JPCERT/CC

WAISE 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

一般社団法人 JPCERT コーディネーションセンター

改訂履歴

Version	変更内容	日付
1.0	新規作成	2007 年 5 月 1 日
1.1	2-3 および 4-9-7 の CRL 発行頻度の記載を変更	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

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 WAISE 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続を記載したものです。これらのサービスを JPCERT/CC WAISE 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 が提供する早期警戒情報サービス内の一部のサービスとして別途 JPCERT/CC により認められた者に提供されます。

本サービスは、JPCERT/CC が管理する JPCERT/CC 脅威情報分析支援サービスにおける WAISE システムと本サービスの利用者がインターネットを経由して安全に通信を行うための仕組みを提供します。

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
1.2.392.200212.1.2	JPCERT/CC WAISE SSL クライアント証明書用認証局
1.2.392.200212.1.2.1	JPCERT/CC WAISE 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。参加者は本認証局、利用者及び信頼者から構成されます。また、本認証局は認証局、登録局、リポジトリの下位組織から構成されています。本認証局は本CPSを定め、これに従い本サービスの提供を行います。本認証局の階層構造及びJPCERT/CCが提供する他の認証局との関係については、図 2の通りです。なお、JPCERT/CCルート認証局の仕様についてはJPCERT/CC SSLクライアント証明書用認証局認証業務運用規程にて規定されています。

