

AI時代のCiscoが考える Identity Security

Cisco Duo が実現する、安全な AI 活用環境



秦 寛樹

シスコシステムズ合同会社 セキュリティ事業 Identity Security 担当

稲澤 敏

シスコシステムズ合同会社 セキュリティ事業 Identity Security 担当SE

本日お持ち帰りいただきたい3つのこと

1. AI Agent は NHI を束ねて使う。守る対象は NHI そのもの

「AI Agent 対策」の実体は非人間アイデンティティの統制。ここを外すとツールを入れても効かない

2. 順番が命 : Discover → Assess → Enforce → Govern

可視化 → 評価 → 制御 → 統制。この順番を飛ばすと抜け漏れが生じやすい

3. 最初の一步は「棚卸し」。すぐに着手できる

社内に何本の資格情報が生きているか。即答できないところが出発点

認証しているのは、人だけではない

NHI（Non-Human Identity）= 人以外のアクセス主体

分類	具体例	主な作成者
サービスアカウント	連携用アカウント、管理者用bot	IT／開発
鍵・資格情報	APIキー、client secret、証明書	開発
SaaS間連携	OAuthアプリ、コネクタ	業務部門
自動化	RPA、バッチ、スクリプト	業務部門／IT
開発基盤	CI/CD、デプロイ用トークン	開発
ワークロード	コンテナ、サーバレス関数	開発
AI Agent	Copilot、Custom GPTs、MCP接続	全員

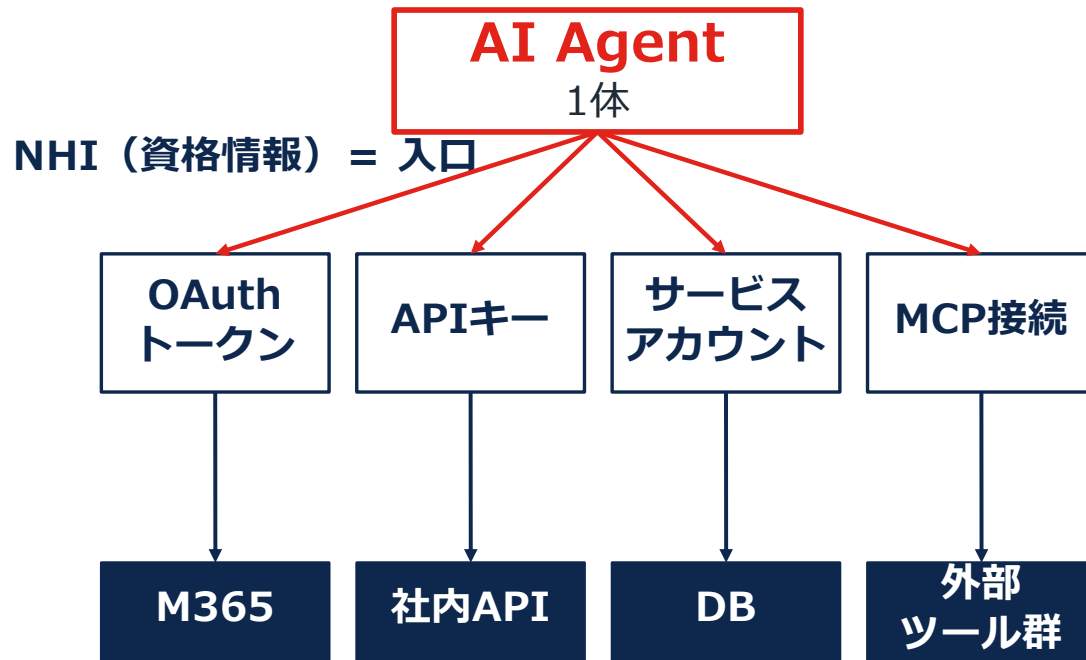
人間ID : NHI
1 : 45
平均的な企業

クラウドネイティブでは
144 : 1 以上

出典 : Cisco Duo (Rubrik Zero Labs 2025 を引用)

