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

Version 2.05

2025 年 10 月 22 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	2007/09/27	新規作成
2.00	2015/06/12	署名アルゴリズム Sha256 の追加
2.01	2022/06/10	全体的な文言および体裁の見直し
2.02	2023/05/17	「4.9.9 オンラインでの失効/ステータス確認の適用性」を更新 「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」を更新 「6.1.5 鍵サイズ」を更新 「7.1.1 CA 証明書のプロファイル」を更新 「7.1.2 証明書利用者証明書のプロファイル」を更新 「7.2 CRL プロファイル」を更新
2.03	2024/10/23	表記の修正 以下を更新 1.5.2 連絡先 1.6 定義と略語 2.1 リポジトリ 2.2 証明情報の公開 6.1.1 鍵ペアの生成 6.2.1 暗号モジュールの標準および管理 7.1 証明書プロファイル 7.1.1 バージョン番号 7.1.2 証明書拡張 7.1.3 アルゴリズムオブジェクト識別子 7.1.4 名前形式 7.1.5 名前制約 7.1.6 CP オブジェクト識別子 7.1.7 証明書プロファイルポリシー制約拡張の利用 7.1.8 ポリシ修飾子の文法および意味 7.1.9 重要な証明書ポリシ拡張の処理の意味 7.2 CRL プロファイル 7.2.1 バージョン番号 7.2.2 CRL 拡張 7.3 OCSP プロファイル 7.3.1 バージョン番号

		7.3.2 OCSP 拡張
2.04	2024/12/19	以下を更新 6.3.2 私有鍵および公開鍵の有効期間
2.05	2025/10/22	以下を更新 1.2 文書名と識別 6.1.5 鍵サイズ 6.1.7 鍵の用途 7.1 証明書プロファイル 7.1.3 アルゴリズムオブジェクト識別子 7.2 CRL プロファイル 7.3 OCSP プロファイル

目次

1. はじめに

1.1 概要

セコムパスポート for Member 2.0 証明書ポリシ（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「セコムトラストシステムズ」という）が運用するセコムパスポート for Member 2.0 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 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、セコムトラストシステムズ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 RFC 3647「Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework」に準拠している。

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 証明書ポリシ」という。本 CP の登録された一意のオブジェクト識別子(以下、OID という)および参照する CPS の OID は、次のとおりである。

CP/CPS	OID
セコムパスポート for Member 2.0 (SHA1)証明書	1.2.392.200091.100.371.1
セコムパスポート for Member 2.0 (SHA-256, SHA-384)証明書	1.2.392.200091.100.371.2
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、IA（Issuing Authority：発行局）および RA（Registration Authority：登録局）によって構成される。電子認証基盤の上で運用される CA の運営主体はセコムトラストシステムズである。

1.3.1.1 IA

IA は、証明書の発行、失効、CRL（Certificate Revocation List：証明書失効リスト）の開示、リポジトリの維持管理等を行う。電子認証基盤の上で運用される CA において、IA の運用はセコムトラストシステムズが行う。

1.3.1.2 RA

RA は、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。
セコムトラストシステムズが事前に審査し、セコムトラストシステムズが実在性を確認した特別な組織または、団体は、LRA（Local Registration Authority）と呼ばれ、LRA は、証明書の発行、失効を申請する利用者の実在性確認、本人性確認の審査および証明書を発行、失効するための登録業務等を行う。

1.3.2 利用者

利用者とは、セコムトラストシステムズに対し、 証明書を利用する個人、法人その他の組織とする。

1.4 証明書の用途

1.4.1 適切な証明書の用途

本 CA が発行する証明書は、同一のイントラネットあるいはその組織、もしくは団体に所属する利用者間で利用される。但し、利用方法はそれだけに限定するものではなく、セコムパスポート for Member 2.0 の利用に際しては、利用者および利用者が本 CP および CPS を理解し承認していることを前提に、利用者および利用者自身の判断に委ねられる。

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、セコムトラストシステムズが行う。

1.5.2 連絡先

本 CP に関する問い合わせ先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

問い合わせ内容	本 CP に関する問い合わせ
E-mail	ca-support@secom.co.jp
受付対応時間	9:00～18:00（土日・祝日および年末年始を除く）

