セコム電子認証基盤
認証運用規程
(Certification Practice Statement)

Version2.20

2024 年 8 月 21 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	2006/03/23	初版発行
2.00	2006/05/22	会社統合にともない、会社名“セコムトラストネット”を“セコムトラストシステムズ”に変更 “セコムトラストネットセキュリティポリシ委員会”を“認証サービス改善委員会”に変更
2.10	2017/05/23	全体的な文言および体裁の見直し
2.11	2018/11/28	文言および体裁の見直し
2.12	2019/05/24	全体的な文言および体裁の見直し
2.13	2020/03/30	章立ての見直し、および一部「規定しない」の内容追加
2.14	2021/03/30	日付およびバージョンの更新
2.15	2021/11/30	全体的な文言および体裁の見直し
2.16	2022/06/10	全体的な文言および体裁の見直し
2.17	2022/12/08	「6.3.2　私有鍵および公開鍵の有効期間」に内容追加
2.18	2023/05/17	「2.3　公開の時期または頻度」を更新 「5.3.2　背景調査」項目名の変更 「5.5.1　アーカイブの種類」を更新 「5.5.2　アーカイブ保存期間」を更新 「5.7.3　私有鍵が危殆化した場合の手続」を更新
2.19	2024/04/01	「1.1　概要」を更新 「1.6　定義と略語」を更新 「5.3.2　背景調査」を更新 「6.1.5　鍵サイズ」を更新 「6.1.6　公開鍵のパラメータの生成および品質検査」を更新 「6.3.2　私有鍵および公開鍵の有効期間」を更新 「8.4　監査で扱われる事項」を更新
2.20	2024/08/21	以下を更新 1.1　概要 1.3.3　証明書利用者 5.2.2　職務ごとに必要とされる人数 5.2.4　職務分割が必要となる役割 5.4.1　記録されるイベントの種類 5.4.3　監査ログを保持する期間

		5.4.5　監査ログのバックアップ手続 5.5.1　アーカイブの種類 5.5.2　アーカイブ保存期間 5.7.1　事故および危殆化時の手続 5.7.3　私有鍵が危殆化した場合の手続 6.1.1　鍵ペアの生成 6.1.5　鍵サイズ 6.2　私有鍵の保護および暗号モジュール技術の管理 6.2.7　暗号モジュールへの私有鍵の格納 6.3.2　私有鍵および公開鍵の有効期間 以下を追加 5.4.1.1 ルーターとファイアウォールのアクティビティログ 5.4.1.2 タイムスタンプ局で記録されるイベントの種類

目次

1. はじめに

1.1 概要

セコム電子認証基盤認証運用規程（以下、「本 CPS」という）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）の電子認証基盤に関する運用規則を定めるものである。

電子認証基盤とは、セコムトラストシステムズの認証局（以下、「CA」という）、およびセコムトラストシステムズのプライベート CA サービスの利用顧客（以下、「プライベート CA 利用者」という）の CA を運用するためのプラットホームであり、その運用はセコムトラストシステムズが行う。

電子認証基盤は、認証局として失効情報および CA 証明書等を公開するためのリポジトリーサーバーや、証明書発行要求を送信するためのアプリケーションを搭載したサーバー等の認証基盤システムから構成されている。

CA の運営主体となる組織等は、電子認証基盤上に CA サーバーを構築することで、信頼性の高い強固なセキュリティを兼ね備えた CA を保有することが可能である。

電子認証基盤の上で運用される CA は、発行する証明書の種類、用途、CA 固有の運用等に関する各種規則を証明書ポリシー（以下、「CP」という）として規定しなければならない。電子認証基盤の上で運用される CA は、本 CPS および CP を遵守し、運用しなければならない。

下位 CA 証明書が「Security Communication RootCA 下位 CA 用証明書ポリシー」に準拠している証明書を発行する CA は、https://www.cabforum.org/で公開される以下、CA/Browser Forum で定められた規準およびアプリケーションソフトウェアサプライヤーの規準の最新版に準拠する。

表 1.1-1 規準一覧

下位 CA で発行する証明書種類	準拠するべき規準
TLS サーバー証明書	● Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates（以下、Baseline Requirements という） ● Guidelines for the Issuance and Management of Extended Validation Certificates (EV 証明書のみが対象。以下、EV Guidelines という）

	● Apple Root Certificate Program ● Chrome Root Program Policy ● Microsoft Trusted Root Program ● Mozilla Root Store Policy
TLS クライアント認証証明書	● Apple Root Certificate Program ● Microsoft Trusted Root Program
S/MIME 証明書	● Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates（以下、S/MIME Baseline Requirements という） ● Apple Root Certificate Program ● Microsoft Trusted Root Program ● Mozilla Root Store Policy
コードサイニング証明書 コードサイニング証明書用のタイムスタンプ証明書	● Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates（以下、Baseline Requirements for Code Signing Certificates という） ● Microsoft Trusted Root Program
AATL ドキュメントサイニング証明書 AATL タイムスタンプ証明書	● Adobe Approved Trust List Technical Requirements (AATL Technical Requirements)
Microsoft ドキュメントサイニング証明書	● Microsoft Trusted Root Program

本 CPS と CP の内容に齟齬がある場合は、CP の内容が優先されるものとする。また、セコムトラストシステムズとの間でサービス契約等が存在する場合は、CP よりサービス契約等が優先されるものとする。本 CPS と Baseline Requirements の間に矛盾がある場合、Baseline Requirements が本 CPS に優先して適用される。

本 CPS 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 CPS の正式名称は、「セコム電子認証基盤認証運用規程」という。本 CPS には、登

録された一意のオブジェクト識別子(以下、「OID」という)が割り当てられる。本 CPS の OID は、次のとおりである。

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

電子認証基盤の上で運用される CA ごとに定められる OID については、CP に規定する。

1.3 PKI の関係者

1.3.1 CA

CA は、証明書の発行、取消、CRL（Certificate Revocation List：証明書失効リスト）の開示、リポジトリーの維持管理等を行う。

電子認証基盤の上で運用される CA の運営主体はセコムトラストシステムズ、またはプライベート CA 利用者である。また CA の運用はセコムトラストシステムズが行う。CA については、「1.6 定義と略語」に定義する。

1.3.2 RA

RA は、証明書の発行、取消を申請する申請者の実在性確認、本人性確認の審査および証明書を発行、失効するための登録業務等を行う。電子認証基盤の上で運用される CA において、RA の運用はセコムトラストシステムズ、またはプライベート CA 利用者が行う。

下位 CA 証明書が「Security Communication RootCA 下位 CA 用証明書ポリシー」に準拠した TLS サーバー証明書を発行する CA の場合、Baseline Requirements 3.2.2.4 および 3.2.2.5 で要求されているドメイン検証および IP アドレス検証を除き、本 CA は Baseline Requirements3.2 の要件のすべてまたは一部の遂行を、第三者に委託することができる。ただし、プロセス全体として、Baseline Requirements3.2 の要件のすべてを満たすことを条件とする。

CA は、委託した職務の遂行を許可する前に、契約を通じて下記を委託先に要求することとする。

(1) 委託した職務に該当する場合、本 CPS「5.3.1 資格、経験および身分証明の要件」の資格要件を満たす。
(2) 本 CPS 「5.5.2 アーカイブの保存期間」に従い、ドキュメントを保持する。
(3) 本書の要件以外にも、委託された職務に適用される条件を遵守する。
(4) CP/CPS、本 CA が Baseline Requirements に準拠していることを認定した委託先の運用規定。

1.3.3 証明書利用者

証明書利用者とは、証明書の発行先であり、加入者契約または利用規約を遵守する自然人または法人をいう。

1.3.4 検証者

検証者とは、電子認証基盤の上で運用される CA が発行した証明書の有効性を検証する主体をいう。依拠当事者とアプリケーションソフトウェアサプライヤーについては、「1.6 定義と略語」に定義する。

1.3.5 他の関係者

他の関係者とは、監査人や、セコムトラストシステムズとの間でサービス契約等が存在する企業や組織、そのシステムインテグレーションを行う業者などが含まれる。

1.4 証明書の用途

1.4.1 適切な証明書の用途

本項は、電子認証基盤の上で運用される CA の CP に規定する。

1.4.2 禁止される証明書の用途

本項は、電子認証基盤の上で運用される CA の CP に規定する。

1.5 ポリシー管理

1.5.1 文書を管理する組織

本 CPS の維持、管理は、セコムトラストシステムズが行う。

1.5.2 連絡先

本 CPS に関する問い合わせ先は次のとおりである。

問い合わせ窓口	：	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
ウェブサイト	：	https://www.secomtrust.net/

加入者、依拠当事者、アプリケーションソフトウェアサプライヤー、その他の第三者は、

私有鍵の危殆化の疑い、証明書の誤用、あるいはその他の種類の詐欺、危殆化、誤用、不適切 な行為、または証明書に関連するその他の事項について、上記の連絡先に報告することができる。本 CA では、失効する必要があると判断した場合、証明書を失効する。

