

# シスコ セキュリティ ウェビナー アイデンティティ セキュリティ最前線

Hiroki Hata

2025 年 10 月

# アジェンダ

- 最近のIdentityを狙った攻撃
  - ✓ フィッシング攻撃
  - ✓ AIの悪用によるサイバー攻撃
- Cisco Duo の提供価値と検討事例
  - ✓ 強度の高い多要素認証
  - ✓ 脅威を迅速に検知可能なITDR
- Cisco Duo のその他の価値

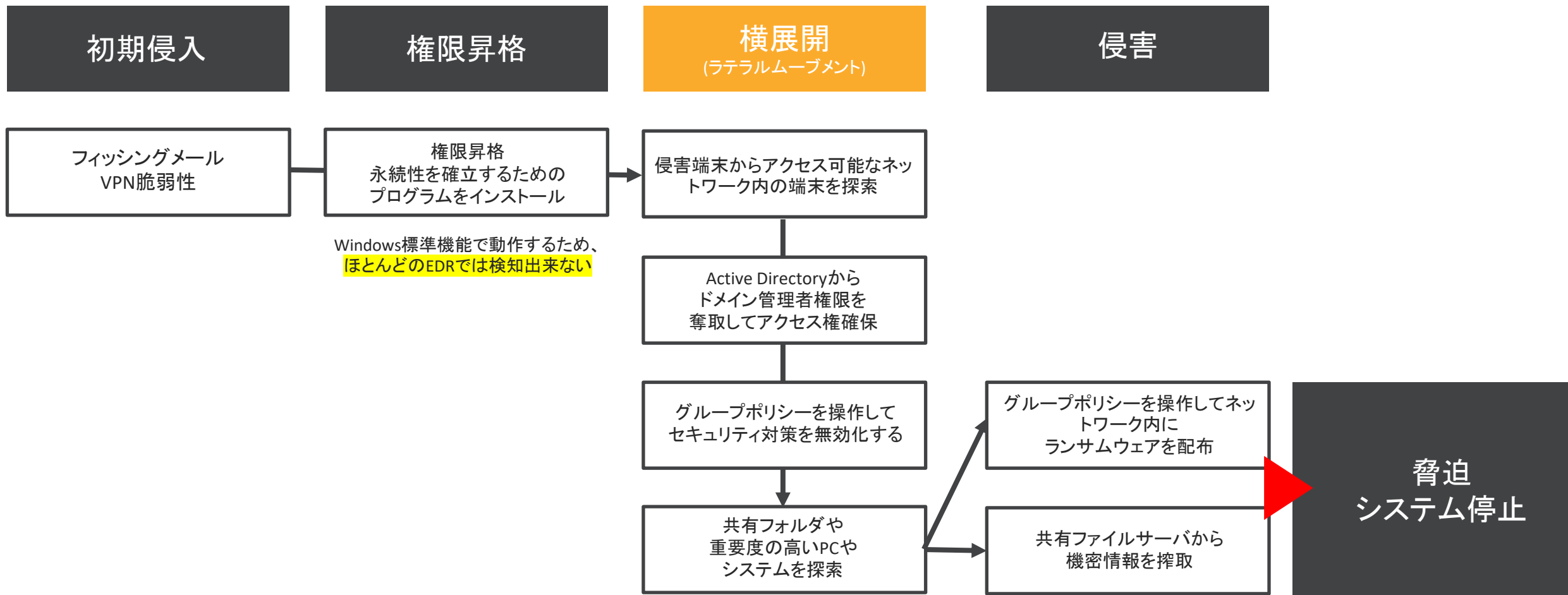
数年前から年々悪化している  
→Identityの危機

60%

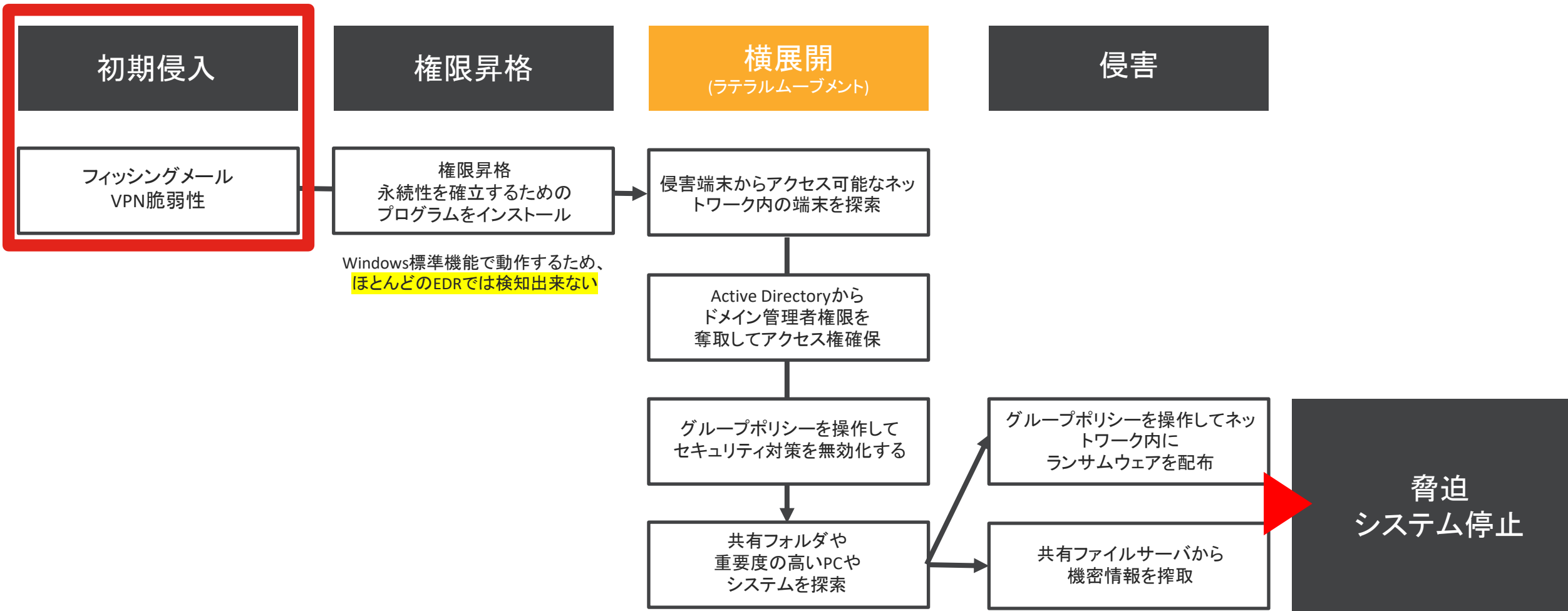
の情報漏洩はIdentityの漏洩が  
重要な要素になっている  
(Identityがなければ起こらない)

*Cisco Talos Incident Response | Year in Review 2024*


# 攻撃のフローとラテラルムーブメント



# 攻撃のフローとラテラルムーブメント



# フィッシング攻撃


 Neuer Tab


←


→


↻


Mit Google suchen oder Adresse eingeben









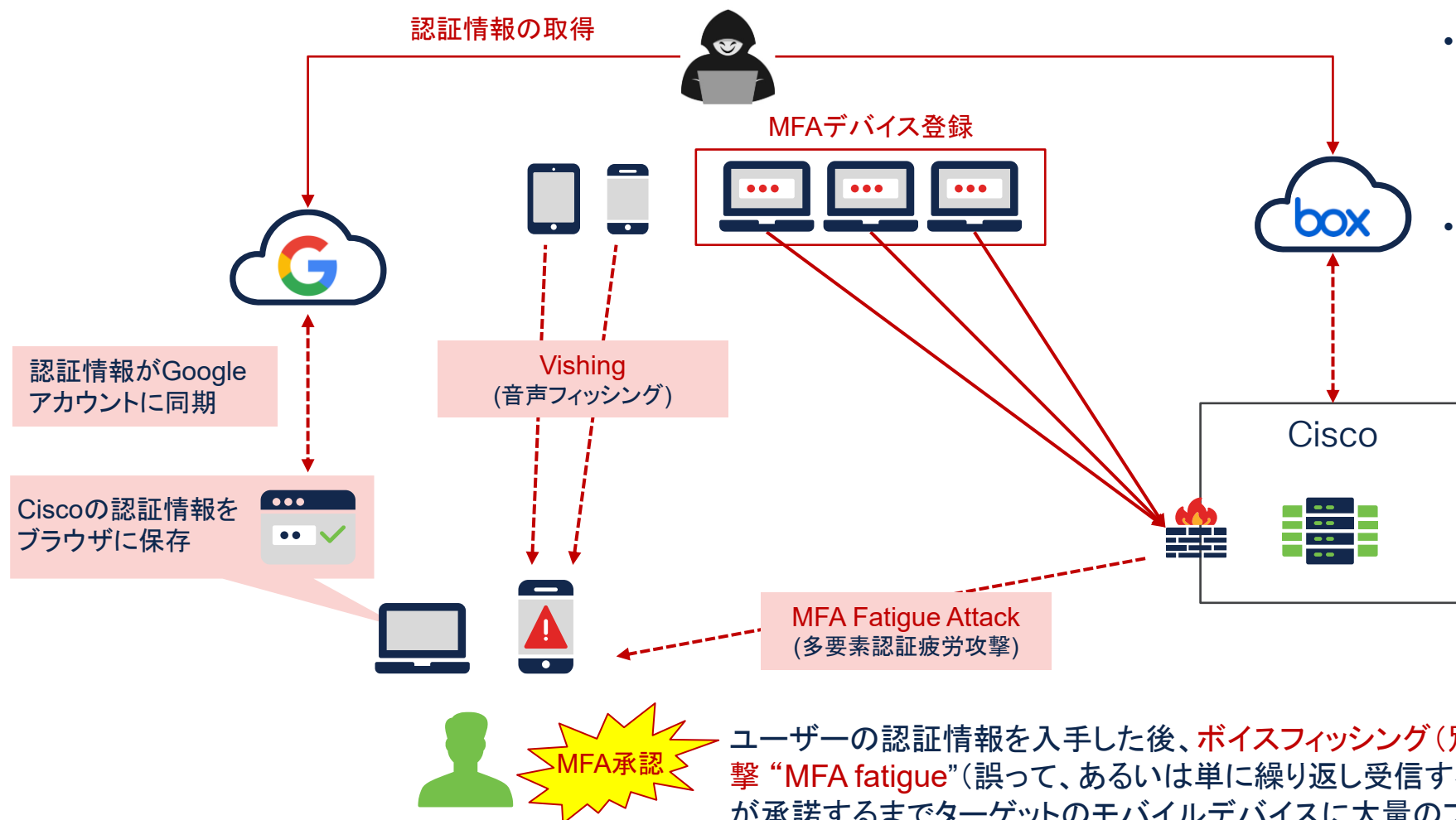


cisco@pi: ~

```
cisco@pi:~$
```

I

# シスコに対するサイバー攻撃の概要



- 最初のアクセスを取得した後、脅威行為者は、アクセスを維持し、フォレンジックアーティファクトを最小限に抑え、環境内のシステムへのアクセスレベルを上げるために、様々な活動を実施
- この脅威アクターを環境から排除することに成功し、攻撃後の数週間、繰り返しアクセスを回復しようとする粘り強さを見せたが、これらの試みは失敗

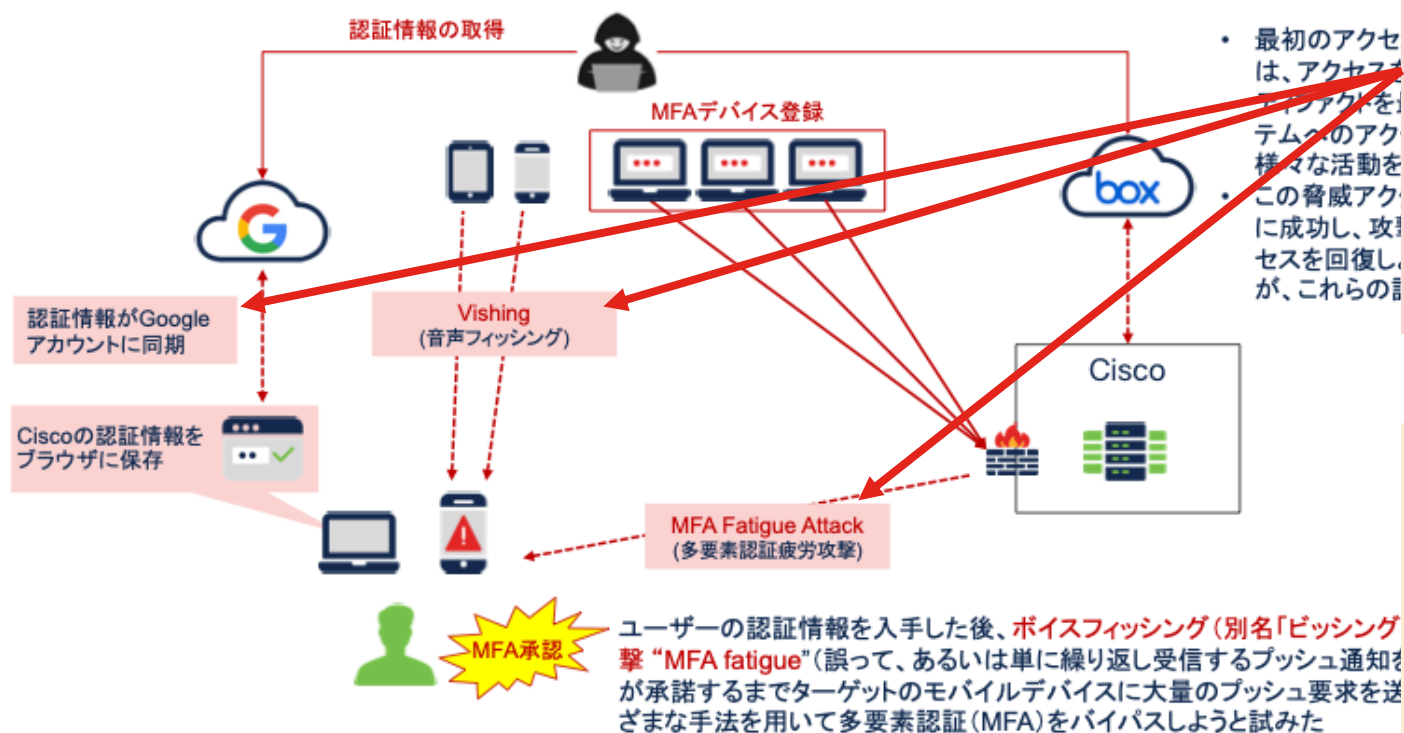
ユーザーの認証情報を入手した後、ボイスフィッシング(別名「ビッシング」"vishing")やMFA疲労攻撃 "MFA fatigue"(誤って、あるいは単に繰り返し受信するプッシュ通知を黙らせるために、ユーザーが承諾するまでターゲットのモバイルデバイスに大量のプッシュ要求を送信するプロセス)など、さまざまな手法を用いて多要素認証(MFA)をバイパスしようと試みた



# AIの悪用によるサイバー攻撃

# AIを使ったサイバー攻撃が本格化

## シスコに対するサイバー攻撃の概要



 © 2025 Cisco and/or its affiliates. All rights reserved.

