日本ベリサイン株式会社
タイムスタンプ局向け
認証局運用規程
（Certification Practice Statement）

Version 1.1

Effective Date: December 15, 2006

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
https://www.verisign.co.jp/

更新日　2006 年 12 月 15 日

商標に関する表示

謝辞

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

目次

1. はじめに

「日本ベリサイン株式会社タイムスタンプ局対応認証局運用規程（Certification Practice Statement)」（以下、「本 CPS」と呼ぶ）は、日本ベリサイン株式会社（以下「日本ベリサイン」と呼ぶ）が「日本ベリサイン株式会社 タイムスタンプ局対応 企業用電子証明書発行サービス」（以下、「本サービス」と呼ぶ）における電子証明書の発行、管理、失効および更新を含む一連の運用に関して採用する手続きを記載したものです。

1.1 概要

1.1.1 サービスの概要

本サービスは日本ベリサインが提供するサービスであり、第三者機関として信頼を提供する組織に対して電子証明書を発行するサービスです。日本ベリサインが発行する電子証明書はタイムスタンプ局が時刻配信業務を行う際に利用されることを目的とします。

なお、本サービスは、以下の文書の適用範囲外です。

- VeriSign, Inc.の規定する「VeriSign Trust Network Certificate Policies」
- 日本ベリサインの規定する「日本ベリサイン株式会社 認証業務運用規程 (Certification Practice Statement)」

1.1.2 CP/CPS の役割

本 CPS は本サービスにおけるビジネス的、法的、技術的な事項について記述しています。本 CPS は本サービス関係者に対し本サービスにおける証明書ポリシー（電子証明書の発行基準)、および、具体的な実践方針について記述します。

本認証サービスでは証明書ポリシーを規定するための CP を本 CPS と独立して規定しません。本認証サービスにおける証明書ポリシーは本 CPS に含まれています。

1.1.3 CP/CPS に関する標準との関係

本 CPS は、IETF(Internet Engineering Task Force) の PKIX(Public Key Infrastructure working group)が提唱する「証明書ポリシーと認証実践の枠組み(Certificate Policy and Certification Practices Framework)」(RFC2527)に従い記述されています。

1.2 文書名と同定

本サービスにおける証明書ポリシーに対するオブジェクト識別子 (OID) は、次の通りとします。

証明書ポリシーOID： 1 2 392 200207 1 1

1.3　参加者と適用範囲

本サービスに関連する参加者は、以下の図１に示す通りです。

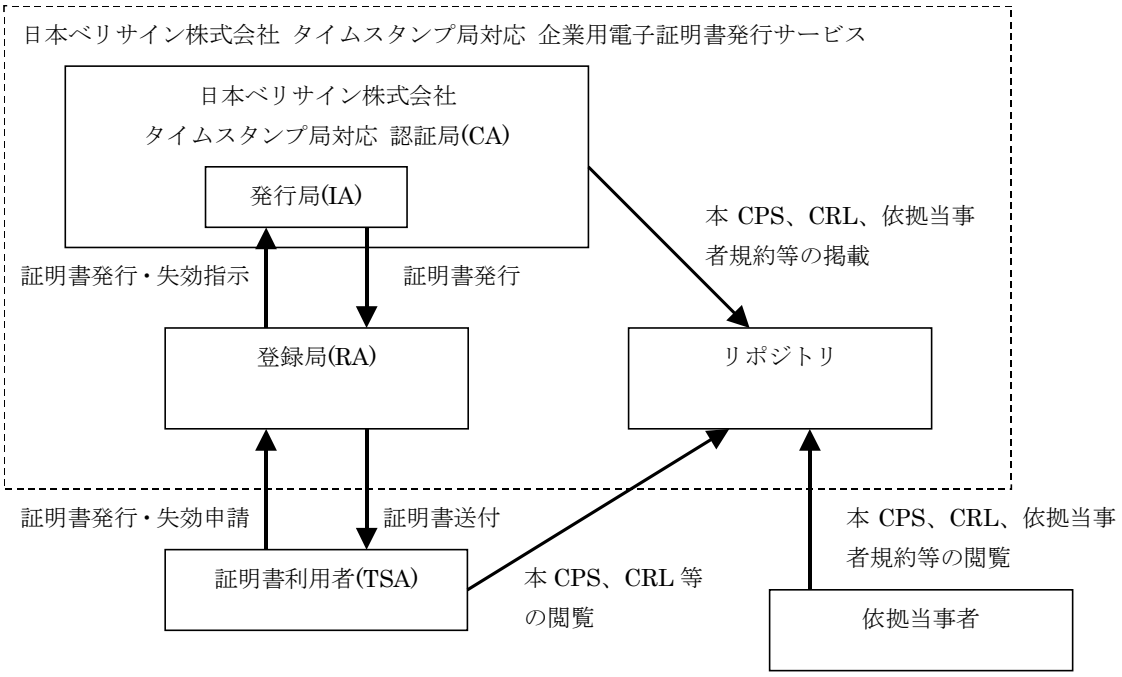

図１　本サービスにおける参加者

本 CPS において、「日本ベリサイン株式会社 タイムスタンプ局対応 企業用電子証明書発行サービス」は、認証局、登録局、およびリポジトリを含む総称として取り扱います。

本節では、これら参加者に関する説明と、本サービスにて発行した電子証明書の適用範囲についての説明を行います。

1.3.1　認証局

認証局（CA：Certification Authority）とは、認証局の秘密鍵を管理し、電子証明書の発行、管理、失効を行う機関です。本サービスおける日本ベリサインタイムスタンプ局対応 認証局（以下、「本認証局」と呼ぶ）は、ルート認証局と発行局（IA: Issuing Authority）を兼ねています。発行局は、登録局から電子証明書の発行および失効指示を受け、証明書発行処理、証明書失効処理を行います。また、失効された電子証明書のリスト（CRL: Certificate Revocation List）の発行を行います。認証局は、認証局自身の公開鍵に対して電子証明書を発行します。認証局の公開鍵に対して発行された電子証明書を、認証局証明書と呼びます。

本サービスにおいて、認証局は日本ベリサインによって運用されています。

1.3.2　登録局

登録局（RA: Registration Authority）とは、証明書利用者の識別と証明書利用者の電子証明書

に関する発行および失効の申請の指示に基づき、発行局に対して利用者証明書に関する発行および失効の指示を行う機関です。電子証明書の発行指示および失効指示は、登録局に設置される端末から安全な通信方法を介して行われます。
本サービスにおいて、登録局は日本ベリサインによって運用されています。

1.3.3　証明書利用者
証明書利用者とは、電子証明書を日本ベリサインタイムスタンプ局向け認証局から取得し、電子証明書に記載された公開鍵と対になる秘密鍵を管理する者あるいは組織です。本 CPS では、利用者に対して発行された電子証明書を利用者証明書と呼びます。

本サービスにおいて証明書利用者は、日本ベリサインの規定する手続きに従って電子証明書の発行を申し込み、本認証局によって電子証明書の発行を受けた TSA です。

1.3.4　依拠当事者
依拠当事者（RP: Relying Parties）とは日本ベリサインタイムスタンプ局向け認証局が発行した電子証明書に記載された公開鍵と対になる秘密鍵によって作成された署名を検証する者あるいは組織です。

本サービスにおいて依拠当事者は、証明書利用者である TSA が発行したタイムスタンプを利用あるいは検証する者です。

1.4　証明書用途
1.4.1　適切な証明書用途
本サービスが提供する電子証明書は、証明書利用者（TSA）の発行するタイムスタンプへの署名付与の際のみに利用することができます。
また、本サービスは、秘密鍵による署名の作成あるいは電子証明書の検証を問わず日本国内でのみの利用されることを想定しています。海外での利用に際しては、証明書利用者、および、依拠当事者は自らの責任において利用の判断を行う必要があります。

1.4.2　禁止される証明書用途
本サービスが発行する電子証明書を、以下のような利用目的のために使用することを禁止します。
・ 原子力の制御、航空管制、重要な交通の制御、医療など人命の危険を伴う状況
・ 障害により、人命や環境が危険にさらされるような重要な状況
・ 犯罪行為、および、公序良俗に反する行為
・ 暗号技術を危殆化させるような試み

1.5 ポリシーの運営

1.5.1 CPS を管理する組織

日本ベリサインにおける本 CPS の管理部署の連絡先は以下の通りです。

日本ベリサイン株式会社
〒104－0028 中央区八重洲 2－8－1 法務部宛
電話 03-3271-7012
FAX 03-3271-7031
practices@verisign.co.jp

1.5.2 サービスの窓口

本サービスに関する問い合わせ窓口は以下の通りです。
担当部署： マーケティング部
住所： 〒104－0028 中央区八重洲 2－8－1
電話番号： 03-3271-7014
FAX 番号： 03-3271-7028

1.5.3 ポリシーに対する CPS の適合性を決定する人

本 CPS1.5.1 に記載の組織が、本 CPS および本 CPS を補充しまたはこれに従属する文書が、CP または本 CPS に適合するかどうかの決定をする責任を有します。

2. 一般規定

2.1 義務

2.1.1 認証局の業務に関する義務

(1) 本認証局は、本 CPS に基づき運用を行います。
(2) 本認証局は秘密鍵（以下「認証局秘密鍵」といいます）が危殆化（盗難、漏洩等によりその機密性を失うこと。以下同じ）しないよう、善良なる管理者の注意をもって管理します。
(3) 本認証局は、システム保守による一時停止、緊急時など、やむを得ない場合の停止を除き、CRL を作成し定期的にリポジトリに登録し、公開します。
(4) 本認証局は登録局の発行指示にもとづき証明書証明書の発行、失効を行います。

