# PKI プラットフォーム認証局
# サーバ証明書　証明書ポリシー
# (Certificate Policy)

Version 3.5

2015 年 8 月 24 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 | 鍵長更新 | ポリシー承認局 |
| 3.3 | 2015年4月1日 | 社名変更 | ポリシー承認局 |
| 3.4 | 2015年7月1日 | 社名変更 | ポリシー承認局 |
| 3.5 | 2015年8月24日 | SHA-256変更対応 | ポリシー承認局 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# 目　　次

# １．　はじめに

本文書は、ソフトバンク株式会社が 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）から発行する利用者証明書のうち、サーバ証明書（以後、「証明書」という）の証明書ポリシーに関する規定（以後、「本 CP」という）である。本 CP と PKI プラットフォーム認証局運用規定（以後、「当該 CPS」という）との間に矛盾がある場合は、本 CP の規定が優先するものとする。

## １．１　概要

本 CP は、本認証局が発行する証明書の発行方針および利用に関する要件を定めるものである。証明書は、ソフトバンク株式会社が提供する本サービスにおいて、利用者（サーバまたはネットワーク機器）に対して発行される。

本サービスの利用に際しては、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、当該 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、当該 CPS に従う。

本 CP 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。ただし、当該 CPS を含む他の規定等を参照する場合には、見出しだけを残し、その旨を明示することとする。

## １．２　文書名称と定義

本 CP の正式名称を、「PKI プラットフォーム認証局　サーバ証明書　証明書ポリシー」とする。

## １．３　PKI の関係者

### １．３．１　ポリシー承認局

当該 CPS に従う。

### １．３．２　発行局

当該 CPS に従う。

### １．３．３　登録局

当該 CPS に従う。

### １．３．４　加入者

当該 CPS に従う。

### １．３．５　利用者

利用者とは、登録局の承認下に発行された証明書を実際に利用するサーバまたはネットワーク機器に対するサーバ管理者をさす。

### １．３．６　信頼者

信頼者とは、証明書によるサーバ機器の認証を行う個人をさす。

### １．３．７　その他の関係者

当該 CPS に従う。

## １．４　証明書の用途

### １．４．１　証明書の種類

本認証局は、利用者証明書として、登録局の審査を通過したサーバ機器に対して証明書を発行する。

### １．４．２　正規の証明書用途

ソフトバンク株式会社が（本サービスとは別途）提供する、サービスにのみ使用される。

### １．４．３　禁止されている証明書用途

本 CP １．４．１　に定められた用途以外での証明書の使用を禁止する。

## １．５　ポリシー管理

### １．５．１　文書の管理組織

本 CP 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 CP の準拠性調査担当者

規定しない。

### １．５．４　CP の承認手続き

本 CP 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

当該 CPS に従う。

## 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 CP を公開する。
その他については、当該 CPS に従う。

## ２．３　公開の時期と周期

本認証局は、本 CP 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 CP ９．１１　の規定に従い個別に通知する。
その他については、当該 CPS に従う。

## ２．４　リポジトリに対するアクセスコントロール

当該 CPS に従う。

# ３．　本人性確認と認証

## ３．１　名称

### ３．１．１　名称のタイプ

当該 CPS に従う。

### ３．１．２　名称の意味に関する要件

当該 CPS に従う。

### ３．１．３　利用者の匿名・仮名についての要件

当該 CPS に従う。

### ３．１．４　様々な名称形式を解釈するためのルール

当該 CPS に従う。

### ３．１．５　名称の一意性

当該 CPS に従う。

### ３．１．６　商標等の認識、認証および役割

当該 CPS に従う。

## 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

証明書の発行要求には、サーバの公開鍵と、それに対応する秘密鍵による電子署名が含まれる。発行要求中の公開鍵を使用して電子署名の検証を行うことにより、発行要求を作成したサーバの秘密鍵の所有を検証する。

### ３．２．２　加入者の確認

当該 CPS に従う。

### ３．２．３　利用者の確認

当該 CPS に従う。

### ３．２．４　確認されない利用者情報

当該 CPS に従う。

### ３．２．５　権限確認

当該 CPS に従う。

### ３．２．６　相互運用性基準

当該 CPS に従う。

## 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

当該 CPS に従う。

### ３．３．２　失効後の鍵（証明書）再発行時の本人性確認と認証

当該 CPS に従う。

## ３．４　失効申請時の本人性確認と認証

当該 CPS 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

本サービスの利用を加入者に認められたサーバ機器のサーバ管理者、またはそれらの代表者。

### ４．１．２　利用申請方法

本認証局は、証明書の利用申請方法として次の２つの方法を提供する。

(1)　PKCS#10 または CSR

証明書利用申請者は、登録局に対して、証明書発行要求(PKCS#10 または CSR) を添えて証明書の利用申請を行う。登録局は、(1) 証明書発行対象となるサーバが加入者から本サービスでの使用を認められたサーバであること、(2) 利用申請者が当該サーバのサーバ管理者であることを確認する。