## AIを使って「自動化」「高度化」

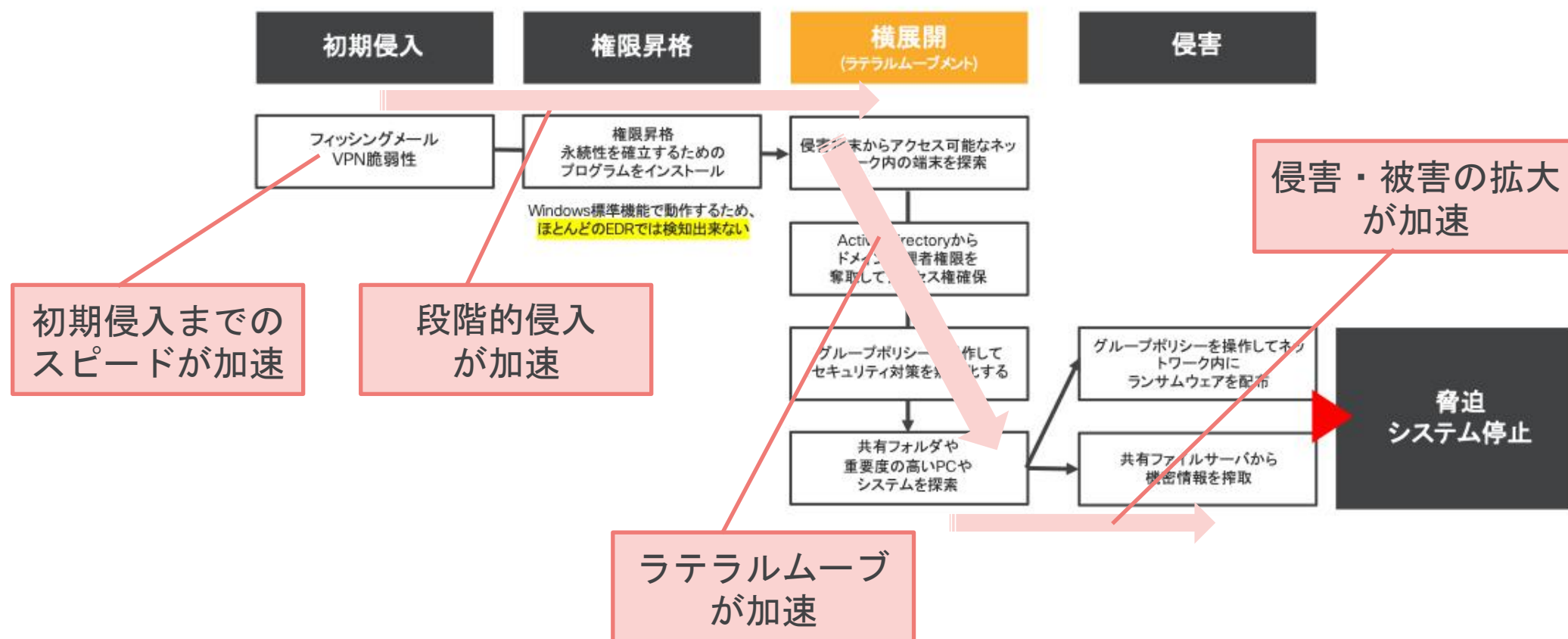
- フィッシングは単純な迷惑メールから多層攻撃へ進化
- メール／SNS／モバイルを組合せ、検知を回避する手法が主流
- 自動化により「瞬時発生」も「段階的侵入」も可能

## 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

# AIによって侵入から侵害までの時間が一気に短縮

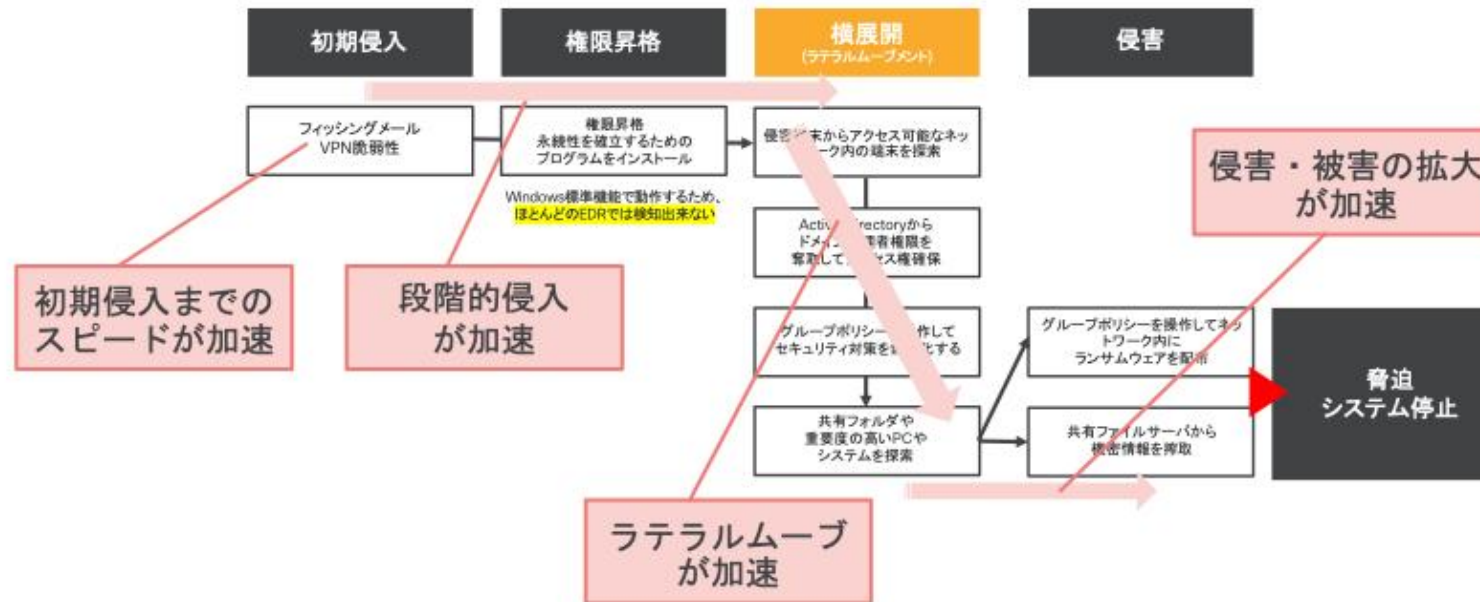
## 攻撃のフローとラテラルムーブメント



# 防御の鍵は“時間”

AIによって侵入から侵害までの時間が一気に短縮

## 攻撃のフローとラテラルムーブメント



サイバーセキュリティにおける勝敗は、“時間”で決まる

# 現時点で可能な短期かつ実行的対策

技術対策

多要素認証の徹底  
ディープフェイク検出ツール導入

迅速検知

多層ログと相関分析の導入

サプライチェーン監視

外部連携点の異常検出ルール化

ユーザ教育

AI生成メッセージの見分け方を周知

# 現時点で可能な短期かつ実行的対策

技術対策

多要素認証の徹底

ディープフェイク検出ツール導入

迅速検知

多層ログと相関分析の導入

サプライチェーン監視

外部連携点の異常検出ルール化

ユーザ教育

AI生成メッセージの見分け方を周知



# 多要素認証の徹底 強度の高い多要素認証の重要性

フィッシング耐性のある MFA		
例 パスワードレス認証、近接認証	脅威力バレッジ 中間者攻撃	強度 最強
疲労耐性 MFA		
Verified Duo Push	プッシュボム	強
プッシュベースの MFA		
プッシュ	SIM スワップ	中
電話ベースの MFA		
SMS、コールバック	パスワードスプレー、ブルートフォース	弱
MFA なし		
ユーザー名 + パスワード	なし	最弱

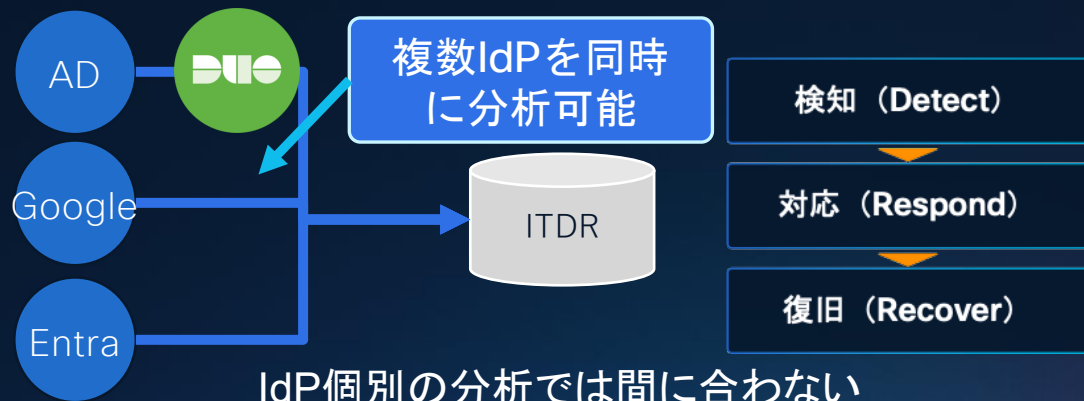
## 規制当局によるフィッシング対策

- 米国
- Office of Management & Budget (OMB) の覚書 22-09 にて、全連邦政府機関とそのサプライヤに対し、フィッシング耐性のある MFA を導入するよう要請
  - CISA の実装ガイドラインでフィッシング耐性のある MFA を明記

- ヨーロッパ
- NIS2 指令「Boosting your Organisation's Cyber Resilience Publication 22-01」にて、MFA において「スマートカードや FIDO2 セキュリティキーなどのフィッシング耐性のあるトークンの導入を検討」すべきと明記

# 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

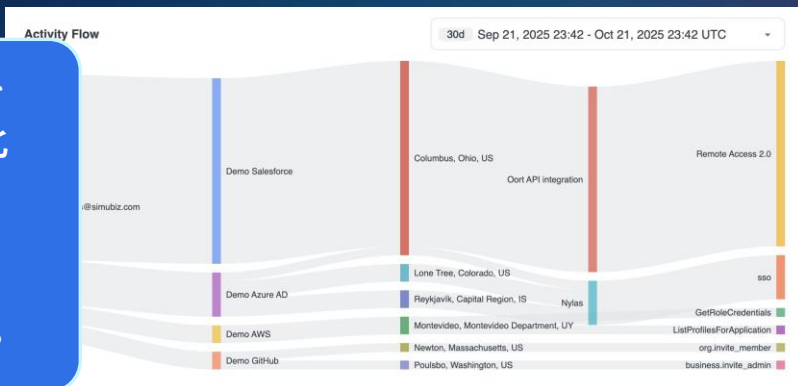


組織に存在するIdを集約化し、可視化

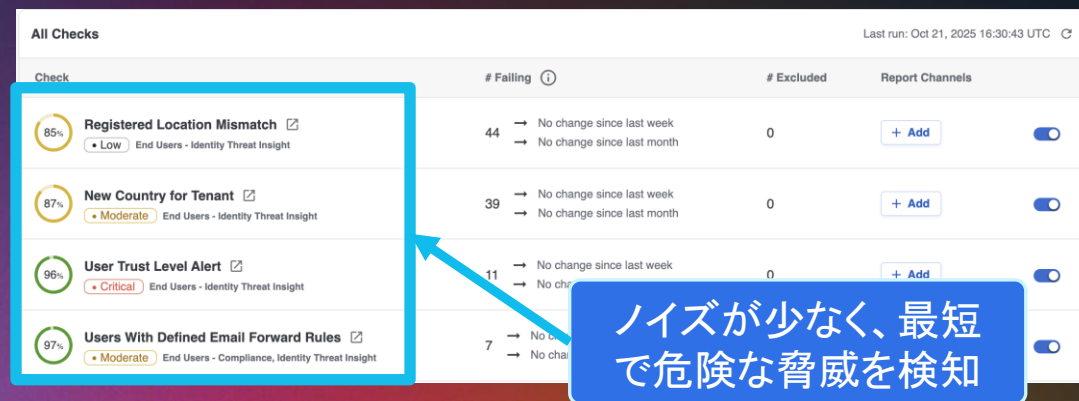


ユーザ毎のIdに関する振舞いを可視化

Idの振舞いを  
一目で可視化  
・どのIdP?  
・どの場所?  
・どのVPN?  
・どのアプリ?



