SECOM Trust.net Root1 CA

証明書ポリシ/認証運用規定

2006 年 5 月 22 日

Version 2.00

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	2003.08.01	初版発行
V1.10	2003.09.29	・「1.2 セキュリティ・ポリシの概要」の「人的リスク」 記述の正確性の見直し ・「11.2.11 証明書のステータス情報」 CRL の発行周期を明示
V2.00	2006.05.22	会社統合に伴い、会社名“セコムトラストネット”を“セコムトラストシステムズ”に変更 “セコムトラストネットセキュリティポリシ委員会”を“認証サービス改善委員会”に変更

目次

1. はじめに

SECOM Trust.net Root1 CA 認証運用規定（以下、「本 CPS」という）は、SECOM Trust.net Root1 CA※1（以下、「本 CA」という）が発行する証明書を信頼し利用する加入者及び利用者に、必要な情報を提供することを目的とするものである。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）は、本 CA を設立し、電子証明書（以下、「証明書」という）の発行、管理を行って、加入者の電子署名、本人認証等をサポートする。

※1 セコムトラストシステムズは 2003 年 7 月 23 日に Valicert, Inc.から「Valicert Class 1 Policy　Validation Authority」の鍵ペアを購入した。セコムトラストシステムズは、本 CPS にしたがい、CA 鍵ペアを安全に管理し、本 CA のサービスを実施する。
本 CA が発行する証明書の issure には、
「E=info@valicert.com CN=http://www.valicert.com/ OU=ValiCert Class 1 Policy Validation Authority O=ValiCert, Inc. L=ValiCert Validation Network」が記載されているが、発行を行う主体はセコムトラストシステムズである。

本 CPS は、責任の制限、保証の放棄、各種損害に対する責任の制限、損害賠償責任、被害者の保護、紛争解決手段等に関する規定を含むいくつかの業務関連事項について規定している。加入者に発行される証明書については、本 CPS の 11 項に付属されている証明書ポリシ（以下、「CP」という）に規定される。本 CPS 及び付属の CP は、本 CA が展開する認証基盤について規定した文書である。

加入者及び利用者は、本 CA が発行する証明書を信頼して利用する前に、本 CPS 及び付属の CP の内容を承諾しなければならない。本 CA が発行する証明書の利用にあたっては、本 CA のリポジトリ※2 にアクセスし、本 CA が発行する証明書が有効であること、および本 CPS に適用された各種変更点に関する情報を取得し確認した後に、証明書の利用を利用者自身の判断で行わなければならない。

※2 本 CA のリポジトリには、本 CPS、CRL 等、本 CA が発行する有効な証明書に関する各種記録が保管される。詳細は、http://repository.secomtrust.net/rootrepository/を参照のこと。

通常、加入者とセコムトラストシステムズとの契約は書面により行う。当該契約書の内容が本 CPS の内容に抵触する場合、両当事者が負うべき義務や行使できる権利については、契約書の規定にしたがって判断される。

1.1 本 CPS の概要

SECOM Trust.net Root1 CA

本 CA のサービスは、本 CA が署名し発行した証明書に含まれる公開鍵が、正に証明書に記載された加入者のものであるということを、加入者及び利用者に対し提供するサービスである。本 CA が証明書に電子署名を行うことは、証明書に含まれる加入者の公開鍵に対して、公開鍵暗号方式によって加入者の名前及び有効期限等のその他の情報と関連していることを意味する。当該証明書を信頼して利用する利用者は、その証明書が本 CA により発行されたものであるかどうかを検証するため、本 CA の公開鍵を使って証明書の電子署名を検証しなければならない。本 CA の証明書は、一般的に使用されているウェブ・ブラウザ（例：ネットスケープ・ナビゲータやマイクロソフト・インターネット・エクスプローラ）等に組み込まれている。当該ブラウザに組み込まれている本 CA の証明書には、本 CA の公開鍵も含まれる。これにより、加入者及び利用者は、本 CA の公開鍵を使って証明書の署名検証をすることで、当該証明書が本 CA により発行されたものであるかどうかを検証できる。

本 CA のサービスは、本 CA が発行する証明書のライフサイクル全般を安全に管理するサービスである。当該ライフサイクルには、証明書の発行、更新、取消し等が含まれる。本 CA では、あらゆる登録業務を直接行う。本 CA は、証明書取消リスト（以下、「CRL」という）を発行して、証明書の取消情報を提供する。本 CA は、有効な証明書と CRL を本 CA のリポジトリに格納し、証明書のステータスを提供する。

加入者

本 CA の加入者とは、本 CA から証明書の発行を受ける下位の CA のことをいう。

加入者の初期登録及び証明書の発行

本 CA の加入者は、証明書のライフサイクルが始まる前に初期登録を行わなければならない。初期登録は、鍵ペアの生成と証明書の発行からなる。初期登録後、発行された証明書は、本 CA のリポジトリに登録され、有効な証明書として公開される。

