Security Communication RootCA
下位 CA 用証明書ポリシー

Version5.20

2022 年 12 月 8 日

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 証明書ポリシー/認証運用規程を分割し、Security Communication RootCA1 下位 CA 用証明書ポリシーを作成。 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ー委員会”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 下位 CA 用証明書ポリシーを Security Communication RootCA 下位 CA 用証明書ポリシーとし、CA の私有鍵 Security Communication RootCA2 を追加する
V4.10	2012/02/15	4.6 証明書の更新手続きを追記。
V4.20	2012/11/09	OCSP サーバーの運用開始にともなう修正
V4.30	2015/03/20	使用署名アルゴリズムの追加 文言の見直しを実施
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	2019/03/12	7.1.2 証明書拡張、7.1.5 名前制約を更新
V5.13	2019/05/24	全体的な文言および体裁の見直し
V5.14	2019/09/25	EV 証明書用の OID を追記
V.5.15	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
V5.16	2020/09/29	CRL 基本領域を修正 下位 CA 証明書拡張 certificatePolicies の HTTPS 表記を修正
V5.17	2021/05/31	証明書失効事由の修正 鍵の危殆化に対する特別要件の追記
V5.18	2021/11/30	RootCA 証明書のプロファイル追記 全体的な文言および体裁の見直し
V5.19	2022/06/10	全体的な文言および体裁の見直し

© 2003 SECOM Trust Systems Co.,Ltd.

V5.20	2022/12/08	「7.1.2 証明書拡張」 「表 7.1-2-8 Security Communication ECC RootCA1 下位 CA 証明書拡張」の修正

© 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.

© 2003 SECOM Trust Systems Co.,Ltd.

© 2003 SECOM Trust Systems Co.,Ltd.

1. はじめに

1.1 概要

Security Communication RootCA 下位 CA 用証明書ポリシー（Certificate Policy : 以下、「本 CP」という）は、セコムトラストシステムズ株式会社（以下、「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）が発行する下位 CA 用証明書（以下、「証明書」という）の利用目的、適用範囲、利用者手続を示し、証明書に関するポリシーを規定するものである。なお、本 CA の運用維持に関する諸手続については、Security Communication RootCA 認証運用規定（Certification Practice Statement：以下、「CPS」という）に規定する。

セコムは、認証局として本 CA の鍵管理、証明書発行、失効等の認証サービス（以下、「本サービス」という）を提供する。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 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 CP の内容が CPS の内容に抵触する場合は、本 CP が優先して適用されるものとする。また、セコムと証明書の利用者との間で別途契約書等が存在する場合、本 CP および CPS より契約書等の文書が優先される。本 CP と Baseline Requirements の間に矛盾がある場合、Baseline Requirements が本 CP に優先して適用される。

本 CP 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 CP の正式名称は「Security Communication RootCA 下位 CA 認証用証明書ポリシー」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

© 2003 SECOM Trust Systems Co.,Ltd.

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

表 1.2-2 OID（本 CP）

CP	OID
Security Communication RootCA1	1.2.392.200091.100.901.1
Security Communication RootCA2	1.2.392.200091.100.901.4
Security Communication RootCA3	1.2.392.200091.100.901.6
Security Communication ECC RootCA1	1.2.392.200091.100.902.1

本 CP に関連する CPS の OID を表「1.2-3 OID（CPS）」に示す。

表 1.2-3 OID（CPS）

CPS	OID
Security Communication RootCA 認証運用規定	1.2.392.200091.100.901.3

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各業務を行う。

CA については、本 CP「1.6 定義と略語」に定義する。

1.3.2 RA

RA は、利用者となる組織、団体からの証明書発行、失効等の要求に対して、組織、団体の識別と認証、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。本 CP および CPS の内容を利用者自身の利用目的に照らして評価し承諾する必要がある。

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 CP および CPS の内容を検証者自身の利用目的に照らして確認および同意したうえで検証しているとみなされる。

© 2003 SECOM Trust Systems Co.,Ltd.

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、本 CP「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 CA であり、利用者の証明書として下位 CA 証明書を発行する。証明書を信頼して利用する検証者は、当該証明書の信頼性を本 CA の公開鍵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

本 CA が発行する証明書は、本 CP の目的以外に証明書を利用してはならない。

1.5 ポリシー管理

1.5.1 文書を管理する組織

本 CP の維持・管理は、セコムが行う。

1.5.2 連絡先

本 CP 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 CP が、本 CA のポリシー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 CP は、最低でも年次でレビューし、改訂する。

© 2003 SECOM Trust Systems Co.,Ltd.

1.5.4 承認手続

本 CP 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

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

CA/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。

OCSP（Online Certificate Status Protocol）
証明書のステータス情報をリアルタイムに提供するプロトコルのことである。

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。

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

© 2003 SECOM Trust Systems Co.,Ltd.

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 が定めた電子証明書および証明書失効リストのフォーマット。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、電子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。

© 2003 SECOM Trust Systems Co.,Ltd.

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。電子証明書を発行する際の元となるデータファイル。CSR には電子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電子証明書を発行する。

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。

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、および、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。電子証明書の申請、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。

認証サービス改善委員会

本 CP の管理、変更の検討等、本サービスの運用ポリシーの決定等を行う意思決定組織。

認証局（CA）

© 2003 SECOM Trust Systems Co.,Ltd.

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 CP 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 CP 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 CP 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 CP 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 CP 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 CP もリポジトリーに格納される。

ルート CA（Root CA）

本 CP 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。

© 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

CPS に規定する。

2.2 証明書情報の公開

CPS に規定する。

2.3 公開の時期および頻度

CPS に規定する。

2.4 リポジトリーへのアクセスコントロール

CPS に規定する。

© 2003 SECOM Trust Systems Co.,Ltd.

3. 識別と認証

3.1 名前

3.1.1 名前の種類

本 CA が発行する証明書は、X.509 規格、RFC5280 規格および Baseline Requirements の要求事項を満たし、証明書所有者に割り当てられる識別名は X.500 の識別名形式に従い、かつ本 CP「7.1.4 名前形式」に則って設定する。

3.1.2 意味のある名前の必要性

利用者の識別名は、意味のある名前を用いる。証明書に記載される主体者名は、組織または団体に適切な範囲で関連したものでなければならない。利用者は、第三者の登録商標や関連する名称を、本 CA に申請してはならない。

3.1.3 利用者の匿名性または仮名性

証明書に記載される主体者名に匿名や仮名は使用しない。

3.1.4 さまざまな名前の形式を解釈するための規則

識別名は、本 CP「3.1.1 名前の種類」および「3.1.2 意味のある名前の必要性」で定義しているとおりに解釈する。

3.1.5 名前の一意性

本 CA では、発行された証明書が、主体者の識別名に含まれる情報により、証明書の所有者を一意に識別できることを保証する。

3.1.6 認識、認証および商標の役割

商標使用の権利については、商標所持者に権利が留保されるものとする。本 CA は、必要に応じて、商標所持者に対し、商標に関する出願等の公的書類の提示を求めることがある。

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

本 CA は、申請者から提出された証明書発行要求（Certificate Signing Request：以下、「CSR」という）の署名の検証を行い、それに含まれている 公開鍵に対応する私有鍵で署名されていることを確認する。また、CSR のフィンガープリントを確認し、公開鍵の所有者を特定する。

3.2.2 組織の認証

申請者は、証明書の発行申請時に本 CA に以下の情報を提出しなければならない。

・ 証明書発行申請書

© 2003 SECOM Trust Systems Co.,Ltd.

・ 組織または団体が実在していることを証明する情報
・ CSR
・ その他、セコムが必要とする書類

本 CA は、以上の情報を用いて、申請に誤りや欠落情報がないことを確認する。

3.2.2.1 アイデンティティ

主体者識別名が組織の名前または住所を含む場合、本 CA は、組織のアイデンティティや住所を検証し、その住所が申請者の現存する、または稼働している住所であることを確認するものとする。本 CA は、次のうち 1 か所以上から提供されたドキュメントや、それとのやり取りを通じて得られた情報を使用して、申請者のアイデンティティと住所を検証するものとする。

1. 申請者の法的な設立、存在、または承認の管轄地域にある行政機関。
2. 定期的に更新され、信頼できるデータ情報源と見なされている第三者のデータベース。
3. 本 CA あるいは、本 CA の代理人としての役割を担っている第三者による現場訪問。
4. 認証書。

本 CA は、上記 1 から 4 と同じ文書または情報を使用して、申請者のアイデンティティと住所の両方を検証してもよい。

3.2.2.2 商号/商標名

主体者のアイデンティティ情報に商号または商標名が含まれる場合、本 CA は、以下の少なくとも 1 つを使用して、商号/商標名を使用するための申請者の権利を検証するものとする

1. 申請者の法的な設立、存在、または承認の管轄地域にある政府機関が提供するドキュメントまたは、このような政府機関とのやり取りで得られた情報。
2. 信頼できるデータ情報源。
3. 当該商号または商標名の管理を担当している政府機関とのやり取りで得られた情報。
4. 文書による裏付けのある意見書。
5. 公共料金請求書、銀行取引明細書、クレジットカード明細書、政府発行の税務書類、その他、本 CA が信頼できると見なした本人確認書類。

3.2.2.3 国の検証

証明書の主体者識別名に countryName フィールドが存在する場合、本 CA は、次のいずれかを使用して主体者と関連付けられた国を検証するものとする

・ドメイン名登録機関によって提供された情報
・本 CP「3.2.2.1 アイデンティティ」に記載されている方法。

3.2.3 個人の認証

本 CA は、個人に対する証明書発行は行わない。

© 2003 SECOM Trust Systems Co.,Ltd.

