クロストラスト認証局
SHA-256 DV2 証明書ポリシー
（Certificate Policy）

Version1.10

2018 年 08 月 01 日

クロストラスト株式会社

変更日付	版数	変更箇所
2018/04/16	1.00	初版
2018/08/01	1.10	ドメイン認証に関する記述の追加

～ 目 次 ～

1. はじめに 1

1.1 概要 1
1.2 文書名と識別 1
1.3 PKI の関係者 2
1.3.1 認証局 2
1.3.2 証明書利用者 2
1.3.3 検証者 2
1.4 証明書の用途 2
1.4.1 適切な証明書の用途 2
1.4.2 禁止される証明書の用途 2
1.5 ポリシー管理 2
1.5.1 文書を管理する組織 2
1.5.2 連絡先 3
1.5.3 ポリシー適合性を決定する者 3
1.5.4 承認手続 3
1.6 定義と略語 3

2. 公開とリポジトリの責任 7

2.1 リポジトリ 7
2.2 証明情報の公開 7
2.3 公開の時期又は頻度 7
2.4 リポジトリへのアクセス管理 7

3. 識別と認証 8

3.1 名前決定 8
3.1.1 名前の種類 8
3.1.2 名前が意味を持つことの必要性 8
3.1.3 証明書利用者の匿名性又は仮名性 8
3.1.4 様々な名前形式を解釈するための規則 8
3.1.5 名前の一意性 8
3.1.6 認識、認証及び商標の役割 8
3.2 初回の本人確認 8
3.2.1 私有鍵の所持を証明する方法 8
3.2.2 組織の認証 9
3.2.3 個人の認証 9
3.2.4 検証されない証明書利用者の情報 9

3.2.5 権限の正当性確認 9
3.2.6 相互運用の基準 9
3.2.7 ドメインの認証 9
3.3 鍵更新申請時の本人性確認と認証 10
3.4 失効申請時の本人性確認と認証 10
4. 証明書のライフサイクルに対する運用上の要件 11
4.1 証明書申請 11
4.1.1 証明書申請を提出することができる者 11
4.1.2 登録手続及び責任 11
4.2 証明書申請手続 11
4.2.1 本人性確認と認証の実施 11
4.2.2 証明書申請の承認又は却下 11
4.2.3 証明書申請の処理時間 11
4.2.4 CAA レコードの確認 11
4.3 証明書の発行 11
4.3.1 証明書発行時の処理手続 11
4.3.2 証明書利用者への証明書発行通知 12
4.4 証明書の受領確認 12
4.4.1 証明書の受領確認手続 12
4.4.2 認証局による証明書の公開 12
4.4.3 他のエンティティに対する認証局の証明書発行通知 12
4.5 鍵ペア及び証明書の用途 12
4.5.1 証明書利用者の私有鍵及び証明書の用途 12
4.5.2 検証者の公開鍵及び証明書の用途 12
4.6 証明書の更新 12
4.7 鍵更新を伴う証明書の更新 13
4.7.1 更新事由 13
4.7.2 新しい証明書の申請を行うことができる者 13
4.7.3 更新申請の処理 13
4.7.4 証明書利用者に対する新しい証明書の通知 13
4.7.5 鍵更新された証明書の受領確認手続き 13
4.7.6 認証局による鍵更新済みの証明書の公開 13
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 13
4.8 証明書の変更 13
4.9 証明書の失効と一時停止 13
4.9.1 証明書失効事由 13

4.9.2 証明書失効を申請することができる者 14
4.9.3 失効申請手続 14
4.9.4 失効申請の猶予期間 14
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 14
4.9.6 失効調査の要求 14
4.9.7 証明書失効リストの発行頻度 15
4.9.8 証明書失効リストの発行最大遅延時間 15
4.9.9 オンラインでの失効/ステイタス確認の適用性 15
4.9.10 オンラインでの失効/ステイタス確認を行うための要件 15
4.9.11 利用可能な失効情報の他の形式 15
4.9.12 鍵の危殆化に対する特別要件 15
4.9.13 証明書の一時停止事由 15
4.9.14 証明書の一時停止を申請することができる者 15
4.9.15 証明書の一時停止申請手続 15
4.9.16 一時停止を継続することができる期間 15
4.10 証明書のステイタス確認サービス 15
4.10.1 運用上の特徴 16
4.10.2 サービスの利用可能性 16
4.10.3 オプショナルな仕様 16
4.11 加入（登録）の終了 16
4.12 キーエスクローと鍵回復 16
4.12.1 キーエスクローと鍵回復ポリシー及び実施 16
4.12.2 セッションキーのカプセル化と鍵回復のポリシー及び実施 16
5. 設備上、運営上、運用上の管理 17
5.1 物理的管理 17
5.2 手続的管理 17
5.3 人事的管理 17
5.4 監査ログの手続 17
5.5 記録の保管 17
5.5.1 アーカイブの種類 17
5.5.2 アーカイブ保存期間 17
5.5.3 アーカイブの保護 17
5.5.4 アーカイブのバックアップ手続 17
5.5.5 記録にタイムスタンプを付与する要件 18
5.5.6 アーカイブ収集システム 18
5.5.7 アーカイブの検証手続 18

