EINS/PKI+パブリック認証局 V2
証明書ポリシー

Ver.1.01

株式会社インテック

改訂履歴

Version	変更内容	日付
1.00	Ver.1.00 公開	2013/12/17
1.01	Ver.1.01 公開 ● Web サーバー証明書の詳細プロファイルの拡張領域から Basic Constrains 属性を削除	2014/9/26

目次

1. はじめに

1.1. 概要

EINS/PKI+パブリック認証局 V2証明書ポリシー（以下「本CP」という）は、株式会社インテック（以下「インテック」という）が提供する EINS/PKI+パブリック認証局 V2 （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の運用は別途記載がある場合を除き、セコムトラストシステムズ株式会社（以下、「セコム」という）に委託される。
本CAの運用維持に関する諸手続については、セコムの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（https://repo1.secomtrust.net/spcpp/SECOM-CPS.pdf） 。
本CAは、セコムが運用するSecurity Communication RootCA1より、ルートサイニングされている。
本CAが発行する証明書の有効期間は、1年、または2年とする。
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、EINS/PKI+パブリック証明書発行サービス利用規定（以下、「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、利用規定、及びCPSとを照らし合わせて評価し、本CP、利用規定、及びCPSを承諾する必要がある。
なお、本CPの内容が利用規定、CPSの内容に抵触する場合は、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、インテック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、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伴い、それらを反映するために必要に応じ改訂されるものとする。
本CPは、IETFが認証局運用のフレームワークとして提唱するRFC3647「Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework」に準拠している。

1.2. 文書名称と定義

本 CP の正式名称は、「EINS/PKI+パブリック認証局 V2 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 及び参照する CPS の OID は、次のとおりである。

CP/CPS	OID
EINS/PKI+パブリック認証局 V2 証明書ポリシー	1.2.392.200057.1.101.1
セコム電子認証基盤認証運用規程	1.2.392.200091.100.401.1

1.3. PKI の関係者

1.3.1. 認証局

CA（Certification Authority：認証局）は、IA 及び RA によって構成される。本サービスにおける CA の運営主体はインテックである。CA の運用は別途記載がある場合を除きセコムに委託される。

1.3.1.1. IA

IA は、証明書の発行、失効、CRL（Certificate Revocation List：証明書失効リスト）の開示、OCSP（Online Certificate Status Protocol）サーバーによる証明書ステータス情報の提供、及びリポジトリの維持管理等を行う。
リポジトリはインテックが運用する。それ以外についてはセコムに運用委託される。

1.3.1.2. 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、本人性確認の審査及び証明書を発行、失効するための登録業務等を行う。RA はセコムに運用委託される。

1.3.2. 証明書利用者
証明書利用者とは、インテックに対し、証明書を申請する法人、その他の組織とする。また、インテックと販売委託契約等の個別契約を締結し、申請手続きの仲介を行い、サーバー管理・証明書配置等を行う法人、その他の組織とする。

1.3.3. 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。

1.4. 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、インテックが行う。

1.5.2. 連絡先
本 CP に関する連絡先は以下の URL に提示する。
https://www.einspki.jp/site_repository/repository_pub/

1.5.3. ポリシー適合性を決定する者
本 CP の適合性については、認証局責任者が決定する。

1.5.4. 承認手続
本 CP は、インテックが作成・改訂を行い、セコムの審査を経て、認証局責任者の承認により発効される。

1.6. 定義と略称
別紙 1 の用語集において定義する。

2. 公開とリポジトリの責任

2.1. リポジトリ
本 CA は、証明書利用者及び検証者が CRL 情報を 24 時間 365 日利用できるようリポジトリを維持管理する。また、証明書利用者及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 サーバーを管理する。ただし、保守等により、一時的にリポジトリ及び OCSP サーバーを利用できない場合もある。

リポジトリはインテックが運用する。OCSP サーバーはセコムに運用委託する。

2.2. 証明情報の公開

本 CA は、次の内容を公開し、証明書利用者及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 公開 URL
- 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、本 CA は、OCSP サーバーにより証明書利用者及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。