・ 加入者は、通常、自身が保有する暗号装置を使って、独自に鍵ペアを生成する。本 CA は、加入者の暗号装置が、秘密鍵を公開することなく、当該鍵ペアの秘密鍵を使って電子署名を作成することができる装置であることを確認する。本 CA は、加入者から証明書発行要求（以下、「CSR」という）を受け取った場合、CSR に記載の当該鍵ペアの公開鍵を使って、CSR に添付の電子署名を検証できることを確認する。

証明書の発行手続きは、加入者の秘密鍵の生成後に行われ、加入者の証明書に含まれる公開鍵の所有者と加入者との同一性を検証する手続きが含まれる。

・ 本 CA は、加入者の証明書を発行する。本 CA は、本 CA の秘密鍵を使って証明書に電

子署名を施す。本 CA は加入者が発行済み証明書を受領した後、加入者の証明書を公開する。これにより、利用者は、証明書が加入者のものであることを確認できる。

- 本 CA と加入者が発行済み証明書の内容を確認した結果に基づいて、本 CA は証明書を公開する。発行済みの証明書は本 CA が公開したことで効力を発する。加入者が証明書の内容を確認するか、受領の意思を示したと考えられる場合、本 CA は、本 CA のリポジトリに証明書を公開する。公開処理を行うことで、利用者が証明書を利用することが可能になると同時に、証明書が効力を発する。効力を持つ証明書には取消された証明書は含まない。
- 本サービスのリポジトリは、オンラインで利用できる電子証明書登録データベースであり、本 CA は、このデータベースを使って、本 CA によって発行した証明書の公開や、証明書が取消された場合に本 CA が発行する CRL の公開を行う。
- 本 CA のリポジトリの保守は本 CA が行う。加入者及び利用者は、リポジトリ内の各種記録にアクセスして、本 CA の加入者の有効な証明書や、当該証明書のステータス情報を取得できる。例えば、加入者の有効な証明書を、本 CA が取消した場合、リポジトリにある CRL に取消情報が付加される。加入者及び利用者が取得する CRL の取消情報は、加入者の証明書が取消されたこと、及び当該証明書を信頼すべきではないことを示すものである。加入者及び利用者は、有効期限が切れた証明書を信頼したり、取消された証明書を信頼してはならない。
- 本 CA は、リポジトリに証明書と CRL を公開して加入者の有効な証明書を管理する。加入者及び利用者は、リポジトリの記録にアクセスして、当該管理情報を取り出すことができる。本 CA が発行する証明書と CRL は、本 CA の秘密鍵による電子署名が施されているため、不当な目的等をもってその内容を改ざんしたりすることはできず、その結果その内容が改ざん等されていないことを検証できる。加入者及び利用者は証明書情報と CRL として公開されている情報をもとに、改ざんなどの各種変更が行われていないかどうかについて確認した上で、提供された加入者の証明書を信頼して使用するか否かを決定しなければならない。

業務内容の開示

本 CA は、自身が生成する鍵ペアや発行する証明書のライフサイクル管理業務、及び情報の保護業務等の内容を、本 CPS 及び付属の CP に規定して開示する。本 CPS 及び付属の CP は、リポジトリに公開され、すべての加入者及び利用者が閲覧可能である。

サービスの完全性

本 CA が提供する認証基盤の信頼性を維持するために、本 CA の秘密鍵の管理に関する規定に基づく厳格な運用が不可欠である。本 CA の秘密鍵の管理に関する規定には、本 CA の鍵ペアの生成、保管、バックアップ、復元、配布、使用法、破壊、アーカイブに関する規定や、本 CA の暗号装置のライフサイクル管理が含まれる。本 CA が提供する認証基盤の完全性を妨げる可能性がある本 CA の秘密鍵の危殆化を極力回避するために、本 CA の秘密鍵のライフサイクル管理を適切に行う。

加入者の証明書のライフサイクル管理は、本 CA が提供するサービスの中核をなすものである。加入者の証明書のライフサイクル管理には次のようなプロセスが含まれる。

- 登録（証明書に含まれる公開鍵の所有者と加入者の同一性の確認、検証を目的とした認証プロセスを意味する。）
- 証明書の更新
- 鍵更新に伴う証明書の発行
- 証明書の取消し
- CRL を使った、証明書のステータス情報の適時公開

環境の管理

信頼性の高いサービス環境を構築し、管理することは、本 CA のサービスの信頼性の維持に不可欠である。本 CA では、鍵のライフサイクル管理、証明書ライフサイクル管理が効果的に行われるよう、サービス環境の適切な管理を実施する。

1.2 セキュリティ・ポリシの概要

セコムトラストシステムズは、セキュリティポリシを定め、許容可能なリスクの範囲内で、本 CA に関するサービスの目標が達成できるように努める。セコムトラストシステムズでは、多くの潜在的なリスクに対して、効果的な内部規定を作成し、これらのリスクのレベルを従業員、株主、加入者や証明書を信頼して利用する利用者等の利益を損なわないよう、許容可能なレベルに抑える対策を積極的に行う。

リスク

セコムトラストシステムズは、認証業務のセキュリティの重要性に鑑み、リスク分析・評価に基づいた対策を講じている。セコムトラストシステムズは、ISMS（Information Security Management System）においてリスク分析手順を定め、トップマネジメントによるリスク評価を行い必要な対策を講じ、見直しを実施している。認証業務に特有の鍵の危殆化というリスクに関しては、詳細な要因分析を行い、対応策を用意して本 CA の運用担当者に教育し、対応策の徹底を図っている。

