Ciscoセキュリティウェビナー
パスワードだけの防御は限界！今すぐ始められる、IDなりすまし対策とは？

2025年12月18日(木) 14:00 – 15:00

シスコシステムズ合同会社　セキュリティ事業部
有光　祥太郎(sarimits@cisco.com)

自己紹介

有光　祥太郎(ありみつ　しょうたろう)

シスコシステムズ合同会社　セキュリティ事業部

SaaS Security Sales Specialist

出身：高知県高知市・愛媛県松山市

趣味：海外旅行・ボクシング・ポーカー

略歴：

- 2020年4月シスコシステムズ新卒入社
  SEとして、DC Network製品やAI Infra, Firewall, SSEなどを担当
- 2025年4月~
  Salesとして、SASE/SSE, ID Security, EDR/XDR等の製品を担当

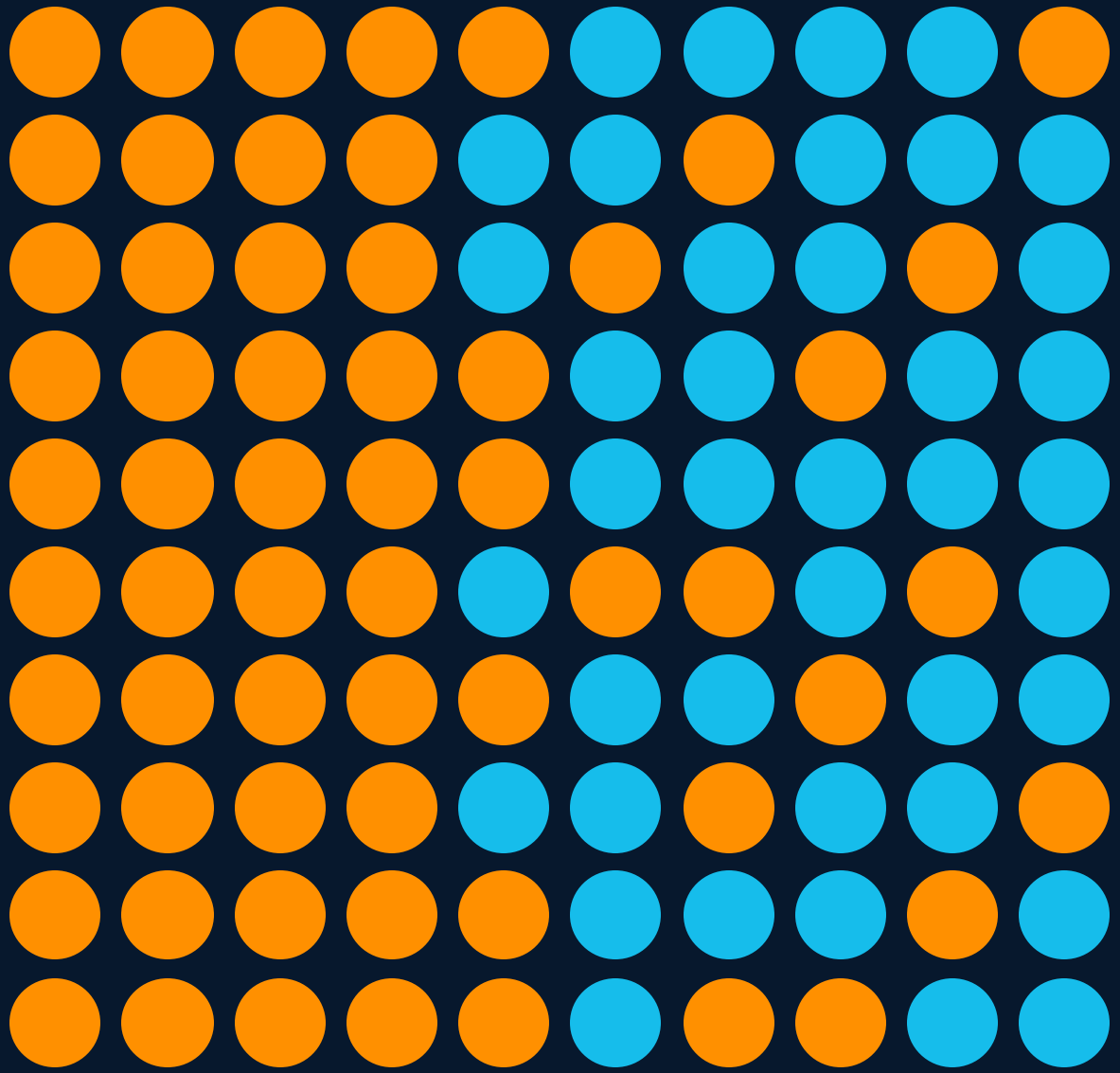
アジェンダ

①最近のランサムウェア被害とIdentityを狙った攻撃について

②Cisco Duo のご紹介

③ここがすごいぞCisco Duo

最近のランサムウェア被害とIdentityを狙った攻撃について



数年前から年々悪化している

→Identityの危機

60%

の情報漏洩はIdentityの漏洩が重要な要素になっている

（Identityがなければ起こらない）

Cisco Talos Incident Response | Year in Review 2024

日本でのランサムウェア被害の状況（2025年上半期）

- 2025年上半期の日本でのランサムウェア被害は、前年同期比の**約1.4倍**に増加。
  被害件数として、2025/01/01～6/30に日本国内の組織で**68件**のランサムウェア被害が確認された。
- ランサムウェア攻撃者は依然として主に日本の**中小企業（資本金1億円未満）を標的**とし、被害組織全体の**38%**を占める。
  最も影響を受けている業種は**製造業**、この傾向は昨年から変化していない
- **日本に最も被害を出しているのは「Qilin」ランサムウェアグループ**
- 6月下旬に新しいランサムウェアグループ**「Kawa4096」**が現れ、日本の2 社が攻撃された可能性がある

日本におけるランサムウェア被害の状況 -2025年上半期-

cisco Talos

No	日付	業種	資本金	ランサムウェアの種類	海外拠点
1	2025年1月	製造	10億円 - 100億円未満	Akira	America
2	2025年1月	放送	1億円 - 10億円未満	Unknown	
3	2025年1月	小売業	1億円未満	Lynx	
4	2025年1月	娯楽	1億円 - 10億円未満	Unknown	
5	2025年1月	商社	1億円未満	Unknown	
6	2025年1月	保険	1億円未満	Unknown	
7	2025年1月	製造	1億円 - 10億円未満	Unknown	
8	2025年1月	建設	1億円未満	Unknown	
9	2025年1月	製造	1億円未満	Qilin	
10	2025年2月	海運	1億円未満	Unknown	
11	2025年2月	製造	10億円 - 100億円未満	Qilin	
12	2025年2月	病院	1億円未満	Qilin	
13	2025年2月	園芸	1億円 - 10億円未満	Hunters International	
14	2025年2月	自動車関連	1億円未満	Qilin	America
15	2025年2月	保険	1億円 - 10億円未満	Space Bears	
16	2025年2月	製造	1億円未満	Ransomhub	
17	2025年2月	通信	10億円 - 100億円未満	Lynx	
18	2025年2月	IT	1億円 - 10億円未満	Cicade3301	
19	2025年2月	IT	10億円 - 100億円未満	Fog	
20	2025年2月	運送	1億円 - 10億円未満	Sarcoma	

https://gblogs.cisco.com/jp/2025/10/uncovering-qilin-attack-methods-exposed-through-multiple-cases/

ランサムウェアグループ「Qilin」

活動開始と別名:
2022年7月頃から活動を開始し、以前は「Agenda」としても知られている。

ビジネスモデル:
Ransomware-as-a-Service (RaaS) モデルを採用しており、
アフィリエイトを通じてその活動範囲を世界的に拡大している。

攻撃手口:
ファイルの暗号化に加えて、窃取した情報を公開するという「二重脅迫」の手法

活動状況:
2025年後半には月間40件以上、6月には100件もの被害者情報をリークサイトに掲載するなど、非常に活発な活動をしている。

主な標的産業:
製造業が最も多く(約23%)、次いで専門・科学技術サービス(約18%)、
卸売業(約10%)が狙われている。

＜初期アクセス経路＞

VPN認証情報の悪用:

ダークウェブで漏洩または販売されたVPN認証情報が悪用されることが
多く、多要素認証が未設定のVPNが特に狙われている。

フィッシング/偽CAPTCHAページ:
偽のGoogle CAPTCHAページやフィッシングキャンペーンを通じて
情報窃取マルウェアを配布し、認証情報を詐取する。

RMMツールの悪用:
AnyDeskやMicrosoft Quick Assistなどの正規のリモート監視・管理
(RMM) ツールを悪用して初期アクセスを獲得する。

脆弱性の悪用:
Citrix NetScaler ADC (CVE-2025-5777) やMicrosoft SharePointなどの
既知の脆弱性も悪用される。

＜偵察活動＞

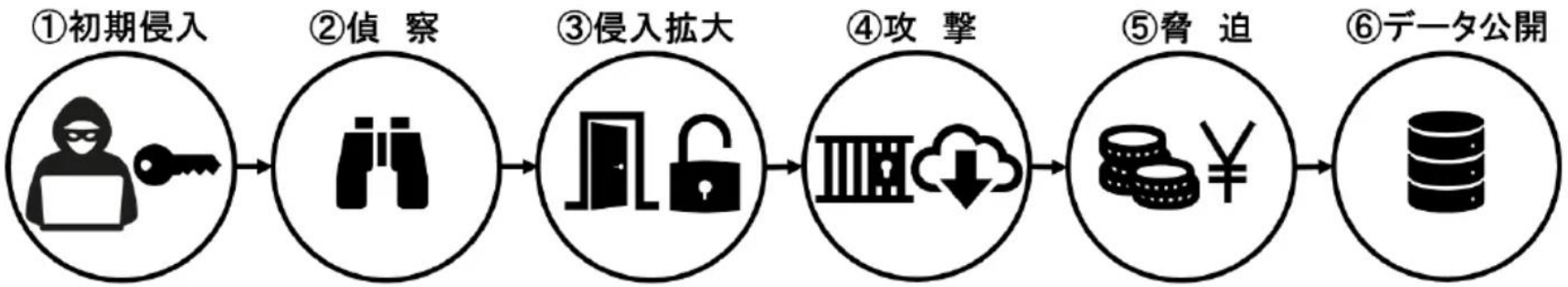
- ネットワーク侵入後、nltest.exeやnet.exe等の組み込みツールを用い、ドメインコントローラーやドメインユーザー情報を列挙します。
- whoamiでユーザー権限を評価し、tasklistでアクティブなプロセスを列挙するほか、netscanツールでネットワークマッピングを行う。

