セコムパスポート for Member 2.0 PUB
証明書ポリシー
（Certificate Policy）

Version 5.06

2021 年 06 月 15 日

セコムトラストシステムズ株式会社

改版履歴		
版数	日付	内容
1.00	2008.04.28	新規作成
1.10	2009.03.19	証明書プロファイル（extendedKeyUsage）の修正
2.00	2009.10.13	ポリシーOID の追加 全体的に体裁の修正を実施
3.00	2013.11.27	Sha256 の追加に伴い、修正 ポリシーOID の追加 RootCA のリポジトリー情報を追加
4.00	2014.05.29	サーバー認証の利用用途追加に伴い、修正 ポリシーOID の追加
5.00	2017.01.20	ポリシーOID の追加 OCSP サーバーの運用開始に伴う修正 全体的に体裁の修正を実施
5.01	2020.02.19	サーバー証明書用証明書ポリシーの削除 BR for Code Signing における内容の追加・修正 全体的な文言および体裁の見直し
5.02	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
5.03	2020.06.15	CA 証明書(sha256)のプロファイルに Extended Key Usage 追加 証明書利用者証明書(sha256)のプロファイルの Extended Key Usage 追加
5.04	2020.07.30	CA 証明書(sha256)の Extended Key Usage から OCSP Signing を削除、OU 変更、CP の URL 変更 証明書利用者証明書(sha256)の OU 変更、CP の URL 変更、AIA の OCSP URL 変更等
5.05	2020.09.29	CRL プロファイルの Reason code を修正
5.06	2021.06.15	電子メールアカウントの認証を追加

目次

1. はじめに

1.1 概要

セコムパスポート for Member 2.0 PUB 証明書ポリシー（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）が運用するセコムパスポート for Member 2.0 PUB 認証局（以下「本 CA」という）が発行する証明書の利用目的、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。本 CA の運用維持に関する諸手続については、セコム電子認証基盤認証運用規程（以下「CPS」という）に規定する。
本 CA は、Security Communication RootCA1 または Security Communication RootCA2 により、片方向相互認証証明書の発行を受けており、各 CA が定める運用基準に従い運用されている。上記 CA の CP および CPS は以下のリポジトリーに公開している。

１．Security Communication RootCA1
https://repository.secomtrust.net/SC-Root1/index.html

２．Security Communication RootCA2
https://repository.secomtrust.net/SC-Root2/index.html

本 CA から証明書の発行を受ける者は、証明書の発行を受ける前に自己の利用目的と本 CP、および CPS とを照らし合わせて評価し、本 CP、および CPS を承諾する必要がある。
なお、本 CP の内容が CPS の内容に抵触する場合は、本 CP、CPS の順に優先して適用されるものとする。また、セコムと契約関係を持つ組織団体等との間で、別途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。

本 CP は、本 CA に関する技術面、運用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。

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。また本 CA は、コードサイニング用証明書ポリシーに適用する証明書を発行する場合は、https://www.cabforum.org/で公開される CA/ Browser Forum の Baseline Requirements for the Issuance and Management of Code Signing Certificates（以下「BR for Code Signing」という）および Baseline Requirements for the Issuance and Management of Publicly -Trusted Certificates に準拠する。

1.2 文書名と識別

本 CP の正式名称は、「セコムパスポート for Member 2.0 PUB 証明書ポリシー」という。本 CP には、発行する証明書の用途ごとに、登録された一意のオブジェクト識別子(以下「OID」という)が割り当てられている。本 CP に適用する OID および参照する CPS の OID は、次のとおりである。

CP/CPS	OID
クライアント用証明書ポリシー (署名アルゴリズム：Sha1)	1.2.392.200091.100.381.1
クライアント用証明書ポリシー (署名アルゴリズム：Sha256)	1.2.392.200091.100.381.4
データ署名用証明書ポリシー (署名アルゴリズム：Sha1)	1.2.392.200091.100.381.2
データ署名用証明書ポリシー (署名アルゴリズム：Sha256)	1.2.392.200091.100.381.5
コードサイニング用証明書ポリシー (署名アルゴリズム：Sha256)	1.2.392.200091.100.381.8
OCSP サーバー用証明書ポリシー (署名アルゴリズム：Sha256)	1.2.392.200091.100.381.9
セコム電子認証基盤認証運用規程	1.2.392.200091.100.401.1

1.3 PKI の関係者

1.3.1 認証局

CA (Certification Authority：認証局) は、本 CA の私有鍵の管理、証明書の発行、失効、CRL(Certificate Revocation List:証明書失効リスト)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、およびリポジトリーの維持管理等を行う。電子認証基盤の上で運用される CA の運営主体はセコムである。

1.3.2 RA

RA は、LRA (Local Registration Authority) および証明書利用者の審査ならびに証明書の発行および失効を行うための登録業務等を行う主体である。電子認証基盤の上で運用される CA において、RA の運用はセコムが行う。

LRA は、RA に代わり、証明書利用者の実在性確認および本人性確認の審査ならびに証明書の発行および失効を行うための登録業務等を行う主体であり、RA が事前に審査し、RA が実在性を確認した特別な組織または団体がその役割を担うことができる。

またLRAは、RAと同様に本CPに定める事項に従うものとする。なおクライアント用証明書ポリシーまたはデータ署名用証明書ポリシーが適用される場合にのみ、LRAが業務を行う場合がある。

1.3.3 申請者および証明書利用者

申請者とは、RAまたはLRAに対し、証明書の発行や失効に関する申込を行う個人、組織または団体等をいい、また証明書利用者とは、本CAから発行された証明書を受領し、当該証明書を利用する個人、組織または団体等をいう。

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個人、組織または団体等をいう。

1.3.5 その他関係者

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 証明書の用途

1.4.1 適切な証明書の用途

本CAが本CPに基づき発行する証明書は、次の目的として利用することができる。

証明書ポリシー	証明書の用途
クライアント用証明書ポリシー	・電子文書への電子署名および電子文書の暗号化 ・個人、機器等を特定するためのクライアント認証 ・電子メールへの電子署名および電子メールの暗号化（S/MIME証明書）
データ署名用証明書ポリシー	・電子文書への電子署名
コードサイニング用証明書ポリシー	・プログラムファイルへの電子署名 （コードサイニング証明書）
OCSPサーバー用証明書ポリシー	・OCSPレスポンスへの電子署名

1.4.2 禁止される証明書の用途

本CAが本CPに基づき発行する証明書は、「1.4.1 適切な証明書の用途」に記載する目的以外で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 に関する連絡先は次のとおりである。
窓口 ： セコムトラストシステムズ株式会社
電子メールアドレス ：ca-support@secom.co.jp

1.5.3 ポリシー適合性を決定する者
本 CP の内容については、認証サービス改善委員会が適合性を決定する。

1.5.4 承認手続
本 CP は、セコムが作成・改訂を行い、認証サービス改善委員会の承認により発効される。

1.6 定義と略語
あ～ん

アーカイブ
法的またはその他の事由により、履歴の保存を目的に取得する情報のことをいう。

エスクロー
第三者に預けること（寄託）をいう。

鍵ペア
公開鍵暗号方式において、私有鍵と公開鍵から構成される鍵の対のことをいう。

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をいい、私有鍵に対応し、通信相手の相手方に公開される鍵のことをいう。

コードサイニング
作成したプログラムファイル等（以下「コード」という）に対し、その作成者や発行者を

示すための電子署名データを埋め込むことをいう。
コードの利用者は、この電子署名を検証することにより、コードの作成者、発行者、有効期限等の情報を得ることができ、また、コードが第三者によって改ざんされていないかどうかを確認することができる。

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をいい、公開鍵に対応する本人のみが保有する鍵のことをいう。

タイムスタンプ
電子ファイルの作成日時やシステムが処理を実行した日時等を記録したデータのことをいう。

電子証明書
ある公開鍵を、記載された者が保有することを証明する電子データのことをいう。CA が電子署名を施すことで、その正当性が保証される。

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。

リポジトリー
CA 証明書および CRL 等を格納し公表するデータベースのことをいう。

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 (Certification Authority)：認証局
証明書の発行・更新・失効、CA 私有鍵の生成・保護、リポジトリーの維持・管理、および証明書利用者の登録等を行う主体のことをいう。

CA/Browser Forum
認証局とインターネット・ブラウザベンダーによって組織され、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。

CP（Certificate Policy）
CA が発行する証明書の種類、用途、申込手続等、証明書に関する事項を規定する文書のことをいう。

CPS（Certification Practices Statement）：認証運用規定
CA を運用する上での諸手続、セキュリティ基準等、CA の運用を規定する文書のことをいう。

