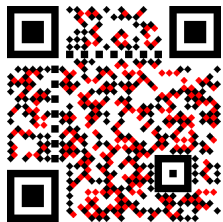


「FIDOとPasskeyの進化」 ～ ID/Passwordからの脱却： 安全な未来への鍵～



次世代セキュリティへ進化する注目のデジタル認証技術を理解する



Our Goal 01

認証の現状

現在の認証システムは、多数のパスワードを管理する必要があります。また、これに伴うセキュリティリスクが高まっています。



Our Goal 02

パスワードレス認証の 革新

パスワードレス認証は、利便性とセキュリティを両立するアプローチとして注目を集めています。企業はこの動向に対応する必要があります。



Our Goal 03

セキュリティ戦略の再考

この新しい認証技術を導入することで、企業は未来のセキュリティ課題に備えた戦略的な基盤を構築できます。



Our Goal 04

XXX

XXX

データ漏洩の増加と多数のアカウント管理が、 現代社会のセキュリティ脆弱性を高める

01

データ漏洩数の増加

年間約80億件のデータ漏洩が発生しており、企業と個人の情報が脅威にさらされています。これにより、信頼できる認証方法の必要性が急速に高まっています。

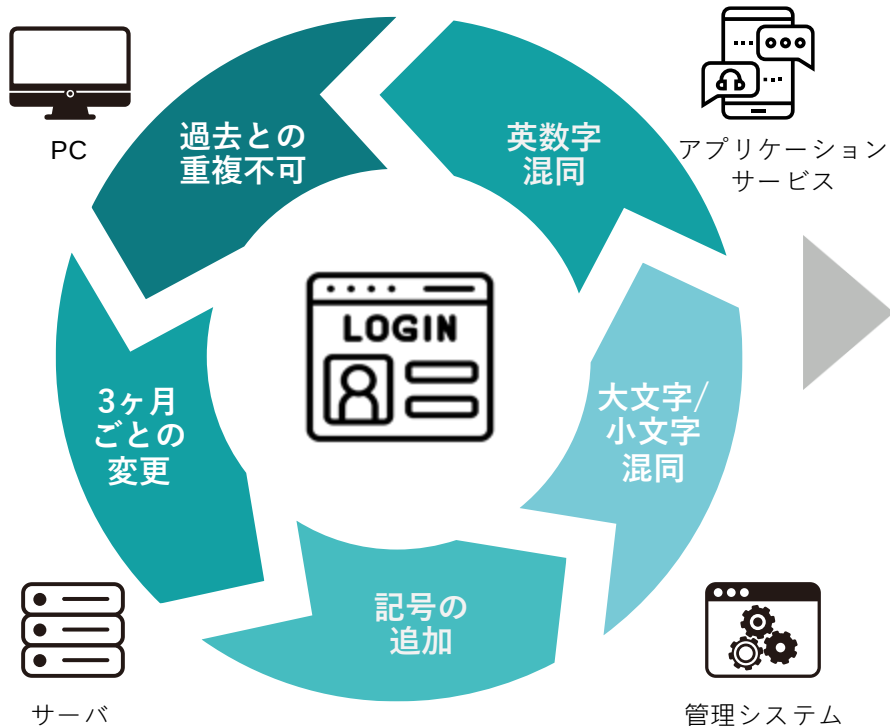
02

増え続けるアカウント数

多くのユーザーが平均100以上のオンラインアカウントを管理しており、これがセキュリティリスクを増大させています。パスワード管理の課題が深刻化しています。

ID/パスワードの複雑化と流出原因

どんどん複雑化するパスワード



パスワード漏洩の4つの原因



複数のウェブサイトで、
同じパスワードを
繰り返し使用



フィッシング攻撃による
情報流出



第三者サービスの
データ漏洩



個人的要因による
情報漏洩

脆弱なパスワード管理と人為的ミスが、サイバー攻撃の脅威を助長



パスワードの重複