資産の分類と管理

セキュリティの基本要素には、資産の分類と管理がある。必要なときに最適な資産が利用できない場合、作業を延期したり、無用なリスクを受容したりしなければならない。したがって、あらゆる資産の所在を明確に把握し、必要な資産を管理者の責任下に置いておく必要がある。使用される資産は登録され、定期的にその状態がチェックされる。また、セコムトラストシステムズは、本 CA の運用担当者に対し、与えられた任務を効果的に遂行するために必要な権限を与え、必要な資産の使用と管理を行っている。

人的リスク

本 CA の運用にかかる諸規定において、人為的ミスの発生を抑えるためのコントロールを

含む手続きを用意し、運用担当者に教育を行っている。万一人為的ミスが発生した場合、運用担当者には即時報告が義務付けられている。報告の義務は全社員の守則として定められている。また、そのミスによる障害を回復するための障害対応手続きも定めている。更に、全社員と機密保持誓約を取り交わし、業務の重要性及びセキュリティのプロフェッショナルとしての自覚を求めている。

物理的リスクや環境上のリスク

セコムトラストシステムズは、本 CA の業務を安全に行うために物理的、環境的な対策を講じている。建物設備の強度はもちろんのこと、回線やシステムに冗長構成、常時監視などを採用している。具体的には、施設設備への入退管理を 7 段階のセキュリティレベルでコントロールし、権限を有する運用担当者のみが必要なエリアへ入室できる仕組みになっている。施設設備やシステムについては 24 時間 365 日監視され、速やかに異常に対処できる仕組みと体制をもっている。

ネットワーク管理ポリシ

セコムトラストシステムズでは、監視システムや監査システムを使って、本 CA サービスに使用するオンライン情報システムやネットワーク資源を管理している。同システムは処理すべきタスクに応じて細分化されている。情報技術は、めまぐるしい速度で変化してゆくため、一定期間、同システムを支えてきた技術も、新しいものに変化してゆく。監視システムは、ネットワーク上の不正な処理や状態を監視し、管理者に報告する。管理者は、報告データに基づきより詳細な調査を行よう担当者に指示し、各種対策を講じる。監査システムは、CA 秘密鍵の操作を含む重要な処理の詳細情報を記録する。管理者は問題が起こった場合でも、適切な対策を講じることができ、問題の再発を防止することに努める。

アクセス・コントロール

アクセス・コントロールは、セキュリティ対策に不可欠な要素である。アクセス・コントロールが効果的に行われれば、アクセスを許可されたあらゆるユーザーは、必要なリソースにアクセスできる。本サービスでは、本 CA のハードウェア及び本 CA の行うサービスを提供するソフトウェアへの物理的なアクセスを制限する適切なセキュリティコントロールを実装する。そのハードウェアやソフトウェアへのアクセスは、権限者に制限される。アクセスの制御は電子的なアクセス制御方法、物理的なアクセス制御方法を組み合わせる。ハードウェア及び本 CA の行うサービスを提供するソフトウェアへの物理的アクセスは記録される。また、許可されているアクセスについても管理者の承認の下に行われる。

開発と保守

本 CA を構成する諸資源は、使用中に開発や保守が必要となる場合がある。あらゆる開発作業は、文書化された適切な方法にしたがって行われる。保守作業は、適切かつ承認を受けて行い、欠陥の詳細、修理内容、予防措置のすべてを記録する必要がある。装置の担当者は、欠陥が生じた旨を管理者に報告する義務がある。各装置の修理や保守は、適切な資格を持つ人物のみが行う。第三者が施設に立ち入ることを許可された場合、当該作業に適

用可能な規定に従い、当該人物は管理者の立会いのもと、その管理下に置かれる。指定の修理業者や保守業者に装置を送るために装置を施設外に持ち出す場合、情報漏洩防止及びその他の対策を講じる。

事業継続計画

本 CA のサービスは、セコムトラストシステムズの事業継続方針に基づき、本 CA の行うサービスの中断を余儀なくする重大な問題や、信頼性を著しく損なわせるような問題が発生した場合でも、本 CA に関するサービスを継続するために必要な計画を作成している。サービスの中断を最小限に抑えるため、セコムトラストシステムズでは、サービスの復旧に必要なリソースの調達手段を予め計画している。

準拠性

本 CA のサービスは、本 CPS やセコムトラストシステムズの情報セキュリティポリシに準拠して行われる。担当者は本 CPS に規定された内容やセコムトラストシステムズの情報セキュリティポリシを理解し業務を行わなければならない。セコムトラストシステムズは、担当者に対して本 CPS に規定された内容やセコムトラストシステムズの情報セキュリティポリシを理解するための教育、訓練を実施している。管理者は、担当者の業務が本 CPS に規定された内容やセコムトラストシステムズの情報セキュリティポリシに準拠して行われているかを日常業務の中でチェックする責任がある。また、本 CA に対して定期的に監査を行い準拠性を監査する。