CRL（Certificate Revocation List）：証明書失効リスト
証明書の有効期間中に、証明書記載内容の変更、私有鍵の紛失等の事由により失効された証明書情報が記載されたリストのことをいう。

FIPS140-2
米国 NIST（National Institute of Standards and Technology）が策定した暗号モジュールに関するセキュリティ認定基準のこという。最低レベル 1 から最高レベル 4 まで定義されている。

HSM（Hardware Security Module）
私有鍵の生成、保管、利用などにおいて、セキュリティを確保する目的で使用する耐タンパー機能を備えた暗号装置のことをいう。

LRA 運用基準
LRA が LRA 業務を行うにあたり、組織、業務、設備、審査に関して遵守すべき基準を記載した文書のことをいう。

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。

OID（Object Identifier）：オブジェクト識別子
ネットワークの相互接続性やサービス等の一意性を維持管理するための枠組みであり、国際的な登録機関に登録された、世界中のネットワーク間で一意となる数字のことをいう。

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。

RA（登録局）(Registration Authority)：登録機関
CA の業務のうち、申込情報の審査、証明書発行に必要な情報の登録、CA に対する証明書発行要求等を行う主体のことをいう。

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。

WebTrustPrinciples and Criteria for Certification Authority（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。

WebTrust for Certification Authorities - Publicly Trusted Code Signing Certificates（WebTrust for CA Code Signing）
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、認証局がコードサイニング証明書を発行するにあたっての審査、証明書に関する規定について策定された監査基準である。

X.500
ネットワーク上での分散ディレクトリサービスに関する、コンピュータネットワーク標準規格のシリーズのことをいう。

2. 公開とリポジトリーの責任

2.1 リポジトリー

セコム は、証明書利用者および検証者が、24時間365日CRL、本CPおよびCPS等を参照できるようリポジトリーを維持管理する。また、証明書利用者および検証者がオンラインでの証明書ステータス情報を24 時間365 日利用できるようにOCSP サーバーを維持管理する。ただし、保守等により、一時的にリポジトリーおよびOCSP サーバーを利用できない場合もある。

2.2 証明情報の公開

セコム は、次の内容をリポジトリーに格納し、証明書利用者がオンラインによって参照できるようにする。

- CRL
- 本 CA の中間証明書
- 最新の本 CP および CPS
- 本 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 サーバーにより証明書利用者および検証者がオンラインによって証明書ステータス情報を閲覧できるようにする。

2.3 公開の時期または頻度

本 CP および CPS は、変更の都度、リポジトリーに公表される。CRL は、本 CP に従って処理された失効情報を含み、発行の都度、リポジトリーに公表される。また、証明書の有効期限を過ぎたものは CRL から削除される。

2.4 リポジトリーへのアクセス管理

証明書利用者および検証者は、随時、リポジトリーを参照できる。リポジトリーへのアクセスに用いるプロトコルは、HTTP（Hyper Text Transfer Protocol）、HTTPS（HTTP に SSL/TLS によるデータの暗号化機能を付加したプロトコル）、LDAP（Lightweight Directory Access Protocol）とする。リポジトリーの情報は一般的な Web インターフェースを通じてアクセス可能である。

3. 識別と認証

3.1 名前決定

3.1.1 名前の種類

証明書に記載される証明書発行者である本CAの名前と発行対象である証明書利用者の名前は、X.500の識別名（DN：Distinguished Name） 形式に従い設定する。

3.1.2 名前が意味を持つことの必要性

本CA が発行する証明書に用いられるDNは、証明書利用者を識別するために使用し、有意義なものとする。

3.1.3 証明書利用者の匿名性または仮名性

本CAが発行する証明書の組織名およびコモンネームには、匿名や仮名での登録は行わない。なお、BR for Code Signingで定められていない各証明書ポリシーにおいては、証明書を管理するための数字や文字列などを登録する場合もある。

3.1.4 様々な名前形式を解釈するための規則

様々な名前の形式を解釈する規則は、X.500シリーズの識別名規定に従う。

3.1.5 名前の一意性

本CAが発行する証明書は、証明書利用者に対し一意となるDNを割り当てる。
主体者名（CN：Common Name）が重複する場合は、Organization、Organizational UnitまたはSerial Number属性等を用いてDNの一意性を確保する。

3.1.6 認識、認証および商標の役割

セコムは、必要に応じて証明書申請に記載される名称について知的財産権を有しているかどうかの確認を行う。証明書利用者は、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。セコムは、登録商標等を理由に証明書利用者と第三者間で紛争が起こった場合、仲裁や紛争解決は行わない。また、セコムは紛争を理由に発行された証明書を失効する権利を有する。

3.2 初回の本人確認

3.2.1 私有鍵の所持を証明する方法

セコムは、証明書の申請手続において、証明書発行要求の署名の検証を行い、証明書発行

要求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。または、本 CA 内において私有鍵を生成し、その私有鍵を証明書利用者に対し安全に配布することで、当該証明書利用者が該当する証明書に対応する私有鍵を所持するということを証明する。

3.2.2 組織の認証

セコムは、セコムが信頼する第三者による調査またはそのデータベース、国や地方公共団体が発行する公的書類もしくはその他これらと同等の信頼に値すると認証サービス改善委員会が判断した方法によって LRA または組織、団体等を認証する。
国や地方公共団体が発行する公的書類により認証する場合は、印鑑証明書(発行日より 3 か月以内のもの)またはこれに相当する書類の提出を求める。

LRA または組織、団体等の審査時における、セコムへの提出書類は次のとおりである。

- LRA または組織、団体等の情報を届出る書類
- その他、審査時にセコムが必要とする書類

審査の結果、セコムが不適合と判断とした場合、提出された公的書類は返却もしくは破棄する。申込書等を受領していた場合、セコムはこれを破棄する。

3.2.3 申請者および証明書利用者の認証

セコムは、国や地方公共団体が発行する公的書類、セコムが信頼する第三者による調査またはそのデータベース、その他これらと同等の信頼に値すると認証サービス改善委員会が判断した方法によって行う。
クライアント用証明書ポリシーおよびデータ署名用証明書ポリシーの証明書の発行に際して、申請者および証明書利用者の審査は、別途セコムが定める約款等や、LRA 運用基準に基づき LRA によって決定された方法により行われる場合がある。

3.2.4 検証されない証明書利用者の情報

セコムは、識別名に含まれる証明書利用者の商号や名称、所在地など証明書の発行に必要な情報を「3.2.2 組織の認証」および「3.2.3 申請者および証明書利用者の認証」で検証する。なお、サービスの提供上、請求先情報などの事務手続きに必要な情報の提供を求めることがある。

3.2.5 権限の正当性確認

申請者の権限の正当性確認は、「3.2.2 組織の認証」または「3.2.3 申請者および証明書利用者の認証」において決定された方法により行われる。

3.2.6 相互運用の基準

本CAは、Security Communication RootCA1、またはSecurity Communication RootCA2より、片方向相互認証証明書を発行されている。

3.2.7 電子メールアカウントの認証

本CAは、S/MIME証明書を発行する際、以下に記載する方法を使用して、証明書に登録される電子メールアドレスに関連付けられた電子メールアカウントを制御しているか、または電子メールアカウントの所有者から、アカウント所有者の代理として申請することを承認されているかを認証する。なお、本項で記載するランダム値は、本CAが生成する112ビット以上の乱数から成るものとし、その生成より30日間のレスポンス確認の使用に有効なものとする。

1. **本CAは、電子メールアドレスに含まれる@以下のドメインにおいて、WHOIS レジストリサービスに登録された登録担当者（Registrant）情報を参照し、申請者がドメインを所有していること**（申請者とドメイン所有者が同一組織であること）**を確認する。なお、ドメインを第三者組織が所有していることを確認した場合、ドメインの所有者より、所有者組織の押印をした「ドメイン名使用承諾書」を本CAに提出することで、電子メールアカウントの利用が承認されていることを確認する。**

2. WHOIS レジストリサービスに登録されたドメイン連絡先へ電子メールにてランダム値を送信し、ランダム値が含まれた確認応答を受け取ることによって、電子メールアカウントの所有者からアカウントの利用が承認されていることを確認する。

3. ローカル部は'admin'、'administrator'、'webmaster'、'hostmaster'、または'postmaster'とし、電子メールアドレスに含まれる@以下のドメインで作成した電子メールアドレスにランダム値を送信して、ランダム値が含まれた確認応答を受け取ることによって、電子メールアカウントの所有者からアカウントの利用が承認されていることを確認する。

