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

Version 4.00

2014 年 5 月 29 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 OID の追加 全体的に体裁の修正を実施
3.00	2013.11.27	Sha2 の追加に伴い、修正 ポリシ OID の追加 RootCA のリポジトリ情報を追加
4.00	2014.5.29	サーバ認証の利用用途追加に伴い、修正 ポリシ OID の追加

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（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 及び CPS は以下のリポジトリに公開している。

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 が発行する証明書の有効期間は、5 年以下とする。

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、及び CPS とを照らし合わせて評価し、本 CP、及び 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。

本 CP は、IETF が認証局運用のフレームワークとして提唱する RFC3647「Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework」に準拠している。

1.2 文書名と識別

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」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 及び参照する 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 (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 (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 (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 (署名アルゴリズム：Sha256)	1.2.392.200091.100.381.5
サーバ認証用証明書ポリシ (署名アルゴリズム：Sha1)	1.2.392.200091.100.381.6
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）及び 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である。

1.3.1.1 IA

IA は、本 CA の秘密鍵の管理、証明書の発行、取消、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主体である。電子認証基盤の上で運用される CA において、IA の運用はセコムが行う。

1.3.1.2 RA

RA は、LRA（Local Registration Authority）及び証明書利用者の審査並びに証明書の発行及び取消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。

1.3.2 LRA

LRA は、RA に代わり、証明書利用者の実在性確認及び本人性確認の審査並びに証明書

の発行及び取消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又は団体がその役割を担うことができる。

1.3.3 申請者

申請者とは、RA 又は LRA に対し、証明書の発行や取消に関する申込を行う個人、組織又は団体等をいう。

1.3.4 証明書利用者

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、組織又は団体等をいう。

1.3.5 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、組織又は団体等をいう。

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	証明書の用途
クライアント用証明書ポリシ	本CP及びLRA運用基準に基づき決定された方法によって、LRA により認証されたものに対し、以下の用途として証明書が発行される。 ・電子メールへの電子署名及び電子メールの暗号化 ・電子文書への電子署名及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
データ署名用証明書ポリシ	本 CP 及び別途セコムが定める約款等に基づき、セコムにより実在性が確認された組織又は団体等に対し、以下の用途として証明書が発行される。 ・電子文書への電子署名
サーバ認証用証明書ポリシ	本 CP 及び別途セコムが定める約款等に基づき、セコムにより実在性が確認された組織又は団体等に対し、以下の用途として証明書が発行される。 ・サーバ認証 ・通信経路でのデータ暗号化

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@ml.secom-sts.co.jp

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
法的又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
作成したソフトウェア等に対し、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。
ソフトウェア等の利用者は、この電子署名を検証することにより、ソフトウェア等の作成者、発行者、有効期限等の情報を得ることができ、また、プログラム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の決定等を行う意思決定組織。

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

A～Z

CA（Certification Authority）：認証局
証明書の発行・更新・取消、CA 私有鍵の生成・保護及び証明書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取消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。

IA（Issuing Authority）：発行局
CA の業務のうち、証明書の発行・更新・取消、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。

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。

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。

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。

2. 公開とリポジトリの責任

2.1 リポジトリ

セコム は、証明書利用者及び検証者が、24 時間 365 日 CRL、本 CP 及び CPS 等を参照できるようリポジトリを維持管理する。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 及び CPS
- 本 CA が発行する証明書に関するその他関連情報

2.3 公開の時期又は頻度

本 CP 及び 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

証明書利用者及び検証者は、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 SSL 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 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 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。

3.1.4 認識、認証及び商標の役割

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取消する権利を有する。

3.2 初回の本人確認

3.2.1 秘密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秘密鍵で署名されていることを確認する。または、本 CA 内において秘密鍵を生成し、その秘密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秘密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又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若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 又は組織、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)又はこれに相当する書類の提出を求める。