2.3. 公開の時期又は頻度

本 CP 及び CPS は、変更の都度、リポジトリに公表される。CRL は、本 CP に従って処理された失効情報を含み、一定期間ごとにリポジトリに記載されている CRL 公開 URL に公表される。また、証明書の有効期限を過ぎたものは CRL から削除される。

2.4. リポジトリへのアクセス管理

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

3. 識別と認証

3.1. 名前決定

3.1.1. 名前の種類

証明書に記載される証明書発行者である本 CA の名前と発行対象である証明書利用者の名前は、X.500 の識別名（DN：Distinguished Name） 形式に従い設定する。
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) 「都道府県名」(S)は、利用者の組織が所在する都道府県名とする。
(3) 「市区町村名」(L)は、利用者の組織が所在する市区町村名とする。
(4) 「組織名」(O)とは、法人、会社、又はその他の法人からなる組織の名称とする。
(5) 「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。
(6) 「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又は仮名性

本 CA が発行する証明書の組織名及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 が発行する証明書に記載される識別名(DN)の属性は、発行対象となる Web サーバーに対して一意なものとする。

3.1.6. 認識、認証及び商標の役割

本 CA 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。本 CA 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、本CA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

本CAは、組織の認証を国や地方公共団体が発行する公的書類、本CAが信頼する第三者による調査又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インテックが判断した方法によって行う。

3.2.3. 個人の認証
本 CA は、個人の確認を行わない。

3.2.4. 検証されない証明書利用者の情報
規定しない。

3.2.5. 権限の正当性確認
本 CA 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」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
規定しない。

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及び認証は、「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及び認証は、「3.2 初回の本人性確認」と同様とする。

3.4. 失効申請時の本人性確認と認証
本 CA 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

証明書の申請、発行、受領、失効などの証明書ライフサイクルに関する本 CA の業務はセコムに委託する。

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、証明書を使用する会社、その他の法人の「EINS/PKI+パブリック証明書発行サービス」お客様組織別提出書類基準に基づく権限者、又は会社、その他の法人の代表者から委任された代理人とする。

4.1.2. 申請手続及び責任

証明書利用者及び証明書利用者から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、利用規定、及び CPS の内容を承諾した上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。

4.2. 証明書申請手続

4.2.1. 本人性確認と認証の実施

本 CA は、証明書申請を受け付け、注文書を受理した後、本 CP「3.2 初回の本人確認」に基づく確認を行う。

4.2.2. 証明書申請の承認又は却下

本 CA 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及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

本 CA は、承認を行った証明書申請について、速やかに証明書の発行を行う。

4.3. 証明書の発行

4.3.1. 証明書発行時の処理手続

本 CA は、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

本 CA 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。

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の確認をもって、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 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担当者以外への証明書発行通知は行わない。

4.5. 鍵ペア及び証明書の用途
4.5.1. 証明書利用者の私有鍵及び証明書の用途
証明書利用者は、私有鍵及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及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. 検証者の公開鍵及び証明書の用途
検証者は、本 CP 及び CPS の内容について理解し、承諾した上で、本 CA の証明書を使用するものとする。
検証者は本 CA の証明書を使用して、証明書利用者の証明書を検証する事ができる。

4.6. 証明書の更新
本 CA は、証明書利用者が証明書を更新する場合、新たな鍵ペアを生成すること推奨する。

4.6.1. 証明書の更新事由
規定しない。

4.6.2. 証明書の更新申請を行うことができる者
規定しない。

4.6.3. 証明書の更新申請の処理手続
規定しない。

4.6.4. 証明書利用者に対する新しい証明書発行通知
規定しない。

4.6.5. 更新された証明書の受領確認手続
規定しない。

4.6.6. 認証局による更新された証明書の公開
規定しない。

4.6.7. 他のエンティティに対する認証局の証明書発行通知
規定しない。

4.7. 鍵更新を伴う証明書の更新
4.7.1. 更新事由
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。失効した証明書又は有効期限が切れた証明書は更新できない。
本 CA は証明書の更新申請を有効期間満了の 60 日前から受け付け、証明書の発行を有効期間満了 30 日前から行う。

