EINS/PKI+ for EDI
認証局運用規程（CPS）

Version 2.00

株式会社インテック

【改訂履歴】

Version	変更内容	改訂日
1.00	第 1.00 版　公開	2007/10/1
1.01	コーポレートマークの変更	2014/6/30
2.00	第 2.00 版　公開 ・認証局証明書および発行される証明書の署名アルゴリズムを sha256WithRSAEncryption に変更 ・誤字等の修正	2015/7/14

【目次】

第1章 はじめに

1.1. 概要

「EINS/PKI+ for EDI 認証局運用規程」(以下、本 CPS という)は「流通業界共通認証局証明書ポリシー」(以下、標準 CP という)に準拠し、株式会社インテック(以下、インテックという)が提供する電子証明書発行サービス「EINS/PKI+ for EDI」(以下、本認証サービスという)の運用規程である。

本認証サービスでは、インターネットを利用した GDS、EDI、EPC 等に関わる通信を安全に行うために利用する証明書を EINS/PKI+ for EDI 認証局 V2(以下、本認証局)から発行するサービスを提供する。

本 CPS は、本認証局が取り扱う証明書の発行、失効、およびその他の本認証局業務の運用管理に関する諸手続きについて規定する。

本認証局は、「流通業界共通認証局」として標準 CP の準拠性に対して「認定機関」により適合性の認定を受けてサービスを提供する。

なお、本 CPS の構成は、標準 CP および RFC3647「インターネット X.509 公開鍵基盤証明書ポリシーおよび認証局運用規程フレームワーク」に準じる。本認証局は、情報セキュリティマネジメント規格 JISQ27001:2006 の審査登録適合を受けた組織がシステム保守を行う。

また、本 CPS で規定された内容は、sha1WutgRSAEbcryption(OID: 1.2.840.113549.1.1.5) 方式を用いて、2048bit の本認証局秘密鍵で署名された利用者証明書についても以下の条件において適用される。

・第4章における証明書申請、証明書発行、鍵の更新を伴う証明書の更新に関する項目、および別紙 1 は適用外。

・別紙1については EINS/PKI+ for EDI 認証局規定 v1.01 の同章内容を適用。

1.2. 文書名称と定義

本 CPS の名称は、「EINS/PKI+ for EDI 認証局運用規程(CPS)」である。本 CPS は、標準 CP に準拠している。

本 CPS の OID は、1.2.392.200057.1.94401.2.1である。

1.3. PKI の関係者

1.3.1. 認証局

認証局は、本認証局の秘密鍵を安全な方法で管理し、利用者からの利用者証明書の申請(EDI サーバ、Web サーバ、クライアント等)に対し、当該申請の正当性および申請者の審査を確実に行い、利用者が保持する秘密鍵と結びついた公開鍵に対し利用者証明書の発行を行う。

また本認証局の失効規定に従い、本認証局が発行した利用者証明書を失効し、リポジトリによる CRL の公開を行う。

なお本認証局は、PKI における信頼階層として以下の 2 階層で構成される。

認証局	説明
ルート認証局	本認証局の最上位の認証局。中間認証局の認証局証明書を発行する。
中間認証局	ルート認証局の下位の認証局として、利用者証明書を発行する。

1.3.2. 登録局

登録局は、利用者からの申請に対して、証明書の発行や失効に関わる審査を行う。本認証局において、登録局は認証局における業務の一部を指す。

1.3.3. 利用者

利用者は、本認証局から証明書の発行を受け、利用を行う者である。

本認証局は流通業界に関わりを有している者の中で、以下の者に対して証明書を発行する。

(1) 法人(個人で事業を行っており、かつ法人登記を行っている者も含む)

(2) 法人の従業者(役員、社員、契約社員等を含む)

(3) 個人事業主(法人登記を行っていない事業者のみを指すものとする)

利用者は、本 CPS の利用者の義務に関する条項および利用者規約に記載された内容をについて理解し承諾した上で、証明書を利用する。法人および個人事業主とは、それぞれ以下の要件を満たす者をいう。

種別	要件
法人	日本において法人登記されている組織(個人で事業を営んでいる場合を含む)
個人事業主	法人登記を行っていない事業者

1.3.4. 依拠当事者

依拠当事者とは、各流通業界共通認証局が発行した証明書に依拠して、以下の行為を行うものである。

- 利用者が作成した電子署名を証明書内の公開鍵を利用して検証行う
- 利用者から提示された証明書により利用者の認証を行う
- 利用者に対して証明書内の公開鍵を利用して暗号化されたデータを送信する

本認証局は、依拠当事者の範囲を限定しない。なお、本認証局においては、依拠当事者を検証者と称する。

1.3.5. 申請責任者

法人に所属し、当該法人組織から権限を委譲され、証明書の申請を行う者、または個人事業主として証明書の取得申請を行う者をいう。申請責任者は証明書取得後における本認証局との連絡窓口となる。

1.3.6. 認定機関

認定機関は、標準 CP に準拠した認証局を認定する機関である。本認証局は、認定機関が定める手続きに従い認定を取得した上で本認証サービスを提供する。

1.3.7. その他の関係者

規定しない。

1.4. 証明書の利用方法

1.4.1. 証明書の種類と用途

本認証局が発行する証明書は、証明書の種類ごとに以下の範囲でのみ使用できる。

(1) 法人向けサーバ証明書

- GDS または EDI 用途の SSL サーバ認証・暗号化
- GDS または EDI 用途の SSL クライアント認証
- GDS または EDI 用途のメッセージ署名・暗号化

(2) 法人向けクライアント証明書

- GDS または EDI 用途の SSL クライアント認証
- GDS または EDI 用途のメッセージ署名・暗号化

(3) 個人事業主向けサーバ証明書

- GDS または EDI 用途の SSL サーバ認証・暗号化
- GDS または EDI 用途の SSL クライアント認証
- GDS または EDI 用途のメッセージ署名・暗号化

(4) 個人事業主向けクライアント証明書

- GDS または EDI 用途の SSL クライアント認証
- GDS または EDI 用途のメッセージ署名・暗号化

なお、EPC で使用する証明書の用途については、本 CPS 策定時点で、証明書を利用した通信プロトコルの仕様が定められていないため規定しない。

1.4.2. 禁止されている証明書用途

本認証局が発行する利用者証明書は、理由の如何を問わず、本 CPS1.4.1 項に規定した用途でのみ使用する。なお、以下の目的での使用は、これを禁止する。

- 法人向けサーバ証明書、あるいは法人向けクライアント証明書を個人の実在性、同一性の裏付けとして使用すること
- 否認防止目的としての使用

1.5. ポリシー管理

1.5.1. 管理組織

本 CPS の管理については、本 CPS1.5.4 項で規定された手続きによる承認のもと、認証局責任者

が行う。

1.5.2. 受付窓口

受付窓口は、以下の URL に提示する。

https://www.einspki.jp/site_repository/repository_edi/

1.5.3. 準拠性の責任

本 CPS の標準 CP への準拠性に対する判断の責任は、認証局責任者が負う。

1.5.4. CPS の承認手続き

本 CPS は、認証局責任者による承認および認定機関による適合性の判断を得て発行する。

1.6. 定義と略称

別紙 2 において定義する。

第2章　公開とリポジトリの責任

2.1.　リポジトリ

本認証局は、以下の URL でリポジトリを公開し、利用者証明書の失効リスト(CRL)を提供する。

https://www.einspki.jp/site_repository/repository_edi/

リポジトリは、本認証局の営業日を問わず、常時利用可能なように運用される。ただしシステムの保守などによりあらかじめ通知し、一時停止することがある。なお、緊急時等やむを得ない場合は、事前通知せずに停止することがある。

2.2.　認証情報の公開

本認証局は、リポジトリにおいて以下の認証情報を公開する。

- 本 CPS
- EINS/PKI+ for EDI 利用者規約
- EINS/PKI+ for EDI 検証者規約
- 本認証局証明書(ルート認証局および中間認証局)
- 本認証局証明書のフィンガープリント(ルート認証局および中間認証局)
- 本認証局が発行した利用者証明書の CRL

2.3.　公開の時期と周期

本 CPS、利用者規約、検証者規約に変更が生じた場合は、直ちに公開する。認証局証明書は発行された都度、当該認証局証明書の利用に先立って、証明書とそのフィンガープリントを公開する。本認証局が発行した利用者証明書の CRL 発行周期は、本 CPS4.9.7 項に定めた頻度で更新され公開される。

2.4.　リポジトリに対するアクセス制限

本認証局が公開するリポジトリの情報の参照については、アクセス制限を設けない。リポジトリで公開する情報の登録、更新、削除は、本認証局に従事するものが定められた手順に従って実施するようコントロールされる。

第3章 識別と認証

3.1. 名称

3.1.1. 名前の種類

本認証局が発行する証明書の発行者名(issuer)および主体者名(subject)は、ITU-T 勧告 X.501 の識別名(Distinguished Name)に従う。

3.1.2. 名前が意味を持つことの必要性

本認証局の認証局証明書および本認証局が発行する各利用者証明書のサブジェクト名には、以下の情報が含まれる。

(1) ルート認証局証明書

本認証局のルート認証局証明書の発行者名およびサブジェクト名には以下の値を含む。

No.	サブジェクト項目		設定値
1	組織名	O	“INTEC Inc.”
2	組織部署名	OU	“CA for manufactures-distributors-retailers”
3	コモンネーム	CN	“EINS/PKI for EDI Root Certificate Authority V2”
6	国名	C	“JP”

(2) 中間認証局証明書

本認証局の中間認証局証明書のサブジェクト名には以下の値を含む。

No.	サブジェクト項目		設定値
1	組織名	O	“INTEC Inc.”
2	組織部署名	OU	“CA for manufactures-distributors-retailers”
3	コモンネーム	CN	“EINS/PKI for EDI Certificate Authority V2”
6	国名	C	“JP”

