インシデント事例から学ぶ「StartIn」の有効性

Agenda

1 IDaaS製品「StartIn」とは

2 正当アカウントを狙う動きと国内事例

3 多要素認証を回避するフィッシングについて

4 「StartIn」の特徴、優位性について

Agenda

1 IDaaS製品「StartIn」とは

2 正当アカウントを狙う動きと国内事例

3 多要素認証を回避するフィッシングについて

4 「StartIn」の特徴、優位性について

「StartIn」とは

安全な「Login」で業務を快適に「Start」できる世界を実現

StartIn™

スタートイン

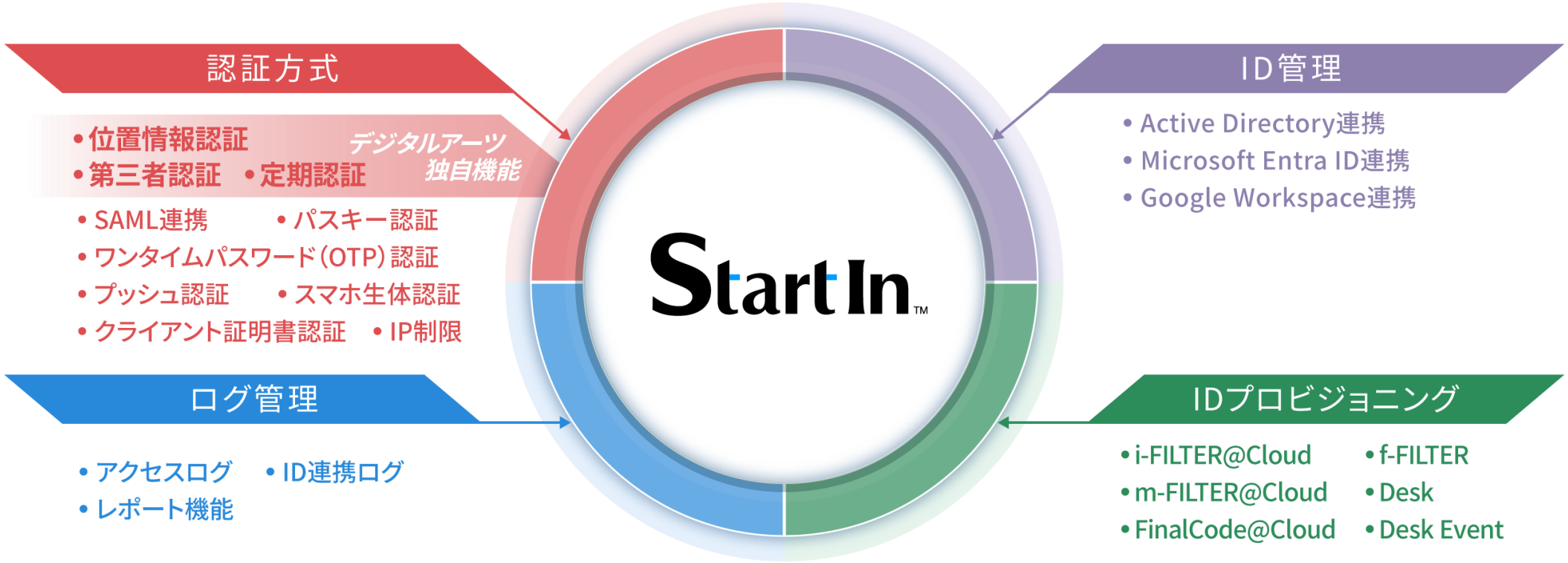
位置情報を活用しセキュリティリスクを可視化！

機密情報へのアクセスには第三者認証で上長承認後に認証！

運用負荷を軽減する定期認証機能を搭載！

「StartIn」で実現可能な機能

ID管理やログ管理に加え、強固な多要素認証を搭載し、クラウドサービスの安全なID管理を実現します



「StartIn」の特徴：多要素認証

ワンタイムパスワード認証や、生体認証など一般的な認証方法に加え、デジタルアーツ独自の認証でセキュアな世界を実現

多彩な多要素認証機能でインターネットの入り口を強固に

標準的な認証方式

＋

独自の認証方式

※標準機能として1ライセンスあたり1枚証明書発行が可能です。ライセンス数以上の証明書を利用したい場合、オプションの購入が必要となります。

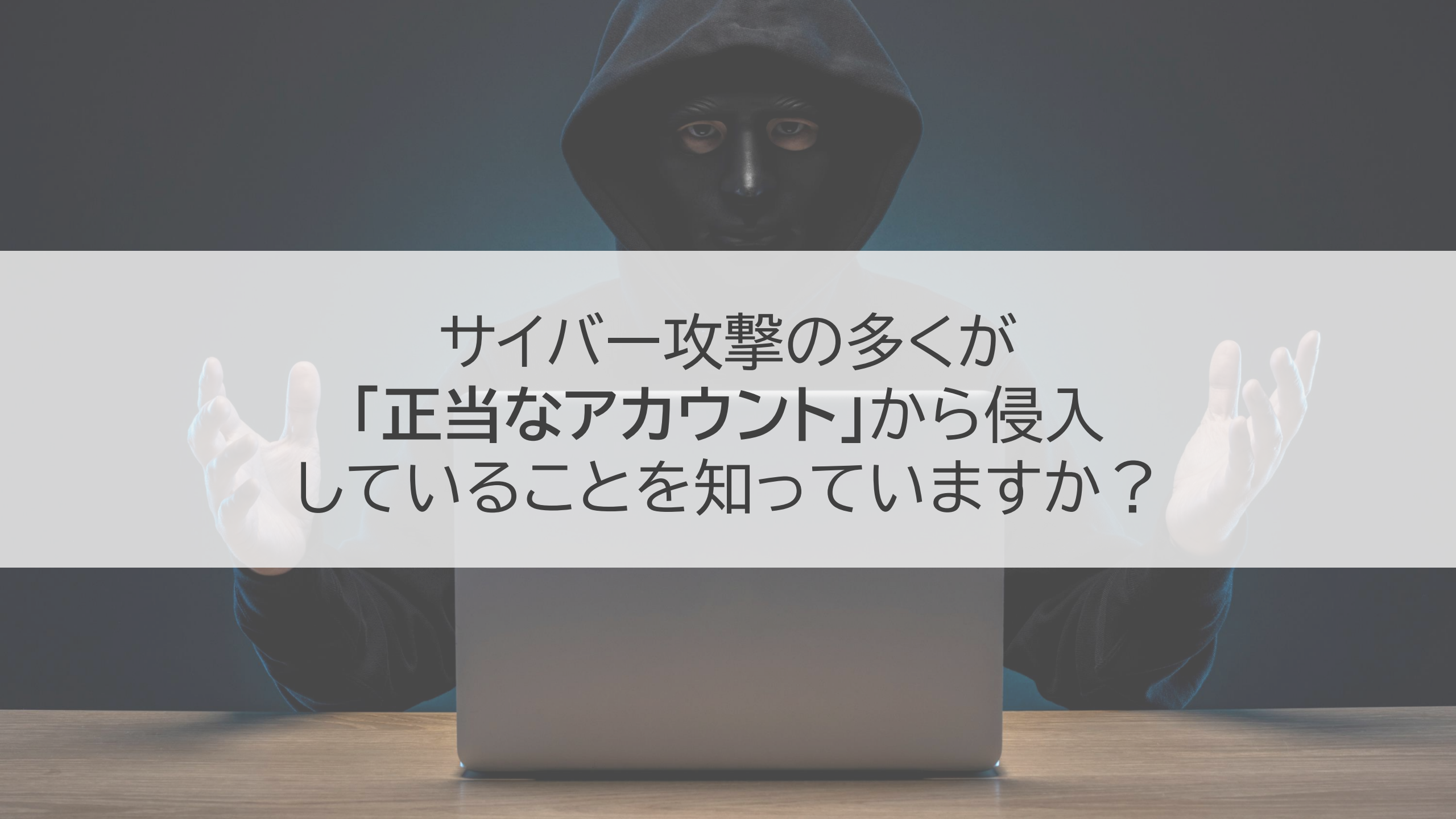
Agenda

1 IDaaS製品「StartIn」とは

2 正当アカウントを狙う動きと国内事例

3 多要素認証を回避するフィッシングについて

4 「StartIn」の特徴、優位性について

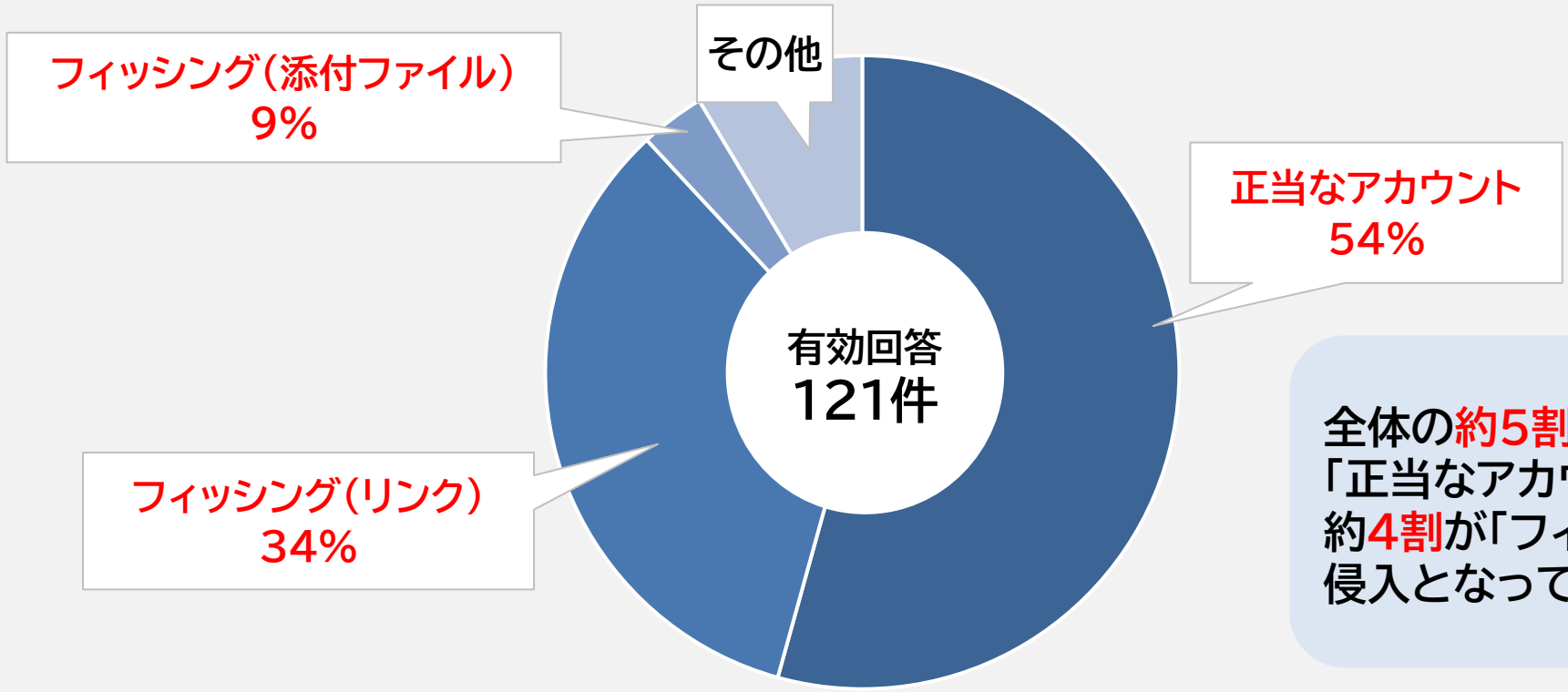


サイバー攻撃の多くが
「**正当なアカウント**」から侵入
していることを知っていますか？

不正アクセスの主な手口

サイバー攻撃の初期アクセスには「正当なアカウント」や
