Security Communication RootCA

認証運用規定

2018年11月28日

Version 5.11

セコムトラストシステムズ株式会社

© 2003 SECOM Trust Systems Co.,Ltd.

改版履歴		
版数	日付	内容
V1.00	2003.09.29	初版発行
V2.00	2004.11.08	メジャーバージョンアップ Security Communication RootCA1 証明書ポリシ/認証運用規程を分割し、Security Communication RootCA1 認証運用規程を作成。 全体的に文言の見直しを実施。
V3.00	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
V4.00	2009.05.29	メジャーバージョンアップ Security Communication RootCA1 認証運用規程を Security Communication RootCA 認証運用規程とし、CA の私有鍵 Security Communication RootCA2 を追加する
V4.10	2012.02.15	・5.6 鍵の切り替え －証明書の更新を追記。
V4.20	2012.11.09	OCSP サーバーの運用開始にともなう修正
V5.00	2016.06.01	メジャーバージョンアップ CA の私有鍵 Security Communication RootCA3 を追加 CA の私有鍵 Security Communication ECC RootCA1 を追加
V5.10	2017.05.23	全体的な文言および体裁の見直し
V5.11	2018.11.28	全体的な文言および体裁の見直し

© 2003 SECOM Trust Systems Co.,Ltd.

目次

© 2003 SECOM Trust Systems Co.,Ltd.

© 2003 SECOM Trust Systems Co.,Ltd.

© 2003 SECOM Trust Systems Co.,Ltd.

© 2003 SECOM Trust Systems Co.,Ltd.

© 2003 SECOM Trust Systems Co.,Ltd.

1. はじめに

1.1 概要

Security Communication RootCA 認証運用規定（Certification Practice Statement：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」という）が運用する Security Communication RootCA1、Security Communication RootCA2、Security Communication RootCA3 および Security Communication ECC RootCA1（以下、「本 CA」という）が証明書の利用者に行う電子証明書（以下、「証明書」という）の発行・失効（以下、「本サービス」という）、本 CA の鍵管理、証明書を基礎とする公開鍵インフラストラクチャ（PKI：Public Key Infrastructure）の運用維持に関する諸手続等、運用に関するポリシを規定した文書である。

本 CA が発行する証明書は、発行対象とその公開鍵が一意に関連づけられることを証明する。本 CA の証明書発行における審査、登録および発行手続は、利用者が使用する証明書に応じた証明書ポリシ（Certificate Policy：以下、「CP」という）によって規定される。

本 CA は、https://www.cabforum.org/で公開される CA/ Browser Forum で定められた規定に準拠する。

なお、本 CPS の内容が CP の内容に抵触する場合は、CP が優先して適用されるものとする。また、セコムと利用者との間で別途契約書等が存在する場合、本 CPS および CP より契約書等の文書が優先される。

本 CPS は、認証業務に関する技術面、サービス面の発展や改良にともない、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。

また本 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 文書の名前と識別

本 CPS の正式名称は「Security Communication RootCA 認証運用規定」という。本サービスの運営母体であるセコムは、表「1.2-1 OID（セコム）」に示す、ISO によって割り振られたオブジェクト識別子（Object ID：OID）を使用する。

表 1.2-1 OID（セコム）

組織名	OID
セコムトラストシステムズ株式会社（SECOM Trust Systems Co.,Ltd.）	1.2.392.200091

本 CPS は、表「1.2-2 OID（本 CPS）」に示す OID により識別される。

表 1.2-2 OID（本 CPS）

© 2003 SECOM Trust Systems Co.,Ltd.

CPS	OID
Security Communication RootCA 認証運用規定	1.2.392.200091.100.901.3

本 CPS は、表「1.2-3 OID（CP)」に示す CP に適用する。

表 1.2-3 OID（CP）

CP	OID
Security Communication RootCA 下位 CA 用証明書ポリシ	1.2.392.200091.100.901.1 (Security Communication RootCA1) 1.2.392.200091.100.901.4 (Security Communication RootCA2) 1.2.392.200091.100.901.6 (Security Communication RootCA3) 1.2.392.200091.100.902.1 (Security Communication ECC RootCA1)
Security Communication RootCA タイムスタンプサービス用証明書ポリシ	1.2.392.200091.100.901.2 (Security Communication RootCA1) 1.2.392.200091.100.901.5 (Security Communication RootCA2) 1.2.392.200091.100.901.7 (Security Communication RootCA3) 1.2.392.200091.100.902.2 (Security Communication ECC RootCA1)

