ID境界時代の新しいIDセキュリティのご提案（Cisco Duo ＋ ITDR）

Cisco Systems G.K.
GSSO サイバーセキュリティ製品担当　秦　寛樹

GSSO テクニカル ソリューションズ アーキテクト　山本 剛之
2024年4月25日

アジェンダ

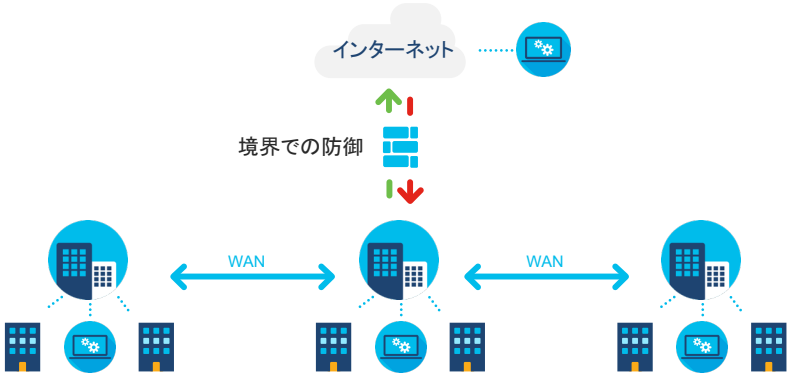
1) セキュリティ動向
2) 認証環境における課題
    I. Identity（ID）のセキュリティ
    II. 業務生産性の維持
    III. 認証環境全体の可視化
3) Ciscoの認証環境へのご提案

セキュリティ動向
(IDセキュリティの重要性)

企業インフラの動向

クラウド利用が加速・多様なユーザが多様な場所から接続・脅威が進化

拠点がベース



ユーザ/デバイス⇔アプリケーション

インフラボトルネックの解消
増え続ける接続に高まる内部脅威対策

Zero Trust へのシフト

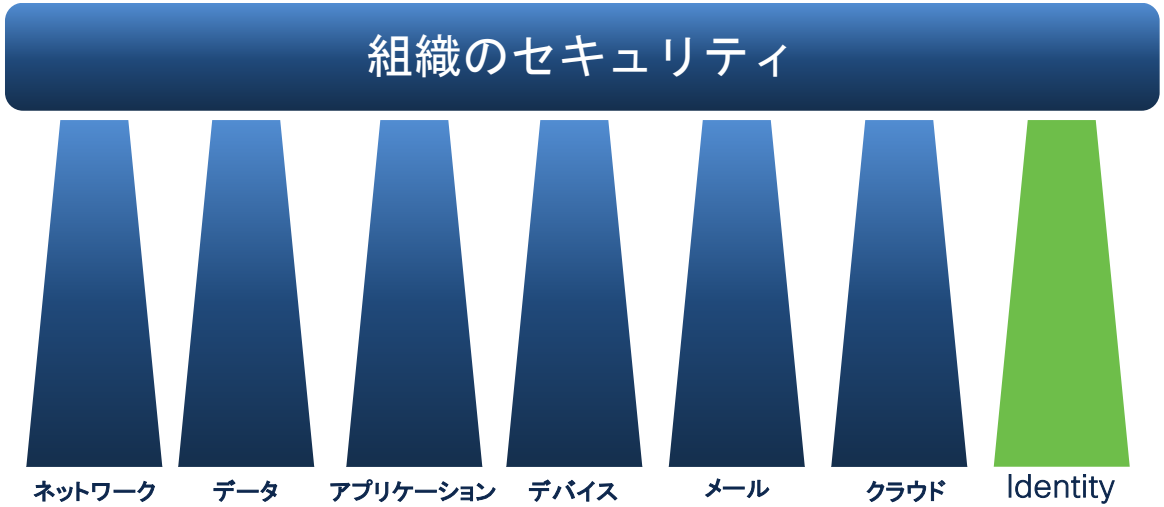
境界はエッジに分散
Never Trust, Always Verify

83%

アイデンティティに
起因したアタックの
割合（2023年）

Identity（ID）のセキュリティ

あなたの組織でIdentitiyセキュリティの重要度はどれくらいですか？



2026 年までに、何らかの組み込み型 ID 脅威検知・対応機能を使用する組織。

ガートナー、2022年

企業の優先事項トップ5に「アイデンティティの管理とセキュリティ確保」。

IDSA、2023年

なぜアイデンティティが境界となりはじめたか？

MS/Googleなどがプラットフォームをクラウド化 （オンプレ版の廃止/値上げ etc）
→ 業務に必要なリソースは、クラウド経由でないと利用できない

社員の業務管理

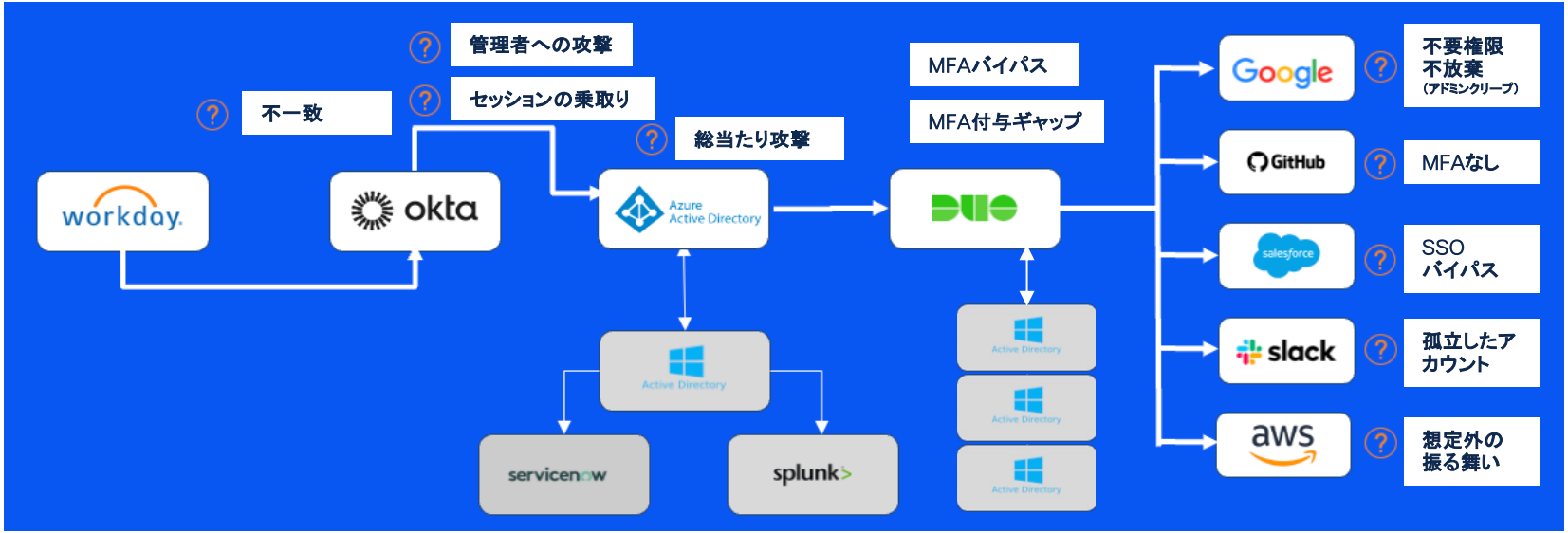
社員の人事管理

業務別の管理

クラウド上のリソースを外部攻撃(窃取など)から守る手立ては、ログインIDのみ
→ ログインID(=アイデンティティ)が防衛ライン（境界）となる

クラウド増加によりIDが分散し、攻撃が増加

個別のIDaaSやアプリケーションを管理しても、クラウドサービス利用が急増している昨今においては、包括的に管理することができなくなってきている。



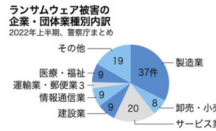
IDを狙った攻撃が増大・高度化

企業のテレワークを狙った攻撃

ランサムウェア被害、右肩上がり　テレワークに必要なVPN狙いか

有料記事

吉沢英将　2022年9月15日 11時30分



パソコンなどのデータを 暗号化 して使えなくし、復元と引き換えに身代金を要求する コンピューターウイルス 「ランサムウェア」の被害を受けたとする国内企業・団体からの申告が、今年上半期（1～6月）で114件あったと 警察庁 が15日発表し

https://www.asahi.com/articles/ASQ9H30VRQ9GUTIL00H.html

学校の個人情報を標的にした攻撃

■佐賀県の実例

本事案では無職少年が他人の実在するユーザ ID とパスワードを利用して、学校ネットワークにアクセスし侵入、さらに侵入されたネットワーク内から別の重要情報が窃取され、被害の範囲が拡大し、14,355 名の個人情報が窃取されました。

佐賀県学校教育ネットワークセキュリティ対策検討委員会（佐賀県教育委員会が設置した有識者などからなる第三者委員会。以下「検討委員会」）がまとめた提言書によれば、本事案の主な経緯は以下のとおりです。

時　期	経　緯
平成 27 年 3 月頃	ある高校においてフィッシング画面を工作した学習用 PC で教師から管理者用の ID とパスワードを取得
平成 27 年 4 月頃～	無職少年が不正アクセスを開始したと考えられる
平成 27 年 6 月 14 日	高校で校内 LAN（校務用サーバ）へアクセスできなくなる事象が発生（無職少年が不正取得し保存した 6 月 14 日付フォルダの中に、校務用サーバより取得したデータが蔵置。なお 6 月 15 日以降の校務用サーバのデータは蔵置されていない。） 上記事案を受け、全校の管理者パスワードの変更とネットワーク設定変更を実施（一部の管理パスワードを変更せず）
平成 27 年 9 月 17 日	高校のヘルプデスク現地員から、管理者の ID とパスワードを入手するため、学習用 PC にフィッシング画面を工作したが未遂
平成 28 年 1 月	無職少年が不正アクセス（立件分）
平成 28 年 2 月 15 日	警視庁から佐賀県教育委員会へ不正アクセス事案の連絡
平成 28 年 2 月 16 日	業者に対しログ保全依頼、管理パスワードの定期変更を開始（一部の管理パスワードを変更せず）
平成 28 年 3 月 11 日	警視庁から SEI-Net システムの脆弱性の情報提供
平成 28 年 3 月 15 日～	SEI-Net の脆弱性への対応を開始（4 月 27 日完了）
平成 28 年 5 月 19 日	警視庁から「パスワード変更以降も不正アクセスを行っていた可能性」について連絡があり、業者に対しサーバパスワードの変更を指示

https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/__icsFiles/afieldfile/2018/04/06/1369637_005.pdf

クラウド業者のサポートを標的にした攻撃

November 28, 2023

Oktaが2023年10月に公表したカスタマーサポート管理システム（Okta Help Center）に対するセキュリティインシデントを受け、Okta Securityは11月3日（米国時間）に共有した初期分析のレビューを継続し、脅威者が実行した行動を調査いたしました。これには、脅威者がカスタマーサポート管理システム内で実行したレポートや、脅威者がダウンロードしたファイルを手動で再現することも含まれております。

本日、お客様のセキュリティに影響を及ぼす可能性のある新たな情報を共有いたします。

追加調査の結果、脅威者がOktaカスタマーサポート管理システムのユーザーの名前と電子メールアドレスを含むレポートをダウンロードしたことを確認しました。FedRamp HighとDOD IL4環境（これらの環境では、脅威者がアクセスしたシステムとは別のサポート管理システムを使用）のお客様を除く、すべてのOktaのWorkforce Identity Cloud (WIC)とCustomer Identity Solution (CIS)のお客様が影響を受けております。Auth0/Customer Identity Cloud (CIC) サポートケース管理システムは、このインシデントによって影響を受けておりません。

脅威者は、2023年9月28日15:06 UTC（協定世界時）に、Oktaのカスタマーサポートシステムの各ユーザーの以下のフィールドを含むレポートを実行しました。

Created Date	Last Login	Full Name	Username	Email
Company Name	User Type	Address	[Date of] Last Password Change or Reset	Role: Name

