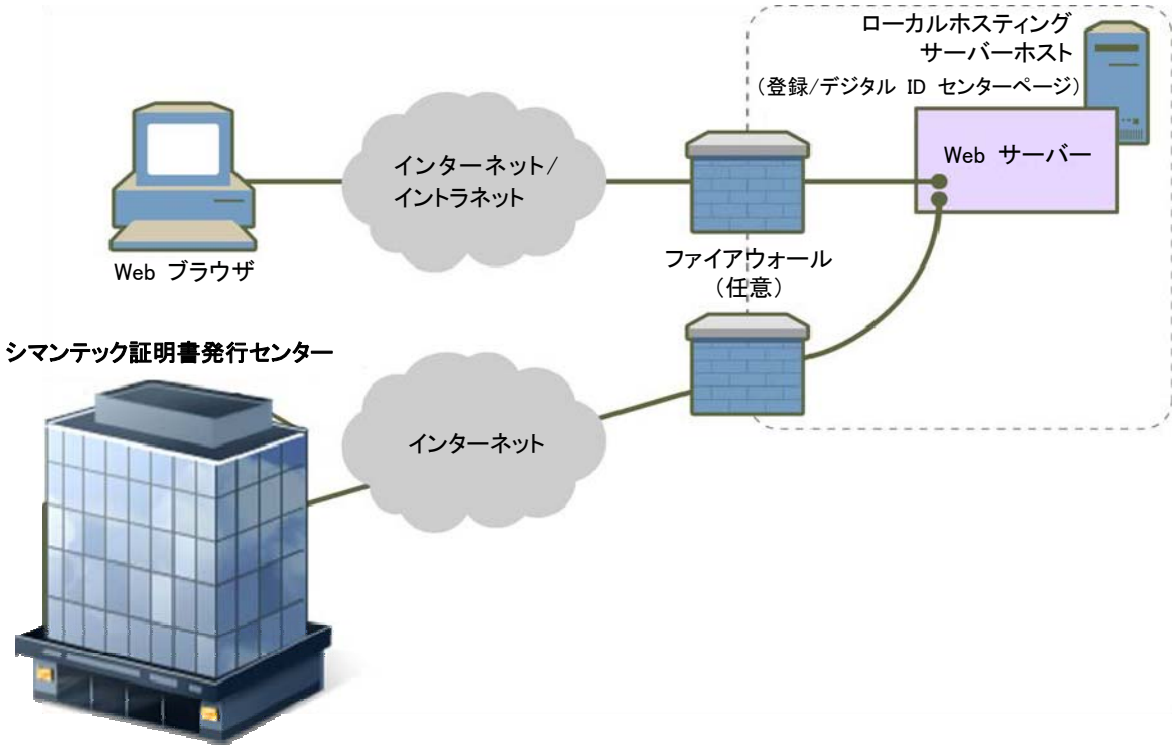
Symantec Managed PKI 認証サービス記述書(バージョン 7.xおよびそれ以前)

はじめに

Symantec Managed PKI Service は、社内で運用管理する PKI ソフトウェア/ハードウェア、一般的なアプリケーションとの互換性、シマンテックの証明書処理サービス/インフラを組み合わせた、統合 PKI プラットフォームを提供します。

PKI ソリューションを独自に実装しようとすると、システム、通信、データベースの設定、運営場所の物理的なセキュリティの確保、インターネットからの攻撃を防ぐ安全なネットワークの構成、高い可用性を維持するための冗長システムの設計、ディザスタリカバリの計画といった作業をすべて行い、PKI に関連する法令に適時準拠し、PKI の専門技能者の雇用を検討することが必要になります。Managed PKI Service では、シマンテックが運用する可用性とセキュリティに優れた PKI バックエンドをインフラとして利用できます。これにより、独自の PKI システムの購入や管理によって生じるリスク、労力、コストを負担せずに PKI 環境を整えることができます。Managed PKI Service は世界規模で企業をサポートしているので、アジアやヨーロッパの主要な言語でデジタル証明書のユーザー登録や内容確認ができます。

