日本ベリサイン株式会社
認証業務運用規程
（Certification Practice Statement）

Version 3.7

Effective Date: 2009/05/01

日本ベリサイン株式会社
東京都中央区八重洲 2 丁目 8-1
TEL: 03-3271-7011
http://www.verisign.co.jp/

日本ベリサイン Certification Practice Statement

Trademark Notices

謝辞

本文書の作成及び検討に際して、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、日本ベリサイン株式会社（以下「日本ベリサイン」という）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、日本ベリサイン認証機関が VeriSign Trust Network 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、失効及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、VTN を統治するポリシーの最上位文書である。ビジネス、法的、また、VTN 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。VTN 基準と呼ばれるこれらの要求事項は、VTN のセキュリティと完全性を維持し、全 VTN 参加者に適用され、それゆえ、VTN 全体に一定の信頼という保証を提供する。VTN と VTN 基準に関する詳細な情報は、CP に記載されている。

日本ベリサインは、サブドメインと呼ばれる VTN の一部について権限を有している。日本ベリサイン・サブドメインは、カスタマ、利用者及び依拠当事者などの日本ベリサインの下位に位置するエンティティを含む。

CP は VTN 参加者が充足すべき要件を規定する一方、本 CPS は、日本ベリサイン・サブドメイン内で当該要件をどのように日本ベリサインが充足するかを定めるものである。特に、本 CPS は、CP 及び VTN スタンダードの要件に従い、VTN の日本ベリサイン・サブドメイン内において、日本ベリサインが採用する次の実務について記載する。

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

VTN 内の日本ベリサイン・サブドメインは、CP と VTN 基準を満たすことが求められる。

本 CPS は、CP 及び本 CPS の構成について Internet Engineering Task Force (IETF) RFC 3647 に従う。

1.1 概要

日本ベリサインは、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化モジュール等の、認証機関システムを収容する安全な施設を有している。日本ベリサインは、VTN 内で認証機関となり、証明書のライフサイクル（発行、管理、失効及び更新）に関するサービスを提供する。また、日本ベリサインは、自らのエンタープライズ・カスタマもしくは日本ベリサイン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、認証機関の鍵管理及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、日本ベリサインは、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）及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。日本ベリサインの提供する上記以外のサービスまたは米国ベリサインが日本ベリサイン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。

- VTN をサポートする、米国ベリサインの第一次認証機関、日本ベリサインのインフラストラクチャ認証機関及び日本ベリサインの管理認証機関
- 日本ベリサインのパブリック認証機関及び VTN の日本ベリサイン・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 は日本ベリサイン・サブドメイン内における全ての個人及び組織（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 VTN サービスの利用にも適用され

る。日本ベリサイン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。日本ベリサイン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。

VTN 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 VTN スタンダードを設定する文書である。

日本ベリサインは、VTN のサブドメイン内で 3 種類(Class1,2,3)の Class の証明書を提供する。本 CPS は、日本ベリサイン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及び管理に関する実務と手続きを対象とする文書である。

日本ベリサインは、政府の要求事項または業界の標準及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及び依拠当事者に適用されるものとする。

本 CPS は、日本ベリサイン・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 及び CPS を補足するセキュリティ及び運用に関する機密文書で、以下のものを含む。
  - VTN 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、米国ベリサインの“Physical Security Policy”
  - 人的、物理的、電気通信、論理的及び暗号鍵管理のセキュリティに関する米国ベリサイン及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”

- 日本ベリサインが制定する付属契約。当該付属契約は、日本ベリサインのカスタマ、利用者及び依拠当事者を拘束する。特に、VTN スタンダードからこれらの VTN 参加者に至る契約がある場合において、VTN 参加者がどのようにして VTN 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、VTN の日本ベリサイン・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、VTN 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、日本ベリサインの CPS である。VTN 証明書は、各 VTN 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、日本ベリサインは、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 CP セクション 7.1.6 に従い使用される。

1.3 PKI参加者

1.3.1 認証機関

認証機関という用語は、VTN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[1]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、米国ベリサインのエンティティである。第一次認証機関の下位に属する日本ベリサインの認証機関は、利用者または他の認証機関に証明書を発行する。

また、米国ベリサインは「ベリサイン・ユニバーサル・ルート認証機関」を管理する。ベリサイン・ユニバーサル・ルート認証機関は、特定の認証Classで定義されるものではなく、下位認証機関の任意のClassを発行する場合がある。

日本ベリサインのエンタープライズ・カスタマは、米国ベリサイン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、VTN CP及び日本ベリサインの本CPSの全要件を順守するために、日本ベリサインと契約を締結する。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。

セキュア・サーバ認証機関は、各第一次認証機関の下にあるそれぞれのClassに技術的に属さないVTN認証機関である。本認証機関は、ルートまたは第一次認証機関のような上位認証機関を有さない。むしろ、セキュア・サーバ認証機関は、それ自身のルートとして、自己署名ルート証明書を発行する。セキュア・サーバ認証機関は、エンドユーザの利用者へも証明書を発行する。従って、セキュア・サーバ階層は、セキュア・サーバ認証機関だけにより成り立っている。セキュア・サーバ認証機関は、Class3組織向け証明書とみなされるセキュア・サーバIDを発行する。

セキュア・サーバ認証機関は、VTN内における他のClass3認証機関と実質的に同様の証明書に関するライフサイクルの運用を行う。従って、米国ベリサインは、VTN内でセキュア・サーバ認証機関をClass3認証機関として承認しかつ指定する。セキュア・サーバ認証機関が発行する証明書は、他のClass3組織向け証明書と同等の信頼性についての保証を提供するものとみなされる。

1.3.2 登録機関

登録機関は、VTN 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。日本ベリサインは、自らが発行する証明書の登録機関になることができる。

日本ベリサインと契約を締結する第三者は、自らの登録機関となり、日本ベリサイン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、VTN のCP、本CPS及び日本ベリサインと締結する契約に定める全ての要件を遵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。[2]

1.3.3 エンド・エンティティ

VTN のエンド・エンティティは、VTN 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

[1] VTN では現在 Class 4 証明書の発行は行われていない。
[2] 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。

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日本ベリサイン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VTN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」及び「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 VTN 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 VTN 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及び電子メールを暗号化するため、及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書の利用形態は、以下の Table1 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、VTN CP、発行された証明書の根拠となる本 CPS 及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及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、VTN CP、発行された証明書の根拠となる本 CPS 及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	中	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		✓		✓	✓	✓	✓

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、Class1 及び 2 に関連して、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、商業用及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、Class1 及び 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及び企業向けの Class3 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”に従ったベリサイン発行のClass3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。

VTN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。

米国ベリサインと日本ベリサインは定期的に中間認証機関をリキーする。中間認証機関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、中間認証機関がリキーされた後は指定されたとおり動作しない可能性がある。従って、日本ベリサインは、中間認証機関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。日本ベリサインは、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 本文書の管理部署

日本ベリサイン株式会社 法務部
〒104－0028 中央区八重洲 2－8－1
電話 03-3271-7012
FAX 03-3271-7027
practices@verisign.co.jp

1.5.2 連絡先

日本ベリサイン株式会社 法務部
〒104－0028 中央区八重洲 2－8－1
電話 03-3271-7012
FAX 03-3271-7027
practices@verisign.co.jp

1.5.3 CPへの適合性の決定者

日本ベリサインは、本 CPS 及び本 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 及び修正の承認は日本ベリサイン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、日本ベリサインのリポジトリの「プラクティス・アップデート及び通知」（https://www.verisign.co.jp/repository/updates/）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 参照。

2. 公表及びリポジトリに関する責任

2.1 リポジトリ

日本ベリサインは、自己の認証機関及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。日本ベリサインは本 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、日本ベリサインはこれをリポジトリにおいて公表する。日本ベリサインは、日本ベリサイン・サブドメイン内の自己の認証機関、サービス・センタ及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、日本ベリサインは本 CPS に従い、OCSP サービスを提供する。

2.2 証明書情報の公表

日本ベリサインは、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。日本ベリサインは、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、及び 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。

日本ベリサインは、自己の認証機関及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、日本ベリサインはこれをリポジトリで公表する。さらに、日本ベリサインは CRL を発行し、利用可能な場合には、自己の認証機関及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。

日本ベリサインは、以下の文書の最新バージョンを公表する。

- VTN CP
- 本 CPS
- 利用規約
- 依拠当事者規約

日本ベリサインは、VTN の日本ベリサイン・サブドメイン内で証明書を発行する日本ベリサイン認証機関及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。

日本ベリサインは、認証機関に関する情報をリポジトリで（https://www.verisign.co.jp/repository）で公表する。

日本ベリサインは、VTN CP、本 CPS、利用規約及び依拠当事者規約を日本ベリサインのウェブ・サイト内のリポジトリで公表する。

日本ベリサインは、Table 3 に従い、証明書を公表する。

証明書の種類	公表の要件
米国ベリサイン第一次認証機関及び米国ベリサイン中間認証機関ルート証明書	最新のブラウザに含まれ、下記のクエリーを通じて利用者証明書と共に取得できる証明書チェーンの一部として、依拠当事者に利用可能

日本ベリサイン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
日本ベリサイン認証機関証明書で、マネージド PKI ライト証明書及びマネージド 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 にある日本ベリサイン 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
日本ベリサイン OCSP レスポンダー証明書	directory.verisign.co.jp にある日本ベリサイン 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
利用者証明書	directory.verisign.co.jp にある日本ベリサイン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。 また、directory.verisign.com にある米国ベリサイン LDAP ディレクトリ・サーバにおけるクエリーを通じても利用可能
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。利用規約及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

日本ベリサインのウェブ・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。日本ベリサインは、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。日本ベリサインは、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及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

VTN 下で発行された証明書に記載されている名称は、VTN 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

日本ベリサイン認証機関証明書は、Issuer 及び Subject フィールドに X.501 識別名を含む。
日本ベリサイン認証機関識別名は、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) =	“VeriSign, Inc.” もしくは“VeriSign Japan K.K.” [3]
Organizational Unit (OU) =	日本ベリサイン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 • VeriSign 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、VeriSign 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。 ● 日本ベリサインの OCSP レスポンダー及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、「VeriSign Japan K.K.」 ウェブ・サーバ向け証明書及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) =	日本ベリサイン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。 ● 組織向け証明書及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 • VeriSign Trust Network

[3] 例外として、”RSA Data Security, Inc.,”（現在は、米国ベリサインの認証機関である）と表記されるセキュア・サーバ CA がある。

属性	値
	• 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 • 申請が日本ベリサインにより認証された証明書中に、“Authenticated by VeriSign Japan K.K.”及び“Member, VeriSign Trust Network” • “Persona Not Validated”(Class1 個人向け証明書) • 証明書の種類を説明する記載
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 レスポンダー証明書の場合、OCSP レスポンダー名 ● ウェブ・サーバ用証明書の場合、ドメイン・ネーム ● コード/オブジェクト・サイニング証明書の場合、組織名 ● 個人向け証明書の場合、名前
E-Mail Address (E) =	Class1 個人向け証明書及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

Table 5 -利用者証明書中の識別名属性

利用者証明書の SubjectDN の CommonName (= CN)の記載事項は、Class 2 及び 3 証明書の場合、認証される。

- 組織向け証明書の SubjectDN に含まれる認証された CommonName の値は、ドメイン・ネーム(セキュア・サーバ ID 及びグローバル・サーバ ID の場合)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 SubjectDN 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。

EV SSL 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 Section 6 に記載される。

3.1.2 意味のある名称であることの必要性

Class2及び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。

日本ベリサイン認証機関証明書は、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

Class1 証明書の利用者の本人確認は行われない。Class1 証明書の利用者は匿名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、Class2 及び 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、日本ベリサイン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

日本ベリサインは利用者の申込手続きを通じて、SubjectDN 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 SubjectDN 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、認証及び役割

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。日本ベリサインは、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。日本ベリサインは、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日本ベリサイン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。キー・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、組織の実在性及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)を、日本ベリサインが規定する認証手順に従い確認される。

日本ベリサイン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並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、日本ベリサイン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及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日本ベリサインが行う。

特定の種類の証明書については、Table6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	ベリサインにおける EV SSL 証明書の発行手続きは、本 CPS の Appendix B1 に記載される。

Table 6 特別な認証手続き

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。Table7 に Class 別の VTN 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。 • 日本ベリサイン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、雇用の確認及び管理者の権限の確認に基づき行う。 日本ベリサインは、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、及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。

- o 部門名(OU)
- o Class 1 証明書の利用者名

o　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、日本ベリサインまたは登録機関は、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並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。日本ベリサインは、一般的に、有効期限が満了するキー・ペアを取り替えるために、新しいキー・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）、日本ベリサインは、既存のキー・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」及び「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、新しいキー・ペアが生成されるかどうかを重要視しないことによる。Class3 サーバ用証明書を除き、全 Class とタイプの証明書について、日本ベリサイン利用者向け証明書更新手続きの一部として、新しいキー・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、Class3 サーバ用証明書については、利用者のキー・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キー・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。