(3) 法人向けサーバ証明書

法人向けサーバ証明書のサブジェクト名には以下の値を含む。

No.	サブジェクト項目		必須	説明
1	組織名	O	○	法人組織の名称
2	組織部署名	OU		法人組織における部署名
3	コモンネーム	CN	○	当該証明書を利用するサーバの FQDN 名
4	都道府県名	S		法人組織が所在する都道府県名
5	市区町村名	L		法人組織が所在する市区町村名

No.	サブジェクト項目		必須	説明
6	国名	C	○	“JP”（固定値）

(4) 法人向けクライアント証明書

法人向けクライアント証明書のサブジェクト名には以下の値を含む。

No.	サブジェクト項目		必須	説明
1	組織名	O	○	法人組織の名称
2	組織部署名	OU		法人組織における部署名
3	コモンネーム	CN	○	法人名または法人組織に所属する従業者の個人名
4	都道府県名	S		法人組織が所在する都道府県名
5	市区町村名	L		法人組織が所在する市区町村名
6	国名	C	○	“JP”（固定値）
7	電子メールアドレス	E	○	法人または法人組織に所属する従業者の電子メールアドレス

(5) 個人事業主向けサーバ証明書

個人事業主向けサーバ証明書のサブジェクト名には以下の値を含む。

No.	サブジェクト項目		必須	説明
1	組織名	O	○	“Natural Person”（固定値）
2	組織部署名	OU	○	事業主の個人名
3	コモンネーム	CN	○	当該証明書を利用するサーバの FQDN 名
4	都道府県名	S		個人事業主が所在する都道府県名
5	市区町村名	L		個人事業主が所在する市区町村名
6	国名	C	○	“JP”（固定値）

(6) 個人事業主向けクライアント証明書

個人事業主向けクライアント証明書のサブジェクト名には以下の値を含む。

No.	サブジェクト項目		必須	説明
1	組織名	O	○	“Natural Person”（固定値）
2	組織部署名	OU		商取引上の名称、屋号等
3	コモンネーム	CN	○	事業主の個人名
4	都道府県名	S		個人事業主が所在する都道府県名
5	市区町村名	L		個人事業主が所在する市区町村名

No.	サブジェクト項目		必須	説明
6	国名	C	○	“JP”(固定値)
7	電子メールアドレス	E	○	個人事業主の電子メールドレス

3.1.3. 利用者の匿名・仮名についての要件

「法人組織の名称」および「個人事業主の個人名」における匿名、仮名および旧名称の使用は、これを許可しない。

3.1.4. 様々な名称形式を解釈するためのルール

様々な名称形式を解釈するルールは ITU-T 勧告 X.501 に従う。

3.1.5. 名称の一意性

本認証局が発行する利用者証明書に記載される識別名(DN)は、一意なものとする。

3.1.6. 商標等の認識、認証および役割

利用者は、本認証局への証明書の申請において、他者が有する知的財産権を侵害してはならない。本認証局は、利用者が証明書申請に記載する名称の知的財産権を有するかに関しては、これを検証しない。また、ドメイン・ネーム、商号、商標、サービス・マークに関する紛争への仲裁、調停、その他の方法による解決は、これを行わない。本認証局は、申請者に対し何らかの責任を負うことなく、上記の紛争を理由として証明書の申請を拒絶する権利を有する。

3.2. 初回登録時の本人性認証

3.2.1. 秘密鍵の所有を検証する方法

本認証局は、利用者から受取った証明書発行要求の電子署名を検証することで、利用者が秘密鍵を所有していることを確認する。

3.2.2. 組織の本人性の確認

本認証局は、法人の実在性、本人性の確認を以下の方法により確認する。

(1) 法人組織の実在性、本人性確認

本認証局は、利用者の法人組織の実在性、本人性を、以下のいずれかの方法により確認する。

- 商業登記簿謄本、法人印の印鑑証明書、および法人印による押印がなされた証明書申請書の確認
- 第三者が提供するデータベースによる企業コードおよび公開情報の確認と公開情報を利用した電話による当該法人に対する申請の意思の確認

(2) ドメイン・ネームの利用者所有確認

本認証局は、法人向けサーバ証明書に記載するサーバの FQDN について、当該 FQDN を利用する権利を有していることを、以下のいずれかの方法により確認する。

- whois 等の第三者が提供するデータベースを利用したドメイン所有権の確認
- 上記ドメイン・ネーム所有者による、当該ドメイン・ネーム使用許諾の確認

3.2.3. 個人の本人性の確認

本認証局は、個人事業主の実在性、本人性の確認を以下の方法により確認する。

(1) 利用者の実在性、本人性確認

本認証局は、事業主の個人の実在性、本人性を、以下の方法により確認する。

- 個人印の印鑑登録証明書、および当該個人印による押印がなされた証明書申請書の確認

(2) ドメイン・ネームの利用者所有確認

本認証局は、個人事業主向けサーバ証明書に記載するサーバの FQDN について、当該 FQDN を利用する権利を有していることを、以下のいずれかの方法により確認する。

- whois 等の第三者が提供するデータベースを利用したドメイン所有権の確認
- 上記ドメイン・ネーム所有者による、当該ドメイン・ネーム使用許諾の確認

3.2.4. 検証対象としない利用者情報

本認証局は、本認証局が発行する利用者証明書に記載される識別名(DN)に記載される、以下の項目については検証対象としない。

(1) 従業者の個人名

法人向けクライアント証明書の CN に従業者の個人名が記載されるケースにおいて、当該氏名は、利用者からの申請情報に基づくものとし、本認証局はその実在性、本人性について検証しない。

(2) 電子メールアドレスに含まれるドメイン・ネームの所有

法人向けクライアント証明書および個人事業主向けクライアント証明書に記載される電子メールアドレスについて、本認証局はそのドメイン・ネームの所有確認は行わない。

3.2.5. 権限の正当性確認

本認証局は、以下の申請責任者からの申請のみを受理し、これ以外の代理人による申請を認めない。

種別	説明
法人	組織に属する従業者で、申請組織を代表して申請する権限を委譲された者。本認証局は、当該従業者が申請組織を代表して申請を行う権限を有していることを、申請組織より提出された書面により確認する。
個人事業主	申請された証明書を利用する個人本人。なお本認証局は、当該申請が証明書利用者本人より提示されたことを、提出された書面により確認する。

3.2.6. 相互運用性基準

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. 証明書更新時の本人性確認と認証

証明書更新時の本人性確認と認証は、初回登録時の本人性確認と同一の方法によって行う。

3.3.2. 証明書の再発行時の本人性確認と認証

何らか事由によって利用者の証明書を失効した後に、証明書の再発行を行う場合の本人性確認と認証は、初回登録時の本人性確認と同一の方法によって行う。

3.4. 失効申請時の本人性確認と認証

利用者による証明書の失効は申請責任者が本認証局の定める所定の手続きにより申請を行うものとする。本認証局は、申請責任者の本人性の確認を行う。

なお、緊急を要する場合には FAX による失効申請を受け付ける。この場合、申請責任者に対する電話連絡により本人性の確認を行う。

第4章　証明書のライフサイクル

4.1.　証明書申請

4.1.1.　証明書申請を提出できる者

本認証局は、以下の者から証明書の申請を受け付ける。

- 流通業界と関係を有する法人の従業者
- 流通業界と関係を有する個人事業主

4.1.2.　登録手続きおよび責任

本認証局に証明書の申請を行おうとするものは、申請責任者を選任する。法人の場合は、当該法人組織から権限を委譲された従業者を申請責任者とする。個人事業主の場合は申請者本人とする。

申請責任者は、申請書に必要事項を記入し、所定の書類および電子データと共に、本認証局の受付窓口に提出する。申請責任者は、本認証局に正確な情報を提示する義務を負う。

4.2.　証明書申請の処理手順

4.2.1.　本人性確認と認証機能の実行

本認証局は、申請者の実在性、本人性および申請内容の真正性を認証する。認証の内容は本CPS3.2.2 項および 3.2.3 項に規定する。

4.2.2.　申請の承認または却下

本認証局は、申請を行った利用者の実在性および同一性、申請内容の真正性を確認した場合に、申請者からの申請を承認する。

申請書類に不備があった場合および 4.2.1 項（本人性確認と認証機能の実行）で規定する本人性確認の手続において疑義、およびその他の懸念が生じた場合には、申請を却下する。

4.2.3.　証明書申請の処理時間

本認証局は、通常、申請受領後 10 営業日以内に審査結果の通知を申請責任者に対して行う。

4.3.　証明書発行

4.3.1.　証明書の発行処理

本認証局は、4.2.3 項（証明書申請の処理時間）の審査結果の通知とともに、証明書を電子メールで送付または証明書発行用 Web サイトからダウンロード可能な状態にする。

4.3.2.　利用者への証明書発行通知

本認証局は、電子メールで証明書を発行する場合、証明書の発行をもって発行通知とする。証明書発行用 Web サイトから証明書を発行する場合、申請責任者に対してダウンロード準備がで

きたことを電子メールで通知する。

4.4. 証明書受領

4.4.1. 証明書の受領確認の行為

利用者は、本認証局から発行された証明書を受領した際に、証明書の記載内容に誤りがないことを確認する義務を負う。証明書記載内容等に誤りがあった場合、申請責任者を通じて、速やかにその旨を申し出なければならない。本認証局は、証明書発行後 5 営業日を経過して申し出がない場合、証明書受領が完了し、記載内容を確認したものと見なす。

