

NTTドコモソリューションズ主催 オンラインセミナー

実際に起きたセキュリティ事故から学ぶ 「起こり得るリスク」とその対策

ドコモグループが培ってきた現場の知見と実際の事例に基づくリアルな対策をお届けします

2025年7月15日 13:00-14:00

セミナー中のご質問・お問い合わせは
Q&Aボタンから受け付けます

NTTドコモソリューションズのご紹介

つなごう。驚きを。幸せを。



- ✓ 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 | NTT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%) NTT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) |



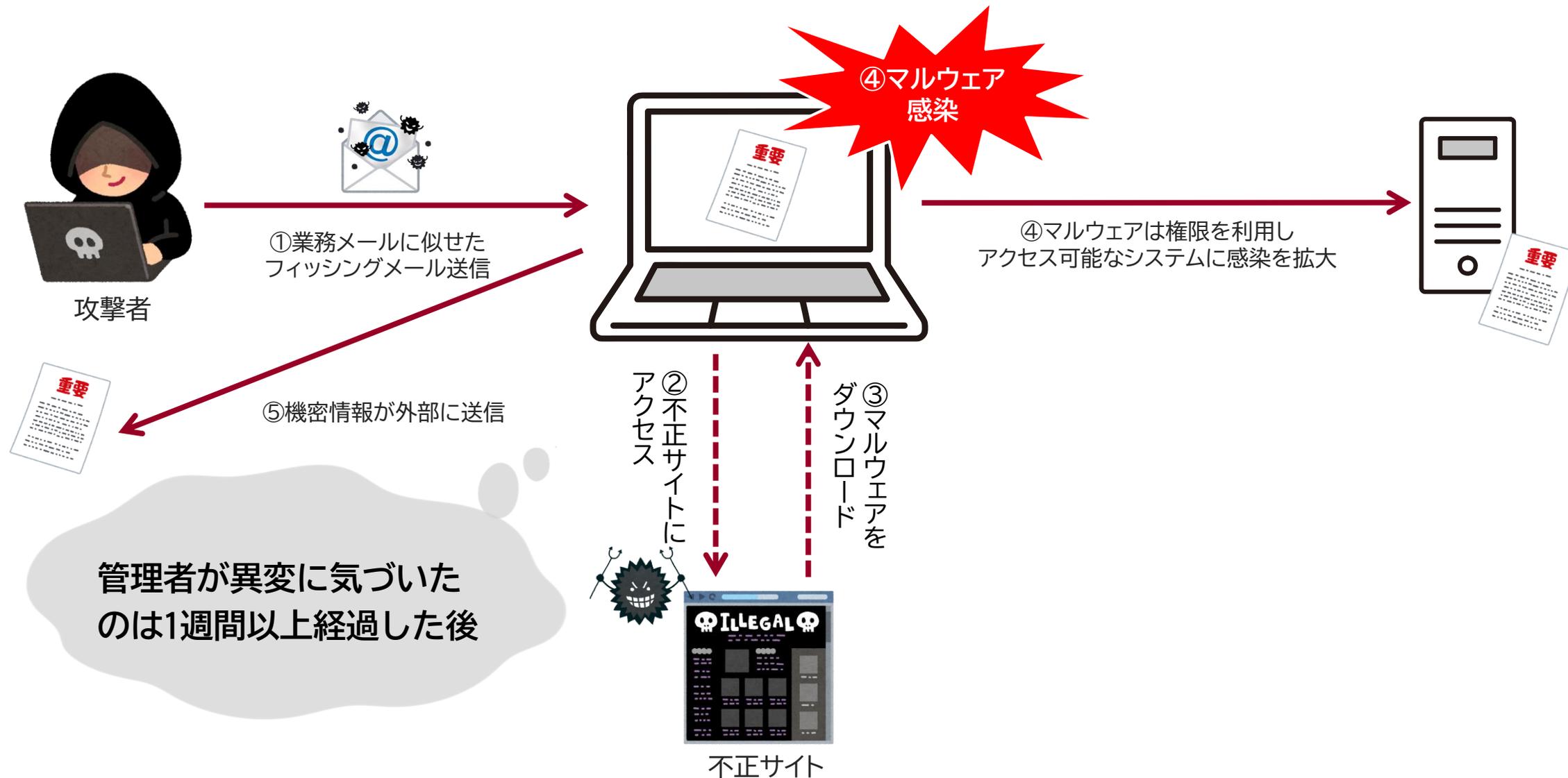
- ・起こり得るリスクについて4つの事例を紹介
- ・共通するリスク構造
- ・NTTドコモソリューションズのゼロトラスト型セキュリティサービスとは
- ・ゼロトラスト型セキュリティサービスによる解決例
- ・次のステップ 情報セキュリティの可視化のご案内