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、申請責任者及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、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またはリニューアル後、そしてそれ以降リキーまたはリニューアルが行われる機会に、日本ベリサイン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。

特に、Class3 組織向け証明書のリキーの申請について、日本ベリサインは、証明書に含まれる組織名称、ドメイン名の再認証を行う。

以下の要件を満たす場合、日本ベリサインは、証明書の申請に際し、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。

- 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こと
- 証明書の DN が変更されていないこと
- 申請責任者及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

証明書の有効期間満了から 30 日後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(Class1 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(Class1 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
- VTN を保全するために米国ベリサインまたは日本ベリサイン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キーについては、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 SubjectDN 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。上記の方法または日本ベリサイン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及び認証の要件が失効後の証明書の更新に適用される。

3.4 失効申請に関する確認と認証

証明書の失効前に、日本ベリサイン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。
- 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。

日本ベリサインの管理者は、日本ベリサイン・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。日本ベリサインは、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 及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VTN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、日本ベリサイン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ハードウェア・トークン内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日本ベリサイン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。

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

4.1.2 登録手続き及び責任

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。

- o 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
- o キー・ペアを生成もしくは生成させる手配をすること
- o 自己の公開鍵を直接もしくは登録機関を通じて日本ベリサインに引き渡すこと
- o 日本ベリサイン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 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、日本ベリサインと契約を締結する。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キー・ペアを生成のキー・セレモニ前に、申請者は、日本ベリサインに協力して、適切な DistinguishedName 及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

日本ベリサイン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及び認証を行う。

4.2.2 証明書申請の承認もしくは拒絶

日本ベリサイン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。

- o 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及び認証が問題なく完了すること
- o 支払いが完了していること

以下の場合、日本ベリサインもしくは登録機関は、証明書申請を拒絶する。

- o 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及び認証を完了することができないとき
- o 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
- o 利用者が、指定された時間内に返答をしないとき
- o 支払いの完了を確認できないとき
- o 登録機関が、利用者へ証明書を発行することが VTN 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

日本ベリサインは、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 VTN 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。日本ベリサインは、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

日本ベリサインは、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。

4.4 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。

- o 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
- o 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

日本ベリサインは、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　キー・ペアと証明書の用途

4.5.1　利用者の秘密鍵及び証明書の使用

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、日本ベリサインの利用規約ならびに VTN の CP 及び本 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。

4.5.2　依拠当事者の公開鍵及び証明書の使用

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。日本ベリサインは、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)。
- 証明書及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 DistinguishedName 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キー・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、キー・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、申請責任者及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。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機会に、日本ベリサイン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。

特に、Class3 組織向け証明書のリニューアルの申請について、日本ベリサインは、証明書に含まれる組織名称、ドメイン名の再認証を行う。

以下の要件を満たす場合、日本ベリサインは、証明書の申請に際し、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。

- 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
- 申請責任者及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

上記の方法または日本ベリサイン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及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、日本ベリサイン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、日本ベリサイン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。

上記の方法または日本ベリサイン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及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、日本ベリサイン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 CPS4.1.1 参照。

4.8.3　証明書の変更申請の手続

日本ベリサイン、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 4.3.2 参照。

4.8.5　変更された証明書の受領確認の行為

本 CPS 4.4.1 参照。

4.8.6　認証機関による変更された証明書の公開

本 CPS4.4.2 参照。

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 CPS4.4.3 参照。

4.9 証明書の失効及び効力の停止

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、日本ベリサイン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、日本ベリサインは、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。

- 日本ベリサイン、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
- 日本ベリサイン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
- 日本ベリサイン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(Class1 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(Class1 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
- 日本ベリサイン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
- 日本ベリサインまたはカスタマが、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
- Class3 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
- その証明書の継続的な使用が、VTN に悪影響を与える場合

日本ベリサインは、証明書の使用が、VTN 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。

- o 受領した苦情の質と回数
- o 苦情を申し立てた者に対する本人確認
- o 効力を有する関連法規
- o 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、VTN に悪影響を与えると考える場合、日本ベリサインは、上記に加えて、特に以下のことを考慮する。

- o 署名されているコードの名前
- o コードの動作
- o コードの配布方法
- o コードの受領者への公開
- o そのコードになされた追加の申し立て

日本ベリサインは、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。

日本ベリサイン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、直ちにその旨を日本ベリサインに通知する義務があることを規定する。

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。日本ベリサイン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。

日本ベリサインは、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、日本ベリサイン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日本ベリサイン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。

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日本ベリサインに指示するものとする。

4.9.3.2　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、日本ベリサインに対しその旨知らせるものとする。日本ベリサインは、それを受けて当該証明書の失効を行う。日本ベリサインは、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

日本ベリサインは、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、ウェブ・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。

4.9.8　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及び他の証明書のステータス情報は、ウェブ・ベースのリポジトリ及び(提供されている場合は)OCSP を通じて提供される。日本ベリサインは、CRL の公表に加え、日本ベリサイン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。

証明書ステータス情報は、次の日本ベリサインのリポジトリにアクセスすることにより LDAP ベースのクエリー機能を通じて利用することができる。

- directory.verisign.co.jp

日本ベリサインは、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。

4.9.10 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

日本ベリサインは、日本ベリサインが日本ベリサイン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、日本ベリサインのウェブ・サイトの CRL、LDAP ディレクトリ、及び(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 サービスの利用可能性

証明書ステータス・サービスは、1 日 24 時間利用可能である。

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、以下の事由により日本ベリサイン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、VTN 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。日本ベリサインは、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 鍵の預託と復旧及び実施

キーマネージメントサービス(または日本ベリサイン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(または日本ベリサイン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及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鍵を引き渡すこと
- 暗号化された鍵を復旧する前に利用者キー・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及び復旧のポリシー及び実施

秘密鍵は、エンタープライズ・カスタマの施設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、破棄される。結果として生じたマスクドセッションキー(MSK)のみが、日本ベリサインに安全に送られ、保管される。
KER(エンドユーザの秘密鍵を含む) とランダムセッションキーマスクは、エンタープライズ・カスタマの施設内のキーマネージャー・データベースに保管される。

秘密鍵及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キー・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、キー・ペアに対するMSKは、日本ベリサインの安全なデータ・センタ外で運用されるマネージドPKIデータベースから返却される。キーマネージャーは、MSKをランダムセッションキーと結合させ、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、管理及び運用統制

5.1 物理的管理

日本ベリサインは、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、日本ベリサイン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 立地場所及び構造

日本ベリサイン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及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、及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、日本ベリサインは認証機関業務のために災害復旧施設を維持している。日本ベリサインの災害復旧施設は日本ベリサイン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

日本ベリサイン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、及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、ログ及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。信頼される者とされていない従業員または訪問者等は、付き添いなしにこれらの保護された階層へ入室することができない。

物理セキュリティシステムは、オンライン及びオフラインのCSUの保管場所、及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。鍵生成及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CSUは施錠されたキャビネットにより保護され、オフラインCSUは施錠された金庫、キャビネット及びコンテナにより保護される。CSU及び鍵管理上必要となる重要資料へのアクセスは、日本ベリサイン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 電源及び空調

日本ベリサインのセキュアな施設は、一次及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
- 温度及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

日本ベリサインは、日本ベリサイン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　火災予防及び保護対策

日本ベリサインは、火災の予防及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。日本ベリサインの火災予防及び保護対策は、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

商用ソフトウェア及びデータ、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、日本ベリサイン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、火事及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

機密文書及び資料は、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、日本ベリサイン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

日本ベリサインは、セキュアなオフサイト施設において、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。

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、独立請負業者及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

日本ベリサインは、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

日本ベリサインは、業務内容に基づく職務の分離、及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。認証機関用暗号ハードウェア(暗号署名ユニット、または CSU) 及び関連する鍵関係資料へのアクセス及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。認証機関用暗号ハードウェアへのアクセスは、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、物理的及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。

自動化された検証及び発行システムによって発行されるもの以外の Class3 証明書の検証及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及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、日本ベリサイン人事部への面前出頭及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。

日本ベリサインは、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及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
- 日本ベリサイン認証機関、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、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、資格及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、経験及び許可要件

日本ベリサインは、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、資格及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、日本ベリサイン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、人事部が査定を行い、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。

経歴調査、及びこれにより収集された情報の取扱は、地域の法律に従う。

5.3.3　トレーニング要件

日本ベリサインは、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。日本ベリサインは、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。

日本ベリサインのトレーニング・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
- 日本ベリサインセキュリティ及び運用ポリシー並びに手順
- 採用されるハードウェア及びソフトウェアの利用と運用
- 事件及び危殆化が発生した場合の報告及び取扱
- 災害復旧及び事業継続の手順

5.3.4　再トレーニングの頻度及び要件

日本ベリサインは、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及び頻度で、再教育を行う。

5.3.5　人事異動の頻度及び順序

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日本ベリサインのポリシー及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及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、同種の地位にある日本ベリサインの従業員に適用されるものと同一または同等の業務上及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日本ベリサイン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

日本ベリサインは、業務を十分に遂行するために必要となるトレーニング及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

日本ベリサインは、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、及び破壊
  - －暗号デバイスのライフサイクル管理イベント
- 次の事項を含む、認証機関証明書及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、リキー及び失効
  - －要求の処理（成功したもの及び不成功に終わったものを含む）
  - －証明書及び 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（成功したもの及び不成功を含む）
  - －日本ベリサインの要員によってなされた PKI 及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及び他の異変
－ファイアウォール及びルーターの動作
－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

日本ベリサイン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）
- 申請書及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

5.4.2 記録を処理する頻度

重要なセキュリティ及び運用イベントが発生した場合、監査記録は、少なくとも1週間に一度の頻度で検査される。更に、日本ベリサインは、日本ベリサイン認証機関及び登録機関のシステム内において、異常及び事故に基づいて生じた警報に反応してなされた不審なまたは通例的でない動作に関する監査記録を調査する。

監査記録の処理は、監査記録の要約中の全重要なイベントに関する監査記録及び書類を調査することにより行われる。監査記録の調査は、当該記録が改ざんされていないことの確認、全ての記録記載についての簡潔な検査並びに記録中の警報または異常に関する徹底した調査を含む。監査記録の調査に基づき取られた記録は、保管される。

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、ネットワーク及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日本ベリサイン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、月次及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

日本ベリサイン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。

- Class1 証明書については 5 年の間
- Class2 及び 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

日本ベリサインは、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及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

日本ベリサインは、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、及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（内部又は外部）

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、日本ベリサイン内部に存在する。エンタープライズ登録機関については、日本ベリサイン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及び検証の手続

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

日本ベリサイン認証機関のキー・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。日本ベリサイン認証機関証明書は、その累計した認証機関キー・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。新規の認証機関キー・ペアは、例えば、役割が終了する認証機関キー・ペアの交換を行う場合、実際に使用されているキー・ペアを補完する場合及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、古い上位認証機関キー・ペアから新しい上位認証機関キー・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。日本ベリサイン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、自己のキー・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キー・ペアを用いて署名されるものとする。
- 上位認証機関は、元のキー・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 危殆化及び災害からの復旧

5.7.1 事故及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。日本ベリサインは、自身、及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変造が生じた場合、当該事象の発生については日本ベリサインのセキュリティ担当部署に報告されるものとし、日本ベリサイン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、事故調査及び事故対応を含む。もし必要であれば、日本ベリサイン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

日本ベリサイン認証機関、日本ベリサイン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、日本ベリサインの鍵危殆化対応手続が、危殆化事故対応チームにより制定される。このチームは、セキュリティ、暗号ビジネス運用、プロダクション・サービスの要員及び他の日本ベリサイン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、日本ベリサイン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、日本ベリサインのリポジトリを通じて、連絡する。
- 影響を受ける全ての VTN 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 に従い新しいキー・ペアを生成する。

5.7.4 災害後の事業継続能力

5.7.4.1 米国ベリサイン

米国ベリサインは、災害復旧サイトを主要な施設から 1000mile 以上離れた場所に設置している。米国ベリサインは、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及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。米国ベリサイン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及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、米国ベリサイン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、米国ベリサインの災害復旧プロセスが米国ベリサイン緊急レスポンスチームにより開始される。

米国ベリサインは、災害後 24 時間以内にきわめて重要な部分の運用を回復し、最低限次の機能をサポートすることができる能力がある。
- 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

米国ベリサイン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。米国ベリサインの災害復旧機器は、本 CPS セクション 5.1.1 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。