これまでは、作る人が IT／開発に限られ、用途も固定されていた。
いまは「全員」が申請なしで数分で作れて、用途も固定されない

AI Agent は NHI の一種ではなく、「NHI を束ねて使う主体」



Agent 1体 = 入口 4つ。Agent を止めても、
4本の NHI は有効なまま残る

この関係が生む3つの帰結

1 Agent の数 ≠ リスクの量。

数えるべきは NHI の本数と権限

2 Agent を止めても、NHI は残る。

資格情報は独立して生き続ける

3 NHI 側から見ると、

Agent が使っているか判別できない

人・従来 NHI・AI Agent を並べてみる

観点	人	従来 NHI	AI Agent
認証手段	MFA・パスキー	鍵・トークン	鍵・トークン（従来NHIと同じ）
行動	判断する	決められたことをする	自分で判断する
予測可能性	中	高（挙動が固定）	低（入力次第）
アクセス先	職務範囲	事前に定義済み	実行時に決まる／広がる
騙されるか	○ フィッシング（訓練で耐性）	× 騙せない	○ 言葉で騙せる。疑わない
作った人	人事プロセス	IT／開発	全社員
止め方	退職処理	鍵の失効	止める対象の特定が困難

青字：従来 NHI = AI Agent（認証の器） 赤字：人 ≡ AI Agent（振る舞い）

認証の器は従来NHI。振る舞いは人に近い。

鍵の管理だけでは振る舞いを見られない。MFA も適用しにくい

同じ経路を、人と Agent が通ると

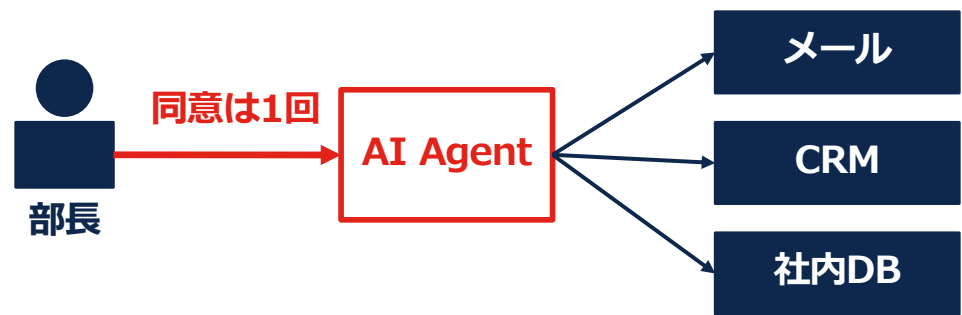


ポリシーが空振り：24時間どこからでも動くので「業務時間内のみ」などの条件が効かない

ログに差が出ない：「検査をスキップした」というログは、通常どこにも出ない

関門は開いたまま。しかも、開いていることに気づきにくい

委任という構造



権限は継承される。
監督は継承されない。

同意は一度きり。以降、確認は来ない。毎回の動作も見えていない

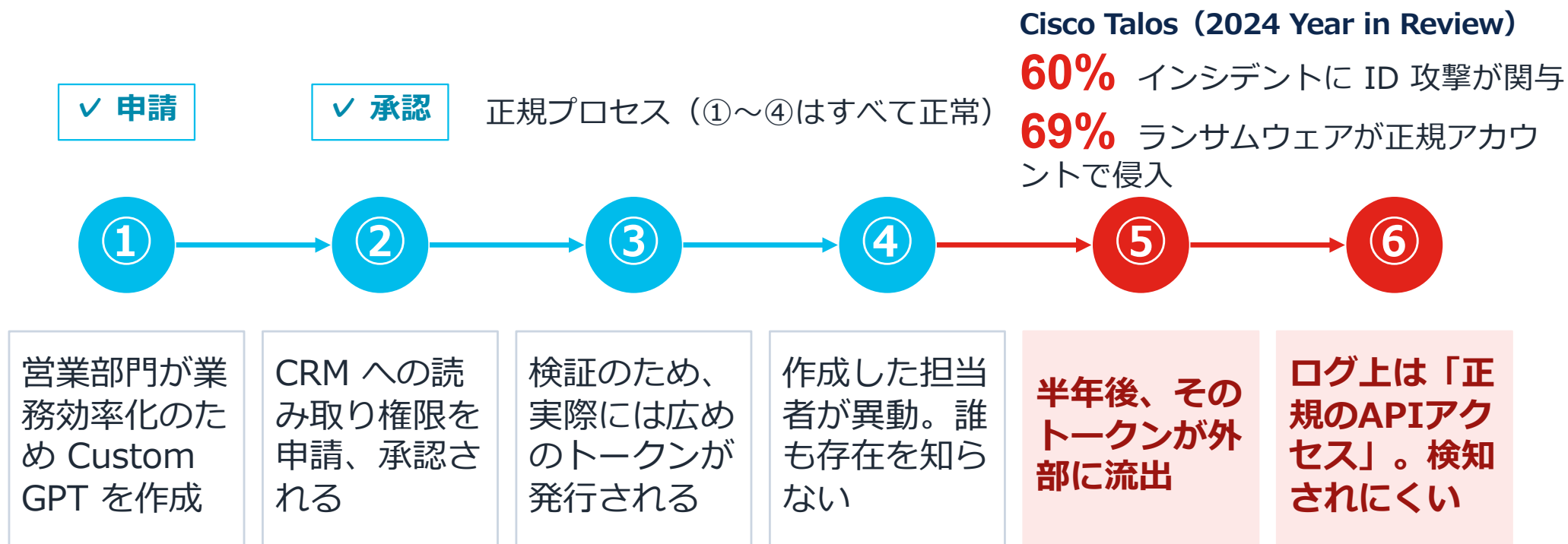
以降の経路に、人はいない（部長の権限で動き続ける）

あわせて注意：権限の"増幅"

	委任権限	アプリケーション権限
範囲	同意した本人のみ	テナント全体
例	「部長のメールを読む」	「全社員のメールを読む」
選ばれる理由	—	自動化のため。人の不在時も動かす