図 1 - 一般的なローカルホスティング構成
注: 点線内のシステムはお客様側に設置されます。



主要機能

- Managed PKI デジタル ID センター
  デジタル ID センターページは、エンドユーザー証明書の登録を受け付けるページで、シマンテック側とお客様側のどちらでホストするかを選択できます。**シマンテックでのホスティング**を選択した場合は、シマンテック証明書発行センターでホストされます。**ローカルでのホスティング**(**図 1**)を選択した場合は、お客様が独自の Web サーバーで管理します。どちらでホストする場合でも、証明書の発行はシマンテックが行います。ローカルでホスティングする場合は、デジタル ID センターページに独自のテキスト、リンク、ロゴを追加してページをカスタマイズし、コブランド化できます。また、ローカルホスティングを使用した構成では、自動認証や認証業務代行サービスなどを実装する必要があります。

- Managed PKI コントロールセンター
  Managed PKI コントロールセンターでは、証明書の登録から承認、失効、更新までのライフサイクルプロセスを管理できます。お客様は、登録プロセスと認証プロセスのすべてを操作できます。Managed PKI 管理者を必要な人数だけ指定して、役割を分担できます。Managed PKI Service 管理者は、組織で定められた手順に沿って適切に認証されたユーザーやエンティティのみにデジタル ID が発行されるよう適切に運営する必要があります。管理者は、まず、証明書要求を審査して、承認または却下します。また、証明書失効リスト(CRL)をダウンロードして、無効な証明書がシステムで受け入れられないようにします。さらに、レポートの生成、Managed PKI Service の運用状況の監視、デジタル ID の使い方をユーザーに指示することもできます。Managed PKI コントロールセンターは、シマンテックのデータセンター内にあります。

- シマンテック証明書発行センター
  シマンテック証明書発行センターでは、証明書の新規発行要求や更新要求が処理されます。Managed PKI Service 管理者が要求を承認すると、証明書発行センターで証明書が発行され、証明書の受け取り方法を知らせる電子メールが申請者に送信されます。証明書発行センターでは、レポートや CRL の生成も行われます。Managed PKI Service 管理者はこれらを使用して、Managed PKI Service カスタマーアカウントを管理できます。証明書発行センターは、シマンテックのデータセンター内にあります。

- 認証方法
  Symantec Managed PKI Service では、手動認証、パスコード認証、自動認証のいずれかの方法で要求を認証および承認できます。

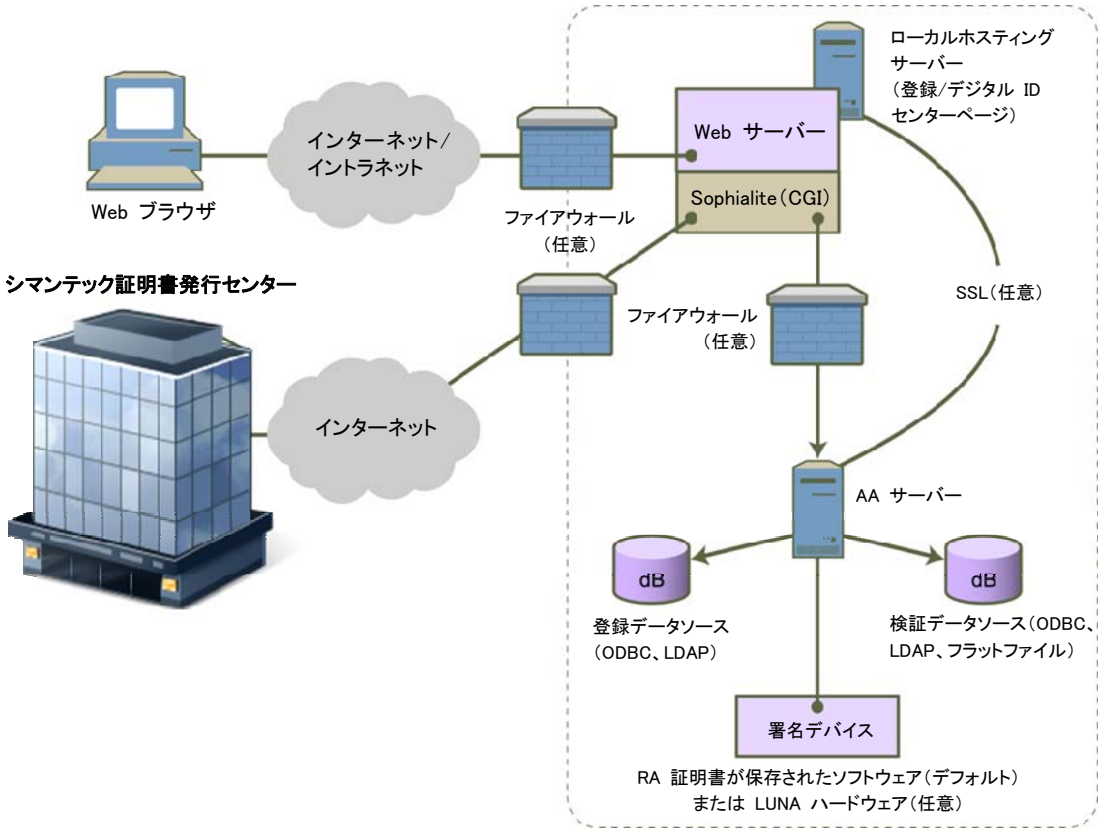
  手動認証
  手動認証では、管理者が証明書要求を 1 つ 1 つ審査して、承認または却下します。管理者の負担が大きくなるため、証明書の発行数が多い組織にはあまり適していません。

