SECOM TimeStamping CA

タイムスタンプサービス用証明書ポリシ

2018 年 5 月 23 日
Version 4.00

セコムトラストシステムズ株式会社

改版履歴		
版数	日付	内容
V1.00	2011.6.27	初版発行
V2.00	2016.3.28	メジャーバージョンアップ SECOM TimeStamping CA1 タイムスタンプサービス用証明書ポリシを SECOM TimeStamping CA タイムスタンプサービス用証明書ポリシとし、CA の私有鍵 SECOM TimeStamping CA2 を追加する
V3.00	2017.1.20	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
V4.00	2018.5.23	CA の私有鍵 SECOM TimeStamping CA3 を追加 TA（Time Authority）用証明書について記載を追加 全体的に文言の修正を実施

目次

1. はじめに

1.1 概要

SECOM TimeStamping CA タイムスタンプサービス用証明書ポリシ（Certificate Policy：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 SECOM TimeStamping CA1、SECOM TimeStamping CA 2 および SECOM TimeStamping CA 3（以下、「本 CA」という）が発行する TSA（Time Stamping Authority）用証明書および TA（Time Authority）用証明書（以下、「証明書」という）の利用目的、適用範囲、加入者手続を示し、証明書に関するポリシを規定するものである。なお本 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（Certification Practice Statement：以下、「CPS」という）に規定する。

本 CA は、Security Communication RootCA（Security Communication RootCA1、Security Communication RootCA2 および Security Communication RootCA3）により、片方向相互認証証明書の発行を受けており、Security Communication RootCA が定める運用基準に従い運用されている。

セコムは、認証局として本 CA の鍵管理、加入者*1 に対する証明書発行、取消等の認証サービス（以下、「本サービス」という）を提供する。本 CA が発行する証明書は、発行対象とその公開鍵が一意に関連づけられることを証明する。本サービスの加入者は、本 CP および CPS の内容を加入者自身の利用目的に照らして評価し承諾する必要がある。また、利用者*2 は、本 CP および CPS の内容を利用者自身の利用目的に照らして評価する必要がある。

なお、本 CP の内容が CPS の内容に抵触する場合は、本 CP が優先して適用されるものとする。また、セコムと加入者との間で別途契約書等が存在する場合、本 CP および CPS より契約書等の文書が優先される。

*1：加入者とは、セコムが運用する本 CA の私有鍵により署名される証明書の発行を受ける組織または団体をいう。
*2：利用者とは、本サービスで発行される証明書を信頼して利用する者をいい、署名検証者と同義である。

本 CP は、認証業務に関する技術面、サービス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。

1.2 文書の名前と識別

本 CP の正式名称は「SECOM TimeStamping CA タイムスタンプサービス用証明書ポリシ」という。本サービスの運営母体であるセコムには、表「1.2-1 OID（セコム）」に示す

ISO によって割り振られたオブジェクト識別子（Object ID：OID）を使用する。

表 1.2-1 OID（セコム）

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

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

表 1.2-2 OID（本 CP）

CP	OID
SECOM TimeStamping CA1（sha1）	1.2.392.200091.100.931.1
SECOM TimeStamping CA2（sha256）	
SECOM TimeStamping CA3（sha384）	1.2.392.200091.100.931.3

本 CP に関連する CPS の OID を表「1.2-3 OID（CPS)」に示す。

表 1.2-3 OID（CPS）

CPS	OID
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 CA

CAは、証明書の発行、取消、取消情報の開示、OCSP（Online Certificate Status Protocol）サーバーによる証明書ステータス情報の提供および保管等の各業務を行う。

1.3.2 RA

RA は、証明書申請者となる組織、団体からの証明書発行、取消等の要求に対して、組織、団体の実在性確認、本人性確認の審査を行う。

1.3.3 加入者

加入者とは、自ら鍵ペアを生成し、本 CA から証明書の発行を受ける組織または団体をいう。本 CA に証明書の発行申請を行い、本 CA から発行された証明書を受容した時点で加入者となる。

1.3.4 利用者

利用者とは、本 CA が発行した証明書を信頼して利用する者をいう。利用者は、本 CP お

よびCPSの内容を利用者自身の利用目的に照らして確認および同意したうえで利用しているとみなされる。

1.4 証明書の使用方法

本CAはTAおよびTSAの上位認証局として機能するCAであり、加入者証明書としてTA、TSA向けの証明書を発行する。証明書を信頼して利用する利用者は、当該証明書の信頼性を本CAおよびSecurity Communication RootCAの公開鍵証明書によって検証することができる。

1.5 ポリシ管理

1.5.1 CP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に関する問い合わせ窓口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 CPのポリシ適合性を決定する者

