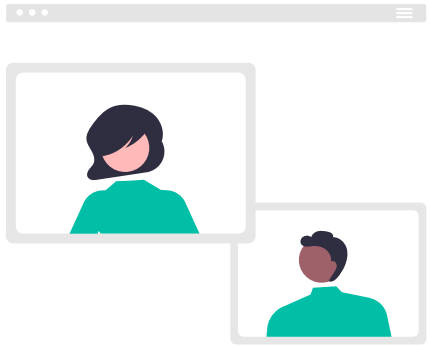
ゼロトラストセキュリティ

ニューノーマル時代に対応するゼロトラスト実現へのアプローチ

なぜゼロトラストセキュリティが必要なのか

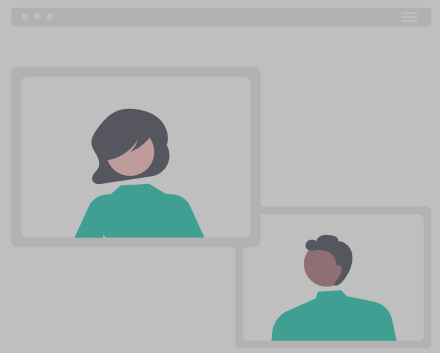
- 働き方改革、BCP対策など、企業価値を高めるために、場所を問わない働き方の導入が必要
  - **多様なアクセス方法への対応↔セキュリティリスク**のトレードオフ
- サイバー攻撃の高度化&セキュリティインシデントに対する企業価値への影響は大きくなっている
  - 従来のセキュリティ基準では防ぐことができない攻撃
  - セキュリティインシデントに対して企業が被る損害は増加

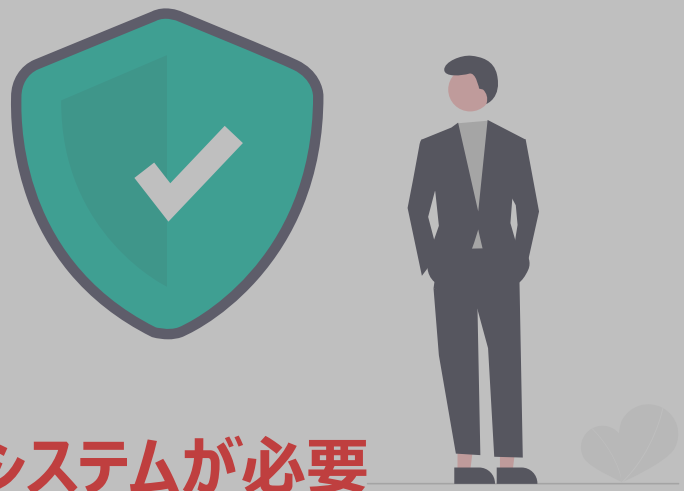


社内ネットワーク(境界型防御)に頼らないセキュリティシステムが必要

なぜゼロトラストセキュリティが必要なのか

- 働き方改革、BCP対策など、企業価値を高めるために、場所を問わない働き方の導入が必要
  - **多様なアクセス方法への対応↔セキュリティリスク**のトレードオフ
- サイバー攻撃の高度化&セキュリティインシデントに対する企業価値への影響は大きくなっている
  - 従来のセキュリティ基準では防ぐことができない攻撃
  - セキュリティインシデントに対して企業が被る損害は増加

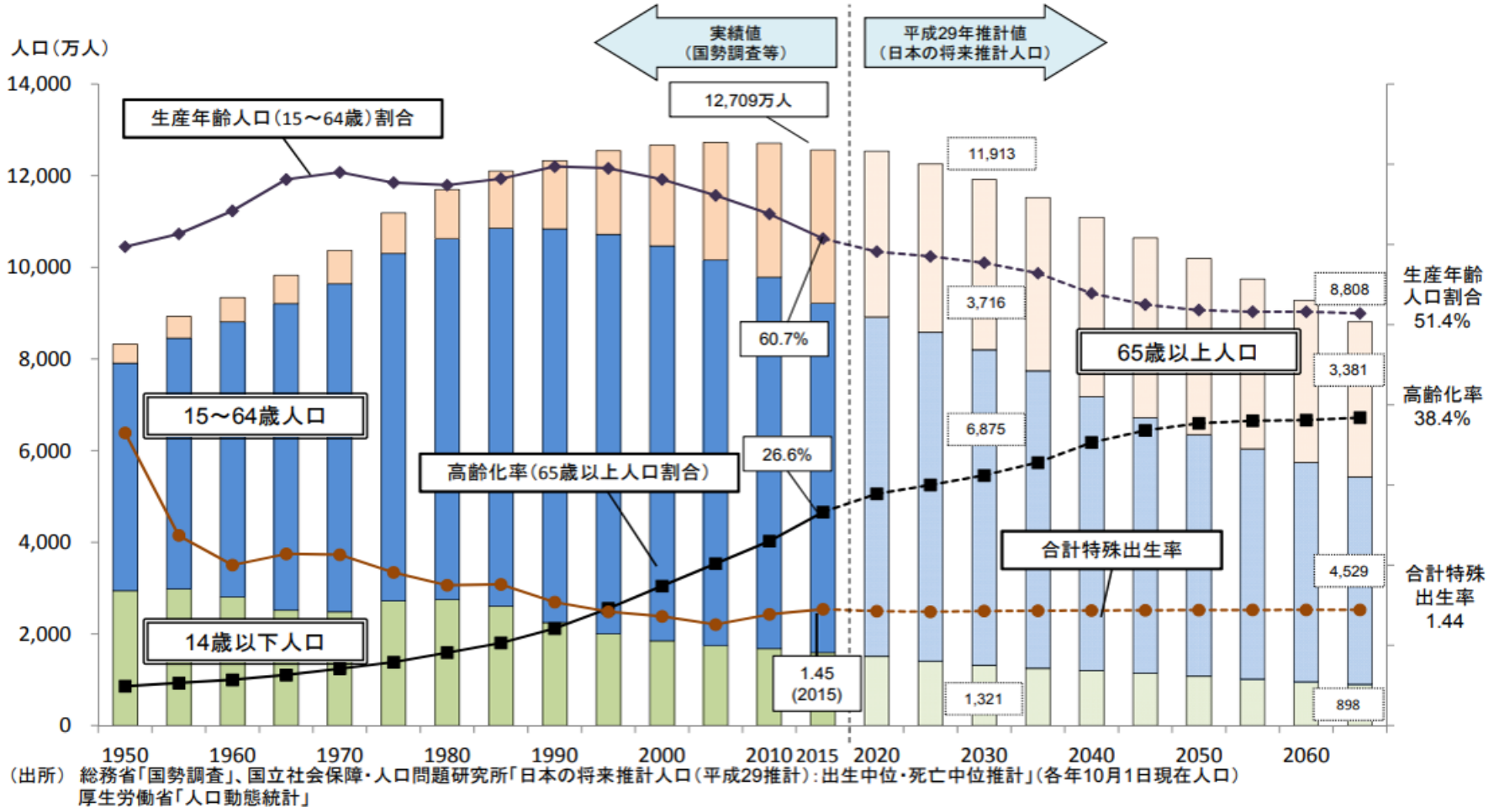




社内ネットワーク(境界型防御)に頼らないセキュリティシステムが必要

日本の人口の推移

- 2065年には総人口が9,000万人を割り込み、高齢化率は38%台の水準になると推計されている。



（出所） 総務省「国勢調査」、国立社会保障・人口問題研究所「日本の将来推計人口（平成29推計）：出生中位・死亡中位推計」（各年10月1日現在人口）
厚生労働省「人口動態統計」