利用申請が代表者によって行なわれた場合は、登録局は代表者の確認を行う。

また、利用申請には、利用申請者により利用者のダウンロード用パスワードも指定される。ダウンロード用パスワードは、証明書受領時に、受領者が利用者本人であることを確認するために用いられる。

(2)　SCEP

証明書利用申請者は、登録局に対して、SCEP を用いた証明書発行要求に必要となる申請用パスワードを添えて利用申請を行う。登録局は、(1)証明書発行対象となるサーバが加入者から本サービスでの使用を認められたサーバであること、(2) 利用申請者が当該サーバのサーバ管理者であることを確認する。

利用申請が代表者によって行なわれた場合は、登録局は代表者の確認を行う。

サーバ管理者は、登録局による利用申請の登録完了の通知を受けた後、当該サーバから SCEP による発行要求を行う。

## 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

本 CP ４．１．２ に従う。

### ４．２．２　証明書申請の承認または拒否

(1)　PKCS#10 または CSR

証明書の利用申請については、書類不備等を確認し、登録局が受理する。その後、登録局が本 CP ４．１．２ に規定する手続きに従い、承認を行う。定められた利用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、利用申請を拒否する。

(2)　SCEP

利用申請の書類確認および承認については、PKCS#10 と同様とする。

また、SCEP を用いた証明書発行要求に対しては、当該要求に含まれる情報を、登録局から登録された申請用パスワードをもって自動的に確認し、発行の承認または拒否を行う。

### ４．２．３　証明書申請プロセスの時間

本認証局は、証明書の利用申請を遅滞なく処理する。

ただし、申請書類に不備があった場合、これの再提出を求め、また再提出後にこれを再審査するための時間を要する。

## ４．３　証明書発行

### ４．３．１　証明書発行時の認証局の行動

(1)　PKCS#10 または CSR

登録局は、サーバ証明書の発行要求(PKCS#10 または CSR)を発行局に対して行う。

発行局は、要求送信元である登録局の正当性を確認した上で、自動的に証明書を発行する。

(2)　SCEP

登録局は、申請用パスワードを登録する。登録終了後、利用申請時に指定されたアドレス宛に Email にて登録完了通知が自動的に送信される。
本認証局は、その後、サーバからの証明書の発行要求(SCEP)を受けた場合、当該発行要求に含まれる情報を、登録局から登録された上記申請用パスワードをもって確認し、自動的に証明書を発行する。

### ４．３．２　認証局から利用者への証明書発行の通知

(1)　PKCS#10 または CSR

本認証局は、証明書発行完了後、自動的に、利用申請時に指定されたアドレス宛に Email にて発行完了通知を行う。

(2)　SCEP

本認証局は、証明書発行完了後、自動的に、利用申請時に指定されたアドレス宛に Email にて発行完了通知を行う。

## ４．４　証明書受領

### ４．４．１　証明書受領確認手続き

(1)　PKCS#10 または CSR

利用者は発行完了通知に記載される URL にアクセスし、利用者の本人確認に必要となるダウンロード用パスワードを入力して、証明書をダウンロードする。
本認証局は、利用者が証明書のダウンロードを行った際、利用申請時に指定されたアドレス宛に Email にてダウンロード完了通知を行う。通知発送後 17 日間（通知発送日を含まない）のうちに、利用者が証明書の内容等に異議を唱えない場合は受領したものとみなす。異議申し立てを受けた場合は、当該 CPS ４．９．１に従い当該証明書の失効を行い、所定の手続きに基づき再発行を行う。
なお、ダウンロードが規定回数以上失敗した場合は、当該証明書の失効を行う場合がある。

(2)　SCEP

本認証局は、SCEP により証明書のダウンロードが完了した時点で、利用申請時に指定されたアドレス宛に Email にてダウンロード完了通知を行う。通知発送後 17 日間（通知発送日を含まない）のうちに、利用者が証明書の内容等に異議を唱えない場合は受領したものとみなす。異議申し立てを受けた場合は、当該 CPS ４．９．１に従い当該証明書の失効を行い、所定の手続きに基づき再発行を行う。

### ４．４．２　認証局による証明書の公開

本認証局は、発行した証明書を公開する義務を負わない。

### 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

規定しない。

## 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

利用者による秘密鍵と証明書の用途については、本 CP １．４　に従う。
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