本サービスは、将来的に新たな CP を追加する場合がある。その都度、新たな CP と OID の対応を本 CPS に追加する。

1.3 PKI の関係者

1.3.1 CA

CA は、証明書の発行、失効、失効情報の開示、OCSP（Online Certificate Status Protocol）サーバーによる証明書ステータス情報の提供および保管等の業務を行う。

1.3.2 RA

RA は、証明書申請者となる組織、団体からの証明書発行、取消等の要求に対して実在性確認、本人性認証、運用規定の審査等を行う。

1.3.3 利用者

利用者とは、自ら鍵ペアを生成し、本 CA から証明書の発行を受ける組織または団体をいう。本 CA に証明書の発行申請を行い、発行された証明書を受容した時点で利用者となる。

© 2003 SECOM Trust Systems Co.,Ltd.

1.3.4 検証者

検証者とは、本 CA が発行した証明書の有効性を検証する者をいう。検証者は、本 CPS および CP の内容を検証者自身の利用目的に照らして評価したうえで検証しているとみなされる。

1.3.5 その他関係者

規定しない。

1.4 証明書の使用方法

1.4.1 適切な証明書の用途

本 CA は下位 CA の頂点として機能するルート CA であり、本 CPS「1.2 文書の名前と識別」に記載する CP に基づく証明書を発行する。検証者は、当該証明書の信頼性を本 CA の証明書によって検証することができる。

1.4.2 禁止される証明書の用途

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、セコムが行う。

1.5.2 連絡先

本 CPS に関する問い合わせ窓口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

1.5.3 ポリシ適合性を決定する者

本 CPS が、本 CA の運用方針として適切か否かの判断は、セコムの認証サービス改善委員会が行う。

1.5.4 承認手続

本 CPS は、セコムの認証サービス改善委員会による承認のもと、作成および変更がなされ、リポジトリーに公開される。

© 2003 SECOM Trust Systems Co.,Ltd.

1.6 定義と略語

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。

HSM(Hardware Security Module)

暗号や電子署名に利用する私有鍵を守る金庫の役目をするハードウェアのことをいい、暗号演算や電子署名演算、私有鍵や乱数の生成を行う。

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。

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。

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-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。

© 2003 SECOM Trust Systems Co.,Ltd.

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。

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。

あ～ん

エスクロー

第三者に預けること（寄託）をいう。

オブジェクト識別子（OID）

Object Identificationの略。世界で一意となる値を登録機関（ISO 、ITU）に登録した識別子。PKI で使うアルゴリズム、証明書内に格納する名前（subject）のタイプ（Country 名等の属性）等は、オブジェクト識別子として登録されているものが使用される。

下位 CA

本 CA が信頼し署名した CA をいう。

鍵ペア

公開鍵暗号方式における私有鍵と公開鍵から構成される。

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。私有鍵に対応する、公開されている鍵。

私有鍵

© 2003 SECOM Trust Systems Co.,Ltd.

公開鍵暗号方式において用いられる鍵ペアの一方。公開鍵に対応する、利用者のみが保有する鍵。

証明書

電子証明書の略。ある公開鍵を、記載されたものが保有することを証明する電子的文書。CA が電子署名を施すことで、その正当性が保証される。

証明書失効リスト(CRL)

Certificate Revocation List の略。本 CA によって失効された証明書情報の一覧が記録されている。

証明書発行要求(CSR)

Certificate Signing Request の略。証明書を発行する際の元となるデータファイル。CSR には証明書の発行要求者の公開鍵が含まれており、その公開鍵に発行者の署名を付与して証明書を発行する。

証明書ポリシ（CP）

Certificate Policy の略。証明書に関するポリシを規定している文書。

タイムスタンプ

電子情報と時刻情報を含めた情報であり、その時刻以前にそのデータが存在したことの証明（存在証明）と、その時刻から検証した時刻までの間にそのデータが変更・改ざんされていないことを証明（非改ざん証明）する事ができる手段、およびその証拠に結びつく情報のことをいう。

