

# パスワードという名のセキュリティリスク ~パスワードのない未来~

マクニカネットワークス株式会社

第3営業統括部 第1営業部

課長代理 プロダクトマネージャー 恒川 雅俊

モバイルアイアン・ジャパン

シニアチャネルセールスマネージャー 李 奇



# アジェンダ

## □現状

- ・ パスワードの課題
- ・ モバイルの現状

## □解決策

- ・ パスワードレスソリューション



password:  
0123456789

Password

\*\*\*\*\*

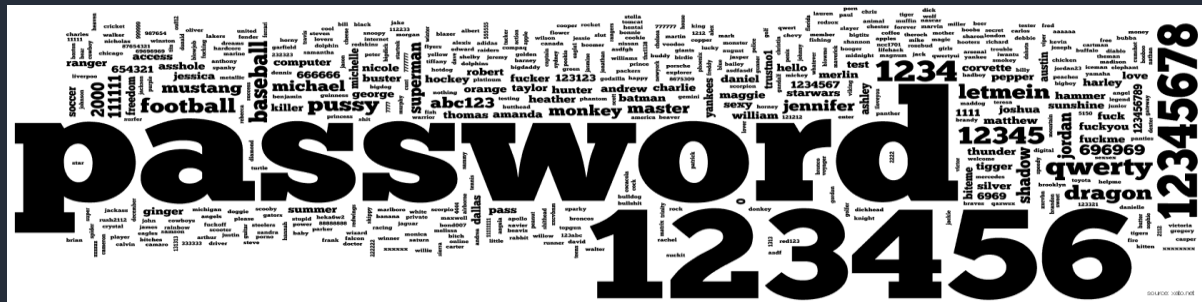


# パスワード

“知っている” = 本人とみなす



# パスワードというセキュリティリスク



弱いパスワード  
デフォルトパスワード  
...



# フィッシング パスワードの売買 ・・・

# 「この中で一番強いパスワードは？」

① Mond@y

② Qwerty

③ Mountain-sunny-nichiyou

1. パスワードの定期的な変更を行ってください。なお、設定される際は、英大文字、英小文字、数字または記号を用いて、8～20文字で、第三者に推測されにくいパスワードにしてください。また、「IDと同じ情報」が含まれていない、「同じ文字や数字の連続」ではない、「生年月日」「電話番号」と同じになっていないなどの点にも、ご注意ください。

2. 他サイトと同じパスワードまたは、それらが容易に類推されるパスワードの使いまわしをすることはお控えください。複数のサイトで同じパスワードを使いまわしされていると、第三者に不正にログインされるリスクが高まります。



My password  
~~123456~~  
~~qwerty~~  
AzEt8MbBFI

- ①覚える
- ②変える



- ①メモる
- ②使い回す





# 世の中の大きな環境変化





デバイスが変わった

働く環境が変わった





モバイルが全ての中心に

A man with a beard, wearing a dark blue suit, white shirt, and dark tie, is holding a black smartphone in his right hand. The background is slightly blurred.

# 80

スマートフォンを  
1日に見る回数は80回

A close-up of a laptop screen displaying a bar chart with red and blue bars. The text 'https:' is visible on the screen. The background is blurred.

# 52%

スマートフォンからの  
Webアクセスが52%

A person's hands are holding a smartphone, with the screen showing a bright light. A laptop keyboard is visible in the foreground. The background is blurred.