企業における働き方改革の必要性

- 働き方改革を構成する3つの柱
  - 長時間労働の是正
  - 正規、非正規の格差解消
  - 多様な働き方の実現

企業における働き方改革の必要性

- 働き方改革を構成する3つの柱
  - 長時間労働の是正
  - 正規、非正規の格差解消
  - **多様な働き方の実現**

多様な働き方の実現

- 優秀な人材の確保や育児・介護などとの両立が可能
- テレワークの導入効果

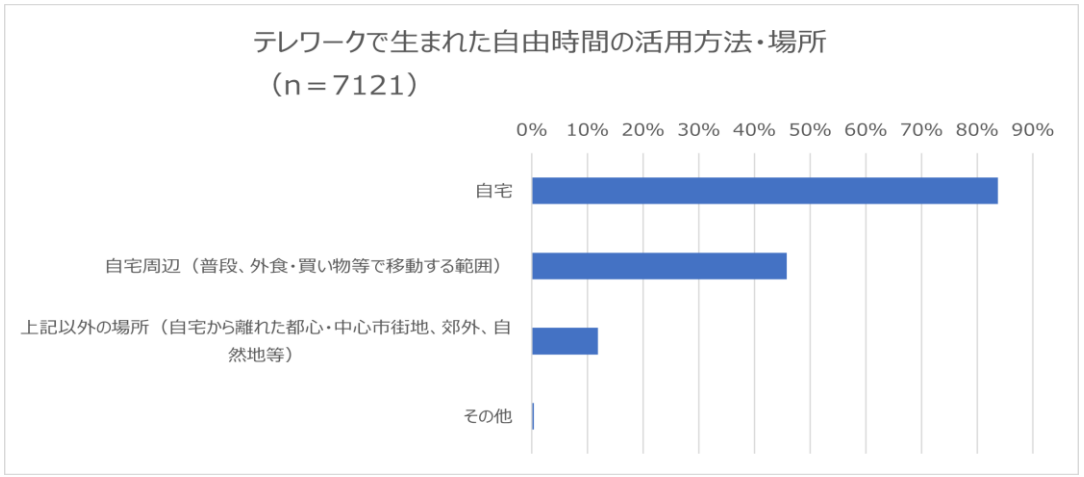
業務生産性の向上

新規雇用・離職防止

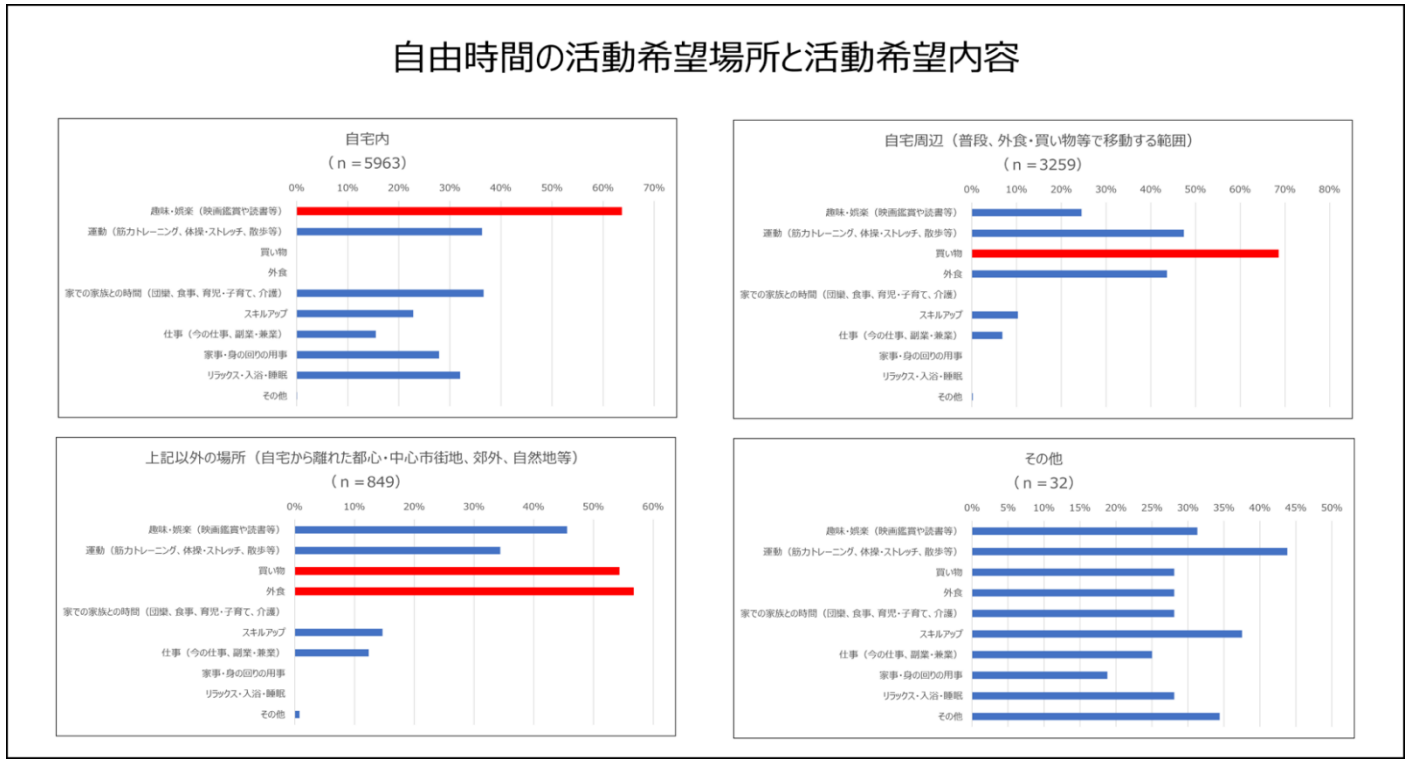
社員のワーク・ライフ・バランス向上

コスト削減

事業継続性の確保

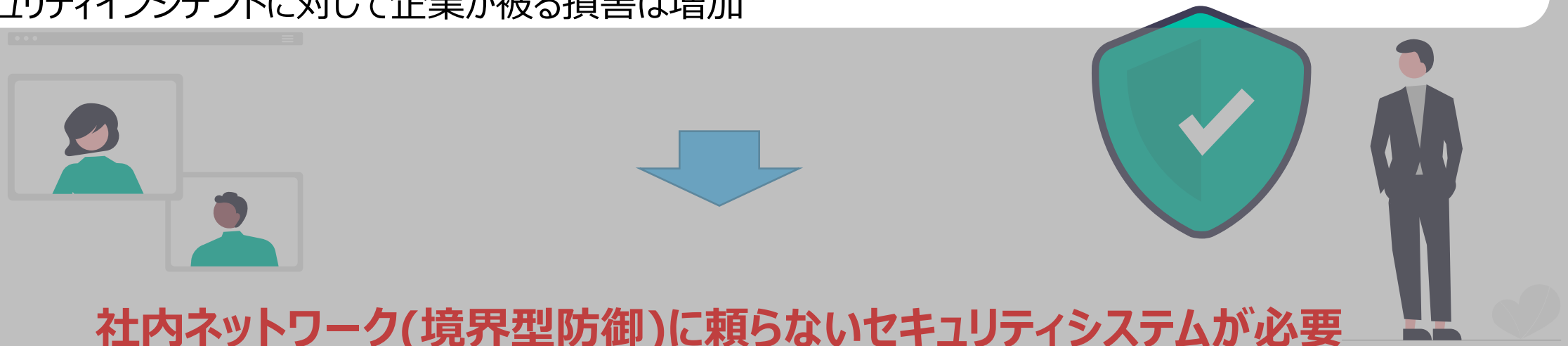


出典:テレワーク総合ポータルサイト[厚生労働省・総務省]https://telework.mhlw.go.jp/telework/effect/



なぜゼロトラストセキュリティが必要なのか

- 働き方改革、BCP対策など、企業価値を高めるために、場所を問わない働き方の導入が必要
  - **多様なアクセス方法への対応↔セキュリティリスク**のトレードオフ
- サイバー攻撃の高度化&セキュリティインシデントに対する企業価値への影響は大きくなっている
  - 従来のセキュリティ基準では防ぐことができない攻撃
  - セキュリティインシデントに対して企業が被る損害は増加



