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

Version1.00

2006 年 3 月 23 日

セコムトラストネット株式会社

改版履歴		
版数	日付	内容
1.00	2006/03/23	初版発行

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、セコムトラストネット株式会社（以下、「セコムトラストネット」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、セコムトラストネットの認証局（以下、「CA」という）、及びセコムトラストネットのプライベート CA サービスの利用顧客の 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ネットが行う。
電子認証基盤は、認証局として失効情報及び CA 証明書等を公開するためのリポジトリサーバや、RA（Registration Authority：登録局）から IA（Issuing Authority：発行局）に対して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（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 及び CP を遵守し、運用しなければならない。
なお、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、セコムトラストネット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 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 認証局

CA（Certification Authority：認証局）は、IA 及び RA によって構成される。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ネット、又はセコムトラストネットのプライベート CA サービスの利用顧客である。

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、リポジトリの維持管理等を行う。電子認証基盤の上で運用される CA において、IA の運用はセコムトラストネットが行う。

1.3.1.2 RA

RA は、証明書の発行、取消を申請する申請者の実在性確認、本人性確認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。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ネット、又はセコムトラストネットのプライベート CA サービスの利用顧客が行う。

1.3.2 証明書利用者

証明書利用者とは、電子認証基盤の上で運用される CA から証明書の発行を受ける主体をいう。

1.3.3 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。

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、セコムトラストネットが行う。

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。
窓口 ： セコムトラストネット株式会社 CA サポートセンター
TEL ： 0422-76-2072

1.5.3 ポリシ適合性を決定する者
本 CPS の内容は､セコムトラストネットセキュリティポリシ委員会において決定される。

1.5.4 承認手続
本 CPS は、セコムトラストネットが作成・改訂を行い、セコムトラストネットセキュリティポリシ委員会の承認により発効される。

1.6 定義と略語

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。

電子認証基盤
セコムトラストネットの CA、及びセコムトラストネットのプライベート CA サービスの利用顧客の 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。

プライベート CA サービス
セコムトラストネット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
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。

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。

CP（Certificate Policy）：証明書ポリシ
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。

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。

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。

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。

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。

2. 公開とリポジトリの責任

2.1 リポジトリ

セコムトラストネットは、電子認証基盤の上で運用される CA のために、リポジトリを用意する。リポジトリは、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

証明書利用者及び検証者がオンラインによって閲覧可能となるように、セコムトラストネットは、本 CPS をリポジトリに格納する。
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 公開の時期又は頻度

本 CPS は、変更の都度、リポジトリに公開する。
電子認証基盤の上で運用される CA 特有の公開情報に関する公開の時期及び頻度ついては、電子認証基盤の上で運用される CA の CP に規定する。

2.4 リポジトリへのアクセス管理

リポジトリへのアクセス管理については、電子認証基盤の上で運用される CA の CP に規定する。

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又は仮名性
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、認証及び商標の役割
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。

3.2.3 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 申請手続及び責任
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 証明書申請の承認又は却下
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
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 検証者の公開鍵及び証明書の用途
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 証明書の更新事由
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。

4.6.2 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 鍵更新を伴う証明書の更新

4.7.1 更新事由
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。

4.7.2 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 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。

4.7.4 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及び実施
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及び実施
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

5.1 物理的管理

5.1.1 立地場所及び構造

セコムトラストネットは、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

セコムトラストネットは、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及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 電源及び空調

データセンターでは、瞬断及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、無停電電源装置及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

セコムトラストネットは、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、火災報知機及び消火設備を設置する。

5.1.6 媒体保管

セコムトラストネットは、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上で必要な情報を、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

セコムトラストネットは、機密情報を含む書類及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

セコムトラストネットは、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又は調達できる手段を講ずる。

5.2 手続的管理

5.2.1 信頼すべき役割

セコムトラストネットは、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、リポジトリサーバ等、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ネット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

セコムトラストネットは、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.信頼すべき役割」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。

5.2.3 個々の役割に対する本人性確認と認証
セコムトラストネットは、認証局基盤システムへのアクセスに関し、物理的又は論理的な方法によってアクセス権限者の識別と認証、及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.信頼すべき役割」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。

5.3 人事的管理

5.3.1 資格、経験及び身分証明の要件
本 CPS「5.2.1.信頼すべき役割」に記載する役割を担う者は、セコムトラストネットの採用基準に基づき採用された従業員とする。
認証基盤システムを直接操作する担当者には、専門のトレーニングを受け、PKI の概要とシステムの操作方法等を理解している者を配置する。

5.3.2 適正調査
セコムトラストネットは、本 CPS「5.2.1.信頼すべき役割」に記載する役割を担う者の信頼性と適性を任命時及び定期的に評価する。

5.3.3 教育要件
セコムトラストネットは、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。

5.3.4 再教育の頻度及び要件
セコムトラストネットは、本 CPS「5.2.1.信頼すべき役割」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。

5.3.5 仕事のローテーションの頻度及び順序
セコムトラストネットは、サービス品質の維持、向上及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
セコムトラストネットの終業規則の罰則に関する規定に従う。

5.3.7 業務委託先の管理

セコムトラストネットは、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。

5.3.8 要員へ提供される資料

セコムトラストネットは、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

セコムトラストネットは、次の内容を監査ログとして記録する。

(1) 認証局システムに関するログ

- 認証局の私有鍵の操作
- 認証局システムの起動･停止
- データベースの操作
- 権限設定の履歴
- 証明書の発行、失効の処理履歴
- CRL の発行の処理履歴

