SafeNet | THE DATA PROTECTION COMPANY

PKI Day 2014

新しい電子署名
～クラウド/モバイル署名と非PKI署名～

亀田 治伸 (Harunobu.Kameda@safenet-inc.com)
JIPDEC客員研究員／日本セーフネット株式会社

2014 年 3 月 13 日

SafeNet | THE DATA PROTECTION COMPANY

クラウド署名について

クラウド署名とは

電子署名の仕組みを、以下2つ、もしくはどちらか1つの技術を使用して実現している仕組みの総称で、決まった定義は存在しない。

1. 電子署名を行う仕組み（HSM/アプリケーション）を重量課金で提供しているもの。

2. 電子署名を行う仕組み自体を仮想化しているもの。

（マッシュアップ開発用APIを有する）

SafeNet. THE DATA PROTECTION COMPANY

AWS Cloud HSM モデル

Safenet社が「LunaSA」というHSM（暗号演算＆鍵管理）デバイスに仮想化技術を施し、重量課金でサービス化したもの。米国（バージニア）、欧州（アイルランド）リージョンのみでビジネス展開。日本は当面導入見送り。

おもな利用用途：

電子契約

改竄防止ソリューション

http://aws.amazon.com/jp/cloudhsm/

SafeNet. THE DATA PROTECTION COMPANY

電子契約における米国市場の状況

電子署名法に相当する法律が存在しない
