

ドメイン認証 証明書ポリシー  
(Certificate Policy)

Version 1.10

2018 年 10 月 12 日

セコムトラストシステムズ株式会社

| 改版履歴 |            |             |
|------|------------|-------------|
| 版数   | 日付         | 内容          |
| 1.00 | 2018/07/24 | 初版発行        |
| 1.10 | 2018/10/12 | プロフィールの内容変更 |

## 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 CA .....               | 2  |
| 1.3.2 RA .....               | 2  |
| 1.3.3 管理者 .....              | 2  |
| 1.3.3.1 証明書利用者 .....         | 2  |
| 1.3.3.2 証明書管理者 .....         | 3  |
| 1.3.4 検証者 .....              | 3  |
| 1.3.5 その他の関係者 .....          | 3  |
| 1.4 証明書の用途.....              | 3  |
| 1.4.1 適切な証明書の用途 .....        | 3  |
| 1.4.2 禁止される証明書の用途.....       | 3  |
| 1.5 ポリシー管理.....              | 3  |
| 1.5.1 文書を管理する組織 .....        | 3  |
| 1.5.2 連絡先.....               | 3  |
| 1.5.3 ポリシー適合性を決定する者 .....    | 4  |
| 1.5.4 承認手続 .....             | 4  |
| 1.6 定義と略語 .....              | 5  |
| 2. 公開とリポジトリの責任 .....         | 9  |
| 2.1 リポジトリ.....               | 9  |
| 2.2 証明情報の公開 .....            | 9  |
| 2.3 公開の時期または頻度 .....         | 9  |
| 2.4 リポジトリへのアクセス管理 .....      | 9  |
| 3. 識別と認証.....                | 10 |
| 3.1 名前決定.....                | 10 |
| 3.1.1 名前の種類.....             | 10 |
| 3.1.2 名前が意味を持つことの必要性.....    | 10 |
| 3.1.3 証明書利用者の匿名性または仮名性 ..... | 10 |
| 3.1.4 様々な名前形式を解釈するための規則..... | 10 |
| 3.1.5 名前の一意性.....            | 10 |
| 3.1.6 認識、認証および商標の役割 .....    | 10 |
| 3.2 初回の本人確認.....             | 10 |
| 3.2.1 秘密鍵の所持を証明する方法 .....    | 10 |

|                                     |    |
|-------------------------------------|----|
| 3.2.2 組織の認証.....                    | 11 |
| 3.2.3 個人の認証.....                    | 11 |
| 3.2.4 検証されない証明書利用者の情報 .....         | 11 |
| 3.2.5 権限の正当性確認.....                 | 11 |
| 3.2.6 相互運用の基準 .....                 | 11 |
| 3.2.7 ドメインの認証 .....                 | 11 |
| 3.3 鍵更新申請時の本人性確認と認証.....            | 12 |
| 3.3.1 通常の鍵更新時における本人性確認と認証 .....     | 12 |
| 3.3.2 証明書失効後の鍵更新時における本人性確認と認証 ..... | 12 |
| 3.4 失効申請時の本人性確認と認証 .....            | 12 |
| 4. 証明書のライフサイクルに対する運用上の要件.....       | 13 |
| 4.1 証明書申請 .....                     | 13 |
| 4.1.1 証明書の申請を行うことができる者 .....        | 13 |
| 4.1.2 申請手続および責任 .....               | 13 |
| 4.2 証明書申請手続.....                    | 13 |
| 4.2.1 本人性確認と認証の実施.....              | 13 |
| 4.2.2 証明書申請の承認または却下 .....           | 13 |
| 4.2.3 証明書申請の処理時間 .....              | 13 |
| 4.2.4 CAA レコードの確認 .....             | 13 |
| 4.3 証明書の発行.....                     | 14 |
| 4.3.1 証明書発行時の処理手続.....              | 14 |
| 4.3.2 証明書利用者への証明書発行通知 .....         | 14 |
| 4.4 証明書の受領確認 .....                  | 14 |
| 4.4.1 証明書の受領確認手続 .....              | 14 |
| 4.4.2 認証局による証明書の公開 .....            | 14 |
| 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 ..... | 14 |
| 4.5 鍵ペアおよび証明書の用途.....               | 14 |
| 4.5.1 証明書利用者の秘密鍵および証明書の用途 .....     | 14 |
| 4.5.2 検証者の公開鍵および証明書の用途 .....        | 14 |
| 4.6 証明書の更新.....                     | 15 |
| 4.6.1 証明書の更新事由.....                 | 15 |
| 4.6.2 証明書の更新申請を行うことができる者 .....      | 15 |
| 4.6.3 証明書の更新申請の処理手続 .....           | 15 |
| 4.6.4 証明書利用者に対する新しい証明書発行通知.....     | 15 |
| 4.6.5 更新された証明書の受領確認手続 .....         | 15 |
| 4.6.6 認証局による更新された証明書の公開.....        | 15 |

|                                        |    |
|----------------------------------------|----|
| 4.6.7 他のエンティティに対する認証局の証明書発行通知 .....    | 15 |
| 4.7 鍵更新を伴う証明書の更新.....                  | 15 |
| 4.7.1 更新事由 .....                       | 15 |
| 4.7.2 新しい証明書の申請を行うことができる者 .....        | 15 |
| 4.7.3 更新申請の処理手続.....                   | 16 |
| 4.7.4 証明書利用者に対する新しい証明書の通知 .....        | 16 |
| 4.7.5 鍵更新された証明書の受領確認手続 .....           | 16 |
| 4.7.6 認証局による鍵更新済みの証明書の公開.....          | 16 |
| 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.....     | 16 |
| 4.8 証明書の変更.....                        | 16 |
| 4.8.1 証明書の変更事由.....                    | 16 |
| 4.8.2 証明書の変更申請を行うことができる者 .....         | 16 |
| 4.8.3 変更申請の処理手続.....                   | 16 |
| 4.8.4 証明書利用者に対する新しい証明書発行通知.....        | 16 |
| 4.8.5 変更された証明書の受領確認手続 .....            | 16 |
| 4.8.6 認証局による変更された証明書の公開.....           | 16 |
| 4.8.7 他のエンティティに対する認証局の証明書発行通知.....     | 17 |
| 4.9 証明書の失効と一時停止 .....                  | 17 |
| 4.9.1 証明書失効事由 .....                    | 17 |
| 4.9.2 証明書の失効申請を行うことができる者 .....         | 18 |
| 4.9.3 失効申請手続.....                      | 18 |
| 4.9.4 失効申請の猶予期間.....                   | 18 |
| 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.....      | 18 |
| 4.9.6 失効確認の要求 .....                    | 18 |
| 4.9.7 証明書失効リストの発行頻度 .....              | 18 |
| 4.9.8 証明書失効リストの発行最大遅延時間.....           | 18 |
| 4.9.9 オンラインでの失効/ステータス確認の適用性.....       | 18 |
| 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 ..... | 19 |
| 4.9.11 利用可能な失効情報の他の形式.....             | 19 |
| 4.9.12 鍵の危殆化に対する特別要件 .....             | 19 |
| 4.9.13 証明書の一時停止事由 .....                | 19 |
| 4.9.14 証明書の一時停止申請を行うことができる者.....       | 19 |
| 4.9.15 証明書の一時停止申請手続.....               | 19 |
| 4.9.16 一時停止を継続することができる期間.....          | 19 |
| 4.10 証明書のステータス確認サービス.....              | 19 |
| 4.10.1 運用上の特徴.....                     | 19 |