信頼者に対する利用者の公開鍵と証明書の用途については、本 CP １．４　に従う。
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

本認証局は、鍵ペアの更新を伴わない証明書更新を認めない。

### ４．６．２　証明書利用申請者

規定しない。

### ４．６．３　証明書申請プロセス

規定しない。

### ４．６．４　利用者への新しい証明書発行の通知

規定しない。

### ４．６．５　証明書受領確認手続き

規定しない。

### ４．６．６　認証局による新しい証明書の公開

規定しない。

### 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

規定しない。

## 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

利用者は、証明書更新に際しての証明書発行要求において、新しい鍵ペアを生成しなければならない。

### ４．７．２　新しい公開鍵に対する証明書利用申請者

本 CP ４．１．１　に従う。

### ４．７．３　鍵更新における証明書申請プロセス

本 CP ４．２　に従う。

### ４．７．４　利用者への新しい証明書発行の通知

本 CP ４．３．２　に従う。

### ４．７．５　鍵更新された証明書の受領確認手続き

本 CP ４．４．１　に従う。

### ４．７．６　鍵更新された証明書の公開

本 CP ４．４．２　に従う。

### 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

本 CP ４．４．３　に従う。

## ４．８　証明書の変更

### ４．８．１　証明書の変更に関する要件

証明書の記載内容に変更の必要が生じた場合、利用者は、登録局に対して変更申請を行うか、または代表者が存在する場合、その代表者に変更の必要が生じたことを伝え、変更申請を行うよう要請しなければならならい。

要請を受けた代表者、または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代表者は、登録局に対して変更申請を行わなければならない。

本認証局は、当該証明書の失効と、変更内容を反映した新しい証明書の発行を行う。

### ４．８．２　証明書変更申請者

本 CP ４．１．１　に従う。

### ４．８．３　証明書変更申請プロセス

利用者証明書の変更申請については、書類不備等を確認し、登録局が受理する。その後、登録局は本 CP ４．１．２　に規定する手続きに従い、承認を行う。定められた変更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、変更申請を拒否する。

