AMANO RootCA for TA/TSA

TSA 用証明書ポリシ

Version 1.10

2010 年 10 月 1 日

アマノビジネスソリューションズ株式会社

改訂履歴

版	発行日	内容
1.00	2006/08/23	初版
1.10	2010/10/01	1. 会社・組織名称をアマノタイムビジネス株式会社からアマノビジネスソリューションズ株式会社に変更 2. 「1.5.2 連絡先」を変更

目次

1. はじめに ……7
1.1 概要 ……7
1.2 文書名と識別 ……7
1.3 PKI の関係者 ……7
1.3.1 CA ……7
1.3.2 RA ……7
1.3.3 加入者 ……8
1.3.4 利用者 ……8
1.4. 証明書の用途 ……8
1.5. ポリシ運用管理 ……8
1.5.1 CP を管理する組織 ……8
1.5.2 連絡先 ……8
1.5.3 CP のポリシの適合性を決定する者 ……8
1.5.4 CP の承認手続 ……8
1.6. 定義と頭字語 ……8
2. 公表とリポジトリの責任 ……9
2.1 リポジトリ ……9
2.2 CA に関する情報の公開 ……9
2.3 公表の頻度 ……9
2.4 公開情報へのアクセス制御 ……9
3. 識別と認証 ……10
3.1 名称 ……10
3.1.1 名称の形式 ……10
3.1.2 名称の意味の必要性 ……10
3.1.3 加入者の匿名性又は仮名性 ……10
3.1.4 名称形式の解釈規則 ……10
3.1.5 名称の一意性 ……10
3.1.6 商標の認識、認証および役割 ……10
3.2 初期の身元検証 ……10
3.2.1 秘密鍵の所有を証明する方法 ……10
3.2.2 加入者の識別と認証 ……10
3.2.3 個人の識別と認証 ……10
3.2.4 検証しない加入者情報 ……11
3.2.5 権限の正当性確認 ……11
3.2.6 相互運用性規準 ……11

3.3 鍵更新要求についての識別と認証……11
3.3.1 通常鍵更新時の識別と認証の要件 ……11
3.3.2 証明書失効後の鍵更新時の識別と認証の要件 ……11
3.4 失効要求についての識別と認証……11
4. 証明書のライフサイクル運用的要件 ……12
4.1 証明書申請……12
4.1.1 証明書申請者 ……12
4.1.2 登録手続と責任 ……12
4.2 証明書申請の手続……12
4.2.1 識別と認証の手続 ……12
4.2.2 証明書申請の承認又は却下 ……12
4.2.3 証明書申請の処理期限 ……12
4.3 証明書の発行……12
4.3.1 証明書発行時の CA の行為……12
4.3.2 加入者への証明書発行の通知方法 ……12
4.4 証明書の受領……12
4.4.1 証明書の受領確認手続 ……12
4.4.2 CA による証明書の公開 ……12
4.4.3 他の関係者に対する証明書発行の通知 ……13
4.5 鍵ペアと証明書の用途……13
4.5.1 加入者の秘密鍵および証明書の用途 ……13
4.5.2 利用者による加入者の公開鍵および証明書の用途 ……13
4.6 証明書の更新……13
4.7 鍵更新を伴う証明書更新……13
4.7.1 鍵更新を伴う証明書更新を行う状況 ……13
4.7.2 鍵更新を伴う証明書更新の申請者 ……13
4.7.3 鍵更新を伴う証明書更新の申請手続 ……13
4.7.4 加入者への新しい証明書の通知 ……13
4.7.5 鍵更新を伴い発行された証明書の受領確認手続 ……13
4.7.6 CA による証明書の公開 ……13
4.7.7 他の関係者に対する証明書発行の通知 ……14
4.8 証明書の変更……14
4.9 証明書の失効および一時停止……14
4.9.1 証明書の失効および一時停止を行う状況 ……14
4.9.2 証明書失効の申請者 ……14
4.9.3 証明書失効の申請手続 ……14