企業間の相対契約のみで電子契約が成立
（自動車会社のローン契約等で使用）

電子契約における米国市場の状況

電子署名法に相当する法律が存在しない
　　企業間の相対契約のみで電子契約が成立
　　（自動車会社のローン契約等で使用）

改竄防止の概念がコモディティ化している。

　　HSMからは鍵が漏洩しない
　　↓
　　HSMで暗号化したデータはそのHSMでしか解読できない
　　↓
　　データが第三者に改竄されていない技術的担保となりうる

　　事例：e-Passport、運転免許証、CISCO、iPhone等

FIPSセキュリティレベル

FIPS140-2認定とは？

米国政府主導にて制定された暗号モジュールにおけるハードウェアおよびソフトウェアの要件

取得にあたり、NIST等第三者外部監査機関の技術的攻撃に耐える必要があるため、未取得製品より安全性が高いといえる

Level1： 大まかに、すべてのコンポーネントにおいて一定の品質が担保され、甚だしくセキュリティの欠如がないこと
ソフトウェア製品の取得上限

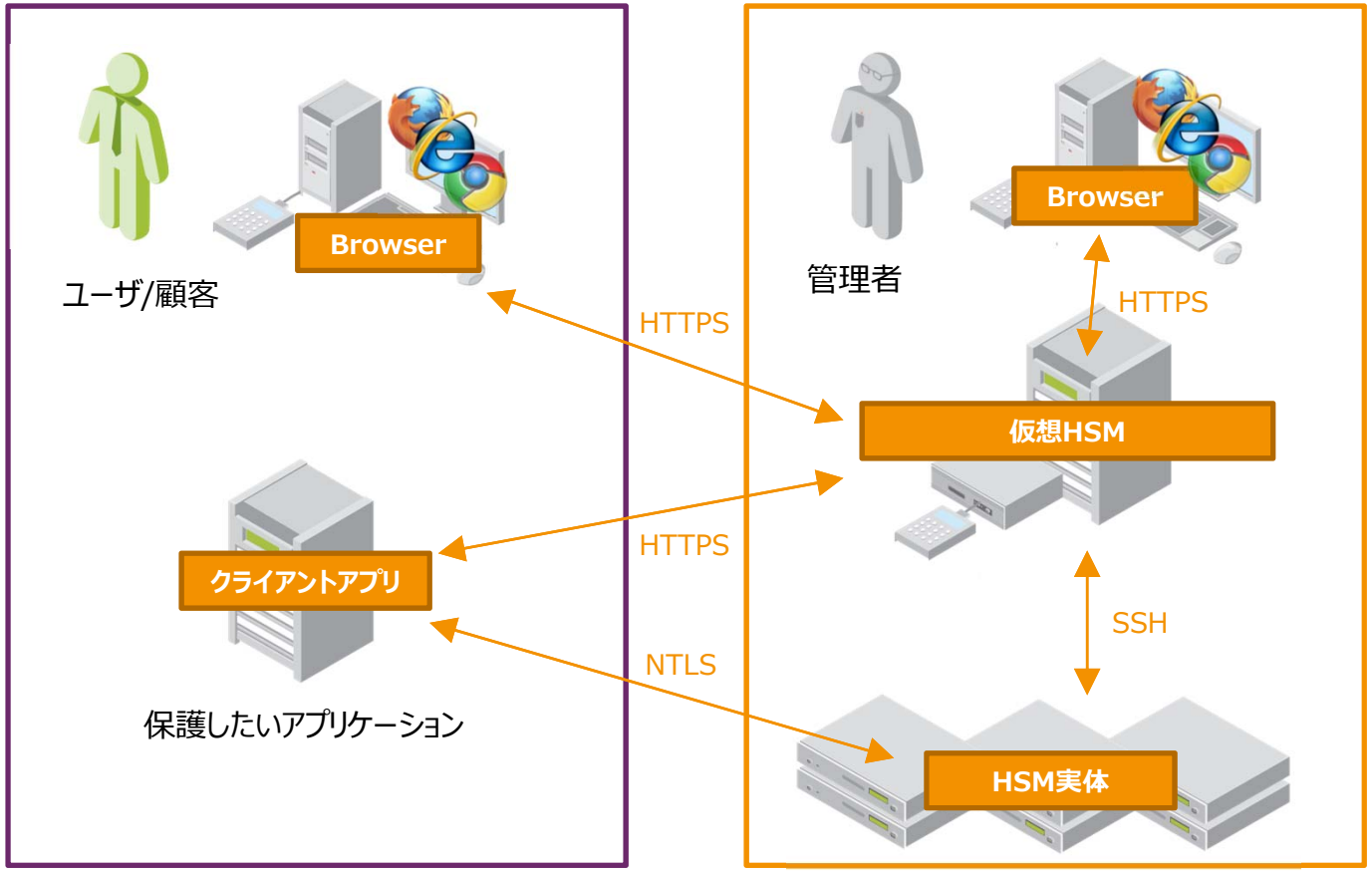
Level2: 上記に加え、物理的な改竄の痕跡を残すこと、及びオペレータの役割ベースでの認証を行うこと

Level3: 上記に加え、**物理的な改竄への耐性を持つこと（耐タンパ性）**、**オペレータのIDベースでの認証を行うこと**、及び重要なセキュリティパラメータがモジュールに出入力するインタフェースと、その他のインタフェースとを物理的又は論理的に分離すること

