

セコムパスポート for Web EV
認証局証明書ポリシー
Version2.78

2021年11月30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	2007/06/29	初版発行
1.10	2008/09/19	EV ガイドライン Ver1.1 への準拠
1.20	2008/12/18	鍵サイズ 2048bit への対応
1.30	2010/11/18	OCSP への対応
1.40	2012/11/09	証明書プロファイルに SubjectAltName を追加 鍵サイズ 1024bit の削除 全体的な文言および体裁の見直し
2.00	2014/08/01	メジャーバージョンアップ SECOM Passport for Web EV2.0CA を追加
2.10	2015/04/15	CAA に関する記述の追加
2.20	2015/04/30	証明書プロファイルに Certificate Transparency の拡張情報を追加
2.30	2015/12/25	ドメイン認証に関する記述の追加
2.40	2017/05/23	SECOM Passport for Web EVCA の削除 更新申請の受付日と発行日を変更 全体的な文言および体裁の見直し
2.50	2017/09/07	CAA レコードに関する記述の修正
2.60	2018/03/29	CPS の変更 EV 識別番号の登録
2.70	2018/08/01	ドメイン認証に関する記述の修正 文言の見直しを実施
2.71	2019/05/24	証明書失効事由の追記 全体的な文言および体裁の見直し
2.72	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
2.73	2020/09/01	証明書有効期間 2 年の削除
2.74	2020/09/29	CRL プロファイルの Reason code を修正
2.75	2020/10/26	組織の認証に関する記述の追加
2.76	2021/05/31	ドメイン認証に関する記述の修正 証明書失効事由の修正 鍵の危殆化に対する特別要件の追記
2.77	2021/06/15	文言および体裁の見直し 証明書失効事由の修正

2.78	2021/11/30	ドメイン認証に関する記述の修正 全体的な文言および体裁の見直し
------	------------	------------------------------------

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 CA.....	2
1.3.2 RA.....	2
1.3.3 証明書利用者.....	2
1.3.4 検証者.....	2
1.3.5 他の関係者.....	2
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.....	3
1.5.3 ポリシー適合性を決定する者.....	3
1.5.4 承認手続.....	3
1.6 定義と略語.....	4
2. 公開とリポジトリの責任.....	9
2.1 リポジトリ.....	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.....	11
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
3.2.2.1 アイデンティティ.....	11

3.2.2.2 商号/商標名	11
3.2.2.3 国の検証	11
3.2.3 個人の認証.....	12
3.2.4 検証されない証明書利用者の情報	12
3.2.5 権限の正当性確認.....	12
3.2.6 相互運用の基準	12
3.2.7 ドメインの認証	12
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.....	15
4.2.1 本人性確認と認証の実施.....	15
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	16
4.2.4 CAA レコードの確認	16
4.3 証明書の発行.....	16
4.3.1 証明書発行時の処理手続.....	16
4.3.2 証明書利用者への証明書発行通知	16
4.4 証明書の受領確認	16
4.4.1 証明書の受領確認手続	16
4.4.2 認証局による証明書の公開	16
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.....	17
4.5 鍵ペアおよび証明書の用途.....	17
4.5.1 証明書利用者の私有鍵および証明書の用途	17
4.5.2 検証者の公開鍵および証明書の用途	17
4.6 証明書の更新.....	17
4.6.1 証明書の更新事由.....	17
4.6.2 証明書の更新申請を行うことができる者	17
4.6.3 証明書の更新申請の処理手続	17
4.6.4 証明書利用者に対する新しい証明書発行通知.....	17
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	18
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	18
4.7	鍵更新をともなう証明書の更新	18
4.7.1	更新事由	18
4.7.2	新しい証明書の申請を行うことができる者	18
4.7.3	更新申請の処理手続	18
4.7.4	証明書利用者に対する新しい証明書の通知	18
4.7.5	鍵更新された証明書の受領確認手続	18
4.7.6	認証局による鍵更新済みの証明書の公開	18
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	18
4.8	証明書の変更	18
4.8.1	証明書の変更事由	19
4.8.2	証明書の変更申請を行うことができる者	19
4.8.3	変更申請の処理手続	19
4.8.4	証明書利用者に対する新しい証明書発行通知	19
4.8.5	変更された証明書の受領確認手続	19
4.8.6	認証局による変更された証明書の公開	19
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	19
4.9	証明書の失効と一時停止	19
4.9.1	証明書失効事由	19
4.9.2	証明書の失効申請を行うことができる者	21
4.9.3	失効申請手続	21
4.9.4	失効申請の猶予期間	22
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	22
4.9.6	失効確認の要求	22
4.9.7	証明書失効リストの発行頻度	22
4.9.8	証明書失効リストの発行最大遅延時間	22
4.9.9	オンラインでの失効/ステータス確認の適用性	23
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	23
4.9.11	利用可能な失効情報の他の形式	24
4.9.12	鍵の危殆化に対する特別要件	24
4.9.13	証明書の一時停止事由	25
4.9.14	証明書の一時停止申請を行うことができる者	25
4.9.15	証明書の一時停止申請手続	25
4.9.16	一時停止を継続することができる期間	25
4.10	証明書のステータス確認サービス	25

4.10.1	運用上の特徴	25
4.10.2	サービスの利用可能性	25
4.10.3	オプションな仕様	25
4.11	加入（登録）の終了	25
4.12	キーエスクローと鍵回復	26
4.12.1	キーエスクローと鍵回復ポリシーおよび実施	26
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	26
5.	設備上、運営上、運用上の管理	27
5.1	物理的管理	27
5.1.1	立地場所および構造	27
5.1.2	物理的アクセス	27
5.1.3	電源および空調	27
5.1.4	水害対策	27
5.1.5	火災対策	27
5.1.6	媒体保管	27
5.1.7	廃棄処理	27
5.1.8	オフサイトバックアップ	27
5.2	手続的管理	27
5.2.1	信頼すべき役割	27
5.2.2	職務ごとに必要とされる人数	27
5.2.3	個々の役割に対する本人性確認と認証	28
5.2.4	職務分割が必要となる役割	28
5.3	人事的管理	28
5.3.1	資格、経験および身分証明の要件	28
5.3.2	背景調査	28
5.3.3	教育要件	28
5.3.4	再教育の頻度および要件	28
5.3.5	仕事のローテーションの頻度および順序	28
5.3.6	認められていない行動に対する制裁	28
5.3.7	独立した契約者の要件	28
5.3.8	要員へ提供される資料	28
5.4	監査ログの手続	28
5.4.1	記録されるイベントの種類	28
5.4.2	監査ログを処理する頻度	29
5.4.3	監査ログを保持する期間	29
5.4.4	監査ログの保護	29

5.4.5	監査ログのバックアップ手続	29
5.4.6	監査ログの収集システム	29
5.4.7	イベントを起こした者への通知	29
5.4.8	脆弱性評価	29
5.5	記録の保管	29
5.5.1	アーカイブの種類	29
5.5.2	アーカイブ保存期間	30
5.5.3	アーカイブの保護	30
5.5.4	アーカイブのバックアップ手続	30
5.5.5	記録にタイムスタンプを付与する要件	30
5.5.6	アーカイブ収集システム	30
5.5.7	アーカイブの検証手続	30
5.6	鍵の切り替え	30
5.7	危殆化および災害からの復旧	30
5.7.1	事故および危殆化時の手続	30
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	31
5.7.3	私有鍵が危殆化した場合の手続	31
5.7.4	災害後の事業継続性	31
5.8	認証局または登録局の終了	31
6.	技術的セキュリティ管理	32
6.1	鍵ペアの生成およびインストール	32
6.1.1	鍵ペアの生成	32
6.1.2	証明書利用者に対する私有鍵の交付	32
6.1.3	認証局への公開鍵の交付	32
6.1.4	検証者への CA 公開鍵の交付	32
6.1.5	鍵サイズ	32
6.1.6	公開鍵のパラメーターの生成および品質検査	32
6.1.7	鍵の用途	32
6.2	私有鍵の保護および暗号モジュール技術の管理	32
6.2.1	暗号モジュールの標準および管理	33
6.2.2	私有鍵の複数人管理	33
6.2.3	私有鍵のエスクロー	33
6.2.4	私有鍵のバックアップ	33
6.2.5	私有鍵のアーカイブ	33
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	33
6.2.7	暗号モジュールへの私有鍵の格納	33