4. 要求トークンまたはランダム値がファイルの内容に含まれていることを検証することにより、電子メールアカウントの制御を確認する。本CAは承認済みポートを介してアクセスし、「http（またはhttps）:// ［電子メールアドレスに含まれる@以下のドメイン］/.well-known/pki-validation」ディレクトリの配下にランダム値が配置されていること、リクエストから正常なHTTPまたはHTTPS応答を受信することを確認する。

5. 電子メールアドレスに含まれる@以下のドメイン（先頭にアンダースコア文字で始まるラベルを接頭語に持つものも含まれる）のいずれかの、DNS CNAME、TXT または CAA レコード内のどちらかに、ランダム値か申請トークンがあることを確認することで、電子メールアカウントの制御を確認する。

3.3 鍵更新申請時の本人性確認と認証

3.3.1 通常の鍵更新時における本人性確認と認証
「3.2.3 申請者および証明書利用者の認証」および「3.2.5 権限の正当性確認」と同様とする。

3.3.2 証明書失効後の鍵更新時における本人性確認と認証
「3.2.3 申請者および証明書利用者の認証」および「3.2.5 権限の正当性確認」と同様とする。

3.4 失効申請時の本人性確認と認証
「3.2.3 申請者および証明書利用者の認証」および「3.2.5 権限の正当性確認」と同様とする。

4. 証明書のライフサイクルに対する運用上の要件

4.1 証明書申請

4.1.1 証明書の申請を行うことができる者

本 CA に対する申請は、「3.2.2 組織の認証」に基づきセコムより認証された LRA または組織、団体等が行うことができる。
LRA に対する申請は、LRA 運用基準に基づき、LRA によって定められた者が行うことができる。

4.1.2 申請手続および責任

証明書の発行申請を行うにあたり、本 CP および CPS の内容を承諾したうえで申請を行うものとする。また、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 本人性確認と認証の実施

セコムは、「3.2 初回の本人確認」に基づき LRA または組織、団体等の本人性確認と認証を行う。また、LRA から受け付ける証明書の申請にあたっては、LRA より提示される証明書を検証することにより、LRA の本人性確認と認証を行う。
LRA は、LRA 運用基準に基づき、LRA によって決定された方法により本人性確認と認証を行う。

4.2.2 証明書申請の承認または却下

本 CA または LRA は、審査の結果、承認を行った申請について証明書を発行する。
また、すべての項目の審査が正常に完了しない証明書の申請は却下できるものとし、以下理由を含むものは却下とする。

- 以前に拒否された、または以前に契約の条項に違反していた申請者または証明書利用者の証明書
- フィッシングやマルウェア、その他の詐欺的使用の疑いがある、あるいは懸念される場合

4.2.3 証明書申請の処理時間

本 CA は、証明書申請を受け付けた後、すみやかに LRA、証明書利用者または申請者が証明書を取得可能な状態とする。

4.3 証明書の発行

4.3.1 証明書発行時の処理手続

本 CA は、申請情報に基づき、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 証明書利用者への証明書発行通知

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、発行した証明書をオンラインまたはオフラインで LRA、証明書利用者または申請者に配付する。証明書利用者の私有鍵を本 CA が生成する場合は、郵送、電子メール、手交等の方法により、私有鍵と PIN を別送する。証明書発行の通知は、証明書を配付することによって行う。

4.4 証明書の受領確認

4.4.1 証明書の受領確認手続

本 CA は、LRA または証明書利用者からの受領の報告を受けた場合、もしくは本 CA による証明書の配布日より 14 日以内に異議申し立てがなかった場合に、LRA または証明書利用者が証明書を受領したものとみなす。

4.4.2 認証局による証明書の公開

本 CA は、証明書利用者の証明書の公開は行わない。

4.4.3 他のエンティティに対する認証局の証明書発行通知

本 CA は、証明書申請時に登録された者以外への証明書発行通知は行わない。

4.5 鍵ペアおよび証明書の利用

4.5.1 証明書利用者の私有鍵および証明書の利用

証明書利用者の私有鍵および証明書の利用については、「1.4.1 適切な証明書の用途」および約款等に従う。また証明書利用者は、「1.4.1 適切な証明書の用途」および約款等に記載された用途に対して、当該証明書および対応する私有鍵を利用するものとする。

4.5.2 検証者の利用者の公開鍵および証明書の利用

検証者は、証明書利用者の公開鍵および証明書を使用し、本 CA が発行した証明書の信頼性を検証することができる。本 CA が発行した証明書の信頼性を検証し、信頼する前に、本 CP および CPS の内容について理解し、承諾しなければならない。

4.6 証明書の更新

本 CA は、証明書利用者が証明書を更新する場合、新たな鍵ペアを生成すること推奨する。

4.6.1 証明書の更新事由

規定しない。

4.6.2 証明書の更新申請を行うことができる者

規定しない。

4.6.3 証明書の更新申請の処理手続

規定しない。

4.6.4 証明書利用者に対する新しい証明書発行通知

規定しない。

4.6.5 更新された証明書の受領確認手続

規定しない。

4.6.6 認証局による更新された証明書の公開

規定しない。

4.6.7 他のエンティティに対する認証局の証明書発行通知

規定しない。

4.7 鍵更新をともなう証明書の更新

4.7.1 更新事由

鍵更新をともなう証明書の更新は、証明書の有効期限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 新しい証明書の申請を行うことができる者

「4.1.1 証明書の申請を行うことができる者」と同様とする。

4.7.3 更新申請の処理手続

「4.3.1 証明書発行時の処理手続」と同様とする。

4.7.4 証明書利用者に対する新しい証明書の通知
「4.3.2 証明書利用者への証明書発行通知」と同様とする。

4.7.5 鍵更新された証明書の受領確認手続
「4.4.1 証明書の受領確認手続」と同様とする。

4.7.6 認証局による鍵更新済みの証明書の公開
「4.4.2 認証局による証明書の公開」と同様とする。

4.7.7 他のエンティティに対する認証局の証明書発行通知
「4.4.3 他のエンティティに対する認証局の証明書発行通知」と同様とする。

4.8 証明書の変更
証明書の記載事項に変更が生じた場合、証明書利用者は、すみやかに変更に関する申請を行わなければならない。変更にともなう手続は、初回発行時の手続と同様とする。また、証明書変更後は、すみやかに変更前の証明書の失効手続を行うこととする。

4.8.1 証明書の変更事由
規定しない。

4.8.2 証明書の変更申請を行うことができる者
「4.1.1 証明書の申請を行うことができる者」と同様とする。

4.8.3 変更申請の処理手続
「4.3.1 証明書発行時の処理手続」と同様とする。変更前の証明書の失効は、「4.9.3 失効申請手続」と同様とする。

4.8.4 証明書利用者に対する新しい証明書発行通知
「4.3.2 証明書利用者への証明書発行通知」と同様とする。

4.8.5 変更された証明書の受領確認手続
「4.4.1 証明書の受領確認手続」と同様とする。

4.8.6 認証局による変更された証明書の公開
「4.4.2 認証局による証明書の公開」と同様とする。

4.8.7 他のエンティティに対する認証局の証明書発行通知
規定しない。

4.9 証明書の失効と一時停止

4.9.1 証明書失効事由
証明書利用者は、次の事由が発生した場合、すみやか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
- 私有鍵の盗難、紛失、漏洩、不正利用等により私有鍵が危殆化したまたは危殆化のおそれがある場合
- 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、セコムは、次の事由が発生した場合に、セコムの判断により証明書利用者の証明書を失効することができる。

- 証明書利用者が本 CP、CPS、関連する契約または法律に基づく義務を履行していない場合
- 契約違反その他の事由によりセコムから証明書の発行拒否または失効を受けたことがあると判明した場合
- 証明書利用者および本 CA の私有鍵が危殆化したまたは危殆化のおそれがあると判断した場合
- 証明書が BR for Code Signing、本 CP または CPS に準拠して発行されていないことを認識した場合
- 本 CP に記載する適切な用途以外の用途で証明書が使用された、またはセコムとの契約等で示された目的以外の目的で証明書が使用された、あるいは証明書が他の方法で悪用されていることを認識した場合
- 証明書に含まれるドメイン、あるいは電子メールアドレスを使用する権利が失われたことを示す状況を認識した場合
- 証明書に含まれる情報の変更を認識した場合
- 証明書利用者の証明書へ不正アクセスされたことを認識した場合
- 証明書を用いて疑わしいコードへ署名されたことを認識した場合
- セコム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 証明書の失効申請を行うことができる者

