Cisco Security Webinar

いますぐ始める Identity Security インシデント急増に備える Cisco Duo 実践対策

平岡　龍弘
Identity Security 担当

2026.10.27

インシデント動向

情報漏洩インシデントの「5大攻撃パターン」

① 境界VPN・露出管理機能の悪用	VPN機器の脆弱性突破に加え、インターネットに露出した社内管理画面やCMSの脆弱性を直接攻撃
② 委託先SaaSの連鎖侵害	自社が堅牢でも、利用中の問い合わせSaaSや保守会社が侵害され、複数顧客のDBが横串で窃取
③ Web API認可不備・A2B攻撃	アプリを解析してバックエンドAPIを特定し、認可制御の不備を突いて大量の会員データを自動スクレイピング
④ 仮想化基盤標的ランサムウェア	個別端末ではなく仮想化基盤（ハイパーバイザー）とオンラインバックアップを同時に暗号化し事業停止
⑤ 人的・運用ミス	サイバー攻撃を伴わない設定ミス（何年間も気づかれず放置）、非表示シート残存、外部生成AIへの誤入力

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Public

情報漏洩が多発する考察

背景①：攻撃側の「産業化」とAIによる効率化

分業化したRaaSエコシステム

開発者・侵入担当・交渉担当が分業し、技術のない犯罪者も参入可能に。Qilinは幹部拘束後もリークサイトへの掲載が続き、1人の逮捕では止まらない

生成AIによる攻撃の量産

偵察・フィッシング文面・脆弱性調査・マルウェア開発にAIが使われ、攻撃の速度と規模が拡大。侵入後の操作をAIエージェントが担ったとみられる事案も報告

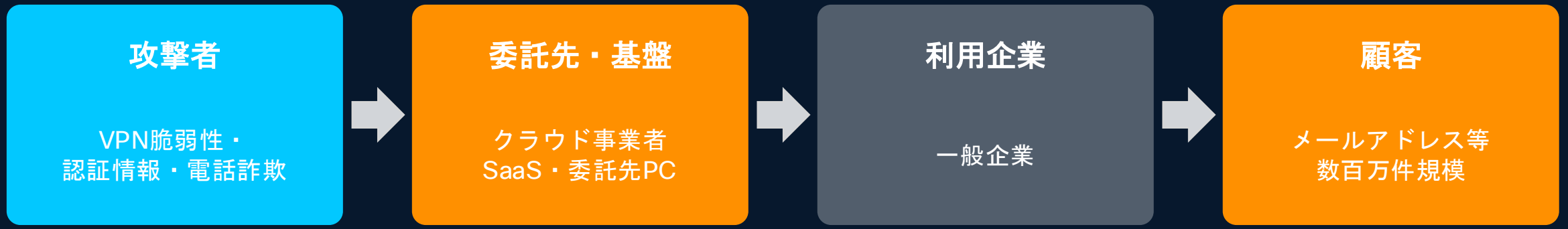
窃取データの換金ルート

本人確認画像・口座情報・認証情報は闇市場で売買され、二次被害（なりすまし・フィッシング）の原資になる。暗号化せず窃取だけで恐喝する手口も増加

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Public

背景②：委託とクラウドの多層化で「1社の侵害」が連鎖する



防御の境界が自社の外に広がった

- 海外調査でも第三者が関与する侵害は30%から48%に上昇
- 委託先管理アカウントのMFA未適用、委託先PC1台のマルウェア感染、古い連携トークンなどサプライチェーンの「最も弱い鍵」が狙われる
- 基盤側データ復元困難とし利用者バックアップからの再構築を案内した例
- クラウド任せの可用性・バックアップ設計の限界が露呈した

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Public

国が求める対策ポイント

国が求める対策ポイント



総務省
MIC Ministry of Internal Affairs and Communications

○ よく見られるページ　○ ご意見・ご提案　○ ENGLISH(TOP)

総務省の紹介 ⌄　報道・広報 ⌄　政策 ⌄　組織案内 ⌄　所管法令

総務省トップ > お知らせ > 不正アクセスによる情報漏えい等の事案を踏まえた対応について（注意喚起）

お知らせ

令和8年10月9日

不正アクセスによる情報漏えい等の事案を踏まえた対応について（注意喚起）

大量の個人情報を取り扱う事業者等の情報システムが不正アクセスにより侵入され、個人情報を含むデータが窃取される事案が相次いで確認されています。

このような状況を踏まえ、内閣官房国家サイバー統括室から、事業者等に対し、迅速な脆弱性対応や、多要素認証等の認証機能の強化、漏えいした情報の悪用を防止する対策等について、委託先も含めた一層の対策の徹底を速やかに検討するよう、注意喚起が行われています。

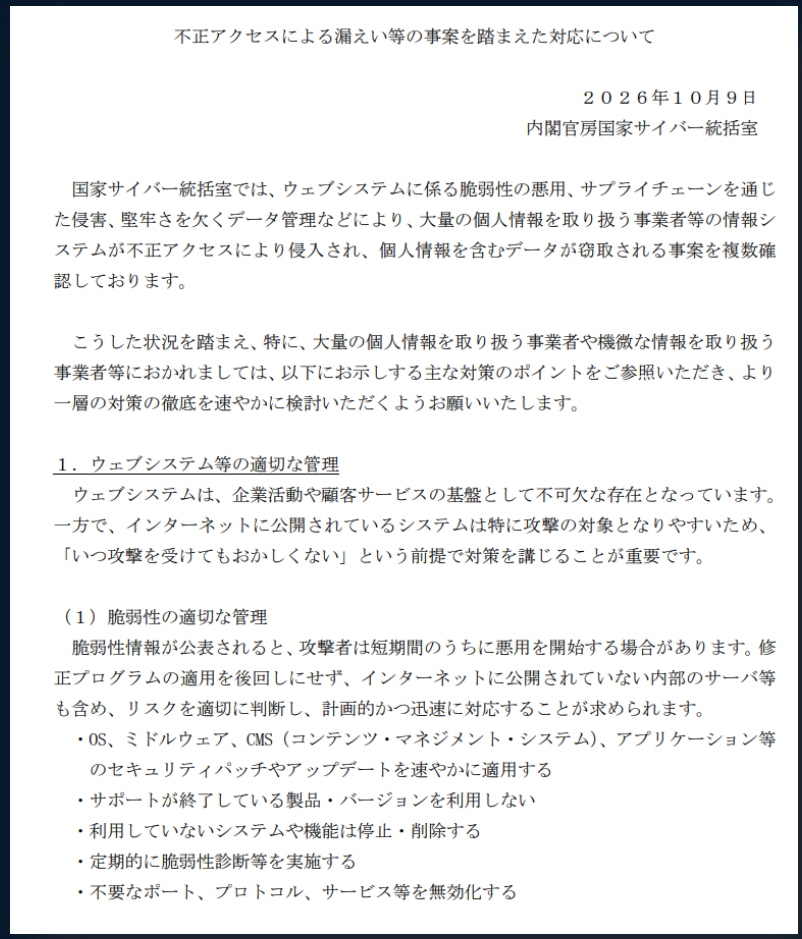
総務省においても、所管事業者及び関係団体に対し、同内容の注意喚起を行いました。事業者の皆様におかれましては、経営層のリーダーシップの下、サイバーセキュリティ対策の一層の強化に取り組んでいただくようお願いいたします。特に、大量の個人情報を保有する事業者や機微な情報を取り扱う事業者等におかれましては、十分に御注意ください。

○不正アクセスによる漏えい等の事案を踏まえた対応について（国家サイバー統括室）
https://www.cyber.go.jp/pdf/press/taiou.pdf

参考情報として、個人情報保護委員会及びJPCERT/CCによる注意喚起についても、以下のとおりお知らせします。

○大規模な漏えい等事案を踏まえた対応について（注意喚起）［個人情報保護委員会］
https://www.ppc.go.jp/news/press/2026/261007_houdou/

○直近で相次いでいる国内組織における不正アクセスに関する注意喚起［JPCERT/CC］
https://www.jpcert.or.jp/at/2026/at260030.html



不正アクセスによる漏えい等の事案を踏まえた対応について

２０２６年１０月９日
内閣官房国家サイバー統括室

国家サイバー統括室では、ウェブシステムに係る脆弱性の悪用、サプライチェーンを通じた侵害、堅牢さを欠くデータ管理などにより、大量の個人情報を取り扱う事業者等の情報システムが不正アクセスにより侵入され、個人情報を含むデータが窃取される事案を複数確認しております。

こうした状況を踏まえ、特に、大量の個人情報を取り扱う事業者や機微な情報を取り扱う事業者等におかれましては、以下にお示しする主な対策のポイントをご参照いただき、より一層の対策の徹底を速やかに検討いただくようお願いいたします。

１．ウェブシステム等の適切な管理

ウェブシステムは、企業活動や顧客サービスの基盤として不可欠な存在となっています。一方で、インターネットに公開されているシステムは特に攻撃の対象となりやすいため、「いつ攻撃を受けてもおかしくない」という前提で対策を講じることが重要です。

（１）脆弱性の適切な管理

脆弱性情報が公表されると、攻撃者は短期間のうちに悪用を開始する場合があります。修正プログラムの適用を後回しにせず、インターネットに公開されていない内部のサーバ等も含め、リスクを適切に判断し、計画的かつ迅速に対応することが求められます。

・OS、ミドルウェア、CMS（コンテンツ・マネジメント・システム）、アプリケーション等のセキュリティパッチやアップデートを速やかに適用する
・サポートが終了している製品・バージョンを利用しない
・利用していないシステムや機能は停止・削除する
・定期的に脆弱性診断等を実施する
・不要なポート、プロトコル、サービス等を無効化する

https://www.cyber.go.jp/pdf/press/taiou.pdf

© 2026 Cisco and/or its affiliates. All rights reserved.