4.4.2. 本認証局による証明書の公開

本認証局は、利用者証明書の公開を行わない。

4.4.3. 他の関係者への通知

本認証局は、利用者以外のエンティティに対して証明書発行通知を行わない。

4.5. 鍵ペアと証明書の使用

4.5.1. 利用者による秘密鍵および証明書の使用

利用者は、秘密鍵および証明書を本 CPS1.4.1 項で規定する証明書の利用用途に即して利用しなければならない。

4.5.2. 検証者による利用者の公開鍵および証明書の利用

検証者は本 CPS1.4.1 項で規定された証明書の利用用途に即した場合のみ依拠することができる。

4.6. 鍵の更新を伴わない証明書の更新

本認証局は、鍵の更新を伴わない証明書の更新は行わない。

4.7. 鍵の更新を伴う証明書の更新

4.7.1. 鍵の更新を伴う証明書の更新の場合

鍵の更新を伴う証明書の更新は、以下の場合において行われる。

- 失効されていない利用者の証明書の有効期限が満了する場合。
- 何らかの理由で証明書を失効し、再発行を行う場合。

4.7.2. 証明書の更新申請を行う者

証明書の更新申請は、申請責任者が行う。

4.7.3. 証明書の鍵更新申請の処理

本認証局は、鍵の更新を伴う証明書の更新は初回発行と同一の処理手続きにより行う。

4.7.4. 利用者に対する新しい証明書の通知

証明書更新における新しい証明書の発行通知は、本 CPS4.3.2 項と同一の方法による。
なお、証明書の有効期限満了に先立ち、申請責任者に対して、更新の案内を電子メールで連絡する。

4.7.5. 鍵更新された証明書の受領確認の行為

利用者は、証明書更新により新しい証明書を受領した際に、本 CPS4.4.1 項に規定される初回発行時と同様の受領確認を行わなければならない。

4.7.6. 認証局による鍵更新済みの証明書の公開

本認証局は、利用者証明書の公開を行わない。

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

本認証局は、利用者以外のエンティティに対して証明書発行通知を行わない。

4.8. 証明書の変更

本認証局は、証明書の変更は実施しない。
証明書の記載内容変更が必要な場合は、使用している証明書を本 CPS4.9 節の手続きに従い失効し、新たな証明書を初回発行の手続きにより取得する。

4.9. 証明書の失効と一時停止

4.9.1. 証明書失効の場合

利用者は、以下の場合証明書を失効する。

- 利用者の秘密鍵が危殆化した、または危殆化した恐れがある場合
- 利用者が証明書の利用を取りやめる場合
- 証明書で記載されている情報に変更があった場合

本認証局は、以下の場合、認証局事由により利用者証明書を失効する。

- 利用者秘密鍵の危殆化あるいはその恐れがある場合
- 利用者証明書の記載事項に誤りがある場合
- 利用者が本 CPS、標準 CP、その他の契約または該当法規の遵守を怠った場合
- 本認証局秘密鍵の危殆化あるいはその恐れがある場合
- 本認証局が認証業務を廃止する場合
- その他、本認証局が必要と判断した場合

本認証局は、失効された利用者証明書とその失効の理由について、利用者および検証者に公

開する。

4.9.2. 証明書失効を申請することができる者

利用者による証明書の失効申請は、申請責任者が行う。

4.9.3. 失効申請手続き

利用者により証明書の失効は、所定の申請書を本認証局の受付窓口に提出する。また、利用者秘密鍵の危殆化等、緊急性を要する場合、本認証局は FAX による失効申請を受け付ける。本認証局は、あらかじめ利用者から登録された申請責任者から申請が提出されたことを確認する。

4.9.4. 失効申請の猶予期間

利用者は本 CPS4.9.1 項で規定された失効事由に該当した場合、速やかに失効手続きを行わなければならない。

4.9.5. 本認証局が失効処理を行うまでの時間

本認証局は、失効申請内容に問題がない場合は、通常、失効申請受理後 5 営業日以内に失効処理を実施する。緊急性を要する場合は、直ちに失効処理を行う。

4.9.6. 検証者の失効確認の要求

検証者は本認証局が発行した証明書に依拠する前に最新の CRL を確認し、当該証明書が失効されていないことを確認しなければならない。

4.9.7. 証明書失効リストの発行周期

本認証局は、通常時は 24 時間に 1 回以上 CRL を発行する。

4.9.8. 証明書失効リストの発行最大遅延時間

本認証局は、システムの障害や罹災等によりメインサイトでのサービス継続が困難な場合、バックアップサイトに切替て CRL の発行を行う。この場合の最大遅延時間は 48 時間を目標とする。

4.9.9. オンラインでの失効/ステータス確認の適用性

本認証局は、OCSP による証明書有効性情報の提供を行わない。

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

規定しない。

4.9.11. 利用可能な失効通知の他の形式

提供しない。

4.9.12. 鍵更新の危殆化に対する特別要件

本認証局は、認証局証明書の秘密鍵が危殆化した場合、直ちに認定機関に報告し、あわせてその事実をリポジトリに公開することで関係者に通知する。

利用者は、利用者証明書の秘密鍵が危殆化した場合、あるいはその恐れがある場合、速やかに本CPS4.9.3項の手続きにより失効申請を行わなければならない。本認証局は、利用者秘密鍵の危殆化による失効申請は緊急性を要するものとして処理する。

4.9.13. 証明書の一時停止の場合

本認証局は、証明書の一時停止を行わない。

4.9.14. 証明書の一時停止を申請できる者

規定しない。

4.9.15. 証明書の一時停止申請手続き

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

本認証局は、証明書のステータス確認サービスを提供しない。

4.11. 利用の終了

利用者が何らかの事由により証明書の利用を終了する場合は、本 CPS4.9 節の手続きにより証明書の失効申請を行わなければならない。

4.12. 鍵預託と鍵回復

本認証局は、鍵預託は行わない。

第5章 設備、管理、運用統制

5.1. 物理的管理

5.1.1. 施設の所在と構造

本認証局は、認証局秘密鍵の管理・利用を行う施設（以下、認証局秘密鍵管理施設という）は通常想定される災害に対しては十分耐え得る建築構造物内に設置され、不正侵入等を防止するためのセキュリティ対策が講じられる。

認証局秘密鍵管理施設は、以下の要件を満たす。

- 建築基準法に適合した堅牢な建物の中の安全な場所に設置されている。
- 洪水・地震等の天災に対する安全性を確保するために十分な立地条件に建築されている。
- 本認証局の所在および仕様は、関係者以外には厳重に秘匿される。
- 常時、不正侵入に備えて監視されている。

5.1.2. 物理的アクセス

本認証局の設備を設置する施設は、生体認証等を利用し厳格な個人による入退室管理を行う。また、秘密鍵管理施設は入室権限を有する複数人以上の立会いがなければ入室が可能とならない仕組みを講じる。本認証局において登録局の業務を行う施設（以下、認証業務室という）は、他の執務室とは隔離し、適切な入退室管理を行う。

5.1.3. 電源および空調

認証局秘密鍵管理施設において利用される機器には、停電に対する対策を講じる。また、認証局秘密鍵管理施設において利用される機器が適切に動作するための空調設備を整備する。

5.1.4. 水害対策

本認証局の設備は、水害防止措置として建物の上層階に配置するとともに、天井に導水管を配置しない、あるいは室内に水場を設けない等の防水対策を講じる。

5.1.5. 火災防止および火災保護対策

本認証局の設備を設置する施設は、不燃性の建材で構成されており、室内センサー、煙検知器、および消火設備が設置されている

5.1.6. 媒体保管場所

本認証局は、記録媒体を施錠した場所に保管する。また、保管した記録に対するアクセスは、適切な搬入出手続きの下で行う。

5.1.7. 廃棄物処理

本認証局は、書類および電子記録媒体等の記録を廃棄するときは、所定の手続きにより適切に

廃棄処理を行う。
書類は、裁断処理した上で廃棄する。光磁気ディスクや固定ディスク等の電子記録媒体は、物理的なダメージを与え破壊するか、無効情報を上書きする等の完全消去処理をした上で廃棄する。

5.1.8. 施設外のバックアップ

本認証局は、バックアップサイトを持つ。バックアップサイトは、メインサイトと地理的に十分に離れた場所に設置され、合理的な物理的および論理的セキュリティを確保するものとする。

5.2. 手続き的管理

5.2.1. 信頼すべき役割

本認証局は、業務の役割および業務を遂行する担当者を定め、各役割に応じた権限を適切に割当てる。

5.2.2. 職務ごとに必要とされる人数

本認証局は、認証局秘密鍵の管理を含む重要な業務については、権限を有する複数の担当者による相互牽制下で実施する。また、利用者から提出された申請の審査に関する業務は、複数担当者によるダブルチェックを行い、一人の担当者では審査が完了しない仕組みを講じている。
各業務の役割に従事する人数は、相互牽制の要求を満たすように定められる。

5.2.3. 個々の役割に対する本人性確認と認証

本認証局に従事するものは、任命の際に適切な本人性の確認を行う。また、本認証局設備に対する物理的、論理的アクセスにおいて、適切な認証を行う。

5.2.4. 職務分割が必要となる役割

本認証局は、職務分離が必要となる役割を定め、分離が必要な役割の兼務を行わない。

5.3. 人事的管理

5.3.1. 資格、経験および身分の要件

本認証局の要員は、インテックおよび株式会社インテックソリューションパワー（以下、ISP という）の役員ならびに従業員とする。

5.3.2. 経歴確認の手続き

本認証局の要員は、インテックおよび ISP の社内規定ならびに手続きに従って実在性と同一性の確認が行われる。また、本認証局は別途定める手順に基づき、業務経歴の管理を行う。

