Security Communication RootCA

認証運用規定

2016年6月1日

Version 5.00

セコムトラストシステムズ株式会社

改版履歴		
版数	日付	内容
V1.00	2003.09.29	初版発行
V2.00	2004.11.08	メジャーバージョンアップ Security Communication RootCA1 証明書ポリシ/認証運用規程を分割し、Security Communication RootCA1 認証運用規程を作成。 全体的に文言の見直しを実施。
V3.00	2006.05.22	会社統合に伴い、会社名“セコムトラストネット”を“セコムトラストシステムズ”に変更 “セコムトラストネットセキュリティポリシ委員会”を“認証サービス改善委員会”に変更
V4.00	2009.05.29	メジャーバージョンアップ Security Communication RootCA1 認証運用規程を Security Communication RootCA 認証運用規程とし、CA の私有鍵 Security Communication RootCA2 を追加する
V4.10	2012.02.15	・5.6 鍵の切り替え －証明書の更新を追記。
V4.20	2012.11.9	OCSP サーバーの運用開始に伴う修正
V5.00	2016.06.01	メジャーバージョンアップ CA の私有鍵 Security Communication RootCA3 を追加 CA の私有鍵 Security Communication ECC RootCA1 を追加

目次

1. はじめに

1.1 概要

Security Communication RootCA 認証運用規定（Certification Practice Statement：以下、「本 CPS」という）は、セコムトラストシステムズ株式会社（以下、「セコム」という）が運用する Security Communication RootCA1、Security Communication RootCA2、Security Communication RootCA3 及び Security Communication ECC RootCA1（以下、「セコムが運用するルート CA」という）が加入者*1 に行う電子証明書（以下、「証明書」という）の発行・取消（以下、「本サービス」という）、セコムが運用するルート CA の鍵管理、証明書を基礎とする公開鍵インフラストラクチャ（PKI : Public Key Infrastructure）の運用維持に関する諸手続等、運用に関するポリシを規定した文書である。

セコムが運用するルート 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。セコムが運用するルート CA の証明書発行における審査、登録及び発行手続は、加入者が使用する証明書に応じた証明書ポリシ（Certificate Policy：以下、「CP」という）によって規定される。利用者*2 はセコムによって発行された証明書を利用する際、本 CPS 及び CP 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、本 CPS の内容が CP の内容に抵触する場合は、CP が優先して適用されるものとする。また、セコムと加入者との間で別途契約書等が存在する場合、本 CPS 及び CP 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 であるセコムが運用するルート CA の私有鍵により署名される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る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。

本 CPS は、認証業務に関する技術面、サービス面の発展や改良に伴い、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。

1.2 文書の名前と識別

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

表 1.2-1 OID（セコム）

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

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

表 1.2-2 OID（本 CPS）

CPS	OID
Security Communication RootCA 認証運用規定	1.2.392.200091.100.901.3

本 CPS は、表「1.2-3 OID（CP)」に示す CP に適用する。

表 1.2-3 OID（CP）

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

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

1.3 PKI の関係者

1.3.1 CA

CA は、証明書の発行、取消、取消情報の開示、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及び保管等の業務を行う。

1.3.2 RA

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

1.3.3 加入者

加入者とは、自ら鍵ペアを生成し、セコムが運用するルート CA から証明書の発行を受ける組織又は団体をいう。セコムが運用するルート 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加入者となる。

1.3.4 利用者

利用者とは、セコムが運用するルート CA が発行した証明書を信頼して利用する者をいう。利用者は、本 CPS 及び CP 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

セコムが運用するルート CA は下位 CA の頂点として機能するルート CA であり、本 CPS「1.2 文書の名前と識別」に記載する CP に基づく証明書を発行する。利用者は、当該証明書の信頼性をセコムが運用するルート CA の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 CPS を管理する組織

本 CPS の維持・管理は、セコムが行う。

1.5.2 連絡先

本 CPS に関する問い合わせ窓口は次のとおりである。

問い合わせ窓口	：	セコムトラストシステムズ株式会社 CA サポートセンター
住所	：	〒150-0001　東京都渋谷区神宮前 1-5-1
電子メールアドレス	：	ca-support@ml.secom-sts.co.jp

1.5.3 CPS のポリシ適合性を決定する者

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

1.5.4 CPS 承認手続

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

2. 公表とリポジトリの責任

2.1 リポジトリ

セコムが運用するルート CA は、加入者及び利用者が 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。また、加入者及び利用者がオンラインでの証明書ステータス情報を 24 時間 365 日利用できるように OCSP サーバーを維持管理する。リポジトリへのアクセスに用いるプロトコルは、HTTP（HyperText Transfar Protocol）、HTTPS（HTTP に SSL によるデータの暗号化機能を付加したプロトコル）とする。リポジトリの情報は一般的な 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