多数の複雑なパスワードを管理する必要があり、ユーザーはパスワードを頻繁に再利用しがちです。パスワードの複雑化は管理を困難にし、安全性の低下を招きます。



人為的エラーに起因する脆弱性

単純なパスワード選択や不適切な保管がセキュリティリスクを増加させ、攻撃者による不正アクセスを招く可能性があります。係る脅威は増え続けています。

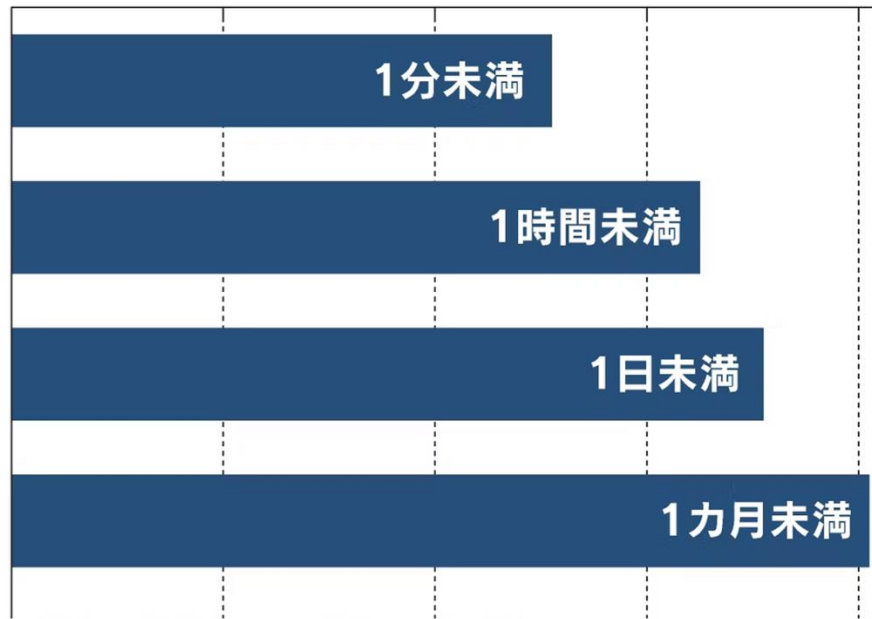


サイバー攻撃の増加数

フィッシングやランサムウェアといった攻撃手法が進化し、年間約80億件のデータ漏洩が発生しており、日々の脅威となっています。適切な対策が不可欠です。

生成AIがパスワードの解読にかかった時間

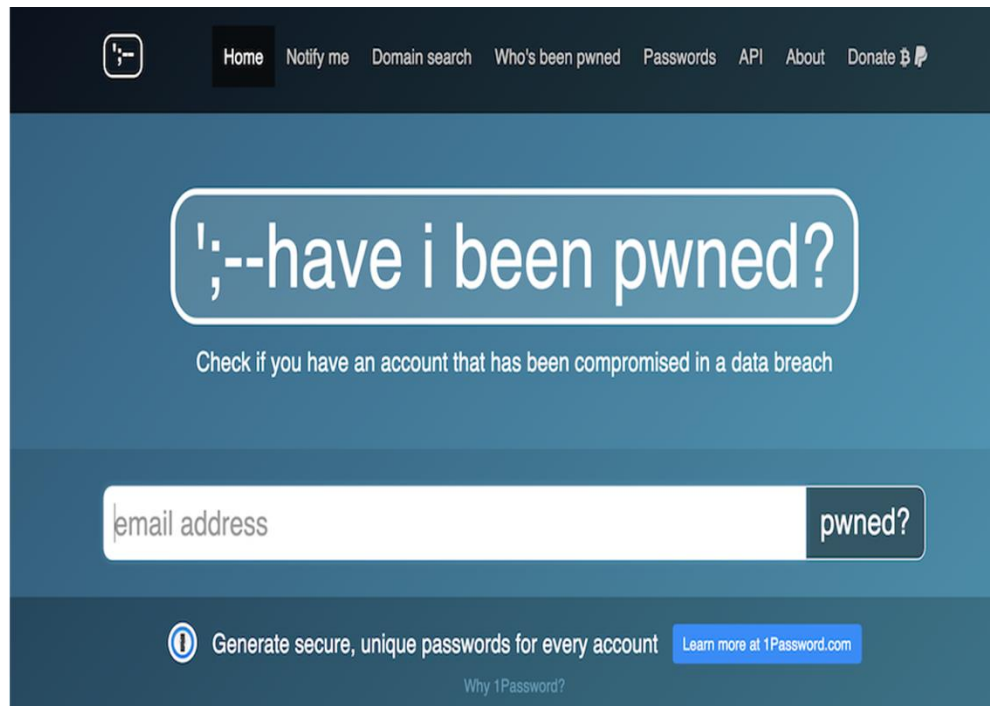
0 20 40 60 % 80



1560万件中

51%

は1分未満で解読可能



引用:日経XTech「パスワードは流出している」が当たり前、管理方法を見直して不正ログインを防ぐ
引用:日経XTech 使い回さずに覚えるのは大変、大量のパスワードの管理方法を教えて

- ① ダークウェブで
確認されている認証情報
120億件以上
- ② 82% は重複利用
- ▼
- パスワードは
流出している/
使い回されている
- 前提での運用が必要

パスワードの脆弱性を克服するため、 FIDOアライアンスが新たな認証技術を提供

01

パスワードの脆弱性

パスワードは総当たり攻撃やフィッシングに弱く、しばしば不正アクセスの原因となります。サイバーセキュリティの脅威に対処するには限界があります。

02

FIDOアライアンスの 設立

2012年、GoogleやMicrosoftなどがFIDOアライアンス設立に参加し、安全で使いやすい認証方法を世界標準化しました。これにより、パスワード依存からの脱却が期待されます。

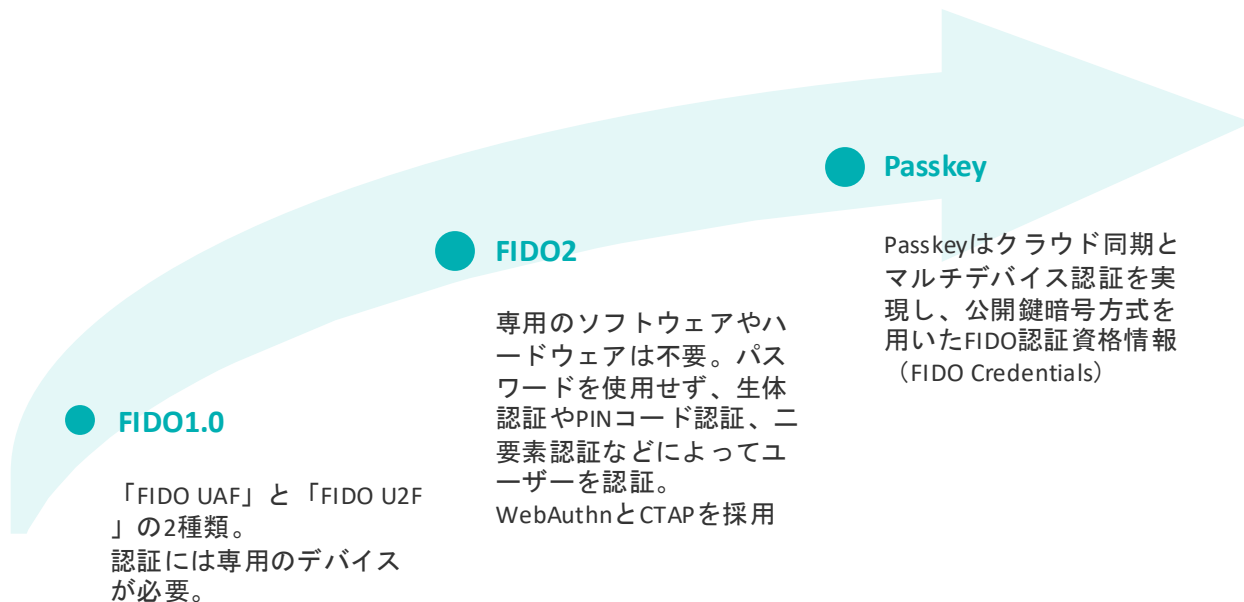
どんな企業がパスワードに危機感を持ち取り組んでいるか

理事会レベルメンバー

etc...