米国ベリサインの災害復旧プランは、米国ベリサインの主要なサイトにおいて災害が生じた日から一週間以内に完全な回復を提供するように設計されている。米国ベリサインは、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、米国ベリサインの認証機関・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、監査及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、米国ベリサインの主要サイトにおける運用は回復される。

米国ベリサインは、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及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。

米国ベリサインは、米国ベリサイン・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）及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 日本ベリサイン

日本ベリサインは、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。日本ベリサインは、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及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。日本ベリサイン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及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、日本ベリサイン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、日本ベリサインの災害復旧プロセスが日本ベリサイン緊急レスポンスチームにより開始される。

日本ベリサイン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

日本ベリサイン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。日本ベリサインの災害復旧機器は、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。

日本ベリサインの災害復旧プランは、日本ベリサイン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。日本ベリサインは、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、日本ベリサインの認証機関・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、監査及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、日本ベリサインの主要サイトにおける運用は回復される。

日本ベリサインは、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及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。

日本ベリサインは、日本ベリサイン・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）及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

日本ベリサイン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、日本ベリサインは、その終了に先立ち、利用者、依拠当事者及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、日本ベリサイン及び、カスタマ認証機関の場合には、当該カスタマは、カスタマ、利用者及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、依拠当事者及びカスタマ等、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
・　日本ベリサイン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
・　利用者及びカスタマ・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、利用者及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及び当該秘密鍵を含むハードウェア・トークンの処分
・　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

6. 技術的セキュリティ・コントロール

6.1 キー・ペア生成及びインストレーション

6.1.1 キー・ペア生成

認証機関キー・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及びセキュリティ並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及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（日本ベリサイン認証機関及びマネージド 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。

全ての認証機関のキー・ペアは、“KeyCeremony Reference Guide”、“CA KeyManagement Tool User’s Guide” 及び“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、日本ベリサインの経営陣が適当であるとみなす期間、監査及び後日の調査の目的で保管される。

登録機関キー・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、自動承認サーバを用いて、自らのキー・ペアを生成する。日本ベリサインは、自動承認サーバによるキー・ペア生成が FIPS140-1 レベル 2 に認定された暗号モジュールを用いて実行されることを推奨している。

利用者のキー・ペアの生成は、一般的には、当該利用者によりなされる。Class1証明書、Class2証明書及び Class3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、暗号化モジュールで生成した乱数シードを使用して、日本ベリサインが利用者の代わりにキー・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。

6.1.2 秘密鍵の受渡

エンドユーザ利用者のキー・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。
登録機関または利用者のキー・ペアが、日本ベリサイン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日本ベリサインにより記録される。

利用者のキー・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）、暗号用キー・ペアを生成し、当該キー・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

利用者及び登録機関は、その公開鍵をその認証のため日本ベリサインに対し、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）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キー・ペアは、日本ベリサイン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

米国ベリサインは、その第一次認証機関及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、利用者及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及びルート認証機関の証明書が生成された場合、米国ベリサインは、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。

- 日本ベリサインは、一般的に、全ての証明書チェーン（発行認証機関及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。日本ベリサイン認証機関証明書は、日本ベリサインの 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

キー・ペアの予想される使用期間においては、キー・ペアは、暗号解読技術によってキー・ペアの秘密鍵が解かれないように十分な長さが使用されるべきである。米国ベリサインの第三世代（G3）の一次認証機関は 2048 ビットの RSA キー・ペアを有する。

日本ベリサインは、登録機関及び利用者に対し 1024 ビットの RSA キー・ペアを生成するように推奨する。日本ベリサインは、利用者のキー・ペアが 512 ビット以下の場合には、承認しない場合がある。

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 7.1.2.1.参照

6.2 秘密鍵の保護

日本ベリサインは、日本ベリサイン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、論理的及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及び中間認証機関のキー・ペアの生成並びに認証機関の秘密鍵の保管に関し、日本ベリサインは 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

日本ベリサインは、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。日本ベリサインは、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

日本ベリサインは、認証機関の秘密鍵のバックアップ用コピーを、通常の復旧及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。

日本ベリサインは、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 を参照されたい。ACS に関しては、日本ベリサインは、利用者秘密鍵の複製を保持することはない。

6.2.5　秘密鍵の暗号化モジュールへの入出力

日本ベリサインは、認証機関のキー・ペアを、当該キー・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、日本ベリサインは、当該キー・ペアのコピーを通常の復旧及び災害復旧の目的で作成する。認証機関のキー・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、当該キー・ペアはモジュール間を暗号化されて移動される。

6.2.6　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保管される。

6.2.7　秘密鍵の起動の方法

日本ベリサイン・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。

6.2.7.1　Class 1 証明書

Class1の秘密鍵の保護に関する VTN 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及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、日本ベリサインは、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。

6.2.7.2　Class 2 証明書

Class2の秘密鍵の保護に関する VTN 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、及び
- 利用者の承認なくして利用者のワークステーション及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。

6.2.7.3　Class 3 証明書(管理者を除く)

Class3 の秘密鍵の保護(管理者を除く)に関する VTN 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及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。

6.2.7.4 管理者の秘密鍵(Class 3)

管理者の秘密鍵の保護に関する VTN 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、及び
- 管理者の承認なくして管理者のワークステーション及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。

6.2.7.5 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 VTN 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、及び
- 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及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

6.2.7.6 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。

6.2.8 秘密鍵の非活性化の方法

日本ベリサイン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。日本ベリサインの登録機関の秘密鍵(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。日本ベリサインの登録機関は、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 Application 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。

6.2.9 秘密鍵の破壊の方法

日本ベリサインは、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。日本ベリサインは、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及び他の適切な方法を活用する。鍵の破壊が完了した際には、認証機関の鍵破壊活動は記録される。

6.2.10 暗号モジュールの評価

本 CPS セクション 6.2.1 参照

6.3 キー・ペアの管理に関する他の点

6.3.1 公開鍵の保管

日本ベリサインの認証機関、登録機関及び利用者の証明書はバックアップされ、日本ベリサイン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 証明書の運用期間及びキー・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。キー・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日本ベリサイン証明書の最長の有効期間はTable 8[#] 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、日本ベリサイン認証機関は、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)	30 年まで
自己署名された第一次認証機関 (2048 ビット)	50 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)

[#] SHA 2 または ECC アルゴリズムや 2048 ビット以上の長さのキーが使用されるなど、より強力な暗号化アルゴリズムやキー長が使用されている証明書の場合、証明書の有効期間は、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。

認証機関(オンライン)から利用者(個人)	通常 2 年まで、ただし以下の(#2)の場合には 5 年まで
認証機関(オンライン)から利用者(組織)	通常 3 年まで(#3) (#4)

(#1) VeriSign Onsite Administrator CA-Class 3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) 5 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キー・ペアの交換を行う。
(#3)組織向けリテール証明書は、3年を上限として発行される。
(#4) 組織向け利用者証明書のうち VTN の一部機能をサポートするためだけの証明書に関しては、有効期間が5年とされ、更新作業後は最長10年とすることができる。

Table 8 – 証明書の運用期間

VTN CP のセクション 6.3.2 について、日本ベリサイン PMA は、米国ベリサインの承認を得た上で、CA キー・ペアの移行中に PKI サービスが中断しないように、指定の制限数を拡張し、CA 数を増加する例外措置を認めるものとする。当該例外措置は、13 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ない。また、2011 年 4 月 30 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、日本ベリサイン・サブドメインの参加者は、キー・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、2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。

- 当該証明書が個人向けの証明書であること
- 利用者のキー・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,
- 利用者はセクション 3.2.3 の規定に従い、最低 25 ヶ月ごとに再認証を受けること
- 利用者はセクション 3.2.3 の規定に従い、秘密鍵と対応する公開鍵を保有していることの証明を最低 25 ヶ月ごとに行うこと
- 万が一、利用者再最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

米国ベリサインは、VTN の一部であって最高 15 年の運用期間を持つ自己署名された発行認証機関として、セキュア・サーバ認証機関を管理する。この認証機関によって発行されたエンドユーザ利用者証明書は、上記の Table8 に記載する利用者証明書の必要条件を満たす。

また、米国ベリサインは「VeriSign Class 3 International Server CA」ならびに「Class 3 Open Financial Exchange CA – G2」も管理する。これらは PCA によって署名されているオンライン認証局である。両認証局の有効期間は、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。

6.4 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

日本ベリサイン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 及び“KeyCeremony Reference Guide”に定める要件に従って生成される。シークレット・シェアの生成及び分配は記録される。

日本ベリサイン登録機関は、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。日本ベリサイン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

日本ベリサインは、マネージド PKI 管理者、登録機関及び利用者に対し、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。日本ベリサインは、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

日本ベリサインのシークレット・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及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。

日本ベリサイン登録機関は、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。

日本ベリサインは、クライアント管理者、登録機関及び利用者に対し、その秘密鍵を暗号化した形式で保管すること及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、VTN 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、日本ベリサインは、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

日本ベリサインは、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

日本ベリサインは、認証機関ソフトウェア及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、日本ベリサインは、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。

日本ベリサイン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。日本ベリサインは、実際に運用に供しているネットワークを、内部及び外部からの侵入並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。

日本ベリサインでは、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。

日本ベリサインのリポジトリをサポートする日本ベリサインのデータベースへの直接的アクセスは、日本ベリサイン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。

6.5.2　コンピュータ・セキュリティの評価

日本ベリサインが使用するプロセッシング・センタ・ソフトウェアのバージョンは、ISO/IEC15408-3:1999 の EAL4 の要件を満たすものである。ISO/IEC15408-3:1999 とは、情報工学－セキュリティ技術－IT セキュリティの評価基準－パート 3：セキュリティ保障要件で、米国ベリサインプロセッシングセンタ・セキュリティ・ターゲットに対するコモン・クライテリアに基づくものである。米国ベリサインは、コモン・クライテリアのもとで、プロセッシング・センタ・ソフトウェアの新製品について、適宜評価することができる。

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、日本ベリサインのシステム開発及び変更管理基準に従い、日本ベリサインにより開発され実施される。日本ベリサインは、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及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日本ベリサインのシステム開発基準に従い開発される。

米国ベリサイン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、米国ベリサインまたは日本ベリサイン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及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

日本ベリサインは、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及び方策を有している。日本ベリサインは、全ソフトウェア・パッケージ及び日本ベリサイン・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及びその後定期的に、日本ベリサイン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

日本ベリサインは、無権限者によるアクセス及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及び登録機関の機能を履行している。日本ベリサインは、暗号化及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 及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 及びOCSP のプロファイル

7.1 証明書のプロファイル

日本ベリサインの証明書は、(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 及び(b) RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, May 2008 (“RFC 5280”) にほぼ準拠する。

少なくとも、日本ベリサインの X.509 証明書は基本フィールドを持ち、Table9 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 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 参照）
Issuer DN	本 CPS セクション 7.1.4 参照
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	CP セクション 7.1.4 参照。
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

日本ベリサインの証明書は、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

日本ベリサインは、X.509 バージョン 3 の VTN 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 及び CP の下では保証されない。

EV SSL 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 Certificate and CRL Profile, May 2008.)に従い設定される。X.509 バージョン3の証明書中の KeyUsageエクステンションは、通常、Table10に示すように、ビットのセット及びクリア、並びにCritical

ityが設定される。
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。

		認証機関	Class 1 及び Class 2 のエンドユーザ利用者	自動承認トークンと Class2/3 エンドユーザ利用者	デュアルキー・ペア・署名 (Managed PKI Key Manager)	デュアルキー・ペア・暗号化 (Managed PKI Key Manager)
Criticality		TRUE	FALSE	FALSE	FALSE	FALSE
0	DigitalSignature	Clear	Set	Set	Set	Clear
1	nonRepudiation	Clear	Clear	Clear	Clear	Clear
2	keyEncipherment	Clear	Set	Set	Clear	Set
3	dataEncipherment	Clear	Clear	Clear	Clear	Clear
4	keyAgreement	Clear	Clear	Clear	Clear	Clear
5	keyCertSign	Set	Clear	Clear	Clear	Clear
6	CRLSign	Set	Clear	Clear	Clear	Clear
7	encipherOnly	Clear	Clear	Clear	Clear	Clear
8	decipherOnly	Clear	Clear	Clear	Clear	Clear

Table 10 – KeyUsage エクステンションの設定

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、日本ベリサインは、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キー・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、日本ベリサインは当該争議に関する一切の責任を負わないものとする。

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 VTN CP のオブジェクト識別子を含み、及び 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。

7.1.2.3 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、RFC3280 に従い設定される。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。

7.1.2.4 Basic Constraints

日本ベリサインの 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、Null 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、他の場合は「FALSE」に設定されなければならない。