4.7.2. 新しい証明書の申請を行うことができる者
「4.1.1.証明書の申請を行うことができる者」と同様とする。

4.7.3. 更新申請の処理手続
「4.3.1.証明書発行時の処理手続」と同様とする。

4.7.4. 証明書利用者に対する新しい証明書の通知
「4.3.2.証明書利用者への証明書発行通知」と同様とする。

4.7.5. 鍵更新された証明書の受領確認手続
「4.4.1.証明書の受領確認手続」と同様とする。

4.7.6. 認証局による鍵更新済みの証明書の公開
「4.4.2.認証局による証明書の公開」と同様とする。

4.7.7. 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
本 CA は、証明書に登録された情報の変更が必要となった場合、その証明書の失効及び新規発行とする。

4.8.1. 証明書の変更事由
規定しない。

4.8.2. 証明書の変更申請を行うことができる者
規定しない。

4.8.3. 変更申請の処理手続
規定しない。

4.8.4. 証明書利用者に対する新しい証明書発行通知
規定しない。

4.8.5. 変更された証明書の受領確認手続
規定しない。

4.8.6. 認証局による変更された証明書の公開
規定しない。

4.8.7. 他のエンティティに対する認証局の証明書発行通知
規定しない。

4.9. 証明書の失効と一時停止
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、本 CA に対し速やかに証明書の失効申請を行わなければならない。

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

- 証明書の利用を中止する場合

また、本 CA は、次の事由が発生した場合に、本 CA 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。

- 証明書利用者が利用規定、本 CP、CPS、関連する契約又は法律に基づく義務を履行していない場合
- 本 CA の私有鍵が危殆化した又は危殆化のおそれがあると判断した場合
- 本 CA が失効を必要とすると判断するその他の状況が認められた場合

4.9.2. 証明書の失効申請を行うことができる者

証明書の失効申請を行うことができる者は、証明書を使用している会社、その他の法人の「EINS/PKI+パブリック証明書発行サービス」お客様組織別提出書類基準に基づく権限者、又は会社、その他の法人の代表者から委任された代理人とする。

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、秘密鍵が危殆化した又は危殆化のおそれがあると判断した場合には、速やかに失効申請を行わなければならない。

4.9.5. 認証局が失効申請を処理しなければならない期間

本 CA は、有効な失効申請を受け付けてから速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。

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、及び OCSP サーバーの URL を記載する。
CRL 及び OCSP サーバーは、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 又は OCSP サーバーの URL により確認する。

4.9.7. 証明書失効リストの発行頻度

CRL は、失効処理の有無にかかわらず、24 時間ごとに更新を行う。証明書の失効処理が行われた場合は、その時点で CRL の更新を行う。

4.9.8. 証明書失効リストの発行最大遅延時間

本 CA が発行した CRL は、一定の時間間隔でリポジトリに掲載している URL 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

オンラインでの証明書ステータス情報は、OCSP サーバーを通じて提供される。証明書の失効処理が行われた場合は、証明書が失効したことは即時に証明書ステータス情報に反映させる。

4.9.10. オンラインでの失効/ステータス確認を行うための要件

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 URL により参照可能な CRL により、証明書の失効登録の有無を確認しない場合には、OCSP サーバーにより提供される証明書ステータス情報の確認を行わなければならない。

4.9.11. 利用可能な失効情報の他の形式
規定しない。

4.9.12. 鍵の危殆化に対する特別要件
規定しない。

4.9.13. 証明書の一時停止事由
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
規定しない。

4.9.15. 証明書の一時停止申請手続
規定しない。

4.9.16. 一時停止を継続することができる期間
規定しない。

4.10. 証明書のステータス確認サービス
4.10.1. 運用上の特徴
加入者及び利用者は OCSP サーバーを通じて証明書ステータス情報を確認することができる。

4.10.2. サービスの利用可能性
本 CA は、24 時間 365 日、証明書ステータス情報を確認できるよう OCSP サーバーを管理する。ただし、保守等により、一時的に OCSP サーバーを利用できない場合もある。