3.2.3 提出書類
LRA 又は組織、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 又は組織、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、提出された書類はすべて返却する。尚、申込書等を受領していた場合、セコムはこれを破棄する。

3.2.4 申請者及び証明書利用者の認証
申請者及び証明書利用者の審査は、LRA 運用基準に基づき、LRA によって決定された方法により行なわれる。
データ署名用証明書ポリシを含む証明書の発行に際しては、セコムによって、電話又は郵送等の手段を用いて申請者に対する申し込みの意思確認を行う。

3.2.5 権限の正当性確認
申請者の権限の正当性確認は、「3.2.4 申請者及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。

3.3 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
「3.2.4 申請者及び証明書利用者の認証」及び「3.2.5 権限の正当性確認」と同様とする。

3.3.2 証明書取消後の鍵更新時における本人性確認と認証
「3.2.4 申請者及び証明書利用者の認証」及び「3.2.5 権限の正当性確認」と同様とする。

3.4 取消申請時の本人性確認と認証
「3.2.4 申請者及び証明書利用者の認証」及び「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 又は組織、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。

4.2 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 又は組織、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 証明書申請の処理時間

本 CA は、証明書申請を受け付けた後、速やかに LRA、証明書利用者又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又はオフラインで LRA、証明書利用者又は申請者に配付する。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 又は証明書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 又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。

4.5 鍵ペア及び証明書の利用

4.5.1 証明書利用者の私有鍵及び証明書の利用

証明書利用者の私有鍵及び証明書の利用については、「1.4.1 適切な証明書の用途」に従う。証明書利用者は、「1.4.1 適切な証明書の用途」に記載された用途に対して、当該証明書及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及び証明書の利用

検証者は、証明書利用者の公開鍵及び証明書を使用し、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 及び 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 鍵更新を伴う証明書の更新

4.7.1 更新事由
鍵更新を伴う証明書の更新は、証明書の有効期限が満了する場合又は鍵の危殆化に伴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。

4.8 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、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、速やかに変更前の証明書の取消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。変更前の証明書の取消は、「4.9.3 取消申請手続」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 証明書の取消と一時停止

4.9.1 証明書取消事由
証明書利用者は、次の事由が発生した場合、速やか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
- 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又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取消すことができる。

- 証明書利用者が本 CP、CPS、関連する契約又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又は危殆化のおそれがあると判断した場合
- セコム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 証明書の取消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 取消申請手続
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取消申請を行う。
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取消申請を行う。
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取消申請を行う。

4.9.4 取消申請の猶予期間
証明書利用者は、証明書取消事由が発生してから速やかに取消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速やかに本 CA に対して取消申請を行わなければならない。

4.9.5 認証局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速やかに証明書の取消処理を行い、CRL へ当該証明書情報を反映させる。

4.9.6 取消確認の要求
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。
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
本 CA は、取消処理の有無にかかわらず、24 時間以内に CRL を発行する。証明書の取消処理が行われた場合は、即時に CRL を発行し、リポジトリに反映させる。

4.9.8 証明書失効リストの発行最大遅延時間
本 CA は、証明書の取消を行ってから、即時に CRL を発行し、リポジトリに公表する。

4.9.9 オンラインでの失効/ステータス確認の適用性
本 CA は、提供しない。

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
規定しない。

4.9.11 利用可能な取消情報の他の形式
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、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、当該証明書の取消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
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 登録の終了

LRA は本サービスの利用を終了する場合、発行した証明書の取消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及び実施

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及び実施

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 立地場所及び構造

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 電源及び空調

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、経験及び身分証明の要件
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 再教育の頻度及び要件
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及び順序
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及び監査報告書
- LRA 又は組織、団体等からの申請書類

5.5.2 アーカイブ保存期間
セコムは、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
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及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及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及び CRL の発行を行う。

