ベリサイン BMS 認証局
認証業務運用規程

Version 1.01

Effective Date: 2011/02/21

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/

ベリサイン BMS 認証局認証業務運用規程

Trademark Notices

VeriSign は、VeriSign Inc.の登録商標である。VeriSign のロゴは、VeriSign Inc.の商標並びにサービス・マークである。本 CPS 中のその他の商標およびサービス・マークは、それぞれの権利者に帰属する。

本 CPS に関するすべての著作権は、日本ベリサインが留保しており、さらに下記で許諾された場合を除き、日本ベリサインの書面による事前の同意なく、電子的、機械的、複写、録音その他手段を問わず、本 CPS のいかなる部分も複製、検索可能なシステム内での保管、送信を行うことはできないものとする。

上記の規定にかかわらず、本 CPS は以下に定める条件を満たす場合に、非独占的かつ無料で複製し配布することができる。(i)冒頭の著作権に関する表示およびこの前書きの部分を、複製されたそれぞれの文書に目立つように表示すること、(ii)本 CPS がすべて正確に複製され、本 CPS が日本ベリサイン株式会社に帰属する旨の記述を含むこと。

上記以外の複製(日本ベリサインからの複製の提供についても同様)についての連絡先は、1.5 節に記載されている。

謝辞
本 CPS 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

改訂履歴

Version	変更内容	日付	変更者 作成者
1.00	初版作成	2009/09/04	日本ベリサイン
1.01	リポジトリの URL 表記変更。サービスの拡張のため 3 章、4 章、6 章に証明書の鍵更新申請に伴う処理を追加	2011/02/21	日本ベリサイン

1. はじめに

本 CPS は、日本ベリサイン株式会社（以下「日本ベリサイン」という）が提供する「ベリサイン BMS 証明書発行サービス」（以下「本サービス」という）に関わる認証局の認証業務運用規程（Certification Practice Statement）（以下「本 CPS」という）である。
日本ベリサインは、本サービスにおいて、流通業界に関係する法人もしくは個人(個人事業主)に対して、電子的な証明書(以下「証明書」という)を提供する。本サービスにより証明書の発行を受けた者は、発行された証明書を、GDS や EDI 等において通信の安全性を確保する目的で利用することができる。

本 CPS は、流通システム標準普及推進協議会が定める「流通業界共通認証局証明書ポリシー」(以下「流通業界共通認証局 CP」という)に定められた要件に基づき証明書の発行、更新、失効、管理を含む一連のサービスに関する手続きその他のポリシーを規定するものである。

本サービスは、サービス開始にあたり、また、サービス内容の重要な変更を行うにあたり、流通業界共通認証局 CP に定められた認定機関に対して適切な情報の開示を行い、認定機関によって流通業界共通認証局 CP への適合性の確認を受けた後で、当該運用を開始する。

本 CPS は、Internet Engineering Task Force (IETF) が定める RFC 3647 (Internet Certificate Policy and Certification Practice Framework)に示された章・節・項の構成に従う。

1.1 概要

日本ベリサインは、本サービスにおいて、流通業界に関係する法人もしくは個人(個人事業主)に対して、電子的な証明書を提供する。本サービスにより証明書の発行を受けた者は、発行された証明書を、GDS や EDI 等において通信の安全性を確保する目的で使用することができる。なお、認証局の運営組織と、登録局の運営組織は、日本ベリサインが実施するものとする。

本 CPS は、米国ベリサインが定める VeriSign Trust Network Certificate Policies ならびに日本ベリサインが定める日本ベリサイン株式会社 認証業務運用規程とは相互に関連性はなくその影響は受けない。

1.2 文書名と識別

本 CPS は、日本ベリサインが提供する「ベリサイン BMS 証明書発行サービス」（本サービス）に関わる認証局についての認証業務運用規程（Certification Practice Statement）である。本 CPS の正式な名称は「ベリサイン BMS 認証局認証業務運用規程」である。
日本ベリサインは、本 CPS が定めた各種ポリシーに従って発行される証明書に対して、以下のオブジェクト識別子（OID）を割り当てる。

- オブジェクト識別子（OID）:1 2 392 00200207 3 1

1.3 PKIの参加者

1.3.1 認証局

日本ベリサインは、本サービスにおいて利用者に証明書を発行するために認証局を構築し、これを運営する。認証局は、認証局自身の公開鍵および秘密鍵を適切に管理し、登録局によって承認された利用者(法人または個人(個人事業主)、後述)に対して証明書を発行する機関である。
本サービスの認証局は、ルート認証局および中間認証局(利用者の証明書を発行する認証局)の2階層構成で、情報公開場所として 2 章で規定するリポジトリを提供する。
日本ベリサインは、認証局の運営にあたり、その業務の一部を外部に委託することができる。

1.3.2 登録局

登録局とは、利用者への窓口となり、利用者から各種の申請を受付け、利用者の識別と認証を行い、証明書の発行、失効、更新等の可否を判断する機関を示す。
本サービスにおいて、日本ベリサインは、本 CPS 1.3.1 項の認証局の業務に加え、登録局の業務を担当する。このため、以降本 CPS では、「認証局」の用語を、登録局の機能を含んだ主体を示すものとして利用する。
日本ベリサインは、登録局の運営にあたり、その業務の一部を外部に委託することができる。

1.3.3 利用者

利用者とは、本サービスにおいて、本認証局より証明を受け、発行された証明書を利用する者である。本サービスでは、流通業界に関わりを持つ以下の者の証明を行う。

(1) 法人
法人は、以下の目的のために本認証局が発行する証明書を利用することができる。
- 法人の従業者(役員、社員、契約社員等を含む)の証明書
- 法人が所有するサーバまたはシステムの証明書

(2) 個人事業主
個人事業主は、以下の目的のために本認証局が発行する証明書を利用することができる。
- 個人事業主の証明書
- 個人事業主が所有するサーバまたはシステムの証明書

ただし、本 CPS において、「個人事業主」とは、法人登記を行っていない個人事業者のみを指し、法人登記を行っている個人事業者については「法人」として取り扱う。

1.3.4 依拠当事者

依拠当事者とは、本認証局が発行した証明書に依拠し、以下の行為を行う者を示す。依拠当事者は、法人であっても個人であってもよい。

1. 利用者が作成した電子署名を、証明書に登録された公開鍵を利用して検証する
2. 利用者から提示された証明書を用いて、利用者の認証を行う
3. 利用者の証明書に登録された公開鍵を用いてデータの暗号化を行い、これを利用者に送信する

1.3.5　認定機関

認定機関は、流通業界共通認証局 CP に準拠した認証局を認定する機関である。本認証局は、流通業界共通認証局 CP に定められた認定機関の手続きに従い認定を取得した上で本認証サービスを提供する。

1.3.6　他の参加者

規定しない。

1.4　証明書の利用

1.4.1 適切な証明書の利用

利用者および依拠当事者は、本認証局が発行する証明書を、以下の用途で利用することができる。

(1) 法人の従業者(役員、社員、契約社員等を含む)の証明書
- GDS または EDI での利用を目的とした、メッセージの電子署名および暗号化
- GDS または EDI での利用を目的とした、SSL クライアント認証

(2) 法人が所有するサーバまたはシステムの証明書
- GDS または EDI での利用を目的とし、当該サーバまたはシステムにおける SSL サーバ認証および暗号化

(3) 個人事業主の証明書
- GDS または EDI での利用を目的とした、メッセージの電子署名および暗号化
- GDS または EDI での利用を目的とした、SSL クライアント認証

(4) 個人事業主が所有するサーバまたはシステムの証明書
- GDS または EDI での利用を目的とし、当該サーバまたはシステムにおける SSL サーバ認証および暗号化

1.4.2　禁止される証明書の用途

利用者および依拠当事者は、本認証局が発行した証明書を、本 CPS 1.4.1 項で規定された以外の用途で利用してはならない。また、日本ベリサインは、どのような場合であっても、発行された証明書を以下の目的のために使用することを禁止する。

- 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　ポリシー管理

1.5.1　本CPSの管理組織

本 CPS の管理は以下の組織にて行う。

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　本サービスの窓口

本サービスに関する問い合わせ窓口は以下にて開示する。

・ https://www.verisign.co.jp/bms/

1.5.3　CPに対するCPS適合性の決定者

本 CPS の、流通業界共通認証局 CP への適合性の判断は、認定機関が行う。

1.5.4　承認手続き

本 CPS は、日本ベリサインにおいて作成、更新および承認が行われる。当該手続きでは、改定後の本 CPS について、流通業界共通認証局 CP への準拠性を確保するために必要な手順を含む。
本 CPS の改訂手続きについては、本 CPS 9.12 節を参照すること。

1.6　定義と略語

Appendix A 参照。

2. 公開およ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、利用者および依拠当事者等に対して、本サービスおよび本認証局に関わる重要な情報を提供することを目的に、インターネット上にリポジトリを設け、これを公開する。日本ベリサインは、リポジトリを 1 日 24 時間、年間を通して運用する。ただし、設備あるいはシステムの保守作業が必要となった場合、その他の緊急時等において、日本ベリサインはリポジトリの提供を一時的に停止することができる。

2.2 証明情報の公開

日本ベリサインは、本サービスに関わる以下の情報をリポジトリにおいて公開する。

(1) 開示情報の種類
- 流通業界共通認証局 CP(リンクのみ)
- 本 CPS
- 利用者規約
- 依拠当事者規約
- 本認証局の認証局証明書
- 失効された証明書のリスト(CRL)
- その他の本認証局または本サービスに係わる重要な情報、あるいは日本ベリサインが必要と判断した情報

(2) リポジトリの場所
- https://www.verisign.co.jp/repository/bms/index.html

2.3 公開の頻度

本 CPS は、本 CPS 9.12 節の内容に従い、公開される。利用者規約および依拠当事者規約は、改定が行われるたびに、随時公開される。認証局証明書は、発行される都度、随時公開される。CRL は本 CPS 4.9.7 項に規定された頻度で更新され、更新後直ちに公開される。
その他の情報については、本認証局において必要性が認められるたびに、随時公開される。

