CloudShift

Stylez

株式会社スタイルズ

2022年４月12日

30分でわかる！クラウドやテレワークの脅威とゼロトラストによる対策

aws partner network

aws PARTNER Select Tier Services

RANCHER PARTNER NETWORK

ZABBIX CERTIFIED PARTNER

Nextcloud Gold partner

vmware PARTNER PROFESSIONAL SOLUTION PROVIDER

自己紹介

- 木村　優也（yuya kimura）

- 株式会社スタイルズ
  - ゼロトラスト関連チームでEDR等を担当

本日、お話する内容

対象

- ゼロトラストについて理解を深めたい方
- 自社のセキュリティを向上させたい方

ゴール

- ゼロトラストとは何かを理解する
- クラウドやテレワーク時代の脅威と対策の始め方を理解する

ゼロトラストとは？～「全てを信頼しない」セキュリティ対策 ～

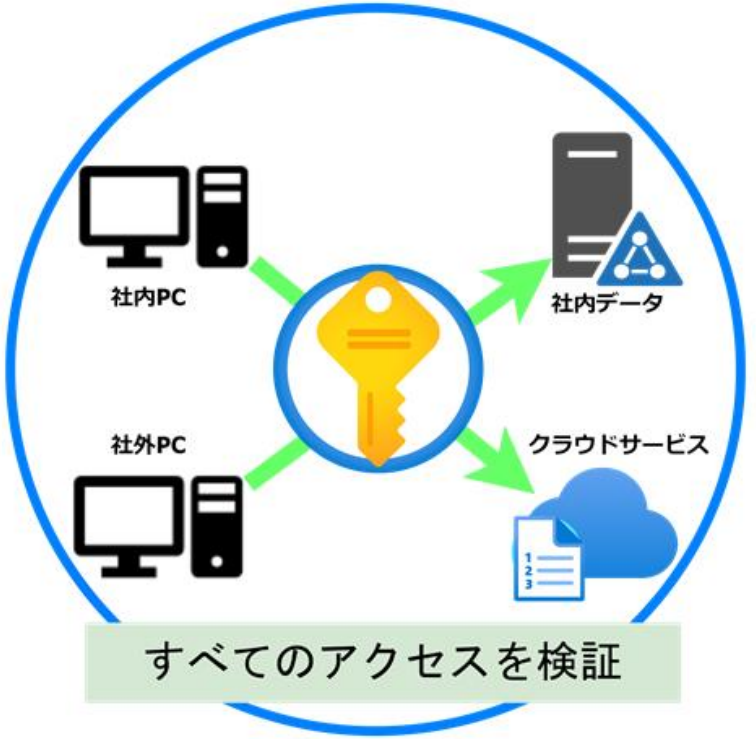
ゼロトラストとは？～「全てを信頼しない」セキュリティ対策 ～

ゼロトラストとは？

トラスト（信頼）＝ゼロ（無い）という名の通り「全てを信頼しない」という考え方から、セキュリティ対策を行います。

内部・外部からのアクセスを問わず、すべてを疑い、検証

テレワークの増加から社内外問わずサービス・データへの接続が行われる現在のセキュリティ対策として有効な手段と言えるでしょう。



ゼロトラストとは？～「全てを信頼しない」セキュリティ対策 ～

ゼロトラストを実現するための７つの要件

#	要件	対応例
1	ネットワークセキュリティ	端末ごとの認証を行い、未許可の端末のアクセスを拒否する等、条件を満たした端末のみネットワークやリソースにアクセスさせる
2	デバイスセキュリティ	従来のセキュリティ製品やEDR製品（侵入後の対策）を導入し、端末を脅威から守る
3	アイデンティティセキュリティ（ID管理）	多要素認証による不正アクセスの防止や、統合ID管理によるIDのメンテナンスを常に行い、IDの不正利用を防ぐ
4	ワークロードセキュリティ	全ての機器やシステムの脆弱性等を可視化し、早期の対処を行い脅威を未然に防ぐ
5	データセキュリティ	データ自体を保護し、内部情報の持ち出しや、外的要因の情報漏洩を防止する
6	可視化・分析	セキュリティ状態を可視化し、攻撃を受けた際は内容の検出や分析、対応を行う
7	自動化	セキュリティの問題発生から対処までの流れを自動化する

- アメリカの調査会社「Forrester Research」が提唱する７つの要件を重視する必要
- 何か一つ製品を導入すればゼロトラストを実現できるというものではない
- ７つの要件を基に複数の製品・サービスを組み合わせて導入する必要がある

