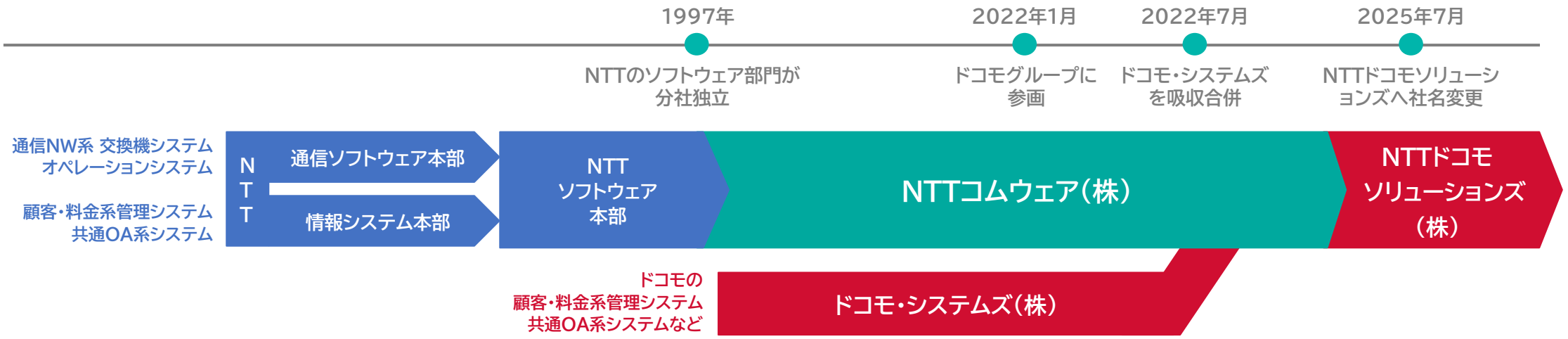
信頼される企業になるための セキュリティの極意

ドコモの経験に学ぶ、ゼロトラスト時代のセキュリティ対策

NTTドコモソリューションズのご紹介

- ✓ NTTグループ、ドコモグループのITインフラ、情報システム、情報セキュリティの**開発・維持・運用を担う専門家集団**
- ✓ ドコモグループ連携強化の一環で、2025年7月から「NTTドコモソリューションズ」へ

社名	エヌ・ティ・ティ・ドコモソリューションズ株式会社
本社所在地	〒108-8019 東京都港区港南1-9-1 NTT品川TWINS アネックスビル
資本金	200億円
株主	株式会社NTTドコモ（66.6%） 日本電信電話株式会社（33.4%）
売上高	2,510億円（2024年4月1日～2025年3月31日）
営業利益	170億円（2024年4月1日～2025年3月31日）
社員数	5,083名（2025年3月末）



本日のアジェンダ

1. ドコモがゼロトラスト環境に移行した背景
2. ドコモのゼロトラスト環境をお客様に提供するにあたっての苦労
3. NTTドコモソリューションズの「ゼロトラスト型セキュリティサービス」ご紹介

1

ドコモグループが
ゼロトラスト環境に移行した背景

今更ですが。。。

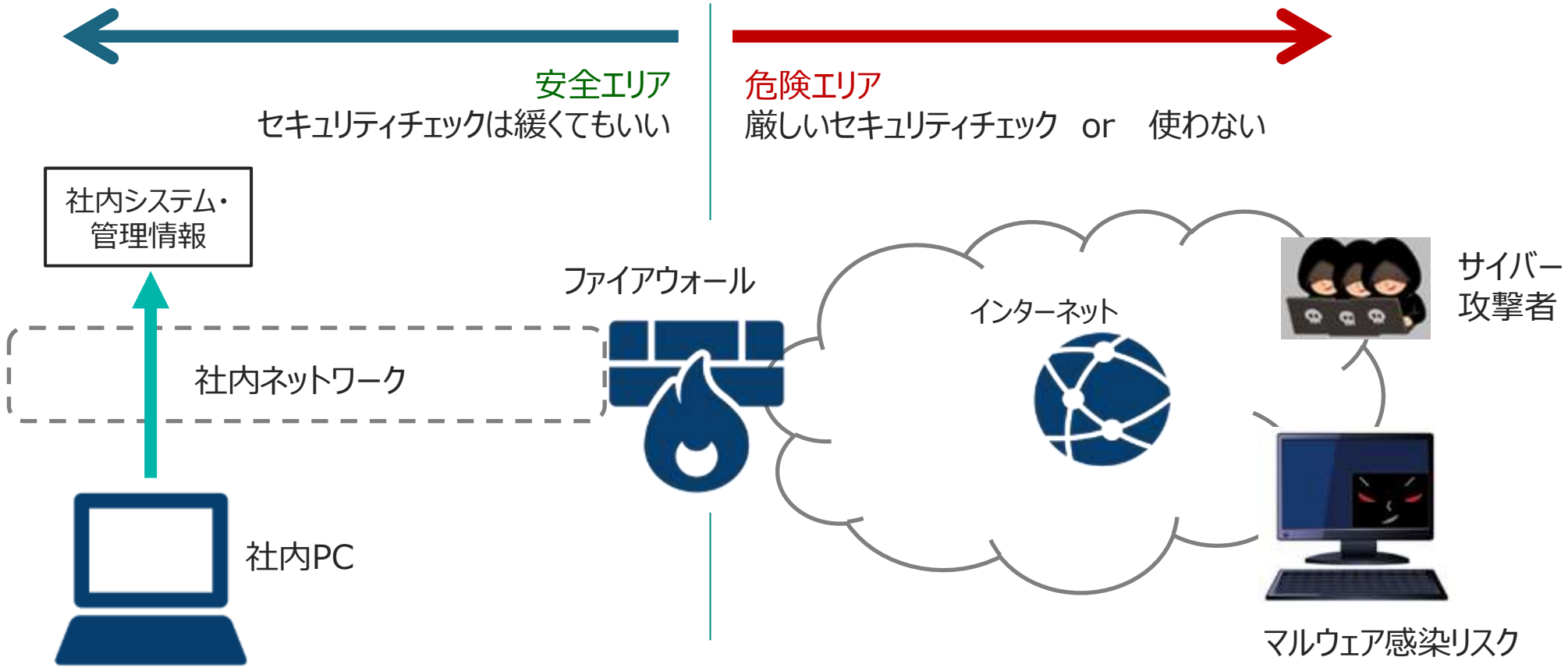
ゼロトラストとは？

ゼロトラストモデルセキュリティは、境界型セキュリティ(ペリメタモデル)のように「**Firewallの内側は安全**」と考えるのではなく、ネットワーク上の「**いかなる場所でも安全ではない**」との考え方を前提に情報アクセスのセキュリティを確保する“考え方”