「Qilin」の侵害活動

- **認証情報窃取**:
  - Mimikatz、NirSoftユーティリティ、カスタムスクリプトなどを用いて認証情報を窃取。また、Veeamバックアップインフラストラクチャを標的とし、バックアップデータから認証情報を抽出する手法も確認。
- **防御回避**:
  - PowerShellコマンドの難読化、EDRの無効化、AMSI（Antimalware Scan Interface）の無効化、を実行。
  - BYOVD（Bring Your Own Vulnerable Driver）攻撃にてEDRツールを無効化し、検出を回避。また、DLLサイドローディングやSOCKS Proxyを展開し、C2（Command and Control）トラフィックを難読化。
- **データ窃取**:
  - 窃取したデータはWinRARで圧縮され、Cyberduck等のオープンソースツールを用いてBackblaze等のクラウドストレージにアップロードされる。
  - mspaint.exeやnotepad.exeといった正規のWindowsユーティリティを悪用し、手動で機密情報を特定・閲覧する巧妙な手法も確認。
- **ランサムウェア展開**:
  - Linuxベースのランサムウェアペイロードを Windowsシステムに展開。WinSCPでファイルを転送し、Splashtop RemoteやWindows Subsystem for Linux（WSL）を介して実行。
  - encryptor_1.exeはPsExecでホスト全体に拡散し、encryptor_2.exeは単一システムから複数のネットワーク共有を暗号化する「二重展開」
  - イベントログの消去やWindows Volume Shadow Copy Service（VSS）のシャドウコピー削除により、復旧を困難にする。

ランサムウェア攻撃の影響調査結果および安全性強化に向けた取り組みのご報告（ランサムウェア攻撃によるシステム障害関連・第 13 報）
アスクル株式会社 2025年12月12日 15時30分

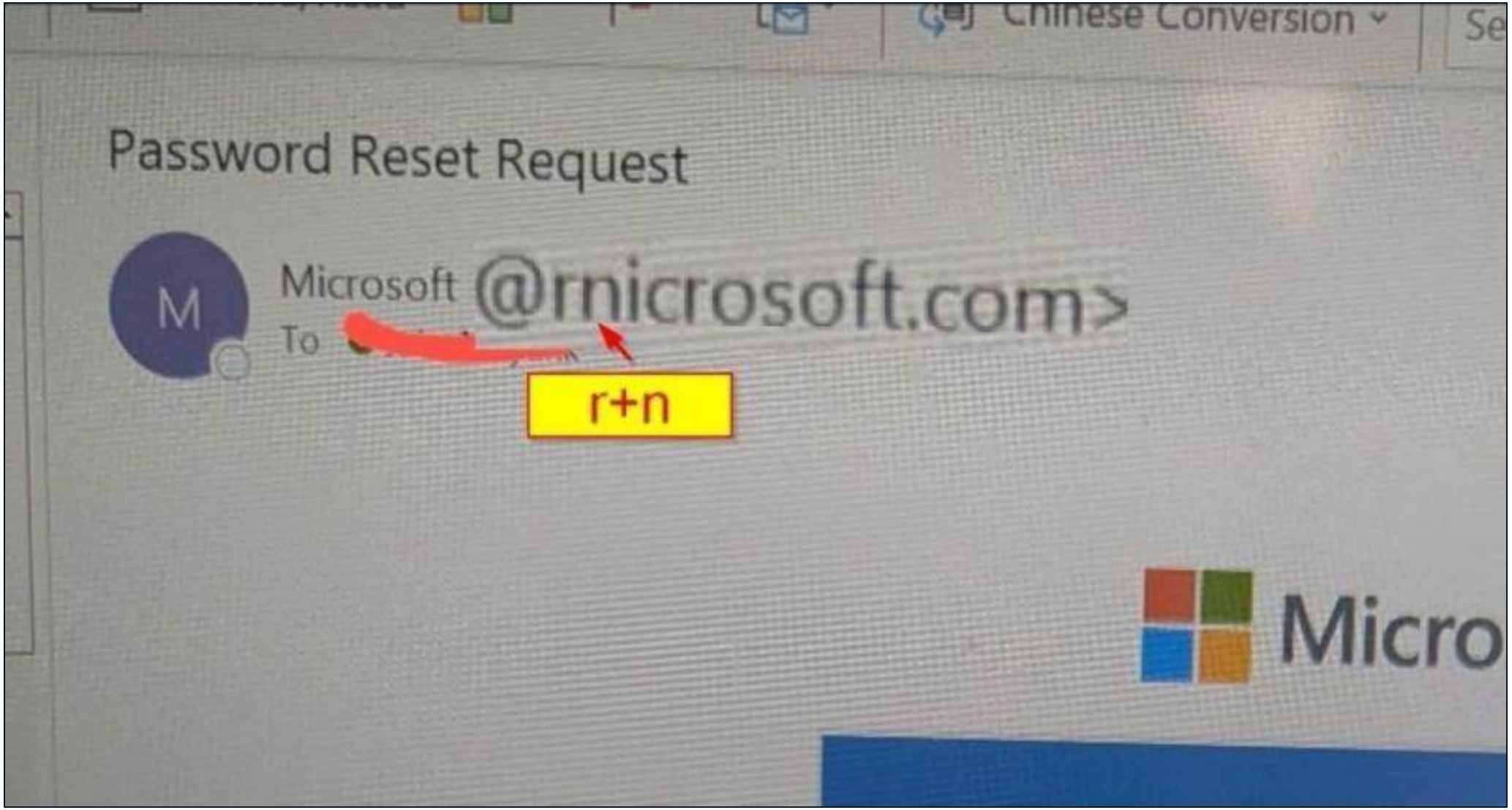
4．攻撃手法の詳細分析



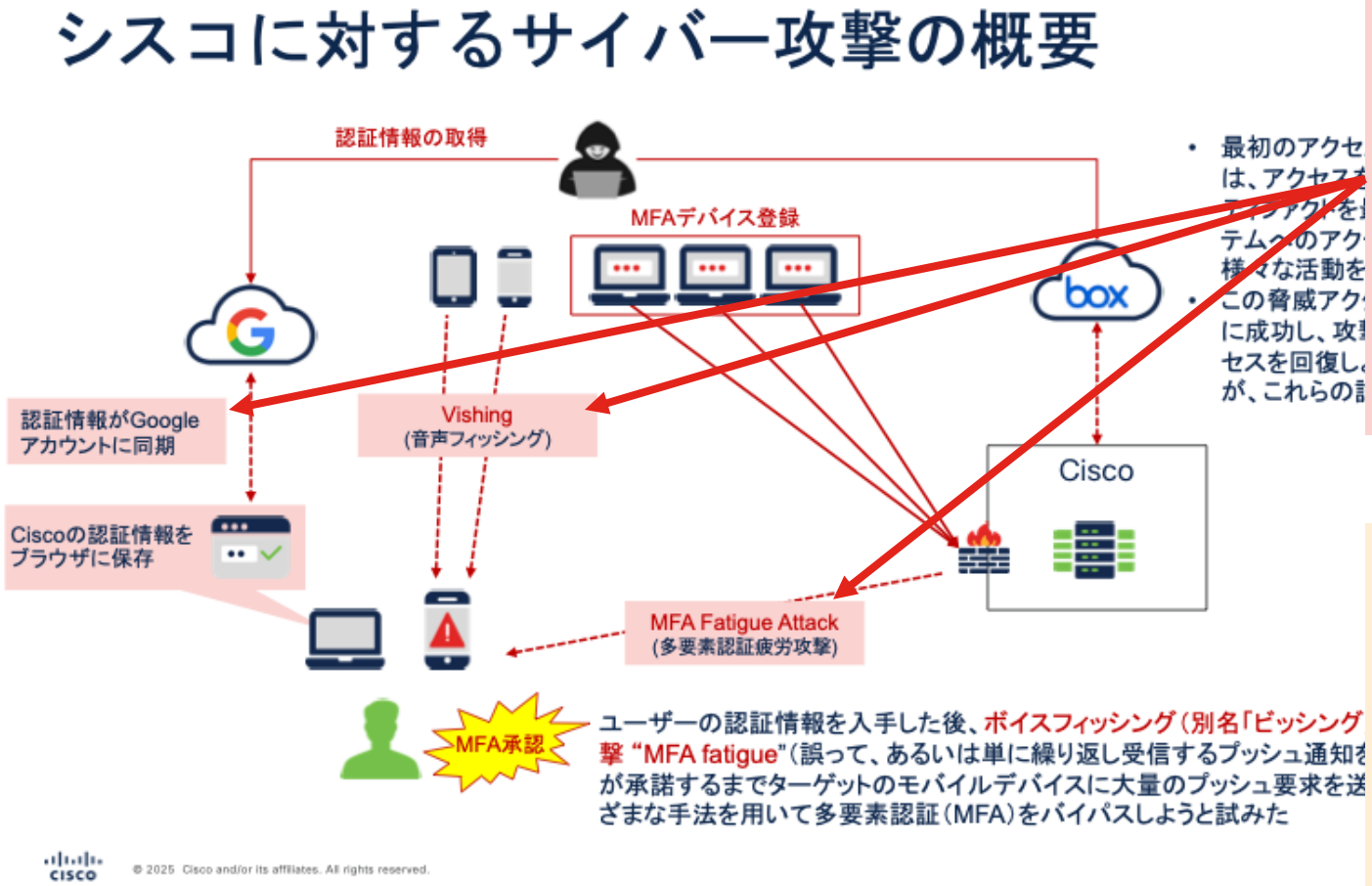
時期	2025/6/5	2025/6 ～ 2025/10/9	2025/7/9 ～ 2025/10/19	2025/10/19～	2025/10/19 2025/10/21 2025/10/27	2025/10/30 2025/11/10 2025/12/2
概要	業務委託先用のアカウントを使用して社外より初期侵入	管理者権限等の取得を目標としたログイン試行(全て失敗)	脆弱性対策ソフトを無効化したうえで物流システムおよび社内システム、端末に侵入拡大し、ランサムウェア配置	事前設定された時刻にランサムウェアが起動し、サーバ暗号化 ファイル削除 クラウド情報窃取	メールによる脅迫文送付	リークサイト上でサンプルデータ公開