2.4 リポジトリへのアクセス制限

日本ベリサインは、リポジトリにおいて公開する本 CPS 2.2 節の情報への参照について、アクセスの制限を行わない。ただし、不正な目的をもってアクセスが行われたと認められた場合、または、本サービスの円滑な運用上必要と認められた場合には、この限りではない。
日本ベリサインは、リポジトリで公開するすべての情報について、権限のない者による追加、変更および削除を防止するために必要な論理的および物理的なセキュリティの手段を講じる。

3. 識別と認証

3.1 名称

3.1.1 識別名の種類

本認証局は、ITU-T Recommendation X.509 のバージョン 3 に準拠した証明書を発行する。本認証局が発行する証明書に登録される発行者(issuer)および利用者(subject)の名称においては、ITU-T Recommendation X.501 で規定された識別名（DN:Distinguished Name）に準拠する。

3.1.2 意味のある名称であることの必要性

本認証局では、利用者が提出する申請書類（データを含む）の記載事項、添付書類の記載事項および本認証局が独自に割当てる情報等を用いて、証明書に登録される利用者(subject)の識別名を決定する。
本認証局から発行する証明書の種類は以下の4種類である。

(1) 法人の従業者(役員、社員、契約社員等を含む)の証明書
(2) 法人が所有するサーバまたはシステムの証明書
(3) 個人事業主の証明書
(4) 個人事業主が所有するサーバまたはシステムの証明書

以下に、それぞれの証明書に登録される識別名の詳細について規定する。

表 1 法人の従業者の証明書

属性	設定値および意味
countryName (C)	日本を示す以下の値で固定。 固定値:“JP”
organization Name (O)	法人の英語名称。商業登記の登記事項証明書に英語名称の記載がある場合は、当該名称を登録する。英語名称の記載がない場合は、本 CPS 3.1.4 項の内容に従うこととする。 例:“VeriSign Japan K.K.”
organizational UnitName (OU)	従業者が所属する部署の英語名称。申請書類において利用者が指定した値が登録される。 例:“Sales division”
organizational UnitName (OU)	発行許可番号。本認証局が決定した値が登録される。 例:“CertNo. – 0123456789abcdef0123456789abcdef”
commonName (CN)	従業者の氏名のヘボン式ローマ字表記。申請書類において利用者が指定した値が登録される。 例:“Taro Suzuki”
emailAddress (E)	従業者の電子メールアドレス。申請書類において利用者が指定した値が登録される。 例:“taro@verisign.co.jp”

表 2 法人が所有するサーバまたはシステムの証明書

属性	設定値および意味
countryName (C)	日本を示す以下の値で固定。 固定値:“JP”
organization Name (O)	法人の英語名称。商業登記の登記事項証明書に英語名称の記載がある場合は、当該名称を登録する。英語名称の記載がない場合は、本 CPS 3.1.4 項の内容に従うこととする。 例:“VeriSign Japan K.K.”
organizational UnitName (OU)	サーバまたはシステムを管理する部署の英語名称。申請書類において利用者が指定した値が登録される。 例:“Sales division”
organizational UnitName (OU)	発行許可番号。本認証局が決定した値が登録される。 例:“CertNo. – 0123456789abcdef0123456789abcdef”
commonName (CN)	サーバまたはシステムの FQDN 名またはシステムの名称。申請書類において利用者が指定した値が登録される。ただし、FQDN 名の場合は、本 CPS 3.2.2 項に従い内容の確認が行われる。 例:“www.verisign.co.jp”、“servername”
emailAddress (E)	連絡先の電子メールアドレス。申請書類において利用者が指定した値が登録される。 例:“taro@varisign.co.jp”

表 3 個人事業主の証明書

属性	設定値および意味
countryName (C)	日本を示す以下の値で固定。 固定値:“JP”
organizationName (O)	個人事業主を示す以下の値で固定。 固定値:“Natural Person”
organizational UnitName (OU)	発行許可番号。本認証局が決定した値が登録される。 例:“CertNo. – 0123456789abcdef0123456789abcdef”
commonName (CN)	個人事業主の氏名の英語表記。印鑑登録証明書等を用いて確認される個人事業主の氏名については、ヘボン式ローマ字表記が登録される。 例:“Taro Suzuki”
emailAddress (E)	個人事業主の電子メールアドレス。申請書類において利用者が指定した値が登録される。 例:“taro@verisign.co.jp”

表 4 個人事業主が所有するサーバまたはシステムの証明書

属性	設定値および意味
countryName (C)	日本を示す以下の値で固定。 固定値:“JP”
organizationName (O)	個人事業主を示す以下の値で固定。 固定値:“Natural Person”
organizational UnitName (OU)	個人事業主の氏名の英語表記。印鑑登録証明書等を用いて確認される個人事業主の氏名については、ヘボン式ローマ字表記が登録される。 例:“Taro Suzuki”
organizational UnitName (OU)	発行許可番号。本認証局が決定した値が登録される。 例:“CertNo. – 0123456789abcdef0123456789abcdef”
commonName (CN)	サーバまたはシステムの FQDN 名またはシステムの名称。申請書類において利用者が指定した値が登録される。ただし、FQDN 名の場合は、本 CPS 3.2.2 項に従い内容の確認が行われる。 例:“www.verisign.co.jp”、“servername”
emailAddress (E)	個人事業主の電子メールアドレス。申請書類において利用者が指定した値が設定される。 例:“taro@varisign.co.jp”

なお、日本ベリサインが運用する本サービスのルート認証局と中間認証局の識別名は以下の表の通りとする。

表 5 ルート認証局の識別名

属性	設定値
countryName (C)	JP
organizationName (O)	VeriSign Japan K.K.
OrganizationalUnitName (OU)	CA for manufacturers-distributors-retailers
commonName (CN)	VeriSign Japan BMS Root CA

表 6 中間認証局の識別名

属性	設定値
countryName (C)	JP
organizationName (O)	VeriSign Japan K.K.
organizationalUnitName (OU)	CA for manufacturers-distributors-retailers
commonName (CN)	VeriSign Japan BMS CA

3.1.3　利用者の匿名性、または仮名性

本認証局が発行する証明書に記載される利用者の識別名は、完全な匿名であることが許されない。証明書に記載された名称の意味については、本 CPS 3.1.2 項において規定される。

3.1.4　種々の名前形式を変換するための規則

証明書に登録される法人の英語名称には、以下のいずれかを採用する。

1. 民間の調査会社において、法人の英語名称として登録されている文字列
2. 利用者が提出した申請書類に法人の英語名称として記載された文字列であって、当該法人の日本語名称から合理的に変換可能であると日本ベリサインの審査担当者が判断したもの
3. 法人の日本語名称をヘボン式ローマ字に変換した文字列

3.1.5　名前の一意性

日本ベリサインは、利用者の名称（subject）について、同一の識別名を登録した証明書を異なる複数の者に発行しない。

3.1.6　認識、認証および商標の役割

利用者は、証明書に登録される名称について、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、利用者が本認証局へ提出した書類（データを含む）に記載された各種の名称について、利用者が知的財産権を有しているかどうかの確認を行わない。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はない。日本ベリサインは、上記の紛争を理由として、証明書の発行を拒絶するもしくは発行された証明書を失効する権利を有する。

3.2　初回の本人性確認

3.2.1　秘密鍵の所持を証明する方法

本認証局より証明書の発行を受けようとする者（法人または個人事業主、以下「申請者」という）は、証明書が発行される前に PKCS#10 形式（またはこれと同等の電子データ等）の情報を本認証局に提出しなければならない。日本ベリサインは、提出された情報を検証することで、申請者が公開鍵に対応した秘密鍵を所有することを確認する。なお、本認証局が利用者の秘密鍵を生成する場合は除く。

3.2.2 組織の認証

日本ベリサインは、法人の従業者の証明書、または法人が所有するサーバまたはシステムの証明書を発行するにあたり、当該証明書の申請者より以下の書類（電子データを含む）の提出を受け、この内容を審査する。

(1) 本認証局が定める所定の申請書
法人の名称（日本語および英語表記）、住所、従業者が所属する部署名（従業者の証明書の場合、日本語および英語表記）、従業者の氏名（従業者の証明書の場合、日本語および英語表記）、従業者の電子メールアドレス（従業者の証明書の場合）、サーバまたはシステムを管理する部署の部署名（サーバまたはシステムの証明書の場合、日本語および英語表記）、FQDN 名またはシステムの名称（サーバまたはシステムの証明書の場合）、連絡先の電子メールアドレス（サーバまたはシステムの証明書の場合）、その他の連絡先等の必要情報を含み、かつ、(3)を用いて照合可能な法人印による押印が施されているもの。
(2) 民間調査会社の企業コードまたは商業登記の登記事項証明書
民間調査会社が割り当てる企業コードまたは当該法人に関わる商業登記の登記事項証明書。発行から 3 ヶ月以内のものに限る。
(3) 法人印の印鑑証明書
当該法人に関わる印鑑の印鑑証明書。発行から 3 ヶ月以内のものに限る。
(4) オンラインでの申請情報
証明書に記載される利用者に関わる情報（法人の名称（英語表記）、部署名（英語表記）、従業者の氏名（従業者の証明書の場合、英語表記））、FQDN 名またはシステムの名称（サーバまたはシステムの証明書の場合）、電子メールアドレス、PKCS#10 形式の情報（またはこれと同等の電子データ等）。
(5) その他の書類または情報
本認証局が必要と判断した場合は、上記以外に情報の提供を求める場合がある。

日本ベリサインは、提出された書類（電子データを含む）の一貫性の確認を適切に審査することで申請者の本人性を確認し、証明書の発行の可否を判断する。サーバまたはシステムの証明書の場合には、申請された FQDN 名について、whois 検索またはその他の確実な方法により、当該法人が当該 FQDN の所有権もしくは使用権を有することを確認する。

3.2.3 個人の認証

日本ベリサインは、個人事業主の証明書、または個人事業主が所有するサーバまたはシステムの証明書を発行するにあたり、当該証明書の申請者より以下の書類（電子データを含む）の提出を受け、この内容を審査する。

(1) 本認証局が定める所定の申請書
個人事業主の氏名（日本語および英語表記）、住所、FQDN 名またはシステムの名称（サーバまたはシステムの証明書の場合）、電子メールアドレス、その他の連絡先等の必要情報を含み、かつ、(2)を用いて照合可能な印鑑による押印が施されているもの。
(2) 印鑑登録証明書
個人事業主の印鑑の印鑑登録証明書。発行から 3 ヶ月以内のものに限る。
(3) オンラインでの申請情報
証明書に記載される利用者に関わる情報（個人事業主の氏名（英語表記）、FQDN 名またはシステムの名称（サーバまたはシステムの証明書の場合）、電子メールアドレス、PKCS#10 形式の情報（またはこれと同等の電子データ等）。
(4) その他の書類または情報
本認証局が必要と判断した場合は、上記以外に情報の提供を求める場合がある。

