間は 24 時間以内とする。

米国シマンテックは、DRF のサービス機能の確認のため災害復旧テストを少なくとも 1 年に 1 回実施する。全社的な事業継続訓練もシマンテック事業継続チームにより年次で追加的なシナリオ(例パンデミック、地震、洪水、停電)を確認し評価するために実施する。

米国シマンテックは事業復旧計画の策定、維持、評価に多大な時間を費やし、米国シマンテックの災害あるいは大きな事業の停止のための計画は業界における最良の方法に一致している。
米国シマンテックは、その災害復旧施設において、冗長なハードウェアと共に自己の認証機関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ている。更に、認証機関の秘密鍵は本 CPS セクション 6.2.4 に従い、災害復旧目的でバックアップされ、維持されている。

米国シマンテックは、米国シマンテック・サブドメイン内のサービス・センタ、エンタープライズ・カスタマの各認証機関のみならず、自らの認証機関に関する重要な認証機関情報のバックアップを、オフサイトで保管している。当該情報は、証明書申請データ、監査データ（本 CPS セクション 5.4 による）および全ての発行済証明書に関するデータベースレコードを含むが、これらに限定されない。

5.7.4.2 シマンテック

シマンテックは、災害復旧サイトを主要な施設から 800 km 以上離れた場所に設置している。シマンテックは、あらゆる種類の自然または人為的な災害の影響を最小化するための災害復旧プランを作成し、実施し、テストしてきた。このプランは、定期的にテストされ、確認され、更新されることにより、災害時に使用できるようにされている。

情報システムサービスおよび主要な業務機能の復旧のための災害復旧計画が制定される。シマンテックの災害復旧サイトは、“ Security and Audit Requirements Guide”により、安全なバックアップ運用設備のために要求される物理的なセキュリティ保護および運用コントロールを実施している。

自然または人為的な災害が生じ、シマンテックの主要施設から一時的または恒久的な運用の停止を余儀なくされた場合、シマンテックの災害復旧プロセスがインシデントレスポンスチームにより開始される。

シマンテックの災害復旧プランは、災害後 24 時間以内に運用を回復し、最低限次の機能をサポートすることができるよう設計されている。

- 証明書の発行
- 証明書の失効
- 失効情報の公表
- キーマネージメントを用いるマネージド PKI カスタマに対する鍵回復情報の提供

シマンテックの災害復旧データベースは、“ Security and Audit Requirements Guide”に定める期限内に、本番環境用のデータベースと定期的に同期をとっている。シマンテックの災害復旧機器は、本

CPS セクション 5.1 に定める物理的セキュリティ層と同様の物理的セキュリティ保護により保護されている。

シマンテックの災害復旧プランは、シマンテックの主要なサイトにおいて災害が生じた日から 10 日以内に商業運用が再開されるよう設計されている。シマンテックは、全ての機能が運用不能となるような災害（大災害の場合を除く）が生じた場合、シマンテックの認証機関・登録機関機能をサポートするために主要サイトに設置されている機器を、検査する。当該検査の結果は、再調査の上、監査および計画のために保管される。可能な場合には、大災害の後可及的速やかに、シマンテックの主要サイトにおける運用は回復される。

シマンテックは、その災害復旧施設に、一部のハードウェアを冗長構成にすると共に自己の認証機関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ている。更に、認証機関の秘密鍵は本 CPS セクション 6.2.4 に従い、災害復旧目的でバックアップされ、維持されている。

シマンテックは、シマンテック・サブドメイン内のマネージド PKI カスタマの各認証機関のみならず、自らの認証機関に関する重要な認証機関情報のバックアップを、オフサイトで保管している。当該情報は、申請記録、証明書申請データ、監査データ（本 CPS セクション 5.4.1 による）および全ての発行済証明書に関するデータベースレコードを含むが、これらに限定されない。

5.8 認証機関または登録機関の終了

シマンテック認証機関またはマネージド PKI カスタマ認証機関が、その運用をやめる必要がある場合、シマンテックは、その終了に先立ち、利用者、依拠当事者および当該終了により影響を受ける他の当事者に対し、その旨を通知するよう商業上合理的な努力をする。認証機関の終了が必要な場合、シマンテックおよび、カスタマ認証機関の場合には、当該カスタマは、カスタマ、利用者および依拠当事者に対する混乱を最小化するために、終了プランを作成する。当該終了プランは、適宜次の事項に言及する。

- 利用者、依拠当事者およびカスタマ等、終了により影響を受ける当事者に対し、当該認証機関の状況を知らせる通知の提供
- 当該通知費用の取扱
- シマンテックにより当該認証機関に発行された証明書の失効
- 本 CPS セクション 5.5 により必要とされる期間中における当該認証機関の記録の保存
- 利用者およびカスタマ・サポート・サービスの継続
- CRL の発行またはオンライン・ステータス・チェッキング・サービスの維持等失効サービスの継続
- 必要に応じ、利用者および下位認証機関の証明書で有効期間満了前かつ、失効されていないものの失効
- 必要な場合、有効期間満了前でかつ失効されていない証明書について、終了プランにより失効された利用者への補償の支払い。または、後継の認証機関による代替証明書の発行
- 当該認証機関の秘密鍵および当該秘密鍵を含むハードウェア暗号モジュールの処分
- 当該認証機関のサービスを後継の認証機関に移行するために必要な規定

5.9 データセキュリティ

EV SSL 証明書、EV コード・サイニング証明書ならびにドメイン認証および組織認証の SSL 証明書の発行について、シマンテックは STN の補足として本 CPS の Appendix B1、Appendix C および Appendix D それぞれのセクション 16 に定める手続きにより、CA/ブラウザフォーラムの定める要件に準拠する。

6. 技術的セキュリティ・コントロール

6.1 鍵ペア生成およびインストレーション

6.1.1 鍵ペア生成

認証機関鍵ペアの生成は、複数の事前に選考され訓練を受けた信頼される個人により、信頼すべきシステムおよびセキュリティならびに鍵生成に要求される暗号強度を提供する手続を用いてなされる。第一次認証機関、その他のルート認証機関および中間認証機関については、鍵生成に用いられる暗号モジュールは、FIPS140-1 レベル 3 の要件を満たす。他の認証機関(シマンテック認証機関およびマネージド PKI カスタマ認証機関を含む)については、鍵生成に用いられる暗号モジュールは最低限 FIPS140-1 レベル 2 の要件を満たすものである。

全ての認証機関の鍵ペアは、“KeyCeremony Reference Guide”、“CA KeyManagement Tool User’s Guide” および“ Security and Audit Requirements Guide ”に従い、予め計画された鍵生成セレモニにおいて生成される。それぞれの鍵生成セレモニにおいて行われた活動は記録され、日付が付され、携わった全ての個人により署名される。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、監査および後日の調査の目的で保管される。

登録機関鍵ペアの生成は、一般的には、ブラウザ・ソフトウェアとともに提供される FIPS140-1 レベル1に認定された暗号モジュールを用いて、当該登録機関自身によりなされる。

マネージド PKI カスタマは、自動承認サーバで使用される鍵ペアを生成する。

利用者の鍵ペアの生成は、一般的には、当該利用者によりなされる。Class 1 証明書、Class 2 証明書および Class 3 コード/オブジェクト・サイニング証明書については、利用者は、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 に認定された暗号モジュールを通常用いる。サーバ用証明書については、利用者は、ウェブ・サーバ・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ーを通常用いる。

ACS アプリケーション ID については、暗号モジュールで生成した乱数シードを使用して、米国シマンテックまたはシマンテックが利用者の代わりに鍵ペアを生成する。当該暗号モジュールは、少なくとも FIPS 140-1 レベル 3 の要件を満たすものとする。

本 CPS に付属される Appendix B および Appendix C では、CA/ブラウザフォーラム要件に準拠する証明書についての追加要件を定義している。

6.1.2 秘密鍵の受渡

エンドユーザ利用者の鍵ペアは、当該利用者自身により通常生成されるため、この場合には利用者への秘密鍵の受渡は生じない。ACS アプリケーション ID の場合も、秘密鍵の受渡は生じない。

登録機関または利用者の鍵ペアが、シマンテックによりハードウェア・トークンまたスマートカードに予め生成されている場合には、当該デバイスは登録機関または利用者に対し、不正開封防止機能を施した上で商用配送サービスを用いて配布される。当該デバイスを起動するために必要なデータは、登録機関または利用者に対し、当該デバイスの配布とは別個の方法により配布される。当該デバイスの配布はシマンテックにより記録される。

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・トークンまたスマートカードに予め生成されている場合には、利用者に対し、不正開封防止機能を施した上で商用配送サービスを用いて配布される。当該デバイスを起動するために必要なデータは、登録機関または利用者に対し、

当該デバイスの配布とは別個の方法により配布される。当該デバイスの配布はエンタープライズ・カスタマにより記録される。

キー・リカバリー・サービスのためキーマネージメントを用いるマネージド PKI カスタマについては、カスタマは（自らが承認した証明書申請をなした利用者に代わり）、暗号用鍵ペアを生成し、当該鍵ペアを当該利用者に対し、パスワードで保護された PKCS#12 ファイルにて送信することが可能である。

6.1.3 公開鍵の証明書発行者への受渡

利用者および登録機関は、その公開鍵をその認証のためシマンテックに対し、PKCS#10 の証明書署名要求(CSR)を用いるか、または、セキュア・ソケット・レイヤ（SSL）/トランスポート・レイヤ・セキュリティ(TLS)によって保護されたセッションにおいて他のデジタル署名の付されたパッケージを用いて、送付するものとする。認証機関、登録機関または利用者の鍵ペアがシマンテックにより生成される場合、本要件は適用されない。

6.1.4 認証機関公開鍵のユーザへの受渡

米国シマンテックは、その第一次認証機関およびルート認証機関の認証機関証明書を、ウェブ・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する。新規の第一次認証機関およびルート認証機関の証明書が生成された場合、米国シマンテックは、当該ブラウザ・ソフトウェアの新版またはアップデート版への組み込みのため、当該新規証明書をブラウザ・ソフトウェア・メーカーに提供する。

シマンテックは、一般的に、全ての証明書チェーン（発行認証機関およびそのチェーン内の認証機関を含む）を、証明書の発行と同時に、利用者に対し提供する。シマンテック認証機関証明書は、シマンテックの LDAP ディレクトリ（directory.verisign.co.jp）からもダウンロードすることができる。

6.1.5 鍵のサイズ

鍵ペアの予想される使用期間においては、暗号解読技術によって鍵ペアの秘密鍵が解かれないように十分な長さの鍵ペアが使用されるべきである。米国シマンテック標準における一次認証局と認証局の最小の鍵のサイズは 2048 ビットのRSAと同等の強度を持つ鍵ペアを使用する [13]。米国シマンテックの第一次認証機関の鍵ペアと強度は次の表のとおりである。

公開鍵アルゴリズム	署名アルゴリズム	Class	世代
2048 bit RSA	SHA 1	Class 1, 2, 3 第一次認証機関	第三世代 (G3)
		Class 3 第一次認証機	第五世代（G5）

[13]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、認証機関の信頼性は 1024 ビットの RSA 鍵ペアからなる米国シマンテックの第一世代(G1)および第二世代(G2)の第一次認証機関をアンカーとするものまで保証される。1024 ビットの RSA 鍵ペアからなる利用者証明書の発行については、2014 年 1 月 31 日を以て有効期間満了となる条件において許可される。また、米国シマンテックの承認のもと、旧式アプリケーションを基盤とする事業継続維持のため、本 CPS セクション 6.3.2 に記載のプロセッシング・センタを運用するアフィリエートに対しても同様に例外として許可される。
シマンテックは、標準のウェブ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を意図された、最小限の数の SSL サーバ証明書を発行する権利を有する。
これらの証明書には、重要度クリティカルとして EKU 拡張が含まれ、その中には serverAuth フラグは設定されず、標準ウェブ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る。
カスタマおよび利用者（場合により依拠当事者を含む）のアプリケーションが、2048 ビットと同等以上の鍵サイズをサポートしていない特殊な環境において、シマンテックは、第一次認証期間および認証期間について、2048 ビット RSA または DSA を満たさない鍵サイズの鍵ペアによる証明書を発行する権利を有する。これらの証明書では、EKU フィールドに serverAuth フラグが除去され、2.16.840.1.113733.1.8.54.1 の OID が設定される。カスタマ、利用者、および依拠当事者は各自のリスクのもとで、かかる証明書を利用することとする。

		関	
	SHA256	Class 1, 2 and Class 3 Universal Root 第一次認証機関	第六世代(G6)
384 bit ECC	SHA384	Class 1, 2, 3(#)第一次認証機関	第四世代(G4)
4096 bit RSA	SHA384	Class 3 第一次認証機関	第六世代(G6)
2048_256 bit DSA	SHA256	Class 1, 2, 3 第一次認証機関	第七世代(G7)
(#) Class 3 の第四世代ルート証明書には、(旧)VeriSign ブランドのものと Symantec ブランドのものの二つが存在する。			

Table – 米国シマンテックの第一次認証機関と鍵のサイズ

全 Class における STN 第一次認証機関とその下位認証機関、登録局および利用者証明書に含まれるデジタル署名では、SHA-1 および SHA-2 署名アルゴリズムが使用される。また、特定のバージョンのプロセッシング・センタでは、利用者証明書の発行において、SHA-256 と SHA-384 を使用することができる。

6.1.5.1 鍵のサイズに関する CA/ブラウザフォーラム要件

EV SSL 証明書、EV コード・サイニング証明書ならびにドメイン認証および組織認証の SSL 証明書は、STN の補足として本 CPS の Appendix B1、Appendix C および Appendix D それぞれのセクション 9.5 に定める手続きにより、CA/ブラウザフォーラムの定める要件に準拠する。

米国シマンテックのルート認証機関証明書は、アルゴリズムと鍵サイズに関する次の要件に合致する。

	有効期間が2010年12月31日以前に開始となるもの	**有効期間が2010年12月31日より後に開始となるもの**
Digest algorithm	MD5 (非推奨) SHA-1, SHA-256, SHA-384 or SHA-512	SHA-1*, SHA-256, SHA-384 or SHA-512
RSAの最少モジュラス (bit)	2048**	2048
DSAの最少モジュラス (bit)	適用外	2048
ECC曲線	NIST P-256、P-384、P-521	NIST P-256、P-384、P-521

Table 4A – ルート認証機関証明書のアルゴリズムと鍵のサイズ

シマンテックの認証機関証明書は、アルゴリズムと鍵サイズに関する次の要件に合致する。

	有効期間が2010年12月31日以前に開始となり、2013年12月31日以前に終了するもの	**有効期間が2010年12月31日より後に開始となるか、もしくは、2013年12月31日より後に終了するもの**
Digest algorithm	SHA-1, SHA-256, SHA-384 or SHA-512	SHA-1*, SHA-256, SHA-384 or SHA-512
RSAの最少	1024	2048

モジュラス (bit)		
DSAの最少モジュラス (bit)	2048	2048
ECC曲線	NIST P-256、P-384、P-521	NIST P-256、P-384、P-521

Table 4B -シマンテックの認証機関証明書のアルゴリズムと鍵のサイズ

シマンテックの認証機関は、アルゴリズムと鍵サイズに関する次の要件に合致する利用者証明書を発行する。

	有効期間が2013年12月31日以前に終了となるもの	**有効期間が2013年12月31日より後に終了となるもの**
Digest algorithm	SHA-1*, SHA-256, SHA-384 or SHA-512	SHA-1*, SHA-256, SHA-384 or SHA-512
RSAの最少モジュラス (bit)	1024	2048
DSAでの最少モジュラス (bit)	2048	2048
ECC曲線	NIST P-256、P-384、P-521	NIST P-256、P-384、P-521

Table 4C - 利用者証明書のアルゴリズムと鍵のサイズ

* SHA-1 は、世間一般に使用されているブラウザでSHA-256が広くサポートされるようになるまでは使用されてもよい。

** 2010年12月31日より前に発行された、RSA2048 ビット未満の鍵長からなるルート認証機関証明書は、上述の要件に則して発行される利用者証明書の信頼の起点として提供されうる。

シマンテックの認証機関は、本セクションに記載されるアルゴリズムもしくは鍵サイズを満たさない公開鍵による証明書発行要求を受けた場合、その要求を却下する。

6.1.6 公開鍵のパラメータの生成

適用せず。

6.1.7 鍵用途目的(X.509 バージョン 3 鍵用途領域のとおり)

セクション 7.1.2.1 を参照のこと。

6.2 秘密鍵の保護

シマンテックは、シマンテックとエンタープライズ・カスタマの秘密鍵のセキュリティを確実にするため、物理的、論理的および手続的管理を実施している。利用者は契約により秘密鍵の紛失、漏洩、変更または無権限の者による使用を防止するために必要な対策を取ることが要求されている。

6.2.1　暗号モジュールの基準

第一次認証機関、その他のルート認証機関および中間認証機関の鍵ペアの生成ならびに認証機関の秘密鍵の保管に関し、シマンテックは FIPS140-1 レベル 3 の認定を受けもしくは重要な点においてこの要求を満たす ハードウェア暗号モジュールを使用している。

6.2.2　複数人による秘密鍵(m out of n) の管理

シマンテックは、機密を要する認証機関の暗号運用について複数の信頼できる個人が関与することを要求する技術的・手続的な仕組みを実施している。シマンテックは、認証機関の秘密鍵を利用するために「シークレット・シェアリング」という手法を用い、必要な起動データを、「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できる個人により保有させている。特定のハードウェア暗号モジュールに関して生成・分配されたシークレット・シェア総数（n）の内、一定数のシークレット・シェア（m）が、当該モジュールに保管されている認証機関の秘密鍵を起動させるために必要となる。

認証機関証明書に署名するために必要なシークレット・シェアは3人としている。災害復旧のための配布されるシェアの数は、通常運用のために用意される数より少ない場合がある。シークレット・シェアは、本CPSに従って保護される。

6.2.3　秘密鍵の預託

認証機関の秘密鍵は、預託を行わない。利用者秘密鍵の預託に関しては、セクション 4.12 で詳述される。

6.2.4　秘密鍵のバックアップ

シマンテックは、認証機関の秘密鍵のバックアップ用コピーを、通常の復旧および災害復旧の目的で生成する。当該鍵は暗号化された形でハードウェア暗号モジュール内にこれと関係する鍵保管デバイスとともに保管される。認証機関の秘密鍵保管に用いられる暗号モジュール は、本 CPS の要件に合致している。認証機関の秘密鍵は、本 CPS に従い、バックアップ用のハードウェア暗号モジュールにコピーされる。

認証機関秘密鍵の施設内バックアップ用コピーを含むモジュールは、本 CPS の要件に従う。認証機関の秘密鍵の災害復旧用コピーを含むモジュールは、本 CPS の要件に従う。

シマンテックは、登録機関の秘密鍵のコピーは保管しない。利用者の秘密鍵のバックアップについては、本 CPS セクション 6.2.3、4.12 を参照のこと。ACS に関しては、シマンテックは、利用者秘密鍵の複製を保持することはない。

6.2.5　秘密鍵の保管

シマンテック認証機関の満了時、その証明書に紐付く鍵ペアは、本 CPS に定める要件に合致するハードウェア暗号モジュールを用い最低 5 年間確実に保存される。認証局証明書は、本 CPS に定める期間内にリニューアルされない限り、これらの認証局鍵ペアは、それらの期間満了後、署名に使用されることはない。

シマンテックは、登録機関および利用者の鍵ペアのコピーについては保管しない。

6.2.6 秘密鍵の暗号モジュールへの入出力

シマンテックは、認証機関の鍵ペアを、当該鍵ペアが使用されるハードウェア暗号モジュールにおいて生成する。更に、シマンテックは、当該鍵ペアのコピーを通常の復旧および災害復旧の目的で作成する。認証機関の鍵ペアが他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、当該鍵ペアはモジュール間を暗号化されて移動される。

6.2.7 秘密鍵の暗号モジュールへの格納

ハードウェア暗号モジュールに保管される認証機関、登録機関の秘密鍵は暗号化された状態で保管される。

6.2.8 秘密鍵の起動の方法

シマンテック・サブドメインへの全参加者は、自己の秘密鍵の起動データにつき滅失、盗難、無権限者による漏洩または使用を防止しなければならない。

6.2.8.1 Class 1 証明書

Class 1 の秘密鍵の保護に関する STN スタンダードは、利用者において、利用者の承認なくして利用者のワークステーションおよびそれに関連づけられた秘密鍵が使用されることを防止するために必要な物理的保護を施すため商業上合理的な手段をとることである。更に、シマンテックは、利用者が、本 CPS セクション 6.4.1 に従いパスワードを用いるか、またはそれと同等の強度のセキュリティを用いて、秘密鍵の起動に先立ち利用者を認証すること、例えば、秘密鍵を運用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、またはネットワーク・ログオンのパスワードを用いることを推奨している。

6.2.8.2 Class 2 証明書

Class 2 の秘密鍵の保護に関する STN スタンダードは、利用者において、次の措置をとることである。

- 利用者が、本 CPS セクション 6.4.1 に従いパスワードを用いるか、またはそれと同等の強度のセキュリティを用いて、秘密鍵の起動に先立ち利用者を認証すること、例えば、秘密鍵を運用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を用いること、ならびに
- 利用者の承認なくして利用者のワークステーションおよびそれに関連づけられた秘密鍵が使用されることを防止するために必要な物理的保護を施すため商業上合理的な手段をとること

秘密鍵を非活性化する場合、暗号化された形式でのみ保管されることを要する。

6.2.8.3 Class 3 証明書(管理者を除く)

Class 3 の秘密鍵の保護（管理者を除く）に関する STN スタンダードは、利用者において、次の措置をとることである。

- スマートカード、生体認証を用いたデバイスと共に使用されるパスワード、また秘密鍵の起動前に利用者を同等の強度のセキュリティで認証すること
- 利用者の承認なくして利用者のワークステーションおよびそれに関連づけられた秘密鍵が使用されることを防止するために必要な物理的保護を施すため商業上合理的な手段をとる

こと

スマートカードまたは生体認証を用いたデバイスをセクション 6.4.1 に従ったパスワードと共に使用することが推奨される。秘密鍵を非活性化状態にする場合、暗号化された状態を維持されなければならない。

6.2.8.4 管理者の秘密鍵(Class 3)

管理者の秘密鍵の保護に関する STN スタンダードは、管理者に対し次のことを要求する。

- スマートカード、生体認証を用いたデバイスもしくは本 CPS セクション 6.4.1 に従ったパスワードを用いるか、またはそれと同等の強度のセキュリティ、例えは、秘密鍵を運用するためのパスワード、Windows ログオン、スクリーン・セーバーもしくはネットワーク・ログオンのパスワードを用いて、秘密鍵の起動に先立ち管理者を認証すること、ならびに
- 管理者の承認なくして管理者のワークステーションおよびそれに関連づけられた秘密鍵が使用されることを防止するために必要な物理的保護を施すため商業上合理的な手段をとること

スマートカード、生体認証を用いたデバイスもしく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 に従ったパスワードと共に使用して、秘密鍵を起動する前に管理者を認証することが推奨される。

秘密鍵を非活性化する場合、暗号化された形式でのみ保管されることを要する。

6.2.8.5 暗号モジュールを使用するエンタープライズ RA (自動承認またはキーマネージメントサービスを用いている場合)

暗号モジュール(自動承認またはキーマネージメントサービスとともに)を用いる管理者の秘密鍵の保護に関する STN スタンダードは、管理者に対し次のことを要求する。

- 秘密鍵の起動に先立ち管理者を認証するため、暗号モジュールを本 CPS セクション 6.4.1 に従ったパスワードと共に使用すること、ならびに
- 管理者の承認なくして暗号モジュール・リーダーを保管するワークステーションおよびそれに関連づけられた秘密鍵が使用されることを防止するために必要な物理的保護を施すため商業上合理的な手段をとること

6.2.8.6 プロセッシング・センタに保管される秘密鍵(Class 1-3)

オンライン認証機関の秘密鍵は本 CPS セクション 6.2.2 に従い、その起動データ(安全なメディアに保存される)を提供する必要数のシェアホルダーによって起動される。ひとたび秘密鍵を起動すると、当該秘密鍵は認証機関がオフラインになるまでの間、動作する。同様に、オフラインの認証機関の秘密鍵を起動させるためにおいても、シェアホルダーの提供する起動データが必要となる。ひとたび秘密鍵が起動されると、当該秘密鍵は一回に限り動作する。

6.2.9 秘密鍵の非活性化の方法

シマンテック認証機関の秘密鍵は、トークンリーダーから引き抜かれると非活性化される。登録機関の秘密鍵(登録機関申請を認証するために用いられたもの)はシステムログオフで非活性化される。登録機関は、その場を離れる場合に自らのワークステーションをログオフすることが要求される。

クライアントの管理者、登録機関、利用者の秘密鍵は作業が終了するたび、システムのログオフを行うたび、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たびといったように、ユーザによって採用された認証メカニズムにより非活性化される。全ての場合において、利用者は、その秘

密鍵を本 CPS に従い適切に保護する義務がある。ACS アプリケーション ID と関連する秘密鍵は、コード・サイニングで使用された後、速やかに削除される。

6.2.10 秘密鍵の破壊の方法

シマンテックは、必要な場合、認証機関の秘密鍵を、鍵の再生ができるような残余物が残らないことが合理的に確保される方法により破壊する。シマンテックは、認証機関の秘密鍵の完全な破壊を確実にするため、そのハードウェア暗号モジュールの初期化機能および他の適切な方法を活用する。鍵の破壊に関する認証機関の活動は記録される。ACS アプリケーション ID の秘密鍵については、証明書の利用と同時に鍵がシステムから破棄される。

6.2.11 暗号モジュールの評価

本 CPS セクション 6.2.1 を参照のこと。

6.3 鍵ペアの管理に関する他の点

6.3.1 公開鍵の保管

シマンテックの認証機関、登録機関および利用者の証明書はバックアップされ、シマンテックの日常バックアップ手続の一部として保管される。

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、その期間満了または失効により終了する。鍵ペアの使用可能期間は、それに関連づけられた証明書の有効期間と同一であるが、秘密鍵に関しては復号化のため使用を継続することができ、公開鍵は署名の検証のために使用を継続することができる。本CPSの発効日以降に発行された証明書に関するシマンテック証明書の最長の有効期間はTable 8 [14] に定めるとおりである。存在している利用者証明書から更新された利用者証明書は、より長い期間を持つ場合がある（上限は3ヶ月である。）。

さらに、シマンテック認証機関は、上位認証機関の証明書の有効期間満了後に下位認証機関が発行した証明書の有効期間が満了する事態が起こらぬよう、自己の認証機関証明書有効期間満了日前の適当な日に、新たな証明書の発行を停止する。

証明書の発行者	有効期間
自己署名された第一次認証機関 （1024 ビット RSA）	30 年まで
自己署名された第一次認証機関 （2048 ビット RSA）	50 年まで
自己署名された第一次認証機関 （256 ビット ECC）	30 年まで

[14] SHA 2 ファミリーまたは ECC アルゴリズムや 2048 ビット以上の鍵サイズの鍵ペアが使用されるなど、より強力な暗号化アルゴリズムや鍵サイズが使用されている証明書の場合、証明書の有効期間は、本 CPS セクション 6.3.2 に定められている制限を超えて拡張できる。

自己署名された第一次認証機関 (384 ビット ECC)	30 年まで
第一次認証機関から中間認証機関(オフライン)	通常 10 年まで(認証機関更新作業後は、15 年まで)
第一次認証機関から認証機関(オンライン)	通常 5 年まで(認証機関更新作業後は、10 年まで) (#1)
中間認証機関(オフライン)から認証機関(オンライン)	通常 5 年まで(認証機関更新作業後は、10 年まで) (#2)
認証機関(オンライン)から利用者(個人)	通常 3 年まで、ただし以下の(#2)の場合には 6 年まで。この場合、リニューアルやリキーは選択できない。6 年後は新規申請が必要である。
認証機関(オンライン)から利用者(組織)	通常 6 年まで(#3)とし、(#4)の場合を除き、リニューアルやリキーは選択できない。6 年後は新規申請が必要である。

Table 8 – 証明書の運用期間

(#1) Symantec Onsite Administrator CA-Class 3、および Class 3 OnSite Enterprise Administrator CA – G2 は、過去のシステムとの関係から10年を超える有効期間を持つが、適切な時期に失効される。
(#2) 6 年の有効期間をもつ利用者証明書が発行されている場合には、オンライン認証機関の証明書の有効期間は更新作業なしに 10 年に設定され、5 年経過後に認証機関鍵ペアの交換を行う。
(#3)組織向けリテール証明書は、6 年を上限として発行される。3 年を超える有効期間をもつ利用者証明書が発行されている場合には、証明書の発行日から 3 年経過後に再度、その識別名についての本人確認がなされる。
(#4)STN の機能の一部として利用される証明書に関しては、有効期間が 5 年までとされ、更新作業後は最長 10 年とすることができる。

STN CP のセクション 6.3.2 について、シマンテックは、認証機関の鍵ペアの移行中に PKI サービスが中断しないように、例外措置として認証機関が上記の指定を超える有効期間を持つことを認めるものとする。当該例外措置はプロセッシング・センタを有するアフィリエートにおいて、SSL サーバ証明書の発行に関与しないインフラ用途、管理用途の認証機関にのみ適用される。また、当該例外措置は、14 年間の有効期間を超えて認証機関の有効期間を延長するために適用してはならず、その場合の有効期限は最大でも 2014 年 8 月 31 日までとし、、2013 年 12 月 31 日以降は使用できないものとする。

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、鍵ペアにつきその使用期間が終了した後は、いかなる使用をも止めなければならない。

利用者に対して認証機関が発行した証明書は、次に定める要件を満たす場合に限り、3 年を越えて最長 5 年までの有効期間を有することができる。

- 組織向け証明書の利用環境での鍵ペアの保護については、データ・センタ内の高度な保護下で利用されること。個人向けの証明書については、利用者の鍵ペアがスマートカードのようなハードウェア・トークン上に存在すること,
- 利用者は本 CPS セクション 3.2.3 の規定に従い、最低 3 年ごとに再認証を受けること
- 万が一、利用者再認証手続きを完了することができず、または秘密鍵を保有していることの証明を行うことができない場合には、認証機関は当該利用者の証明書を取り消すものとされていること

また、米国シマンテックは「Symantec Class 3 International Server CA」、「Thawte SGC CA」ならびに「Class 3 Open Financial Exchange CA」も管理する。これらは第一次認証機関によって署名されているオンライン認証機関である。これらの認証機関の有効期間は、SGC および OFX の機能を提供する証明書の継続的な相互接続性を確保するため、Table 8 にある期間を超えて延長される。

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・サイニング証明書ならびにドメイン認証および組織認の SSL 証証明書は、STN の補足として本 CPS の Appendix B1、Appendix C および Appendix D それぞれのセクション 9.4 に定める手続きにより、CA/ブラウザフォーラムの定める要件に準拠する。

6.4 起動データ

6.4.1 起動データの生成とインストレーション

シマンテック認証機関の秘密鍵を含むトークンを保護するために用いられる起動データ(シークレット・シェア)は、本 CPS セクション 6.2.2 および"KeyCeremony Reference Guide"に定める要件に従って生成される。シークレット・シェアの生成および分配は記録される。

シマンテック登録機関は、自己の秘密鍵を保護するため、強度のパスワードを選択することを要求される。シマンテックのパスワード選択に関するガイドラインはパスワードに関し、次の要件を定めている。

