cisco Secure

多要素認証の始め方
事例に基づくパターン別解説

Cisco Secure Access by Duoの導入事例

Cisco Systems G.K.
GSSO
Hiroki Hata, Takehiro Nishi , Katsuhiko Yoshida
March.26, 2021

本日のセミナーについて

Duo 専任担当営業
Cisco Secure Access by Duo
専任担当営業

セキュリティSE
マネージャー
セキュリティ商品全体の
SE担当マネージャー

セキュリティパートナー
担当営業
セキュリティ商品全体の
パートナー様担当

アジェンダ

なぜ今
多要素認証が
必要なのか

多要素認証の
導入パターン別・
事例・活用方法

事例に基づく、
多要素認証の
検討パターン

なぜ今多要素認証が必要なのか

なぜ多要素認証が必要なのか？（一般論）

- 昨今の高度化する攻撃を防ぐため、多要素認証の必要が高まっている

これまで

➢ 旧来の対策で問題がなかった

<u>一般的な対策</u>

- VPN
- UTM
- アンチウィルス
- アンチマルウェア

現在

➢ サイバー犯罪が高度化し、セキュリティインシデントが多発

✓ ランサムウェアによる大規模被害
✓ フィッシングによる情報漏洩
✓ ソフトウェアのアップデートを利用した大規模被害

➢ 防ぐ手段も高度化を求められる

○ Zero Trust
○ SASE

多要素認証の重要性が増している

<u>検討企業も増加</u>

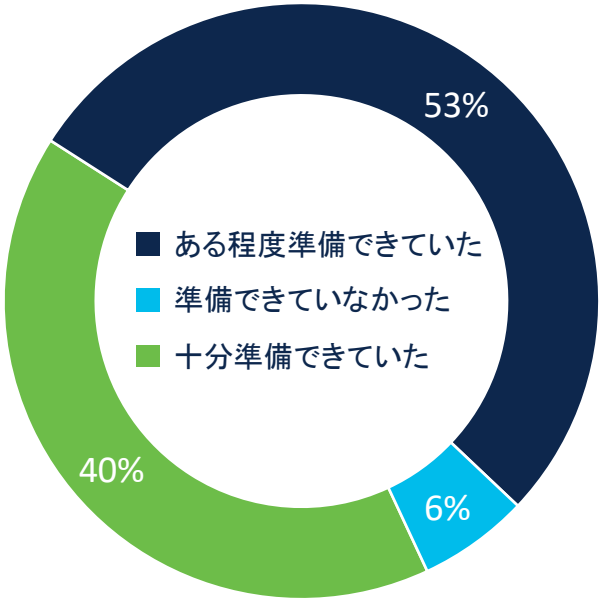
情報セキュリティ10大脅威 2021

出典IPA https://www.ipa.go.jp/security/vuln/10threats2021.html

昨年順位	個人	順位	組織	昨年順位
1位	スマホ決済の不正利用	1位	ランサムウェアによる被害	5位
2位	フィッシングによる個人情報等の詐取	2位	標的型攻撃による機密情報の窃取	1位
7位	ネット上の誹謗・中傷・デマ	3位	テレワーク等のニューノーマルな働き方を狙った攻撃	NEW
5位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	4位	サプライチェーンの弱点を悪用した攻撃	4位
3位	クレジットカード情報の不正利用	5位	ビジネスメール詐欺による金銭被害	3位
4位	インターネットバンキングの不正利用	6位	内部不正による情報漏えい	2位
10位	インターネット上のサービスからの個人情報の窃取	7位	予期せぬIT基盤の障害に伴う業務停止	6位
9位	偽警告によるインターネット詐欺	8位	インターネット上のサービスへの不正ログイン	16位
6位	不正アプリによるスマートフォン利用者への被害	9位	不注意による情報漏えい等の被害	7位
8位	インターネット上のサービスへの不正ログイン	10位	脆弱性対策情報の公開に伴う悪用増加	14位

- 「ランサムウェアによる被害」が1位
- 「テレワーク等のニューノーマルな働き方を狙った攻撃」が初登場で3位

テレワーク移行準備の心構えの差が浮き彫りに



ある程度準備できていた
（割合が高い業種）

設計 / エンジニアリング
72%

準備できていなかった
（割合が高い業種）

卸売 / 流通
15%

教育
14%

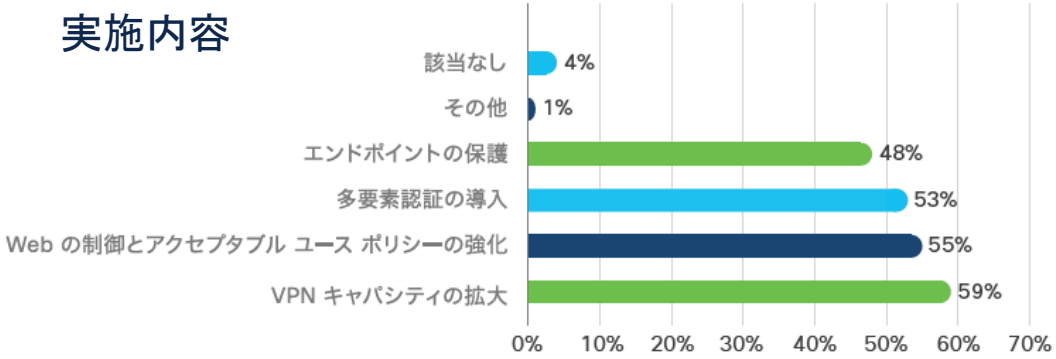
化学 / 製造
非コンピュータ関連製造
非営利 / 慈善事業
10%

- 多くの組織が「ある程度の準備ができている」に留まる
- 日本は比較して準備ができていない回答が多い

	Global	APJC	Japan
十分準備できていた	40%	39%	19%
ある程度準備できていた	53%	54%	63%
準備できていなかった	6%	7%	17%

出典:シスコシステムズ 2020.10 次世代のセキュアなリモートワークレポート

どういったセキュリティ対策やポリシー変更が実施されたか



	Global	APJC	Japan
VPNキャパシティの増大	59%	56%	49%
Web制御と許可ポリシー強化	55%	61%	35%
多要素認証の導入	53%	59%	35%
エンドポイントの保護	48%		36%

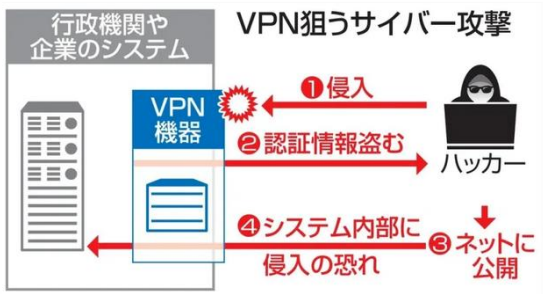
出典:シスコシステムズ 2020.10 次世代のセキュアなリモートワークレポート

狙われるテレワーク

600超の組織にサイバー攻撃

テレワーク機器の欠陥悪用

2020/12/1 06:00 (JST) | 12/1 06:17 (JST) updated ©一般社団法人共同通信社



VPN狙うサイバー攻撃

テレワークや遠隔操作に使われる情報機器の欠陥が悪用され、少なくとも607の国内企業や行政機関などがサイバー攻撃を受けていたことが30日、専門家への取材で分かった。警察庁や日本政府観光局、岐阜県庁、リクルート、札幌大などで被害が判明。多くがID、パスワードなどの認証情報を盗まれていた。

この機器は外部からネットワーク内部に安全に接続するために利用され「VPN（仮想私設網）」と呼ばれる。新型コロナウイルス流行で利用が増えている。問題のVPNは米フォーティネット社製で、欠陥が放置されている機器は世界で約5万台あり、うち1割超の約5400台が日本関連だった。

Source:共同通信社
https://this.kiji.is/706248789438039137

Talos 脅威情報ニュースレター（2019 年 8 月 29 日）
https://gblogs.cisco.com/jp/2019/09/talos-threat-source-newsletter-aug-22_29/

件名：人気の VPN サービスの脆弱性により攻撃が集中し、情報が漏えい中
説明：Fortigate および Pulse の各 VPN サービスで見つかった脆弱性で、攻撃者によるエクスプロイトが多発し、暗号化キーやパスワードなどの機密データが盗まれています。先週開始されたこれらのキャンペーンは、Linux および * NIX システムを管理するための Webmin ユーティリティを対象としています。Linux や *NIX システムは企業ネットワーク内のデバイスです。関連する脆弱性により、攻撃者がシステムを完全に乗っ取る危険性があります。
Snort SID：51240 ～ 51243（作成者：John Levy）、51288、51289（作成者：Joanne Kim）

複数の SSL VPN 製品の脆弱性に関する注意喚起

最終更新: 2019-09-06

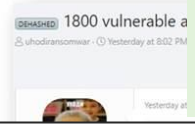
JPCERT-AT-2019-0033
JPCERT/CC
2019-09-02(新規)
2019-09-06(更新)

Source:JPCERT
https://www.jpcert.or.jp/at/2019/at190033.html

I. 概要

JPCERT/CC では、複数の SSL VPN 製品の脆弱性について、脆弱性に対す
います。

- Palo Alto Networks (CVE-2019-1579)
- Fortinet (CVE-2018-13379)
- Pulse Secure (CVE-2019-11510)



Source:https://www.zdnet.com/article/hacker-leaks-passwords-for-900-enterprise-vpn-servers/
900以上の企業VPNサーバのパスワードが公開
2020年6月24日～7月8日の間
Pulse Secure VPN 全体をスキャン・自動収集

Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性 (CVE-2018-13379) の影響を受けるホストに関する情報の公開について

最終更新: 2020-11-27

Source:JPCERT
https://www.jpcert.or.jp/newsflash/2020112701.html

CyberNewsFlash一覧

(1) 概要

JPCERT/CC は、2020年11月19日以降、Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性の影響を受けるホストに関する情報が、フォーラムなどで公開されている状況を確認しています。当該情報は、FortiOS の既知の脆弱性 (CVE-2018-13379) の影響を受けるとみられるホストの一覧です。この一覧は、攻撃者が脆弱性を悪用可能であることを確認した上で作成したものとみられ、ホストの IP アドレスに加え、SSL VPN 接続を利用するユーザーアカウント名や平文のパスワードなどの情報が含まれているとのことです。

