CloudShift

Stylez

株式会社スタイルズ

2022年6月7日

30分でわかる！2022年IPA10大脅威に対する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

- 会社が晒されている脅威について知識を深めたい方
- ゼロトラストがどういった効果を発揮するか知りたい方

ゴール

- 今多い脅威や対策を理解する
- 今話題のゼロトラストの効果を理解する

IPA10大脅威について

IPA10大脅威について

- IPA10大脅威とは？

IPA Better Life with IT 情報処理推進機構

- IPA（独立行政法人情報処理推進機構）の毎年発表する、脅威のランキング
- 攻撃を受けるリスクが増えている今、これを見れば具体的に何が危険か分かる

引用元：独立行政法人情報処理推進機構　https://www.ipa.go.jp/index.html

IPA10大脅威について

2022年IPA10大脅威

順位	脅威	前年の順位
１位	ランサムウェアによる被害	１位
２位	標的型攻撃による機密情報の窃取	２位
３位	サプライチェーンの弱点を悪用した攻撃	４位
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	３位
５位	内部不正による情報漏えい	６位
６位	脆弱性対策情報の公開に伴う悪用増加	１０位
７位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
８位	ビジネスメール詐欺による金銭被害	５位
９位	予期せぬIT基盤の障害に伴う業務停止	７位
１０位	不注意による情報漏えい等の被害	９位

- １～４位は前年に引き続き変わらず、注意が必要
- 脆弱性情報の公開に伴う悪用増加が10位⇒6位
- ゼロデイ攻撃が新たにランクイン

引用元：独立行政法人情報処理推進機構　https://www.ipa.go.jp/index.html

ゼロトラストについて

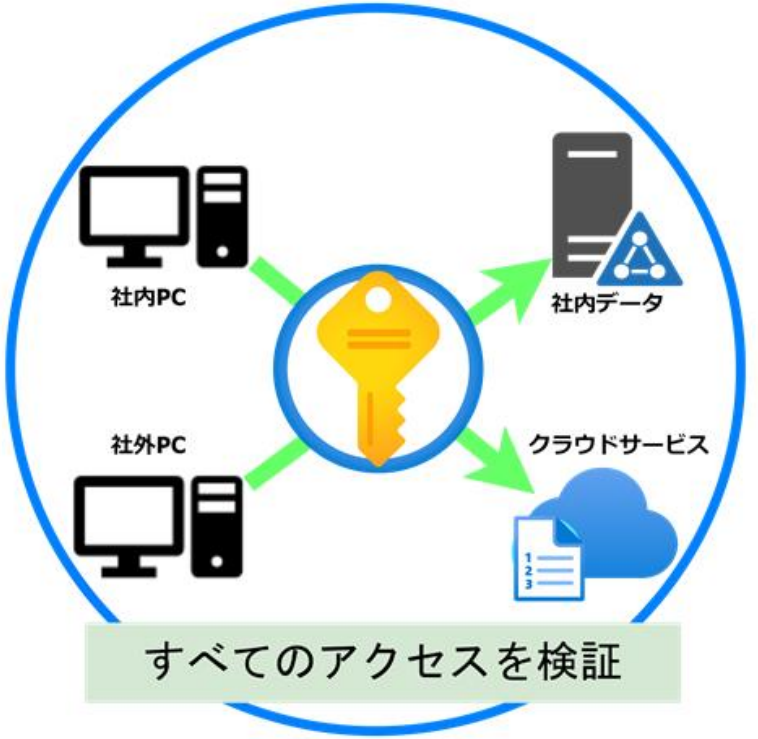
ゼロトラストについて

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。

クラウド・テレワーク等昨今の働き方にマッチ

内部・外部からのアクセスを問わず、すべてを疑い、検証するという考え方が、現在のセキュリティ対策として有効



ゼロトラストについて

ゼロトラストを実現するための７つの要件とソリューション

#	要件	ソリューション例
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)、CSPM（Cloud Security Posture Management)
7	自動化	SOAR (Security Orchestration and Automation Response)

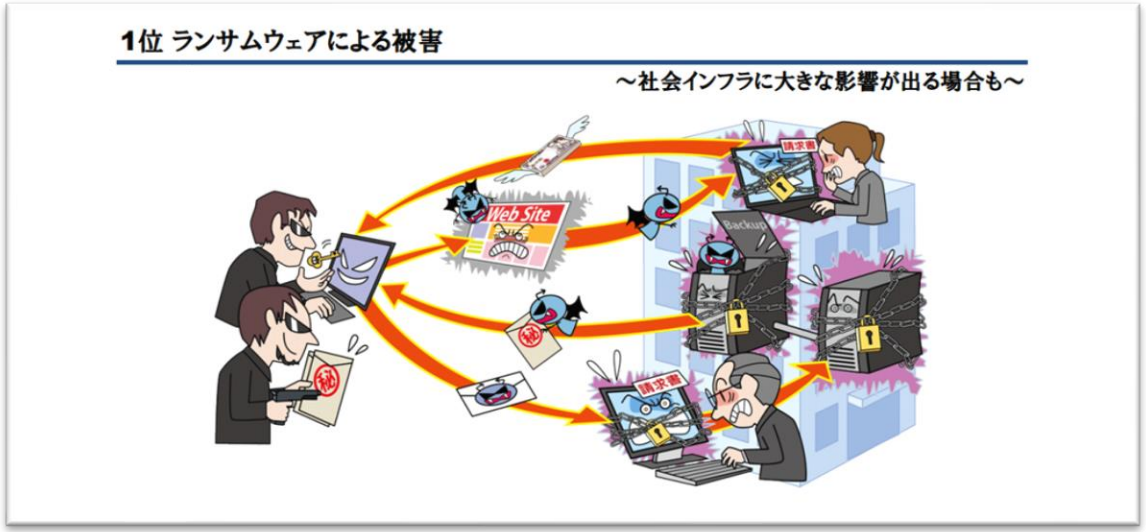
- アメリカの調査会社「Forrester Research」が提唱する７つの要件を重視する必要
- 何か一つ製品を導入すればゼロトラストを実現できるというものではない
- ７つの要件を基に複数の製品・サービスを組み合わせて導入する必要がある

IPA10大脅威解説

IPA10大脅威解説

第１位　ランサムウェアによる被害

マルウェアの一種であり、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）されるケースがあります。



- 感染経路・手口
  - メールからの感染
  - 脆弱性をついた攻撃
  - 不正アクセスによる攻撃…等

引用元：独立行政法人情報処理推進機構「情報セキュリティ10大脅威 2022」解説書 https://www.ipa.go.jp/security/vuln/10threats2022.html

