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

Version 6.05

2023 年 8 月 28 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	ポリシーOID の追加 全体的に体裁の修正を実施
3.00	2013/11/27	Sha256 の追加に伴い、修正 ポリシーOID の追加 RootCA のリポジトリー情報を追加
4.00	2014/05/29	サーバー認証の利用用途追加に伴い、修正 ポリシーOID の追加
5.00	2017/01/20	ポリシーOID の追加 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
5.01	2020/02/19	サーバー証明書用証明書ポリシーの削除 BR for Code Signing における内容の追加・修正 全体的な文言および体裁の見直し
5.02	2020/03/30	章立ての見直し、および一部「規定しない」の内容追加
5.03	2020/06/15	CA 証明書(sha256)のプロファイルに Extended Key Usage 追加 証明書利用者証明書(sha256)のプロファイルの Extended Key Usage 追加
5.04	2020/07/30	CA 証明書(sha256)の Extended Key Usage から OCSP Signing を削除、OU 変更、CP の URL 変更 証明書利用者証明書(sha256)の OU 変更、CP の URL 変更、AIA の OCSP URL 変更等
5.05	2020/09/29	CRL プロファイルの Reason code を修正
5.06	2021/06/15	電子メールアカウントの認証を追加
6.00	2021/08/03	CA の私有鍵 Security Communication RootCA3 を追加 コードサイニング用証明書ポリシーの公開鍵情報を修正
6.01	2022/06/10	全体的な文言および体裁の見直し
6.02	2022/12/08	「6.1.5 鍵ペアサイズ」にコードサイニング証明書の要件を追加 「6.2.7 暗号モジュールへの私有鍵の格納」にコードサイニ

		ング証明書の要件を追加 「7.1 証明書プロファイル」 「表 7.1-1 CA 証明書(sha1)のプロファイル」 「表 7.1-2 CA 証明書(sha256)のプロファイル」 「表 7.1-3 CA 証明書(sha384)のプロファイル」の修正 「表 7.1-5 証明書利用者証明書(sha256)のプロファイル」の修正
6.03	2023/02/17	「1.1 概要」文言修正 「1.2 文書名と識別」CP/OID 追加、文言修正 「1.4.1 適切な証明書の用途」文言修正 「1.6 定義と略語」定義の追加 「3.2.3 申請者および証明書利用者の認証」文言追加 「3.2.6 相互運用の基準」Root CA の追加 「4.3.1 証明書発行時の処理手続」文言修正 「6.1.1 鍵ペアの生成」文言修正 「6.1.2 証明書利用者に対する私有鍵の交付」文言修正 「6.2.1 暗号モジュールの標準および管理」文言追加 「6.2.7 暗号モジュールへの私有鍵の格納」文言追加 「7.1 証明書プロファイル」文言修正、プロファイル追加 「7.1.3 アルゴリズムオブジェクト識別子」Root CA の追加 「7.2 CRL プロファイル」文言修正、プロファイル追加 「7.3 OCSP のプロファイル」文言修正、プロファイル追加
6.04	2023/05/17	「1.1 概要」を更新 「1.2 文書名と識別」を更新 「1.6 定義と略語」を更新 「2.3 公開の時期または頻度」を更新 「3.2.2 組織の認証」を更新 「3.2.6 相互運用の基準」を更新 「3.2.7 認証する情報の信頼性」を更新 「4.1.2 申請手続および責任」を更新 「4.2.1 本人性確認と認証の実施」を更新 「4.9.1 証明書失効事由」を更新 「4.9.2 証明書の失効申請を行うことができる者」を更新 「4.9.3 失効申請手続」を更新

		「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」を更新 「4.9.7 証明書失効リストの発行頻度」を更新 「4.9.9 オンラインでの失効/ステータス確認の適用性」を更新 「4.9.10 オンラインでの失効/ステータス確認を行うための要件」を更新 「4.9.11 利用可能な失効情報の他の形式」を更新 「4.10.2 サービスの利用可能性」を更新 「5.5.1　アーカイブの種類」を更新 「5.5.2　アーカイブ保存期間」を更新 「5.5.3　アーカイブの保護」を更新 「5.5.4　アーカイブのバックアップ手続」を更新 「5.5.5　記録にタイムスタンプを付与する要件」を更新 「5.5.6　アーカイブ収集システム」を更新 「5.5.7　アーカイブの検証手続」を更新 「5.7.1 事故および危殆化時の手続」を更新 「5.7.2 ハードウェア、ソフトウェアまたはデータが破損した場合の手続」を更新 「5.7.3 私有鍵が危殆化した場合の手続」を更新 「5.7.4 災害後の事業継続性」を更新 「6.1.2 証明書利用者に対する私有鍵の交付」を更新 「6.1.6 公開鍵のパラメーターの生成および品質検査」を更新 「7.1 証明書プロファイル」を更新 「7.1.4 名前形式 」を更新 「7.1.6 CP オブジェクト識別子 」を更新 「7.2 CRL プロファイル」を更新 「7.3　OCSP のプロファイル」を更新
6.05	2023/08/28	「4.9.1 証明書失効事由」を更新 「6.1.2 証明書利用者に対する私有鍵の交付」を更新 「7.1 証明書プロファイル」を更新 「7.3　OCSP のプロファイル」を更新 「9.6.1 認証局の表明保証」を更新

		「9.6.3 申請者および証明書利用者の表明保証」を更新

目次

1. はじめに 1
1.1 概要 1
1.2 文書名と識別 2
1.3 PKI の関係者 2
1.3.1 認証局 2
1.3.2 RA 2
1.3.3 申請者および証明書利用者 3
1.3.4 検証者 3
1.3.5 その他関係者 3
1.4 証明書の用途 3
1.4.1 適切な証明書の用途 3
1.4.2 禁止される証明書の用途 3
1.5 ポリシー管理 3
1.5.1 文書を管理する組織 3
1.5.2 連絡先 4
1.5.3 ポリシー適合性を決定する者 4
1.5.4 承認手続 4
1.6 定義と略語 4
2. 公開とリポジトリーの責任 9
2.1 リポジトリー 9
2.2 証明情報の公開 9
2.3 公開の時期または頻度 9
2.4 リポジトリーへのアクセス管理 9
3. 識別と認証 10
3.1 名前決定 10
3.1.1 名前の種類 10
3.1.2 名前が意味を持つことの必要性 10
3.1.3 証明書利用者の匿名性または仮名性 10
3.1.4 様々な名前形式を解釈するための規則 10
3.1.5 名前の一意性 10
3.1.6 認識、認証および商標の役割 10
3.2 初回の本人確認 10
3.2.1 私有鍵の所持を証明する方法 11
3.2.2 組織の認証 11

3.2.3 申請者および証明書利用者の認証 13
3.2.4 検証されない証明書利用者の情報 14
3.2.5 権限の正当性確認 14
3.2.6 相互運用の基準 14
3.2.7 認証する情報の信頼性 14
3.3 鍵更新申請時の本人性確認と認証 14
3.3.1 通常の鍵更新時における本人性確認と認証 14
3.3.2 証明書失効後の鍵更新時における本人性確認と認証 14
3.4 失効申請時の本人性確認と認証 14
4. 証明書のライフサイクルに対する運用上の要件 15
4.1 証明書申請 15
4.1.1 証明書の申請を行うことができる者 15
4.1.2 申請手続および責任 15
4.2 証明書申請手続 16
4.2.1 本人性確認と認証の実施 16
4.2.2 証明書申請の承認または却下 16
4.2.3 証明書申請の処理時間 17
4.3 証明書の発行 17
4.3.1 証明書発行時の処理手続 17
4.3.2 証明書利用者への証明書発行通知 17
4.4 証明書の受領確認 17
4.4.1 証明書の受領確認手続 17
4.4.2 認証局による証明書の公開 17
4.4.3 他のエンティティに対する認証局の証明書発行通知 18
4.5 鍵ペアおよび証明書の利用 18
4.5.1 証明書利用者の私有鍵および証明書の利用 18
4.5.2 検証者の利用者の公開鍵および証明書の利用 18
4.6 証明書の更新 18
4.6.1 証明書更新の状況 18
4.6.2 証明書の更新申請を行うことができる者 18
4.6.3 証明書の更新申請の処理手続 18
4.6.4 証明書利用者に対する新しい証明書発行通知 18
4.6.5 更新された証明書の受領確認手続 18
4.6.6 認証局による更新された証明書の公開 19
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 19

4.7 証明書の鍵更新 19
4.7.1 鍵更新の状況 19
4.7.2 新しい証明書の申請を行うことができる者 19
4.7.3 鍵更新をともなう証明書申請の処理手続 19
4.7.4 証明書利用者に対する新しい証明書の通知 19
4.7.5 鍵更新された証明書の受領確認手続 19
4.7.6 認証局による鍵更新済みの証明書の公開 19
4.7.7 他のエンティティに対する認証局の証明書発行通知 19
4.8 証明書の変更 19
4.8.1 証明書の変更事由 20
4.8.2 証明書の変更申請を行うことができる者 20
4.8.3 変更申請の処理手続 20
4.8.4 証明書利用者に対する新しい証明書発行通知 20
4.8.5 変更された証明書の受領確認手続 20
4.8.6 認証局による変更された証明書の公開 20
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 20
4.9 証明書の失効と一時停止 20
4.9.1 証明書失効事由 20
4.9.2 証明書の失効申請を行うことができる者 23
4.9.3 失効申請手続 24
4.9.4 失効申請の猶予期間 24
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 24
4.9.6 失効確認の要求 25
4.9.7 証明書失効リストの発行頻度 26
4.9.8 証明書失効リストの発行最大遅延時間 26
4.9.9 オンラインでの失効/ステータス確認の適用性 26
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 26
4.9.11 利用可能な失効情報の他の形式 27
4.9.12 鍵の危殆化に対する特別要件 27
4.9.13 証明書の一時停止事由 27
4.9.14 証明書の一時停止申請を行うことができる者 28
4.9.15 証明書の一時停止申請手続 28
4.9.16 一時停止を継続することができる期間 28
4.10 証明書のステータス確認サービス 28
4.10.1 運用上の特徴 28

4.10.2 サービスの利用可能性 28
4.10.3 オプショナルな仕様 28
4.11 登録の終了 28
4.12 キーエスクローと鍵回復 28
4.12.1 キーエスクローと鍵回復ポリシーおよび実施 29
4.12.2 セッションキーのカプセル化と鍵回復のポリシーおよび実施 29
5. 設備上、運営上、運用上の管理 30
5.1 物理的管理 30
5.1.1 立地場所および構造 30
5.1.2 物理的アクセス 30
5.1.3 電源および空調 30
5.1.4 水害対策 30
5.1.5 火災対策 30
5.1.6 媒体保管 30
5.1.7 廃棄処理 30
5.1.8 オフサイトバックアップ 30
5.2 手続的管理 30
5.2.1 信頼すべき役割 30
5.2.2 職務ごとに必要とされる人数 30
5.2.3 個々の役割に対する本人性確認と認証 31
5.2.4 職務分割が必要となる役割 31
5.3 人事的管理 31
5.3.1 資格、経験および身分証明の要件 31
5.3.2 背景調査 31
5.3.3 教育要件 31
5.3.4 再教育の頻度および要件 31
5.3.5 仕事のローテーションの頻度および順序 31
5.3.6 認められていない行動に対する制裁 31
5.3.7 独立した契約者の要件 31
5.3.8 要員へ提供される資料 31
5.4 監査ログの手続 31
5.4.1 記録されるイベントの種類 31
5.4.2 監査ログを処理する頻度 32
5.4.3 監査ログを保持する期間 32
5.4.4 監査ログの保護 32

5.4.5 監査ログのバックアップ手続 32
5.4.6 監査ログの収集システム 32
5.4.7 イベントを起こした者への通知 32
5.4.8 脆弱性評価 32
5.5 記録の保管 32
5.5.1 アーカイブの種類 32
5.5.2 アーカイブ保存期間 32
5.5.3 アーカイブの保護 32
5.5.4 アーカイブのバックアップ手続 32
5.5.5 記録にタイムスタンプを付与する要件 33
5.5.6 アーカイブ収集システム 33
5.5.7 アーカイブの検証手続 33
5.6 鍵の切り替え 33
5.7 危殆化および災害からの復旧 33
5.7.1 事故および危殆化時の手続 33
5.7.2 ハードウェア、ソフトウェアまたはデータが破損した場合の手続 33
5.7.3 私有鍵が危殆化した場合の手続 33
5.7.4 災害後の事業継続性 33
5.8 認証局または登録局の終了 33
6. 技術的セキュリティ管理 34
6.1 鍵ペアの生成およびインストール 34
6.1.1 鍵ペアの生成 34
6.1.2 証明書利用者に対する私有鍵の交付 34
6.1.3 認証局への公開鍵の交付 34
6.1.4 検証者への CA 公開鍵の交付 35
6.1.5 鍵サイズ 35
6.1.6 公開鍵のパラメーターの生成および品質検査 35
6.1.7 鍵の用途 35
6.2 私有鍵の保護および暗号モジュール技術の管理 35
6.2.1 暗号モジュールの標準および管理 35
6.2.2 私有鍵の複数人管理 36
6.2.3 私有鍵のエスクロー 36
6.2.4 私有鍵のバックアップ 36
6.2.5 私有鍵のアーカイブ 36
6.2.6 私有鍵の暗号モジュールへのまたは暗号モジュールからの転送 36

