

JNSA アイデンティティ管理WG主催
「クロスボーダー時代のアイデンティティ管理セミナー」

クロスボーダー時代の 認証技術と海外・国内の動向

EMCジャパン株式会社RSAシステムズ・エンジニアリング部 部長 八束 啓文

ジェムアルト株式会社 IDP事業部 ディレクター OEM & グローバルパートナー 木村 優一

エントラストジャパン株式会社 Senior Technical Sales Consultant CISSP/CISA/CISM 佐藤 公理

1. ユーザ認証の重要性の高まりと課題
2. 解決策としての多要素認証(MFA)
3. 多要素認証(MFA)を構成する認証手段
・方法の紹介
4. 多要素認証(MFA)事例

ユーザ認証の重要性の 高まりと課題

ユーザ認証とセキュリティ

各種サービスにおける本人確認



質問

ご本人確認をさせていただきます。
氏名、住所、生年月日…

コールセンター



身分証

支店



本人確認
は大丈夫
なのか？



指紋

モバイル



ATM

ENTER PIN

— — — — —

ピンコード

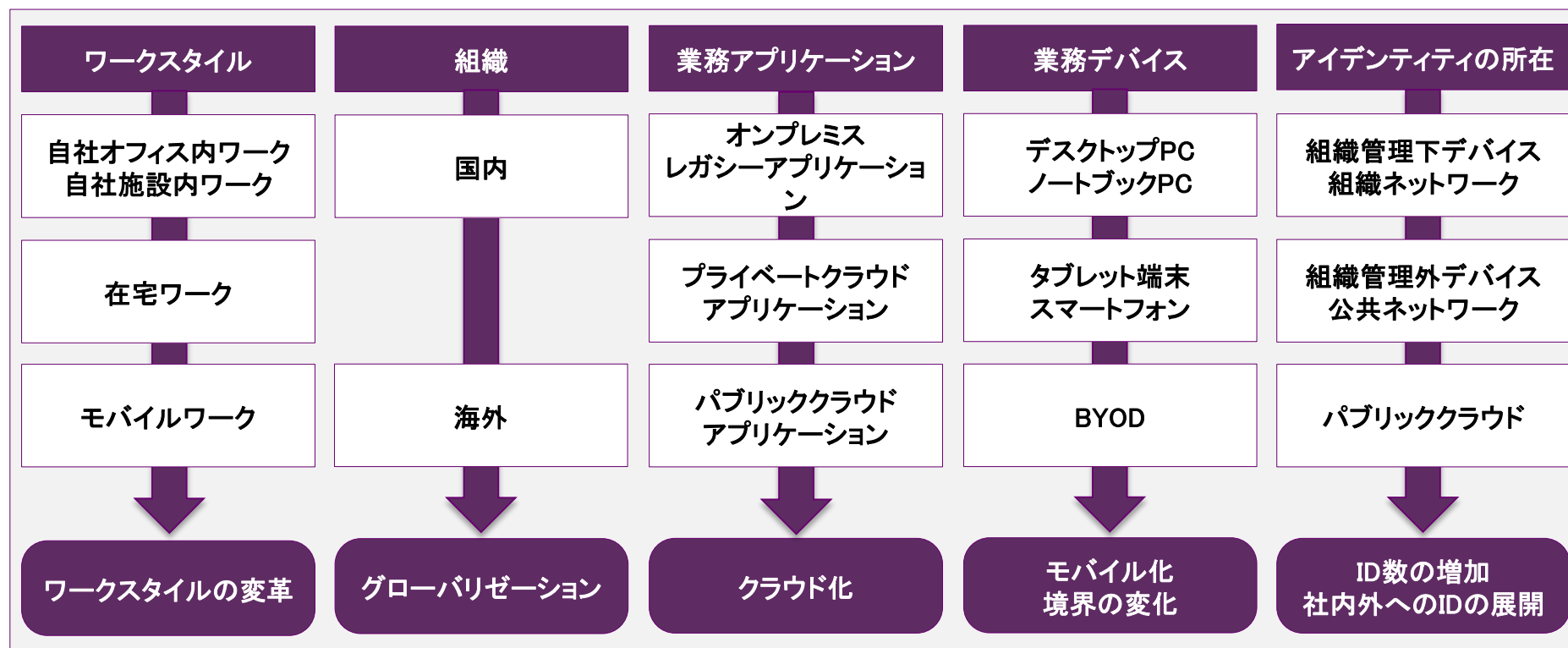
オンライン



ユーザID/パスワード

ユーザ認証の重要性

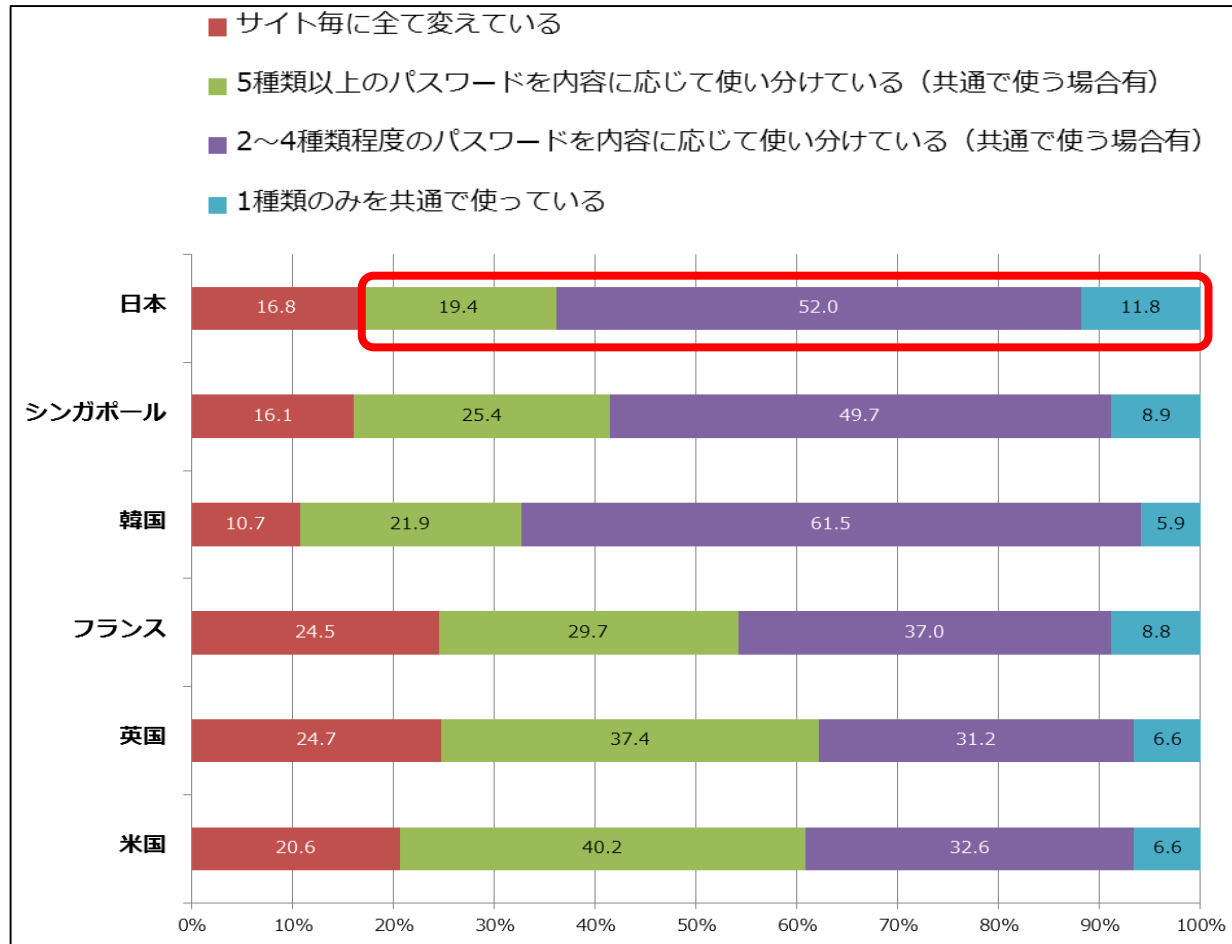
働き方改革・テレワークの推進に伴いユーザの所在および利用が広範囲に及び、認証セキュリティの重要度が高まっている。