ゼロトラストとは？～「全てを信頼しない」セキュリティ対策 ～

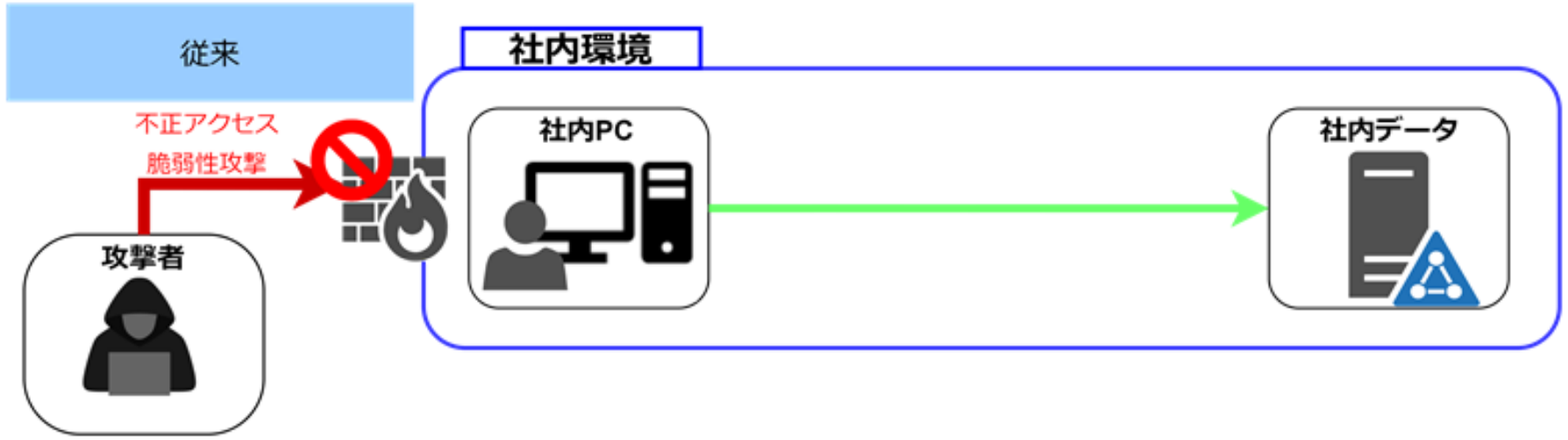
ゼロトラストとは

- すべてを信頼しない新時代のセキュリティ対策
- 7つの要件を考慮しながら構築する必要がある
- 何か1つ製品を導入すればいい、というものではない

従来の「境界型セキュリティ」との違いと、ゼロトラストの必要性

従来の「境界型セキュリティ」との違いと、ゼロトラストの必要性

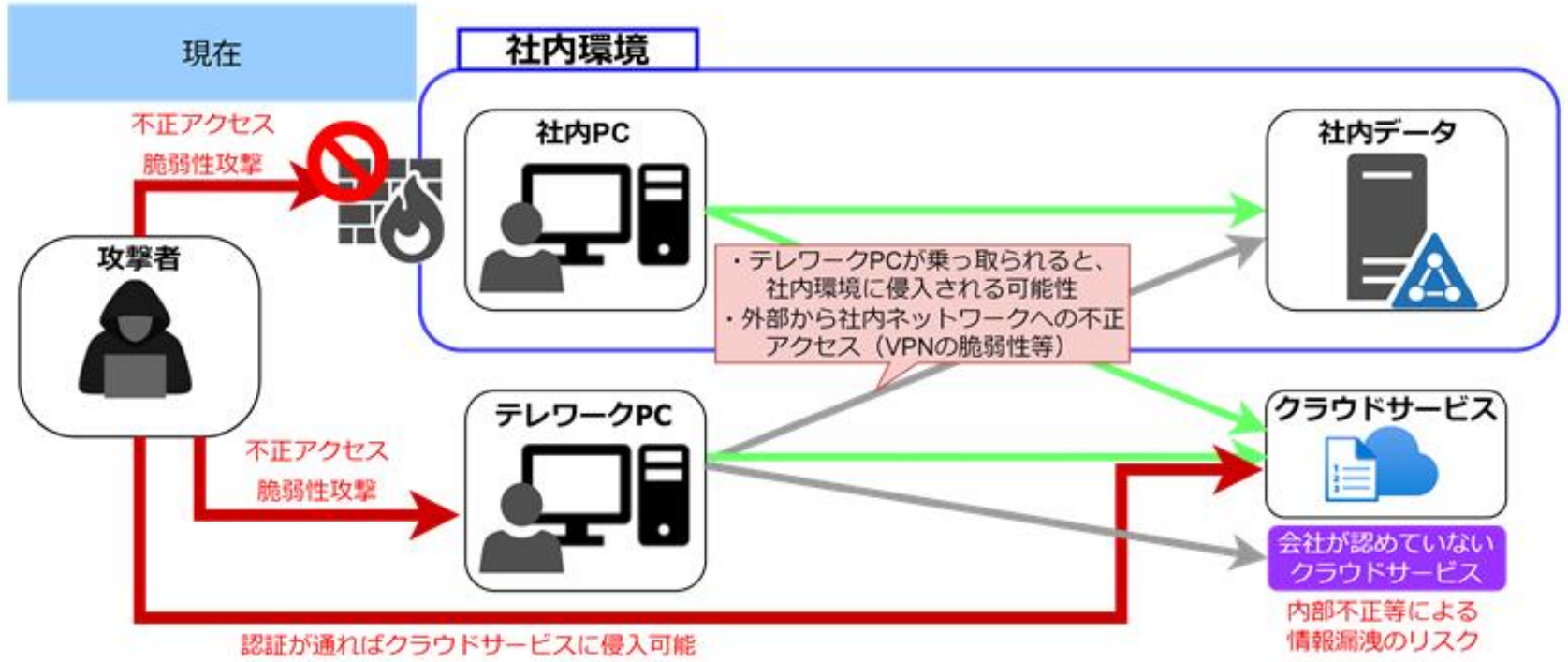
境界型セキュリティとは？



- 内部と外部の間に境界線（ファイアーウォール）を引き、その境界線にのみセキュリティ対策を行う方法
- 社内ネットワークに入れた者は全て信頼される

従来の「境界型セキュリティ」との違いと、ゼロトラストの必要性

- 境界型セキュリティは危険？

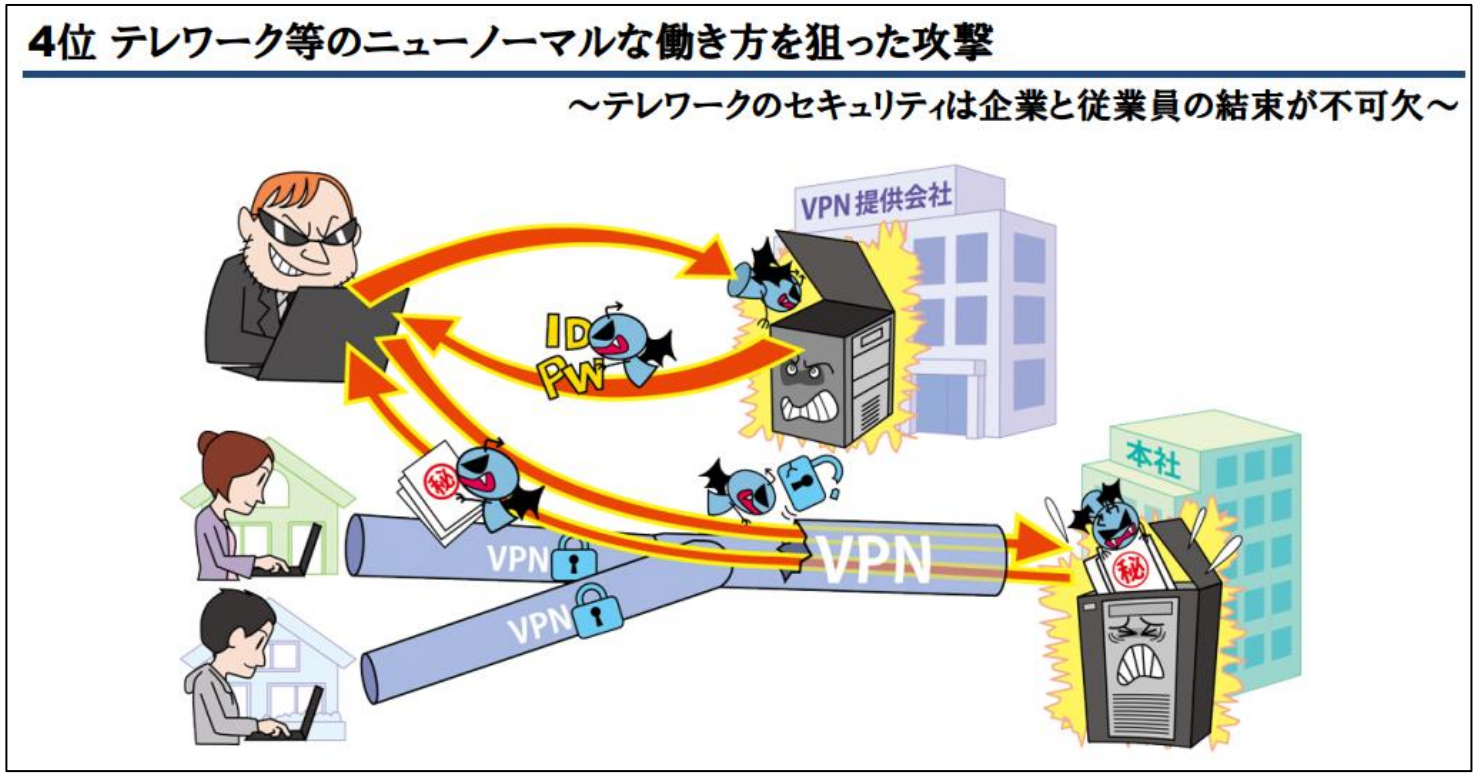


これまでの境界の外側に端末やクラウドサービスが位置するため、
セキュリティリスクは増大します。

従来の「境界型セキュリティ」との違いと、ゼロトラストの必要性

脅威も新時代の形に

IPAの10大脅威においても、テレワーク等のニューノーマルな働き方を狙った攻撃は4位にランクインしております。境界の外へ端末が出ている、VPNで接続が恒常的に行われていることは、対策をしていないと攻撃者から狙われやすいセキュリティホールにもなりえます。



IPA情報処理推進機構 「情報セキュリティ10大脅威2022」解説書より引用
https://www.ipa.go.jp/security/vuln/10threats2022.html

従来の「境界型セキュリティ」との違いと、ゼロトラストの必要性

ゼロトラストの必要性

- 境界の外に出ているものを守る必要が出てきた
- 境界があいまいになってきているため

境界型防御は必要無くなる？

- いきなりゼロトラストの7つの要件を満たした環境を構築するのは難しいため、現在の境界型セキュリティを維持したまま、段階的にゼロトラスト化をすすめていく「ハイブリッド環境」がIPA（独立行政法人 情報処理推進機構）のゼロトラスト指南書のモデルケースとしても紹介されております。

ゼロトラストを始めるためには

ゼロトラストを始めるためには

7つの要件をすべて満たす必要があるのか？

#	要件	製品例
1	ネットワークセキュリティ	SWG (Secure Web Gateway)、SDP (Software Defined Perimeter)
2	デバイスセキュリティ	EDR (Endpoint Detection and Response)、 MDM (Mobile Device Management)
3	アイデンティティセキュリティ（ID管理）	IDaaS(Identity As A Service)、 IAM (Identity and Access Management)
4	ワークロードセキュリティ	CWPP (Cloud Workload Protection Platform)
5	データセキュリティ	DLP (Data Loss Prevention)
6	可視化・分析	CASB (Cloud Access Security Broker)、SIEM (Security Information and Event Management)
7	自動化	SOAR (Security Orchestration and Automation Response)

- 7つの要件を満たすべく全ての製品が導入されていることが望ましい
- 全てを満たすには多大なコストがかかる
- 段階的にゼロトラストを導入していく「ハイブリッド環境」から始めることを推奨します

ゼロトラストを始めるためには

何が必要かを考える

機密情報を守るためにはどこを強化するべきなのか（アカウント（ID）、デバイス（PC・スマートフォン）、ネットワーク等）を考え、製品を導入していくことを推奨します。

例

- テレワークPC自体を守りたい　⇒　EDR製品
- クラウドサービスの認証を強化したい　⇒　IDaaS製品
- VPNに替わる通信手段の導入をしたい　⇒　SDP製品