6.2.7 暗号モジュールへの私有鍵の格納 36
6.2.8 私有鍵の活性化方法 38
6.2.9 私有鍵の非活性化方法 38
6.2.10 私有鍵の破棄方法 38
6.2.11 暗号モジュールの評価 38
6.3 鍵ペアのその他の管理方法 38
6.3.1 公開鍵のアーカイブ 38
6.3.2 私有鍵および公開鍵の有効期間 39
6.4 活性化データ 39
6.4.1 活性化データの生成および設定 39
6.4.2 活性化データの保護 39
6.4.3 活性化データの他の考慮点 39
6.5 コンピューターのセキュリティ管理 39
6.5.1 コンピューターセキュリティに関する技術的要件 39
6.5.2 コンピューターセキュリティ評価 39
6.6 ライフサイクルセキュリティ管理 39
6.6.1 システム開発管理 39
6.6.2 セキュリティ運用管理 39
6.6.3 ライフサイクルセキュリティ管理 40
6.7 ネットワークセキュリティ管理 40
6.8 タイムスタンプ 40
7. 証明書および CRL、OCSP のプロファイル 41
7.1 証明書プロファイル 41
7.1.1 バージョン番号 56
7.1.2 証明書拡張 56
7.1.3 アルゴリズムオブジェクト識別子 56
7.1.4 名前形式 57
7.1.5 名前制約 57
7.1.6 CP オブジェクト識別子 57
7.1.7 ポリシー制約拡張の利用 58
7.1.8 ポリシー修飾子の文法および意味 58
7.1.9 重要な証明書ポリシー拡張の処理の意味 58
7.2 CRL プロファイル 58
7.2.1 バージョン番号 61
7.2.2 CRL 拡張 61

7.3 OCSP のプロファイル 61
7.3.1 バージョン番号 65
7.3.2 OCSP 拡張 65
8. 準拠性監査と他の評価 66
8.1 監査の頻度 66
8.2 監査人の身元／資格 66
8.3 監査人と被監査部門の関係 66
8.4 監査で扱われる事項 66
8.5 不備の結果としてとられる処置 66
8.6 監査結果の開示 66
9. 他の業務上および法的事項 67
9.1 料金 67
9.1.1 証明書の発行または更新にかかる料金 67
9.1.2 証明書のアクセス料金 67
9.1.3 失効またはステータス情報のアクセス料金 67
9.1.4 他サービスの料金 67
9.1.5 返金ポリシー 67
9.2 財務的責任 67
9.2.1 保険の補償 67
9.2.2 その他の資産 67
9.2.3 エンドエンティティの保険または保証範囲 67
9.3 企業情報の機密性 67
9.3.1 機密情報の範囲 67
9.3.2 機密情報の範囲外の情報 67
9.3.3 機密情報を保護する責任 68
9.4 個人情報の保護 68
9.4.1 個人情報保護方針 68
9.4.2 個人情報として扱われる情報 68
9.4.3 個人情報とみなされない情報 68
9.4.4 個人情報を保護する責任 68
9.4.5 個人情報の使用に関する通知と同意 68
9.4.6 司法または行政手続に沿った情報開示 68
9.4.7 その他の情報開示条件 68
9.5 知的財産権 68
9.6 表明保証 69

9.6.1 認証局の表明保証 69
9.6.2 RA の表明保証..... 71
9.6.3 申請者および証明書利用者の表明保証 71
9.6.4 検証者の表明保証 73
9.6.5 他の関係者の表明保証 74
9.7 無保証 74
9.8 責任の制限 74
9.9 補償 74
9.10 有効期間と終了 74
9.10.1 有効期間 74
9.10.2 終了 75
9.10.3 終了の効果と効果継続 75
9.11 関係者間の個別通知と連絡 75
9.12 改訂 75
9.12.1 改訂手続 75
9.12.2 通知方法および期間 75
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 75
9.13 紛争解決手続 75
9.14 準拠法 76
9.15 適用法の遵守 76
9.16 雑則 76
9.16.1 完全合意条項 76
9.16.2 権利譲渡条項 76
9.16.3 分離条項 76
9.16.4 強制執行条項 77
9.16.5 不可抗力 77
9.17 その他の条項 77

1. はじめに

1.1 概要

セコムパスポート for Member 2.0 PUB 証明書ポリシー（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ーを規定するものである。本 CA の運用維持に関する諸手続については、セコム電子認証基盤認証運用規程（以下「CPS」という）に規定する。

本 CA から証明書の発行を受ける者は、証明書の発行を受ける前に自己の利用目的と本 CP、および CPS とを照らし合わせて評価し、本 CP、および CPS を承諾する必要がある。

本 CP は、本 CA に関する技術面、運用面の発展や改良にともない、それらを反映するために必要に応じ改訂されるものとする。

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

コードサイニング証明書を発行する場合は、https://www.cabforum.org/で公開される CA/ Browser Forum の Baseline Requirements for the Issuance and Management of Code Signing Certificates（以下「Baseline Requirements (Code Signing)」という）および Baseline Requirements for the Issuance and Management of Publicly -Trusted Certificates（以下「Baseline Requirements」という）の最新版に準拠する。

S/MIME 証明書を 2023 年 9 月 1 日以降に発行する場合は、https://www.cabforum.org/で公開される Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates（以下「Baseline Requirements (S/MIME)」という）の最新版に準拠する。

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 と Baseline Requirements の間に矛盾がある場合、Baseline Requirements が本 CP に優先して適用される。

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 証明書ポリシー」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 および参照する 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ー (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ー (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ー (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ー (署名アルゴリズム：SHA256)	1.2.392.200091.100.381.5
コードサイニング用証明書ポリシー (署名アルゴリズム：SHA256)	1.2.392.200091.100.381.8
OCSP レスポンダー用証明書ポリシー (署名アルゴリズム：SHA256)	1.2.392.200091.100.381.9
AATL ドキュメントサイニング用証明書ポリシー	1.2.392.200091.100.382.1
S/MIME 用証明書ポリシー	1.2.392.200091.100.383.1
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、本 CA の私有鍵の管理、証明書の発行、失効、CRL（Certificate Revocation List：証明書失効リスト）の開示、OCSP（Online Certificate Status Protocol）レスポンダーによる証明書ステータス情報の提供、およびリポジトリーの維持管理等を行う。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。

1.3.2 RA

RA は、LRA（Local Registration Authority）および証明書利用者の審査ならびに証明書の発行および失効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。

LRAは、RAに代わり、証明書利用者の実在性確認および本人性確認の審査ならびに証明書の発行および失効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または団体がその役割を担うことができる。

またLRAは、RAと同様に本CPに定める事項に従うものとする。なおクライアント用証明書ポリシーまたはデータ署名用証明書ポリシーが適用される場合にのみ、LRAが業務を行う場合がある。

1.3.3 申請者および証明書利用者

申請者とは、RA またはLRAに対し、証明書の発行や失効に関する申込を行う個人、組織または団体等をいい、また証明書利用者とは、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、組織または団体等をいう。

1.3.4 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、組織または団体等をいう。

1.3.5 その他関係者

他の関係者とは、監査人や、セコムとの間でサービス契約等が存在する企業や組織、そのシステムインテグレーションを行う業者などが含まれる。

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、証明書に記載される Key Usage および Extended Key Usage フィールドで指定された目的に使用することができる。

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 ポリシー管理

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@secom.co.jp

ウェブサイト：https://www.secomtrust.net/

加入者、依拠当事者、アプリケーションソフトウェアサプライヤー、その他の第三者は、私有鍵の危殆化の疑い、証明書の誤用、あるいはその他の種類の詐欺、危殆化、誤用、不適切 な行為、または証明書に関連するその他の事項について、上記の連絡先に報告することができる。本 CA では、失効する必要があると判断した場合、証明書を失効する。

1.5.3 ポリシー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

法的またはその他の事由により、履歴の保存を目的に取得する情報のことをいう。

エスクロー

第三者に預けること（寄託）をいう。

エンタープライズ RA

本 CA とは無関係の組織の従業員または代理人で、その組織への証明書の発行を承認するもの。

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。

クロス証明書

2 つのルート CA 間の信頼関係を確立するために使用される証明書。

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

作成したプログラムファイル等（以下「コード」という）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。

コードの利用者は、この電子署名を検証することにより、コードの作成者、発行者、有効期限等の情報を得ることができ、また、コード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ーの決定等を行う意思決定組織。

メールボックス認証

主体者の識別名(DN)がメールアドレスまたはシリアルナンバー属性に制限された S/MIME 証明書の認証方式。

メールボックスアドレス

メールアドレスのこと。メールの送信先のユーザーまたは場所を識別する文字列（RFC5321 より）。

メールボックスフィールド

主体者のメールアドレスを S/MIME 証明書の subjectAltName 拡張の rfc822Name に含むもの。

リポジトリー

CA 証明書および CRL 等を格納し公表するデータベースのことをいう。

A～Z

AATL（Adobe Approved Trust List）

Adobe® Acrobat®または Acrobat® Reader®で署名済みの文書を開く際、信頼されるデジタル署名を作成できるプログラム。

Baseline Requirements

CA/Browser Forum が証明書の発行・管理に関する基本要件を定めた文書のことをいう。

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、リポジトリーの維持・管理、および証明書利用者の登録等を行う主体のことをいう。

CA/Browser Forum

認証局とインターネット・ブラウザベンダーによって組織され、証明書の要件を定義し、標準化する活動をしている非営利団体組織である。

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。

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。

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。

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。

RA（登録局）（Registration Authority）：登録機関

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。

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。

S/MIME

Secure MIME (Multipurpose Internet Mail Extensions)の略称。電子メールの公開鍵暗号方式による電子署名と暗号化に関する標準規格。電子署名の場合は、送信者の私有鍵で署名し、受信者は送信者の公開鍵で署名検証を行う。暗号化の場合は、受信者の公開鍵で暗号化し、受信者の私有鍵で復号する。

WebTrust Principles and Criteria for Certification Authority (WebTrust for CA)

CPA Canada によって、認証局の信頼性、および、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およびその基準に対する認定制度である。

WebTrust Principles and Criteria for Certification Authorities - Code Signing Baseline Requirements (WebTrust for CA - Code Signing Baseline Requirements)

CPA Canada によって、認証局がコードサイニング証明書を発行するにあたっての審査、証明書に関する規定について策定された監査基準である。

X.500

ネットワーク上での分散ディレクトリサービスに関する、コンピュータネットワーク標準規格のシリーズのことをいう。

2. 公開とリポジトリーの責任

2.1 リポジトリー

セコム は、証明書利用者および検証者が、24時間365日CRL、本CPおよびCPS等を参照できるようリポジトリーを維持管理する。また、証明書利用者および検証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レスポンダーを維持管理する。ただし、保守等により、一時的にリポジトリーおよびOCSPレスポンダー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ーに格納し、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 の下位証明書
- 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レスポンダーにより証明書利用者および検証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 公開の時期または頻度

本 CA は、Baseline Requirements(Code Signing および S/MIME)の最新バージョンをどのように実施するかを詳細に記述した CP および CPS の策定、導入、施行、年次更新を行うものとする。本 CA は、CP および CPS に変更が加えられていない場合でも、バージョン番号を増やし、変更履歴を追加することにより、Baseline Requirements(Code Signing および S/MIME)への準拠を示す。

2.4 リポジトリーへのアクセス管理

本 CA はリポジトリーを読み取り専用の形で公開するものとする。本 CA では、許可された CA 管理者のみがリポジトリーの追加、削除、変更、公開などの操作を実行できる。

3. 識別と認証

3.1 名前決定

3.1.1 名前の種類

本 CA が発行する証明書は、X.509 規格、RFC5280 規格および Baseline Requirements の要求事項を満たし、証明書所有者に割り当てられる識別名は X.500 の識別名形式に従い設定する。

3.1.2 名前が意味を持つことの必要性

本 CA が発行する証明書に用いられる識別名は、証明書利用者を識別するために使用し、有意義なものとする。

3.1.3 証明書利用者の匿名性または仮名性

本 CA が発行する証明書の組織名およびコモンネームには、匿名や仮名での登録は行わない。なお、Baseline Requirements (Code Signing)で定められていない各証明書ポリシーにおいては、証明書を管理するための数字や文字列などを登録する場合もある。

3.1.4 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。

3.1.5 名前の一意性

本 CA では、発行された証明書が、主体者の識別名(DN)に含まれる情報により、証明書の所有者を一意に識別できることを保証する。証明書のシリアルナンバーは、CSPRNG で生成した乱数を含むシリアルナンバーとする。本 CA 内で割り当てられたシリアルナンバーは一意である。

3.1.6 認識、認証および商標の役割

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失効する権利を有する。

3.2 初回の本人確認

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

LRA または組織、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 または組織、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、提出された公的書類は返却もしくは破棄する。申込書等を受領していた場合、セコムはこれを破棄する。

[S/MIME 証明書]

2023 年 8 月 31 日以前に本 CA が S/MIME 証明書を発行する際、以下に記載する方法を使用して、証明書に登録される電子メールアドレスに関連付けられた電子メールアカウントを制御しているか、または電子メールアカウントの所有者から、アカウント所有者の代理として申請することを承認されているかを認証する。なお、本項で記載するランダム値は、本 CA が生成する 112 ビット以上の乱数から成るものとし、その生成より 30 日間のレスポンス確認の使用に有効なものとする。

1. 本 CA は、電子メールアドレスに含まれる@以下のドメインにおいて、WHOIS レジストリサービスに登録された登録担当者（Registrant）情報を参照し、申請者がドメインを所有していること（申請者とドメイン所有者が同一組織であること）を確認する。なお、ドメインを第三者組織が所有していることを確認した場合、ドメインの所有者より、所有者組織の押印をした「ドメイン名使用承諾書」を本 CA に提出することで、

電子メールアカウントの利用が承認されていることを確認する。

2. WHOIS レジストリサービスに登録されたドメイン連絡先へ電子メールにてランダム値を送信し、ランダム値が含まれた確認応答を受け取ることによって、電子メールアカウントの所有者からアカウントの利用が承認されていることを確認する。

3. ローカル部は'admin'、 'administrator'、 'webmaster'、 'hostmaster'、または'postmaster'とし、電子メールアドレスに含まれる@以下のドメインで作成した電子メールアドレスにランダム値を送信して、ランダム値が含まれた確認応答を受け取ることによって、電子メールアカウントの所有者からアカウントの利用が承認されていることを確認する。