3.2.4 検証されない利用者の情報

本 CA は、利用者から提出された証明書発行申請書類および CSR 情報から、部門名（Organizational Unit Name）については、誤解を与えるものでないことを確認する。それ以外、検証されていない情報は証明書に含まれない。

3.2.5 権限の正当性確認

主体者識別名を含む証明書の申請者が組織である場合、本 CA は、信頼できる連絡手段を使用して、申請権限者による証明書要求の真正性を検証するものとする。

本 CA は、「3.2.2.1 アイデンティティ」に掲載された情報源を使用して、信頼できる連絡手段を検証できる。CA が信頼できる連絡手段を使用することを条件として、本 CA は、申請権限者、申請者組織内の権限のある情報源(申請者の本社、経営部門、人事部門、情報技術部門、または本 CA が適切と見なすその他の部門)と直接やり取りして、証明書要求の真正性を確認できる。

加えて、本 CA は、証明書を申請できる個人を申請者に指定させるプロセスを確立するものとする。申請者が、証明書を申請できる個人を書面で指定している場合、本 CA は指定外の者による証明書要求を受け入れないものとする。本 CA は、申請者の検証済み申請書に関して、認証された証明書要求者のリストを提供する。

3.2.6 相互運用の基準

本 CA は、本 CP に基づき本 CA が識別し認証した CA に対し、片方向相互認証証明書を発行する。

本 CA は、信頼関係の確立（クロス証明書）を本 CA が取り決めた場合または受諾した場合、本 CA を主体者として識別するすべてのクロス証明書を開示しなければならない。

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

本 CP「3.2 初回の識別と認証」と同様の手続による。

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

本 CP「3.2 初回の識別と認証」と同様の手続による。

3.4 失効申請時の識別と認証

本 CA は、証明書の失効申請を受け付けた場合、提出された利用者の情報をもとに、適正な要求であることを確認する。

© 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

4.1.1 証明書申請を行うことができる者

証明書の発行申請は、発行申請を行う組織または団体の代表者、社員または代理人が行うことができる。

本 CP「5.5.2 アーカイブ保存期間」に従い、本 CA は、フィッシングまたはその他の詐欺的使用の疑いあるいは懸念を理由に、以前に失効した証明書および以前に拒否した証明書要求をすべて含む内部データベースを保持するものとする。本 CA は、この情報を使用して、以降の疑わしい証明書要求を識別するものとする。

4.1.2 申請手続および責任

証明書の発行前に、本 CA は申請者から以下のドキュメントを入手するものとする。

1. 証明書要求。電子版でも可。
2. 署名された加入者契約または利用規約。電子版でも可。

本 CA は、本要件を満たすために必要であると本 CA が判断するその他のドキュメントをすべて取得する。

証明書の発行前に、本 CA は、本 CA が指定した形式で、かつ Baseline Requirements に準拠する証明書要求を、申請者から取得するものとする。本 CP「4.2.1 識別と認証の手続」の有効期間および更新要件に従い、同じ申請者に発行される複数の証明書に 1 つの証明書要求で対応してもよい。ただし、各証明書が、申請者を代表する適切な申請権限者によって署名された有効な最新の証明書要求によってサポートされていることを条件とする。証明書要求は、電子的に作成、送信、または署名してもよい。

証明書要求には、証明書の発行申請者から、または申請者の代理人からの要求とともに、要求に含まれるすべての情報が正しいことを示す、申請者による、または申請者の代理人による証明が含まれていなければならない。

4.2 証明書申請手続

4.2.1 識別と認証の手続

本 CA は、利用者からの申請に対し、受領した申請書類および CSR の真正性を、本 CP「3.2 初回の識別と認証」に基づき確認する。

証明書要求には、証明書に含めるべき申請者に関するすべての事実情報、および本 CA が Baseline Requirements および本 CA の証明書ポリシーや認証局運用規定に準拠するために申請者から取得する必要がある追加情報を含めてもよい。証明書要求が申請者に関する必要な情報の一部を欠いている場合、本 CA は、残りの情報を申請者から取得するか、または信頼できる独立した第三者機関のデータ情報源から情報を取得して申請者に確認するものとする。本 CA は、申請者によって証明書に含めることを要求されたすべてのデータを検証するための文書化された手順を確立し、それに従うものとする。

© 2003 SECOM Trust Systems Co.,Ltd.

本 CA および下位 CA は、ハイリスクの証明書要求が Baseline Requirements に従って適切に検証されるようにするために合理的に必要な場合において、証明書の承認前にハイリスク証明書要求に対する追加の検証活動を識別し要求する、文書化された手順を作成、保持、実施するものとする。

4.2.2 証明書申請の受理または却下

本 CA は、利用者からの申請に対し予め定められた審査手続に従い、証明書の発行申請の諾否を決定し、その結果を利用者に通知する。

4.2.3 証明書申請の処理時間

本 CA は、利用者からの発行申請を承諾した場合、すみやかに証明書を発行する。

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

本 CA は、利用者から提出された CSR の公開鍵に対し、本 CP「7.1 証明書プロファイル」に準じた内容で、本 CA の私有鍵を用いて署名を付した証明書を発行する。

本 CA による証明書発行では、証明書への署名操作を実行するために、本 CA によって承認された個人(つまり、CA システムオペレーター、システム責任者、または PKI 管理者)に対し、直接コマンドを実行し、慎重に発行する。

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。

本 CA では、有効期限、禁止事項またはコードによる制限回避のため、証明書の notBefore の日付をさかのぼることはしない。

4.3.2 利用者に対する証明書発行通知

本 CA は、受け付けた申請に対する証明書の発行が完了した後、発行した証明書を外部記憶媒体に格納し、受領書とともに封緘したうえで、利用者へ手交、または利用者へ送付する。

4.4 証明書の受領確認

4.4.1 証明書の受領確認手続

利用者は、証明書の内容を確認し、問題が無いと判断した時点で本 CA に対し受領書を送付しなければならない。本 CA は、受領書を受領した時点で証明書の受け入れの完了とする。なお、証明書の内容に誤りがあった場合、利用者は遅滞なくその旨を本 CA に連絡しなければならない。証明書の内容に関する申し立ては、証明書の送付日より 14 日以内に行わなければならない。

© 2003 SECOM Trust Systems Co.,Ltd.

4.4.2 CA による証明書の公開

本 CA の CA 証明書は、リポジトリーに公開される。下位 CA では、CT（Certificate Transparency）ログに登録することにより、証明書利用者の証明書を公開することができる。

4.4.3 他のエンティティに対する CA の証明書発行通知

本 CA は、他のエンティティに対して証明書の発行通知を行わない。

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

本 CA が発行する証明書および利用者が所持する私有鍵の用途は、セコムが提供しているサービスや、セコムと契約関係にある本 CA の利用者が提供しているサービスまたは製品に定めている用途に制限されている。本 CA が発行する証明書を、その他の用途に使用してはならない。

4.5.2 検証者の公開鍵および証明書の用途

検証者は、本 CP および CPS の内容について理解し、承諾した上で本 CA の証明書を使用し、本 CA が発行した証明書の信頼性を検証しなければならない。

4.6 証明書の更新

4.6.1 証明書更新の状況

証明書の更新は、証明書を継続して利用するために、鍵ペアを更新することなく新たな証明書を同じ識別名で発行することをいう。

証明書の更新は、証明書の有効期間が満了する場合等に、更新時点でその鍵に用いられる暗号アルゴリズムが安全であるとセコムが判断した場合に行われる。

4.6.2 証明書更新申請を行うことができる者

本 CP「4.1.1 証明書申請を行うことができる者」と同様とする。

4.6.3 証明書更新申請の処理手続

本 CP「4.2 証明書申請手続」と同様とする。

4.6.4 利用者に対する新しい証明書の通知

本 CP「4.3.2 利用者に対する証明書発行通知」と同様とする。

4.6.5 更新された証明書の受領確認手続

本 CP「4.4.1 証明書の受領確認手続」と同様とする。

© 2003 SECOM Trust Systems Co.,Ltd.

4.6.6 更新された証明書の公開
本 CP「4.4.2 証明書の公開」と同様とする。

4.6.7 他のエンティティに対する CA の証明書発行通知
本 CP「4.4.3 他のエンティティに対する CA の証明書発行通知」と同様とする。

4.7 証明書の鍵更新

4.7.1 鍵更新の状況
鍵更新をともなう証明書の発行は、証明書の有効期間が満了する場合または鍵の危殆化にともない証明書の失効を行った場合等に行われる。

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
本 CP「4.1.1 証明書申請を行うことができる者」と同様とする。

4.7.3 鍵更新をともなう証明書申請の処理手続
本 CP「4.2 証明書申請手続」と同様とする。

4.7.4 利用者に対する新しい証明書の通知
本 CP「4.3.2 利用者に対する証明書発行通知」と同様とする。

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
本 CP「4.4.1 証明書の受領確認手続」と同様とする。

4.7.6 鍵更新済みの証明書の公開
本 CP「4.4.2 証明書の公開」と同様とする。

4.7.7 他のエンティティに対する CA の証明書発行通知
本 CP「4.4.3 他のエンティティに対する CA の証明書発行通知」と同様とする。

4.8 証明書の変更

4.8.1 証明書を変更する場合
証明書の記載事項に変更が生じた場合、利用者は本 CA に対しすみやかに変更に関する申請を行わなければならない。変更にともなう証明書の再発行手続は、初回発行時の手続をもって行われる。なお、変更前の証明書は本 CA の判断により失効が行われる。

4.8.2 証明書の変更申請をすることができる者
本 CP「4.9.2 証明書失効を申請することができる者」および「4.1.1 証明書申請を行うことができる者」と同様とする。

© 2003 SECOM Trust Systems Co.,Ltd.