ビジネスを取り巻く環境変化に合わせた認証セキュリティが求められている。

認証における課題①-①

使い回しされるパスワード

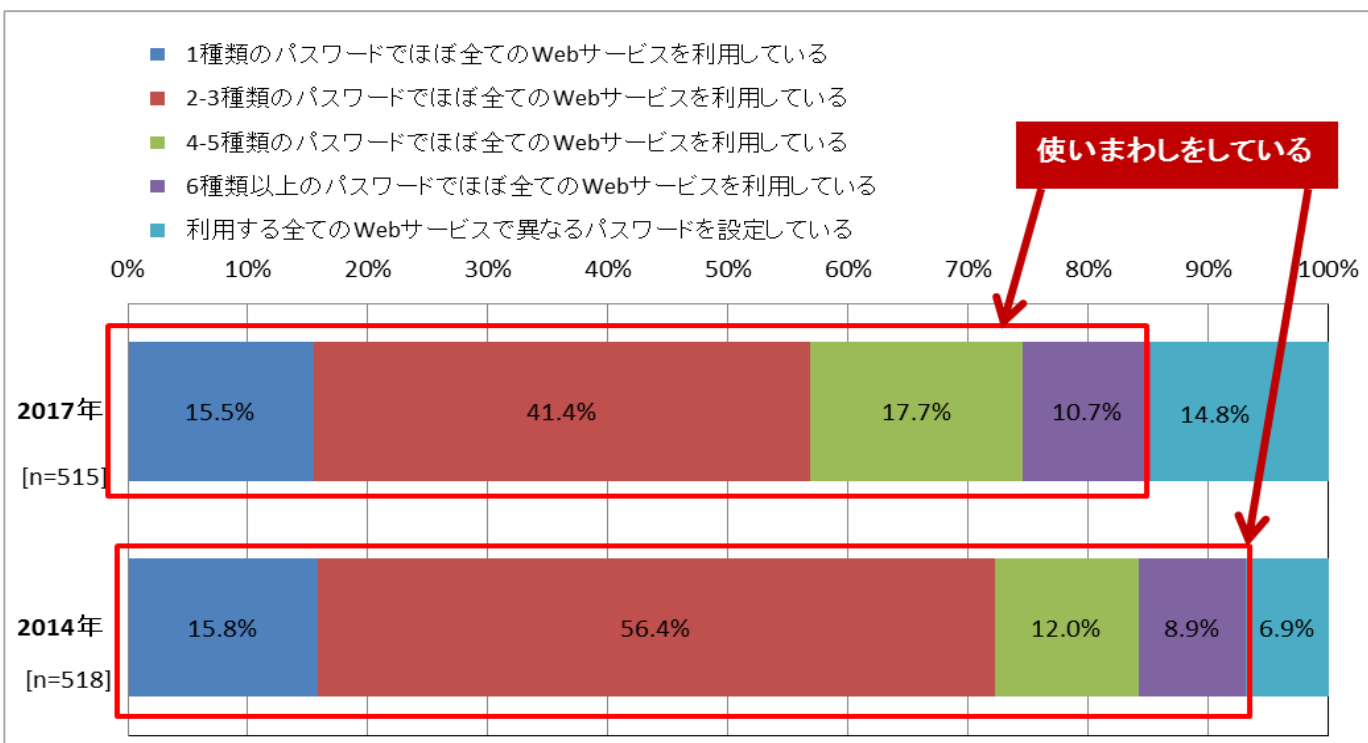


83%のユーザが
パスワードを
使いまわし！！

出展:平成26年版 総務省 情報通信白書 ICTがもたらす世界規模でのパラダイムシフト
第4章 第3節
<http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h26/pdf/n4300000.pdf>

認証における課題①-②

使い回しされ続けるパスワード



パスワードは使い回さないことが前提、使いまわさないことで効果的になるが、実際は、
「パスワードを使い回す人が8割以上」

管理するパスワードの増加に伴い、**企業・組織のコントロール範囲外の使いまわしによるリスク(なりすまし、不正ログイン)が増大**

引用元: パスワードの利用実態調査 2017ー パスワードを使いまわしている利用者が8割以上 | トレンドマイクロ
https://www.trendmicro.com/ja_jp/about/press-release/2017/pr-20171005-01.html

