PKI プラットフォーム認証局運用規程

(Certification Practice Statement)

Version 3.8

2022 年 4 月 1 日

変更履歴

バージョン	変更年月日	変更点	承認者
1.0	2004 年 6 月 1 日	初版	ポリシー承認局
2.0	2005 年 10 月 3 日	第 2 版　対応サービス追加	ポリシー承認局
3.0	2006 年 10 月 1 日	第 3 版　社名変更	ポリシー承認局
3.1	2008 年 2 月 4 日	自動インポート/更新、閉域網接続、有効期間変更対応	ポリシー承認局
3.2	2011 年 9 月 12 日	CDP 更新	ポリシー承認局
3.3	2012 年 6 月 25 日	一時停止対応	ポリシー認証局
3.4	2013 年 3 月 22 日	設備更新	ポリシー認証局
3.5	2015 年 4 月 1 日	社名変更	ポリシー認証局
3.6	2015 年 7 月 1 日	社名変更	ポリシー認証局
3.7	2015 年 8 月 24 日	SHA-256 変更対応	ポリシー認証局
3.8	2022 年 4 月 1 日	個人情報保護法改正	ポリシー認証局

目　　次

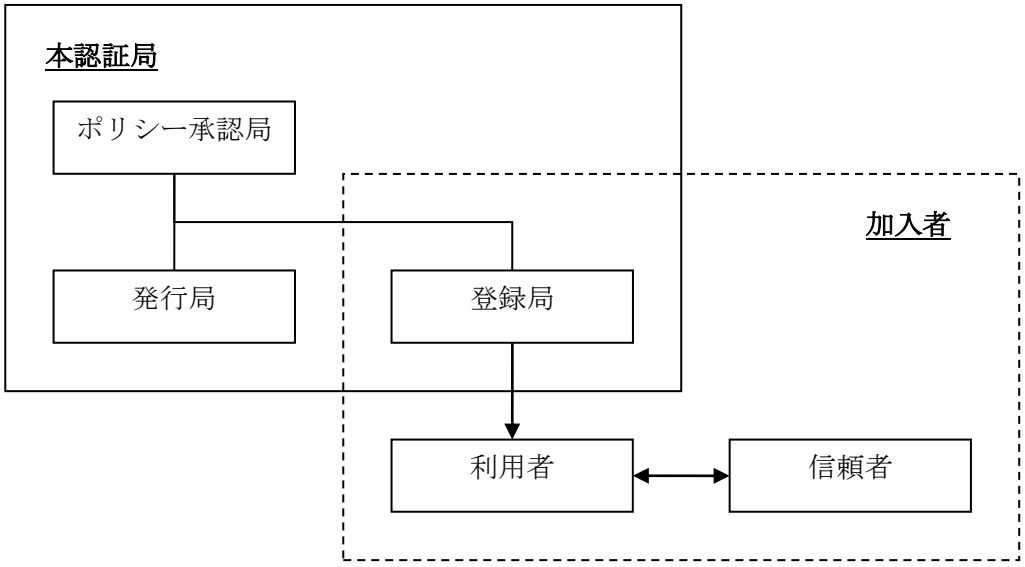
１．　はじめに

ソフトバンク株式会社は、PKI プラットフォーム（以後、「本サービス」という）として、PKI プラットフォーム認証局（以後、「本認証局」という）を設置し、本認証局による電子証明書（以後、「証明書」という）の発行を行う。

１．１　概要

本文書は、本サービスに係る認証業務を行う際の運用に関する規定（CPS: Certification Practice Statement、以後、「本 CPS」という）であり、発行局および登録局を含む本認証局の運用方針、加入者・利用者と本認証局との関係、本認証局が発行する証明書の取り扱い等について規定する。証明書の取り扱いについては、申請・登録・発行・更新・再発行・失効・有効期間満了に関する記述が含まれる。本認証局が発行する利用者証明書の発行方針および利用に関連する要件は、各利用者証明書の証明書ポリシー（以後、「各証明書の CP」という）として、本 CPS とは分けて規定する。

本認証局およびその関係者について下記の図に示す。



本サービスの利用に関しては、ソフトバンク株式会社と加入者との間に別途、本サービスに係る契約（以後、「本サービス契約」という）が定められるが、本サービス契約は、本 CPS に同意の上締結されるものとする。

定義と略称については、本 CPS １０．　に規定する。

本 CPS は、IETF PKIX ワーキンググループによる RFC 3647「Certificate Policy and Certification Practices Statement Framework」を基礎にして記述される。

１．２　文書名称と定義

本 CPS の正式名称を、「PKI プラットフォーム認証局運用規程」とする。

１．３　PKI の関係者

下記の PKI の関係者は、本 CPS に同意し、本 CPS の義務を遵守しなければならない。

１．３．１　ポリシー承認局

本認証局に係る最高意思決定機関であり、本認証局のポリシーの決定や承認、本 CPS 等重要ドキュメントの変更の承認などを行う。

１．３．２　発行局

登録局の登録・削除および当該登録局からの申請に従った利用者証明書の発行・失効を行う。この他、本認証局自身の証明書である自己署名証明書および本認証局の運用上必要となるオペレータ証明書の発行管理等を行う。登録局の申請により、利用者鍵ペアの生成、利用者証明書の USB トークンへの発行および当該 USB トークンの配送の業務を行う場合もある。

１．３．３　登録局

登録局は、本サービス契約の下、加入者毎に設置され、証明書利用申請や失効申請に対する審査・登録、発行局に対する証明書の発行・失効の申請等を行う。
また、利用者からの問い合わせ等に対する一次窓口対応を行う。

１．３．４　加入者

加入者は、本サービス契約の契約主体である法人等であり、自らが管理する利用者に対し、ソフトバンク株式会社から提供を受ける本サービスの利用の許可を行う。

１．３．５　利用者

利用者については、各証明書の CP に規定する。

１．３．６　信頼者

信頼者については、各証明書の CP に規定する。

１．３．７　その他の関係者

規定しない。

１．４　証明書の用途

１．４．１　証明書の種類

本認証局は、次の証明書を発行する。

(1)　自己署名証明書

本認証局の証明書であり、自身の公開鍵に対して本認証局の秘密鍵で電子署名をしたもの。本認証局の秘密鍵は、利用者証明書、オペレータ証明書、CRL/ARL への電子署名の用途に使用される。

(2)　利用者証明書

登録局の審査を通過した個人やサーバ機器等に対して発行される証明書。

詳細は各証明書の CP に規定する。

(3)　オペレータ証明書

発行局の審査を通過した、本認証局運用上必要な個人に対して発行される証明書。

各証明書については、本認証局の判断および管理の下、試験目的の発行・失効が行われる場合がある。

１．４．２　正規の証明書用途

本認証局が発行する証明書の用途については、各証明書の CP に規定する。

１．４．３　禁止されている証明書用途

本認証局が発行する証明書において禁止されている用途については、各証明書の CP に規定する。

１．５　ポリシー管理

１．５．１　文書の管理組織

本 CPS の管理については、ポリシー承認局が行う。

１．５．２　窓口

規定しない。

１．５．３　ポリシーに対する本 CPS の準拠性調査担当者

規定しない。

１．５．４　CPS の承認手続き

本 CPS の承認については、ポリシー承認局が行う。

２．　公開とリポジトリの責任

２．１　リポジトリ

本認証局は、本認証局に係る情報を公開するため、Web サーバを持つ。また、CRL/ARL を公開するため、WEB サーバを持つ。

２．２　認証情報の公開

本認証局は、リポジトリ（Web サーバ）にて、本 CPS を公開する。また、リポジトリ（WEB サーバ）にて、自己署名証明書および CRL/ARL を公開する。

２．３　公開の時期と周期

本認証局は、本 CPS が改訂され承認されたときは、速やかにこれを公開し、有効開始日についても明示する。また、加入者に対しては、本 CPS ９．１１　の規定に従い個別に通知する。

CRL/ARL については、本 CPS ４．９．７　で示された周期で更新、公開する。

２．４　リポジトリに対するアクセスコントロール

本認証局は、CRL/ARL を公開するためリポジトリ（WEB サーバ）に対する参照権限の制限を行わない。リポジトリ（Web サーバ）に対しては、本認証局により許可された企業管理者のみに制限する。

３．　本人性確認と認証

３．１　名称

３．１．１　名称のタイプ

本認証局が発行する利用者証明書の主体者（Subject）は、利用者証明書の中の X.500 識別名（DN）で、一意に識別される。X.500 は、ITU-T で 1988 年に規格化されたディレクトリ・サービスの勧告（国際標準）である。

３．１．２　名称の意味に関する要件

利用者証明書中の DN に含まれる第一組織名（OU）には、本サービスにおいて加入者を識別するためにソフトバンク株式会社が定めた識別子（英数字表記）を記載する。これは、利用者に発行許可した登録局の識別子と一致する。

３．１．３　利用者の匿名・仮名についての要件

規定しない。

３．１．４　様々な名称形式を解釈するためのルール

本認証局が発行する証明書の DN の形式は、X.500 に従う。

３．１．５　名称の一意性

本認証局が発行する証明書は、DN により利用者を一意に割り当てる。

３．１．６　商標等の認識、認証および役割

本認証局は、商標、ドメイン名について認証を行わない。

３．２　初回の利用者の本人性確認

３．２．１　秘密鍵の所有を検証する方法

各証明書の CP に規定する。

３．２．２　加入者の確認

本サービス契約の締結をもって加入者の確認が行われたものとする。

３．２．３　利用者の確認

利用者に対する本サービス利用の許可およびそれら利用者の管理は加入者の責任において行われ、利用者の確認は、当該管理情報をもって行なわれる。本認証局は、証明書の組織名として記載される加入者の識別子についてのみ責任を負う。

