

JPCERT/CC

SSL クライアント証明書用認証局

認証業務運用規程

Ver 1.2

改訂履歴

Version	変更内容	日付
1.0	新規作成	2006年7月12日
1.1	2-3 および 4-9-7 の GRL 発行頻度の記載を変更 1-6 の JVN の説明記載を変更	2008年6月26日
1.2	法人名称中の「有限責任中間法人」を「一般社団法人」に変更	2009年11月2日

1.	はじめに	8
1-1.	概要	8
1-2.	文書の名前と識別	8
1-3.	PKIの関係者	8
1-3-1.	認証局	9
1-3-2.	登録局	10
1-3-3.	利用者	10
1-3-4.	信頼者	10
1-3-5.	その他の関係者	10
1-4.	証明書の利用方法	10
1-4-1.	適切な証明書の利用方法	10
1-4-2.	禁止される証明書の利用方法	10
1-5.	ポリシー管理	10
1-5-1.	CPSを管理する組織	11
1-5-2.	CPSに関する連絡窓口	11
1-5-3.	CPSのCPへの適合性を判断する人物	11
1-5-4.	CPSの承認手続き	11
1-6.	定義と略語	11
2.	認証局に関する情報の公表とリポジトリの責任	17
2-1.	リポジトリ	17
2-2.	認証局に関連する情報の公表	17
2-3.	公表の頻度	17
2-4.	リポジトリへのアクセス管理	17
3.	識別及び認証	18
3-1.	名称決定	18
3-1-1.	名称の形式	18
3-1-2.	名称の意味	18
3-1-3.	利用者の匿名性または仮名性	19
3-1-4.	名称の変換ルール	19
3-1-5.	名称の唯一性	19
3-1-6.	商標に関する扱い	19
3-2.	証明書初回発行時の識別及び認証	20
3-2-1.	秘密鍵の所有を証明する方法	20
3-2-2.	組織の識別及び認証	20
3-2-3.	個人の識別及び認証	20
3-2-4.	確認しない個人の情報	21

3-2-5. 役職等の確認方法.....	21
3-2-6. 相互運用の基準.....	22
3-3. 証明書更新時または再発行時の識別及び認証.....	22
3-3-1. 証明書更新時の識別及び認証.....	22
3-3-2. 証明書失効後における再発行時の識別及び認証.....	22
3-4. 失効申請時の識別及び認証.....	22
4. 証明書のライフサイクルに関わる運用要件.....	23
4-1. 証明書申請.....	23
4-1-1. 証明書申請を行える者.....	23
4-1-2. 登録手続き及び責任.....	23
4-2. 証明書申請手続き.....	23
4-2-1. 本人識別と認証の実施.....	23
4-2-2. 証明書申請の承認または却下.....	24
4-2-3. 証明書申請の処理時間.....	24
4-3. 証明書発行.....	24
4-3-1. 証明書の発行時における認証局の処理.....	24
4-4. 証明書受領時の処理.....	24
4-4-1. 証明書の受領確認.....	24
4-5. 鍵ペアと証明書の利用用途.....	24
4-6. 証明書の更新.....	24
4-6-1. 証明書の更新が行われる場合.....	24
4-6-2. 証明書の更新を申請できる者.....	25
4-6-3. 証明書の更新申請の処理.....	25
4-6-4. 利用者に対する新しい証明書の通知.....	25
4-6-5. 更新された証明書の受領確認.....	25
4-6-6. 認証局による更新された証明書の公開.....	25
4-6-7. 認証局による更新された証明書の通知.....	25
4-7. 鍵ペア更新による証明書の更新.....	25
4-8. 証明書の内容の変更による更新.....	25
4-9. 証明書の失効と一時停止.....	25
4-9-1. 証明書失効の場合.....	26
4-9-2. 証明書失効を申請することができる者.....	26
4-9-3. 失効申請手続き.....	26
4-9-4. 失効申請の猶予期間.....	26
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.....	26
4-9-6. 信頼者の失効情報の調査要件.....	26
4-9-7. CRL発行頻度.....	26
4-9-8. CRLの発行最大遅延時間.....	27

4-9-9.	オンラインでの失効/ステータス確認の適用性	27
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	27
4-9-11.	利用可能な失効通知の他の形式	27
4-9-12.	鍵危殆化による失効時の特別要件	27
4-9-13.	証明書の一時的停止が行われる状況	27
4-9-14.	証明書の一時的停止を要求できる者	27
4-9-15.	証明書の一時的停止要求の手続き	27
4-9-16.	証明書の一時的停止を継続できる期間	27
4-10.	証明書ステータス確認サービス	27
4-11.	利用者の本サービス利用の停止	28
4-12.	鍵預託と鍵の回復	28
5.	物理的管理、運営上の管理、運用上の管理	29
5-1.	物理的管理	29
5-1-1.	施設の立地場所及び構造	29
5-1-2.	施設内の物理的アクセス	29
5-1-3.	電源及び空調	29
5-1-4.	水害	29
5-1-5.	火災防止及び火災保護対策	30
5-1-6.	媒体保管場所	30
5-1-7.	廃棄処理	30
5-1-8.	施設外のバックアップ	30
5-2.	手続的管理	30
5-2-1.	信頼すべき役割	30
5-2-2.	職務ごとに必要とされる人数	31
5-2-3.	職務実施時の本人識別と認証	31
5-2-4.	職務分割が要求される役割	31
5-3.	人事的管理	32
5-4.	監査ログに関する手続き	32
5-4-1.	記録されるイベントの種類	32
5-4-2.	監査ログを確認する頻度	33
5-4-3.	監査ログを保持する期間	33
5-4-4.	監査ログの保護方法	33
5-4-5.	監査ログのバックアップ手法	33
5-4-6.	監査ログの収集方法	33
5-4-7.	イベントを引き起こした対象に対する通知	33
5-4-8.	脆弱性評価	33
5-5.	記録の長期保管	33
5-5-1.	長期保管する記録の種類	33

5-5-2.	記録を長期保管する期間.....	34
5-5-3.	長期保管する記録の保護方法.....	34
5-5-4.	長期保管する記録のバックアップ手続き.....	35
5-5-5.	長期保管する記録へのタイムスタンプ.....	35
5-5-6.	長期保管する記録の収集方法.....	35
5-5-7.	長期保管する記録の可読性、完全性確認.....	35
5-6.	認証局秘密鍵の切替.....	35
5-7.	危殆化及び災害からの復旧.....	35
5-7-1.	事故及び災害からの復旧.....	35
5-7-2.	コンピュータ資源、ソフトウェア、または、データが破壊された場合.....	35
5-7-3.	利用者の秘密鍵が危殆化した場合の手続き.....	35
5-7-4.	被災後の事業継続能力.....	36
5-8.	認証業務の終了.....	36
6.	技術的セキュリティ管理.....	37
6-1.	鍵ペアの生成及びインストール.....	37
6-1-1.	鍵ペアの生成.....	37
6-1-2.	利用者に対する秘密鍵の交付.....	37
6-1-3.	認証局に対する公開鍵の交付.....	37
6-1-4.	信頼者に対する認証局の公開鍵の送付.....	37
6-1-5.	鍵サイズ.....	37
6-1-6.	鍵生成に利用するパラメータの生成及び品質検査.....	37
6-1-7.	鍵の利用用途.....	37
6-2.	秘密鍵の保護及び暗号モジュール技術の管理.....	38
6-2-1.	暗号モジュールの標準及び管理.....	38
6-2-2.	秘密鍵の複数人による管理.....	38
6-2-3.	秘密鍵の預託.....	38
6-2-4.	秘密鍵のバックアップ.....	38
6-2-5.	秘密鍵の長期保管.....	38
6-2-6.	秘密鍵の暗号モジュールへの格納及び取出.....	38
6-2-7.	秘密鍵の暗号モジュール内での格納形式.....	38
6-2-8.	秘密鍵の活性化方法.....	39
6-2-9.	秘密鍵の非活性化方法.....	39
6-2-10.	秘密鍵の破棄方法.....	39
6-2-11.	暗号モジュールの評価.....	39
6-3.	その他の鍵ペア管理について.....	39
6-3-1.	公開鍵の長期保管.....	39
6-3-2.	証明書使用期間及び鍵ペア使用期間.....	39
6-4.	活性化データ.....	39

6-4-1.	活性化データの生成及び設定	39
6-4-2.	活性化データの保護	39
6-5.	コンピュータセキュリティ管理	40
6-5-1.	特定のコンピュータのセキュリティに関する技術的要件	40
6-5-2.	コンピュータセキュリティの評価	40
6-6.	ライフサイクルの技術上の管理	40
6-6-1.	システム開発時の管理	40
6-6-2.	システム運用時の管理	40
6-6-3.	ライフサイクルセキュリティ管理	40
6-7.	ネットワークセキュリティ管理	40
6-8.	タイムスタンプ	41
7.	証明書及びCRLプロファイル	42
7-1.	証明書のプロファイル	42
7-2.	CRLのプロファイル	45
7-3.	OCSPのプロファイル	45
8.	準拠性監査とその他の評価	46
8-1.	監査の頻度	46
8-2.	監査人の身元または資格	46
8-3.	監査人と被監査人の関係	46
8-4.	監査項目	46
8-5.	監査指摘事項に対する処置	46
8-6.	監査結果の公表	46
9.	その他の業務上及び法的問題	47
9-1.	料金	47
9-2.	財務的責任	47
9-3.	秘密として扱う情報の保護	47
9-3-1.	秘密として扱う情報の範囲	47
9-3-2.	秘密として扱わない情報の範囲	47
9-3-3.	秘密として扱う情報を保護する責任	48
9-4.	個人情報の保護	48
9-4-1.	個人情報保護方針	48
9-4-2.	個人情報の定義	48
9-4-3.	個人情報として扱われない情報	48
9-4-4.	個人情報を保護する責任	48
9-4-5.	個人情報の利用に関する通知と同意	49
9-4-6.	司法手続きまたは行政手続による個人情報の開示	49

9-5. 知的財産権	49
9-6. 表明保証	49
9-6-1. 認証局の表明保証.....	49
9-6-2. 登録局の表明保証.....	49
9-6-3. 利用者の表明保証.....	50
9-6-4. 信頼者の表明保証.....	50
9-6-5. その他の関係者の表明保証.....	50
9-7. 保証の対象外	50
9-8. 責任の制限	50
9-9. 補償	51
9-10. 有効期間と終了.....	51
9-10-1. 有効期間.....	51
9-10-2. 終了	51
9-10-3. 終了によって無効化される事項、及び継続する事項.....	51
9-11. 関係者間の連絡方法.....	52
9-12. CPSの改訂.....	52
9-12-1. CPSの改訂手続き.....	52
9-12-2. CPSの改訂通知方法及び実施時期.....	52
9-12-3. オブジェクト識別子に変更される条件.....	52
9-13. 紛争解決手続.....	52
9-14. 準拠法.....	52
9-15. 適用法の遵守.....	53
9-16. 雑則.....	53
9-16-1. 完全合意条項.....	53
9-16-2. 権利譲渡条項.....	53
9-16-3. 分離条項.....	53
9-16-4. 強制執行条項.....	53
9-16-5. 不可抗力条項.....	53
9-17. その他の条項.....	53