|                                           |    |
|-------------------------------------------|----|
| 4.10.2 サービスの利用可能性 .....                   | 19 |
| 4.10.3 オプショナルな仕様 .....                    | 19 |
| 4.11 加入（登録）の終了 .....                      | 20 |
| 4.12 キーエスクローと鍵回復 .....                    | 20 |
| 4.12.1 キーエスクローと鍵回復ポリシーおよび実施 .....         | 20 |
| 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および実施 .....  | 20 |
| 5. 設備上、運営上、運用上の管理 .....                   | 21 |
| 5.1 物理的管理 .....                           | 21 |
| 5.2 手続的管理 .....                           | 21 |
| 5.3 人事的管理 .....                           | 21 |
| 5.4 監査ログの手続 .....                         | 21 |
| 5.5 記録の保管 .....                           | 21 |
| 5.5.1 アーカイブの種類 .....                      | 21 |
| 5.5.2 アーカイブ保存期間 .....                     | 21 |
| 5.5.3 アーカイブの保護 .....                      | 21 |
| 5.5.4 アーカイブのバックアップ手続 .....                | 22 |
| 5.5.5 記録にタイムスタンプを付与する要件 .....             | 22 |
| 5.5.6 アーカイブ収集システム .....                   | 22 |
| 5.5.7 アーカイブの検証手続 .....                    | 22 |
| 5.6 鍵の切り替え .....                          | 22 |
| 5.7 危殆化および災害からの復旧 .....                   | 22 |
| 5.7.1 事故および危殆化時の手続 .....                  | 22 |
| 5.7.2 ハードウェア、ソフトウェアまたはデータが破損した場合の手続 ..... | 22 |
| 5.7.3 秘密鍵が危殆化した場合の手続 .....                | 23 |
| 5.7.4 災害後の事業継続性 .....                     | 23 |
| 5.8 認証局または登録局の終了 .....                    | 23 |
| 6. 技術的セキュリティ管理 .....                      | 24 |
| 6.1 鍵ペアの生成およびインストール .....                 | 24 |
| 6.1.1 鍵ペアの生成 .....                        | 24 |
| 6.1.2 証明書利用者に対する秘密鍵の交付 .....              | 24 |
| 6.1.3 認証局への公開鍵の交付 .....                   | 24 |
| 6.1.4 検証者への CA 公開鍵の交付 .....               | 24 |
| 6.1.5 鍵サイズ .....                          | 24 |
| 6.1.6 公開鍵のパラメーターの生成および品質検査 .....          | 24 |
| 6.1.7 鍵の用途 .....                          | 24 |
| 6.2 秘密鍵の保護および暗号装置技術の管理 .....              | 25 |

|                                          |    |
|------------------------------------------|----|
| 6.2.1 暗号装置の標準および管理 .....                 | 25 |
| 6.2.2 秘密鍵の複数人管理 .....                    | 25 |
| 6.2.3 秘密鍵のエスクロー .....                    | 25 |
| 6.2.4 秘密鍵のバックアップ .....                   | 25 |
| 6.2.5 秘密鍵のアーカイブ .....                    | 25 |
| 6.2.6 秘密鍵の暗号モジュールへのまたは暗号モジュールからの転送 ..... | 25 |
| 6.2.7 暗号装置への秘密鍵の格納 .....                 | 26 |
| 6.2.8 秘密鍵の活性化方法 .....                    | 26 |
| 6.2.9 秘密鍵の非活性化方法 .....                   | 26 |
| 6.2.10 秘密鍵の破棄方法 .....                    | 26 |
| 6.2.11 暗号装置の評価 .....                     | 26 |
| 6.3 鍵ペアのその他の管理方法 .....                   | 26 |
| 6.3.1 公開鍵のアーカイブ .....                    | 26 |
| 6.3.2 秘密鍵および公開鍵の有効期間 .....               | 26 |
| 6.4 活性化データ .....                         | 26 |
| 6.5 コンピュータのセキュリティ管理 .....                | 27 |
| 6.6 ライフサイクルセキュリティ管理 .....                | 27 |
| 6.7 ネットワークセキュリティ管理 .....                 | 27 |
| 6.8 タイムスタンプ .....                        | 27 |
| 7. 証明書および証明書失効リストおよび OCSP のプロファイル .....  | 28 |
| 7.1 証明書のプロファイル .....                     | 28 |
| 7.2 CRL のプロファイル .....                    | 30 |
| 7.3 OCSP のプロファイル .....                   | 30 |
| 7.3.1 バージョン番号 .....                      | 30 |
| 7.3.2 OCSP 拡張 .....                      | 30 |
| 8. 準拠性監査と他の評価 .....                      | 31 |
| 8.1 監査の頻度 .....                          | 31 |
| 8.2 監査人の身元／資格 .....                      | 31 |
| 8.3 監査人と被監査部門の関係 .....                   | 31 |
| 8.4 監査で扱われる事項 .....                      | 31 |
| 8.5 不備の結果としてとられる処置 .....                 | 31 |
| 8.6 監査結果の開示 .....                        | 31 |
| 9. 他の業務上および法的事項 .....                    | 32 |
| 9.1 料金 .....                             | 32 |
| 9.2 財務的責任 .....                          | 32 |
| 9.3 企業情報の機密性 .....                       | 32 |

