Security Communication RootCA

下位 CA 用証明書ポリシ

2018 年 11 月 28 日
Version5.11

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 下位 CA 用証明書ポリシを作成。 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 下位 CA 用証明書ポリシを Security Communication RootCA 下位 CA 用証明書ポリシとし、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

© 2003 SECOM Trust Systems Co.,Ltd.

目次

1. はじめに....1
1.1 概要....1
1.2 文書の名前と識別....1
1.3 PKI の関係者....2
1.3.1 CA....2
1.3.2 RA....2
1.3.3 利用者....2
1.3.4 検証者....2
1.3.5 その他関係者....2
1.4 証明書の使用方法....2
1.4.1 適切な証明書の用途....3
1.4.2 禁止される証明書の用途....3
1.5 ポリシ管理....3
1.5.1 文書を管理する組織....3
1.5.2 連絡先....3
1.5.3 ポリシ適合性を決定する者....3
1.5.4 承認手続....3
1.6 定義と略語....3
2. 公表とリポジトリーの責任....7
2.1 リポジトリー....7
2.2 証明書情報の公開....7
2.3 公開の時期および頻度....7
2.4 リポジトリーへのアクセスコントロール....7
3. 識別と認証....8
3.1 名前....8
3.1.1 名前の種類....8
3.1.2 意味のある名前の必要性....8
3.1.3 利用者の匿名性または仮名性....8
3.1.4 さまざまな名前の形式を解釈するための規則....8
3.1.5 名前の一意性....8
3.1.6 認識、認証および商標の役割....8
3.2 初回の識別と認証....8
3.2.1 私有鍵の所有を証明する方法....8
3.2.2 組織の認証....8
3.2.3 個人の認証....9
3.2.4 検証されない利用者の情報....9
3.2.5 権限の正当性確認....9
3.2.6 相互運用の基準....9

© 2003 SECOM Trust Systems Co.,Ltd.

3.3 鍵更新申請時の識別と認証 9
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 9
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 9
3.4 失効申請時の識別と認証 9
4. 証明書のライフサイクルに対する運用要件 9
4.1 証明書申請 9
4.1.1 証明書申請を行うことができる者 9
4.1.2 申請手続および責任 10
4.2 証明書申請手続 10
4.2.1 識別と認証の手続 10
4.2.2 証明書申請の受理または却下 10
4.2.3 証明書申請の処理時間 10
4.3 証明書発行 10
4.3.1 証明書の発行時における CA の処理手続 10
4.3.2 利用者に対する証明書発行通知 10
4.4 証明書の受領確認 10
4.4.1 証明書の受領確認手続 10
4.4.2 CA による証明書の公開 11
4.4.3 他のエンティティに対する CA の証明書発行通知 11
4.5 鍵ペアと証明書の用途 11
4.5.1 利用者の私有鍵および証明書の用途 11
4.5.2 検証者の公開鍵および証明書の用途 11
4.6 証明書の更新 11
4.6.1 証明書の更新事由 11
4.6.2 証明書更新申請を行うことができる者 11
4.6.3 証明書更新申請の処理手続 11
4.6.4 利用者に対する新しい証明書の通知 11
4.6.5 更新された証明書の受領確認手続 11
4.6.6 更新された証明書の公開 11
4.6.7 他のエンティティに対する CA の証明書発行通知 12
4.7 鍵更新をともなう証明書の更新 12
4.7.1 鍵更新をともなう証明書の更新事由 12
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 12
4.7.3 鍵更新をともなう証明書更新申請の処理手続 12
4.7.4 利用者に対する新しい証明書の通知 12
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 12
4.7.6 鍵更新済みの証明書の公開 12
4.7.7 他のエンティティに対する CA の証明書発行通知 12
4.8 証明書の変更 12
4.8.1 証明書を変更する場合 12

© 2003 SECOM Trust Systems Co.,Ltd.