リンク、添付ファイルを利用した「フィッシング」が手法として利用されている

【サイバー攻撃の初期アクセス】

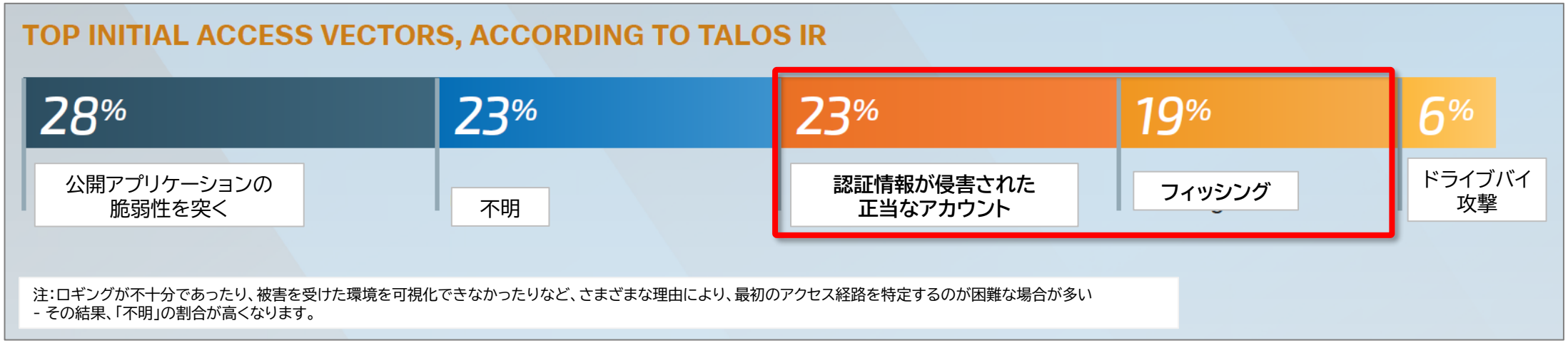


全体の約5割が
「正当なアカウント」からの侵入、
約4割が「フィッシング」からの
侵入となっている

出典：米CISA「2022年リスクと脆弱性の評価結果」
https://www.cisa.gov/sites/default/files/2023-07/FY22%20RVA%20Infographic_508c.pdf

インシデントにおける初期アクセスについて

Cisco Talos が対応したインシデントにおける初期アクセスの内訳は下記の通り



「最近の攻撃者は、ハッキングはしないでログインする」という話をきっと耳にしたことがあるでしょう。

攻撃者は正当（有効）なユーザーアカウントの詳細情報を入手（または窃取）し、まずシステムにアクセスしてそのまま潜み続け、権限を昇格させて、ネットワークのより多くの領域に「ログイン」できるようにします。

残念なことに、正当なアカウントを使用する手法は、脅威をめぐる状況において広く利用されています。この手法は、Talos が 2023 年に脅威テレメトリで観測した MITRE ATT&CK の手法の中では 2 番目に多いものでした。昨年の Talos インシデント対応チームのすべての業務の 26% は、正当なアカウントの使用に関するものでした。

2023 Talos Year In Review
https://blog.talosintelligence.com/content/files/2023/12/2023 Talos Year In Review.pdf

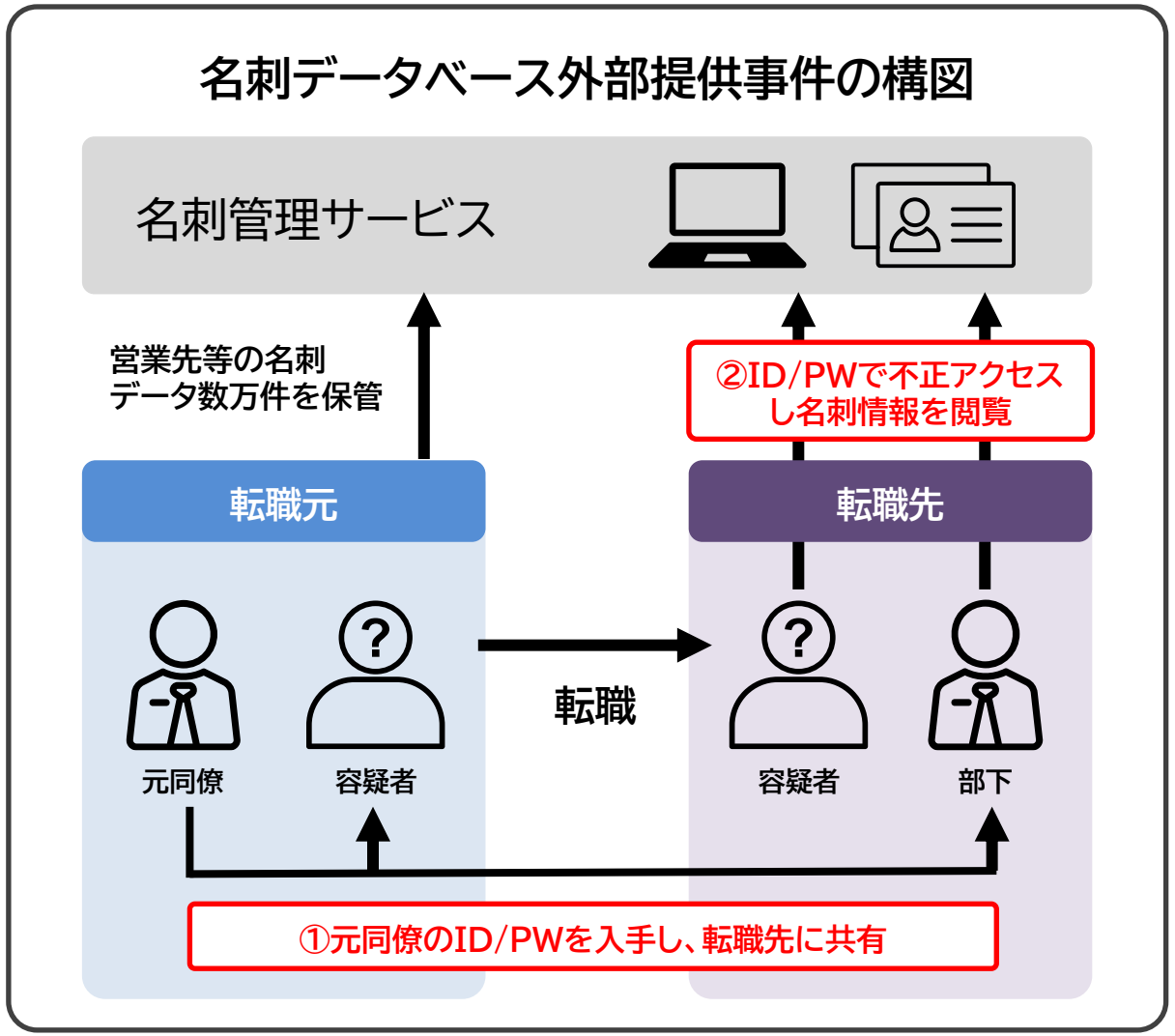
攻撃者がユーザーのログイン情報を窃取して悪用する仕組みについて | Cisco Japan Blog
2024年2月15日
https://gblogs.cisco.com/jp/2024/02/talos-how-are-user-credentials-stolen-and-used-by-threat-actors/

