XiPS 認証局証明書ポリシー
(Certificate Policy)

Version1.4

2017年9月5日

株式会社シーサイドネット

更新履歴

Version 1.0	2008/07/16	初版発行
Version 1.1	2012/12/14	RootCAの変更
Version 1.2	2014/07/31	証明書のプロファイルの変更
Version 1.3	2015/02/16	証明書のプロファイルを追加
Version 1.4	2017/09/05	連絡先とCAA対応の修正

目次

1.はじめに

1.1 概要

XiPS 認証局証明書ポリシー（以下、「本CP」といいます）は、株式会社シーサイドネット（以下「シーサイドネット」といいます）が認証局（以下、「CA」といいます）として発行する電子証明書の用途、利用者手続、発行手続等、電子証明書に関するポリシーを規定するものである。本CA の運用維持に関する諸手続については、セコム認証基盤運用規程（以下、「CPS」という）に規定する。
本 CA は、Security Communication RootCA1、Security Communication RootCA2 より、片方向相互認証証明書を発行されている。
本 CA が発行する証明書は、通信経路で情報の暗号化を行うことに利用する。また、発行対象は、シーサイドネットが提供するサービスの契約を必要とし、証明書はサービスのシステム上で使用するものとする。
本 CA から証明書の発行を受ける者は、証明書の発行を受ける前に自己の利用目的と本CP 及びCPS とを照らし合わせて評価し、本CP 及びCPS を承諾する必要がある。
本CAは、CA/Browser Forumがhttps://www.cabforum.org/で公開する「Baseline Requirements」に準拠している。

本 CP は、IETF が認証局運用のフレームワークとして提唱するRFC3647「Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework」に準拠している。
本 CP は、本CA に関する技術面、運用面の発展や改良に伴い、それらを反映するために必要に応じ改訂されるものとする。

1.2 文書名と識別

本 CP の正式名称は、「XiPS 認証局証明書ポリシー」という。本CA では、発行する証明書の
種類及び発行基準に応じて一意となるオブジェクト識別子（以下、OID という）が割り当てられ、各証明書内に示すものとする。本CA が本CP に基づき発行する証明書及び対応するOID、並びに本CP が参照するCPS のOID は、次のとおりである。
CP OID
XiPS 認証局証明書ポリシー1.2.392.200091.110.171.1
XiPS2 認証局証明書ポリシー1.2.392.200091.110.171.2
CPS OID
セコム電子認証基盤認証運用規程1.2.392.200091.100.401.1

1.3 PKI の関係者

1.3.1 認証局

CA（Certification Authority：認証局）とは、IA（Issuing Authority：発行局）及びRA（Registration
Authority：登録局）によって構成する。IA は、証明書の発行、取消、CRL（Certificate Revocation
List：証明書失効リスト）の開示等を行い、RA は、証明書の発行、取消を申請する申請者の審査及び証明書を発行、失効するための登録業務等を行う。

1.3.2 登録局

上記に含む

1.3.3 証明書利用者

証明書利用者とは、シーサイドネットが提供するサービスの契約と合わせ、証明書を申請する個人、法人及び組織とする。

1.3.4 検証者

検証者とは、電子署名の付されたメッセージ等について、その電子署名が間違いなく証明書利用者によって行われているということを検証する者をいう。

1.4 証明書の用途

適切な証明書の用途
本 CA が発行する証明書は、通信経路で情報の暗号化を行うことに利用する。

1.4.1 禁止される証明書の用途

CA が発行する証明書の用途は「1.4.1 適切な証明書の用途」のとおりであり、証明書をそれ以外の目的に利用することはできないものとする。

1.5 ポリシー管理

1.5.1 文書を管理する組織

本 CP の維持、管理は、シーサイドネットが行う。

1.5.2 連絡先

本 CP に関する連絡先は、次のとおりである。
窓口：株式会社シーサイドネット

住所：東京都千代田区三番町 14-2 シーサイドビル
e-Mail：ssl.pfw@cssv.jp

1.5.3 ポリシー適合性を決定する者

本 CP の内容について、シーサイドネットポリシー管理者において決定される。

1.5.4 承認手続

本 CP は、シーサイドネットポリシー管理者の承認によって発効される。

2. 公開とリポジトリの責任

2.1 リポジトリ

本 CA は、リポジトリを24 時間365 日利用できるように維持管理を行う。ただし、利用可能な時間内においてもシステム保守等により利用できない場合がある。

2.2 証明情報の公開

本 CA は、証明書失効リスト（以下「CRL」という）、本CP およびCPS をリポジトリ上に公
開し、証明書利用者および検証者がオンラインによって閲覧できるようにする。