5.3.3. 教育訓練要件

認証局は、認証業務を担う要員に対し、業務を遂行する上で必要となる知識を習得させる教育を適切に行う。

5.3.4. 再研修の頻度および要件

本認証局は、定期的に危機管理に関する教育訓練を実施する。また、業務手順の変更時には、手順の変更に係る教育訓練を実施する。

5.3.5. 職務のローテーションの頻度および要件

規定しない。

5.3.6. 許可されていない行動に対する罰則

本認証局は、許可されていない行動、許可されていないシステムへのアクセス、CA の濫用等の行為を行った要員に対し、直ちに本認証局における業務上の権限を停止する。また、義務の不完全履行、職務怠慢および不正行為等に該当する場合は、社内規定の罰則を適用する。

5.3.7. 独立した契約者の要件

本認証局は、請負業者との契約書にセキュリティ上必要な条項を含め、適切な業務管理を行う。また、本認証局の施設設備への業者のアクセスが本 CPS5.1.2 項に従って行われるよう義務付ける。

5.3.8. 要員に提供する資料

本認証局は、要員に対して、その役割に応じた業務の遂行に必要なマニュアルおよび手順書を容易に参照できる状態に置く。

5.4. 監査ログの取扱い

5.4.1. 記録されるイベントの種類

本認証局は、以下のイベントを含む監査ログを記録し、保管する。

- CA の構築
- 証明書プロファイルの設定
- 認証局秘密鍵の操作
- 証明書の発行
- 証明書の失効
- CRL の発行

本認証局は、入退室管理システムにより、以下のイベントを含むログを記録し、保管する。

- 認証局秘密鍵管理施設の入退室
- 認証局設備を設置する施設の入退室

- 登録局の業務を行う認証業務室の入退室

5.4.2. 監査ログを処理する頻度

本認証局は、日次で監査ログのデータバックアップを行い、月次でバックアップ媒体を安全な場所に保管する。

5.4.3. 監査ログを保持する期間

本認証局は、監査ログを少なくとも1ヶ月以上は容易に参照できる場所に保持する。

5.4.4. 監査ログの保護

監査ログは、そのアクセス権限を持つ要員のみが参照可能となるよう保護する。また、監査ログには改ざんを防止するために電子署名を付加する。

5.4.5. 監査ログのバックアップ手続き

監査ログのバックアップは、安全な環境で行う。

5.4.6. 監査ログの収集システム

規定しない。

5.4.7. イベントを起こした当事者への通知

監査ログは、対象となる事象を発生させた当事者に対して通知を行うことなく記録される。

5.4.8. 脆弱性の評価

監査ログとして記録される事象の一部は、システムの脆弱性を把握するために用いられる。本認証局は、脆弱性の評価を行い、必要に応じて措置を講ずる。

5.5. 記録のアーカイブ

5.5.1. アーカイブされる記録の種類

本認証局は、以下の記録をアーカイブする。

(1) 証明書の初回発行に関する記録

- 利用者が提出した書類
- 本認証局における審査記録(審査結果、審査日時、審査担当者、承認者に関する情報等)

(2) 証明書の更新に関する記録

- 利用者が提出した書類
- 本認証局における審査記録(審査結果、審査日時、審査担当者、承認者に関する情報等)

(3) 証明書の失効に関する記録
- 利用者が提出した書類
- 本認証局における審査記録(審査結果、審査日時、審査担当者、承認者に関する情報等)

(4) 認証局秘密鍵の操作に関する記録

(5) 各流通業界共通認証局の組織の維持管理に関する記録
- 認証局に関連する規程類(各 CPS、利用者規約、依拠当事者規約等)
- 認証局組織図および任命・解任記録

5.5.2. アーカイブ保持期間

本認証局は、アーカイブの保持機関を以下の通り定める。

(1) 証明書の初回発行に関する記録
当該証明書の有効期間が満了してから少なくとも 3 年間。

(2) 証明書の更新に関する記録
当該証明書の有効期間が満了してから少なくとも 3 年間。

(3) 証明書の失効に関する記録
当該証明書を失効してから少なくとも 3 年間。

(4) 認証局秘密鍵の操作に関する記録
当該秘密鍵のライフサイクル終了まで。

(5) 共通認証局の組織の維持管理に関する記録
改訂より少なくとも 10 年間。

5.5.3. アーカイブの保護

本認証局は、アーカイブに対して、容易にアクセスできないよう保護措置を講ずる。電子データをアーカイブした媒体は適切な環境下に保管する。アーカイブを記録した媒体は、定期的に可読性を検査する。

5.5.4. アーカイブのバックアップ手続き

電子データをアーカイブした媒体は 2 式作成し、メインサイトとバックアップサイトに分散して保管する。

5.5.5. 記録にタイムスタンプを付ける要件

記録に付加するタイムスタンプは正確を期する。

5.5.6. アーカイブ収集システム

規定しない。

5.5.7. アーカイブの情報を入手し検証する手続

規定しない。

5.6. 本認証局の鍵更新

認証局証明書の有効期間満了等により、認証局が使用する鍵の更新が必要な場合、本 CPS6.1 節に定める要件に従い、新しい鍵ペアを生成する。

5.7. 危殆化および災害からの復旧

5.7.1. 事故および危殆化の取扱い手続き

本認証局は、本認証局秘密鍵の危殆化した場合、認定機関および利用者への連絡方法を含む対処手続きを定める。

また、大規模なシステム障害により、48 時間以内に復旧の見込が立たない場合は、オフサイトバックアップ設備に切り替えて業務を継続する。

5.7.2. コンピュータの資源、ソフトウェア、またはデータが破損した場合

本認証局は、機器、ソフトウェア、データ等の破損に備え、システムおよびデータのバックアップ等の措置を講じる。これらに破損が生じた場合は、復旧手順に従い、速やかな業務再開に努める。

5.7.3. 利用者秘密鍵が危殆化した場合の手続き

本認証局は、利用者秘密鍵の危殆化の事実を知った場合に、速やかに該当する利用者証明書を失効する。

5.7.4. 災害後の事業継続能力

本認証局は、災害および大規模な障害の発生に備え、オフサイトバックアップ設備への切り替えを含む事業継続計画を定め、定期的に試験する。

5.8. 本認証局の業務終了

インテックにおける本認証局の業務終了についての最終意思決定は、認証局責任者がこれを行う。本認証局が業務終了を意思決定した場合、認証局責任者は合わせて業務終了手続きを決定する。

インテックは、本認証局が認証業務を終了する場合、その終了に先立ち、利用者証明書利用者、検証者に対し、その旨を通知するよう商業上合理的な努力を行う。また認定機関に対して速やかに通知を行い、本認証局が発行した全ての利用者証明書を失効し、バックアップを含む全ての認証局秘密鍵を削除する。

本認証局の業務終了にあたっては、その終了の 3 ヶ月前に通知を行う。リポジトリの公開期間は、業務終了手続きの一部として決定されるものとし、本 CPS では明記しない。

本認証局の業務終了後のアーカイブデータの管理は、インテックが行う。

第6章 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

本認証局の秘密鍵は、秘密鍵管理施設内で、権限を有する複数の担当者の関与下で、FIPS140-2 レベル 3 以上の暗号モジュールを用いて生成する。

本認証局は利用者鍵の生成は行わない。利用者証明書の秘密鍵の生成は利用者自身が行う。

6.1.2. 利用者に対する秘密鍵の配送

本認証局は利用者秘密鍵の配送は行わない。

6.1.3. 認証局に対する利用者の公開鍵

オンラインによる利用者から認証局に対する証明書発行要求は、SSL によって保護される。

6.1.4. 検証者に対する認証局の公開鍵の交付

本認証局の証明書は、本認証局のリポジトリに掲示し、検証者に交付する。リポジトリには認証局証明書との照合を可能とするため、フィンガープリントを合せて掲示する。

6.1.5. 鍵サイズ

本認証局は、全ての階層の認証局証明書に 2,048 ビット以上の鍵長を備えた RSA 暗号鍵アルゴリズムを使用する。

利用者証明書は 2,048 ビット以上の鍵長を備えた RSA 暗号鍵アルゴリズムを使用する。

6.1.6. 公開鍵のパラメータの生成および品質検査

規定しない。

6.1.7. 鍵用途の目的

本認証局の全ての階層の認証局証明書の鍵用途（keyUsage）は、公開鍵証明書への署名（keyCertSign）および CRL への署名（cRLSign）を設定する。

利用者証明書の鍵用途（keyUsage）には、デジタル署名（disitalSignature）および鍵暗号化（keyEncipherment）を設定する。

本認証局は、本認証局内の全階層の認証局について、2,048 ビットの鍵長を備えた RSA 暗号鍵アルゴリズムを使用する。

6.2. 秘密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と管理

本認証局の認証局秘密鍵は、FIPS140-2 レベル 3 以上の機能を有する暗号モジュール内で管理する。

本認証局は、利用者秘密鍵の生成および管理には関与しない。

6.2.2. 秘密鍵の複数人管理

本認証局の秘密鍵は、関連する暗号モジュールの「M of N」動作要件に基づき、権限を有する複数人の関与により管理される。

6.2.3. 秘密鍵の預託

本認証局は、秘密鍵の預託を行わない。

6.2.4. 秘密鍵のバックアップ

本認証局の認証局秘密鍵のバックアップは、秘密鍵管理施設内で複数複数人の関与により行う。
認証局秘密鍵のバックアップは、暗号化された状態で記録し、安全な場所で保管する。
本認証局は、利用者秘密鍵のバックアップには関与しない。