起こり得るリスクについて 4つの事例を紹介

起こり得るリスク① マルウェアによる情報漏洩

マルウェアは見えない侵入者。気づいた時には手遅れ

起こり得るリスク① マルウェアによる情報漏洩

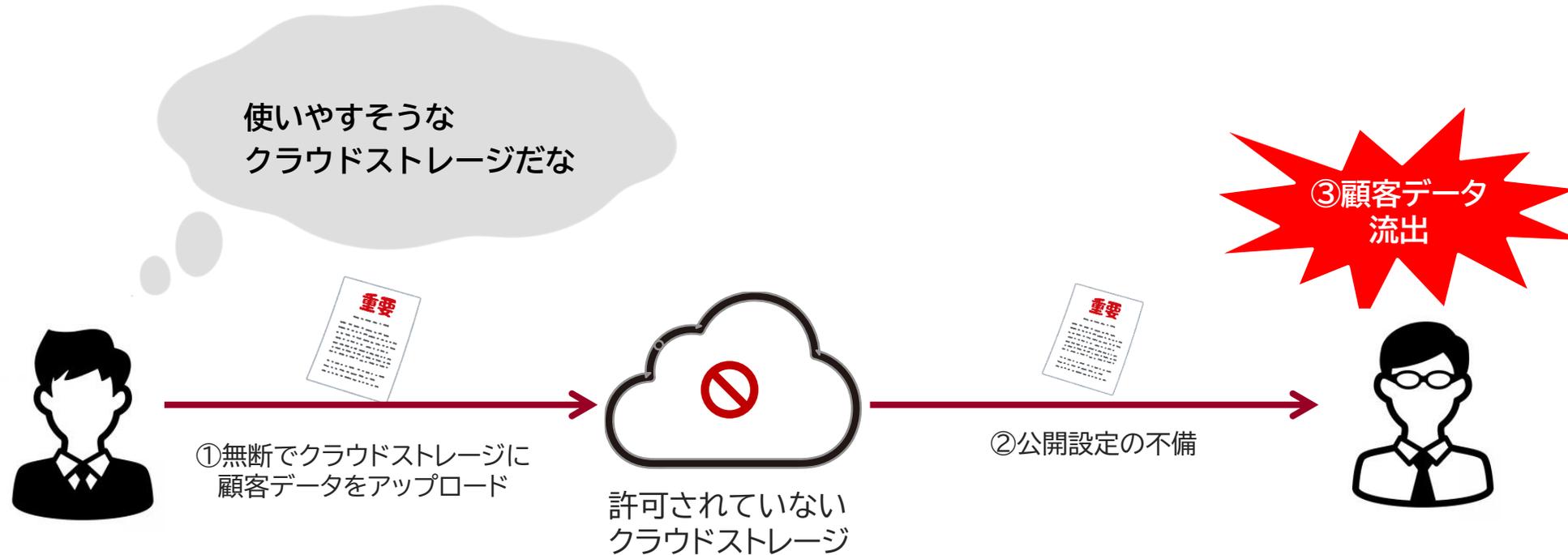


防げなかったでは済まされない時代。拡大を防ぐ備えがカギ

起こり得るリスク② シャドーIT(SaaS)による情報漏洩
気づかぬうちに漏れていた。それが「シャドーIT」の怖さ

起こり得るリスク② シャドーIT(SaaS)による情報漏洩

つながり。驚きを。幸せを。



起こり得るリスク② シャドーIT(SaaS)による情報漏洩

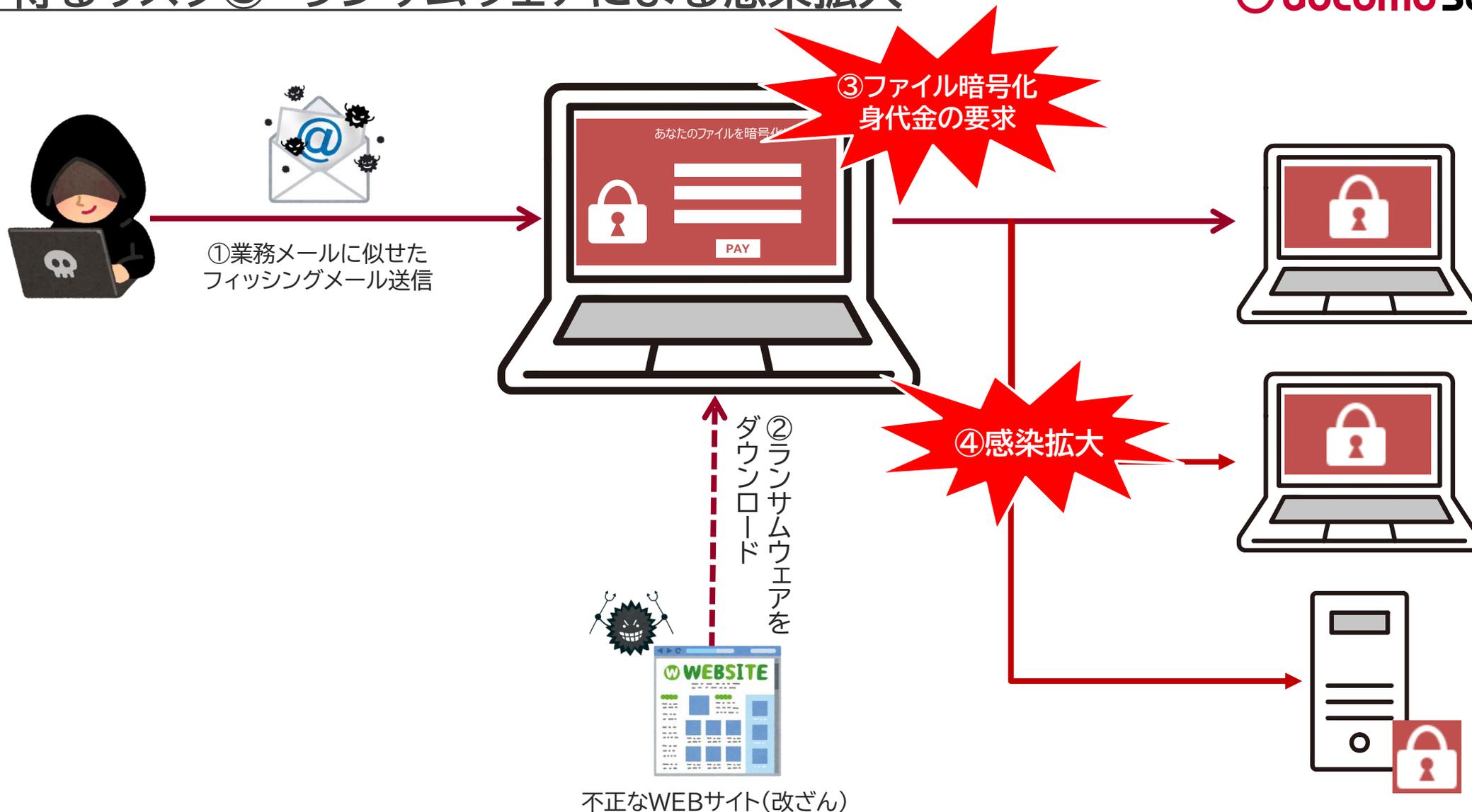
つながる。驚きを。幸せを。

 NTT docomo Solutions

全体の可視化と統制が必要

起こり得るリスク③ ランサムウェアによる感染拡大
広がるのは速い。止める手は遅い

起こり得るリスク③ ランサムウェアによる感染拡大



起こり得るリスク③ ランサムウェアによる感染拡大

つながる。驚きを。幸せを。

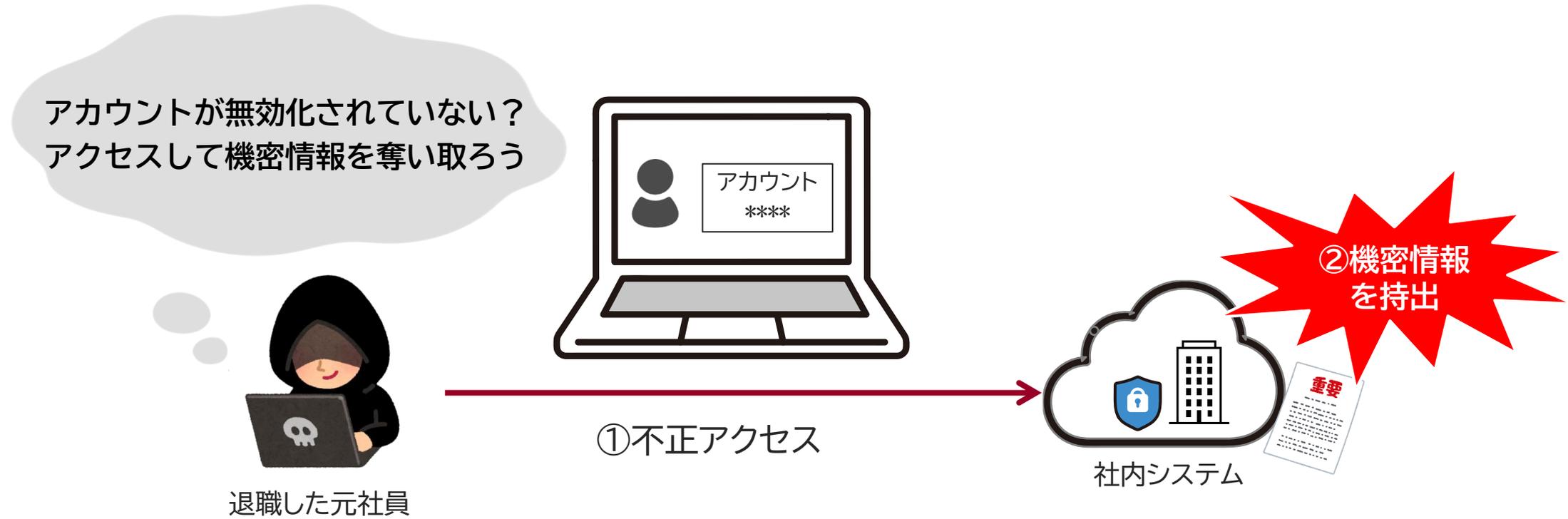
 NTT docomo Solutions

止められないのは、備えていなかったから

起こり得るリスク④ 退職者アカウント放置
もういないはずの元社員が、まだアクセスできる

起こり得るリスク④ 退職者アカウント放置

つながる。驚きを。幸せを。



出典:退職者アカウントが原因とされる約900万件流出事案

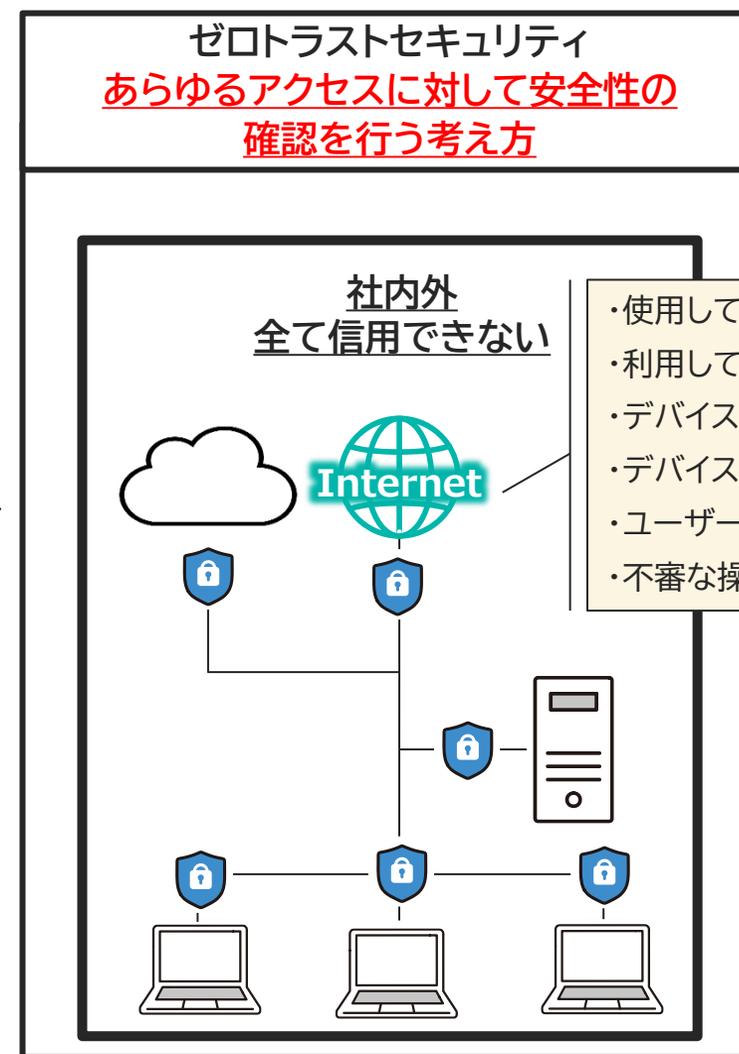
