「英国オープン・バンキング」におけるトラストの確立

崎村夏彦／IT基盤技術戦略室

2019年4月17日

Share the Next Values!

野村総合研究所
Nomura Research Institute

「トラスト」の本質

野村総合研究所
Nomura Research Institute

確認しないこと

「信頼とは、想定される将来の挙動に関して、実際の行動の根拠となるのに十分確かな仮説で、その人に対する知と無知の中間の状態である。」

（出所）Simmel, Georg: *Soziologie Untersuchungen über die Formen der Vergesellschaftung*, Duncker & Humblot, Berlin 1908 (初版) をもとに、崎村訳

ゲオルグ・ジンメル
（1858－1918）
形式社会学の父

情報システムにおける「トラスト」とは？

✓その情報システムが期待通りに動くと、
✓自ら検証することなく、
✓信じて使うことができること。

そのシステム全体について、誰かがどこかできちんと
検証していることを期待するということになると言えよう。

たとえば、典型的なPKIベースの電子署名システムだと以下のようなことを「期待」しているわけだが

ドメインの管理はきちんとされていて	
発行に際しての本人確認もきちんとしていて	
証明書発行のための鍵は全て厳密に管理されていて	
証明書を生成するソフトウェアもきちんと動いていて	
ユーザは署名鍵を本人利用しかできないよう厳密に管理していて	
署名作成ソフトはきちんと動いていて	
受取手が動かす署名検証ソフトもきちんと動いている。	

* 最近では yamanashi-med.ac.jp なども

往々にして期待は裏切られる。

ドメインの管理はきちんとされていて	lovelive-anime.jp
発行に際しての本人確認もきちんとしていて	Symantec/Google*
証明書発行のための鍵は全て厳密に管理されていて	DigiNotar
証明書を生成するソフトウェアもきちんと動いていて	Debian OpenSSL Predictable PRNG
ユーザは署名鍵を本人利用しかできないよう厳密に管理していて	ヾ(o´∀｀o)ﾉｫ''
署名作成ソフトはきちんと動いていて	PRNGガァァ
受取手が動かす署名検証ソフトもきちんと動いている。	鶴亀メールのS/MIME機能 XML Dsigの２重署名問題

* 最近では yamanashi-med.ac.jp なども

もっとも、日本でしばしば見られる、三次元凹凸固形物で顔料を紙等の物理媒体に付着させるという行為よりはマシ

- 欧米のサイン制度と違い、代理決済できるという印章の特長が、迅速な意思決定や決裁に繋がり、戦後の日本の急速な発展にも寄与してきたという自負もあります。
  - （出所）全日本印章業協会他『デジタル・ガバメント実行計画』に対する要望書」(2019-02-02)
- 無断で上司の印鑑100回超押す　区役所職員を懲戒免職　神戸
  - （出所）神戸新聞NEXT (2019/3/8)

気を取り直して

野村総合研究所
Nomura Research Institute

「トラスト」できる系の維持はeIDASの証明書使えば良いとか、そういう問題ではない。

ドメインの管理はきちんとされていて	lovelive-anime.jp
発行に際しての本人確認もきちんとしていて	Symantec/Google*
証明書発行のための鍵は全て厳密に管理されていて	DigiNotar
証明書を生成するソフトウェアもきちんと動いていて	Debian OpenSSL Predictable PRNG
ユーザは署名鍵を本人利用しかできないよう厳密に管理していて	ヾ(o´∀｀o)ﾉｫ''
署名作成ソフトはきちんと動いていて	PRNGガァァ
受取手が動かす署名検証ソフトもきちんと動いている。	鶴亀メールのS/MIME機能 XML Dsigの２重署名問題