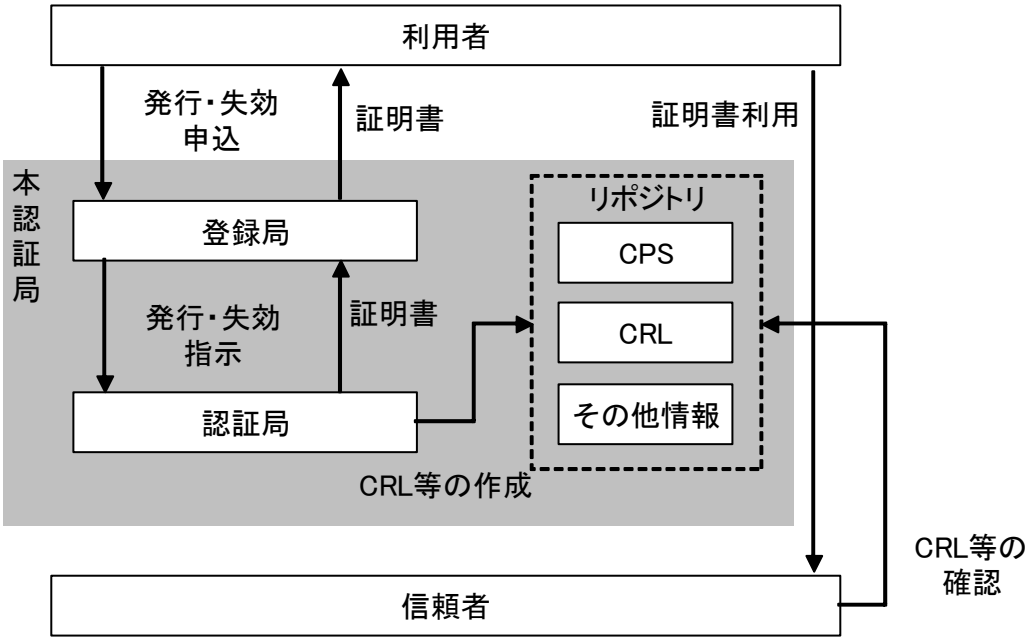

図 1　参加者の構造

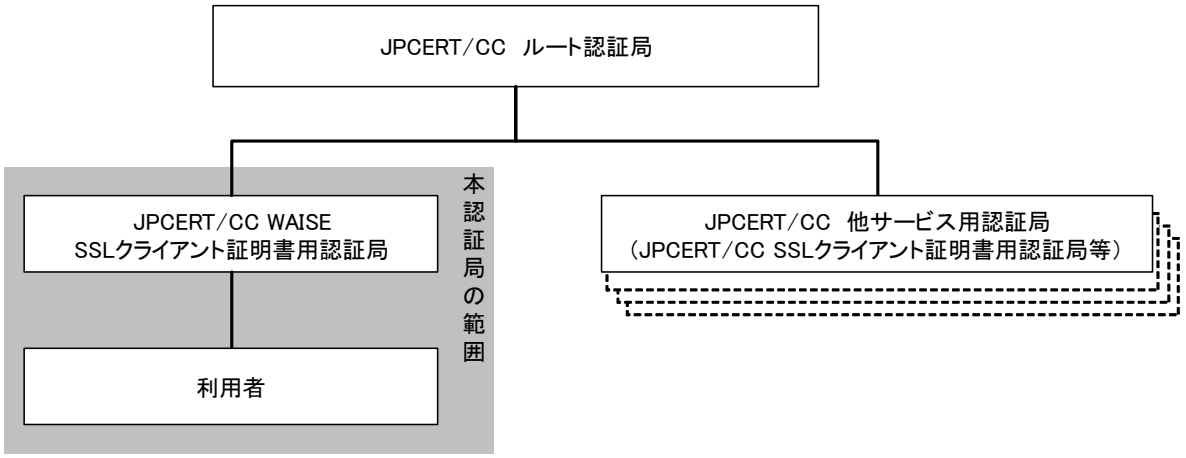

図 2　認証局の階層構造

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(「本認証局」が「認証局」、「登録局」及び「リポジトリ」を含む本サービス全体を提供する機関を示す用語であることとの違いに注意)。また、認証局は CRL 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 CPS 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、JPCERT/CC 脅威情報分析支援サービスの利用者として JPCERT/CC に登録されて、本認証局により証明書の利用が認められた者が該当します。利用者は、JPCERT/CC 脅威情報分析支援サービスを提供する WAISE 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。

JPCERT/CC は、早期警戒情報サービスを、別途 JPCERT/CC が定める基準を満たすグループ（法人、法人内の事業部、研究者個人等の場合もある。以下、総称して「利用グループ」という）として JPCERT/CC が管理する「利用グループリスト」に登録された組織に対して提供します。また、利用グループは利用グループリストに登録される際に、早期警戒情報サービスの利用等に関わる担当者（以下、担当者）を選定し、これを登録しなければなりません。なお、JPCERT/CC は JPCERT/CC 脅威情報分析支援サービスを、利用グループに所属する者に対してのみ提供します。

JPCERT/CC 脅威情報分析支援サービスの利用を希望する者は、利用グループ内の担当者と協力し JPCERT/CC 脅威情報分析支援サービスの利用に関する手続きに従い、JPCERT/CC が管理する「WAISE 利用者リスト」に登録されなければなりません。本認証局は WAISE 利用者リストに登録された者より所定の手続きが行われた場合は、証明書の発行を行います。

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、WAISE 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

本認証局は、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から WAISE 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、WAISE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 CPS 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巻末の付録を参照してください。

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。

また、リポジトリに関する物理的管理、運用上の管理、技術的セキュリティ上の管理等(5 章、6 章、8 章の内容に相当)の要件については登録局の仕様に準ずるものとします。

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/waise/jpcert-waise-cps.pdf
- 『CRL』: http://www.jpcert.or.jp/ca-info/waise/waise-crl-list.crl
- 『本認証局に関する通知』: http://www.jpcert.or.jp/ca-info/waise/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。なお、JPCERT/CC ルート認証局の名称は JPCERT/CC SSL クライアント証明書用認証局認証業務運用規程に記載されています。

表 2 JPCERT/CC WAISE 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 WAISE SSL Clients”	JPCERT/CC WAISE SSL クライアント証明書発行認証局の英語名

