iTrust リモート署名サービス
運用規程
(iTrust RS Practice Statement)

Version 1.20

サイバートラスト株式会社

2023 年 2 月 17 日

■iTrust リモート署名サービス　運用規程の著作権と配布条件

Version 1.20
制定日：2023 年 2 月 17 日

改訂履歴

Version	日付	改訂事由
0.9	2018 年 12 月 1 日	・ ドラフト版作成
0.91	2019 年 1 月 18 日	・ 「6.6.3 利用システムの表明保証」に追記 ・ 「3.6.4 災害時等の事業継続性」の記載変更 ・ 「6.4.5 個人情報の使用に関する個人への通知および同意」の記載変更
1.1	2022 年 1 月 17 日	・ 「4.1 暗号鍵の生成」「4.2 秘密鍵の保護および暗号モジュール技術の管理」の記載変更 ・ 「5 準拠性監査およびその他の評価」の記載変更
1.2	2023 年 2 月 17 日	・ 「1.2 概要」の記載変更

目次

1. 概説

1.1 はじめに

本文書「iTrustリモート署名サービス運用規程」（iTrust RS Practice Statements 以下、「本 iRSPS」という）は、サイバートラスト株式会社（以下、「サイバートラスト」という）が運営する iTrustリモート署名サービス（以下、「本サービス」という）のリモート署名業務における運用管理に関する諸手続き、およびサービスを構成する要素である認証局ならびに、利用システムの運営組織の義務及び責任等について規定する。

1.2 概要

iTrust リモート署名サービスは、書面の電子化や電子契約で求められる電子文書の長期間に渡る真正性を確保する長期署名に対応したクラウドサービスです。本サービスは、サイバートラストが提供する認証局のアウトソーシングサービスである「サイバートラスト マネージド PKI」により構築された認証局から発行された利用者の電子証明書と秘密鍵、または「iTrust 電子署名用証明書」から発行された利用者の電子証明書と秘密鍵を本サービスの HSM に格納し、その HSM 内の秘密鍵を利用し電子データ（PDF）に対してリモートで電子署名（ES 形式、ES_T 形式）、及びタイムスタンプ（ES_A 形式）を付与する。電子署名（ES 形式、ES_T 形式）、及びタイムスタンプ（ES_A 形式）を付与した後の電子データ（PDF）は、最大 8 時間で削除する。本サービスの機能は REST API 形式で提供され、事前に本サービスを契約した組織に対して RS-API 接続用証明書を提供し、その証明書を利用し利用システムが TLS 暗号化通信によって REST API で接続し、API を実行する。

付与するタイムスタンプは、（一般）日本データ通信協会の「タイムビジネス信頼・安心認定制度」の認定を受けたサービスから日本標準時を本サービスが取得する。

1.3 用語解説

- 認証局（CA：Certification Authority）
  本サービスと連携し、電子証明書を発行する認証機関。

- 時刻認証局（TA：Time Authority）
  原子時計による高精度のマスタークロックの時刻源を内部に維持し、タイムスタンプ局に対して UTC（Coordinated Universal Time：協定世界時）に基づく正確な時刻情報を配信し、かつ当該タイムスタンプ局における時刻情報の運用状況を監査する、信頼できる第三者機関。時刻認証局の内部の情報センターからタイムスタンプ局のタイムスタンプサーバ（タイムスタンプ用内部時計）に対し、PKI による相互認証を行った上、時刻同期をとるサービスを提供する。

- タイムスタンプ局（TSA：Time Stamp Authority）
  タイムスタンプの発行要求に対し、時刻認証局から定期的に配信され、かつ監査された時刻情報を基に、タイムスタンプトークンを作成し発行する機関。

- サイバートラスト マネージド PKI（MPKI）
  本サービスと連携するプライベートの認証局をクラウド型で構築するサービスです。本書の認証局は、このサービスで構築された認証局と連携可能となります。

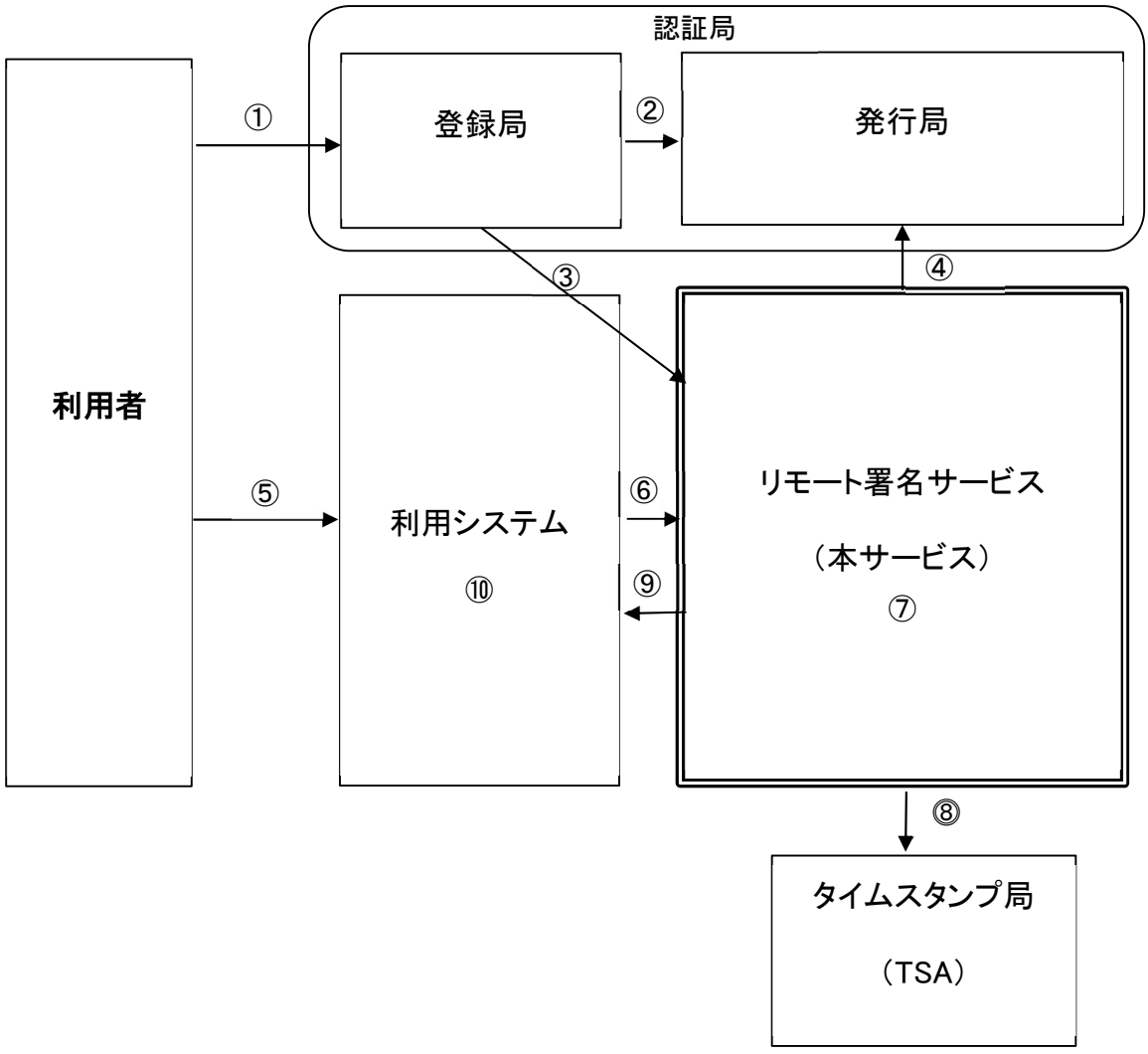
- iTrust 電子署名用証明書
  本サービスと連携する AATL に登録された認証局から電子文書への電子署名用証明書を発行するサービスです。本書の認証局は、このサービスの認証局と連携可能となります。