本サービスでは、タイムスタンプを行う TSA（Time Stamping Authority：タイムスタンプ局）および TSA に対し標準時の配信、時刻監査を行う TA（Time Authority：標準時配信局）向けの証明書を発行する。

電子署名

特定の人物が特定の電子文書の作成者であることを証明する電子的な情報であり、当該文書に含まれる情報の信頼性を作成者が保証していることを意味する署名である。

登録局（RA）

Registration Authority の略。本サービスでは CA の業務のうち、審査業務を行う機関。

認証運用規定（CPS）

Certification Practice Statement の略。証明書の申請、申請の審査、証明書発行、失効し、保管、開示を含む本サービスの提供および利用にあたっての注意点等を規定するもの。

© 2003 SECOM Trust Systems Co.,Ltd.

認証局（CA）

Certification Authority の略。証明書の発行・更新・失効し、CA 等私有鍵の生成・保護および利用者の登録を行う機関。

マイナーバージョン番号

本 CPS の内容変更に際して、変更レベルが利用者や検証者が証明書や CRL を使用する上で、全く影響しないかまたは無視できると判断した場合、本 CPS の改訂版に付ける枝番号（例：Version 1.02 ならば、下線部（02））を示す。

メジャーバージョン番号

本 CPS の内容変更に際して、変更レベルが、明らかに利用者や検証者が証明書や CRL を使用するうえで影響すると判断した場合、本 CPS の改訂版に付ける番号（例：Version 1.02 ならば、下線部（１））を示す。

リポジトリー

CA が発行した証明書等の格納庫である。ユーザまたはアプリケーションがネットワークのどこからでも証明書にアクセスできるようにするための仕組みである。CRL や本 CPS もリポジトリーに格納される。

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。

© 2003 SECOM Trust Systems Co.,Ltd.

2. 公表とリポジトリーの責任

2.1 リポジトリー

本 CA は、利用者および検証者が CRL 情報にアクセスできるようリポジトリーを維持管理する。また、利用者および検証者がオンラインでの証明書ステータス情報を 24 時間 365 日利用できるように OCSP サーバーを維持管理する。リポジトリーへのアクセスに用いるプロトコルは、HTTP（HyperText Transfar 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。リポジトリーの情報は一般的な Web インターフェースを通じてアクセス可能である。

2.2 証明書情報の公開

本 CA は、次の内容をリポジトリーに格納し、利用者および検証者がオンラインによって閲覧できるようにする。

- 本 CPS および CP に基づくすべての失効情報を含む証明書失効リスト（以下、「CRL」という）
- 本 CA の自己署名証明書
- 最新の本 CPS および CP
- 本 CA が発行する証明書に関するその他関連情報

また、セコムは、OCSP サーバーにより利用者および検証者がオンラインによって証明書ステータス情報を閲覧できるようにする。

2.3 公開の時期および頻度

本 CPS および CP は、変更の都度、リポジトリーに公表される。CRL は、本 CPS および CP に従って処理されたすべての失効情報を含み、発行の都度、リポジトリーに公表される。

2.4 リポジトリーへのアクセスコントロール

利用者および検証者は、随時、リポジトリーを参照できる。ただし、保守等により、一時的にリポジトリーを利用できない場合もある。

© 2003 SECOM Trust Systems Co.,Ltd.

3. 識別と認証

3.1 名前
CP に規定する。

3.2 初回の識別と認証
CP に規定する。

3.3 鍵更新申請時の識別と認証
CP に規定する。

3.4 失効申請時の識別と認証
CP に規定する。

© 2003 SECOM Trust Systems Co.,Ltd.

4. 証明書のライフサイクルに対する運用要件

4.1 証明書申請
CP に規定する。

4.2 証明書申請手続
CP に規定する。

4.3 証明書発行
CP に規定する。

4.4 証明書の受領確認
CP に規定する。

4.5 鍵ペアと証明書の用途
CP に規定する。

4.6 証明書の更新
CP に規定する。

4.7 鍵更新をともなう証明書の更新
CP に規定する。

4.8 証明書の変更
CP に規定する。

4.9 証明書の失効および一時停止
CP に規定する。

4.10 証明書のステータス確認サービス
CP に規定する。

4.11 加入（登録）の終了
CP に規定する。

4.12 キーエスクローと鍵回復
CP に規定する。

© 2003 SECOM Trust Systems Co.,Ltd.