6.2.8	私有鍵の活性化方法	33
6.2.9	私有鍵の非活性化方法	34
6.2.10	私有鍵の破棄方法	34
6.2.11	暗号モジュールの評価	34
6.3	鍵ペアのその他の管理方法	34
6.3.1	公開鍵のアーカイブ	34
6.3.2	私有鍵および公開鍵の有効期間	34
6.4	活性化データ	34
6.4.1	活性化データの生成および設定	34
6.4.2	活性化データの保護	34
6.4.3	活性化データの他の考慮点	34
6.5	コンピュータのセキュリティ管理	35
6.5.1	コンピュータセキュリティに関する技術的要件	35
6.5.2	コンピュータセキュリティ評価	35
6.6	ライフサイクルセキュリティ管理	35
6.6.1	システム開発管理	35
6.6.2	セキュリティ運用管理	35
6.6.3	ライフサイクルセキュリティ管理	35
6.7	ネットワークセキュリティ管理	35
6.8	タイムスタンプ	35
7.	証明書および証明書失効リストおよび OCSP レスポンダー証明書のプロファイル	36
7.1	証明書のプロファイル	36
7.1.1	バージョン番号	39
7.1.2	証明書拡張	39
7.1.3	アルゴリズムオブジェクト識別子	39
7.1.4	名前形式	39
7.1.5	名前制約	39
7.1.6	CP オブジェクト識別子	39
7.1.7	ポリシー制約拡張の利用	40
7.1.8	ポリシー修飾子の文法および意味	40
7.1.9	重要な証明書ポリシー拡張の処理の意味	40
7.2	CRL のプロファイル	40
7.2.1	バージョン番号	40
7.2.2	CRL 拡張	41
7.3	OCSP のプロファイル	41
7.3.1	バージョン番号	41

7.3.2 OCSP 拡張	42
8. 準拠性監査と他の評価	43
8.1 監査の頻度	43
8.2 監査人の身元／資格	43
8.3 監査人と被監査部門の関係	43
8.4 監査で扱われる事項	43
8.5 不備の結果としてとられる処置	43
8.6 監査結果の開示	43
8.7 自己監査	43
9. 他の業務上および法的事項	44
9.1 料金	44
9.1.1 証明書の発行または更新にかかる料金	44
9.1.2 証明書のアクセス料金	44
9.1.3 失効またはステータス情報のアクセス料金	44
9.1.4 他サービスの料金	44
9.1.5 返金ポリシー	44
9.2 財務的責任	44
9.2.1 保険の補償	44
9.2.2 その他の資産	44
9.2.3 エンドエンティティの保険または保証範囲	44
9.3 企業情報の機密性	44
9.3.1 機密情報の範囲	44
9.3.2 機密情報の範囲外の情報	45
9.3.3 機密情報を保護する責任	45
9.4 個人情報の保護	45
9.4.1 個人情報保護方針	45
9.4.2 個人情報として扱われる情報	45
9.4.3 個人情報とみなされない情報	45
9.4.4 個人情報を保護する責任	45
9.4.5 個人情報の使用に関する通知と同意	45
9.4.6 司法または行政手続に沿った情報開示	45
9.4.7 その他の情報開示条件	45
9.5 知的財産権	45
9.6 表明保証	45
9.6.1 CA の表明保証	46
9.6.2 RA の表明保証	47

9.6.3 証明書利用者の表明保証.....	48
9.6.4 検証者の表明保証.....	49
9.6.5 他の関係者の表明保証.....	49
9.7 無保証.....	49
9.8 責任の制限.....	50
9.9 補償.....	50
9.10 有効期間と終了.....	50
9.10.1 有効期間.....	50
9.10.2 終了.....	50
9.10.3 終了の効果と効果継続.....	51
9.11 関係者間の個別通知と連絡.....	51
9.12 改訂.....	51
9.12.1 改訂手続.....	51
9.12.2 通知方法および期間.....	51
9.12.3 オブジェクト識別子を変更されなければならない場合.....	51
9.13 紛争解決手続.....	51
9.14 準拠法.....	51
9.15 適用法の遵守.....	52
9.16 雑則.....	52
9.16.1 完全合意条項.....	52
9.16.2 権利譲渡条項.....	52
9.16.3 分離条項.....	52
9.16.4 強制執行条項.....	52
9.16.5 不可抗力.....	52
9.17 その他の条項.....	52

1. はじめに

1.1 概要

セコムパスポート for Web EV 認証局証明書ポリシー（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「セコムトラストシステムズ」という）が運用する SECOM Passport for Web EV 2.0 CA（以下「本 CA」という）が発行する EV SSL 証明書（以下「証明書」という）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。

SECOM Passport for Web EV 2.0 CA は、Security Communication RootCA2 より片方向相互認証証明書を発行されている。

本 CA が発行する証明書は、サーバー認証や、通信経路で情報の暗号化を行うことに利用する。また、発行対象は、セコムパスポート for Web EV サービス利用規定（以下「サービス利用規定」という）により定める。

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、サービス利用規定および CPS とを照らし合わせて評価し、本 CP、サービス利用規定および CPS を承諾する必要がある。

本 CA は、<https://www.cabforum.org/>で公開される CA/ Browser Forum の EV SSL Certificate Guidelines（以下「EV ガイドライン」という）および Baseline Requirements（以下「BR」という）に準拠する。さらに、本 CA は、下位 CA、RA、委託先 RA との EV SSL 証明書および SSL 証明書の発行や保守に関連する全契約に（直接あるいは参照によって）EV ガイドラインと BR の適用しうる要件を含める。

なお、本 CP の内容がサービス利用規定、CPS の内容に抵触する場合は、サービス利用規定、本 CP、CPS の順に優先して適用されるものとする。また、セコムトラストシステムズと契約関係を持つ組織団体等との間で、別途契約書等が存在する場合、サービス利用規定、本 CP、CPS より契約書等の文書が優先される。

本 CP は、本 CA に関する技術面、運用面の発展や改良にともない、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。

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 Web EV 認証局証明書ポリシー」という。本 CP には、登録された一意のオブジェクト識別子(以下「OID」という)が割り当てられている。本 CP の OID および参照する CPS の OID は、次のとおりである。

CP/CPS	OID
セコムパスポート for Web EV 認証局証明書ポリシー	1.2.392.200091.100.721.1
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 CA

CA は、証明書の発行、失効、CRL (Certificate Revocation List : 証明書失効リスト) の開示、OCSP 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トラストシステムズである。

1.3.2 RA

RA は、証明書の発行、失効を申請する証明書利用者の実在性確認、本人性確認の審査および証明書を発行、失効するための登録業務等を行う。

1.3.3 証明書利用者

証明書利用者とは、セコムトラストシステムズに対し、証明書を申請する法人その他の組織とする。

1.3.4 検証者

検証者とは、証明書利用者の身元と公開鍵の有効性を検証する個人、法人その他の組織をいう。また、かかる公開鍵を使って証明書利用者が所有する Web サーバーとの間で暗号化通信を行う目的で、CP、CPS を信頼し、利用する個人、法人その他の組織をいう。

1.3.5 他の関係者

他の関係者とは、監査人や、セコムトラストシステムズ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 が発行する証明書は、サーバー認証や、通信経路でデータの暗号化を行うことに利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 が発行する証明書は、サーバー認証や、通信経路でデータの暗号化を行うこと以外に証明書を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、セコムトラストシステムズが行う。

1.5.2 連絡先

本 CP、証明書の申請（新規発行、更新、失効）についての問い合わせ、クレーム（利用、検証に対する不具合、証明書利用者のフィッシング）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 CA サポートセンター

住所：〒112-0015 東京都文京区目白台 2-7-8

電子メールアドレス：ra-support@secom.co.jp

ウェブサイト：<https://www.secomtrust.net/>

証明書発行・失効要求、その他証明書に関する問題の報告については 24 時間 365 日受け付ける。なお、営業時間外（09:00～18:00 以外）の問合せに関しては、緊急対応を要するもの以外は、翌営業日以降の対応になる場合がある。

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。本 CP は、最低でも年次でレビューし、改訂する。

1.5.4 承認手続

本 CP は、セコムトラストシステムズが作成・改訂を行い、認証サービス改善委員会の承認により発効される。

1.6 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。

アプリケーションソフトウェアサプライヤー(Application Software Supplier)