5.6 鍵の切り替え 18
5.7 危殆化及び災害からの復旧 18
5.8 認証局又は登録局の終了 18
6. 技術的セキュリティ管理 19
6.1 鍵ペアの生成及びインストール 19
6.1.1 鍵ペアの生成 19
6.1.2 証明書利用者に対する私有鍵の交付 19
6.1.3 認証局への公開鍵の交付 19
6.1.4 信頼者への CA 公開鍵の交付 19
6.1.5 鍵サイズ 19
6.1.6 公開鍵のパラメータの生成及び品質検査 19
6.1.7 鍵の用途 19
6.2 私有鍵の保護及び暗号モジュール技術の管理 20
6.3 鍵ペアのその他の管理方法 20
6.4 活性化データ 20
6.5 コンピュータのセキュリティ管理 20
6.6 ライフサイクルセキュリティ管理 20
6.7 ネットワークセキュリティ管理 20
6.8 タイムスタンプ 20
7. 証明書及び証明書失効リストのプロファイル 21
7.1 証明書のプロファイル 21
7.2 CRL のプロファイル 22
7.3 OCSP のプロファイル 22
7.3.1 バージョン番号 23
7.3.2 OCSP 拡張 23
8. 準拠性監査と他の評価 23
8.1 監査の頻度 23
8.2 監査者の身元／資格 23
8.3 監査者と被監査者の関係 23
8.4 監査で扱われる事項 23
8.5 不備の結果としてとられる処置 23
8.6 監査結果の開示 23
9. 他の業務上及び法的事項 25
9.1 料金 25

9.2 財務的責任 25
9.3 企業情報の機密性 25
9.3.1 機密情報の範囲 25
9.3.2 機密情報の範囲外の情報 25
9.3.3 機密情報を保護する責任 25
9.4 個人情報の保護 25
9.5 知的財産権 26
9.6 表明保証 26
9.6.1 認証局の表明保証 26
9.6.2 証明書利用者の表明保証 26
9.6.3 検証者の表明保証 26
9.6.4 他の関係者の表明保証 26
9.7 無保証 26
9.8 責任の制限 27
9.9 補償 27
9.10 有効期間と終了 27
9.10.1 有効期間 27
9.10.2 終了 27
9.10.3 終了の効果と効果継続 28
9.11 関係者間の個別通知と連絡 28
9.12 改訂 28
9.12.1 改訂手続 28
9.12.2 通知方法及び期間 28
9.12.3 オブジェクト識別子が変更されなければならない場合 28
9.13 紛争解決手続 28
9.14 準拠法 28
9.15 適用法の遵守 29
9.16 雑則 29
9.17 その他の条項 29

1. はじめに

1.1 概要

クロストラスト認証局 DV 証明書ポリシー（以下、「本 CP」という）は、クロストラスト株式会社（以下「クロストラスト」という）が認証局（以下、「本 CA」という）として発行する電子証明書の用途、利用者手続、発行手続等、電子証明書に関するポリシーを規定するものである。本 CA の運用維持に関する諸手続については、セコム認証基盤運用規程（以下、「CPS」という）に規定する。

本 CA は、セコムトラストシステムズ株式会社（以下、「セコムトラストシステムズ」という）が運営する認証局である Security Communication RootCA2 より、片方向相互認証証明書の発行を受けており、中間 CA として証明書利用者に対する証明書発行を行う。

本 CA が発行する証明書は、サーバ認証及び通信経路で情報の暗号化を行うことに利用する。証明書の有効期間は、証明書を有効とする日から起算して 825 日以内とする。

本 CA から証明書の発行を受ける者は、証明書の発行を受ける前に自己の利用目的と本 CP 及び CPS とを照らし合わせて評価し、本 CP 及び CPS を承諾する必要がある。

本 CP は、IETF が認証局運用のフレームワークとして提唱する RFC3647「Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework」に準拠している。

本 CP は、CA/Browser Forum が https://www.cabforum.org/で公開する「Baseline Requirements」に準拠している。

本 CP は、本 CA に関する技術面、運用面の発展や改良に伴い、それらを反映するために必要に応じ改訂されるものとする。

1.2 文書名と識別

本 CP の正式名称は、「クロストラスト認証局 SHA-256 DV2 証明書ポリシー」という。本 CA では、発行する証明書の種類及び発行基準に応じて一意となるオブジェクト識別子（以下、OID という）が割り当てられ、各証明書内に示すものとする。本 CA が本 CP に基づき発行する証明書及び対応する OID、並びに本 CP が参照する CPS の OID は、次のとおりである。

CP OID クロストラスト認証局 SHA-256 DV2 証明書ポリシー 1.2.392.200220.1.8

CPS OID セコム電子認証基盤認証運用規程 1.2.392.200091.100.401.1

1.3　PKI の関係者

1.3.1　認証局

CA（Certification Authority：認証局）とは、IA（Issuing Authority：発行局）及び RA（Registration Authority：登録局）によって構成される。本 CA においては、セコムトラストシステムズが IA としての役割を担い、クロストラストおよびセコムトラストシステムズが RA としての役割を担う。