危険な脅威を最短で検知可能





# Cisco Duo の提供価値と検討事例

# Cisco Duoが提供する新しい IAM (Identity & Access Management)

お客様が信頼できるIdentityを提供

NEW

セキュリティFirstのIAM

導入時点で守られている

NEW

End to Endで  
フィッシング耐性のMFA

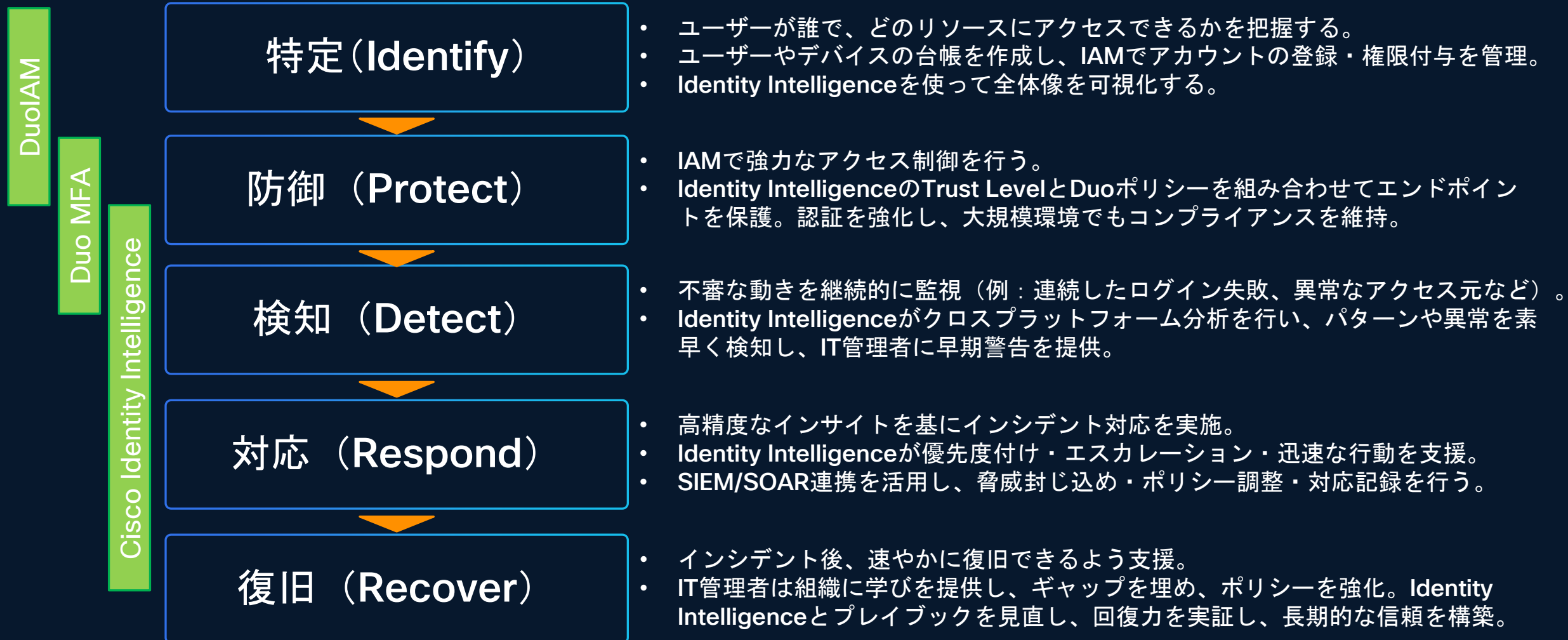
完全にフィッシングの  
可能性を排除

統合  
Identity Intelligence  
(ITDR)

継続的に信頼を検証する

世界レベルのユーザエクスペリエンスをエンドユーザーと管理者に  
攻撃者を困らせ, ユーザが使いやすい

# 参考：Cisco Duoによるアイデンティティセキュリティ設計



Cisco Duo

強度の高い多要素認証

# Cisco Duo 最新UPDATE

Cisco Duoが提供する新しい IAM (Identity & Access Management) 機能

NEW

セキュリティFirstのIAM

導入時点で守られている

NEW

End to Endで  
フィッシング耐性のMFA

完全にフィッシングの  
可能性を排除

統合  
Identity Intelligence  
(ITDR)

継続的に信頼を検証する

世界レベルのユーザエクスペリエンスをエンドユーザーと管理者に  
攻撃者を困らせ, ユーザが使いやすい

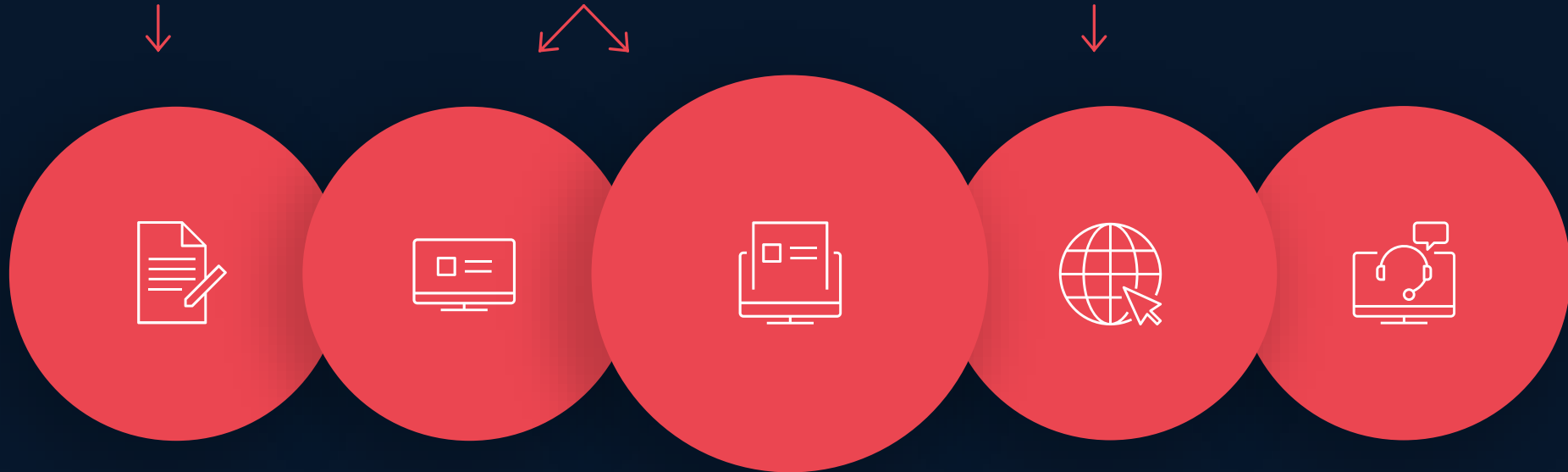
# end-to-end で狙われるIdentity

攻撃対象は拡大しており、脅威は急速に拡大している⇒MFA だけではもはや不十分

新しい社員に対するブルートフォース攻撃やパスワードスプレー攻撃が拡大

MFAをバイパスするため、疲労攻撃やVishing攻撃が拡大

セッションのクッキーを盗むフィッシング攻撃が急速に拡大



ID新規登録

OS ログイン

Application ログイン

中間セッション

ヘルプデスク

攻撃者は組織内にアクセスできるデバイスを登録しようとしている

攻撃者はMFAオプションの選択で弱いMFAでの認証を狙っている

攻撃者はヘルプデスクに対し、SNSの情報を利用して攻撃し、アクセス方法を確保しようとしている

# Duoは end-to-end のフィッシング耐性プロセスを提供



**ID新規登録**

信頼できるIDのみ登録



**OS ログイン**

フィッシング耐性MFA



**Application ログイン**

フィッシング耐性MFA



**中間セッション**

中間者攻撃への防御



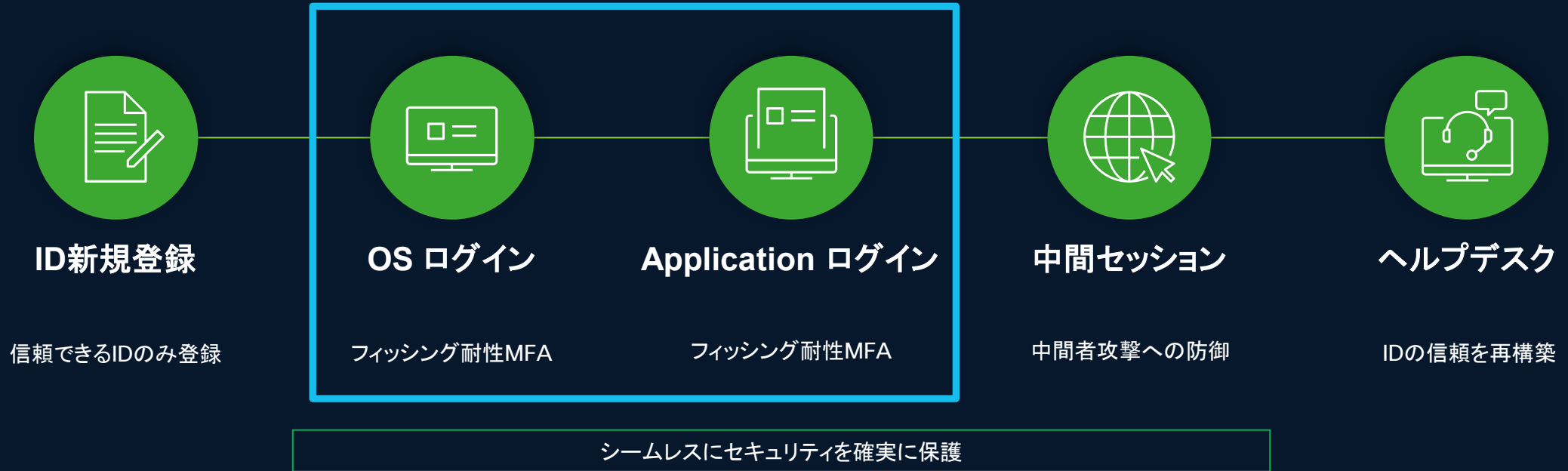
**ヘルプデスク**

IDの信頼を再構築

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

# Duoは end-to-end のフィッシング耐性プロセスを提供



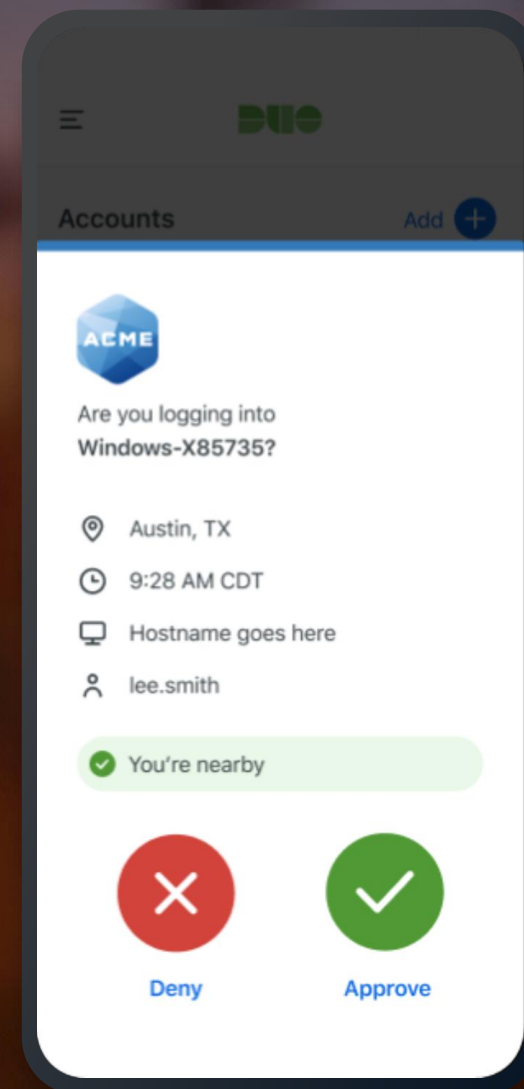
Cisco Identity Intelligence (ITDR)にてID可視化→脅威検知と対策



