cybertrust

電子署名やタイムスタンプをクラウドで実現する
「iTrust リモート署名サービス」のご紹介

2025/02

はじめに

「iTrust リモート署名サービス」は、
契約書や控除証明書などの書面の電子化で求められる長期間に渡る真正性を確保するための長期署名に対応した電子署名やタイムスタンプ機能をAPIで提供するクラウドサービスです。

昨今、大手の金融機関をはじめとして電子契約の導入が進んでいる一方で、本格的な電子契約を実現するためには専門的な知識やノウハウ、また公開鍵基盤の中でも長期署名のような高度な技術を用いる必要があり、導入による運用管理の負荷が課題となっております。

サイバートラストは、電子認証事業者として長年に渡って蓄積してきたノウハウをもとに、利用者の秘密鍵を厳格に管理し、またその秘密鍵を用いてクラウドで安全に電子署名ができる環境を提供することでビジネスプロセスのデジタル化に関わる課題を解決します。

事業領域

認証・セキュリティサービス

パブリック証明書

SSL/TLSサーバ証明書
- SureServer / SureServer EV

S/MIME署名証明書
- SureMail

トラストサービス

本人確認
- iTrust 本人確認サービス

電子署名用証明書
- iTrust 電子署名用証明書

電子署名
- iTrust リモート署名サービス

電子認証局サービス

認証局アウトソーシング
- サイバートラスト マネージドPKI

ユーザ認証用証明書
- サイバートラスト パーソナルID

デバイス認証用証明書
- サイバートラスト デバイスID

セキュリティサービス

脆弱性診断
- Webアプリケーション診断 / 脆弱性ツール診断
- ネットワーク診断
- スマートフォンアプリ診断

セキュリティコンサルティングサービス

プラットフォームサービス（Linux/OSS/IoT）

プロフェッショナルサービス

認証・セキュリティ事業の沿革

- **1997年 国内初の商用電子認証センターとして開局**
  - GTE Government Systems（現Verizon）の米国政府向け電子認証センターをベースに設計・施工
- **1997年 国内初のSSL/TLSサーバ証明書を発行**
- **2001年 国内初の電子署名法対応認証局を運用開始**
  - 帝国データバンク様と協業し、日本初となる国土交通省様の電子入札で利用
- **2006年 国際規格 WebTrust for CA/EV 監査に合格（サーバ証明書）**
- **2009年 国内初の端末認証サービス「サイバートラスト デバイスID」提供開始**
  - 国内で初めて iPhone/iPadや Android端末などに対応した業界 No.1サービス
- **2016年 公的個人認証におけるプラットフォーム事業者として総務大臣認定取得**
- **2017年 WebTrust for CA 監査に合格（電子署名用証明書）**
- **2019年 AATL（Adobe Approved Trust List）登録（電子署名用証明書）**

iTrust サービス　～ DXに必要なトラストサービス基盤 ～

cybertrust

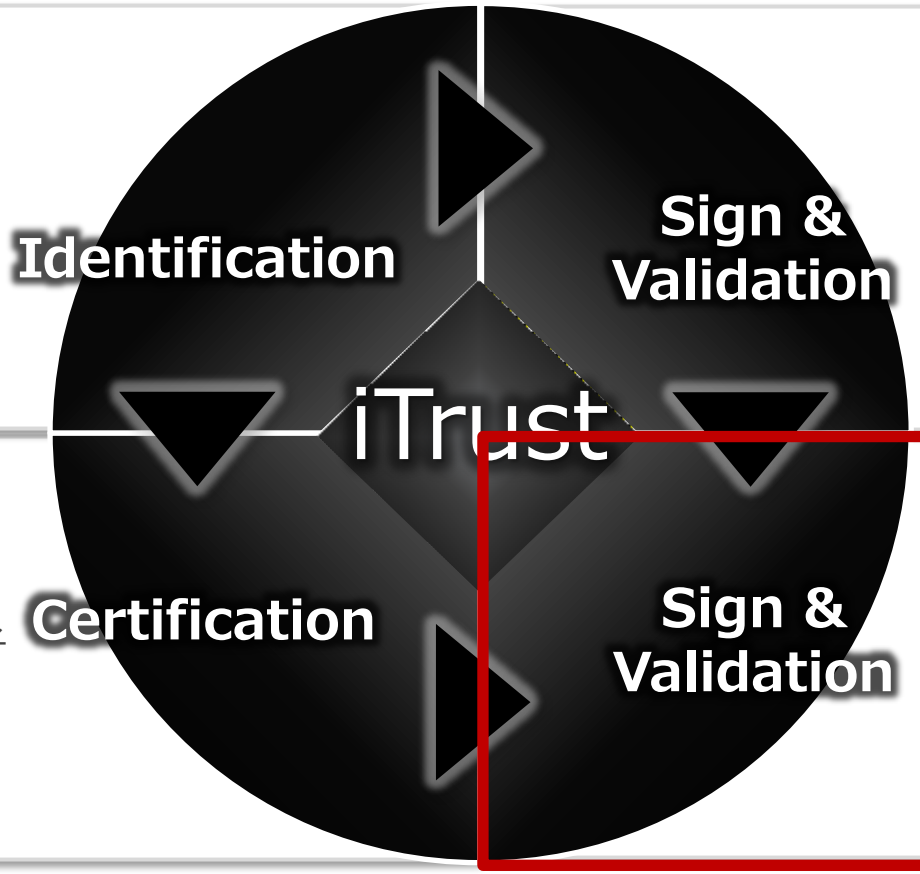
cybertrust iTrust
Identification & Trust

本人確認サービス

- 公的個人認証のプラットフォーム事業者として主務大臣認定を取得
- 本人確認、所在確認や生存確認などの現況確認が可能
- 犯罪収益移転防止法およびその運用で求められる要件に対応
- IC免許証や在留カードの真贋判定

電子署名用証明書

- 電子署名用途専用認証局として国内で初めてWebTrust監査に合格
- 個人（自然人）と法人の 2種類の電子署名用証明書を発行
- AATL：Adobe Approved Trust List に登録され安全性を視覚的に確認可



電子委任状サービス（検討中）

- 電子委任状法に則ったサービス
- 電子委任状取扱事業者として、総務大臣認定の取得を検討中
- 企業間の電子契約における委任関係を第三者機関として保証

リモート署名サービス

- 認証設備内で管理された秘密鍵によるクラウド署名サービス
- 長期署名（PAdES：PDF Advanced Electronic Signatures）に対応
- 日本情報経済社会推進協会：JIPDEC JCANトラステッドサービス登録済

iTrustリモート署名サービス ご活用事例

電子契約

電子署名法により、紙契約書を電子化する場合、適切な電子署名、タイムスタンプが必須

- 導入事例：弁護士ドットコム様「クラウドサイン」など電子契約サービス

電子帳簿保存法（電帳法）対応

電帳法により、2024年1月以降、電子化された請求書の紙での保存はNG

電帳法では、請求書にタイムスタンプを付与して保管することで、送受信パターンに依存せず対応が可能

- 導入事例：コクヨ様「電子帳票配信システム@TOVAS」など電子請求書管理サービス

eシール（PDFファイルの発行元証明と改ざん検知）

総務省より各種電子的な情報へeシール付与（PDFファイルの発行元証明/改ざん検知）することを推奨

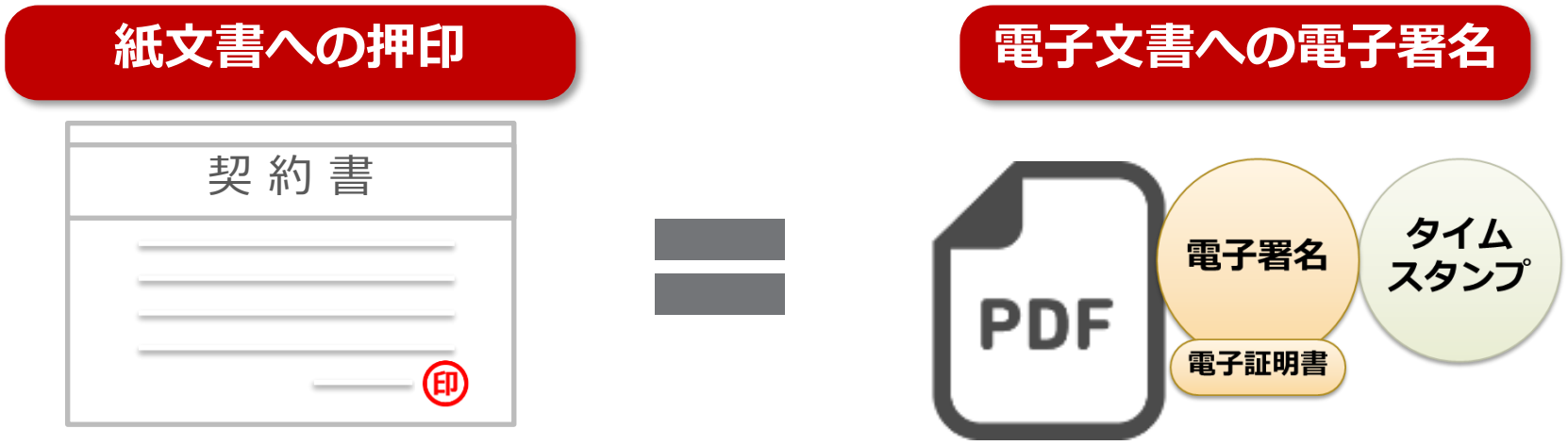
- 導入事例：日本品質保証機構様「校正証明書」など協会・保証機能の証書・証明書

文書の電子化と電子署名

電子文書に適切な電子署名とタイムスタンプを付与することで、「いつ」「誰が」「何に」合意したかを担保し、紙の契約書と同等の法的効力を持たせることが可能です。
※ 電子署名には署名した本人/組織を証明する電子証明書が添付されます。

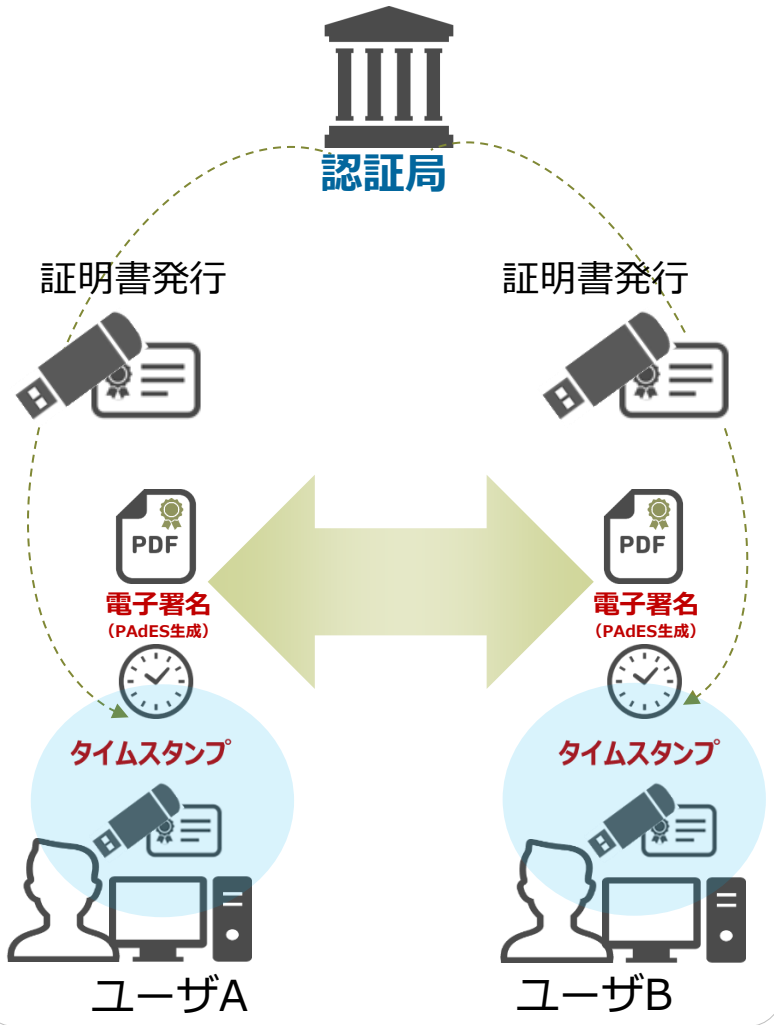
- 電子署名は、電子署名法第３条により、紙文書における押印や署名と同等の法的効力を持つものとされています。

電子化された文書に「電子署名」をすることで、以下を実現します。
・その文書の内容に「いつ」「誰が」「何に」合意したか担保
・その文書が改ざんされていないことを担保