1.5.3 ポリシー適合性を決定する者

本 CPS の内容は、セコムトラストシステムズの認証サービス委員会において決定される。本 CPS は、最低でも年次でレビューし、改訂する。

1.5.4 承認手続

本 CPS は、セコムトラストシステムズが作成・改訂を行い、セコムトラストシステムズの認証サービス委員会の承認により発効される。

1.6 定義と略語

五十音順（あ行～わ行）

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。

アプリケーションソフトウェアサプライヤー(Application Software Supplier)

証明書を表示または使用し、ルート CA 証明書を組み込むインターネットブラウザソフトウェアまたはその他の依拠当事者アプリケーションソフトウェアのサプライヤー。

依拠当事者(Relying Party)

有効な証明書に依拠する個人または法人。アプリケーションソフトウェアサプライヤーによって配布されるソフトウェアが単に証明書に関連する情報を表示するだけの場合、そのサプライヤーは依拠当事者とは見なされない。

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。

電子認証基盤

セコムトラストシステムズの CA、およびプライベート CA 利用者の CA を運用するためのプラットホームのことをいう。

電子証明書

本人にしか保有し得ない私有鍵と対になる公開鍵であ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。

認証書（Attestation Letter）

会計士、弁護士、政府関係者、またはその他の信頼できる第三者によって書かれた、主体者情報が正しいことを証明する文書。

プライベート CA サービス

セコムトラストシステムズが提供する認証サービスの名称のことをいう。

リポジトリー

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。

ルート CA

本 CPS でいう Security Communication RootCA は、セコムが所有し運営する機関で、下位 CA の証明書を発行するルート CA である。下位 CA の頂点として機能する CA である。

アルファベット順（A～Z）

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。

CA（Certification Authority）：認証局

証明書を発行する認証局であり、証明書の発行・更新・失効、CA 私有鍵の生成・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。本 CPS では発行局（IA:Issuing Authority）も含まれる。

CP（Certificate Policy）：証明書ポリシー

CA が発行する証明書の種類、発行対象、用途、申込手続、発行基準等、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 を運用するうえでの諸手続、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、私有鍵の危殆化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。

EV Processes：EV プロセス

EV Guidelines に基づく証明書データの検証、EV 証明書の発行、リポジトリーの保守、および EV 証明書の失効に用いられる鍵、ソフトウェア、プロセス、および手順。

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。

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。

NTP（Network Time Protocol）

コンピュータの内部時計を、ネットワークを介して正しく調整するプロトコルのことをいう。

OCSP

Online Certificate Status Protocol の略。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である。

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（Registration Authority）：登録局

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。

RSA

公開鍵暗号方式として普及している最も標準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。

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-2

電子署名に使われる Secure Hash Algorithm シリーズのハッシュ関数であり、SHA-1 の改良版である。本 CP にある SHA-256 のビット長は 256 ビット、SHA-384 のビット長は 384 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

CPA Canada 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。

X.500

名前およびアドレスの調査から属性による検索まで広範囲なサービスを提供することを目的に ITU-T が定めたディレクトリ標準。X.500 識別名は、X.509 の発行者名および主体者名に使用される。

X.509

X.509 ITU-T が定めた証明書および CRL のフォーマット。X.509 v3(Version 3)では、任意の情報を保有するための拡張領域が追加された。

2. 公開とリポジトリーの責任

2.1 リポジトリー

セコムトラストシステムズは、電子認証基盤の上で運用される CA のために、リポジトリーを用意する。リポジトリーは、24 時間 365 日利用できるよう維持管理を行う。ただし、利用可能な時間帯においてもシステム保守、CA ごとの要件等により、利用できない場合がある。

2.2 証明情報の公開

証明書利用者および検証者がオンラインによって 24 時間 365 日閲覧可能となるように、セコムトラストシステムズは、本 CPS をリポジトリーに格納する。

電子認証基盤の上で運用される CA 特有の公開情報については、電子認証基盤の上で運用される CA の CP に規定する。

2.3 公開の時期または頻度

本 CA は、Baseline Requirements の最新バージョンをどのように実施するかを詳細に記述した CP および CPS の策定、導入、施行、年次更新を行うものとする。本 CA は、CP および CPS に変更が加えられていない場合でも、バージョン番号を増やし、変更履歴を追加することにより、Baseline Requirements への準拠を示す。

2.4 リポジトリーへのアクセス管理

本 CA はリポジトリーを読み取り専用の形で公開するものとする。本 CA では、許可された CA 管理者のみがリポジトリーの追加、削除、変更、公開などの操作を実行できる。

3. 識別と認証

3.1 名前決定

3.1.1 名前の種類

本項は、電子認証基盤の上で運用される CA の CP に規定する。

3.1.2 名前が意味をもつことの必要性

本項は、電子認証基盤の上で運用される CA の CP に規定する。

3.1.3 証明書利用者の匿名性または仮名性

本項は、電子認証基盤の上で運用される CA の CP に規定する。

3.1.4 様々な名前形式を解釈するための規則

本項は、電子認証基盤の上で運用される CA の CP に規定する。

3.1.5 名前の一意性

本項は、電子認証基盤の上で運用される CA の CP に規定する。

3.1.6 認識、認証および商標の役割

本項は、電子認証基盤の上で運用される CA の CP に規定する。

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

本項は、電子認証基盤の上で運用される CA の CP に規定する。

3.2.2 組織の認証

本項は、電子認証基盤の上で運用される CA の CP に規定する。

3.2.2.1 アイデンティティ

本項は、電子認証基盤の上で運用される CA の CP に規定する。

3.2.2.2 商号/商標名

本項は、電子認証基盤の上で運用される CA の CP に規定する。

3.2.2.3 国の検証

本項は、電子認証基盤の上で運用される CA の CP に規定する。

3.2.3 個人の認証

本項は、電子認証基盤の上で運用される CA の CP に規定する。

3.2.4 検証されない証明書利用者の情報

本項は、電子認証基盤の上で運用される CA の CP に規定する。

3.2.5 権限の正当性確認

本項は、電子認証基盤の上で運用される CA の CP に規定する。

3.2.6 相互運用の基準

本項は、電子認証基盤の上で運用される CA の CP に規定する。

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

本項は、電子認証基盤の上で運用される CA の CP に規定する。

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

本項は、電子認証基盤の上で運用される CA の CP に規定する。

3.4 失効申請時の本人性確認と認証

本項は、電子認証基盤の上で運用される CA の CP に規定する。

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

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.1.2 申請手続および責任

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.2 証明書申請手続

4.2.1 本人性確認と認証の実施

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.2.2 証明書申請の承認または却下

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.2.3 証明書申請の処理時間

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.3 証明書の発行

4.3.1 証明書発行時の処理手続

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.3.2 証明書利用者への証明書発行通知

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.4 証明書の受領確認

4.4.1 証明書の受領確認手続

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.4.2 認証局による証明書の公開

本項は、電子認証基盤の上で運用される CA の CP に規定する。

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
本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.5 鍵ペアおよび証明書の用途

4.5.1 証明書利用者の私有鍵および証明書の用途
本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.5.2 検証者の公開鍵および証明書の用途
本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.6 証明書の更新

4.6.1 証明書更新の状況
本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.6.2 証明書の更新申請を行うことができる者
本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.6.3 証明書の更新申請の処理手続
本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.6.4 証明書利用者に対する新しい証明書の発行通知
本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.6.5 更新された証明書の受領確認手続
本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.6.6 認証局による更新された証明書の公開
本項は、電子認証基盤の上で運用される CA の CP に規定する。

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
本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.7 証明書の鍵更新

4.7.1 鍵更新の状況

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.7.2 新しい証明書の申請を行うことができる者

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.7.3 鍵更新をともなう証明書申請の処理手続

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.7.4 証明書利用者に対する新しい証明書の発行通知

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.7.5 鍵更新された証明書の受領確認手続

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.7.6 認証局による鍵更新済みの証明書の公開

本項は、電子認証基盤の上で運用される CA の CP に規定する。

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

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.8 証明書の変更

4.8.1 証明書の変更事由

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.8.2 証明書の変更申請を行うことができる者

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.8.3 変更申請の処理手続

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.8.4 証明書利用者に対する新しい証明書の発行通知

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.8.5 変更された証明書の受領確認手続

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.8.6 認証局による変更された証明書の公開

本項は、電子認証基盤の上で運用される CA の CP に規定する。

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

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.9 証明書の失効と一時停止

4.9.1 証明書失効事由

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.9.2 証明書の失効申請を行うことができる者

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.9.3 失効申請手続

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.9.4 失効申請の猶予期間

本項は、電子認証基盤の上で運用される CA の CP に規定する。

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

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.9.6 失効確認の要求

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.9.7 証明書失効リストの発行頻度

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.9.8 証明書失効リストの発行最大遅延時間

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.9.9 オンラインでの失効/ステータス確認の適用性

本項は、電子認証基盤の上で運用される CA の CP に規定する。

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

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.9.11 利用可能な失効情報の他の形式

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.9.12 鍵の危殆化に対する特別要件

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.9.13 証明書の一時停止事由

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.9.14 証明書の一時停止申請を行うことができる者

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.9.15 証明書の一時停止申請手続

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.9.16 一時停止を継続することができる期間

本項は、電子認証基盤の上で運用される CA の CP に規定する。

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

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.10.2 サービスの利用可能性

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.10.3 オプショナルな仕様

本項は、電子認証基盤の上で運用される CA の CP に規定する。

4.11 加入（登録）の終了

本項は、電子認証基盤の上で運用される CA の CP に規定する。

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

本項は、電子認証基盤の上で運用される CA の CP に規定する。

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

本項は、電子認証基盤の上で運用される CA の CP に規定する。

5. 設備上、運営上、運用上の管理

CA/Browser Forum の「Network and Certificate System Security Requirement」は、参照することにより本書に完全に組み込まれる。