- ユーザによって生成されること
- 少なくとも 8 文字以上であること
- 少なくとも 1 文字以上のアルファベットと1文字以上の数字を含むこと
- 少なくとも 1 以上の小文字を含むこと
- 同じ文字が多く含まれないこと
- オペレータの氏名等の属性と同一でないこと
- ユーザの属性から容易に推測される文字列を含むものでないこと

シマンテックは、マネージド PKI 管理者、登録機関および利用者に対し、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する。シマンテックは、2 つの要素による認証メカニズム(例えば、トークンとパスフレーズ、生体認証とトークン、または生体認証とパスフレーズ)を、秘密鍵の起動のために使用することも推奨する。

6.4.2 起動データの保護

シマンテックのシークレット・シェア保有者は、そのシークレット・シェアを保護することおよび保有者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る。

登録機関は、その管理者/登録機関の秘密鍵を、パスワード保護とブラウザの「セキュリティ高」オプションを用い、暗号化した形式で保管することが要求される。

シマンテックは、クライアント管理者、登録機関および利用者に対し、その秘密鍵を暗号化した形式で保管することおよびその秘密鍵をハードウェア・トークンまたは強度なパスフレーズのいずれかまたは双方を用いて保護することを強く推奨する。2つの方法による認証メカニズム(例えば、トークンとパスフレーズ、生体認証とトークン、または生体認証とパスフレーズ)が推奨される。

6.4.3 起動データに関する他の点

6.4.3.1 起動データの転送

秘密鍵の起動データを転送する場合、STN 参加者は、当該秘密鍵の紛失、盗難、改ざん、不正な開示、無権限の使用が行われないようにしなければならない。Windows やネットワークのログインのためのユーザネームとパスワードの組み合わせがエンドユーザ利用者の起動データとして用いられ

る場合、ネットワークを経由したパスワードの転送は、無許可のユーザのアクセスから保護されなければならない。

6.4.3.2 起動データの破壊

認証機関の秘密鍵の起動データは、当該起動データによって保護される秘密鍵の紛失、盗難、改ざん、不正な開示、無権限の使用を防止する方法を用いて、運用を中止する。セクション 5.5.2 に記載する期間を経過後、シマンテックは、起動データを上書きもしくは物理的破壊をもって、運用を中止する。

6.5 コンピュータ・セキュリティ管理

シマンテックは、全登録機関、認証機関の機能を“ Security and Audit Requirements Guide ”を満たす信頼されるシステムで実装する。エンタープライズ・カスタマは、信頼されるシステムを使用しなければならない。

6.5.1 特定のコンピュータ・セキュリティの技術的要件

シマンテックは、認証機関ソフトウェアおよびデータファイルを維持するシステムが信頼できるシステムであり、無権限者によるアクセスから安全なものであることを確保する。さらに、シマンテックは、実際に運用に供しているサーバへのアクセスを、業務上必要な個人のみに限定する。それ以外の者は、当該サーバへのアクセスをすることはできない。

シマンテックが実際に運用に供している証明書発行ネットワークは、論理的に他の部分から分離されており、必要なアプリケーション以外の通信は許可されない。シマンテックは、実際に運用に供しているネットワークを、内部および外部からの侵入ならびに許可されていない通信を制限するために、ファイアウォールを使用する。

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記号の組み合わせによるパスワードを使用する。このパスワードは定期的に変更される。

シマンテックのリポジトリをサポートするシマンテックのデータベースへの直接的アクセスは、シマンテックの運用グループに属する有効な業務上の理由を有する信頼される者に限定される。

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・サイニング証明書ならびにドメイン認証および組織認証の SSL 証明書は、STN の補足として本 CPS の Appendix B1、Appendix C および Appendix D それぞれのセクション 16.5 に定める手続きにより、CA/ブラウザフォーラムの定める要件に準拠する。

6.5.2 コンピュータ・セキュリティの評価

適用せず。

6.6 ライフサイクル技術管理

6.6.1 システム開発管理

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い、シマンテックにより開発され実施される。シマンテックは、そのマネージド PKI カスタマに対し、当該カスタマが登録機関および認証機関の機能を果たすために、ソフトウェアも提供する。当該ソフトウェアはシマンテックのシステム開発基準に従い開発される。

米国シマンテックが開発したソフトウェアは、最初にロードされる際、システム上の当該ソフトウェアが、米国シマンテックまたはシマンテックにより開発されたもので、インストレーションの前に変更されていないことおよび使用しようと意図しているバージョンであることを証明する方法を提供する。

6.6.2 セキュリティ管理

シマンテックは、その認証機関システムの状況を管理し、監視するための仕組みおよび方策を有している。シマンテックは、全ソフトウェア・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、ハッシュを生成する。当該ハッシュは、当該ソフトウェアの完全性を手動で証明するために用いられるものである。インストレーション時およびその後定期的に、シマンテックはその認証機関システムの完全性を確認する。

6.6.3 ライフサイクル・セキュリティ

適用せず。

6.7 ネットワーク・セキュリティ管理

シマンテックは、無権限者によるアクセスおよび他の不正な活動を防止するため、“Security and Audit Requirements Guide”に従い、セキュリティの施されたネットワークを用いて、その全ての認証機関および登録機関の機能を履行している。シマンテックは、暗号化およびデジタル署名を用いて、機密情報の通信を行なっている。

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のエントリは、日時情報を含む。当該時間情報は、暗号化を要件とされない。

7. 証明書、CRL および OCSP のプロファイル

7.1 証明書のプロファイル

シマンテックの証明書は、(a) 国際電気通信連合･電気通信標準化部門勧告X.509 (1997): 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, May 2008 ("RFC 5280") にほぼ準拠する。証明書の分類で適用されるように、STN 証明書は、最新バージョンのCA/ブラウザフォーラムのBaseline Requirementsに準拠する。[15]

少なくとも、シマンテックの X.509 証明書は基本フィールドを持ち、Table 9 に示す所定の値を含まなければならない。

フィールド	値/値の制限
Serial Number	Issuer DN（発行者識別名）毎の一意の値
Signature Algorithm	証明書に署名するために使用されるアルゴリズムを示すオブジェクト識別子（CP セクション 7.1.3 を参照のこと）
Issuer DN	発行者識別名。本 CPS セクション 7.1.4 を参照のこと。
Valid From	Universal Coordinate Time を基準とする。RFC 5280 に従いエンコードされる。
Valid To	Universal Coordinate Time を基準とする。RFC 5280 に従いエンコードされる。
Subject DN	Subject 識別名。CP セクション 7.1.4 を参照のこと。
Subject Public Key	RFC 5280 に従いエンコードされる。
Signature	RFC 5280 に従い生成されエンコードされる。

Table 9 – 基本的な証明書プロファイル･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 である。ただし、古いシステムをサポートする場合にのみ、特定のルート証明書は X.509 バージョン 1 であることが許される。認証機関証明書は、X.509 バージョン 1 もしくはバージョン 3 でなければならない。エンドユーザ利用者証明書は、X.509 バージョン 3 でなければならない。

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 からセクション 7.1.2.8 で要求される各エクステンションを設定する。プライベート･エクステンションの使用は許可されるが、プライベート･エクステンションの使用は、特別な参照を含めない限り、この本 CPS および CP の下では保証されない。

EV 証明書のエクステンションについての要求事項は、本 CPS の Appendix B3 に記載される。

7.1.2.1 Key Usage

X.509 バージョン3証明書は、一般に、RFC 5280(Internet X.509 Public Key Infrastructure

[15] 現行バージョンの CA/ブラウザフォーラム要件に一致しない STN 証明書は、2048 ビット未満の鍵サイズから成り、serverAuth フラグが除去されているか 2.16.840.1.113733.1.8.54.1 の OID を含むか、いずれかまたは両方の設定がなされている。

Certificate and CRL Profile, May 2008.)に従い設定される。
KeyUsage エクステンションの Criticality は、認証機関証明書は通常「TRUE」に設定され、個人向け証明書は通常「TRUE」もしくは「FALSE」に設定される。

注釈:
nonRepudiation ビットが KeyUsage エクステンションにセットされていない場合であっても、シマンテックは、これらの証明書について否認防止サービスをサポートする。PKI 一般において、nonRepudiation ビットの意味するところにおいてコンセンサスがとれておらず、nonRepudiation ビットがこれらの証明書中にセットされることは必須ではない。 そのようなコンセンサスが得られるまで、nonRepudiation ビットは潜在的な依拠当事者に対して意味のあるものにはならない。さらに、ほとんどの一般的アプリケーションは、nonRepudiation ビットを適切に扱っていない。それゆえ、 当該ビットをセットすることは、依拠当事者に対する信頼の決定の助けとならない可能性がある。そのため、nonRepudiation ビットの設定は、本 CPS では必ずしも要求されない。しかし、マネージド PKI キーマネージャーより発行されたデュアル鍵ペアの署名証明書の場合や、要求される場合には、当該ビットが設定されていてもよい。 デジタル証明書の使用に起因する非否認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であり、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する。

X.509 標準仕様に従って、nonRepudiation ビットはデジタル証明書では ContentCommitment として参照される場合がある。

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 に従い STN CP のオブジェクト識別子を含み、および CP セクション 7.1.8 に従いポリシー修飾子(policy qualifiers)が設定される。Criticality に関するフィールドは、「FALSE」に設定されなければならない。

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・サイニング証明書ならびにドメイン認証および組織認証の SSL 証明書は、STN の補足として本 CPS の Appendix B1、Appendix C および Appendix D それぞれのセクション 9.3 に定める手続きにより、CA/ブラウザフォーラムの定める要件に準拠する。

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 に従い設定される。ただし、一部の利用者証明書については、subjectAltName に電子メールアドレスが含まれないことがある。Criticality に関するフィールドは、「FALSE」に設定されなければならない。

7.1.2.4 Basic Constraints

シマンテックの X.509 バージョン 3 の認証機関証明書における basicConstraints エクステンションは、CA フィールドが「TRUE」に設定されなければならない。エンドユーザ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」に設定されなければならない。このエクステンションの Criticality は、認証機関証明書においては「TRUE」に、利用者証明書の場合は「TRUE」または「FALSE」のいずれかに設定される。

シマンテックの X.509 バージョン 3 認証機関証明書は、BasicConstraints エクステンション中に、その認証機関証明書の下に置かれる認証機関証明書の最大数を示す pathLenConstraint フィールドを持たなければならない。個人向け証明書を発行するオンライン・エンタープライズ・カスタマに対し発行される認証機関証明書については、pathLenConstraint フィールドは、個人向け証明書のみを発行するという意味の「0」に設定されなければならない。

7.1.2.5 Extended Key Usage

通常、Extended Key Usage エクステンションが設定される場合、Criticality に関するフィールドは、「FALSE」に設定される。一部を除き、STN に属する認証機関証明書には Extended Key Usage は含まれない。

7.1.2.6 CRL Distribution Points

ほとんどのシマンテックの X.509 バージョン 3 の個人向け証明書および中間認証機関証明書は、依拠当事者が CRL を入手し認証機関の証明書のステータス情報を確認できるように、cRLDistributionPoints エクステンション中に URL のロケーション情報を持つ。Criticality に関するフィールドは、「FALSE」に設定される。

7.1.2.7 Authority Key Identifier

通常、シマンテックは、X.509 バージョン 3 個人向け証明書と中間認証機関証明書の Authority Key Identifier エクステンションを設定する。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 は、当該証明書を発行する認証機関の公開鍵の 160-bit SHA-1 のハッシュの値が設定される。またあるときは、Authority Key Identifier エクステンションには、発行する認証機関の Subject 識別名の名称とシリアル・ナンバーが含まれる。Criticality に関するフィールドは、「FALSE」に設定される。

7.1.2.8 Subject Key Identifier

シマンテックが、Subject Key Identifier 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 Subject の公開鍵に基づく Subject Key Identifier が、RFC 5280 に記述された方法の一つに従い生成される。このエクステンションが使用される場合、Criticality に関するフィールドは、「FALSE」に設定される。

7.1.3 アルゴリズムオブジェクト識別子

シマンテックの証明書は、以下のアルゴリズムのうち一つを用いて署名される。

- 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}

- md5WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 4}

これらのアルゴリズムを用いて生成された証明書の署名は、RFC3279 に従わなければならない。
sha-1WithRSAEncryption は今後、md5WithRSAEncryption に代わって使用される。
md5WithRSAEncryption による署名は、レガシー・アプリケーションをサポートし事業継続性を保全する目的であると事前の承認を得た場合においてのみ使用される。

7.1.4 名前の形式

シマンテックは、本 CPS セクション 3.1.1 に従い、発行者(Issuer) および Subject 識別名を含む STN 証明書を発行する。各種証明書は、発行者識別名に、発行認証機関の Country、Organization Name、および Common Name を含んで生成される。

さらに、シマンテックは、利用者証明書中に、関連する依拠当事者に対し証明書の使用条件の URL を示す情報を含む追加の Organizational Unit フィールドを含めることができる。有効な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においては、本 Organizational Unit フィールドは、記述されなければならない。

7.1.5 名前制約

規定しない。

7.1.6 証明書ポリシー・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、証明書は、STN CP セクション 1.2 に定められた適切な証明書の Class に対応する CertificatePolicy のオブジェクト識別子を含む。STN CP の公表以前に発行された古い証明書で、CertificatePolicies エクステンションを含むものについては、証明書は STN の CPS を参照する。

7.1.6.1 証明書ポリシー・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・サイニング証明書ならびにドメイン認証および組織認証の SSL 証明書は、STN の補足として本 CPS の Appendix B1、Appendix C および Appendix D それぞれのセクション 9.3 に定める手続きにより、CA/ブラウザフォーラムの定める要件に準拠する。

7.1.7 ポリシー制約エクステンションの使用

規定しない。

7.1.8 ポリシー修飾子の構文および意味

通常、シマンテックは、Certificate Policies エクステンションにポリシー修飾子を含むX.509 Version3 STN証明書を作成する。一般的にそのような証明書は、適用される依拠当事者規約もしくはSTNのCPSを指し示すCPS pointer修飾子を含む。加えて、いくつかの証明書は、適用される依拠当事者規

約を指し示すUser Notice修飾子を含む。

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

規定しない。

7.2　CRL のプロファイル

CRL は基本フィールドを持ち、Table 10 に規定する内容を含む。

フィールド	値/値の制限
Version	本 CPS セクション 7.2.1 を参照のこと。
Signature Algorithm	CRL に署名するために使用されるアルゴリズム。RFC3279 (CP セクション 7.1.3)に従う。
Issuer	CRL を署名し発行したエンティティ。
Effective Date	CRL の発行日。CRL は発行と同時に有効となる。
Next Update	その日までに、次の CRL が発行される。CRL の発行頻度は、本 CPS セクション 4.9.7 の要求に従う。
Revoked Certificates	失効した証明書のシリアル・ナンバーおよび失効日を含む、失効した証明書のリスト。

Table 10 – 基本的な CRL プロファイル項目

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 をサポートする。バージョン 2 の CRL は RFC 5280 の要求に従う。

7.2.2 CRL および証明書失効リストエントリ・エクステンション

規定しない。

7.3 OCSP プロファイル

OCSP（Online Certificate Status Protocol）は、ある特定の証明書に対する失効情報を速やかに得るための一つの方法である。シマンテックは、OCSP を以下の証明書に対して使用する。

- RFC2560 に準拠する、Class 2 におけるエンタープライズ向け証明書
- RFC5019 に準拠する、TGV (Symantec Trusted Global Validation)サービスにおいて使用される Class 2 エンタープライズ向け証明書、および 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・サイニング証明書ならびにドメイン認証および組織認証の SSL 証明書について、シマンテックは、STN の補足として本 CPS の Appendix B1 および Appendix C それぞれのセクション 13 ならびに Appendix D セクション 13.2.5 にそれぞれ定める手続きにより、CA/ブラウザフォーラムの定める要件に準拠して OCSP レスポンスを提供する。

7.3.1 バージョン番号

RFC2560 もしくは RFC5019 に規定される OCSP のバージョン 1 の仕様がサポートされる。

7.3.2 OCSP エクステンション

TGV サービスでは、OCSP レスポンスの最新性を確立するためにタイム・スタンプと有効期限を参照する。シマンテックでは OCSP レスポンスの最新性の確立のために Nonce エクステンションを使用しない。また、クライアントは OCSP レスポンスに含まれる Nonce エクステンションの値がこれに該当する OCSP リクエストの値と一致することを要求できない。OCSP レスポンスの最新性の確認のためにはローカル時刻を参照することとする。

8. 準拠性監査とその他の評価

セクション 1.3.1 に記述された STN のルート認証機関、Class 3 組織向け認証機関、Class 2 組織向けおよび個人向け認証機関、Class 1 個人向け認証機関を含む、シマンテックのパブリックおよびマネージド PKI 認証機関サービスをサポートするシマンテックのデータ・センタの運用およびキーマネージメントの運用に関しては、年次の ISAE3402 監査および SSAE16 監査が行われる。カスタマ固有の認証機関は、カスタマが要求しない限り、シマンテックの運用に関する監査の一環としては、特段の監査は行われない。シマンテックは、エンタープライズ・カスタマに対し、本 CPS に従った準拠性監査およびこれらのカスタマの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。

準拠性監査に加えて、シマンテックは、STN 内のシマンテック・サブドメインの信頼性を確保するため、次に例示する審査および調査を行うことができるがこれに限定されない。

- シマンテックは、自らの判断により、被監査組織が STN スタンダードを充足しない場合、事故または危殆化に遭遇したか、または STN のセキュリティもしくは完全性を現実にまたは潜在的に脅かすような作為または不作為があると信ずべき理由がある場合には、カスタマについていつでも「緊急監査または調査」を行う権利がある。
- シマンテックは、準拠性監査または通常のビジネスにおける全体的リスク・マネージメント・プロセスにおいて、不完全または例外的な事由が発見された場合には、カスタマについて、「追加的リスク・マネジメント・レビュー」を行う権利がある。

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ことができる。監査、審査または調査の対象である組織は、シマンテックおよび監査、審査または調査を行う要員に、合理的な協力を行うものとする。

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・サイニング証明書ならびにドメイン認証および組織認証の SSL 証明書について、シマンテックは、STN の補足として本 CPS の Appendix B1 および Appendix C それぞれのセクション 17.5 ならびに Appendix D セクション 17.8 にそれぞれ定める手続きにより、CA/ブラウザフォーラムの定める要件に準拠して内部監査を実施する。

8.1 評価の頻度・状況

準拠性監査は、被監査組織の費用負担により、少なくとも年 1 回実施される。一回の監査期間は 1 年未満とし、監査の空白期間が無いよう実施される。

8.2 評価人の身元と資格

シマンテック認証機関の準拠性監査は、次のような公的な監査法人により遂行される。

- 公開鍵インフラストラクチャ技術、情報セキュリティツールおよび技術、セキュリティ監査ならびに第三者証明の職務に深い知識を有すること。ならびに、
- 米国公認会計士協会（AICPA）または同様の組織から認定された者で、特定の技術の保有に加え、専門家同士の審査、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といった品質を保障する手段、ならびに継続的な職業教育の要件を備えていること。

8.3 評価人と被評価者との関係

シマンテックの運用についての準拠性監査は、シマンテックとは独立の監査法人によって遂行される。

8.4 評価対象項目

シマンテックが行う認証機関（またはこれと同等のもの）監査のための年次の ISAE3402 監査および SSAE16 監査の範囲は、認証機関の環境統制、キーマネージメントの運用、インフラストラクチャおよび管理認証機関の統制、証明書ライフサイクルマネージメントならびに認証機関の業務に関する情報開示を含むものである。

8.5 欠陥の結果としてとられる処置

シマンテックの運用に関する準拠性監査に関し、重大な例外または欠陥が当該準拠性監査において指摘された場合、とるべき措置が決定される。当該決定は、監査人からの指摘を受けて、シマンテックの経営陣によりなされる。シマンテックの経営陣は、是正措置の策定および実施につき責任を負う。もし、シマンテックが、当該例外または欠陥が STN のセキュリティもしくは完全性に対する直接的な脅威を示すものであると決定した場合には、是正措置は 30 日以内に策定され、商業的に合理的な期間内に実施される。これよりも深刻度の低い例外または欠陥については、シマンテックの経営陣は、当該事由の重要性について評価し、適切な措置を決定する。

8.6 結果の伝達

シマンテックの運用に関する準拠性監査の結果は、シマンテックの経営陣の任意の判断により公開することができる。

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 証明書発行または更新の手数料

シマンテックおよびカスタマは、利用者に対し、証明書の発行、管理および更新に関し、手数料を請求することができる。

9.1.2 証明書のアクセス手数料

シマンテックおよびカスタマは、証明書をリポジトリに置くかまたは他の方法により、依拠当事者がこれを利用することができるようにする対価としての手数料を請求しない。

9.1.3 失効またはステータス情報のアクセス手数料

シマンテックは、CP の定めにより CRL をリポジトリで利用できるようにすること、または他の方法により、依拠当事者がこれを利用することができるようにする対価としての手数料を請求しない。ただし、シマンテックは、特別にカスタマイズされた CRL、OCSP サービス、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に関しては手数料を請求することができる。シマンテックの書面による事前の明示的な同意がない限り、証明書ステータス情報を活用する製品または役務を提供する第三者は、失効情報、証明書ステータス情報またはリポジトリ内のタイム・スタンプに対するアクセスをすることが許されない。

9.1.4 他のサービスの手数料

シマンテックは、本 CPS に対するアクセスに関し手数料を請求しない。文書の単純な閲覧以外の目的、例えば複製、再配布、変更または派生的文書の作成等を目的とする利用については、当該文書の著作権を有する者とのライセンスに関する合意を得ることを条件とする。

9.1.5 返金制度

シマンテック・サブドメインにおいて、次の返金制度が適用される。
https://www.verisign.co.jp/repository/refund/index.html

シマンテックは、証明書業務の運用および証明書の発行において、厳格な実務と方針を厳守し、これに従う。しかしながら、理由の如何を問わず、利用者が自己に発行された証明書について十分に満足しない場合、利用者はシマンテックに対して、発行から 30 日以内に証明書を破棄し、利用者に返金をするよう要請することができる。利用者または利用者の証明書に関して、本 CPS 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、その最初の 30 日の期間後も、利用者は、シマンテックに対し、証明書を破棄し、返金をするよう要請することができる。シマンテックは、利用者の証明書を破棄した後、速やかに、証明書に支払われた申請料の全額を、証明書の料金がクレジット・カードで支払われた場合には利用者のクレジット・カードへの返金により、その他の方法による場合には、利用者の指定する銀行口座への振込みにて利用者に返金する。利用者が返金を要請する場合は、シマンテックカスタマサポート 03-5114-4137 に連絡することができる。この返金制度は、利用者にとっての唯一の救済方法ではなく、また利用者がよることのできる他の救済方法を制限するものではない。

9.2 財務的責任

9.2.1 保険

エンタープライズ・カスタマは、過失および怠慢によるリスクを担保するため、商業的に合理的な水準の"errors and omissions"賠償責任保険に加入することが推奨される。当該保険は、保険会社と締結するか、自家保険とするかを問わない。シマンテックはこのような"errors and omissions"賠償責任保険を付保する準備がある。

9.2.2 その他の資産

エンタープライズ・カスタマは、自己の業務の遂行と義務の履行をするに足る十分な財政的基盤を有し、利用者および依拠当事者に対する責任を合理的な範囲で負担することができなければならない。シマンテックの財務状況は、https://www.verisign.co.jp/corporate/investor/で公開されている。

9.2.3 拡張された保証

NetSure プロテクション・プランは、シマンテックの不注意や契約上の責任による証明書発行時やその他の不正行為によって発生した欠陥による紛失/損害から保護するためにシマンテックが提供する SSL サーバ証明書およびコード・サイニング証明書利用者への拡張された保証である。証明書利用者は、適用されるサービス規約に準じることで適用される。
NetSure プロテクション・プランに関する一般的な情報およびどの証明書がこの対象になるかは、https://www.verisign.co.jp/repository/refund/index.html にて参照できる。

9.3 業務情報の機密保持

9.3.1 機密情報の範囲

利用者の次の記録については、本 CPS セクション 9.3.2 の定めるところに従い、機密に保持されなければならない（以下「秘密情報」という）。

- 認証機関申請記録（承認、不承認を問わない）
- 証明書申請記録
- キーマネージメントサービスを用いて、エンタープライズ・カスタマが保有する秘密鍵および当該秘密鍵を回復させるために必要な情報
- 処理記録（全部の記録および監査証跡記録の双方を含む）
- 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記録
- シマンテックもしくはカスタマまたはそれぞれの担当監査人（内部監査人であるか外部監査人であるかを問わない）によって作成された監査報告
- 偶発事故に対する計画および災害復旧計画
- シマンテックのハードウェアおよびソフトウェアの運用ならびに証明書サービスおよび申請サービスの管理を制御するセキュリティの手段

9.3.2 機密とみなされない情報

シマンテック・サブドメインの参加者は、証明書、証明書失効および他のステータス情報、シマンテックのリポジトリならびにそれらに含まれている情報が秘密情報であるとみなされないことを承諾する。本 CPS セクション 9.3.1 により明示的に機密とみなされる情報以外の情報については、機密とみなされない。本条は、適用される個人情報保護法規に従う。

9.3.3 機密情報保護責任

シマンテックは、重要な秘密情報が損なわれ、第三者に漏洩しないよう安全な措置を講じる。

9.4 個人情報の保護

9.4.1 プライバシーポリシー

シマンテックは、CP セクション 9.4.1 に従い、プライバシーポリシーを作成し、
https://www.symantec.com/ja/jp/about/profile/policies/privacy.jsp で、公開している。

9.4.2 個人情報

利用者に関する情報で、証明書、証明書ディレクトリおよびオンラインの CRL を通じて入手できない情報は、個人情報として取り扱う。

9.4.3 個人情報とみなされない情報

法律に従うことを条件に、証明書で公開される情報は、秘密情報とみなされない。

9.4.4 個人情報の保護責任

個人情報を受領した STN 参加者は、当該情報が損なわれ、第三者に漏洩しないよう安全な措置を講じると共に、適用される個人情報保護に関する法律に従うものとする。

9.4.5 個人情報を利用するための通知および同意

本 CPS またはプライバシーポリシーに別途定めのない限り、もしくは別段の合意のない限り、個人情報は当該情報者の同意がない限り、利用することはできないものとする。本セクションは、適用される個人情報保護に関する法律に従うものとする。

9.4.6 司法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実に判断する場合、秘密情報および非公開情報を開示することができる。

- 司法、行政、その他の法的な手続きにより情報開示が必要な場合

9.4.7 他の情報開示に関する状況

規定しない。

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・サブドメインの参加者間での知的財産権の帰属は、シマンテック・サブドメインの参加者間での契約により定められる。本 CPS セクション 9.5 以下の各項は、利用者と依拠当事者に関する知的財産権について適用される。

9.5.1　証明書および失効情報に関する財産権

認証機関は、自己が発行した証明書および証明書失効情報に関する全ての知的財産権を留保する。シマンテックおよびカスタマは、証明書を複製し、配布することを、非独占かつ無償で認めるが、当該複製はそれら全ての情報を完全な形で複製するものでなければならず、かつ、当該証明書の使用は当該証明書において引用される依拠当事者規約に従うものでなければならない。シマンテックおよびカスタマは、依拠当事者規約および他の適用される契約の定めるところに従い、依拠当事者機能を果たすため証明書失効情報を使用することを認める。

9.5.2　本 CPS に関する知的財産権

STN 参加者は、シマンテックが本 CPS に関する全ての知的財産権を有することを確認する。

9.5.3　名称に含まれる権利

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、商号ならびに証明書申請者に発行される証明書中の識別名に関する全ての権利を留保する。

9.5.4　鍵および鍵のデータに関する財産権

認証機関および利用者の証明書に対応する鍵ペアは、それらが保管および保護されている物理的媒体の如何にかかわらず、キーマネージメントサービスを使用するエンタープライズ・カスタマの権利を条件として、当該証明書における Subject となっている認証機関および利用者が保有するものであり、当該鍵ペアに係る全ての知的財産権は当該認証機関および利用者に帰属する。前記の一般性を制限することなく、全ての第一次認証機関公開鍵および自己署名証明書を含む米国シマンテックのルート公開鍵ならびにそれを含むルート証明書については、米国シマンテックに帰属する。米国シマンテックは、ソフトウェアおよびハードウェア製造者に対し、信頼できるハードウェア・デバイスおよびソフトウェア上に当該ルート証明書のコピーを置くために、当該ルート証明書を複製する権利を与えている。最後に、認証機関の秘密鍵のシークレット・シェアは、当該認証機関が保有するものであり、その認証機関は、シマンテックから当該シークレット・シェアを物理的に取得することができないにもかかわらず、これらに関する全ての知的財産権を保有する。

9.6　表明と保証

9.6.1　認証機関の表明と保証

シマンテックは、以下の事項を保証する。

- 証明書に記載される事実には、証明書申請を承認、または、証明書を発行するエンティティが知り、またはこれらに起因する重要な不実の記載は存在しないこと
- 証明書中の情報には、証明書申請を承認、または、証明書を発行するエンティティが、証明書申請の取扱または証明書の生成過程において合理的注意を用いることを怠ったことによ

り生じた誤りが存在しないこと
- 証明書が本 CPS に定める全ての重要な要件に合致していること
- 失効サービスおよびリポジトリの使用が全ての重要な点において本 CPS に、合致していること

利用規約には、追加の表明と保証を定めることができる。

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・サイニング証明書ならびにドメイン認証および組織認証の SSL 証明書は、STN の補足として本 CPS の Appendix B1 および Appendix C それぞれのセクション 7.1 およびセクション 18、ならびに Appendix D セクション 7.1 (「CA によるもの」)およびセクション 18.3(「ルート CA の義務」)に定める手続きにより、CA/ブラウザフォーラムの定める要件に準拠する。

9.6.2 登録機関の表明と保証

登録機関は、以下の事項を保証する。
- 証明書に記載される事実には、証明書申請を承認、または、証明書を発行するエンティティが知り、またはこれらに起因する重要な不実の記載は存在しないこと
- 証明書中の情報には、証明書申請を承認するエンティティが、証明書申請の取扱において合理的注意を用いることを怠ったことにより生じた誤りが存在しないこと
- 証明書が本 CPS に定める全ての重要な要件に合致していること
- 失効サービス(該当ある場合)およびリポジトリの使用が本 CPS に定めるところに、重要な点において全て合致していること

利用規約には、追加の表明と保証を定めることができる。

9.6.3 利用者の表明と保証

利用者は以下の事項を保証する。
- 証明書に記載される公開鍵に対応する秘密鍵を用いて生成するそれぞれのデジタル署名が、利用者のデジタル署名であり、デジタル署名を生成する時点において、証明書が受領され、有効なものであること(有効期間が満了しておらず、失効されてもいないこと)
- 利用者の秘密鍵については、十分な保護がされており、かつ、権限を付与された者以外の何人もアクセスしたことがないこと
- 利用者が証明書申請時行った表明が真実であること
- 利用者によって提供され、証明書に記載されている全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、かつ、本 CPS を順守した態様によってのみ、使用されていること
- 利用者は、エンドユーザの利用者であって認証機関でなく、また、証明書に記載された公開鍵に対応する秘密鍵を、認証機関であるかどうかを問わず、証明書(あるいは公開鍵を証明するその他の形式)または CRL に、デジタル署名をする目的で使用していないこと