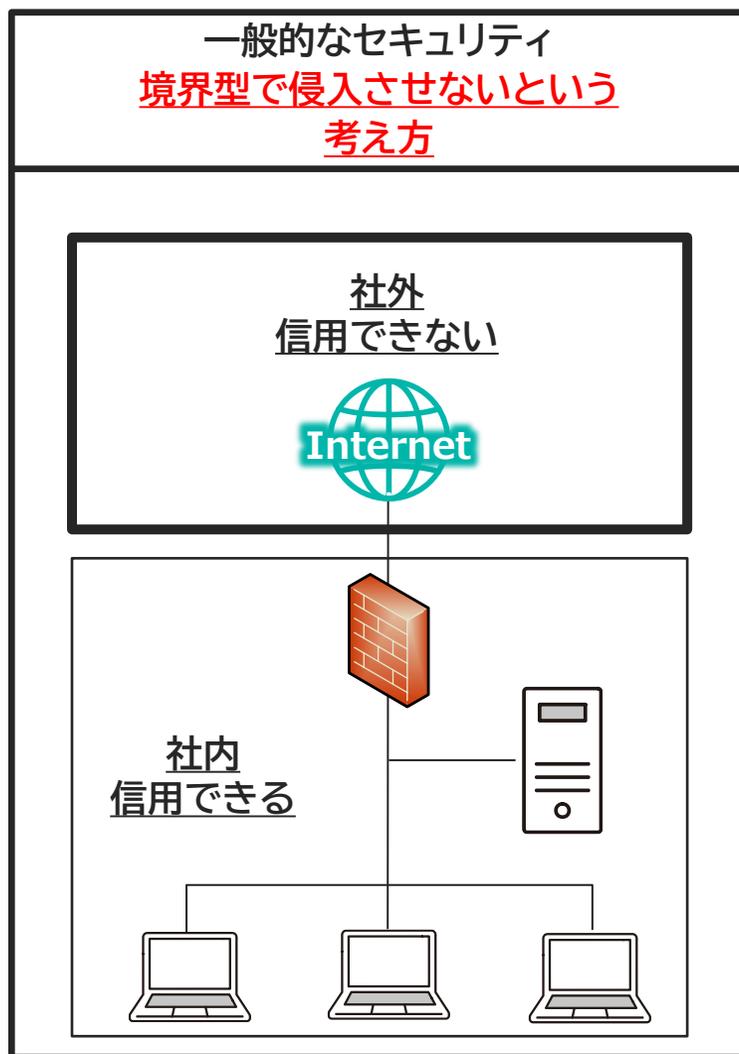
起こり得るリスク④ 退職者アカウント放置

アカウントは「人」に紐づく。だからこそ、「退職」で終わらせない管理が必要

| リスク構造要素 | 説明 | 関連する事例 |
|------------------|--|-------------------------------|
| 見えないアクセス経路 | IT部門が把握できていない場所から利用・侵入される | マルウェア、シャドーIT、退職者アカウント |
| 過剰な信頼 (暗黙の前提) | 「社内だからOK」、「一度認証すれば安全」という暗黙の信頼に依存している | マルウェア、シャドーIT、ランサムウェア、退職者アカウント |
| 認証や権限の不備 | 不要なアカウント/広すぎる権限が放置され侵入後に拡大されやすい | 退職者アカウント、シャドーIT、マルウェア |
| 検知・遮断の遅れ | 侵入後の異常行動に気づくのが遅れ、社内で被害が拡大 | マルウェア、ランサムウェア |
| ネットワーク境界依存の限界 | 「社内＝安全、社外＝危険」という前提で対策しているが、内部からの脅威に無防備 | ランサムウェア、マルウェア、退職者アカウント |
| ユーザ任せの運用 | 現場判断でのクラウド利用・アプリ利用など、人に依存したセキュリティ | シャドーIT |

ゼロトラストとは

ゼロトラストは、従来の境界型セキュリティとは異なり、社内、社外を区別せず、すべての通信を信用しない考え方となります。そのため、厳格なユーザ認証、端末の管理やネットワーク監視などのセキュリティ対策を施します。