IDに起因するインシデントのご紹介

従業員/元従業員

内部犯

1.元従業員が元同僚の名刺データにID/PWでアクセス（2023年9月）



概要

容疑者は人材派遣会社の元従業員

転職前に（入手方法は不明）**元同僚の名刺管理サービスのID/PWを入手**し、同業他社である転職先へ共有

共有された転職先で**ID/PWを使ってアクセスしていた名刺情報をすべて閲覧可能**だった

インシデントの原因と求められる対策

容疑者が元同僚のID/PWを入手し、転職先で共有していたことが問題のため、**ID/PWだけでなく、別要素での認証をすることが効果的**

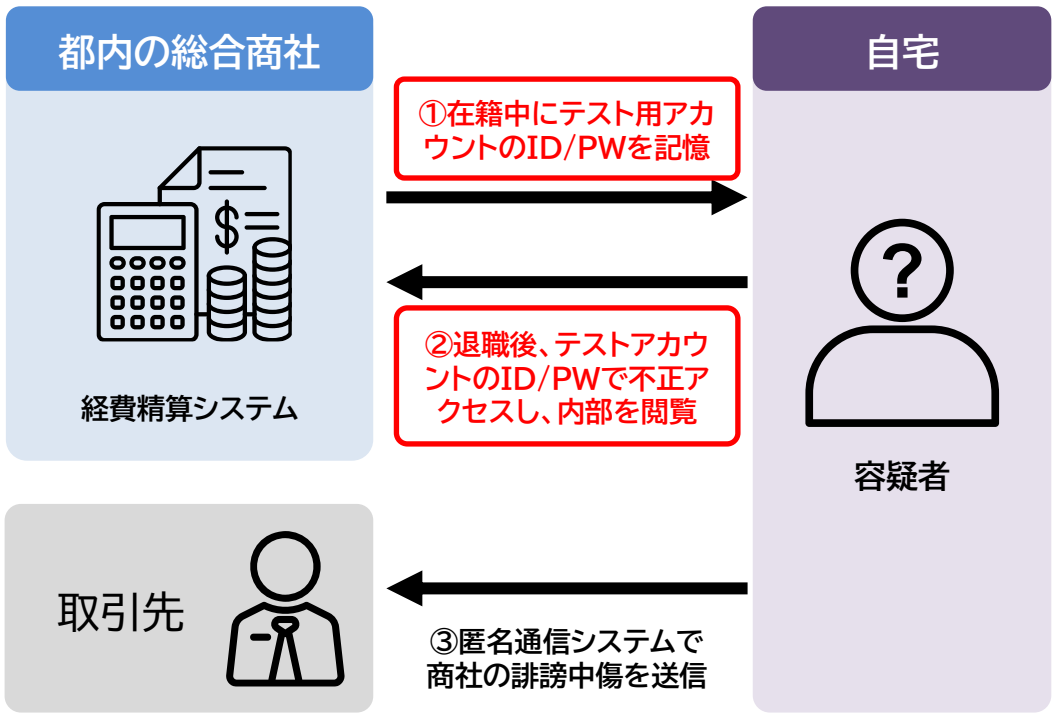
「StartIn」で有効な対策

- ✓ ワンタイムパスワード認証
- ✓ IP制限
- ✓ クライアント証明書認証
- ✓ パスワードレス認証（パスキー）
- ✓ **位置情報認証（GPS）**
- ✓ **第三者認証**

出典：日本経済新聞
https://www.nikkei.com/article/DGXZQOUE1421N0U3A910C2000000/

2.元従業員が未削除アカウントID/PWでアクセス(2023年11月)

元従業員による不正アクセス事件の構図



概要

容疑者は都内の総合商社の元従業員

クラウド型の経費精算システムの未削除のテストアカウントのID/PWを記憶していた

退職後に自宅から**テストアカウントのID/PWで不正アクセス**
経理情報を不正に閲覧

インシデントの原因と求められる対策

アカウント削除忘れがあり、それを悪用された
テストアカウントは複数人でID/PWを共有していた可能性があるため、
生体情報による認証や、端末の情報による認証が効果的

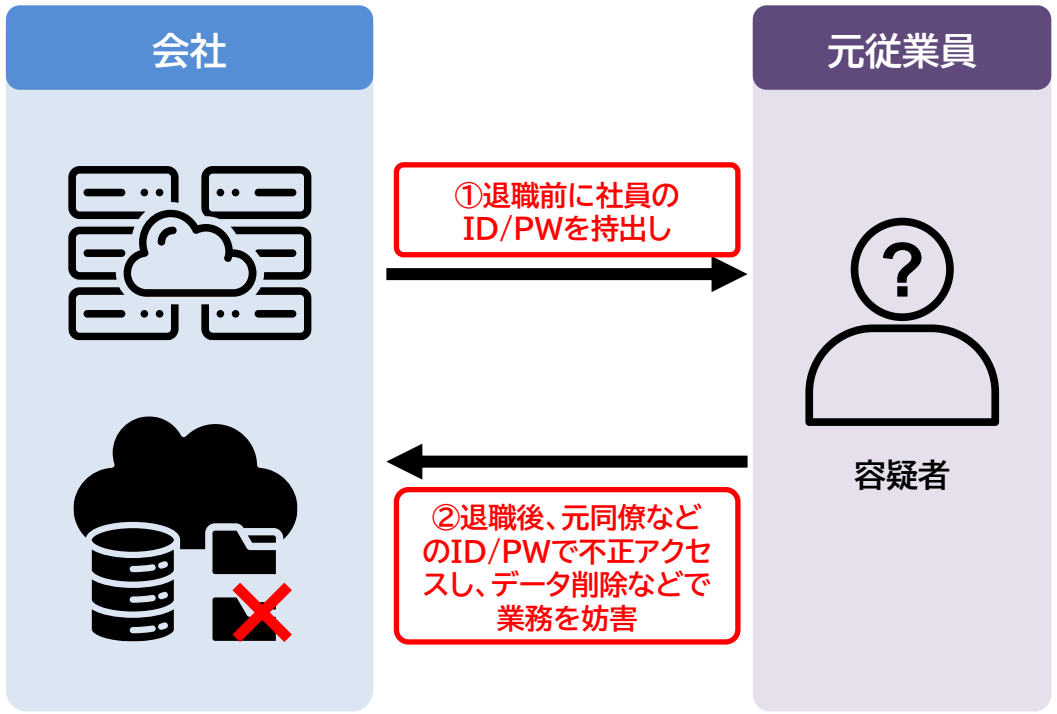
「StartIn」で有効な対策

- ✓ クライアント証明書認証
- ✓ パスワードレス認証(パスキー)
- ✓ **位置情報認証(GPS)**

出典: ITmedia NEWS
https://www.itmedia.co.jp/news/articles/2311/27/news104.html

3.元従業員がID/PWを持出し退職後に不正アクセス（2023年1月）

元従業員が退職後に不正アクセスの構図



概要

容疑者は電気計測器メーカーの元従業員
社内システム管理を担当しており、**退職前に社員のID/PWを持ち出した**

退職後に元同僚や元上司のID/PWで、社内ネットワークやクラウドサービスに不正アクセス

会社のサーバーに保管されていたデータを削除し業務を妨害

インシデントの原因と求められる対策

元同僚や元上司のIDやパスワードを勝手に使い、社内ネットワークや同社が契約しているクラウドサービスに不正にログインを実施しているため、**ID/PWだけでなく、別要素での認証をすることが効果的**

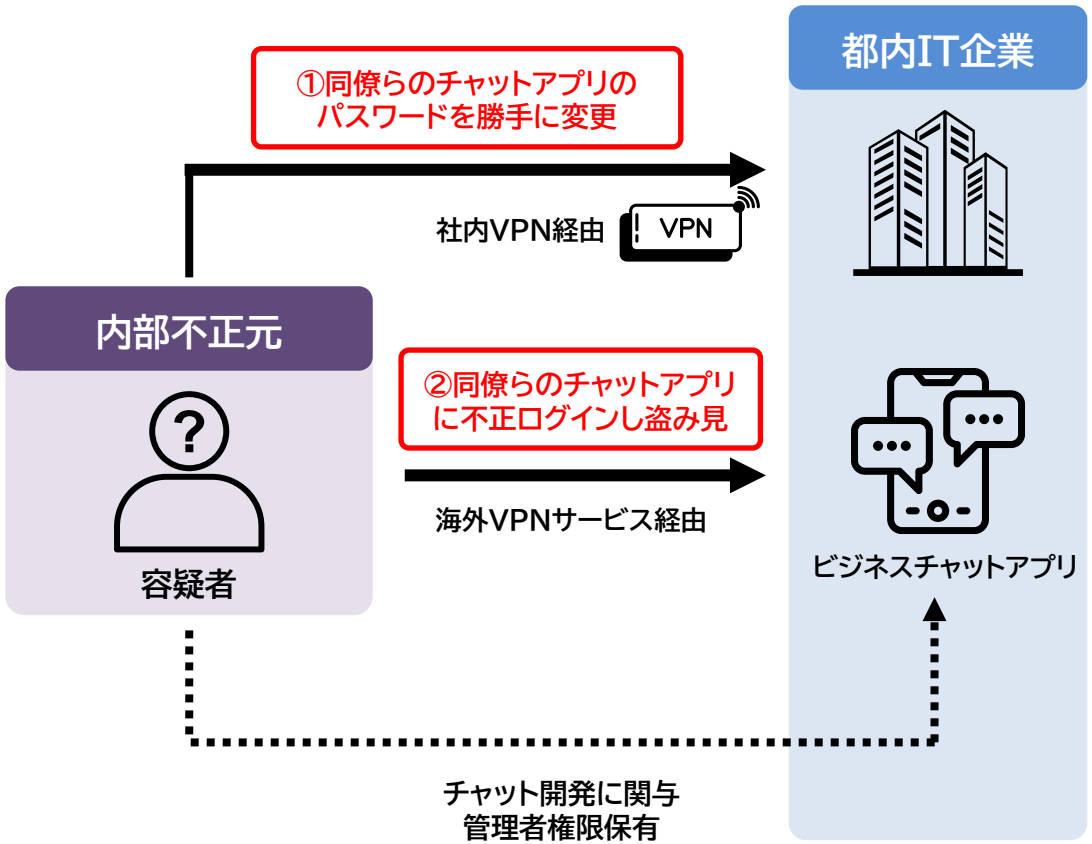
「StartIn」で有効な対策

- ✓ ワンタイムパスワード認証
- ✓ IP制限
- ✓ クライアント証明書認証
- ✓ パスワードレス認証（パスキー）
- ✓ **位置情報認証（GPS）**
- ✓ **第三者認証**

