Security Communication RootCA1

証明書ポリシ/認証運用規定

2003 年 9 月 29 日

Version 1.00

セコムトラストネット株式会社

改版履歴		
版数	日付	内容
V1.00	2003.09.29	初版発行

目次

1. はじめに

1.1 概要

証明書ポリシ（CP：Certificate Policy）及び認証運用規定（CPS：Certification Practice Statement）は、認証機関（CA:Certification Authority）が行う証明書の発行、取消、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き、証明書の発行、利用に関わる主体の責任及び証明書に関して、適用範囲、セキュリティ基準、審査基準を記述したものである。

Security Communication RootCA1（以下、「本 CA」という）の行うサービス（以下、「本サービス」という）は、セコムトラストネット株式会社（以下、「セコムトラストネット」という）が運営し、認証機関として CA の鍵管理を行い、加入者*1 に対して証明書発行、取消等を提供するサービスである。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し、その審査過程、登録、発行手続は、本 CP/CPS によって規定される。利用者*2 はセコムトラストネットによって発行された証明書を利用する際、本 CP/CPS の内容を利用者自身の利用方法に照らし、評価する必要がある。

なお、別途加入者との間で契約書等が存在する場合、本 CP/CPS より契約書等の文書が優先される。

*1：加入者とは、ルート CA である本 CA の秘密鍵により署名された下位 CA の証明書の発行を受ける組織又は団体をいう。
*2：利用者とは、本サービスで発行された証明書を信頼して利用する者をいい、署名検証者と同義である。

1.2 文書の名前と識別

本 CP/CPS の正式名称は「Security Communication RootCA1 証明書ポリシ/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トラストネットには、次表に示す ISO 割当に従ったオブジェクト識別子（Object ID：OID）が割り当てられている。

組織名	OID
セコムトラストネット株式会社（SECOM Trust.net Co., Ltd.）	1.2.392.200091

本 CP/CPS は、次表に示す OID により識別される。

CP/CPS	OID
Security Communication RootCA1 証明書ポリシ/認証運用規定	1.2.392.200091.100.901.1

1.3 PKI の関係者

1.3.1 CA

CA は、証明書の発行、取消、取消情報の開示及び保管等の各業務を行う。

1.3.2 RA

RA は、証明書発行申請者となる組織、団体からの証明書発行、取消等の各種要求に対する実在性確認、本人性認証、運用規定の審査等を行う。

1.3.3 加入者

加入者とは、証明書発行申請を行い、自ら鍵を生成し、本 CA より下位 CA としての証明書の発行を受ける組織又は団体をいう。本 CA に証明書の発行申請を行い、本 CA より発行された証明書を受容した時点で加入者となる。

1.3.4 利用者

利用者とは署名検証者と同義であり、加入者証明書を信頼して利用する者をいう。利用者は、本 CP/CPS の内容を利用者自身の利用目的に照らして評価したうえで利用しているとみなされる。

1.4 証明書の使用方法

本 CA はルート CA であり、加入者に対して下位 CA の証明書を発行する。下位 CA を信頼して利用する利用者は、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。

1.5 ポリシ管理

1.5.1 CP/CPS を管理する組織

本 CP/CPS の維持・管理は、セコムトラストネットが行う。

1.5.2 連絡先

本 CP/CPS に関しての問い合わせ窓口は次のとおりである。

本サービス窓口	：	セコムトラストネット株式会社　CA サポートセンタ
住所	：	〒150-0001　東京都渋谷区神宮前 1-5-1
電子メールアドレス	：	root1-support@secomtrust.net

1.5.3 CP/CPS のポリシ適合性を決定する者

本 CP/CPS が、本サービスの運営方針として適切か否かの判断は、セコムトラストネットセキュリティポリシ委員会が行う。

1.5.4 CP/CPS 承認手続

本 CP/CPS は、セコムトラストネットセキュリティポリシ委員会による承認のもと、作成、変更、リポジトリでの公開が行われる。

2. 公表とリポジトリの責任

2.1 リポジトリ

本 CA は、CRL 情報にアクセスできるようリポジトリを維持管理する。リポジトリへのアクセスに用いるプロトコルは HTTP（HyperText Transfar Protocol)、HTTPS（HTTP に SSL によるデータの暗号化機能を付加したプロトコル）を用いる。リポジトリの情報は一般的な 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に格納し、加入者および利用者がオンラインによって閲覧可能とする。