トークンは文字列。1本の漏えいが、全社分の漏えいにつながり得る

こうして事故は起きる（想定シナリオ）

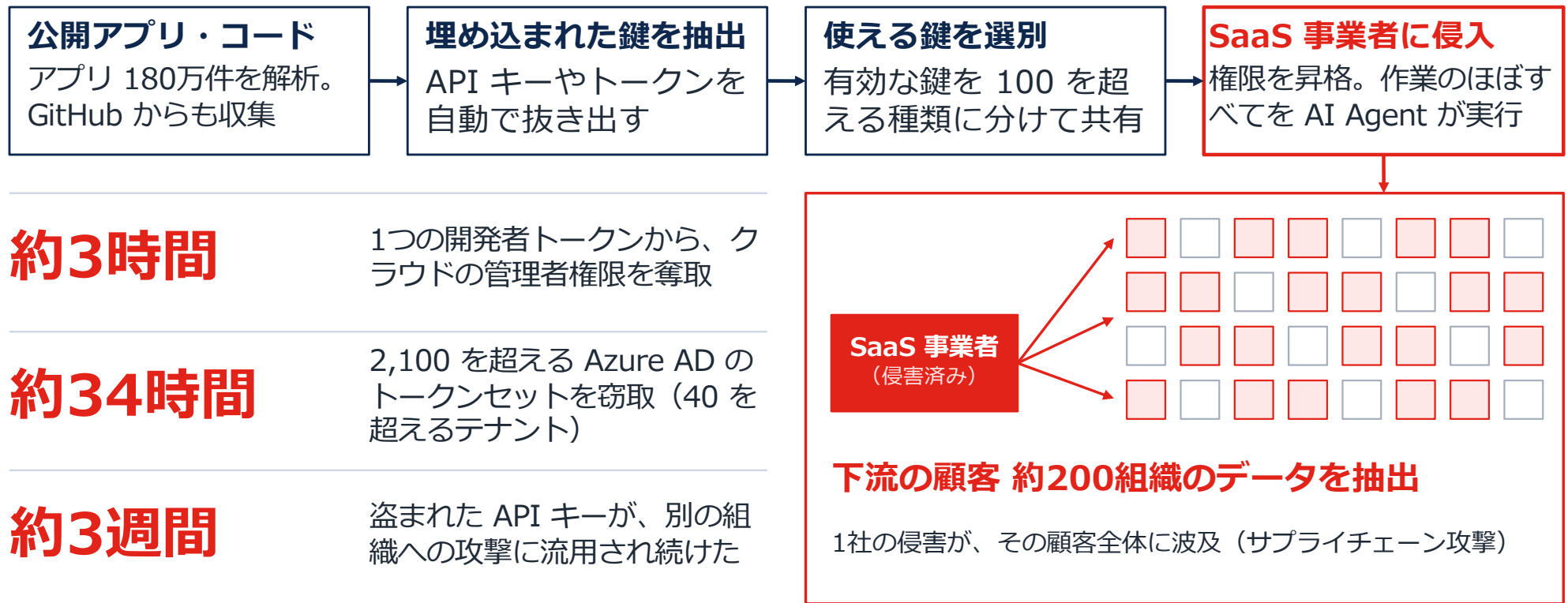


悪意ある人物は登場しない。

全員が善意で、申請も承認も通っている。攻撃者は侵入する必要がない

アプリに埋め込まれた「鍵」から、取引先の顧客へ波及

実例：Anthropic 社の脅威レポート（2026年9月）より



狙われたのは人のパスワードではなく、アプリや開発環境に置かれた「鍵」、つまり NHI

出典：Anthropic「Detecting and countering misuse of AI: September 2026」（2026年9月10日公開）p.11-14

NHI ごとに「責任を取る人」を決める

「所有者」「管理者」の意味は会社ごとに違う。大事なのは、次の3つに答えられる人がいるか

1 何のために使っているか

2 権限は今も適切か

3 不要になったら、誰が止めると決めるか

責任者が決まっている

人に紐づく NHI 作った人が責任者
例：個人の API キー、Custom GPT

人に紐づかない NHI チーム・担当者を責任者に指名
例：連携用アカウント、バッチ、CI/CD

責任者がいない

作った人が退職・異動済み
用途が分からない
アプリに埋め込まれたままの鍵

最優先。責任者を決めるか、止める

人に紐づかない NHI も、責任を取る人は決められる

ここからは、Cisco の Identity Security

ここまで AI Agent と NHI は、人のために作った関門をすり抜ける。しかも気づきにくい。

ここから **Cisco がこれをどう見つけ、どう管理するか**

- 1 全体像** 一つの製品 Cisco Duo で、人と NHI・AI Agent を扱う
- 2 既存環境との関係** IdP は置き換えない。レガシーやインフラともつなぐ
- 3 進め方と Agent Discovery** Discover → Assess → Enforce → Govern
- 4 デモと事例** 実際の画面と米国の導入事例

