「続々登場中！クライアント証明書対応アプリ！」～JCANパス（FCFキャンパスカード対応）、スマホSIM活用、ROBINS連携（Thunderbirdアドオン）等～

2014年5月

JIPDEC（一般財団法人日本情報経済社会推進協会）
安信簡情報環境推進部　事業推進室
室長　大泰司　章（おおたいし　あきら）

0．はじめに
「クライアント証明書の普及活動やってます」

JIPDEC組織概要

■ **名称**　JIPDEC（ジプデック）
一般財団法人日本情報経済社会推進協会
Japan Institute for Promotion
of Digital Economy and Community

旧　財団法人日本情報処理開発協会
Japan Information Processing
Development Corporation

■ **設立**　昭和42年12月20日

■ **基金**　39億9,900万円

■ **事業規模**　26億4,300万円（平成25年度予算）

■ **職員数**　126名（平成25年4月現在）

Route 1　六本木一丁目駅より（東京メトロ南北線）徒歩4分
改札を出て泉ガーデンテラス脇エスカレーターを一番上まで上がり、
そのまま庭園内を直進し、車道を右へ

Route 2　神谷町駅より（東京メトロ日比谷線）徒歩10分
4aまたは4b番出口を出て左に進み、ホテルオークラ別館の手前の角を左折、
1つ目の角を左折し、スウェーデン大使館前を直進

■制度

- ●プライバシーマーク制度の運用
- ●ISMS／ITSMS／BCMS適合性評価制度の運営
- ●電子署名・認証制度に基づく特定認証業務の調査

■サービス

- ●サイバーID証明書JCANの普及
- ●サイバー法人台帳ROBINSの運用
- ●標準企業コードの登録・管理

■提言

- ●電子情報の利活用基盤の整備のための調査研究
- ●IT資産マネジメントに関する調査研究
- ●産官学連携による課題の検討、政府への提言
- ●電子情報利活用に関するさまざまな情報提供