1. はじめに

1-1. 概要

本書は一般社団法人 JPCERT コーディネーションセンター（以下「JPCERT/CC」という）が運営する JPCERT/CC SSL クライアント証明書用認証局（以下「本認証局」という）の認証業務運用規程（Certification Practice Statement、以下「本 CPS」という）です。本 CPS は本認証局が証明書の発行、管理、失効及び更新を含む一連のサービスを提供する際に実施する手順を記載したものです。これらのサービスを JPCERT/CC SSL クライアント証明書発行サービス（以下「本サービス」という）と呼びます。本サービスは、JPCERT/CC が管理する JVN ベンダステータス情報収集システムと製品開発者がインターネットを經由して安全に通信を行うための仕組みを提供します。

本認証局が発行する証明書の利用用途は SSL クライアント認証に制限されますが、JPCERT/CC では今後、S/MIME 用の証明書を発行する認証局の構築を行うことや、他の認証機関との相互接続を実施することも検討しています。（実施を保証するものでもありません。）

なお、本 CPS は、IETF の PKIX WG において標準化されている「証明書ポリシーと認証実践の枠組み (Certificate Policy and Certification Practices Framework)」(RFC3647) の構成に従い、記述されています。

1-2. 文書の名前と識別

本認証局に関連するオブジェクト識別子 (OID) は表 1 の通りです。

表 1 OID の割当

OID	対象
1. 2. 392. 200212	一般社団法人 JPCERT コーディネーションセンター
1. 2. 392. 200212. 1	JPCERT/CC 証明書発行サービス
1. 2. 392. 200212. 1. 1	JPCERT/CC SSL クライアント証明書用認証局
1. 2. 392. 200212. 1. 1. 1	JPCERT/CC SSL クライアント証明書用認証局 CPS

1-3. PKI の関係者

図 1 に本サービスの参加者を示します。参加者は認証局、登録局、利用者及び信頼者から構成されます。また、情報を公開するための機関としてリポジトリが存在します。本認証局の階層構造については、図 2 の通りです。

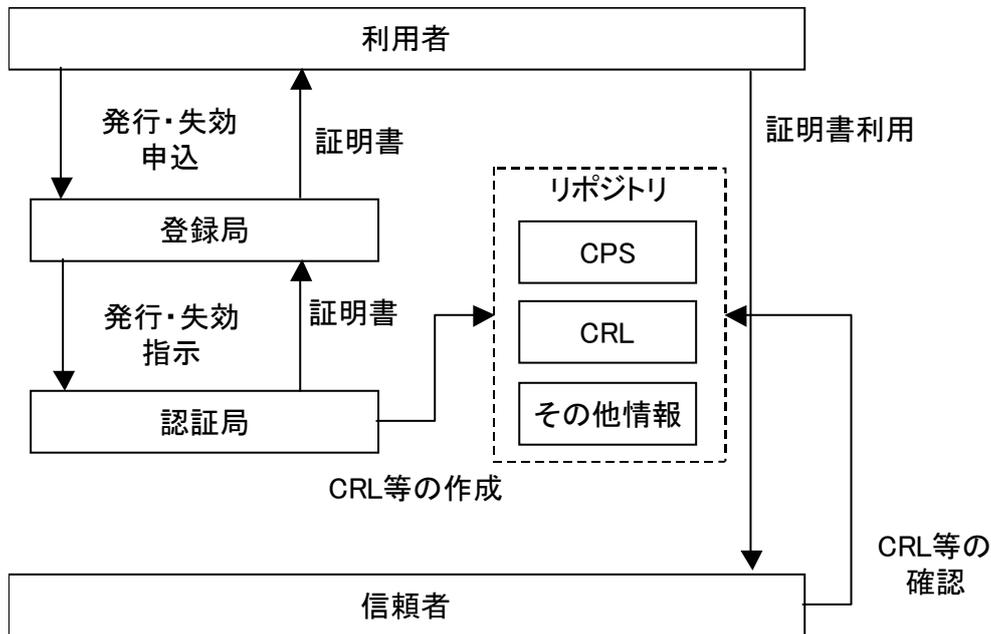


図 1 参加者の構造

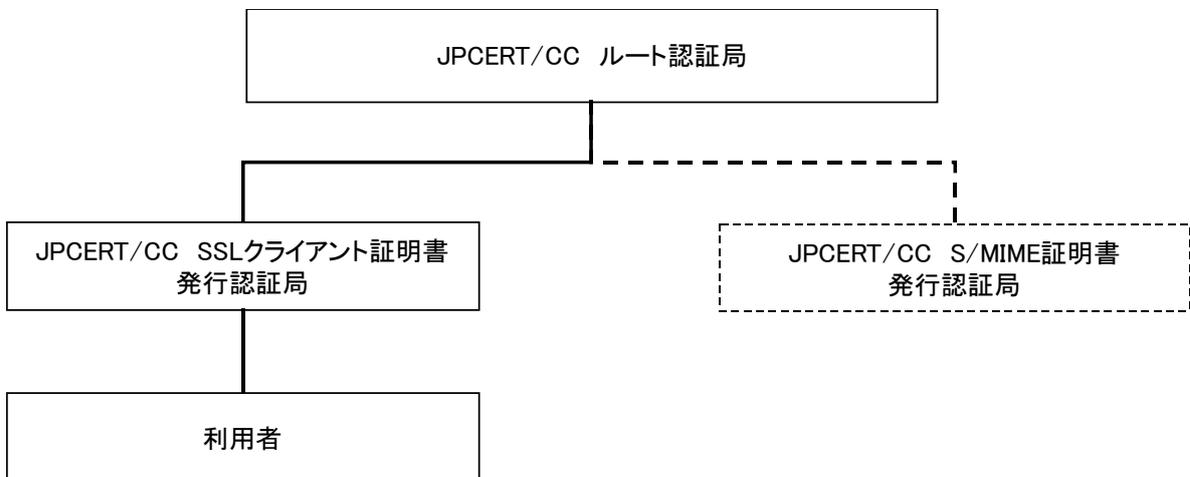


図 2 認証局の階層構造

1-3-1. 認証局

本 CPS において、特別な修飾を伴わずに「認証局」と記述されている場合、認証局は登録局の指示にもとづき、証明書発行及び失効を行うための機関を指します。また、認証局は CRL や CPS の作成を行い、リポジトリ上に公開します。

1-3-2. 登録局

登録局は、本 GPS に従い証明書の発行申請及び失効申請の真偽の確認を行います。登録局は、十分な審査を行った上で認証局に対し証明書の発行指示及び失効指示を行います。

1-3-3. 利用者

利用者は、証明書を本認証局から取得し、証明書に記載された（証明書で証明された）公開鍵と対になる秘密鍵を管理します。本サービスにおける利用者は、製品開発者の中で本認証局より証明書の発行を受ける者が相当します。利用者は、JVN ベンダステータス情報収集システムに、自身の秘密鍵と本認証局が発行した証明書を利用し、SSL クライアント認証を受けることで、アクセスすることが可能になります。

1-3-4. 信頼者

信頼者は本認証局が発行した証明書に記載された公開鍵を使用して利用者の認証を行います。本サービスにおける信頼者は、JVN ベンダステータス情報収集システムが相当します。

1-3-5. その他の関係者

規定しません。

1-4. 証明書の利用方法

本節では本認証局が発行する証明書が利用される範囲について規定します。

1-4-1. 適切な証明書の利用方法

JPCERT/CC は本認証局が発行した証明書の利用用途を以下のように指定します。指定された用途以外では、利用者は証明書を利用してはなりません。

「利用者が管理するクライアント端末から JVN ベンダステータス情報収集システムにインターネットを経由して接続する際の、SSL 通信のクライアント認証のための証明書」

1-4-2. 禁止される証明書の利用方法

本認証局は 1-4-1 項で明確に規定されている用途以外の証明書の利用を禁止します。利用者はいかなる理由においても、JVN ベンダステータス情報収集システム以外において、本認証局が発行した証明書を利用してはなりません。

1-5. ポリシー管理

本節では本 GPS の管理方法について規定します。

1-5-1. CPS を管理する組織

本 CPS の管理部署は以下の通りです。

- ◆ 『組織名称』：一般社団法人 JPCERT コーディネーションセンター
- ◆ 『担当部署』：認証局運用担当窓口

1-5-2. CPS に関する連絡窓口

本 CPS に関する問い合わせ窓口及び、その連絡先は以下の URL で公開されています。

- ◆ 『問い合わせ窓口及び連絡先』：<http://www.jpCERT.or.jp/ca-info/contact.html>

1-5-3. CPS の CP への適合性を判断する人物

規定しません。

1-5-4. CPS の承認手続き

規定しません。

1-6. 定義と略語

本CPSで使用する用語の定義は表 2の通りです。

表 2 用語の定義

用語	用語の意味
【A - Z】	
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。
CPS	Certificate 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。 証明書ポリシーが何を運用方針にするのかを示すのに対して、認証業務運用規程は運用方針をどのように実施するのかを示す。
CRL	Certificate Revocation List (証明書失効リスト)。 失効が行われた証明書のリスト。認証機関の電子署名が付され、定期的に(または緊急に)発行される。通常このリストには、 ① 証明書失効リスト発行者の名称 ② 発行日 ③ 次の証明書失効リスト発行予定日 ④ 効力が停止されまたは破棄された証明書のシリアル番号

	等が記載される。
FIPS 140-1 (Federal Information Processing Standard)	<p>NIST (National Institute of Standards and Technology : 米国標準技術研究所) が策定した米国連邦情報処理標準のうち、暗号技術に関するセキュリティ要件を規定しているもの。</p> <p>以下のようなレベルが規定されている。</p> <p>レベル1 : FIPSで定義している最低限のセキュリティレベル。一般的なPCに適用されているような暗号モジュールに適用されているレベル。</p> <p>レベル2: 暗号化モジュールに、不正アクセスされた場合に、侵入の痕跡を残せるような仕組みを備えているレベル。</p> <p>レベル3: 暗号化モジュールに、不正アクセスされた場合に、侵入の痕跡を残せるような仕組みを備えている。レベル2に比べ、痕跡をより厳密に追跡できるような仕組みを備えているレベル。特殊なハードウェア装置を使い、侵入があった場合にはデータを消去するような仕組みをもつ。</p> <p>レベル 4 : FIPS で定義されている最高のセキュリティレベル。温度の変化や電流の変化等の環境の変動も検知できるような仕組みを導入しているレベル。</p>
HSM (Hardware Security Module : ハードウェアセキュリティモジュール)	<p>ハードウェアによる秘密鍵の管理装置。</p> <p>不正アクセスに備えるための機能(耐タンパ機能)を保有した秘密鍵の管理装置。</p> <p>耐タンパ機能とは不正アクセスに対してその侵入の痕跡を残したり、データを消去する機能であり、不正アクセスの証拠を残す不正顕示機能、不正アクセスからデータを防護する不正防護機能、不正アクセスに対してデータを消去する対抗動作を行う不正対抗機能等がある。</p> <p>【暗号モジュール】と同義。</p>
JVN	Japan Vulnerability Notes の略。経済産業省告示「ソフトウェア等脆弱性関連情報取扱基準」を受けて、日本国内の製品開発者の脆弱性対応状況を公開するサイトのこと。
JVN ベンダステータス情報収集システム	JVN に掲載する製品開発者からの提供情報を、製品開発者自ら入力できるシステムのこと。
OCSP	Online Certificate Status Protocol : リアルタイムで証明書の状態を確認するためのプロトコル。OCSP サーバへのステー