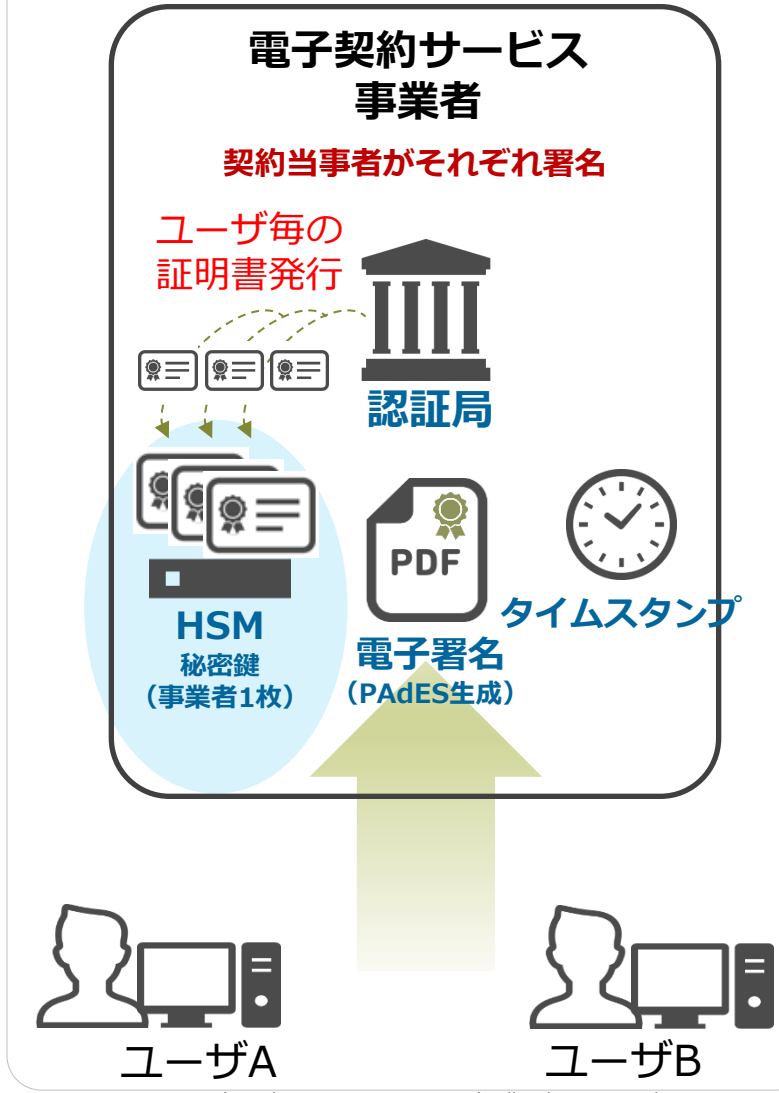


電子契約の形態

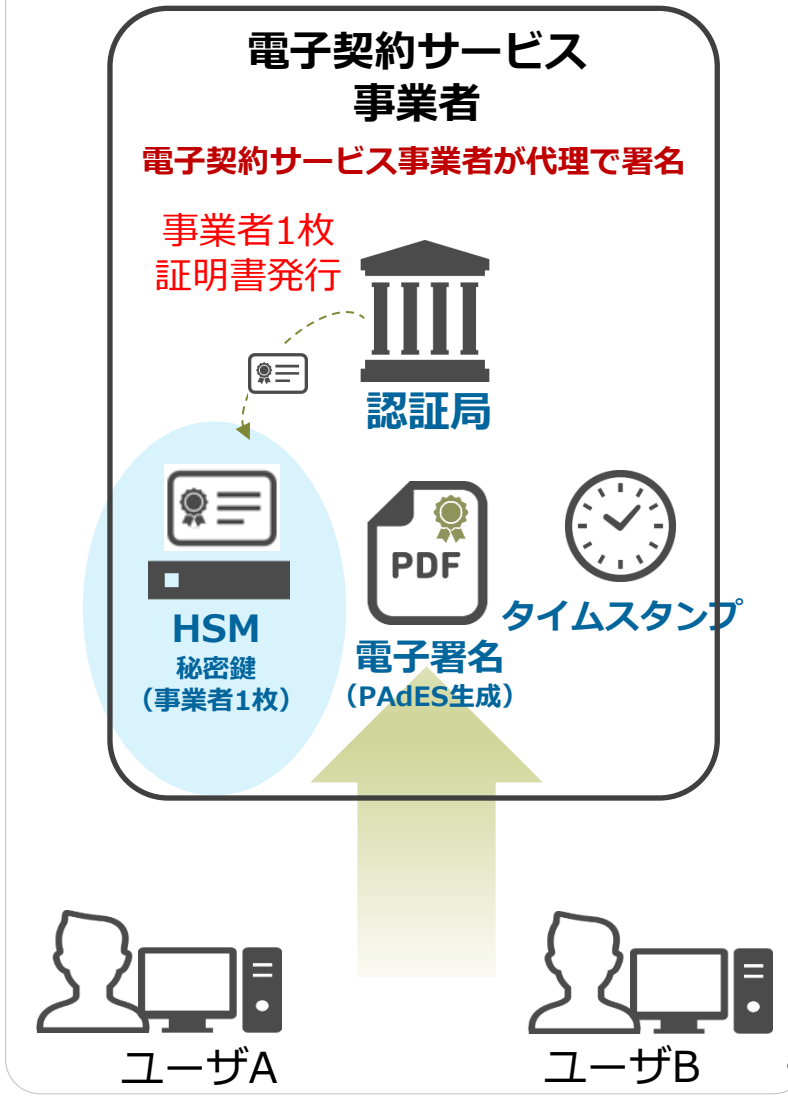
ローカル署名（当事者型）



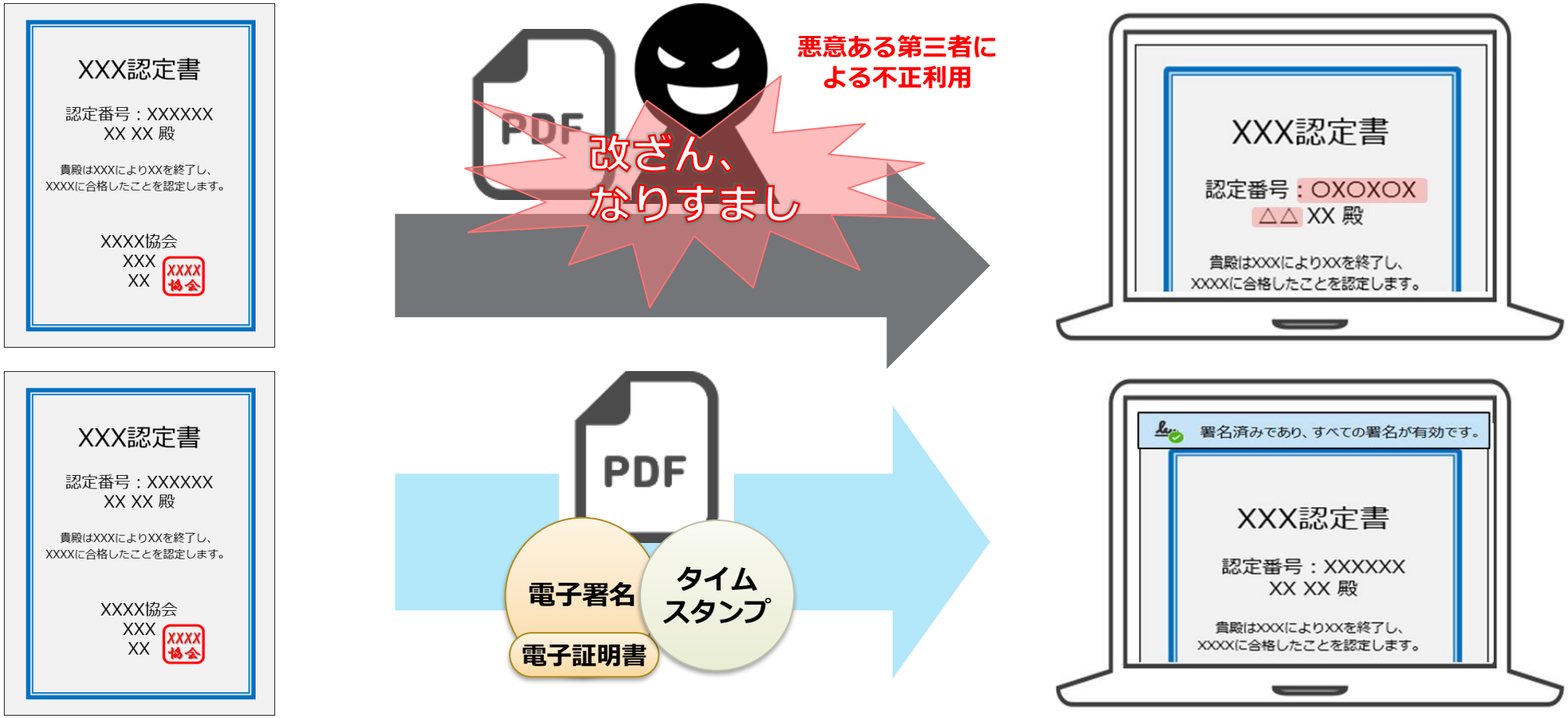
サーバ署名（当事者型）



サーバ署名（事業者型）



電子文書の不正利用リスク対策＝eシール付与



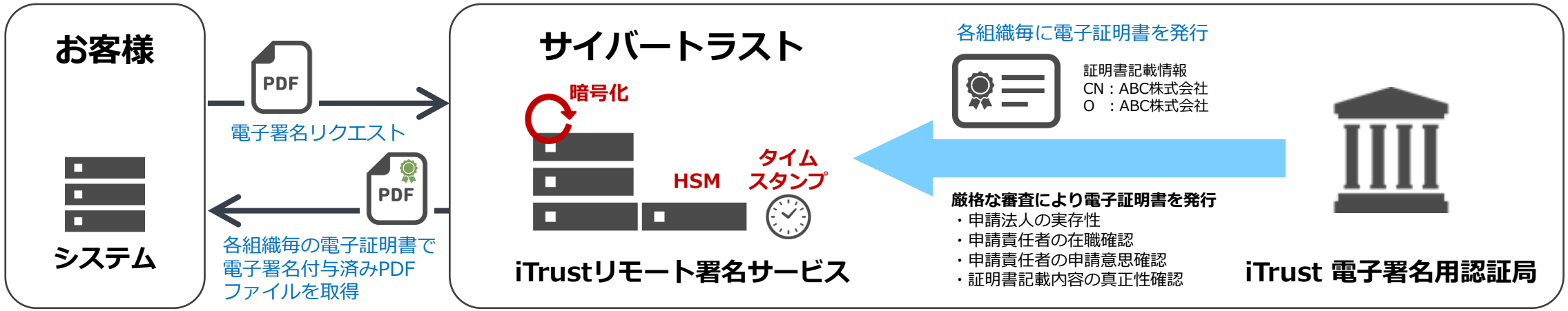
PDFファイルにeシールを付与することで、以下を実現

・誰により発行された電子文書なのか確認できる（発行元証明）

・改ざんされていることを確認できる（改ざん検知）

eシールとは

- eシール： 組織が発行するデータの信頼性確保を目的とし、各組織が取得した電子証明書を使い電子文書へ電子署名を付与すること
- eシールによる信頼性の確保
  - 電子文書の発行元証明　/　改ざん検知

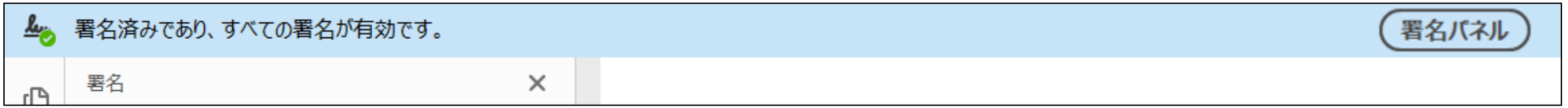


厳格な審査により「なりすまし」ができない組織向け電子証明書で
デジタル署名を付与することで電子文書の発行元証明、改ざん検知を実現

MDP署名により発行元を視覚的に確認

MDP署名を用いることで、署名済みPDFファイルを開いた時点で「署名した電子証明書の組織名や個人名」と「電子証明書を発行した認証局」を視覚的に確認することが可能です。

■一般的な電子署名（ES/ES-T/PAdES）の場合：



■MDP署名の場合：

署名パネルを開かなくても、「署名した電子証明書の組織名/個人名」「電子証明書を発行した認証局」を視覚的に確認が可能

※ MDP署名は、電子署名やタイムスタンプが付与されていないPDFファイルへ付与可能となっております。また、追加の署名/タイムスタンプを付与することができませんので、署名検証期間は最大10年となります。なお、MDP署名の署名レベルはES-Tです。

eシール活用イメージ

発行元証明や改ざん検知が必要なPDFファイルへ幅広く活用が可能

※以下、総務省「eシールに係る指針」を参照（https://www.soumu.go.jp/main_sosiki/joho_tsusin/top/ninshou-law/law-index.html）

契約に紐付いて発生する書類

電子インボイス

- 領収書、請求書、見積書等の契約に紐付いて発生する書類等については、受領側に　おいて、これらの書類が確かにやりとりを行っている相手から送られてきたものであるかを確認した上で、その後の処理を行うことが想定される。

組織等が公開する情報

株主総会資料電子化など

- 各企業のIR関連資料、広報資料等の組織等が外部に公開する情報について、情報を組織等が間違いなく発行したかどうか（発行元の確認）が重要となる。また、悪意のある者によって改ざんされた情報あるいは当該組織等になりすまして作成された情報が流通した場合は、誤った情報が流通することとなり、発行元の組織等の信頼失墜につながりかねない。

組織等が発行する証明書

卒業証明書、廃棄証明書、資格認定証書など

- 各種証明書、各種保証書等の組織等が発行する証明書については、当該証明書の発行者あるいは第三者への提出・提示が必要となる場合がある。例えば、製品の保証書であれば、保証を受ける際に製品の製造元（発行元）への提出・提示が必要となる。また、資格関係の証明書であれば、企業や学校側から提出・提示を求められる可能性がある。