本認証局は、変更申請が承認された場合、当該利用者の証明書を失効し、その後、変更内容を反映した新しい証明書の発行を行う。

### ４．８．４　利用者への新しい証明書発行の通知

変更申請により、新しい証明書が発行された場合の通知は、本 CP ４．３．２　に従う。

### ４．８．５　変更された証明書の受領確認手続き

本 CP ４．４．１　に従う。

### ４．８．６　変更された証明書の公開

本 CP ４．４．２　に従う。

### 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

本 CP ４．４．３　に従う。

## ４．９　証明書の失効と一時停止

### ４．９．１　失効の要件

当該 CPS に従う。

### ４．９．２　失効申請者

当該 CPS に従う。

### ４．９．３　失効申請プロセス

当該 CPS に従う。

### ４．９．４　失効申請までの猶予期間

当該 CPS に従う。

### ４．９．５　失効申請プロセスの時間

当該 CPS に従う。

### ４．９．６　信頼者による失効情報確認の要件

当該 CPS に従う。

### ４．９．７　CRL 発行周期

当該 CPS に従う。

### 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

当該 CPS に従う。

### ４．９．９　オンラインでの証明書の有効性確認

当該 CPS に従う。

### ４．９．１０　オンラインでの証明書の失効情報確認要件

当該 CPS に従う。

### ４．９．１１　その他の利用可能な失効情報確認の手段

当該 CPS に従う。

### ４．９．１２　鍵の危殆化の特別な要件

当該 CPS に従う。

### ４．９．１３　一時停止の要件

当該 CPS に従う。

### ４．９．１４　一時停止申請者

当該 CPS に従う。

### ４．９．１５　一時停止申請の手続き

当該 CPS に従う。

### ４．９．１６　一時停止可能な期間

当該 CPS に従う。

## ４．１０　証明書ステータス確認サービス

当該 CPS に従う。

### ４．１０．１　運用上の特徴

当該 CPS に従う。

### ４．１０．２　サービスの可用性

当該 CPS に従う。

### ４．１０．３　他の特徴

当該 CPS に従う。

## ４．１１　認証局への登録の終了

当該 CPS に従う。

## 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

当該 CPS に従う。

### 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

当該 CPS に従う。

# 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

当該 CPS に従う。

### ５．１．２　物理的アクセス

当該 CPS に従う。

### ５．１．３　電源設備と空調設備

当該 CPS に従う。

### ５．１．４　水害対策

当該 CPS に従う。

### ５．１．５　火災に対する予防措置と対策

当該 CPS に従う。

### ５．１．６　媒体保管場所

当該 CPS に従う。

### ５．１．７　廃棄物処理

当該 CPS に従う。

### ５．１．８　オフサイトバックアップ

当該 CPS に従う。

## ５．２　　職務統制

### ５．２．１　　信頼される役割

当該 CPS に従う。

### ５．２．２　　役割ごとに必要な人員の数

当該 CPS に従う。

### ５．２．３　　各役割における本人性確認と認証

当該 CPS に従う。

### ５．２．４　　職務の分離が要求される役割

当該 CPS に従う。

## 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

当該 CPS に従う。

### ５．３．２　　身元調査手続き

当該 CPS に従う。

### ５．３．３　　教育訓練要件

当該 CPS に従う。

### ５．３．４　　教育訓練の周期

当該 CPS に従う。

### ５．３．５　　ジョブローテーションの周期と順序

当該 CPS に従う。

### ５．３．６　許可されていない行動に対する罰則

当該 CPS に従う。

### ５．３．７　職員に対する契約要件

当該 CPS に従う。

### ５．３．８　職員が参照できるドキュメント

当該 CPS に従う。

## 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

当該 CPS に従う。

### ５．４．２　監査ログを処理する頻度

当該 CPS に従う。

### ５．４．３　監査ログの保持期間

当該 CPS に従う。

### ５．４．４　監査ログの保護

当該 CPS に従う。

### ５．４．５　監査ログのバックアップ手続き

当該 CPS に従う。

### ５．４．６　監査ログ収集システム（内部、外部）

当該 CPS に従う。

### ５．４．７　当事者に対する通知

当該 CPS に従う。

### ５．４．８　脆弱性評価

当該 CPS に従う。

## ５．５　アーカイブ

### ５．５．１　アーカイブの種類

当該 CPS に従う。

### ５．５．２　アーカイブの保持期間

当該 CPS に従う。

### ５．５．３　アーカイブの保護

当該 CPS に従う。

### ５．５．４　アーカイブのバックアップ手続き

当該 CPS に従う。

### ５．５．５　アーカイブの日付要件

当該 CPS に従う。

### ５．５．６　アーカイブ収集システム（内部、外部）

当該 CPS に従う。

### ５．５．７　アーカイブ情報の入手と検証手続き

当該 CPS に従う。

## ５．６　認証局の鍵更新

当該 CPS に従う。

## 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

当該 CPS に従う。

### 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

当該 CPS に従う。

### ５．７．３　利用者秘密鍵危殆化時の手続き

当該 CPS に従う。

### 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

当該 CPS に従う。

## ５．８　認証局の業務終了

当該 CPS に従う。

# 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

証明書に係る鍵ペアの生成は、サーバ管理者が行う。その方法には関知しない。

### ６．１．２　利用者への秘密鍵の配送

本認証局は、利用者の秘密鍵を配送しない。

### ６．１．３　本認証局への公開鍵の配送

証明書発行要求データ中に公開鍵を含むことにより､本認証局への公開鍵の配送を行う。

### ６．１．４　信頼者への認証局公開鍵の配送

当該 CPS に従う。

### ６．１．５　鍵長

証明書に係る鍵は、下記の仕様に適合する鍵を利用する。

(1)　署名方式　　:　　SHA-1withRSA、SHA-256withRSA

(2)　合成数　　:　　1024 bit、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 CP 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。