* 最近では yamanashi-med.ac.jp なども

Open Banking UK

4つの仕様

どこでも同じように使える

01
- **Read/Write API**仕様

03
- セキュリティプロファイル

安全に使える

誰でも使える

02
- カスタマー・エクスペリエンス・ガイドライン

04
- 運用ガイドライン

安定的に使える

野村総合研究所
Nomura Research Institute

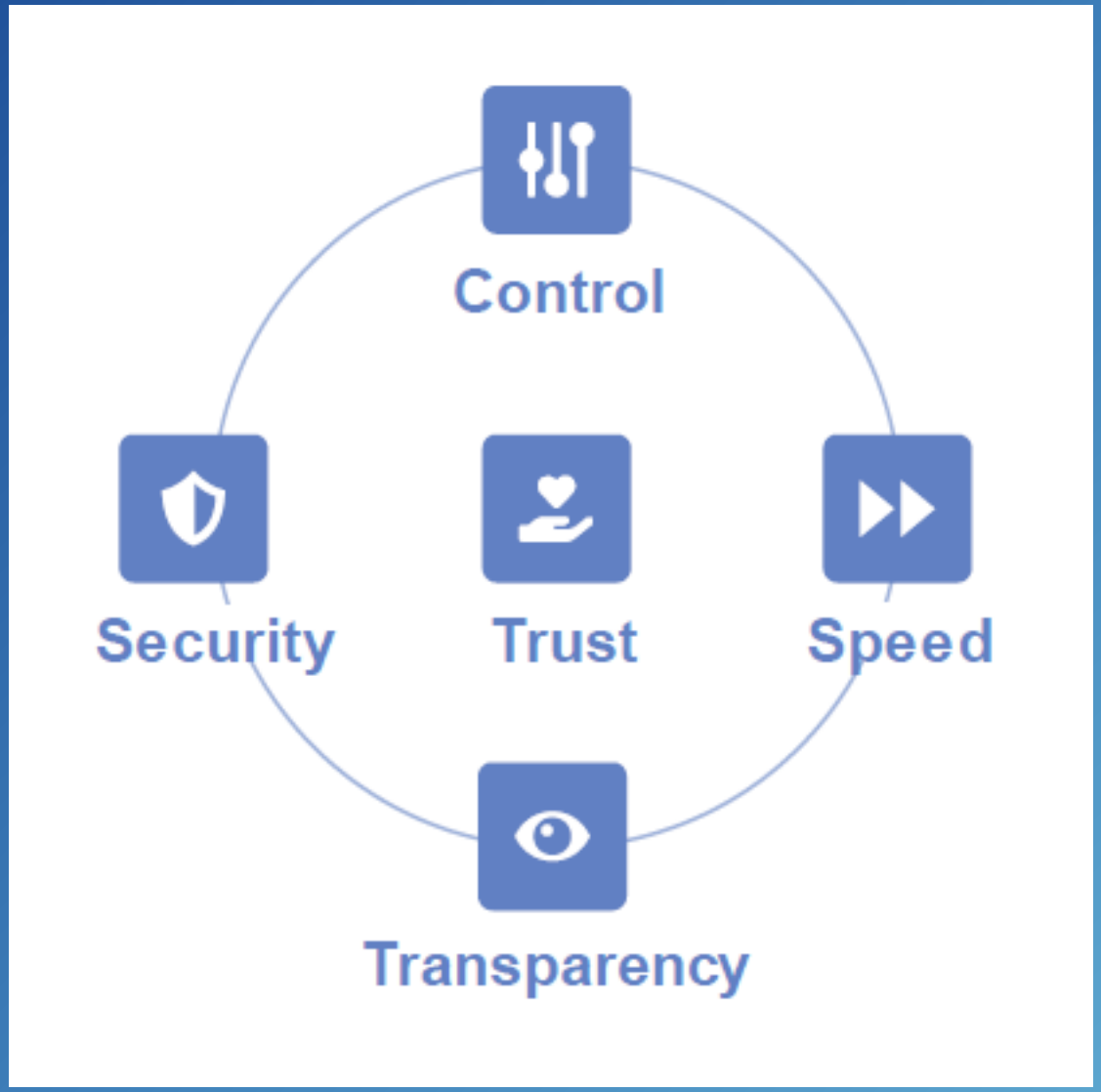
どこでも同じように使える

- CME9 全行で、同じAPIを提供。
- 仕様は完全公開なので、Fintechが開発しやすい。
  - REST/JSON
  - OpenID FAPI Part 2

誰でも使える

- カスタマー・エクスペリエンス・ガイドライン
  - 使いやすくなければ使われない
    - 期待したように動く
    - きびきび動く
    - 透明性が高い
    - 安心
  - 使われなければ意味がない
  - 弱者に優しく

Availability
Integrity
Confidentiality



(出所)Open Banking UK: Customer Experience Guidelines (2019)