確定情報：総務大臣によるeシール認定制度の設立

総務省主管eシールに係る検討会での決定事項：
「総務大臣によるeシール認定制度の設立」

認定eシール：国が認定した認証局から発行した組織向け証明書を利用したデジタル署名

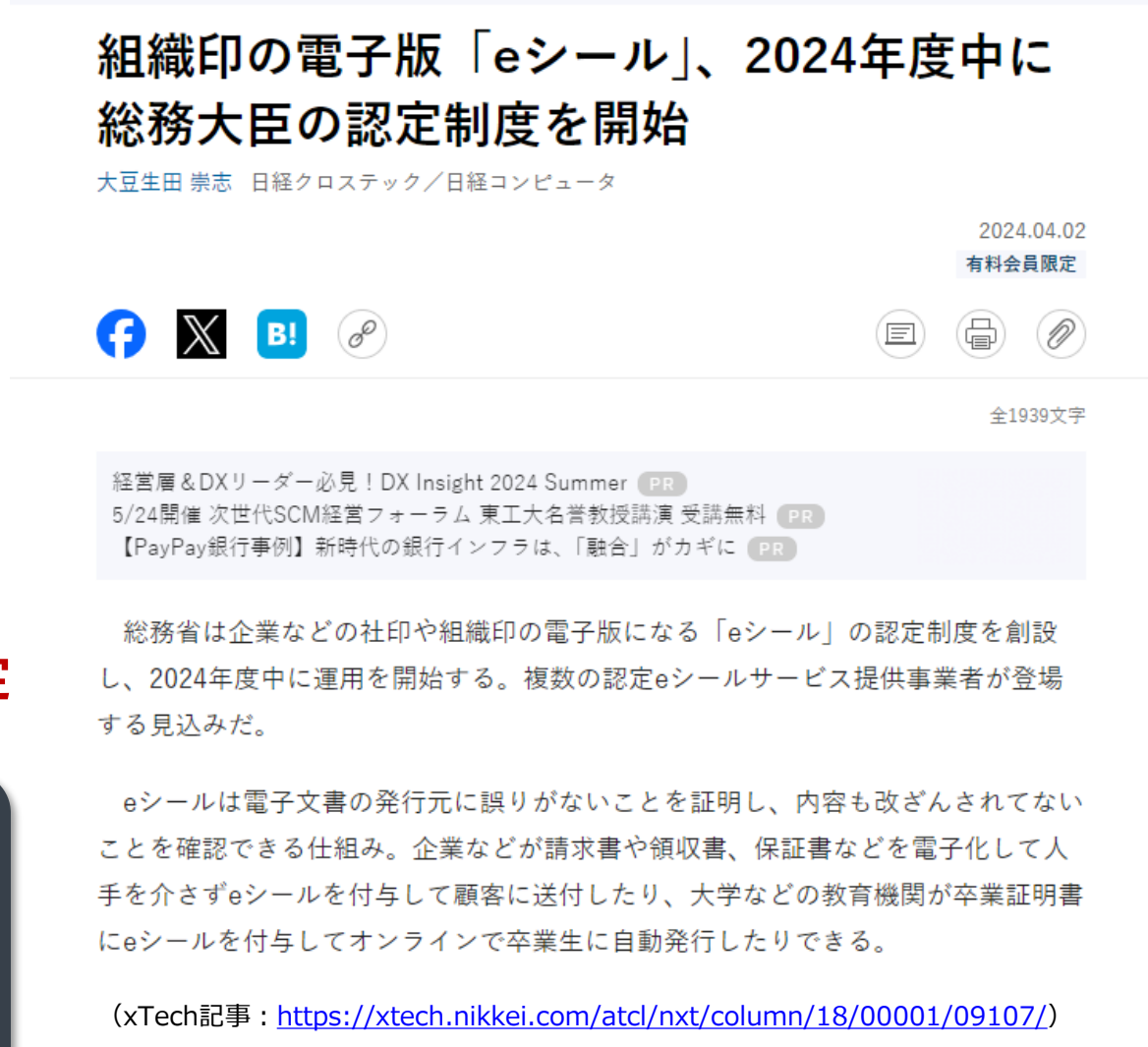
■今後の想定

個人の特定：マイナンバーカード

組織の特定：eシール

サイバートラスト：2025年中認定eシール提供予定

**2025年度以降、行政/自治体でデータ信頼性確保が必要な各種要件に「eシール要件」が含まれることが想定されます。
国での推進により民間企業でのeシール活用の市場が伸びる想定です。**



組織印の電子版「eシール」、2024年度中に総務大臣の認定制度を開始

大豆生田 崇志　日経クロステック／日経コンピュータ

2024.04.02

有料会員限定

全1939文字

総務省は企業などの社印や組織印の電子版になる「eシール」の認定制度を創設し、2024年度中に運用を開始する。複数の認定eシールサービス提供事業者が登場する見込みだ。

eシールは電子文書の発行元に誤りがないことを証明し、内容も改ざんされてないことを確認できる仕組み。企業などが請求書や領収書、保証書などを電子化して人手を介さずeシールを付与して顧客に送付したり、大学などの教育機関が卒業証明書にeシールを付与してオンラインで卒業生に自動発行したりできる。

（xTech記事：https://xtech.nikkei.com/atcl/nxt/column/18/00001/09107/）

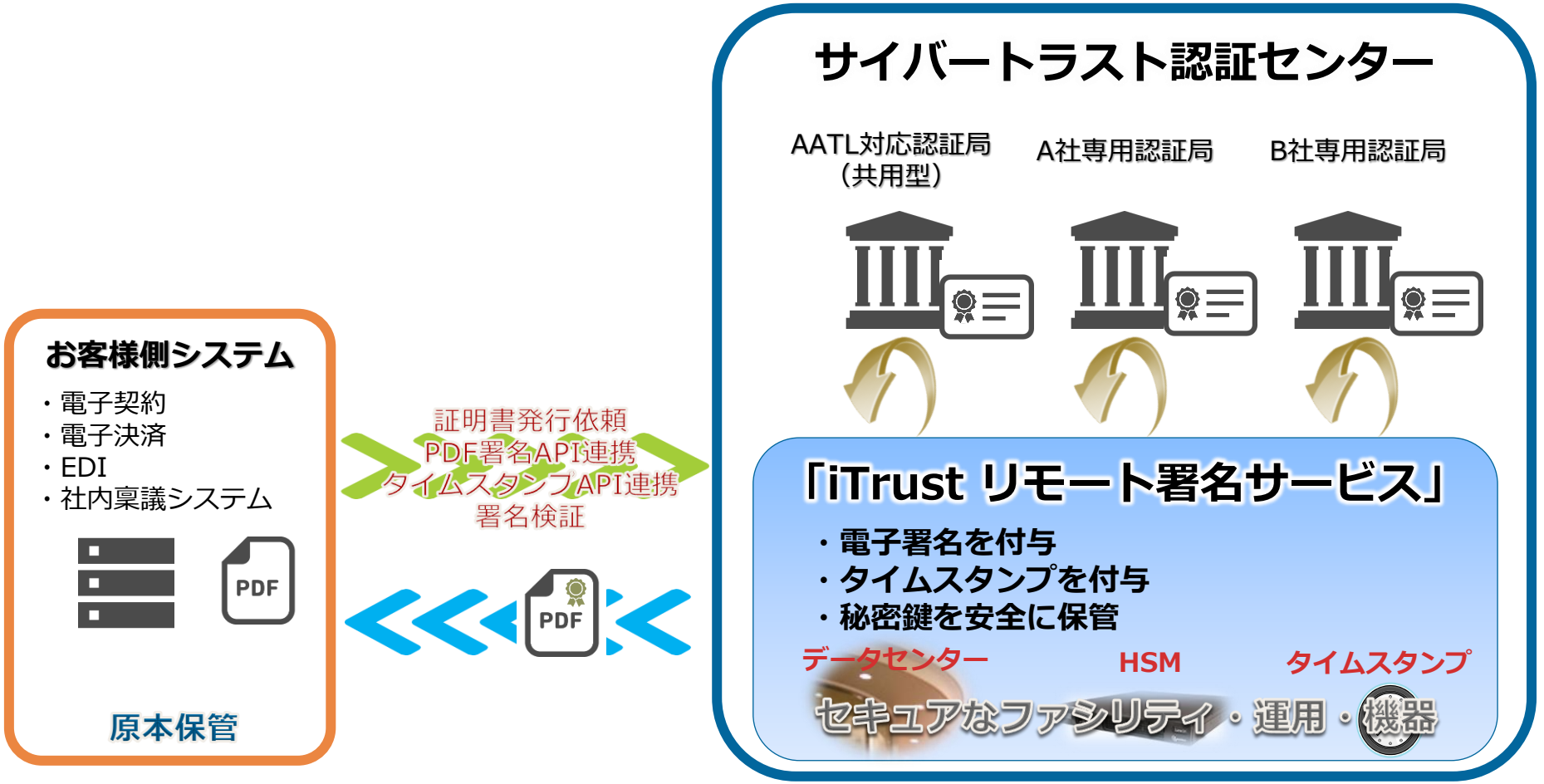
「iTrust リモート署名サービス」とは…

「iTrust リモート署名サービス」は、電子証明書をセキュアに保管し、
長期署名に対応した電子署名やタイムスタンプ機能をAPIで提供するクラウドサービスです。

**電子化された文書（電磁的記録）に対して、
「誰」が「何」を「いつ」の証明を長期に保障します。**

iTrust リモート署名サービス システム構成

cybertrust



認定タイムスタンプ
利用登録

認定タイムスタンプを利用する事業者として登録

https://www.dekyo.or.jp/touroku/contents/repository/index.html

JTSR
JIPDEC Trusted Service Registration

JIPDEC

JIPDECトラステッド・サービス登録

https://www.jipdec.or.jp/project/jtsr/tl/isp54l0000000rec-att/Cybertrust_Japan_Co_Ltd_JTS.pdf

お客様システムとはAPIで連携し、弊社認証局サービスとは内部連携のうえ、電子署名・タイムスタンプの付与を、サーバサイドで実現します。

iTrust リモート署名サービスの特徴

ポイント１：　事業者様が安心してご利用可能な署名インフラ基盤

クラウドHSM、電子署名、認定タイムスタンプをREST-APIにてワンストップでご提供します。
複数の電子署名形式（ES/ES-T/MDP/ES-A）に対応し、管理画面の提供により、監査に必要な
ログの閲覧、検索が可能です。

ポイント２：　事業者様の運用負荷軽減

署名インフラ基盤をクラウド環境にて、本番用、開発用など柔軟にご提供します。
リモート署名サービスを利用することで、事業者様サービスの短期間でのリリースが可能です。
また、運用中に発生する署名機能開発・保守から解放されることで自社サービス開発に専念できます。

ポイント３：　厳格な運用管理

秘密鍵は、日本国内の電子認証センター内のHSM（FIPS 140-2 Level 3準拠）で安全に保護し、
証明書発行対象者のみが電子署名のために利用できるよう厳格に管理されています。
一般財団法人日本情報経済社会推進協会（JIPDEC） の厳格な基準に基づく審査を実施しており、
「JIPDEC トラステッド・サービス（リモート署名（電子契約））」として国内第一号登録となります。

iTrustリモート署名サービス ご提供機能

API連携

- RESTインターフェースによるAPI連携
- 接続用証明書によるセキュアな認証
- 署名対象データは、通信経路上暗号化を行う。

PDF署名＆タイムスタンプ付与

- 電子署名の署名アルゴリズムは、SHA-2対応
- PAdESに対する再度のタイムスタンプ付与も可能
  ※10年以上の電子的記録の保管
- 電子署名時に印影イメージを付与が可能

PDF署名検証

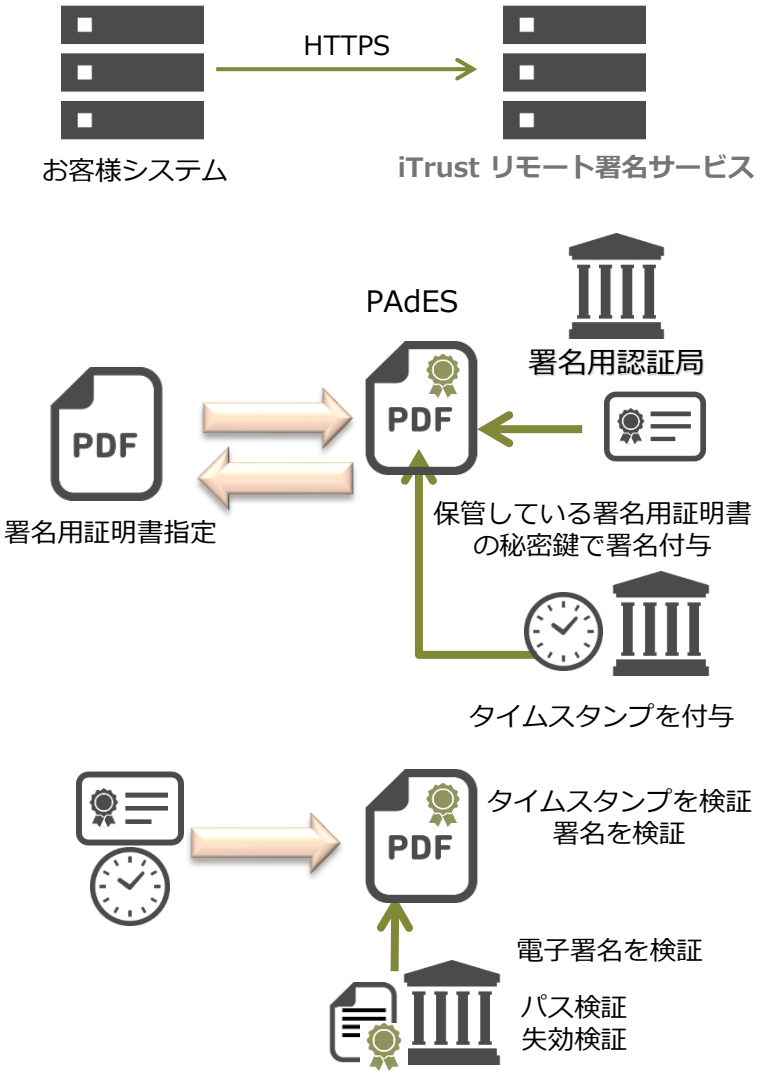
- 指定された電子署名／タイムスタンプの署名検証を実施

トランザクションログ

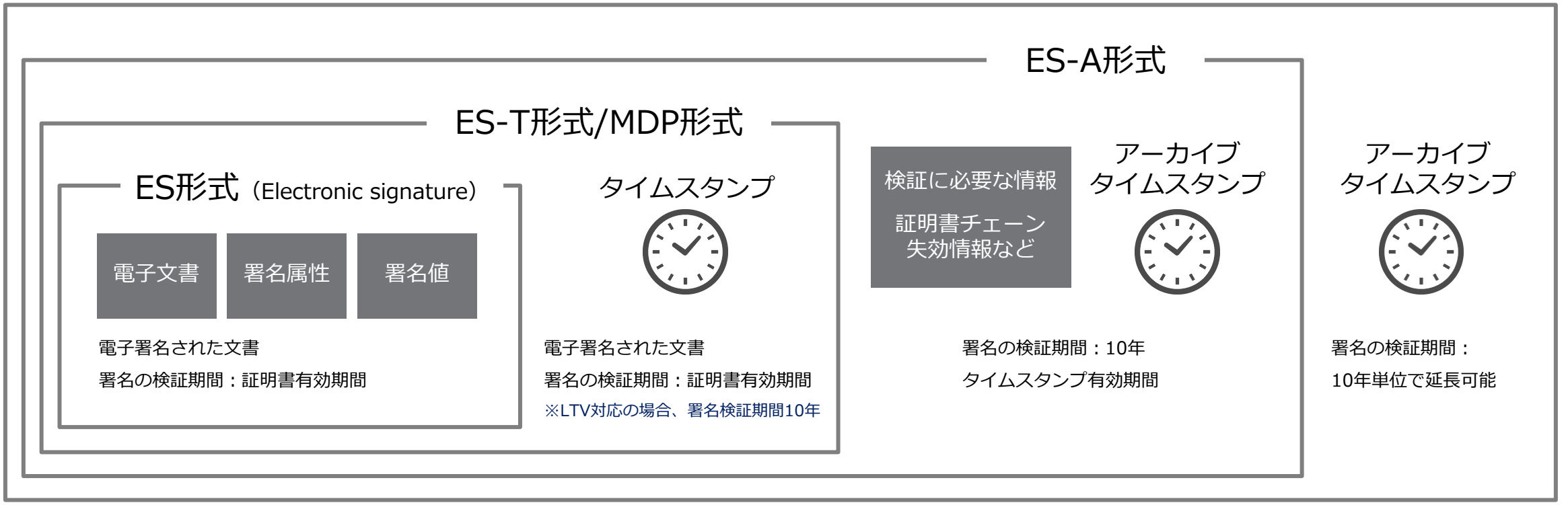
- 署名／署名検証のトランザクションログを記録

管理者向け画面

- 署名ログ一覧の検索、PDF署名検証が可能な管理画面
- 「iTrust 電子署名用証明書」のCSR作成や証明書登録・署名機能
  ※署名データの保管は行いません。