セコムが運用するルート CA は、次の内容をリポジトリに格納し、加入者及び利用者がオンラインによって閲覧できるようにする。

- 本 CPS 及び CP に基づく全ての取消情報を含む証明書取消リスト（以下、「CRL」という）
- セコムが運用するルート CA の自己署名証明書
- 最新の本 CPS 及び CP
- セコムが運用するルート CA が発行する証明書に関するその他関連情報

また、セコムは、OCSP サーバーにより加入者及び利用者がオンラインによって証明書ステータス情報を閲覧できるようにする。

2.3 公開の時期及び頻度

本 CPS 及び CP は、変更の都度、リポジトリに公表される。CRL は、本 CPS 及び CP に従って処理された全ての取消情報を含み、発行の都度、リポジトリに公表される。

2.4 リポジトリへのアクセスコントロール

加入者及び利用者は、随時、リポジトリを参照できる。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
CP に規定する。

3.2 初回の識別と認証
CP に規定する。

3.3 鍵更新申請時の識別と認証
CP に規定する。

3.4 取消申請時の識別と認証
CP に規定する。

4. 証明書のライフサイクルに対する運用要件

4.1 証明書申請
CP に規定する。

4.2 証明書申請手続
CP に規定する。

4.3 証明書発行
CP に規定する。

4.4 証明書の受領確認
CP に規定する。

4.5 鍵ペアと証明書の用途
CP に規定する。

4.6 証明書の更新
CP に規定する。

4.7 鍵更新を伴う証明書の更新
CP に規定する。

4.8 証明書の変更
CP に規定する。

4.9 証明書の取消及び一時停止
CP に規定する。

4.10 証明書のステータス確認サービス
CP に規定する。

4.11 加入（登録）の終了
CP に規定する。

4.12 キーエスクローと鍵回復
CP に規定する。

5. 物理的、手続上、人事上のセキュリティ管理

5.1 物理的管理

5.1.1 立地及び建物構造

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あり、かつ建物構造上、これら災害防止のための対策を講ずる。また、施設内において使用する機器等を、災害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

セコムが運用するルート CA のハードウェア及びソフトウェアには、物理的なアクセス及び電子的なアクセス制御を組み合わせた適切なセキュリティコントロールを装備する。ハードウェア及び CA サービスを提供するソフトウェアへのアクセスは常時監視され、アクセスは、サービス運用管理者の承認を必要とする。

5.1.3 電源管理及び空調管理

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により電源供給を受け保護される。また CA システムは、最適な温度、湿度を一定に保つことが可能な環境下に設置される。

5.1.4 水害対策

CA システムを設置する室は、漏水検知器の設置等、防水対策を講ずる。

5.1.5 火災防止

CA システムを設置する室は、防火壁によって区画された防火区画内とし、火災報知器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、安全な保管場所に保管される。

5.1.8 廃棄処理

CA 私有鍵、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 私有鍵やバックアップ媒体等は完全な初期化を行うか又は物理的に破壊を行い、文書等の紙ベースのものはシュレッダーにかけ廃棄を行う。

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又は調達できる手段を講ずるものとする。

5.2 手続上の管理

5.2.1 信頼される役割

証明書の登録、発行、取消業務に携わる者は、本 CPS 及び CP 上信頼される役割を担っている。セコムが運用するルート 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。セコムが運用するルート CA における役割を表「5.2-1 信頼される役割」に示す。

表 5.2-1 信頼される役割

役割名称	主な職務内容
認証サービス改善委員会	・本 CPS 及び CP の策定、改廃に関する承認 ・監査指摘事項への対応指示
サービス責任者	・セコムが運用するルート CA 運用組織の統括 ・セコムが運用するルート CA のシステム変更、運用手続変更の承認
サービス運用管理者	・運用担当者への作業指示及び作業立会い ・CA システム及び CA 私有鍵に関する作業立会い ・その他サービス運用の全般管理
CA 管理者	・証明書の登録作業、発行作業 ・CRL 発行作業
RA 担当者	・証明書申請に関する受付 ・加入者の審査
ログ検査者	・入退室ログ、システムログ等の検査

5.2.2 必要とされる人数

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

5.2.3 個々の役割に対する識別と認証

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

5.2.4 権限分離が必要となる役割

セコムが運用するルート CA では、権限を特定の個人に集中させず権限を分離することで、権限集中により可能となる単独操作で発生する不正行為等の防止を図る。システム操作、

承認行為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、セコムの採用基準に基づき採用された正社員とする。