1.3 識別

本サービスでは、加入者に証明書を発行し、当該証明書のライフサイクルを管理する。

本 CA は本 CPS 及び付属の CP に準拠し、証明書を発行する。本 CPS には、付属の CP に関する規定が含まれ、その最新版は、本 CA のリポジトリに公開されている。

本 CA の加入者の証明書は、付属の CP に基づいて発行されるものでなければならない。付属の CP は、本 CA の担当者が証明書を発行する際に準拠する内容をまとめたものである。

1.4 コミュニティ及び適用

本 CPS は、本 CA の運用担当者が行う証明書の発行及び管理業務のすべてに適用される。本 CA が発行する証明書や CRL を信頼して利用する加入者及び利用者や、本 CA のリポジトリを利用する加入者及び利用者は、本 CPS に拘束される。

本 CA は、本 CPS や付属の CP に基づいて証明書を発行する。本 CA はルート CA であり、下位 CA に対して CA の証明書を発行する。本 CA の下位 CA である加入者が発行した証明書及び CRL を信頼して利用する利用者は、当該証明書及び CRL の信頼性を加入者の証明書によって検証することができる。

1.5 連絡先

本 CPS 及び付属の CP の維持・管理は、セコムトラストシステムズの認証サービス改善委員会が行う。本 CPS 及び付属の CP に関する問い合わせ窓口は次のとおりである。

認証事業者 ：名称 セコムトラストシステムズ株式会社
住所 〒150-0001 東京都渋谷区神宮前 1-5-1

連絡先
本サービス窓口 ：名称 セコムトラストシステムズ株式会社 CA サポートセンタ
電子メールアドレス：root1-support@secomtrust.net

2. 関係者の義務

2.1 本 CA の通知義務

本 CA の運用にあたり、セコムトラストシステムズは以下の義務を負う。

- リポジトリに公開されている本 CPS 及び付属の CP に従って本 CA を運用する。なお、本 CPS 及び付属の CP は、適宜改訂される場合がある。
- 証明書を発行し、公開する。
- 有効な証明書取消要求を受領した場合には、本 CA は証明書の取消しを実施する。
- 本 CA は、証明書の取消処理を行った場合や、CRL の有効期限が満了した場合、CRL を更新する。
- 最新の CRL をリポジトリに公表する。
- 本 CA の加入者及び利用者に、証明書の発行及び取消しに関する情報を提供するために、リポジトリに公開済みの有効な証明書及び最新の CRL へのアクセスを可能とさせる。

2.2 本 CA の検証義務

本 CA は、加入者の証明書の登録を行う。具体的には次のことを行う。

- 証明書を発行する前に、加入者の本人確認を行う。
- リポジトリに証明書を公開する前に、加入者が証明書を受領したこと、または受領とみなせることを確認する。
- 証明書取消要求を確認する。
- 更新に伴う証明書の発行を行う前に、取消されてなくかつ有効期限内の証明書の更新を要求する加入者が、本人であることを確認する。

2.3 リポジトリの義務

セコムトラストシステムズは本 CA のリポジトリを運営する義務を負う。本 CA は、本 CA が発行する証明書を、適時、リポジトリに公開する。

本 CA は、CRL 及び本 CPS の改訂版を、適時、リポジトリに公開する。

本 CA の加入者及び利用者は、インターネットを経由しリポジトリに直接アクセスすることができる。

2.4 加入者の義務

本 CA のサービスの加入者は、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、その旨を速やかに本 CA に通知する。

- 危殆化から自身の秘密鍵を保護する。
- 証明書の使途は本 CPS 及び付属の CP 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秘密鍵が危殆化した、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 に証明書の取消しを速やかに要求すること。

2.5 利用者の義務

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 CPS 及び付属の CP 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、リポジトリ内の CRL 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 CPS 及び付属の CP 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。

3. 関係者の責任

3.1 本 CA が発行する証明書の使用制限

本 CA が発行する証明書の用途は、セコムトラストシステムズが提供しているサービスや、セコムトラストシステムズと良好な関係にある本 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。また、本 CA が発行する証明書は、法令に即した範囲で使用すること。

3.2 関係者間での責任の分担

本 CA が発行した証明書又は当該証明書に関連して発生する取引の件数、電子署名の数、損害を被った加入者や利用者の人数、あるいは訴訟の原因に関係なく、本 CA が発行した証明書一枚に起因する当社の賠償限度額は、金 1,000,000 円を超えないものとする。

3.3 本 CA の保証制限

3.3.1 保証

セコムトラストシステムズは、本 CPS 及び付属の CP に規定した内容を遵守して電子証明書の発行、取消しを含む認証サービスを提供し、本 CPS 及び付属の CP の範囲内で、本 CA の秘密鍵の信頼性を含む認証業務の信頼性の確保を保証する。

本 CPS に規定された保証を除き、セコムトラストシステムズは、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。

3.3.2 一定の損害に対する免責

セコムトラストシステムズは、本 CPS「3.3.1 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。

3.3.3 免責

本 CPS「3.3.1 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、不正使用並びに過失等により発生する一切の損害
- 加入者又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
- 加入者又は利用者のシステムに起因して発生した一切の損害
- 加入者又は利用者が使用する端末の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電子証明書及び 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