認証強化の課題②-①

攻撃されるパスワード

クラウド・
ウェブアプリへの
攻撃の81%が
盗まれた
ID/パスワード
を使用*

81%

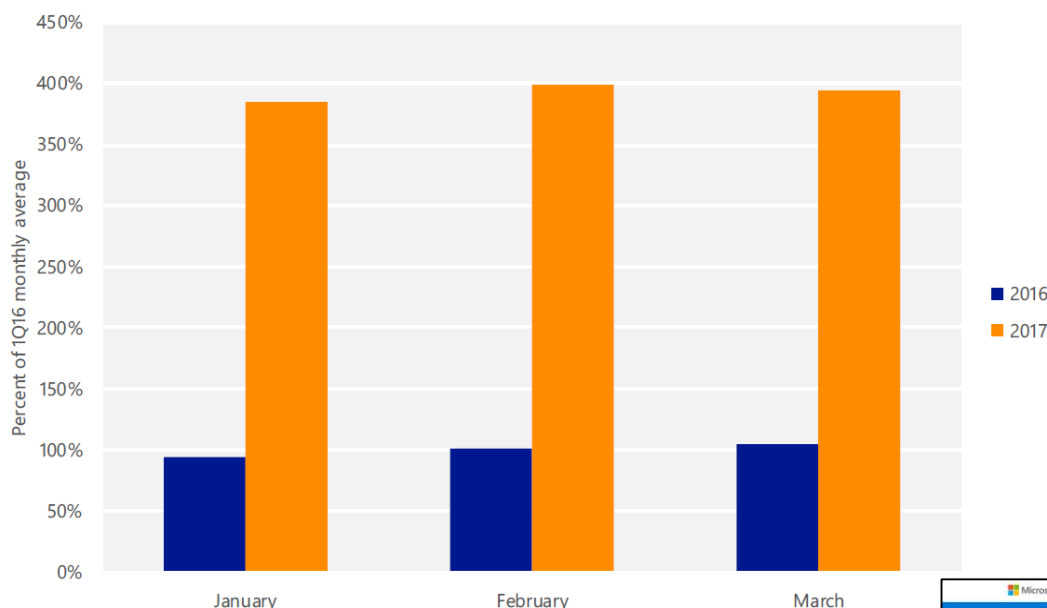
*Verizon Data Breach Investigations Report 2017



認証強化の課題②-②

攻撃され続けるパスワード

Figure 1. Observed accounts under attack during the first three months of 2016 and 2017



引用元: — Global Security Intelligence Report | Microsoft
http://download.microsoft.com/download/F/C/4/FC41DE26-E641-4A20-AE5B-E38A28368433/Security_Intelligence_Report_Volume_22.pdf

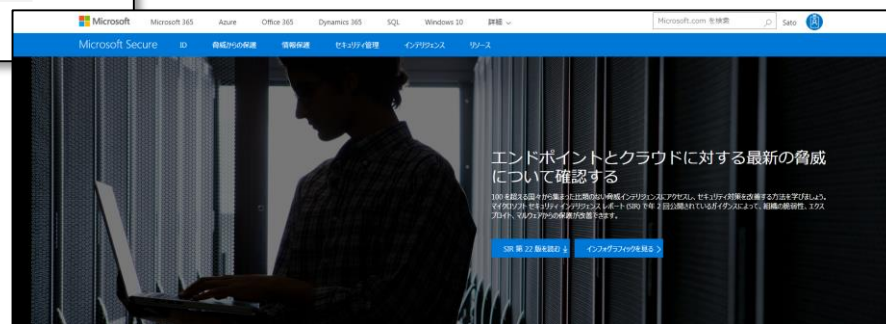
急増するクラウドサービスのアカウントへの攻撃!!

マイクロソフト社によるとMSのクラウドサービス(コンシューマ・エンタープライズ)のアカウントへの攻撃は、

➤ 前年比**3倍**

➤ 原因は、

- ✓ 脆弱かつ容易に推測されるパスワード
- ✓ 弱いパスワード管理



認証強化の課題②-③

さらに攻撃される続けるパスワード

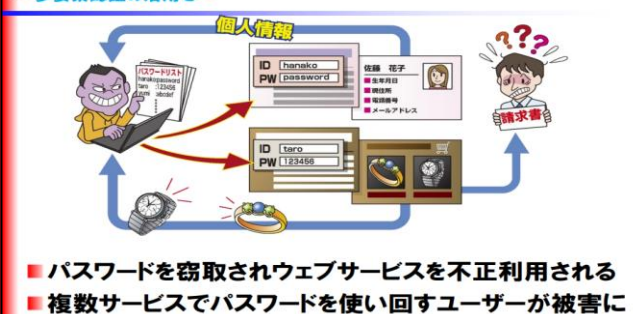
IPA情報セキュリティ10大脅威2017『ウェブサービスへの不正ログイン』

個人編 4位 2016年は5位

【4位】ウェブサービスへの不正ログイン

～多要素認証の活用を～

IPA



組織編 7位 2016年は9位

【7位】ウェブサービスへの不正ログイン

～多要素認証の活用を～

IPA



● 手口/影響

- パスワードの推測攻撃
- パスワードリスト攻撃(別サービスから窃取したIDやパスワード)
- サービスに不正ログインされ、
個人情報の窃取やポイントを不正利用される

パスワードリスト
saro: 198910
jiro: 215544
saburo: 212031
saro: 199234
goro: 194122

● 2016年の事例/傾向

- ブログへの不正ログイン
 - ・ 5月と11月に「Ameba」への不正ログインの被害
 - ・ 11月の攻撃では約59万の不正ログインを確認
- オンラインショッピングへの不正ログイン
 - ・ 「ビックカメラドットコム」にて不正ログインされ、ポイントを不正利用
 - ・ 他のサイトで漏えいしたパスワードが使われた可能性があった



引用元: IPA情報セキュリティ10大脅威2017 個人編 <https://www.ipa.go.jp/files/000059211.pdf>
IPA情報セキュリティ10大脅威2017 組織編 <https://www.ipa.go.jp/files/000059212.pdf>

解決策としての 多要素認証(MFA)

攻撃され続けるパスワードを守るには？

【4位】ウェブサービスへの不正ログイン

～多要素認証の活用を～

● 対策一覧

■ ウェブサービス利用者

- ・ 情報リテラシーの向上
 - － パスワードは長く、複雑にする
 - － パスワードの使い回しをしない
- ・ 被害の予防
 - － パスワード管理ソフトの利用
 - － 多要素認証等の強い認証方式の利用
 - － 利用をやめたウェブサービスの退会



パスワードは推測されにくいものを設定し、
複数のサービスで使い回さない

【7位】ウェブサービスへの不正ログイン

～多要素認証の活用を～

● 対策一覧

■ ウェブサービス運営者

- ・ 被害の予防
 - － 簡単なパスワードを許可しない
 - － 多要素認証の導入



ID PW



利用者が被害に遭わないために
多要素認証等の適切なセキュリティ対策の提供



Reduce risk of credential compromise
by educating users on why they should
avoid simple passwords, enforcing
multi-factor authentication and applying
alternative authentication methods
(e.g., gesture or PIN).