社内ネットワーク(境界型防御)に頼らないセキュリティシステムが必要

省庁からのセキュリティ要件向上の要請

- サイバーセキュリティ経営ガイドライン(経済産業省・IPA)
  - サイバーセキュリティは経営問題
    1. 経営者は、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要
    2. 自社は勿論のこと、ビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策が必要
    3. 平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開示など、関係者との適切なコミュニケーションが必要

経済産業省 独立行政法人 情報処理推進機構
サイバーセキュリティ経営ガイドライン https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide2.0.pdf

企業規模に関わらず対策は必要

- 情報セキュリティ10大脅威(IPA)
  - サプライチェーンの弱点を悪用した攻撃(2021年4位→2022年3位)
- セキュリティ対策は自社だけの問題ではない

MITSUBISHI ELECTRIC
Changes for the Better

NEWS RELEASE

（経営 No.2108）

2021 年 3 月 26 日
三菱電機株式会社

不正アクセスによる情報流出について（調査結果）

三菱電機株式会社は、2020 年 11 月 20 日に公表した第三者による不正アクセス事案※ について、行っていた調査を終えましたので以下にお知らせします。

調査の過程で新たに当社子会社の国内お取引先の金融機関口座（子会社の支払先口座）に関する情報および同子会社の国内お取引先の連絡先に関する個人情報の流出と、当社の国内お取引先の一部に関する情報が流出したことが判明しました。

セキュリティー体制の強化に取り組む中、対象となるお取引先に多大なるご迷惑とご心配をおかけしたこと、また、調査に時間を要したことを深くお詫び申し上げます。

なお、新たな攻撃につながる可能性があるため、攻撃と対策の詳細は差し控えますが、情報セキュリティーに関する関係機関および当社が契約している当該クラウドサービス事業者へ情報を提供しております。

当社は、引き続き、セキュリティー対策のさらなる強化に努めてまいります。

※「不正アクセスによる情報流出について」 https://www.MitsubishiElectric.co.jp/news/2020/1120.pdf

三菱電機子会社へ不正アクセス、情報流出
(三菱電機) https://www.mitsubishielectric.co.jp/news/2021/0326.pdf

2022 年 3 月 31 日

小島プレス工業株式会社　システム停止事案調査報告書（第 1 報）

小島プレス工業株式会社（以下、「当社」といいます。）は、3 月 1 日付け「ウィルス感染被害によるシステム停止事案発生のお知らせ」にてシステム障害発生等について公表したとおり、当社ファイルサーバが第三者による不正アクセスを受けた（以下、「本件」といいます。）ことを確認し、さらなる攻撃予防のため取引先様及び外部とのネットワークを遮断しました。

当社は、ネットワーク遮断後、緊急対策本部を立ち上げ、侵害調査と緊急対策のために、外部のセキュリティ専門家を起用し、本件被害の全容解明と復旧、さらには再発防止に向けて総力を挙げて取り組んでいるところです。

お客様、取引先様をはじめとする関係者の皆様には、多大なるご迷惑とご心配をおかけしておりますことを深くお詫び申し上げます。

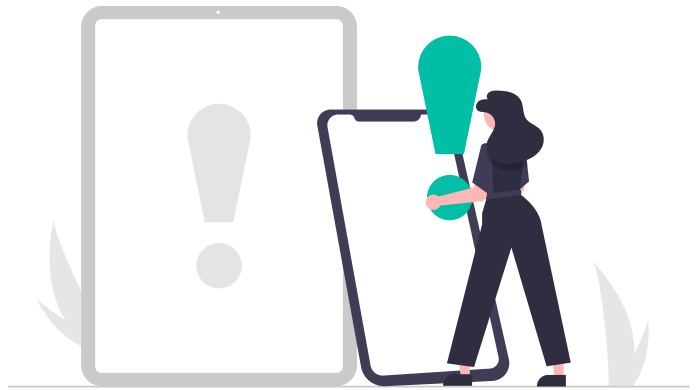
トヨタ自動車の取引先にサイバー攻撃、全工場停止
(小島プレス工業株式会社)
https://www.kojima-tns.co.jp/wp-content/uploads/2022/03/20220331_システム障害調査報告書（第1報）.pdf

インシデント発生時の被害の例

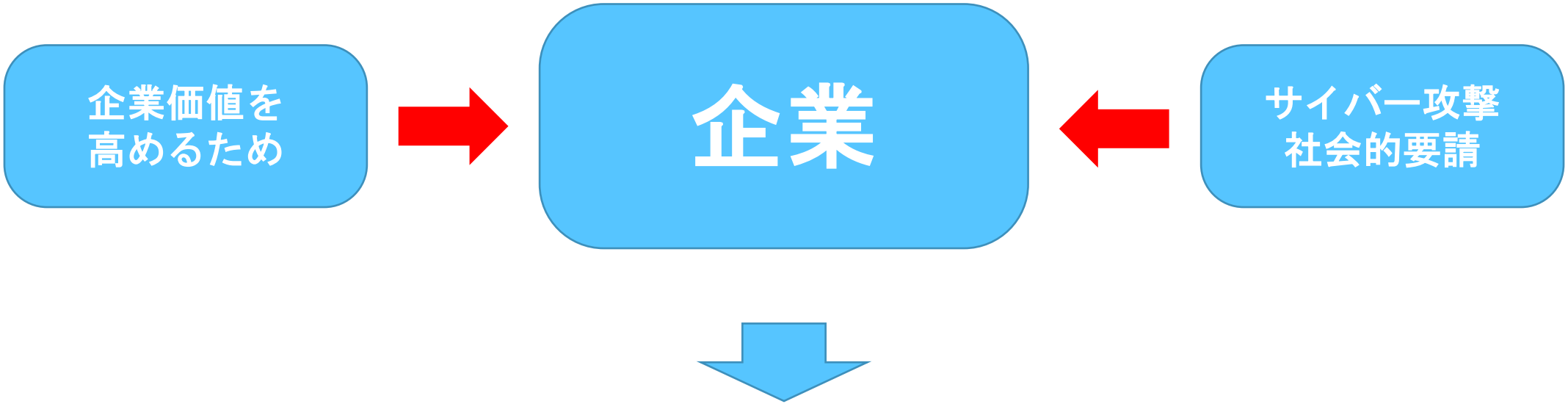
- インシデント損害額調査レポート　2021年版(JNSA)
  - インシデント発生時において生じる損害

費用損害　賠償損害　利益損害　金銭損害　行政損害　無形損害

- モデルケース
  - 軽微なマルウェア感染　600万円
  - ECサイトからのクレジットカード情報等の漏洩　9,490万円
  - 大規模なマルウェア感染　3億7,600万円



