



FIDO 1.0 スペックが公開されました。

2014/12/9

発表

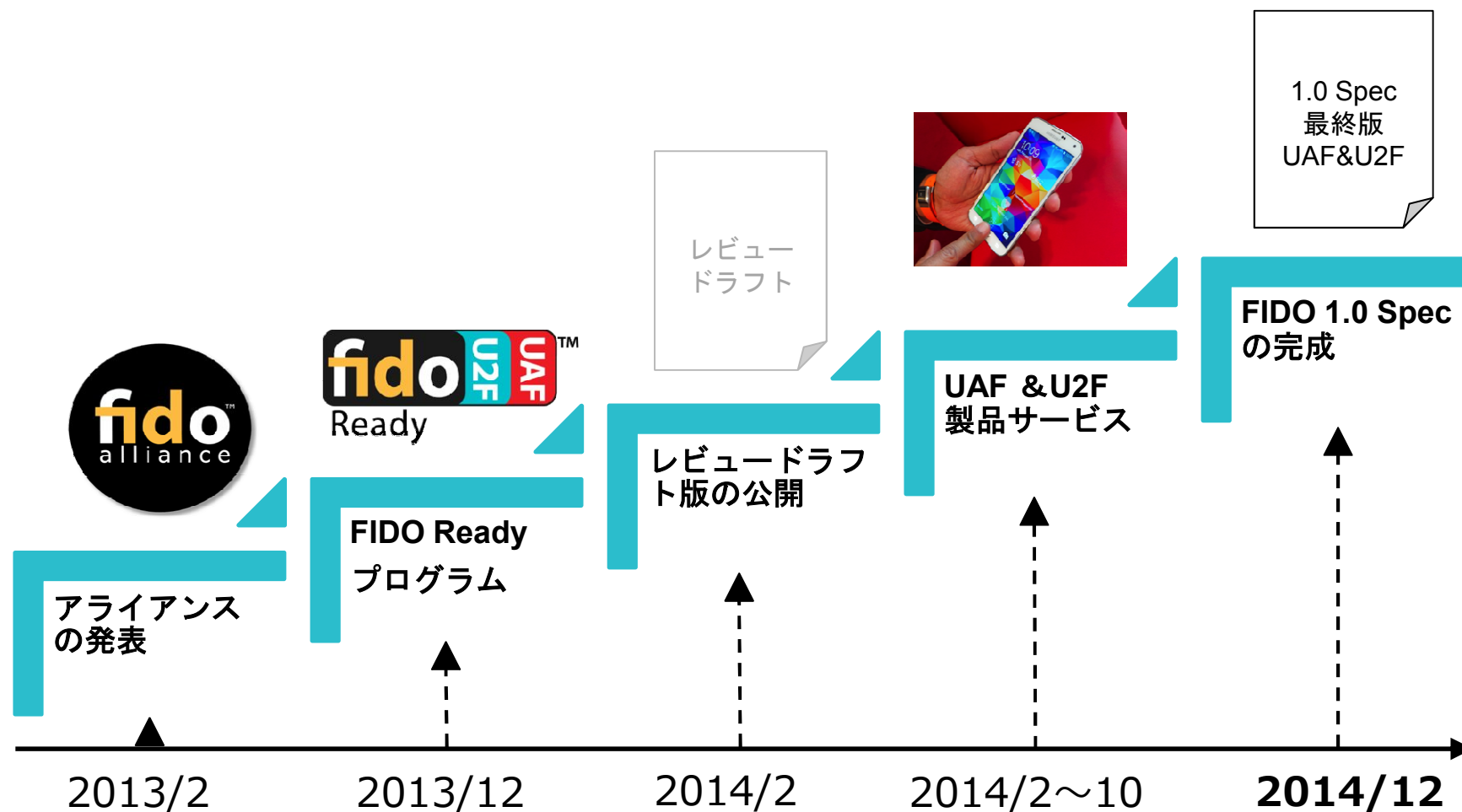
- タイムライン：結成からFIDO 1.0発表まで
- 今回の発表内容

FIDOの目的

FIDO とは何か

FIDOの最新情報

タイムライン: 結成からFIDO 1.0仕様の完成まで



- FIDO 1.0 スペック（仕様）
 - 「U2F : Universal 2nd Factor」 と 「UAF : Universal Authentication Framework」 の 2 つの認証プロトコルから成るFIDO1.0スペック
 - FIDO 1.0スペック（最終版ドラフト）
- FIDOに準拠した製品サービスの販売
 - アライアンスのメンバーは協力し合い、認証プロトコルを共有
 - FIDOアライアンスのメンバーが、FIDOに準拠した製品サービスを販売
- FIDO Ready[™]準拠の認定
 - FIDO Ready[™] の相互運用テストを、1.0スペックに対応
 - コンプライアンス対応含め、認定内容を拡大

発表

FIDOの目的

- パスワード認証の課題と解決策
- FIDOの利点

FIDO とは

FIDOの最新情報

パスワード認証の課題と解決策

- オンラインサービスを安全に利用するためには、パスワード認証が安全だと言えない。
 - 使いまわしやフィッシング、キーロガーによる盗難リスクがある。
 - 長い、複雑なパスワードは、モバイルで使いにくい。
 - ワンタイムパスワードは、モバイルで使いにくく、安全とは言えない。
- 情報の漏洩事故は頻繁に発生しており、被害額も大きい。
 - 事故一件あたりの被害額は、平均350万ドル。 ([Ponemon Institute](#))
 - 最近の事故として、ターゲット（個人情報7000万件）、ホーム・デポ（カード情報5600万件）、JPモルガン・チェース（アカウント情報8300万件）などが報告されている。
- パスワードは、運用や維持コストが高い。
 - パスワードは、従業員 1 人あたり年420ドルの生産性を下げている。
