Security Communication RootCA
認証運用規定

Version 6.00

2023 年 01 月 16 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
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 証明書ポリシー/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
V5.12	2019/05/24	全体的な文言および体裁の見直し
V5.13	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
V5.14	2021/03/30	日付およびバージョンの更新
V5.15	2021/11/30	全体的な文言および体裁の見直し
V5.16	2022/06/10	全体的な文言および体裁の見直し
V6.00	2023/01/16	メジャーバージョンアップ CA の私有鍵 SECOM TLS RSA Root CA 2023 を追加 CA の私有鍵 SECOM RSA Root CA 2023 を追加 CA の私有鍵 SECOM Document Signing RSA Root CA 2023 を追加

目次

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、Security Communication ECC RootCA1、SECOM TLS RSA Root CA 2023、SECOM RSA Root CA 2023 および SECOM Document Signing RSA Root CA 2023（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ー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ー（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 Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, Guidelines for the Issuance and Management of Extended Validation Certificates, Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates（以下、Baseline Requirements という）の最新版に準拠する。

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 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、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 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。

本 CPS は、本 CA のルート CA 証明書を表「1.1-1 ルート CA 証明書」に示す。

表 1.1-1 ルート CA 証明書

識別名	SHA256 Fingerprint
C = JP, O = SECOM Trust.net, OU = Security Communication RootCA1	E75E72ED9F560EEC6EB4800073A43FC3AD19195A392282017895974A99026B6C
C = JP, O = SECOM Trust Systems CO.,LTD., OU = Security Communication RootCA2	513B2CECB810D4CDE5DD85391ADFC6C2DD60D87BB736D2B521484AA47A0EBEF6
C = JP, O = SECOM Trust Systems CO.,LTD., CN = Security Communication RootCA3	24A55C2AB051442D0617766541239A4AD032D7C55175AA34FFDE2FBC4F5C5294
C = JP, O = SECOM Trust Systems CO.,LTD., CN = Security Communication ECC RootCA1	E74FBDA55BD564C473A36B441AA799C8A68E077440E8288B9FA1E50E4BBACA11
C = JP, O = SECOM Trust Systems Co., Ltd., CN = SECOM TLS RSA Root CA 2023	**未定**
C = JP, O = SECOM Trust Systems Co., Ltd., CN = SECOM RSA Root CA 2023	未定
C = JP, O = SECOM Trust Systems Co., Ltd., CN = SECOM Document Signing RSA Root CA 2023	未定

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）

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 用証明書ポリシー	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) 1.2.392.200091.100.901.8 (SECOM TLS RSA Root CA 2023) 1.2.392.200091.100.901.9 (SECOM RSA Root CA 2023) 1.2.392.200091.100.901.10 (SECOM Document Signing RSA Root CA 2023)
Security Communication RootCA タイムスタンプサービス用証明書ポリシー	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)

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）レスポンダ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。

CA については、「1.6 定義と略語」に定義する。

1.3.2 RA

RA は、証明書申請者となる組織、団体からの証明書発行、失効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。

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 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 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。

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。

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
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 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。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。

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 CPS 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。

あ～ん

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。

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

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。

証明書ポリシー（CP）

Certificate Policy の略。証明書に関するポリシー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。

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。本 CPS では発行局（IA:Issuing Authority）も含まれる。

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。

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、まった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。ユーザー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（Root CA）

本 CPS でいうルート CA 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。

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 レスポンダーを維持管理する。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/TLS 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 24 時間 365 日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

本 CA では、アプリケーションソフトウェアサプライヤーが各パブリックルート証明書までつながる加入者証明書を使用してソフトウェアをテストできるよう、テスト用ウェブページをホストするものとする。最低限、本 CA は、i. 有効、ii. 失効、および iii. 有効期限切れの加入者証明書用のウェブページを別々にホストするものとする。

また、セコムは、OCSP レスポンダ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

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

3.1.1 名前の種類
CP に規定する。

3.1.2 意味のある名前の必要性
CP に規定する。

3.1.3 利用者の匿名性または仮名性
CP に規定する。

3.1.4 さまざまな名前の形式を解釈するための規則
CP に規定する。

3.1.5 名前の一意性
CP に規定する。

3.1.6 認識、認証および商標の役割
CP に規定する。

3.2 初回の識別と認証

3.2.1 私有鍵の所有を証明する方法
CP に規定する。

3.2.2 組織の認証
CP に規定する。

3.2.2.1 アイデンティティ
CP に規定する。

3.2.2.2 商号/商標名
CP に規定する。

3.2.2.3 国の検証
CP に規定する。

3.2.3 個人の認証
CP に規定する。

3.2.4 検証されない利用者の情報
CP に規定する。

3.2.5 権限の正当性確認
CP に規定する。

3.2.6 相互運用の基準
CP に規定する。

3.3 鍵更新申請時の識別と認証

3.3.1 通常の私有鍵更新にともなう証明書申請時の識別と認証
CP に規定する。

3.3.2 証明書失効後の私有鍵更新にともなう証明書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。

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

4.1.1 証明書申請を行うことができる者
CP に規定する。

4.1.2 申請手続および責任
CP に規定する。

4.2 証明書申請手続

4.2.1 識別と認証の手続
CP に規定する。

4.2.2 証明書申請の受理または却下
CP に規定する。

4.2.3 証明書申請の処理時間
CP に規定する。

4.3 証明書発行

4.3.1 証明書の発行時における CA の処理手続
CP に規定する。

4.3.2 利用者に対する証明書発行通知
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
CP に規定する。