出典：朝日新聞デジタル
https://www.asahi.com/articles/ASR1S4HC4R1SUTIL008.html

4.従業員が他従業員のPW変更し不正アクセス(2023年7月)

他従業員のPW変更した後不正アクセスの構図



概要

容疑者はIT企業従業員
ビジネスチャットアプリの開発者権限を持っていた

上司や同僚のPWを勝手に変更、その後不正にログイン

他人になりすまして悪口を投稿したり投稿内容の改ざんや設定変更を行った

インシデントの原因と求められる対策

勝手にPWを変更していた点については防ぐことが困難だが、PW変更後の不正ログインについては**多要素認証**を実施していれば防げる

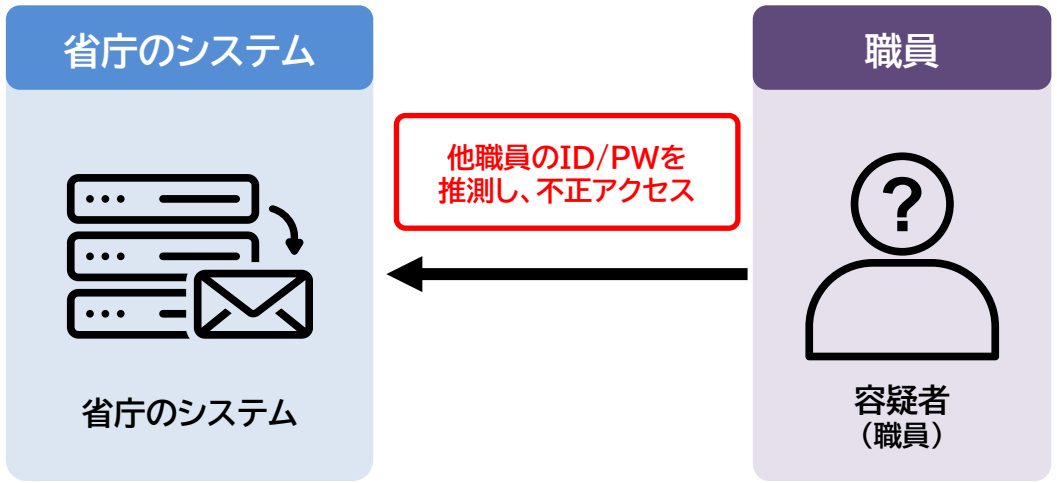
「StartIn」で有効な対策

- ✓ ワンタイムパスワード認証
- ✓ IP制限
- ✓ クライアント証明書認証
- ✓ パスワードレス認証(パスキー)
- ✓ **位置情報認証(GPS)**
- ✓ **第三者認証**

出典:Piyolog
https://piyolog.hatenadiary.jp/entry/2023/07/07/015246

5.従業員が他従業員のID/PWを推測し不正アクセス（2024年2月）

他従業員のID/PWを推測し不正アクセスの構図



例

容疑者	他職員
ID: A000-123 PW: Password123	ID: A000-124 PW: Password124

概要

容疑者は奈良県A市の職員で、庁内システムに不正にログインし他職員のメールを閲覧していた

ログインしたアカウントは、IDは自分のIDから他職員のIDを推測、PWは初期設定のままなど容易に推測できたもの

2020年度～2023年度にかけて職員271人がログインされていた

インシデントの原因と求められる対策

ID/PWを推測して庁内システムに不正ログインしメールを盗み見していたため、**ID/PWだけでなく、別要素での認証をすることが効果的**

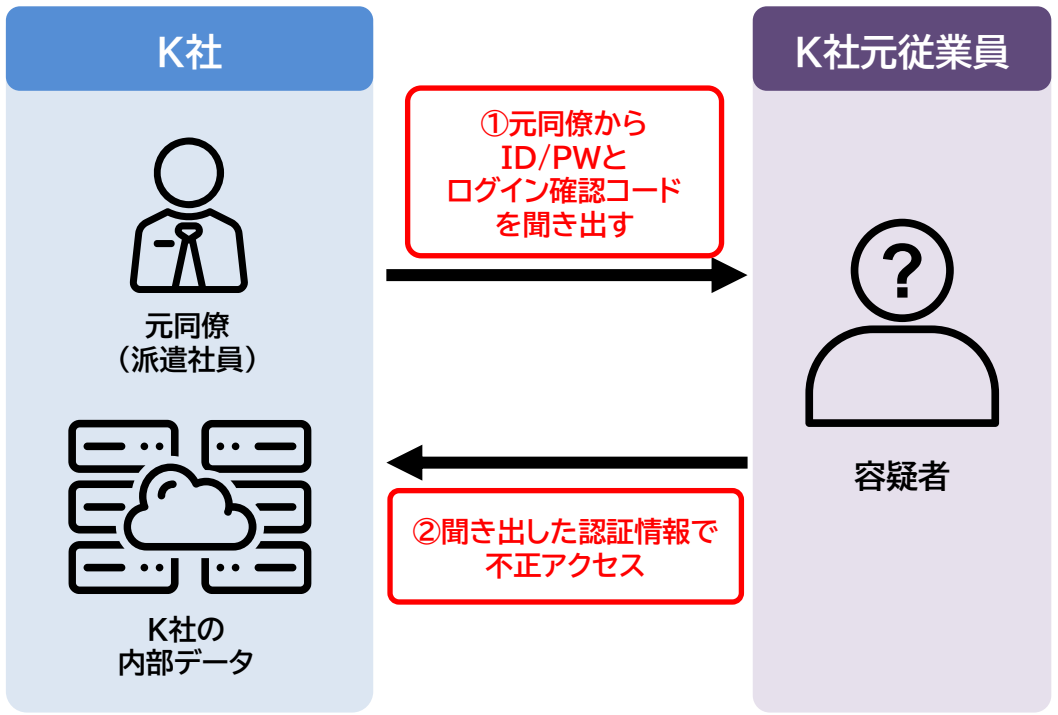
「StartIn」で有効な対策

- ✓ ワンタイムパスワード認証
- ✓ IP制限
- ✓ クライアント証明書認証
- ✓ パスワードレス認証（パスキー）
- ✓ **位置情報認証（GPS）**
- ✓ **第三者認証**

出典：Security NEXT
https://www.security-next.com/154269

6.元従業員が元同僚からID/PWを聞き出しアクセス（2023年9月）

元同僚から認証情報を聞き出しアクセスの構図



概要

容疑者はK社の元従業員で、転職後にウソをつき、元同僚（派遣社員）から、**サーバー（何かは不明）のID/PWとログイン時の確認コードを聞き出し、アクセスを実施**

営業秘密データを不正取得

※確認コードがあるということは、アクセスされたK社側に多要素認証的なものはあったと思われる。

インシデントの原因と求められる対策

容疑者は派遣社員からID/PWを聞き出し、警視庁の任意聴取に**「上司や同僚には聞けないので連絡した」**と供述しているため、**認証する際に上長が確認する仕組み**があれば防止と、そもそも行動を起こさせない抑止効果が期待できる

「StartIn」で有効な対策

- ✓ クライアント証明書認証
- ✓ パスワードレス認証（パスキー）
- ✓ **位置情報認証（GPS）**
- ✓ **第三者認証**

出典：日本経済新聞
https://www.nikkei.com/article/DGXZQOUE2914W0Z20C23A9000000/

内部犯：事例まとめ

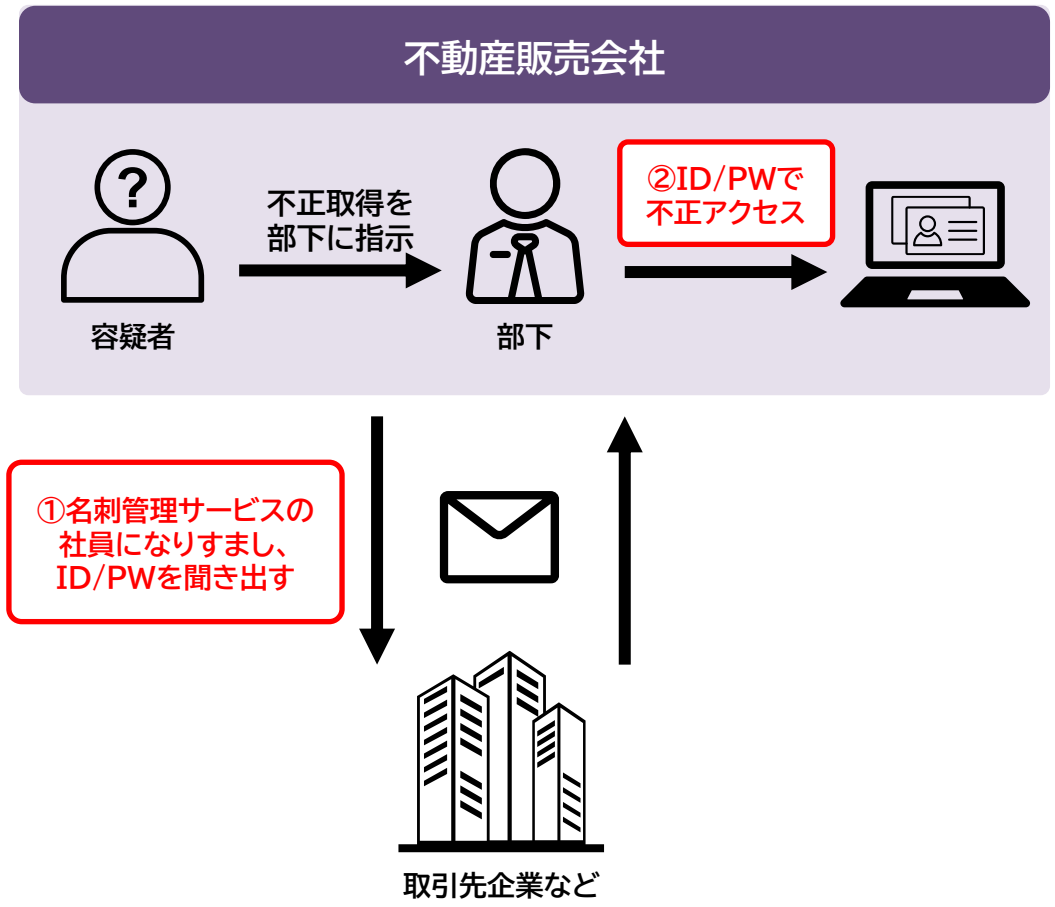
	事例	訴求できる機能
1	名刺管理サービスのID/PWを盗みアクセス （派遣会社、転職先で利用）	何かしらの多要素認証（パスワード以外の要素） （ワンタイムパスワード、IP制限、クライアント証明書、パスキー、位置情報（GPS）、第三者認証 など）
2	未削除テストアカウントでアクセス （都内の総合商社、会社に不満）	クライアント証明書認証、パスキー認証、位置情報（GPS）、 など
3	社内NWやクラウドサービスのID/PWを盗みアクセス （会社に不満）	上記1と同じ
4	他従業員のPWを開発権限で変更したあと 外部からアクセス（会社に不満）	〃
5	他従業員のID/PWを推測しアクセス（興味本位）	〃
6	元同僚をからID/PWと確認コードも聞き出し、 外部からアクセス	クライアント証明書認証、パスキー認証、IP制限、位置情報 （GPS）、第三者認証