1.5.3 ポリシ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、セコムトラストシステムズが作成・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

五十音順（あ行～わ行）

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。

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。

リポジトリ
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。

アルファベット順（A～Z）

CA（Certification Authority）：認証局
証明書の発行・更新・失効、CA 私有鍵の生成・保護および利用者の登録等を行う主体のことをいう。

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。

FIPS 140

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。

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。

IA（Issuing Authority）：発行局

CA の業務のうち、証明書の発行・更新・失効、CA 秘密鍵の生成・保護、リポジトリの維持・管理等を行う主体のことをいう。

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。

RFC 3647（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。

2. 公開とリポジトリの責任

2.1 リポジトリ

本 CA は、本 CP に基づき利用者証明書に対する失効情報を提供する。

2.2 証明情報の公開

セコムトラストシステムズは、次の内容をリポジトリに格納し利用者および検証者がオンラインによって参照できるようにする。

- CRL
- 本 CA 証明書
- 最新の本 CP、CPS
- 本 CA が発行する証明書に関するその他関連情報

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 リポジトリへのアクセス管理

利用者および検証者は、随時、リポジトリを参照できる。リポジトリへのアクセスに用いるプロトコルは、HTTP（Hyper Text Transfer Protocol）、HTTPS（HTTP に 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 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。

3.1.3 認識、認証および商標の役割

セコムトラストシステムズは、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検証を行わない。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。セコムトラストシステムズは、登録商標等を理由に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、セコムトラストシステムズは紛争を理由に利用者からの証明書申請の拒絶や発行された証明書失効をする権利を有する。

3.2 初回の本人確認

3.2.1 LRA 組織の認証

セコムトラストシステムズは、セコムトラストシステムズが信頼する第三者による調査またはそのデータベース、組織の認証を国や地方公共団体が発行する公的書類、または、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認証する。組織の認証を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を提出する。

3.2.2 提出書類

LRA 組織の審査時に、LRA 組織がセコムトラストシステムズへ提出する書類は、次のとおりである。

- LRA 業務を担う者を届出る書類
- その他、認定時にセコムトラストシステムズが必要とする書類

(注) 審査の結果により、セコムトラストシステムズが LRA として認定不可とした場合、

LRA からセコムトラストシステムズへ提出された書類は、すべて返却する。尚、契約書を受領していたときは、セコムトラストシステムズがこれを破棄する。

3.2.3 利用者の認証

利用者の審査、本人確認は事前に LRA 組織によって決定された方法（LRA 運用規準）により行なわれる。

3.2.4 権限の正当性確認

セコムトラストシステムズは、証明書に関する申請を行う者が、その申請を行うための正当な権限を有していることを本 CP「3.2.1 LRA 組織の認証」によって確認する。

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

鍵更新時における利用者の本人性確認および認証は、「3.2 初回の本人性認証」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

失効した証明書の更新は行わない。証明書申請は新規扱いとし、利用者の本人性確認および認証は、「3.2 初回の本人性確認」と同様とする。

3.4 失効申請時の本人性確認と認証

利用者の審査、本人確認は事前に LRA 組織によって決定された方法により行なわれる。

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

証明書の申請を行うことのできる者は、セコムトラストシステムズが LRA 組織を審査および本人確認を行った後、RA 受付システムにアクセス権限を有する。申請方法は、発行申請者の情報を送付し、証明書の発行申請を行うことができる。

4.2 証明書申請手続

4.2.1 本人性確認と認証の実施

セコムトラストシステムズは、証明書申請を受け付けた後、本 CP「3.2 初回の識別と認証」に基づく確認を行う。

4.2.2 証明書申請の処理時間

セコムトラストシステムズは、証明書申請について、すみやかに証明書の発行を行う。

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 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 組織または利用者に配付する。オフラインの場合は、郵送、電子メール、手交等の方法により、秘密鍵と 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 組織または利用者からの受領の報告を受けた場合、若しくは、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 組織または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、利用者証明書の公開は行わない。