表 3 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 WAISE SSL Clients”	JPCERT/CC WAISE SSL クライアント証明書発行認証局の英語名
commonName	“SSL-W-999999-999999-9999a”	ハイフン(-)で区切られる cn の第 1 カラム及び第 2 カラムは、証明書利用目的である JPCERT/CC 脅威情報分析支援サービスにおける SSL クライアント認証を示した文字列。 同第 3 カラムは、JPCERT/CC が利用グループに対して任意に割り当てる 6 桁の数字。 同第 4 カラムは、JPCERT/CC が各利用グループ内の利用者に任意に割り当てる 6 桁の数字。 同第 5 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。

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、各参加者の名称として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

本節では利用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。本認証局は JPCERT/CC が管理する WAISE 利用者リストに登録されている者に対し、証明書を発行します。JPCERT/CC 脅威情報分析支援サービスの利用者として WAISE 利用者リストに登録されるためには、利用グループに所属し、かつ自グループの担当者より承諾を得た上で JPCERT/CC 脅威情報分析支援サービスの利用登録手続きを行わなければなりません。また、早期警戒情報サービスを利用するグループとして利用グループリストに登録されるためには、別途定められた早期警戒情報サービスの利用登録手続きを行わなければなりません。

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、利用者の公開鍵を、利用者本人から PKCS#10（またはそれと同等の形式）で受け取ります。

3-2-2. 組織の識別及び認証

本サービスは JPCERT/CC が管理する利用グループリストに登録されているグループに所属している個人に対してのみ証明書の発行を行います。利用グループリストに登録されているグループについては、早期警戒情報サービスの利用登録手続きの一環として JPCERT/CC により当該グループの存在確認および担当者の身元確認等の手続きが行われています。

3-2-3. 個人の識別及び認証

利用グループの担当者は、同じ利用グループに所属し、かつ WAISE 利用者リストに登録されている者が本認証局の証明書の利用を希望する場合、本認証局より WAISE SSL クライアント証明書発行申請様式を入手し、必要事項を記載した上で、本認証局に対して送付し、証明書の申請を行うことができます。当該様式には少なくとも以下の項目の記載が必要です。

- ◆ 利用グループ名
- ◆ 担当者名
- ◆ 担当者の捺印または署名（捺印の場合は JPCERT/CC に登録したものと同一印鑑による

もの。署名の場合は JPCERT/CC に登録したものと同等の形式であること）

（以下、複数名記載可能）

◆ 証明書を必要とする者の氏名

◆ 証明書を必要とする者のメールアドレス

当該様式を受領した本認証局は、当該様式上の「利用グループ名」と「担当者名」が JPCERT/CC が管理する利用グループリストに登録されていること及び「担当者の捺印または署名」が、利用グループリストに登録されている担当者の捺印または署名と同一であることの確認を行います。また、当該様式上の「証明書を必要とする者の氏名」と「証明書を必要する者のメールアドレス」が JPCERT/CC が管理する WAISE 利用者リストに登録されていることの確認を行います。これにより本認証局は証明書の発行を希望する者が、JPCERT/CC が管理する WAISE 利用者リストに登録されており、かつ担当者に証明書の利用を認められた者であることを確認します。

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、利用グループリスト及び WAISE 利用者リストに記載されている情報をもとに証明書の発行を行います。また、本認証局は 3-2-3 項で規定された内容以上の利用者の確認は実施しません。

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。本認証局は利用者の証明書の有効期間が満了する 30 日以上前に、利用者及び利用者と同じ利用グループの担当者に対し電子メールにより更新の手続きを促す案内を送ります。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。証明書を新規に発行する際の認証等の手続きは 3-2節で規定されている初回発行時の手続きと同様です。

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グループの担当者に依頼し、WAISE SSL クライアント証明書失効申請様式に必要事項を記載の上、本認証局に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。

- 利用グループ名
- 担当者名
- 担当者の捺印または署名（捺印の場合は JPCERT/CC に登録したものと同一印鑑によるもの。署名の場合は JPCERT/CC に登録したものと同等の形式であること）
- 証明書の利用者名
- 証明書の利用者のメールアドレス
- 失効を希望する証明書に関する情報（可能な範囲で記入）