利用規約には、追加の表明と保証を定めることができる。

9.6.4 依拠当事者の表明と保証

依拠当事者規約は、依拠当事者が証明書中の情報につき依拠すべき範囲を決定するために必要十分な情報を受領していること、および当該証明書中の情報について依拠するか否かを決定するこ

とに関しては依拠当事者のみが責任を負うこと、ならびに本 CPS に定め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ことを認識し確認することを要求する。

依拠当事者規約には、追加の表明と保証を定めることができる。

9.6.5 その他の参加者の表明と保証

規定しない。

9.7 保証の否認

適用される法律上許される範囲内において、シマンテックの利用規約および依拠当事者規約、ならびにその他の利用規約は、商品性および特定目的への適合性を含むシマンテックのその他一切の保証を否認する。

9.8 責任の制限

シマンテックが CP および本 CPS を順守して証明書を発行し管理する範囲内において、シマンテックは利用者、当事者、もしくは他の第三者機関が証明書を利用または依拠することで生じる損害や損失に関しては何らの責任も負わない。適用される法律上許される範囲内において、利用規約および依拠当事者規約は、シマンテックの責任を制限しなければならない。シマンテックは、間接損害、特別損害、付随的損害および結果的損害に関しては何らの責任も負わない。また、利用規約および依拠当事者規約は、シマンテックがある特定の証明書に関して負うべき損害賠償額の上限が次のとおりであることを含まなければならない。

Class	損害賠償額の上限
Class 1	100 米ドル相当円
Class 2	5,000 米ドル相当円
Class 3	100,000 米ドル相当円

Table 11 – 損害賠償額の上限

[注] Table 11 に定める損害賠償額の上限は、シマンテックの NetSure プロテクション・プランにより賠償を受けられるもの以外の損害賠償金の上限である。シマンテックの NetSure プロテクション・プランに定める支払金額は、当該プランの定めるところによる。シマンテックの NetSure プロテクション・プランに基づく各種類の証明書に関する損害賠償額の上限は、金 50,000 米ドル相当円から金 250,000 米ドル相当円の範囲である。より詳細なことは次のサイトにて閲覧可能である。
https://www.verisign.co.jp/repository/refund/index.html

利用者の責任の上限は、適用される利用規約の中に記載される。

エンタープライズ登録機関、適用される認証機関の責任の上限は、彼らの中で結ばれる契約中に記載される。

依拠当事者の責任の上限は、適用される依拠当事者規約の中に記載される。

EV 証明書に対するシマンテックの責任の制限は、本 CPS Appendix D のセクション 18 に記述される。

9.9 補償

9.9.1 利用者による補償

適用される法律上許される範囲内において、利用者は以下の事項から発生する損害を、シマンテックに補償するものとする。

- 利用者の証明書申請につ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関する重要な事実を開示することを怠った場合で、不実の表明または事実を開示しないことが懈怠または関係者を欺く意図をもってなされたとき
- 利用者が利用者の秘密鍵の保護、信頼すべきシステムの使用、またはその他利用者の秘密鍵の危殆化、喪失、開示、変更もしくは権限のない使用を防ぐために必要な措置をと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（CommonName、ドメイン・ネームまたは電子メールアドレスを含むがこれに限られない）を使用した場合

利用規約には、追加の補償義務を定めることができる。

9.9.2 依拠当事者による補償

適用される法律上許される範囲内において、依拠当事者規約は、依拠当事者が以下の事項から発生する損害をシマンテックに補償することを規定しなければならない。

- 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下において合理的でない場合
- 依拠当事者が、依拠しようとする証明書につき、有効期間が満了し、または失効されているか否かを決定するために証明書のステータスを確認するのを怠った場合

依拠当事者規約には、追加の補償義務を定めることができる。

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責任の限定にもかかわらず、ルート 認証機関との間でルート証明書配付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、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、認証機関の義務または潜在的な責任を負わないことを認証機関は理解し、同意するものとする。

したがって、認証機関が行政機関である場合を除き、認証機関は、認証機関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すべての申し立て、損害、および損失について、訴因または関連法理論にかかわらず、各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、免責するものとする。

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が、以下のような不正な証明書を有効、または信頼可能と表示したことによって直接引き起こされた場合には、認証機関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、上記は適用されない。
(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、現在認証機関が失効ステータスを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に限る）。

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掲載されたときに有効となる。本 CPS の変更も、シマンテックのリポジトリに掲載されたときに有効となる。

9.10.2 終了

本 CPS は、新たな CPS が効力を発するまで、有効とする。

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、発行した証明書の残存有効期間中は、本 CPS の条項に拘束されるものとする。

9.11 参加者の個別の通知と連絡

関係者間で別途合意のない限り、シマンテック・サブドメインの参加者は、連絡事項の重要性と内容を考慮し、相互に連絡を取り合うために商業上合理的な方法をとるものとする。

9.12 改訂

9.12.1 改訂手続き

本 CPS の変更は、シマンテックによりなされる。変更は、本 CPS の改定部分を含む文書の形式によるか、改定部分を示した形式によるかのいずれかの方法でなされなければならない。上記の何れの形式によるかを問わず、改訂の内容は、シマンテックのリポジトリの「プラクティス・アップデートおよび通知」（https://www.symantec.com/about/profile/policies/repository.jsp）からリンクされなければならない。改定部分として記載されている事項は、参照されたバージョンの本 CPS の全ての指定されたまたは矛盾する条項に優先する。シマンテックは、本 CPS の変更が、各 Class の証明書に対応する証明書ポリシーの証明書ポリシー識別子の変更を要するかどうかを決定するものとする。

9.12.2 通知方法と期間

シマンテックは、誤植の訂正、URL の変更、連絡先の変更といった重要でない変更については、変更に関する通知を行わずに、本 CPS を変更する権利を留保する。変更事項が重要であるか否かについての判断は、シマンテックの単独の判断による。

本 CPS の変更内容は、シマンテックのリポジトリの「プラクティス・アップデートおよび通知」（https://www.symantec.com/about/profile/policies/repository.jsp）に置かれるものとする。

本 CPS の定めにかかわらず、シマンテックが STN の全体またはその一部のセキュリティの違反を停止させ、またはこれを防止するために本 CPS の重要な変更を直ちに行うことが必要であると信ずる場合には、シマンテックはシマンテックのリポジトリに公表することにより当該変更を行うことができる。この場合、当該変更は公表をもって直ちに効力を生ずるものとする。シマンテックは、公表後相当な期間内に、当該変更の内容をシマンテック・サブドメイン参加者に通知するものとする。

9.12.2.1 コメント期間

他に定められた場合を除き、本 CPS の重要な変更についてコメントを求める期間は、当該変更がシマンテックのリポジトリに掲載されてから 15 日間にわたり設定されなければならない。シマンテック・サブドメイン参加者は、シマンテックに対し、当該期間の終了までの間、コメントを提出することができる。

9.12.2.2 コメントの取扱

シマンテックは、提案した変更内容についてのコメントを検討しなくてはならない。シマンテックは(a)変更内容を修正なしに発効させるか、(b)提案した変更内容を修正し、必要な場合、新たな変更内容として公表するか、または(c)変更内容を撤回するか、いずれかの方策をとらなければならない。シマンテックは、提案した変更を、シマンテックのリポジトリの「プラクティス・アップデートおよび通知」で通知することにより、撤回することができる。提案した変更が修正または撤回されない限り、当該変更はコメントを求める期間の満了をもって発効する。

9.12.3 OID の変更が必要な場合

シマンテックが証明書ポリシーに対応するオブジェクト識別子の変更が必要だと判断した場合、変更内容には、証明書の各 Class 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なければならない。そうでない場合、証明書ポリシーのオブジェクト識別子の変更を要求してはならない。

9.13 紛争の解決

9.13.1 サブドメインの参加者間の紛争

シマンテック・サブドメインの参加者間の紛争は、関係当事者間に適用される契約に従い解決するものとする。

9.13.2 利用者または依拠当事者との紛争

適用される法律上許される範囲内において、シマンテックの利用規約および依拠当事者規約は、紛争解決条項を有するものでなければならない。当該条項において、東京地方裁判所を、第一審の専属管轄裁判所とする旨を定めるものとする。

9.14 準拠法

適用される法律上の制限に従い、本 CPS の執行力、解釈および有効性については、契約その他法の選択についての規定にかかわらず、また日本における商業的な関連を立証することなく、日本法に準拠し、日本法に従って解釈される。当該準拠法に関する規定は、シマンテック・サブドメインの参加者全てについて、当該参加者の所在地にかかわらず、統一的手続および解釈を確保するために行われるものである。

上記の準拠法規定は、本 CPS に限って適用されるものである。本 CPS を参照することで、本 CPS をその一部として締結される契約は、これと異なる準拠法に関する定めを行うことができるものとす

る。ただし、本セクション 9.14 の規定は、当該契約のその他の条項とは別に、適用される法律の制限に従い、本 CPS の執行力、解釈および有効性を支配する。

9.15 法の順守

本 CPS は、ソフトウェア、ハードウェア、技術情報の輸出入に関する制限を含む国内外の法律、法令、規則、命令に従う。シマンテックは、認証機関に対し、業務を行う各管轄地において認証機関としての認可を与える(証明書の発行に対して、該当管轄地の法令によって認可が必要な場合)。

9.16 雑則

9.16.1 完全合意条項

適用せず。

9.16.2 譲渡

適用せず。

9.16.3 分離可能

本 CPS の一部の条項が裁判所によって執行不能であると判断された場合、これ以外の条項は有効に存続する。

9.16.4 強制執行(弁護士費用と権利放棄)

適用せず。

9.16.5 不可抗力

適用される法律上許される範囲内において、シマンテックの利用規約および依拠当事者規約、ならびにその他の利用規約はシマンテックを保護する不可抗力条項を含むものである。

9.17 その他の条項

適用せず。

Appendix A. 略語・定義表

略語

Term	Definition
AICPA	American Institute of Certified Public Accountants.
ANSI	The American National Standards Institute.
ACS	Authenticated Content Signing.
BIS	The United States Bureau of Industry and Science of the United States Department of Commerce.
CA	Certification Authority.
ccTLD	Country Code Top-Level Domain
CP	Certificate Policy.
CPS	Certification Practice Statement.
CRL	Certificate Revocation List.
DBA	Doing Business As
DNS	Domain Name System
EV	Extended Validation
FIPS	United State Federal Information Processing Standards.
FQDN	Fully Qualified Domain Name
ICC	International Chamber of Commerce.
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ISO	International Organization for Standardization
KRB	Key Recovery Block.
LSVA	Logical security vulnerability assessment.
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol.
OID	Object Identifier
PCA	Primary Certification Authority.
PIN	Personal identification number.
PKCS	Public-Key Cryptography Standard.
PKI	Public Key Infrastructure.
QGIS	QGIS Qualified Government Information Source
QIIS	QIIS Qualified Independent Information Source
RA	Registration Authority.
RFC	Request for comment.
SAS	Statement on Auditing Standards (promulgated by the American Institute of Certified Public Accountants).
S/MIME	Secure multipurpose Internet mail extensions.
SSL	Secure Sockets Layer.
STN	Symantec Trust Network.
TLD	Top-Level Domain
TLS	Transport Layer Security.

定義

Term	Definition
Administrator 管理者	プロセッシング・センタ、サービス・センタ、マネージド PKI カスタマの組織内で、検証その他認証機関または登録機関の役割を果たす信頼される者。
Administrator Certificate 管理者証明書	管理者に発行される証明書で、認証機関または登録機関としての機能を果たすためにのみ利用される。
Affiliate アフィリエート	技術、通信または金融サービス等の事業における、一流の信頼される第三者で、ある特定の地域において STN サービスを提供するために米国シマンテックと契約を締結している者。
Affiliate Practices Legal Requirements Guidebook	アフィリエートの CPS、契約、認証手続き、プライバシー・ポリシーの要件ついて、アフィリエート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米国シマンテックの文書。
Affiliated Individual 関連する個人	マネージド PKI カスタマ、マネージド PKI ライトカスタマ、ゲートウェイカスタマのエンティティとして関連する自然人。(ⅰ)役員、取締役、従業員、パートナー、請負人、インターンまたは当該エンティティ内部の人物、(ⅱ)シマンテックとの利害関係のあるコミュニティ、(ⅲ) 当該エンティティと契約関係があり、取引関係に基づき当該エンティティがその身元に関し強固な保証をすることができる個人。
Applicant 申請者	証明書の申請(または更新要求)をする個人または法的組織体。証明書が発行されると、申請者は加入者と呼ばれるようになる。デバイスに対して発行される証明書については、デバイスが実際の証明書要求を送信する場合であっても、申請者は証明書で指定されているデバイスを管理または運用する組織体である。
Applicant Representative 申請権限者	申請者である、申請者によって雇用されている、または申請者を代表するための明示的な権限を持ち、(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)申請者を代表して加入者契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利用規約を認め、同意する認定機関である個人または保証人。
Application Software Supplier アプリケーションソフトウェアサプライヤ	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であるアプリケーションソフトウェアのサプライヤ。
Automated Administration 自動承認	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。
Automated Administration Software Module 自動承認モジュール	自動承認を行うシマンテックが提供するソフトウェア。
Certificate 証明書	少なくとも、認証機関の名称を記載しまたは認証機関を識別し、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・ナンバーを含み、これに認証機関がデジタル署名したメッセージ。
Certificate Applicant 証明書申請者	認証機関に対して証明書の発行を要求する個人または組織。
Certificate Application 証明書申請	証明書申請者(または証明書申請者から授権された代理人)から認証機関に対して証明書の発行を求める要求。
Certificate Approver 証明書承認者	権限のある証明書承認者が、EV 証明書要求を承認しなければならない。証明書承認者は、(i)証明書要求者として行動するとともに他の従業員または第三者に証明書要求者として行動する権限を付与し、(ii)他の証明書要求者が提出した証明書要求を承認する、申請者に雇われた自然人または申請者の代理を務める明示的な権限を有する代理人である。
Certificate Chain 証明書チェーン	利用者および認証機関の証明書を含む、一連の証明書リストのことで、ルート証明書で終了する。
Certificate Data	CA の所有または管理下にある、または CA がアクセスすることができる、証明書要求

Term	Definition
証明書データ	およびそれに関連するデータ(申請者から取得したかどうかを問わない)。
Certificate Management Control Objectives **証明書管理の統制対象**	エンティティが準拠性監査を満たすための基準
Certificate Policies (CP) **サーティフィケート・ポリシー**	STN・サーティフィケート・ポリシーと呼ばれるもので、STN を支配する主要な方針を記載している文書。
Certificate Problem Report **証明書問題レポート**	鍵の危殆化の疑い、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申し立て。
Certificate Requester **証明書要求者**	証明書要求者は、申請者に雇われた自然人、申請者の代理を務める明示的な権限を有する代理人、または申請者の代理で EV 証明書要求を作成、提出する第三者(ISP、ホスティング会社など)である。
Certificate Revocation List (CRL) CRL	CP セクション 3.4 に基づき有効期間満了前に効力を失効された証明書を特定する目的で、認証機関によってデジタル署名された定期的または緊急に発行されるリスト。このリストは、一般的に CRL 発行者の名前、発効日、次回 CRL 発行予定日、効力を失効された証明書のシリアル・ナンバーならびにその具体的時期および理由を示す。
Certificate Signing Request **証明書署名要求**	証明書を発行させるための要求を伝達するメッセージ。
Certification Authority (CA) **認証機関**	STN 内で証明書の発行、管理、失効および更新を授権されたエンティティ。
Certification Practice Statement (CPS) **サーティフィケーション・プラクティス・ステートメント**	米国シマンテックまたはアフィリエートが証明書申請の承認または拒絶、証明書を発行、管理および失効をする際に採用する運用手続を規定した文書で、STN 内で証明書を発行するマネージド PKI カスタマ、ゲートウェイカスタマはこれを採用することを要求される。
Challenge Phrase **チャレンジフレーズ**	証明書申請の際に、証明書申請者が選ぶ秘密のフレーズ。証明書申請者が証明書を発行すると、証明書申請者は利用者になり、認証機関または登録機関は利用者がその証明書を失効または更新を求めるとき、利用者を認証するためにチャレンジフレーズを利用する。
Class	各 class の保障は CP セクション 1.4.1 に記述されている。
Client Service Center **クライアントサービスセンタ**	コンシューマー、エンタープライズ・カスタマに対してクライアント証明書を提供しているシマンテックの提供するサービス・センタ
Compliance Audit **準拠性監査**	プロセッシング・センタ、サービス・センタまたはマネージド PKI カスタマ、ゲートウェイカスタマがそれぞれに適用される STN スタンダードと一致しているかどうかを決定するために受ける定期的な監査。
Compromise **危殆化**	セキュリティ・ポリシーの違反またはその疑いのある行為で、機密情報の無権限の開示または管理の喪失が生じかねないこと。秘密鍵に関する危殆化は、紛失、盗難、開示、改変、無断使用または当該秘密鍵のセキュリティのその他の危殆化を意味する。
Confidential/Private Information **秘密情報**	CP セクション 9.3.1 に従い秘密にすることを要求される情報。
Contract Signer **契約書署名者**	契約書署名者は、申請者の代理を務める明示的な権限を持ち、かつ申請者の代理で利用規約に署名する権限を有する、申請者、申請者に雇われた自然人または代理人である。
Country	国とは本ガイドランでは、独立国であると定義する。

Term	Definition
国	
Customer **カスタマ**	マネージド PKI カスタマ、ゲートウェイカスタマである組織
Delegated Third Party **権限委譲先の第三者機関**	CA ではないが、本ドキュメントに定められた 1 つ以上の CA 要件を実施または履行し、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個人または法人。
Demand Deposit Account **要求払預金口座**	要求に基づき支払いが可能な銀行もしくは他の金融機関の預金口座。小切手、銀行手形、口座引き落とし、電子的な資産移動などを円滑に行うことを目的とする。用途は国より異なるが、"checking account"," a share draft account", "a current account"などとして知られる。
Domain Authorization	特定のドメイン名前空間に関する証明書を要求する申請者を証明するために、ドメイン名登録者によって提供される書状もしくはドキュメント。
Domain Name **ドメイン名**	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。
Domain Namespace **ドメイン名前空間**	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。
Domain Name Registrant **ドメイン名登録者**	ドメイン名の「所有者」を表すこともあるが、正確には、ドメイン名が使用される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で登録されている個人または組織体のこと。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個人または法人など。
Domain Name Registrar **ドメイン名登録機関**	(i) Internet Corporation for Assigned Names and Numbers (ICANN)、(ii)全国的なドメインネーム機関/レジストリ、または(iii) Network Information Center (その関連会社、契約人、代理人、後継者、譲受人を含む)の指揮の下、または合意によって、ドメイン名を登録する個人または組織体。
Enterprise, as in Enterprise Service Center **エンタープライズ・サービス・センタとしての事業**	アフィリエートがマネージド PKI カスタマに対してマネージド PKI を提供するために加入する事業。
Enterprise EV Certificate:	発行にあたり、第三者認証、ドメインレベルの認証を含めることに関し、EV 証明書を使用するマネージド PKI カスタマは、シマンテックに権限を与える。
Enterprise RA **エンタープライズ RA**	CA/ブラウザフォーラムのガイドラインの要件に従い、シマンテックにより審査済みの最初の EV 証明書に記載のドメインを含む第 3 ドメインレベル以上のドメインに関して、シマンテックに審査を受けるドメイン認証および組織認証の EV 証明書を、複数要求することができるマネージド PKI for SSL のカスタマ。
Expiry Date **有効期限日**	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」日付。
EV Certificate: **EV 証明書**	EV ガイドラインに記載ある事項を含むデジタル証明書は、そのガイドラインに従い認証される。
EV OID	EV 証明書中に certificatePolicies フィールドを含む object identifier と呼ばれる識別番号は、(1)証明書に関連する証明書ポリシーを指すこと(2) EV 証明書としてマークされるいくつかのアプリケーション・ベンダーとの事前合意を含む。
Exigent Audit/Investigation **緊急監査または調査**	STN スタンダードに従うことに関するあるエンティティの怠慢、当該エンティティに関連する事故または危殆化、または当該エンティティが起こしたことによりもたらされる STN のセキュリティについての現実または可能性のある脅威を理由として米国シマンテックまたはシマンテックが行う監査または調査。
Extended Validation **エクステンディッド・バリ**	主要認証機関とブラウザベンダにより構成されたフォーラムから発行されたEV証明書に関するガイドラインで定義された審査の手続き。

Term	Definition
デーション(EV)	
FQDN(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。
Government Entity **政府機関**	政府が運営する法人、機関、部署、省庁、支部、または同様の構成要素、あるいはかかる国内の下位行政機関（州、市、郡など）
Intellectual Property Rights **知的財産権**	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。
Intermediate Certification Authority (Intermediate CA) **中間認証機関**	ルート証明書とエンドユーザ証明書を発行する証明書のチェーン内にある認証機関
Internal Server Name **内部サーバ名**	パブリック DNS では解決できないサーバ名（未登録ドメイン名を含む場合もある）。
International Organization **国際機関**	国際組織とは制定文書により設立された組織。制定文書とは2つ以上の独立国政府またはその代行者によって署名されている憲章、条約、協定または同等の文書である。
Issuing CA **発行 CA**	特定の証明書に関連して、証明書を発行した CA。これは、ルート CA または下位 CA の可能性がある。
Key Compromise **鍵の危殆化**	秘密鍵は、その値が権限のない人物に開示された、権限のない人物がアクセスした、または権限のない人物がその値を検出することができる実用的な技法が存 在する場合、危殆化したと考えられる。
Key Generation Ceremony **鍵ペア生成セレモニーf**	認証機関または登録機関の鍵ペアが生成され、その秘密鍵が暗号モジュール へ移転され、その秘密鍵の予備がとられ、その公開鍵が認証される手続き。
Key Generation Script **鍵生成スクリプト**	CA 鍵ペアの生成手順が記述された計画書。
Key Manager Administrator **キーマネジメントサービス管理者**	マネージド PKI のキーマネジメント・サービスを利用するカスタマにおいて、キ・ージェネレーションとキー・リカバリを実行する管理者。
Key Pair **鍵ペア**	秘密鍵とそれに関連付けられた公開鍵。
Key Recovery Block (KRB) **キー・リカバリー・ブロック**	暗号鍵を利用して暗号化された利用者の秘密鍵を含んでいるデータ構造。KRB はキーマネジメントサービスソフトウェアを利用して生成される。
Key Recovery Service **キー・リカバリー・サービス**	利用者の秘密鍵を復旧するために、マネージド PKI カスタマがキーマネジャーサービス・オプションを使用することによって、KRB を復旧させるために必要とする暗号鍵を提供するシマンテックのサービス。
Legal Entity **法人**	当該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、またはその他の組織体。
Managed PKI **マネージド PKI**	シマンテックのエンタープライズ・カスタマが STN 内で証明書を従業員、パートナー、サプライヤーおよび顧客、さらにサーバ、ルーターおよびファイアウォール等のデバイスに発行することのできるシマンテックの完全に統合された PKI サービス。Symantec Managed PKI を意味する。マネージド PKI は、エンタープライズ・カスタマにセキュアなメッセージ、イントラネット、エクストラネット、バーチャル・プライベート・ネットワークおよび電子商取引を可能にする。
Managed PKI	マネージド PKI カスタマのために認証その他の登録機関の役割を果たす管理者。

Term	Definition
Administrator マネージド PKI 管理者	
Managed PKI Control Center マネージド PKI コントロール・センタ	マネージド PKI 管理者が証明書申請を手動認証することができるウェブベースのインターフェース。
Managed PKI Customer マネージド PKI カスタマ	シマンテックからマネージド PKI サービスの提供を受ける組織で、その組織はクライアント証明書を発行するために STN 内で認証機関になる。マネージド PKI カスタマは、シマンテックに発行、管理および失効に関するバックエンド機能をアウトソースするが、証明書申請を承認または拒絶し、証明書の失効および更新を申請する登録機関としての機能は保持する。
Managed PKI Key Manager キーマネージメントサービス	特別なマネージド PKI 契約に基づき、キー・リカバリーを実行することを選択するマネージド PKI カスタマのためのキー・リカバリー・ソリューション。
Managed PKI Key Management Service Administrator's Guide キーマネージメントサービス管理者ガイド	キーマネージメントを利用するマネージド PKI カスタマのために運用要件および実務を規定する文書。
Manual Authentication 手動承認	証明書申請に関し、管理者によりウェブに基づくインターフェースを利用して一件ずつ手動で調査され承認される手続。
NetSure Protection Plan NetSure プロテクション・プラン	CP セクション 9.2.3 に規定される拡張された保証プログラム。
Nonverified Subscriber Information 確認を実施しない利用者情報	I 証明書申請者から認証機関または登録機関に対し送信された情報で、証明書に含まれるが、当該認証機関または登録機関により確認されていない情報。当該認証機関および登録機関は当該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には何らの保証も行わない。
Non-repudiation 否認防止	通信の発信者についての不当な否認、送信したことの否認、もしくは到達の否認に対する保護を与える通信の属性。発信者の否認には、過去に通信したことのある相手（その者を知らない場合でも）からのメッセージの否認を含む。注意：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、否認を否定するものである。例えば、STN の証明書を引用するデジタル署名は、裁判所による否認を否定する判断のための証拠を提供するものであるが、デジタル署名自体が否認を否定するものではない。
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該当する国際標準化機構（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 Responder OCSP レスポンダ	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。「Online Certificate Status Protocol」も参照のこと。
Offline CA	ネットワーク経由で侵入者から予期される攻撃を防ぐためのセキュリティ要件により、オフラインにて保全される STN の第一次認証機関、下位を発行するルート CA、他の中間 CA。これらの CA は直接エンドユーザ利用者の証明書を署名することはない。
Online CA	エンドユーザ利用者の証明書を署名する CA は、署名サービスを継続して提供するため、オンラインにて保全される。
Online Certificate Status Protocol (OCSP)	依拠当事者に対しリアルタイムの証明書ステータス情報を提供するプロトコル
Operational Period 運用期間	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当該記載された日時による）に始まり、当該証明書の効力が終了する日時（それ以前に失効された場合には当該失効の日時による）に終了する期間。

Term	Definition
Parent Company **親会社**	親会社とは、子会社の過半数を所有する会社であって、QIIS 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されたもの。
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、証明書署名要求の構造について定義する。
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、秘密鍵受渡のための安全な方法について定義する。
Primary Certification Authority (PCA) **第一次認証機関**	ある特定の Class の証明書に対するルート認証機関として行動する認証機関で、下位の認証機関に対して証明書を発行する。
Principal Individual(s)	雇用者、従業員、関連会社、代理人から事業の実行者であると認識されている、民間組織、行政機関、個人事業主の個人のオーナー、パートナー、経営陣、重役、役員である個人の EV 証明書の要求、発行、使用。
Private Key 秘密鍵	鍵ペアの一方の鍵。所有者によって秘匿性が保たれ、デジタル署名を作成したり、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を復号したりするために使用される。
Processing Center **プロセッシング・センタ**	証明書発行のための暗号モジュール等を収容するセキュアな施設および設備。リテール証明書発行サービスにおいて、プロセッシング・センタは、STN 内において認証機関として行動し、証明書の発行、管理、失効および更新といった証明書の全てのライフサイクル・サービスを提供する。企業向けサービスに関しては、プロセッシング・センタは、そのマネージド PKI カスタマまたは自己より下位のサービス・センタのマネージド PKI カスタマに代わり、証明書のライフサイクル・サービスを提供する。
Public Key **公開鍵**	鍵ペアの一方の鍵。対応する秘密鍵の所有者によって広く公開され、所有者の対応する秘密鍵を用いて作成されたデジタル署名を検証したり、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したりするために、依拠当事者によって使用される。
Public Key Infrastructure (PKI) **公開鍵インフラストラクチャ(PKI)**	証明書を基盤とする公開鍵暗号システムの実施および運用を総体的に成立させるアーキテクチャー、組織、技術、実務および手続のこと。STN PKI は STN の提供および実装を連携して行う複数のシステムから成り立つ。
Publicly-Trusted Certificate **パブリック証明書**	広く利用可能なアプリケーションソフトウェアにおいて対応するルート証明書が信頼されたルート証明機関として配布されている事実によって信頼されている証明書。
Qualified Auditor **公認監査人**	セクション 17.6 (監査役の資格)の要件を満たす個人または法人。
Registered Domain Name **登録ドメイン名**	ドメイン名登録機関で登録されているドメイン名。
Registration Agency	政府機関が登録したエンティティのビジネス形態、ライセンス、代理店、その他承認されたビジネスとして実する許可に関連した企業情報。以下のものに制限されない。(i) 国営企業; (ii) 政府認可の企業(iii) 特定企業
Registration Authority (RA) **登録機関(RA)**	認証機関から承認されたエンティティであって、証明書申請に際し証明書申請者を支援し、証明書申請に関し承認または拒絶し、証明書の失効または証明書の更新を行う。
Regulated Financial Institution **統制された金融機関**	認定を受けた地域の適用法のもと、政府、国、地方自治体により規制当局の統制、監督、検査を受けた金融機関。
Reliable Method of Communication **信頼できる連絡手段**	申請権限者以外の情報源を使用して確認された、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。

Term	Definition
Relying Party 依拠当事者	証明書またはデジタル署名に依拠して行為する個人または組織。
Relying Party Agreement 依拠当事者規約	認証機関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行動するための諸条件を規定する。
Repository リポジトリ	公開された PKI 管理ドキュメント(証明書ポリシーや認証局運用規定など)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。
Reseller リセラ	特定の市場に対し、シマンテックに代わり、サービスを販売するエンティティ。
Reserved IP Address 予約 IP アドレス	IANA が予約済みとしている IPv4 または IPv6 アドレス。 http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml
Retail Certificate リテール証明書	認証機関であるシマンテックによって、ウェブ・サイトで申請した個人または組織に対して発行される証明書。
Root CA ルート 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る最高位の認証局。下位 CA 証明書を発行する。
Root Certificate ルート証明書	自身を識別し、下位 CA に発効される証明書の検証を容易にするためにルート CA によって発行される自己署名証明書。
RSA	公開鍵暗号方式は、Rivest, Shamir, Adelman によって発明された。
Secret Share シークレット・シェア	シークレット・シェアリング契約に基づく、認証機関の鍵の一部分または認証機関の秘密鍵を運用するために必要な起動データの一部。
Secret Sharing シークレット・シェアリング	認証機関の秘密鍵または認証機関の秘密鍵を運用するための起動データを分割する実務で、本 CPS セクション 6.2.2 に定める認証機関の秘密鍵の運用を複数人の管理下におくためになされる。
Secure Sockets Layer (SSL) セキュア・ソケット・レイヤ (SSL)	Netscape Communications Corporation によって開発されたウェブ通信を保護するための業界標準方法。SSL セキュリティ・プロトコルはデータの暗号化、サーバ認証、メッセージの完全性およびオプションとしてクライアント認証を提供する。
Security and Audit Requirements (SAR) Guide	プロセッシング・センタおよびサービス・センタのセキュリティおよび監査の要件および実務を規定するシマンテックの文書。
Security and Practices Review セキュリティ・レビュー	アフィリエートが運用の許可を得る前に米国シマンテックが行うレビュー。
Service Center サービス・センタ	特定の Class または種類の証明書を発行するための証明書署名ユニットを保有せず、プロセッシング・センタに依拠し当該証明書の発行、管理、失効および更新を行うアフィリエート(シマンテックを含む)。
Sovereign State 独立国	独立国は州または国であり、独自の政府によって統治されていて、他の権力による従属、属国状態でないもの。
STN Participant STN 参加者	STN 内において、次の一つ以上に該当する個人または組織:米国シマンテック、アフィリエート(シマンテックを含む)、カスタマ、利用者または依拠当事者
STN Standards STN スタンダード	STN 内の証明書発行、管理、失効、更新、使用に関するビジネス的、法的、技術的な要求事項
Sub-domain サブドメイン	STN 階層内においてあるエンティティとそれより下位のエンティティの管理を受ける STN の一部分。
Subject	公開鍵に対応する秘密鍵の保有者。Subject という用語は、組織向け証明書の場合には、秘密鍵を保有する装置またはデバイスを指すこともある。Subject は、当該 Subject の証明書中に含まれる公開鍵と結合した明確な名称を割り当てられる。
Subject Identity	証明書の サブジェクトを識別する情報。サブジェクトアイデンティティ情報には、