2.1.2 登録局の業務に関する義務

(1) 登録局は、本 CPS に基づき運用を行います。
(2) 登録局は、証明書利用者の証明書発行申請を、本 CPS に定められた手続きにしたがって適正に審査し、発行局に対して利用者証明書の発行指示を行います。
(3) 登録局は、証明書利用者の証明書失効申請を、本 CPS に定められた手続きにしたがって適正

に審査し、発行局に対して利用者証明書の失効指示を行います。
(4) 登録局は、電子証明書の発行および失効に関わる証明書利用者の秘密情報を適切に管理します。
(5) 登録局は、証明書利用者に利用規約への合意を要求し、また、合意を確認します。

2.1.3　証明書利用者の義務

証明書利用者は、利用者証明書の利用に先立ち、利用規約に合意する必要があります。利用規約には以下のような、証明書利用者の義務が含まれています。
(1) 秘密鍵の保護
証明書利用者は秘密鍵が他人に使用されないように十分な管理を行う必要があります。証明書利用者は秘密鍵が記録された装置を他人に貸与してはならず、また、複製などが行われないように安全に保護する義務があります。
(2) 虚偽申請の禁止
証明書利用者は利用者証明書の申請にあたり、虚偽の申告や記載を行った申請を行ってはなりません。
(3) 申請の義務
証明書利用者は秘密鍵が危殆化した恐れのある場合、使用を中止する場合、または、申請情報に変更が生じた場合に、遅延なく登録局に対し失効申請を含む適切な申請を行う必要があります。
(4) 証明書及の利用範囲
本 CPS では、利用者証明書の利用範囲を記載しています。利用者はその範囲外の用途に、証明書を使用してはなりません。
(5) 証明書利用制限
証明書利用者は、秘密鍵が危殆化につながるような行為を行ったり、悪意を持った利用を行ってはなりません。利用者は利用者証明書を危険な環境で利用してはならず、また、認証局証明書として使用してはなりません。
(6) 秘密鍵生成時の義務
証明書利用者は、RSA 方式（オブジェクト識別子：1 2 840 113549 1 1 1)、2048bit の鍵長で秘密鍵と公開鍵の鍵ペアを自ら適切に作成し、電子証明書の発行申請時にその公開鍵を提示しなければなりません。
(7) 秘密鍵の有効期間
証明書利用者は、秘密鍵を本 CPS6.3.2 で定める有効期間を超えて使用してはなりません。
(8) 名称に関する所有権の確認
証明書利用者は、申請時に記載する個人あるいは組織の名称の所有権が申請者に帰属することを確認し、また、その名称が他人の名称に関する所有権を侵害していないことを事前に確認する必要があります。
(9) CPS への準拠

証明書利用者は、本 CPS の内容を理解し、合意する必要があります。
(10) 利用規約への合意
証明書利用者は、別途定める利用規約を理解し、合意する必要があります。

2.1.4　依拠当事者の義務
依拠当事者は、依拠しようとする電子証明書が、自己の利用の目的に対して適切であることを自己の判断で確認しなければなりません。依拠当事者は本 CPS、日本ベリサインが公表する情報、証明書利用者が公表する情報、および、暗号技術に関する一般的な情報が上記の判断に十分でないと判断した場合には電子証明書に依拠してはなりません。
また、依拠当事者は、以下の義務を負います。
(1) 電子証明書の真正の確認
依拠当事者は、証明書の信頼の起点とすべき信頼点（トラストアンカ）となる認証局を判断し、当該認証局の認証局証明書をリポジトリから確実に入手しなければなりません。依拠当事者は、依拠しようとする利用者証明書に認証局の秘密鍵による電子署名が正しく付与されており、当該利用者証明書が本認証局から発行されたものであること、並びに当該利用者証明書が改ざんされていないことを確認しなければなりません。
(2) 電子証明書の有効性の確認
依拠当事者は、利用者証明書が検証時点において有効期間内であることを確認しなければなりません。また、依拠当事者は、利用者証明書内に記載されたリポジトリから CRL を取得し、利用者証明書が検証時点において失効されていないことを確認しなければなりません。
(3) リポジトリの閲覧
依拠当事者は、本サービスに関する変更の情報や CRL の情報を取得するため、リポジトリを閲覧しなければなりません。
(4) CPS への準拠
依拠当事者は電子証明書への依拠に先立ち、本 CPS の内容を理解し、合意する必要があります。
(5) 依拠当事者規約の合意
依拠当事者は電子証明書への依拠に先立ち、依拠当事者規約（RPA: Relying Party Agreement）を理解し、合意する必要があります。
(6) 利用範囲の確認
利用者証明書の利用範囲は本 CPS1.4.1 で規定されています。依拠当事者は、本 CPS が規定する利用範囲以外の目的において電子証明書に依拠してはなりません。

2.1.5　リポジトリの義務
リポジトリは、依拠当事者が利用者証明書の有効性を検証できるように以下の情報を公開します。

- 本 CPS（過去のものも含む）
- 利用者証明書（失効されたものや有効期間満了後のものも含む）

・ CRL（過去のものも含む）
・ その他、本 CPS2.6 で規定する情報

また、リポジトリは、災害や障害あるいは保守などのやむを得ない場合を除き、1 日 24 時間、年間を通じて運用します。

2.2 責任

2.2.1 認証局の責任

2.2.1.1 認証局の保証

日本ベリサインは、本サービスの提供において、以下の事項を保証します。

・本認証局の業務が、本 CPS に基づき運用されていること
・本 CPS および関連文書が、適切に管理されていること

2.2.1.2 認証局の責任の制限

本認証局の責任は、本 CPS に定める認証局業務を善良なる管理者の注意をもって行うことに限られます。日本ベリサインは、本 CPS において本認証局が免責される旨を明示している事項や、本認証局の責任や義務を明示していない一切の事項について何ら保証せず、一切の義務および責任を負わないものとします。

また、日本ベリサインは、証明書利用者である TSA の時刻認証業務に関する責任を負いません。

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および依拠当事者規約および他の利用規約は、日本ベリサインの責任を制限しています。日本ベリサインは、間接損害、特別損害、付随的損害および結果的損害に関しては何らの責めをも負いません。

2.2.1.3 免責事項

以下の事象が発生した場合、日本ベリサイン、証明書利用者および依拠当事者に対し免責とします。

(1) 地震、水害、噴火などのあらゆる天災に起因する損害
(2) 火災、停電などのあらゆる災害に起因する損害
(3) 戦争、動乱、および、その他のあらゆる不可抗力に起因する損害
(4) 証明書利用者、および、依拠当事者における署名、および、署名の検証に用いるソフトウェア、ハードウェアの誤動作、または、障害に起因する損害
(5) 認証業務の一部、または、全部の終了に伴う証明書発行の停止、ならびに、停止するリポジトリサービスに起因する損害
(6) 電子証明書の失効処理を遅延なく行い、CRL に登録し、これを公表したにもかかわらず、当該失効情報が掲載された CRL の公表前に依拠当事者が利用者証明書への依拠を行った結果発生する損害

(7) 利用者、および、依拠当事者が CPS、利用規約、または、依拠当事者規約に定められた義務を果たさなかった結果発生した損害

また、本認証局は ISO や IETF 等の国際的な技術検討機関によって標準技術と定められた十分に解読が困難であると考えられる高度な暗号技術に基づいて提供されていますが、当該暗号技術が将来において解読危殆化した結果発生しうる損害について一切責任を負わないものとします。

2.2.2　登録局の責任

登録局は、本 CPS に従い、利用者証明書の発行申請および失効申請を行った証明書利用者の真偽の確認を適切に行い、発行局に対して適切な指示を行うことで、本認証局の発行・失効する利用者証明書に係る情報の信頼性を確保します。また、利用者の真偽確認のために提供された個人情報等を適切に保護します。

2.2.3　証明書利用者の責任

証明書利用者は本 CPS2.1.3 ならびに利用規約で示される利用者の義務を順守しなかった場合、あるいは、利用者証明書を利用すべきではない環境において使用した結果発生する日本ベリサインおよび依拠当事者の損害に対し責任を負うものとします。

2.2.4　依拠当事者の責任

依拠当事者は本 CPS2.1.4 ならびに依拠当事者規約で示される依拠当事者の義務を順守しなかった場合、あるいは、利用者証明書に依存すべきではない環境において使用した結果発生する損害、日本ベリサインおよび証明書利用者の損害に対し責任を負うものとします。

2.3 財務上の責任

日本ベリサインの財務情報は、下記の URL より入手が可能です。

https://www.verisign.co.jp/corporate/investor/index.html

2.3.1　証明書利用者、および、依拠当事者による保証

2.3.1.1 証明書利用者による保証

証明書利用者は、本 CPS2.1.3 で示される義務について、その他の参加者に対し保証を行う必要があります。利用者はこの保証が守られなかった結果発生する損害に対し賠償責任が発生します。

2.3.1.2 依拠当事者による保証

依拠当事者は、本 CPS2.1.4 で示される義務について、その他の参加者に対し保証を行う必要があります。依拠当事者はこの保証が守られなかった結果発生する損害に対し賠償責任が発生します。