本認証局では、当該様式上の「担当者の捺印または署名」が、JPCERT/CC が管理する利用グループリストに登録されている担当者の捺印または署名と同一であることの確認を行った上で、当該利用者の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）JPCERT/CC が管理する利用グループリストに担当者として登録されている者

- 担当者自身が利用する証明書
- 同じ利用グループに所属している者が利用する証明書

なお、JPCERT/CC が管理する WAISE 利用者リストに登録されている担当者以外の者が証明書の利用を希望する場合は、自グループの担当者に申請を依頼しなければなりません。

また、利用グループに所属していない者が、本サービスの利用を希望する場合は、早期警戒情報サービスの利用登録手続きに従い、自グループを JPCERT/CC が管理する利用グループリストに登録させる必要があります。利用グループに所属しているものの、JPCERT/CC が管理する WAISE 利用者リストに登録されていない者が、本サービスの利用を希望する場合は、担当者と協力のもと JPCERT/CC 脅威情報分析支援サービスの利用登録手続きに従い、本サービスに関わる手続き行う前に、自らを JPCERT/CC が管理する WAISE 利用者リストに登録させる必要があります。

4-1-2. 登録手続き及び責任

利用グループの担当者は、同じ利用グループに所属し、かつ WAISE 利用者リストに登録されている者が本認証局の証明書の利用を希望する場合、本認証局より WAISE SSL クライアント証明書発行申請様式を入手し、必要事項を記載した上で、本認証局に対して送付し、証明書の申請を行うことができます。当該様式には少なくとも以下の項目の記載が必要です。

- 利用グループ名
- 担当者名
- 担当者の捺印または署名（捺印の場合は JPCERT/CC に登録したものと同一印鑑によるもの。署名の場合は JPCERT/CC に登録したものと同等の形式であること）

（以下、複数名記載可能）

- 証明書を必要とする者の氏名
- 証明書を必要とする者のメールアドレス

4-2. 証明書申請の処理手続き

本節では証明書申請の処理手続き等について規定します。

4-2-1. 本人識別と認証の実施

本認証局が、担当者より WAISE SSL クライアント証明書発行申請様式を受領した場合、以下の確認を行います。

（1）当該様式に記載されている「利用グループ名」と「担当者名」が JPCERT/CC が管理する利用グループリストに登録されていること

（2）当該様式に記載されている「担当者の捺印または署名」が JPCERT/CC が管理する利用グループリストに登録されている担当者の捺印または署名と同一であること

（3）当該様式に記載されている「証明書を必要とする者」と「証明書を必要とする者のメールアドレス」が JPCERT/CC が管理する WAISE 利用者リストに登録されていること

上記 3 項目の確認が取れた場合、本認証局は証明書の申請を完了させるために必要な識別子及びパスワードの組み合わせを証明書を希望する者の数だけ、書面に記載し、担当者に対して配達証明付郵便にて送付します。

当該書面を受領した担当者は、自グループ内で証明書を希望していた者に対し、識別子及びパスワードを安全な方法にて配布しなければなりません。識別子及びパスワードを受領した者は本認証局が別途指定したウェブサイト上（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）にて当該識別子及び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

本認証局は本認証局が配布した識別子及びパスワードが、利用者によって本認証局が指定したウェブサイト上に入力された場合、当該情報の真正性を確認した上で、申請を承認します。また、本認証局は利用者の公開鍵等の情報を識別子及びパスワードと同時に利用者から受領し、当該情報を用いて証明書の発行を行います。利用者が間違った識別子またはパスワードを入力した場合、または当該処理を実施しなかった場合は本認証局は証明書の発行を行いません。

4-2-3. 証明書申請の処理時間

本認証局は利用者により識別子及びパスワード等の必要な情報が入力された場合、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 4-2-2項の処理が完了後、速やかに証明書の発行を行います。また、利用者が当該ウェブサイトより当該証明書をダウンロードすることが可能となるための処理を行います。