国が求める対策ポイント

ウェブシステム等の適切な管理

1. 脆弱性の適切な管理
   インターネットに公開されていない内部のサーバ等も含める
2. アカウント管理・認証
   ・MFAを導入する
   ・アクセス権を必要最小限にする
   ・不要なアカウントを速やかに無効化する
3. レジリエンスの向上
   ・ログを適切に管理・保管する
   ・不正な通信やアクセスを監視する
   ・外部からの異常な認証試行を把握する

サプライチェーンを通じた侵害への対策

1. 委託先企業等のセキュリティ対策状況の把握
2. 委託契約におけるセキュリティ要件の明確化
3. 情報共有範囲の適正化
4. サプライチェーン全体のリスクマネジメント

データの適切な管理

1. 保有する情報資産の適切な管理
2. 保有情報の最小化
3. 適切なアカウント管理・アクセス制御
   ・業務上必要な者のみにアクセスを許可する
   ・閲覧権限と更新権限を適切に分離する
   ・管理者権限の付与を必要最小限とする
   ・定期的にアカウントや権限設定を確認する
4. データ保護の徹底
5. ログ取得・監視・分析の強化

https://www.cyber.go.jp/pdf/press/taiou.pdf

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Public

Cisco Duo

Duoによる Identity Security

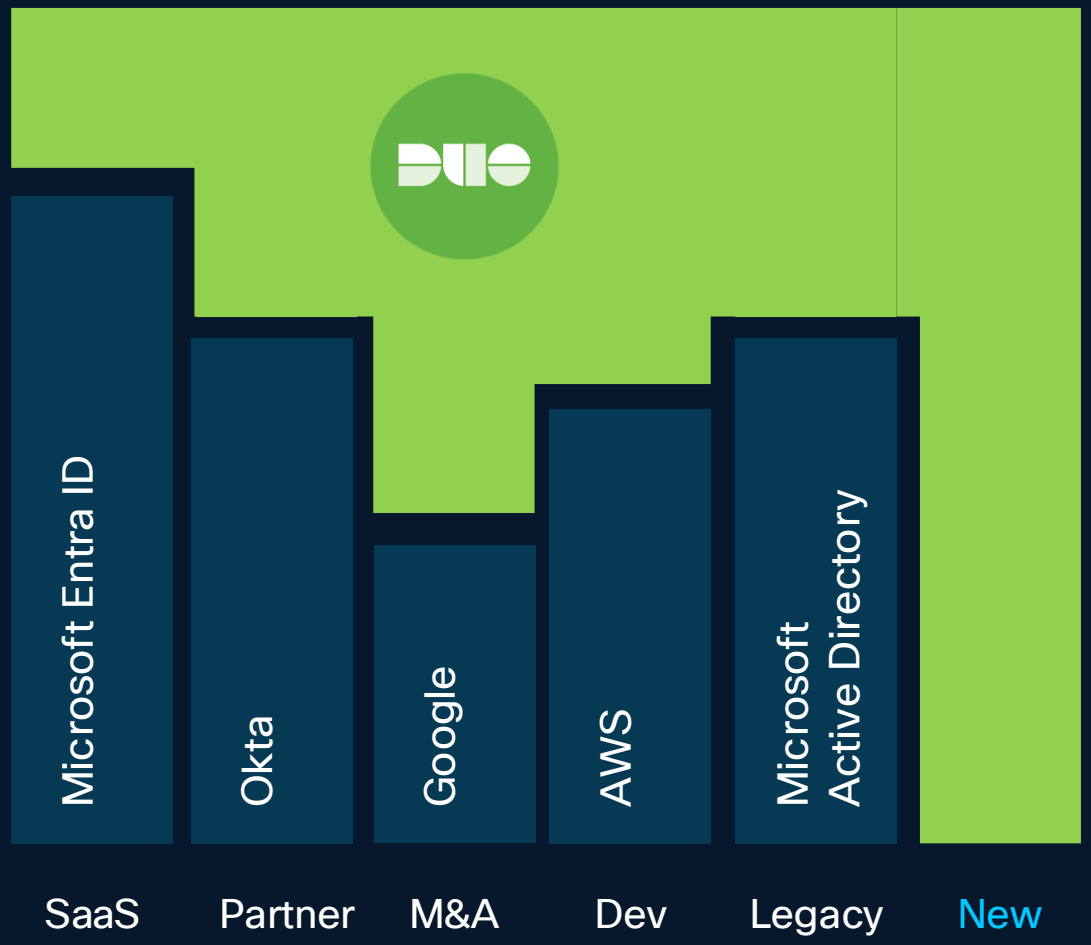
高い安全性

低いコスト

シンプルさ

© 2026 Cisco and/or its affiliates. All rights reserved.

DuoはIdentityのセキュリティにフォーカス



複雑なID環境へ強力なセキュリティを柔軟に安価に提供し、ギャップを埋める

ユーザーの快適性を損なわず、すべてのユーザーを守る

© 2026 Cisco and/or its affiliates. All rights reserved.

Gartnerのレポート



Gartner® Peer Insights™ 2026 Voice of the Customerのアクセスマネジメント領域で

Customers Choice に選出

https://www.gartner.com/doc/reprints?id=1-2NADO242&ct=260501&st=sb

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Duoが選ばれる理由

MFA・IAM・ITDRを統合した唯一のセキュリティファーストのIdentityプラットフォーム

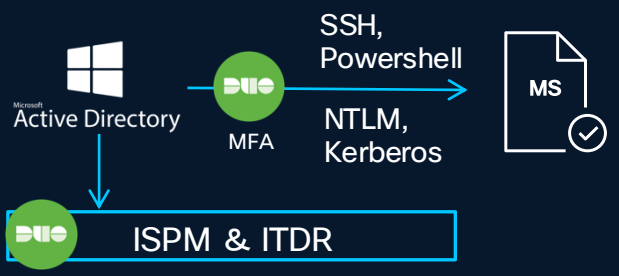
フィッシング対策MFA

組織に合わせた柔軟なMFA

パスワードレス
近接認証
モバイルApp
Desktop
SMS
電話

Active Directory保護

Active Directoryを標的とした攻撃を阻止



デバイスポスチャー

証明書に頼らない
安全なデバイスだけ認証を許可



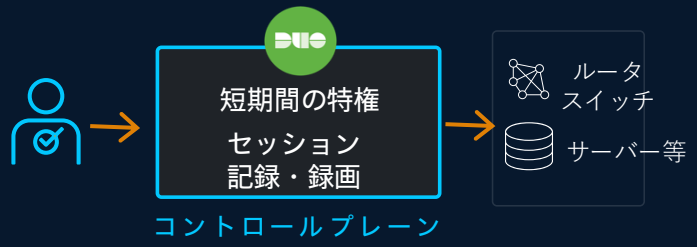
PCの可視化



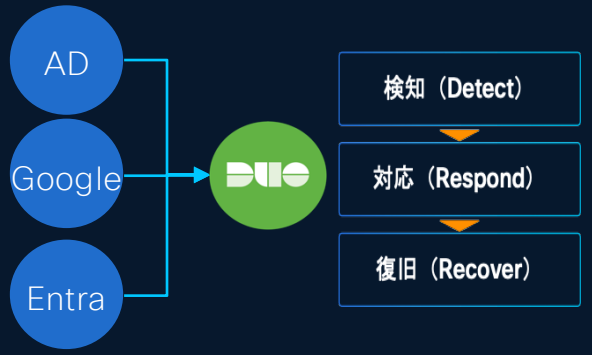
モバイルの可視化

特権インフラアクセス

管理者に必要なアクセス権を
必要なときだけ付与する



ISPM & ITDR



ISPM　アイデンティティの健全性管理



MFA未適用、休眠ID、過剰特権アカウント

ITDR アイデンティティの振る舞い検知



怪しい振る舞いのユーザーを即座に特定・隔離

© 2026 Cisco and/or its affiliates. All rights reserved.

フィッシング対策MFA

MFA強度の階層

フィッシング耐性や攻撃の難易度に基づくセキュリティレベルの分類

MFAなし

攻撃者の理想的なターゲット
極めて危険

侵入のリスク大

電話・SMS

SIMスワップや通信傍受に極めて弱い。自動音声の脆弱性。

傍受のリスク大

メール・OTP

メール乗っ取りや、偽サイトへの入力ミスを防げない。

通知(承認のみ)

内容を見ずに承認する「MFA疲労攻撃」に脆弱

疲労攻撃のリスク

通知(マッチング)