外部の第三者

外部犯

1.フィッシングで Sansan ID/PW窃取(2024年2月)

名刺データが不正閲覧された事件の構図



概要

容疑者は不動産販売会社の幹部とその部下
名刺管理サービスの社員になりすましてフィッシングメールを送り
ID/PWを窃取(メール前後に電話していたという報告もあり)

盗んだID/PWで名刺管理サービスにアクセス

400万件以上の名刺情報を閲覧できる状態だった

インシデントの原因と求められる対策

ID/PWを窃取されてログインされたことから、
ID/PWだけでなく、別要素での認証をすることが効果的

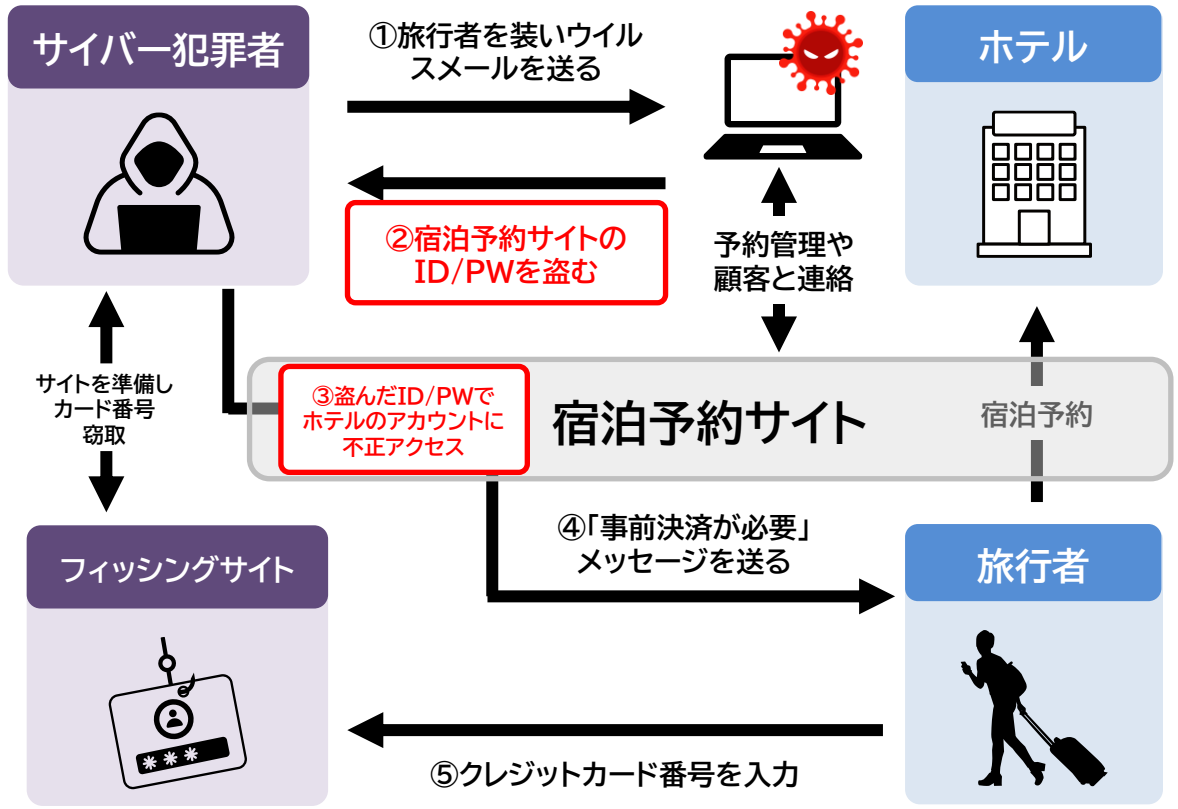
「StartIn」で有効な対策

- ✓ ワンタイムパスワード認証
- ✓ IP制限
- ✓ クライアント証明書認証
- ✓ パスワードレス認証(パスキー)
- ✓ **位置情報認証(GPS)**
- ✓ **第三者認証**

出典:日本経済新聞
https://www.nikkei.com/article/DGXZQOUE315N50R30C24A1000000/

2.マルウェアでBooking.comのID/PW窃取(2023年6月)

元従業員が元同僚から情報を聞き出しアクセスの構図



概要

マルウェアを使う犯罪者(Vidar(ヴィーザル)といわれている)
メールやメッセージ添付ファイルからホテルの端末がマルウェア感染

マルウェアがホテルの宿泊予約サイトアカウントのID/PWを窃取

攻撃者が窃取したホテルのアカウントに不正アクセスし、旅行者に
フィッシングメッセージ送付、クレカ情報が窃取された

インシデントの原因と求められる対策

ID/PWを窃取されてログインされたことから、
ID/PWだけでなく、別要素での認証をすることが効果的

「StartIn」で有効な対策

- ✓ ワンタイムパスワード認証
- ✓ IP制限
- ✓ クライアント証明書認証
- ✓ パスワードレス認証(パスキー)
- ✓ **位置情報認証(GPS)**
- ✓ **第三者認証**

出典:朝日新聞デジタル
https://www.asahi.com/articles/ASRCC5GK1RC2ULZU00D.html

Agenda

1 IDaaS製品「StartIn」とは

2 正当アカウントを狙う動きと国内事例

3 多要素認証を回避するフィッシングについて

4 「StartIn」の特徴、優位性について

多要素認証について

Microsoftアカウントの例

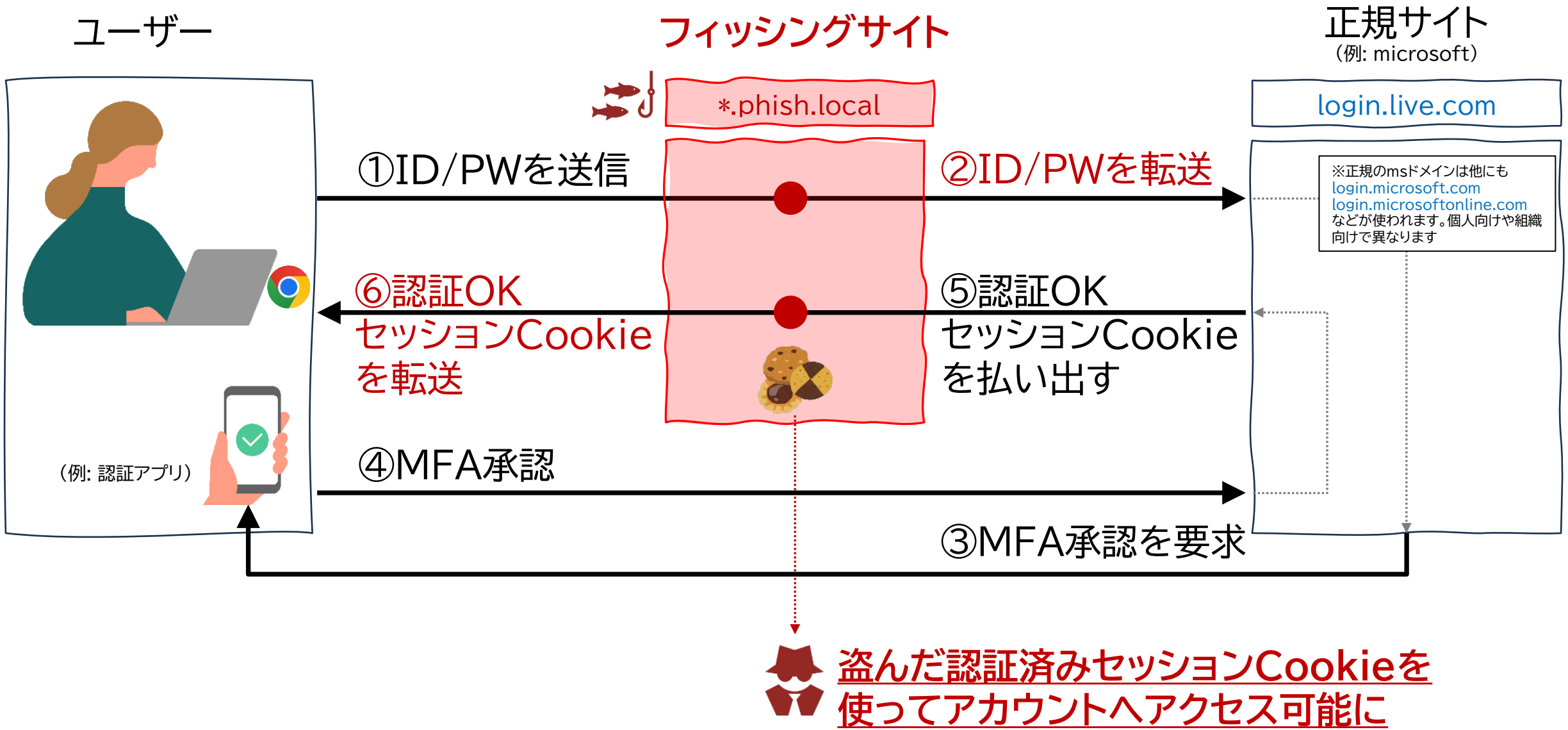
最近では多要素認証(パスワード以外での認証)が
当然のように利用できるようになってきた。
どの認証方法が利用できるかはサービス次第。