不正送金・不正アクセス

Press Release
報道関係者各位

Source:Kyash

株式会社　Kyash
2020年9月15日

弊社に関する一部報道について

一部
以下
・金
・対
・金
・事
当口
※現

PayPayからのお知らせ

Source:PayPay

2020.09.15　セキュリティ

「PayPay」利用時の本人確認および不正利用防止に向けた対応について

PayPayと連携する金融機関について調査し、追記しました。また、ゆうちょ銀行における不正利用として公表した件数、金額を当社で再調査し、修正しました。

ドコモからのお知らせ

Source:NTT DoCoMo

一部銀行の口座情報を使用したドコモ口座の不正利用について

2020年9月8日

一部の銀行において、ドコモ口座を利用した不正利用が発生しております。

本件は、不正に取得された銀行口座番号やキャッシュカードの暗証番号等を悪用したものであり、当社システムに不正アクセスされ情報を取得されたものではございません。

当社は、これまで不正アクセスに対する二段階認証やアカウントロック等、様々なセキュリティ対策を講じておりますが、お客さまにより安心・安全にご利用頂けるよう、更なる対策強化に努めてまいります。

悪意のある第三者による不正アクセスに関するお知らせ

- ニュースリリース
- 当社
- 岡三証券
- 岡三オンライン証券
- 2020年
- 2019年
- 2018年
- その他の

Source:岡三オンライン証券

2020年9月18日
岡三オンライン証券株式会社

悪意のある第三者による不正アクセスに関するお知らせ

各　位

Source:SBI証券

株式会社SBI証券

悪意のある第三者による不正アクセスに関するお知らせ

2020年9月16日

当社のお客さま口座への悪意のある第三者による不正アクセスにより、お客さまの資産が流出したことが判明いたしました。お客さまには大変ご迷惑、ご心配をおかけいたしましたことを深くお詫び申し上げます。
被害を受けられたお客さまには個別にご連絡を行っており、捜査当局および資産流出先の銀行である株式会社ゆうちょ銀行、株式会社三菱UFJ銀行と連携して対応を進めております。なお、お客さまの被害につきましては資産保護を最優先として、当社が責任をもって速やかに補償することを予定しております。

1.　経緯

当社は、不正アクセスに対するモニタリングを常に行っており、不審なアクセスがあればお客さまに直接ご連絡を行うなどして対応を行っておりますが、直近においても不正ログインを検知し、調査・対策を行っておりました。その過程において、2020年9月7日に寄せられた身に覚えのない取引があったとのお客さまからのお申し出を端緒として、当該お客さまのログ調査等により、不審なアクセス元を特定し、そこからアクセスされたその他の口座や同様の特徴のある取引履歴等を分析いたしました。その結果、悪意のある第三者による不正アクセスが行われ、お客さまの有価証券の売却およびお客さま名義の出金先銀行口座への出金を複数件、確認いたしました。現在、出金先銀行と連携して対応を進めております。

2.　現在判明している被害の状況

・口座数：6口座　（出金先銀行：ゆうちょ銀行5口座、三菱UFJ銀行1口座）
・被害総額：合計9,864万円（ゆうちょ銀行：9,229万円、三菱UFJ銀行：635万円）

3.　再発防止策

引き続き、本事案の個別原因の分析を継続し、より有効な施策を速やかに実施してまいります。

（1）監視

・不正アクセスに対する24時間モニタリング体制のさらなる強化
・不正アクセス検知システム（WAF）による新たな攻撃手法への対応
・不審なIPアドレスからのアクセス排除（IPレピュテーションサービスの一層の活用）

コロナ渦で狙われるもの

Talos 脅威情報
https://gblogs.cisco.com/jp/author/talosjapan/

インシデント対応では、4 四半期連続で Ryuk が他を圧倒していました。前四半期のレポートで説明したとおり、Ryuk は、商用化されたトロイの木馬ではなく、環境寄生型ツールを駆使する手口へと転換が進みました。そのため、商用化されたトロイの木馬を利用する攻撃の観測は減少しています。Citrix デバイスと Pulse VPN や、リモート デスクトップ サービス（RDS）に対するセキュリティ侵害も増加していますが、最大の感染ベクトルは今でも電子メールです。今四半期で特に注目すべきが新型コロナ感染症の影響です。興味深いことに、IR 業務では感染症に便乗した事例が観測されませんでした。ただし、コロナ禍の影響で、組織のサイバーセキュリティ インシデントへの対応と封じ込めに影響が出ています。

初期ベクトル

ロギングの量が十分ではないため、ほとんどの IR 業務では初期ベクトルを明確に特定することが困難でした。ただし、初期ベクトルを特定できた事例や合理的に推測できた事例に基づく限り、最多の感染ベクトルは依然としてフィッシングです。標的組織の RDS にブルートフォース攻撃を仕掛けた事例もいくつか観測しています。これは、ランサムウェア Phobos の増加や、コロナ禍のリモートワークで攻撃対象が拡大したことと関連しているようです。通例、初期ベクトルとして利用されるのは侵害された RDS 接続です。Citrix Application Discovery Controller および Citrix Gateway（CVE-2019-19781）、さらに Pulse Secure VPN（CVE-2019-11510）に関しては、複数の侵害が継続的に観測されました。

最近の注目すべきセキュリティ問題

件名：Zerologon の脆弱性を悪用する攻撃者が増加
説明：Cisco Talos では、Microsoft 社の脆弱性 CVE-2020-1472 に対する攻撃が急増していることを確認しています。この脆弱性は Netlogon における権限昇格の不具合であり、8 月の Microsoft セキュリティ更新プログラムで概要が公開されました。脆弱性は Netlogon Remote Protocol で使用される暗号化認証方式の不備に起因しています。エクスプロイトされた場合、特定の Netlogon 機能の認証トークンが偽造され、コンピュータのパスワードを更新される可能性があります。脆弱性を利用すればドメイン コントローラ自体を含むあらゆるコンピュータを装えるため、ドメイン管理者のログイン情報にアクセスされる危険性があります。
Snort SID：55703、55704

インシデント対応チームによる分析情報

医療機関を狙ったランサムウェア攻撃への複数の対応事案にも、Talos が携わっています。直近 90 日間を見ると、今四半期のインシデント対応事案のうち約 20% は医療分野で起きています。米国内のある医療センターが標的となった事案では、Ryuk に加え、レッドチーム活動ツールである Cobalt Strike が使用されていました（Cobalt Strike は Ryuk と併用されることが少なくありません。詳細については、以下をご覧ください）。ただし、米国の医療センターを狙った別のインシデント対応事案では、Ryuk 以外のランサムウェアが使用されていました。現時点では Vatet または Defray であると推定されます。どちらのインシデントに関しても、Trickbot の存在は確認されていません。

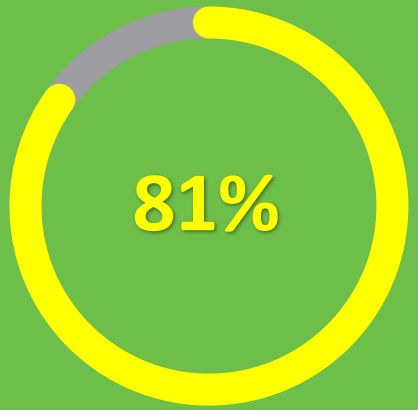
- サイバー犯罪者、裕福な都市部の学校を狙う傾向が強まる。それらの学校には大量のデータが保存されているため、身代金を支払える可能性がより高いと攻撃者が考えているようです。
- 新学期をリモート授業で迎えた教員と生徒たちは、新しい仮想クラスの利用方法とサイバー攻撃への対処方法を学ぶ必要に迫られる。フロリダ州マイアミはその代表例と言えます。市当局は域内の学校システムが 1 日で 12 回の攻撃を撃退したと発表しています。
- コネチカット州ハートフォード市、サイバー攻撃を受け新学期の開始を延期。市当局の発表によれば、学校教育に不可欠な 200 台のサーバが侵入されました。
- コロナ禍が依然として終息しない中、世界各地の教育機関がハイブリッド学習環境の維持に注力。しかし多くの教育機関は、オンライン学習を妨げるサイバー攻撃からの防御にも追われています。
- 国家の支援を受けた攻撃者、新型コロナウイルスのワクチン研究を標的とする攻撃を継続。
- チリの大手銀行、サイバー攻撃を受け今週すべての支店を閉鎖。現時点の報道では、従業員が開いた悪意のある Microsoft Office ドキュメントから攻撃が始まったようです。
- ノルウェー議会、今年初めに同国政府のネットワークに対してサイバー攻撃を仕掛けたとして、[redacted]政府の支援を受けた攻撃者集団を正式に告発。この攻撃により複数の政治家の電子メールアドレスがハッキングされています。

現実の脅威：不正侵入は、ID/パスワード漏洩から
セキュリティの新しいアプローチが必要とされる

Targeting Identity

81%のハッキングによる侵害は、パスワード漏洩や弱いパスワードなど、クレデンシャルに関連している

*Verizon Data Breach Investigations Report



* https://gblogs.cisco.com/jp/2020/06/unpacking-2020s-verizon-dbir-human-error-and-greed-collide/

多要素認証（Duo）の導入パターン別事例・活用方法

Over 20,000 Customers

- 3000+ Technology
- 500+ Higher Education
- 600+ Healthcare
- 1500+ Financial Services
- 350+ Government
- 80+ Fortune 500

Duo Security is now part of Cisco.

Over 20,000 Customers

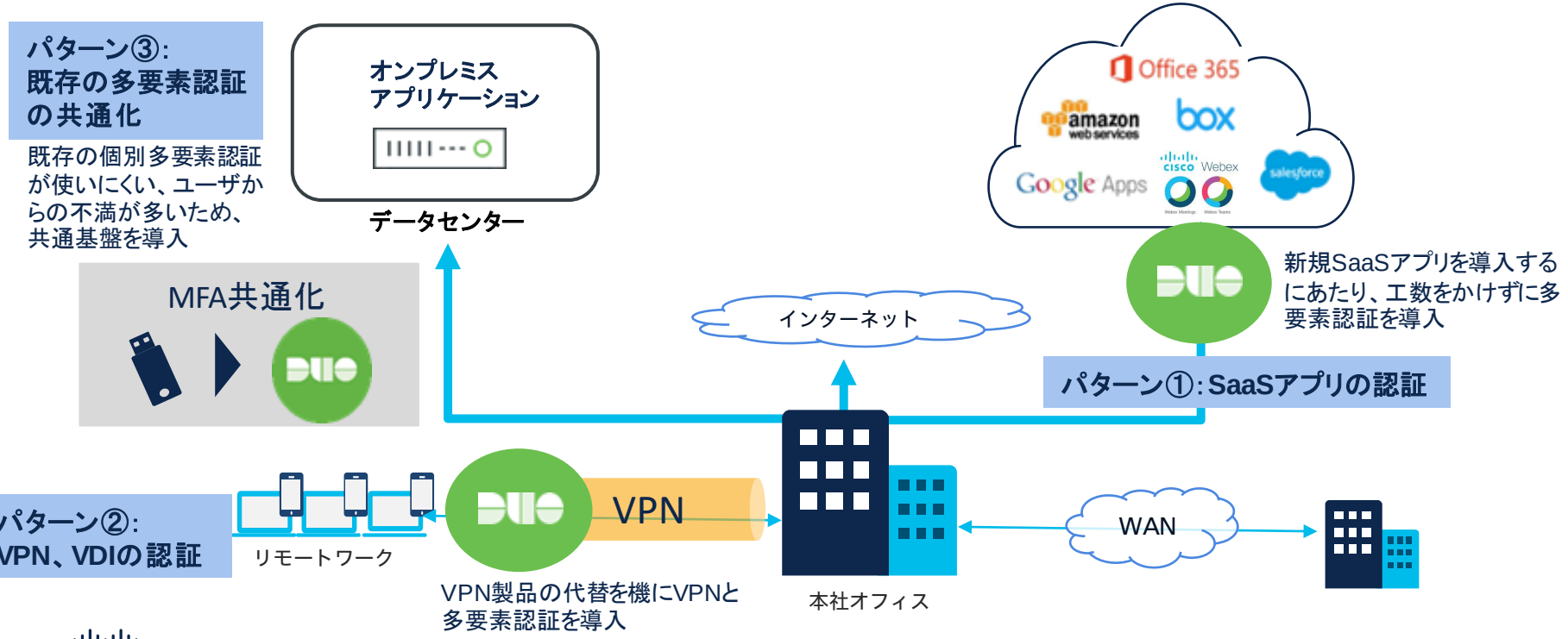
約30,000ユーザー

- 3000+ Technology
- 500+ Higher Education
- 600+ Healthcare
- 1500+ Financial Services
- 350+ Government
- 80+ Fortune 500

Duo Security is now part of Cisco.