|                                       |    |
|---------------------------------------|----|
| 9.4 個人情報の保護.....                      | 32 |
| 9.5 知的財産権 .....                       | 32 |
| 9.6 表明保証.....                         | 32 |
| 9.6.1 認証局の表明保証.....                   | 32 |
| 9.6.1.1 IA の表明保証.....                 | 32 |
| 9.6.1.2 RA の表明保証 .....                | 32 |
| 9.6.2 証明書利用者の表明保証.....                | 33 |
| 9.6.3 検証者の表明保証.....                   | 33 |
| 9.6.4 他の関係者の表明保証 .....                | 33 |
| 9.7 無保証 .....                         | 33 |
| 9.8 責任の制限 .....                       | 33 |
| 9.9 補償 .....                          | 34 |
| 9.10 有効期間と終了.....                     | 34 |
| 9.10.1 有効期間 .....                     | 34 |
| 9.10.2 終了 .....                       | 34 |
| 9.10.3 終了の効果と効果継続 .....               | 34 |
| 9.11 関係者間の個別通知と連絡.....                | 34 |
| 9.12 改訂 .....                         | 35 |
| 9.12.1 改訂手続 .....                     | 35 |
| 9.12.2 通知方法および期間.....                 | 35 |
| 9.12.3 オブジェクト識別子を変更されなければならない場合 ..... | 35 |
| 9.13 紛争解決手続.....                      | 35 |
| 9.14 準拠法 .....                        | 35 |
| 9.15 適用法の遵守.....                      | 35 |
| 9.16 雑則 .....                         | 35 |
| 9.16.1 完全合意条項.....                    | 35 |
| 9.16.2 権利譲渡条項.....                    | 35 |
| 9.16.3 分離条項 .....                     | 36 |
| 9.16.4 強制執行条項.....                    | 36 |
| 9.17 その他の条項.....                      | 36 |

## 1. はじめに

### 1.1 概要

ドメイン認証 証明書ポリシー（以下「本 CP」という）は、セコムトラストシステムズ株式会社（以下「当社」という）が運用する SC Domain Validation CA（以下「本 CA」という）が発行する証明書の利用目的、適用範囲、利用者手続を示し、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、セコム電子認証基盤認証運用規程（以下「CPS」という）に規定する。

本 CA は、Security Communication RootCA2 より、片方向相互認証証明書の発行を受けている。

本 CA が発行する証明書は、サーバー認証や、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 および CPS とを照らし合わせて評価し、承諾する必要がある。

本 CA は、<https://www.cabforum.org/>で公開される CA/ Browser Forum の Baseline Requirements（以下「BR」という）に準拠する。

本 CA から発行する証明書は、証明書の管理者が運営するサービス（以下「認証サービス」という）で提供され、二社間の契約については PB-SSL/TLS 証明書発行サービス約款（以下「当約款」という）に定めるものとする。

なお、本 CP の内容が当約款、CPS の内容に抵触する場合は、当約款、本 CP、CPS の順に優先して適用されるものとする。また、当社と契約関係を持つ組織団体等との間で、別途契約書等が存在する場合、当約款、本 CP、CPS より契約書等の文書が優先される。

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。

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。

### 1.2 文書名と識別

本 CP の正式名称は、「ドメイン認証 証明書ポリシー」という。

本 CP は、表「1.2-1 OID（本 CP）」に示す OID により識別される。

表 1.2-1 OID（本 CP）

| CP                       | OID                      |
|--------------------------|--------------------------|
| SC Domain Validation CA1 | 1.2.392.200091.110.213.1 |
| SC Domain Validation CA2 | 1.2.392.200091.110.213.2 |
| SC Domain Validation CA3 | 1.2.392.200091.110.213.3 |

本 CP に関連する CPS の OID を表「1.2-2 OID（CPS）」に示す。

表 1.2-2 OID（CPS）

| 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 CA

CA（Certification Authority：認証局）は、IA および RA によって構成される。電子認証基盤上で運用される CA の運営主体は当社である。

IA は、証明書の発行、失効、CRL（Certificate Revocation List：証明書失効リスト）の開示、OCSP（Online Certificate Status Protocol）による証明書ステータス情報の提供などを行う。

#### 1.3.2 RA

RA は、CA の業務のうち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。

証明書申請を受け、内容の審査、および証明書発行、失効するための登録業務等を行い、また、証明書発行の承認または却下、証明書の失効要求を受けた場合は承認を行う。

#### 1.3.3 管理者

管理者とは、本 CA から発行された証明書を利用する証明書利用者と、証明書の発行のため本 CA と契約した証明書管理者の両方を指すものとする。

##### 1.3.3.1 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、その他の組織とする。

#### 1.3.3.2 証明書管理者

証明書管理者とは、本 CA と契約関係がある組織であり、認証サービスを運営し発行された証明書を証明書利用者へ提供する事業者のことをいう。

本 CP のすべての要件および契約条件を遵守しなければならず、本 CA から指示する運用および技術的な実装に関して受け入れ、実施するものとする。

#### 1.3.4 検証者

検証者とは、証明書利用者の身元と公開鍵の有効性を検証する個人、法人その他の組織をいう。また、かかる公開鍵を使って証明書利用者が所有する Web サーバーとの間で暗号化通信を行う目的で、CP、CPS を信頼し、利用する個人、法人その他の組織をいう。

#### 1.3.5 その他の関係者

規定しない。

### 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、サーバー認証や通信経路でデータの暗号化を行うことに利用することができる。

#### 1.4.2 禁止される証明書の用途

本 CA が発行する証明書は、サーバー認証や通信経路でデータの暗号化を行うこと以外に証明書を利用してはならない。

### 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、当社が行う。

#### 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：セコムトラストシステムズ株式会社 CA サポートセンター

住所：〒181-8528 東京都三鷹市下連雀 8-10-16

電子メールアドレス : [ca-support@secom.co.jp](mailto:ca-support@secom.co.jp)

#### 1.5.3 ポリシー適合性を決定する者

本 CP の内容については、認証サービス改善委員会（以下「本委員会」という）が適合性を決定する。

#### 1.5.4 承認手続

本CPは、本CAの本委員会の承認によって発効する。

## 1.6 定義と略語

あ〜ん

### アーカイブ

法的また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、秘密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、秘密鍵に対応し、通信相手の相手方に公開される鍵のことをいう。

### 秘密鍵

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。「私有鍵」ともいう。

### 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 証明書および CRL 等を格納し公表するデータベースのことをいう。

A～Z

### Baseline Requirements

CA/Browser Forum が証明書の発行・管理に関する基本要件を定めた文書のことをいう。

### CA (Certification Authority) : 認証局

証明書の発行・更新・失効、CA 秘密鍵の生成・保護およ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 Authorization)

ドメインを使用する権限において、DNS レコードの中にドメインに対して証明書を発行できる認証局情報を記述し、意図しない認証局からの証明書誤発行を防ぐ機能をいう。

### CA/Browser Forum

認証局とインターネット・ブラウザベンダによって組織され、証明書の要件を定義し、標準化する活動をしている非営利団体組織である。

### 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) : 認証運用規程

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、秘密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。