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

5.3.2 背景調査

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

5.3.3 トレーニング要求

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

5.4 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

セコムが運用するルート CA では、CA システム、リポジトリシステム、セコムが運用するルート CA に関連するネットワーク・デバイスの監査証跡やイベント・ログを、手動あるいは自動で取得する。

5.4.2 監査ログの処理頻度

セコムが運用するルート CA は、監査ログを定期的に精査する。

5.4.3 監査ログの保存期間

監査ログの保存期間は、最低 10 年とする。

5.4.4 監査ログの保護

セコムが運用するルート CA は､認可された者のみが監査ログにアクセスすることができるよう、適切なアクセスコントロールを採用し、許可されていない者が閲覧できないようにする。

5.4.5 監査ログのバックアップ

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

5.5 記録の保管

5.5.1 アーカイブの種類

セコムが運用するルート CA のアーカイブには、次の情報が含まれる。

- 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
- セコムが運用するルート CA の自己署名証明書
- 加入者の証明書
- CRL
- OCSP サーバーへのアクセスログ

5.5.2 アーカイブの保存期間

アーカイブする情報の保存期間は、最低 10 年間とする。

5.5.3 アーカイブの保護

アーカイブ情報の収められた媒体は物理的に保護され、許可された者しかアクセスできないよう制限された施設において保管される。

アーカイブ情報は、1 年に一度、データの障害や欠損が起きていないことを確認する。

5.5.4 アーカイブのバックアップ手順

証明書発行、取消又は CRL の発行等、セコムが運用するルート CA に影響のある重要なデータに変更がある場合は、都度バックアップを正副取得する。副の媒体については遠隔地に保管する。

5.5.5 アーカイブの検証

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

5.6 鍵の切り替え

セコムが運用するルート CA 自身の鍵ペア更新又は証明書更新は、原則として加入者に発行した証明書の最大有効期間よりも短くなる前に実施する。

セコムが運用するルート CA の有効期間が、加入者に発行する証明書の最大有効期間よりも短くなる場合、加入者に発行する証明書の有効期間は、セコムが運用するルート CA の有効期間内に納まるよう変更する。

なお、セコムが運用するルート CA の私有鍵の有効期間は 20 年を想定している。

5.7 信頼性喪失や災害からの復旧

5.7.1 事故及び危殆化の対応手続

CA 私有鍵が危殆化又は危殆化のおそ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状況が発生した場合には、予め定められた計画、手順に従い、安全にサービスを再開させる。

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

セコムが運用するルート CA は、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 加入者の私有鍵が危殆化した場合の手続

加入者は、加入者の私有鍵が危殆化した又は危殆化のおそれがあると判断した場合、セコムが運用するルート 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。セコムが運用するルート CA は、取消申請を受け付けた場合、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、セコムの事業継続方針に基づき、サービスの中断を余儀なくする状態や、信頼性を著しく損なわせるような事態の際にも、セコムが運用するルート CA に関するサービスを継続するために必要な計画を作成している。サービスの中断を最小限に抑えるため、セコムでは、サービスの復旧に必要なリソースの調達手段を予め計画している。

5.8 認証業務の終了

セコムが本サービスを終了する場合、サービス終了の 3 か月前までに加入者その他の関係者にその旨を通知する。セコムが運用するルート CA によって発行された全ての証明書は、本サービスの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、セコムが運用するルート CA の鍵ペアを FIPS140-1 レベル 3 の認定を取得したハードウェアセキュリティモジュール（Hardware Security Module：以下、「HSM」という）上で生成する。セコムが運用するルート CA の私有鍵の生成作業は、サービス運用管理者立会いのもと、複数名の権限者による操作によって行われる。

6.1.2 加入者への私有鍵の送付

加入者の鍵ペアは、加入者自身で生成するため、私有鍵は加入者のみが所持する。

6.1.3 CA への公開鍵の送付

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

6.1.4 利用者への CA 公開鍵の送付

利用者は、セコムが運用するルート CA のリポジトリにアクセスするか、又は一般的に使用される Web ブラウザを通してセコムが運用するルート CA の公開鍵を入手することができる。

6.1.5 鍵長

CA の鍵ペアの電子署名方式を表「6.1-1 電子署名方式」に示す。

表 6.1-1 電子署名方式

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

6.1.6 鍵利用目的

CA 私有鍵は、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 私有鍵の保護

6.2.1 暗号モジュール

CA 私有鍵の生成、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 私有鍵の複数人コントロール

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

6.2.3 私有鍵の外部公開とバックアップ

CA 私有鍵に、外部の第三者がアクセスすることはない。

6.2.4 私有鍵のバックアップ

CA 私有鍵は、CA 室内で FIPS140-1 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 私有鍵の複数人コントロール」と同じコントロールがなされる。また、そのバックアップについても安全に管理する。