しかしながら、**多要素認証をも回避するフィッシング**がある。

次のページでは「AiTM」(※) を取り上げる。

(※) Adversary-in-the-Middle、中間者攻撃などともいわれる

AiTMが多要素認証を回避する手法



フィッシング攻撃に対応するために

多要素認証を突破する中間者攻撃（AiTM）などのフィッシングに対しては、
「FIDO 認証」と「証明書ベースの認証」による対策が有効

Defending against AiTM phishing and BEC

This AiTM phishing campaign is another example of how threats continue to evolve in response to the security measures and policies organizations put in place to defend themselves against potential attacks. And since credential phishing was leveraged in many of the most damaging attacks last year, we expect similar attempts to grow in scale and sophistication.

While AiTM phishing attempts to circumvent MFA, it's important to underscore that MFA implementation remains an essential pillar in identity security. MFA is still very effective at stopping a wide variety of threats; its effectiveness is why AiTM phishing emerged in the first place. Organizations can thus make their MFA implementation "phish-resistant" by using solutions that support Fast ID Online (FIDO) v2.0 and certificate-based authentication.

Defenders can also complement MFA with the following solutions and best practices to further protect their organizations from such types of attacks:

出典：Microsoft
https://www.microsoft.com/en-us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/

2024年3月新機能：パスキーを用いたパスワードレス認証

2024年
3月新機能

パスキーを用いてパスワードレスで認証することで
利便性の向上とセキュリティ強化を実現

パスワード利用による「第三者に容易に資格情報を不正利用されるリスク」を軽減することが可能

STEP 1

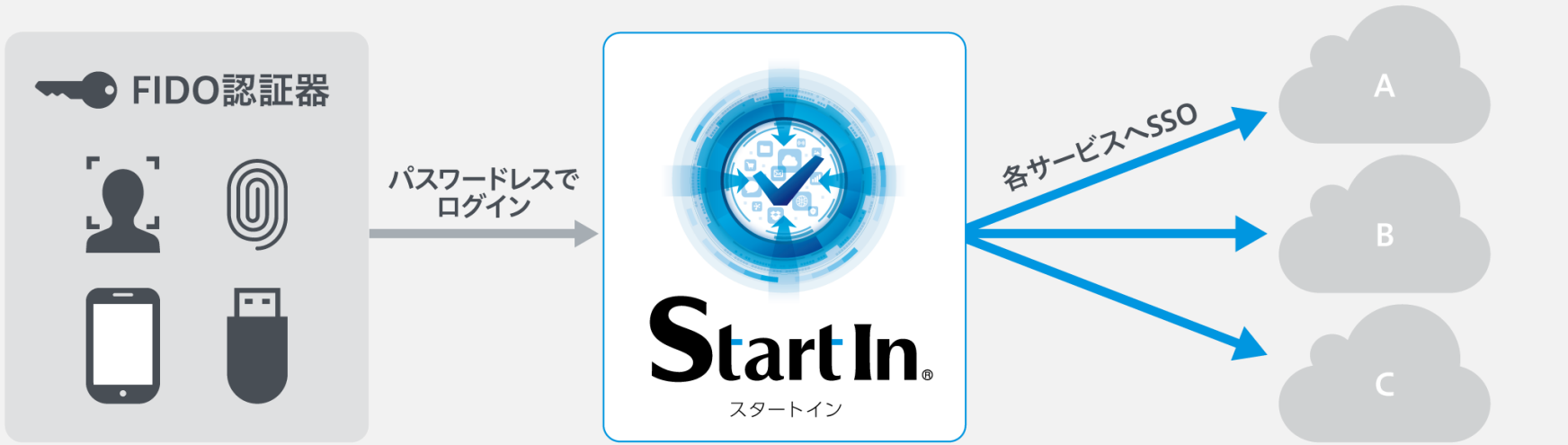
指紋や顔などの生体情報や
PINを利用し本人確認を実施

STEP 2

本人確認の結果を基に
「StartIn」にログイン

STEP 3

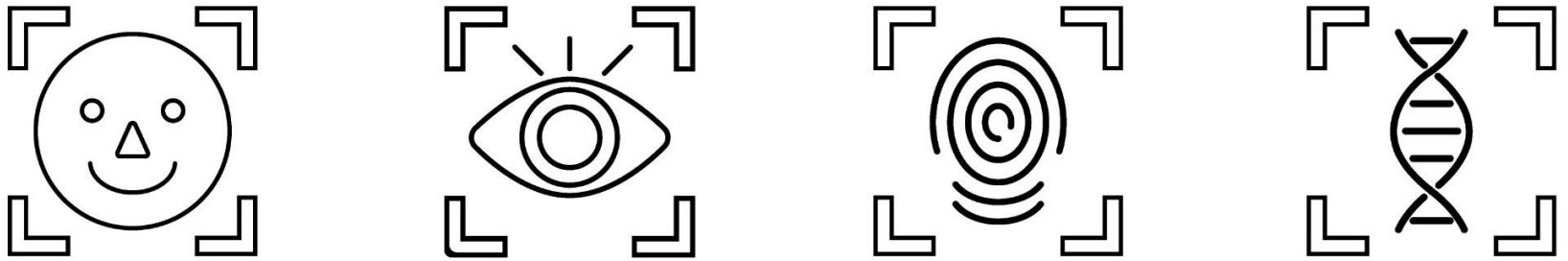
複数のサービスに対して
SSOで一括でログイン実施



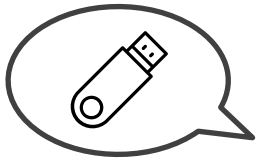
※「パスワードレス」で認証するか、ID/Passの後の第二要素の認証として利用するかは運用次第で変更が可能

パスキーとは

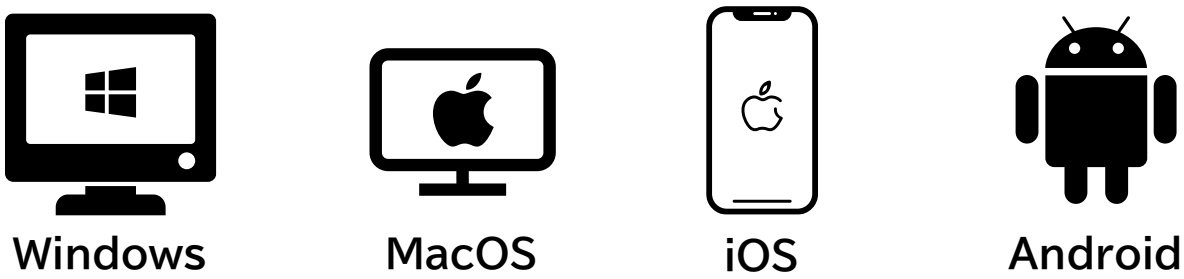
「パスキー」は非営利団体のFIDO(Fast IDentity Online、通称ファイド)アライアンスが提唱する、
技術仕様「FIDO」に基づく**パスワードレス**の認証方式で、
指紋や顔といった**生体情報**や、**PIN**などを利用し、
「認証デバイス」や「端末」で本人検証を行い、その結果をもとに認証を行う方式。



パスキーが普及している背景



従来、「FIDO（パスワードレス）」対応にあたってネックだったのが、
認証用のデバイスを別途購入しないといけないという点であったが、
昨今AppleやGoogle、Microsoftなどの主要OSを抱える
プラットフォーマーが「パスキー」の対応を拡大し、
認証用のデバイスの別途購入が不要となったことから普及が拡大。