電子署名の形式と署名検証の有効期間

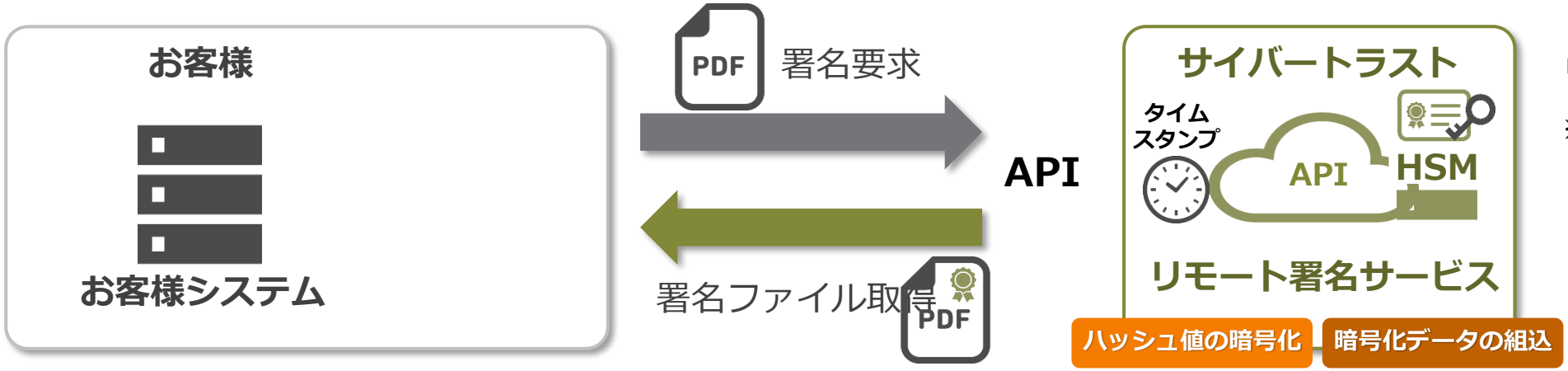


iTrustリモート署名サービスご提供形式

・ タイムスタンプなし電子署名	（ES型式）	PDF	XML
・ タイムスタンプあり電子署名（LTV）	（ES-T型式）	PDF	XML
・ タイムスタンプあり電子署名（LTV）	（MDP形式）	PDF	
・ 長期署名（PAdES/XAdES）	（ES-A型式）	PDF	XML
・ タイムスタンプのみ付与		PDF	

リモート署名サービス 署名方式

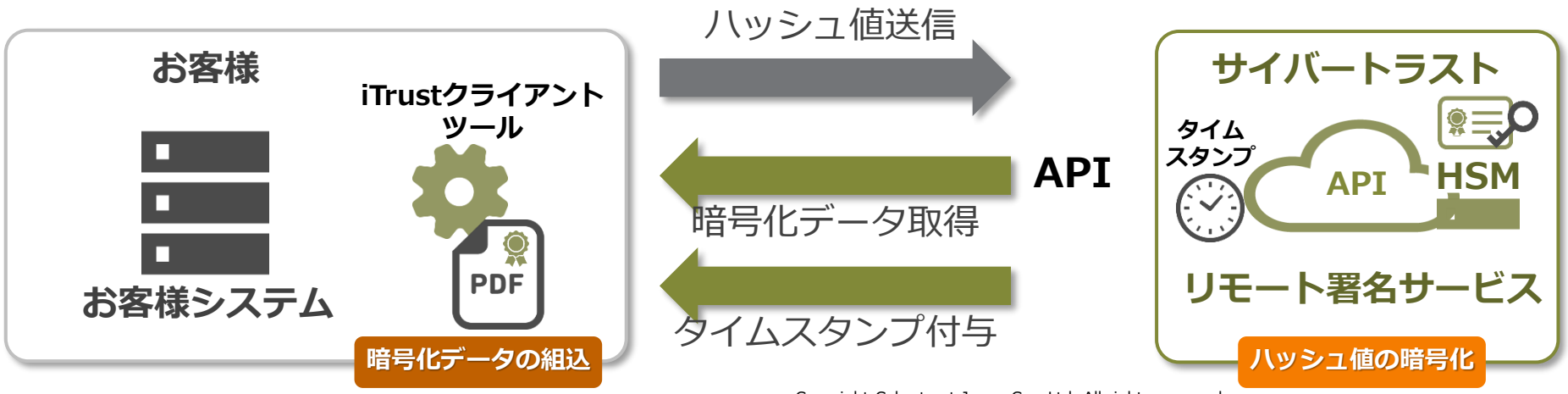
PDFファイル署名方式（REST API）



■メリット
・送信データがPDF（Base64）
※すぐ連携可能、短期導入の実現

■デメリット
・リクエストデータ60M以内

ハッシュ署名方式（クライアントツール＋REST API）



■メリット
・送受信データがハッシュ値
※ファイルサイズ200Mまで
（ハッシュ化ファイルは約43KB）
※大容量ファイル/大量データも可

・他サービスでの署名済PDFも検証可

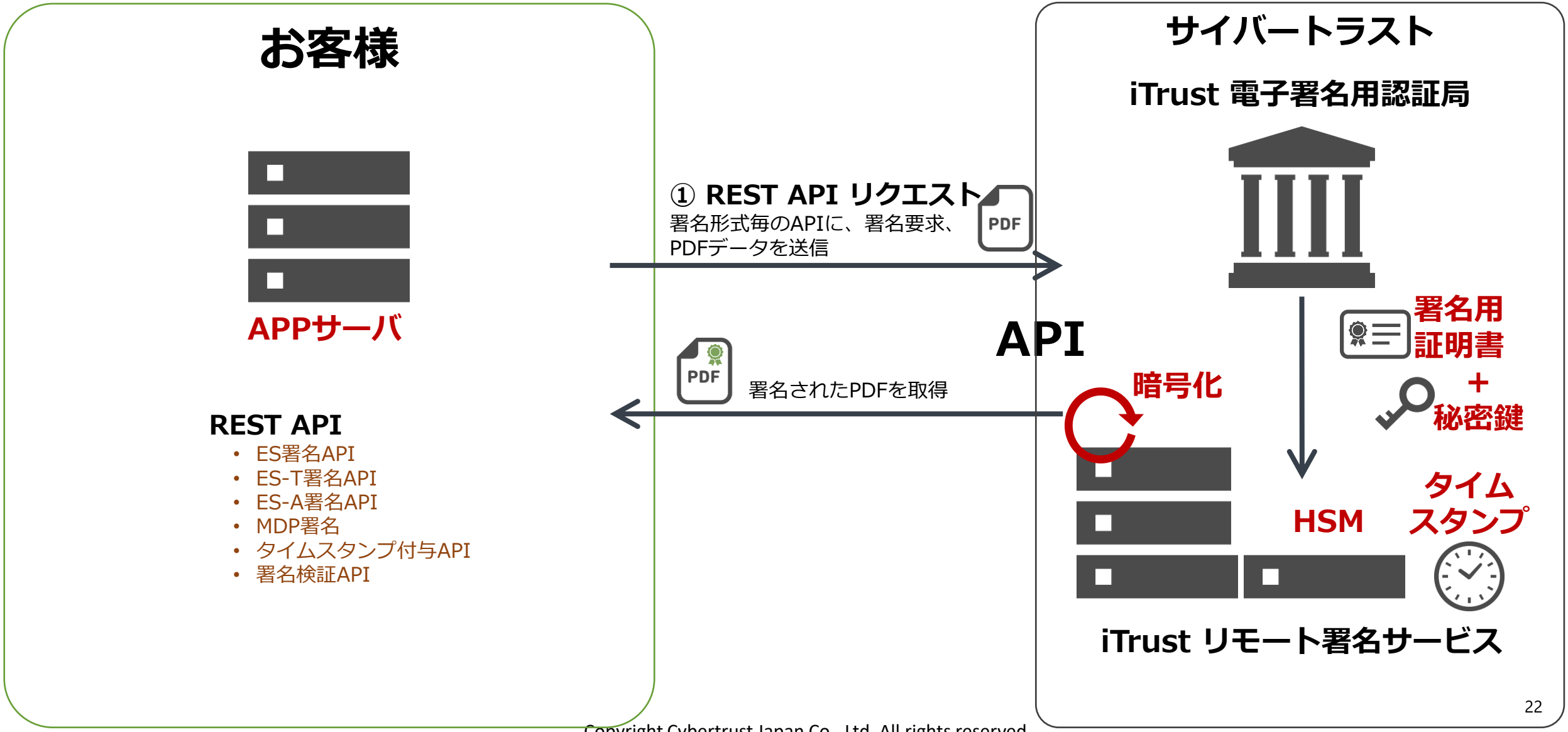
iTrust リモート署名サービス各方式比較

方式	APIのみ利用	クライアントライブラリ	クライアント アプリケーション	クライアントプロキシ	クライアントライブラリ for XAdES
対象ファイル	PDF	PDF	PDF	PDF	XML
仕様	API	アプリ組込用ライブラリ	Javaアプリ （スタンドアロン）	AWS専用アプリ	アプリ組込用ライブラリ
インターフェイス	REST API	Java API	コマンドラインI/F	REST API	Java API
APIへの最大同時接続数	10	30	30	30	30
オートスケール対応	○	○	○	○	○
リクエスト最大サイズ	60MB	200MB	200MB	200MB	200MB
開発工数	低	高	中	中	高
実行環境	-	**開発環境** 開発言語：Java JDK：OpenJDK 17（動作確認はAmazon Corretto 17にて実施） **実行環境** OS：CentOS Linux release 7.x 64bit / Red Hat Enterprise Linux 8.x 64bit / Amazon Linux release 2 64bit WindowsServer 2022/2019/2016 64bit	**実行環境** JRE：OpenJDK 17（動作確認はAmazon Corretto 17にて実施） OS：CentOS Linux release 7.x 64bit / Red Hat Enterprise Linux 8.x 64bit / Amazon Linux release 2 64bit WindowsServer 2022/2019/2016 64bit	AWS ECS上で動作する コンテナイメージをご提供	**動作環境** 開発言語： Java JDK： OpenJDK 17 （※動作確認は、Amazon Correto17にて実施）
通信データサイズ	署名するPDFファイル サイズに依存	1 KB未満 ハッシュ値/署名値 タイムスタンプ	1 KB未満 ハッシュ値/署名値 タイムスタンプ	1 KB未満 ハッシュ値/署名値 タイムスタンプ	1 KB未満 ハッシュ値/署名値 タイムスタンプ
その他		システムをJavaで開発している場合、性能的にお薦め	システムをJava以外で開発している場合、スクリプトなどで裏側バッチ的に動かす場合にお薦め		