	タス要求と応答からなる。IETF 勧告 (RFC2560) を参照。
OID (Object Identification : オブジェクト識別子)	世界で一意となる値による識別子。登録機関 (ISO、ITU) に登録される。PKIで使うアルゴリズム、証明書内に格納する名前 (subject) のタイプ (Country名等の属性) 等は、オブジェクト識別子として登録されているものが使用される。
PKCS (Public Key Cryptography Standards) #10	PKCSとは、米国RSA Data Security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 (Certification Request Syntax Standard) に関する規格。 IETFにおいてRFC2986として規定されている。
PKI	Public Key Infrastructure の略。 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。
RFC	Request for Comments の略。 インターネット上の標準勧告をおこなう IETF (Internet Engineering Task Force) の勧告。
RSA	公開鍵暗号方式の暗号アルゴリズムの1つ。十分に大きな2つの異なる素数を掛け合わせた整数の素因数分解が困難であることを基盤に暗号アルゴリズムが設計されている。
SSL	Secure Socket Layer。Netscape 社が開発したトランスポート層セッションセキュリティ。 SSLはIETFにおいて改版されRFC2246 (TLS : Transport Layer Security) 勧告として採用された。
X. 500 識別名 (DN : DistinguishedName)	X. 500とは、名前及びアドレスの調査から属性による検索まで広範囲なサービスを提供することを目的にITUが開発したディレクトリ標準。X. 500識別名は、X. 509の証明書での発行者識別名称及び利用者識別名称に使用される。
X. 509	ITUによって策定された証明書の書式や失効リストに関する標準勧告。証明書、失効リストのフォーマットに加え、権限管理や相互認証に関する規定も行われている。
【あ - ん】	
アルゴリズム	計算や問題を解決するための手順、方式。
暗号	①データの機密性を確保するため、これを別のフォームに変換し、適切な暗号アルゴリズムと鍵を持つ者だけが再変換して元のデータを復元できるようにするために用いる数理科学。 ② 情報の内容を隠し、検知されない改変を不可能にし、無断

	使用を妨げる目的でデータを変換するための原理、手段及び方法を体現する規則。
暗号モジュール	【HSM】参照。
改ざん（改竄）	データの内容を書き換えられること。
鍵サイズ	暗号の強度を決定する要素の1つ。鍵の長さをビット数で表したものが鍵サイズであり、鍵サイズが大きいほど暗号の強度は増す。
鍵ペア（鍵対）	公開鍵暗号方式のアルゴリズムで利用される秘密鍵と公開鍵のペア。
活性化	システム、装置等を使用可能な状態にすること。
活性化データ	システム、装置等を活性化するために必要となるデータ（パスワード等）。
監査	管理が十分と行われており、かつ、その目的に照らして適切であることを確認するために使用される手続。情報システムへの侵入またはその誤用を検知するための、記録、解析作業を含む。監査により発見された不適切な点は、担当の管理職員に報告される。
完全性	無権限でデータが改ざんされたり、破壊されていない状態。
共通鍵	発信者と受信者が同一の暗号鍵を使用してデータの暗号化と復号化を行う対称暗号方式 (symmetric cryptographic algorithm) における鍵。
機密性	機密を要するデータの秘密が保持され、権限を付与された人たちに対してだけ開示される状態。
検証	ある電子署名または証明書について、当該電子署名または証明書の有効性を確認すること。
公開鍵暗号方式	メッセージを暗号化した鍵と異なる鍵を用いて、暗号化されたメッセージを復号する暗号方式。代表的なものにRSA暗号方式がある。
公開鍵基盤	【PKI】参照。
公開鍵	公開鍵暗号方式における鍵ペアのうちの一つで、通信相手等の他人に知らせて利用してもらうための鍵。
更新（Renewal）	現在の証明書の有効期間の終了に伴い、同一の対象につき、同一種類の証明書を取得するための手続。
コンピュータセキュリティ	権限に基づかないアクセスや、制御機能の消失またはその他の影響から保護されている状態。 絶対的な安全保護は現実には有り得ず、実際の安全システムの

	有効性は相対的なものに留まる。状態モデルに基づく安全システムの場合、セキュリティとは、種々の操作の下で一定の「状態」が保持されることを意味する。
再発行	現在の証明書が失効した後に、同一の対象につき、同一種類の証明書を発行するための手続。
失効	ある特定の日時以降永久に証明書の有効期間を終了させる手続。
証明書チェーン	証明書は上位認証局の秘密鍵によって署名されるが、この署名は上位認証局の証明書に記載された公開鍵によって検証が可能となる。このために証明書を検証するためには上位認証局の証明書が常に必要となり、これはトラスタンカ認証局証明書（通常はルート認証局の自己署名証明書）まで連鎖的に必要となる。この連鎖を証明書チェーンと呼び、署名の連鎖を検証することを「証明書のチェーン検証」と呼ぶ。
自己署名証明書	自らの公開鍵に対して、自らの秘密鍵で署名した証明書。
信頼者	本認証局が発行した証明書を検証する人、または、機関。
製品開発者	ソフトウェア製品を開発した者、もしくは、ソフトウェア製品の開発、加工、輸入または販売に関する形態その他の事情からみて、当該ソフトウェア製品の実質的な開発者と認められる者。
製品開発者リスト	国内での脆弱性関連情報の円滑な流通を目的とした経済産業省告示「ソフトウェア等脆弱性関連情報取扱基準」に基づき、JPCERT/CC が整備している製品開発者のリストのこと。
セキュリティ	安全な状態。特に指定がない限りコンピュータセキュリティを示す。
タイムスタンプ	信頼できる時刻管理システムによって管理される時刻を基に、ログ等に記録される事象の発生時刻を示す値。 時刻情報の完全性を保証するために電子署名などによる暗号処理がなされる。
証明書	認証対象者の識別情報と公開鍵とが対応していることを証明するデジタルデータ。 ① 発行者の識別名 ② 利用者の識別名 ③ 利用者の公開鍵情報 ④ 有効期間 ⑤ シリアル番号

	などの情報を含み、これに発行者の電子署名が付される。
電子署名	公開鍵暗号方式の秘密鍵を利用した、メッセージの完全性を保証する仕組み。代表的な方法としては、メッセージの送信者が保有する秘密鍵でメッセージのハッシュ値を暗号化し、このデータをメッセージに付与する。メッセージの受信者は、署名者の公開鍵を用いて、送信者の本人確認及びメッセージの改ざん検知を行う。
認証	人の同一性を確認、またはある情報の完全性を証明するために用いられる手続。
リポジトリ (Repository)	証明書や失効リスト等を保管し、証明書の利用者等に対してこれらの開示や配布もしくは検索等のサービスを提供するシステム。ディレクトリシステムと呼ばれる場合がある。
パスワード (パス・フレーズ、暗証番号)	認証のための秘密の情報。通常は、コンピュータ資源 (メモリなど) にアクセスすることを可能にする一連の文字列で成り立っている。
ハッシュ関数	異なる2つの入力値から同じ出力値を算出したり、出力値から入力値を逆算することが困難な関数。SHA-1, MD5といった関数が主に用いられる。
ハッシュ値	ある値に対するハッシュ関数の出力値。
非活性化	システム、装置等を使用不可能な状態にすること。
秘密鍵	公開鍵暗号方式における鍵ペアのうちの一つで、他人には知られないように秘密にしておく鍵。
秘密鍵の預託	秘密鍵を第三者に預けること。
プロファイル	証明書、及び、CRLのデータ構造、記載内容を定義したもの。
ポリシー (Policy)	方針や規定、基準。
危殆化 (Compromise)	秘密鍵やその他の機密情報が、盗難や漏洩、第三者による解読等によってその機密性を失ったか、あるいはその可能性があること。
ルート認証局 (Root CA)	【証明書チェーン】参照。
ログ	コンピュータシステムや、アクセス制御システムにおいて発生する処理の履歴。運用手続きにおける記録を含む場合もある。

2. 認証局に関する情報の公表とリポジトリの責任

2-1. リポジトリ

JPCERT/CC は、本認証局の運営を円滑に行うことを目的として、本認証局に関わる情報を提供するためのリポジトリを運営します。リポジトリは、原則的に 365 日 24 時間の間、運用されます。ただし、システムの保守などの場合には、予め通知の上、リポジトリの運用を一時停止することがあります。なお、緊急時等のやむを得ない場合は、事前に連絡できないことがあります。

2-2. 認証局に関連する情報の公表

JPCERT/CC はリポジトリ上において以下の情報を公開します。

- ◆ 『本 CPS』 : <http://www.jpcert.or.jp/ca-info/jpcert-cps.pdf>
- ◆ 『CRL』 : <http://www.jpcert.or.jp/ca-info/crl-list.crl>
- ◆ 『本認証局に関する通知』 : <http://www.jpcert.or.jp/ca-info/index.html>

2-3. 公表の頻度

リポジトリ上に公表される情報の更新頻度は以下の通りとします。

- ◆ 『本 CPS』 : 改訂の都度
- ◆ 『CRL』 : 24 時間に一度以上
- ◆ 『本認証局に関する通知』 : 必要に応じて随時

2-4. リポジトリへのアクセス管理

リポジトリで公開する情報は、2-2節で規定された通りに、インターネットを通じて提供が行われます。JPCERT/CCは、リポジトリ上の情報の参照に関するアクセス制限を行いません。ただし、JPCERT/CCはリポジトリへの情報の書き込みをJPCERT/CC以外の者が行うことは認めません。

3. 識別及び認証

3-1. 名称決定

本節では各参加者の名称の決定ルールについて規定します。

3-1-1. 名称の形式

本認証局が発行する証明書の発行者名及び利用者名は、X.500 識別名の形式に従って設定されます。

3-1-2. 名称の意味

発行者及び利用者の名称は以下の通りです。

表 3 JPCERT/CC ルート認証局

属性	値	説明
countryName	“jp”	日本
organizationName	“Japan Computer Emergency Response Team Coordination Center”	JPCERT/CC の英語名
commonName	“JPCERT/CC Root CA”	JPCERT/CC ルート認証局の英語名