### CT (Certificate Transparency)

RFC 6962 で規定され、発行された証明書の情報を監視・監査するためにログサーバーに証明書の情報を登録し、公開する仕組みのことをいう。

### 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。最低レベル 1 から最高レベル 4 まで定義

されている。

IA (Issuing Authority) : 発行局

CA の業務のうち、証明書の発行・更新・失効、CA 秘密鍵の生成・保護等を行う主体のことをいう。

INAN(Internet Assigned Numbers Authority)

IP アドレスやポート番号など、インターネットに関連する情報をグローバルに管理している団体のことをいう。

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。

OCSP (Online Certificate Status Protocol)

証明書のステータス情報をリアルタイムに提供するプロトコルのことをいう。

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、リポジトリの維持・管理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。

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 (Secure Hash Algorithm 1)

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。ビット長は160ビット。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。

#### SHA-256 (Secure Hash Algorithm 256)

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。ビット長は256ビット。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。

#### WebTrust for CA

米国公認会計士協会（AICPA）とカナダ勅許会計士協会（CICA）によって、認証局の信頼性、および、電子商取引の安全性等に関する内部統制について策定された基準およびその基準に対する認定制度である。

#### WebTrust for Baseline Requirements

米国公認会計士協会（AICPA）とカナダ勅許会計士協会（CICA）によって、認証局がSSL 証明書を発行するにあたっての審査、証明書に関する規定について策定された監査基準である。

#### WHOIS

IP アドレスやドメイン名の登録者などに関する情報を、インターネット上で参照できるサービスのことをいう。

#### X.500

ネットワーク上での分散ディレクトリサービスに関する、コンピュータネットワーク標準規格のシリーズのことをいう。

## 2. 公開とリポジトリの責任

### 2.1 リポジトリ

本 CA は、証明書利用者および検証者が CRL 情報を 24 時間 365 日利用できるようリポジトリを維持管理する。ただし、保守等により、一時的にリポジトリおよび OCSP を利用できない場合もある。

### 2.2 証明情報の公開

本 CA は、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参照できるようにする。

### 2.3 公開の時期または頻度

本 CP および CPS は、変更の都度、リポジトリに公開される。CRL は、本 CP に従って処理された失効情報を含み、発行の都度、リポジトリに公開される。

### 2.4 リポジトリへのアクセス管理

証明書利用者および検証者は、随時、リポジトリを参照できる。リポジトリへのアクセスに用いるプロトコルは、HTTP (HyperText Transfer Protocol)、HTTPS (HTTP に SSL によるデータの暗号化機能を付加したプロトコル) とする。リポジトリの情報は一般的な Web インターフェースを通じてアクセス可能である。

### 3. 識別と認証

#### 3.1 名前決定

##### 3.1.1 名前の種類

証明書に記載される証明書発行者である本 CA の名前と発行対象である証明書利用者の名前は、X.500 の識別名 (DN : Distinguished Name) 形式に従い設定する。

##### 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 Web サーバーの 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または仮名性

本 CA が発行する証明書コモンネームには、匿名や仮名での登録は行わない。

##### 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)の属性は、発行対象となる Web サーバーに対して一意なものとする。

##### 3.1.6 認識、認証および商標の役割

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 秘密鍵の所持を証明する方法

証明書利用者が秘密鍵を所有していることの証明は、次の方法で行う。

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、公開鍵に対応する秘密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、個人の実在性を確認しない。

証明書管理者は、証明書の申請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、本人性の確認や申込の意思確認などを行う。

### 3.2.4 検証されない証明書利用者の情報

規定しない。

### 3.2.5 権限の正当性確認

本 CA は、証明書に記載されるドメイン名の管理者より、証明書利用者が利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、Security Communication RootCA2 より、片方向相互認証証明書を発行されている。

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

IP アドレスにおいては、証明書利用者が IP アドレスの使用权を有しているかを確認するため、次の方法で認証を行う。

1. IP アドレスを含む統一されたリソース識別子によって識別されるオンライン Web ペ

ージ上の情報に合意した変更を加えることにより、IP アドレスに対する実用的な制御を実証する。

2. IANA (Internet Assigned Numbers Authority) または Regional Internet Registry (RIPE、APNIC、ARIN、AfriNIC、LACNIC) から IP アドレス割り当てに関する情報を取得し記録する。
3. 逆 IP アドレス検索を実行し、結果のドメイン名に対する制御を検証する。
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

#### 3.3.1 通常の鍵更新時における本人性確認と認証

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

#### 3.3.2 証明書失効後の鍵更新時における本人性確認と認証

失効した証明書の更新は行わない。証明書申請は新規扱いとし、証明書利用者の本人性確認および認証は、「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、証明書利用者または申請者から所定の手続きにより失効申請を受け付ける、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 証明書の申請を行うことができる者

証明書の申請を行うことのできる者は、証明書を利用する会社、その他の法人、その他法人の代表者から委任された代理人（以下「申請者」という）とする。

###### 4.1.2 申請手続および責任

証明書利用者および申請者は、証明書の申請を行うにあたり、本 CP および 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

証明書利用者または申請者は、証明書管理者が提供する認証サービスをとおして証明書の申請をする。

###### 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 証明書申請の承認または却下

本 CA は、審査の結果、承認を行った申請について証明書の発行を行い、証明書管理者は、証明書利用者に審査終了および証明書発行について通知する。また、すべての項目の審査が正常に完了しない証明書の申請を却下できるものとするのとし、以下理由を含むものは却下とする。

- ・以前に拒否された、または以前に契約の条項に違反していた申請者または証明書利用者の証明書。
- ・内部のサーバー名または予約済みの IP アドレス

本CAは、不備がある申請については証明書管理者へ通知する。証明書管理者は申請を却下し、申請を行った者に対し再申請を依頼する。

###### 4.2.3 証明書申請の処理時間

本 CA は、承認を行った証明書申請についてすみやかに証明書の発行を行う。

###### 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「secomtrust.net」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、証明書申請の審査終了後に証明書発行を行い、証明書管理者は証明書利用者だけがアクセス可能なホームページ、メール送付、または郵送にて証明書を証明書利用者に対して送付する。

##### 4.3.2 証明書利用者への証明書発行通知

証明書利用者に対し、証明書管理者は証明書利用者だけがアクセス可能なホームページ、メール送付、または郵送で証明書を送付することで発行通知とする。

#### 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をダウンロードしたことをもって、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ー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 および証明書管理者は、証明書申請時に登録された担当者以外への証明書発行通知は行わない。