4.10.3. オプショナルな仕様
規定しない。

4.11. 加入(登録)の終了
証明書利用者は本サービスの利用を終了する場合、証明書の失効申請を行わなければならない。

4.12. キーエスクローと鍵回復
4.12.1. キーエスクローと鍵回復ポリシー及び実施
本 CA は、証明書利用者の私有鍵のエスクローは行わない。

4.12.2. セッションキーのカプセル化と鍵回復のポリシー及び実施
規定しない。

5. 設備上、運営上、運用上の管理

本CAの設備上、運営上、運用上の管理は、別途記載がある場合を除き、セコムに委託する。

5.1. 物理的管理

5.1.1. 立地場所及び構造
本項については、CPS に規定する。

5.1.2. 物理的アクセス
本項については、CPS に規定する。

5.1.3. 電源及び空調
本項については、CPS に規定する。

5.1.4. 水害対策
本項については、CPS に規定する。

5.1.5. 火災対策
本項については、CPS に規定する。

5.1.6. 媒体保管
本項については、CPS に規定する。

5.1.7. 廃棄処理
本項については、CPS に規定する。

5.1.8. オフサイトバックアップ
本項については、CPS に規定する。

5.2. 手続的管理

5.2.1. 信頼すべき役割
本項については、CPS に規定する。

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

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

5.2.4. 職務分割が必要となる役割
本項については、CPS に規定する。

5.3. 人事的管理

5.3.1. 資格、経験及び身分証明の要件
本項については、CPS に規定する。

5.3.2. 背景調査
本項については、CPS に規定する。

5.3.3. 教育要件
本項については、CPS に規定する。

5.3.4. 再教育の頻度及び要件
本項については、CPS に規定する。

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

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

5.3.7. 業務委託先の管理
本CAは、認証基盤システムの運用のすべてあるいは一部を外部組織に委託する場合、業務委託先との契約によって、業務委託先のもとで運用業務が適切に行われていることを確認する。

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 CA は、CPS「5.4.1.記録されるイベントの種類」の EINS/PKI+パブリック証明書発行サービスに関

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。

- 発行した証明書及び CRL
- CRL の発行に関する処理履歴
- CPS
- CPS 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おいては、委託契約に関する書類
- 監査の実施結果に関する記録及び監査報告書
- 証明書利用者からの申請書類
- OCSP サーバーへのアクセスログ

5.5.2. アーカイブ保存期間
本 CA は、アーカイブを最低 5 年間保存する。

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 の鍵ペア更新又は証明書更新は、原則として加入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実施する。
本 CA の有効期間が、加入者に発行する証明書の最大有効期間よりも短くなる場合、加入者に発行する証明書の有効期間は、本 CA の有効期間内に納まるよう変更する。
なお、本 CA の私有鍵の有効期間は 20 年を想定している。

5.7. 危殆化及び災害からの復旧
5.7.1. 事故及び危殆化時の手続
本項については、CPS に規定する。

5.7.2. ハードウェア、ソフトウェア又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. 認証局又は登録局の終了

本 CA を終了する場合、3 か月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全ての証明書は、本 CA の終了以前に失効を行う。

6. 技術的セキュリティ管理

本項に記述される本 CA の鍵管理、セキュリティ管理、およびタイムスタンプについてはセコムに委託する。

6.1. 鍵ペアの生成及びインストール

6.1.1. 鍵ペアの生成

本 CA の鍵ペアの生成については、CPS に規定する。その他関係者の鍵ペアの生成については、規定しない。

6.1.2. 証明書利用者に対する私有鍵の交付

証明書利用者の私有鍵は、証明書利用者自身が生成する。本 CA からの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