簡単なパスワードを使わない
多要素認証を利用する

引用元：— Global Security Intelligence Report |
Microsoft
http://download.microsoft.com/download/4/E/F/4EFA4D41-EF9A-4B5A-B638-2AC564D210F2/Security_Intelligence_Report_Info_graphic_EN_US.pdf

パスワード強度向上

多要素認証

多要素認証(MFA)とは

多要素認証(MFA-Multi Factor Authentication) 複数の要素・方法・手段を用いて認証を行うこと

多要素認証(MFA)に包含されるものの例(ウェブや本などで見かける用語)

- ・二要素認証(2FA) : 2つの要素・方法・手段を用いて認証。
- ・二経路認証 : 2つの経路(PCとスマホなど)を用いて認証。
- ・OOB認証(アウトオブバウンド認証) : 二経路認証の別の言い方。PCで振込実施する際にPCとオンラインバンク以外の経路(OutOfBand)の経路を使って(スマホなど)認証を実施する。
- ・多段階認証・ステップアップ認証 : 実施している処理や状況に応じて追加で認証要求する仕組み。

多要素認証(MFA)紹介例

各社のMFA紹介資料

セキュリティと利便性のニーズに応じた様々な認証強化方式

RSA SecurID Token ワンタイム・パスワード/二要素認証のデファクトスタンダード



ハードウェアトークン ソフトウェアトークン On-Demand トークン

RSA SecurID Authenticate モバイルデバイスを活用した多要素認証(MFA)



iOS-Android-Android TVデバイス ワンタイムパスワード プッシュ承認 フェンガープリント アイプリント

トークンとスマホを利用した認証方法を紹介
提供: EMCジャパン株式会社

SAFENET認証サービス
各種認証デバイス/方式

ソフトウェアトークンマルチプラットフォーム対応(電子メール配信含む)

ハードウェア BlackBerry iOS OSx Android Microsoft Microsoft SMS Java USB Grid



認証要素:
 > 期限切れなし・電池切れ時は交換
 > シード鍵は企業側に保持可能
 > 簡単に新規ユーザへ再利用可能

gemalto

様々なトークン(HW,SW)を幅広く紹介
提供: ジェムアルト株式会社

Entrust Datacard 認証スイート

エンタープライズのビジネス戦略およびセキュリティポリシーの要求に対して柔軟かつ迅速に対応可能な認証プラットフォームを提供。



ENTRUST DATACARD AUTHENTICATION SUITE
OTP and Certificate-based authentication options

シンプルかつ豊富な認証の選択支を提供

© Entrust Datacard Corporation. All rights reserved. Entrust Datacard

製品で提供する認証方式を幅広く紹介
提供: エントラストジャパン株式会社

製品展開・提案ポイント・ユースケース・対象マーケット等に応じて
MFAの紹介内容を異なる

多要素認証(MFA)を 構成する認証手段・方法 の紹介

1,PKI(証明書)

2,OTP(ワンタイムパスワード)

3,生体認証

1,PKI(証明書)

PKIの歴史と国内例

PKI(Public Key Infrastructure)公開鍵基盤の歴史

1976年	Whitfield DiffieとMartin Hellmanが公開鍵暗号の概念(D-H鍵共有)を発表・提案。
1978年	Ronald Rivest, Adi Shamir, Leonard Adlemanの3人がRSA暗号を提案。
1982年	RSA Data Security創業
1994年	Netscape がSSLを開発。Entrust創業(最初の商用PKI)

国内の行政関連認証局(PKI)

政府認証基盤	GPKI : Government PKI http://www.gpki.go.jp/ 総務省行政管理局が運営
地方公共団体組織認証基盤	LGPKI https://www.lgpki.jp/ 地方公共団体情報システム機構
公的個人認証サービス	JPKI https://www.jpki.go.jp/ 住民基本台帳カード、マイナンバーカード

PKI利用の拡大

PKIの利用用途

Web(サーバ証明書等)

メール(S/MIME,暗号メール、
メッセージ署名)

ドキュメント
(電子署名)

デバイス(デバイス認証,クラ
イアント証明書)

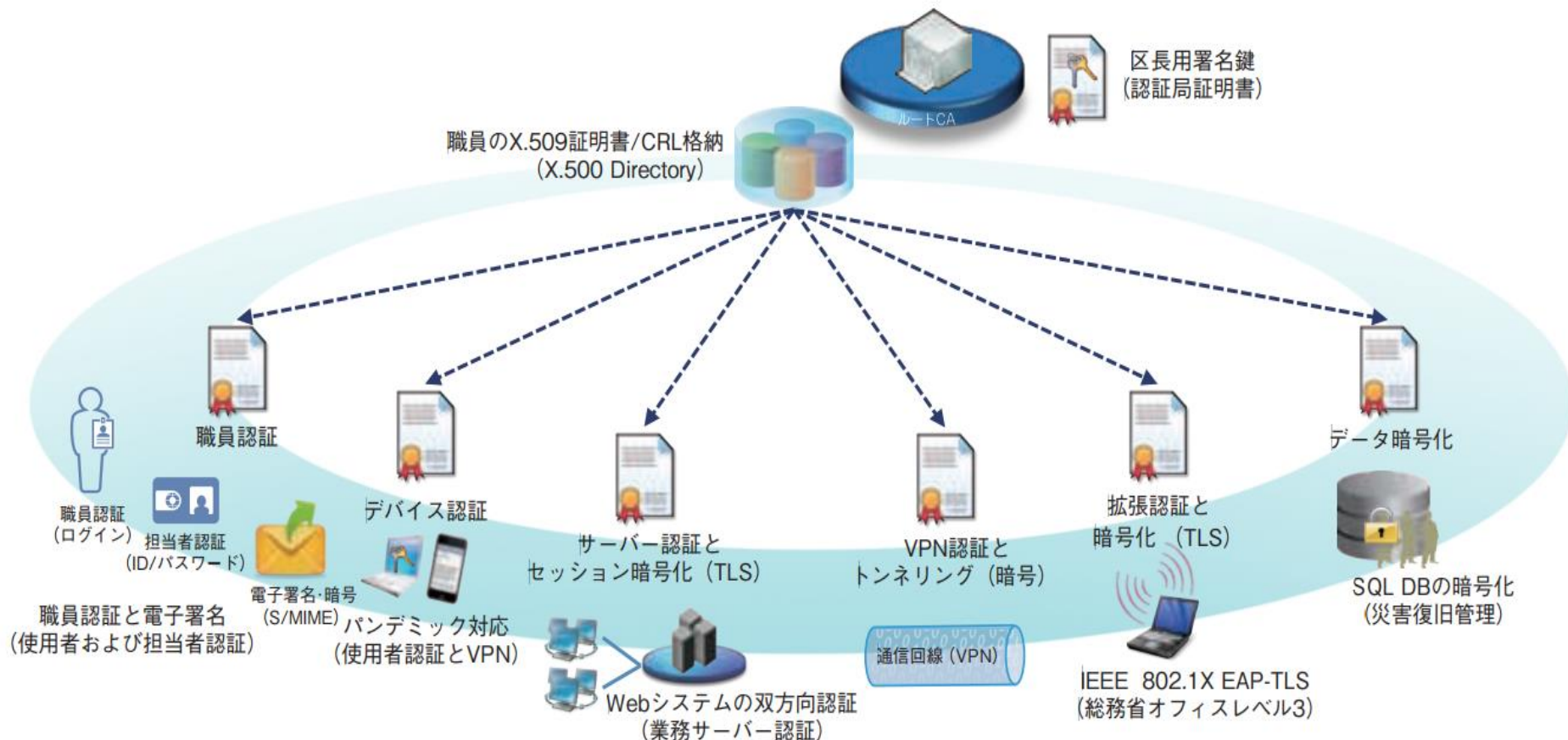
ネットワーク(VPN,有線/無線 (802.1x))