# 近接認証 Proximity Verification

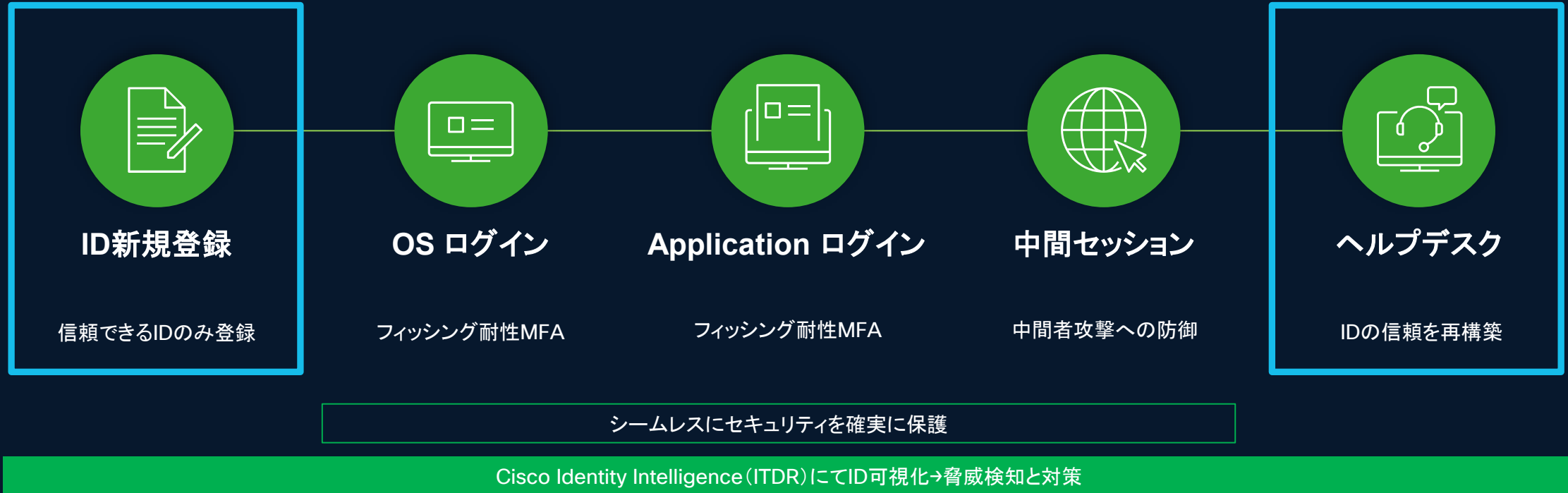


## Bluetooth Low Energy (BLE)



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）

# Duoは end-to-end のフィッシング耐性プロセスを提供



本人の信頼性を確実に確認

# Duo Identity Verification Integration

## ユースケース



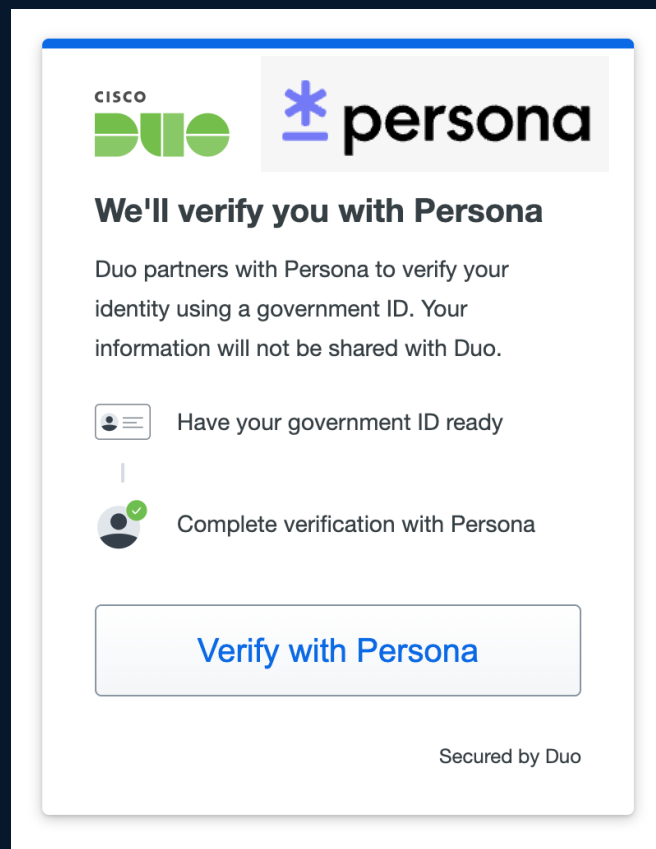
ID新規登録

- 新入社員のID新規登録時の本人確認
- パートナーID新規登録時の本人確認



ヘルプデスク

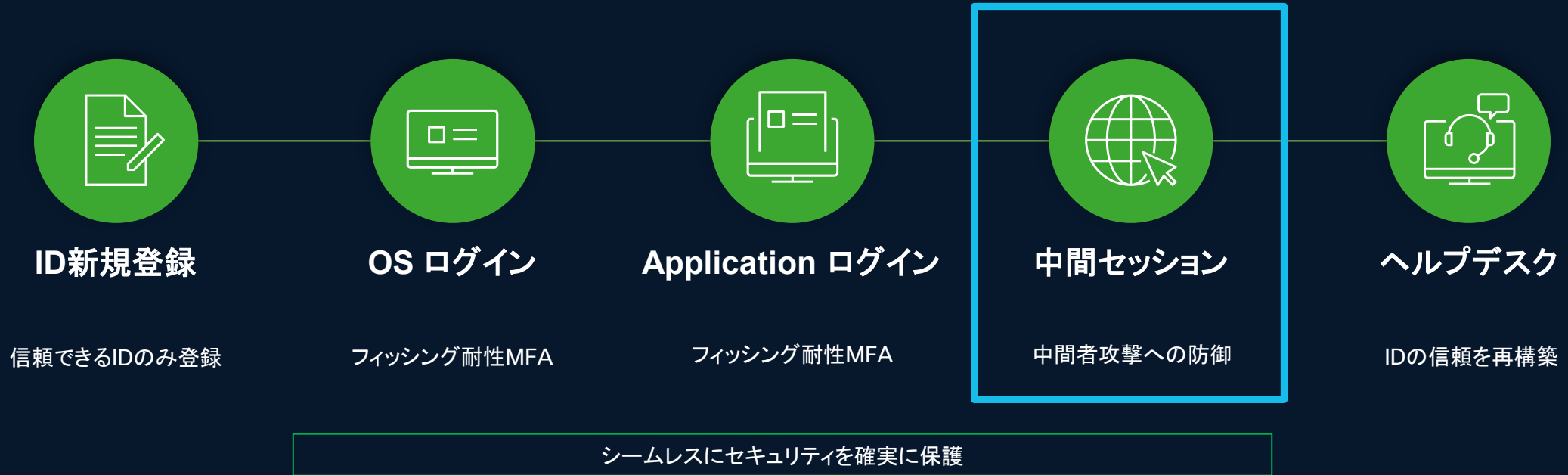
- 問い合わせ時の本人確認
- 脅威検出時の本人確認



信頼を確立するために、ユーザーはDuoに保存されている情報を照合し、政府発行のIDと自撮り写真を提出しなければならない。



# Duoは end-to-end のフィッシング耐性プロセスを提供



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





実際のログインページ

ハッカーにコントロールされるプロキシページ

通常と同じように見える偽のページ

# セッション盗難防止 (Session Theft Protection)



## 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。

Duo がセッション・クッキーを排除 - 特許出願中の独自技術

Cisco Duo

脅威を迅速に検知可能なITDR

IDアクセス統合と複数IDPを統合可能なITDR



# Cisco Duo 最新UPDATE

Cisco Duoが提供する新しい IAM (Identity & Access Management) 機能

IDアクセス統合

セキュリティFirstのIAM

導入時点で守られている

NEW

End to Endで  
フィッシング耐性のMFA

完全にフィッシングの  
可能性を排除

ITDR

統合  
Identity Intelligence  
(ITDR)

継続的に信頼を検証する

世界レベルのユーザエクスペリエンスをエンドユーザーと管理者に  
攻撃者を困らせ, ユーザが使いやすい



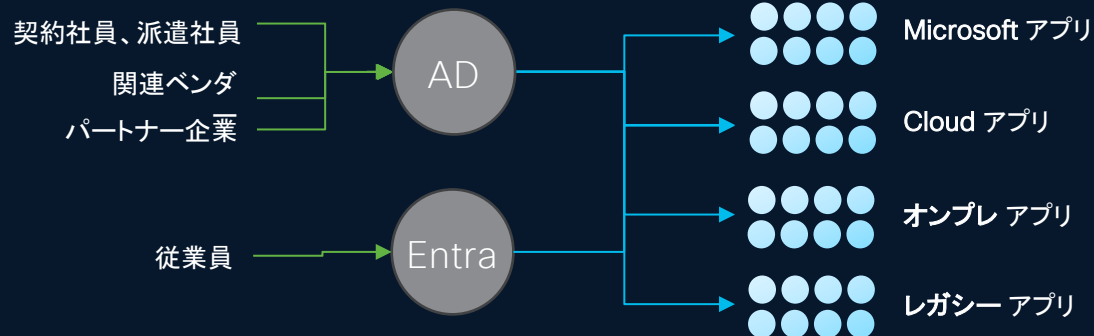
# 新機能Duo IAM ユースケース

# ユースケース①複数IDP環境の統合

## 複数IDP環境の統合におけるお客様課題・想定リスク

## 課題

本社A社インフラ



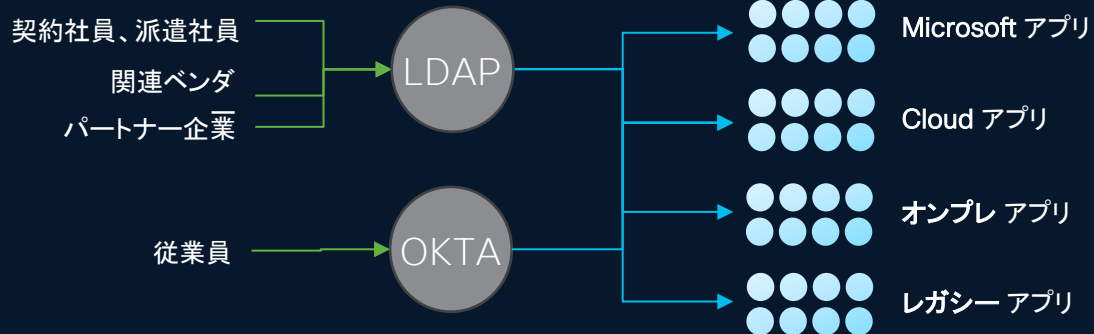
課題①：断片化したID環境の一貫した可視化と安定運用

- 各社が独自のActive Directory、LDAP環境を保有
- 異なるIdP（OKTA、EntraID、GWS等）の混在

（お客様課題・想定リスク）

- ✓ ユーザ情報の属性やフォーマットの不整合で統合不可
- ✓ 認証ポリシーとセキュリティ基準の相違で統合不可
- ✓ 既存システムとの依存関係の複雑性→独立したIDP