PC画面の数字をスマホで入力。
Duo推奨設定。

「うっかり承認」を物理的に防ぎ、ヒューマンエラーを大幅に低減

AiTMのリスク

近接認証

物理的な距離制限により遠隔攻撃を遮断。

パスワードレス

公開鍵暗号を使用。偽サイトでは認証不可。

フィッシング耐性MFA

規制当局によるフィッシング対策の推奨

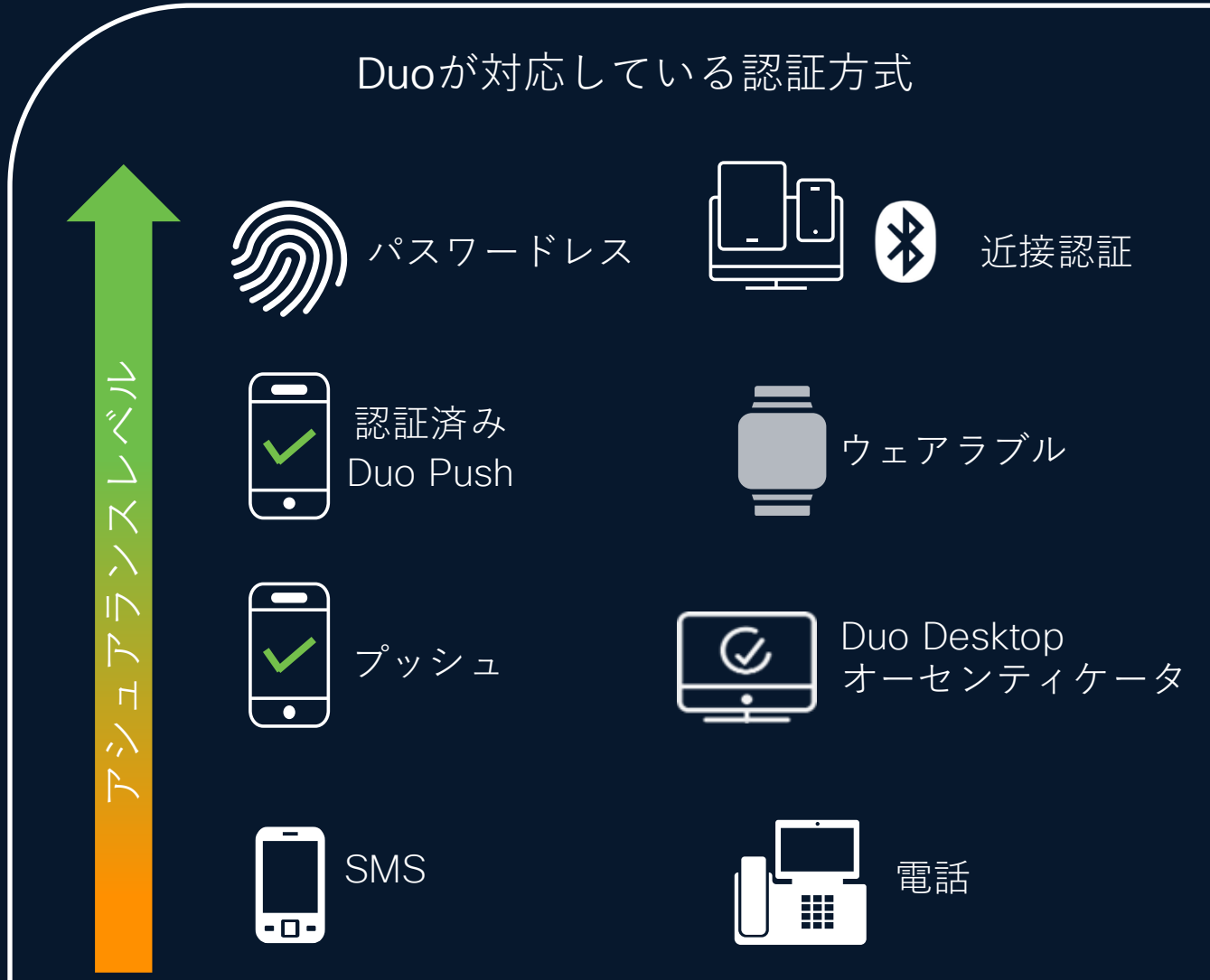
NIST AAL 1 | NIST AAL 2 | NIST AAL 3

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Public

環境に合わせた多様なMFA

- 業界をリードする多様な認証手段
- ユーザーまたはアプリケーショングループごとに柔軟な認証ポリシーが設定可能
- フィッシングに強いMFA とパスワードレスを簡単に導入
- ニーズに応じて、複数の要素やオフラインの認証手段を展開



© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Public

デバイストラスト

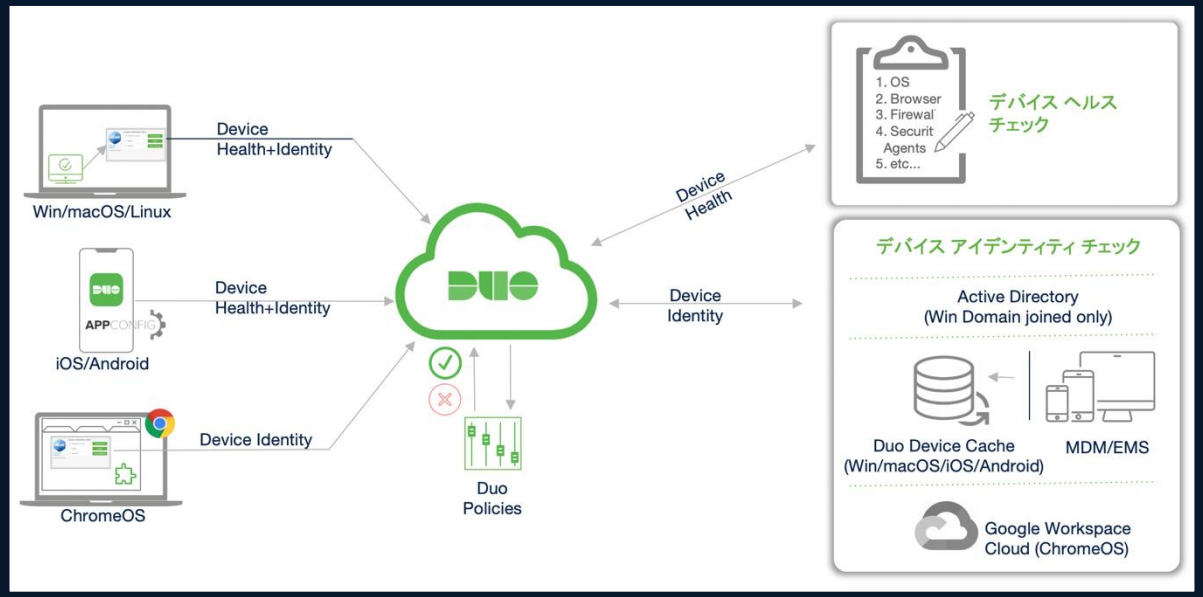
デバイストラスト　証明書に頼らないリアルタイムなデバイス認証

Device Health - デバイスのコンプライアンスチェック

- アクセス時にデバイスのセキュリティ情報を取得し、セキュリティ コンプライアンスチェックと検疫を実施
- OSバージョン（パッチ）、ブラウザバージョン、Firewallの状態、セキュリティエージェントの動作などを検査

Trusted Endpoint - デバイス認証 -

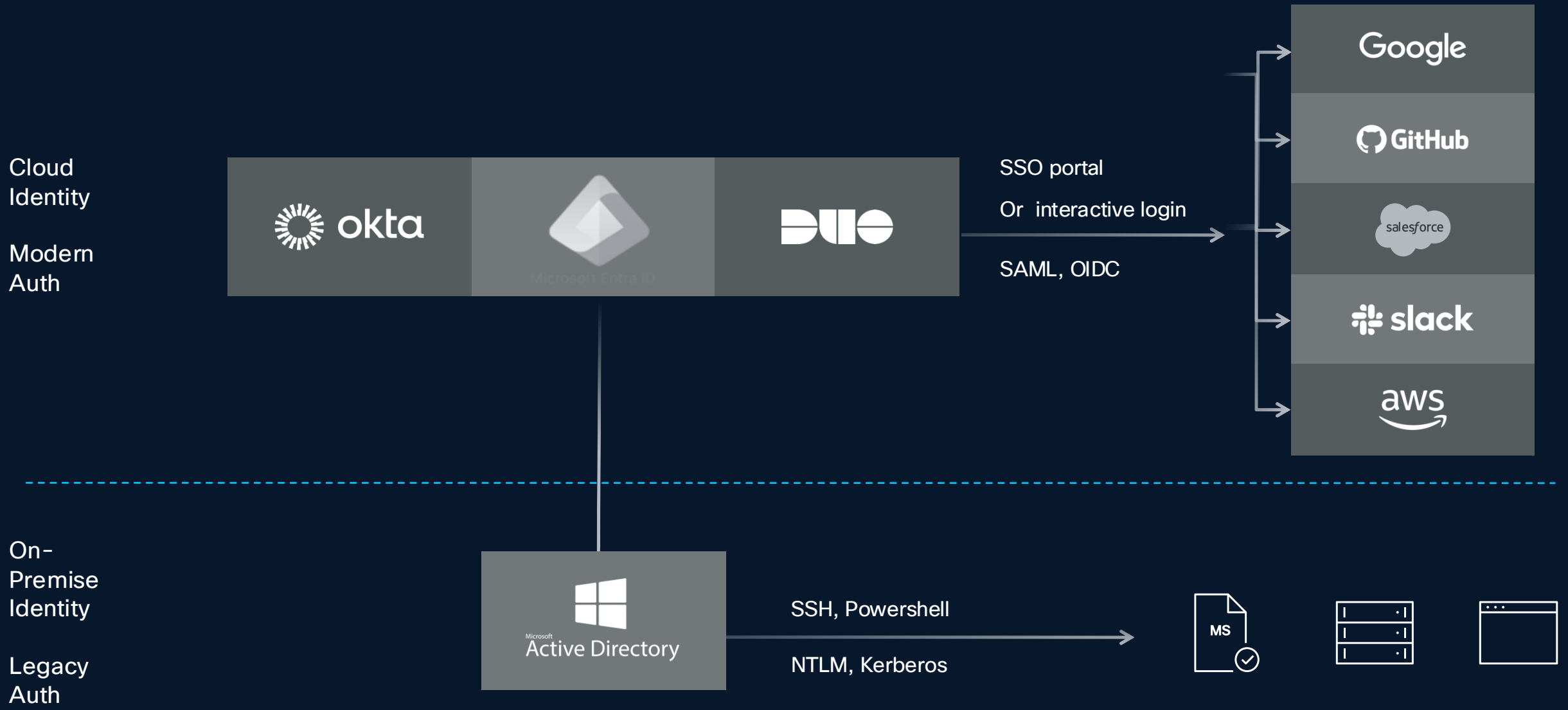
- アクセス時に、MDM/EMSとAPI連携によるデバイス認証や手動登録によるデバイスのユニークなIDを利用したデバイス認証で管理デバイスとして認識
- デバイスの盗難や紛失の際、Block-Listに追加することで、そのデバイスからのアクセスをブロックする



© 2026 Cisco and/or its affiliates. All rights reserved.