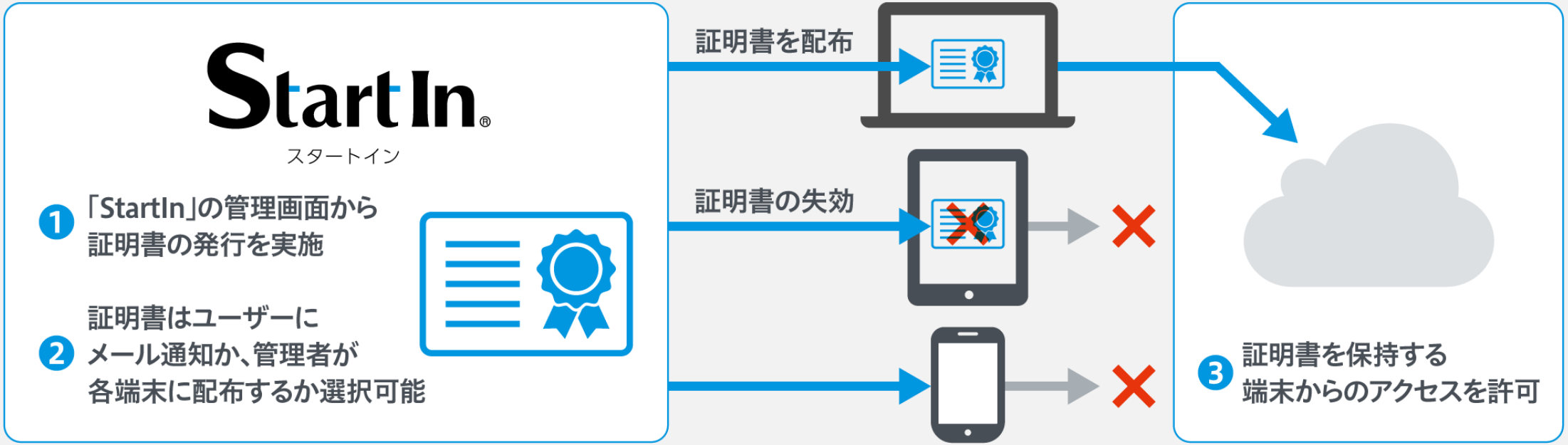
各OSのプラットフォーマーが対応したことで認証用のデバイスの別途購入が不要に

2024年6月新機能：証明書発行機能

2024年
6月新機能

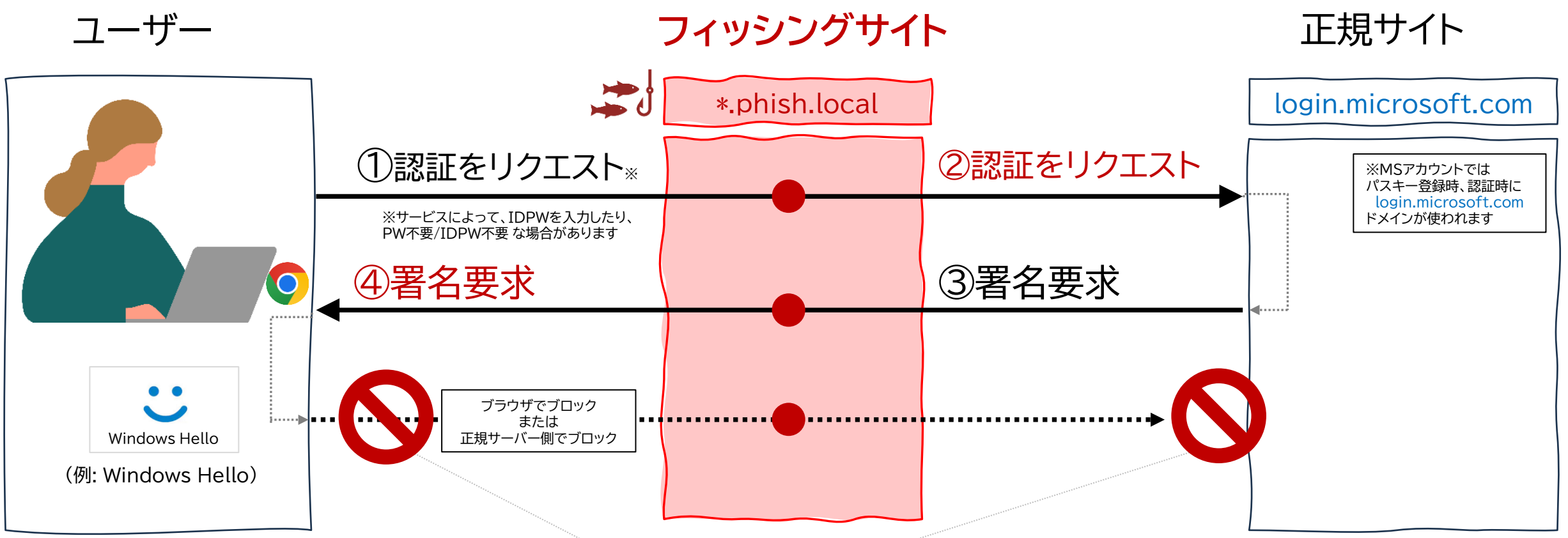
「StartIn」から証明書を発行、失効することが可能で、証明書を保持する端末にのみアクセスを許可し、保持しない端末からのアクセスを防止

事前に証明書を端末にインストールしておくことで「StartIn」がアクセスした端末が証明書を保持しているか確認



※2024年3月時点で予定している仕様であり実装にあたり仕様を変更する場合がございますのでご了承ください

AiTMが突破できない例(パスキーによる認証)



正規サイトのパスキー認証登録時、
ローカルの認証器に秘密鍵と公開鍵の
キーペアが生成され保存される。
また、RPID(※)も含まれる。

※RPID (Relying Party ID)は、認
証を行うサイトを識別するID。要するに
正規サイトのドメイン。

④のあと、「通信相手(origin)」と「登録済み正規サイト(RPID)」が検証される。例では、
通信相手はフィッシングサイト「*.phish.local」となるため、
登録済み正規サイト「login.microsoft.com」と一致せず
認証処理が中止される。