本CPが、本CAのポリシとして適切か否かの判断は、セコムの認証サービス改善委員会が行う。

1.5.4 CP承認手続

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

2. 公表とリポジトリーの責任

2.1 リポジトリー

本CAは、加入者および利用者がCRL情報にアクセスできるようリポジトリーを維持管理する。また、加入者および利用者がオンラインでの証明書ステータス情報を24 時間365 日利用できるようにOCSP サーバーを維持管理する。リポジトリーへのアクセスに用いるプロトコルは、HTTP（HyperText 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）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。

2.2 証明書情報の公開

本 CA は、次の内容をリポジトリーに格納し、加入者および利用者がオンラインによって閲覧できるようにする。

- 本 CP に基づくすべての失効情報を含む証明書失効リスト（以下、「CRL」という）
- 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 サーバーにより加入者および利用者がオンラインによって証明書ステータス情報を閲覧できるようにする。

2.3 公開の時期および頻度

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すべての失効情報を含み、発行の都度、リポジトリーに公表される。

2.4 リポジトリーへのアクセスコントロール

加入者および利用者は、随時、リポジトリーを参照できる。ただし、保守等により、一時的にリポジトリーを利用できない場合もある。

3. 識別と認証

3.1 名前

3.1.1 名前の種類

証明書の発行者の名前と発行対象である加入者の名前は、X.500 の識別名（DN：Distinguished Name） 形式に従い、かつ本 CP「7.1.4 名前形式」に則って設定する。

3.1.2 意味のある名前の必要性

加入者の識別名は、意味のある名前を用いる。証明書に記載される主体者名は、組織または団体に適切な範囲で関連したものでなければならない。

加入者は、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。

3.1.3 加入者の匿名性または仮名性

証明書に記載される主体者名に匿名や仮名は使用しない。

3.1.4 さまざまな名前の形式を解釈するための規則

DN は、本 CP「3.1.1 名前の種類」および「3.1.2 意味のある名前の必要性」で定義しているとおりに解釈する。

3.1.5 名前の一意性

証明書に記載される主体者名は、本 CA の発行したすべての証明書 において一意とする。

3.1.6 認識、認証および商標の役割

商標使用の権利については、商標所持者に権利が留保されるものとする。本 CA は、必要に応じて、商標所持者に対し、商標に関する出願等の公的書類の提示を求めることがある。

3.2 初回の識別と認証

3.2.1 私有鍵の所有を証明する方法

本 CA は、証明書申請者 から提出された証明書発行要求（Certificate Signing Request ：以下、「CSR」という）の署名の検証を行い、それに含まれている 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、CSR のフィンガープリントを確認し、 公開鍵の所有者を特定する。

3.2.2 組織または団体の認証

証明書申請者は、証明書の発行申請時に、本 CA に以下の情報を提供しなければならない。

- 証明書発行申請書
- 組織もしくは団体が実在していることを証明する情報

・ CSR
・ その他、セコムが必要とする書類

本 CA は、以上の情報を用いて申請に誤りや欠落情報がないことを確認する。

3.2.3 個人の認証

本 CA は、個人に対して証明書の発行は行わない。

3.2.4 権限の正当性確認

本 CA は、証明書申請者となる組織または団体の代表者、社員または代理人が、その組織または団体に関する情報の申請を行うための正当な権限を有していることを確認する。

3.3 鍵更新申請時の識別と認証

3.3.1 通常の私有鍵更新に伴う証明書申請時の識別と認証

本 CP「3.2 初回の識別と認証」と同様の手続による。

3.3.2 証明書取消後の私有鍵更新に伴う証明書申請時の識別と認証

本 CP「3.2 初回の識別と認証」と同様の手続による。

3.4 取消申請時の識別と認証

本 CA は、証明書の取消申請を受け付けた場合、提出された加入者の情報をもとに、適正な要求であることを確認する。

4. 証明書のライフサイクルに対する運用要件

4.1 証明書申請

4.1.1 証明書申請を行うことができる者

証明書の発行申請は、発行申請を行う組織または団体の代表者、社員または代理人が行うことができる。

4.1.2 登録手続および責任

証明書申請者は、本 CA より事前に周知された手続に従い、証明書の申請を行う。

証明書申請者は、証明書の発行申請を行うにあたり、本 CP、CPS、その他本 CA より開示された文書の内容を承諾しているものとする。

証明書申請者は､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 識別と認証の手続

本 CA は、証明書申請者からの発行申請に対し、受領した申請書類および CSR の真正性を、「3.2 初回の識別と認証」に基づき確認する。

4.2.2 証明書申請の受理または却下

本 CA は､証明書申請者からの申請に対し予め定められた審査手続に従い､証明書の発行申請の諾否を決定し、その結果を証明書申請者に通知する。

4.2.3 証明書申請の処理時間

本 CA は、証明書申請者からの発行申請を承諾した場合、すみやかに証明書を発行する。

4.3 証明書発行

4.3.1 証明書の発行時における CA の処理手続

本 CA は、証明書申請者から提出された CSR の公開鍵に対し、本 CP「7.1 証明書プロファイル」に準じた内容で、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 加入者に対する証明書発行通知