Term	Definition
Information サブジェクト アイデンティティ情報	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で指定されるドメイン名は含まれない。
Subordinate CA 下位 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局。
Subscriber 利用者	利用者証明書の場合には、証明書が発行され、その Subject となっている人物をいう。組織向け証明書の場合には、証明書が発行され、その Subject となっている装置またはデバイスを所有する組織を言う。利用者は、証明書中に記載された公開鍵に対応する秘密鍵を利用することができ、また、利用する権限がある。
Subscriber Agreement 利用規約	認証機関または登録機関により利用される規約で、個人または組織が利用者として行動するための諸条件を規定する。
Subsidiary Company 子会社	子会社とは、申請者が全てを所有する会社であって、QIIS が登録されている 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書によって確認されたもの。
Superior Entity 上位エンティティ	Class 1, 2, もしくは 3 の STN 証明書階層における特定のエンティティ以上のエンティティ。
Supplemental Risk Management Review 追加リスク・マネジメント・レビュー	シマンテックによってあるエンティティについてなされる検査で、当該エンティティに関する準拠性監査において不完全もしくは例外的な結果が発見された場合になされるか、または通常業務の過程でなされる全体的リスク・マネージメント・プロセスの一部としてなされる。
Symantec 米国シマンテック	本 CPS の全ての記載に関して、米国シマンテック・コーポレーションとその子会社は、問題となる特定の活動に対し、責任を負う。
Symantec Repository シマンテック・レポジトリ	証明書および関連する STN の情報についてオンラインでアクセス可能な米国シマンテックのデータベース。
Symantec Trust Network (STN)	証明書を基盤とする公開鍵インフラストラクチャで、STN 証明書ポリシーにより運営され、米国シマンテックおよびそのアフィリエート、それらの関連するカスタマ、利用者および依拠当事者による証明書の全世界レベルでの展開および使用を可能とするもの。
Terms of Use 利用規約	申請者/加入者が CA の関連会社である場合、CA/ブラウザフォーラムの Baseline Requirements に従って発行される証明書の保管および利用に関する規約。
Transport Layer Security (TLS) トランスポート・レイヤ・セキュリティ (TLS)	SSL をもとに開発されたウェブ通信を保護するための業界標準方法。SSL と同じく、データの暗号化、サーバ認証、メッセージの完全性およびオプションとしてクライアント認証を提供する。
Trusted Person 信頼される者	STN 内のエンティティの従業員、独立請負業者またはコンサルタントで、当該エンティティ、その製品、サービス、施設または実務に関する基盤となる信頼性を管理する責を負う者。本 CPS セクション 5.2.1 においてより詳細に規定される。
Trusted Position 信頼される地位	STN のエンティティにおける地位で、信頼される者がその任につくことを要する。
Trustworthy System 信頼すべきシステム	侵入、誤用から合理的に保護され、合理的レベルの可用性、信頼性および操作の正確性を備え、意図する機能を合理的な程度に満たし、かつ、該当するセキュリティ・ポリシーを実施するコンピュータ・ハードウェア、ソフトウェアおよび手続き。アメリカ合衆国政府が定めた用語体系中の「信頼されるシステム（Trusted system）」とは必ずしも一致しない。
Unregistered Domain Name 未登録ドメイン名	登録ドメイン名ではないドメイン名。
Valid Certificate 有効な証明書	RFC 5280 で規定されている検証手順に合格した証明書。

Term	Definition
Validation Specialists **認証スペシャリスト**	CA/ブラウザフォーラムの Baseline Requirements によって規定されている情報検証職責を果たす人物。
Validity Period **有効期間**	証明書が発行された日から有効期限日までの期間。
Symantec Repository **シマンテック・リポジトリ**	証明書および他の関連する STN 情報に関するシマンテックのデータベースでオンラインでのアクセスが可能なもの。
Wildcard Certificate **ワイルドカード証明書**	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。

Appendix B1

EV SSL 証明書の追加認証手続き

参照 : 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
www.cabforum.org

目次

1. 概要

本 Appendix では、CA/ブラウザフォーラム(www.cabforum.org) により発行された、Extended Validation証明書（以下、「EV証明書」）に関するEVガイドライン（以下、「ガイドライン」という）に基づいてEV 証明書を発行するにあたっての、シマンテック CPS に対する追加手続きを記述する。このガイドラインは認証機関（Certification Authority、以下「CA」という）がEV 証明書を発行するにあたり守るべき必要最低限の要件を記述する。本 Appendix ではインターネットのSSL/TLS 認証で使用されるEV 証明書について記載する。

有効なEV 証明書の組織情報は、対応するソフトウェアアプリケーション(例、ブラウザ)によって、アクセス先のウェブ・サイトを監督している組織の名称について信頼できる確認の証を提供するために特別な手段で表示される可能性がある。

2. EV 証明書の基本概念

2.1 EV 証明書の目的

EV 証明書は、TLS/SSLプロトコルを使ったウェブベースのデータ通信の確立のために使われることを意図している。

2.1.1 主目的

ガイドラインにより、EV 証明書の主目的を以下の通りとする。

- ウェブ・サイトを運営する組織の法的存在の確認:
  ブラウザを使用するユーザがアクセスしているウェブ・サイトが、EV 証明書に記載の名前、事業拠点の住所、法人設立/登録管轄地、登録番号で特定される法人によって運営されていることをそのユーザに対して合理的に保証する。および、

- ウェブ・サイトとの暗号化通信の有効化:
  ブラウザのユーザとウェブ・サイト間の、インターネットを介した情報の暗号化通信を可能にするための暗号鍵の交換を容易にする。

2.1.2 副次的目的

EV 証明書の副次的な目的は、ウェブ・サイトを運営している組織の正当性の立証を支援すること、および、フィッシングその他のオンラインアイデンティティ詐欺に関連する問題に対処する手段を提供することである。EV 証明書は、組織に関して第三者が審査した信頼性の高いアイデンティティ情報および住所情報を提供することによって、以下に貢献する。

- SSLサーバ証明書を使用するフィッシング詐欺およびその他のオンラインアイデンティティ詐欺の実施をより困難にする。

- 企業のアイデンティティやウェブ・サイトの正当性を確認する手段をユーザに提供することによって、フィッシング攻撃やオンラインアイデンティティ詐欺の標的となる企業を支援する。また、

- 適用可能な場合、サブジェクトに対する連絡、調査、法的措置を実施することで、、フィッシン

グおよびその他のオンラインアイデンティティ詐欺の調査を支援する。

2.1.3 除外される目的

EV 証明書は証明書に記載されているサブジェクトのアイデンティティのみ扱い、サブジェクトの行動には関知しない。したがって、EV 証明書は、以下の保証あるいは別段の表明または保証を行うことを意図するものではない。

- EV 証明書に記載されているサブジェクトが積極的に業務に従事していること
- EV 証明書に記載されているサブジェクトが適用法規を順守していること
- EV 証明書に記載されているサブジェクトが事業において信頼でき、公正で、評判がよいこと、また
- EV 証明書内に記載のサブジェクトとの取引を行うことが「安全で」あること

3. 参照先

http://cabforum.org/documents.html にあるガイドラインを参照。

4. 定義

http://cabforum.org/documents.html にあるガイドラインの定義を参照。

5. 略語と頭字語

http://cabforum.org/documents.html にあるガイドラインの略語と頭字語を参照。

6. 規約

http://cabforum.org/documents.html にあるガイドラインの規約を参照。

7. EV 証明書の保証および表明

7.1 EV 証明書の保証

シマンテックが発行したEV 証明書について、シマンテックは、EV証明書が有効である間、EV証明書の発行、管理および証明書に含まれる情報の正確性の確認において、ガイドラインおよびEVポリシーに従っていることについて、EV 証明書受益者に表明および保証する(EV 証明書保証)。EV 証明書保証には具体的に以下の保証を含むが、制限されない。

A. 法的存在:
シマンテックが、EV 証明書を発行した時点において、EV 証明書に記載されているサブジェクトがその法人設立/登録管轄地内に有効な組織(エンティティ)として法的に存在することを、サブジェクトの法人設立/登録管轄地の法人設立/登録機関に確認したこと

B. アイデンティティ:
シマンテックが、EV 証明書を発行した時点において、EV 証明書に記載されているサブジェクトの法的名称が、サブジェクトの法人設立/登録管轄地の法人設立/登録機関の公式記録の名前と一致していること、また、屋号が含まれる場合は、サブジェクトが事業拠点の管轄地でその屋号を正しく登録していることを確認したこと

C. ドメイン名を使用する権利:
シマンテックが、EV 証明書を発行した時点において、EV 証明書に記載されているサブジェクトが、EV 証明書に記載のあらゆるドメイン名の排他的使用権を有することを審査するために必要と合理的に認められる手段をすべて講じたこと。

D. EV 証明書に対する承認:
シマンテックが、EV 証明書に記載されているサブジェクトがEV 証明書の発行を承認したことを審査するために合理的に必要と判断された手段をすべて講じたこと。

E. 情報の正確性:
シマンテックが、EV 証明書を発行した時点において、EV 証明書に記載のその他の情報がすべて正確であることを審査するに合理的に必要と判断された手段をすべて講じたこと。

F. 加入者契約:
EV 証明書に記載されているサブジェクトが、ガイドラインの要件を満たし、法的に有効かつ強制力を有する加入者契約をシマンテックと締結したこと。CA および加入者が関連会社である場合、申請権限者が利用規約を認め、同意したこと。

G. ステータス:
シマンテックおよび米国シマンテックが、ガイドラインの要件に従い、EV 証明書の現在のステータスが有効か失効されているかという情報を掲載した24時間365日オンラインアクセスが可能なリポジトリを保守すること。

H. 失効:
シマンテックおよび米国シマンテックが、ガイドラインの要件に従い、ガイドラインと本 Appendix に特定された失効事象発生時にはEV 証明書を速やかに失効させること。

7.2 申請者によるもの

シマンテックは、加入者契約の一部として、シマンテックおよびEV 証明書受益者の利益のために、加入者がガイドラインの加入者契約の要件の節で規定したコミットメントおよび保証を行うことを要求する。

8. コミュニティおよび利用可能性

8.1 EV 証明書の発行

EV 証明書を発行する場合、シマンテックは、ガイドラインおよび本 Appendix に沿って以下の要件を満たす。

シマンテックが業務を行う管轄地において、シマンテックの事業およびシマンテックが発行する証明書に適用されうる全法規に準拠する。ガイドラインの要件の対象となる活動（運用または証明書の発行）に対して司法権を有する裁判所または政府機関が、本要件の必須要件の履行を違法

と判決した場合、シマンテックはあらゆる状況についてについてもCA/ブラウザフォーラムに通知するものとする。

8.2 EV ポリシー

8.2.1 実装

この追加のAppendix B を伴う本CPSは、

- 折々の改訂時にガイドラインの要件を充足する
- (i) その時点の WebTrust Program for CAs および (ii) その時点の WebTrust EV Program、または、 CA/ブラウザフォーラムが承認した (i) および (ii) の相当物の要件を充足する
- EV 証明書の信頼性の拠りどころとなる全ルートを含む、シマンテック全体のルートCAのルート証明書の全階層を指定する。また、米国シマンテックのルート階層の構造は、https://www.symantec.com/about/profile/policies/repository.jspで参照可能である。

8.2.2 開示

シマンテックは、24時間365日利用可能なCPSを通じてEVポリシーを開示する。STN CPSは、RFC 3647に従って構成される。

8.3 準拠のコミットメント

シマンテックは、http://www.cabforum.org で公開される、最新バージョンの CA/ブラウザフォーラム「EV 証明書の発行と管理のためのガイドライン」(「以下、ガイドライン」)に準拠する。本 Appendix と同ガイドラインの間に不一致が生ずる場合は、ガイドラインがこのドキュメントよりも優先される。

さらに、シマンテックは、ガイドラインの適用される要件を、EV 証明書の発行または保守に関連する下位CA、RA、エンタープライズRA、および下請業者との契約書に(直接または参照されることによって)組み込む。

8.4 保険

シマンテックは、ガイドラインに基づくかかる当事者の履行および義務に起因して生じる賠償責任を自家保険とする。

8.5 EV 証明書の取得

8.5.1 概要

ガイドラインにおいて、EV 証明書は、以下の要件を満たす民間組織、事業体、行政機関および非営利団体に対してのみ発行される。

8.5.2 民間組織のサブジェクト

民間組織は、以下の要求を満たす必要がある。

(1) 民間組織は、法人設立/登録管轄地の法人設立/登録機関への届け出(または法人設立/登録機関の行為)(例:法人の設立を証明する証明書の発行など)によってその存在が確認できるものでなければならない。

(2) 民間組織は、(法人設立/登録管轄地の法律に基づき要求される場合)法人設立/登録機関に、Registered Agent, Registered Officeまたはこれに相当する施設を登録しなければならない。

(3) 民間組織は、法人設立/登録機関の記録に、「休眠(inactive)」、「無効(invalid)」、「不在(not current)」またはその相当物であると指定されていてはならない。

(4) 民間組織は、確認可能な物理的な存在と事業の存在がなければならない。

(5) 民間組織の法人設立、登録、公認、認可地および/または事業拠点の管轄地は、シマンテックまたは米国シマンテックの管轄地の法律によって取引または証明書の発行を禁じられているいかなる国にもあってはならない。

(6) 組織は、シマンテックの管轄地の法律に基づく行政機関の拒否リストまたは禁止リスト(輸出禁止など)に記載されていてはならない。

8.5.3 行政機関のサブジェクト

行政機関は、以下の要求を満たす必要がある。

(1) 行政機関の法的存在について行政機関が運営されている政治上の下部組織によって確立されていなければならない。

(2) 行政機関は、シマンテックまたは米国シマンテックの管轄地の法律によって取引または証明書の発行を禁じられているいかなる国であってはならない。

(3) 行政機関は、シマンテックまたは米国シマンテックの管轄地の法律に基づく行政機関の拒否リストまたは禁止リスト(輸出禁止など)に記載されていてはならない。

8.5.4 事業体

事業体は、以下の要求を満たす必要がある。

(1) 事業体は、法的に確認できる団体で、管轄される登録機関で一定の様式で登録認可する登録機関によって保証ないし承認、証明書、ライセンスがあり、登録機関によって存在が確認できなければならない。

(2) 事業体は確認可能な物理的存在および事業の存在がなければならない。

(3) 事業体は、最低一名の代表者は身元の確認が取れなければならない。

(4) 確認された代表者は代表者が利用者規約に同意したことを証明しなければならない。

(5) 事業体が屋号を使う場合は、シマンテックは、セクション 11.3 の要件事項に準じた確認をしなければならない。

(6) 事業体および確認された代表者は、シマンテックまたは米国シマンテックの管轄地の法律によって取引または証明書の発行を禁じられているいかなる国にもあってはならない。

(7) 事業体および確認された代表者は、シマンテックまたは米国シマンテックの管轄地の法律に基づく行政機関の拒否リストまたは禁止リスト(輸出禁止など)に記載されていてはならない。

8.5.5 非営利団体

シマンテックは、セクション8.5.2 から 8.5.4 を満たさない非営利団体に対して、以下の要件を満たせばEV 証明書を発行することができる。

(A) 申請者は国際的な組織体で、2 カ国以上またはその代行者によって署名されている国際憲章、国際協定または同等の協定書によって成立していること。CA ブラウザフォーラムでは、EV 証明書に適合した国際的な組織体のリストを発行している。

(B) 国際的な組織体は、その本部がシマンテックまたは米国シマンテックの管轄地の法律によって取引または証明書の発行を禁じられているいかなる国にもあってはならない。

(C) 国際的な組織体はシマンテックの管轄地の法律に基づく行政機関の拒否リストまたは禁止リスト(輸出禁止など)に記載されていてはならない。

適格な国際的な組織体の下部組織または部局はガイドラインに従って発行される EV 証明書に適格となる。

9. EV 証明書の内容およびプロファイル

本セクションでは、EV証明書のシマンテックおよびサブジェクトのアイデンティティに関連する、EV 証明書の内容の必須要件を規定する。

9.1 発行者情報

EV証明書は基本要件で規定される発行者情報を含まなければならず、基本要件からの補足である Appendix D セクション 9.1「発行者情報」で規定される。

9.2 サブジェクト情報

ガイドラインの要件に従い、EV 証明書およびその発行者となる下位 CA は、サブジェクトの組織についての以下の情報を含まなければならない。

9.2.1 サブジェクト組織名（必須）

認証された組織名は、organizationName(OID 2.5.4.10)に含まれる。

このフィールドには、サブジェクトの法人設立/登録管轄地の法人設立/登録機関の公式記録に記載されているか、確認されたサブジェクトの組織名を記載する。シマンテックは、組織名の先頭または末尾の法人格を略称にすることができる。例: Official Record で、"*会社名* Incorporated"となっている場合、"*会社名*, inc."とすることができる。シマンテックは、法人設立/登録管轄地で一般的に受入られている共通の略称をつかわなければならない。

さらに完全な法的組織名をかっこに入れて後続させることにより、サブジェクトが使用する屋号すなわち DBA をこのフィールドの先頭に記載することができる。完全な法的組織名と屋号すなわち DBA の合計がRFC 5280で定義された64文字を超過する場合は、シマンテックは、証明書中に完全な法的組織名のみを使用する。

組織名が 64 文字を超える場合、64 文字を超えないようにするために、シマンテックは組織名の一部を省略することができ、組織名に含まれる主体的でない単語を省くことができるが、依拠者が異なる組織と認識されてしまわないようにする。

9.2.2 Subject Alternative Name エクステンション（必須）

DNS名などの認証されたドメイン名は、SubjectAlternativeName に含まれる。

このフィールドには、サブジェクトのサーバに関連付けられた、サブジェクトが所有または支配する1つ以上のホストドメイン名を含む。かかるサーバの所有および運営は、サブジェクトまたは他のエンティティ(ホスティングサービスなど)が行うことができる。EV 証明書ではワイルドカード証明書は許可されない。

9.2.3 サブジェクトコモンネーム（廃止予定/推奨されないが、禁止されてはいない）

DNS 名のような認証されたドメイン名は、サブジェクトの CommonName (OID 2.5.4.3) に含まれる。

このフィールドには、サブジェクトのサーバに関連付けられたサブジェクトが所有または支配する1つのホストドメイン名を含む。かかるサーバの所有および運営は、サブジェクトまたは他のエンティティ(ホスティングサービスなど)が行うことができる。EV 証明書ではワイルドカード証明書は許可されない。

9.2.4 サブジェクト事業種別（必須）

事業種別名は、サブジェクトの businessCategory (OID 2.5.4.15) に含まれる。

このフィールドには、次に示す文字列のいずれかが含まれる。'Private Organization', 'Government Entity', 'Business Entity' または 'Non-Commercial Entity'。これはそれぞれ、本章の 8.5.2, 8.5.3, 8.5.4 または 8.5.5 で定義しているサブジェクトに依存する。

9.2.5 サブジェクトの法人設立/登録管轄地（必須）

シマンテックのEV 証明書は、サブジェクトの認証された法人設立/登録機関の管轄地を以下のTable 1の通り記載する。

所在地	必須/任意	証明書のフィールド
市区町村	任意	jurisdictionOfIncorporationLocalityName (OID 1.3.6.1.4.1.311.60.2.1.1) RFC 5280に指定のASN.1 - X520LocalityName
州または県 (該当する場合)	任意	jurisdictionOfIncorporationStateOrProvinceName (OID 1.3.6.1.4.1.311.60.2.1.2)

		RFC 5280に指定のASN.1 X520StateOrProvinceName
国	必須	jurisdictionOfIncorporationCountryName (OID 1.3.6.1.4.1.311.60.2.1.3) RFC 5280に指定のASN.1 – X520countryName

Table 1. Jurisdiction of Incorporation or Registration Certificate Fields

これらのフィールドには、法人設立/登録機関に関連のない情報を含んではならない。。たとえば、国レベルの管轄地の法人設立/登録機関の場合は、国の情報を記載するが、州または県、あるいは市区町村の情報は記載してはならない。同様に、州または県レベルの管轄地の法人設立/登録機関の場合は、国の情報および州または県の情報を記載するが、市区町村の情報は記載しない。そして、市区町村レベルの管轄地の法人設立/登録機関の場合は、国の情報および州または県、そして市区町村レベルの情報だけでなく、そのエンティティを登録する州または県の情報も記載する。国の情報は該当するISO国コードを使用して指定されなければならない。サブジェクトの法人設立/登録管轄地の州または県の情報および市区町村の情報(該当する場合)は、該当する管轄地の完全な名前を使用して指定しなければならない。日本の民間機関の法人設立は法務省の管轄であるため、国の情報(JP)にのみを記載する。

9.2.6 サブジェクト登録番号(必須)

シマンテックのEV 証明書は、サブジェクトが民間機関の場合、法人設立/登録管轄地の法人設立機関がサブジェクトに割り当てた登録(または同様の)番号をサブジェクトのserialNumber フィールド(OID 2.5.4.5)に含む。日本の民間機関の場合、会社法人等番号を記載する。

登録番号や確認可能な設定日を持たない行政機関の場合、シマンテックはサブジェクトが行政機関であることを示す適切な言語を記載する。

法人設立/登録管轄地が登録番号を提供していない場合、設立/登録日を共通の日付様式でこのフィールドに記載する。

9.2.7 実際の事業拠点の住所

シマンテックのEV 証明書は、サブジェクトの確認された事業拠点の住所を以下のTable 3の通り記載する。

所在地	必須/任意	証明書のフィールド
番地および丁目	任意	streetAddress (OID 2.5.4.9)
市区町村	必須	localityName (OID 2.5.4.7)
州または県 (該当する場合)	必須	stateOrProvinceName (OID 2.5.4.8)
国	必須	countryName (OID 2.5.4.6)
郵便番号	任意	postalCode (OID 2.5.4.17)

Table 2 実際の事業拠点の住所を示す証明書のフィールド

9.2.8 その他の属性

サブジェクトフィールドとして存在する全てのその他の任意のオプション属性は、シマンテックによっ

て確認された情報を入れなければならない。
FQDN名は、本Appendix 9.2.1 に記載するサブジェクト組織名として明記され、サブジェクトの組織情報が本Appendix 9.2 に記載するサブジェクト情報としてのみ明記される形で含まれている場合を除き、サブジェクト属性に含まれるべきではない。

サブジェクトフィールドの任意の属性フィールドには、審査を通過した情報を含むか、空白とする。シマンテックは、「.」、「-」、「」(空白)の文字などのメタデータや、値が存在しない、不完全である、または適用不可であることを示すものを含めない。

9.3 証明書ポリシーの識別

9.3.1 EV 証明書ポリシーの識別の要件

以降に記載するポリシー識別子を含んで発行される証明書は、CAブラウザフォーラムのガイドラインに従い、米国シマンテックにより管理される。

9.3.2 EV 加入者証明書

シマンテックから加入者に発行される各 EV 証明書には、証明書の certificatePolicies エクステンションに米国シマンテックの EV 用ポリシー識別子が含まれる。このために使用される米国シマンテックのポリシー識別子は、2.16.840.1.113733.1.7.23.6 である。

9.3.3 ルート CA 証明書

EV 証明書のための米国シマンテック ルート CA 証明書は、Symantec Class 3 Primary Certification Authority である。このルート CA には、certificatePolicies または extendedKeyUsage エクステンションは含まれていない。

9.3.4 EV 下位 CA 証明書

Symantec Class 3 High Assurance CA は、米国シマンテックのポリシー識別子を含むと同時に、特殊な anyPolicy OID (2.5.29.32.0) も含む。

9.4 有効期間

EV 証明書の最大有効期間は、27ヶ月である。

9.5 加入者の公開鍵

シマンテックが発行する証明書は、本CPS セクション 6.1.5 で要求されるアルゴリズムと鍵サイズの要件を満たす。また、最低限の暗号化アルゴリズムと鍵サイズの条件については Appendix B2 も参照のこと。

9.6 証明書シリアルナンバー

シマンテックおよび米国シマンテックのCAは、少なくとも 20 ビットのエントロピーを表す、非連続の証明書シリアルナンバーを生成する。

9.7 その他の EV 証明書の技術要件

最低限の暗号化アルゴリズムと鍵サイズの条件については Appendix B2 を参照のこと。EV証明書のエクステンションについては Appendix B3 を参照のこと。

10. EV 証明書要求の要件

10.1 一般的要件

10.1.1 ドキュメント要件

シマンテックは、EV 証明書の発行前に、ガイドラインの基本要件からの補足である本CPS Appendix D セクション 10.1 に規定したように、申請者からドキュメントを取得しなければならない。

10.1.2 役割の要件

EV 証明書の発行に際し、申請に関する以下の役割が必要である。

- **証明書要求者** –権限のある証明書要求者が、EV 証明書要求を実施しなければならない。証明書要求者は、申請者に雇われた自然人、申請者の代理を務める明示的な権限を有する代理人、または申請者の代理でEV 証明書要求を作成、提出する第三者(ISP、ホスティング会社など)である。

- **証明書承認者** –権限のある証明書承認者が、EV 証明書要求を承認しなければならない。証明書承認者は、(i)証明書要求者として行動するとともに他の従業員または第三者に証明書要求者として行動する権限を付与し、(ii)他の証明書要求者が提出した証明書要求を承認する、申請者に雇われた自然人または申請者の代理を務める明示的な権限を有する代理人である。

  STNでは、証明書承認者は、リテール証明書については法人窓口、と、マネージド PKI for SSLアカウントから発行された証明書についてはマネージド PKI for SSL管理者と、それぞれ同等である。

- **契約書署名者** – 権限のある契約書署名者は、要求されたEV 証明書に適用される利用規約に署名しなければならない。契約書署名者は、申請者の代理を務める明示的な権限を持ち、かつ申請者の代理で利用規約に署名する権限を有する、申請者、申請者に雇われた自然人または代理人である。

  STNでは、契約書署名者は、リテール証明書の法人窓口、マネージド PKI for SSLのアカウントのマネージド PKI for SSLの組織窓口と同等である。

- **申請権限者** –申請者が CA の関連会社である場合に、権限のある申請権限者がEV 証明書要求に適用される証明書利用規約を認め、同意しなくてはならない。申請権限者は申請者によって雇用されている、または申請者を代表するための明示的な権限を持ち、申請者に代わって利用者規約を認め、同意する権限を持つ自然人である。

申請者は、1 名の人物に上記役割の一つ、二つ、または三つの権限を付与することができるが、いずれの場合についても、証明書承認者および契約書署名者が申請者の従業員でなければならない。申請者は、上記の各役割をつとめる権限を複数の人物に付与することもできる。

10.2 EV 証明書要求の要件

EV 証明書の発行前に、本 Appendix セクション 11.13 に規定する有効期間および更新についての要件を前提として、シマンテックは、(申請者を代表することを承認された証明書要求者を通して)申請者から、基本要件からの補足である Appendix D セクション 10.2 に従い適切に不足なく記入され署名された EV 証明書要求を取得する。

10.3 加入者契約の要件

EV 証明書の発行前に、シマンテックは、基本要件からの補足である Appendix D セクション 10.3 に従い、法的強制力を有する加入者契約に対する申請者の同意を取得する。

リテール証明書において証明書要求ごとに個別の加入者契約を用意する場合や、マネージド PKI for SSL アカウントにおいて単一の加入者契約で将来の複数にわたった証明書要求と証明書をカバーする場合がある。

さらに、証明書要求が申請者のすべての必要事項を満たさない場合、シマンテックは申請者でなく証明書承認者もしくは契約書署名者と、不足する情報について確認する。

11. 情報の審査の要件

11.1 概要

このセクションではガイドラインの審査要件およびこれを満たすようシマンテックが実施する手続きを規定する。

EV 証明書発行前に、シマンテックは、EV 証明書の全てのサブジェクトの組織情報がガイドラインの要件を満たし、かつこれに従って検証されたことを確認し、さらに認証作業に準じて確認および記録された情報との照合を行う。

11.2 申請者の法的存在およびアイデンティティの検証

(1) 民間組織

<u>法的存在</u>

シマンテックは、申請者の法的存在およびアイデンティティを審査するため、申請団体が法的に存在を認められた法人であり、申請団体の法人設立/登録管轄地の法人設立/登録機関によって形成（法人化など）されており、法人設立/登録機関の記録で「活動中(active)」、「有効(valid)」、「存在(current)」、またはこれらに相当する指定を受けていることを審査する。

組織名
シマンテックは、申請団体の法人設立/登録管轄地の法人設立/登録機関に記録された申請団体の正式な法的名称とEV 証明書要求内の申請団体の名前が一致していることを審査する。

登録番号
シマンテックは、申請者の法人設立/登録管轄地の法人設立/登録機関が申請者に割り当てた登録番号を取得する。法人設立/登録機関が申請者に登録番号を割り当てない場合、シマンテックは申請者の法人設立/登録の日付を取得する。

Registered Agent
シマンテックはさらに、申請者の法人設立/登録管轄地における申請者のRegistered Agentまたは Registered Office(該当する場合)のアイデンティティおよび住所を取得する。

(2) 行政機関

法的存在、機関名、登録番号
シマンテックは、申請者が法的に行政機関であり、行政機関が運営する下位行政機関として存在していること、および、申請者の法的正式名称が EV 証明書申請の申請者名称と一致していること、を審査する。シマンテックは申請者の設立、登録または立法上で行政機関が作られ確認された日を確認する。これらの情報が得られない場合は、サブジェクトが行政機関であることを示す適切な言語を入力しなければならない。

行政機関は以下のいずれかの方法により審査される。

a)行政機関が運営する下位行政機関の QGIS、もしくは
b)申請者と同じ行政区分における上位の行政機関、もしくは
（例；州知事は特定の州庁の部署の法的存在を審査することができる）
c)国、州、または下位行政機関である地方の司法機関の一員である裁判官
d)行政機関を代理する弁護士

この審査は、QIIS から取得した住所もしくは電話番号を用いて、行政機関との対面での直接の確認もしくは書簡、E メール、ウェブのアドレス、または電話により実施される。