「安信簡情報環境」とは

インターネット（サイバー空間）をもっと

安心　信頼　簡単

にします。

サイバーID証明書「JCAN」（ジェイキャン）

Japan CA Network

組織内個人を電子証明書のしくみで認証します。

サイバー法人台帳「ROBINS」（ロビンズ）

Reference Of Business Identity for Networked Society

組織（法人）を認証するデータベースです。

企業の英字名称、Webサイトのドメイン、メールの送信ドメイン等の
ホワイトリスト作ってます。

「安信簡情報環境」における各種サービス

JIPDEC

安信簡情報環境

JCAN

サイバー法人台帳 ROBINS

クライアント認証

電子契約

メール署名、暗号化

S/MIME

エスマいぬ

企業コード検索

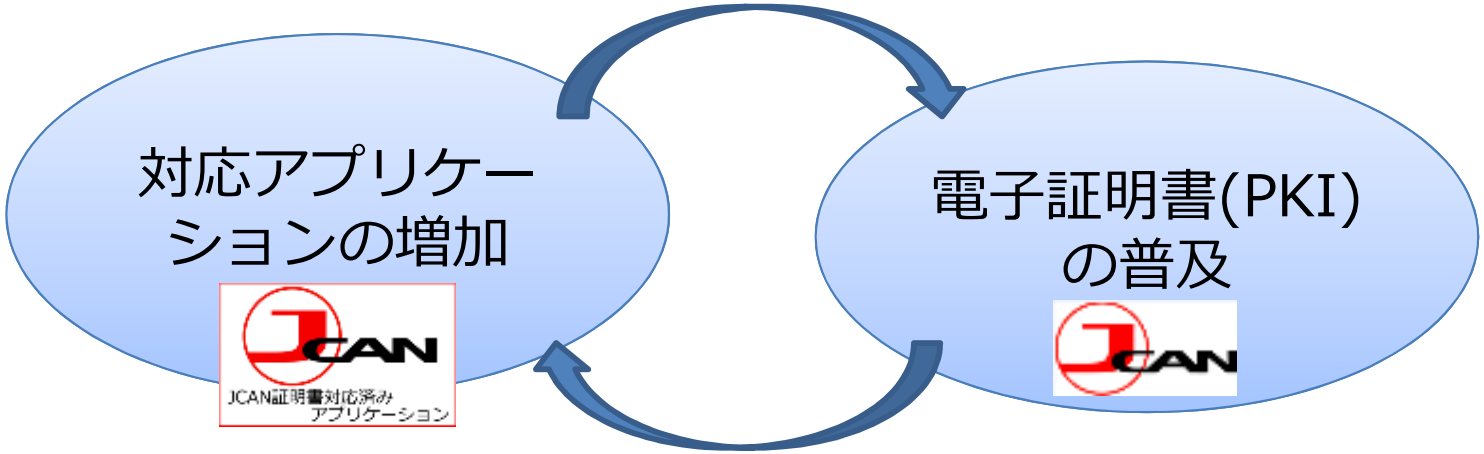
メールなりすまし対策
「安心マーク」

DKIM

ディーキぃぬ

Webサイトなりすまし対策
「ROBINSシール」
「ブランドシール」

JCAN対応アプリケーション普及に向けて



（１）クライアント認証用途 ⇒ 社員証・職員証

（２）電子契約用途 ⇒ ハンコ

（３）S/MIMEメール用途 ⇒ 封筒、差出人署名

クライアント認証用途

■ **JIPDEC**
・職員にJCAN配付。
・メール（クラウド）やグループウェア（オンプレ）に社外からアクセス。

■ **松本商工会議所**
・日商タブレットから会議所基幹システム「TOAS」に「CCIセキュアアクセス」！

■ **株式会社スマイルワークス**
・会計販売給与のクラウド「ClearWorks」へのアクセス。（ＳＳＯ）

■ **某国立研究機関**
・職員にJCAN配付。職員証はFCF。JCANパスとして利用。
・サーバへのアクセスのほか、フォルダ暗号化、S/MIME等検討中。

最近頻発しているID、パスワード窃盗問題解決の切り札になりうるか！？

トラストフレームワーク（ID連携）

JPKI普及で証明書に慣れ？？

電子契約用途

■ **新日鉄住金ソリューションズ株式会社**
・「Nsxpress Ⅱ 電子契約サービス」

○印紙税削減。郵送費削減。CO2削減。
○電子化による業務効率向上。

■ **セイコーソリューションズ株式会社**
・京都大学にてJCANパス＋FCFキャンパスカード実験中。
・「かんたん電子契約」

■ **イマジニアス株式会社**
・電子文書ASPサービス「e-Pru(イプル)」

民間有志にて
領収書電子化WG
も開始

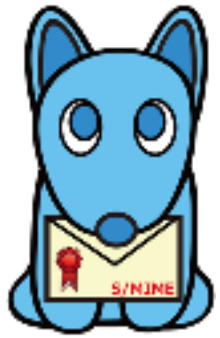
■ **株式会社日本BPO株式会社／シヤチハタ株式会社**
・「電子契約」スタート支援サービス／「電子印鑑システム　パソコン決裁」

昨年後半より問合せ急増。2014年電子契約元年プロジェクト始動。

普及団体立ち上げ。

S/MIMEメール用途

S/MIME（エスマイム：Secure / Multipurpose Internet Mail Extensions）
　メールに署名を打ったり、暗号化することが可能



■**金融機関、官公庁、政党等（JCANではありませんが・・・）**
・なりすまし被害が大きいと想定される業界で、メルマガや案内メールで利用。

■**JIPDEC（再掲）**
・原則としてメールには署名
・機密性が高いメールについては暗号化
・取引先にもJCANを配付し暗号メールでやりとり。
→相手の証明書がないと聞いてくるので、誤送信防止にも効果。

昨年来、標的型攻撃への対抗手段として総務省での取組開始。

暗号化の見直し。

JCAN対応アプリケーション普及状況

	事業者名	アプリケーション名
1	株式会社ユニクラウド	ブラウザPC＆ストレージ「iDesktop」
2	株式会社スマイルワークス	会計・販売・給与をまとめて管理！ SaaS/クラウド型の統合業務システム「ClearWorks」
3		オンライン・データストレージ「セキュア・フォルダ」
4	株式会社日本BPO	「電子契約」スタート支援サービス
5		「電子証明書」発行代行サービス
6		「USB認証トークン」向けJCAN証明書プリインストールサービス
7	セイコーソリューションズ株式会社	かんたん時刻認証
8		かんたん電子契約
9	新日鉄住金ソリューションズ株式会社	NsxpressⅡ電子契約サービス
10	株式会社ジェイエムエーシステムズ	クライアント証明書対応スマートデバイス用 高セキュリティブラウザ「KAITO」

JCAN対応アプリケーション普及状況

	事業者名	アプリケーション名
11	松本商工会議所	全国の商工会議所を支援するトータルOAシステム「TOAS」
12		大切なクラウド上のデータを守る「CCIセキュアアクセス」
13	BizMobile株式会社	モバイルデバイス管理ソフトウェア「BizMobile」
14	マジック・ソフトウェア・ジャパン株式会社	スマートフォン/タブレット端末対応 超高速全文検索・活用システム「Smart DocFinder」
15	ジェムアルト株式会社	セキュリティーソリューション
16	インタセクト・コミュニケーションズ株式会社	セキュリティ万全の電子署名で、 ビジネスをグンと効率的に「オープンリミットCCサイン」
17	株式会社JCCH ・セキュリティ・ソリューション・システムズ	認証局アプライアンス プライベートCA 「Gleas」
18		証明書ベースの PKI 対応「USB 認証トークン」
19	日本セーフネット株式会社	SAMLによるSSOサービス「JCANクラウドID」
20		ハードウェア セキュリティ モジュール（HSM）

JCAN対応アプリケーション普及状況

	事業者名	アプリケーション名
21	イマジニアス株式会社	電子文書ASPサービス「e-Pru(イプル)」
22	東北インフォメーション・システムズ株式会社	NFC対応Android™スマートフォン端末へ電子証明書を配信する試験用プラットフォーム
23	伊藤忠テクノソリューションズ株式会社	教育機関向けクラウドサービス「A-Cloud」
24	株式会社エアー	次世代メッセージングプラットフォーム「CommuniGate Pro」
25	デジタル・インフォメーション・テクノロジー株式会社	電子署名メールソリューション「AntiPhishingMailGateway®(APMG®)」
26	株式会社日立ソリューションズ	メールからの情報漏えい防止ソフトウェア「秘文AE Email Gateway」
27		暗号メールチェックゲートウェイ「SMIME Inspection Gateway」
28	シヤチハタ株式会社	紙文書にも電子文書に「シヤチハタ印」が使えます！電子決裁支援ツール「電子印鑑システム パソコン決裁」
29		電子文書ワークフロー＆管理「ワークフロー機能搭載文書管理システム　DocGearCabinet」
30	マクニカネットワークス株式会社	IDフェデレーションソフトウェア「PingFederate」