証明書を表示または使用し、ルート CA 証明書を組み込むインターネットブラウザソフトウェアまたはその他の依頼当事者アプリケーションソフトウェアのサプライヤー。

依頼当事者(Relying Party)

有効な証明書に依頼する個人または法人。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が単に証明書に関連する情報を表示するだけの場合、そのサプライヤーは依頼当事者とは見なされない。

エスクロー

第三者に預けること（寄託）をいう。

鍵ペア

公開鍵暗号方式において、私有鍵と公開鍵から構成される鍵の対のことをいう。

監査ログ

認証局システムへのアクセスや不正操作の有無を検査するために記録される認証局システムの動作履歴やアクセス履歴等をいう。

公開鍵

公開鍵暗号方式において用いられる鍵ペアの一方をいい、私有鍵に対応し、通信相手の相手方に公開される鍵のことをいう。

認証ドメイン名 : ADN (Authorization Domain Name)

特定の FQDN に対して、証明書発行のための認証を取得するために使用されるドメイン名

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、公開鍵に対応する証明書利用者のみが保有する鍵のことをいう。

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。

認証書 (Attestation Letter)

会計士、弁護士、政府関係者、またはその他の信頼できる第三者によって書かれた、主体者情報が正しいことを証明する文書。

リポジトリ

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

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

証明書を発行する認証局であり、証明書の発行・更新・失効、CA 私有鍵の生成・保護および証明書利用者の登録等を行う主体のことをいう。本 CP では発行局 (IA:Issuing Authority) も含まれる。

CAA (Certificate Authority Authorization)

ドメインを使用する権限において、DNS レコードの中にドメインに対して証明書を発行できる認証局情報を記述し、意図しない認証局からの証明書誤発行を防ぐ機能をいう。

CA/Browser Forum

認証局とインターネット・ブラウザベンダによって組織され、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) : 認証運用規程

CA を運用するうえでの諸手続、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。

CT (Certificate Transparency)

RFC 6962 で規定され、発行された証明書の情報を監視・監査するためにログサーバーに証明書の情報を登録し、公開する仕組みのことをいう。

EV SSL 証明書

非営利団体「CA/ Browser Forum」により新たに指針化された審査基準に従って発行される電子証明書の総称を“Extended Validation Certificate (EV 証明書) 特に Web サーバーに対し発行される場合、「EV SSL 証明書」と呼ばれる。

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。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。

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。

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、証明書利用者の代わりに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。

SHA-1 (Secure Hash Algorithm 1)

電子署名に使われるハッシュ関数 (要約関数) のひとつである。ハッシュ関数とは、与えられた原文から固定長のビット列を生成する演算手法をいう。ビット長は 160 ビット。データの送信側と受信側でハッシュ値を比較することで、通信途中で原文が改ざんされていないかを検出することができる。

SHA-256 (Secure Hash Algorithm 256)

電子署名に使われるハッシュ関数 (要約関数) のひとつである。ハッシュ関数とは、与えられた原文から固定長のビット列を生成する演算手法をいう。ビット長は 256 ビット。データの送信側と受信側でハッシュ値を比較することで、通信途中で原文が改ざんされていないかを検出することができる。

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、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 for EV

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、認証局が EV SSL 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。

WebTrust for Baseline Requirements

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、認証局が SSL 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。

WHOIS

IP アドレスやドメイン名の登録者などに関する情報を、インターネット上で参照できるサービスのことをいう。

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. 公開とリポジトリの責任

2.1 リポジトリ

セコムトラストシステムズは、証明書利用者および検証者が CRL 情報を 24 時間 365 日利用できるようなリポジトリを維持管理する。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 日利用できるような OCSP レスポンダーを管理する。ただし、保守等により、一時的にリポジトリおよび 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

セコムトラストシステムズは、次の内容をリポジトリに格納し、証明書利用者および検証者がオンラインによって参照できるようにする。

- ・ CRL
- ・ 本 CA 証明書
- ・ 最新の本 CP、CPS
- ・ 本 CA が発行する証明書に関するその他関連情報

また、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参照できるようにする。その他公開情報として、ベンダーが検証を行うためにテストサイトを用意している。

2.3 公開の時期または頻度

本 CP および CPS は、変更の都度、リポジトリに公表される。CRL は、本 CP に従って処理された失効情報を含み、発行の都度、リポジトリに公表される。また、証明書の有効期限を過ぎたものは CRL から削除される。

2.4 リポジトリへのアクセス管理

証明書利用者および検証者は、随時、リポジトリを参照できる。リポジトリへのアクセスに用いるプロトコルは、HTTP (HyperText Transfer Protocol)、HTTPS (HTTP に SSL/TLS によるデータの暗号化機能を付加したプロトコル) とする。リポジトリの情報は一般的な Web インターフェースを通じてアクセス可能である。

3. 識別と認証

3.1 名前決定

3.1.1 名前の種類

証明書に記載される証明書発行者である本 CA の名前と発行対象である証明書利用者の名前は、X.500 の識別名形式に従い設定する。

本 CA が発行する証明書には下記の情報を含むものとする。

1. 「国名」(C) は JP とする。
2. 「組織名」(O) とは、法人、またはその他の組織の名称とする。
3. 「組織単位名」(OU) は、任意選択の記入欄とする。OU の欄は、組織内のさまざまな部門等（例えば、人事、マーケティング、開発の各部門）を区別するために使用する。ただし、2022 年 9 月 1 日以降に発行される証明書には使用禁止とする。
4. 「コモンネーム」(CN) は本 CA が発行する 証明書をインストールする予定の Web サーバーにおいて使用するホスト名とする。

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コモンネームの有用性は、証明書利用者が 本 CA が発行する証明書をインストールする予定の Web サーバーの DNS 内で使われるホスト名とする。

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。

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

セコムトラストシステムズは、証明書申請に記載される名称について知的財産権を有しているかどうかの検証を行わない。証明書利用者は、第三者の登録商標や関連する名称を、本 CA に申請してはならない。セコムトラストシステムズは、登録商標等を理由に証明書利用者と第三者間で紛争が起こった場合、仲裁や紛争解決は行わない。また、セコムトラストシステムズは紛争を理由に証明書利用者からの証明書申請の拒絶や発行された証明書失効をする権利を有する。

3.2 初回の本人確認

3.2.1 私有鍵の所持を証明する方法

証明書利用者が私有鍵を所有していることの証明は、次の方法で行う。

証明書発行要求 (Certificate Signing Request : 以下「CSR」という) の署名の検証を行い、当該 CSR が、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。

3.2.2 組織の認証

セコムトラストシステムズは、組織の認証を国や地方公共団体が発行する公的書類、セコムトラストシステムズが信頼する第三者による調査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。なお、セコムトラストシステムズのサイト内 (<https://www.secomtrust.net/>) に検証ソースを開示する。

3.2.2.1 アイデンティティ

証明書利用者が、証明書利用者の設立または登録管轄地の設立機関または登録機関によって、その存在と設立(法人化)の有効性が法的に認められた組織体であるか、設立/登録機関の記録上、「不活動」、「無効」、「現行ではない」、またはこれらに相当するラベルがつけられていない組織体であるか、また政府機関についてはかかる政府組織が運営されている下位政府組織内で、申請者が法的に認められた政府組織として存在するかを検証する。

3.2.2.2 商号/商標名

主体者のアイデンティティ情報に商号または商標名が含まれる場合、本 CA は、以下の方法により商号/商標名を使用するための申請者の権利を検証するものとする。

1. 申請者の法的な設立、存在、または承認の管轄地域にある政府機関が提供するドキュメントまたは、このような政府機関とのやり取りで得られた情報。

3.2.2.3 国の検証

証明書の主体者識別名に **countryName** フィールドが存在する場合、本 CA は、次のいずれかを使用して主体者と関連付けられた国を検証するものとする

- ・ドメイン名登録機関によって提供された情報
- ・本 CP 「3.2.2.1 アイデンティティ」に記載されている方法。

3.2.3 個人の認証

セコムトラストシステムズは、個人の認証を、国や地方公共団体が発行する公的書類、セコムトラストシステムズが信頼する第三者による調査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。