5. 物理的、手続上、人事的管理

5.1 物理的管理

5.1.1 立地および建物構造

本 CA のシステム（以下、「CA システム」という）を設置する施設は、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あり、かつ建物構造上、これら災害防止のための対策を講ずる。また、施設内において使用する機器等を、災害および不正侵入防止策の施された安全な場所に設置する。

5.1.2 物理的アクセス

本 CA のハードウェアおよびソフトウェアには、物理的なアクセス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装備する。ハードウェアおよび CA サービスを提供するソフトウェアへのアクセスは常時監視され、アクセスは、サービス運用管理者の承認を必要とする。

5.1.3 電源管理および空調管理

CA システムを設置する室は、CA システムの運用のために十分な容量の電源を確保するとともに、長時間停電時においても自家発電装置により電源供給を受け保護される。また CA システムは、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される。

5.1.4 水害対策

CA システムを設置する室は、漏水検知器の設置等、防水対策を講ずる。

5.1.5 火災防止

CA 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内とし、火災報知器および消火設備を設置する。

5.1.6 地震対策

CA システムを設置する室は、機器･什器の転倒および落下を防止するために必要な対策を講ずる。

5.1.7 媒体管理

アーカイブデータ、バックアップデータを含む重要な媒体は、安全な保管場所に保管される。

5.1.8 廃棄処理

本 CA の私有鍵（以下、「CA 私有鍵という」）、機密情報を含む紙面の文書および磁気媒体等の廃棄の方法は、CA 私有鍵やバックアップ媒体等は完全な初期化を行うかまたは物理

© 2003 SECOM Trust Systems Co.,Ltd.

的に破壊を行い、文書等の紙ベースのものはシュレッダー、焼却、溶解のいずれかにて廃棄を行う。

5.1.9 オフサイトバックアップ

本サービスに必要なデータ、機器等は、遠隔地に保管するかまたは調達できる手段を講ずるものとする。

5.2 手続上の管理

5.2.1 信頼される役割

証明書の登録、発行、失効業務に携わる者は、本 CPS および CP 上信頼される役割を担っている。本 CA では、業務上の役割を特定の個人に集中させず、複数人に権限を分離している。本 CA における役割を表「5.2-1 信頼される役割」に示す。

表 5.2-1 信頼される役割

役割名称	主な職務内容
認証サービス改善委員会	・本 CPS および CP の策定、改廃に関する承認 ・監査指摘事項への対応指示
サービス責任者	・本 CA 運用組織の統括 ・本 CA のシステム変更、運用手続変更の承認
サービス運用管理者	・運用担当者への作業指示および作業立会い ・CA システムおよび CA 私有鍵に関する作業立会い ・その他サービス運用の全般管理
CA 管理者	・証明書の登録作業、発行作業 ・CRL 発行作業
RA 担当者	・証明書申請に関する受付 ・利用者の審査
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

CA システムは、物理的に単独でのアクセスが不可能な設計となっており、作業は複数人によって行われる。

5.2.3 個々の役割に対する識別と認証

CA システムを設置する室への入室は、生体認証によるコントロールを採用し、CA 私有鍵へのアクセスについては、複数人によるコントロールを採用している。

5.2.4 権限分離が必要となる役割

本 CA では、権限を特定の個人に集中させず権限を分離することで、権限集中により可能となる単独操作で発生する不正行為等の防止を図る。システム操作、承認行為および監査

© 2003 SECOM Trust Systems Co.,Ltd.