4.5 鍵ペアおよび証明書の用途

4.5.1 利用者の私有鍵および証明書の用途
利用者は、同一のイントラネットあるいはその組織、もしくは団体に所属する利用者間で利用される。但し、利用方法はそれだけに限定するものではなく、セコムパスポート for Member 2.0 の利用に際しては、LRA 組織および利用者が本 CP および CPS を理解し承認していることを前提に、LRA 組織および利用者の判断に委ねられる。

4.6 証明書の更新
本 CA は、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 証明書更新の状況
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 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 証明書の鍵更新

4.7.1 鍵更新の状況
証明書の鍵更新は、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 新しい公開鍵の証明書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 鍵更新をともなう証明書申請の処理手続
「4.3.1.証明書発行時の処理手続」と同様とする。

4.7.4 利用者に対する新しい証明書の通知
「4.3.2.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。

4.8 証明書の変更
本 CA は、証明書に登録された情報の変更が必要となった場合、その証明書の失効および新規発行とする。

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
規定しない。

4.8.3 変更申請の処理手続
規定しない。

4.8.4 利用者に対する新しい証明書発行通知
規定しない。

4.8.5 変更された証明書の受領確認手続
規定しない。

4.8.6 認証局による変更された証明書の公開
規定しない。

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
LRA 組織および利用者は、次の事由が発生した場合、セコムトラストシステムズに対し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、セコムトラストシステムズは、次の事由が発生した場合に、セコムトラストシステムズの判断により利用者証明書を失効することができる。

- 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
- 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
- セコムトラストシステムズ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
証明書の失効申請を行うことができる者は、セコムトラストシステムズが LRA 組織を審査および本人確認を行った後、RA 受付システムにアクセス権限を有する者。申請方法は、失効申請者の情報を送付し、証明書の失効申請を行うことができる。

4.9.3 失効申請手続
LRA 組織は、LRA 組織だけがアクセス可能なサイトから該当の証明書情報を選択し失効申請を行う。

4.9.4 失効申請の猶予期間
利用者は、秘密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には、すみやかに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
セコムトラストシステムズは、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。
CRL は、一般的な Web インターフェースを用いてアクセスすることができる。なお、CRL には、有効期限の切れた証明書情報は含まれない。
検証者は、利用者証明書について、有効性を確認しなければならない。証明書の有効性は、リポジトリサイトに掲載している CRL により確認する。

4.9.7 証明書失効リストの発行頻度
CRL は、失効処理の有無にかかわらず、24 時間ごとに更新を行う。証明書の失効処理が行われた場合は、その時点で CRL の更新を行う。

4.9.8 証明書失効リストの発行最大遅延時間
本 CA が発行した CRL は、即時にリポジトリに反映させる。

4.9.9 オンラインでの失効/ステータス確認の適用性
必要に応じて OCSP レスポンダ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、利用者証明書について、有効性を確認しなければならない。リポジトリに掲載している CRL により、証明書の失効登録の有無を確認しない場合には、OCSP レスポンダーにより提供される証明書ステータス情報の確認を行わなければならない。

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 証明書の一時停止事由
証明書の一時停止は、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、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 LRA に対して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、LRA 組織または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
セコムトラストシステムズから事前に通知されるサイトにアクセスし、別途 LRA 組織から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
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
規定しない。

4.10.2 サービスの利用可能性
規定しない。

4.10.3 オプショナルな仕様
規定しない。

4.11 利用の終了
LRA 組織、および利用者は本サービスの利用を終了する場合、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および実施
本 CA は、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および実施

規定しない。

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
セコムトラストシステムズは、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 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。

- 発行した証明書および CRL
- 本 CPS
- 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 組織からの申請書類

5.5.2 アーカイブ保存期間
セコムトラストシステムズは、アーカイブを最低 5 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

証明書発行、取消または CRL の発行等、セコムパスポート for Member 2.0 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

セコムトラストシステムズは、NTP（Network Time Protocol）を使用してセコムパスポート for Member 2.0 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 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 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、定期的に媒体の保管状況の確認を行う。また必要に応じ、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。