3.2.4 検証されない証明書利用者の情報

本 CA は、利用者から提出された証明書発行申請書類および CSR 情報から、部門名 (**Organizational Unit Name**) については、誤解を与えるものでないことを確認する。

3.2.5 権限の正当性確認

セコムトラストシステムズは、証明書に関する申請を行う者が、その申請を行うための正当な権限を有していることを本 CP 「3.2.2 組織の認証」または「3.2.3 個人の認証」によって確認する。また、証明書利用者以外の第三者からの申請の場合で、証明書利用者に直接申込の意思確認ができない時は、当該第三者が証明書利用者の代理人であることを証する委任状を必要とする。

- ※ 本項の証明書利用者とは、「3.1.1 名前の種類」で定める証明書のコモンネームに記載されるホスト名を使用する法人、その他の組織をいう。

3.2.6 相互運用の基準

本 CA は **Security Communication RootCA2** より、片方向相互認証証明書を発行されている。

3.2.7 ドメインの認証

セコムトラストシステムズは、証明書利用者がドメイン名の利用権を有しているか確認するため、BR に準拠した次の方法を使用してドメインの認証を行う。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. **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、ファックス、**SMS**、または郵便にてランダム値を送信し、ランダムな値が含まれた確認応答を受け取ることによって、**FQDN** に対する申請者の権限を立証する。

ランダム値は、ドメイン連絡先と認識される電子メールアドレス、ファックス番号、SMS番号、または住所宛に送付する。また、電子メール、ファックス、SMS、または郵便で、複数の認証ドメイン名の管理を確認することもできる。

(BR セクション 3.2.2.4.2)

2. ローカル部は'admin'、'administrator'、'webmaster'、'hostmaster'、または'postmaster'とし、「@」以下は認証ドメイン名として作成した電子メールアドレスにランダム値を送信して、ランダムな値が含まれた確認応答を受け取ることによって、要求された FQDN の制御を実証する。電子メールアドレスで使用する「@」以下の認証ドメイン名は、証明書発行対象となる FQDN に含まれるドメイン名とし、また、認証ドメインが同じであれば、電子メールで複数の FQDN を確認することもできる。(BR セクション 3.2.2.4.4)
3. 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、FQDN に対する申請者の制御を確認する。本 CA は承認済みポートを介してアクセスし、「http(またはhttps):// [証明書発行対象となる FQDN] /.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。(BR セクション 3.2.2.4.18)
4. 証明書発行対象となる FQDN、または認証ドメイン名（それぞれ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、FQDN に対する申請者の権限を立証する。関連する CAA リソースレコードは、RFC 8659 のセクション 3 で定義されている検索アルゴリズムを使用して確認する必要がある。(BR セクション 3.2.2.4.7)
5. 認証ドメイン名の DNS CAA レコードの Email 連絡先へ、電子メール経由で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、FQDN に対する申請者の権限を立証する。また、Email 連絡先が同じであれば、電子メールで複数の FQDN を確認することもできる。(BR セクション 3.2.2.4.13)
6. 認証ドメイン名の DNS TXT レコードの Email 連絡先へ、電子メール経由で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、

FQDN に対する申請者の権限を立証する。また、Email 連絡先が同じであれば、電子メールで複数の FQDN を確認することもできる。(BR セクション 3.2.2.4.14)

7. ドメイン連絡先の電話番号へ電話し、認証ドメイン名の使用許可のレスポンスを得ることで、FQDN に対する申請者の権限を立証する。また、複数の認証ドメイン名においてドメイン連絡先の電話番号が同じ場合、各認証ドメイン名を提示して使用許可のレスポンスを得ることで、複数の FQDN に対して権限を立証することもできる。(BR セクション 3.2.2.4.15)
8. DNS TXT レコードの電話連絡先の電話番号へ電話し、認証ドメイン名の使用許可のレスポンスを得ることで、FQDN に対する申請者の権限を立証する。また、複数の認証ドメイン名において電話連絡先の電話番号が同じ場合、各認証ドメイン名を提示して使用許可のレスポンスを得ることで、複数の FQDN に対して権限を立証することもできる。(BR セクション 3.2.2.4.16)
9. DNSCAA レコードの電話連絡先の電話番号へ電話し、認証ドメイン名の使用許可のレスポンスを得ることで、FQDN に対する申請者の権限を立証する。また、複数の認証ドメイン名において電話連絡先の電話番号が同じ場合、各 FQDN を提示して使用許可のレスポンスを得ることで、複数の FQDN に対して権限を立証することもできる。(BR セクション 3.2.2.4.17)

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

鍵更新時における証明書利用者の本人性確認および認証は、本 CP「3.2 初回の本人確認」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

失効した証明書の更新は行わない。証明書申請は新規扱いとし、証明書利用者の本人性確認および認証は、本 CP「3.2 初回の本人確認」と同様とする。

3.4 失効申請時の本人性確認と認証

セコムトラストシステムズは、証明書利用者だけがアクセス可能なホームページからの失効申請を受け付けた後、証明書利用者の本人性確認と認証を行う。

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

証明書の申請を行うことのできる者は、証明書を使用する法人、その他の法人のお客様組織別提出書類基準[セコムパスポート for Web EV]に基づく権限者、または権限者から委任された代理人とする。

本 CP「5.5.2 アーカイブ保存期間」に従い、本 CA は、フィッシングまたはその他の詐欺的使用の疑いあるいは懸念を理由に、以前に失効した証明書および以前に拒否した証明書要求をすべて含む内部データベースを保持するものとする。本 CA は、この情報を使用して、以降の疑わしい証明書要求を識別するものとする。

4.1.2 申請手続および責任

証明書利用者および証明書利用者から申請手続きを委任された代理人は、証明書の発行申請を行うにあたり、本 CP、サービス利用規定および 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。

証明書申請の方法は、ホームページに掲載している「お申し込み手順」に従い、必要書類をセコムトラストシステムズに提出する。

4.2 証明書申請手続

4.2.1 本人性確認と認証の実施

セコムトラストシステムズは、証明書申請を受け付けた後、本 CP「3.2 初回の本人確認」に基づく確認を行う。

証明書要求には、証明書に含めるべき申請者に関するすべての事実情報、および本 CA が **Baseline Requirements** および本 CA の証明書ポリシーや認証局運用規定に準拠するために申請者から取得する必要がある追加情報を含めてもよい。証明書要求が申請者に関する必要な情報の一部を欠いている場合、本 CA は、残りの情報を申請者から取得するか、または信頼できる独立した第三者機関のデータ情報源から情報を取得して申請者に確認するものとする。本 CA は、申請者によって証明書に含めることを要求されたすべてのデータを検証するための文書化された手順を確立し、それに従うものとする。

本 CA は、ハイリスクの証明書要求が **Baseline Requirements** に従って適切に検証されるようにするために合理的に必要な場合において、証明書の承認前にハイリスク証明書要求に対する追加の検証活動を識別し要求する、文書化された手順を作成、保持、実施

するものとする。

4.2.2 証明書申請の承認または却下

セコムトラストシステムズは、審査の結果、承認を行った申請について証明書の発行を行い、証明書利用者に審査終了および証明書発行について通知する。証明書の申請に不備があった場合は、証明書利用者に対し、不備の理由と必要書類等の再提出を通知する。

4.2.3 証明書申請の処理時間

セコムトラストシステムズは、承認を行った証明書申請について、すみやかに証明書の発行を行う。

4.2.4 CAA レコードの確認

本CAは、申請情報の審査時にCAAレコードを確認する。CAAレコードに記載する本CAのドメインは「secomtrust.net」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

セコムトラストシステムズは、証明書申請の審査終了後に、証明書発行を行い、証明書利用者だけがアクセス可能なホームページに証明書ダウンロード設定を行う。

4.3.2 証明書利用者への証明書発行通知

セコムトラストシステムズは証明書利用者に対し、証明書利用者だけがアクセス可能なホームページに証明書ダウンロード設定が完了したことを、電子メールで通知する。証明書利用者は、本CAからの通知を受信した後、証明書をダウンロードすることができる。または、証明書利用者に対して証明書を送付することで発行通知とする。

4.4 証明書の受領確認

4.4.1 証明書の受領確認手続

証明書利用者が、証明書利用者だけがアクセス可能なホームページから証明書をダウンロードしたことをもって、証明書が受領されたものとする。または、証明書利用者に対して証明書を送付した場合、送付後 1 週間以内に証明書利用者から証明書記載の誤りなどの申し出が無いことをもって証明書が受領されたものとする。