ゼロトラストを始めるためには

スタイルズの考える導入順

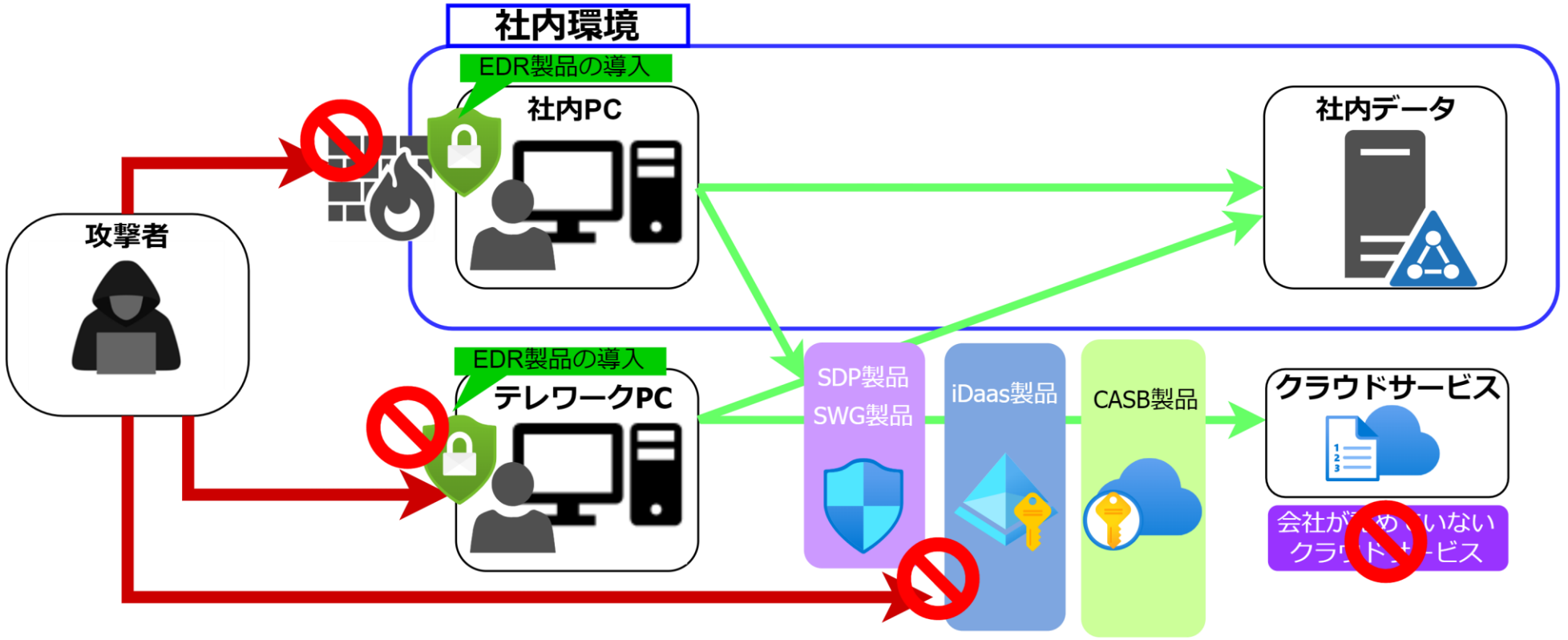
7つの要件を大別して以下の3つのソリューション群に分けられると考えます。

分類	保護対象	ソリューションの例
ユーザ認証・認可	ログイン情報	IDaaS
エンドポイントセキュリティ	PC、モバイル端末	EDR、EPP
ネットワーク/クラウドセキュリティ	リモート接続者/クラウド利用者	SWG、SDP、CASB、CSPM

どこから対策を始めればいいか分からない方や、クラウド・テレワークのセキュリティを向上させたい方は上図の上から対策を始めていくこと推奨します。

ゼロトラストを始めるためには

- スタイルズの考える導入の例



ゼロトラストを始めるためには

ゼロトラストの始め方

- ハイブリッド環境から始めてみる（段階的導入）
- どこを守りたいのかを考えてみる
- スタイルズの推奨は

  ①ユーザ認証・認可製品

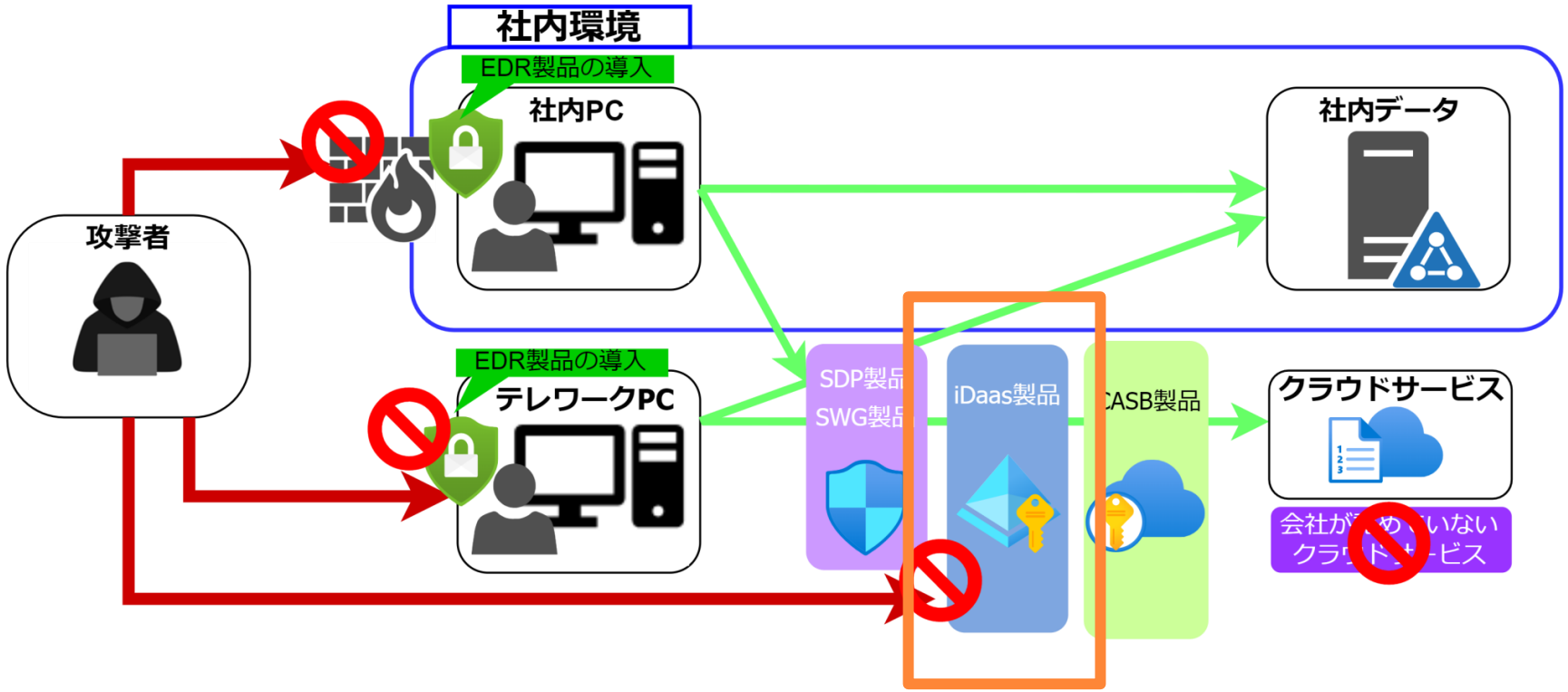
  ②エンドポイントセキュリティ製品

  ③ネットワーク/クラウドの順

ゼロトラスト導入の第一歩：ユーザ認証・認可

ゼロトラスト導入の第一歩：ユーザ認証・認可

分類	保護対象	ソリューションの例
ユーザ認証・認可	ログイン情報	IDaaS
エンドポイントセキュリティ	PC、モバイル端末	EDR、EPP
ネットワーク/クラウドセキュリティ	リモート接続者/クラウド利用者	SWG、SDP、CASB、CSPM



ゼロトラスト導入の第一歩：ユーザ認証・認可

ユーザ認証・認可のIDaaSとは？

ユーザーIDやパスワードなどのログイン情報の管理や認証を行うソリューションです。

主な機能

- 各種クラウドサービス等への認証（多要素認証，シングルサインオン）
- 認可（アクセスコントロール）
- ID 管理
- ID 連携

複雑化・多様化するクラウドサービスなどのID認証やアクセス権限の管理などを一元化して行っているのがIDaaSです。

ゼロトラスト導入の第一歩：ユーザ認証・認可

IDaaSの機能説明

- ユーザー認証
  - 多要素認証
    パスワードに加え指紋やスマートフォン等のデバイスで２つ以上の要素を用いて認証を行う
  - シングルサインオン
    ひとつのID/パスワードで複数のサービスを利用することができる
- 認可

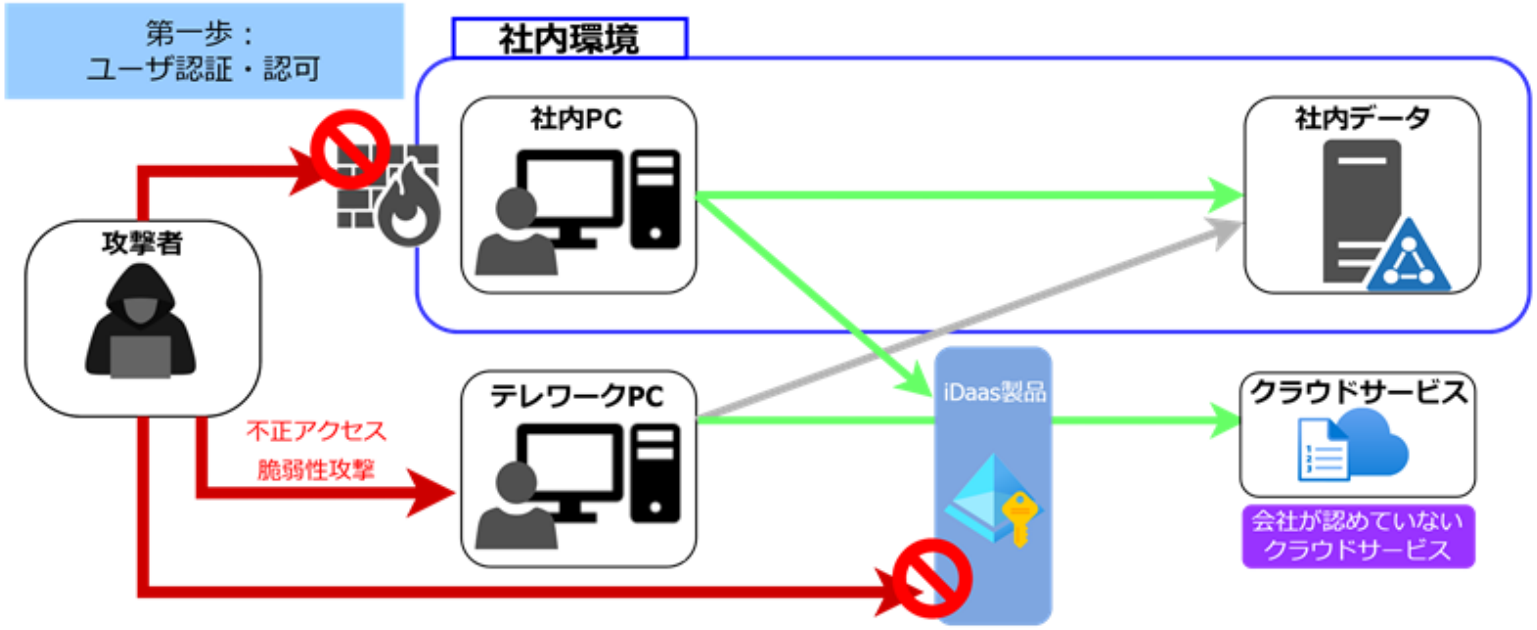
  アクセスできる場所やパソコンを限定しアクセスを制限することや、
  閲覧・変更等の操作を社員の役割ごとに限定できます。
- ID管理