500人規模であれば、年間21万ドルの損害である。 ([Widmeyer Survey](#))

「よりシンプル、より強固なオンライン認証方式」が必要。

オンライン・サービス・ プロバイダ

- 優れたユーザーエクスペリエンス（UX）
- より強固なセキュリティ
- セキュリティを維持するコストの低減

企業

- コストと複雑なシステムの削減
- 企業の重要情報を強力に保護
- 効果的な BYOD（個人端末の利用）の推進

一般消費者

- 使いやすさ
- 相互運用性（端末のローカル認証を利用して、たくさんのサービスの認証に利用）
- セキュリティやプライバシーの保護

発表

FIDOの目的

FIDO とは

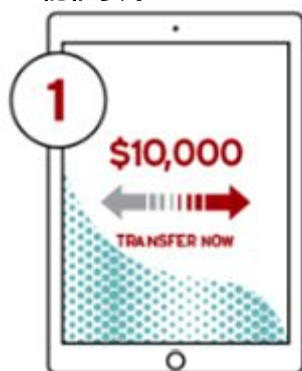
- FIDOを利用した認証の仕組み
- FIDOアライアンスのメンバー

FIDOの最新情報

FIDOを利用した認証の仕組み

1. UAF standards : パスワードレス・エクスペリエンス

オンラインサービスの
認証要求



決済などの処理を実行

デバイスでの
ローカル認証



指紋などでユーザーを認証

オンラインサービスの
認証の成功！



決済などの処理を
完了！

2. U2F standards : セカンド・ファクタ・エクスペリエンス

オンラインサービスの
認証要求



ログイン&パスワード
を入力

デバイスでの
ローカル認証



dongle挿して、
ボタンを押す

オンラインサービスの
認証の成功！



決済などの処理を
完了！

Bank of America.



IdentityX[®]

Google



DISCOVER[®]

PayPal[™]

QUALCOMM[®]

BlackBerry[®]

ARM[®]

lenovo[®] FOR
THOSE
WHO DO[™]



oberthur
TECHNOLOGIES
THE M COMPANY

Synaptics[®]

Nok Nok
LABS

加盟企業
(150社以上)

NXP

Microsoft

CrucialTec

MasterCard

yubico
Trust the Net.