日本ベリサインの 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

日本ベリサインは、Table 11 に示す特定の種類の X.509 バージョン 3 証明書について、Extended Key Usage エクステンションを使用することができる。通常、その他の種類の証明書については、日本ベリサインは Extended Key Usage エクステンションを使用しない。

証明書の種類	証明書の種類
Certification Authority (CA)	Class 3 International Server CA
OCSP Responder	Class 1-3 Public Primary OCSP Responders Secure Server OCSP Responder
Class 3 Web Server Certificates	Secure Server IDs Global Server IDs
Authenticated Content Signing Certificates (ACS)	Authenticated Content Signing Certificates
Individual Certificates	Class 1 Individual Certificates Class 2 Individual Certificates

Table 11 – 証明書における Extended Key Usage エクステンションの使用

上記の証明書について、日本ベリサインは、Table 12 に従い、Extended Key Usage エクステンションを使用することができる。

	クラス 3 インターナショナル・サーバ認証機関	OCSP レスポンダー	セキュア・サーバ ID	グローバル・サーバ ID	コード/オブジェクト・サイニング利用者証明書	Class 1 /2 個人向け証明書
Criticality	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
ServerAuth	Set	Clear	Set	Set	Clear	Clear
ClientAuth	Set	Clear	Set	Set	Clear	Set
CodeSigning	Clear	Clear	Clear	Clear	Set	Clear
EmailProtection	Clear	Clear	Clear	Clear	Clear	Set
ipsecEndSystem	Clear	Clear	Clear	Clear	Clear	Clear
ipsecTunnel	Clear	Clear	Clear	Clear	Clear	Clear
ipsecUser	Clear	Clear	Clear	Clear	Clear	Clear
TimeStamping	Clear	Clear	Clear	Clear	Clear	Clear
OCSP Signing	Clear	Set	Clear	Clear	Clear	Clear
Microsoft Server Gated Crypto (SGC)	Clear	Clear	Clear	Set	Clear	Clear

	クラス 3 インターナショナル・サーバ認証機関	OCSP レスポンダー	セキュア・サーバ ID	グローバル・サーバ ID	コード/オブジェクト・サイニング利用者証明書	Class 1 /2 個人向け証明書
OID: 1.3.6.1.4.1.311.10.3.3						
Netscape SGC – OID: 2.16.840.1.113730.4.1	Set	Clear	Clear	Set	Clear	Clear
VeriSign SGC Identifier for CA Certificates – OID: 2.16.840.1.113733.1.8.1	Set	Clear	Clear	Clear	Clear	Clear

Table 12 – ExtendedKeyUsage エクステンションの設定

7.1.2.6 CRL Distribution Points

ほとんどの日本ベリサインの X.509 バージョン 3 の個人向け証明書及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、日本ベリサインは、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 SubjectDN 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

日本ベリサインが、Subject Key Identifier エクステンションを有する X.509 バージョン 3 VTN 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 3280 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

日本ベリサインの証明書は、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-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}

- md2WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 2}

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 の使用は、md5WithRSAEncryption よりも強く推奨される。md2WithRSAEncryption は、利用者証明書にはもはや使用されない。ただし、一部のとても古い認証機関及び利用者証明書のための CRL への署名においては使用される。

7.1.4 名前の形式

日本ベリサインは、本 CPS セクション 3.1.1 に従い、発行者(Issuer) 及び SubjectDN を含む VTN 証明書を発行する。

さらに、日本ベリサインは、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、VTN 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。VTN 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、証明書は米国ベリサインの CPS を参照する。

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及び意味

通常、ベリサインは、Certificate Policies エクステンションにポリシー修飾子を含むX.509 Version3 VTN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ベリサインの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 13 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 参照。
Signature Algorithm	CRL に署名するために使用されるアルゴリズム。ベリサインの CRL は、RFC 3279 に従い、sha1RSA(OID: 1.2.840.113549.1.1.5)、md5RSA(OID:1.2.840.113549.1.1.4)または md2RSA(OID: 1.2.840.113549.1.1.2)アルゴリズムを用い署名される。
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・ナンバー及び失効日を含む、失効した証明書のリスト。

Table 13 – 基本的な CRL プロファイル項目

7.2.1 バージョン番号

日本ベリサインは、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 RFC3280 の要求に従う。

7.2.2 CRL 及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。日本ベリサインは、OCSP を以下に対して使用する。

- Class 2 におけるエンタープライズ向け証明書

OCSP レスポンダーは、RFC2560 に準拠する。

7.3.1 バージョン番号

RFC2560 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

規定しない。

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 VTN のルート認証機関、Class 3 組織向け認証機関、Class 2 組織向け及び個人向け認証機関、Class1個人向け認証機関を含む、日本ベリサインのパブリック及びマネージド PKI 認証機関サービスをサポートする日本ベリサインのデータ・センタの運用及びキーマネージメントの運用に関しては、年次の SAS70 タイプⅡ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、日本ベリサイン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。日本ベリサインは、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及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、日本ベリサインは、VTN 内の日本ベリサイン・サブドメインの信頼性を確保するため、次に例示する審査及び調査を行うことができるがこれに限定されない。

- 日本ベリサインは、自らの判断により、被監査組織が VTN 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 VTN 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。
- 日本ベリサインは、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。

日本ベリサインは、これらの監査、審査及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、日本ベリサイン及び監査、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。

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。

8.2 評価人の身元と資格

日本ベリサイン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及び技術、セキュリティ監査並びに第三者証明の職務に深い知識を有すること。及び、
- 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、並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

日本ベリサインの運用についての準拠性監査は、日本ベリサイン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

日本ベリサインが行う認証機関（またはこれと同等のもの）監査のための年次の SAS70 タイプⅡ監査範囲は、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及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及び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

日本ベリサイン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、日本ベリサインの経営陣によりなされる。日本ベリサインの経営陣は、是正措置の策定及び実施につき責任を負う。もし、日本ベリサインが、当該例外または欠陥が VTN 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、日本ベリサインの経営陣は、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

日本ベリサインの運用に関する準拠性監査の結果は、日本ベリサインの経営陣の任意の判断により公開することができる。

9. 業務及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

日本ベリサイン及びカスタマは、利用者に対し、証明書の発行、管理及び更新に関し、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

日本ベリサイン及びカスタマは、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

日本ベリサインは、本 CPS 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、日本ベリサインは、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及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。日本ベリサイン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

日本ベリサインは、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

日本ベリサイン・サブドメインにおいて、次の返金制度
（https://www.verisign.co.jp/repository/refund/index.html）が適用される。

日本ベリサインは、証明書業務の運用及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、利用者は日本ベリサインに対して、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日本ベリサイン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、日本ベリサインに対し、証明書を破棄し、返金をするよう要請することができる。日本ベリサインは、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、日本ベリサインカスタマサポート 044-520-7210 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、過失及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。日本ベリサインはこのような"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、利用者及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。日本ベリサインの財務状況は、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、日本ベリサイン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のベリサインが提供する SSL/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及びどの証明書がこの対象になるかは、http://www.verisign.co.jp/repository/netsure/summary.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及び当該秘密鍵を回復させるために必要な情報
- 処理記録（全部の記録及び監査証跡記録の双方を含む）
- 日本ベリサイン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
- 日本ベリサイン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及び災害復旧計画
- 日本ベリサインのハードウェア及びソフトウェアの運用並びに証明書サービス及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

日本ベリサイン・サブドメインの参加者は、証明書、証明書失効及び他のステータス情報、日本ベリサインのリポジトリ並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

日本ベリサインは、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

日本ベリサインは、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.verisign.co.jp/repository/privacy/privacy_statement.html 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及びオンラインの 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

法律を従うことを条件に、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 VTN 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及び同意

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

日本ベリサインは、日本ベリサインが以下に相当すると誠実に判断する場合、秘密情報及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

利用者及び依拠当事者を除く、日本ベリサイン・サブドメインの参加者間での知的財産権の帰属は、日本ベリサイン・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　証明書及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及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。日本ベリサイン及びカスタマは、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。日本ベリサイン及びカスタマは、依拠当事者規約及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

VTN 参加者は、日本ベリサインが本 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、商号並びに証明書申請者に発行される証明書中の DistinguishedName に関する全ての権利を留保する。

9.5.4　鍵及び鍵のデータに関する財産権

認証機関及び利用者の証明書に対応するキー・ペアは、それらが保管及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及び利用者が保有するものであり、当該キー・ペアに係る全ての知的財産権は当該認証機関及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及び自己署名証明書を含む米国ベリサインのルート公開鍵及びそれを含むルート証明書については、米国ベリサインに帰属する。米国ベリサインは、ソフトウェア及びハードウェア製造者に対し、信頼できるハードウェア・デバイス及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、米国ベリサイン及び日本ベリサイン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

日本ベリサインは、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
- 失効サービス及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。

9.6.2 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）及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 を遵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、及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、並びに本 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、日本ベリサインの利用規約及び依拠当事者規約、およびその他の利用規約は、商品性及び特定目的への適合性を含む日本ベリサインのその他一切の保証を否認する。

9.8　責任の制限

適用される法律上許される範囲内において、利用規約及び依拠当事者規約は、日本ベリサインの責任を制限しなければならない。日本ベリサインは、間接損害、特別損害、付随的損害及び結果的損害に関しては何らの責任も負わない。また、利用規約及び依拠当事者規約は、日本ベリサインがある特定の証明書に関して負うことある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 14　損害賠償額の上限
[注] Table 14 に定める損害賠償額の上限は、日本ベリサインの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。日本ベリサインの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。日本ベリサインの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。
http://www.verisign.co.jp/repository/netsure/summary.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 SSL 証明書に対するベリサインの責任の制限は、本 CPS Appendix B1 のセクション 37 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、日本ベリサイン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日本ベリサイン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。

9.10 有効期間と終了

9.10.1 有効期間

本 CPS は、日本ベリサイン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、日本ベリサイン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、日本ベリサイン・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、日本ベリサイン・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、日本ベリサインによりなされる。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、日本ベリサインのリポジトリの「プラクティス・アップデート及び通知」(https://www.verisign.co.jp/repository/updates/)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。日本ベリサインは、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

日本ベリサインは、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、日本ベリサインの単独の判断による。

本CPSの変更内容は、日本ベリサインのリポジトリの「プラクティス・アップデート及び通知」(http://www.verisign.co.jp/repository/updates/)に置かれるものとする。

本 CPS の定めにかかわらず、日本ベリサインが VTN 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、日本ベリサインは日本ベリサイン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。日本ベリサインは、公表後相当な期間内に、当該変更の内容を日本ベリサイン・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、当該変更が日本ベリサイン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。日本ベリサイン・サブドメイン参加者は、日本ベリサインに対し、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

日本ベリサインは、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。日本ベリサインは(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。日本ベリサインは、提案した変更を、日本ベリサインのリポジトリの「プラクティス・アップデート及び通知」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

日本ベリサイン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

日本ベリサイン・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、日本ベリサインの利用規約及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、解釈及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、日本ベリサイン・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、統一的手続及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、解釈及び有効性を支配する。

9.15 法の遵守

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。

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、日本ベリサインの利用規約及び依拠当事者規約、及びその他の利用規約は日本ベリサイン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
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.
CP	Certificate Policy.
CPS	Certification Practice Statement.
CRL	Certificate Revocation List.
EAL	Evaluation assurance level (pursuant to the Common Criteria).
EV	Extended Validation
FIPS	United State Federal Information Processing Standards.
ICC	International Chamber of Commerce.
KRB	Key Recovery Block.
LSVA	Logical security vulnerability assessment.
OCSP	Online Certificate Status Protocol.
PCA	Primary Certification Authority.
PIN	Personal identification number.
PKCS	Public-Key Cryptography Standard.
PKI	Public Key Infrastructure.
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.
VTN	VeriSign Trust Network.