クラウド・IoTの広がり

システムの利用範囲の拡大
境界防御の限界

デバイス認証・クライアント証明書・ネットワークでの
PKI利用の拡大

電子証明書による認証



引用元: 導入事例 足立区役所 https://japan.entrust.com/pdf/Adachi_Kuyakusho.pdf

2,OTP(ワンタイムパスワード)

ワンタイムパスワードとは？

- ✓ 一度だけ使えるパスワード
- ✓ User ID（ユーザー固有のID）
- ✓ シードファイル（ユーザーとサーバーで共有）
- ✓ トークン（ユーザー側）とサーバー側で照合
- ✓ タイムベース（時刻同期）、イベントベース（生成回数）
など

MFA(多要素認証)の一要素としてのOTP



自分自身である

- 指紋、静脈、網膜、声紋など

自分のみ持っている

- トークン、スマートカード、電子証明書など

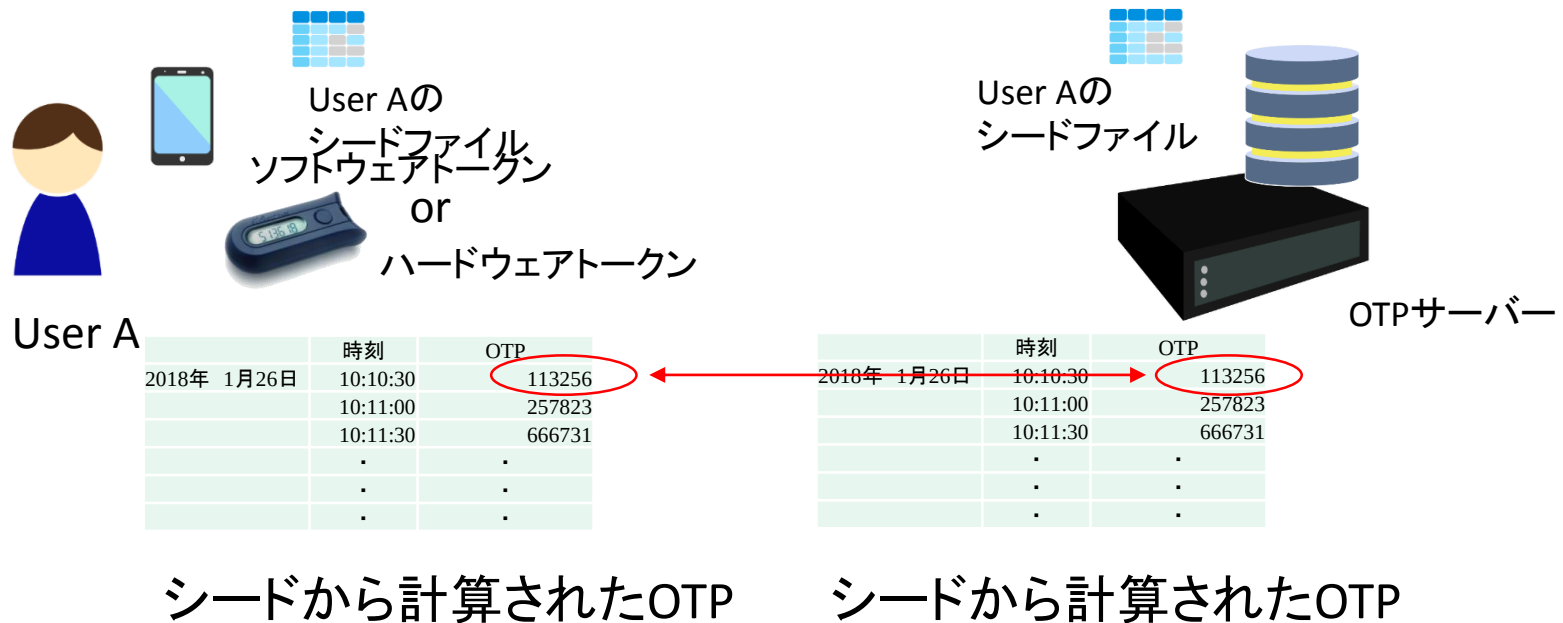
自分だけ知っている

- パスワード、PIN、認証用IDなど

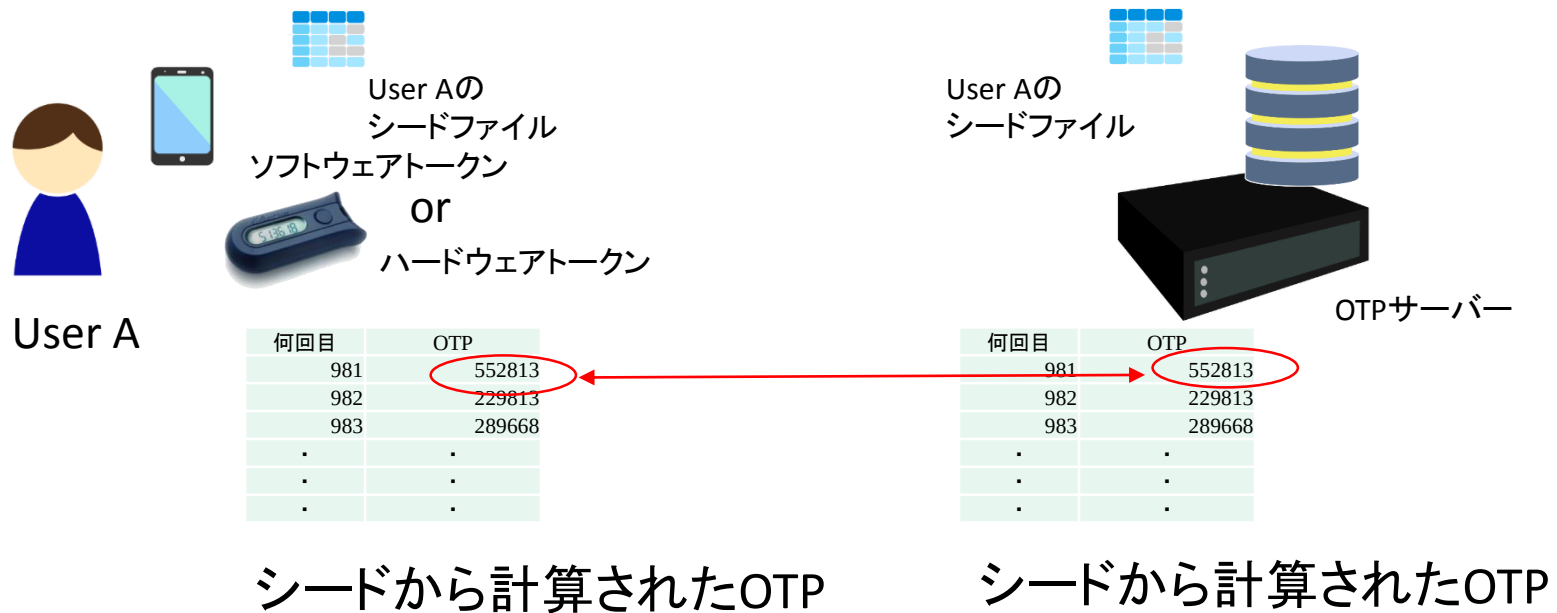
MFA(多要素認証)は
2つ以上の要素の組合せ

例
トークンから計算されたもしくは送付された
OTP(持っている)
とID,パスワード(知っている)
の組合せ

OTP認証の仕組み（タイムベース）



OTP認証の仕組み（イベントベース）



新世代のワンタイムパスワードサービスの特長