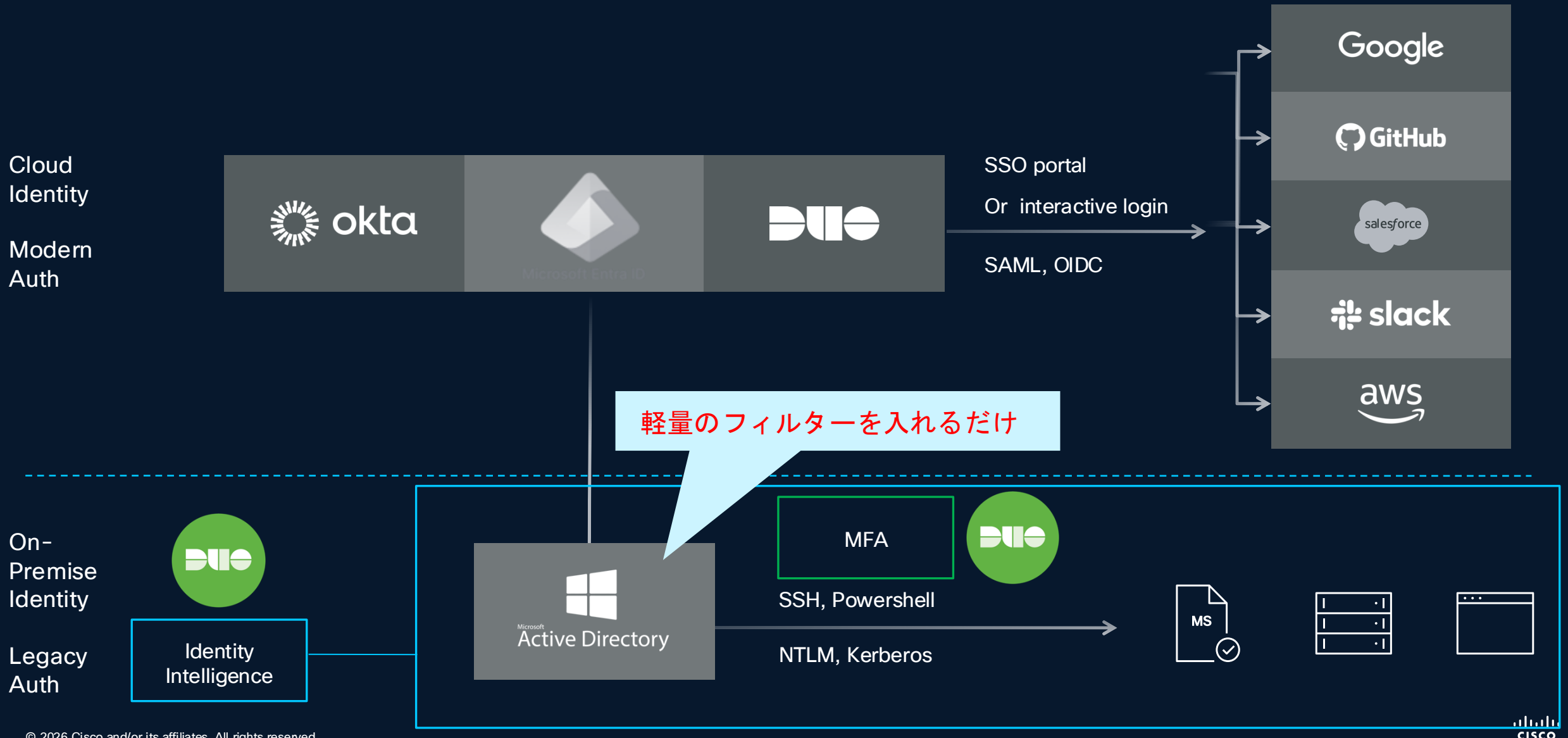
Active Directory保護

クラウドのアイデンティティは既に保護されている



© 2026 Cisco and/or its affiliates. All rights reserved.

Active Directory Defenseはレガシーインフラを保護



© 2026 Cisco and/or its affiliates. All rights reserved.

Demo
- AD Defense

Duo は、Windows と Active Directory のログインも守る

サインイン・権限昇格・リモート デスクトップ・PowerShell・ファイル共有の5場面

	守る入口	攻撃者が狙う場面	機能の名称	対応エディション
デモ 1	**PC へのサインイン**	盗んだパスワードで PC に入る	**Duo Authentication for Windows Logon**	全エディション
デモ 2	**管理者権限への昇格**	一般ユーザーから管理者権限を取る		
デモ 3	**リモート デスクトップ**	別の端末からサーバーに入る		
デモ 4	**PowerShell リモート接続**	画面なしで次のサーバーへ（横展開）	**Duo Windows Command Line Protection**	Advantage / Premier
デモ 5	**ファイル共有**	AD 認証を使う接続全般	**Duo Legacy AD Protection**	Advantage / Premier

手元・昇格・リモート・コマンド・AD を、同じ Duo Mobile の Push で守る

動画は、左が PC の画面、右がスマートフォン（Duo Mobile）の画面です

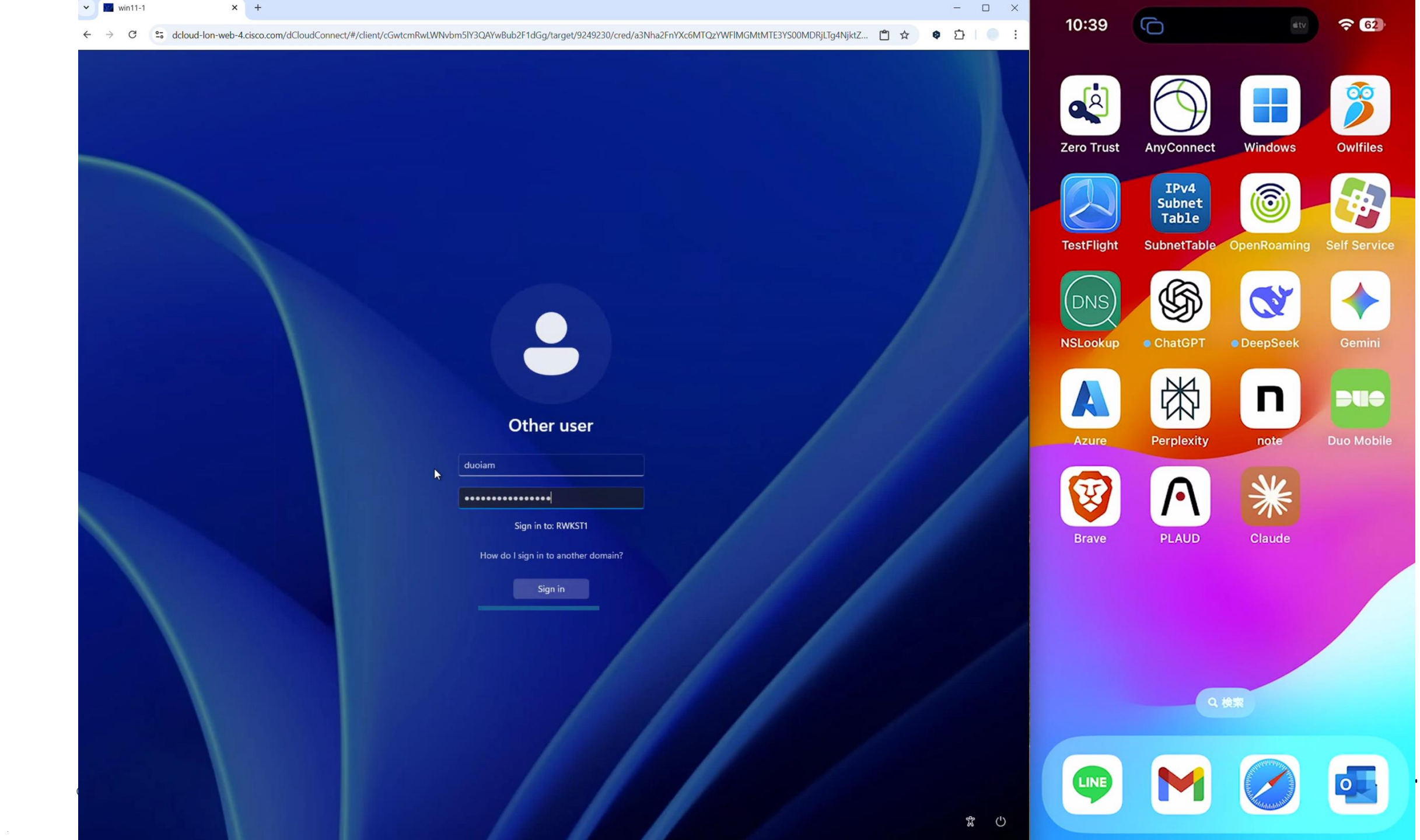
© 2026 Cisco and/or its affiliates. All rights reserved.

デモ 1｜PC へのサインインに MFA

見せること	Windows のサインイン画面でパスワードを入力すると、Duo の認証が始まります。
流れ	1　ユーザー名とパスワードでサインイン 2　Duo の認証画面が表示される 3　スマートフォンの Duo Mobile に届いた通知（Push）を承認 4　デスクトップが開く
ポイント	**パスワードが漏れても、Push を承認しない限り PC は使えません。**
デモする機能	**Duo Authentication for Windows Logon**

※ Push の画面には「RDP: Microsoft RDP」と表示されます。デモ 1〜3 は同じアプリケーションのため、同じ名前になります。
※ 動画の左が PC、右がスマートフォン（Duo Mobile）の画面です。

© 2026 Cisco and/or its affiliates. All rights reserved.