出典：https://prtimes.jp/main/html/rd/p/000000500.000021550.html

なぜID・パスワードは漏洩するのか？



AIを使ったサイバー攻撃が本格化



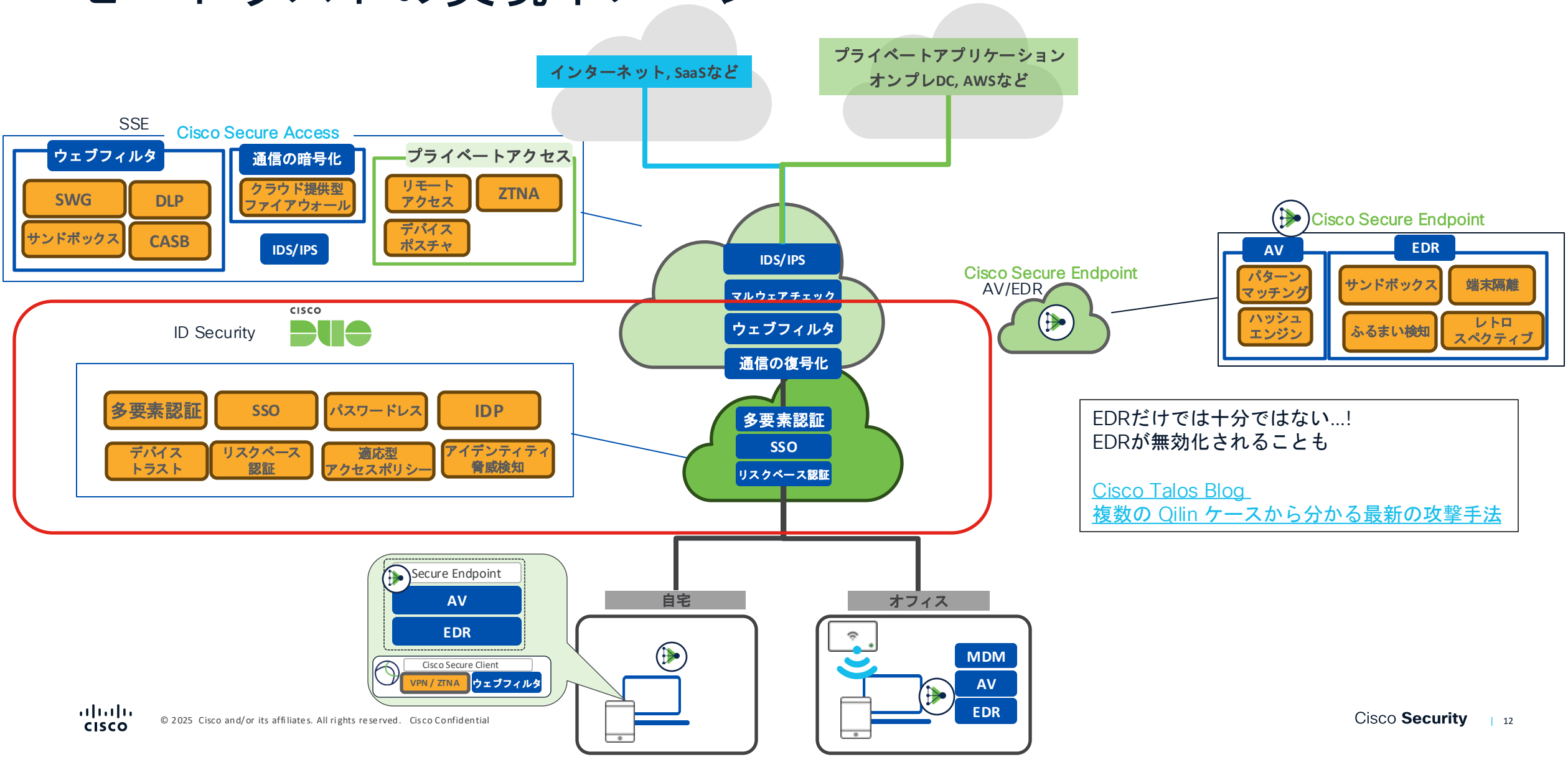
AIを使って「自動化」「高度化」

- フィッシングは単純な迷惑メールから多層攻撃へ進化
- メール／SNS／モバイルを組合せ、検知を回避する手法が主流
- 自動化により「瞬時発生」も「段階的侵入」も可能

LLM（大規模言語モデル）の悪用

- ChatGPT等で「説得力ある文面」を短時間で大量生成
- ソーシャルメディア調査＋デューデリジェンスで標的特定を自動化
- 深層合成（ディープフェイク）で信用を奪う音声・映像も併用

Cisco Security Platformによる ゼロトラストの実現イメージ



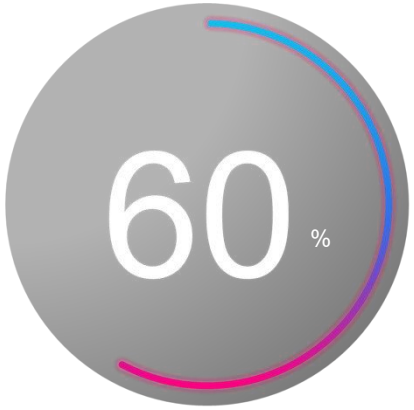
EDRだけでは十分ではない…!
EDRが無効化されることも

Cisco Talos Blog
複数の Qilin ケースから分かる最新の攻撃手法

Cisco Duoのご紹介

何故Identity Securityが重要なのか？

侵害の60% は アイデンティティに関係している



ID（認証基盤）を狙った攻撃が依然として活発であり、多くの侵害の起点となっている

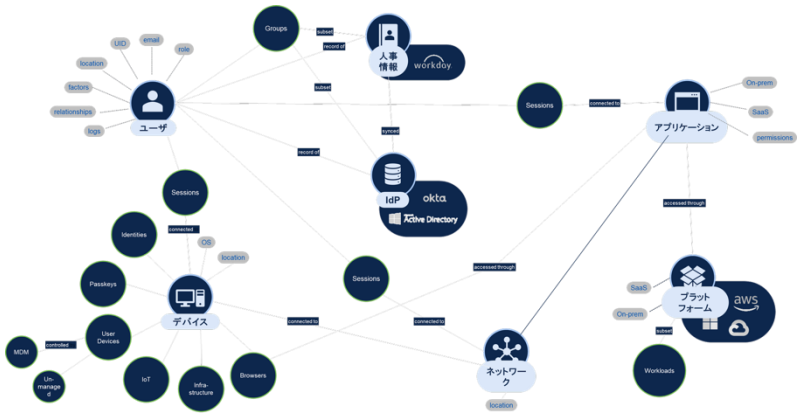
Talosの2024年調査レポートによると60%の侵害がアイデンティティに関係していると発表

今後 AI・クラウドの加速によりNHIも重要に

クラウドサービスがさらに利用拡大することで、IDの種類・権限の管理がさらに重要に

AIの台頭に伴い、人間以外のアイデンティティ（Non-Human Identity: NHI）への対応も必要となる

アイデンティティは更に複雑に拡がる



AD

MS Entra

Okta

AWS

Git Hub

…

今までのIAMはセキュリティがオプションで高コスト

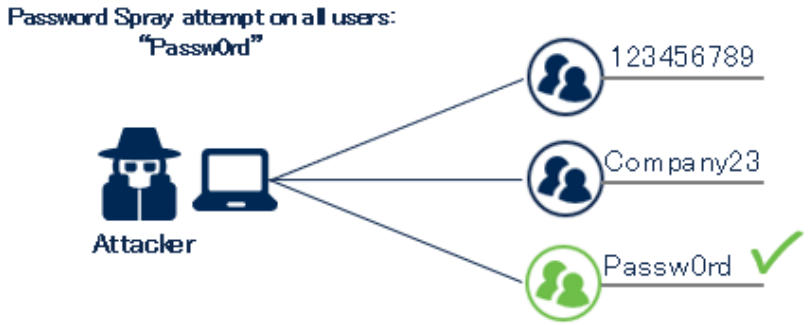
今までのアイデンティティソリューションはセキュリティ機能がオプション扱いとなっており、包括的にセキュリティ対策を実施しようとすると高コストで運用が困難

IDに対する攻撃

✓ ブルートフォース(総当たり攻撃)

Brute Force: Password Spraying [T1110.003]

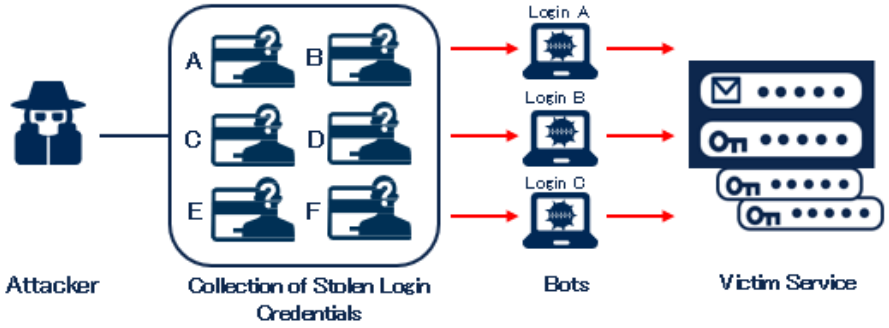
少数の一般的なパスワードを多数のアカウントに順番に試す



✓ 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

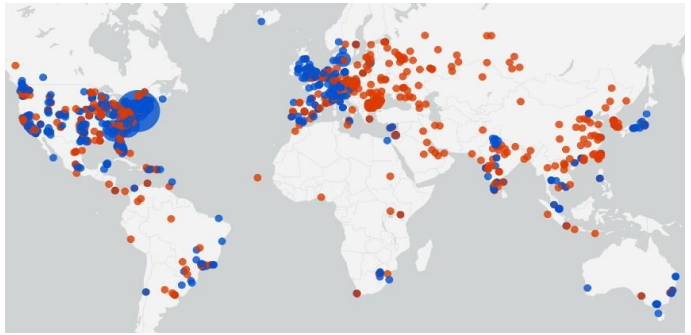
Targeting Dormant Accounts

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。



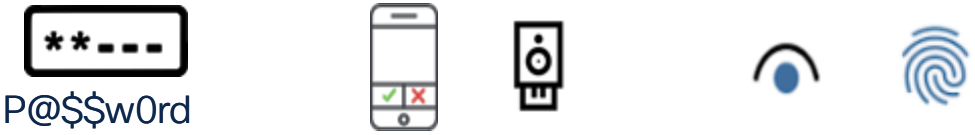
※2022 年下半期のエグゼクティブによるログインの失敗と成功

Duoの主要機能

ゼロトラスト ネットワーク アクセス (ZTNA) の最重要要素であるアイデンティティ保護を実現、最新型脅威にも対応

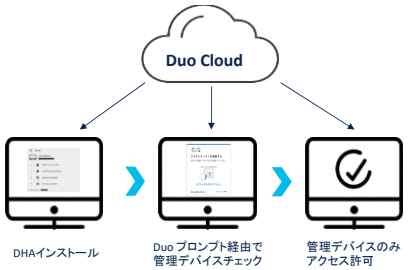
多要素認証

知識要素 ＋ 所有要素 ＋ or 生体要素



- ✓ ユーザの認証は瞬時に – ワンタップで承認
- ✓ パスワードに依存しないセキュアなアクセス
- ✓ パスワード漏洩による不正アクセスを防御

デバイスの信頼性評価

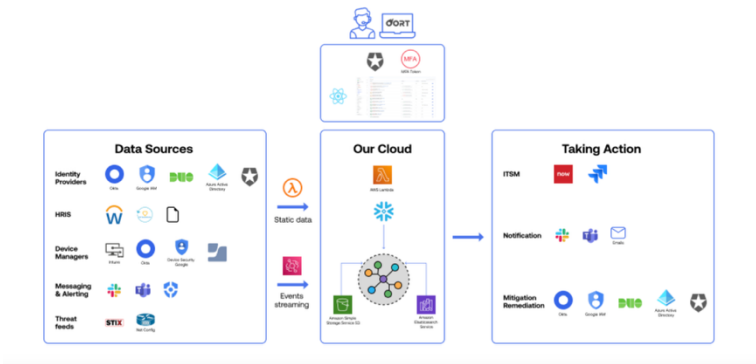


- ✓ 認証時の検疫機能と管理デバイスかどうかの検査
- ✓ 古いバージョンのOSやブラウザの通知と制御
- ✓ セキュリティソフトウェアの検査
- ✓ 振る舞いベースのリスク分析

シングルサインオン

- ✓ シングルサインオンによるユーザエクスペリエンス向上

Cisco Identity Intelligence



- ✓ マルチプラットフォームのID管理状況を可視化し、脅威検知からその対応までを実現可能

Cisco Duo 機能紹介

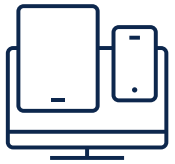
包括的でクロスプラットフォームに提供可能な Identity セキュリティ・ソリューション