クラウドでのサービス提供

利用者によるアクティベーション

プッシュ型 二経路認証(アウト・オブ・バンド)

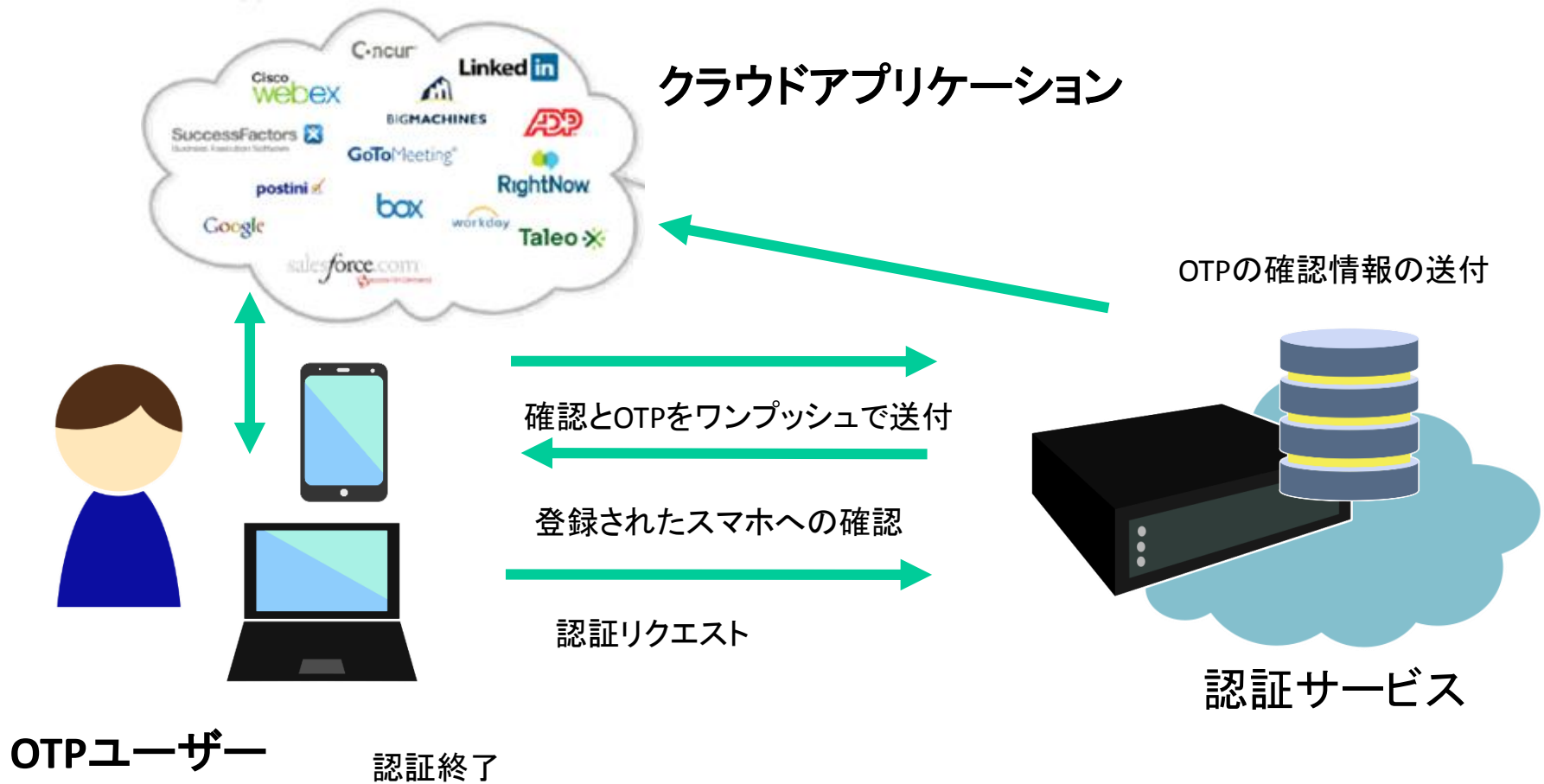
管理コストを大幅に削減

マルチトークンの利用

クラウド型サービス 利用準備(ソフトウェアトークンの場合)



プッシュ型（アウト・オブ・バンド 二経路認証）



3,生体認証

生体認証の歴史と実用化

生体認証 = バイオメトリクス

“Something you are”

“Biometrics” はギリシャ語の “Bio” (生物)と “Metrics” (計測)から派生

1896年	・指紋情報を蓄積して活用する“Henry分類システム”を開発
1903年	・NY州の刑務所で指紋の利用開始
1936年	・虹彩パターンによる認証というコンセプトを提案
1960年代	・顔認識が半自動化 ・FBIが指紋認識プロセスを自動化
1970年代	・音声の振動要素を初めてモデル化 ・US空軍が、音声認識のプロトタイプを開発 ・最初の“ハンドジオメトリ(手の形状認識)商用システム
1980年代	・半自動化された顔認識システムの活用 ・顔認識のために固有顔(アイゲンフェイス)技術の開発
1990年代	・顔検知システムによるリアルタイム顔認識が可能に ・顔、指紋、手、虹彩の認証技術と精度が大幅に向上 ・FBIが、犯罪歴チェック用のIAFIS(指紋認識システム)の運用開始

