セコムあんしんログインサービス認証局
証明書ポリシ
(Certificate Policy)

Version 1.00

2012 年 12 月 19 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	2012.12.19	新規作成

目次

1. はじめに

1.1 概要

セコムあんしんログインサービス認証局 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）が運用するセコムあんしんログインサービス 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 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が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 とを照らし合わせができるよう、リポジトリに本 CP、及び CPS を公開する。
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、「セコムあんしんログインサービス認証局 証明書ポリシ」という。
本 CP には、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 の OID 及び参照する CPS の OID は、次のとおりである。

CP/CPS	OID
セコムあんしんログインサービス認証局 証明書ポリシ	1.2.392.200091.100.391.1
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。
本サービスにおいては、本サービス契約先の組織が RA 業務の一部を担い、証明書利用者の管理業務等を行う。

1.3.2 証明書利用者

証明書利用者は、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、ウェブサイトへのアクセス時の認証、電子データへの署名、電子メールの暗号化やデジタル署名等に利用される。

1.4.2 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。

1.4.3 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 ： anshinlogin@secom.co.jp

1.4.4 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。

1.4.5 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。

1.5 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。

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
セコムトラストシステムズ情報セキュリティポリシの決定機関のことをいう。

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・失効、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。

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。

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。

SHA-1（Secure Hash Algorithm 1）
電子署名に使われる ハッシュ関数（要約関数）のひとつである。ハッシュ関数とは、与えられた原文から固定長のビット列を生成する演算手法をいう。
データの送信側と受信側でハッシュ値を比較することで、通信途中で原文が改ざんされていないかを検出することができる。

2. 公開とリポジトリの責任

2.1 リポジトリ

セコムトラストシステムズ は、証明書利用者が CRL 情報に 24 時間 365 日利用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

セコムトラストシステムズ 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 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）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 認識、認証及び商標の役割

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。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。セコムトラストシステムズは、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、セコムトラストシステムズは紛争を理由に証明書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 初回のサービス契約先組織の審査

3.2.1 本サービス契約先組織の実在確認と証明書利用者の管理業務等を行う者の在籍確認

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又はそのデータベースにより本サービス契約先の組織の実在確認を行う。証明書利用者の管理業務等を行う者の在籍確認は、本サービス契約先の組織が提出する書類をもって行う。

3.2.2 提出書類

本サービス契約先の組織がセコムトラストシステムズへ提出する書類は、別途セコムトラストシステムズが必要とする書類を提出するものとする。

(注) 審査の結果により、セコムトラストシステムズが本サービス契約先の組織として認定不可とした場合、本サービス契約先の組織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 証明書利用者へのサービスの利用意思確認

証明書利用者へのサービスの利用意思確認は、事前に本サービス契約先の組織によって決定された方法により行なわれる。

3.2.4 権限の正当性確認

セコムトラストシステムズは、証明書利用者の管理業務等を行う者が、その管理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 本サービス契約先組織の実在確認と証明書利用者の管理業務等を行う者の在籍確認」により確認する。

3.3 鍵更新申請時の審査

3.3.1 通常の鍵更新時における審査

鍵更新時における証明書利用者の審査は、「3.2 初回のサービス契約先組織の審査」と同様とする。

3.3.2 証明書失効後の鍵更新時における審査

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、証明書利用者の審査は、「3.2 初回のサービス契約先組織の審査」と同様とする。

3.4 失効申請時の審査

証明書利用者の審査は、本サービス契約先の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
規定しない。

4.2 証明書申請手続

4.2.1 本人性確認と認証の実施
規定しない。

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、速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 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本サービス契約先の組織又は証明書利用者に配付する。
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
規定しない。

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用途

4.5.1 証明書利用者の私有鍵及び証明書の用途
ウェブサイトへのアクセス時の認証、電子データへの署名、電子メールの暗号化やデジタル署名等に利用される。

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
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、その証明書の失効及び新規発行とする。

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 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。

4.8.5 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

4.9.1 証明書失効事由
本サービス契約先の組織及び証明書利用者は、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速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、本サービス契約先の組織内において、本サービスの管理者権限を有する者及び証明書利用者が行う。

4.9.3 失効申請手続
本サービス契約先の組織内において、本サービスの管理者権限者を有する者及び証明書利者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
本サービスの管理者権限者を有する者及び証明書利用者は、秘密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には、速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、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
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。

4.10 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 加入（登録）の終了
本サービス契約先の組織、及び証明書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
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」の本 CA に関連する監査ログ、作業記録等を定期的にアーカイブとして作成、保管する。

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 10 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、取消又は CRL の発行等、本 CA 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）を使用して本 CA に関連するシステムの時刻同期を行い、本 CA 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、本 CA 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。

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

セコムトラストシステムズは、事故及び危殆化が発生した場合に速やかに本 CA 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

セコムトラストシステムズは、本 CA 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、速やかに本 CA 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、及び災害等により本 CA 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速やかに復旧作業を実施できるよう、予め本 CA 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