6.2.5. 秘密鍵のアーカイブ

本認証局は、本認証局秘密鍵のアーカイブを行わない。

6.2.6. 秘密鍵の暗号モジュールへの移動

本認証局の認証局秘密鍵のバックアップから暗号モジュールへのリストアは、秘密鍵管理施設内で「M of N」動作要件に基づき、権限を有する複数人の関与の下で行う。

6.2.7. 暗号モジュール内での秘密鍵保存

本認証局で使用する暗号モジュールは、その内部に格納してある鍵を取出すことができない仕様を有する。

6.2.8. 秘密鍵の活性化方法

暗号モジュール内の秘密鍵の活性化は、秘密鍵管理施設内において権限を有する複数人の関与の下で行う。

6.2.9. 秘密鍵非活性化の方法

暗号モジュール内の秘密鍵の非活性化は、秘密鍵管理施設内において権限を有する複数人の関与の下で行う。

6.2.10. 秘密鍵の破棄方法

本認証局は、認証局秘密鍵が利用されなくなった場合、バックアップも含めて全て廃棄する。認証局秘密鍵の廃棄は、権限を有する複数の担当者関与の下で行う。

6.2.11. 暗号モジュールの評価

本認証局の認証局秘密鍵は FIPS140-2 レベル 3 以上暗号モジュールに格納する。

6.3. その他の鍵ペア管理

6.3.1. 公開鍵のアーカイブ

本認証局は、発行した全ての利用者証明書を、当該証明書の有効期間の満了後、3 年間以上保管する。

6.3.2. 証明書の運用上の期間および鍵ペアの使用期間

本認証局の全ての階層の認証局証明書および認証局秘密鍵の利用期間は、最大で 20 年とする。

本認証局が発行する利用者証明書および利用者秘密鍵の有効期間は、最大で 3 年 2 ヶ月とする。

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

本認証局秘密鍵の活性化情報は、別途定める手順に従い、権限を有する複数人の関与の下、生成および設定を行う。本認証局は、利用者秘密鍵の活性化情報の生成および設定には関与しない。

6.4.2. 活性化データの保護

本認証局秘密鍵の活性化情報は、別途定める手順に従い、権限を有する複数人の関与の下において管理される。利用者は、自身で作成した活性化データを安全に保管しなければならない。

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

本認証局は、情報セキュリティマネジメント規格 JIS Q27001:2006 の審査登録適合を受けた組織が運用・管理する。

6.6. ライフサイクルの技術上の管理

本認証局は、情報セキュリティマネジメント規格 JIS Q27001:2006 の審査登録適合を受けた組織がシステム保守を行う。

6.7. ネットワークセキュリティ管理

本認証局は、情報セキュリティマネジメント規格 JIS Q27001:2006 の審査登録適合を受けた組織

がネットワークセキュリティの維持を行う。

6.8. タイムスタンプ

本認証局は、本 CPS5.4.1 項および 5.5.1 項で定めた電子データ・書類に日時、または日付情報を付与する。

第7章 証明書、CRL の各プロファイル

7.1. 証明書プロファイル

本項では、本認証局の認証局証明書のプロファイル、ならびに本認証局が発行する利用者証明書のプロファイルを規定する。

別紙 1 に、各証明書の詳細プロファイルを記載する。

7.1.1. バージョン番号

本認証局が発行する証明書のバージョンは 3 である。

7.1.2. 証明書の拡張領域

本認証局は、RFC 3280「インターネット X.509 公開鍵基盤証明書および CRL プロファイル」(2002 年 4 月付)に従って、バージョン 3 拡張をサポートする。

本認証局の認証局証明書(ルート認証局、中間認証局)の拡張領域は以下の通りとする。

No.	フィールド	クリティカル	内容
1	authorityKeyIdentifier	FALSE	発行された証明書の署名に用いられた秘密鍵に対応する CA の公開鍵を識別する手段を提供する。
2	subjectKeyIdentifier	FALSE	特定の公開鍵を含む証明書を識別する手段を提供する。
3	keyUsage	TRUE	cRLSign、keyCertSign とする。
4	basicConstraints	FALSE	cA=TRUE とする。 下位の認証パスを次のように設定する。 ルート認証局 ・・・ 1 中間認証局 ・・・ 0

また、本認証局が発行する法人向けサーバ証明書、個人事業主向けサーバ証明書の拡張領域を以下の通りとする。

No.	フィールド	クリティカル	内容
1	authorityKeyIdentifier	FALSE	発行された証明書の署名に用いられた秘密鍵に対応する CA の公開鍵を識別する手段を提供する。
2	subjectKeyIdentifier	FALSE	特定の公開鍵を含む証明書を識別する手段を提供する。
3	keyUsage	TRUE	digitalSignature, keyEncipherment, dataEncipherment とする。
4	extendedKeyUsage	FALSE	サーバ認証(1.3.6.1.5.5.7.3.1) クライアント認証(1.3.6.1.5.5.7.3.2) 電子メールの保護(1.3.6.1.5.5.7.3.4)

No.	フィールド	クリティカル	内容
5	certificatePolicies	FALSE	本 CPS の公開先のポイントの識別を行う。
6	subjectAltName	FALSE	URL 表示を行っているサーバの名前を設定する。
7	basicConstraints	FALSE	cA=FALSE とする。
8	cRLDistributionPoints	FALSE	失効情報のための CRL 公開先のポイントを提供する。

本認証局が発行する、法人向けクライアント証明書、個人向けクライアント証明書の拡張領域は以下の通りとする。

No.	フィールド	クリティカル	内容
1	authorityKeyIdentifier	FALSE	発行された証明書の署名に用いられた秘密鍵に対応する CA の公開鍵を識別する手段を提供する。
2	subjectKeyIdentifier	FALSE	特定の公開鍵を含む証明書を識別する手段を提供する。
3	keyUsage	TRUE	digitalSignature, keyEncipherment, dataEncipherment とする。
4	extendedKeyUsage	FALSE	クライアント認証(1.3.6.1.5.5.7.3.2) 電子メールの保護(1.3.6.1.5.5.7.3.4)
5	certificatePolicies	FALSE	本 CPS の公開先のポイントの識別を行う。
6	subjectAltName	FALSE	URL 表示を行っているサーバの名前を設定する。
7	basicConstraints	FALSE	cA=FALSE とする。
8	cRLDistributionPoints	FALSE	失効情報のための CRL 公開先のポイントを提供する。

7.1.3. アルゴリズムオブジェクト識別子

本節では、証明書への署名形式と証明書で証明される公開鍵の形式を規定する。

2015 年 9 月 30 日までに本認証局が発行する利用者証明書は、sha1WithRSAEncryption(OID: 1.2.840.113549.1.1.5)方式を用いて、2048bit の本認証局秘密鍵で署名される。基本領域の signature フィールドには当該アルゴリズム識別子の OID が設定される。また、rsaEncryption 形式(OID: 1.2.840.113549.1.1.1) の公開鍵を使用し、基本領域の subjectPublicKeyInf フィールドに当該公開鍵が設定される。

2015 年 10 月 1 日以降に本認証局が発行する利用者証明書は、sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)方式を用いて、2048bit の本認証局秘密鍵で署名される。基本領域の signature フィールドには当該アルゴリズム識別子の OID が設定される。また、rsaEncryption 形式(OID: 1.2.840.113549.1.1.1) の公開鍵を使用し、基本領域の subjectPublicKeyInf フィールドに当該公開鍵が設定される。

ただし、ビジネス上緊急であると本認証局が認めた場合、2015 年 10 月 1 日以降に sha1WithRSAEncryption(OID: 1.2.840.113549.1.1.5)方式を用いて証明書を限定的に発行

することがある。なお本例外ケースで発行した証明書の有効期限は 2018 年 10 月 1 日を越えてはならない。

7.1.4. 名前形式

本認証局証明書および本認証局が発行する利用者証明書は、PKIX Part1 標準に従った X.501 識別名(DN)の規定に従い決定する。また、本認証局証明書、利用者証明書に記載される名称は、本 CPS3.1.2 項に従う。

issure および subject のデータ型は全て Printable String を使用する。

7.1.5. 名前制約

設定しない。

7.1.6. 証明書ポリシーオブジェクト識別子

本 CPS の OID は 1.2.392.200057.1.94401.2.1である。

7.1.7. ポリシー制約拡張の使用

本認証局が発行する利用者証明書は、ポリシー制約拡張を設定しない。

7.1.8. ポリシー設定子の構文および意味

規定しない。

7.1.9. クリティカルな証明書ポリシー拡張に対する処理の意味

規定しない。

7.2. CRL プロファイル

別紙 1 に、CRL の詳細プロファイルを記載する。

7.2.1. バージョン番号

本認証局は、RFC 3280「インターネット X.509 公開鍵基盤証明書および CRL プロファイル」(2002 年 4 月付)に従って、X.509 バージョン 2 証明書失効リストを発行するものとする。

7.2.2. CRL エントリ拡張

本認証局は、以下の CRL エントリ拡張領域をサポートし、使用するものとする。

No.	フィールド	クリティカル	内容
1	reasonCode	FALSE	利用者証明書の失効事由

7.2.3. CRL 拡張

本認証局は、以下の CRL 拡張領域をサポートし、使用するものとする。

No.	フィールド	クリティカル	内容
1	auThorityKeyIdentifier	FALSE	CRL の署名用に用いられる秘密鍵に対応する認証局公開鍵の識別手段を提供する。
2	cRLNumber	FALSE	CRL 番号拡張は、本認証局が発行した CRL ごとに連続番号を明記する。