2.3 公開の時期又は頻度

本 CP 及びCPS は、改訂の都度、リポジトリ上に公開する。
本 CA は、24 時間ごとに新たなCRL を発行し、リポジトリ上に公開する。また、証明書の失効が行われた場合、即時に新たなCRL を発行し、リポジトリ上に公開する。また、証明書の有効期間を過ぎたものはCRL から削除する。

2.4 リポジトリへのアクセス管理

本 CA は、リポジトリでの公開情報に関して、特段のアクセスコントロールは行わない。証明書利用者は、本CA のCRL を、リポジトリを通じて入手することを可能とする。リポジトリへのアクセスは、一般的なWeb インターフェースを通じて可能とする。

3. 識別と認証

3.1 名前決定

3.1.1 名前の種類

本 CA が発行する証明書に記載される発行者及び証明書利用者の名前は、X.500 シリーズの識別名規定に従い設定する。

3.1.2 名前が意味を持つことの必要性

本 CA が発行する証明書中に用いられるコモンネームの有用性は、証明書利用者が本 CA が発行する証明書をインストールする予定のサーバのDNS 内で使われるホスト名とする。

3.1.3 加入者の匿名性又は仮名性

本 CA が発行する証明書のコモンネームには、匿名や仮名での登録は行わないものとする。

3.1.4 様々な名前形式を解釈するための規則

様々な名前の形式を解釈する規則は、X.500 シリーズの識別名規定に従う。

3.1.5 名前の一意性

本 CA が発行する証明書に記載される識別名(DN) (distinguished name) の属性は、通常発行対象となるサーバに対して一意なものとする。

3.1.6 認識、認証及び商標の役割

シーサイドネットは、証明書申請に記載される名称について知的財産権を有しているかどうかの検証を行わない。証明書利用者は、第三者の登録商標や関連する名称を、本CA に申請してはならない。シーサイドネットは、登録商標等を理由に証明書利用者と第三者間で紛争が起こった場合、仲裁や紛争解決は行わない。また、紛争を理由に証明書利用者からの証明書申請の拒絶や発行された証明書失効をする権利を有する。

3.2 初回の本人確認

証明書利用者が私有鍵を所有していることの証明は、証明書発行要求（Certificate Signing Request：以下、「CSR」という）の署名の検証を行い、当該CSR が、公開鍵に対応する私有鍵で署名されていることを確認する。
また、証明書利用者は証明書申請情報とシーサイドネットのサービスの契約情報が一致す

ることをもって、シーサイドネットのサービス契約者であることを確認し、契約者からの申請により証明書を発行する。

3.3 鍵更新申請時の本人性確認と認証

鍵更新時における証明書利用者の本人性確認及び認証は、「3.2 初回の本人性確認」と同様とします。

3.4 失効申請時の本人性確認と認証

証明書の失効申請者が証明書の契約者本人であることの証明は、失効申請時に提出される情報と証明書の契約情報が一致することをもって行うこととする。

4. 証明書のライフサイクルに対する運用上の要件

4.1 証明書申請

4.1.1 証明書申請を提出することができる者

証明書の発行申請を行うことができる者は、シーサイドネットのサービス契約者、又は契約組織の担当者とする。

4.1.2 登録手続及び責任

証明書利用者は、証明書の発行申請を行うにあたり、本CP 及びCPS の内容を承諾した上で申請を行うものとする。また、本CA に対する申請内容が正確な情報であることを保証しなければならない。