6.2.5 私有鍵のアーカイブ

CA 私有鍵は、アーカイブを行わない。

6.2.6 私有鍵の暗号モジュールからの移動

CA 私有鍵は 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って私有鍵が取り出されることはない。

6.2.7 私有鍵の暗号モジュールへの格納

CA 私有鍵は、FIPS140-1 レベル 3 の認定を取得した HSM に格納される。

6.2.8 私有鍵の活性化の方法

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

6.2.9 私有鍵の非活性化の方法

CA 私有鍵は、CA 私有鍵へのアクセス終了後、自動的に非活性化される。

6.2.10 私有鍵の廃棄方法

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

6.2.11 暗号モジュールの技術管理

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、本 CPS「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。有効期間の変更は行わない。

6.4 活性化データ

6.4.1 活性化データの生成とインストール

CA 私有鍵の活性化には、複数の電子鍵を用いる。

6.4.2 活性化データの保護

活性化に必要な複数の電子鍵は、分散して保管する。

6.5 コンピュータのセキュリティ管理

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

6.6 セキュリティ技術のライフサイクル管理

セコムが運用するルート 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評価し、必要に応じて、本 CPS 及び CP 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、不正侵入検知システム等により、不正アクセスから保護される。

7. 証明書、CRL 及び OCSP のプロファイル

7.1 証明書のプロファイル
CP に規定する。

7.2 CRL のプロファイル
CP に規定する。

7.3 OCSP のプロファイル
CP に規定する。

8 準拠性監査

8.1 監査の頻度

セコムは、本サービスが本 CPS 及び CP に準拠して運用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。この準拠性監査は、認証局のための WebTrust for CA 規準に基づいて行われることもある。

8.2 監査人の身分と資格

セコムが運用するルート 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、セコムとの間に特別な利害関係のない監査人を選定する。

8.4 監査対象

監査は、セコムが運用するルート CA の運用にかかる業務を対象として行う。

8.5 監査指摘事項への対応

セコムは、監査報告書で指摘された事項に関し、速やかに必要な是正措置を行う。

8.6 監査結果の報告

監査報告書は、認証サービス改善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される。

なお、WebTrust for CA の検証に関する報告書は、WebTrust for CA 認定の規則に従い、特定のサイトにて参照可能となる。

9. 他の業務上及び法的問題

9.1 料金
CP に規定する。

9.2 財務的責任
CP に規定する。

9.3 機密保持
CP に規定する。

9.4 個人情報の保護
CP に規定する。

9.5 知的財産権
CP に規定する。

9.6 表明保証
CP に規定する。

9.7 保証の制限
CP に規定する。

9.8 責任の制限
CP に規定する。

9.9 補償
CP に規定する。

9.10 改訂

9.10.1 改訂手続

(1) 重要な変更

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

(2) 重要でない変更

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

9.10.2 通知方法及び期間

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

9.11 紛争解決手段

CP に規定する。

9.12 準拠法

CP に規定する。

9.13 雑則

CP に規定する。

10. 用語解説

O

OCSP

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

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 が定めた証明書及び CRL のフォーマット。X.509 v3(Version 3)では、任意の情報を保有するための拡張領域が追加された。

あ～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、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
セコムが運用するルート 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。

加入者
セコムが運用するルート CA から証明書の発行を受ける組織又は団体のことをいう。

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。私有鍵に対応する、公開されている鍵。

さ～そ

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、加入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。

証明書取消リスト(CRL)
Certificate Revocation List の略。セコムが運用するルート 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。証明書を発行する際の元となるデータファイル。CSR には証明書の発行要求者の公開鍵が含まれており、その公開鍵に発行者の署名を付与して証明書を発行する。

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

た～と

タイムスタンプ

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

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

電子署名

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

な～の

認証運用規定（CPS）

Certification Practice Statement の略。証明書の申請、申請の審査、証明書発行、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。

認証局（CA）

Certification Authority の略。証明書の発行・更新・取消し、CA 等私有鍵の生成・保護及び加入者の登録を行う機関。

ま～も

マイナーバージョン番号

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

メジャーバージョン番号

本 CPS の内容変更に際して、変更レベルが、明らかに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 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。ユーザ又はアプリケーションがネットワークのどこからでも証明書にアクセスできるようにするための仕組みである。CRL や本 CPS もリポジトリに格納される。

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 CPS でいう Security Communication RootCA は、セコムが所有し運営する機関で、下位 CA の証明書を発行するルート CA である。下位 CA の頂点として機能する CA である。