1.4 本サービスのステークホルダー及び適用可能性

1.4.1 本サービスのステークホルダーの適用範囲

本サービスを中心として構成されるリモート署名業務のステークホルダーの全体像を以下に示す。本業務のコミュニティ構成員は、リモート署名サービス、認証局、利用システム、利用者、タイムスタンプ局である。

本書は、本サービスにステークホルダーのリモート署名サービス、認証局、利用システムに対し適用される。



① 登録局にて利用者の電子証明書の発行審査を実施
② 発行局に電子証明書の発行依頼を実施し、証明書を発行
③ リモート署名サービスに利用者の電子証明書の登録依頼
④ リモート署名サービスが発行局から電子証明書を暗号化し登録
⑤ 利用システムにて利用者を認証
⑥ 利用システムから利用者に紐づく電子証明書を利用した電子署名要求
⑦ HSM に格納している利用者の電子証明書を利用した電子署名実行
⑧ タイムスタンプ要求と取得

⑨ 電子署名付き電子データの返却
⑩ 電子署名付き電子データの保存

1.4.2 リモート署名サービス

本サービスは、サイバートラストにより、本 iRSPS に準拠して運用される。

本サービスは、認証局の登録局経由で発行された利用者の電子証明書・秘密鍵を登録・保管し、厳格に運用する。本サービスは、利用システムから要求された利用者に紐づく電子証明書・秘密鍵による電子署名を実行する。利用者より、電子署名に加えタイムスタンプを要求された場合には、タイムスタンプをタイムスタンプ局から取得し該当電子データに付与する。

本サービスは本 iRSPS「3.2.1 信頼される役割および人物」に定めるサービス責任者が総括し、Cybertrust Japan Policy Authority（以下、「CTJ PA」という。）が本 iRSPS を承認する。

1.4.3 認証局

認証局は、サイバートラストが運営する「サイバートラスト マネージド PKI」上の認証局、または「iTrust 電子署名用証明書」の認証局となり、発行局および登録局から構成される。

登録局は、リモート署名サービスに登録する電子証明書について、利用者からの申請を受け付け、認証局の CPS に準拠した本人確認手順による審査を行い、発行依頼を発行局に対して実施する。発行局は、登録局の指示に基づき電子証明書の発行を行う。

1.4.4 利用システム

利用システムとは、本 iRSPS の内容に同意し、別途定めるサービス利用約款に基づく契約をサイバートラストと締結した組織の運営するシステムとなる。リモート署名サービスに対して、電子署名要求やタイムスタンプ付与要求を行う接続元のシステムとなる。

1.4.5 利用者

利用者とは、利用システムを利用する法人、個人の総称となる。利用者は、利用システムの運営組織と約款、もしくは契約などを行い、利用システムへの登録を事前に承諾している事を前提とする。

1.4.6 タイムスタンプ局

サイバートラストと契約している（一般）日本データ通信協会の「タイムビジネス信頼・安心認定制度」の認定を受けたタイムスタンプサービス事業者が運営しているタイムスタンプ局となる。

1.5 連絡窓口

本サービス、及び本 iRSPS に関する照会を以下の連絡先でメールにて受け付ける。

サイバートラスト株式会社 iTrust サポートデスク
住　所　　：〒060-0807　札幌市北区北 7 条西 1 丁目 1-2 SE 札幌ビル 13 階
メールアドレス　：itrust_support@cybertrust.co.jp
受付日　　：月曜日～金曜日（祝祭日およびサイバートラストの Web サイトに掲載の年末年始、指定日を除く）
受付時間　　：9:00～18:00