4.2 証明書申請手続

4.2.1 本人性確認と認証の実施

本 CA は、本CP「3.2. 初回の本人確認」に記載の情報をもって、申請情報の審査を行う。

4.2.2 証明書申請の承認又は却下

本 CA は、審査の結果、承認を行った申請について証明書の発行登録を行いう。
不備がある申請については、申請を却下し、申請を行った者に対し申請の再提出を依頼す。

4.2.3 証明書申請の処理時間

本 CA は、承認を行った申請について、適時証明書の発行登録を行う。

4.2.4 CAA レコードの確認

本CAは、申請情報の審査時にCAAレコードを確認する。CAAレコードに記載する本CAのドメインは「xips.jp」とする。

4.3 証明書の発行

4.3.1 証明書発行時の処理手続

本 CA は、受け付けた申請に対し、証明書の発行が完了した後、発行した証明書をシーサイドネットが管理する証明書利用者のサーバに配置する。

4.3.2 証明書利用者への証明書発行通知

本 CA はシーサイドネットが管理する証明書利用者のサーバに証明書を配置し、設定完了の

通知を行うことで、証明書発行通知とする。

4.4 証明書の受領確認

4.4.1 証明書の受領確認手続

シーサイドネットが管理する証明書利用者のレンタルサーバに証明書を配置することで証明書の受領とする。

4.4.2 認証局による証明書の公開

本 CA は、証明書利用者の証明書の公開は行わない。

4.4.3 他のエンティティに対する認証局の証明書発行通知

本 CA は、第三者に対する証明書の発行通知は行わない。

4.5 鍵ペア及び証明書の用途

4.5.1 証明書利用者の私有鍵及び証明書の用途

証明書利用者は、私有鍵及び証明書の用途として、サーバ認証や、通信経路で情報の暗号化を行うことに利用する。証明書利用者は、本CA が承認をした用途のみに当該証明書及び対応する私有鍵を利用するものとする。その他の用途に利用してはならない。

4.5.2 信頼者の公開鍵及び証明書の用途

検証者は、本CA の証明書を使用し、本CA が発行した証明書の信頼性を検証することができる。本CA が発行した証明書の信頼性を検証し、信頼する前に、本CP 及びCPS の内容について理解し、承諾しなければならない。

4.6 証明書の更新

私有鍵の更新を行わない証明書更新は行わない。

4.7 鍵更新を伴う証明書の更新

4.7.1 更新事由

証明書の更新は、証明書の有効期間が満了する場合に行う。

4.7.2 新しい証明書の申請を行うことができる者

「4.1.1.証明書申請を提出することができる者」と同様とする。

4.7.3 更新申請の処理

「4.3.1.証明書発行時の処理手続」と同様とする。

4.7.4 証明書利用者に対する新しい証明書の通知

「4.3.2.証明書利用者への証明書発行通知」と同様とする。

4.7.5 鍵更新された証明書の受領確認手続き

「4.4.1.証明書の受領確認手続」と同様とする。

4.7.6 認証局による鍵更新済みの証明書の公開

「4.4.2.認証局による証明書の公開」と同様とする。

4.7.7 他のエンティティに対する認証局の証明書発行通知

「4.4.3.他のエンティティに対する認証局の証明書発行通知」と同様とする。

4.8 証明書の変更

本 CA は、証明書に登録された情報の変更が必要となった場合、その証明書の失効及び新規発行とする。

4.8.1 証明書の変更事由

規定しない。

4.8.2 証明書の変更を申請することができる者

規定しない。

4.8.3 変更申請の処理

規定しない。

4.8.4 証明書利用者に対する新しい証明書発行通知

規定しない。

4.8.5 変更された証明書の受領確認の行為

規定しない。

4.8.6 認証局による変更された証明書の公開。

規定しない。

4.8.7 他のエンティティに対する認証局の証明書発行通知

規定しない。

4.9 証明書の失効と一時停止

4.9.1 証明書失効事由

証明書利用者は、次の事由が発生した場合、シーサイドネットに対し速やかに証明書の失効申請を行わなければならない。

- 証明書記載情報に変更があった場合
- 私有鍵の盗難、紛失、漏洩、不正利用等により私有鍵が危殆化した又は危殆化のおそれがある場合
- 証明書の内容、利用目的が正しくない場合
- 証明書の利用を中止する場合

また、シーサイドネットは、次の事由が発生した場合に、シーサイドネットの判断により証明書利用者の証明書を失効することができる。

- 証明書利用者が本CP、CPS、関連する契約又は法律に基づく義務を履行していない場合
- 本 CA の私有鍵が危殆化した又は危殆化のおそれがあると判断した場合
- シーサイドネットが失効を必要とすると判断するその他の状況が認められた場合

4.9.2 証明書失効を申請することができる者

証明書の失効の申請を行うことができる者は、シーサイドネットのサービス契約者、又は契約組織の担当者とする。なお、本CP/CPS「4.9.1. 証明書失効事由」に該当すると本CAが判断した場合、本CA が失効申請者となる。

4.9.3 失効申請手続

失効申請者は、本CP「3.4. 失効申請時の本人性確認と認証」に定める手続きを行うことにより本CA へ届け出るものとする。
本 CA は、所定の手続によって受け付けた情報を確認し、証明書の失効処理を行う。