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､発行した証明書を外部記憶媒体に保管し、受領書とともに封緘したうえで、証明書申請者との間で手交するかまたは郵送により証明書申請者宛に送付する。

4.4 証明書の受領確認

4.4.1 証明書の受領確認手続

証明書申請者は、証明書の内容を確認し、問題が無いと判断した時点で、本 CA に対し受領書を送付しなければならない。本 CA は、受領書を受領した時点で証明書の受け入れの完了とする。なお、証明書の内容に誤りがあった場合、証明書申請者は遅滞なくその旨を本 CA に連絡しなければならない。証明書の内容に関する申し立ては、証明書の送付日より 14 日以内に行わなければならない。

4.4.2 証明書の公開

本 CA が発行した TA および TSA 証明書は、必要に応じてリポジトリー上で公開する。

4.4.3 他のエンティティに対する CA の証明書発行通知

本 CA は、他のエンティティに対して証明書の発行通知を行わない。

4.5 鍵ペアと証明書の用途

4.5.1 加入者の私有鍵および証明書の用途

本 CA が発行する証明書および加入者が所持する私有鍵の用途は、セコムが提供しているサービスや、セコムと契約関係にある本 CA の加入者が提供しているサービスまたは製品に定めている用途に制限されている。本 CA が発行する証明書を、その他の用途に使用してはならない。

4.5.2 利用者の公開鍵および証明書の用途

利用者は、本 CP および CPS の内容について理解し、承諾したうえで本 CA の証明書を使用し、本 CA が発行した証明書の信頼性を検証しなければならない。

4.6 証明書の更新

本 CA は、加入者の鍵ペアの更新をともなわない証明書更新を認めない。証明書を更新する場合は、新たな鍵ペアを生成することとし、本 CP「4.7 証明書の鍵更新」に定める手続に従う。

4.7 鍵更新を伴う証明書の更新

4.7.1 鍵更新を伴う証明書の更新事由

鍵更新を伴う証明書の更新は、証明書の有効期間が満了する場合または鍵の危殆化にともない証明書の取消を行った場合等に行われる。

4.7.2 新しい公開鍵の証明書申請を行うことができる者

本 CP「4.1.1 証明書申請を行うことができる者」と同様とする。

4.7.3 鍵更新を伴う証明書更新申請の処理手続
本 CP「4.2 証明書申請手続」と同様とする。

4.7.4 加入者に対する新しい証明書の通知
本 CP「4.3.2 加入者に対する証明書発行通知」と同様とする。

4.7.5 鍵更新にともない発行された証明書の受領確認手続
本 CP「4.4.1 証明書の受領確認手続」と同様とする。

4.7.6 鍵更新済みの証明書の公開
本 CP「4.4.2 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 CA の証明書発行通知
本 CP「4.4.3 他のエンティティに対する CA の証明書発行通知」と同様とする。

4.8 証明書の変更

4.8.1 証明書を変更する場合
証明書の記載事項に変更が生じた場合、加入者は本 CA に対しすみやかに変更に関する申請を行わなければならない。変更に伴う証明書の再発行手続は、証明書の取消および初回発行時の手続をもって行われる。

4.8.2 証明書の変更申請をすることができる者
本 CP「4.9.2 証明書取消を申請することができる者」および「4.1.1 証明書申請を行うことができる者」と同様とする。

4.8.3 証明書の変更申請の処理手続
本 CP「4.9.3 取消申請手続」および「4.2 証明書申請手続」と同様とする。

4.8.4 加入者に対する新しい証明書の発行通知
本 CP「4.3.2 加入者に対する証明書発行通知」と同様とする。

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

4.8.6 変更された証明書の公開
本 CP「4.4.2 証明書の公開」と同様とする。

4.8.7 利用者に対する証明書の発行通知

本 CP「4.4.3 利用者に対する証明書発行通知」と同様とする。

4.9 証明書の取消および一時停止

4.9.1 証明書取消事由

加入者は、自らの判断に基づいて証明書の取消申請を行うことができる。ただし、次の事由が発生した場合、加入者は、本 CA 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
- 私有鍵が盗難、紛失、漏洩、不正利用等により証明書の信頼性を喪失した可能性がある場合
- 私有鍵が危殆化し機密性が失われた場合またはその可能性がある場合
- 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、本 CA は、次の事由に該当すると判断した場合、加入者からの取消申請の有無に関わらず、証明書の取消ができるものとする。

- 加入者が本 CP および CPS、契約、法律に基づく義務を履行していない場合
- セコムが、本サービスを終了する場合
- 本 CA の私有鍵が危殆化したまたはそのおそれがあると判断された場合
- 本 CA 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 証明書取消を申請することができる者