病院の医療データを狙った攻撃

病院サイバー攻撃　VPN機器に安全上の欠陥、国内400台未対策

毎日新聞　2022/12/23 21:45（最終更新 12/24 07:49）　有料記事　2321文字

大阪急性期・総合医療センターへのサイバー攻撃を巡り、侵入経路とされるVPN機器のセキュリティー上の欠陥（脆弱<ぜいじゃく>性）について、未対策のまま使われている同じ製品が国内で少なくとも400台あるとみられることがサイバーセキュリティーの専門団体への取材で判明した。この製品では2021年9月に国内最大規模となる認証情報の流出事案が起きており、専門家やメーカーは「ソフトウエアの更新だけでは十分でない」と注意を呼びかけ

https://mainichi.jp/articles/20221223/k00/00m/040/178000c

クラウド業者の子会社・関連会社を踏み台にした攻撃

不正アクセスによる、情報漏えいに関するお知らせとお詫び

2023年11月27日　|　お知らせ

LINEヤフー株　　よる不正アクセス（以下、本事案）を受け、ユーザー情報・取引先情報・従業者等*1に関する情報の漏えいがあることが判明しましたのでお知らせいたします。

本件につきまして、以下の通り報告いたしますとともに、ユーザーおよび関係者の皆さまに多大なるご迷惑とご心配をおかけする事態となりましたことを、心より深くお詫び申し上げます。

なお、後述の当社へのアクセスの経路となったと推測される当社関係会社のシステムからは、当社の各サーバーに対するアクセスを遮断しております。11月27日時点でユーザー情報や取引先情報を利用した二次被害の報告は受けておりませんが、引き続き影響調査を進め必要な対応が発生した場合は速やかに対応してまいります。

利用停止中のアカウントを狙った攻撃

使用停止中のメルアカ奪われ不審メールを大量送信

“境界”の変化

ネットワークが境界

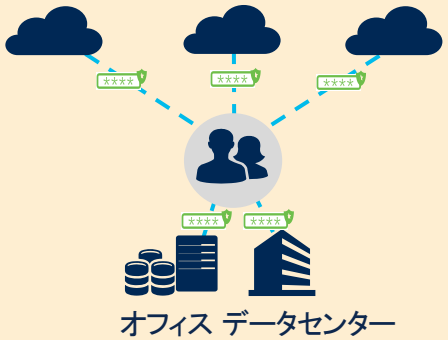
ネットワーク情報に基づいた
アクセス制御の実現(ACLなど)

エンドポイントも境界

端末の振舞い/ポスチャに基づいた
アクセス制御の実現 (検疫NWなど)

アイデンティティも境界

クラウドへのログイン情報(=アイデンティティ)に基づくアクセス制御
(MFA/SSOなど)



認証環境における課題

ID境界時代の
認証環境における３課題

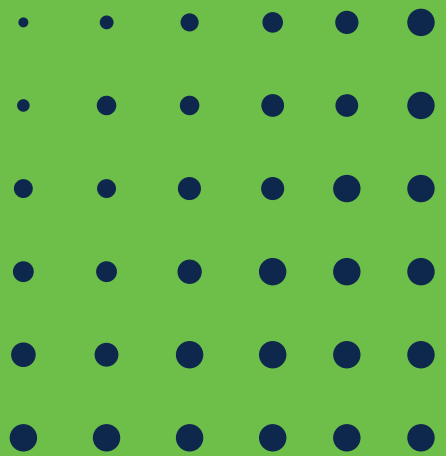
Identity（ID）のセキュリティ	境界となるIDをどのように守るか？
業務生産性の維持	増えるクラウドと共に認証が増え、業務生産性が低下することをどう防ぐか？
認証環境全体の可視化	クラウドが増えると共に増えるID管理による認証環境の複雑化をどう防ぐか？

認証環境における課題

-Identity（ID）のセキュリティ

-業務生産性

-認証環境全体の可視化

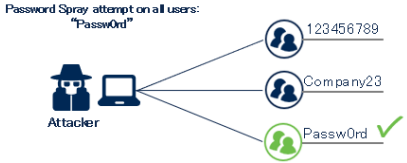


IDを狙った攻撃パターン

✓ ブルートフォース(総当たり攻撃)

Brute Force: Password Spraying [T1110.003]

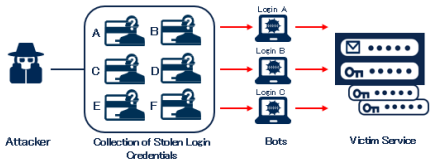
少数の一般的なパスワードを多数のアカウントに順番に試す



✓ クレデンシャルスタッフィング攻撃

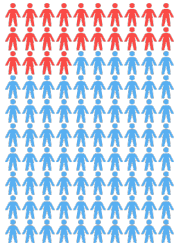
Credential stuffing attacks

他のサービスで漏洩したクレデンシャルを再利用



✓ 休眠アカウント乗っ取り

Targeting Dormant Accounts

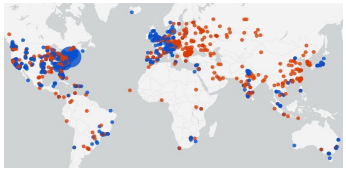


最初に MFA を適用する場合、ユーザーが次回のログイン時に最初の MFA デバイスを登録するワークフローが一般的。
APT29は休眠アカウントを何らかの方法で見つけ出し、MFAを登録を行い、正規のユーザーとしてVPNを利用出来るようになった。

✓ エグゼクティブを標的とした攻撃

Targeting Executives

最も機密性の高いアプリケーションやデータにアクセス出来るのはエグゼクティブで、セキュリティ制御に関してより多くの余裕と柔軟性を得ることができます。

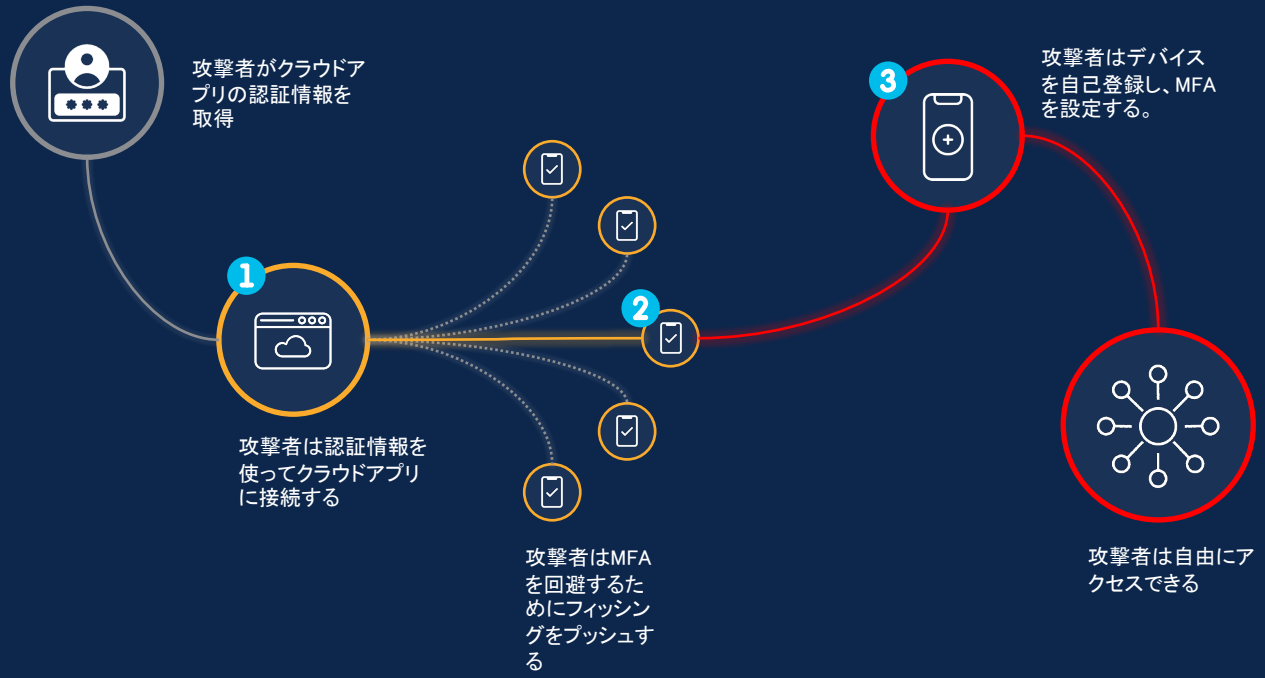


※2022 年下半期のエグゼクティブによるログインの失敗と成功

✓ ブラウザ保護クレデンシャルの窃取

ブラウザの保護した認証情報を保持するクラウドに不正アクセス
→様々な認証情報をまとめて取得

クラウドを狙った攻撃

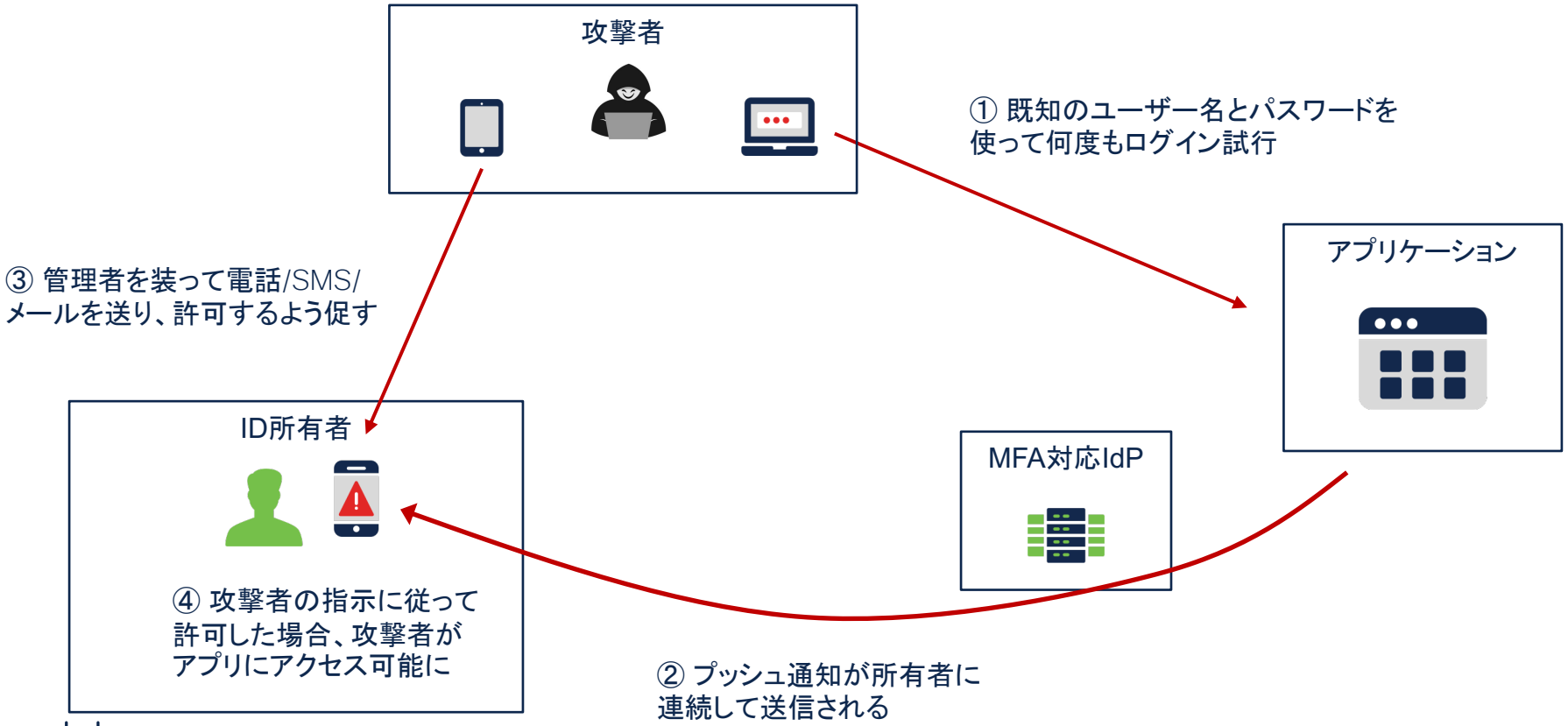


使用されている攻撃技術

- 有効なアカウント利用
有効なアカウントを使ってアクセスする MITRE ID T1078
- デバイス登録
二要素認証(2FA)を行うための代替デバイスの登録 – MITRE ID T1098.005
- MFA リクエスト生成
リクエストでユーザーを疲弊させることでMFAをバイパスする – MITRE ID T1621