4.9.4 失効申請の猶予期間

失効申請を行うものは、私有鍵が危殆化した又は危殆化のおそれがあると判断した場合には、速やかに失効申請を行わなければならない。

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

本 CA は、有効な失効申請を受け付けてから速やかに証明書の失効処理を行い、CRL へ当該証明書情報を反映させる。

4.9.6 失効調査の要求

本 CA が発行する証明書には、CRL の格納先であるURL を記載する。検証者は、証明書利用
者の証明書について信頼し、利用する前に、当該証明書の有効性をCRL により確認しなければならない。なお、CRL には、有効期限の切れた証明書情報は含まれない。

4.9.7 証明書失効リストの発行頻度

CRL は、失効処理の有無に関わらず、24 時間ごとに更新を行う。証明書の失効処理が行われた場合は、その時点でCRL の更新を行う。

4.9.8 証明書失効リストの発行最大遅延時間

本 CA は、発行したCRL を即時にリポジトリに反映させる。

4.9.9 オンラインでの失効/ステータス確認の適用性

オンラインでの証明書ステータス情報は、OCSPサーバを通じて提供される。

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

利用者は本CAにより発行された証明書を信頼し、利用する前に、証明書の有効性を確認しなければならない。リポジトリに掲載しているCRLにより、証明書の失効登録の有無を確認しない場合には、OCSPサーバにより提供される証明書ステータス情報の確認を行わなければならない。

