Symantec™ Managed PKI サービス記述書

はじめに

Symantec™ Managed PKI(Public Key Infrastructure)サービスは、新しい証明書の発行から、既存の証明書の更新、信頼に値しない証明書の失効まで、証明書のライフサイクル全体を管理するための柔軟な PKI プラットフォームを提供します。また、電子メール、ファイルシステム、その他のデータの暗号化に使用する証明書の秘密鍵の預託やリカバリもできます。さらに、証明書の現在のステータスを確認するためのさまざまな検証サービスが用意されているので、信頼に値する証明書のみを使用できます。その主な用途はデータの暗号化、文書へのデジタル署名、ネットワーク接続のための認証などです。

Symantec Managed PKI はマネージドサービスであるため、PKI を社内で構築する場合と比べてコストを大幅に削減できます。たとえば、PKI を社内運用して証明書を発行するには、まず、暗号化とアプリケーション用のサーバーハードウェアを調達し、サーバーとクライアントのライセンスを購入して、スタッフを教育する必要があります。さらに、PKI 階層の管理に関する基本方針をまとめた証明書ポリシー(CP)や、証明書に関するプロセスと手続きおよび役割と責任を定義した認証局運用規定(CPS)を独自に作成する必要もあります。Symantec Managed PKI サービスは、暗号化とアプリケーションの運用に最適なサーバーハードウェアを基盤とした可用性の高いマルチテナント環境を提供します。また、専門教育を受けたうえで厳格な身元調査に合格したスタッフが 24 時間 365 日監視しています。さらに、WebTrust と SAS70 の認定を維持するために監査を定期的に受けています。

このサービス記述書では、Symantec Managed PKI サービスが提供する基本機能の概要を示します。

認証局(CA)

Symantec Managed PKI サービスでは、認証局(CA)階層を構築および管理できます。

- 標準 CA 階層

  Symantec Managed PKI サービスでは、CA 階層として、Symantec Trust Network(STN)、プライベート認証局、Adobe®ドキュメント認証サービス(CDS)を利用できます。STN、プライベート認証局、Adobe CDS の利用条件については、それぞれ付録 A、付録 B、付録 C を参照してください。

証明書ライフサイクル管理

Symantec Managed PKI サービスでは、クラウドとハイブリットの 2 種類の展開モデルで証明書ライフサイクルを管理できます。クラウド展開モデルでは、アカウント、証明書、鍵管理ツールをシマンテックのデータセンターでホストします。ハイブリッド展開モデルでも、アカウント、証明書、鍵管理ツールはすべてシマンテックのデータセンターでホストしますが、登録局(RA)とディレクトリ統合ツールはお客様のデータセンターに配置します。これらの展開モデルは、どちらか一方に

統一する必要はなく、PKI プロジェクトでの必要に応じて組み合わせて使用することもできます。さらに、どちらの展開モデルでも、デスクトップミドルウェアである PKI Client を使用して、証明書ライフサイクルに関するユーザーの操作性を大幅に向上できます。これらの各ツールについて以下に説明します。

- PKI Manager

  PKI Manager は、シマンテックのデータセンターでホストされる、PKI 管理者向けの Web ポータルです。このツールを使って、アカウント、ユーザー、証明書、鍵管理に関するタスクを実行できます。

  - *アカウント管理*

    PKI 管理者は、PKI Manager を使ってアカウントに関連付けられた認証局（CA）、シート数、レポートを確認できます。また、PKI管理者が他の PKI 管理者を追加して責務を割り当てることもできます。

- *ユーザー管理*

  PKI Manager を使って PKI 管理者は、ユーザーを追加したり、各ユーザーに一意のパスコードを生成したり、ユーザーに送信する電子メールをカスタマイズしたりできます。また、新しく発行された証明書をサードパーティアプリケーションで使用するための設定手順を文書やビデオでユーザーに知らせることもできます。

- *証明書管理*

  PKI 管理者は、PKI Manager を使ってアカウント内の各 CA の証明書プロファイルを設定できます。証明書のプロファイルとして、鍵のサイズ、鍵の使用法、署名アルゴリズムなどのパラメータを設定できます。また、ユーザー操作（ネーティブまたは PKI Client）やセキュリティ保護レベルを選択することもできます。さらに、証明書の秘密鍵を預託するかどうかの選択も可能です。証明書プロファイルの設定に加えて、ユーザーが退職するなどして不要になった証明書や、ノートブックコンピュータの紛失によって秘密鍵が危険にさらされたなどの理由で信頼に値しない証明書を失効させることもできます。

- *鍵管理*

  PKI Manager を使って PKI 管理者は、暗号化用の証明書の秘密鍵をリカバリできます。

- PKI Certificate Service

  PKI Certificate Service は、シマンテックのデータセンターでホストされるサービスで、ユーザー（利用者）が証明書を要求するための証明書登録 Web ページを提供します。ユーザーは、Web ページに表示される手順に従って証明書を要求できます。PKI 管理者は、この Web ページにサードパーティ製品の設定手順を表示することもできます。

- Certificate Issuance Center

  Certificate Issuance Center は、シマンテックのデータセンターでホストされる証明書エンジンです。この証明書エンジンでは、PKI Certificate Service、PKI Enterprise Gateway、または Web サービスから送られた証明書署名要求に基づいて証明書が作成されます。また、発行元認証局（CA）による証明書への署名もここで行われます。

- PKI Enterprise Gateway

  PKI Enterprise Gateway は、必要に応じてお客様のデータセンターにインストールされる登録局（RA）アプリケーションです。Microsoft® Active Directory® などの LDAP（Lightweight Directory Access Protocol）ソースと密接に連携して、証明書要求の承認や LDAP ソースへの証明書データの追加を自動化します。

- PKI Client

  PKI Client は、証明書ライフサイクルに関するユーザーの操作性を大幅に向上させることを目的としたエンドポイントミドルウェアです。Windows オペレーティングシステムと Mac オペレーティングシステムのデスクトップで利用できます。ネーティブで操作する場合、ユーザーは Microsoft Internet Explorer® や Mozilla® Firefox® を使って証明書の登録 Web ページから証明書を要求します。この場合、追加のソフトウェアは不要ですが、一般的に操作性は低下します。たとえば、Microsoft Internet Explorer では、警告メッセージを表示するポップアップウ

ィンドウが多数表示されて、ユーザーを煩わせることがあります。PKI Client を使用すれば、よく使われる機能（証明書の更新など）を自動化することでユーザーの操作を最小限に抑え、証明書ライフサイクルの管理を効率化できます。また、集中型のポリシー管理機能（PIN やエクスポートなど）も提供されるため、証明書の保護にも役立ちます。さらに、証明書を使用するようにサードパーティ製品（ワイヤレスネットワーククライアントや仮想プライベートネットワーククライアントなど）を自動設定することも可能です。Symantec Managed PKI の証明書ライフサイクル管理機能は、モバイルデバイスからも利用できます。iOS の場合は、内蔵の OTA（Over-the-Air）プロトコル機能が利用されます。このため、iOS デバイスや iOS アプリケーションでは、Apple 社の SCEP プロトコルを介して証明書登録を要求できます。iOS の OTA に相当する機能を持たない Android OS などのモバイルオペレーティングシステムでは、シマンテックが提供する専用の PKI Client を使って、証明書を使用するようにデバイスやアプリケーションを簡単に設定できます。

- PKI Web サービス

  PKI Web サービスは、シマンテックのデータセンターでホストされるサービスで、Symantec Managed PKI とプログラム的に統合するための機能を提供します。サードパーティ製アプリケーションは、PKI Web サービスで提供される API を使って、証明書ポリシーを取得したり、証明書ライフサイクル機能(登録や更新など)を実行したりできます。

認証方法

Symantec Managed PKI サービスでは以下の認証方法を利用できます。

- 申請コードを使用した認証

  このタイプの認証では、PKI 管理者が各ユーザー用に、証明書要求を自動的に承認するための一意の申請コードを生成します。PKI 管理者は、証明書登録 Web ページへのリンクを記載した証明書案内メールをユーザーに送信する際に、そのユーザー用の一意のパスコードを一緒に記載します。ユーザーは、証明書登録 Web ページで、他の情報とともに自分のパスコードを入力します。Certificate Issuance Center では、ユーザーが入力した申請コードと、PKI Manager で生成された情報が照合されます。この 2 つが一致した場合は、証明書が発行されます。一致しない場合は、ユーザーにエラーメッセージが表示されます。