「4.1.1 証明書の申請を行うことができる者」と同様とする。

4.9.3 失効申請手続

証明書利用者は、所定の手続きに基づき、本 CA に対し利用者証明書の失効申請を行う。LRA によって申請され発行された証明書については、LRA 運用基準に基づき、LRA によって決定された方法により利用者証明書の失効申請を行う。

LRA は、LRA の証明書を用いて、セコムが提供するサイトにアクセスし、本 CA に対して利用者証明書の失効申請を行う。

4.9.4 失効申請の猶予期間

証明書利用者は、証明書失効事由が発生してからすみやかに失効申請を行わなければならない。

LRA は、証明書利用者から申請を受け付けてからすみやかに本 CA に対して失効申請を行わなければならない。

4.9.5 認証局が失効申請を処理しなければならない期間

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処理を行い、CRL へ当該証明書情報を反映させる。

4.9.6 失効確認の要求

本 CA が発行する証明書には、CRL の格納先である URL を記載する。また、コードサイニング用証明書ポリシーで発行する証明書については、OCSP サーバーの URL についても記載をする。検証者は、証明書利用者の証明書について、有効性を確認しなければならない。証明書の有効性は、リポジトリーに掲載している CRL または OCSP サーバーにより確認する。

4.9.7 証明書失効リストの発行頻度

本 CA は、失効処理の有無にかかわらず、24 時間以内に CRL を発行する。証明書の失効処理が行われた場合は、即時に CRL を発行し、リポジトリーに反映させる。

4.9.8 証明書失効リストの発行最大遅延時間

本 CA は、証明書の失効を行ってから、即時に CRL を発行し、リポジトリーに公表する。

4.9.9 オンラインでの失効/ステータス確認の適用性

コードサイニング用証明書ポリシーで発行する証明書について、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。コードサイニング用証明書ポリシ

ー以外のポリシーについては、必要に応じて提供される。

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、利用者の証明書について、有効性を確認しなければならない。コードサイニング用証明書ポリシーで発行した証明書を検証する際、リポジトリーに掲載している CRL を用いて、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
本 CA は、RFC4366 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 は証明書利用者が 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、証明書利用者に対してこの要件を実施する場合は、サービス利用規定または証明書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
「4.9.1.証明書失効事由」に記載する。

4.9.13 証明書の一時停止事由
証明書の一時停止は、証明書利用者の判断により行うことができる。証明書の一時停止は、証明書利用者自身の責任のもと、行うものとする。なお、証明書の一時停止を行った場合、当該証明書の失効申請を行わなければならない。

4.9.14 証明書の一時停止申請を行うことができる者
証明書の一時停止は、証明書利用者によって行われるものとする。

4.9.15 証明書の一時停止申請手続
本 CA から事前に通知される Web サイトにアクセスし、別途通知されるログイン用のパスワードを使用して、一時停止申請を行う。

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

CRL または OCSP サーバーの失効情報は、失効した証明書に記載されている有効期限までは確認できるものとする。なお、コードサイニング用証明書ポリシーで発行した証明書については、有効期限後も最低 10 年間は失効情報を確認できるものとする。

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 CRL および 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 登録の終了

LRA または証明書利用者は本サービスの利用を終了する場合、発行した証明書の失効申請を行わなければならない。

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、証明書利用者の私有鍵のエスクローは行わない。

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。

5. 設備上、運営上、運用上の管理

5.1 物理的管理

5.1.1 立地場所および構造

本項については、CPS に規定する。

5.1.2 物理的アクセス

本項については、CPS に規定する。

5.1.3 電源および空調

本項については、CPS に規定する。

5.1.4 水害対策

本項については、CPS に規定する。

5.1.5 火災対策

本項については、CPS に規定する。

5.1.6 媒体保管

本項については、CPS に規定する。

5.1.7 廃棄処理

本項については、CPS に規定する。

5.1.8 オフサイトバックアップ

本項については、CPS に規定する。

5.2 手続的管理

5.2.1 信頼すべき役割

本項については、CPS に規定する。

5.2.2 職務ごとに必要とされる人数

本項については、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
本項については、CPS に規定する。

5.2.4 職務分割が必要となる役割
本項については、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
本項については、CPS に規定する。

5.3.2 背景調査
本項については、CPS に規定する。

5.3.3 教育要件
本項については、CPS に規定する。

5.3.4 再教育の頻度および要件
本項については、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
本項については、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
本項については、CPS に規定する。

5.3.7 独立した契約者の要件
本項については、CPS に規定する。

5.3.8 要員へ提供される資料
本項については、CPS に規定する。

5.4 監査ログの手続

5.4.1 記録されるイベントの種類
本項については、CPS に規定する。

5.4.2 監査ログを処理する頻度
本項については、CPS に規定する。

5.4.3 監査ログを保持する期間
本項については、CPS に規定する。

5.4.4 監査ログの保護
本項については、CPS に規定する。

5.4.5 監査ログのバックアップ手続
本項については、CPS に規定する。

5.4.6 監査ログの収集システム
本項については、CPS に規定する。

5.4.7 イベントを起こした者への通知
本項については、CPS に規定する。

5.4.8 脆弱性評価
本項については、CPS に規定する。

5.5 記録の保管

5.5.1 アーカイブの種類
セコムは、CPS「5.4.1.記録されるイベントの種類」のセコムパスポート for Member 2.0 PUB に関連するシステムに係るログに加えて、次の情報をアーカイブとして保存する。

- 本 CP
- 認証業務を他に委託する場合においては、委託契約に関する書類
- 監査の実施結果に関する記録および監査報告書
- LRA または組織、団体等からの申請書類および申請に関するデータ
- OCSP サーバーへのアクセスログ

5.5.2 アーカイブ保存期間
セコムは、アーカイブを本 CA から発行された証明書が有効でなくなってから、また本 CA の運用に関するものは本 CA が最後に発行した証明書が有効でなくなってから最低 7 年間

保存する。

5.5.3 アーカイブの保護
アーカイブは、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する。

5.5.4 アーカイブのバックアップ手続
セコムパスポート for Member 2.0 PUB に関連するシステムに関する重要なデータに変更がある場合は、適時、アーカイブのバックアップを取得する。

5.5.5 記録にタイムスタンプを付与する要件
セコムは、NTP（Network Time Protocol）を使用してセコムパスポート for Member 2.0 PUB に関連するシステムの時刻同期を行い、セコムパスポート for Member 2.0 PUB に関連するシステム内で記録される重要な情報に対しタイムスタンプを付与する。

5.5.6 アーカイブ収集システム
アーカイブの収集システムは、セコムパスポート for Member 2.0 PUB に関連するシステムの機能に含まれている。

5.5.7 アーカイブの検証手続
アーカイブは、セキュアな保管庫からアクセス権限者が入手し、定期的に媒体（データおよび文書）の保管状況の確認を行う。また必要に応じ、文書においてはデータ化して保管し、アーカイブの完全性および機密性の維持を目的として、新しい媒体への複製を行う。

5.6 鍵の切り替え
本 CA の私有鍵は、私有鍵に対応する証明書の有効期間が証明書利用者に発行した証明書の最大有効期間よりも短くなる前に新たな私有鍵の生成および証明書の発行を行う。新しい私有鍵が生成された後は、新しい私有鍵を使って証明書および CRL の発行を行う。

5.7 危殆化および災害からの復旧

5.7.1 事故および危殆化時の手続
セコムは、事故および危殆化が発生した場合にすみやかにセコムパスポート for Member 2.0 PUB に関連するシステムおよび関連する業務を復旧できるよう、以下を含む事故および危殆化に対する対応手続を策定する。
・ CA 私有鍵の危殆化

・ ハードウェア、ソフトウェア、データ等の破損、故障
・ 火災、地震等の災害

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
セコムは、セコムパスポート for Member 2.0 PUB に関連するシステムのハードウェア、ソフトウェアまたはデータが破損した場合、バックアップ用として保管しているハードウェア、ソフトウェアまたはデータを使用して、すみやかにセコムパスポート for Member 2.0 PUB に関連するシステムの復旧作業を行う。

5.7.3 私有鍵が危殆化した場合の手続
セコムは、本 CA の私有鍵が危殆化したまたは危殆化のおそれがあると判断した場合、および災害等によりセコムパスポート for Member 2.0 PUB に関連するシステムの運用が中断、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、安全に運用を再開させる。