VISA

Alibaba Group

RSA[®]

発表

FIDOの目的

FIDO とは

FIDOの最新情報

- レビュー・ドラフトからの変更点
- FIDOに準拠した製品サービス

レビュードラフトからの変更点

- FIDO U2F
 - Windows USBからHID（ヒューマン・インターフェイス・デバイス）へ通信方法の変更
 - webAPI syntaxの修正
 - app/URL keyの共有を許可するApplication IDの確認手順を追加
- FIDO UAF
 - 詳細レベルの開発と改良
 - メタデータ・サービスの仕様を追加
 - app/URL keyの共有を許可するApplication IDの確認手順を追加

UAF製品サービスの提供

2014年4月より、サムソンの新Galaxy S5と自分の指で、PayPal社のオンライン決済を利用できます。端末に搭載されているFIDO ReadyTMのソフトウェアを使って、指紋センサーとPayPal社のクラウドサービスとの安全な通信を行っています。2014年7月、アリババ社も、Samsung Galaxy S5を利用した、FIDO仕様のオンライン決済サービスを開始しています。

- 生体認証を利用した、より強固な認証方式
- サービスの拡大が簡単
- 生体情報は絶対に端末から外部に送信されない。
- 各アプリケーションやサービス毎に、ユニークな公開鍵と秘密鍵のキーペアを提供する。



クライアントソフトは、
次のOSで動作可能です。



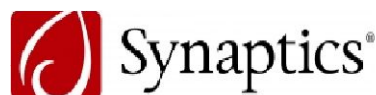
iOS

・ソフトウェア認証要素の例:

音声／顔認証、PIN、QRコードなど

・後付けハードウェア認証要素の例:

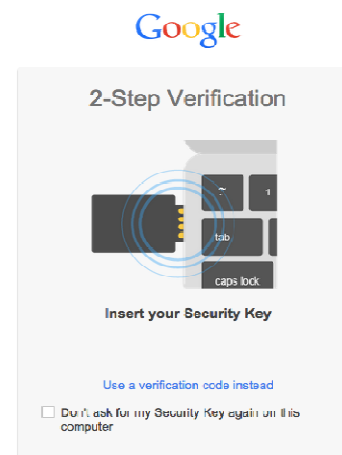
USB指紋スキャナ、MicroSDセキュアエレメント



U2F製品サービスの提供

2014年10月後半に、**Google**は**Chromeブラウザ**でのU2Fサポートを発表。同時に、**Yubico**社と**Plug-Up**社は、公開鍵ハードウェアデバイスのFIDO U2F セキュリティキーを紹介。セキュリティキーを利用して、FIDO U2Fプロトコルベースの強力な認証方式による、高いセキュリティを実現します。

- グーグルアカウントの利用ユーザー向けの強力な2段階確認 (2SV)
- サービスの拡大が簡単
- ウィンドウズやOSX、Linux上で、シームレスに動作する。
- セキュリティキーは、パスワードなどの暗号化する機能を持つ。
- 各アプリケーション毎に、ユニークな公開鍵と秘密鍵のキーペアを作成する。



yubico

FIDO Ready™ の製品

UAF Server / Client	UAF ASM / Authenticator	UAF Cryptography	U2F Authenticator	U2F Server
<ul style="list-style-type: none">• NNL	<ul style="list-style-type: none">• AGNITiO• Diamond Fortress• Egis• GoTrust• NNL• Plug-up• Synaptics	<ul style="list-style-type: none">• Infineon• NXP	<ul style="list-style-type: none">• Entersekt• Infineon• Plug-up• Sonovation• ST• Yubico	<ul style="list-style-type: none">• Duo• NNL• Plug-up• SurePass• Yubico

 FIDO Ready™ products

<http://fidoalliance.org/adoption/fido-ready/>

- FIDO 1.0スペックの完成を発表しました。
- アライアンスへの加入数が急激に拡大しています。
- FIDO対応製品が、発売開始しました。
- FIDO対応製品サービスが提供開始しました。
- 2015年に向けて、大きく飛躍してゆきます。



THANK YOU

FIDO 1.0 スペックが公開されました。

2014/12/9