SafeNet. THE DATA PROTECTION COMPANY

仮想HSM動作イメージ

仮想HSMは、HSM実体に対するProxyであり、仮想OSの概念とは異なる



SafeNet. THE DATA PROTECTION COMPANY

SafeNet | THE DATA PROTECTION COMPANY

OCRA
ワンタイムパスワード型電子署名

なぜ今　ワンタイムパスワード署名か？

Webのアーキテクチャは、

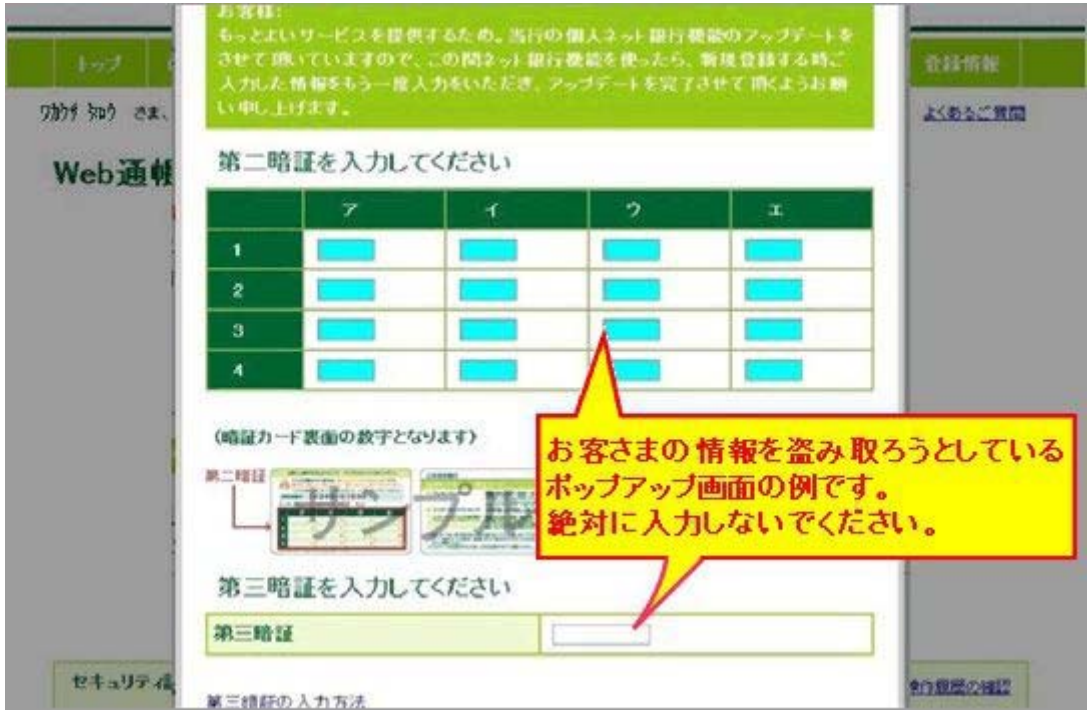
- ログイン時にユーザーを認証する
- その後の同一セッションでの処理は同一ユーザーが実施している

Man In the Browserにより
「ブラウザがのっとられており信頼できない」（データを改竄する）と想定する。

ログインとは別に、トランザクション専用セッションを構築する必要がある。

日本の銀行不正アクセス

2013年1月から10月15日までに1315件、計約14億円（警視庁発表）



SafeNet. THE DATA PROTECTION COMPANY

なぜ今　ワンタイムパスワード署名か？

Webのアーキテクチャは、
- ログイン時にユーザーを認証する
- その後の同一セッションでの処理は同一ユーザーが実施している

Man In the Browserにより
「ブラウザがのっとられており信頼できない」（データを改竄する）と想定する。

ログインとは別に、トランザクション専用セッションを構築する必要がある。

PKIはブラウザに依存する。 → ブラウザ外で動作不可能

RFC6287として　OATH方式ワンタイムパスワード　チャレンジレスポンスが定義されている。（OCRA）
- その実装の一例としてオンラインバンキング向けトランザクション署名が定義されている。

SafeNet. THE DATA PROTECTION COMPANY

もう一つなまなましい話

PKIは電子データでありブラウザに格納される。

- 管理責任の範囲特定が極端に難しく、ユーザーと銀行の責任範囲の定義が難しい

OTPはハードウェアをユーザに持たすことで責任範囲の明確化が可能

三菱東京UFJ銀行 MUFG

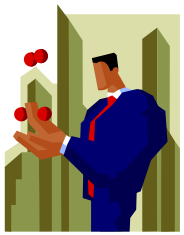
原則として通知があった日から30日前の日以降になされた払出しについて被害補償いたします。なお、ご本人に過失があることを当行が証明した場合の被害補償額は4分の3となります。ただし、これらは番号等の盗用から2年を経過する日後に通知をいただいた場合には適用されません。さらに、ご本人に重大な過失がある場合、ご本人の配偶者、二親等以内の親族、その他同居人または家事使用人によって行われた場合、またはご本人が被害状況の説明において重要な事項について偽りの説明を行った場合には被害補償の対象とはなりません。