攻撃事例とDemo

デモ: 多要素認証疲労攻撃



デモ: 多要素認証疲労攻撃

多要素認証(MFA)バイパス攻撃の事例 – Uber

攻撃内容

- ✓ 2022年9月、Uber EXTの契約者のアカウントが攻撃者により侵害を受けた。
- ✓ 契約者の個人所有の端末がマルウェアに感染し、パスワードが流出した後、攻撃者がダークウェブで契約者のUberコーポレートパスワードを購入したと思われる。 その後、攻撃者は、契約者のUberアカウントへのログインを繰り返し試み、その都度、契約者はMFAログイン（プッシュ通知）の承認要求を受け、当初はアクセスをブロックしていました。しかし、攻撃者のプッシュ疲労攻撃により、最終的に契約者はMFAログインを承認してしまい、攻撃者はログインに成功した。
- ✓ その後、攻撃者は他の複数の従業員アカウントにアクセスし、最終的にSlackなど多くのツールへのアクセス権限を与えることができた。

検知 / 分析 / 対策

検知 セキュリティ監視プロセスにより、問題を迅速に特定し対応に移ることができた。

分析 システム、ユーザーアカウント、クレジットカード番号や銀行口座情報などの機密情報へのアクセス、コードの変更、顧客データやユーザーデータへのアクセスも確認されていない。ただし、攻撃者は社内のSlackメッセージをダウンロードし、財務チームが一部の請求書を管理する社内ツールから情報にアクセスしたりダウンロードした可能性あり。

対策 主要なアクション：

漏洩した、または漏洩の可能性がある従業員のアカウントを特定し、Uberのシステムへのアクセスをブロックするか、パスワードのリセットを要求

社内ツールへのアクセスを回復する際には、従業員に再認証を求めました。また、多要素認証（MFA）ポリシーをさらに強化

出展：https://www.uber.com/newsroom/security-update/

認証を守るための各種ガイドライン

参考）各種セキュリティガイドライン

MFA（多要素認証の記載）

デバイス健全性の記載

多要素認証とデバイス健全性確認は同時に実現することが明記

自動車産業サイバーセキュリティガイドライン

【規則】・インターネットを経由した認証において、知識、所持、生体の いずれか 2 つ以上の認証を実装すること

【規則】・サポートのある OS、ソフトウェアを利用すること ・やむを得ずサポート切れの OS 、ソフトウェアを利用する場合は、できる限り脆弱性悪用のリスクを低減すること

医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起）（令和4年11月10日）

3-(1)-② なりすまし、不正ログイン対策 組織外からの認証・認可の対象や範囲を特定し、限定する。多要素認証等の 強固な認証方式を採用するとともに、アクセスや認証のログを取得し、監視 する。

〇VPN 装置を含むインターネットとの接続を制御するゲートウェイ装置の脆弱性 は、攻撃に悪用される可能性があるので、セキュリティパッチ（最新のファーム ウェアや更新プログラム等）を迅速に適用する。

地方公共団体における情報セキュリティポリシーに関する自治体ガイドライン（令和4年3月版）

②情報のアクセス及び持ち出しにおける対策 （ア）情報のアクセス対策 情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を 併用する認証（多要素認証）を利用しなければならない。

⑥職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を庁内のネットワーク に接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等 を確認し、情報セキュリティ管理者の許可を得るか、もしくは情報セキュリティ管理者によって事前に定義されたポリシーに従って接続しなければならない。

教育情報セキュリティポリシーに関するガイドライン（令和4年3月版）（令和4年3月版）

教育情報システム管理者は、取り扱う情報の重要度に応じてパスワード以外に生体認証や物理認証等の多要素認証を設定しなければならない。特にアクセス制御による対策を講じたシステム構成の場合、校務情報等の重要な情報資産へのアクセスについては、多要素認証を必須とすること。

教職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を施設内のネット ワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの 適用状況等を確認しなければならない。

PCDISS4.0

8.4.2 カード会員データ環境（CDE）へのすべ てのアクセスに多要素認証が適用される。

悪意を持った行為者は、セキュリティの脆弱性を利用して、システムに特権的にアクセスすることができます。これらの脆弱性の多くは、ベ ンダが提供するセキュリティパッチによって修正され、システムを管理する主体によってインストールされなければならない。

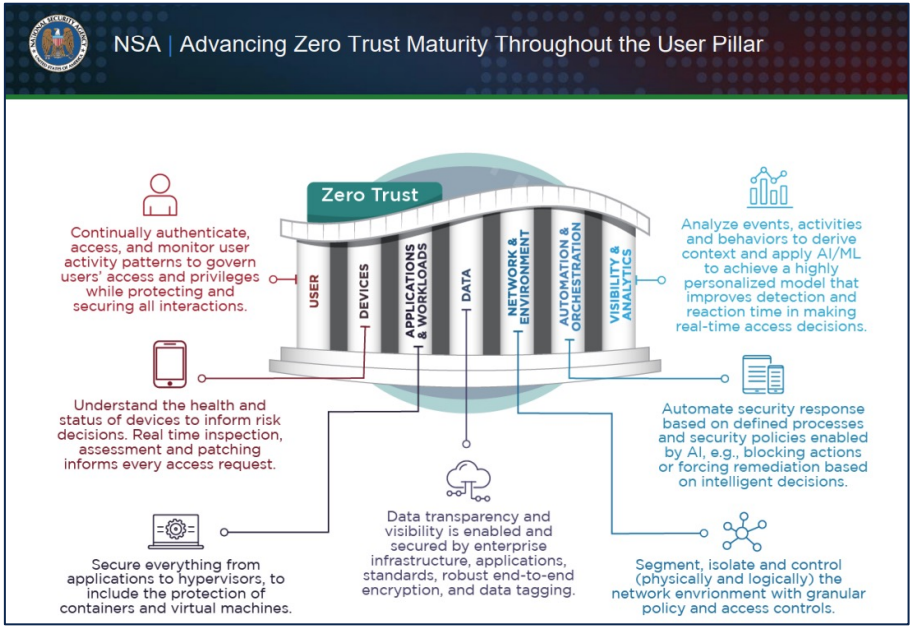
（ご参考）National Security Agency（米国）Cybersecurity Information Sheet

ゼロ・トラスト成熟の推進の柱　概要

- ハッキングによる侵害の80%以上は、紛失や盗難を問わず、ユーザーになりすますためのクレデンシャルが関与しています
- ユーザーになりすまし、さらなる侵害を行うものであった
- このようなサイバー事件は増加の一途をたどっており、経済的混乱と国家安全保障への影響をもたらしている。

- 成熟したZTフレームワークに沿った能力を構築するには、企業内のあらゆるシステムを、定義されたコントロールと統合する必要がある。
- ユーザー、デバイス、データ、アプリケーション／ワークロードの7つの柱ごとに定義されたコントロールと、企業内のすべてのシステムを統合する必要がある。

- 継続的なユーザ認証の検証とリアルタイムのデバイス健全性確認が必須



https://media.defense.gov/2023/Mar/14/2003178390/-1/-1/0/CSI_Zero_Trust_User_Pillar_v1.1.PDF
2023年4月版 ver.1.1

（ご参考）CISA（米国）からリリースされたガイダンス

Phishing-Resistant and Numbers Matching Multifactor Authentication

概要

- 2022年10月31日にリリース（MFAの脅威に対する2つのファクトシート）
- モバイルプッシュ通知のフィッシングや既知の攻撃に対して、耐性を持ったMFAの導入を推奨
- モバイルプッシュ通知ベースのMFAを使用しており、フィッシング耐性MFAを実装できない場合、番号マッチングによりMFA疲労を軽減することを推奨

Implementing Phishing-Resistant MFA

- 一部のMFAは、フィッシングに対して脆弱（”プッシュ爆撃” 攻撃 、SIMスワップ攻撃など）
- ゼロトラストの原則を適用する一環として、フィッシングに強いMFAを実装することを強く推奨
- フィッシング耐性MFA：例）FIDO2/WebAuthn（生体認証）

Implementing Number Matching in MFA Applications

- プッシュ通知MFAを利用している場合、番号マッチング利用を推奨

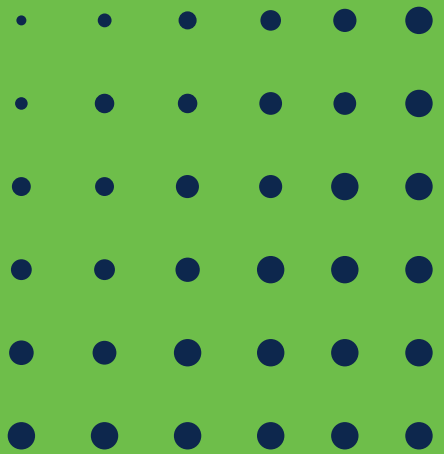
https://www.cisa.gov/uscert/ncas/current-activity/2022/10/31/cisa-releases-guidance-phishing-resistant-and-numbers-matching
https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf
https://www.cisa.gov/sites/default/files/publications/fact-sheet-implement-number-matching-in-mfa-applications-508c.pdf

認証環境における課題

-Identity（ID）のセキュリティ

-業務生産性の維持

-認証環境全体の可視化



業務環境の複雑化

増える脅威 と 増えるクラウド利用

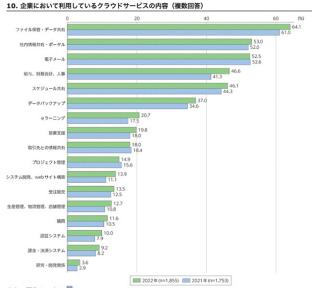
- 不正侵入
- データ窃取
- ランサムウェア
- ラテラルムーブメント
- Web上の脅威
- クレデンシャルの盗難
- スパム
- フィッシング
- 機械学習攻撃
- ・・・