IT領域での利用開始

生体認証のトレンド

生体認証のトレンドはスマホの普及に同期

✓ 生体認証を使うスマホユーザの急速な成長

- 2017年までに**4.71億**のユーザ数 - 2013年から**900%以上**の成長 ^{*1}



✓ モバイルトラフィックの成長と共にモバイル関連の不正増加

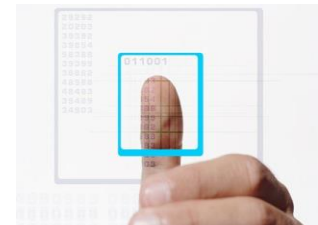
- モバイルのトランザクションの成長
- PCからモバイルへ不正行為がシフト - 2012年の10%から現在は**54%**に ^{*2}

✓ コンシューマがトレンドを牽引、特に銀行の顧客

- **72%**のコンシューマが金融サービスのトランザクションにモバイル生体認証を希望 ^{*3}
- **63%**のATMや支払い時の生体認証に対して有用と回答 ^{*3}

✓ FIDOによるオンライン認証方式の標準化

- **FIDO Alliance** (2012年7月発足)
- UAF(スマホの生体認証など)とU2F(二段階認証方式)



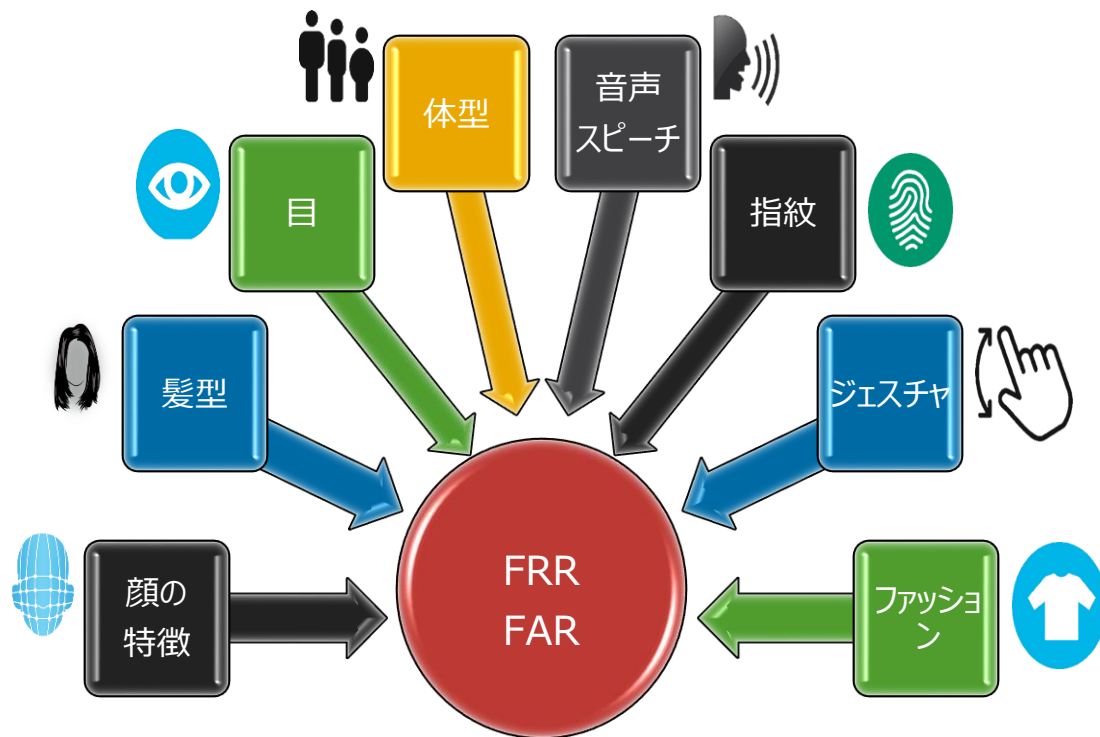
^{*1} Frost and Sullivan

^{*2} RSA Adaptive Authentication Hosted

^{*3} Deloitte

さまざまな生体認証方式と精度

スマホの普及により専用デバイスが不要に

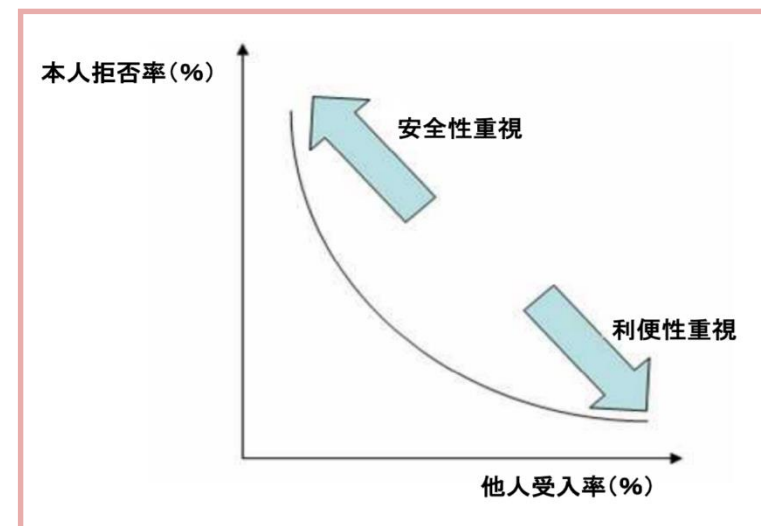


FRR (本人拒否率)

- 誤って本人を拒否する確率
- 高いと利便性が損なわれる

FAR (他人受入率)

- 誤って他人を受け入れる確率
- 高いと安全性が損なわれる



多要素認証(MFA)事例

RSA顧客導入事例(認証ソリューション)

顧客プロフィール 米国フォーチュン100企業



Before

- バラバラなID管理と認証
 - **35種類**の異なるテクノロジーで構築されたSSOと認証システム
- 巨大なIT環境
 - **300,000人**の社員がアクセスする**3,000以上**のアプリケーション
- 煩雑なシステム運用
 - 高い運用コストと低い社員満足度
- 統合されていない複雑なIT環境
 - シャドウITの温床となるリスクが高い

After

- 包括的な認証ソリューションの導入
 - RSA SecurID Access
- リスクベース認証
 - エンタープライズ専用のリスク分析エンジンにより**セキュリティと利便性をバランス**
- MFAの採用
 - **モバイルベースの生体認証とプッシュ承認**
- 段階的な導入
 - 第1フェーズで**100,000ユーザ**に導入済み
- ばらばらなIDストアを1つに統合
 - 運用コストの削減とセキュリティリスクの低減を実現