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

セコムトラストシステムズは、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 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
セコムトラストシステムズは、セコムパスポート for Member 2.0 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 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
セコムトラストシステムズは、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 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
セコムトラストシステムズは、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 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
セコムトラストシステムズが本 CA を終了する場合、事前に LRA 組織および利用者その旨を通知する。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、CPS「6.2.7 私有鍵の暗号モジュールへの格納」に準拠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 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。

利用者の鍵ペアは、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 利用者に対する私有鍵の交付

利用者の私有鍵は、利用者自身が生成する。本 CA が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 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、以下のいずれかの方式および鍵長とする。

- RSA 方式：2048 ビットまたは 4096 ビット
- ECC 方式：256 ビット以上

利用者証明書の鍵ペアについては、以下の方式および鍵長を推奨する。

- RSA 方式：2048 ビット以上
- ECC 方式：256 ビット以上

OCSP 証明書の鍵ペアについては、以下の方式および鍵長とする。

- RSA 方式：2048 ビット以上
- ECC 方式：256 ビット以上

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。

利用者の公開鍵のパラメータの生成および品質検査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 が発行する利用者証明書の KeyUsage には、digitalSignature、nonRepudiation、keyEncipherment（RSA 方式のみ）、dataEncipherment（RSA 方式のみ）を設定可能とする。

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、CPS「6.2.7 私有鍵の暗号モジュールへの格納」に準拠した HSM を用いて行う。

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。

利用者の私有鍵の活性化、非活性化、バックアップ等の操作は、利用者の管理の下で安全に行わなければならない。

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、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。

利用者の私有鍵のバックアップは、利用者の管理の下で安全に保管しなければならない。

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。

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。

利用者の私有鍵については規定しない。

6.2.7 私有鍵の暗号モジュールへの格納

本電子認証基盤の上で運用される CA の私有鍵は、暗号化された状態で CPS「6.2.7 私有鍵の暗号モジュールへの格納」に準拠した HSM 内に格納する。

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。

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。

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。バックアップについても同様の手続によって行う。

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

本 CA で使用する HSM の品質基準については、本 CP「6.2.1.暗号モジュールの標準および管理」のとおりである。

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 の公開鍵については CPS「6.2.1 暗号モジュールの標準および管理」のとおりである。

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。
利用者の私有鍵については規定しない。なお、本 CA が発行する利用者証明書の有効期間は 5 年以下とする。ただし、タイムスタンプ証明書については有効期間を 5 年 6 か月以下とする。

6.4 活性化データ

6.4.1 活性化データの生成および設定
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
規定しない。

6.5 コンピュータのセキュリティ管理

6.5.1 コンピュータセキュリティに関する技術的要件
本項については、CPS に規定する。

6.5.2 コンピュータセキュリティ評価
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 のプロファイル

7.1 証明書プロファイル

CA 証明書のプロファイル

基本領域		内容	Critical
version (X.509 証明書バージョン)		Version 3	-
serialNumber (証明書シリアル番号)		例) 123456789abcdef0	-
signatureAlgorithm (署名アルゴリズム)		以下のいずれかを設定 sha1WithRSAEncryption sha256WithRSAEncryption sha384WithRSAEncryption ecdsa-with-SHA256 ecdsa-with-SHA384	-
issuer (発行者)	countryName (国)	JP	-
	organizationName (組織)	以下のいずれかを設定 SECOM Trust Systems CO.,LTD. SECOM Trust Systems Co., Ltd. SECOM Trust Systems CO., LTD.	
	organizationalUnitName (組織単位)	本 CA の organizationalUnitName を設定可能	
	commonName (CN)	本 CA の commonName を設定	
validity (有効期限)	notBefore (有効性開始日時)	証明書署名以前の時刻で 1 日以内の値	-
	notAfter (有効性終了日時)	本 CP「6.3.2 私有鍵および公開鍵の有効期間」に規定	
subject (主体者)	countryName (国)	JP	-
	organizationName (組織)	以下のいずれかを設定 SECOM Trust Systems CO.,LTD. SECOM Trust Systems Co., Ltd. SECOM Trust Systems CO., LTD.	
	organizationalUnitName (組織単位)	本 CA の organizationalUnitName を設定可能	
	commonName (CN)	本 CA の commonName を設定	
subjectPublicKeyInfo (主体者公開鍵情報)		本 CP「6.1.5 鍵サイズ」に規定	-