7.3. OCSP プロファイル

規定しない。

第8章　準拠性監査とその他の評価

8.1.　監査の頻度あるいは条件

本認証局は、標準 CP および本 CPS に準拠して業務が遂行されていることについて、1年に1回以上、監査を実施し、運用状況を認定機関に報告する。

8.2.　監査人の要件

本認証局の監査を行うものは、監査に関する知識を有し、かつ認証業務に関する知識を有していなければならない。

8.3.　監査人と非監査人の関係

監査は、外部の監査法人等に所属する者、あるいは監査対象業務の運用に直接携わっていないインテックの従業員が行う。

8.4.　監査の対象

準拠性監査は、標準 CP および本 CPS に準拠して発行業務、更新業務、失効業務を実施していることを検証することを目的とするが、監査の対象は、これらの業務に限定しない。

8.5.　監査指摘事項への対応

監査の結果、本認証局の業務が標準 CP および本 CPS に反していることが判明した場合は、本認証局は、ただちに是正処置を実施し、その処置について認定機関に報告する。それ以外の監査指摘事項については、本認証局の判断により是正処置を行う。

8.6.　監査結果の開示

本認証局は、認定機関より監査結果の照会を求められた場合、監査指摘事項の有無やその対応状況について報告を行う。

第9章 他のビジネス的・法的問題

9.1. 料金

9.1.1. 証明書の発行および証明書の更新に関わる料金

本認証局が発行する利用者証明書の発行および更新に関わる料金については、以下のURLに提示する。

https://www.einspki.jp/services/services_foredi/

9.1.2. 証明書の参照に関わる料金

本認証局は、検証者またはその他のエンティティが本認証局の認証局証明書を参照するためリポジトリにアクセスすることに関して、料金を課さない。

9.1.3. 失効情報の参照に関わる手数料

本認証局は、検証者またはその他のエンティティが本認証局より発行された利用者証明書の失効情報参照するためリポジトリにアクセスすることに関して、料金を課さない。

9.1.4. 他のサービスに関する利用料金

規定しない。

9.1.5. 返金制度

利用者が証明書の利用を中止した場合の料金の返金は行わない。

9.2. 財務的責任

9.2.1. 保険の範囲

適用しない。

9.2.2. 他の資産

本認証局を運営するインテックは、その財務状況を以下のURLに提示する。

https://www.intec.co.jp/

9.2.3. 拡張された保証の範囲

規定しない。

9.3. 業務情報の機密性

9.3.1. 機密として扱う情報の範囲

本認証局は、以下の情報を機密情報として取り扱う。

(1) 提出された書類を含む利用者の情報

(2) 本 CPS9.3.2 項を除く本認証局の文書および記録
(3) 認証局の所在

9.3.2. 機密として扱わない情報

本認証局は以下の情報を機密としない。
(1) 各 CPS
(2) 利用者規約
(3) 検証者規約
(4) 自身が発行した証明書および証明書に記載されている情報
(5) CRL、および CRL に記載されている情報

9.3.3. 機密として扱う情報を保護する責任

認証業務を実施する上で利用者から入手した情報を、認証業務を実施する上で必要とする目的以外に利用しない。

9.4. 個人情報のプライバシー保護

本認証局は以下の URL で公開されているインテックの個人情報保護方針および「個人情報の取扱いについて」に従って個人情報を保護する。

https://www.intec.co.jp/

9.5. 知的財産権

以下の情報資料およびデータの知的財産権は、本認証局に帰属する。

- 本 CPS およびその他の公開情報
- 本認証局証明書の秘密鍵および公開鍵
- 本認証局から発行された利用者証明書
- 本認証局から発行された CRL

9.6. 表明保証

9.6.1. 認証局の義務と責任

本認証局は、本 CPS および標準 CP の規定に従い、認証局の運用を行う。
また本認証局が実施する認証業務について、本 CPS8.3 節で規定する者による監査を実施する。
監査報告に基づき、改善が必要と判断される場合には、速やかに対応する。

9.6.2. 利用者の義務と責任

利用者は、以下の事項を保証することに対し、義務と責任を負う。なお利用者の義務の詳細については、「利用者規約」に定める。
(1) 本 CPS および利用者規約の承諾

利用者は、利用者証明書発行申請にあたり、本 CPS および利用者規約を理解し、承諾する。

(2) 証明書申請内容の正確さ

利用者証明書発行申請にあたり、利用者が本認証局に提供した情報(所定の申請書に記載された内容を含む)は正確である。

(3) 証明書記載事項の確認

利用者は、利用者証明書の受領時において、利用者証明書の記載事項を確認し、その内容が申請内容と相違ないことを確認する。利用者証明書の記載事項が申請内容と異なる場合には、申請責任者を通じて本認証局に通知する。

(4) 適切な鍵ペアの生成

ハードウェアまたはソフトウェアのいずれかを使用して適切な鍵ペアを生成する。また、その秘密鍵が適切にインストールされることを確保する。使用する秘密鍵は、過去において本認証局以外の他の人または当事者との通信で使用されていない。

(5) 秘密鍵の保護

パスワード保護、ハードウェア・セキュリティ・モジュールまたは他の合理的な保護手段を用いて、秘密鍵を危殆化から保護すべく最善の努力を払う。

9.6.3. 検証者の義務と責任

検証者は、以下の事項を保証することに対し、義務と責任を負う。なお検証者の義務の詳細については、「検証者規約」に定める。

(1) 本 CPS および検証者規約への同意

検証者は、利用者証明書の利用において、本 CPS および検証者規約へ同意しなければならない。

(2) 本認証局証明書の有効性の確認

検証者は、本認証局証明書のフィンガープリントをリポジトリから入手し、取得した認証局証明書が本認証局のものであることを確認する。

(3) 証明書の有効性の確認

検証者は、本認証局が発行した利用者証明書を信頼すべきかどうかを判断するために、証明書の有効性を確認しなければならない。

9.7. 無保証

本認証局の保証は、本 CPS9.6.1 項に定めた内容に限定される。本認証局は、申請者契約または他の該当顧客契約等に別途定めがある場合を除き、何の責任も負わない。いかなる場合も、本認証局は、相手先当事者の如何を問わず、本認証局が発行した証明書から生ずるか、何らかの方法でこれに関連する付随的損害、派生的損害、特別損害、間接損害または懲罰的損害、逸失事業利益、またはデータの損失、損傷もしくは破壊に対しては責任を負わないものとし、これはその訴訟の形式が債務不履行、不法行為(過失を含む)、保証違反またはその他にあるかどうかを問わない。

本 CPS のいずれの条項も、該当契約に記載がある場合を除き、他人のために行動したり、他人を拘束したり、他人のために義務や責任を創出もしくは引き受けたり、または他人に代って何らかの表明を行う権限をいかなる第三者に対しても委ねるものではない。本 CPS に従った証明書の発行によって、本認証局が、申請者、顧客または他の利用者の代理人、パートナー、ジョイントベンチャー先、受託者、信託者もしくは他の代表者の立場に置かれるものではない。本認証局と利用者の間の関係は、該当する契約によってのみ定義される。

9.8. 責任の制限

9.8.1. 認証局の責任

本認証局は、本 CPS および標準 CP に規定した責任を果たさなかった場合にのみ、その責任を負う。

9.8.2. 利用者、検証者の義務違反

(1) 利用者の義務違反

利用者が本CPS9.6.2項、その他本CPSで定める利用者の義務に違反したことに起因して生じた損害について、本認証局は、関係者に対し一切の責任を負わないものとする。

(2) 検証者の義務違反

検証者が本CPS9.6.3項、その他本CPSで定める検証者の義務に違反したことに起因して生じた損害について、本認証局は、関係者に対し一切の責任を負わないものとする。

9.8.3. 利用者の義務違反による証明書の失効

利用者が、本 CPS 9.8.2 項の(1)に述べる責任・義務に違反していることが明らかな場合、本認証局は、利用者への事前の通知を行うことなく、発行した利用者証明書を失効させることができるものとし、これに対し利用者は一切の請求、異議申し立てを行うことができない。

9.9. 補償

本 CPS および標準 CP に規定された責任を果たさなかったことに起因して、本認証局が利用者に対して損害を与えた場合、本認証局は、責任を果たせなかった利用者証明書の料金を上限として、損害を賠償する。ただし、本認証局側の責に帰さない事由から発生した損害、逸失利益、間接損害、または予見の有無を問わず特別損害、暗号アルゴリズムの脆弱性が発見された場合の損害、コンピュータによる不測の攻撃による損害およびデータの喪失については、いかなる場合でも一切の責任を負わない。また、本認証局は、本認証局の発行する証明書の不適切な使用に起因して発生した各種損害に対して、利用者、その他第三者(検証者を含むがこれに限らない)に対し、一切の責任を負わない。

また標準CP、本CPSおよび利用者規約に別途の定めがない限り、利用者はここに、証明書の使用もしくは開示を原因とし、かつ以下のいずれかから発生する請求、訴訟もしくは要求につき、それらから本認証局を防禦しこれを補償することに合意する。

(1) 利用者による事実の虚偽表明または誤解を招く表明。
(2) 利用者による重大な事実の非開示で、その不作為が過失によるか、もしくは詐害の意図をもってなされたもの。
(3) 利用者側における、その秘密鍵、パスワードもしくは PIN(該当する場合)の保護の不履行、または利用者の秘密鍵の危殆化、開示、紛失、修正もしくは不正使用を防ぐために必要な措置の不履行。
(4) 申請責任者が一旦利用者の秘密鍵の危殆化、開示、紛失、修正もしくは不正使用について知ったか、または擬制上知るべきこととなった時において、当該事態につき速やかに本認証局に対して通知することを怠ること。

9.10. 文書の有効期間と終了

9.10.1. 文書の有効期間

本 CPS の有効期間は、本 CPS が認証局責任者による承認および認定機関の認定を受けてから、本 CPS が無効となるまでの間である。本 CPS の無効については、本 CPS9.10.2 項において規定する。