- 自動認証

  自動認証では、LDAP データソース(Microsoft Active Directory など)のデータに基づいて証明書要求が承認されます。この認証方法を使用するには、お客様のデータセンターに PKI Enterprise Gateway をインストールして、LDAP ソースと連携させる必要があります。ユーザーが PKI Certificate Service を介して証明書要求を送信すると、PKI Enterprise Gateway で証明書要求のデータと LDAP ソースのデータが照合されます。データが一致した場合は、証明書要求が承認され、登録局(RA)証明書によって署名され、署名された証明書要求が Certificate Issuance Center に送信されます。一致しない場合は、証明書要求が却下されます。

証明書検証

Symantec Managed PKI サービスでは以下の証明書検証ツールを利用できます。

- 証明書失効リスト

  サードパーティ製品の多くは、証明書失効リスト(CRL)を使って証明書の現在のステータス(有効や失効など)を確認する機能を備えています。CRL は、有効期限切れになる前に失効した証明書が記載される一種のブラックリストです。CRL に対応した製品では、最新の CRL を定期的にダウンロードしてステータスを確認するように設定できます。証明書が CRL に記載されている場合はアクセスが拒否されます(ネットワーク認証に失敗する、文書にデジタル署名できないなど)。シマンテックでは、少なくとも 24 時間に 1 回の間隔で CRL を生成しています。

- OCSP

  サードパーティ製品の多くは、OCSP(Online Certificate Status Protocol)を使って証明書の

現在のステータス（有効や失効など）を確認する機能も備えています。失効した証明書はすべて CRL に記載されますが、証明書が失効してから新しい CRL が生成されるまでには、標準の CRL で最大 24 時間のずれが生じます。シマンテックの OCSP ツール TGV（Trusted Global Validation）では、証明書のステータス変更（失効や停止など）があったときに、ほぼリアルタイムで変更が反映されます。

ハードウェアオプション

シマンテックでは、Symantec Managed PKI サービスを補う以下のハードウェアオプションを提供しています。

- Aladdin PKI トークン

  シマンテックは Aladdin eToken シリーズの認定リセラーです。取り扱いモデルには、PRO、NG-OTP、NG-FLASH トークンが含まれます。これらのトークンには 3 年間の保証が付きます（詳しくは、保証情報補足を参照してください）。また、これらのトークンは FIPS（Federal Information Processing Standard）140-2 標準と CC（Common Criteria）標準に準拠しています。

- SafeNet ハードウェアセキュリティモジュール（HSM）

  シマンテックは、SafeNet® Luna® ハードウェアセキュリティモジュール（HSM）の認定リセラーです。HSM は、Luna® PCI カード、Luna® SA ネットワークアプライアンス、Luna® PCM トークンで構成されます。HSM には 1 年間の基本保証が付きます。また、シマンテックでは SafeNet 延長保証プログラムもオプションとして有料で提供しています。これらの HSM も FIPS 140-2 Level 2 標準と CC 標準に準拠しています。

サポートとメンテナンス

シマンテックのサポートとメンテナンスに関する取り組みについては、適用されるサービスレベル保証を参照してください。

Symantec MPKI サービスで Microsoft 社の自動登録コンポーネントを使用する場合は、以下の「MICROSOFT に対する発意義務」が適用されます。

(a) **免責** Microsoft 社とその関連会社は、この取り決めに従って提供されるサーバーソフトウェア（「サーバーソフトウェア」）について一切の明示的、黙示的、法的保証をせず、その実行または実行不能について一切の責任を負いません。 Microsoft 社のサーバーソフトウェアは、何ら保証のない現状有姿のままで提供されます。Microsoft 社とその関連会社は、本文書によって、サーバーソフトウェアに関するその他一切の明示的、黙示的、法的な保証、義務、条件（商品性、特定目的への適合性、信頼性、可用性に関する黙示的な保証と条件を含むが、これに限定されない）を免責されるものとします。また、Microsoft 社とその関連会社は、サーバーソフトウェアに関して、権原、平穏享有、説明との一致、非侵害性に対する一切の保証および条件を免責されるものとします。

(b) **特定の損害の除外** 適用される法律によって許容される最大限の範囲で、いかなる場合においても、Microsoft 社は、サーバーソフトウェアの使用または使用不能、あるいはサーバーソフトウェアを通じたサポートやその他のサービス、情報、ソフトウェア、関連コンテンツの提供または不提供、あるいは本サービス記述書の条件に起因もしくは関連する、特別損害、付随的損害、懲罰的損害、間接損害、結果的損害、その他一切の損害（利益の損失、機密情報やその他の情報の喪失、事業の中断、人身傷害、プライバシーの喪失、誠実義務の不履行、注意義務の不履行、過失、その他の金銭的損失、その他一切の損失による損害を含むが、これに限定されない）に対して、それが Microsoft 社の過失、不法行為（怠慢を含む）、厳格責任違反、契約違反、保証違反によるものであったとしても、また、かかる損害が発生する可能性を Microsoft 社が事前に通知されていた場合であっても、一切の責任を負わないものとします。

(c) **サーバーソフトウェア要件** お客様は、この取り決めに従って提供されるサーバーソフトウェアを、ネーティブの Microsoft Windows 2000 Professional、Windows XP Home/Professional、Windows Vista、またはその後継となるクライアントオペレーティングシステムとの相互運用や通信のみを目的として、本ソフトウェアの付属文書に明示されているとおり 1 部のみ使用できます（適用されるサービス注文書または作業範囲記述書で別途明示されている場合を除く）。お客様は、いかなる状況であっても、パーソナルコンピュータ上でサーバーソフトウェアを使用することはできません。前記において「**パーソナルコンピュータ**」とは、一度に 1 人のユーザーが使用することを主な目的として構成され、ディスプレイやキーボードを備えたコンピュータを指します。

(d) **第三受益者** 契約の条項と矛盾する場合でも、本文書によってお客様は、Microsoft 社が、サーバーソフトウェアに含まれる知的財産権のライセンサーとして本サービス記述書の条件における第三受益者となり、かかる Microsoft 社の知的財産や本条件に関連する Microsoft 社のその他の権益に影響を与える本条件の条項を行使する権利を持つことに同意するものとします。

(e) **サーバークラス 2** お客様がサーバークラス 2を選択した場合、お客様は、(a)処理能力が最大 32 ビットで RAM が最大 4 GB のプロセッサ 4 基以下で構成され、(b)サーバーを再起動せずにメモリの追加、交換、取りはずしができる能力(「**ホットスワップ機能**」)を持たないサーバー上で、サーバーソフトウェアを使用できます。ホットスワップ機能やクラスタ機能をサポートするソフトウェアをサーバーソフトウェアと組み合わせて使用することはできません。「**クラスタ機能**」とは、複数のサーバーをグループ化し、グループ内のサーバーノード間でのアプリケーションフェールオーバーを実装することによって、アプリケーション実行のための単一の高可用性プラットフォームとして機能させることを指します。

(f) **監査権** シマンテックは、お客様が本条件のすべての条項に準拠していることを確認するため、監査を実施し、通常の営業時間中にお客様の敷地内でお客様の施設と手続きを調査する場合があります。監査の際には、少なくとも 14 日前までにお客様にその旨を通知します。契約の条項と矛盾する場合でも(機密保持規定を含むが、これに限定されない)、お客様が監査の実施を拒否し、お客様がサービス記述書の条件に準拠していないとシマンテックが判断する十分な理由がある場合には、シマンテックがお客様の身元情報とお客様が不適合であると考える根拠を Microsoft 社に開示することにお客様は同意するものとします。