4. 要求トークンまたはランダム値がファイルの内容に含まれていることを検証することにより、電子メールアカウントの制御を確認する。本 CA は承認済みポートを介してアクセスし、「http（または https）:// [電子メールアドレスに含まれる@以下のドメイン] /.well-known/pki-validation」ディレクトリの配下にランダム値が配置されていること、リクエストから正常な HTTP または HTTPS 応答を受信することを確認する。

5. 電子メールアドレスに含まれる@以下のドメイン（先頭にアンダースコア文字で始まるラベルを接頭語に持つものも含まれる）のいずれかの、DNS CNAME、TXT または CAA レコード内のどちらかに、ランダム値か申請トークンがあることを確認することで、電子メールアカウントの制御を確認する。

2023 年 9 月 1 日以降に本 CA が Baseline Requirements (S/MIME)に準拠する S/MIME 証明書を発行する際、本 CA は申請者が証明書で参照されているすべてのメールボックスフィールドに関連付けられたメールアカウントを管理していること、またはアカウント所有者に代わって行動することをメールアカウント所有者から許可されていることを確認する。本 CA は、メールボックスの承認または制御の認証を第三者に委任しない。

本 CA の CP および CPS では、本 CA がこの認証を実行するために採用する手順を指定する。本 CA は、発行された証明書のすべてのドメインまたはメールアドレスを認証するために、Baseline Requirements または Baseline Requirements (S/MIME)の関連するバージョン番号を含む、どの検証方法が使用されたかの記録を保持する。

1. 本 CA は、エンタープライズ RA などの申請者が、証明書で使用されるメールボックスアドレスのドメイン部分の管理権限を確認することによって、メールアカウント所有

者によってアカウント所有者の代理として行動する権限を与えられていることを確認する。本 CA は、この認証を実行するために Baseline Requirements 3.2.2.4 で承認された方法のみを使用する。申請者には、申請者の親会社、子会社、または関連会社が含まれる。(Baseline Requirements (S/MIME) 3.2.2.1 Validating authority over mailbox via domain)

2. 本 CA は、メールでランダム値を送信し、そのランダム値を用いた確認応答を受信することにより、証明書に含まれる各メールボックスフィールドに対する申請者の管理権限を確認する。各メールボックスアドレスに対する制御は、一意のランダム値を使用して確認する。ランダム値は、認証されるメールアドレスにのみ送信し、他の方法で共有しない。ランダム値は、各メールで一意とする。ランダム値は、作成から 24 時間以内に確認応答で使用する場合に限り有効である。(Baseline Requirements (S/MIME) 3.2.2.2 Validating control over mailbox via email)

3. 本 CA は、メールボックスアドレスに配信されるメッセージの宛先となる SMTP FQDN の制御を確認することにより、証明書に含まれる各メールボックスフィールドに対する申請者の制御を確認する。SMTP FQDN は、RFC 5321 セクション 5.1 で定義されているアドレス解決アルゴリズムを使用して識別し、このアルゴリズムは、特定のメールボックスアドレスに対してどの SMTP FQDN が信頼できるかを決定する。複数の SMTP FQDN が検出された場合、本 CA は RFC 5321 セクション 5.1 の選択プロセスに従って SMTP FQDN の制御を認証する。MX レコード RDATA のエイリアスは、この認証メソッドに使用しない。(Baseline Requirements (S/MIME) 3.2.2.3 Validating applicant as operator of associated mail server(s))

3.2.3 申請者および証明書利用者の認証

セコムは、国や地方公共団体が発行する公的書類、セコムが信頼する第三者による調査またはそのデータベース、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行う。

クライアント用証明書ポリシーおよびデータ署名用証明書ポリシーの証明書の発行に際して、申請者および証明書利用者の審査は、別途セコムが定める約款等や、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われる場合がある。

AATL ドキュメントサイニング用証明書ポリシーの証明書の発行に際して、次の方法を使用する。組織に所属する個人の認証は、代表者または代表者より委任された者に対し、本 CA が実在性について確認を行う。代表者または代表者より委任された者は、対面で個人を身分証明書と照合し一致することを確認した者とする。審査に使用した情報は、本 CA

であらかじめ定めた期間内であれば、再利用できる。

3.2.4 検証されない証明書利用者の情報

セコムは、識別名に含まれる証明書利用者の商号や名称、所在地など証明書の発行に必要な情報を「3.2.2 組織の認証」および「3.2.3 申請者および証明書利用者の認証」で検証する。なお、サービスの提供上、請求先情報などの事務手続きに必要な情報の提供を求めることがある。

3.2.5 権限の正当性確認

申請者の権限の正当性確認は、「3.2.2 組織の認証」または「3.2.3 申請者およ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。

3.2.6 相互運用の基準

本 CA は、Security Communication RootCA1、Security Communication RootCA2、Security Communication RootCA3、SECOM RSA Root CA 2023 および SECOM Document Signing RSA Root CA 2023 より片方向相互認証証明書を発行されている。

本 CA は、本 CA が信頼関係の確立を手配または受諾した場合に、本 CA をサブジェクトとして識別するすべてのクロス証明書（発行元のクロス証明書）を開示する。

3.2.7 認証する情報の信頼性

証明書要求を認証するために認証する情報に依存する前に、本 CA は信頼できる情報元としての適合性を認証するものとする。

3.3 鍵更新申請時の本人性確認と認証

3.3.1 通常の鍵更新時における本人性確認と認証

「3.2.3 申請者および証明書利用者の認証」および「3.2.5 権限の正当性確認」と同様とする。

3.3.2 証明書失効後の鍵更新時における本人性確認と認証

「3.2.3 申請者および証明書利用者の認証」および「3.2.5 権限の正当性確認」と同様とする。

3.4 失効申請時の本人性確認と認証

「3.2.3 申請者および証明書利用者の認証」および「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 または組織、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。

4.1.2 申請手続および責任

証明書の発行申請を行うにあたり、本 CP および CPS の内容を承諾したうえで申請を行うものとする。また、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。

[S/MIME 証明書]

S/MIME 証明書の発行に際して、本 CA は申請者から以下すべての文書を取得する。

1. 証明書要求。
2. 締結された加入者契約、利用規約。

証明書要求および加入者契約、利用規約は、本 CA が規定する形式であり、本 CP「9.6.3 申請者および証明書利用者の表明保証」を含む Baseline Requirements に準拠しているものとする。本 CA は、Baseline Requirements を満たすために必要であると本 CA が判断した場合、追加の文書を取得する。

証明書要求には、申請者または申請者の代理人による証明書発行の要求と、申請者または申請者の代理人による証明書のすべての情報が正確であることの証明が含まれているものとする。

本 CP「4.2.1 本人性確認と認証の実施」に規定された認証再利用期間を条件として、1 つの証明書要求で複数の証明書を同じ申請者に発行することが可能である。ただし、各証明書は、申請者に代わって適切な申請者代表者が署名した有効で最新の証明書要求によってサポートされている必要がある。

本 CA は、次の場合をすべて満たすときに、以前に認証された証明書要求に依拠して、代わりの証明書を発行することができる。

1. 参照される、以前に発行された証明書が失効されていない。
2. 代わりの証明書の有効期限が参照される以前の証明書と同じ。

3. 証明書の主体者識別名の情報が、参照される以前の証明書と同じ。

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 または組織、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。

[S/MIME 証明書]

S/MIME 証明書の申請者情報には、subjectAltName 拡張に少なくとも 1 つのメールボックスフィールドを含める必要がある。

本 CA は、本 CP「3.2 初回の本人確認」に従って実行され完了した認証、裏付けとなる証拠を以下の範囲内で再利用することができる。

メールボックスの承認または制御の認証:

「Baseline Requirements (S/MIME) 3.2.2.1 Validating authority over mailbox via domain」または「Baseline Requirements (S/MIME) 3.2.2.3 Validating applicant as operator of associated mail server(s)」に従って完了したメールサーバーの制御の認証は、証明書を発行する 398 日前までに取得する。

「Baseline Requirements (S/MIME) 3.2.2.1 Validating authority over mailbox via domain」に規定されている Baseline Requirements に変更が加えられた場合、本 CA は、バロットに特別な指示がない限り、このセクションに記載されている期間、完了した認証、裏付けとなる証拠を引き続き再利用することができる。

「Baseline Requirements (S/MIME) 3.2.2.2 Validating control over mailbox via email」に従ったメールボックス管理の認証は、証明書を発行する 30 日前までに取得する。

4.2.2 証明書申請の承認または却下

本 CA または LRA は、審査の結果、承認を行った申請について証明書を発行する。

また、すべての項目の審査が正常に完了しない証明書の申請は却下できるものとし、以下理由を含むものは却下とする。

・以前に拒否された、または以前に契約の条項に違反していた申請者または証明書利用者の証明書
・フィッシングやマルウェア、その他の詐欺的使用の疑いがある、あるいは懸念される

場合

4.2.3 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、すみやかに LRA、証明書利用者また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。

ルート CA による下位 CA 証明書発行では、証明書への署名操作を実行するために、本 CA によって承認された個人(つまり、CA システムオペレーター、システム責任者、または PKI 管理者)に対し、直接コマンドを実行し、慎重に発行する。

コードサイニング用証明書ポリシーの証明書発行に際して、本 CA は証明書発行前にリンティング機能により発行する証明書の形式が Baseline Requirements に準拠しているかどうか確認し、要件を満たしていない場合は発行拒否している。

本 CA は、証明書を直接発行させることができるすべてのアカウントに対して、多要素認証を実施するものとする。

本 CA では、有効期限、禁止事項またはコードによる制限回避のため、証明書の notBefore の日付をさかのぼることはしない。

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 LRA、証明書利用者または申請者に配付する。証明書利用者の私有鍵を本 CA が生成する場合は、郵送、電子メール、手交等の方法により、私有鍵と 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 または証明書利用者からの受領の報告を受けた場合、もしくは本 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 また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。

4.4.3 他のエンティティに対する認証局の証明書発行通知

本 CA は、証明書申請時に登録された者以外への証明書発行通知は行わない。

4.5 鍵ペアおよび証明書の利用

4.5.1 証明書利用者の私有鍵および証明書の利用

証明書利用者の私有鍵および証明書の利用については、「1.4.1 適切な証明書の用途」および約款等に従う。また証明書利用者は、「1.4.1 適切な証明書の用途」および約款等に記載された用途に対して、当該証明書およ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および証明書の利用

検証者は、証明書利用者の公開鍵および証明書を使用し、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 および 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 証明書更新の状況

規定しない。

4.6.2 証明書の更新申請を行うことができる者

規定しない。

4.6.3 証明書の更新申請の処理手続

規定しない。

4.6.4 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 証明書の鍵更新

4.7.1 鍵更新の状況

鍵更新をともなう証明書の発行は、証明書の有効期限が満了する場合または鍵の危殆化にともない証明書の失効を行った場合等に行われる。

4.7.2 新しい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 鍵更新をともなう証明書申請の処理手続

「4.3.1 証明書発行時の処理手続」と同様とする。

4.7.4 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。

4.7.7 他のエンティティに対する認証局の証明書発行通知

「4.4.3 他のエンティティに対する認証局の証明書発行通知」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、すみやかに変更に関する申請を行わなければならない。変更にともなう手続は、初回発行時の手続と同様とする。また、証明書変更後は、すみやかに変更前の証明書の失効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。変更前の証明書の失効は、「4.9.3 失効申請手続」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 証明書の失効と一時停止

4.9.1 証明書失効事由

証明書利用者は、次の事由が発生した場合、すみやかに証明書の失効申請を行わなければならない。

- 証明書記載情報に変更があった場合
- 私有鍵の盗難、紛失、漏洩、不正利用等により私有鍵が危殆化したまたは危殆化のおそれがある場合
- 証明書の内容、利用目的が正しくない場合
- 証明書の利用を中止する場合

また、セコムは、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、関連する契約または法律に基づく義務を履行していない場合
- 契約違反その他の事由によりセコムから証明書の発行拒否または失効を受けたことがあると判明した場合
- 証明書利用者および本 CA の私有鍵が危殆化したまたは危殆化のおそれがあると判断した場合
- 証明書が本 CP または CPS に準拠して発行されていないことを認識した場合
- 本 CP に記載する適切な用途以外の用途で証明書が使用された、またはセコムとの契約等で示された目的以外の目的で証明書が使用された、あるいは証明書が他の方法で悪用されていることを認識した場合
- 証明書に記載されたメールアドレスの使用が法的に許可されなくなったことを示す状況について通知を受けるか、またはその他の方法で認識した場合
- 証明書に含まれる情報の変更を認識した場合
- 証明書利用者の証明書へ不正アクセスされたことを認識した場合
- 証明書を用いて疑わしいコードへ署名されたことを認識した場合
- S/MIME 証明書が Mozilla Root Store Policy または Apple Root Certificate Program の最新バージョンに違反して発行された場合
- セコム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

[コードサイニング証明書]

以下の 1 つ以上が発生した場合、本 CA は 24 時間以内に証明書を失効する。

1. 加入者が、本 CA に対して証明書を失効するよう書面で要求した場合。
2. 加入者が、本 CA に元の証明書要求が承認されておらず、過去にさかのぼって承認しないことを通知した場合。
3. 本 CA が、証明書内の公開鍵に対応する加入者の私有鍵が鍵の危殆化を受けたという証拠を入手した場合。
4. 本 CA が、証明書内の公開鍵に基づいて加入者の私有鍵を簡単に計算できる実証済みの方法を認識した場合。
5. 本 CA が、加入者の私有鍵を危殆化にさらす実証済みの方法、または私有鍵の生成に使用された特定の方法に欠陥があるという明確な証拠があることを認識した場合。
6. 本 CA が、証明書が疑わしいコードの署名に使用されたという合理的な確証を持っている場合。