３．２．４　確認されない利用者情報

規定しない。

３．２．５　権限確認

利用者に対する本サービス利用の許可およびそれら利用者の管理は加入者の責任において行われ、権限確認は、当該管理情報をもって行なわれる。

３．２．６　相互運用性基準

規定しない。

３．３　鍵（証明書）更新申請時の本人性確認と認証

３．３．１　鍵（証明書）定期更新時の本人性確認と認証

（１）PKCS#12 形式または USB トークンでの発行

本 CPS ３．２．３　に従う。

（２）パソコンまたは USB トークンへの自動インポートでの発行

ブラウザによる証明書提示により認証を実施する。

３．３．２　失効後の鍵（証明書）再発行時の本人性確認と認証

本 CPS ３．２．３　に従う。

３．４　失効申請時の本人性確認と認証

本 CPS ３．２．３　に従う。

４．　証明書のライフサイクル

４．１　証明書申請

４．１．１　証明書利用申請者

各証明書の CP に規定する。

４．１．２　利用申請方法

各証明書の CP に規定する。

４．２　証明書申請プロセス

４．２．１　本人性確認と認証業務の実行

各証明書の CP に規定する。

４．２．２　証明書申請の承認または拒否

各証明書の CP に規定する。

４．２．３　証明書申請プロセスの時間

各証明書の CP に規定する。

４．３　証明書発行

４．３．１　証明書発行時の認証局の行動

各証明書の CP に規定する。

４．３．２　認証局から利用者への証明書発行の通知

各証明書の CP に規定する。

４．４　証明書受領

４．４．１　証明書受領確認手続き

各証明書の CP に規定する。

４．４．２　認証局による証明書の公開

各証明書の CP に規定する。

４．４．３　認証局による他の関係者に対する証明書発行の通知

各証明書の CP に規定する。

４．５　鍵ペアと証明書の利用

４．５．１　利用者による秘密鍵と証明書の利用

各証明書の CP に規定する。
利用者は、規定された用途以外に使用してはならない。

４．５．２　信頼者に対する利用者の公開鍵と証明書の利用

各証明書の CP に規定する。
信頼者は、規定された用途以外に使用してはならない。

４．６　鍵更新を伴わない証明書更新

４．６．１　鍵更新を伴わない証明書更新に関する要件

各証明書の CP に規定する。

４．６．２　証明書利用申請者

各証明書の CP に規定する。

４．６．３　証明書申請プロセス

各証明書の CP に規定する。

４．６．４　利用者への新しい証明書発行の通知

各証明書の CP に規定する。

４．６．５　証明書受領確認手続き

各証明書の CP に規定する。

４．６．６　認証局による新しい証明書の公開

各証明書の CP に規定する。

４．６．７　認証局による他の関係者に対する新しい証明書の発行の通知

各証明書の CP に規定する。

４．７　鍵更新を伴う証明書更新

４．７．１　鍵更新に関する要件

各証明書の CP に規定する。

４．７．２　新しい公開鍵に対する証明書利用申請者

各証明書の CP に規定する。

４．７．３　鍵更新における証明書申請プロセス

各証明書の CP に規定する。

４．７．４　利用者への新しい証明書発行の通知

各証明書の CP に規定する。

４．７．５　鍵更新された証明書の受領確認手続き

各証明書の CP に規定する。

４．７．６　鍵更新された証明書の公開

各証明書の CP に規定する。

４．７．７　鍵更新された証明書の他の関係者に対する発行の通知

各証明書の CP に規定する。

４．８　証明書の変更

４．８．１　証明書の変更に関する要件

各証明書の CP に規定する。

４．８．２　証明書変更申請者

各証明書の CP に規定する。

４．８．３　証明書変更申請プロセス

各証明書の CP に規定する。

４．８．４　利用者への新しい証明書発行の通知

各証明書の CP に規定する。

４．８．５　変更された証明書の受領確認手続き

各証明書の CP に規定する。

４．８．６　変更された証明書の公開

各証明書の CP に規定する。

４．８．７　変更された証明書の他の関係者に対する発行の通知

各証明書の CP に規定する。

４．９　証明書の失効と一時停止

４．９．１　失効の要件

本認証局は、下記の事由により当該証明書の失効を行う。

(1)　利用者による失効事由

（ア）　利用者の秘密鍵が危殆化もしくは危殆化の可能性がある場合

（イ）　利用者証明書の記載内容に変更の必要が生じた場合

（ウ）　利用者が本サービスの利用を中止する場合

(2)　代表者が存在する場合、代表者による失効事由

（ア）　利用者の秘密鍵が危殆化もしくは危殆化の可能性があることを知り得た場合

（イ）　利用者証明書の記載内容に変更の必要が生じたことを知り得た場合

（ウ）　利用者が本サービスの利用を中止することを知り得た場合

(3)　登録局による失効事由

（ア）　利用者の秘密鍵が危殆化もしくは危殆化の可能性があることを知り得た場合

（イ）　利用者から USB トークンの動作不良の申し立てがあった場合

（ウ）　利用者証明書の記載内容に誤りがある場合

（エ）　その他、登録局が必要と判断した場合

(4)　発行局による失効事由

（ア）　利用者の秘密鍵が危殆化もしくは危殆化の可能性があることを知り得た場合

（イ）　加入者との本サービス契約が終了した場合

（ウ）　本認証局の秘密鍵が危殆化もしくは危殆化の可能性がある場合

（エ）　本認証局が認証業務を廃止する場合

（オ）　利用者証明書の記載内容に誤りがある場合

（カ）　その他、発行局が必要と判断した場合

４．９．２　失効申請者

失効申請者は、当該証明書の利用・更新申請を行った者とする。ただし、当該申請者の異動・退職・死亡など、当該申請者が失効申請を行えない場合、本サービスについて当該利用者を管理する加入者は、他の代表者をして、失効申請を行わせなければならない。

４．９．３　失効申請プロセス

利用者証明書の失効申請については、書類不備等を確認し、登録局が受理する。その後登録局は、申請者の正当性および申請内容を確認した上で、当該失効申請を承認する。定められた失効申請以外の方法による申請であった場合や申請内容に疑義が生じた場合は､失効申請を拒否する。

４．９．４　失効申請までの猶予期間

失効申請者は、本 CPS ４．９．１　に定める事由が発生した場合、遅滞なく申請を行わなければならない。

４．９．５　失効申請プロセスの時間

本認証局は、失効申請を受領後、証明書の失効を行う。

４．９．６　信頼者による失効情報確認の要件

信頼者は、リポジトリにて公開される CRL/ARL により、証明書の失効情報を確認しなければならない。

４．９．７　CRL 発行周期

本認証局は、CRL/ARL の発行を 24 時間以内に行う。

４．９．８　CRL がリポジトリに格納されるまでの最大遅延時間

本認証局は、発行した CRL/ARL を遅滞なくリポジトリにて公開する。

４．９．９　オンラインでの証明書の有効性確認

本認証局は、CRL/ARL を証明書の失効情報確認の手段として提供する。
有効期間の満了した証明書の失効情報確認についての問い合わせには応じない。

４．９．１０　オンラインでの証明書の失効情報確認要件

規定しない。

４．９．１１　その他の利用可能な失効情報確認の手段

本認証局は、CRL/ARL 以外の失効情報確認の手段を提供しない。

４．９．１２　鍵の危殆化の特別な要件

規定しない。

４．９．１３　一時停止の要件

本 CPS ４．９．１　に従う。

４．９．１４　一時停止申請者

一時停止申請者は、当該証明書の利用・更新申請を行った者とする。

４．９．１５　一時停止申請の手続き

利用者は、本 CPS ４．９．１　に従い、秘密鍵の危殆化、もしくは危殆化の可能性がある場合、本認証局に対し、失効申請もしくは、一時停止申請の手続きを行わなければならない。

４．９．１６　一時停止可能な期間

規定しない。

４．１０　証明書ステータス確認サービス

本認証局は、証明書ステータス確認サービスを提供しない。

４．１０．１　運用上の特徴

規定しない。

４．１０．２　サービスの可用性

規定しない。

４．１０．３　他の特徴

規定しない。

４．１１　認証局への登録の終了

利用者は、証明書の利用を中止する場合、当該利用者の鍵ペアおよび証明書の抹消、もしくはUSB トークンの廃棄を行わなければならない。

また、証明書が有効である場合、当該証明書の失効申請を行わなければならない。

４．１２　鍵預託とリカバリ

４．１２．１　鍵預託とリカバリのポリシーと手順

本認証局は、鍵預託および鍵のリカバリを行わない。

４．１２．２　セッションキーのカプセル化・復旧のポリシーと手順

規定しない。

５．　設備、管理、運用統制

５．１　物理的な管理

５．１．１　施設の所在と構造

本認証局に係る施設は、水害、地震および火災その他の災害による影響を容易に受けない場所に設置され、建物構造上、耐震、耐火および不正侵入防止対策が講じられる。また、使用する機器、装置類は、災害および不正侵入から防護された安全な場所に設置される。

なお、本施設は、建築物の外部および建築物内に本認証局の所在を明示または暗示する名称を看板もしくは表示板等により一切掲示しない。

５．１．２　物理的アクセス

本認証局に係る施設は、入退館等に際して資格審査が行われ、識別証等により入退出が管理される。また、行われる認証業務の重要度に応じ、同業務を行う各室に対し、複数のセキュリティレベルで入退室管理が行われる。

認証には、各室内において行われる認証業務の重要度に応じ、操作権限者が識別できるICカード認証等が用いられる。

各室への入退室権限は、本 CPS ５．２．１　において定める各要員の業務に応じて、認証局責任者の承認を得た者に付与される。

建物内および各室内は、別個の監視システムおよび監視要員により、24 時間 365 日監視が行われる。

５．１．３　電源設備と空調設備

本認証局に係る施設は、機器類の運用のために十分な容量の電源が確保され、瞬断、停電、電圧・周波数の変動に備えた対策が講じられている。商用電源が供給されない事態においては、自家発電機による電源供給に切り換えられる。