本項については、CPS に規定する。

6.1.4. 検証者への CA 公開鍵の交付

検証者は、本 CA のリポジトリにアクセスすることによって、本 CA の公開鍵を入手することができる。

6.1.5. 鍵サイズ

本 CA の鍵ペアは、RSA 方式で鍵長 2048 ビットとする。
証明書利用者の鍵ペアについては、RSA 方式で鍵長 2048 ビットとする。

6.1.6. 公開鍵のパラメーターの生成及び品質検査

本 CA の公開鍵のパラメーターの生成および品質検査については、CPS に規定する。その他関係者の公開鍵のパラメーターの生成及び品質検査については規定しない。

6.1.7. 鍵の用途

本 CA 及び本 CA が発行する証明書の鍵の用途は以下の通りとする。

	本 CA の証明書	本 CA が発行する証明書
digital Signature	—	yes
nonRepudiation	—	—
keyEncipherment	—	yes
dataEncipherment	—	—
keyAgreement	—	—
keyCertSign	yes	—
cRLSign	yes	—
encipherOnly	—	—
decipherOnly	—	—

6.2. 私有鍵の保護及び暗号装置技術の管理

6.2.1. 暗号装置の標準及び管理

本 CA の暗号装置の標準及び管理については、CPS に規定する。その他関係者の暗号装置の標準及び管理については、規定しない。

6.2.2. 私有鍵の複数人管理
本 CA の私有鍵の複数人管理については、CPS に規定する。
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 の私有鍵のエスクローについては、CPS に規定する。
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については、CPS に規定する。
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 の私有鍵のアーカイブについては、CPS に規定する。
証明書利用者の私有鍵については規定しない。

6.2.6. 私有鍵の暗号装置への又は暗号装置からの転送
本 CA の私有鍵の暗号装置への又は暗号装置からの転送については、CPS に規定する。
証明書利用者の私有鍵については規定しない。

6.2.7. 暗号装置への私有鍵の格納
本 CA の私有鍵の暗号装置への格納については、CPS に規定する。
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 の私有鍵の活性化方法については、CPS に規定する。
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方法については、CPS に規定する。
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 の私有鍵の破棄方法については、CPS に規定する。
証明書利用者の私有鍵については規定しない。

6.2.11. 暗号装置の評価
本 CA の暗号装置の評価については、CPS に規定する。
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 暗号装置の標準及び管理」のとおりである。
証明書利用者の私有鍵については規定しない。

6.3.2. 私有鍵及び公開鍵の有効期間
本 CA の私有鍵及び公開鍵の有効期間については、CPS に規定する。
証明書利用者の私有鍵及び公開鍵については規定しない。なお、本 CA が発行する証明書利用者の証明書の有効期間は 1 年、または 2 年とする。

6.4. 活性化データ
6.4.1. 活性化データの生成及び設定
本項については、CPS に規定する。

6.4.2. 活性化データの保護
本項については、CPS に規定する。

6.4.3. 活性化データの他の考慮点
規定しない。

6.5. コンピュータのセキュリティ管理
6.5.1. コンピュータセキュリティに関する技術的要件
本項については、CPS に規定する。

6.5.2. コンピュータセキュリティ評価
本項については、CPS に規定する。

6.6. ライフサイクルセキュリティ管理
6.6.1. システム開発管理
本項については、CPS に規定する。

6.6.2. セキュリティ運用管理
本項については、CPS に規定する。

6.6.3. ライフサイクルセキュリティ管理
本項については、CPS に規定する。

6.7. ネットワークセキュリティ管理
本項については、CPS に規定する。

6.8. タイムスタンプ
本項については、CPS に規定する。

7. 証明書及び証明書失効リスト及び OCSP サーバー証明書のプロファイル

7.1. 証明書プロファイル

別紙 2 に、証明書の詳細プロファイルを記載する。

7.2. CRL プロファイル

別紙 2 に、CRL の詳細プロファイルを記載する。

8. 準拠性監査と他の評価

本 CA は、本 CP 及び CPS に準拠して運用がなされているかについて、適時監査を行う。本 CA が行う準拠性監査に関する諸事項については CPS に規定する。
本 CA の監査はセコムに委託する。

