AMANO RootCA for TA/TSA

認証局運用規程

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

1.1 概要

AMANO RootCA for TA/TSA 認証局運用規程（Certification Practice Statement：以下、「本 CPS」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）が行う電子証明書（以下、「証明書」と呼ぶ）の発行、失効、およびその他の本 CA の運用管理についての手続やポリシを規定した文書である。尚、本 CA によって発行される証明書のポリシは、証明書ポリシ（Certificate Policy：以下、「当該 CP」と呼ぶ）に規定する。

本 CPS 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 CPS の正式名称は「AMANO RootCA for TA/TSA 認証運用規程」である。

また、本 CPS 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
運用規程		
	AMANO RootCA for TA/TSA　認証局運用規程	0.2.440.200217.100.10.100
証明書ポリシ		
	AMANO RootCA for TA/TSA　TA 用証明書ポリシ	0.2.440.200217.100.10.200
	AMANO RootCA for TA/TSA　TSA 用証明書ポリシ	0.2.440.200217.100.10.201

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 および TA を示す。

1.3.4 利用者

利用者とは、本 CA から発行された証明書を信頼し、利用する者を示す。

1.4. 証明書の用途

本 CA は、本 CPS の 1.2 節に記載した各 CP に従った証明書を発行する。

1.5. ポリシ運用管理

1.5.1 CPS を管理する組織

本 CPS 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 CPS のポリシの適合性を決定する者

本 CPS 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 CPS の承認手続

本 CPS 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 CPS 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

本 CA のリポジトリは、下記 URL において公表する。

URL: https://www.e-timing.ne.jp/repository/ca/ca4tatsa_repository.html

2.2 CA に関する情報の公開

本 CA は、リポジトリにおいて以下の情報を公開する。

・本 CPS
・当該 CP
・CRL
・本 CA 証明書
・本 CA 証明書のハッシュ値

2.3 公表の頻度

本 CPS の 2.2 節に記載した情報は、発行の都度、リポジトリに公表される。

2.4 公開情報へのアクセス制御

リポジトリで開示する公開情報に関しては、アクセス制御を行わない。

3. 識別と認証

3.1 名称

当該 CP に規定する。

3.2 初期の身元検証

当該 CP に規定する。

3.3 鍵更新要求についての識別と認証

当該 CP に規定する。

3.4 失効要求についての識別と認証

当該 CP に規定する。

4. 証明書のライフサイクル運用的要件

4.1 証明書申請

当該 CP に規定する。

4.2 証明書申請の手続

当該 CP に規定する。

4.3 証明書の発行

当該 CP に規定する。

4.4 証明書の受領

当該 CP に規定する。

4.5 鍵ペアと証明書の用途

当該 CP に規定する。

4.6 証明書の更新

当該 CP に規定する。

4.7 鍵更新を伴う証明書更新

当該 CP に規定する。

4.8 証明書の変更

当該 CP に規定する。

4.9 証明書の失効および一時停止

当該 CP に規定する。

4.10 証明書状態サービス

当該 CP に規定する。

4.11 登録の終了

当該 CP に規定する。

4.12 鍵預託とキーリカバリ

当該 CP に規定する。

5. 管理、運用、設備の制御

5.1 物理的セキュリティ制御

5.1.1 施設の場所と構造

本 CA の設備は、火災などの災害対策設計された施設内の施錠された区画内に設置する。

5.1.2 物理的アクセス

本 CA の設備が設置されている区画は、入退室管理が行われており、入室する際は事前に登録が必要である。また、入室時に本人認証が行われるため、入室権限の無い者は、入室することができない。

5.1.3 電源および空調設備

本 CA の設備が設置されている場所は、十分な電源を確保している。また、空調設備により、設備に最適な温度が保たれている。

5.1.4 火災防止および対策

本 CA の設備が設置されている場所は、火災報知器により火災対策が施されている。

5.1.5 媒体保管

システムやデータをバックアップした記憶媒体は、セキュリティと空調が管理された場所に保管する。

5.1.6 廃棄物処理

機密扱いと見なす情報を含む書類、記憶媒体の廃棄は、厳密な分類の後、適切に処理する。特に情報の格納に使用した媒体は、破壊してから廃棄する。

5.1.7 オフサイトバックアップ

本 CA は、オフサイトバックアップを行わない。

5.2 手続上の制御

5.2.1 信頼される役割

本サービス責任者より承認された各オペレータのシステムへのアクセスは、その業務遂行上、実行しなければならない行為に限定される。

表 5.1 役割と職務内容

役割名	職務内容
サービス責任者	・本サービスの運用組織統括 ・本サービスのシステム運用および手続類の承認

ポリシ策定者	・本 CPS および CP の策定 ・監査指摘事項に関する対応指示
システム運用管理者	・システム運用の統括管理 ・運用担当者への作業指示および作業立会い ・その他全般の管理
運用担当者	・CA の秘密鍵管理 ・証明書の発行および管理 ・証明書の失効および CRL の開示 ・証明書申請の受付 ・申請者および申請内容の審査