困難な認証管理

クラウドを利用している企業

72.2%

多くの企業が複数利用

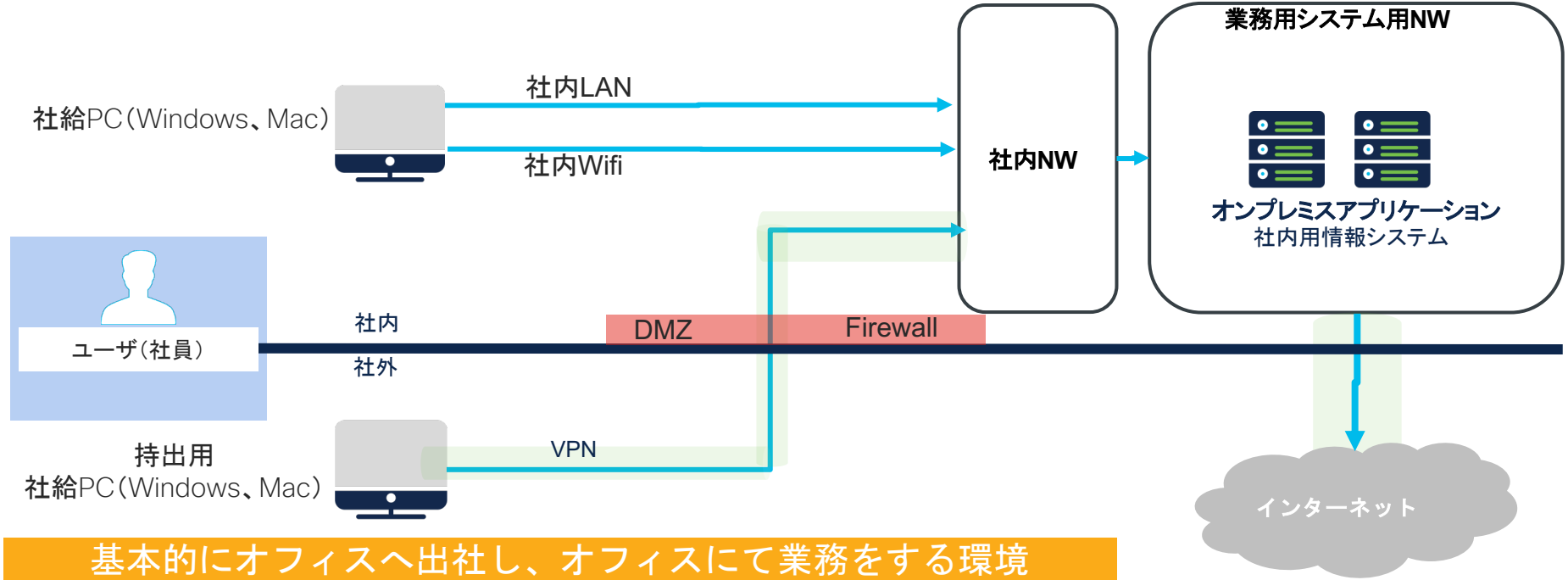


（出典）総務省「通信利用動向調査」

増えるクラウド利用と共に新たな脅威が増え、コストと運用の負担を強いることになる

業務環境①:オフィス中心の働き方

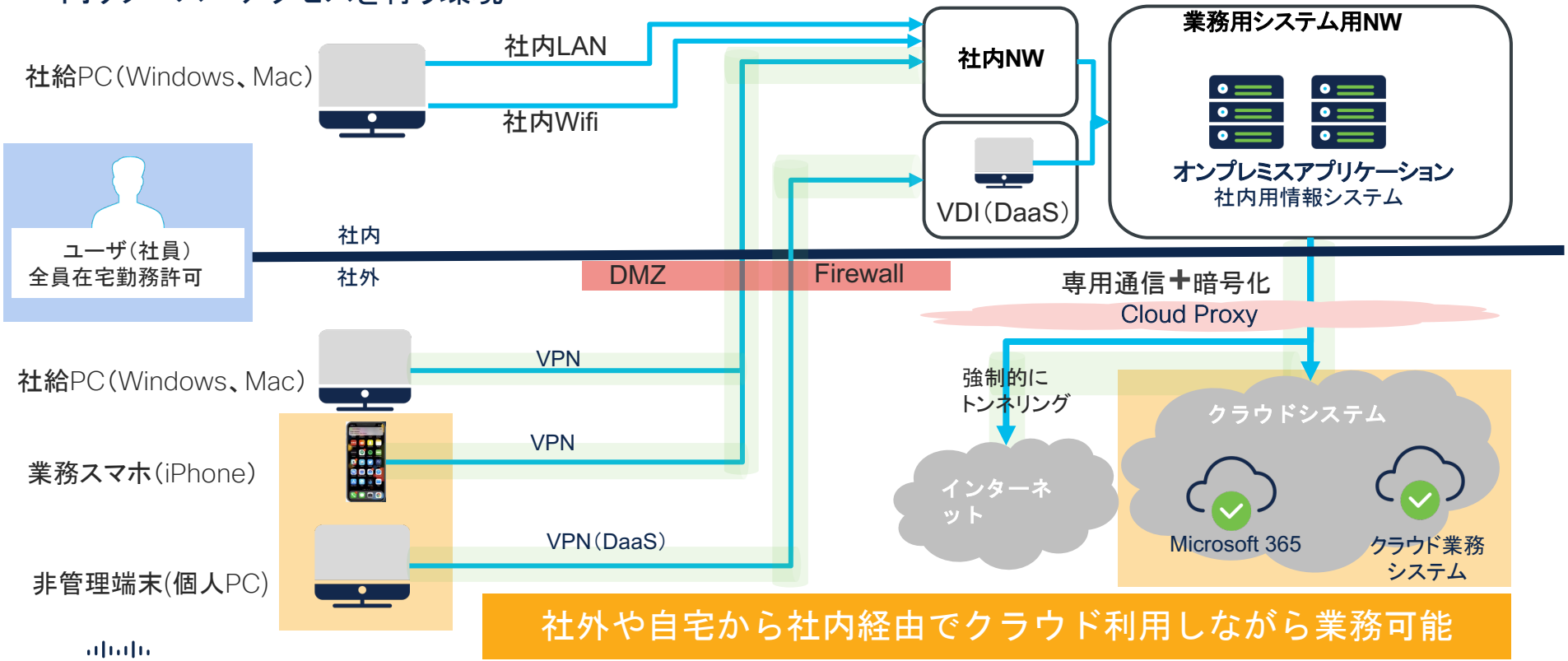
オフィス内からはオフィスLAN・Wifiでアクセス、社外からはVPNを経由した社内NWへのアクセス、業務用のオフィス内NW内に置かれた全ての社内リソースへアクセスを行う環境



基本的にオフィスへ出社し、オフィスにて業務をする環境
例外として、持出用PCにて社外から業務可能

業務環境②：クラウド利用・社外業務可能な働き方

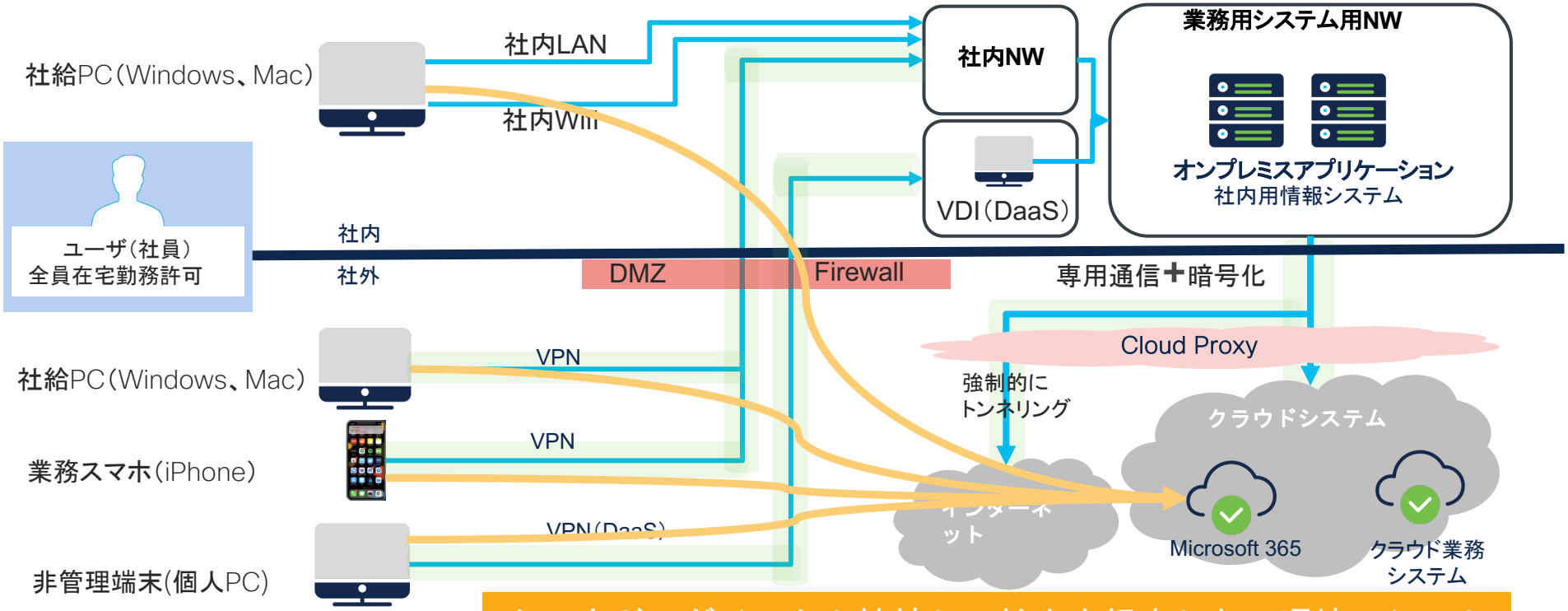
社外からはVPNを経由した社内NWへのアクセス、必要に応じVDIも併用して、クラウドも含めた全ての社内リソースへアクセスを行う環境



社外や自宅から社内経由でクラウド利用しながら業務可能

業務環境③：クラウド・リモートワーク中心の働き方へシフト

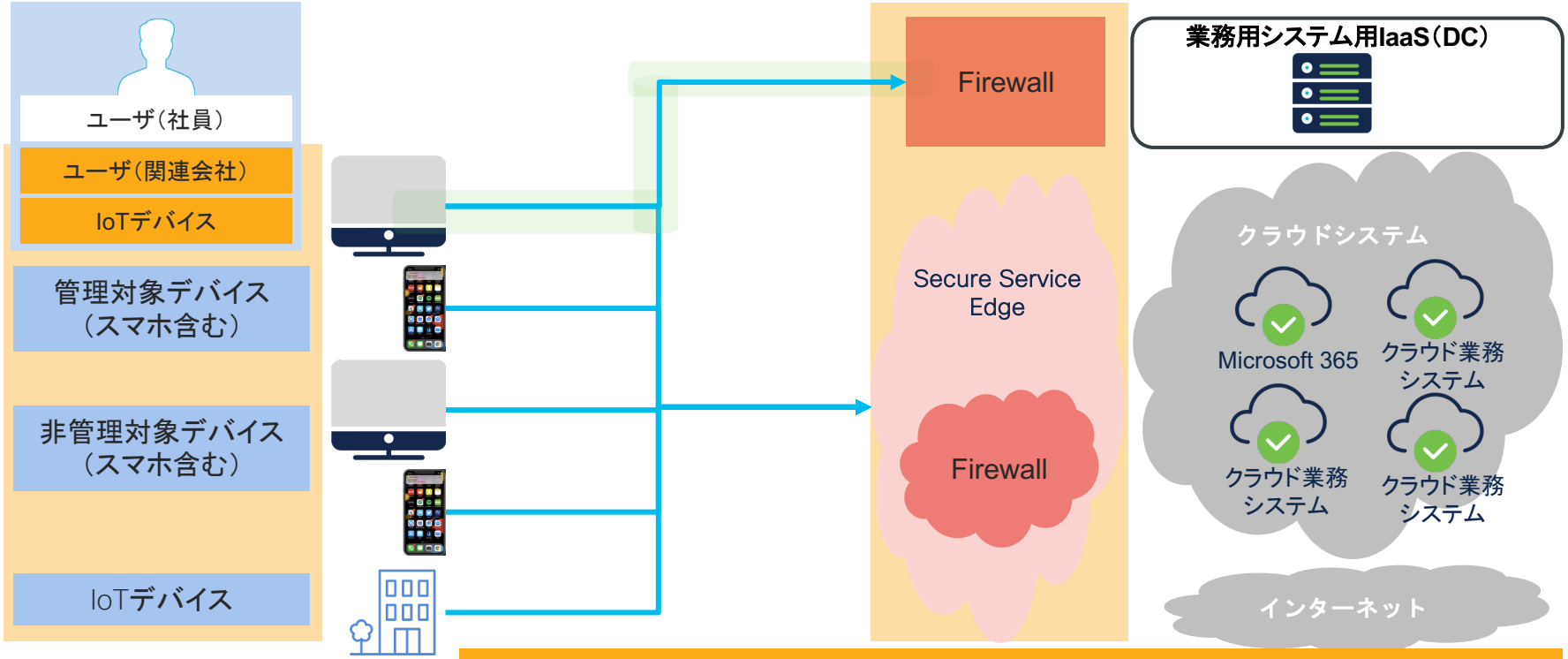
環境②に加えて、一部のクラウドシステムに限り直接クラウドを参照できるよう環境



クラウドへダイレクト接続し、社内を経由しない環境へシフト

今後の環境：クラウド・リモートワークのみの働き方

ユーザ及びデバイスは管理・非管理で分別され、接続するサービスごとにアクセスレベルが設定される。



社内・社外の概念が消え、クラウド・リモートワークのみに

今後想定されるリモートアクセスの多様化

リモートアクセス頻度の増加

- コロナ期間にリモートアクセス環境が構築されたため、必ずしも出社する必要がなくなっている
- 出勤率は上昇しているが、リモートアクセス環境があるため出先から社内リソースを使う事も増加