セコムトラストシステムズが本 CA を終了する場合、事前に本サービス契約先の組織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 と私有鍵を異なる経路で送付する。

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 2048 ビットを推奨とする。

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のパラメータの生成及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 が発行する証明書利用者の証明書の KeyUsage には、digitalSignature、

keyEncipherment を設定可能とする。但し、KeyUsage の設定はそれだけに限定はしない。

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の活性化、非活性化、バックアップ等の操作は、証明書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、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のバックアップは、証明書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。
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

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。バックアップ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
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及び管理」のとおりである。
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 の公開鍵については CPS「6.2.1 暗号モジュールの標準及び管理」のとおりである。
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 Systems CO.,LTD.	
	Organizational Unit （組織単位）	OU=SECOM Anshin Login Service	
	Common Name (CN)	CN=SECOM Anshin Login CA"数字" *"数字"の値は任意	
Validity （有効期限）	NotBefore （有効性開始日時）	例） 2012/12/01 00:00:00 GMT	-
	NotAfter （有効性終了日時）	例） 2032/12/01 00:00:00 GMT ＊20 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 Anshin Login Service	
	Common Name (CN)	CN=SECOM Anshin Login 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	critical
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）		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 証明書利用者の証明書のプロファイル

証明書フィールド（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 Anshin Login Service	
	Common Name (CN)	CN=SECOM Anshin Login CA"数字" *"数字"の値は任意	
Validity （有効期限）	NotBefore （有効性開始日時）	例） Dec 10 09:55:27 2012 GMT	-
	NotAfter （有効性終了日時）	例） Dec 10 10:25:27 2013 GMT ＊有効期間 5 年以下	
Subject （主体者）	Country （国）	C=JP	-
	Organization （組織）	O=SECOM Anshin Login CA"数字" *"数字"の値は任意	
	Organizational Unit （組織単位）	OU="任意の値" ＊契約先を識別するための ID	
	Common Name （主体者名）	CN="任意の値" ＊証明書利用者証明書を識別するための ID	
Subject PublicKey Info （主体者公開鍵情報）		主体者の公開鍵データ	-

証明書フィールド（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】 keyEncipherment（鍵暗号化）【オプション】 Non Repudiation（否認防止）【オプション】 dateEncipherment（データ暗号化）【オプション】	Y
Certificate Policies （証明書ポリシ）	Policy: 1.2.392.200091.100.371.1 CPS: https://repo1.secomtrust.net/spcpp/al/	N
Subject Alt Name （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
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】 *SmartCard Login 選択時は clientAuth も同時選択	N
CRL Distribution Points （CRL 配布ポイント）	http://repo1.secomtrust.net/spcpp/al/ca"数字"/fullcrl.crl *"数字"の値は任意	N

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	-
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 Anshin Login Service	
	Common Name（CN）	CN=SECOM Anshin Login CA"数字" *"数字"の値は任意	
This Update（更新日時）		例） Dec 1 00:00:00 2012 GMT	-
Next Update（次回更新予定日時）		例） Dec 5 00:00:00 2012 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） 2012/12/01 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	critical
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
・ 証明書の正確な発行、失効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
・ 本サービス契約に関する書類の授受を的確に行うこと
・ IA への証明書発行・失効等の指示を正確かつ速やかに行うこと

9.6.2 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。
・ 危殆化から自身の私有鍵を保護すること。
・ 証明書利用者が、証明書に記載の公開鍵に対応する私有鍵が危殆化した、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、証明書利用者は本サービス契約先の組織内において、本サービスの管理者権限者を有する者に証明書の失効を速やかに申請する、または証明書利用者が証明書の失効を行うこと。

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。
・ 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 により証明書の失効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。

9.6.4 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
- セコムトラストシステムズ、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及び CRL に公開された情報に起因する損害
- セコムトラスト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 有効期間と終了

9.9.1 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。

9.9.2 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あんしんログインサービス認証局 を終了した時点で無効となる。

9.9.3 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証明書利用者、検証者、セコムトラストシステムズの契約先及びセコムトラストシステムズに適用されるものとする。

9.10 証明書利用者及び検証者への通知や連絡の方法

セコムトラストシステムズから証明書利用者及び検証者への通知は、電子メール、書面またはホームページに掲載する等、セコムトラストシステムズが適当と判断する方法により行う。セコムトラストシステムズから証明書利用者及び検証者への連絡は、電話、電子メール等、セコムトラストシステムズが適当と判断する方法により行う。

9.11 改訂

9.11.1 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。

9.11.2 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。

9.11.3 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。

9.12 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。仲裁及び裁判地は東京都区内における紛争処理機関を専属的管轄とする。

9.13 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。

9.14 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。

9.15 雑則

9.15.1 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、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。

9.15.2 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、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。

9.15.3 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。

9.15.4 強制執行条項

規定しない。

9.16 その他の条項

規定しない。