CA は、以下の目的で設計された包括的なセキュリティプログラムを開発、実装、維持する。

1. 証明書データおよび証明書管理プロセスの機密性、完全性、および可用性を保護する。
2. 証明書データおよび証明書管理プロセスの機密性、完全性、および可用性にとっての潜在的な脅威または危険から保護する。
3. 証明書データおよび証明書管理プロセスに対する不正または違法なアクセス、使用、開示、改変、または破壊から保護する。
4. 証明書データおよび証明書管理プロセスの不慮の損失、破壊、または損傷から保護する。
5. 法律によって CA に適用されるその他のセキュリティ要件すべてに準拠する。

証明書管理プロセスは、以下を含む必要がある。

1. 物理的なセキュリティ制御や環境制御。
2. 構成管理、信頼済みコードの整合性メンテナンス、マルウェア検出/防止を含む、システム整合性制御。
3. ポート制限や IP アドレスフィルタリングを含む、ネットワークセキュリティおよびファイアウォール管理。
4. ユーザー管理、信頼済みロールの分担、教育、意識向上、トレーニング。
5. 個々の責任を明確にするための論理的なアクセス制御、アクティビティロギング、およびアイドル時のタイムアウト。

CA のセキュリティプログラムには、以下のような年次リスクアセスメントを含める必要がある。

1. 証明書データまたは証明書管理プロセスに対する不正なアクセス、開示、不正使用、改変、または破壊につながる、予測可能な内外の脅威を特定する。
2. これらの脅威がもたらす可能性があるダメージについて、証明書データや証明書管理プロセスの秘密度を考慮に入れて評価する。
3. このような脅威に対抗するために CA が配備したポリシー、手順、情報システム、技術、その他の手配の充実度に関して評価する。

リスクアセスメントに基づき、CA は、上述の目的を実現するべく設計されたセキュリティ手順、対策、および製品で構成されるセキュリティ計画を開発、実装、および維持し、リスクアセスメント中に識別されたリスクを、証明書データおよび証明書管理プロセスの重要度に応じて管理するものとする。セキュリティ計画には、証明書データおよび証明書管理

プロセスの秘密度に適した管理上、組織的、技術的、および物理的な保護対策を含めなければならない。また、セキュリティ計画では、その時点で利用可能な技術および特定の対策の実装コストを考慮に入れなければならず、セキュリティの侵害から生じる可能性がある損害および保護対象のデータの性質に適した合理的な水準のセキュリティを実装するものとする。

5.1 物理的管理

5.1.1 立地場所および構造

セコムトラストシステムズは、認証基盤システムをセキュアなデータセンター内に設置する。データセンターは、水害、地震、火災、その他の災害の被害を容易に受けない場所に建設されており、かつ建物の構造上も、これら災害防止のための対策を講じている。

5.1.2 物理的アクセス

セコムトラストシステムズは、認証基盤システムの重要性に応じて、物理的なアクセス制御および電子的なアクセス制御を組み合わせた適切なセキュリティコントロールを実装する。また、監視カメラ、各種センサーを設置し、認証基盤システムへのアクセスを監視する。

5.1.3 電源および空調

データセンターでは、瞬断および長時間の停電時においても認証基盤システムの運用を可能とするために、無停電電源装置および自家発電装置による電源対策を施している。また、認証基盤システムは、空気調和機により最適な温度、湿度を一定に保つことが可能な環境下に設置する。

5.1.4 水害対策

セコムトラストシステムズは、水害対策として、認証基盤システムを建物の二階以上に設置する。また、防水対策として、認証基盤システムを設置する室には漏水検知器を設置する。

5.1.5 火災対策

認証基盤システムを設置する室は、防火壁によって区画された防火区画とし、火災報知機および消火設備を設置する。

5.1.6 媒体保管

セコムトラストシステムズは、アーカイブデータ、バックアップデータを含む認証業務

を行ううえで必要な情報を、適切な入退管理が行われた室内の保管庫に保存するとともに、毀損、滅失防止のための措置を施す。

5.1.7 廃棄処理

セコムトラストシステムズは、機密情報を含む書類および電子媒体の廃棄を、情報の初期化、裁断等により行う。

5.1.8 オフサイトバックアップ

セコムトラストシステムズは、認証基盤システムの運用のために必要なデータ、機器等を、遠隔地に保管するかまたは調達できる手段を講ずる。

5.2 手続的管理

5.2.1 信頼される役割

セコムトラストシステムズは、認証基盤システムの運用を行うために必要な役割を次のとおり定める。

(1) サービス責任者
- 電子認証基盤の統括
- 認証基盤システムの変更、運用手続変更の承認

(2) サービス運用管理者
- 運用担当者への作業指示
- CA 私有鍵に関する作業立会い
- サービス運用の全般管理

(3) CA 管理者
- CA サーバー、リポジトリーサーバー等、認証基盤システムの維持管理
- CA 私有鍵の活性化、非活性化等の操作

(4) RA 担当者
- 認証基盤システムを利用して RA 業務を行う顧客情報の登録・削除
- 認証基盤システムを利用してセコムトラストシステムズが提供するサービスの CA に関する RA 業務

(5) ログ検査者
- 入退室ログ、システムログ等の検査

5.2.2 職務ごとに必要とされる人数

セコムトラストシステムズは、サービス提供に支障をきたさないよう、サービス責任者を除く本 CPS「5.2.1 信頼される役割」に記載する役割に関し、複数名の要員を配置する。

なお、CA 私有鍵の操作等の重要な業務については複数名の要員で行う。

CA 私有鍵のバックアップ、保管、回復は、信頼済みロールを持つ担当者が、少なくとも物理的に安全な環境で、二重制御を用いながら行うものとする。

5.2.3 個々の役割に対する本人性確認と認証

セコムトラストシステムズは、認証局基盤システムへのアクセスに関し、物理的または論理的な方法によってアクセス権限者の識別と認証、および認可された権限の操作であることを確認する。

5.2.4 職務分割が必要となる役割

本 CPS「5.2.1 信頼される役割」に記載する役割は、原則として異なる要員がその役割を担う。なお、サービス運用管理者については、ログ検査者との兼務を可能とする。

EV Guidelines に準拠した EV TLS サーバー証明書を発行する下位 CA では以下を実施する。

1. 本 CA は、一人の担当者が単独で EV 証明書の検証と発行を許可できないことを保証するために検証義務を分離に関する厳格な管理手順を実施する。EV Guidelines セクション 3.2.2.13 で概説されている最終的な相互相関およびデューデリジェンスの手順は、一人の担当者が実行しても良い。例えば、一人目の検証スペシャリストがすべての申請者の情報を検証し、二人目の検証スペシャリストが TLS サーバー証明書の発行を承認することができる。
2. 本管理は、監査可能とする。

5.3 人事的管理

5.3.1 資格、経験および身分証明の要件

CA の従業員、代理人、または契約社員として個人を証明書管理プロセスに関与させる前に、CA は、かかる個人のアイデンティティと信頼性を検証するものとする。

5.3.2 背景調査

セコムトラストシステムズは、本 CPS「5.2.1 信頼される役割」に記載する役割を担う者の信頼性と適性を任命時および定期的に評価する。

EV プロセスに従事する従業員、代理人、または契約社員を雇用する前に、以下を実行する。

1. 当該人物のアイデンティティの検証 : アイデンティティの検証は、次のすべてを行う。

A. 人事またはセキュリティ職を務める信頼済みの人物に、当該人物を物理的に対面させる。

B. 官公庁発行の写真付き ID (パスポート、運転免許証など) の検証。

2. 当該人物の信頼性の検証 : 信頼性の検証には、少なくとも以下に相当する素性の確認を含める。

A. 前職の確認。

B. 経歴推薦状の確認。

C. 最終学歴または業務に最も関連する教育資格の確認。

5.3.3 教育要件

セコムトラストシステムズは、要員が役割に就く前に認証基盤システムの運用に必要な教育を実施し、以降、必要に応じ、役割に応じた教育・訓練を実施する。また、 業務手順に変更がある場合はその変更に関わる教育・訓練を実施する。

CA は、情報検証業務を実行するすべての要員に、基本的な公開鍵インフラストラクチャの知識、認証および検証ポリシーおよび手順（CA の CP/CPS を含む)、情報検証プロセ スに対する一般的な脅威（フィッシングおよびその他のソーシャル・エンジニアリング手法を含む)、および Baseline Requirements を網羅したスキル研修を提供するものとする。