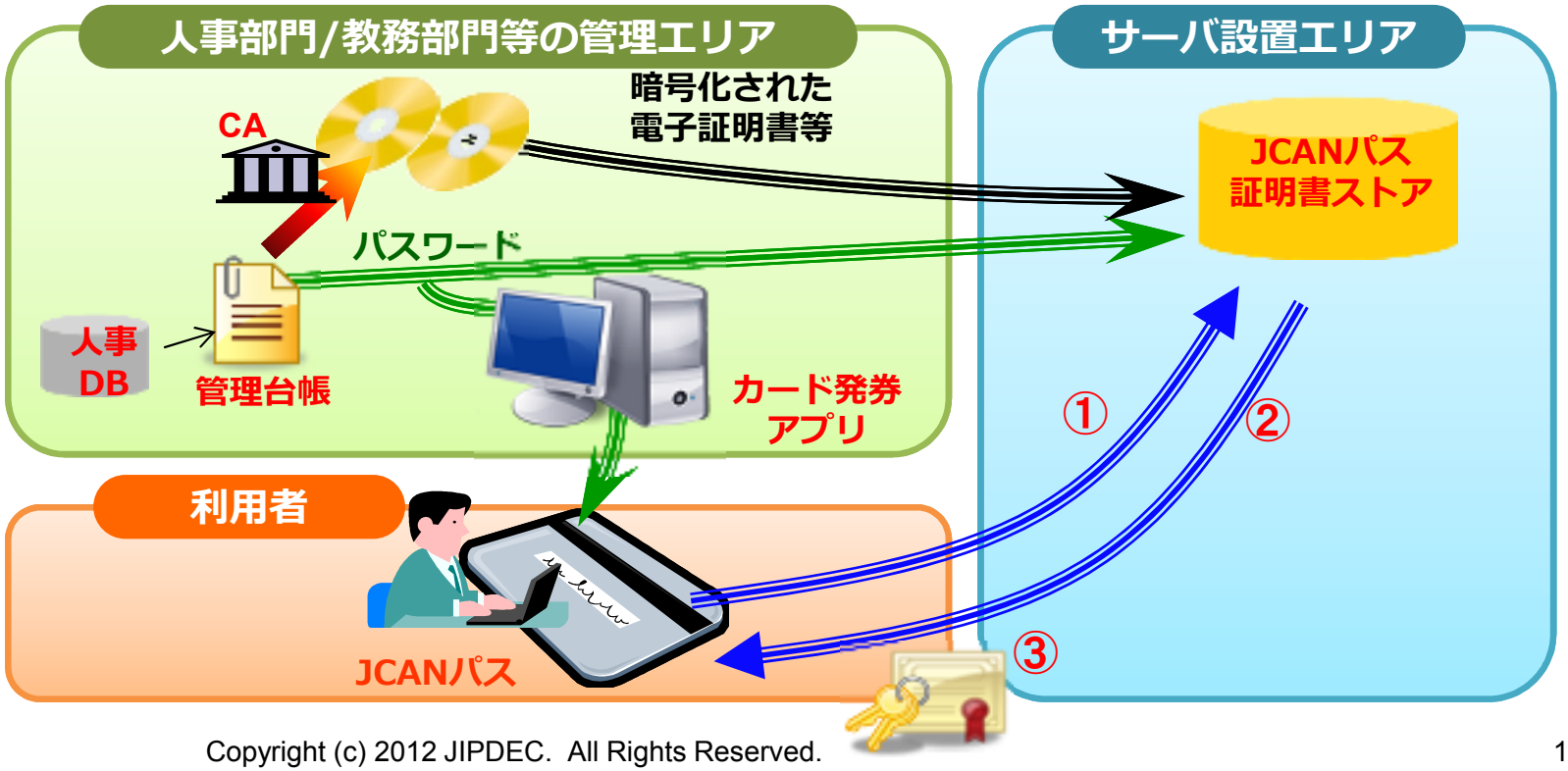
1．JCANパス（FCFキャンパスカード対応）

JCANパス

JCANパスSDK

■ JCANパスとは、暗号化された電子証明書のパスワードをFCF対応ICカードに書き込むことで、電子証明書の3大用途である「電子認証」「暗号化」「電子署名」等の機能を使用可能としたもの

■JCANパスSDKとは、JCANパスを扱うドライバで下記機能開発で用いるツールセット
①FCF対応ICカードからPKCS#12を復号するパスワードを読み出す機能
②同パスワードを書き込む機能
③Windows（XP/Vista/7）にPKCS#12をインストールする機能



SDK:
Software Development Kit の略

JCANパスのメリット

◆パスワードさえ決めておけば、証明書発行に関係なくICカードを発行可能
⇒4月の入学/入社等でのIC発行作業に支障を与えない
⇒従来のFCF対応ICカードと同様、段階的なアプリケーション導入が可能