1.3.1.1　IA

IA は、証明書の発行、取消、CRL（Certificate Revocation List：証明書失効リスト）の開示等を行う。

1.3.1.2　RA

RA は、証明書の発行、取消を申請する申請者の審査及び証明書を発行、失効するための登録業務等を行う。

1.3.2　証明書利用者

証明書利用者とは、本 CA より証明書の発行を受け、発行された証明書を利用する個人、法人及び組織とする。

1.3.3　検証者

検証者とは、本 CA が発行する証明書の有効性を検証する個人、法人及び組織とする。

1.4　証明書の用途

1.4.1　適切な証明書の用途

本 CA が発行する証明書は、通信経路で情報の暗号化を行うことに利用する。

1.4.2　禁止される証明書の用途

本 CA が発行する証明書の用途は「1.4.1 適切な証明書の用途」のとおりであり、証明書をそれ以外の目的に利用することはできないものとする。

1.5　ポリシー管理

1.5.1　文書を管理する組織

本 CP の維持、管理は、本 CA が行う。

1.5.2　連絡先

本 CP に関する連絡先は、次のとおりである。

窓口：クロストラスト株式会社　認証サービス部

電話：0120-979-717

電子メール：support@crosstrust.co.jp

1.5.3　ポリシー適合性を決定する者

本 CP の内容について、本 CA の意思決定組織において決定される。

1.5.4　承認手続

本 CP は、本 CA の意思決定組織の承認によって発効される。

1.6　定義と略語

(1)　「あ」～「ん」

アーカイブ

法的又はその他の事由により、履歴の保存を目的に取得する情報のことをいう。

エスクロー

第三者に預けること（寄託）をいう。

鍵ペア

公開鍵暗号方式において、私有鍵と公開鍵から構成される鍵の対のことをいう。

監査ログ

認証局システムへのアクセスや不正操作の有無を検査するために記録される認証局システムの動作履歴やアクセス履歴等をいう。

公開鍵

公開鍵暗号方式において用いられる鍵ペアの一方をいい、私有鍵に対応し、通信相手の相手方に公開される鍵のことをいう。

私有鍵

公開鍵暗号方式において用いられる鍵ペアの一方をいい、公開鍵に対応する本人のみが保有する鍵のことをいう。

タイムスタンプ

電子ファイルの作成日時やシステムが処理を実行した日時等を記録したデータのことをいう。

電子証明書

ある公開鍵を、記載された者が保有することを証明する電子データのことをいう。CA が電子署名を施すことで、その正当性が保証される。

リポジトリ

CA 証明書及び CRL 等を格納し公表するデータベースのことをいう。

(2) 「A」～「Z」

CA（Certification Authority）：認証局

証明書の発行・更新・失効、CA 私有鍵の生成・保護及び証明書利用者の登録等を行う主体のことをいう。

CAA（Certificate Authority Authentication）：レコード

証明書の発行申請を受けた CA が該当ドメインにおいて正当な証明書発行者として登録されているかどうかを確認するために利用される DNS リソースレコードのことをいう。

CP（Certificate Policy）

CA が発行する証明書の種類、用途、申込手続等、証明書に関する事項を規定する文書のことをいう。

CPS（Certification Practices Statement）：認証運用規定

CA を運用する上での諸手続、セキュリティ基準等、CA の運用を規定する文書のことをいう。

CRL（Certificate Revocation List）：証明書失効リスト

証明書の有効期間中に、証明書記載内容の変更、私有鍵の紛失等の事由により失効された証明書情報が記載されたリストのことをいう。

FIPS140-2

米国 NIST（National Institute of Standards and Technology）が策定した暗号モジュールに関するセキュリティ認定基準のこという。最低レベル 1 から最高レベル 4 まで

定義されている。

FIPS180-4

米国 NIST（National Institute of Standards and Technology）が策定したハッシュ関数（要約関数）に関する基準のこという。SHA-1、SHA-224、SHA-256、SHA-384、SHA-512、SHA-512/t が規定されている。

HSM（Hardware Security Module）

私有鍵の生成、保管、利用などにおいて、セキュリティを確保する目的で使用する耐タンパー機能を備えた暗号装置のことをいう。

IA（Issuing Authority）：発行局

CA の業務のうち、証明書の発行・更新・失効、CA 私有鍵の生成・保護、リポジトリの維持・管理等を行う主体のことをいう。

OCSP（Online Certificate Status Protocol）：オンライン証明書状態プロトコル

オンラインによる証明書の失効/ステイタス情報の確認の為のプロトコルのことをいう。

OID（Object Identifier）：オブジェクト識別子

ネットワークの相互接続性やサービス等の一意性を維持管理するための枠組みであり、国際的な登録機関に登録された、世界中のネットワーク間で一意となる数字のことをいう。

PKI（Public Key Infrastructure）：公開鍵基盤

電子署名、暗号化、認証といったセキュリティ技術を実現するための、公開鍵暗号方式という暗号技術を用いる基盤のことをいう。

RA（登録局）（Registration Authority）：登録機関

CA の業務のうち、申込情報の審査、証明書発行に必要な情報の登録、CA に対する証明書発行要求等を行う主体のことをいう。

RFC3647（Request For Comments 3647）

インターネットに関する技術の標準を定める団体である IETF（The Internet Engineering Task Force）が発行する文書であり、CP/CPS のフレームワークを規定した文書のことをいう。

RFC5019（Request For Comments 5019）

インターネットに関する技術の標準を定める団体である IETF（The Internet Engineering Task Force）が発行する文書であり、大容量環境の為の軽量 OCSP のプロファイルを規定した文書のことをいう。

RFC5280（Request For Comments 5280）

インターネットに関する技術の標準を定める団体である IETF（The Internet Engineering Task Force）が発行する文書であり、証明書と失効リストのプロファイルを規定した文書のことをいう。

RFC6844（Request For Comments 6844）

インターネットに関する技術の標準を定める団体である IETF（The Internet Engineering Task Force）が発行する文書であり、CAA（Certificate Authority Authentication）を規定した文書のことをいう。

RFC6960（Request For Comments 6960）

インターネットに関する技術の標準を定める団体である IETF（The Internet Engineering Task Force）が発行する文書であり、OCSP を規定した文書のことをいう。