#### 4.5 鍵ペアおよび証明書の用途

##### 4.5.1 証明書利用者の秘密鍵および証明書の用途

証明書利用者は、秘密鍵および証明書の用途として、サーバー認証や通信経路で情報の暗号化を行うことに利用する。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および対応する秘密鍵を利用するものとする。その他の用途に利用してはならない。

##### 4.5.2 検証者の公開鍵および証明書の用途

検証者は、本 CP および CPS の内容について理解し、承諾したうえで、本 CA の証明書

を使用するものとする。

検証者は本 CA の証明書を使用して、証明書利用者の証明書を検証する事ができる。

#### 4.6 証明書の更新

本 CA は、証明書利用者が証明書を更新する場合、新たな鍵ペアを生成すること推奨する。

##### 4.6.1 証明書の更新事由

鍵更新を伴わない証明書の更新は、証明書の有効期間が満了する場合に行う。

##### 4.6.2 証明書の更新申請を行うことができる者

「4.1.1.証明書の申請を行うことができる者」と同様とする。

##### 4.6.3 証明書の更新申請の処理手続

「4.3.1.証明書発行時の処理手続」と同様とする。

##### 4.6.4 証明書利用者に対する新しい証明書発行通知

「4.3.2.証明書利用者への証明書発行通知」と同様とする。

##### 4.6.5 更新された証明書の受領確認手続

「4.4.1.証明書の受領確認手続」と同様とする。

##### 4.6.6 認証局による更新された証明書の公開

「4.4.2.認証局による証明書の公開」と同様とする。

##### 4.6.7 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。

#### 4.7 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ことができる。失効した証明書または有効期限が切れた証明書は更新できない。

##### 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.証明書の申請を行うことができる者」と同様とする。

#### 4.7.3 更新申請の処理手続

「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

「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

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

#### 4.8.1 証明書の変更事由

規定しない。

#### 4.8.2 証明書の変更申請を行うことができる者

「4.1.1.証明書の申請を行うことができる者」と同様とする。

#### 4.8.3 変更申請の処理手続

「4.3.1.証明書発行時の処理手続」と同様とする。

#### 4.8.4 証明書利用者に対する新しい証明書発行通知

「4.3.2.証明書利用者への証明書発行通知」と同様とする。

#### 4.8.5 変更された証明書の受領確認手続

「4.4.1.証明書の受領確認手続」と同様とする。

#### 4.8.6 認証局による変更された証明書の公開

「4.4.2.認証局による証明書の公開」と同様とする。

#### 4.8.7 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。

### 4.9 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、証明書管理者に対しすみ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
- ・ 秘密鍵の盗難、紛失、漏洩、不正利用等により秘密鍵が危殆化したまた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利用者の証明書を失効することができる。

- ・ 本 CP、CPS、関連する契約または法律に基づく義務を履行していない場合
- ・ 本 CA の秘密鍵が危殆化した、または危殆化のおそれがあると判断した場合
- ・ 本 CA が、証明書に記載されている情報のいずれかに不適切な文字列や記号を使用、不正確または誤解を招く内容と判断した場合
- ・ 証明書が BR、本 CP または CPS に準拠して発行されていないことを知りえた場合
- ・ 証明書利用者および本 CA の秘密鍵が侵害され、アルゴリズムのタイプと基準要件の鍵サイズの要件を遵守していないこと、あるいは証明書が他の方法で悪用されているという合理的な証拠を得た場合
- ・ 本 CA の管轄権の法律に基づき、証明書利用者が拒否された当事者、または禁止された人物としてブラックリストに追加されたことを合理的な証拠に基づき知り得た場合
- ・ 証明書のドメイン名または IP アドレスの使用が、もはや法的に許可されていない合理的な証拠を得た場合（例えば、ドメイン名登録者と証明書利用者との間のライセンス契約またはサービス契約が終了した場合、またはドメイン名登録者がドメイン名の更新に失敗した場合など）
- ・ 証明書管理者と本 CA との二者間の契約の契約条項をもはや満たしていない場合
- ・ 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 証明書の失効申請を行うことができる者

証明書の失効申請を行うことができる者は、証明書利用者または申請者とする。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 が申請者となる場合もある。

#### 4.9.3 失効申請手続

証明書利用者または申請者は、本 CA または証明書管理者が提供するアプリケーションなどを使用し、定める手続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

証明書利用者または申請者は、秘密鍵が危殆化したまたは危殆化のおそれがあると判断した場合には、すみ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すみ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 失効確認の要求

本 CA が発行する証明書には、CRL 格納先の URL、および OCSP の URL を記載する。CRL および OCSP は、一般的な Web インターフェースを用いてアクセスすることができる。なお、CRL には、有効期限の切れた証明書情報は含まれない。

検証者は、証明書利用者の証明書について、有効性を確認しなければならない。証明書の有効性は、リポジトリに掲載している CRL または OCSP により確認する。

#### 4.9.7 証明書失効リストの発行頻度

CRL は、失効処理の有無にかかわらず、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 が発行した CRL は、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/ステータス確認の適用性

オンラインでの証明書ステータス情報は、OCSP を通じて提供される。証明書の失効ステータス情報は、失効処理の有無にかかわらず、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、その時点で証明書ステータス情報を更新し OCSP を通じて提

供される。

#### 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

検証者は、証明書利用者の証明書について、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 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

本 CA は、証明書の一時停止は行わない。

#### 4.9.14 証明書の一時停止申請を行うことができる者

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 証明書のステータス確認サービス

#### 4.10.1 運用上の特徴

証明書利用者は OCSP 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 を管理する。ただし、保守等により、一時的に OCSP 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

証明書利用者は証明書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。なお、証明書の更新申請を行わず、該当する証明書の有効期間が満了した場合にも終了となる。

#### 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および実施

本 CA は、証明書利用者の秘密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および実施

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 「5.4.1.記録されるイベントの種類」の本 CA に関連するシステムに係るログに加えて、次の情報をアーカイブとして保存する。

- ・ 発行した証明書および CRL
- ・ CRL の発行に関する処理履歴
- ・ CPS
- ・ CPS に基づき作成された認証局の業務運用を規定する文書
- ・ 認証業務を他に委託する場合には、委託契約に関する書類
- ・ 監査の実施結果に関する記録および監査報告書
- ・ OSCP へのアクセスログ
- ・ 証明書利用者からの審査に関する提出書類