２重化された空調設備により機器類の動作環境および要員の作業環境は適切に維持される。

５．１．４　水害対策

本認証局に係る施設は、水害による影響を容易に受けない場所に設置される。

また、建物および各室に漏水検知器が設置され、天井、床には防水対策が講じられている。

５．１．５　火災に対する予防措置と対策

本認証局に係る施設は、建物は耐火構造、各室は防火区画とし、窒素ガス消火設備を備える。

５．１．６　地震に対する予防措置と対策

本認証局に係る施設は、現行の建築基準法に規定する構造上の安全を有する。　建物は、新耐震規準に基づいた耐震構造にて設計している。各室は耐震装置設備を備える。

５．１．７　媒体保管場所

バックアップデータを含む媒体、および USB トークン等は、適切に入退出管理された室内に設置する施錠可能な保管庫に保管するとともに、適切に搬入出管理を行う。

５．１．８　廃棄物処理

秘密情報を含む書類・媒体等の廃棄については、適切に廃棄処理を行う。

５．１．９　オフサイトバックアップ

規定しない。

５．２　職務統制

５．２．１　信頼される役割

信頼される役割としては、下記のものが挙げられるがこれらに限定されない。

(1)　ポリシー承認局

本認証局におけるポリシーの決定、承認、CPS 等の重要ドキュメントの変更、承認等を行う最高意思決定機関である。

(2)　認証局責任者

認証局責任者は本認証局を統括し、業務管理責任者および認証局運用責任者を管理する。

(3)　業務管理責任者

本認証局の発行局に係る業務を統括し、業務オペレータを管理する。

(4)　業務オペレータ

本認証局の発行局に係る業務を行う。

(5)　認証局運用責任者

本認証局に係るシステムの運用・保守および鍵管理業務を統括し、認証局運用担当者および認証局保守担当者を管理する。

(6)　認証局運用担当者

本認証局に係るシステムの運用および鍵管理を行う。

(7)　認証局保守担当者

本認証局に係るシステムにて用いられるマシン等の保守を行う。

(8)　企業管理者

本認証局の登録局に係る業務を行う。登録局側窓口として、利用者からの問い合わせにも対応する。

(9)　加入者

本サービス契約の契約主体である法人等で、利用者の管理を行う。

(10)　サポート窓口・サービス障害窓口

企業管理者からの問い合わせ対応業務を行う。

(11)　業務監査担当者

本認証局とは独立した組織で監査を行う。

５．２．２　役割ごとに必要な人員の数

下記の役割については少なくとも 2 名の職員が個々の役割に従事するように組織される。

(1)　認証局運用担当者

(2)　認証局保守担当者

(3)　業務オペレータ

５．２．３　各役割における本人性確認と認証

各担当者がシステム操作を行う際には、本認証局に係るシステムは、担当者が正当な権限者であることの識別・認証を行う。

５．２．４　職務の分離が要求される役割

下記の業務については、兼務することができない。

(1)　ポリシー承認局の代表者
(2)　認証局責任者
(3)　業務管理責任者
(4)　業務オペレータ
(5)　認証局運用責任者
(6)　認証局運用担当者
(7)　企業管理者
(8)　業務監査担当者

５．３　人事面の管理

５．３．１　経歴、資格、経験などに関する要求事項

発行局業務に従事する全ての職員は、ソフトバンク株式会社の職務規定に基づき、審査、教育、配置転換等が行われる。また、登録局業務に従事する全ての職員は、加入者の職務規定に基づき審査、教育、配置転換等が行われる。

５．３．２　身元調査手続き

規定しない。

５．３．３　教育訓練要件

本認証局は、本認証局の運用を行う要員に対し、必要に応じて、その業務に応じた知識・技術情報の提供または教育訓練を行う。

５．３．４　教育訓練の周期

本 CPS ５．３．３　に従う。

５．３．５　ジョブローテーションの周期と順序

ソフトバンク株式会社もしくは加入者の職務規定に従うものとする。

５．３．６　許可されていない行動に対する罰則

過失､故意に関わらず運用手順書に定める手続きおよび本 CPS に記載されるポリシーと手続きに違反した場合、その職員は本認証局職員としての権限を剥奪される。

５．３．７　職員に対する契約要件

通常、本認証業務に従事する職員は、ソフトバンク株式会社の社員、加入者の社員、もしくは業務委託会社の社員である。原則として、本認証局の職員は秘密保持契約を書面で結ばなければならない。ただし、加入者もしくは業務委託会社の職員については、ソフトバンク株式会社と加入者もしくは業務委託会社との間で本サービス契約にて秘密保持を締結するものとし､加入者もしくは業務委託会社がその職員に対して秘密保持義務を遵守させるものとする。

５．３．８　職員が参照できるドキュメント

本認証業務に従事する職員は、運用手順書等、業務に係るドキュメントをその役割に応じて参照することができる。

５．４　監査ログの手続き

５．４．１　記録されるイベントの種類

本認証局における業務およびセキュリティに関する重要な事象を対象に､アクセスログや操作ログ等監査ログを記録する。

５．４．２　監査ログを処理する頻度

監査ログは、機能不全、脆弱性または悪意の行動を検出する目的で、最低でも１ヶ月に一度行う。

５．４．３　監査ログの保持期間

監査ログは、2 年間保持する。

５．４．４　監査ログの保護

監査ログには、アクセス制御を施す。監査ログのバックアップは日次で外部記憶媒体に取得し、適切な入退出管理が行われている室内に設置された施錠可能な場所に保管する。

５．４．５　監査ログのバックアップ手続き

監査ログは日次でバックアップおよび外部記憶媒体に取得する。

５．４．６　監査ログ収集システム（内部、外部）

監査ログの収集機能は本認証局のシステムの一機能とし、業務およびセキュリティに関する重要な事象をシステムの起動時から監査ログとして収集する。

５．４．７　当事者に対する通知

監査ログの検査は、事象を発生させた者に通知することなく行う。

５．４．８　脆弱性評価

インターネット等の外部システムからの接続を許可されているシステムについては、定期的に脆弱性評価を行う。また、その評価結果を文書化し保管する。

５．５　アーカイブ

５．５．１　アーカイブの種類

下記の情報を含むアーカイブを保存する。

(1)　利用申請データ・失効申請データ
(2)　証明書
(3)　CRL/ARL
(4)　監査報告書
(5)　本サービス申込書

５．５．２　アーカイブの保持期間

アーカイブは、30ヶ月保持する。

５．５．３　アーカイブの保護

本 CPS ５．４．４　と同一とする。

５．５．４　アーカイブのバックアップ手続き

アーカイブは、電子媒体の場合、日次でバックアップおよび外部記憶媒体に取得する。

５．５．５　アーカイブの日付要件

アーカイブは、電子媒体の場合、レコード単位でタイムスタンプを付与する。紙媒体の場合は、同媒体中に日付を記載する。

５．５．６　アーカイブ収集システム（内部、外部）

本 CPS ５．４．６　と同一とする。

５．５．７　アーカイブ情報の入手と検証手続き

アーカイブが記録された外部記憶媒体は、本 CPS ５．５．２　で規定される保時期間内はアクセスできるように保持する。

５．６　認証局の鍵更新

本認証局は鍵ペアの更新は行わず、認証局の証明書の有効期間を延長する手続きをする。

５．７　危殆化、災害からの復旧

５．７．１　認証局秘密鍵の危殆化および災害からの復旧手続き

本認証局の秘密鍵が危殆化した場合は、本 CPS ５．７．４　に規定する業務継続計画に基づき、下記を行うと同時に、利用者・加入者・信頼者への周知を図る。

(1)　本認証業務の停止
(2)　全証明書の失効
(3)　本認証局の秘密鍵の破棄および再作成
(4)　証明書の再発行

本認証局が罹災した場合には、本 CPS ５．７．４　に規定する業務継続計画に基づき、バックアップ用のハードウェア、ソフトウェア、データ等により、遅滞なく復旧作業を行い、運用を再開する。併せて、利用者・加入者・信頼者への周知を図る。

５．７．２　ハードウェア、ソフトウェア、データの障害時の手続き

ハードウェア、ソフトウェア、データが破壊された場合には、バックアップ用のハードウェア、ソフトウェア、データにより、遅滞なく復旧作業を行う。

５．７．３　利用者秘密鍵危殆化時の手続き

本認証局は、利用者の秘密鍵には関知しない。

利用者は、本 CPS ４．９．１　に従い、秘密鍵の危殆化、もしくは危殆化の可能性がある場合、本認証局に対し、失効申請を行わなければならない。

５．７．４　認証局秘密鍵の危殆化および災害後の事業継続性

本認証局は、秘密鍵の危殆化および災害に対する業務継続計画を定める。

５．８　認証局の業務終了

本認証局は、業務終了の３ヶ月前までにその旨、および関連する事項を公開する。

業務終了は、本認証局が定める業務終了手続きに従い行なわれる。

６．　技術面のセキュリティ管理

６．１　鍵ペア生成と導入

６．１．１　鍵ペアの生成

本認証局の鍵ペアは、認証局責任者の管理の下、認証局運用担当者により FIPS 140-1 レベル 4 の秘密鍵管理モジュール（HSM）を用いて生成される。

利用者については、各証明書の CP に規定する。

６．１．２　利用者への秘密鍵の配送

各証明書の CP に規定する。

６．１．３　本認証局への公開鍵の配送

各証明書の CP に規定する。

６．１．４　信頼者への認証局公開鍵の配送

信頼者への本認証局の公開鍵の配送は行わない。自己署名証明書は、リポジトリで公開する。

６．１．５　鍵長

本認証局が発行する自己署名証明書に係る鍵は、下記の仕様に適合する鍵を利用する。利用者証明書については、各証明書の CP に規定する。

(1)　署名方式　：　SHA-1withRSA、SHA-2withRSA

(2)　合成数　：　2048 bit

６．１．６　公開鍵パラメータ生成および検査

規定しない。

６．１．７　鍵用途（X.509 v3 key usage フィールド）

本認証局の秘密鍵は署名に用いる。利用者証明書については、各証明書の CP に規定する。

６．２　秘密鍵保護と秘密鍵管理モジュール技術の管理

６．２．１　秘密鍵管理モジュールの標準と管理

本認証局の鍵ペアは、FIPS 140-1 レベル 4 の秘密鍵管理モジュールにて保護される。上記のモジュールは、認証局運用担当者により管理される。

６．２．２　秘密鍵の複数人管理 (n out of m)