1.6 ポリシー管理

1.6.1 文書を管理する組織

本 iRSPS は、サイバートラストにより管理される。

1.6.2 iRSPS の適合性を決定する者

iRSPS の適合性については CTJ PA が決定する。

1.6.3 適合性の承認手続き

サイバートラストの社内規程に定められる評価・承認手続きの中で、CTJ PA が承認する。

2. 一般規定

2.1 義務

サイバートラストは、リモート署名業務における本サービス、認証局、利用システムの義務を、以下に定める。

2.1.1 リモート署名サービスの義務

本サービスは、本 iRSPS で規定する利用システム、利用者に対して、以下の義務を負う。

① 本サービスは、本 iRSPS に基づき、本サービスの運用を行う。

2.1.2 認証局の義務

認証局は、本 iRSPS で規定する本サービスに対し、以下の義務を負う。

① 認証局は、本 iRSPS における認証局に係る規定を遵守しなければならない。

② 認証局は、本サービスから CP/CPS の提示を求められた際には、速やかに CP/CPS を提示しなければならない。

③ 認証局は、認証局の運用を定めた CPS に基づき利用者の証明書を発行しなければならない。

④ 認証局は、不正な証明書の発行を防止しなければならない。

2.1.3 利用システムの義務

利用システムは、本 iRSPS で規定する本サービスに対し、以下の義務を負う。

① 利用システムは、本 iRSPS における利用システムに係る規定を遵守しなければならない。

② 利用システムは、リモート署名業務を行う利用者の認証を行い、利用者を特定（2 要素認証もしくは、同等レベルの認証）したうえで本サービスに対して電子署名要求を行わなければならない。なお、2 要素認証等で利用する PIN については、利用者のみが知り得るものでなければならない。

③ 本サービスに接続するための RS-API 接続用証明書は、厳格に管理しなければならない。

2.2 責任の制限

2.2.1 リモート署名サービスの責任

本サービスは、本 iRSPS で示される本サービスの義務を遵守しないことに起因して発生する、認証局、利用システムの損害に対し、責任を負うものとする。

本サービスの責任範囲は、本 iRSPS に定める業務を信頼できる従事者が行うことにより、利用システムより要求された電子証明書の本サービスへの登録、及び電子署名を行う機能に限られる。

本サービスは、以下の免責事項、及び本サービスの義務及び責任を明示していない一切の事項について、義務及び責任を負わない。

免責事項：以下の事象が発生した場合、本サービスは認証局及び利用システムに対し、免責されるものとする。

① 地震、水害等のあらゆる天災に起因する損害

② 火災、停電等のあらゆる外部からの災害に起因する損害

④ 戦争、暴動等のあらゆる不可抗力に起因する損害

⑤ 本サービスが、技術的又は運用上のやむを得ない理由により、緊急に本リモート署名業務を停止することに起因する損害

⑥ 認証局又は利用システムにおける、ソフトウェア及びハードウェア等の誤動作又は障害に起因する損害

⑦ 本サービスが管理できない、技術上又は運用上の理由に起因する損害

⑧ 認証局又は利用システムが、本 iRSPS に規定された義務及び責任を果たさない結果として発生する損害

⑨ 本リモート署名業務の一部、又は全部の終了に伴い発生する損害

2.2.2 認証局の責任

認証局は、本 iRSPS で示される認証局の義務を遵守しないことに起因して発生する本サービスの損害に対し、責任を負うものとする。

2.2.3 利用システムの責任

利用システムは、本 iRSPS で示される利用システムの義務を遵守しないことに起因して発生する本サービスの損害に対し、責任を負うものとする。

2.3 財務上の保証

2.3.1 リモート署名サービスによる保証

本サービスが、「本 iRSPS 2.2.1 リモート署名サービスの責任」に定める責任に違反し、損害賠償責任を負う場合は、別途定めるサービス利用約款にて規定する金額を上限とする。いかなる場合も、当該賠償額の上限を超える請求には応じない。

2.3.2 認証局による保証

認証局は、本 iRSPS で示される認証局の義務を遵守しないことに起因して発生する本サービスの損害に対し、賠償しなければならない。

2.3.3 利用システムによる保証

利用システムは、本 iRSPS で示される利用システムの義務を遵守しないことに起因して発生する本サービスの損害に対し、賠償しなければならない。

3. 運営、運用、物理的管理

3.1 物理的管理

3.1.1 立地場所および構造

本サービスのシステムは、地震、火災、水害およびその他の災害による影響を容易に受けない施設（以下、「本施設」といい、特段の規定がない限り、「本施設」という場合は、メインサイトおよび本 iRSPS「3.1.9 バックアップサイト」に定めるバックアップサイトを含むものとする。）内に設置される。また、本施設には、建築構造上、耐震、耐火および水害その他の災害防止ならびに不正侵入防止の措置が講じられる。なお、本施設が設置される建築物の外部および建築物内には、本サービスの所在に関わる情報を表示しない。

3.1.2 物理的アクセス

本施設および本施設内で本サービス業務が行われる各室は、業務の重要度に応じたセキュリティ・レベルが設けられ、相応する入退室管理が行われる。入退室時の認証には、セキュリティ・レベルに応じ、入退室用カードまたは生体認証その他の実装可能な技術的手段を用いる。また、特に重要な各室への入室および同室内において本サービスのシステムその他重要資産が保管される保管庫の開扉の両方またはいずれか一方は、入室権限を有する複数名が揃わなければ開扉されない措置を講ずる。

本施設および本施設内の本サービス業務が行われる各室は、監視システムにより、24 時間 365 日の監視が行われる。

3.1.3 電源・空調設備

本施設では、本サービスのシステムおよび関連機器類の運用のために必要かつ十分な容量の電源を確保する。また、瞬断ならびに停電対策として、無停電電源装置および自家発電機を設置する。さらに、本サービス業務を行う各室には空調設備を設置し、特に重要な室内は 2 重化する。