(g) **多重化デバイス** サーバーソフトウェアで提供されるサービスに直接接続するユーザーやそれらを直接使用するユーザーの数を減らすハードウェアまたはソフトウェアを使用した場合でも、接続ユーザーまたは使用ユーザーと見なされるユーザーの数は減りません。サーバーソフトウェアの接続ユーザー数または使用ユーザー数は、直接であるか多重化デバイスを介するかに関係なく、(a)サーバーソフトウェアまたは(b)サーバーソフトウェアが認証を行うその他のソフトウェアやシステム(「**その他の認証対象システム**」)によって提供されるサービスに接続するユーザーまたはそれらを使用するユーザーの数と等しくなります。ここで述べる「**多重化デバイス**」とは、サーバーソフトウェアまたはその他の認証対象システムによって提供されるサービスに直接的または間接的に、あるいは複数のユーザーが少ない接続数でアクセスできるようにするためのハードウェアまたはソフトウェアを指します。

(h) **Windows CAL 要件** お客様は、直接であるか多重化デバイスを介するかに関係なく、サーバーソフトウェアまたはその他の認証対象システムによって提供されるサービスに接続する各ユーザーまたはそれらを使用する各ユーザーに、個別の Windows CAL を取得して割り当てる必要があります。「**Windows CAL**」とは、(a) Microsoft Windows Server 2003 Standard Edition/Enterprise Edition/Datacenter Edition またはその後継となるサーバーオペレーティングシステム製品(「**Windows Server**」)の Windows Device クライアントアクセスライセンス(「**CAL**」)または Windows User CAL、(b)Windows Server にアクセスして使用する権利を個々のユーザーや電子デバイスに与える Microsoft Core CAL を指します。この(a)と(b)のいずれの場合でも、CAL は、1 つ以上の Microsoft Windows Server オペレーティングシステム製品または電子デバイスで使用するために取得し、ユーザー単位またはデバイス単位で割り当てます。

Copyright © 2011 Symantec Corporation. All rights reserved. Symantec、Symantec ロゴ、Norton、および Checkmark ロゴは、Symantec Corporation またはその関連会社の米国およびその他の国における商標または登録商標です。その他の会社名、製品名は各社の登録商標または商標です。

付録 A: Symantec Trust Network（STN）

Symantec™ Managed PKI（Public Key Infrastructure）サービスでは、お客様が Symantec Trust Network（STN）から証明書を発行できます。シマンテックは、ハードウェアベンダーやソフトウェアベンダーの協力の下で、STN の主認証局（PCA）を一般的なほとんどの Web ブラウザ、電子メールアプリケーション、オペレーティングシステム、ネットワークアプライアンスに前もって登録しています。そのため、これらのアプリケーションでは、STN の PCA のいずれかに関連付けられた証明書が自動的に信頼されます。これらの証明書は、通常、管理者やユーザーが特別な準備をしなくても他の組織との間で使用できます。たとえば、多くのお客様が、STN 証明書を使用して電子メールにデジタル署名を付けたり、電子メールを暗号化したりしてセキュリティを強化しています。

標準パッケージでは、すべてのお客様が、クラス 2 の PCA につながる発行元認証局（CA）を自動的に利用できます。別の商標名を使用したい場合や、CA のデフォルト値を変更したい場合は、追加の CA を作成するオプションを購入することもできます。

注: これらの証明書を発行、管理、使用するには、お客様とユーザーが Symantec Trust Network 認証局運用規定（CPS）に準拠する必要があります。

SYMANTEC TRUST NETWORK のサービス利用規約

1. 定義

「管理者証明書」とは、Managed PKI 管理者として任命されたお客様側の従業員またはその他の信頼される者に対し、PKI Manager にアクセスして管理業務を行うことのみを目的としてシマンテックが発行する証明書を指します。

「関連する個人」とは、お客様と関係のある人物を指します。（a）役員、取締役、従業員、パートナー社員、契約社員、インターン、その他お客様の組織内の人物、または（b）お客様の組織と契約関係を結び、身元を確実に保証できるビジネス記録をお客様が所有している人物が該当します。

「契約」とは、シマンテックとお客様の間で結ばれ、本サービス記述書に適用されるサービス注文書が発行された、プロフェッショナルサービス契約またはその他のマスター契約や規約を指します。

「証明書」または**「デジタル証明書」**とは、少なくとも発行元 CA の名前または識別情報、利用者の識別情報、利用者の公開鍵、証明書有効期間、証明書のシリアル番号、発行元 CA のデジタル署名を含むメッセージを指します。

「証明書申請者」とは、CA に証明書の発行を要求する個人または委任代理人を指します。

「証明書申請」とは、証明書申請者（または委任代理人）から CA に提出される証明書発行要求を指します。

「証明書署名ユニット」または**「CSU」**とは、証明書への署名と鍵の保管用に設計されたハードウェア装置またはソフトウェアを指します。

「認証局」または**「CA」**とは、証明書を発行、停止、失効する権限を持つ個人またはエンティティを指します。

「認証局運用規定」または**「CPS」**とは、CA または RA による証明書発行業務の運用規定を定めた文書を指します。この文書は必要に応じて改訂されます。STN CPS は、シマンテック Web サイトのリポジトリで公開されています。

「誤発行」とは、（a）STN CPS で定められた手順とは大きく異なる方法で証明書を発行すること、（b）証明書の主体として指定されている人物とは異なる人物に証明書を発行すること、（c）証明書の主体として指定されている人物の認可なく証明書を発行することを指します。

「鍵生成」とは、シマンテックがお客様の CA 公開鍵/秘密鍵を厳密な手順に従って適切に生成し、生成された秘密鍵と関連ドキュメントを保管する手続きを指します。

「Managed PKI 管理者」とは、登録局の従業員、または登録局の業務を行う権限を与えられたその他の信頼される者を指します。

「証明書有効期間」とは、証明書が発行された日時（または証明書に記載されている、それより後の特定の日時）から、有効期限が切れる日時またはそれ以前の失効が実行された日時までの期間を指します。

「秘密鍵」とは、デジタル署名の作成に使用される数学的な鍵を指します。この鍵は他人に知られないように、所有者が秘密に保管する必要があります。アルゴリズムによっては、対になる公開鍵で暗号化された機密のメッセージやファイルを復号化するためにも使用されます。

「公開鍵」とは、対になる秘密鍵で作成された署名の検証に使用される数学的な鍵を指します。この鍵は一般に公開されます。アルゴリズムによっては、メッセージやファイルを暗号化するためにも使用されます。暗号化されたメッセージやファイルは、対にな

る秘密鍵で復号化できます。

「登録局」または**「RA」**とは、証明書申請者の身元確認と認証、証明書失効要求の手続き開始と伝達、証明書の更新または鍵更新の申請承認を行うエンティティを指します。RA は、証明書申請者の代理人とは異なります。RA は、RA の認可された Managed PKI 管理者以外に証明書申請の承認権限を委任することはできません。

「シート」とは、サービスの正規エンドユーザーである単一の利用者を指します。その利用者に実際に発行された証明書数は関係ありません。

「利用者」とは、証明書の主体であり、発行対象である、個人またはエンティティを指します。利用者は、発行時に証明書に含まれる公開鍵に対応した秘密鍵を使用でき、使用する権限を持ちます。

「利用規約」とは、利用者と CA またはシマンテックとの間で結ばれる、指定された証明書関連サービスのプロビジョニングに関する規約を指します。この規約により、証明書に関する利用者の権利と義務が定められます。

STN の利用規約は、シマンテック Web サイトのリポジトリで公開されています。

「信頼される者」の定義は、CPS での定義に従います。

「Symantec Trust Network」または**「STN」**とは、Symantec Trust Network 証明書ポリシーの下で管理される、証明書ベースの公開鍵基盤(PIK)を指します。シマンテックとその関連会社、それぞれのお客様、利用者、依拠する当事者は、この基盤を利用して証明書をグローバルに展開および使用できます。

2. 任命

(a) **任命** 本文書によって、シマンテックはお客様を STN 内の STN CPS に従う非シマンテック CA として任命し、お客様はこの任命を受け入れるものとします。

(b) **STN CPS** 本サービス記述書の下でシマンテックに委託された業務を除いて、お客様は、(i)STN CPS(改正を含む)および(ii)これらのサービス条件の第 4 項で定められた義務を含む(ただしこれに限定されない)、STN 内の CA や RA に課されるすべての要件を満たし、すべての義務を果たすものとします。シマンテックは、改正の内容を PKI Manager に掲示することによって、お客様が任命した登録局管理者に通知するものとします。