に関する権限は分離される。

5.3 人事的管理

信頼される役割を担う者は、本サービスに関して操作や管理の責務を負う。本サービスにおいては、これら役割の信頼性、適合性および合理的な職務執行能力を保証する人事管理がなされ、そのセキュリティを確立するものとする。

5.3.1 資格、経験および身分証明の要件

本サービスに関して信頼される役割を担う者は、セコムの採用基準に基づき採用された正社員とする。CA 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ものを配置する。

5.3.2 背景調査

信頼される役割を担う者の信頼性と適格性は、本 CPS、CP およびセコムの規則に従って、任命時および定期的に評価される。

5.3.3 **教育要件**

信頼される役割を担う者は、新任時にその業務を行うための適切な教育を受け、以降必要に応じて再教育を受けなければならない。

5.3.4 再教育の頻度および要件

本 CA 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、必要に応じ再教育を行う。

5.3.5 仕事のローテーションの頻度および順序

本 CA 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

セコムの就業規則の制裁に関する規定に従う。

5.3.7 独立した契約者の要件

本 CA は、CA 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

本 CA 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。

© 2003 SECOM Trust Systems Co.,Ltd.

5.4 監査ログの手順

5.4.1 記録されるイベントの種類

本 CA では、CA システム、リポジトリーシステム、本 CA に関連するネットワーク・デバイスの監査証跡やイベント・ログを、手動あるいは自動で取得する。

5.4.2 監査ログの処理頻度

本 CA は、監査ログを定期的に精査する。

5.4.3 監査ログの保存期間

監査ログの保存期間は、最低 10 年とする。

5.4.4 監査ログの保護

本 CA 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

監査ログは、オフラインの記録媒体にバックアップがとられ、それらの媒体は安全な保管場所に保管される。

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、CA システムの機能に実装されており、自動または手動で監査ログを収集する。

5.4.7 イベントを起こした者への通知

本 CA 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

本 CA 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。

5.5 記録の保管

5.5.1 アーカイブの種類

本 CA のアーカイブには、次の情報が含まれる。

- 証明書の発行/失効に関する処理履歴
- CRL の発行に関する処理履歴
- 本 CA の自己署名証明書

© 2003 SECOM Trust Systems Co.,Ltd.

・ 利用者の証明書
・ CRL
・ OCSP サーバーへのアクセスログ

5.5.2 アーカイブの保存期間

アーカイブする情報の保存期間は、最低 10 年間とする。

5.5.3 アーカイブの保護

アーカイブ情報の収められた媒体は物理的に保護され、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される。アーカイブ情報は、１年に一度、データの障害や欠損が起きていないことを確認する。

5.5.4 アーカイブのバックアップ手順

証明書発行、失効または CRL の発行等、本 CA に影響のある重要なデータに変更がある場合は、都度バックアップを正副取得する。副の媒体については遠隔地に保管する。

5.5.5 記録にタイムスタンプを付与する要件

本 CA は、適切に CA システムの時刻同期を行い、CA 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、CA 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き

アーカイブ情報は、定期的に保管状況を確認する。必要に応じ、新しい媒体へ複製を行う。

5.6 鍵の切り替え

本 CA 自身の鍵ペア更新または証明書更新は、原則として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。本 CA の有効期間が、利用者に発行する証明書の最大有効期間よりも短くなる場合、利用者に発行する証明書の有効期間は、本 CA の有効期間内に納まるよう変更する。

なお、本 CA の私有鍵の有効期間は 20 年を想定している。

5.7 信頼性喪失や災害からの復旧

5.7.1 事故および危殆化の対応手続

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。

© 2003 SECOM Trust Systems Co.,Ltd.

5.7.2 コンピューターのハードウェア、ソフトウェアまたはデータが破損した場合の手続

本 CA は、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、バックアップ用に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、すみやかにシステムの復旧作業を行う。

5.7.3 利用者の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、本 CPS「4.9 証明書の取消および一時停止」に示す手続に従って、証明書の失効を行う。

5.7.4 災害後の事業継続能力

本サービスは、セコムの事業継続方針に基づき、サービスの中断を余儀なくする状態や、信頼性を著しく損なわせるような事態の際にも、本 CA に関するサービスを継続するために必要な計画を作成している。サービスの中断を最小限に抑えるため、セコムでは、サービスの復旧に必要なリソースの調達手段を予め計画している。

5.8 認証業務の終了

セコムが本サービスを終了する場合、サービス終了の 3 か月前までに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、本サービスの終了以前に失効される。

© 2003 SECOM Trust Systems Co.,Ltd.