5.7 危殆化及び災害からの復旧

5.7.1 事故及び危殆化時の手続
セコムは、事故及び危殆化が発生した場合に速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及び関連する業務を復旧できるよう、以下を含む事故及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、ソフトウェア又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、ソフトウェア又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、ソフトウェア又はデータを使用して、速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又は危殆化のおそれがあると判断した場合、及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速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、可能な限り速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 認証局又は登録局の終了
セコムが本 CA を終了する場合、事前に LRA 及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全ての証明書は、本 CA の終了以前に取消を行う。

6. 技術的セキュリティ管理

6.1 鍵ペアの生成及びインストール

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、又は本 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。又は、対面により、PIN 及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 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、RSA 方式で鍵長 2048 ビットとする。
証明書利用者の鍵ペアについては、RSA 方式で鍵長 1024 または 2048 ビットとする。

6.1.6 公開鍵のパラメータの生成及び品質検査

本 CA の公開鍵のパラメータの生成、及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 を設定可能とする。

6.2 私有鍵の保護及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及び管理

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又は暗号モジュールからの転送

本 CA の私有鍵の HSM への転送又は 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又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及び管理」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 の公開鍵及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 私有鍵及び公開鍵の有効期間
本 CA の私有鍵及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 5 年以下とする。

6.4 活性化データ

6.4.1 活性化データの生成及び設定
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. 証明書及び CRL のプロファイル

7.1 証明書プロファイル

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） 2007/10/01 00:00:00 GMT	-
	NotAfter （有効性終了日時）	例） 2017/10/01 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/SC Root1CRL.crl	N
Certificate Policies (証明書ポリシ)		Policy: 1.2.392.200091.100.901.1 CPS:	N

	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

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.net	
	Organizational Unit （組織単位）	OU= Security Communication RootCA2	
Validity （有効期限）	NotBefore （有効性開始日時）	例） 2007/10/01 00:00:00 GMT	-
	NotAfter （有効性終了日時）	例） 2017/10/01 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-Root2/SC Root2CRL.crl	N
Certificate Policies（証明書ポリシ）		Policy: 1.2.392.200091.100.901.4	N

	CPS: https://repository.secomtrust.net/SC-Root2/	
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

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 2006 GMT	-
	NotAfter （有効性終了日時）	例） Feb 10 10:25:27 2007 GMT ＊有効期間 5 年以下	
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="企業名"	
	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 Numbewr （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）	digitalSignature（ディジタル署名）【オプション】 Non Repudiation（否認防止）【オプション】 keyEncipherment（鍵暗号化）【オプション】 dataEncipherment（データ暗号化）【オプション】	Y
Certificate Policies （証明書ポリシ）	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）	OtherName: UPN="ユーザプリンシパル名" 【任意に指定可能】 OtherName: "OID"="任意文字列" 【任意に指定可能】 Rfc822Name:"メールアドレス" 【任意に指定可能】 dNSName:"サーバ名" 【任意に指定可能】	N
Extended Key Usage （拡張鍵用途）	clientAuth（クライアント認証）【オプション】 serverAuth（サーバ認証）【オプション】 emailProtection（E-mail 保護）【オプション】 SmartCard Logon（スマートカードログオン）【オプション】 codeSigning（コードサイニング） ＊SmartCard Logon 選択時は、clientAuth も同時選択 ＊codeSigning は、本 CA が提供するアプリケーションのみに限定	N
CRL Distribution Points （CRL 配布ポイント）	http://repo1.secomtrust.net/spcpp/pfm20pub/ca"数字"/fullCRL.crl *"数字"の値は任意 ldap://repo1.secomtrust.net/"IssuerDN"?certificateRe	N

	vocationList	
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】 codeSigning ＊codeSigning は、本 CA が提供するアプリケーションのみに限定	N