  IDaaSで管理しているIDの作成／変更／削除などを行う機能。
- ID連携

  ID管理などで変更したユーザ情報をほかのクラウドサービスにも
  同期させることができる機能

ゼロトラスト導入の第一歩：ユーザ認証・認可

なぜ最初に導入するべきなのか、メリット

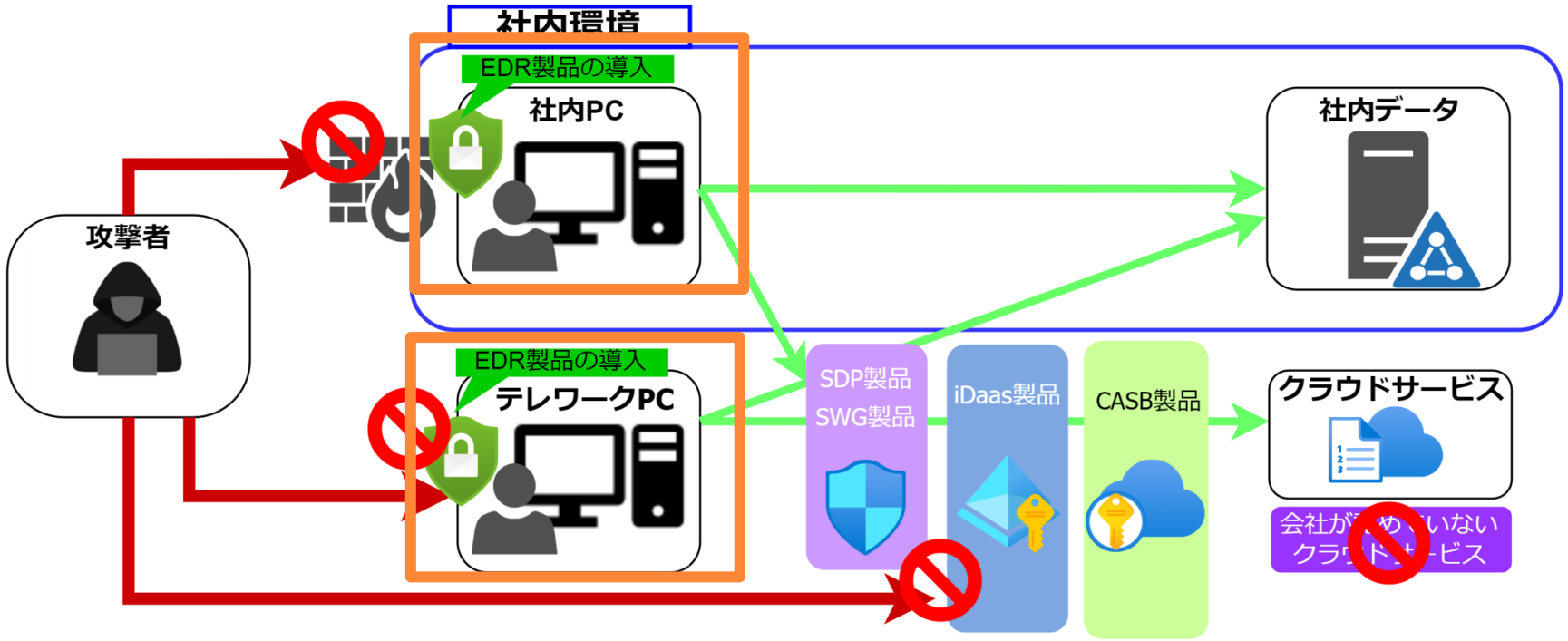


- 多要素認証によりクラウドサービス利用のセキュリティ向上
- 認可機能でユーザごとの役割を決め、社内不正を防止する
- シングルサインオンやID管理による利便性向上
- 適切なID管理はゼロトラストの基盤

ゼロトラスト導入の第二歩：エンドポイントセキュリティ

ゼロトラスト導入の第二歩：エンドポイントセキュリティ

分類	保護対象	ソリューションの例
ユーザ認証・認可	ログイン情報	IDaaS
エンドポイントセキュリティ	PC、モバイル端末	EDR、EPP
ネットワーク/クラウドセキュリティ	リモート接続者/クラウド利用者	SWG、SDP、CASB、CSPM



ゼロトラスト導入の第二歩：エンドポイントセキュリティ

エンドポイントセキュリティ製品のEDRとは？

EDRとはEndpoint Detection and Responseの略称であり、端末の動きを監視し、侵入されてしまった後の対処をするエンドポイントセキュリティ製品です。

アンチウイルスソフトとの違いは？

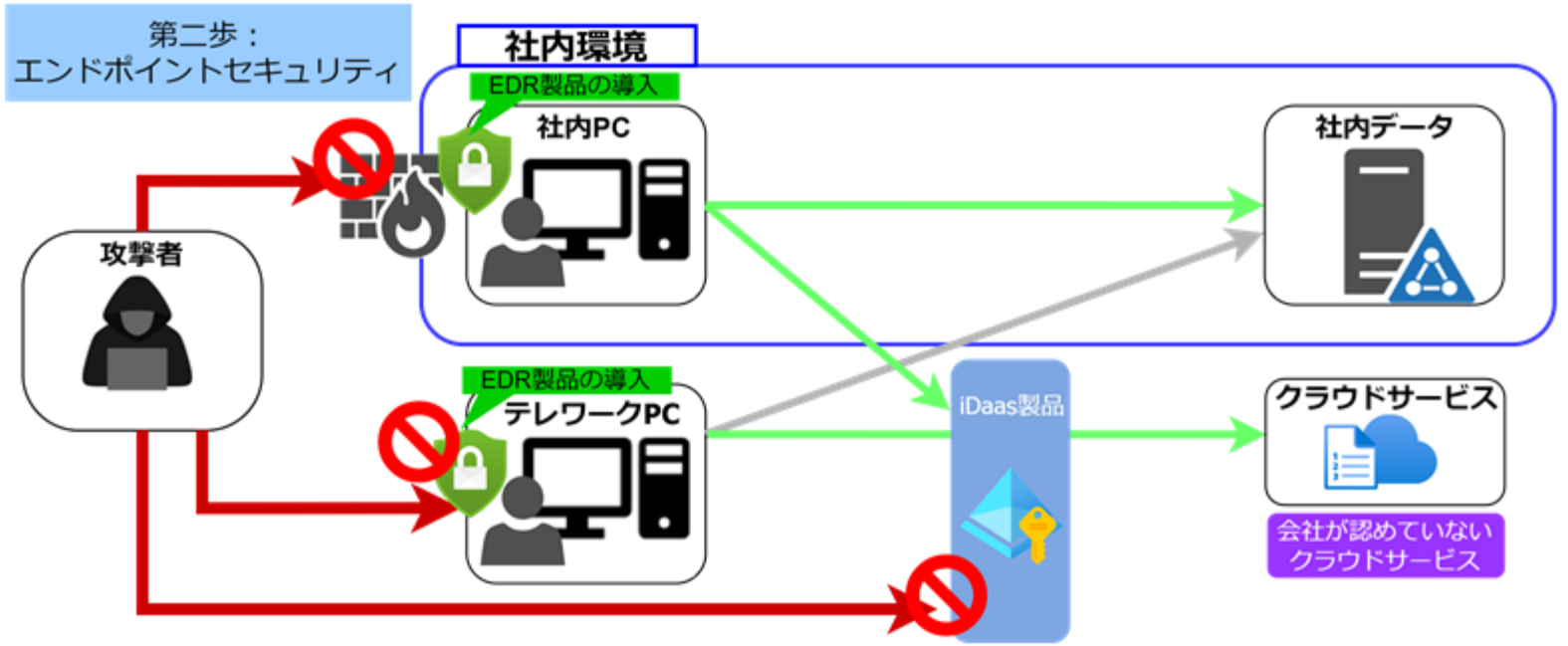
デバイスの保護といえばアンチウイルスソフト（セキュリティソフト）を思い浮かべると思います。EDRとアンチウイルスソフトの違いは以下です。