4.4.2 CA による証明書の公開
CP に規定する。

4.4.3 他のエンティティに対する CA の証明書発行通知
CP に規定する。

4.5 鍵ペアと証明書の用途

4.5.1 利用者の私有鍵および証明書の用途
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
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
CP に規定する。

4.6.2 証明書更新申請を行うことができる者
CP に規定する。

4.6.3 証明書更新申請の処理手続
CP に規定する。

4.6.4 利用者に対する新しい証明書の通知
CP に規定する。

4.6.5 更新された証明書の受領確認手続
CP に規定する。

4.6.6 更新された証明書の公開
CP に規定する。

4.6.7 他のエンティティに対する CA の証明書発行通知
CP に規定する。

4.7 証明書の鍵更新

4.7.1 鍵更新の状況
CP に規定する。

4.7.2 新しい公開鍵の証明書申請を行うことができる者
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
CP に規定する。

4.7.4 利用者に対する新しい証明書の通知
CP に規定する。

4.7.5 鍵更新にともない発行された証明書の受領確認手続
CP に規定する。

4.7.6 鍵更新済みの証明書の公開
CP に規定する。

4.7.7 他のエンティティに対する CA の証明書発行通知
CP に規定する。

4.8 証明書の変更

4.8.1 証明書を変更する場合
CP に規定する。

4.8.2 証明書の変更申請をすることができる者
CP に規定する。

4.8.3 証明書の変更申請の処理手続
CP に規定する。

4.8.4 利用者に対する新しい証明書の発行通知
CP に規定する。

4.8.5 変更された証明書の受領確認手続
CP に規定する。

4.8.6 変更された証明書の公開
CP に規定する。

4.8.7 他のエンティティに対する CA の証明書発行通知
CP に規定する。

4.9 証明書の失効および一時停止

4.9.1 証明書失効事由
CP に規定する。

4.9.2 証明書失効を申請することができる者
CP に規定する。

4.9.3 失効申請手続
CP に規定する。

4.9.4 失効申請の猶予期間
CP に規定する。

4.9.5 CA の失効申請処理の許容時間
CP に規定する。

4.9.6 失効確認要求
CP に規定する。

4.9.7 証明書失効リストの発行頻度
CP に規定する。

4.9.8 証明書失効リストの発行の最大遅延時間
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
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
CP に規定する。

4.9.11 利用可能な失効情報の他の形式
CP に規定する。

4.9.12 鍵の危殆化に対する特別要件
CP に規定する。

4.9.13 証明書の一時停止
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
CP に規定する。

4.9.15 証明書の一時停止申請手続
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
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
CP に規定する。

4.10.2 サービスの利用可能性
CP に規定する。

4.10.3 オプショナルな仕様
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

4.12.1 キーエスクローと鍵回復ポリシーおよび実施
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
CP に規定する。

5. 物理的、手続上、人事的管理

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。

本 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. 法律によって本 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。

本 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本 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、本 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 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。

5.1.7 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。

5.1.8 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。

5.1.9 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。

5.2 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。

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 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、本 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

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。

本 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。
本 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。
本 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。

本 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

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。

信頼される役割のすべての要員は、本 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

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。

本 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

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。

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。

本 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. 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. 証明書失効リストおよび OCSP エントリの生成。
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. ファイアウォールおよびルーターアクティビティ。

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。

5.4.2 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。

ただし、Baseline Requirements に関連する場合、本 CA 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 CPS「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 CPS「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 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

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。

さらに本 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およ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 本 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

本 CA 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。

- 発行した証明書および CRL
- 本 CPS、Security Communication RootCA 下位 CA 用証明書ポリシー、Security Communication RootCA タイムスタンプサービス用証明書ポリシー
- 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および監査報告書

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。
ただし、Baseline Requirements に関連する場合、本 CA は、証明書要求およびその検証に関するすべての文書、ならびにすべての証明書およびその失効を、その文書に基づく証明書が有効でなくなった後、少なくとも 7 年間保持するものとする。

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。

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。

本 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。

本 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 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、Security Communication RootCA 下位 CA 用証明書ポリシーまたは Security Communication RootCA タイムスタンプサービス用証明書ポリシー「4.9 証明書の失効および一時停止」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、アプリケーションソフトウェアサプライヤーを含む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。

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

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、または CA 鍵ペア生成プロセス全体を録画する。
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、または CA 鍵ペア生成プロセス全体を録画する。

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。

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 鍵長」または本 CPS「6.1.6 公開鍵のパラメーター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「4.9.1 証明書失効事由」の規定などにより、申請者の私有鍵が鍵の危殆化を受けたことを以前に認識していた。