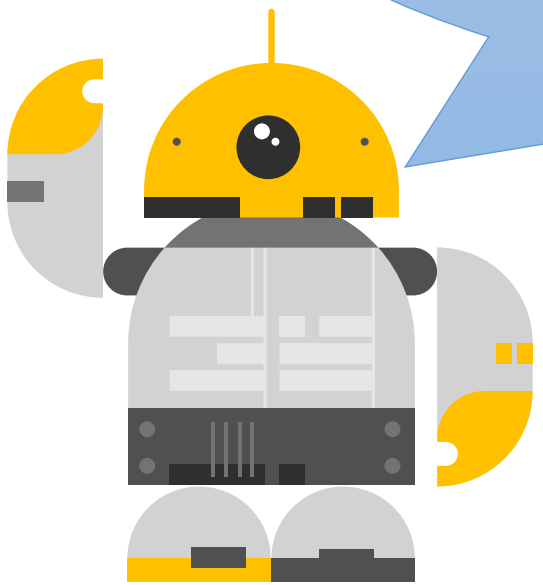
なぜゼロトラストセキュリティが必要なのか



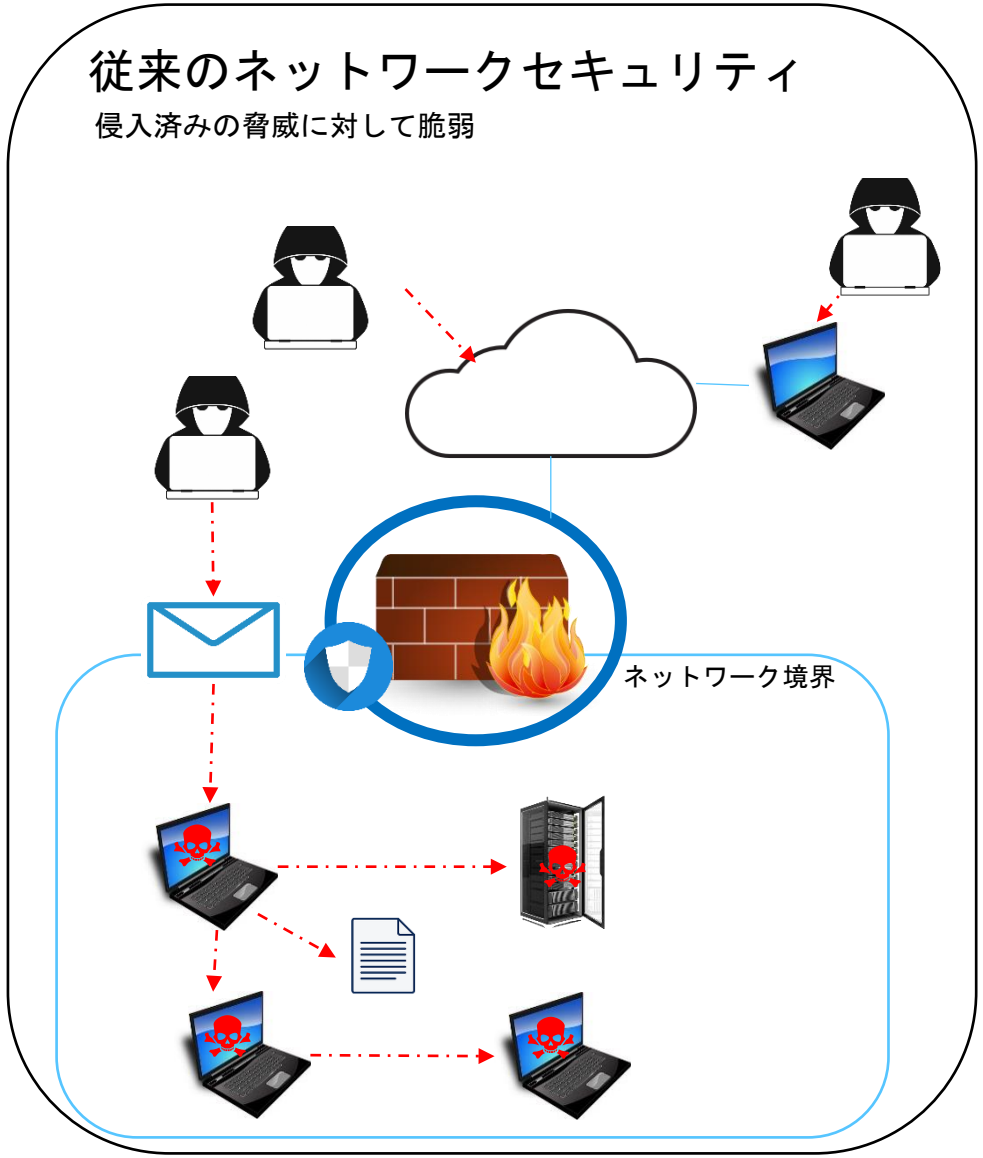
従来の境界型防御での対応に限界
新たなセキュリティシステムが必要

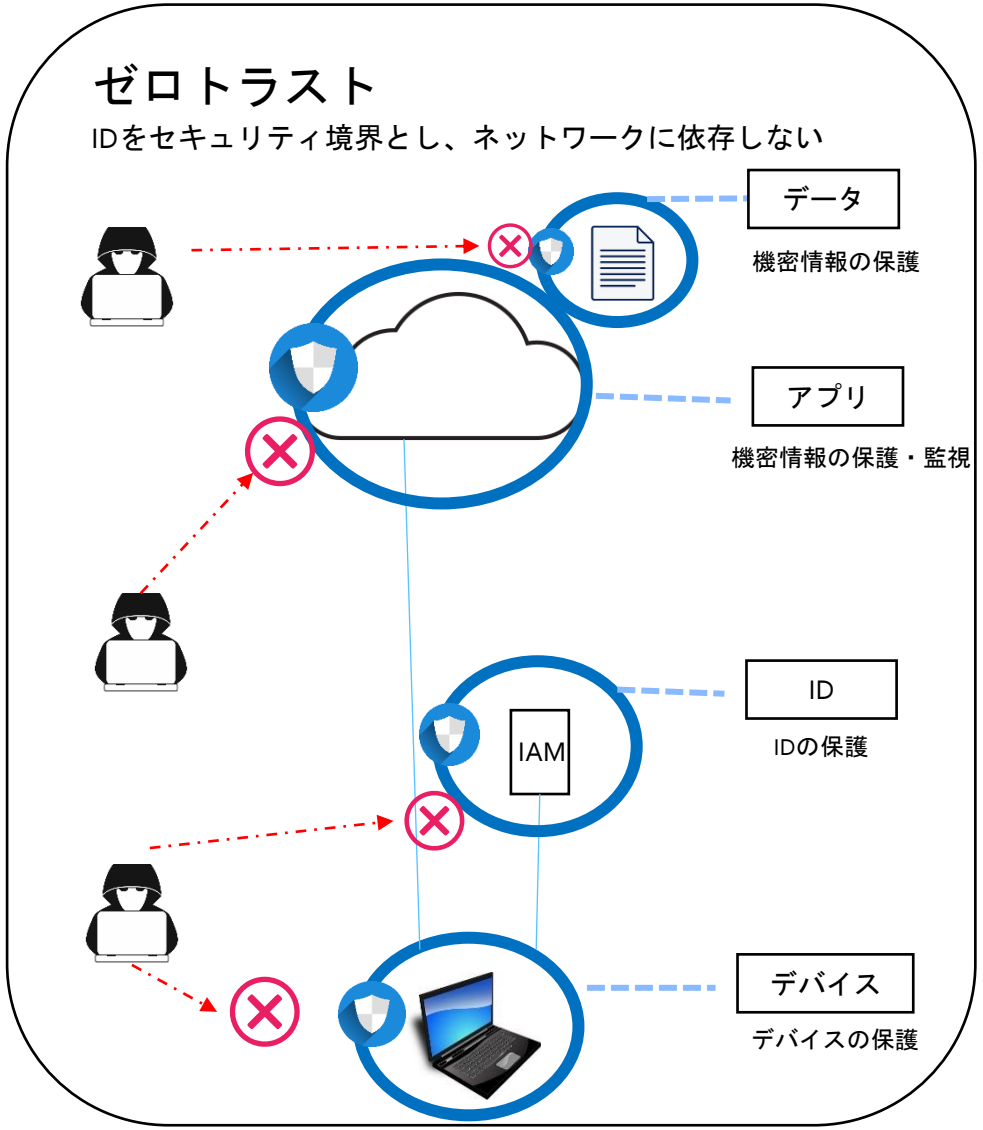
ゼロトラストセキュリティの検討

ゼロトラストセキュリティを構成する要素



ゼロトラストセキュリティとは





ゼロトラストセキュリティを構成する要素

IAM　IAP　EDR　MDM　MAM　SIEM　CASB　SWG　DLP

- これを入れればOKというゼロトラスト製品は存在しない
  - 複数の製品を組み合わせる必要がある
    →これらの複数の技術は相互に連携する必要がある
  - 例えば上記の9種類の技術を全て製品として提供するベンダーは存在しない
  - 製品間で情報を正しく連携できるようにアライアンスの形成が行われている