野村総合研究所
Nomura Research Institute

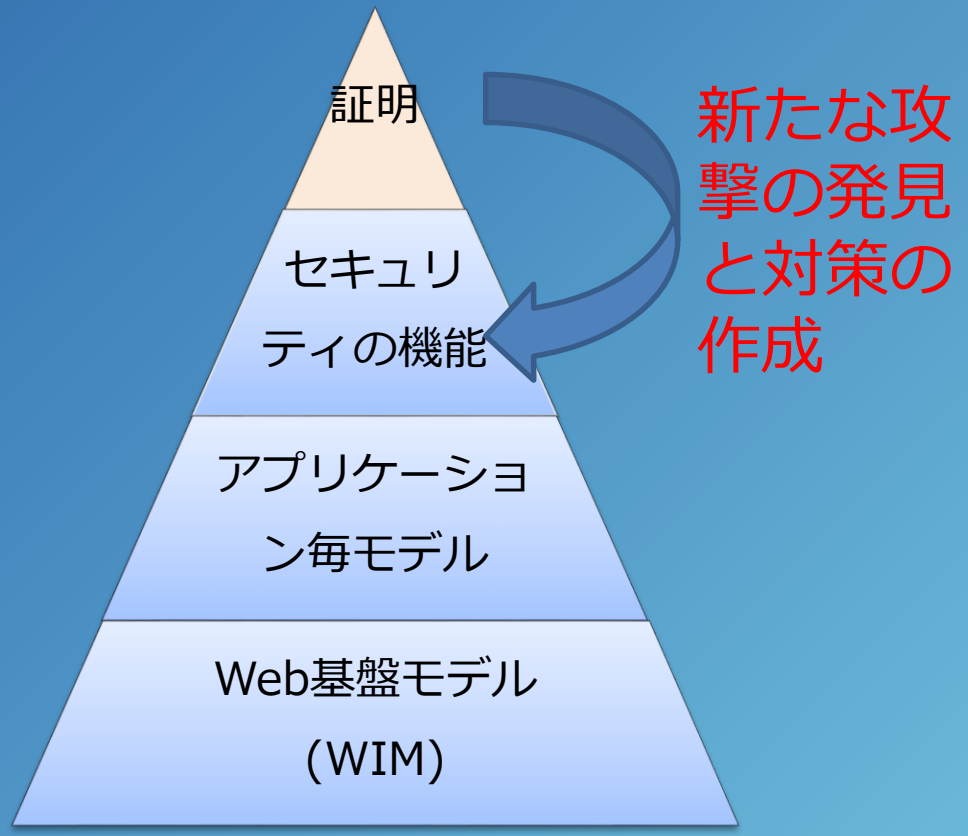
安全に使える

- プロトコル安全性
  - 非常に強い攻撃者モデルを想定した上での、形式証明済プロトコル(FAPI R/W profile)を採用

FAPI: プロトコル安全性

Hosseyni, Fett, Küsters: An Extensive Formal Security Analysis of the OpenID Financial-grade API , Forthcoming (2019)

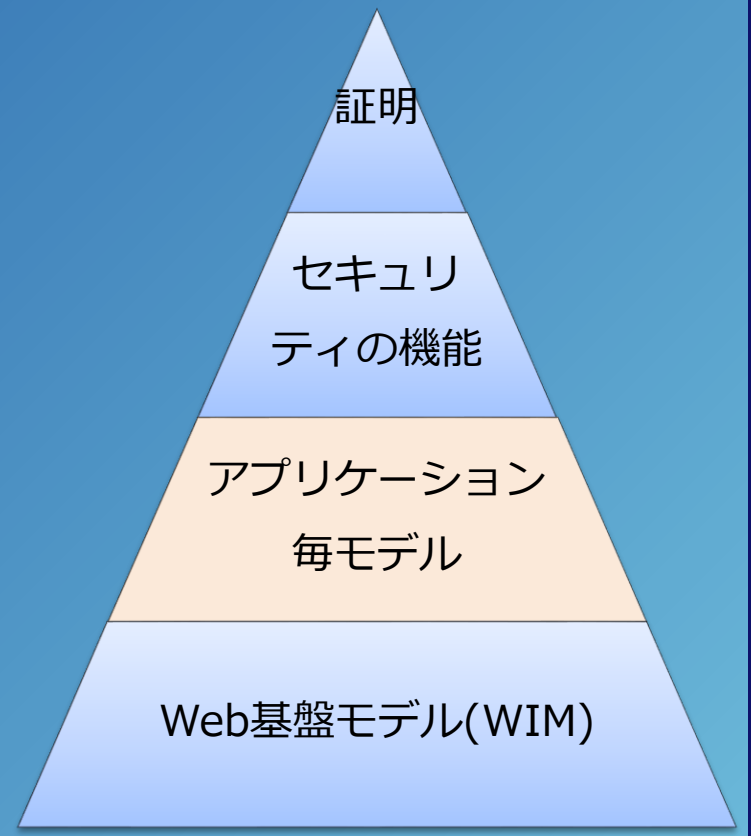
- モデルベース・アプローチを採用
- 強固なセキュリティ保証
  - 未知の攻撃にも対応