重要アプリへのセキュリティ適用

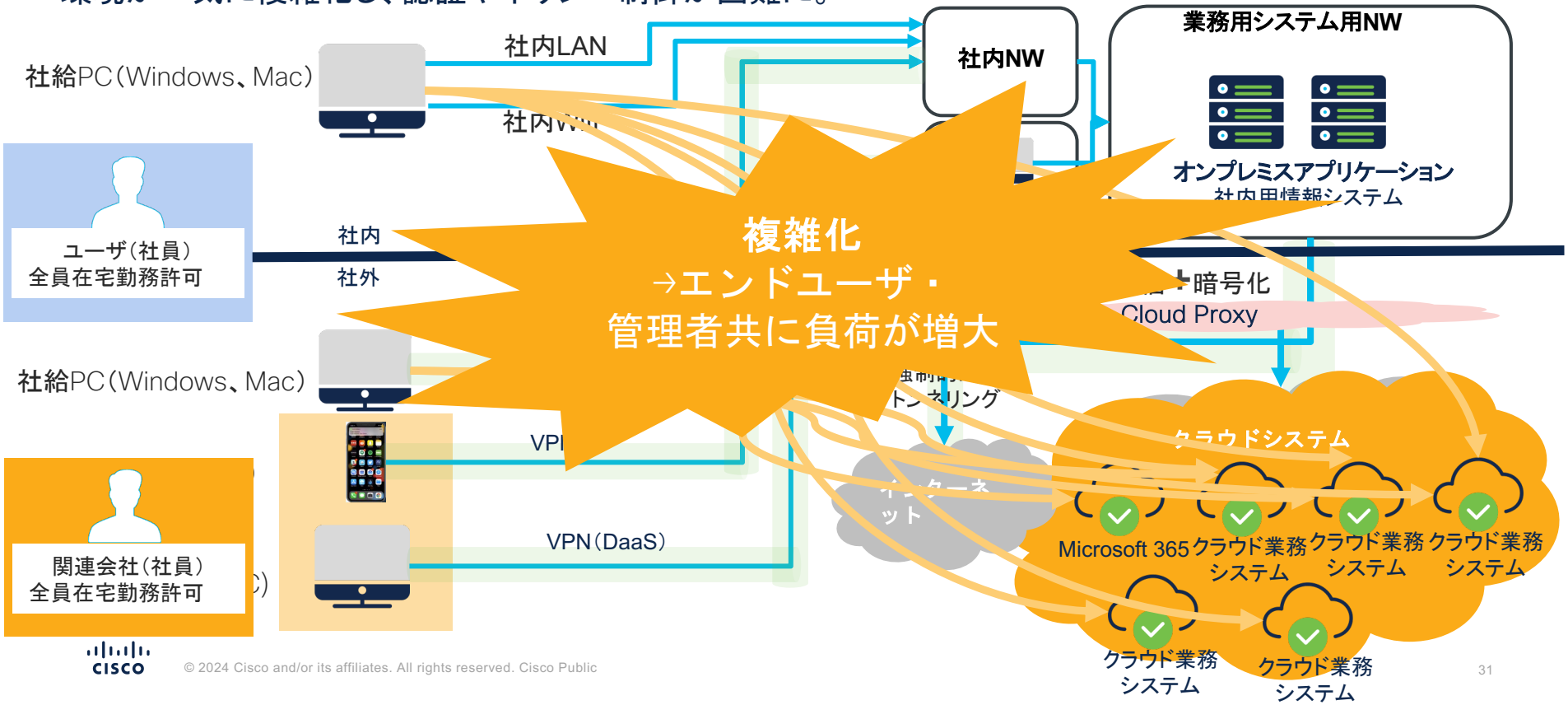
- 重要情報を含む内部システムや開発情報については必要関係者のみがアクセスできるよう厳格な管理が必要

アプリケーション重要度に応じたゼロトラストポリシーの例

機密レベル	アプリケーション例	ユーザロール	接続元ロケーション	認証要素	セッション保持	デバイス信頼性	OS	ブラウザ	EDR/EPP（AV）
重要機密を扱うアプリケーション	個人情報取扱・基幹アプリ・インフラ	特権ユーザ	限定的	フィッシング耐性MFA（Verify Push or 生体認証）	セッションは保持しない（都度確認）	管理端末のみ（BYOD禁止）	アップデートされたOSのみ	Chromeはアップデートされた状態	有効な状態（脅威インテリジェンスによる保護）
コンフィデンシャル情報を扱うアプリケーション	クラウドストレージ クラウドメール Microsoft 365 box	ナレッジワーカー	Any	MFA・リスクベース認証	リスク状態に応じたセッション保持	管理端末（条件付きでBYODは許可）	アップデート猶予期間あり	アップデート猶予期間あり	有効な状態
一般アプリケーション	その他一般アプリケーション	全社員	Any	MFA・SMS・ワンタイムパスワード	一定期間のセッション保持	Any	EoL以外	アップデート猶予期間あり	Any

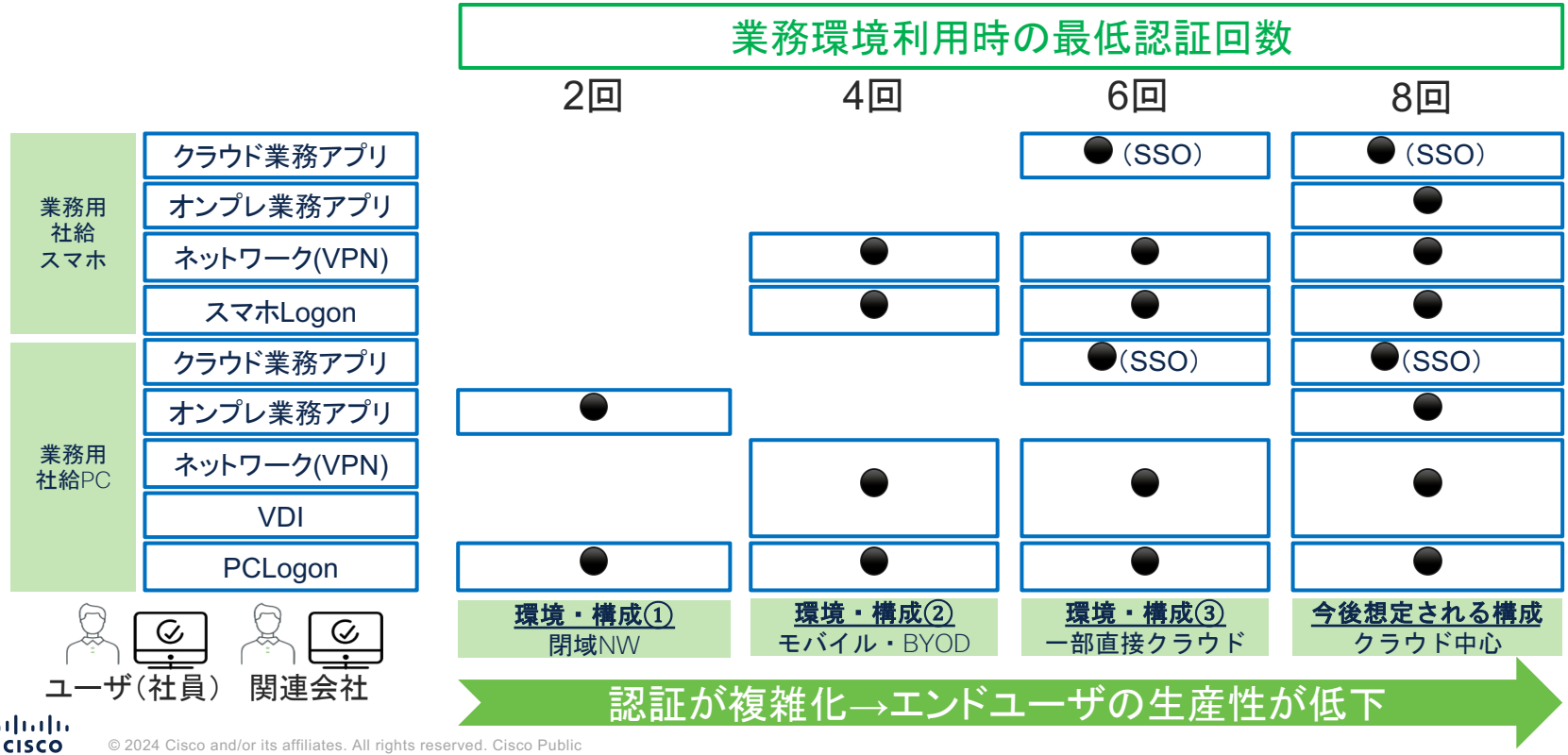
現在お客様環境で起きていること

社員に加え、関連会社社員が自社NWにアクセスして業務を行うケースが増え、クラウド接続が増加すると環境が一気に複雑化し、認証やポリシー制御が困難に。

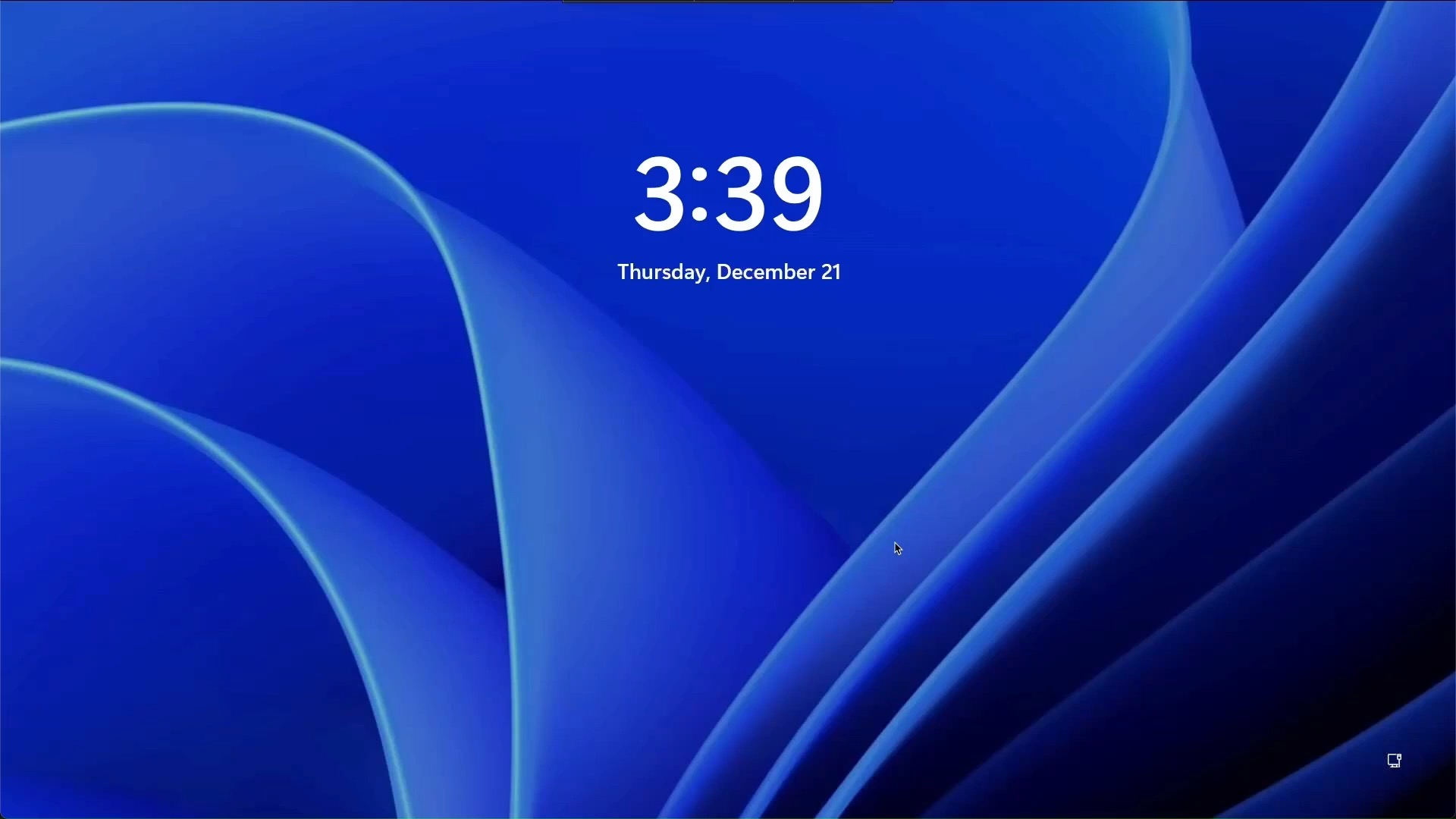


業務環境利用時の認証回数

SSOを利用できない、異なるIDPを利用している等、クラウド環境への移行及びセキュリティの強化を図ると認証回数が増え、エンドユーザの生産性低下につながる



Demo

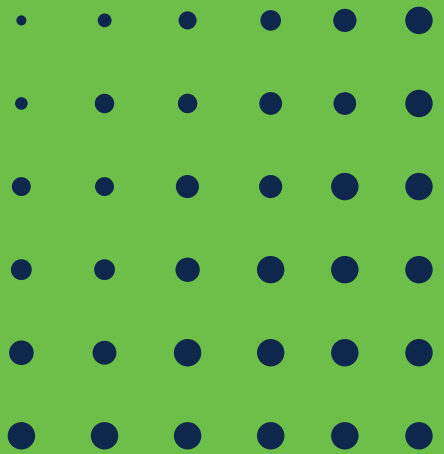

3:39
Thursday, December 21

認証環境における課題

-Identity（ID）のセキュリティ

-業務生産性の維持

-認証環境全体の可視化



ITDR (ID Threat Detection and Response) とは

2022年にGartnerによって提唱

侵入前の対策

侵入後の対策

IDに対する攻撃

ID管理・保護・予防対策
- MFA（Multi-Factor Authentication）
- IAM（Identity Access Management）
- PAM（Privileged Access Management）
- IGA（Identity Governance & Administration）
- CIEM（Cloud Infrastructure Entitlement Management）