5. 下位 CA は、公開鍵（Debian の弱い鍵など。 https://wiki.debian.org/SSLkeys を参照）に基づいて申請者の私有鍵を簡単に計算するための実証済みまたは証明された方法を認識している。

6.1.2 利用者への私有鍵の送付

私有鍵は利用者のみが所持し、本 CA より私有鍵の送付は行わない。

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

本 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
4096 bit RSA	SHA384	SECOM TLS RSA Root CA 2023
4096 bit RSA	SHA384	SECOM RSA Root CA 2023
4096 bit RSA	SHA384	SECOM Document Signing RSA Root CA 2023

Baseline Requirements に関連した TLS サーバー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。

・法の長さ（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。

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。

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 Routin 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べきである。[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

ルート証明書に対応する私有鍵は、以下の場合を除き、証明書の署名に使用してはならない。

1. ルート CA 自体を表すための自己署名証明書
2. 下位 CA 証明書およびクロス証明書
3. インフラストラクチャ目的の証明書(管理者証明書、内部 CA 運用デバイス証明書)
4. OCSP からのレスポンスを検証する証明書

6.2 私有鍵の保護および暗号装置技術の管理

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

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

本 CA の CA 私有鍵は本 CA の 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。

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 の鍵ペアおよび CA 証明書の有効期間は 8 年以上、25 年以下を想定している。
下位 CA の鍵ペアの有効期間は定めないが、証明書の有効期間は、20 年以下を想定してい

る。
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
本 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ー認証を必要とする。また、ウイルス対策を施す等により、様々な脅威から保護される。
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。

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

7.1.1 バージョン番号
CP に規定する。

7.1.2 証明書拡張
CP に規定する。

7.1.3 アルゴリズムオブジェクト識別子
CP に規定する。

7.1.4 名前形式
CP に規定する。

7.1.5 名前制約
CP に規定する。

7.1.6 CP オブジェクト識別子
CP に規定する。

7.1.7 ポリシー制約拡張の利用
CP に規定する。

7.1.8 ポリシー修飾子の文法および意味
CP に規定する。

7.1.9 重要な証明書ポリシー拡張の処理の意味
CP に規定する。

7.2 CRL のプロファイル

7.2.1 バージョン番号
CP に規定する。

7.2.2 CRL 拡張
CP に規定する。

7.3 OCSP のプロファイル

7.3.1 バージョン番号

CP に規定する。

7.3.2 OCSP 拡張

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. 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。

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、CP「7.1.5 名前制約」に従って技術的に制約され、かつ本 CPS「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 監査人の身分と資格

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

本 CA は、必要に応じて以下のスキーム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 – Publicly Trusted Code Signing Certificates
・WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL

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 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。

監査レポートは、CP「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 または下位 CA が証明書を発行する期間中、本 CA または下位 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 または下位 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 または下位 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下位 CA が証明書を発行する期間中、下位 CA に署名した本 CA は、本 CA の CP や下位本 CA の CPS 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下位 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問題

9.1 料金

CP に規定する。

9.1.1 証明書の発行または更新にかかる料金

CP に規定する。

9.1.2 証明書のアクセス料金

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

CP に規定する。

9.1.4 他サービスの料金

CP に規定する。

9.1.5 代金返金ポリシー

CP に規定する。

9.2 財務的責任

9.2.1 保険の補償

CP に規定する。

9.2.2 その他の資産

CP に規定する。

9.2.3 エンドエンティティの保険または保証範囲

CP に規定する。

9.3 機密保持

9.3.1 機密情報の範囲

CP に規定する。

9.3.2 機密保持対象外の情報

CP に規定する。

9.3.3 機密情報の保護責任
CP に規定する。

9.4 個人情報の保護

9.4.1 個人情報保護方針
CP に規定する。

9.4.2 個人情報として扱われる情報
CP に規定する。

9.4.3 個人情報とみなされない情報
CP に規定する。

9.4.4 個人情報を保護する責任
CP に規定する。

9.4.5 個人情報の使用に関する通知と同意
CP に規定する。

9.4.6 司法または行政手続に沿った情報開示
CP に規定する。

9.4.7 その他の情報開示条件
CP に規定する。

9.5 知的財産権
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
CP に規定する。

9.6.2 RA の表明保証
CP に規定する。

9.6.3 利用者の表明保証
CP に規定する。

9.6.4 検証者の表明保証
CP に規定する。

9.6.5 他の関係者の表明保証
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

9.10.1 有効期間
CP に規定する。

9.10.2 終了
CP に規定する。

9.10.3 終了の効果と効果継続
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
(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。

9.12.3 オブジェクト識別子が変更されなければならない場合

CP に規定する。

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

9.16.1 完全合意条項

CP に規定する。

9.16.2 権利譲渡条項

CP に規定する。

9.16.3 分離条項

本 CP および 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

CP に規定する。

9.16.5 不可抗力

CP に規定する。

9.17 その他の条項

CP に規定する。