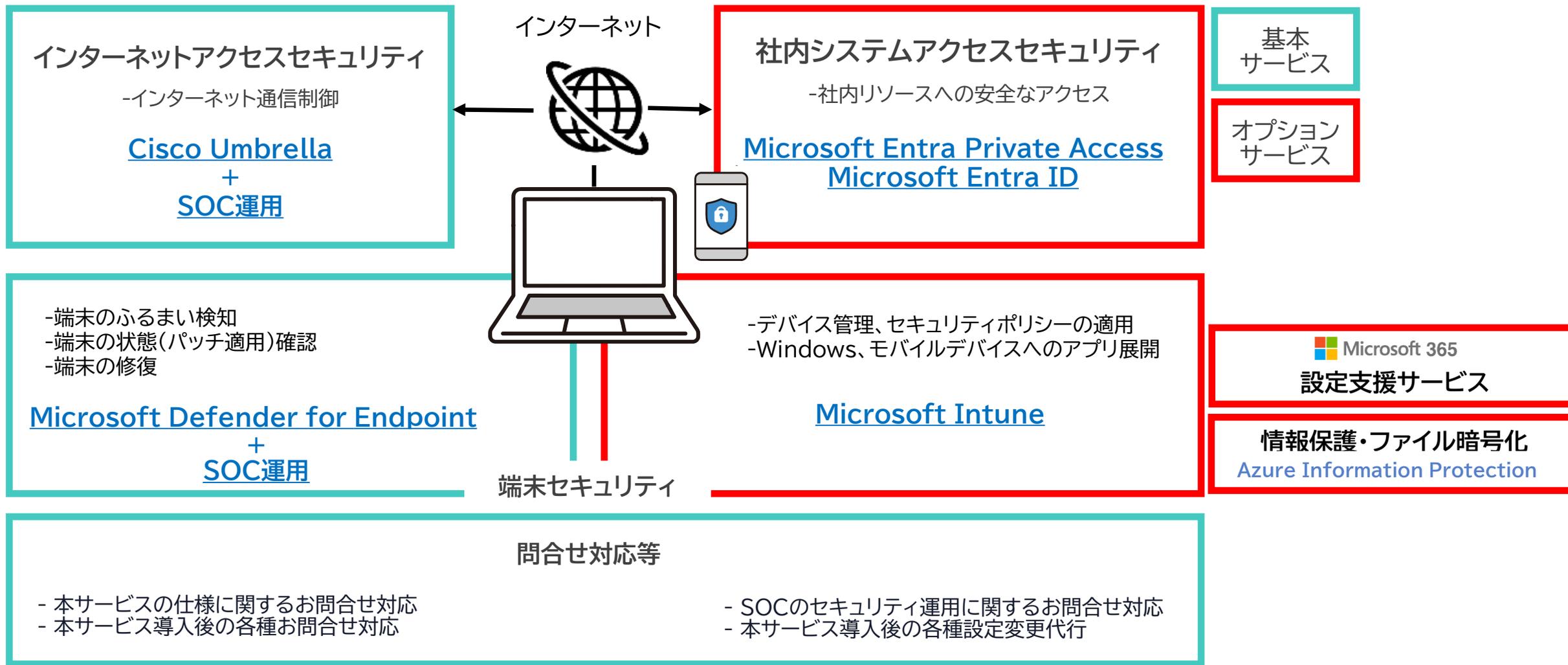


https://www.youtube.com/watch?v=Pg0GvItz_YI



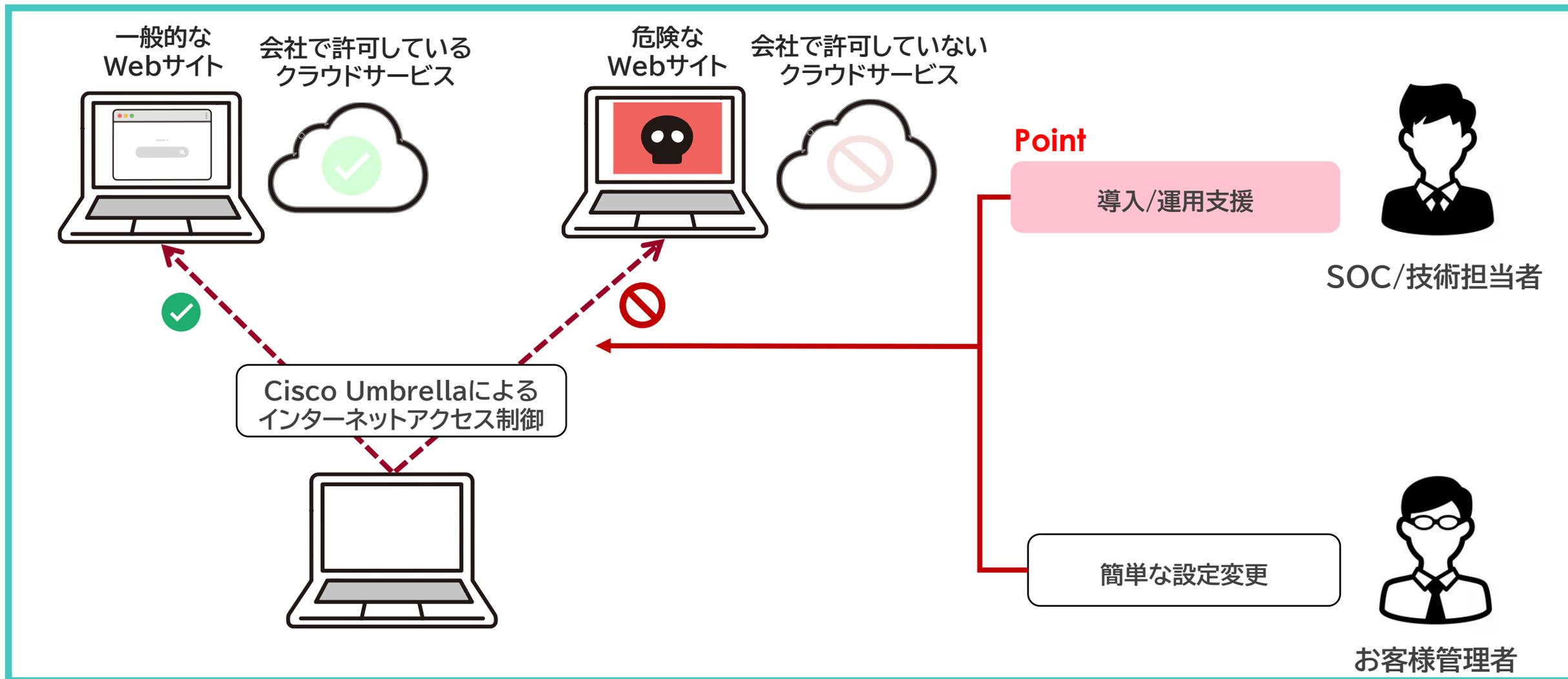
NTTドコモソリューションズのゼロトラスト型セキュリティサービスとは

- 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
- ゼロトラスト型セキュリティの実装に必要な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(Microsoftライセンスはお客様用意)



インターネットアクセスセキュリティ(基本サービス)