5.2.2 必要な人数

本サービスにおける重要な作業は、物理的および役割的な権限を持つ複数人で行う。

5.2.3 役割に対する本人性確認と認証

システム運用管理者および各オペレータは、本サービス責任者により事前に識別・承認され、各役割に応じたアクセス権限が発行される。また本 CA は、本 CA の施設への入室およびシステムへのログインの際には、各役割に対する本人性の確認と認証を行う。

5.2.4 役割に関する職務分轄

本サービス責任者、ポリシ策定者およびシステム運用管理者は、それぞれの役割を兼務する事はできない。

5.3 個人のセキュリティ制御

5.3.1 資格、経験および身分証明

本 CA の職務に関わる者は、ABS の正社員とし、その者の適性を評価した上で任命される。

5.3.2 経歴調査と身分証明手続

本 CA の職務に関わる者の適性は、任命時および定期的に調査・評価される。

5.3.3 トレーニングの要件と手順

本 CA の職務に関わる者は、任命時に職務に必要な教育を受け、その後必要に応じて再度教育を受ける。

5.3.4 ジョブローテーションの頻度と手順

本 CA は、必要に応じてジョブローテーションを行う。

5.3.5 不正行為の罰則

本 CA の職務において不正行為を行った者は、社内規定および契約に応じて処分される。

5.4 監査記録の手順

5.4.1 記録されるイベントの種類

本 CA は、以下のイベントの実行記録を実行者の情報と共に記録する。

・CP/CPS の更新
・リポジトリの更新
・証明書の発行および失効
・業務担当者の変更

5.4.2 監査記録の処理又は保管の頻度

本 CA は、5.4.1 節に記載したイベントが起こる度に、監査記録を取得し、保管する。

5.4.3 監査記録の保管期間

監査記録の保管期間は、10 年とする。

5.4.4 監査記録の保護

監査記録は、アクセス制御が施され、許可された者以外は、閲覧することができない。

5.4.5 監査記録のバックアップ

監査記録は、バックアップされ、安全な場所に保管される。

5.5 記録の保管

5.5.1 記録の種類

本 CA は、以下の情報を記録する。

・証明書ライフサイクル運用に関する処理履歴
・本システムへのアクセス履歴
・本システムへのリクエスト履歴
・本 CA の自己証明書
・加入者の証明書
・CRL
・本 CPS および当該 CP

5.5.2 記録の保存期間

記録の保存期間は、10 年とする。

5.5.3 記録の保護

記録は、アクセス制御が施され、許可された者以外は、閲覧することができない。

5.5.4 記録のバックアップ手順

記録のバックアップは、定期的になされ、重要な記録のバックアップについては、記録が更新される都度行われる。

5.5.5 記録の収集および検証

記録は、定期的に保管状況を確認する。

5.6 鍵の更新

本 CA の秘密鍵は、有効期間が満了した時点で鍵の更新が行われる。

5.7 危殆化および災害からの復旧

5.7.1 事故および危殆化に対する手続

本 CA は、災害および本 CA の秘密鍵の危殆化により、本サービスを停止する必要が生じた際は、加入者および利用者に対して速やかに通知を行い、サービスの復旧作業を行う。

5.7.2 ハードウェア、ソフトウェア又はデータが破損した場合の手続

本 CA は、ハードウェア、ソフトウェア又はデータが破損した場合、速やかに復旧作業を行う。

5.7.3 加入者の秘密鍵が危殆化した場合の手続

加入者は、加入者の秘密鍵が危殆化した場合又は危殆化する可能性が生じた場合、本 CA に対して速やかに失効申請を行わなければならない。

5.7.4 災害後の事業持続性

本 CA は、災害後によりサービスが停止した場合、リポジトリにおける公開業務を速やかに復旧することを目標とする。また、その他の業務については、リポジトリにおける公開業務の復旧後、随時行うこととする。