8.1. 監査の頻度
本項については、CPS に規定する。

8.2. 監査人の身元／資格
本項については、CPS に規定する。

8.3. 監査人と被監査部門の関係
本項については、CPS に規定する。

8.4. 監査で扱われる事項
本項については、CPS に規定する。

8.5. 不備の結果としてとられる処置
本項については、CPS に規定する。

8.6. 監査結果の開示
本項については、CPS に規定する。

9. 他の業務上及び法的事項

9.1. 料金
本 CA が発行する証明書に関する料金については、別途規定する。

9.2. 財務的責任
本 CA の運用維持にあたり、十分な財務的基盤を維持するものとする。

9.3. 企業情報の機密性
機密情報の種類には、本 CA の設備仕様、システム仕様、ネットワーク仕様、詳細な業務手順、委託先との契約内容などが含まれる。本 CA は、本 CA が決定するか、法律が義務付ける場合を除き、原則としてこれら機密情報を公開しない。本 CA は、本 CA が発行する利用者証明書に記載される情報、CRL に記載される情報およびリポジトリに公開される情報を機密情報とみなさない。

9.4. 個人情報の保護
本 CA は、認証業務に関連して申請者または利用者から提示される個人情報を保護する。本 CA は、本認証サービスを提供するために必要な範囲において、委託先であるセコムにこれらの個人情報を契約に基づき提供する。本 CA は、本認証サービスを提供するために必要な範囲を超えて、これらの個人情報を使用しない。
申請者または利用者から、自己の情報について開示を求められた場合、原則として合理的な期間内にこれに応じる。

9.5. 知的財産権
以下に示す著作物は、インテックに帰属する財産である。
- 本 CP
- ステッカー

以下に示す著作物は、セコムに帰属する財産である。
- ・ステッカー証明ページ

9.6. 表明保証
9.6.1. 認証局の表明保証

9.6.1.1. IA の表明保証
本 CA は、IA の業務を遂行するにあたり、次を行うこと、および業務委託先であるセコムに行わせることの義務を負う。
- CA 私有鍵のセキュアな生成・管理を行うこと
- RA からの申請に基づいた証明書の正確な発行、失効及び管理を行うこと
- IA のシステムの運用、稼動監視を行うこと
- CRL の発行、公表を行うこと
- OCSP サーバーの公開を行うこと
- リポジトリの維持管理を行うこと

9.6.1.2. RA の表明保証
本 CA は、RA の業務を遂行するにあたり、次を行うこと、および業務委託先であるセコムに行わせることの義務を負う。
- 登録端末のセキュアな環境への設置・運用を行うこと
- 証明書発行時、実在性確認等の審査を的確に行うこと
- IA への証明書発行・失効等の指示を正確かつ速やかに行うこと

9.6.2. 証明書利用者の表明保証
証明書利用者は、次の義務を負うものとする。
- 証明書利用者は証明書の発行申請に際して、正確かつ完全な情報を提供すること。当該情報に変更があった場合には、その旨を速やかに本 CA まで通知すること。
- 危殆化から自身の私有鍵を保護すること。
- 証明書の使途は利用規定、及び本 CP に従うこと。
- 証明書利用者が、証明書に記載の公開鍵に対応する私有鍵が危殆化した、又はそのおそれがあると判断した場合、若しくは登録情報に変更があった場合、証明書利用者は本 CA に証明書の失効を速やかに申請すること。

9.6.3. 検証者の表明保証
検証者は、次の義務を負うものとする。
- 本 CA の証明書について、有効性の確認を行うこと。
- 証明書利用者が使用している証明書の有効性について、証明書の有効期限を過ぎていないか、CRL、または OCSP サーバーにより証明書の失効登録がされていないか確認を行うこと。
- 証明書利用者の情報を信頼するかの判断は検証者の責任で行うこと。

9.6.4. 他の関係者の表明保証
規定しない。

9.7. 無保証
本 CA は、本 CP「9.6.1 認証局の表明保証」に規定する保証に関連して発生するいかなる間接損害、特別損害、付随的損害又は派生的損害に対する責任を負わず、また、いかなる逸失利益、データの紛失又はその他の間接的若しくは派生的損害に対する責任を負わない。