RSA

公開鍵暗号方式として普及している最も標準的な暗号技術のひとつである。

SHA-1, SHA-256（Secure Hash Algorithm）

電子署名に使われるハッシュ関数（要約関数）のひとつである。ハッシュ関数とは、与えられた原文から固定長のビット列を生成する演算手法をいう。

データの送信側と受信側でハッシュ値を比較することで、通信途中で原文が改ざんされていないかを検出することができる。

2. 公開とリポジトリの責任

2.1 リポジトリ

本 CA は、リポジトリを 24 時間 365 日利用できるように維持管理を行う。ただし、利用可能な時間内においてもシステム保守等により利用できない場合がある。

2.2 証明情報の公開

本 CA は、証明書失効リスト（以下「CRL」という）、本 CP および CPS をリポジトリ上に公開し、証明書利用者および検証者がオンラインによって閲覧できるようにする。

2.3 公開の時期又は頻度

本 CP 及び CPS は、改訂の都度、リポジトリ上に公開する。

本 CA は、24 時間ごとに新たな CRL を発行し、リポジトリ上に公開する。また、証明書の失効が行われた場合、即時に新たな CRL を発行し、リポジトリ上に公開する。また、証明書の有効期間を過ぎたものは CRL から削除する。

2.4 リポジトリへのアクセス管理

本 CA は、リポジトリでの公開情報に関して、特段のアクセスコントロールは行わない。証明書利用者は、本 CA の CRL を、リポジトリを通じて入手することを可能とする。リポジトリへのアクセスは、一般的な Web インターフェースを通じて可能とする。

3. 識別と認証

3.1 名前決定

3.1.1 名前の種類

本 CA が発行する証明書に記載される発行者及び証明書利用者の名前は、X.500 シリーズの識別名規定に従い設定する。

3.1.2 名前が意味を持つことの必要性

本 CA が発行する証明書中に用いられるコモンネームの有用性は、証明書利用者が本 CA が発行する証明書をインストールする予定のサーバの DNS 内で使われるホスト名とする。

3.1.3 証明書利用者の匿名性又は仮名性

本 CA が発行する証明書のコモンネームには、匿名や仮名での登録は行わないものとする。

3.1.4 様々な名前形式を解釈するための規則

様々な名前の形式を解釈する規則は、X.500 シリーズの識別名規定に従う。

3.1.5 名前の一意性

本 CA が発行する証明書に記載される識別名(DN) (distinguished name) の属性は、発行対象となるサーバに対して一意なものとする。

3.1.6 認識、認証及び商標の役割

本 CA は、証明書申請に記載される名称について知的財産権を有しているかどうかの検証を行わない。証明書利用者は、第三者の登録商標や関連する名称を、本 CA に申請してはならない。本 CA は、登録商標等を理由に証明書利用者と第三者間で紛争が起こった場合、仲裁や紛争解決は行わない。また、紛争を理由に証明書利用者からの証明書申請の拒絶や発行された証明書失効をする権利を有する。

3.2 初回の本人確認

3.2.1 私有鍵の所持を証明する方法

証明書利用者が私有鍵を所有していることの証明は、証明書発行要求（Certificate Signing Request：以下、「CSR」という）の署名の検証を行い、当該 CSR が、公開鍵に対応する私有鍵で署名されていることを確認する。

3.2.2 組織の認証

本 CA は、組織の実在性を確認しない。

3.2.3 個人の認証

本 CA は、証明書の申込を行う者が証明書利用者もしくはその代理人であることについて、本人性確認及び申込の意思確認を行う。

3.2.4 検証されない証明書利用者の情報

証明書に記載されるドメイン名もしくは IP アドレス以外の情報については、その真正性及び正確性を確認しない。

3.2.5 権限の正当性確認

本 CA は、証明書を発行した時点において、証明書利用者が証明書に記載されるドメイン名もしくは IP アドレスを所有しているか、あるいはその所有者より排他的な使用権を許諾されていることを確認する。

3.2.6 相互運用の基準

本 CA は、セコムトラストシステムズが運営する認証局である Security Communication RootCA2 より、片方向相互認証証明書を発行されている。当該証明書に関するポリシーについては、Security Communication RootCA2 の CP/CPS で規定される。

3.2.7 ドメインの認証

本 CA は、証明書利用者がドメイン名の利用権を有しているか確認するため、次の方法でドメインの認証を行う。

1. ローカル部は’admin’、’administrator’、’webmaster'、’hostmaster’、または ’postmaster’とし、「@」以下は認証ドメイン名として作成した電子メールアドレスにランダム値を送信して、ランダムな値が含まれた確認応答を受け取ることによって、要求された FQDN の制御を実証する。
2. WHOIS レジストリサービスに登録されたドメイン管理者の電子メールアドレスにランダム値を送信し、ランダムな値が含まれた確認応答を受け取ることによって、要求された FQDN の制御を実証する。
3. HTTP または HTTPS でアクセスが可能な認証ドメイン名の

″/.well-known/pki-validation″ directory 配下に配置されたファイルの値が認証局から指定された値であるか確認することにより、ドメイン審査を行う。

4. その他 Baseline Requirements に準拠した合理的な方法で確認する。

3.3 鍵更新申請時の本人性確認と認証

鍵更新時における証明書利用者の本人性確認及び認証は、「3.2 初回の本人性確認」と同様とする。

3.4 失効申請時の本人性確認と認証

本 CA は、証明書利用者だけがアクセス可能なホームページから失効申請を受け付けるか、あるいは他の通信手段によって本 CA と証明書利用者だけが知りえる情報の提示を受けることによって、証明書失効申請時の本人性確認を行う。