Agenda

1 IDaaS製品「StartIn」とは

2 正当アカウントを狙う動きと国内事例

3 多要素認証を回避するフィッシングについて

4 **「StartIn」の特徴、優位性について**

再掲 -「StartIn」の特徴：多要素認証

ワンタイムパスワード認証や、生体認証など一般的な認証方法に加え、
デジタルアーツ独自の認証でセキュアな世界を実現

多彩な多要素認証機能でインターネットの入り口を強固に

標準的な認証方式

＋

独自の認証方式

※標準機能として1ライセンスあたり1枚証明書発行が可能です。ライセンス数以上の証明書を利用したい場合、オプションの購入が必要となります。

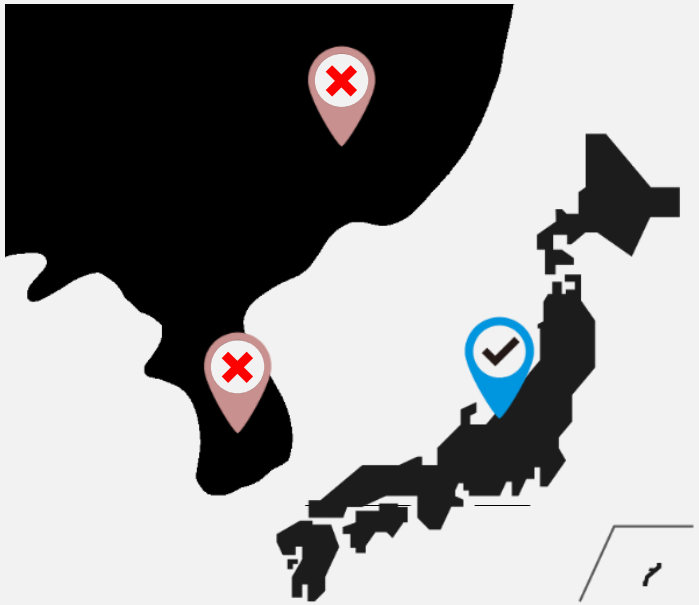
多要素認証の特徴①：位置情報認証

独自機能

位置情報を登録し、許可されたエリア内の場合に認証を許可することで
海外からのログインや勤務地、居住地以外からのログインをブロック！

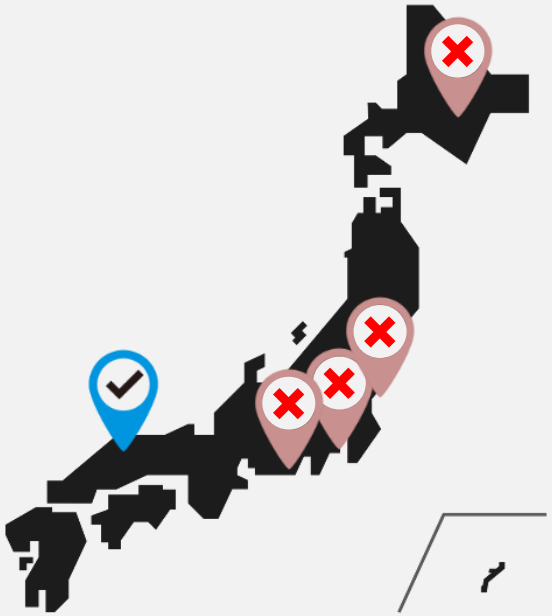
日本国内

ログイン範囲を日本国内とすることで
海外からのログインを防止可能



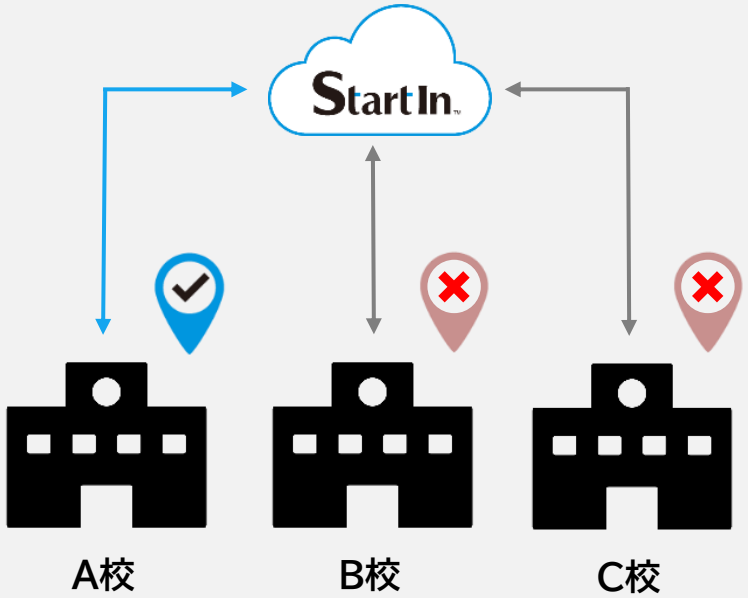
営業所・工場拠点

許可したい拠点や営業所、工場等、
都道府県やエリアごとの認証が可能



自宅・学校・病院

自宅、会社、学校など、建物単位で
認証の許可、不許可を設定可能

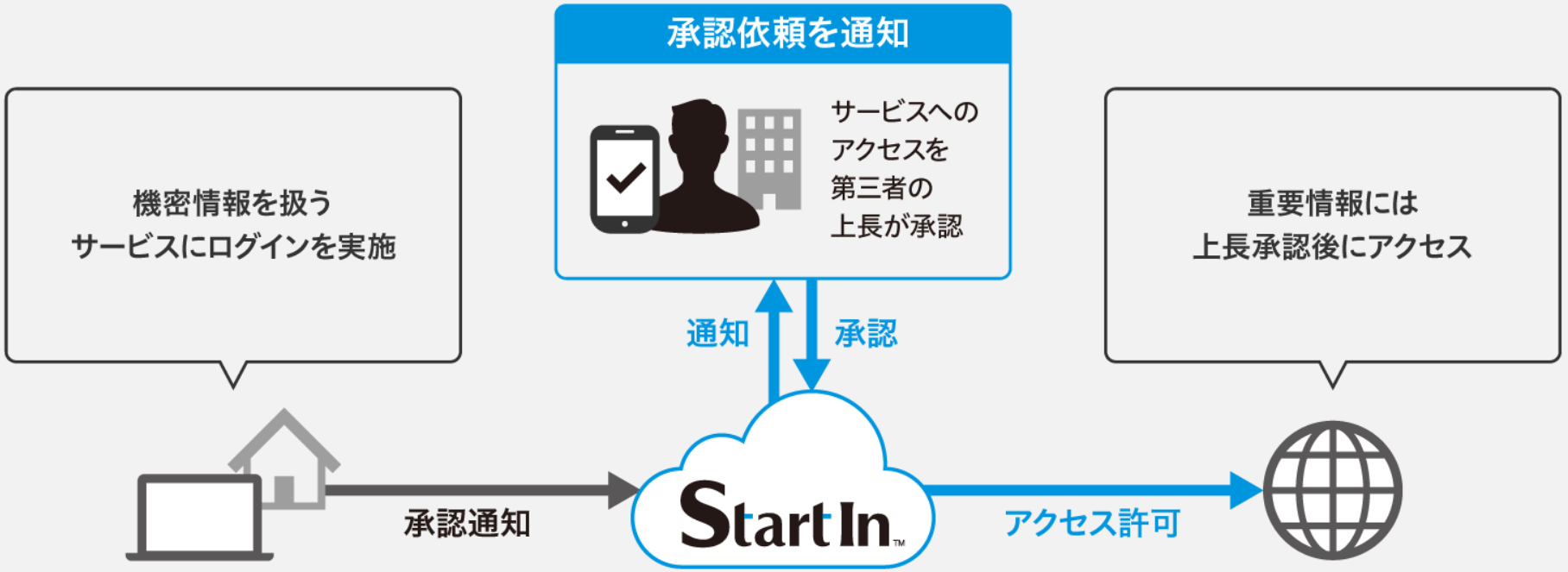


多要素認証の特徴②：第三者認証

独自機能

上長等の「第三者」が承認することで認証！機密情報を扱う際など、上長承認が可能で、承認者を複数人設定することも可能！

重要情報にアクセスする際に最終確認を「人」が実施することが可能！



多要素認証の特徴③：定期認証

独自機能

定期認証を実施することで、定期的に従業員の位置情報を確認し、認証キャッシュによるセキュリティリスクを回避！従業員の管理も可能！

通常のログインは1日1回に設定し、1日数回の定期認証により
ユーザーの継続利用を確認することで認証の強度を簡易的に向上することが可能！

今までのIDaaS

09:00 ログイン → ID/Passの入力が必要
12:00 ログイン → ID/Passの入力が必要
15:00 ログイン → ID/Passの入力が必要
18:00 ログアウト

ログインユーザー本人が継続して利用していることを確認するにはログインを短時間で無効にし、その都度ID/Passの入力から求める必要がある

「StartIn」の定期認証

09:00 ログイン → ID/Passの入力が必要
12:00 定期認証 →
15:00 定期認証 →
スマホで1クリックで承認
18:00 ログアウト

スマホの1クリック操作でログイン継続を許可。最小限の手間でユーザー本人の継続利用を確認できる。位置情報を併せて取得することで、所在の把握も可能。

「StartIn」の優位性

管理画面の分かりやすさや、会社としてのセキュリティやサポート体制
コストパフォーマンスにおいて高い評価をいただいております

① 視認性を意識したシンプルなUI

シンプルで直感的なUIで、誰でも簡単に操作することが可能。さらに、ログインやサービス利用状況をレポートで表示するため一目で利用状況を確認することが可能

② 堅牢なセキュリティ体制

セキュリティメーカーとしての技術・ノウハウを用いて、サービスの堅牢なセキュリティ対策を実現。認証としてISO/IEC 27001 、27017を取得

③ 純国産で柔軟なサポート体制

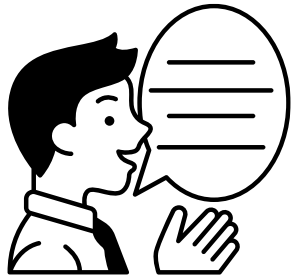
国産のセキュリティメーカーのため、管理画面やマニュアル等、日本語で分かりやすさを重視した仕様となっており、サポートも電話、メールにて迅速に対応いたします。

④ 最高のコストパフォーマンス

初期費用なしで1ユーザー300円/月で提供。
さらに「DigitalArts@Cloud」を既にご利用、もしくは同時購入をご検討のお客様には1ユーザー150円/月で提供いたします。

これまでにいただいたお客様の声

事例①

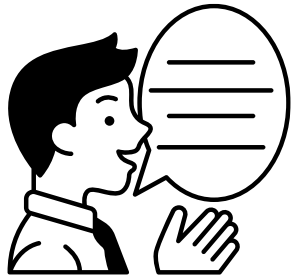


設定の分かりやすさ、柔軟性を評価

・位置情報認証設定時に、都道府県や、住所等を細かく設定できる点が良い

・テンプレートの組み合わせができる点やテンプレートに加え、利用者の住所をON/OFFで簡単に設定できる点が良い

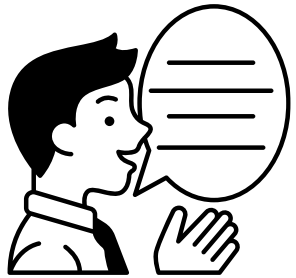
事例②



@Cloud製品の設定簡略化を評価

・既存で「i-FILTER@Cloud」と「m-FILTER@Cloud」を利用しているが、それぞれユーザー登録する手間があったが、「StartIn」では、「StartIn」上で登録したユーザー情報を各製品に反映できるため、設定の手間が省ける点が良い

事例③

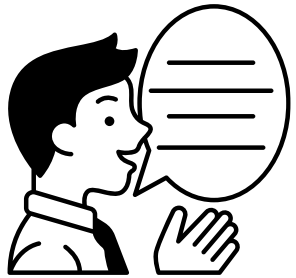


退職者のアクセス制御が容易な点を評価

・「StartIn」にて該当のユーザーを削除することで全てのサービスをアクセス不可にできるので安心できる

・ユーザーの有効期限を定められるので運用もしやすい点が良い

事例④



安価でセキュリティが強固にできる点を評価

・生体情報で本人が確認できるのに加え、証明書で端末を特定でき、かつ、位置の情報も取れるため、強固にできるのが良い

・既存で「i-FILTER@Cloud」を利用しており、低価格な点も評価

ビデオチャットやデモ実演も可能です！
ご質問等がございましたら、お気軽にお問い合わせください。

メール	sales-info@daj.co.jp
お問い合わせフォーム	https://sec2.daj.co.jp/bs/contact/

- 本書 は2024年5月現在の情報に基づいて作成しております。(※記載内容は予告無く変更される場合があります)
- 本書は、弊社「i-FILTER」、「m-FILTER」および関連製品の導入検討のためにのみご利用いただき、他の目的のためには使用しないようご注意ください。
- デジタルアーツ、DIGITAL ARTS、i-FILTER、i-FILTER Anti-Virus & Sandbox、i-FILTER@Cloud Anti-Virus & Sandbox、i-FILTER@Cloud Dアラート発信レポートサービス、info board、Active Rating System、D-SPA、Anti-Virus & Sandbox for D-SPA、NET FILTER、SP-Cache、White Web、ZBRAIN、クレデンシャルプロテクション、ホワイト運用、m-FILTER、m-FILTER MailFilter、m-FILTER Archive、m-FILTER Anti-Spam、m-FILTER Anti-Virus & Sandbox、m-FILTER@Cloud Anti-Virus & Sandbox、m-FILTER@Cloud Dアラート発信レポートサービス、m-FILTER MailAdviser、MailAdviser、m-FILTER File Scan、Mail Detox、m-FILTER EdgeMTA、EdgeMTA、FinalCode、i-フィルター、DigitalArts@Cloud、Desk、Desk Event、StartIn、f-FILTER、Dアラートおよび Dコンテンツその他の弊社・弊社製品関連の各種名称・ロゴ・アイコン・デザイン等はデジタルアーツ株式会社の登録商標または商標です。

デジタルアーツ株式会社

〒100-0004 東京都千代田区大手町1-5-1
大手町ファーストスクエア ウエストタワー14F
Tel 03-5220-3090 Fax 03-5220-1130
sales-info@daj.co.jp www.daj.jp