・ 本 CP/CPS に基づく証明書取消リスト（CRL）
・ 本 CA の自己署名証明書
・ 最新の CP/CPS
・ 本 CP/CPS に基づく証明書に関するその他関連情報

2.3 公開の時期および頻度

本 CP/CPS は、本 CP/CPS「9.12 改訂」に記述されているとおり随時変更の都度公表される。CRL は発行の都度、リポジトリに公表される。CRL 発行の頻度は、本 CP/CPS「4.9.7 証明書取消リストの発行頻度」で規定される。

2.4 リポジトリへのアクセスコントロール

リポジトリは加入者及び利用者に対して参照可能とする。ただし、保守等により、一時的にリポジトリを利用できない場合もある。

3. 識別と認証

3.1 名前

3.1.1 名前の種類

電子証明書発行者の名前と発行対象である加入者の名前は、X.500 の識別名（DN：Distinguished Name）形式に従い、且つ本 CP/CPS「7.1.4 名前形式」に則って設定する。

3.1.2 意味ある名前の必要性

加入者の識別名は、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、組織もしく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。

加入者は、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 加入者の匿名性又は仮名性

証明書に記載される主体者名は、匿名や仮名は原則使用しない。

3.1.4 さまざまな名前の形式を解釈するためのルール

DN は、本 CP/CPS「3.1.1 名前の種類」および「3.1.2 意味ある名前の必要性」で定義しているとおりに解釈する。

3.1.5 名前の一意性

証明書に記される主体者名は､本 CA の発行した全ての証明書において明瞭かつ一意とする。

3.1.6 認識、認証及び商標の役割

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 初回の本人性確認

3.2.1 秘密鍵の所有を証明する方法

本 CA は、証明書申請者 から提出された証明書発行要求（CSR：Certificate Signing Request）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 秘密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 組織もしくは団体の本人性認証

証明書申請者は、証明書の発行申請時に、申請者の公開鍵と組織又は団体に関する情報を、本 CA に提供しなければならない。本 CA は、申請に誤りや欠落情報がないことを確認

する。

3.2.3 個人の本人性認証

本 CA は、個人に対する証明書発行は行わない。

3.2.4 権限の正当性確認

本 CA は、組織又は団体に関する情報の申請を行う組織又は団体の代表者、社員もしくは代理人が、その組織又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か確認する。

3.3 鍵更新申請時の本人性確認と認証

3.3.1 通常の秘密鍵更新に伴なう証明書申請時の本人性確認と認証

本 CP/CPS「3.2 初回の本人性確認」と同様の手続による。

3.3.2 証明書取消後の秘密鍵更新に伴なう証明書申請時の本人性確認と認証

本 CP/CPS「3.2 初回の本人性確認」と同様の手続による。

3.4 取消申請時の本人性確認と認証

本 CA は、証明書の取消申請を受付けた場合、提出された加入者の情報を元に、適正な要求である事を確認する。

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 証明書申請を提出することができる者

証明書の発行申請は、組織又は団体の代表者、社員もしくは代理人が行うことができる。

4.1.2 登録手続及び責任

証明書申請者は、証明書申請に際して、本 CA に以下の情報を提供するものとする。

・証明書発行申請書
・組織若しくは団体が実在していることを証明する情報
・CSR

証明書申請者は、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。

証明書申請者は、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 本人確認と認証機能の実行

本 CA は、証明書申請者からの申請に対し、受領した申請書類及び CSR の真正性を、「3.2 初回の本人性確認」に基づき確認する。

4.2.2 証明書申請の承認又は却下

本 CA は、証明書申請者からの申請に対しあらかじめ定められた審査基準に従い、証明書申請の諾否を決定し、その結果を証明書申請者に通知する。

4.2.3 証明書申請の処理時間

本 CA は、証明書申請者からの申請を承諾した場合、速やかに証明書を発行する。

4.3 証明書発行

4.3.1 証明書の発行過程における認証局の行為

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

4.3.2 加入者に対する証明書発行通知

本 CA は、受付けた申請に対する証明書の発行が完了した後、発行した証明書をフロッピ

ーディスク等の外部記憶媒体に保管し、受領書とともに封緘し、手交又は郵送により証明書申請者宛に送付する。

4.4 証明書の受領確認

4.4.1 証明書の受領確認の行為

証明書申請者が証明書の内容を確認し、受容の意思を示したと考えられる時点で、証明書の受入れの完了とする。なお、証明書の内容に誤りがあった場合、証明書申請者は遅滞なくその旨を本 CA に連絡しなければならない。証明書の送付日より 14 日経過しても受容の連絡がなければ、本 CA は証明書申請者が証明書を受容したものとみなす。