本 CA は、以下の 1 つ以上が発生した場合、24 時間以内に証明書を失効するべきであり、5 日以内に証明書を失効する。

7. 証明書が Baseline Requirements (Code Signing)6.1.5 および 6.1.6 の要件に準

拠していない場合。

8. 本 CA が、証明書が悪用されたという証拠を入手した場合。
9. 本 CA が、加入者が加入者契約または利用規約に基づく 1 つ以上の重要な義務に違反したことを認識した場合。
10. 本 CA が、証明書に含まれる情報の重大な変更を認識した場合。
11. 本 CA が、証明書が Baseline Requirements (Code Signing)または CA の CP/CPS に従って発行されていないことを認識した場合。
12. 本 CA が、証明書に含まれる情報のいずれかが不正確であると判断したか、それを認識した場合。
13. 本 CA が CRL/OCSP リポジトリーの維持を継続する取り決めを行わず、Baseline Requirements (Code Signing)に基づいて証明書を発行する CA の権利が、、期限切れ、失効または終了した場合。
14. 失効が本 CA の CP/CPS によって要求された場合。

本 CA は、即時失効がエコシステムに大きな悪影響を与える可能性がある場合、アプリケーションソフトウェアサプライヤーの要求に基づいて失効を遅らせることができる。

[S/MIME 証明書]

本 CA は、次の 1 つ以上が発生した場合、24 時間以内に加入者証明書を失効させるものとする。

1. 加入者が書面で本 CA に証明書の失効を要求している場合。
2. 加入者が CA に対し、元の証明書要求が承認されていなかったこと、および遡及的に承認を許可しないことを通知した場合。(CRLReason #9, privilegeWithdrawn [証明書を利用する権利の撤回])。
3. 本 CA が、加入者の証明書内の公開鍵に対応する私有鍵が危殆化された証拠を得た場合 (CRLReason #1, keyCompromise [私有鍵の危殆化])。
4. 本 CA が、証明書の公開鍵(Debian の弱い鍵など。https://wiki.debian.org/SSLkeys を参照) に基づいて加入者の私有鍵を簡単に計算できる、実証済みまたは証明された方法を認識した場合 (CRLReason #1, keyCompromise [私有鍵の危殆化])。
5. 本 CA が、証明書内の電子メールアドレスのドメイン承認またはメールボックス制御の認証に依存してはならないという証拠を取得した場合。 (CRLReason #4, superseded [証明書の破棄])

本 CA は、以下のいずれかが発生した場合、24 時間以内に加入者証明書を失効するべきであり、5 日以内に証明書を失効する。

1. 証明書が本CP「6.1.5 鍵サイズ」および本CP「6.1.6 公開鍵のパラメーターの生成および品質検査」の要件に準拠しなくなった場合 (CRLReason #4, superseded [証明書の破棄])。
2. 本CAが証明書の不正使用の証拠を得た場合 (CRLReason #9, privilegeWithdrawn [証明書を利用する権利の撤回])。
3. 加入者が加入者契約または利用規約に基づく重大な義務の1つ以上に違反していることを本CAが知り得た場合 (CRLReason #9, privilegeWithdrawn [証明書を利用する権利の撤回])。
4. 本CAが、証明書での電子メールアドレスまたはFQDNの使用が法的に許可されなくなったことを示す状況を知り得た場合(たとえば、裁判所または仲裁人が電子メールアドレスまたはドメイン名を使用する権利を取り消した、加入者間の関連ライセンスまたはサービス契約が終了した、またはアカウント所有者が電子メールアドレスまたはドメイン名のアクティブなステータスを維持できなかったなど)(CRLReason #5, cessationOfOperation [証明書の運用停止])。
5. 本CAが、証明書に含まれている情報の重大な変更を知り得た場合 (CRLReason #9, privilegeWithdrawn [証明書を利用する権利の撤回])。
6. 証明書がBaseline Requirements (S/MIME)またはCAのCP/CPSに従って発行されなかったことを本CAが知り得た場合 (CRLReason #4, superseded [証明書の破棄])。
7. 証明書に表示されている情報のいずれかが不正確であると、本CAが判断または知り得た場合(CRLReason #9, privilegeWithdrawn [証明書を利用する権利の撤回])。
8. Baseline Requirements S/MIME)に基づいて証明書を発行するためのCAの権利が期限切れ、失効、または終了となった場合。(本CAがCRL/OCSPリポジトリーの保守を継続するための手配を済ませている場合を除く)(CRLReason "unspecified (0)" [未定義]の場合、CRL に reasonCode 拡張が提供されない)
9. 本CAのCP/CPSによって失効が必要になった場合(CRLReason "unspecified (0)" [未定義]の場合、CRL に reasonCode 拡張が提供されない)。
10. 本CAに、加入者の私有鍵を危殆化させる実証済みまたは証明済みの方法、または私有鍵の生成に使用された特定の方法に欠陥があるという明確な証拠がある場合。(CRLReason #1, keyCompromise [私有鍵の危殆化])

4.9.2 証明書の失効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。

[コードサイニング証明書]

本CAは、マルウェア対策組織、加入者、署名検証者、アプリケーションソフトウェア

サプライヤー、およびその他のサードパーティに対して、疑わしい私有鍵の危始化、証明書の誤用、疑わしいコードへの署名に使用される証明書、乗っ取り攻撃、またはその他の種類の詐欺、危殆化、誤用、不適切な行為、または証明書に関連するその他の問題の、報告方法に関する明確な手順を提供する。本 CA は、Web サイトで手順を公開する。

[S/MIME 証明書]

加入者、RA、発行 CA が失効手続きを開始できる。加えて、加入者、署名検証者、アプリケーションソフトウェアサプライヤー、およびその他の第三者は、証明書失効に関する妥当な根拠となる証明書問題レポートを発行 CA に提出できる。

4.9.3 失効申請手続

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失効申請を行う。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失効申請を行う。

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失効申請を行う。

本 CA は、失効要求を受け入れ、問い合わせに対応する機能を 24 時間 365 日体制で維持する。

4.9.4 失効申請の猶予期間

証明書利用者は、証明書失効事由が発生してからすみやかに失効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すみやかに本 CA に対して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

本 CA は、有効な失効申請を受け付けてからすみやかに証明書の失効処理を行い、CRL へ当該証明書情報を反映させる。

[コードサイニング証明書]

本 CA は、マルウェア対策組織、アプリケーションソフトウェアサプライヤー、および法執行機関とコミュニケーションを取り、悪意のあるコード、詐欺、またはその他の違法行為に署名するために使用される証明書の失効を要求するレポートなど、優先度の高い証明書の問題レポートに対応するために、24 時間 365 日の継続的な能力を維持する。

本 CA は、本 CA または下位 CA によって発行された証明書で署名された疑わしいコード

に関する通知の受信を確認しなければならない。

本 CA は、受領から 24 時間以内に証明書の問題報告の調査を開始し、少なくとも次の基準に基づいて、失効またはその他の適切な措置を保証するかどうかを決定する。

1. 疑わしい問題の性質（アドウェア、スパイウェア、マルウェア、ソフトウェアのバグなど)。
2. 特定の証明書または加入者について受け取った証明書問題レポートの数。
3. レポートを作成するエンティティ（例えば、マルウェア対策組織または法執行機関からの通知は、匿名の苦情よりも重要なものとして扱う)。
4. 関連する法律。

証明書を失効させる場合、本 CA は、有効な署名付きコードへの失効の影響を軽減する目的で失効が発生する日付を推定するために加入者と連携する。危始化事象が発生の場合、この日付は危殆化の疑いのある最も早い日付を採用する。

[S/MIME 証明書]

証明書問題レポートを受領してから 24 時間以内に、本 CA は証明書問題レポートに関する事実と状況の調査を開始し、加入者と証明書問題レポートを提出した両者の見分に基づく予備調査報告書を提出する。事実と状況のレビュー後、本 CA は加入者、証明書問題レポートを報告した事業者、または他の失効関連の通知を報告する者と協力し、証明書を失効させるか否か、もしそうなら、本 CA が証明書を失効させる日時を決定する。証明書問題レポートまたは失効関連告知の受領から失効までの期間は、セクション 4.9.1.1 に記載された時間枠を超えないものとする。本 CA が選択した日付は、次の基準を考慮する。

1. 申し立てられた問題の性質(範囲、状況、重大度、規模、被害リスク）。
2. 失効の結果（加入者と認証者への直接的そして付随的影響)。
3. 特定の証明書または加入者に関して受領した証明書問題レポートの数。
4. 苦情を申し立てる事業体（たとえば、法執行機関からの要請には、より高い優先度で対処する)。
5. 関連法規。

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。また、コードサイニング用証明書ポリシーで発行する証明書については、OCSP レスポンダーの URL についても記載をする。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、リポジトリーに掲載している CRL または OCSP レスポンダーにより確認する。

4.9.7 証明書失効リストの発行頻度

本 CA が CRL を発行する場合、本 CA は少なくとも 7 日に一度は CRL を更新・再発行し、nextUpdate フィールドの値は thisUpdate フィールドの値よりも 10 日以上先にしないものとする。

4.9.8 証明書失効リストの発行最大遅延時間

本 CA は、証明書の失効を行ってから、即時に CRL を発行し、リポジトリーに公表する。

4.9.9 オンラインでの失効/ステータス確認の適用性

コードサイニング証明書および S/MIME 証明書について、オンラインでの証明書ステータス情報は OCSP レスポンダーを通じて提供される。コードサイニング用証明書ポリシー以外のポリシーについては、必要に応じて提供される。

OCSP レスポンスは、RFC6960 や RFC5019 に準拠している必要がある。OCSP レスポンスは、以下のいずれかの条件を満たす必要がある。

1. 失効ステータスの確認対象となる証明書を発行した CA によって署名されている。
2. 失効ステータスの確認対象となる証明書を発行した CA によって証明書が署名されている OCSP レスポンダーによって署名されている。

後者の場合、OCSP 署名証明書には、RFC6960 に定義されている、タイプ id-pkix-ocsp-nochek の拡張領域が含まれていなければならない。

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

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。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 レスポンダーにより提供される証明書ステータス情報の確認を行わなければならない。

RFC 6960、RFC 5019 で説明されているように、CA が運用する OCSP レスポンダーは HTTP GET メソッドをサポートする必要がある。

OCSP 応答の有効期間は、thisUpdate と nextUpdate の時間差（両端を含む）である。その差を算出する目的で、うるう秒を無視すると、3,600 秒の差は 1 時間に等しく、86,400 秒の差は 1 日に等しくなる。

加入者証明書のステータスの場合

1. OCSP 応答には、8 時間以上の有効期間が必要である。
2. OCSP 応答には、10 日以下の有効期間が必要である。
3. 有効期間が 16 時間未満の OCSP 応答の場合、CA は nextUpdate の前の有効期間半分に先立ち、オンライン証明書ステータスプロトコルを介して提供される情報

を更新する必要がある。

4. 有効期間が 16 時間以上の OCSP 応答の場合、CA は nextUpdate の少なくとも 8 時間前、および thisUpdate の 4 日後までに、オンライン証明書ステータスプロトコルを介して提供される情報を更新する必要がある。

下位 CA 証明書のステータスの場合

CA は、

i. 少なくとも 12 カ月ごと、および

ii.下位 CA 証明書の失効から 24 時間以内にオンライン証明書ステータスプロトコルを介して提供された情報を更新するものとする。

OCSP レスポンダーが「未使用」の証明書シリアル番号のステータスのリクエストを受信した場合、レスポンダーは「good」ステータスで応答すべきではない。OCSP レスポンダーが本 CP「7.1.5 名前制約」に沿って技術的に制約されていない CA 向けである場合、レスポンダーはそのような要求に対して「good」ステータスで応答してはならない。

本 CA は、セキュリティ応答手順の一部として、「未使用」シリアル番号のリクエストについて OCSP レスポンダーを監視するべきである。

OCSP リクエスト内の証明書のシリアル番号は、そのシリアル番号を持つ証明書が、発行 CA によって発行された場合は、その CA サブジェクトに関連付けられた現在または以前の鍵を使用して「割り当てられ」、そうでない場合は「未使用」になる。

4.9.11 利用可能な失効情報の他の形式

本 CA は、RFC4366、RFC 5246、RFC 8446 に従い、ステープリングを利用して OCSP レスポンスを配布できる。この場合、本 CA は証明書利用者が TLS 処理に証明書の OCSP レスポンスを含めることを確実なものにする。本 CA は、証明書利用者に対してこの要件を実施する場合は、サービス利用規定または証明書利用者との契約書等、あるいは本 CA による技術確認およびサービス責任者の承認を経て対応するものとする。

4.9.12 鍵の危殆化に対する特別要件

「4.9.1.証明書失効事由」に記載する。

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、当該証明書の失効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

適用外とする。

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

CRL または OCSP レスポンダーの失効情報は、失効した証明書に記載されている有効期限までは確認できるものとする。なお、コードサイニング用証明書ポリシーで発行した証明書については、有効期限後も最低 10 年間は失効情報を確認できるものとする。

4.10.2 サービスの利用可能性

本 CA は、通常の運用状況の下で 10 秒以内のレスポンス時間を提供するために十分なリソースで、CRL および OCSP 機能を運用および維持するものとする。

本 CA は、アプリケーションソフトウェアが、本 CA によって発行されたすべての有効期限内証明書の現在のステータスを自動的にチェックするために使用できるオンラインリポジトリを 24 時間 365 日体制で維持するものとする。

本 CA は、優先度の高い証明書問題の報告を内部で対応し、必要に応じて当該苦情を法執行機関に通報し、または当該苦情の対象となった証明書を失効させる能力を 24 時間 365 日維持しなければならない。

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 または証明書利用者は本サービスの利用を終了する場合、発行した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ーおよび実施