4.8.3 証明書の変更申請の処理手続

本 CP「4.9.3 失効申請手続」および「4.2 証明書申請手続」と同様とする。

4.8.4 利用者に対する新しい証明書の発行通知

本 CP「4.3.2 利用者に対する証明書発行通知」と同様とする。

4.8.5 変更された証明書の受領確認手続

本 CP「4.4.1 証明書の受領確認手続」と同様とする。

4.8.6 変更された証明書の公開

本 CP「4.4.2 証明書の公開」と同様とする。

4.8.7 他のエンティティに対する CA の証明書発行通知

本 CP「4.4.3 他のエンティティに対する CA の証明書発行通知」と同様とする。

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

利用者は、自らの判断に基づいて証明書の失効申請を行うことができる。ただし、次の事由が発生した場合、利用者は、本 CA に証明書の失効申請を行わなければならない。

- 証明書記載情報に変更があった場合
- 私有鍵が盗難、紛失、漏洩、不正利用等により証明書の信頼性を喪失した可能性がある場合
- 私有鍵が危殆化し機密性が失われた場合またはその可能性がある場合
- 証明書の内容、利用目的が正しくない場合
- 証明書の利用を中止する場合

また、本 CA は、次の事由に該当すると判断した場合、利用者からの失効申請の有無に関わらず、証明書の失効ができるものとする。

- 利用者が本 CP および CPS、契約、法律に基づく義務を履行していない場合
- セコムが、本サービスを終了する場合
- 本 CA が、利用者および本 CA の私有鍵が危殆化した、またはそのおそれがあると判断した場合
- 本 CA が失効を必要とすると判断するその他の状況が認められた場合

下位 CA は、次の 1 つ以上が発生した場合、24 時間以内に Baseline Requirements に基づいて発行される加入者証明書を失効させるものとする。

1. 加入者が書面で下位 CA に加入者証明書の失効を要求している場合。
2. 加入者が下位 CA に対し、元の証明書要求が承認されていなかったこと、および遡

© 2003 SECOM Trust Systems Co.,Ltd.

及的に承認を許可しないことを通知した場合。

3. 下位 CA が、加入者の証明書内の公開鍵に対応する私有鍵が危殆化された証拠を得た場合。
4. 下位 CA は、加入者証明書の公開鍵（Debian の弱い鍵など。 https://wiki.debian.org/SSLkeys を参照）に基づいて加入者の私有鍵を簡単に計算できる、実証済みまたは証明された方法を認識した場合。
5. 下位 CA が、加入者証明書内におけるドメイン認証の承認、または完全修飾ドメイン名や IP アドレスの管理が信用できない証拠を得た場合。

下位 CA は、以下のいずれかが発生した場合、24 時間以内に Baseline Requirements に基づいて発行される加入者証明書を失効させるべきであり、5 日以内に証明書を失効させなければならない。

1. 証明書が本 CP「6.1.5 鍵サイズ」および本 CP「6.1.6 公開鍵のパラメーターの生成および品質検査」の要件に準拠しなくなった場合。
2. 下位 CA が加入者証明書の不正使用の証拠を得た場合。
3. 加入者が加入者契約または利用規約に基づく重大な義務の 1 つ以上に違反していることを本 CA が知り得た場合。
4. 下位 CA が、加入者証明書内における完全修飾ドメイン名または IP アドレスの使用が法的にもはや許可されていないことを示す状況を知り得た場合(たとえば、ドメイン名を使用するドメイン名登録者の権利が裁判所または裁定者によって失効となった、ドメイン名登録者と申請者との間の関連するライセンス契約またはサービス契約が解除された、ドメイン名登録者がドメイン名の更新を怠ったなど)。
5. 詐欺的な紛らわしい下位完全修飾ドメイン名を認証するためにワイルドカード証明書が使用されていたことを本 CA が知り得た場合。
6. 下位 CA が、加入者証明書に含まれている情報の重大な変更を知り得た場合。
7. 証明書が Baseline Requirements または下位 CA の CP や CPS に従って発行されなかったことを下位 CA が知り得た場合。
8. 加入者証明書に表示されている情報が不正確であると、下位 CA が判断または知り得た場合。
9. Baseline Requirements に基づいて加入者証明書を発行するための下位 CA の権利が期限切れ、失効、または終了となった場合。(下位 CA が CRL/OCSP リポジトリーの維持を継続するための手配を済ませている場合を除く)
10. 下位 CA の CP や CPS によって失効が必要になった場合。
11. 下位 CA に、加入者の私有鍵を危殆化させる実証済みの方法、または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場合。

次の 1 つ以上が発生した場合、本 CA は 7 日間以内に Baseline Requirements に基づいて発行される下位 CA 証明書を失効させるものとする。

1. 下位 CA が書面で失効を要求した場合。
2. 下位 CA が発行 CA に対し、元の証明書要求が承認されていなかったこと、および

© 2003 SECOM Trust Systems Co.,Ltd.

遡及的に承認を許可しないことを通知した場合。

3. 発行 CA が、下位 CA の証明書内の公開鍵に対応する私有鍵が危殆化された、または本 CP「6.1.5 鍵サイズ」および本 CP「6.1.6 公開鍵のパラメーターの生成および品質検査」の要件に準拠しなくなった証拠を得た場合。
4. 発行 CA が、証明書の不正使用の証拠を得た場合。
5. 証明書が Baseline Requirements または適用される CP や CPS に従って発行されなかったこと、または下位 CA が Baseline Requirements または適用される CP や CPS に準拠していないことを、発行 CA が知り得た場合。
6. 証明書に表示されている情報が不正確または誤解を招く恐れがあると発行 CA が判断した場合。
7. 発行 CA または下位 CA が何らかの理由で運用を中止したが、証明書の失効サポートが別の CA によって提供されるように手配しなかった場合。
8. Baseline Requirements に基づいて証明書を発行するための発行 CA または下位 CA の権利が期限切れ、失効、または終了となった場合。(発行 CA が CRL/OCSP リポジトリーの維持を継続するための手配を済ませている場合を除く)
9. 発行 CA の CP や CPS によって失効が必要になった場合。

4.9.2 証明書失効を申請することができる者

加入者、RA、または本 CA が失効手続きを開始できる。加えて、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、およびその他の第三者は、証明書失効に関する妥当な根拠となる証明書問題レポートを本 CA に提出できる。

4.9.3 失効申請手続

証明書の失効申請手続は、本 CA に対し証明書失効に関する必要な情報を送付することで行われる。ただし、緊急を要する場合や上記の方法による要求ができない場合、電子メールによる申請も可能である。

本 CA は、失効要求を受け入れ、関連する問い合わせに対応する機能を 24 時間 365 日体制で維持するものとする。

本 CA は、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、およびその他の第三者機関に、私有鍵の危殆化の疑い、証明書の不正使用、またはその他の種類の詐欺、危殆化、不正使用、不適切な実施、あるいは証明書に関連するその他の問題を報告するための明確な指示を与えるものとする。本 CA は、容易にアクセス可能なオンライン手段、ならびに本 CP「1.5.2 連絡先」を通してその指示を公開するものとする。

4.9.4 失効申請の猶予期間

私有鍵が危殆化した場合を除く失効申請は、失効を希望する 5 営業日前までに、本 CA に行わなければならない。ただし、私有鍵が危殆化したまたはそのおそれがある場合は、当該問題を発見後、すみやかに失効申請を行わなければならない。

© 2003 SECOM Trust Systems Co.,Ltd.

4.9.5 CA の失効申請処理の許容時間

証明書問題レポートを受領してから 24 時間以内に、本 CA は証明書問題レポートに関する事実と状況の調査を開始するものとし、加入者と証明書問題レポートを提出した事業体両者の見分に基づく予備調査報告書を提出する。

事実と状況のレビュー後、本 CA は加入者そして証明書問題レポートを報告した事業、または他の失効関連告知と協力するものとし、証明書を失効させるか否か、もしそうなら、本 CA が証明書を失効させる日時を決定する。証明書問題レポートまたは失効関連告知の受領から失効までの期間は、本 CP「4.9.1 証明書失効事由」に記載された時間枠を超えない。

CA に選ばれた日時は次の基準を考慮する。

1. 申し立てられた問題の性質(範囲、状況、厳しさ、規模、被害リスク)
2. 失効の結果（加入者と依拠当事者への直接的そして間接的影響）
3. 特定の証明書または加入者に関して受領した証明書問題レポートの数
4. 苦情を申し立てている組織体

なお、本 CA は、失効日が指定された失効申請を受領した場合は、指定日に失効を行う。

4.9.6 失効確認要求

検証者は、本 CA により発行された証明書を信頼し、利用する前に、CRL または OCSP レスポンダーを確認することにより証明書が失効されていないことを確認しなければならない。

4.9.7 証明書失効リストの発行頻度

本 CA は、少なくとも

i. 12 か月ごと、および

ii. 下位 CA 証明書の失効から 24 時間以内に、CRL を更新および再発行するものとする。

nextUpdate フィールドの値は thisUpdate フィールドの値から 12 か月を超えてはならない。

4.9.8 証明書失効リストの発行の最大遅延時間

CRL は、証明書の発行および失効を行ってから、すみやかに新たな CRL を発行し、リポジトリーに公開する。

4.9.9 オンラインでの失効/ステータス確認の適用性

OCSP レスポンスは、RFC6960 や RFC5019 に準拠している必要がある。OCSP レスポンスは、以下のいずれかの条件を満たす必要がある。

1. 失効ステータスの確認対象となる証明書を発行した CA によって署名されている。
2. 失効ステータスの確認対象となる証明書を発行した CA によって証明書が署名されている OCSP レスポンダーによって署名されている。

後者の場合、OCSP 署名証明書には、RFC6960 に定義されている、タイプ id-pkix-ocsp-nochek の拡張領域が含まれていなければならない。

© 2003 SECOM Trust Systems Co.,Ltd.