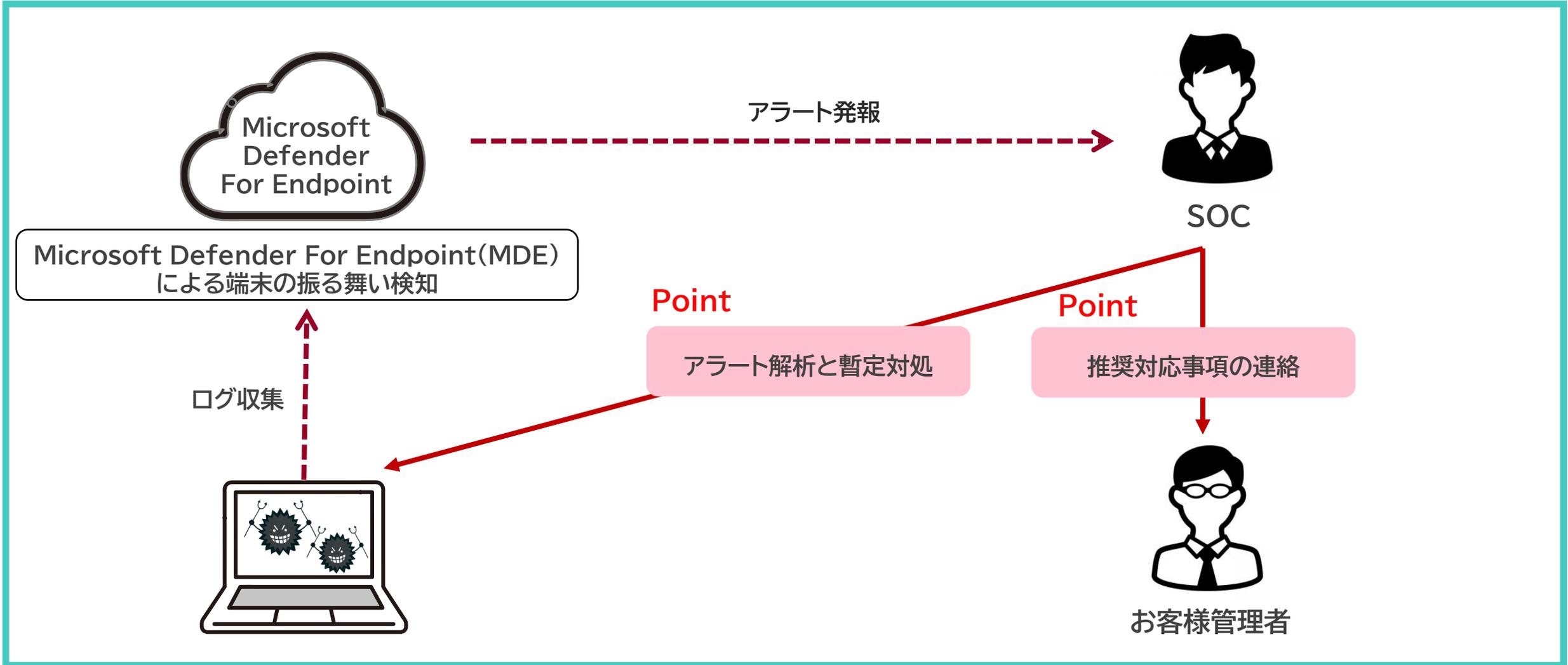
お客様の業務用PCに、Secure Web Gateway(SWG)製品であるCisco Umbrellaを導入し、インターネット通信を制御します。



端末セキュリティ(MDE) (基本サービス)

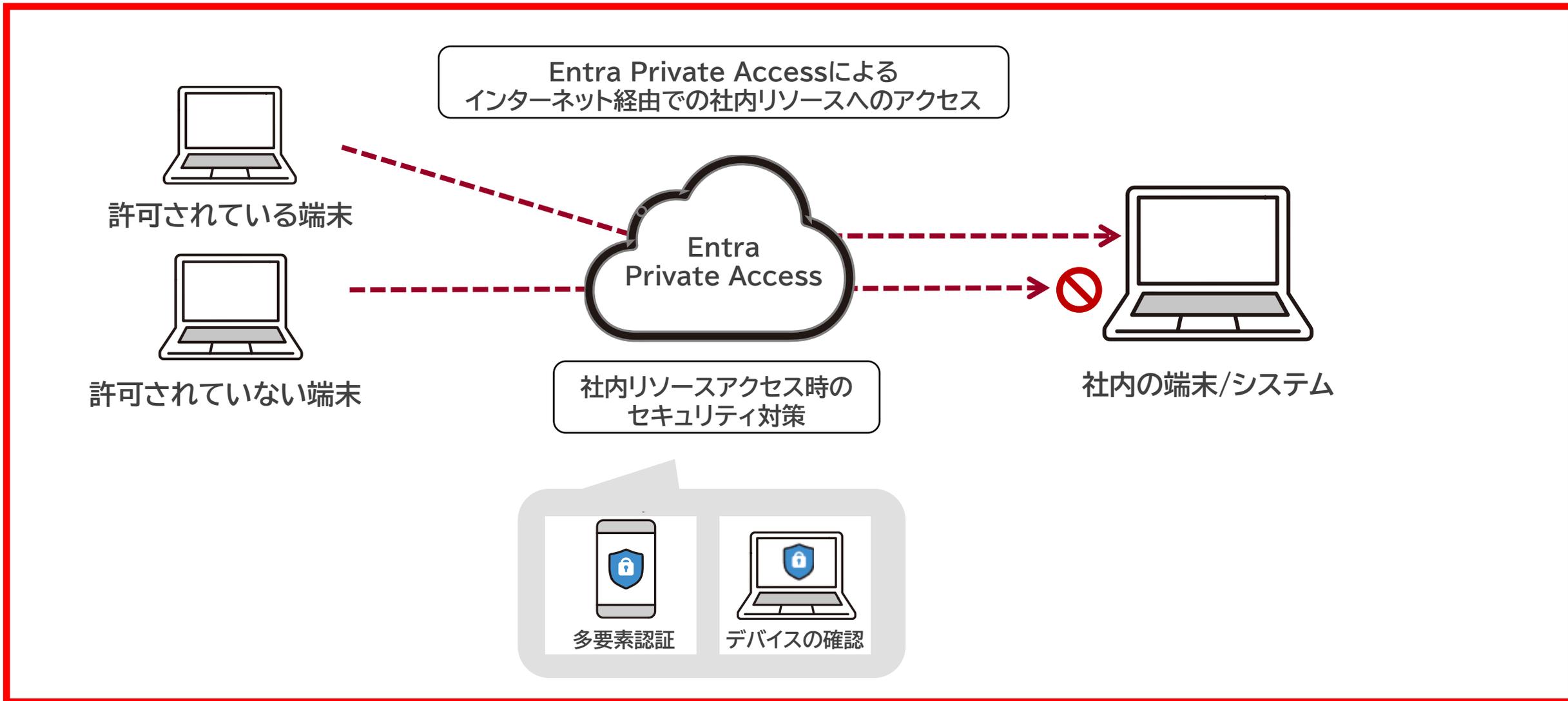
つながる。驚きを。幸せを。

お客様の業務用PCに、EDR製品であるMicrosoft Defender for Endpoint P2(MDE)を導入し、PCの不自然な振る舞いを検知します。