どんな企業が危ない？

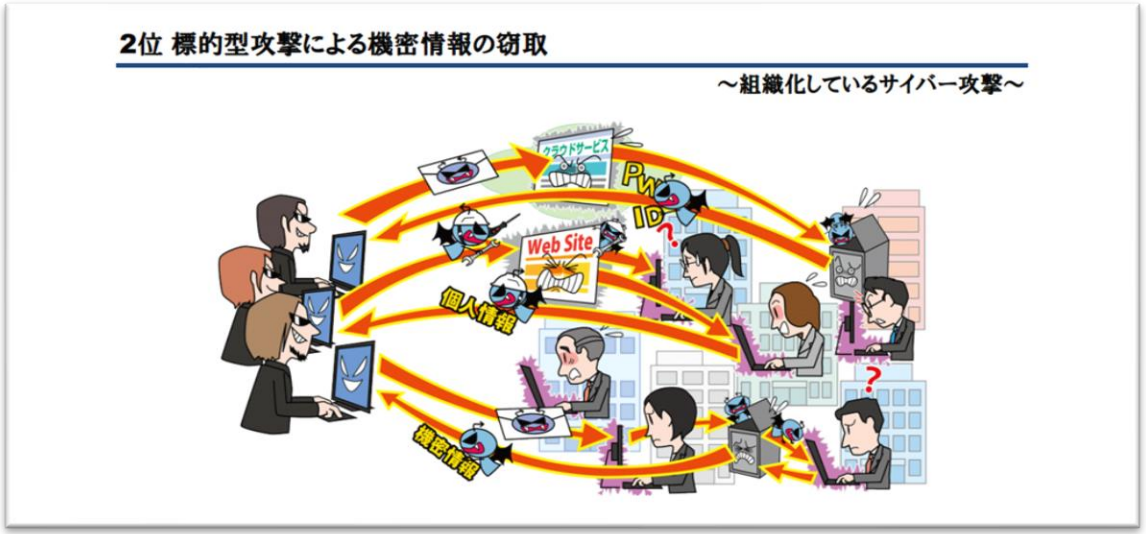
- 適切なID管理や認証の仕組みを導入していない
  退職者やテストID、また認証の弱さを攻撃される可能性 → IDaaSの導入

- フィルタリングツールの導入をしていない
  不審なWEBサイトやクラウドサービスから感染する可能性 → SWG・CSPMの導入

- 一般的なセキュリティソフトしか導入していない
  侵入を未然に防ぐものであり、侵入されると対処ができない → EDRの導入

第２位　標的型攻撃による機密情報の窃取

特定の組織を調査し、狙い撃ちをして不正アクセス等の攻撃をしかけ、情報を搾取する攻撃です。搾取した情報を用いて社内システムに侵入し、PCやサーバーをマルウェアに感染させ機密情報の搾取やシステムの破壊を行います。



- 感染経路・手口
  - 主に1位のランサムウェアと同じ

※特定企業向けに用意されたツールを使用する

引用元：独立行政法人情報処理推進機構「情報セキュリティ10大脅威 2022」解説書 https://www.ipa.go.jp/security/vuln/10threats2022.html

どんな企業が危ない？

- 主に1位のランサムウェアと同じ

標的型攻撃で用いられるマルウェアは巧妙に作られた1点物であり、
攻撃対象のPCのOS標準機能を悪用して侵害を行う傾向があります。

- 使用していないOS機能等を制限していない

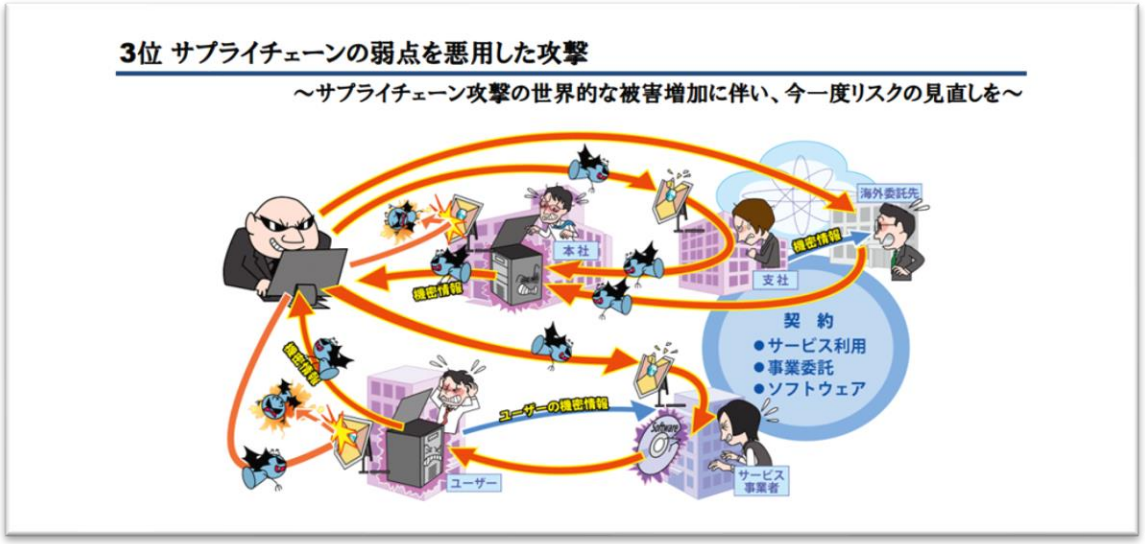
使用していない、見落としがちな機能が狙われる可能性

→ MDMの導入

第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。

例えば、国外にある拠点のサーバーがマルウェア等のウィルスに感染し、そこを経由して国内のサーバーへ侵入され情報を搾取される場合があります。



- 感染経路・手口
  - 標的となる組織の取引先や委託先を攻撃
  - ソフトウェア開発会社の製品にウィルスを仕込む…等

引用元：独立行政法人情報処理推進機構「情報セキュリティ10大脅威 2022」解説書 https://www.ipa.go.jp/security/vuln/10threats2022.html

IPA10大脅威解説

どんな企業が危ない？

- 委託先にプラットフォームを提供していない

情報のやりとりの仕組みを整備しないと攻撃を受けやすい

➡ IDaaS＋αの導入

- 一般的なセキュリティソフトしか導入していない

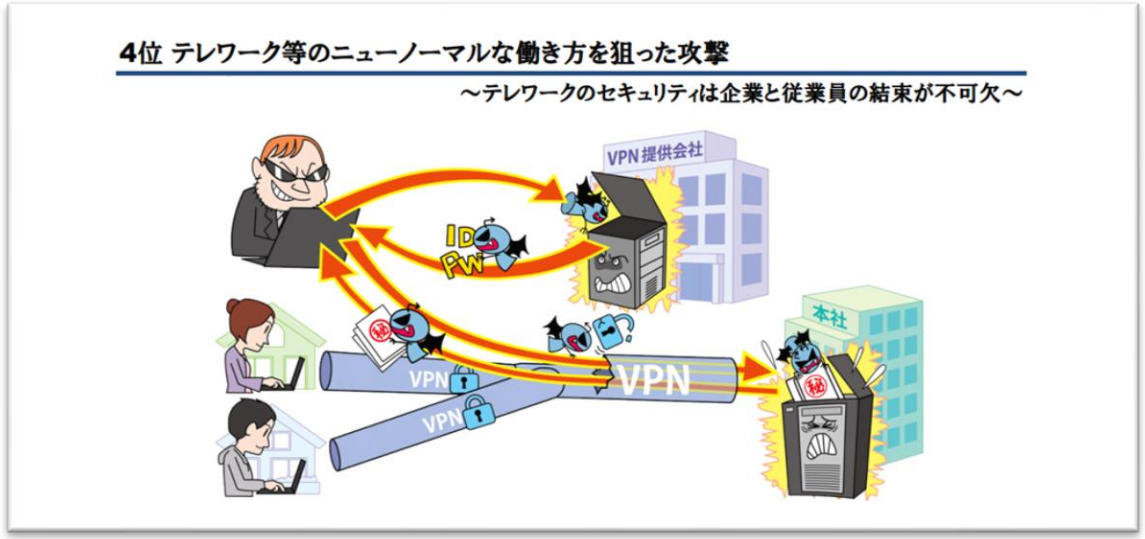
➡ EDRの導入

- その他の対策
  - 業務委託や情報管理における規則の徹底
  - 信頼できる委託先、取引先組織の選定
  - 公的機関が公開している資料の活用

例：IPA「サプライチェーンのセキュリティ脅威に備える」https://www.ipa.go.jp/files/000073868.pdf

第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。社内ネットワークへ侵入する足掛かりにされ、社内へウィルス感染が拡大してしまう場合があります。