## 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

本認証局は、利用者の秘密鍵には関知しない。

### ６．２．２　秘密鍵の複数人管理（n out of m）

本認証局は、利用者の秘密鍵には関知しない。

### ６．２．３　秘密鍵の預託

本認証局は、利用者の秘密鍵には関知しない。

### ６．２．４　秘密鍵のバックアップ

本認証局は、利用者の秘密鍵には関知しない。

### ６．２．５　秘密鍵のアーカイブ

本認証局は、利用者の秘密鍵には関知しない。

### 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

本認証局は、利用者の秘密鍵には関知しない。

### ６．２．７　秘密鍵管理モジュール内での秘密鍵保存

本認証局は、利用者の秘密鍵には関知しない。

### ６．２．８　秘密鍵の活性化

本認証局は、利用者の秘密鍵には関知しない。

### ６．２．９　秘密鍵の非活性化

本認証局は、利用者の秘密鍵には関知しない。

### ６．２．１０　秘密鍵破壊の方法

本認証局は、利用者の秘密鍵には関知しない。

### ６．２．１１　秘密鍵管理モジュールの評価

本認証局は、利用者の秘密鍵には関知しない。

## 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

証明書は、その有効期間の終了後、２年間保存する。

### ６．３．２　証明書と鍵ペアの使用期間

証明書の有効期間は、3 年 2 ヶ月以内とする。

## 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

利用者の秘密鍵の活性化情報については関知しない。

### ６．４．２　活性化情報の保護

利用者の秘密鍵の活性化情報は、利用者の責任を持って管理しなければならない。

### 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

当該 CPS に従う。

### ６．５．２　コンピュータセキュリティの評価

当該 CPS に従う。

## 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

当該 CPS に従う。

### ６．６．２　セキュリティマネジメント管理

当該 CPS に従う。

### ６．６．３　ライフサイクルセキュリティの管理

当該 CPS に従う。

## ６．７　ネットワークセキュリティ管理

当該 CPS に従う。

## ６．８　日時の記録

当該 CPS に従う。

# 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

本 CP 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。

### ７．１．２　証明書拡張領域

本 CP 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。

### ７．１．３　アルゴリズムオブジェクト識別子

本 CP 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。

### ７．１．４　名前の形式

本 CP 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。

### ７．１．５　名称制約

規定しない。

### ７．１．６　証明書ポリシーオブジェクト識別子

本 CP 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。

### ７．１．７　ポリシー制約拡張の使用

規定しない。

### ７．１．８　ポリシー修飾子の構文と意味

本 CP 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。

### ７．１．９　重要な証明書ポリシー拡張についての処理方法

規定しない。

## ７．２　CRL プロファイル

### ７．２．１　バージョン番号

当該 CPS に従う。

### ７．２．２　CRL、CRL エントリ拡張

当該 CPS に従う。

## ７．３　OCSP プロファイル

### ７．３．１　バージョン番号

当該 CPS に従う。

### ７．３．２　OCSP 拡張

当該 CPS に従う。

# ８．　準拠性監査とその他の評価

## ８．１　監査の頻度と要件

当該 CPS に従う。

## ８．２　監査人の要件

当該 CPS に従う。

## ８．３　監査人と被監査者の関係

当該 CPS に従う。

## ８．４　監査の範囲

当該 CPS に従う。

## ８．５　監査における指摘事項への対応

当該 CPS に従う。

## ８．６　監査結果の開示

当該 CPS に従う。

# 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

当該 CPS に従う。

### ９．１．２　証明書へのアクセス料金

当該 CPS に従う。

### ９．１．３　失効またはステータス情報へのアクセス料金

当該 CPS に従う。

### ９．１．４　その他のサービスに関する料金

当該 CPS に従う。

### ９．１．５　払い戻し指針

当該 CPS に従う。

## ９．２　金銭上の責任

### ９．２．１　保険の適用範囲

当該 CPS に従う。

### ９．２．２　その他の資産

当該 CPS に従う。

### ９．２．３　利用者を保護する保険、保証

当該 CPS に従う。

## ９．３　企業情報の秘密性

### ９．３．１　秘密情報の範囲

当該 CPS に従う。

### ９．３．２　秘密情報の範囲外の情報

当該 CPS に従う。

### ９．３．３　秘密情報の保護責任

当該 CPS に従う。

## ９．４　個人情報の保護

### ９．４．１　プライバシープラン

当該 CPS に従う。

### ９．４．２　プライバシーとして扱われる情報

当該 CPS に従う。