4.9.4 失効要求までの猶予期間 ……14
4.9.5 CA が失効申請の処理を完了するまでの時間 ……14
4.9.6 利用者が証明書の状態を確認する仕組み ……15
4.9.7 CRL の発行頻度 ……15
4.9.8 CRL がリポジトリで公開されるまでの最大遅延時間 ……15
4.9.9 オンラインでの状態確認 ……15
4.9.10 証明書の一時停止 ……15
4.10 証明書状態サービス ……15
4.10.1 証明書状態サービスの特徴 ……15
4.10.2 サービスの可用性 ……15
4.11 登録の終了 ……15
4.12 鍵預託とキーリカバリ ……15
5. 管理、運用、設備の制御 ……16
5.1 物理的セキュリティ制御 ……16
5.2 手続上の制御 ……16
5.3 個人のセキュリティ制御 ……16
5.4 監査記録の手順 ……16
5.5 記録の保管 ……16
5.6 鍵の更新 ……16
5.7 危殆化および災害からの復旧 ……16
5.8 CA 業務の終了 ……16
6. 技術的セキュリティ制御 ……17
6.1 鍵ペア生成とインストール ……17
6.2 秘密鍵防護と暗号モジュールのエンジニアリング制御 ……17
6.3 鍵ペア管理の他の局面 ……17
6.4 活性化データ ……17
6.5 コンピュータセキュリティ制御 ……17
6.6 ライフサイクルセキュリティ制御 ……17
6.7 ネットワークセキュリティ制御 ……17
7. 証明書および CRL のプロファイル ……18
7.1 証明書プロファイル ……18
7.1.1 バージョン番号 ……18
7.1.2 証明書拡張 ……18
7.1.3 アルゴリズムオブジェクト識別子 ……18
7.1.4 名称形式 ……18
7.1.5 名称制約 ……18

7.1.6 CP オブジェクト識別子 ……18
7.1.7 ポリシ制約拡張の用途 ……18
7.1.8 ポリシ修飾子の文法と意味 ……18
7.1.9 重要な CP 拡張に対する処理の意味 ……19
7.2 CRL プロファイル ……19
7.2.1 バージョン番号 ……19
7.2.2 CRL および CRL エントリ拡張 ……19
8. 準拠性監査や他の評価 ……20
8.1 監査または他の評価の頻度 ……20
8.2 監査者の身元および資格 ……20
8.3 監査者と監査対象者の関係 ……20
8.4 監査の対象 ……20
8.5 監査指摘事項への対応 ……20
8.6 監査結果の開示 ……20
9. 他の業務事項と法的事項 ……21
9.1 料金 ……21
9.2 財務上の責任 ……21
9.3 機密情報 ……21
9.3.1 機密情報の範囲 ……21
9.3.2 機密範囲外の情報 ……21
9.3.3 機密情報の保護責任 ……21
9.4 個人情報の保護 ……21
9.5 知的財産権 ……21
9.6 表明と保証 ……22
9.6.1 CA および RA の表明と保証 ……22
9.6.2 加入者の表明と保証 ……22
9.6.3 利用者の表明と保証 ……22
9.7 免責事項 ……22
9.8 責任の制限 ……22
9.9 損害補償 ……22
9.10 文書の有効期間と終了 ……22
9.11 関係者に対する通知と連絡 ……22
9.12 改訂 ……23
9.12.1 改訂手続 ……23
9.12.2 通知方法と期間 ……23
9.13 紛争解決手段 ……23

9.14 準拠法 ……23
9.15 適用される準拠法 ……23
9.16 雑則 ……23
9.16.1 完全合意条項 ……23
9.16.2 権利譲渡条項 ……23
9.16.3 分離条項 ……23
9.17 その他の規定 ……24
10. 用語解説 ……25
11. 付録 ……27
11.1 証明書のプロファイル ……27
11.2 CRL のプロファイル ……27

1. はじめに

1.1 概要

AMANO RootCA for TA/TSA　TSA 用証明書ポリシ（Certificate Policy：以下、「本 CP」と呼ぶ）は、アマノビジネスソリューションズ株式会社（AMANO Business Solutions：以下、「ABS」と呼ぶ）が運用する認証局である AMANO RootCA for TA/TSA（以下、「本 CA」と呼ぶ）がタイムスタンプ局（Time-Stamping Authority：以下、「TSA」と呼ぶ）に対して発行する電子証明書の利用用途・適用範囲・義務・責任等について規定した文書である。尚、本 CA の運用規定については、AMANO RootCA for TA/TSA 認証局運用規程（Certificate Practice Statement：以下、「当該 CPS」と呼ぶ）に規定する。

本 CP は、IETF(Internet Engineering Task Force)の PKIX(Public Key Infrastructure working group)が提唱する「インターネット X.509 PKI：証明書ポリシと認証実施フレームワーク（Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework）」（RFC3647）に従い記述されている。