4.4.2 証明書の公開

本 CA は、加入者の証明書の公開は原則として行わない。

4.4.3 利用者に対する証明書発行通知

下位 CA となる加入者のエンドエンティティ、その他利用者に対する証明書の発行通知は、加入者の責任のもと行うものとする。

4.5 鍵ペアと証明書の用途

4.5.1 加入者の秘密鍵及び証明書の使用

本 CA が発行する証明書の用途は、セコムトラストネットが提供しているサービスや、セコムトラストネットと契約関係にある本 CA の加入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。また、本 CA が発行する証明書は、法令に即した範囲で使用すること。

4.5.2 利用者の公開鍵及び証明書の使用

利用者は、本 CP/CPS の内容について理解し、承諾した上で、本 CA が発行した加入者の証明書を利用しなければならない。

4.6 証明書の更新

本 CA は、鍵ペアの更新を伴わない証明書更新を認めない。証明書記載事項の変更においても鍵ペアの更新を行う必要がある。証明書を更新する場合は、新たな鍵ペアを生成することとし、本 CP/CPS「4.7 証明書の鍵更新」に定める手続とする。

4.7 鍵更新に伴なう証明書の更新

4.7.1 鍵更新に伴なう証明書の更新が行われる場合

鍵更新に伴なう証明書の更新は、証明書の有効期間が満了する場合又は鍵の危殆化に伴ない証明書の取消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/CPS「4.1.1 証明書申請を提出することができる者」と同様とする。

4.7.3 鍵更新に伴なう証明書更新申請の処理
本 CP/CPS「4.2 証明書申請手続」と同様とする。

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

4.7.5 鍵更新に伴ない発行された証明書の受領確認の行為
本 CP/CPS「4.4.1 証明書の受領確認の行為」と同様とする。

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

4.7.7 利用者に対する証明書発行通知
本 CP/CPS「4.4.3 利用者に対する証明書発行通知」と同様とする。

4.8 証明書の変更

4.8.1 証明書の変更の場合
証明書の記載事項に変更が生じた場合､加入者は本 CA に対し速やかに変更に関する申請を行わなければならない。変更に伴なう証明書の再発行手続は、証明書の取消及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/CPS「4.9.2 証明書取消を申請することができる者」及び「4.1.1 証明書申請を提出することができる者」と同様とする。

4.8.3 変更申請の処理
本 CP/CPS「4.9.3 取消申請手続」及び「4.2 証明書申請手続」と同様とする。

4.8.4 加入者に対する新しい証明書発行通知
本 CP/CPS「4.3.2 加入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の行為
本 CP/CPS「4.4.1 証明書の受領確認の行為」と同様とする。

4.8.6 変更された証明書の公開

本 CP/CPS「4.4.2 証明書の公開」と同様とする。

4.8.7 利用者に対する証明書発行通知

本 CP/CPS「4.4.3 利用者に対する証明書発行通知」と同様とする。

4.9 証明書の取消及び一時停止

4.9.1 証明書取消事由

加入者は、自らの判断に基づいて証明書の取消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、加入者は、本 CA に証明書の取消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
- 秘密鍵が盗難、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
- 秘密鍵が危殆化し機密性が失われた場合又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、証明書の取消ができるものとする。

- 加入者が本 CP/CPS、契約、法律に基づく義務を履行していない場合
- セコムトラストネットが、本サービスを終了する場合
- 本 CA の秘密鍵が危殆化した又はそのおそれがあると判断された場合
- 本 CA が取消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 証明書取消を申請することができる者

証明書の取消申請は、組織又は団体の代表者、社員もしくは組織又は団体の正当な代理人が行うことができる。

4.9.3 取消申請手続

証明書の取消申請手続は、本 CA に対し証明書取消に関する必要な情報を郵送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、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 取消申請の猶予期間

秘密鍵が危殆化した場合を除く取消申請は、取消を希望する 2 営業日前までに、本 CA に行わなければならない。ただし、秘密鍵が危殆化した又はそのおそれがある場合は、当該問題を発見後、速やかに取消申請を行わなければならない。