表 4 JPCERT/CC SSL クライアント証明書発行認証局

属性	値	説明
countryName	“jp”	日本
organizationName	“Japan Computer Emergency Response Team Coordination Center”	JPCERT/CC の英語名
commonName	“JPCERT/CC CA for SSL Clients”	JPCERT/CC SSL クライアント証明書発行認証局の英語名

表 5 利用者

属性	値	説明
organizationName	“Japan Computer Emergency Response Team Coordination Center”	JPCERT/CC の英語名
organizationalUnitName	“JPCERT/CC CA for SSL Clients”	JPCERT/CC SSL クライアント証明書発行認証局の英語名
commonName	“SSL-999999-999999-9999a”	ハイフン(-)で区切られる cn の第 1 カラムは、証明書利用目的である SSL クライアント認証の略称を示した文字列。同第 2 カラムは、JPCERT/CC が製品開発者に対して割り当てる 6 桁の数字。同第 3 カラムは、JPCERT/CC が製品開発者内の個人に割り当てる 6 桁の数字。同第 4 カラムは、証明書取得年度及び、年度内の取得回数を表す 5 桁の文字列です。

3-1-3. 利用者の匿名性または仮名性

本認証局が発行する証明書内に記載される利用者の名称は、3-1-2項で規定した通り、JPCERT/CCが任意に割り当てる、利用者の名称に関する情報を含まない文字列によって構成されています。

3-1-4. 名称の変換ルール

各参加者の名称は 3-1-2項で規定された内容に従い決定されます。

3-1-5. 名称の唯一性

各参加者の名称は 3-1-2項で規定された内容に従い決定されます。このため、本認証局は各参加者間の名称が一致することを想定しません。

3-1-6. 商標に関する扱い

各参加者の名称は 3-1-2項で規定された内容に従い決定されます。このため本認証局は、

各参加者の名称にJPCERT/CC以外の者の商標が証明書内に含まれることを想定しません。

3-2. 証明書初回発行時の識別及び認証

本節では製品開発者が証明書を初めて取得する際の認証手続きについて規定します。
なお、本認証局は証明書を発行する対象となる製品開発者を以下の2通りに分類します。

- A) 営利組織（製品ベンダ等）または、組織固有の事務所等を有する非営利組織（大規模なオープンソースコミュニティ等）
- B) 組織固有の事務所等を有さない非営利組織（オープンソースコミュニティ等）または、個人（ソフトウェア開発者等）

3-2-1. 秘密鍵の所有を証明する方法

本サービスでは利用者の秘密鍵と公開鍵の鍵ペアは、利用者自身が利用者の管理する装置上で生成しなければなりません。本認証局は、利用者の公開鍵と証明書に記載する情報を、利用者本人から PKCS#10 の形式で受け取ります。

3-2-2. 組織の識別及び認証

本認証局は、3.2節で規定したA)の組織について最低限以下の確認を実施します。

- ◆ 組織が存在すること
ホームページ等の公開された情報及び、公開されている連絡先にコンタクトとることにより組織の存在確認を行います。また、3-2-3項で規定する通りに、証明書発行に先立ち、組織名を含む住所宛に配達証明付郵便を送付し、組織の住所及び名称の確認を行います。
- ◆ 組織に所属する人物が特定の製品の開発に関わっていること
公開された組織の連絡先とのコンタクトの結果として、少なくとも一度は特定の製品の修正が行われたことなどを受けて、JPCERT/CCでは当該組織に所属する人物が特定の製品の開発に関わっていることの確認を行います。

3-2-3. 個人の識別及び認証

本認証局は、3-2節で規定したA)の組織に属する人物、及びB)に属する人物に対して以下の確認を行います。

- ◆ A)の組織に所属する人物の場合
本認証局は3-2-2項で規定された方法による認証を受けた組織内の一人または複数の人物に対して証明書の発行を認めます。本認証局は別途登録されている組織の申請責任者宛に配達証明付郵便にてSSLクライアント証明書発行様式を送付します。

当該様式を受領後、組織内の申請責任者は証明書の申請のために、当該様式に必要な事項を記入し、本認証局まで送付しなければなりません。当該様式には以下の項目の記載が必要です。

「組織名」、「役職」、「申請責任者の氏名」、「組織の住所」、「申請責任者のメールアドレス」、「電話番号」、「証明書の必要とする者の氏名（複数可）」、「申請責任者の捺印または署名」。

当該様式を受け取った本認証局は、当該様式に記載された「メールアドレス」が、過去に製品の修正に関する連絡を行う際に使用されていたメールアドレスであることの確認を行います。また、「組織名」、「（組織に関連する）住所」、「申請責任者氏名」については、本認証局より当該様式を配達証明付郵便にて送付した際に使用したものと同一であることの確認を行います。

◆ B) に属する人物の場合

本認証局は製品等に示された連絡先をもとに、製品を開発した組織の中の個人、または製品を開発した個人にコンタクトを行います。当該連絡先をもとに連絡を行った結果として、少なくとも一度は特定の製品の修正が行われたことなどを受けて、JPCERT/CC では当該個人が特定の製品の開発に関わっていることの確認を行い、証明書の発行を認めます。本認証局は別途登録されている個人の住所宛に配達証明付郵便にて SSL クライアント証明書発行様式を送付します。

当該様式を受領後、個人は証明書の申請のために、当該様式に必要な事項を記入し、本認証局まで送付しなければなりません。当該様式には以下の項目の記載が必要です。

「申請責任者名（個人名）」、「住所」、「申請責任者のメールアドレス」、「電話番号」、「申請責任者の捺印または署名」。

当該様式を受け取った本認証局は申請書に書かれた「メールアドレス」が、過去に製品の修正に関する連絡を行う際に使用されていたメールアドレスであることの確認を行います。また、「申請責任者名」、「住所」については、本認証局より当該様式を配達証明付郵便にて送付した際に使用したものと同一であることの確認を行います。

3-2-4. 確認しない個人の情報

本認証局は、証明書の初回発行に際し、製品開発者内の申請責任者の氏名、申請責任者の連絡先住所、メールアドレスの確認、及び製品開発者が特定の製品の開発に関係していることの確認を実施します。本認証局が、製品開発者内の複数の人物に対し証明書の発行を実施する場合は、製品開発者内における申請責任者以外の個人の認証は実施しません。

3-2-5. 役職等の確認方法

規定しません。

3-2-6. 相互運用の基準

規定しません。

3-3. 証明書更新時または再発行時の識別及び認証

本節では証明書の更新申請時に行われる認証手続きについて規定します。

3-3-1. 証明書更新時の識別及び認証

証明書の有効期間満了に伴う、証明書の更新は、証明書を新規に発行することにより実現されます。本認証局は証明書の有効期間が満了する 60 日以上前に登録してある製品開発者の申請責任者の住所に対し、配達証明付郵便にてSSLクライアント証明書発行申請様式を送付します。以降の本人性確認の方法は 3-2-3項の内容に従います。

3-3-2. 証明書失効後における再発行時の識別及び認証

何らかの理由による証明書の失効後に行われる証明書の更新は、証明書を新規に発行することにより実現されます。証明書の失効後に証明書の再発行を希望する利用者の所属する組織の申請責任者は、本認証局に連絡し、SSLクライアント証明書発行申請様式を郵送によって受領しなければなりません。その後の本人性確認の方法は 3-2-3項の内容に従います。

3-4. 失効申請時の識別及び認証

何らかの理由により、自身の証明書の失効を希望する利用者は自組織の申請責任者と協力し、本認証局に対し SSL クライアント証明書失効申請様式を提出しなければなりません。

当該様式には以下の項目の記載が必要です。

「申請責任者氏名」、「証明書の利用者名」、「申請責任者のメールアドレス」、「申請責任者の捺印または署名」。

JPCERT/CC では当該様式を受領後、自身が管理している当該申請責任者のメールアドレスに対し、失効の意思を確認するための電子メールを送付し、その意思を確認した上で、当該証明書の失効を行います。

4. 証明書のライフサイクルに関わる運用要件

4-1. 証明書申請

本節では証明書申請について規定します。

4-1-1. 証明書申請を行える者

本認証局の証明書の申請を行える者は以下の者に制限されます。

- (1) 本登録済みの製品開発者
- (2) 仮登録済みの製品開発者であり、JPCERT/CC が別途定める規定により証明書付与の許可を得た者

4-1-2. 登録手続き及び責任

証明書の申請を行う製品開発者は、本認証局に対し別途定める SSL クライアント証明書発行申請様式を送付しなければなりません。

4-2. 証明書申請手続き

本節では証明書申請時の手続きについて規定します。

4-2-1. 本人識別と認証の実施

証明書の発行を希望する製品開発者は、証明書の申請に先立ち、本認証局に対する窓口となる申請責任者を選出しなければなりません。申請責任者は製品開発者リスト登録申請等により、本認証局に対し、「氏名」、「連絡先住所」、「メールアドレス」等の情報を開示する必要があります。

本認証局は証明書の発行を認める製品開発者の申請責任者に対し、SSL クライアント証明書発行申請様式を配達証明付郵便にて郵送します。

当該様式を受領した申請責任者は、当該様式に対し 3-2-3項で規定された内容の記載を行い、本認証局宛に当該様式を送付する必要があります。

当該様式を受領した本認証局は別途定める基準に従い、当該様式の受理または不受理の判断を行います。

当該様式が受理された場合、本認証局は申請責任者に対し、証明書申請を完了させるために必要となるパスワード（場合によっては複数）が記載された書面を配達証明付郵便にて郵送します。

当該書面を受け取った申請責任者は、自組織内で証明書の利用を希望する者（利用者）に対し、個別に各利用者向けのパスワードを配布します。

パスワードを受領した利用者は、本認証局より別途指定されたウェブサイト上（ウェブサイトのサービス時間についてはリポジトリ上に掲載）にて当該パスワードを入力するこ

とで証明書申請を完了させることができます。

4-2-2. 証明書申請の承認または却下

本認証局は利用者によって本認証局が配布したパスワードが、本認証局が指定するウェブサイト上に入力された場合、証明書申請を承認します。利用者が間違ったパスワードを入力した場合、または利用者がパスワードの入力を行わなかった場合、本認証局は証明書の申請を承認しません。

4-2-3. 証明書申請の処理時間

本認証局は利用者によりパスワードが入力された後、速やかに証明書の発行を行います。

4-3. 証明書発行

本節では証明書発行時の手続きについて規定します。

4-3-1. 証明書の発行時における認証局の処理

本認証局は利用者による証明書申請完了後、速やかに証明書の発行を行い、ウェブサイトより当該証明書がダウンロード可能な状態にするための処理を行います。

4-4. 証明書受領時の処理

本節では証明書の受領時の手続きについて規定します。

4-4-1. 証明書の受領確認

本認証局は利用者が証明書をダウンロードしたことをもって証明書の受領が完了したと見なします。

4-5. 鍵ペアと証明書の利用用途

利用者が所有する秘密鍵及び公開鍵は SSL クライアント認証以外の目的で使用してはなりません。

4-6. 証明書の更新

本節では証明書の更新について規定します。

4-6-1. 証明書の更新が行われる場合

前年度に本認証局より証明書を受領していた利用者で、翌年度も証明書の使用を希望し、本認証局もそれを認める場合は証明書の更新が行われます。

4-6-2. 証明書の更新を申請できる者

証明書の更新を申請できる者は以下の者としてします。

- ◆ 証明書の更新を希望し、本認証局もそれを認める利用者

4-6-3. 証明書の更新申請の処理

本認証局は証明書が失効される各年の4月30日より60日以上前に製品開発者の申請責任者に対し、証明書の更新に関する連絡及びSSLクライアント証明書発行申請様式を配達証明付郵便にて送付します。その後の証明書の更新処理は新規発行処理と同様の手続きに従います。