FIDO (Fast IDentity Online)



それぞれのFIDOの違い

	FIDO1.0	FIDO2	Passkey
目的	主に 2 要素認証(2FA)を提供	パスワードレス認証を実現	FIDO2を基盤とした パスワードレス認証
認証方法	セキュリティキー(USBなど)を 使った認証	セキュリティキー、 生体認証を利用	生体認証や端末に保存された 暗号鍵を使用
パスワードレス	×(2FAの一部)	○	○
使用例	企業向けの2FA (セキュリティキー)	Webアプリ、オンラインサー ビス、モバイルアプリなど	iCloudやGoogleアカウントを利用 したログイン
ユーザ体験	セキュリティキーの 常時携帯が必要	物理デバイス、スマホ、 PCでのシームレスな認証	シームレスで簡単な認証、 端末間での同期が可能

FIDOは公開鍵暗号と生体認証を組み合わせ、 安全かつ便利なパスワードレス認証を実現

公開鍵暗号方式の仕組み

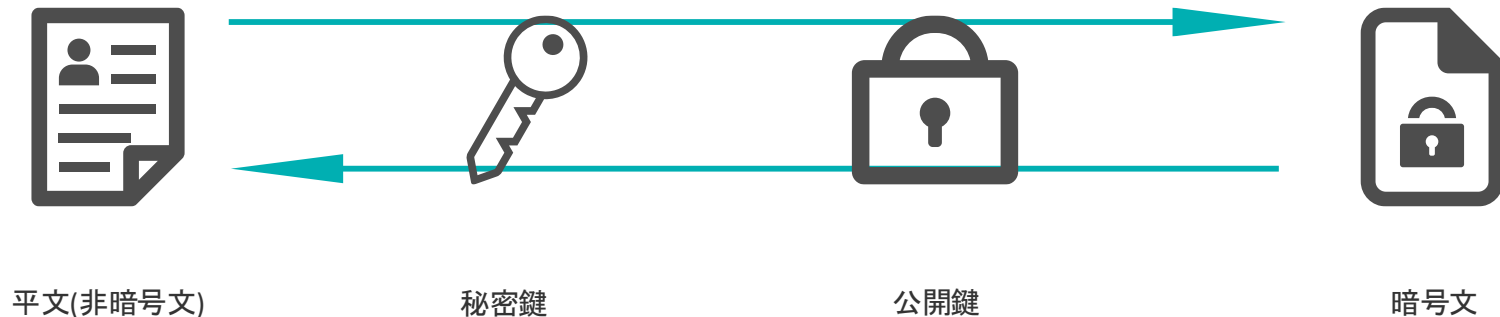
FIDO認証では秘密鍵をデバイスに保存、公開鍵のみをサーバーに保管。これにより、第三者の不正アクセスを防ぎます。

生体認証との統合

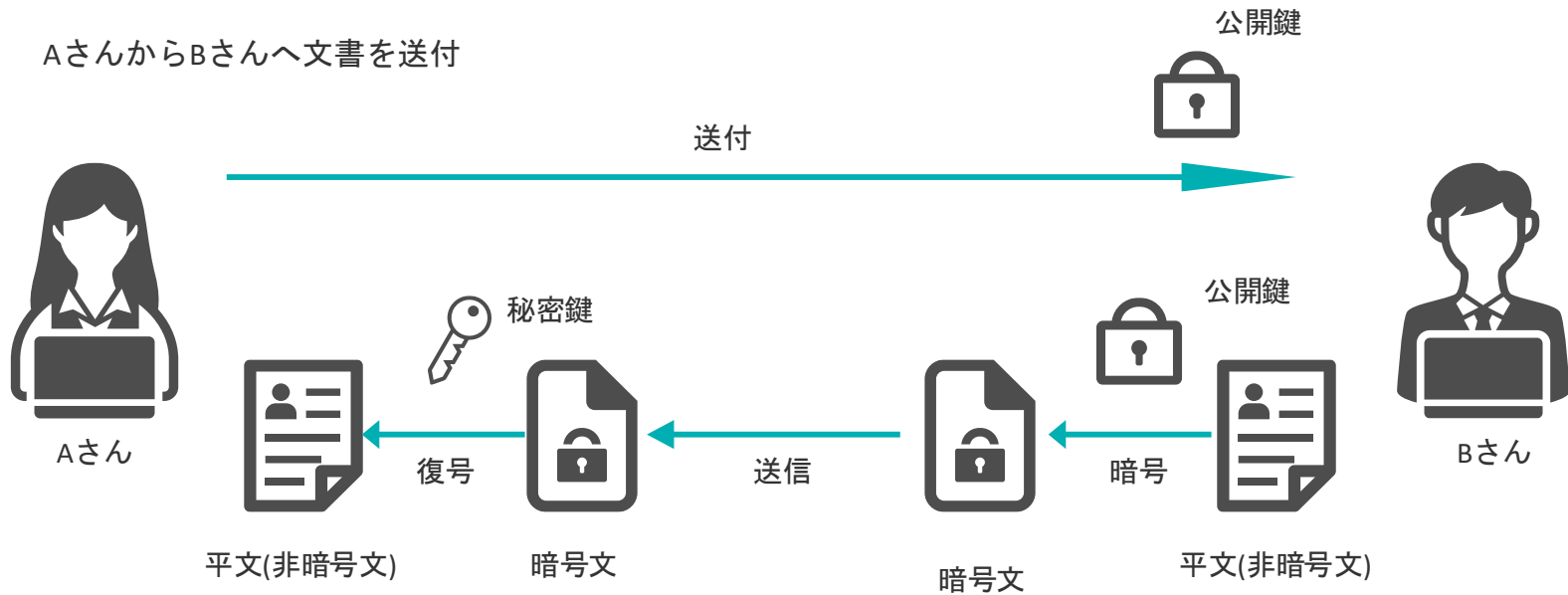
指紋や顔認証をFIDO認証と一体化し、本人確認の精度を向上。パスワードを使わない安全な認証方法を提供します。

PKIとは

PKI(公開鍵暗号基盤 Public Key Infrastructure)とは、公開鍵と秘密鍵のキーペアからなる「公開鍵暗号方式」という技術を利用。暗号化と復号を行うことで安全なやりとりを行う。