4.9.10 オンラインでの失効/ステータス確認を行うための要件

検証者は、本 CA により発行された証明書を信頼し、利用する前に、証明書の有効性を確認しなければならない。リポジトリーに掲載している CRL により、証明書の失効登録の有無を確認しない場合には、OCSP レスポンダーにより提供される証明書ステータス情報の確認を行わなければならない。

RFC 6960 および/または RFC 5019 で説明されているように、CA が運用する OCSP レスポンダーは HTTP GET メソッドをサポートする必要がある。

OCSP 応答の有効期間は、thisUpdate と nextUpdate の時間差（両端を含む）である。その差を算出する目的で、うるう秒を無視すると、3,600 秒の差は 1 時間に等しく、86,400 秒の差は 1 日に等しくなる。

加入者証明書のステータスの場合

1. OCSP 応答には、8 時間以上の有効期間が必要である。
2. OCSP 応答には、10 日以下の有効期間が必要である。
3. 有効期間が 16 時間未満の OCSP 応答の場合、CA は nextUpdate の前の有効期間半分に先立ち、オンライン証明書ステータスプロトコルを介して提供される情報を更新する必要がある。
4. 有効期間が 16 時間以上の OCSP 応答の場合、CA は nextUpdate の少なくとも 8 時間前、および thisUpdate の 4 日後までに、オンライン証明書ステータスプロトコルを介して提供される情報を更新する必要がある。

下位 CA 証明書のステータスの場合

本 CA は、

i. 少なくとも 12 カ月ごと、および
ii. 下位 CA 証明書の失効から 24 時間以内にオンライン証明書ステータスプロトコルを介して提供された情報を更新するものとする。

OCSP レスポンダーが「未使用」の証明書シリアル番号のステータスのリクエストを受信した場合、レスポンダーは「good」ステータスで応答すべきではない。OCSP レスポンダーが本 CP「7.1.5 名前制約」に沿って技術的に制約されていない CA 向けである場合、レスポンダーはそのような要求に対して「good」ステータスで応答してはならない。

本 CA は、セキュリティ応答手順の一部として、「未使用」シリアル番号のリクエストについて OCSP レスポンダーを監視するべきである。

OCSP レスポンダーは、「予約済み」証明書のシリアル番号について、Precertificate [RFC 6962]に一致する対応する証明書があるかのように、明確な応答を提供する場合がある。

OCSP 要求内の証明書シリアル番号は、次の 3 つのオプションのいずれか

1. その CA の主体者に関連付けられている現在または以前のキーを使用して、そのシリアル番号の証明書が発行 CA によって発行された場合、「割り当て済み」
2. そのシリアル番号を持つ事前証明書 [RFC6962]が a または b のいずれか
   a. 発行 CA によって発行された場合、「予約済み」
   b. 発行 CA に関連付けられた事前証明書署名証明書[RFC6962]
3. 上記の条件のいずれも満たされない場合は「未使用」

© 2003 SECOM Trust Systems Co.,Ltd.

4.9.11 利用可能な失効情報の他の形式

本 CA は、RFC4366、RFC 5246、RFC 8446 に従い、ステープリングを利用して OCSP レスポンスを配布できる。この場合、本 CA は利用者が TLS 処理に証明書の OCSP レスポンスを含めることを確実なものにする。本 CA は、利用者に対してこの要件を実施する場合、サービス利用規定または利用者との契約書等、あるいは本 CA による技術確認およびサービス責任者の承認を経て対応するものとする。

4.9.12 鍵の危殆化に対する特別要件

検証者は、次の方法で鍵の危殆化を実証するものとする。

- 私有鍵自体の提出、または私有鍵を含むデータと、データから私有鍵を抽出する方法の提出
- 危殆化されたと認識される識別名などのデータを含み、かつ署名の検証ができる CSR の提出
- 公開鍵によって検証可能な、本 CA が指定したチャレンジ・レスポンスと公開鍵への私有鍵による署名の提出
- 侵害を検証できる脆弱性や、参照したセキュリティ・インシデント・ソースの提供

本 CA は、利用者の私有鍵が危殆化した可能性があることを知りえた場合、利用者に私有鍵が危殆化された可能性があることを通知する。

なお本 CA が、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 CP「4.9.1 証明書失効事由」の対応を行うものとする。

4.9.13 証明書の一時停止

本 CA は、証明書の一時停止を行わない。

4.9.14 証明書の一時停止申請を行うことができる者

適用外とする。

4.9.15 証明書の一時停止申請手続

適用外とする。

4.9.16 一時停止を継続することができる期間

適用外とする。

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

利用者および検証者は OCSP レスポンダーを通じて証明書ステータス情報を確認することができる。

© 2003 SECOM Trust Systems Co.,Ltd.

本 CA は、CRL または OCSP レスポンスの失効エントリーは、失効した証明書の有効期限日が過ぎるまで削除してはならない。

4.10.2 サービスの利用可能性

本 CA は、通常の運用状況の下で 10 秒以内のレスポンス時間を提供するために十分なリソースで、CRL および OCSP 機能を運用および維持するものとする。

本 CA は、アプリケーションソフトウェアが、本 CA によって発行されたすべての有効期限内証明書の現在のステータスを自動的にチェックするために使用できるオンラインリポジトリを 24 時間 365 日体制で維持するものとする。

本 CA は、優先度の高い証明書問題の報告を内部で対応し、必要に応じて当該苦情を法執行機関に通報し、または当該苦情の対象となった証明書を失効させる能力を 24 時間 365 日維持しなければならない。

4.10.3 オプショナルな仕様

規定しない。

4.11 加入（登録）の終了

利用者は本サービスの利用を終了する場合、契約書等に定めたサービスの利用終了手続きを必要とする。

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 CA は、CA 私有鍵を第三者に預託することはない。

4.12.2 セッションキーのカプセル化と鍵回復のポリシーおよび実施

適用外とする。

© 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 立地場所および構造
CPS に規定する。

5.1.2 物理的アクセス
CPS に規定する。

5.1.3 電源および空調
CPS に規定する。

5.1.4 水害対策
CPS に規定する。

5.1.5 火災対策
CPS に規定する。

5.1.6 媒体保管
CPS に規定する。

5.1.7 廃棄処理
CPS に規定する。

5.1.8 オフサイトバックアップ
CPS に規定する。

5.2 手続上の管理

5.2.1 信頼すべき役割
CPS に規定する。

5.2.2 職務ごとに必要とされる人数
CPS に規定する。

5.2.3 個々の役割に対する本人性確認と認証
CPS に規定する。

© 2003 SECOM Trust Systems Co.,Ltd.

5.2.4 職務分割が必要となる役割
CPS に規定する。

5.3 人事的管理

5.3.1 資格、経験および身分証明の要件
CPS に規定する。

5.3.2 背景調査
CPS に規定する。

5.3.3 教育要件
CPS に規定する。

5.3.4 再教育の頻度および要件
CPS に規定する。

5.3.5 仕事のローテーションの頻度および順序
CPS に規定する。

5.3.6 認められていない行動に対する制裁
CPS に規定する。

5.3.7 独立した契約者の要件
CPS に規定する。

5.3.8 要員へ提供される資料
CPS に規定する。

5.4 監査ログの手順

5.4.1 記録されるイベントの種類
CPS に規定する。

5.4.2 監査ログを処理する頻度
CPS に規定する。

5.4.3 監査ログを保持する期間
CPS に規定する。

© 2003 SECOM Trust Systems Co.,Ltd.

5.4.4 監査ログの保護
CPS に規定する。

5.4.5 監査ログのバックアップ手続
CPS に規定する。

5.4.6 監査ログの収集システム
CPS に規定する。

5.4.7 イベントを起こした者への通知
CPS に規定する。

5.4.8 脆弱性評価
CPS に規定する。

5.5 記録の保管

5.5.1 アーカイブの種類
CPS に規定する。

5.5.2 アーカイブ保存期間
CPS に規定する。

5.5.3 アーカイブの保護
CPS に規定する。

5.5.4 アーカイブのバックアップ手続
CPS に規定する。

5.5.5 記録にタイムスタンプを付与する要件
CPS に規定する。

5.5.6 アーカイブ収集システム
CPS に規定する。

5.5.7 アーカイブの検証手続
CPS に規定する。

5.6 鍵の切り替え
CPS に規定する。

© 2003 SECOM Trust Systems Co.,Ltd.

5.7 信頼性喪失や災害からの復旧

5.7.1 事故および危殆化時の手続

CPS に規定する。

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

CPS に規定する。

5.7.3 私有鍵が危殆化した場合の手続

CPS に規定する。

5.7.4 災害後の事業継続性

CPS に規定する。

5.8 認証業務の終了

CPS に規定する。

© 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 鍵ペアの生成
CPS に規定する。

6.1.2 利用者に対する私有鍵の交付
CPS に規定する。

6.1.3 認証局への公開鍵の交付
CPS に規定する。

6.1.4 検証者への CA 公開鍵の交付
CPS に規定する。

6.1.5 鍵サイズ
CPS に規定する。

6.1.6 公開鍵のパラメーターの生成および品質検査
CPS に規定する。

6.1.7 鍵の用途
CPS に規定する。

6.2 私有鍵の保護および暗号装置技術の管理

6.2.1 暗号装置の標準および管理
CPS に規定する。

6.2.2 私有鍵の複数人管理
CPS に規定する。

6.2.3 私有鍵のエスクロー
CPS に規定する。

6.2.4 私有鍵のバックアップ
CPS に規定する。

© 2003 SECOM Trust Systems Co.,Ltd.

6.2.5 私有鍵のアーカイブ
CPS に規定する。

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
CPS に規定する。

6.2.7 暗号装置への私有鍵の格納
CPS に規定する。

6.2.8 私有鍵の活性化方法
CPS に規定する。

6.2.9 私有鍵の非活性化方法
CPS に規定する。

6.2.10 私有鍵の破棄方法
CPS に規定する。

6.2.11 暗号装置の評価
CPS に規定する。

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
CPS に規定する。

6.3.2 私有鍵および公開鍵の有効期間
CPS に規定する。

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
CPS に規定する。

6.4.2 活性化データの保護
CPS に規定する。

6.4.3 活性化データの他の考慮点
CPS に規定する。

© 2003 SECOM Trust Systems Co.,Ltd.