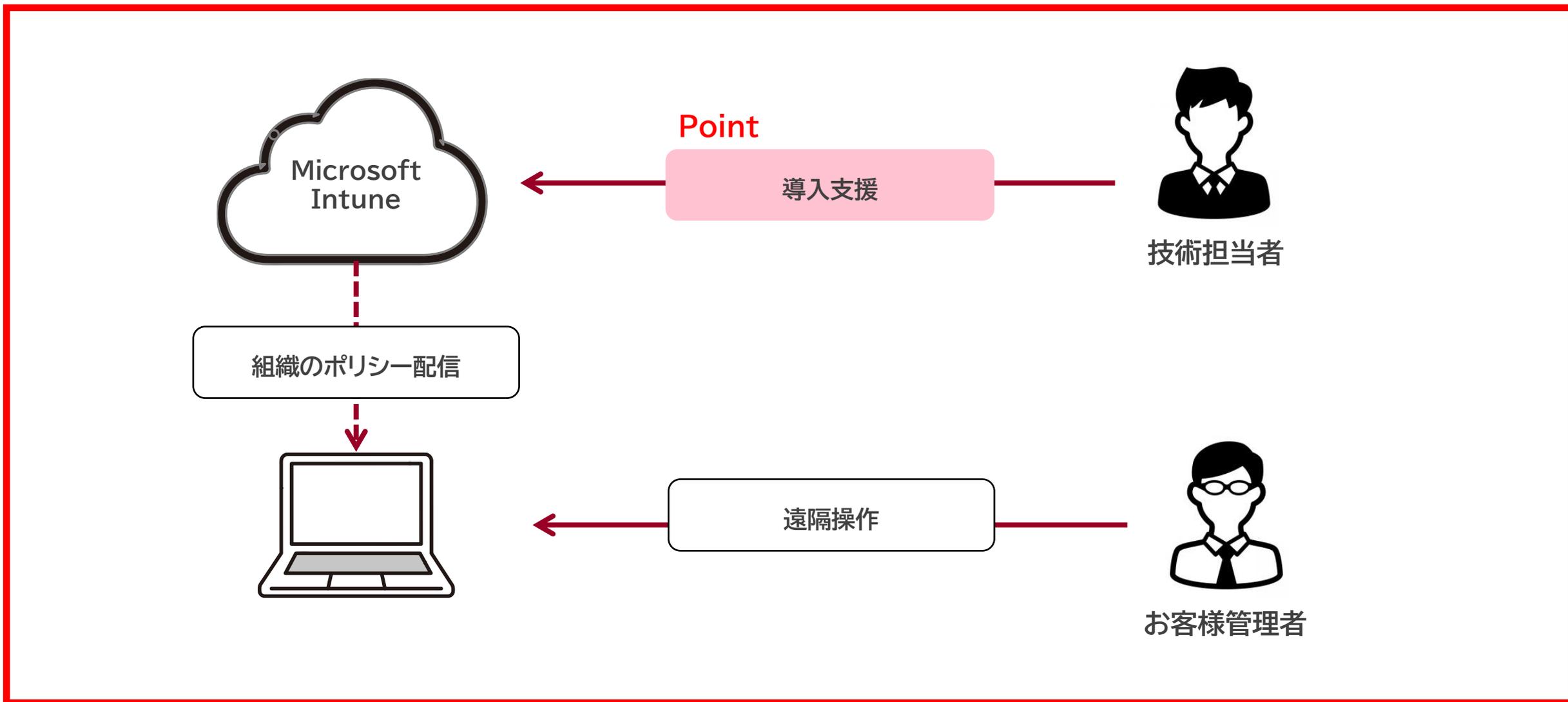
社内システムアクセスセキュリティ(オプションサービス)

ZTNA製品であるEntra Private Accessを導入し、インターネットから社内リソースに安全にアクセスできるようにします。



端末セキュリティ(Intune) (オプションサービス)

MDM製品であるMicrosoft Intuneを利用し、お客様の業務用PCを管理します。スマートフォンについても管理可能です。



Microsoft365設定支援サービスのご紹介

- ゼロトラスト型セキュリティサービスのオプションとしてM365導入支援をご提供
- ドコモの設定ノウハウを元にセキュリティを意識した設定内容をテンプレート化

Microsoft 365

<対象>
 M365 E5/E3
 M365 BusinessPremium

| サービス名 | 機能と設定支援 |
|-----------------|---|
| Entra ID | 【アイデンティティ管理、アクセス制御等】 シングルサインオン(SSO)や多要素認証(MFA)などのセキュリティ設定を支援 |
| Exchange Online | 【メール管理、予定表、連絡先管理】 メールのスパムやマルウェア対策を加味した設定を支援 |
| Teams | 【コミュニケーションとコラボレーションのツール】 ゲスト共有の範囲等コラボ機能に関する設定を支援 |
| SharePoint | 【チームやプロジェクト間のドキュメント管理と共同作業プラットフォーム】 同上 |

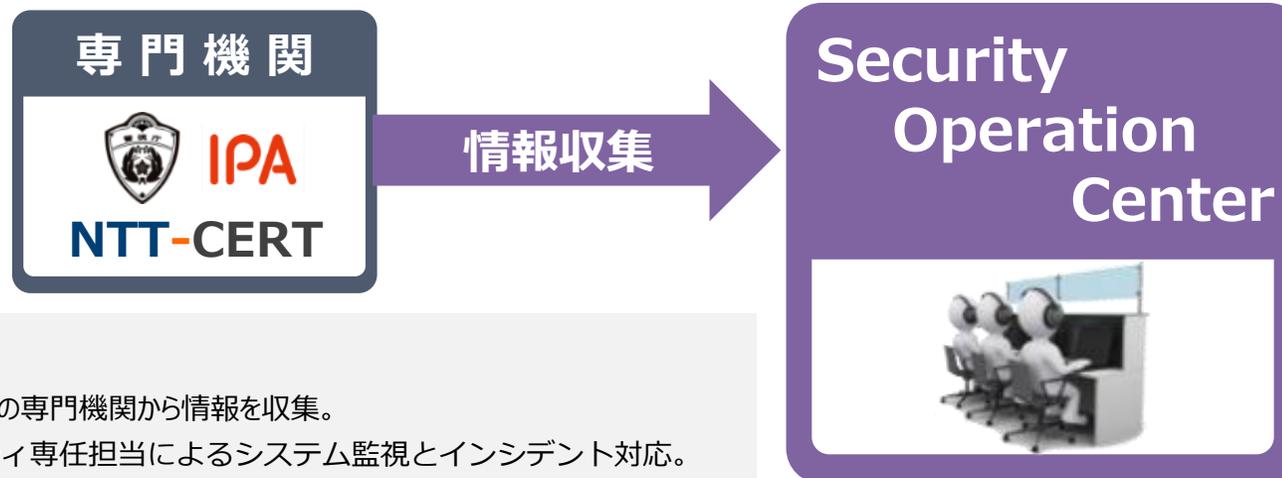


問い合わせ対応等

- 本サービスの仕様に関するお問合せ対応
- 本サービス導入後の各種お問合せ対応

- 本サービス導入後の各種設定変更代行

- 当社のSOCが、お客様に成り代わって必要なセキュリティ運用を実施
- セキュリティインシデント発生時におけるアラート解析、対処案検討、お客様への通知など



Point

様々な外部の専門機関から情報を収集。
セキュリティ専任担当によるシステム監視とインシデント対応。



Point

システムでの自動検知に加え、アナリストによる端末とNWの相関分析を実施。
アラート発生時の調査実施、対処方法検討、お客様へのご連絡。
インターネットアクセスセキュリティ設定のチューニングを実施。
セキュリティレポートの提供。



導入 / 運用支援

NTTドコモソリューションズでは、ゼロトラスト型セキュリティサービスの導入から運用までを一貫してサポートします。お客様に代わり、当社の技術担当者がサービスの導入/運用を支援いたします。また、当社のセキュリティオペレーションセンタ(SOC)が、セキュリティ関連の運用を実施します。

導入支援でできること

①ノウハウも基づいた初期設定

MicrosoftやCiscoのクラウドサービスについて、当社の技術担当者が、当社のノウハウをベースとした推奨設定をお客様環境に実施させていただきます。

②ヒアリングを通じた設定のカスタマイズ

MicrosoftやCiscoのクラウドサービスについて、当社の技術担当者が、お客様の要望をヒアリングしご要望に沿った形で初期設定をさせていただきます。

お客様に代わり、当社の技術担当者がサービスの導入/運用を支援いたします。また、当社のセキュリティオペレーションセンタ(SOC)が、セキュリティ関連の運用を実施します。

運用支援でできること

①サイバー攻撃の検知と通知

お客様の運用端末PCにてサイバー攻撃を受けていることが検知された場合、お客様に通知を行うとともに、関連対応策を講じます。

②サイバー攻撃の拡大防止

お客様の運用端末PCでサイバー攻撃を受けていることが検知された場合、当該PCやネットワークから切り離すなどして被害拡大防止策を講じます
(24H365日対応)