裁判官からのいかなる連絡も、本 Appendix セクション 11.10.1 に規定する、弁護士による事実の主張と同様の方法で審査されなければならない。

(3) 事業体

法的存在
申請者が申請書に含まれる名称で事業を行っているか審査する。

組織名
申請者の法的正式名称が EV 証明書申請の申請者名と一致し、申請者の登録管轄地で登録機関によって認識されていることを審査する。

登録番号

申請者の登録管轄地の登録機関によって割り当てられた特定の固有の登録番号を確認する。登録機関が登録番号を割り当てない場合は、申請者の登録日を確認する。

代表者
代表者のアイデンティティを審査する。審査手続きはガイドラインのセクション 11.2.2(4) に従う。

(4) 非営利団体(国際組織体)
法的存在
申請者が法的に存在を認められた国際組織体であること、申請者の法的正式名称が EV 証明書申請の申請者名と一致していることを審査する。

登録番号
シマンテックは申請者の設立、登録または立法上で国際組織体が作られ確認された日を確認すべきである。これらの情報が得られない場合は、サブジェクトが国際組織体であることを示す適切な言語を入力しなければならない。

国際組織体は以下のいずれかの方法で審査される。

- 国際組織体が設立された際の制定文書の記述、もしくは
- シマンテックが事業を行うことを許可された加盟国政府に直接の確認を行う。この審査の場合、適切な政府の代理人もしくは憲法により行われるか、もしくはその政府が国際組織体を代表する役割であることを確認する、もしくは
- CA/ブラウザフォーラムが www.cabforum.org にて維持する、資格のあるエンティティを記載した最新のリストを直接確認する、もしくは
- EV 証明書を申請する国際組織体が、審査済みの非政府組織(NGO)を含む機関の場合、シマンテックは、国際組織体の申請者が機関として機能する、審査済みの包括的な国際組織体への確認によって申請者を審査する。

11.3 申請者の法的存在およびアイデンティティの検証 – 屋号

EV 証明書内で主張する申請者のアイデンティティに、申請者の法人設立/登録管轄地の法人設立/登録機関もしくは登録簿に登録された正式な法的名称に加えて屋号もしくはDBAを含める場合、シマンテックは、(i)申請者が、事業拠点の管轄地の該当する行政機関に屋号もしくはDBAの使用を登録済みであること(ガイドラインに従う検証手続きによって確認)、および、(ii)届出が現在有効であること、を検証する。

シマンテックは、公認独立情報源を利用して屋号を確認するか、または、認証された弁護士意見書や会計士の意見に含まれる屋号によって確認を行う。

11.4 申請者の物理的存在の検証

11.4.1 申請者の事業拠点の住所

シマンテックは、申請者の物理的存在および事業の存在を検証するために、申請者が提示した住所が(郵便受けや郵便箱ではなく)申請者または親会社もしくは子会社が事業を行っている場所であり、かつ申請者の事業拠点の住所であることを検証しなければならない。

行政機関の申請者においては、QGIS の記録にある申請者の管轄における住所が、識別される住所とされる。

シマンテックは、法的な効力を持つ意見書が無い場合、下記のような独自の方法で住所を確認する。

(A) 事業拠点が法人設立/登録管轄地と同じ国にある申請者の場合

(1) 1つ以上の公認独立情報源に同じ住所の事業所で登録されている申請者の場合
シマンテックは、そのデータベースを参照することによって、EV 証明書要求に記載の申請者の住所が、申請者または親/子会社の事業を行っている場所の有効な住所であることを確認する。もしくは、事業所の住所に関する申請者の陳述書に依拠しても良い。

(2) 1つ以上の最新バージョンの公認独立情報源に同じ住所の事業所で登録されていない申請者の場合
シマンテックは、信頼できる個人または企業による事業所の現地訪問記録を取得することによって、申請者がEV 証明書申請に記入した住所が、実際に申請者または親/子会社が事業を行っている場所の住所であることを確認する。訪問記録では、以下を確認する。

(a) (永続的な看板や従業員の立証によって)申請者の事業所が正確にEV明書要求に記載のとおりの住所にあることを検証する。

(b) 施設の種類(商業ビル内のオフィス、民間住宅、店頭など)を明確にし、永続的に事業を展開する場所と思われるかどうかを判定する。

(c) 申請者を示す永続的な(移動不可能な)看板などがあることを示確認する。

(d) (郵便受けや郵便箱ではなく)申請者がその場所で継続的に事業活動を行っている証拠があるかどうかを確認する。また、

(e) (i)その場所の外観(申請者の名前を示す看板(該当する場合)や住所を示す標識(可能な場合))および(ii)内部の受付や仕事場の写真1枚以上を撮影しなければならない。

(B) 事業の実施場所が、申請者もしくは登録簿の法人設立管轄と同一の国でない申請者の場合、シマンテックは、申請者の住所、事業の実施場所を含む弁護士意見書を要求する。

11.4.2 申請者の事業所の電話番号

申請者の物理的存在および事業の存在をさらに検証し、他の検証要件の確認を支援するために、シマンテックは申請者が提示した電話番号が申請者の事業所の代表番号であることを検証する。同一の住所の親会社もしくは子会社のリストは、受入れられる。

シマンテックは、事業所の電話番号について、認証された弁護士意見書や会計士の意見を要求する。それらの法的な効力を持つ意見書が無い場合、シマンテックは、申請者の電話番号を以下の方法で検証する。

(A) 申請者が提示した電話番号が、申請者の検証済み事業所住所の電話番号として、該当する電話会社提供の記録もしくは QIIS または QGITS の1つ以上のリストに掲載されていることを確認する。

(B) 訪問中に、訪問を行う人物は、申請者または親/子会社の代表電話番号に電話をかけ、その電話番号に電話することによって申請者に通じると合理的に判断するに足る十分な応答を得ることによって、申請者の電話番号を確認する。

行政機関の場合、シマンテックは、申請者の法的管轄地のQGISに記載される電話番号に依拠することができる。

以降のセクション11.8.1 にあるように、シマンテックは、申請者の電話番号に電話をかけて、その電話番号に電話することによって申請者に通じると合理的に判断するに足る十分な応答を得ることによって、申請者の電話番号を確認する。

11.5 申請者の事業の存在の検証

法人設立/登録機関の記録が示す申請者の設立日が3年未満で、かつ申請者がQIISもしくはQGTISの情報に含まれない場合、シマンテックは、申請者が確実に事業を行っていることを確認する。申請者が、シマンテックが3年以上継続的に存在していることを審査している Entity の子会社もしくは関連会社である場合、シマンテックは親会社もしくはパートナー企業の存在検証結果を、申請者の事業の検証結果として依拠することができる。

有効な金融機関の活動要求払預金口座のに対する弁護士もしくは会計士意見書がない場合、シマンテックは、以下のうち一つの方法で申請者の運営状況を確認する。

(1) 現場を訪問し確認がとれること

(2)申請者による有効な活動要求払預金口座であるかどうかを、金融機関に直接文書で確認する。

11.6 申請者のドメイン名の検証

シマンテックは、EV 証明書中に申請者のドメイン名の記載があることを検証し、以下の事項を満たす。

(1) ドメイン名がICANN認定の登録機関または、IANAがリストしたレジストリに登録されていること。

(2) WHOISデータベース内のドメイン登録情報が公開され、その組織の名前、住所、管理者の連絡先が表示されていること。
政府機関の申請者においては、シマンテックは、QGISにある申請者の支配するドメイン名があることでドメイン名を信頼する。

(3) 申請者が、そのドメイン名の登録所有者であること。またはそのドメイン名の登録所有者からそのドメイン名の排他的使用権を付与されていること。

(4) 申請者がそのドメイン名の登録または排他的使用権を認識していること。

シマンテックは、インターネットで、申請者が提示したドメイン名のWHOIS照会を行い、そのドメイン名が申請者に対して登録されていることを確認する。WHOISのレコードが他のものを指している場合には、シマンテックは、申請者に申請者がドメインの所有者であるようにWHOISのレコードを更新するよう要求する。ドメインの所有者は、申請者の親会社もしくは子会社であるか、申請者の登録された商標であることで、申請者が、ドメインの所有者であることが確認される。

申請者が登録所有者でない、もしくは、ドメインの登録情報がWHOISから得られない場合には、シマンテックは、ドメインの登録所有者から申請者が要求されたFQDNの排他的使用権を認められていることの確認を得なければならない。このような状況下で、シマンテックは、以下のいずれかの方法を用いて、ドメイン名使用に関する申請者の排他的使用権を確認する。

(A) 申請者がインターネット上で自身を識別するためにそのドメイン名を使用する排他的権利を有するという旨を検証済み弁護士意見書に記載する。または、

(B) 契約書署名者または証明書承認者が相互に合意した契約で明示的に権限を付与されてい

る場合は、確認されたドメイン名を申請者が支配していることを示すことにより確認する。

ドメインの登録所有者に連絡できない場合は、シマンテックは以下の処置を講じなければならない。;

- 申請者がインターネット上で自身を識別するためにそのドメイン名を使用する排他的権利を有するという旨を検証済み弁護士意見書に記載する。かつ
- 契約書署名者または証明書承認者が相互に合意した契約で明示的に権限を付与されている場合は、それによる表明に加えて、申請者のFQDNを含むURIで識別できるウェブページで情報修正を実施してオンラインで見せるという、確認されたドメイン名を申請者が支配していることを示すことにより確認する。

シマンテックは、申請者が、ドメイン名に対する排他的使用権もしくは所有権を持っていることを、申請責任者に直接確認する。

11.7 契約書署名者および証明書承認者の名前、肩書、権限の検証

11.7.1 審査の要件

シマンテックは、契約書署名者と証明書承認者のどちらについても、以下を検証しなければならない。

(1) 名前、役職、代理権
CAは、契約書署名者および証明書承認者(該当する場合)の名前、役職を検証する。彼らが申請者の代理人であるという事実についても同様である。

(2) 契約書署名者の権限の付与
シマンテックは、契約書署名者が申請者の代理で1人以上の証明書承認者を指定する契約を含め、申請者の代理で利用規約(およびその他の関連する契約上の義務)契約を締結する権限を申請者から明示的に付与されていることを、契約書署名者以外の情報源によって検証する(「署名権限」)。

(3) EV証明書承認者の権限の付与
シマンテックは、証明書承認者以外の情報源により、証明書承認者が、EV 証明書要求を作成した時点において、申請者から明示的に以下の権限を付与されていることを検証する(「EV権限」)。

(a) 申請者の代理でEV 証明書申請を提出する権限、および、該当する場合は、申請者の代理でEV 証明書申請を提出する権限を証明書申請者に付与する権限。および、

(b) EV 証明書発行のためにシマンテックが申請者に要求した情報を提供する権限、および、該当する場合は、EV 証明書発行のためにシマンテックが申請者に要求した情報を提供する権限を証明書申請者に付与する権限。および、

(c) 証明書申請者が提出したEV 証明書申請を承認する権限。

契約書署名者と証明書承認者が同一人物である場合、契約書署名者として許可されていれば、証明書の承認者として許可されていることになる。

証明書承認者が、契約書署名者と異なる場合には、シマンテックは、名前、役職、代理権(必要な場合)、契約書署名者の許可を伴う証明書承認者の許可を確認する。

11.7.2 名前、肩書、代理人の検証

シマンテックは、証明書承認者の権限と契約書署名者雇用について以下の確認をする。

(A) 申請者の人事部に(ガイドラインに従って検証した申請者の事業所の電話番号や住所を使用して)電話または郵便で連絡し、契約書署名者および証明書承認者(あるいは適宜、契約書署名者または証明書承認者)が従業員であることの確認を得る。または、

(B) 契約書署名者および証明書承認者が申請者の従業員であること、または、別の方法で申請者の代理人に指定されていることを検証する、申請に直接携わらない者への確認を得る。

11.7.3 権威の審査

シマンテックは、以下に示す方法の一つを用い契約書署名者の権威を確認する。

(1) 取締役会決議
契約書署名者の署名権限および証明書承認者のEV権限(あるいは、契約書署名者の署名権限または証明書承認者のEV権限)は、その人物がかかる署名権限を付与されたことを確認できる、正式に認められた取締役会決議に依拠して検証可能である。ただし、かかる決議が、(1)適切な幹部職(書記官など)によって証明されており、(2)その証明書にかかる人物の有効な署名があることおよびかかる人物がかかる証明書を発行する必要権限を有することをシマンテックが検証できる場合に限る。

(2) 申請に直接携わらない者への確認
契約書署名者の署名権限および証明書承認者のEV権限(あるいは、契約書署名者の署名権限または証明書承認者のEV権限)は、申請に直接携わらない者への確認を得ることによって確認する。

(3) CAと申請者間の契約
証明書承認者のEV権限は、かかるEV権限を有する証明書承認者を指定するシマンテックと申請者間の契約に依拠して検証できる。ただし、契約書署名者がその契約書に署名し、契約書署名者の代理権および署名権限が検証されている場合に限る。

(4) 事前同等権限
契約書署名者の署名権限および証明書承認者のEV権限(あるいは、契約書署名者の署名権限または証明書承認者のEV権限)は、事前同等権限の証明に依拠して検証できる。

契約書署名者が、シマンテックと申請者の間で締結された法的に有効で強制力のある印鑑または手書きの署名がなされた拘束力を持つ契約を履行した場合で、なおかつ同契約がEV 証明書の申請の90日前までに履行された場合に限り、契約書署名者の署名権限の確認または検証については、契約書署名者の事前同等権限に依拠できる。

シマンテックは、事前の契約を正しく特定し、EV申請に関連付けできるよう、事前の契約について詳細を記録しなければならない。 当該の詳細には、以下の項目が含まれる。

1.契約の表題と契約書署名者の署名の日付
2. 契約の参照番号
3. ファイルの保管場所

証明書承認者が以下のいずれかに該当する場合には、証明書承認者のEV権限の確認または検

証については、証明書承認者の事前同等権限に依拠できる。

(1) シマンテックまたは親会社/子会社と締結した契約において、申請者のエンタープライズRAの役割を果たした(または現在も果たしている)。
(2) 申請者が管理する公開サーバで現在使用されている、当該CAが発行した1つ以上のSSLサーバ証明書の承認に参加した。この場合、シマンテックまたは親会社もしくは子会社(またはその両方)は、あらかじめ承認された電話番号を用いて証明書承認者に事前に電話で連絡するか、証明書要求を承認する旨の署名済みかつ認証済みの書簡を事前に受理していなければならない。

11.7.4 事前に権限を付与された証明書承認者

シマンテックおよび申請者が、シマンテックが以下を完了した後、(例えば、マネージド PKI for SSL アカウントを用いて)将来的に複数のEV 証明書要求の提出を計画している場合。

- 契約書署名者の名前および肩書きと、その人物が申請者の従業員または代理人であることを検証した。
- 本 Appendix のセクション 11.7.3 に記載の手順のいずれかに従って、かかる契約書署名者の署名権限を検証した。

申請者が、申請者の代理である契約書署名者が署名した書面による契約を締結し、この契約によって、指定の期間中、申請者の代理で提出されかかる証明書承認者が発信したか他の方法で承認したと正しく認証された将来の全EV 証明書申請に対してEV権限を行使する権限を、申請者がかかる契約で指定された1 人以上の証明書承認者に明示的に付与することができる。

申請者が、かかるEV権限が取り消されるまで、かかる証明書承認者の要求に応じて発行された全EV 証明書またはかかる証明書承認者が承認した全EV 証明書の利用規約に定めた義務を負う旨を規定しなければならず、(i)EV 証明書要求承認時の証明書承認者の認証 (ii)証明書承認者の権限の定期的な再確認 (iii)申請者がシマンテックの証明書承認者のEV権限失効を通知するセキュアな手順、 (iv)合理的に必要と考えられるその他の適切な予防措置に関する相互に合意した条項を含めなければならない。

11.8 利用規約および EV 証明書要求への署名の検証

リテールの EV 証明書に対して、各 EV 証明書要求の利用規約は、申請者に権限を付与された契約書署名者によって署名されなければならない。証明書要求者が権限を付与された証明書承認者もしくは権限を付与された契約書署名者でない場合、権限を付与された証明書承認者もしくは契約書署名者は別個にその EV 証明書申請を承認しなければならない。承認者、契約者いずれの署名も、申請者を各文書の条件で拘束する法的に有効で強制力のある印または直筆の署名(書面による利用規約および EV 証明書要求の場合)、あるいは、法的に有効で強制力のある電子署名(電子的な利用規約および EV 証明書要求の場合)でなければならない。

11.8.1 検証要件

リテールEV 証明書が発行される前に、シマンテックは、該当する文書の署名者として指名された人物が実際に申請者の代理で署名を行った人物であることを申請時認証された電話番号を用いて契約書署名者に本当に申請書類に署名したことを尋ねることで、利用規約の契約書署名者の署名および各EV 証明書要求の証明書要求者の署名を認証しなければならない。

EV 証明書を発行するためのマネージド PKI for SSL アカウントが承認される前に、シマンテックは、

該当する文書の署名者として指名された人物が実際に申請者の代理で署名を行った人物であることを申請時認証された電話番号を用いて契約書署名者に本当に申請書類に署名したことを尋ねることで、利用規約の契約書署名者、企業契約の署名およびEV 証明書要求の証明書要求者の署名を認証しなければならない。その後、これらEV手続き期間中に申請によって許可された証明書承認者は、これらの手続き、ガイドラインを守り、契約書署名者の追加の署名無しで証明書要求を許可できる。

マネージド PKI for SSLアカウントへEV用ドメインが追加される前に、シマンテックは申請者もしくは、証明書署名者に直接、ドメインの権限に関する知識を持っていることを確認する。

11.8.2 署名の検証

先に記述した電話での応答ができない場合、シマンテックは、契約書署名者の署名の確信を得るために以下の手段を用いる。

(1) ガイドラインに準拠する独立した方法で検証した、申請者または登録機関の住所で証明書要求者または契約書署名者に郵便を送付し、その人物を自称する人物から電話または郵便で申請者の代理で該当する文書に署名したことを確認する返答を得る方法。

(2) 署名前に署名者を識別するセキュアなログインプロセスや適切に検証された証明書を参照するデジタル署名など、セキュアな方法で名前および肩書きを証明する署名プロセスの使用。

(3) 公証人による公証:ただし、かかる公証人が証明書申請者または契約書署名者の管轄地の法的に資格のある公証人であることをシマンテックが独自に検証できる場合に限る。

11.9 EV 証明書要求の承認の検証

シマンテックは、要求された EV 証明書発行前に、許可された証明書発行者が、EV 証明書要求を確認し承認したことを確認する。シマンテックは、証明書承認者に電話かメール(確認された電話番号かアドレス)で連絡し、リテール EV 証明書要求の承認について、口頭もしくは書面で取得した証明書承認者による確認により、EV 証明書要求を承認する。

マネージド PKI for SSL アカウントを経由して発行する EV 証明書の場合には、申請の承認は、証明書承認者が電子証明書を使用してアカウントにログインすることにより行う。

11.10 特定の情報源の検証

11.10.1 検証済み弁護士意見書

シマンテックは、提出された弁護士意見書に依拠する前に、かかる弁護士意見書が以下の要件を充足することを検証する(「検証済み弁護士意見書」)。

(A) 作成者の地位
シマンテックは、弁護士意見書の作成者が申請者に雇われて申請者の代理となる独立した法律専門家(または申請者雇用の社内の法律専門家)(法律専門家)で以下の条件のいずれかを充足することを検証する。

(i) 申請者の法人設立の管轄または申請者の保有する事業所や施設の管轄の国で弁護士を開業する免許を有する弁護士(あるいは、法務官、法廷弁護士またはこれに相当するもの)。シマンテックは、弁護士の資格について直接確認する。

(ii) International Union of Latin Notariesの会員で、申請者の法人設立の管轄または申請者が保有する任意の事業所や施設の管轄の国で業務を行う免許を有する公証人(かつ、かかる管轄地がInternational Union of Latin Notariesの役割を認識していること)。

(B) 意見の根拠

シマンテックは、法律専門家が申請者の代理で行動していること、また検証済み弁護士意見書の結論が、関連する事実に対する法律専門家の規定の知識と、法律専門家としての専門的判断および専門知識の行使に基づくことを検証しなければならない。

(C) 真正性

シマンテックは、検証済み弁護士意見書の真正性を、法律専門家の登録または認可を担当する機関に登録された法律専門家の住所、電話番号、ファクシミリ番号、(利用できる場合は)電子メールアドレス宛に法律専門家に電話をかけるか弁護士意見書のコピーを返送し、法律専門家または法律専門家の助手からその弁護士意見書が真正である旨の確認を得ることで確認しなければならない。

電子署名である意見書の場合には、書類の信憑性と署名確認の方法でシマンテックによりセクション11.10.1(A)により確認され、信憑性に関するそれ以上の要求はされない。

11.10.2 検証済み会計士意見書

シマンテックは、提出された会計士意見書に依拠する前に、かかる会計士意見書が以下の要件を充足することを検証する(「検証済み会計士意見書」)。

(A) 作成者の地位

会計士意見書が、公認会計士、勅許会計士または、申請者の法人設立管轄または申請者が保有する任意の事業所や施設の管轄の国で会計を行うことを国際会計士連盟(IFAC)から全員一致で許可された公認会計士に相当する資格を持つ独立した会計士によるものであることを確認するために、シマンテックは、管轄の地域でかかる会計士の登録または認可を行った機関に会計士について直接確認する。

(B) 意見の根拠

会計士が申請者の代理で行動し、検証済み会計士意見書の結論が、関連する事実に対する会計士の規定の知識と、会計士としての専門的判断および専門知識の行使に基づくことを検証しなければならない。

(C) 真正性

シマンテックは、会計士意見書の真正性を確認するために、かかる会計士の登録または認可を担当する機関に登録された会計士の住所、電話番号、ファクシミリ番号、(利用できる場合は)電子メールアドレス宛に会計士に電話をかけるか会計士意見書のコピーを返送し、会計士または会計士の助手からその会計士意見書が真正である旨の確認を得なければならない。

電子署名である意見書の場合には、書類の信憑性と署名確認の方法でシマンテックによりセクション11.10.2 (A)により確認され、信憑性に関するそれ以上の要求はされない。

11.10.3 対面認証

対面確認の前に、シマンテックは、審査を行う第三者機関が以下の要件を満たすことを確認する。

(A) 審査を行う第三者機関の資格
シマンテックは、審査を行う第三者機関が、法的に認められた公証役場、(申請者の管轄法において法的に同等の)公証役場、もしくはその居住地において弁護士、会計士であることを、管轄の地域でかかる審査機関の登録または認可を行った機関に直接確認することにより、独自に認証を行う。

(B) 関連する資料の管理
シマンテックは、審査を行う第三者機関が、認証される個人との対面確認の中で確認資料を精査することを確認する。審査を行う第三者機関は、認証局に提出する確認資料が認証される個人との対面の中で作られ、得たことを証明しなければならない。

(C) 公証人の確認
審査を行う第三者機関が、ラテン系の公証人でない場合、シマンテックは、審査を行う第三者機関への電話確認と本人もしくは対面面談に同席したアシスタントの確認書の取得をもって、宣誓書と確認資料の信憑性を確認する。シマンテックは、この認証手続きに関して、単に審査を行う第三者機関からのセルフレポートの情報をもって信頼することがある。

この場合、宣誓書は、書類の信憑性を確認する方法と同じく電子署名に限られ、シマンテックによって行われる署名の確認はセクション 11.10.3 (A)の方法を用い、信憑性の確認に関するそれ以上の要求は行われない。

11.10.4 申請に直接携わらない者への確認

「申請に直接携わらない者への確認」は、以下の条件を満たす、特定の事実の確認(ドメイン名の排他的支配の認識、契約書署名者または証明書承認者の従業員または代理人の地位の確認、証明書承認者のEV権限の確認など)である。

(i) かかる事実を確認する適切な権限を有し(「確認者」)、かかる事実を確認したことを表明する、申請者が雇用する従業員(照会の対象者以外の人物)からシマンテックが受領したもの。

(ii) 確認元を認証および検証できる方法でシマンテックが受領したもの。および、

(iii) 申請者を拘束するもの。

申請に直接携わらない者への確認は、以下の手順で取得することができる。

(1) 確認要求
シマンテックは、以下のような、問題となっている特定の事実の検証または確認を要求する適切な手段を実施しなければならない(「確認要求」)。

(A) 受取人:確認要求の宛先は以下でなければならない。

(i) 確認者(書記官、社長、CEO、CFO、COO、CIO、CSO、取締役など)の資格を有し、現行の公認の行政機関の情報源(SECファイルなど)、公認の独立情報源、検証済み弁護士意見書、検証済み会計士意見書内の名前および肩書によって特定される人物、または、

(ii) 法人設立もしくは登記の公式記録に記載された、適切な確認者に転送される旨の記述

が付されている、管轄区域に登録されている申請者の代理人または事業所

(iii)(申請者の事業所所在地として認証された電話番号もしくは住所への)申請者の人事部への電話もしくは郵便を用い、契約書署名者もしくは証明書承認者の直接の上長として確認される個人。

(B) 連絡手段

確認要求は、確認者に届くと合理的に考えられる方法で確認者宛に送付しなければならない。確認要求は以下の方法により行う。

(i) 郵便による確認

以下の住所の確認者宛の郵便によって:

(a) 要件に従ってシマンテックが検証した申請者の事業所所在地の住所、または

(b) 現行の政府が運営する公認独立情報源(SECファイルなど)、QIIS、QGTIS、検証済み弁護士意見書、検証済み会計士意見書などに明記された、かかる確認者の勤務先の住所、または、

(c) 法人設立管轄地の公式記録に記載された、申請者の登録代理人または登録事業所の住所、または、

(ii) 電子メールによる確認

現行のQGIS、QIIS、QGTIS、検証済み弁護士意見書、検証済み会計士意見書などに明記された、確認者の勤務先電子メールアドレスへの電子メールによって、または、

(iii) 電話による確認

(ガイドラインに従って検証された)申請者の事業所所在地の代表番号に電話をかけて確認者を呼び出すことによって確認者と連絡でき、電話を受けた人物が確認者であると認める場合は、確認者に電話をかけることによって、または、

(iv) ファクシミリによる確認

事業所所在地宛で確認者にファクシミリを送信することによって。ファクシミリの番号は現行のQGIS、QIIS、検証済み弁護士意見書、検証済み会計士意見書などに記載されていなければならない。表紙は確認者宛であることが明確でなければならない。

(2) 確認の返答

シマンテックは、確認要求に対して、問題となっている特定の事実を確認する旨の返答を確認者から得なければならない。かかる返答は、確認者が確認要求に答えて提出したものであることをシマンテックが検証できる限り、電話、電子メール、郵便のいずれを使用して送付することもできる。

シマンテックは、確認者にその連絡先情報(電子メールアドレス、電話番号、ファクシミリ番号)を確認することで、検証された確認者に依拠することができる。以下の場合、シマンテックは、次にこの確認者に連絡を取る際に、この確認済みの連絡先情報に依拠することができる。

1. 電子メールアドレスのドメインが申請者により所有されており、そのドメインが確認者自身の電子メールアドレスのものであり、グループエイリアスの電子メールアドレスではないこと。

2. 確認者の電話番号/ファクシミリ番号が当該組織の電話システムの一部であり、個人の電話番号ではないとシマンテックによって確認されていること。

11.10.5 公認独立情報源(QIIS)

シマンテックによってEV 証明書申請情報の検証に使用される情報である商用の情報源は、ガイドラインの要件に適合するデータベースを使用する。

11.10.6 公認の行政機関データベース(QGIS)

シマンテックによってEV 証明書申請情報の検証に使用される情報である公認の行政機関の情報源は、ガイドラインの要件に適合するデータベースを使用する。シマンテックは、行政機関から直接情報を得るような第三者機関を、行政機関情報を得るために使用する場合がある。

11.10.7 Qualified Government Tax Information Source (QGTIS)

民間組織、企業、個人に関連する税金情報を含む認定された政府の情報ソース(例:米国 における I.R.S.)