1.2 文書名と識別

本 CP の正式名称は「AMANO RootCA for TA/TSA　TSA 用証明書ポリシ」である。

また、本 CP に関連するのオブジェクト識別子（OID）は、次の通りとする。

表 1.1 オブジェクト識別子（OID）

内容	OID
組織	
アマノビジネスソリューションズ株式会社	0.2.440.200217
本サービス	
AMANO RootCA for TA/TSA	0.2.440.200217.100.10
証明書ポリシ	
AMANO RootCA for TA/TSA　TSA 用証明書ポリシ	0.2.440.200217.100.10.201
運用規程	
AMANO RootCA for TA/TSA　認証局運用規程	0.2.440.200217.100.10.100

1.3 PKI の関係者

1.3.1 CA

CA（Certificate Authority：認証局）は、CA の秘密鍵を管理しており、証明書の発行、管理、失効、失効情報の開示及び保管等を行う機関である。また、本 CA は、ルート認証局を兼ねている。

1.3.2 RA

RA（Registration Authority：登録局）は、組織や団体における証明書申請者と申請内容の識別および認証を行い、証明書の発行、更新、失効等の要求を審査すると共に、それらの各

要求を CA に対して要求する機関である。

1.3.3 加入者

加入者とは、本 CA から証明書を発行され、証明書に記載された公開鍵と対応する秘密鍵を管理する者を示す。但し、ここでの加入者は、本 CA により証明書を発行された TSA を示す。

1.3.4 利用者

利用者とは､本 CA から証明書を発行された TSA によるタイムスタンプトークンを信頼し、利用する者を示す。

1.4. 証明書の用途

本 CP に従って発行される証明書は、TSA 用の証明書である。また、本証明書は、加入者である TSA が発行するタイムスタンプトークンに利用される。

1.5. ポリシ運用管理

1.5.1 CP を管理する組織

本 CP を管理する組織は、アマノビジネスソリューションズ株式会社である。

1.5.2 連絡先

組織名　　：アマノビジネスソリューションズ株式会社
住所　　：〒222-0011 神奈川県横浜市港北区菊名 7 丁目 3 番 24 号
E-MAIL フォーム ： http://www.e-timing.ne.jp/tsa/purchase/inquiry.html

1.5.3 CP のポリシの適合性を決定する者

本 CP のポリシの適合性は、本 CA のポリシ策定者が判断し、決定を下す。

1.5.4 CP の承認手続

本 CP は、本 CA のサービス責任者により承認手続が行われる。

1.6. 定義と頭字語

本 CP の 10 章に規定する。

2. 公表とリポジトリの責任

2.1 リポジトリ

当該 CPS に規定する。

2.2 CA に関する情報の公開

当該 CPS に規定する。

2.3 公表の頻度

当該 CPS に規定する。

2.4 公開情報へのアクセス制御

当該 CPS に規定する。

3. 識別と認証

3.1 名称

3.1.1 名称の形式

本 CA が発行する証明書における発行者名及び加入者名は、X.500 の識別名（DN: Distinguished Name）形式に従って設定する。

3.1.2 名称の意味の必要性

本 CA における加入者は、加入者の識別および認証を行う際に適した意味を名称に持たせる必要がある。

3.1.3 加入者の匿名性又は仮名性

本 CA は、加入者の匿名または仮名を、許可しない。

3.1.4 名称形式の解釈規則

本 CA が発行する証明書の識別名の形式は、X500 の識別名形式に従う。

3.1.5 名称の一意性

本 CA が発行する証明書に記載される加入者の識別名は、一意に割り当てる。

3.1.6 商標の認識、認証および役割

本 CA は、商標、商号、ドメイン名、サービスマークについて、認識、認証を行わない。

3.2 初期の身元検証

3.2.1 秘密鍵の所有を証明する方法

本 CA は、加入者からの PKCS#10 の証明書署名要求（Certificate Signing Request ：以下、「CSR」と呼ぶ）の署名検証を行うことで、加入者が CSR に含まれる公開鍵に対応した秘密鍵を所有していることを確認する。

3.2.2 加入者の識別と認証

本 CA は、本 CA が定める規程により、証明書発行時の申請書および CSR 等を基に、加入者の識別と認証を行う。

3.2.3 個人の識別と認証

本 CA は、個人への証明書発行を行わない。

3.2.4 検証しない加入者情報

本 CA は、3.2.2 節で述べた項目以外の加入者情報については、対象としない。

3.2.5 権限の正当性確認

本 CA は、申請者となる組織の責任者またはその代理人から提出される申請書等により、当該申請者が申請を行う権限の正当性を有していることを 3.2.2 節で述べた項目を基に確認する。