2.4 解釈、および、執行

2.4.1 準拠法

本 CPS の執行、解釈および有効性は、証明書利用者と依拠当事者間の契約や他の準拠法を選択する旨の規定の有無に係らず、また、日本国に営業上の関連性を有するか否かを問わず、日本国内法および規則に従って判断されます。この準拠法の選択は、証明書利用者の住所地または電子証明書の使用地の場所を問わず、全関係者において統一的な手続きおよび解釈を確保するためのものであり、証明書利用者の使用するソフトウェア、ハードウェアや、技術情報の輸出入を制限するものではありません。

証明書利用者および依拠当事者が電子証明書の利用、または、依拠のために使用するソフトウェア、ハードウェアや、技術情報に関しては、証明書利用者、または、依拠当事者の責任において適切な関連法を遵守する必要があります。

2.4.2 分割、継続、併合および、通知

2.4.2.1 CPS 等の可分性

本 CPS、および、その他の契約、合意の一部分の規定が、いかなる程度でも無効または執行不可能であるとされた場合であっても、本 CPS、および、その他の契約、合意のその他の規定の有効性には影響を及ぼさず、日本ベリサインの意思に最も合理的に合致するよう解釈されるものとします。

2.4.2.2 効力の存続

本認証局が廃止され、または本サービスが終了した場合においても、秘密情報の扱いに関する規定の効力は存続するものとします。

2.4.2.3 CPS、および、その他の契約、合意の完全性と通知

本サービスの権利義務に直接影響する本 CPS、および、その他の契約、合意の規定は、本 CPS に別段の定めをしている場合を除き、書面によらず口頭で修正、放棄、追加、変更、削除または終了させることはできないものとします。

証明書利用者や依拠当事者が、本 CPS、および、その他の契約、合意に対して何らかの通知、請求、依頼をする場合の連絡手段は、本 CPS で定められた通知先に対し行われるものとします。また、日本ベリサインが重要な通知を行う場合にはリポジトリを通じて行うこととします。

2.4.3　紛争解決の手続き

本 CPS、その他の契約、または本認証局が発行した電子証明書に関して生じた紛争についての専属的合意管轄裁判所は東京地方裁判所とします。本 CPS およびその他の契約に定められていない事項やこれらの文書の解釈に関して疑義が生じた場合、各当事者は、その課題を解決するために訴訟に先立ち誠意をもって協議するものとします。

2.5 料金

2.5.1　証明書の発行料金

日本ベリサインは、証明書利用者に対し、利用者証明書の発行、管理および更新に関して手数料を請求することができるものとします。

2.5.2　証明書アクセスに関する料金

日本ベリサインは、電子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できるようにする対価としての手数料を請求しません。

2.5.3　失効、および、ステータス情報アクセスに関する料金

日本ベリサインは、本 CPS4.4.9 により要求される CRL 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ません。

2.5.4　ポリシー情報などの他のサービスに関する料金

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ません。文書の単純な閲覧以外の目的、例えば複製、再配布、変更または派生的書面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契約を締結することを条件とします。

2.5.5　払い戻しポリシー

本サービスにおいては、次の返金制度
（http://www.verisign.co.jp/repository/refund/index.html）が適用されます。

日本ベリサインは、証明書業務の運用および電子証明書の発行において、厳格な実務と方針を厳守し、これに従います。しかしながら、理由の如何を問わず、証明書利用者が自己に発行された利用者証明書について十分に満足しない場合、証明書利用者は日本ベリサインに対して、発行から 30 日以内に利用者証明書を破棄し、証明書利用者に払戻しをするよう要請することができます。証明書利用者または利用者証明書に関して、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、証明書利用者は、日本ベリサインに対し、利用者証明書を破棄し、払戻しをするよう要請することができます。日本ベリ

サインは、利用者証明書を破棄した後、速やかに、利用者証明書に支払われた申請料の全額を、利用者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証明書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、証明書利用者の指定する銀行口座への振込みにて証明書利用者に償還します。証明書利用者が払戻しを要請する場合は、日本ベリサインカスタマサポート 044-520-7210 に連絡ください。この払戻制度は、証明書利用者にとっての唯一の救済方法ではなく、また証明書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ありません。

2.6 公表とリポジトリ

2.6.1 認証局に関する情報の公表

日本ベリサインは、リポジトリ上において本サービスに関連する以下の情報を公開します。

本 CPS：

https://www.verisign.co.jp/repository/tsa/cps.pdf

依拠当事者規約：

https://www.verisign.co.jp/repository/tsa/rpa.pdf

認証局証明書：

https://www.verisign.co.jp/repository/tsa/root.zip

認証局証明書のハッシュ値：

https://www.verisign.co.jp/repository/tsa/index.html

CRL：

http://onsitecrl.verisign.co.jp/VeriSignJapanKKVeriSignJapanTimeStampingCA/LatestCRL.crl

2.6.2 公表の頻度

本サービスのリポジトリ上に公表される情報の更新頻度は以下の通りとします。

本 CPS：

改版の都度

依拠当事者規約：

改版の都度

認証局証明書：

認証局証明書の発行の都度

認証局証明書のハッシュ値：

認証局証明書の発行の都度

CRL：

24 時間ごと

2.6.3　アクセス制御

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、公にアクセス可能なものです。当該情報に対する閲覧だけのアクセスは制限されないものとします。日本ベリサインは、電子証明書、電子証明書の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します。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および物理的なセキュリティの手段を講じています。

2.6.4　リポジトリ

本 CPS 2.1.5 参照。

2.7　準拠性監査

2.7.1　準拠性監査の頻度

本サービスの認証局の設備（以下、「認証局設備」と呼ぶ）においては、準拠性監査を随時実施します。

2.7.2　監査人の識別／認定

認証局設備の監査人は PKI に関する十分な知識を持った者が任命されます。

2.7.3　監査人の被監査人との関係

認証局設備の監査人は運用部門とは独立した部門の者が任命されます。

2.7.4　準拠性監査のトピック

規定しません。

2.7.5　監査指摘事項への対応

監査結果での指摘事項を踏まえ、新技術の動向を考慮して業務、および、設備の改善を行い、必要である場合は本 CPS を改訂し、その結果の評価を行います。

2.7.6　監査結果

認証局設備の監査結果は公開されません。ただし、公的機関から法律に基づく開示要求があった場合や、公表が妥当であると認証局運用者が判断した場合、監査結果を開示します。

2.8 機密保持

2.8.1 機密扱いとする情報

2.8.1.1 機密扱いとする情報の種類

本サービスが保有する以下の情報は秘密情報とします。

(1) 証明書申請記録

(2) 処理記録（全ての記録および監査証跡記録の双方を含む）

(3) 偶発事故に対する災害復旧計画

(4) 認証局設備のハードウェアおよびソフトウェアの運用並びに証明書サービスおよび申請サービスの管理を制御するセキュリティの手段

(5) 監査人によって作成された監査記録

2.8.1.2 個人情報の取り扱い

個人情報とは、証明書利用者から提供される名称、属性、その他証明書利用者から利用者証明書の登録、申請、失効に関する契約時に提供される情報であって、個人を特定可能な情報を指します。個人情報が利用者証明書、CRL など公開することが規定された情報である場合には秘密情報として取り扱いません。

日本ベリサインのプライバシー・ポリシーは、以下の URL にて閲覧可能です。

http://www.verisign.co.jp/repository/privacy/privacy_statement.html

2.8.2 秘密扱いとしない情報

本サービスは以下の情報を秘密扱いとしません。

(1) 電子証明書に記載される情報

(2) 本 CPS2.8.3 において、公表されると記載されている証明書失効に関する情報および他のステータス情報

(3) リポジトリ上に公開される情報

2.8.3 証明書失効情報の公表

電子証明書が失効された場合、CRL 内の情報として、失効された電子証明書のシリアル番号および失効日時が記載されます。また、失効事由が記載される場合があります。CRL に記載された情報は秘密とみなされません。また、失効に関するその他の情報は秘密情報として扱います。

2.8.4　法執行機関への情報公開

本サービスで取扱う秘密情報に対して、裁判手続き、行政手続きまたはその他の法的手続きに対応するために法執行機関から開示の要求があった場合、法執行機関に対し秘密情報を開示することができるものとします。また、本サービスで取扱う個人情報については、個人情報保護に関する法令に従います。

2.8.5　民事手続き上の情報公開

訴訟、調停等の裁判手続き、行政手続きまたはその他の法的手続きに対応するために、日本ベリサインが必要と判断した場合は、本サービスで取扱う秘密情報を開示することができるものとします。また、本サービスで取扱う個人情報については、個人情報保護に関する法令に従います。

2.8.6　利用者の要求に基づく公開

本 CPS 2.8.1.2 参照。

2.8.7　その他の公開条件

規定しません。

2.9　知的財産権

別段の合意がなされない限り、以下の情報およびデータに関する著作権その他の知的財産権は日本ベリサインに帰属し、その他の者には帰属しないものとします。

(1)本認証局から発行された利用者証明書（ただし、利用者の公開鍵情報を除く）
(2)本認証局から発行された認証局証明書
(3)本認証局の秘密鍵
(4)本認証局により作成された失効情報（CRL を含む）
(5)本 CPS
(6)利用規約
(7)依拠当事者規約
(8)その他リポジトリで公表する情報

日本ベリサインは本 CPS に合意した証明書利用者、または、依拠当事者にのみ失効情報、認証局証明書の複製を許可します。その他、リポジトリで公開される情報は、無断で複製、転載などを行うことを禁止します。

別段の合意がなされない限り、以下の情報およびデータに関する著作権その他の知的財産権は証明書利用者に帰属し、依拠当事者その他の者には帰属しないものとします。

(1)電子証明書に記載される情報のうち、サブジェクト名の識別名として記載される名称の知的

財産権、および、商標
(2)証明書利用者の秘密鍵

3. 識別と認証
3.1 初期登録
3.1.1 名称のタイプ
本認証局が発行する電子証明書の発行者名(issuer)フィールドおよびサブジェクト名(subject)フィールドに含まれる識別名が準拠する規格は、ITU-T Recommendation X.500 形式の識別名（DN：Distinguished Name）です。

3.1.2 名称の意味
本認証局が発行する認証局証明書の発行者名フィールドおよびサブジェクト名フィールドに記載される名称は、表１のように設定されます。

属性名		属性値	備考
発行者名（issuer）			
	国名（country）	c=JP	
	組織名（organizationName）	o=VeriSign Japan K.K.	
	共通名（commonName）	cn=VeriSign Japan Time Stamping CA	
サブジェクト名（subject）			
	国名（country）	c=JP	
	組織名（organizationName）	o=VeriSign Japan K.K.	
	共通名（commonName）	cn=VeriSign Japan Time Stamping CA	

表１ 認証局証明書の発行者名フィールドおよびサブジェクト名フィールド

本認証局が発行する利用者証明書の発行者名フィールドおよびサブジェクト名フィールドに記載される名称は、表２のように設定されます。

属性名		属性値	備考
発行者名（issuer）			
	国名（country）	c=JP	
	組織名（organizationName）	o=VeriSign Japan K.K.	