11.11 その他の検証の要件

11.11.1 ハイリスクステータス

シマンテックは、ガイドライン基本要件からの補足である本 CPS Appendix Dのセクション 11.5 に従い、ハイリスクな要求を処理する。

11.11.2 拒否リストおよびその他の法的ブラックリスト

シマンテックは、申請者のEV証明書を発行する前に、申請者、契約書署名者、もしくは証明書承認者、または申請者の法人設立/登録管轄地もしくは事業所所在地のいずれかが以下の事項に該当するか否かを、関連する政府機関から明確にするための適切な手順を講じる。:

(a) 申請者、契約書署名者または証明書承認者が、行政機関の拒否リスト、重大な性犯罪者リスト、その他シマンテックおよび米国シマンテックの業務運営管轄国の法律で取引を禁止された組織または人物のリストに記載されているかどうか、および

(b) 申請者の法人設立/登録管轄地または事業所所在地がシマンテックおよび米国シマンテックの管轄地の法律によって取引を禁じられた国にあるかどうか。

シマンテックは、EV 証明書の申請において、以下のようなリストや規制の確認を行う。

(A)シマンテックは、合理的な手段を講じて、下記に相当するアメリカ政府の禁輸リストや輸出規制と照合して検証しなければならない。

(i) BIS禁輸対象者リスト
(ii) BIS禁輸対象組織リスト
(iii) 米国財務省の特定国籍業者リスト
(iv) アメリカ政府の輸出規制

(B)米国以外での国での発行に関しては、かかる国での上記に相当する禁止リストにより合理的

な検証を行う。

11.11.3 親会社/子会社/関連会社との関係

シマンテックは、本 Appendix セクション 11.4.1、11.4.2、11.5、ならびに 11.6に規定のとおり、申請者の親会社、子会社もしくは関連会社の情報を基に審査を行う。かかる申請者との関係は、以下の情報を用いて審査をしなければならない;

1) QIIS もしくは QGIS
申請者と親会社、子会社もしくは関連会社との関係は、QIIS もしくはQGIS により確認される。もしくは
2) 親会社、子会社もしくは関連会社への独立した確認
シマンテックは、申請者と親会社、子会社もしくは関連会社との関係を、適切な親会社、子会社もしくは関連会社への独立した確認(本 Appendix セクション 11.10.4 参照)により審査することがある。もしくは
3) CAと親会社、子会社もしくは関連会社との契約
シマンテックは、申請者と親会社、子会社もしくは関連会社との関係を、CAと申請者と親会社、子会社もしくは関連会社との、証明書承認者のかかるEV権限を明示する契約に依拠して審査することがある。かかる契約は契約書署名者により署名されること、および、代理人と契約書署名者の署名権限が確認済みであることが記載されていることを条件とする。もしくは
4) 弁護士意見書
シマンテックは、申請者と親会社、子会社もしくは関連会社との関係を、検証済みの弁護士意見書(本 Appendix セクション 11.10.1 参照)に依拠して審査することがある。もしくは
5) 会計士意見書
シマンテックは、申請者と親会社、子会社もしくは関連会社との関係を、検証済みの会計士意見書(本 Appendix セクション 11.10.2 参照)に依拠して審査することがある。もしくは
6) 取締役会決議
シマンテックは、申請者と子会社との関係を、子会社もしくは申請者の設立を承認する正当な取締役会決議に依拠して審査することがある。かかる決議が、(i)適切な幹部職(書記官など)によって証明されており、(ii)その証明書にかかる人物の有効な署名があることおよびかかる人物がかかる証明書を発行する必要権限を有することをシマンテックが検証できることを条件とする。

11.12 最終的な相互確認およびデューデリジェンス

全ての確認作業が完了した後で、資料の確認作業を実施していないEVの認証担当者は、契約書署名者に電話確認を実施し、終了後、証明書を発行する。

これは、マネージド PKI for SSL 顧客に対しては行われない。

11.13 既存文書の再利用の要件

11.13.1 検証済みデータの再利用

(1) EV証明書の発行に使用された検証済みデータの(再検証実施前の)有効期間の上限は以下のとおりである。

- 法的存在とアイデンティティ — 13か月;
- 屋号 — 13か月;
- 事業所の住所 — 13か月。ただし、訪問確認が行われていた場合でも以後はQIISにより情報の更新を確認する;

- 事業所の電話番号 — 13か月;
- 銀行口座の確認 — 13か月;
- ドメイン名 — 13か月;
- 証明書承認者のアイデンティティと権限の確認 — 13か月。ただし、異なる期間を特定し、その期間に従う旨の契約がシマンテックと申請者の間で締結されていない場合。例えば、そのような契約では、役割が失効されるまで、もしくは同意書が期限切れもしくは破棄されるまでの恒久的な役割任命を許可するように期間が指定されることがある。

(2) シマンテックがEV 証明書要求の検証に使用する情報の有効期間は、情報取得日(確認電話の日付など)と情報源による情報最終更新日のうち先の方を基準にして、ガイドラインの最長有効期限に定める情報の最長有効期間を超えてはならない(たとえば、シマンテックが7月1日にオンラインデータベースにアクセスしたがベンダによる掲載データの最終更新が2月1日であった場合は、情報の日付は2月1日とみなす)。

(3) シマンテックは前項の記載の有効期間および更新にかかわる要件に従って、単一のEV証明書要求に基づいて、同じサブジェクトを持つ複数のEV証明書を発行する場合がある。シマンテックが発行する全EV証明書は、現行の有効なEV証明書要求と申請権限者が署名した加入者契約もしくは適切な申請権限者が同意した利用規約に基づくものでなければならない。

情報が期限切れである場合は、CAは、ガイドラインが要求する検証プロセスを再実行しなければならない。

11.13.2 既存の加入者の検証

すでにシマンテックの顧客となっている申請者によりEV証明書要求がなされた場合、シマンテックは、その要求が申請者に承認されたものであること、および、EV証明書に記載される情報が最新で有効なものであるかを確実にするために、本 CPS で要求されるすべての認証と審査を行う。

11.13.3 例外

(既存の情報と文書の利用およびそれらの情報の有効な期間の上限についての)セクション 11.13.1 および 11.13.2 に規定した要件にもかかわらず、シマンテックは、以前に発行された EV 証明書の更新における認証と審査を行う際に、以下を実施することがある。

(1) 前回実施した以下の内容の認証と審査に依拠する;

(A) 事業体の長となる個人が前回発行されたEV証明書の検証時と同じ人物の場合、ガイドラインのセクション 112.2(4) に規定される、事業体の長となる個人。もしくは

(B) セクション 11.4.1 に規定される、申請者の事業所。もしくは

(C) セクション 11.4.2で要求される、申請者の事業所の電話番号の確認。ただし、申請者がその電話番号で連絡可能であることを確認できるよう、セクション 11.4.2(B) で要求される電話による確認は、必ず実施されなければならない。もしくは

(D) セクション 11.5 に規定される、申請者の事業運営。もしくは

(E) セクション 11.7 に規定される、契約書署名者、証明書承認者もしくは証明書要求者の名前、肩書および権限。ただし、シマンテックと申請者の間で、契約書署名者、証明書承認者および証明書要求者の権限について特別な項目を特定した契約が締結されて

おり、契約の内容が優先する旨が記載されている場合はこの限りでない。もしくは

（F） シマンテックが電子メールによってセクション 11.10.4(1)(B)(ii)に規定される独立した確認を前回の検証時に行った場合、その時に使用された電子メールアドレス

（2） 以下による前回の弁護士/会計士意見書に依拠する;

（A） ガイドラインのセクション 11.6.2(2)A(i) および 11.6.2(2)B(i) に規定される、特定のドメインの使用に関する申請者の排他的な権利。シマンテックが以下のいずれかを審査していることが条件となる;
(i) WHOIS検索結果が、シマンテックが前回弁護士意見書を受領した際に確認したものと同じ登録者を示す。もしくは
(ii) ガイドラインのセクション 11.6.2(2)B(ii) に規定される内容の実演により、申請者がドメインを設立している。

（B） ガイドラインのセクション 11.6.2(3) に規定される、申請者がそのドメイン名の排他的使用権を認識していることの検証。

12. ルート CA による証明書発行

米国シマンテックはルートCAの証明書発行に際し、複数名による管理を行う。ルートCAの秘密鍵はEV証明書を署名することには使用されない。

13. 証明書失効およびステータスチェック

EV証明書の失効は、CA/ブラウザフォーラム基本要件からの補足である Appendix D セクション 13 に従い実行される。

シマンテックは EV証明書チェーン用のCRL を、通常のネットワーク状況下でアナログ回線であれば3秒以内にダウンロードできるよう、提供する。

14. 従業員および第三者機関

14.1 信頼性および能力

14.1.1 本人確認および身元審査

本 CPS のセクション 5.2 および 5.3 に記載される手続きに加えて、シマンテックで従業員、代理人、契約社員としてEV 証明書手続きを行う人員は、以下の追加手続きを受ける必要がある。

(A) 人事またはセキュリティに携わる信頼できる人物(公証人などを含む)と対象人物の同席。および、
(B) 一般的な行政機関発行の写真つき身分証明書による検証
（例えば、パスポート、運転免許証など）

14.1.2 トレーニングおよびスキルレベル

シマンテックは、全認証スペシャリストが、基本要件からの補足である Appendix D セクション14.1.2 に記載する EV 証明書認証基準の概要に関する試験に合格することを要求する。

14.1.3 職務の分離

シマンテックは、一名の人員が EV 証明書の発行の際の認証と承認を個別に行うことを確実にするため、本 CPS セクション 5.2.4 に規定する職務の分離を実施する。EV 証明書の申請におけるすべてのプロセスは記録され、監査可能であることとする。

14.2 登録機関および下請け業者への職務の委譲

14.2.1 概要

米国シマンテックの明確な同意のある場合のみ、シマンテックは、ガイドライン要件のすべてまたは一部の履行を登録代理人(登録機関)または下請け業者に委任することができる。ただし、本 Appendixのセクション 11.12 に記載の最終的な相互確認およびデューデリジェンスの要件の履行はこの限りではない。

14.2.2 エンタープライズ RA

シマンテックは、登録機関機能履行の権限、および、最初のEV 証明書に記載のドメインを含む第3ドメインレベル以上のEV 証明書(「企業EV 証明書」としても知られる)を追加発行する権限を、契約により、指定の有効なマネージド PKI for SSL顧客に付与することができる。その場合は、サブジェクトはエンタープライズRAとみなされ、以下が適用される。

(1) いかなるエンタープライズRAも、そのエンタープライズRAとそのエンタープライズRAが所有または直接支配する企業以外のサブジェクトに第3ドメインレベル以上の企業EV 証明書を発行する権限を、シマンテックに付与することはできない。
(2) いかなる場合も、企業EV 証明書のサブジェクトは、ガイドラインに従ってシマンテックが検証した組織でなければならない。
(3) シマンテックは、エンタープライズRAとの契約要件としてこれらの制限を強制し、承認されたマネージド PKI for SSLの管理者によって、エンタープライズRAのコンプライアンスを監視しなければならない。
(4) 本Appendix セクション 11.12 の最終的な相互確認およびデューデリジェンスの要件については、エンタープライズRAがこれを実施することができる。また、
(5) シマンテックおよび米国シマンテックがルートCAの秘密鍵もしくは下位CAの秘密鍵の管理を維持できない場合、エンタープライズRAは、セクション 17.1 に従って監査を受けなければならない。

14.2.3 準拠義務

シマンテックは、シマンテック自体が要求された、ガイドラインに定められた適用しうる要件への準拠および履行を、契約により、かかる登録機関、下請け業者、エンタープライズRAに義務付けなければならない。

14.2.4 責任の割り当て

基本要件からの補足である Appendix D セクション14.2.3 に規定する。

15. データレコード

EV 証明書のため、データレコードは、基本要件からの補足である Appendix D のセクション 15 に規定されるとおり取得され維持される。

16. データセキュリティ

シマンテックのデータのセキュリティについては、基本要件からの補足である Appendix D のセクション 16 に規定される。

17. 監査

17.1 年次の第三者監査

シマンテックは、年次の以下の監査を受ける
(i) WebTrust Program for CAs 監査
(ii) WebTrust EV Program 監査
(iii) (i)もしくは(ii)と同等の、CA/ブラウザフォーラムーラムにより承認された監査

また、Issuing CAとして米国シマンテックは、シマンテックによって処理された証明書を含んだ年次の WebTrust Program for CAs 監査を受ける。

このような監査は、シマンテックにより直接実施されるか、またはRAやサブコントラクタに委譲されるかに関わらず、CA/ブラウザフォーラムのガイドライン下のCAの義務を全て網羅する。

17.2 監査期間

シマンテックおよび米国シマンテックは、セクション17.1に規定のとおり、年次で監査を受ける。

17.3 監査記録

本 CPS セクション 8.6 に規定のとおり、本監査報告書は、シマンテック、米国シマンテックによって公開される。

17.4 発行開始前の準備状況の監査

シマンテックがEV 証明書を発行する前に、シマンテックおよび米国シマンテックは、WebTrust EV Programに照らした期限内準備完了評価監査に合格しなければならない。

17.5 定期的な自主監査

シマンテックは、EV 証明書発行期間中は、最後のサンプル採取直後から開始される期間に発行した EV 証明書のうちランダムに選択した 3%以上のサンプルを使用して、継続的に自主監査を行うことによって、サービスの質を厳格に管理しなければならない。

17.6 監査役の資格

本 CPS セクション 8.2 に規定したように、ガイドラインが要求する全監査は、以下の条件を満たす資格のある監査人が実行しなければならない。

(1) PKI、情報セキュリティツールおよび技術、情報技術およびセキュリティの監査、第三者認証機能の審査に熟達し、現在WebTrust for CA auditsおよびWebTrust EV Program auditsまたはこれに代わるCA/ブラウザフォーラムが承認した同等の監査を実行する免許を有する独立した会計事務所であること。および、

(2) 米国公認会計士協会(AICPA)の会員またはアメリカ以外のこれに相当するもの、すなわち、一定の技術、同業者による評価などの品質保証手段、能力試験、業務へのスタッフの適切な割り当て基準、および職業教育の継続の要求をはじめとする、定義された標準に従って監査が行われることを要求する団体の会員であること。

(3) 補償限度額100万ドル以上の専門職業責任保険/エラーズ&オミッションズ保険に加入していること。

17.7 ルート CA 鍵ペア生成

ガイドライン発表後に生成されるルートCA鍵については、米国シマンテックの資格のある監査人は、プロセスおよび生成される米国シマンテックルート鍵の完全性および秘密性の管理を監視するために、ルート鍵の生成プロセスに立ち会わなければならない。資格のある監査人は、ルート鍵および証明書の生成プロセスにおける米国シマンテックについて以下に示す見解を述べる報告書を発行しなければならない。

(1) CPに記載のルートCA鍵の生成および保護手順、バージョン、日付およびCPS、バージョン、日付を記録したこと。

(2) ルートCAの鍵ペアを生成するために実施する手順の計画書(「ルート鍵生成の手順」)に、適切な詳細手順および管理を含めたこと。

(3) CP/CPSに記載の手順およびルート鍵生成手順に従って、ルートCAを生成および保護することを合理的に保証する効果的な管理を行ったこと。

(4) ルート鍵生成プロセス中、ルート鍵生成手順が要求する全手順を実行したこと。

鍵生成の全プロセスを監査に備えてビデオに記録する。

18. 責任と補償

基本要件からの補足である本CPS Appendix D セクション18 に規定する。

Appendix 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. Root CA Certificates

	アルゴリズムの最低強度
Digest algorithm	SHA-1*, SHA-256, SHA-384 or SHA-512
RSA	2048 bit
ECC	256 or 384 bits

2. Subordinate CA Certificates

	アルゴリズムの最低強度
Digest algorithm	SHA-1*, SHA-256, SHA-384 or SHA-512
RSA	2048 bit
ECC	256 or 384 bits

3. Subscriber Certificates

	アルゴリズムの最低強度
Digest algorithm	SHA-1*, SHA-256, SHA-384 or SHA-512
RSA	2048 bit
ECC	256 or 384 bits

*SHA-1 は、世間一般に使用されているブラウザでSHA-256が、広くサポートされるようになるまでは使用されるべきである。

Appendix B3

EV 証明書で要求される証明書エクステンション

1. Root CA Certificate

ルート証明書は、2006年10月以後に生成され、かつ、X.509 v3でなければならない。

(a) **BasicConstraints**
証明書が、v3で、かつ、2006年10月以降に生成されているならば、本エクステンションはすべての電子署名に使用される有効なCA証明書でCriticalとして設定されなければならない。CAフィールドは、Trueに設定されなければならない。pathLenConstraintは、設定されるべきではない。

(b) **KeyUsage**
証明書が、v3で、かつ、2006年10月以降に生成されているならば、このエクステンションは、Criticalとして設定されなければならない。CertSign、cRLSignのビットが、設定されなければならない。その他のビットは、設定されるべきではない。

(c) **certificatePolicies**
本エクステンションは設定されるべきではない。

(d) **extendedKeyUsage**
本エクステンションは使用されない。

他のフィールドとエクステンションは、RFC5280に従う。

2. Subordinate CA Certificate

(a) **CertificatePolicies**
有効にしなければならない、かつ、Criticalに設定されてはならない。もし、証明書が、米国シマンテックのコントロール下にない下位CAに発行されたならば、policy identifiersは、米国シマンテックのEVポリシーに対する識別をもたなければならない。

CertificatePolicies:policyIdentifier (Required)
- (ルートCAによってコントロールされる下位CAならば) anyPolicy
- (ルートCAによってコントロールされない下位CAならば) explicit EV policy OID(s)

次のフィールドは、米国シマンテックにコントロールされない場合には有効とされてはならない。
CertificatePolicies: policyQualifiers: policyQualifierId
- id-qt 2 [RFC 5280]

CertificatePolicies: policyQualifiers: qualifier
- CPSへのURI

(b) **cRLDistributionPoint**
有効にされなければならない、かつ、Criticalに設定されてはならない。米国シマンテックのCRLサービスへのHTTP URLを含む。

(c) **authorityInformationAccess**
有効にされるべきであり、かつ、Criticalに設定されてはならない。米国シマンテックのOCSPレ

スポンダーへのHTTP URLを含む(accessMethod = 1.3.6.1.5.5.7.48.1)。HTTP accessMethodは、米国シマンテックの証明書に含まれる場合がある(accessMethod = 1.3.6.1.5.5.7.48.2)。

(d) **basicConstraints**
すべての証明書の電子署名に使用される公開鍵を含む証明書中で、このエクステンションは、Criticalと設定されなければならない。CA フィールドは、Trueに設定されなければならない。pathLenConstraint フィールドは、有効にされる場合がある。

(e) **keyUsage**
このエクステンションは有効とされ、かつ、Criticalに設定されなければならない。CertSign、cRLSignのビットが、有効とされなければならない。その他のビットに関しては、設定してはならない。

他のフィールドとエクステンションに関しては、RFC5280に従う。

3. Subscriber Certificate

(a) **certificatePolicies**
有効とされ、かつ、Criticalに設定されてはならない。policyIdentifiersは、米国シマンテックEVポリシーへの識別子を含まなければならない。

certificatePolicies:policyIdentifier (Required)
- EV policy OID

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

certificatePolicies:policyQualifiers:qualifier (Required)
- CPSへのURI

(b) **cRLDistributionPoint**
有効とされ、かつ、Criticalに設定されてはならない。有効であれば、米国シマンテックのCRLサービスのHTTP URLを含む。

(c) **authorityInformationAccess**
有効とされるべきであり、かつ、Criticalに設定されてはならない。米国シマンテックのOCSPレスポンダーは、HTTP URLを含むべきである (accessMethod = 1.3.6.1.5.5.7.48.1)。HTTP accessMethodは、STN証明書に含まれる場合がある (accessMethod = 1.3.6.1.5.5.7.48.2)。

(d) **basicConstraints** (optional)
存在するならば、CAフィールドは、falseに設定されなければならない。

(e) **keyUsage** (optional)
存在するならば、CertSign、cRLSignのビットは、設定されてはならない。

(f) **extKeyUsage**
id-kp-serverAuth [RFC5280] または id-kp-clientAuth [RFC5280] のいずれか、もしくは両方が設定されなければならない。その他の値は、設定されてはならない。

(g) **SubjectAltName**
RFC 5280に従って設定され、かつ、Criticalに設定されてはならない。

他のフィールドとエクステンションは、RFC 5280に従う。

Appendix B4

外国の組織名称ガイドライン

注意:本 Appendix 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 申請にのみ適用される。特定の国々に関する更に詳細な情報が将来付け加えられる可能性がある。

1. ラテン名ではない組織名称
EV 申請者の組織名称が QGIS にラテン文字で登録されず申請者の国の文字で登録されており、登録がガイドラインに従い QGIS で確認ができた場合、CA はラテン文字の組織名称を EV 証明書に入れることができる。この様な場合、本 Appendix に示す以下の手順に従わなければならない。

2. ローマ字名称
登録名称の翻字/ローマ字名を入れる場合、ローマ字名は、申請者の登録管轄地の政府機関によって正式に認められたシステムを使用して CA によって確認されなければならない。

もしシマンテックが申請者の登録管轄地の政府機関によって正式に認められたシステムを使用した翻字/ローマ字名に依拠できない場合は、以下の順でいずれかの方法に依拠しなければならない。

(a) 国際標準(ISO)によって認められたシステム
(b) 国連によって認められたシステム
(c) 弁護士意見書による登録名のローマ字名称確認

3. 英語名称
登録名称のローマ字名ではないラテン文字名を入れる場合、シマンテックはラテン文字名を審査しなければならない:

(a) 組織登録の一部である定款(または同等の文書)に含まれている
(b) 納税申告の申請者が認識している名称が申請者の登録管轄地の QGTIS によって認識されている。または
(c) 登録されている組織に関連付けられている QIIS 上での名称。または
(d) 登録されている組織に関連付けられている商標について弁護士意見書での確認

国ごとの方法

日本
上記方法に加え以下:

(a) ヘボン式ローマ字名は日本式ローマ字名として使用できる。
(b) シマンテックは申請者の正式な法的名称のローマ字翻字の確認として、QIIS か弁護士意見書を使用することができる
(c) シマンテックは英語名称の確認に金融庁を使うことができる。この手段を用いる場合、シマンテックは、金融庁に登録されている監査済み財務報告書に記録されている英語名称確認しなければならない。
(d) 定款によって英語名称を確認する場合、定款は登録印鑑で押印し定款が正しく現行のものであることを表記するかまたは弁護士意見書がついていなければならない。シマンテックは登録印鑑が正式なものであることを確認しなければならない。

Appendix C

EV コード・サイニング証明書の追加認証手続き

参照 : 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
www.cabforum.org

目次

1. 概要

このAppendixでは、Extended Validation証明書（以下、「EV証明書」）に関するEVガイドライン（以下、「ガイドライン」）に基づいてEV証明書を発行するにあたっての、シマンテック CPSに対する追加手続きを記述する。このガイドラインは認証機関（Certification Authority、以下「CA」という）がEV証明書を発行するにあたり守るべき必要最低限の要件を記述する。

有効なEV コード・サイニング証明書の組織情報は、対応するソフトウェアアプリケーションによって、組織の名称について信頼できる確認の証を提供するために特別な手段で表示される可能性がある。

2. 目的

2.1 EV コード・サイニング証明書の目的

EV コード・サイニング(EV Code-Signing、以下「EV CS」)証明書と署名は、証明書所持者のアイデンティティとコードの一貫性の検証のために使われることを意図している。これらはユーザやプラットフォーム提供者にコードは証明書によって確認されオリジナルから変更されておらず、EV コード・サイニング証明書に記載される名前、事業所住所、管轄、その他によって特定される事業体によって配布されているということの保証を提供する。EV コード・サイニング証明書は証明されたコードの正当性、ソフトウェアプラットフォームの信頼性の維持、ユーザのソフトウェア選択を助け、マルウェア拡散の制限をする。
EV コード・サイニング証明書は特定のソフトウェアそのものを特定するものではなく、提供者のみを特定するものである。

2.1.1 副次的目的

Appendix B1 EV SSL証明書のセクション2.1に規定される。

2.1.2 除外される目的

EV CS証明書は署名者を特定し、署名されたコードはオリジナルから改変されていないことのみを保証することに焦点を絞っている。EV コード・サイニング証明書は、その他のいかなる保証、表明または保障を提供することを意図していない。EV コード・サイニング証明書は脆弱性、マルウェア、バグその他不具合が含まれていないことを保証しない。EV コード・サイニング証明書は以下について保証または表明しない:

i. EV コード・サイニング証明書に記載されているサブジェクトが積極的に業務に従事していること
ii. EV コード・サイニング証明書に記載されているサブジェクトが適用法規を順守していること
iii. EV コード・サイニング証明書に記載されているサブジェクトが事業において信頼でき、公正で、評判がよいこと、また
iv. EV コード・サイニング証明書内に記載のサブジェクトが提供しているソフトウェアをインストールすることが「安全で」あること

3. 参照先

http://cabforum.org/documents.htmlにあるガイドラインを参照。

4. 定義

http://cabforum.org/documents.htmlにあるガイドラインの定義を参照。

5. 略語と頭字語

http://cabforum.org/documents.htmlにあるガイドラインの略語と頭字語を参照。

6. 規約

規定しない。

7. 証明書の保証および表明

7.1 EV コード・サイニング証明書の保証

シマンテックが発行したEV コード・サイニング証明書について、シマンテックおよび米国シマンテックの発行CAおよびルートCAは、EV コード・サイニング証明書が有効である間、EV コード・サイニング証明書の発行、管理、および証明書に含まれる情報の正確性の確認において、ガイドラインおよびEVポリシーの要件に従っていることを、基本要件からの補足である Appendix Dセクション7.1.1に記載される 証明書受益者に表明および保証する。

これらの保証には具体的には以下が含まれるが、制限されない。

(A) **法的存在**:シマンテックが、EV コード・サイニング オブジェクトを発行した時点において、EV コード・サイニング オブジェクトのサブジェクトがその法人設立/登録管轄地内に有効な組織またはエンティティとして法的に存在することを、サブジェクトの法人設立/登録管轄地の法人設立/登録機関に確認したこと

(B) **アイデンティティ**:シマンテックが、EV コード・サイニング オブジェクトを発行した時点において、EV コード・サイニング オブジェクトのサブジェクトの法的名称が、サブジェクトの法人設立/登録管轄地の法人設立/登録機関の公式記録の名前と一致していること、また、屋号が含まれる場合は、サブジェクトが事業所所在地の管轄地でその屋号を正しく登録していることを確認したこと

(C) **EV コード・サイニング証明書に対する承認**:シマンテックが、EV コード・サイニング オブジェクトに記載されているサブジェクトがEV コード・サイニングオブジェクトの発行を承認したことを審査するために合理的に必要と判断された手段をすべて講じたこと

(D) **情報の正確性**:シマンテックが、EV コード・サイニング オブジェクトを発行した時点において、EV コード・サイニングオブジェクトのその他の情報がすべて正確であることを審査するに合理的に必要と判断された手段をすべて講じたこと

(E) **加入者契約**: EV コード・サイニングオブジェクトのサブジェクトは、ガイドラインの要件を満たし、法的に有効かつ強制力を有する加入者契約をシマンテックと締結したこと、あるいは系列組織の場合は、申請者の代理人が利用規約を理解し同意したこと

(F) **ステータス**:発行者は、ガイドラインの要件に従い、EV コード・サイニング オブジェクトの現在のステータスが有効か失効されているかという情報を掲載した24時間365日オンラインアクセスが可能なリポジトリを保守すること

(G) **失効**:シマンテックが、ガイドラインの要件に従い、ガイドラインと本Appendixに特定された失効事象発生時にはEV コード・サイニングオブジェクトを速やかに失効させること

7.2 加入者によるもの

加入者は、発行者およびE証明書受益者の恩恵のために、本Appendixの10.3.2章の約束および保証を行う。

8. コミュニティおよび利用可能性

8.1 EV コード・サイニング 証明書の発行

EV CS証明書を発行する場合、シマンテックは、ガイドラインおよび本Appendixの要件を常に満たす。

シマンテックが業務を行う管轄地において、シマンテックの事業およびシマンテックが発行する証明書に適用されうる全法規に準拠する。ガイドラインの要件の対象となる活動(運用または証明書の発行)に対して司法権を有する裁判所または政府機関が、本要件の必須要件の履行を違法と判決した場合、シマンテックはあらゆる状況についてについてもCA/ブラウザフォーラムに通知するものとする。

8.2 EV コード・サイニング ポリシー

8.2.1 実装

この追加のAppendix Cを伴う本CPSは、
・折々の改訂時にガイドラインの要件を充足する
・(i)その時点の WebTrust Program for CAs および(ii)その時点の WebTrust EV Program 、または、CA/ブラウザフォーラムが承認した(i)および(ii)の相当物の要件を充足する
・EV 証明書の信頼性の拠りどころとなる全ルートを含む、シマンテック全体のルート認証機関のルート証明書の全階層を指定する。また、米国シマンテックのルート階層の構造は、https://www.symauth.com/repository/hierarchy/hierarchy.pdf で参照可能である。

8.2.2 開示

シマンテックは、24時間365日利用可能なCPSを通じてEVポリシーを公開する。STN CPSは、RFC 3647に従って構成される。

8.3 準拠のコミットメント

シマンテックは、http://www.cabforum.org で公開される、最新バージョンの CA/ブラウザフォーラム「EV コード・サイニング証明書の発行と管理のためのガイドライン」に準拠する。本書と同ガイドラインの間に不一致が生ずる場合は、ガイドラインがこのドキュメントよりも優先される。

さらに、シマンテックは、ガイドラインの適用される要件を、EV コード・サイニング証明書の発行または保守に関連する下位 CA、RA、エンタープライズ RA、および下請業者との契約書に(直接または参照されることによって)組み込む。

8.4 保険

シマンテックは、Appendix B1 EV SSL証明書 のセクション 8.4で規定される保険を維持する。

8.5 EV コード・サイニング 証明書の取得

シマンテックは、Appendix B1 EV SSL証明書のセクション 8.5で規定される要件を満たす申請者だけにEV コード・サイニング証明書を発行する。

9. EV 証明書の内容およびプロファイル

本セクションでは、EV コード・サイニング証明書のCAおよびサブジェクトのアイデンティティに関連するEV コード・サイニング証明書の内容の必須要件を規定する。

9.1 発行者情報

EV コード・サイニング証明書は基本要件で規定される発行者情報を含まなければならず、基本要件からの補足であるAppendix D セクション 9.1「発行者情報」で規定される。

9.2 サブジェクト情報

加入者に発行されるEV コード・サイニングオブジェクトは列挙されるフィールドのサブジェクト組織についての以下の情報を含まなければならない。

9.2.1 サブジェクト組織名フィールド

Appendix B1 EV SSL証明書のセクション 9.2.1で規定される。

9.2.2 Subject Alternative Name エクステンション

本フィールドは、EV コード・サイニングオブジェクトには含めない。

9.2.3 サブジェクト コモンネーム フィールド

本フィールドは、EV コード・サイニングオブジェクトには含めない。
Certificate Field: subject:commonName(OID 2.5.4.3)
必須/オプション: 廃止予定(推奨されないが、禁止されてはいない)
内容: 存在する場合、本フィールドにドメイン名を入れてはならない

9.2.4 サブジェクト 事業種別 フィールド

Appendix B1 EV SSL証明書のセクション 9.2.4で規定される。

9.2.5 サブジェクトの法人設立または登録管轄地 フィールド

Appendix B1 EV SSL証明書のセクション 9.2.5で規定される。

9.2.6 サブジェクト 登録番号 フィールド

Appendix B1 EV SSL証明書のセクション 9.2.6で規定される。

9.2.7 サブジェクト 事業所所在地フィールド

Appendix B1 EV SSL証明書のセクション 9.2.7で規定される。

9.2.8 その他サブジェクト属性

サブジェクトフィールドとして存在する全てのその他の任意の属性は、シマンテックによって確認された情報を入れなければならない。サブジェクト フィールドのオプション サブフィールドは、発行者によって確認された情報を入れるか、空のままにしておけなければならない。’.’, ’–‘および’ ‘のようなメタデータやフィールドが空、空白または不完全などを表わすものなどは使ってはならない。

9.3 証明書ポリシーの識別

Appendix B1 EV SSL証明書のセクション 9.3で規定される。

9.4 EV コード・サイニング証明書最大有効期間

加入者に発行されるEV コード・サイニング証明書の有効期間は、39ヶ月を超えてはならない。

9.5 加入者の公開鍵

シマンテックが発行する証明書は、本CPS セクション 6.1.5 で要求されるアルゴリズムと鍵サイズの要件を満たす。また、最低限の暗号化アルゴリズムと鍵サイズの条件については Appendix B2 も参照のこと。

9.6 証明書シリアルナンバー

シマンテックおよび米国シマンテックのCAは、少なくとも 20 ビットのエントロピーを表す、非連続の証明書シリアルナンバーを生成する。

9.7 EV コード・サイニング証明書の追加技術要件

以下の例外を除き、Appendix B1 EV SSL証明書 のセクション 9.7で規定される。

(A) EV SSL証明書で要求されるドメイン名は除外される。

(B) 証明書は以下の内容を含むSubjectAltName:permanentIdentifierを入れなければならない。

1） subjectjurisdictionOfIncorporationCountryNameで規定される:サブジェクトの設立または登録の管轄に対応するISO 3166-2 国コード。

2） 適用される場合、subjectjurisdictionOfIncorporationLocalityNameまたは、州は省略しない形式で表現されるsubjectjurisdictionOfIncorporationStateorProvinceNameフィールドで規定される、サブジェクトの設立管轄の大文字で表現された州、地域、または住所.。

3） 以下のうち最初に適用されるもの
   a. Subject:serialNumberフィールド(REG)で規定される登録番号。または、
   b. YYY-MM-DD形式(DATE)で表現される設立または登記された日とorganizationNameフィールド(ORG)で規定されるサブジェクトの組織名。または、
   c. YYY-MM-DD形式(DATE)で表現される確認できる作成日とorganizationNameフィールド(ORG)で規定されるサブジェクトの組織名。または、
   d. organizationNameフィールド(O)に含まれるサブジェクトの組織名。

ユニコードを使ったSubjectAltName:permanentIdentifier エクステンションのシマンテックでの形式は、以下の通り: CC-STATE(適用される場合)-REG or DATE (可能であれば)-ORG(もしREGが無ければ)。組織名を表現する文字は、大文字のユニコードでなけkればならない。文字列に含まれる"-"文字は、ユニコードの002Dでなければならない。REG、STATEまたはORGに含まれる空白文字は、ユニコードの0020でなければならない。

シマンテックは、組織名のフィールドが64文字を超えないようにするために、シマンテックは Appendix B1 EV SSL証明書のセクション 11に従って、依拠当事者が誤って他の組織と思わない限りにおいてフィールドを確認し、組織名を短くしたり省略したりすることがある。これができなければ、シマンテックはEV Code Signingコード・サイニング証明書を発行してはならない。

(C) keyUsageエクステンションは以下の通り設定しなけれならない:
本エクステンションは存在しなければならず、クリティカルに設定しなければならない。
digitalSignatureのビット位置は設定しなければならない。全ての他のビット位置は、設定してはないらない;かつ