4-6-4. 利用者に対する新しい証明書の通知

規定しません。

4-6-5. 更新された証明書の受領確認

4-4-1項と同様です。

4-6-6. 認証局による更新された証明書の公開

規定しません。

4-6-7. 認証局による更新された証明書の通知

規定しません。

4-7. 鍵ペア更新による証明書の更新

証明書の失効により証明書の再発行が必要な場合において利用者に求められる手続きは、原則として証明書初回発行時の手続きと同様です。証明書の再発行を希望する利用者は本認証局に連絡し、再度SSLクライアント証明書発行申請様式の送付を依頼しなければなりません。

4-8. 証明書の内容の変更による更新

本認証局が発行する証明書内に含まれる利用者の情報は3-1-2項に規定した通り識別以外の意味を成さない情報です。このため本認証局は証明書に記載される内容が変更されたことに伴う証明書の更新を想定しません。

4-9. 証明書の失効と一時停止

本節では証明書の失効及び一時停止について規定します。

4-9-1. 証明書失効の場合

証明書は以下の理由により失効されます。

- (1) 利用者の秘密鍵が危殆化した、または危殆化したと判断するにたる理由があるとき
- (2) 利用者が自身の秘密鍵を紛失したとき
- (3) 利用者が転属等の理由により証明書の利用を終了するとき
- (4) 利用者の所属する組織が、JPCERT/CC が管理する製品開発者リストから除名されたとき
- (5) その他、本認証局が必要と認めたとき

4-9-2. 証明書失効を申請することができる者

証明書の失効を申請できる者は以下の通りとします。

- (1) 当該証明書の利用者と同じ組織に属する申請責任者
- (2) 本認証局

4-9-3. 失効申請手続き

失効を希望する者は、同じ組織に属する申請責任者を通じて、本認証局に対し別途定められたSSLクライアント証明書失効申請様式を提出しなければなりません。当該様式に記載しなければならない項目は3-4節で規定した通りです。当該様式を受領した本認証局は別途定める基準に従い、提出された当該様式を確認した上で、当該書類を受理します。

本認証局では当該様式を受理後、本認証局が管理している当該申請責任者のメールアドレスに対し、失効の意思を確認するための電子メールを送付し、その意思を確認した上で、当該証明書の失効を行います。

4-9-4. 失効申請の猶予期間

利用者が4-9-1項に規定された失効理由に該当することに気がついた場合は遅滞無く4-9-3項に規定された失効申請手続きを行わなければなりません。

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

SSL クライアント証明書失効申請様式を受理した本認証局は、10 営業日以内に失効処理を実施します。

4-9-6. 信頼者の失効情報の調査要件

規定しません。

4-9-7. CRL 発行頻度

本認証局は24時間に一度以上、CRLの更新を実施します。

4-9-8. CRL の発行最大遅延時間

規定しません。

4-9-9. オンラインでの失効/ステータス確認の適用性

本認証局はオンラインによる失効情報の提供を実施しません。

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

規定しません。

4-9-11. 利用可能な失効通知の他の形式

規定しません。

4-9-12. 鍵危殆化による失効時の特別要件

自身が所有する秘密鍵が危殆化した、または危殆化したと判断するにたる状況にあるとき、利用者は自組織の申請責任者と協力し、速やかに、SSL クライアント証明書失効申請様式を本認証局に対し、FAX にて送付しなければなりません。

本認証局では当該 FAX を受領後、JPCERT/CC が管理する当該申請責任者の電話番号に対して連絡を行うことで失効に関わる意思の確認を行い、早急に証明書の失効を行います。

なお、申請責任者は当該様式を FAX にて送付後、原本を本認証局まで郵送しなければなりません。

4-9-13. 証明書の一時的停止が行われる状況

規定しません。

4-9-14. 証明書の一時的停止を要求できる者

規定しません。

4-9-15. 証明書の一時的停止要求の手続き

規定しません。

4-9-16. 証明書の一時的停止を継続できる期間

規定しません。

4-10. 証明書ステータス確認サービス

規定しません。

4-11. 利用者の本サービス利用の停止

何らかの理由により本サービスの利用の停止を希望する製品開発者は、自身に所属する利用者が所有する全ての証明書失効申請を行わなければなりません。

また、何らかの理由により製品開発者が製品開発者リストから除名された場合は、本認証局は当該製品開発者に所属する利用者が所有する全ての証明書の失効を行います。

4-12. 鍵預託と鍵の回復

規定しません。

5. 物理的管理、運営上の管理、運用上の管理

5-1. 物理的管理

本節では本認証局が設置される設備の物理的な管理について規定します。

5-1-1. 施設の立地場所及び構造

認証局の設備を収容する施設は、地震、水害、火災等の災害に対する対策がなされた施設です。当該施設の所在地は、認証局の運営に係る人物以外には公表されません。バックアップ施設についても本番センタと同様の管理を行います。

登録局の設備を収容する施設については、日本国内の基準に則った耐震耐火設計がなされています。

5-1-2. 施設内の物理的アクセス

認証局の設備においては以下の物理的アクセス管理が行われています。

- (1) 認証局設備室は厳重に施錠管理されており、入室の際には、バイオメトリクス等の技術を利用した本人認証を受ける必要があります。認証局設備室に入室権限を有しない者は、入室権限を有する者の付添が無ければ入室することができません。
- (2) 入室のための装置操作等に、設定されたしきい値以上の時間を要した場合は、アラームが鳴るような仕組みが施されています。
- (3) セキュリティ上重要な部屋への入室には複数人の立会いが必要となるような仕組みが施されています。
- (4) 認証設備室内の状況は、遠隔監視装置によって記録されています。また、その記録は一定の期間、保存されています。

登録局における重要な業務を実施する登録局業務室には、電子錠によって施錠管理が行われている複数の扉を経由することなしに入室することはできません。また、登録局業務室には、特定の権限を有する者の許可無しに入室することができません。

5-1-3. 電源及び空調

認証局の設備を収容する施設には自家発電装置・UPSが設置されており、停電等に対する対策が成されています。また、認証局設備室には適切な空調機器が設置されています。

登録局で利用する重要な機器については、UPSの利用等による瞬電対策がなされています。

5-1-4. 水害

認証局の設備を収容する施設は水害防止等の対策が行われています。登録局については規定しません。

5-1-5. 火災防止及び火災保護対策

認証局の設備を収容する施設は火災予防と火災被害に対する対策が行われています。

登録局の設備を収容する施設には、日本国内の基準に則った消化装置が設置されています。

5-1-6. 媒体保管場所

認証局の設備で取得された長期保管するデータ及び、バックアップデータは、認証局内またはバックアップセンタに保管されます。保管されるデータは施錠可能な場所に保管されます。

登録局にて使用する記録可能媒体は、施錠可能な場所に保管します。

5-1-7. 廃棄処理

認証局において暗号モジュールを破棄する場合は、記録されていた情報を読み取りまたは解析することが不可能となるような処理を行った上で破棄します。重要な情報が含まれていた記録可能媒体についても同様の対策を実施します。また、重要な文書は、破棄を行う際に、記載されていた内容を読み取ることが不可能となるような処理を実施します。

登録局において使用した書面等を破棄する場合は、シュレッダーにかける等の対策を行います。また、記録可能媒体を破棄する場合は、記録していた情報の読み出しが不可となるような対策を行います。

5-1-8. 施設外のバックアップ

認証局については5-7項の通りです。登録局については規定しません。

5-2. 手続的管理

本節では本認証局で行われる手続きの管理方法について規定します。

5-2-1. 信頼すべき役割

本項では認証局及び登録局における信頼すべき役割を規定します。

5-2-1-1. 認証局

認証局の設備において信頼される人物となるためには、当該人物は面接及び身分証明書（運転免許証等）の確認などによる身元の確認作業を受けなければなりません。

認証局における信頼される人物は以下の者が含まれますが、これに限定されません。

- ◆ システム管理者
- ◆ 鍵管理者
- ◆ セキュリティ管理者

5-2-1-2. 登録局

登録局においては以下の体制により登録業務を実施します。

- ◆ 登録局設備管理者（1名）

登録局設備管理者は、以下の業務を行う。

 - 登録局設備の管理、入退室に関する情報の記録の取得及びその保護
- ◆ 登録局業務監督者（1名）

登録局業務監督者は、以下の業務を行う。

 - 各種申請書類の最終チェック
 - 登録局端末操作員によって行われた作業の履歴の確認
 - 登録局端末操作員及び登録審査員の監督指導
- ◆ 登録局端末操作員（1名）

登録局端末操作員は、以下の業務を行う。

 - 登録局業務監督者の指示の元に、証明書の新規発行、更新、失効に関わる登録局内の端末の操作
- ◆ 登録審査員（1名）

登録審査員は、以下の業務を行う。

 - 本サービスに関わる各種申請書類の審査等

5-2-2. 職務ごとに必要とされる人数

認証局の設備では、業務ごとの内部牽制を確実にするための厳格な管理手続きを維持しています。また、認証局用暗号ハードウェア等の最も機密を要するデバイスには、そのライフサイクルを通じて、複数人の信頼される人物の権限がなければアクセスができないような仕組みが施されています。

登録局においては、製品開発者より提出された各種申請書類は登録審査員及び登録局業務監督者の確認を受けた上で、承諾または、不承諾の判断が行われます。また、登録局端末操作員によって行われた作業については、作業後、登録局業務監督者によってその履歴の確認が行われます。

5-2-3. 職務実施時の本人識別と認証

認証局については5-2-1項で規定した通りです。登録局においては、登録局業務室への入室の際は電子錠等による本人性確認が行われます。また、登録局端末操作員が端末の操作を実施する場合は、パスワード等を用いた本人性の確認が行われます。

5-2-4. 職務分割が要求される役割

本認証局内の各役割については全て異なる人物が担当します。ただし、緊急に証明書の

失効を実施する際などについては、役割を兼務することがあります。そのような場合においても、各作業は複数人により作業内容の確認が行われた上で処理されます。

5-3. 人事的管理

本サービスに関わる要員の任命、教育、配置転換等については、JPCERT/CC の内部の規程に基づいて運用します。また、すべての要員には、運営を行うために必要な知識及び技術を習得するための教育訓練を行います。