4.8.2 証明書の変更申請をすることができる者 12
4.8.3 証明書の変更申請の処理手続 13
4.8.4 利用者に対する新しい証明書の発行通知 13
4.8.5 変更された証明書の受領確認手続 13
4.8.6 変更された証明書の公開 13
4.8.7 他のエンティティに対する CA の証明書発行通知 13
4.9 証明書の失効および一時停止 13
4.9.1 証明書失効事由 13
4.9.2 証明書失効を申請することができる者 13
4.9.3 失効申請手続 13
4.9.4 失効申請の猶予期間 14
4.9.5 CA の失効申請処理の許容時間 14
4.9.6 失効確認要求 14
4.9.7 証明書失効リストの発行頻度 14
4.9.8 証明書失効リストの発行の最大遅延時間 14
4.9.9 オンラインでの失効/ステータス確認の適用性 14
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 14
4.9.11 利用可能な失効情報の他の形式 14
4.9.12 鍵の危殆化に対する特別要件 14
4.9.13 証明書の一時停止 14
4.9.14 証明書の一時停止申請を行うことができる者 15
4.9.15 証明書の一時停止申請手続 15
4.9.16 一時停止を継続することができる期間 15
4.10 証明書のステータス確認サービス 15
4.10.1 運用上の特徴 15
4.10.2 サービスの利用可能性 15
4.10.3 オプショナルな仕様 15
4.11 加入（登録）の終了 15
4.12 キーエスクローと鍵回復 15
4.12.1 キーエスクローと鍵回復ポリシおよび実施 15
4.12.2 セッションキーのカプセル化と鍵回復のポリシおよび実施 15
5. 物理的、手続上、人事的管理 16
5.1 物理的管理 16
5.2 手続上の管理 16
5.3 人事的管理 16
5.4 監査ログの手順 16
5.5 記録の保管 16
5.6 鍵の切り替え 16
5.7 信頼性喪失や災害からの復旧 16
5.8 認証業務の終了 16

© 2003 SECOM Trust Systems Co.,Ltd.

6. 技術的セキュリティ管理 17
6.1 鍵ペアの生成とインストール 17
6.2 私有鍵の保護および暗号装置技術の管理 17
6.3 鍵ペア管理のその他の側面 17
6.4 活性化データ 17
6.5 コンピュータのセキュリティ管理 17
6.6 セキュリティ技術のライフサイクル管理 17
6.7 ネットワークセキュリティ管理 17
6.8 タイムスタンプ 17
7. 証明書、CRL および OCSP のプロファイル 18
7.1 証明書のプロファイル 18
7.1.1 バージョン番号 18
7.1.2 証明書拡張 18
7.1.3 アルゴリズムオブジェクト識別子 23
7.1.4 名前形式 24
7.1.5 名前制約 24
7.1.6 CP オブジェクト識別子 24
7.1.7 ポリシ制約拡張の利用 24
7.1.8 ポリシ修飾子の文法および意味 24
7.1.9 重要な証明書ポリシ拡張の処理の意味 24
7.2 CRL のプロファイル 25
7.2.1 バージョン番号 25
7.2.2 CRL 拡張 25
7.3 OCSP のプロファイル 25
7.3.1 バージョン番号 25
7.3.2 OCSP 拡張 25
8 準拠性監査 26
8.1 監査の頻度 26
8.2 監査人の身分と資格 26
8.3 監査人と被監査対象との関係 26
8.4 監査で扱われる事項 26
8.5 監査指摘事項への対応 26
8.6 監査結果の報告 26
9. 他の業務上および法的問題 27
9.1 料金 27
9.1.1 証明書の発行または更新にかかる料金 27
9.1.2 証明書のアクセス料金 27
9.1.3 失効またはステータス情報のアクセス料金 27
9.1.4 他サービスの料金 27
9.1.5 代金返金ポリシ 27

© 2003 SECOM Trust Systems Co.,Ltd.