CA は、かかる訓練の記録を維持し、検証スペシャリスト業務を委託された要員が、かかる業務を十分に 遂行できるスキルレベルを維持することを保証しなければならない。CA は、検証スペシャリストにそのタスクの実行を許可する前に、各検証スペシャリストがタスクに必要なスキルを有していることを文書化しなければならない。

CA は、すべての検証スペシャリストに対し、Baseline Requirements に概説されている情報検証要件に ついて CA が提供する試験に合格することを要求しなければならない。

5.3.4 再教育の頻度および要件

セコムトラストシステムズは、本 CPS「5.2.1 信頼される役割」に記載する役割を担う者に対して、必要に応じ再トレーニングを行う。

信頼される役割のすべての要員は、CA のトレーニングおよびパフォーマンスプログラムと一致したスキル レベルを維持するものとする。

5.3.5 仕事のローテーションの頻度および順序

セコムトラストシステムズは、サービス品質の維持、向上および不正防止の観点から、必要に応じて要員のジョブローテーションを行う。

5.3.6 認められていない行動に対する制裁

セコムトラストシステムズの就業規則の制裁に関する規定に従う。

5.3.7 業務委託先の管理

セコムトラストシステムズは、認証基盤システムの運用のすべてあるいは一部を外部組織に委託する場合、業務委託先との契約によって、業務委託先のもとで運用業務が適切に行われていることを確認する。

CA は、証明書の発行に携わる外部委託先の担当者が本 CPS「5.3.3 教育要件」ならびに本CPS「5.4.1 記録されるイベントの種類」を満たしていることを検証するものとする。

5.3.8 要員へ提供される資料

セコムトラストシステムズは、関連する業務上必要な文書のみの閲覧を要員に対して許可する。

5.4 監査ログの手続

5.4.1 記録されるイベントの種類

セコムトラストシステムズは、次の内容を監査ログとして記録する。

CA は、少なくとも以下のイベントを記録するものとする。

1. 以下を含む CA 証明書と鍵ライフサイクルイベント
   1. 鍵の生成、バックアップ、保管、回復、アーカイブ化、破棄。
   2. 証明書の要求、更新、鍵の再生成の要求、および失効。
   3. 証明書要求の承認と拒否。
   4. 暗号化デバイスライフサイクル管理イベント。
   5. 証明書失効リストと OCSP エントリの生成。
   6. OCSP 応答の署名。
   7. 新しい証明書プロファイルの導入と既存の証明書プロファイルの廃止。
2. 以下を含む加入者証明書ライフサイクル管理イベント
   1. 証明書の要求、更新、鍵の再生成要求、および失効化。
   2. Baseline Requirements および CA の証明書運用規定で定められたすべての検証アクション。
   3. 証明書要求の承認と拒否。
   4. 証明書の発行。
   5. 証明書失効リストの生成。
   6. OCSP 応答の署名。
3. 以下を含むセキュリティイベント

1. 成功および失敗した PKI システムアクセス試行。
2. 実行された PKI およびセキュリティシステムアクション。
3. セキュリティプロファイルの変更。
4. 証明書システムへのソフトウェアのインストール、更新、および削除。
5. システムクラッシュ、ハードウェア障害、およびその他の異常。
6. 関連するルーターおよびファイアウォールのアクティビティ。(本 CPS「5.4.1.1 ルーターとファイアウォールのアクティビティログ」を参照。TLS サーバー証明書および S/MIME 証明書の CA が対象)
7. CA 施設への出入記録。

ログ記録には、以下の要素を含める必要がある。

1. 記録の日時。
2. ジャーナルレコードを作成する人の身元。
3. 記録の詳細。

5.4.1.1 ルーターとファイアウォールのアクティビティログ

本 CPS「5.4.1　記録されるイベントの種類」3.6 の要件を満たすために必要なルーターとファイアウォールのアクティビティのログには、少なくとも次のものが含む。(TLS サーバー証明書および S/MIME 証明書の CA が対象)

1. ルーターとファイアウォールへのログイン試行の成功と失敗。
2. 構成の変更、ファームウェアの更新、アクセス制御の変更など、ルーターおよびファイアウォール上で実行されたすべての管理アクションのログ。
3. 追加、変更、削除を含む、ファイアウォール ルールに対して行われたすべての変更のログ。
4. ハードウェアの障害、ソフトウェアのクラッシュ、システムの再起動など、すべてのシステム イベントとエラーのログ。

5.4.1.2 タイムスタンプ局で記録されるイベントの種類

[コードサイニング証明書]

タイムスタンプ局は、以下の情報を記録し、タイムスタンプ機関が Baseline Requirements for Code Signing Certificates に準拠していることの証拠として、これらの記録を監査人が利用できるようにする。

1. タイムスタンプサーバーへの物理的またはリモートアクセス(アクセスの時刻およびサーバーにアクセスする個人の ID を含む)
2. タイムスタンプサーバー設定の履歴

3. タイムスタンプログを削除または変更しようとする試み
4. 以下を含むセキュリティイベント
   a. タイムスタンプ局のアクセス試行の成功と失敗
   b. 実行されたタイムスタンプ局サーバーアクション
   c. セキュリティプロファイルの変更
   d. システムクラッシュおよびその他の異常
   e. ファイアウォールとルーターのアクティビティ
5. タイムスタンプ証明書の失効
6. タイムスタンプサーバーの時刻の大幅な変更
7. システムの起動とシャットダウン。

5.4.2 監査ログを処理する頻度

セコムトラストシステムズは、監査ログを定期的に確認する。

5.4.3 監査ログを保持する期間

セコムトラストシステムズは、少なくとも 2 年間、以下を保持するものとする。

1.CA 証明書および鍵のライフサイクル管理イベント記録（本 CP「5.4.1 記録されるイベントの種類」に記載）は、以下のいずれかが発生した後に保持する。
   1. CA 私有鍵の破壊。
   2. cA フィールドが true に設定された X.509v3 basicConstraints 拡張を持ち、CA 私有鍵に対応する共通の公開鍵を共有する一連の証明書のうち、最後の CA 証明書の失効または有効期限切れ。
2. 加入者証明書の失効または満了後の加入者証明書ライフサイクル管理イベントレコード（本 CP「5.4.1 記録されるイベントの種類」に記載）。
3. イベント発生後のセキュリティイベントレコード（本 CP「5.4.1 記録されるイベントの種類」に記載）
4. コードサイニング証明書の場合、タイムスタンプ証明書私有鍵の失効または更新後のタイムスタンプ局データレコード(本 CPS「5.4.1.2 タイムスタンプ局で記録されるイベントの種類」に規定))、イベント発生後のセキュリティイベントレコード（本 CPS「5.4.1 記録されるイベントの種類」に記載）

5.4.4 監査ログの保護

セコムトラストシステムズは、認可された者のみが監査ログにアクセスすることができるよう、適切なアクセスコントロールを採用し、許可されていない者が閲覧できないようにする。

5.4.5 監査ログのバックアップ手続

監査ログは監査ログを生成する機器とは分離された安全なオフサイト環境にバックアップし保管する。

5.4.6 監査ログの収集システム

監査ログの収集システムは、認証基盤システムの機能に含まれている。

5.4.7 イベントを起こした者への通知

セコムトラストシステムズは、監査ログの収集を、事象を発生させた人、システムまたはアプリケーションに対して通知することなく行う。

5.4.8 脆弱性評価

セコムトラストシステムズは、監査ログの検査結果をもとに、運用面およびシステム動作面におけるセキュリティ上のぜい弱性を評価するとともに、必要に応じて最新の実装可能なセキュリティテクノロジの導入等、セキュリティ対策の見直しを行う。

さらに CA のセキュリティプログラムには、以下のような年次リスクアセスメントを含める必要がある。

1. 証明書データまたは証明書管理プロセスに対する不正なアクセス、開示、不正使用、改変、または破壊につながる、予測可能な内外の脅威を特定する。
2. 証明書データおよび証明書管理プロセスの機密性を考慮して、これらの脅威の可能性及び潜在的な損害を評価する。
3. このような脅威に対抗するために CA が導入しているポリシー、手順、情報システム、技術、およびその他の取り決めが十分であるかどうかを評価する。

5.5 記録の保管

5.5.1 アーカイブの種類

セコムトラストシステムズは、本 CPS「5.4.1 記録されるイベントの種類」の認証局システムに関するログに加えて、次の情報をアーカイブとして保存する。

- 証明書システム、証明書管理システム、ルート CA システム、および委任されたサードパーティシステムのセキュリティに関連する文書
- 証明書要求と証明書の検証、発行、および失効に関連するドキュメント

電子認証基盤の上で運用される CA 特有のアーカイブ情報については CP に規定する。

5.5.2 アーカイブ保存期間

セコムトラストシステムズはアーカイブされた監査ログ(本 CPS「5.5.1　アーカイブの種類」で規定)は、記録作成タイムスタンプから少なくとも 2 年間、または本 CPS「5.4.3 監査ログを保持する期間」に従って保持する必要がある限り、いずれか長い方の期間保持する。