日本ベリサインは、提出された書類（電子データを含む）の一貫性の確認を適切に審査することで申請者の本人性（実在性および同一性）を確認し、証明書の発行の可否を判断する。サーバまたはシステムの証明書の場合には、申請された FQDN 名について、whois 検索またはその他の確実な方法により、当該個人事業主が当該 FQDN の所有権もしくは使用権を有していることを確認する。

3.2.4 確認を行わない利用者の情報

日本ベリサインは、証明書に登録される以下の情報について、実在性、正確性、使用権等の確認を行わない。

(1) 従業者が所属する部署の名称
(2) 従業者の氏名
(3) FQDN 名におけるドメイン部分以外の文字列
(4) システムの名称
(5) 従業者、連絡先または個人事業主の電子メールアドレス

3.2.5 権限の正当性確認

規定しない。

3.2.6 相互運用の基準

規定しない。

3.3　鍵更新申請時の識別と認証

3.3.1　証明書更新時の識別と認証

本認証局では、有効期間の満了に伴う証明書の更新の手続きについて、証明書の初回発行と同様の利用者に対する認証を行うか、または利用者からの電子署名を確認することで更新に関する申請が利用者から行われていることの確認を行う。
この場合における認証の方法は、当該証明書の申請者より以下の書類または電子データの提出を受け、この内容を審査することとする。

(1) 本認証局が定める所定の申請書
　個人事業主の氏名（日本語および英語表記）、住所、FQDN 名またはシステムの名称（サーバまたはシステムの証明書の場合）、電子メールアドレス、その他の連絡先等の必要情報を含み、かつ、(2)を用いて照合可能な印鑑による押印が施されているもの。
(2) 印鑑登録証明書
　個人事業主の印鑑の印鑑登録証明書。発行から 3 ヶ月以内のものに限る。
(3) オンラインでの申請情報
　利用者が証明書の初回発行時に設定し、同じく初回発行時に登録した申請情報を呼び出すためのパスワード。
(4) その他の書類または情報
　本認証局が必要と判断した場合は、上記以外に情報の提供を求める場合がある。

日本ベリサインは、提出された書類（電子データを含む）の一貫性の確認を適切に審査することで申請者の本人性（実在性および同一性）を確認し、証明書の発行の可否を判断する。サーバまたはシステムの証明書の場合には、申請された FQDN 名について、whois 検索またはその他の確実な方法により、当該個人事業主が当該 FQDN の所有権もしくは使用権を有していることを確認する。

3.3.2　証明書再発行時の識別と認証

本認証局では、何らかの理由により証明書が失効された後に当該証明書の再度の発行が必要となった場合、新たな証明書の発行によりこれに対応する。この場合における認証の方法は、本 CPS 3.2 節の内容に従う。

3.4　失効の申請に関する識別と認証

日本ベリサインは、証明書の利用者より、当該証明書の失効の申請を受け付ける。失効の申請は、以下のいずれかの方法によるものが認められる。

(1) 所定の書類の提出による方法
　利用者は、本認証局が指定する所定の申請書に必要事項を記入の上、印鑑証明書（法人の場合）または印鑑登録証明書（個人事業主の場合）で照合可能な印鑑による押印を施し、本認証局に提出する。
　ただし、本認証局が当該利用者について発行から 3 ヶ月以内の有効な印鑑証明書もしくは印鑑登録証明書を保持しない場合、利用者は、当該書類を追加で本認証局に提出しなければならない。
(2) オンラインでの情報登録による方法
　利用者は、証明書の申請時において、任意のパスワードを本認証局に登録することが求められる。利用者は、当該パスワードをオンラインにて本認証局に提示することにより、失効の申請をオンラインで行うことができる。

日本ベリサインは、提出された書類(データを含む)の一貫性の確認を適切に審査することで、失効の申請が失効対象となる証明書の正しい利用者により行われていることを確認し、失効の可否を判断する。

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 証明書を申請できる者

本認証局に証明書の申請を行うことができる者は、流通業界と関係を有する法人または個人事業主である。

(1) 法人
法人は、以下の証明書について、本認証局に発行を申請することができる。
- 法人の従業者(役員、社員、契約社員等を含む)を示す証明書
- 法人が所有するサーバまたはシステムを示す証明書

(2) 個人事業主
個人事業主は、以下の証明書について、本認証局に発行を申請することができる。
- 個人事業主を示す証明書
- 個人事業主が所有するサーバまたはシステムを示す証明書

ただし、法人は、本認証局への申請にあたり、適切な者を選任し必要な権限を与え、当該法人の代表として本認証局への申請、連絡その他の処理を担当させるものとする。

4.1.2 登録手続きおよび責任

申請者は、本認証局が別途定める手続きに従い、本認証局へ証明書の申請を行わなければならない。これらの手続きには、以下の内容が含まれる。

- 申請者は、本 CPS 3.2 節に定められた必要な書類(電子データを含む)を、本認証局が指定する方法で、本認証局に提出する
- 申請者は、本認証局に対して虚偽なく正確な内容の申請を行う
- 申請者は、本認証局が定める規定の料金について、本認証局が指定する方法で支払いを行う
- 申請者は、本 CPS 9.6.2 項の内容および利用者規約の内容を理解し承諾する

4.2 証明書申請の処理

4.2.1 識別と認証の実施

日本ベリサインは、本 CPS 3.2 節の規定に従い、申請者の識別および認証等審査を行う。日本ベリサインは、審査における具体的な基準および方法を定め、手順書等として文書化し、これに従って審査を実施する。当該手順においては、申請の内容に何らかの疑義が生じた場合、申請者に追加の情報の提示を求める等の処理を含めることができる。

4.2.2　証明書申請の承認もしくは否認

日本ベリサインは、本 CPS 3.2 節の規定に従って申請の内容を審査し、これに基づいて証明書の発行の承認もしくは否認を行う。日本ベリサインは、提出された書類（電子データを含む）に不備が発見された場合または審査の過程において疑義が生じた場合等において、追加情報の提出等によって当該問題が解決されるまで、証明書の発行を承認しない。あるいは、日本ベリサインは、当該申請を否認する。
発行の申請が承認されるためには、少なくとも以下の条件が満たされなければならない。

- 本 CPS 3.2.2 項（法人の場合）または 3.2.3 項（個人事業主の場合）の規定に従い、必要な書類（電子データを含む）が正しく提出され、本人性の確認を含む本認証局の審査に合格すること
- 証明書の発行に関わる料金について、本認証局が指定する方法で支払いが行われていること（もしくは将来支払いが行われることについて本認証局が合意できること）
- 当該申請に関わる証明書の発行を行うことが、本認証局の信頼を脅かす結果になると判断されないこと

4.2.3　証明書申請の処理時間

日本ベリサインは、申請者から申請に必要なすべての書類の申請を受け付けた後、10 営業日以内に、当該申請についての処理を完了させる。ただし、この期間は、提出された書類（電子データを含む）の不備等の理由により申請者に追加情報の提出を求める必要が生じた場合等、日本ベリサインの責に帰さない理由により延長される場合がある。

4.3　証明書発行

4.3.1　証明書の発行過程における認証局の行為

日本ベリサインは、本 CPS 4.2 節に従い発行が承認された申請者に対して、証明書の発行を行う。
日本ベリサインは、申請者が提出した申請書類（電子データを含む）に含まれた情報等を用い、日本ベリサインの管理する設備において、証明書を作成する。

4.3.2　認証局による利用者に対する証明書の発行通知

日本ベリサインは、証明書の作成を完了した後、遅滞なく申請者にこの旨を通知する。通常、証明書は、インターネットを用いてオンラインでダウンロードする形で申請者に提供される。日本ベリサインは、証明書のダウンロードに必要な情報を申請者に通知し、申請者が証明書を自身でダウンロードできるようにする。

4.4　証明書の受領

4.4.1　証明書の受領となる行為

申請者は、証明書をダウンロードまたは電子メールの受信をもって受領した後、遅滞なく当該証明書の登録内容に誤りがないことを確認しなければならない。申請者が証明書に何らかの誤りを発見した場合、申請書は当該証明書の利用を開始せず、当該誤りについて本 CPS 1.5.2 項に記載する本サービスの窓口に通知しなければならない。

4.4.2　認証局による証明書の公開

日本ベリサインは、利用者の証明書について、リポジトリでの公開を行わない。

4.4.3　認証局による他のエンティティに対する証明書の発行通知

規定しない。

4.5　鍵ペアと証明書の用途

4.5.1　利用者の秘密鍵および証明書の使用

利用者は、証明書の利用を行う前に、利用者規約に同意しなければならない。利用者は、証明書の受領を完了した場合にのみ、当該証明書とこれに対応する秘密鍵を利用することを許される。利用者は、本 CPS 1.4 節の規定および利用者規約の定める条件等に従い、認められた範囲内でのみ当該証明書とこれに対応する秘密鍵を利用することができる。証明書は、登録された keyUsage の値に違反しない範囲内でのみ利用されなければならない。
利用者は、自らの秘密鍵を不正に利用されないように保護し管理しなければならない。また、有効期間の満了または証明書の失効に伴い、当該証明書とこれに対応する秘密鍵の利用を終了しなければならない。

4.5.2　依拠当事者の公開鍵および証明書の使用

依拠当事者は、証明書に依拠する前に、依拠当事者規約に同意しなければならない。依拠当事者は、本 CPS 1.4 節の規定および依拠当事者規約の定める条件等に従い、認められた範囲内でのみ証明書に依拠することができる。
依拠当事者は、証明書に依拠する前に、以下のことを行わなければならない。

- 自身の目的のために証明書を利用することが適切かどうかを評価し、また、証明書の利用の目的が本 CPS 1.4 節において認められた範囲内であることを確認する
- 証明書は、証明書に登録された keyUsage の拡張領域の値に違反しない範囲内でのみ利用されていることを確認する
- 本認証局が発行する正しい認証局の証明書をリポジトリ等から入手し、利用者の証明書に施された電子署名が本認証局の秘密鍵で正しくおこなわれていること、および利用者の証明書が改ざんされていないことを確認する。また、これらのすべての証明書が有効期間内であること、および失効リストにおいて失効されていないことを確認する