拡張領域	内容	
subjectKeyIdentifier （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
keyUsage （鍵用途）	keyCertSign（証明書への署名） cRLSign（CRL への署名）	Y
basicConstraints（基本制約）	TRUE （CA である）	Y

利用者証明書のプロファイル

基本領域		内容	Critical
version（X.509 証明書バージョン）		Version 3	-
serialNumber （証明書シリアル番号）		例） 123456789abcdef0	-
signatureAlgorithm （署名アルゴリズム）		以下のいずれかを設定 sha1WithRSAEncryption sha256WithRSAEncryption sha384WithRSAEncryption ecdsa-with-SHA256 ecdsa-with-SHA384	-
issuer （発行者）	countryName（国）	JP	-
	organizationName（組織）	以下のいずれかを設定 SECOM Trust Systems CO.,LTD. SECOM Trust Systems Co., Ltd. SECOM Trust Systems CO., LTD.	
	organizationalUnitName （組織単位）	本 CA の organizationalUnitName を設定可能	
	commonName（CN）	本 CA の commonName を設定	
validity （有効期限）	notBefore （有効性開始日時）	証明書署名以前の時刻で 48 時間以内の値	-
	notAfter （有効性終了日時）	本 CP「6.3.2 私有鍵および公開鍵の有効期間」に規定	
subject （主体者）	countryName（国）	JP	-
	stateOrProvinceName (都道府県)	都道府県名 【オプション】	

	localityName （市区町村）	市区町村名 【オプション】	
	organizationName（組織）	組織名	
	organizationalUnitName （組織単位）	組織単位 【オプション】	
	organizationalUnitName （組織単位）	組織単位 【任意に指定可能】	
	organizationalUnitName （組織単位）	組織単位 【任意に指定可能】	
	commonName （主体者名）	利用者名	
	serialNumber（シリアル番号）	シリアル番号 【任意に指定可能】	
subjectKeyIdentifier （主体者公開鍵情報）		本 CP「6.1.5 鍵サイズ」に規定	-

拡張領域	内容	Critical
authorityKeyIdentifier （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
subjectKeyIdentifier （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
keyUsage（鍵用途）	以下のいずれかを設定 digitalSignature（デジタル署名）【オプション】 nonRepudiation（否認防止）【オプション】 keyEncipherment（鍵暗号化）【オプション・RSA 方式のみ】dataEncipherment（データ暗号化）【オプション・RSA 方式のみ】	Y
certificatePolicies （証明書ポリシ）	Policy: 1.2.392.200091.100.371.1 または 1.2.392.200091.100.371.2 CPS: https://repo1.secomtrust.net/spcpp/pfm20/ または http://repo1.secomtrust.net/spcpp/pfm20/	N
subjectAltName （主体者別名）	OtherName: UPN="ユーザプリンシパル名" 【オプション】 OtherName: "OID"="任意文字列" 【オプション】 Rfc822Name:"メールアドレス" 【オプション】	N

	dNSName:"サーバー名" 【オプション】	
extKeyUsage （拡張鍵用途）	id-kp-clientAuth（クライアント認証）【オプション】 id-kp-emailProtection（E-mail 保護）【オプション】 id-kp-serverAuth（サーバー認証）【オプション】 id-kp-timeStamping（タイムスタンプ）【オプション】 SmartCard Logon（スマートカードログオン）【オプション】 ＊SmartCard Logon 選択時は id-kp-clientAuth も同時選択	N
crlDistributionPoints （CRL 配布ポイント）	本 CA の CRL サービスの HTTP URL ldap://repo1.secomtrust.net/"IssuerDN"?certificateRevocationList【オプション】	N
authorityInformationAccess （機関情報アクセス）	accessMethod id-ad-ocsp（1.3.6.1.5.5.7.48.1） accessLocation OCSP レスポンダーの HTTP URL【オプション】 id-ad-caIssuers（1.3.6.1.5.5.7.48.2） accessLocation 本 CA 証明書の HTTP URL【オプション】	N
Netscape Certificate Type （Netscape 証明書タイプ）	SSL Client 【オプション】 S/MIME Client 【オプション】	N