- 感染経路・手口
  - VPN製品への攻撃
  - 個人所有デバイスへの攻撃…等

引用元：独立行政法人情報処理推進機構「情報セキュリティ10大脅威 2022」解説書 https://www.ipa.go.jp/security/vuln/10threats2022.html

IPA10大脅威解説

- ＶＰＮ製品への攻撃
  - 脆弱性をついた攻撃
  - 認証の突破
  - テレワーク端末への攻撃

- どんな企業が危ない？
  - 認証の仕組みを整えていない

認証を突破されやすく、攻撃を受けるリスクが増える

→ IDaaSの導入

  - VPN機器のアップデートをしていない

アップデートをしないと、脆弱性の発覚で攻撃の起点になる

→ SDPの導入

  - 一般的なセキュリティソフトしか導入していない

→ EDRの導入

IPA10大脅威解説

- 個人所有ＰＣ・家庭用ネットワークを使用している場合の脅威
  - 個人のWEB利用によるマルウェア感染
  - 家庭用ネットワーク機器等の脆弱性悪用による攻撃

- 対策
  - 社給のデバイス・ネットワーク設備を利用する
  - セキュリティ運用ルールの徹底
  - セキュリティ教育の実施

第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。
組織の社会的信用の喪失や、損害賠償による経済的損失が発生します。

● 感染経路・手口
- 離職前に使用していたアカウントの不正利用
- 外部記憶装置やメールによる情報の持ち出し

引用元：独立行政法人情報処理推進機構「情報セキュリティ10大脅威 2022」解説書 https://www.ipa.go.jp/security/vuln/10threats2022.html

どんな企業が危ない？

- ID管理が適切に行われていない

退職者やテストIDが残るとセキュリティリスクになる

→ IDaaSの導入

- 外部記憶装置の利用制限がされていない

情報の持ち出しをされてしまうリスクがある

→ MDMの導入

- データを守る製品を導入していない

誰でもデータを持ち出しが出来てしまうと漏洩リスクになる

→ DLPの導入

第６位　脆弱性対策情報の公開に伴う悪用増加

脆弱性対策のために公開された情報を悪用し、攻撃を仕掛けられる脅威です。
近年、脆弱性情報の公開後、攻撃が本格化するまでの時間が短くなっています。

●感染経路・手口

- 対策する前の脆弱性をついた攻撃

引用元：独立行政法人情報処理推進機構「情報セキュリティ10大脅威 2022」解説書 https://www.ipa.go.jp/security/vuln/10threats2022.html

どんな企業が危ない？

- 一般的なセキュリティソフトしか導入していない
  侵入を未然に防ぐものであり、侵入されると対処ができない
  → EDRの導入

- 脆弱性対策運用をしていない
  脆弱性を放置するとセキュリティホールになる
  → 脆弱性対策運用の実施

- 使用していないOS機能等を制限していない
  使用していない、見落としがちな機能が狙われる可能性
  → MDMの導入

第７位　修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

OSやソフトウェア等のセキュリティホールが発見されてから、その情報やパッチが出る前に攻撃を仕掛ける脅威です。パッチ等の対策公開（1日目）よりも前の攻撃（0日）なのでゼロデイ攻撃と呼ばれています。

- 感染経路・手口
  - 6位とほぼ同様

※情報公開前、対策パッチやウィルスパターン定義ファイル更新前に攻撃を仕掛けるという、さらに素早く対策が難しい脅威

引用元：独立行政法人情報処理推進機構「情報セキュリティ10大脅威 2022」解説書 https://www.ipa.go.jp/security/vuln/10threats2022.html

どんな企業が危ない？

- 一般的なセキュリティソフトしか導入していない
  侵入を未然に防ぐものであり、侵入されると対処ができない
  → EDRの導入

- 脆弱性対策運用をしていない
  脆弱性を放置するとセキュリティホールになる
  → 脆弱性対策運用の実施

- 使用していないOS機能等を制限していない
  使用していない、見落としがちな機能が狙われる可能性
  → MDMの導入

脅威の対策ソリューションまとめ

脅威の対策ソリューションまとめ

順位	脅威	対応ソリューション例
1位	ランサムウェアによる被害	EDR、CSPM、SWG、IDaaSなど
2位	標的型攻撃による機密情報の窃取	EDR、SWGなど
3位	サプライチェーンの弱点を悪用した攻撃	EDR、IDaaSなど
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	EDR、IDaaS、SDPなど
5位	内部不正による情報漏えい	IDaaS、MDM、DLPなど
6位	脆弱性対策情報の公開に伴う悪用増加	EDR、MDMなど
7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	EDR、MDMなど
8位	ビジネスメール詐欺による金銭被害	IDaaSなど
9位	予期せぬIT基盤の障害に伴う業務停止	ー
10位	不注意による情報漏えい等の被害	MDM、DLPなど