Duoの導入パターン

- Duo をご導入いただいたお客様のユースケースはほぼ3パターンに集約可能

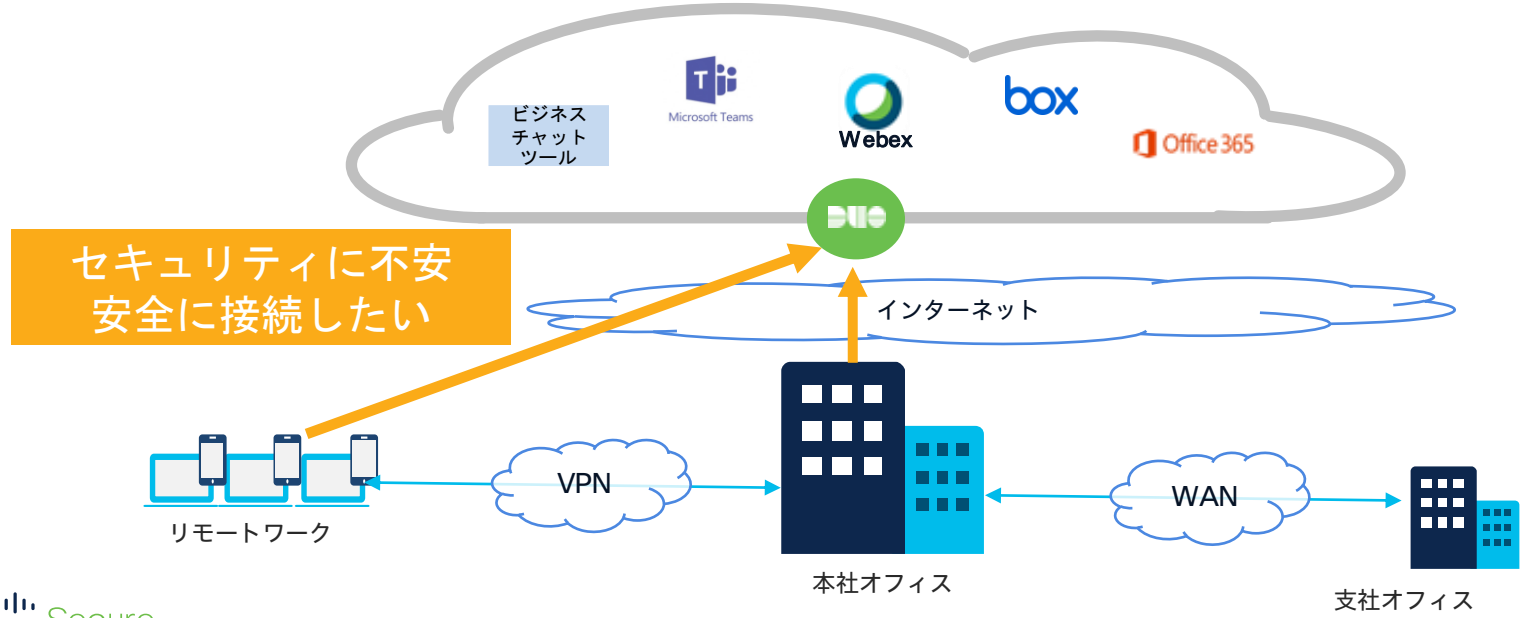


導入パターン①
SaaSアプリの認証

（パターン①：SaaSアプリの認証）

SaaSアプリ導入時にMFAを導入

- SaaSアプリを便利に安く導入したいが、セキュリティに不安がある。
- 昨今のリモートワーク拡大により、社内外問わずSaaSアプリへのセキュリティ対策がお客様の課題になっている。



お客様事例

（パターン①：SaaSアプリの認証）

中西金属工業様（製造業：従業員数 約4,500名）

在宅勤務・リモートワーク環境におけるセキュリティ強化

在宅勤務環境から利用するアプリケーションの セキュリティを多要素認証で強化

背景・課題

- 新型コロナウイルスの感染拡大により、これまでの想定を上回る600名超の従業員が一気に在宅勤務にシフト
- 従業員間のコミュニケーションを支 えるために急遽導入したビジネスチャットツールセキュリティ対策が急務

ソリューション

- 認証方式にシンプルな「プッシュ通知にワンタップ応答」を選択。ITリテラシーの高くない従業員もストレスなく操作可能
- クラウドベースのサービスで、 既存の社内ITインフラへの影響を最小限に抑えつつ短期間で導入可能

結果～今後

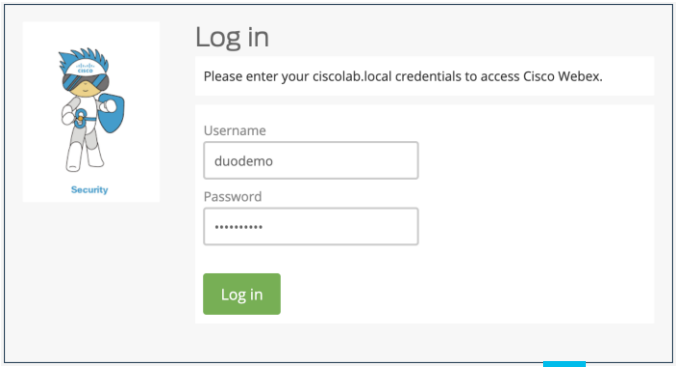
- 【構築】構築作業は2、3日で完了し、予定どおりのスケジュールでビジネスチャットツールを多要素認証のもとで運用
- 【運用】大きなトラブルを起こすことなく安定した稼働を続けており、在宅勤務のセキュリ ティ強化に貢献
- 【今後】VDIやSSL-VPNを経由した社内システムへのリモートアクセス、SaaS利用にいたるまでほぼ全てのシステムへ多要素認証を適用していく

（パターン①：SaaSアプリの認証）

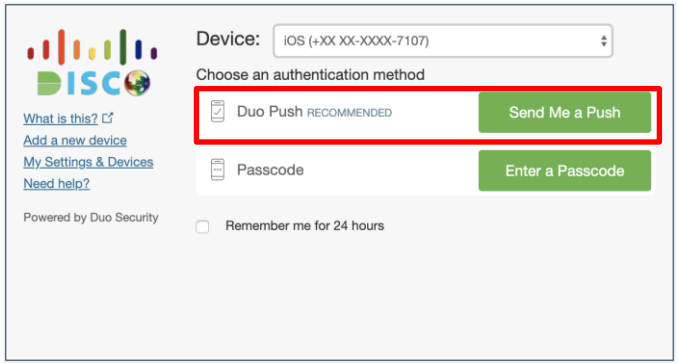
SaaSアプリ（Webex）ログイン時の多要素認証

1 Webexログイン – メールアドレス入力

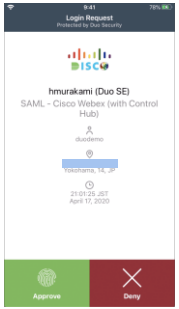
2 Duo DAG (SAML IdP) へリダイレクトし、プライマリ認証



3 多要素認証方法選択(Duo Push)



4 Duo Pushで認証



5 Webexログイン成功

（パターン①：SaaSアプリの認証）

Duo と Webex SAML連携

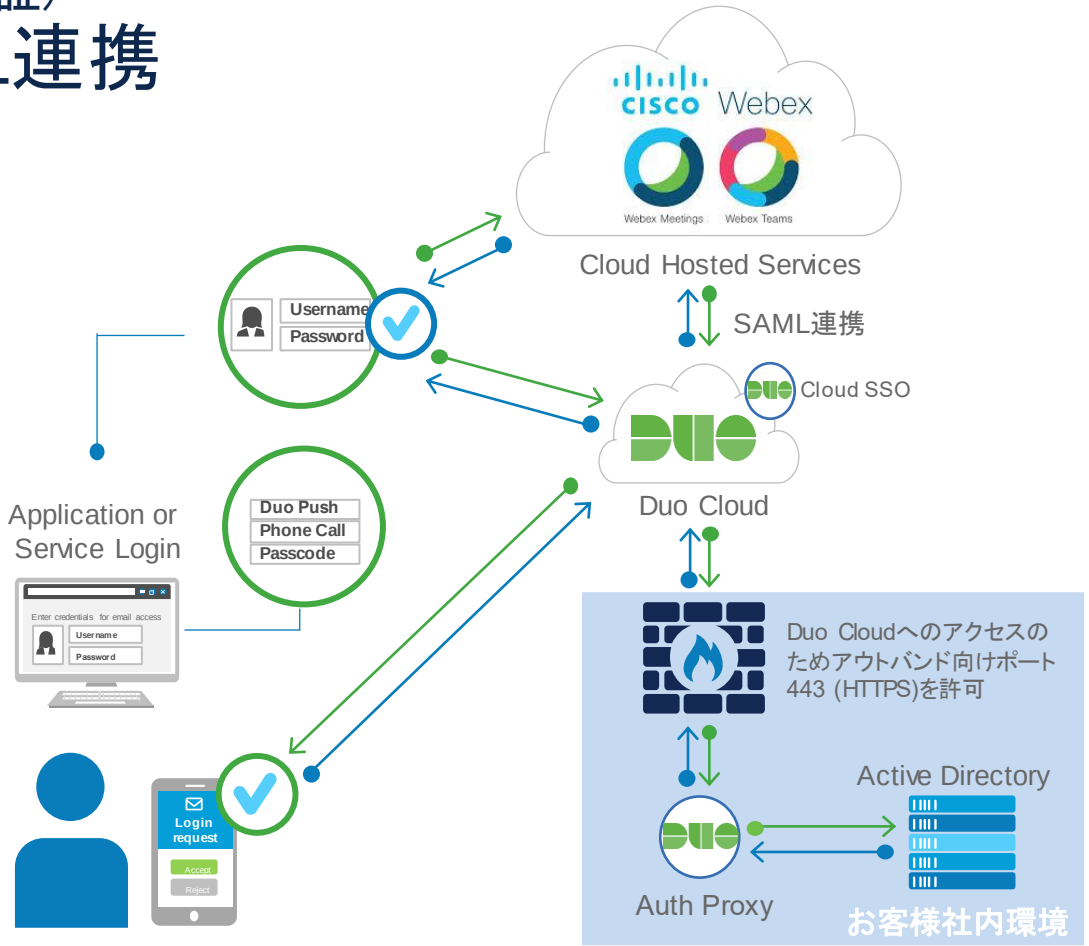
Webex SAML連携

概要:

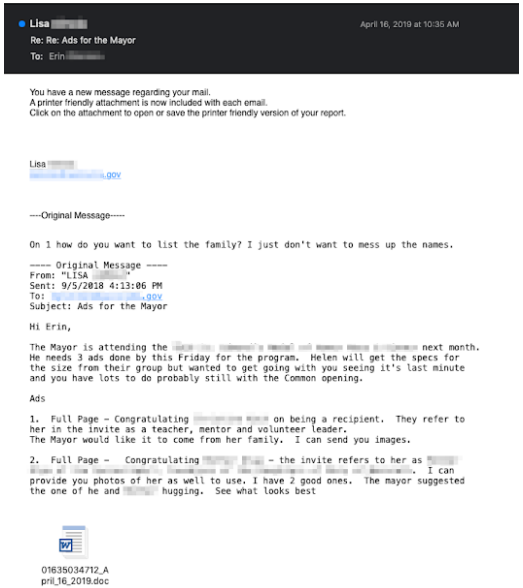
Webexに対し、DuoでSAML IdP機能を提供し、SSOと多要素認証を実現

特徴:

- SAML2.0をサポートして連携
- SSOソリューションを提供
- プライマリ認証とセカンダリ認証(2FA)を分離して多要素認証を実現
- デバイス検疫をしたデバイスからのみアクセス
- 証明書を利用して、管理端末のみにアクセスさせることが可能



（導入パターン①：SaaSアプリの認証）
送信メールで攻撃されるEmotetを阻止



Lisa [redacted] April 16, 2019 at 10:35 AM
Re: Re: Ads for the Mayor
To: Erin [redacted]

You have a new message regarding your mail.
A printer friendly attachment is now included with each email.
Click on the attachment to open or save the printer friendly version of your report.

Lisa [redacted]
[redacted].gov

---Original Message-----

On 1 how do you want to list the family? I just don't want to mess up the names.

----- Original Message -----
From: "LISA [redacted]"
Sent: 9/5/2018 4:13:06 PM
To: [redacted].gov
Subject: Ads for the Mayor

Hi Erin,

The Mayor is attending the [redacted] next month.
He needs 3 ads done by this Friday for the program. Helen will get the specs for
the size from their group but wanted to get going with you seeing it's last minute
and you have lots to do probably still with the Common opening.

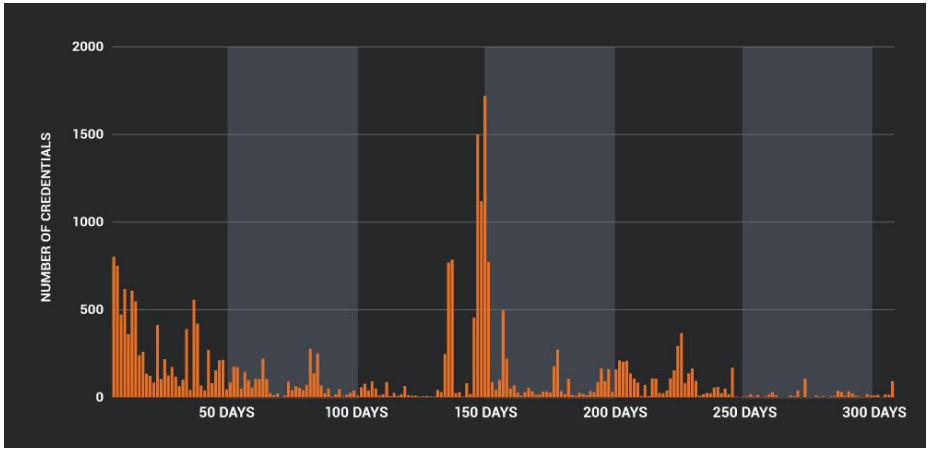
Ads

1. Full Page - Congratulating [redacted] on being a recipient. They refer to
her in the invite as a teacher, mentor and volunteer leader.
The Mayor would like it to come from her family. I can send you images.

2. Full Page - Congratulating [redacted] - the invite refers to her as [redacted]. I can
provide you photos of her as well to use. I have 2 good ones. The mayor suggested
the one of he and [redacted] hugging. See what looks best

01635034712_April_16_2019.doc

本文に加えて、メール送信に必要な情報（ユーザ名、パスワード、メールサーバ情報など）も盗む



Number of smtp Accounts	Password
401	123456
340	media@2018
252	ballia@159
205	123@babu
138	omics@123
134	pal-hari-
127	password
121	8960311541
120	1234
112	Welcome@123
103	123khushboo123
100	123omsai123
97	Dinesh@1234
97	12345678
96	test123
95	narendra@rudra852
87	12345
77	123456789
74	itechfast@1234512
72	Password1

メールを盗んで攻撃に利用
メールの続きだと考えてしまう

盗まれた後何ヵ月も悪用される

「123456」や「password」など問題のあるパスワードや、別アカウントで同じパスワードの使いまわしが致命傷に

（導入パターン①：SaaSアプリの認証）

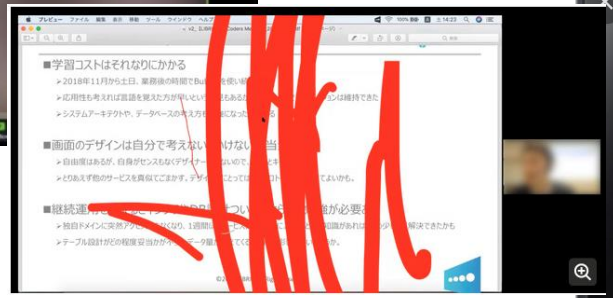
不正なWeb会議の参加を阻止

- 会議用URLの公開、画面共有の許可、参加者のリモート制御などの運用対策が徹底されない場合に、会議参加の許可に多要素認証も併用し、会議に参加できるユーザ・デバイスを信頼していいか確認する対策をとる

不正参加

ZoomBombing

画面共有



乗っ取り

盗聴

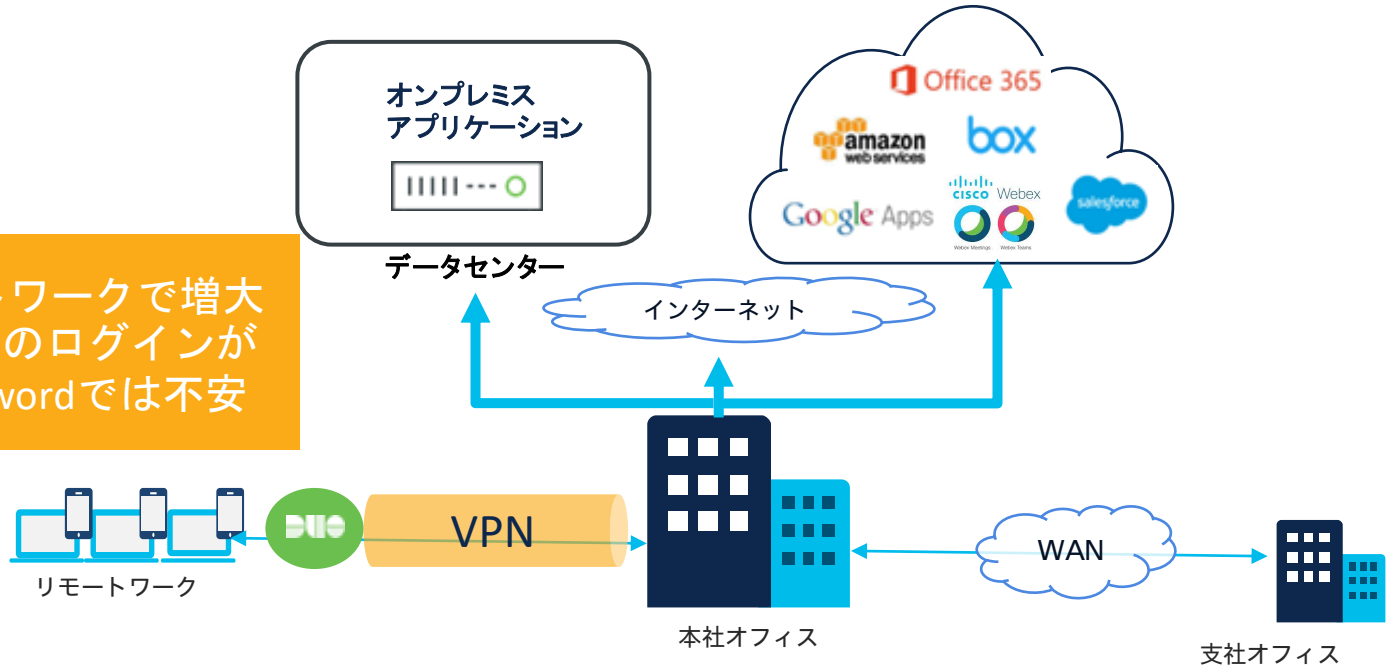
導入パターン②
VPN、VDIの認証

（パターン② ：VPN、VDIの認証）

VPN、VDIの入り口に多要素認証を導入

昨今のリモートアクセスの増大により、VPN経由でのアクセスが増え、VPNへのアクセスがIDとパスワードのみの場合には社内リソースがリスクにさらされている。

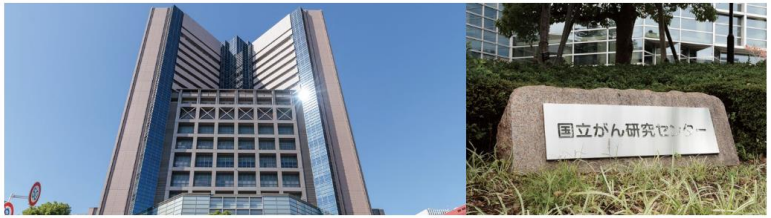
リモートワークで増大したVPNのログインがID/Passwordでは不安



お客様事例

（パターン② ： VPN、VDIの認証）

国立がん研究センター様



在宅勤務・リモートワーク環境におけるセキュリティ強化

多要素認証とPC健全性確認で安全性を高め
テレワーク拡大に向けた先行導入を実施

背景・課題

- COVID-19感染拡大によりテレワークの拡大が急務に
- 貸与PCの調達が難しい緊急事態に、自己保有PCの利用を決断
- 多要素認証によるユーザ確認とデバイスの健全性チェックを実施したい