証明書の取消申請は、取消申請を行う組織または団体の代表者、社員または代理人が行うことができる。

4.9.3 取消申請手続

証明書の取消申請手続は､本 CA に対し証明書取消に関する必要な情報を郵送することで行われる。ただし、緊急を要する場合や上記の方法による要求ができない場合、代替策として、電子メールによる申請も可能である。

4.9.4 取消申請の猶予期間

私有鍵が危殆化した場合を除く取消申請は、取消を希望する 5 営業日前までに、本 CA に行わなければならない。ただし、私有鍵が危殆化したまたはそのおそれがある場合は、当該問題を発見後、すみやかに取消申請を行わなければならない。

4.9.5 CA の取消申請処理の許容時間

本 CA は、有効な取消申請を受け付けてから 1 営業日以内に証明書の取消を実行する。

4.9.6 利用者の取消確認要求

利用者は、本 CA により発行された証明書を信頼し、利用する前に、CRL または OCSP サーバーを確認することにより証明書が取消されていないことを確認しなければならない。

4.9.7 証明書取消リストの発行頻度

CRL は、前回の発行から 1 年以内に新たな CRL が発行される。また、証明書の発行および取消を行った場合にも新たな CRL が発行される。

4.9.8 証明書取消リストの発行の最大遅延時間

CRL は、証明書の発行および取消を行ってから、1 営業日以内に新たな CRL を発行し、リポジトリーに公開する。

また、本 CA は CRL とともに取消理由を示す情報をリポジトリーに公開する。

4.9.9 オンラインでの失効/ステータス確認の適用性

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。

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

利用者は、本 CA により発行された証明書を信頼し、利用する前に、証明書の有効性を確認しなければならない。リポジトリーに掲載している 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 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

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

本 CA は、証明書の一時停止を行わない。

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

加入者および利用者は OCSP サーバーを通じて証明書ステータス情報を確認することができる。

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 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 加入（登録）の終了

証明書加入者は本サービスの利用を終了する場合、契約書等に定めたサービスの利用終了手続きを必要とする。

4.12 キーエスクローと鍵回復

本 CA が、CA 私有鍵を第三者に預託することはない。

5. 物理的、手続上、人事上のセキュリティ管理

5.1 物理的管理
CPS に規定する。

5.2 手続上の管理
CPS に規定する。

5.3 人事上のセキュリティ管理
CPS に規定する。

5.4 セキュリティ監査の手順
CPS に規定する。

5.5 記録の保管
CPS に規定する。

5.6 鍵の切り替え
本 CA の私有鍵の有効期間が満了した時点で、新しい私有鍵が生成され、その後は、新しい私有鍵を使って証明書および CRL が発行される。

5.7 信頼性喪失や災害からの復旧
CPS に規定する。

5.8 認証業務の終了
セコムが本サービスを終了する場合、サービス終了の 3 か月前までに加入者その他の関係者にその旨を通知する。本 CA によって発行されたすべての証明書は、本サービスの終了以前に失効される。

6. 技術的セキュリティ管理

6.1 鍵ペアの生成とインストール

6.1.1 鍵ペア生成

CPS に規定する。

6.1.2 加入者への私有鍵の送付

加入者の鍵ペアは、加入者自身で生成するため、私有鍵は加入者のみが所持する。

6.1.3 CA への公開鍵の送付

加入者の公開鍵は、CP「3.2.1 私有鍵の所有を証明する方法」に定める手続により検証され、その受渡しは手交または郵送で行う。

6.1.4 利用者への CA 公開鍵の送付

利用者は、本 CA のリポジトリーにアクセスするか、または一般的に使用される Web ブラウザを通して本 CA の公開鍵を入手することができる。

6.1.5 鍵長

CA の鍵ペアの電子署名方式を以下の表に示す。

表 6.1-1 電子署名方式

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

6.1.6 公開鍵のパラメータの生成および品質検査

CPS に規定する。

6.1.7 鍵利用目的

CA 私有鍵は、原則として、加入者に対して発行する証明書および CRL への署名に使用する。

6.2 CA 私有鍵の保護

CPS に規定する。

6.3 鍵ペア管理のその他の側面

CPS に規定する。

6.4 活性化データ

CPS に規定する。

6.5 コンピュータのセキュリティ管理

CPS に規定する。

6.6 セキュリティ技術のライフサイクル管理

CPS に規定する。

6.7 ネットワークセキュリティ管理

CPS に規定する。

7. 証明書および CRL のプロファイル

7.1 証明書のプロファイル

本 CA が発行する証明書は、X.509 フォーマット証明書形式により作成される。

表「7.1-1 基本証明書領域」に示すフィールドを用いる。

表 7.1-1 証明書基本領域

フィールド	説明
Version （バージョン番号）	証明書フォーマットの番号*1
SerialNumber （シリアル番号）	CA 内で一意の番号*2
Signature （電子署名アルゴリズム識別子）	本サービスで用いられる電子署名アルゴリズムの識別子*3
Issuer （発行者名）	発行者情報 （本 CA が指定する情報）
Validity （有効期間）	証明書の有効期間 （開始期日および終了期日）
Subject （加入者名）	加入者情報
SubjectPublicKeyInfo （加入者の公開鍵情報）	加入者の公開鍵アルゴリズム識別子と公開鍵データ
Extensions （拡張フィールド）	本 CP「7.1.2 証明書拡張」を参照