本サービスの業務の一部を外部委託する場合の、その要員に関する要件は本 CPS では規定しません。ただし、JPCERT/CC は本 CPS で規定される要件に照らして十分な要件を満たしていることを事前に確認します。

5-4. 監査ログに関する手続き

本節では本認証局内で取得される監査ログについて規定します。

5-4-1. 記録されるイベントの種類

5-4-1-1. 認証局

認証局の設備では、次のイベントが記録されます。

- (1) 物理的セキュリティ及び論理的セキュリティに関するイベント
 - 認証局設備における入退室
 - 認証局内のシステムに対するアクセス
 - セキュリティ上重要なファイル等に対する操作
- (2) 証明書のライフサイクルに関するイベント
 - 証明書申請、更新申請、失効申請
 - 証明書発行
 - CRL 作成

5-4-1-2. 登録局

登録局の設備では次の重要なイベントの記録を行います。

- (1) 端末の操作に関するイベント
 - 登録局業務室への入室者及びその入室時間
 - 登録局端末へのログインに関するログ
 - 登録局端末において実施した作業内容
- (2) 申請に関するイベント
 - 各種申請書の受領履歴

5-4-2. 監査ログを確認する頻度

本認証局の設備で取得された監査ログの検査は、適切と考えられる頻度で実施されます。

5-4-3. 監査ログを保持する期間

認証局の設備で取得された監査ログは 2 ヶ月間以上、また証明書ライフサイクルに関連するログは 5 年間以上保存されます。

登録局の設備では認証業務が継続している範囲において以下の期間、監査ログを保存します。

- (1) 書面による記録は 3 年間
- (2) 電子データによる記録は 1 年間

5-4-4. 監査ログの保護方法

本認証局の設備で取得された監査ログは改ざん、破壊、情報漏えい等が行われないうように保管されます。

5-4-5. 監査ログのバックアップ手法

本認証局の設備で取得された監査ログの中でバックアップが必要とされるものは、定められた手続きに従い、バックアップが行われます。

5-4-6. 監査ログの収集方法

本認証局の設備で取得された監査ログはオペレータによる手動、またはシステムによる自動処理により収集されます。

5-4-7. イベントを引き起こした対象に対する通知

本認証局は監査ログの内容により、当該事象を発生させた者に対する通知を行わず調査を行うことがあります。

5-4-8. 脆弱性評価

規定しません。

5-5. 記録の長期保管

本節では本認証局内で長期保管を行う書類または電子データについて規定します。

5-5-1. 長期保管する記録の種類

認証局の設備で長期保管する書類または電子データは以下の通りです。

- ◆ 5-4-1-1小項で規定されている監査ログ

- ◆ 本認証局が発行した利用者の証明書

登録局の設備で長期保管する書類または電子データは以下の通りです。

- ◆ 5-4-1-2小項で規定されている監査ログ
- ◆ 証明書申請に関する情報
 - SSL クライアント証明書発行申請様式
- ◆ 証明書失効に関する情報
 - SSL クライアント証明書失効申請様式
- ◆ 組織管理に関する情報
 - 本 CPS とその変更に関する記録
 - 業務手順を記述した書類とその変更に関する記録
 - 業務に従事する者の責任及び権限並びに指揮命令系統を記述した書類とその変更に関する記録
 - 認証業務の一部を外部に委託する場合の委託契約に関わる書類

5-5-2. 記録を長期保管する期間

認証局の設備において長期保管する書面または電子データは 5-4-3項に規定されている通り保存します。

登録局の設備において長期保管する書面または電子データの保管期間は以下の通りとします。

- ◆ 5-4-1項で規定されている監査ログ
 - 5-4-3項で規定する期間
- ◆ それ以外の長期保管する書面または電子データ
 - 書面による記録は3年間
 - 電子データによる記録は1年間

5-5-3. 長期保管する記録の保護方法

認証局の設備において長期保管を行う記録の保護については5-4-4項の通りです。

登録局の設備において長期保管を行う記録については以下の通りです。

- ◆ 5-4-1-2小項で規定されている監査ログ
5-4-4項の通りです。
- ◆ それ以外の書面または電子データ
電子データとして保存される帳簿書類の保存に使用する媒体は、漏洩、改ざん、毀損などが行われないように安全に保管します。原本として紙で保存される帳簿書類につ

いては、施錠可能なキャビネットに保管されます。

5-5-4. 長期保管する記録のバックアップ手続き

規定しません。

5-5-5. 長期保管する記録へのタイムスタンプ

規定しません。

5-5-6. 長期保管する記録の収集方法

5-4-6項と同様です。

5-5-7. 長期保管する記録の可読性、完全性確認

規定しません。

5-6. 認証局秘密鍵の切替

規定しません。

5-7. 危殆化及び災害からの復旧

本節では認証局秘密鍵の危殆化時や本認証局の設備が被災したときの手続きについて規定します。

5-7-1. 事故及び災害からの復旧

本認証局では、認証局秘密鍵の危殆化またはセキュリティインシデント発生時の手続きを定めており、事故が発生した場合には当該手続きに従い、適切に対応します。

5-7-2. コンピュータ資源、ソフトウェア、または、データが破壊された場合

認証局の設備におけるハードウェアは二重化されており、片系のハードウェアに問題が生じた場合は、残りのハードウェアにて業務を継続します。

ソフトウェアまたはデータに問題が生じた場合は、バックアップされているソフトウェアまたはデータにより復旧が行われます。

登録局の設備において利用されるハードウェア、ソフトウェア、データの破壊が発生した場合は予め定められた手続きに基づき復旧作業を行います。

5-7-3. 利用者の秘密鍵が危殆化した場合の手続き

利用者の秘密鍵が危殆化した場合は、4-9-12項で規定したように、利用者は遅滞無く本認証局に対し、その事実を伝えなければなりません。本認証局では当該証明書を直ちに失

効いたします。

5-7-4. 被災後の事業継続能力

認証局の設備は遠隔地に災害対策用のバックアップセンターが設けられています。本番センターの被災時は、認証局の秘密鍵の危殆化の恐れが無い事を確認した上で、バックアップセンターへの切り替えを実施し、業務を継続します。登録局については規定しません。

5-8. 認証業務の終了

本認証局が認証業務を終了する場合は、本認証局は参加者の混乱を最小限にするために本認証局の業務を終了させるためのプランを作成します。本認証局は、当該プランの作成において以下の事項の検討を行うことを想定しています。

- ◆ 利用者に対し、本認証局の終了を通知するための方法
- ◆ 上記通知の実施時期
- ◆ 本認証局が発行した全ての証明書の失効を行うか否かについて
- ◆ 本認証局終了後のリポジトリの運営について
- ◆ 5-5節で必要とされる期間中における本認証局の記録の保存
- ◆ 秘密として取り扱う情報及び個人情報の措置

6. 技術的セキュリティ管理

6-1. 鍵ペアの生成及びインストール

本節では各参加者の鍵ペアの生成及びインストールについて規定します。

6-1-1. 鍵ペアの生成

認証局の鍵ペアは、認証局の設備内において、複数人の信頼される人物の操作によって暗号モジュール内で作成されます。

利用者は自己の責任によって鍵ペアの生成を行わなければなりません。

6-1-2. 利用者に対する秘密鍵の交付

利用者の秘密鍵は利用者自身が作成しなければなりません。

6-1-3. 認証局に対する公開鍵の交付

利用者は証明書の取得の際に、自身の公開鍵を PKCS#10 の形式にて本認証局に送付する必要があります。

6-1-4. 信頼者に対する認証局の公開鍵の送付

信頼者に対する認証局の公開鍵の交付については規定しません。ただし、認証局の公開鍵を含む認証局証明書は、利用者が証明書を取得する際に、利用者に交付されます。

6-1-5. 鍵サイズ

本サービスで利用される公開鍵の技術的仕様は以下の通りです。

JPCERT/CC ルート認証局：1024bit の RSA

JPCERT/CC SSL クライアント証明書発行認証局：1024bit の RSA

利用者：1024bit の RSA

6-1-6. 鍵生成に利用するパラメータの生成及び品質検査

規定しません。

6-1-7. 鍵の利用用途

認証局の秘密鍵は、以下の目的のみに使用されます。

- ◆ 利用者の証明書に対する署名
- ◆ 認証局証明書に対する自己署名、及び、下位認証局が存在する場合には下位認証局証明書に対する署名
- ◆ CRL に対する署名

利用者の秘密鍵は、以下の目的のみに使用されます。

◆ SSL 通信におけるクライアント認証

6-2. 秘密鍵の保護及び暗号モジュール技術の管理

本節では認証局の秘密鍵の保護方法について規定します。利用者の秘密鍵の保護方法については規定しませんが、利用者は自身の責任により厳重に秘密鍵を管理しなければなりません。

6-2-1. 暗号モジュールの標準及び管理

暗号モジュールには FIPS140-1 level 3 相当の HSM を使用します。

6-2-2. 秘密鍵の複数人による管理

本認証局は、認証局秘密鍵の活性化データを複数の情報に分割しそれぞれのデータは複数人の信頼される人物に配布されて厳重に保管されます。HSM に保管されている認証局秘密鍵を活性化するには、それらのデータのうち、一定数のデータが必要となります。

6-2-3. 秘密鍵の預託

規定しません。

6-2-4. 秘密鍵のバックアップ

認証局秘密鍵のバックアップは、認証局秘密鍵が格納されている HSM と同型の HSM を利用し、HSM の機能を用いて行われます。当該作業は、認証局内において、複数人の信頼される人物の立会いの下、実施されます。また、バックアップ用の HSM は認証局内の施錠可能な場所に保管されます。

6-2-5. 秘密鍵の長期保管

規定しません。

6-2-6. 秘密鍵の暗号モジュールへの格納及び取出

規定しません。

6-2-7. 秘密鍵の暗号モジュール内での格納形式

規定しません。

6-2-8. 秘密鍵の活性化方法

認証局の秘密鍵については 6-2-2項を参照してください。

6-2-9. 秘密鍵の非活性化方法

規定しません。

6-2-10. 秘密鍵の破棄方法

規定しません。

6-2-11. 暗号モジュールの評価

規定しません。

6-3. その他の鍵ペア管理について

本節では鍵ペア管理のその他の項目について規定します。

6-3-1. 公開鍵の長期保管

認証局公開鍵が記載された認証局証明書は、本サービス提供中、認証局内で保管されています。

6-3-2. 証明書使用期間及び鍵ペア使用期間

規定しません。

6-4. 活性化データ

本節では各参加者の秘密鍵を活性化するためのデータについて規定します。

6-4-1. 活性化データの生成及び設定

認証局秘密鍵は 6-2-2項によって規定された分割されたデータが、一定数集められることにより活性化されます。分割されたデータは認証局秘密鍵生成時に、それぞれの信頼される人物に配布されます。

利用者の秘密鍵の活性化情報については本 CPS では規定しません。ただし、本認証局は、利用者が、秘密鍵の活性化情報として妥当な強度のパスワードの設定を行うことを推奨します。