依拠当事者は、適切なソフトウェアおよびハードウェアを用いて証明書およびこれに登録された利用者の公開鍵を利用しなければならない。

4.6　証明書の更新

本節では、公開鍵またはその他の証明書登録情報の更新を伴わない証明書の更新について規定する。本認証局では、利用者の公開鍵の更新を伴わない証明書の更新を認めない。利用者は、何らかの理由によって新しい証明書が必要となった場合、本CPS 4.7節の規定に従い証明書の申請を行わなければならない。

4.7　証明書の鍵更新

4.7.1　証明書の鍵更新が行われる場合

本節では、公開鍵の更新を伴う証明書の更新について規定する。利用者は、何らかの理由によって新しい証明書が必要となった場合、本CPS 3.3節の規定に従い本認証局に新しい証明書の発行の申請を行わなければならない。
証明書の鍵更新が行われる場合には以下のものが含まれるが、これに限らない。

- 利用中の証明書の有効期間が満了した場合、もしくは満了する場合
- 利用中の証明書が何らかの理由により失効された場合

4.7.2　新しい公開鍵の証明書の申請を行うことができる者

本 CPS 4.1 節の規定に従う。

4.7.3　証明書の鍵更新申請の処理

証明書の鍵更新の手続きは、証明書の初回発行と同様の利用者に対する認証を行うか、または利用者からの電子署名を確認することで更新に関する申請が利用者から行われていることの確認を行う。

4.7.4　利用者に対する新しい証明書の通知

本 CPS 4.3.2 項の規定に従う。

4.7.5　鍵更新された証明書の受領となる行為

本 CPS 4.4.1 項 の規定に従う。

4.7.6　認証局による鍵更新済みの証明書の公開

本 CPS 4.4.2 項の規定に従う。

4.7.7　他のエンティティに対する認証局の証明書発行通知

本 CPS 4.4.3 項の規定に従う。

4.8　証明書の変更

本節では、公開鍵を除く他の証明書登録情報の変更に伴う証明書の更新について規定する。本認証局では、利用者の公開鍵の更新を伴わない証明書の更新を認めない。利用者は、何らかの理由によって新しい証明書が必要となった場合、本CPS 4.7節の規定に従い証明書の申請を行わなければならない。

4.9　証明書の失効と一時停止

4.9.1　失効が行われる場合

利用者の証明書は以下の場合に失効される。

- 利用者の秘密鍵が危殆化した、または危殆化した恐れのある場合
- 利用者が証明書の利用を終了する場合
- 証明書に登録された情報に変更が生じた場合
- 証明書の失効について利用者が本認証局に申請を行いこれが認められた場合
- 本認証局にて証明書の失効が必要と判断した場合

本認証局が失効を必要と判断する場合には、利用者規約に定められた重要な事項に利用者が違反したと本認証局が判断する合理的な理由がある場合等が含まれる。

4.9.2　証明書の失効を申請できる者

証明書の失効を申請できる者は以下の通りとする。

・　利用者
利用者が法人の場合（法人の従業者を示す証明書または法人が所有するサーバまたはシステムを示す証明書の場合）、法人は、自身の業務に従事する適切な従業者を選任し、当該法人の代表として本認証局へ申請を行わせることができる。
利用者が個人事業主の場合（個人事業主を示す証明書または個人事業主が所有するサーバまたはシステムを示す証明書の場合）、個人事業主は、自身に発行された証明書の失効を申請することができる。
・　本認証局
本認証局は、利用者の証明書について失効が必要と判断した場合、当該証明書の失効を申請し、必要な手続きを開始することができる。

4.9.3　失効申請の手続き

利用者による失効申請の手続きは、本 CPS 3.4 節の規定に従い実施される。利用者は、本 CPS 3.4 節の規定に従って本認証局が別途指定する方法で、本認証局に失効の申請を行わなければならない。当該手順においては、申請の内容に何らかの疑義が生じた場合、利用者に追加の情報の提示を求める等の処理を含めることができる。本認証局は利用者証明書について失効すべき事由を知った場合、複数の認証担当者により事由の確認を行い利用者証明書の失効を行う。

4.9.4　失効申請の猶予期間

利用者は、本 CPS 4.9.1 項で規定された失効の事由(本認証局にて証明書の失効が必要と判断した場合を除く)に相当する事象の発生を認識した場合、速やかに失効の申請を行わなければならない。

4.9.5　認証局が失効申請を処理しなければならない期間

本 CPS 3.4 節(2)の方法で失効の申請が行われた場合、通常、当該申請は逐次処理される。本 CPS 3.4 節(1)の方法で失効の申請が行われた場合、日本ベリサインは、失効の申請を遅滞なく処理するように、商業上合理的な方策を講じる。

4.9.6　依拠当事者に対する失効確認の要求

依拠当事者は、利用者の証明書に依拠する前に、本 CPS 2.2 節の規定に従いリポジトリで公開された最新の CRL を参照し、当該証明書が失効されていないことを確認しなければならない。各々の証明書に関係する最新の CRL の開示場所は、本 CPS 7.1 節の規定に従い、各証明書の拡張領域に登録される。

4.9.7　証明書失効リスト の発行頻度

利用者の証明書についての CRL は、少なくとも 1 日 1 回以上の頻度で発行される。
ただし、失効された証明書について、発行時に定められた有効期間が満了した場合、その後に発行される CRL からは当該証明書の情報が削除される。

4.9.8　証明書失効リストの発行最大遅延時間

特段の事情がない限り、CRL は作成後速やかにリポジトリで開示される。通常は、作成から数分以内である。

4.9.9　オンラインでの失効/ステータス確認の適用性

規定しない。

4.9.10 オンラインでの失効/ステータス確認を行うための要件

規定しない。

4.9.11 利用可能な失効通知の他の形式

規定しない。

4.9.12 鍵の危殆化に関する特別な要件

利用者は、自身の秘密鍵が危殆化したまたは危殆化した恐れがあることを認識した場合、可能な限り速やかに当該証明書について失効の申請を行わなければならない。
日本ベリサインは、本認証局の秘密鍵が危殆化したまたは危殆化した恐れがあることを認識した場合、リポジトリまたはその他の手段を通じて、利用者、依拠当事者、およびその他の関係者に通知を行う。

4.9.13 証明書の一時停止の場合

規定しない。

4.9.14 証明書の一時停止を申請できる者

規定しない。

4.9.15 証明書の一時停止の手続き

規定しない。

4.9.16 証明書の一時停止期間の制限

規定しない。

4.10 証明書のステータス・サービス

規定しない。

4.11 利用の終了

利用者は、証明書の有効期間が満了する前に証明書の利用を終了する場合、当該証明書について本認証局に失効の申請を行い、当該証明書を失効させなければならない。利用者に発行されたすべての証明書について、有効期間が満了したかもしくは失効が行われた場合、利用者は本サービスの利用を終了したものとみなされる。

4.12 鍵の預託と復旧

規定しない。

5. 設備、管理および運用統制

5.1 物理的管理

5.1.1 立地場所および構造

本認証局の設備を収容する建築物（建物および部屋）は、耐震耐火設計、防火区画の設定、自動火災報知器と消火装置の設置、水害防止等の措置が予め十分講じられており、地震、火災、水害等を想定した災害対策がなされた施設である。本認証局の秘密鍵を取り扱う設備を収容する室（以下「認証設備室」という）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する。
認証設備室の所在および仕様は、関係者以外には公表されない。建物の内外には認証設備室の所在については表示されない。

5.1.2 物理的アクセス

本認証局の業務に関連する各室への入退室は、以下のように管理する。また、入室権限を有しない者が入室する場合は、入室権限保持者同行の上、入退室記録を作成した上でのみ入室できる。

(1) 本認証局の秘密鍵を保管または取り扱う室は、権限を有する2名以上の者をもって入室する。
(2) 本認証局が利用する電子署名用サーバ機器への物理アクセスは、権限を有する2名以上の者をもって可能とする。
(3) 認証局の業務に利用する重要な設備が設置された室は、生体認証を利用した入退室管理を実施する。
(4) 登録局が設置されている部屋は生体認証を利用した入室管理を実施する。また、登録局の業務を実施する部屋は権限を有する者が入室することができる。

5.1.3 電源、および空調

本認証局の業務に利用される重要な設備（認証設備室内設置の設備を含む、以下同様）は、UPS、自家発電機等の停電対策が実施される。また、日本ベリサインは、各設備の仕様に応じた空調機器の設置等、本サービスの継続的な運用に必要な合理的な措置を講じる。

5.1.4 水害対策

本認証局の設備は、水害への対策として合理的な措置が講じられる。配管および空調設備に対する漏水対策や、重要な設備室内での水使用設備の非設置などはこれに含まれる。

5.1.5 火災防止、および火災保護対策

本認証局の設備は、火災の予防およ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措置が講じられる。設備を収容する建物は耐火設計が施されたものであり、各設備は防火区画内に設置される。各室には、自動火災報知器と消火装置が設置される。日本ベリサインの火災予防および保護対策は、国内の火災安全規則に則って設計されるものである。

5.1.6　媒体保管場所

本認証局の業務に関連して作成され保管対象とされたメディアは、適切なアクセス管理（入退出管理を含む）が行われた日本ベリサインの施設内において保管されるか、または、物理的および論理的なアクセス管理が施された前記施設外において保管される。これらの保管場所は、火災や水害および電磁気等による障害に対して、メディアの不測の損傷を防止するのに必要な措置を含む。
メディアは、適切な搬入出管理（記録の作成を含む）が施される。

5.1.7　廃棄物処理

本認証局において書類またはメディア等記録媒体の廃棄が行われる場合、日本ベリサインが別途定める社内標準に従い、適切に廃棄が行われる。

5.1.8　施設外のバックアップ

規定しない。

5.2　手続き的管理

5.2.1　信頼すべき役割

日本ベリサインは、本認証局の運営にあたり、以下の事項に影響する全ての者について、信頼すべき役割を担う者として取り扱う。

- 証明書の発行申請の内容についての検証
- 証明書の発行申請、失効申請、更新申請等の承認または否認その他の判断
- 証明書の発行または失効の実施、リポジトリの制限された部分へのアクセスおよび利用者の情報または要求の取り扱い