### ９．４．３　プライバシーとみなされない情報

当該 CPS に従う。

### ９．４．４　個人情報を保護する責任

当該 CPS に従う。

### ９．４．５　個人情報の使用に関する個人への通知および承認

当該 CPS に従う。

### ９．４．６　司法手続または行政手続に基づく公開

当該 CPS に従う。

### ９．４．７　他の情報公開の場合

当該 CPS に従う。

## ９．５　知的財産権

当該 CPS に従う。

## ９．６　表明および保証

### ９．６．１　発行局の表明および保証

当該 CPS に従う。

### ９．６．２　登録局の表明および保証

当該 CPS に従う。

### ９．６．３　加入者の表明および保証

当該 CPS に従う。

### ９．６．４　利用者の表明および保証

当該 CPS に従う。

### ９．６．５　信頼者の表明および保証

当該 CPS に従う。

### ９．６．６　他の関係者の表明および保証

当該 CPS に従う。

## ９．７　無保証

当該 CPS に従う。

## ９．８　責任制限

### ９．８．１　利用者の義務違反

当該 CPS に従う。

### ９．８．２　信頼者の義務違反

当該 CPS に従う。

### ９．８．３　不可抗力等

当該 CPS に従う。

### ９．８．４　賠償

当該 CPS に従う。

## ９．９　補償

当該 CPS に従う。

## ９．１０　文書の有効期間と終了

### ９．１０．１　文書の有効期間

本 CP は、ポリシー承認局の承認を得た後、指定された有効開始日より有効となる。本 CP ９．１０．２　で記載する本 CP の終了をもって有効期間を終了する。

### ９．１０．２　終了

当該CPS ９．１０．２に記載する当該CPSの終了またはポリシー承認局により承認された本CP終了日をもって、本CPは無効となる。

### ９．１０．３　終了の影響と存続条項

当該CPSに従う。

## ９．１１　個々の関係者間に対する通知と連絡

当該CPSに従う。

## 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CP の改訂・承認を行う。

### ９．１２．２　通知方法と期間

当該CPSに従う。

### ９．１２．３　オブジェクト識別子の変更理由

当該CPSに従う。

## ９．１３　紛争解決手続き

当該CPSに従う。

## ９．１４　準拠法

当該CPSに従う。

## ９．１５　適用される準拠法

当該 CPS に従う。

## ９．１６　その他の条項

### ９．１６．１　完全合意

当該 CPS に従う。

### ９．１６．２　譲渡

当該 CPS に従う。

### ９．１６．３　分離可能性

当該 CPS に従う。

### ９．１６．４　執行（弁護士費用と権利の放棄）

当該 CPS に従う。

# １０．　【別紙 1】　用語集

当該 CPS 参照。

# １１．　【別紙 2】　証明書プロファイル

## １１．１　サーバ証明書

(1) Basic

SHA-1 認証局

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

| subject | | |
|---|---|---|
| CountryName | | 証明書所有者の国名 |
| type | 型: OID | 国名のオブジェクトID |
| | 値: 2 5 4 6 | |
| | | |
| value | 型: PrintableString | 国名の値 |
| | 値: JP | |
| | | JP ※固定 |
| StateOrProvinceName | | 証明書所有者の都道府県名 |
| type | 型: OID | 都道府県名のオブジェクトID |
| | 値: 2 5 4 8 | |
| | | |
| value | 型: PrintableString | 都道府県名の値 |
| | 値: (都道府県名) | *加入企業の道府県名(英字) |
| | | |
| LocalityName | | 証明書所有者の所在地 |
| type | 型: OID | 所在地のオブジェクトID |
| | 値: 2 5 4 7 | |
| | | |
| value | 型: PrintableString | 所在地の値 |
| | 値: (所在地住所) | *加入企業の所在地(英語) |
| | | |
| OrganizationName | | 証明書発行者の組織名 |
| type | 型: OID | 組織名のオブジェクトID |
| | 値: 2 5 4 10 | |
| | | |
| value | 型: PrintableString | 組織名の値 |
| | 値: SOFTBANK TELECOM Corp. | |
| | | |
| OrganizationalUnitName | | 証明書発行者の部門名 |
| type | 型: OID | 部門名のオブジェクトID |
| | 値: 2 5 4 11 | |
| | | |
| value | 型: PrintableString | 部門名の値 |
| | 値: (サービス加入企業組織名等) | *加入企業の組織名等 |
| | | |
| CommonName | | 証明書所有者の固有名称 |
| type | 型: OID | 固有名称のオブジェクトID |
| | 値: 2 5 4 3 | |
| | | |
| value | 型: PrintableString | 固有名称の値 |
| | 値: (利用者の氏名) | *利用者の氏名(ローマ字表記) |
| **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 | 暗号アルゴリズムのオブジェクトID |
| | 値: 1 2 840 113549 1 1 1 | |
| | | |
| parameters | 型: NULL | 暗号アルゴリズムの引数 |
| | 値: NULL | |
| | | |
| subjectPublicKey | 型: BIT STRING | 公開鍵値 |
| | 値: 公開鍵値 | |