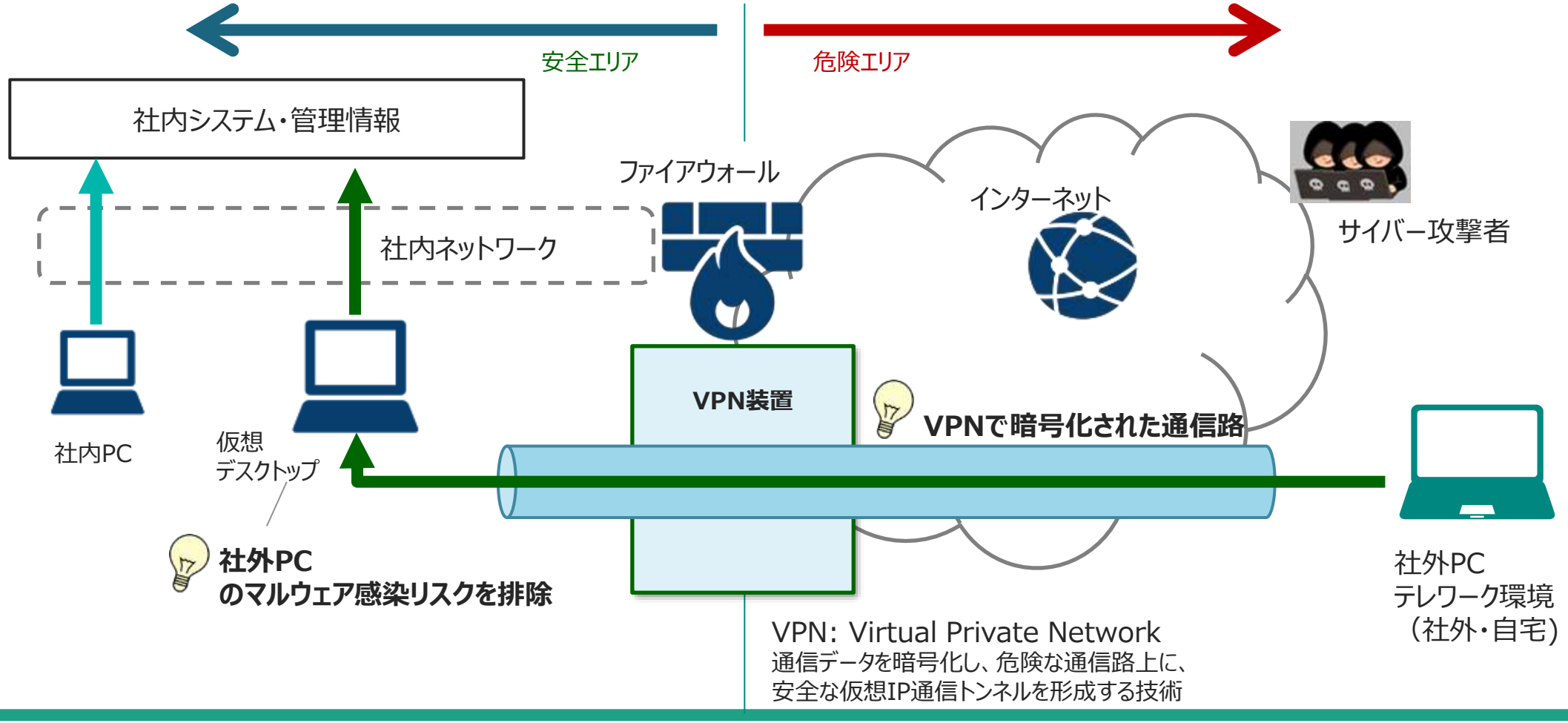
境界型(Perimeter)モデル	ゼロトラストモデル
情報のありかは、**社内**(Firewallの内側)	**情報**のありかは、主に**クラウド**上
Firewallの内外で**認証方法が異なる** 内側(社内)では認証がないことも許容	IDにより認証、アクセス権を**都度確認する**
Firewallの**内側のPCを管理**する 外側のPCはから直接業務情報にアクセスさせない	接続位置に関わらず **安全に管理された端末**からアクセスさせる
VPNを使って、 社内PCと同じ情報アクセス経路にする	すべての場所から**最適な経路で** 情報にアクセスする

境界型(ペリメタ)のセキュリティとは

インターネットと社内ネットワークの接続点に設置されるFirewall装置を境界線(Perimeter)として、内側(安全と考える)と外側(危険と考える)でセキュリティ制御が異なる

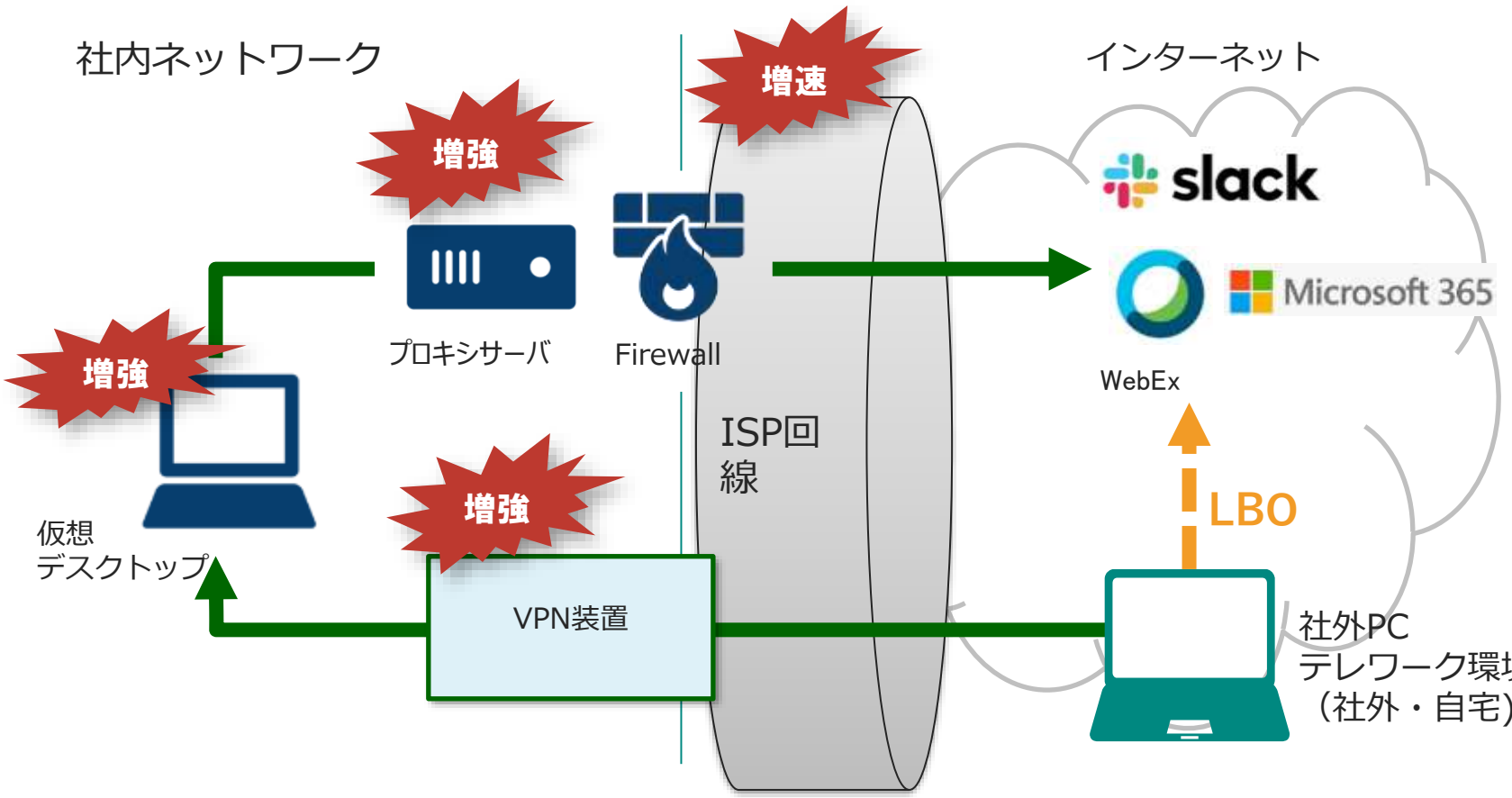


境界型(ペリメタ)モデルでのテレワーク環境



境界型(ペリメタ)モデルの限界

コロナ禍をきっかけとして、リモートワーク時のコミュニケーションツールとして、slackやWebExといったパブリッククラウドの利用が増えた
また、内製の社内システム→Microsoft365中心の業務環境に移行した