# 3X

スマートフォンは  
PCの3倍の台数





# BUSINESS

アプリのカテゴリで  
ビジネスが人気第2位



Slackのアクティブユー  
ザは700万人/日超



# 5G

4Gより  
はるかに高速な5G

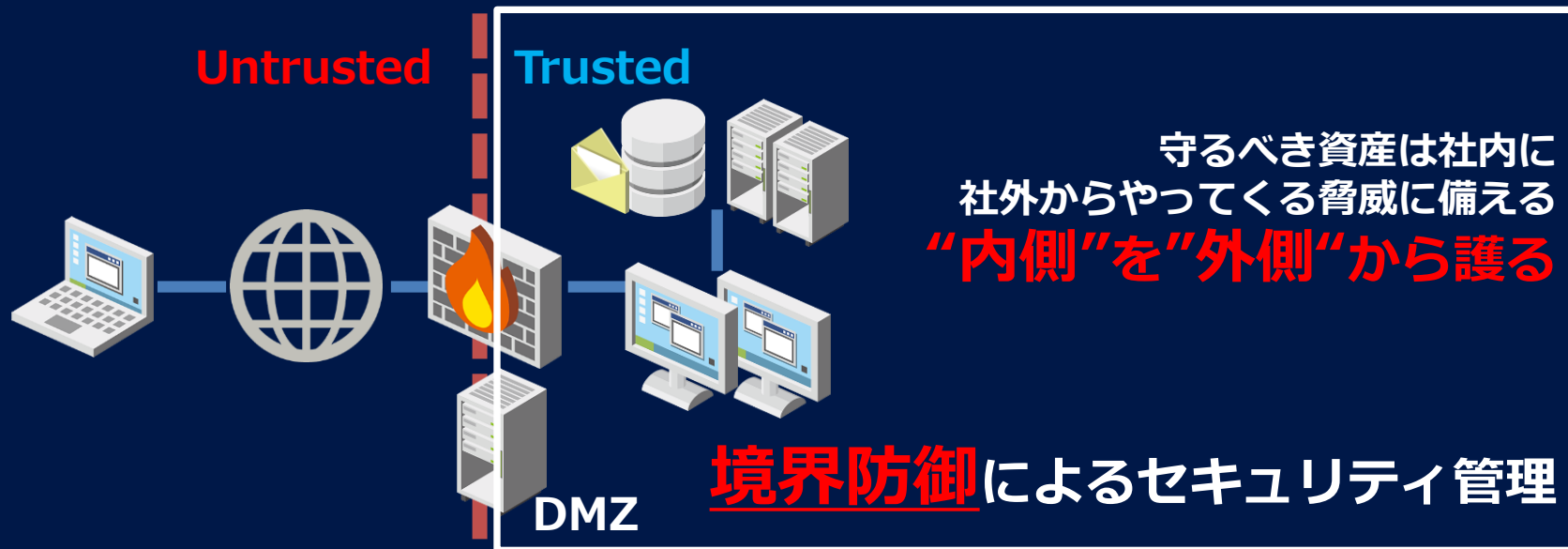


ユーザーの意識が変わった



# これまでの仕事場/~~今までの~~セキュリティ

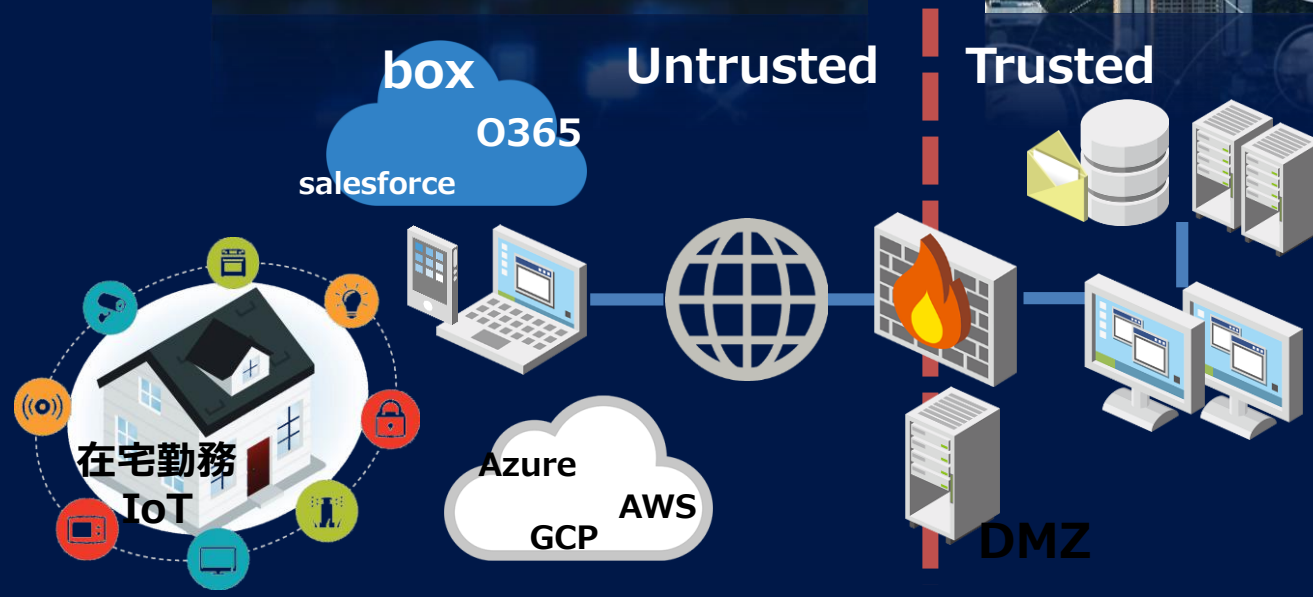
- ・基本的に仕事は社内・オフィスで行う
- ・一部の従業員が外出時にリモートアクセスをする
- ・インターネットはデータセンタ経由でアクセスをする