9.10.2. 終了

本 CPS は、本 CPS9.10.3 項に規定した存続条項を除き、本認証局が業務を終了した時点で無効となる。
認定機関が標準 CP を無効とした場合も、本認証局は本項の定めに従い、終了手続きを実施するものとする。

9.10.3. 終了の影響と存続事項

本認証局が本認証サービスを終了した場合においても、本 CPS における以下の条項の効力は存続する。

- 本 CPS9.3 項
- 本 CPS9.4 項
- 本 CPS9.5 項
- 本 CPS9.7 項
- 本 CPS9.8 項
- 本 CPS9.9 項

9.11. 個々の関係者間に対する通知と連絡

本認証局は、利用者に対して電子署名の実施の方法および認証業務の利用に関する重要な事項についての説明を利用者規約の配布により行う。利用者規約は、利用者証明書の発行申請時に所定の申請書のダウンロードとともに取得できる。
また本認証局は、以下の事項について、リポジトリにおいて通知する。

- 本 CPS で定める公開文書が改訂された場合。
- 本認証局の秘密鍵が危殆化した場合。
- 本認証局の認証業務を終了する場合。

本認証局から利用者に対し個別の通知が必要となった場合、当該利用者に対して、最新の申請情報に基づいた住所に対し郵送を行うか、電子メール、電話、FAX 等を使用して連絡を行うものとする。

9.12. 改訂

9.12.1. 改訂手続き

本 CPS の改訂については、本認証局が起案し、認証局責任者の承認および認定機関の認定を受ける。

9.12.2. 通知方法および期間

本認証局は、本 CPS の変更内容をリポジトリにおいて公開することをもって通知する。本 CPS の初版公開後、その内容を改訂した場合は、公開後 14 日間の経過をもって、本認証局は、利用者が変更事項を承認したとみなし、本 CPS の効力を有効なものとする。なお当該期間において、関係するエンティティは、本認証局に対してコメント等を提出できる。コメント等を提出する場合は、本 CPS1.5.2 項に記載した窓口に対して行うものとする。

9.12.3. OID の変更

規定しない。

9.13. 紛争解決手段

本認証局とその他のエンティティとの間の鍵および証明書管理に関連する紛争は、適切な紛争解決方法を用いて解決することを要する。紛争は、可能な限り交渉を経て解決すべきものとする。
本認証局は、締結する契約に、適切な紛争解決手続きを定めるものとする。
交渉、調停または仲裁により解決できない紛争は、関係者の所在にかかわらず、東京地方裁判所を専属的合意管轄裁判所とする。

9.14. 準拠法

本認証局と関係者の間で紛争が生じた場合に適用される法令は、日本国内法を準拠法とする。

9.15. 適用法の遵守

本 CPS の規定もしくは本 CPS に基づく運用が、日本国内法規の定めに抵触する可能性がある場合、日本国内法規による定めを優先する。

9.16. 雑則

9.16.1. 完全合意条項

本 CPS の規定は、当事者が、文書で本 CPS の特別規定となる旨を合意した場合を除き、口頭での追加、変更、削除、または終了させることはできない。

9.16.2. 権利譲渡条項

関係者は、本認証局が本 CPS で定めた権利および義務を、いかなる担保にも供してはならない。

9.16.3. 分離条項

本 CPS の一部または複数の条項が、何らかの事情によって無効化されたとしても、本 CPS における他の条項の有効性は失われないものとする。

9.16.4. 強制執行条項

規定しない。

9.16.5. 不可抗力条項

本認証局は次に掲げる事象または状況によって利用者、その他第三者（検証者を含むがこれに限らない）に損害が生じた場合でも、一切の責任を負わないものとする。

- 天災：火災、雷、噴火、洪水、地震、嵐、台風、津波、疫病等
- 人災：戦争、革命、暴動、内乱、テロ、労働争議等
- 裁判所、政府、行政、省庁等による作為、不作為、または命令等
- 電源の供給停止、回線の停止等、本認証局以外のシステムの停止
- 技術上若しくは運用上緊急に本認証局に係わるシステムを停止する必要があると本認証局が判断した場合
- 本認証局が、本 CPS に基づく義務を適切に履行したにも関わらず、不完全履行または履行遅滞を生じさせ、または、係る結果に至ることとなった事象若しくは状況
- その他本認証局の責に帰すべからざる事由

9.17. その他の条項

規定しない。

別紙 1　詳細プロファイル

【認証局証明書の詳細プロファイル】

(1) ルート認証局証明書の詳細プロファイル

No	フィールド	設定値	補足説明
1	version	v3	バージョン 3 を示す
2	serialNumber		自動生成
3	signature	sha256WithRSAEncryption	
	aigorithmIdentifier	1.2.840.113549.1.1.11	sha256withRSAEncryption を示す
4	issuer	CN=EINS/PKI for EDI Root Certificate Authority V2 OU=CA for manufactures and distributors and retailers O=INTEC Inc. C=JP	自己署名証明書
5	validity		20 年間
	notBefore	YYYYMMDDHHMMSS	
	notAfter	YYYYMMDDHHMMSS	
6	subject （主体者名）	CN=EINS/PKI for EDI Root Certificate Authority V2 OU=CA for manufactures and distributors and retailers O=INTEC Inc. C=JP	
7	subjectPublicKeyInfo		
	algorithm	1.2.840.113549.1.1.1	rsaEncryption を示す
	subjectPublicKey		自動生成

extention（拡張領域）				
No	フィールド	クリティカル	設定値	補足説明
1	authorityKeyIdentifier	FALSE		本ルート認証局証明書公開鍵のハッシュ値
	keyIdentifier			
2	subjectKeyIdentifier	FALSE		本証明書公開鍵のハッシュ値
3	keyUsage	TRUE	cRLSign keyCertSign	CRL の署名 証明書の署名
4	basicConstraints	FALSE	Subject Type=CA Path Length Constraint=1	

(2) 中間認証局証明書の詳細プロファイル

No	フィールド	設定値	補足説明
1	version	v3	バージョン 3 を示す
2	serialNumber		自動生成
3	signature	sha256WithRSAEncryption	
	aigorithmIdentifier	1.2.840.113549.1.1.11	sha256withRSAEncryption を示す
4	issuer	CN=EINS/PKI for EDI Root Certificate Authority V2 OU=CA for manufactures and distributors and retailers O=INTEC Inc. C=JP	
5	validity		20 年間
	notBefore	YYYYMMDDHHMMSS	
	notAfter	YYYYMMDDHHMMSS	
6	subject （主体者名）	CN=EINS/PKI for EDI Certificate Authority V2 OU=CA for manufactures and distributors and retailers O=INTEC Inc. C=JP	
7	subjectPublicKeyInfo		
	algorithm	1.2.840.113549.1.1.1	rsaEncryption を示す
	subjectPublicKey		自動生成

extention(拡張領域)				
No	フィールド	クリティカル	設定値	補足説明
1	authorityKeyIdentifier	FALSE		本ルート認証局証明書公開鍵のハッシュ値
	keyIdentifier			
2	subjectKeyIdentifier	FALSE		本証明書公開鍵のハッシュ値
3	keyUsage	TRUE	cRLSign keyCertSign	CRL の署名 証明書の署名
4	basicConstraints	FALSE	Subject Type=CA Path Length Constraint=1	

【利用者証明書の詳細プロファイル】

(1) 法人向けサーバ証明書の詳細プロファイル

No	フィールド	設定値	補足説明
1	version	v3	バージョン 3 を示す
2	serialNumber		自動生成
3	signature	sha256WithRSAEncryption	
	aigorithmIdentifier	1.2.840.113549.1.1.11	sha256withRSAEncryption を示す
4	issuer	CN=EINS/PKI for EDI Certificate Authority V2 OU=CA for manufactures and distributors and retailers O=INTEC Inc. C=JP	
5	validity		3 年間
	notBefore	YYYYMMDDHHMMSS	
	notAfter	YYYYMMDDHHMMSS	
6	subject （主体者名）	（下線は必須属性） CN= OU= O= L= S= C=JP	設定例 CN=www.einspki.jp OU=EINSPKI Support O=INTEC Inc. L=Koto-ku S=Tokyo C=JP
7	subjectPublicKeyInfo		
	algorithm	1.2.840.113549.1.1.1	rsaEncryption を示す
	subjectPublicKey		自動生成

extention(拡張領域)				
No	フィールド	クリティカル	設定値	補足説明
1	authorityKeyIdentifier	FALSE		本中間認証局証明書公開鍵のハッシュ値
	keyIdentifier			
2	subjectKeyIdentifier	FALSE		本証明書公開鍵のハッシュ値
3	keyUsage	TRUE	disitalSignature keyEncipherment dataEncipherment	電子署名 鍵暗号化 データ暗号化
4	extendedKeyUsage	FALSE	1.3.6.1.5.5.7.3.1 1.3.6.1.5.5.7.3.2 1.3.6.1.5.5.7.3.4	SSL/TLS サーバ認証 SSL/TLS クライアント認証 電子メールの保護
5	certificatePolicies	FALSE		
	policyIdentifier		1.2.392.200057.1.94401.2.1	本認証局の証明書ポリシー(OID)
	policyQualifiers			
	policyQualifierId		CPS	
	qualifier		https://www.einspki.jp/repository_files/EINSPKI_EDI_CPS.pdf	CP 公開 URL
6	subjectAltName	FALSE		
	DNS Name			例 www.einspki.jp
7	basicConstraints	FALSE	Subject Type=End Entity Path Length Constraint=None	
8	cRLDistributionPoints	FALSE		
	distributionPoint		http://www.einspki.jp/repository/crl/EINSPKI_EDI_V2.crl	CRL 配布先 URL