BeyondCorp Alliance

BeyondCorp Alliance
10社
Googleが中心

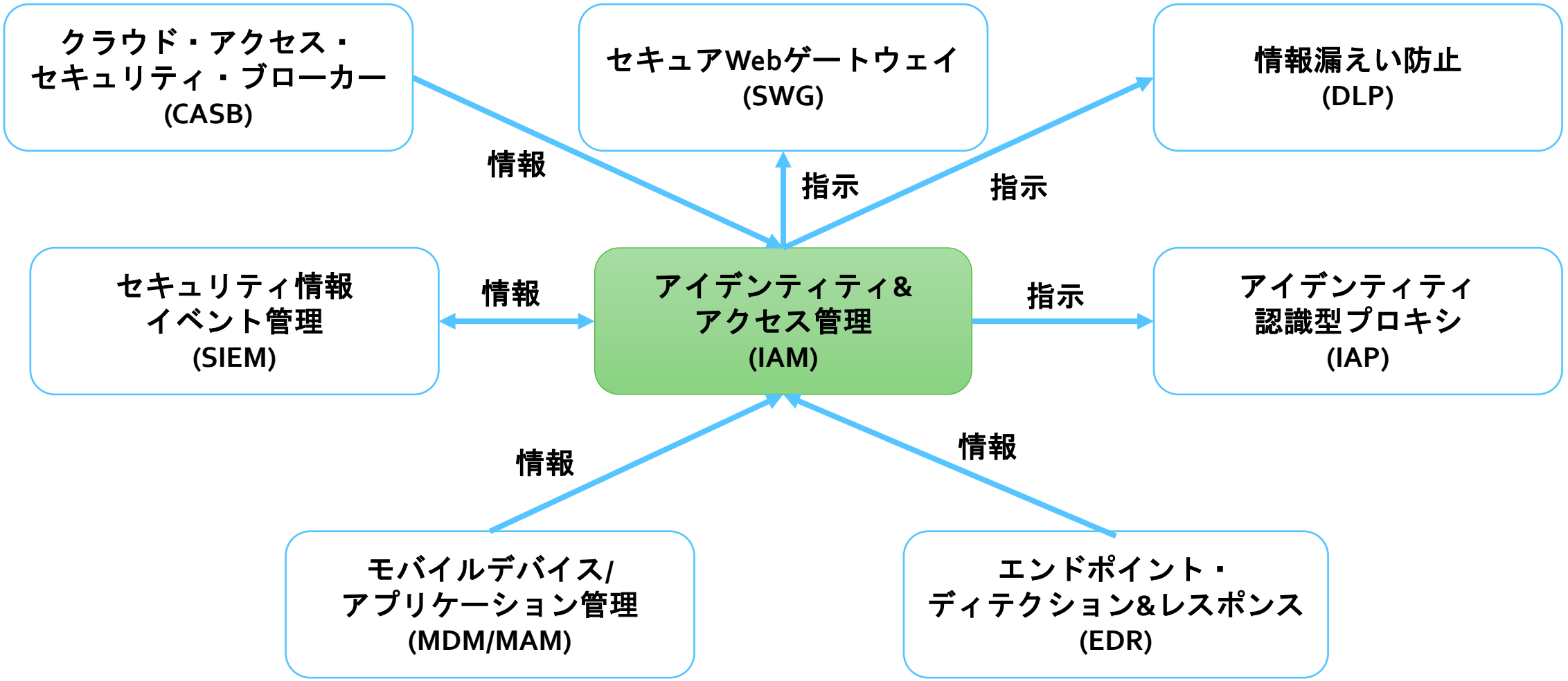
Microsoft Intelligent Security Association
Microsoft