#### 5.5.2 アーカイブ保存期間

本 CA は、アーカイブを最低 7 年間保存する。

#### 5.5.3 アーカイブの保護

アーカイブは、許可された者しかアクセスできないよう制限された施設において保管する。

#### 5.5.4 アーカイブのバックアップ手続

証明書発行、取消または CRL の発行等、本 CA に関連するシステムに関する重要なデータに変更がある場合は、適時、アーカイブのバックアップを取得する。

#### 5.5.5 記録にタイムスタンプを付与する要件

本 CA は、NTP (Network Time Protocol) を使用して本 CA に関連するシステムの時刻同期を行い、本 CA に関連するシステム内で記録される重要な情報に対しタイムスタンプを付与する。

#### 5.5.6 アーカイブ収集システム

アーカイブの収集システムは、本 CA に関連するシステムの機能に含まれている。

#### 5.5.7 アーカイブの検証手続

アーカイブは、セキュアな保管庫からアクセス権限者が入手し、定期的に媒体の保管状況の確認を行う。また必要に応じ、アーカイブの完全性および機密性の維持を目的として、新しい媒体への複製を行う。

### 5.6 鍵の切り替え

本 CA の鍵ペア更新または証明書更新は、原則として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実施する。新しい鍵ペアが生成された後は、新しい鍵ペアを使って証明書および CRL の発行を行う。

### 5.7 危殆化および災害からの復旧

#### 5.7.1 事故および危殆化時の手続

本 CA は、事故および危殆化が発生した場合に速やかに本 CA に関連するシステムおよび関連する業務を復旧できるよう、以下を含む事故および危殆化に対する対応手続を策定する。

- ・ CA 秘密鍵の危殆化
- ・ ハードウェア、ソフトウェア、データ等の破損、故障
- ・ 火災、地震等の災害

#### 5.7.2 ハードウェア、ソフトウェアまたはデータが破損した場合の手続

本 CA は、本 CA に関連するシステムのハードウェア、ソフトウェアまたはデータが破損した場合、バックアップ用として保管しているハードウェア、ソフトウェアまたはデータを使用して、すみやかに本 CA に関連するシステムの復旧作業を行う。

#### 5.7.3 秘密鍵が危殆化した場合の手続

本 CA は、本 CA の秘密鍵が危殆化したまたは危殆化のおそれがあると判断した場合、および災害等により本 CA に関連するシステムの運用が中断、停止につながるような状況が発生した場合には、予め定められた計画、手順に従い、安全に運用を再開させる。

#### 5.7.4 災害後の事業継続性

本 CA は、不測の事態が発生した場合に速やかに復旧作業を実施できるよう、あらかじめ本 CA に関連するシステムの代替機の確保、復旧に備えたバックアップデータの確保、復旧手続の策定等、可能な限り速やかに認証基盤システムを復旧するための対策を行う。

#### 5.8 認証局または登録局の終了

本 CA を終了する場合、3 か月前に証明書管理者を通じて証明書利用者その他の関係者にその旨を通知する。本 CA によって発行されたすべての証明書は、本 CA の終了以前に失効を行う。

## 6. 技術的セキュリティ管理

### 6.1 鍵ペアの生成およびインストール

#### 6.1.1 鍵ペアの生成

認証基盤システムでは、FIPS140-2 レベル 3 準拠の暗号装置で CA の鍵ペアを生成する。  
鍵ペアの生成作業は、複数名の権限者による操作によって行う。  
証明書利用者の鍵ペアは、証明書を配置する Web サーバー上で生成する。

#### 6.1.2 証明書利用者に対する秘密鍵の交付

証明書利用者の秘密鍵は、証明書利用者自身が生成する。本 CA からの秘密鍵の交付は行わない。

#### 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、オンラインによって行うことができる。  
この時の通信経路は SSL により暗号化を行う。

#### 6.1.4 検証者への 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 ビットとする。

#### 6.1.6 公開鍵のパラメーターの生成および品質検査

本 CA の公開鍵のパラメーターの生成、およびパラメーターの強度の検証は、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ーの生成および品質検査について規定しない。

#### 6.1.7 鍵の用途

本 CA および本 CA が発行する証明書の鍵の用途は以下のとおりとする。

表 6.1-1 鍵の用途

|                   | 本 CA | 本 CA が発行する証明書 |
|-------------------|------|---------------|
| digital Signature | —    | yes           |

|                  |     |     |
|------------------|-----|-----|
| nonRepudiation   | —   | —   |
| keyEncipherment  | —   | yes |
| dataEncipherment | —   | —   |
| keyAgreement     | —   | —   |
| keyCertSign      | yes | —   |
| cRLSign          | yes | —   |
| encipherOnly     | —   | —   |
| decipherOnly     | —   | —   |

## 6.2 秘密鍵の保護および暗号装置技術の管理

### 6.2.1 暗号装置の標準および管理

本 CA の秘密鍵の生成、保管、署名操作は、FIPS140-2 レベル 3 準拠の暗号装置を用いて行う。証明書利用者の秘密鍵については規定しない。

### 6.2.2 秘密鍵の複数人管理

本 CA の秘密鍵の活性化、非活性化、バックアップ等の操作は、安全な環境において複数人の権限者によって行う。証明書利用者の秘密鍵の活性化、非活性化、バックアップ等の操作は、証明書利用者の管理の下で安全に行わなければならない。

### 6.2.3 秘密鍵のエスクロー

本 CA は、本 CA の秘密鍵のエスクローは行わない。

本 CA は、証明書利用者の秘密鍵のエスクローは行わない。

### 6.2.4 秘密鍵のバックアップ

本 CA の秘密鍵のバックアップは、セキュアな室において複数名の権限者によって行われ、暗号化された状態で、セキュアな室に保管される。

証明書利用者の秘密鍵のバックアップは、証明書利用者の管理の下で安全に保管しなければならない。

### 6.2.5 秘密鍵のアーカイブ

本 CA では、本 CA の秘密鍵のアーカイブは行わない。

証明書利用者の秘密鍵については規定しない。

### 6.2.6 秘密鍵の暗号モジュールへのまたは暗号モジュールからの転送

本 CA の秘密鍵の暗号装置への転送または暗号装置からの転送は、セキュアな室において、秘密鍵を暗号化した状態で行う。証明書利用者の秘密鍵については規定しない。

#### 6.2.7 暗号装置への秘密鍵の格納

本電子認証基盤の上で運用される CA の秘密鍵は、暗号化された状態で暗号装置内に格納する。証明書利用者の秘密鍵については規定しない。

#### 6.2.8 秘密鍵の活性化方法

本 CA の秘密鍵の活性化は、セキュアな室において複数名の権限者によって行う。証明書利用者の秘密鍵については規定しない。

#### 6.2.9 秘密鍵の非活性化方法

本 CA の秘密鍵の非活性化は、セキュアな室において複数名の権限者によって行う。証明書利用者の秘密鍵については規定しない。

#### 6.2.10 秘密鍵の破棄方法

本 CA の秘密鍵の廃棄は、複数名の権限者によって完全に初期化または物理的に破壊することによって行う。バックアップについても同様の手続によって行う。証明書利用者の秘密鍵については規定しない。