- IDaaSとEDRの対応範囲が広いが、それだけで脅威をカバーはできない
- 紹介したもの以外にも有効なゼロトラストソリューションは存在する

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

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

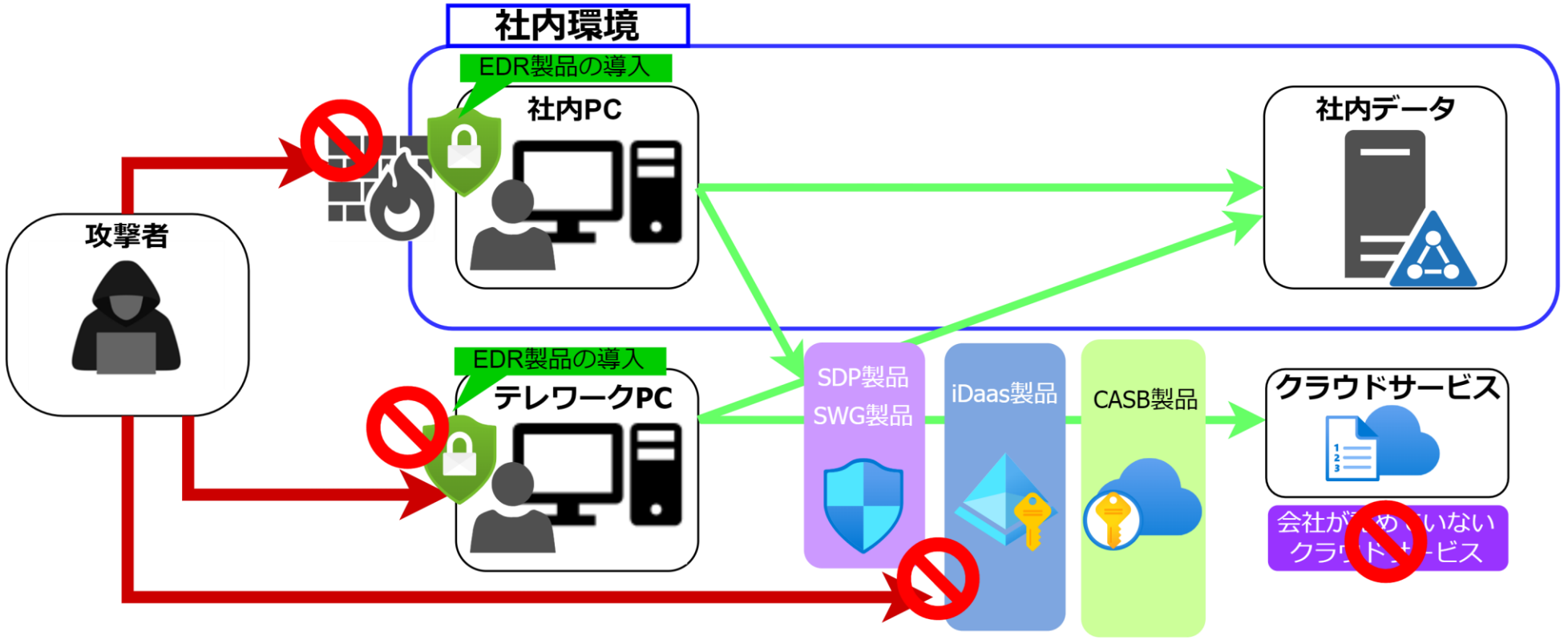
7つの要件を大別して以下の3つのソリューション群に分けられると考えます。

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

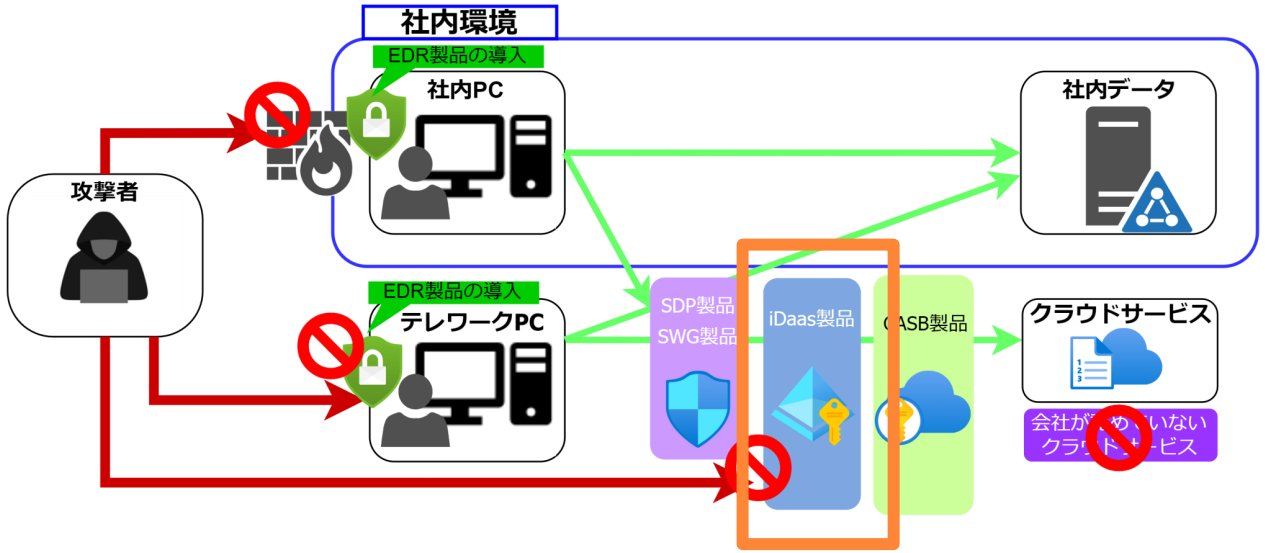
- スタイルズの考える導入の例



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

順位	脅威	対応ソリューション例
1位	ランサムウェアによる被害	EDR、CSPM、SWG、IDaaSなど
2位	標的型攻撃による機密情報の窃取	EDR、SWGなど
3位	サプライチェーンの弱点を悪用した攻撃	EDR、IDaaSなど
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	EDR、IDaaS、SDPなど
5位	内部不正による情報漏えい	IDaaS、MDM、DLPなど
6位	脆弱性対策情報の公開に伴う悪用増加	EDR、MDMなど
7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	EDR、MDMなど
8位	ビジネスメール詐欺による金銭被害	IDaaSなど
9位	予期せぬIT基盤の障害に伴う業務停止	ー
10位	不注意による情報漏えい等の被害	MDM、DLPなど