Cisco が描く AI 時代の Identity Security



Zero Trust for Agentic AI

Discover

Assess

Enforce

Govern

※ 機能の提供時期・エディションは別途ご確認ください

(参考) Cisco Duo とは

セキュリティを起点にした IAM。人の認証から NHI・AI Agent まで、一つの製品でできること

強い認証

なりすましを止める

フィッシングに強い MFA とパスワードレス。盗まれたパスワードだけでは入れない

MFA ・ Passwordless

アクセス管理

アクセスをまとめる

SSO とディレクトリで、Entra ID など既存の IdP ともつながる

Duo SSO ・ Duo Directory

デバイス信頼

危ない端末を入れない

管理下にあり、健全な端末だけにアクセスを許可する

Device Trust

可視化と脅威検知

ID のリスクを見える化

すべての ID を横断して、設定の不備や攻撃を検知する

Cisco Identity Intelligence

AI Agent ・ NHI

人以外の ID も管理する

NHI と AI Agent を見つけ、責任者と権限を明らかにする

Agent Discovery

月間の認証回数

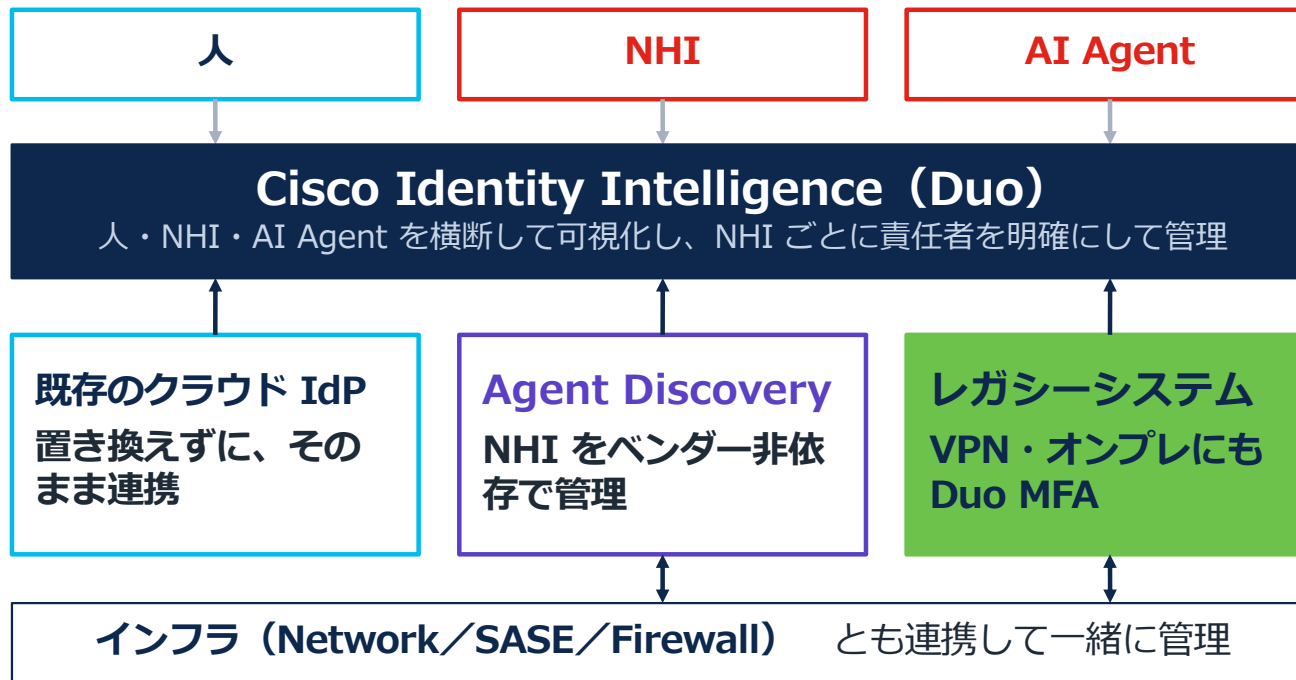
13億回

既存の IdP を置き換えずに、その上に重ねて使える

出典：duo.com

IdP は置き換ええない。既存環境のまま、全体を見て・守る

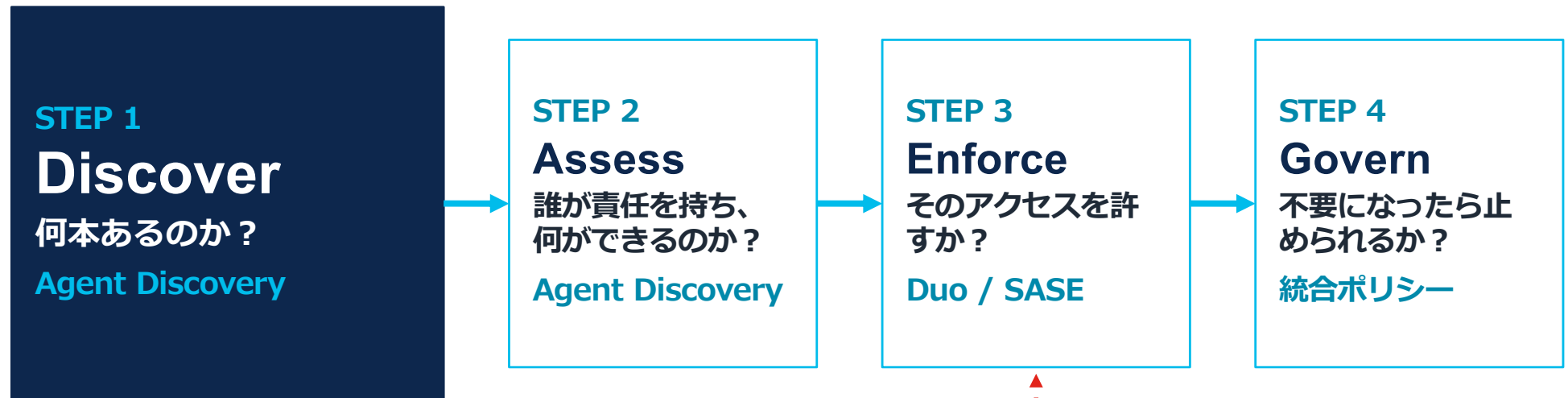
前提： IdP を Duo に入れ替える提案ではありません



- 1 置き換ええない**
既存の Entra ID 等を活かし、その上で全体を見る
- 2 ホワイトエリアを埋める**
IdP だけでは見えない NHI を管理する
- 3 取り残さない**
レガシーにも MFA を追加し、穴を減らす