*1　証明書フォーマットの番号は Version3 に設定される。

*2　新規に証明書が作成されたとき CA サーバーにより付与される。

*3　証明書に電子署名する際に用いられる。

7.1.1 バージョン番号

本 CA が発行する証明書の X.509 フォーマットのバージョン番号は、Version3 である。

7.1.2 証明書拡張

本 CA が発行する TSA 証明書は、 x 509 証明書拡張フィールドを使用し、以下の表に示すフィールドを用いる。

表 7.1-2 SECOM TimeStamping CA1 証明書拡張

フィールド	記載事項(説明)
authorityKeyIdentifier (2.5.29.35)	CA の公開鍵を SHA-1 によりハッシュした 160bit 値
subjectKeyIdentifier (2.5.29.14)	加入者の公開鍵を SHA-1 によりハッシュした 160bit 値
keyUsage (2.5.29.15)	digitalSignature, nonRepudiation （keyCertSign, CRLSign を除くその他の目的については、本 CA で必要に応じて設定する場合がある）
extendedKeyUsage (2.5.29.37)	timestamping(1.3.6.1.5.5.7.3.8)

フィールド	記載事項(説明)
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.931.1 policyQualifierID=id-qt-cps qualifier=https://repo1.secomtrust.net/spcpp/ts/
cRLDistributionPoints (2.5.29.31)	URI: http://repo1.secomtrust.net/spcpp/ts/ca1/fullCRL.crl （ディレクトリ上にある CRL 配布場所）

表 7.1-3 SECOM TimeStamping CA2 証明書拡張

フィールド	記載事項(説明)
authorityKeyIdentifier (2.5.29.35)	CA の公開鍵を SHA-1 よりハッシュした 160bit 値
subjectKeyIdentifier (2.5.29.14)	加入者の公開鍵を SHA-1 よりハッシュした 160bit 値
keyUsage (2.5.29.15)	digitalSignature, nonRepudiation （keyCertSign, CRLSign を除くその他の目的については、本 CA で必要に応じて設定する場合がある）
extendedKeyUsage (2.5.29.37)	timestamping(1.3.6.1.5.5.7.3.8)
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.931.1 policyQualifierID=id-qt-cps qualifier=https://repo1.secomtrust.net/spcpp/ts/
cRLDistributionPoints (2.5.29.31)	URI: http://repo1.secomtrust.net/spcpp/ts/ca2/fullCRL.crl （ディレクトリ上にある CRL 配布場所）
Authority Information Access(1.3.6.1.5.5.7.1.1)	OCSP - URI:http://ts2.ocsp.secomtrust.net（OCSP サーバー公開場所） ※証明書申請毎に設定の有無を変えられる

表 7.1-4 SECOM TimeStamping CA3 証明書拡張

フィールド	記載事項(説明)
authorityKeyIdentifier (2.5.29.35)	CA の公開鍵を SHA-1 よりハッシュした 160bit 値
subjectKeyIdentifier (2.5.29.14)	加入者の公開鍵を SHA-1 よりハッシュした 160bit 値
keyUsage (2.5.29.15)	digitalSignature, nonRepudiation （keyCertSign, CRLSign を除くその他の目的については、本 CA で必要に応じて設定する場合がある）
extendedKeyUsage (2.5.29.37)	timestamping(1.3.6.1.5.5.7.3.8)
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.931.3 policyQualifierID=id-qt-cps qualifier= https://repo1.secomtrust.net/spcpp/ts/
cRLDistributionPoints (2.5.29.31)	URI: http://repo1.secomtrust.net/spcpp/ts/ca3/fullCRL.crl （ディレクトリ上にある CRL 配布場所）
Authority Information Access(1.3.6.1.5.5.7.1.1)	OCSP - URI:http://ts3.ocsp.secomtrust.net（OCSP サ

フィールド	記載事項(説明)
	ーバー公開場所） ※証明書申請毎に設定の有無を変えられる

表 7.1-5 Secom Time Stamping CA2 OCSP サーバー証明書拡張

フィールド	記載事項(説明)
authorityKeyIdentifier (2.5.29.35)	CA の公開鍵を SHA-1 よりハッシュした 160bit 値
subjectKeyIdentifier (2.5.29.14)	加入者の公開鍵を SHA-1 よりハッシュした 160bit 値
keyUsage (2.5.29.15)	digitalSignature（加入者公開鍵の使用目的）
extendedKeyUsage (2.5.29.37)	OCSPSigning
OCSP No Check (1.3.6.1.5.5.7.48.1.5)	null
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.931.1 policyQualifierID=id-qt-cps qualifier=https://repo1.secomtrust.net/spcpp/ts/