ソリューション

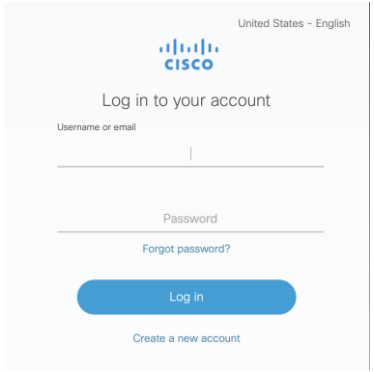
- 従来のAnyConnect（VPN）によるリモートデスクトップにDuoによる多要素認証とデバイス健全性チェックを追加
- ユーザの利便性を損なわずテレワークの安全性を強化

結果～今後

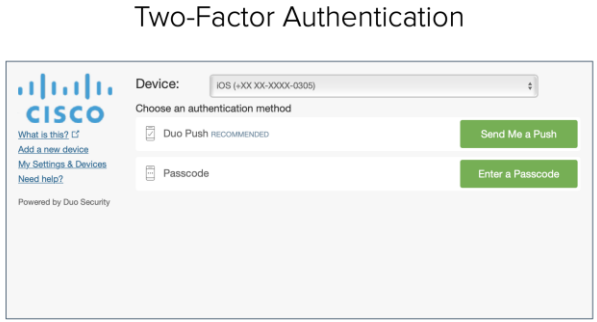
- 【構築】検討から約 1 ヵ月の短期間で立ち上げ
- 【運用】事務系職員約20名を対象としたテレワーク拡大トライアルを実行
- 【今後】ユーザのリテラシーやコスト面などを勘案しベストな方策を継続して検討

（パターン② ：VPN、VDIの認証）

VPNログイン時の多要素認証



ブラウザで自社独自のログイン

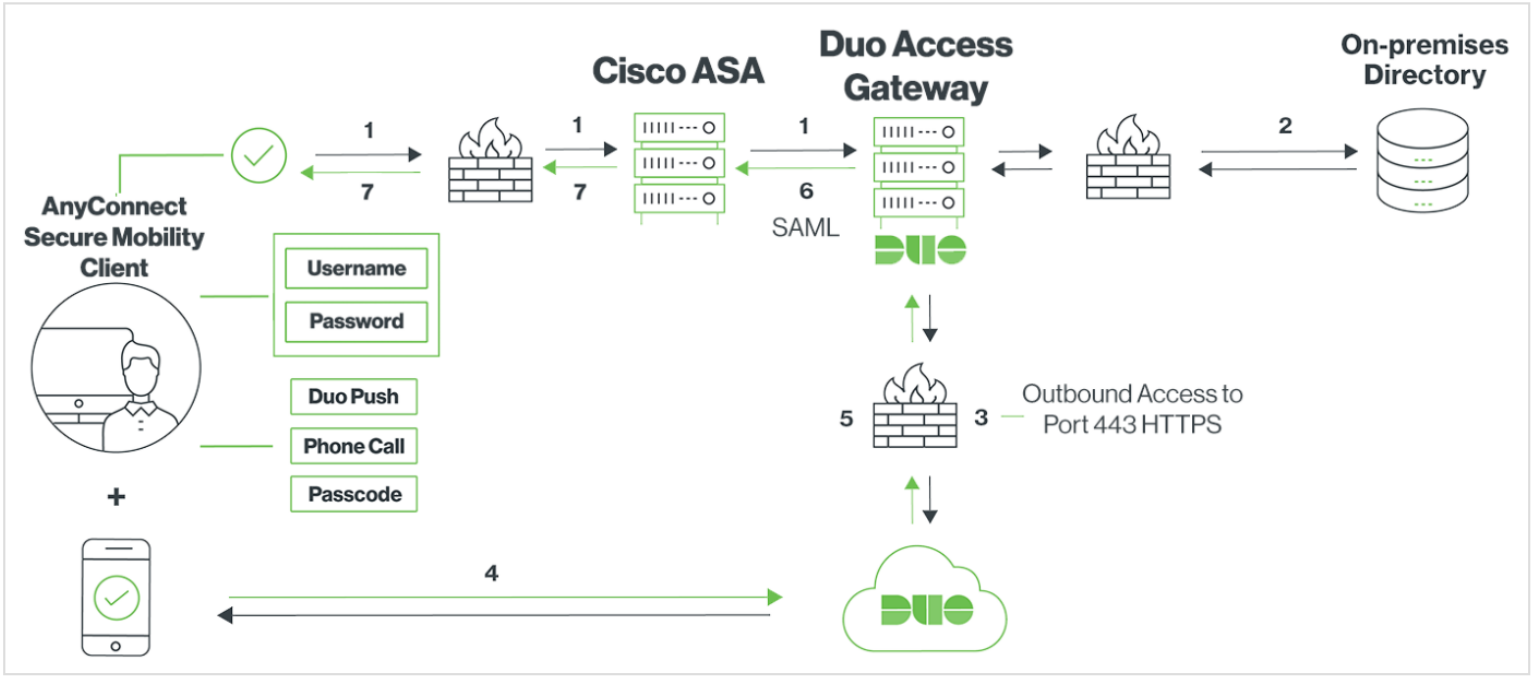


2要素目の指定（Duoプロンプト）

Duo Push等
2要素目の認証
左記は、
Duo Push＋FaceID

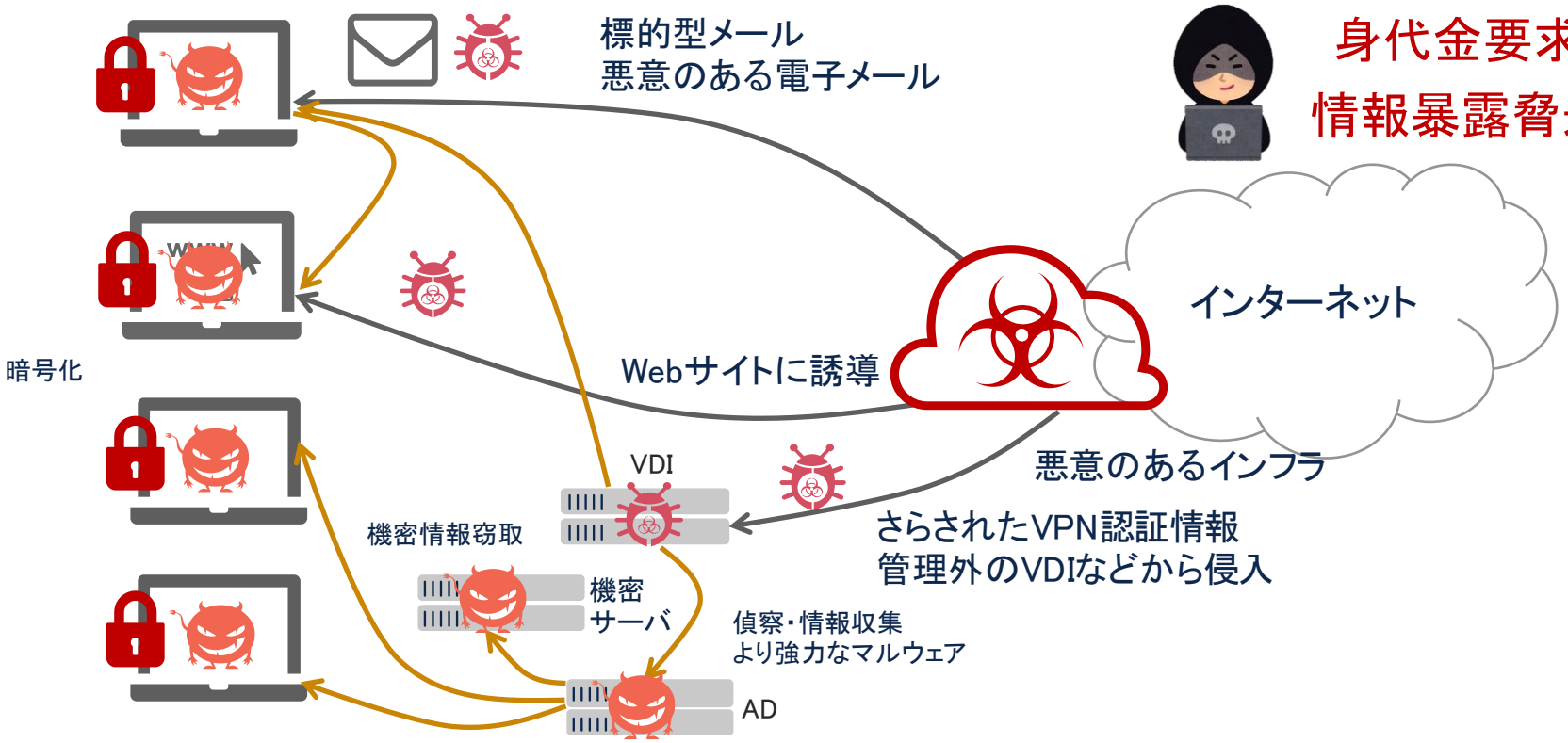
（パターン② ：VPN、VDIの認証）

DUOとASA/AnyConnectのVPN連携(SAML)