【初年度】
初期導入アプリ

【2年目】
アプリの追加

【3年目以降】
さらに
アプリの追加

最初からJCANパスを導入

JCANパスはそのままで
アプリを追加

JCANパスはそのままで
アプリを追加

入退室管理

勤怠管理

ログイン

電子メール

電子文書保存

電子決裁

JCANパスのメリット

◆証明書が期間満了となっても、いままでのICカードがそのまま使用可能
⇒大学院等へ進学しても、いままでのICカードがそのまま使用可能

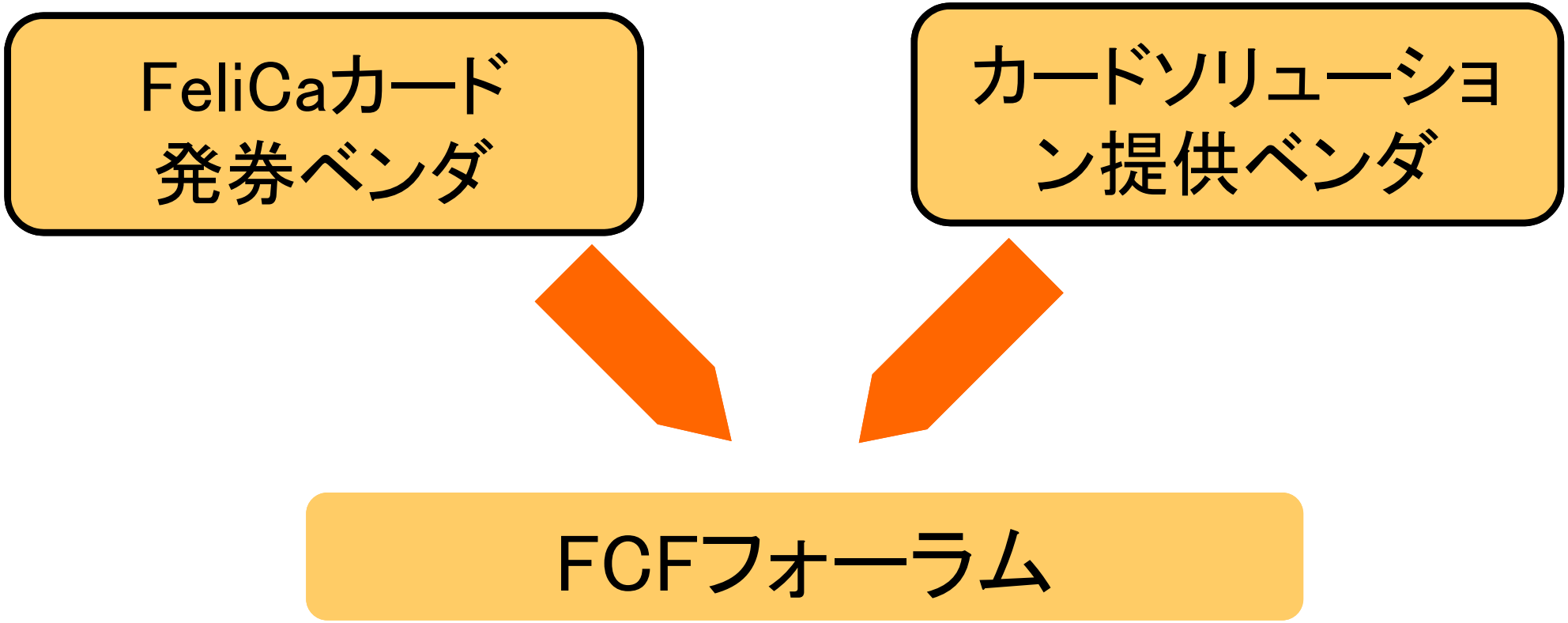
◆証明書ストアをアプリケーションに置くと、そのアプリケーションだけしか証明書を利用できなくすることが可能
⇒全社員/全学生が利用できるが、特定の人しかタイムスタンプを打てないサービスを提供可能

◆ICカード毀損による証明書の再発行を必要としない
⇒紛失であっても、証明書のパスワードを替えるだけで失効する必要はない

◆ICカードの着脱で、証明書のインポート/エクスポートが可能【JCANパスSDK標準機能】
⇒JCANパスを持った人しかアクセスができないので、共有端末でも安全に利用可能
※ JCANパスSDK標準機能としてiOS、Androidへの対応を予定

◆FCF対応ICカードが指定のリーダライタにタッチすればJCANパスになる【 JCANパスSDK標準機能】
⇒既に発行済みのFCF対応ICカードもたちまちJCANパスとして利用可能
※だたし、B、C4エリアのあるカードのみ

共通フォーマットの普及と運用管理



- 基本情報の規定コード（利用者区分コード、学校識別コード）の管理と配布
- 共通アクセスツールの企画
- 共通フォーマットの広報と流通推進
- 共通フォーマット利用によるサービスの拡大推進

2013年3月「FCFフォーラムご紹介」より引用

FCF共通利用フォーマット導入状況

2013年2月現在

◆導入数：

企業、自治体　　66企業

大学等教育機関　　144機関

◆発行枚数：　初期発行分のみカウント

企業、自治体　　約23万枚

大学等教育機関　　約78万枚

総数　約101万枚

➢ 教育機関で毎年追加発行されるカードも含めると約100万枚を超える発行枚数がある

2013年3月「FCFフォーラムご紹介」より引用

FCF独自のユニークナンバー（FCF-UN）の提供

FCF

○ FCF会員のカード製造企業が提供するユニークナンバー

- FCF推進フォーラムの会員であるカード製造会社が共通領域にFCFフォーラム所定のフォーマットで書き込むFCF内での一意の番号です。
- カード製造段階で入力される情報であり、フォーマット／コード体系を維持する当事者は、ＦＣＦフォーラム事務局とカード製造会社に限られるため、カード発行者の負担も少なくなります。