3. お客様の義務

(a) **任命** お客様は、認可された 1 人以上のお客様側の従業員または信頼される者を Managed PKI 管理者として任命するものとします。任命された Managed PKI 管理者は、お客様に代わって追加の Managed PKI 管理者を任命する権利を有するものとします。お客様は、この取り決めに従って証明書を受け取る Managed PKI 管理者に、適用される利用規約の条項に従わせる義務を持つものとします。

(b) **管理業務** お客様は、STN CPS(改正を含む)で定められた要件に従うものとします。これには、証明書申請に含まれる情報の検証、検証後の証明書申請の承認または却下、証明書の失効、シマンテック指定のハードウェアとソフトウェアの使用に関する要件が含まれますが、これに限定されません。お客様は、十分な資格と能力を備えた適切な資質を持つ担当者としてこれらの業務を遂行するものとします。お客様は、証明書申請者がお客様の関連する個人である場合にのみ、証明書申請を承認するものとします。お客様が証明書を発行した利用者がお客様の関連する個人でなくなった場合、お客様はすみやかに PKI Manager から当該利用者の証明書の失効を要求するものとします。Managed PKI 管理者が、お客様に代わって Managed PKI 管理者としての任務を果たす権限を取り消された場合、お客様はすみやかに当該 Managed PKI 管理者の管理者証明書の失効を要求するものとします。

(c) **お客様の利用者** お客様は、この取り決めに従って証明書を受け取る利用者に、適切な利用規約の条項に従わせる義務を持つものとします。また、利用者は、証明書の登録条件としてその利用規約に合意するものとします。お客様は、その利用規約の条項によって、CA に対して STN CPS の条項と同等の安全性を保証するものとします。

(d) **存続** 契約で定められた終了規定に加えて、本サービス記述書および STN CPS で定められた失効要件とセキュリティ要件は、契約の終了日または適用されるサービス注文の終了日を超えて、この取り決めに従って発行されたすべての証明書有効期間の終了まで存続するものとします。

(e) **お客様の保証** お客様は、契約で明示的に定められた限定的保証に加えて、以下の項目もシマンテックに保証するものとします。(i)証明書の発行に必要なすべての情報、およびお客様が検証する、またはお客様に代わって検証されるすべての情報が、重要なすべての点において真実であり正しいこと、(ii)証明書申請に対するお客様の承認が誤発行を引き起こさないこと、(iii)お客様が、STN CPS と RA 要件に十分に準拠していること、(iv)シマンテックに提出される証明書情報が第三者の知的財産権を侵害していないこと、(v)証明書申請に含まれる情報(電子メールアドレスを含む)が違法な目的に使用されたことがなく、今後も使用されないこと、(vi)お客様側の Managed PKI 管理者が、管理者証明書が作成されて以来、その管理者証明書の秘密鍵、およびその秘密鍵を守るためのチャレンジフレーズ、PIN、ソフトウェア、またはハードウェアメカニズムを扱う唯一の人物であり、今後もそうであり続けること、ならびに認可されていない人物がこれらの情報やシステムにアクセスしたことがなく、今後もアクセスしないこと、(vii)お客様が、本サービス記述書に準拠し認可された合法的な目的にのみ管理者証明書を使用すること、(viii)お客様が、シマンテックの一切のシステム、ソフトウェア、STN の技術的実装を監視、妨害、リバースエンジニアリングせず、またはその他の方法でそれらのセキュリティを故意に侵害しないこと。

(f) **監査権** シマンテックは、お客様の手続きが本サービス記述書の条項に準拠していることを確認するため、年 1 回以上の監査を行うことがあります。このような監査は、文書によってお客様に妥当な通知が送られた後、営業時間内に、お客様の業務を不当に妨害することなく行われます。お客様は、これらの監査において合理的な範囲でシマンテックに協力するものとします。監査によってお客様が本サービス記述書に記載の条件の条項に違反していることが明らかになった場合、(i)お客様はシマンテックに相応の監査実施費用を支払い、(ii)シマンテックは上記の年 1 回の監査に加え、必要に応じて、適用される条項への準拠を徹底するための追加監査を実施できるものとします。年 1 回の定期監査は、前年の活動のみを対象とすることができます。

(g) **現地法への準拠** お客様は、本サービス記述書に従ってシマンテックが生成した公開鍵/秘密鍵ペアの取得、使用、受領において、お客様がその鍵ペアを取得、使用、受領した管轄で適用されるすべての現地法や規定(輸出入に関する法律や規制を含むが、これに限定されない)に準拠する責任があります。

4. **シマンテックの義務**

(a) **サービス** 必要な導入作業の完了後、シマンテックは、本サービス記述書に明示されているサービスを、記載の条件に従って、サービス期間にわたってお客様に提供するものとします。シマンテックは、お客様およびお客様側の Managed PKI 管理者からの指示に従って証明書の発行、管理、失効、更新を行うものとします。シマンテックは、お客様から提出された適切な構造の XKMS 要求に従って、XKMS での公開鍵の登録、依拠する当事者への公開鍵の提供、公開鍵の登録取り消しも行うものとします。お客様が証明書申請を承認した後、シマンテックは(i)承認された各証明書申請に含まれる情報の正確性を信頼する権利を有し、(ii)その証明書申請を提出した証明書申請者に対して証明書を発行するものとします。本サービス記述書の下で発行または許諾された証明書(管理者証明書を含む)には、その証明書の発行日から最大 12 カ月の証明書有効期間が定められます。

(b) **管理者証明書** お客様が管理者証明書の証明書申請を提出した場合、シマンテックは、管理者証明書に必要な認証手続きを行ってから証明書申請を処理します。シマンテックは、管理者証明書の証明書申請が承認されたか却下されたかをお客様に通知します。Managed PKI 管理者が、管理者証明書を受け取るためにシマンテックから提供された PIN を使用した時点、またはその他の方法で管理者証明書をインストールまたは使用した時点で、Managed PKI 管理者による管理者証明書の受領が成立するものとします。Managed PKI 管理者は、管理者証明書の受け取りまたはインストール後、使用を開始する前に、証明書に含まれる情報を確認し、誤りがあった場合はすみやかにシマンテックに通知する必要があります。シマンテックは、このような通知を受け取った場合、その管理者証明書を失効させ、修正された管理者証明書を発行するものとします。

(c) **CA 鍵生成** シマンテックは、1 回の CA 鍵生成イベントで、お客様に代わってシマンテックが発行する証明書に署名するための STN 用の CA 鍵ペアをお客様に生成するものとします。各鍵ペアのお客様の CA 秘密鍵は、1 つ以上の証明書署名ユニットに保管されるものとします。

(d) **シマンテックの保証** シマンテックは以下の項目を保証します。(i)シマンテックが証明書作成の際に注意を怠ったために証明書の情報に誤りが入り込むような事態が起きないこと、(ii)シマンテックによる証明書の発行が、重要なすべての点において STN CPS に準拠すること、(iii)シマンテックの失効サービスとリポジトリの使用が、重要なすべての点において STN CPS に従うこと。

5. **追加条項**

(a) **CA 証明書** 各サービスアカウントには、少なくとも 1 つの CA 証明書が含まれます。特定数量に対する追加の CA 証明書は後から購入できます。シマンテックのシステムとサービスからの CA 証明書やその鍵ペアの抽出は、各当事者との同意に基づくものとします。

(b) **管理者キット** 管理者キットは、トークン、ソフトウェア、および 1 つの管理者証明書で構成されます。特定数量に対する追加の管理者キットは後から購入できます。

付録 B: プライベート認証局

Symantec™ Managed PKI(Public Key Infrastructure)サービスでは、お客様がプライベート認証局(CA)から証明書を発行できます。シマンテックは、セキュリティ保護された環境で厳密な手順に従って、この CA の秘密鍵/公開鍵ペアを生成します。この手続きはキーセレモニーと呼ばれます。プライベート CA で発行した証明書は、通常、組織内のリソースへのアクセスを制御するために使用します。たとえば、多くのお客様が、仮想プライベートネットワーク(VPN)の認証で自社のプライベート CA のみを信頼することで、社内ネットワークへの無断アクセスを防止しています。