③定期セキュリティレポート

月次にて、セキュリティ対策状況や脅威分析結果についてレポートをご提供します。

④設定変更代行

Cisco UmbrellaやMicrosoft Intune等、お客様環境機器設定変更作業をご支援します。

⑤お問い合わせ対応

サービスごとの共通SOCのセキュリティ運用担当者が、お問い合わせ内容に応じた回答・アドバイスをご提供します。

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のまとめ

つながり。驚きを。幸せを。



当社のゼロトラスト型セキュリティサービスはM365製品を中心に構成したサービスとなります。

| 項目 | NTTドコモソリューションズ ゼロトラスト型セキュリティサービス |
|------|--|
| 特徴 | M365製品を中心に構成したゼロトラスト型セキュリティ |
| 対象企業 | ゼロトラストネットワークに対するセキュリティを求める企業。 Microsoft365をこれから導入または利用中でセキュリティに不安を感じる企業 |
| 提供内容 | Cisco Umbrella(SWG)およびMicrosoft365で構成されたセキュリティ対策をパッケージとして提供 |
| 導入 | テンプレート化された設計で短期間導入 |
| メリット | M365を活用した業務効率化を支援 (例) ・M365 EntraIDによるユーザとグループでアクセス権限を集中管理し、権限設定作業負荷を軽減 ・M365のSharePointやTeamsを活用して社外とのスムーズな情報共有を構築する等 |

ゼロトラスト型セキュリティサービスによる解決例

| リスク構造要素 | 関連する事例 | ゼロトラストによる解決策 | NTTドコモソリューションズ ゼロトラスト型セキュリティサービス 関連サービス |
|-------------------|-----------------------------------|--------------------------------------|---|
| 見えないアクセス経路 | マルウェア、シャドーIT、 退職者アカウント | アクセスの可視化と制御 (SaaS制御、シャドーITの抑止) | <u>インターネットアクセスセキュリティ</u> (Cisco Umbrella) |
| 過剰な信頼 (暗黙の前提) | マルウェア、シャドーIT、ランサムウェア、 退職者アカウント | ID・端末ごとに毎回認証/アクセス制御 | <u>Microsoft365設定支援サービス</u> (Microsoft Entra ID) 社内システムアクセスセキュリティ (Microsoft Entra Private Access) |
| 認証や権限の不備 | 退職者アカウント、シャドーIT、 マルウェア | 最小権限管理 (ユーザ単位でのきめ細かい制御) | <u>Microsoft365設定支援サービス</u> (Microsoft Entra ID) |
| 検知・遮断の遅れ | マルウェア、ランサムウェア | 常時監視と振る舞い検知 | <u>端末セキュリティ(MDE)</u> (Microsoft Defender for Endpoint) |
| ネットワーク境界依存の 限界 | ランサムウェア、マルウェア、 退職者アカウント | アクセスする人のIDや端末、 セキュリティ状態に応じてアクセス制御 | <u>インターネットアクセスセキュリティ</u> (Cisco Umbrella) |
| ユーザ任せの運用 | シャドーIT | デバイス管理・アプリ制御・ポリシー強制 | <u>端末セキュリティ(MDE)</u> (Microsoft Intune) <u>インターネットアクセスセキュリティ</u> Cisco Umbrella |

どんなに優れたセキュリティ対策にも限界があり、絶対に安全という状態は存在しません。

特に、未知の脅威やゼロデイ攻撃、内部不正など、
検知が難しい攻撃に対しては、限界があることも事実です。

だからこそ、ゼロトラストの導入だけで終わらせず、

継続的な監視

インシデント対応体制の整備

社員教育や運用ルールの徹底

といった、多層的なセキュリティ対策が不可欠です。

提供価格について

つながり。驚きを。幸せを。



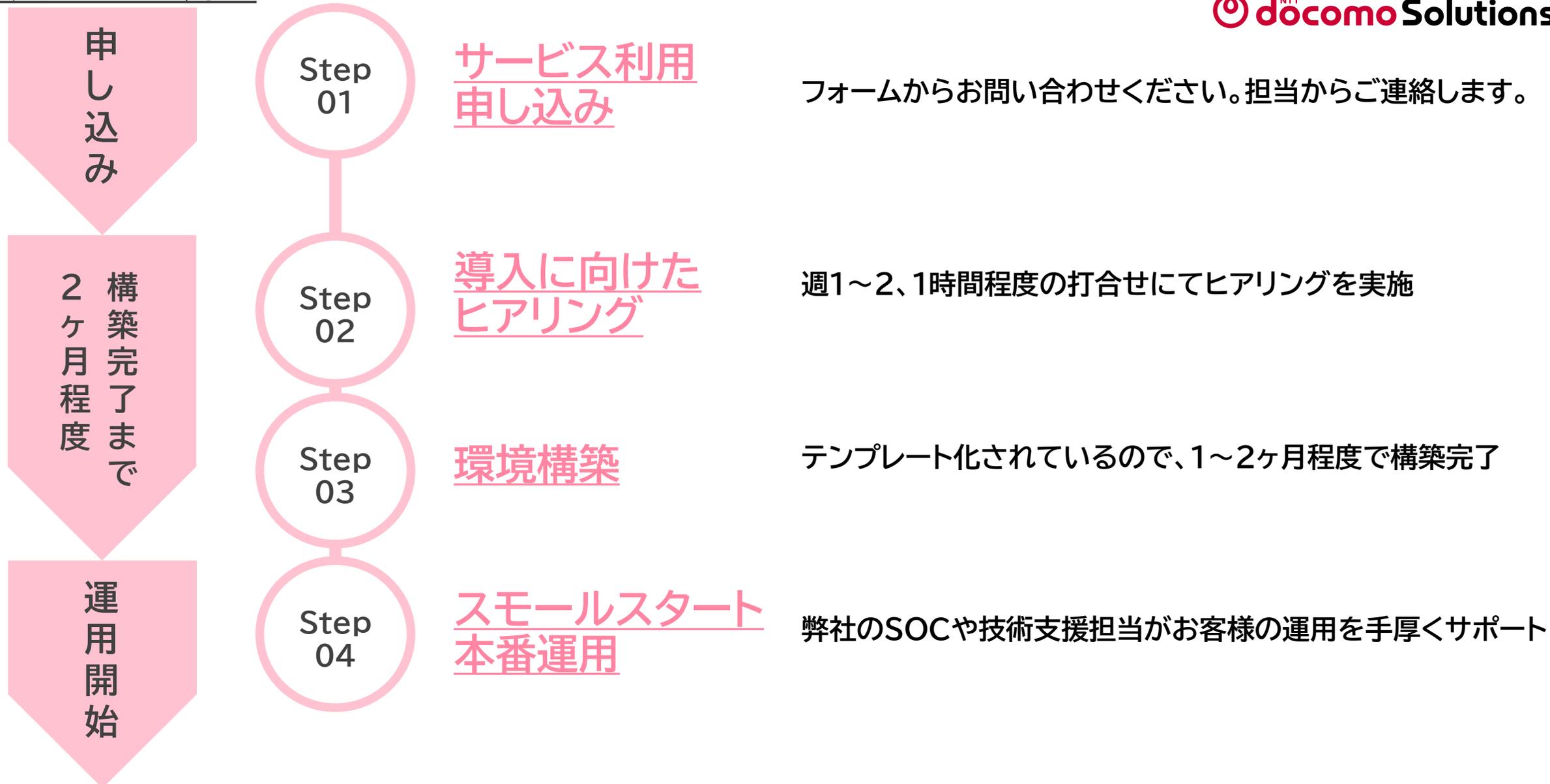
| 項目 | 価格 | | サービス内容 |
|-------|--------------|---------------|--|
| 初期費用 | 175万円 | | <ul style="list-style-type: none">・<u>ドコモの情報セキュリティポリシーをベースとした初期設定</u>・運用上必要となる各種日本語マニュアル |
| 月額利用料 | 1社 | 20万 | <ul style="list-style-type: none">・導入後の設定変更代行(毎月2.5時間分対応)・セキュリティ観点での月次レポート |
| | 1ID | 2,400円 | <ul style="list-style-type: none">・Cisco Umbrellaのライセンス・<u>当社SOC(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⇔通信ログの相関分析-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 |