継続的な認証と信頼の検証

ユーザの認証

- MFA
- フィッシングに強い要素
- 従業員、請負業者、ベンダー外部の第三者など

デバイスの検証

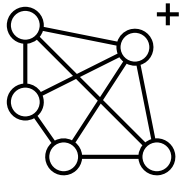


- デバイスの信頼性
- デバイスの健全性とコンプライアンス
- Mac、Windows、iOS、Android、BYOD

アクセス有効化

- シングルサインオン（SSO）
- きめ細かなポリシー構築
- すべてのアプリケーション - クラウド、オンプレ、プライベート

IDリスクを最小限に



- アイデンティティ・セキュリティポスチャ管理
- リスクベースのアクセス制御
- すべてのIDソース - HRIS、ディレクトリ、SaaSソース

ITDR
Identity Threat Detection & Response

Directory

- IdPを持たない環境に対する新規Directory
- SAML IdPのプライマリと連携し ブローカーとして動作
- 既存のIdPとは別の用途に対する代替のユースケースのためのディレクトリとして利用

あらゆる用途に対応するMFAオプション

共有端末で利用可能なMFA
Bluetoothを活用したより強度の高いMFA
（セキュリティ強化）

認証(MFA)設定

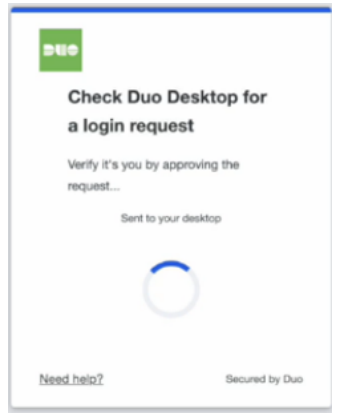
- ユーザグループやアプリケーションごとに多様なMFAオプションを設定できる
- 容易にユーザ自身でMFAデバイスの追加や削除が可能、複数MFAデバイス登録可能（認証時に選択可能）

Duo Mobile + Wearables

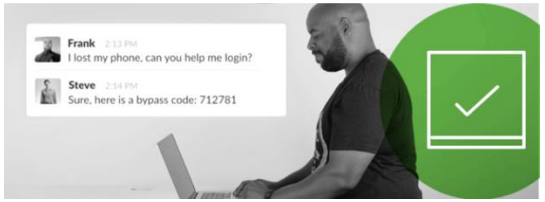
Hardware Token

Phone Callback

WebAuthn and Biometrics

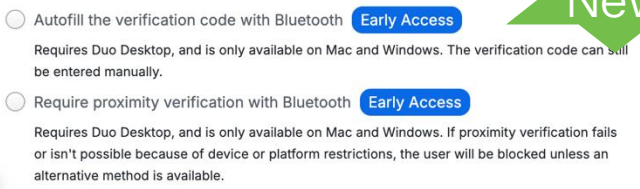


Duo Desktop authentication

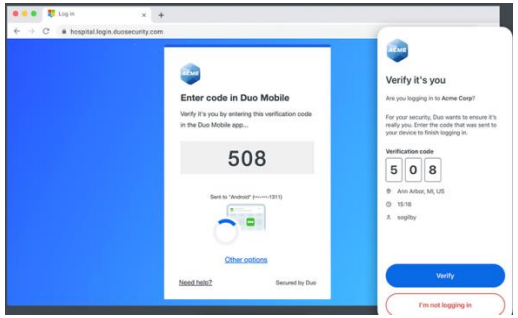


bypass code

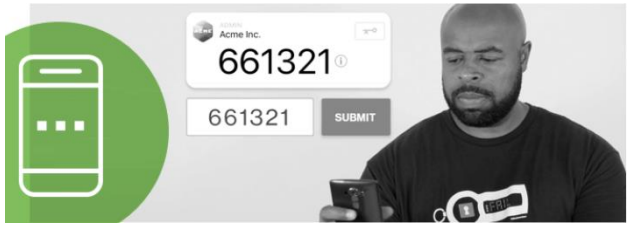
New



Duo Mobile + Bluetooth verification



Verify Push



Passcode：SMS & Soft Token

U2F Token

正当なユーザーアクセスと認証デバイスが近くにあることを確認
追加のハードウェアは不要（セキュリティキーなど）

Cisco Duo 機能紹介

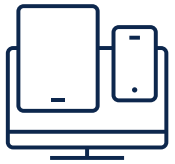
包括的でクロスプラットフォームに提供可能な Identity セキュリティ・ソリューション

継続的な認証と信頼の検証

ユーザの認証

- MFA
- フィッシングに強い要素
- 従業員、請負業者、ベンダー外部の第三者など

デバイスの検証

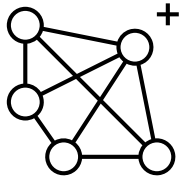


- デバイスの信頼性
- デバイスの健全性とコンプライアンス
- Mac、Windows、iOS、Android、BYOD

アクセス有効化

- シングルサインオン（SSO）
- きめ細かなポリシー構築
- すべてのアプリケーション - クラウド、オンプレ、プライベート

IDリスクを最小限に



- アイデンティティ・セキュリティポスチャ管理
- リスクベースのアクセス制御
- すべてのIDソース - HRIS、ディレクトリ、SaaSソース

ITDR
Identity Threat Detection & Response

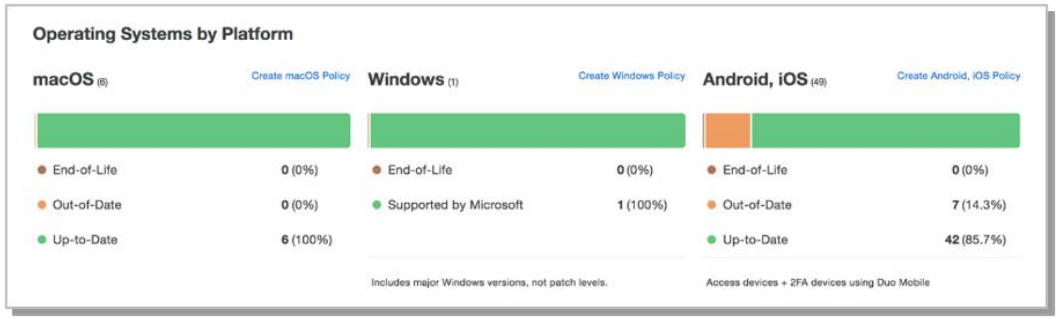
Directory

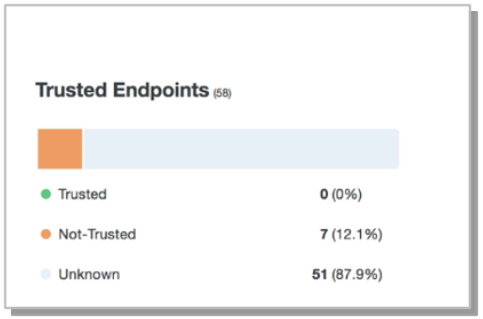
- IdPを持たない環境に対する新規Directory
- SAML IdPのプライマリと連携し ブローカーとして動作
- 既存のIdPとは別の用途に対する代替のユースケースのためのディレクトリとして利用

全てのデバイスの健全性チェック

認証時、リアルタイムにチェック
＊MDM製品ではリアルタイムにチェック出来ない

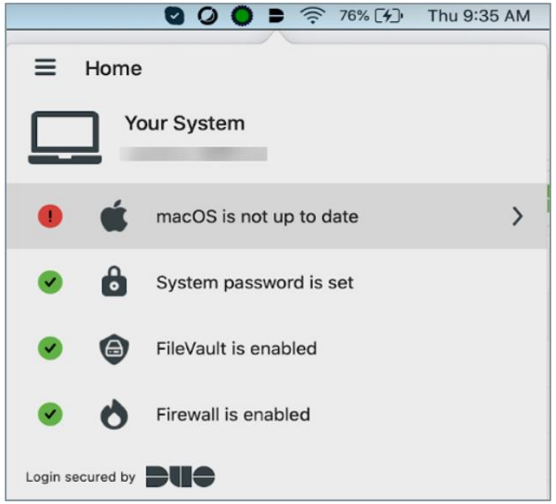
- 管理デバイスに限らず全てのデバイスを包括的に、アクセス時にリアルタイムで、デバイスの情報を取得し健全性チェックを実施 →管理することなくデバイスの健全性を維持できる





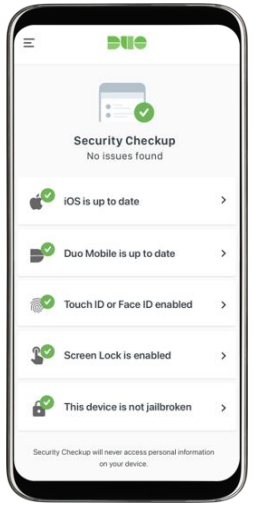
PCの収集情報（ Duo Desktop ）

- ✓ ディスク暗号化ステータス
- ✓ ホストのファイアウォールの稼働有無
- ✓ デバイスのパスワードの設定有無
- ✓ OS のタイプとバージョン
- ✓ OS のパッチレベル
- ✓ サードパーティのセキュリティエージェントの稼働有無
- ✓ 企業による管理デバイスか
- ✓ ブラウザのタイプとバージョン
- ✓ Flash および Java プラグインのバージョン



モバイルの収集情報（ Duo Mobile ）

- ✓ 会社が管理するアセットのステータス
- ✓ 生体認証（Touch ID/Face ID）のステータス
- ✓ 画面ロックのステータス
- ✓ OS（改ざん）のステータス
- ✓ 暗号化のステータス
- ✓ プラットフォームタイプ
- ✓ デバイスの OS の種類
- ✓ デバイスの OS バージョン
- ✓ デバイスの所有者
- ✓ Duo Mobile のバージョン



Cisco Duo 機能紹介

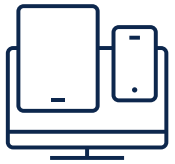
包括的でクロスプラットフォームに提供可能な Identity セキュリティ・ソリューション