（導入パターン②：VPN、VDIの認証）

初期感染要因としてコロナ渦で狙われる（VPN,RDS,VDI）



1.侵入開始・初期感染

2.偵察行動・感染拡大

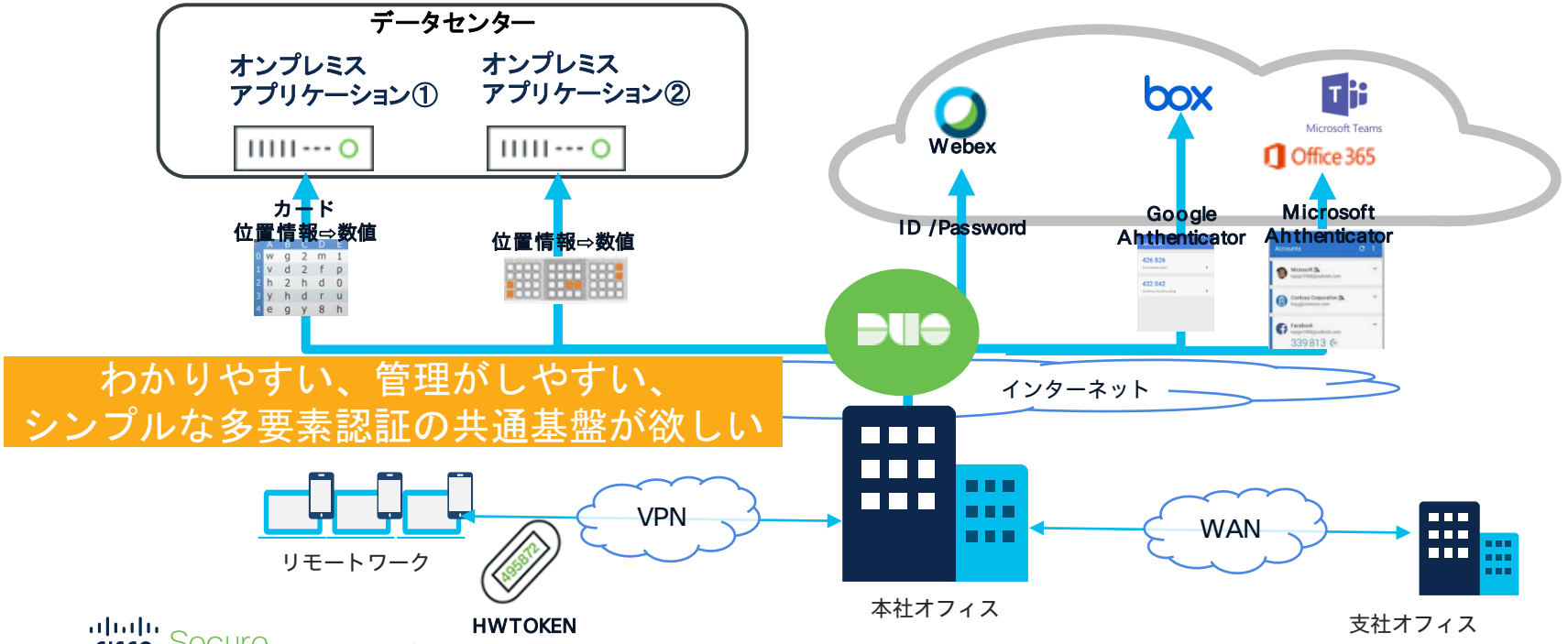
3.実行・被害

導入パターン③
既存の多要素認証の共通化

（パターン③：既存の多要素認証の共通化）

既存の共通化で新たな多要素認証を導入

- 既存の多要素認証の利用にユーザから不満がある。管理者として、複数の多要素認証を管理することに工数を要し、改善したい。といった要望から多要素認証を導入



お客様事例

（パターン③：既存の多要素認証の共通化）

製造業B社様

※グローバルで幅広い分野での機器メーカー、グローバルで世界各国に拠点を保持する企業

背景・課題

- 利用していた多要素認証の製品に不満を持っており、その代替製品を探していた。

多要素認証の要件

- ユーザビリティ（現在の商品よりもユーザビリティが落ちないこと）
- 導入が容易にできること（POVにてそれが確認できること）
- グローバルでのサポート体制があること
- サポート体制が整っていること