4-3-2. 認証局の利用者に対する証明書発行通知

規定しません。

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

4-3-1項で規定されたとおりに本認証局が証明書を発行した場合、利用者は直ちに証明書をダウンロードすることができます。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。

4-4-2. 認証局による証明書の公開

規定しません。

4-4-3. 他の参加者に対する認証局の証明書発行通知

規定しません。

4-5. 鍵ペアと証明書の利用用途

利用者は本認証局が発行した証明書と利用者の秘密鍵の利用に関して以下の事項を遵守しなければなりません。

（1）自身の秘密鍵を厳重に管理し、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
（2）1-4-1項で規定された証明書の利用用途を遵守すること
（3）証明書の有効期間が満了した場合、当該証明書の利用を行わないこと
（4）何らかの事由により証明書が失効した場合、証明書内に記載された公開鍵と対応する秘密鍵の利用を行わないこと

4-6. 証明書の更新

本認証局が発行する証明書の有効期間は 1 年間です。証明書の有効期間満了に伴う、証明書の更新手続きは証明書初回発行時の手続きと同様です。本認証局は利用者の証明書の

有効期間が満了する 30 日以上前に、利用者及び利用者と同じ利用グループの担当者に対し電子メールにより更新の手続きを促す案内を送ります。

4-7. 鍵ペア更新による証明書の更新

証明書の失効等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、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、自グループの担当者に依頼し、再度 WAISE SSL クライアント証明書発行申請様式を本認証局に対して送付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項に規定した通りに、利用者を識別することのみを目的とした情報です。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

本認証局が発行した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）利用者の所属するグループが、JPCERT/CC が管理する利用グループリストから除名されたとき
（５）利用者が、JPCERT/CC が管理する WAISE 利用者リストから除名されたとき
（６）その他、本認証局が必要と認めたとき

なお、秘密鍵の危殆化等の理由により利用者が証明書の緊急な失効を希望する場合は、4-9-12項で規定された緊急に証明書の失効を行うための手続きが適用されます。

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）利用グループの担当者
（２）本認証局

担当者以外の者が証明書の失効を希望する場合は、自グループの担当者に申請を依頼し

なければなりません。また、本認証局による具体的な失効手続きについては本 CPS において規定しません。

4-9-3. 失効申請手続き

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グループの担当者に依頼し、WAISE SSL クライアント証明書失効申請様式に必要事項を記載の上、本認証局に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。

- 利用グループ名
- 担当者名
- 担当者の捺印または署名（捺印の場合は JPCERT/CC に登録したものと同一印鑑によるもの。署名の場合は JPCERT/CC に登録したものと同等の形式であること）
- 証明書の利用者名
- 証明書の利用者のメールアドレス
- 失効を希望する証明書に関する情報（可能な範囲で記入）

本認証局では、当該様式上の「担当者の捺印または署名」が、JPCERT/CC が管理する利用グループリストに登録されている担当者の捺印または署名と同一であることの確認を行った上で、当該利用者の証明書の失効を行います。なお、利用者によって提供された情報によって失効対象の証明書が一意に判別できない場合は、当該利用者が所有する全ての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

WAISE 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

信頼者は利用者が提出した証明書を信頼する前に、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わなければなりません。

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

利用者自身が所有する秘密鍵が危殆化したとき、危殆化したと判断するにたる状況にあるとき、または緊急に証明書を失効が必要と判断した場合、利用者は自グループの担当者に依頼し、速やかに、WAISE SSL クライアント証明書失効申請様式を必要事項記載の上で、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 が管理する利用グループリストに記載されている当該担当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、担当者は当該様式を 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. 証明書の一時停止が行われる状況

規定しません。

4-9-14. 証明書の一時停止を要求できる者

規定しません。

4-9-15. 証明書の一時停止要求の手続き

規定しません。

4-9-16. 証明書の一時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終了を希望する利用グループは、担当者により自グループに所属する利用者が所有する全ての証明書の失効申請を、4-9節で規定された手続きに従って行わなければなりません。また、何らかの理由により利用グループがJPCERT/CCが管理する利用グループリストから除名された場合は、本認証局は当該利用グループ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。