#### 6.2.11 暗号装置の評価

本 CA で使用する暗号装置の品質基準については、本 CP「6.2.1.暗号装置の標準および管理」のとおりである。証明書利用者の秘密鍵については規定しない。

### 6.3 鍵ペアのその他の管理方法

#### 6.3.1 公開鍵のアーカイブ

本 CA の公開鍵については CPS「6.2.1 暗号装置の標準および管理」のとおりである。証明書利用者の秘密鍵については規定しない。

#### 6.3.2 秘密鍵および公開鍵の有効期間

本 CA の秘密鍵および公開鍵の有効期間は 20 年以内とする。証明書利用者の秘密鍵については規定しない。

### 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. 証明書および証明書失効リストおよび OCSP のプロファイル

## 7.1 証明書のプロファイル

本 CA が発行する証明書は RFC5280 に準拠している。プロファイルは、次表のとおりである。

表 7.1-1 サーバー証明書プロファイル

| 基本領域                         |                     | 設定内容                                                                                                                                                          | critical |
|------------------------------|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| Version                      |                     | Version 3                                                                                                                                                     | -        |
| Serial Number                |                     | 例) 0123456789                                                                                                                                                 | -        |
| Signature Algorithm          |                     | sha256 With RSA Encryption                                                                                                                                    | -        |
| Issuer                       | Country             | C=JP                                                                                                                                                          | -        |
|                              | Organization        | O=SECOM Trust Systems CO.,LTD                                                                                                                                 | -        |
|                              | Common Name         | CN=各認証局のコモンネームを設定                                                                                                                                             | -        |
| Validity                     | NotBefore           | 例) 2008/3/1 00:00:00 GMT                                                                                                                                      | -        |
|                              | NotAfter            | 例) 2009/3/1 00:00:00 GMT                                                                                                                                      | -        |
| Subject                      | Country             | 任意                                                                                                                                                            | -        |
|                              | State Or Province   | 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         | サーバー名 (必須)                                                                                                                                                    | -        |
| Subject Public Key Info      |                     | 主体者の公開鍵 2048 ビット                                                                                                                                              | -        |
| 拡張領域                         |                     | 設定内容                                                                                                                                                          | critical |
| KeyUsage                     |                     | digitalSignature, keyEncipherment                                                                                                                             | y        |
| ExtendedKeyUsage             |                     | serverAuth                                                                                                                                                    | n        |
| Subject Alt Name             |                     | dNSName=サーバー名                                                                                                                                                 | n        |
| CertificatePolicies          |                     | [1]policyIdentifier<br>OID=本 CP の[1.2-1 OID]を設定<br>policyQualifiers<br>policyQualifierId=CPS<br>qualifier=各認証局の URL を設定<br>[2]policyIdentifier=2.23.140.1.2.1 | n        |
| CRL Distribution Points      |                     | 各認証局の URL を設定                                                                                                                                                 | n        |
| Authority Information Access |                     | accessMethod<br>ocsp (1 3 6 1 5 5 7 48 1)                                                                                                                     | n        |

|                                                           |                                       |   |
|-----------------------------------------------------------|---------------------------------------|---|
|                                                           | accessLocation<br>各認証局の URL を設定       |   |
| Authority Key Identifier                                  | 発行者公開鍵の SHA-1 ハッシュ値<br>(160 ビット)      | n |
| Subject Key Identifier                                    | 主体者公開鍵の SHA-1 ハッシュ値<br>(160 ビット)      | n |
| Certificate Transparency 用拡張<br>(1.3.6.1.4.1.11129.2.4.2) | SignedCertificateTimestampList の<br>値 | n |

表 7.1-2 OCSP サーバー証明書プロファイル

| 基本領域                     |              | 設定内容                                                                                                                 | critical |
|--------------------------|--------------|----------------------------------------------------------------------------------------------------------------------|----------|
| Version                  |              | Version 3                                                                                                            | -        |
| Serial Number            |              | 例) 0123456789                                                                                                        | -        |
| Signature Algorithm      |              | sha256 With RSA Encryption                                                                                           | -        |
| Issuer                   | Country      | C=JP                                                                                                                 | -        |
|                          | Organization | O=SECOM Trust Systems CO.,LTD                                                                                        | -        |
|                          | Common Name  | CN=各認証局のコモンネームを設定                                                                                                    | -        |
| Validity                 | NotBefore    | 例) 2008/3/1 00:00:00 GMT                                                                                             | -        |
|                          | NotAfter     | 例) 2008/3/5 00:00:00 GMT                                                                                             | -        |
| Subject                  | Country      | C=JP (固定値)                                                                                                           | -        |
|                          | Organization | SECOM Trust Systems CO.,LTD.<br>(固定値)                                                                                | -        |
|                          | Common Name  | OCSP サーバー名 (必須)                                                                                                      | -        |
| Subject Public Key Info  |              | 主体者の公開鍵 2048 ビット                                                                                                     | -        |
| 拡張領域                     |              | 設定内容                                                                                                                 | critical |
| KeyUsage                 |              | digitalSignature                                                                                                     | y        |
| ExtendedKeyUsage         |              | OCSPSigning                                                                                                          | n        |
| OCSP No Check            |              | null                                                                                                                 | n        |
| CertificatePolicies      |              | policyIdentifier<br>OID=本 CP の[1.2-1 OID]を設定<br>policyQualifiers<br>policyQualifierId=CPS<br>qualifier=各認証局の URL を設定 | n        |
| Authority Key Identifier |              | 発行者公開鍵の SHA-1 ハッシュ値                                                                                                  | n        |

|                        |                                  |   |
|------------------------|----------------------------------|---|
|                        | (160 ビット)                        |   |
| Subject Key Identifier | 主体者公開鍵の SHA-1 ハッシュ値<br>(160 ビット) | n |

## 7.2 CRL のプロファイル

本 CA が発行する CRL は RFC5280 に準拠している。プロファイルは、次表のとおりである。

表 7.2 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    | O= SECOM Trust Systems CO.,LTD.                   | -        |
|                          | Common Name     | CN=各認証局のコモンネームを設定                                 | -        |
| This Update              |                 | 例) 2008/3/1 00:00:00 GMT                          | -        |
| Next Update              |                 | 例) 2008/3/5 00:00:00 GMT<br>更新間隔=24H、有効期間=96H とする | -        |
| Revoked<br>Certificates  | Serial Number   | 例) 0123456789                                     | -        |
|                          | Revocation Date | 例) 2008/3/1 00:00:00 GMT                          | -        |
|                          | Reason Code     | 失効事由 (unspecified, etc.)                          | -        |
| 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<br>(160 ビット)                  | n        |