野村総合研究所
Nomura Research Institute

FAPI: 攻撃者モデル

- 認可要求は漏れる
  - Referrerや履歴からなど
- 認可応答も漏れる
  - 同上
- Token Endpointが攻撃者の手に渡る
  - DNS乗っ取り
  - 開発者フィッシングなど
- アクセス・トークンは漏れる
  - 一部のリソース・サーバー乗っ取り
  - ログからの漏洩など



野村総合研究所
Nomura Research Institute

FAPI: セキュリティ機能

認証 (Authentication)	• 攻撃者は真の利用者のアイデンティティではクライアントにログインできない。
認可 (Authorization)	• 攻撃者は、真の利用者の資源にアクセスできない。
セッション完全性 (Session Integrity)	• 真の利用者は、自分のアカウントでログインし、自らの資源を利用する。

Theorem 1.

- $\mathcal{FAPI}$ をネットワーク攻撃者のもとのFAPI web システムとする。すると, $\mathcal{FAPI}$ は認証と認可に関して安全である。
- さらに、 OAUTBを用いるWebクライアントに関しては、 $\mathcal{FAPI}$ はセッション完全性に関しても安全である。

安全に使える

- プロトコル安全性
  - 非常に強い攻撃者モデルを想定した上での、形式証明済プロトコル(FAPI R/W profile)を採用
- 実装安全性
  - 実装の安全性を確保するために、年２回、Conformance Test を通す必要が有る。

実装安全性: Conformance Testing

- Conformance Testing for FAPI OP and RPs
  - https://openid.net/certification/fapi_op_testing/
  - 機能テスト、セキュリティ上のテスト（ネガティブテスト含む）を提供
- 開発中も、Conformance Test をCI/CDパイプラインに組み込むこと推奨。
- 各ディプロイメントは、Conformance Testに年２回は合格しなければならない
  - かつて、SAMLであったような、実は署名は検証していなかったような問題(2018)を起こさないように。

Open Banking Directory

安全に使える

- プロトコル安全性
  - 非常に強い攻撃者モデルを想定した上での、形式証明済プロトコル(FAPI R/W profile)を採用
- 実装安全性
  - 実装の安全性を確保するために、年２回、Certification Test を通す必要が有る。
- 運用安全性
  - 可用性、パフォーマンス、他

1.0 Introduction

1.1 The Operational Guidelines

1.2 The Operational Guidelines Checklist

2.0 Availability and performance

2.1 Key Indicators for availability and performance

2.2 Publication of statistics

3.0 Dedicated interface requirements

3.1 Design and Testing

3.2 Stress Testing

3.3 Wide Usage

3.4 Obstacles

4.0 Problem resolution

4.1 Procedures, processes and systems for problem resolution

4.2 OBIE Support

5.0 Change and communication management

5.1 Downtime

5.2 Implementation of a new OBIE Standard

5.3 Changes to an ASPSP's infrastructure, configuration, or software

5.4 Notification of a change

6.0 The OG Checklist

6.1 Explanation of the Operational Guidelines Checklist

6.2 The Operational Guidelines Checklist

(出所)Open Banking UK: Operational Guidelines (2019)

まとめ

1. 「トラスト」されるには、利用者が自ら調べることなく安心して使えなければだめ。
2. そのためには、CX（簡単に安心して使えて、期待通りにサクサク動く）はクリティカル。これは広義のAvailability(可用性)。トラスト・サービスの文脈ではここが見落とされることが多い。
3. UK Open Bankingでは、これを実現するために、４種類の規格を制定・公開している。
4. プロトコルの安全性の確率のために、形式証明もおこなっている。
5. また、実装の安全性・互換性を確かめるために年２回適合テストの実施と結果の公表が求められる。これらは、Open Banking Directoryに反映される。
6. Open Banking UKの「トラスト」はこれらを総合的に実施することによって確保されている。

NRI

未来創発

Dream up the future.

野村総合研究所
Nomura Research Institute