4.9.5 CA が取消申請を処理しなければならない期間

本 CA は、有効な取消申請を受け付けてから 1 営業日以内に証明書の取消を実行する。

4.9.6 利用者の取消確認要求

利用者は、本 CA により発行された証明書を信頼し、利用する前に、CRL を確認することにより証明書が取消されていないことを確認しなければならない。

4.9.7 証明書取消リストの発行頻度

CRL は、通常 365 日ごとに新たな CRL が発行される。また、証明書の発行及び取消を行った場合にも新たな CRL が発行される。

4.9.8 証明書取消リストの発行最大遅延時間

CRL は、証明書の発行及び取消を行ってから、1 営業日以内に新たな CRL を発行し、リポジトリに公開する。

4.9.9 証明書の一時停止の場合

本 CA は、証明書の一時停止を行わない。

4.10 キーエスクローと鍵回復

本 CA が、CA 秘密鍵を第三者に預託することはない。

5. 物理的、手続き上、人事上のセキュリティ管理

5.1 物理的管理

5.1.1 立地場所及び構造

本サービスの CA システムを設置する施設は、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設置し、且つ建物構造上、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、災害及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

本サービスでは、CA のハードウェア及び CA サービスを提供するソフトウェアへの物理的なアクセスを制限する適切なセキュリティコントロールを装備する。アクセスの制御は電子的なアクセス制御方法、物理的なアクセス制御方法を組み合わせる。ハードウェア及び CA サービスを提供するソフトウェアへの物理的アクセスは常時監視され、また、許可されているアクセスについても運用管理者の承認の下に行われる。

5.1.3 電源管理及び空調管理

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より電源供給を受け保護される。また、機器類に最適な温度、湿度を一定に保つことが可能な設備において保護される。

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、防水対策を施して浸水による被害を最低限に抑える。

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、火災報知器及び消火設備を設置する。

5.1.6 地震対策

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

5.1.7 媒体管理

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

5.1.8 廃棄処理

CA 秘密鍵、機密情報を含む紙面の文書及び磁気媒体等の廃棄の方法は、CA 秘密鍵やバックアップ媒体等は完全な初期化を行うか物理的に破壊を行い、紙面･文書等の紙ベースのものはシュレッダーにかけ廃棄を行う。

5.1.9 オフサイトバックアップ

本サービスに必要なデータ、機器等は、遠隔地に保管するかもしくは調達可能なようにする。

5.2 手続き上の管理

5.2.1 信頼される役割

証明書の登録、発行、取消等の業務及び関連する業務に携わる者は、本 CPS 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。

5.2.2 必要とされる人数

CA システムは、物理的又は論理的に単独でのアクセスが不可能となるよう設計されている。

5.2.3 個々の役割に対する本人性確認と認証

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

5.2.4 職務分割が必要となる役割

本 CA では、権限を特定の個人に集中させず複数人に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、承認行為及び監査に関する権限は分離される。

5.3 人事上のセキュリティ管理

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、適合性及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、経験及び身分証明の要件

本サービスに関して信頼される役割を担う者は、セコムトラストネット株式会社の採用基準に基づき採用された正社員とする。

CA システムを直接操作する担当者は、専門のトレーニングを受け、PKI の概要とシステムの操作方法等を理解しているものを配置する。

5.3.2 背景調査

信頼される役割を担う者の信頼性と適格性を、本 CP/CPS 及びセコムトラストネットの規則の要求に従って、任命時及び定期的に検証する。

5.3.3 トレーニング要求

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

5.4 セキュリティ監査の手順

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、手動或いは自動で取得出来る。

5.4.2 監査ログの処理頻度

本 CA は、監査ログを定期的に精査する。

5.4.3 監査ログの保存期間

監査ログは、最低 10 年保存される。

5.4.4 監査ログの保護

本 CA は、認可された人員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することから保護する。

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、それらの媒体はセキュアな保管場所に保管される。

5.5 記録の保管

5.5.1 アーカイブの種類

本 CA は、以下の情報をアーカイブする。

- 証明書の発行/取消に関する処理履歴
- CRL の発行に関する処理履歴
- 本 CA の証明書
- 加入者の証明書
- CRL

5.5.2 アーカイブの保存期間

アーカイブする情報は、最低 10 年間は保存する。

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セキュリティによって保護され、許可されたものしかアクセスできないよう制限された施設に保存される。