信頼すべき役割を担う者になるためには、日本ベリサインが別途定める要求事項を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、個々の職務の内容および必要人数を明確に定め、役割に応じた権限を担当者に適切に割り当てる。本認証局の秘密鍵の取り扱いを行うに際しては、必ず複数の者がこれに関与するようにシステム上および運用上必要な統制を行う。また、利用者からの申請に対する審査については、少なくとも 2 人以上の者が担当し相互に牽制を行い、故意および不注意による間違いを防止する。

5.2.3　個々の役割に対する本人性確認と認証

本認証局において、信頼すべき役割を担う者として新しく職務に従事する者は、事前に、日本ベリサインが別途定める本人確認および認証等の要件を満たさなければならない。当該要件には、身分証明書の提示等による本人確認要件等が含まれる。

日本ベリサインは、各職務に従事する者が当該業務を実施するに際して、物理的または論理的なコントロールにより当該担当者の識別を行い、職務の実施の権限を確認する。これらのコントロールには、特定の室への入退室管理（生体認証によるものを含む）、特定システムへのアクセス管理（パスワードやその他の手段の利用）、物理的な鍵や電子鍵またはカードの貸与による管理等が含まれるがこれに限らない。

5.2.4　職務の分離を必要とする役割

日本ベリサインは、本認証局の業務が適正に実施され、その安全性を確保し信頼性を確立するために必要な手段として、各職務について兼務の禁止の範囲を明確に定め、これに従って担当者のアサイン等を行う。兼務の禁止の範囲についての規定は、別途定められる。

5.3　人事的管理

5.3.1　資格、経験および身分の要件

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、資格および経験を有することを要求する。

5.3.2　経歴の調査手続き

日本ベリサインは、信頼すべき役割を担う者が就任する前に、その者の提出された経歴の調査等を行う。

5.3.3　研修要件

本認証局では、認証業務に従事する者について、業務を行う上で必要な知識を習得させる研修を、業務が開始される前に実施する。

5.3.4　再研修の頻度および要件

規定しない。

5.3.5　職務のローテーションの頻度および要件

規定しない。

5.3.6　認められていない行動に対する制裁

規定しない。

5.3.7　独立した契約者の要件

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、信頼される地位に就くことがある。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およびセキュリティ上の基準が適用される。

5.3.2 項 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本認証局に関わる業務を実施できる。ただし、信頼される者のみが実施できる業務を実施することはできない。

5.3.8　要員に提供される資料

規定しない。

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、次のイベントについて記録し保管する。

- 認証局秘密鍵の操作
- 認証局秘密鍵が保管される部屋の入退出
- 認証局設備が設置される部屋の入退出
- 登録局が設置される部屋の入退出
- 証明書の発行
- 証明書の失効
- CRL の発行

5.4.2　監査ログを処理する頻度

重要なセキュリティおよび運用イベントが発生した場合、当該監査記録は、1週間以内に検査される。更に、日本ベリサインは、本認証局のシステム内において、異常およ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。

5.4.3　監査ログを保持する期間

監査ログは、少なくとも取得後 1 ヶ月間は容易に読み取りができる場所で保管される。その後は移設されることがある。また、アーカイブ対象ではない監査記録は抹消される場合がある。

5.4.4　監査ログの保護

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監査ログを保護するため権限者により物理的または電子的に保護する。

5.4.5　監査ログのバックアップ手続き

認証局秘密鍵の操作、証明書の発行・証明書の失効・CRL の発行についての監査記録のバックアップは毎日生成され、入退室管理についての監査ログは月に一度の頻度でされる。また、認証局秘密鍵の操作についての監査記録のバックアップは、認証局が構築されるときにされる。

5.4.6　監査ログの集計システム

規定しない。

5.4.7　イベントを起こしたサブジェクトへの通知

規定しない。

5.4.8　脆弱性の評価

規定しない。

5.5　記録のアーカイブ

5.5.1　アーカイブされる記録の種類

日本ベリサインは次の記録を保管する。
(1) 証明書の初回発行に関する記録
・ 利用者が提出した書類
・ 本認証局内での審査記録（審査結果、審査日時、審査担当者、承認者に関する情報等）
(2) 証明書の更新に関する記録
・ 利用者が提出した書類
・ 本認証局内での審査記録（審査結果、審査日時、審査担当者、承認者に関する情報等）
(3) 証明書の失効に関する記録
・ 利用者が提出した書類
・ 本認証局内での審査記録（審査結果、審査日時、審査担当者、承認者に関する情報等）
(4) 認証局秘密鍵の操作に関する記録
(5) 本認証局の組織の維持管理に関する記録
・ 認証局の体制図及びこれに準ずる書類
・ 認証局に関連する規程類（各 CPS、利用者規約、依拠当事者規約等）

5.5.2　アーカイブ保持期間

記録は、少なくとも次の期間保管される。
(1) 証明書の初回発行に関する記録・・・当該証明書の有効期間が満了してから 3 年間
(2) 証明書の更新に関する記録・・・当該証明書の有効期間が満了してから 3 年間
(3) 証明書の失効に関する記録・・・当該証明書の有効期間が満了してから 3 年間
(4) 認証局秘密鍵の操作に関する記録・・・当該認証局秘密鍵が利用されている限り
(5) 本認証局の組織の維持管理に関する記録・・・改訂後より 10 年間

5.5.3　アーカイブの保護

本認証局は、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、無権限者による閲覧、変更、削除、その他操作ができないよう、権限者によって保管された記録の保護を行う。

5.5.4　アーカイブのバックアップ手続き

本認証局は、電子的な記録について、毎日バックアップを実施する。

5.5.5　記録にタイム・スタンプを付ける要件

本認証局は、電子的な記録について、タイムスタンプを正確につける。

5.5.6　アーカイブ収集システム

規定しない。

5.5.7　アーカイブ情報を入手し検証する手続き

規定しない。

5.6　鍵の切り替え

本認証局の鍵は、本 CPS に定められたルート認証局と中間認証局の有効期間の満了時にその役割を終了する。新規の認証局の鍵ペアは、例えば、実際に使用されている鍵ペアを補完する場合およ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。

5.7　危殆化および災害からの復旧

5.7.1　事故および危殆化の取り扱い手続き

本認証局では以下のインシデントに対し、迅速な復旧作業を実施するために、関係する要員に必要な教育および訓練を実施する。

- 認証局秘密鍵の危殆化
- 認証局で使用しているシステムの障害

5.7.2　コンピュータの資源、ソフトウェアまたはデータが破損した場合

本認証局は、自身のハードウェア、ソフトウェアまたはデータの破壊が生じた場合は、可能な限り速やかにバックアップ機、バックアップデータ等を用いて復旧作業を行い、速やかに業務再開に努める。

5.7.3　エンティティの秘密鍵が危殆化した場合の手続き

本認証局の秘密鍵についての危殆化が確認された場合、認証局証明書の失効を行い、次の手続きが実施される。。

- 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、4.9.7 項 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利用者に対して、失効の通知を実施する。
- 認証局が 5.8 節に従い終了していない限り、5.6 節 に従い新しい鍵を生成し、認証局証明書を発行する。

5.7.4　災害後の事業継続能力

本認証局は、災害復旧サイトを主要施設から 800 km 以上離れた場所に設置しており、自然または人為的な災害が生じ、本認証局の主要施設が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、災害復旧プロセスを開始する。

災害復旧プランは、被災し災害復旧プランを発動した後、24 時間以内に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
- CRL の公表

5.8　認証局または登録局の終了

日本ベリサインが本認証局の業務を終了する場合、業務を終了する3ヶ月以上前に、利用者、依拠当事者およ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。また、認証局が保管する記録等に関して、継続保管または廃棄に関する取り決めを行い、必要に応じて当該処置内容を利用者、依拠当事者および当該処置により影響を受ける他の当事者へ通知する。また、日本ベリサインは、業務を終了する際には、自身が発行した有効な利用者の証明書を全て失効する

6. 技術的セキュリティ管理

6.1 鍵ペア生成およびインストール

6.1.1 鍵ペア生成

本認証局鍵ペアの生成は、権限を有する信頼される者により、FIPS140-1 レベル 3 に対応する暗号モジュール上で行う。尚、暗号モジュールの取り出し、活性化、鍵生成にあたっては、分離された権限を有する複数の信頼される者の立会いが必要である。

利用者の秘密鍵の生成は、一般的には利用者自身により行うが、日本ベリサインが鍵生成をする場合がある。日本ベリサインが利用者の鍵生成をする場合は、当該秘密鍵の紛失、盗難、改ざん、不正な開示、無権限での使用等が行われないよう実施される。

6.1.2 利用者に対する秘密鍵の配送

利用者によって秘密鍵の生成が行われる場合は、秘密鍵の配送は行われない。
日本ベリサインが秘密鍵を生成する場合、その秘密鍵は、利用者が指定した情報を用いて保護される。また、オンラインの場合、通信経路は SSL によって保護される。また当該秘密鍵は、利用者へ配送された後に廃棄される。

6.1.3 認証局に対する利用者の公開鍵

本認証局は利用者からの公開鍵を受領するために SSL によって保護された仕組みを利用する。

6.1.4 依拠当事者に対する認証局の公開鍵の交付

本認証局の証明書は、本認証局のリポジトリからダウンロードすることができる。また、本認証局は、本認証局の証明書（ルート認証局の証明書を除く）を、利用者の証明書の発行と共に利用者に対し提供する場合がある。

6.1.5 鍵サイズ

日本ベリサイン BMS 証明書発行サービスで用いられる鍵対に関する技術的仕様は以下の通り。
(1) ルート認証局 :rsaEncryption(1.2.840.113549.1.1.1) 2048bit
(2) 本認証局 :rsaEncryption(1.2.840.113549.1.1.1) 2048bit
(3) 利用者 :rsaEncryption(1.2.840.113549.1.1.1) 1024bit 以上