4. 証明書のライフサイクルに対する運用上の要件

4.1 証明書申請

4.1.1 証明書申請を提出することができる者

証明書の発行申請を行うことができる者は、クロストラストが提供する SSL サーバ証明書発行サービスの契約者、契約組織の担当者又はその代理人とする。

4.1.2 登録手続及び責任

証明書利用者は、証明書の発行申請を行うにあたり、本 CP 及び CPS の内容を承諾した上で申請を行うものとする。また、本 CA に対する申請内容が正確な情報であることを保証しなければならない。

4.2 証明書申請手続

4.2.1 本人性確認と認証の実施

本 CA は、本 CP「3.2. 初回の本人確認」に記載の情報をもって、申請情報の審査を行う。

4.2.2 証明書申請の承認又は却下

本 CA は、承認を行った申請について証明書の発行登録を行う。

不備がある申請については、申請を却下し、申請を行った者に対し申請の再提出を依頼する。

4.2.3 証明書申請の処理時間

本 CA は、承認を行った申請について、適時証明書の発行登録を行う。

4.2.4 CAA レコードの確認

本 CA は、申請情報の審査時に CAA レコードを確認する。CAA レコードに記載する本 CA のドメインは「crosstrust.co.jp」とする。

4.3 証明書の発行

4.3.1 証明書発行時の処理手続

本 CA は、証明書申請の承認が完了した後、申請された情報に基づき証明書を発行する。

4.3.2　証明書利用者への証明書発行通知

本 CA は、証明書利用者に対し電子メールを送付することにより証明書の発行通知を行う。

4.4　証明書の受領確認

4.4.1　証明書の受領確認手続

証明書利用者が、証明書利用者だけがアクセス可能なホームページから証明書をダウンロードするか、あるいは他の方法によって証明書利用者が送付された証明書をサーバに導入した時点をもって、証明書が受領されたものとする。

4.4.2　認証局による証明書の公開

本 CA は、証明書利用者の証明書の公開は行わない。

4.4.3　他のエンティティに対する認証局の証明書発行通知

本 CA は、第三者に対する証明書の発行通知は行わない。

4.5　鍵ペア及び証明書の用途

4.5.1　証明書利用者の私有鍵及び証明書の用途

証明書利用者は、本 CA が発行する証明書及び対応する私有鍵を、サーバ認証及び通信経路で情報の暗号化を行うことにのみ利用するものとする。証明書利用者は、本 CA が承認をした用途のみに当該証明書及び対応する私有鍵を利用するものとし、その他の用途に利用してはならない。

4.5.2　検証者の公開鍵及び証明書の用途

検証者は、本 CA の証明書を使用することで、本 CA が発行した証明書の信頼性を検証することができる。本 CA が発行した証明書の信頼性を検証し、信頼する前に、本 CP 及び CPS の内容について理解し、承諾しなければならない。

4.6　証明書の更新

本 CA は私有鍵の変更を伴わない証明書更新は行わない。

4.7　鍵更新を伴う証明書の更新

4.7.1　更新事由

証明書の更新は、証明書の有効期間が満了する場合に行う。

4.7.2　新しい証明書の申請を行うことができる者

「4.1.1.証明書申請を提出することができる者」と同様とする。

4.7.3　更新申請の処理

「4.3.1.証明書発行時の処理手続」と同様とする。

4.7.4　証明書利用者に対する新しい証明書の通知

「4.3.2.証明書利用者への証明書発行通知」と同様とする。

4.7.5　鍵更新された証明書の受領確認手続き

「4.4.1.証明書の受領確認手続」と同様とする。

4.7.6　認証局による鍵更新済みの証明書の公開

「4.4.2.認証局による証明書の公開」と同様とする。

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

「4.4.3.他のエンティティに対する認証局の証明書発行通知」と同様とする。

4.8　証明書の変更

証明書に登録された情報の変更が必要となった場合は、その証明書の失効及び新規発行とする。

4.9　証明書の失効と一時停止

4.9.1　証明書失効事由

証明書利用者は、次の事由が発生した場合、本 CA に対し速やかに証明書の失効申請を行わなければならない。

- 証明書記載情報に変更があった場合
- 私有鍵の盗難、紛失、漏洩、不正利用等により私有鍵が危殆化した又は危殆化のおそれがある場合
- 証明書の内容、利用目的が正しくない場合
- 証明書の利用を中止する場合

また、本 CA は、次の事由が発生した場合に、本 CA の判断により証明書を失効することができる。

- 証明書利用者が本 CP、CPS、関連する契約又は法律に基づく義務を履行していない場合
- 本 CA の私有鍵が危殆化した又は危殆化のおそれがあると判断した場合
- 本 CA が失効を必要とすると判断するその他の状況が認められた場合

4.9.2 証明書失効を申請することができる者

証明書の失効の申請を行うことができる者は、クロストラストが提供する SSL サーバ証明書発行サービスの契約者、又は契約組織の担当者とする。なお、本 CP/CPS「4.9.1. 証明書失効事由」に該当すると本 CA が判断した場合、本 CA が失効申請者となる。

4.9.3 失効申請手続

失効申請者は、本 CP「3.4. 失効申請時の本人性確認と認証」に定める手続きを行うことにより本 CA へ届け出るものとする。

本 CA は、所定の手続によって受け付けた情報を確認し、証明書の失効処理を行う。

4.9.4 失効申請の猶予期間

失効申請者は、私有鍵が危殆化した又は危殆化のおそれがあると判断した場合には、速やかに失効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 CA は、有効な失効申請を受け付けてから速やかに証明書の失効処理を行い、CRL へ当該証明書情報を反映させる。