継続的な認証と信頼の検証

ユーザの認証

- MFA
- フィッシングに強い要素
- 従業員、請負業者、ベンダー外部の第三者など

デバイスの検証

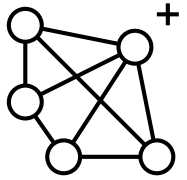


- デバイスの信頼性
- デバイスの健全性とコンプライアンス
- Mac、Windows、iOS、Android、BYOD

アクセス有効化

- シングルサインオン（SSO）
- きめ細かなポリシー構築
- すべてのアプリケーション - クラウド、オンプレ、プライベート

IDリスクを最小限に



- アイデンティティ・セキュリティポスチャ管理
- リスクベースのアクセス制御
- すべてのIDソース - HRIS、ディレクトリ、SaaSソース

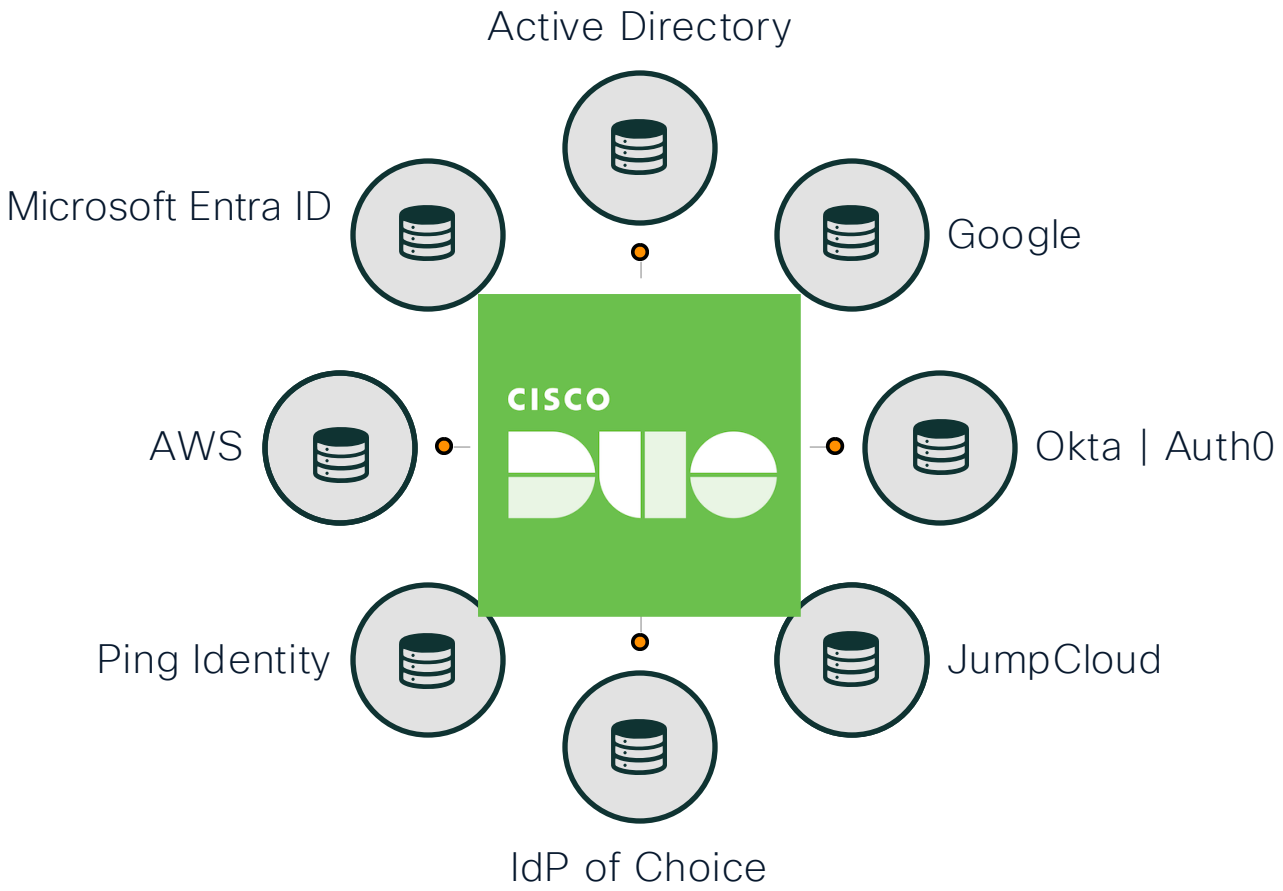
ITDR
Identity Threat Detection & Response

Directory

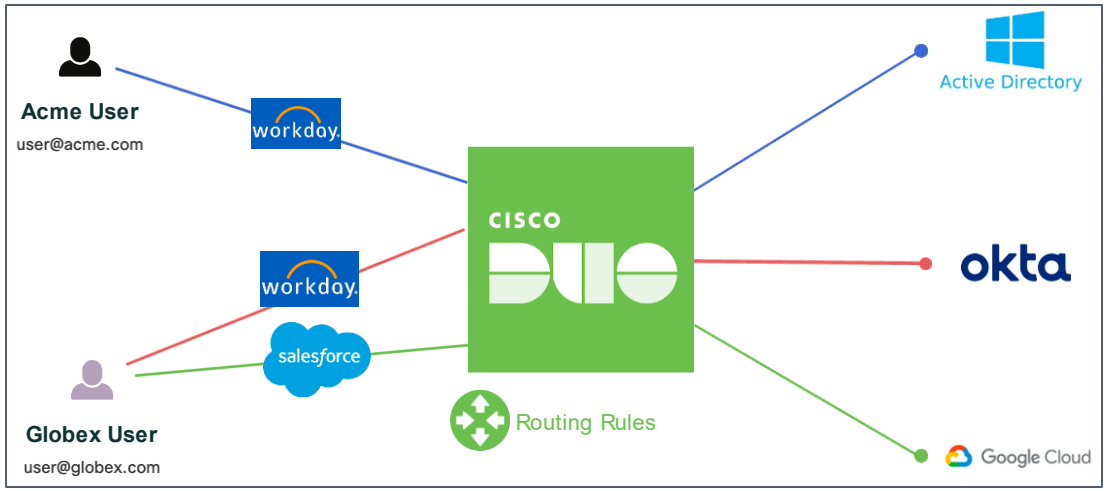
- IdPを持たない環境に対する新規Directory
- SAML IdPのプライマリと連携し ブローカーとして動作
- 既存のIdPとは別の用途に対する代替のユースケースのためのディレクトリとして利用

Duo SSO Routing Rules

- アクセス制御の統合、組織への共通ポリシーの適用を可能に。エンドユーザのU/Iもシンプルに。



SSO Routing Rules 動作概要



Solution

Duo SSOにて、複数のActive Directoryと複数のIDPソースを同時利用可能に
ドメイン、IP、アプリケーションへのアクセスなど、お客様が定義した一連のポリシーに基づいて、ユーザーを適切なダウンストリームソースに自動的にルーティング

Cisco Duo 機能紹介

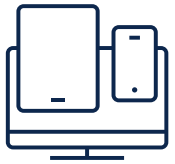
包括的でクロスプラットフォームに提供可能な Identity セキュリティ・ソリューション

継続的な認証と信頼の検証

ユーザの認証

- MFA
- フィッシングに強い要素
- 従業員、請負業者、ベンダー外部の第三者など

デバイスの検証

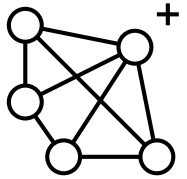


- デバイスの信頼性
- デバイスの健全性とコンプライアンス
- Mac、Windows、iOS、Android、BYOD

アクセス有効化

- シングルサインオン（SSO）
- きめ細かなポリシー構築
- すべてのアプリケーション - クラウド、オンプレ、プライベート

IDリスクを最小限に



- アイデンティティ・セキュリティポスチャ管理
- リスクベースのアクセス制御
- すべてのIDソース - HRIS、ディレクトリ、SaaSソース

ITDR
Identity Threat Detection & Response

Directory

- IdPを持たない環境に対する新規Directory
- SAML IdPのプライマリと連携し ブローカーとして動作
- 既存のIdPとは別の用途に対する代替のユースケースのためのディレクトリとして利用

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）

侵入

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

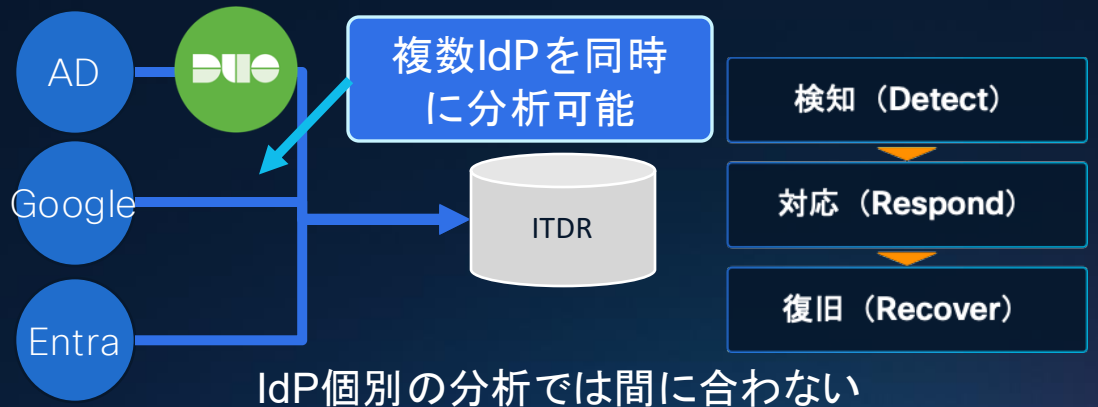
対応(Response)
・脅威の隔離
・IDの削除・無効化
・MFAのリセット
・ログアウトの強制
・脅威に応じた自動メッセージの送信
・レポート、報告
・XDRとの連携
等