3.4 加入者及び利用者の損害賠償責任

本 CA が発行する証明書を申請、受領、信頼した時点で、加入者及び利用者には、セコムトラストシステムズ及びセコムトラストシステムズの役員、取締役、従業員、子会社、関連会社、下請業者、顧問、サプライヤ、ベンダ、代表者、エージェント等に対する損害賠償責任及び保護責任が発生する。当該責任の対象となる事象には、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及び利用者のミス、怠慢な行為、各種行為、履行遅滞、不履行等が含まれる。

3.5 非信託関係

本 CA は、加入者、利用者または証明書のその他ユーザー等のエージェント、受託者または代理人ではない

3.6 準拠法

本 CA、加入者及び利用者の所在地にかかわらず、本 CPS 及び付属の CP の解釈、有効性及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。

3.7 本 CA の目的、管理、運営方法の変更

セコムトラストシステムズが、本 CA に関連する事業部門等を分離したり、他社等と合併したりした場合、本 CA の目的、管理法、運営法が変更される。またこの場合、本 CPS 及び付属の CP の内容も修正される。

3.8 紛争解決プロセス

本 CA のサービスの利用に関し、セコムトラストシステムズに対して訴訟、仲裁を含む解決手段に訴えようとする場合、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。

4. 料金及び課金

セコムトラストシステムズは、本 CA のサービスの加入者に、本 CA の証明書発行サービス及び管理サービス等の利用料金を請求できる。

5. 公開及びリポジトリに関する要件

本 CPS 及び付属 CP の最新版は、本 CA のリポジトリから入手できる。本 CA が発行する証明書及び CRL は、本 CA のリポジトリに公開する。すべての加入者及び利用者は本 CA のリポジトリにインターネットからアクセスできる。

本 CA のリポジトリは、加入者及び利用者に対して 24 時間 365 日参照可能とする。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。

6. 準拠性監査要件

セコムトラストシステムズは、アメリカ公認会計士協会（AICPA）が開発した Webtrust for CA に準拠して本 CA を維持管理する。Webtrust for CA には、次のような内容が含まれる。

- 事業の内容や情報管理に関する規定の開示を要求する規定
- サービスの完全性維持に関する規定
- サービス提供環境の管理状況の維持管理に関する規定

監査の結果、修正すべき点が発見された場合、セコムトラストシステムズは、速やかに必要な修正作業を行い、本 CA のサービスの運用状況が、Webtrust for CA に準拠する状態を回復する。

本 CA の加入者に対し、本 CA のサービスの評価のために、Webtrust for CA の監査報告書が参照可能である。

7. 本 CA の鍵ペアの生成

7.1 鍵のサイズ

本 CA で使用する CA の鍵ペアは、RSA アルゴリズムで、鍵長は 1024 ビットである。

7.2 鍵のアルゴリズム

本 CA の鍵ペアの生成に使用するアルゴリズムは、RSA アルゴリズムである。

7.3 鍵の生成に使用するハードウェア及びソフトウェア

本 CA は、暗号装置を使って本 CA の鍵ペアを生成する。暗号モジュールは、少なくとも FIPS 140-1 level 3 に認定済みのものを使用する。

7.4 鍵の用途

本 CA の秘密鍵は、原則として、CA に対して発行する証明書及び CRL への署名に使用する。

7.5 鍵の有効期間

本 CA の秘密鍵の有効期間は、20 年を想定している。

8. 本 CA の秘密鍵の保護

8.1 本 CA の秘密鍵の保管基準

本 CA の秘密鍵は、規格 FIPS 140-1 Level 3 に認定済みの専用の暗号装置に保管される。

8.2 鍵へのアクセス

本 CA が使用するあらゆる暗号装置は、物理的かつ論理的なアクセス・コントロールを受ける。暗号装置内のあらゆる鍵ペアへのアクセスは、複数の担当者による操作を必須とする。

8.3 キー・エスクロー

本 CA が生成した本 CA の秘密鍵を第三者に寄託することはない。

8.4 本 CA の秘密鍵のバックアップ

本 CA の秘密鍵は、実際のサービスに使用する暗号装置と、バックアップ用として保管する暗号装置に保管される。バックアップ用鍵を保管する暗号装置は遠隔地に保管される。

8.5 鍵情報のアーカイブ

本 CA は、取消された証明書、有効期限切れの証明書、古い CRL をアーカイブする。ただし、アーカイブした情報は、通常、加入者及び利用者はアクセスできない。

9. 本 CA の公開鍵の配布

9.1 配付方法

本 CA の公開鍵は、付属の CP にしたがって、本 CA の加入者及び利用者に配布される。

9.2 本 CA の秘密鍵の更新

本 CA の秘密鍵の有効期間は 20 年を想定し、対応する証明書の有効期間は 20 年とする。

本 CA の秘密鍵の有効期間が満了した時点で、新しい秘密鍵が生成され、その後、新しい秘密鍵を使って署名された証明書及び CRL が発行される。

本 CA の新しい公開鍵は、付属の CP にしたがって加入者に配布される。

10. サービス環境の管理

10.1 仕様変更手続き

10.1.1 重要な変更

認証サービス改善委員会は､本 CPS の内容変更に際して､加入者または利用者に対して、証明書または CRL を使用するうえで CPS の内容の変更が明らかに影響すると判断した場合、本 CPS のメジャーバージョン番号を更新し、本 CPS の変更内容をリポジトリに公開する。公開後は、変更内容の撤回を告知しない限り、14 日を経過した時点で変更内容が有効になるものとする。