9.2 財務的責任 27
9.2.1 保険適用範囲 27
9.2.2 その他の資産 27
9.2.3 エンドエンティティの保険または保証範囲 27
9.3 企業情報の機密性 27
9.3.1 機密情報の範囲 27
9.3.2 機密保持対象外の情報 28
9.3.3 機密情報の保護責任 28
9.4 個人情報の保護 28
9.5 知的財産権 28
9.6 表明保証 29
9.6.1 CA の表明保証 29
9.6.2 RA の表明保証 29
9.6.3 利用者の表明保証 29
9.6.4 検証者の表明保証 29
9.6.5 他の関係者の表明保証 29
9.7 保証の制限 30
9.8 責任の制限 30
9.9 補償 30
9.10 有効期間と終了 30
9.10.1 有効期間 30
9.10.2 終了 31
9.10.3 終了の効果と効果継続 31
9.11 関係者間の個別通知と連絡 31
9.12 改訂 31
9.12.1 改訂手続 31
9.12.2 通知方法および期間 31
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 31
9.13 紛争解決手段 32
9.14 準拠法 32
9.15 適用法の遵守 32
9.16 雑則 32
9.16.1 完全合意条項 32
9.16.2 権利譲渡条項 32
9.16.3 分離条項 32
9.16.4 強制執行条項 32
9.16.5 不可抗力 32
9.17 その他の条項 32

© 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（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 で定められた規定に準拠する。
なお、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 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」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 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）

© 2003 SECOM Trust Systems Co.,Ltd.

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。

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。

1.3.5 その他関係者

規定しない。

1.4 証明書の使用方法

© 2003 SECOM Trust Systems Co.,Ltd.

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

1.5.3 ポリシ適合性を決定する者

本 CP が、本 CA のポリシ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 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。

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。

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

© 2003 SECOM Trust Systems Co.,Ltd.

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

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

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。

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（CP）

© 2003 SECOM Trust Systems Co.,Ltd.

Certificate Policy の略。証明書に関するポリシ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の決定等を行う意思決定組織。

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 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、全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

本 CP 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
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

証明書発行者の名前と発行対象である利用者の名前は、X.500 の識別名（DN：Distinguished Name） 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

DN 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

証明書に記載される主体者名は､本 CA の発行したすべての証明書 において一意とする。

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、利用者 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

利用者は、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
- 組織または団体が実在していることを証明する情報

© 2003 SECOM Trust Systems Co.,Ltd.

・ 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。

3.2.3 **個人の認証**
本 CA は、個人に対する証明書発行は行わない。

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）について検証を行なわない。

3.2.5 **権限の正当性確認**
本 CA は、利用者となる組織または団体の代表者、社員または代理人が、その組織または団体に関する情報の申請を行うための正当な権限を有していることを確認する。

3.2.6 **相互運用の基準**
設定しない。

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。

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。

© 2003 SECOM Trust Systems Co.,Ltd.

4.1.2 申請手続および責任

利用者は、本 CA より事前に通知された手続に従い、証明書の申請を行う。利用者は、証明書の発行申請を行うにあたり、本 CP、CPS、その他本 CA より開示された文書の内容を承諾しているものとする。
利用者は、本 CA に対する申請内容が正確な情報であることを保証しなければならない。

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。

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。

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 は、下位 CA となる利用者の証明書の公開を原則として行わない。

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 証明書の更新事由

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 DN 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であって、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。

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。

© 2003 SECOM Trust Systems Co.,Ltd.

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 **鍵更新をともなう証明書の更新**

4.7.1 **鍵更新をともなう証明書の更新事由**

鍵更新をともなう証明書の更新は、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。

4.7.4 **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、証明書の失効および初回発行時の手続をもって行われる。

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 の私有鍵が危殆化したまたはそのおそれがあると判断された場合
- 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

4.9.2 証明書失効を申請することができる者

証明書の失効申請は、失効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。

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

© 2003 SECOM Trust Systems Co.,Ltd.

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、代替策として、電子メールによる申請も可能である。

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。

4.9.5 CA の失効申請処理の許容時間

本 CA は、有効な失効申請を受け付けてからすみやかに証明書の失効を実行する。

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 サーバ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

CRL は、前回の発行から 1 年以内に新たな CRL が発行される。また、証明書の発行および失効を行った場合にも新たな CRL が発行される。

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

オンラインでの証明書ステータス情報は、OCSP サーバーを通じて提供される。

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

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 サーバ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。

4.9.11 利用可能な失効情報の他の形式

規定しない。

4.9.12 鍵の危殆化に対する特別要件

規定しない。

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。

© 2003 SECOM Trust Systems Co.,Ltd.