5.5.4 アーカイブのバックアップ手順

証明書発行、取消又は CRL の発行等、本 CA に影響のある重要なデータに変動がある場合は、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 アーカイブの検証

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が確かめられる。

5.6 鍵の切り替え

本 CA の秘密鍵の有効期間は 20 年を想定し､対応する証明書の有効期間は 20 年とする。

本 CA の秘密鍵の有効期間が満了した時点で、新しい秘密鍵が生成され、その後、新しい秘密鍵を使って署名された証明書及び CRL が発行される。

5.7 信頼性喪失や災害からの復旧

5.7.1 事故及び危殆化の対応手続

CA 秘密鍵の危殆化又は危殆化の恐れがある場合及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問題が発生した場合、あらかじめ定められた計画、手順に従い、安全にサービスを再開させる。

5.7.2 コンピューターのハードウェア、ソフトウェア又はデータが破損した場合

本 CA のハードウェア、ソフトウェア又はデータが破損した場合、バックアップ用に保管しているハードウェア、ソフトウェア又はデータを使用して、速やかにシステムの復旧作業を行う。

5.7.3 加入者の秘密鍵が危殆化した場合の手続

加入者は、加入者の秘密鍵が危殆化した又はそのおそれがあると判断した場合、本 CA に対して速やかに証明書の取消申請を行わなければならない。本 CA は、取消申請を受付けた場合、本 CPS「4.9 証明書の取消及び一時停止」に示す手続に従って、証明書の取消を行う。

5.7.4 災害後の事業継続能力

本サービスは、セコムトラストネット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重大な問題や、信頼性を著しく損なわせるような問題が発生した場合でも、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、セコムトラストネットでは、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

セコムトラストネットが本サービスを終了する場合、サービス終了の 3 ヶ月前までに加入者その他の関係者にその旨を通知する。本 CA によって発行された全ての証明書は、終了以前に取消される。

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

本サービスでは CA の署名用鍵ペアを FIPS140-1 レベル 3 の認定を取得したハードウェアセキュリティモジュール（Hardware Security Module、以下、「HSM」という）上で生成する。CA の秘密鍵の生成作業は、運用管理者立会いのもと、複数名の権限者が操作を行うことによって行われる。

6.1.2 加入者への秘密鍵の送付

加入者の鍵ペアは、加入者自身で生成するため、秘密鍵は加入者のみが所持する。

6.1.3 CA への公開鍵送付

加入者の公開鍵は、「3.2.1 秘密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 利用者への CA 公開鍵送付

利用者は、本 CA のリポジトリへアクセスするか、又は一般的に使用されるウェブブラウザを通して本 CA の公開鍵を入手することができる。

6.1.5 鍵長

CA の鍵ペアの電子署名方式は、ハッシュアルゴリズムとして SHA-1 を用いた RSA 方式であって、鍵長は 2048 ビットである。

6.1.6 鍵利用目的

CA 秘密鍵は、原則として、加入者に対して発行する証明書及び CRL への署名に使用する。

6.2 CA 秘密鍵の保護

6.2.1 暗号モジュール

CA 秘密鍵の生成、保管、署名操作は、FIPS140-1 レベル 3 の認定を取得した HSM を用いて行われる。

6.2.2 秘密鍵の複数人コントロール

CA 秘密鍵の生成には、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、破棄等の秘密鍵管理についても同様である。

6.2.3 秘密鍵の外部公開とバックアップ

CA 秘密鍵は、外部の第三者がアクセスすることはない。

6.2.4 秘密鍵のバックアップ

CA 秘密鍵は、CA 室内で FIPS140-1 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 秘密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、そのバックアップの管理についても同様である。