○ 従来のFeliCa製造番号（IDm）に代わる番号の提供

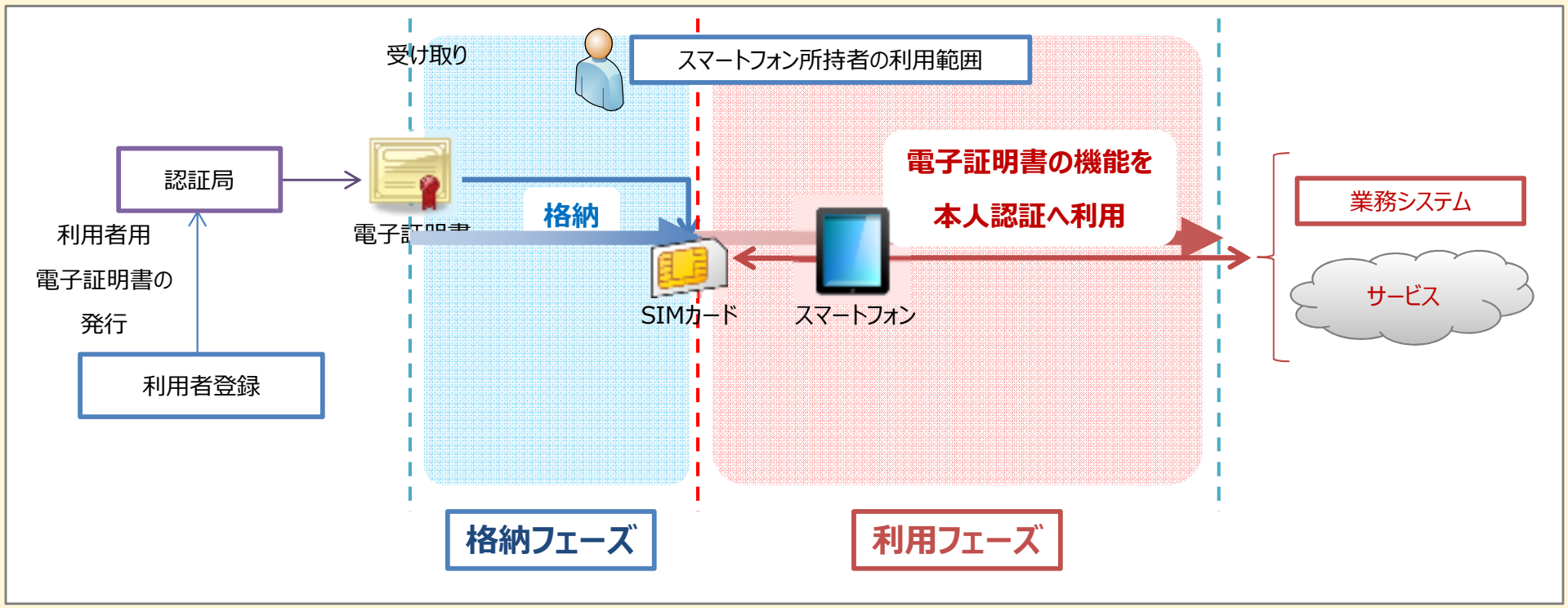
- FeliCaでの一意な番号としてFeliCa製造番号であるIDmを認証に用いてサービスを提供しているベンダーが多くありますが、最近の技術では、エミュレータによる「Idmのなりすまし」が可能となってきており、セキュリティの用途での利用は控えるべきものとの認識が高まってきております。
- FCF-UNは、IDmを代替するサービスとして、IDカードを幅広く共用していくためのセキュリティ認証基盤となります。

2013年3月「FCFフォーラムご紹介」より引用

2．スマホSIM活用

技術のご紹介　–格納フェーズと利用フェーズ-

- スマートフォンを利用したセキュリティ基盤について試験用プラットフォームを構築することで，2012年12月にJIPDEC様とKDDI様と共同でJCAN証明書を対象とした実証実験を実施し，良好な結果を収めました。