※ 【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 組織毎に設定の有無を変えられる項目である。但し、セコムトラストシステムズが定める組み合わせでのみ設定可能とする。

7.1.1 バージョン番号

X.509 v3 を使用する。

7.1.2 証明書拡張

RFC 5280 に準拠した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。

アルゴリズム	オブジェクト識別子
rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 11}
sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 12}
id-ecPublicKey	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1 }
ecdsa-with-SHA256	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)}
ecdsa-with-SHA384	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)}

7.1.4 名前形式

本 CA では、RFC 5280 で定められた識別名を使用する。

すべての有効な認証パス（RFC 5280, Section 6 で定義）について認証パスの証明書ごとに、証明書発行者の識別名フィールドのエンコードされた内容は、発行される CA 証明書の主体者識別名フィールドのエンコードされた形式とバイト単位で同一とする。

7.1.5 名前制約

規定しない。

7.1.6 CP オブジェクト識別子

「1.2 文書名と識別」の OID に従う。

7.1.7 証明書プロファイルポリシー制約拡張の利用

規定しない。

7.1.8 ポリシ修飾子の文法および意味

証明書には RFC 5280 で規定されたポリシ修飾子を含めることができる。

7.1.9 重要な証明書ポリシ拡張の処理の意味

規定しない。

7.2 CRL 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	-
signatureAlgorithm（署名アルゴリズム）		以下のいずれかを設定 sha1WithRSAEncryption sha256WithRSAEncryption sha384WithRSAEncryption ecdsa-with-SHA256 ecdsa-with-SHA384	-
issuer （発行者）	countryName（国）	JP	-
	organizationName （組織）	以下のいずれかを設定 SECOM Trust Systems CO.,LTD. SECOM Trust Systems Co., Ltd. SECOM Trust Systems CO., LTD.	
	organizationalUnitName （組織単位）	本 CA の organizationalUnitName を設定可能	
	commonName（CN）	本 CA の commonName を設定	
thisUpdate（更新日時）		CRL が発行される日時。	-
nextUpdate（次回更新予定日時）		次の CRL が発行される日時。 thisUpdate から最大 10 日後。	
revokedCertificates （失効証明書）	serialNumber （失効証明書シリアル番号）	失効した証明書に含まれる serialNumber とバイト単位で同一の値	-
	revocationDate （失効日時）	失効が発生した日時	
	reasonCode （失効理由）	以下のいずれかを設定 unspecified（未定義） keyCompromise（鍵危殆化） affiliationChanged（内容変更） superseded（証明書更新による破棄） cessationOfOperation（運用停止） certificateHold（一時停止）	
フィールド（拡張領域）		内容	
CRLNumber （CRL 番号）		CRL 番号	N

authorityKeyIdentifier （発行者鍵識別子）	発行者公開鍵の 160 ビット SHA-1 ハッシュ値	N

7.2.1 バージョン番号

RFC 5280 に規定された X.509 v2 CRL を使用する

7.2.2 CRL 拡張

reasonCode (OID 2.5.29.21) 拡張は critical とマークしない。

CRL エントリー拡張は存在すべきだが、以下の要件に従って省略することができる。

CRLReason に unspecified (0)を含まない。

失効の理由が指定されていない場合、reasonCode エントリーの拡張を省略する。

7.3 OCSP プロファイル

基本領域		設定内容	Critical
version		Version 3	-
serialNumber		CSPRNG からの 64 ビット以上の出力を含む 1 以上かつ 2^{159} 未満の連番ではない値	-
signatureAlgorithm		以下のいずれかを設定 sha256WithRSAEncryption sha384WithRSAEncryption ecdsa-with-SHA256 ecdsa-with-SHA384	-
issuer	countryName	JP	-
	organizationName	本 CA の組織名	-
	commonName	本 CA の commonName を設定	-
validity	notBefore	証明書署名以前の時刻で 1 日以内の値	-
	notAfter	CPS「6.3.2 私有鍵および公開鍵の有効期間」に規定	-
subject	countryName	JP	-
	organizationName	本 CA の組織名	-
	commonName	OCSP レスポンダー名	-
subjectPublicKeyInfo		本 CP「6.1.5 鍵サイズ」に規定	-
拡張領域		設定内容	Critical
keyUsage		digitalSignature	Y
extKeyUsage		id-kp-OCSPSigning	N