(2) 入退室・ネットワークに関するログ

- 認証基盤システムを設置する室への入退室に関する記録
- 認証基盤システムへの不正アクセスに関する記録

監査ログは、以下の項目を含む。

- 日付
- 時刻
- イベントを発生させた主体
- イベントの内容

5.4.2 監査ログを処理する頻度

セコムトラストネットは、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

セコムトラストネットは、認証局システムに関する監査ログを、アーカイブとして最低

10 年保存する。入退室、ネットワークに関するログについては最低 1 年間保存する。

5.4.4 監査ログの保護
セコムトラストネットは、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
監査ログはオフラインの記録媒体にバックアップとして取得し、それらの媒体を安全な場所に保管する。

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
セコムトラストネットは、監査ログの収集を、事象を発生させた人、システム又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
セコムトラストネットは、監査ログの検査結果をもとに、運用面及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。

5.5 記録の保管

5.5.1 アーカイブの種類
セコムトラストネットは、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。
- 発行した証明書及び CRL
- 本 CPS
- 本 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おいては、委託契約に関する書類
- 監査の実施結果に関する記録及び監査報告書

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
セコムトラストネットは、アーカイブを最低 10 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、取消又は 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
セコムトラストネットは、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及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 危殆化及び災害からの復旧

5.7.1 事故及び危殆化時の手続
セコムトラストネットは、事故及び危殆化が発生した場合に速やかに認証基盤システム及び関連する業務を復旧できるよう、以下を含む事故及び危殆化に対する対応手続を策定する。

- CA 私有鍵の危殆化
- 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、ソフトウェア又はデータが破損した場合の手続
セコムトラストネットは、認証基盤システムのハードウェア、ソフトウェア又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、ソフトウェア又はデータを使用して、速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
セコムトラストネットは、認証基盤システムを利用する 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、及び災害等により認証基盤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
セコムトラストネットは、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、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 認証局又は登録局の終了
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 鍵ペアの生成及びインストール

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

電子認証基盤の上で運用される CA の鍵ペアの生成には、FIPS140-2 レベル 3 準拠の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）を使用する。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。

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 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

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。

6.1.6 公開鍵のパラメータの生成及び品質検査

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。

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 私有鍵の保護及び暗号モジュール技術の管理

6.2.1 暗号モジュールの標準及び管理

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又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 への転送又は 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。

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又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及び管理」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 私有鍵及び公開鍵の有効期間
電子認証基盤の上で運用される CA の私有鍵の有効期間は 20 年以内とする。

6.4 活性化データ

6.4.1 活性化データの生成及び設定
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
規定しない。

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
セコムトラストネットは、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。

6.5.2 コンピュータセキュリティ評価
セコムトラストネットは、認証基盤システムにおいて使用する全てのソフトウェア、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、速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及びメンテナンスは、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

セコムトラストネットは、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

セコムトラストネットは、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

セコムトラストネットは、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. 証明書及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 ポリシ修飾子の構文及び意味
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 証明書失効リスト及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

8.1 監査の頻度

セコムトラストネットは、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。

8.2 監査人の身元／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ものとする。

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

監査は、電子認証基盤の運用の本 CPS に対する準拠性を中心とする。

8.5 不備の結果としてとられる処置

セコムトラストネットは、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、監査人からセコムトラストネットに対して報告される。
セコムトラストネットは、法律に基づく開示要求があった場合、セコムトラストネット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、及びセコムトラストネットセキュリティポリシ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。

9. 他の業務上及び法的事項

9.1 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。

9.2 財務的責任

セコムトラストネットは、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

セコムトラストネットが保持する個人及び組織の情報は、証明書、CRL、本 CPS 及び関連する 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。セコムトラストネットは、法の定めによる場合及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及び財務顧問に対し、セコムトラストネット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、金融機関及びその他の専門家に対しても、セコムトラストネット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。

- セコムトラストネット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
- セコムトラストネット以外の出所から、機密保持の制限無しにセコムトラストネットに知られた、あるいは知られるようになった情報
- セコムトラストネット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

セコムトラストネットは、法の定めによる場合及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

セコムトラストネットは、当社の認証サービスやプライベート CA サービスの利用顧客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。セコムトラストネットの個人情報保護方針については、セコムトラストネットのホームページ（http://www.secomtrust.net）において公表する。

9.5 知的財産権

セコムトラストネットと証明書利用者、又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、セコムトラストネット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。

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。

9.6.1.2 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。

9.6.2 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。

9.6.3 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。

9.6.4 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、セコムトラストネットセキュリティポリシ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、セコムトラストネット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、セコムトラストネットと契約先との間で契約が終了する場合、又はセコムトラストネット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、セコムトラストネットの契約先及びセコムトラストネット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

セコムトラストネットは、証明書利用者、検証者及び契約先に対する必要な通知をホームページ、電子メール又は書面等によって行う。

9.12 改訂

9.12.1 改訂手続

本 CPS は、セコムトラストネットの判断によって適宜改訂され、セコムトラストネットセキュリティポリシ委員会の承認によって発効する。

9.12.2 通知方法及び期間

本 CPS を変更した場合、変更した本 CPS を速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
規定しない。

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
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。

9.16.4 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。

9.17 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。