表 7.1-6 Secom Time Stamping CA3 OCSP サーバー証明書拡張

フィールド	記載事項(説明)
authorityKeyIdentifier (2.5.29.35)	CA の公開鍵を SHA-1 よりハッシュした 160bit 値
subjectKeyIdentifier (2.5.29.14)	加入者の公開鍵を SHA-1 よりハッシュした 160bit 値
keyUsage (2.5.29.15)	digitalSignature（加入者公開鍵の使用目的）
extendedKeyUsage (2.5.29.37)	OCSPSigning
OCSP No Check (1.3.6.1.5.5.7.48.1.5)	null
certificatePolicies (2.5.29.32)	certPolicyId=1.2.392.200091.100.931.3 policyQualifierID=id-qt-cps qualifier=https://repo1.secomtrust.net/spcpp/ts/

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、以下の表のとおりである。

表 7.1-7 SECOM TimeStamping CA 1 アルゴリズム OID

アルゴリズム	オブジェクト識別子（OID）

Sha1 With RSA Encryption	1 2 840 113549 1 1 5
RSA Encryption	1 2 840 113549 1 1 1

表 7.1-8 SECOM TimeStamping CA 2 アルゴリズム OID

アルゴリズム	オブジェクト識別子（OID）
sha256 With RSA Encryption	1.2.840.113549.1.1.11
RSA Encryption	1 2 840 113549 1 1 1

表 7.1-9 SECOM TimeStamping CA 3 アルゴリズム OID

アルゴリズム	オブジェクト識別子（OID）
Sha384 With RSA Encryption	1.2.840.113549.1.1.12
RSA Encryption	1 2 840 113549 1 1 1

7.1.4 名前形式

本 CA および加入者は、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。

表「7.1-7 使用可能文字」に DN に使用可能な文字を示す。

表 7.1-7 使用可能文字

英字	数字	記号
A～Z、a～z	0～9	：- . と空白

7.1.5 名前制約

設定しない。

7.1.6 CP オブジェクト識別子

本 CA が発行する TSA 証明書に記載されるポリシ OID は表「1.2-2 OID（本 CP)」のとおりである。

7.1.7 ポリシ制約拡張の利用

設定しない。

7.1.8 ポリシ修飾子の文法および意味

ポリシ修飾子については、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拡張の処理の意味

設定しない。

7.2 CRL のプロファイル

本 CA が発行する CRL は、X.509 CRL フォーマット形式により作成される。

表「7.2-1 CRL 基本領域」に示すフィールドを用いる。

表 7.2-1 CRL 基本領域

フィールド	説明
Version （バージョン番号）	CRL フォーマットの番号*1
Signature （電子署名アルゴリズム識別子）	本 CA が電子署名に用いるアルゴリズムの識別子*2
Issuer （発行者名）	CRL の発行者情報 （本 CA が指定する情報）
ThisUpdate （更新日）	CRL の発行日時
NextUpdate （次回更新予定日）	CRL の次の更新予定日時
RevokedCertificates （取消リスト）	取消となった証明書の情報 SerialNumber（シリアル番号） RevocationDate（取消日付） が設定される

*1　CRL フォーマットの番号は Version2 に設定される。

*2　CRL に署名する際に用いられる。

7.2.1 バージョン番号

本 CA が発行する CRL の X.509 フォーマットバージョン番号は、Version2 である。

7.2.2 CRL 拡張

本 CA が発行する X.509CRL 拡張フィールドを使用する。

表「7.2-2 CRL 拡張」に示すフィールドを用いる。

表 7.2-2 CRL 拡張

フィールド	説明
AuthorityKeyIdentifier （認証機関鍵識別子）	CA の公開鍵を SHA-1 によりハッシュした 160bit 値

7.3 OCSP のプロファイル

本 CA は、RFC2560、5019 に準拠する OCSP サーバーを提供する。

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

規定しない。

8 準拠性監査

8.1 監査の頻度

セコムは、本サービスが本 CP および CPS に準拠して運用されているかに関して、年に１回の準拠性監査を行う。

8.2 監査人の身分と資格

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。

8.3 監査人と被監査対象との関係

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とする。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 監査対象