4.4.2 認証局による証明書の公開

本 CA の CA 証明書は、リポジトリに公開される。本 CA は、CT (Certificate Transparency) ログに登録することにより、証明書利用者の証明書を公開することができる。

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

セコムトラストシステムズは、証明書申請時に登録された担当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用途

4.5.1 証明書利用者の私有鍵および証明書の用途

証明書利用者は、私有鍵および証明書の用途として、サーバー認証や、通信経路で情報の暗号化を行うことに利用する。証明書利用者は、本 CA が承認をした用途のみに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。その他の用途に利用してはならない。

4.5.2 検証者の公開鍵および証明書の用途

検証者は、本 CA の証明書を使用し、本 CA が発行した証明書の信頼性を検証することができる。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を推奨する。

4.6.1 証明書の更新事由

規定しない。

4.6.2 証明書の更新申請を行うことができる者

規定しない。

4.6.3 証明書の更新申請の処理手続

規定しない。

4.6.4 証明書利用者に対する新しい証明書発行通知

規定しない。

4.6.5 更新された証明書の受領確認手続
規定しない。

4.6.6 認証局による更新された証明書の公開
規定しない。

4.6.7 他のエンティティに対する認証局の証明書発行通知
規定しない。

4.7 鍵更新をとまなう証明書の更新

4.7.1 更新事由

証明書の更新は、証明書の有効期間が満了する場合に行うことができる。失効した証明書または有効期限が切れた証明書は更新できない。

証明書の更新申請は、有効期間満了の 90 日前から行うことができる。

4.7.2 新しい証明書の申請を行うことができる者

本 CP「4.1.1 証明書の申請を行うことができる者」と同様とする。

4.7.3 更新申請の処理手続

本 CP「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

本 CP「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

本 CP「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

本 CP「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

本 CP「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

本 CA は、証明書に登録された情報の変更が必要となった場合、その証明書の失効および

新規発行とする。

4.8.1 証明書の変更事由

規定しない。

4.8.2 証明書の変更申請を行うことができる者

規定しない。

4.8.3 変更申請の処理手続

規定しない。

4.8.4 証明書利用者に対する新しい証明書発行通知

規定しない。

4.8.5 変更された証明書の受領確認手続

規定しない。

4.8.6 認証局による変更された証明書の公開

規定しない。

4.8.7 他のエンティティに対する認証局の証明書発行通知

規定しない。

4.9 証明書の失効と一時停止

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、セコムトラストシステムズに対し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、セコムトラストシステムズは、次の事由が発生した場合に、失効申請の有無に関わらず、セコムトラストシステムズの判断により証明書利用者の証明書を失効することができるものとする。

- ・ 証明書利用者がサービス利用規定、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
- ・ 本 CA が、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
- ・ 証明書利用者および本 CA の私有鍵が侵害され、アルゴリズムのタイプと基準要件の鍵サイズの要件を遵守していないこと、あるいは証明書が他の方法で悪用されているという合理的な証拠を得た場合
- ・ 証明書が BR、本 CP または CPS に準拠して発行されていないことを知りえた場合
- ・ 契約違反その他の事由によりセコムトラストシステムズ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
- ・ サービス契約に基づき、セコムトラストシステムズとの契約を解除した場合
- ・ セコムトラストシステムズが失効を必要とすると判断するその他の状況が認められた場合

なお、本 CA は次の事象のうち1つ以上が発生した場合、24 時間以内に失効を行うものとする。

- ・ 証明書利用者が書面で本 CA に証明書の失効を要求した場合
- ・ 証明書利用者が本 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
- ・ 本 CA が、証明書利用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
- ・ 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)に基づいて利用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
- ・ 本 CA が、証明書内におけるドメイン認証の承認、または完全修飾ドメイン名や IP アドレスの管理が信用できない証拠を得た場合

また、本 CA は次の事象のうち1つ以上が発生した場合、24 時間以内に失効させるべきであり、5 日以内に失効を行うものとする。

- ・ 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
- ・ 本 CA が、証明書の不正使用の証拠を得た場合
- ・ 証明書利用者がサービス契約、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
- ・ 本 CA が、証明書内における完全修飾ドメイン名または IP アドレスの使用が、法的にもはや許可されていないことを示す状況を知り得た場合(たとえば、ドメイン名を

使用するドメイン名登録者の権利が裁判所または裁定者によって失効となった、ドメイン名登録者と申請者との間の関連するライセンス契約またはサービス契約が解除された、ドメイン名登録者がドメイン名の更新を怠ったなど)

- ・ 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
- ・ 証明書が BR または本 CP や CPS に従って発行されなかったことを本 CA が知り得て、失効が必要と判断した場合
- ・ 証明書に表示されている情報が不正確であると、本 CA が判断または知り得た場合
- ・ BR に基づいて証明書を発行するための本 CA の権利が期限切れ、失効、または停止となった場合(本 CA が CRL/OCSP リポジトリーの維持を継続するための手配を済ませている場合を除く)
- ・ 本 CP や CPS により、失効が必要とされた場合
- ・ 本 CA が、証明書利用者の私有鍵を危殆化させる実証済みの方法、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

また、以下のような場合では、商業的に合理的な期間内に失効を行う場合もある。

- ・ 利用者事由の証明書記載情報に変更にともなう証明書の失効
- ・ サービス終了やサイト閉鎖などの利用者事由による、証明書の利用中止にともなう証明書の失効
- ・ 利用者からの支払いの遅延や滞納にともなう証明書の失効
- ・ サーバーの入れ替えなどの利用者事由により証明書が再発行された場合の、元証明書の失効
- ・ セコムトラストシステムズとの契約終了にともなう、証明書の失効
- ・ 倒産や会社閉鎖にともなう証明書の失効

4.9.2 証明書の失効申請を行うことができる者

証明書の失効申請を行うことができる者は、証明書を使用している法人、その他の法人のお客様組織別提出書類基準[セコムパスポート for Web EV]に基づく権限者、または権限者から委任された代理人とする。

また、RA、本 CA が失効手続きを開始できる。加えて、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、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本 CA に提出できる。

4.9.3 失効申請手続

証明書利用者は、証明書利用者だけがアクセス可能なホームページから該当の証明書情報を選択し失効申請を行う。

4.9.4 失効申請の猶予期間

証明書利用者は、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には、すみやかに失効申請を行わなければならない。

4.9.5 認証局が失効申請を処理しなければならない期間

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するものとし、加入者と証明書問題レポートを提出した事業者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 は加入者そして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告知と協力するものとし、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、本 CP「4.9.1 証明書失効事由」に記載された時間枠を超えない。

CA に選ばれた日時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、厳しさ、規模、被害リスク)
2. 失効の結果(加入者と依拠当事者への直接的そして間接的影響)
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. 苦情を申し立てている組織体

なお、本 CA は、失効日が指定された失効申請を受領した場合は、指定日に失効を行う。

4.9.6 失効確認の要求

本 CA が発行する証明書には、CRL 格納先の URL、および OCSP レスポンダーの URL を記載する。

CRL および OCSP レスポンダーは、一般的な Web インターフェースを用いてアクセスすることができる。なお、CRL には有効期限の切れた証明書情報は含まれない。

検証者は、証明書利用者の証明書について、有効性を確認しなければならない。証明書の有効性は、リポジトリサイトに掲載している CRL または OCSP レスポンダーにより確認することができる。

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 が発行した CRL は、即時にリポジトリに反映させる。

4.9.9 オンラインでの失効/ステータス確認の適用性

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-nocheck` 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 および/または 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 レスポンダーは、「予約済み」証明書のシリアル番号について、Precertificate [RFC 6962]に一致する対応する証明書があるかのように、明確な応答を提供する場合がある。

OCSP 要求内の証明書シリアル番号は、次の 3 つのオプションのいずれか

1. その CA の主体者に関連付けられている現在または以前のキーを使用して、そのシリアル番号の証明書が発行 CA によって発行された場合、「割り当て済み」
2. そのシリアル番号を持つ事前証明書 [RFC6962]が a または b のいずれか
 - a. 発行 CA によって発行された場合、「予約済み」
 - b. 発行 CA に関連付けられた事前証明書署名証明書[RFC6962]
3. 上記の条件のいずれも満たされない場合は「未使用」