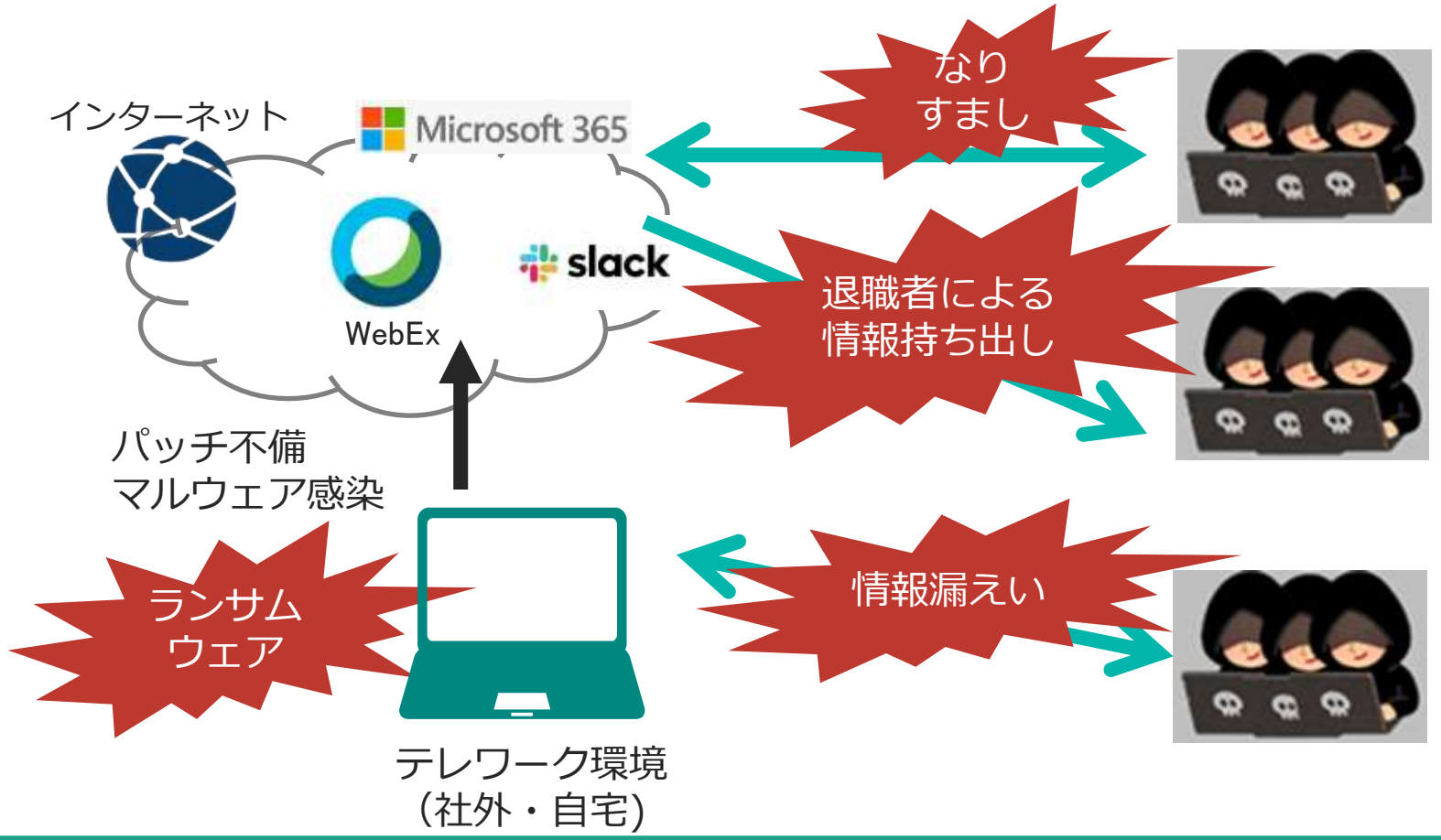
クラウドサービスを利用するため、社内とインターネット接続点をトラヒックが往復する

社内とインターネット回線の帯域、VPN、インターネット接続装置の増強

クラウドサービスへのアクセスは最適経路でオフロードする
LBO: Local Break Out

パブリッククラウド活用/LBOの課題

なにもセキュリティ対策せずに、
パブリッククラウドへの移行や
クラウド通信の経路変更だけするのは危険



(参考)2024年のNTTグループへの攻撃状況

攻撃メール数
1億4000万通

攻撃メールの内、大半はフィッシングメール。
攻撃メールの内、99.2%はメールボックス着弾前にブロック。

EDRでの検知数
2万4000件

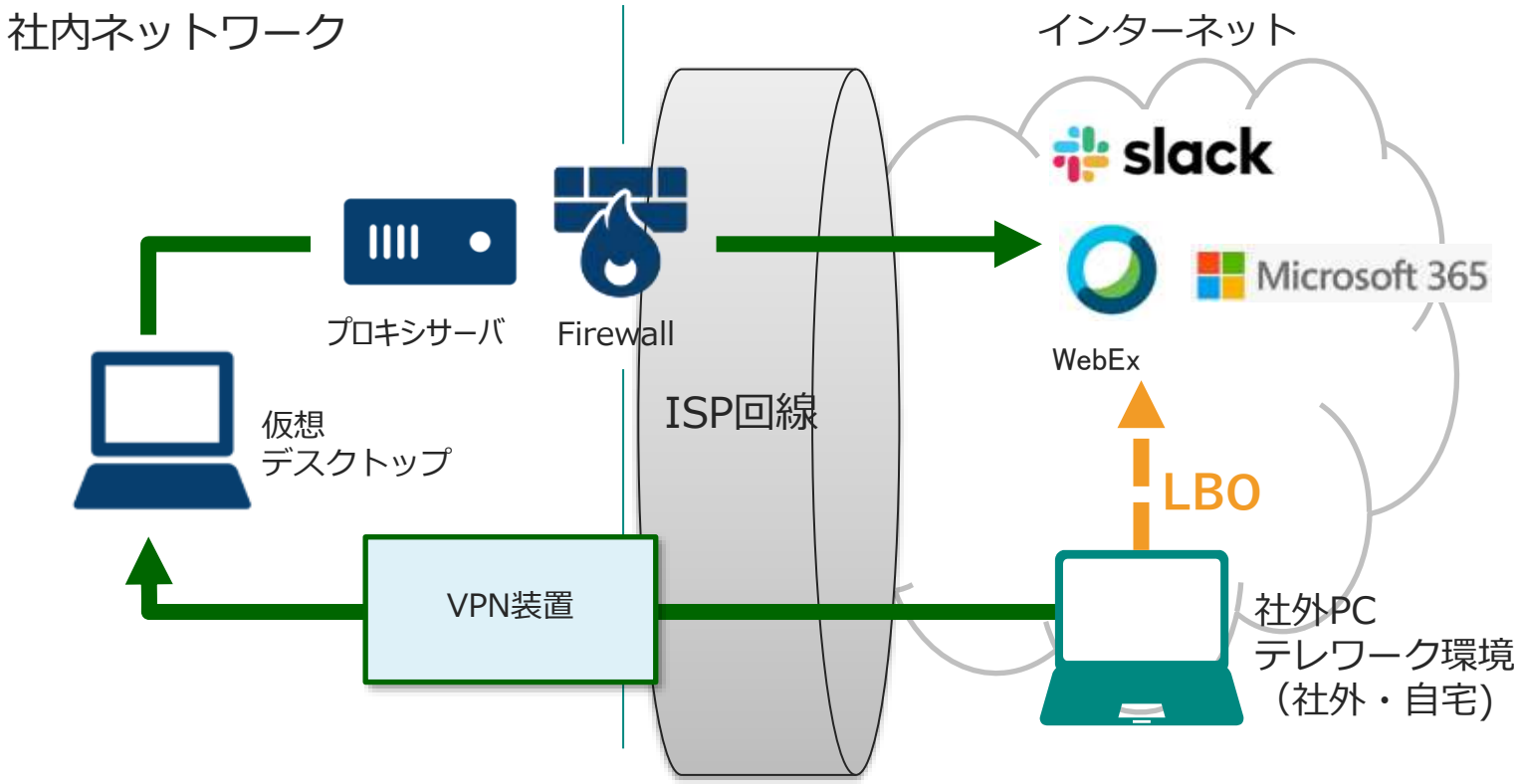
大半は過検知だが、約200件のアラートについては真に脅威があると思わしきアラートであり、対処が必要だった。