本認証局の秘密鍵の管理は、複数人の認証局運用担当者により行われる。

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

本認証局の秘密鍵のバックアップは、認証局運用担当者により行われる。

秘密鍵管理モジュールからバックアップした本認証局の秘密鍵は､暗号化して複数に分割し、施錠可能な保管庫にて安全に保管する。

６．２．５　秘密鍵のアーカイブ

本認証局は、本認証局の秘密鍵のアーカイブを行わない。

６．２．６　秘密鍵管理モジュールへまたはからの秘密鍵の転送

秘密鍵管理モジュールの故障など､秘密鍵の復元が必要な場合､認証局責任者の管理の下、認証局運用担当者により、本 CPS ６．２．４　で取得したバックアップを用いて秘密鍵の復元を行う。

６．２．７　秘密鍵管理モジュール内での秘密鍵保存

本認証局の秘密鍵は、秘密鍵管理モジュール内で生成される。秘密鍵管理モジュール内では、暗号化されて保存される。

６．２．８　秘密鍵の活性化

本認証局の秘密鍵は､本認証局起動手順において､認証局運用担当者の下､活性化される。

６．２．９　利用者秘密鍵の非活性化

本認証局の秘密鍵は、本認証局停止手順において、認証局運用担当者の下、非活性化される。

６．２．１０　秘密鍵破壊の方法

本認証局の秘密鍵は、認証局運用担当者により、秘密鍵管理モジュールから完全に削除される。

また、本認証局の秘密鍵のバックアップについても、物理的に破壊される。

６．２．１１　秘密鍵管理モジュールの評価

規定しない。

６．３　鍵ペア管理に関するその他の項目

６．３．１　公開鍵の保存

公開鍵の保存については、それを含む証明書を保存することによって行う。

自己署名証明書は、その有効期間の終了後、2 年間保存する。利用者証明書については、各証明書の CP に規定する。

６．３．２　証明書と鍵ペアの使用期間

証明書の有効期間を次に示す。

(1)　自己署名証明書：

・SHA-1 認証局　　2004/5/27～2014/5/27、2011/6/6～2036/1/1

・SHA-256 認証局　2015/3/24～2036/6/15

(2)　利用者証明書　：　各証明書の CP に規定する。

６．４　秘密鍵の活性化情報

６．４．１　活性化情報の作成と設定

本認証局内で使用されるの活性化情報は、認証局責任者の管理・指示の下、容易に推測されぬよう配慮して生成され、設定される。

６．４．２　活性化情報の保護

本認証局内で使用される活性化情報は、認証局責任者の管理・指示の下、施錠可能な保管庫にて保管される。

６．４．３　活性化情報に関するその他の項目

規定しない。

６．５　コンピュータセキュリティ管理

６．５．１　特定のコンピュータセキュリティに関する技術的要件

本認証局に係るシステムは、アクセス制御機能、操作員の識別と認証機能、システムのバックアップ・リカバリ機能等を備える。

６．５．２　コンピュータセキュリティの評価

本認証局は、使用される機器におけるセキュリティ上の脆弱性についての情報収集、評価を継続的に行い、重大な脆弱性が発見された場合には、速やかに必要な対処を行う。

６．６　技術的面におけるライフサイクルの管理

６．６．１　システム開発管理

本認証局の開発・構築・修正・変更は、ソフトバンク株式会社の管理の下、信頼できる組織および環境にて作業を実施する。開発・構築・修正・変更に際しては、テスト環境において検証を行い、認証局責任者の承認を得た上で導入する。ただし、軽微な修正・変更については、認証局運用責任者の承認により、作業を実施する。また、システム仕様および検証報告については、文書化し保管する。

６．６．２　セキュリティマネジメント管理

本認証局に係るシステムは、十分なセキュリティレベルを確保するために必要な設定が行われる。また、システムのセキュリティ上の脆弱性についての情報収集、評価が継続的に行われ、重大な脆弱性が発見された場合には、速やかに必要な対処が行われ、これを検証する。

６．６．３　ライフサイクルセキュリティの管理

開発においては、設計・開発・試験のフェーズごとに品質とセキュリティレベルについての評価が行われる。

６．７　ネットワークセキュリティ管理

本認証局とインターネット等の外部システムとは、ファイアウォール等を介して接続され、また侵入検知システムが設置される。これらのログについては、監視が行われる。

６．８　日時の記録

本認証局に係るシステムには、発行する証明書および監査用記録に対して正確な日付・時刻を記録するために必要な措置が取られる。

７．　証明書、CRL、OCSP の各プロファイル

７．１　証明書プロファイル

７．１．１　バージョン番号

自己署名証明書については、本 CPS 別紙 １１．１　に定める証明書プロファイルにおいて規定する。利用者証明書については、各証明書の CP に規定する。

７．１．２　証明書拡張領域

自己署名証明書については、本 CPS 別紙 １１．１　に定める証明書プロファイルにおいて規定する。利用者証明書については、各証明書の CP に規定する。

７．１．３　アルゴリズムオブジェクト識別子

自己署名証明書については、本 CPS 別紙 １１．１　に定める証明書プロファイルにおいて規定する。利用者証明書については、各証明書の CP に規定する。

７．１．４　名前の形式

自己署名証明書については、本 CPS 別紙 １１．１　に定める証明書プロファイルにおいて規定する。利用者証明書については、各証明書の CP に規定する。

７．１．５　名称制約

自己署名証明書については規定しない。利用者証明書については、各証明書の CP に規定する。

７．１．６　証明書ポリシーオブジェクト識別子

自己署名証明書については規定しない。利用者証明書については、各証明書の CP に規定する。

７．１．７　ポリシー制約拡張の使用

自己署名証明書については規定しない。利用者証明書については、各証明書の CP に規定する。

７．１．８　ポリシー修飾子の構文と意味

自己署名証明書については規定しない。利用者証明書については、各証明書の CP に規定する。

７．１．９　重要な証明書ポリシー拡張についての処理方法

自己署名証明書については規定しない。利用者証明書については、各証明書の CP に規定する。

７．２　CRL プロファイル

７．２．１　バージョン番号

本 CPS 別紙 １１．２ 、１１．３ に規定する。

７．２．２　CRL、CRL エントリ拡張

本 CPS 別紙 １１．２ 、１１．３ に規定する。

７．３　OCSP プロファイル

７．３．１　バージョン番号

規定しない

７．３．２　OCSP 拡張

規定しない

８．　準拠性監査とその他の評価

８．１　監査の頻度と要件

本認証局は監査人による監査を必要に応じて実施する。

８．２　監査人の要件

本認証局の監査は、監査業務および認証業務に精通した者が行う。

８．３　監査人と被監査者の関係

公正な監査を遂行するために、監査人は本認証局とは独立していなければならない。

８．４　監査の範囲

本認証局の業務が本 CPS に準拠して実施されていることを監査する。本 CPS の内容については監査の対象とならない。

８．５　監査における指摘事項への対応

本認証局は、重要または緊急を要する監査指摘事項について、ポリシー承認局の承認の元、速やかに対応する。重要または緊急を要する監査指摘事項が改善されるまでの間、本認証業務を停止するか否かはポリシー承認局が決定する。また、ポリシー承認局は、監査指摘事項に対して本認証局が対策を実施したことを確認する。

８．６　監査結果の開示

監査結果は、ポリシー承認局およびポリシー承認局が認めた対象にのみ開示される。

９．　他のビジネス的・法的問題

９．１　料金

９．１．１　証明書発行または更新料

別途本サービス契約に規定する。

９．１．２　証明書へのアクセス料金

別途本サービス契約に規定する。

９．１．３　失効またはステータス情報へのアクセス料金

別途本サービス契約に規定する。

９．１．４　その他のサービスに関する料金

別途本サービス契約に規定する。

９．１．５　払い戻し指針

別途本サービス契約に規定する。

９．２　金銭上の責任

９．２．１　保険の適用範囲

規定しない。

９．２．２　その他の資産

規定しない。

９．２．３　利用者を保護する保険、保証

規定しない。

９．３　企業情報の秘密性

９．３．１　秘密情報の範囲

本認証局においては、下記の情報を秘密情報とする。

(1)　本サービス申込書により提出された情報（公知のものを除く)。

(2)　証明書利用申請時に提出された情報で､証明書に記載されない事項(公知のものを除く）。

９．３．２　秘密情報の範囲外の情報

本認証局が保持する情報のうち、証明書、失効情報、本 CPS 等は秘密情報としない。

９．３．３　秘密情報の保護責任

本認証局は､秘密情報の漏洩を防ぎ､また本認証業務の用に供する以外には使用しない責任を負う。

９．４　パーソナルデータの保護

９．４．１　プライバシーポリシー

発行局は､発行局が保持するパーソナルデータの取り扱いについては、ソフトバンク株式会社のプライバシーポリシーに従う。また、登録局は、各加入者の規定に従う。

９．４．２　パーソナルデータとして扱われる情報

本認証局は､利用者証明書の利用申請および失効申請に含まれる情報で､個人の特定に結びつく情報をパーソナルデータとして扱う。ただし、証明書中に含まれる情報については、パーソナルデータとして扱わない。