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。

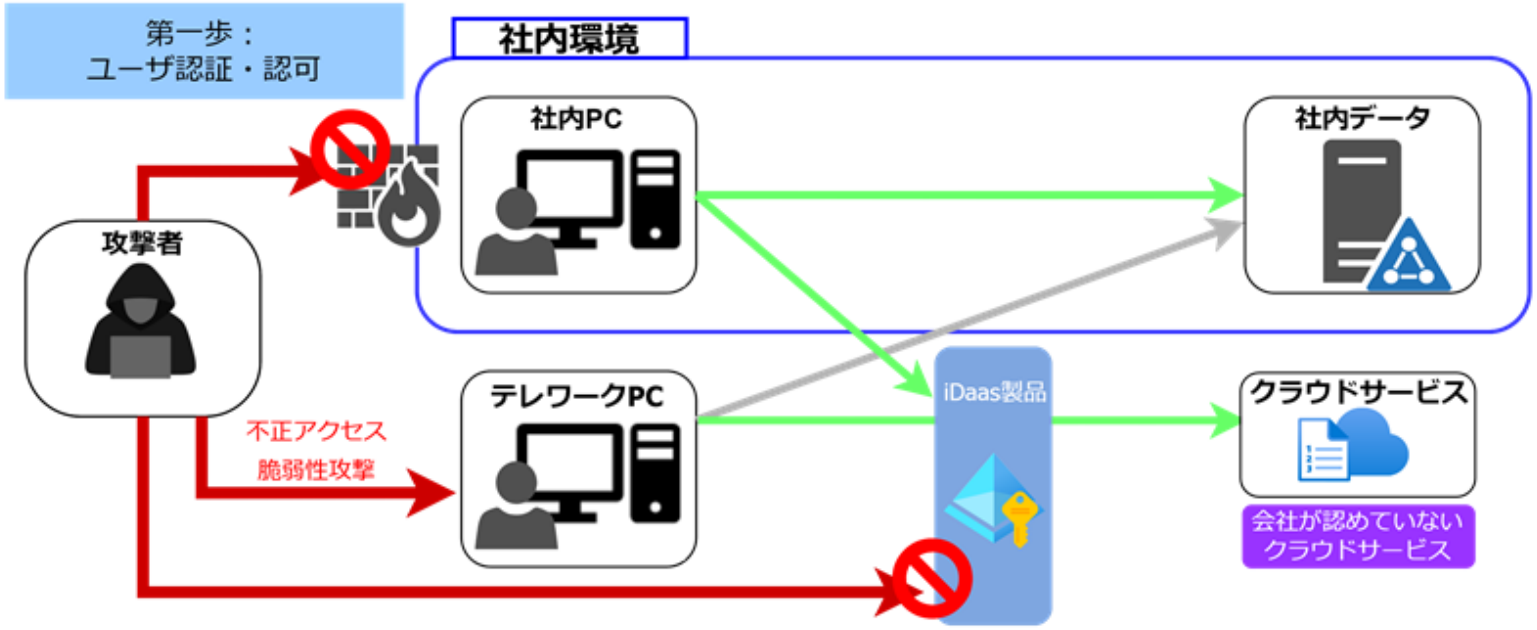
主な機能

- 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

なぜ最初に導入するべきなのか、メリット

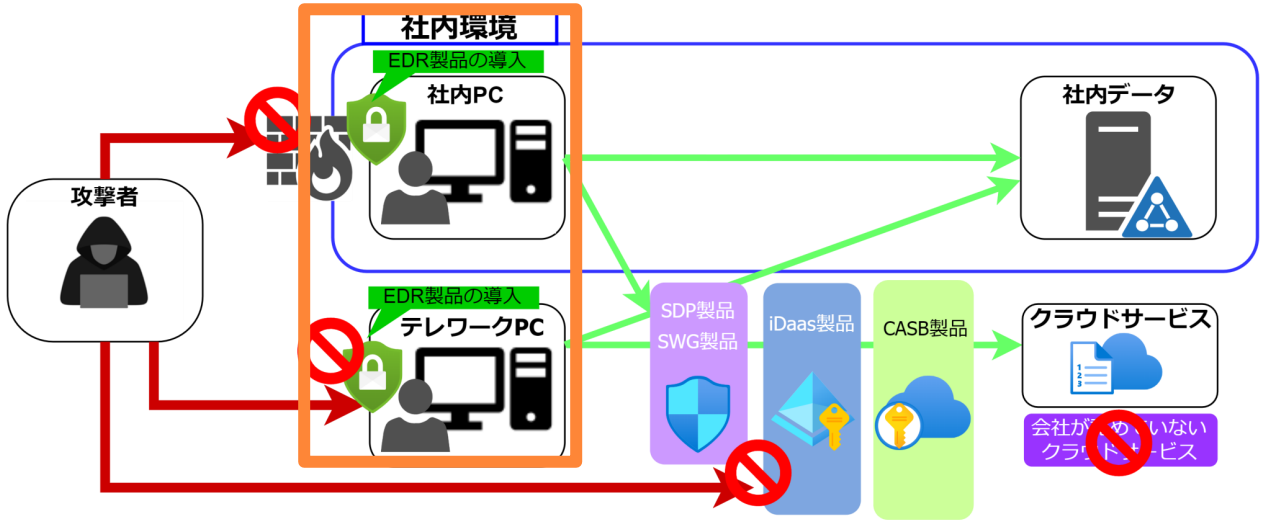


- 多要素認証によりクラウドサービス利用のセキュリティ向上
- 認可機能でユーザごとの役割を決め、社内不正を防止する
- シングルサインオンやID管理による利便性向上
- 適切なID管理はゼロトラストの基盤

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

順位	脅威	対応ソリューション例
1位	ランサムウェアによる被害	EDR、CSPM、SWG、IDaaSなど
2位	標的型攻撃による機密情報の窃取	EDR、SWGなど
3位	サプライチェーンの弱点を悪用した攻撃	EDR、IDaaSなど
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	EDR、IDaaS、SDPなど
5位	内部不正による情報漏えい	IDaaS、MDM、DLPなど
6位	脆弱性対策情報の公開に伴う悪用増加	EDR、MDMなど
7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	EDR、MDMなど
8位	ビジネスメール詐欺による金銭被害	IDaaSなど
9位	予期せぬIT基盤の障害に伴う業務停止	ー
10位	不注意による情報漏えい等の被害	MDM、DLPなど



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？

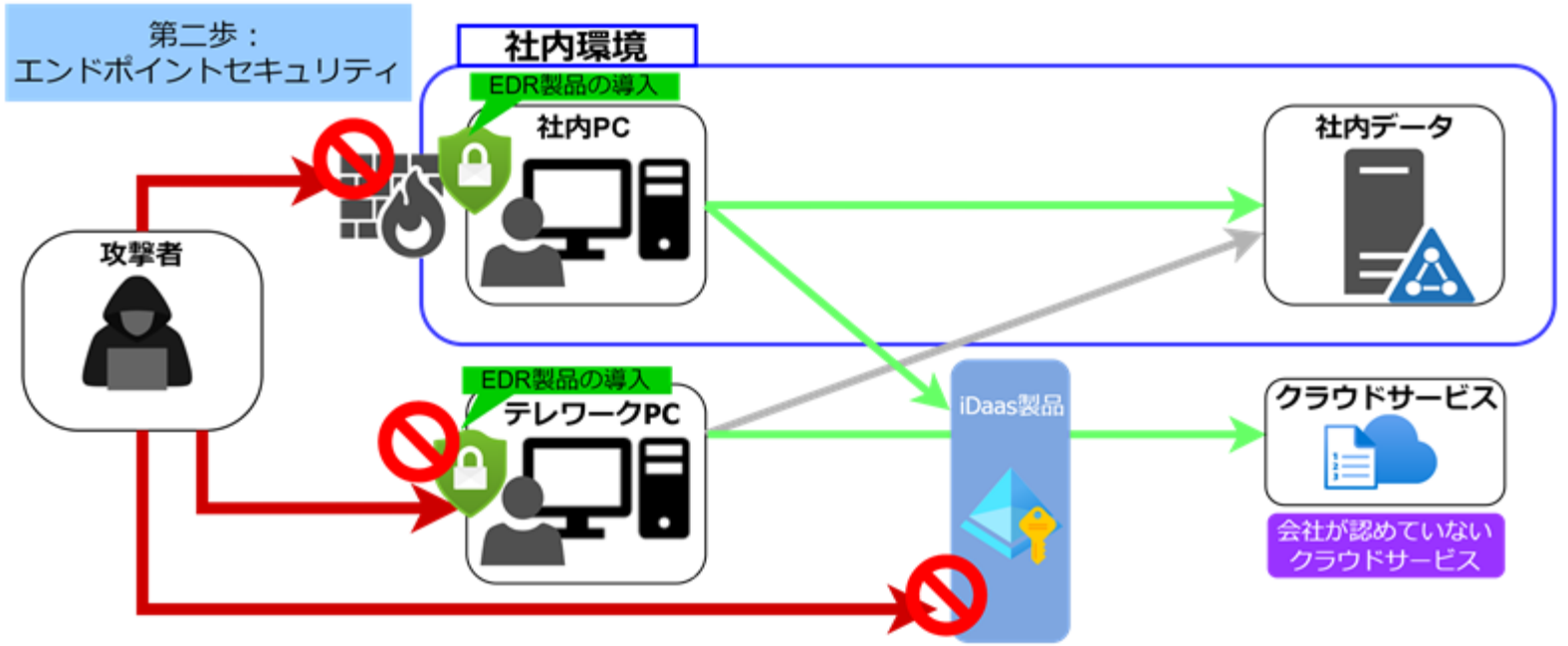
デバイスの保護といえばアンチウイルスソフト（セキュリティソフト）を思い浮かべると思います。EDRとアンチウイルスソフトの違いは以下です。