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

CPS に規定する。

6.5.2 コンピュータセキュリティ評価

CPS に規定する。

6.6 セキュリティ技術のライフサイクル管理

6.6.1 システム開発管理

CPS に規定する。

6.6.2 セキュリティ運用管理

CPS に規定する。

6.6.3 ライフサイクルセキュリティ管理

CPS に規定する。

6.7 ネットワークセキュリティ管理

CPS に規定する。

6.8 タイムスタンプ

CPS に規定する。

© 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

本 CA は、本 CP「2.2 証明書情報の公開」、本 CP「6.1.5 鍵サイズ」、本 CP「6.1.6 公開鍵のパラメーターの生成および品質検査」に規定された技術要件を満たすものとする。
本 CA が下位 CA の CA 証明書を発行する際や下位 CA から加入者証明書を発行する際、暗号論的擬似乱数生成器(CSPRNG)からの 64 ビット以上の出力を含む 1 以上の連番ではない証明書シリアル番号を生成するものとする。

本 CA が発行する証明書は、X.509 フォーマット証明書形式により作成される。
表「7.1-1 基本証明書領域」に示すフィールドを用いる。

表 7.1-1 証明書基本領域

フィールド	説明
Version （バージョン番号）	Version: 3 (0x2)
SerialNumber （シリアル番号）	CA 内で一意の番号*1
Signature （電子署名アルゴリズム識別子）	本サービスで用いられる電子署名アルゴリズムの識別子*2
Issuer （発行者名）	発行者情報 （本 CA が指定する情報）
Validity （有効期間）	証明書の有効期間 （開始期日および終了期日）
Subject （下位 CA 利用者名）	下位 CA 利用者情報
SubjectPublicKeyInfo （下位 CA 利用者の公開鍵情報）	下位 CA 利用者の公開鍵アルゴリズム識別子と公開鍵データ
Extensions （拡張フィールド）	本 CP「7.1.2 証明書拡張」を参照

*1　新規に証明書が作成されたとき CA サーバーにより付与される。
*2　証明書に電子署名する際に用いられる。

7.1.1 バージョン番号

本 CA が発行する証明書の X.509 フォーマットのバージョン番号は、Version3 である。

7.1.2 証明書拡張

本 CA が発行する証明書は、X.509 証明書拡張フィールドを使用する。
次の表に示すフィールドを用いる。

© 2003 SECOM Trust Systems Co.,Ltd.

表 7.1-2-1 Root CA 共通の証明書拡張

フィールド	記載事項(説明)
authorityKeyIdentifier (2.5.29.35)	存在しない
subjectKeyIdentifier (2.5.29.14)	Root CA の公開鍵を SHA-1 によりハッシュした 160bit 値
keyUsage (2.5.29.15)	Criticalに設定 keyCertSign,cRLSign RootCA 私有鍵が OCSP 応答の署名に使用される場合は、digitalSignature を設定
extendedKeyUsage (2.5.29.37)	存在しない
certificatePolicies (2.5.29.32)	存在しない
basicConstraints (2.5.29.19)	Criticalに設定 Subject Type=CA pathLenConstraints は存在しない

© 2003 SECOM Trust Systems Co.,Ltd.

表 7.1-2-2 Security Communication RootCA1 下位 CA 証明書拡張

フィールド	記載事項(説明)
authorityKeyIdentifier (2.5.29.35)	CA の公開鍵を SHA-1 によりハッシュした 160bit 値
subjectKeyIdentifier (2.5.29.14)	利用者の公開鍵を SHA-1 によりハッシュした 160bit 値
keyUsage (2.5.29.15)	Criticalに設定 keyCertSign,cRLSign（利用者公開鍵の使用目的）
extendedKeyUsage (2.5.29.37)	2019 年 1 月 1 日以降は必ず設定するが、 anyExtendedKeyUsage は設定しない。id-kp-serverAuth と id-kp-emailProtection は同時に設定しない。 クロス証明書の場合は、必要に応じて設定する。
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.901.1　または any Policy policyQualifierID=id-qt-cps any Policy qualifier=CPS=http(s)://repository.secomtrust.net/SC-Root1/ ※()内は任意
basicConstraints (2.5.29.19)	Criticalに設定 Subject Type=CA pathLenConstraints（必要に応じて設定する）
cRLDistributionPoints (2.5.29.31)	URI:http://repository.secomtrust.net/SC-Root1/ SCRoot1CRL.crl（ディレクトリ上にある CRL 配布場所）
Authority Information Access(1.3.6.1.5.5.7.1.1)	accessMethod OCSP (1.3.6.1.5.5.7.48.1) accessLocation URI:http://scrootca1.ocsp.secomtrust.net accessMethod CA Issuers (1.3.6.1.5.5.7.48.2) accessLocation http://repository.secomtrust.net/SC-Root1/SCRoot1ca.cer *OCSP, CA Issuers は必要に応じて設定する

表 7.1-2-3 Security Communication RootCA1 OCSP レスポンダー証明書拡張

フィールド	記載事項(説明)
authorityKeyIdentifier (2.5.29.35)	CA の公開鍵を SHA-1 によりハッシュした 160bit 値
subjectKeyIdentifier (2.5.29.14)	利用者の公開鍵を SHA-1 によりハッシュした 160bit 値
keyUsage (2.5.29.15)	digitalSignature（利用者公開鍵の使用目的）
extendedKeyUsage (2.5.29.37)	OCSPSigning
OCSP No Check (1.3.6.1.5.5.7.48.1.5)	null
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.901.1 policyQualifierID=id-qt-cps qualifier=CPS=http(s)://repository.secomtrust.net/SC-Root1/ ※()内は任意

© 2003 SECOM Trust Systems Co.,Ltd.

表 7.1-2-4 Security Communication RootCA2 下位 CA 証明書拡張

フィールド	記載事項(説明)
authorityKeyIdentifier (2.5.29.35)	CA の公開鍵を SHA-1 によりハッシュした 160bit 値
subjectKeyIdentifier (2.5.29.14)	利用者の公開鍵を SHA-1 によりハッシュした 160bit 値
keyUsage (2.5.29.15)	Criticalに設定 keyCertSign,cRLSign（利用者公開鍵の使用目的）
extendedKeyUsage (2.5.29.37)	2019 年 1 月 1 日以降は必ず設定するが、anyExtendedKeyUsage は設定しない。id-kp-serverAuth と id-kp-emailProtection は同時に設定しない。 id-kp-codeSigning は、単独で設定する。 クロス証明書の場合は、必要に応じて設定する。
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.901.4、CA/Browser Forum の予約済み証明書ポリシー識別子、 1.2.392.200091.100.721.1 または any Policy *1 policyQualifierID=id-qt-cps qualifier=CPS=http(s)://repository.secomtrust.net/SC-Root2/ ※()内は任意
basicConstraints (2.5.29.19)	Criticalに設定 Subject Type=CA pathLenConstraints（本 CA で必要に応じて設定する）
Name Constraints (2.5.29.30)	Criticalに設定するべき （extendedKeyUsage が id-kp-serverAuth または id-kp-emailProtection で発行先を限定する場合に設定する）
cRLDistributionPoints (2.5.29.31)	URI:http://repository.secomtrust.net/SC-Root2/ SCRoot2CRL.crl（ディレクトリ上にある CRL 配布場所）
Authority Information Access(1.3.6.1.5.5.7.1.1)	accessMethod OCSP (1.3.6.1.5.5.7.48.1) accessLocation URI:http://scrootca2.ocsp.secomtrust.net accessMethod CA Issuers (1.3.6.1.5.5.7.48.2) accessLocation http://repository.secomtrust.net/SC-Root2/SCRoot2ca.cer *OCSP, CA Issuers は必要に応じて設定する

*1　EV 証明書の発行の場合、EV 証明書用の OID（1.2.392.200091.100.721.1）または any Policy を設定しても良い。

表 7.1-2-5 Security Communication RootCA2 OCSP レスポンダー証明書拡張

フィールド	記載事項(説明)
authorityKeyIdentifier	CA の公開鍵を SHA-1 によりハッシュした 160bit 値

© 2003 SECOM Trust Systems Co.,Ltd.

フィールド	記載事項(説明)
(2.5.29.35)	
subjectKeyIdentifier (2.5.29.14)	利用者の公開鍵を SHA-1 によりハッシュした 160bit 値
keyUsage (2.5.29.15)	digitalSignature（利用者公開鍵の使用目的）
extendedKeyUsage (2.5.29.37)	OCSPSigning
OCSP No Check (1.3.6.1.5.5.7.48.1.5)	null
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.901.4 policyQualifierID=id-qt-cps qualifier=CPS=http(s)://repository.secomtrust.net/SC-Root2/ ※()内は任意

© 2003 SECOM Trust Systems Co.,Ltd.

表 7.1-2-6 Security Communication RootCA3 下位 CA 証明書拡張

フィールド	記載事項(説明)
authorityKeyIdentifier (2.5.29.35)	CA の公開鍵を SHA-1 によりハッシュした 160bit 値
subjectKeyIdentifier (2.5.29.14)	利用者の公開鍵を SHA-1 によりハッシュした 160bit 値
keyUsage (2.5.29.15)	Criticalに設定 keyCertSign,cRLSign（利用者公開鍵の使用目的）
extendedKeyUsage (2.5.29.37)	2019 年 1 月 1 日以降は必ず設定するが、anyExtendedKeyUsage は設定しない。id-kp-serverAuth と id-kp-emailProtection は同時に設定しない。 id-kp-codeSigning は、単独で設定する。 クロス証明書の場合は、必要に応じて設定する。
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.901.6、CA/Browser Forum の予約済み証明書ポリシー識別子、 1.2.392.200091.100.721.1 または any Policy *1 policyQualifierID=id-qt-cps qualifier=CPS=http(s)://repository.secomtrust.net/SC-Root3/ ※()内は任意
basicConstraints (2.5.29.19)	Criticalに設定 Subject Type=CA pathLenConstraints（本 CA で必要に応じて設定する）
Name Constraints (2.5.29.30)	Criticalに設定するべき （extendedKeyUsageがid-kp-serverAuthまたは id-kp-emailProtectionで発行先を限定する場合に設定する）
cRLDistributionPoints (2.5.29.31)	URI:http://repository.secomtrust.net/SC-Root3/ SCRoot3CRL.crl（ディレクトリ上にある CRL 配布場所）
Authority Information Access(1.3.6.1.5.5.7.1.1)	accessMethod OCSP (1.3.6.1.5.5.7.48.1) accessLocation URI:http://scrootca3.ocsp.secomtrust.net accessMethod CA Issuers (1.3.6.1.5.5.7.48.2) accessLocation http://repository.secomtrust.net/SC-Root3/SCRoot3ca.cer *OCSP, CA Issuers は必要に応じて設定する

*1　EV 証明書の発行の場合、EV 証明書用の OID（1.2.392.200091.100.721.1）または any Policy を設定しても良い。

表 7.1-2-7 Security Communication RootCA3 OCSP レスポンダー証明書拡張

フィールド	記載事項(説明)

© 2003 SECOM Trust Systems Co.,Ltd.