10.1.2 重要でない変更

認証サービス改善委員会は、本 CPS の内容変更に際して、加入者や利用者が証明書や CRL を使用するうえで CPS 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、本 CPS のマイナーバージョン番号を更新し、かつ加入者に告知することなしに変更を実施する。

10.1.3 公開と告知方法

本 CPS の重要な変更については、加入者及び利用者に対して、その内容と変更期日をリポジトリへの公開を以って告知とする。加入者は、告知日から 14 日以内の間、異議を申し立てることができる。告知日から 14 日を経過した時点で異議申し立てがない場合、変更された CPS は加入者及び利用者に同意されたものとみなされる。

10.2 本 CA の業務停止

本 CA のサービスは、認証サービス改善委員会の権限で終了される。

本 CA のサービスを終了する場合、

- 本 CA が発行した全ての証明書が取消されると同時に、本 CA は、新たな証明書の発行を停止する。
- 本 CA は、サービス終了の 1 ヶ月前までに、サービス終了の旨を、本 CA の加入者に通知する。
- 本 CA が保有する記録は、本 CA のサービス終了後も保管される。

10.3 機密情報、非開示情報、非機密情報の取扱い

本 CA が保持する個人及び組織の情報は、証明書、CRL、本 CPS 及び付属の CP の一部として明示的に公開されたものを除き、機密保持対象として扱われる。本 CA は、法の定めによる場合及び加入者若しくは利用者の書面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。かかる法的手続き、司法手続き、行政手続きあるいは法律で要求されるその他の手続きに関連してアドバイスする法律顧問及び財務顧問に対し、本 CA

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、金融機関及びその他の専門家に対しても、本 CA 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。

監査の結果は、機密保持対象情報である。本 CA は、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。Webtrust for CA の監査報告書は、Webtrust for CA の定めにより、開示される事がある。

証明書が取消される場合、取消事由、取消日時を取消された証明書の CRL 情報に含める場合、この取消事由のコード等は機密とみなされず、全加入者及び利用者に共有される。取消しに関するその他の詳細情報は原則として開示しない。

本 CA で取扱う情報に関して、法的根拠に基づいて情報を開示するように請求があった場合、本 CA は法の定めにしたがって法執行機関へ情報を開示する。

10.4 知的所有権

本 CA が発行する証明書及び CRL の所有権はセコムトラストシステムズに帰属する。本 CPS 及び付属の CP の所有権もセコムトラストシステムズに帰属する。

10.5 物理的セキュリティ

本 CA のコンピュータ・システム及びリポジトリのコンピュータ・システムは、本 CA のサービスの運営及びリポジトリへのアクセスの提供に使用される。本 CA のコンピュータ・システムは他のコンピュータ・システムとは接続されないスタンドアロンシステムで、本 CA が運用するその他の情報システムとは物理的に隔離されている。本 CA のリポジトリの機器はインターネットに接続されている。両コンピュータ・システムは、物理的セキュリティが確保された場所に置かれる。

本 CA のコンピュータ・システム、またはリポジトリのコンピュータ・システムへのアクセスは、当該システムが設置・運用されている閉鎖エリアに施された物理的なセキュリティ機構により、厳しく制限されている。正当な業務上の理由がある信頼された担当者のみが、当該エリアにアクセスできる。当該エリアのセキュリティ確保を目的とする物理的なアクセス・コントロール・システムは、常時稼動しており、非接触型 IC カード及び生体情報を使ってアクセス権限者を認証する。

本 CA のコンピュータ・システムと本 CA のリポジトリのコンピュータ・システムは、各装置、担当者に最適な温度、湿度を一定に保つことが可能な設備において保護される。

本 CA のコンピュータ・システム及びリポジトリのコンピュータ・システムが設置されている施設には、防水対策を施して、浸水による被害を最低限に抑える。

本 CA のコンピュータ・システム及びリポジトリのコンピュータ・システムが設置されている施設には、適切な地震対策及び電源対策が講じられている。

本 CA のコンピュータ・システム及びリポジトリのコンピュータ・システムのバックアップ媒体は、封印などの改ざん防止の処理が行われる。また、複数名の担当者によるアクセスを必須とする物理的なアクセス制御が施されている。

非電子媒体に記録された情報の廃棄は、裁断又は焼却によって行う。

電子媒体に記録された情報は、初期化した後、更に必要に応じて、物理的に破砕して廃棄する。暗号装置の廃棄は、初期化した後、更に必要に応じて、物理的に破砕して廃棄する。
本 CA のコンピュータ・システム上の情報の廃棄は、ファイル消去によって行う。