９．４．３　パーソナルデータとみなされない情報

本認証局は、本 CPS ９．４．２　に規定される情報以外の情報については、パーソナルデータとみなさない。

９．４．４　パーソナルデータを保護する責任

発行局は、ソフトバンク株式会社のプライバシーポリシーに従い、パーソナルデータを保護する責任を負う。また、登録局は、各加入者の規定に従う。

９．４．５　パーソナルデータの使用に関する個人への通知および承認

本認証局は、証明書利用申請者による利用申請もしくは失効申請者による失効申請をもって、本認証業務上必要とするパーソナルデータの使用の承認を利用者から得たものとする。本認証局は、パーソナルデータを本認証業務の用に供する以外は使用しない。ただし、本CPS ９．４．６　に規定する場合を除く。

９．４．６　司法手続または行政手続に基づく公開

本認証局は、司法手続、行政手続その他の法的手続に際し、裁判的行政措置に従ってパーソナルデータを開示する権限を有する。

９．４．７　他の情報公開の場合

規定しない。

９．５　知的財産権

下記の情報およびデータは、ソフトバンク株式会社の知的財産である。

(1)　発行された全ての証明書
(2)　本 CPS、各証明書の CP、およびその他関連文書
(3)　本認証局の秘密鍵および公開鍵

９．６　表明および保証

９．６．１　発行局の表明および保証

発行局は下記の事項を保証することに対し、義務および責任を負う。

(1)　本 CPS に従って運用を行うこと。
本認証局秘密鍵を適切に管理し、発行した証明書および CRL/ARL の信頼の確保を行うこと。

９．６．２　登録局の表明および保証

登録局は下記の事項を保証することに対し、義務および責任を負う。

(1)　証明書利用申請を審査し、発行処理を行うこと。

(2)　利用者証明書に記載された利用者名と、利用者から利用申請に記載され申し出のあった利用者名とが一致していること。

(3)　証明書失効申請を審査し、失効処理を行うこと。

９．６．３　加入者の表明および保証

加入者は下記の事項を保証することに対し、義務および責任を負う。

(1)　利用者に対し、本サービスの利用を許可すること。

(2)　上記利用者の管理を行うこと。

９．６．４　利用者の表明および保証

利用者は下記の事項を保証することに対し、義務および責任を負う。

(1)　本 CPS １．４　で規定された証明書用途を遵守すること。

(2)　利用申請にあたり利用者が本認証局に提供した情報が正確であること。

(3)　秘密鍵、パスワードについて、充分な注意をもって厳重に保管し、紛失、改変、第三者による使用・複製等が行われない様、厳重に管理すること。

(4)　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、本 CPS ４．９．２　に規定する失効申請者をして本認証局に対し、直ちに利用者証明書の失効申請を行わせること。

(5)　本 CPS ４．８．１　に示す内容に変更があるとき、本 CPS ４．９．２　に規定する失効申請者をして本認証局に対し、遅滞なく失効申請を行わせること。

９．６．５　信頼者の表明および保証

信頼者は下記の事項を保証することに対し、義務および責任を負う。

(1)　本 CPS １．４　で規定された証明書用途を遵守すること

(2)　証明書の有効性の確認等により、証明書を信頼するか否かを自らの責任において判断すること

９．６．６　他の関係者の表明および保証

規定しない。

９．７　無保証

本認証局は、本 CPS に記載してある事項を遵守し、記載事項に適合するよう本認証局の運用を行うが､これにも関わらず発生した損害について､本認証局は一切の責任を負わない。

本認証局は、他の関係者に対し、利用者、代表者、もしくは信頼者が本 CPS ９．６．４および本 CPS ９．６．５　に記述されている事項を遵守することは、保証しない。

９．８　責任制限

９．８．１　利用者の義務違反

利用者が本 CPS ９．６．４　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。

利用者が本 CPS ９．６．４　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､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する。

９．８．２　信頼者の義務違反

信頼者が本 CPS ９．６．５　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　不可抗力等

(1)　本認証局は、利用者が利用者証明書を取得、利用することによりコンピュータシステム等のハードウェア・ソフトウェアに何らかの影響、障害が発生しても、その責を一切負わない。

(2)　本認証局は、利用者や代表者からの失効申請に伴う本認証局内での失効処理が、正当な事由により遅延した場合、これにより発生した損害については、一切損害賠償責任を負わない。

(3)　本認証局は、本認証局を廃止することにより発生した損害については、一切損害賠償責任を負わない。

(4)　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（信頼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。

（ア）　天災：火災、雷、噴火、洪水、地震、嵐、台風、津波等

（イ）　人災：戦争、革命、暴動、内乱、労働争議等

（ウ）　裁判所、政府、行政、省庁等による作為、不作為、命令等

（エ）　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

（オ）　技術上もしくは運用上緊急に本認証局に係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

（カ）　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、不完全履行もしくは履行遅滞を生じさせ、係る結果に至ることとなった事象または状況

（キ）　その他本認証局の責に帰すべからざる事由

９．８．４　賠償

本認証局が、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、利用者または信頼者に対して損害を与えた場合の賠償については、本サービス契約に規定する。

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､本利用者証明書を提供する際に用いる暗号アルゴリズムの退化による損害、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（信頼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。

９．９　補償

利用者、信頼者の行為に起因して、第三者に損害が生じた場合、本認証局は免責されるものとし、利用者または信頼者は、損害賠償の責めを負わなくてはならないものとする。本認証局が第三者に損害賠償を行った場合､利用者または信頼者は本認証局に対してその賠償額および本認証局において発生する訴訟に係る費用等の損害を補償しなくてはならないものとする。

９．１０　文書の有効期間と終了

９．１０．１　文書の有効期間

本 CPS は、文書の作成後、ポリシー承認局が承認することにより有効となる。本 CPS　９．１０．２　で記載する本 CPS の終了以前に本 CPS が無効となることはない。

９．１０．２　終了

本 CPS は、本 CPS ９．１０．３　に掲げる存続条項を除き、本認証局が業務を終了した時点で無効となる。

９．１０．３　終了の影響と存続条項

本 CPS が無効となった後も、本 CPS ９．４　、９．５　、９．６　、９．７　、９．８　、９．９　、９．１０．２　、９．１０．３　、９．１３　、９．１４　、９．１５　、９．１６　の各項の規定については効力をもつものとする。

９．１１　個々の関係者間に対する通知と連絡

本認証局から加入者に対し個別の通知が必要となった場合、本サービス契約において申請された当該加入者の連絡先に対して、郵送、電子メール、電話、FAX 等の手段を用いて通知を行うものとする。

９．１２　改訂

９．１２．１　改訂手続き

ポリシー承認局は、必要に応じ、本 CPS の改訂・承認を行う。

９．１２．２　通知方法と期間

変更内容をリポジトリである Web サーバ上において公開することをもって通知する。公開後 14 日（公開日を含まない）を経過しても加入者から本サービスから脱退する旨の申し出がなかった場合は、当該加入者に属する利用者は当該期間満了日に変更事項を承認したものとする。

９．１２．３　オブジェクト識別子の変更理由

規定しない。

９．１３　紛争解決手続き

本認証局の利用に関して生じた全ての訴訟の際、全ての当事者は、東京地方裁判所を第一審の専属管轄裁判所とする。

９．１４　準拠法

本 CPS に基づく認証業務から生ずる紛争については、日本国の法令を適用する。

９．１５　適用される準拠法

規定しない。

９．１６　その他の条項

９．１６．１　完全合意

本 CPS の規定は、当事者が文書で本 CPS の規定の特別規定となる旨を合意した場合または本 CPS が別段の定めをしている場合を除き、口頭で修正、放棄、追加、変更、または終了させることはできない。

９．１６．２　譲渡

規定しない。

９．１６．３　分離可能性

本 CPS 中のある規定が、何らかの理由により、無効または執行不可能であるとされた場合においても、残余の規定は有効であり、当事者の意思に最も合理的に合致するよう解釈される。

責任制限、保証、免責、または損害の排除等について規定する本 CPS の各条項は、他の規定と分離され、また、その条項に従って執行可能であることにつき当事者は合意するものとする。

９．１６．４　執行（弁護士費用と権利の放棄）

規定しない。

１０．　【別紙 1】　用語集

あ行

- アーカイブ（Archive）
  証明書の発行履歴､失効履歴等を必要に応じて閲覧可能な状態にて長期間保管すること。

- アクセス制御（Access Control）
  ユーザの権限に応じた制御を行う方法。データへのアクセスについて、閲覧が許可されている人に限りアクセスできるように物理的、電子的な手法で制御すること。

- アルゴリズム（Algorithm）
  ここにおいては、暗号化アルゴリズムをさす。暗号化アルゴリズムは、情報に対して一連の変換を施して情報を第三者に理解困難な形式にするための数学的に表現した規則の集まりをさす。

- 暗号モジュール（Cryptographic Module）
  暗号鍵等の生成、保管、利用などにおいて、セキュリティを確保する目的で使用されるソフトウェア、ハードウェアあるいはそれらを組み合わせた装置。