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、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

検証者は、次の方法で鍵の危殆化を実証するものとする。

- ・ 私有鍵自体の提出、または私有鍵を含むデータと、データから私有鍵を抽出する方法の提出
- ・ 危殆化されたと認識される識別名などのデータを含み、かつ署名の検証ができる CSR の提出
- ・ 公開鍵によって検証可能な、本 CA が指定したチャレンジ・レスポンスと公開鍵への私有鍵による署名の提出
- ・ 侵害を検証できる脆弱性や、参照したセキュリティ・インシデント・ソースの提供

本 CA は、証明書利用者の私有鍵が危殆化した可能性があることを知りえた場合、証明書利用者に私有鍵が危殆化された可能性があることを通知する。

なお本 CA が、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、本

CP「4.9.1 証明書失効事由」の対応を行うものとする。

4.9.13 証明書の一時停止事由

本 CA は、証明書の一時停止は行わない。

4.9.14 証明書の一時停止申請を行うことができる者

適用外とする。

4.9.15 証明書の一時停止申請手続

適用外とする。

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

証明書利用者および検証者は OCSP レスポンダーを通じて証明書ステータス情報を確認することができる。本 CA は、CRL または OCSP レスポンスの失効エントリは、失効した証明書の有効期限日が過ぎるまで削除してはならない。

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りソースで、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 オプションな仕様

規定しない。

4.11 加入（登録）の終了

証明書利用者は本サービスの利用を終了する場合、証明書の失効申請を行わなければな

らない。なお、証明書の更新申請を行わず、証明書の有効期間が満了した場合にも終了となる。

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

セコムトラストシステムズは、CPS「5.4.1 記録されるイベントの種類」の本CAに関連するシステムに係るログに加えて、次の情報をアーカイブとして保存する。

- ・ 発行した証明書およびCRL
- ・ CRLの発行に関する処理履歴
- ・ 本CP
- ・ 本CPに基づき作成された認証局の業務運用を規定する文書
- ・ 認証業務を他に委託する場合には、委託契約に関する書類
- ・ 監査の実施結果に関する記録および監査報告書
- ・ 証明書利用者からの申請書類
- ・ OCSPレスポンスへのアクセスログ

5.5.2 アーカイブ保存期間

セコムトラストシステムズは、アーカイブを最低 10 年間保存する。

5.5.3 アーカイブの保護

アーカイブは、許可された者しかアクセスできないよう制限された施設において保管する。

5.5.4 アーカイブのバックアップ手続

証明書発行、失効または CRL の発行等、本 CA に関連するシステムに関する重要なデータに変更がある場合は、適時、アーカイブのバックアップを取得する。

5.5.5 記録にタイムスタンプを付与する要件

セコムトラストシステムズは、NTP (Network Time Protocol) を使用して本 CA に関連するシステムの時刻同期を行い、本 CA に関連するシステム内で記録される重要な情報に対しタイムスタンプを付与する。

5.5.6 アーカイブ収集システム

アーカイブの収集システムは、本 CA に関連するシステムの機能に含まれている。

5.5.7 アーカイブの検証手続

アーカイブは、セキュアな保管庫からアクセス権限者が入手し、定期的に媒体の保管状況の確認を行う。また必要に応じ、アーカイブの完全性および機密性の維持を目的として、新しい媒体への複製を行う。

5.6 鍵の切り替え

本 CA の私有鍵は、私有鍵に対応する証明書の有効期間が証明書利用者に発行した証明書の最大有効期間よりも短くなる前に新たな私有鍵の生成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

セコムトラストシステムズは、事故および危殆化が発生した場合にすみやかに本 CA に関連するシステムおよび関連する業務を復旧できるよう、以下を含む事故および危殆化に対する対応手続を策定する。

- ・ CA 私有鍵の危殆化

- ・ ハードウェア、ソフトウェア、データ等の破損、故障
- ・ 火災、地震等の災害

5.7.2 ハードウェア、ソフトウェアまたはデータが破損した場合の手続

セコムトラストシステムズは、本 CA に関連するシステムのハードウェア、ソフトウェアまたはデータが破損した場合、バックアップ用として保管しているハードウェア、ソフトウェアまたはデータを使用して、すみやかに本 CA に関連するシステムの復旧作業を行う。

5.7.3 私有鍵が危殆化した場合の手続

セコムトラストシステムズは、本 CA の私有鍵が危殆化したまたは危殆化のおそれがあると判断した場合、および災害等により本 CA に関連するシステムの運用が中断、停止につながるような状況が発生した場合には、予め定められた計画、手順に従い、安全に運用を再開させる。

5.7.4 災害後の事業継続性

セコムトラストシステムズは、不測の事態が発生した場合にすみやかに復旧作業を実施できるよう、予め本 CA に関連するシステムの代替機の確保、復旧に備えたバックアップデータの確保、復旧手続の策定等、可能な限りすみやかに認証基盤システムを復旧するための対策を行う。

5.8 認証局または登録局の終了

セコムトラストシステムズが本 CA を終了する場合、事前に証明書利用者その他の関係者にその旨を通知する。本 CA によって発行されたすべての証明書は、本 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、証明書利用者自身が生成する。

本 CA が推奨する Web サーバーの鍵ペア生成方法については、セコムトラストシステムズのホームページに記載する。

6.1.2 証明書利用者に対する私有鍵の交付

本 CA から私有鍵の交付は行わない。

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

本項については、CPS に規定する。

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, keyEncipherment を設定する。

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。

証明書利用者の私有鍵については規定しない。

6.2.2 私有鍵の複数人管理

本 CA の私有鍵の活性化、非活性化、バックアップ等の操作は、安全な環境において複数人の権限者によって行う。

証明書利用者の私有鍵の活性化、非活性化、バックアップ等の操作は、証明書利用者の管理の下で安全に行わなければならない。

6.2.3 私有鍵のエスクロー

本 CA は、本 CA の私有鍵のエスクローは行わない。

本 CA は、証明書利用者の私有鍵のエスクローは行わない。

6.2.4 私有鍵のバックアップ

本 CA の私有鍵のバックアップは、セキュアな室において複数名の権限者によって行われ、暗号化された状態で、セキュアな室に保管される。

証明書利用者の私有鍵のバックアップは、証明書利用者の管理の下で安全に保管しなければならない。

6.2.5 私有鍵のアーカイブ

本 CA では、本 CA の私有鍵のアーカイブは行わない。

証明書利用者の私有鍵については規定しない。

6.2.6 私有鍵の暗号モジュールへの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

本電子認証基盤の上で運用される CA の私有鍵は、HSM 内に格納する。

証明書利用者の私有鍵については規定しない。

6.2.8 私有鍵の活性化方法

本 CA の私有鍵の活性化は、セキュアな室において複数名の権限者によって行う。

証明書利用者の私有鍵については規定しない。

6.2.9 私有鍵の非活性化方法

本 CA の私有鍵の非活性化は、セキュアな室において複数名の権限者によって行う。
証明書利用者の私有鍵については規定しない。

6.2.10 私有鍵の破棄方法

本 CA の私有鍵の廃棄は、複数名の権限者によって完全に初期化または物理的に破壊することによって行う。バックアップについても同様の手続によって行う。
証明書利用者の私有鍵については規定しない。

6.2.11 暗号モジュールの評価

本 CA で使用する HSM の品質基準については、本 CP 「6.2.1 暗号モジュールの標準および管理」のとおりである。
証明書利用者の私有鍵については規定しない。

6.3 鍵ペアのその他の管理方法

6.3.1 公開鍵のアーカイブ

本 CA の公開鍵については CPS 「6.2.1 暗号モジュールの標準および管理」のとおりである。
証明書利用者の私有鍵については規定しない。

6.3.2 私有鍵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 コンピュータのセキュリティ管理

6.5.1 コンピュータセキュリティに関する技術的要件

本項については、CPSに規定する。

6.5.2 コンピュータセキュリティ評価

本項については、CPSに規定する。

6.6 ライフサイクルセキュリティ管理

6.6.1 システム開発管理

本項については、CPSに規定する。

6.6.2 セキュリティ運用管理

本項については、CPSに規定する。

6.6.3 ライフサイクルセキュリティ管理

本項については、CPSに規定する。

6.7 ネットワークセキュリティ管理

本項については、CPSに規定する。

6.8 タイムスタンプ

本項については、CPSに規定する。

7. 証明書および証明書失効リストおよび OCSP レスポンダー証明書のプロファイル

7.1 証明書のプロファイル

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 SECOM Passport for Web EV 2.0 CA サーバー証明書プロファイル