SafeNet Authentication Service コロンビア政府（金融部門）



Colombia's Fondo Nacional del Ahorro
(FNA)について

- コロンビアでの労働者向けに設立
- 住宅の購入向け
- 47年以上の実績
- 150万人以上のユーザー



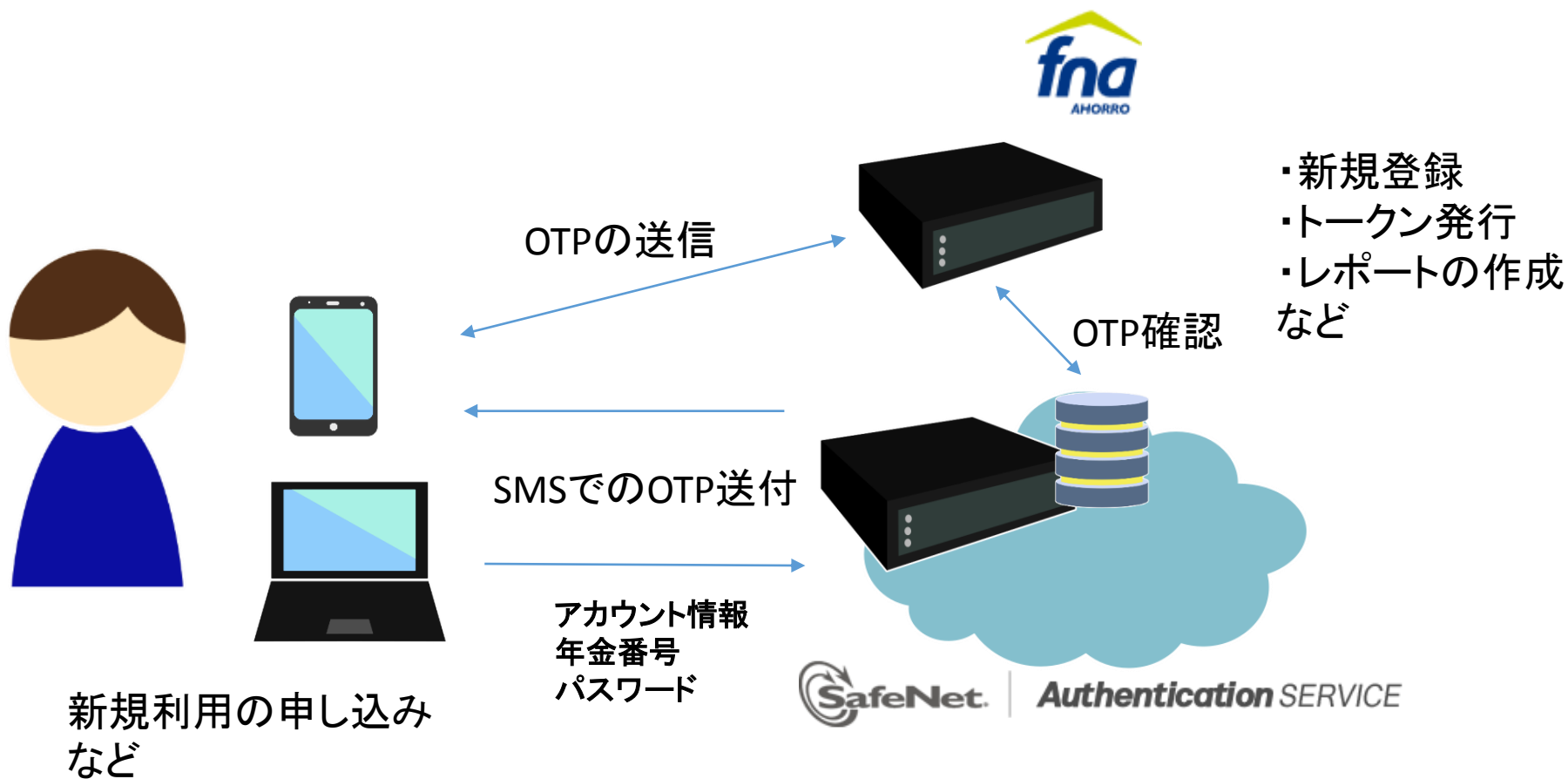
FNAでのSAS導入の背景



Safenet Authentication Service (SAS)の選定ポイント

- ・FNAでは数百万人レベルで利用可能な強力な認証ソリューション
- ・多要素認証でかつシンプルで大幅な変更が必要としなかった
- ・導入から利用開始まで短期間である必要があった
- ・なにより利用者にとって利用が簡単であった

FNAでの利用イメージ



NASAジェット推進研究所はNASAおよびカリフォルニア工科大学の一部門です



- NASAが所有する連邦政府出資研究開発センター（FFRDC）
- 大学による運営（カリフォルニア工科）
- 経営規模：23億ドル
- 従業員数：5,800名
- 敷地面積：167エーカー（約68万m²）
（12エーカー（約5万m²）の駐車場用の借地を含む）
- 建造物数：139棟、移動住宅数：36戸
- 事務所スペース面積：正味673,000平方フィート（約63000m²）
- 非事務所スペース（研究所などの）面積：正味906,000平方フィート（約85000m²）

Gartner Identity & Access Management Summit 2017（米国）Entrust Datacardセッション発表資料 より引用

エントラスト顧客事例(IntelliTrust /Identity Guard)

業種：航空宇宙

導入目的：従業員のアクセス管理の効率化



背景 / 課題



- 長年にわたりスマートカードを利用してきた
- ユーザーは、政府機関向け企業向け等、複数のスマートカードを管理しなければならず煩雑だった。
- モバイルの利用が拡大
 - カードは適さない環境になった
- SaaSアプリケーションの導入
 - カードは適さない環境になった
- アプリケーション数の増大
 - 頻繁に認証が必要となる

ソリューション

Mobile Smart Credential (MSC) が提供する インテリジェントアクセス

- 自動的にログイン/ログアウトが可能のため、ユーザーの操作が不要
- VPN, クラウドアプリケーションのシングルサインオン
- 1台のモバイルデバイスで認証可能（複数のスマートカードを持ち歩く必要がなくなる）



Gartner Identity & Access Management Summit 2017（米国）Entrust Datacardセッション発表資料 より引用

1つのスマホ、複数の利用ケース

派生モバイルクレデンシャル(Derived Mobile Credential)により、ユーザビリティを犠牲にすることなく「高いセキュリティ強度」を実現

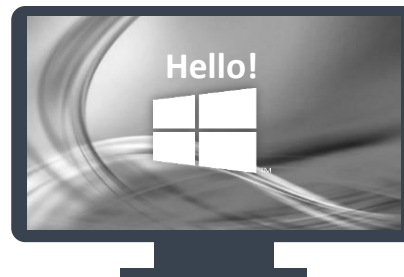


スマートフォン

EMMアプリケーションに対する
ネイティブ認証 (Mobile Iron、
AirWatch)



モバイルプッシュ



Windowsデスクトップ

無線 (Bluetooth) 経由でワ
ークステーションに
ログイン



ウェブ、VPN

セキュアなモバイルプッ
シュを通じてVPNやSaaS
アプリに対する認証を実
施



物理アクセス

NFCやBluetooth経由でドア
にアクセス