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

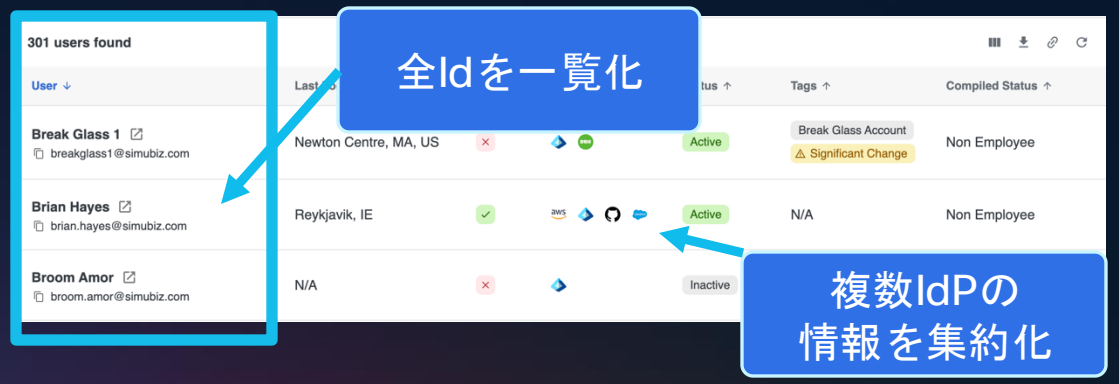
多層ログと相関分析の導入
脅威を迅速に検知可能なITDRの重要性

複数のIdソースを同時に分析・検知可能

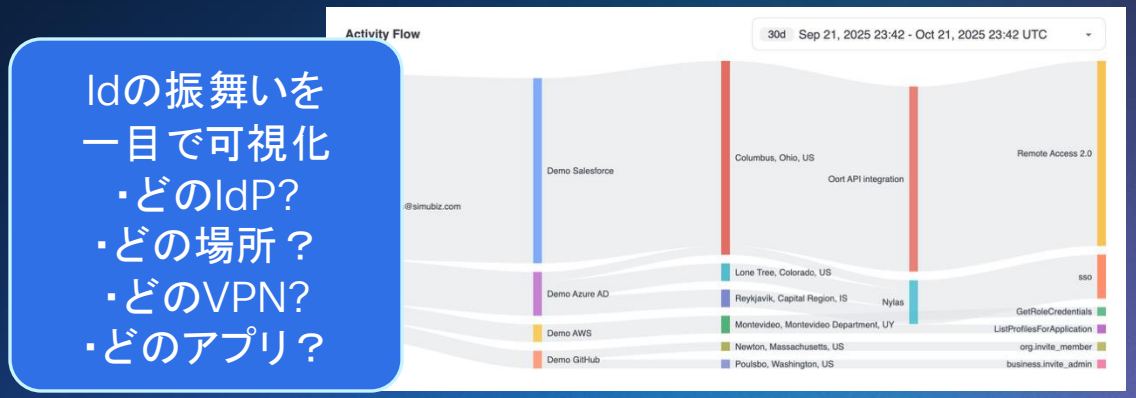


IdP個別の分析では間に合わない

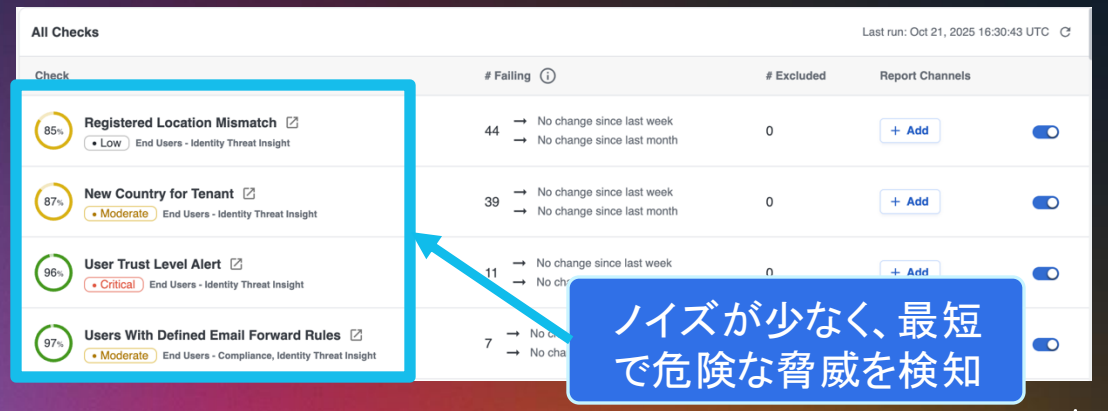
組織に存在するIdを集約化し、可視化



ユーザ毎のIdに関する振舞いを可視化



危険な脅威を最短で検知可能



ITDRをテスト導入されたお客様の検知例と活用ユースケース

35

非アクティブアカウント数

Threat: Critical

90

７日以上ログインがなく、
その後１回以上の
ログイン失敗を検知

- 非アクティブなアカウントは盗まれてもバレにくいため攻撃者から狙われやすい
- 退職、休職、出向中などのアカウント管理の見直しに
- 必要のないアカウントの削除によるコスト削減

Threat: Critical

3

1日あたりのログインが
非常に多い(1000回以上)
アカウントを検出

Threat: Critical

5

MFA疲労攻撃を受けている
可能性のあるアカウント

- 異常なログインを検知
- 攻撃者にアカウント情報を盗まれており侵入を試みられている可能性大
- アカウントの無効化、アクセスブロックなどの対応に

Threat: Moderate

5

信頼性が低いISPあるいは
一般的ではないISPからの
ログインを検出

Posture: Low

60

アクセス時に個人向けVPN
サービスを５回以上
利用したユーザ

- ログイン環境にリスクがある
- 会社のポリシーに準拠した運用が行われているか可視化
- 社員教育、セキュリティ意識向上に

Cisco Duo 機能紹介

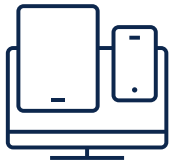
包括的でクロスプラットフォームに提供可能な Identity セキュリティ・ソリューション

継続的な認証と信頼の検証

ユーザの認証

- MFA
- フィッシングに強い要素
- 従業員、請負業者、ベンダー外部の第三者など

デバイスの検証

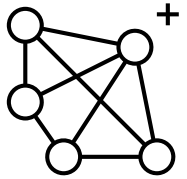


- デバイスの信頼性
- デバイスの健全性とコンプライアンス
- Mac、Windows、iOS、Android、BYOD

アクセス有効化

- シングルサインオン（SSO）
- きめ細かなポリシー構築
- すべてのアプリケーション - クラウド、オンプレ、プライベート

IDリスクを最小限に



- アイデンティティ・セキュリティポスチャ管理
- リスクベースのアクセス制御
- すべてのIDソース - HRIS、ディレクトリ、SaaSソース

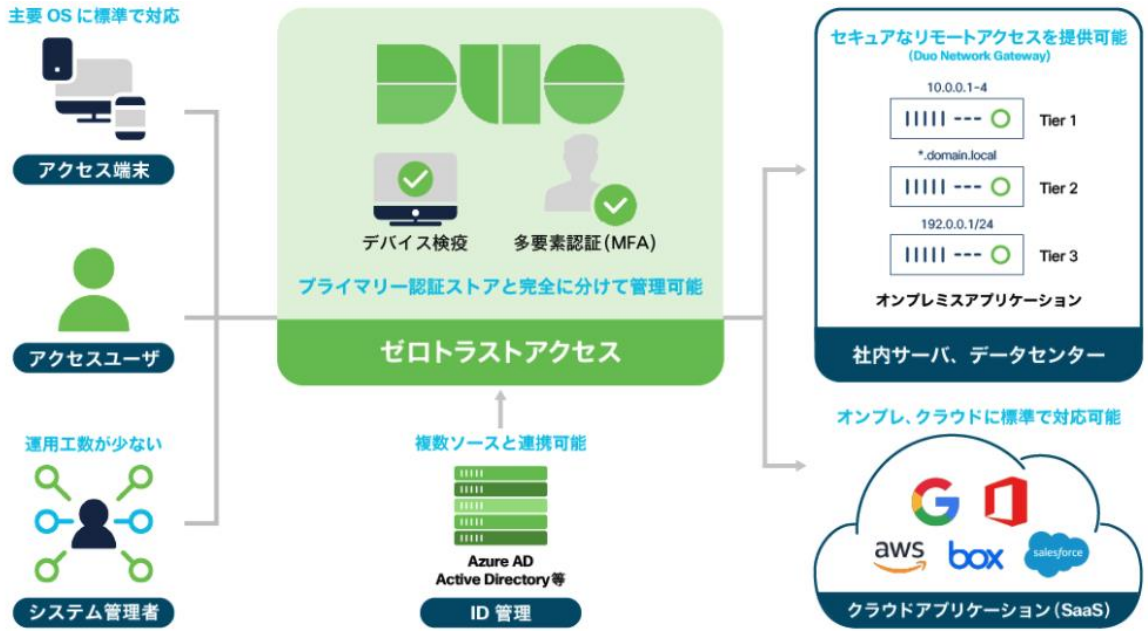
ITDR
Identity Threat Detection & Response

Directory

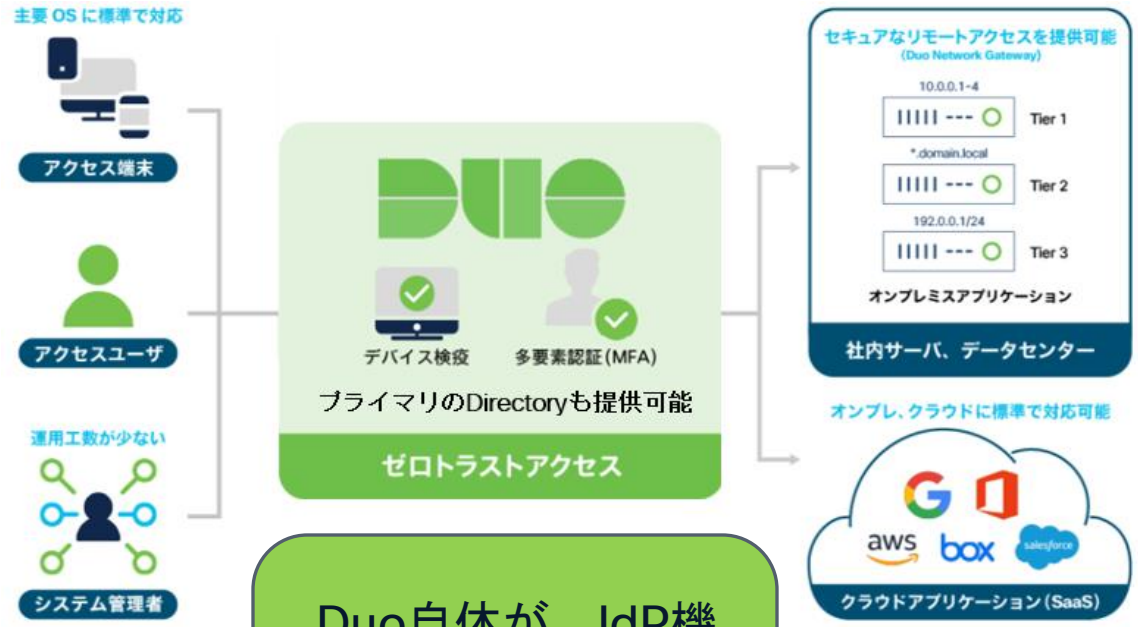
- IdPを持たない環境に対する新規Directory
- SAML IdPのプライマリと連携し ブローカーとして動作
- 既存のIdPとは別の用途に対する代替のユースケースのためのディレクトリとして利用

Duo Identity and Access Management (Duo IAM)への進化

多要素認証中心のクラウドサービスからITDRやDirectory機能も備えたIdentity and Access Managementへ進化



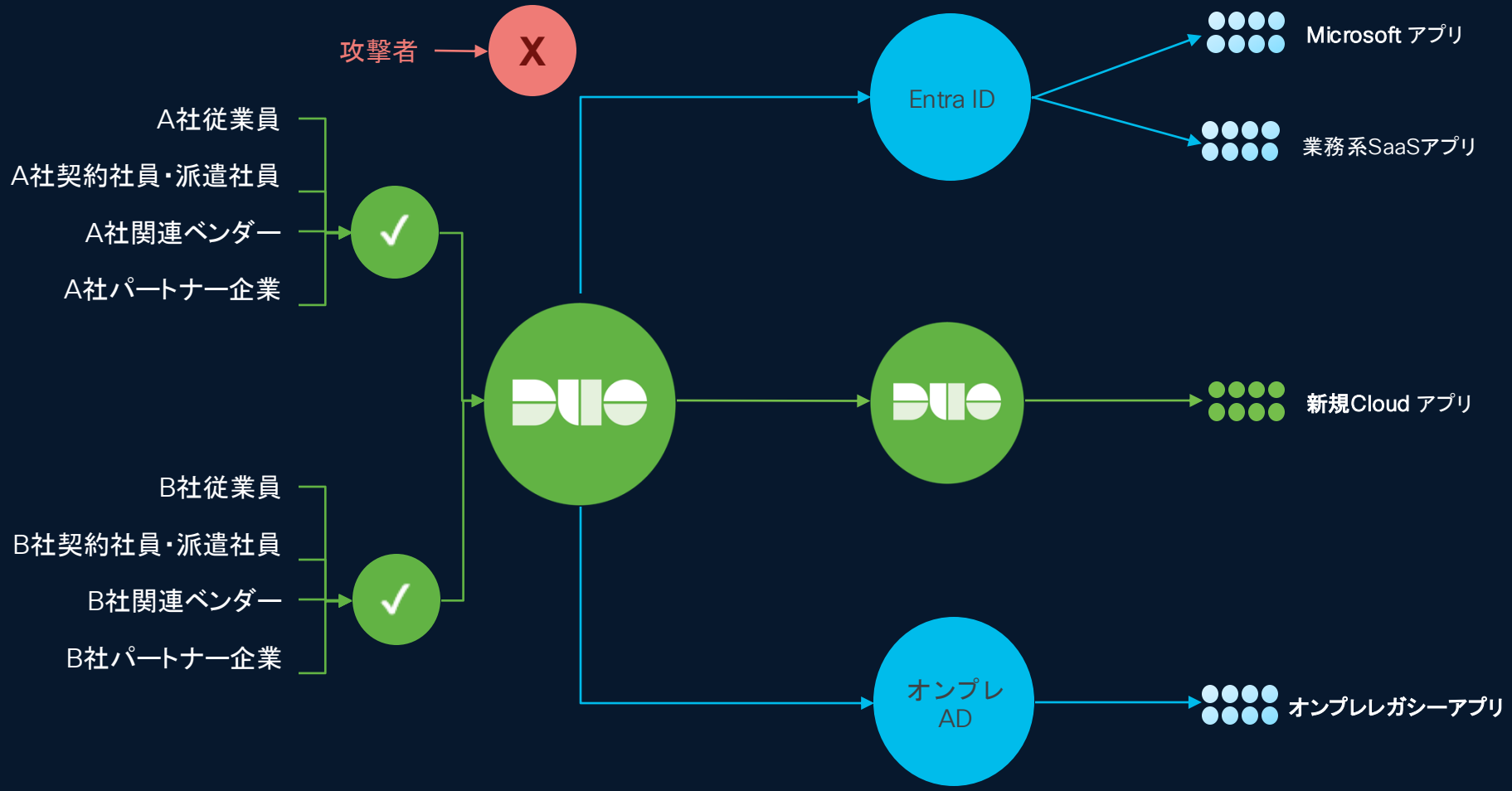
オンプレAD→DuoでのID管理へ移行



Duo自体が、IdP機能を持てるようになった
(ID/Passを保持)