6.2.5 秘密鍵のアーカイブ

CA 秘密鍵は、アーカイブは行わない。

6.2.6 秘密鍵の暗号化モジュールからの移動

CA 秘密鍵は、HSM の内部で生成され、他のハードウェア及びソフトウェア等により秘密鍵を取り出すことはできない。

6.2.7 秘密鍵の暗号化モジュールへの格納

CA 秘密鍵は、FIPS140-1 レベル 3 の認定を取得した暗号モジュールに格納される。

6.2.8 秘密鍵の活性化の方法

CA 秘密鍵の活性化の方法は、CA 室内において本 CPS「6.2.2 秘密鍵の複数人コントロール」と同じく、複数名の権限を有する者を必要とする。

6.2.9 秘密鍵の非活性化の方法

CA 秘密鍵の非活性化の方法は、CA 秘密鍵へのアクセス終了後、自動的に非活性化される。

6.2.10 秘密鍵の破棄方法

CA 秘密鍵を破棄しなければならない状況の場合、CA 室内で本 CPS「6.2.2 秘密鍵の複数人コントロール」と同じく、複数人によって、秘密鍵の格納された HSM を完全に初期化し、又は物理的に破壊する。同時に、バックアップの秘密鍵に関しても同様の手続きによって破棄する。

6.2.11 暗号モジュールの技術管理

CA 鍵ペアの管理に用いる HSM は、FIPS140-1 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 CA 公開鍵のアーカイブ

CA 公開鍵のアーカイブは、「5.5.1 アーカイブの種類」に含まれる。

6.3.2 CA 鍵ペアの有効期間

CA 鍵ペアの有効期間は 20 年を想定している。有効期間の変更はできない。

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 秘密鍵の活性化には、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、個々に保管する。

6.5 コンピュータのセキュリティ管理

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

6.6 セキュリティ技術のライフサイクル管理

本 CA のハードウェア及びソフトウェアは、適切なサイクルで最新のセキュリティテクノロジを導入すべく、随時本 CP/CPS の見直し及びセキュリティチェックを行う。

6.7 ネットワークセキュリティ管理

CA システムは社内及び社外の他のシステムとは接続しない。リポジトリシステムは、ファイアウォール、IDS 等により、様々な脅威から保護される。

7. 証明書及び CRL 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、X509 フォーマット証明書形式により作成される。
次表に示すフィールドを用いる。

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 （加入者名）	加入者情報
SubjectPublicKeyInfo （加入者の公開鍵情報）	加入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、ｘ509 証明書拡張フィールドを使用する。
次表に示すフィールドを用いる。

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 160bits 値
subjectKeyIdenrifier (2.5.29.14)	証明書の公開鍵を SHA-1 によりハッシュした 160bits 値
keyUsage (2.5.29.15)	keyCertSign,cRLSign（加入者公開鍵の使用目的） extendedKeyUsage（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 policyQualifierID=id-qt-cps qualifier=CPS=https://repository.secomtrust.net/SC-Root1/
basicConstraints (2.5.29.19)	Subuject Type=CA,pathLenConstraints=1
cRLDistributionPoints (2.5.29.31)	URI:http://repository.secomtrust.net/SC-Root1/

フィールド	記載事項(説明)
	SCRoot1CRL.crl（ディレクトリ上にあるCRL配布場所）

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、次表のとおりである。

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
RSA Encryption	1 2 840 113549 1 1 1

7.1.4 名前形式

本 CA および加入者は、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。

次表に DN に使用可能な文字を示す。

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、以下のとおりである。

・ 1.2.392.200091.100.901.1

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及び意味

ポリシ修飾子については、本 CP/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。

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。

次表に示すフィールドを用いる。

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）

フィールド	説明
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 （取消リスト）	取消となった証明書の情報 SerialNumber（シリアル番号） RevocationDate（取消日付） 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。

次表に示すフィールドを用いる。

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 160bits 値

8 準拠性監査

8.1 監査の頻度

セコムトラストネットは、本サービスが本 CP/CPS に準拠して運営されているかに関して、年に１回以上の準拠性監査を行う。

8.2 監査人の身分と資格

セコムトラストネットは、CA の準拠性監査について CA 業務に精通しているものを監査人として、本サービスの監査を実施する。

8.3 監査人と被監査対象との関係

監査人は、本サービスの開発、運用、その他いかなる関与もしていないものを選定し、監査の客観性を確保する。

8.4 監査対象

監査は、本 CA の業務内容、運営手続等を本 CP/CPS に基づいて行う。さらに WebTrust for CA の認定基準を満たすことが必要な場合、その基準への準拠性を含めて監査を行う。