4.9.11 利用可能な失効情報の他の形式

規定しない。

4.9.12 証明書の一時停止事由

規定しない。

4.9.13 証明書の一時停止を申請することができる者

規定しない。

4.9.14 証明書の一時停止申請手続

規定しない。

4.9.15 一時停止を継続することができる期間

規定しない。

4.10 証明書のステータス確認サービス

規定しない。

4.10.1 運用上の特徴

規定しない。

4.10.2 サービスの利用可能性

規定しない。

4.10.3 オプショナルな仕様

規定しない。

4.11 加入（登録）の終了

証明書利用者だけがアクセス可能なホームページ内で、継続した証明書の利用を意図した更新申請を行わない場合、本サービスへの登録が終了となる。

4.12. キーエスクローと鍵回復

4.11.1 キーエスクローと鍵回復ポリシー及び実施

本 CA は、証明書利用者の私有鍵のエスクローは行わない。

4.11.2 セッションキーのカプセル化と鍵回復のポリシー及び実施

規定しない。

5. 設備上、運営上、運用上の管理

5.1 物理的管理

5.1.1 立地場所及び構造

本項については、CPS に規定する。

5.1.2 物理的アクセス

本項については、CPS に規定する。

5.1.3 電源及び空調

本項については、CPS に規定する。

5.1.4 水害対策

本項については、CPS に規定する。

5.1.5 火災防止及び火災保護対策

本項については、CPS に規定する。

5.1.6 媒体保管

本項については、CPS に規定する。

5.1.7 廃棄処理

本項については、CPS に規定する。

5.1.8 オフサイトバックアップ

本項については、CPS に規定する。

5.2 手続的管理

5.2.1 信頼すべき役割

本項については、CPS に規定する。

5.2.2 職務ごとに必要とされる人数

本項については、CPS に規定する。

5.2.3 個々の役割に対する本人性確認と認証

本項については、CPS に規定する。

5.2.4 職務分割が必要となる役割

本項については、CPS に規定する。

5.3 人事的管理

5.3.1 資格、経験及び身分証明の要件

本項については、CPS に規定する。

5.3.2 背景調査

本項については、CPS に規定する。

5.3.3 教育要件

本項については、CPS に規定する。

5.3.4 再教育の頻度及び要件

本項については、CPS に規定する。

5.3.5 仕事のローテーションの頻度及び順序

本項については、CPS に規定する。

5.3.6 認められていない行動に対する制裁

本項については、CPS に規定する。

5.3.7 独立した契約者の要件

本項については、CPS に規定する。

5.3.8 要員へ提供される資料

本項については、CPS に規定する。

5.4 監査ログの手続

5.4.1 記録されるイベントの種類

本項については、CPS に規定する。

5.4.2 監査ログを処理する頻度

本項については、CPS に規定する。

5.4.3 監査ログを保持する期間

本項については、CPS に規定する。

5.4.4 監査ログの保護

本項については、CPS に規定する。

5.4.5 監査ログのバックアップ手続

本項については、CPS に規定する。

5.4.6 監査ログの収集システム

本項については、CPS に規定する。

5.4.7 イベントを起こした者への通知

本項については、CPS に規定する。

5.4.8 脆弱性評価

本項については、CPS に規定する。

5.4.9 監査ログのバックアップ手続

本項については、CPS に規定する。

5.5 記録の保管

5.5.1 アーカイブの種類

シーサイドネットは、CPS の「5.5. 記録の保管」に加えて、次の情報をアーカイブとして保存する。

- 本 CP
- 本 CP に基づき作成された認証局の業務運用を規定する文書

- **監査の実施結果に関する記録及び監査報告書**
- **証明書利用者からの申請データ等**

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

6.1.1 鍵ペアの生成

本 CA 秘密鍵についてはCPS「6.1.1 鍵ペアの生成」に規定する。
証明書利用者の鍵ペアは、シーサイドネットの管理するサーバ内で生成される。

6.1.2 加入者に対する私有鍵の交付

証明書利用者の私有鍵は、シーサイドネットの管理するサーバ内で生成し、本CA からの私有鍵の交付は行わない。

6.1.3 認証局への公開鍵の交付

本 CA に対する証明書利用者の公開鍵は、シーサイドネットの管理するサーバに配置することで交付とする。

6.1.4 信頼者への CA 公開鍵の交付

検証者は、本CA のリポジトリにアクセスすることによって、本CA の公開鍵を入手することができる。

6.1.5 鍵サイズ

本 CA の鍵ペアは、RSA 方式で鍵長2048 ビットとする。
証明書利用者の鍵ペアについては、RSA 方式で鍵長2048 ビットを推奨とする。

6.1.6 公開鍵のパラメータの生成及び品質検査

本 CA の公開鍵のパラメータの生成、及びパラメータの強度の検証は、鍵ペア生成に使用される暗号装置に実装された機能を用いて行われる。
証明書利用者の公開鍵のパラメータの生成及び品質検査について規定しない。

6.1.7 鍵の用途

本 CA の証明書のKeyUsage にはkeyCertSign,、cRLSign のビットを設定する。
本 CA が発行する証明書利用者の証明書のKeyUsage には、digitalSignature,
keyEncipherment
を設定する。

6.2 私有鍵の保護及び暗号モジュール技術の管理

6.2.1 暗号モジュールの標準及び管理

本項については、CPS に規定する。

6.2.2 私有鍵の複数人管理

本項については、CPS に規定する。

6.2.3 私有鍵のエスクロー

本項については、CPS に規定する。

6.2.4 私有鍵のバックアップ

本項については、CPS に規定する。

6.2.5 私有鍵のアーカイブ

本項については、CPS に規定する。

6.2.6 私有鍵の暗号モジュールへの又は暗号モジュールからの転送

本項については、CPS に規定する。

6.2.7 暗号モジュールへの私有鍵の格納

本項については、CPS に規定する。

6.2.8 私有鍵の活性化方法

本項については、CPS に規定する。

6.2.9 私有鍵の非活性化方法

本項については、CPS に規定する。

6.2.10 私有鍵の破棄方法

本項については、CPS に規定する。

6.2.11 暗号モジュールの評価

本項については、CPS に規定する。

6.3 鍵ペアのその他の管理方法

6.3.1 公開鍵のアーカイブ
本項については、CPS に規定する。

6.3.2 私有鍵及び公開鍵の有効期間
本項については、CPS に規定する。

6.4 活性化データ
本項については、CPS に規定する。

6.4.1 活性化データの生成及び設定
本項については、CPS に規定する。

6.4.2 活性化データの保護
本項については、CPS に規定する。

6.4.3 活性化データの他の考慮点
規定しない。

6.5 コンピュータのセキュリティ管理

6.5.1 コンピュータセキュリティに関する技術的要件
本項については、CPS に規定する。

6.5.2 コンピュータセキュリティ評価
本項については、CPS に規定する。

6.6 ライフサイクルセキュリティ管理
本項については、CPS に規定する。

6.6.1 システム開発管理
本項については、CPS に規定する。

6.6.2 セキュリティ運用管理
本項については、CPS に規定する。

6.6.3 ライフサイクルセキュリティ管理

本項については、CPS に規定する。

6.7 ネットワークセキュリティ管理

本項については、CPS に規定する。

6.8 タイムスタンプ

本項については、CPS に規定する。

7. 証明書及び証明書失効リストのプロファイル

7.1 証明書のプロファイル

本 CA が発行する証明書のプロファイルは、次表のとおりである。

表 7.1-1 証明書プロファイル(XiPS)