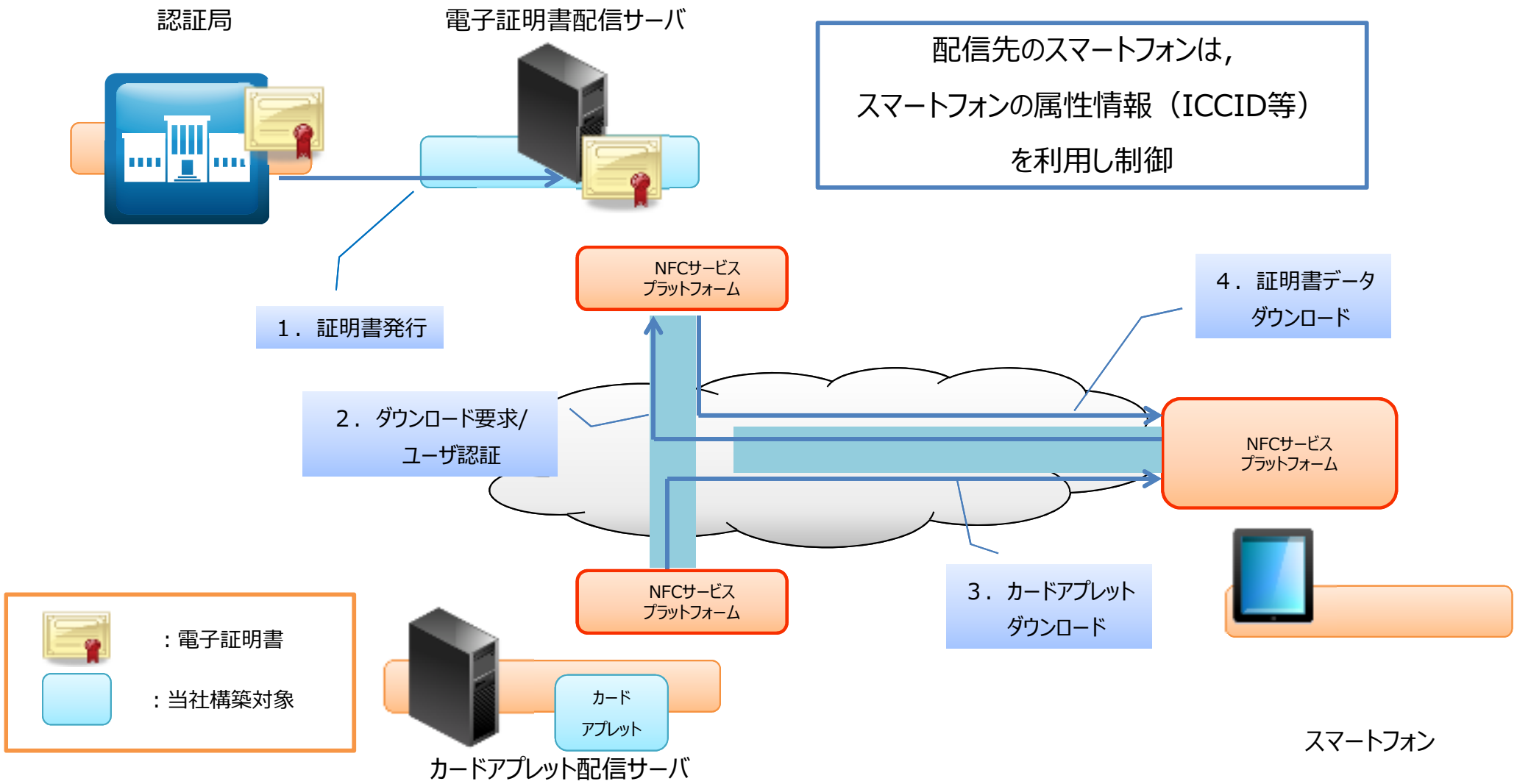


※2013年11月にてNTTドコモ様における環境にて接続試験を実施

参考：　http://www.toinx.co.jp/company/information/H24/h25-02-21/
「国内初、KDDIの「NFCサービスプラットフォーム」を利用し、NFC対応Android™スマートフォン端末へ電子証明書を配信する試験用プラットフォームを構築」