標準パッケージでは、すべてのお客様がプライベート CA を自動的に利用できます。この CA の名義には、アカウントのセットアップ時にシマンテックに提示され、入念にチェックされた、お客様の正式な法人名が使用されます。自社の別の商標名(商標登録済みのブランド名など)を使用したい場合や、CA のデフォルト値を変更したい場合は、追加の CA を作成するオプションを購入することもできます。

注: お客様は、適用されるプライベート CA での証明書の発行、管理、使用に関する独自の認証局運用規定(CPS)を定義し、それに従う義務があります。

プライベート認証局の利用規約

1. 定義

「管理者証明書」とは、Managed PKI 管理者として任命されたお客様側の従業員またはその他のる者された個人に対し、PKI Manager にアクセスして管理業務を行うことのみを目的としてシマンテックが発行する証明書を指します。

「契約」とは、シマンテックとお客様の間で結ばれ、本サービス記述書に適用されるサービス注文書が発行された、プロフェッショナルサービス契約またはその他のマスター契約や規約を指します。

「証明書」または**「デジタル証明書」**とは、少なくとも発行元 CA の名前または識別情報、利用者の識別情報、利用者の公開鍵、証明書有効期間、証明書のシリアル番号、発行元 CA のデジタル署名を含むメッセージを指します。

「証明書申請者」とは、CA に証明書の発行を要求する個人または委任代理人を指します。

「証明書申請」とは、証明書申請者(または委任代理人)から CA に提出される証明書発行要求を指します。

「証明書署名ユニット」または**「CSU」**とは、証明書への署名と鍵の保管用に設計されたハードウェア装置またはソフトウェアを指します。

「認証局」または**「CA」**とは、証明書を発行、停止、失効する権限を持つ個人を指します。

「誤発行」とは、(a)証明書の主体として指定されている人物とは異なる人物に証明書を発行すること、(b)証明書の主体として指定されている人物の認可なく証明書を発行することを指します。

「鍵生成」とは、シマンテックがお客様の公開鍵/秘密鍵を厳密な手順に従って適切に生成し、生成された秘密鍵と関連ドキュメントを保管する手続きを指します。

「Managed PKI 管理者」とは、登録局の従業員、または登録局の業務を行う権限を与えられたその他の信頼される者を指します。

「証明書有効期間」とは、証明書が発行された日時(または証明書に記載されている、それより後の特定の日時)から、有効期限が切れる日時またはそれ以前の失効が実行された日時までの期間を指します。

「プライベート階層」とは、お客様のルート CA から、1 つ以上の認証局、そして利用者へとつながるチェーンの中で、お客様が定めた手順に従って証明書を発行する一連の CA によるドメインです。プライベート階層で発行される証明書は、組織が社内で発行を認可することを目的としており、公共のチャネルを介して組織や個人の間でやり取りすることは目的としていません。

「秘密鍵」とは、デジタル署名の作成に使用される数学的な鍵を指します。この鍵は他人に知られないように、所有者が秘密に保管する必要があります。アルゴリズムによっては、対になる公開鍵で暗号化された機密のメッセージやファイルを復号化するためにも使用されます。

「公開鍵」とは、対になる秘密鍵で作成された署名の検証に使用される数学的な鍵を指します。この鍵は一般に公開されます。アルゴリズムによっては、メッセージやファイルを暗号化するためにも使用されます。暗号化されたメッセージやファイルは、対になる秘密鍵で復号化できます。

「登録局」または**「RA」**とは、証明書申請者の身元確認と認証、証明書失効要求の手続き開始と伝達、証明書の更新または鍵更

新の申請承認を行うエンティティを指します。RA は、証明書申請者の代理人とは異なります。RA は、RA の認可された Managed PKI 管理者以外に証明書申請の承認権限を委任することはできません。

「シート」とは、サービスの正規エンドユーザーである単一の利用者を指します。その利用者に実際に発行された証明書数は関係ありません。

「利用者」とは、証明書の主体であり、発行対象である、個人またはエンティティを指します。利用者は、発行時に証明書に含まれる公開鍵に対応した秘密鍵を使用でき、使用する権限を持ちます。

「利用規約」とは、利用者と CA またはシマンテックとの間で結ばれる、指定された証明書関連サービスのプロビジョニングに関する規約を指します。この規約により、証明書に関する利用者の権利と義務が定められます。

「信頼される者」とは、お客様およびお客様の製品、サービス、設備、手順の基盤をなす信頼性に対して責任を持つ、お客様の従業員、契約社員、コンサルタントを指します。

2. **お客様の義務**

(a) **任命** お客様は、認可された 1 人以上のお客様側の従業員または信頼される者を Managed PKI 管理者として任命するものとします。任命された Managed PKI 管理者は、お客様に代わって追加の Managed PKI 管理者を任命する権利を有するものとします。お客様は、この取り決めに従って証明書を受け取る Managed PKI 管理者に、適用される利用規約の条項に従わせる義務を持つものとします。

(b) **管理業務** お客様は、シマンテック指定のハードウェアとソフトウェアを使用するお客様側の Managed PKI 管理者を通して、証明書申請に含まれる情報を検証し、検証後の証明書申請を承認または却下して、シマンテックに発行を指示し、証明書の更新と失効を行うものとします。Managed PKI 管理者が、お客様に代わって Managed PKI 管理者としての任務を果たす権限を取り消された場合、お客様はすみやかに当該 Managed PKI 管理者の管理者証明書の失効を要求するものとします。

(c) **存続** 契約で定められた終了規定に加えて、本サービス条件で定められた失効要件とセキュリティ要件は、契約の終了日または適用されるサービス注文の終了日を超えて、この取り決めに従って発行されたすべての証明書有効期間の終了まで存続するものとします。

(d) **お客様の保証** お客様は、契約で明示的に定められた限定的保証に加えて、以下の項目も保証するものとします。(i)証明書の発行に必要なすべての情報、およびお客様が検証する、またはお客様に代わって検証されるすべての情報が、重要なすべての点において真実であり正しいこと、(ii)証明書申請に対するお客様の承認が誤発行を引き起こさないこと、(iii)シマンテックに提出される証明書情報が第三者の知的財産権を侵害していないこと、(iv)証明書申請に含まれる情報(電子メールアドレスを含む)が違法な目的に使用されたことがなく、今後も使用されないこと、(v)お客様側の Managed PKI 管理者が、管理者証明書が作成されて以来、その管理者証明書の秘密鍵、およびその秘密鍵を守るためのチャレンジフレーズ、PIN、ソフトウェア、またはハードウェアメカニズムを扱う唯一の人物であり、今後もそうであり続けること、ならびに認可されていない人物がこれらの情報やシステムにアクセスしたことがなく、今後もアクセスしないこと、(vi)お客様が、本サービス記述書に準拠し認可された合法的な目的にのみ管理者証明書を使用すること、(vii)お客様が、シマンテックのシステムまたはソフトウェアの技術的実装を監視、妨害、リバースエンジニアリングせず、またはその他の方法でそれらのセキュリティを故意に侵害しないこと。

(e) **現地法への準拠** お客様は、本サービス記述書に従ってシマンテックが生成した公開鍵/秘密鍵ペアの取得、使用、受領において、お客様がその鍵ペアを取得、使用、受領した管轄で適用されるすべての現地法や規定(輸出入に関する法律や規制を含むが、これに限定されない)に準拠する責任があります。

3. **シマンテックの義務**

(a) **サービス** 必要な導入作業の完了後、シマンテックは、本サービス記述書に明示されているサービスを、記載の条件に従って、サービス期間にわたってお客様に提供するものとします。シマンテックは、お客様およびお客様側の Managed PKI 管理者からの指示に従って証明書の発行、管理、失効、更新を行うものとします。シマンテックは、お客様から提出された適切な構造の XKMS 要求に従って、XKMS での公開鍵の登録、依拠する当事者への公開鍵の提供、公開鍵の登録取り消しも行うものとします。お客様が証明書申請を承認した後、シマンテックは(i)承認された各証明書申請に含まれる情報の正確性を信頼する権利を有し、(ii)その証明書申請を提出した証明書申請者に対して証明書を発行するものとします。本サービス記述書の下で発行または許諾された証明書(管理者証明書を含む)には、その証明書の発行日から最大 12 カ月の証明書有効期間が定められます。