フィールド	記載事項(説明)
authorityKeyIdentifier (2.5.29.35)	CA の公開鍵を SHA-1 によりハッシュした 160bit 値
subjectKeyIdentifier (2.5.29.14)	利用者の公開鍵を SHA-1 によりハッシュした 160bit 値
keyUsage (2.5.29.15)	digitalSignature（利用者公開鍵の使用目的）
extendedKeyUsage (2.5.29.37)	OCSPSigning
OCSP No Check (1.3.6.1.5.5.7.48.1.5)	null
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.901.6 policyQualifierID=id-qt-cps qualifier=CPS=http(s)://repository.secomtrust.net/SC-Root3/ ※()内は任意

© 2003 SECOM Trust Systems Co.,Ltd.

表 7.1-2-8 Security Communication ECC RootCA1 下位 CA 証明書拡張

フィールド	記載事項(説明)
authorityKeyIdentifier (2.5.29.35)	CA の公開鍵を SHA-1 によりハッシュした 160bit 値
subjectKeyIdentifier (2.5.29.14)	利用者の公開鍵を SHA-1 によりハッシュした 160bit 値
keyUsage (2.5.29.15)	Criticalに設定 keyCertSign,cRLSign（利用者公開鍵の使用目的）
extendedKeyUsage (2.5.29.37)	以下のいずれかを設定 (1) id-kp-serverAuth (2) id-kp-serverAuth および id-kp-clientAuth クロス証明書の場合は、必要に応じて設定する。
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.902.1、CA/Browser Forum の予約済み証明書ポリシー識別子、 1.2.392.200091.100.721.1 または any Policy *1 policyQualifierID=id-qt-cps qualifier=CPS=http(s)://repository.secomtrust.net/SC-ECC-Root1/ ※()内は任意
basicConstraints (2.5.29.19)	Criticalに設定 Subject Type=CA pathLenConstraints（必要に応じて設定する）
Name Constraints (2.5.29.30)	Criticalに設定するべき （extendedKeyUsageがid-kp-serverAuthまたは id-kp-emailProtectionで発行先を限定する場合に設定する）
cRLDistributionPoints (2.5.29.31)	URI:http://repository.secomtrust.net/SC-ECC-Root1/ SCECCRoot1CRL.crl（ディレクトリ上にある CRL 配布場所）
Authority Information Access(1.3.6.1.5.5.7.1.1)	accessMethod OCSP (1.3.6.1.5.5.7.48.1) accessLocation URI:http://sceccrootca1.ocsp.secomtrust.net accessMethod CA Issuers (1.3.6.1.5.5.7.48.2) accessLocation http://repository.secomtrust.net/SC-ECC-Root1/SCECCRoot1ca.cer *OCSP, CA Issuers は必要に応じて設定する

*1　EV 証明書の発行の場合、EV 証明書用の OID（1.2.392.200091.100.721.1）または any Policy を設定しても良い。

表 7.1-2-9 Security Communication ECC RootCA1 OCSP レスポンダー証明書拡張

© 2003 SECOM Trust Systems Co.,Ltd.

フィールド	記載事項(説明)
authorityKeyIdentifier (2.5.29.35)	CA の公開鍵を SHA-1 によりハッシュした 160bit 値
subjectKeyIdentifier (2.5.29.14)	利用者の公開鍵を SHA-1 によりハッシュした 160bit 値
keyUsage (2.5.29.15)	digitalSignature（利用者公開鍵の使用目的）
extendedKeyUsage (2.5.29.37)	OCSPSigning
OCSP No Check (1.3.6.1.5.5.7.48.1.5)	null
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.902.1 policyQualifierID=id-qt-cps qualifier=CPS=http(s)://repository.secomtrust.net/SC-ECC-Root1/ ※()内は任意

7.1.3 アルゴリズムオブジェクト識別子

本サービスにおいて用いられるアルゴリズム OID は、次のとおりである。

Baseline Requirements に準拠している下位 CA は、「Security Communication RootCA1」を RootCA とせず、アルゴリズムに「sha1 With RSA Encryption」を使用しない。

表 7.1-3-1 Security Communication RootCA1 アルゴリズム OID

アルゴリズム	オブジェクト識別子
sha1 With RSA Encryption	1.2.840.113549.1.1.5
sha256 With RSA Encryption	1.2.840.113549.1.1.11
RSA Encryption	1.2.840.113549.1.1.1

表 7.1-3-2 Security Communication RootCA2 アルゴリズム OID

アルゴリズム	オブジェクト識別子
sha256 With RSA Encryption	1.2.840.113549.1.1.11
RSA Encryption	1.2.840.113549.1.1.1

表 7.1-3-3 Security Communication RootCA3 アルゴリズム OID

アルゴリズム	オブジェクト識別子
sha384 With RSA Encryption	1.2.840.113549.1.1.12
RSA Encryption	1.2.840.113549.1.1.1

表 7.1-3-4 Security Communication ECC RootCA1 アルゴリズム OID

アルゴリズム	オブジェクト識別子
ecdsa-with-SHA384	1.2.840.10045.4.3.3

© 2003 SECOM Trust Systems Co.,Ltd.

ecPublicKey	1.2.840.10045.2.1
secp384r1	1.3.132.0.34

© 2003 SECOM Trust Systems Co.,Ltd.

7.1.4 名前形式

本 CA では、RFC5280 で定められる、識別名を使用する。

TLS 証明書の発行に使用されない、新規発行される全下位 CA 証明書は、以下の要件を満たすべきであり、その他の全証明書については、当該証明書が CA 証明書であるか加入者証明書であるかにかかわらず、満たさなければならない。

すべての有効な認証パス（RFC 5280、セクション 6 で定義されているとおり）について

- 認証パスの加入者証明書ごとに、証明書発行者の識別名フィールドのエンコードされた内容は、発行される CA 証明書の主体者識別名フィールドのエンコードされた形式とバイト単位で同一である必要がある。
- 認証パスの CA 証明書ごとに、加入者証明書の主体者識別名フィールドのエンコードされた内容は、期限切れおよび失効した証明書を含み、RFC 5280 セクション 7.1 に従い主体者識別名が等しいとされるすべての証明書間で、バイト単位で同一でなければならない。

本 CA および利用者は、X.500 識別名に従って定義された識別名によって一意に識別される。

表「7.1-4-1 使用可能文字」に識別名に使用可能な文字を示す。

表 7.1-4-1 使用可能文字

英字	数字	記号
A～Z、a～z	0～9	- . と空白

7.1.5 名前制約

下位 CA 証明書の extendedKeyUsage に id-kp-serverAuth が含まれている場合、下位 CA 証明書には、dNSName、iPAddress、および DirectoryName が以下のように制約される X.509v3 Name Constraints 拡張領域が含まれている必要がある。

a. Permitted サブツリー内の各 dNSName に関して、CA は、Baseline Requirements 3.2.2.4 の検証手順に従い、申請者が dNSName を登録したこと、または申請者がドメイン登録者の代わりを務める権限を登録者から得ていることを確認する必要がある。

b. Permitted サブツリー内の各 IP アドレス範囲に関して、CA は、申請者が IP アドレス範囲を割り当てられていること、または IP アドレス範囲を割り当てられている者から代理権限が与えられていることを確認する必要がある。

c. Permitted サブツリー内の各 DirectoryName に関して、CA は、下位 CA 証明書から発行されたエンドエンティティ証明書が Baseline Requirements 7.1.2.4 や Baseline Requirements 7.1.2.5 に準拠するよう、申請者またはその子会社の組織名や場所を確認する必要がある。

下位 CA 証明書が IP アドレスのある証明書の発行を禁じられている場合、下位 CA 証明書は、Excluded サブツリー内で IPv4 および IPv6 のアドレス範囲全体を指定する必要がある。下位 CA 証明書には、Excluded サブツリー内に、8 つのゼロオクテット(0.0.0.0/0 の IPv4

© 2003 SECOM Trust Systems Co.,Ltd.

アドレス範囲を含む)から成る iPAddress GeneralName を含める必要がある。下位 CA 証明書にはまた、Excluded サブツリー内に、32 個のゼロオクテット(0/0 の IPv6 アドレス範囲を含む)から成る iPAddress GeneralName を含める必要がある。そうでない場合、下位 CA 証明書には、Permitted サブツリー内に少なくとも 1 つの iPAddress を含める必要がある。

下位 CA が DNS ドメイン名のある証明書の発行を禁じられている場合、下位 CA 証明書の Excluded サブツリー内には、長さゼロの dNSName を含める必要がある。そうでない場合、下位 CA 証明書の Permitted サブツリー内には、少なくとも 1 つの dNSName を含める必要がある。

下位 CA 証明書の extendedKeyUsage に id-kp-emailProtection が含まれている場合、rfc822Name に制約を加えた Name Constraints X.509v3 拡張領域を含むものとし、permittedSubtrees に少なくとも 1 つの名前が含まれ、そのような名前はそれぞれ Baseline Requirements 3.2.2.4 の検証手順に従い所有権が検証されるものとする。

7.1.6 CP オブジェクト識別子

本 CA が発行する証明書に記載されるポリシーOID は、表「1.2-2 OID（本 CP)」のとおりである。

次の証明書ポリシー識別子は、証明書または加入者証明書が Baseline Requirements に準拠していることを表明するオプションの手段として本 CA または下位 CA が使用するために用意されている。

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) domain-validated(1)} (2.23.140.1.2.1)

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)} (2.23.140.1.2.2)

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) ev-guidelines(1)} (2.23.140.1.1)

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) code-signing-requirements(3)} (2.23.140.1.3)

7.1.7 ポリシー制約拡張の利用

設定しない。

7.1.8 ポリシー修飾子の文法および意味

ポリシー修飾子については、本 CP および CPS を公表する Web ページの URI を格納し

© 2003 SECOM Trust Systems Co.,Ltd.