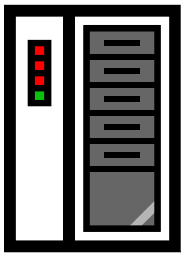
つまり、どっちが安いか？

OATHワンタイムパスワード

RSAの独自方式に対抗して生み出された、ワンタイムパスワードのベンダー相互運用を目的とした共通規格

主なベンダ：Safenet、Symantec、Vasco、DNP、Toppan等





シードといわれる暗号情報を
事前に双方が持っておく

シードに「何か」を加えてワン
タイムパスワードを生成する

クライアント、サーバともにシードは共通で
あり、「何か」が同じであれば、同じOTPが
生成

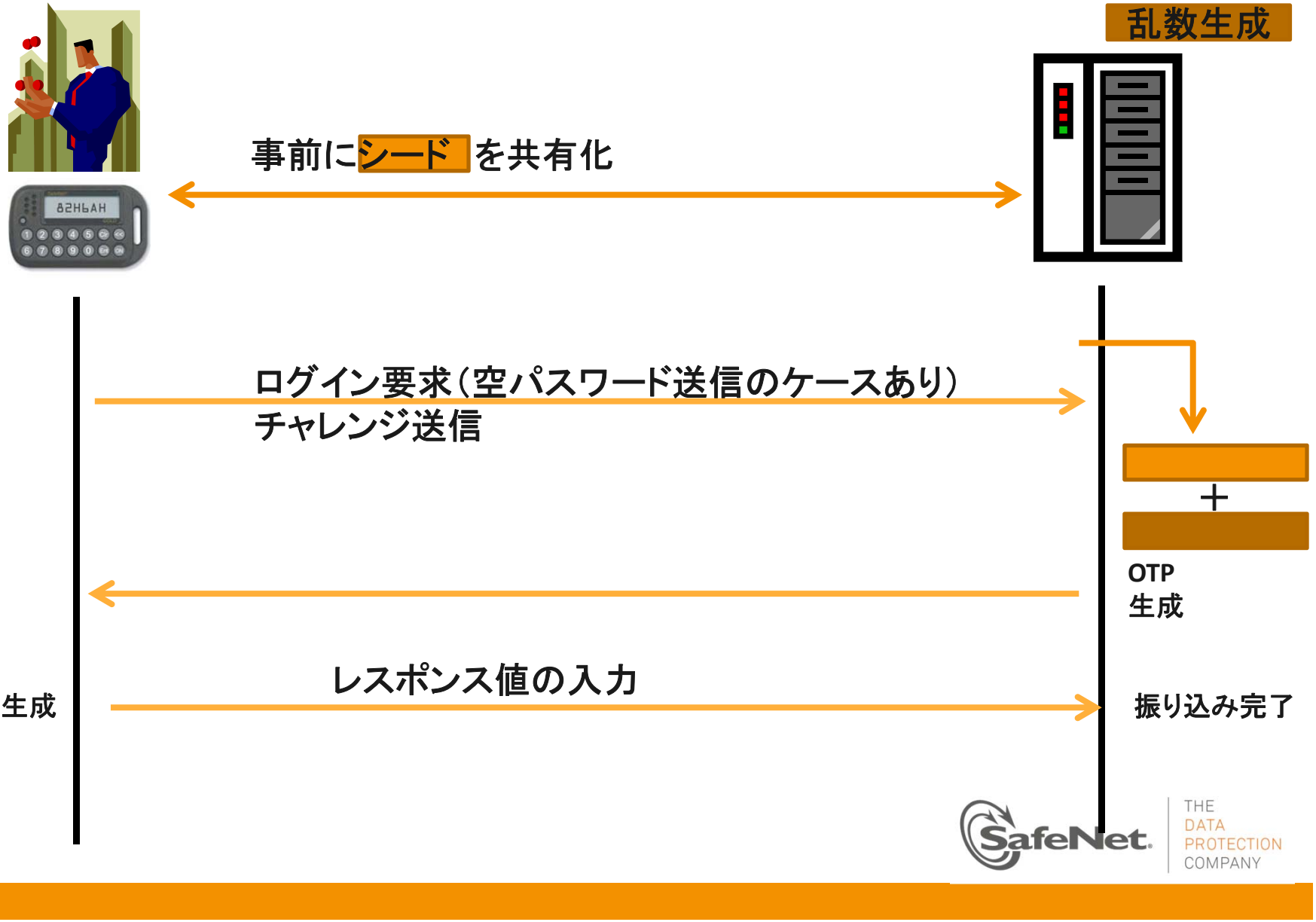
時間：TOPT：時刻同期

OTP生成回数：HOPT：イベント同期

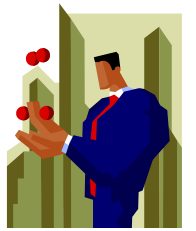
サーバで生成した乱数、もしくは外部からの入力：OCRA：チャレンジレスポンス型

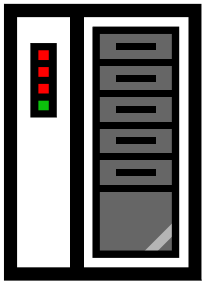
SafeNet. THE DATA PROTECTION COMPANY

RFC6287　トランザクション署名　Oath Challenge Response Algorithmのご説明



RFC6287　トランザクション署名　Oath Challenge Response Algorithmのご説明





事前に**シード**を共有化

振り込み指示:
銀行名、口座番号、金額等　→　**文字列変換**

パスワード
生成

ブラウザにパスワード表示

パスワード入力

レスポンス生成

レスポンス値の入力

振り込み完了

PKI署名とOCRA署名

PKI署名：
公的にサーバ、ユーザー双方の存在を立証可能な認証モデル
サーバサイド、ユーザーサイド双方が、署名を保存時、後日検証が可能

PC（ブラウザ）での実装が主流でモバイル対応は一部

PKI署名とOCRA署名

PKI署名：
公的にサーバ、ユーザー双方の存在を立証可能な認証モデル
サーバサイド、ユーザーサイド双方が、署名を保存時、後日検証が可能