グループ会社B社インフラ



課題②：セキュリティ維持とコンプライアンス準拠の継続

- 各社の権限管理ルール of 統合困難
- コンプライアンス要件の不一致

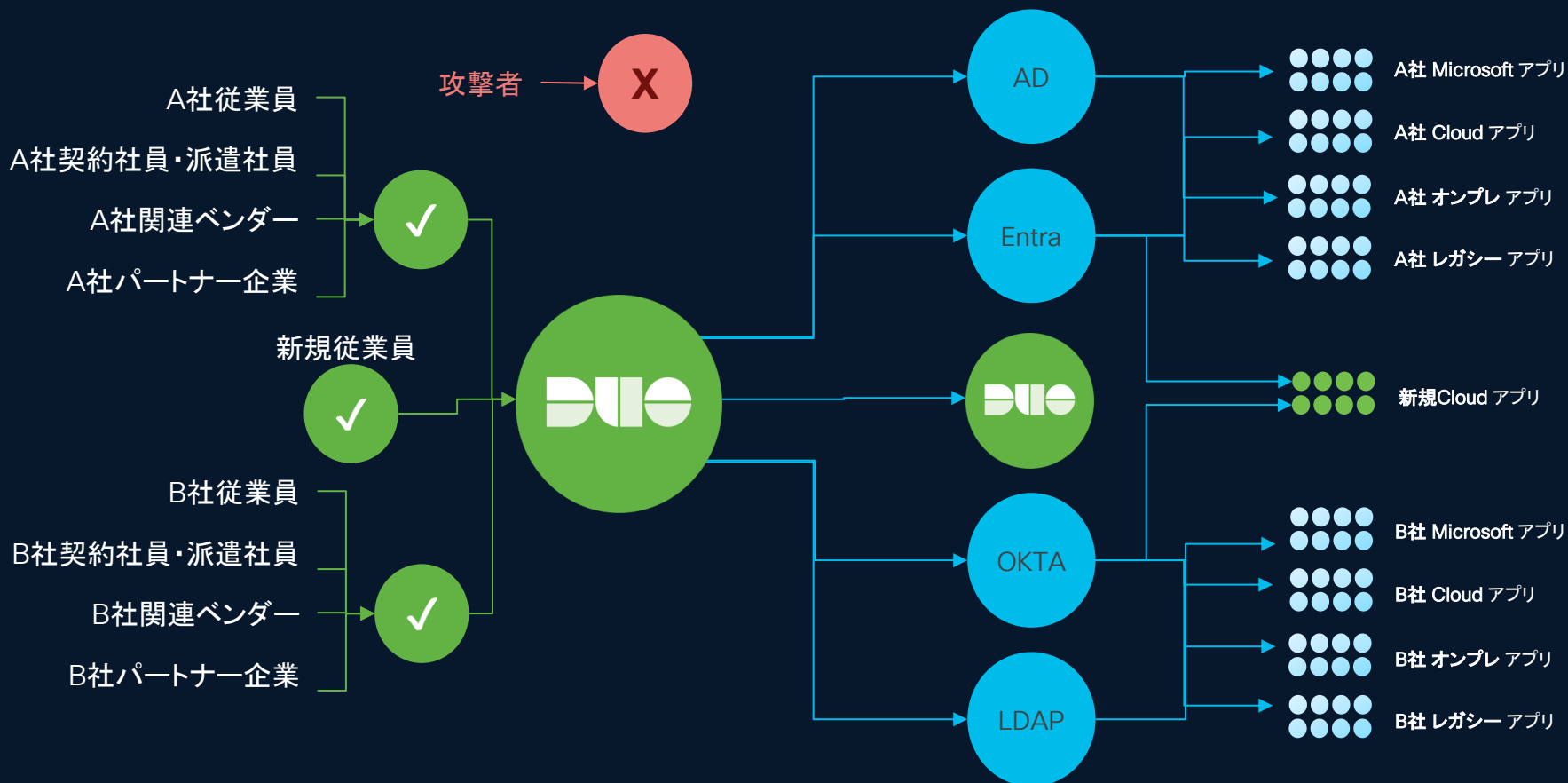
（お客様課題・想定リスク）

- ✓ 統合期間中の侵害リスク増加（30%程度増加）
- ✓ 一時的なアクセス権の重複や漏れ
- ✓ 監査ログの分散により、整合性と一次切り分けが遅延

# ユースケース① IdPの仲介(ブローカー)

## 効果

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

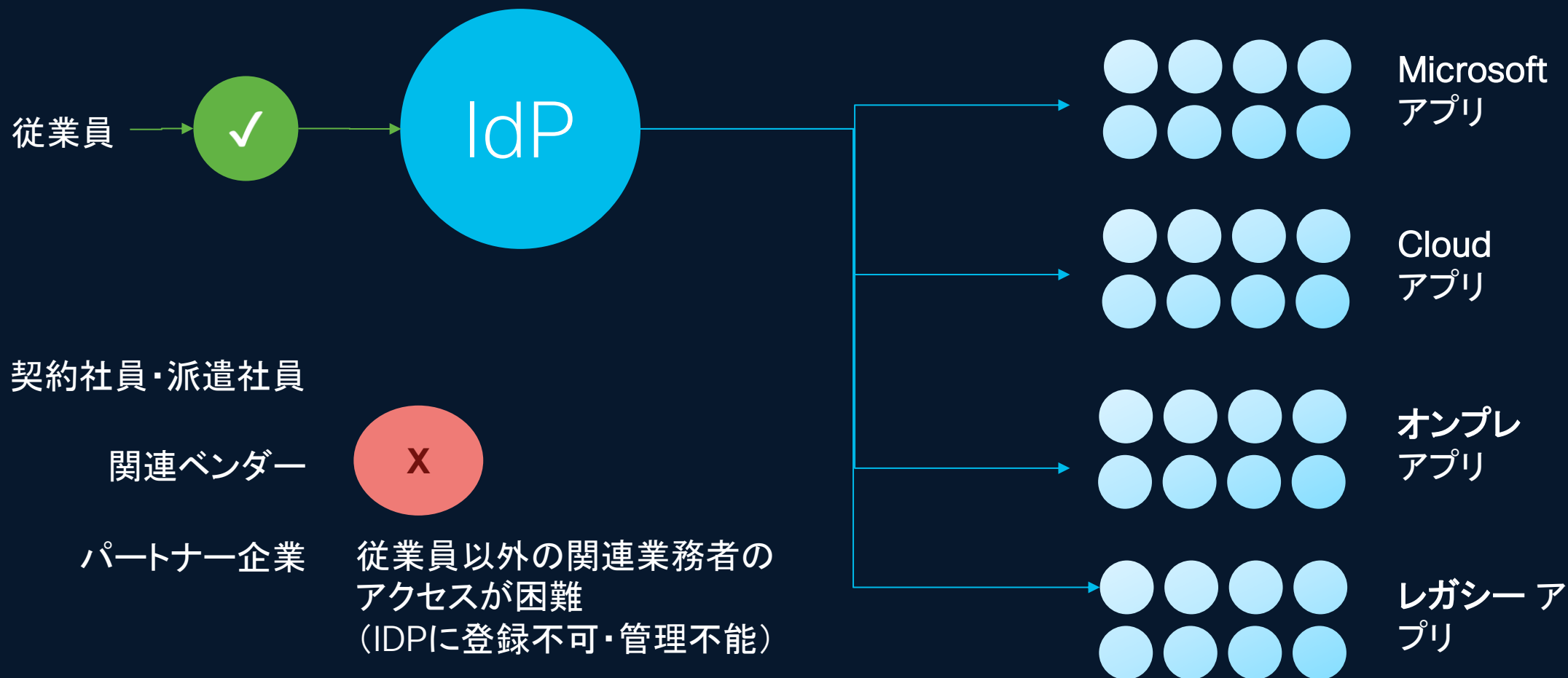
- 複雑な既存システムの困難な統合を実施する必要なし
- ユーザ属性やフォーマットはそのままDuoにてアクセスポリシーを設定可能

### 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。

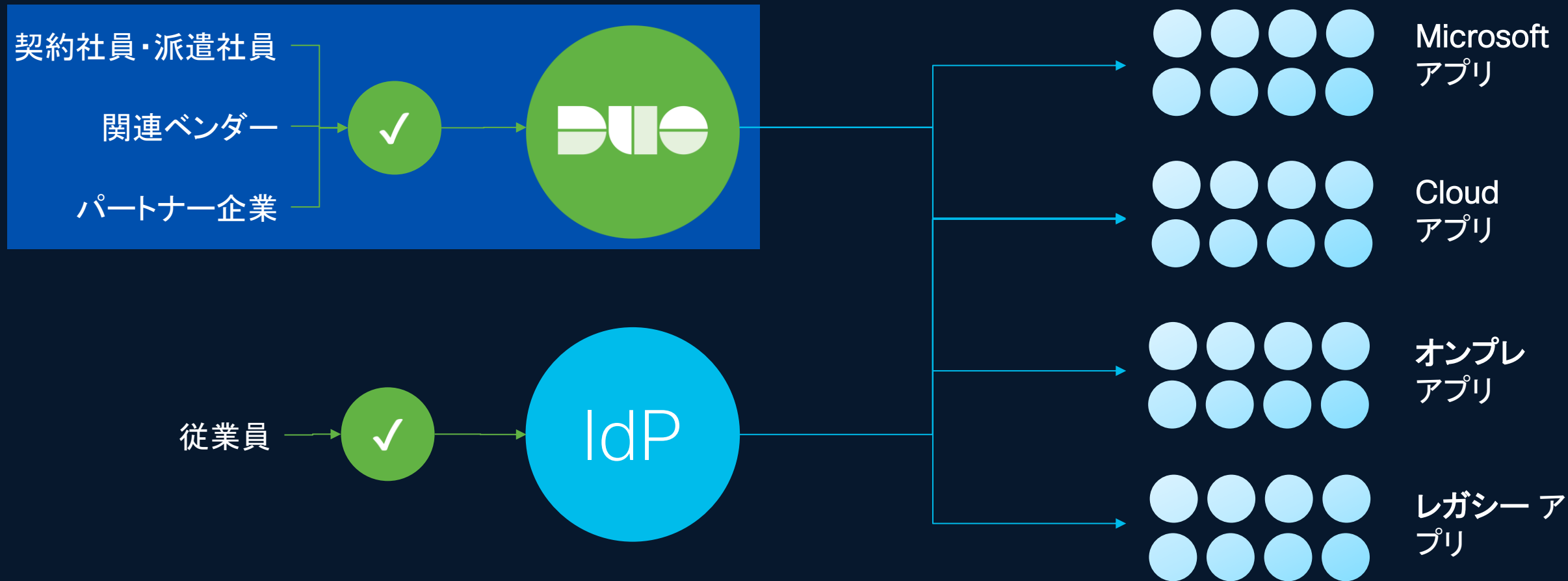
# ユースケース② 従業員以外のIDP利用

## 課題



他社との協業できないことがプロジェクトの推進に弊害となっている

## ユースケース②従業員以外のIDP利用



Duo IAMにて関連業務者を管理して、セキュリティを確保

# Cisco Duo 最新UPDATE

Cisco Duoが提供する新しい IAM (Identity & Access Management) 機能

IDアクセス統合

セキュリティFirstのIAM

導入時点で守られている

NEW

End to Endで  
フィッシング耐性のMFA

完全にフィッシングの  
可能性を排除

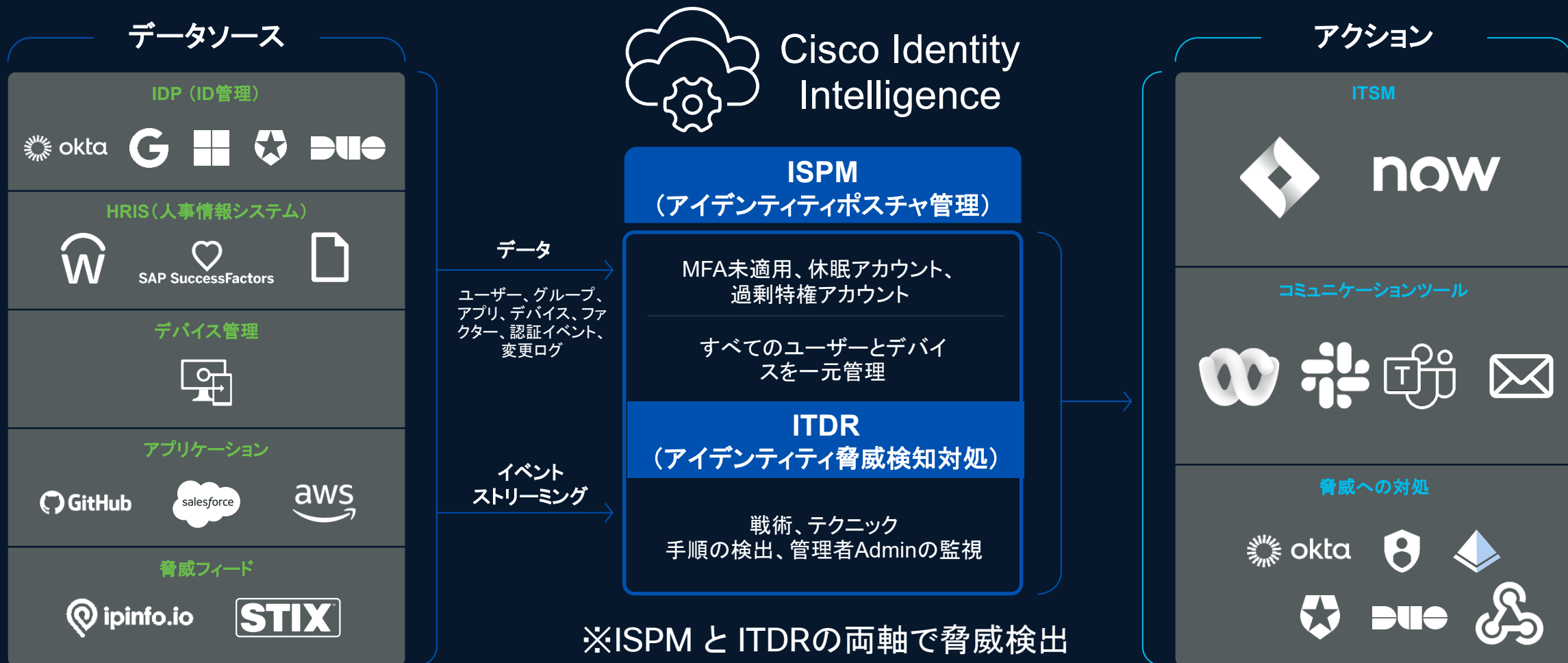
ITDR

統合  
Identity Intelligence  
(ITDR)

継続的に信頼を検証する

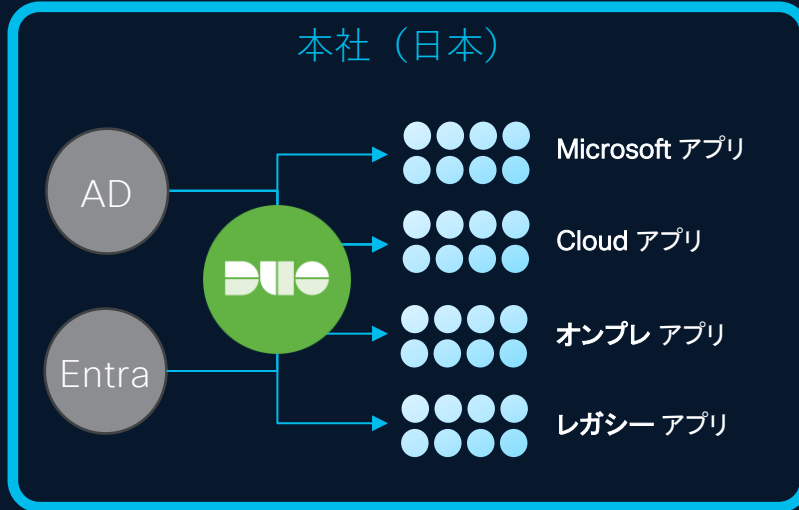
世界レベルのユーザエクスペリエンスをエンドユーザーと管理者に  
攻撃者を困らせ, ユーザが使いやすい