アンチウイルスソフト
パターンマッチ等によるマルウェア等の侵入を未然に防ぐ製品

EDR
侵入されることを前提に考えた、侵入後の対処をする製品

ゼロトラスト導入の第二歩：エンドポイントセキュリティ

なぜ導入するべきなのか・メリット

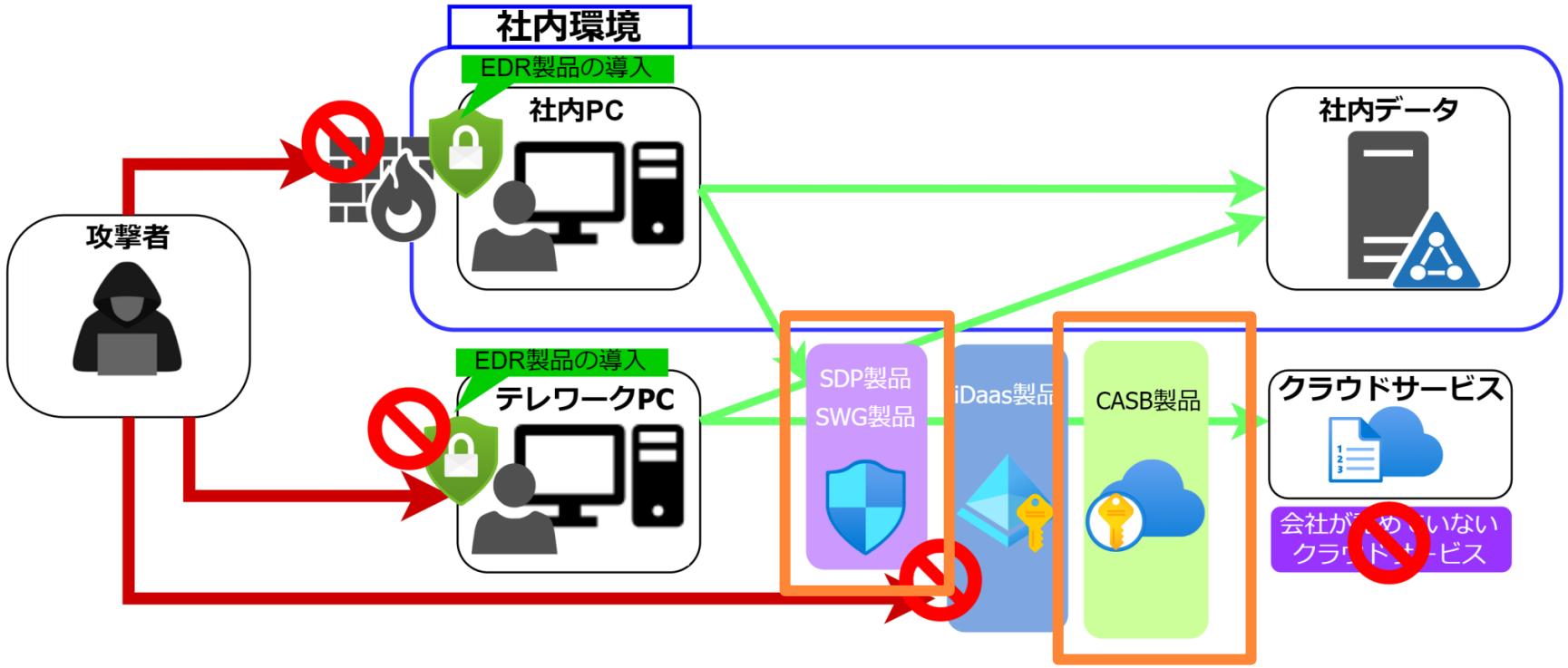


- テレワークにより低下したセキュリティを強化することができる
- 未知のマルウェアに感染しても、端末の動きで検知可能

ゼロトラスト導入の第三歩：ネットワーク/クラウドセキュリティ

ゼロトラスト導入の第三歩：ネットワーク/クラウドセキュリティ

分類	保護対象	ソリューションの例
ユーザ認証・認可	ログイン情報	IDaaS
エンドポイントセキュリティ	PC、モバイル端末	EDR、EPP
ネットワーク/クラウドセキュリティ	リモート接続者/クラウド利用者	SWG、SDP、CASB、CSPM



ゼロトラスト導入の第三歩：ネットワーク/クラウドセキュリティ

ネットワークセキュリティとは？

ネットワークの各種アクセス権限を設定するとともに、セキュリティを確保するソリューションです。

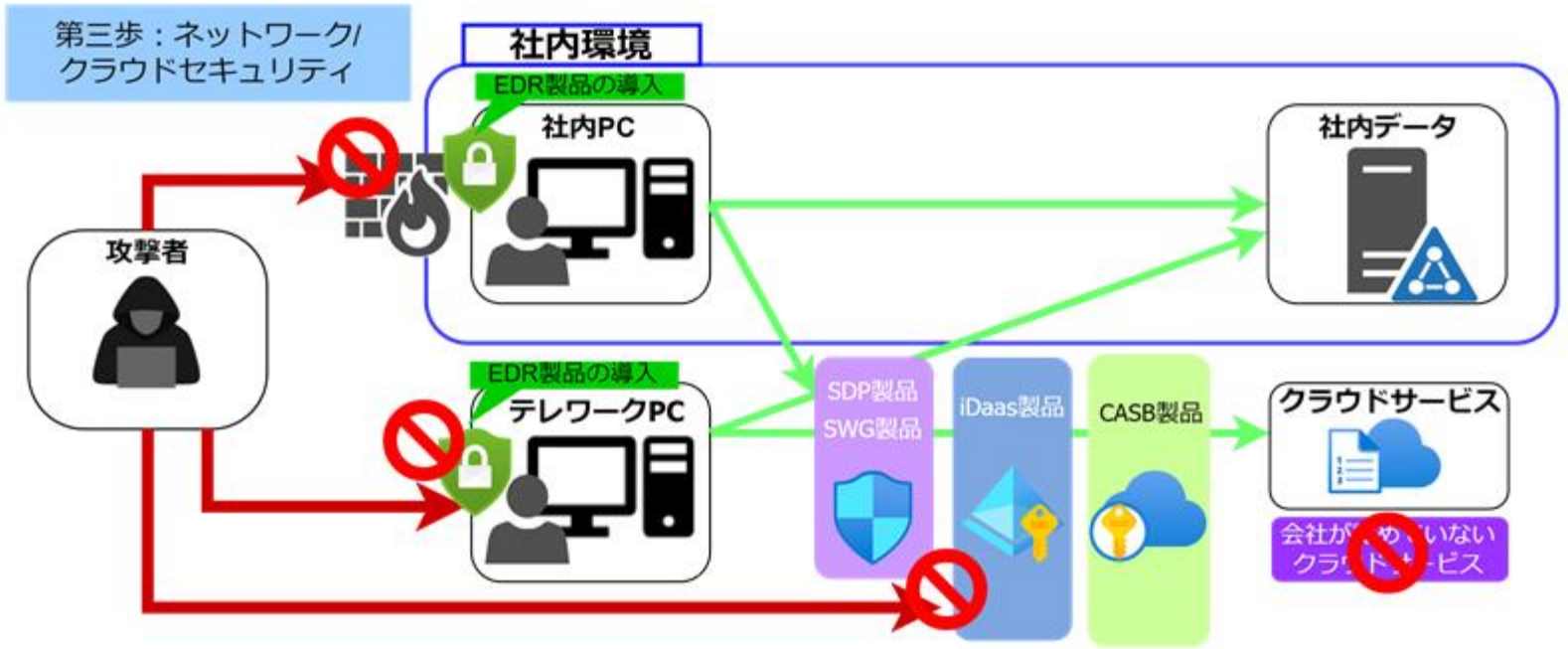
危険なサイトなどへのアクセスを遮断するSWG（Secure Web Gateway）、リアルタイムに接続可否を判断するSDP（Software Defined Perimeter）などがあります。

クラウドセキュリティとは？

クラウドサービスの利用状況を可視化・制御するCASB（Cloud Access Security Broker）、クラウドサービスの安全性を確認するCSPM（Cloud Security Posture Management）などがあります。

ゼロトラスト導入の第三歩：ネットワーク/クラウドセキュリティ

なぜ導入するべきなのか・メリット



- 会社が認めていないクラウドサービスを利用させない
- クラウドの利用状況確認・制御による不正防止
- 外部からの社内ネットワークへの接続防止

クラウド・テレワークの脅威とゼロトラストによる対策

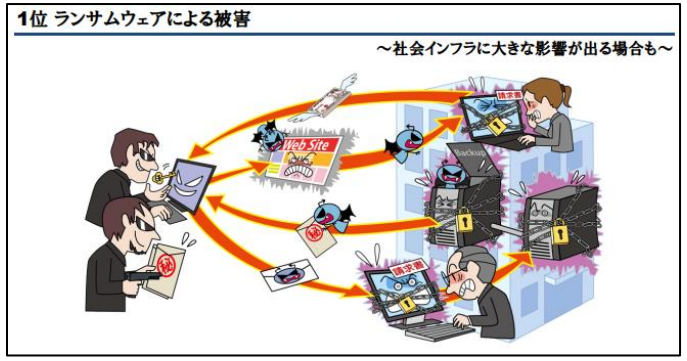
クラウド・テレワークの脅威とゼロトラストによる対策

クラウド・テレワークにおけるセキュリティリスク

- テレワークPCに対する攻撃
- VPN機器の脆弱性をついた攻撃
- クラウドサービスの認証情報搾取による情報漏洩

IPA10大脅威

4位のテレワーク等を狙った攻撃以外にも、クラウド・テレワークに関する脅威があります。
例えば、1位のランサムウェアによる被害では、アメリカ最大の石油パイプライン会社がVPN認証を突破されてランサムウェアに感染し、5日間営業停止した事例も紹介されております。



IPA情報処理推進機構 「情報セキュリティ10大脅威2022」解説書より引用
https://www.ipa.go.jp/security/vuln/10threats2022.html