暗号化と復号



デバイス間のシームレス同期とクラウドベースでの安全な鍵管理が、 Passkeyの最大の強み

シームレス同期

Passkeyはデバイス間での認証情報のシームレスな同期を実現し、利便性と効率を向上させます。ユーザー体験を大幅に改良しています。

クラウドで鍵を安全管理

Passkeyはクラウドベースで暗号化された鍵を安全に管理し、セキュリティリスクを低減しつつ、高度な保護を提供します。

FIDO導入で、GoogleやMicrosoftなどがセキュリティを強化し、コスト削減を実現

01

Google

GoogleはFIDO認証を採用し、従業員のパスワード漏洩を99.9%防止。クラウドサービスのセキュリティが劇的に向上しました。

02

Microsoft

MicrosoftはクラウドサービスでFIDOを活用し、パスワードリセット対応コストを大幅に削減。生産性が向上しました。

03

LINEヤフー

アクティブユーザは、2,700万人。スマートフォン利用者の50%はPasskeyによる認証。

04

KDDI

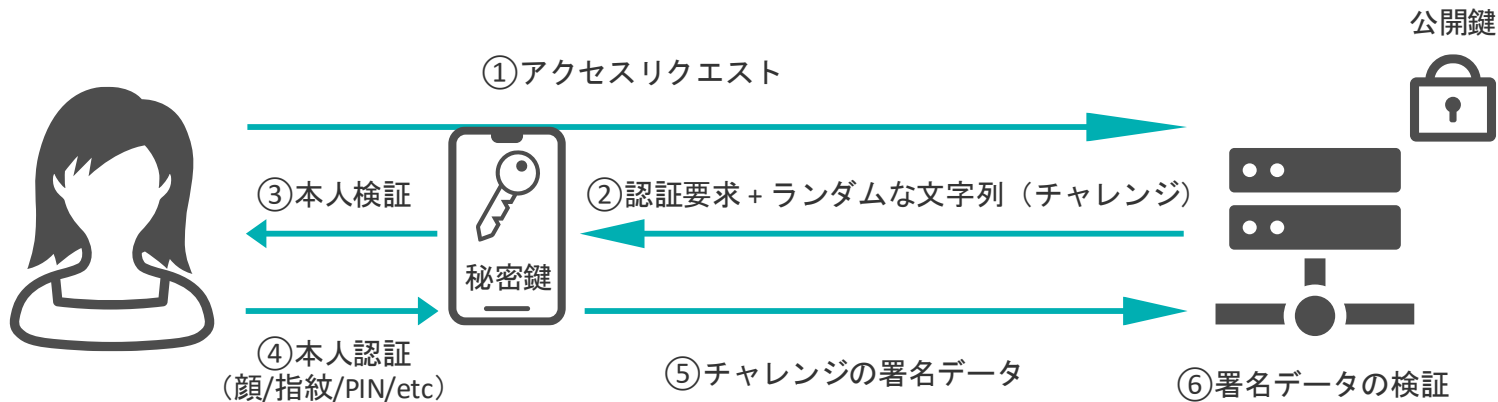
au IDでFIDO認証を利用しているユーザは1,300万人。パスワード忘れの顧客サポートへの問い合わせは35%減。

デモンストレーション内容

Passkeyを利用したサービス



FIDO認証の流れ



生体認証などのデータは、**クライアント側でのみ**
扱われ、ブラウザやサーバ側に送信されない

レガシーシステムとの互換性を確保しつつ、 柔軟な未来の認証技術を追求する重要性



レガシー互換性

既存システムとの互換性は導入の鍵です。負担を掛けずに新技術を組み込む方法が求められています。



認証技術の進化

セキュリティ向上と利便性の両立へ。生体認証やパスワードレス化が推進されています。



将来への影響

技術進化がもたらす可能性は無限です。認証の常識を変える機会が目の前に広がっています。

次世代セキュリティへ進化する注目のデジタル認証技術を理解する



Our Goal 01

デジタル認証の現状

現在の認証システムは、多数のパスワードを管理する必要があります。また、これに伴うセキュリティリスクが高まっています。



Our Goal 02

パスワードレス認証の革新

パスワードレス認証は、利便性とセキュリティを両立するアプローチとして注目を集めています。企業はこの動向に対応する必要があります。



Our Goal 03

セキュリティ戦略の再考

この新しい認証技術を導入することで、企業は未来のセキュリティ課題に備えた戦略的な基盤を構築できます。



Our Goal 04

XXX

XXX

登壇者について

ふるたて ゆうき

古舘 侑樹



・中国(北京)/マルタ共和国に留学経験有

2016- GMOグローバルサイン株式会社

2017- IoT Systems株式会社

2017- Ricolink Electronics株式会社

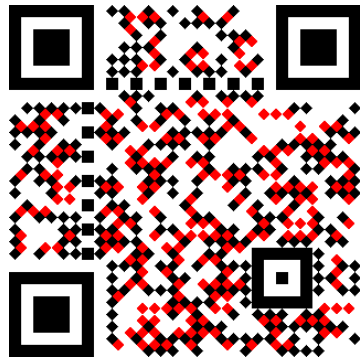
2019- GlobalSign China Co., Ltd.,

2020- GMOグローバルサイン株式会社

2022- 古舘商事株式会社 CEO(現在)

2024- Net Peace株式会社 CEO(現在)

2024- KeyXentic Inc. 営業部長(現在)



ハードウェア / ソフトウェアの統合セキュリティを提供

2017年

資本金

技術

開発拠点



会社設立



2億7000万円
(5,600万台湾ドル)



ゼロトラスト
特権ID
生体認証
FIDO



全サービス/
プロダクト
Made in Taiwan

導入実績



金融



企業



政府



軍



兆豐國際商業銀行
Mega International Commercial Bank



LINE Bank



CTBC BANK
中國信託銀行



國泰世華銀行
Cathay United Bank



MEDIATEK

NSW



FATC

福懋科技股份有限公司
FORMOSA ADVANCED TECHNOLOGIES CO., LTD.



臺北市政府
Taipei City Government



中華民國外交部
MINISTRY OF FOREIGN AFFAIRS
REPUBLIC OF CHINA (TAIWAN)