(b) **管理者証明書** お客様が管理者証明書の証明書申請を提出した場合、シマンテックは、管理者証明書に必要な認証手続きを行ってからお客様の証明書申請を処理します。シマンテックは、管理者証明書の証明書申請が承認されたか却下されたかをお客様に通知します。Managed PKI 管理者が、管理者証明書を受け取るためにシマンテックから提供された PIN を使用した時点、またはその他の方法で管理者証明書をインストールまたは使用した時点で、Managed PKI 管理者による管理者証明書の受領が成立するものとします。Managed PKI 管理者は、管理者証明書の受け取りまたはインストール後、使用を開始する前に、証明書に含まれる情報を確認し、誤りがあった場合はすみやかにシマンテックに通知する必要があります。シマンテックは、このような通知を受け取った場合、その管理者証明書を失効させ、修正された管理者証明書を発行するものとします。

(c) **CA 鍵生成** シマンテックは、1 回の CA 鍵生成イベントで、お客様に代わってシマンテックが発行する証明書に署名するための、お客様のプライベート階層用の CA 鍵ペアをお客様に生成するものとします。各ペアのお客様の秘密鍵は、1 つ以上の証明書署名ユニットに保管されるものとします。

(d) **シマンテックの保証** シマンテックは、シマンテックが証明書作成の際に注意を怠ったために証明書の情報に誤りが入り込むような事態が起きないことを保証します。

4. **追加条項**

(a) **CA 証明書** 各サービスアカウントには、少なくとも 1 つの CA 証明書が含まれます。特定数量に対する追加の CA 証明書は後から購入できます。シマンテックのシステムとサービスからの CA 証明書やその鍵ペアの抽出は、各当事者との同意に基づくものとします。

(b) **管理者キット** 管理者キットは、トークン、ソフトウェア、および 1 つの管理者証明書で構成されます。特定数量に対する追加の管理者キットは後から購入できます。

付録 C: Adobe® ドキュメント認証サービス

Symantec™ Managed PKI（Public Key Infrastructure）サービスでは、お客様が Adobe® ドキュメント認証サービス（CDS）から証明書を発行できます。シマンテックは、Adobe 社の協力の下で、Adobe Acrobat®、Reader®、LiveCycle® の各製品で自動的に信頼される証明書を発行できるようにしています。この証明書を前述の製品で使って、PDF にデジタル署名ができます。

標準パッケージでは、すべてのお客様が、シマンテック中間 CA for Adobe CDS につながる発行元認証局（CA）を自動的に利用できます。この CA の名義には、アカウントのセットアップ時にシマンテックに提示され、入念にチェックされた、お客様の正式な法人名が使用されます。自社の別の商標名（商標登録済みのブランド名など）を使用したい場合や、CA のデフォルト値を変更したい場合は、追加の CA を作成するオプションを購入することもできます。

注: これらの証明書を発行、管理、使用するには、お客様とユーザーが Adobe CDS 認証局運用規定（CPS）に準拠する必要があります。

ADOBE CDS の利用規約

1. 定義

「管理者証明書」とは、Managed PKI 管理者として任命されたお客様側の従業員またはその他の信頼される者に対し、PKI Manager にアクセスして管理業務を行うことのみを目的としてシマンテックが発行する証明書を指します。

「契約」とは、シマンテックとお客様の間で結ばれ、本サービス記述書に適用されるサービス注文書が発行された、プロフェッショナルサービス契約またはその他のマスター契約や規約を指します。

「証明書」または**「デジタル証明書」**とは、少なくとも発行元 CA の名前または識別情報、利用者の識別情報、利用者の公開鍵、証明書有効期間、証明書のシリアル番号、発行元 CA のデジタル署名を含むメッセージを指します。

「証明書申請者」とは、CA に証明書の発行を要求する個人または委任代理人を指します。

「証明書申請」とは、証明書申請者（または委任代理人）から CA に提出される証明書発行要求を指します。

「認証局運用規定」または**「CPS」**とは、CA または RA による証明書発行業務の運用規定を定めた文書を指します。この文書は必要に応じて改訂されます。本 Managed PKI for Adobe® CDS サービス記述書では、「CPS」は、シマンテック Web サイトのリポジトリで公開されている、シマンテック Adobe ドキュメント認証サービス（CDS）PKI 認証局運用規定を指すものとします。

「証明書署名ユニット」または**「CSU」**とは、証明書への署名と鍵の保管用に設計されたハードウェア装置またはソフトウェアを指します。

「認証局」または**「CA」**とは、証明書を発行、停止、失効する権限を持つ個人を指します。

「誤発行」とは、（a）CPS で定められた手順とは大きく異なる方法で証明書を発行すること、（b）証明書の主体として指定されている人物とは異なる人物に証明書を発行すること、（c）証明書の主体として指定されている人物の認可なく証明書を発行することを指します。

「鍵生成」とは、シマンテックがお客様の公開鍵/秘密鍵を厳密な手順に従って適切に生成し、生成された秘密鍵と関連ドキュメントを保管する手続きを指します。

「Managed PKI 管理者」とは、登録局の従業員、または登録局の業務を行う権限を与えられたその他の信頼される者を指します。

「証明書有効期間」とは、証明書が発行された日時（または証明書に記載されている、それより後の特定の日時）から、有効期限が切れる日時またはそれ以前の失効が実行された日時までの期間を指します。

「プライベート階層」とは、STN 以外の階層で証明書を発行する認証局を指します。Adobe CDS では、この認証局の上層にシマンテック中間 CA for Adobe CDS があり、さらにその上層に Adobe ルート CA があります。

「秘密鍵」とは、デジタル署名の作成に使用される数学的な鍵を指します。この鍵は他人に知られないように、所有者が秘密に保管する必要があります。アルゴリズムによっては、対になる公開鍵で暗号化された機密のメッセージやファイルを復号化するためにも使用されます。

「公開鍵」とは、対になる秘密鍵で作成された署名の検証に使用される数学的な鍵を指します。この鍵は一般に公開されます。アルゴリズムによっては、メッセージやファイルを暗号化するためにも使用されます。暗号化されたメッセージやファイルは、対になる秘密鍵で復号化できます。

「登録局」または**「RA」**とは、証明書申請者の身元確認と認証、証明書失効要求の手続き開始と伝達、証明書の更新または鍵更新の申請承認を行うエンティティを指します。RA は、証明書申請者の代理人とは異なります。RA は、RA の認可された Managed PKI 管理者以外に証明書申請の承認権限を委任することはできません。

「シート」とは、サービスの正規エンドユーザーである単一の利用者を指します。その利用者に実際に発行された証明書数は関係ありません。

「利用者」とは、証明書の主体であり、発行対象である、個人またはエンティティを指します。利用者は、発行時に証明書に含まれる公開鍵に対応した秘密鍵を使用でき、使用する権限を持ちます。

「利用規約」とは、利用者と CA との間で結ばれる、指定された証明書関連サービスのプロビジョニングに関する規約を指します。この規約により、証明書に関する利用者の権利と義務が定められます。

「Symantec Trust Network」または**「STN」**とは、Symantec Trust Network 証明書ポリシーの下で管理される、証明書ベースの公開鍵基盤(PIK)を指します。シマンテックとその関連会社、それぞれのお客様、利用者、依拠する当事者は、この基盤を利用して証明書をグローバルに展開および使用できます。

「信頼される者」とは、お客様およびお客様の製品、サービス、設備、手順の基盤をなす信頼性に対して責任を持つ、お客様の従業員、契約社員、コンサルタントを指します。

2. お客様の義務

(a) **任命** お客様は、認可された 1 人以上のお客様側の従業員または信頼される者を Managed PKI 管理者として任命するものとします。任命された Managed PKI 管理者は、お客様に代わって追加の Managed PKI 管理者を任命する権利を有するものとします。お客様は、この取り決めに従って証明書を受け取る Managed PKI 管理者に、適用される利用規約と CPS の条項に従わせる義務を持つものとします。

(b) **管理業務** お客様は、シマンテック指定のハードウェアとソフトウェアを使用するお客様側の Managed PKI 管理者を通して、CPS に従って、証明書申請に含まれる情報を検証し、検証後の証明書申請を承認または却下して、シマンテックに発行を指示し、証明書の更新と失効を行うものとします。CPS は、PKI Manager で公開され、必要に応じて改正されます。Managed PKI 管理者が、お客様に代わって Managed PKI 管理者としての任務を果たす権限を取り消された場合、お客様はすみやかに当該 Managed PKI 管理者の管理者証明書の失効を要求するものとします。