3.1.4 水害対策

本施設内の本サービス業務を行う特に重要な各室には漏水検知機を設置し、防水対策を講じる。

3.1.5 火災対策

本施設は、耐火構造の建物である。また、特に重要な各室は防火区画内に設置され、火災報知機および自動ガス式消火設備を備える。

3.1.6 地震対策

本施設は耐震構造の建物であり、また、本サービスのシステム機器および什器には転倒および落下を防止する対策を講じる。

3.1.7 媒体保管場所

本サービスのシステムのバックアップデータが含まれる媒体、本業務で使用した書類等については、職務上許可された者のみが入室できる室内に保管する。

3.1.8 廃棄物処理

機密情報を含む書類はシュレッダーにより裁断の上、廃棄する。電子媒体については、物理的破壊、初期化、消磁等の措置によって記録されたデータを完全に抹消の上、廃棄する。

3.1.9 バックアップサイト

本サービスのシステムの復旧上重要な資産の原本またはコピーは、メインサイト内のほか、遠隔地のバックアップサイトにも保管する。バックアップサイトの保管庫は、複数名の者により施錠管理され、また、開扉の記録が残される。

3.2 手続的管理

3.2.1 信頼される役割および人物

本サービスは、本サービスを運営するために必要な人員（以下、「運用員」という。）およびその役割を以下のとおり定める。

3.2.1.1 サービス責任者

サービス責任者は、本サービスを総括する。

3.2.1.2 システム管理者

システム管理者は、本サービスの各種業務を管理する。

3.2.1.3 システムアドミニストレータ

システムアドミニストレータは、システム管理者の管理の下、本サービスのシステムの維持・管理を行う。

3.2.1.4 オペレータ

オペレータは、システム管理者およびシステムアドミニストレータの業務を補佐する。ただし、本サービスのシステムを操作する権限は付与されない。

3.2.2 役割ごとに必要とされる人数

本サービスは、システムアドミニストレータについては、2 名以上配置する。

3.2.3 各役割における本人性確認と認証

本サービスは、各役割に応じ、業務を行う各室の入室権限および本サービスのシステムの操作権限を定める。各室の入室時またはシステムの操作時においては、入退室カード、生体認証、電子証明書、ID およびパスワード等の単体または組合せより、本人性および入室・操作権限の確認ならびに認証が行われる。

3.2.4 職務の分離が必要とされる役割

サービス責任者が他の役割を兼務することを認めない。

3.3 人事的管理

3.3.1 外部委託

本サービスは、本サービスにおける運用管理等、本業務の一部を信頼の置ける第三者に委託することができる。本業務の一部を委託した場合、委託先は、本 iRSPS を遵守して業務を行う。

3.3.2 専門性

本公サービスは、本 iRSPS に従い、サービスしての信頼性を維持するため、専門性を持つ要員によって運用される。

3.3.3 組織体制

本サービスは、本 iRSPS に従い、リモート署名業務としての信頼性を維持するため、必要な組織体制を構築し運用する。

3.3.4 人事管理

本サービスは、各業務の運用員の適正を考慮の上、本サービスにおいて十分に信頼の置ける職務の執行が可能となる、人事管理を行う。

3.3.5 事務取扱要綱等の規程

本サービスは、本 iRSPS に従い、本サービスとしての信頼性を維持するため、必要なリモート署名業務の事務取扱要綱等の内部規程を定める。本 iRSPS の改訂を行う場合、必要に応じ、事務取扱要綱等の内部規程も速やかに改訂する。なお、内部規程は非公開とする。

3.3.6 経歴、資格、経験等に関する要求事項

運用員は、サイバートラストが別途定める採用基準に基づき採用され、配置される。

3.3.7 身元調査手続き

運用員として配置される社員の身元調査は、サイバートラストの社内規程に基づき行われる。

3.3.8 教育および訓練

本サービスは、運用員として配置されるすべての従業員に対し教育および訓練を実施する。教育および訓練には、本 iRSPS および関連諸規程の教育のほか、運用員の役割に応じた必要な教育および訓練を含む。

また、教育および訓練の有効性はシステム管理者が評価し、必要に応じ再教育・訓練を実施する。

3.3.9 再教育・訓練の周期と要件

本サービスは、運用員に対する再教育および訓練を適宜実施する。少なくとも以下の事態が生じた場合は、教育・訓練を実施する。

- 本 iRSPS、関連諸規程の変更時で、CTJ PA、サービス責任者、システム管理者が必要と判断した場合
- 本サービスのシステムの変更をする場合であって、CTJ PA、サービス責任者、システム管理者が必要と判断した場合
- その他、CTJ PA、サービス責任者、システム管理者が必要と判断した場合

3.3.10 職務ローテーションの周期と順序

本サービスは、必要に応じ運用員の配置転換を行う。

3.3.11 許可されていない行動に対する罰則

サイバートラストは、運用員が本 iRSPS および関連諸規程に反する行動をした場合、速やかに原因ならびに影響範囲等の調査を行った上で、サイバートラストの就業規則に準じ、処罰を課す。

3.3.12 契約社員等に対する契約要件

サイバートラストは、業務委託先の社員、契約社員または派遣社員等（以下、「契約社員等」という。）を運用員として配置する場合、委託業務の内容、契約社員等に課す守秘義務および罰則等を明確に定めた契約を結ぶとともに、契約社員等に対し、本 iRSPS およびサイバートラストの社内規程の遵守を要求する。契約社員等が本 iRSPS およびサイバートラストの社内規程に反する行動をした場合、処罰については、当該契約に基づき行う。

3.3.13 運用員が参照できる文書

本サービスは、各運用員に対し、役割に応じた必要な文書のみが参照できる措置を講ずる。

3.4 監査ログの手続き

3.4.1 記録されるイベントの種類

本サービスは、本 iRSPS の準拠性およびセキュリティの妥当性を評価するため、監査ログとして以下の記録を収集する。なお、記録には日時、記録の主体、イベントの内容を記録する。

