Symantec™ Custom Device Certificate Service の説明

はじめに

お客様は、Symantec™ Custom Device Certificate Service（以下、「CDCS」または「本サービス」）を利用して、シマンテックがホスティングするサービスコンソール経由でお客様または製造元からシマンテックに送信された一括証明書署名要求に基づき、特定のハードウェアデバイスに組み込むためのプライベート階層のデバイス証明書を入手できます。

条件

1. 定義

「管理者証明書」とは、サービスコンソールにアクセスして CDCS エンドエンティティデバイス証明書を要求する目的でのみ、お客様が指定したサービス管理者にシマンテックが発行するクライアント証明書のことです。

「管理者キット」とは、USB トークンと延長ケーブル、またはその代替となる強力な 2 要素認証デバイス、関連するソフトウェア、当該キットの 1 年間の保守およびサポートから成るキットのことです。

「契約書」とは、本サービス説明に付加されるサービス注文が発行される根拠となる、シマンテックとお客様の間で締結されたマスターサービス契約書のことです。

「証明書」または**「電子証明書」**とは、少なくとも、発行元 CA についてその名前を記載するか特定し、申請者を特定し、申請者の公開鍵を含み、証明書の有効期間を特定し、証明書のシリアル番号を含み、発行元 CA の電子署名を含むメッセージのことです。このサービス注文の目的に応じて、これらの用語は、特に言及されていない限り、CDCS エンドエンティティデバイス証明書に関連するものと見なされます。

「認証局」または**「CA」**とは、証明書の発行、保留、失効に関する権限を有する個人または主体のことです。

「製造元」とは、事業主体のことで、(i)お客様が本サービス説明に従って発行される証明書を受け取る権限を当該主体に付与済みであり、かつ(ii)お客様と当該主体との間で正当に履行される完全に有効な電子証明書契約が存在する場合を指します。かかる事業主体は、たとえば、お客様によって電子証明書を受け取る権限を付与されたデバイスを製造している場合がありますが、それに限定されません。

「有効期間」とは、証明書が発行される日時から始まり、証明書が期限切れになる日時で終了する期間のことです。

「秘密鍵」とは、電子署名の作成、およびアルゴリズムによっては、対応する公開鍵を使って（秘密保持のために）暗号化されたメッセージまたはファイルの復号化に使用される、（保持者が公開しない）数学的な鍵のことです。

「公開鍵」とは、だれでも利用できるように公開でき、対応する秘密鍵を使って作成された署名の検証に使用される、数学的な鍵のことです。アルゴリズムによっては、公開鍵はメッセージまたはファイルの暗号化にも使用されます。暗号化したメッセージやファイルは、対応する秘密鍵を使って復号化できます。

「CDCS 顧客 CA」とは、Symantec™ CDCS ルート証明書によって署名され、本契約の詳細な説明に従ってお客様向けのエンドエンティティデバイス証明書を発行するために使用される、電子証明書のことです。

「サービス管理者」とは、本サービス説明に記述されている特定の証明書関連の管理機能を実行するように指名された、お客様または製造元の信頼できる従業員のことです。

「サービスコンソール」とは、デバイス証明書を要求する目的でサービス管理者がアクセスできる、シマンテックがホスティングする Web インターフェースのことです。

2. お客様の義務

(a)指定。お客様は、承認されたお客様、製造元の両方またはいずれかの 1 人以上の従業員を、かかる人員を雇用する主体のためのサービス管理者として指定するものとします。お客様は、ここに規定する管理者証明書を受領するサービス管理者に対し、かかる証明書と関連する適用可能な利用規約の条項に従うこと、およびサービス管理者証明書を本契約と矛盾しない承認された合法的な目的にのみ使用することを要求するものとします。申請者が承認されたサービス管理者でなくなった場合、お客様は直ちに、該当する管理者証明書の失効を要求しなければなりません。お客様は、サービス管理者 1 人につき 1 つの管理者キットを購入する必要があります。

(b)管理者の機能。お客様、その製造元の両方またはいずれかは、適切な場合には、指定されたサービス管理者を通して、デバイス証明書要求内の情報の検証、サービスコンソールを使用したデバイス証明書要求の送信、およびデバイス証明書の当該の証明書要求で特定された対応するデバイスへの統合に関する責任を負うものとします。お客様は、証明書の発行に必須であり、かつ、お客様またはかかる製造元（該当する場合）によってまたはそれに代わって検証されるすべての情報が、すべての必須事項において事実かつ正しいことを保証し、その製造元が同様の保証をするように要求するものとします。

(c)当事者の関係。各当事者は、本契約またはお客様と製造元との間のいずれかの契約にこれと矛盾するいかなる文言がある場合でも、本サービス説明に従っ

て提供されるサービスに関してシマンテックがお客様の限定的な代理人と見なされることに同意します。さらに、お客様は、ここに説明されている証明書を受領するためにお客様が行ういかなる製造元の承認よりも前に、かかる代理行為について規定するかかる製造元との間の書面による電子証明書契約を締結すること、それによって、シマンテックに対し本サービス説明の条件より不利にならない責任の制限、拒否事項、および免責保護を提供し、当該製造元が本契約の受益者である第三者とは見なされないことを条件として要求することになります。お客様は、本サービス説明に従って発行される証明書の受領に関連して、製造元によって支払われるべきいかなる料金の賦課、回収の両方またはいずれかについての全責任を単独で負うものとします。