6. 技術的セキュリティ管理

6.1 鍵ペアの生成とインストール

6.1.1 鍵ペア生成

本サービスでは、本 CA の鍵ペアを 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。本 CA の私有鍵の生成作業は、サービス運用管理者立会いのもと、複数名の権限者による操作によって行われる。

6.1.2 利用者への私有鍵の送付

利用者の鍵ペアは、利用者自身で生成するため、私有鍵は利用者のみが所持する。

6.1.3 CA への公開鍵の送付

利用者の公開鍵は、CP「3.2.1 私有鍵の所有を証明する方法」に定める手続により検証され、その受渡しはオフラインで行う。

6.1.4 検証者への CA 公開鍵の送付

検証者は、本 CA のリポジトリーにアクセスするか、または一般的に使用される Web ブラウザを通して本 CA の公開鍵を入手することができる。

6.1.5 鍵長

CA の鍵ペアの電子署名方式を表「6.1-1 電子署名方式」に示す。

表 6.1-1 電子署名方式

公開鍵アルゴリズム	署名アルゴリズム	CA 鍵
2048 bit RSA	SHA1	Security Communication RootCA1
2048 bit RSA	SHA256	Security Communication RootCA2
4096 bit RSA	SHA384	Security Communication RootCA3
384 bit ECC	SHA384	Security Communication ECC RootCA1

6.1.6 公開鍵のパラメーターの生成および品質検査

CA 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ーは、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

CP に規定する。

© 2003 SECOM Trust Systems Co.,Ltd.

6.2 私有鍵の保護および暗号装置技術の管理

6.2.1 暗号モジュールの標準および管理

CA 私有鍵の生成、保管、署名操作は、FIPS140-2 レベル 3 の認定を取得した HSM を用いて行われる。

6.2.2 私有鍵の複数人コントロール

CA 私有鍵の生成には、サービス運用管理者と複数名の権限者を必要とする。生成後に発生する暗号モジュールの搬送、廃棄等の私有鍵管理についても同様である。

6.2.3 私有鍵のエクスロー

CA 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

CA 私有鍵は、CA 室内で FIPS140-2 レベル 3 の認定を取得した HSM にバックアップされる。バックアップ作成時も本 CPS「6.2.2 私有鍵の複数人コントロール」と同じコントロールがなされる。また、そのバックアップについても安全に管理する。

6.2.5 私有鍵のアーカイブ

CA 私有鍵は、アーカイブを行わない。

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

CA 私有鍵は HSM の内部で生成され、他のハードウェアおよびソフトウェア等によって私有鍵が取り出されることはない。

6.2.7 私有鍵の暗号モジュールへの格納

CA 私有鍵は、FIPS140-2 レベル 3 の認定を取得した HSM に格納される。

6.2.8 私有鍵の活性化の方法

CA 私有鍵の活性化は、CA 室内において本 CPS「6.2.2 私有鍵の複数人コントロール」と同様に、複数人の権限を有する者によって行われる。

6.2.9 私有鍵の非活性化の方法

CA 私有鍵は、CA 私有鍵へのアクセス終了後、自動的に非活性化される。

6.2.10 私有鍵の廃棄方法

CA 私有鍵を廃棄しなければならない状況の場合、CA 室内において本 CPS「6.2.2 私有鍵の複数人コントロール」と同様に、複数人によって、私有鍵の格納された HSM を完全に初期化、または物理的に破壊する。同時に、バックアップの私有鍵に関しても同様の手続によって廃棄する。

© 2003 SECOM Trust Systems Co.,Ltd.

6.2.11 暗号モジュールの技術管理

本 CA の鍵ペアの管理に用いる HSM は、FIPS140-2 レベル 3 の認定を取得した製品を用いる。

6.3 鍵ペア管理のその他の側面

6.3.1 公開鍵のアーカイブ

本 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 鍵ペアの有効期間

本 CA の鍵ペアの有効期間は 20 年を想定している。有効期間の変更は行わない。

6.4 活性化データ

6.4.1 活性化データの生成とインストール

CA 私有鍵の活性化には、複数の電子鍵を用いる。

6.4.2 活性化データの保護

活性化に必要な複数の電子鍵は、分散して保管する。

6.4.3 活性化データの他の考慮点

規定しない。

6.5 コンピューターのセキュリティ管理

6.5.1 コンピューターセキュリティに関する技術的要件

本 CA のハードウェアは、本 CPS「5.1 物理的管理」に記述される方法により物理的に保護され、ログイン時にユーザ認証を必要とする。また、ウィルス対策を施す等により、様々な脅威から保護される。

6.5.2 コンピューターセキュリティ評価

本 CA は、CA 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、信頼性の確保に努める。また、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 セキュリティ技術のライフサイクル管理

本 CA のハードウェアおよびソフトウェアは､適切なサイクルで最新のセキュリティテクノロジを評価し、必要に応じて、本 CPS および CP の見直しおよびセキュリティチェック

© 2003 SECOM Trust Systems Co.,Ltd.