5.7.4 災害後の事業継続性
セコムは、不測の事態が発生した場合にすみやかに復旧作業を実施できるよう、予めセコムパスポート for Member 2.0 PUB に関連するシステムの代替機の確保、復旧に備えたバックアップデータの確保、復旧手続の策定等、可能な限りすみやかに認証基盤システムを復旧するための対策を行う。

5.8 認証局または登録局の終了
セコムが本 CA を終了する場合、事前に LRA および本サービスの契約先にその旨を通知する。本 CA によって発行されたすべての証明書は、本 CA の終了以前に失効を行う。

6. 技術的セキュリティ管理

6.1 鍵ペアの生成およびインストール

6.1.1 鍵ペアの生成

認証基盤システムでは、FIPS140-2 レベル 3 準拠の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 CA の鍵ペアを生成する。鍵ペアの生成作業は、複数名の権限者による操作によって行う。
証明書利用者の鍵ペアは、証明書利用者の所持するブラウザ上で生成するか、または本 CA の施設内において生成する。

6.1.2 証明書利用者に対する私有鍵の交付

証明書利用者の私有鍵は、証明書利用者自身が生成する。本 CA が証明書利用者の私有鍵を生成する場合は、私有鍵を使用するための PIN と私有鍵を、それぞれ異なる経路で送付する。または、対面により、PIN および私有鍵を手交する。

6.1.3 認証局への公開鍵の交付

本 CA に対する証明書利用者の公開鍵の交付は、オンラインによって行うことができる。この時の通信経路は SSL/TLS により暗号化を行う。

6.1.4 検証者への CA 公開鍵の交付

検証者は、本 CA のリポジトリーにアクセスすることによって、本 CA の公開鍵を入手することができる。

6.1.5 鍵サイズ

本 CA の鍵ペアは、RSA 方式で鍵長 2048 ビットまたは 4096 ビットとする。証明書利用者の鍵ペアは、RSA 方式で鍵長 1024、2048、3072 または 4096 ビットとする。

6.1.6 公開鍵のパラメータの生成および品質検査

本 CA の公開鍵のパラメータの生成、およびパラメータの強度の検証は、鍵ペア生成に使用される暗号装置に実装された機能を用いて行われる。
証明書利用者の公開鍵について規定しない。

6.1.7 鍵の用途

本 CA の証明書の KeyUsage には keyCertSign、cRLSign のビットを設定する。
本 CA が発行する証明書利用者の証明書の KeyUsage には、digitalSignature、

nonRepudiation、keyEncipherment、dataEncipherment のいずれかを設定し、設定可能な組み合わせは証明書の利用用途ごと適切に限定される。

6.2 私有鍵の保護および暗号モジュール技術の管理

6.2.1 暗号モジュールの標準および管理

本 CA の私有鍵の生成、保管、署名操作は、FIPS140-2 レベル 3 準拠の HSM を用いて行う。
証明書利用者の私有鍵については規定しない。

6.2.2 私有鍵の複数人管理

本 CA の私有鍵の活性化、非活性化、バックアップ等の操作は、安全な環境において複数人の権限者によって行う。
証明書利用者の私有鍵については規定しない。

6.2.3 私有鍵のエスクロー

本 CA は、本 CA の私有鍵のエスクローは行わない。
本 CA は、証明書利用者の私有鍵のエスクローは行わない。

6.2.4 私有鍵のバックアップ

本 CA の私有鍵のバックアップは、セキュアな室において複数名の権限者によって行われ、暗号化された状態で、セキュアな室に保管される。
証明書利用者の私有鍵については規定しない。

6.2.5 私有鍵のアーカイブ

本 CA では、本 CA の私有鍵のアーカイブは行わない。
証明書利用者の私有鍵については規定しない。

6.2.6 私有鍵の暗号モジュールへのまたは暗号モジュールからの転送

本 CA の私有鍵の HSM への転送または HSM からの転送は、セキュアな室において、私有鍵を暗号化した状態で行う。
証明書利用者の私有鍵については規定しない。

6.2.7 暗号モジュールへの私有鍵の格納

本 CA の私有鍵は、暗号化された状態で HSM 内に格納する。
証明書利用者の私有鍵については規定しない。

6.2.8 私有鍵の活性化方法
本 CA の私有鍵の活性化は、セキュアな室において複数名の権限者によって行う。
証明書利用者の私有鍵については規定しない。

6.2.9 私有鍵の非活性化方法
本 CA の私有鍵の非活性化は、セキュアな室において複数名の権限者によって行う。
証明書利用者の私有鍵については規定しない。

6.2.10 私有鍵の破棄方法
本 CA の私有鍵の廃棄は、複数名の権限者によって完全に初期化または物理的に破壊することによって行う。同時に、バックアップの私有鍵についても同様の手続によって行う。
証明書利用者の私有鍵については規定しない。

6.2.11 暗号モジュールの評価
「6.2.1 暗号モジュールの標準および管理」と同様とする。
証明書利用者の私有鍵については規定しない。

6.3 鍵ペアのその他の管理方法

6.3.1 公開鍵のアーカイブ
本 CA の公開鍵および利用者の公開鍵のアーカイブは、本 CP「5.5.1 アーカイブの種類」に含まれる。
証明書利用者の私有鍵については規定しない。

6.3.2 私有鍵および公開鍵の有効期間
本 CA の私有鍵および公開鍵の有効期間は 20 年以下とする。
証明書利用者の私有鍵については規定しない。なお、本 CA が発行する証明書利用者の証明書の有効期間は以下のとおりとする。

CP/CPS	有効期間
クライアント用証明書ポリシー （署名アルゴリズム：Sha1）	5 年以下
クライアント用証明書ポリシー （署名アルゴリズム：Sha256）	5 年以下
データ署名用証明書ポリシー （署名アルゴリズム：Sha1）	5 年以下

データ署名用証明書ポリシー （署名アルゴリズム：Sha256）	5 年以下
コードサイニング用証明書ポリシー （署名アルゴリズム：Sha256）	3 年 3 か月以下
OCSP サーバー用証明書ポリシー （署名アルゴリズム：Sha256）	4 か月以下

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

本項については、CPS に規定する。

6.4.2 活性化データの保護

本項については、CPS に規定する。

6.4.3 活性化データの他の考慮点

本項については、CPS に規定する。

6.5 コンピューターのセキュリティ管理

6.5.1 コンピューターセキュリティに関する技術的要件

本項については、CPS に規定する。

6.5.2 コンピューターセキュリティ評価

本項については、CPS に規定する。

6.6 ライフサイクルセキュリティ管理

6.6.1 システム開発管理

本項については、CPS に規定する。

6.6.2 セキュリティ運用管理

本項については、CPS に規定する。

6.6.3 ライフサイクルセキュリティ管理

本項については、CPS に規定する。

6.7 ネットワークセキュリティ管理

本項については、CPS に規定する。

6.8 タイムスタンプ

本項については、CPS に規定する。

7. 証明書およびCRL、OCSPのプロファイル

7.1 証明書プロファイル

本CAが発行する証明書はRFC5280に準拠している。プロファイルは、次表のとおりである。

表 7.1-1 CA証明書(sha1)のプロファイル

フィールド（基本領域）		内容	critical
Version （X.509証明書バージョン）		Version 3	-
Serial Number （証明書シリアル番号）		例） 123456789abcdef0	-
Signature Algorithm （署名アルゴリズム）		SHA-1 with RSAEncryption	-
Issuer （発行者）	Country （国）	C=JP	-
	Organization （組織）	O=SECOM Trust.net	
	Organizational Unit （組織単位）	OU=Security Communication RootCA1	
Validity （有効期限）	NotBefore （有効性開始日時）	例） 2016/10/01 00:00:00 GMT	-
	NotAfter （有効性終了日時）	例） 2026/10/01 00:00:00 GMT ＊10年以下の有効期間	
Subject （主体者）	Country （国）	C=JP	-
	Organization （組織）	O=SECOM Trust Systems CO.,LTD.	
	Organizational Unit （組織単位）	OU=SECOM Passport for Member 2.0 PUB	
	Common Name (CN)	CN=SECOM Passport for Member PUB CA"数字" ＊"数字"の値は任意	
Subject PublicKey Info （主体者公開鍵情報）		主体者のRSA公開鍵（2048bit）	-
フィールド（拡張領域）		**内容**	
Subject Key Identifier （主体者鍵識別子）		主体者の公開鍵識別子 （主体者公開鍵の160bit SHA-1ハッシュ値）	N
Authority Key Identifier （発行者鍵識別子）		発行者の公開鍵識別子 （発行者識別子の160bit SHA-1ハッシュ値）	N
CRL Distribution Points（CRL 配付ポイント）		http://repository.secomtrust.net/SC-Root1/SCRoot1CRL.crl	N
Certificate Policies（証明書ポリシー）		Policy: 1.2.392.200091.100.901.1	N