4.9.6 失効調査の要求

本 CA が発行する証明書には、CRL の格納先である URL を記載する。検証者は、本 CA が発行するの証明書について信頼し、利用する前に、当該証明書の有効性を CRL により確認しなければならない。なお、CRL には、有効期限の切れた証明書情報は含まれない。

4.9.7　証明書失効リストの発行頻度

CRL は、失効処理の有無に関わらず、24 時間ごとに更新を行う。証明書の失効処理が行われた場合は、その時点で CRL の更新を行う。

4.9.8　証明書失効リストの発行最大遅延時間

本 CA は、発行した CRL を即時にリポジトリに反映させる。

4.9.9　オンラインでの失効/ステイタス確認の適用性

オンラインでの証明書ステータス情報は、OCSP サーバを通じて提供される。

4.9.10 オンラインでの失効/ステイタス確認を行うための要件

利用者は本 CA により発行された証明書を信頼し、利用する前に、証明書の有効性を確認しなければならない。リポジトリに掲載している CRL により、証明書の失効登録の有無を確認しない場合には、OCSP サーバにより提供される証明書ステータス情報の確認を行わなければならない。

4.9.11 利用可能な失効情報の他の形式

規定しない。

4.9.12 鍵の危殆化に対する特別要件

規定しない。

4.9.13 証明書の一時停止事由

規定しない。

4.9.14 証明書の一時停止を申請することができる者

規定しない。

4.9.15 証明書の一時停止申請手続

規定しない。

4.9.16 一時停止を継続することができる期間

規定しない。

4.10 証明書のステイタス確認サービス

4.10.1 運用上の特徴

加入者及び利用者は OCSP サーバを通じて証明書ステータス情報を確認することができる。

4.10.2 サービスの利用可能性

本 CA は、24 時間 365 日、証明書ステータス情報を確認できるよう OCSP サーバを管理する。ただし、保守等により、一時的に OCSP サーバを利用できない場合もある。

4.10.3 オプショナルな仕様

規定しない。

4.11 加入（登録）の終了

証明書利用者が本サービスの利用を終了する場合、証明書の失効申請を行わなければならない。または、証明書の更新手続を行わなず、該当する証明書の有効期間が満了した場合に終了となる。

4.12 キーエスクローと鍵回復

4.12.1 キーエスクローと鍵回復ポリシー及び実施

本 CA は、証明書利用者の私有鍵のエスクローは行わない。

4.12.2 セッションキーのカプセル化と鍵回復のポリシー及び実施

規定しない。

5. 設備上、運営上、運用上の管理

5.1 物理的管理

本項については、CPS に規定する。

5.2 手続的管理

本項については、CPS に規定する。

5.3 人事的管理

本項については、CPS に規定する。

5.4 監査ログの手続

本項については、CPS に規定する。

5.5 記録の保管

5.5.1 アーカイブの種類

本 CA は、CPS の「5.5. 記録の保管」に加えて、次の情報をアーカイブとして保存する。

- 本 CP
- 本 CP に基づき作成された認証局の業務運用を規定する文書
- 監査の実施結果に関する記録及び監査報告書
- 証明書利用者からの申請情報及びその処理履歴

5.5.2 アーカイブ保存期間

本項については、CPS に規定する。

5.5.3 アーカイブの保護

本項については、CPS に規定する。

5.5.4 アーカイブのバックアップ手続

本項については、CPS に規定する。

5.5.5　記録にタイムスタンプを付与する要件

本項については、CPS に規定する。

5.5.6　アーカイブ収集システム

本項については、CPS に規定する。

5.5.7　アーカイブの検証手続

本項については、CPS に規定する。

5.6　鍵の切り替え

本 CA の私有鍵は、私有鍵に対する証明書の有効期間が証明書利用者に発行した証明書の最大有効期間よりも短くなる前に新たな私有鍵の生成及び証明書の発行を行う。新しい私有鍵が生成された後は、新しい私有鍵を使って証明書及び CRL の発行を行う。

5.7　危殆化及び災害からの復旧

本項については、CPS に規定する。

5.8　認証局又は登録局の終了

本 CA は、業務停止する必要がある場合、その旨を事前に「9.11.関係者間の個別通知と連絡」に定められた方法で証明書利用者に通知する。

6. 技術的セキュリティ管理

6.1 鍵ペアの生成及びインストール

6.1.1 鍵ペアの生成

本 CA 私有鍵については CPS「6.1.1 鍵ペアの生成」に規定する。
証明書利用者の鍵ペアは、証明書を配置する Web サーバ上で生成する。

6.1.2 証明書利用者に対する私有鍵の交付

証明書利用者の私有鍵は、証明書利用者自身が生成するものとし、本 CA は証明書利用者の私有鍵生成及び交付は行わない。

6.1.3 認証局への公開鍵の交付

本 CA に対する証明書利用者の公開鍵の交付は、証明書の申請時にオンラインによって行われる。この時の通信経路は SSL により暗号化を行う。

6.1.4 信頼者への CA 公開鍵の交付

検証者は、本 CA のリポジトリにアクセスすることによって、本 CA の公開鍵を入手することができる。

6.1.5 鍵サイズ

本 CA の鍵ペアは、RSA 方式で鍵長 2048 ビットとする。
証明書利用者の鍵ペアについては、RSA 方式で鍵長 2048 ビット以上とする。

6.1.6 公開鍵のパラメータの生成及び品質検査

本 CA の公開鍵のパラメータの生成、及びパラメータの強度の検証は、鍵ペア生成に使用される暗号装置に実装された機能を用いて行われる。
証明書利用者の公開鍵のパラメータの生成及び品質検査について規定しない。