Web通信のブロック数
17億件

総通信数350億件のうち、当社独自に設定したブロックリストに合致する通信の数。

ゼロトラストモデルの採用

パブリッククラウドの活用やローカルブレイクアウトの導入により、発生する新たな脅威に対応するため、ゼロトラスト型のセキュリティを採用



クラウドサービスを利用するため、社内とインターネット接続点をトラヒックが往復する

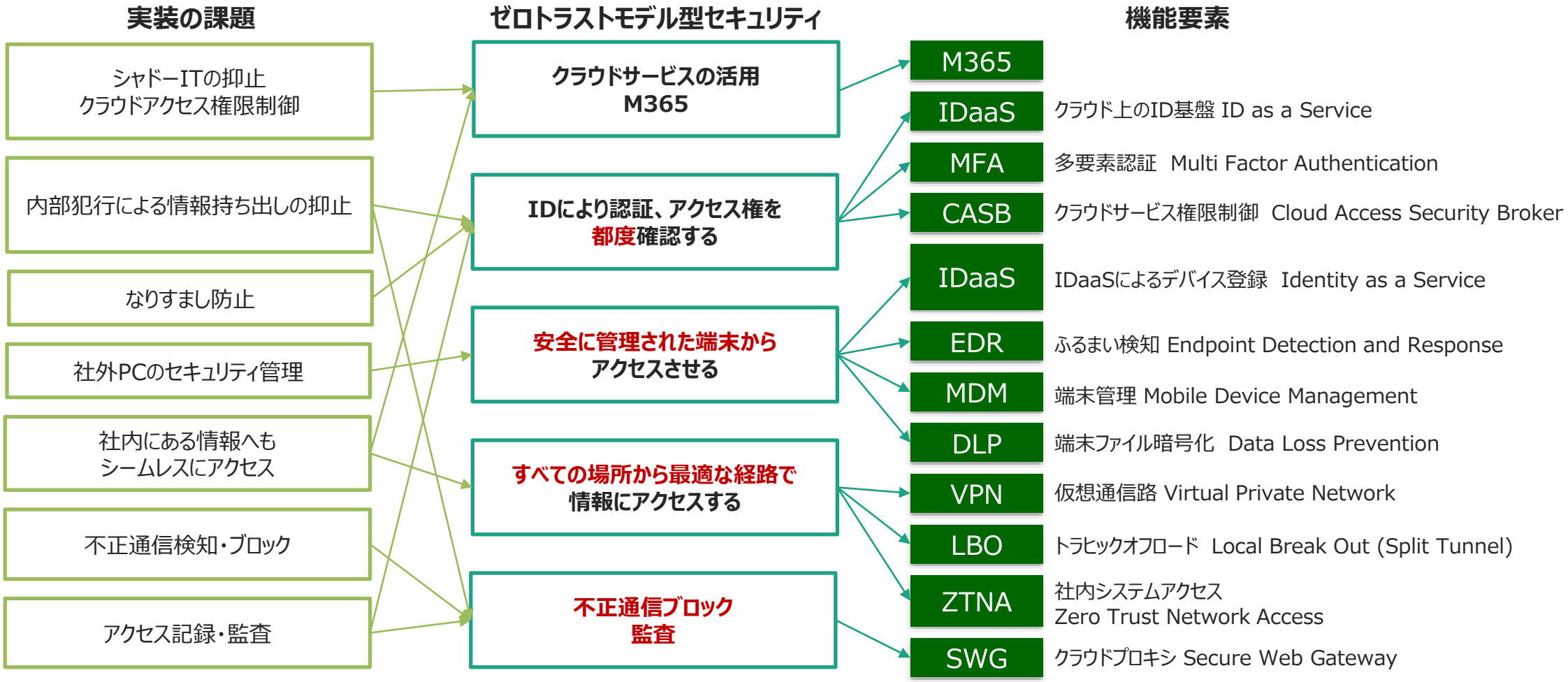
社内とインターネット回線の帯域、VPN、インターネット接続装置の増強

クラウドサービスへのアクセスは最適経路でオフロードする
LBO: Local Break Out

なりすましアクセス、
内部犯行による情報持ち出し、
端末のマルウェア感染

ゼロトラスト型セキュリティの実装が必要

ゼロトラストモデル導入の道筋



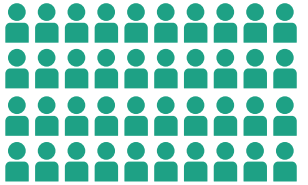
(参考)ドコモGrのゼロトラスト実装状況

ZTXフレームワーク構成要素	機能	機能概要	ドコモGrの実装状況
アイデンティティセキュリティ	IDaaS	ID管理、SSO、アクセス条件制御	○
	MFA	多要素認証	○
ネットワークセキュリティ	SWG	Webアクセスセキュリティ	○
	ZTNA	社内アプリ含むアプリケーションへの安全なアクセス	○
デバイスセキュリティ	EDR	エンドポイントのふるまい検知・対応	○
	MDM	モバイルデバイス管理	○
	MAM	モバイルアプリケーション管理	○
ワークロードセキュリティ	CWPP	クラウドワークロードの脅威検出と防御	×
	CSPM	クラウドの設定管理	×
データセキュリティ	DLP	情報のタグ付け、漏洩対策	○
	ファイル暗号化	-	○
セキュリティの可視化と分析	CASB	クラウドサービスアクセス制御	○
	SIEM	ログ収集、分析	○
	UEBA	機器のログをベースとしたふるまい検知	×
セキュリティの自動化	SOAR	インシデント対応の自動化	△(検討中)

凡例： Microsoft Cisco

初期構築期間 約1年間

構築に携わった人数



数知れず

社員のみではなく、ビジネスパートナーやベンダの協力も得ながら構築を実施。

MicrosoftやCisco社のゼロトラスト系サービスを中心に、必要な機能を選定し実装していった。

まとめ

1. コロナ禍でのリモートワーク中心の働き方への移行をきっかけとして、境界型(ペリメタ)のセキュリティに限界を感じた
2. インターネット環境で業務を完結させるために、クラウドシフトとLBOを検討した
3. 端末が社内LANではなくインターネットに直接接続することになるので、様々な脅威に対応する必要があった
4. 脅威に対処するための課題を洗い出し、その課題に対処するのに必要な機能を取り揃え、構築していった