  パスコード認証
  パスコード認証では、証明書要求の認証を自動化できます。管理者は、Managed PKI コントロールセンターでパスコード認証の設定を行います。利用者が証明書を要求すると、管理者が SSL 通信を通じて、事前にシマンテックにアップロードされた登録情報と照合されます。組織が定める承認基準に従って、証明書要求が承認または却下されます。自動認証とは異なり、パスコード認証では、お客様側で認証サーバーを構築および管理する必要はありません。認証はすべて、管理者がアップロードした利用者データに基づいてシマンテック側で行われます。そのため、パスコード認証は自動認証に比べて実装が簡単ですが、柔軟性はやや劣ります。

  自動認証
  自動認証(AA)オプションでは、証明書の申請を自動化できます。管理者による情報の登録は必要ありません。**図 2** を参照してください。自動認証では、証明書の申請者から提供された登録データが組織のデータソース(人事データベースや LDAP ディレクトリなど)と照合されます。申請者が認証される(データが一致する)と、要求が承認されます。自動認証 API を使用すれば、承認された要求データを自動的に追加できます。シマンテックで要求が受け付けられた時点で、新しい証明書にデータが追加されます。このように、証明書の承認および発行プロセスをカスタマイズしながら自動化できます。自動認証サーバーはお客様側に置きます。

図 2 – 一般的な自動認証構成

注: 点線内のシステムはお客様側に設置されます。次の図で使われている用語の定義は以下のとおりです: RA – 登録局(Registration Authority)、LUNA ハードウェア – 証明書署名ハードウェア、LDAP – Lightweight Directory Access Protocol、ODBC – Open Database Connectivity、Sophialite(CGI) – ローカルでホストされている証明書登録ページから利用者登録データを受け取るシマンテック CGI(Common Gateway Interface)プログラム



追加オプション

以下の追加オプションを有料で利用できます。

- プレミアムバリデーションサービス: 証明書の失効をいくつかの方法で確認できます。
  - リアルタイムバリデーションサービス

    このサービスでは、OCSP(Online Certificate Status Protocol)または XKMS(XML Key Management Specification)を使用して証明書を確認できます。対応アプリケーションでは、証明書の失効ステータスが自動的に認識されます。失効ステータスには、有効、失効、停止、期限切れ、不明の 5 種類があります。OCSP の場合は、ユーザーが Web サーバーやその他のネットワークリソースに証明書を提示したときに、CVM(Certificate Validation Module)が認証局(CA)に証明書ステータスを要求します。XKMS の場合は、アプリケーションが XKMS クライアントと連携して、XKMS クライアントが CA に証明書ステータスを要求します。

– プレミアム CRL サービス

このサービスでは、シマンテックが CRL の更新を 1 日ごとではなく 1 時間ごとに行います。ユーザーが Web サーバーやその他のネットワークリソースに証明書を提示したときに、対応アプリケーションが証明書を CRL と照合します。証明書が失効している場合は、ユーザーはリソースにアクセスできません。証明書がリストにない場合は、ユーザーはリソースにアクセスできます。