また、何らかの理由により本サービスの利用の終了を希望する利用者は、自グループの担当者に依頼し、自身が所有する証明書の失効申請を、4-9節で規定された手続きに従って、行わなければなりません。また、何らかの理由により利用者がJPCERT/CCが管理するWAISE利用者リストから除名された場合は、本認証局は当該利用者が所有する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、認証局の運営に関係す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能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

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

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、利用グループの担当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、原則とし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。その様な場合においても、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に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

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

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項で規定されている監査ログ
- 証明書申請に関する情報
  - WAISE 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
  - WAISE 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項で規定された通り
◆ 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、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。また、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項で規定されたように、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が設けられています。本番センタの被災時は、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（または同等）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方法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（参考）: 1024bit の RSA
- JPCERT/CC WAISE 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

本認証局の秘密鍵は、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
- 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。ただし、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厳重に保管されます。

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。

6-4-3. 活性化データの他の考慮点

規定しません。

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 4 JPCERT/CC WAISE 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 WAISE 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 5 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 WAISE 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366日
subject （主体者名）	o=Japan Computer Emergency Response Team Coordination Center ou = JPCERT/CC CA for WAISE SSL Clients cn = SSL-W-**999999-999999-9999a**	PrintableString で記載 太字部分は利用者ごとの可変値
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/waise/waise-crl-list.crl	
netscapeCertType (2.16.840.1.113730.1.1)	FALSE	SSL client	
certificatePolicies （証明書ポリシー）	FALSE	PolicyIdentifier: OID=1.2.392.200212.1.2.1 PolicyQualifier: ID=CPS URI=http://www.jpcert.or.jp/ca-info/waise/waise-jpcert-cps.pdf	

なお、JPCERT/CC ルート認証局の証明書については、JPCERT/CC SSL クライアント証明書用認証局認証業務運用規程に記載されています。

7-2. CRL のプロファイル

表 6 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 WAISE SSL Clients	PrintableString で記載
lastUpdate （今回更新日時）	YYMMDDHHMMSSZ	UTCTime で記載
nextUpdate （次回更新日時）	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）	…	領域が割り当てられない場合もある

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

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

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

本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）利用グループリスト
（２）WAISE 利用者リスト
（３）証明書申請に関わる記録
（４）失効申請に関わる記録
（５）パスワードが記載された書面または電子データ
（６）偶発事故に対する災害復旧計画
（７）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
（８）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

本認証局は 9-3-1項に拘らず、下記の情報を秘密情報として扱いません。

◆ 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 で取り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こととします。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 9-4節で規定された内容に従います。

9-4. 個人情報の保護

本認証局は、以下の URL にて記載されている JPCERT/CC が保持する個人情報保護方針に従って、本サービスを提供する際に取り扱う個人情報の保護を行います。

『個人情報保護方針』: http://www.jpcert.or.jp/privacy.html

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。

◆　証明書及び自身の秘密鍵を利用する前に JPCERT/CC 脅威情報分析支援サービスの利用規約に同意していること
◆　1-4-1項 で規定された証明書用途を遵守すること
◆　証明書申請の際に同じ利用グループの担当者を通じて、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、同じ利用グループの担当者に依頼し本認証局に対し、直ちに証明書の失効申請を行うこと
◆　証明書の有効期間が満了した場合、当該証明書の利用を行わないこと
◆　何らかの事由により証明書が失効した場合、証明書内に記載された公開鍵と対応する秘密鍵の利用を行わないこと

また、利用グループの担当者は証明書申請の際に、本認証局に対し提供した利用者に関する情報が正確であることを保証しなければなりません。

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前に、本認証局に関する有効な認証局証明書を誤り無く入手すること
◆　利用者が提出した証明書を信頼する前に、当該証明書に付与されている電子署名が、本認証局によって作成されていることを検証すること
◆　利用者が提出した証明書を信頼する前に、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 CPS 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