- 本サービスが維持管理するシステム上の記録
- ネットワークセキュリティに関する記録
- 本施設の入退室に関する記録
- 本施設の維持管理に関する記録

3.4.2 監査ログを処理する頻度

本サービスは、本 iRSPS「3.4.1 記録されるイベントの種類」に規定された監査ログに関し、週次、月次または四半期に一度の頻度で検査する。

3.4.3 監査ログの保管期間

イベントの記録については、少なくとも 7 年間は保管する。

本サービスは、監査ログが不要となったとき、本 iRSPS「3.1.8 廃棄物処理」の規定に基づき廃棄する。

3.4.4 監査ログの保護

本サービスは、許可された者のみが閲覧可能となるよう、監査ログへのアクセスコントロールを施す。保管庫への物理的なアクセスコントロール、電子媒体であればフォルダ等への論理的なアクセスコントロールを施す。

3.4.5 監査ログのバックアップ手続き

本サービスは、システム上のログについては、バックアップを取得する。紙媒体については、原本のみを保管する。

3.4.6 監査ログの収集システム

本サービスのシステムは、実装された機能により監査ログを自動的に収集する。

3.4.7 当事者への通知

本サービスは、イベントを発生させた当事者に通知することなく、監査ログを収集、検査する。

3.4.8 脆弱性評価

本サービスは、内部の脆弱性診断専門部署による脆弱性に関する評価を受け、当該脆弱性を是正するために必要な対応を行う。また、監査ログの検査により脆弱性が発見された場合についても、同様に必要な対応を行う。

3.5 記録の保管

3.5.1 保管対象となる記録

本サービスは、本 iRSPS「3.4.1 記録されるイベントの種類」で規定された監査ログのほか、以下の情報を保管する。

- 連携する認証局から発行された利用者の証明書
- 連携する認証局の証明書
- 内部監査報告書
- 外部監査報告書
- 申請時に運営組織より受理した書類・データ
- 本 iRSPS および関連諸規程

3.5.2 記録の保管期間

本サービスは、本 iRSPS「3.5.1 保管対象となる記録」に規定される記録について、7 年間保管する。

本サービスは、記録が不要となったとき、本 iRSPS「3.1.8 廃棄物処理」の規定に基づき廃棄する。

3.5.3 記録の保護

本 iRSPS「3.4.4 監査ログの保護」と同様の手続きにより行う。

3.5.4 記録のバックアップ手続き

本 iRSPS「3.4.5 監査ログのバックアップ手続き」と同様の手続きにより行う。

3.5.5 タイムスタンプ

本サービスは、帳票類については起票日もしくは処理した日付を記録する。また、日付のみでは記録としての立証性に欠ける場合は、時刻も記録する。本サービスでの電子署名およびタイムスタンプについては、処理された日時を記録する。また、処理された日時に対して正確な日付・時刻を記録するために必要な措置を講じる。

3.5.6 記録収集システム

電子署名およびタイムスタンプの付与結果については、本サービスのシステムの機能により自動的に収集する。その他の紙媒体については、運用員が収集する。

3.5.7 記録の取得と検証手続き

本サービスは、記録の取得および閲覧が認められる者として、運用員、監査人および CTJ PA、が認めた者に限定する。また、記録の可読性に関わる検証は、必要に応じ、実施する。

3.6 危殆化および災害からの復旧

3.6.1 危殆化および災害からの復旧手続き

本サービスは、本サービスの HSM が危殆化した場合、以下を実行すると同時に、危殆化の事実を関係者へ公開する。

- 危殆化した HSM を用いた業務の停止
- 危殆化の原因調査
- 是正処置案の策定ならびに CTJ PA による評価・承認
- 是正処置の実行
- 業務再開の妥当性の評価
- 新たな HSM の調達
- 業務の再開（関係者への通知を含む）

また、本サービスが被災した場合には、本 iRSPS「3.6.4 災害時等の事業継続性」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、ソフトウェアおよびデータにより復旧作業を行い、業務の再開に努め、再開時には再開の事実を関係者に公開する。

3.6.2 システム資源の障害時の手続き

本サービスは、ハードウェア、ソフトウェアまたは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、ソフトウェアまたはデータを用いて業務を継続する。

3.6.3 利用者秘密鍵の危殆化時の手続き

利用者は、自己の責任により本サービスが保持する秘密鍵の危殆化もしくは危殆化が疑われる事態が生じた場合、認証局の CPS に規定された手続に基づき、証明書の失効手続を行わなければならない。

3.6.4 災害時等の事業継続性

本サービスは、災害等からの復旧対策ならびに業務継続について、本施設に保管されたデータ等を用い、本サービスの業務の全体または一部の復旧・再開を実施する。

3.7 本サービスの業務の終了

本サービスは、本サービスの業務を終了する場合、事前に利用システムに通知するほか、サイバートラストの Web サイトにおいても、その旨公開する。

本サービスが保有する利用システムの情報については、廃棄もしくは業務移管先へ提供するものとし、この旨は業務終了時にサイバートラストの Web サイト上で告知される。

4. 技術的なセキュリティ管理

4.1 暗号鍵の生成および導入

4.1.1 暗号鍵の生成

本サービスで使用する利用者の電子証明書・秘密鍵を暗号化する暗号鍵に関しては、FIPS 140-2 Level 3 の規格を満たした HSM 内の機能を用いて生成し、その毀損、紛失、改変、漏洩、及び無断使用等に対する防止措置を十分に講じ保護する。

4.1.2 鍵長および暗号アルゴリズム

電子証明書・秘密鍵の暗号処理	
暗号アルゴリズム	AES
鍵長	256bit

4.1.3 ハードウェア及びソフトウェアにおける暗号鍵の生成

本サービスで利用する暗号鍵は、HSM 内で生成される。

4.2 秘密鍵の保護および暗号モジュール技術の管理

4.2.1 暗号モジュールの標準および管理

本サービスの暗号鍵を管理するための暗号モジュールは、FIPS 140-2 レベル 3 の規格を満たした HSM とする。HSM は、本サービスが管理する。

4.2.2 暗号鍵の複数人管理

本サービスで使用する暗号鍵の管理は、常時複数のシステムアドミニストレータが行う。

4.2.3 暗号鍵の預託

本サービスは、暗号鍵の預託を行わない。

4.2.4 暗号鍵のバックアップ

本サービスの暗号鍵のバックアップは、システムアドミニストレータが行う。HSM からバックアップされた暗号鍵は、バックアップサイトのバックアップ用機材に保管を行う。