# Cisco IT にて現在も継続利用 ID環境に対する可視化→ポスチャ→脅威検出→対応を強力に実現

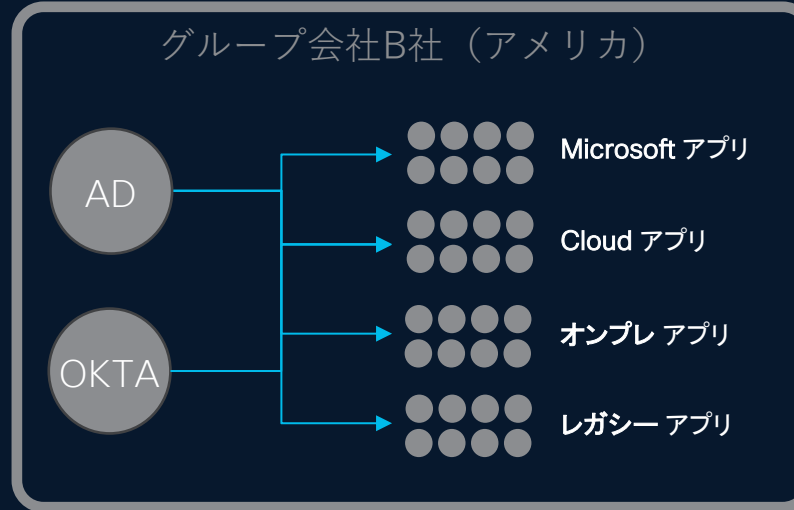


Cisco Duo (多要素認証・デバイス認証) Advantageに搭載

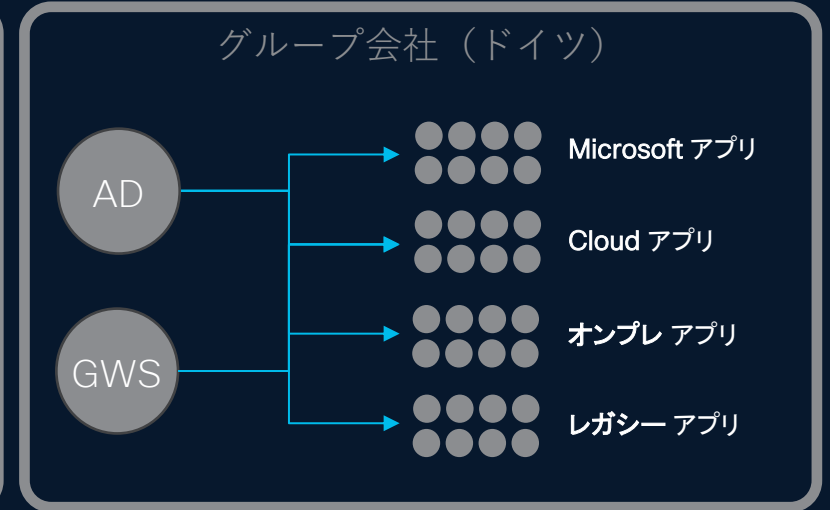
# ユースケース④ 複数環境のIDの振舞い分析 (ITDR) 課題



日本の管理下のため、  
全て可視化可能



アメリカ管理下、  
一部日本のユーザも登録さ  
れるも可視化不可

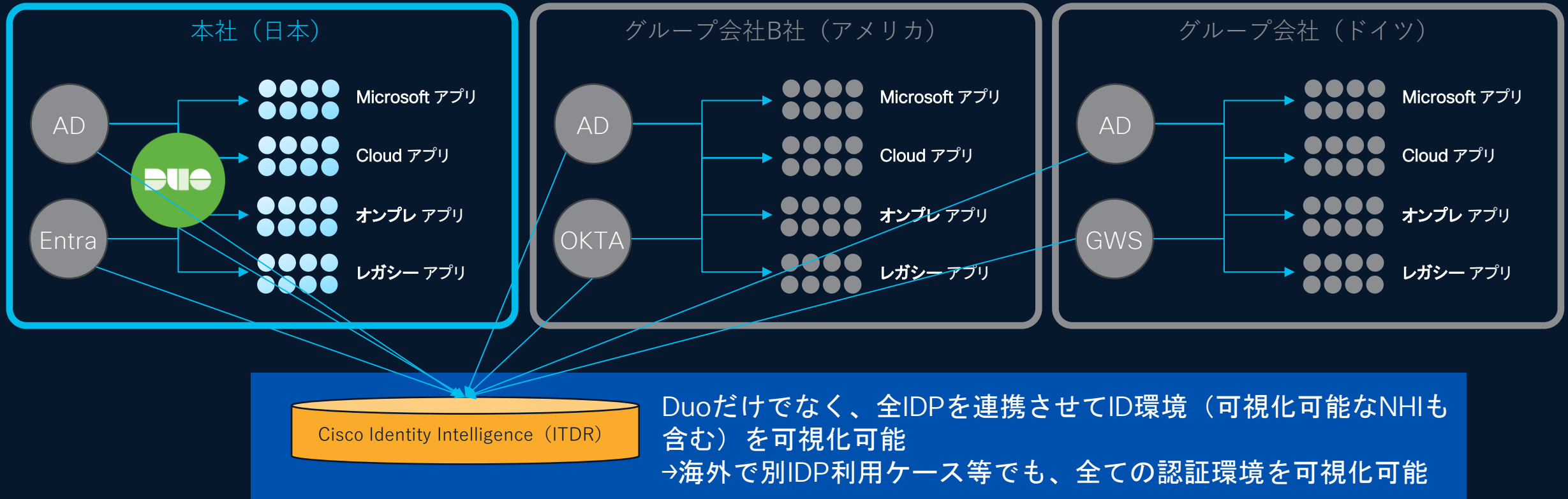


EU（GDPR）管理下、  
一部日本のユーザも登録さ  
れるも可視化不可

海外拠点を含めたID環境の可視化が困難で統合管理ができない

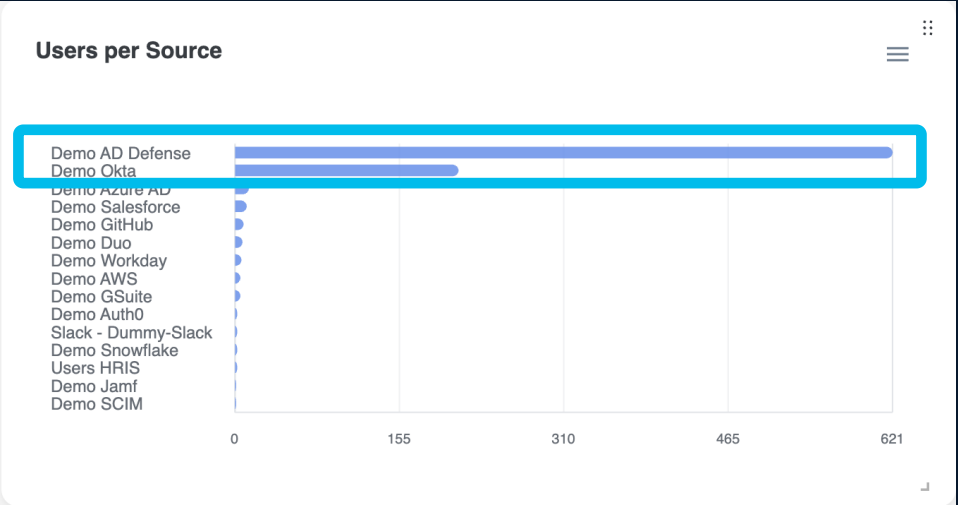
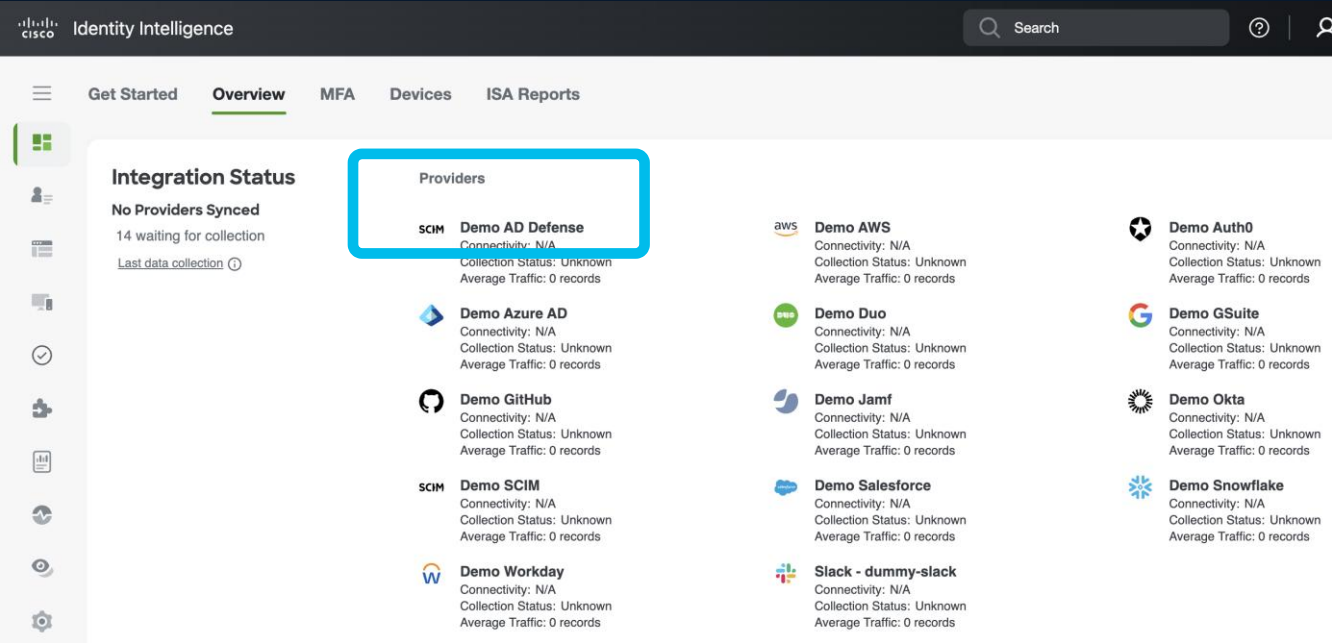


# ユースケース④ 複数環境のIDの振舞い分析 (ITDR) 効果



Duo IAMの柔軟性とCIIの拡張性がポイント

# Active Directory Defense (Private Preview前)



Cisco Identity Intelligence  
オンプレADサポートがPrivate Previewに

621 users found

# IPs ↑	# Logins ↑	Last Seen (UTC) ↑	Last IP Address ↑	Last Location	MFA ↑	Providers	Status ↑
(Admin) Adelle Francesco <input checked="" type="checkbox"/>	1	3, 2025 11:01:11	N/A	N/A	<input checked="" type="checkbox"/>	SCIM	Active
(Admin) Balan Malachi <input checked="" type="checkbox"/>	1		N/A	N/A	<input checked="" type="checkbox"/>	SCIM	Inactive
(Admin) Burdette Dan <input checked="" type="checkbox"/>	1	4, 2025 13:48:31	N/A	N/A	<input checked="" type="checkbox"/>	SCIM	Inactive
(Admin) Burdette Izabella <input checked="" type="checkbox"/>	1	8, 2025 10:33:05	N/A	N/A	<input checked="" type="checkbox"/>	SCIM	Inactive
(Admin) Dessie Judge <input checked="" type="checkbox"/>	1	1, 2025 12:27:34	N/A	N/A	<input checked="" type="checkbox"/>	SCIM	Active
(Admin) Echo Mauricio <input checked="" type="checkbox"/>	1	1, 2025 00:13:43	N/A	N/A	<input checked="" type="checkbox"/>	SCIM	Active

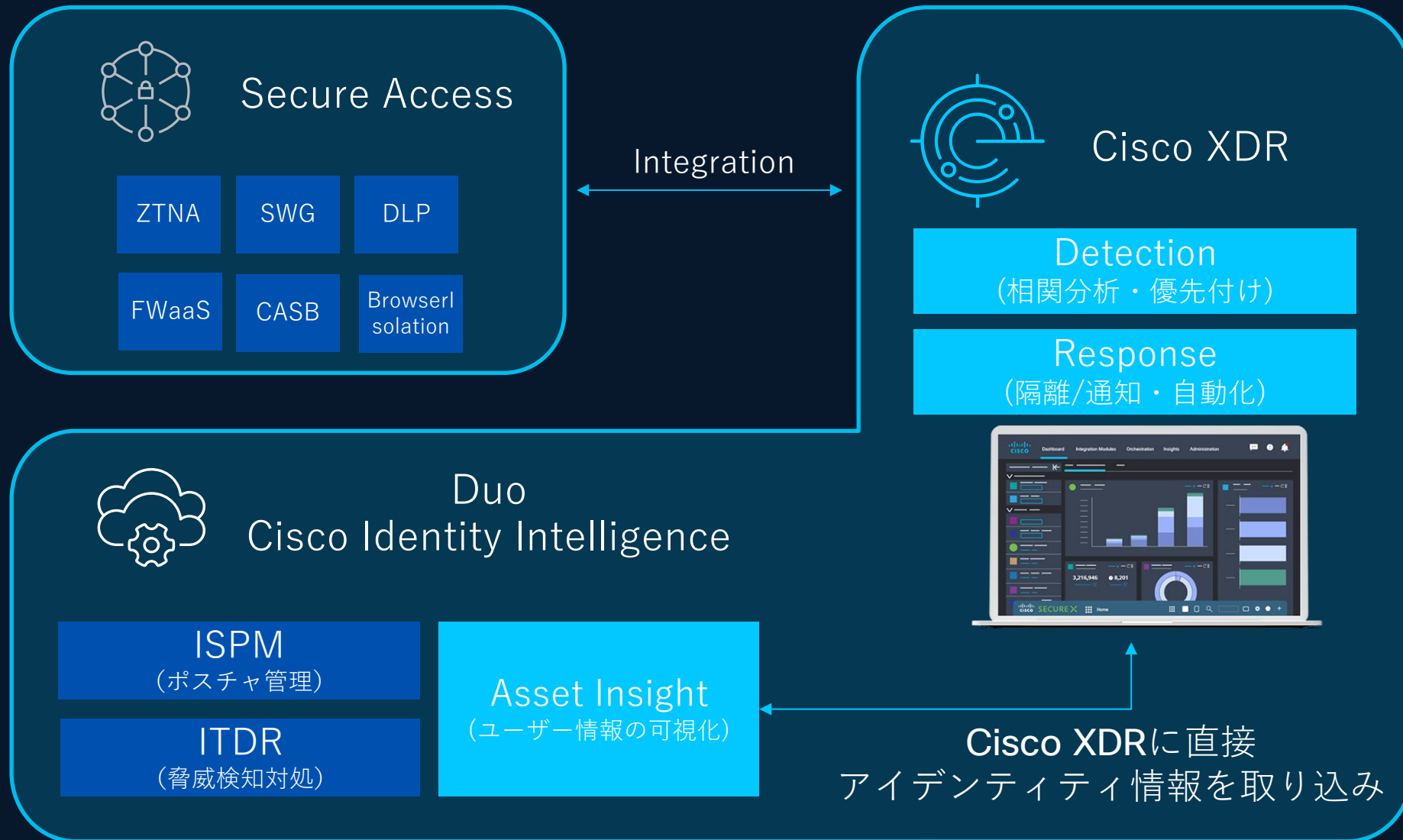
# Demo

# Cisco Identity Intelligence



# Cisco XDR - Cisco Identity Intelligence (CII) 連携

Released



# Splunk - Cisco Identity Intelligence (CII) 連携

Released

splunk>cloud

Apps

15 Messages

Settings

Activity

Find

Mission Control

Analytics

Security content

Configure

Search

Start investigation

FINDING

24 hour risk threshold exceeded for user=fyodor@splunkshirtcompany.com

Risk Threshold Exceeded for an object over a 24 hour period

Owner

unassigned

Status

New

Urgency

Informational

Sensitivity

Unassigned

Disposition

Undetermined

Time

Apr 16th, 2025 11:22 PM

Last updated

Apr 16th, 2025 11:22 PM

Reference ID

299f20c1-53e5-4216-9dc2-ddc7d8146734@@notable@@299f20c153e542169dc2ddc7d8146734

Detection

Cisco CII - Multiple failed checks from single user - Rule Audit - Possible Brute Force Activity - Rule ESCU - Malicious PowerShell Process - Encoded Command Demo - Rule

All entities

fyodor@splunkshirtcompany.com

Detection name

Cisco CII - Multiple failed checks from single user - Rule

Audit - Possible Brute Force Activity - Rule

ESCU - Malicious PowerShell Process - Encoded Command Demo - Rule

Entity

fyodor@splunkshirtcompany.com

Entity type

user

Intermediate findings

334

MITRE

T1021

T1030

T1059.001

Show more

Risk score

19460

Analyst queue

Search findings & investigations

Last 24 hours

Saved Views

Select...