お客様の声

今回はMFAの代替での導入となったが、今後の利用システム拡大も見据えて**<u>汎用性の高いDuo</u>**を採用した

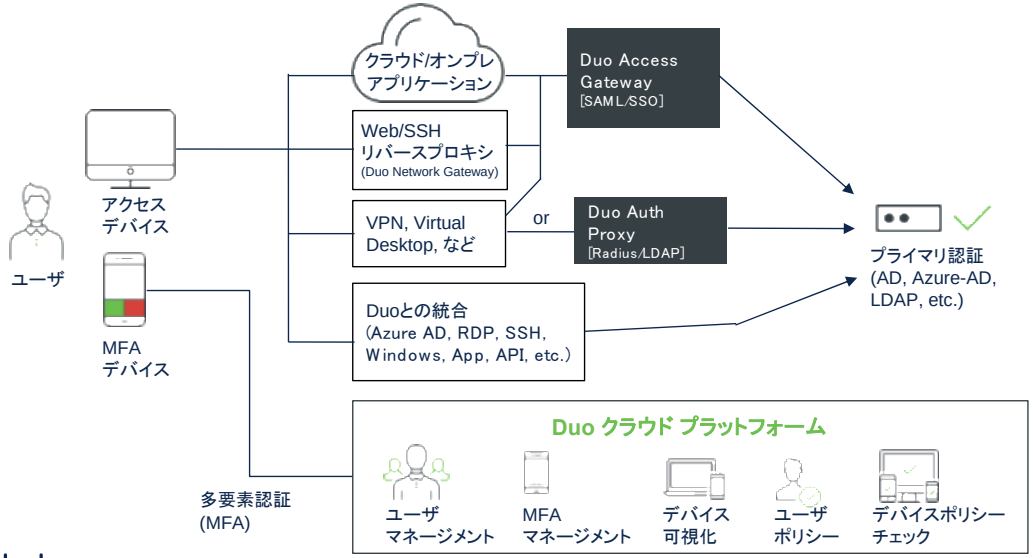
（パターン③：既存の多要素認証の共通化）多要素認証に求められる機能群

汎用性が高さと豊富なMFAオプション

- 汎用性の高いアーキテクチャーと豊富なMFAオプションで将来性を評価

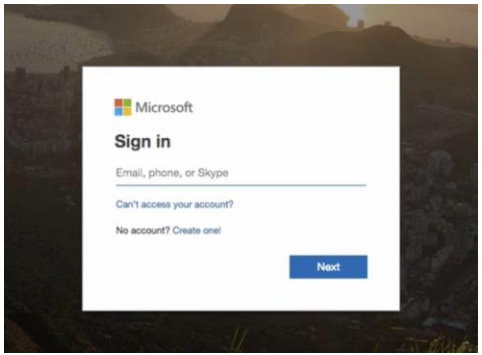
ほぼ全てのアプリケーションへ導入可能	豊富なMFAオプション

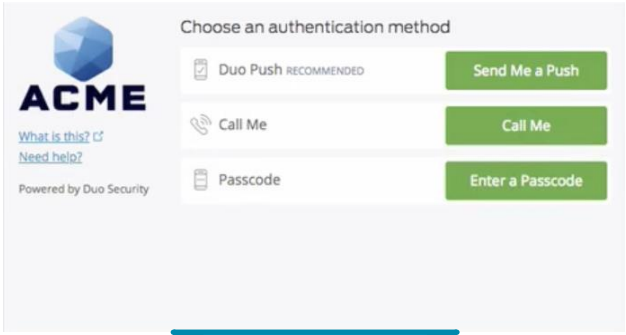
Duo アーキテクチャ 概要

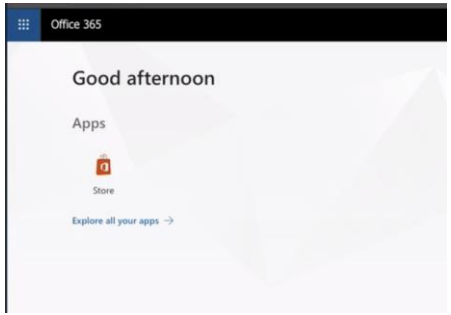


（パターン③：既存の多要素認証の共通化）多要素認証に求められる機能群

Azure AD連携（Conditional Access :O365）

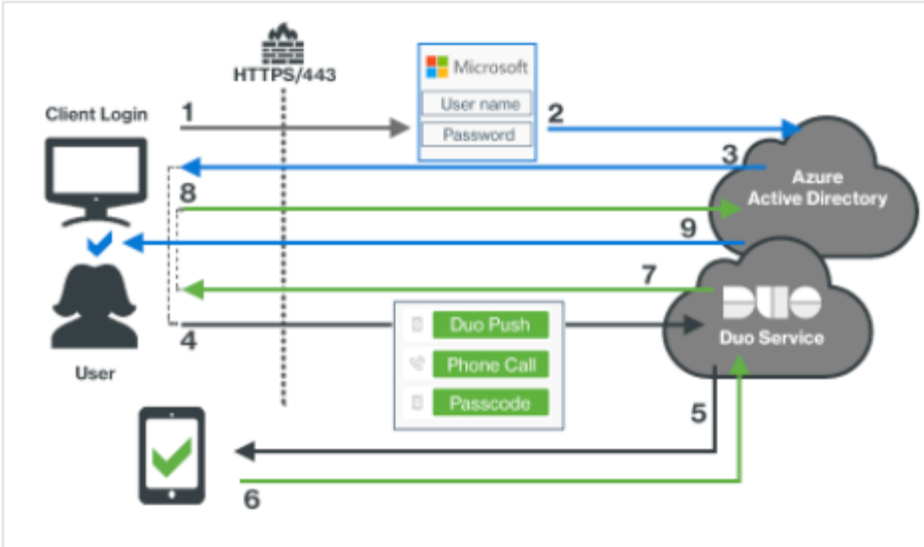


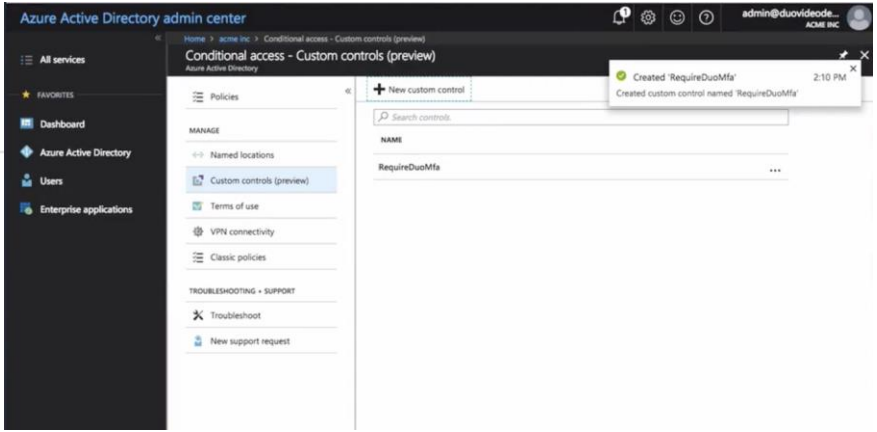


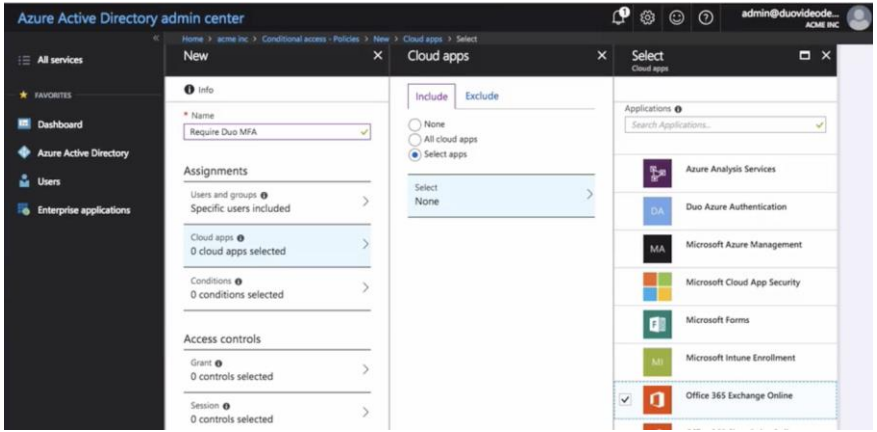


（パターン③：既存の多要素認証の共通化）多要素認証に求められる機能群

Azure AD連携（Conditional Access :O365）



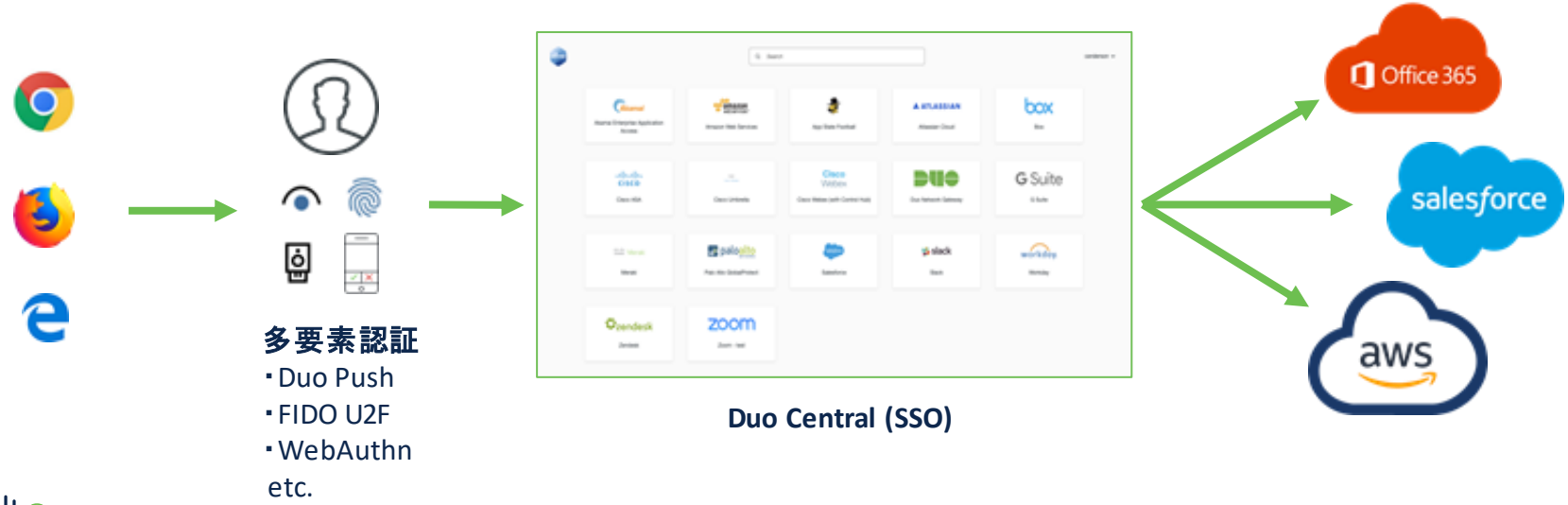




（パターン③：既存の多要素認証の共通化）多要素認証に求められる機能群

シングルサインオン（SSO）

- ユーザーは、Duo Central (SSO)を介して、SAMLフェデレーションされた任意のアプリケーションに任意のブラウザから接続できる



（パターン③：既存の多要素認証の共通化）多要素認証に求められる機能群

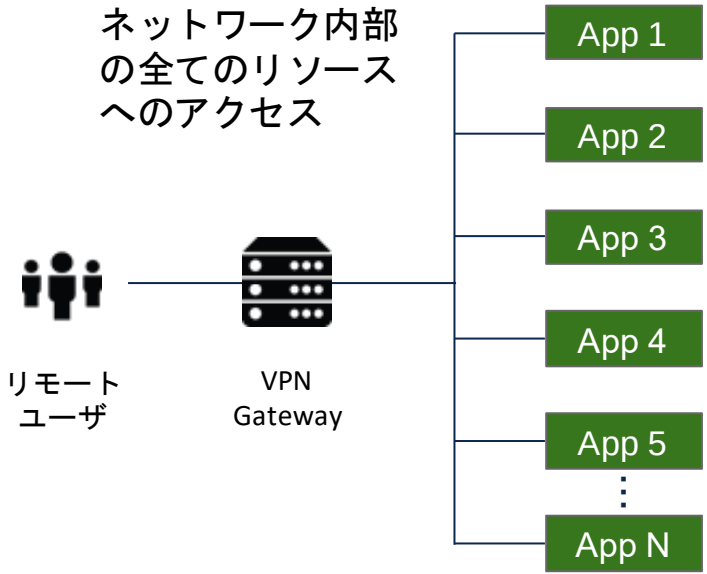
ネットワークとアプリケーションへのアクセス

セッション単位でアプリケーションごとの制御

VPN

VPN のアプローチ:

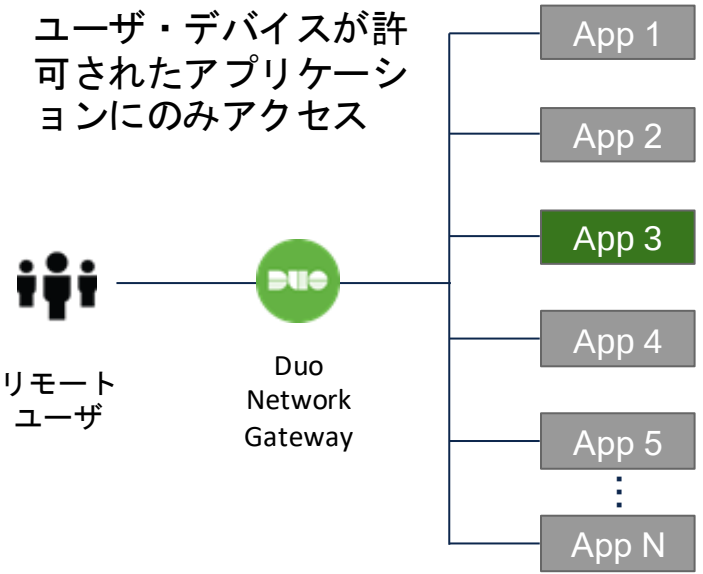
ネットワーク内部の全てのリソースへのアクセス



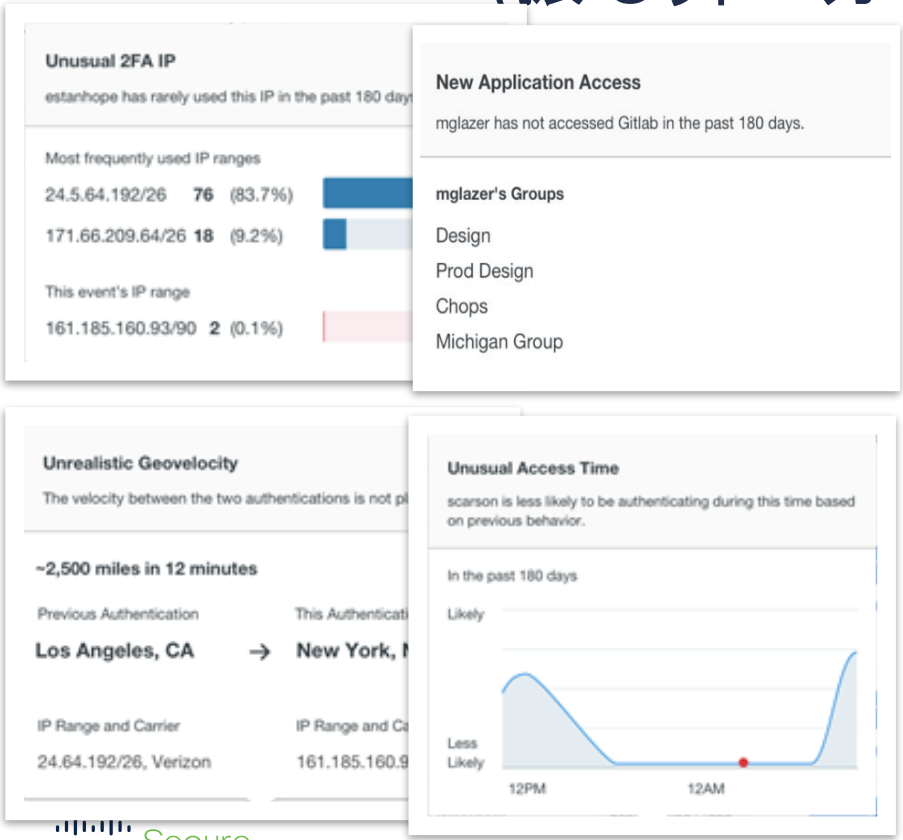
Duo Network Gateway

DNG のアプローチ:

ユーザ・デバイスが許可されたアプリケーションにのみアクセス



（パターン③：既存の多要素認証の共通化）多要素認証に求められる機能群
Trust Monitor (振る舞い分析、脅威検知)