3.2.6 相互運用性規準

規定しない。

3.3 鍵更新要求についての識別と認証

3.3.1 通常鍵更新時の識別と認証の要件

本 CP の 3.2 節と同様の方法で行う。

3.3.2 証明書失効後の鍵更新時の識別と認証の要件

本 CP の 3.2 節と同様の方法で行う。

3.4 失効要求についての識別と認証

本 CA は、証明書失効に関する必要事項を記載した申請書を基に、申請者と失効要求の識別と認証を行う。

4. 証明書のライフサイクル運用的要件

4.1 証明書申請

4.1.1 証明書申請者

証明書申請は、申請を行う組織の責任者またはその代理人が行うことができる。

4.1.2 登録手続と責任

証明書申請者は、本 CP について承諾した上で、事前に周知された手続に従い申請を行うものとする。

4.2 証明書申請の手続

4.2.1 識別と認証の手続

本 CA は、3.2 節と同様の方法で、申請者の本人性と申請内容の真正性を確認する。

4.2.2 証明書申請の承認又は却下

本 CA は、申請者の本人性と申請内容の真正性の確認が取れ次第、申請を承認する。但し、申請者や申請内容に不備があった場合は、その申請を却下する。

4.2.3 証明書申請の処理期限

本 CA は、申請を承諾した場合、速やかに証明書を発行する。

4.3 証明書の発行

4.3.1 証明書発行時の CA の行為

本 CA は、承認された申請者の PKCS#10 の CSR に含まれる公開鍵に対して、本 CA の秘密鍵で署名を付与し、証明書を発行する。

4.3.2 加入者への証明書発行の通知方法

本 CA は、発行した証明書を外部記憶媒体に格納し、受領書と共に送付する。

4.4 証明書の受領

4.4.1 証明書の受領確認手続

申請者は、証明書を受領し、内容に誤りが無いことを確認次第、本 CA に対して受領証を送付しなければならない。証明書の内容に誤りがあった場合、申請者は、速やかに本 CA に対してその旨を通知しなければならない。

4.4.2 CA による証明書の公開

本 CA は、発行した証明書をリポジトリおいて公開する。

4.4.3 他の関係者に対する証明書発行の通知
本 CA は、他の関係者に対する証明書発行の通知を行わない。

4.5 鍵ペアと証明書の用途
4.5.1 加入者の秘密鍵および証明書の用途
加入者の秘密鍵および本 CA が発行する証明書は、本 CP および当該 CPS で規定されている用途に限り使用し、その他の用途に使用してはならない。

4.5.2 利用者による加入者の公開鍵および証明書の用途
利用者による加入者の公開鍵および証明書は、本 CP および当該 CPS で規定されている用途に限り使用し、その他の用途に使用してはならない。

4.6 証明書の更新
本 CA は、鍵更新を伴わない証明書更新を行わない。

4.7 鍵更新を伴う証明書更新
4.7.1 鍵更新を伴う証明書更新を行う状況
本 CA は、証明書の有効期間が満了する場合、鍵が危殆化等により証明書が失効した場合、および鍵の試用期間が満了する場合に、鍵更新を伴う証明書更新を行う。

4.7.2 鍵更新を伴う証明書更新の申請者
本 CP の 4.1.1 節と同様とする。

4.7.3 鍵更新を伴う証明書更新の申請手続
本 CP の 4.2 節と同様とする。

4.7.4 加入者への新しい証明書の通知
本 CP の 4.3.2 節と同様とする。

4.7.5 鍵更新を伴い発行された証明書の受領確認手続
本 CP の 4.4.1 節と同様とする。

4.7.6 CA による証明書の公開
本 CP の 4.4.2 節と同様とする。

4.7.7 他の関係者に対する証明書発行の通知
本 CP の 4.4.3 節と同様とする。

4.8 証明書の変更
本 CA は、証明書の内容を変更する場合、本 CP の 4.7 節と同様の手続で証明書を更新する。

4.9 証明書の失効および一時停止
4.9.1 証明書の失効および一時停止を行う状況
本 CA は、加入者からの失効申請があった場合、失効申請を受け付け、証明書の失効および一時停止を行う。
また、本 CA は、以下の状況において、加入者からの失効申請の有無に関わらず、証明書の失効および一時停止を行う。
・加入者の秘密鍵が危殆化した場合またはその可能性がある場合
・証明書の内容に誤りがあった場合
・加入者が本 CA の本 CP および当該 CPS に則っていなかった場合
・本 CA の秘密鍵が危殆化した場合またはその可能性がある場合
・本 CA がサービスを終了する場合
・本 CA が失効または一時停止を必要と判断した場合