(D) 拡張keyUsageエクステンションは以下の通り設定しなけれならない:
本エクステンションは存在しなければならず、ip-kp-codeSigning値が存在しなければならない。
他の値は存在すべきではない。

10. EV コード・サイニング 証明書要求の要件

10.1 一般的要件

Appendix B1 EV SSL証明書のセクション 10.1 で規定する。

10.2 EV コード・サイニング証明書要求の要件

Appendix B1 EV SSL証明書のセクション 10.2 で規定する。

10.3 加入者契約および利用規約の要件

10.3.1 概要

EV コード・サイニング証明書を発行する前に、シマンテックは、発行者と証明書受益者の恩恵を表明するために、以下のいずれかを取得する。

1. 発行者との加入者契約に対する申請者の承諾
2. 利用規約に対する申請者の承諾

EV コード・サイニング証明書を発行する前に、シマンテックは、依拠当事者およびアプリケーションソフトウェアベンダの恩恵を表明するために法的拘束力を持つ加入者契約に対する申請者の承諾を取得する。加入者契約は申請者の代理を務める権限のある契約書署名者によって署名されなければならず、証明書要求に応じて発行されるEV コード・サイニング証明書に適用されなければならない。証明書要求ごとに個別の加入者契約を用意する場合や、一つの加入者契約で将来の複数にわたった証明書要求と証明書をカバーする場合がある。

10.3.2 契約要件

加入者契約に対する申請者の同意には、少なくとも申請者自身および申請者の代理として同意の署名を行う契約書署名者の両方の名前が必要である。加入者契約は申請者が以下の義務と保証を課す条項を含まなければならない:

1. **情報の正確性**証明書要求において、および証明書の発行に関連して、シマンテックから要求された場合において、シマンテックに常に正確で完全な情報を提供する義務および保証。

2. **秘密鍵の保護**
   証明書（およびパスワードやトークンなど、関連付けられたすべてのアクティベーションデータまたはデバイス）に含まれる公開鍵に対応する秘密鍵を、単独で管理し、秘密を保持し、常に適切に保護するためにあらゆる合理的な手段を講じることに関する、申請者あるいは（例えばホスティングベンダのような）契約者の義務および保証。

3. **証明書の受理**
   加入者が証明書の内容の正確性を確認および検証する義務およびその保証。

4. **証明書の使用**疑わしいコードを含むソフトウェアに故意に署名をしないこと、およびEV コード・サイニング証明書を以下のように利用することに関する義務と保証

   a.ガイドラインの要件に準拠するコードの署名のみとする
   b. もっぱら、適用される全ての法律に従い作成されている
   c. もっぱら、正式な会社の事業である
   d. もっぱら、加入者契約に沿っている

5. **報告および失効**
   以下の事象が発生した場合、証明書およびその関連付けられた秘密鍵の使用を直ちに中止し、速やかに シマンテックに証明書の失効を要求する義務およびその保証。

a. 疑わしいコードに証明書を使って署名をした証拠が見つかった
b. 証明書の情報が不適当もしくは不正確である、または、そのようになった
c.証明書に含まれている公開鍵に関連付けられた加入者の秘密鍵の不正使用もしくは危殆化が実際に発生している、または疑われる

6. **証明書の使用の終了**
鍵の危殆化を理由とする証明書の失効時に証明書に含まれる公開鍵に対応する秘密鍵のすべての使用を速やかに中止する義務およびその保証。

7. **対応**
指定された期間内の鍵の危殆化または証明書の不正使用に関する、シマンテックからの指示に対応する義務

8. **確認および同意**
申請者が加入者契約またはCA/ブラウザフォーラムの利用規約の条項に違反した場合、またはシマンテックが証明書がフィッシング攻撃、詐欺、マルウェアの配付などの犯罪行為を可能にするために使用されていることを発見した場合、シマンテックには証明書を直ちに失効する権利があることに対する確認および同意。

11. 審査の要件

11.1 概要

このセクションでは審査要件、審査要件に対して許容できる確認手法およびシマンテックが要件を満たすために実施する手続きについて規定する。

11.2 申請者の法的存在およびアイデンティティの検証

Appendix B1 EV SSL証明書のセクション 11.2 で規定する。

11.3 申請者の法的存在およびアイデンティティの検証 – 屋号

Appendix B1 EV SSL証明書のセクション 11.3 で規定する。

11.4 申請者の物理的存在の検証

Appendix B1 EV SSL証明書のセクション 11.4 で規定する。

11.5 申請者の事業の存在の検証

Appendix B1 EV SSL証明書のセクション 11.5 で規定する。

11.6 申請者のドメイン名の検証

コード・サイニング証明書はドメイン名を含んではならない。

11.7 契約書署名者および証明書承認者の名前、肩書、権限の検証

Appendix B1 EV SSL証明書のセクション 11.7 で規定する。

11.8 利用規約および EV コード・サイニング 証明書要求への署名の検証

Appendix B1 EV SSL証明書のセクション 11.8 で規定する。

11.9 EV コード・サイニング証明書要求の承認の検証

Appendix B1 EV SSL証明書のセクション 11.9 で規定する。

11.10 特定の情報源の検証

Appendix B1 EV SSL証明書のセクション 11.10 で規定する。

11.11 その他の検証の要件

Appendix B1 EV SSL証明書のセクション 11.11 で規定する。

11.12 最終的な相互確認およびデューデリジェンス

Appendix B1 EV SSL証明書のセクション 11.12 で規定する。

11.13 既存文書の再利用の要件

Appendix B1 EV SSL証明書のセクション 9.7 および 11.13 で規定する。

12. ルート CA による証明書発行

米国シマンテックはルートCAの証明書発行に際し、複数名による管理を行う。ルートCAの秘密鍵はEV コード・サイニング証明書を署名することには使用されない。

13. 証明書失効およびステータスチェック

Appendix B1 EV SSL証明書のセクション 13 および以下で規定する。

(A) 失効理由 : 加入者は疑わしいコードを署名されたソフトウェアに意図的に含めることを予期していない。意図的に疑わしいコードに署名することは加入者契約の条項に違反する。このため、EV コード・サイニングオブジェクトは失効される結果となる。

1. 失効状況の情報 : シマンテックは該当する証明書の有効期間から少なくとも1年間正確で最新の失効ステータスの情報を提供する。依頼に応じて、EV コード・サイニング証明書の有効期間から1年以上提供する。

2. 失効の方法：実用的には、プラットフォームは必要とするたびに証明書の失効ステータスを確認すべきである。しかしながら、この方法は常に現実的ではあるとは限らず、たとえば、署名されたコードが起動順序でネットワーク通信層よりも早くロードされることがある。

   タイムスタンプのモデルでは、プラットフォームがRFC5280のパス検証アルゴリズムから逸脱し、タイムスタンプ証明書の失効ステータスの確認だけでなく、タイムスタンプがなされた時刻よりむしろ、依拠時刻における加入者のEV コード・サイニング証明書の失効状態の確認がなされるべきである。

   失効ステータスの確認に加えて、実務的には、プラットフォームは、疑わしいソフトウェアのブラックリストを調べるべきである。

(B) 失効の影響：証明書は確認するソフトウェアオブジェクトと1対1の関係にある場合がある。そのような場合、証明書の失効によって一つの疑わしいコードになされた署名が無効になるだけである。一方、証明書が確認するソフトウェアオブジェクトと1対多の関係にある場合は、証明書の失効によって、問題なく思われるものをいくつか含む全てのソフトウェアオブジェクトの署名が無効となる。

(C) 応答：シマンテックは、シマンテックが発行した証明書で検証できた署名されたソフトウェアオブジェクトの疑わしいコードに関する全ての妥当な通知に対し、証明書の失効ステータスを「失効済み」にすることで応答する。

14. 従業員および第三者機関

14.1 信頼性および能力

Appendix B1 EV SSL証明書のセクション 14.1 で規定する。

14.2 登録機関および下請け業者への職務の委譲

シマンテックはEV コード・サイニング証明書の登録機関機能を委任しない。

15. データレコード

シマンテックは、基本要件からの補足である Appendix D セクション 15 に従って イベントを記録する。

16. データセキュリティ

シマンテックおよび米国シマンテックは、基本要件からの補足である Appendix D セクション 16 に従って、包括的なセキュリティプログラムを実施する。加えて、シマンテックではEV コード・サイニング証明書作成にあたって2名以上の信頼される人物の関与を必要とする。
加えて:

(1) 米国シマンテックのEV コード・サイニング証明書を署名するCAは本CPS セクション 6.2.1 に記載の通りFIPS 140-2 level3 (または同等)の暗号化モジュールで秘密鍵を保護する。
(2) シマンテックはFIPS 140-2 level 2 またはそれ以上の暗号化モジュールの中で加入者の秘密鍵が作成され、保存され、利用されることを保証する。シマンテックはFIPS 140-2 level 2暗号

化モジュールは加入者が必要なドライバと一緒に発送する。加入者はドライバをインストールし、シマンテックのウェブサイトでFIPS 140-2 level 2デバイス上に鍵を生成する。

17. 監査

17.1 適格な監査スキーム

シマンテックは、本CPSセクション8で定義される、WebTrust for Certification Authorities v2.0 以降の年次監査を実施する。

このような監査は、シマンテックにより直接実施されるか、またはRAやサブコントラクタに委譲されるかに関わらず、CA/ブラウザフォーラムのガイドライン下のCAの義務を全て網羅する。

17.2 監査期間

セクション17.1 を参照のこと。

17.3 監査記録

セクション 17.1 を参照のこと。

17.4 発行開始前の準備状況の監査

適用しない。

17.5 定期的な自主監査

シマンテックおよび関連会社は、最後のサンプルが取得された直後から始まる期間に発行された証明書の1つあるいは 3% のいずれか多いほうの数の証明書をサンプルとしてランダムに選択し、四半期に一度の自己監査を実施し、CPおよびCPSの要件への順守と、サービスの品質への厳格なコントロールを監視するものとする。

RAによって実施される本Appendixのセクション 11.12で要求されている最終的な相互確認およびデューデリジェンスに関して全てのEV コード・サイニング証明書については、シマンテックはサービス品質を厳密に管理するために、前回のサンプル抽出完了直後から開始される期間において無作為に抽出した少なくとも6%以上の発行済み証明書に対して自主監査を実施している。

17.6 監査役の資格

資格を持つ監査人(本CPS セクション 8.2 で定義される)が定期監査を実施する。

17.7 ルート CA 鍵ペア生成

Appendix B1 EV SSL証明書のセクション 17.7 で規定される。

18. 責任と補償

シマンテックはAppendix B1 EV SSL証明書のセクション 18 に規定される責任と補償に従わなければならない。

Appendix 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』

参照:『パブリック証明書の発行および管理に関する基本要件』
www.cabforum.org

目次

1. 概要

この Appendix では、『パブリック証明書の発行および管理に関する基本要件』(以下「基本要件」)に基づいて組織認証(Organization Validated、以下「OV」)証明書およびドメイン認証(Domain Validated、以下「DV」)証明書を発行するにあたっての、シマンテック CPS に対する補足的手続きを説明する。また、この Appendix の中のいくつかのセクションは、EV SSL 証明書の発行に関する追加手続き(Appendix B1)および EV コード・サイニング証明書の発行に関する追加手続き(Appendix C)から参照される。

基本要件は、パブリック証明書を発行するために認証機関(Certification Authority、以下「CA」という)が満たさなければならない最低限の要件について説明することを目的として、CA ブラウザフォーラムによって、www.cabforum.org に公開される。

この Appendix によって定義される補足的手続きを踏まえて発行されるシマンテックの OV 証明書および DV 証明書は、インターネット経由でアクセス可能なサーバの認証を目的として利用される。

2. 目的

基本要件第 2 章で定義。

3. 参照

基本要件第 3 章で定義。

4. 定義

基本要件第 4 章で定義。

5. 略語および頭字語

基本要件第 5 章で定義。

6. 規約

基本要件第 6 章で定義。

7. 証明書の保証および表明

7.1 CA によるもの

証明書を発行することによって、シマンテック はセクション 7.1.1 に規定されている証明書の受益者に対して、セクション 7.1.2 に規定されている証明書の保証を行う。

7.1.1 証明書の受益者

シマンテックの証明書の受益者には、以下が含まれるが、これらに限定されない。

1. 証明書の加入者契約または利用規約の当事者である加入者。
2. ルート CA が契約を締結しているすべてのアプリケーションソフトウェアサプライヤ。契約は、かかるアプリケーションソフトウェアサプライヤによって配布されるソフトウェアにルート証明書を含めるためのものである。
3. 有効な証明書に合理的に依拠するすべての依拠当事者。

7.1.2 証明書の保証

CA は、証明書が有効である間、CA が証明書の発行および管理において本要件およびその証明書ポリシーや認証局運用規定に従っていることを、証明書の受益者に表明および保証する。

証明書の保証には、具体的に以下が含まれるが、これらに限定されない。

1. ドメイン名または IP アドレスを使用する権利: 発行の時点で、CA が、(i)申請者が、証明書の サブジェクトフィールドおよび subjectAltName エクステンションに指定されているドメイン名および IP アドレスを使用する権利を持つ、またはこれらを管理していること(または、ドメイン名の場合のみ、かかる権利または管理がかかる使用または管理の権利を有する他の人物によって委譲されたこと)を検証するための手順を実装し、(ii)証明書を発行する際にその手順に従い、(iii)CA の証明書ポリシーや認証局運用規定にその手順を正確に記述したこと。
2. 証明書に対する承認: 発行の時点で、CA が、(i) サブジェクト が証明書の発行を承認し、申請権限者が サブジェクト を代表して証明書を要求する権限を持っていることを確認す

るための手順を実装し、(ii)証明書を発行する際にその手順に従い、(iii)CA の証明書ポリシーや認証局運用規定にその手順を正確に記述したこと。

3. 情報の正確性: 発行の時点で、CA が、(i)証明書に含まれるすべての情報(サブジェクト:organizationalUnitName 属性を除く)の正確性を検証するための手順を実装し、(ii)証明書を発行する際にその手順に従い、(iii) CA の証明書ポリシーや認証局運用規定にその手順を正確に記述したこと。
4. 誤解を招く情報の不存在: 発行の時点で、CA が、(i)証明書の サブジェクト:organizationalUnitName 属性に含まれる情報が誤解を与えるものである可能性を減らすための手順を実装し、(ii)証明書を発行する際にその手順に従い、(iii) CA の証明書ポリシーや認証局運用規定にその手順を正確に記述したこと。
5. 申請者のアイデンティティ: 証明書に サブジェクト アイデンティティ情報が含まれる場合、CA が、(i)セクション 9.2 および 11.2 に従って申請者のアイデンティティを検証するための手順を実装し、(ii)証明書を発行する際にその手順に従い、(iii) CA の証明書ポリシーや認証局運用規定にその手順を正確に記述したこと。
6. 加入者契約: CA および加入者が関連会社でない場合、加入者および CA は、本要件を満たす法的に有効で施行可能な加入者契約の当事者であること、または CA および加入者が関連会社である場合、申請権限者が利用規約を認め、同意したこと。
7. ステータス: CA が、すべての有効期限内の証明書のステータス(有効または失効)に関する最新情報を含む 24 時間 365 日対応のパブリックにアクセス可能なリポジトリを保守していること。
8. 失効: 本要件で規定されている事由が発生した場合、CA が証明書を失効すること。

7.2 申請者によるもの

シマンテックは、CA および証明書の受益者の利益のために、申請者が本要件のセクション 10.3.2 で規定されているコミットメントおよび保証を行うことを要求する。

8. コミュニティおよび利用可能性

8.1 準拠

シマンテックは、この Appendix で定義されている要件に準拠するものとする。シマンテックは業務を行うすべての管轄地においてその事業および発行する証明書に適用されるすべての法規に従って証明書を発行し、PKI を運用する。

本要件の対象となる活動に対して司法権を有する裁判所または政府機関が、本要件の必須要件の履行を違法と判決した場合、かかる要件は、その要件を有効かつ合法にするために必要な最小限の範囲において是正されると見なされる。これは、その管轄地の法律の対象となる運用または証明書発行にのみ適用される。関与する当事者は、CA/ブラウザフォーラムが本要件を適宜改訂できるよう、事実、状況、および関係する法について CA/ブラウザフォーラムに通知するものとする(SHALL)。

8.2 証明書ポリシー

8.2.1 実装

シマンテックは、本要件の最新バージョンをどのように実装するかを詳細に記述した証明書ポリシーや認証局運用規定を作成、実装、施行し、年に一度更新するものとする。

8.2.2 開示

シマンテックは、証明書ポリシーや認証局運用規定を、24 時間 365 日利用可能な適切で容易にアクセスできるオンライン手段を通して公的に開示する。CA の業務運用は、RFC 3647 および WebTrust for CA 準拠の監査スキーム に従って提供される。

8.3 準拠のコミットメント

Symantec Trust Network（以下、「STN」）階層内の CA は、www.cabforum.org で公開される、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』の最新バージョンに準拠することを表明する。このドキュメントと基本要件の間に不一致が生ずる場合は、基本要件がこのドキュメントよりも優先される。

8.4 信頼モデル

本 CPS 規定しない。

9. 証明書のコンテンツおよびプロファイル

9.1 発行者情報

以下の名前属性は本 CPS に基づいて発行される証明書の発行者フィールドを設定するために使われるものとする（SHALL）。

9.1.1 発行者コモンネームフィールド（任意）

Issuer commonName フィールドが存在する場合、このフィールドには発行 CA を正確に識別する名前を含めなければならない（MUST）。

9.1.2 発行者ドメインコンポーネントフィールド

規定しない。

9.1.3 発行者組織名フィールド（必須）

organizationName (O=) フィールドには、シマンテック（Symantec Corporation）を正確に識別するものであることを条件として、CA の名前（またはその略称）、商標、またはその他の意味のある識別子を含める。このフィールドには、「Root」や「CA1」などの汎用的な指定を含めてはならない（MUST NOT）。

9.1.4 発行者国名フィールド（必須）

countryName (C=) フィールドには、発行者の事業拠点がある国の 2 文字の ISO 3166-1 国別コードを含める。

9.2 サブジェクト 情報

以下の名前属性は本 CPS に基づいて発行される証明書のサブジェクトフィールドを設定するために使われるものとする（SHALL）。

9.2.1 Subject Alternative Name エクステンション（必須）

subjectAlternativeName エクステンションには、少なくとも 1 つのエントリを含める。各エントリは、

FQDN を含む dNSName、サーバの IP アドレスを含む iPAddress のいずれかである。 シマンテックは、申請者が FQDN または IP アドレスを管理している、またはドメイン名登録者または IP アドレス譲受人から使用権を付与されていることを確認する。ワイルドカード FQDN を使用できる。

本要件の発効日以降、予約 IP アドレスまたは内部サーバ名を含む subjectAlternativeName エクステンションまたは サブジェクト コモンネーム フィールドを備えた証明書を発行する前に、シマンテックは、かかる証明書の使用を CA/ブラウザフォーラムでは推奨していないこと、およびその運用が 2016 年 10 月までに廃止されることを申請者に通知する。また、発効日以降、シマンテックは、予約 IP アドレスまたは内部サーバ名を含む subjectAlternativeName エクステンションまたは サブジェクト コモンネーム フィールドを備えた、有効期限日が 2015 年 11 月 1 日以降の証明書を発行しないものとする（SHALL NOT）。2016 年 10 月 1 日以降、シマンテックは、subjectAlternativeName エクステンションまたは サブジェクト コモンネーム フィールドに予約 IP アドレスまたは内部サーバ名が含まれている、すべての有効期限内の証明書を失効するものとする（SHALL）。

9.2.2 サブジェクト コモンネームフィールド（任意）

commonName （CN=） は廃止予定である。（推奨されないが、禁止されてはいない）。存在する場合、このフィールドには、証明書の subjectAltName エクステンション（セクション 9.2.1 を参照）に含まれている値のいずれかである単一の IP アドレスまたは FQDN を含める。

9.2.3 サブジェクト ドメインコンポーネントフィールド（任意）

domainComponent （dc=） コンポーネントは任意である。存在する場合、このフィールドには、サブジェクト の登録ドメイン名のすべてのコンポーネントを、ドメイン名空間のルートに最も近い最も重要なコンポーネントを最後に記述するという順序で含める。

9.2.4 サブジェクト 組織名フィールド（任意）

organizationName （O=） が存在する場合、organizationName フィールドには、サブジェクト名または DBA、およびセクション 11.2 で検証したサブジェクトの所在地住所情報を含める。

個人名のサブジェクト属性（givenName （2.5.4.42）、surname （2.5.4.4）など）はアプリケーションソフトウェアによって広範にサポートされていないため、CA は、個人のサブジェクト名または DBA を伝達するために organizationName フィールドを使用してもよい（MAY）（セクション 11.2「サブジェクトアイデンティティ情報の認証」参照）。

一般的なばらつきや略称などの検証した名前とは多少異なる情報については、CA がその違いや略称がその地域で受け入れられている略称であることを文書化している場合には、このフィールドに含めてもよい。たとえば、公認記録が「Company Name Incorporated」の場合、CA は「Company Name, Inc.」を使用してもよい（MAY）。organizationNameフィールドは検証したサブジェクトのDBAあるいは商標を含めてもよい（MAY）
organizationName が存在する場合は、localityName、stateOrProvinceName（可能な場合）、および countryName フィールドも必須であるものとする（SHALL）。また streetAddress と postalCode は任意であるものとする（SHALL）。organizationName が存在しない場合、証明書は streetAddress、localtyName、stateOrProvinceName、あるいは postalCode 属性を含めないものとする（SHALL NOT）。CA は、他のサブジェクト識別名情報を含めることなく、countryName の要件に従ってサブジェクトの countryName フィールドを含めてもよい(MAY)

9.2.5 サブジェクト 国名フィールド（任意）

存在する場合、countryName （C=） コンポーネントには ISO 3166-1 国別コードを含めるものとする（SHALL）。存在する場合、シマンテックはセクション 11.2.5 に従って検証したサブジェクトに関連付けられる国を検証するものとする（SHALL）。

9.2.6 サブジェクトのその他の属性

その他のすべての任意の属性は、サブジェクト フィールド内に存在する場合、CA によって検証済みの情報を含めなければならない（MUST）。任意の属性には、「.」、「-」、「 」（空白）文字などのメタデータや、値が存在しない、不完全である、または適用不可であることを示すものを使用しないものとする（SHALL NOT）。

シマンテックはサブジェクト属性に上記のsubjectAlternativeNameとCommonNameで定義されているケースを除いて、FQDNを含めないものとする（SHALL NOT）。

OrganizationalUnitName（任意）

存在する場合、OrganizationalUnitName (OU=) コンポーネントは、CAによって検証されていない情報を含めてもよい（MAY）。このコンポーネントには「.」、「-」、「 」（空白）文字などのメタデータや、値が存在しない、不完全である、または適用不可であることを示すものを使用しないものとする（SHALL NOT）。
シマンテックは、OU 属性に名前、DBA、商号、商標、アドレス、場所、または特定の個人や法人を表すその他のテキストが含まれるのを防止するプロセスを実装する。ただし、シマンテック がセクション 11.2 に従ってこの情報を検証済みであり、証明書にも同じくセクション 11.2.5に従って検証済みの subject:organizationName、subject:localityName、および subject:countryName属性が含まれている場合を除く。
証明書要求にOU属性が含まれる時、この属性はセクション11.5「ハイリスク要求」で規定される幾つかのハイリスクリストを使った検証を受ける。もし一致する場合、この属性はRAによって、値が正しく、ミスリーディングでないことが確認される。OUの値が法的エンティティの名前を識別するものである場合、セクション11.2に従って、値が検証される。

9.3 証明書ポリシーの識別

9.3.1 予約された証明書ポリシー識別子

規定しない。

9.3.2 ルート CA 証明書

ルート CA 証明書には、certificatePolicies エクステンションを含めないものとする（SHALL NOT）。

9.3.3 下位 CA 証明書

シマンテックおよび米国シマンテックの証明書は、CA/ブラウザフォーラムの要件に従い発行され管理されることを示す、STN CP セクション 1.2 で規定される対応するポリシー識別子を含む。

CA/ブラウザフォーラムの基本要件の発効日は 2012年7月1日 である。
発行 CA の関連会社ではない下位 CA に、発効日以降に発行された証明書は、以下に準拠するものとする。

1. 下位 CA の、CA/ブラウザフォーラムの要件への準拠を示す、STN CP セクション 1.2 で規定される、対応するポリシー識別子を含めなければならない（MUST）、および
2. 「anyPolicy」識別子（2.5.29.32.0）を含めてはならない（MUST NOT）。

発行 CA の関連会社である下位 CA に、発効日以降に発行された証明書は、以下に準拠するものとする。

1. 下位 CA の、CA/ブラウザフォーラムの要件への準拠を示す、STN CP セクション 1.2 で規定される、対応するポリシー識別子を含めてもよい（MAY）、および
2. 明示的なポリシー識別子の代わりに「anyPolicy」識別子（2.5.29.32.0）を含めてもよい（MAY）。

9.3.4 加入者証明書

シマンテックは予約された OID の値を、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』に準拠するために、STN CP セクション 1.2 で規定している。この OID の値は、CA/ブラウザフォーラムのこの要件に準拠するために米国シマンテック CA の全ブランドのために予約され使用される。それ自体は特定のブランドや証明書のクラスを識別するものではない。

シマンテックのドメイン認証および組織認証 SSL サーバ証明書は、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』への準拠を示す、STN CP セクション 1.2 に対応する OID を含む。

9.4 有効期間

CA/ブラウザフォーラムが定める OV および DV 証明書に関する要件の発効日（2012 年 7 月 1 日）以降に発行される、シマンテックのドメイン認証および組織認証 SSL サーバ証明書には、48 カ月（4 年）以下の有効期間を設けなければならない（MUST）。

以下に規定される内容を除き、2015 年 4 月 1 日以降に発行される証明書には、36 カ月（3 年）以下の有効期間を設けなければならない（MUST）。2015 年 4 月 1 日以降、CA は、有効期間が 36 カ月を超えるが 48 カ月を超えない証明書を引き続き発行してもよい（MAY）。ただし、証明書が以下のようなシステムまたはソフトウェア用であることを CA が文書化することを条件とする。

（a） 発効日よりも前に使用していた。

（b） 申請者または多数の依拠当事者によって現在使用されている。

（c） 有効期間が 48 カ月未満の場合、運用できない。

（d） 依拠当事者に対する既知のセキュリティリスクを含んでいない。および

（e） 多額の経済的支出なしではパッチ適用または交換が難しい。

9.5 加入者公開鍵

シマンテックが発行する証明書は、本 CPS セクション 6.1.5 で要求されるアルゴリズムと鍵サイズの要件を満たす。最低限の暗号アルゴリズムと鍵サイズについては Appendix B2 も参照のこと。

9.6 証明書シリアルナンバー

シマンテックは、少なくとも 20 ビットのエントロピーを表す、非連続の証明書シリアルナンバーを生成する。

9.7 その他の技術要件

Appendix B2 最低限の暗号化アルゴリズムおよび鍵サイズ要件を参照のこと。また、EV 証明書の証明書エクステンション要件は Appendix B3 を参照のこと。

10. 証明書申請

10.1 ドキュメント要件

証明書の発行前に、シマンテックは、申請者から以下のドキュメントを取得する。

1. 証明書要求（電子媒体による取得でもよい）、および
2. 署名された加入者契約または利用規約（電子媒体による取得でもよい）

シマンテックは、本要件を満たすために必要であるその他のドキュメントをすべて取得する。

10.2 証明書要求

10.2.1 概要

証明書の発行前に、シマンテックは、シマンテックが指定する形式であり、本要件に準拠する証明書要求を申請者から取得する。セクション 11.3 の有効期間および更新要件に従い、同じ申請者に発行される複数の証明書に 1 つの証明書要求で対応してもよい（MAY）。ただし、各証明書が、申請者を代表する適切な申請権限者によって署名された有効な最新の証明書要求によってサポートされていることを条件とする。証明書要求は、電子的に作成、送信、または署名してもよい（MAY）。

10.2.2 要求および証明

証明書要求には、証明書の発行申請者から、または申請者の代理人からの要求、および申請者から、または申請者の代理人による、要求に含まれるすべての情報が正しいことの証明が含まれていなければならない（MUST）。

10.2.3 情報要件

証明書要求には、証明書に含まれる申請者に関するすべての事実情報、および CA が本要件およびシマンテックの証明書ポリシーや認証局運用規定に準拠するために申請者から取得する必要がある追加情報を含めてもよい（MAY）。証明書要求が申請者に関する必要な情報の一部を含んでいない場合、シマンテックは、残りの情報を申請者から取得する、または信頼できる独立した第三者機関のデータソースから情報を取得して申請者に確認する。

申請者情報には、証明書の subjectAltName エクステンションに含まれる FQDN または IP アドレスを少なくとも 1 つ含めなければならない（MUST）が、これに限定されるものではない。

10.2.4 加入者秘密鍵

加入者以外の当事者は、加入者秘密鍵をアーカイブしないものとする（SHALL NOT）。

シマンテックまたはその指定された RA が、加入者の秘密鍵が加入者と関連会社でない、権限を持たない個人または組織に伝達されたことを認識した場合、シマンテックは、伝達された秘密鍵に対応する公開鍵を含むすべての証明書を失効するものとする（SHALL）。

10.3 加入者契約および利用規約

10.3.1 概要

証明書の発行前に、シマンテックは、依拠当事者およびアプリケーションソフトウェアベンダの明示的な利益のために、法的拘束力を有する加入者契約に対する申請者の同意を取得する。加入者契約は申請者の代理を務める権限のある契約書署名者によって署名されなければならず、また、加入者契約は証明書要求に応じて発行される証明書に適用されなければならない（MUST）。

シマンテックは、各加入者契約が申請者に対して法的強制力を持つことを確実にするためのプロセスを実装するものとする。いずれの場合も、契約書は、証明書要求に従って発行される証明書に適用しなければならない（MUST）。

シマンテックは、電子媒体による契約または「クリックスルー」契約を使用する。ただし、かかる契約は法的強制力を持つことを条件とする。証明書要求ごとに別の契約を使用してもよい（MAY）。または、複数の将来の証明書要求およびその結果発行される証明書のために単一の契約を使用してもよい（MAY）。ただし、シマンテックが申請者に発行する各証明書が明確にその加入者契約または利用規約の対象となっていることを条件とする。

10.3.2 契約要件

申請者の加入者契約への同意には、申請者自身および申請者の代理として同意の署名を行う契約書署名者の両方の名前が含まれているものとする（SHALL）。加入者契約には、以下の義務および保証を課す条項が含まれているものとする（SHALL）。

1. 情報の正確性:
証明書要求において、および証明書の発行に関連して、シマンテックから要求された場合において、シマンテックに常に正確で完全な情報を提供する義務および保証。

2. 秘密鍵の保護:
証明書（およびパスワードやトークンなど、関連付けられたすべてのアクティベーションデータまたはデバイス）に含まれる公開鍵に対応する秘密鍵を、単独で管理し、秘密を保持し、常に適切に保護するためにあらゆる合理的な手段を講じることに関する、申請者あるいは（例えばホスティングベンダのような）契約者の義務および保証。