監査は、本 CA の運用にかかる業務を対象として行う。

8.5 監査指摘事項への対応

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

8.6 監査結果の報告

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。

監査報告書は、認証サービス改善委員会に報告される。監査報告書は、許可されたものだけがアクセスできるよう保管管理される。

9. 他の業務上および法的問題

9.1 料金

料金体系については、契約書等に別途定める。

9.2 財務的責任

セコムは、本サービスの提供にあたり、十分な財務的基盤を維持するものとする。

9.3 機密保持

9.3.1 機密情報の範囲

CA であるセコムが保持する個人および組織の情報は、証明書、CRL、本 CP および CPS の一部として明示的に公表されたものを除き、機密保持対象として扱われる。セコムは、法の定めによる場合および加入者による事前の承諾を得た場合を除いてこれらの情報を社外に開示しない。かかる法的手続、司法手続、行政手続あるいは法律で要求されるその他の手続に関連してアドバイスする法律顧問および財務顧問に対し、セコムは機密保持対象として扱われる情報を開示することができる。また会社の合併、買収あるいは再編成に関連してアドバイスする弁護士、会計士、金融機関およびその他の専門家に対しても、セコムは機密保持対象として扱われる情報を開示することができる。

加入者の私有鍵は、その加入者によって機密保持すべき情報である。本サービスでは、いかなる場合でもこれらの鍵へのアクセス手段を提供していない。

監査ログに含まれる情報および監査報告書は、機密保持対象情報である。セコムは、CPS「8.6 監査結果の報告」に記載されている場合および法の定めによる場合を除いて、これらの情報を社外へ開示しない。

9.3.2 機密保持対象外の情報

証明書および CRL に含まれている情報は機密保持対象外として扱う。その他、次の状況におかれた情報は機密保持対象外とする。

- セコムの過失によらず知られた、あるいは知られるようになった情報
- セコム以外の出所から、機密保持の制限無しにセコムに知られた、あるいは知られるようになった情報
- セコムによって独自に開発された情報
- 開示に関して加入者によって承認されている情報

9.3.3 機密情報の保護責任

CA であるセコムが保持する機密情報を、法の定めによる場合および加入者による事前の承諾を得た場合に開示することがある。その際、その情報を知り得たものは、契約あるいは法的な制約によりその情報を第三者に開示することはできない。

9.4 個人情報の保護

本 CA が取得する個人情報は、本 CP「9.3 機密保持」のとおり機密情報として取り扱う。また、本 CA は、個人情報に関する法律または関連する法令およびセコムが一般に公開しているプライバシポリシを遵守する。

9.5 知的財産権

セコムと加入者との間で別段の合意がなされない限り、本サービスにかかわる情報資料およびデータは、次に示す当事者の権利に属するものとする。

加入者証明書	:	セコムに帰属する財産である
CRL	:	セコムに帰属する財産である
識別名（DN）	:	加入者証明書に対して対価が支払われている限りにおいて、その名前が付与された者に帰属する財産である
加入者の私有鍵	:	私有鍵は、その保存方法または保存媒体の所有者にかかわらず、公開鍵と対になる私有鍵を所有する加入者に帰属する財産である
加入者の公開鍵	:	保存方法または保存媒体の所有者にかかわらず、対になる私有鍵を所有する加入者に帰属する財産である
本 CP および CPS	:	セコムに帰属する財産（著作権を含む）である

9.6 表明保証

9.6.1 CA および RA の表明保証

セコムは、本 CP および CPS に規定した内容を遵守して証明書申請者に関する審査、証明書の登録、発行、取消を含む認証サービスを提供し、CA 私有鍵の信頼性を含む認証業務の信頼性を確保する。

本 CP および CPS に規定された保証を除き、セコムは、明示的あるいは暗示的に、もしくはその他の方法を問わず、一切の保証を行わない。

9.6.2 加入者の表明保証

本 CA の加入者は、以下の義務を負う

- 本 CA に、加入者が把握できる範囲内で正確かつ完全な情報を提供する。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 に通知する
- 危殆化から自身の私有鍵を保護する
- 証明書の使途は本 CP および CPS に従うものとし、かつ法令に反しないこと
- 加入者が、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や、登録情報に変更があった場合、加入者は本 CA に証明書の取消をすみやかに要求すること

9.6.3 利用者の表明保証

本 CA のサービスの利用者は、以下の義務を負う

- 本 CA が発行する証明書を信頼し、本 CP および CPS に規定されている本 CA が意図する目的のみに証明書を使用すること
- 証明書を信頼しようとするときは、リポジトリー内の CRL または OCSP サーバーに含まれる取消情報を取得して、証明書が取消されていないことを確認すること
- 証明書を信頼しようとするときは、当該証明書の有効期間を確認し、有効期間内であることを確認すること
- 本 CA が発行した証明書を信頼しようとするときは、当該証明書が本 CA の証明書によって署名検証できることを確認すること
- 本 CA の証明書を信頼して利用する際、本 CP および CPS に規定されている利用者として責任を負うことに合意すること

9.7 保証の制限

セコムは、本 CP「9.6.1 CA および 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 CA および 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、不正使用ならびに過失等により発生する一切の損害
- 加入者または利用者が自己の義務の履行を怠ったために生じた損害
- 加入者または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、加入者または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
- 加入者が契約に基づく契約料金を支払っていない間に生じた損害
- 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 の業務停止を含む本 CA のサービスの業務停止に起因する一切の損害