4.2.5 暗号鍵のアーカイブ

本サービスは、暗号鍵のアーカイブを行わない。

4.2.6 暗号鍵の移送

本サービスで使用する暗号鍵のコピーを安全な方法でバックアップサイトへ移送する。HSM の故障等により本サービスの暗号鍵の復元が必要となる場合、システムアドミニストレータは、メインサイトまたはバックアップサイトに保管されたバックアップを用いて復元する。

4.2.7 暗号モジュール内での暗号鍵保存

本サービスの暗号鍵は、HSM 内で生成され、冗長化された HSM にてそれぞれで保存される。

4.2.8 暗号鍵の活性化

本サービスで使用する暗号鍵は、システム管理者の承認の下、別途規定された手順に基づき、複数のシステムアドミニストレータにより活性化される。また、活性化作業は記録される。

4.2.9 暗号鍵の非活性化

本サービスで使用する暗号鍵は、システム管理者の承認の下、別途規定された手順に基づき、複数のシステムアドミニストレータにより非活性化される。また、非活性化作業は記録される。

4.2.10 暗号鍵破壊の方法

本サービスで使用する暗号鍵は、サービス責任者の指示を受け、システム管理者の管理の下、別途規定された手順に基づき、複数のシステムアドミニストレータにより破壊される。同時に、本 iRSPS「4.2.4 暗号鍵のバックアップ」に規定されたバックアップされた暗号鍵についても、同様の手順に基づき破壊される。また、破壊作業は記録される。

4.2.11 暗号モジュールの評価

本サービスは、本 iRSPS「4.2.1 暗号モジュールの標準と管理」に定める標準を満たした HSM を使用する。

4.3 コンピュータのセキュリティ管理

4.3.1 コンピュータセキュリティに関する技術的要件

本サービスのシステムは、セキュリティ対策として以下を実施する。

- 操作者の権限の認証
- 操作者の識別と認証
- 重要なシステム操作に対する操作ログの取得
- 適切なパスワード設定および定期的な変更
- バックアップ・リカバリ

4.3.2 コンピュータセキュリティの評価

本サービスは、本サービスが導入するハードウェア、ソフトウェアに対して、事前に導入評価を実施する。また、使用するシステムにおけるセキュリティ上の脆弱性に関する情報収集および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、速やかに必要な対応を行う。

4.4 ライフサイクルセキュリティ管理

4.4.1 システム開発管理

本サービスのシステムの構築および変更は、サイバートラスト内部で任命された開発責任者の管理の下、別途定められた規定に基づき行う。開発責任者が必要と判断する場合は、テスト環境において必要かつ十分な検証を行い、セキュリティ上問題がないことを確認する。

4.4.2 セキュリティ運用管理

本サービスのシステムは、十分なセキュリティを確保するために必要な設定が行われる。また、セキュリティ・レベルに則した入退室管理やアクセス権限管理、同システムのウィルス対策等を実施するとともに、セキュリティ上の脆弱性についての情報収集および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、速やかに必要な対応を行う。

4.4.3 ライフサイクルセキュリティ管理

本サービスのシステムの開発、運用、変更、廃棄の各工程において責任者を定め、作業計画または手順を策定・評価し、必要に応じ試験を行う。また、各作業は記録される。

4.5 ネットワークセキュリティ管理

本サービスのシステム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接続され、また、侵入防御システムによる監視が行われる。

4.6 タイムスタンプ

本 iRSPS「3.5.5 タイムスタンプ」に準じる。

5. 準拠性監査およびその他の評価

5.1 監査の頻度および要件

本サービスは、JIPDECトラステッド・サービス登録の監査を年に一度、あるいは本 iRSPS「5.2 監査人の要件」で定める監査人が必要と判断した時期に往査する。

5.2 監査人の要件

JIPDECトラステッド・サービス登録の検証は、資格を有する外部の監査人が実施する。

5.3 監査人と被監査者の関係

監査人は、原則としてサービスの業務から独立し、中立性を保つ者とする。

5.4 監査の範囲

JIPDECトラステッド・サービス登録については、このプログラムが定める範囲とする。

5.5 指摘事項の対応

検証により発見された指摘事項は、サービス責任者、システム管理者へ報告される。監査人、サービス責任者、システム管理者により是正措置が必要と判断された場合、サービス管理者またはシステム管理者の管理の下、是正措置を実施する。

5.6 監査結果の開示

JIPDECトラステッド・サービス登録の検証結果は、各ガイドラインの定めに従い、公開される。

6. その他の業務上および法的な事項

6.1 料金

本サービスに関する料金および支払方法については、サイバートラストの Web サイト上、あるいは見積書等、利用システムの運営者が適切に確認できる手段により通知する。なお、サイバートラストの Web サイト上の記載と、別途サイバートラストが提出した見積書等の記載との間に齟齬がある場合には、見積書等の記載が優先的に適用されるものとする。

6.2 財務的責任

サイバートラストは、本 iRSPS に定める内容を遵守のうえ本サービスを運営するために、十分な財務的基盤を維持するものとする。また、賠償責任への対応に備え、適切な保険に加入する。

6.3 企業情報の機密性

6.3.1 機密情報の範囲

本サービスは、以下の情報を機密として取り扱う(以下、「機密情報」という。)。

- 利用システム及び利用者からの申込情報
- 本 iRSPS「6.4.2 個人情報として扱われる情報」に定める情報
- 利用システム、認証局、その他第三者より受けた問合せ情報
- 本サービスのセキュリティに関する情報

6.3.2 機密情報の範囲外の情報

本サービスが保有する情報のうち、以下の情報は機密情報の範囲外とする。

- 利用者の証明書
- 本サービスの過失によらず公知となった情報
- 本サービス以外のものから機密保持の制限なしに公知となった情報
- 利用システムから事前に開示または第三者への提供に関する合意を得た情報