ゼロトラストでの重要な対策

クラウドサービスやテレワークの普及、ランサムウェア被害の拡大などの背景から、
「ゼロトラストセキュリティ」への移行をしていく中で重要な要素は

『本人』であるかどうか

『本人』を特定するクラウド認証基盤が

IDaaS（Identity as a Service）

IDaaSについて再確認

主に以下のような機能を有します。

- 多要素認証
- シングルサインオン
- 認可（アクセス制御）
- ID管理・ID連携

何に対して有効なのか？

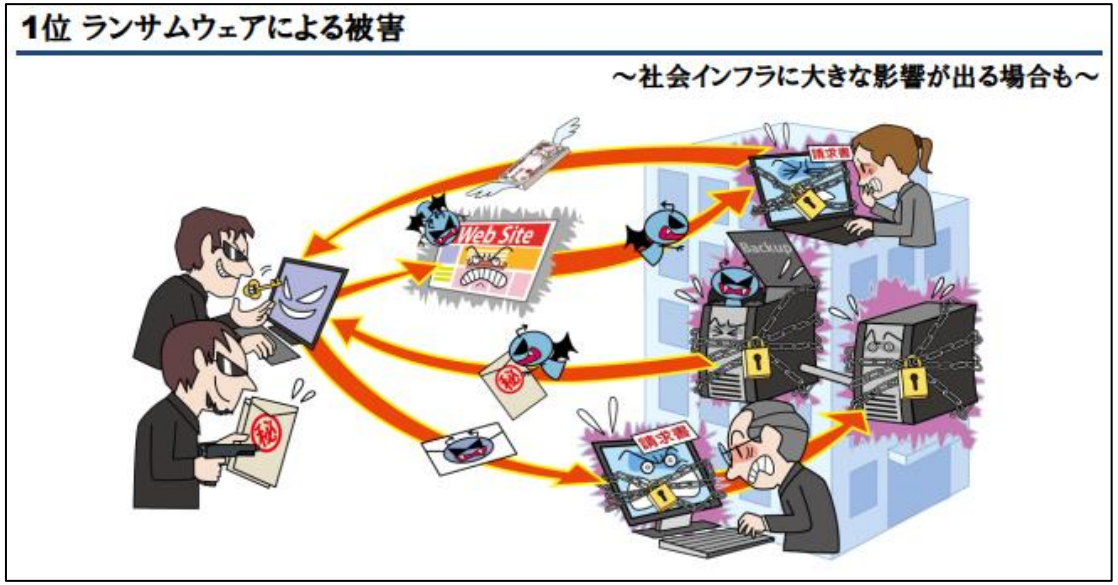
IPAの10大脅威解説書の中で多要素認証は、「１位：ランサムウェアによる被害」「４位：テレワーク等のニューノーマルな働き方を狙った攻撃」、「８位：ビジネスメール詐欺による金銭被害」に有効と記載されています。

その他にもIDaaSで対策できる脅威があります

クラウド・テレワークの脅威とゼロトラストによる対策

- IPA10大脅威への対応　１位　ランサムウェアによる被害

PC、ネットワークがランサムウェアに感染すると、システムやPCへのアクセスがロックされるか、保存されているファイルを暗号化され使用できなくなります。その復旧と引き換えに金銭を要求（脅迫）されます。



IPA情報処理推進機構 「情報セキュリティ10大脅威2022」解説書より引用
https://www.ipa.go.jp/security/vuln/10threats2022.html

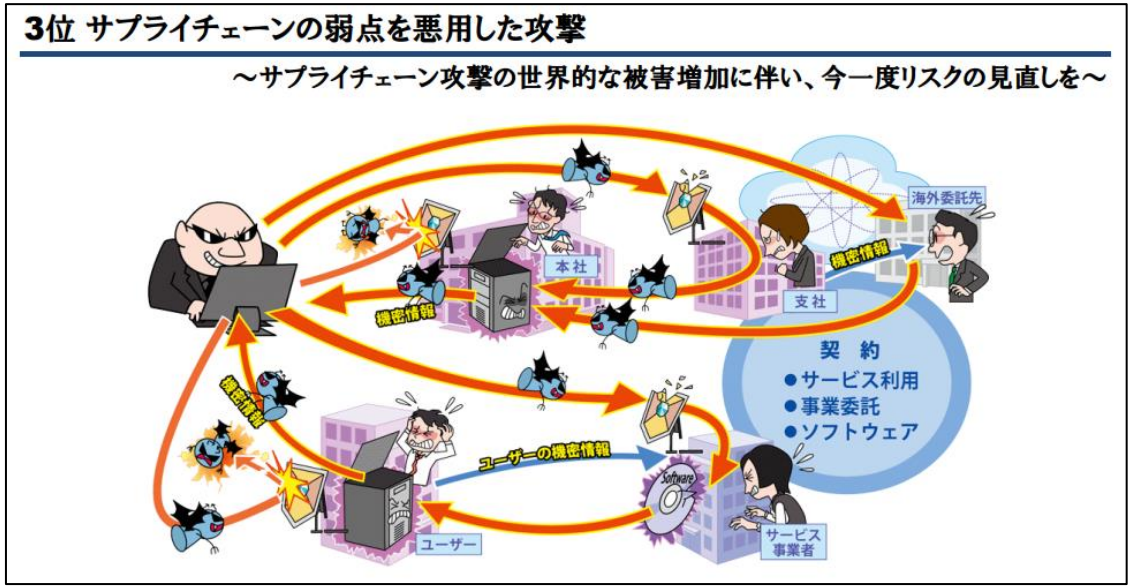
- IDaaSの対策
  - VPN認証の強化

    先ほど紹介したアメリカのパイプライン会社の例では、VPNの認証に多要素認証を導入していれば被害を防げていた可能性が高いです。

クラウド・テレワークの脅威とゼロトラストによる対策

- IPA10大脅威への対応　3位　サプライチェーンの弱点を悪用した攻撃

標的となる組織の取引先や委託先を攻撃し、標的組織の情報を搾取する攻撃です。



IPA情報処理推進機構 「情報セキュリティ10大脅威2022」解説書より引用
https://www.ipa.go.jp/security/vuln/10threats2022.html

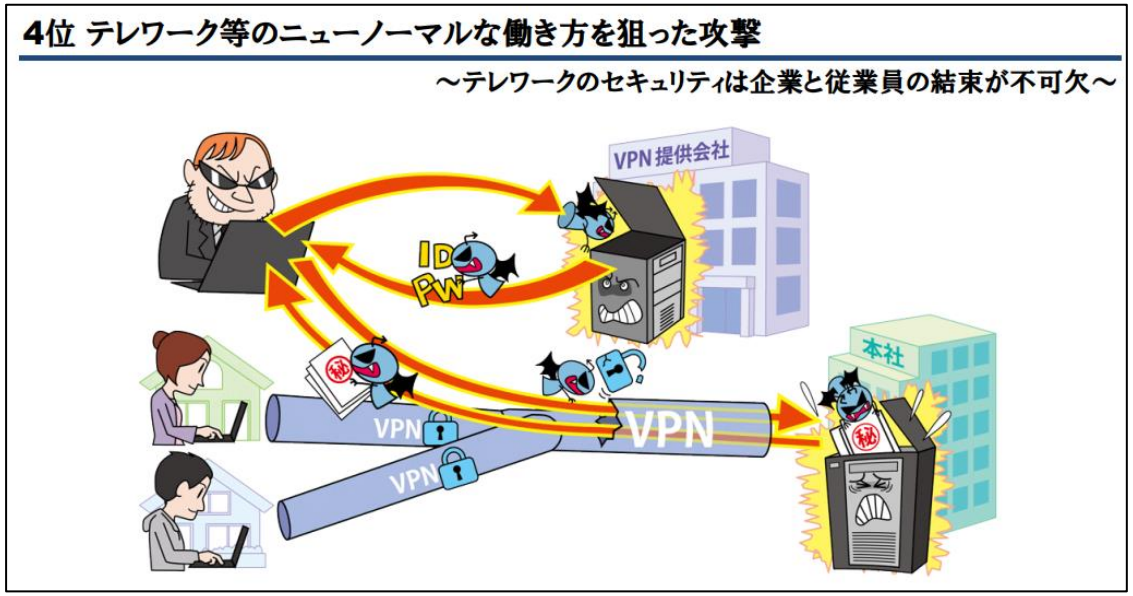
- IDaaSの対策
  - 委託先にプラットフォームを提供

クラウドストレージを用意し、自社に関わる情報を保管・管理する環境として利用してもらい、そのクラウドストレージの認証にIDaaSを活用することで、情報の搾取を防ぐことが可能。

クラウド・テレワークの脅威とゼロトラストによる対策

- IPA10大脅威への対応　4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

これまでの境界型防御で守られていたデバイスが境界の外に出ることによりセキュリティが低下し、そこに目を付けた攻撃です。



IPA情報処理推進機構 「情報セキュリティ10大脅威2022」解説書より引用
https://www.ipa.go.jp/security/vuln/10threats2022.html

- IDaaSの対策
  - VPN認証の強化

    多要素認証をVPN接続のログインに適用することで、IDとパスワードが漏洩してしまった場合でも、不正アクセスを防ぐことが可能です。

クラウド・テレワークの脅威とゼロトラストによる対策

IPA10大脅威への対応　5位　内部不正による情報漏えい

組織の従業員や元従業員、組織の関係者による不正行為で機密情報が漏洩する脅威です。

IPA情報処理推進機構 「情報セキュリティ10大脅威2022」解説書より引用
https://www.ipa.go.jp/security/vuln/10threats2022.html