SHA-256 認証局

| version | 値 | 説明 |
|---|---|---|
| Version | | 証明書フォーマットのバージョン番号 |
| | 型:INTEGER | |
| | 値:2 | 2 (Ver.3) |
| **serialNumber** | | |
| CertificateSerialNumber | | 証明書のシリアル番号 |
| | 型:INTEGER | |
| | 値:ユニークな整数 | |
| **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<br>(公開鍵暗号とハッシュ関数) |
| algorithm | 型:OID<br>値:1.2.840.113549.1.1.11<br>(SHA256withRSAEncryption) | 暗号アルゴリズムのオブジェクトID |
| parameters | 型:NULL<br>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<br>値:2 5 4 6 | 国名のオブジェクトID |
| value | 型:PrintableString<br>値:JP | 国名の値 |
| OrganizationName | | 証明書発行者の組織名 |
| type | 型:OID<br>値:2 5 4 10 | 組織名のオブジェクトID |
| value | 型:PrintableString<br>値:SOFTBANK TELECOM CO., LTD. | 組織名の値 |
| CommonName | | 証明書発行者の固有名称 |
| type | 型:OID<br>値:2 5 4 3 | 固有名称のオブジェクトID |
| value | 型:PrintableString<br>値:PKI PLATFORM CA G2 | 固有名称の値<br>証明書を発行する認証局名 |
| **validity** | | |
| Validity | | 証明書の有効期間 |
| notBefore | 型:UTC Time<br>値:yymmddhhmmssZ | 有効開始日時 |
| notAfter | 型:UTC Time<br>値:yymmddhhmmssZ | 終了日時 |
| **subject** | | |
| CountryName | | 証明書所有者の国名 |
| type | 型:OID<br>値:2 5 4 6 | 国名のオブジェクトID |
| value | 型:PrintableString<br>値:JP | 国名の値 |
| OrganizationName | | 証明書所有者の組織名 |
| type | 型:OID<br>値:2 5 4 10 | 組織名のオブジェクトID |
| value | 型:PrintableString<br>値:PKI PLATFORM Corp. | 組織名の値 |
| OrganizationalUnitName | | 証明書所有者の部門名 |
| type | 型:OID<br>値:2 5 4 11 | 部門名のオブジェクトID |
| value | 型:PrintableString<br>値:(サービス加入企業の顧客識別子) | 部門名の値<br>*加入企業の顧客識別子 |
| CommonName | | 証明書所有者の固有名称 |
| type | 型:OID<br>値:2 5 4 3 | 固有名称のオブジェクトID |
| value | 型:PrintableString<br>値:Webサーバー／ネットワーク機器のFQDN | 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<br>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<br>値:NULL | 暗号アルゴリズムの引数 |
| subjectPublicKey | 型:BIT STRING<br>値:公開鍵値 | 公開鍵値 |

## (2) Standard Extensions

SHA-1 認証局

| **authoritytKeyIdentifier (entnID :== 2 5 29 35, critical :== FALSE)** | **値** | **説明** |
|---|---|---|
| AuthorityKeyIdentifier | | 認証局の公開鍵識別子 |
| keyIdentifier | 型: OctetString | 公開鍵の識別子 |
| | 値: 認証局のsubjectPublicKeyのHASH値 | |
| | | |
| authorityCertSerialNumber | 型: INTEGER | 認証局の証明書のシリアル番号 |
| | 値: 認証局のシリアル番号 | |
| | | |
| authorityCertIssuer | | 認証局に関する情報 |
| directoryName | 型: PrintableString | ディレクトリ名 |
| CountryName | | 証明書発行者の国名 |
| type | 型: OID | 国名のオブジェクトID |
| | 値: 2 5 4 6 | |
| | | |
| value | 型: PrintableString | 国名の値 |
| | 値: JP | |
| | | |
| OrganizationName | | 証明書発行者の組織名 |
| type | 型: OID | 組織名のオブジェクトID |
| | 値: 2 5 4 10 | |
| | | |
| value | 型: PrintableString | 組織名の値 |
| | 値: JAPAN TELECOM CO., LTD. | |
| | | |
| CommonName | | 証明書所有者の固有名称 |
| type | 型: OID | 固有名称のオブジェクトID |
| | 値: 2 5 4 3 | |
| | | |
| value | 型: PrintableString | 固有名称の値 |
| | 値: JAPAN TELECOM CA | |
| | | |
| **subjectKeyIdentifier (entnID :== 2 5 2 14 , critical :== FALSE)** | | |
| SubjectKeyIdentifier | | 証明書所有者の公開鍵に関する情報 |
| keyIdentifier | 型: OCTET STRING | 公開鍵の識別子 |
| | 値: 所有者のsubjectPublicKeyのHash値 | |
| | | |
| **keyUsage (entnID :== 2 5 29 15, critical :== TRUE)** | | |
| KeyUsage | | 鍵の使用目的 |
| | 型: BitString | |
| | 値: 101100000 | digitalSignature,keyEnciperment,DataEnciperment |
| | | (DataEnciphermentは記載有無選択可、標準は無し) |
| **privateKeyUsagePeriod (entnID :== 2 5 29 16, critical :== -)** | | |
| privateKeyUsagePeriod | | 秘密鍵使用期間 |
| | 設定しない | |
| | | |
| **certificatePolicies (entnID :== 2 5 29 32, critical :== FALSE)** | | |
| PolicyInformation | | 証明書ポリシー |
| CertPolicyID | 型: OID | ポリシーID |
| | 値: 1.3.6.1.4.1.1657.105.1.2 | PKIプラットフォーム サーバ証明書 |
| | | |
| **PolicieMapping (entnID :== 2 5 29 33, critical :== -)** | | |
| policyMapping | | ポリシーマッピング |
| | 設定しない | |
| | | |
| **subjectAltName (entnID :== 2 5 29 17, critical :== FALSE)** | | |
| subjectAltName | 型: PrintableString | 証明書主体者別名(記載有無選択可) |
| | 値: (証明書主体者別名) | |
| | | |
| **issuerAltName (entnID :== 2 5 29 18, critical :== -)** | | |
| issuerAltName | | 証明書発行者別名 |
| | 設定しない | |
| | | |
| **subjectDirecotryAttribute (entnID :== 2 5 29 9, critical :== -)** | | |
| subjectDirecotryAttribute | | 証明書利用者ディレクトリ属性 |
| | 設定しない | |
| | | |