さらに、CA および委任された第三者は、少なくとも 2 年間、以下を保持するものとする。

1. 証明書システム、証明書管理システム、ルート CA システムおよび委任された第三者システムのセキュリティに関連するすべてのアーカイブされた文書（本 CPS「5.5.1　アーカイブの種類」参照）
2. 証明書の要求および証明書の検証、発行、および失効（本 CPS「5.5.1　アーカイブの種類」参照）に関連するすべてのアーカイブ文書。
   i. 記録と文書は、証明書の要求と証明書の検証、発行または失効において最後に依拠した場合。
   ii. 当該記録と文書に依拠した加入者証明書の有効期限。

5.5.3 アーカイブの保護

アーカイブは、許可された者以外が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、認証基盤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

セコムトラストシステムズは、NTP（Network Time Protocol）を使用して認証基盤システムの時刻同期を行い、認証基盤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、認証基盤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

本項は、電子認証基盤の上で運用される CA の CP に規定する。

5.7 危殆化および災害からの復旧

5.7.1 事故および危殆化時の手続

CA 私有鍵が危殆化または危殆化のおそれがある場合および災害等により本サービスの中断、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、安全にサービスを再開させる。

CA は、インシデント対応計画および災害復旧計画を準備するものとする。

CA は、災害、セキュリティの危殆化、または企業倒産が発生した場合にアプリケーションソフトウェアサプライヤー、加入者、および依拠当事者に通知し、それらを合理的に保護するように設計された、事業継続および災害復旧手順を文書化するものとする。CA は事業継続計画を公開する必要はないが、CA の監査人が要求した時には事業継続計画とセキュリティ計画を提供できるようにするものとする。CA は、年 1 回これらの手順をテスト、レビュー、および更新するものとする。

事業継続計画には以下を含めなければならない。

1. 計画を始動するための条件
2. 緊急対応手順
3. フォールバック手順
4. 再開手順
5. 計画の保守スケジュール
6. 意識向上および教育要件
7. 個人の責任範囲
8. 目標復旧時間(RTO)
9. 緊急対策計画の定期的なテスト
10. 重要な事業プロセスの中断または障害発生後、タイムリーに CA の事業運営を維持または復元するための計画
11. 重要な暗号化資材(つまり、セキュリティ保護された暗号化装置やアクティベーション資材)を代替場所に保管するための要件
12. 容認可能なシステム停止期間および回復時間
13. 必須の事業情報およびソフトウェアのバックアップコピーの作成頻度
14. 復旧施設から CA のメインサイトまでの距離
15. 災害発生から元のサイトまたはリモートサイトで安全な環境を復元するまでの期間に可能な範囲で設備を保護するための手順

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

セコムトラストシステムズは、認証基盤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、すみやかに認証基盤システムの復旧作業を行う。

5.7.3 私有鍵が危殆化した場合の手続

利用者は、利用者の私有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 に対してすみやかに証明書の失効申請を行わなければならない。本 CA は、失効申請を受け付けた場合、電子認証基盤で運用される CA の CP「4.9 証明書の失効と一時停止」に示す手続に従って、証明書の失効を行う。

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、アプリケーションソフトウェアサプライヤーを含む関係者に通知し安全に運用を再開させる。

5.7.4 災害後の事業継続性

セコムトラストシステムズは、不測の事態が発生した場合にすみやかに復旧作業を実施できるよう、予め認証基盤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、可能な限りすみ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

本項は、電子認証基盤の上で運用される CA の CP に規定する。

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

本項について、本 CPS では、電子認証基盤の上で運用される CA の鍵管理に関して規定する。証明書利用者を含むその他関係者に関する鍵管理については CP に規定する。

6.1.1 鍵ペアの生成

ルート CA の鍵ペアに対しては以下の管理を行う。

1. 鍵生成スクリプトを用意して、それに従って実施する。
2. 公認監査人に CA 鍵ペア生成プロセスに立ち会わせる。（CA/Browser Forum で定められた規準に準拠した CA）
3. 公認監査人に、CA が鍵と証明書の生成プロセス中においてキーセレモニーを行ったこと、また鍵ペアの整合性と機密性を保証するための統制を実施したことについての見解を示すレポートを発行させる。

下位 CA の鍵ペアに対しては以下の管理を行う。

1. 鍵生成スクリプトを用意して、スクリプトに従って実施する。
2. 公認監査人に CA 鍵ペア生成プロセスに立ち会わせる。（CA/Browser Forum で定められた規準に準拠した CA）

本 CA は以下を実施するものとする。

1. CA の CP/CPS の内容に従って物理的に保護された環境で CA 鍵ペアを生成する。
2. 複数人物による統制および知識分割の原則に基づく信頼された役割の担当者により CA 鍵ペアを生成する。
3. CA の CP/CPS で公開されている適切な技術および事業要件を満たす暗号化モジュール内で CA 鍵ペアを生成する。本 CA の鍵ペアは FIPS140-1 レベル 3 の認定を取得したハードウェアセキュリティモジュール（Hardware Security Module：以下、「HSM」という）上で生成する。
4. CA 鍵ペア生成アクティビティをログ記録する。
5. 私有鍵が CP/CPS および鍵生成スクリプトに記載されている手順に従って生成および保護されたことを合理的に保証する効果的な統制を維持する。

Baseline Requirements に準拠した TLS サーバー証明書の加入者証明書の鍵ペア生成に関しては、次の条件の 1 つ以上が満たされた場合、下位 CA は証明書要求を拒否する必要がある。下位 CA は以下を実施するものとする。

1. 鍵ペアが本 CPS「6.1.5 鍵サイズ」または本 CPS「6.1.6 公開鍵のパラメータの生成

および品質検査」に記載されている要件を満たしていない。

2. 私有鍵の生成に使用された特定の方法に欠陥があるという明確な証拠がある。
3. 下位 CA は、申請者の私有鍵を危殆化させる、実証済みまたは証明された方法を認識している。
4. 下位 CA は、CP「4.9.3　失効申請手続」および CP「4.9.12　鍵の危殆化に対する特別要件」に記載される本 CA の失効要求手続きを用いて、申請者の私有鍵が危殆化したことを事前に通知されている。
5. 公開鍵は、業界で実証された脆弱な私有鍵に対応する。2024 年 11 月 15 日以降の申請については、少なくとも以下の予防措置を講じる。
    1. Debian weak keys 脆弱性（https://wiki.debian.org/SSLkeys）の場合、本 CA は、リポジトリーに記載される鍵の種類（RSA、 ECDSA 等）およびサイズごとに https://github.com/cabforum/Debian-weak-keys/ で発見されたすべての鍵を拒否する。8192 ビットを超える RSA 鍵サイズを除き、本 CPS「6.1.5　鍵サイズ」の要件を満たすその他の鍵について、本 CA は、Debian weak keys を拒否する。
    2. ROCA 脆弱性の場合、本 CA は、 https://github.com/crocs-muni/roca または同等のツールによって識別される鍵を拒否する。
    3. Close Primes 脆弱性(https://fermatattack.secvuln.info/)の場合、本 CA は、フェルマーの因数分解法を用いて 100 ラウンド以内に因数分解できる弱い鍵を拒否する。

利用者証明書に、id-kp-serverAuth[RFC5280] または anyExtendedKeyUsage[RFC5280]のいずれかの値を含む extKeyUsage 拡張が含まれる場合、本 CA は、利用者に代わって鍵ペアを生成してはならず、また本 CA が以前に生成した鍵ペアを使用する証明書要求を受理しない。

6.1.2　証明書利用者に対する私有鍵の交付

本項は、電子認証基盤の上で運用される CA の CP に規定する。

6.1.3　認証局への公開鍵の交付

電子認証基盤の上で運用される CA に対する証明書利用者の公開鍵の送付は、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/TLS により暗号化を行う。

6.1.4　検証者への CA 公開鍵の交付

本項は、電子認証基盤の上で運用される CA の CP に規定する。

6.1.5 鍵サイズ

Baseline Requirements に準拠した TLS サーバー証明書、S/MIME Baseline Requirements に準拠した S/MIME 証明書、AATL ドキュメントサイニング証明書、AATL タイムスタンプ証明書を発行する場合は、次のことを行う必要がある。

RSA 鍵ペアの場合

・エンコードされる時点での法の長さは、少なくとも 2048 ビットであることを確認する。

・係数のサイズ（ビット単位）が 8 で割り切れるのを確認する。

ECDSA 鍵ペアの場合

・キーが NIST P-256、NIST P-384 楕円曲線上の有効な点を表していることを確認する。

Baseline Requirements for Code Signing Certificates に準拠したコードサイニング証明書およびタイムスタンプ証明書を発行する場合は、次のことを行う必要がある。

RSA 鍵ペアの場合

・エンコードされる時点での法の長さは、少なくとも 3072 ビットであることを確認する。

・係数のサイズ（ビット単位）が 8 で割り切れるのを確認する。

ECDSA 鍵ペアの場合

・キーが NIST P-256、NIST P-384 楕円曲線上の有効な点を表していることを確認する。

他のアルゴリズムや鍵サイズは許可されていないことを確認する。

上記以外の証明書の鍵ペアは、RSA 方式で鍵長 1024 ビット、2048 ビット、3072 ビットまたは 4096 ビット、ECDSA 方式で鍵長 256 ビットまたは 384 ビットとする。

6.1.6 公開鍵のパラメータの生成および品質検査

認証基盤システムで使用する HSM は、暗号機能の品質検査機能を有する。公開鍵のパラメータは、品質検査の行われた暗号機能を用いて生成される。

RSA

本 CA は、公開指数の値が 3 以上の奇数であることを確認する。加えて、公開指数は 2^16+1 および 2^256-1 の範囲内であるべきとする。法の特性として、奇数であること、素数の累乗ではないこと、752 より小さい因数がないこととする。[参照: Section 5.3.3, NIST SP 800-89].