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 VTN サービスを提供するために米国ベリサインと契約を締結している者。
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)ベリサイン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。
Automated Administration	申請情報がデータベースにある情報と一致する場合、証明書の申請が自動的に承認される手続き。

Term	Definition
自動承認	
Automated Administration Software Module **自動承認モジュール**	自動承認を行う日本ベリサイン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 Chain **証明書チェーン**	利用者及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 Policies (CP) **サーティフィケート・ポリシー**	VTN・サーティフィケート・ポリシーと呼ばれるもので、VTN を支配する主要な方針を記載している文書。
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・ナンバー及びその具体的時期及び理由を示す。
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**	VTN 内で証明書の発行、管理、失効及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**	米国ベリサイン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、管理及び失効をする際に採用する運用手続を規定した文書で、VTN 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 の保障は本 CPS 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日本ベリサイン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 VTN 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**	本 CPS 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。

Term	Definition
Country 国	国とは本ガイドランでは、独立国であると定義する。
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
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 SSL 証明書を使用する Managed PKI カスタマは、ベリサインに権限を与える。
EV Certificate: EV SSL 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 SSL 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 SSL 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	VTN 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 VTN 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ベリサインまたは日本ベリサインが行う監査または調査。
Intellectual Property Rights 知的財産権	著作権、特許権、企業秘密、商標及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
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。
Key Generation Ceremony キー・ジェネレーション・セレモニ	認証機関または登録機関のキー・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 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日本ベリサインのサービス。
Managed PKI マネージド PKI	日本ベリサインのエンタープライズ・カスタマが VTN 内で証明書を従業員、パートナー、サプライヤー及び顧客、さらにサーバ、ルーター及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日本ベリサインの完全に統合された PKI サービス。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・ネットワーク及び電子商取引を可能にする。
Managed PKI Administrator マネージド PKI 管理者	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。
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	日本ベリサインからマネージド 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 VTN 内で認証機関になる。マネージド PKI カスタマ

Term	Definition
	は、日本ベリサインに発行、管理及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、証明書の失効及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及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	本 CPS セクション 9.8 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。当該認証機関及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、VTN 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。
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。
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 SSL 証明書の要求、発行、使用。
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及び設備。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、VTN 内において認証機関として行動し、証明書の発行、管理、失効及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

Term	Definition
	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 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及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、実務及び手続のこと。VTN PKI は VTN の提供及び実装を連携して行う複数のシステムから成り立つ。
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ません。(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。
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。
Retail Certificate リテール証明書	認証機関である日本ベリサインによって、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。
RSA	公開鍵暗号方式は、Rivest, Shamir, Adelman によって発明された。
RSA Secure Server Certification Authority (RSA Secure Server CA) RSA セキュア・サーバ認証機関	セキュア・サーバ ID を発行する認証機関
RSA Secure Server Hierarchy RSA セキュア・サーバ階層	RSA セキュア・サーバ認証機関から構成される PKI 階層。
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 Server ID セキュア・サーバ ID	ウェブ・ブラウザとウェブ・サーバ間の SSL セッションをサポートするために用いられる Class3組織向け証明書。
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及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 Guide	プロセッシング・センタ及びサービス・センタのセキュリティ及び監査の要件及び実務を規定する日本ベリサインの文書。
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、失効及び更新を行うアフィリエート(日本ベリサインを含む)。
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。
Subdomain サブドメイン	VTN 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 VTN 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

Term	Definition
	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。
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。
Supplemental Risk Management Review 追加リスク・マネジメント・レビュー	日本ベリサイン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。
Reseller リセラ	特定の市場に対し、日本ベリサインに代わり、サービスを販売するエンティティ。
Trusted Person 信頼される者	VTN 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	VTN 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、信頼性及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、ソフトウェア及び手続き。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。
VeriSign Repository 日本ベリサイン・リポジトリ	証明書及び他の関連する VTN 情報に関する日本ベリサイン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。
VeriSign Trust Network (VTN)	証明書を基盤とする公開鍵インフラストラクチャで、VTN 証明書ポリシーにより運営され、米国ベリサイン及びそのアフィリエート、それらの関連するカスタマ、利用者及び依拠当事者による証明書の全世界レベルでの展開及び使用を可能とするもの。
VTN Participant VTN 参加者	VTN 内において、次の一つ以上に該当する個人または組織：米国ベリサイン、アフィリエート（日本ベリサインを含む）、カスタマ、利用者または依拠当事者
VTN Standards VTN スタンダード	VTN 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

Appendix B1

EV SSL証明書の追加発行手続き

A. 概要

1. 概要

EV証明書のための本手続きは、EVガイドラインで定められているEV証明書の発行手続きについて、ベリサインの現行CPSの追加手続きとして記述する。ガイドラインはCA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求事項を記述する。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。

B. EV SSL 証明書の基本概念

2. EV SSL 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を確立するために使われることを意図している。

(a) 主目的

本書では、EV SSL証明書の主目的を以下に記載する。

- ウェブ・サイトを運営する組織の法的実在確認: 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 SSL証明書に記載の名前、事業所所在地の住所、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。及び、
- 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。

(b) 副次的目的

EV SSL証明書の第2の目的は、ウェブ・サイトを運営する組織の正当性の立証を支援すること、及び、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 SSL証明書は、ウェブ・サイト所有者に関する第三者が審査した信頼性の高いアイデンティティ情報及び住所情報を提供することによって、以下に貢献する。

- SSL証明書を使用するフィッシング詐欺及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、、フィッシング及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。

(c) 除外される目的

EV SSL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 SSL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 SSL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 SSL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 SSL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
o EV SSL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. EV SSL 証明書の保証及び表明
(a) 日本ベリサインによるもの

EV SSL証明書の受益者:
o EV SSL証明書の利用規約に合意する加入者
o EV SSL証明書に記載されたサブジェクト
o日本ベリサイン、ベリサイン及びルート認証機関と、配布するアプリケーションソフトウェアにルート証明書を搭載する旨の契約を締結した全アプリケーションソフトウェアのベンダ
o EV SSL証明書の有効期間中、実際にEV SSL証明書に依拠する全依拠当事者

ベリサインによって発行されたEV証明書について、ガイドラインと発行および証明書に含まれる情報の正確性の確認に関するポリシーの要求事項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障します(EV証明書保障)。EV証明書保障とは特に以下の保障を含みますが、制限されるものではありません。

o 法的存在:日本ベリサインは、EV SSL証明書を発行した時点において、EV SSL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

o アイデンティティ:日本ベリサインは、EV SSL証明書を発行した時点において、EV SSL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

o ドメイン名使用権:日本ベリサインは、EV SSL証明書を発行した時点において、EV SSL証明書に記載されているサブジェクトが、EV SSL証明書に記載の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

o EV SSL証明書の承認:日本ベリサインは、EV SSL証明書に記載されているサブジェクトがEV SSL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

o 情報が正確であること:日本ベリサインは、EV SSL証明書を発行した時点において、EV SSL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

o 利用規約: EV SSL証明書に記載されているサブジェクトは、本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利用規約の契約をベリサインと締結したこと

o ステータス:日本ベリサインは、本ガイドラインの要件に従い、EV SSL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レポジトリを保守すること

o 失効:日本ベリサインは、本ガイドラインの要件に従い、本ガイドラインとこのAppendixに特定された失効事象発生時にはEV SSL証明書を速やかに失効させること

EV SSL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 SSL証明書の発行した時点において、日本ベリサインは、以下の保証あるいは別段の表明または保証を提供しない。

- EV SSL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 SSL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 SSL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 SSL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

(b) 加入者によるもの

日本ベリサインは、利用規約の一部として、日本ベリサイン及びEV SSL証明書受益者のために、加入者が本ガイドラインの利用規約の要件の節で規定した約束及び保証を行うことを要求する。

C. コミュニティ及び利用可能性

4. EV SSL 証明書の発行

EV SSL証明書を発行する場合、ベリサインは、ガイドラインに沿って以下の要求事項を満たす。

(a) 準拠

ベリサインは以下に準拠する。

(1) ベリサインが業務を行う管轄地において、ベリサインの事業及びベリサインが発行する証明書に適用されうる全法規に準拠すること。
(2) EVガイドラインに準拠すること
(3) (i)その時点のWebTrust Program for CAs及び(ii)その時点のWebTrust EV Program、あるいはCA/ブラウザフォーラムが承認した(i)及び(ii)の相当物の要件に準拠すること。及び、
(4) 認証機関が業務を行う各管轄地の法律によってEV SSL証明書発行のためのライセンス取得を要求される場合は、その管轄地で認証機関のライセンスを取得していること。

(b) EV ポリシー

(1) **実施**

このAppendix Bを伴う日本ベリサイン認証局運用規程は、
(A) 折々の改訂時に本ガイドラインの要件を充足する
(B) (i)その時点のWebTrust Program for CAs及び(ii)その時点のWebTrust EV Program、あるいは、CA/ブラウザフォーラムが承認した(i)及び(ii)の相当物の要件を充足する
(C) EV SSL証明書の裏付けとして依存する全ルートを含む、ベリサイン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、ベリサインのルート階層の構造は、
http://www.verisign.com/repository/hierarchy/hierarchy.pdfで参照可能である。

(2) **公開**

ベリサインは、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。日本ベリサインのCPSは、RFC 3647に従って構成される。

(3) **ガイドラインコンプライアンスの確約**

日本ベリサインは、http://www.cabforum.org で公開される現バージョンの CA/ブラウザフォーラム EV SSL 証明書の発行と管理のためのガイドライン (「ガイドライン」)に準拠する。本書と同ガイドラインに矛盾が生じた場合は、本書より同ガイドラインを優先する。

さらに、日本ベリサインは登録機関として要求事項に準拠するとともに、MPKI for SSL EV 顧客や下請業者に対して要求事項に準拠するよう指導しなければならない。

(c) 保険

ベリサインは、現行バージョンのBest's Insurance Guideに記載されているPolicy Holder's Ratingにおいて格付けがA以上の会社と以下の保険契約を締結する。

- 補償限度額200万ドル以上の企業総合賠償責任保険及び

o (i)EV SSL証明書発行または保守時の履行、過失、怠慢、悪意のない契約違反、不履行に起因する損害賠償の請求、及び、(ii)任意の第三者の所有権侵害(著作権及び商標の侵害を除く)、プライバシー侵害ならびに広告上の損害に起因する損害賠償請求に対する補償を含む、補償限度額500万ドル以上の専門職責任保険/エラーズ&オミッションズ保険

5. EV SSL 証明書の取得

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

(a) 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かまたは、州または連邦の管轄機関のよって認められた法人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、認可地及び/または事業所所在地は、日本ベリサインもしくはベリサイン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。また、

(6) 組織は、日本ベリサイン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。

(b) 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、日本ベリサインもしくはベリサイン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。また、
(3) 行政機関は、日本ベリサインもしくベリサイン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。

(c) 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障ないし承認、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及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、日本ベリサインは、Section15 の要件事項に準じた確認をしなければならない。

(d) 非営利団体

ベリサインは、(a)、(b)および(c)を満たさない非営利団体に対して、以下の要求事項を満たせばEV SSL証明書を発行することができる。

(1) 国際的な組織体

(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。

(B) 国際的な組織体は、その本部が日本ベリサイン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) 国際的な組織体は日本ベリサイン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本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。

D. EV SSL 証明書の内容及び特徴

6. EV SSL 証明書の内容の要件

EV SSL証明書のサブジェクトのアイデンティティに関連するEV SSL証明書内容の最小限の要件を規定する。

(a) サブジェクトの組織の情報

本ガイドラインの要求事項に従い、EV SSL証明書は、以下に列挙したフィールドにサブジェクトの組織に関する情報を含まなければならない(「サブジェクトの組織の情報」)。

(1) 組織名

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。ベリサインは、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:QGIS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。ベリサインは、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d/b/a/ 名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d/b/a 名の合計がRFC 5280で定義された64文字を超過する場合は、ベリサインは、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、ベリサイン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。

(2) ドメイン名

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つ以上のホストドメイン名を記載しなければならない。かかるサーバの所有及び運営は、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 SSL証明書ではワイルドカード証明書は許可されない。

(3) 事業種別

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、以下に示す文字列のいずれかを記載しなければならない。' V1.0, Clause 5.(b)', 'V1.0, Clause 5.(c)', 'V1.0, Clause 5.(d)' または'V1.0, Clause 5(e)' 。これはそれぞれ、本ガイドラインの 5b、5c、5d または 5e で定義しているサブジェクトに依存する。

事業種別	事業種別として記載される値
民間組織	V1.0, Clause 5.(b)
行政機関	V1.0, Clause 5.(c)
事業体	V1.0, Clause 5.(d)
非営利団体	V1.0, Clause 5.(e)

Table 1. Business category field content

(4) 法人設立/登録管轄地

ベリサインのEV SSL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Table2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 2. Jurisdiction of Incorporation or Registration Certificate Fields

これらのフィールドには、法人設立/登録機関のレベルの情報を記載する。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ない。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、市区町村の情報は記載しない。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。

(5) 登録番号

ベリサインのEV SSL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。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。

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、ベリサイン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。

(6) 事業所所在地の住所

ベリサインのEV SSL証明書は、サブジェクトの確認された事業所所在地の住所を以下のTable3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 3. Physical address of Place of Business Certificate Fields

7. EV SSL 証明書を認識するための要件

(a) EV 加入者証明書

ベリサインから加入者に発行される各 EV SSL 証明書には、証明書の certificatePolicies エクステンションにベリサインの EV OID が含まれる。このために使用されるベリサインの EV OID は、2.16.840.1.113733.1.7.23.6 である。

(b) EV 下位認証機関証明書

VeriSign Class3 High Assurance CA は、ベリサインの EV OID を含むと同時に、特殊な anyPolicy OID (2.5.29.32.0)も含まれる。