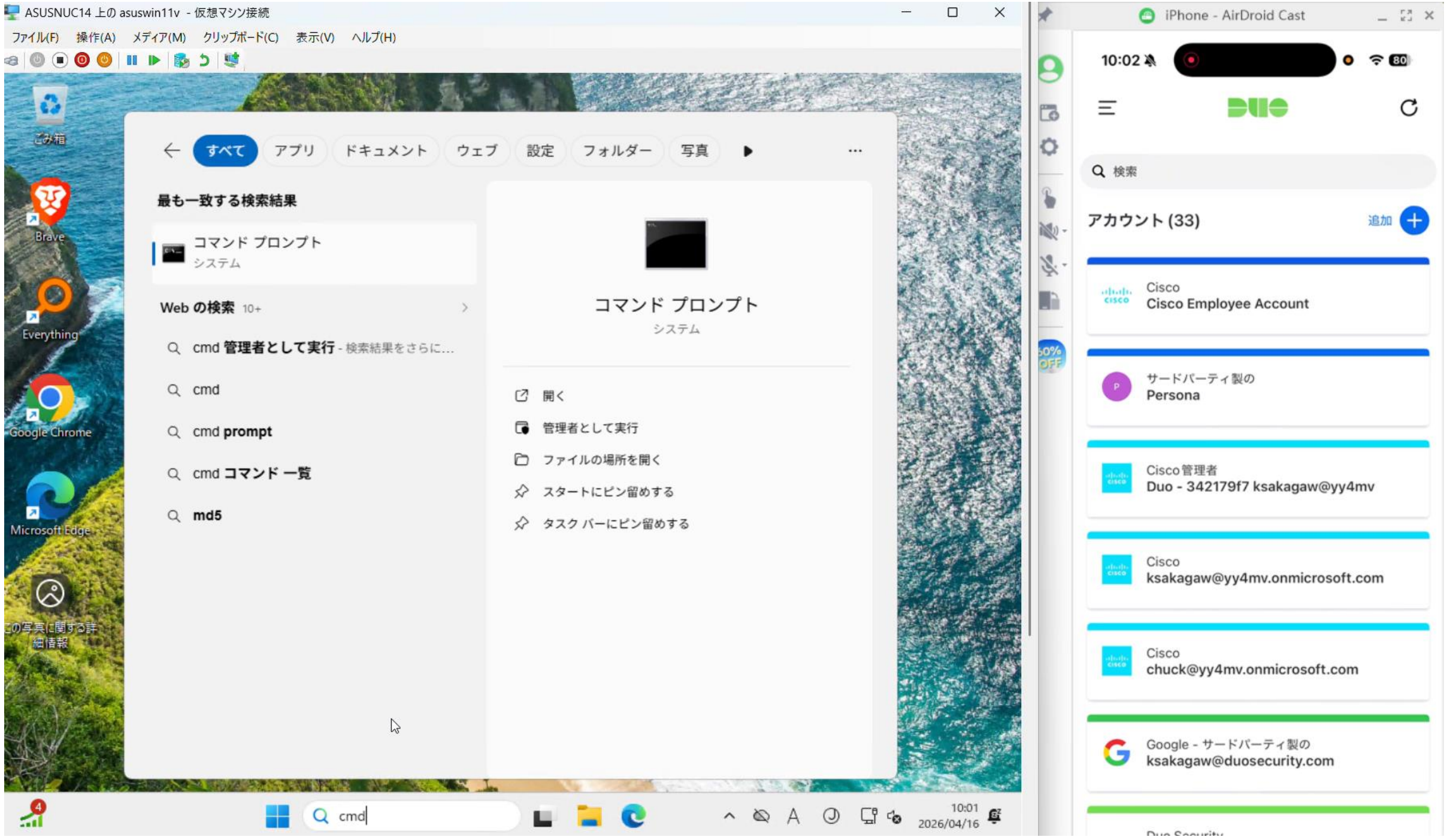

win11-1
dcloud-lon-web-4.cisco.com/dCloudConnect/#/client/cGwtcmRwLWNvbm5lY3QAYwBub2F1dGg/target/9249230/cred/a3Nha2FnYXc6MTQzYWFlMGMtMTE3YS00MDRjLTg4NjktZ...
Other user
duoiam
Sign in to: RWKST1
How do I sign in to another domain?
Sign in
10:39
62
Zero Trust
AnyConnect
Windows
Owlfiles
TestFlight
IPv4 Subnet Table
SubnetTable
OpenRoaming
Self Service
DNS
NSLookup
ChatGPT
DeepSeek
Gemini
Azure
Perplexity
note
Duo Mobile
Brave
PLAUD
Claude
検索
LINE

デモ 2｜管理者権限への昇格に MFA

見せること	サインイン済みの PC でも、UAC 昇格のときに Duo の認証がかかります。
流れ	1　コマンド プロンプトを「管理者として実行」 2　UAC の画面で資格情報を入力 3　Push を承認 4　管理者としてコマンド プロンプトが起動
ポイント	**サインイン済みでも、管理者権限を使う瞬間にもう一度本人確認します。**
デモする機能	**Duo Authentication for Windows Logon**

※ Push の画面には「Elevation: Microsoft RDP」と表示されます（末尾の名称は伏せています）。デモ 1・3 と同じアプリケーションです。

© 2026 Cisco and/or its affiliates. All rights reserved.

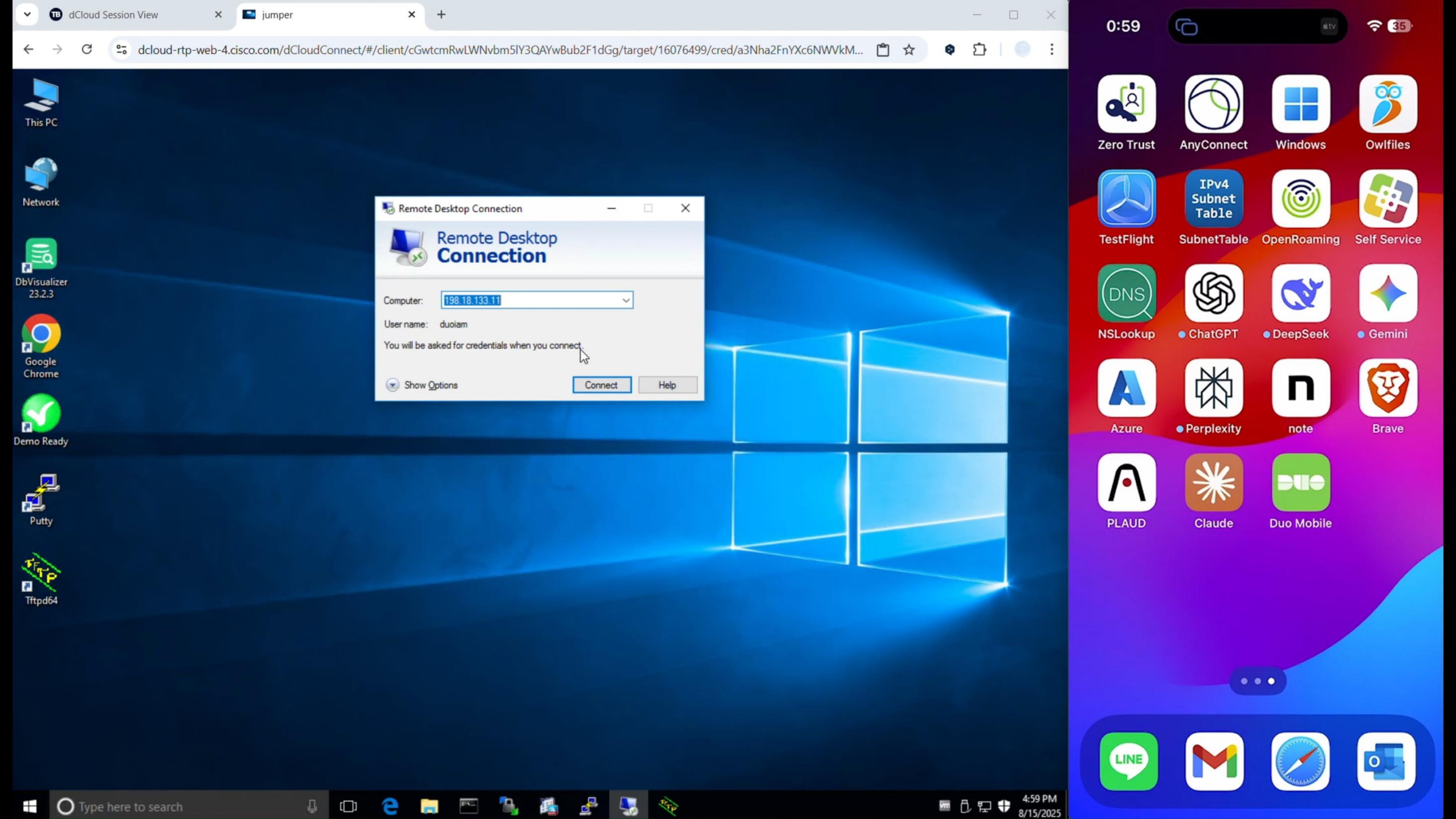

ASUSNUC14 上の asuswin11v - 仮想マシン接続
ファイル(F) 操作(A) メディア(M) クリップボード(C) 表示(V) ヘルプ(H)
ごみ箱
Brave
Everything
Google Chrome
Microsoft Edge
この写真に関する詳細情報
すべて
アプリ
ドキュメント
ウェブ
設定
フォルダー
写真
最も一致する検索結果
コマンド プロンプト
システム
Web の検索 10+
cmd 管理者として実行 - 検索結果をさらに...
cmd
cmd prompt
cmd コマンド 一覧
md5
コマンド プロンプト
システム
開く
管理者として実行
ファイルの場所を開く
スタートにピン留めする
タスク バーにピン留めする
cmd
10:01
2026/04/16
iPhone - AirDroid Cast
10:02
検索
アカウント (33)
追加
Cisco
Cisco Employee Account
サードパーティ製の
Persona
Cisco管理者
Duo - 342179f7 ksakagaw@yy4mv
Cisco
ksakagaw@yy4mv.onmicrosoft.com
Cisco
chuck@yy4mv.onmicrosoft.com
Google - サードパーティ製の
ksakagaw@duosecurity.com

デモ 3｜リモート デスクトップ接続に MFA

見せること	リモート デスクトップで接続すると、接続先で Duo の認証がかかります。
流れ	1　踏み台からリモート デスクトップで接続 2　接続先に切り替わり、Duo の認証画面が表示される 3　Push を承認 4　接続先で whoami・ipconfig・hostname の結果を確認
ポイント	**リモートからの入口も、手元の PC と同じ仕組みで守れます。**
デモする機能	**Duo Authentication for Windows Logon**