基本領域		設定内容	Critical
Version		Version 3	-
Serial Number		例) 0123456789	-
Signature Algorithm		SHA1 with RSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O=XiPS	-
	Common Name	CN=XiPS CA	-
Validity	NotBefore	例) 2006/2/1 00:00:00 GMT	-
	NotAfter	例) 2007/2/1 00:00:00 GMT	-
Subject	Country	C=JP(固定値)	-
	State Or Province	ST=XiPS(固定値)	-
	Locality	(任意)	-
	Organization	(任意)	-
	Organizational Unit	(任意)	-
	Common Name	サーバー名(必須)	-
Subject Public Key Info		主体者の公開鍵2048 ビット	-
拡張領域		**設定内容**	**Critical**
KeyUsage		digitalSignature, keyEncipherment	y
ExtendedKeyUsage		TLSWeb Server Authentication	n
NSCertType		SSL Server(サーバー認証)	n
Subject Alt Name		dNSName=サーバー名	n
CertificatePolicies		policyIdentifier OID=1.2.392.200091.110.171.1 policyQualifiers policyQualifierId=CPS qualifiier=https://repo1.secomtrust.net/sppca/xips/	n
CRL Distribution Points		http://repo1.secomtrust.net/sppca/xips/fullcrl.crl	n
Authority Key Identifier		発行者公開鍵のSHA-1 ハッシュ値(160 ビット)	n

Subject Key Identifier	主体者公開鍵のSHA-1 ハッシュ値(160 ビット)	n

表 7.1-2 証明書プロファイル(XiPS2)

基本領域		設定内容	Critical
Version		Version 3	-
Serial Number		例) 0123456789	-
Signature Algorithm		SHA256 with RSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O=XiPS	-
	Common Name	CN=XiPS CA2	-
Validity	NotBefore	例) 2015/2/1 00:00:00 GMT	-
	NotAfter	例) 2015/2/1 00:00:00 GMT	-
Subject	Country	C=JP(固定値)	-
	State Or Province	ST=XiPS(固定値)	-
	Locality	(任意)	-
	Organization	(任意)	-
	Organizational Unit	(任意)	-
	Common Name	サーバー名(必須)	-
Subject Public Key Info		主体者の公開鍵2048 ビット	-
拡張領域		**設定内容**	**Critical**
KeyUsage		digitalSignature, keyEncipherment	y
ExtendedKeyUsage		TLSWeb Server Authentication	n
Subject Alt Name		dNSName=サーバー名	n
CertificatePolicies		policyIdentifier OID=1.2.392.200091.110.171.2 policyQualifiers policyQualifierId=CPS qualifiier=https://repo1.secomtrust.net/sppca/xips2/	n
CRL Distribution Points		http://repo1.secomtrust.net/sppca/xips2/fullcrl.crl	n
Authority Key Identifier		発行者公開鍵のSHA-1 ハッシュ値(160 ビット)	n
Subject Key Identifier		主体者公開鍵のSHA-1 ハッシュ値(160 ビット)	n
Authority Infomation Access		accessMethod oscp(1 3 6 1 5 5 7 48 1)	n

	accessLocation http://xips2.ocsp.secomtrust.net	

7.2 CRL のプロファイル

本 CA が発行するCRL のプロファイルは、次表のとおりである。

表 7.2-1 CRL プロファイル(XiPS)

基本領域		設定内容	Critical
Version		Version 2	-
Signature Algorithm		SHA1 with RSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O=XiPS	-
	Common Name	CN=XiPS CA	-
This Update		例) 2006/2/1 00:00:00 GMT	-
Next Update		例) 2006/2/5 00:00:00 GMT 更新間隔=24H、有効期間=96H とする	-
Revoked Certificates	Serial Number	例) 0123456789	-
	Revocation Date	例) 2006/2/1 00:00:00 GMT	-
	Reason Code	失効事由(unspecifiled, etc.)	-
拡張領域		**設定内容**	**Critical**
CRL Number		CRL 番号	
Authority Key Identifier		発行者公開鍵のSHA-1 ハッシュ値 (160 ビット)	

表 7.2-2 CRL プロファイル(XiPS2)

基本領域		設定内容	Critical
Version		Version 2	-
Signature Algorithm		SHA256 with RSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O=XiPS	-
	Common Name	CN=XiPS CA2	-
This Update		例) 2015/2/1 00:00:00 GMT	-
Next Update		例) 2015/2/5 00:00:00 GMT 更新間隔=24H、有効期間=96H とす	-