属性名		属性値	備考
	共通名 (commonName)	cn=VeriSign Japan Time Stamping CA	
サブジェクト名 (subject)			
	国名 (country)	c=……	利用者の申請に応じて記載。
	都道府県名 (stateOrProvinceName)	st=……	利用者の申請に応じて記載。
	市町村名 (localityName)	l=……	利用者の申請に応じて記載。
	組織名 (organizationName)	o=……	利用者の申請に応じて記載。
	組織単位名 (organizationalUnitName)	ou=……	利用者の申請に応じて記載。
	共通名 (commonName)	cn=……	利用者の申請に応じて記載。

表 2　利用者証明書の発行者名フィールドおよびサブジェクト名フィールド

利用者証明書のサブジェクト名フィールドに含まれる識別名の組織名 (= o)の記載事項は、組織もしくは組織内の部署の正当な名称です。

3.1.3　名称の変換ルール

規定しません。

3.1.4　名称の一意性

本認証局が発行する有効な電子証明書の証明書利用者の識別名は、一意に割り当てられるものとします。

3.1.5　名称に関する紛争解決手段

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りません。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いません。また、日本ベリサインは、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もありません。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します。

3.1.6　商標の認識、認証および役割

本 CPS3.1.5 参照。

3.1.7　秘密鍵の所有を証明する方法

日本ベリサインは、証明書申請者が秘密鍵を所有していることを、PKCS #10 に従った電子署名のされた証明書リクエストの利用、これと技術的に同等とみなすことができる方法その他日本ベリサインが認めた方法を通じて、検証します。

3.1.8　組織の認証

法人による電子証明書の申請に先立って、登録局は以下の方法により法人の真偽の確認、および、申請情報の真正性確認を行います。

(1)日本ベリサイン株式会社タイムスタンプ局向け証明書発行サービス利用申し込み書

(2)法人登記簿謄本の写し、もしくは日本ベリサインが定める方法

(3)代表者の印鑑証明

3.2　証明書の更新

電子証明書の更新時における鍵ペアの扱いについては 2 通りの方式が想定されます。

方式 1：認証局証明書の更新に合わせ鍵ペアを置き換える鍵更新方式（リキー）

方式 2:同じ鍵ペアに対し有効期間を延長した電子証明書を発行する延長方式(リニューアル)

本認証局が発行した電子証明書は、上記の 2 つのいずれかの方式により更新されます。

3.2.1　利用者証明書の更新

利用者証明書の更新に際して、日本ベリサインは本 CPS3.1.8 と同等の認証を行います。なお、本サービスでは、利用者証明書および証明書利用者の秘密鍵の有効期間を本 CPS6.3.2 で定めています。

3.2.2　認証局証明書の更新

本認証局では、方式 2 により認証局証明書の延長（リニューアル）を行います。

延長（リニューアル）が行われた場合、延長（リニューアル）後の認証局証明書の識別名、および、有効期間の開始日時は延長（リニューアル）前の認証局証明書と同じ値です。

認証局証明書の延長(リニューアル)は認証局の運用者により、複数人の信頼できる人間のもと、制御された手順によって行われます。

3.3　証明書失効後の再発行

利用者証明書が失効された後の再発行は、本 CPS 3.2.1 に従って行うことができます。

3.4　失効要求

電子証明書の失効前に、日本ベリサインは失効要求が証明書利用者によってなされたものであることを検証します。証明書利用者の失効要求を認証するための手続きには、次のものを含みます。

・ 失効を要求する者または組織が、実際に証明書利用者であるという合理的な保証を提供する者と連絡すること。状況に応じて、この連絡には、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、本認証局が発行した利用者証明書の失効を要求することができます。日本ベリサインは、管理書の同一性を SSL およびクライアント認証を利用するアクセス・コントロールを通じ認証したうえで、管理者が失効を行うための役割を果たすことを認めます。

4. 運用要件

4.1 証明書申請

全ての利用者証明書の申請者は、利用者証明書の証明書申請にあたり、次の各項目からなる申請手続きを履行するものとします。

・ 証明書申請フォームを完成させ、要求される情報を提供すること
・ 本 CPS6.1.1.1 に従い、鍵ペアを生成すること
・ 証明書申請者が、本 CPS6.1.3 に従い、自己の公開鍵を直接、日本ベリサインに引き渡すこと
・ 本 CPS3.1.7 に従い、証明書申請者が日本ベリサインに引き渡した公開鍵に対応する秘密鍵を所有していることを明らかにすること、並びに
・ 関連する利用規約に対する同意を明示すること

4.2 証明書発行

証明書申請者が、証明書申請を送信した後、日本ベリサインは、証明書申請中の情報（ただし、未検証利用者情報を除く）を、本 CPS3.1.8 および 3.1.9 に従い、確認するよう試みます。本 CPS3.1 に従い、全ての必要な認証手続きが成功裡に完了次第、日本ベリサインは証明書申請を承認します。もし、認証が不成功に終わった場合には、日本ベリサインは証明書申請を拒絶します。

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の後に、証明書を生成し発行します。本節に定める手続きは、電子証明書の更新（すなわち、リキー）の要求の送信に関連して電子証明書を発行する場合にも適用されます。

4.3 証明書の受領

電子証明書が生成され次第、日本ベリサインは証明書利用者に対し、その電子証明書が利用可能になった旨を通知するとともに、証明書利用者に対し、当該証明書を入手する手段を通知します。電子証明書が発行され次第、電子証明書は証明書利用者がウェブ・サイトからダウンロードするか、または当該利用者に対する電子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証明書利用者が利用することができるようになります。例えば、日本ベリサインは証

明書利用者に対し、個人識別番号(PIN)を送り、当該利用者は当該個人識別番号(PIN)を利用して申込用ウェブ・ページに入って電子証明書を取得することができます。電子証明書は、また証明書利用者に対し電子メールによって送信することもできます。電子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電子証明書のインストールは、証明書利用者による電子証明書の受領とみなします。

4.4 証明書失効、および、一時停止

4.4.1 失効条件

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ます。

- 日本ベリサインまたは証明書利用者において、証明書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
- 日本ベリサインにおいて、証明書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
- 証明書利用者との契約が終了した場合
- 日本ベリサインにおいて、電子証明書が本 CPS によって要求される手続きに重要な点において従っていないか、電子証明書が電子証明書上にサブジェクト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、または電子証明書が当該証明書上にサブジェクト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
- 証明書利用者の組織名が変更となった場合
- 電子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
- 証明書利用者が本 CPS3.4 に従い利用者証明書の失効を要求した場合

4.4.2 失効要求者

次の者は、利用者証明書の失効を要求することができます。

- 日本ベリサインは、本 CPS4.4.1 に従い、全ての利用者証明書の失効を要求することができます。
- 証明書利用者（当該組織内の正当な権限のある者）は、自己の利用者証明書につき失効を要求することができます。

4.4.3　失効手続き

電子証明書の失効を要求しようとする証明書利用者は、日本ベリサインに対してその旨知らせるものとし、日本ベリサインは速やかに電子証明書の失効に着手します。失効要求の連絡については、本 CPS3.4 に定めるところに従います。

4.4.4　失効要求の猶予期間

証明書の失効要求は、商業上合理的な期間内に、可能な限り速やかに送信されるものとします。

4.4.5　一時停止条件

本サービスでは、利用者証明書の一時停止を行いません。

4.4.6　一時停止要求者

規定しません。

4.4.7　一時停止手続き

規定しません。

4.4.8　一時停止期間の制限

規定しません。

4.4.9　CRL 発行頻度

利用者証明書の失効情報(CRL)は、システム保守による一時停止、緊急時など、やむを得ない場合を除き、24 時間ごとに CRL に反映され、更新された CRL はリポジトリで公開されます。

4.4.10 CRL の確認要件

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チェックすることを要します。依拠当事者が証明書ステータスをチェック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局が公表した最新の CRL を調査することです。本認証局では、本 CPS 2.6.1 に示すリポジトリにおいて CRL を公開します。