※ Push の画面には「RDP: Microsoft RDP」と表示されます（デモ 1 と同じアプリケーション）。

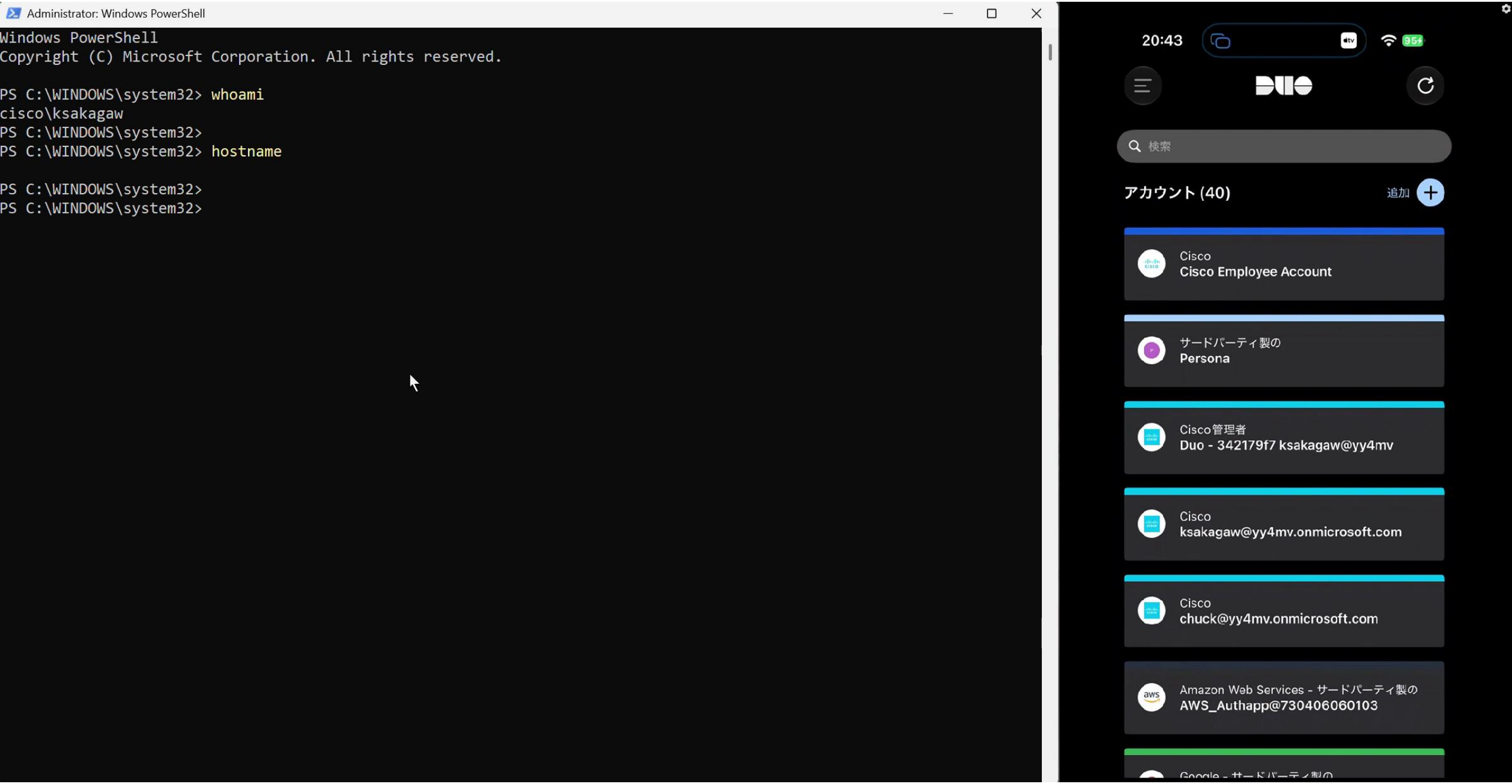
© 2026 Cisco and/or its affiliates. All rights reserved.


dCloud Session View
jumper
dcloud-rtp-web-4.cisco.com/dCloudConnect/#/client/cGwtcmRwLWNvbm5lY3QAYwBub2F1dGg/target/16076499/cred/a3Nha2FnYXc6NWVkM...
This PC
Network
DbVisualizer 23.2.3
Google Chrome
Demo Ready
Putty
Tftpd64
Remote Desktop Connection
Remote Desktop Connection
Computer:
198.18.133.11
User name:
duoiam
You will be asked for credentials when you connect.
Show Options
Connect
Help
Type here to search
4:59 PM
8/15/2025
0:59
Zero Trust
AnyConnect
Windows
Owlfiles
TestFlight
SubnetTable
OpenRoaming
Self Service
NSLookup
ChatGPT
DeepSeek
Gemini
Azure
Perplexity
note
Brave
PLAUD
Claude
Duo Mobile

デモ 4｜コマンドラインのリモート接続に MFA

見せること	Enter-PSSession によるリモート接続は、攻撃者が横展開に使う経路です。ここでも Push の承認が必要です。
流れ	1　Enter-PSSession でリモート接続 2　資格情報を入力 3　「Pushed a login request」と表示され、Push を承認 4　認証成功の表示の後、whoami / hostname で接続先を確認
ポイント	**Windows Logon では守れない「画面のない接続」を、この製品で守ります。**
デモする機能	**Duo Windows Command Line Protection** Advantage / Premier

© 2026 Cisco and/or its affiliates. All rights reserved.

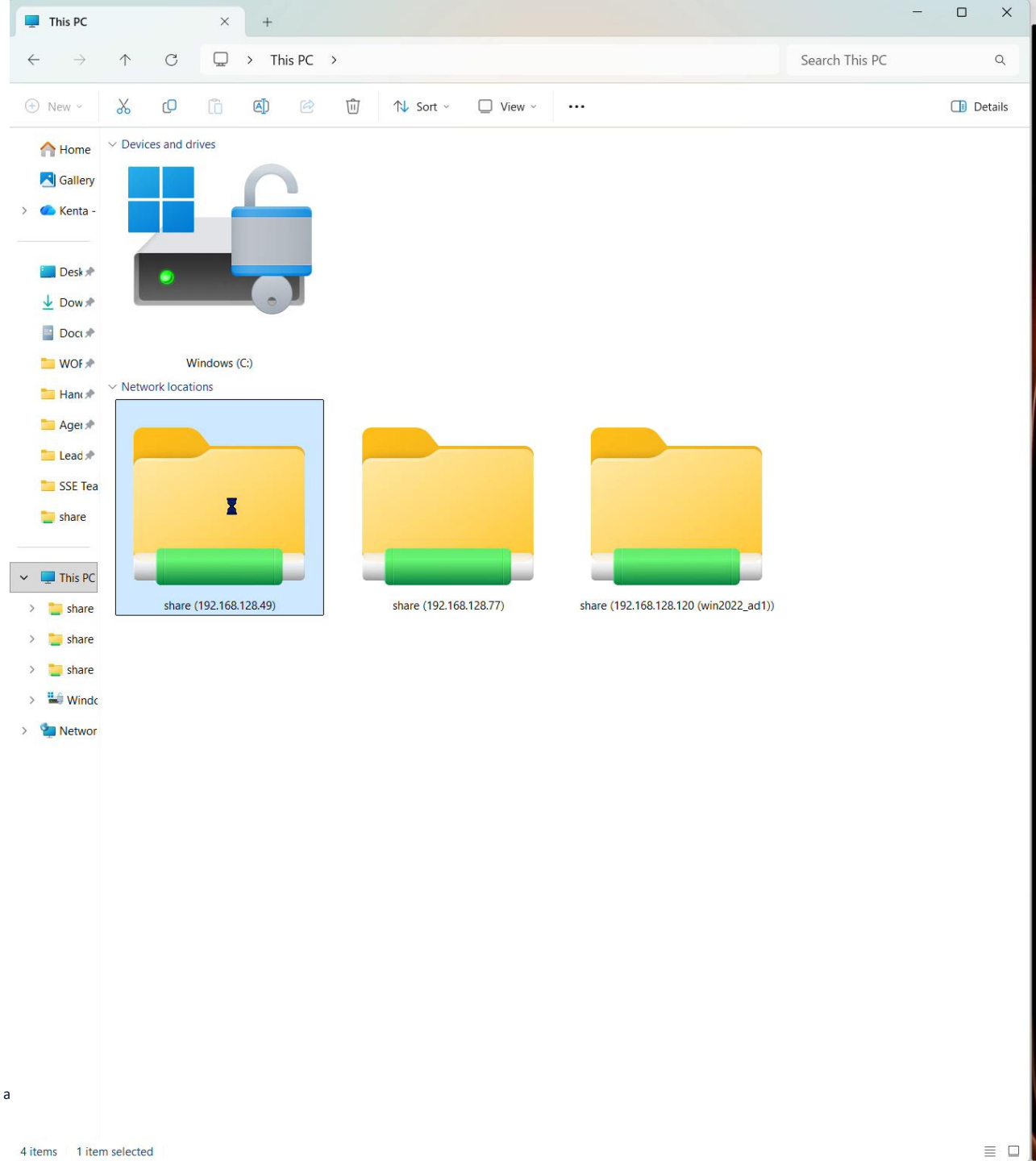

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
PS C:\WINDOWS\system32> whoami
cisco\ksakagaw
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> hostname
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
20:43
検索
アカウント (40)
追加
Cisco
Cisco Employee Account
サードパーティ製の
Persona
Cisco管理者
Duo - 342179f7 ksakagaw@yy4mv
Cisco
ksakagaw@yy4mv.onmicrosoft.com
Cisco
chuck@yy4mv.onmicrosoft.com
Amazon Web Services - サードパーティ製の
AWS_Authapp@730406060103

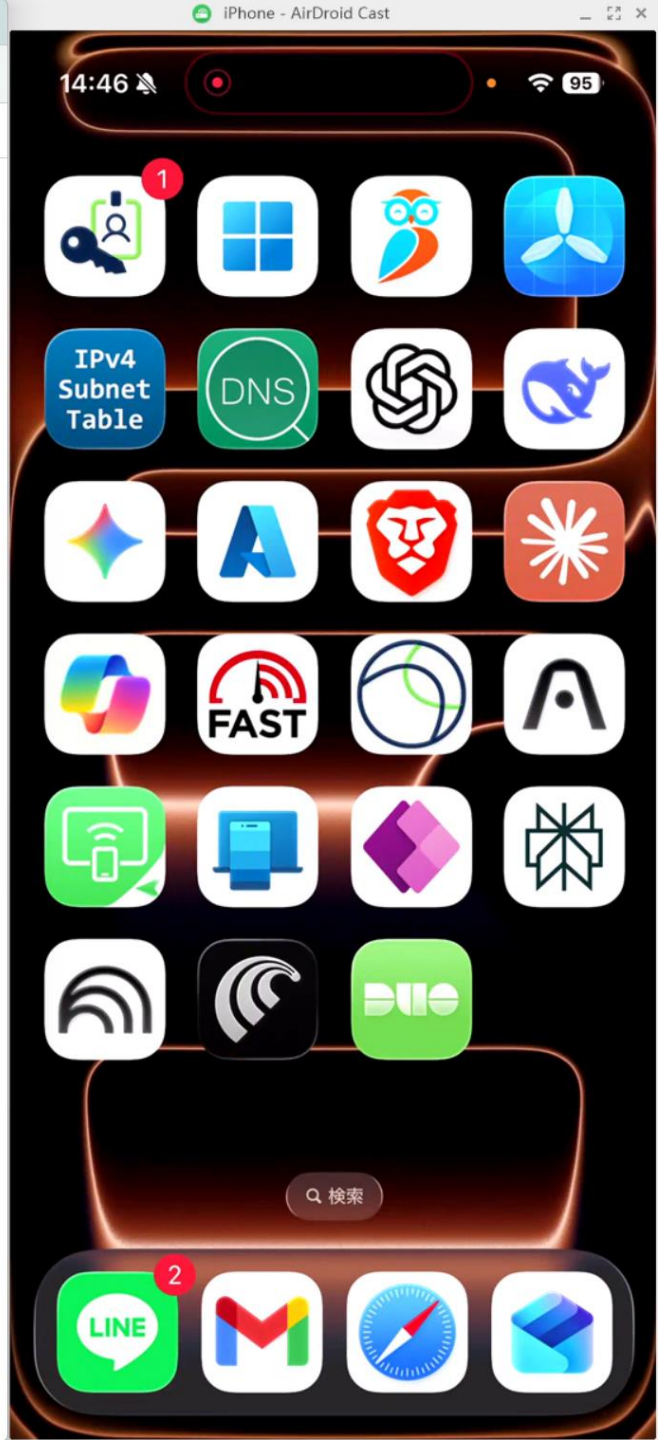
デモ 5｜Active Directory の認証に MFA

見せること	共有フォルダーを開くときの Active Directory 認証で、Duo の Push が届きます。
流れ	1　共有フォルダーを開く 2　資格情報を入力（Windows セキュリティの画面） 3　Push（Legacy AD Authentications）を承認 4　フォルダーが開く
ポイント	**Active Directory の認証（Kerberos / NTLM）そのものに MFA をかけます。**
デモする機能	**Duo Legacy AD Protection**　Advantage / Premier

※ Push に表示される接続元の端末名は伏せています。

© 2026 Cisco and/or its affiliates. All rights reserved.