2

ドコモのゼロトラスト環境を
お客様に提供するにあたっての苦労

誰でも最初は初心者

ゼロトラは、ある朝突然に

ある日の社員A

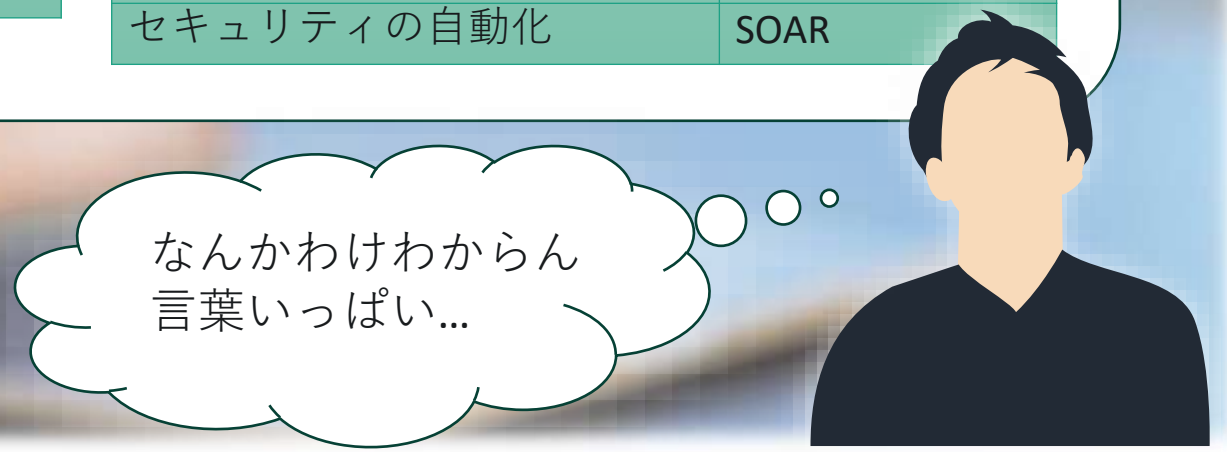

偉い人
ドコモのゼロトラスト環境ってお客様に売れるんじゃね？
サービス化してね
えー！無理
でも頑張りまーす
社員A

まずやったこと

ゼロトラストについて調べてみたが・・・

アイデンティティセキュリティ	IDaaS
	MFA
ネットワークセキュリティ	SWG
	ZTNA
デバイスセキュリティ	EDR
	MDM
	MAM

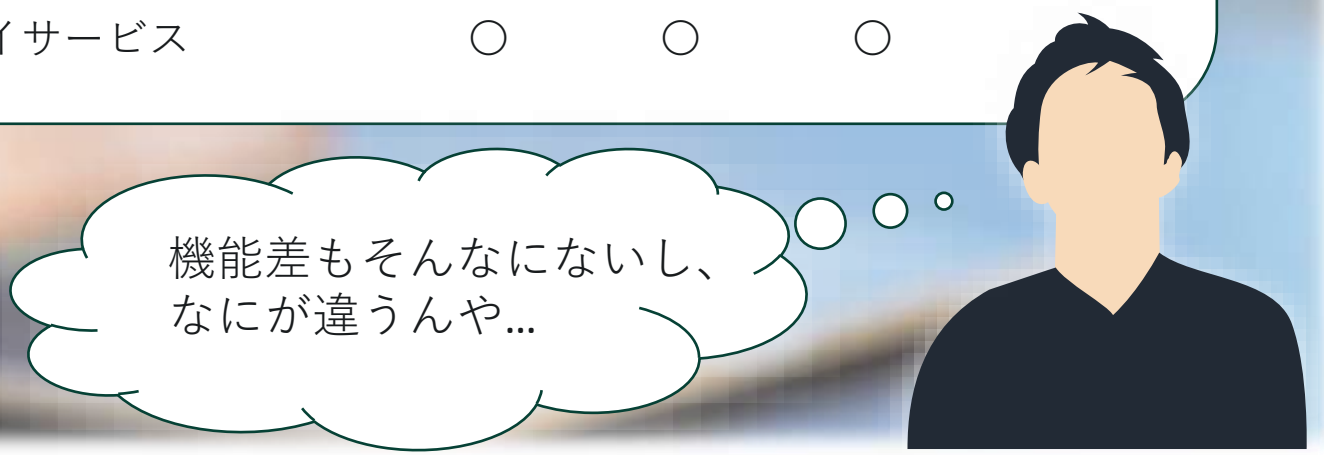
ワークロードセキュリティ	CWPP
	CSPM
データセキュリティ	DLP
	ファイル暗号化
セキュリティの可視化と分析	CASB
	SIEM
	UEBA
セキュリティの自動化	SOAR



機能カテゴリ毎に製品調査してみた

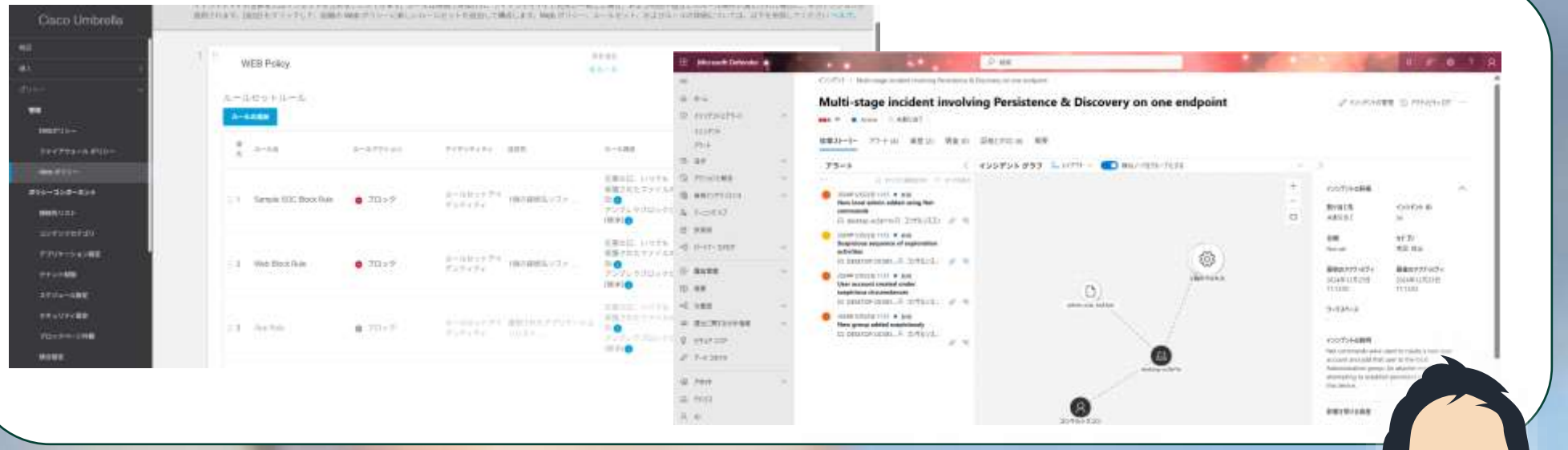
SWGの製品を調査したが・・・

	機能A	機能B	機能C
Cisco Umbrella	○	○	○
i-FILTER@Cloud	○	○	△
Zscaler Internet Access	○	○	○
Symantec Web Security Service	○	△	○
iboss cloud platform	○	△	○
Netskope	○	○	△
IIJセキュアWebゲートウェイサービス	○	○	○