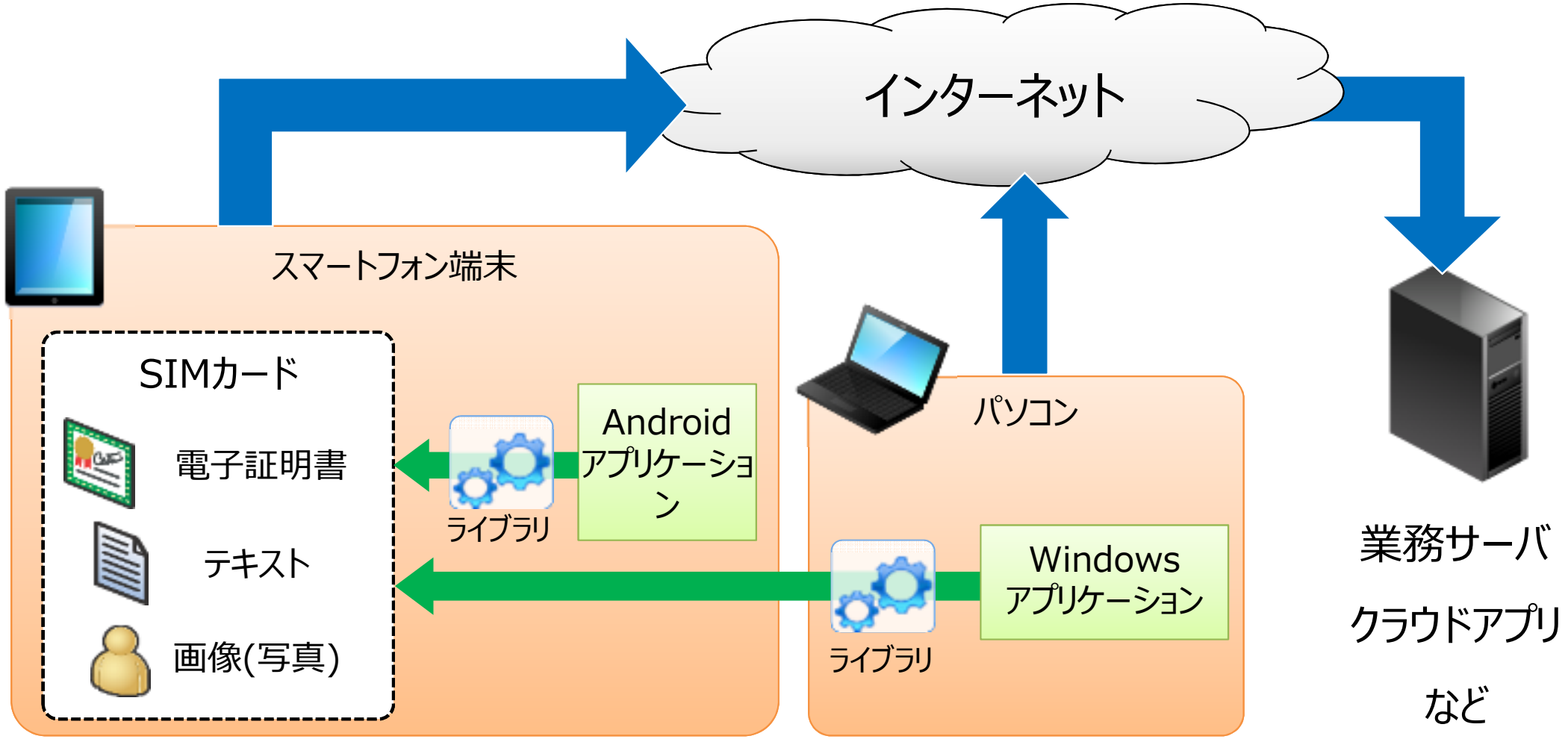
技術のご紹介　–格納フェーズについて-

■ NFCサービスプラットフォームを利用し，電子証明書の配信・再配信・削除を実行



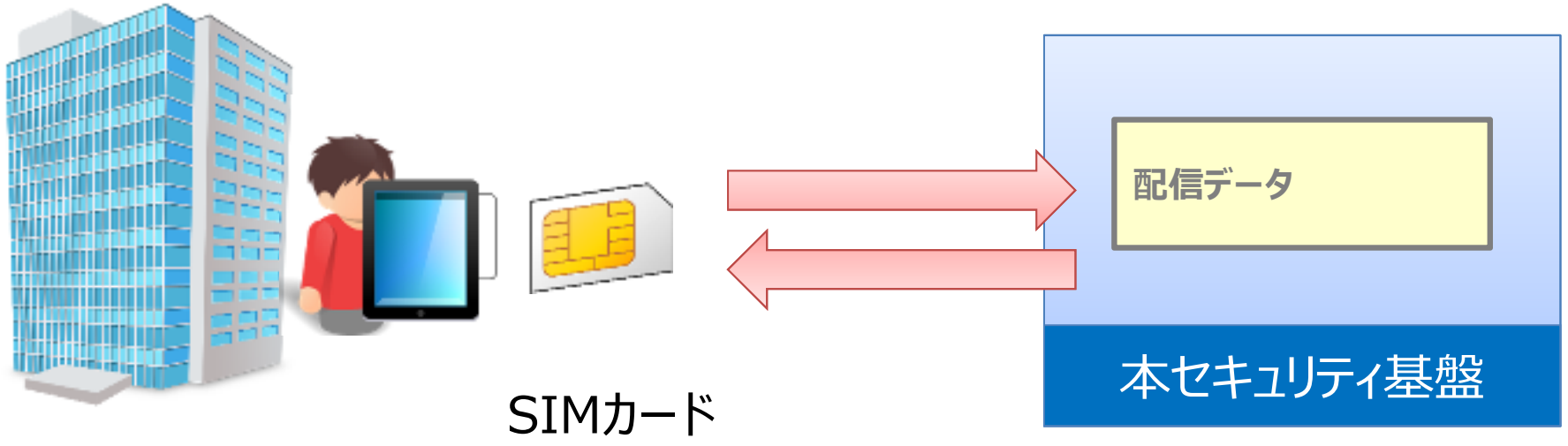
技術のご紹介　–利用フェーズについて-

- １つの認証情報が スマホでも パソコンでも 利用できる



利用例　-①配信データ受信-

■ 配信データ受信
作業員証としてたろうさんへ対応する個人データをSIMカードへとダウンロードします。



・対象のスマートフォンに対して登録している配信データを即時に発行できる

・セキュアエレメントへ書き込むため，書き込んだデータは強固に保護される

利用例　-②入退認証-

■ 入退認証
スマホカードまたはICカードを用いて入退館の合否を判断します。

・スマホカードは，電源が入っていなくてもICカードとして振る舞うことができる

・PCと連携して本人確認による入退認証が実現できる

・NFC対応スマートフォンと連携して簡易的な入退認証が実現できる

適用できる他の利用シーン

・社員証

・カード忘失者用の臨時証

・災害時入退館証

利用例　-③作業実績報告-

■ 作業実績報告
SIMカード内の電子証明書を用いて秘密鍵演算を行います。
ここでは，点検作業の作業データとして写真を想定し，その作業データへ署名値を付加します。