※参考価格であり、要件により価格は変動いたします。詳細はお問い合わせください。

Microsoftライセンスはお客様側でご用意いただく必要があります

導入までの流れ

つながる。驚きを。幸せを。



※スケジュールはあくまで目安であり、企業規模や導入範囲により変動します。

ゼロトラストが必要なのはわかるけど、何から手を付けていいか分からない
まずは現状のセキュリティリスクを見える化しませんか？

今、必要な対策を今すぐ把握しよう

—継続的なセキュリティ対策が重要—

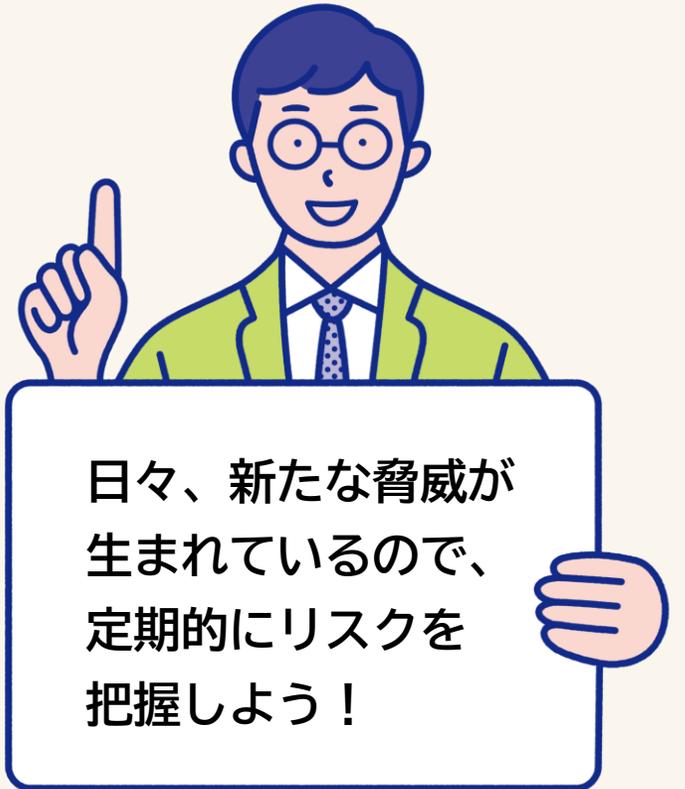


気づいていないリスクが最大の脅威

情報セキュリティリスクを
可視化してみませんか？



お客様のセキュリティの可視化と
適切な対策をご提示します。



NTTドコモソリューションズでできること

ーセキュリティリスクレポートの診断項目ー

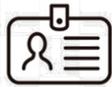


インターネット出入口対策、端末管理、サーバ/ミドルウェア管理に関するリスクを下記の項目で診断します。



入口対策（メール）

- ・危険度の高い拡張子を持つ添付ファイルのメール受信を拒否する
- ・メールの添付ファイルのウイルスチェックを行う



ID管理

- ・クラウドサービスのID管理が適切に行われている
- ・従業員の雇用/退出と連動したID管理ができている



リモートアクセス

- ・社内NWへのリモートアクセスにおいて適切に認証が行われている



外部公開Webサイト

- ・自社公開Webサイトへのセキュリティ対策がされている



モバイル端末

- ・スマートフォンなどのモバイル端末にて業務を行う場合にモバイル端末の管理、セキュリティ対応がとられている



社内からのWebアクセス/社外でのWebアクセス

- ・業務に不要なWebサイトへのアクセスをフィルタリングする
- ・マルウェア設置サイトおよびC&Cサーバへの通信をブロックする
- ・HTTP/HTTPS通信ログを取得する



端末管理等

- ・ウイルス対策ソフトで既知のウイルスをブロックする
- ・パターンファイルが最新化されている
- ・ふるまい検知型のエンドポイントセキュリティを導入している



クラウドサービス

- ・利用可能なクラウドサービスを制限している
- ・クラウドサービスの利用において、アクセス元の制限や多要素認証を実装している



セキュリティ運用（SOC）

- ・ファイアウォールやIPS/IDS、プロキシサーバ等のログ監視・分析を行う
- ・セキュリティ状況を定期的に分析する

NTTドコモソリューションズでできること

—セキュリティリスクレポートの診断結果—



リスクの可視化と推奨する対策をレポートにまとめて報告します。

- ① 現構成のセキュリティリスクを解説
- ② 分析結果の共有
 1. 分析結果
 2. 検出された箇所
 3. 主なリスクにおける事例紹介
- ③ リスクに対する対策案の提示



NTTドコモソリューションズでできること

—セキュリティリスクレポートの診断フロー—



全工程を1~1.5カ月程度で実施します。



1

ヒアリング



セキュリティ診断
項目に基づく
現状対策の調査

2

実機確認



業務端末を用いた
実際のセキュリティ
対策状況の確認

3

分析



ヒアリング内容および
実機の確認をもとに
リスク評価の実施

4

中間報告



リスク提示と認識の
共有、分析結果に関す
る詳細レポートの提示

5

最終報告



想定されるリスクに
対する具体的な
対策案のご提案

金額：¥300,000～ ※診断内容に応じてお見積りさせていただきます。

私たちは、ドコモグループで培ったノウハウを活かし、
皆様のセキュリティ強化を全力でサポートします。
どんな小さな不安でも、ぜひご相談ください。

質疑応答

NTTドコモソリューションズ ゼロトラスト型セキュリティサービスのモデル

つながり。驚きを。幸せを。



Q: ゼロトラストセキュリティは色々な種類がありますが、どこをカバーしていますか。

A: ・ゼロトラスト型セキュリティの実装に必要な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いたします。
 ・Cisco系サービスについては当社からライセンスを提供いたします。

| 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

必要なMicrosoft365ライセンス

つながろう。驚きを。幸せを。



Q: 必要なライセンスを教えてください。

A: ゼロトラスト型セキュリティサービスをご利用するにあたり必要となるMicrosoftのライセンスは下記の表の通りとなります。

| | 項目 | 必要となるMicrosoftライセンス | M365プランに含まれているかどうか | | |
|-------|---------------------------|------------------------------------|--------------------|----------------------------------|---|
| | | | M365 E5 | M365 E3 M365 Business Premium | M365 Business Standard M365 Business Basic M365 Apps for business |
| 基本 | インターネットアクセス セキュリティ | 当社がCiscoのライセンスをご用意 | | | |
| | 端末セキュリティ (MDE) | Microsoft Defender for Endpoint P2 | ○ | × | × |
| オプション | 端末セキュリティ (Intune) | Microsoft Intune P1 | ○ | ○ | × |
| | 社内システムアクセス セキュリティ(EPA) | Microsoft Entra Private Access | ○ | × | × |
| | 情報保護・ファイル暗号 化(AIP) | Azure Information Protection P1 | ○ | ○ | × |

つなごう。驚きを。幸せを。

 ^{NTT} **docomo** **Solutions**