3. 証明書の受理:
加入者が証明書の内容の正確性を確認および検証する義務およびその保証。

4. 証明書の使用:
証明書を、証明書に記載されているドメイン名でアクセス可能なサーバにのみインストールし、すべての適用法規に準拠し、承認された会社の事業のみを対象とし、加入者契約に従う方法でのみ証明書を使用する義務およびその保証。

5. 報告および失効:
(a)証明書の情報が不適当もしくは不正確である、または不適当もしくは不正確になる場合、または(b)証明書に含まれている公開鍵に関連付けられた加入者の秘密鍵の不正使用もしくは危殆化が実際に発生している、または疑われる場合、証明書およびその関連付けられた秘密鍵の使用を直ちに中止し、速やかに シマンテックに証明書の失効を要求する義務およびその保証。

6. 証明書の使用の終了:
証明書の失効時に証明書に含まれる公開鍵に対応する秘密鍵のすべての使用を速やかに中止する義務およびその保証。

7. 対応:
指定された期間内の鍵の危殆化または証明書の不正使用に関する、シマンテックからの指示に対応する義務。

8. 確認および同意:
申請者が加入者契約または利用規約の条項に違反した場合、またはシマンテックが証明書がフィッシング攻撃、詐欺、マルウェアの配付などの犯罪行為を可能にするために使用されていることを発見した場合、シマンテックには証明書を直ちに失効する権利があることに対する確認および同意。

11. 認証の実行

11.1 利用権限の確認

11.1.1 ドメイン名登録者による利用権限の確認

証明書に記載された各 FQDN と IP アドレスに対して、シマンテックは証明書が発行された日付時点で、申請者がドメイン名登録者である、または FQDN を管理している人物であること、またはかかる権限も持つ者から許可されていること(例えば被代理人・代理人の関係やライセンサー・ライセンシー関係)を、確認する。

ドメイン名登録者からの登録ドメイン名の使用権または管理の確認に依拠し、トップレベルドメインが 2 文字の国別コード(ccTLD)である場合、シマンテックは、ccTLD のルールが適用されるドメイン名レベルについて、ドメイン名登録者から直接確認をする。たとえば、要求された FQDN が www.mysite.users.exmaple.co.uk の場合、シマンテックは、ドメイン名 example.co.uk のドメイン名登録者から確認を取得する。.co.uk の直下のドメイン名の申請は .uk レジストリのルールに準拠するためである。

申請者がドメイン名登録機関から、要求された FQDN に対して証明書を取得できる権限を持っていることを確認するためにインターネットのメールシステムを使う場合、シマンテックは以下のいずれかの方法で作成されたメールアドレスを使用する:

1. ドメイン名登録機関から提供。
2. ドメインの WHOIS レコードに記載されているドメイン名登録者の「registrant」、「technical」、または「administrative」の連絡先情報から取得。
3. 次のようにドメイン名の先頭にローカル部分を追加:

a. ローカル部分 – 次のいずれか: 「admin」、「administrator」、「webmaster」、「hostmaster」、または「postmaster」

b. ドメイン名 – 登録ドメイン名または要求される FQDN から 0 個以上のコンポーネントを取り除いて作成。

ドメイン名登録者がプライベート、匿名、または代理登録サービスを使用しており、かつシマンテックが前述の代替としてドメイン利用権限に依拠する場合は、ドメイン承認を、登録ドメイン名の WHOIS レコードに指定されているプライベート、匿名、または代理登録サービスから直接受領する。ドキュメントには、プライベート、匿名、または代理登録サービスのレターヘッド、統括責任者または同等の人物、あるいはかかる役員から承認された担当者の署名、証明書要求日またはそれ以降の日付、証明書に含まれる FQDN が含まれていなければならない(MUST)。WHOIS レコードがプライベート、匿名、またはプロキシ登録サービスをドメイン名登録者として識別している場合、ドメイン承認には、証明書で FQDN を使用する権利を申請者に許可する声明が含まれていなければならない(MUST)。シマンテックは、信頼できる独立した第三者機関データソースから取得した連絡先情報を使用して、プライベート、匿名、またはプロキシ登録サービスに直接連絡し、ドメイン承認が真正であることの確認をドメイン名登録者から取得するものとする(SHALL)。

11.2 サブジェクトアイデンティティ情報の認証

申請者が countryName フィールドのみで構成されている サブジェクト アイデンティティ情報を含む証明書を要求する場合、シマンテックは、セクション 11.2.5 の要件を満たし、サブジェクト と関連付けられている国を認証するものとする(SHALL)。

申請者が countryName フィールドおよびその他の サブジェクト アイデンティティ情報を含む証明書を要求する場合、シマンテックは、この後の要件を満たす認証プロセスを使用して、申請者、および申請権限者の証明書要求の真正性を認証する。シマンテックは、本セクションに基づいて依拠され

るドキュメントに修正や改ざんがないかどうかを調査する。

11.2.1 アイデンティティ

サブジェクト アイデンティティ情報に組織の名前または住所が含まれる場合、シマンテックは、組織のアイデンティティおよび住所、およびその住所が申請者が存在する、または事業を行っている住所であることを認証する。シマンテックは、以下の少なくとも 1 つが提供する、または以下の少なくとも 1 つと連絡を取ることによって得られるドキュメントを使用して申請者のアイデンティティと住所を認証する。

1. 申請者が法的に設立、存在、または承認されている管轄地にある政府機関（例えば国務省）
2. 定期的に更新され、シマンテックが後述する「データソースの正確性」セクションに従って、信用できるデータソースと見なした第三者機関データベース（例えば Duns and Bradstreet データベース）
3. シマンテック CA または CA の代理人を務める第三者機関によるサイト訪問、または
4. 意見書

シマンテックは、上記の 1 から 4 に記載されているものと同じドキュメントまたは連絡方法を使用して、申請者のアイデンティティと住所の両方を検証してもよい（MAY）。

または、シマンテックは、公共料金請求書、銀行取引明細書、クレジットカード請求書、政府発行の税務書類、またはセクション 11.6 「データソースの正確性」の要件を満たすその他の識別方法を使用して、申請者の住所を検証してもよい（MAY）（ただし、申請者のアイデンティティの検証には使用できない）。

11.2.2 商号/屋号

サブジェクト アイデンティティ情報に 商号 または屋号が含まれる場合、シマンテックは、以下の少なくとも 1 つを使用して、商号/屋号を使用するための申請者の権利を検証する。

1. 申請者の法的な設立、存在、または認識の管轄地にある政府機関が提供するドキュメントまたは、このような政府機関との連絡
2. セクション 11.6「データソースの正確性」の要件を満たす第三者ソースが提供するドキュメントまたは、このような機関との連絡
3. かかる 商号 または屋号の管理を担当する政府機関との連絡
4. 以下の「データソースの正確性」セクションの要件を満たすドキュメントが添付された意見書、または
5. 公共料金請求書、銀行取引明細書、クレジットカード請求書、政府発行の税務書類、またはセクション 11.6「データソースの正確性」の要件を満たすその他の識別形式

11.2.3 証明書要求の真正性（信頼できる連絡手段）

サブジェクト アイデンティティ情報を含む証明書の申請者が組織の場合、シマンテックは、信頼できる連絡手段を使用して、申請権限者の証明書要求の真正性を検証する。

シマンテックは、信頼できる連絡手段を検証するために、セクション 11.2.1 に記載されているソースを使用する。信頼できる連絡手段を使用することを条件として、シマンテックは、申請権限者または申請者の組織（申請者の主なビジネスオフィス、本社オフィス、人事オフィス、IT オフィス、または CA が適切と見なすその他の部門）内の信頼できるソースとの間で直接、証明書要求の真正性を確認する。

さらに、シマンテックは、申請者が証明書を要求できる個人を指定するためのプロセスを確立する。申請者が書面にて証明書を要求できる個人を指定する場合、シマンテックは、この指定以外での証

明書要求を受け入れないものとする（SHALL NOT）。シマンテックは、申請者の検証済みの書面による要求に応じて、承認された証明書要求者のリストを申請者に提供する。

11.2.4　個人の申請者の検証

申請者が個人の場合、シマンテックは、申請者の氏名、申請者の住所、および証明書要求の真正性を検証する（セクション 9.2.4「サブジェクト 識別名組織名フィールド」を参照のこと）。

シマンテックは、申請者の顔が識別できる、少なくとも 1 つの現在有効な政府発行のフォト ID（パスポート、運転免許証、ミリタリー ID、または同等のドキュメント）の判読可能なコピーを使用して、申請者の氏名を検証する。シマンテック は、コピーに修正や改ざんがないかどうかを調査する。

シマンテックは、政府により発行された ID、公共料金請求書、銀行取引明細書、クレジットカード請求書など、「データソースの正確性」要件を満たす識別方法を使用して申請者の住所を検証する。シマンテックは、申請者の氏名を検証するために使用した同じ政府発行の ID に依拠してもよい（MAY）

シマンテックは、信頼できる連絡手段を使用して申請者と証明書要求を検証する。

11.2.5　国の検証（国名だけで構成されるサブジェクトアイデンティティ）

サブジェクト countryName フィールドだけが存在する場合、シマンテックは、次のいずれかを使用して サブジェクト と関連付けられた国を検証する。

（a）以下のいずれかに関する国による IP アドレス範囲割り当て

（i） Web サイトの DNS レコードで示されている Web サイトの IP アドレスまたは

（ii）申請者の IP アドレス、

（b）要求されたドメイン名の 2 文字の国コード（ccTLD）、

（c）ドメイン名登録者によって提供された情報、または

（d）セクション「国名とその他識別情報で構成されるサブジェクト識別情報の検証」に記載されている方法。

シマンテックは、申請者の実際の拠点以外の国で割り当てられた IP アドレスへの依拠を防ぐために、プロキシ サーバを審査するプロセスを実装する。

11.3　証明書データの有効期間

シマンテックは、証明書の発行前 39 カ月よりさらに前にデータまたはドキュメントを取得した場合、証明書要求の検証にそのデータまたはドキュメントを使用しないものとする（SHALL NOT）。

11.4　拒否リスト

本 CPS のセクション 5.5.2 に従い、シマンテックは、フィッシングまたはその他の詐欺的使用の疑いあるいは懸念を理由に、以前に失効した証明書および以前に拒否した証明書をすべて含む内部データベースを最低 7 年間保持する。

シマンテックは、この情報を使用して、以降の疑わしい証明書要求を識別する。

11.5　ハイリスクステータス

シマンテックは、合理的な手続きを講じてハイリスク、即ち詐欺的攻撃（ハイリスク申請者）に利用されるかもしれない申請者を識別し、かかる申請者が本ガイドラインに従って適切に検証されたことを確認するために、合理的に必要と判断された追加の検証活動を実施する。

シマンテックは、フィッシングまたはその他の詐欺的使用を疑われる、以前に失効された証明書および以前に拒否された証明書要求を含む内部データベースを保持する。この情報は、疑わしい証明書

要求を識別するための以降の精査に使用される。シマンテックは、疑わしい証明書要求を識別するためのシマンテックのハイリスク基準によって識別された情報を使用する。シマンテックは、疑わしいまたはハイリスクと識別された証明書要求の追加検証のために、文書化された手順に従う。申請者がハイリスク申請者と識別された場合、シマンテックは、申請者と疑惑のターゲットが同じ組織であるという合理的な疑いを検証するための、適切な追加認証プロセスを実施する。

11.6 データソースの正確性

データソースをサブジェクトアイデンティティ情報を検証するために使用する前に、シマンテックはデータソースの信頼性、正確性を評価する。サブジェクトアイデンティティ情報を検証するために、シマンテックは合理的に正確で信頼できると評価したデータソースのみを使用する。

12. ルート CA による証明書発行

証明書に署名するために米国シマンテックのルート CA 秘密鍵を使用しないものとする（SHALL NOT）。以下の場合にのみ、証明書に署名するために米国シマンテックのルート CA 秘密鍵を使用するものとする（SHALL）。

1. ルート CA 自体を表すための自己署名証明書
2. 下位 CA 用の証明書およびクロス証明書
3. インフラストラクチャ目的の証明書（管理者証明書、内部 CA 運用機器用証明書、OCSP レスポンス検証証明書など）

ルート CA による証明書発行では、ルート CA が証明書への署名操作を実行するために直接コマンドを慎重に発行する、CA によって承認された個人（つまり、CA システムオペレータ、システム責任者、または PKI 管理者）が必要となる。ルート CA による証明書発行のための追加管理に関しては、セクション 5.6「鍵の切り替え」および、セクション 6.1「鍵ペア生成およびインストレーション」で説明されている。

13. 証明書失効およびステータスチェック

13.1 失効

13.1.1 失効要求

シマンテックは、本 CPS セクション 4.9 で規定されているように、加入者が自身の証明書の失効を要求するためのプロセスを提供する。シマンテックは、失効要求を受け入れ、関連する問い合わせに対応する機能を 24 時間 365 日体制で維持する。

13.1.2 証明書問題レポート

シマンテックは、加入者、依拠当事者、アプリケーションソフトウェアサプライヤ、およびその他の第三者機関に、秘密鍵の危殆化の疑い、証明書の不正使用、またはその他の種類の詐欺、危殆化、不正使用、不適切な実施、あるいは証明書に関連するその他の問題を報告するためのオンラインフォーム（証明書問題レポート）を https://www.symauth.com/support/ssl-support/ev-misuse/index.html にて提供する。

13.1.3 調査

シマンテックは、証明書問題レポートに関する調査を受領から 24 ビジネス時間以内に開始し、少なくとも以下の条件に基づいて、失効またはその他の適切なアクションを行うかどうかを決定する。

1. 申し立てられた問題の性質

2. 特定の証明書または加入者に関して受領した証明書問題レポートの数
3. 苦情を申し立てている組織体（たとえば、Web サイトが違法な活動に関与しているという捜査当局からの苦情は、注文した商品が届かなかったと申し立てる消費者からの苦情よりも重要視されるべきである）
4. 関連法規

13.1.4 レスポンス

シマンテックは、高優先度の証明書問題レポートに内部で対応し、適宜、かかる苦情を捜査当局に転送したり、かかる苦情の対象である証明書を失効するための機能を 24 時間 365 日体制で維持する。

13.1.5 失効理由

本 CPS セクション 4.9.1 で規定される全ての失効に関する状況に加えて、シマンテックは、以下が 1 つ以上発生した場合、24 時間以内に証明書を失効する。

1. 加入者が CA による証明書の失効を書面で要求した。
2. 加入者が、元の証明書要求が承認されていなかったこと、および遡及的に承認を許可しないことをシマンテックに通知した。
3. シマンテックが、加入者の秘密鍵（証明書の公開鍵に対応）が鍵の危殆化に遭っている、または証明書がそれ以外の方法で不正使用されているという証拠を入手した（例えば秘密鍵がアーカイブされた）
4. シマンテックが、加入者が加入者契約または利用規約に基づく 1 つ以上の重要な義務に違反したことを知った
5. シマンテックが、証明書での FQDN または IP アドレスの使用が合法的に許可されたものではなくなっていることを示す状況を知った（たとえば、裁判所または仲裁人がドメイン名登録者のドメイン名使用権を失効化した、ドメイン名登録者と申請者との間の関連ライセンスまたはサービスが解除された、またはドメイン名登録者がドメイン名を更新しなかった、など）
6. CA が、詐欺的な紛らわしい下位 FQDN を認証するためにワイルドカード証明書が使用されていたことを知った
7. シマンテックが、証明書に含まれている情報の重大な変更を知った
8. シマンテックが、証明書がシマンテック CP あるいは CPS に従って発行されなかったことを知った
9. シマンテックが、証明書に表示されている情報が不正確または誤解を招く恐れがあると判断した
10. シマンテックが何らかの理由で運用を中止し、別の CA が証明書の失効サポートを提供するように手配していない。
11. 本 CPS に基づいて証明書を発行するためのシマンテックの権利が失効、廃止、終了されている（シマンテックが CRL/OCSP リポジトリの維持を継続するための手配を行っている場合を除く）。
12. シマンテックが、証明書の発行に使用される下位 CA の秘密鍵の危殆化の可能性を知った。
13. 加入者が拒否された団体もしくは禁止された個人としてブラックリストに追加された、もしくはシマンテックが業務遂行する管轄地の法律に基づいて禁じられているような業務を行っていると、シマンテックが通知を受けた、または知った。

14. シマンテックの CPS や CP によって失効が必要になった。または
15. 証明書の技術的内容または形式が、アプリケーションソフトウェアまたは依拠当事者に容認できないリスクを与えている（たとえば、CA/ブラウザフォーラムによって決定されている）。

13.2 証明書ステータスチェック

13.2.1 メカニズム

シマンテックは、Appendix B3「EV 証明書で要求される証明書エクステンション」に従って、下位証明書および加入者証明書の失効情報を利用可能にする。

13.2.2 リポジトリ

シマンテックは、インターネットブラウザが、シマンテックによって発行されたすべての有効期限内証明書の現在のステータスを自動的にチェックするために使用できるオンラインリポジトリを 24 時間 365 日体制で維持する。

加入者証明書のステータスの場合:

1. CRL は、少なくとも 7 日に一度を更新および再発行されるものとし、nextUpdate フィールドの値は thisUpdate フィールドの値から 10 日を超えないものとする（SHALL NOT）。
2. シマンテックは、少なくとも 4 日ごとに OCSP 経由で提供される情報を更新する。このサービスからの OCSP レスポンスは、最大で 10 日の有効期間を持つ。

シマンテックの下位 CA 証明書のステータスの場合:

1. CRL は、少なくとも（i） 12 カ月ごとに一度、および（ii）下位 CA 証明書の失効から 24 時間以内に、更新および再発行され、nextUpdate フィールドの値は thisUpdate フィールドの値から 12 カ月を超えない。
2. シマンテックは、少なくとも（i） 12 カ月ごと、および（ii）下位 CA 証明書の失効から 24 時間以内に、OCSP 経由で提供される情報を更新する。

シマンテックは CRL と OCSP 機能を、発行した全ての証明書によって生成される問い合わせに対して、商業的に合理的なレスポンスタイムを提供するのに十分なリソースで運用、維持する。

CRL あるいは OCSP の失効エントリは、失効された証明書の、有効期限まで削除されない。

2013 年 1 月 1 日から、CA は、本要件に従って発行された証明書に関して GET メソッドを使用した OCSP 機能をサポートするものとする（SHALL）。

13.2.3 レスポンス時間

シマンテックは、通常の運用状況の下で 10 秒以内のレスポンス時間を提供するために十分なリソースで、CRL および OCSP 機能を運用および維持するものとする（SHALL）。

13.2.4 エントリの削除

本 CPS セクション 4.9.7 参照。

13.2.5 OCSP 署名

OCSP レスポンスは、RFC5019 および以下のいずれかに準拠するものとする（SHALL）。

1. 失効ステータスの確認対象となる証明書を発行した CA によって署名されている。

2. 失効ステータスの確認対象となる証明書を発行した CA によって証明書が署名されている OCSP レスポンダによって署名されている。このような OCSP 署名証明書には、RFC2560 に定義されている、タイプ id-pkix-ocsp-nochek のエクステンションが含まれているものとする（SHALL）。

14. 従業員および第三者機関

14.1 信頼性および能力

14.1.1 本人確認および身元審査

本 CPS セクション 5.3.2 で規定されている。

14.1.2 トレーニングおよびスキルレベル

シマンテックは、情報検証職務を履行するすべての担当者に、公開鍵基盤の基本知識、認証ポリシーおよび手順（本 CPS を含む）、情報検証プロセスに対する一般的な脅威（フィッシングやその他のソーシャルエンジニアリング戦術を含む）、および関連する CA/ブラウザフォーラムの要件について取り上げたスキルトレーニングを提供する。

シマンテックは、かかるトレーニングの記録を維持し、認証スペシャリスト職務を委託されている担当者が、かかる職務を十分に履行できるためのスキルレベルを維持していることを確認する。証明書発行に従事する認証スペシャリストは、CA のトレーニングおよびパフォーマンスプログラムと一致したスキルレベルを維持する。

シマンテックは、各認証スペシャリストがタスクによって必要とされるスキルを所有していることを、認証スペシャリストにそのタスクの履行を許可する前に、文書化する。シマンテックは、すべての認証スペシャリストが、CA/ブラウザフォーラムの要件に記載されている情報認証要件について CA が実施する試験に合格することを要求する。

14.2 職務の委譲

14.2.1 全般

シマンテックは、本 Appendix のセクション 11 の全部または一部の履行を、委譲先の第三者機関に委譲する前に、委譲先の第三者機関に対して、CA/ブラウザフォーラムの基本要件セクション 14.2.1 で規定される要件を要求するものとする（SHALL）。

14.2.2 準拠義務

シマンテックは、本 Appendix のセクション 11 の全部または一部の履行を、委譲先の第三者機関に委譲する前に、委譲先の第三者機関に対して、CA/ブラウザフォーラムの基本要件セクション 14.2.2 で規定される要件を要求するものとする（SHALL）。

14.2.3 責任の割り当て

シマンテックは、本 Appendix のセクション 11 の全部または一部の履行を、委譲先の第三者機関に委譲する場合でも、タスクが委譲されていない場合と同じように、本要件に従い、すべての当事者の履行について完全に責任を負うものとする（SHALL）。

14.2.4 エンタープライズ RA

シマンテックは、本 Appendix のセクション 11 の全部または一部の履行を、委譲先の第三者機関に委譲する前に、委譲先の第三者機関に対して、CA/ブラウザフォーラムの基本要件セクション 14.2.1

で規定される要件を要求するものとする（SHALL）。

15. データレコード

15.1 文書化およびイベントログ記録

シマンテックおよび各委譲先の第三者機関は、証明書要求と関連して生成されるすべての情報および受領されるドキュメントを含め、証明書要求の処理および証明書の発行のために実行するアクションの詳細、日付と時刻、および関与した担当者を記録する。シマンテックは、規定への準拠の証拠として、これらの記録を公認監査人に対して提供する。これは、RA とその下請け業者を含む全ての委譲先第三者機関でも実施される。

15.2 イベントおよびアクション

記録の要件には、少なくとも以下のイベントを含むが、これらに限定されない。

1. CA 鍵ライフサイクルマネジメントイベント（以下を含む）:
    a. 鍵の生成、バックアップ、格納、リカバリ、アーカイブ、および破棄
    b. 暗号化デバイスライフサイクル管理イベント
2. CA および加入者証明書ライフサイクルマネジメントイベント（以下を含む）:
    a. 証明書要求、更新、鍵の再生成要求、および失効
    b. 本要件および CA の認証局運用規定に規定されているすべての認証アクティビティ
    c. 認証のための電話連絡の日付、時刻、使用された電話番号、電話対応者、および認証の最終結果
    d. 証明書要求の承諾および却下
    e. 証明書の発行
    f. 証明書失効リストおよび OCSP エントリの生成
3. セキュリティイベント（以下を含む）
    a. 成功および失敗した PKI システムアクセス試行
    b. 実行された PKI およびセキュリティシステムアクション
    c. セキュリティプロファイルの変更
    d. システムクラッシュ、ハードウェア障害、およびその他の異常
    e. ファイアウォールおよびルーターアクティビティ
    f. CA 施設への出入記録
4. ログエントリには、以下の要素を含めなければならない（MUST）。
    a. 記録の日付と時刻
    b.情報を記録した担当者情報
    c.記録の詳細

15.3 保管

15.3.1 監査ログの保管

発効日以降に生成された監査ログは少なくとも 7 年間保存される。要求に応じてこれらの監査ログを公認監査人に対して提出する。

15.3.2 ドキュメントの保管

シマンテックは、証明書要求、その検証、およびそのすべての証明書と失効に関するすべてのドキュメントを、そのドキュメントに基づく証明書が有効でなくなってから少なくとも 7 年間保存する。シマンテックは、フィッシングまたはその他の詐欺への利用が疑われたために、以前失効された全ての証明書と以前拒否された全ての証明書要求の内部データベースを保持する。

16. データセキュリティ

16.1 目的

シマンテックは、以下を目的として設計された包括的なセキュリティプログラムを開発、実装、および保守する。

1. 証明書データおよび証明書管理プロセスの機密性、整合性、および可用性の保護
2. 既知の脅威や危険から証明書データおよび証明書管理プロセスの機密性、整合性、および可用性の保護
3. 証明書データまたは証明書管理プロセスの不正または違法なアクセス、使用、開示、変更、または破壊の防止
4. 証明書データまたは証明書管理プロセスの事故による損失または破壊、あるいは損害の防止
5. 法令によって CA に適用されるその他のすべてのセキュリティ要件への準拠

16.2 リスクアセスメント

シマンテックは、以下を行う年に一度のリスクアセスメントを含める。

1. 証明書データまたは証明書管理プロセスの不正なアクセス、開示、不正使用、変更、または破壊につながる可能性がある予測可能な内部および外部脅威を識別する
2. 証明書データおよび証明書管理プロセスの秘密度を考慮に入れて、これらの脅威の可能性および考えられる損害を評価する
3. かかる脅威に対抗するために CA が実装しているポリシー、手順、情報システム、技術、およびその他の準備の十分性を評価する

16.3 セキュリティ計画

リスクアセスメントに基づき、シマンテックは、上述の目的を実現し、証明書データおよび証明書管理プロセスの重要度に応じたリスクアセスメント中に識別されたリスクを管理するように設計されたセキュリティ手順、対策、および製品で構成されるセキュリティ計画を開発、実装、および維持する。

セキュリティ計画には、証明書データおよび証明書管理プロセスの秘密度に適した管理上、組織的、技術的、および物理的な保護対策を含める。また、セキュリティ計画では、その時点で提供可能な技術および特定の対策の実装コストを考慮に入れ、セキュリティの侵害から生じる可能性がある損害および保護対象のデータの性質に適した合理的なセキュリティレベルを実装する。

16.4 事業継続

シマンテックおよび米国シマンテックは、重要なビジネスプロセスの中断または障害発生後、タイムリーにビジネスオペレーションを維持または復元するための災害復旧計画（DRP）を保持する。

シマンテックおよび米国シマンテックの DRP は、バックアップデータと STN キーのバックアップコピーを使用して、シマンテック STN の運用を再開する手順を定義する。DRP は緊急事態発生時の手順、フォールバック手順　、再開手順、計画を始動するための条件、容認可能なシステム停止期間および回復時間の構成要素と目標復旧時間を定義する。

シマンテックおよび米国シマンテックの DRP は、以下の管理要件を含める。

- 計画の保守スケジュール
- 意識向上および教育要件
- 個人の責任範囲
- 緊急対策計画の定期的なテスト

更にシマンテックおよび米国シマンテックの DRP は、以下を含める。

- .重要な暗号化マテリアル（つまり、安全な暗号化デバイスおよび起動マテリアル）を代替場所に保管するための要件
- 必須のビジネス情報およびソフトウェアのバックアップコピーが作成される頻度
- 復旧施設から CA のメインサイトまでの距離
- 災害発生から元のサイトまたはリモートサイトで安全な環境を復元するまでの期間に、可能な範囲でファシリティを保護するための手順

16.5 システムセキュリティ

シマンテックは、証明書管理プロセスにシステムセキュリティ管理として以下を含める。

1. 物理セキュリティおよび環境管理（本 CPS セクション 5.1 参照）
2. 構成管理、信頼できるコードの整合性の保守、マルウェア検出/防止を含む、システムの整合性制御（本 CPS セクション 6.6.2 参照）
3. ポート制限および IP アドレスフィルタリングを含む、ネットワークセキュリティおよびファイアウォール管理（本 CPS セクション 6.7 参照）
4. ユーザー管理、職務分担、教育、認知、トレーニング（本 CPS セクション 5.2 参照）
5. 個々人の責任を明確にするための論理的なアクセス制御、アクティビティロギング、およびアイドル時のタイムアウト（本 CPS セクション 5.2.3 および 5.4.1 参照）

シマンテックは、証明書の発行を直接的に引き起こすことができるすべてのアカウントに対して多要素認証を施行する。

16.6 秘密鍵保護

シマンテックの秘密鍵の保護は本 CPS のセクション 5.1.2（物理的アクセス）、5.2.3（それぞれの任務に必要な身元の確認）、6.2.9（秘密鍵の非活性化の方法）および 6.6.1（システム開発管理）にて説明されている。

17. 監査

17.1 適格な監査スキーム

シマンテックは、本 CPS セクション 8 で定義される、WebTrust for Certification Authorities v2.0 以降の年次監査を受ける。このような監査は、シマンテックにより直接実施されるか、または RA やサブコントラクタに委譲されるかに関わらず、CA/ブラウザフォーラムのガイドライン下の CA の義務を全て網羅する。

17.2 監査期間

シマンテックおよび米国シマンテックは本 CPS セクション 8.1 に規定されているように年に 1 度の監査を実施する。

17.3 監査レポート

シマンテックおよび米国シマンテックは、本 CPS セクション 8.6 に規定されているように年次監査レポートを公開する。

17.4 発行開始前の準備状況の監査

規定しない。

17.5 委譲された職務の監査

規定しない。

17.6 監査役の資格

シマンテックおよび米国シマンテックの監査は、本 CPS セクション 8.2 で規定されている公認監査人によって実施される。

17.7 鍵生成セレモニー

シマンテックおよび米国シマンテックは、本 CPS セクション 6.1.1 および STN 機密の情報セキュリティポリシーで規定されている鍵生成セレモニーを実施する。

17.8 定期的な品質保証自主監査

シマンテックおよび関連会社は、最後のサンプルが取得された直後から始まる期間に発行された証明書の 1 つあるいは 3% のいずれか多いほうの数の証明書をサンプルとしてランダムに選択し、四半期に一度の自己監査を実施し、CP および CPS の要件への順守と、サービスの品質への厳格なコントロールを監視するものとする（SHALL）。

18. 責任および補償

18.1 加入者および依拠当事者に対する責任

シマンテックが CA/ブラウザフォーラムの要件およびその証明書ポリシーや認証局運用規定に準拠して証明書を発行および管理している限り、証明書の受益者またはその他の第三者機関が証明書の使用または依拠の結果被った被害については、責任を拒否するものとする（SHALL）。

シマンテックが、CA/ブラウザフォーラムの要件およびその証明書ポリシーや認証局運用規定に準拠して証明書を発行または管理していなかった場合、この証明書の使用または依拠の結果被った被害について法的に認識され証明される加入者へのシマンテックの責任は、(a) Netsure Protection あるいは (b) $2,000 いずれか大きい方であるとする(SHALL)。証明書の利用あるいは依拠に伴って発生した、法的に認識され証明される、依拠当事者あるいはその他の第三者機関の損失あるいはダメージへの、シマンテックの責任は、$2,000 を超えないものとする(SHALL NOT)。

18.2 アプリケーションソフトウェアサプライヤの補償

加入者および依拠当事者への責任の限定にもかかわらず、ルート CA との間でルート証明書配付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、これらのガイドラインに基づく、または証明書の発行保守あるいは依拠当事者、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、シマンテックの義務あるいは潜在的責任を前提としないことをシマンテックは理解し、同意するものとする。

シマンテックは、シマンテック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すべての申し立て、損害、および損失について、訴因または関連法理論にかかわらず、各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、免責するものとする(SHALL)。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が、以下のような不正な証明書を有効、または信頼可能と表示したことによって直接引き起こされた場合には、シマンテック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、上記は適用されない。(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シマンテック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に限る)。

18.3 ルート CA の義務

ルート CA は、下位 CA の本要件への準拠、および本要件の下での下位 CA のすべての責任および補償義務について、ルート CA が証明書を発行する下位 CA であるかのごとく、下位 CA の履行および保証について責任を持つものとする(SHALL)。