- 一時失効（Suspension）
  証明書の有効期間中に証明書を一時的に無効な状態にすること。

か行

- 鍵ペア（Key Pair）
  公開鍵暗号方式における公開鍵およびそれに対応する秘密鍵。２つの鍵は、一方の鍵から他方の鍵を導き出せない性質を持つ。

- 鍵長（Key Length）
  鍵の長さをビット数で表したもの。暗号の強度を決定する要素の１つ。一般に鍵長が長いほど解読がされにくいとされる。

- 鍵の預託（Key Escrow）
  秘密鍵または公開鍵を第三者機関に登録保管すること。

- 活性化（Activation）
  システムや装置等を使用可能な状態にすること。

- 活性化情報（Activation Data）
  システムや装置等を活性化するために必要となるデータ。具体的には、PIN コードやパスフレーズ等をさす。

- 危殆化（Compromise）
  秘密鍵や関連秘密情報等の秘密性が、盗難や漏洩、第三者による解読等によって失われた事態の発生をいう。認証局の秘密鍵が危殆化した場合、当該認証局から発行された全ての証明書の信頼性が失われる。

- 公開鍵（Public Key）
  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。

- 公開鍵暗号方式（Public Key Cryptographic Algorithm）
  関連した２つの鍵（公開鍵と秘密鍵）を使用する非対称暗号方式(asymmetric cryptographic algorithm)の１つであり、一方の鍵（公開鍵）で暗号化したデータは、他方の鍵（秘密鍵）でのみ復号化できるようになっている。

さ行

- 自己署名証明書（Self-signed Certificate）
  認証局が、自己を証明するために発行する証明書。証明書に記載される証明書発行主体（Issuer）と被発行者（Subscriber）とが同一になっている。

- 失効（Revocation）
  証明書の有効期間内に、秘密鍵が危殆化もしくはその可能性が発生した場合、証明書の記載内容に変更が生じた場合等において、証明書を無効にすること。

- 失効リスト（Certificate Revocation List = CRL、Authority Revocation List=ARL）
  失効した証明書のリスト。本認証局においては、失効された利用者証明書のリストがCRL に掲載される。また、ARL には、失効された自己署名証明書のリストが記載される。失効リストには、証明書を発行した認証局による電子署名が付される。

- 証明書（Certificate）
  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電子文書。認証対象者の識別情報、その公開鍵、鍵の利用目的・範囲、発行認証局名などが含む一連の情報に、認証局の電子署名を付加したもの。

- 証明書ポリシー（Certificate Policy = CP）
  認証局が証明書を発行する際の運用方針を定めた文書。

- 信頼者（Relying Party）
  証明書を受け取って、それを信頼して行動する者。

た行

- タイムスタンプ(Time Stamp)
  信頼できる時刻管理機器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。

- 登録局（Registration Authority = RA）
  証明書の発行や失効のプロセスにおいて、本人性確認や認証局システムへのデータ登録等の一部機能を認証局の承認を受けて行う組織。登録局は、証明書および失効リストの生成は行わない。

- 電子署名（Electronic Signature）
  間違いなく本人であることを証明する電子的なデータで、広義ではアナログ署名を電子データにしたものも含まれるが、ここでは、デジタル署名(digital signature)の意味で用いる。具体的には、署名対象データのハッシュ値に対して、秘密鍵で暗号化したもの。電子署名の検証は、電子署名を公開鍵で復号化した値と元のデータのハッシュ値とを照合することで可能となる。

な行

- 認証局（Certification Authority = CA）
  証明書の発行、失効、失効リストの開示等のサービスを行う信頼された組織。

- 認証局運用規程（Certification Practice Statement = CPS）
  認証局の信頼性、安全性を対外的に示すために、認証局の運用規則、鍵の生成・管理、遵守事項等を文書化したもの。利用者・信頼者等の認証局の外部者に開示されるもの。

は行

- 発行局（Issuing Authority = IA）
  登録局において審査・承認され、送信される証明書発行リクエストに対し、電子署名を行い、電子証明書を発行する機関。

- 秘密鍵（Private Key）
  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。

- ハッシュ関数（Hash Function）
  データを数学的な操作によって一定の長さに縮小させる関数であり、異なる２つの入力値から同じ出力値を算出することが困難な関数。出力値から入力値を逆算することは不可能。

- ハッシュ値（Hash Value）
  ある値に対するハッシュ関数の出力値。「ハッシュ関数」参照。

- 秘密鍵管理モジュール（Hardware Security Module = HSM）
  暗号モジュールのうちハードウェアにより秘密鍵を安全に管理する装置。主に認証局で使用され、耐タンパ性をもち安全な秘密鍵管理機能を備えた暗号モジュールのこと。「暗号モジュール」参照。

- フィンガープリント（Finger Print）
  自己署名証明書などの証明書が改ざんされていないことを証明するためのデータ(ハッシュ値）のことをいう。その証明書が唯一無二であることを証明できることから、拇印と呼ばれている。SHA-1（ハッシュ関数）により算出したフィンガープリントは、40 桁の 16 進数であり、「0」～「9」及び「A」～「F」の文字の組合せで示される。ただし、フィンガープリントを表示するソフトウェアの種類又はバージョンにより､大文字又は小文字の相違、「:」又は「 」（スペース）の付加等表示方法が異なることがある。

- 複数人管理（Dual Control）
  秘密情報へのアクセス､システム運用・操作等における不正行為を防止する為に、複数の人間に管理機能を分散させ､全員がそれぞれの管理機能を遂行してはじめて所定の機能が働くようにする作業方式または管理方式。

- プロファイル（Profile）
  証明書（自己署名証明書、利用者用証明書）、失効リスト（CRL／ARL）等の設定情報のこと。

- ポリシー承認局(Policy Authority = PA)
  本認証局のポリシーの決定や CPS の承認等を行う､本認証局における最高意思決定機関。

- 本人性確認（Identification and Authentication）
  個人や機器等の認証対象に関する情報が、本人（本体）のものであることを審査する行為。

ま行

ら行

- リポジトリ（Repository）
  証明書や失効リスト､CPS 等を保管し、証明書利用者等に対してこれらの開示等のサービスを提供するシステム。

- 利用者（Subscriber）
  本認証局への申請主体である個人もしくは機器等であり､実際に証明書を利用する者をさす。利用者の希望により、利用者個人の所属先を証明する場合もある。

- ログ（Log）
  コンピュータの利用状況や通信の記録。操作やデータの送受信等が行われた日時と、操作者、操作内容、通信内容等が記録される。

Ａ－Ｇ

- ARL（Authority Revocation List）
  「失効リスト」参照。

- CA（Certification Authority）
  「認証局」参照。

- CN（Common Name）
  ITU-T（国際電気通信連合－Ｔ）が策定したX.500 勧告において定められた、識別名（Distinguished Name）の中のひとつの属性。通常、一般的な名称（対象が人であれば人名）を表す。

- CP（Certificate Policy）
  「証明書ポリシー」参照。

- CPS（Certification Practices Statement）
  「認証局運用規定」参照。

- CRL（Certificate Revocation List）
  「失効リスト」参照。

- DN（Distinguished Name）
  ITU-T（国際電気通信連合－Ｔ）が策定したX.500 勧告において定められた識別名。C（Country Name = 国名）、O（Organization Name = 組織名）、OU（Organization Unit Name = 組織部局名）、CN（Common Name = 一般名）等の属性で構成される。

- FIPS 140-1 (Federal Information Processing Standard 140-1)
  FIPS は商務省連邦情報処理規格を指し、140-1 は暗号モジュール用セキュリティ要件を規定している。暗号モジュールは、セキュリティレベルという段階基準があり、どの要件に適合するかにより、最低レベル 1 から最高レベル 4 のいずれかにあて当てはめられる。

H－N

- HSM (Hardware Security Module)
  「秘密鍵管理モジュール」参照。

- IETF (Internet Engineering Task Force)
  インターネットで利用される技術を標準化する組織。インターネットの標準化を統括する IAB の下部機関。ここで策定された技術仕様は RFC として公表される。

- IPSec (IP Security)
  IP パケットの暗号化と認証を行なう、TCP/IP 環境で汎用的に用いることができるネットワーク層で動作するセキュリティ技術。IETF により標準化され、フレーム構成、データの暗号化や受信パケットの改ざんチェックなど､暗号通信の基本部分が規定されている。IPSec 通信を行う相手との鍵交換方式には、IKE (Internet KeyExchange) が使用される。

- ISO(International Organization for Standardization)
  国際標準化機構。電気分野を除くあらゆる分野において、国際的に通用する規格・標準類の制定を目的としている。

- ITU (International Telecommunication Union)
  国際連合(UN)の専門機関の１つである国際電気通信連合。電気通信の改善、合理的利用を目的としている。

- ITU-T(International Telecommunication Union - Telecommunication Standardization Sector)
  国際電気通信連合の電気通信標準化部門。

- LDAP（Lightweight Directory Access Protocol）
  インターネット、イントラネット等の TCP/IP ネットワークで、ディレクトリデータベースにアクセスするためのプロトコル。

O－U

- OCSP（Online Certificate Status Protocol）
  証明書のステータス(失効･一時停止していないかどうか)をオンラインで問い合わせるプロトコル。OCSP クライアントと OCSP レスポンダ（サーバ）との間の通信方法について取り決めている。OCSP クライアントは、OCSP レスポンダに対して、対象となる証明書のシリアル番号を、電子署名付きで送信する。
  OCSP レスポンダは、問い合わせのあった証明書の状態を電子署名付きで返答する。

- OID（Object Identification：オブジェクト識別子）
  世界で一意となる値を登録機関（ISO、ITU）に登録した識別子。暗号アルゴリズムや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。

- PIN（Personal Identification Number）
  個人識別番号のこと。本認証局においては、利用者の秘密鍵を活性化するための PIN 及び利用者に配付する IC カードの活性化用に用いる IC カード PIN がこれに該当する。

- PKI（Public Key Infrastructure）
  公開鍵暗号方式を用いて情報システム､コミュニケーションシステムのセキュリティを確保するための一連の技術及びサービス。

- RA（Registration Authority）
  「登録局」参照。

- RFC3647（Request For Comments 3647）
  RFC とは、インターネットに関する標準文書の総称。その１つである RFC3647 は、CP もしくは CPS を作成するためのフレームワーク及びガイドラインを提供している。