4.9.14 **証明書の一時停止申請を行うことができる者**
規定しない。

4.9.15 **証明書の一時停止申請手続**
規定しない。

4.9.16 **一時停止を継続することができる期間**
規定しない。

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 **サーバ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。**

4.10.2 **サービスの利用可能性**
本 CA **は、**24 **時間** 365 **日、証明書ステータス情報を確認できるよう** OCSP **サーバーを管理する。ただし、保守等により、一時的に** OCSP **サーバーを利用できない場合もある。**

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**
証明書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および実施**
規定しない。

© 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
CPS に規定する。

5.2 手続上の管理
CPS に規定する。

5.3 人事的管理
CPS に規定する。

5.4 監査ログの手順
CPS に規定する。

5.5 記録の保管
CPS に規定する。

5.6 鍵の切り替え
CPS に規定する。

5.7 信頼性喪失や災害からの復旧
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
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
CPS に規定する。

6.3 鍵ペア管理のその他の側面
CPS に規定する。

6.4 活性化データ
CPS に規定する。

6.5 コンピュータのセキュリティ管理
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
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 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）	証明書フォーマットの番号*1
SerialNumber （シリアル番号）	CA 内で一意の番号*2
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*3
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 （利用者名）	利用者情報
SubjectPublicKeyInfo （利用者の公開鍵情報）	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　証明書フォーマットの番号は Version3 に設定される。

*2　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。

*3　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。

表「7.1-2 Security Communication RootCA1 下位 CA 証明書拡張」、表「7.1-3 Security Communication RootCA1 OCSP サーバー証明書拡張」、表「7.1-4 Security Communication RootCA2 下位 CA 証明書拡張」、表「7.1-5 Security Communication RootCA2 OCSP サーバー証明書拡張」表「7.1-6 Security Communication RootCA3 下位 CA 証明書拡張」、表「7.1-7 Security Communication RootCA3 OCSP サーバー証明書拡張」、表「7.1-8 Security Communication ECC RootCA1 下位 CA 証明書拡張」、表「7.1-9 Security Communication ECC RootCA1 OCSP サーバー証明書拡張」、に示すフィールドを用いる。

表 7.1-2 Security Communication RootCA1 下位 CA 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)	keyCertSign,cRLSign（利用者公開鍵の使用目的）
extendedKeyUsage (2.5.29.37)	（必要に応じて本 CA で設定する）
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=https://repository.secomtrust.net/SC-Root1/
basicConstraints (2.5.29.19)	Subject Type=CA pathLenConstraints（本 CA で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)	OCSP - URI:http://scrootca1.ocsp.secomtrust.net（OCSP サーバー公開場所）

表 7.1-3 Security Communication RootCA1 OCSP サーバー証明書拡張

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=https://repository.secomtrust.net/SC-Root1/

© 2003 SECOM Trust Systems Co.,Ltd.

表 7.1-4 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)	keyCertSign,cRLSign（利用者公開鍵の使用目的）
extendedKeyUsage (2.5.29.37)	（必要に応じて本 CA で設定する）
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.901.4　または any Policy policyQualifierID=id-qt-cps qualifier=CPS=https://repository.secomtrust.net/SC-Root2/
basicConstraints (2.5.29.19)	Subject Type=CA pathLenConstraints（本 CA で必要に応じて設定する）
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)	OCSP - URI:http://scrootca2.ocsp.secomtrust.net（OCSP サーバー公開場所）

表 7.1-5 Security Communication RootCA2 OCSP サーバー証明書拡張

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=1.2.392.200091.100.901.4 policyQualifierID=id-qt-cps qualifier=CPS=https://repository.secomtrust.net/SC-Root2/

© 2003 SECOM Trust Systems Co.,Ltd.

表 7.1-6 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)	keyCertSign,cRLSign（利用者公開鍵の使用目的）
extendedKeyUsage (2.5.29.37)	（必要に応じて本 CA で設定する）
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.901.6　または any Policy policyQualifierID=id-qt-cps qualifier=CPS=https://repository.secomtrust.net/SC-Root3/
basicConstraints (2.5.29.19)	Subject Type=CA pathLenConstraints（本 CA で必要に応じて設定する）
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)	OCSP - URI:http://scrootca3.ocsp.secomtrust.net（OCSP サーバー公開場所）

表 7.1-7 Security Communication RootCA3 OCSP サーバー証明書拡張

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=1.2.392.200091.100.901.6 policyQualifierID=id-qt-cps qualifier=CPS=https://repository.secomtrust.net/SC-Root3/

© 2003 SECOM Trust Systems Co.,Ltd.