4.4.11 オンラインによる失効・ステータスチェック

本認証局は CRL 以外のオンラインによる証明書ステータス確認方法（OCSP を含む）を提供しません。

4.4.12 オンラインによる失効チェック要件
規定しません。

4.4.13 その他の利用可能な失効情報確認手段
規定しません。

4.4.14 その他の利用可能な失効情報確認手段における要件
規定しません。

4.4.15 危殆化時の特別対応
日本ベリサインは、本認証局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、その旨を証明書利用者および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行います。

4.5 セキュリティ監査の手順
4.5.1 記録される情報のタイプ
認証局設備において、次の重要なイベントについて記録します。
(1) 以下の事項を含む、証明書のライフサイクル管理イベント
・証明書申請、更新、失効
・要求の処理
・証明書および CRL の生成および発行
(2) 以下の事項を含む、セキュリティに関連するイベント
・認証局設備への来訪者の入退室
・認証局設備システムへのアクセスの試み
・セキュリティ上取扱い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

なお、各記録は以下の情報を含みます。
- 記録の種別
- 記録の日時
- 記録者の身元（特定できる場合）

登録局では、次の事項を含む証明書申請情報に関する記録をとります。
- 証明書申請者により提出された身元確認の書類の種類
  申請者の同一性確認のための書類がある場合、これに関するデータ、番号またはその組み合わせ（例えば、証明書申請者の運転免許証番号）

・　申請書および同一性確認のための書類の写しの保管場所
・　申請を受領した主体の身元
・　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

4.5.2　ログが処理、検査される頻度
重要なイベントが発生した場合、認証局設備内の監査ログの確認は随時実施します。

4.5.3　ログの保管期間
認証局設備において、監査ログは少なくとも２ヶ月間保管されます。
証明書のライフサイクルに関する監査ログは少なくとも 10 年間保管されます。

4.5.4　監査ログの保護
認証局設備における監査ログは漏洩、改竄、毀損などが行われないように安全に保管管理します。

4.5.5　監査ログのバックアップ手順
バックアップが必要な監査ログは、所定のバックアップ手順に従いバックアップされます。

4.5.6　監査ログの収集システム（内部・外部）
認証局設備における監査ログは、認証局設備内のシステムによる自動処理および認証局設備の要員による手作業を組み合わせて収集されます。

4.5.7　監査結果の通知
認証局設備における監査ログの監査において調査の必要性がある事象が検出された場合、当該事象の発生者に対し通知なく調査を行います。

4.5.8　脆弱性評価
規定しません。

4.6　記録アーカイブ
4.6.1　アーカイブデータの種類
日本ベリサインは、本 CPS4.5.1 で規定される記録を保管します。
また、CPS（過去のものも含む）、発行したすべての利用者証明書、認証局証明書、CRL（有効期間満了後の証明書、CRL も含む）を保管します。
これらの保管される記録等をまとめて「アーカイブデータ」と呼びます。

4.6.2　アーカイブデータの保管期間

保管される記録については、本 CPS4.5.3 参照。

CPS（過去のものも含む)、発行したすべての利用者証明書、認証局証明書、CRL（有効期間満了後の証明書、CRL も含む）については、本サービスが存続する限り保管されます。

4.6.3　アーカイブデータの保護

アーカイブデータは漏洩、改竄、毀損などが行われないように安全に保管管理します。

4.6.4　アーカイブデータのバックアップ手順

バックアップが必要なアーカイブデータは､所定のバックアップ手順に従いバックアップされます。

4.6.5　記録へのタイムスタンピング要件

認証局設備で管理される記録は、日時の情報を含みます。これらは暗号化されていません。

4.6.6　アーカイブデータ収集システム

アーカイブデータは日本ベリサイン内のシステムによる自動処理および日本ベリサインの要員による手作業を組み合わせて収集されます。

4.6.7　アーカイブデータの入手、検証手続き

本 CPS4.6.4 参照。

4.7　鍵更新

認証局証明書の更新はリニューアル方式を採用しているため､認証局の鍵更新については規定しません。

4.8　危殆化と災害復旧

4.8.1　ハードウェア、ソフトウェア又はデータの破壊

認証局設備におけるハードウェアは二重化されており､ハードウェアの破壊が発生した場合､待機系のハードウェアにより業務を継続します。

認証局設備におけるソフトウェア又はデータの破壊が発生した場合､認証設備運用者はバックアップされたソフトウェア又はデータにより復旧を行います。

4.8.2　利用者の公開鍵証明書の失効と再発行

本認証局は必要に応じて利用者証明書の失効を行い、再発行を行う場合があります。再発行は、初期発行と同じ手続きを行う必要があります。

4.8.3　利用者秘密鍵の危殆化

本 CPS4.4.1 参照。

4.8.4　災害等発生時の設備の確保

認証局設備は日本国内において十分に遠隔な地域に災害対策用の設備を設けています。災害発生時には鍵の危殆化の恐れがない場合、本災害対策用設備により運用を継続します。

4.9　認証業務の終了

認証業務の終了が必要な場合、本認証局は、証明書利用者および依拠当事者に対する混乱を最小化するために、終了プランを作成します。当該終了プランは、適宜次の事項に言及します。

・利用者、依拠当事者等、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

・失効情報確認手段の継続

・本 CPS（過去のものも含む）、発行したすべての利用者証明書、認証局証明書、CRL（有効期間満了後の証明書、CRL も含む）、審査記録・発行記録の保管

5.　物理面、手続面および人事面のセキュリティ統制

5.1　物理的統制

5.1.1　施設の位置と建物構造

認証局設備を収容する建築構造物（建物および部屋）は、耐震耐火設計、自動火災報知器と消火装置の設置、防火区画内設置、隔壁による区画、水害防止等の措置が予め十分講じられている等、地震、火災、水害等を想定した災害対策がなされた施設です。認証局設備を収容する設備室（以下、「認証局設備室」と呼ぶ）へは、建物に入館後、複数のセキュリティレベルで区画された場所を通った後に入室できるものとします。

認証局設備室の所在および仕様は、関係者以外には公表されません。建物の内外には認証局設備室の所在については表示されません。

災害対策設備に関しても認証局設備室と同等の管理を行います。

5.1.2　　物理的アクセス

認証局設備ついては、次により厳重に管理されるものとします。

1）認証局設備室は厳重に施錠管理され、その入室は入室者の身体的特徴の識別手段を用いた施錠設備による本人認証を行ってはじめて可能となるよう予め防護措置が講じられています。認証

局設備室に入室権限を有しない者は、付添なしで入室することはできません。
2)セキュリティおよび監査要件ガイドに従い、認証局設備室の一部には、複数人によってのみ入退室可能な領域を設置しています。
3）入室のための装置操作に不正常な時間を要した場合においては、警報が発せられるよう予め設定されるものとします。
4）認証局設備室への入退室者および在室者の状況については、遠隔監視装置、モーションセンサーおよび映像記録装置によって自動的かつ継続的に監視記録され、その記録については、正確に点検され、定められた期間、安全に保存されます。

5.1.3　電源設備と空調設備
認証局設備は停電に備えた UPS・自家発電機の設置、配置された設備に応じた空調機器の設置等、サービスの継続に必要な適切な措置が講じられています。

5.1.4　水害対策
認証局設備は水害防止等の措置が予め講じられています。

5.1.5　火災対策
認証局設備は、火災予防と火災被害への対応に関して合理的な対策を講じています。認証局設備の火災予防対策は、国内の火災予防規則に則って設計されています。

5.1.6　媒体管理
認証局設備におけるアーカイブ、および、バックアップデータは認証局設備内、または、安全なオフサイト設備に保管されています。これらの設備は不適切なアクセスがないように適切な物理的論理的アクセスコントロールが実施されており、また、事故的な災害から媒体を保護するように設計されています。

5.1.7　廃棄物処理
重要な文書などは廃棄時に回復不可能な方法により処理されます。重要な情報を含む媒体は廃棄前に再読み出しが不可能なようにフォーマットします。また、暗号モジュールデバイスは廃棄前に物理的に破壊されるか、デバイスの機能を用い初期化します。

5.1.8　オフサイトバックアップ
本 CPS4.8.4 参照。

5.2 手続統制

5.2.1　信頼される役割

認証局設備において信頼される人物となるためには、人事担当者との面接および広く認識されている身分証明書（パスポート、運転免許証等）の調査により、身元についての確認作業を行います。

信頼される人物には、以下の事項に重大な影響を及ぼすような、認証または暗号作業に関わる全ての従業員、独立請負業者およびコンサルタントが含まれます。

・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のアクセスを含む）
・利用者の情報または要求の取扱い

信頼される人物には、以下の者が含まれますが、これに限定されません。

・カスタマ・サービス要員
・キーマネージャ
・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
・認証事業の基盤の信頼性を管理するために指名された経営陣

5.2.2　役割毎の職務者数

認証局設備では、業務内容に基づく職務分掌を確実にするための方針と厳格な管理手続きを維持しています。認証局用暗号ハードウェアおよび関連する鍵関係資料等の最も機密を要する業務へのアクセスおよび管理は、複数の信頼される人物により行われます。

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 名の信頼される人物が確実に必要となるよう設計されています。認証局用暗号ハードウェアへのアクセスは、その受入れから最終の論理的・物理的破壊の検査までのライフサイクルを通じて、複数の信頼される人物により厳格に実施されています。モジュールがサービスに供されると、当該モジュールに関する一切の操作は、物理的および論理的にも複数人および複数の権限により管理されます。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ません。