(c)ルート認証機関証明書

EV 証明書のためのベリサイン ルート CA 証明書は、VeriSign Class3 Primary Certification Authority です。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ません。

8. 最大有効期限

(a) EV SSL証明書の最長有効期間

EV SSL証明書の最大有効期限は、27ヶ月です。

(b) 審査で有効と判断されたデータの最長有効期間

EV SSL証明書の発行に際して、審査済みのデータの(再審査が必要となるまでの)有効期間は以下の通りである。

o 法的存在及びアイデンティティ – 1年
o 屋号 – 1年
o 事業所所在地の住所 – 1年、ただし、審査当初は現地訪問により確認されたデータであっても、公認データベースの確認より、データが更新された場合、更新日から1年とする。
o 事業所所在地の電話番号 – 1年
o 銀行口座の検証 – 1年
oドメイン名 – 1年
o 証明書承認者のアイデンティティ及び権限 – 1年、ただし、日本ベリサインと申請者間で別段の条件を指定する契約が締結されている場合は、この限りではない。その場合は、その契約の条件に支配される。たとえば、契約によって、失効、契約の期限満了、または解約されない限り、永続的に割り当てられた権限を有効とすることもできる。

9. その他のEV SSL 証明書の技術要件

Appendix B2 、Appendix B3を参照。

E. EV SSL 証明書要求の要件

10. 一般的要件

(a) 文書の要件

日本ベリサインは、本ガイドラインの要件に従い、EV SSL証明書を発行する前に、申請者から以下の文書を取得しなければならない。

- EV SSL証明書申請
- 署名済み利用規約
- 本ガイドラインに基づく義務を履行するために日本ベリサインが申請者に要求するその他の文書

(b) 役割の要件

EV SSL証明書の発行に際し、以下の申請者の役割が必要である。

- **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 SSL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 SSL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。

VTNの証明書承認者は、企業に対するリテール証明書、ベリサインManaged PKI SSLアカウントを経由したManaged PKI for SSL管理者と同等である。

- **契約書署名者** – 権限のある契約書署名者は、要求されたEV SSL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。

VTNでは、契約書署名者は、リテール証明書の法人窓口、ベリサインのManaged PKI for SSLのアカウントのManaged PKI for SSLの組織窓口と同等である。

申請者は、1 人の人物に上記役割の 1 つ、2 つ、または 3 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、証明書承認者及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。

11. EV SSL 証明書要求の要件

(a) 一般

日本ベリサインは、EV SSL証明書を発行する前に、(申請者の代理で行動する権限を有する証明書要求者を介して)申請者から、本ガイドラインに従って適切に作成、署名されたEV SSL証明書要求を取得する。

(b) 要求及び証明

EV SSL証明書要求には、申請者または申請者の代理によるEV SSL証明書発行の要求であり、記載された情報が真正かつ正確であるということを記載しなければならない。

(c) 情報要件

EV SSL証明書要求には、EV SSL証明書に記載される申請者の事実に関する情報や、本ガイドラインおよび日本ベリサイン独自のポリシーに準拠するために申請者から取得する必要があるその他の情報も記載できる。申請者に関するすべての必要な情報がEV SSL証明書要求に記載されていない場合は、日本ベリサインは残りの情報を、証明書承認者または契約書署名者から取得し、もしくは信頼できる情報源から取得し、証明書承認者または契約書署名者に確認する。

EV SSL証明書発行前、日本ベリサインは、以下のような情報を入手しなければならない。

o 組織名: EV SSL 証明書に記載される申請者の正式な法的組織名で、申請者の法人設立/登録管轄地の法人設立機関に記録された名前(民間組織の場合)、または行政機関の運営の政治上の下部組織の法律で指定される名前(行政機関の場合)、または行政による事業の登録機関に登録されている名前(事業体の場合)。

o 屋号(任意):EV SSL証明書に記載される申請者の屋号(d/b/a名など)で、申請者の事業所所在地の管轄地に登録された名前(申請者により要求された場合)。

o ドメイン名:EV SSL証明書に記載される申請者のドメイン名。

o 法人設立/登録管轄地:EV SSL証明書に記載される申請者の法人設立/登録管轄地で、以下が含まれます。
(a) 市区群
(b) 都道府県
(c) 国

o 法人設立/登録機関:申請者の法務局の名前

o 登録番号:EV SSL証明書に記載される、申請者の法人設立/登録管轄地の法務省が申請者に割り当てた登録番号。

o 申請者住所: 申請者の事業所所在地の住所で、以下が含まれる。
(a) 地域・番地
(b) 市区群
(c) 都道府県
(d) 国
(e) 郵便番号、及び
(f) 代表電話番号

o 証明書承認者: 申請者の代理でEV SSL証明書申請を提出、署名する証明書承認者または申請者の代理で証明書要求者による申請の提出及び署名を許可した証明書承認者の名前及び連絡先。及び、

o 証明書要求者: 証明書承認者と別人の場合に、申請者の代理でEV SSL証明書要求を提出する証明書要求者の名前及び連絡先。

12. 利用規約の要件

(a) 一般

EV SSL証明書を発行する前に、日本ベリサインは、依拠当事者及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、申請者と法的強制力を有する利用規約を締結する。利用規約は、申請者の代理人として行動する権限を有する契約書署名者が署名を行い、EV SSL証明書要求に従って発行されるEV SSL証明書に適用される。リテール証明書の場合、個別に利用規約を締結することができる。また、Managed PKI for SSLの場合、複数の証明書申請に対して一つの利

用規約を適用することもできる。

(b) 利用規約の要件

利用規約には、最低限、申請者名及び申請者の代理で契約に署名する契約書署名者を指定しなければならない。また、利用規約には、義務及び保証を申請者に強制する条項を含めなければならない。

o 情報の正確さ:EV SSL証明書要求内で、また、日本ベリサインによるEV SSL証明書の発行に関連して日本ベリサインからの要求に応じて、常に正確かつ完全な情報を日本ベリサインに提供する義務と保証。

o 秘密鍵の保護:要求したEV SSL証明書に含まれる公開鍵に対応する秘密鍵(及び、パスワードやトークンなど、関連付けられたあらゆるアクセス情報またはアクセスデバイス)を独占的に支配し、その秘密性を維持し、適切に保護するために必要なあらゆる合理的な対策を常に講じる、加入者または下請け業者(ホスティングプロバイダなど)の義務及び保証。

o EV SSL証明書の受領:各EV SSL証明書内のデータの正確性についての検討及び確認が完了するまでEV SSL証明書をインストール及び使用しないという義務及び保証。

o EV SSL証明書の使用:EV SSL証明書に記載のドメイン名でアクセスできるサーバのみにEV SSL証明書をインストールし、適用法規に準拠のうえ使用し、申請者に承認された業務のためのみに使用し、かつ利用規約を順守する方法でのみ使用するという義務及び保証。

o 危殆化に際しての報告及び失効: (a)EV SSL証明書内の情報が誤りまたは不正確であるときや、誤りまたは不正確になったとき、または、(b)EV SSL証明書内の公開鍵と関連付けられた秘密鍵の誤用や危殆の事実または疑いがあるときに、EV SSL証明書及び関連付けられた秘密鍵の使用を中止して速やかにEV SSL証明書の失効を日本ベリサインに要求する義務及び保証。

o EV SSL証明書の使用の中止:EV SSL証明書の期限満了または失効に際してEV SSL証明書内に記載の公開鍵に対応する秘密鍵の使用をすべて速やかに停止する義務及び保証。

F. 証明書要求に対する審査の要件

13. 概要

EV SSL証明書発行に関する日本ベリサインの手続きは、このガイドラインに沿って認証要求が定められ、この手続きは、要求事項を満足するようベリサインによって行われる。

EV SSL証明書発行前に、日本ベリサインは、EV SSL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求事項を満たし、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。

14. 申請者の法的存在及びアイデンティティ(本人であること)の検証

(1) 民間組織

日本ベリサインは、申請者の法的存在及びア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「休眠(inactive)」、「無効(invalid)」、「不在(not current)」、またはこれからに相当する指定を受けていないことを審査する。

日本ベリサインは、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 SSL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。

日本ベリサインは、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。
日本ベリサインはさらに、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及び住所を取得する。

(2) 行政機関

日本ベリサインは、申請者が法的に行政機関であることを審査する。行政機関の運営の政治上の下部組織として存在。

a. 名称:申請者の法的正式名称が EV SSL 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。

b. 登録番号: 日本ベリサインは申請者の設立、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。

(3) 事業体

a. 法的存在: 申請者が申請に含まれる名称で事業を行っているか審査する。

b. 組織名: 申請者の法的正式名称が EV SSL 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。

c. 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。

d. 代表者: 代表者の存在を審査する。

(4) 非営利団体(国際組織体)

a. 法的存在: 申請者が法的に存在を認められた国際組織体か審査する。

b. 組織名: 申請者の法的正式名称が EV SSL 証明書申請の申請者名と一致していることを審査する。

c. 登録番号: 日本ベリサインは申請者の設立、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。

15. 申請者の法的存在及び本人であること)の検証(屋号)

EV SSL証明書内で主張する申請者の同一性に、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、「d/b/a」を含める場合は、日本ベリサインは、(i)申請者が、(本ガイドラインに従う検証)事業所の管轄地の該当する行政機関に屋号の使用を登録済みであること、(ii)届出が現在有効であることを検証しなければならない。

日本ベリサインは、公認データベース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。

16. 申請者の物理的存在の検証

(a) 申請者の事業所の住所

日本ベリサインは、申請者の物理的存在及び事業の存在を検証するために、申請団体が提示した住所が(郵便受けや郵便箱ではなく)申請団体が事業を行っている場所及び申請団体の事業所または親会社もしくは子会社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。

日本ベリサインは、下記のような独自の方法で住所を確認する。

(A) 事業所が法人設立/登録管轄地と同じ国にある申請者の場合:

(1) 1つ以上の公認データベースに同じ住所の事業所で登録されている申請者の場合は、日本ベリサインは、そのデータベースを参照することによって、EV SSL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。

(2) 1つ以上の現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は、ベリサインは、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 SSL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))及び(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りません。

(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については、日本ベリサインは、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。

(b) 申請者の事業所の電話番号

申請者の物理的存在及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、日本ベリサイン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、受入られる。

日本ベリサインは、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または1つ以上の公認データベース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。

日本ベリサインは、Section21にあるように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します。

17. 申請者の事業の存在の検証

検証の要件: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、日本ベリサインは、申請者が確実に事業を行っていることを確認する。

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、日本ベリサインは、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) 銀行に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直接文書で確認する。

18. 申請者のドメイン名の検証

日本ベリサインは、EV SSL証明書中に申請者のドメイン名があること検証し、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、日本ベリサインは、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。

日本ベリサインは、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、ベリサインは、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。ドメインの登録された所有者は、親会社もしくは子会社の申請者であるか、申請者の登録された業界一般名であることで、申請者が、ドメインの登録された所有者であることが確信される。

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、日本ベリサインは、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、日本ベリサインは、以下の一つの方法を用いて、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、日本ベリサインは以下の処置を講じなければならない。:
o 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
o 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。

日本ベリサインは、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。

19. 契約書署名者及び証明書承認者の名前、肩書、権限の検証

日本ベリサインは、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：認証機関は、契約書署名者及び証明書承認者(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：日本ベリサインは、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(及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)証明書承認者の権限の付与：日本ベリサインは、証明書承認者以外の情報源により、証明書承認者が、EV SSL 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 SSL証明書申請を提出する権限、及び、該当する場合は、申請者の代理でEV SSL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。及び、
(b) EV SSL証明書発行のために日本ベリサインが申請者に要求した情報を提供する権限、及び、該当する場合は、EV SSL証明書発行のために日本ベリサイン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。及び、
(c) 証明書申請者が提出したEV SSL証明書申請を承認する権限。

契約署名者と証明書承認者が同一人物である場合、契約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、契約署名者と異なる場合には、ベリサインは、名前、役職、代理権(必要な場合)、契約署名者の許可を伴う証明書承認者の許可を確認する。
日本ベリサインは、証明書承認者の権限と契約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(本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、契約書署名者及び証明書承認者(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) 契約書署名者及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、申請者から独立した確認を入手する。

日本ベリサインは、以下に示す方法の一つを用い契約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及び証明書承認者の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する適切に認証された取締役会決議に依拠して検証できます。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及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ベリサインが検証できる場合に限ります。

(2) **申請者から独立した確認**:契約書署名者の署名権限及び証明書承認者の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、申請者から独立した確認を得ることによって確認する。

(3) **認証機関と申請者間の契約**: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日本ベリサイン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及び署名権限が検証されている場合に限る。