9.8. 責任の制限
本 CP「9.6.1 認証局の表明保証」の内容に関し、次の場合、本 CA は責任を負わないものとします。
- 本 CA に起因しない不法行為、不正使用又は過失等により発生する一切の損害
- 証明書利用者が自己の義務の履行を怠ったために生じた損害
- 証明書利用者のシステムに起因して発生した一切の損害
- 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
- 本CAの責に帰することのできない事由で証明書及びCRL、OCSPサーバーに公開された情報に起因する損害
- 本 CA 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 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します。また、それ

以外の一切の責任を有しないものとする。

9.10. 文書の有効期間と終了
9.10.1. 有効期間
本 CP は、認証局責任者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本 CA が EINS/PKI+パブリック証明書発行サービス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、又は、本 CA がサービス提供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及び本 CA に適用されるものとします。

9.11. 関係者間の個別通知と連絡
本 CA は、証明書利用者及び検証者に対する必要な通知をホームページ、電子メール又は書面等によって行う。

9.12. 改訂
9.12.1. 改訂手続
本 CP は、インテックの判断によって適宜改訂され、セコムの審査を経て、認証局責任者の承認によって発効する。

9.12.2. 通知方法及び期間
本 CP を変更した場合、変更した本 CP を速やかに公表することをもって、関係者に対しての告知とする。

9.12.3. オブジェクト識別子が変更されなければならない場合
規定しない。

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、本 CA 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、本 CA に対して事前にその旨を通知するものとする。仲裁及び裁判地は東京都区内における紛争処理機関を専属的管轄とする。

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

9.15. 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、暗号ハードウェア及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
本 CA は、本サービスの提供にあたり、証明書利用者又は検証者の義務等を本 CP 及び利用規定、

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、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
本 CA が本サービスを第三者に譲渡する場合、本 CP 及び利用規定、CPS において記載された責務及びその他の義務の譲渡を可能とする。

9.16.3. 分離条項
本 CP 及び利用規定、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
規定しない。

9.17. その他の条項
規定しない。

別紙 1 用語集

アルファベット

CA（Certification Authority）：認証局	証明書の発行・更新・失効、CA 私有鍵の生成・保護及び証明書利用者の登録等を行う主体のことをいう。
CP（ Certificate Policy）	CA が発行する証明書の種類、用途、申込手続等、証明書に関する事項を規定する文書のことをいう。
CPS （ Certification Practices Statement）：認証運用規定	CA を運用する上での諸手続、セキュリティ基準等、CA の運用を規定する文書のことをいう。
CRL （ Certificate Revocation List）：証明書失効リスト	証明書の有効期間中に、証明書記載内容の変更、私有鍵の紛失等の事由により失効された証明書情報が記載されたリストのことをいう。
FIPS140-2	米国 NIST（National Institute of Standards and Technology）が策定した暗号モジュールに関するセキュリティ認定基準のこという。最低レベル1から最高レベル 4 まで定義されている。
IA（Issuing Authority）：発行局	CA の業務のうち、証明書の発行・更新・失効、CA 秘密鍵の生成・保護、リポジトリの維持・管理等を行う主体のことをいう。
OID（Object Identifier）：オブジェクト識別子	ネットワークの相互接続性やサービス等の一意性を維持管理するための枠組みであり、国際的な登録機関に登録された、世界中のネットワーク間で一意となる数字のことをいう。
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、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。 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。

あ～ん

アーカイブ	法的又はその他の事由により、履歴の保存を目的に取得する情報のことをいう。
エスクロー	第三者に預けること（寄託）をいう。
鍵ペア	公開鍵暗号方式において、私有鍵と公開鍵から構成される鍵の対のことをいう。
監査ログ	認証局システムへのアクセスや不正操作の有無を検査するために記録される認証局システムの動作履歴やアクセス履歴等をいう。
公開鍵	公開鍵暗号方式において用いられる鍵ペアの一方をいい、私有鍵に対応し、通信相手の相手方に公開される鍵のことをいう。
私有鍵	公開鍵暗号方式において用いられる鍵ペアの一方をいい、公開鍵に対応する本人のみが保有する鍵のことをいう。
タイムスタンプ	電子ファイルの作成日時やシステムが処理を実行した日時等を記録したデータのことをいう。
電子証明書	ある公開鍵を、記載された者が保有することを証明する電子データのことをいう。CA が電子署名を施すことで、その正当性が保証される。
リポジトリ	CA 証明書及び CRL 等を格納し公表するデータベースのことをいう。