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

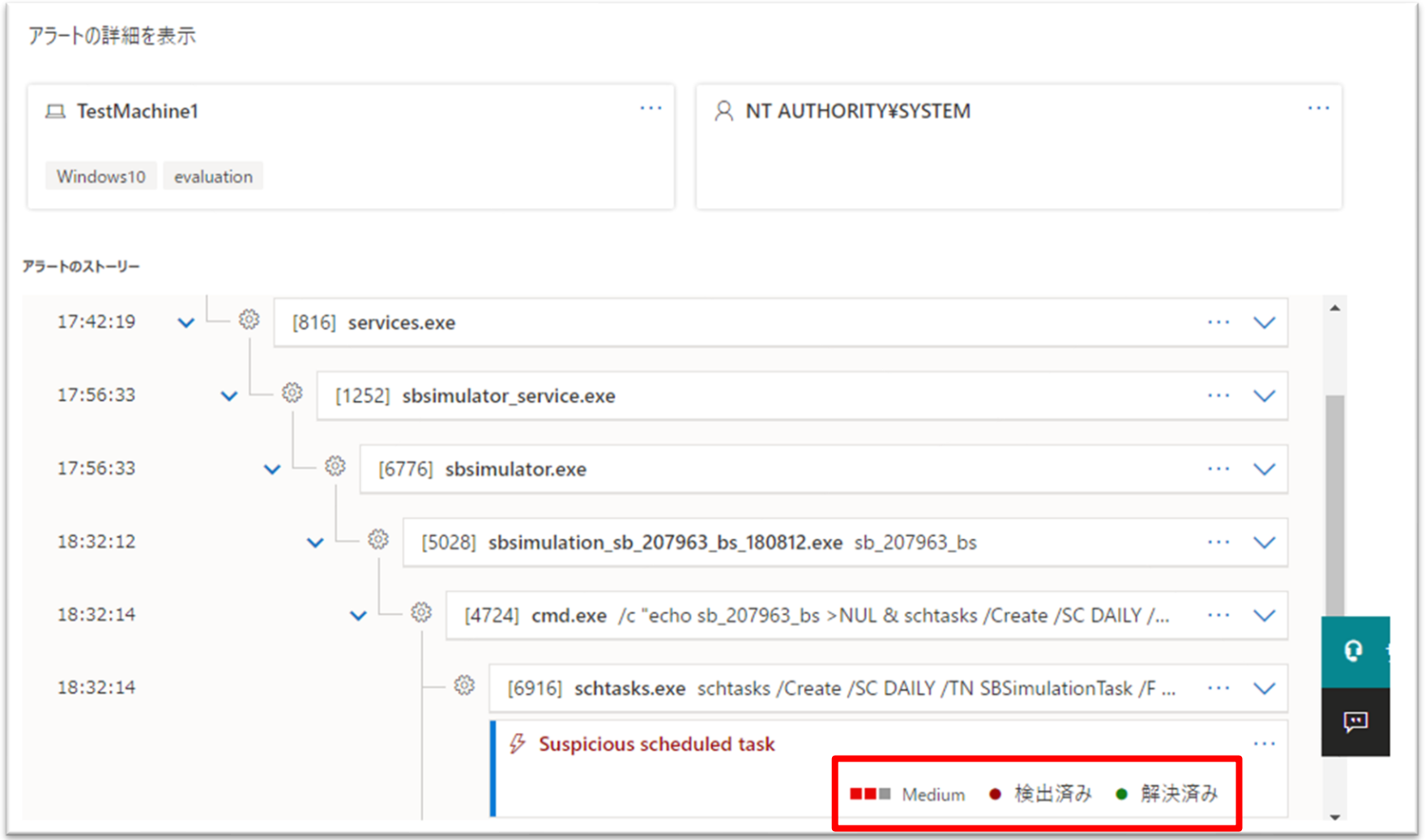
なぜ導入するべきなのか・メリット



- 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二歩：エンドポイントセキュリティ

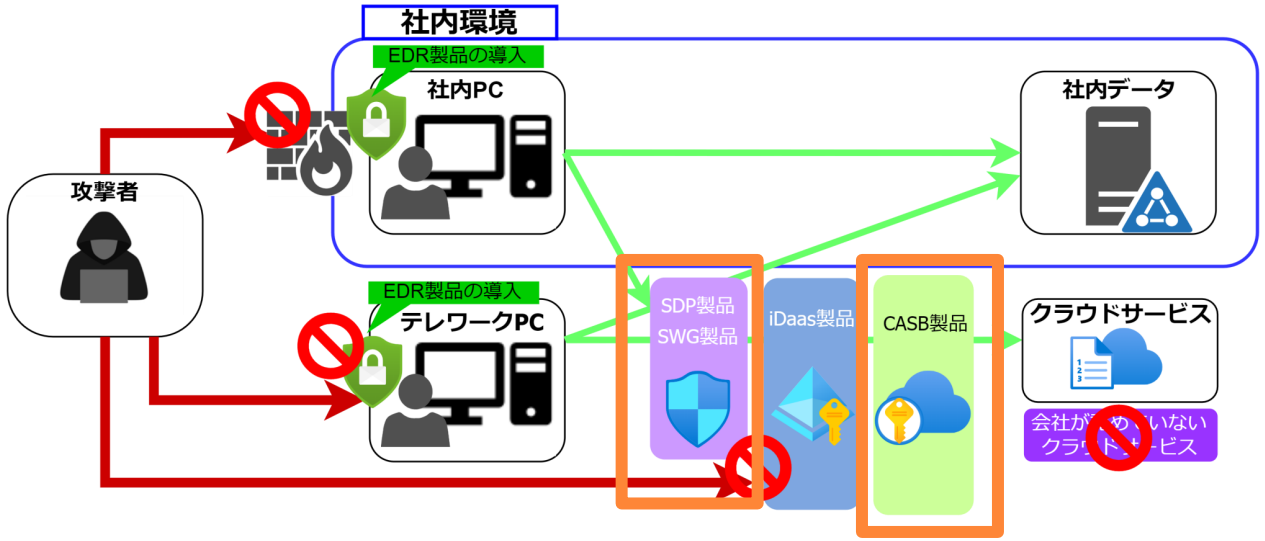
検知例



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二歩：エンドポイントセキュリティ

順位	脅威	対応ソリューション例
1位	ランサムウェアによる被害	EDR、CSPM、SWG、IDaaSなど
2位	標的型攻撃による機密情報の窃取	EDR、SWGなど
3位	サプライチェーンの弱点を悪用した攻撃	EDR、IDaaSなど
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	EDR、IDaaS、SDPなど
5位	内部不正による情報漏えい	IDaaS、MDM、DLPなど
6位	脆弱性対策情報の公開に伴う悪用増加	EDR、MDMなど
7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	EDR、MDMなど
8位	ビジネスメール詐欺による金銭被害	IDaaSなど
9位	予期せぬIT基盤の障害に伴う業務停止	ー
10位	不注意による情報漏えい等の被害	MDM、DLPなど