5.2.3　識別と認証

本 CPS5.2.1 参照。

5.3　人事統制

日本ベリサインは、本サービスを運用する要員が、本 CPS で規定される業務の運用要件に照らして十分な要件を満たしていることを事前に確認しています。

6.　技術的セキュリティ統制

6.1 鍵ペア生成とインストール

6.1.1　鍵ペア生成

6.1.1.1 利用者鍵ペア生成

証明書利用者の鍵ペアは、証明書利用者により、暗号モジュール内で安全に生成しなければなりません。

6.1.1.2 認証局鍵ペア生成

認証局鍵ペアは、認証局設備室内で、権限を持つ複数名の要員がそろい、一人の操作だけではできない方法により暗号モジュール内で生成します。

6.1.2　秘密鍵の配布方法

証明書利用者の鍵ペアは、当該証明書利用者自身により通常生成されるため、秘密鍵の証明書利用者への配布は生じません。

6.1.3　公開鍵の提出方法

証明書利用者は、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・レイヤー（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、送付するものとします。

6.1.4　認証局の公開鍵の提供方法

認証局の公開鍵は、認証局証明書に含まれており、リポジトリにより公開されます。依拠当事者は入手した認証局証明書のフィンガープリント(証明書データのハッシュ値)が同リポジトリか、または、十分に信頼可能な方法で入手したフィンガープリント(認証局証明書情報のハッシュ値)と同値であることを確認する必要があります。

6.1.5　鍵長

本サービスで用いられる鍵ペアの鍵長は以下の通りです。

・認証局の秘密鍵：rsaEncryption(1 2 840 113549 1 1 1) 2048bit

・証明書利用者の秘密鍵：rsaEncryption(1 2 840 113549 1 1 1) 2048bit

6.1.6　公開鍵パラメータの生成
規定しません。

6.1.7　パラメータ精度の検査
規定しません。

6.1.8　鍵を生成するハードウェア／ソフトウェア
認証局における鍵を生成するハードウェア/ソフトウェアについては､本 CPS6.2.1 を参照してください。

6.1.9　鍵使用目的
証明書利用者の秘密鍵は、以下の目的以外に使用されることはありません。
1）タイムスタンプへの署名付与

認証局の秘密鍵は、以下の目的以外に使用されることはありません。
1）利用者証明書に対する署名
2）認証局証明書に対する自己署名、および、下位認証局が存在する場合には下位認証局証明書に対する署名
3）CRL、ARL に対する署名

6.2　秘密鍵の保護
6.2.1　暗号モジュールに関する標準
認証局の秘密鍵は認証局設備内において暗号モジュール内で保護されています。
暗号モジュールに FIPS 140-1 level 3 の基準を満たすハードウエアセキュリティモジュール（HSM）を利用しています。

6.2.2　秘密鍵の複数人制御
本認証局は､機密を要する認証局設備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ます。本認証局は、認証局の秘密鍵を利用するために「シークレット・シェアリング」という手法を用います。この手法では、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が保有します｡特定のハードウェア暗号モジュールに保管されている認証局の秘密鍵を起動させるためには、当該モジュールに関して生成・分配されたシークレット・シェア総数の内、一定数のシークレット・シェアが必要となります。

6.2.3　秘密鍵の預託

証明書利用者の秘密鍵の預託（エスクロー）は行いません。

6.2.4　秘密鍵のバックアップ

認証局の秘密鍵のバックアップは、鍵が格納されている暗号モジュールと同型の暗号モジュール間のクローニング（複製）機能によりバックアップを行います。バックアップは、複数人の管理の下、認証局設備室内において行われます。バックアップ用の暗号モジュールは認証局設備内の安全な場所に保管されます。

6.2.5　秘密鍵のアーカイブ

認証局の秘密鍵のアーカイブは行いません。

6.2.6　暗号モジュールへの秘密鍵の格納

6.2.6.1 利用者秘密鍵の暗号モジュールへの格納

証明書利用者の秘密鍵は安全な方法で暗号モジュール内に格納されなければなりません。

6.2.6.2 認証局秘密鍵の暗号モジュールへの格納

認証局の秘密鍵は暗号モジュール内で生成されるため、規定しません。

6.2.7　秘密鍵の活性化方法

認証局の秘密鍵の活性化方法については、本 CPS 6.2.2 参照。

証明書利用者の秘密鍵の保護に関しては、次の措置をとることとします。

- 暗号モジュールまたはそれと同様の強度のセキュリティを用いて、秘密鍵の起動に先立ち証明書利用者を認証すること、および
- 証明書利用者の承認なくして証明書利用者のワークステーションおよびそれに関連づけられた秘密鍵が使用されることを防止するために必要な物理的保護を施すため商業上合理的な手段をとること

暗号モジュールとともに、本 CPS6.4.1 に従いパスワードを用いることが推奨されます。非活性化する場合、秘密鍵は暗号化された形式でのみ保管されることを要します。

6.2.8　秘密鍵の非活性化方法

認証局の秘密鍵はシステムの停止、もしくは、暗号モジュールをトークンリーダから抜き取ることにより非活性化します。

証明書利用者の秘密鍵は、証明書利用者によって採用されている認証メカニズムに従い、非活性化されます。その場合、証明書利用者は、証明書利用者の秘密鍵を本 CPS2.1.3 に従い、適切に保護する義務を負います。

6.2.9　秘密鍵の破棄方法

認証局の秘密鍵の廃棄を行う場合は、専用の電子計算機を用いて、複数人の管理のもと鍵を完全に復元できない方法により行われます。また、バックアップされた暗号モジュール内にある当該認証局の秘密鍵も同じ方法により破棄されます。

6.3　鍵ペア管理に関するその他の項目

6.3.1　公開鍵のアーカイブ

認証局の公開鍵を含む公開鍵証明書、および、証明書利用者の公開鍵を含む利用者証明書は、本 CPS4.6 に従い保管されます。

6.3.2　鍵ペアの利用期間

認証局証明書の有効期間は 30 年までとします。また、利用者証明書の有効期間は最長 11 年までとします。

証明書利用者の秘密鍵の有効期間は、利用者証明書の有効期間開始日から 1 年とし、毎年更新するものとします。証明書利用者は、秘密鍵の有効期間の開始前あるいは満了後に秘密鍵を利用してはなりません。

日本ベリサインが証明書利用者に対し利用者証明書の更新を認めた場合、証明書利用者は、証明書利用者の秘密鍵の有効期間満了後 30 日以内に利用者証明書及び秘密鍵を更新することができるものとします。更新までの間、証明書利用者が引き続き秘密鍵を利用することを認めますが、秘密鍵の更新後に更新前の秘密鍵を利用してはなりません。

6.4　活性化データ

6.4.1　活性化データの生成とインストール

6.4.1.1 利用者秘密鍵の活性化データの生成とインストール

証明書利用者の秘密鍵の活性化情報は、利用者の責任において設定されます。利用者は活性化情報（パスワード）に生年月日、名称、電話番号などの容易に想像できる文字列を使用してはなりません。

6.4.1.2 認証局秘密鍵の活性化データの生成とインストール

認証局の秘密鍵は本 CPS6.2.2、および、6.2.7 に規定したシェア情報によって活性化されます。

シェア情報は本 CPS6.1.1.2 で規定された秘密鍵の生成時に権限者へ渡されます。

6.4.2　活性化データの保護

認証局の秘密鍵の活性化情報は複数人に分割されて管理されています。また、各活性化情報は権限者の責任で厳重に管理されます。

6.4.3　活性化データに関するその他の項目

規定しません。

6.5　コンピュータセキュリティ統制

6.5.1　コンピュータセキュリティ機能要件

認証局設備に用いられるシステムはアクセス制御機能、監査ログ記録機能を持つ信頼性の高いシステムにより構築されます。

6.5.2　コンピュータセキュリティ評価：Computer Security Rating

認証局設備のうち専ら証明書の作成に係る装置は ISO/IEC 15408-3:1999, Information technology－Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements」の EAL４レベル相当のシステムを利用しています。

6.6　システムのライフサイクルにおけるセキュリティ統制

6.6.1　システム開発統制

認証局設備において、アプリケーションは、システム開発および変更管理基準に従い、開発され実装されます。

6.6.2　セキュリティマネージメント統制

認証局設備では、システムの状況を管理し、監視するための仕組みおよび方策を有しています。認証局設備におけるすべてのソフトウェア・パッケージおよびソフトウェアのアップデートについて、ハッシュを生成します。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す。インストレーション時およびその後定期的に、システムの完全性を確認します。

6.6.3　セキュリティ評価の基準

規定しません。

6.7　ネットワークセキュリティ統制

認証局設備では、権限のない者によるアクセスおよび他の不正な活動を防止するため、セキュリ

ティおよび監査要件ガイドに従い、セキュリティの確保されたネットワークを用いて、その全ての業務を実施しています。秘密情報の通信は、暗号化およびデジタル署名を用いて行います。

6.8 暗号モジュールの技術統制

本認証局で使用する暗号モジュールは、本 CPS 6.2.1 に定める要件に合致しています。

7. 証明書と CRL のプロファイル

7.1 証明書のプロファイル

7.1.1 認証局証明書のプロファイル

本サービスにおいて発行される認証局証明書のプロファイルは、以下の通りです。

【基本部】

領域名	型	値	備考
version	INTEGER	2	v3 を表す。
serialNumber	INTEGER	……	ユニークな値を設定。
signature			
algorithm	OID	1 2 840 113549 1 1 5	sha1WithRSAEncryption を表す。
parameters	NULL	（なし）	
issuer			
commonName	OID	2 5 4 3	
	PrintableString	VeriSign Japan Time Stamping CA	
organizationName	OID	2 5 4 10	
	PrintableString	VeriSign Japan K.K.	
countryName	OID	2 5 4 6	
	PrintableString	JP	
validity			
notBefore	UTCTime	yymmddhhmmssZ	
notAfter	UTCTime	yymmddhhmmssZ	
subject			
commonName	OID	2 5 4 3	
	PrintableString	VeriSign Japan Time Stamping CA	
organizationName	OID	2 5 4 10	
	PrintableString	VeriSign Japan K.K.	
countryName	OID	2 5 4 6	
	PrintableString	JP	
subjectPublicKeyInfo			
algorithm	OID	1 2 840 113549 1 1 1	rsaEncryption を表す。
subjectPublicKey	BIT STRING	……	RSA 公開鍵の値。