## 7.3 OCSP のプロファイル

本 CA は、RFC5019 および 6960 に準拠する OCSP 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

本 CA は、本 CP および CPS に準拠して運用がなされているかについて、適時監査を行う。本 CA が行う準拠性監査に関する諸事項については本 CP および CPS に規定する。

### 8.1 監査の頻度

本 CA は、本 CA が本 CP および CPS に準拠して運用されているかに関して、定期的に準拠性監査を行う。

### 8.2 監査人の身元／資格

本 CA の準拠性監査は、CA の業務に精通している監査人が行う。また、WebTrust 認証を受ける CA の監査は、監査法人が行う。

### 8.3 監査人と被監査部門の関係

監査人は、本 CA との間に特別な利害関係のない監査人を選定する。

### 8.4 監査で扱われる事項

監査は、本 CA の運用にかかる業務を対象として行う。

また、認証局のための WebTrust for CA 規準、WebTrust for BR 規準に基づいて行われることもある。

### 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、すみやかに必要な是正措置を行う。

### 8.6 監査結果の開示

監査報告書は、本委員会に報告される。監査報告書は、許可されたものだけがアクセスできるよう保管管理される。

なお、WebTrust for CA、WebTrust for BR の検証に関する報告書は、WebTrust for CA、WebTrust for BR 認定の規則に従い、特定のサイトにて参照可能となる。

## 9. 他の業務上および法的事項

### 9.1 料金

本 CA が発行する証明書に関する料金については、別途規定する。

### 9.2 財務的責任

本 CA 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

本項については、CPS に規定する。

### 9.4 個人情報の保護

本項については、CPS に規定する。

### 9.5 知的財産権

本 CP は著作権を含み、当社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 秘密鍵のセキュアな生成・管理を行うこと
- ・ RA からの申請に基づいた証明書の正確な発行、失効および管理を行うこと
- ・ IA のシステムの運用、稼動監視を行うこと
- ・ CRL の発行、公表を行うこと
- ・ OCSP の公開を行うこと

##### 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・運用を行うこと
- ・ 証明書発行時、実在性確認等の審査を的確に行うこと
- ・ IA への証明書発行・失効等の指示を正確かつすみやかに行うこと
- ・ リポジトリの維持・管理を行うこと

#### 9.6.2 証明書利用者の表明保証

証明書利用者は、次の義務を負うものとする。

- ・ 証明書利用者は証明書の発行申請に際して、正確かつ完全な情報を提供すること
- ・ 当該情報に変更があった場合には、その旨をすみやかに証明書管理者まで通知すること
- ・ 危殆化から自身の秘密鍵を保護すること
- ・ 証明書の使途は当約款、本 CP および本 CPS に従うこと
- ・ 証明書に記載の公開鍵に対応する秘密鍵が危殆化した、またはそのおそれがあると証明書利用者が判断した場合、登録情報に変更があった場合、または本 CA から「4.9.1 証明書失効事由」にもとづき証明書失効の指示があった場合は、証明書利用者は証明書の失効をすみやかに申請すること

#### 9.6.3 検証者の表明保証

検証者は、次の義務を負うものとする。

- ・ 本 CA の証明書について、有効性の確認を行うこと
- ・ 証明書利用者の情報を信頼するかの判断は検証者の責任で行うこと
- ・ 秘密鍵が侵害されたことを認識した、またはその疑いがある場合は、本 CA にすみやかに通知すること

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、付随的損害また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、データの紛失またはその他の間接的も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 において、次の場合、本 CA は責任を負わないものとします。

- ・ 本 CA に起因しない不法行為、不正使用または過失等により発生する一切の損害
- ・ 確認された情報の誤りが申請者の詐欺または故意の不正行為の結果である場合、いかなる場合にも生じるすべての責任
- ・ 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

- ・ 証明書管理者および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
- ・ 証明書管理者および証明書利用者の環境（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
- ・ 本 CA の責に帰することのできない事由で証明書および CRL、OCSP 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
- ・ 認証サービスの提供終了など、証明書管理者がサービス提供の義務の履行を怠ったために生じた損害
- ・ 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 が発行する証明書に関する補償については、別途規定する。

#### 9.10 有効期間と終了

##### 9.10.1 有効期間

本 CP は、本委員会の承認により有効となる。

##### 9.10.2 終了

本 CP は、本 CA を終了した時点で無効となる。

##### 9.10.3 終了の効果と効果継続

証明書利用者が証明書の利用を終了する場合、証明書管理者がサービスの提供を終了する場合、または、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、証明書管理者および本 CA に適用されるものとしします。

#### 9.11 関係者間の個別通知と連絡

本 CA は必要な通知を証明書管理者に行い、証明書管理者は証明書利用者および検証者に対する必要な通知をホームページ、電子メールまた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、本委員会の承認によって発効する。

### 9.12.2 通知方法および期間

本 CP を変更した場合、変更した本 CP をすみやかに公表することをもって、関係者に対しての告知とする。

### 9.12.3 オブジェクト識別子の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

本 CA が発行する証明書に関わる紛争について、本 CA に対して訴訟、仲裁等を含む法的解決手段に訴えようとする場合は、本 CA に対して事前にその旨を通知するものとする。仲裁および裁判地は東京都区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 CP、CPS の解釈、有効性および証明書の利用にかかわる紛争については、日本国の法律を適用する。

## 9.15 適用法の遵守

本 CA は、国内における各種輸出規制を遵守し、暗号ハードウェアおよびソフトウェアを取扱うものとする。

## 9.16 雑則

### 9.16.1 完全合意条項

当社は、証明書利用者または検証者の義務等を本 CP および当約款、CPS によって包括的に定め、これ以外の口頭であると書面であるとを問わず、いかなる合意も効力を有しないものとする。

### 9.16.2 権利譲渡条項

当社が本 CA を第三者に譲渡する場合、本 CP および当約款、CPS において記載された責務およびその他の義務の譲渡を可能とする。

#### 9.16.3 分離条項

本 CP および当約款、CPS の一部の条項が無効であったとしても、当該文書に記述された他の条項は有効であるものとする。

#### 9.16.4 強制執行条項

規定しない。

#### 9.17 その他の条項

規定しない。