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。

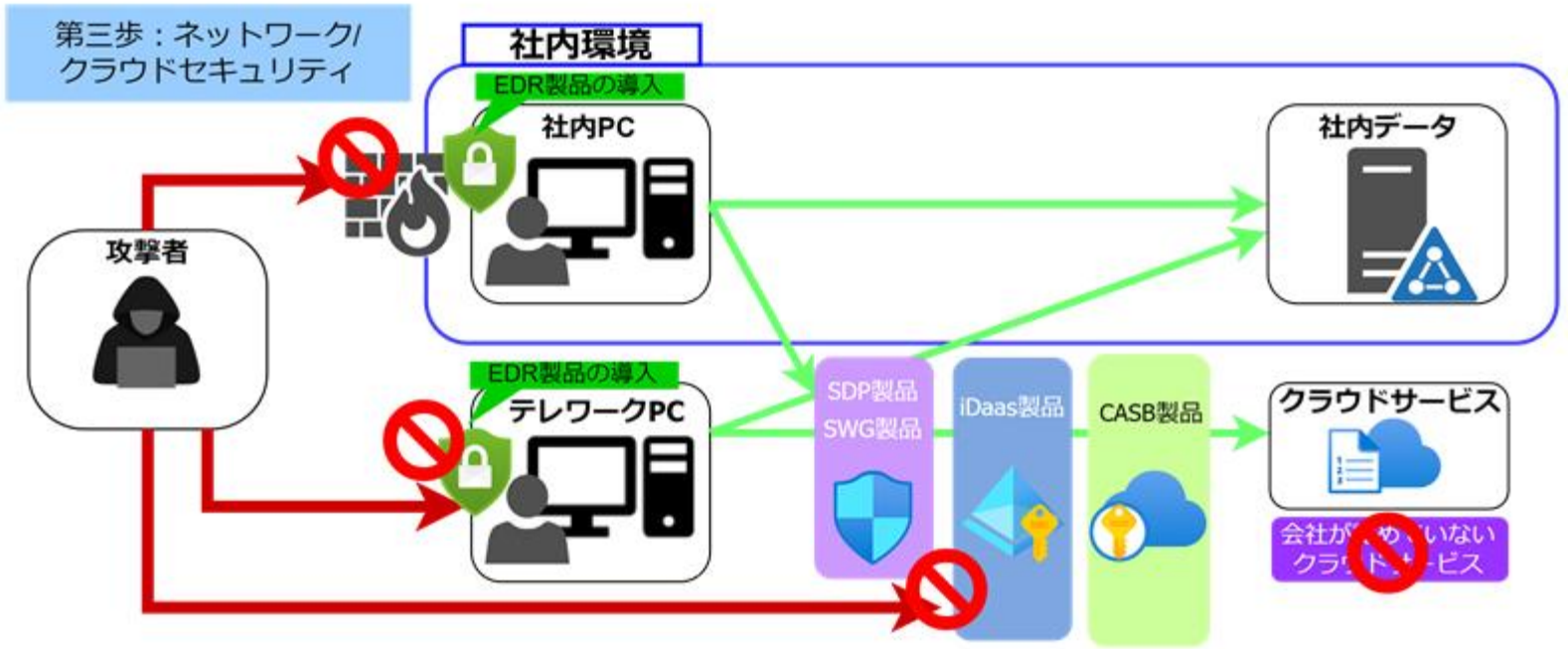
危険なサイトなどへのアクセスを遮断するSWG（Secure Web Gateway）、リアルタイムに接続可否を判断するSDP（Software Defined Perimeter）などがあります。

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

ゼロトラストでの重要な対策

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）

ゼロトラストでの重要な対策

- 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。

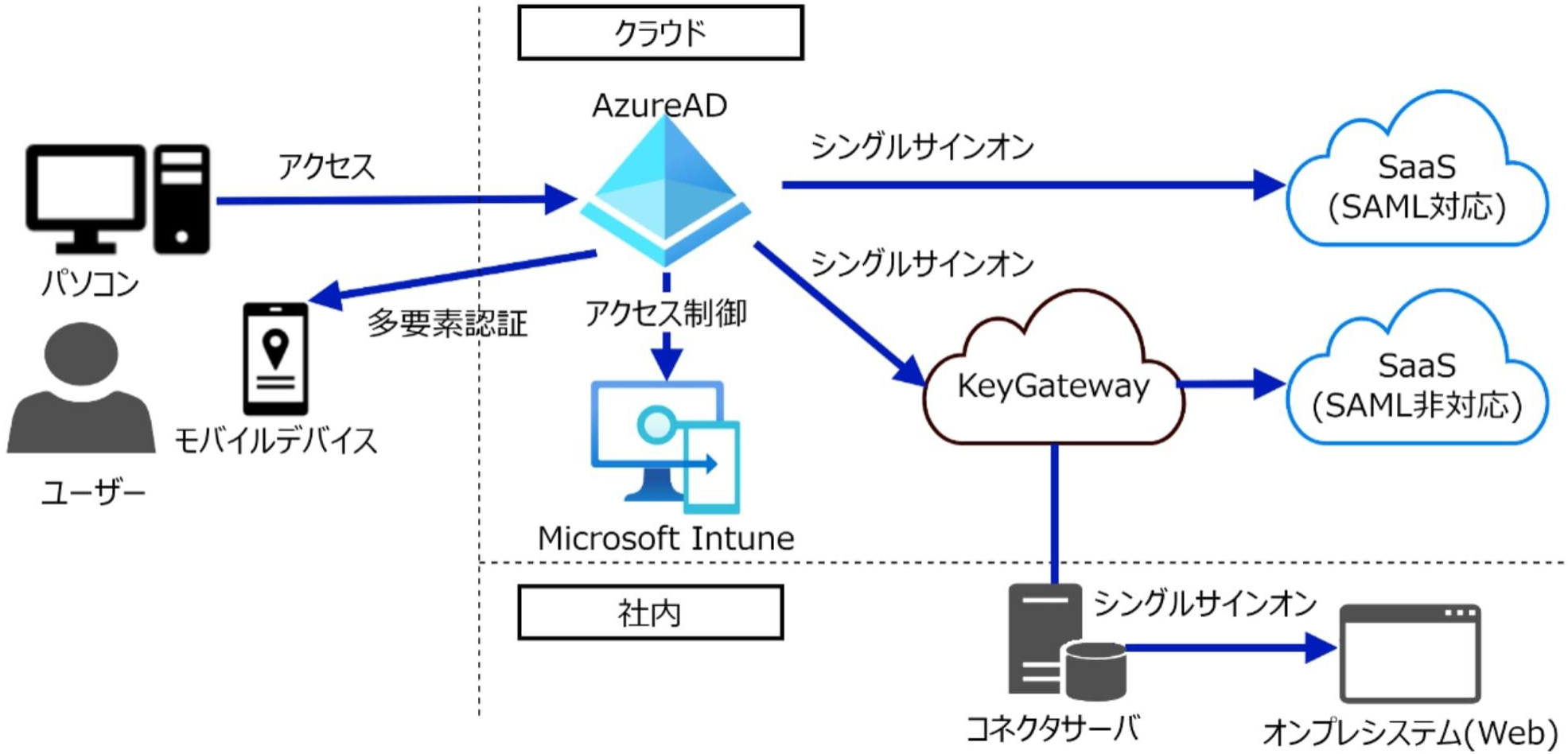
AzureADでもシングルサインオンに対応しているシステム数が数千に対して、IDプロビジョニングの対応数は約250となります。（2021年12月現在）クラウドサービスが普及して数が増していく中、IDプロビジョニングによる作業負荷軽減を求める方も多いと思います。