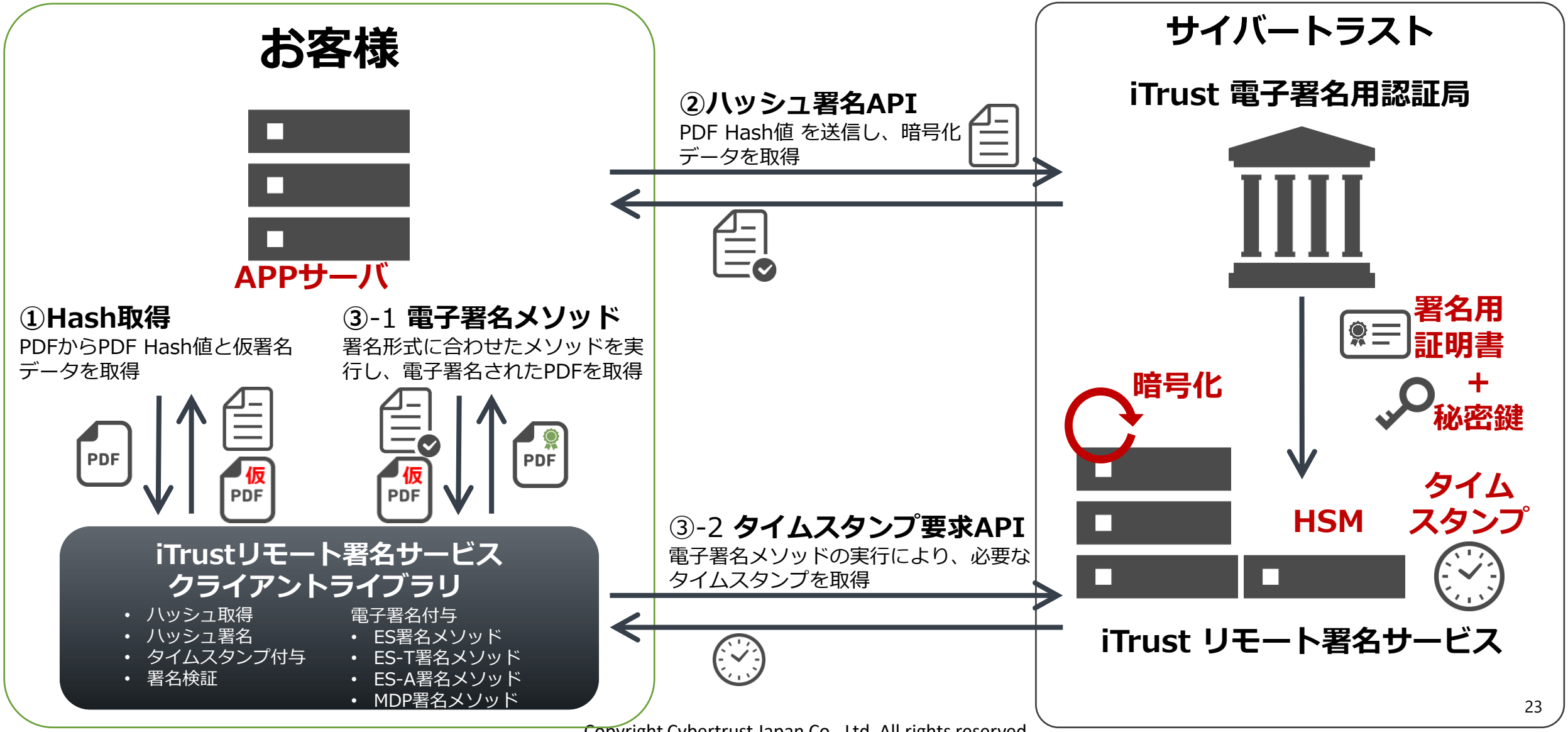
リモート署名サービス API一覧

	処理項目	概要	課金対象				
			RestAPI	クライアント ライブラリ	クライアント アプリ	クライアント プロキシ	XAdES ライブラリ
1	証明書登録	サイバートラスト マネージドPKIで作成された電子署名用証明書を本サービスに登録 ※「iTrust 電子署名用証明書」では利用しません。		–	–	–	–
2	証明書チェーン取得	RSクライアントライブラリ利用時に証明書チェーン取得	–	–	–	–	–
3	ES署名	PDFドキュメントへの電子署名付与(ES形式)を申請/取得 ※署名した時刻は、Siningtime形式を付与	○	–	○	○	○
4	ES-T署名	PDFドキュメントへの電子署名付与(ES-T形式)を申請/取得	○	–	○	○	○
5	MDP署名	PDFドキュメントへの電子署名付与(ES-T形式)を申請/取得（一方向署名のみ） ※署名用証明書のサブジェクトが Acrobat Reader 上で強調表示されます	○	–	○	○	–
6	ES-TL署名	PDFドキュメントへの電子署名付与(ES-X Long形式)を申請/取得	–	–	–	–	○
6	ES-A署名	PDFドキュメントへの電子署名付与(ES-A形式)を申請/取得	○	–	○	○	○
7	タイムスタンプ付与	PDFドキュメントへのタイムスタンプ付与を申請/取得	○	○ ※1	○	○	○
8	ハッシュ署名	ハッシュ値への電子署名付与を申請/取得	○	○ ※1	–	–	–
9	署名検証	ドキュメントに付与された電子署名をサーバ側で検証		–	–	–	–
10	メンテナンス確認	サービスがメンテナンス中であるかどうかを返却		–	–	–	–