Duo Trust Monitor は、企業/組織環境でアクセスアクティビティの調整されたベースラインを作成：

- 通常アクセスする人
- どのアプリケーション
- どのデバイスから
- いつ（時間）
- どこから（場所）

Trust Monitor機能により、異常または危険なユーザー認証の試みをハイライトし、アクセスポリシーを修正または更新することができる。

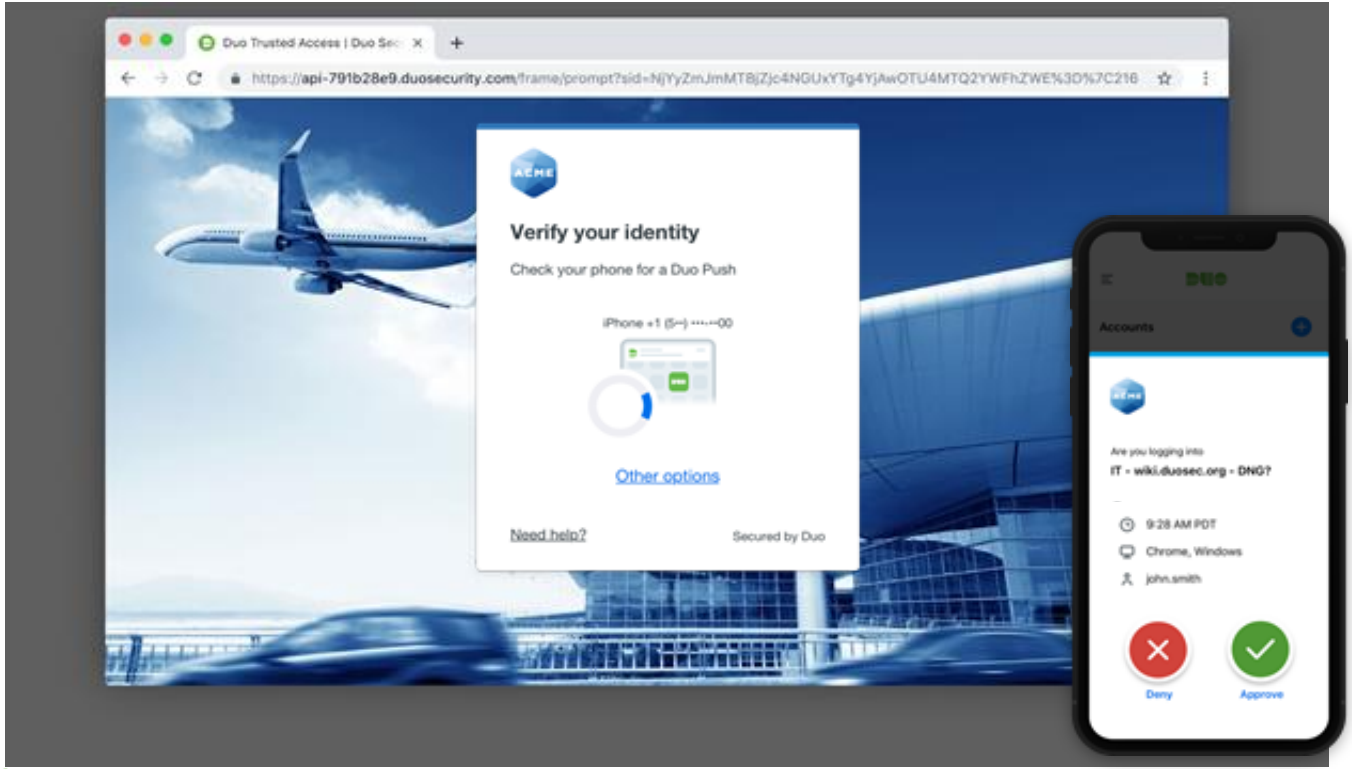
（パターン③：既存の多要素認証の共通化）多要素認証に求められる機能群

多要素認証とエンドポイントセキュリティの連携

- Duo + Cisco の新しい統合機能 (Windws10は既にサポート済み、MacOSは将来サポート予定)
- AMP4Eによって侵害されたと見なされるエンドポイントから、Duoで保護されたアプリケーションへのアクセスを防ぐ
- ユーザは、Duoポリシーに適合する別の正常なエンドポイントからのアクセスは可能
- 他のポリシー制御と同じように、グローバル、アプリケーション、ユーザグループのスコープで実施
- AMPクラウドで修正されたエンドポイントは、自動的にアクセス可能となる

（パターン③：既存の多要素認証の共通化）多要素認証に求められる機能群

エンドユーザの利用しやすさ（ユニバーサルプロンプト）

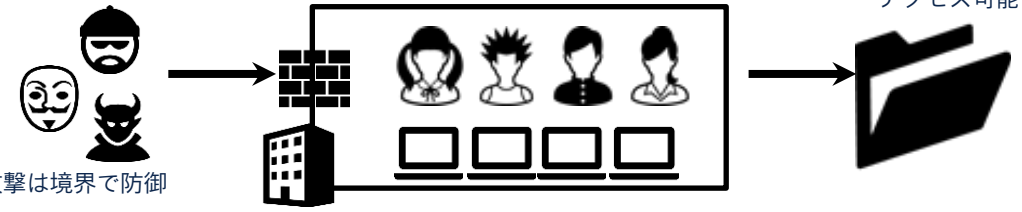


（パターン③：既存の多要素認証の共通化）多要素認証に求められる機能群

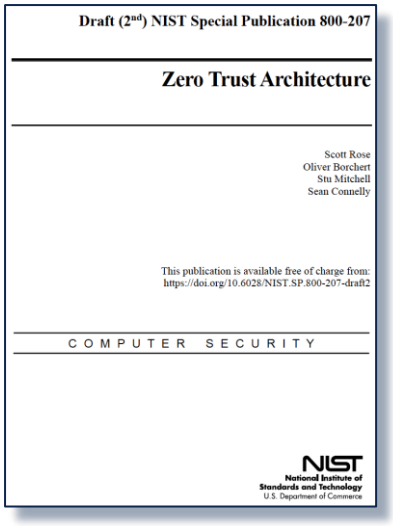
日本語UI（ユニバーサルプロンプト）

✓ 直近でよく利用するオプションが優先されるが、登録されている他のオプションから選択することも可能

旧来の考え方



ゼロトラストの考え方



NIST SP 800-207
Zero Trust Architecture

Zero Trust 目標:
必要最小限の特権のみをアクセスに付与しリソースを制限
リソースの保護方法、信頼が暗黙に付与されず、継続的に
評価

守れる被害・ユースケース：ゼロトラストによる信頼の確立

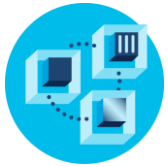
これまでの対策と課題

ユーザ名・パスワード定期的変更

複雑なパスワードで！

- VPN情報乗っ取り犯罪
- 情報を盗まれて侵入される

静的ポリシーでの通信制御



継ぎ足しACLで守る！

- 内部可視化へは未着手
- 侵入後は静的ポリシーの範囲で自由に行動

とにかくマルウェアを検知する

マルウェア検知99%！

- 特定の標的マルウェア
- 1つの侵入で十分

これからの対策＝ゼロトラスト

パスワードが盗まれても
不審者かどうか
不適切な端末でないか
見極める仕組みが必要

多要素認証
Duo

- 多要素認証に加え
- アップデート必要なデバイスをを許可しない
- 10分後の遠隔地でログインブロック
- 突然深夜にログインすると警告

異常な振る舞いや
疑わしい通信を
検知して対処する
仕組みが必要

- 通信を継続的に診断し、ラテラルムーブメントを防止する

アプリ保護
Tetration

- ネットワーク脅威検知と対処
- 正しいユーザとデバイスを継続的に診断

脅威検出
StealthWatch

脅威収集・隔離
ISE

感染が広がっても
初期感染者や
どこまで広がっているか
の把握して対処する
仕組みが必要

- マルウェアを継続的に可視化して、ネットワークレベルで制御

マルウェア対策
AMP/TG

脅威収集・隔離
ISE

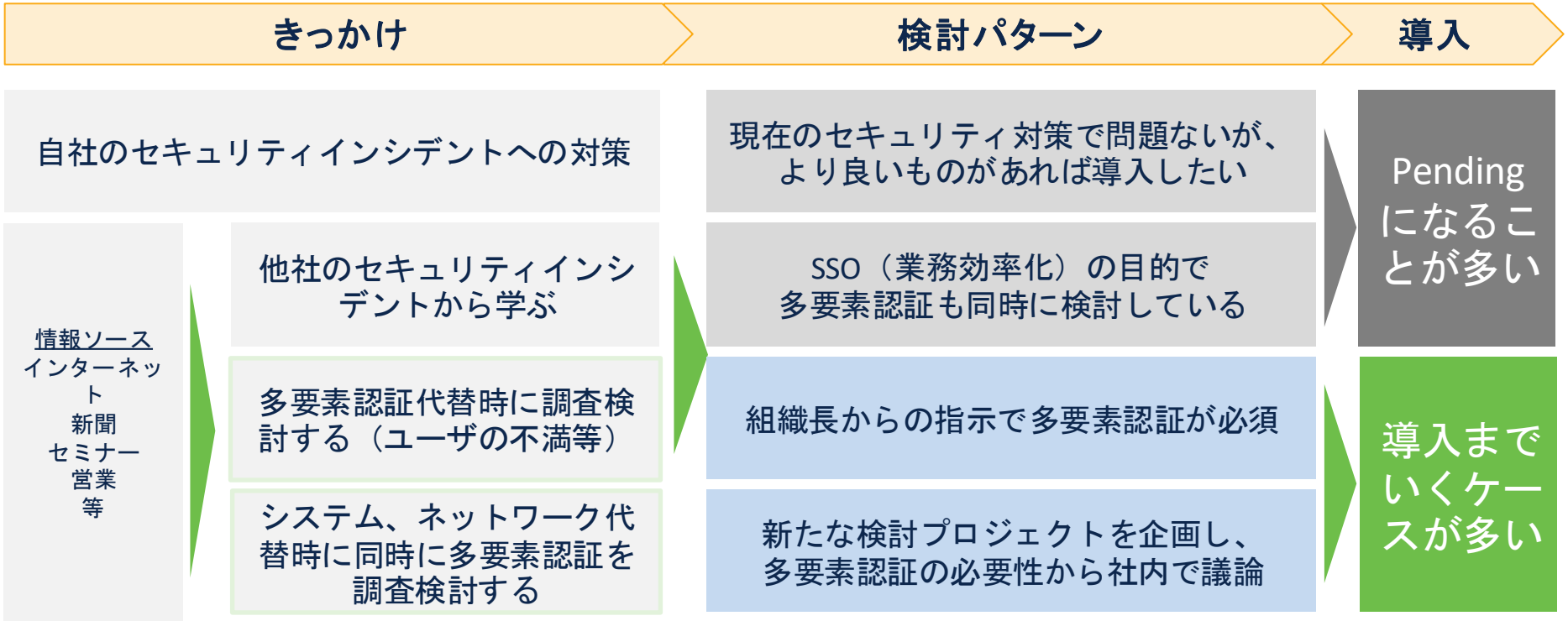
cisco Secure

信頼の確立・信頼に応じた制御・継続的な診断

検討パターン③
多要素認証の検討から導入まで

多要素認証の検討パターン

- 多要素認証検討のきっかけは様々だが、実際に導入するパターンは限られる



本日のまとめ

本日のまとめ
（多要素認証の始め方　事例に基づくパターン別解説）

【背景】
リモートワークが急速に普及する中で、サイバー攻撃は高度化しており、情報資産を守るために多要素認証は必須となってきている。

【多要素認証の導入パターンは3パターン】
① SaaSアプリの認証
② VPN、VDIの認証
③既存の多要素認証の共通化

【多要素認証の検討を進めるために】
セキュリティを目的に、多要素認証を進める社内の意思決定またはプロジェクトを企画することが出発点

Q&A

ご質問、ご意見があれば、Q&Aパネルに
ご記入ください。


cisco
Secure