5.8 CA 業務の終了

本 CA は、本サービスを終了する際に、加入者および利用者に対して事前に通知を行い。また、サービス終了時には、発行した全ての証明書を失効する。

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

6.1.1 鍵ペア生成

本 CA は、システム運用管理者を含む職務権限を持つ複数人によって、鍵管理モジュール内において鍵ペア生成を行う。

6.1.2 加入者への秘密鍵配布

加入者の秘密鍵は、加入者自身で生成されるため、本 CA は加入者への秘密鍵配布を行わない。

6.1.3 CA への公開鍵配布

加入者の公開鍵は、PKCS#10 の証明書署名要求（CSR）を用いて、本 CA へ配布される。

6.1.4 CA の公開鍵配布

本 CA の公開鍵は、リポジトリにおいて公開される。

6.1.5 鍵長

本 CA は、RSA2048bit の鍵ペアを使用する。

6.1.6 鍵の用途

本 CA の秘密鍵用途は、加入者の公開鍵証明書および CRL への署名に限る。

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

6.2.1 暗号モジュールの基準

本 CA の秘密鍵は、物理的セキュリティ制御およびソフトウェアによるログイン制御で保護されているモジュールで管理される。

6.2.2 秘密鍵の複数人管理

本 CA は、生成から廃棄に至るまでの秘密鍵の管理を、システム運用管理者を含む職務権限を持つ複数人によって行う。

6.2.3 秘密鍵の預託

本 CA の秘密鍵は、預託されない。

6.2.4 秘密鍵のバックアップ

本 CA は、サービス運用管理者を含む職務権限を持つ複数人による管理の下、安全な方法に

より秘密鍵のバックアップを行う。また、バックアップされた秘密鍵の管理は、本 CPS の 6.2.2 節に記載した内容と同様の方法で管理する。

6.2.5 秘密鍵のアーカイブ
本 CA の秘密鍵は、アーカイブされない。

6.2.6 暗号モジュールへの保管
本 CA の秘密鍵は、物理的セキュリティ制御およびログイン制御されているモジュールで保管される。

6.2.7 秘密鍵の活性化
本 CA の秘密鍵は、システム運用管理者を含む職務権限を持つ複数人によって、活性化される。

6.2.8 秘密鍵の非活性化
本 CA の秘密鍵は、システム運用管理者を含む職務権限を持つ複数人によって、非活性化される。

6.2.9 秘密鍵の破棄
本 CA の秘密鍵は、システム運用管理者を含む職務権限を持つ複数人によって、破棄される。また、バックアップされた秘密鍵も、同様の方法で破棄される。

6.3 鍵ペア管理の他の局面
6.3.1 公開鍵のアーカイブ
本 CA の公開鍵は、本 CPS の 5.5 節に記載した内容にそって、アーカイブされる。

6.3.2 鍵ペアの有効期間
本 CA の鍵ペアの有効期間は、20 年とする。

6.4 活性化データ
6.4.1 活性化データの生成とインストール
本 CA の秘密鍵の活性化データは、システム運用管理者を含む職務権限を持つ複数人によって、生成およびインストールされる。

6.4.2 活性化データの保護
本 CA の秘密鍵は、システム運用管理者を含む職務権限を持つ複数人による管理の下で、物

理的セキュリティ制御およびソフトウェアによるログイン制御で保護される。

6.5 コンピュータセキュリティ制御

本 CA の装置やソフトウェアは、本 CPS の 5.1 節、5.2 節および 5.3 節に記載した、
本 CA の装置やソフトウェアは、入退室時およびシステムへのログイン・ログアウト時のユーザ認証により、コンピュータへのセキュリティ制御が行われている。

6.6 ライフサイクルセキュリティ制御

本 CA で使用される装置やソフトウェアは、導入時にセキュリティの確認調査を行い、定期的に脆弱性の確認および対応を行う。

6.7 ネットワークセキュリティ制御

本 CA のシステムは、社内および社外との接続を行わない。

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

当該 CP に規定する。

7.2 CRL プロファイル

当該 CP に規定する。

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

本 CA は、CP および CPS の準拠性に関して、年に 1 回以上、監査または他の評価を行う。

8.2 監査者の身元および資格

本 CA の監査者は、本 CA の準拠性監査および PKI についての十分な知識を有する者とする。

8.3 監査者と監査対象者の関係

監査者は、監査対象である本 CA のシステム運用部門に属さない者とする。

8.4 監査の対象

監査は、本 CA のシステム運用に関わる業務を対象とする。

8.5 監査指摘事項への対応

監査指摘事項は、本 CA のサービス責任者により評価・判断され、必要に応じて対応する。

8.6 監査結果の開示

本 CA の監査結果は、原則的に開示されない。但し、サービス責任者が公表することを妥当と判断した場合、および、法律に基づく開示要求があった場合には、監査結果が開示される。

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 CPS および当該 CP 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 CPS 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 CPS 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 CPS、当該 CP 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 CPS および当該 CP の規定を遵守し、本サービスを提供する。

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 CPS および当該 CP 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 CPS および当該 CP 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 CPS 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 CPS 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 CPS 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 CPS 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 CPS 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 CPS 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 CPS 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程を本 CPS および当該 CP 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 CPS および当該 CP 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 CPS 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。

表 10.1 用語解説

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。