検知(Detection)
- 認証ソースのトラフィックの分析
- AD設定の監査
- 不正なアクセス権限取得の検知
- 異常な振舞いの検知
- 脅威インテリジェンスやダークウェブ情報との合致

等

対応(Response)
- 脅威の隔離
- IDの削除・無効化
- MFAのリセット
- ログアウトの強制
- 脅威に応じた自動メッセージの送信
- レポート、報告
- XDRとの連携

等

侵入

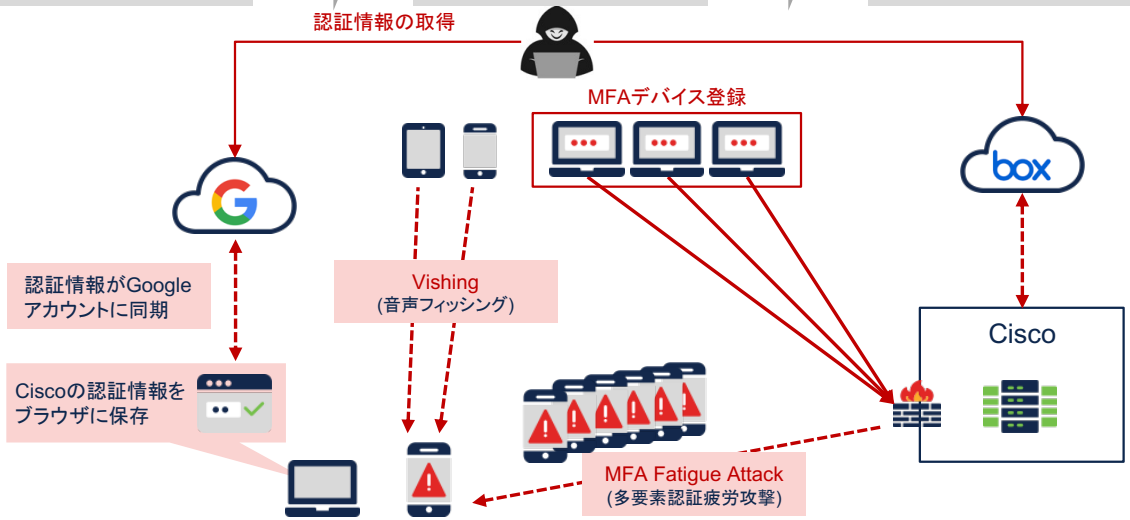
ITDR の提供範囲

ITDRの主目的：ID・認証情報をモニタリングし、脅威や不正を検出・防御すること

なぜITDRが必要か？

クレデンシャル漏洩が多発/ID攻撃が長期的な攻撃に変化

初期侵入 → 権限昇格 → 特権昇格 → 横展開



攻撃者はクレデンシャル情報を不正に入手した後、その権限を昇格させることを目的に環境内に長期間活動を継続する。
その間に横展開を目的に、ユーザ・デバイスの追加、活動ログの削除等痕跡を残さず、社員として活動できる環境を構築する

ID・認証情報が漏洩していることを前提としたモニタリングを実施し、脅威や不正を検出・防御する必要性が出てきた

Ciscoの認証環境へのご提案

ID境界時代の
認証環境における３課題へのご提案

	セキュリティと生産性向上の両立を実現
Identity（ID）のセキュリティ	**パスワードレス認証とリスクベース認証** MFAの中でもより強固な生体認証を利用するFIDO2の認証とリスクに応じてより強固な認証を要求するリスクベース認証でIDのセキュリティを確保
業務生産性の維持	**シームレスログオンによる認証回数削減** PCデバイスへのログイン情報を保持し、SAMLのSSOへも認証することなくログオンできるようにするソリューションにて業務生産性の向上を実現
認証環境全体の可視化	**ITDR機能により認証環境全体を可視化** IDに関わる全ての情報を収集し、IDの可視化を実現。問題がある場合には即時対応が可能

CiscoのVision
セキュリティと生産性向上の両立を目指して

Ciscoの解決を目指す課題（Vision）

"ユーザー認証のUXが悪いと、社員のアジリティが低下したり、顧客の離脱が増えたりします。最終的には、業務パフォーマンスを低下させ、ビジネス収益を減少させます。"

Gartner: Market Guide for User Authentication, Report

LEE
EMPLOYEE

"何度も何度も認証せずに仕事をしたい"

KIT
IT ADMINISTRATOR

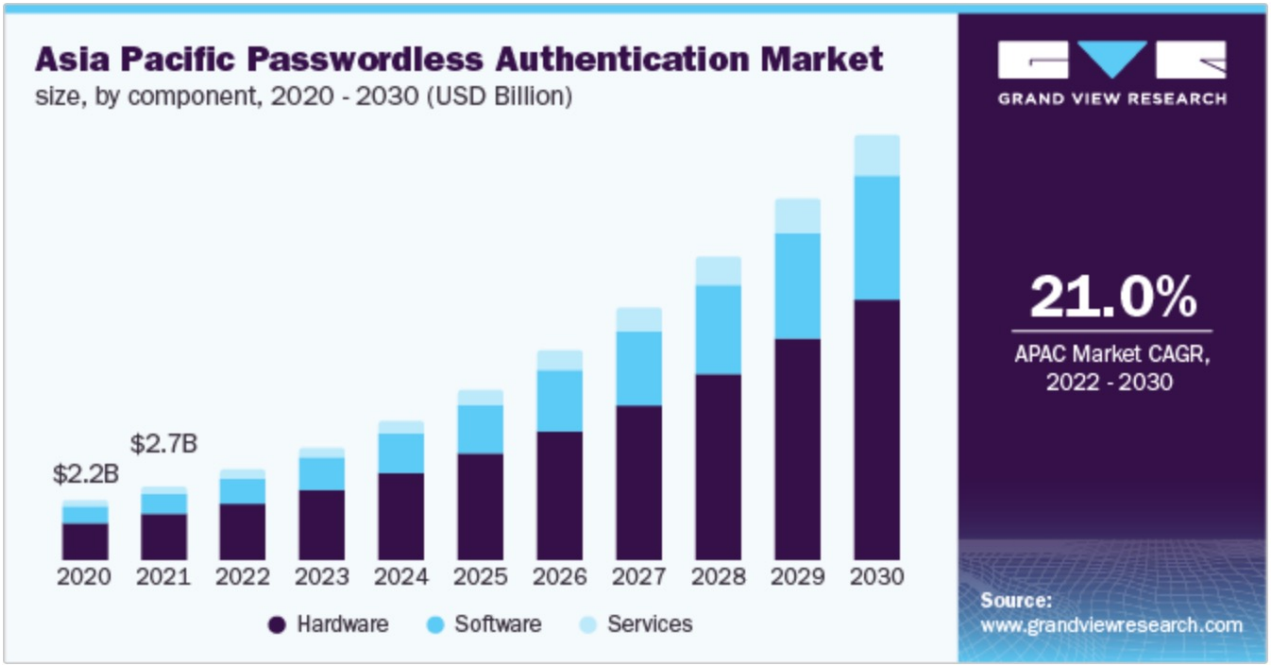
"すべてのアプリケーションに強力な認証を導入するために、関係者の賛同を得るのに苦労しています。より寛容な環境を用意せざるを得ない。"

Duo機能
パスワードレス認証
リスクベース認証

Duoパスワードレス認証（生体認証）

セキュリティ	パスワードレス認証	ユーザビリティ
非常に高い	2ファクター ・Something You Are ・Something You Have	非常に高い
生体認証	キーペア 秘密鍵 / 公開鍵	1ステップで認証

パスワードレス市場はCAGR20%を超える市場



なぜ今パスワードレス認証なのか？ World Economic Forum 調査結果より

- ✓ 従業員は年間平均11時間パスワードの入力とリセットに費やしている。（15,000人企業で年間520万ドルのコストに相当）
  employees worldwide spend an average of 11 hours each year entering or resetting their password. For a company of 15,000 employees, on average, this represents a direct productivity loss of $5.2 million.
- ✓ サインイン成功の確率を99.9%にあげることでサインイン時間を78%削減可能。同時に攻撃対象を激減可能。
  US financial software company has been able to bring its authentication success rate to 99.9% and reduce signin time by 78%. Because of its simpler user experience, the company was also able to introduce other security features, shortening the life of the authentication tokens and dramatically reducing the potential attack surface.
- ✓ パスワードレスに移行することで企業侵害リスク対策予算を5分の4に削減可能。
  From a risk management perspective, this implies that transitioning to passwordless authentication allows companies to cut the budgets associated with their breach risk exposure by 4/5.(80% of all data breaches involve weak or stolen passwords)
- ✓ ITヘルプデスク予算を20%から50%削減可能。（1コールの問い合わせコスト：$30-$70）
  20% to 50% of all calls to the IT helpdesk concern password resets, and the estimated cost of a single reset ranges from $30 to $70.
- ✓ Google社ではFIDOに基づく認証で認証にかかる時間が3分の2に。認証失敗率0%（OTP利用時は3%）
  Google employees use FIDO-based security keys to authenticate internally. Total time spent authenticating with security keys dropped nearly two-thirds. Most importantly, there were zero authentication failures. In their examination of the time period studied, the failure rate for OTP-based authentications was 3%.