6-4-2. 活性化データの保護

認証局秘密鍵の活性化データは 6-2-2項で規定された通りに分割されて、複数人の信頼される人物によって管理されています。また、それぞれの分割したデータは各管理者により

嚴重に保管されます。

利用者の秘密鍵の活性化データを保護する方法については本 CPS では規定しません。ただし、利用者は自身の責任により活性化データを適切に管理しなければなりません。

6-5. コンピュータセキュリティ管理

本節では認証局のコンピュータセキュリティ管理について規定します。

6-5-1. 特定のコンピュータのセキュリティに関する技術的要件

認証局の設備で用いられるシステムは監査ログ記録機能、アクセス制御機能等を有しています。登録局については規定しません。

6-5-2. コンピュータセキュリティの評価

認証局の設備において、証明書の発行に関連する装置は ISO/IEC15408 によって定義された評価保証レベル (EAL) の EAL4 に相当するシステムが利用されています。登録局については規定しません。

6-6. ライフサイクルの技術上の管理

本節では本認証局を構成するシステムのライフサイクルにおけるセキュリティ統制について規定します。

6-6-1. システム開発時の管理

認証局の設備において利用するアプリケーションは定められた基準に従い、開発または変更されます。登録局については規定しません。

6-6-2. システム運用時の管理

認証局の設備では、システムの完全性を維持するために、ソフトウェア等のアップデートを行う際は、定められた手続きに従い、システムの完全性のチェックを実施します。登録局については規定しません。

6-6-3. ライフサイクルセキュリティ管理

規定しません。

6-7. ネットワークセキュリティ管理

認証局の設備では、定められたガイドに基づき、ネットワークセキュリティの確保を行います。

登録局の設備では、ファイアウォール及び IDS (侵入検知システム) 等を利用し、適切な

ネットワークセキュリティの管理を実施します。秘密とすべき情報の通信は、暗号化等を用いて行います。

6-8. タイムスタンプ

規定しません。

7. 証明書及び CRL プロファイル

7-1. 証明書のプロファイル

表 6 JPCERT/CC ルート認証局の証明書プロファイル

領域名	設定値	補足説明	
version (バージョン番号)	2	バージョン 3 を示す	
serialNumber (シリアル番号)	...	ユニークな整数	
signature (署名アルゴリズム)			
algorithm identifier (アルゴリズム識別子)	1.2.840.113549.1.1.5	sha1WithRSAEncryption を示す	
issuer (発行者名)	c=jp o=Japan Computer Emergency Response Team Coordination Center cn=JPCERT/CC Root CA	PrintableString で記載	
validity (証明書有効期間)			
notBefore (発行日)	YYMMDD000000Z	UTCTime で記載	
notAfter (終了日)	YYMMDD235959Z	UTCTime で記載 発行日より10年	
subject (主体者名)	c=jp o=Japan Computer Emergency Response Team Coordination Center cn=JPCERT/CC Root CA	PrintableString で記載	
subjectPublicKeyInfo (主体者検証鍵情報)			
algorithm (アルゴリズム識別子)	1.2.840.113549.1.1.1	rsaEncryption を示す	
subjectPublicKey (検証鍵の値)	...	公開鍵(1024bit)の値	
extensions (拡張領域)			
領域名	クリティカルフラグ	設定値	補足説明
keyUsage (鍵用途)	FALSE	keyCertSign cRLSign	
basicConstraints (基本制約)	FALSE		
cA		TRUE	
pathLenConstraint		1	

表 7 JPCERT/CC SSL クライアント証明書発行認証局の証明書プロファイル

領域名	設定値	補足説明	
version (バージョン番号)	2	バージョン 3 を示す	
serialNumber (シリアル番号)	...	ユニークな整数	
signature (署名アルゴリズム)			
algorithm identifier (アルゴリズム識別子)	1.2.840.113549.1.1.5	sha1WithRSAEncryption を示す	
issuer (発行者名)	c=jp o=Japan Computer Emergency Response Team Coordination Center cn=JPCERT/CC Root CA	PrintableString で記載	
validity (証明書有効期間)			
notBefore (発行日)	YYMMDD000000Z	UTCTimeで記載	
notAfter (終了日)	YYMMDD235959Z	UTCTimeで記載 発行日より5年	
subject (主体者名)	c=jp o=Japan Computer Emergency Response Team Coordination Center cn=JPCERT/CC CA for SSL Clients	PrintableString で記載	
subjectPublicKeyInfo (主体者検証鍵情報)			
algorithm (アルゴリズム識別子)	1.2.840.113549.1.1.1	rsaEncryption を示す	
subjectPublicKey (検証鍵の値)	...	公開鍵(1024bit)の値	
extensions (拡張領域)			
領域名	クリティカルフラグ	設定値	補足説明
keyUsage (鍵用途)	FALSE	keyCertSign cRLSign	
basicConstraints (基本制約)	FALSE		
cA		TRUE	
pathLenConstraint		0	
netscapeCertType (2.16.840.1.113730.1.1)	FALSE	SSL CA	
subjectAltName	FALSE		
directoryName			
commonName		HSMトークン番号	

表 8 利用者の証明書プロファイル

領域名	設定値	補足説明	
version (バージョン番号)	2	バージョン3を示す	
serialNumber (シリアル番号)	...	各証明書にユニークな整数	
signature (署名アルゴリズム)			
algorithm identifier (アルゴリズム識別子)	1.2.840.113549.1.1.5	sha1WithRSAEncryptionを示す	
issuer (発行者名)	c=jp o=Japan Computer Emergency Response Team Coordination Center cn=JPCERT/CC CA for SSL Clients	PrintableStringで記載	
validity (証明書有効期間)			
notBefore (発行日)	YYMMDD000000Z	UTCTimeで記載	
notAfter (終了日)	YYMMDD235959Z	UTCTimeで記載 発行日より最大1年1ヵ月後 (但し、毎年4/30 23:59:59UTC で失効する)	
subject (主体者名)	o=Japan Computer Emergency Response Team Coordination Center ou = JPCERT/CC CA for SSL Clients cn = SSL-999999-999999-9999a	左記の項目は例) PrintableStringで記載	
subjectPublicKeyInfo (主体者検証鍵情報)			
algorithm (アルゴリズム識別子)	1.2.840.113549.1.1.1	rsaEncryptionを示す	
subjectPublicKey (検証鍵の値)	...	公開鍵(1024bit)の値	
extensions (拡張領域)			
領域名	クリティカルフラグ	設定値	補足説明
basicConstraints (基本制約)	FALSE		
cA		FALSE	
pathLenConstraint		NULL	
keyUsage (鍵用途)	FALSE	digitalSignature keyEncipherment	
cRLDistributionPoints (CRL 配布点)	FALSE	http://www.jpCERT.or.jp/ca-info/crl-list.crl	
netscapeCertType (2.16.840.1.113730.1.1)	FALSE	SSL client	
certificatePolicies (CPS)	FALSE	PolicyIdentifier: OID=1.2.392.200212.1.1.1 PolicyQualifier: ID=CPS URI=http://www.jpCERT.or.jp/ca-info/jpCERT-cps.pdf	

7-2. CRLのプロファイル

表 9 CRLのプロファイル

領域名	設定値	補足説明
version (バージョン番号)	1	バージョン 2 を示す
signature (署名アルゴリズム)		
algorithm identifier (アルゴリズム識別子)	1.2.840.113549.1.1.5	sha1WithRSAEncryption を示す
issuer (発行者名)	c=jp o=Japan Computer Emergency Response Team Coordination Center cn=JPCERT/CC CA for SSL Clients	PrintableString で記載
lastUpdate (今回更新日時)	YYMMDDhhmmssZ	UTCTime で記載
nextUpdate (今回更新日時)	YYMMDDhhmmssZ	UTCTime で記載 (lastUpdate の 4 日後)

領域名	設定値	補足説明
revokedCertificates (失効された証明書リスト)		
userCertificate (失効された証明書のシ リアル番号)	...	整数
revocationDate (失効日)	YYMMDDhhmmssZ	UTCTimeで記載
reasonCode (失効理由)	...	ENUMERATED

extensions (拡張領域)			
領域名	クリティカルフラグ	設定値	補足説明
cRLNumber (失効リスト番号)	FALSE	...	CRL 生成毎に 1 ずつ増 加して設定する整数

領域名	設定値	補足説明
subjectPublicKeyInfo (主体者検証鍵情報)		
algorithm (アルゴリズム識別子)	1.2.840.113549.1.1.5	sha1WithRSAEncryption を示す
subjectPublicKey (検証鍵の値)	...	公開鍵(1024bit)の値

7-3. OCSPのプロファイル

規定しません。

8. 準拠性監査とその他の評価

8-1. 監査の頻度

認証局及び登録局に対する準拠性の監査はそれぞれ随時実施します。

8-2. 監査人の身元または資格

認証局の監査を実施する監査人は、PKI に関する知識を十分に有している者が任命されます。また、登録局の監査を実施する監査人は、認証局における登録局業務に関する知識を十分に有している者が任命されます。

8-3. 監査人と被監査人の関係

認証局の監査を実施する監査人は、認証局の運用部門と独立した部門に所属する者が任命されます。また、登録局の監査を実施する監査人は、JPCERT/CC の経営部門によって任命されます。

8-4. 監査項目

登録局の監査は登録局業務が本 CPS に従って行われていることを確認するために実施されます。主な監査項目は以下の通りです。

- ◆ 登録局の物理的環境及びその保護
- ◆ 証明書の発行、失効、更新に関する登録局の業務
- ◆ 登録局内のハードウェア、ソフトウェア、ネットワークの妥当性
- ◆ 登録局が扱う個人情報、機密情報の保護

なお、認証局の監査項目については規定しません。

8-5. 監査指摘事項に対する処置

JPCERT/CC では監査結果での指摘事項を踏まえ、セキュリティ対策技術の最新の動向を考慮して、業務及び設備の改善や必要に応じ本 CPS を改訂し、その結果の評価を行います。また、必要に応じて当該評価結果に基づき対応措置の見直しを行います。

8-6. 監査結果の公表

JPCERT/CC は原則として監査結果の外部への開示を行いません。ただし公的機関から法律に基づく開示要求があった場合や、公表が妥当であると JPCERT/CC が判断した場合、監査結果の開示を行うことがあります。

9. その他の業務上及び法的問題

9-1. 料金

本認証局が提供するサービスの利用料金については以下の URL で公表されています。

- ◆ 『利用料金』: <http://www.jpcert.or.jp/ca-info/contact.html>

9-2. 財務的責任

本 CPS では損害保険加入の有無、支払能力の有無等財務的な責任については規定しません。

9-3. 秘密情報の保護

本節では本認証局が管理する秘密情報の取扱いについて規定します。

9-3-1. 秘密情報の範囲

認証局が保有する情報は、本 CPS で公表すると定めた情報、本 CPS の一部として明示的に公表された情報、ウェブページ等で公表している情報、証明書の発行者である認証局情報と失効日時を含む CRL 等を除き、原則として秘密情報として取り扱われます。かかる秘密情報には以下の情報を含みます。本認証局は以下の情報を本サービス以外の利用目的に使用しません。