(c) **存続** 契約で定められた終了規定に加えて、本サービス条件および CPS で定められた失効要件とセキュリティ要件は、契約の終了日または適用されるサービス注文の終了日を超えて、この取り決めに従って発行されたすべての証明書有効期間の終了まで存続するものとします。

(d) **お客様の保証** お客様は、契約で明示的に定められた限定的保証に加えて、以下の項目も保証するものとします。(i)証明書の発行に必要なすべての情報、およびお客様が検証する、またはお客様に代わって検証されるすべての情報が、重要なすべての点において真実であり正しいこと、(ii)証明書申請に対するお客様の承認が誤発行を引き起こさないこと、(iii)お客様が、CPS に十分に準拠していること、(iv)シマンテックに提出される証明書情報が第三者の知的財産権を侵害していないこと、(v)証明書申請に含まれる情報(電子メールアドレスを含む)が違法な目的に使用されたことがなく、今後も使用されないこと、(vi)お客様側の Managed PKI 管理者が、管理者証明書が作成されて以来、その管理者証明書の秘密鍵、およびその秘密鍵を守るためのチャレンジフレーズ、PIN、ソフトウェア、またはハードウェアメカニズムを扱う唯一の人物であり、今後もそうであり続けること、ならびに認可されていない人物がこれらの情報やシステムにアクセスしたことがなく、今後もアクセスしないこと、(vii)お客様が、本サービス記述書に準拠し認可された合法的な目的にのみ管理者証明書を使用すること、(viii)お客様が、シマンテックのシステムまたはソフトウェアの技術的実装を監視、妨害、リバースエンジニアリングせず、またはその他の方法でそれらのセキュリティを故意に侵害しないこと。

(e) **お客様の利用者** お客様は、この取り決めに従って証明書を受け取る利用者に、適切な利用規約の条項に従わせる義務を持つものとします。また、利用者は、証明書の登録条件としてその利用規約に合意するものとします。お客様は、その利用規約の条項によって、CA に対して CPS の条項と同等の安全性を保証するものとします。

(f) **現地法への準拠** お客様は、本サービス記述書に従ってシマンテックが生成した公開鍵/秘密鍵ペアの取得、使用、受領において、お客様がその鍵ペアを取得、使用、受領した管轄で適用されるすべての現地法や規定(輸出入に関する法律や規制を含むが、これに限定されない)に準拠する責任があります。

3. シマンテックの義務

(a) **サービス** 必要な導入作業の完了後、シマンテックは、本サービス記述書に明示されているサービスを、記載の条件に従って、サービス期間にわたってお客様に提供するものとします。シマンテックは、お客様およびお客様側の Managed PKI 管理者からの指示に従って証明書の発行、管理、失効、更新を行うものとします。シマンテックは、お客様から提出された適切な構造の XKMS 要求に従って、XKMS での公開鍵の登録、依拠する当事者への公開鍵の提供、公開鍵の登録取り消しも行うものとします。お客様が証明書申請を承認した後、シマンテックは(i)承認された各証明書申請に含まれる情報の正確性を信頼する権利を有し、(ii)その証明書申請を提出した証明書申請者に対して証明書を発行するものとします。本サービス記述書の下で発行または許諾された証明書(管理者証明書を含む)には、その証明書の発行日から最大 12 カ月の証明書有効期間が定められます。

(b) **管理者証明書** お客様が管理者証明書の証明書申請を提出した場合、シマンテックは、管理者証明書に必要な認証手続きを行ってから証明書申請を処理します。シマンテックは、管理者証明書の証明書申請が承認されたか却下されたかをお客様に通知します。Managed PKI 管理者が、管理者証明書を受け取るためにシマンテックから提供された PIN を使用した時点、またはその他の方法で管理者証明書をインストールまたは使用した時点で、Managed PKI 管理者による管理者証明書の受領が成立するものとします。Managed PKI 管理者は、管理者証明書の受け取りまたはインストール後、使用を開始する前に、証明書に含まれる情報を確認し、誤りがあった場合はすみやかにシマンテックに通知する必要があります。シマンテックは、このような通知を受け取った場合、その管理者証明書を失効させ、修正された管理者証明書を発行するものとします。

(c) **CA 鍵生成** 必要に応じて、シマンテックは、1 回の CA 鍵生成イベントで、お客様に代わってシマンテックが発行する証明書に署名するための CA 鍵ペアをお客様に生成するものとします。各ペアのお客様の秘密鍵は、1 つ以上の証明書署名ユニットに保管されるものとします。

(d) **シマンテックの保証** シマンテックは、シマンテックが証明書作成の際に注意を怠ったために証明書の情報に誤りが入り込むような事態が起きないことを保証します。

4. サービスの追加条項

(a) **CA 証明書** 各サービスアカウントには、少なくとも 1 つの CA 証明書が含まれます。特定数量に対する追加の CA 証明書は後から購入できます。シマンテックのシステムとサービスからの CA 証明書やその鍵ペアの抽出は、各当事者との同意に基づくものとします。

(b) **管理者キット** 管理者キットは、トークン、ソフトウェア、および 1 つの管理者証明書で構成されます。特定数量に対する追加の管理者キットは後から購入できます。

付録 D: LTE 証明書サービス

シマンテックの LTE サービス（以下「LTES」または「サービス」）では、プライベート階層内でデバイスを通信事業者の LTE 機器に統合するためのデバイス証明書を取得できます。お客様またはお客様の通信事業者は、CMP（Certificate Management Protocol）などのプログラム的なインターフェースを介してシマンテックに LTES の要求を送信します。

1. 定義

「管理者証明書」とは、お客様が任命したサービス管理者、または Managed PKI 管理者として任命されたその他の信頼される者に対し、Web ポータルにアクセスして LTE エンドエンティティのデバイス証明書を管理することを目的としてシマンテックが発行するクライアント証明書を指します。

「関連する個人」とは、お客様と関係のある人物を指します。(a)役員、取締役、従業員、パートナー社員、契約社員、インターン、その他お客様の組織内の人物、または(b)お客様の組織と契約関係を結び、身元を確実に保証できるビジネス記録をお客様が所有している人物が該当します。

「契約規約」とは、シマンテックとお客様の間で結ばれ、本サービス記述書に適用されるサービス注文書が発行された、プロフェッショナルサービス契約またはその他のマスター契約や規約を指します。

「認証局」または**「CA」**とは、証明書を発行、停止、失効する権限を持つ個人またはエンティティを指します。

「CMP」または**「Certificate Management Protocol」**とは、デバイス証明書の自動登録やライフサイクル管理に使用されるプロトコルを指します。デバイスは、CMP を介してシマンテックの PKI システムと直接通信します。デバイスから PKI システムに CMP 要求を送信できるようにするには、管理者が前もってそのデバイスを認可する必要があります。

「証明書有効期間」とは、証明書が発行された日時から有効期限が切れる日時までの期間を指します。

「通信事業者」とは、通常は他の国または地域に置かれ、シマンテックでお客様のサブアカウントとして扱われる、お客様の関連会社である企業体を指します。

「LTE 証明書」とは、名前、発行元 CA、通信事業者ネットワーク内のネットワーク構成要素などを含む、デバイスに保存されるメッセージを指します。ネットワーク構成要素には、通信事業者の基地局、セキュリティゲートウェイ、その他同様のデバイスが該当します。いずれの場合でも、LTE 証明書には、ネットワーク構成要素の公開鍵、証明書有効期間、証明書のシリアル番号、発行元 CA のデジタル署名が含まれます。

「プライベート階層」とは、お客様のルート CA から、1 つ以上の認証局、そして利用者へとつながるチェーンの中で、お客様が定めた手順に従って証明書を発行する一連の CA によるドメインです。

プライベート階層で発行される証明書は、組織が社内で発行を認可することを目的としており、公共のチャネルを介して組織や個人の間でやり取りすることは目的としていません。

「秘密鍵」とは、デジタル署名の作成に使用される数学的な鍵を指します。この鍵は他人に知られないように、所有者が秘密に保管する必要があります。アルゴリズムによっては、対になる公開鍵で暗号化された機密のメッセージやファイルを復号化するためにも使用されます。