ECDSA

本 CA は、ECC Full Public Key Validation Routine または ECC Partial Public Key Validation Routine を使用して、すべての鍵の有効性を確認する。[参照: Sections 5.6.2.3.2 and 5.6.2.3.3, respectively, of NIST SP 800-56A: Revision 2]

6.1.7 鍵の用途

本項は、電子認証基盤の上で運用される CA の CP に規定する。

6.2 私有鍵の保護および暗号モジュール技術の管理

本 CA は、不正な証明書発行を防止するための物理的および論理的な保護対策を実装する。前述の検証済みのシステムまたはデバイス外部での CA 私有鍵の保護は、CA 私有鍵の開示を防止する方法で実装された、物理セキュリティ、暗号化、またはその両方の組み合わせから構成する。CA は、暗号化された鍵または鍵の一部の残存期間中、暗号解読攻撃に耐えることができる最先端技術のアルゴリズムおよび鍵長によって、私有鍵を暗号化する。

6.2.1 暗号モジュールの標準および管理

電子認証基盤の上で運用される CA の私有鍵の生成、保管、署名操作は、FIPS140-2 レベル 3 準拠の HSM を用いて行う。

6.2.2 私有鍵の複数人管理

電子認証基盤の上で運用される CA の私有鍵の活性化、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。

6.2.3 私有鍵のエスクロー

電子認証基盤の上で運用される CA の私有鍵のエスクローは行わない。

6.2.4 私有鍵のバックアップ

電子認証基盤の上で運用される CA の私有鍵のバックアップは、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。

6.2.5 私有鍵のアーカイブ

電子認証基盤の上で運用される CA 私有鍵のアーカイブは行わない。

6.2.6 私有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

電子認証基盤の上で運用される CA の私有鍵の HSM への転送または HSM からの転送は、セキュアな室において、私有鍵を暗号化した状態で行う。

6.2.7 暗号モジュールへの私有鍵の格納

電子認証基盤の上で運用される CA の私有鍵は、暗号化された状態で HSM 内に格納する。HSM は、FIPS 140-2 level 3, FIPS 140-3 level 3, Common Criteria Protection Profile または Security Target, EAL 4 以上を満たすものとする。

6.2.8 私有鍵の活性化方法

電子認証基盤の上で運用される CA の私有鍵の活性化は、セキュアな室において複数名の権限者によって行う。

6.2.9 私有鍵の非活性化方法

電子認証基盤の上で運用される CA の私有鍵の非活性化は、セキュアな室において複数名の権限者によって行う。

6.2.10 私有鍵の破棄方法

電子認証基盤の上で運用される CA の私有鍵の廃棄は、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。

6.2.11 暗号モジュールの評価

認証基盤システムで使用する HSM の品質基準については、本 CPS「6.2.1 暗号モジュールの標準および管理」のとおりである。

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

電子認証基盤の上で運用される CA の公開鍵のアーカイブは、本 CPS「5.5.1 アーカイブの種類」に含まれる。

6.3.2 私有鍵および公開鍵の有効期間

電子認証基盤の上で運用される CA の鍵ペアの有効期間は定めないが、CA 証明書の有効期間は 20 年以下を想定している。

2020 年 9 月 1 日以降に発行される Baseline Requirements に準拠した TLS サーバー証明書は、397 日を超えるべきではなく、398 日を超える有効期間を設定してはならない。2018 年 3 月 1 日以降、2020 年 9 月 1 日より前に発行された TLS サーバー証明書は、有

効期間が 825 日を超えてはならない。2016 年 7 月 1 日以降、2018 年 3 月 1 日より前に発行された TLS サーバー証明書は、有効期間が 39 か月を超えてはならない。

EV Guidelines に準拠した EV TLS サーバー証明書は、398 日を超える有効期間を設定しない。

Baseline Requirements for Code Signing Certificates に準拠したコードサイニング証明書の有効期間は、39 か月を超えてはならない。コードサイニング証明書に使用されるタイムスタンプ局は、タイムスタンプ証明書の私有鍵が危殆化した場合のユーザーへの影響を最小限にするために、15 か月ごとに新しい私有鍵を持つ新しいタイムスタンプ証明書を使用しなければならない。

タイムスタンプ証明書の有効期間は、135 か月を超えてはならない。

2022 年 4 月 1 日以降に発行される Mozilla Root Store Policy, Apple Root Certificate Program および S/MIME Baseline Requirements に準拠した S/MIME 証明書は、825 日を超える有効期間を設定してはならない。

下位 CA 証明書が「Security Communication RootCA 下位 CA 用証明書ポリシー」に準拠している、上記以外の加入者証明書は、1827 日を超える有効期間を設定してはならない。

OCSP 証明書は、125 日を超える有効期間を設定してはならない。

計算上、1 日は 86,400 秒となる。これを超える時間は、小数点以下の秒数やうるう秒を含めて、追加の 1 日を意味する。このため、加入者証明書は、そのような調整を考慮して、デフォルトでは、最大許容時間で発行すべきではない。

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

電子認証基盤の上で運用される CA の私有鍵を操作するために必要な活性化データは、複数名の権限者によって生成され、電子媒体に格納する。

6.4.2 活性化データの保護

電子認証基盤の上で運用される CA の私有鍵の活性化に必要なデータが格納された電

子媒体は、セキュアな室において保管管理を行う。

6.4.3 活性化データの他の考慮点

電子認証基盤の上で運用される CA の私有鍵の活性化データの生成や設定等の管理は、本 CPS「5.2.1 信頼される役割」に記載された者が行う。

6.5 コンピュータのセキュリティ管理

6.5.1 コンピュータセキュリティに関する技術的要件

セコムトラストシステムズは、認証基盤システムに導入するハードウェア、ソフトウェアに対して、その品質、安定性、安全性等について十分に検討を行い、導入を決定する。

本 CA は、証明書を直接発行させることができるすべてのアカウントに対して、多要素認証を実施するものとする。

6.5.2 コンピュータセキュリティ評価

セコムトラストシステムズは、認証基盤システムにおいて使用するすべてのソフトウェア、ハードウェアに対して事前にシステムテストを行い、認証基盤システムの信頼性の確保に努める。また、認証基盤システムのセキュリティ上の脆弱性についての情報収集、評価を継続的に行い、脆弱性が発見された場合には、すみやかに必要な対処を行う。

6.6 ライフサイクルセキュリティ管理

6.6.1 システム開発管理

認証基盤システムの構築およびメンテナンスは、安全な環境下で行う。認証基盤システムの変更を行う場合は、十分に安全性の評価、確認を行う。また、認証基盤システムに対して、適切なサイクルで最新のセキュリティ技術を導入するためにセキュリティチェックを行い、セキュリティを確保する。

6.6.2 セキュリティ運用管理

セコムトラストシステムズは、情報資産管理、要員管理、権限管理等の運用管理の実施、不正侵入対策、ウイルス対策等のセキュリティ対策ソフトウェアの適時更新等を行い、セキュリティを確保する。