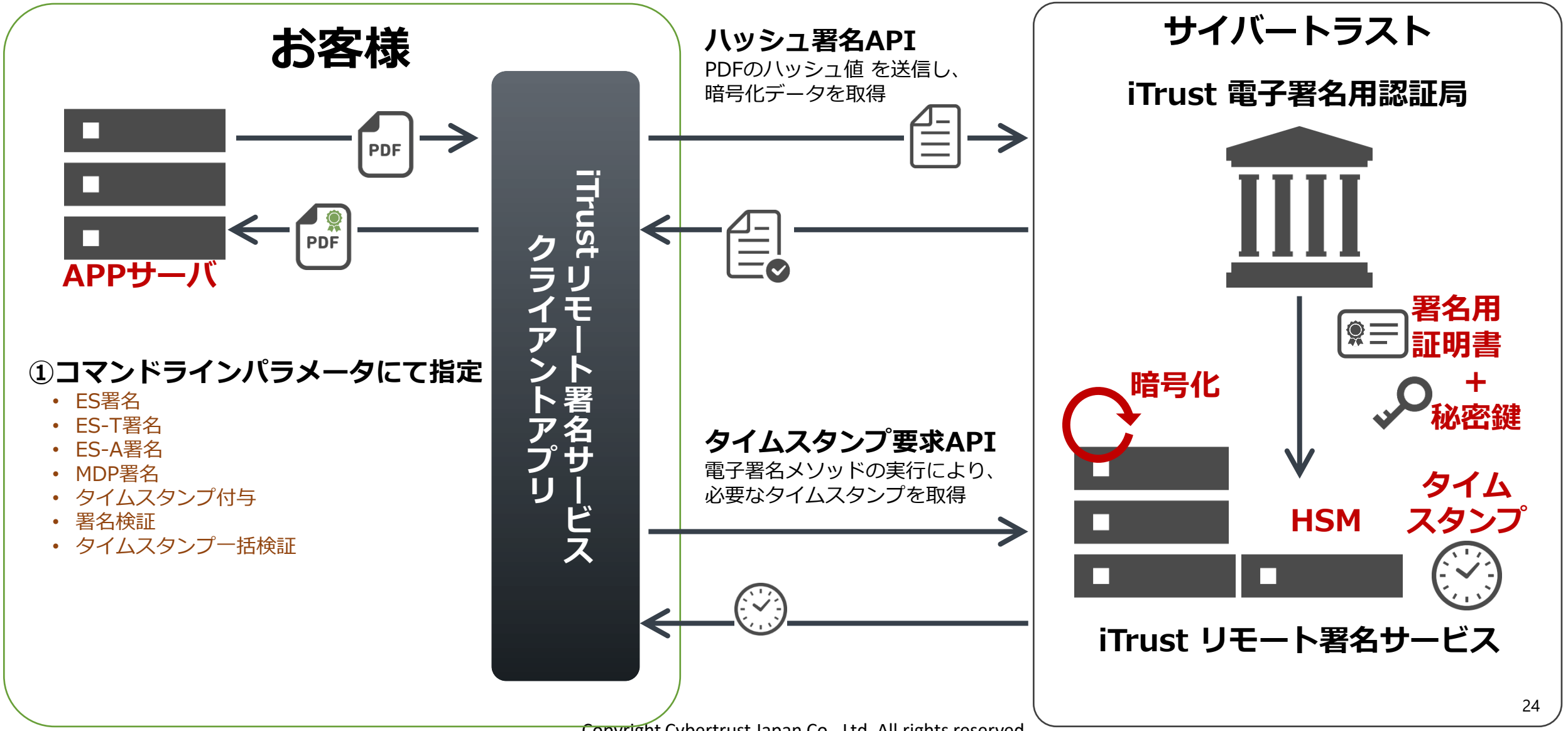
各APIを利用したリモート署名



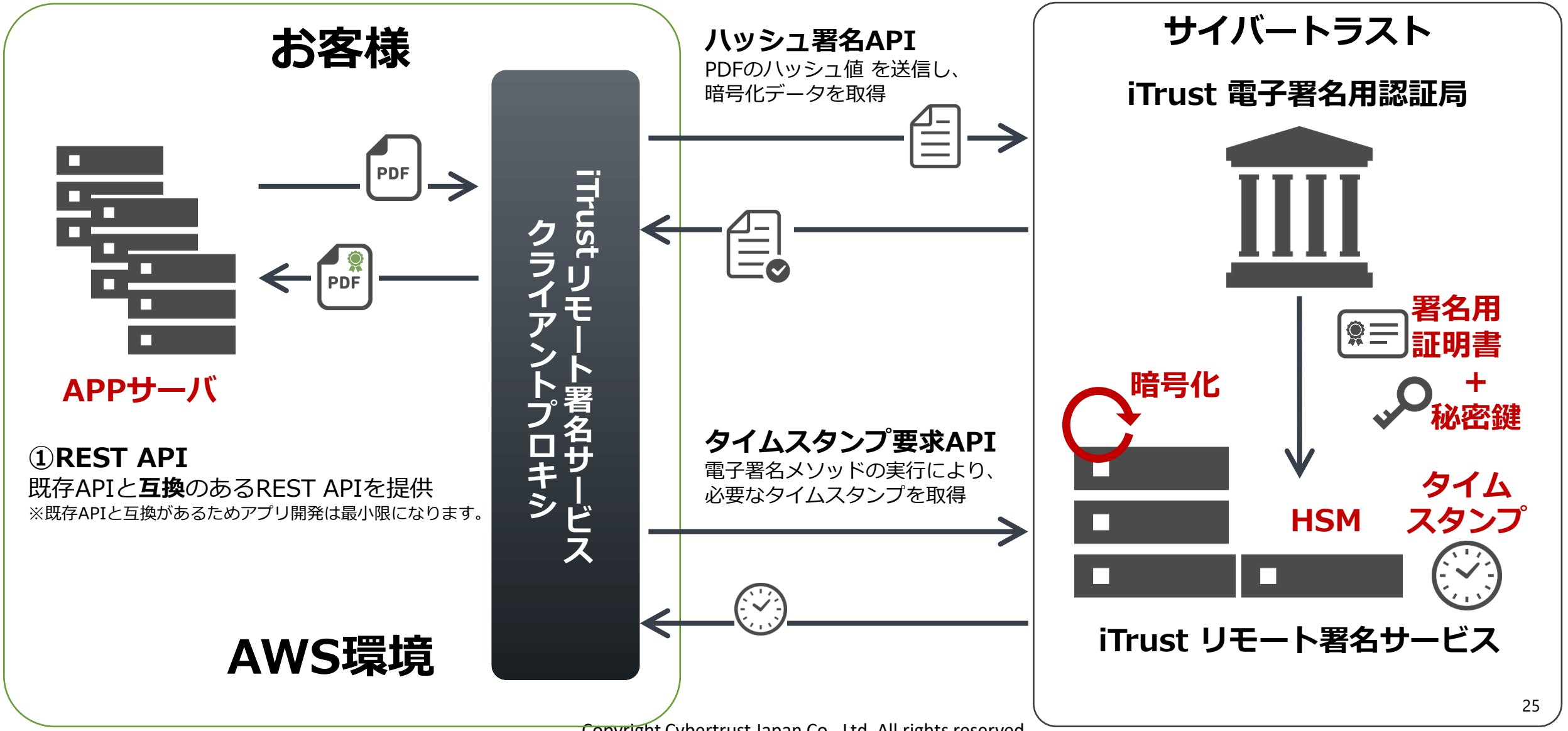
クライアントライブラリによるHash署名イメージ



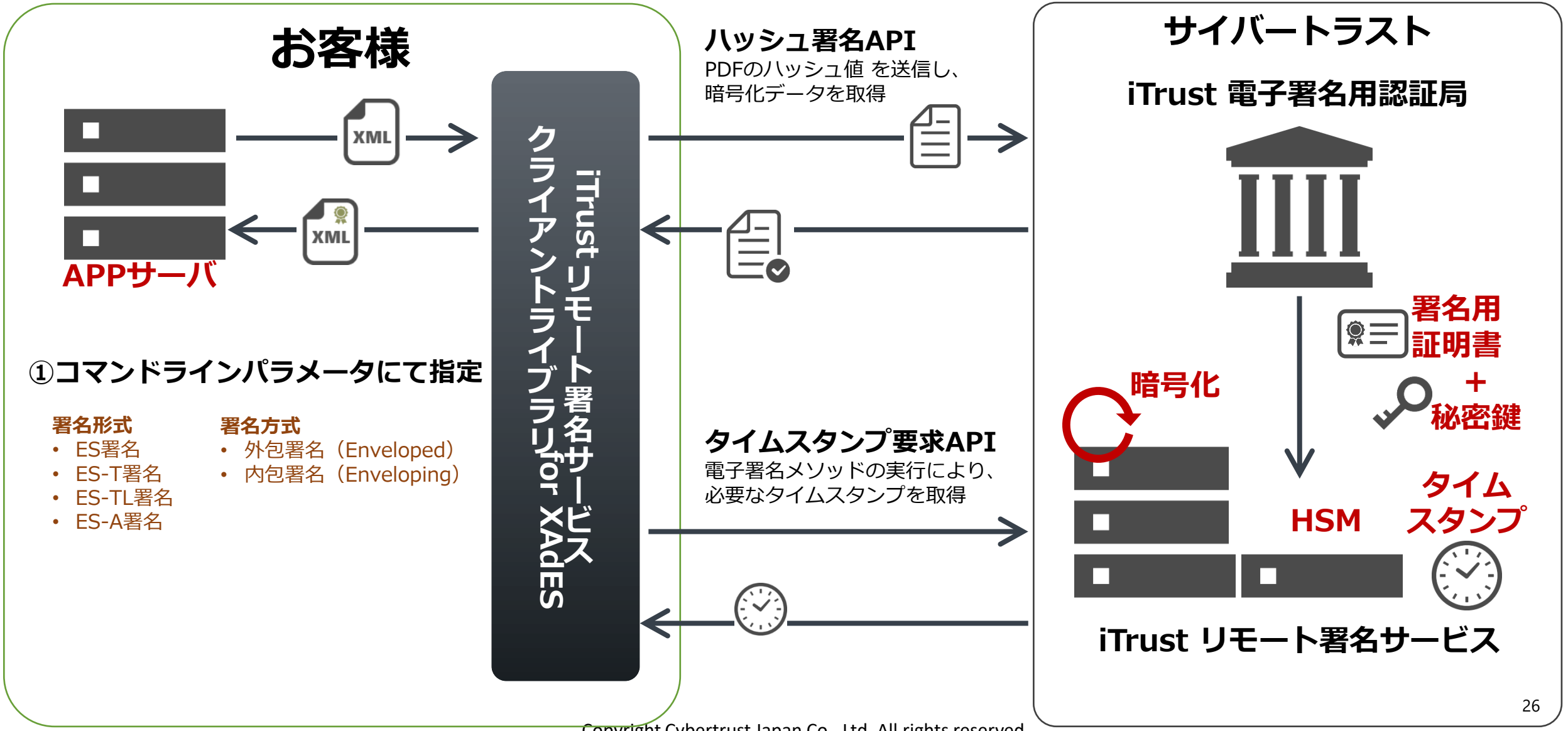
クライアントアプリによるHash署名イメージ



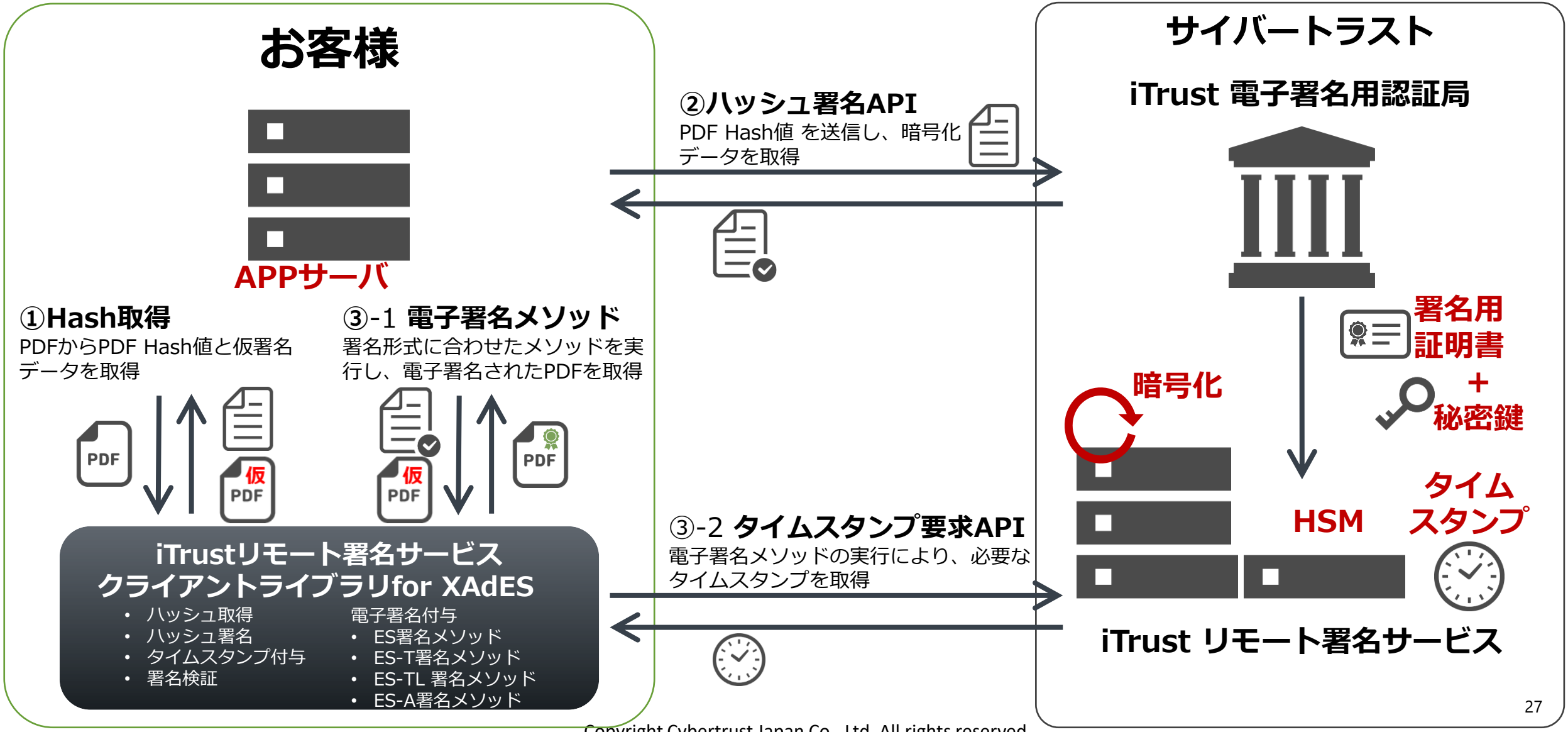
クライアントプロキシによるHash署名イメージ



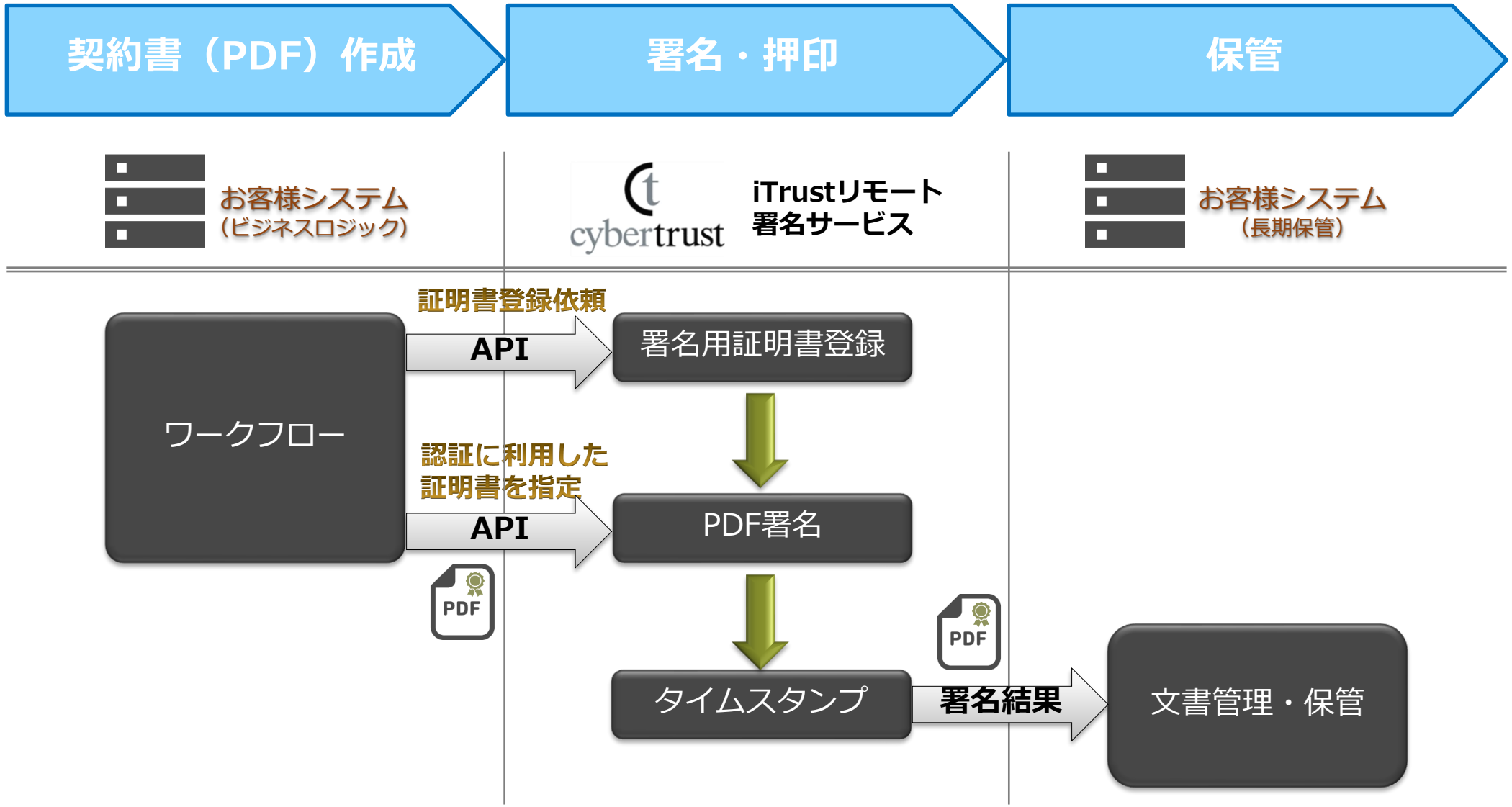
クライアントライブラリ for XAdESによるHash署名イメージ



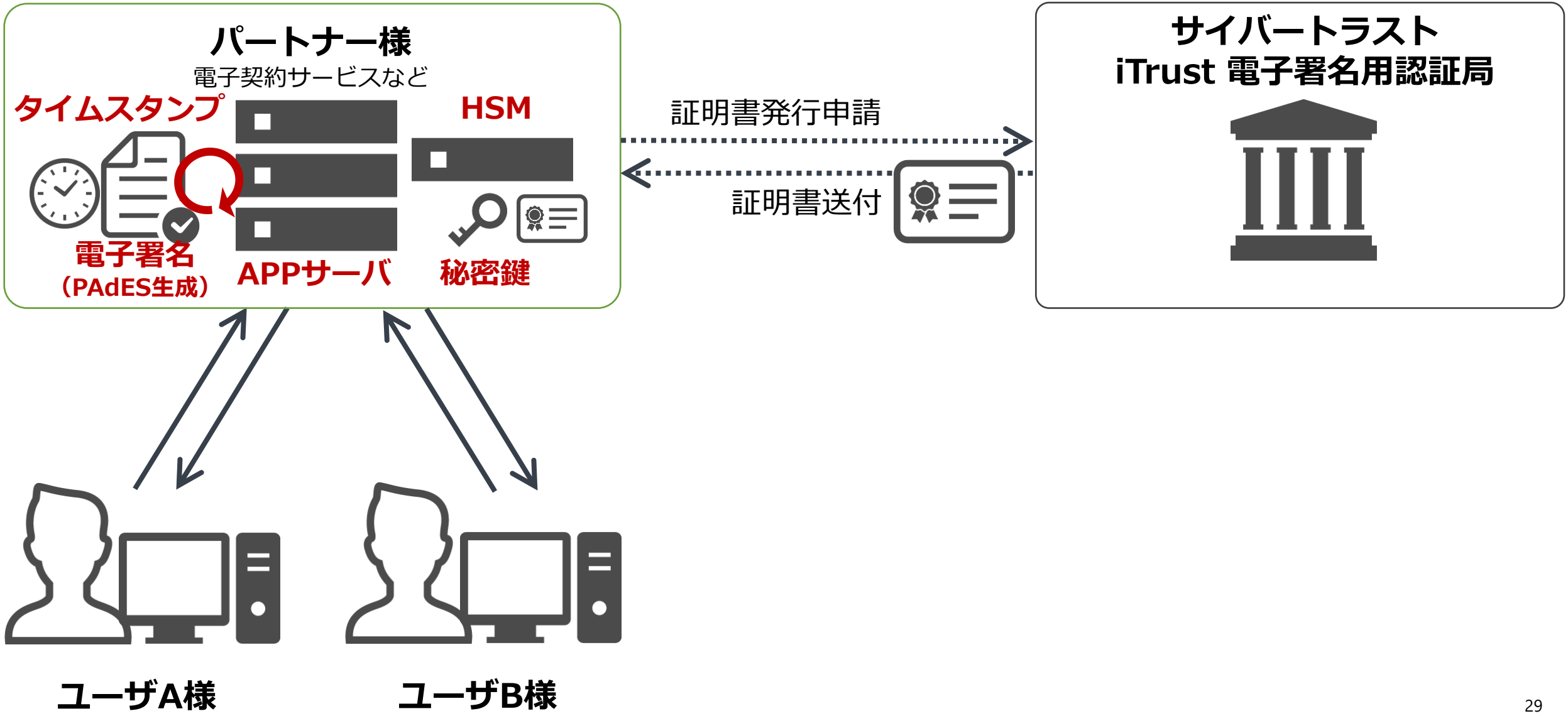
クライアントライブラリ for XAdESによるHash署名イメージ



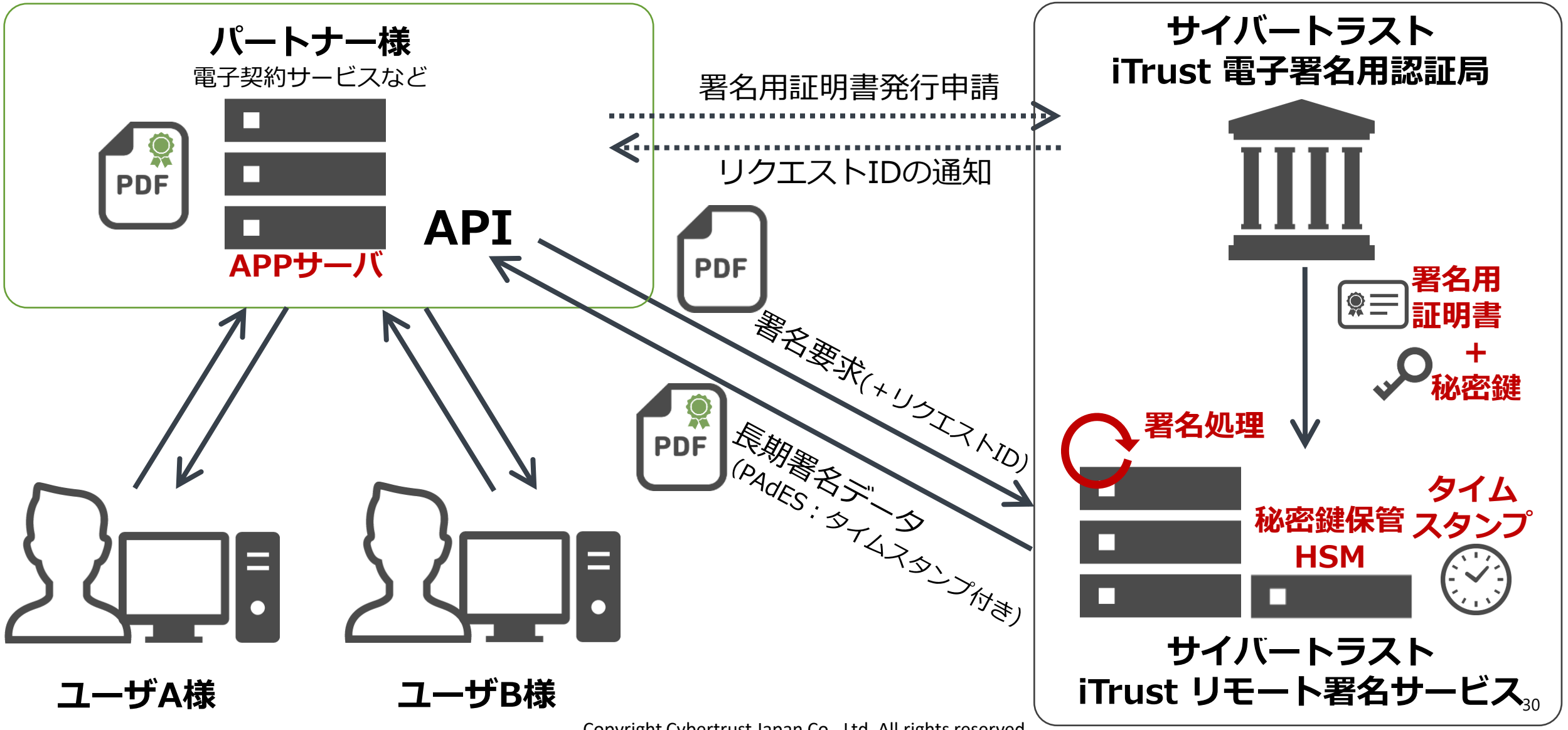
参考例：電子契約システム構成



ご利用イメージ：電子署名用証明書のみ利用



ご利用イメージ：電子契約サービスでのリモート署名サービス



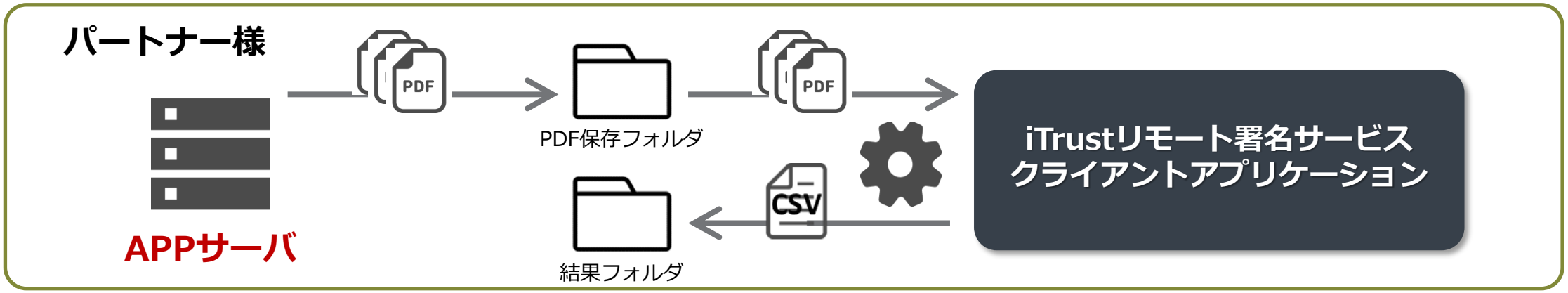
ご利用イメージ：電帳法対応 一括署名検証での活用

リモート署名サービス クライアントアプリケーション一括署名検証機能の活用

クライアントアプリケーション一括署名検証機能は、バッチ実行により指定フォルダへ保存した複数PDFファイルの署名検証結果をCSVで一括出力します

出力項目：検証結果（有効/無効/対象外/不明）/署名時刻/有効期間の開始/有効期間の終了/総務大臣認定済など

- 出力情報の対象は、タイムスタンプのみ（電子署名は対象外）
- 複数タイムスタンプが付与されている場合にはタイムスタンプごとに情報を出力



出力イメージ（Excelで表示した場合）

ファイル名	検証結果（有効/無効/対象外/不明）	検証結果理由	検証時刻	署名フィールド名	TS証明書のサブジェクト
timestamp-sample.pdf	有効		2023/10/6 10:35	Signature1	CN=AMANO-TSU-T2P2-1, OU=nShield TSS ESN:1720-8531-E357, OU=e-timin
timestamp-sample2.pdf	有効		2023/10/6 10:35	Signature1	CN=AMANO-TSU-T2P2-1, OU=nShield TSS ESN:1720-8531-E357, OU=e-timin

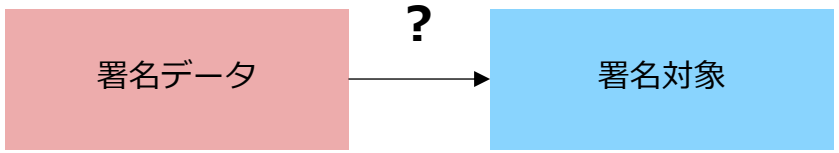
iTrustリモート署名サービス XAdES対応