作業データ

証明データ

署名値

SIMカード内で
生成

SIMカード

・SIMカード内で電子証明書の処理を実行するため，秘密鍵が外部へ漏洩しない
（暗号化およびデジタル署名）

・Windows上で電子証明書の処理が実行可能

適用できる他の利用シーン

・スマートカードログオン認証
（WindowsPC）

・SSLクライアント認証

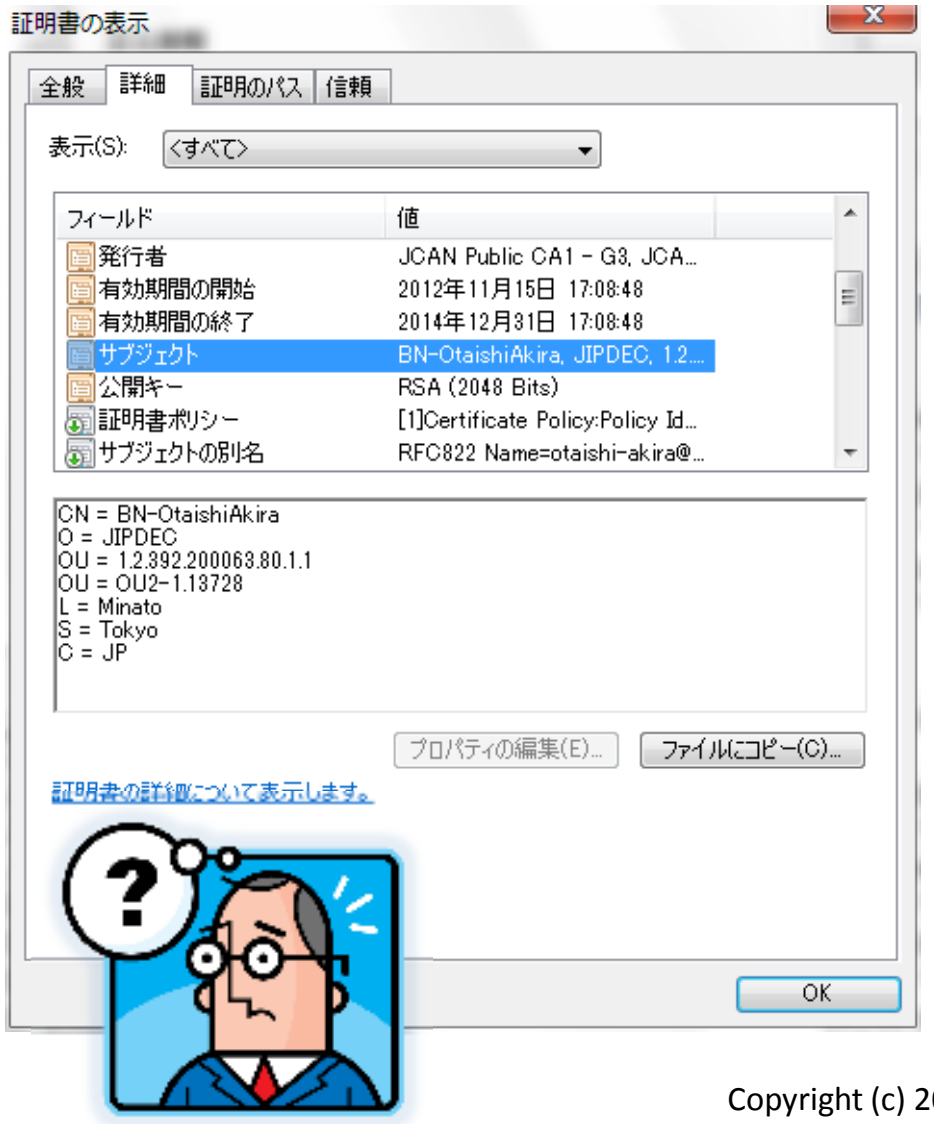
・タイムスタンプ

3. ROBINS連携（Thunderbirdアドオン）

署名検証をもっと見える化したい

技術的な検証結果は正しいが、
見ても分からない・・・・

→ 見て分かる！



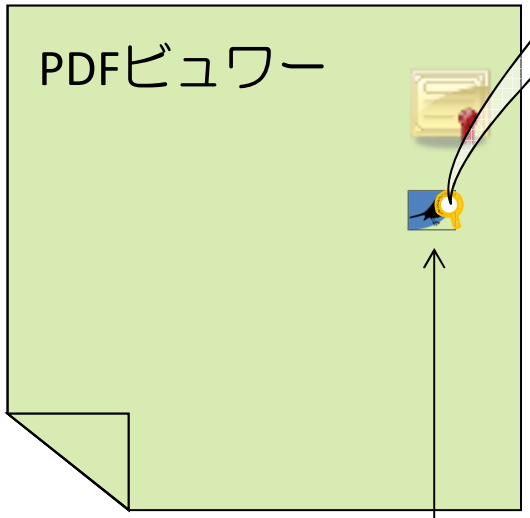
たとえば、PDF署名で

PDF署名文書との連携

- JCAN証明書に、第三者確認された会社情報の、ROBINSのURLを記載。
- PDF文書作成者が、JCAN証明書でPDFに電子署名
- PDF表示ソフトで、アイコン をクリック
- 電子署名を検証して、JCAN証明書に記載されたROBINSのURLを抽出し、ブラウザに渡す。
- ブラウザが、第三者確認された会社情報を表示

PDF文書作成者の会社情報表示(ブラウザ)

電子署名付きPDF(JCAN証明書)



ROBINS連携のアイコン

JCAN 証明書のSUBJECT領域に、ROBINSのURLを記載
OU = OU2-https://robins.jipdec.or.jp/Key.do?99999999999999&J=1

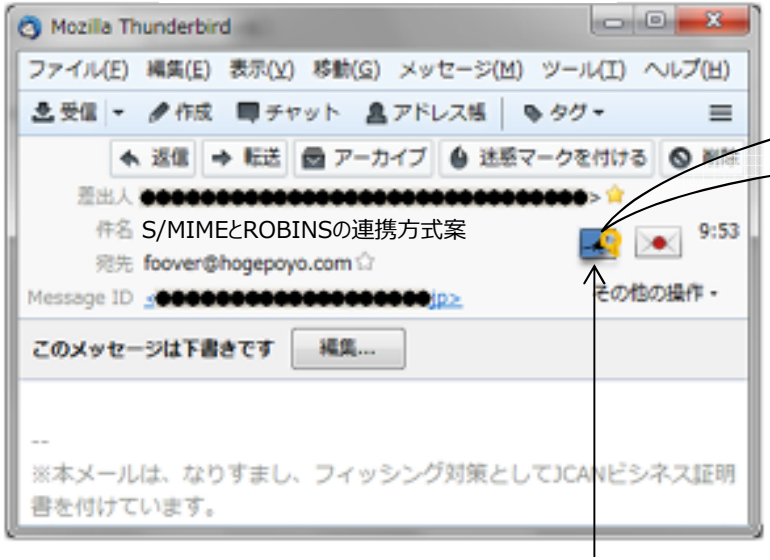
たとえば、S/MIMEメールで（デモ）

S/MIMEメールとの連携の例

- JCAN証明書に、第三者確認された会社情報の、ROBINSのURLを記載。
- 差出人が、JCAN証明書でS/MIME電子署名
- 受取人が、メールソフトADD-ONのアイコン をクリック
- メールソフトADD-ONが、 S/MIME電子署名を検証して、JCAN証明書に記載されたROBINSのURLを抽出し、ブラウザに渡す。
- ブラウザが、第三者確認された会社情報を表示

差出人の会社情報表示(ブラウザ)

メールソフトの表示



メールソフト ADD-ON

S/MIME
電子署名付き
メール
(JCAN証明書)

ROBINS連携ADD-ONのアイコン

JCAN 証明書のSUBJECT領域に、ROBINSのURLを記載
OU = OU2-https://robins.jipdec.or.jp/Key.do?99999999999999&J=1

DKIMベースではすでに稼働済み

ネット選挙運動で適用した例

ニフティ(株)、ヤフー(株)などと連携して、本仕組みを
金融機関、自治体、商工会議所等へ展開推進中。

政党

○○党

件名: メールマガジン vol.XX
送信元: xxxx@mail.○○.jp

mail.○○.jpから
メルマガ送信を依頼

本物メールの見える化の仕組み

メール送信事業者

DKIMで送信

政党情報とメール送信用ドメイン
mail.○○.jp を申告

DKIM送受信で
メールドメイン認証

信頼できる法人情報のデータベース

第三者確認

ROBINS

・公正、中立な運営（JIPDEC）
※送信事業者、ISP/ASPとは独立な組織

ROBINSで
送信者特定

mail.○○.jp の
政党情報を提供

大手ISP/ASP

メール
ボックス

YAHOO! JAPAN メール

@nifty

WEBメールサービス

安心マーク
の表示

有権者(ユーザ)

送信者が一目で
わかって安心！

Webメール一覧