4.9.2 証明書失効の申請者
証明書失効の申請は、申請を行う組織の責任者またはその代理人が行うことができる。

4.9.3 証明書失効の申請手続
証明書失効の申請手続は、証明書失効に関する必要事項を申請書に記載し、本 CA に対して、送付することで行われるものとする。

4.9.4 失効要求までの猶予期間
加入者は、危殆化および利用不能以外の理由で失効が必要な場合、5 営業日前までに失効申請を行わなければならない、また、危殆化および利用不能の場合、速やかに失効申請を行わなければならない。

4.9.5 CA が失効申請の処理を完了するまでの時間
本 CA は、申請者の本人性と申請内容の真正性の確認が取れてから、失効処理を 1 営業日以内に完了する。

4.9.6 利用者が証明書の状態を確認する仕組み

利用者は、リポジトリで公開されている CRL を確認し、証明書の失効の有無を確認しなければならない。

4.9.7 CRL の発行頻度

本 CA は、CRL の発行頻度を原則 1 年毎とする。但し、証明書の失効処理が発生した場合は、その都度 CRL を発行する。

4.9.8 CRL がリポジトリで公開されるまでの最大遅延時間

本 CA は、証明書の失効処理が完了した時点で、1 営業日以内に CRL をリポジトリで公開する。

4.9.9 オンラインでの状態確認

本 CA は、OCSP などオンラインで証明書の状態確認を行う仕組みを提供しない。

4.9.10 証明書の一時停止

本 CA は、証明書の一時停止を行わない。

4.10 証明書状態サービス

4.10.1 証明書状態サービスの特徴

本 CA は、CRL をリポジトリで公開することで、証明書の状態を確認できるようにする。

4.10.2 サービスの可用性

本 CA は、原則的に証明書状態サービスを常に利用可能とする。但し、運用保守等の理由でサービスを停止する場合は、事前にリポジトリにおいて告知する。また、緊急時等の場合は、事前通知を行わずに停止する可能性がある。

4.11 登録の終了

本 CA は、証明書の失効手続が完了した時点で、加入者が本 CA サービスの登録を終了したものとする。また、その際の手続は、本 CP の 4.9.3 節に定めた手続と同様とする。

4.12 鍵預託とキーリカバリ

本 CA は、鍵預託およびキーリカバリを行わない。

5. 管理、運用、設備の制御

5.1 物理的セキュリティ制御

当該 CPS に規定する。

5.2 手続上の制御

当該 CPS に規定する。

5.3 個人のセキュリティ制御

当該 CPS に規定する。

5.4 監査記録の手順

当該 CPS に規定する。

5.5 記録の保管

当該 CPS に規定する。

5.6 鍵の更新

当該 CPS に規定する。

5.7 危殆化および災害からの復旧

当該 CPS に規定する。

5.8 CA 業務の終了

当該 CPS に規定する。

6. 技術的セキュリティ制御

6.1 鍵ペア生成とインストール

当該 CPS に規定する。

6.2 秘密鍵防護と暗号モジュールのエンジニアリング制御

当該 CPS に規定する。

6.3 鍵ペア管理の他の局面

当該 CPS に規定する。

6.4 活性化データ

当該 CPS に規定する。

6.5 コンピュータセキュリティ制御

当該 CPS に規定する。

6.6 ライフサイクルセキュリティ制御

当該 CPS に規定する。

6.7 ネットワークセキュリティ制御

当該 CPS に規定する。

7. 証明書および CRL のプロファイル

7.1 証明書プロファイル

本 CA は、X.509 で規定されている証明書形式に則った証明書を発行する。
証明書のプロファイルは、本 CP の 11.1 節に記載する。

7.1.1 バージョン番号

本 CA が発行する X.509 証明書のバージョン番号は、Version3 である。

7.1.2 証明書拡張

本 CA が発行する証明書は、X.509(Version3)証明書の拡張領域の形式に則って、以下の拡張領域を設定・使用する。
証明書拡張領域の設定は、本 CP の 11.1 節に記載する。