IDaaSの対策

適切なID管理運用・認可機能の活用

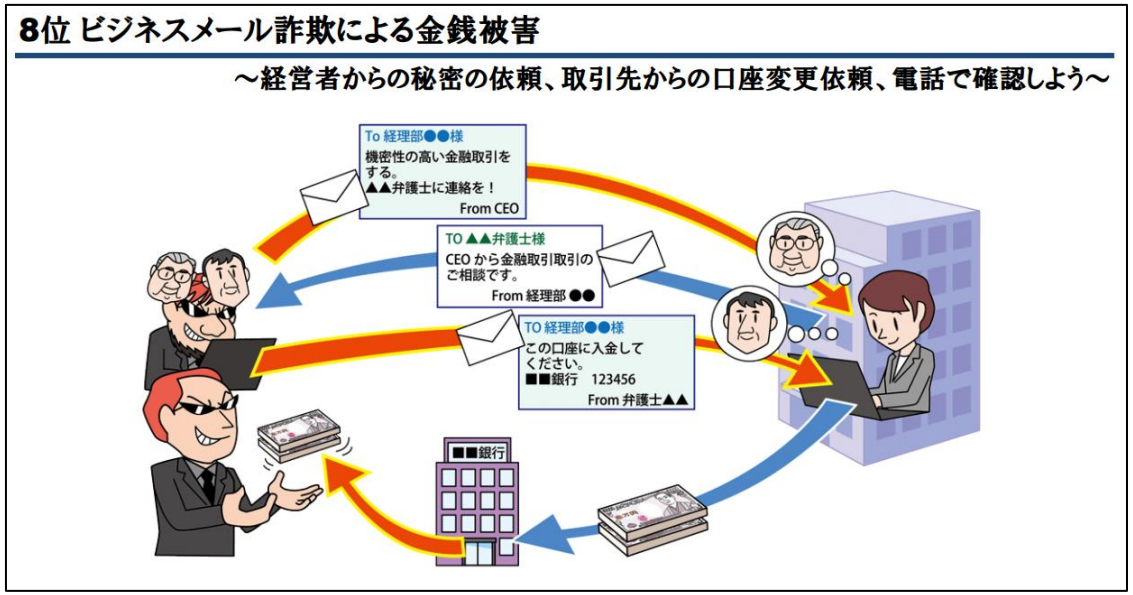
IDaaS製品のプロビジョニング機能を利用すれば、ID管理作業の負担も軽減され、退社したユーザーのアカウントが残り続けるといったセキュリティリスクを減らすことができます。

また、認可機能によりクラウドサービスにアクセスが可能な利用者や端末、場所等に制限をかけ、情報漏洩のリスクを減らすことができます。

クラウド・テレワークの脅威とゼロトラストによる対策

IPA10大脅威への対応　8位　ビジネスメール詐欺による金銭被害

取引先や経営者になりすましたビジネスメールを送り、企業の金銭を取り扱う担当者を騙し、攻撃者の口座へ金銭を振り込ませる脅威です。



IPA情報処理推進機構 「情報セキュリティ10大脅威2022」解説書より引用
https://www.ipa.go.jp/security/vuln/10threats2022.html

IDaaSの対策

メールアカウントの認証の強化

メールアカウントを搾取され、なりすましをされるケースがあるため、多要素認証をメールアカウントの認証に用いることでなりすましを防ぐことができます。

クラウド・テレワークの脅威とゼロトラストによる対策

- IDaaSで何が解決できる？
  - 多要素認証による認証強化で不正アクセスの防止
  - シングルサインオンによる利便性向上
  - 認可（アクセス制御）による社内不正防止
  - IDの適切な管理によるセキュリティリスク低減

まずはIDaaSの導入から始めることを推奨します

IDaaS＆ゼロトラストサービス

・AzureADによるIDaaS実現
　（シングルサインオンと多要素認証の実現）
・オンプレADとの連携
・SAML非対応のSaaSや社内Webシステムも対応
・ IDプロビジョニング（IDや権限の連携）も対応

株式会社スタイルズ

お客様の悩みにお答えするスタイルズのIDaaS&ゼロトラスト

シングルサインオンやIDaaSの導入で悩んでいませんか？

- クラウドサービスが増えてID、パスワード管理が大変！
- クラウドサービスに不正アクセスされないか不安・・・
- 人事異動や入退社時のアカウントや権限対応がしんどい・・・

スタイルズは、お客様の抱えるID周りのお悩みを、
AzureAD、Keygateway、IDプロビジョニングツール等の
様々なサービスを組み合わせて適切なサービス構成をご提案します。

お悩み１：クラウドと社内のIDを統合管理したい！

解決方法：AzureADによるIDaaS導入、社内ADとの連携

AzureADは、マイクロソフトが提供するIDaaSサービスとなります。主にクラウドサービスのID管理に利用されます。
社内のID管理と言えば、ActiveDirectory（AD）が有名ですが、AzureADは社内ADとID連携できるため、IDの管理を統合できます。Microsoft365（旧Office365）を契約している場合、無料でAzureADが使えるため、すでにIDaaSを導入されている可能性があります。

おすすめポイント

•AzureADは、社内ADとID情報を連携できるため、IDの統合管理ができる。
•既に導入されている場合は、AzureADを活用できる。新たにID管理（IDaaS）の導入や管理をする必要がない。

お悩み２：社内システム（Web）もシングルサインオンしたい！

解決方法：Keygateway でSAML認証非対応システムもシングルサインオン可能

AzureADのシングルサインオンは、すべてのクラウドサービスや社内システム（Web）に対応しているわけではありません。

AzureADで社内システム（Web）のシングルサインオンを対応する場合、社内にリバースプロキシサーバ等を構築して運用・管理する必要があります。また、SAML認証非対応のクラウドサービスもシングルサインオンできるようにしたい方も多いと思います。

おすすめポイント

•弊社が取り扱っているKeygatewayはクラウドサービスのため、社内システム（Web）のシングルサインオン対応による運用・管理負担を軽減できます。
•SAML認証非対応のクラウドサービスもKeygatewayサービスを使ってSAML認証と同様のシングルサインオンに対応できます。

お悩み３：ID連携（プロビジョニング）できる対象を増やしたい

解決方法：弊社IDプロビジョニングツールで広範囲のID連携を実現

AzureADのIDプロビジョニングは、シングルサインオンと比較して対応しているシステムが少ないのが現状です。

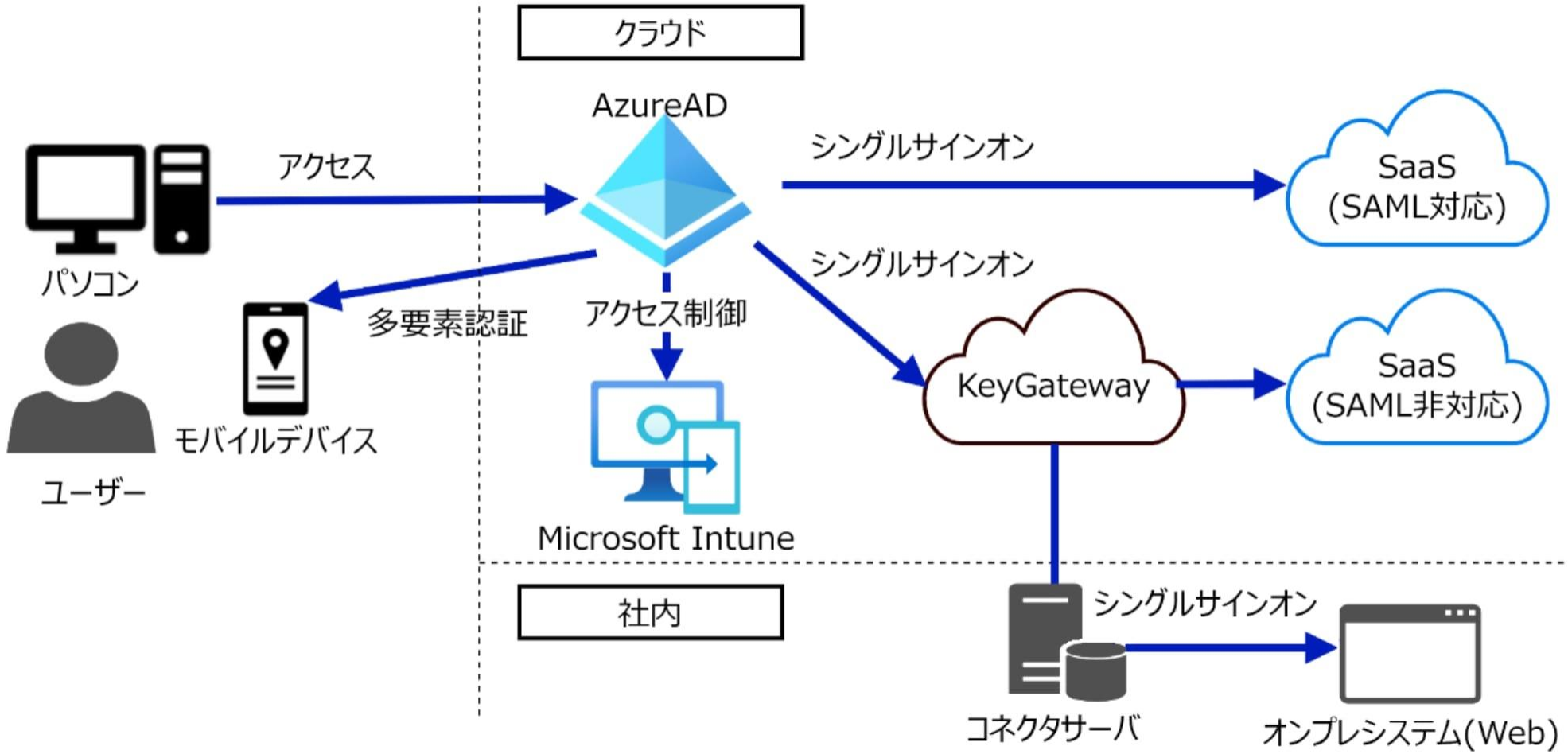
AzureADでもシングルサインオンに対応しているシステム数が数千に対して、IDプロビジョニングの対応数は約250となります。（2021年12月現在）クラウドサービスが普及して数が増していく中、IDプロビジョニングによる作業負荷軽減を求める方も多いと思います。