- (1) 製品開発者リストに関する登録の記録
- (2) 証明書申請に関わる記録
- (3) 失効申請に関わる記録
- (4) パスワードが記載された書面または電子データ
- (5) 偶発事故に対する災害復旧計画
- (6) 本認証局内で利用するハードウェア及びソフトウェアの運用方法
- (7) 監査人によって作成された監査記録

9-3-2. 秘密情報の範囲外の情報

9-3-1項に拘らず、下記の情報を秘密情報に含まれません。

- JPCERT/CC の過失によらず公知になった情報
- JPCERT/CC 以外の出所から、機密保持の制限なしに JPCERT/CC に知られるようになった情報
- JPCERT/CC によって独自に開発された情報
- 開示対象の情報に関連する人又は組織により承認を得ている情報

9-3-3. 秘密情報を保護する責任

JPCERT/CC で取扱う秘密情報に関して、捜査機関、裁判所その他法的権限に基づいて情報を開示するよう請求があった場合、JPCERT/CC は、法の定めに従って法執行機関へ秘密情報を開示することができるものとします。また、本認証局で取扱う秘密情報に関して、調停、訴訟、仲裁その他の法的、裁判上又は行政手続の過程において、裁判所、弁護士その他の法律上の権限を有する者から任意に開示要求があった場合、JPCERT/CC は、当該要求事項に関しかかる情報を開示することができます。

JPCERT/CC は、業務の一部を委託する場合、秘密保持義務を課した上で、秘密情報を委託先に開示することがあります。

なお、個人情報の保護に関しては別段の規定に従います。

9-4. 個人情報の保護

本節では本認証局が管理する個人情報の取扱いについて規定します。

9-4-1. 個人情報保護方針

本認証局は以下の URL にて公表されている JPCERT/CC が保持する個人情報保護方針に従います。

◆ 『個人情報保護方針』: <http://www.jpccert.or.jp/privacy.html>

9-4-2. 個人情報の定義

個人情報とは、生存する個人に関する情報であつて、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む）をいいます

9-4-3. 個人情報として扱われない情報

以下に例示列挙される情報には、個人情報が含まれず、本認証局はこれらの情報を個人情報として取り扱いません。

- (1) 証明書に記載される情報
- (2) CRL に記載される情報
- (3) リポジトリで公開される情報

9-4-4. 個人情報を保護する責任

本認証局は、個人情報の保護を十分に行い、JPCERT/CC の策定する個人情報保護方針に従って個人情報を取り扱います。

9-4-5. 個人情報の利用に関する通知と同意

利用者は、本認証局に対し、書面による証明書申請、失効申請、更新申請等を行うにあたり個人情報を提供する場合には、本認証局が本サービス上必要とする個人情報を使用することに予め同意し、または当該個人の同意を取り付けた上で提供することとします。

9-4-6. 司法手続きまたは行政手続きによる個人情報の開示

本認証局は、司法手続き、行政手続きを含む法的手続きに際し、個人情報を開示する権限を有するものとします。

9-5. 知的財産権

別段の合意がなされない限り、以下の情報資料及びデータに関する著作権その他の知的財産権は本認証局を運営する JPCERT/CC に帰属し、その他の者には帰属しないものとします。リポジトリで公開される情報は、利用者または信頼者に参照されることを目的としており、無断で複製、転載などを行うことを禁止します。

- (1) 本認証局から発行された証明書（ただし、利用者の公開鍵情報を除く）
- (2) 本認証局から発行された認証局証明書
- (3) 本認証局秘密鍵
- (4) 本認証局により作成された失効情報（CRL を含む）
- (5) 本 CPS
- (6) その他リポジトリで公表する情報
- (7) 上記（1）から（6）までに関連する知的財産権

9-6. 表明保証

本節では各参加者が実施することを表明し、保証しなければならない事項について規定します。

9-6-1. 認証局の表明保証

認証局は下記の事項を実施することを表明し、それを保証しなければなりません。

- ◆ 本 CPS に従って運用を行うこと
- ◆ 認証局秘密鍵を適切に管理して、発行した証明書及び CRL の信頼の確保を行うこと

9-6-2. 登録局の表明保証

登録局は下記の事項を実施することを表明し、それを保証しなければなりません。

- ◆ 証明書利用申請または更新申請を適切に審査し、証明書の発行処理を行うこと
- ◆ 証明書失効申請を適切に審査し、証明書の失効処理を行うこと

9-6-3. 利用者の表明保証

利用者は下記の事項を実施することを表明し、それを保証しなければなりません。

- ◆ 1-4項 で規定された証明書用途を遵守すること
- ◆ 証明書申請の際に利用者及び同じ組織に属する申請責任者が本認証局に提供した情報が正確であること
- ◆ 自身の秘密鍵及び活性化情報を厳重に保管し、紛失、改変、第三者による使用・複製等が行われないように、万全な管理をおこなうこと
- ◆ 秘密鍵が危殆化している、または危殆化の可能性があると判断したとき、自身または同じ組織に属する申請責任者を通じて本認証局に対し、直ちに証明書の失効申請を行うこと

9-6-4. 信頼者の表明保証

信頼者は下記の事項を実施することを表明し、それを保証しなければなりません。

- ◆ 利用者が提出した証明書を信頼するまえに、証明書が有効期間内にあること、及び本認証局が発行した最新の CRL 上に当該証明書が掲載されていないことの確認を行うこと

9-6-5. その他の関係者の表明保証

規定しません。

9-7. 保証の制限

JPCERT/CC は、本 GPS に記載してある事項を遵守しているにも拘らず発生した損害については、一切の責任を負わないものとします。

また、JPCERT/CC は、利用者が 9-6-3項 を遵守することを、他の関係者に保証しないものとします。

9-8. 責任の制限

利用者が 9-6-3項 に違反したことに起因して生じた損害について、JPCERT/CC は、第三者に対し一切の責任を負わないものとします。利用者が 9-6-3項 で表明したことに違反していることが明らかな場合、JPCERT/CC は利用者への事前の通知を行うことなく、利用者に対して発行した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ものとします。

また、JPCERT/CC が、本 GPS に規定された責任を果たさなかったことに起因して、利用者に対して損害を与えた場合においても、本 GPS に別段の定めが無い限り、利用者に対して行う損害賠償の上限は、当該年度に当該利用者が、本サービスの利用に関して JPCERT/CC に支払いを行った金額を超えないものとします。

本 GPS 「9.6.1 認証局の表明保証」及び「9.6.2 登録局の表明保証」に関し、以下の場合には JPCERT/CC は責任を負わないものとします。

- JPCERT/CC に起因しない不法行為、不正使用並びに過失等により発生する一切の損害
- 利用者が自己の義務の履行を怠ったために生じた損害
- 利用者の端末のソフトウェアの瑕疵、不具合その他の動作自体によって生じた損害
- JPCERT/CC の責に帰することのできない事由で証明書及び CRL に公開された情報に起因する損害
- JPCERT/CC 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
- 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、認証局業務の停止に起因する一切の損害

9-9. 補償

利用者の行為に起因して、第三者に損害が生じた場合、JPCERT/CC は免責されるものとします。利用者は、第三者に対し損害賠償の責めを負わなくてはならず、また、JPCERT/CC が第三者に損害賠償を行った場合、利用者は JPCERT/CC に対しその賠償額及び JPCERT/CC において発生する訴訟に係わる費用等の損害を補償しなくてはならないものとします。

9-10. 有効期間と終了

本節では本 GPS の有効期間及び終了について規定します。

9-10-1. 有効期間

本 GPS は本サービスが継続する限り有効であるものとします。本 GPS の改訂が行われた場合は、最も新しく改訂された GPS が有効なものであるものとします。

9-10-2. 終了

本サービスは、JPCERT/CC が JVN ベンダステータス情報収集システムの運用を停止する場合等においては、サービスの提供を終了することがあります。その場合、本サービスの終了に伴い、本 GPS は無効化されます。

9-10-3. 終了によって無効化される事項、及び継続する事項

本サービスが終了し、本 GPS が無効化された場合においても、9-3節及び 9-4節で規定され

た項目の効力は存続するものとします。

9-11. 関係者間の連絡方法

本認証局から利用者への連絡は原則として電子メールにて行うものとします。また、利用者全般に対して行われる連絡は電子メールの他、リポジトリ上にも公開されます。なお、利用者から本認証局に連絡を行う必要がある場合は 1-5-2項で規定された連絡先に連絡を行うものとします。

9-12. CPS の改訂

本節では本 CPS の改訂手続きについて規定します。

9-12-1. CPS の改訂手続き

本 CPS は、本認証局が必要と考える場合は、利用者または信頼者に事前の了承なく改訂を行う場合があります。改訂の通知は電子メール及びリポジトリを通じて行います。改訂の通知から改訂が有効になるまでの期間に改訂に対する異議の申出がない場合は、改訂に対する合意が得られたものとします。改訂に対し合意できない関係者においては、即時に本認証局から発行された証明書の使用を中止するものとします。

9-12-2. CPS の改訂通知方法及び実施時期

本認証局が本 CPS の改訂を行う場合は、本 CPS の改訂を行う旨を利用者に電子メールで周知するとともに、改訂された CPS が有効となる 30 日以上より前にリポジトリに公開を行います。

9-12-3. オブジェクト識別子の変更される条件

本 CPS の大幅な改訂が行われた場合は、JPCERT/CC の判断により、本 CPS に付与されるオブジェクト識別子の変更が行われることがあります。

9-13. 紛争解決手続

本サービスに関して生じた紛争についての管轄裁判所は、東京地方裁判所とします。なお、各関係者はその係争を解決するために訴訟に先立ち誠意をもって協議するものとします。

9-14. 準拠法

本 CPS の失効、解釈及び有効性は、その他の規程の有無によらず、日本国内法に従って判断されるものとします。

9-15. 適用法の遵守

規定しません。

9-16. 雑則

本節では、本 CPS に関わるその他の条項について規定します。

9-16-1. 完全合意条項

本 CPS は、本 CPS において別段の定めをしている場合を除き、書面によらず口頭で修正、放棄、追加、変更、削除または終了させることはできないものとします。

9-16-2. 権利譲渡条項

規定しません。

9-16-3. 分離条項

本 CPS の規定が、いかなる程度でも無効または執行不可能となった場合であっても本 CPS その他の項目の有効性には影響を及ぼさず、本サービス参加者の意思に最も合理的に合致するよう解釈されるものとします。

9-16-4. 強制執行条項

規定しません。

9-16-5. 不可抗力条項

以下の事象が発生した場合、本認証局は利用者及び信頼者に対し免責とします。

- (1) 地震、水害、噴火などのあらゆる天災に起因する損害
- (2) 火災、停電などのあらゆる災害に起因する損害
- (3) 戦争、動乱、及び、その他のあらゆる不可抗力に起因する損害

9-17. その他の条項

規定しません。