7.1.3 アルゴリズムオブジェクト識別子

本 CA が発行する証明書に用いられるアルゴリズムオブジェクト識別子（OID）は、次の通りである。

表 7.1 アルゴリズムオブジェクト識別子（OID）

アルゴリズム	識別子（OID）
SHA1WithRSAEncryption	1.2.840.113549.1.1.5
rsaEncryption	1.2.840.113549.1.1.1

7.1.4 名称形式

本 CA が発行する証明書における発行者名及び加入者名は、X.500 の識別名（DN: Distinguished Name）形式に従って設定する。

7.1.5 名称制約

設定しない。

7.1.6 CP オブジェクト識別子

本 CP のオブジェクト識別子は、0.2.440.200217.100.10.201 である。

7.1.7 ポリシ制約拡張の用途

設定しない。

7.1.8 ポリシ修飾子の文法と意味

本 CA が発行する証明書のポリシ修飾子では、本 CP を公開しているリポジトリの URL を

設定する。

7.1.9 重要な CP 拡張に対する処理の意味
設定しない。

7.2 CRL プロファイル
本 CA は、X.509 で規定されている CRL 形式に則った CRL を発行する。
CRL のプロファイルは、本 CP の 11.2 節に記載する。

7.2.1 バージョン番号
本 CA が発行する X.509CRL のバージョン番号は、Version2 である。

7.2.2 CRL および CRL エントリ拡張
本 CA が発行する CRL は、拡張領域およびエントリ拡張領域を使用しない。

8. 準拠性監査や他の評価

8.1 監査または他の評価の頻度

当該 CPS に規定する。

8.2 監査者の身元および資格

当該 CPS に規定する。

8.3 監査者と監査対象者の関係

当該 CPS に規定する。

8.4 監査の対象

当該 CPS に規定する。

8.5 監査指摘事項への対応

当該 CPS に規定する。

8.6 監査結果の開示

当該 CPS に規定する。

9. 他の業務事項と法的事項

9.1 料金

規定しない。

9.2 財務上の責任

規定しない。

9.3 機密情報

9.3.1 機密情報の範囲

本 CA は、その情報が漏えいすることによって本 CA および加入者の信頼性、適格性が損なわれる恐れのある情報を機密情報とする。本 CA により機密情報と見なされた情報は、本 CA により安全に保管管理される。また、本 CA により機密情報と見なされた情報は、本 CP および当該 CPS に定められている場合を除いて、如何なる者にも原則的に開示しない。

9.3.2 機密範囲外の情報

次に定める情報については、9.3.2 節の規定に関わらず、機密情報と見なさない。

・本 CP 等公開情報として明示する情報
・本 CA の責任の範囲外で公知となった情報
・合法的に入手し、かつ加入者、利用者または第三者から機密保持の義務を負っていない情報
・本 CA または加入者が第三者に対し機密保持の義務を課す事無く開示した情報
・所有者を識別出来ないようにした統計目的で編集した情報

9.3.3 機密情報の保護責任

本 CA は、法的根拠に基づく情報開示の要求があった場合、または情報開示に対して加入者の承認を得た場合に、法で定められた範囲内で当該情報を開示する。

9.4 個人情報の保護

本 CA は、加入者の個人情報を、本 CP の 9.3 節と同様に扱う。

9.5 知的財産権

以下の情報についての知的財産権は、ABS に帰属するものとする。

・本 CP、当該 CPS およびその他公開情報
・本 CA の秘密鍵および公開鍵
・本 CA が発行した証明書および CRL

9.6 表明と保証

9.6.1 CA および RA の表明と保証

本 CA および RA は、本 CP および当該 CPS の規定を遵守し、本サービス提供する。

9.6.2 加入者の表明と保証

加入者は、以下の事項について義務を負う。

・加入者は、本 CA が発行した証明書を、本 CP および当該 CPS に従って、利用すること。

・加入者は、自身の秘密鍵を保護すること。

・加入者は、自身の秘密鍵が危殆化した際は、速やかに失効申請を行うこと。

・加入者は、本 CA に対して申請を行う際に、正確な内容で申請すること。

9.6.3 利用者の表明と保証

利用者は、以下の項目について義務を負う。

・利用者は、本 CA が発行した証明書を、本 CP および当該 CPS に従って、利用すること。

・利用者は、本 CA から発行された証明書の有効性を確認すること。

9.7 免責事項

ABS は、本 CP の 9.6.1 節に規定する保証に関連して生じたあらゆる損失、損害または費用については責任を負わない。

9.8 責任の制限

本 CA は、加入者および利用者が被る損害については、一切責任を負わない。

9.9 損害補償

規定しない。

9.10 文書の有効期間と終了

規定しない。

9.11 関係者に対する通知と連絡

本 CA は、加入者に対する個別の通知が必要となった場合、加入者の申請責任者に対して書面もしくは電子メールで通知を行うものとする。また、本 CA は、利用者に対する通知が必要となった場合、リポジトリで告知することで通知を行ったものとする。