別紙 2 詳細プロファイル

(1) Webサーバー証明書の詳細プロファイル

基本領域		設定内容	critical
Version		Version 3	−
Serial Number		例) 0123456789	−
Signature Algorithm		SHA1 with RSAEncryption	−
Issuer	Country	C=JP	−
	Organization	O=INTEC INC.	−
	Common Name	CN= EINS/PKI Public Certification Authority V2	−
Validity	NotBefore	例) 2008/3/1 00:00:00 GMT	−
	NotAfter	例) 2009/3/1 00:00:00 GMT	−
Subject	Country	C=JP(固定値)	−
	State Or Province	必須	−
	Locality	必須	−
	Organization	必須	−
	Organizational Unit	任意	−
	Common Name	サーバー名(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**
Authority Key Identifier		発行者公開鍵の SHA-1 ハッシュ値(160 ビット)	n
Subject Alt Name		dNSName=サーバー名	n
CertificatePolicies		policyIdentifier OID=1.2.392.200057.1.101.1 policyQualifiers policyQualifierId=CPS qualifiier=https://repo1.secomtrust.net/sppca/intecca/	n
ExtendedKeyUsage		serverAuth	n
CRL Distribution Points		http://repo1.secomtrust.net/sppca/intecca/fullcrl.crl	n
Subject Key Identifier		主体者公開鍵の SHA-1 ハッシュ値(160 ビット)	n
KeyUsage		digitalSignature, keyEncipherment	y
Authority Information Access		accessMethod ocsp(1 3 6 1 5 5 7 48 1) accessLocation http://intec.ocsp.secomtrust.net	n

(2) OCSPサーバー証明書の詳細プロファイル

基本領域		設定内容	critical
Version		Version 3	−
Serial Number		例) 0123456789	−
Signature Algorithm		SHA1 with RSAEncryption	−
Issuer	Country	C=JP	−
	Organization	O= INTEC INC.	−
	Common Name	CN= EINS/PKI Public Certification Authority V2	−
Validity	NotBefore	例) 2013/11/1 00:00:00 GMT	−
	NotAfter	例) 2014/3/5 00:00:00 GMT	−
Subject	Country	C=JP	−
	Organization	O=INTEC INC.	−
	Organizational Unit	OU=EINS/PKI Public Web Certificate Service	
	Common Name	CN=EINS/PKI Public Web Certificate OCSP Responder	−
Subject Public Key Info		主体者の公開鍵 2048 ビット	−
拡張領域		**設定内容**	**critical**
ExtendedKeyUsage		OCSPSigning	n
Subject Key Identifier		主体者公開鍵の SHA-1 ハッシュ値(160 ビット)	n
Authority Key Identifier		発行者公開鍵の SHA-1 ハッシュ値(160 ビット)	n
CertificatePolicies		policyIdentifier OID=1.2.392.200057.1.101.1 policyQualifiers policyQualifierId=CPS qualifiier= https://repo1.secomtrust.net/sppca/intecca/	n
OCSP No Check		null	n
KeyUsage		digitalSignature	y

(3) CRLの詳細プロファイル

基本領域		設定内容	critical
Version		Version 2	−
Signature Algorithm		SHA1 with RSAEncryption	−
Issuer	Country	C=JP	−
	Organization	O= INTEC INC.	−
	Common Name	CN= EINS/PKI Public Certification Authority V2	−
This Update		例) 2008/3/1 00:00:00 GMT	−
Next Update		例) 2008/3/5 00:00:00 GMT 更新間隔=24H、有効期間=96H とする	−
Revoked Certificates	Serial Number	例) 0123456789	−
	Revocation Date	例) 2008/3/1 00:00:00 GMT	−
	Reason Code	失効事由(unspecified, etc.)	−
拡張領域		**設定内容**	**critical**
Authority Key Identifier		発行者公開鍵の SHA-1 ハッシュ値(160 ビット)	n
CRL Number		CRL 番号	n