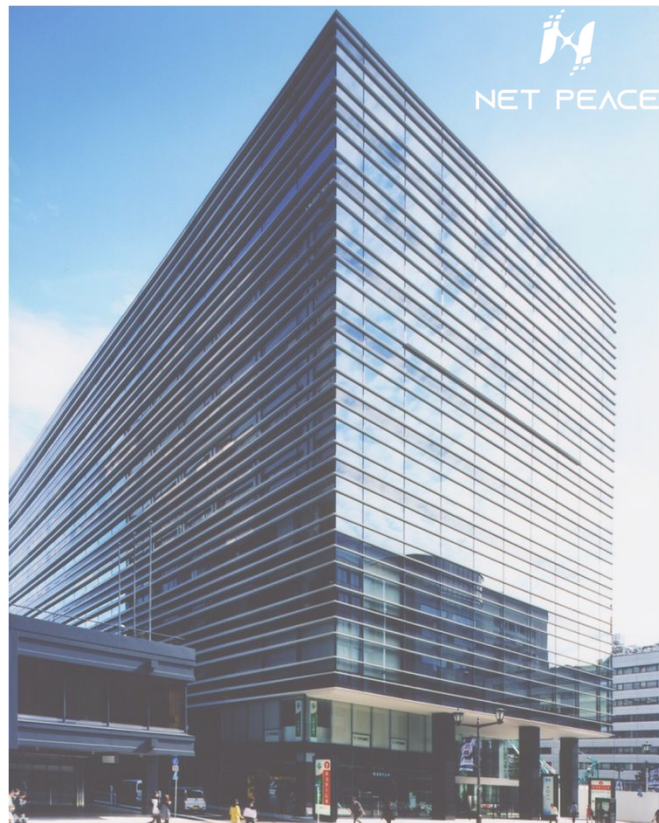
上海商業儲蓄銀行
THE SHANGHAI COMMERCIAL & SAVINGS BANK, LTD.



HongLeong Bank

Net Peace株式会社について

会社名	Net Peace株式会社
代表者	古舘 侑樹
設立	2024年1月24日
所在地	東京都中央区日本橋3丁目6番2号 日本橋フロント1階
取引先	GMOグローバルサイン株式会社 NSW株式会社 KeyXentic Inc. UPAS INFORMATION SECURITY CORP.



九州大学 櫻井 幸一 教授

所属

システム情報科学研究所 情報学部門 教授
サイバーセキュリティセンター（併任）
工学部 電気情報工学科（併任）
システム情報科学府 情報理工学専攻（併任）
マス・フォア・イノベーション関係学府（併任）



サービス一覧

ソフトウェア



Keyper

▽パスワードレス認証
▽ファイル暗号化



電子証明書

▽電子署名
▽暗号化/復号



電子契約

▽電子契約
▽証跡管理(認証・監査)



UPAS NOC

▽プラットフォーム
▽ネットワーク/デバイス管理



eKYC

▽顔認証
▽身分認証

ハードウェア



KX901

▽FIDO2 Token
▽指紋認証 可能



KX701

▽FIDO2 Token
▽NFC



KX905

▽iPad専用のカードリーダー
▽マイナンバーの読み取り可能

サービス



脆弱性診断

ペネトレーションテスト

▽ホワイトハッカー
▽システムの脆弱性診断

NSW

NSW、日台サイバーセキュリティ企業と協業検討について 発表

企業：NSW 産業：商社・サービス

2024年10月15日 17:31



【リリース】発表日:2024年10月15日

NSW、日台サイバーセキュリティ企業と協業検討

半導体開発環境、半導体デザインサービスのセキュリティ向上、安心安全
提案に向けて～

シンジプロバイダのNSW株式会社（本社：東京都渋谷区、代表取締役執行
田 尚二、以下 NSW）は、情報セキュリティサービス「Keyper」を提供
ntic Inc.（本社：台湾台北市、CEO 洪伯岳(Sean Hung)、以下 KX）、KX 日
の Net Peace 株式会社（本社：東京都中央区、代表取締役 古舘 侑樹、以
共同で、多要素認証やパスワードレス化によるセキュリティ向上に向けた
協業検討を10月15日より開始いたしました。



ゼロトラスト パスワードレス 管理プラットフォーム



ユーザ権限の割り当て

- ローカルまたはADユーザー
- グループの割り当て
- 役割の割り当て



検証メカニズム

- FIDO
- PKI
- TOTP
- Mobile



デバイス /
ウェブアクセスコントロール

- PC機器
- ウェブシステム



認証サービス

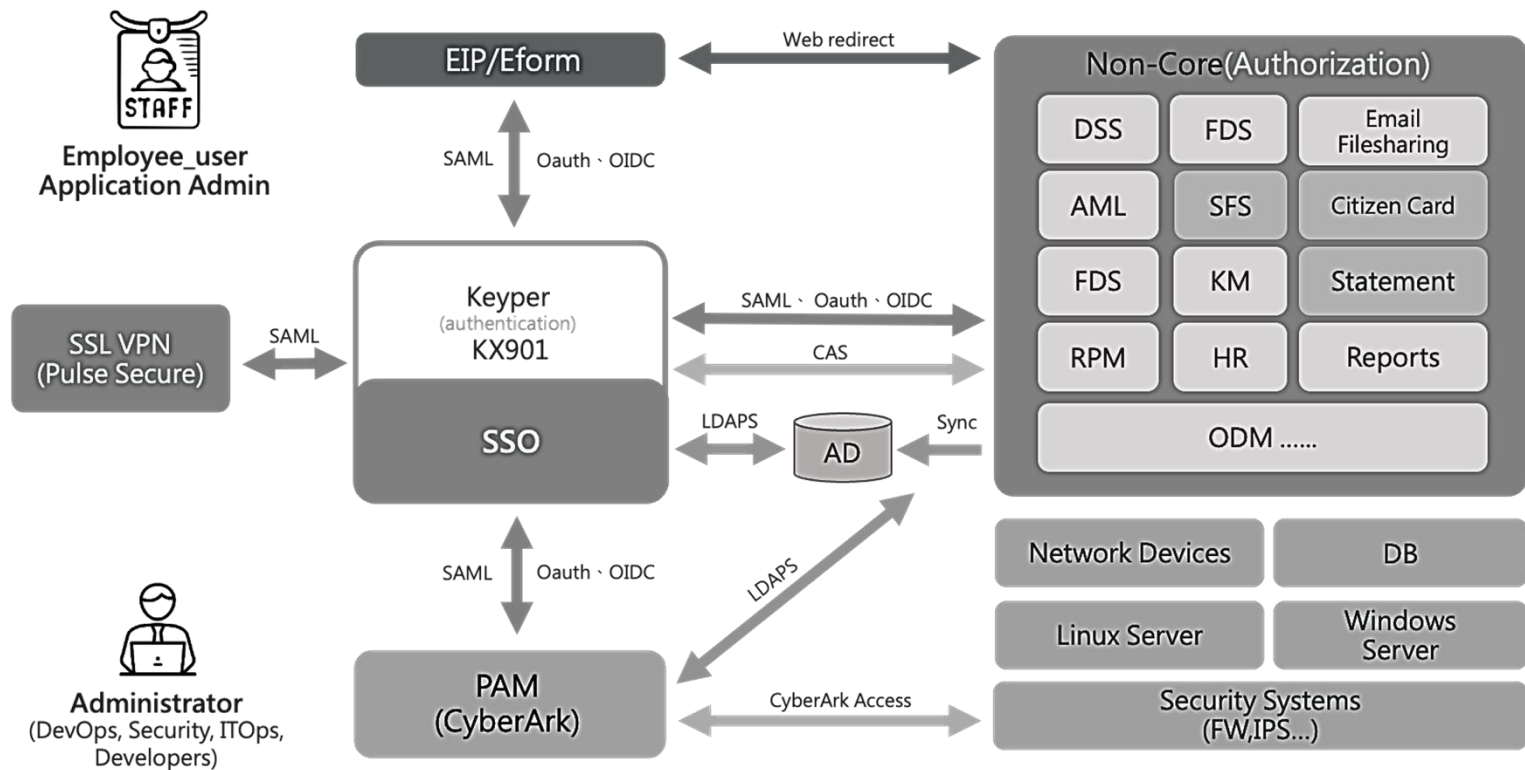
- VPN
- Linux
- Windows
- SSO
- Oauth
- Open ID