6.1.7 鍵の用途

本 CA の証明書の KeyUsage には keyCertSign,、cRLSign のビットを設定する。
本 CA が発行する証明書利用者の証明書の KeyUsage には、digitalSignature, keyEncipherment を設定する。

6.2　私有鍵の保護及び暗号モジュール技術の管理

本項については、CPS に規定する。

6.3　鍵ペアのその他の管理方法

本項については、CPS に規定する。

6.4　活性化データ

本項については、CPS に規定する。

6.5　コンピュータのセキュリティ管理

本項については、CPS に規定する。

6.6　ライフサイクルセキュリティ管理

本項については、CPS に規定する。

6.7　ネットワークセキュリティ管理

本項については、CPS に規定する。

6.8　タイムスタンプ

本項については、CPS に規定する。

7. 証明書及び証明書失効リストのプロファイル

7.1 証明書のプロファイル

本 CA が発行する証明書のプロファイルは、次表のとおりである。

表 1 証明書プロファイル

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		例) 12:34:56:78:90:ab:cd:ef	-
Signature Algorithm		SHA256 with RSAEncryption	-
Issuer	Country	C=JP	-
	Organization	CrossTrust	-
	Common Name	CrossTrust DV CA4	-
Validity	NotBefore	例）2017/12/01 00:00:00 GMT	-
	NotAfter	例）2019/12/01 00:00:00 GMT	-
Subject	Country	JP	-
	stateOrProvinceName	記載しない	-
	Locality	記載しない	-
	Organization	記載しない	-
	Organizational Unit	記載しない	-
	Common Name	任意	-
Subject Public Key Info		主体者の公開鍵データ	-
拡張領域		設定内容	critical
ExtendedKeyUsage		TLS Web Server Authentication	n
Authority Key Identifier		発行者公開鍵の SHA-1 ハッシュ値（160 ビット）	n
CRL Distribution Points		URL=http://crl.crosstrust.net/sppca/xt/dvca4.crl	n
KeyUsage		digitalSignature, keyEncipherment	y
Subject Key Identifier		主体者公開鍵の SHA-1 ハッシュ値（160 ビット）	n

CertificatePolicies	[1]policyIdentifier OID=1.2.392.200220.1.8 policyQualifiers policyQualifierId=CPS qualifiier=https://repository.crosstrust.net/cps/ [2]policyIdentifier=2.23.140.1.2.1	n
Authority Information Access	accessMethod: OCSP URI: http://dvca4.ocsp.crosstrust.net	n
Subject Alt Name	dNSName iPAddress	n
Certificate Transparency 用拡張 (1.3.6.1.4.1.11129.2.4.2)	SignedCertificateTimestampList の値	n

7.2 CRL のプロファイル

本 CA が発行する CRL のプロファイルは、次表のとおりである。

表 2 CRL プロファイル

基本領域		設定内容	critical
Version		Version 2	-
Signature Algorithm		SHA256 with RSAEncryption	-
Issuer	Country	C=JP	-
	Organization	CrossTrust	-
	Common Name	CrossTrust DV CA4	-
This Update		例) 2014/12/01 00:00:00 GMT	-
Next Update		例) 2014/12/01 00:00:00 GMT 更新間隔=24H、有効期間=96H とする	-
Revoked Certificates	Serial Number	例) 1234567890	-
	Revocation Date	例) 2014/12/01 00:00:00 GMT	-
	Reason Code	失効事由（unspecifiled, Key Compromise, Affiliation Changed, superseded, cessation of operation）	-
拡張領域		設定内容	critical
CRL Number		CRL 番号	n
Authority Key Identifier		発行者公開鍵の SHA-1 ハッシュ値（160 ビット）	n

7.3 OCSP のプロファイル

本 CA は、RFC5019、6960 に準拠する OCSP サーバを提供する。

7.3.1　バージョン番号

本 CA は、OCSP バージョン 1 を適用する。

7.3.2　OCSP 拡張

規定しない。

8.　準拠性監査と他の評価

8.1　監査の頻度

本 CA は、本 CA の運用が本 CP に準拠して行われているかについて、定期的に監査を行う。

8.2　監査者の身元／資格

準拠性監査は、十分な監査経験を有する監査人が行う。

8.3　監査者と被監査者の関係

監査人は、監査に関する事項を除き、被監査部門の業務から独立した立場にあるものとする。

8.4　監査で扱われる事項

監査は、本 CA の運用の本 CP に対する準拠性を中心として行う。

8.5　不備の結果としてとられる処置

本 CA は、監査報告書で指摘された事項に関し、速やかに必要な是正措置を行う。

8.6　監査結果の開示

監査結果は、監査人から本 CA に対して報告される。
本 CA は、法律に基づく開示要求があった場合、当社との契約に基づき関係組織から

の開示要求があった場合、又は本 CA の意思決定組織が承認した場合を除き、監査結果を外部へ開示することはない。

9. 他の業務上及び法的事項

9.1 料金

規定しない。

9.2 財務的責任

本 CA は、電子認証基盤の運用維持にあたり、十分な財務的基盤を維持するものとする。

9.3 企業情報の機密性

9.3.1 機密情報の範囲

本 CA が保持する個人情報及び組織情報は証明書、CRL、本 CP 及び CPS の一部として明示的に公開されたものを除き、機密保持対象として扱う。

9.3.2 機密情報の範囲外の情報

証明書及び CRL に含まれている情報は機密保持対象外として扱う。その他、次の状況におかれた情報は機密保持対象外とする。

- 本 CA の過失によらず知られた、あるいは知られるようになった情報
- 本 CA 以外の出所から、機密保持の制限無しに本 CA に知られた、あるいは知られるようになった情報
- 本 CA によって独自に開発された情報
- 開示に関して証明書利用者によって承認されている情報