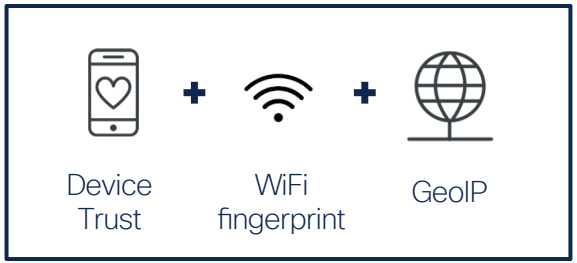
https://www3.weforum.org/docs/WEF_Passwordless_Authentication.pdf

リスクベース認証：Risk Based Authentication

New

エンドユーザによるアクセス

トラストエンジン（解析、シグナル）



エンドユーザアクセス許可

認証
Passwordless
多要素認証

追加認証の採用

信頼性が低い	**信頼性が高い**
エンドユーザーの負担増	**フリクションレス**
追加検証が必要	MFA不要 生体認証不要

認証よりセキュアなファクターへのステップアップ
YubiKey
Biometrics
Verify Push (Passcode)

リスクベース認証：Risk Based Authentication

既知の攻撃パターンが検出されると自動的にステップアップ認証を要求

User Marked Fraud

ユーザーにより認証要求が不正であることを示す

Push Harassment

ユーザーが複数のプッシュを受信し、そのすべてが失敗している

Push Spray

1つのIPアドレスが複数の異なるユーザーにリクエストを送信

Consecutive Failures

1つのIP + IKEY (integration key) に複数の障害が発生

Country Code Mismatch

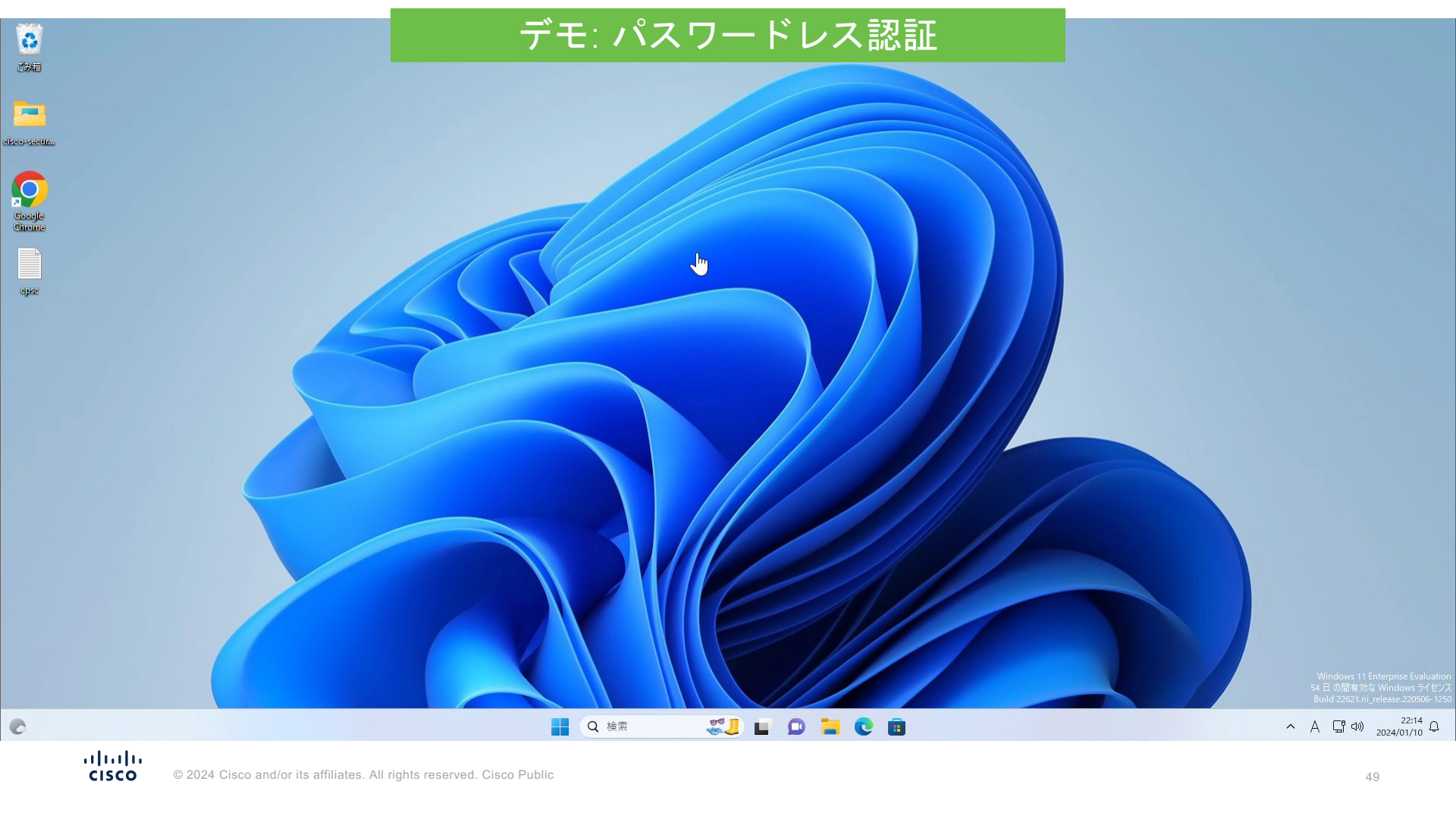
認証デバイスとアクセスデバイスが別々の国にある場合

Unrealistic Travel

最後に認証に成功した時間/場所から、到達することが不可能な場所から認証されたユーザー

セキュリティ強化
Demo

デモ: パスワードレス認証



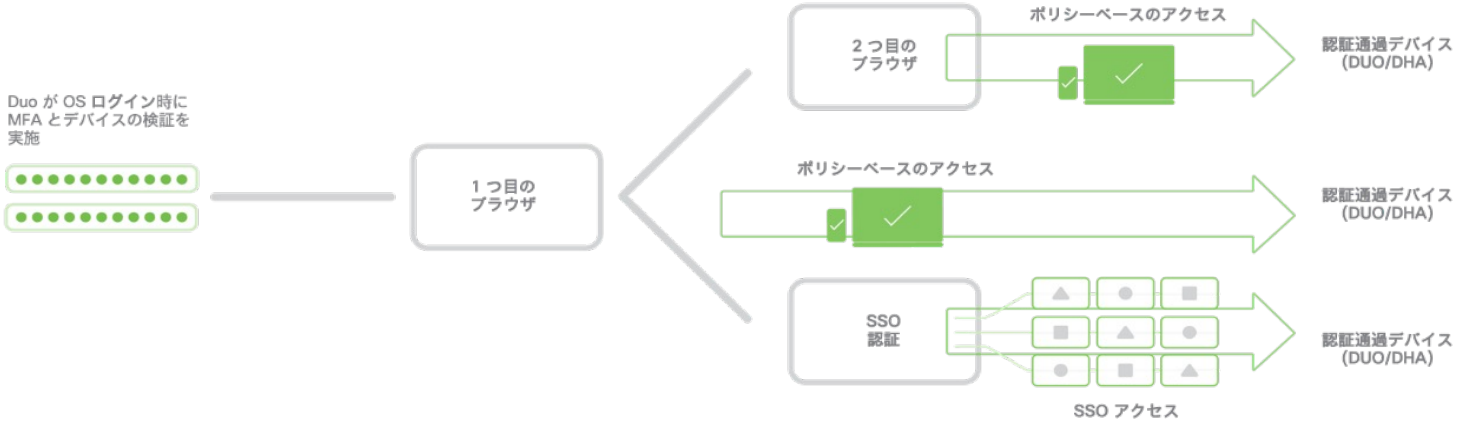
デモ: リスクベース認証 (平常時)

デモ: リスクベース認証 (リスク検知時)

生産性向上
Demo

Streamline Authentication (Desktop SSO)
1回の認証で中断されることなく安全に作業継続

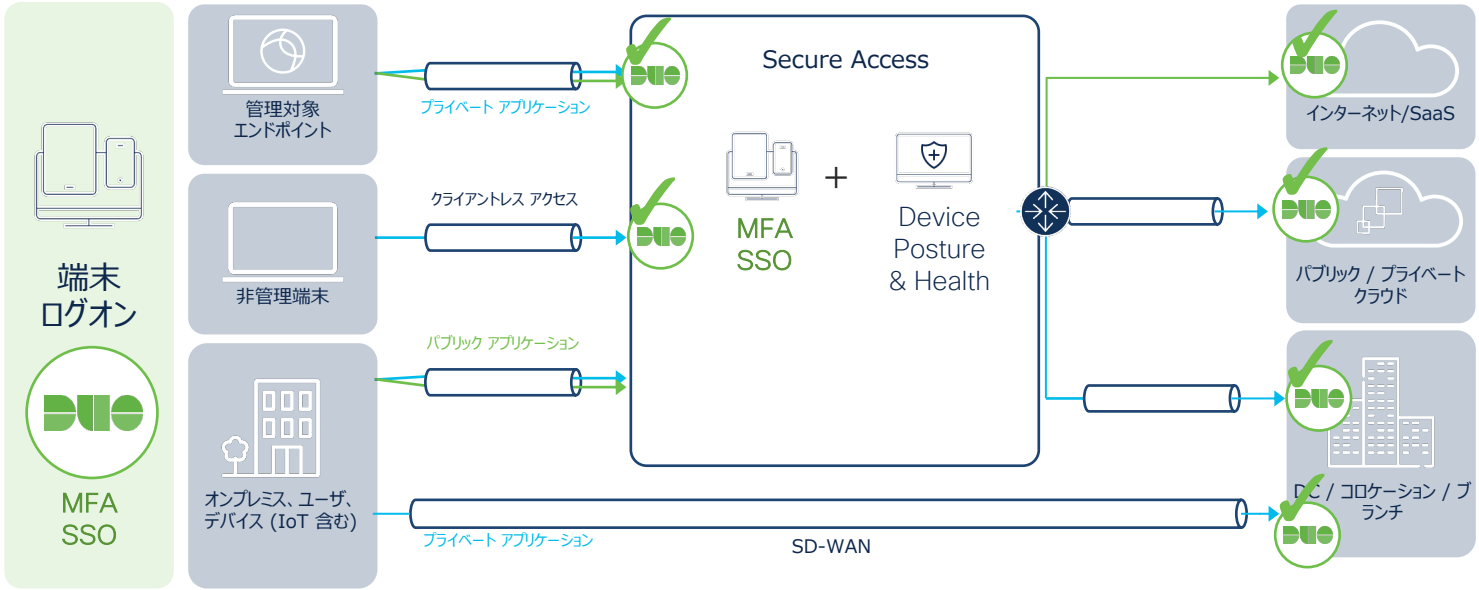
- デバイスで 1 回認証を行えば、後は認証を求められることなくアプリケーションにアクセス可能
- 強力な認証とデバイスの検証を導入することで侵害のリスクを緩和し、漏えいしたログイン情報による不正アクセスをブロック
- 認証要求の頻度を下げることで生産性を向上させ、円滑なアクセスを実現
- パスワード管理にまつわる管理面での負担を軽減し、IT コストを抑制
- MFA の対応範囲の広さ、アプリケーションごとのカスタムポリシー、IT 監査に対応した包括的なレポートにより、規制要件やガバナンスポリシーに準拠していることの証明が容易



認証強化とユーザーエクスペリエンス向上のDuo連携

Remote Access や Private Access を備えた Secure Access は、機微なトラフィックが増加するため、 SaaSや内部アプリへのアプリケーションアクセス時と合わせて、接続時の強固な認証としてMFAが必須。

Duoなら、**1日のはじめの端末ログオン時に1回認証をするだけ**で、各種ネットワーク接続時や異なるブラウザ間でWebアプリケーションにも**シームレスに認証**が可能。



【参考】 https://duo.com/blog/enhancing-user-authentication-experience

参考
Duoの利便性に関するForrester調査結果

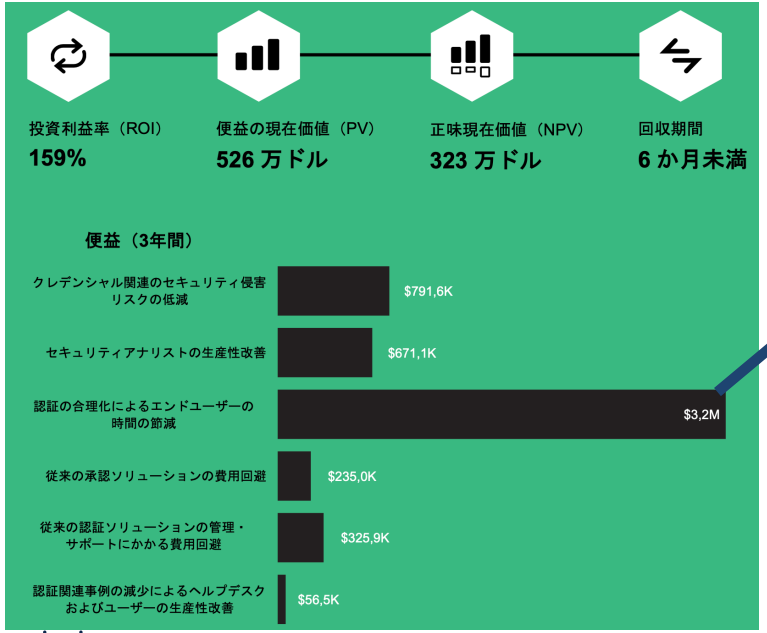
認証の合理化による費用対効果

https://www.cisco.com/c/dam/global/ja_jp/products/collateral/security/the-tei-of-cisco-duo-final-at-feb-2-2023-ja-jp.pdf