- 鍵管理サービス: Managed PKI Service では、集中型の鍵生成、秘密鍵のバックアップ、分散型のキーリカバリの実現によって、利用者秘密鍵に対するセキュリティを最大限に高めることができます。デュアルキーペアの生成もサポートされているので、暗号化用の鍵ペアと署名用の鍵ペアを別々に発行およびバックアップできます。

パブリック証明書

パブリック証明書は、Symantec™ Trust Network(STN)に属しています。STN は、世界中の認証局 の信頼ネットワークに基づくグローバルに相互運用可能なデジタル証明書基盤です。STN の最上位認証局(ルート CA)は、一般的なブラウザ、サーバー、電子メールアプリケーションに前もって登録されています。そのため、パブリック証明書は、証明書ユーザー側で特別な準備をしなくてもさまざまな組織間で使用できます。Symantec Managed PKI コブランド証明書サービスはパブリック認証局の下で提供されるため、お客様はシマンテックの認証局運用規定(CPS)に準拠する必要があります。

プライベート証明書

お客様が Symantec Managed PKI プライベート証明書サービスに登録した場合は、プライベートな 信頼階層構造の最上位となるお客様独自のルート CA のキーセレモニーをシマンテックが実施します。キーセレモニーとは、セキュリティ保護された環境で厳密な手順に従って秘密鍵/公開鍵ペアを生成する手続きのことです。プライベート証明書は、通常、イントラネットや仮想プライベートネットワーク(VPN)などの社内アプリケーションで使用します。場合によっては、Web アクセスに使用されることもあります。プライベートドメインの外部で使用することもできますが、その場合は、事前に通信する相手に対して自社のルート証明書を配布する必要があります。プライベート認証局を運用する組織は、証明書の使用ルールや手順を独自に定めてそれに従う必要があります。

注:IPSec を実装した VPN を使用するためには、プライベート証明書が必要です。

付録 A – MPKI コブランド証明書サービス利用規約

1. 定義

「管理者証明書」とは、Managed PKI 管理者として指定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、Managed PKI コントロールセンター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。

「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(PKI)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 Managed PKI コントロールセンターに掲示することによって、お客様が任命した登録局の Managed PKI 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 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、STN CPS 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、これらに限定されません。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 Managed PKI コントロールセンター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、CPS に定められた 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、契約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。本契約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 – MPKI プライベート証明書サービス利用規約

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、Managed PKI コントロールセンター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。

「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 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。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、契約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) 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。本契約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、Managed PKI コントロールセンター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。

「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(PKI)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 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、

Managed PKI コントロールセンターで公開され、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、契約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。本契約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 – 鍵管理サービス利用規約

1. 定義

「誤キーリカバリ」とは、(a)適用される CPS で定められた手順とは大きく異なる方法で秘密鍵のリカバリと伝達を行うこと、(b)秘密鍵の正当な所有者である利用者以外の人物に対して秘密鍵のリカバリと伝達を行うこと、(c)秘密鍵の正当な所有者である利用者の認可なく秘密鍵のリカバリと伝達を行うことを指します。

上記にかかわらず、以下のことは誤キーリカバリには該当しません。(d)捜査令状や召喚状に応じて、利用者の秘密鍵をお客様がリカバリし、警察や司法当局者に伝達すること、(e)裁判手続きや行政手続きでの求めに応じて、利用者の秘密鍵をお客様がリカバリし、伝達すること、(f)利用者の認可がない場合を含め、お客様側の正当な理由のある合法的な業務目的で、秘密鍵を使用してメッセージを復号化するために、利用者の秘密鍵をお客様がリカバリすること。

「キーマネージャ管理者」とは、信頼できるシステムを使用して鍵ペアを生成し、公開鍵と秘密鍵のリカバリ情報をシマンテックに送信して、秘密鍵を保管し、秘密鍵を利用者に伝達する責任を持つ、お客様が指定した人物を指します。

「なりすましキーリカバリ」とは、第三者が実際の利用者のふりをして名前や身元を偽った情報を提出し、その利用者の秘密鍵をお客様に要求して、お客様から受け取ることを指します。