id-pkix-ocsp-nocheck	NULL	N
certificatePolicies	禁止	N
authorityKeyIdentifier	発行者公開鍵の 160 ビット SHA-1 ハッシュ値	N
subjectKeyIdentifier	主体者公開鍵の 160 ビット SHA-1 ハッシュ値	N

7.3.1 バージョン番号

本 CA は、RFC 5019 および RFC 6960 に準拠する。

7.3.2 OCSP 拡張

OCSP 応答の singleExtensions には、reasonCode（OID 2.5.29.21）CRL エントリー拡張を含めない。

8. 準拠性監査と他の評価

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。本 CA が行う準拠性監査に関する諸事項については CPS に規定する。

8.1 監査の頻度

本項については、CPS に規定する。

8.2 監査人の身元／資格

本項については、CPS に規定する。

8.3 監査人と被監査部門の関係

本項については、CPS に規定する。

8.4 監査で扱われる事項

本項については、CPS に規定する。

8.5 不備の結果としてとられる処置

本項については、CPS に規定する。

8.6 監査結果の開示

本項については、CPS に規定する。

9. 他の業務上および法的事項

9.1 料金

本 CA が発行する証明書に関する料金については、別途規定する。

9.2 財務的責任

セコムトラストシステムズは、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。

9.3 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

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、セコムトラストシステムズに帰属する財産である。

- 本 CP　：　セコムトラストシステムズに帰属する財産（著作権を含む）である
- CPS　：　セコムトラストシステムズに帰属する財産（著作権を含む）である
- CRL　：　セコムトラストシステムズ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

9.6.1.1 IA の表明保証

セコムトラストシステムズは、IA 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 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
・ IA 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
・ リポジトリの維持管理を行うこと

9.6.1.2 RA の表明保証

セコムトラストシステムズは、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
・ 証明書発行時、実在性確認等の審査を的確に行うこと
・ IA への証明書発行・失効等の指示を正確かつすみやかに行うこと

9.6.2 利用者の表明保証

利用者は、次の義務を負うものとする。

・ 利用者は証明書の発行申請に際して、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セコムトラストシステムズまで通知すること。
・ 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 に従うこと。
・ 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、若しくは登録情報に変更があった場合、利用者はセコムトラストシステムズに証明書の失効をすみやかに申請すること。

9.6.3 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。
・ 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 により証明書の失効登録がされていないか確認を行うこと。
・ 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。

9.6.4 他の関係者の表明保証

規定しない。

9.7 無保証

セコムトラストシステムズは、本 CP「9.6.1 認証局の表明保証」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 CP「9.6.1 認証局の表明保証」の内容に関し、次の場合、セコムトラストシステムズは責任を負わないものとする。

- セコムトラストシステムズ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
- 利用者が自己の義務の履行を怠ったために生じた損害
- 利用者のシステムに起因して発生した一切の損害
- セコムトラストシステムズ、利用者のハードウェア、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
- セコムトラストシステムズの責に帰することのできない事由で証明書および CRL に公開された情報に起因する損害
- セコムトラストシステムズ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トラストシステムズがセコムパスポート for Member 2.0 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、セコムトラストシステムズと契約先との間で契

約が終了する場合、セコムトラストシステムズ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利用者、検証者、セコムトラストシステムズの契約先およびセコムトラストシステムズ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

セコムトラストシステムズは、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、セコムトラストシステムズ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

規定しない。

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、セコムトラストシステムズに対して訴訟、仲裁等を含む法的解決手段に訴えようとする場合は、セコムトラストシステムズ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

セコムトラストシステムズは、本サービスの提供にあたり、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

セコムトラストシステムズ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。

9.17 その他の条項

規定しない。