「公開鍵」とは、対になる秘密鍵で作成された署名の検証に使用される数学的な鍵を指します。この鍵は一般に公開されます。アルゴリズムによっては、メッセージやファイルを暗号化するためにも使用されます。暗号化されたメッセージやファイルは、対になる秘密鍵で復号化できます。

「ルート CA」とは、信頼された階層のドメイン内で最上位に位置し、**「ルート証明書」**でルート CA として指定されるエンティティを指します。

「サービス管理者」とは、サービス記述書に記載されている証明書関連の管理業務を実行するために任命された、お客様側の信頼された従業員または信頼された関連する個人を指します。

「利用者」とは、証明書の主体であり、発行対象である、個人またはエンティティを指します。利用者は、発行時に証明書に含まれる公開鍵に対応した秘密鍵を使用でき、使用する権限を持ちます。

「利用規約」とは、利用者と CA またはシマンテックとの間で結ばれる、指定された証明書関連サービスのプロビジョニングに関する規約を指します。この規約により、証明書に関する利用者の権利と義務が定められます。

「ベンダー」または「製造元」とは、通信事業者にネットワーク構成要素を提供した企業体を指します（この 2 つの用語は区別なく使用されることがあります）。

「Web ポータル」とは、サービス管理者が LTE 証明書を要求するときにアクセスする、シマンテックでホストされる Web インターフェースを指します。

2. お客様の義務

(a) **任命** お客様は、認可された 1 人以上のお客様側または通信事業者側の従業員を、その雇用先企業体のサービス管理者として任命するものとします。お客様は、この取り決めに従って管理者証明書を受け取るサービス管理者に、その証明書に関連付けられた適用される利用規約の条項に従わせ、本サービス記述書に準拠し認可された合法的な目的にのみサービス管理者証明書を使用させる義務を持つものとします。かかる利用者がサービス管理者としての権限を取り消された場合、お客様はすみやかに当該の管理者証明書の失効を要求するものとします。

(b) **管理業務** お客様とその通信事業者は、任命したサービス管理者を通して、以下のうちの該当する業務の責任を持つものとします。

i. 通信事業者のサブアカウントの作成
ii. 証明書プロファイルの作成
iii. ベンダーへの CA 証明書の提供
iv. 検証のための IP アドレスブロックの提供
v. 新しいデバイスの登録と要求の事前承認の設定
vi. ネットワーク構成要素の CMP レスポンダ URL の設定

(c) **アカウント認可** お客様は、この取り決めに従って発行された LTE 証明書を受け取る権限を持つ通信事業者の事前認可を書面にてシマンテックに提供するものとします。この書類には、通信事業者の連絡先、サービス管理者として任命された人物の身元確認情報（登録に使用される情報を含む）、各通信事業者に認可された LTE 証明書と拠点の数などを記載します。お客様は、各サービス管理者が、適用されるサービス管理者証明書が作成されて以来、その証明書の秘密鍵、およびその秘密鍵を守るためのチャレンジフレーズ、PIN、ソフトウェア、またはハードウェアメカニズムを扱う唯一の人物であり、今後もそうであり続けること、ならびに認可されていない人物がこれらの情報やシステムにアクセスしたことがなく、今後もアクセスしないことを保証し、通信事業者にこれらを保証させる義務を持つものとします。

(d) **その他の義務** お客様は、シマンテックのシステムまたはソフトウェアの技術的実装を監視、妨害、リバースエンジニアリングせず、またはその他の方法でそれらのセキュリティを故意に侵害しないものとします。また、指定されたベンダーおよび製造元に対しても同様の義務を持つものとします。

(e) **存続** 契約で定められた終了規定に加えて、本サービス記述書で定められた失効要件とセキュリティ要件は、契約の終了日または適用されるサービス注文の終了日を超えて、この取り決めに従って発行されたすべての証明書有効期間の終了まで存続するものとします。

(f) **現地法への準拠** お客様は、本サービス記述書に従ってシマンテックが生成した公開鍵/秘密鍵ペアの取得、使用、受領において、お客様がその鍵ペアを取得、使用、受領した管轄で適用されるすべての現地法や規定（輸出入に関する法律や規制を含むが、これに限定されない）に準拠する責任があります。

3. シマンテックの義務

(a) **サービス管理者証明書** お客様から管理者証明書を要求されたときは、シマンテックは、必要な検証手続きが完了した後、その管理者証明書を適切なサービス管理者に提供します。サービス管理者が、管理者証明書を受け取るためにシマンテックから提供された PIN を使用した時点、またはその他の方法で管理者証明書をインストールまたは使用した時点で、管理者証明書の受領が成立したと見なされます。サービス管理者は、管理者証明書の受け取りまたはインストール後、使用を開始する前に、証明書に含まれる情報を確認し、誤りがあった場合はすみやかにシマンテックに通知する必要があります。シマンテックは、このような通知を受け取った場合、その管理者証明書を失効させ、修正された管理者証明書を発行するものとします。

(b) **サービス構造** シマンテックは、シマンテックの標準 PKI 手順とポリシーに従って、お客様の 2 つのルート証明書、およびオプションで各ルート証明書の下で発行される最大 2 つまでの CA 証明書を作成およびホストします。この CA 証明書は、この取り決めに従ってお客様に本サービスを提供することのみを目的としています。追加の CA 証明書は別途購入できます。シマンテックは、お客様からの要求に基づき、標準の PKI 手順とポリシーに従って通信事業者を本サービスに追加し、そのサブアカウントを作成します。

(c) **IP アドレス設定** 新しい通信事業者を追加する際に、有効な IP アドレスの範囲をシマンテックに提供していただきます。シマンテックのシステムは、有効な IP アドレスから送られた CMP 要求にのみ応答し、それ以外の IP アドレスから送られた要求はすべて拒否します。この設定は、通信事業者側で行っていただく必要があります。

(d) **サービス** 本サービス記述書の第 2 項(c)に従ってお客様が認可した数の証明書をサービス管理者が Web ポータルから要求したとき、シマンテックは(i)各証明書要求に含まれる情報の正確性を信頼し、(ii)要求元のサービス管理者に対して証明書を発行および提供する権利を有するものとします。本サービス記述書の下で発行または許諾されたデバイス証明書は、(i)証明書の発行日から 1 年、2 年、または 3 年の証明書有効期間が定められ、(ii)その証明書要求で指定されていないデバイスには統合またはインストールできないものとします。シマンテックは、前述の要件に従って、すべての注文を受領順に履行します。本条件の条項と矛盾する場合でも、証明書を要求できる通信事業者の数、および証明書の要求元となる拠点とサービス管理者の数は、適用されるサービス注文書で指定された数に厳格に制限されます。

(e) **アカウントの有効化** サービス注文書を通した料金の前払いを前提として、(i)必要な登録手続きの完了、(ii)通信事業者とそのサービス管理者の認証(シマンテックが認証手続きを滞りなく行えるように、この期間中、サービス管理者は常に連絡可能であることが求められます)という要件が満たされた時点で、シマンテックは、米国内では 10 営業日以内、米国外では商業上道理にかなった期間を基準に、商業上道理にかなった労力を費やしてサブアカウントを有効化するものとします。

(f) **シマンテックの保証** シマンテックは、シマンテックが証明書作成の際に注意を怠ったために、この取り決めに従って発行される証明書に誤りが入り込むような事態が起きないことを保証します。

(g) **監査権** シマンテックは、お客様の手続きが本サービス記述書の条項に準拠していることを確認するため、年 1 回以上の監査を行うことがあります。このような監査は、文書によってお客様に妥当な通知が送られた後、営業時間内に、お客様の業務を不当に妨害することなく行われます。お客様は、これらの監査において合理的な範囲でシマンテックに協力するものとします。監査によってお客様が本サービス記述書に記載の条件の条項に違反していることが明らかになった場合、(i)お客様はシマンテックに相応の監査実施費用を支払い、(ii)シマンテックは上記の年 1 回の監査に加え、必要に応じて、適用される条項への準拠を徹底するための追加監査を実施できるものとします。年 1 回の定期監査は、前年の活動のみを対象とすることができます。