監査証跡

- ユーザー権限レポート
- 認証機器管理レポート
- ユーザーログインタイプレポート
- ユーザー権限変更レポート
- ユーザーログイン機器レポート
- インポート/エクスポート特定
フォーマットレポート

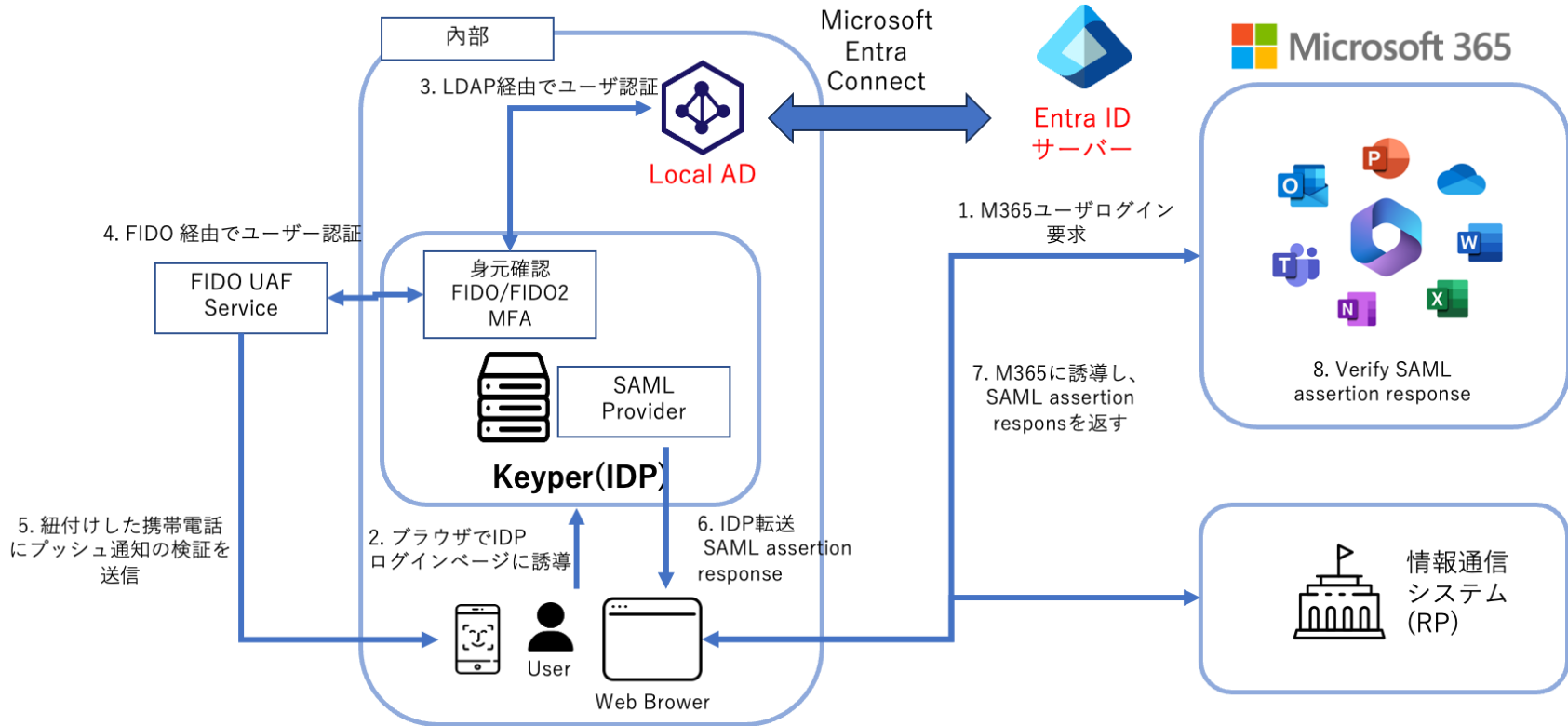
一般的な企業におけるインストール例



Windows Logon アプリケーションフロー(FIDO2 Tokenによる認証)