8.5 監査指摘事項への対応

監査報告書で指摘された事項に関しては、セコムトラストネットは、速やかに必要な修正作業を行う。

8.6 監査結果の報告

監査報告書は、セコムトラストネットセキュリティポリシ委員会に報告される。監査報告書は、許可されたものだけがアクセスできるよう保管管理する。

9. 他の業務上及び法的問題

9.1 料金

料金体系については、契約書等に別途定める。

9.2 財務的責任

セコムトラストネットは、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する。

9.3 機密保持

9.3.1 機密情報の範囲

CA であるセコムトラストネットが保持する個人および組織の情報は、証明書、CRL、本 CP/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。セコムトラストネットは、法の定めによる場合及び加入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。かかる法的手続き、司法手続き、行政手続きあるいは法律で要求されるその他の手続き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、セコムトラストネットは機密保持対象として扱われる情報を開示することができる。また会社の合併、買収あるいは再編成に関連してアドバイスする弁護士、会計士、金融機関およびその他の専門家に対しても、セコムトラストネットは機密保持対象として扱われる情報を開示することができる。

加入者の秘密鍵は、その加入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及び監査報告書は、機密保持対象情報である。セコムトラストネットは、本 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

証明書及び CRL に含まれている情報は機密保持対象外として扱う。その他、次の状況におかれた情報は機密保持対象外とする。

- セコムトラストネットの過失によらず知られた、あるいは知られるようになった情報
- セコムトラストネット以外の出所から、機密保持の制限無しにセコムトラストネットに知られた、あるいは知られるようになった情報
- セコムトラストネットによって独自に開発された情報
- 開示に関して加入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 であるセコムトラストネットが保持する機密情報を、法の定めによる場合及び加入者

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。にもかかわらず、そのような情報が漏洩した場合、その責は漏洩したものが負う。

9.4 個人情報のプライバシー保護

本 CA が取得する個人情報は、本 CPS「9.3 機密保持」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又は関連する法令及びセコムトラストネット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

セコムトラストネットと加入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及びデータは、次に示す当事者の権利に属するものとする。

- 加入者証明書 ： セコムトラストネットに帰属する財産である
- CRL ： セコムトラストネットに帰属する財産である
- 識別名（DN） ： 加入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
- 加入者の秘密鍵 ： 秘密鍵は、その保存方法又は保存媒体の所有者にかかわらず、公開鍵と対になる秘密鍵を所有する加入者に帰属する財産である
- 加入者の公開鍵 ： 保存方法又は保存媒体の所有者にかかわらず、対になる秘密鍵を所有する加入者に帰属する財産である
- 本 CP/CPS ： セコムトラストネットに帰属する財産（著作権を含む）である

9.6 保証

9.6.1 CA 及び RA の保証

セコムトラストネットは、本 CP/CPS に規定した内容を遵守して電子証明書の審査、登録、発行、取消を含む認証サービスを提供し、CA 秘密鍵の信頼性を含む認証業務の信頼性の確保を保証する。

本 CPS に規定された保証を除き、セコムトラストネットは、明示的あるいは暗示的に、若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 加入者の表明保証

本 CA の加入者は、以下の義務を負う。

- 本 CA に、加入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、その旨を速やかに本 CA に通知する。
- 危殆化から自身の秘密鍵を保護する。
- 証明書の使途は本 CP/CPS に従うものとし、かつ法令に反しないこと。
- 加入者が､証明書に記載の公開鍵に対応する秘密鍵が危殆化した,又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、加入者は本 CA に証明書の取消を速やかに要求すること。

9.6.3 利用者の表明保証

本 CA のサービスの利用者は、以下の義務を負う。

- 本 CA が発行する証明書を信頼し、本 CP/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、リポジトリ内の CRL に含まれる取消情報を取得して、証明書が取消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/CPS に規定されている利用者として責任を負うことに合意すること。

9.7 保証の制限

セコムトラストネットは、本 CPS「9.6.1 CA 及び RA の保証」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、付随的損害又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、データの紛失又はその他の間接的若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 CPS「9.6.1 CA 及び RA の保証」の内容に関し、次の場合、セコムトラストネットは責任を負わないものとする。

- セコムトラストネットに起因しない不法行為、不正使用並びに過失等により発生する一切の損害
- 加入者又は利用者が自己の義務の履行を怠ったために生じた損害
- 加入者又は利用者のシステムに起因して発生した一切の損害
- 加入者又は利用者が使用する端末の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
- 加入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
- セコムトラストネットの責に帰することのできない事由で電子証明書及び CRL に公開された情報に起因する損害
- セコムトラストネット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、加入者及び利用者には、セコムトラストネット及び関連する組織等に対する損害賠償責任及び保護責任が発生する。当該責任の対象となる事象には、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、証明書申請時に加入者が本 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加入者及び利用者のミス、怠慢な行為、各種行為、履行遅滞、不履行等が含まれる。