Time Range: Last 24 hours

Clear All

Save

Apply

Zoom To Selection

Zoom Out

Deselect

Findings and investigations 633

Last refresh at 11:27 PM

Auto-refresh off

20 per page

	Title	ID	Type	Entity	Ris...
<input type="checkbox"/>	24 hour risk threshold exceeded for user=shaun.stuart@splunkshirtcompany.com		FINDING	shaun.stuart@...	1040
<input type="checkbox"/>	24 hour risk threshold exceeded for user=mickey.perre@splunkshirtcompany.com		FINDING	mickey.perre...	1040
<input type="checkbox"/>	24 hour risk threshold exceeded for user=Varsha.Mahadevan@splunkshirtcompany.com		FINDING	Varsha.Mahad...	1040
<input type="checkbox"/>	24 hour risk threshold exceeded for user=Hayley.Jensen@splunkshirtcompany.com		FINDING	Hayley.Jensen...	1040
<input type="checkbox"/>	24 hour risk threshold exceeded for system=58.96.44.0		FINDING	58.96.44.0	1040
<input type="checkbox"/>	24 hour risk threshold exceeded for user=fyodor@splunkshirtcompany.com		FINDING	fyodor@splun...	19460
<input type="checkbox"/>	Geographically Improbable Access Detected For shaun.stuart@splunkshirtcompany.com		FINDING	--	2420
<input type="checkbox"/>	Geographically Improbable Access Detected For fyodor@splunkshirtcompany.com		FINDING	--	1985

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Security

Cisco Security Summit Tokyo 2025

CISCO

Cisco Public

# Secure Access – Cisco Identity Intelligence (CII) 連携

PRIVATE  
PREVIEW

Secure Access の利用ユーザーにリスクがある場合にフラグを立てる

## User Risks

ディレクトリから Secure Access に同期されたユーザーは、CII によって発見された脅威に関連するコンテキストを持つ

The screenshot displays the Cisco Secure Access interface. On the left, a sidebar contains navigation icons for Home, Experience Insights, Connect, Resources, Secure, Monitor, Admin, and Workflows. The main content area is titled 'Users and User Groups' and includes a 'Users' tab. Below this, a table lists users with columns for Name, Email, Source, Directory, Trust Level, and Connected(VPN). The user 'Josh Green' is highlighted, with a 'Trust Level' of 'Neutral'. An orange box highlights the 'Trust Level' column header and the 'Neutral' status for Josh Green. To the right, a 'User Details' panel is open, showing general information (Name: Josh Green, Email: jgreen@securitydemo.net, Identity Provider: /azure-ad/scimv2) and a 'Trust Level' section. The 'Trust Level' section shows a status of 'Neutral' and a 'Last updated' timestamp of 'Feb 04 2025 5:11:49 PM UTC'. Below this, it lists factors for the risk level: 'SpecialAccount' and 'ResurrectedAccount', with a sub-point '1. access-from-dormant-account'. The 'Groups' section shows 'Cisco-Global-Admins', 'LabUsers', and 'oort\_admins'.

Name	Email	Source	Directory	Trust Level	Connected(VPN)
Josh Green	jgreen@securitydemo.net	azure	Azure	Neutral	0

**Trust Level**  
Last updated: Feb 04 2025 5:11:49 PM UTC  
The level changed to **Neutral** because of the following factors:  
• SpecialAccount  
• ResurrectedAccount  
1. access-from-dormant-account

Cisco Identity IntelligenceのTrust Levelが  
Secure Accessで将来的に利用可能に

Timing: In Private Preview now

# Secure Access – Cisco Identity Intelligence (CII)

FUTURE

リスクがあるユーザーアクセスを動的に制御 ※Phase2での対応予定

## Trust Levels

Secure Access は、  
各ユーザーの信頼レベル  
(Trust Level) により  
アクセスポリシーを制御

**User Trust Profiles**  
User trust profiles adaptively modify authentication and security based on trust levels—untrusted, neutral, trusted—incorporated into access rules, powered by Cisco Identity Intelligence. [Help](#)

**Trust levels**

1 profile  
Define authentication and security conditions for users based on their user trust level. Profiles can be auto-applied to access rules by linking to a resource.

Search: 1 profile

Profile name	Assigned to	Used in
System-provided Default for private access policy rules ⓘ	All private resources	0 rules

Trust level	Authentication controls	Security Controls
Trusted	Single Sign On	IPS: Connectivity Over Security
Neutral	Reauthenticate Every 24hrs	IPS: Security Over Connectivity Geolocation: US only
Untrusted	Block	-

**Trusted**  
Settings for Trusted user trust level

**Authentication controls**  
Type of authentication required for user to access the resource.

**Authentication Options**  
Single Sign On (SSO) [checked]  
Step up authentication  
Duo (Most secure)  
Block

**IPS Profile** Enabled  
IPS Profile enabled based on User Trust Level

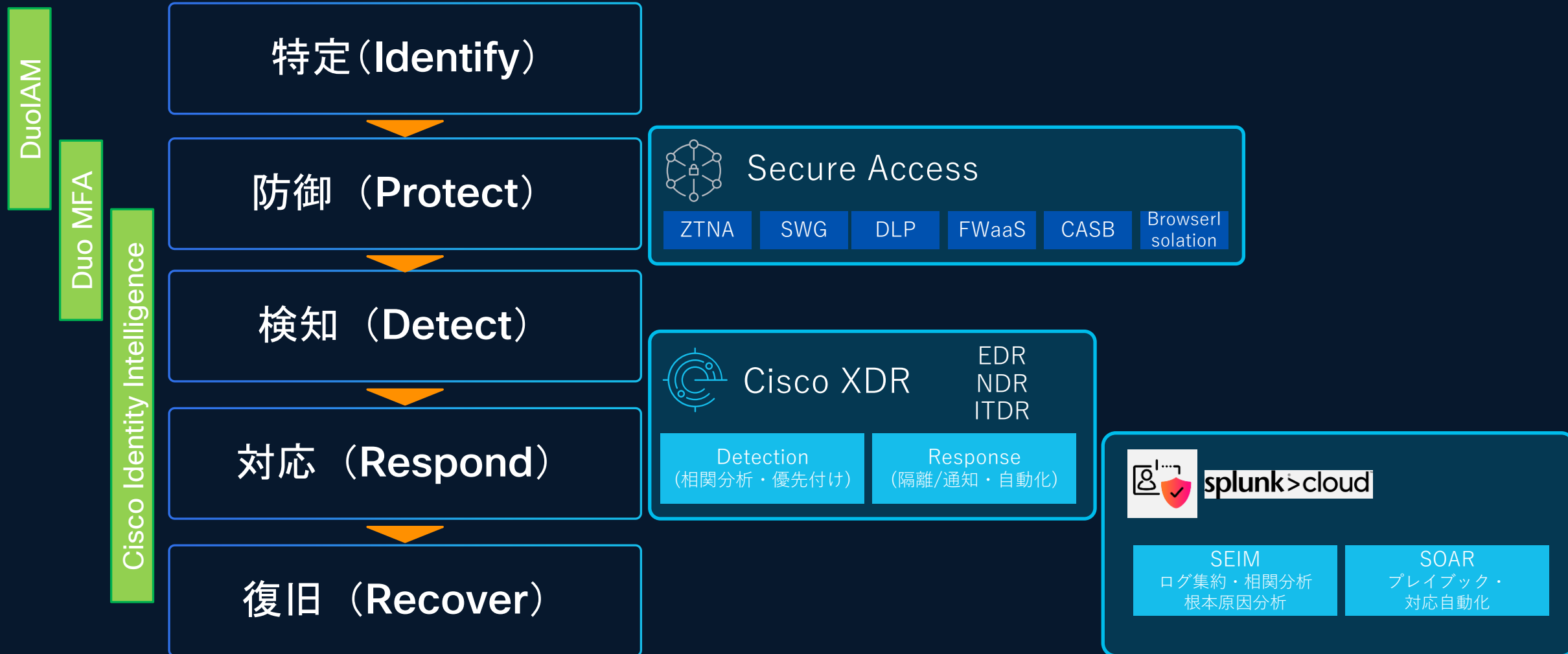
**IPS Profiles**  
Connectivity Over Security

**Geolocation** Enabled

**Cisco Identity IntelligenceのTrust Levelが  
Secure Accessで将来的に利用可能に**



# Cisco Identity Intelligence (CII) のCisco製品連携



# Cisco Duo 最新UPDATE

Cisco Duoが提供する新しい IAM (Identity & Access Management) 機能

NEW

セキュリティFirstのIAM

導入時点で守られている

NEW

End to Endで  
フィッシング耐性のMFA

完全にフィッシングの  
可能性を排除

統合  
Identity Intelligence  
(ITDR)

継続的に信頼を検証する

世界レベルのユーザエクスペリエンスをエンドユーザーと管理者に  
攻撃者を困らせ, ユーザが使いやすい

# 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

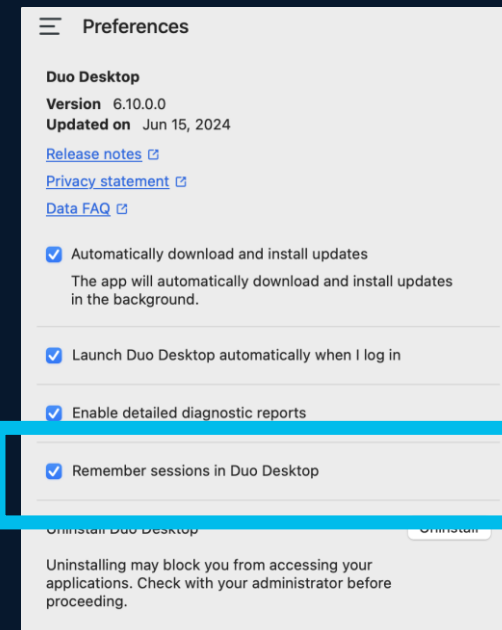
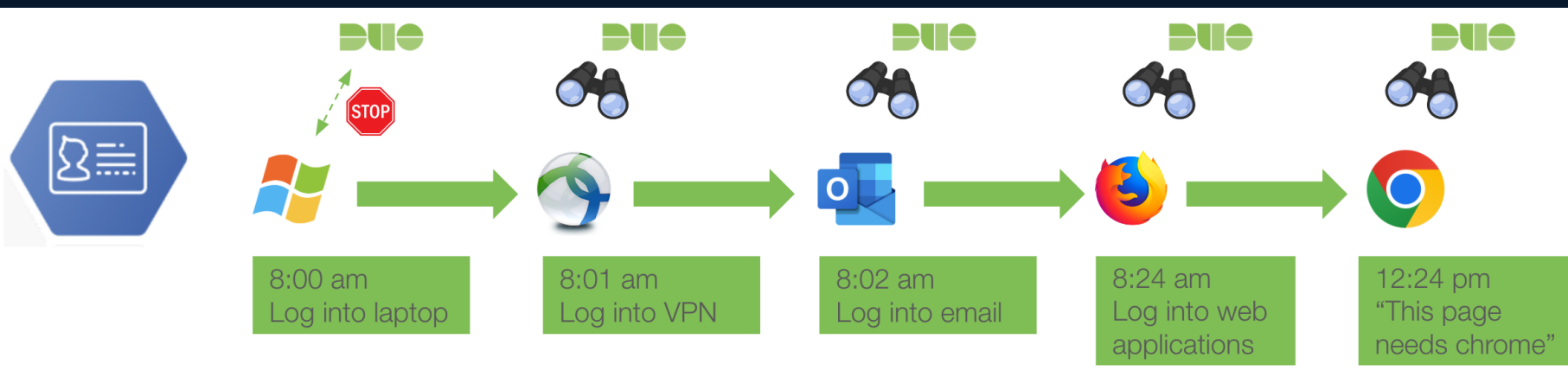
PC ログオン