6.3.3 機密情報の保護責任

本サービスは、機密情報の漏洩を防止する対策を実施する。また、本サービスの運営の用に供する以外には使用しない。ただし、機密情報に関して、裁判上、行政上その他の法的手続きの過程において機密情報の開示要求があった場合、買収、合併等に関連して財務アドバイザー、潜在的買収・合併当事者などサイバートラストとの間で守秘義務契約を締結した者および／または弁護士、公認会計士、税理士等の法により守秘義務を負う者に開示する場合、または利用システムの運営者から事前の承諾を得た場合、サイバートラストは、当該機密情報を開示要求者に対して開示することができるものとする。この場合、開示を受ける当該開示要求者は当該当該情報をいかなる方法によっても第三者に開示し、または漏洩させてはならない。

なお、個人情報の保護の取扱いは、本 iRSPS「6.4 個人情報の保護」に規定する。

6.4 個人情報の保護

6.4.1 プライバシー・ポリシー

本サービスが保有する個人情報の取り扱いは、サイバートラストの Web サイト（https://www.cybertrust.co.jp/corporate/privacy-policy.html）で公開するプライバシー・ポリシーに定める。

6.4.2 個人情報として扱われる情報

本サービスは、電子データ（PDF）、利用者の証明書、問合せ等に含まれる特定の個人を識別することができる情報を個人情報として扱う。

6.4.3 個人情報とみなされない情報

本サービスは、本 iRSPS「6.4.2 個人情報として扱われる情報」に定める情報以外は、個人情報とみなさない。

6.4.4 個人情報の保護責任

本サービスが保有する個人情報の保護責任は、本 iRSPS「6.4.1 プライバシー・ポリシー」に定めるとおりとする。

6.4.5 個人情報の使用に関する個人への通知および同意

本サービスは、監査の実施のために利用システムの運営者の個人情報を使用することについて、利用システムの運営者より同意を得たものとみなす。

また、本サービスは、個人情報について、本業務を実施する目的以外で使用しない。ただし、本 iRSPS「6.4.6 司法手続または行政手続に基づく開示」、「6.15 法執行機関への情報開示」、および「6.16 民事手続き上の開示」に定める場合を除くものとする。

6.4.6 司法手続または行政手続に基づく開示

本サービスで取扱う個人情報に関して、裁判上、行政上その他の法的手続きの過程において情報の開示要求があった場合、サイバートラストは、当該個人情報を開示することができるものとする。

6.4.7 他の情報公開又は開示の場合

本サービスは、業務の一部を外部に委託する場合、機密情報を委託先に対して開示することがある。この場合、当該委託に関する契約において、当該委託先に対して機密情報の守秘義務を課す規定を置くものとする。

6.5 知的財産権

特段の合意がなされない限り、以下の情報に関するすべての知的財産権は、サイバートラストまたは本サービスに関するサイバートラストの仕入先またはライセンサーに帰属するものとする。

- 本 iRSPS および関連文書
- 本サービスの HSM 内に格納された暗号鍵
- 本サービスから貸与されたソフトウェア、ハードウェア

6.6 表明保証

以下に本サービス、認証局、利用システムの表明保証を規定する。なお、本 iRSPS「6.6 表明保証」で明示的に規定された本サービス、認証局、利用システムの表明保証を除き、各当事者はいかなる明示的または黙示的な表明保証をも行わないことを相互に確認する。

6.6.1 本サービスの表明保証

サイバートラストは、リモート署名業務の遂行にあたり、以下の義務を負うことを表明し保証する。

- 本サービスの HSM 内に格納された暗号鍵の安全な管理を行うこと
- 認証局から登録した利用者の電子証明書及び秘密鍵の安全な管理を行うこと
- システムの監視および運用を行うこと

6.6.2 認証局の表明保証

認証局における業務の遂行にあたり、以下の義務を負うことを表明し保証する。

- CPS に基づく加入者の審査を行うこと
- 本サービスに登録した利用者の電子証明書及び秘密鍵の安全な管理を行うこと
- 利用者が電子証明書の利用を中止した場合は、速やかに電子証明書を失効すること

6.6.3 利用システムの表明保証

利用システムは、以下の義務を負うことを表明し保証する。

- 証明書の発行申請時における真正かつ正確な情報提供を行うこと
- 証明書用途の遵守（認証局の CPS にて規定された証明書の利用用途の厳守 ）
- 利用システムは、利用者が利用システムを利用する際の通信経路を TLS 等で暗号化するなど、安全にするための措置を講じること
- 利用者のアカウント情報が漏洩した疑義がある場合、または利用者の認証の失敗が連続して発生した場合には、利用者アカウントの停止を行うこと
- 利用システムは、利用者だけが利用可能なアカウントを開設すること
- 利用者のアカウント情報の変更要求があった時には、利用者情報を速やかに変更すること
- 定期的に利用者の休眠状況を確認し、休眠利用者についてはアカウントの停止等の措置を行うこと
- 利用者と利用システムの契約終了時には、速やかに利用システム上のアカウント利用停止を行うこと
- 公序良俗に反する電子文書で証明書を利用しないこと
- 証明書に含まれる情報の正確性に疑義が生じた場合は、当該疑義を解消するまで、証明書を使用しないこと
- 有効期間が満了した証明書および失効された証明書を使用しないこと
- 関連法規制を遵守すること

6.6.4 他の関係者の表明保証

規定しない。

6.7 不保証

本サービスは、本 iRSPS「6.6.1 本サービスの表明保証」および「6.6.2 認証局の表明保証」に定める保証に関連して発生する直接損害以外の損害については、本 iRSPS に基づく債務不履行に関していかなる責任も負わない。

6.8 責任の制限

サイバートラストは、本 iRSPS「6.6.1 本サービスの表明保証」および「6.6.2 認証局の表明保証」の内容に関し、以下の場合に一切の責任を負わないものとする。