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。

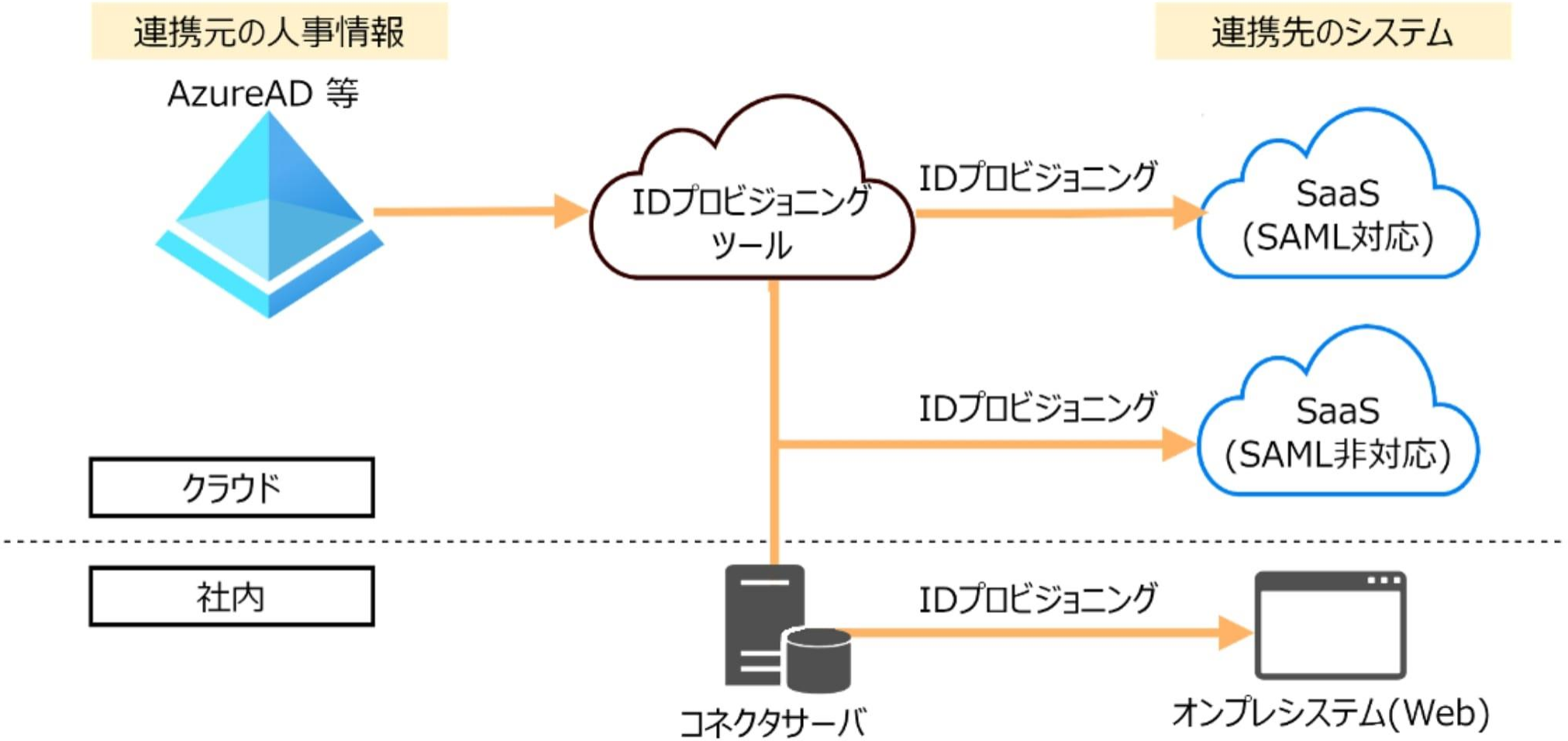
スタイルズのIDaaSサービスの構成例

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

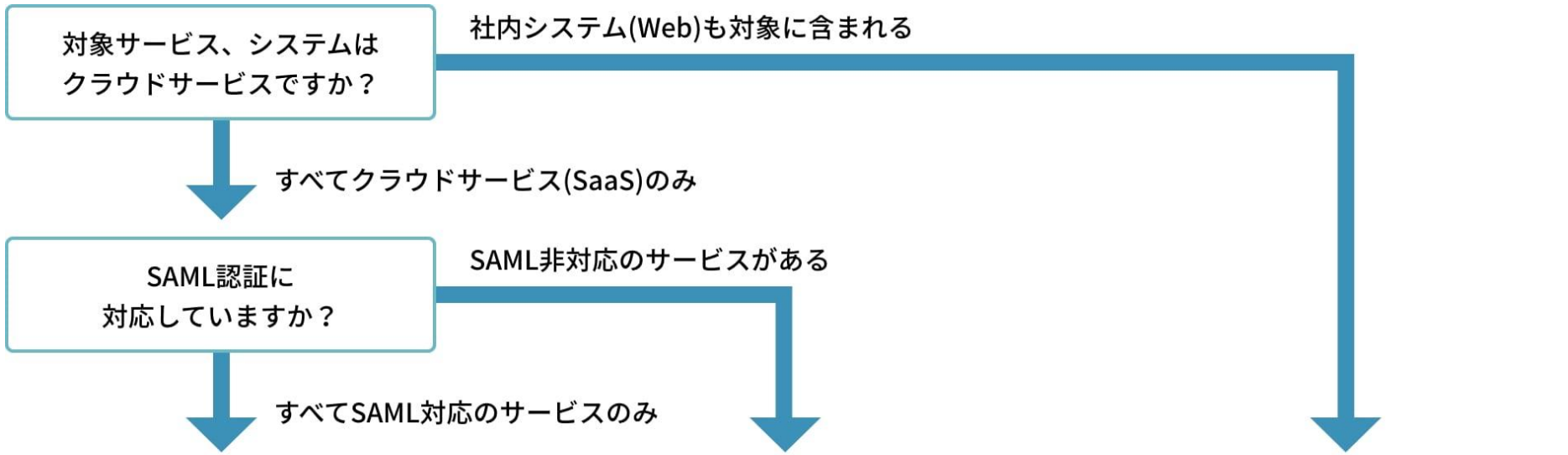
IDプロビジョニング構成



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