- RSA
  Rivest、Shamir、Adelman の 3 人が開発した公開鍵暗号方式の一つ。

- SHA-1、SHA-256（Secure Hash Algorithm）
  電子署名等に使われるハッシュ関数のひとつ。原文から疑似乱数（ハッシュ値）を発生し、通信経路の両端で比較することで、通信途中で原文が改ざんされていないかを検出することができる。不可逆な一方向関数を含むため、ハッシュ値から原文を再現することはできず、また同じハッシュ値を生成する別のメッセージを作成することは極めて困難である。

- SSL（Secure Socket Layer）
  ネットワーク上の、２つのアプリケーション間の相互認証、通信の暗号化を行うプロトコル。米 Netscape 社が開発した。HTTP、SMTP、POP3 等のアプリケーション層のプロトコルと組み合わせて用いる（それぞれ HTTPS、SSMTP、SPOP3 と呼ぶ）。認証、暗号化に使う方法は通信の両端で打ち合わせて決めるようになっており、一般には、RSA、MD5、DES 等を用いている。

Ｖ－Ｚ

- X.500
  X.500 シリーズは、ITU-T で 1988 年に規格化されたディレクトリ・サービスの勧告（国際標準）である 1997 年に新しい仕様が加えられている。この仕様には、ディレクトリの概念やその階層構造、サービスやオブジェクトの定義などが含まれる。

- X.509
  ITU-T が定めた、証明書に関する規格。バージョンが 1, 2, 3 とある。本認証局が発行する証明書はバージョン 3 を用いており、CRL/ARL はバージョン 2 を用いている。

- X.509v3
  証明書に関する ITU-T 規格のバージョン 3。既にエクステンション（拡張領域）を含むか、含むことが可能な証明書のこと。

- X.509v3 key usage
  証明書エクステンションの一つで、鍵が利用される目的を設定する項目のこと。電子署名、否認防止等の鍵利用目的がある。

１１．　【別紙 2】　証明書プロファイル

１１．１　自己署名証明書

(1)　Basic

SHA-1 認証局

version	値	説明
Version	型:INTEGER 値:2	証明書フォーマットのバージョン番号 2 (Ver.3)
serialNumber		
CertificateSerialNumber	型:INTEGER 値:ユニークな整数	証明書のシリアル番号
signature		
AlgorithmIdentifier		証明書への署名に使用された暗号アルゴリズムの識別子 (公開鍵暗号とハッシュ関数)
algorithm	型:OID 値:1 2 840 113549 1 1 5	暗号アルゴリズムのオブジェクトID sha1WithRSAEncryption
parameters	型:NULL 値:NULL	暗号アルゴリズムの引数
issuer		
CountryName		証明書発行者の国名
type	型:OID 値:2 5 4 6	国名のオブジェクトID
value	型:PrintableString 値:JP	国名の値
OrganizationName		証明書発行者の組織名
type	型:OID 値:2 5 4 10	組織名のオブジェクトID
value	型:PrintableString 値:JAPAN TELECOM CO., LTD.	組織名の値
OrganizationalUnitName		証明書発行者の部門名
type	型:OID 値:2 5 4 11	部門名のオブジェクトID
value	型:PrintableString 値:N/A	部門名の値
CommonName		証明書所有者の固有名称
type	型:OID 値:2 5 4 3	固有名称のオブジェクトID
value	型:PrintableString 値:JAPAN TELECOM CA	固有名称の値
validity		
Validity		証明書の有効期間
notBefore	型:UTC Time 値:yymmddhhmmssZ	有効開始日時
notAfter	型:UTC Time 値:yymmddhhmmssZ	終了日時

subject		
CountryName		証明書発行者の国名
type	型:OID 値:2 5 4 6	国名のオブジェクトID
value	型:PrintableString 値:JP	国名の値
OrganizationName		証明書発行者の組織名
type	型:OID 値:2 5 4 10	組織名のオブジェクトID
value	型:PrintableString 値:JAPAN TELECOM CO., LTD.	組織名の値
OrganizationalUnitName		証明書発行者の部門名
type	型:OID 値:2 5 4 11	部門名のオブジェクトID
value	型:PrintableString 値:N/A	部門名の値
CommonName		証明書所有者の固有名称
type	型:OID 値:2 5 4 3	固有名称のオブジェクトID
value	型:PrintableString 値:JAPAN TELECOM CA	固有名称の値
subjectPublicKeyInfo		
SubjectPublicKeyInfo		証明書所有者の公開鍵に関する情報
AlgorithmIdentifier		暗号アルゴリズムの識別子
algorithm	型:OID 値:1 2 840 113549 1 1 1	暗号アルゴリズムのオブジェクトID
parameters	型:NULL 値:NULL	暗号アルゴリズムの引数
subjectPublicKey	型:BIT STRING 値:公開鍵値	公開鍵値

SHA-256 認証局

version	値	説明
Version	型:INTEGER 値:2	証明書フォーマットのバージョン番号 2 (Ver.3)
serialNumber		
CertificateSerialNumber	型:INTEGER 値:ユニークな整数	証明書のシリアル番号
signature		
AlgorithmIdentifier		証明書への署名に使用された暗号アルゴリズムの識別子 (公開鍵暗号とハッシュ関数)
algorithm	型:OID 値:1.2.840.113549.1.1.11 (SHA256withRSAEncryption)	暗号アルゴリズムのオブジェクトID
parameters	型:NULL 値:NULL	暗号アルゴリズムの引数
issuer		
CountryName		証明書発行者の国名
type	型:OID 値:2 5 4 6	国名のオブジェクトID
value	型:PrintableString 値:JP	国名の値
OrganizationName		証明書発行者の組織名
type	型:OID 値:2 5 4 10	組織名のオブジェクトID
value	型:PrintableString 値:SOFTBANK TELECOM CO., LTD.	組織名の値
CommonName		証明書所有者の固有名称
type	型:OID 値:2 5 4 3	固有名称のオブジェクトID
value	型:PrintableString 値:PKI PLATFORM CA G2	固有名称の値
validity		
Validity		証明書の有効期間
notBefore	型:UTC Time 値:150324073128Z	有効開始日時 年(2 桁or4 桁)月日時分秒Z
notAfter	型:UTC Time 値:360615145959Z	終了日時 年(2 桁or4 桁)月日時分秒Z
subject		
CountryName		証明書所有者の国名
type	型:OID 値:2 5 4 6	国名のオブジェクトID
value	型:PrintableString 値:JP	国名の値
OrganizationName		証明書所有者の組織名
type	型:OID 値:2 5 4 10	組織名のオブジェクトID
value	型:PrintableString 値:SOFTBANK TELECOM CO., LTD.	組織名の値
CommonName		証明書所有者の固有名称
type	型:OID 値:2 5 4 3	固有名称のオブジェクトID
value	型:PrintableString 値:PKI PLATFORM CA G2	固有名称の値
subjectPublicKeyInfo		
SubjectPublicKeyInfo		証明書所有者の公開鍵に関する情報
AlgorithmIdentifier		暗号アルゴリズムの識別子
algorithm	型:OID 値:1 2 840 113549 1 1 1	暗号アルゴリズムのオブジェクトID
parameters	型:NULL 値:NULL	暗号アルゴリズムの引数
subjectPublicKey	型:BIT STRING 値:公開鍵値	公開鍵値 ※2048Bit長の公開鍵

(2) Standard Extensions

authoritytKeyIdentifier (entnID := 2 5 29 35, critical := -)	**値**	**説明**
AuthorityKeyIdentifier keyIdentifier	設定しない	認証局の公開鍵識別子 公開鍵の識別子
authorityCertSerialNumber	設定しない	認証局の証明書のシリアル番号
authorityCertIssuer directoryName	設定しない	認証局に関する情報 ディレクトリ名
subjectKeyIdentifier (entnID := 2 5 2 14 , critical := FALSE)		
SubjectKeyIdentifier keyIdentifier	型:OCTET STRING 値:subjectPublicKeyのHash値	証明書所有者の公開鍵に関する情報 公開鍵の識別子
keyUsage (entnID := 2 5 29 15, critical := TRUE)		
KeyUsage	型:BitString 値:000001100	鍵の使用目的 keyCertSign,cRLSign
privateKeyUsagePeriod (entnID := 2 5 29 16, critical := -)		
privateKeyUsagePeriod	設定しない	秘密鍵使用期間
certificatePolicies (entnID := 2 5 29 32, critical := -)		
PolicyInformation	設定しない	証明書ポリシー
PolicieMapping (entnID := 2 5 29 33, critical := -)		
policyMapping	設定しない	ポリシーマッピング
subjectAltName (entnID := 2 5 29 17, critical := -)		
subjectAltName	設定しない	証明書主体者別名
issuerAltName (entnID := 2 5 29 18, critical := -)		
issuerAltName	設定しない	証明書発行者別名
subjectDirecotryAttribute (entnID := 2 5 29 9, critical := -)		
subjectDirecotryAttribute	設定しない	証明書利用者ディレクトリ属性
basicConstraints (entnID := 2 5 29 19, critical := TRUE)		
basicConstraints cA pathLenConstraints	型:Boolean 値:True 設定しない	基本的制限 CAかどうかを示すフラグ Trueの場合はCAである
nameConstraints (entnID := 2 5 29 30, critical := -)		
nameConstraints	設定しない	名称制約

policyConstraints (entnID := 2 5 29 36, critical := -)		
policyConstraints	設定しない	ポリシー制約
extendKeyUsage (entnID := 2 5 29 37, critical := -)		
extendKeyUsage	設定しない	拡張した鍵の使用目的
cRLDistributionPoints (entnID := 2 5 29 31, critical := FALSE)		
cRLDistributionPoints DistributionPoint fullName uniformResourceIdentifier		CRL配布ポイント CRLを配布するURI
inhibitAnyPolicy (entnID := 2 5 29 54, critical := -)		
InhibitAnyPolicy	設定しない	全ポリシー禁止
FreshestCRL (entnID := 2 5 29 46, critical := -)		
freshestCrl	設定しない	デルタCRL