9.3.3 機密情報を保護する責任

本 CA は、法の定めによる場合、機密情報を開示することがある。その際、その情報を知り得た者は、契約あるいは法的な制約によりその情報を第三者に開示させない。

9.4 個人情報の保護

本 CA の個人情報保護方針については、クロストラストのホームページにて公表する。

9.5　知的財産権

本 CP は著作権を含み、クロストラストの権利に属するものとする。

9.6　表明保証

9.6.1　認証局の表明保証

9.6.1.1　IA の表明保証

本 CA は、IA の業務を遂行するにあたり次の義務を負う。

- CA 私有鍵のセキュアな生成・管理
- RA からの申請に基づいた証明書の正確な発行・失効管理
- IA のシステム稼動の監視・運用
- CRL の発行・公表

9.6.1.2　RA の表明保証

本 CA は、RA の業務を遂行するにあたり次の義務を負う。

- 登録端末のセキュアな環境への設置・運用
- 証明書発行・失効申請における IA への正確な情報伝達
- 証明書失効申請における IA への運用時間中の速やかな情報伝達
- リポジトリの維持管理

9.6.2　証明書利用者の表明保証

証明書利用者は、本 CP に定める諸事項を遵守することについて保証するものとする。また、証明書利用者は、本 CP に遵守しない場合、すべての責任を有するものとする。

9.6.3　検証者の表明保証

検証者は、本 CP に定める諸事項を遵守することについて保証するものとする。また、検証者は、本 CP に遵守しない場合、すべての責任を有するものとする。

9.6.4　他の関係者の表明保証

規定しない。

9.7　無保証

本 CA は、本 CP「9.6.1 認証局の表明保証」に規定する保証に関連して発生するいかなる間接損害、特別損害、付随的損害又は派生的損害に対する責任を負わず、また、い

かなる逸失利益、データの紛失又はその他の間接的若しくは派生的損害に対する責任を負わない。

9.8　責任の制限

本 CP「9.6.1 認証局の表明保証」の内容に関し、次の場合、本 CA は責任を負わないものとする。

- 本 CA に起因しない不法行為、不正使用又は過失等により発生する一切の損害
- 証明書利用者が自己の義務の履行を怠ったために生じた損害
- 証明書利用者のシステムに起因して発生した一切の損害
- 本 CA、証明書利用者のハードウェア、ソフトウェアの瑕疵、不具合あるいはその他の動作自体によって生じた損害
- 証明書利用者が契約に基づく契約料金を支払っていない間に生じた損害
- 本 CA の責に帰することのできない事由で証明書及び CRL に公開された情報に起因する損害
- 本 CA の責に帰することのできない事由で正常な通信が行われない状態で生じた一切の損害
- 証明書の使用に関して発生する取引上の債務等、一切の損害
- 現時点の予想を超えた、ハードウェア的あるいはソフトウェア的な暗号アルゴリズム解読技術の向上に起因する損害
- 天変地異、地震、噴火、火災、津波、水災、落雷、戦争、動乱、テロリズムその他の不可抗力に起因する、本 CA の業務停止に起因する一切の損害

9.9　補償

本 CA が発行する証明書を申請、受領、信頼した時点で、証明書利用者には、本 CA 及び関連する組織等に対する損害賠償責任及び保護責任が発生するものとする。当該責任の対象となる事象には、損失、損害、訴訟、あらゆる種類の費用負担の原因となるようなミス、怠慢な行為、各種行為、履行遅滞、不履行等の各種責任が含まれる。

9.10 有効期間と終了

9.10.1 有効期間

本 CP は、本 CA の意思決定組織の承認により有効となる。

9.10.2 終了

本 CP は、本 CA の終了と同時に無効となる。

9.10.3 終了の効果と効果継続

証明書利用者と本 CA との間で利用契約等を終了する場合、又は、本 CA 自体を終了する場合であっても、その性質上存続されるべき条項は終了の事由を問わず証明書利用者及び本 CA に適用されるものとする。

9.11 関係者間の個別通知と連絡

本 CA は、証明書利用者に対する必要な通知をホームページ上、電子メール又は書面等によって行う。

9.12 改訂

9.12.1 改訂手続

本 CP は、本 CA の判断によって適宜改訂され、本 CA の意思決定組織の承認によって発効する。

9.12.2 通知方法及び期間

本 CP を変更した場合、速やかに変更した本 CP を公表することにより、証明書利用者に対しての告知とする。証明書利用者は告知日から一週間の間、異議を申し立てることができ、異議申し立てがない場合、変更された本 CP は証明書利用者に同意されたものとみなす。

9.12.3 オブジェクト識別子が変更されなければならない場合

規定しない。

9.13 紛争解決手続

証明書の利用に関し、本 CA に対して訴訟、仲裁を含む解決手段に訴えようとする場合、本 CA に対して事前にその旨を通知するものとする。なお、仲裁及び裁判地は東京都内における紛争処理機関を専属的管轄とする。

9.14 準拠法

本 CA、証明書利用者の所在地にかかわらず、本 CP の解釈、有効性及び証明書の利

用にかかわる紛争については、日本国の法律が適用されるものとする。

9.15 適用法の遵守

規定しない。

9.16 雑則

規定しない。

9.17 その他の条項

規定しない。