M365統合アーキテクチャ

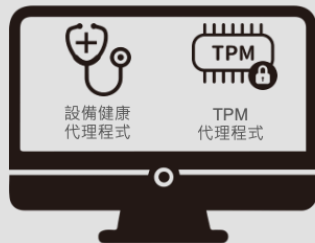


正確な身元確認



生物識別鑑別器/使用者

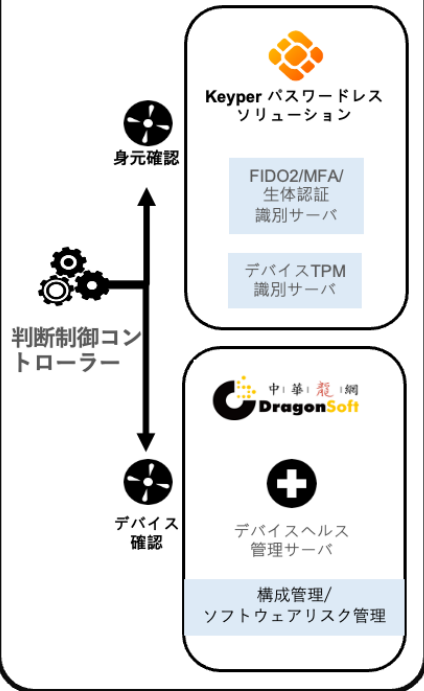
正確な端末確認



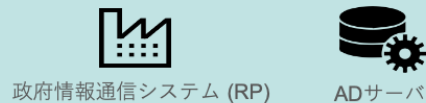
設備健康
代理程式

TPM
代理程式

判断制御



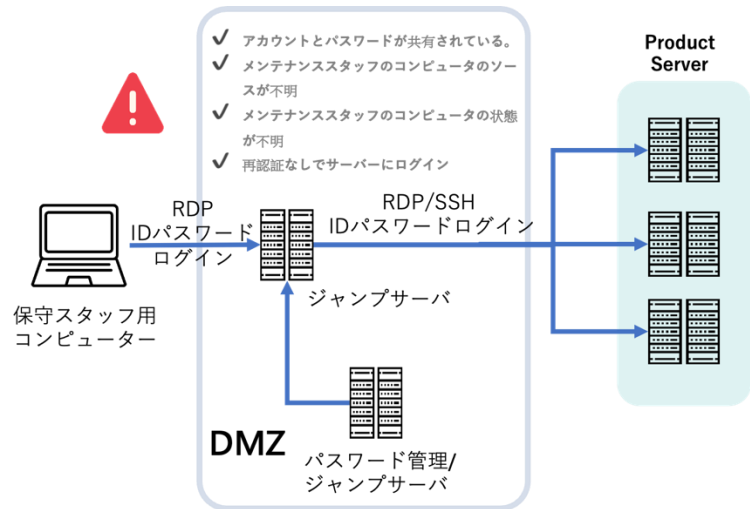
現行システム



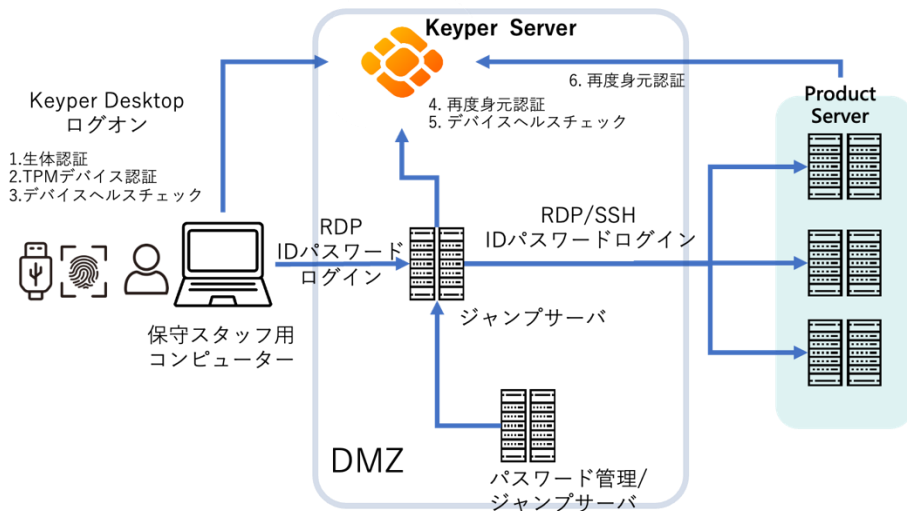
ERP	EIP	Email
KM	SFS	Citizen Card
FDS	KM	Statement
RPM	HR	Reports