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ーおよび実施

適用外とする。

5. 設備上、運営上、運用上の管理

5.1 物理的管理

5.1.1 立地場所および構造
本項については、CPS に規定する。

5.1.2 物理的アクセス
本項については、CPS に規定する。

5.1.3 電源および空調
本項については、CPS に規定する。

5.1.4 水害対策
本項については、CPS に規定する。

5.1.5 火災対策
本項については、CPS に規定する。

5.1.6 媒体保管
本項については、CPS に規定する。

5.1.7 廃棄処理
本項については、CPS に規定する。

5.1.8 オフサイトバックアップ
本項については、CPS に規定する。

5.2 手続的管理

5.2.1 信頼すべき役割
本項については、CPS に規定する。

5.2.2 職務ごとに必要とされる人数
本項については、CPS に規定する。

5.2.3 個々の役割に対する本人性確認と認証
本項については、CPS に規定する。

5.2.4 職務分割が必要となる役割
本項については、CPS に規定する。

5.3 人事的管理

5.3.1 資格、経験および身分証明の要件
本項については、CPS に規定する。

5.3.2 背景調査
本項については、CPS に規定する。

5.3.3 教育要件
本項については、CPS に規定する。

5.3.4 再教育の頻度および要件
本項については、CPS に規定する。

5.3.5 仕事のローテーションの頻度および順序
本項については、CPS に規定する。

5.3.6 認められていない行動に対する制裁
本項については、CPS に規定する。

5.3.7 独立した契約者の要件
本項については、CPS に規定する。

5.3.8 要員へ提供される資料
本項については、CPS に規定する。

5.4 監査ログの手続

5.4.1 記録されるイベントの種類

本項については、CPS に規定する。

5.4.2 監査ログを処理する頻度
本項については、CPS に規定する。

5.4.3 監査ログを保持する期間
本項については、CPS に規定する。

5.4.4 監査ログの保護
本項については、CPS に規定する。

5.4.5 監査ログのバックアップ手続
本項については、CPS に規定する。

5.4.6 監査ログの収集システム
本項については、CPS に規定する。

5.4.7 イベントを起こした者への通知
本項については、CPS に規定する。

5.4.8 脆弱性評価
本項については、CPS に規定する。

5.5 記録の保管

5.5.1 アーカイブの種類
本項については、CPS に規定する。

5.5.2 アーカイブ保存期間
本項については、CPS に規定する。

5.5.3 アーカイブの保護
本項については、CPS に規定する。

5.5.4 アーカイブのバックアップ手続

本項については、CPS に規定する。

5.5.5 記録にタイムスタンプを付与する要件

本項については、CPS に規定する。

5.5.6 アーカイブ収集システム

本項については、CPS に規定する。

5.5.7 アーカイブの検証手続

本項については、CPS に規定する。

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およ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および CRL の発行を行う。

5.7 危殆化および災害からの復旧

5.7.1 事故および危殆化時の手続

本項については、CPS に規定する。

5.7.2 ハードウェア、ソフトウェアまたはデータが破損した場合の手続

本項については、CPS に規定する。

5.7.3 私有鍵が危殆化した場合の手続

本項については、CPS に規定する。

5.7.4 災害後の事業継続性

本項については、CPS に規定する。

5.8 認証局または登録局の終了

セコムが本 CA を終了する場合、事前に LRA、本サービスの契約先、アプリケーションソフトウェアサプライヤーを含むその他の関係者に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 CA の終了以前に失効を行う。

6. 技術的セキュリティ管理

6.1 鍵ペアの生成およびインストール

6.1.1 鍵ペアの生成

認証基盤システムでは、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、証明書利用者の利用する端末内、HSM 内または本 CA の施設内において生成する。

AATL ドキュメントサイニング用証明書ポリシーの証明書利用者の鍵ペアは、証明書利用者の利用する HSM 内または本 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

本 CA は、私有鍵を使用するための PIN と私有鍵を、それぞれ異なる経路で送付する。または、対面により、PIN および私有鍵を手交する。

[S/MIME 証明書]

加入者以外の当事者は、加入者の許可なしに加入者私有鍵を保存しないものとする。

本 CA または RA のいずれかが、加入者の私有鍵が加入者によって承認されていない個人または組織に配布されたことに気付いた場合、本 CA は配布された私有鍵に対応する公開鍵を含むすべての証明書を失効させる。

本 CA あるいは委任された第三者が、私有鍵を加入者に代わって生成する場合、私有鍵の生成エンティティは、128 ビットの暗号化と同等の活性化方法で私有鍵をハードウェアにて配布するか、128 ビット以上の暗号化強度で私有鍵を暗号化する。方法の例としては、128 ビットの AES 鍵を使用して私有鍵を格納するか、大文字、小文字、数字、記号を含む 16 文字を超えるランダムに生成されたパスワードで暗号化した PKCS12 ファイルに私有鍵を格納して配布することが挙げられる。本 CA または委任された第三者は、利用者の私有鍵を平文で保存しない。

私有鍵を有効化または保護するために使用されるもの(PKCS12 ファイルを保護するために使用されるパスワードなど）は、私有鍵を格納するものとは別に、安全に加入者に配布する。

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/TLSにより暗号化を行う。

6.1.4 検証者へのCA公開鍵の交付

検証者は、本CAのリポジトリー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ビットまたは4096ビットとする。

証明書利用者の鍵ペアは、RSA方式で鍵長1024ビット、2048ビット、3072ビットまたは4096ビットとする。

コードサイニング証明書の鍵ペアは、RSA方式で鍵長3072ビットまたは4096ビットとする。

S/MIME証明書、AATLドキュメントサイニング証明書の鍵ペアは、RSA方式で鍵長2048ビット、3072ビットまたは4096ビットとする。

6.1.6 公開鍵のパラメーターの生成および品質検査

本項については、CPSに規定する。

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のいずれかを設定し、設定可能な組み合わせは証明書の利用用途ごと適切に限定される。

6.2 私有鍵の保護および暗号モジュール技術の管理

6.2.1 暗号モジュールの標準および管理

本CAの私有鍵の生成、保管、署名操作は、FIPS140-2レベル3準拠のHSMを用いて行う。

AATLドキュメントサイニング用証明書ポリシーの証明書の場合は、次の認定のいずれかを受けているものとする。

1. FIPS 140-2 レベル2以上
2. Common Criteria (ISO 15408 & ISO 18045) - Protection Profiles CEN prEN 14169 (all parts applicable to the device type)またはCEN EN 419 241か同等の基準（リモート管理デバイス用）

3. 2016 年 7 月 1 日以降に EU 加盟国が認定署名作成デバイス（QSCD）として認定、または 2016 年 7 月 1 日前に EU 加盟国の指定機関が安全な署名作成デバイス（SSCD）として認定

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または暗号モジュールからの転送

本 CA の私有鍵の HSM への転送または HSM からの転送は、セキュアな室において、私有鍵を暗号化した状態で行う。

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、少なくとも FIPS 140 レベル 3 または Common Criteria Protection Profile またはセキュリティターゲット、EAL 4 以上を満たしていると検証されたシステムまたはデバイス内で私有鍵を保護するものとする。これには、私有鍵や他の資産を既知の脅威から保護することも含まれる。

コードサイニング用途のタイムスタンプ局は、少なくとも FIPS 140-2 レベル 3、共通基準 EAL 4+（ALC_FLR.2）以上のプロセスを使用して、私有鍵を保護する。本 CA は、CA/Browser Forum’s Network Security Guidelines に従って署名操作を保護する。

2023 年 6 月 1 日より、コードサイニング証明書の加入者私有鍵は、次の要件に従って保護されることとする。本 CA は、少なくとも FIPS 140-2 レベル 2 または Common Criteria EAL4 +に準拠していると認定されたユニット設計フォームファクタを備えたハードウェア暗号化モジュールでコードサイニング証明書私有鍵を生成および保護するために、加入者が次のいずれかを使用するという契約上の表明を加入者から取得する。

(1) 加入者は、指定された要件を満たすハードウェア暗号化モジュールを使用する。
(2) 加入者は、次の要件を持つクラウドベースのキー生成および保護ソリューションを使用する。
   a 私有鍵の作成、保存、および使用は、指定された要件に準拠するクラウドソリューションのハードウェア暗号化モジュールのセキュリティ境界内にとどまらなければならない。
   b 私有鍵を管理するレベルのサブスクリプションは、私有鍵を保護するリソースに対するすべてのアクセス、操作、および構成の変更をログに記録するように構成しなければならない。
(3) 加入者は、Baseline Requirements (Code Signing) 6.2.7.3 の要件を満たす署名サービスを使用する。

2023 年 6 月 1 日より、コードサイニング証明書について、CA は、加入者の私有鍵が、Baseline Requirements (Code Signing) 6.2.7.4.1 で指定された要件を満たす、または超える適切なハードウェア暗号化モジュールで生成、保存、および使用されることを保証する。この要件を満たすには、次のいずれかの方法を使用する。

1. CA が適切なハードウェア暗号化モジュールと、ハードウェア暗号化モジュールを用いて生成した 1 つ以上の事前生成鍵ペアを出荷する。
2. 加入者は、一般に鍵認証と呼ばれる製造元の証明書を使用して検証できる証明書要求に副署名する。これは、私有鍵が適切なハードウェア暗号モジュールを使用してエクスポートできない方法で生成されたことを示す。
3. 加入者が、CA で規定された暗号化ライブラリと鍵ペアの生成と保存に適したハードウェア暗号化モジュールの組み合わせを使用する。
4. 加入者が、コードサイニング証明書に関連付けられる鍵ペアを生成するために、適切なハードウェア暗号化モジュールのみを使用していることを示す内部または外部の IT 監査の提供をする。
5. 加入者が、クラウドベースの鍵保護ソリューションサブスクリプションからの適切なレポートと適切なハードウェア暗号化モジュールの私有鍵を保護するリソース構成を提供する。
6. CA は、CA が承認し、IT セキュリティトレーニングを受けた監査人または CISA

資格を持つ監査人が署名した報告書に基づき、クラウドベースの鍵生成・保護ソリューションを含む適切なハードウェア暗号モジュールソリューションで鍵ペアが生成されていることを確認する。

7. 加入者が、Baseline Requirements (Code Signing) 6.2.7.3 の要件を満たす署名サービスを使用することに同意する。

AATL ドキュメントサイニング証明書の場合は、本 CA が証明書利用者の利用する HSM 内において私有鍵を生成していることを確認した場合、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私有鍵で署名されていることを確認する。または、暗号化ハードウェアデバイスに本 CA にて私有鍵を生成し、その私有鍵を証明書利用者に対し安全に配布することで、証明書利用者が該当する証明書に対応する私有鍵を所持するということを証明する。

コードサイニング証明書および AATL ドキュメントサイニング証明書以外の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また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および管理」と同様とする。

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 の公開鍵およ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 私有鍵および公開鍵の有効期間

本項については、CPS に規定する。

6.4 活性化データ

6.4.1 活性化データの生成および設定

本項については、CPS に規定する。

6.4.2 活性化データの保護

本項については、CPS に規定する。

6.4.3 活性化データの他の考慮点

本項については、CPS に規定する。

6.5 コンピューターのセキュリティ管理

6.5.1 コンピューターセキュリティに関する技術的要件

本 CA は、証明書を直接発行させることができるすべてのアカウントに対して、多要素認証を実施するものとする。

6.5.2 コンピューターセキュリティ評価

本項については、CPS に規定する。

6.6 ライフサイクルセキュリティ管理

6.6.1 システム開発管理

本項については、CPS に規定する。

6.6.2 セキュリティ運用管理

本項については、CPS に規定する。

6.6.3 ライフサイクルセキュリティ管理

本項については、CPS に規定する。

6.7 ネットワークセキュリティ管理

本項については、CPS に規定する。

6.8 タイムスタンプ

本項については、CPS に規定する。

7. 証明書および CRL、OCSP のプロファイル

7.1 証明書プロファイル

本 CA は、本 CP「2.2 証明書情報の公開」、本 CP「6.1.5 鍵サイズ」、本 CP「6.1.6 公開鍵のパラメーターの生成および品質検査」に規定された技術要件を満たすものとする。

本 CA が加入者証明書を発行する際、暗号論的擬似乱数生成器(CSPRNG)からの 64 ビット以上の出力を含む 1 以上かつ 2^{159} 未満の連番ではない証明書シリアル番号を生成するものとする。本 CA が発行する証明書は RFC5280 に準拠している。プロファイルは、次表のとおりである。

表 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） 2016/10/01 00:00:00 GMT	-
	NotAfter （有効性終了日時）	例） 2026/10/01 00:00:00 GMT	
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/SCRoot1CRL.crl	N
Certificate Policies（証明書ポリシー）	Policy: 1.2.392.200091.100.901.1 CPS: https://repository.secomtrust.net/SC-Root1/	N
Key Usage （鍵用途）	keyCertSign（証明書への署名） cRLSign（CRL への署名）	Y
Extended Key Usage （拡張鍵用途）	以下を設定可能 clientAuth（クライアント認証） SmartCard Logon（スマートカードログオン） ＊SmartCard Logon 選択時は、clientAuth も同時選択	N
Basic Constraints （基本的制約）	TRUE （CA である）	Y

表 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 Systems CO.,LTD.	
	Organizational Unit （組織単位）	OU=Security Communication RootCA2	
Validity （有効期限）	NotBefore （有効性開始日時）	例） 2016/10/01 00:00:00 GMT	-
	NotAfter （有効性終了日時）	例） 2026/10/01 00:00:00 GMT	
Subject （主体者）	Country （国）	C=JP	-
	Organization （組織）	本 CA の Organization を設定	

	Organizational Unit （組織単位）	本 CA の Organizational Unit を設定可能	
	Common Name (CN)	本 CA の Common Name を設定	
Subject PublicKey Info （主体者公開鍵情報）		主体者の RSA 公開鍵（コードサイニング用証明書ポリシーでは 4096bit とし、それ以外は 2048bit 以上）	-