ている。

7.1.9 重要な証明書ポリシー拡張の処理の意味

設定しない。

© 2003 SECOM Trust Systems Co.,Ltd.

7.2 CRL のプロファイル

本 CA が発行する CRL は、X.509 CRL フォーマット形式により作成される。

表「7.2-1 CRL 基本領域」に示すフィールドを用いる。

表 7.2-1 CRL 基本領域

フィールド	説明
Version （バージョン番号）	Version: 2 (0x1)
Signature （電子署名アルゴリズム識別子）	本 CA が電子署名に用いるアルゴリズムの識別子*1
Issuer （発行者名）	CRL の発行者情報 （本 CA が指定する情報）
ThisUpdate （更新日）	CRL の発行日時
NextUpdate （次回更新予定日）	CRL の次の更新予定日時
RevokedCertificates （失効リスト）	失効となった証明書の情報 SerialNumber（シリアル番号） RevocationDate（失効日付） Reason Code（失効事由） が設定される

*1　CRL に署名する際に用いられる。

7.2.1 バージョン番号

本 CA が発行する CRL の X.509 フォーマットバージョン番号は、Version2 である。

7.2.2 CRL 拡張

本 CA が発行する X.509CRL 拡張フィールドを使用する。

reasonCode (OID 2.5.29.21)

2020 年 9 月 30 日より、次の要件をすべて満たす必要がある。

reasonCode が存在する場合、この拡張を critical としてマークしてはならない。

CRL エントリーがルート CA または下位 CA 証明書（クロス証明書を含む）のためのものである場合、この CRL エントリー拡張が存在しなければならない。

CRL エントリーが CA ではなく、加入者証明書用である場合、この CRL エントリー拡張は存在すべきであるが、以下の要件を満たすことを条件に省略してもよい。

CRLReason は、unspecified (0)であってはならない。失効の理由が特定されていない場合、以前の要件で許可されていれば、CA は reasonCode エントリー拡張を省略しなければならない。CRL エントリーが Baseline Requirements の対象とならない証明書用であり、2020 年 9 月 30 日以降に発行されたか、2020 年 9 月 30 日以降に notBefore（発行日）である場合、CRLReason は certificateHold (6)を使用してはいけない。CRL エントリーが Baseline Requirements の対象となる証明書用である場合、CRLReason は certificateHold (6)を使用してはいけない。

reasonCode CRL エントリー拡張が存在する場合、CRLReason は、その CP/CPS 内の CA によって定義されているように、証明書の失効の最も適切な理由を示さなければならない。

© 2003 SECOM Trust Systems Co.,Ltd.

本 CA では、以下の reasonCode を使用するものとする。

keyCompromise (1)
affiliationChanged (3)
superseded (4)
cessationOfOperation (5)

表「7.2-2-1 CRL 拡張」に示すフィールドを用いる。

表 7.2-2-1 CRL 拡張

フィールド	説明
AuthorityKeyIdentifier （認証機関鍵識別子）	CA の公開鍵を SHA-1 によりハッシュした 160bit 値

7.3 OCSP のプロファイル

本 CA は、RFC6960、5019 に準拠する OCSP レスポンダーを提供する。

2020 年 9 月 30 日以降より、OCSP 応答がルート CA または下位 CA 証明書（クロス証明書を含む）に対するものであり、その証明書が失効されている場合、CertStatus の RevokedInfo 内の revocationReason フィールドが存在する必要がある。

2020 年 9 月 30 日以降より、CRLReason は、本 CP「7.2.2 CRL 拡張」で指定されているように、CRL に許可された値を含める必要があることを示す。

7.3.1 バージョン番号

本 CA は、OCSP バージョン 1 を適用する。

7.3.2 OCSP 拡張

「7.1 証明書のプロファイル」に記載する。

OCSP 応答の singleExtensions には、reasonCode（OID 2.5.29.21）CRL エントリー拡張を含めてはならない。

© 2003 SECOM Trust Systems Co.,Ltd.

8. 準拠性監査

8.1 監査の頻度

CPS に規定する。

8.2 監査人の身分と資格

CPS に規定する。

8.3 監査人と被監査対象との関係

CPS に規定する。

8.4 監査で扱われる事項

CPS に規定する。

8.5 監査指摘事項への対応

CPS に規定する。

8.6 監査結果の報告

CPS に規定する。

8.7 自己監査

CPS に規定する。

© 2003 SECOM Trust Systems Co.,Ltd.

9. 他の業務上および法的問題

9.1 料金

9.1.1 証明書の発行または更新にかかる料金

契約書等に別途定める。

9.1.2 証明書のアクセス料金

規定しない。

9.1.3 失効またはステータス情報のアクセス料金

規定しない。

9.1.4 他サービスの料金

規定しない。

9.1.5 代金返金ポリシー

契約書等に別途定める。

9.2 財務的責任

9.2.1 保険の補償

セコムは、本 CA の提供にあたり、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

CA であるセコムが保持する個人および組織の情報は、証明書、CRL、本 CP および CPS 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。セコムは、法の定めによる場合および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

© 2003 SECOM Trust Systems Co.,Ltd.

ム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。

利用者の私有鍵は、その利用者によって機密保持すべき情報である。本サービスでは、いかなる場合でもこれらの鍵へのアクセス手段を提供していない。

監査ログに含まれる情報および監査報告書は、機密保持対象情報である。セコムは、CPS「8.6 監査結果の報告」に記載されている場合および法の定めによる場合を除いて、これらの情報を社外へ開示しない。

9.3.2 機密保持対象外の情報

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
- セコム以外の出所から、機密保持の制限無しにセコムに知られた、あるいは知られるようになった情報
- セコムによって独自に開発された情報
- 開示に関して利用者によって承認されている情報

9.3.3 機密情報の保護責任

CA であるセコムが保持する機密情報を、法の定めによる場合および利用者による事前の承諾を得た場合に開示することがある。その際、その情報を知り得たものは、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本 CA の運用に必要な範囲で利用する。セコムの個人情報保護方針については、セコムのホームページ(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。本 CA の運用

© 2003 SECOM Trust Systems Co.,Ltd.

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

セコムは、法令で定められた場合を除き、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、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

セコムと利用者との間で別段の合意がなされない限り、本サービスにかかわる情報資料およびデータは、次に示す当事者の権利に属するものとする。

利用者証明書	セコムに帰属する財産である。
CRL	セコムに帰属する財産である。
識別名	利用者証明書に対して対価が支払われている限りにおいて、その名前が付与された者に帰属する財産である。
利用者の私有鍵	私有鍵は、その保存方法または保存媒体の所有者にかかわらず、公開鍵と対になる私有鍵を所有する利用者に帰属する財産である。
利用者の公開鍵	保存方法または保存媒体の所有者にかかわらず、対になる私有鍵を所有する利用者に帰属する財産である。
本 CP および CPS	セコムに帰属する財産（著作権を含む）である。 本 CP, 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

セコムは、本 CP および CPS に規定した内容を遵守して利用者に関する審査、証明書の

© 2003 SECOM Trust Systems Co.,Ltd.

登録、発行、失効を含む認証サービスを提供し、CA 私有鍵の信頼性を含む認証業務の信頼性を確保する。

本 CP および CPS に規定された保証を除き、セコムは、明示的あるいは暗示的に、もしくはその他の方法を問わず、一切の保証を行わない。

本 CA または下位 CA は、証明書を発行することによって、下記の証明書受益者に対し、本書に規定されている証明書の保証を行うものとする。

1. 証明書の加入者契約または利用規約の当事者である加入者。
2. 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にルート証明書を含めるため、ルート CA と契約を締結しているすべてのアプリケーションソフトウェアサプライヤー。
3. 有効な証明書に合理的に依拠しているすべての依拠当事者。CA は、証明書の受益者に対し、証明書が有効である間、CA が証明書の発行および管理において Baseline Requirements およびその CP/CPS に従ってきたことを表明し、保証するものとする。

証明書の保証には、具体的に以下が含まれるが、これらに限定されない。

1. ドメイン名または IP アドレスを使用する権利
   発行の時点で、下位 CA が、以下を満たすこと。
   i. 証明書の主体者フィールドおよび subjectAltName 拡張領域に指定されているドメイン名および IP アドレスを使用する権利を申請者が保持または管理していること(あるいは、ドメイン名の場合のみ、かかる権利または管理が、それらを使用または管理する権利を有する他の人物によって委託されたこと)を検証するための 手順を導入していること。
   ii. 証明書を発行する際にその手順に従っていること。
   iii. CA の CP/CPS にその手順を正確に記述していること。
2. 証明書に対する承認
   発行の時点で、下位 CA が、以下を満たすこと。
   i. 主体者によって証明書の発行が承認され、主体者を代表して証明書を要求する権限を申請権限者が有していることを確認するための手順を導入していること。
   ii. 証明書を発行する際にその手順に従っていること。
   iii. CA の CP/CPS にその手順を正確に記述していること。
3. 情報の正確性
   発行の時点で、下位 CA が、以下を満たすこと。
   i. 証明書に含まれるすべての情報(主体者識別名の organizationalUnitName 属性を除く)の正確性を検証するための手順を導入していること。
   ii. 証明書を発行する際にその手順に従っていること。
   iii. CA の CP/CPS にその手順を正確に記述していること。
4. 誤解を招く情報の排除
   発行の時点で、下位 CA が、以下を満たすこと。
   i. 証明書の主体者識別名の organizationalUnitName に含まれる情報が誤解

© 2003 SECOM Trust Systems Co.,Ltd.