トライアル利用してみた①

MicrosoftやCiscoのサービスの管理画面を操作してみると・・・



トライアル利用してみた②

MicrosoftやCiscoのサービスの管理画面を操作してみると・・・

社員Aのイメージ

- デフォルト設定1
- デフォルト設定2
- ⋮
- デフォルト設定X

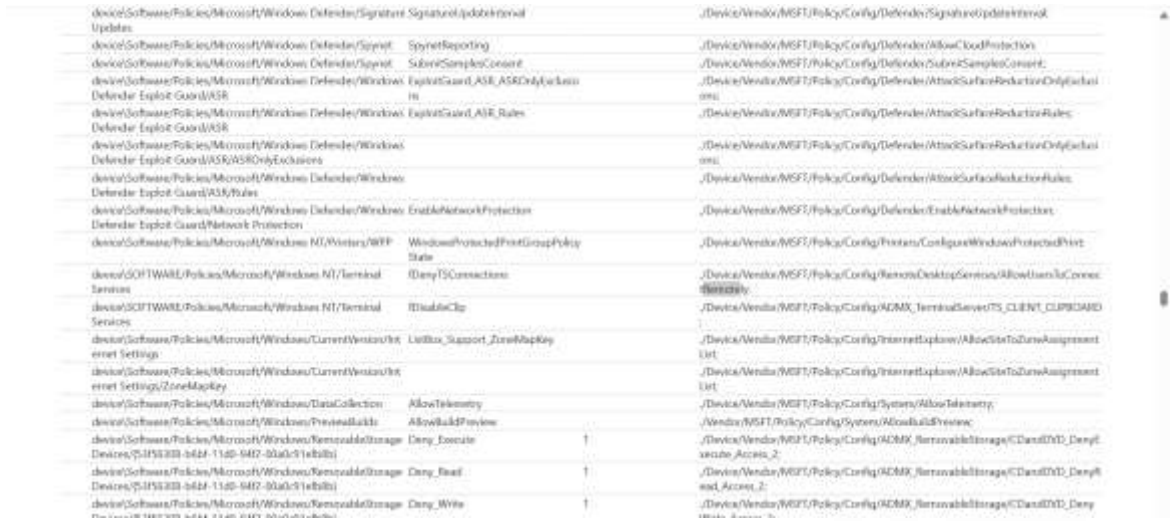
実際には…

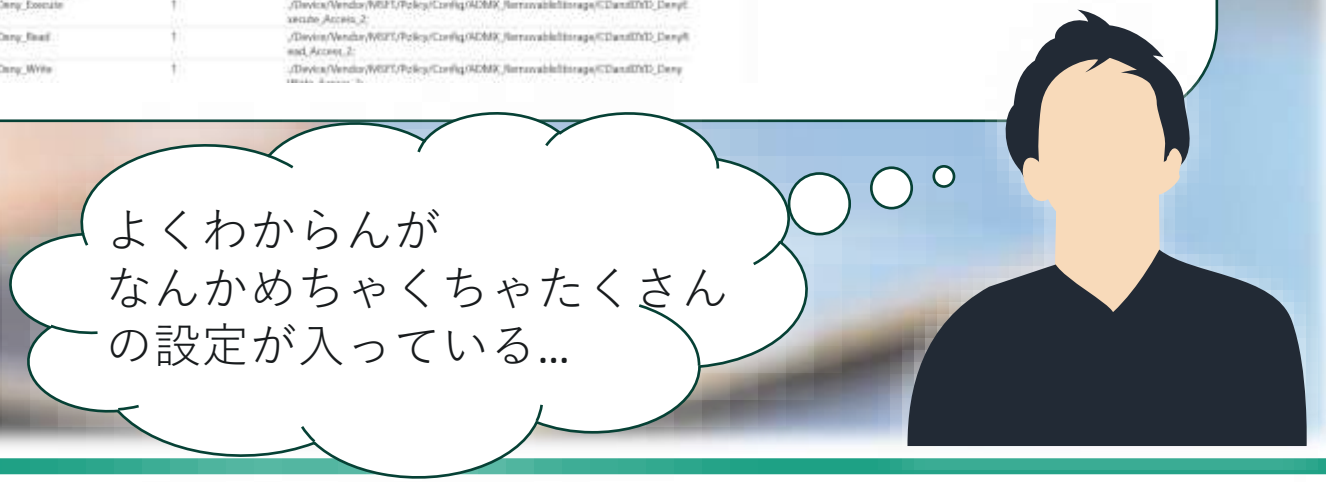
空っぽ

ちょっとカスタマイズすれば
いいだけと思ってた…
ちゃんと初期設定しないと
使い物にならなそうだ

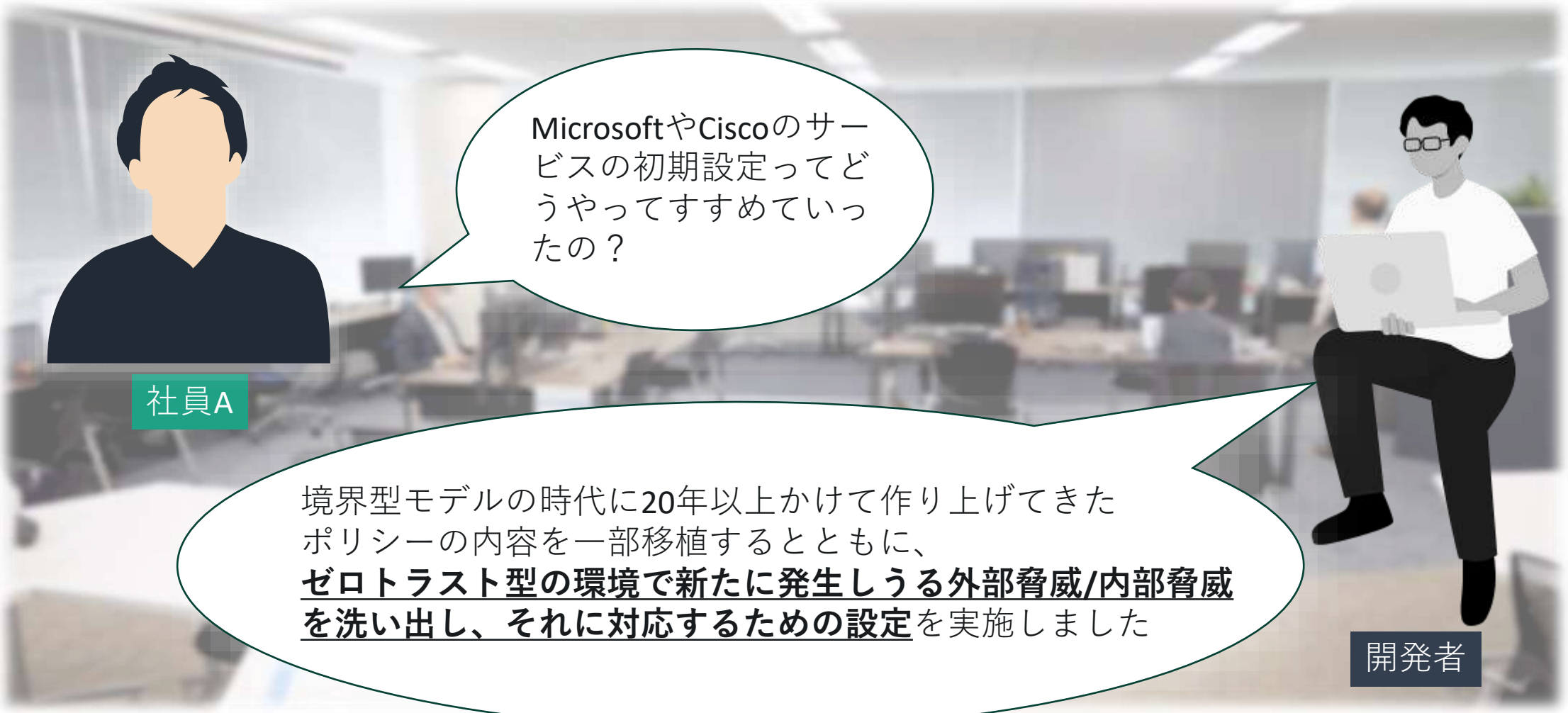
ドコモのゼロトラスト環境を覗いてみた

MicrosoftやCiscoのサービスのドコモ環境の管理画面を覗いてみると・・・





ドコモのゼロトラスト環境を開発した人にインタビューしてみた



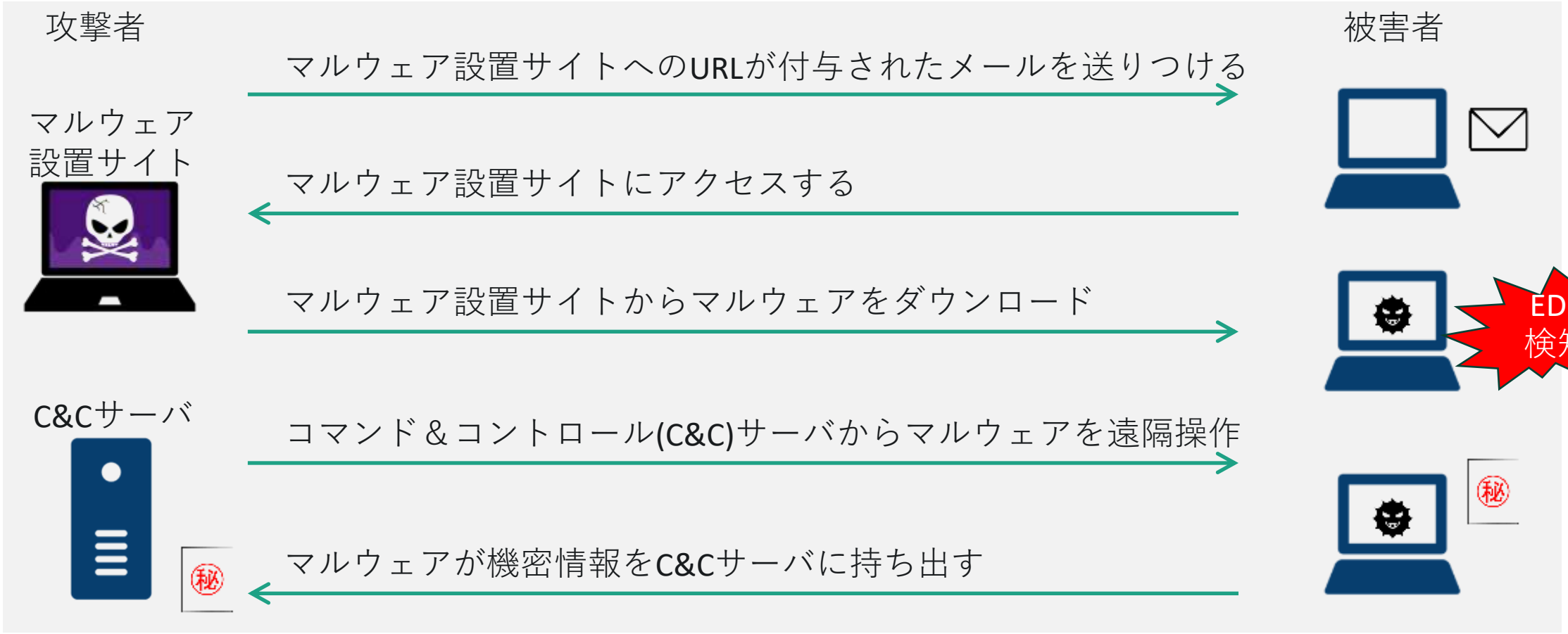
ご参考：ドコモの情報セキュリティポリシー(一部抜粋)

カテゴリ	ポリシー	目的	
パスワード関連	PW桁数は8桁以上	ブルートフォース攻撃(パスワード総あたり攻撃)対策	
	単純なPWを禁止		
	有効期間は1年		
	PINの利用を強制	M365アカウントのフィッシング対策	←New!
パソコン関連	外部記憶媒体の利用を原則禁止	悪意のある社員/ビジネスパートナーによる情報漏えい対策	
	ウィルス対策ソフトの利用を強制	マルウェア対策	
	WinOSのパッチ適用を強制	脆弱性対策	
	リモートデスクトップの利用禁止	RDPブルートフォース攻撃※対策 ※自宅ルータ等の設定不備等をきっかけとし、在宅勤務用PCに不正接続しようとする攻撃	←New!
	プリンタの追加禁止	自宅プリンタを利用した印刷物による情報漏えい対策	←New!
	紛失時はリモートワイプ(初期化)実施	自宅等への持ち出し端末の紛失/盗難による情報漏えい対策	←New!
スマホ関連	業務情報のローカル保存禁止	紛失/盗難による情報漏えい対策	
	紛失時はリモートワイプ(初期化)実施	紛失/盗難による情報漏えい対策	