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/SCRoot2CRL.crl	N
Authority Information Access （機関情報アクセス）	accessMethod ocsp (1.3.6.1.5.5.7.48.1) accessLocation http://scrootca2.ocsp.secomtrust.net accessMethod caIssuers (1.3.6.1.5.5.7.48.2) accessLocation http://repository.secomtrust.net/SC-Root2/SCRoot2ca.cer ＊必要に応じて設定する	N
Certificate Policies（証明書ポリシー）	Policy: 1.2.392.200091.100.901.4 Policy: 2.23.140.1.4.1（コードサイニング用証明書ポリシーのみ付与） CPS: リポジトリーの URL	N
Key Usage （鍵用途）	keyCertSign（証明書への署名） cRLSign（CRL への署名）	Y
Extended Key Usage （拡張鍵用途）	以下を設定可能 clientAuth（クライアント認証） emailProtection（E-mail 保護） SmartCard Logon（スマートカードログオン）	N

	codeSigning（コードサイニング） Adobe Authentic Documents Trust =1.2.840.113583.1.1.5 Microsoft Signer of documents =1.3.6.1.4.1.311.10.3.12 ＊SmartCard Logon 選択時は、clientAuth も同時選択 ＊codeSigning（コードサイニング）は単独で選択	
Basic Constraints （基本的制約）	TRUE （CA である）	Y

表 7.1-3 CA 証明書(SHA384：クライアント用証明書ポリシー、データ署名用証明書ポリシー、コードサイニング用証明書ポリシー、S/MIME 用証明書ポリシー)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-384 with RSAEncryption	-
Issuer （発行者）	Country （国）	C=JP	-
	Organization （組織）	ルート CA の Organization を設定	
	Common Name (CN)	ルート CA の Common Name を設定	
Validity （有効期限）	NotBefore （有効性開始日時）	例） 2021/05/01 00:00:00 GMT	-
	NotAfter （有効性終了日時）	例） 2031/05/01 00:00:00 GMT	
Subject （主体者）	Country （国）	C=JP	-
	Organization （組織）	本 CA の Organization を設定	
	Organizational Unit （組織単位）	本 CA の Organizational Unit を設定可能	
	Common Name (CN)	本 CA の Common Name を設定	
Subject PublicKey Info （主体者公開鍵情報）		主体者の RSA 公開鍵（コードサイニング用証明書ポリシーでは 4096bit とし、それ以外は 2048bit 以上）	-

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）	本 CA の CRL サービスの HTTP URL	N
Authority Information Access （機関情報アクセス）	accessMethod ocsp（1.3.6.1.5.5.7.48.1） accessLocation OCSP レスポンダーの HTTP URL accessMethod caIssuers（1.3.6.1.5.5.7.48.2） accessLocation 本 CA 証明書の HTTP URL ＊それぞれ必要に応じて設定する	N
Certificate Policies（証明書ポリシー）	Policy: 1.2.392.200091.100.901.4（Security Communication RootCA2 下位 CA 用証明書ポリシー）、Policy: 1.2.392.200091.100.901.6（Security Communication RootCA3 下位 CA 用証明書ポリシー）または 1.2.392.200091.100.901.9（SECOM RSA Root CA 2023 下位 CA 証明書ポリシー） Policy: 2.23.140.1.4.1（コードサイニング用証明書ポリシーのみ付与） Policy: 2.23.140.1.5.1.3（S/MIME 用証明書ポリシーのみ付与） CPS: Root CA のリポジトリーHTTP URL	N
Key Usage （鍵用途）	keyCertSign（証明書への署名） cRLSign（CRL への署名）	Y
Extended Key Usage （拡張鍵用途）	以下を設定可能 clientAuth（クライアント認証） emailProtection（E-mail 保護） SmartCard Logon（スマートカードログオン）	N

	codeSigning（コードサイニング） Adobe Authentic Documents Trust =1.2.840.113583.1.1.5 Microsoft Signer of documents =1.3.6.1.4.1.311.10.3.12 ＊SmartCard Logon 選択時は、clientAuth も同時選択 ＊codeSigning（コードサイニング）は単独で選択	
Basic Constraints （基本的制約）	TRUE （CA である）	Y

表 7.1-4 CA 証明書(AATL ドキュメントサイニング用証明書ポリシー)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-384 with RSAEncryption	-
Issuer （発行者）	Country （国）	C=JP	-
	Organization （組織）	SECOM Trust Systems Co., Ltd.	
	Common Name (CN)	SECOM Document Signing RSA Root CA 2023	
	organizationIdentifier(2.5.4.97)	NTRJP-4011001040781 （NTRJP-本 CA の法人番号）	
Validity （有効期限）	NotBefore （有効性開始日時）	例） 2023/02/16 00:00:00 GMT	-
	NotAfter （有効性終了日時）	例） 2043/02/01 00:00:00 GMT	
Subject （主体者）	Country （国）	C=JP	-
	Organization （組織）	SECOM Trust Systems Co., Ltd.	
	Common Name (CN)	本 CA の Common Name を設定	
	organizationIdentifier(2.5.4.97)	NTRJP-4011001040781 （NTRJP-本 CA の法人番号）	
Subject PublicKey Info （主体者公開鍵情報）		主体者の RSA 公開鍵 (4096bit)	-

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://repo1.secomtrust.net/root/docrsa/docrsarootca2023.crl	N
Authority Information Access （機関情報アクセス）	accessMethod ocsp（1.3.6.1.5.5.7.48.1） accessLocation http://docrsarootca2023.ocsp.secom-cert.jp accessMethod caIssuers（1.3.6.1.5.5.7.48.2） accessLocation http://repo2.secomtrust.net/root/docrsa/docrsarootca2023.cer	N
Certificate Policies（証明書ポリシー）	Policy: 1.2.392.200091.100.901.10（SECOM Document Signing RSA Root CA 2023 下位 CA 証明書ポリシー） CPS: http://repo1.secomtrust.net/root/docrsa/	N
Key Usage （鍵用途）	keyCertSign（証明書への署名） cRLSign（CRL への署名）	Y
Extended Key Usage （拡張鍵用途）	Adobe Authentic Documents Trust =1.2.840.113583.1.1.5	N
Basic Constraints （基本的制約）	TRUE （CA である）	Y

表 7.1-5 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） 2017/02/10 09:55:27 GMT	－
	NotAfter （有効性終了日時）	例） 2018/02/10 10:25:27 GMT ＊各証明書ポリシーに準ずる	
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="組織名"	
	Organizational Unit （組織単位）	OU="組織単位" 【オプション】	
	Common Name （主体者名）	CN="利用者名"	
	Serial Number （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）	以下を設定可能 digitalSignature（デジタル署名） Non Repudiation（否認防止） keyEncipherment（鍵暗号化） dataEncipherment（データ暗号化）	Y

Certificate Policies (証明書ポリシー)	以下を設定可能 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)	以下を設定可能 OtherName: UPN="ユーザープリンシパル名" OtherName: "OID"="任意文字列" Rfc822Name:"メールアドレス" dNSName:"サーバー名"	N
Extended Key Usage (拡張鍵用途)	以下を設定可能 clientAuth (クライアント認証) emailProtection (E-mail 保護) SmartCard Logon (スマートカードログオン) codeSigning (コードサイニング) ＊SmartCard Logon 選択時は、clientAuth も同時選択 ＊codeSigning (コードサイニング) は単独で選択	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 vocationList	N
Netscape Certificate Type (Netscape 証明書タイプ)	以下を設定可能 SSL Client S/MIME Client codeSigning	N

表 7.1-6 証明書利用者証明書(SHA256：クライアント用証明書ポリシー、
データ署名用証明書ポリシー)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）	本 CA の Organization を設定	
	Organizational Unit （組織単位）	本 CA の Organizational Unit を設定可能	
	Common Name （CN）	本 CA の Common Name を設定	
Validity （有効期限）	NotBefore （有効性開始日時）	例） 2017/02/10 09:55:27 GMT	–
	NotAfter （有効性終了日時）	例） 2018/02/10 10:25:27 GMT ＊各証明書ポリシーに準ずる	
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="組織名"	
	Organizational Unit （組織単位）	OU="組織単位" 【オプション】	
	Common Name （主体者名）	CN="利用者名"	
	Serial Number （シリアル番号）	SerialNumber="シリアル番号" 【オプション】	
Subject PublicKey Info （主体者公開鍵情報）		主体者の RSA 公開鍵データ （2048bit 以上）	–

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）	以下を設定可能 digitalSignature（デジタル署名） Non Repudiation（否認防止） keyEncipherment（鍵暗号化） dataEncipherment（データ暗号化）	Y

Certificate Policies (証明書ポリシー)	以下を設定可能 Policy: 1.2.392.200091.100.381.4 Policy: 1.2.392.200091.100.381.5 CPS:リポジトリーの URL	N
Subject Alt Name (主体者別名)	以下を設定可能 OtherName: UPN="ユーザープリンシパル名" OtherName: "OID"="任意文字列" Rfc822Name:"メールアドレス" (2023/08/31 まで設定可能)	N
Extended Key Usage (拡張鍵用途)	以下を設定可能 clientAuth (クライアント認証) emailProtection (E-mail 保護) (2023/08/31 まで設定可能) SmartCard Logon (スマートカードログオン) Adobe Authentic Documents Trust =1.2.840.113583.1.1.5 Microsoft Signer of documents =1.3.6.1.4.1.311.10.3.12 ＊SmartCard Logon 選択時は、clientAuth も同時選択	N
CRL Distribution Points (CRL 配布ポイント)	本 CA の CRL サービスの HTTP URL ldap://repo1.secomtrust.net/"IssuerDN"?certificateRevocationList ＊ldap は必要に応じて設定する	N
Authority Information Access (機関情報アクセス)	accessMethod ocsp (1.3.6.1.5.5.7.48.1) accessLocation OCSP レスポンダーの URL accessMethod caIssuers (1.3.6.1.5.5.7.48.2) accessLocation 下位 CA 証明書の URL ＊必要に応じて設定する	N
Netscape Certificate Type (Netscape 証明書タイプ)	以下を設定可能 SSL Client S/MIME Client (2023/08/31 まで設定可能)	N

表 7.1-7 証明書利用者証明書(SHA256：コードサイニング用証明書ポリシー)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）	本 CA の Organization を設定	
	Common Name (CN)	本 CA の Common Name を設定	
Validity （有効期限）	NotBefore （有効性開始日時）	例） 2023/08/28 10:00:00 GMT	-
	NotAfter （有効性終了日時）	例） 2026/08/28 10:00:00 GMT	
Subject （主体者）	Country （国）	C=JP	-
	stateOrProvinceName （都道府県）	ST="都道府県名"	
	localityName （市区町村）	L="市区町村名"	
	Organization （組織）	O="組織名"	
	Organizational Unit （組織単位）	OU="組織単位" 【オプション】	
	Common Name （主体者名）	CN="利用者名（組織名）"	
Subject PublicKey Info （主体者公開鍵情報）		主体者の RSA 公開鍵データ （3072bit または 4096bit）	-

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（デジタル署名）	Y
Certificate Policies （証明書ポリシー）	Policy: 1.2.392.200091.100.381.8 CPS:リポジトリーの URL Policy: 2.23.140.1.4.1（コードサイニング用証明書ポリシー）	N
Subject Alt Name （主体者別名）	使用しない	N
Extended Key Usage （拡張鍵用途）	codeSigning（コードサイニング）	N
CRL Distribution Points （CRL 配布ポイント）	本 CA の CRL サービスの HTTP URL	N
Authority Information Access （機関情報アクセス）	accessMethod ocsp（1.3.6.1.5.5.7.48.1） accessLocation OCSP レスポンダーの URL accessMethod caIssuers（1.3.6.1.5.5.7.48.2） accessLocation 下位 CA 証明書の URL	N

表 7.1-8 証明書利用者証明書(AATL ドキュメントサイニング用証明書ポリシー)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）	SECOM Trust Systems Co., Ltd.	
	Common Name（CN）	本 CA の Common Name を設定	
	organizationIdentifier(2.5.4.97)	NTRJP-4011001040781 （NTRJP-本 CA の法人番号）	
Validity （有効期限）	NotBefore （有効性開始日時）	例） 2023/02/21 00:00:00 GMT	-

	NotAfter （有効性終了日時）	例） 2026/02/21 00:00:00 GMT	
Subject （主体者）	Country （国）	C=JP	-
	stateOrProvinceName （都道府県）	ST="都道府県名"	
	localityName （市区町村）	L="市区町村名"	
	Organization （組織）	O="組織名"	
	Organizational Unit （組織単位）	OU="組織単位" 【オプション】	
	Common Name （主体者名）	CN="組織名または利用者名"	
Subject PublicKey Info （主体者公開鍵情報）		主体者の RSA 公開鍵データ（2048bit 以上）	-

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（デジタル署名） Non Repudiation（否認防止）	Y
Certificate Policies （証明書ポリシー）	Policy: 1.2.392.200091.100.382.1 CPS:リポジトリーの URL	N
Subject Alt Name （主体者別名）	使用しない	N
Extended Key Usage （拡張鍵用途）	Adobe Authentic Documents Trust =1.2.840.113583.1.1.5	N
CRL Distribution Points （CRL 配布ポイント）	本 CA の CRL サービスの HTTP URL	N
Authority Information Access （機関情報アクセス）	accessMethod ocsp（1.3.6.1.5.5.7.48.1） accessLocation OCSP レスポンダーの URL accessMethod	N

	caIssuers (1.3.6.1.5.5.7.48.2) accessLocation 下位 CA 証明書の URL	

表 7.1-9 証明書利用者証明書(SHA256：S/MIME 用証明書ポリシー)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）	本 CA の Organization を設定	
	Common Name (CN)	本 CA の Common Name を設定	
Validity （有効期限）	NotBefore （有効性開始日時）	例） 2023/09/01 00:00:00 GMT	-
	NotAfter （有効性終了日時）	例） 2025/08/31 23:59:59 GMT	
Subject （主体者）	Common Name （主体者名）	CN=メールアドレス	-
Subject PublicKey Info （主体者公開鍵情報）		主体者の RSA 公開鍵データ（2048bit 以上）	-