(3) Internet Certificate Extensions

authorityInfoAccess (entnID := 1 3 6 1 5 5 7 1 1, critical := -)	**値**	**説明**
authorityInfoAccess	設定しない	認証局情報アクセス
subjectInfoAccess (entnID := 1 3 6 1 5 5 7 1 11, critical := -)		
subjectInfoAccess	設定しない	主体者情報アクセス

１１．２　証明書失効リスト

(1)　Basic

version	値	説明
Version	型:INTEGER 値:1	証明書失効リストフォーマットのバージョン番号
signature		
AlgorithmIdentifier		証明書失効リストへの署名に使用された暗号アルゴリズムの識別子
algorithm	型:OID 値:1 2 840 113549 1 1 5	暗号アルゴリズムのオブジェクトID sha1WithRSAEncryption
parameters	型:NULL 値:NULL	暗号アルゴリズムの引数
issuer		
CountryName		証明書発行者の国名
type	型:OID 値:2 5 4 6	国名のオブジェクトID
value	型:PrintableString 値:JP	国名の値
OrganizationName		証明書発行者の組織名
type	型:OID 値:2 5 4 10	組織名のオブジェクトID
value	型:PrintableString 値:JAPAN TELECOM CO., LTD. 値:SOFTBANK TELECOM CO., LTD.	組織名の値
OrganizationalUnitName		証明書発行者の部門名
type	型:OID 値:2 5 4 11	部門名のオブジェクトID
value	型:PrintableString 値:N/A	部門名の値
CommonName		証明書所有者の固有名称
type	型:OID 値:2 5 4 3	固有名称のオブジェクトID
value	型:PrintableString 値:JAPAN TELECOM CA/PKI PLATFORM CA G2	固有名称の値
ThisUpdate		
ThisUpdate	型:UTC Time 値:yymmddhhmmssZ	CRL発行日時
NextUpdate		
NextUpdate	型:UTC Time 値:yymmddhhmmssZ	次回CRL発行予定日時
RevokedCertificates		
userCertificate	型:INTEGER 値:証明書シリアル番号	証明書シリアル番号
revocationDate	型:UTC Time 値:yymmddhhmmssZ	失効申請受理日時
crlEntry Extensions		

(2) Crl Entry Extensions

reasonCode (extnID :== 2 5 29 21, critical :== FALSE)	値	説明
reasonCode	型:ENUMERATED 値:	理由コード unspecified,keyCompromise,cACompromise,affiliationChanged, cessationOfOperation,certificateHold ,removeFromCRL,privilegeWithdrawnaACompromise
holdInstructionCode (extnID :== 2 5 29 23, critical :== -)		
holdInstructionCode	設定しない	保留命令コード
invalidityDate (extnID :== 2 5 29 24, critical :== FALSE)		
invalidityDate	型:GeneralizedTime 値:yyyymmddhhmmssZ	無効となった日時
certificateIssuer (extnID :== 2 5 29 29, critical :== -)		
certificateIssuer	設定しない	証明書発行者

(3) Crl Extensions

authorityKeyIdentifier (entnID :== 2 5 29 35, critical :== FALSE)	値	説明
AuthorityKeyIdentifier		失効リスト発行者の公開鍵識別子
keyIdentifier	型:OctetString 値:認証局のsubjectPublicKeyのHASH値	公開鍵の識別子
authorityCertSerialNumber	型:INTEGER 値:認証局のシリアル番号	失効リスト発行者の証明書のシリアル番号
authorityCertIssuer		失効リスト発行者に関する情報
directoryName	型:PrintableString	ディレクトリ名
CountryName		証明書発行者の国名
type	型:OID 値:2 5 4 6	国名のオブジェクトID
value	型:PrintableString 値:JP	国名の値
OrganizationName		証明書発行者の組織名
type	型:OID 値:2 5 4 10	組織名のオブジェクトID
value	型:PrintableString 値:JAPAN TELECOM CO., LTD. 値:SOFTBANK TELECOM CO., LTD.	組織名の値
CommonName		証明書所有者の固有名称
type	型:OID 値:2 5 4 3	固有名称のオブジェクトID
value	型:PrintableString 値 JAPAN TELECOM CA/PKI PLATFORM CA G2	固有名称の値
crlNumber (entnID :== 2 5 29 20, critical :== FALSE)		
cRLNumber	型:INTEGER 値:ユニークな整数	失効リストのシーケンス番号 失効リストのシーケンス番号の値 認証局が割り当てるシーケンス番号

issuingDistributionPoint （entnID ::= 2 5 29 28, critical ::= FALSE）		
issuingDistributionPoint DistributionPoint fullName onlyContainsUserCerts		 失効リストが利用者に関するもののみであることを示すフラグ
FreshestCRL （entnID ::= 2 5 29 46, critical ::= -）		
freshestCrl	設定しない	デルタCRL
issuerAltName （entnID ::= 2 5 29 18, critical ::= -）		
issuerAltName	設定しない	証明書発行者別名
crlNumber （entnID ::= 2 5 29 20, critical ::= FALSE）		
crlNumber	値：シリアル番号	CRL番号

１１．３　認証局失効リスト

(1)　Basic

version	値	説明
Version	型:INTEGER 値:1	証明書失効リストフォーマットのバージョン番号
signature		
AlgorithmIdentifier		証明書失効リストへの署名に使用された暗号アルゴリズムの識別子
algorithm	型:OID 値:1 2 840 113549 1 1 5	暗号アルゴリズムのオブジェクトID sha1WithRSAEncryption
parameters	型:NULL 値:NULL	暗号アルゴリズムの引数
issuer		
CountryName		証明書発行者の国名
type	型:OID 値:2 5 4 6	国名のオブジェクトID
value	型:PrintableString 値:JP	国名の値
OrganizationName		証明書発行者の組織名
type	型:OID 値:2 5 4 10	組織名のオブジェクトID
value	型:PrintableString 値:JAPAN TELECOM CO., LTD. 値:SOFTBANK TELECOM CO., LTD.	組織名の値
OrganizationalUnitName		証明書発行者の部門名
type	型:OID 値:2 5 4 11	部門名のオブジェクトID
value	型:PrintableString 値:N/A	部門名の値
CommonName		証明書所有者の固有名称
type	型:OID 値:2 5 4 3	固有名称のオブジェクトID
value	型:PrintableString 値 JAPAN TELECOM CA/PKI PLATFORM CA G2	固有名称の値
ThisUpdate		
ThisUpdate	型:UTC Time 値:yymmddhhmmssZ	CRL発行日時
NextUpdate		
NextUpdate	型:UTC Time 値:yymmddhhmmssZ	次回CRL発行予定日時
RevokedCertificates		
userCertificate	型:INTEGER 値:証明書シリアル番号	証明書シリアル番号
revocationDate	型:UTC Time 値:yymmddhhmmssZ	失効申請受理日時
crlEntry Extensions		

(2) Crl Entry Extensions

holdInstructionCode (extnID :== 2 5 29 23, critical :== -)		
holdInstructionCode	設定しない	保留命令コード
invalidityDate (extnID :== 2 5 29 24, critical :== FALSE)		
invalidityDate	型:GeneralizedTime 値:yyyymmddhhmmssZ	無効となった日時
certificateIssuer (extnID :== 2 5 29 29, critical :== -)		
certificateIssuer	設定しない	証明書発行者

(3) Crl Extensions

authoritytKeyIdentifier (entnID :== 2 5 29 35, critical :== FALSE)	値	説明
AuthorityKeyIdentifier		失効リスト発行者の公開鍵識別子
keyIdentifier	型:OctetString 値:認証局のsubjectPublicKeyのHASH値	公開鍵の識別子
authorityCertSerialNumber	型:INTEGER 値:認証局のシリアル番号	失効リスト発行者の証明書のシリアル番号
authorityCertIssuer		失効リスト発行者に関する情報
directoryName	型:PrintableString	ディレクトリ名
CountryName		証明書発行者の国名
type	型:OID 値:2 5 4 6	国名のオブジェクトID
value	型:PrintableString 値:JP	国名の値
OrganizationName		証明書発行者の組織名
type	型:OID 値:2 5 4 10	組織名のオブジェクトID
value	型:PrintableString 値:JAPAN TELECOM CO., LTD. 値:SOFTBANK TELECOM CO., LTD.	組織名の値
CommonName		証明書所有者の固有名称
type	型:OID 値:2 5 4 3	固有名称のオブジェクトID
value	型:PrintableString 値 JAPAN TELECOM CA/PKI PLATFORM CA G2	固有名称の値
crlNumber (entnID :== 2 5 29 20, critical :== FALSE)		
cRLNumber	型:INTEGER 値:ユニークな整数	失効リストのシーケンス番号 失効リストのシーケンス番号の値 認証局が割り当てるシーケンス番号

issuingDistributionPoint （entnID := 2 5 29 28, critical := FALSE）		
issuingDistributionPoint DistributionPoint fullName onlyContainsCACerts		失効リストが認証局に関するもののみであることを示すフラグ
FreshestCRL （entnID := 2 5 29 46, critical := -）		
freshestCrl	設定しない	デルタCRL
issuerAltName （entnID := 2 5 29 18, critical := -）		
issuerAltName	設定しない	証明書発行者別名
crlNumber （entnID := 2 5 29 20, critical := FALSE）		
crlNumber	値：シリアル番号	CRL番号

１１．４　利用者証明書

各証明書の CP に規定する。