	M365アプリ→他のアプリへのデータコピーの禁止	M365上の業務情報の情報漏えい対策	←New!
クラウドサービス関連	他テナントや個人契約のM365への接続禁止	悪意のある社員/ビジネスパートナーによる情報漏えい対策	←New!

在宅勤務の浸透やクラウドシフトをきっかけとした、新たに発生しうる脅威に対応するために
ポリシーをアップデートし、ポリシーに沿った設定をゼロトラスト型モデルの各機能に設定して
いく必要がある

ドコモのゼロトラスト環境を運用している人にインタビューしてみた

ご参考：マルウェアによる情報漏えいのシーケンス



通信ログからC&Cサーバへの通信が確認できない場合は、マルウェアが活動しているとは言えず
情報漏えいは起きていないといえる
⇒通信ログを確認することで、どの程度攻撃が進行しているか把握し、適切な対処を実施することができる

社員Aが感じたこと

- そもそもゼロトラストという**概念が難しい**
- ゼロトラストの構成要素ごとに色んな製品があるけど、**大差はない**のでは？
- ゼロトラスト関連のサービスは**きちんと設定しないと利用できない**
- ゼロトラスト環境を作り上げるには、**まず外部/内部脅威を洗い出し、それに対処するための会社のポリシーを決め、それを実装していく必要がある**
- 管理者系の機能を駆使して**運用まわしていくのも大変**

ドコモはお金とマンパワーをかけて比較的短期間でゼロトラスト環境を構築したけど、一企業が独自でゼロトラスト環境を作り、運用していくのはかなりの体力がいるのでは？

その後の社員A


ドコモのゼロトラスト環境作ったり、
運用しているひとたちすごいです！
ドコモのゼロトラスト環境の構築ノウハウや運用ノウハウってすごいので、それをテンプレート化すれば売れると思います！
社員A
売っちゃお！
たくさん売っちゃお！
偉い人
完

3

NTTドコモソリューションズの「ゼロトラスト型セキュリティサービス」ご紹介

ゼロトラスト型セキュリティサービスとは？

- ドコモグループやNTTグループのゼロトラスト型セキュリティの導入、運用ノウハウを一般のお客様にご提供
- 本サービスの導入により、エンドユーザはインターネット環境で安心、安全、快適に日常業務ができる