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（デジタル署名） keyEncipherment（鍵暗号化）	Y
Certificate Policies (証明書ポリシー)	Policy: 2.23.140.1.5.1.3 Policy: 1.2.392.200091.100.383.1 CPS:リポジトリーの URL	N
Subject Alt Name	Rfc822Name:"メールアドレス"	N

(主体者別名)		
Extended Key Usage (拡張鍵用途)	emailProtection (E-mail 保護)	N
CRL Distribution Points (CRL 配布ポイント)	本 CA の CRL サービスの HTTP URL	N
Authority Information Access (機関情報アクセス)	accessMethod ocsp (1.3.6.1.5.5.7.48.1) accessLocation OCSP レスポンダーの URL accessMethod caIssuers (1.3.6.1.5.5.7.48.2) accessLocation 下位 CA 証明書の URL	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。ただし、セコムが定める組み合わせでのみ設定可能とする。
なお、コードサイニング用証明書ポリシーを含む証明書の発行に際しては、Baseline Requirements (Code Signing)に準拠した登録とする。

7.1.1 バージョン番号

本 CA は、バージョン 3 を適用する。

7.1.2 証明書拡張

本 CA が発行する証明書は、証明書拡張フィールドを使用する。

7.1.3 アルゴリズムオブジェクト識別子

本サービスにおいて用いられるアルゴリズム OID は、次のとおりである。

Security Communication RootCA1 アルゴリズム OID

アルゴリズム	オブジェクト識別子
Sha1 With RSA Encryption	1 2 840 113549 1 1 5
sha256 With RSA Encryption	1.2.840.113549.1.1.11
RSA Encryption	1 2 840 113549 1 1 1

Security Communication RootCA2 アルゴリズム OID

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

Security Communication RootCA3 アルゴリズム OID

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

SECOM RSA Root CA 2023 アルゴリズム OID

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

SECOM Document Signing RSA Root CA 2023 アルゴリズム OID

アルゴリズム	オブジェクト識別子
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 では、RFC5280 で定められる、識別名を使用する。

すべての有効な認証パス（RFC 5280、セクション 6 で定義されているとおり）について認証パスの加入者証明書ごとに、証明書発行者の識別名フィールドのエンコードされた内容は、発行される CA 証明書の主体者識別名フィールドのエンコードされた形式とバイト単位で同一である必要がある。

本 CA は、証明書を発行することにより、CP/CPS に定められた手順に従い、証明書の発行日時点で、すべての識別名が正確であることを確認することを表明する。

7.1.5 名前制約

必要に応じて本 CA で設定する。

7.1.6 CP オブジェクト識別子

本 CA が発行する証明書の OID は、「1.2 文書名と識別」の OID のとおりである。

次の証明書ポリシー識別子は、証明書または加入者証明書が Baseline Requirements に準拠していることを表明するオプションの手段として本 CA が使用するために用意されている。

【コードサイニング証明書】

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) code-signing-requirements(4) code signing(1)} (2.23.140.1.4.1)

【S/MIME 証明書（メールボックス認証 Strict プロファイル)】

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) mailbox-validated (1) strict (3)} (2.23.140.1.5.1.3)

7.1.7 ポリシー制約拡張の利用

設定しない。

7.1.8 ポリシー修飾子の文法および意味

ポリシー修飾子については、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ー拡張の処理の意味

設定しない。

7.2 CRL プロファイル

表 7.2-1 CRL(SHA1)のプロファイル

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)　2016/10/01 00:00:00 GMT	-
Next Update (次回更新予定日時)		例)　2016/10/05 00:00:00 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)　123456789abcdef0	-
	Revocation Date (失効日時)	例)　2016/09/01 12:00:00 GMT	
	Reason Code (失効事由)	例) cessation of operation(運用停止) ＊設定は任意	

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

表 7.2-2 CRL(SHA256：クライアント用証明書ポリシー、
データ署名用証明書ポリシー、コードサイニング用証明書ポリシー)のプロファイル

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 (発行者)	Country (国)	C=JP	-
	Organization (組織)	本 CA の Organization を設定	
	Organizational Unit (組織単位)	本 CA の Organizational Unit を設定可能	
	Common Name (CN)	本 CA の Common Name を設定	
This Update (更新日時)		例)　2016/10/01 00:00:00 GMT	-
Next Update (次回更新予定日時)		例)　2016/10/05 00:00:00 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)　123456789abcdef0	-
	Revocation Date (失効日時)	例)　2016/09/01 12:00:00 GMT	
	Reason Code (失効事由)	例) cessation of operation(運用停止)	

		＊設定は任意	

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

表 7.2-3 CRL(AATL ドキュメントサイニング用証明書ポリシー)のプロファイル

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）		以下のいずれかを設定 SHA-256 with RSAEncryption SHA-384 with RSAEncryption	-
Issuer （発行者）	Country （国）	C=JP	-
	Organization （組織）	SECOM Trust Systems Co., Ltd.	
	Common Name（CN）	本 CA の Common Name を設定	
	organizationIdentifier(2.5.4.97)	NTRJP-4011001040781 （NTRJP-本 CA の法人番号）	
This Update（更新日時）		例） 2023/02/16 00:00:00 GMT	-
Next Update（次回更新予定日時）		例） 2023/02/20 00:00:00 GMT	
Revoked Certificates （失効証明書）	Serial Number （失効証明書シリアル番号）	例） 123456789abcdef0	-
	Revocation Date （失効日時）	例） 2023/02/16 00:00:00 GMT	
	Reason Code （失効事由）	例）cessation of operation(運用停止) ＊設定は任意	

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

表 7.2-4 CRL(S/MIME 用証明書ポリシー)のプロファイル

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）		以下のいずれかを設定 SHA-256 with RSAEncryption SHA-384 with RSAEncryption	-
Issuer（発行者）	Country （国）	C=JP	-
	Organization （組織）	本 CA の Organization を設定	
	Common Name（CN）	本 CA の Common Name を設定	
This Update（更新日時）		例） 2023/05/01 00:00:00 GMT	-
Next Update（次回更新予定日時）		例） 2023/05/05 00:00:00 GMT	
Revoked Certificates（失効証明書）	Serial Number （失効証明書シリアル番号）	例） 123456789abcdef0	-
	Revocation Date （失効日時）	例） 2023/04/30 00:00:00 GMT	
	Reason Code （失効事由）	例）cessation of operation(運用停止) ＊設定は任意	

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

7.2.1 バージョン番号

本 CA は、CRL バージョン 2 を適用する。

7.2.2 CRL 拡張

本 CA が発行する CRL 拡張フィールドを使用する。

7.3 OCSP のプロファイル

表 7.3-1 OCSP プロファイル(SHA256：クライアント用証明書ポリシー、データ署名用証明書ポリシー、コードサイニング用証明書ポリシー)

フィールド（基本領域）	内容	critical

Version		Version 3	-
Serial Number		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）	本CAのOrganizationを設定	
	Organizational Unit（組織単位）	本CAのOrganizational Unitを設定可能	
	Common Name（CN）	本CAの Common Nameを設定	
Validity（有効期限）	NotBefore（有効性開始日時）	例） 2023/02/16 00:00:00 GMT	-
	NotAfter（有効性終了日時）	例） 2023/02/20 00:00:00 GMT	-
Subject（主体者）	Country （国）	C=JP	-
	Organization （組織）	本CAのOrganizationを設定	-
	Organizational Unit（組織単位）	本CAのOrganizational Unitを設定可能	-
	Common Name（CN）	OCSPレスポンダー名（必須）	-
Subject Public Key Info（主体者公開鍵情報）		主体者の公開鍵データ	-

フィールド（拡張領域）	内容	
KeyUsage（鍵用途）	digitalSignature	Y
ExtendedKeyUsage（拡張鍵用途）	OCSPSigning	N
OCSP No Check	null	N
CertificatePolicies（証明書ポリシー）	2023年9月14日以前は任意設定とし、2023年9月15日以降は設定禁止とする。 policyIdentifier OID= 1.2.392.200091.100.381.9 policyQualifiers policyQualifierId=CPS qualifiier=リポジトリーのURL	N
Authority Key Identifier（発行者鍵識別子）	発行者公開鍵のSHA-1 ハッシュ値（160ビット）	N
Subject Key Identifier	主体者公開鍵のSHA-1 ハッシュ値（160ビット）	N

（主体者鍵識別子）		

表 7.3-2 OCSP プロファイル(AATL ドキュメントサイニング用証明書ポリシー)

フィールド（基本領域）		内容	critical
Version		Version 3	-
Serial Number		例） 123456789abcdef0	-
Signature Algorithm（署名アルゴリズム）		以下のいずれかを設定 SHA-256 with RSAEncryption SHA-384 with RSAEncryption	-
Issuer（発行者）	Country （国）	C=JP	-
	Organization （組織）	SECOM Trust Systems Co., Ltd.	
	Common Name（CN）	本 CA の Common Name を設定	
	organizationIdentifier(2.5.4.97)	NTRJP-4011001040781 （NTRJP-本 CA の法人番号）	
Validity（有効期限）	NotBefore（有効性開始日時）	例） 2023/02/16 00:00:00 GMT	-
	NotAfter（有効性終了日時）	例） 2023/02/20 00:00:00 GMT	-
Subject（主体者）	Country （国）	C=JP	-
	Organization （組織）	本 CA の Organization を設定	-
	Organizational Unit（組織単位）	本 CA の Organizational Unit を設定可能	-
	Common Name（CN）	OCSPレスポンダー名（必須）	-
Subject Public Key Info（主体者公開鍵情報）		主体者の公開鍵データ	-

フィールド（拡張領域）	内容	
KeyUsage（鍵用途）	digitalSignature	Y
ExtendedKeyUsage（拡張鍵用途）	OCSPSigning	N
OCSP No Check	null	N
CertificatePolicies（証明書ポリシー）	2023年9月14日以前は任意設定とし、2023年9月15日以降は設定禁止とする。 policyIdentifier OID= 1.2.392.200091.100.382.1	N

	policyQualifiers policyQualifierId=CPS qualifiier=リポジトリーのURL	
Authority Key Identifier （発行者鍵識別子）	発行者公開鍵のSHA-1 ハッシュ値（160ビット）	N
Subject Key Identifier （主体者鍵識別子）	主体者公開鍵のSHA-1 ハッシュ値（160ビット）	N

表 7.3-3 OCSP プロファイル(S/MIME 用証明書ポリシー)

フィールド（基本領域）		内容	critical
Version		Version 3	-
Serial Number		例） 123456789abcdef0	-
Signature Algorithm（署名アルゴリズム）		以下のいずれかを設定 SHA-256 with RSAEncryption SHA-384 with RSAEncryption	-
Issuer（発行者）	Country （国）	C=JP	-
	Organization （組織）	本 CA の Organization を設定	
	Common Name（CN）	本 CA の Common Name を設定	
Validity（有効期限）	NotBefore（有効性開始日時）	例） 2023/02/16 00:00:00 GMT	-
	NotAfter（有効性終了日時）	例） 2023/02/20 00:00:00 GMT	-
Subject（主体者）	Country （国）	C=JP	-
	Organization （組織）	本 CA の Organization を設定	-
	Organizational Unit（組織単位）	本 CA の Organizational Unit を設定可能	-
	Common Name（CN）	OCSPレスポンダー名（必須）	-
Subject Public Key Info （主体者公開鍵情報）		主体者の公開鍵データ	-

フィールド（拡張領域）	内容	
KeyUsage（鍵用途）	digitalSignature	Y
ExtendedKeyUsage（拡張鍵用途）	OCSPSigning	N
OCSP No Check	null	N

Authority Key Identifier （発行者鍵識別子）	発行者公開鍵のSHA-1 ハッシュ値（160ビット）	N
Subject Key Identifier （主体者鍵識別子）	主体者公開鍵のSHA-1 ハッシュ値（160ビット）	N

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

本 CA が発行する OCSP 拡張フィールドを使用する。

8. 準拠性監査と他の評価

8.1 監査の頻度

本 CA は、本 CP および CPS に準拠して運用がなされているかについて、適時監査を行う。S/MIME 証明書およびコードサイニング証明書の運用に関しては、本 CP および CPS に準拠して運用がなされているか、年に 1 回以上、WebTrust 規準に基づく準拠性監査を行う。

8.2 監査人の身元／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。また、WebTrust 認証を受ける CA の監査は、監査法人が行う。

8.3 監査人と被監査部門の関係

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、もしくはセコムとの間に特別な利害関係のない監査人を選定する。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 監査で扱われる事項

監査は、本 CA の運用にかかる業務を対象として行う。

また、認証局のための WebTrust for CA 規準、WebTrust for CA - Code Signing Baseline Requirements 規準に基づいて行われることもある。

8.5 不備の結果としてとられる処置

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 監査結果の開示

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。

なお、WebTrust for CA 、WebTrust for CA - Code Signing Baseline Requirements の検証に関する報告書は、WebTrust for CA 規準、WebTrust for CA - Code Signing Baseline Requirements 規準に従い、特定のサイトにて参照可能となる。