JPCERT/CCは、利用者または担当者が 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、第三者に対し一切の責任を負わないものとします。利用者または担当者が 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 CPS 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 CPS 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。

また、9-6-1項及び 9-6-2項に関し、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、津波、洪水、落雷、火災、水災、停電、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 CPS 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 CPS は本サービスが継続する限り有効であるとします。本 CPS の改訂が行われた場合は、最も新しく改訂された CPS が有効なものであるとします。

9-10-2. 終了

本サービスは、JPCERT/CC が WAISE システムの運用を停止する場合等においては、サービスの提供が終了されることがあります。その場合、本サービスの終了に伴い、本 CPS 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CPS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される場合があります。本認証局が軽微と判断する本 CPS の変更（誤記の訂正、リンク先の変更）を行う際は、改訂された CPS がリポジトリ上に掲載された段階で当該改訂内容は有効なものとします。また、本認証局が軽微ではないと判断する CPS の改訂を行う場合は、関係者に対し電子メール及びリポジトリを通じて通知を行います。改訂の通知から改訂が有効になるまでの猶予期間内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

本認証局が軽微と判断する本 CPS の改訂が行われる場合、本認証局が改訂された CPS をリポジトリに掲載した段階で当該 CPS は有効なものとします。また、本認証局が軽微ではないと判断する本 CPS の改訂が行われる場合、本認証局は改訂に関する通知を関係者に電子メール及びリポジトリを通して、当該 CPS が有効になる 30 日以上前に行うものとします。

9-12-3. オブジェクト識別子が変更される条件

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 に割り当てら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 の執行、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

利用者は、本サービスにおいて本認証局から認められた権利を、如何なる理由においても、他人に譲渡、貸付または担保にしてはなりません。

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

以下の事象に起因する損害が発生した場合、本認証局は利用者及び信頼者に対し免責とします。

（１）天変地異、地震、噴火、津波、洪水、落雷などのあらゆる天災

（２）火災、水災、停電などのあらゆる災害

（３）戦争、動乱、テロリズム及びその他のあらゆる不可抗力

9-17. その他の条項

規定しません。

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)	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。 以下のようなレベルが規定されている。 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。 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。 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。 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。
HSM （ Hardware Security Module：ハードウェアセキュリティモジュール）	ハードウェアによる秘密鍵の管理装置。 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。 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。 【暗号モジュール】と同義。
JPCERT コーディネーションセンター	JPCERT コーディネーションセンター（JPCERT/CC）は、日本を代表するインシデント対応組織（CSIRT：Computer Security Incident Response Team）として、国内外から届くインシデント報告の対応を中心とした情報セキュリティ対策活動のコーディネーションを行っている。特に、アジア太平洋地域においては、CSIRT 間の情報交換網の構築や組織の設立支援活動等を主導して、積極的に各地域の対策活動を支援している。
JPCERT/CC 脅威情報分析支援サービス	JPCERT/CCが提供する早期警戒情報サービスを利用するユーザに対して、早期警戒情報を提供するためのサービス。
JPCERT/CC 脅威情報分析支援サービスの利用規約	JPCERT/CC 脅威情報分析支援サービスにおいて、当該サービスの利用者が守るべき事項等が記載された規約
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。
WAISEシステム	JPCERT/CC脅威情報分析支援サービスを提供するためのシステム
WAISE利用者リスト	早期警戒情報サービスの提供を受ける利用グループの担当者が、WAISEサービスの利用に関する手続きを行った際にJPCERT/CCにより登録されるWAISE利用者のリスト。
【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、監査対象の管理者に報告される。
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、これはトラストアンカ認証局証明書（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。
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。
早期警戒情報サービス	JPCERT/CCが日本における重要なシステムを管理・運用しているグループの担当者に必要な情報を提供するサービス。
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。
利用グループ	JPCERT/CCが定める基準を満たし、早期警戒情報サービスの提供を受けるグループ
利用グループリスト	JPCERT/CCが定める基準を満たし、早期警戒情報サービスの提供を受けるグループのリスト
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。