© 2026 Cisco and/or its a

Identity Intelligence

そもそも何か？

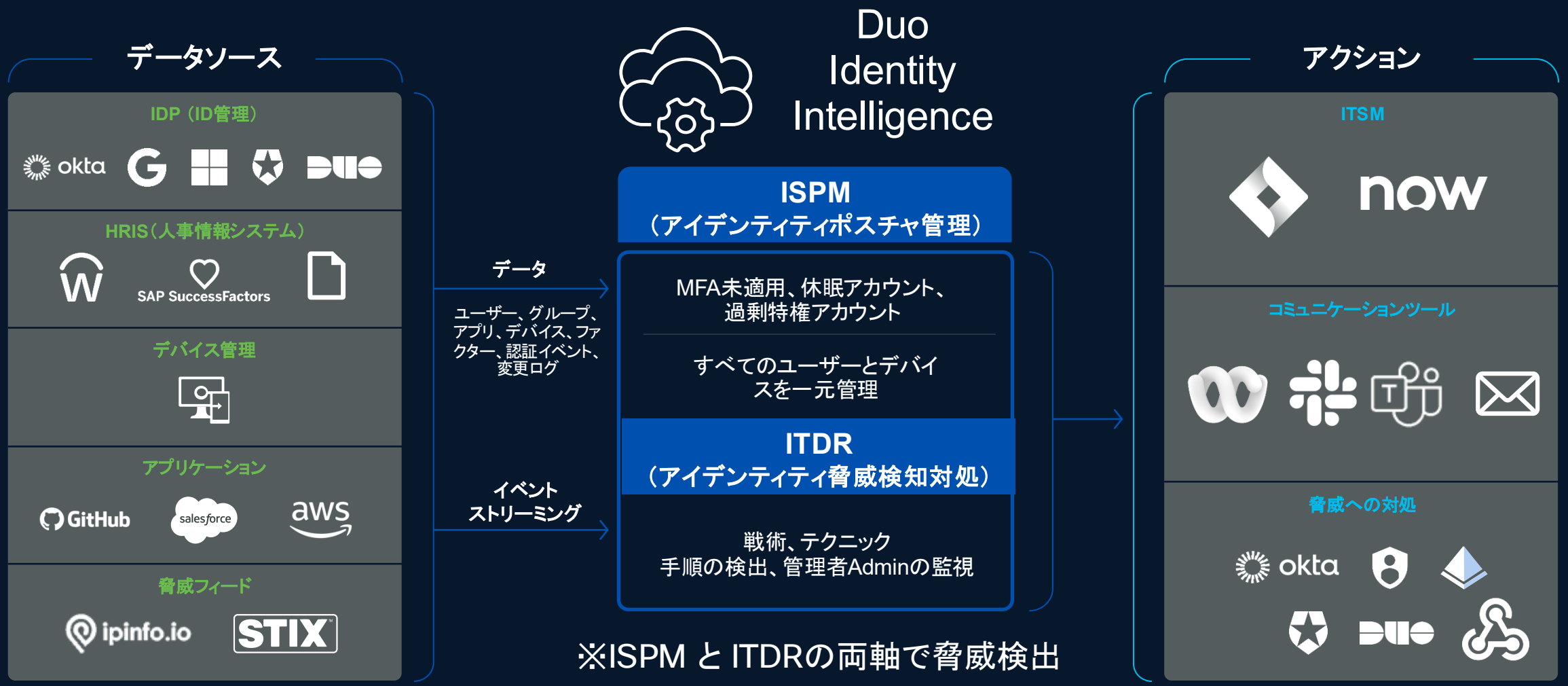
- ISPM（Identity Security Posture Management）
  - 組織全体のアイデンティティに関するセキュリティ上の弱点を継続的に評価・改善するアプローチ
- ITDR（Identity Threat Detection and Response）
  - 認証情報の窃取、権限昇格、横移動など、アイデンティティを標的にした脅威を検出・対応するフレームワーク

観点	ISPM（予防）	ITDR（検知・対応）
目的	弱点の事前発見・修正	リアルタイム脅威の検知とアクション
アプローチ	継続的なポスチャ評価	行動分析・異常検知
例	MFA設定不備、休眠アカウント、等	MFA洪水攻撃、セッションハイジャック、等
タイミング	攻撃前（プロアクティブ）	攻撃中・後（リアクティブ）

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Public

既存のID基盤の構成変更なく、Idenitityのポスチャーチェック、脅威検知が可能



© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Public

Demo
- Cisco Identity Intelligence (CII)

CII は、ID のリスクを 3 つの観点で確認できる

Entra ID・Okta・Duo などに分散した ID 情報を、API 連携で横断して可視化

		見えること	使う画面
観点 1	**危険なユーザーの特定**	Trust Level の低いユーザーと、その理由	**Threats → User 360**
観点 2	**管理者のログイン状況**	管理者の数と、直近のログイン元・場所	**Identities / Threats**
観点 3	**組織の弱点と改善の優先順位**	組織のスコア、優先して直す項目、MFA の利用状況	**Overview / MFA**

危険なユーザー・管理者・組織の弱点を、同じ Cisco Identity Intelligence で確認する

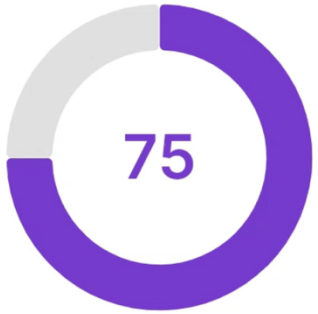
サービスアカウントや AI エージェントなど、人以外のアイデンティティは、後続の Astrix セッションで扱います

© 2026 Cisco and/or its affiliates. All rights reserved.

Overview
Configure
Download PDF Report

Dashboard
Users
Applications
Devices
Non-Human Identities
Campaigns
Checks
Reports
Integrations
ISE Monitoring
System Logs
Tenant Settings

Organization Posture Score



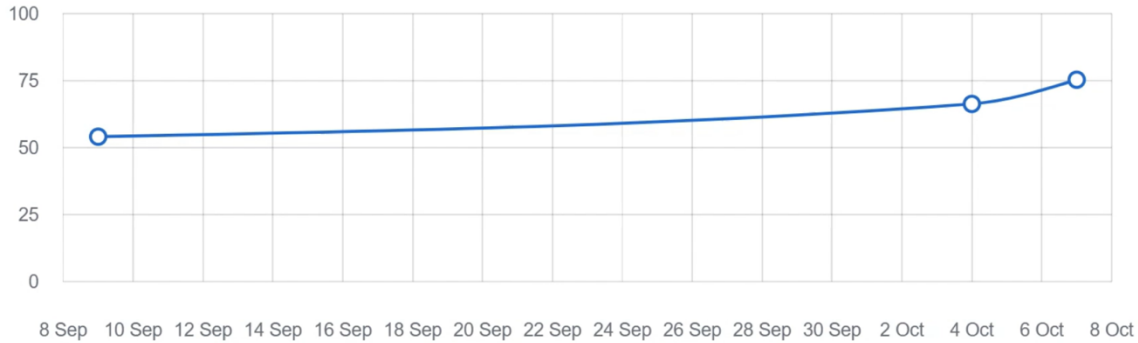
Neutral

+21 (29 days)

Your posture score falls within the lowest 20th percentile for similarly sized organizations.

Posture score trend

30d Sep 08, 2026 12:59 - Oct 08, 2026 12:59 UTC



Top Recommendations

Human Identities



Recommendation:
Review AD accounts with password or account issues and

Non-Human Identities



Recommendation:
Assign owners to non-human identities without an

© 2026 Identity Intelligence

CII は、ID のリスクを 3 つの観点で確認できる

Entra ID・Okta・Duo などに分散した ID 情報を、API 連携で横断して可視化

		見えること	使う画面
観点 1	**危険なユーザーの特定**	Trust Level の低いユーザーと、その理由	**Threats → User 360**
観点 2	**管理者のログイン状況**	管理者の数と、直近のログイン元・場所	**Identities / Threats**
観点 3	**組織の弱点と改善の優先順位**	組織のスコア、優先して直す項目、MFA の利用状況	**Overview / MFA**

危険なユーザー・管理者・組織の弱点を、同じ Cisco Identity Intelligence で確認する

サービスアカウントや AI エージェントなど、人以外のアイデンティティは、後続の Astrix セッションで扱います

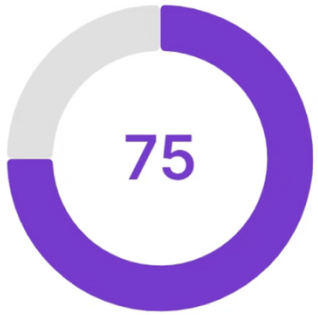
© 2026 Cisco and/or its affiliates. All rights reserved.