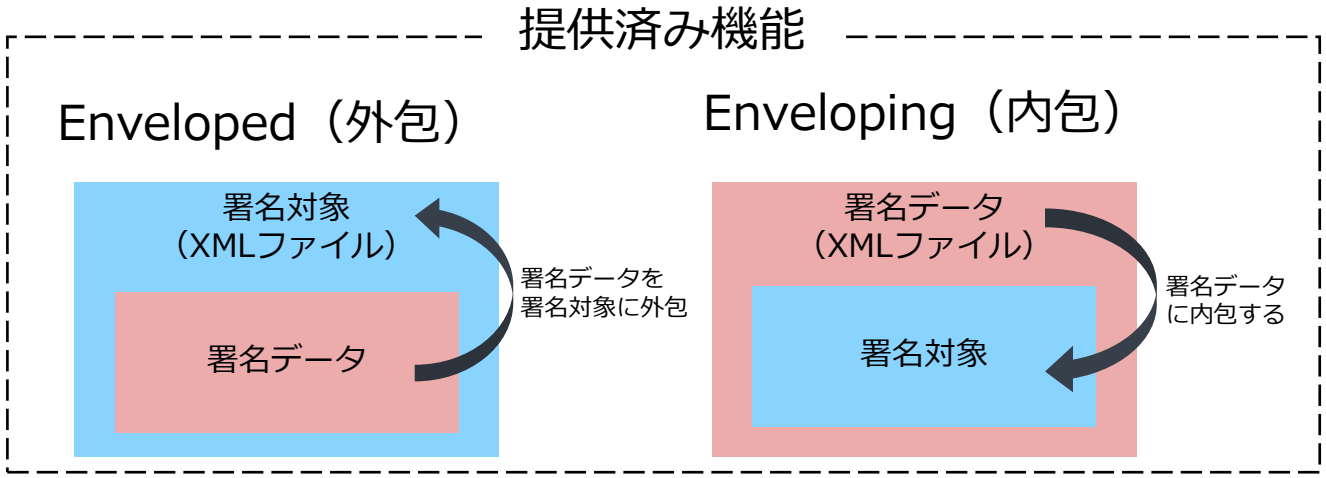
- **クライアントライブラリ for XAdESを提供**
  - 主な機能
    - XAdES形式の署名（内包形式、外包形式）を提供
      - 内包形式：XMLファイルを作成し内部に署名対象ファイルを格納して署名
      - 外包形式：XMLファイルへ対する署名
  - 動作環境
    - Java 17
  - 以下の機能は、今後のロードマップにて対応予定
    - 署名検証機能
    - Detached形式：外部のファイルを参照し署名

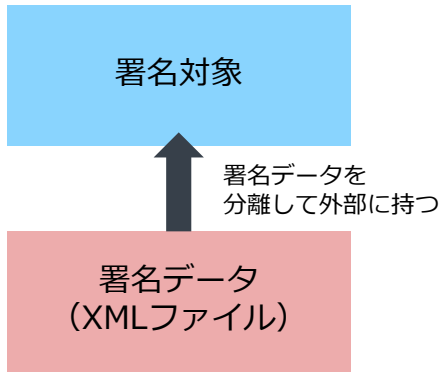
XAdESの形式とは

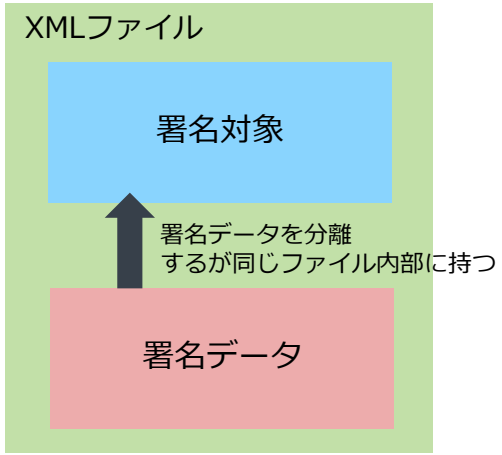
- **XAdESの参照形式**
  - Enveloped（外包）
  - Enveloping（内包）
  - 外部Detatched
  - 内部Detatched

→署名データと署名対象の関係性によって呼び方が異なり、署名値の生成規則も異なります。



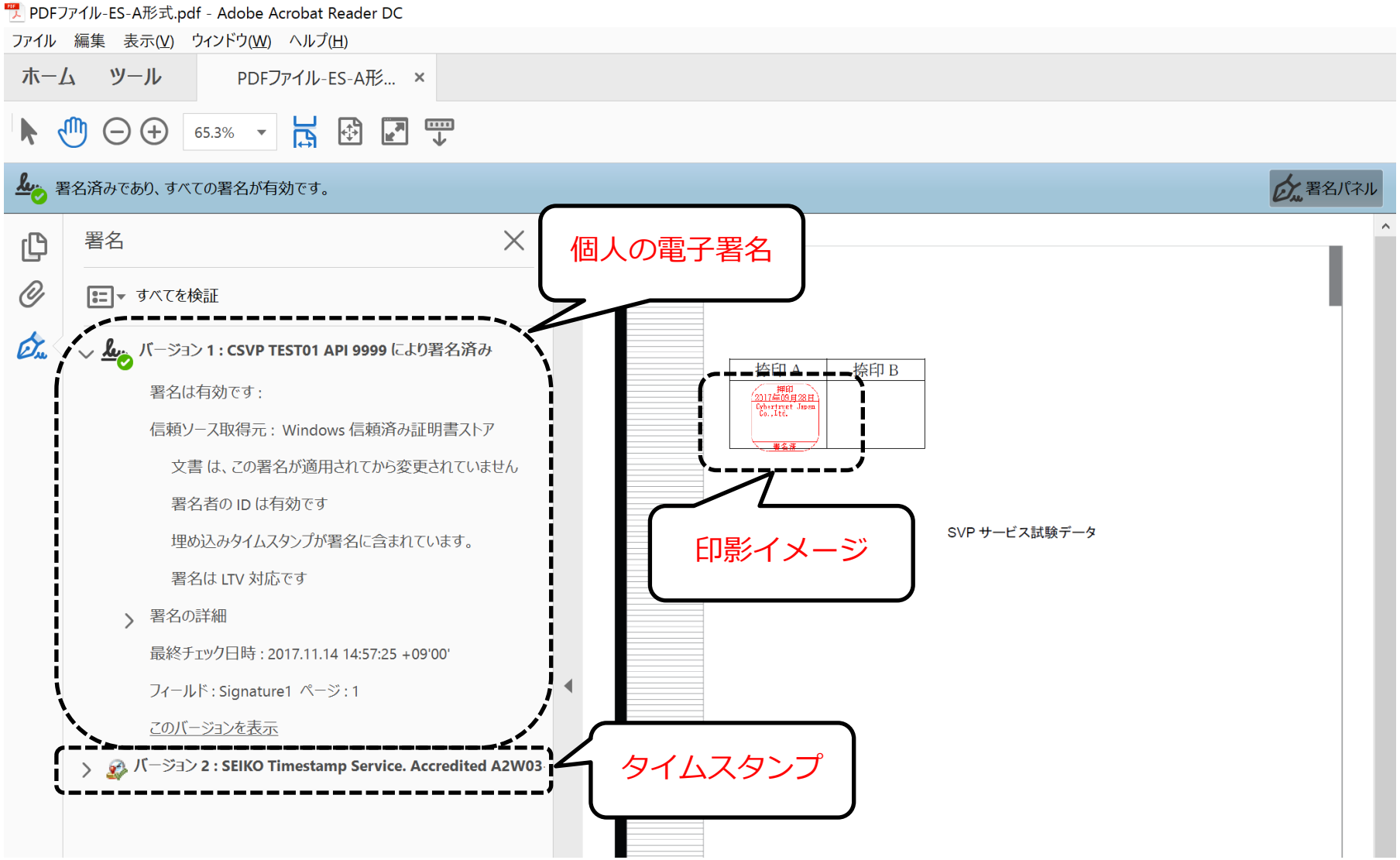






Appendix

【Appendix.1】Acrobat Reader DCでのPAdES表示画面



【Appendix.2】セキュリティ基盤

「WebTrust EV Program監査基準」・「WebTrust for CA監査基準」

- 第三者認証機関として、毎年認証事業者に課せられる監査基準としてグローバルスタンダードなWebTrust監査を、毎年取得しています。※1

「JIPDEC トラステッド・サービス登録（リモート署名（電子契約））」

- 一般財団法人日本情報経済社会推進協会（JIPDEC） の厳格な基準に基づく審査を実施し、厳格な規程をもって運用されているリモート署名サービスとして、国内で初めて登録が完了し、お客様は安心して電子契約など書面の電子化におけるリモート署名を利用可能になります。

「ISO/IEC27001（ISMS）」 = サイバートラスト

- サイバートラストは、情報セキュリティサービスを提供する企業として、全社でのISO/IEC27001（ISMS）認定を取得し、お客様に安心してサービスをご利用頂けるよう、内部管理体制を整備しております。

※1：WebTrust とは、米国公認会計士協会およびカナダ勅許会計士協会が共同で開発・管理運営している認定制度です。事業者が国際的な電子商取引保証規準に基づいた電子商取引を行なっているかを審査するサービスです。マイクロソフト社をはじめとする各種ウェブブラウザの「信頼されたルート証明機関」に登録されるための要件の一つともなっています。