【標準拡張領域】

領域名	criticality	型	値	備考
subjectAltName	FALSE	OID	2 5 29 17	
commonName		OID	2 5 4 3	
		PrintableString	……	本認証局により設定。
keyUsage	FALSE	OID	2 5 29 15	
		BIT STRING	keyCertSign(bit5) cRLSign(bit6)	
basicConstraints	FALSE	OID	2 5 29 19	
cA		BOOLEAN	TRUE	
pathLenConstraints		INTEGER	0	
certificatePolicies	FALSE	OID	2 5 29 32	
policyIdentifier		OID	1 2 392 200207 1 1	本認証局が発行する証明書ポリシーの OID。
policyQualifiers				
policyQualifierId		OID	1 3 6 1 5 5 7 2 1	本 CPS の公開場所を示していることを表す OID。
qualifier		IA5String	（下記※１）	

※１：https://www.verisign.co.jp/repository/tsa/

7.1.2　利用者証明書（TSA 証明書）のプロファイル

本サービスにおいて発行される利用者証明書（TSA 証明書）のプロファイルは、以下の通りです。

【基本部】

領域名	型	値	備考
version	INTEGER	2	v3 を表す。
serialNumber	INTEGER	……	ユニークな値を設定。
signature			
algorithm	OID	1 2 840 113549 1 1 5	sha1WithRSAEncryption を表す。
parameters	NULL	（なし）	
issuer			
commonName	OID	2 5 4 3	
	PrintableString	VeriSign Japan Time Stamping CA	
organizationName	OID	2 5 4 10	
	PrintableString	VeriSign Japan K.K.	
countryName	OID	2 5 4 6	
	PrintableString	JP	
validity			
notBefore	UTCTime	yymmddhhmmssZ	
notAfter	UTCTime	yymmddhhmmssZ	
subject			
commonName	OID	2 5 4 3	
	PrintableString	……	本 CPS3.1.2 参照。
organizationalUnitName	OID	2 5 4 11	
	PrintableString	……	本 CPS3.1.2 参照。
organizationName	OID	2 5 4 10	
	PrintableString	……	本 CPS3.1.2 参照。
localityName	OID	2 5 4 7	
	PrintableString	……	本 CPS3.1.2 参照。
stateOrProvinceName	OID	2 5 4 8	
	PrintableString	……	本 CPS3.1.2 参照。
countryName	OID	2 5 4 6	
	PrintableString	……	本 CPS3.1.2 参照。
subjectPublicKeyInfo			
algorithm	OID	1 2 840 113549 1 1 1	rsaEncryption を表す。
subjectPublicKey	BIT STRING	……	RSA 公開鍵の値。

【標準拡張領域】

領域名	criticality	型	値	備考
keyUsage	FALSE	OID	2 5 29 15	
		BIT STRING	digitalSignature (bit0)	
basicConstraints	FALSE	OID	2 5 29 19	
cA		BOOLEAN	FALSE	
extKeyUsage	TRUE	OID	2 5 29 37	
KeyPurposeId		OID	1 3 6 1 5 5 7 3 8	タイムスタンプでの利用を表す OID。
cRLDistributionPoints	FALSE	OID	2 5 29 31	
distributionPoint				
fullName		OID	2 23 42 2 0	
uniformResourceIdentifier			（下記※１）	
certificatePolicies	FALSE	OID	2 5 29 32	
policyIdentifier		OID	1 2 392 200207 1 1	本認証局が発行する証明書ポリシーの OID。
policyQualifiers				
policyQualifierId		OID	1 3 6 1 5 5 7 2 1	本 CPS の公開場所を示していることを表す OID。
qualifier		IA5String	（下記※２）	

※１：http://onsitecrl.verisign.co.jp/VeriSignJapanKKVeriSignJapanTimeStampingCA/LatestCRL.crl
※２：https://www.verisign.co.jp/repository/tsa/

7.2 Critical にセットされた拡張に対するポリシー

本サービスでは依拠当事者側システムの解釈を制限しないために、証明書拡張を Non-Critical に設定する場合があります。これは、RFC3280 で推奨されている設定とは異なる場合があります。依拠当事者は Non-Critical が指定されている拡張についても、可能な限り解釈しなければなりません。

7.3 CRL プロファイル

本サービスにおいて発行される CRL のプロファイルは、以下の通りです。

【基本部】

領域名		型	値	備考
version		INTEGER	1	v2 を表す。
signature				
	algorithm	OID	1 2 840 113549 1 1 5	sha1WithRSAEncryption を表す。
	parameters	NULL	（なし）	
issuer				
	organizationalUnitName	OID	2 5 4 3	
		PrintableString	VeriSign Japan Time Stamping CA	
	organizationName	OID	2 5 4 10	
		PrintableString	VeriSign Japan K.K.	
	country	OID	2 5 4 6	
		PrintableString	JP	
thisUpdate		UTCTime	yymmddhhmmssZ	
nextUpdate		UTCTime	yymmddhhmmssZ	
revokedCertificates				
	userCertificates	INTEGER	……	失効された証明書の serialNumber を表す。
	revocationDate	UTCTime	yymmddhhmmssZ	失効された日時を表す。

【CRL 拡張領域】

領域名	criticality	型	値	備考
cRLNumber	FALSE	OID	2 5 29 20	
		INTEGER	……	ユニークな値を設定。

【CRL エントリ拡張領域（失効された証明書ごとの拡張領域）】

領域名	criticality	型	値	備考
cRLReason	FALSE	OID	2 5 29 21	
		ENUMERATED	……	証明書の失効理由に応じて設定。 例） keyCompromise (1) affiliationChanged(3) superseded(4) cessationOfOperation(5) 等

8. CP/CPS の管理

8.1 CP/CPS の変更

日本ベリサインは、証明書利用者、または、依拠当事者に事前の承諾なしに随時、本 CPS を変更することができます。日本ベリサインは、CPS の修正版、または変更部分をリポジトリに掲載します。本 CPS の変更は猶予期間に関する指定がない限り、リポジトリへの公開時点で有効とみなします。

8.2 公表と通知に関する方針

日本ベリサインは本 CPS の改版履歴をリポジトリ
(https://www.verisign.co.jp/repository/tsa/index.html)において公開します。

8.3 CPS の承認手順

規定しません。

9. 用語

本 CPS 内で利用されている用語についての説明を以下に示します。

用語	説明
【A～Z】	
ARL	Authority Revocation List。認証局の証明書廃棄リスト。 証明書の有効期間中に、認証局秘密鍵の危殆化等の事由により失効された自己署名証明書及び下位認証局証明書のリスト。【「CRL」参照】。
CA	Certification Authority（認証局、または、認証機関)。 認証業務に必要な各機関のうち、証明書の発行の権限を付与された人、または、機関。
CP	Certificate Policy（証明書ポリシー)。 認証局が証明書を発行する際の運用方針を定めた文書。
CPS	Certificate Practice Statement（認証局運用規定)。 認証局の信頼性、安全性を対外的に示すために、認証局の運用、証明書ポリシー、鍵の生成・管理、責任等に関して定めた文書。 証明書ポリシーが何を運用方針にするのかを示すのに対して、認証局運用規程は運用方針をどのように実施するのかを示す。
CRL	Certificate Revocation List（証明書失効リスト)。 認証機関のデジタル署名が付され、定期的に（または緊急に）発行されるリストで、当該認証機関が発行した証明書の有効期間が到来する前に証明書の効力が停止され、または失効された証明書を特定したもの。このリストには、一般に ① 失効証明書リスト発行者の名称 ② 発行日 ③ 次の失効証明書リスト発行予定日 ④ 効力が停止されまたは失効された証明書の発行番号（Serial Number） ⑤ 証明書の効力の停止または失効された時間および理由 が記載される。
FIPS 140-1(Federal Information Processing Standard)	NIST(National Institute of Standards and Technology：米国標準技術研究所)が策定した米国連邦情報処理標準のうち、暗号技術に関するセキュリティ要件を規定しているもの。
IA	Issuing Authority（発行局)。 認証局階層のうち、エンドユーザへ証明書を発行する機能、および、部位の総称。中間 CA と呼ばれる場合もある。
IETF(Internet Engineering Task Force)	インターネットの技術的活動部会。インターネットにおけるプロトコルの技術開発、標準化を主な目的としている。作成された勧告はRFC（Request For Comments）と呼ばれる。 http://wwww.ietf.org参照。
HSM（Hardware Security Module：ハードウェアセキュリティモジュール)	ハードウェアによる秘密鍵の管理装置。 不正アクセスに備えるための機能（耐タンパ機能という）を保有した秘密鍵の管理装置。 耐タンパ機能とは不正アクセスに対してその侵入の痕跡を残したり、データを消去する機能であり、不正アクセスの証拠を残す不正顕示機能、不正アクセスからデータを防護する不正防