資産は“内側”にあるとは限らない  
クラウド利活用 @

“外側”との連携  
モバイル化



資産は“内側”にあるとは限らない  
クラウド利活用 @

“外側”との連携  
モバイル化

# 境界防御の限界



変化する環境で必要とされる  
新しいセキュリティアプローチ



- 新しいアクセスをどのようにチェックするか？

## Where?

ネットワーク

ネットワークゾーン

- Trusted
- Untrusted
- DMZ

例えば、FireWall

## Who?

ユーザ

ユーザグループ

- 部署
- 役職
- 特権ユーザ

例えば、ADサーバ

## What?

デバイス

- 管理下のデバイスか？
- セキュアな状態か？

例えば、資産管理・MDM

## 境界防御

ネットワーク

ユーザ

デバイス

- ネットワークの信頼レベルに応じたアクセス制御
- 社内ネットワークに接続したユーザとデバイスは**信頼される**



## ゼロトラスト

(決して信用しない)

ネットワーク

ユーザ

デバイス

- ネットワークを信頼しない  
(**すべてUntrusted**と想定)
- **ユーザ**と**デバイス**の信頼レベルに応じたアクセス制御

# 最適なアプローチとは？



ID志向の  
アプローチ



デバイス、アプリ、脅威の  
可視性に限界

**パスワードは  
セキュリティリスク**



ゲートウェイ志向の  
アプローチ



デバイス、アプリ、脅威の  
可視性に限界

**企業トラフィックの25%は  
企業ネットワークを通っていない**



デバイス志向の  
アプローチ



ユーザー、デバイス、アプリ、  
ネットワーク、脅威を包括的に相関  
分析

**モバイルが企業を中心に**



モバイルを  
中心に考える



ユーザー、デバイス、アプリ、  
ネットワーク、脅威の  
包括的な相関分析

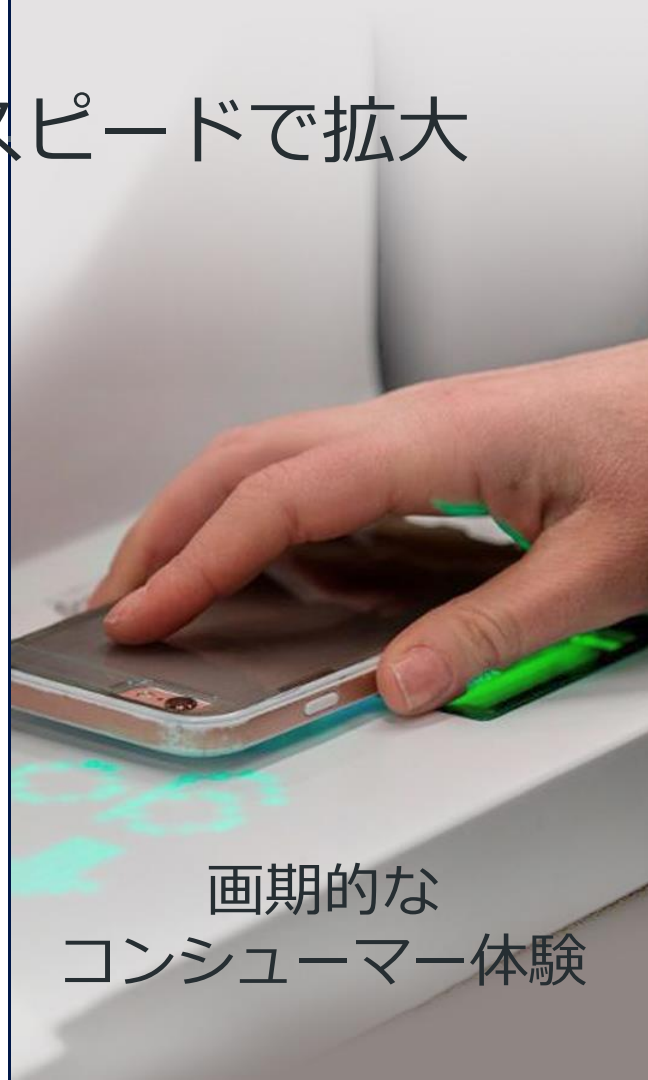
モバイルのパワーは想像以上のスピードで拡大



常時利用



生体認証が  
IDになり代わる



画期的な  
コンシューマー体験

A close-up of a person's face, focusing on the eye area. A futuristic, glowing eye overlay is visible on the left side of the image. The background is dark with some bokeh light effects.