| | | |
|---|---|---|
| **basicConstraints (entnID :== 2 5 29 19, critical :== -)** | | |
| basicConstraints | | 基本的制限 |
| cA | 設定しない | CAかどうかを示すフラグ |
| pathLenConstraints | 設定しない | |
| | | |
| **nameConstraints (entnID :== 2 5 29 30, critical :== -)** | | |
| nameConstraints | | 名称制約 |
| | 設定しない | |
| | | |
| **policyConstraints (entnID :== 2 5 29 36, critical :== -)** | | |
| policyConstraints | | ポリシー制約 |
| | 設定しない | |
| | | |
| **extendKeyUsage (entnID :== 2 5 29 37, critical :== FALSE)** | | |
| extendKeyUsage | | 拡張した鍵の使用目的 |
| | 設定しない | |
| | | |
| **cRLDistributionPoints (entnID :== 2 5 29 31, critical :== FALSE)** | | |
| cRLDistributionPoints | | CRL配布ポイント |
| DistributionPoint | 設定しない | |
| fullName | | CRLを配布するURI |
| uniformResourceIdentifier | | |
| | | |
| **inhibitAnyPolicy (entnID :== 2 5 29 54, critical :== -)** | | |
| InhibitAnyPolicy | | 全ポリシー禁止 |
| | 設定しない | |
| | | |
| **FreshestCRL (entnID :== 2 5 29 46, critical :== -)** | | |
| freshestCrl | | デルタCRL |
| | 設定しない | |
| | | |

SHA-256 認証局

| **certificatePolicies (entnID :== 2 5 29 32, critical :== FALSE)** | | |
|---|---|---|
| PolicyInformation | | 証明書ポリシー |
| CertPolicyID | 型:OID | ポリシーID |
| | 値:1.3.6.1.4.1.1657.105.1.2 | PKIプラットフォーム サーバ証明書 |
| | | |
| **keyUsage (entnID :== 2 5 29 15, critical :== TRUE)** | | |
| KeyUsage | | 鍵の使用目的 |
| | 型:BitString | |
| | 値:101000000 | digitalSignature,keyEnciperment |
| | | |
| **authoritytKeyIdentifier (entnID :== 2 5 29 35, critical :== FALSE)** | **値** | **説明** |
| AuthorityKeyIdentifier | | 認証局の公開鍵識別子 |
| keyIdentifier | 型:OctetString | 公開鍵の識別子 |
| | 値:認証局のsubjectPublicKeyのHASH値 | |
| | | |
| authorityCertSerialNumber | 型:INTEGER | 認証局の証明書のシリアル番号 |
| | 値:認証局のシリアル番号(01) | |
| | | |
| authorityCertIssuer | | 認証局に関する情報 |
| directoryName | 型:PrintableString | ディレクトリ名 |
| CountryName | | 証明書発行者の国名 |
| type | 型:OID | 国名のオブジェクトID |
| | 値:2 5 4 6 | |
| | | |
| value | 型:PrintableString | 国名の値 |
| | 値:JP | |
| | | |
| OrganizationName | | 証明書発行者の組織名 |
| type | 型:OID | 組織名のオブジェクトID |
| | 値:2 5 4 10 | |
| | | |
| value | 型:PrintableString | 組織名の値 |
| | 値:SOFTBANK TELECOM CO., LTD. | |
| | | |
| CommonName | | 証明書発行者の固有名称 |
| type | 型:OID | 固有名称のオブジェクトID |
| | 値:2 5 4 3 | |
| | | |
| value | 型:PrintableString | 固有名称の値 |
| | 値:PKI PLATFORM CA G2 | |
| | | |
| **subjectKeyIdentifier (entnID :== 2 5 2 14 , critical :== FALSE)** | | |
| SubjectKeyIdentifier | | 証明書所有者の公開鍵に関する情報 |
| keyIdentifier | 型:OCTET STRING | 公開鍵の識別子 |
| | 値:所有者のsubjectPublicKeyのHash値 | |
| | | |

## (3) Private Internet Extensions

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