Duoの利便性に関する調査結果

DuoはMFAを提供することにより

Forrester社によるCisco Duo の Total Economic ImpactTM (TEI、総経済効果)



認証の合理化によってエンドユーザーが節減した時間

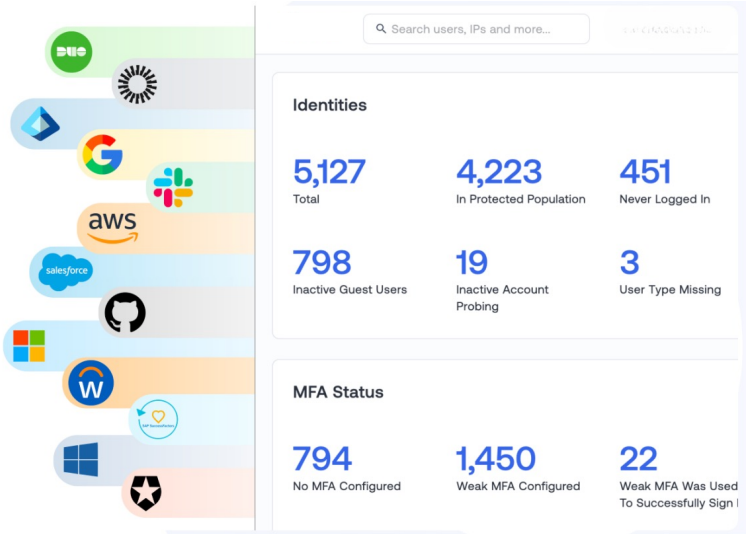
参照	指標	出典	1 年目	2 年目	3 年目
C1	エンドユーザーの人数	仮想組織	10,000	10,000	10,000
C2	エンドユーザー1 人あたりの認証の年間平均回数	インタビュー	500	500	500
C3	Duo 導入前にエンドユーザーが 1 回の認証に費やした時間（分）	インタビュー	1.5	1.5	1.5
C4	Duo 導入後にエンドユーザーが 1 回の認証に費やした時間（分）	インタビュー	0.5	0.5	0.5
C5	小計：エンドユーザーが 1 年間に節減する時間の合計（時間）	(C1*C2*(C3-C4))/60	83,333	83,333	83,333
C6	エンドユーザーの間接費込みの混合時給	TEI 標準	35.10 ドル	36.15 ドル	37.23 ドル
C7	エンドユーザーの生産性回復	TEI 標準	50%	50%	50%
Ct	認証の合理化によってエンドユーザーが節減した時間	C5*C6*C7	1,462,494 ドル	1,506,244 ドル	1,551,244 ドル
	リスク調整	↓15%			
Ctr	認証の合理化によってエンドユーザーが節減した時間（リスク調整後）		1,243,120 ドル	1,280,307 ドル	1,318,557 ドル
	3 年間の合計：3,841,985 ドル		**3 年間の現在価値：3,178,866 ドル**		

認証環境の可視化
Demo

全てのアイデンティティの可視化するITDR

すべてのアイデンティティに対する
比類のない可視性を提供

コアとなるID管理システムから遠隔にて
情報を取得して分析する。
-従業員のアイデンティティを発見
-ベストプラクティスで保護
-アイデンティティの脅威を継続的に監視



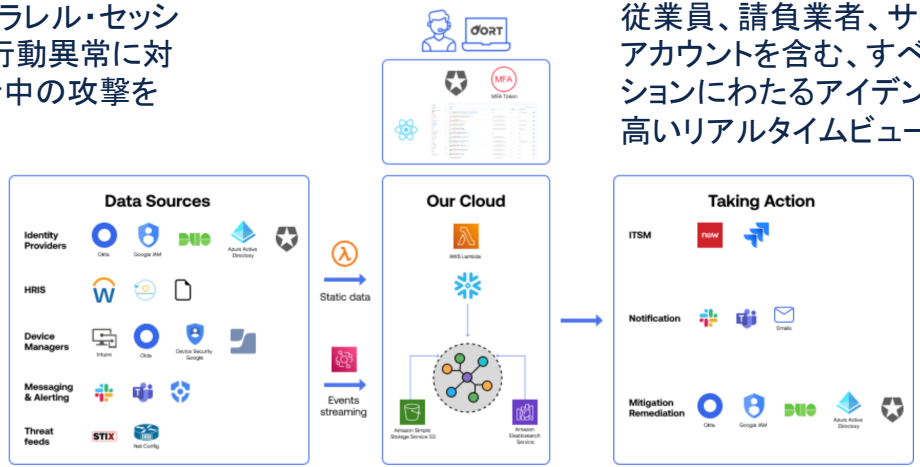
ITDRの特徴

アイデンティティの脅威を検出する

セッション・ハイジャック、危険なパラレル・セッション、不審なユーザー行動を示す行動異常に対する低ノイズ・アラートにより、進行中の攻撃を特定し、阻止します。

IAMの瞬時の保護

ITDRのソリューションはエージェントレスで、数分ですべてのアイデンティティ・ツールに接続し、継続的なリアルタイム監視を提供します。



ユーザー集団をマッピング

従業員、請負業者、サードパーティ、サービスのアカウントを含む、すべてのクラウドアプリケーションにわたるアイデンティティ集団の信頼性の高いリアルタイムビューを取得します。

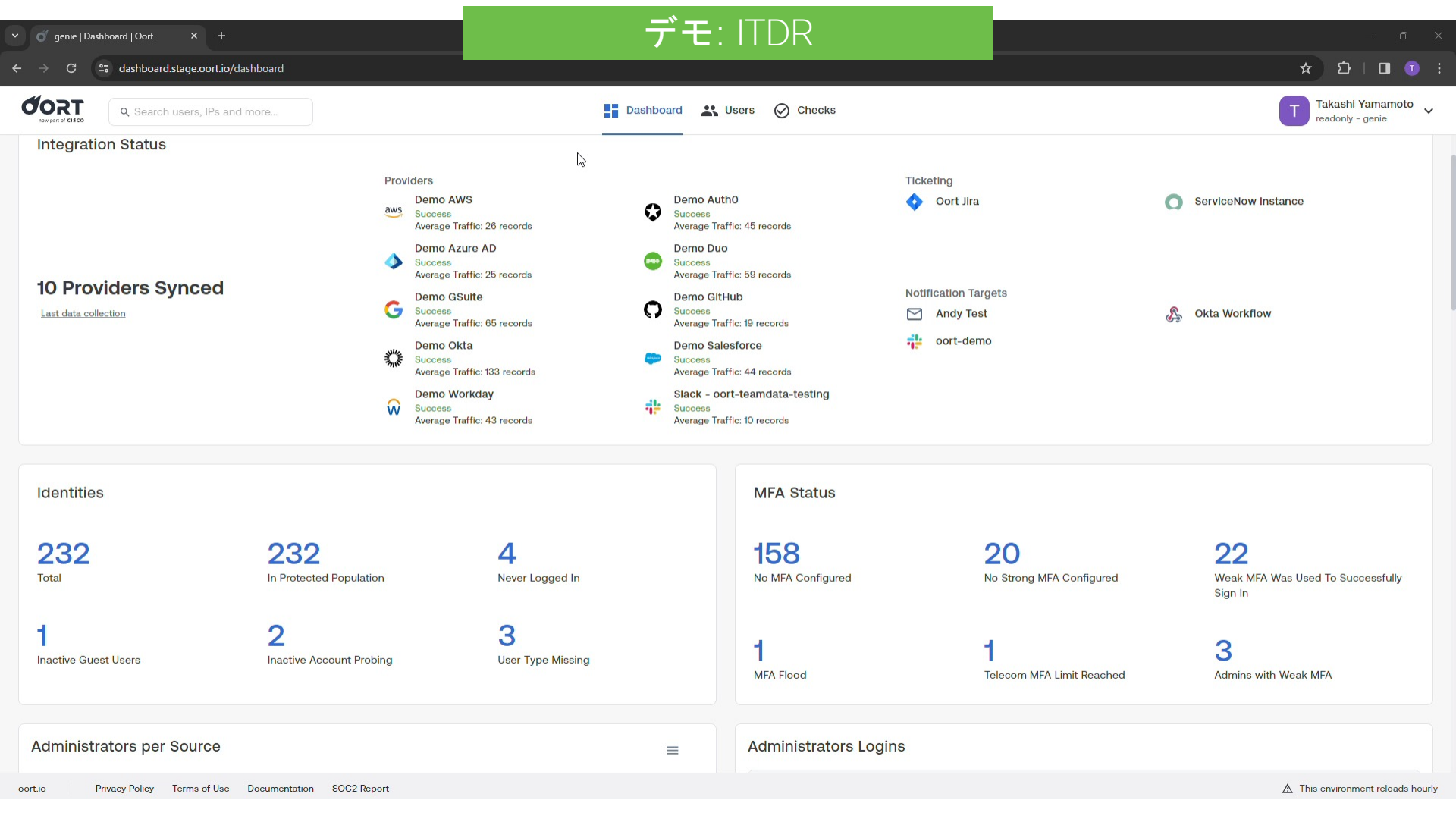
攻撃対象領域を防御する

基本的な衛生管理やプロセスの失敗を発見することで、攻撃対象が攻撃されやすい状態になります。MFAの不十分な使用、休眠アカウント、過剰な特権アカウントなどを特定し、修正します。

迅速かつ容易な対処

ユーザー調査を数時間から数分に短縮し、ボタンをクリックするだけで、アクセス削除、セッションの強制終了、隔離、チケットの発行などのアクションを実行できます。

デモ: ITDR


genie | Dashboard | Oort
dashboard.stage.oort.io/dashboard
Search users, IPs and more...
Dashboard
Users
Checks
Takashi Yamamoto
readonly - genie
Integration Status
10 Providers Synced
Last data collection
Providers
Demo AWS
Success
Average Traffic: 26 records
Demo Auth0
Success
Average Traffic: 45 records
Demo Azure AD
Success
Average Traffic: 25 records
Demo Duo
Success
Average Traffic: 59 records
Demo GSuite
Success
Average Traffic: 65 records
Demo GitHub
Success
Average Traffic: 19 records
Demo Okta
Success
Average Traffic: 133 records
Demo Salesforce
Success
Average Traffic: 44 records
Demo Workday
Success
Average Traffic: 43 records
Slack - oort-teamdata-testing
Success
Average Traffic: 10 records
Ticketing
Oort Jira
ServiceNow Instance
Notification Targets
Andy Test
Okta Workflow
oort-demo
Identities
232
Total
232
In Protected Population
4
Never Logged In
1
Inactive Guest Users
2
Inactive Account Probing
3
User Type Missing
MFA Status
158
No MFA Configured
20
No Strong MFA Configured
22
Weak MFA Was Used To Successfully Sign In
1
MFA Flood
1
Telecom MFA Limit Reached
3
Admins with Weak MFA
Administrators per Source
Administrators Logins
oort.io
Privacy Policy
Terms of Use
Documentation
SOC2 Report
This environment reloads hourly

まとめ

ID境界時代の
認証環境における３課題へのご提案

	セキュリティと生産性向上の両立を実現
Identity（ID）のセキュリティ	**パスワードレス認証とリスクベース認証** MFAの中でもより強固な生体認証を利用するFIDO2の認証とリスクに応じてより強固な認証を要求するリスクベース認証でIDのセキュリティを確保
業務生産性の維持	**シームレスログオンによる認証回数削減** PCデバイスへのログイン情報を保持し、SAMLのSSOへも認証することなくログオンできるようにするソリューションにて業務生産性の向上を実現
認証環境全体の可視化	**ITDR機能により認証環境全体を可視化** IDに関わる全ての情報を収集し、IDの可視化を実現。問題がある場合には即時対応が可能

The bridge to possible

お時間を頂き、ありがとうございました