		る	
Revoked Certificates	Serial Number	例) 0123456789	-
	Revocation Date	例) 2015/2/1 00:00:00 GMT	-
	Reason Code	失効事由(unspecifiled, etc.)	-
拡張領域		設定内容	Critical
CRL Number		CRL 番号	
Authority Key Identifier		発行者公開鍵のSHA-1 ハッシュ値（160 ビット）	

7.3 OCSP のプロファイル

本 CA が発行するOCSP のプロファイルは、次表のとおりである。

表 7.3-1 OCSP プロファイル(XiPS2)

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		例) 0123456789	-
Signature Algorithm		SHA256 with RSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O=XiPS	-
	Common Name	CN=XiPS CA2	-
Validity	NotBefore	例) 2015/2/1 00:00:00 GMT	-
	NotAfter	例) 2016/2/1 00:00:00 GMT	-
Subject	Country	C=JP	-
	Organization	O=XiPS	-
	Organizational Unit	-	
	Common Name	CN=XiPS CA2 OCSP Responder	-
Subject Public Key Info		主体者の公開鍵 2048 ビット	-
拡張領域		設定内容	critical
ExtendedKeyUsage		OCSPSigning	n
Subject Key Identifier		主体者公開鍵の SHA-1 ハッシュ値（160 ビット）	n
Authority Key Identifier		発行者公開鍵の SHA-1 ハッシュ値（160 ビット）	n
CertificatePolicies		policyIdentifier OID=1.2.392.200091.110.171.2 policyQualifiers policyQualifierId=CPS	n

	qualifiier= https://repo1.secomtrust.net/sppca/xips2/	
OCSP No Check	Null	n
KeyUsage	digitalSignature	y

8. 準拠性監査と他の評価

8.1 監査の頻度

シーサイドネットは、本CA の運用が本CP に準拠して行われているかについて、適時、監査を行う。

8.2 監査者の身元／資格

準拠性監査は、十分な監査経験を有する監査人が行う。

8.3 監査者と被監査者の関係

監査人は、監査に関する事項を除き、被監査部門の業務から独立した立場にあるものとする。監査の実施にあたり、被監査部門は監査に協力するものとする。

8.4 監査で扱われる事項

監査は、本CA の運用の本CP に対する準拠性を中心として行う。

8.5 不備の結果としてとられる処置

本 CA は、監査報告書で指摘された事項に関し、速やかに必要な是正措置を行う。

8.6 監査結果の開示

監査結果は、監査人から本CA に対して報告される。
本 CA は、法律に基づく開示要求があった場合、当社との契約に基づき関係組織からの開示要求があった場合、及びシーサイドネットポリシー委員会が承認した場合を除き、監査結果を外部へ開示することはない。

9. 他の業務上及び法的事項

9.1 料金

規定しない。

9.1.1 証明書の発行又は更新料

規定しない。

9.1.2 証明書へのアクセス料金

規定しない。

9.1.3 失効又はステータス情報へのアクセス料金

規定しない。

9.1.4 その他のサービスに対する料金

規定しない。

9.1.5 払い戻し指針

規定しない。

9.2 財務的責任

シーサイドネットは、電子認証基盤の運用維持にあたり、十分な財務的基盤を維持するものとする。

9.3 企業情報の機密性

9.3.1 機密情報の範囲

シーサイドネットが保持する個人情報及び組織情報は証明書、CRL、本CP 及びCPS の一部として明示的に公開されたものを除き、機密保持対象として扱う。

9.3.2 機密情報の範囲外の情報

証明書及びCRL に含まれている情報は機密保持対象外として扱う。その他、次の状況におかれた情報は機密保持対象外とする。

・ シーサイドネットの過失によらず知られた、あるいは知られるようになった情報
・ シーサイドネット以外の出所から、機密保持の制限無しにシーサイドネットに知られた、あるいは知られるようになった情報
・ シーサイドネットによって独自に開発された情報
・ 開示に関して証明書利用者によって承認されている情報

9.3.3 機密情報を保護する責任

シーサイドネットは、法の定めによる場合、機密情報を開示することがある。その際、その情報を知り得た者は、契約あるいは法的な制約によりその情報を第三者に開示させない。

9.4 個人情報の保護

シーサイドネットの個人情報保護方針については、シーサイドネットのホームページにて公表する。

9.5 知的財産権

本 CP は著作権を含み、シーサイドネットの権利に属するものとする。

9.6 表明保証

9.6.1 認証局の表明保証

本 CA は、認証業務を遂行するにあたり次の義務を負う。
・CA 私有鍵のセキュアな生成・管理
・RA からの申請に基づいた証明書の正確な発行・失効管理
・IA のシステム稼動の監視・運用
・CRL の発行・公表
・リポジトリの維持管理