Dashboard
Users
Applications
Devices
Non-Human Identities
Campaigns
Checks
Reports
Integrations
ISE Monitoring
System Logs
Tenant Settings

Overview

Configure | Download PDF Report

Organization Posture Score



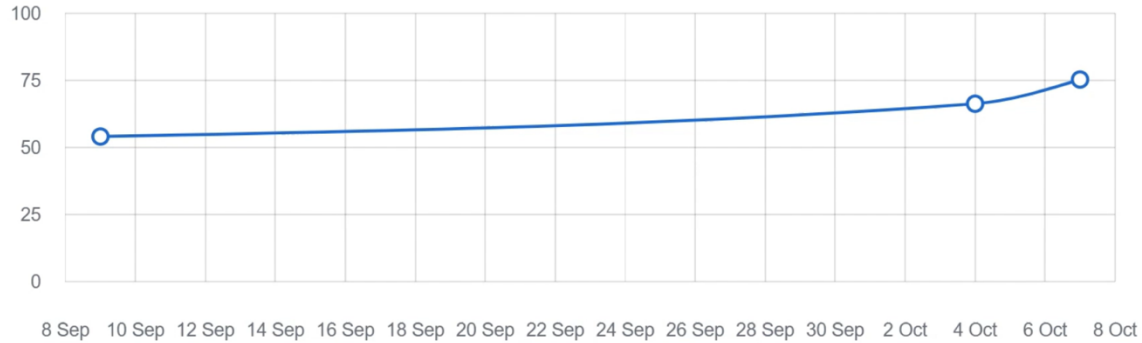
Neutral

+21 (29 days)

Your posture score falls within the lowest 20th percentile for similarly sized organizations.

Posture score trend

30d Sep 08, 2026 13:08 - Oct 08, 2026 13:08 UTC



Top Recommendations

Human Identities



Recommendation:
Review AD accounts with password or account issues and

Non-Human Identities



Recommendation:
Assign owners to non-human identities without an

© 2026 Identity Intelligence

CII は、ID のリスクを 3 つの観点で確認できる

Entra ID・Okta・Duo などに分散した ID 情報を、API 連携で横断して可視化

		見えること	使う画面
観点 1	**危険なユーザーの特定**	Trust Level の低いユーザーと、その理由	**Threats → User 360**
観点 2	**管理者のログイン状況**	管理者の数と、直近のログイン元・場所	**Identities / Threats**
観点 3	**組織の弱点と改善の優先順位**	組織のスコア、優先して直す項目、MFA の利用状況	**Overview / MFA**

危険なユーザー・管理者・組織の弱点を、同じ Cisco Identity Intelligence で確認する

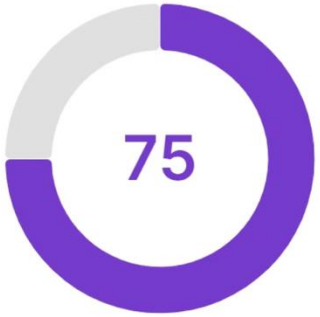
サービスアカウントや AI エージェントなど、人以外のアイデンティティは、後続の Astrix セッションで扱います

© 2026 Cisco and/or its affiliates. All rights reserved.

Overview

Configure | Download PDF Report

Organization Posture Score



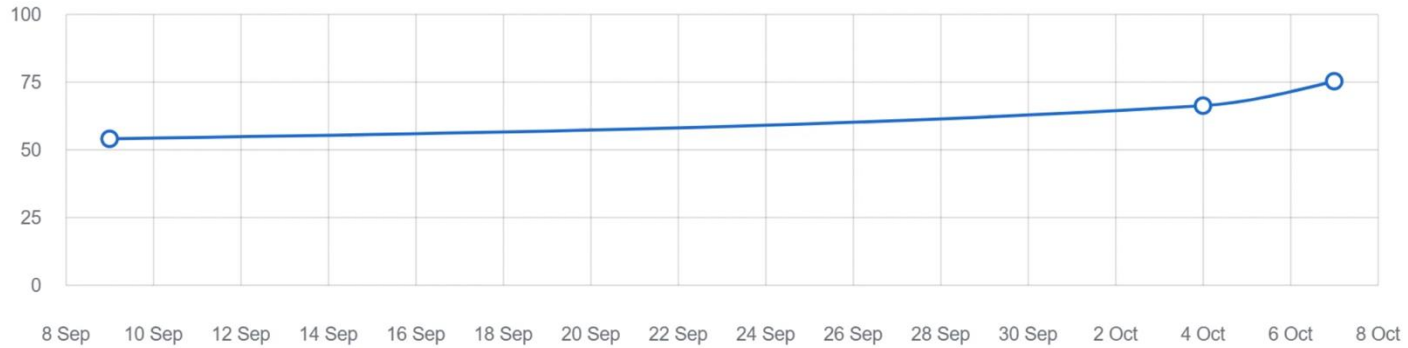
Neutral

+21 (29 days)

Your posture score falls within the lowest 20th percentile for similarly sized organizations.

Posture score trend

30d Sep 08, 2026 14:40 - Oct 08, 2026 14:40 UTC



Top Recommendations

Human Identities



Recommendation:

Review AD accounts with password or account issues and remediate as needed

Non-Human Identities



Recommendation:

Assign owners to non-human identities without an accountable owner

© 2026 Identity Intelligence

CII は、ID のリスクを 3 つの観点で確認できる

Entra ID・Okta・Duo などに分散した ID 情報を、API 連携で横断して可視化

		見えること	使う画面
観点 1	**危険なユーザーの特定**	Trust Level の低いユーザーと、その理由	**Threats → User 360**
観点 2	**管理者のログイン状況**	管理者の数と、直近のログイン元・場所	**Identities / Threats**
観点 3	**組織の弱点と改善の優先順位**	組織のスコア、優先して直す項目、MFA の利用状況	**Overview / MFA**

危険なユーザー・管理者・組織の弱点を、同じ Cisco Identity Intelligence で確認する

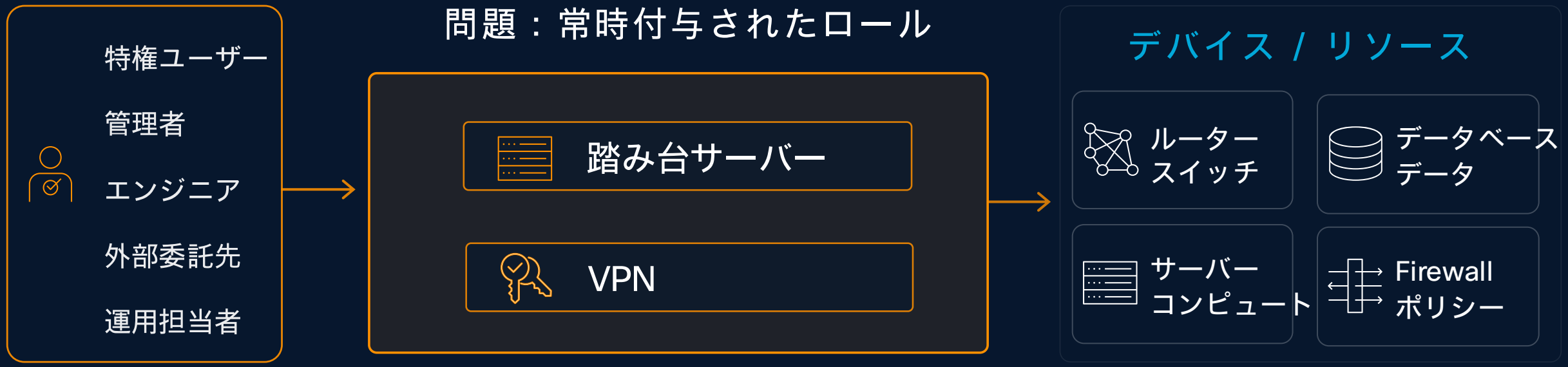
サービスアカウントや AI エージェントなど、人以外のアイデンティティは、後続の Astrix セッションで扱います

© 2026 Cisco and/or its affiliates. All rights reserved.

PAM (特権アクセス)

- Roadmap -

インフラアクセスの問題点



長期間有効な認証情報

恒久的なSSHキー

共有の認証情報

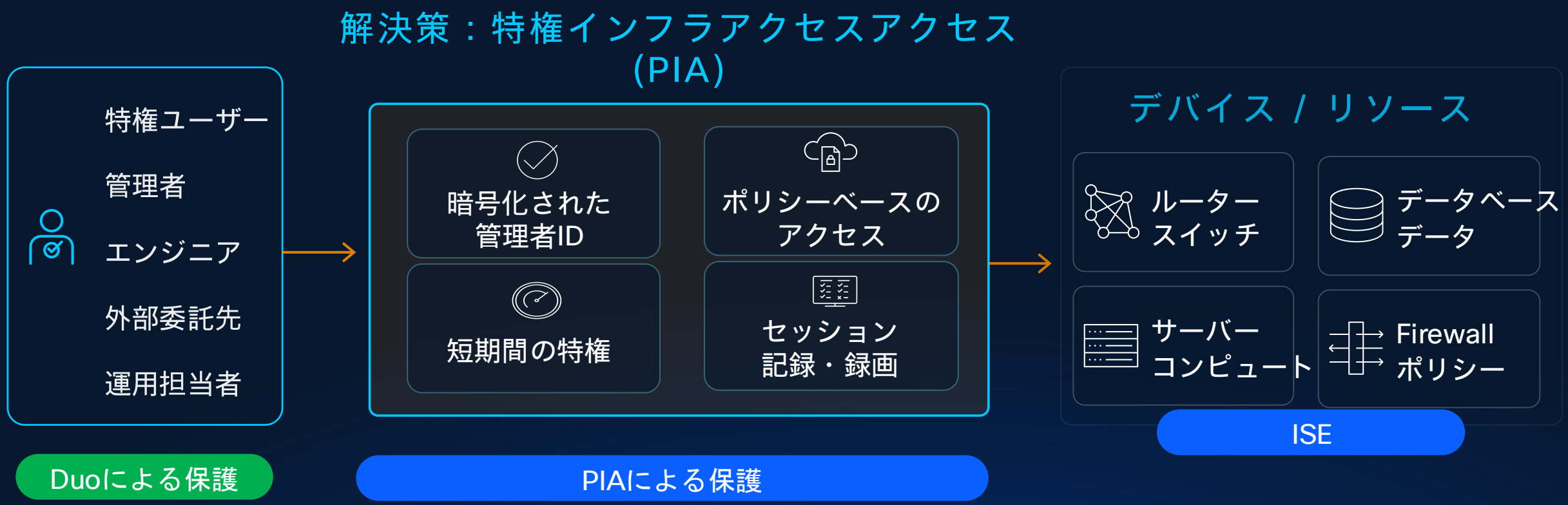
分断された監査チェーン

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Public

インフラアクセスの解決方法

管理者に必要なアクセス権を、必要なときだけ付与する



© 2026 Cisco and/or its affiliates. All rights reserved.

Thank you