6.6.3 ライフサイクルセキュリティ管理

セコムトラストシステムズは、認証基盤システムのシステム開発、運用、保守が適切に行われていることを適時評価し、必要に応じ改善を行う。

6.7 ネットワークセキュリティ管理

セコムトラストシステムズは、認証基盤システムへのネットワークからの不正アクセス対策として、ファイアウォール、IDS 等を設置する。

6.8 タイムスタンプ

タイムスタンプに関する要件は、本 CPS「5.5.5 記録にタイムスタンプを付与する要件」と同様とする。

7. 証明書および証明書失効リストのプロファイル

7.1 証明書プロファイル

7.1.1 バージョン番号

本項は、電子認証基盤の上で運用される CA の CP に規定する。

7.1.2 証明書の拡張

本項は、電子認証基盤の上で運用される CA の CP に規定する。

7.1.3 アルゴリズムオブジェクト識別子

本項は、電子認証基盤の上で運用される CA の CP に規定する。

7.1.4 名前の形式

本項は、電子認証基盤の上で運用される CA の CP に規定する。

7.1.5 名前制約

本項は、電子認証基盤の上で運用される CA の CP に規定する。

7.1.6 証明書ポリシーオブジェクト識別子

本項は、電子認証基盤の上で運用される CA の CP に規定する。

7.1.7 ポリシー制約拡張の使用

本項は、電子認証基盤の上で運用される CA の CP に規定する。

7.1.8 ポリシー修飾子の構文および意味

本項は、電子認証基盤の上で運用される CA の CP に規定する。

7.1.9 クリティカルな証明書ポリシー拡張に対する解釈の方法

本項は、電子認証基盤の上で運用される CA の CP に規定する。

7.2 CRL プロファイル

7.2.1 バージョン番号

本項は、電子認証基盤の上で運用される CA の CP に規定する。

7.2.2 証明書失効リストおよび証明書失効リストエントリ拡張

本項は、電子認証基盤の上で運用される CA の CP に規定する。

7.3 OCSP プロファイル

7.3.1 バージョン番号

本項は、電子認証基盤の上で運用される CA の CP に規定する。

7.3.2 OCSP 拡張

本項は、電子認証基盤の上で運用される CA の CP に規定する。

8. 準拠性監査と他の評価

本 CA は、常に以下の条件を満たすものとする。

1. 業務を行うすべての地域においてその事業および発行する証明書に適用されるすべての法規に従って証明書を発行し、PKI を運用する。
2. Baseline Requirements に従う。
3. 本 CP で規定されている監査要件に従う。
4. 業務を行う各地域において CA としての認可を受ける(証明書の発行に対して、該当地域の法令によって認可が必要な場合)。

8.1 監査の頻度

セコムトラストシステムズは、電子認証基盤の運用が本 CPS に準拠して行われているかについて、適時、監査を行う。

新しい加入者証明書を発行するために使用することができる証明書は、本 CP「7.1.5 名前制約」に従って技術的に制約され、かつ本 CP「8.7 自己監査」に従って監査されているか、制約はされていないものの、このセクションの残りすべての要件に従って完全に監査されているかのいずれかである必要がある。証明書は、X.509v3 basicConstraints 拡張領域を含み、cA boolean が true に設定された、ルート CA 証明書または下位 CA 証明書である場合、新規証明書の発行に使用可能と見なされる。

本 CA が加入者証明書を発行している期間は、監査期間の連続したシーケンスに分割されるものとする。監査期間は 1 年を超えてはならない。

本 CA が、本 CPS「8.4 監査で扱われる事項」に記載された監査スキームに準拠していることを示す現在有効な監査レポートを有している場合、発行前準備の評価は必要ない。

本 CA が、本 CPS「8.4 監査で扱われる事項」に記載された監査スキームのいずれかに準拠していることを示す現在有効な監査レポートを有していない場合、本 CA は、パブリックな信頼された加入者証明書を発行する前に、本 CPS「8.4 監査で扱われる事項」に記載された監査スキームのいずれかに基づき、適用される規準に従って実施される時点での準備状況の評価を完了しなければならない。当該準備状況の評価は、パブリック証明書を発行する 12 か月前までに完了し、最初のパブリック証明書を発行してから 90 日以内に、当該スキームに基づく完全な監査を受けなければならない。

8.2 監査人の身元／資格

本 CA の監査は、公認監査人が行わなければならない。公認監査人とは、以下の資格および技能を総合的に有する自然人、法人、または自然人もしくは法人のグループをいう。

1. 監査の対象から独立している。
2. 適格な監査スキームで指定されている条件に対応する監査を実施できる(本 CPS

「8.4 監査で扱われる事項」を参照)。

3. 公開鍵基盤技術、情報セキュリティツールおよび技法、情報技術およびセキュリティ監査、および第三者認証機能の審査に熟達している人材を採用している。
4. (WebTrust 規格に基づいて実施される監査の場合)WebTrust による実施許可を受けている。
5. 法律、政府の規制、または職業倫理に準拠している。
6. 国内政府監査機関の場合を除き、少なくとも 100 万米ドルの補償を保険範囲とする業務上の過失および不備に対する責任保険に加入している。

8.3 監査人と被監査部門の関係

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。監査の実施にあたり、被監査部門は監査に協力するものとする。

8.4 監査で扱われる事項

本 CA は、必要に応じて以下の WebTrust 規準に従って監査を受けるものとする。

・WebTrust for CAs
・WebTrust for CAs SSL Baseline with Network Security
・WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL
・WebTrust Principles and Criteria for Certification Authorities - Network Security
・WebTrust Principles and Criteria for Certification Authorities – Publicly Trusted Code Signing Certificates
・WebTrust Principles and Criteria for Certification Authorities - S/MIME

監査が継続的にスキームの要件に従って実施されるようにするため、定期的な監査手順や説明責任手順を組み込む必要がある。
監査は、本 CPS「8.2 監査人の身分と資格」の規定どおり、公認監査人によって実施される必要がある。

外部委託先がエンタープライズ RA でない場合、本 CA は、本 CPS「8.4 監査で扱われる事項」に記載された容認されている監査スキームの基になる監査標準に従って発行された監査レポートを取得するものとする。この監査レポートは、外部委託先の遂行する監査が外部委託先の運用規定または本 CA の CP/CPS に準拠するかどうかについての意見を提供する。外部委託先が条件に準拠しないという意見である場合、本 CA は、外部委託先による委託職務の履行継続を許可しないものとする。

外部委託先による監査期間は、1 年を超えないものとする(この場合、本 CA の監査と整合することが望ましい)。

8.5 不備の結果としてとられる処置

セコムトラストシステムズは、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

監査結果は、監査人からセコムトラストシステムズに対して報告される。

セコムトラストシステムズは、法律に基づく開示要求があった場合、セコムトラストシステムズ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、および認証サービス改善委員会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。

監査レポートは、本 CPS「7.1.6 CP オブジェクト識別子」に記載されたポリシー識別子の 1 つ以上を表示しているすべての証明書の発行で使用された関連システムやプロセスを対象としていることを明示するものとする。本 CA は、Baseline Requirements で求められた監査レポートは公開するものとする。3 か月を越えて遅延し、アプリケーションソフトウェアサプライヤーによって要求された場合、CA は、公認監査人によって署名された説明書簡を提供するものとする。

監査レポートのドキュメントには、少なくとも以下の明確にラベル付けされた情報を含めなければならない。

1. 監査対象の組織の名前
2. 監査を実施する組織の名前と住所
3. 主任監査人の名前と監査を行うチームの資格
4. 監査の範囲内にあった、クロス証明書を含む、すべてのルートおよび下位 CA 証明書の SHA-256 フィンガープリント
5. 各証明書（および関連するキー）を監査するために使用された監査基準とバージョン番号
6. 監査中に参照される CA ポリシードキュメントとバージョン番号のリスト
7. 監査が期間または時点を評価したかどうか
8. 期間を対象とする監査期間の開始日と終了日
9. ある時点のものである場合は、その時点の日付
10. レポートが発行された日付。これは必ず終了日または特定の時点より後の日付になる
11. 監査期間中に起票され、Bugzilla に公開されていた「CA が開示、監査人が発見、第三者が報告した」すべてのインシデント
12. 監査された、または監査されなかった CA 拠点

公に入手可能な監査情報の信頼できる英語版は、公認監査人によって提供されなければならず、本 CA はそれが公に入手可能であることを保証するものとする。

監査レポートは PDF として利用可能でなければならず、必要なすべての情報をテキス

トで検索できる必要がある。監査レポート内の各 SHA-256 フィンガープリントは大文字にする必要があり、コロン、スペース、または改行を含めることはできない。

8.7 自己監査

本 CA が証明書を発行する期間中、本 CA は、前の自己監査でサンプルが取得された直後から始まる期間に発行された Baseline Requirements に準拠した証明書のうち 2 つ以上、または 3%（EV TLS サーバー証明書の場合は 6%）のいずれか多い方の数の証明書をサンプルとしてランダムに選択し、少なくとも四半期に 1 回の頻度で自己監査を実施して、CP/CPS、および Baseline Requirements への準拠を監視し、サービス品質を厳密に管理するものとする。本 CPS「8.4 監査で扱われる事項」に規定されている条件を満たす年次監査対象の外部委託先を除き、本 CA は、最後のサンプルが取得された直後から始まる期間に外部委託先によって検証された Baseline Requirements に準拠した証明書のうち 2 つ以上、あるいは 3%（EV TLS サーバー証明書の場合は 6%）のいずれか多い方の数の証明書をサンプルとしてランダムに選択し、本 CA が雇用する検証スペシャリストに四半期に 1 回の監査を継続的に実施させることで、外部委託先によって発行された証明書または検証された情報を含む証明書のサービス品質を厳密に管理するものとする。本 CA は、各外部委託先の運用および手順をレビューして、外部委託先が Baseline Requirements、ならびに関連する CP/CPS に準拠していることを保証するものとする。本 CA は、年 1 回の頻度で、各外部委託先が Baseline Requirements に準拠しているかどうかを内部監査するものとする。