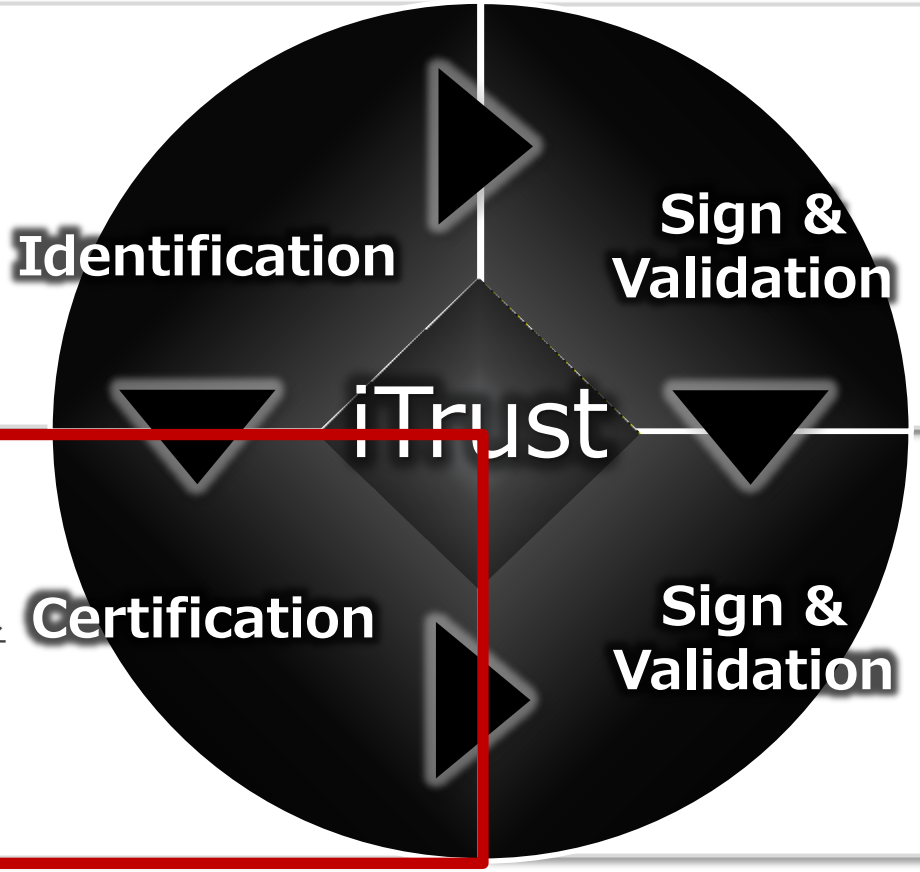
iTrust サービス　～ DXに必要なトラストサービス基盤 ～

cybertrust

cybertrust iTrust
Identification & Trust

本人確認サービス

- 公的個人認証のプラットフォーム事業者として主務大臣認定を取得
- 本人確認、所在確認や生存確認などの現況確認が可能
- 犯罪収益移転防止法およびその運用で求められる要件に対応
- IC免許証や在留カードの真贋判定



電子委任状サービス（検討中）

- 電子委任状法に則ったサービス
- 電子委任状取扱事業者として、総務大臣認定の取得を検討中
- 企業間の電子契約における委任関係を第三者機関として保証

電子署名用証明書

- 電子署名用途専用認証局として国内で初めてWebTrust監査に合格
- 個人（自然人）と法人の 2種類の電子署名用証明書を発行
- AATL：Adobe Approved Trust List に登録され安全性を視覚的に確認可

リモート署名サービス

- 認証設備内で管理された秘密鍵によるクラウド署名サービス
- 長期署名（PAdES：PDF Advanced Electronic Signatures）に対応
- 日本情報経済社会推進協会：JIPDEC JCANトラステッドサービス登録済

iTrust 電子署名用証明書の概要

**iTrust 電子署名用証明書は、WebTrust監査に合格し、
Adobe Acrobatに「信頼される署名」としてルート証明書が登録された、
信頼性の高いAATL対応電子署名用証明書です。**

法人向け電子署名用証明書
iTrust Digital Signature Certificated for Legal Person

法人の実在性確認を行い、法人名が記載される法人向けの
電子署名用証明書です。社印のような使い方をする場合には、
こちらを選択頂けます。

個人向け電子署名用証明書
iTrust Digital Signature Certificate for Natural Person

個人の本人確認を行い、個人名が記載される個人向けの
電子署名用証明書です。従業員個人向け、一般コンシューマ
向けなど個人での利用は、こちらを選択頂けます。

eシール用証明書
iTrust Digital Signature Certificated for e-Seal

eIDAS 規則でのeシール定義を参考に日本の各種機関が
日本版eシールとして作成したガイドラインを基に、JIPDECが
定義したeシールの基準を網羅したeシール専用証明書です。

証明書有効期間：　1年、　2年、　3年

※ AATLとは、アドビシステムズ社の「Adobe Approved Trust List」の略称です。AATLに登録されている電子認証局から発行された電子証明書を用いて PDFに電子署名すると、PDFを Adobe Acrobatなどで閲覧した際、信頼される署名として確認できます。

iTrust 電子署名用証明書の特長

電子署名用途専用の認証局

- 日本国内で運営される電子署名用途専用のルート認証局として、国内で初めて国際的な監査規格である「WebTrust for CA」に合格しました。
  用途を電子署名に限定し、書面の電子化や電子契約に最も適した信頼性の高い電子署名用証明書として提供しています。

AATL対応

- AATLに対応しているため、iTrust 電子署名用証明書を用いて電子署名されたPDFを Adobe Acrobat や Acrobat Readerで開くと緑色のチェックマークと共に「署名済みであり、すべての署名が有効です」と表示されるため、全ての利用者が直観的・視覚的に信頼できる PDFであることを確認できます。

柔軟な署名用証明書の提供方式

- 電子署名用証明書の格納先として、「iTrust リモート署名サービス連携タイプ」、「HSM タイプ ※」、「USB トークンタイプ」をご用意しています。
- 「iTrust リモート署名サービス連携タイプ」は、「iTrust リモート署名サービス」をご利用いただくことで、別途 HSM をご用意いただくことなく、CSR 作成や発行された証明書で電子署名が可能です。

※ HSMタイプをご利用時には、お客様側にて FIPS 140-2 レベル 2 以上の HSM をご準備いただく必要があります。
本サービスにおいて、以下の HSM が問題なく動作することを確認しております。

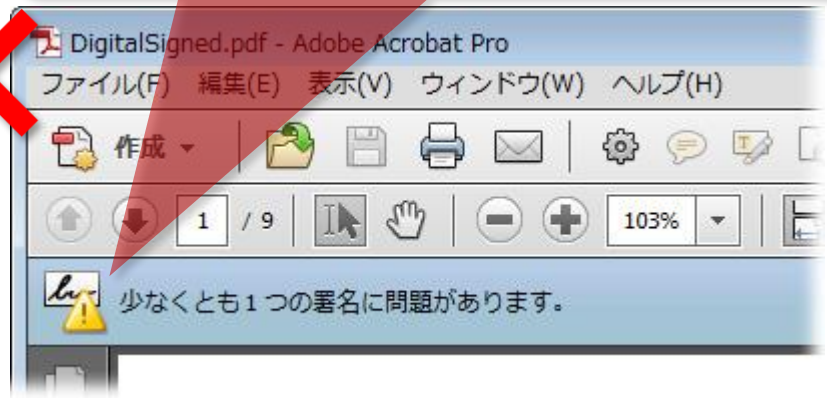
・Amazon Web Services(AWS)：AWS CloudHSM
・Gemalto 社：SafeNet Data Protection On Demand（DPoD）

課題：（相手が）信頼できるか？

Q：電子契約書類を受け取った相手は、どちらが安心でしょうか？

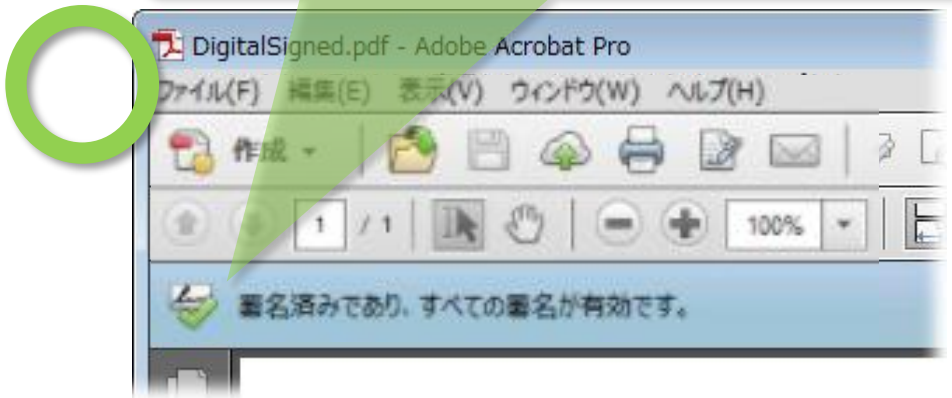
「信頼された署名」にルート証明書が登録されていない場合

少なくとも 1つの署名に
問題があります。



「信頼された署名」にルート証明書が登録されている場合

署名済みであり、
すべての署名が有効です。



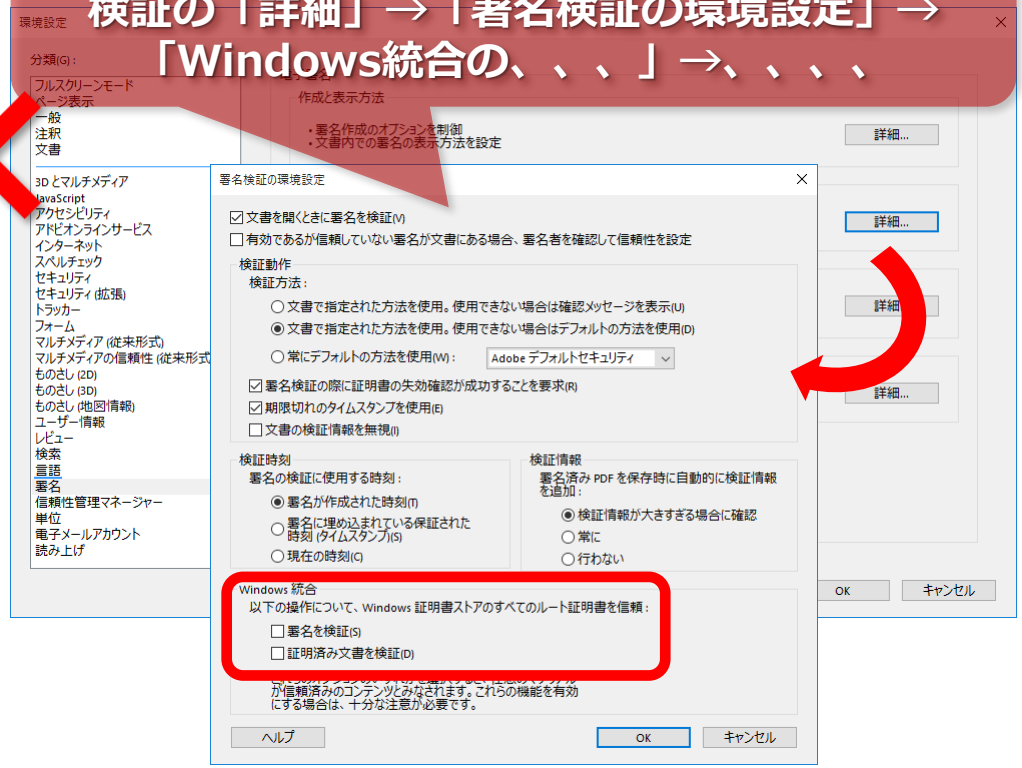
一般的な電子証明書を用いた電子署名では、PDFを受け取った相手が閲覧しようとすると
「警告のアイコン」とともに**「少なくとも 1つの署名に問題があります。」**
と表示されます。
PDFを受け取った相手が、閲覧しただけで信頼できる PDFであることを確認できる電子証明書を用いて電子署名をすることが大切です。

課題：（相手にとって）簡単か？ルート証明書の登録

Q：電子契約書類を受け取った相手は、どちらが簡単に署名を確認できるでしょうか？

「信頼された署名」にルート証明書が登録されていない場合

「編集」メニュー →「環境設定」→「署名」→
検証の「詳細」→「署名検証の環境設定」→
「Windows統合の、、、」→、、、、



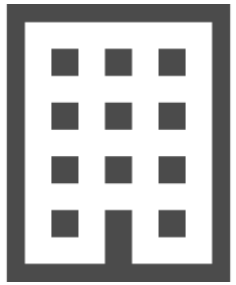
「信頼された署名」にルート証明書が登録されている場合

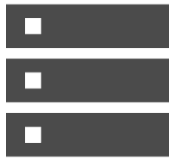
何もしなくても OK！

一般的な電子証明書を用いた電子署名では、PDFを受け取った相手側で複雑な設定をしなければ**「信頼された署名」**と表示されません。PDFを受け取った相手が閲覧しただけで信頼できる PDFであることを確認できる電子証明書を用いて電子署名をすることが大切です。

iTrust 電子署名用証明書（法人向け）の提供形態

法人





HSM

証明書発行申請

HSMタイプ

利用例：HSMに秘密鍵を保管（サーバ署名）

USBトークンタイプ

利用例：各利用者のパソコンで署名（ローカル署名）

サイバートラスト
iTrust 電子署名用認証局

署名用証明書 発行

iTrustリモート署名
連携タイプ

サイバートラスト
iTrust リモート署名サービス

参考：　iTrustパートナー様向け特別価格のご案内

サーバ証明書：SureServer Prime（iTrustパートナー様向け価格）

- **SureServer Prime　　定価：52,800円/年　→ 30,000円/年**
  - 対象：　1 FQDN
- **SureServer Prime ワイルドカード　　定価：120,000円/年　→ 80,000円/年**
  - 対象：　1 ドメイン + 無制限のサブドメイン
  - 階層違いのサブドメインを追加可能（最大 150 個）

Webアプリケーション脆弱性診断

- **精度の高い診断の提供**
  - 技術者によるマニュアル診断を提供
  - IPAをはじめとしたセキュリティ機関の勧告に基づいた診断の提供
- **参考価格：iTrustパートナー様向け：857,000円**
  - 診断対象30ページ、報告会あり、再診断あり
  - 価格は、診断対象、提供内容により異なります。上記は参考価格です。

cybertrust

信頼とともに

留意事項

本資料に記載されている会社名、製品名、サービス名は、当社または各社、各団体の商標もしくは登録商標です。
その他本資料に記載されているイラスト・ロゴ・写真・動画・ソフトウェア等は、当社または第三者が有する知的財産権やその他の権利により守られております。
お客様は、当社が著作権を有するコンテンツについて、特に定めた場合を除き、複製、改変、頒布などをすることはできません。
本資料に記載されている情報は予告なしに変更されることがあります。また、時間の経過などにより記載内容が不正確となる場合がありますが、当社は、当該情報を更新する義務を負うものではありません。