利用者の証明書は西暦 2010 年以降においては 2048 ビット以上の RSA 鍵を利用するよう推奨する。

6.1.6 公開鍵のパラメータの生成

規定しない。

6.1.7　鍵用途の目的

本認証局のルート認証局および中間認証局の証明書の keyUsage には、keyCertSign と cRLSign を設定する。

6.2　秘密鍵の保護、および暗号モジュール技術の管理

日本ベリサインは、ルート認証局および中間認証局の秘密鍵のセキュリティを確実にするため、論理的および手続き的な管理の下に物理的な保護を実施している。

6.2.1　暗号モジュールの標準と管理

本認証局の認証局秘密鍵は、FIPS 140-1 レベル 3 を満たす暗号モジュール内で管理する。
日本ベリサインが利用者の鍵生成をする場合、6.1.1 項および、6.1.2 項の規定に従い、日本ベリサインが管理する。

6.2.2　秘密鍵の複数人管理

本認証局では、認証局秘密鍵を格納する暗号モジュールの取り出し、活性化、鍵生成にあたっては、分離された権限を有する複数の信頼される者の立会いが必要である。
日本ベリサインが利用者の鍵生成をする場合、6.1.1 項および 6.1.2 項の規定に従い、日本ベリサインが実施する。

6.2.3　秘密鍵の預託

規定しない。

6.2.4　秘密鍵のバックアップ

本認証局の認証局秘密鍵のバックアップを、障害復旧および災害復旧の目的で行う。秘密鍵のバックアップは、FIPS 140-1 レベル3の暗号モジュール内に保管される。
日本ベリサインが利用者の鍵生成をする場合、6.1.1 項および、6.1.2 項の規定に従い、秘密鍵のバックアップは行わない。

6.2.5　秘密鍵のアーカイブ

規定しない。

6.2.6　秘密鍵の暗号モジュールへの移動

規定しない。

6.2.7　暗号モジュール内での秘密鍵保存

暗号モジュールは、権限が分離された複数名の信頼される者によって開錠可能な金庫内に保管する。

6.2.8　秘密鍵の活性化方法

本認証局の認証局秘密鍵を格納する暗号モジュールを活性化するあたっては、分離された権限を有する複数の信頼される者の立会いが必要である。

6.2.9　秘密鍵の非活性化の方法

規定しない。

6.2.10 秘密鍵の破棄方法

本認証局の認証局秘密鍵を破棄する場合は、日本ベリサイン社内規定に基づき鍵を破壊する。
6.1.1 項および、6.1.2 項の規定に従って日本ベリサインが利用者の鍵生成をする場合は、日本ベリサインが廃棄する。

6.2.11 暗号モジュールの評価

本認証局の鍵を格納する暗号モジュールは FIPS 140-1 レベル 3 を満たすものを利用する。
日本ベリサインが利用者の鍵生成をする場合、6.1.1 項および、6.1.2 項の規定に従い、日本ベリサインが秘密鍵の生成を実施する。

6.3　その他の鍵ペア管理

6.3.1　公開鍵のアーカイブ

本認証局が発行した全ての証明書は、証明書の有効期間満了後、3 年以上保管する。

6.3.2　証明書の運用上の期間、および鍵ペアの使用期間

本認証局で使用する証明書の有効期間および秘密鍵の利用期間は最大で 20 年とする。利用者の証明書の有効期間および秘密鍵の利用期間は最大で 3 年 2 ヶ月とする。

6.4　活性化データ

6.4.1　活性化データの生成、および設定

暗号化モジュールに含まれる本認証局の秘密鍵のための活性化データは、複数の権限を有する信頼される者によって生成され適切に分配される。

6.4.2　活性化データの保護

本認証局の秘密鍵のための活性化データは複数人に分割され、権限が分離された金庫で保管される。

6.4.3　活性化データに他の考慮点

規定しない。

6.5　コンピュータのセキュリティ管理

日本ベリサインは、お客様および企業の情報資産を保護することの重要性を認識し、法令または規制の要求事項、並びに契約上のセキュリティ義務および国際標準のガイドライン JIS Q 27001:2006（ISO/IEC 27001:2005）を遵守し、適性かつ安全に情報資産を取扱い、その信頼に応えるべく認証局に対し登録している当社データセンター「公開鍵基盤（PKI）をベースとした電子証明書発行システムの運用・保守業務」を実施する。

6.6　ライフサイクルの技術上の管理

日本ベリサインは、お客様および企業の情報資産を保護することの重要性を認識し、法令または規制の要求事項、並びに契約上のセキュリティ義務および国際標準のガイドライン JIS Q 27001:2006（ISO/IEC 27001:2005）を遵守し、適性かつ安全に情報資産を取扱い、その信頼に応えるべく認証局に対し登録している当社データセンター「公開鍵基盤（PKI）をベースとした電子証明書発行システムの運用・保守業務」を実施する。

6.7　ネットワークセキュリティ管理

日本ベリサインは、お客様および企業の情報資産を保護することの重要性を認識し、法令または規制の要求事項、並びに契約上のセキュリティ義務および国際標準のガイドライン JIS Q 27001:2006（ISO/IEC 27001:2005）を遵守し、適性かつ安全に情報資産を取扱い、その信頼に応えるべく認証局に対し登録している当社データセンター「公開鍵基盤（PKI）をベースとした電子証明書発行システムの運用・保守業務」を実施する。

6.8　タイム・スタンプ

本認証局は、が 5.4.1 項および 5.5.1 項で保存すると規定した書類・電子データには日時、または日付情報を付与するが、当該情報に対して暗号技術によるタイムスタンプを付与しない。

7. 証明書、CRL、およびOCSP のプロファイル

7.1 証明書のプロファイル

7.1.1 バージョン番号

本認証局は、ITU-T Recommendation X.509 のバージョン 3 に準拠した証明書を発行する。

7.1.2 証明書拡張領域

本認証局の発行する証明書の拡張領域は、下表に従って設定される。

表 7 証明書の拡張領域

拡張領域の名称	Criticality	ルート認証局の証明書	中間認証局の証明書	利用者の証明書
authorityKeyIdentifier	False	○	○	○
subjectKeyIdentifier	False	○	○	○
keyUsage	True/False (※1)	○	○	○
certificatePolicies	False	×	×	○
subjectAltName	False	×	△	×
basicConstraints	True/False (※1)	○	○	○
cRLDistributionPoints	False	×	○	○

“○”:拡張領域が含まれることを示す、“×”:拡張領域が含まれないことを示す、“△”:拡張領域が含まれる場合があることを示す。表に記載されていない拡張領域については、すべての証明書において利用されない。
※1: 認証局を示す証明書(ルート認証局および中間認証局)の場合は True、利用者の証明書の場合は False とする。

(1) authorityKeyIdentifier
当該証明書を発行した認証局の鍵を示す識別子を登録する。
(2) subjectKeyIdentifier
当該証明書の発行対象者(subject)の鍵を示す識別子を登録する。
(3) keyUsage
認証局を示す証明書の場合は keyCertSign と cRLSign を設定する。利用者の証明書の場合は digitalSignature、keyEncipherment、および dataEncipherment を登録する。
(4) certificatePolicies
利用者の証明書の場合、policyIdentifier に本 CPS 1.2 節で規定されたオブジェクト識別子および policyQualifiers に本 CPS 7.1.8 項で規定された値を登録する。
(5) subjectAltName
中間認証局の証明書の場合、当該認証局に係る情報が登録される場合がある。

(6) basicConstraints
ルート認証局の証明書の場合は cA=True および pathLenConstraint=1、中間認証局の証明書の場合は cA=True および pathLenConstraint=0、利用者の証明書の場合は cA=False とする。
(7) cRLDistributionPoints
中間認証局および利用者の証明書において、当該証明書についての失効情報が登録される失効リストが開示される場所を、distributionPoint に URI にて登録する。

7.1.3 アルゴリズムのオブジェクト識別子

本認証局が発行する証明書では、基本領域の signature フィールド内のアルゴリズムを示す部分に sha1WithRSAEncryption（1.2.840.113549.1.1.5）を、基本領域の subjectPublicKeyInfo フィールド内のアルゴリズムを示す部分には rsaEncryption（1.2.840.113549.1.1.1）を登録する。また、本認証局が発行する証明書では、これらのオブジェクト識別子に対応したアルゴリズムを使用する。

7.1.4 名前の形式

本認証局が発行する証明書に登録される発行者の名称（issuer）および発行対象者の名称（subject）は、本 CPS 3.1.2 項に従い、各々と対応する識別名とする。これらのデータ型は、すべて、PrintableString とする。

7.1.5 名前制約

本認証局は、nameConstraints の拡張領域を使用しない。

7.1.6 証明書ポリシー・オブジェクト識別子

本認証局が発行する利用者の証明書では、certificatePolicies の拡張領域を使用する。当該拡張領域では、policyIdentifier において、本 CPS 1.2 節にて規定されたオブジェクト識別子が登録される。

7.1.7 ポリシー制約エクステンションの使用

本認証局は、policyConstraints 拡張領域を使用しない。

7.1.8 ポリシー修飾子の構文および意味

本認証局が発行する利用者の証明書では、certificatePoliciesの拡張領域において、policyQualifiers フィールドを利用する。当該フィールドは、本CPSの開示場所を示すCPSuriを含む。

7.1.9 クリティカルな証明書ポリシー拡張に対する処理の意味

規定しない。

7.2 CRL のプロファイル

7.2.1 バージョン番号

本認証局は、ITU-T Recommendation X.509 で規定されるバージョン 2 に準拠した証明書の失効リスト(CRL)を発行する。

7.2.2 CRLおよびCRLエントリの拡張領域

本認証局の発行する失効リストの拡張領域は、下表に従って設定される。ただし、本項において、ARL とはルート認証局が発行する失効リストを示し、CRL とは中間認証局が発行する失効リストのみを示す。

表 8 CRL 拡張領域

	Criticality	ARL	CRL
authorityKeyIdentifier	False	○	○
cRLNumber	False	○	○

“○”:拡張領域が含まれることを示す。表に記載されていない拡張領域については利用されない。

表 9 CRL エントリ拡張領域

	Criticality	ARL	CRL
reasonCode	False	○	○

“○”:拡張領域が含まれることを示す。表に記載されていない拡張領域については利用されない。

なお、基本領域の thisUpdate フィールドは常に利用され、CRL の場合は当該失効リストの更新時間(thisUpdate フィールドの値) + 96 時間(4 日間)の値が登録される。ARL の場合は本認証局が指定する期間が登録される。また、失効リストへの電子署名に利用されるアルゴリズムは sha1WithRSAEncryption であり、このアルゴリズムを示すオブジェクト識別子(1.2.840.113549.1.1.5)が失効リストの signature フィールドに登録される。