既存環境のまま、人と NHI をインフラと一緒に管理する。これが **Cisco Identity Security**

Zero Trust for Agentic AI の4ステップ



ここが最重要



3から始める（制御から入る） = 失敗パターン

見えていないものは、野放しのまま残る

順番は飛ばせない。

Agent Discovery とは

社内の NHI・AI Agent を全部見つけて、リスク順に並べ、止めるところまで

Discovery & Governance

1. 発見と可視化

AI Agent と NHI を自動で洗い出し、責任者・権限・最終利用日を一覧にする

Access & Lifecycle

2. ライフサイクル管理

最小権限へ見直し、作成から廃止まで責任者を決めて管理する

Threat Detection & Response

3. 脅威の検知と対応

普段と違う接続や使われ方を検知し、すぐに対処する

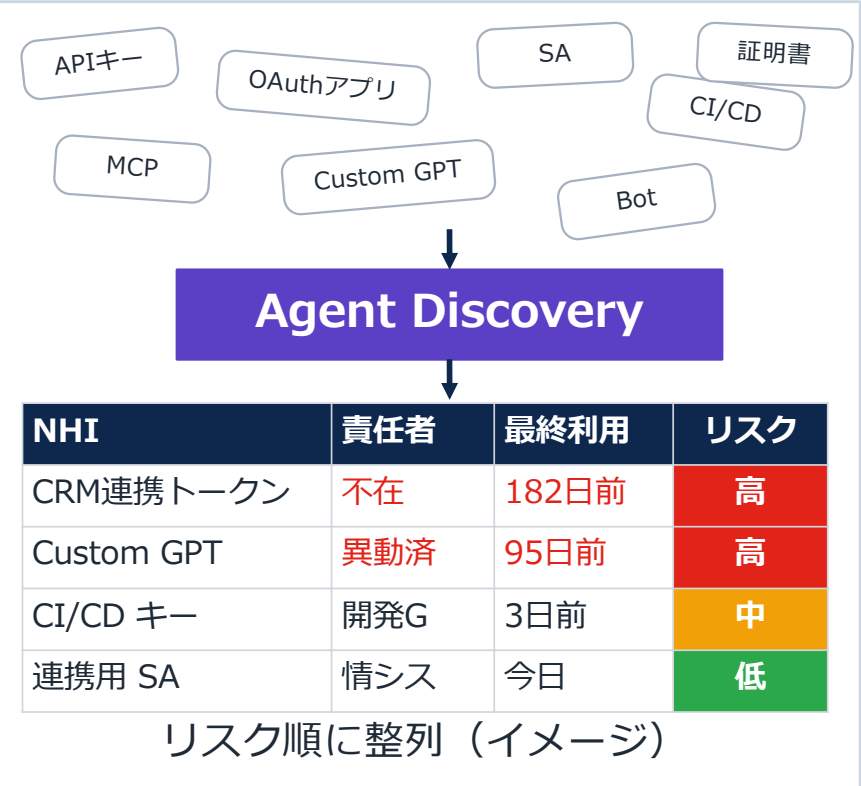
Secrets Management

4. シークレット管理

API キーやトークンを棚卸しし、漏えいや放置を防ぐ

エージェントレスで導入

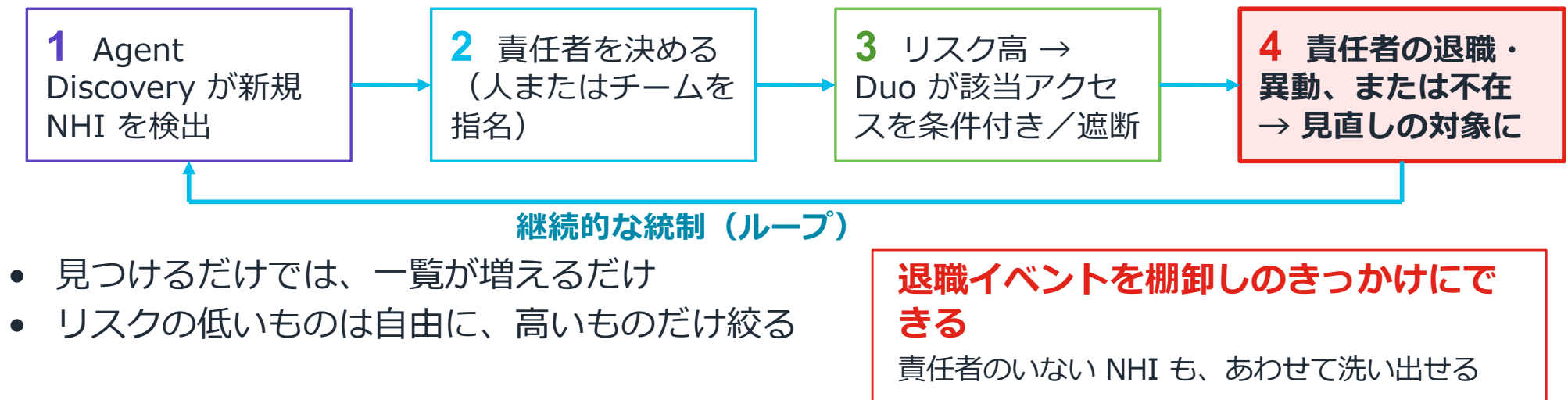
NHI 全体が対象



人と NHI を同じ土台で管理する価値

NHI だけを管理	人だけを管理	Cisco Duo で一緒に管理すると
見つかる	制御できる	見つけたものを制御につなげられる