10.6 事業継続計画

セコムトラストシステムズのセキュリティ・ポリシに含まれる事業継続方針のもとに、本 CA のサービスにおける災害復旧計画が作成されている。当該計画は、本 CA の重要なサービスを担うコンピュータ・システムの中断、停止につながるような問題が発生した場合に、当該サービスを担当するコンピュータ・システムの問題部分をできる限り早く修復することを目的とするものである。

本 CA のコンピュータ・システムについては、遠隔地に保管している媒体に保存されているシステムの運用に必要なデータのバックアップを使って、速やかにシステムを修復できる。

本 CA のリポジトリのコンピュータ・システムは、主に、証明書、CRL、CPS の公開を行う。リポジトリのコンピュータ・システムについても、システムの運用に必要なデータのバックアップを使って、速やかにシステムを修復できる。リポジトリのコンピュータ・システムの復旧作業時、加入者は、本 CA に連絡することで、同データの情報を得る事が出来る。リポジトリのコンピュータ・システム内のファイル・システムは、定期的にファイルのバックアップを行う。

10.7 各種記録と監査証跡

本 CA の担当者は、本 CA のコンピュータ・システム、本 CA のリポジトリのコンピュータ・システム、本 CA に関連するネットワーク・デバイスの監査証跡やイベント・ログを、手動或いは自動で取得出来る。

11. 証明書ポリシ

証明書ポリシ（以下、「CP」という）は、本 CA が発行する証明書及び本 CA のサービスを信頼し利用するあらゆる加入者及び利用者に適用されるものである。セコムトラストシステムズは本 CA を設立して、電子証明書の発行・管理サービスを提供し、加入者が行う電子署名、本人認証等をサポートする。

CP は、本 CA の証明書によりその信頼性が提供される下位 CA の証明書の発行を希望する加入者への証明書の発行及び管理に適用される。

11.1 本ポリシに固有の認証規定

11.1.1 加入者の種別

CP は、加入者を対象に、本 CA が提供する証明書の発行・管理サービスに適用される。

加入者とは、本 CA から、証明書の発行を受ける下位の CA のことをいう。

11.1.2 加入者の識別名

加入者の識別名は、意味のある名前を用いる。加入者は、以下の英数記号から識別名を申請する事が出来る。本 CA は、加入者から申請された識別名を確認の上、問題がなければ割り当てを行う。

英字	数字	記号
A ～ Z 、a ～ z	0 ～ 9	-.,_()と空白

11.1.3 本人確認方法

加入者は、組織の情報と組織が申請した事を示す情報を本 CA に提出する。本 CA は、提出された加入者の情報をもとに、組織の情報が間違いない事を確認する。また、間違いなく加入者からの申請であること確認する。

11.1.4 本 CA の公開鍵の配布

本 CA の公開鍵は、信頼されているソフトウェアによる配布法や、マイクロソフト・ウィンドウズ、リナックス等で利用可能なダウンロード技術を使用し、本 CA のリポジトリを経由して、加入者及び利用者に配布される。

11.1.5 加入者の鍵の管理

本 CA では、加入者の鍵管理を行わない。

11.1.6 受領後の証明書の公開

加入者に発行された証明書は、加入者による受領後、原則として直ちに本 CA のリポジトリに公開され、効力を発する。

11.1.7 加入者の取消要求

加入者は、自身の証明書の取消しを本 CA に要求できる。本 CA の担当者は、提出された加入者の情報を元に、適正な要求である事を確認する。

11.2 本 CA に固有の証明書のライフサイクル管理

11.2.1 証明書のプロファイル

本 CA は、X.509 に準拠する証明書を発行する。その他の基準に準拠する証明書や、その他の基準に準拠するプロファイルを持つ証明書は認められない。一般的に、加入者に発行される証明書は、マイクロソフトのウィンドウズ、アップルコンピュータのマッキントッシュ、リナックス等のコンシューマーソフトで一般的に使用される証明書とほぼ同じフィールドを持っている。2003 年 8 月 1 日以降に本 CA が発行する証明書には、一定の規則にしたがって増加するシリアルナンバーが表示される。

11.2.2 初期登録

本 CA は、加入者に、(エンティティの識別に使用する)X.500 標準の識別名(Distinguished Name、以下 DN という) を割り当てる。

あらゆる加入者は、本 CA の命名規則に基づいて識別される。

原則として、本 CA のサービスは加入者の正式名称を使用する。加入者の証明書は DN により一意に識別される。

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。

加入者は、秘密鍵を開示する事なく保有する。加入者が秘密鍵を開示する事なく保有している事実は、証明書発行前に加入者が秘密鍵を用いて電子署名を行ったデータを、加入者の公開鍵で検証することによって証明される。

証明書の発行申請時に、加入者は、加入者の公開鍵と加入者の正式名称に関する情報を、本 CA に提供しなければならない。本 CA の担当者は、申請に誤りや欠落情報がないことを確認する。

11.2.3 外部の登録機関

本 CA は、外部の登録機関を使用しない。あらゆる登録作業は、本 CA の担当者が行う。

11.2.4 証明書の発行

本 CA は、申請にかかる処理が問題なく終了した時点で、加入者の証明書を発行する。

証明書のフォーマット、バージョン、有効期間、拡張フィールド、鍵の使用法に関する拡張フィールド等に関する要件は、本 CA によって決定される。加入者と本 CA は、事前に、これらの技術的なパラメータについて合意しているものとする。