表 7.1-8 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)	keyCertSign,cRLSign（利用者公開鍵の使用目的）
extendedKeyUsage (2.5.29.37)	（必要に応じて本 CA で設定する）
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.902.1　または any Policy policyQualifierID=id-qt-cps qualifier=CPS=https://repository.secomtrust.net/SC-ECC-Root1/
basicConstraints (2.5.29.19)	Subject Type=CA pathLenConstraints（本 CA で必要に応じて設定する）
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)	OCSP - URI:http://sceccrootca1.ocsp.secomtrust.net（OCSP サーバー公開場所）

表 7.1-9 Security Communication ECC RootCA1 OCSP サーバー証明書拡張

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=1.2.392.200091.100.902.1 policyQualifierID=id-qt-cps qualifier=CPS=https://repository.secomtrust.net/SC-ECC-Root1/

© 2003 SECOM Trust Systems Co.,Ltd.

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、表「7.1-10 Security Communication RootCA1 アルゴリズム OID」、表「7.1-11 Security Communication RootCA2 アルゴリズム OID」、表「7.1-12 Security Communication RootCA3 アルゴリズム OID」、表「7.1-13 Security Communication ECC RootCA1 アルゴリズム OID」のとおりである。

表 7.1-10 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 7.1-11 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 7.1-12 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 7.1-13 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
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 および利用者は、X.500 識別名に従って定義された DN によって一意に識別される。
表「7.1-14 使用可能文字」に DN に使用可能な文字を示す。

表 7.1-14 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

設定しない。

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 OID は、表「1.2-2 OID（本 CP)」のとおりである。

7.1.7 ポリシ制約拡張の利用

設定しない。

7.1.8 ポリシ修飾子の文法および意味

ポリシ修飾子については、本 CP および CPS を公表する Web ページの URI を格納している。

7.1.9 重要な証明書ポリシ拡張の処理の意味

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）	CRL フォーマットの番号*1
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*2
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） が設定される

*1　CRL フォーマットの番号は Version2 に設定される。

*2　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。

表「7.2-2 CRL 拡張」に示すフィールドを用いる。

表 7.2-2 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、RFC2560、5019 に準拠する OCSP サーバーを提供する。

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

規定しない。

© 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。

© 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
料金体系については、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
規定しない。

9.2 財務的責任

9.2.1 保険適用範囲
セコムは、本サービスの提供にあたり、十分な財務的基盤を維持するものとし、別途定める。

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
本 CP「9.2.1 保険適用範囲」と同様とする。

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

© 2003 SECOM Trust Systems Co.,Ltd.

として扱われる情報を開示することができる。また会社の合併、買収あるいは再編成に関連してアドバイスする弁護士、会計士、金融機関およびその他の専門家に対しても、セコム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

本 CA が取得する個人情報は、本 CP「9.3 企業情報の機密性」のとおり機密情報として取り扱う。また、本 CA は、個人情報に関する法律または関連する法令およびセコムが一般に公開しているプライバシポリシを遵守する。

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（DN）	：	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

© 2003 SECOM Trust Systems Co.,Ltd.

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

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。

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 の利用者は、以下の義務を負う。

- **本 CA に、利用者が把握できる範囲内で正確かつ完全な情報を提供する。当該情報に変更があった場合には、その旨をすみやかに本 CA に通知する。**
- **危殆化から自身の私有鍵を保護する。**
- **証明書の使途は本 CP および CPS に従うものとし、かつ法令に反しないこと。**
- **利用者が､証明書に記載の公開鍵に対応する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や、登録情報に変更があった場合、利用者は本 CA に証明書の失効をすみやかに要求すること。**

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 サーバーにより、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。

© 2003 SECOM Trust Systems Co.,Ltd.

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 サーバ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

⑴ 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。

⑵ 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

規定しない。

© 2003 SECOM Trust Systems Co.,Ltd.

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。

9.16.4 強制執行条項

規定しない。

9.16.5 不可抗力

規定しない。

9.17 その他の条項

規定しない。

© 2003 SECOM Trust Systems Co.,Ltd.