Microsoft Intelligent Security Association
500社
Microsoftが中心

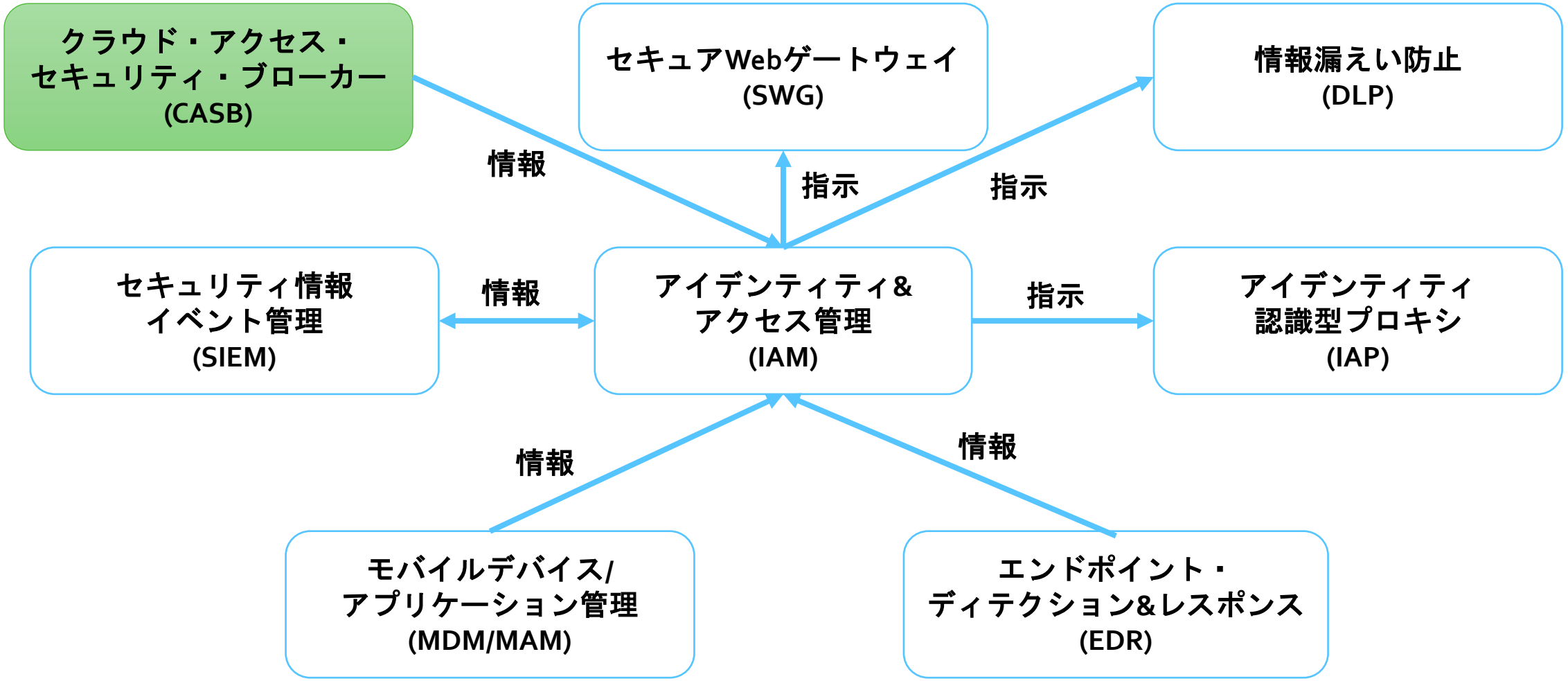
IDENTITY DEFINED SECURITY ALLIANCE

IDENTITY DEFINED SECURITY ALLIANCE
33社
Okta, Ping Identityが中心

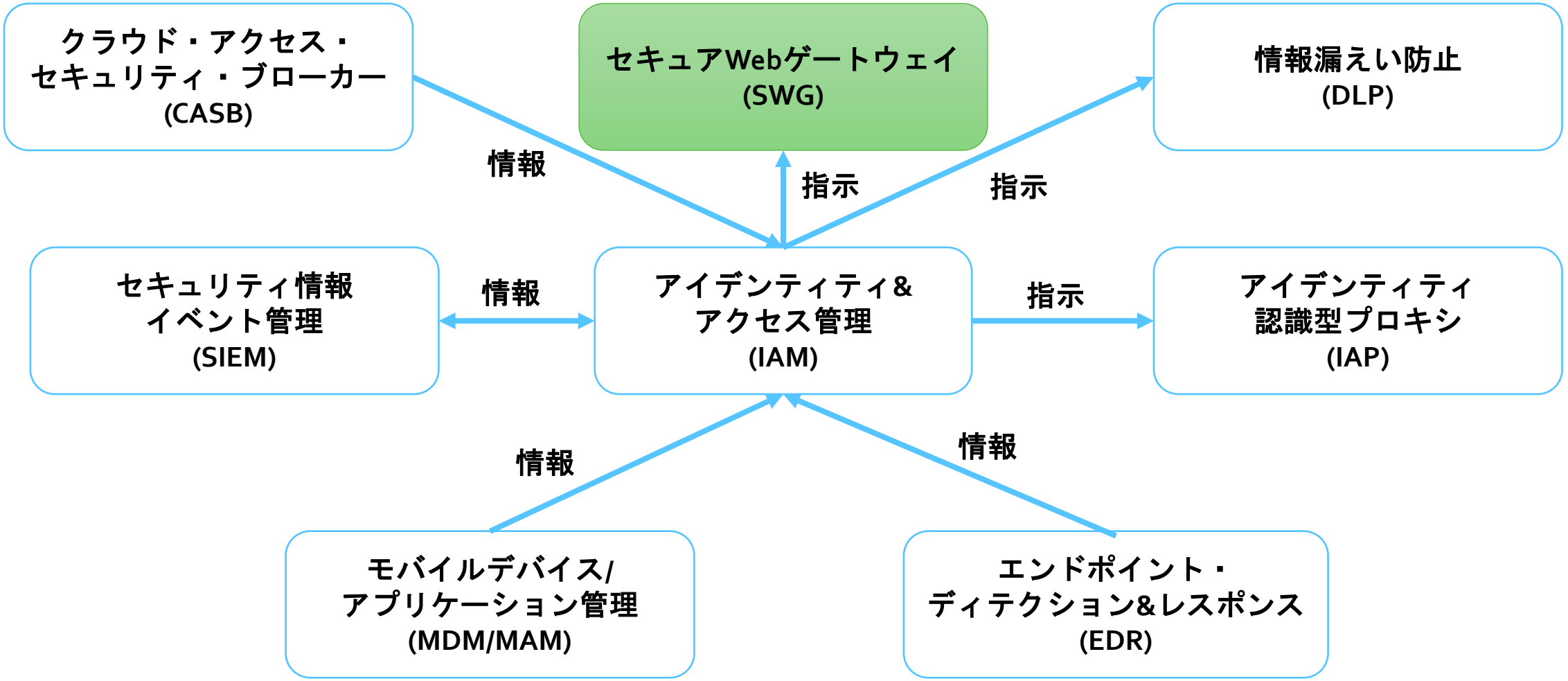
ゼロトラストの機能要素



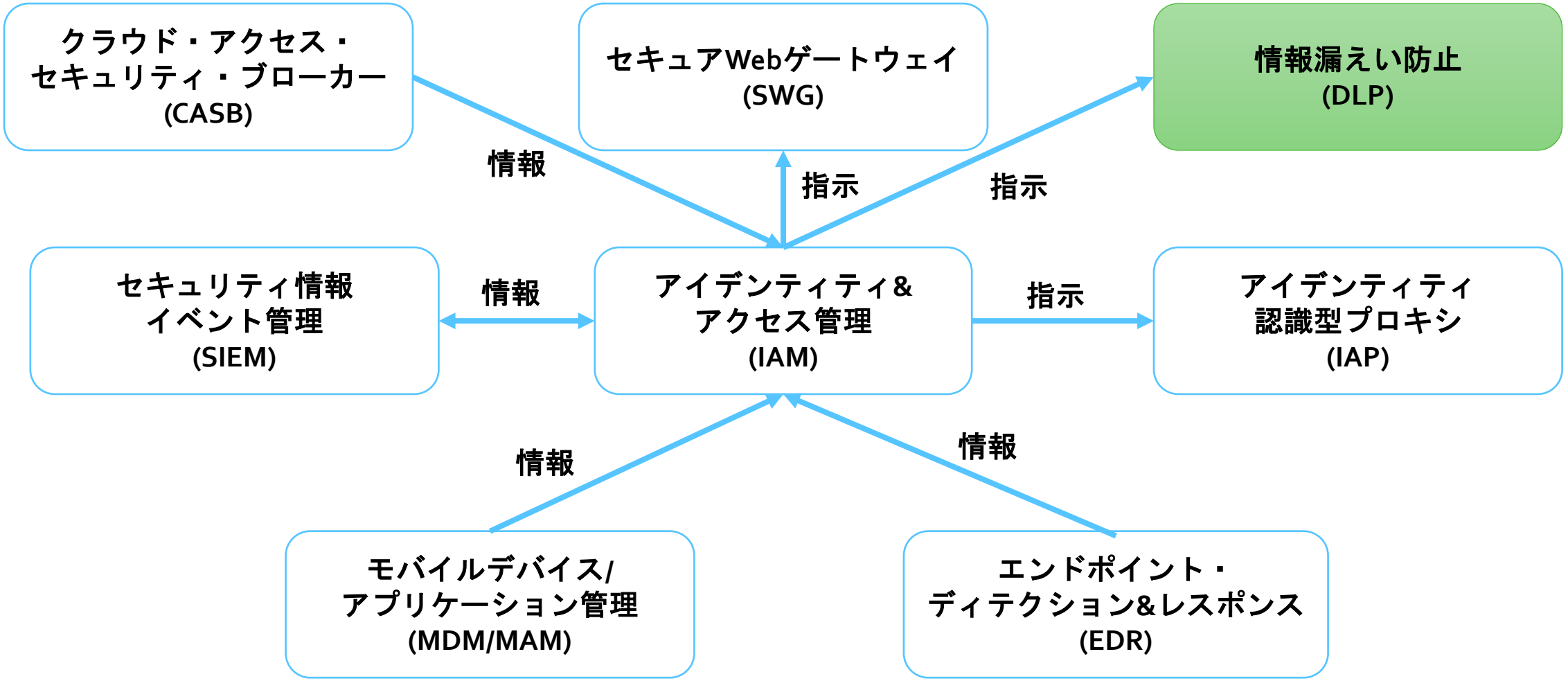