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		例) 0123456789	-
Signature Algorithm		SHA256 with RSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O=SECOM Trust Systems CO.,LTD.	-
	Common Name	CN=SECOM Passport for Web EV 2.0 CA	-
Validity	NotBefore	例) 2018/2/1 00:00:00 GMT	-
	NotAfter	例) 2019/2/1 00:00:00 GMT	-
Subject	Country	C=JP (固定値)	-
	State Or Province	必須	-
	Locality	必須	-
	jurisdictionOfIncorporationCountryName	JP (固定値)	-
	Organization	必須	-
	Organizational Unit	任意 ただし、2022 年 9 月 1 日以降に発行される場合、禁止	-
	Common Name	サーバー名 (必須)	-
	Serial Number	必須 (※1)	-
	businessCategory	必須 (※2)	-
Subject Public Key Info		主体者の公開鍵 2048 ビット	-
拡張領域		設定内容	critical
KeyUsage		digitalSignature, keyEncipherment	y

ExtendedKeyUsage	serverAuth	n
Subject Alt Name	dnsName=サーバー名	n
CertificatePolicies	[1]policyIdentifier OID=1.2.392.200091.100.721.1 policyQualifiers policyQualifierId=CPS qualifier=本 CA のリポジトリ HTTP(S) URL [2]policyIdentifier=2.23.140.1.1	n
CRL Distribution Points	本 CA の CRL サービスの HTTP URL	n
Authority Information Access	accessMethod ocsp (1.3.6.1.5.5.7.48.1) accessLocation OCSP レスポンダーの HTTP URL CA Issuers (1.3.6.1.5.5.7.48.2) accessLocation 本 CA 証明書の HTTP URL * CA Issuers は必要に応じて設定する	n
Authority Key Identifier	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
Certificate Transparency 用拡張 (1.3.6.1.4.1.11129.2.4.2)	SignedCertificateTimestampList の 値	n

表 7.1-2 SECOM Passport for Web EV 2.0 CA OCSP レスポンダー証明書プロファイル

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		例) 0123456789	-
Signature Algorithm		SHA256 with RSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O=SECOM Trust Systems CO.,LTD.	-
	Common Name	CN=SECOM Passport for Web EV 2.0 CA	-
Validity	NotBefore	例) 2018/12/1 00:00:00 GMT	-
	NotAfter	例) 2019/4/1 00:00:00 GMT	-

Subject	Country	C=JP (固定値)	-
	Organization	SECOM Trust Systems CO.,LTD. (固定値)	-
	Common Name	OCSP レスポンダー名 (必須)	-
Subject Public Key Info		主体者の公開鍵 2048 ビット	-
拡張領域		設定内容	critical
KeyUsage		digitalSignature	y
ExtendedKeyUsage		OCSPSigning	n
OCSP No Check		null	n
CertificatePolicies		policyIdentifier OID=1.2.392.200091.100.721.1 policyQualifiers policyQualifierId=CPS qualifier=本 CA のリポジトリ HTTP(S) URL	n
Authority Key Identifier		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

(※1) 証明書利用者が次の場合、本 CA は **Serial Number** に以下を設定する。

登記されている法人 : 会社法人等番号、または法人番号
 中央省庁および国の機関 : 法人番号、または設立日
 地方公共団体およびその機関 : 法人番号、または設立日
 国立大学・高校機関 : 法人番号、または設立日

なお、セコムトラストシステムズにより法人番号も設立日も確認できなかった場合、**Serial Number** には以下の文言を記載する。

中央省庁および国の機関 : Government
 地方公共団体およびその機関 : Local Government
 国立大学・高校機関 : Public School

(※2) 証明書利用者が次の場合、本 CA は **businessCategory** に以下を設定する。

登記されている法人 : Private Organization
 中央省庁および国の機関 : Government Entity
 地方公共団体およびその機関 : Government Entity

国公立大学・高校機関 : Government Entity

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。

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

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。本 CA は、BR セクション 3.2.2.4 または BR セクション 3.2.2.5 に定める場合を除き、識別名にドメイン名または IP アドレスを含めてはならない。

識別名には、'!', '!', " (スペース) 文字などのメタデータや、値が存在しない、不完全、または適用できないことを示すその他の記号のみを含めてはならない。

7.1.5 名前制約

本 CA では設定しない。

7.1.6 CP オブジェクト識別子

本 CA が発行する証明書の OID は、本 CP 「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 BR 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。

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140)
certificate-policies(1) ev-guidelines(1)} (2.23.140.1.1)

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 のプロファイル

本 CA が発行する CRL 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 7.2-1 SECOM Passport for Web EV 2.0 CA CRL プロファイル

基本領域		設定内容	critical
Version		Version 2	-
Signature Algorithm		SHA256 with RSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O= SECOM Trust Systems CO.,LTD.	-
	Common Name	CN=SECOM Passport for Web EV 2.0 CA	-
This Update		例) 2018/2/1 00:00:00 GMT	-
Next Update		例) 2018/2/5 00:00:00 GMT	-
Revoked Certificates	Serial Number	例) 0123456789	-
	Revocation Date	例) 2018/2/1 00:00:00 GMT	-
	Reason Code	例) cessation of operation (失効事由) *設定任意	-
拡張領域		設定内容	critical
CRL Number		CRL 番号	n
Authority Key Identifier		発行者公開鍵の SHA-1 ハッシュ値 (160 ビット)	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。

reasonCode (OID 2.5.29.21)

2020 年 9 月 30 日より、次の要件をすべて満たす必要がある。

reasonCode が存在する場合、この拡張を **critical** としてマークしてはならない。

CRL エントリーがルート CA または下位 CA 証明書（クロス証明書を含む）のためのものである場合、この CRL エントリー拡張が存在しなければならない。

CRL エントリーが CA ではなく、加入者証明書用である場合、この CRL エントリー拡張は存在すべきであるが、以下の要件を満たすことを条件に省略してもよい。

CRLReason は、**unspecified (0)**であってはならない。失効の理由が特定されていない場合、以前の要件で許可されていれば、CA は **reasonCode** エントリー拡張を省略しなければならない。CRL エントリーが **Baseline Requirements** の対象とならない証明書用であり、2020 年 9 月 30 日以降に発行されたか、2020 年 9 月 30 日以降に **notBefore**（発行日）である場合、**CRLReason** は **certificateHold (6)**を使用してはいけない。CRL エントリーが **Baseline Requirements** の対象となる証明書用である場合、**CRLReason** は **certificateHold (6)**を使用してはいけない。

reasonCode CRL エントリー拡張が存在する場合、**CRLReason** は、その CP/CPS 内の CA によって定義されているように、証明書の失効の最も適切な理由を示さなければならない。

本 CA では、以下の **reasonCode** を使用するものとする。

- keyCompromise (1)**
- affiliationChanged (3)**
- superseded (4)**
- cessationOfOperation (5)**

7.3 OCSP のプロファイル

本 CA は RFC5019 および 6960 に準拠する証明書に対して OCSP レスポンダーを提供する。2020 年 9 月 30 日以降より、OCSP 応答がルート CA または下位 CA 証明書（クロス証明書を含む）に対するものであり、その証明書が失効されている場合、**CertStatus** の **RevokedInfo** 内の **revocationReason** フィールドが存在する必要がある。

2020 年 9 月 30 日以降より、**CRLReason** は、本 CP「7.2.2 CRL 拡張」で指定されているように、CRL に許可された値を含める必要があることを示す。

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 CP 「7.1 証明書のプロファイル」に記載する。OCSP 応答の `singleExtensions` には、`reasonCode` (OID 2.5.29.21) CRL エントリー拡張を含めてはならない。

8. 準拠性監査と他の評価

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。本 CA が行う準拠性監査に関する諸事項については本 CP および CPS に規定する。

8.1 監査の頻度

セコムトラストシステムズは、本サービスが本 CPS および CP に準拠して運用されているかに関して、年に 1 回以上の準拠性監査を行う。

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、セコムトラストシステムズとの間に特別な利害関係のない監査人を選定する。