11.2.5 証明書の受領

加入者に発行された証明書は、加入者が受領し、内容を確認するまでの間、本 CA が安全な保管場所で管理する。加入者に発行された証明書を加入者が受領した場合、当該証明書はリポジトリに公開される。

11.2.6 証明書の配布

本 CA の行うサービスは、インターネット経由でアクセス可能なリポジトリを設け、管理する。本 CA が加入者に発行し取消されていないもので、かつ有効期間が満了していない証明書、及び、当該証明書に関連する有効な CRL のすべては、リポジトリに公開され、配布される。

11.2.7 証明書の再発行、更新、鍵の更新に伴う発行

証明書の再発行、更新、鍵の更新に伴う発行は、初回と同じ手続きを行う。

11.2.8 証明書の一時停止

本 CA は、加入者の証明書の一時停止を行わない。

11.2.9 証明書の取消し

加入者に発行された証明書は、さまざまな理由で取消される。当該理由には、証明書に含まれる公開鍵に対応する秘密鍵の危殆化、またはそのおそれがある場合や、秘密鍵を使用不能にするようなハードウェアまたはソフトウェアの欠陥等が含まれる。加入者が自身の証明書の取消を希望する場合、加入者は、本 CA にその旨を連絡しなければならない。当該担当者は、取消要求者が本人であることを確かめられる能力を持つものでなければならない。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。申請先は、root1-support@secomtrust.net とする。本 CA は、当該申請の信頼性を確認した後、一定の期間内に当該申請を処理する。取消請求の信頼性は、受領後 72 時間以内に確認される。有効な取消要求に基づく処理は、受領後 7 日以内に完了する。

加入者の不履行等の事由によっては、本 CA の判断によって証明書の取消しを行う事がある。

秘密鍵が危殆化した場合を除く取消要求は、取消しを希望する少なくとも 48 時間前までに、本 CA に行わなければならない。ただし、秘密鍵が危殆化したおそれがある場合、または実際に危殆化した場合、当該問題を発見後、直ちに取消要求を行わなければならない。

本 CA のサービスの証明書取消し方法として、取消要求の信頼性を確認し、CRL を発行・公開することにより、有効期間内の証明書が取消されたことが速やかに通知される。加入者の証明書取消し後、取消された証明書の情報は CRL に記録され、発行される。

11.2.10 証明書取消リストのプロファイル

本 CA は、X.509 に準拠する失効リスト形式で、CRL を発行する。本 CA の CRL は、マイクロソフト・ウィンドウズ、アップルコンピュータ・マッキントッシュ、リナックス等のコンシューマーソフトで一般的に使用されている CRL に準拠する。

11.2.11 証明書のステータス情報

本 CA は、一年ごと及び加入者の証明書の発行・取消を行った場合、その他本 CA が必要と認めた場合に CRL を発行する。

CRL のチェックは、すべての加入者及び利用者の義務である。

本 CA が発行した有効期限が切れた証明書及び CRL のすべてを、アーカイブする。ただし、アーカイブした情報は、通常、加入者及び利用者はアクセスできない。

用語解説

I

ISMS
情報セキュリティマネジメントシステム：Information Security Management System の略。情報セキュリティマネジメントシステム適合性評価制度は、情報システムのセキュリティ管理に対する第三者適合性評価制度である。

W

Webtrust for CA
米国公認会計士協会(ＡＩＣＰＡ)とカナダ勅許会計士協会(ＣＩＣＡ)によって、認証局の信頼性、及び、電子商取引の安全性等に関する内部統制について策定された基準及びその基準に対する認定制度である。

X

X.500
名前及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 の発行者名及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及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。

か～こ

下位 CA
Root CA 以外の認証局で、SECOM Trust.net Root1 CA が署名し発行した証明書に対応する秘密鍵を保有する CA をいう。

鍵ペア
公開鍵暗号方式における秘密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下位の CA 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。秘密鍵に対応する、公開されている鍵。

さ～そ

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。

認証サービス改善委員会

本 CPS の管理、変更の検討、サービスの運用チェック等を行う機関。

た～と

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署名、及び、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。

登録機関

CA の業務のうち、登録業務を行う機関。主な業務は、証明書発行対象者の本人確認、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である。

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、停止、取消し、保管、開示を含む電子認証サービスの提供及び利用にあたっての注意点等を規定するもの。

認証機関（CA）
Certification Authority の略。証明書の発行・更新・取消し、CA 等秘密鍵の生成・保護及び加入者の登録を行う機関。本 CPS 内で、単に CA という場合は証明書の発行業務及び登録業務を含む。

は～ほ

秘密鍵
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。

ま～も

マイナーバージョン番号
CPS 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、CPS 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
CPS 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、CPS 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
CA が発行した証明書等の格納庫である。ユーザ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 CPS も

リポジトリに格納される。

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。

ルート CA

本 CPS でいう SECOM Trust.net Root1 CA は、セコムトラストシステムズが所有し運営する機関で、下位 CA の証明書を発行するルート CA である。下位 CA の頂点として機能する CA である。