# VISION

## モバイルを

企業資産へのアクセスの**鍵**とすることで

**パスワード**という“脆弱性”**を終わり**にする

# 脱・パスワードの流れ

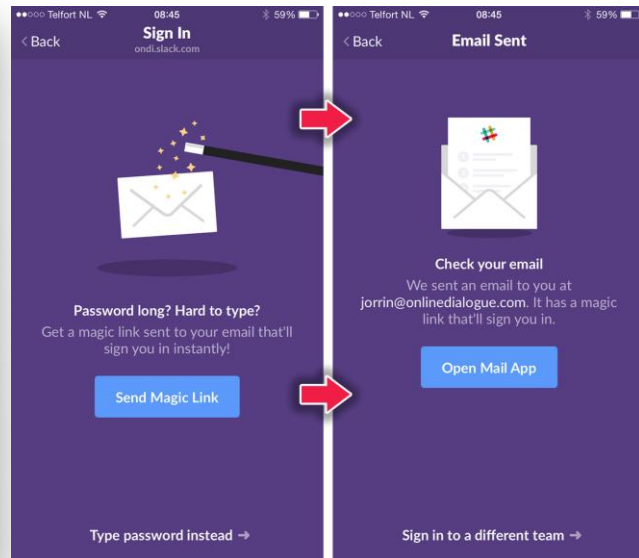


# 86%

の会社はパスワード以外の  
認証方式を採用したい、更  
にパスワードを利用しなけ  
れば、セキュリティ侵害を劇  
的に減らすことができると信  
じている



# 他に様々な認証方式



# 我々の提案: パスワードのない世界

## PHASE 0

**Access +  
MFA**

*Mobile to cloud for  
managed devices*

## PHASE 1

**iPhone  
as identity**

*Any device  
to cloud*

## PHASE 2

**Any device  
Any login**

*Zero password  
everywhere with high  
security for unmanaged  
devices*

## PHASE 3

**Any device  
Any login  
Any UEM**

*Zero password  
experience everywhere  
with high security for  
unmanaged devices*

# パスワードのない世界(デモ)

---

- パスワードを使わずにモバイルデバイスをEMMに登録する
- パスワードを使わずにSFDC、Box、Office 365、G Suite等の企業アプリにログインする
- モバイルアイアンで管理されていないパソコンから、管理デバイスでQR Codeをスキャンして、パスワードを使わずにログインする

# なぜモバイル？



- 肌に離さず持ち歩いている
- 既に毎日の生活に浸透している、モバイルを使って電車に乗ったり、支払を行ったり、重要な情報を扱ったりしている
- 生体認証等の高度なテクノロジーが実装されている



# モバイル業界のリーダー

**19,000社** のお客さま

**1,100万** ビジネスクリティカルなエンドポイント

**80件以上** セキュリティの特許

**105%** リニューアル率  
(アップグレード含む)

**380社以上** エコシステム・パートナー

**9年連続** ガートナー社のMagic Quadrantでリーダー評価

**7年連続** 日本国内EMMシェア一位 (ITR調べ)

**2018** 年の市場評価



# ガートナー社の評価

2019 Magic Quadrant for UEM Tools\*<sub>1</sub>

リーダー評価のベンダの中で

Peer Insights Customers' Choice\*<sub>2</sub>

も同時に受賞しているのはMobileIronのみ

2018年



2019年

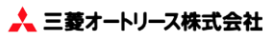
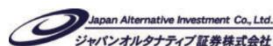


\*<sub>1</sub> [2019 Magic Quadrant for UEM Tools](#)のダウンロードサイト

\*<sub>2</sub> Peer Insights Customers' Choice: 実際に利用しているお客さまの声に基づく評価。

# 日本のお客さま（一部抜粋）

<https://www.mobileiron.com/ja/customers/case-studies>





デバイス管理



クラウドセキュリティ



iOS/Android専用アンチウィルス



# まとめ

- パスワードはセキュリティのリスクとして考えられている、パスワードを使わない認証方式が必要とされている
- モバイルアイアンではパスワードのない世界を提案する; モバイルデバイスからも、パソコンからもパスワードを入力せずログインできる
- パスワードをなくすことで、セキュリティと利便性はトレードオフではなく、初めて両立できるようになる
- モバイルアイアンのMTDでデバイス、情報をしっかりリスクから守り、真のセキュリティを実現できる

## 【お問い合わせ先】

マクニカネットワークス株式会社

MobileIron製品担当

TEL : 045-476-1997

Email : [mobileiron\\_sales@cs.macnica.net](mailto:mobileiron_sales@cs.macnica.net)

- 本資料に記載されている会社名、商品、サービス名等は各社の登録商標または商標です。なお、本資料中では、「™」、「®」は明記しておりません。
- 本資料は、出典元が記載されている資料、画像等を除き、弊社が著作権を有しています。
- 著作権法上認められた「私的利用のための複製」や「引用」などの場合を除き、本資料の全部または一部について、無断で複製・転用等することを禁じます。
- 本資料は作成日現在における情報を元に作成されておりますが、その正確性、完全性を保証するものではありません。