リスクが分かる	ポリシーが打てる	リスクに応じたポリシーを適用できる
NHI が分かる	人が分かる	すべての NHI に責任者を決めて統制できる

具体的な動き



米国での導入事例 Mercury

フィンテック 2,000社を超えるスタートアップの財務業務を支援

課題	NHI がセキュリティの死角に 人の IAM は整っていたが、API キーや OAuth 連携は DevOps 任せ。NHI は 900 以上
取り組み	可視化と、現場を巻き込む統制 NHI を継続的に可視化。新しいアプリは導入前に権限を評価。利用部門が「なぜ必要か」を説明する仕組みに
成果	侵害時の対応が劇的に速く 外部 SaaS (Dropbox Sign) 侵害時、影響アカウントの特定と対処を 30 分で完了

インシデント対応の時間

数日



30分

NHI の数 : 900 以上

「人の IAM は確立しているが、非人間 ID は見落とされがちだ」
Branden Wagner, Head of Information Security

出典 : 公開されている顧客事例。日本では現時点で公開事例なし

まとめ

1. AI Agent は NHI を束ねて使う。守る対象は NHI そのもの

AI 以前からあった課題の延長線上にある

2. Discover → Assess → Enforce → Govern の順番を守る

まず見つける。次に評価する。それから制御する

3. 入口は棚卸し。90日を目安に運用へ

まず数えて、すべての NHI に責任者を決める

このあと、実際の画面でご覧いただきます → SE 稲澤