用語	説明
	護機能、不正アクセスに対してデータを消去する対抗動作を行う不正対抗機能等がある。 【暗号モジュール】と同義。
OCSP	Online Certificate Status Protocol：リアルタイムで証明書の状態を確認するためのプロトコル。OCSP サーバへのステータス要求と応答からなる。IETF 勧告（RFC2560）。
OID（Object Identification：オブジェクト識別子）	世界で一意となる値による識別子。登録機関（ISO、ITU）に登録される。PKIで使うアルゴリズム、証明書内に格納する名前（subject）のタイプ（commonName等の属性）等は、オブジェクト識別子として登録されているものが使用される。
PKI	Public Key Infrastructure の略。 公開鍵基盤。公開鍵暗号方式を基盤としたセキュリティ技術基盤、環境の総称。
PKIX(Public-Key Infrastructure（X.509))	IETF セキュリティ分野の１つの作業部会。証明書及び CRL/ARL のプロファイル、CP と CPS のフレームワーク等の制定を目的としている。
RA	Registration Authority（登録局)。 認証業務のうち、利用者へ証明書を発行するための登録申請処理を行う機関であり、利用者の識別と証明書申請（書）の審査・承認、証明書の失効処理（失効通知)、証明書の再発行を行う。
RFC	Request for Comment の略。 インターネット上の標準に関して勧告を行う IETF（Internet Engineering Task Force）の勧告。
RFC2527	RFC2527は、インターネットにおいて利用される認証局のCP又はCPSを作成するためのフレームワーク及びガイドラインを提供している。 http://www.ietf.org 参照。
RFC3280	X.509 を基盤として IETF によって策定された公開鍵証明書、失効リストに関する勧告。 http://www.ietf.org参照。
RSA	公開鍵暗号方式で利用する暗号アルゴリズムの１つ。十分に大きな２つの異なる素数を掛け合わせた整数の素因数分解が困難であることに安全性の根拠をおく。
RP	Relying Partyの略。 【依拠当事者】参照。
RPA	Relying Party Agreementの略。 依拠当事者者が当該認証局の発行した証明書に依存する前に、認証サービス提供者と依拠当事者の間で結ばれる合意文書。
SSL	Secure Socket Layer。Netscape 社が開発した Transport 層セッションセキュリティ。 SSL は IETF において改版され RFC2246（TLS：Transport Layer Security）勧告として採用された。
S/MIME	Secure MIME。インターネット電子メールの標準プロトコルである MIME のセキュリティ仕様。 IETF 勧告（RFC2632、RFC2633）
TLS	Transport Layer Security の略。 Transport 層において認証、暗号化などを実現する通信プロトコル。SSL をベースに IETF で勧告となったセキュリティプロ

用語	説明
	トコル。RFC2246。(【SSL】参照)。
TSA (Time Stamping Authority)	時刻認証業務を行う組織等。時刻認証事業者と呼ぶことがある。
TSA 証明書	TSA に対して発行され、TSA が付与するタイムスタンプの有効性を証明するための電子証明書。
X.500 識別名 (DN : DistinguishedName)	X.500とは、名前及びアドレスの調査から属性による検索まで広範囲なサービスを提供することを目的にITUが開発したディレクトリ標準。X.500識別名は、X.509の発行者識別名称及び利用者識別名称に使用される。
X.509	ITU (International Telecommunication Union：国際電気通信連合) によって策定された公開鍵証明書、失効リストに関する標準勧告。
【あ～ん】	
アーカイブ	安全保持、バックアップデータまたは監査目的のために、記録および関連するドキュメント等を一定期間保存すること、あるいは、保管されている記録等を表す。
アルゴリズム	計算や問題を解決するための手順、方式。
暗号	①データの秘密性と認証を確保するため、これを別のフォームに変換し、適切な暗号アルゴリズムと鍵を持つ者だけが再変換して元のデータを復元できるようにするために用いる数理科学。 ② 情報の内容を隠し、検知されない改変を不可能にし、無断使用を妨げる目的でデータを変換するための原理、手段および方法を体現する規則。
暗号モジュール	【HSM】参照。
依拠当事者	本認証局が発行した証明書を検証する人、または、機関。
改ざん (改竄)	データの内容を書き換えられること。
鍵長	暗号の強度を決定する要素の１つ。鍵の長さをビット数で表したものが鍵長（鍵のサイズ）であり、鍵長が大きいほど暗号の強度は増す。
鍵ペア (鍵対)	当該PKIシステムにおいて基礎となる秘密鍵、公開鍵のペア。
活性化	システム、装置等を使用可能な状態にすること。
活性化データ	システム、装置等を活性化するために必要となるデータ（パスワード等）。
監査	管理がきちんと行われており、かつ、その目的に照らして適切であることを確認するために使用される手続。情報システムへの侵入またはその誤用を検知するための、記録、解析作業を含む。
完全性	無権限でデータが改ざんされたり、破壊されていない状態。
危殆化 (Compromise)	秘密鍵や関連機密情報等が、盗難や漏えい、第三者による解読等によってその機密性を失ったか、あるいはその可能性があること。
機密性	機密を要するデータの秘密が保持され、権限を付与された人たちに対してだけ開示される状態。
検証	あるデジタル署名に関し、 ① このデジタル署名が、証明書の有効期間内に、証明書に含まれる公開鍵に対応する秘密鍵を用いて作成され ② デジタル署名作成後、関係するメッセージが改変されてい

用語	説明
	ないこと を間違いなく判定すること。 証明書の検証という場合、 ① 当該証明書に付与されたデジタル署名が、当該証明書の発行者の公開鍵に対応する秘密鍵を用いて作成され、 ② 検証時点が証明書に記載された有効期間の範囲内であることを間違いなく判定することをいう。
公開鍵暗号方式	メッセージを暗号化した鍵と異なる鍵を用いて復号する暗号方式。代表的なものにRSA暗号方式がある。
公開鍵基盤	【PKI】参照。
公開鍵証明書	認証対象者の識別情報と公開鍵とが対応していることを証明するデジタル文書。 ① 証明書発行者の識別名 ② 証明書利用者の識別名 ③ 証明書利用者の公開鍵情報 ④ 証明書の有効期間 ⑤ 証明書の発行番号（Serial Number） などの情報を含み、これに発行機関のデジタル署名が付されたデジタル文書。
公開鍵	公開鍵暗号方式における鍵ペアのうちの一つで、通信相手等の他人に知らせて利用してもらうための鍵。
失効（Revocation）	ある特定の日時以降、証明書の有効期間を終了させる手続。
シークレット・シェア	暗号化された機密で、いくつかの論理的、または、物理的トークンに分割された、分割後の1単位。
証明書	【公開鍵証明書】参照。
証明書利用者	電子証明書を認証局から取得し、電子証明書に記載された公開鍵と対になる秘密鍵を管理する者あるいは組織。 本サービスにおいて証明書利用者は、日本ベリサインの規定する手続きに従って電子証明書の発行を申し込み、本認証局によって電子証明書の発行を受けたTSAである。
署名	公開鍵暗号方式の秘密鍵を利用した、メッセージの完全性を保証する仕組み。メッセージの送信者が保有する秘密鍵でメッセージのハッシュ値を暗号化し、メッセージに付与すること。メッセージ受信者側は、署名者の公開鍵を用いて、送信者の本人確認及びメッセージの改ざん検知を行う。
時刻認証業務	電子データに係る情報について行われる措置であるタイムスタンプの付与および当該タイムスタンプの有効性を証明する業務。
自己署名証明書	自らの公開鍵に対して、自らの秘密鍵で署名した証明書。
タイムスタンプ	電子データがある時刻に存在していたことおよびその時刻以降に当該電子データが改ざんされていないことを証明できる機能を有する時刻証明情報。
タイムスタンプ局	【TSA】参照。
デジタル署名	【署名】参照。
電子証明書	【公開鍵証明書】参照。
電子データ	電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子

用語	説明
	計算機による情報処理の用に供されるものをいう。）に記録された情報。
トラストアンカ	信頼の根拠となる認証局。証明書の連鎖を検証する場合に信頼可能な認証局の証明書による署名が正当であることを確認することにより検証対象の証明書の信頼性を確認できる。
認証局	【CA】参照。
認証機関	【CA】参照。
発行局	【IA】参照
パスワード（パス・フレーズ、暗証番号）	認証のための秘密の情報。通常は、コンピュータ資源（メモリーなど）にアクセスすることを可能にする一連の文字列で成り立っている。
ハッシュ関数	異なる２つの入力値から同じ出力値を算出すること、および、出力値から入力値を逆算することが困難な関数。SHA-1，MD-5といった関数が主に用いられる。
非活性化	システム、装置等を使用不可能な状態にすること。
秘密鍵	公開鍵暗号方式における鍵ペアのうちの一つで、他人には知られないように秘密にしておく鍵。
秘密鍵の預託	秘密鍵を第三者に預けること。
プロファイル	証明書、および、CRL/ARLのデータ構造、記載内容を定義したもの。
ポリシー（Policy）	方針や規定、基準。
有効性確認	証明書の有効性確認時点にといて、 ① 当該証明書は失効されていないこと ② 当該証明書を発行した発行局が失効していないこと を間違いなく確認することである。
リポジトリ（Repository）	認証書や失効リスト等を保管し、認証書利用者等に対してこれらの開示や配布もしくは検索等のサービスを提供するシステム。
利用者	【証明書利用者】参照。
利用者証明書	証明書利用者に対して発行された電子証明書。 本サービスにおいて発行する利用者証明書は、TSA 証明書として利用される。
ルート認証局（root CA）	ツリー構造の最上位にある認証局のこと。