	CPS: https://repository.secomtrust.net/SC-Root1/	
Key Usage （鍵用途）	keyCertSign（証明書への署名） cRLSign（CRL への署名）	Y
Basic Constraints （基本的制約）	TRUE （CA である）	Y

表 7.1-2 CA 証明書(sha256)のプロファイル

フィールド（基本領域）		内容	critical
Version （X.509 証明書バージョン）		Version 3	-
Serial Number （証明書シリアル番号）		例） 123456789abcdef0	-
Signature Algorithm （署名アルゴリズム）		SHA-256 with RSAEncryption	-
Issuer （発行者）	Country （国）	C=JP	-
	Organization （組織）	O=SECOM Trust Systems CO.,LTD.	
	Organizational Unit （組織単位）	OU=Security Communication RootCA2	
Validity （有効期限）	NotBefore （有効性開始日時）	例） 2016/10/01 00:00:00 GMT	-
	NotAfter （有効性終了日時）	例） 2026/10/01 00:00:00 GMT ＊10 年以下の有効期間	
Subject （主体者）	Country （国）	C=JP	-
	Organization （組織）	O=SECOM Trust Systems CO.,LTD.	
	Organizational Unit （組織単位）	以下を設定可能 OU=SECOM Passport for Member 2.0 PUB	
	Common Name (CN)	CN=SECOM Passport for Member PUB CodeSigning CA G"数字" （コードサイニング用証明書ポリシー） CN=SECOM Passport for CodeSigning CA G"数字"（コードサイニング用証明書ポリシー） CN=SECOM Passport for Member PUB CA"数字"（上記以外の証明書ポリシーおよび上記を除くコードサイニング用証明書ポリシー） ＊"数字"の値は任意	

Subject PublicKey Info （主体者公開鍵情報）	主体者の RSA 公開鍵（コードサイニング用証明書ポリシーでは 2048bit または 4096bit とし、それ以外は 2048bit）	-
フィールド（拡張領域）	内容	
Subject Key Identifier （主体者鍵識別子）	主体者の公開鍵識別子 （主体者公開鍵の 160bit SHA-1 ハッシュ値）	N
Authority Key Identifier （発行者鍵識別子）	発行者の公開鍵識別子 （発行者識別子の 160bit SHA-1 ハッシュ値）	N
CRL Distribution Points（CRL 配付ポイント）	http://repository.secomtrust.net/SC-Root2/SCRoot2CRL.crl	N
Authority Information Access （機関情報アクセス）	accessMethod ocsp（1.3.6.1.5.5.7.48.1） accessLocation http://scrootca2.ocsp.secomtrust.net accessMethod caIssuers（1.3.6.1.5.5.7.48.2） accessLocation http://repository.secomtrust.net/SC-Root2/SCRoot2ca.cer ＊必要に応じて設定する	N
Certificate Policies（証明書ポリシー）	Policy: 1.2.392.200091.100.901.4 Policy: 2.23.140.1.4.1（コードサイニング用証明書ポリシーのみ付与） CPS: リポジトリーの URL	N
Key Usage （鍵用途）	keyCertSign（証明書への署名） cRLSign（CRL への署名）	Y
Extended Key Usage （拡張鍵用途）	以下を設定可能 clientAuth（クライアント認証） emailProtection（E-mail 保護） SmartCard Logon（スマートカードログオン） codeSigning（コードサイニング） Adobe Authentic Documents Trust =1.2.840.113583.1.1.5	N

	Microsoft Signer of documents =1.3.6.1.4.1.311.10.3.12 ＊SmartCard Logon 選択時は、clientAuth も同時選択 ＊codeSigning（コードサイニング）は単体で選択	
Basic Constraints （基本的制約）	TRUE （CA である）	Y

表 7.1-3 証明書利用者証明書(sha1)のプロファイル

フィールド（基本領域）		内容	critical
X.509 Version （X.509 証明書バージョン）		Version 3	-
Serial Number （証明書シリアル番号）		例） 123456789abcdef0	-
Signature Algorithm （署名アルゴリズム）		SHA-1 with RSAEncryption	-
Issuer （発行者）	Country （国）	C=JP	-
	Organization （組織）	O=SECOM Trust Systems CO.,LTD.	
	Organizational Unit （組織単位）	OU=SECOM Passport for Member 2.0 PUB	
	Common Name (CN)	CN=SECOM Passport for Member PUB CA"数字" ＊"数字"の値は任意	
Validity （有効期限）	NotBefore （有効性開始日時）	例） Feb 10 09:55:27 2017 GMT	-
	NotAfter （有効性終了日時）	例） Feb 10 10:25:27 2018 GMT ＊各証明書ポリシーに準ずる	
Subject （主体者）	Country （国）	C=JP	-
	stateOrProvinceName （都道府県）	ST="都道府県名" 【オプション】	
	localityName （市区町村）	L="市区町村名" 【オプション】	
	Organization （組織）	O="組織名"	
	Organizational Unit （組織単位）	OU="組織単位" 【オプション】	
	Organizational Unit （組織単位）	OU="任意の値" 【任意に指定可能】	
	Organizational Unit （組織単位）	OU="任意の値" 【任意に指定可能】	

	Common Name （主体者名）	CN="利用者名"	
	Serial Number （シリアル番号）	SerialNumber="シリアル番号" 【任意に指定可能】	
Subject PublicKey Info （主体者公開鍵情報）		主体者の公開鍵データ	-

フィールド（x.509 v3 拡張領域）	内容	critical
Authority Key Identifier （発行者鍵識別子）	発行者の公開鍵識別子 （発行者公開鍵の 160bit SHA-1 ハッシュ値）	N
Subject Key Identifier （主体者鍵識別子）	主体者の公開鍵識別子 （主体者公開鍵の 160bit SHA-1 ハッシュ値）	N
Key Usage （鍵用途）	以下を設定可能 digitalSignature（ディジタル署名） Non Repudiation（否認防止） keyEncipherment（鍵暗号化） dataEncipherment（データ暗号化）	Y
Certificate Policies （証明書ポリシー）	以下を設定可能 Policy: 1.2.392.200091.100.381.1 Policy: 1.2.392.200091.100.381.2 Policy: 1.2.392.200091.100.381.6 CPS: https://repo1.secomtrust.net/spcpp/pfm20pub/	N
Subject Alt Name （主体者別名）	以下を設定可能 OtherName: UPN="ユーザープリンシパル名" OtherName: "OID"="任意文字列" Rfc822Name:"メールアドレス" dNSName:"サーバー名"	N
Extended Key Usage （拡張鍵用途）	以下を設定可能 clientAuth（クライアント認証） emailProtection（E-mail 保護） SmartCard Logon（スマートカードログオン） codeSigning（コードサイニング） ＊SmartCard Logon 選択時は、clientAuth も同時選択 ＊codeSigning（コードサイニング）は単体で選択	N
CRL Distribution Points （CRL 配布ポイント）	http://repo1.secomtrust.net/spcpp/pfm20pub/ca"数字"/fullCRL.crl	N

	＊"数字"の値は任意 ldap://repo1.secomtrust.net/"IssuerDN"?certificateRevocationList	
Netscape Certificate Type （Netscape 証明書タイプ）	以下を設定可能 SSL Client S/MIME Client codeSigning	N