おすすめポイント

•弊社IDプロビジョニングツールでは、AzureAD等のIDaaSで対応できないシステムにもID連携（プロビジョニング）することができます。
•IDプロビジョニングする人事情報をAD、CSVファイルなど多彩なデータ形式で取り込み、各システムへ連携することができます。

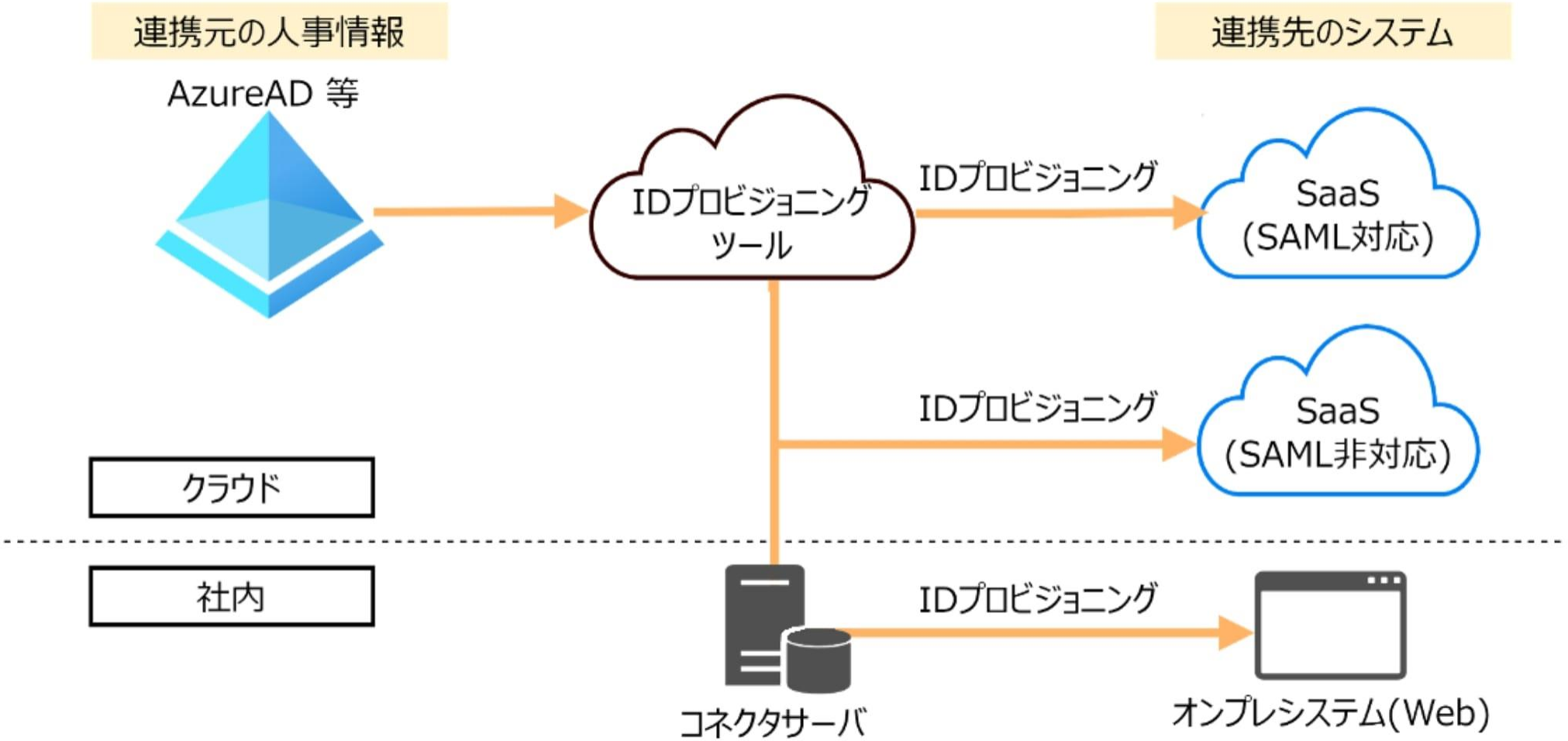
スタイルズのIDaaSサービスの構成例

シングルサインオン構成。



スタイルズのIDaaSサービスの構成例

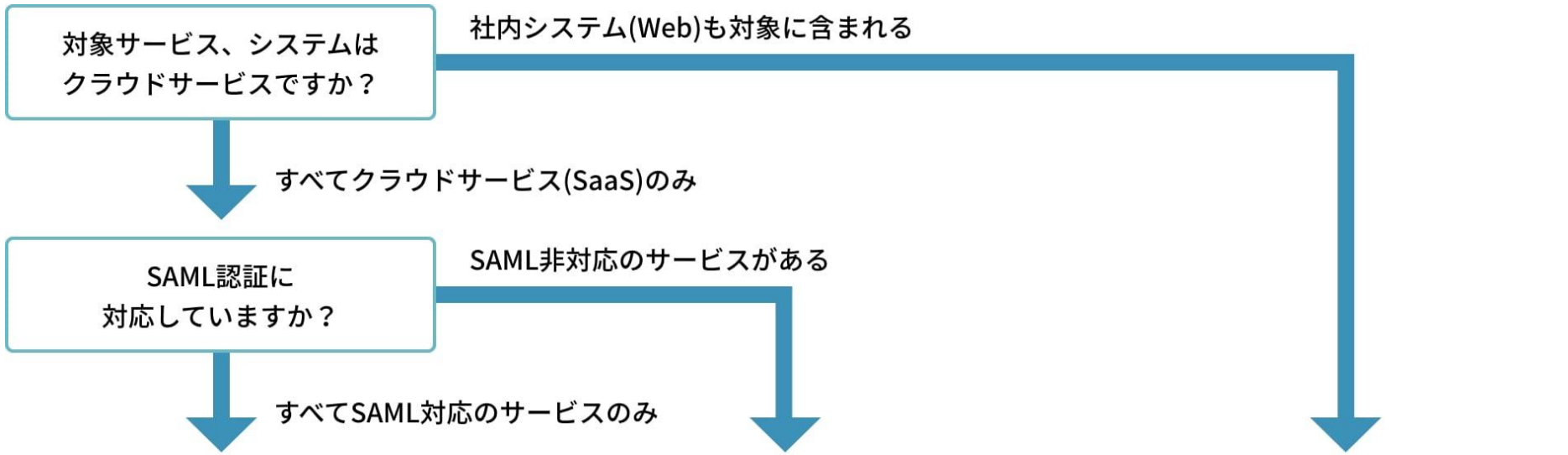
IDプロビジョニング構成



スタイルズのIDaaSサービスの構成例

製品	機能	対象	備考
AzureAD	シングル サインオン	クラウドサービス （SaaS：SAML対応）	AzureADの無料ライセンスでご利用できます。 クラウドサービス側でシングルサインオン機能が使用できるプランである必要があります。
	多要素認証	クラウドサービス（SaaS） 社内システム（Web）	一部機能はAzureADの無料ライセンスでご利用できます。
AzureAD Intune	アクセス制御	クラウドサービス（SaaS） 社内システム（Web）	Azure Active Directory Premium P1が必要になります。デバイスやアプリベースによるアクセス制御を行う場合は、Intuneが必要になります。
Keygateway	シングルサイン オン	クラウドサービス （SaaS：SAML非対応） 社内システム（Web）	KeygatewayやIDプロビジョニングツールは、クラウドサービス（SaaS）のため、対象がクラウドサービスのみであれば、社内にサーバ等は不要です。ただし、社内システムも対象とする場合は、社内にコネクタサーバを設置する必要があります。
IDプロビジョ ニング ツール	IDプロビジョニ ング	クラウドサービス（SaaS） 社内システム（Web）	

スタイルズのIDaaSサービスメニュー



SAML対応プラン

クラウドサービス（SAML認証対応）へのシングルサインオンや多要素認証の導入

AzureADで構成

SAML非対応プラン

クラウドサービスへのシングルサインオンや多要素認証の導入

AzureAD、KeyGatewayで構成

社内システム対応プラン

クラウドサービスおよび社内システム（Web）へのシングルサインオンや多要素認証の導入

AzureAD、KeyGateway、コネクタサーバで構成

オプションサービス

オプション	概要
IDプロビジョニング	人事情報を各プランの対象システムに連携して、アカウントや権限の設定を自動化する。 IDプロビジョニングツールを導入
アクセス制御	デバイス制御やアクセス元のIPアドレス制御などを実装する アクセス制御方法によりIntuneを導入
ActiveDirectory連携	既存ActiveDirectoryのIDをAzureADに連携する 社内にAzureAD Connectサーバを導入

前提条件

- AzureAD、Intune等のライセンス費用は、お客様にて製品ベンダーと契約していただきます。
  ライセンスは利用ユーザー分必要となります。
- 構築期間中から発生するライセンス費用は、お客様にて負担していただきます。
- お見積りの価格は、ユーザー数やシステム数により変動します。また、お客様の解決したい課題、ゴールによっても変動します。

価格

お客様ごとに対応する規模や内容が異なるため、ヒアリング後にお見積りをいたしますので、まずはお問い合わせフォームよりご連絡ください。弊社営業より折り返し、ご返信差し上げます。

お問合せ、ご相談は株式会社スタイルズ https://www.stylez.co.jp まで

実績豊富なエンジニア集団の技術と開発ツールで「開発期間/コスト削減」「品質向上」を実現

株式会社スタイルズ

https://www.stylez.co.jp

東京都千代田区神田小川町1-2　風雲堂ビル6階

Tel:03-5244-4111

オープンソースソフトウェア推進