7.3 OCSP のプロファイル

規定しない。

8. 準拠性監査とその他の評価

8.1 監査の頻度あるいは条件

本認証局は、本認証局の運用が、流通業界共通認証局 CP および本 CPS に準拠して行われていることを確認するため、必要に応じて準拠性監査を実施する。ただし、利用者の識別および書類の審査を行う業務については 1 年に 1 回の準拠性監査を実施する。

8.2 監査人の要件

監査人は、監査および認証業務に関する知識を有していなければならない。

8.3 監査人と被監査人の関係

監査人は、外部の監査法人等に所属する者、または日本ベリサインに所属する者とする。ただし、監査人は監査対象業務の運用に直接的な関わりを持たない。

8.4 監査の対象

準拠性監査は、流通業界共通認証局 CP および本 CPS への準拠性を基準として実施される。監査対象項目は、証明書の発行業務、更新業務、失効業務、およびその他の監査人が必要と認めた事項を含むこととするが、これらに限られない。認証局の全般的な環境統制、インフラストラクチャ、証明書ライフサイクルマネージメントおよび情報開示についての項目は、通常の監査対象項目に含まれる。

8.5 監査指摘事項への対応

準拠性監査において、本認証局の運用が流通業界共通認証局 CP または本 CPS に違反すること、または重大な欠陥が発見された場合、日本ベリサインは直ちに是正措置を検討しこれを作成、作成された措置に従って問題の修正を行う。
準拠性監査において、流通業界共通認証局 CP または本 CPS に違反することが発見された場合には、当該内容とその是正処置について認定機関へ報告を行う。

8.6 監査結果の開示

本認証局は、準拠性監査の結果について、外部に開示を行わない。ただし、認定機関より監査結果について照会を受けた場合、監査指摘事項の有無およびその対応状況について、当該認定機関に対して開示を行う。

9. 業務および法律に関するその他の事項

9.1 料金

9.1.1 証明書の発行または更新の料金

日本ベリサインは、証明書の発行、管理および更新についての料金は、以下に開示する。

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

9.1.2 証明書へのアクセスの料金

日本ベリサインは、本認証局がリポジトリにて本認証局に係る証明書を公開し、依拠当事者等がこれを参照することに関して、依拠当事者等に課金を行わない。

9.1.3 失効またはステータス情報へのアクセスの料金

日本ベリサインは、本認証局がリポジトリにて本認証局に係る証明書の失効情報(CRL)を公開し、依拠当事者等がこれを参照することに関して、依拠当事者等に課金を行わない。

9.1.4 他のサービスの料金

日本ベリサインは、本 CPS の閲覧に関して料金を課さない。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、本 CPS の著作権を有する者とのライセンスに関する合意を必要とする。

9.1.5 返金制度

規定しない。

9.2 財務的責任

9.2.1 保険

日本ベリサインは、利用者および依拠当事者に対して、本サービスの利用から生じる損害を補償することを目的とする保険のプログラムを提供しない。

9.2.2 その他の資産

日本ベリサインは、本認証局を運営し、この業務を円滑に実施するために必要となる、十分な財務的基盤を有する。日本ベリサインの財務状況は、https://www.verisign.co.jp/corporate/investor/において公開されている。

9.2.3　拡張された保証

規程しない。

9.3　業務情報の機密性

9.3.1　機密として扱う情報の範囲

日本ベリサインは、利用者または本サービスに係る以下の情報について、機密に取り扱う。ただし、本CPS 9.3.2 項または他の項目において別途規定されている場合を除く。

- 証明書の申請の記録(利用者が提出した書類等に含まれる各種の個人情報を含む)
- トランザクションの記録(記録そのものおよびトランザクションの監査証跡の両方を含む)
- 日本ベリサインにより生成または保有される監査証跡
- 日本ベリサインまたは担当監査人(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
- コンティンジェンシープラン、災害復旧計画、事業継続計画、情報セキュリティ等を定めた日本ベリサイン社内規程
- 日本ベリサイン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

日本ベリサインは、本認証局の運用にあたり証明書の申請者または利用者から入手した各種の機密情報を、本認証局の業務を実施するのに必要とする範囲内でのみ利用する。

9.3.2　機密として扱わない情報

日本ベリサインは、発行された証明書および証明書に登録されている情報、証明書の失効リストおよび失効リストに登録されている情報、および本 CPS 2.2 節に規定されたリポジトリにて開示される情報について、機密として取り扱わない。

9.3.3　機密として扱う情報を保護する責任

日本ベリサインは、機密情報が損なわれ、または第三者に漏えいしないように必要な措置を講じる。また、本認証局の運用にあたり証明書の申請者または利用者から入手した各種の機密情報を、本認証局の業務を実施するのに必要とする範囲内でのみ利用する。

9.4　個人情報のプライバシー保護

9.4.1　プライバシーポリシー

日本ベリサインは、プライバシーポリシーを作成し、以下にて公開している。

・ https://www.verisign.co.jp/repository/privacy/privacy_statement.html

本認証局における個人情報の取り扱いの方針は、本 CPS あるいは関連する契約文書に別途規定されている場合、または別段の合意が当該情報主体者とされない限り、上記のプライバシーポリシーに従うものである。

9.4.2　個人情報

個人情報とは、「個人情報の保護に関する法律」（以下「個人情報保護法」という）および関連法令等で定義される個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む）を示す。
日本ベリサインは、本認証局の運用にあたり入手した各種の個人情報を、本認証局の業務を実施するために必要とする範囲でのみ利用する。

9.4.3　個人情報とみなされない情報

法律に従うことを条件に、証明書および証明書の失効リストにおいて公開される情報は、機密情報とみなさない。

9.4.4　個人情報の保護責任

日本ベリサインは、保護すべき個人情報について、個人情報の保護に関する法令およびプライバシーポリシーの規定に従い適切に管理する。

9.4.5　個人情報を利用するための通知および同意

日本ベリサインは、個人情報を、当該個人情報の主体者から個別の同意を得た場合および法令に定められた場合を除き、あらかじめ定められた利用目的の範囲内でのみ利用する。個人情報の利用目的は、本 CPS または関連する契約文書、あるいはプライバシーポリシーのインターネット上での開示等を通して利用者に通知される。
日本ベリサインは、個人情報の保護に関する法令の規定に従う。

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、以下に相当すると誠実に判断する場合、該当する個人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　その他の情報開示に関する状況

規定しない。

9.5　知的財産権

日本ベリサインは、本認証局が発行したすべての証明書および失効情報に関する知的財産権を留保する。日本ベリサインは、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、当該複製はそれらすべ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依拠当事者規約(利用者の場合には利用者規約)に従うものでなければならない。日本ベリサインは、依拠当事者規約および他の適用される契約の定めるところに従い、依拠当事者としての機能を果たすために証明書の失効情報を使用することを認める。
以下については、本認証局が知的財産権を有するものである。

・　本 CPS
・　利用者規約
・　依拠当事者規約
・　本認証局自身の鍵ペア
・　本認証局から発行されたすべての証明書
・　本認証局から発行された証明書に関わるすべての失効情報

9.6　表明と保証

9.6.1　認証局の表明と保証

日本ベリサインは、本 CPS に定められた各種規定に従い本認証局の運営を行う。日本ベリサインは、以下の事項を保証する。

・　証明書に登録された事項には、本認証局が把握し、または本認証局に起因する重要な不実の記載が存在しないこと
・　証明書には、本認証局が証明書の申請の処理において、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
・　証明書は、本 CPS に定めるすべての重要な要件に合致していること
・　失効情報およびリポジトリのサービスは、すべての重要な点において本 CPS の規定に合致していること

9.6.2　利用者の表明と保証

利用者は、本サービスの利用にあたり、以下の事項を実施または遵守することを保証しなければならない。日本ベリサインが定める利用者規約は、これらと同等の内容を含み、リポジトリにて公開される。

- 証明書の申請
  利用者は、証明書の発行、更新、再発行等の申請時において、本認証局に対して虚偽なく正確な内容の申請を行うこと
- 証明書の登録内容
  利用者は、本認証局から証明書の発行を受けた際に、証明書に登録された内容に、自身が申請した内容と異なる情報が含まれないことの確認を行うこと。また、登録された内容に誤りが発見された場合、または変更が生じた場合には、速やかに当該証明書についての失効の申請を行うこと
- 鍵ペアの管理
  利用者は、自身の秘密鍵を、権限のない者による使用、紛失、改ざんまたは盗難から保護するために必要な十分な処置を講じること
- 証明書の利用の範囲
  利用者は、本 CPS 1.4 節の規定に従い、認められた範囲でのみ証明書を利用すること
- 適切なシステムの利用
  依拠当事者は、証明書の取り扱いにおいて、適切なソフトウェアおよびハードウェアを利用すること
- 従業者の管理（利用者が法人の場合）
  法人は、自身の業務のために本認証局に各種の申請を行わせる者（役員、社員、契約社員等を含む）、または発行した証明書を利用させる者（同左）について、適切な管理を行い、本 CPS および利用者規約等で定められた各種の要件を理解させ承諾させ、遵守させること。これらの者の行為によって何らの損害が発生した場合、法人は、その賠償について責任を負うこと
- 本 CPS および利用者規約
  利用者は、本 CPS および利用者規約の内容を理解し承諾し、これに従うこと

9.6.3　依拠当事者の表明と保証

依拠当事者は、本認証局が発行する証明書を利用するにあたり、以下の事項を実施または遵守することを保証しなければならない。日本ベリサインが定める依拠当事者規約は、これらと同等の内容を含み、リポジトリにて公開される。

- 証明書の利用の範囲
  依拠当事者は、本 CPS 1.4 節の規定に従い、認められた範囲でのみ証明書を利用すること
- 証明書への依拠
  依拠当事者は、自身の目的のために当該証明書を利用することが適切かどうかを、十分な情報に基づき、自身で評価し判断すること
- 証明書の検証
  依拠当事者は、証明書の利用にあたり、本認証局が発行する正しい認証局の証明書をリポジトリ等から入手し、利用者の証明書に施された電子署名が本認証局の秘密鍵で正しくおこなわれていること、および利用者の証明書が改ざんされていないことを確認すること。また、これらのすべての証明書が有効期間内であること、および失効リストにおいて失効されていないことを確認すること
- 適切なシステムの利用
  依拠当事者は、証明書の取り扱いにおいて、適切なソフトウェアおよびハードウェアを利用すること
- 本 CPS および依拠当事者規約
  依拠当事者は、本 CPS および依拠当事者規約の内容を理解し承諾し、これに従うこと