ゼロトラストの機能要素



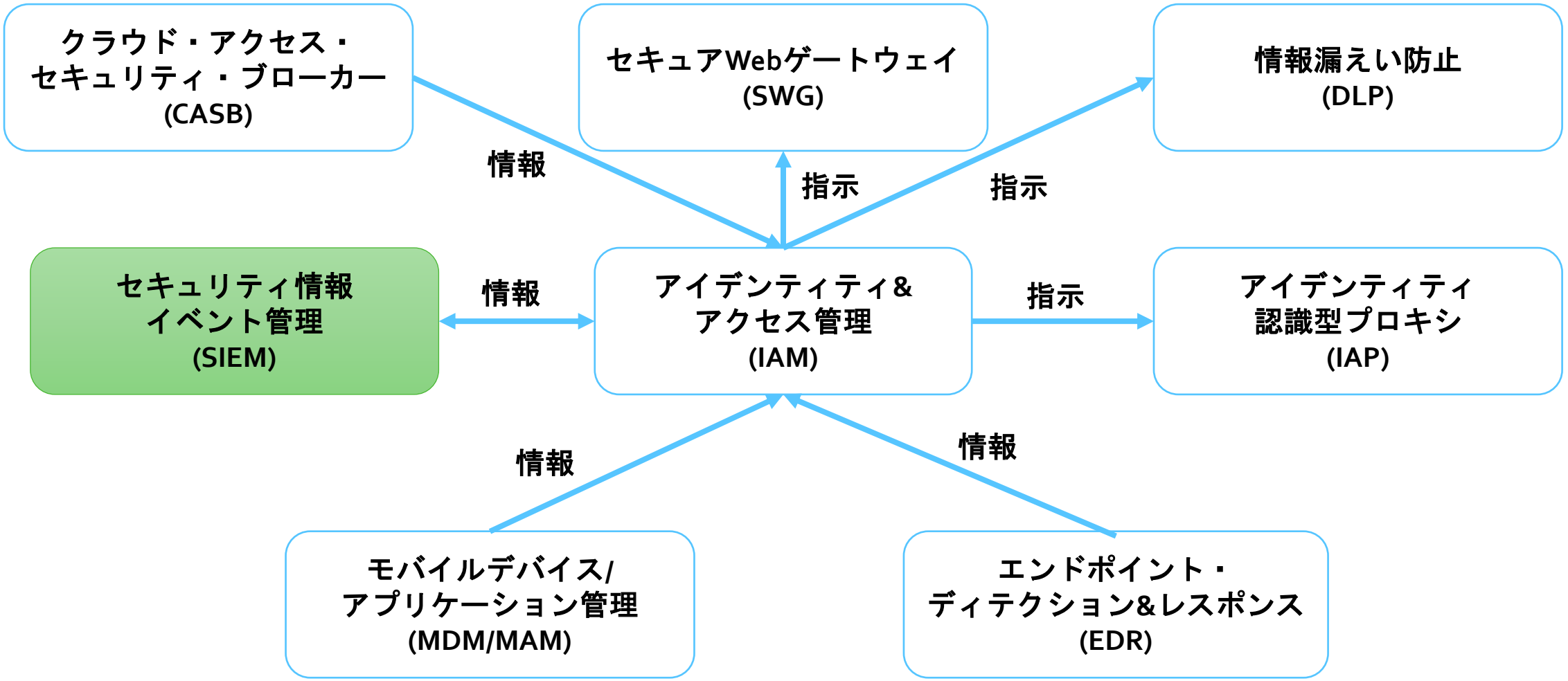
ゼロトラストの機能要素



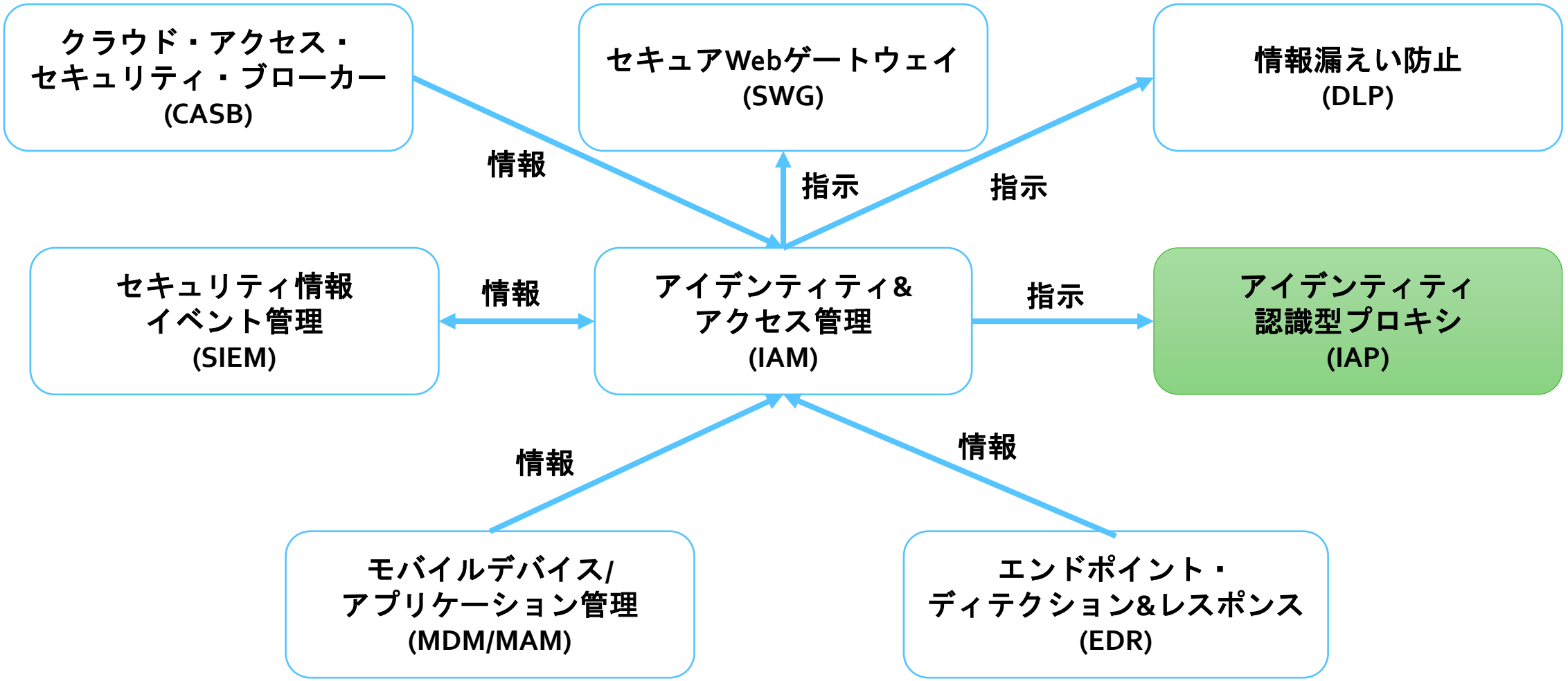
ゼロトラストの機能要素



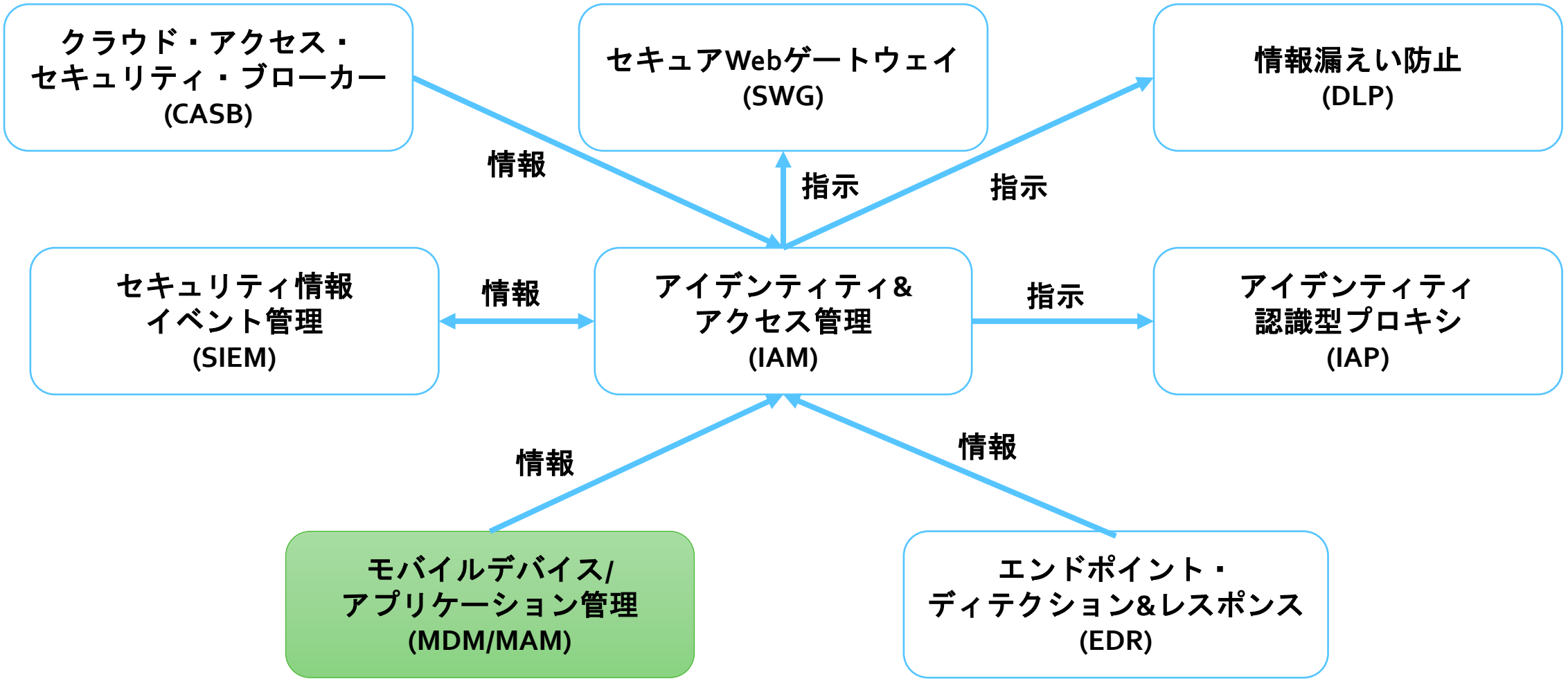
ゼロトラストの機能要素



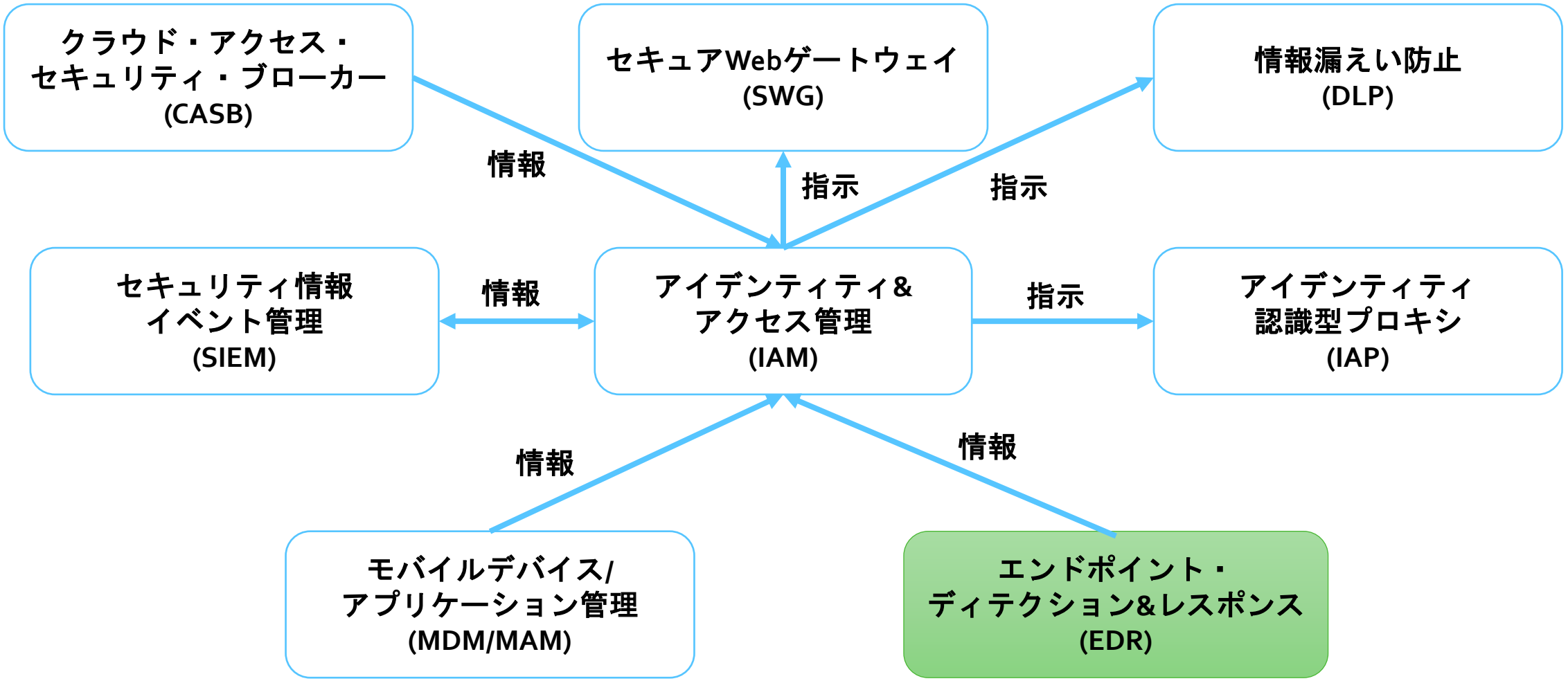
ゼロトラストの機能要素



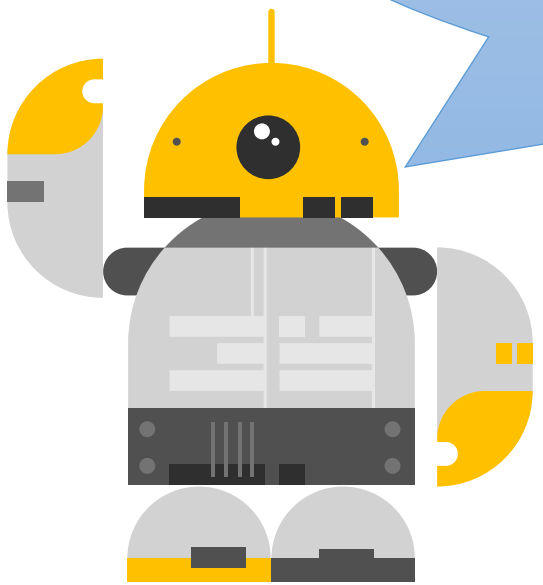