(2) 法人向けクライアント証明書の詳細プロファイル

No	フィールド	設定値	補足説明
1	version	v3	バージョン 3 を示す
2	serialNumber		自動生成
3	signature	sha256WithRSAEncryption	
	aigorithmIdentifier	1.2.840.113549.1.1.11	sha256withRSAEncryption を示す
4	issuer	CN=EINS/PKI for EDI Certificate Authority V2 OU=CA for manufactures and distributors and retailers O=INTEC Inc. C=JP	
5	validity		3 年間
	notBefore	YYYYMMDDHHMMSS	
	notAfter	YYYYMMDDHHMMSS	
6	subject （主体者名）	（下線は必須属性） E= CN= OU= O= L= S= C=JP	設定例 E=user@einspki.jp CN=User Name OU=EINSPKI Support O=INTEC Inc. L=Koto-ku S=Tokyo C=JP
7	subjectPublicKeyInfo		
	algorithm	1.2.840.113549.1.1.1	rsaEncryption を示す
	subjectPublicKey		自動生成

extention(拡張領域)				
No	フィールド	クリティカル	設定値	補足説明
1	authorityKeyIdentifier	FALSE		本中間認証局証明書公開鍵のハッシュ値
	keyIdentifier			
2	subjectKeyIdentifier	FALSE		本証明書公開鍵のハッシュ値
3	keyUsage	TRUE	disitalSignature keyEncipherment dataEncipherment	電子署名 鍵暗号化 データ暗号化
4	extendedKeyUsage	FALSE	1.3.6.1.5.5.7.3.2 1.3.6.1.5.5.7.3.4	SSL/TLS クライアント認証 電子メールの保護
5	certificatePolicies	FALSE		
	policyIdentifier		1.2.392.200057.1.94401.2.1	本認証局の証明書ポリシー(OID)
	policyQualifiers			
	policyQualifierId		CPS	
	qualifier		https://www.einspki.jp/repository_files/EINSPKI_EDI_CPS.pdf	CP 公開 URL
6	subjectAltName	FALSE		
	DNS Name			例 www.einspki.jp
7	basicConstraints	FALSE	Subject Type=End Entity Path Length Constraint=None	
8	cRLDistributionPoints	FALSE		
	distributionPoint		http://www.einspki.jp/repository/crl/EINSPKI_EDI_V2.crl	CRL 配布先 URL

(3) 個人事業主向けサーバ証明書の詳細プロファイル

No	フィールド	設定値	補足説明
1	version	v3	バージョン 3 を示す
2	serialNumber		自動生成
3	signature	sha256WithRSAEncryption	
	aigorithmIdentifier	1.2.840.113549.1.1.11	sha256withRSAEncryption を示す
4	issuer	CN=EINS/PKI for EDI Certificate Authority V2 OU=CA for manufactures and distributors and retailers O=INTEC Inc. C=JP	
5	validity		3 年間
	notBefore	YYYYMMDDHHMMSS	
	notAfter	YYYYMMDDHHMMSS	
6	subject （主体者名）	（下線は必須属性） CN= OU= O=Natural Person L= S= C=JP	設定例 CN=www.einspki.jp OU=User Name O=Natural Person L=Koto-ku S=Tokyo C=JP
7	subjectPublicKeyInfo		
	algorithm	1.2.840.113549.1.1.1	rsaEncryption を示す
	subjectPublicKey		自動生成

extention(拡張領域)				
No	フィールド	クリティカル	設定値	補足説明
1	authorityKeyIdentifier	FALSE		本中間認証局証明書公開鍵のハッシュ値
	keyIdentifier			
2	subjectKeyIdentifier	FALSE		本証明書公開鍵のハッシュ値
3	keyUsage	TRUE	disitalSignature keyEncipherment dataEncipherment	電子署名 鍵暗号化 データ暗号化
4	extendedKeyUsage	FALSE	1.3.6.1.5.5.7.3.1 1.3.6.1.5.5.7.3.2 1.3.6.1.5.5.7.3.4	SSL/TLS サーバ認証 SSL/TLS クライアント認証 電子メールの保護
5	certificatePolicies	FALSE		
	policyIdentifier		1.2.392.200057.1.94401.2.1	本認証局の証明書ポリシー(OID)
	policyQualifiers			
	policyQualifierId		CPS	
	qualifier		https://www.einspki.jp/repository_files/EINSPKI_EDI_CPS.pdf	CP 公開 URL
6	subjectAltName	FALSE		
	DNS Name			例 www.einspki.jp
7	basicConstraints	FALSE	Subject Type=End Entity Path Length Constraint=None	
8	cRLDistributionPoints	FALSE		
	distributionPoint		http://www.einspki.jp/repository/crl/EINSPKI_EDI_V2.crl	CRL 配布先 URL

(4) 個人事業主向けクライアント証明書の詳細プロファイル

No	フィールド	設定値	補足説明
1	version	v3	バージョン 3 を示す
2	serialNumber		自動生成
3	signature	sha256WithRSAEncryption	
	aigorithmIdentifier	1.2.840.113549.1.1.11	sha256withRSAEncryption を示す
4	issuer	CN=EINS/PKI for EDI Certificate Authority V2 OU=CA for manufactures and distributors and retailers O=INTEC Inc. C=JP	
5	validity		3 年間
	notBefore	YYYYMMDDHHMMSS	
	notAfter	YYYYMMDDHHMMSS	
6	subject （主体者名）	（下線は必須属性） E= CN= OU= O=Natural Person L= S= C=JP	設定例 E=user@einspki.jp CN=User Name OU=EINSPKI Support O=Natural Person L=Koto-ku S=Tokyo C=JP
7	subjectPublicKeyInfo		
	algorithm	1.2.840.113549.1.1.1	rsaEncryption を示す
	subjectPublicKey		自動生成

extention(拡張領域)				
No	フィールド	クリティカル	設定値	補足説明
1	authorityKeyIdentifier	FALSE		本中間認証局証明書公開鍵のハッシュ値
	keyIdentifier			
2	subjectKeyIdentifier	FALSE		本証明書公開鍵のハッシュ値
3	keyUsage	TRUE	disitalSignature keyEncipherment dataEncipherment	電子署名 鍵暗号化 データ暗号化
4	extendedKeyUsage	FALSE	1.3.6.1.5.5.7.3.2 1.3.6.1.5.5.7.3.4	SSL/TLS クライアント認証 電子メールの保護
5	certificatePolicies	FALSE		
	policyIdentifier		1.2.392.200057.1.94401.2.1	本認証局の証明書ポリシー(OID)
	policyQualifiers			
	policyQualifierId		CPS	
	qualifier		https://www.einspki.jp/repository_files/EINSPKI_EDI_CPS.pdf	CP 公開 URL
6	subjectAltName	FALSE		
	RFC822 Name			例 user@einspki.jp
7	basicConstraints	FALSE	Subject Type=End Entity Path Length Constraint=None	
8	cRLDistributionPoints	FALSE		
	distributionPoint		http://www.einspki.jp/repository/crl/EINSPKI_EDI_V2.crl	CRL 配布先 URL

【CRL の詳細プロファイル】

(1) CRL の詳細プロファイル

No	領域名	フィールド	設定値	クリティカル	補足説明
1	CRL 基本領域	version	v2		バージョン 2 を示す
2		signature	1.2.840.113549.1.1.11		sha1withRSAEncryption を示す
3		issuer	CN= OU= O=INTEC Inc. C=JP		本認証局の名称
4		thisUpdate	YYYYMMDDHHMMSS		CRL 更新日時
5		nextUpdate	YYYYMMDDHHMMSS		次回更新日時
6*		revokedCertificates			失効した利用者証明書のリスト
7*		userCertificate			失効した利用者証明書のシリアル番号
8*		revocationDate	YYYYMMDDHHMMSS		失効処理が行われた日時
9		crlExtensions (No.12～13)			CRL 拡張領域
10	CRL エントリ拡張領域	reasonCode		FALSE	失効事由
11	CRL 拡張領域	authorityKeyIdentifier		FALSE	本認証局公開鍵のハッシュ値
12		cRLNumber		FALSE	CRL 番号

＊ No.6～8 の値は、失効された利用者証明書ごとの情報が記載される。

別紙 2 用語集

No.	用語	意味
1	CP	Certificate Policy（証明書ポリシー）。 認証局が証明書を発行する際の運用方針を定めた文書。
2	CPS	Certification Practice Statement（認証業務運用規程）。認証局の信頼性、安全性を対外的に示すために、認証局の運用、証明書ポリシー、鍵の生成・管理、責任等に関して定めた文書。
3	CRL	Certification Practice Statement（認証業務運用規程）。認証局の信頼性、安全性を対外的に示すために、認証局の運用、証明書ポリシー、鍵の生成・管理、責任等に関して定めた文書。
4	FIPS 140-2	米国 NIST(National Institute of Standards and Technology)が策定した米国連邦情報処理標準。暗号モジュールが満たすべきセキュリティ要件等について定めている。
5	FQDN	Fully Qualified Domain Name（完全に条件付けられたホスト名）。インターネット上でホストを唯一に識別するために設定される。
6	GDS	Global Data Synchronization（商品情報同期化）。
7	PKCS#10	PKCSとは旧米国RSA Data Security社（現在、米国EMC社）による公開鍵暗号方式を実現するための技術標準。その1つであるPKCS #10は、証明書発行要求メッセージの構文に関する規格。 IETFにおいてRFC2986として規定されている。
8	PKI	Public Key Infrastructure（公開鍵基盤）。公開鍵暗号方式を基盤としたセキュリティ技術基盤、環境の総称。
9	認証局秘密鍵	認証局が所有する秘密鍵。証明書または CRL の作成に利用される。