VPN接続

メール参照

Webアプリ1

Webアプリ2

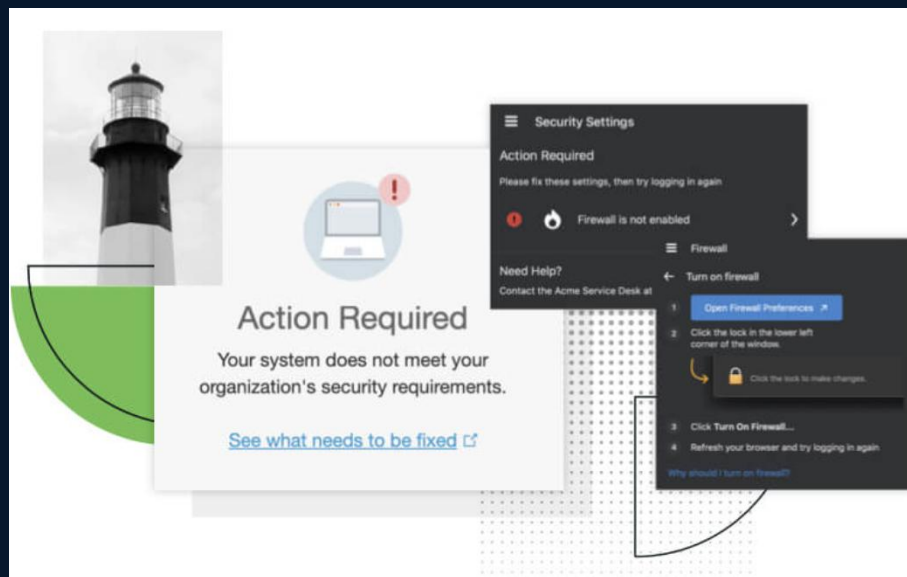


セッションをDuo Desktop  
にて保管して実現  
危険な状態になった場合に  
すぐにセッション削除

# Self-remediation & instant restore

## ユーザ自身がデバイスの自己修復・自己管理可能

### ユーザーによる自己修復を強く推進



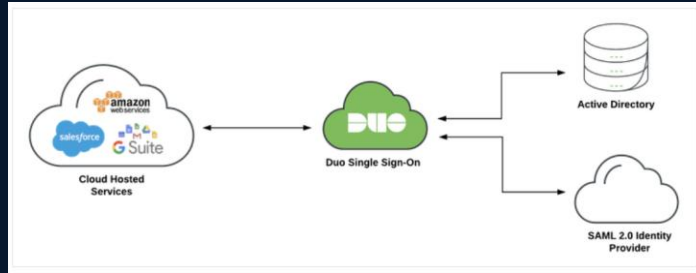
### ユーザーによる簡単デバイス管理



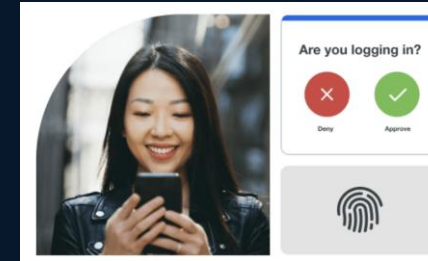
デバイス環境変更時に、エンドユーザーと管理者業務を大幅に削減可能

# シンプルな設計と構成で短期間で導入

## シンプルな設計と構成



## 創業当時から追求するユーザーエクスペリエンス



### ビデオの概要

**Duo シングル サインオンを構成する**

必要な役割: オーナー

1 Duo 管理パネルにログインし、「アプリ」

2 「認証ソースの追加」ページで、認証ソースを使用するオプションの下部にあるボタンを

**認証ソースを設定する**

必要な役割: 所有者、管理者、またはアプリケーション マネージャー

Duo シングル サインオンを使用すると、**Active Directory (AD)** ドメインとフォレスト、または**SAML ID プロバイダー**を単一要素認証ソースとして使用できます。

環境内で複数の AD および SAML 認証ソースを使用している場合は、**ルーティングルール**を使用して、ユーザーをアプリケーション アクセスの適切な認証ソースに誘導できます。

**アクティブディレクトリ**

以下の手順に従って、オンプレミスの認証プロキシをまずDuoシングルサインオンに接続できるように設定してください。次に、認証プロキシを介してActive Directoryドメインコントローラーと通信するようにDuoシングルサインオンを設定してください。

**AD認証の計画**

初めてActive Directoryを設定する場合、「」して同意するよう求められます。追加のAI再度表示されません。

<https://duo.com/docs/sso#overview>

アプリケーションへのDuo構成を全てわかりやすいガイダンスや動画で解説。機能開発と同時にガイダンスも更新。  
→常に最新の環境とともに最新のドキュメントを提供

**認証ログ画面**

イベント発生時、即時ログに反映される！

**Duo Admin Panel**

Timestamp (JST)	Result	User	Application	Access Device	Authentication Method
04:32:27 2022年2月24日	❌ Denied Endpoint is not healthy	duodemo	Duo Central	Windows 10, version 21H1 (19043.1466) As reported by Device Health Hostname: DESKTOP-LT4P291 Chrome: 97.0.4692.99 Flash: Not installed Java: Not installed Device Health Application: Installed Firewall: ❌ Off Encryption: On Password: Set Security Agents: Running: Windows Defender Minatomirai, 14, Japan 218.221.174.253 Trusted Endpoint: determined by Device Health	Unknown

**ユーザ画面**

ファイアウォールがオフになっています

ユーザで何が問題なのか把握できる

管理者は簡単に問題点を把握できる

1つのエントリーでアクセスデバイスの状態(バージョン、ビルド番号、セキュリティチェック、ロケーション)を確認することができます。

エンドユーザにわかりやすく、管理者が管理しやすい構成のため、双方にとって高い可視性を提供  
→全てのDuoユーザに最高のユーザーエクスペリエンス

# 直感的で強力なポリシーエンジン

最も単純な方法でアプリケーション別のポリシーを設定可能



## ベースが認証Deny→許可設定のみ

### Group policies

**O365** Edit | Replace | Unassign

This policy applies to 1 group: **Staff**

- Authentication policy** (Enabled) Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.
- User location** (Enabled) No action: United States. All other countries: Deny access.
- Operating systems** (Enabled) **MacOS, Windows**

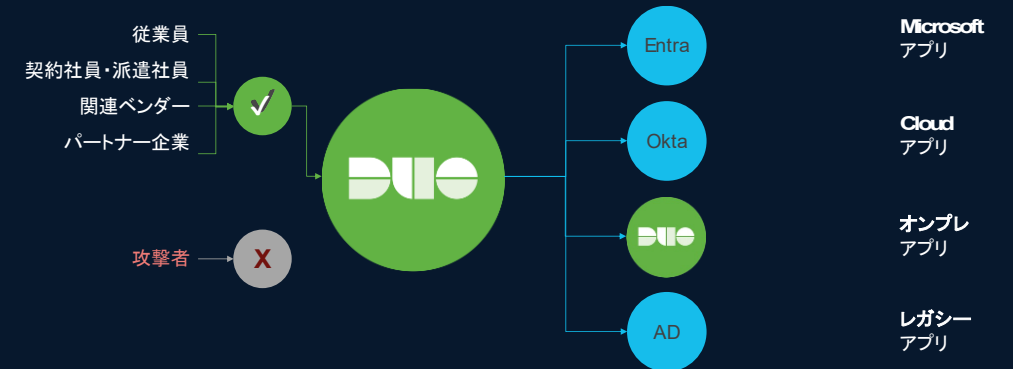
### Global Policy

This policy always applies to all applications.

- New User policy** (Enabled) Prompt unenrolled users to enroll whenever possible.
- Authentication policy** Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.

Duoでのポリシー設計はアプリケーションごとに上記の設定のみ  
(White List型のポリシー設定→許可のみをユーザ、デバイス、ロケーション別に登録が必要)  
複数のアプリケーションに対するポリシー設計が容易

どのような環境でも最小の工数で設定可能



お客様の環境に適合するため、  
最も少ない数のポリシーで強力なポリシーを設定可能  
設定期間、設定工数を大幅に削減。

※アプリケーション別、グループ別のポリシーを簡単に  
設定可能

# 導入当初から使えるAIアシスタント (Private Preview)

USにてGA済→APJC準備  
中

- Duoの設定方法を単純化して、アシスト

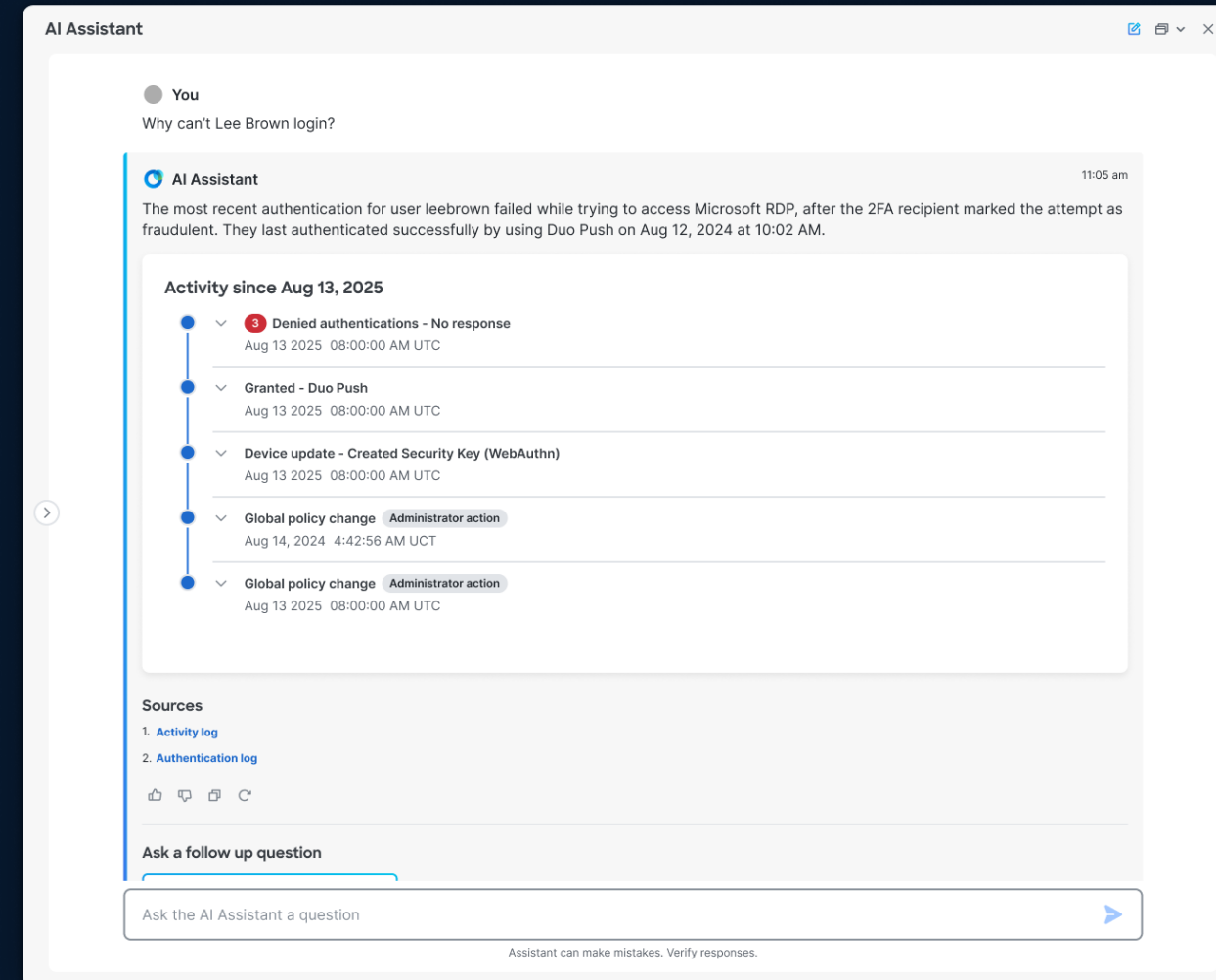
“How do I set group policy?”

→グループポリシーの設定方法をAIが単純化して管理者をアシスト

- ユーザの調査を容易に

“Why is Lee blocked?”

→ユーザの認証がなぜブロックされたのかをAIが調査して必要な情報を表示します



Duo の AI Assistant は、シームレスに認証ログ、デバイスのデータ、管理者の行動ログ、Duoのドキュメント及びナレッジベース(KB)を検索することができます。



# Pricing & Packaging

## Duo Essentials

シンプルで効果的なツールを導入し、従業員のアイデンティティ境界を保護

\$3 | User | Month

- Duo Directory
- Complete Passwordless
- Proximity Verification
- AI Assistant
- Multi-Factor authentication
- Single Sign-On
- Trusted Endpoints
- Unlimited applications

## Duo Advantage

ログイン前、ログイン中、ログイン後に機能する継続的なアイデンティティ・セキュリティへのアップグレード

\$6 | User | Month

- Duo Passport
  - Session Protection
- Cisco Identity Intelligence
- Adaptive authentication
- Risk-based authentication

## Duo Premier

クラウド、オンプレミス、プライベートのアプリケーションやリソースへの保護と容易なアクセスを拡大

\$9 | User | Month

- Secure VPN-less remote access
- 3rd party EDR agent check

# 現時点で可能な短期かつ実行的対策

技術対策

多要素認証の徹底

ディープフェイク検出ツール導入

迅速検知

多層ログと相関分析の導入

サプライチェーン監視

外部連携点の異常検出ルール化

ユーザ教育

AI生成メッセージの見分け方を周知

# 現時点で可能な短期かつ実行的対策

技術対策



強度の高い多要素認証

迅速検知



脅威を迅速に検知可能なITDR

サプライチェーン監視

外部連携点の異常検出ルール化

ユーザ教育

AI生成メッセージの見分け方を周知