- サイバートラストの本サービスが、本 iRSPS および法規制を遵守したにも関わらず発生するいかなる損害
- サイバートラストに起因しない、不法行為、不正使用または過失等により発生するいかなる損害
- 暗号アルゴリズム解読技術の向上等、技術の進歩に伴う暗号強度の弱体化、その他の暗号アルゴリズムの脆弱性等に起因する損害

6.9 補償

本サービスが電子署名またはタイムスタンプ付与した電子データを、利用者または利用システムが受領した時点で、利用者または利用システムには、自らのなした以下に掲げるいずれかの行為に起因して生じた第三者からのサイバートラストに対する請求、訴訟の提起その他の法的措置によってサイバートラストが被った損害を賠償し、かつサイバートラストに損害を生ぜしめないようにする責任が生じるものとする。

- 電子データ（PDF）の不正使用、改ざん、利用時の不実の表明
- 本 iRSPS またはサービス利用約款への違反
- 利用システムによる利用者認証のセキュリティの怠慢

また、本サービスは、利用者または利用システムの代理人、受託者またはその他代表者ではない。

6.10 文書の有効期間と終了

6.10.1 文書の有効期間

本 iRSPS は、CTJ PA が承認することにより有効となる。また、本 iRSPS「6.10.2 終了」に定める時点の前に本 iRSPS が無効となることはない。

6.10.2 終了

本 iRSPS は、本 iRSPS「6.10.3 終了の影響と存続条項」に定める規定を除き、本サービスが業務を終了した時点で無効となる。

6.10.3 終了の影響と存続条項

本 iRSPS 6.3、6.4、6.5、6.6、6.7、6.8、6.9、6.10.2、6.10.3、6.13、6.14、6.15、6.16、6.19 の規定については本 iRSPS の終了後も、存続するものとする。

6.11 関係者間の個別通知と連絡

サイバートラストから認証局、利用システム、利用者に対し個別の通知を行う場合は、書面による手渡しがなされたとき、受取確認付き書留郵便により配達されたとき、または電子メールを送信したときをもって通知がなされたものとみなす。また、認証局、利用システム、利用者からサイバートラストへのすべての通知はサイバートラスト所定の方法により通知がなされるものとする。なお、書面による通知の場合は、当該通知が郵送され、サイバートラストが受領した場合に到達したものとみなす。

6.12 改訂

6.12.1 改訂手続き

本サービスは、CTJ PA の指示に基づき、適宜、本 iRSPS の改訂を行うことができる。運用員の評価、あるいは弁護士等外部の専門家または有識者の評価を得た後、CTJ PA が改訂の承認を行う。

6.12.2 通知方法と期間

本サービスは、本 iRSPS の改訂を CTJ PA が承認した後、改訂後および改訂前の iRSPS を一定期間 Web サイトに公開し、加入者および信頼当事者がその変更内容について確認できる措置を講ずる。サイバートラストから当該改訂の撤回の通知が公表されない限り、当該改訂は CTJ PA が別途定める時点をもって発効するものとする。認証局、利用システム、利用者がその発効後 15 日以内に、異議を表明しない場合、改訂後の本 CPS につき同意したものとみなされる。

6.12.3 オブジェクト識別子の変更

規定しない。

6.13 紛争解決手続き

全ての当事者は、本 iRSPS 又は本サービスの業務の運用に関して生じた紛争に関する第一審の専属的合意管轄裁判所を、東京地方裁判所とすることで、合意するものとする。本 iRSPS 及び別途定めるサービス約款等に定められていない事項、又はこれらの文書の解釈に関して疑義が生じた場合、各当事者は、その課題を解決するため誠意を持って協議するものとする。

本 iRSPS または本サービスに関連して生じたすべての訴訟については、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。また、本 iRSPS に定めのない事項または本 iRSPS に疑義が生じた場合は、当事者が誠意をもって協議するものとする。

6.14 準拠法

本 iRSPS の解釈およびに本 iRSPS に基づくリモート署名業務にかかわる紛争については、日本国の法律が適用される。

6.15 法執行機関への情報開示

本サービスは、行政機関、裁判所、又はその他の法律上権限を有する者から強制力を伴う開示要求があった場合、法令に従い、それらの法執行機関に対し機密情報を開示する。

6.16 民事手続き上の開示

本サービスは、調停、起訴、及びその他の裁判又は行政手続きの過程において、機密保持対象である情報を開示する。

6.17 iRSPS の有効性

本 iRSPS における特定の規定が、何らかの理由、いかなる程度であれ、無効又は執行不可能であるとされた場合、本 iRSPS 上のその他の規定については、なお有効である。無効又は執行不可能であるとされた規定については、iTrust 評議会にて当該規定の内容を検討の上、CTJ PA の承認に基づき、改善を図る。

6.18 iRSPS の完全性

本サービスの権利及び義務に直接影響する本 iRSPS の規定を修正する場合は、本 iRSPS「6.12 改定」に準拠する。

6.19 雑則

6.19.1 完全合意条項

本 iRSPS における合意事項は、特段の定めをしている場合を除き、本 iRSPS が改訂または終了されない限り、他のすべての合意事項より優先される。

6.19.2 権利譲渡条項

サイバートラストが本サービスを第三者に譲渡する場合、本 iRSPS および本 iRSPS に定める責務およびその他の義務の譲渡を可能とする。

6.19.3 分離条項

本 iRSPS の一部の条項が、何らかの事由により無効となった場合においても、その他の条項は有効であるものとする。

6.19.4 強制執行条項

規定しない。

6.19.5 不可抗力条項

天災地変、裁判所の命令、労働争議、その他本サービスの責に帰さない事由により、本 iRSPS 上の義務の履行が一部または全部を遅延した場合には、サイバートラストは当該遅延期間について本 iRSPS 上の義務の履行を免れ、認証局、利用システム、利用者は一部を信頼し、もしくは利用した第三者に対し、何らの責任をも負担しない。