KMS.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キーマネージャ管理者(「KMA」)として任命するものとします。複数の KMA を任命して、セキュリティ管理者やキーリカバリ担当者など、異なる役割を分担できます。セキュリティ管理者の役割を持つ KMA のみが、お客様に代わって追加の KMA を任命する権利を有するものとします。KMA がキーリカバリの権限を持たなくなった場合、お客様は Managed PKI コントロールセンターから当該の権限を失効させるものとします。お客様は、鍵管理サービス管理者ガイドに記載の適用される要件に準拠する義務があります。このガイドは、Managed PKI コントロールセンターで公開され、必要に応じて改正されます。シマンテックは、改正の内容を Managed PKI コントロールセンターに掲示することによって、お客様が任命した KMA に通知するものとします。

(b) 管理業務 お客様は、鍵管理サービス管理者ガイドに記載の要件に準拠するものとします。これには、証明書申請者に代わって鍵ペアを生成すること、その証明書申請者に発行する証明書に含める公開鍵をシマンテックに伝達すること、キーリカバリ情報をシマンテックに伝達すること、秘密鍵のリカバリを希望する利用者からの要求を検証して要求者が確かに利用者本人であることを確認すること、その要求を承認または却下すること、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こと、統合認証 Managed PKI 鍵管理サービスを使用して秘密鍵のリカバリに必要な情報を要求すること、リカバリした秘密鍵を要求者である利用者に伝達すること(必要な場合)などに関する要件が含まれます(ただしこれらに限定されません)。

お客様は、信頼できるシステムを使用して鍵ペアを生成し、公開鍵と秘密鍵のリカバリ情報をシマンテックに送信して、秘密鍵を保管し、秘密鍵を利用者に伝達するものとします。

(c) 業務遂行 お客様は、上記 KMS.2 の(b)項に示した業務を、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遂行するものとします。お客様は、本サービス記述書の下で提供されるシマンテックのソフトウェアとサービスを、合法的な目的および鍵管理サービス管理者ガイドに準拠した目的にのみ使用するものとします。

(d) お客様の保証 お客様は、本契約において適用される各サービス記述書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)お客様が提出する利用者の秘密鍵リカバリ要求が、実際にその利用者からお客様に提出され、認可されたものであること、(ii)利用者の許可なくお客様が提出する利用者の秘密鍵リカバリ要求が、正当な理由のある合法的な業務目的によるものとしてお客様が認可していること、(iii)上記の一般論に制限されることなく、お客様が提出する利用者の秘密鍵リカバリ要求が誤キーリカバリを引き起こさないこと、(iv)お客様が、鍵管理サービス管理者ガイドに十分に準拠していること。

(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。

KMS.3. シマンテックの義務

シマンテックは、Symantec Managed PKI Service for Windows と同時に使用するための、本書で定められた鍵管理サービスを提供するものとします。

(a) KMA 証明書 KMA の証明書申請が承認されたときは、シマンテックは、本サービス記述書の下で提供されるサービスにアクセスするための KMA 証明書または管理者証明書(いずれか適切な方)を当該の各 KMA に発行するものとします。

(b) 証明書への公開鍵の埋め込み お客様が証明書申請の承認後、証明書申請者に代わって鍵ペアを生成し、シマンテックに公開鍵を伝達したときは、シマンテックは、適用される Symantec Managed PKI Service for Windows サービス条件に従って、その公開鍵を証明書に埋め込み、証明書を発行するものとします。

(c) シマンテックによる集中型の鍵管理サービス。お客様が鍵管理サービス管理者ガイドに従って

生成または承認した利用者の秘密鍵をお客様側の KMA から求められたときは、シマンテックはその要求を認証するものとします。要求の正当性が確認された場合、シマンテックは、利用者の秘密鍵をリカバリするために必要なキーリカバリ情報をお客様に提供するものとします。

KMS.4. 秘密鍵の要求に関する責任

お客様は、お客様がシマンテックに提出するすべての秘密鍵リカバリ要求の生成または認証に関して、およびお客様側の KMA の業務遂行に関して、全責任を負うものとします。シマンテックは、これに関する一切の責任を免責されるものとします。