ユースケース① IdPの仲介(ブローカー)

分散IdP環境 / ID統合の最中でも、運用もポリシーも一本化し、組織全体を守る



既存環境への影響最小限

- 複雑な既存システムの困難な統合を実施する必要なし
- ユーザ属性やフォーマットはそのままでDuoにてアクセスポリシーを設定可能

コンプライアンスを統合

- 統一ポリシーをDuoのみで設定すれば、そのまま適用可能
- 監査ログも同時に統一
- 双方のアプリへアクセスする一時的なアクセス権はDuoでも保持可能。アクセス権の漏れや重複を排除。

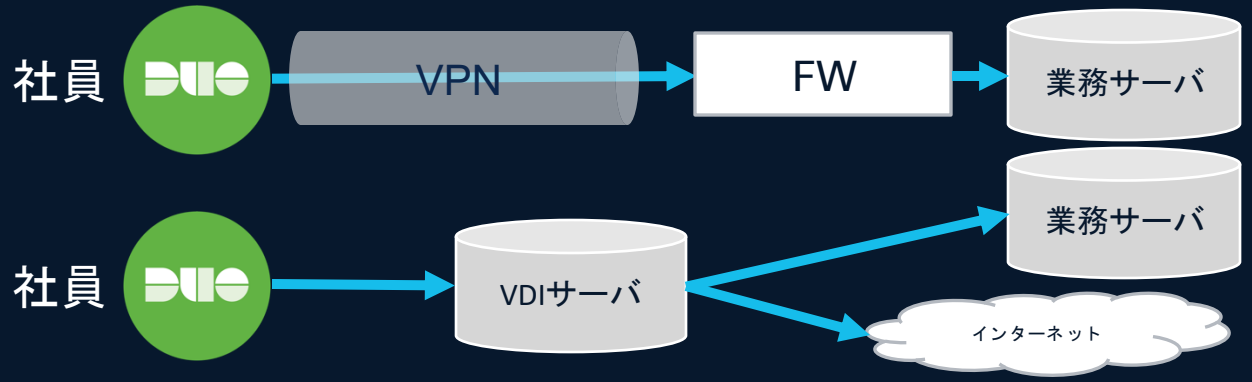
Duo 導入パターン

SSE+IDセキュリティ

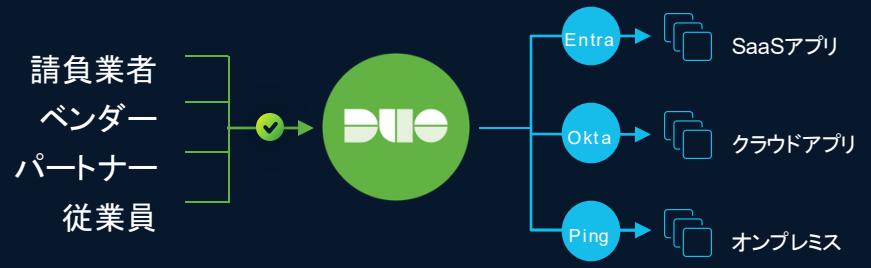
DuoはIdPにもなれる
IDセキュリティ+IdP

アプリケーション

リモートアクセスの保護

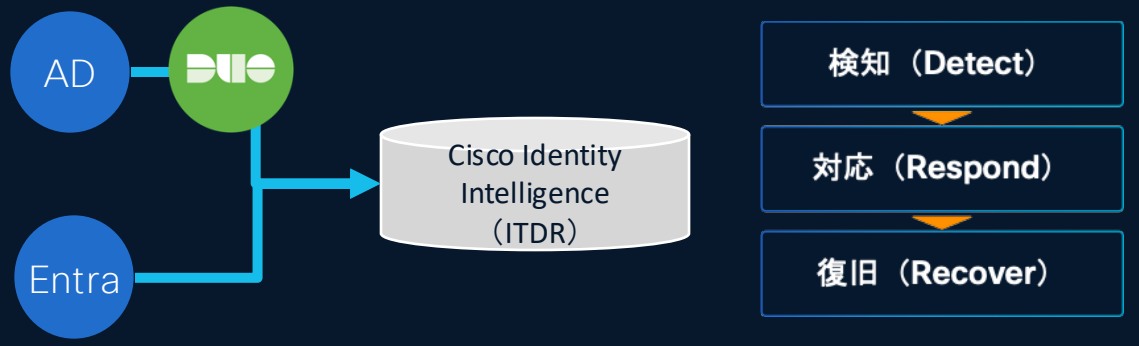


IdPの仲介とアクセスポリシーの統合



セキュリティ強化に必要なID管理の統合をDuoで実現

IDの振舞い分析（ITDR）



ここがすごいぞCisco Duo

Duoは end-to-end のフィッシング耐性プロセスを提供

シームレスにセキュリティを確実に保護

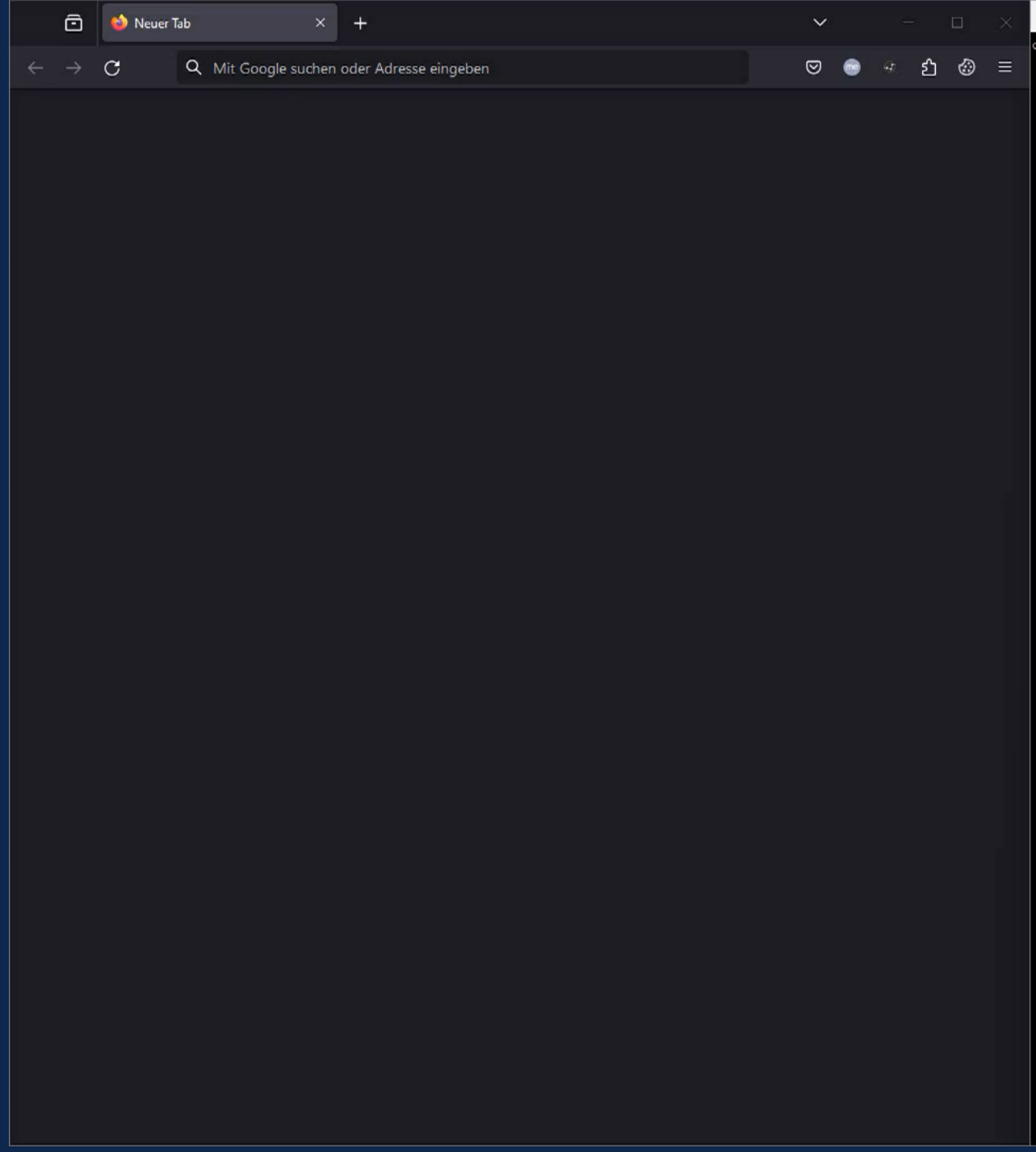
Cisco Identity Intelligence（ITDR）にてID可視化→脅威検知と対策