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）	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 2006 GMT	-
	NotAfter （有効性終了日時）	例）　Feb 10 10:25:27 2007 GMT ＊有効期間 5 年以下	
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="企業名"	
	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 Numbewr （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）	digitalSignature（ディジタル署名）【オプション】 Non Repudiation（否認防止）【オプション】 keyEncipherment（鍵暗号化）【オプション】 dataEncipherment（データ暗号化）【オプション】	Y
Certificate Policies （証明書ポリシ）	Policy: 1.2.392.200091.100.381.4 Policy: 1.2.392.200091.100.381.5 CPS: https://repo1.secomtrust.net/spcpp/pfm20pub/	N
Subject Alt Name （主体者別名）	OtherName: UPN="ユーザプリンシパル名" 【任意に指定可能】 OtherName: "OID"="任意文字列" 【任意に指定可能】 Rfc822Name:"メールアドレス" 【任意に指定可能】	N
Extended Key Usage （拡張鍵用途）	clientAuth（クライアント認証）【オプション】 emailProtection（E-mail 保護）【オプション】 SmartCard Logon（スマートカードログオン）【オプション】 codeSigning（コードサイニング） ＊SmartCard Logon 選択時は、clientAuth も同時選択 ＊codeSigning は、本 CA が提供するアプリケーションのみに限定	N
CRL Distribution Points （CRL 配布ポイント）	http://repo1.secomtrust.net/spcpp/pfm20pub/ca"数字"/fullCRL.crl *"数字"の値は任意 ldap://repo1.secomtrust.net/"IssuerDN"?certificateRevocationList	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】 codeSigning ＊codeSigning は、本 CA が提供するアプリケーションのみに限定	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 毎に設定の有無を変えられる項目である。但し、セコムが定める組み合わせでのみ設定可能とする。

7.2 CRL プロファイル

7.2.1 CRL(sha1)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 2007 GMT	-
Next Update（次回更新予定日時）		例） Oct 5 00:00:00 2007 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） 2005/09/01 12:00:00 GMT	
	Reason Code （失効理由）	unspecified(未定義) Key Compromise(鍵危殆化) Affiliation Changed(内容変更) superseded(証明書更新による破棄) cessation of operation(運用停止) certificate hold(一時停止)	
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

7.2.2 CRL(sha256)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	Country （国）	C=JP	-

（発行者）	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 2007 GMT	-
Next Update（次回更新予定日時）		例） Oct 5 00:00:00 2007 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） 2005/09/01 12:00:00 GMT	
	Reason Code （失効理由）	unspecified(未定義) Key Compromise(鍵危殆化) Affiliation Changed(内容変更) superseded(証明書更新による破棄) cessation of operation(運用停止) certificate hold(一時停止)	
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

8. 準拠性監査と他の評価

本 CA は、本 CP 及び 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. 他の業務上及び法的事項

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

9.6.1.1 IA の表明保証

セコムは、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 及び申請者からの申請に基づいた証明書の正確な発行、取消及び管理を行うこと
・ 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 及び組織、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

9.6.2 LRA の表明保証
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
・ 申請者及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・取消等の申請を正確かつ速やかに行うこと

9.6.3 申請者の表明保証
申請者は、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 又は LRA に正確かつ完全な情報を提供すること

9.6.4 証明書利用者の表明保証
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 又は 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、その旨を速やかに本 CA 又は 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 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、又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、証明書利用者は本 CA 又は LRA に証明書の取消を速やかに申請すること

9.6.5 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 により証明書の取消登録が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

9.6.6 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」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 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、不正使用又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
・ 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
・ セコム、証明書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
・ セコムの責に帰することのできない事由で証明書及び CRL 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、セコムの契約先及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、証明書利用者及び検証者に対する必要な通知をホームページ、電子メール又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 通知方法及び期間
本 CP を変更した場合、変更した本 CP を速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。

9.14 準拠法

本 CP、CPS の解釈、有効性及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、暗号ハードウェア及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、証明書利用者又は検証者の義務等を本 CP、及び 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、及び CPS におい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。

9.16.3 分離条項

本 CP、及び 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。