(d)アカウントの承認。お客様はシマンテックに対し、本サービス説明に従って発行される証明書を受領する権限を付与されるいかなる製造元についても、かかる製造元の連絡先情報、かかる製造元のサービス管理者として指名された個人を特定する情報(そのための登録情報を含む)、証明書の数、サイトの数、または、承認を受けた各製造元に対応する管理者キットの数を含む、事前の書面による承認を提供するものとします。

(e)その他の義務。お客様は、適用可能なサービス管理者証明書の作成時点以降、各サービス管理者が、かかる証明書の秘密鍵、すべてのチャレンジフレーズ、PIN、秘密鍵を保護するソフトウェアまたはハードウェアメカニズムを保持する唯一の個人であり続けたこと、今後もそうあり続けること、また権限のない個人がかかるデータまたは情報にアクセスしたことはなく、今後もアクセスしないことを保証し、その製造元が同様の内容を保証するように要求するものとします。お客様は、シマンテックのいかなるシステムまたはソフトウェアに対しても、その技術的実装の監視、干渉、リバースエンジニアリングを行わず、その他の方法でかかるシステムまたはソフトウェアのセキュリティを故意に危殆化しません。さらに、お客様は、任命した製造元に同様の制限を課すものとします。

(f)現地法への準拠。お客様は、シマンテックがこのサービス説明に従って生成した公開鍵と秘密鍵のペアを取得、使用、承認するにあたり、かかる鍵ペアをお客様が取得、使用、承認、または他の方法で受領する管轄地域の適用可能な法律、規則、および規制(輸出入に関する法律、規則、および規制が含まれそれに限定されません)に準拠することを保証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。お客様によって要求された管理者証明書に必要なシマンテックの検証手続きが正常に完了した時点で、シマンテックは、かかる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、シマンテックから提供された PIN を使用して管理者証明書を入手するか、または他の方法で管理者証明書をインストールまたは使用すると、当該管理者証明書を承認したものと見なされます。サービス管理者が管理者証明書を入手するか、または他の方法でインストールした後、サービス管理者は、その使用を開始する前に当該管理者証明書内の情報を確認し、見つかったエラーについて直ちにシマンテックに通知しなければなりません。シマンテックは、かかる通知を受領した時点で当該管理者証明書を失効させて、訂正された管理者証明書を発行できます。

(b)サービス構造。シマンテックは、実質的にシマンテックの標準 PKI 方式とポリシーに従って、1 つの CDCS 顧客ルート CA 証明書およびかかる CDCS ルート証明書の下で発行される 1 つの CDCS CA 証明書を作成し、ホスティングします。それらの証明書は、本サービス説明に従ったサービスをお客様に(またはお客様の書面による明確な同意がある場合に限り、他のシマンテックのお客様に)提供する目的でのみ使用されます。追加の CDCS CA は別途購入できます。

(c)サービスの提供。本サービス説明のセクション 2(d)に従ってお客様により承認された証明書の要求数に応じて、サービス管理者がサービスコンソールを使用して証明書要求を送信した時点で、シマンテックには、(i)かかる各証明書要求に含まれる情報の正確性を信頼する、さらに(ii)要求元のサービス管理者にかかる証明書を発行および提供する権限が付与されるものとします。本契約に従って発行またはライセンス付与されるデバイス証明書については、(1)当該証明書が発行された日から 20 年の有効期間を有し、(2)20,000 通を超えない一括サイズで証明書を要求する必要があり(それよりも大きい一括バッチ要求および鍵の長さが 1024 ビットを超える証明書の要求は、シマンテックの単独の裁量により拒絶されることがあります)、および(3)適切な証明書要求に対応しないいかなるデバイスにも統合またはインストールできません。シマンテックは、前記の要件を満たす受信したすべての注文を履行します。本サービス説明にそれとは矛盾するいかなる規定がある場合でも、証明書を要求できる製造元の数、証明書を要求できる運用サイトおよびサービス管理者の数は、該当するサービス注文に指定された数までに厳密に制限されます。

(d)アカウントのアクティブ化。シマンテックは、サービス注文経由の事前のご購入を条件として、国内のサイト向けにはお客様による適切な製造元の承認を受領してから 10 日以内に、国外サイト向けには特殊な手続きまたは行政上の要件に適合するための商業上合理的な期間内に、管理者キットを出荷するため商業上合理的な努力を払うものとします。シマンテックは、管理者キットの配送に続いて、国内アカウントについては 10 営業日以内、国外アカウントについては以下の要件を満たすための商業上合理的な期間内に、アカウントをアクティブ化するための商業上合理的な努力を払いま

す。(i)必須の登録手続きの完了、(ii)製造元およびそのサービス管理者の認証(サービス管理者は、シマンテックがタイムリーな方法で認証を実行するために、この期間中にアクセス可能になっている必要があります)、(iii)USB トークンのインストール、およびサービス管理者証明書の USB トークンと復号化ユーティリティへのダウンロード。

(e)シマンテックの保証。シマンテックは、証明書作成時にシマンテックが合理的な注意を払うことが出来なかった結果として、本サービス説明に従って発行される証明書にシマンテックが発生させたエラーがないことを保証します。