9.7　保証の否認

日本ベリサインは、本 CPS 9.6.1 項において明確に規定された以上の内容を保証しない。

9.8　責任の制限

日本ベリサインの責任は、本認証局の運用が、本 CPS および流通業界共通認証局 CP に定められた要件を果たさなかった場合に限定される。
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何らの責任を負わない。また、地震、洪水、火災、暴風、天変地異、戦争、テロ、武力衝突、ストライキ、ロックアウト、ボイコット、その他当事者の合理的な支配を超えた類似の事由により、本 CPS または流通業界共通認証局 CP に定められた義務の履行が停止、中断または遅延した場合（ただし、支払いの義務を除く）、何れの当事者も債務の不履行とはみなされず、これによる責任を他の当事者に対し負わない。

日本ベリサインの責による損害に対して、日本ベリサインがある特定の証明書に関して負う損害賠償額の上限は、利用者が本 CPS9.6.2 項、その他本 CPS で定める利用者の義務に違反したことに起因して生じた損害について、本認証局に支払った料金を超えないものとする。また、検証者が本 CPS9.6.3 項、その他本 CPS で定める検証者の義務に違反したことに起因して生じた損害についても、本認証局に支払った料金を超えないものとする。

9.9 補償

日本ベリサインは、本認証局の責に帰さない事由により生じた損害について、賠償の責任を有しない。日本ベリサインによる補償の範囲および額については、本 CPS 9 章の他の項目および利用者規約または依拠当事者規約に定められた内容に従う。

日本ベリサインは、利用者または依拠当事者の行為により日本ベリサインその他の関係者に損害が発生した場合に利用者または依拠当事者が負うべき補償の内容について、利用者規約または依拠当事者規約に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、本 CPS 2.2 節に規定されたリポジトリに掲載された時点で有効とする。また、本 CPS の変更についても、リポジトリに掲載された時点で有効とする。

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。ただし、本 CPS は、リポジトリにおいて最新版でないことが示された場合、または、日本ベリサインが本サービスの提供を終了した時点で無効となる。

9.10.3 終了の効果と効力の残存

本 CPS の効力が終了した場合においても、本 CPS 9.3 節、9.4 節、9.5 節、9.7 節、9.8 節、9.9 節の効力は存続する。

9.11 参加者の個別の通知と連絡

本認証局は、1.5.2 で定める本サービスに関する問い合わせ窓口を通じて参加者から通知を受領するものとし、また、参加者へ連絡を行う。

9.12 改訂

9.12.1 改訂手続き

日本ベリサインは、最新技術の動向や社会的状況その他の状況等を踏まえ、本サービスおよび本認証局の仕様に変更が必要と考えた場合、本 CPS および関連するその他の文書を改訂することができる。本 CPS の改訂は、日本ベリサインにおいて定められた手続きに従う。日本ベリサインは、本 CPS について重要な改訂と判断した場合、当該変更について認定機関に照会を行い、当該変更が流通業界共通認証局 CP に違反しないことの確認を行う。

日本ベリサインは、利用者または依拠当事者の事前の了承なしに、本 CPS を改訂することができる。本 CPS に変更が発生した場合、日本ベリサインは当該 CPS の最新版、もしくはその時点で有効な本 CPS との差分について、本 CPS 2.2 節に規定されたリポジトリにて開示する。

9.12.2 通知方法と期間

本 CPS の改訂が行われる場合、日本ベリサインは、当該 CPS の最新版、もしくはその時点で有効な CPS との差分について、本 CPS 2.2 節に規定されたリポジトリにて開示する。開示された CPS またはその差分についての情報は、別段の指定がない限り、開示時点から有効である。

本 CPS の変更を承諾しない利用者は、日本ベリサインが変更の開示を行ってから 15 日以内に、自身に発行された証明書について、本認証局に失効の申請をしなければならない。また、本 CPS の変更を承諾しない利用者および依拠当事者は、開示後 15 日以内に、本認証局が発行したすべての証明書の利用を停止しなければならない。

ただし、日本ベリサインは、本 CPS について、重要な変更を行う場合、変更を行う前にこれをリポジトリに掲示し、利用者、依拠当事者その他の者から当該変更に係る意見の募集を行うことができる。
当該手続きによって本 CPS の変更を検討する場合の具体的な手順（コメント募集期間等を含む）は、当該手続きの実施時にリポジトリにおいて開示する。

9.12.3 OID の変更が必要な場合

規定しない。

9.13 紛争の解決

別段の合意がされない限り、本認証局または本サービスに関し何らかの紛争が生じ、関係者がその解決のために訴訟手段等の申し立てを行う場合には、東京地方裁判所を第一審の専属的合意管轄裁判所とする。
本認証局の利用者規約および依拠当事者規約は、紛争の解決に係る条項を含むものとする。

9.14 準拠法

本 CPS は日本国内法に準拠し解釈される。日本ベリサインと関係者間で紛争が生じた場合に適用される法律は、日本国内法とする。

9.15 法の遵守

日本ベリサインは、日本国内法に従い、本認証局の運営を行う。本 CPS の一部の規定またはその運用が日本国内法の定めに抵触することが発見された場合には、日本国内法を優先する。

9.16 雑則

9.16.1 完全合意条項

本 CPS は、口頭で変更、追加、削除または終了させることはできない。

9.16.2 権利譲渡条項

関係者は、本 CPS において別途定められた場合を除き、本 CPS に定められた地位もしくは権利を第三者に譲渡または担保に供してはならず、また、本 CPS に定められた義務を第三者に引き受けさせてはならない。

9.16.3 分離可能性

本 CPS の一部の規定が裁判所等により何らかの理由で無効または執行不可能であるとされた場合においても、残存する規定については有効とされる。

9.16.4 強制執行(弁護士費用と権利放棄)

規定しない。

9.16.5 不可抗力

地震、洪水、火災、暴風、天変地異、戦争、テロ、武力衝突、ストライキ、ロックアウト、ボイコット、その他当事者の合理的な支配を超えた類似の事由により、本 CPS に定められた義務の履行が停止、中断または遅延した場合(ただし、支払いの義務を除く)、何れの当事者も契約の不履行とはみなされず、これによる責任を他の当事者に対し負わない。
本認証局の利用者規約および依拠当事者規約は、不可抗力に係る条項を含むものとする。

9.17 その他の条項

規定しない。

Appendix A. 略語・定義表

略語

Term	Definition
CA	Certification Authority.
CP	Certificate Policy.
CPS	Certification Practice Statement.
CRL	Certificate Revocation List.
EDI	Electronic Data Interchange
EPC	Electronic Product Code
FIPS	United State Federal Information Processing Standards.
FQDN	Fully Qualified Domain Name
GDS	Global Data Synchronization
OCSP	Online Certificate Status Protocol.
PKCS	Public-Key Cryptography Standard.
PKI	Public Key Infrastructure.
RA	Registration Authority.
RFC	Request for comment.
SSL	Secure Sockets Layer.

定義

Term	Definition
Certificate 証明書	少なくとも、認証局の名称を記載しまたは認証局を識別し、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、これに認証局がデジタル署名したメッセージ。
Certificate Policies (CP) サーティフィケート・ポリシー	流通システム標準普及推進協議会が定める流通業界共通認証局証明書ポリシー
Certificate Revocation List (CRL)	本 CPS 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、認証局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・ナンバーおよびその具体的時期および理由を示す。
Certification Authority (CA) 認証局	日本ベリサイン内で証明書の発行、管理、失効および更新を授権された認証局
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	日本ベリサインが証明書申請の承認または拒絶、証明書を発行、管理および失効をする際に採用する運用手続きを規定した文書。
Electronic Data Interchange (EDI)	商取引に関する情報を標準的な書式に統一して、企業間で電子的に交換する仕組み。受発注や見積もり、決済、出入荷などに関わるデータを、あらかじめ定められた形式に従って電子化し、専用線や VAN などのネットワークを通じて送受信する。
Electronic Product Code (EPC)	IC タグを利用して製品識別を行う場合に利用されるコード。
Fully Qualified Domain Name (FQDN)	インターネットやイントラネットなどの TCP/IP ネットワーク上で、ドメイン名・サブドメイン名・ホスト名を省略せずにすべて指定した記述形式のこと。
Global Data Synchronization (GDS)	Global Data Synchronization(商品マスターデータの国際的な同期化)という標準規格。食品や日用品といった商品は、メーカーが商品発売時に 1 度だけ商品名や寸法、外観写真、重量などの項目を含む「商品マスター」情報を提供し、卸や小売りが

Term	Definition
	そのまま共有して使えるという取り組み。
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
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。
Public Key Infrastructure (PKI) 公開鍵インフラストラクチャ	証明書を基盤とする公開鍵暗号システムの実施およ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、実務および手続きのこと。
Registration Authority (RA) 登録局	認証局から承認された登録局であって、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	認証局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。
RSA	公開鍵暗号方式は、Rivest, Shamir, Adelman によって発明された。
Secure Sockets Layer (SSL) セキュア・ソケット・レイヤ	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およびオプションとしてクライアント認証を提供する。
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 利用者規約	認証局または登録局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。
Repository リポジトリ	証明書および他の関連する情報に関するデータベースでオンラインでのアクセスが可能なもの。
WHOIS 検索 フーイズ検索	Whois とは、IP アドレスやドメイン名の登録者などに関する情報を、インターネットユーザが誰でも参照できるサービス。このサービスは、主に以下の目的でレジストリやレジストラが提供している。
本サービス	流通業界に関係する法人もしくは個人(個人事業主)に対して、電子的な証明書(以下「証明書」という)を提供するベリサイン BMS 証明書発行サービス
ベリサイン BMS ルート認証局	本サービスのルート認証局
流通 Bussiness Message Standards (流通 BMS)	流通ビジネスメッセージ標準のこと。消費財流通業界で唯一の標準となることを目標に策定している、メッセージ(電子取引文書)と通信プロトコル/セキュリティに関する EDI 標準仕様です。(BMS は Business Message Standards の略)