(4) **事前に権限を付与された証明書承認者**:日本ベリサイン及び申請者が、日本ベリサインが以下を完了した後、将来的に複数のEV SSL証明書要求の提出を計画している場合。
- o 日本ベリサインが、契約書署名者の名前及び肩書きと、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。
- o 日本ベリサインが、Section19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 SSL 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 SSL証明書またはかかる証明書承認者が承認した全EV SSL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 SSL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)申請者が日本ベリサインの証明書承認者の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りません。

(5) **事前同等権限**: 契約書署名者の署名権限及び証明書承認者の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、ベリサインまたはベリサインの親会社/子会社(あるいはその両方)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 SSL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。
ベリサインは、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) ベリサインまたは親会社/子会社と締結した契約において、申請者の企業登録機関の役割を果たした (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、当該認証機関が発行した1つ以上のSSL証明書の承認に参加した。 この場合、ベリサイン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に電話で証明書承認者に事前に連絡するか、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。

20. 利用規約及びEV SSL 証明書要求の検証

リテールの EVSSL 証明書に対して、各 EV SSL 証明書要求に対して利用規約は、利用規約には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でない場合は、権限を付与された証明書承認者が、別個にそのEVSSL 証明書申請を承認しなければなりません。承認者、契約者いずれの署名も、署名は、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手書き署名(書面による利用規約及び EV SSL 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(電子的な利用規約及び EV SSL 証明書要求の場合)でなければなりません。

(a) 検証要件
リテールEV SSL証明書の発行前、日本ベリサインは、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署名者に本当に申請書類に署名したことを尋ねことで、利用規約の契約書署名者の署名及び各EV SSL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 SSL証明書を発行するためのManaged PKI for SSL アカウントが承認される前に、日本ベリサインは、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、企業契約の署名及びEV SSL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、契約署名者の追加の署名無しで証明書要求を許可できる。

Managed PKI for SSLアカウントへEV用ドメインの追加を行う前に、日本ベリサインは申請者もしくは、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。

先に記述した電話での応答ができない場合、日本ベリサインは、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) 本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申請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及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日本ベリサインが独自に検証できる場合に限ります。

21. EV SSL 証明書申請の承認の検証

日本ベリサインは、要求された EV SSL 証明書発行前に、許可された証明書発行者が、EV SSL 証明書申請を確認し承認したことを確認する。日本ベリサインは、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)で接触しリテール EV SSL 証明書申請の承認について、口頭もしくは書面で入手した証明書承認者による確認により、EV SSL 証明書申請を承認する。

Managed PKI for SSL アカウントを経由して発行する EV SSL 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。

22. 特定の情報源の検証

(a) 検証済み弁護士意見書

(1) 検証の要件:日本ベリサインは、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しなければならない(「検証済み弁護士意見書」)。

(A) 作成者の地位:日本ベリサインは、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しなければならない。

(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)。日本ベリサインは、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:日本ベリサインは、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及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：日本ベリサインは、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日本ベリサインによりセクション22(b)(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。

(b) 検証済み会計士意見書

(1) 検証の要件。日本ベリサインは、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(「検証済み会計士意見書」)ことを検証しなければならない。

(A) 作成者の根拠：日本ベリサインは、会計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会計士(または申請者雇用の社内会計士)(会計士)で、公認会計士、勅許会計士または国際会計士連盟(IFAC)から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全員一致で許可された公認会計士に相当する人物に直接接触する。

(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及び専門知識の行使に基づいて行動する。

(C) 真正性：日本ベリサインは、弁護士意見書の真正性を確認するために、かかる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日本ベリサインによりセクション22(b)(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。

(c)対面認証

対面確認の前に、日本ベリサインは、第三者認証機関が以下の要件を満たすことを確認する。

(A)第三者認証機関の資格：
日本ベリサインは、第三者認証機関は、法的に認められた公証役場もしく(申請者の管轄における法律と同等の)公証役場、弁護士、会計士、公邸権限ある者に直接コンタクトすることで登録者に対する信頼もしくは受入られる管轄内の第三者認証機関からのライセンスによりで独自に認証する。

(B) 関連する資料の管理
日本ベリサインは、第三者認証機関が、個々の認証における対面確認の中で確認資料をみることを確認する。第三者認証機関は、個々の対面の中で個々の認証局に対する確認資料が作られ、得たことを証明しなければならない。

(C) 第三者認証機関が、ラテン系の公証人でない場合、日本ベリサインは、第三者認証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入手をもって、宣誓書と確認資料の信憑性を確認する。日本ベリサインは、この認証手続きに関して、単に第三者認証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、日本ベリサインによって行われる署名の確認はセクション 22(c)(2)(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。

(d) 申請者から独立した確認

「申請者から独立した確認」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)から日本ベリサインが受領したもの。
(ii) 確認元を認証及び検証できる方法で日本ベリサインが受領したもの。及び、
(iii) 申請者を拘束するもの。

申請者から独立した確認は、以下の手順で取得することができる。

(1) 確認要求:日本ベリサインは、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(秘書、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及び肩書によって特定されるか、公認データベース、確認された法的見解、確認された会計士の見解、または、
(ii) 法人設立機関の公式記録に記載された申請者もしくは登録簿の登録代理人または登録事業所宛に、該当する確認者に転送する旨の指示を添付、または
(iii) 個人名においては、申請者の人事部へ電話もしくはメールを用い、契約署名者もしくは証明書承認者に対し代表番号で確認される。(申請者の事業地の認証された電話番号もしくは住所)

(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。以下の方法により行う。
(i) 以下の住所の確認者宛の郵便によって:
(a) これら手続きに従って日本ベリサインが検証した申請者の事業所所在地の住所、または
(b) 現行の公認データベース(SEC ファイルなど)、公認データベース、検証済み弁護士意見書、検証済み会計士レターなどに明記された、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もしくは登録簿の登録代理人または登録事業所の住所、または、

(ii) 現行のQGIS(SECファイルなど)、公認データベース、検証済み弁護士意見書、検証済み会計士レターなどに明記された、確認者の勤務先電子メールアドレスにかかる確認者宛の電子メールによって、または、

(iii) (本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) 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、公認データベース、検証済み弁護士意見書、検証済み会計士レター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: 日本ベリサインは、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日本ベリサインが検証できる限り、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。

(e) 公認データベース(QIIS)
日本ベリサインによってEV SSL証明書申請情報の検証に使用される情報である公認の情報源は、本ガイドラインの要求事項に適合するデータベースを使用する。

(f) 公認の行政機関データベース(QGIS)
日本ベリサインによってEV SSL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、本ガイドラインの要求事項に適合するデータベースを使用する。日本ベリサインは、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。

(g) 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:USA における I.R.S.)

23. その他の検証の要件
(a) 高リスクステータス
日本ベリサインは、詐欺攻撃の標的となるリスクが高いと思われる申請者(「高リスク申請者」)を識別する努力をしなければならず、本ガイドラインに従ってかかる申請者を適切に検証するための合理的に必要と考えられるさらなる検証処置及び予防措置を講じなければならない。

日本ベリサインはフィッシングの疑いや、その他悪意ある使用に備え、失効済みのSSL証明書やEV SSL証明書、以前に拒否されたEV SSL証明書要求を含むデータベースを維持する。
このデータベースは悪意があると思われる疑わしいEV SSL証明書発行要求を判別するために使用される。申請者が疑わしいと判別された場合、日本ベリサインは発行要求者と質問された対象が同一組織に所属していることを確実なものとするため、適切な追加的な認証作業を行う。

(b) 拒否リスト及びその他の法的ブラックリスト
日本ベリサインは、もし申請者、契約書署名者、証明書承認者、申請者の法人設立/登録管轄地および事業所所在地のいずれかが該当するか否かを、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、その他日本ベリサインおよびベリサイン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、または、
(b) 申請者の法人設立/登録管轄地または事業所所在地が日本ベリサイン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。

日本ベリサインは、EV SSL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) 日本ベリサインは、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。
(B) BIS禁輸対象者リスト
(C) BIS禁輸対象組織リスト
(D) 米国財務省の特定国籍業者リスト
(E) アメリカ政府の輸出規制

24. 最終的な相互相関及び
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、Managed PKI for SSL 顧客に対しては行われない。

25. 証明書更新の検証要件

EV SSL 証明書を更新する際、日本ベリサインは、本ガイドラインが要求する全認証及び検証作業を実施して、申請者が更新要求を適切に承認していること、及び EV SSL 証明書に記載の情報が依然として正確かつ有効であることを確認しなければならない。

G. 証明書のステータスの確認及び取り消しの問題

26. EV SSL 証明書のステータスの確認

ベリサインは、ブラウザによって全証明書の現在のステータスをオンラインで自動的に確認できる、24時間365日稼動のオンラインレポジトリ機構を保守する。

(1) EV SSL証明書:
  (A) CRLは、少なくとも7日ごとに更新および再発行され、nextUpdateフィールドの値は10日を超えてはならない。または、
  (B) OCSPは、最大有効期限を10日とし、少なくとも4日ごとに更新しなければならない。

(2) EV SSL証明書のための中間CA証明書:
  (A) CRLは、最大有効期限を12ヶ月とし、少なくとも12ヶ月ごとに更新及び再発行しなければならない。または、
  (B) OCSP. 使用されているならば、EVに対する認証機関証明書のOCSPは、最大有効期限を12ヶ月とし、少なくとも12ヶ月ごとに更新しなければならない。

ベリサインの発行した全EV SSL証明書が生成する多数のクエリーに対して、商業的に合理的と考えられるレスポンスタイムで応答するに十分なリソースを用意して、CRL及びOCSP(あるいは、CRLまたはOCSP)を運用及び保守しなければならない。

CRLまたはOCSPに登録されたエントリーは、失効されたEV SSL証明書の有効期限を越えるまで削除してはならない。

27. EV SSL 証明書の失効

CPS セクション 4.9 に示される失効条件に加え、日本ベリサインは、以下のような場合にはEV SSL証明書の失効を行う。

(1) 加入者がEV SSL証明書の失効を要求したとき
(2) 加入者が、最初のEV SSL証明書要求を承認しなかったことを表明し、さかのぼって承認しないとき
(3) 加入者の(EV SSL証明書内の公開鍵に対応する)秘密鍵に危殆が生じたこと、または、EV SSL証明書の使用にその他の誤りがあったことの合理的な証拠を日本ベリサインが入手したとき
(4) 加入者が利用規約に定める重要な義務に違反したことを、日本ベリサインが通知されたときまたはその他の方法でこれを知ったとき
(5) 裁判所または調停人が加入者のEV SSL証明書に記載されたドメイン名の使用権を取り消したこと、または、加入者がドメイン名の更新を怠ったことを、日本ベリサインが通知されたときまたはその他の方法でこれを知ったとき
(6) EV SSL証明書に記載された情報の大きな変更を、日本ベリサインが通知されたときまたはその他の方法でこれを知ったとき
(7) EV SSL証明書が本ガイドラインまたは日本ベリサインのEVポリシーの条件に従って発行されなかったと、ベリサイン独自の判断で判定したとき
(8) EV SSL証明書に記載の情報のいずれかが正確でないと日本ベリサインが判定したとき。
(9) 日本ベリサインが何らかの理由で業務を停止し、他のEV認証機関によるEV SSL証明書失効の手配をしなかったとき
(10)本ガイドラインに基づく日本ベリサインのEV SSL証明書発行権限が期限切れになったとき、または失効または解約されたとき(日本ベリサインがCRL/OCSPレポジトリの運営継続の手配をした場合を除きます)
(11) EV SSL証明書を発行するCAの秘密鍵に危殆が発生したとき
(12) 加入者が禁輸対象者または重大な性犯罪者としてブラックリストに追加されたこと、あるいは、

業務管轄地の法律で禁止された場所で業務を行っていることを、ベリサインが通知されたときまたはその他の方法でこれを知ったとき

28. EV SSL 証明書に関する問題の報告及び回答

EV SSL証明書加入者、依拠する当事者、アプリケーションソフトウェアベンダ、その他の第三者に対し、EV SSL証明書の悪用に加えて、秘密鍵の危殆の申し立てまたは悪用、EV SSL証明書の誤用、EV SSL証明書に関するその他の詐欺、危殆化、誤用、不適切な行為の報告(「証明書に関する問題の報告」)、24時間365日の報告の受入及び確認体制について、レポートの公開を行う。
https://www.verisign.com/support/ssl-support/ev-misuse/index.html

ベリサインは、全証明書に関する問題の報告の調査を24時間以内に開始し、最低限以下の基準に基づいて失効またはその他の適切な措置を保証するかどうかを決定しなければならない。

(i) 申し立てのあった問題の特性
(ii) 特定のEV SSL証明書またはウェブ・サイトに関する問題の報告件数
(iii) 申し立て主の同一性(たとえば、あるウェブ・サイトが違法な活動をしているという捜査当局からの申し立ては、注文品が届かないという消費者のクレームより重要性が高い)、また、
(iv) 有効な関連法規