9. 他の業務上および法的事項

9.1 料金

9.1.1 証明書の発行または更新にかかる料金

契約書等に別途定める。

9.1.2 証明書のアクセス料金

規定しない。

9.1.3 失効またはステータス情報のアクセス料金

規定しない。

9.1.4 他サービスの料金

規定しない。

9.1.5 返金ポリシー

契約書等に別途定める。

9.2 財務的責任

9.2.1 保険の補償

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。

9.2.2 その他の資産

規定しない。

9.2.3 エンドエンティティの保険または保証範囲

規定しない。

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

9.4.1 個人情報保護方針

本項については、CPS に規定する。

9.4.2 個人情報として扱われる情報

本項については、CPS に規定する。

9.4.3 個人情報とみなされない情報

本項については、CPS に規定する。

9.4.4 個人情報を保護する責任

本項については、CPS に規定する。

9.4.5 個人情報の使用に関する通知と同意

本項については、CPS に規定する。

9.4.6 司法または行政手続に沿った情報開示

本項については、CPS に規定する。

9.4.7 その他の情報開示条件

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

本 CP は、原文が適切に参照されることを条件に、複製することができる。「Creative Commons license Attribution-NoDerivatives (CC-BY-ND) 4.0」で公開する。

https://creativecommons.org/licenses/by-nd/4.0/

9.6 表明保証

9.6.1 認証局の表明保証

セコムトラストシステムズは、本 CP および CPS に規定した内容を遵守して利用者に関する審査、証明書の登録、発行、失効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。

本 CA は、証明書を発行することによって、下記の証明書受益者に対し、本書に規定されている証明書の保証を行うものとする。

1. 証明書の加入者契約または利用規約の当事者である加入者。
2. アプリケーションソフトウェアサプライヤーによって配布されるソフトウェアにルート証明書を含めるため、ルート CA と契約を締結しているすべてのアプリケーションソフトウェアサプライヤー。
3. 有効な証明書に合理的に依拠しているすべての依拠当事者。CA は、証明書の受益者に対し、証明書が有効である間、CA が証明書の発行および管理において Baseline Requirements およびその CP/CPS に従ってきたことを表明し、保証するものとする。

証明書の保証には、具体的に以下が含まれるが、これらに限定されない。

1. コンプライアンス
   コードサイニング証明書の場合、本 CA および署名サービスは、コードサイニング証明書の発行およびその PKI または署名サービスの運用において、Baseline Requirements (Code Signing)および CP/CPS に準拠していることを表明する。
2. 加入者のアイデンティティ
   コードサイニング証明書の場合、発行時に、本 CA または署名サービスは、(i) 少なくとも Baseline Requirements (Code Signing)3.2 の要件を満たす加入者の身元を確認する手順を実施したことを表明し、(ii) 証明書を発行または管理する際の手順に従い、(iii) 本 CA の CP/CPS に同じ手順を正確に記述する。
   S/MIME 証明書の場合、証明書にサブジェクト ID 情報が含まれている場合、本 CA は次のことを行う。(i) Baseline Requirements (S/MIME)3.2 および 7.1.4.2.2

の要件を満たす加入者の身元を確認する手順を実施したことを表明し、（ii）証明書を発行または管理する際の手順に従い、（iii）本 CA の CP/CPS に同じ手順を正確に記述する。

3.メールボックスアドレスを使用する権利

S/MIME 証明書の場合、発行時に、本 CA は次のことを行う。(i). 証明書の Subject フィールドおよび subjectAltName 拡張に記載されるメールボックスアドレスの使用権限または管理権限を申請者が有していること（使用権限または管理権限を有する者から委任されていることを含む）を検証する手続きを実施し、(ii). 証明書を発行する際、手続きに従い、(iii). 本 CA の CP/CPS にその手続きを正確に記載する。

4. 証明書の承認

発行時に、本 CA は、（i）申請者が証明書の発行を承認したことを確認する手順を実行し、（ii）手順に従い、（iii）本 CA の CP/CPS にその手順を正確に記述している。

5. 情報の正確性

証明書発行時に、本 CA は、（i）証明書に含まれるすべての情報（コードサイニング証明書の場合は subject：organizationalUnitName 属性を除く、S/MIME 証明書の場合は subject：serialNumber 属性を除く）が真実かつ正確であることを確認する手順を実行し、（ii）手順に従い、（iii）本 CA の CP/CPS にその手順を正確に記述している。

6. 鍵の保護

コードサイニング証明書の場合、本 CA は、発行時に、コードサイニング証明書に関連付けられた私有鍵を安全に保管し、不正使用を防止する方法に関する文書を加入者に提供、署名サービスの場合、コードサイニング証明書に関連付けられた私有鍵の安全な保管と不正使用を防止する方法に関する文書を加入者に提供することを表明する。

7. 加入者契約

本 CA または署名サービスは、申請者と Baseline Requirements を満たす法的に有効かつ強制力のある利用契約を締結したこと、または提携する場合は申請者の代表者が利用規約を承認し受諾したことを表明する。

8. ステータス

本 CA が、有効期限内のすべての証明書のステータス(有効または失効)に関する最新情報を掲載した、24 時間 365 日アクセス可能なリポジトリーを保守し、公開していることを表明する。

9. 失効

Baseline Requirements に示された事由が発生した場合、本 CA が証明書を失効させること。

ルート CA は、自らが証明書を発行する下位 CA であるかのように、下位 CA による責務の履行と保証、下位 CA による Baseline Requirements の遵守、Baseline Requirements に基づく下位 CA のすべての責任および免責義務に対して責任を負う。

9.6.2 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 および組織、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

また 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
- 申請者およ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・失効等の申請を正確かつすみやかに行うこと

9.6.3 申請者および証明書利用者の表明保証

本 CA は、加入者契約または利用規約の一部として、本 CA および証明書の受益者の利益のために、申請者が本項で規定されているコミットメントおよび保証を行うことを要求するものとする。

本 CA は、本 CA と証明書受益者の明示的な利益のため、証明書の発行前に下記のいずれかを取得するものとする。

1. 本 CA との加入者契約に対する申請者の合意。
2. 利用規約に対する申請者の合意。

本 CA は、各加入者契約または利用規約が申請者に対して法的強制力を持つことを確実にするためのプロセスを実装するものとする。いずれの場合も、契約書は、証明書要求に従って発行される証明書に準じている必要がある。本 CA は、電子契約または「クリックスルー」契約を使用してもよい。ただし、このような契約が法的強制力を持つと本 CA が判断した場合に限る。証明書要求ごとに別々の契約を用いることも、または単一の契約で複数の将来の証明書要求およびその結果発行される証明書を対象とすることもできる。ただし本 CA が申請者に対して発行する各証明書が、明確にその加入者契約書または利用規約の対象となっていることを条件とする。

加入者契約または利用規約には、以下の義務および保証が申請者自身に課される(または請負やホスティングサービス関係に基づいて、申請者が本人や代理人を代表して策定した)条項が含まれていなければならない。

1. 情報の正確性
   証明書要求内において、また証明書の発行に関連して本 CA から要求された場合において、常に正確で完全な情報を本 CA に提供する義務および保証。
2. 私有鍵の保護
   利用者は、要求された証明書に含まれる公開鍵に対応する私有鍵（および関連する活性化データまたはデバイス（パスワードまたはトークンなど)）の管理を保証し、秘密を保持し、常に適切に保護するために、あらゆる合理的な手段を講じる義務および保証を負うものとする。
   コードサイニング証明書の場合、本 CA は、私有鍵を保護する方法に関する文書を加入者に提供する。本 CA は、この文書をホワイトペーパーとして、または利用契約の一部として提供することがある。加入者は、コード署名のベストプラクティスの文書に記載されているように、私有鍵を保管するデバイスを安全な方法で生成および運用することを表明しなければならず、この文書は、本 CA が注文手続き中に加入者へ提供する。本 CA は、利用者に対し、大文字、小文字、数字、記号を含む少なくとも 16 文字でランダムに生成されるパスワードを私有鍵の伝送に使用することを義務付ける。
3. 私有鍵再利用
   コードサイニング証明書の場合、証明書の公開鍵が他の用途の証明書に使用される予定があるか、使用されている場合、その公開鍵を使用して証明書の申請を行わない。
4. 証明書の使用
   コードサイニング証明書の場合、証明書および関連する私有鍵を、疑わしいコードに署名するために証明書を使用せず、適用されるすべての法律に準拠し、加入者契約または利用規約のみに従って証明書および私有鍵を使用することを含む、許可された法的目的のみに使用する。
   S/MIME 証明書の場合、証明書に記載されているメールボックスアドレスにおいてのみ証明書を使用し、すべての適用法に準拠し、加入者契約または利用規約に従ってのみ証明書を使用する。
5. 業界標準への準拠
   Baseline Requirements に準拠するために必要な場合、本 CA が加入者契約または利用規約を更新する可能性があることを認識し、承諾するものとする。
6. 誤用の防止

私有鍵を不正使用から保護するための適切なネットワークおよびその他のセキュリティ制御を提供し、私有鍵への不正アクセスがあった場合は、本 CA が事前の通知を必要とせずに証明書を失効する。

7. 証明書の受理

申請者または申請者の代理人が証明書の内容を正確に確認および検証するまで、証明書を使用しない。

8. 報告と失効

加入者が（a）証明書の情報が不正確または誤りである、(b）証明書に含まれる公開鍵に関連付けられた私有鍵が悪用または侵害された、(c）証明書が疑わしいコードの署名に使用されたという証拠があると判断した場合（コードサイニング証明書の場合)、証明書とそれに関連付けられた私有鍵の使用をすみやかに停止し、本 CA に証明書失効するよう、すみやかに要求する。

9. 情報の共有

(a)証明書または申請者が疑わしいコードのソースとして識別されている場合、(b)証明書を要求する権限を確認できない場合、(c）証明書が加入者リクエスト以外の理由で失効されている場合 (例えば、私有鍵の侵害、マルウェアの発見などの結果)を認識し、本 CA は、申請者、署名済みアプリケーション、証明書、および周囲の状況に関する情報を CA/ブラウザフォーラムを含む他の CA または業界グループと共有する。

10. 証明書の使用の終了

証明書の有効期限終了または失効時に、証明書に記載されている公開鍵に対応する私有鍵の使用を直ちに停止する。

11. 対応

指定された期間内の鍵の危殆化または証明書の誤用に関する本 CA の指示に対応する義務がある。

12. 承諾

申請者が利用規約または利用契約に違反した場合、本 CA は直ちに証明書を失効させる権利を有することを認め、承諾する。

9.6.4 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 または OCSP レスポンダーにより証明書が失効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

9.6.5 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」および「9.6.2 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 認証局の表明保証」および「9.6.2 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、不正使用また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
・ LRA または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
・ LRA または証明書利用者の環境（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および CRL、OCSP レスポンダ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、セコムの契約先およ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、証明書利用者および検証者に対する必要な通知をホームページ、電子メールまたは書面等によって行う。

9.12 改訂

9.12.1 改訂手続

本 CP は、セコムの判断によって適宜改訂され、認証サービス改善委員会の承認によって発効する。

9.12.2 通知方法および期間

本 CP を変更した場合、変更した本 CP をすみやかに公表することをもって、関係者に対しての告知とする。

9.12.3 オブジェクト識別子が変更されなければならない場合

認証サービス改善委員会で必要であると判断した場合に、OID を変更する。

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。仲裁および裁判地は東京都区内における紛争処理機関を専属的管轄とする。

9.14 準拠法

本 CP、CPS の解釈、有効性および証明書の利用にかかわる紛争については、日本国の法律を適用する。

9.15 適用法の遵守

本 CA は、国内における各種輸出規制を遵守し、暗号ハードウェアおよびソフトウェアを取扱うものとする。

9.16 雑則

9.16.1 完全合意条項

セコムは、本サービスの提供にあたり、証明書利用者または検証者の義務等を本 CP、および CPS によって包括的に定め、これ以外の口頭であると書面であるとを問わず、如何なる合意も効力を有しないものとする。

9.16.2 権利譲渡条項

セコムが本サービスを第三者に譲渡する場合、本 CP、および CPS において記載された責務およびその他の義務の譲渡を可能とする。

9.16.3 分離条項

本 CP、および CPS の一部の条項が無効であったとしても、当該文書に記述された他の条項は有効であるものとする。

Baseline Requirements と本 CA が業務の遂行と証明書の発行を行う地域の法律、規制、行政命令(以下、「法律」という)との間に矛盾が生じる場合、本 CA は、矛盾する要件が地域で有効かつ合法となるために必要な最小限の範囲内で Baseline Requirements の修正を行うことができる。このことは、その法律の対象となる業務または証明書発行にのみ適用される。そのような場合、本 CA はただちに(また修正された要件に基づいて証明書を発行する前に)、本 CA の CPS の本項に、Baseline Requirements への修正を必要としている法律への詳細な参照と、本 CA によって実施された Baseline Requirements への具体的な修正を盛り込むものとする。

本 CA は（修正された要件に基づく証明書を発行する前に）CA/Browser Forum に対し、CPS に新たに追加された情報について、questions@cabforum.org 宛にメールを送信するとともに、それがパブリックメーリングリストに掲載されたこと、および https://cabforum.org/pipermail/public/ (または CA/Browser Forum が指定するその他のメールアドレスやリンク)で閲覧可能なパブリックメールアーカイブでインデックス化さ

れたことを確認する通知を受信する必要がある。これにより、CA/Browser Forum は Baseline Requirements を改訂するかどうかを適宜検討できる。

法律が適用されなくなった場合、または Baseline Requirements が修正され、Baseline Requirements と法律を同時に遵守することが可能となった場合、本項に基づく本 CA の運用変更を中止する必要がある。前述した運用への適切な変更、本 CA の CPS に対する修正、および CA/Browser Forum への通知は、90 日以内に行われる必要がある。

9.16.4 強制執行条項

サービスに関する紛争は東京地方裁判所を管轄裁判所とし、セコムは、各規定文書の契約条項に起因する紛争、当事者の行為に関する損害、損失および費用について、補償および弁護士費用を当事者に求めることができる。

9.16.5 不可抗力

セコムは、天変地異、地震、噴火、火災、津波、水災、落雷、動乱、テロリズム、その他の不可抗力により生じた一切の損害について、その予見可能性の有無を問わず一切責任を負わないものとし、本 CA の提供を不可能にするに至ったときは、セコムはその状況の止むまでの間、本 CA を停止することができる。

9.17 その他の条項

規定しない。