ODM

既存の構造

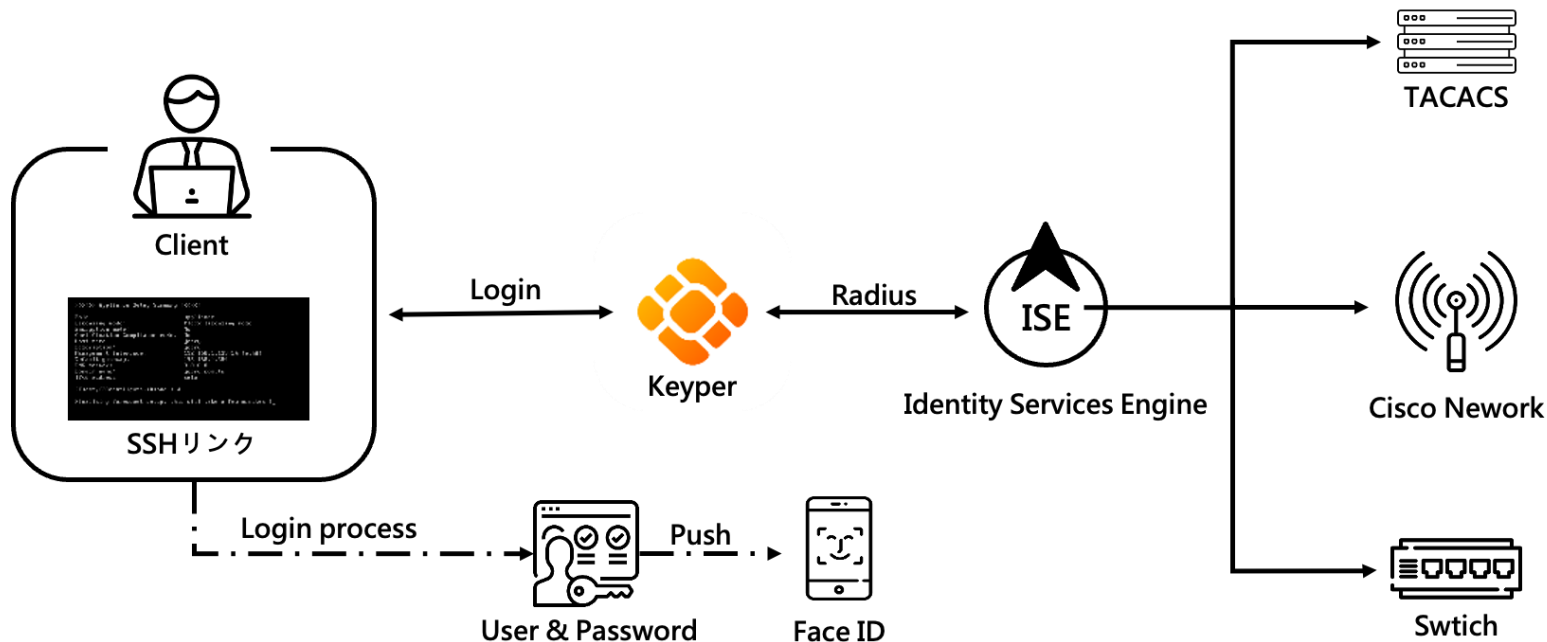


Keyperによる強化構造



サーバールームマネジメント 導入事例

ISEネットワーク機器を統合し二要素認証を行うことで、
サーバールームのネットワーク制御のセキュリティを強化



管理者の負担を減らす管理方法

Dashboard

Account

Services

Report

Keyper

English

Welcome to Keyper Manager

2024/12/19 17:37:10 yuki Macintosh; Intel Mac OS X 10_15_7 Chrome 1.21.119.182 Success	2024/12/19 17:25:15 superadmin Windows NT 10.0; Win64; x64 Chrome 192.168.1.254 Success	2024/12/19 16:58:46 superadmin Windows NT 10.0; Win64; x64 Chrome 192.168.1.254 Success	2024/12/19 12:11:16 superadmin Windows NT 10.0; Win64; x64 Chrome 192.168.1.254 Success	2024/12/19 11:09:10 superadmin Windows NT 10.0; Win64; x64 Chrome 192.168.1.254 Success	2024/12/18 17:16:14 superadmin Windows NT 10.0; Win64; x64 Chrome 192.168.1.254 Success	2024/12/18 16:34:48 superadmin Windows NT 10.0; Win64; x64 Chrome 39.14.57.168 Success	2024/12/18 11:44:37 eqlt_waiting Windows NT 10.0; Win64; x64 Chrome 60.251.164.242 Success	2024/12/18 11:43:28 eqlt_tester Windows NT 10.0; Win64; x64 Chrome 60.251.164.242 Success
---	--	--	--	--	--	---	---	--

Total Logins

2024/12/06 ~ 2024/12/19

158

Total Successful Logins

2024/12/06 ~ 2024/12/19

133

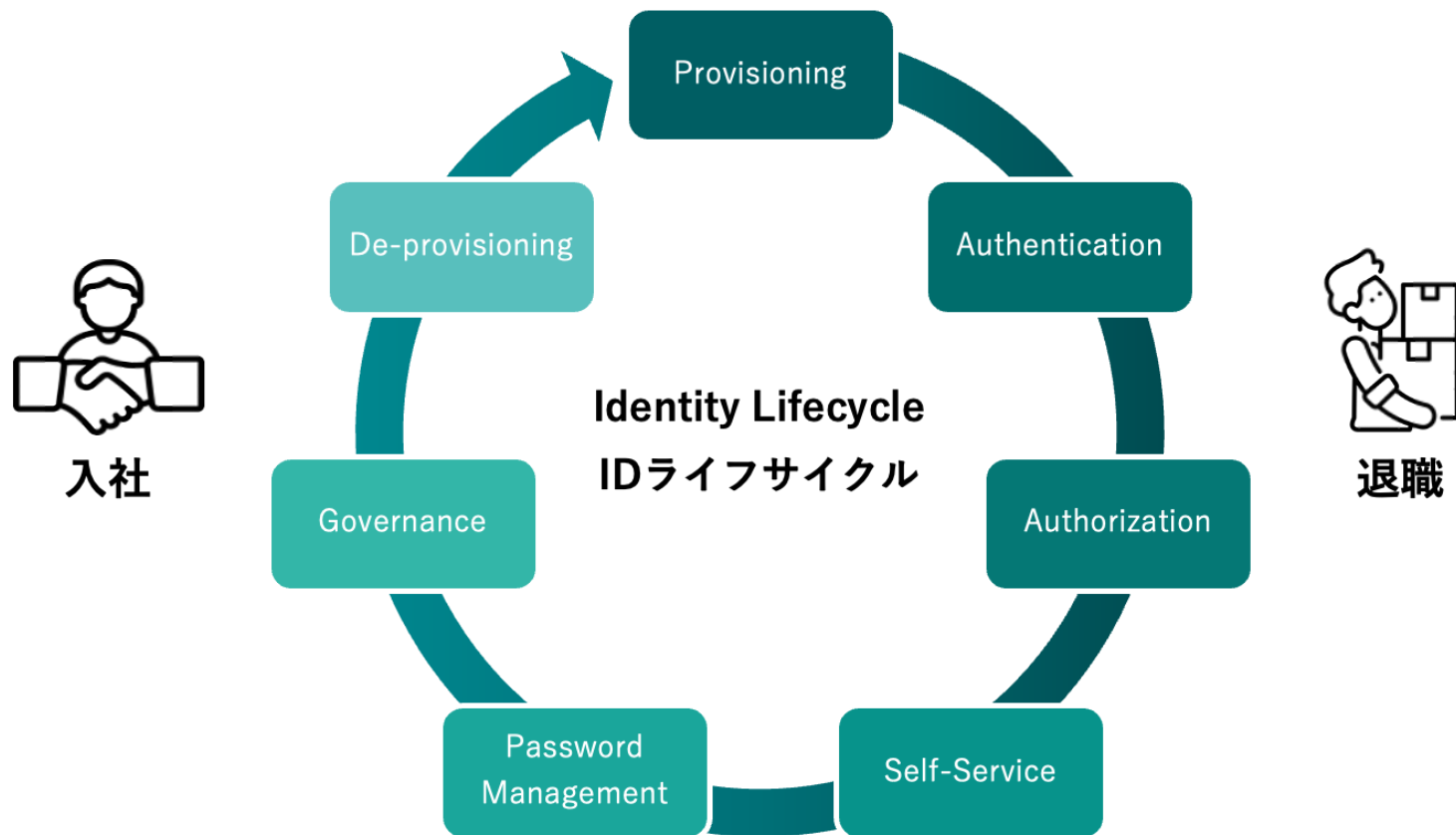
Total Failed Logins

2024/12/06 ~ 2024/12/19

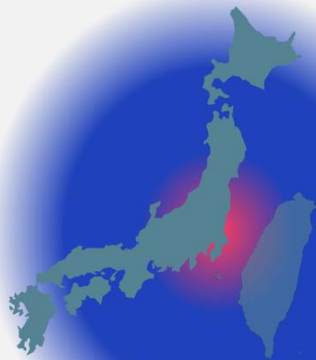
25

Login Methods

2024/12/06 ~ 2024/12/19



台湾と日本は
地政学的に似ている



力を合わせて
日本を守る



日本の
ビジネスパートナー
を募集



Thank you

Net Peace株式会社
代表取締役 古舘 侑樹
yuki@furutatecorp.com