PC（ブラウザ）での実装が主流でモバイル対応は一部

OCRA署名：
特定領域（特定オンラインバンキング）のみでユーザーの存在が立証可能
サーバサイドのみが署名保存、後日検証が可能

PC（ブラウザ）での動作は原則不可能。モバイル、専用ハードウェアで実装

PKI署名とOCRA署名

PKI署名：
公的にサーバ、ユーザー双方の存在を立証可能な認証モデル
サーバサイド、ユーザーサイド双方が、署名を保存時、後日検証が可能

PC（ブラウザ）での実装が主流でモバイル対応は一部

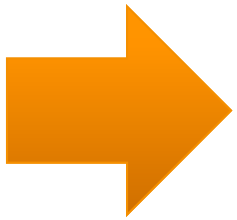
OCRA署名：
特定領域（特定オンラインバンキング）のみでユーザーの存在が立証可能
サーバサイドのみが署名保存、後日検証が可能

PC（ブラウザ）での動作は原則不可能。モバイル、専用ハードウェアで実装

有効期限・失効の概念がない

将来的に必要となるかもしれない、言葉の整理

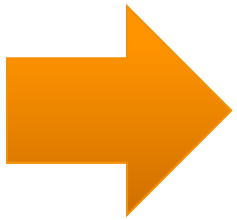
Digital signature
Digital sign
Transaction sign
E-sign



大きく「署名」という概念で定義される

将来的に必要となるかもしれない、言葉の整理

Digital signature
Digital sign
Transaction sign
Electronic Sign



大きく「署名」という概念で定義される

Everything Goes to Digital

派生フロー

携帯にSMSで送付 （Androidが不安）

メールで送付 （東京三菱UFJ銀行で不正ログイン事件あり）

- Outlookでメールを受信したため、IEと同時にのっとられていた、とされている。
- 同様の理由でWebメールはNG
- （受け入れられるとしたら）携帯ドメイン限定

光のモールス信号で伝達

- モールス信号を光に変換しFlashをリアルタイム生成
- ブラウザで表示させ、トークンの裏側のカメラで読み取る

音のモールス信号で伝達

携帯アプリにPush配信