を与えるものである可能性を減らすための手順を導入していること。
ii. 証明書を発行する際にその手順に従っていること。
iii. CA の CP/CPS にその手順を正確に記述していること。

5. 申請者のアイデンティティ
証明書に主体者アイデンティティ情報が含まれる場合、下位 CA が、以下を満たすこと。
i. Baseline Requirements セクション 3.2 およびセクション 7.1.4.2.2 に従って申請者のアイデンティティを検証するため手順を導入していること。
ii. 証明書を発行する際にその手順に従っていること。
iii. CA の CP/CPS にその手順を正確に記述していること。

6. 加入者契約
下位 CA および加入者が関連会社でない場合、加入者および下位 CA は、Baseline Requirements を満たす法的に有効で実施可能な加入者契約の当事者であること。あるいは、下位 CA および加入者が同じ組織体または関連会社である場合、申請権限者が利用規約に同意したこと。

7. ステータス
本 CA または下位 CA が、有効期限内のすべての証明書のステータス(有効または失効)に関する最新情報を掲載した、24 時間 365 日アクセス可能なリポジトリーを保守し、公開していること。

8. 失効
Baseline Requirements に示された事由が発生した場合、本 CA または下位 CA が証明書を失効させること。

ルート CA は、自らが証明書を発行する下位 CA であるかのように、下位 CA による責務の履行と保証、下位 CA による Baseline Requirements の遵守、Baseline Requirements に基づく下位 CA のすべての責任および免責義務に対して責任を負う。

9.6.2 RA の表明保証
本 CP「9.6.1 CA の表明保証」と同様とする。

9.6.3 利用者の表明保証
本 CA または下位 CA は、加入者契約または利用規約の一部として、CA および証明書の受益者の利益のために、申請者が本項で規定されているコミットメントおよび保証を行うことを要求するものとする。
本 CA または下位 CA は、CA と証明書受益者の明示的な利益のため、証明書の発行前に下記のいずれかを取得するものとする。

1. CA との加入者契約に対する申請者の合意。
2. 利用規約に対する申請者の合意。

本 CA または下位 CA は、各加入者契約または利用規約が申請者に対して法的強制力を持つことを確実にするためのプロセスを実装するものとする。いずれの場合も、契約書は、

© 2003 SECOM Trust Systems Co.,Ltd.

証明書要求に従って発行される証明書に準じている必要がある。CA は、電子契約または「クリックスルー」契約を使用してもよい。ただし、このような契約が法的強制力を持つと CA が判断した場合に限る。証明書要求ごとに別々の契約を用いることも、または単一の契約で複数の将来の証明書要求およびその結果発行される証明書を対象とすることもできる。ただし CA が申請者に対して発行する各証明書が、明確にその加入者契約書または利用規約の対象となっていることを条件とする。

加入者契約または利用規約には、以下の義務および保証が申請者自身に課される(または請負やホスティングサービス関係に基づいて、申請者が本人や代理人を代表して策定した)条項が含まれていなければならない。

1. 情報の正確性
   証明書要求内において、また証明書の発行に関連して CA から要求された場合において、常に正確で完全な情報を CA に提供する義務および保証。
2. 私有鍵の保護
   利用者は、要求された証明書に含まれる公開鍵に対応する私有鍵（および関連する活性化データまたはデバイス（パスワードまたはトークンなど））の管理を保証し、秘密を保持し、常に適切に保護するために、あらゆる合理的な手段を講じる義務および保証を負うものとする。
3. 証明書の受理
   利用者が証明書の内容の正確性を確認および検証する義務およびその保証。
4. 証明書の使用
   TLS サーバー証明書の場合、証明書に記載されている subjectAltName でアクセス可能なサーバーにのみ証明書をインストールする。
   すべての適用法規に準拠し、加入者契約または利用規約に従う方法でのみ証明書を使用する義務およびその保証。
5. 報告および失効
   以下を実行する義務および保証。
   a. 証明書に含まれる公開鍵に対応する加入者の私有鍵が不正使用または危殆化された事実または疑いがある場合、すみやかに証明書の失効を要求し、証明書と関連する私有鍵の使用を中止する。
   b. 証明書内の情報が正確ではない、または正確でなくなる場合、直ちに証明書の失効を要求し、証明書の使用を中止する。
6. 証明書の使用の終了
   鍵の危殆化を理由として証明書が失効された場合、証明書に含まれる公開鍵に対応する私有鍵のすべての使用を直ちに中止する義務および保証。
7. 対応
   鍵の危殆化または証明書の不正使用に関して CA から指示があった場合、指定された期間内に対応する義務。
8. 確認および承認
   申請者が加入者契約の条件または利用規約に違反した場合、または CA の CP、CPS、

© 2003 SECOM Trust Systems Co.,Ltd.

もしくはBaseline Requirementsによって失効が要求された場合、CAが証明書を直ちに失効する権利があることの確認と承認。

9.6.4 検証者の表明保証

本CAのサービスの検証者は、以下の義務を負う。

- 本CAが発行する証明書を信頼し、本CPおよびCPSに規定されている本CAが意図する目的のみに証明書を使用すること
- 証明書を信頼しようとするときは、リポジトリー内のCRLまたはOCSPレスポンダーにより、証明書が失効されていないことを確認すること
- 証明書を信頼しようとするときは、当該証明書の有効期間を確認し、有効期間内であることを確認すること
- 本CAが発行した証明書を信頼しようとするときは、当該証明書が本CAの証明書によって署名検証できることを確認すること
- 本CAの証明書を信頼して利用する際、本CPおよびCPSに規定されている検証者として責任を負うことに合意すること

9.6.5 他の関係者の表明保証

規定しない。

9.7 保証の制限

セコムは、本CP「9.6.1 CAの表明保証」および「9.6.2 RAの表明保証」に規定する保証に関連して発生するいかなる間接損害、特別損害、付随的損害または派生的損害に対する責任を負わず、また、いかなる逸失利益、データの紛失またはその他の間接的もしくは派生的損害に対する責任を負わない。

9.8 責任の制限

本CP「9.6.1 CAの表明保証」および「9.6.2 RAの表明保証」の内容に関し、次の場合、セコムは責任を負わないものとする。

- セコムに起因しない不法行為、不正使用ならびに過失等により発生する一切の損害
- 利用者または検証者が自己の義務の履行を怠ったために生じた損害
- 利用者または検証者のシステムに起因して発生した一切の損害
- セコム、利用者または検証者のハードウェア、ソフトウェアの瑕疵、不具合あるいはその他の動作自体によって生じた損害
- 利用者が契約に基づく契約料金を支払っていない間に生じた損害
- セコムの責に帰することのできない事由で証明書、CRLおよびOCSPレスポンダーに公開された情報に起因する損害
- セコムの責に帰することのできない事由で正常な通信が行われない状態で生じた一切の損害
- 証明書の使用に関して発生する取引上の債務等、一切の損害
- 現時点の予想を超えた、ハードウェア的あるいはソフトウェア的な暗号アルゴリズム解

© 2003 SECOM Trust Systems Co.,Ltd.

読技術の向上に起因する損害

・ 天変地異、地震、噴火、火災、津波、水災、落雷、戦争、動乱、テロリズムその他の不可抗力に起因する、本 CA の業務停止を含む本 CA のサービスの業務停止に起因する一切の損害

9.9 補償

本 CA が発行する証明書を申請、受領、信頼した時点で、利用者および検証者には、セコムおよび関連する組織等に対する損害賠償責任および保護責任が発生する。当該責任の対象となる事象には、損失、損害、訴訟、あらゆる種類の費用負担の原因となるようなミス、怠慢な行為、各種行為、履行遅滞、不履行のうち、証明書申請時に利用者が本 CA に最新かつ正確な情報を提供しなかったことに起因するもの、または各種責任、損失、損害、訴訟、あらゆる種類の費用負担の原因となるような利用者および検証者のミス、怠慢な行為、各種行為、履行遅滞、不履行等の各種責任が含まれる。

9.10 有効期間と終了

9.10.1 有効期間

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

9.10.2 終了

本 CP 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が本 CA を終了した時点で無効となる。

9.10.3 終了の効果と効果継続

利用者が証明書の利用を終了する場合、または、セコムがサービス提供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、利用者および本 CA に適用されるものとします。

9.11 関係者間の個別通知と連絡

本 CA は、利用者および検証者に対する必要な通知を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

(1) 重要な変更

セコムは、本 CP 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 CP 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 CP（本 CP 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

© 2003 SECOM Trust Systems Co.,Ltd.

び検証者に対して変更の告知を行う。また、本 CP 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 CP 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 CP 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 CP（本 CP 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 CP 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 CP を変更した場合、すみやかに変更した本 CP（本 CP 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 CP 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

認証サービス改善委員会で必要であると判断した場合に、OID を変更する。

9.13 紛争解決手段

本 CA のサービスの利用に関し、セコムに対して訴訟、仲裁を含む法的またはその他の解決手段に訴えようとする場合、セコムに対して事前にその旨を通知するものとする。

9.14 準拠法

本 CA、利用者および検証者の所在地にかかわらず、本 CP および CPS の解釈、有効性および本サービスにかかわる紛争については、日本国の法律が適用される。仲裁および裁判地は東京都区内における紛争処理機関を専属的管轄とする。

9.15 適用法の遵守

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

9.16 雑則

9.16.1 完全合意条項

セコムは、本サービスの提供にあたり、自らのポリシーおよび保証ならびに利用者または検証者の義務等を本 CP、CPS および契約によって包括的に定め、これ以外の口頭、書面または黙示的になされたいかなる合意も効力を有しないものとする。

9.16.2 権利譲渡条項

セコムが本サービスを第三者に譲渡する場合、本 CP および CPS において記載された責

© 2003 SECOM Trust Systems Co.,Ltd.

務およびその他の義務の譲渡を可能とする。

9.16.3 分離条項

本 CP および 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

本サービスに関する紛争は東京地方裁判所を管轄裁判所とし、セコムは、各規定文書の契約条項に起因する紛争、当事者の行為に関する損害、損失および費用について、補償および弁護士費用を当事者に求めることができる。

9.16.5 不可抗力

セコムは、天変地異、地震、噴火、火災、津波、水災、落雷、動乱、テロリズム、その他の不可抗力により生じた一切の損害について、その予見可能性の有無を問わず一切責任を負わないものとし、本 CA の提供を不可能にするに至ったときは、セコムトラストシステムズはその状況の止むまでの間、本 CA を停止することができる。

9.17 その他の条項

規定しない。

© 2003 SECOM Trust Systems Co.,Ltd.