技術的に制約された CA が Baseline Requirements に準拠した証明書を発行する期間中、本 CA の CP への準拠状況を監視するものとする。本 CA は、少なくとも四半期に 1 回の頻度で、最後のサンプルが取得された直後から始まる期間において CA によって発行された証明書のうち 2 つ以上、あるいは 3%（EV TLS サーバー証明書の場合は 6%）のいずれか多い方の数の証明書をサンプルとしてランダムに選択し、適用されるすべての証明書ポリシーに準拠していることを確認する。

9. 他の業務上および法的事項

9.1 料金

9.1.1 証明書の発行または更新にかかる料金

本項は、電子認証基盤の上で運用される CA の CP に規定する。

9.1.2 証明書のアクセス料金

本項は、電子認証基盤の上で運用される CA の CP に規定する。

9.1.3 失効またはステータス情報のアクセス料金

本項は、電子認証基盤の上で運用される CA の CP に規定する。

9.1.4 他サービスの料金

本項は、電子認証基盤の上で運用される CA の CP に規定する。

9.1.5 代金返金ポリシー

本項は、電子認証基盤の上で運用される CA の CP に規定する。

9.2 財務的責任

9.2.1 保険の補償

セコムトラストシステムズは、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。

9.2.2 その他の資産

規定しない。

9.2.3 エンドエンティティの保険または保証範囲

規定しない。

9.3 企業情報の機密性

9.3.1 機密情報の範囲

セコムトラストシステムズが保持する個人および組織の情報は、証明書、CRL、本 CPS および関連する CP の一部として明示的に公表されたものを除き、機密保持対象として扱

われる。セコムトラストシステムズは、法の定めによる場合および証明書利用者による事前の承諾を得た場合を除いてこれらの情報を社外に開示しない。かかる法的手続、司法手続、行政手続あるいは法律で要求されるその他の手続に関連してアドバイスする法律顧問および財務顧問に対し、セコムトラストシステムズは機密保持対象として扱われる情報を開示することができる。また会社の合併、買収あるいは再編成に関連してアドバイスする弁護士、会計士、金融機関およびその他の専門家に対しても、セコムトラストシステムズは機密保持対象として扱われる情報を開示することができる。

9.3.2 機密情報の範囲外の情報

証明書および 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。

- セコムトラストシステムズ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
- セコムトラストシステムズ以外の出所から、機密保持の制限無しにセコムトラストシステムズに知られた、あるいは知られるようになった情報
- セコムトラストシステムズ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

セコムトラストシステムズは、法の定めによる場合および証明書利用者による事前の承諾を得た場合に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することはできない。

9.4 個人情報の保護

9.4.1 個人情報保護方針

セコムトラストシステムズは、当社の認証サービスの利用者から収集した個人情報を、申請内容の確認、必要書類等の送付、権限付与対象者の確認など電子認証基盤の上に構築する CA の運用に必要な範囲で利用する。セコムトラストシステムズの個人情報保護方針については、セコムトラストシステムズのホームページ(http://www.secomtrust.net)において公表する。

9.4.2 個人情報として扱われる情報

セコムトラストシステムズは、国内の法令に基づき個人情報として定められた情報（セコムトラスシステムズの認証サービスの利用者から収集した情報など）を個人情報として取り扱い、適切に管理する。

9.4.3 個人情報とみなされない情報

セコムトラストシステムズは、「9.4.2 個人情報として扱われる情報」に定めたとおり、個人情報を取り扱う。

9.4.4 個人情報を保護する責任

セコムトラストシステムズは、契約の実施および終結にあたり知りえた相手方の個人情報は、契約期間中と契約終了後であるとを問わず、一切第三者に漏洩してはならないものとする。電子認証基盤の上で運用される CA の運用における個人情報保護管理者を選任するものとし、個人情報保護管理者は個人情報の取り扱いに関し、サービスに従事する社員に対し社内規定を遵守させるものとする。

9.4.5 個人情報の使用に関する通知と同意

セコムトラストシステムズは、法令で定められた場合を除き、証明書利用者から同意を得た利用目的以外で個人情報を利用しない。個人番号、特定個人情報については、法令で認められた利用目的の範囲内、かつ証明書利用者から同意を得た利用目的で利用する。

9.4.6 司法または行政手続に沿った情報開示

法令、規則、裁判所の決定・命令、行政庁の命令・指示等により開示を要求された場合は、証明書利用者の個人情報を開示することができるものとする。

9.4.7 その他の情報開示条件

規定しない。

9.5 知的財産権

セコムトラストシステムズと証明書利用者、または契約先との間で別段の合意がなされない限り、本 CPS は著作権を含み、セコムトラストシステムズの権利に属するものとする。CA 特有の情報については CP に規定する。

本 CPS は、原文が適切に参照されることを条件に、複製することができる。「Creative Commons license Attribution-NoDerivatives (CC-BY-ND) 4.0」で公開する。

https://creativecommons.org/licenses/by-nd/4.0/

9.6 表明保証

9.6.1 CA の表明保証

本項は、電子認証基盤の上で運用される CA の CP に規定する。

9.6.2 RA の表明保証

本項は、電子認証基盤の上で運用される CA の CP に規定する。

9.6.3 証明書利用者の表明保証

本項は、電子認証基盤の上で運用される CA の CP に規定する。

9.6.4 検証者の表明保証

本項は、電子認証基盤の上で運用される CA の CP に規定する。

9.6.5 他の関係者の表明保証

本項は、電子認証基盤の上で運用される CA の CP に規定する。

9.7 無保証

本項は、電子認証基盤の上で運用される CA の CP に規定する。

9.8 責任の制限

本項は、電子認証基盤の上で運用される CA の CP に規定する。

9.9 補償

本項は、電子認証基盤の上で運用される CA の CP に規定する。

9.10 有効期間と終了

9.10.1 有効期間

本 CPS は、認証サービス改善委員会の承認により有効となる。本 CPS「9.10.2 終了」に規定する終了以前に本 CPS が無効となることはない。

9.10.2 終了

本 CPS は、「9.10.3 終了の効果と効果継続」に規定する内容を除き、セコムトラストシステムズが電子認証基盤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、セコムトラストシステムズと契約先と

の間で契約が終了する場合、またはセコムトラストシステムズが提供するサービス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、検証者、セコムトラストシステムズの契約先およびセコムトラストシステムズ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

セコムトラストシステムズは、証明書利用者、検証者および契約先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 CPS は、セコムトラストシステムズの判断によって適宜改訂され、認証サービス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 CPS を変更した場合、変更した本 CPS をすみやかに公表することをもって、関係者に対する告知とする。

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

本項は、電子認証基盤の上で運用される CA の CP に規定する。

9.13 紛争解決手続

本項は、電子認証基盤の上で運用される CA の CP に規定する。

9.14 準拠法

本項は、電子認証基盤の上で運用される CA の CP に規定する。

9.15 適用法の遵守

本項は、電子認証基盤の上で運用される CA の CP に規定する。

9.16 雑則

9.16.1 完全合意条項

本項は、電子認証基盤の上で運用される CA の CP に規定する。

9.16.2 権利譲渡条項

本項は、電子認証基盤の上で運用される CA の CP に規定する。

9.16.3 分離条項

CP およびサービス利用規定、本 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。

Baseline Requirements と本 CA が業務の遂行と証明書の発行を行う地域の法律、規制、行政命令(以下、「法律」という)との間に矛盾が生じる場合、本 CA は、矛盾する要件が地域で有効かつ合法となるために必要な最小限の範囲内で Baseline Requirements の修正を行うことができる。このことは、その法律の対象となる業務または証明書発行にのみ適用される。そのような場合、本 CA はただちに(また修正された要件に基づいて証明書を発行する前に)、本 CA の CPS の本項に、Baseline Requirements への修正を必要としている法律への詳細な参照と、本 CA によって実施された Baseline Requirements への具体的な修正を盛り込むものとする。

本 CA は（修正された要件に基づく証明書を発行する前に）CA/Browser Forum に対し、CPS に新たに追加された情報について、questions@cabforum.org 宛にメールを送信するとともに、それがパブリックメーリングリストに掲載されたこと、および https://cabforum.org/pipermail/public/ (または CA/Browser Forum が指定するその他のメールアドレスやリンク)で閲覧可能なパブリックメールアーカイブでインデックス化されたことを確認する通知を受信する必要がある。これにより、CA/Browser Forum は Baseline Requirements を改訂するかどうかを適宜検討できる。

法律が適用されなくなった場合、または Baseline Requirements が修正され、Baseline Requirements と法律を同時に遵守することが可能となった場合、本項に基づく本 CA の運用変更を中止する必要がある。前述した運用への適切な変更、本 CA の CPS に対する修正、および CA/Browser Forum への通知は、90 日以内に行われる必要がある。

9.16.4 強制執行条項

本項は、電子認証基盤の上で運用される CA の CP に規定する。

9.16.5 不可抗力

本項は、電子認証基盤の上で運用される CA の CP に規定する。

9.17 その他の条項

本項は、電子認証基盤の上で運用される CA の CP に規定する。