9.12 改訂

9.12.1 改訂手続

本 CP は、本 CA のポリシ策定者により改定手続が行われる。

9.12.2 通知方法と期間

本 CP は、リポジトリで公開することで通知を行ったものとする。また、改訂された CP が公開されてから 1 週間の間に異議申し立てが無い場合、加入者および利用者は、当該 CP の改訂を承諾したものとする。

9.13 紛争解決手段

本サービスに関する一切の訴訟については、東京地方裁判所を、第一審の専属的合意管轄裁判所とする。

9.14 準拠法

本 CP の適用、構成、解釈、有効性等は、日本法に従って判断される。また、本サービスに関わる関係者間の紛争が生じた場合には、日本法を準拠法とする。但し、本準拠法は、利用者が使用するソフトウェア、ハードウェアおよび技術情報の輸出入を制限するものではない。

9.15 適用される準拠法

本 CP は、日本法に準拠するが、ソフトウェア、ハードウェアおよび技術情報の輸出入を制限するものではなく、利用者の責任において適切な関連法を遵守する必要がある。

9.16 雑則

9.16.1 完全合意条項

ABS は、本サービスにおけるポリシ、運用規定およびサービス利用規定を本 CP および当該 CPS に定め、それ以外の書面や口頭による合意は効力をなさないものとする。

9.16.2 権利譲渡条項

規定しない。

9.16.3 分離条項

本 CP および当該 CPS の一部の条項が、何らかの理由で、無効または執行できない場合、当該文書に規定されている他の条項は有効であるものとする。

9.17 その他の規定

規定しない。

10. 用語解説

本 CP で使用されている用語についての解説を以下の表に示す。

用語	解説
A-Z	
CRL	Certificate Revocation List：証明書失効リスト。 失効した証明書のリスト。
IETF	Internet Engineering Task Force. インターネットで利用される技術仕様を標準化する任意団体。
PKI	Public Key Infrastructure：公開鍵基盤。 公開鍵暗号技術を利用して構築されたセキュリティ基盤。
PKIX	Public Key Infrastructure working group. X.509 の規定に従い、PKI を実現するための技術仕様の標準化を行う IETF のワーキンググループの１つ。
RFC	Request For Comment. IETF が発行する技術仕様書。
RFC3647	PKI における関係者のために証明書ポリシもしくは認証実施フレームワークを書く人を支援するためのフレームワーク。
TSA	Time-Stamping Authority：タイムスタンプ局。 タイムスタンプサービス（タイムスタンプトークンを発行するサービス）を行う機関。
X.500	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-T （International Telecommunication Union-Telecommunication Standardization Sector：国際電気通信連合 電気通信標準化部門）が規定したディレクトリサービスの国際標準。
X.509	ITU-T により規定された PKI における証明書と CRL のフォーマット仕様書。
あ-ん	
オブジェクト識別子	Object Identification (OID). 登録機関（ISO, ITU）に登録された世界で一意となる値による識別子。
鍵ペア	公開鍵暗号方式における一組の秘密鍵と公開鍵。
危殆化	秘密鍵の漏洩や紛失、暗号アルゴリズムの脆弱化などにより、暗号に基づいた安全性が失われた状態。
公開鍵	公開鍵暗号方式における鍵ペアの一方で、秘密鍵により暗号化されたデータを復号するための公開されている鍵。
証明書	公開鍵暗号方式における公開鍵の所有者を証明する情報。CA が当該公開鍵に対して署名を付与することで、証明書の真正性が保証される。
証明書署名要求	Certificate Signing Request (CSR). 証明書を発行する際に加入者が CA に対して送付するデータ。CSR には加入者の公開鍵が含まれている。
証明書ポリシ	CA が発行する証明書のポリシを規定した文書。
署名	公開鍵暗号方式によって、秘密鍵所有者の本人性を証明することができるデータ。
署名検証	公開鍵暗号方式によって、署名の本人性を確認する行為。