表 7.1-4 証明書利用者証明書(sha256)のプロファイル

フィールド（基本領域）		内容	critical
X.509 Version （X.509 証明書バージョン）		Version 3	-
Serial Number （証明書シリアル番号）		例） 123456789abcdef0	-
Signature Algorithm （署名アルゴリズム）		SHA-256 with RSAEncryption	-
Issuer （発行者）	Country （国）	C=JP	-
	Organization （組織）	O=SECOM Trust Systems CO.,LTD.	
	Organizational Unit （組織単位）	以下を設定可能 OU=SECOM Passport for Member 2.0 PUB	
	Common Name (CN)	CN=SECOM Passport for Member PUB CodeSigning CA G"数字" （コードサイニング用証明書ポリシー） CN=SECOM Passport for CodeSigning CA G"数字" （コードサイニング用証明書ポリシー） CN=SECOM Passport for Member PUB CA"数字" （上記以外の証明書ポリシーおよび上記を除くコードサイニング用証明書ポリシー） ＊"数字"の値は任意	
Validity （有効期限）	NotBefore （有効性開始日時）	例） Feb 10 09:55:27 2017 GMT	-
	NotAfter （有効性終了日時）	例） Feb 10 10:25:27 2018 GMT ＊各証明書ポリシーに準ずる	
Subject （主体者）	Country （国）	C=JP	-
	stateOrProvinceName （都道府県）	ST="都道府県名" 【オプション】	

	localityName （市区町村）	L="市区町村名" 【オプション】	
	Organization （組織）	O="組織名"	
	Organizational Unit （組織単位）	OU="組織単位" 【オプション】	
	Organizational Unit （組織単位）	OU="任意の値" 【任意に指定可能】	
	Organizational Unit （組織単位）	OU="任意の値" 【任意に指定可能】	
	Common Name （主体者名）	CN="利用者名"	
	Serial Number （シリアル番号）	SerialNumber="シリアル番号" 【任意に指定可能】	
Subject PublicKey Info （主体者公開鍵情報）		主体者の公開鍵データ コードサイニング用証明書ポリシーでは2048bit 、3072bit または 4096bit とし、それ以外は 2048bit	-

フィールド（x.509 v3 拡張領域）	内容	critical
Authority Key Identifier （発行者鍵識別子）	発行者の公開鍵識別子 （発行者公開鍵の 160bit SHA-1 ハッシュ値）	N
Subject Key Identifier （主体者鍵識別子）	主体者の公開鍵識別子 （主体者公開鍵の 160bit SHA-1 ハッシュ値）	N
Key Usage （鍵用途）	以下を設定可能 digitalSignature（ディジタル署名） Non Repudiation（否認防止） keyEncipherment（鍵暗号化） dataEncipherment（データ暗号化）	Y
Certificate Policies （証明書ポリシー）	以下を設定可能 Policy: 1.2.392.200091.100.381.4 Policy: 1.2.392.200091.100.381.5 Policy: 1.2.392.200091.100.381.8 CPS:リポジトリーの URL Policy: 2.23.140.1.4.1（コードサイニング用証明書ポリシーのみ付与）	N
Subject Alt Name （主体者別名）	以下を設定可能 OtherName: UPN="ユーザープリンシパル名"	N

	OtherName: "OID"="任意文字列" Rfc822Name:"メールアドレス" ＊コードサイニング用証明書ポリシーは使用しない	
Extended Key Usage （拡張鍵用途）	以下を設定可能 clientAuth（クライアント認証） emailProtection（E-mail 保護） SmartCard Logon（スマートカードログオン） codeSigning（コードサイニング） Adobe Authentic Documents Trust =1.2.840.113583.1.1.5 Microsoft Signer of documents =1.3.6.1.4.1.311.10.3.12 ＊SmartCard Logon 選択時は、clientAuth も同時選択 ＊codeSigning（コードサイニング）は単体で選択	N
CRL Distribution Points （CRL 配布ポイント）	http://repo1.secomtrust.net/spcpp/pfm20pub/codecag"数字"/fullCRL.crl（コードサイニング用証明書ポリシー） http://repo1.secomtrust.net/spcpp/pfm20pub/ca"数字"/fullCRL.crl（上記以外の証明書ポリシーおよび上記を除くコードサイニング用証明書ポリシー） ＊"数字"の値は任意 ldap://repo1.secomtrust.net/"IssuerDN"?certificateRevocationList ＊ldap は必要に応じて設定する	N
Authority Information Access （機関情報アクセス）	accessMethod ocsp（1.3.6.1.5.5.7.48.1） accessLocation OCSP レスポンダーの URL accessMethod caIssuers（1.3.6.1.5.5.7.48.2） accessLocation 中間 CA 証明書の URL ＊必要に応じて設定する	N
Netscape Certificate Type （Netscape 証明書タイプ）	以下を設定可能 SSL Client S/MIME Client	N

	codeSigning	

※ 【任意に指定可能】と記載している項目は、証明書申請毎に設定の有無を変えられる項目である。

※ 【オプション】と記載している項目は、LRA 毎に設定の有無を変えられる項目である。ただし、セコムが定める組み合わせでのみ設定可能とする。
なお、コードサイニング用証明書ポリシーを含む証明書の発行に際しては、BR for Code Signing に準拠した登録とする。

7.1.1 バージョン番号

本 CA は、バージョン 3 を適用する。

7.1.2 証明書拡張

本 CA が発行する証明書は、証明書拡張フィールドを使用する。

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。

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

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

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。

7.1.5 名前制約

必要に応じて本 CA で設定する。

7.1.6 CP オブジェクト識別子

本 CA が発行する証明書の OID は、「1.2 文書名と識別」の OID のとおりである。

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。

7.2 CRL プロファイル

表 7.2-1 CRL(sha1)のプロファイル

フィールド（基本領域）		内容	critical
Version（X.509CRL バージョン）		Version 2	-
Signature Algorithm（署名アルゴリズム）		SHA-1 with RSAEncryption	-
Issuer（発行者）	Country （国）	C=JP	-
	Organization （組織）	O=SECOM Trust Systems CO.,LTD.	
	Organizational Unit（組織単位）	OU=SECOM Passport for Member 2.0 PUB	
	Common Name（CN）	CN= SECOM Passport for Member PUB CA″数字″ ＊″数字″の値は任意	
This Update（更新日時）		例） Oct 1 00:00:00 2016 GMT	-
Next Update（次回更新予定日時）		例） Oct 5 00:00:00 2016 GMT ＊実更新間隔 24 時間、有効期間 96 時間	
Revoked Certificates（失効証明書）	Serial Number（失効証明書シリアル番号）	例） 1234567890	-
	Revocation Date （失効日時）	例） 2016/09/01 12:00:00 GMT	
	Reason Code （失効事由）	例）cessation of operation(運用停止) ＊設定は任意	
フィールド（拡張領域）		内容	
CRL Number （CRL 番号）		例） 1 （CRL の発行順序を示す整数値）	N
Authority Key Identifier （発行者鍵識別子）		発行者の公開鍵識別子 （公開鍵の SHA-1 ハッシュ値）	N

表 7.2-2 CRL(sha256)のプロファイル

フィールド（基本領域）		内容	critical
Version（X.509CRL バージョン）		Version 2	-
Signature Algorithm（署名アルゴリズム）		SHA-256 with RSAEncryption	-
Issuer（発行者）	Country （国）	C=JP	-
	Organization （組織）	O=SECOM Trust Systems CO.,LTD.	
	Organizational Unit（組織単位）	以下を設定可能 OU=SECOM Passport for Member 2.0 PUB	

	Common Name (CN)	CN=SECOM Passport for Member PUB CodeSigning CA G"数字" (コードサイニング用証明書ポリシー) CN=SECOM Passport for CodeSigning CA G"数字" (コードサイニング用証明書ポリシー) CN=SECOM Passport for Member PUB CA"数字"(上記以外の証明書ポリシーおよび上記を除くコードサイニング用証明書ポリシー) ＊"数字"の値は任意	
This Update (更新日時)		例) Oct 1 00:00:00 2016 GMT	-
Next Update (次回更新予定日時)		例) Oct 5 00:00:00 2016 GMT ＊実更新間隔 24 時間、有効期間 96 時間	
Revoked Certificates (失効証明書)	Serial Number (失効証明書シリアル番号)	例) 1234567890	-
	Revocation Date (失効日時)	例) 2016/09/01 12:00:00 GMT	
	Reason Code (失効事由)	例) cessation of operation(運用停止) ＊設定は任意	
フィールド (拡張領域)		内容	
CRL Number (CRL 番号)		例) 1 (CRL の発行順序を示す整数値)	N
Authority Key Identifier (発行者鍵識別子)		発行者の公開鍵識別子 (公開鍵の SHA-1 ハッシュ値)	N

7.2.1 バージョン番号

本 CA は、CRL バージョン 2 を適用する。

7.2.2 CRL 拡張

本 CA が発行する CRL 拡張フィールドを使用する。

7.3 OCSP のプロファイル

表 7.3-1 OCSP プロファイル(sha256)