導入ノウハウ

- ✓ Cisco製品<Umbrella>の導入手順
- ✓ MS製品<Entra ID(旧Azure AD), Intune…>　の導入手順

etc…

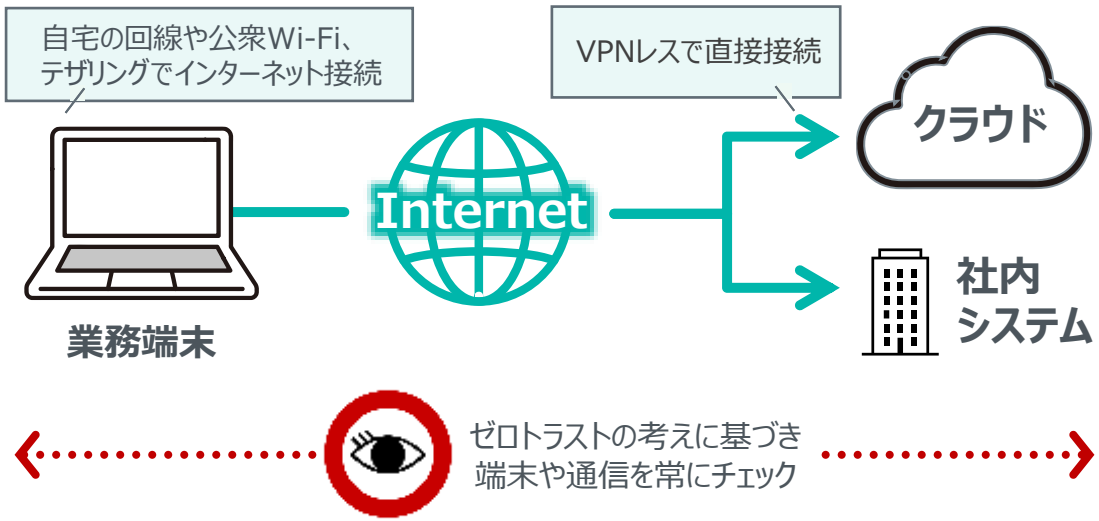
＋

運用ノウハウ

- ✓ 当社SOCのEDRアラート対応
- ✓ 当社SOCのSWGブロックリスト登録
- ✓ Intuneのポリシーカスタマイズ

etc…

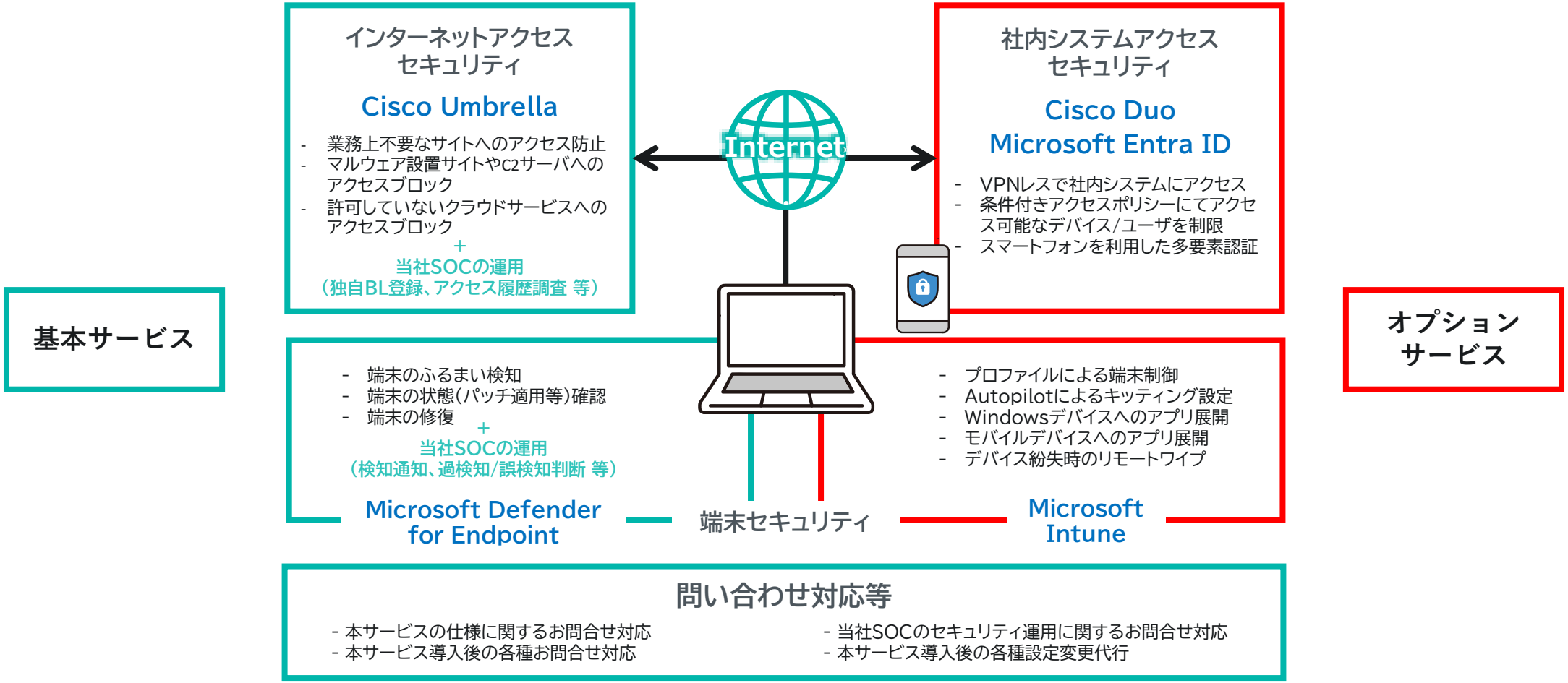
ご提供



インターネット環境の外部脅威、内部脅威に対応！

サービス概要①

- ゼロトラスト型セキュリティの実装に必要となるCiscoやMicrosoftのサービスの導入、および運用支援をサービスとしてご提供
- Cisco系サービスについては当社からライセンスを提供



サービス概要②

- ゼロトラスト型セキュリティの実装に必要となるCiscoやMicrosoftのサービスの導入、および運用支援をサービスとしてご提供
- Cisco系サービスについては当社からライセンスを提供

ZTXフレームワーク構成要素	機能	機能概要	ゼロトラスト型セキュリティサービス
アイデンティティセキュリティ	IDaaS	ID管理、SSO、アクセス条件制御	○
	MFA	多要素認証	○
ネットワークセキュリティ	SWG	Webアクセスセキュリティ	○
	ZTNA	社内アプリ含むアプリケーションへの安全なアクセス	○
デバイスセキュリティ	EDR	エンドポイントのふるまい検知・対応	○
	MDM	モバイルデバイス管理	○
	MAM	モバイルアプリケーション管理	○
ワークロードセキュリティ	CWPP	クラウドワークロードの脅威検出と防御	×
	CSPM	クラウドの設定管理	×
データセキュリティ	DLP	情報のタグ付け、漏洩対策	×
	ファイル暗号化	-	×
セキュリティの可視化と分析	CASB	クラウドサービスアクセス制御	×
	SIEM	ログ収集、分析	×
	UEBA	機器のログをベースとしたふるまい検知	×
セキュリティの自動化	SOAR	インシデント対応の自動化	×

ゼロトラスト環境を実現するのに必要最低限の機能の導入/運用を支援します

当社が導入/運用支援するにあたり、以下サービスをご利用いただく事を前提とします

IDaaS/MFA：
Microsoft Entra ID

SWG：
Cisco Umbrella

ZTNA：
Microsoft Entra Private Access

EDR：
Microsoft Defender for Endpoint P2

MDM/MAM：
Microsoft Intune

価格表
（参考価格）

- 導入の初期費用と、月額利用料金が発生します。
- 月額は、１社ごとの費用と、利用者1IDあたりの費用があります。

項目	価格		サービス内容
初期費用	175万円		• <u>ドコモの情報セキュリティポリシーをベースとした、各種機能の初期設定</u> • 運用上必要となる各種日本語マニュアル
月額費用	１社	20万円	• 導入後の設定変更代行(毎月2.5時間分対応) • セキュリティ観点での月次レポート
	１ID	2,400円	• Cisco Umbrellaのライセンス • <u>当社セキュリティオペレーションセンタによるセキュリティ運用</u> - アラート検知時の端末ログ⇔通信ログの相関的なチェック - ウィルス感染時のNW遮断 - お客様への推奨対応事項ご案内　など

直近だと、初期費用：130万円、月額費用：15万円/1社、1,600円/1ユーザ で価格提示したお客様もいます
ご要件によって変動しますので、お気軽にお問合せ下さい！

こんなお客様に
おすすめ

- ✓ M365を中心としたクラウドシフトを検討している
- ✓ M365の不正利用に不安を抱えている
- ✓ ゼロトラスト環境を構築したいが、人手も知識も不足している
- ✓ 短期間でゼロトラスト環境を構築したい
- ✓ セキュリティ運用を外部委託したい

まとめ

「餅は餅屋」がセキュリティの極意です

ゼロトラストの導入と運用には専門知識が必要です
ドコモでのノウハウをパッケージ化した
ドコモソリューションズのゼロトラスト型
セキュリティサービスをご検討ください。

詳細はこちら ▶ https://www.nttcom.co.jp/dscb/zerotrust/