9.6.2 登録局の表明保証

本 CA は、RA の業務を遂行するにあたり次の義務を負う。
・登録端末のセキュアな環境への設置・運用
・証明書発行・失効申請におけるIA への正確な情報伝達
・証明書失効申請におけるIA への運用時間中の速やかな情報伝達

9.6.3 証明書利用者の表明保証

証明書利用者は、本CP に定める諸事項を遵守することについて保証するものとする。また、

証明書利用者は、本CP に遵守しない場合、すべての責任を有するものとする。

9.6.4 信頼者の表明保証

検証者は、本CP に定める諸事項を遵守することについて保証するものとする。また、信頼者は、本CP に遵守しない場合、すべての責任を有するものとする。

9.6.5 他の関係者の表明保証

規定しない。

9.7 無保証

本 CA は、本CP「9.6.1 認証局の表明保証」に規定する保証に関連して発生するいかなる間接損害、特別損害、付随的損害又は派生的損害に対する責任を負わず、また、いかなる逸失利益、データの紛失又はその他の間接的若しくは派生的損害に対する責任を負わない。

9.8 責任の制限

本 CP「9.6.1 認証局の表明保証」の内容に関し、次の場合、本CA は責任を負わないものとする。

・本CA に起因しない不法行為、不正使用又は過失等により発生する一切の損害
・証明書利用者が自己の義務の履行を怠ったために生じた損害
・証明書利用者のシステムに起因して発生した一切の損害
・本CA、証明書利用者のハードウェア、ソフトウェアの瑕疵、不具合あるいはその他の動作自体によって生じた損害
・証明書利用者が契約に基づく契約料金を支払っていない間に生じた損害
・本CA 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
・本CA 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
・証明書の使用に関して発生する取引上の債務等、一切の損害
・現時点の予想を超えた、ハードウェア的あるいはソフトウェア的な暗号アルゴリズム解読技術の向上に起因する損害
・天変地異、地震、噴火、火災、津波、水災、落雷、戦争、動乱、テロリズムその他の不可抗力に起因する、本CA の業務停止に起因する一切の損害

9.9 補償

本 CA が発行する証明書を申請、受領、信頼した時点で、証明書利用者には、本CA 及び関

連する組織等に対する損害賠償責任及び保護責任が発生するものとする。当該責任の対象となる事象には、損失、損害、訴訟、あらゆる種類の費用負担の原因となるようなミス、怠慢な行為、各種行為、履行遅滞、不履行等の各種責任が含まれる。

9.10 有効期間と終了

9.10.1 有効期間

本 CP は、シーサイドネットポリシー委員会の承認により有効とする。

9.10.2 終了

本 CP は、本CA の終了と同時に無効とする。

9.10.3 終了の効果と効果継続

証明書利用者とシーサイドネットとの間で利用契約等を終了する場合、又は、本CA 自体を終了する場合であっても、その性質上存続されるべき条項は終了の事由を問わず証明書利用者及び本CA に適用されるものとする。

9.11 関係者間の個別通知と連絡

本 CA は、証明書利用者に対する必要な通知をホームページ上、電子メール又は書面等によって行う。

9.12 改訂

9.12.1 改訂手続

本 CP は、本CA の判断によって適宜改訂され、シーサイドネットポリシー委員会の承認によって発効する。

9.12.2 通知方法及び期間

本 CP を変更した場合、速やかに変更した本CP を公表することにより、証明書利用者に対しての告知とする。証明書利用者は告知日から一週間の間、異議を申し立てることができ、異議申し立てがない場合、変更された本CP は証明書利用者に同意されたものとみなす。

9.12.3 オブジェクト識別子が変更されなければならない場合

規定しない。

9.13 紛争解決手続

証明書の利用に関し、本CA に対して訴訟、仲裁を含む解決手段に訴えようとする場合、本CA に対して事前にその旨を通知するものとする。なお、仲裁及び裁判地は東京都内における紛争処理機関を専属的管轄とする。

9.14 準拠法

本 CA、証明書利用者の所在地にかかわらず、本CP の解釈、有効性及び証明書の利用にかかわる紛争については、日本国の法律が適用されるものとする。

9.15 適用法の遵守

規定しない。

9.16 雑則

規定しない。

9.17 その他の条項

規定しない。