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 EV 規準、WebTrust for BR 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

セコムトラストシステムズは、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

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

なお、WebTrust for CA、WebTrust for EV、WebTrust for BR の検証に関する報告書は、WebTrust for CA、WebTrust for EV、WebTrust for BR 認定の規則に従い、特定のサイトにて参照可能となる。

8.7 自己監査

CPS に規定する。

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
セコムトラストシステムズは、本 CA の運用維持にあたり、十分な財務的基盤を維持するものとする。

9.2.2 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、セコムトラストシステムズに帰属する財産である。

- ・ 本 CP
- ・ セコムステッカーおよびステッカー証明ページ

9.6 表明保証

9.6.1 CA 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. ドメイン名または IP アドレスを使用する権利
発行の時点で、本 CA が、以下を満たすこと。
 - i. 証明書の主体者フィールドおよび **subjectAltName** 拡張領域に指定されているドメイン名および IP アドレスを使用する権利を申請者が保持または管理していること(あるいは、ドメイン名の場合のみ、かかる権利または管理が、それらを使用または管理する権利を有する他の人物によって委託されたこと)を検証するための 手順を導入していること。
 - ii. 証明書を発行する際にその手順に従っていること。
 - iii. CA の CP/CPS にその手順を正確に記述していること。
2. 証明書に対する承認
発行の時点で、本 CA が、以下を満たすこと。
 - i. 主体者によって証明書の発行が承認され、主体者を代表して証明書を要求する権限を申請権限者が有していることを確認するための手順を導入していること。
 - ii. 証明書を発行する際にその手順に従っていること。
 - iii. CA の CP/CPS にその手順を正確に記述していること。
3. 情報の正確性
発行の時点で、本 CA が、以下を満たすこと。

- i. 証明書に含まれるすべての情報(主体者識別名の `organizationalUnitName` 属性を除く)の正確性を検証するための手順を導入していること。
 - ii. 証明書を発行する際にその手順に従っていること。
 - iii. CA の CP/CPS にその手順を正確に記述していること。
4. 誤解を招く情報の排除
- 発行の時点で、本 CA が、以下を満たすこと。
- i. 証明書の主体者識別名の `organizationalUnitName` に含まれる情報が誤解を与えるものである可能性を減らすための手順を導入していること。
 - ii. 証明書を発行する際にその手順に従っていること。
 - iii. CA の CP/CPS にその手順を正確に記述していること。
5. 申請者のアイデンティティ
- 証明書に主体者アイデンティティ情報が含まれる場合、本 CA が、以下を満たすこと。
- i. **Baseline Requirements** セクション 3.2 およびセクション 7.1.4.2.2 に従って申請者のアイデンティティを検証するため手順を導入していること。
 - ii. 証明書を発行する際にその手順に従っていること。
 - iii. CA の CP/CPS にその手順を正確に記述していること。
6. 加入者契約
- 本 CA および加入者が関連会社でない場合、加入者および本 CA は、**Baseline Requirements** を満たす法的に有効で実施可能な加入者契約の当事者であること。あるいは、本 CA および加入者が同じ組織体または関連会社である場合、申請権限者が利用規約に同意したこと。
7. 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を保守し、公開していること。
8. 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

本 CP 「9.6.1CA の表明保証」と同様とする。

9.6.3 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、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、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. 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。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 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 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 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 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。

3. 証明書の受理

利用者が証明書の内容の正確性を確認および検証する義務およびその保証。

4. 証明書の使用

TLS サーバー証明書の場合、証明書に記載されている `subjectAltName` でアクセス可能なサーバーにのみ証明書をインストールする。

すべての適用法規に準拠し、加入者契約または利用規約に従う方法でのみ証明書を使用する義務およびその保証。

5. 報告および失効

以下を実行する義務および保証。

- a. 証明書に含まれる公開鍵に対応する加入者の私有鍵が不正使用または危殆化された事実または疑いがある場合、すみやかに証明書の失効を要求し、証明書と関連する私有鍵の使用を中止する。
- b. 証明書内の情報が正確ではない、または正確でなくなる場合、直ちに証明書の失効を要求し、証明書の使用を中止する。

6. 証明書の使用の終了

鍵の危殆化を理由として証明書が失効された場合、証明書に含まれる公開鍵に対応する私有鍵のすべての使用を直ちに中止する義務および保証。

7. 対応

鍵の危殆化または証明書の不正使用に関して CA から指示があった場合、指定された期間内に対応する義務。

8. 確認および承認

申請者が加入者契約の条件または利用規約に違反した場合、または CA の CP、CPS、もしくは **Baseline Requirements** によって失効が要求された場合、CA が証明書を直ちに失効する権利があることの確認と承認。

9.6.4 検証者の表明保証

本 CA のサービスの検証者は、以下の義務を負う。

- ・ 本 CA が発行する証明書を信頼し、本 CP および CPS に規定されている本 CA が意図する目的のみに証明書を使用すること
- ・ 証明書を信頼しようとするときは、リポジトリ内の 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ことを確認すること
- ・ 証明書を信頼しようとするときは、当該証明書の有効期間を確認し、有効期間内であることを確認すること
- ・ 本 CA が発行した証明書を信頼しようとするときは、当該証明書が本 CA の証明書によって署名検証できることを確認すること
- ・ 本 CA の証明書を信頼して利用する際、本 CP および CPS に規定されている検証者として責任を負うことに合意すること

9.6.5 他の関係者の表明保証

規定しない。

9.7 無保証

セコムトラストシステムズは、本 CP 「9.6.1 CA 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若しくは派生的損害に対する責任を負わない。

9.8 責任の制限

本 CP「9.6.1 CA 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、セコムトラストシステムズは責任を負わないものとします。

- ・ 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
- ・ 証明書利用者のシステムに起因して発生した一切の損害
- ・ セコムトラストシステムズ、証明書利用者のハードウェア、ソフトウェアの瑕疵、不具合あるいはその他の動作自体によって生じた損害
- ・ セコムトラストシステムズの責に帰することのできない事由で証明書、CRL、および OCSP レスポンダーに公開された情報に起因する損害
- ・ セコムトラストシステムズの責に帰することのできない事由で正常な通信が行われない状態で生じた一切の損害
- ・ 証明書の使用に関して発生する取引上の債務等、一切の損害
- ・ 現時点の予想を超えた、ハードウェア的あるいはソフトウェア的な暗号アルゴリズム解読技術の向上に起因する損害
- ・ 天変地異、地震、噴火、火災、津波、水災、落雷、戦争、動乱、テロリズムその他の不可抗力に起因する、本 CA の業務停止に起因する一切の損害

9.9 補償

セコムトラストシステムズは、証明書に起因して発生した証明書利用者の損害に対し、受領した契約料金を上限とし、残存利用月数（1 か月未満は切捨て）相当額を証明書利用者に賠償するものとする。また、それ以外の一切の責任を有しないものとする。

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トラストシステ

ムズが本 CA 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、セコムトラストシステムズと契約先との間で契約が終了する場合、セコムトラストシステムズが提供するサービスを終了する場合であっても、その性質上存続されるべき条項は終了の事由を問わず証明書利用者、検証者、セコムトラストシステムズの契約先およびセコムトラストシステムズに適用されるものとする。

9.11 関係者間の個別通知と連絡

セコムトラストシステムズは、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、セコムトラストシステムズによって定期的に確認される。また、本 CP はセコムトラストシステムズの判断によって適宜改訂され、認証サービス改善委員会の承認によって発効する。

9.12.2 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を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、セコムトラストシステムズに対して訴訟、仲裁等を含む法的解決手段に訴えようとする場合は、セコムトラストシステムズに対して事前にその旨を通知するものとする。仲裁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 CA および本 CP は日本国の法律に準拠する。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、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

セコムトラストシステムズは、本サービスの提供にあたり、証明書利用者または検証者の義務等を本 CP およびサービス利用規定、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、いか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

セコムトラストシステムズが本サービスを第三者に譲渡する場合、本 CP およびサービス利用規定、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 およびサービス利用規定、CPS の一部の条項が無効であったとしても、当該文書に記述された他の条項は有効であるものとする。

9.16.4 強制執行条項

本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、セコムトラストシステムズは、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

セコムトラストシステムズは、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、セコムトラストシステムズ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。