タイムスタンプ	信頼の置ける時刻と文書などのデジタル情報に対し、変更、改ざんがあったかどうかを検知できる情報もしくはそれを指し示す情報を付与し、それ以降、内容や時刻に変更・改ざんがあったかどうかを証明する技術。
タイムスタンプトークン	信頼の置ける時刻と文書などのデジタル情報に対し、変更、改ざんがあったかどうかを検知できる情報。もしくはそれを指し示す情報。デジタル情報のハッシュデータに時刻情報等を付与し、電子署名として発行する。
認証局運用規定	CA の認証サービスにおける一連の運用規定書。
秘密鍵	公開鍵暗号方式における鍵ペアの一方で、データに対して署名を付与する際に用いる所有者が秘匿しておく鍵。
リポジトリ	CA の証明書、CP/CPS、CRL などのデータを格納する場所。
ルート認証局	ツリー構造の最上位にある認証局であり、下位の認証サービスを行う機関に対し証明書を発行する機関。

11. 付録

11.1 証明書のプロファイル

領域名	説明	設定値
version （バージョン）	X.509証明書のバージョン	3
serialNumber （シリアル番号）	証明書を一意に識別するための番号	*
signature （アルゴリズム識別子）	発行者が証明書に署名する際に用いるアルゴリズム	1.2.840.113549.1.1.5（SHA1WithRSAEncryption）
issuer （発行者）	証明書を発行した機関（CA）の名前	C=JP, O=AMANO Time Business Corporation, OU=AMANO RootCA for TA/TSA
validity （有効期間）	証明書の有効期間	
notBefore （開始時刻）	証明書が有効になる時刻	YYMMDDHHMMSSZ
notAfter （終了時刻）	証明書が無効になる時刻	YYMMDDHHMMSSZ
subject （主体者）	証明書所有者の名前	C=JP, ST=Kanagawa, L=Yokohama, O=AMANO Time Business Corporation, OU=e-timing Free TSA, OU=nCipher DSE ESN:****-****-****, CN=dse200-F***
subjectPublicKeyInfo （主体者公開鍵情報）	証明書所有者の公開鍵に関する情報	
algorithm （アルゴリズム）	公開鍵のアルゴリズム名	1.2.840.113549.1.1.1（rsaEncryption）
subjectPublicKey （主体者公開鍵）	証明書所有者の公開鍵	*
extensions （拡張領域）	証明書の拡張領域	

extensions（拡張領域）			
領域名	説明	Critical	設定値
subjectKeyIdentifier （主体者鍵識別子）	証明書所有者の公開鍵の特定に用いるハッシュ値	FALSE	*
authorityKeyIdentifier （機関鍵識別子）	CAの公開鍵の特定に用いるハッシュ値	FALSE	*
keyUsage （鍵使用目的）	公開鍵の使用目的	FALSE	digitalSignature, nonRepudiation
extendedKeyUsage （拡張鍵使用目的）	公開鍵の詳細な使用目的	TRUE	1.3.6.1.5.5.7.3.8 = PKIX-IDKP-TimeStamp
cRLDistributionPoints （CRL配布点）	CRLを入手するための情報	FALSE	http://www.e-timing.ne.jp/repository/ca4tatsa/AmanoCA4TATSACRL.crl
certificatePolicies （証明書ポリシー）	証明書ポリシーに関する情報	FALSE	policyID = 0.2.440.200217.100.10.201 qualifierID = pkix-id-qt CPSurl qualifier = https://www.e-timing.ne.jp/repository/ca/ca4tatsa_repository.html

11.2 CRL のプロファイル

領域名	説明	設定値
version （バージョン）	CRLのバージョン	3
signature （アルゴリズム識別子）	CRL発行者の署名アルゴリズム	1.2.840.113549.1.1.5（SHA1WithRSAEncryption）
issuer （発行者）	CRL発行者の名前	C=JP, O=AMANO Time Business Corporation, OU=AMANO RootCA for TA/TSA
thisUpdate （今回更新日時）	CRLの更新日時	YYMMDDHHMMSSZ
nextUpdate （次回更新日時）	次回のCRLの更新日時	YYMMDDHHMMSSZ
revokedCertificates （失効証明書のリスト）	失効された証明書の一覧	
crlExtensions （CRL拡張）	CRLの拡張領域	