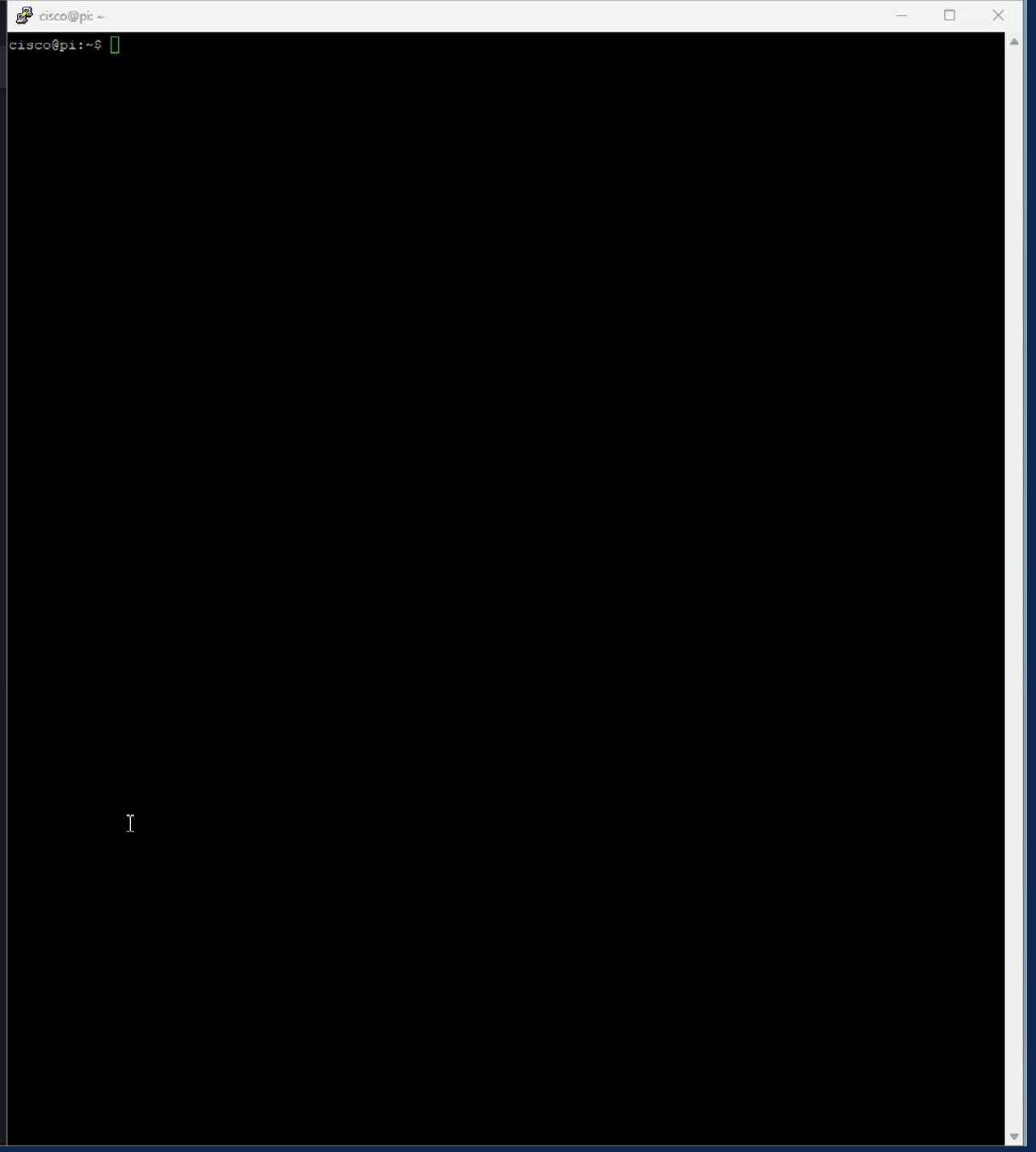
セッション盗難防止（Session Theft Protection）

Duo がセッション・クッキーを排除 – 特許出願中の独自技術

Cookieがないため Cookieは盗めない

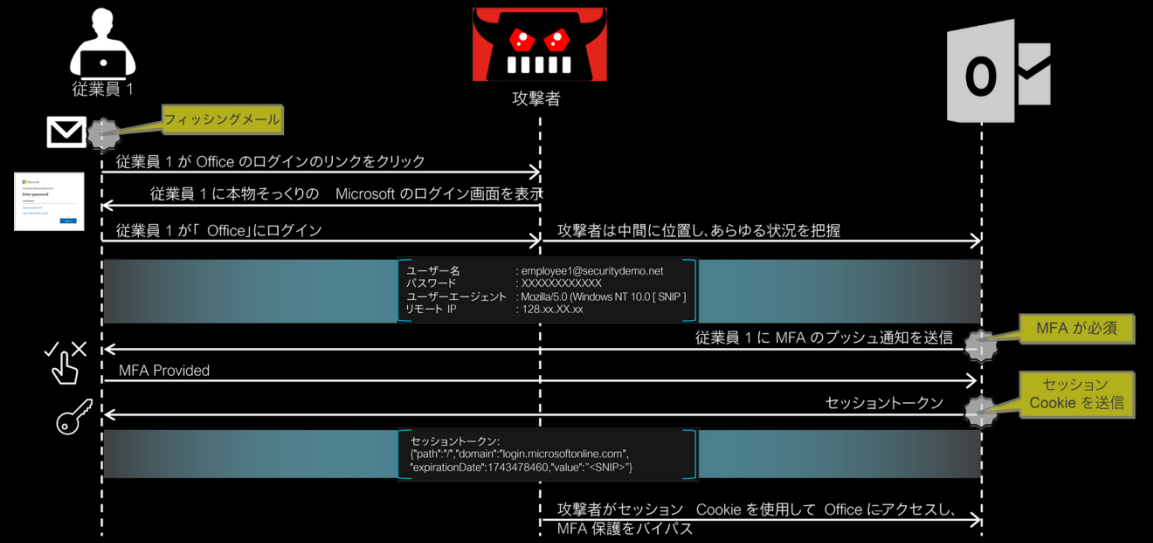
攻撃者はセッション Cookie を盗んで、すでに確立されたアクセスを乗っ取ります。セッション盗難防止機能を備えた Duo Passport は、認証フローから Cookie を削除するため、攻撃者は何も盗むものがなくなります。Duo のクッキーレスソリューションは、エンドユーザーエクスペリエンスを維持しながら、セキュリティにバランスの取れたアプローチを提供します。


Neuer Tab
Mit Google suchen oder Adresse eingeben


cisco@pi: ~
cisco@pi:~$

Duo Passport の Cookie レス認証

- 一般的なアカウント乗っ取り攻撃：
  - 中間者攻撃（AITM）のサービスへのリンクを含むフィッシングメールを送信
  - 従業員がログインし、AITM で Cookie を取得
  - Cookie を再生し、不正アクセスを取得
- Duo Passport の強力なデバイス紐づけ：Duo はセッションの Cookie を削除可能
  - 更新トークンは引き続き利用されるが、有効期間を短縮することでユーザーへの影響を軽減

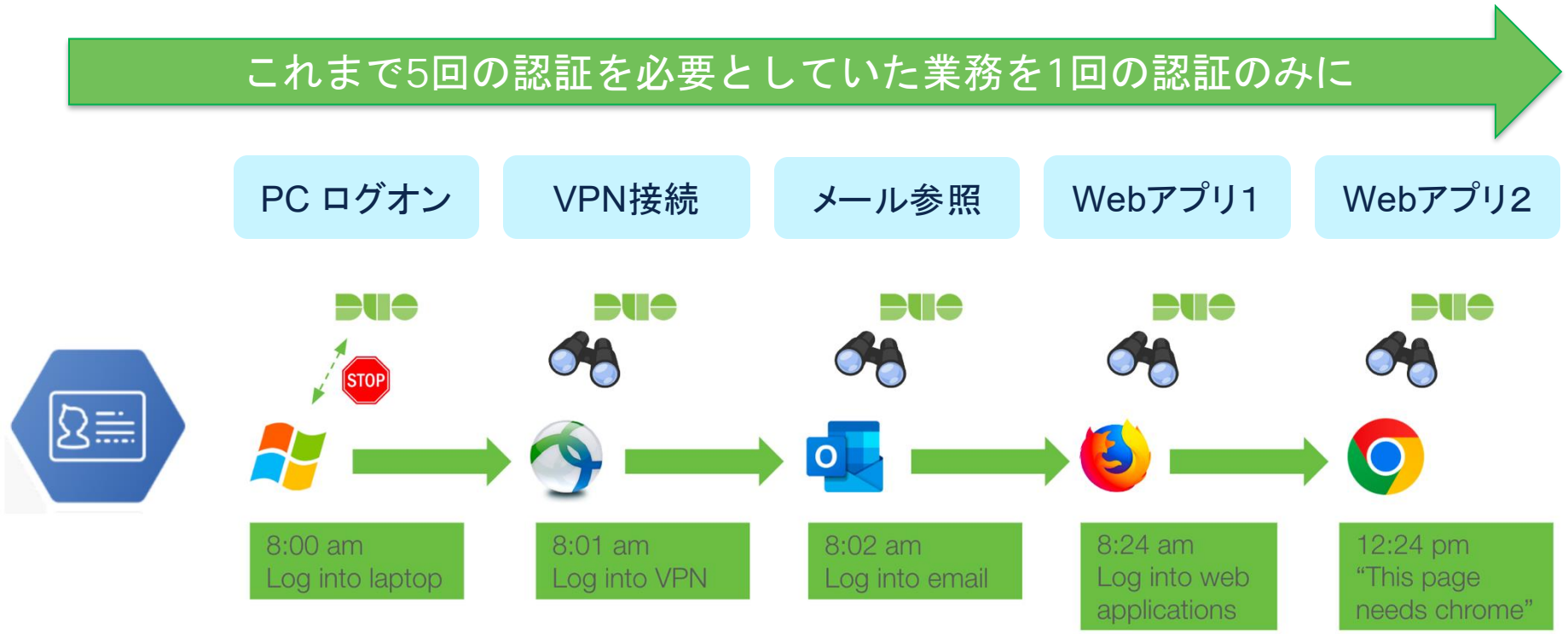


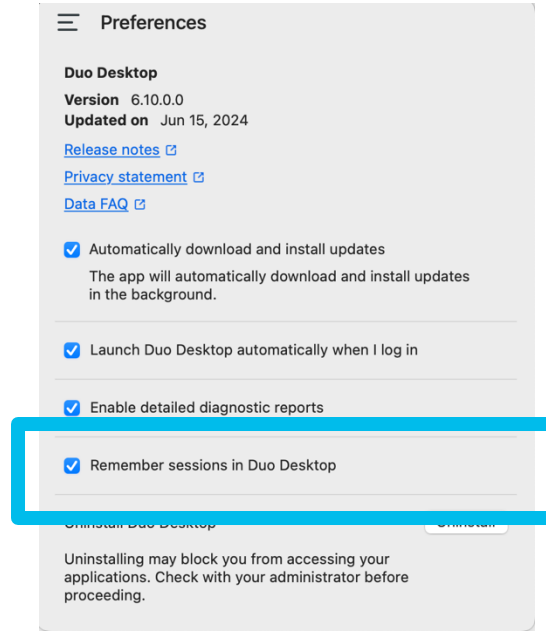
Duo Passport

Windows Logon時の１回の認証で
１日認証なし業務可能（生産性向上）

エンドユーザー一人ひとりの生産性が向上し、会社全体の業績向上に貢献

これまで5回の認証を必要としていた業務を1回の認証のみに





セッションをDuo Desktop
にて保管して実現
危険な状態になった場合に
すぐにセッション削除

まとめ

Cisco Duoによるアイデンティティセキュリティ設計

特定（Identify）

- ユーザーが誰で、どのリソースにアクセスできるかを把握する。
- ユーザーやデバイスの台帳を作成し、IAMでアカウントの登録・権限付与を管理。
- Identity Intelligenceを使って全体像を可視化する。

防御（Protect）

- IAMで強力なアクセス制御を行う。
- Identity IntelligenceのTrust LevelとDuoポリシーを組み合わせてエンドポイントを保護。認証を強化し、大規模環境でもコンプライアンスを維持。

検知（Detect）

- 不審な動きを継続的に監視（例：連続したログイン失敗、異常なアクセス元など）。
- Identity Intelligenceがクロスプラットフォーム分析を行い、パターンや異常を素早く検知し、IT管理者に早期警告を提供。

対応（Respond）

- 高精度なインサイトを基にインシデント対応を実施。
- Identity Intelligenceが優先度付け・エスカレーション・迅速な行動を支援。
- SIEM/SOAR連携を活用し、脅威封じ込め・ポリシー調整・対応記録を行う。

復旧（Recover）

- インシデント後、速やかに復旧できるよう支援。
- IT管理者は組織に学びを提供し、ギャップを埋め、ポリシーを強化。Identity Intelligenceとプレイブックを見直し、回復力を実証し、長期的な信頼を構築。


CISCO