9.9 補償

本 CA が発行する証明書を申請、受領、信頼した時点で、加入者および利用者には、セコムおよび関連する組織等に対する損害賠償責任および保護責任が発生する。当該責任の対象となる事象には、損失、損害、訴訟、あらゆる種類の費用負担の原因となるようなミス、怠慢な行為、各種行為、履行遅滞、不履行のうち、証明書申請時に加入者が本 CA に最新かつ正確な情報を提供しなかったことに起因するもの、または各種責任、損失、損害、訴訟、あらゆる種類の費用負担の原因となるような加入者および利用者のミス、怠慢な行為、各種行為、履行遅滞、不履行等の各種責任が含まれる。

9.10 改訂

9.10.1 改訂手続

(1) 重要な変更

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

(2) 重要でない変更

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

9.10.2 通知方法および期間

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

9.11 紛争解決手段

本 CA のサービスの利用に関し、セコムに対して訴訟、仲裁を含む法的またはその他の解決手段に訴えようとする場合、セコムに対して事前にその旨を通知するものとする。

9.12 準拠法

本 CA、加入者および利用者の所在地にかかわらず、本 CP および CPS の解釈、有効性および本サービスにかかわる紛争については、日本国の法律が適用される。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。

9.13 雑則

9.13.1 完全合意条項

セコムは、本サービスの提供にあたり、自らのポリシおよび保証ならびに加入者または利用者の義務等を本 CP、CPS および契約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。

9.13.2 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。

9.13.3 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。

10. 用語解説

O

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。

X

X.500
名前およびアドレスの調査から属性による検索まで広範囲なサービスを提供することを目的に ITU-T が定めたディレクトリ標準。X.500 識別名は、X.509 の発行者名および主体者名に使用される。

X.509
X.509 ITU-T が定めた電子証明書および証明書失効リストのフォーマット。X.509 v3(Version 3)では、任意の情報を保有するための拡張領域が追加された。

あ～お

オブジェクト識別子（OID）
Object Identificationの略。世界で一意となる値を登録機関（ISO 、ITU）に登録した識別子。PKI で使うアルゴリズム、電子証明書内に格納する名前（subject）のタイプ（Country名等の属性）等は、オブジェクト識別子として登録されているものが使用される。

か～こ

鍵ペア
公開鍵暗号方式における私有鍵と公開鍵から構成される。

加入者
本 CA から証明書の発行を受ける組織または団体のことをいう。

公開鍵
公開鍵暗号方式において用いられる鍵ペアの一方。私有鍵に対応する、公開されている鍵のことをいう。

さ～そ

私有鍵
公開鍵暗号方式において用いられる鍵ペアの一方。公開鍵に対応する、加入者のみが保有する鍵のことをいう。

証明書
電子証明書の略。ある公開鍵を、記載されたものが保有することを証明する電子的文書。CA が電子署名を施すことで、その正当性が保証される。

証明書取消リスト(CRL)
Certificate Revocation List の略。本 CA によって取消された証明書情報の一覧が記録されている。

証明書発行要求(CSR)
Certificate Signing Request の略。電子証明書を発行する際の元となるデータファイル。CSR には電子証明書の発行要求者の公開鍵が含まれており、その公開鍵に発行者の署名を付与して電子証明書を発行する。

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

た～と

タイムスタンプ
電子情報と時刻情報を含めた情報であり、その時刻以前にそのデータが存在したことの証明（存在証明）と、その時刻から検証した時刻までの間にそのデータが変更・改ざんされていないことを証明（非改ざん証明）する事ができる手段、およびその証拠に結びつく情報のことをいう。
本サービスでは、タイムスタンプを行う TSA（Time Stamping Authority：タイムスタンプ局）および TSA に対し標準時の配信、時刻監査を行う TA（Time Authority：標準時配信局）向けの証明書を発行する。

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

登録局（RA）
Registration Authority の略。本サービスでは CA の業務のうち、審査業務を行う機関のことをいう。

な～の

認証運用規定（CPS）
Certification Practice Statement の略。電子証明書の申請、申請の審査、証明書発行、取消し、保管、開示を含む本サービスの提供および利用にあたっての注意点等を規定するもの。

認証局（CA）
Certification Authority の略。証明書の発行・更新・取消し、CA 等私有鍵の生成・保護および加入者の登録を行う機関のことをいう。

ま～も

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

メジャーバージョン番号
本 CP の内容変更に際して、変更レベルが、明らかに加入者や利用者が証明書や CRL を使用するうえで影響すると判断した場合、本 CP の改訂版に付ける番号（例：Version 1.02 ならば、下線部（1））を示す。

ら

リポジトリー
CA が発行した証明書等の格納庫である。ユーザーまたはアプリケーションがネットワークのどこからでも証明書にアクセスできるようにするための仕組みである。CRL や本 CP もリポジトリーに格納される。

利用者
認証局から発行された証明書を利用する個人あるいは組織をさす。