を行う。

6.6.1 システム開発管理

CA システムの構築およびメンテナンスは、安全な環境下で行い、変更を行う場合は、十分に安全性の評価、確認を行う。また、CA 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

本 CA 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

本 CA は、CA 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

CA システムは社内および社外の他のシステムとは接続しない。リポジトリーシステムは、ファイアウォール、不正侵入検知システム等により、不正アクセスから保護される。

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。

© 2003 SECOM Trust Systems Co.,Ltd.

7. 証明書、CRL および OCSP のプロファイル

7.1 証明書のプロファイル
CP に規定する。

7.2 CRL のプロファイル
CP に規定する。

7.3 OCSP のプロファイル
CP に規定する。

© 2003 SECOM Trust Systems Co.,Ltd.

8 準拠性監査と他の評価

8.1 監査の頻度

セコムは、本サービスが本 CPS および CP に準拠して運用されているかに関して年に 1 度、あるいは本 CPS「8.2 監査人の身分と資格」で定める監査人が必要と判断した時期に監査を行う。

8.2 監査人の身分と資格

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 監査人と被監査対象との関係

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、WebTrust for CA 規準に基づいて行われ、本 CA の運用にかかる業務を対象として行う。

8.5 監査指摘事項への対応

セコムは、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 監査結果の報告

監査結果は、監査人からセコムに対して報告される。セコムは、法律に基づく開示要求があった場合、セコム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。

© 2003 SECOM Trust Systems Co.,Ltd.

9. 他の業務上および法的問題

9.1 料金
CP に規定する。

9.2 財務的責任
CP に規定する。

9.3 機密保持
CP に規定する。

9.4 個人情報の保護
CP に規定する。

9.5 知的財産権
CP に規定する。

9.6 表明保証
CP に規定する。

9.7 保証の制限
CP に規定する。

9.8 責任の制限
CP に規定する。

9.9 補償
CP に規定する。

9.10 有効期間と終了
CP に規定する。

9.11 関係者間の個別通知と連絡
CP に規定する。

9.12 改訂

9.12.1 改訂手続

© 2003 SECOM Trust Systems Co.,Ltd.

(1) 重要な変更

セコムは、本 CPS の内容変更に際して、利用者および検証者が証明書または CRL を使用するうえで本CPSの内容の変更が明らかに影響すると判断した場合､変更した本CPS(本 CPS の変更内容と変更実施日を含む）をリポジトリー上に掲載することにより、利用者および検証者に対して変更の告知を行う。また、本 CPS のメジャーバージョン番号を更新する。

(2) 重要でない変更

セコムは、本 CPS の内容変更に際して、利用者および検証者が証明書または CRL を使用するうえで本 CPS の内容の変更が全く影響しないかまたは無視できると判断した場合、変更した本 CPS（本 CPS の変更内容と変更実施日を含む）をリポジトリー上に掲載することにより、利用者および検証者に対して変更の告知を行う。また、本 CPS のマイナーバージョン番号を更新する。

9.12.2 通知方法および期間

本 CPS を変更した場合、すみやかに変更した本 CPS（本 CPS の変更内容と変更実施日を含む）をリポジトリー上に掲載することにより、利用者および検証者に対しての告知とする。利用者は告知日から一週間の間、異議を申し立てることができ、異議申し立てがない場合、変更された本 CPS は利用者に同意されたものとみなされる。

9.13 紛争解決手段

CP に規定する。

9.14 準拠法

CP に規定する。

9.15 適用法の遵守

CP に規定する。

9.16 雑則

CP に規定する。

9.17 その他の条項

CP に規定する。

© 2003 SECOM Trust Systems Co.,Ltd.