ベリサインは、証明書に関する優先度の高い問題の報告に対し24時間365日、内部で対応する体制を整え、申し立てを捜査当局に報告し、申し立ての対象であるEV SSL証明書を失効しなくてはならない。

H. 従業員及び第三者の問題

29. 信頼性及び能力

日本ベリサイン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、日本ベリサインで従業員、代理人、契約社員としてEV SSL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。及び、
(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

日本ベリサインは、全認証スタッフが、本ガイドライン記載のEV SSL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。

30. 登録機関及び下請け業者への機能の委任

ベリサインの明確な同意のある場合のみ、日本ベリサインは、本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、本ガイドラインのSection 24に記載の最終的な相互相関及び適切な注意の要件の履行はこの限りではない。

日本ベリサインは、登録機関機能履行の権限、及び、最初のEV SSL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 SSL証明書(「企業EV SSL証明書」としても知られる)を追加発行する権限を日本ベリサインに付与する権限を、契約により、指定の有効なManaged PKI for SSL顧客に付与することができる。その場合は、サブジェクトは企業登録機関とみなされ、以下が適用される。

(i) いかなる企業登録機関も、その企業登録機関とその企業登録機関が所有または直接支配する企業以外のSubjectに第3ドメインレベル以上の企業EV SSL証明書を発行する権限を、日本ベリサインに付与することはできない。

(ii) いかなる場合も、企業EV SSL証明書のSubjectは、本ガイドラインに従って日本ベリサインが検証した組織でなければならない。
(iii)日本ベリサインは、企業登録機関との契約要件としてこれらの制限を強制し、承認された Managed PKI for SSLの管理者によって、企業登録機関のコンプライアンスを監視しなければならない。
(iv) 本ガイドラインセクション24の最終的な相互相関及び適切な注意の要件については、企業登録機関がこれを実施することができる。また、
(v) 日本ベリサインは、日本ベリサイン自体が要求された本ガイドラインに定められた適用しうる要件への準拠及び履行を、契約により、かかる登録機関、下請け業者、企業登録機関に義務付けなければならない。

I. データ及び記録の問題

31. 書類作成及び監査証跡の要件

(a) ベリサインおよび日本ベリサインは、EV SSL証明書発行の処理に要した全行動を詳細に記録する。たとえば、EV SSL証明書要求に関連して生成された、あるいは受け取った関連する情報、EV SSL証明書要求の処理に要した行動である。これらの記録は、日本ベリサインの業務の監査可能な証拠として使用できるように備えなければならない。また、上記は全登録機関や下請け業者にも適用される。

(b) 前述の記録の要件には、以下の事象を記録する義務が含まれるが、これだけに制限されるものではない。

(i) 以下に示す、認証機関鍵のライフサイクル管理事象:
- (a) 鍵の生成、バックアップ、格納、復元、保管及び廃棄、及び
- (b) 暗号デバイスのライフサイクル管理事象

(ii) 以下に示す、認証機関及び加入者のEV SSL証明書のライフサイクル管理事象
- (a) EV SSL 証明書申請、更新及びリキー要求、及び失効
- (b) 本ガイドラインが要求する全検証活動
- (c) 検証のための電話の日時、使用した電話番号、問い合わせた人物及び結果
- (d) EV SSL 証明書要求の受理及び拒否
- (e) EV SSL 証明書の発行、及び
- (f) EV SSL 証明書失効リスト(CRL)の 作成、OCSP エントリー

(iii) 以下に示すセキュリティ事象
- (a) 成功および失敗したPKIシステムへのアクセスの試み
- (b) PKIおよびセキュリティシステムが実行した処置
- (c) セキュリティ・プロファイルの変更
- (d) システムの故障、ハードウェアエラー、その他の異常
- (e) ファイアウォール及びルーターの動作、及び
- (f) 認証機関施設への出入り

(iv) ログ項目には、以下の要素を含めなければならない
- (a) 記入の日付及び時刻
- (b) 項目の記入を行う人物及びエンティティの同一性
- (c) 項目の説明

32. 文書の保存

(a) 監査記録の保存

独立の監査法人のリクエストに応じて監査記録を提供しなければならない。監査記録は、少なくても7年間保存される。

(b) 文書の保存
ベリサインは、全EV SSL証明書要求及びその検証と全EV SSL証明書及びその失効に関する全文書を、その文書に基づくEV SSL証明書の有効性が停止された後最低7年保存する。それに関連して、ベリサインは、フィッシングまたはその他詐欺の疑いのある使用あるいはその懸念のために、過去に失効されたEV SSL証明書及び過去に拒否されたEV SSL証明書要求の内部データベースを最新の状態に保守する。かかる情報によって、疑わしいEV SSL証明書要求にフラグをつける。

33. 情報及び文書の再使用及び更新

(a) 複数のEV SSL 証明書に対応できる文書の使用
ベリサインは、以下の(b)の記載の期間および更新に関わる要件に従って、単一のEV SSL証明書要求に基づいて、同じSubjectを持つ複数のEV SSL証明書を発行する場合がある。

(b) 既存の情報または文書の使用
(1) 日本ベリサインが発行する全EV SSL証明書は、現行の有効なEV SSL証明書要求と申請者の代理を務める代理人が署名した利用規約に基づくものでなければならない。

(2) 日本ベリサインがEV SSL証明書要求の検証に使用する情報の有効期間は、情報入手日(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、本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、ベリサインが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) 情報が期限切れである場合は、認証機関は、本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。

34. データのセキュリティ
日本ベリサインのセキュリティ・コントロールについては、日本ベリサインCPSのセクション5および6に記述される。

J. コンプライアンス

35. 監査要件
(a) 発行前の準備状況の監査
日本ベリサインがEV SSL証明書を発行する前に、ベリサインは、WebTrust EV Programに照らした期限内準備完了評価監査、または、CA/Browser Forumが承認した同等の監査手順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。

(b) 定期的な自己監査
日本ベリサインは、EV SSL 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 SSL 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、継続的に自己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。

(c) 年次の第三者監査
日本ベリサインは、CA/Browser Forumにより承認された年次の(i) WebTrust Program for CAs auditを行う。また、Issuing CAとしてベリサインは、日本ベリサインによって処理された証明書を含んだ年次のWebTrust Program for CAs auditを行う。このような監査は、ガイドライン下の全認証局の責任に対し、日本ベリサインが直接実行したか代理のRAであるか下請企業であるかに関らず実施される。

本監査報告書は、日本ベリサイン、ベリサインによって公開される。

(d) 監査人の資格
本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及び技術、情報技術及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及びWebTrust EV Program auditsまたはこれに代わるCA/Browser Forum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。及び、

(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、及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。

(e) ルート鍵の生成
本ガイドライン発表後に生成される認証機関ルート鍵については、ベリサインの資格のある監査人は、プロセス及び生成されるベリサインルート鍵の完全性及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、ルート鍵及び証明書の生成プロセスにおけるベリサイン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。

o CPに記載のルート認証機関鍵の生成及び保護手順、バージョン、日付及びCPS、バージョン、日付を記録したこと。
o ルート認証機関のルート認証機関キー・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、適切な詳細手順及び管理を含めたこと。
o CP/CPSに記載の手順及びルート鍵生成手順に従って、ルート認証機関を生成及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。
o 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。
o 鍵生成の全プロセスを監査に備えてビデオに記録する。

K. その他の契約上のコンプライアンス

36. プライバシー/機密に関する事項
EV SSL 証明書検証プロセスの一環として非公開の個人情報を収集、使用、公開するときは、日本ベリサインは、適用されるすべてのプライバシー関連法規及び規制、ならびに公開したプライバシーポリシーを順守する。

37. EV SSL 証明書の損害賠償責任の制限
(a) 認証機関の損害賠償責任
(1) 加入者及び依拠する当事者
日本ベリサインがガイドラインとCPSに準拠してEV SSL証明書の発行および管理を行った場合、日本ベリサインはEV SSL証明書の使用の結果について証明書加入者、依拠者または他の団体のいかなる損害に対しても補償を行わない。日本ベリサインがガイドラインとCPSの従ってEV SSL証明書を発行していなかった場合、利用者対する日本ベリサインの法的責任は、そのEV SSL証明書の使用や信頼したことの結果に対して、紛失や損害を受けた場合は
a. Netsure Protection Plan で保証される損害金額か
b. ＄2.000
の何れかの大きい金額とする。また、依拠当事者や他の第三者に損害が発生した場合、日本ベリサインの責任は、＄2,000を上限として紛失や損害の賠償をする。

(2) アプリケーションソフトウェアベンダの保護
加入者及び依拠する当事者に対する損害賠償責任の制限にかかわらず、日本ベリサインは、ベリサインとルート証明書ライセンス契約を締結しているアプリケーションソフトウェアベンダが、本ガイドラインに定められた認証機関の義務や起こりうる損害賠償責任あるいはEV SSL証明書の発行や保守または依拠する当事者やその他によるこれへの依拠に起因して発生するその他の義務及び起こりうる損害賠償の責を負わないことを理解し確認する。したがって、日本ベリサインは、関連する訴因や法理論にかかわらず、日本ベリサインが処理したEV SSL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ベンダがこうむった申し立て、損害、被害から各アプリケーションソフトウェアベンダを保護するものとする。ただし、日本ベリサインが処理したEV SSL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ベンダがこうむった申し立て、損害、被害が、アプリケーションソフトウェアベンダのソフトウェアが有効なEV SSL証明書を信頼できないと表示した場合の被害については適用されない。

(1)期限切れのEV SSL証明書、または

(2) 失効されたEV SSL証明書

(ただし、無効状態であることをオンラインでCAから判定でき、ブラウザがステータスの確認に失敗したか無効のステータスの表示を無視した場合に限る)

Appendix B2

EV証明書の最小限の暗号アルゴリズムと鍵のサイズ

1. Root CA Certificates

	Certificate issued on or before 31 Dec 2010	Certificate issued after 31 Dec 2 2010
Digest algorithm	MD5 (NOT RECOMMENDED), SHA-1	SHA-1*, SHA-256, SHA-384 or SHA-512
RSA	2048 bit (An end-entity certificate MAY, in addition, chain to an EV-enabled 1024-bit RSA root CA certificate key.)	2048 bit
ECC	224, 233, 256 or 283 bits	224, 233, 256 or 283 bits

2. Subordinate CA Certificates

	Certificate issued on or before 31 Dec 2010	Certificate issued after 31 Dec 2010
Digest algorithm	SHA-1	SHA-1*, SHA-256, SHA-384 or SHA-512
RSA	1024 bit or 2048 bit	2048 bit
ECC	224, 233, 256 or 283 bits	224, 233, 256 or 283 bits

3. Subscriber Certificates

	Certificate issued on or before 31 Dec 2010	Certificate issued after 31 Dec 2010
Digest algorithm	SHA-1	SHA-1*, SHA-256, SHA-384 or SHA-512
RSA	1024 bit or 2048 bit (Note:subscriber certificates containing a 1024 bit RSA key MUST expire on or before 31 Dec 2010)	2048 bit
ECC	224, 233, 256 or 283 bits	224, 233, 256 or 283 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認証機関証明書で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。

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、ベリサインのコントロール下にない下位認証機関に発行されたならば、policy identifiersは、ベリサインの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)
o (ルート認証機関によってコントロールされる下位認証機関ならば) anyPolicy
o (ルート認証機関によってコントロールされない下位認証機関ならば) explicit EV policy OID(s)

次のフィールドは、ベリサイン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
o id-qt 2 [RFC 5280]

CertificatePolicies: policyQualifiers: qualifier
o 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。ベリサインの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。ベリサインの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、ベリサイン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、設定されない。

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) certificate Policies
有効とされ、かつ、Criticalに設定されてはならない。policyIdentifiersは、ベリサインEVポリシーへの識別子を含まなければならない。

certificatePolicies:policyIdentifier (Required)
o EV policy OID

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

certificatePolicies:policyQualifiers:qualifier (Required)
o 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、ベリサインのCRLサービスのHTTP URLを含む。このエクステンションは、証明書が、OCSPレスポンダーを証明書エクステンション中のauthorityInformationAccessで識別しない場合には、有効でなければならない。詳細は、section 26(b)を参照。

(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。ベリサインの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、ベリサイン証明書に含まれる場合がある (accessMethod = 1.3.6.1.5.5.7.48.2)。証明書にcRLDistributionPointエクステンションが含まれないならば、このエクステンションは、必須である。

(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。

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:本付録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、登録が本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、本付録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。

もし日本ベリサイン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、日本ベリサイン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) 日本ベリサイン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) 日本ベリサイン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、Cに本ベリサインは、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。日本ベリサイン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。