フィールド（基本領域）		内容	critical
Version		Version 3	-
Serial Number		例）0123456789	-
Signature Algorithm（署名アルゴリズム）		SHA-256 with RSAEncryption	-
Issuer（発行者）	Country （国）	C=JP	-
	Organization （組織）	O=SECOM Trust Systems CO.,LTD.	
	Organizational Unit（組織単位）	以下を設定可能 OU=SECOM Passport for Member 2.0 PUB	
	Common Name（CN）	CN=SECOM Passport for Member PUB CodeSigning CA G"数字" （コードサイニング用証明書ポリシー） CN=SECOM Passport for CodeSigning CA G"数字"（コードサイニング用証明書ポリシー） CN=SECOM Passport for Member PUB CA"数字"（上記以外の証明書ポリシーおよび上記を除くコードサイニング用証明書ポリシー） ＊"数字"の値は任意	
Validity（有効期限）	NotBefore（有効性開始日時）	例）2017/1/1 00:00:00 GMT	-
	NotAfter（有効性終了日時）	例）2017/5/1 00:00:00 GMT ＊有効期間 4 か月	-
Subject（主体者）	Country （国）	C=JP	-
	Organization （組織）	O=SECOM Trust Systems CO.,LTD.	-
	Organizational Unit（組織単位）	OU=SECOM Passport for Member 2.0 PUB Service	-
	Common Name（CN）	OCSPサーバー名（必須）	-
Subject Public Key Info（主体者公開鍵情報）		主体者の公開鍵データ	-
フィールド（拡張領域）		内容	
KeyUsage（鍵用途）		digitalSignature	Y
ExtendedKeyUsage（拡張鍵用途）		OCSPSigning	N
OCSP No Check		null	N

CertificatePolicies（証明書ポリシー）	policyIdentifier OID= 1.2.392.200091.100.381.9 policyQualifiers policyQualifierId=CPS qualifiier=リポジトリーのURL	N
Authority Key Identifier （発行者鍵識別子）	発行者公開鍵のSHA-1 ハッシュ値（160ビット）	N
Subject Key Identifier （主体者鍵識別子）	主体者公開鍵のSHA-1 ハッシュ値（160ビット）	N

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

本 CA が発行する OCSP 拡張フィールドを使用する。

8. 準拠性監査と他の評価

8.1 監査の頻度

本 CA は、本 CP および CPS に準拠して運用がなされているかについて、適時監査を行う。S/MIME 証明書およびコードサイニング証明書の運用に関しては、本 CP および CPS に準拠して運用がなされているか、年に１回以上、WebTrust 規準に基づく準拠性監査を行う。

8.2 監査人の身元／資格

本 CA の準拠性監査は、CA の業務に精通している監査人が行う。また、WebTrust 認証を受ける CA の監査は、監査法人が行う。

8.3 監査人と被監査部門の関係

監査人は、監査に関する事項を除き、被監査部門の業務から独立した立場にあるもの、もしく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。監査の実施にあたり、被監査部門は監査に協力するものとする。

8.4 監査で扱われる事項

監査は、本 CA の運用にかかる業務を対象として行う。
また、認証局のための WebTrust for CA 規準、WebTrust for CA Code Signing 規準に基づいて行われることもある。

8.5 不備の結果としてとられる処置

セコムは、監査報告書で指摘された事項に関し、すみやかに必要な是正措置を行う。

8.6 監査結果の開示

監査結果は、監査人からセコムに対して報告される。
セコムは、法律に基づく開示要求があった場合、セコムとの契約に基づき関係組織からの開示要求があった場合、および認証サービス改善委員会が承認した場合を除き、監査結果を外部へ開示することはない。
なお、WebTrust for CA 、WebTrust for CA Code Signing の検証に関する報告書は、WebTrust for CA 規準、WebTrust for CA Code Signing 規準に従い、特定のサイトにて参照可能となる。

9. 他の業務上および法的事項

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 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 の運用維持にあたり、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

本項については、CPS に規定する。

9.3.2 機密情報の範囲外の情報

本項については、CPS に規定する。

9.3.3 機密情報を保護する責任
本項については、CPS に規定する。

9.4 個人情報の保護

9.4.1 個人情報保護方針
本項については、CPS に規定する。

9.4.2 個人情報として扱われる情報
本項については、CPS に規定する。

9.4.3 個人情報とみなされない情報
本項については、CPS に規定する。

9.4.4 個人情報を保護する責任
本項については、CPS に規定する。

9.4.5 個人情報の使用に関する通知と同意
本項については、CPS に規定する。

9.4.6 司法または行政手続に沿った情報開示
本項については、CPS に規定する。

9.4.7 その他の情報開示条件
本項については、CPS に規定する。

9.5 知的財産権
以下に示す著作物は、セコムに帰属する財産である。

- 本 CP : セコムに帰属する財産（著作権を含む）である
- CPS : セコムに帰属する財産（著作権を含む）である
- CRL : セコムに帰属する財産である

9.6 表明保証

9.6.1 認証局の表明保証

セコムは、CA の業務を遂行するにあたり次の義務を負う。

- CA 私有鍵のセキュアな生成・管理を行うこと
- LRA および申請者からの申請に基づいた証明書の正確な発行、失効および管理を行うこと
- CA のシステムの運用、稼動監視を行うこと
- CRL の発行、公表を行うこと
- OCSP サーバーの公開を行うこと
- リポジトリーの維持管理を行うこと

9.6.2 RA の表明保証

セコムは、RA の業務を遂行するにあたり次の義務を負う。

- 登録端末のセキュアな環境への設置・運用を行うこと
- LRA および組織、団体等からの申請に対して、実在性確認等の審査を的確に行うこと

また LRA は、LRA の業務を遂行するにあたり次の業務を負う。

- 登録端末のセキュアな環境への設置・運用を行うこと
- 申請者および証明書利用者からの申請に対して、実在性確認等の審査を的確に行うこと
- 本 CA への証明書発行・失効等の申請を正確かつすみやかに行うこと

9.6.3 申請者および証明書利用者の表明保証

申請者および証明書利用者は、次の義務を負うものとする。

- 証明書の発行申請に際して、本 CA または LRA に正確かつ完全な情報を提供すること
- 証明書の発行申請に際して、本 CA または LRA に正確かつ完全な情報を提供すること。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 または LRA まで通知すること
- 危殆化から自身の私有鍵を保護すること
- 証明書の使途は本 CP および CPS に従うこと
- 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、もしくは登録情報に変更があった場合や、本 CA から「4.9.1 証明書失効事由」にもとづき証明書失効の指示があった場合は、証明書利用者は本 CA または LRA に証明書の失効をすみやかに申請すること

9.6.4 検証者の表明保証

検証者は、次の義務を負うものとする。

- 本 CA の証明書について、有効性の確認を行うこと

- 証明書利用者が使用している証明書の有効性について、証明書の有効期限を過ぎていないか、CRL または OCSP サーバーにより証明書が失効されていないか確認を行うこと
- 証明書利用者の情報を信頼するかの判断は検証者の責任で行うこと

9.6.5 他の関係者の表明保証

規定しない。

9.7 無保証

セコムは、本 CP「9.6.1 認証局の表明保証」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 認証局の表明保証」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、不正使用または過失等により発生する一切の損害
- 証明書利用者が自己の義務の履行を怠ったために生じた損害
- LRA または証明書利用者のシステムに起因して発生した一切の損害
- LRA または証明書利用者の環境（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
- セコムの責に帰することのできない事由で証明書および CRL、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 の業務停止に起因する一切の損害

9.9 補償

本 CA が発行する証明書に関する補償については、別途規定する。

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セコムパスポート for Member 2.0 PUB 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

証明書利用者が証明書の利用を終了する場合、セコムと契約先との間で契約が終了する場合、セコムが提供するサービス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証明書利用者、検証者、セコムの契約先およびセコムに適用されるものとする。

9.11 関係者間の個別通知と連絡

セコムは、LRA、証明書利用者および検証者に対する必要な通知をホームページ、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

本 CP は、セコムの判断によって適宜改訂され、認証サービス改善委員会の承認によって発効する。

9.12.2 通知方法および期間

本 CP を変更した場合、変更した本 CP をすみやかに公表することをもって、関係者に対しての告知とする。

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 紛争解決手続

本 CA が発行する証明書に関わる紛争について、セコムに対して訴訟、仲裁等を含む法的解決手段に訴えようとする場合は、セコムに対して事前にその旨を通知するものとする。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。

9.14 準拠法

本 CP、CPS の解釈、有効性および証明書の利用にかかわる紛争については、日本国の法律を適用する。

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、証明書利用者または検証者の義務等を本 CP、および CPS 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。

9.16.2 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

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。