9.10 改訂

9.10.1 改訂手続

(1) 重要な変更

セコムトラストネットは、本 CP/CPS の内容変更に際して、加入者または利用者に対して、証明書又は CRL を使用するうえで本 CP/CPS の内容の変更が明らかに影響すると判断した場合、本 CP/CPS のメジャーバージョン番号を更新し、本 CP/CPS の変更内容をリポジトリに公開する。公開後は、変更内容の撤回を告知しない限り、14 日を経過した時点で変更内容が有効になるものとする。

(2) 重要でない変更

セコムトラストネットは、本 CP/CPS の内容変更に際して、加入者や利用者が証明書や CRL を使用するうえで本 CP/CPS の内容の変更が全く影響しないか又は無視できると判断した場合、本 CP/CPS のマイナーバージョン番号を更新し、かつ加入者に告知することなしに変更を実施する。

9.10.2 通知方法及び期間

本 CP/CPS の重要な変更については、加入者及び利用者に対して、その内容と変更期日をリポジトリへの公開を以って告知とする。加入者は、告知日から 14 日以内の間、異議を申し立てることができる。告知日から 14 日を経過した時点で異議申し立てがない場合、変更された CP/CPS は加入者及び利用者に同意されたものとみなされる。

9.11 紛争解決手段

本 CA のサービスの利用に関し、セコムトラストネットに対して訴訟、仲裁を含む解決手段に訴えようとする場合、セコムトラストネットに対して事前にその旨を通知するものとする。

9.12 準拠法

本 CA、加入者及び利用者の所在地にかかわらず、本 CP/CPS の解釈、有効性及び本サー

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。仲裁及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。

9.13 雑則

9.13.1 完全合意条項

セコムトラストネットは、本サービスの提供にあたり、自らのポリシ及び保証並びに加入者又は利用者の義務等を本 CP/CPS、契約によって包括的に定め、これ以外の口頭であると書面であるとを問わず、如何なる合意も効力を有しないものとする。

9.13.2 権利譲渡条項

セコムトラストネットが本サービスを第三者に譲渡する場合、本 CP/CPS にて記載された責務及びその他の義務の譲渡を可能とする。

9.13.3 分離条項

本 CP/CPS、加入者利用規定、利用者利用規定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。

10. 用語解説

W

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、及び、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及びその基準に対する認定制度である。

X

X.500
名前及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 の発行者名及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及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～お

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。

か～こ

下位 CA
Root CA 以外の認証局で、Security Communication RootCA1 が署名し発行した証明書に対応する秘密鍵を保有する CA をいう。

鍵ペア
公開鍵暗号方式における秘密鍵と公開鍵から構成される。

加入者
本 CA から証明書の発行を受ける下位の CA のことをいう。

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。秘密鍵に対応する、公開されている鍵。

さ～そ

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。

証明書取消リスト(CRL)
Certificate Revocation List の略。本 CA によって取消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）
Certificate Policy の略。証明書に関するポリシを規定している文書。

セコムトラストネットセキュリティポリシ委員会
本 CP/CPS 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。

た～と

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署名、及び、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事を意味する署名である。

登録機関（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。

な～の

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、取消し、保管、開示を含む本サービスの提供及び利用にあたっての注意点等を規定するもの。

認証機関（CA）
Certification Authority の略。証明書の発行・更新・取消し、CA 等秘密鍵の生成・保護及び加入者の登録を行う機関。

は～ほ

秘密鍵
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、加入者のみが保有する鍵。

ま～も

マイナーバージョン番号
本 CP/CPS の内容変更に際して、変更レベルが加入者や利用者が証明書や 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/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 CP/CPS の内容変更に際して、変更レベルが、明らかに加入者や利用者が証明書や CRL を使用するうえで影響すると判断した場合、本 CP/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。

ら

リポジトリ
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/CPS もリポジトリに格納される。

利用者

認証局から発行された証明書を利用する個人あるいは組織をさす。

ルート CA

本 CP/CPS でいう Security Communication RootCA1 は、セコムトラストネット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。