ゼロトラストの機能要素



ゼロトラストの機能要素



事例によるゼロトラストアプローチ

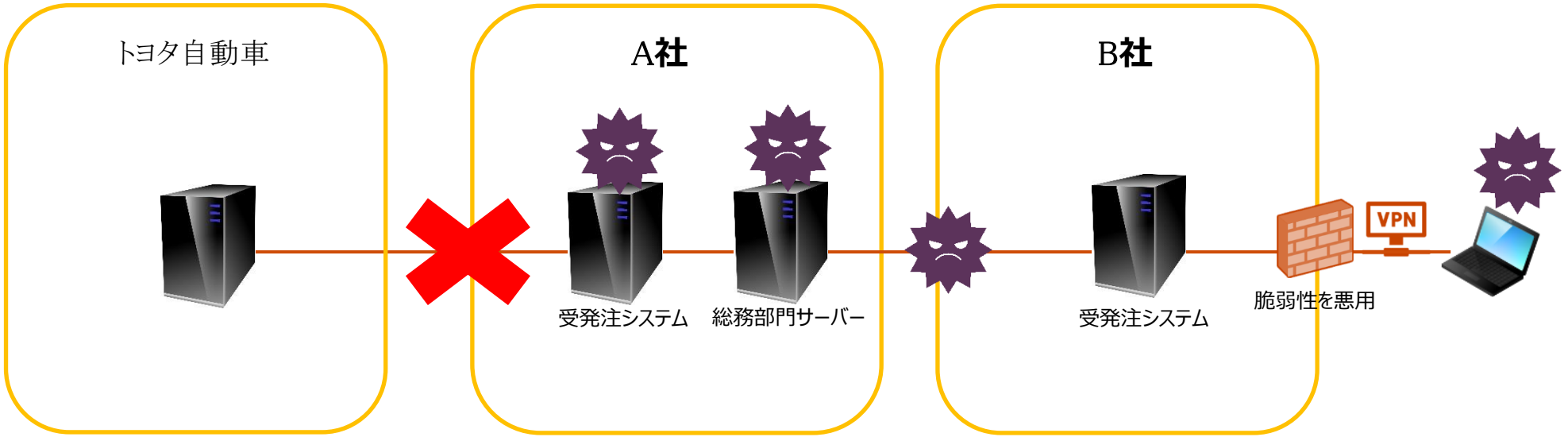


事例1

「トヨタ供給網へのサイバー攻撃により全工場の稼働が停止」

- 2022 年 3 月、トヨタ自動車のサプライチェーンの 1 つ、 A 社に対して行われたサイバー攻撃が発覚したことで、トヨタ自動車は国内の全工場を停止した。
  A 社が予防措置として取引先とのネットワークを遮断したことにより、トヨタ自動車も受発注システムを利用できなくなり工場の稼働が停止した。

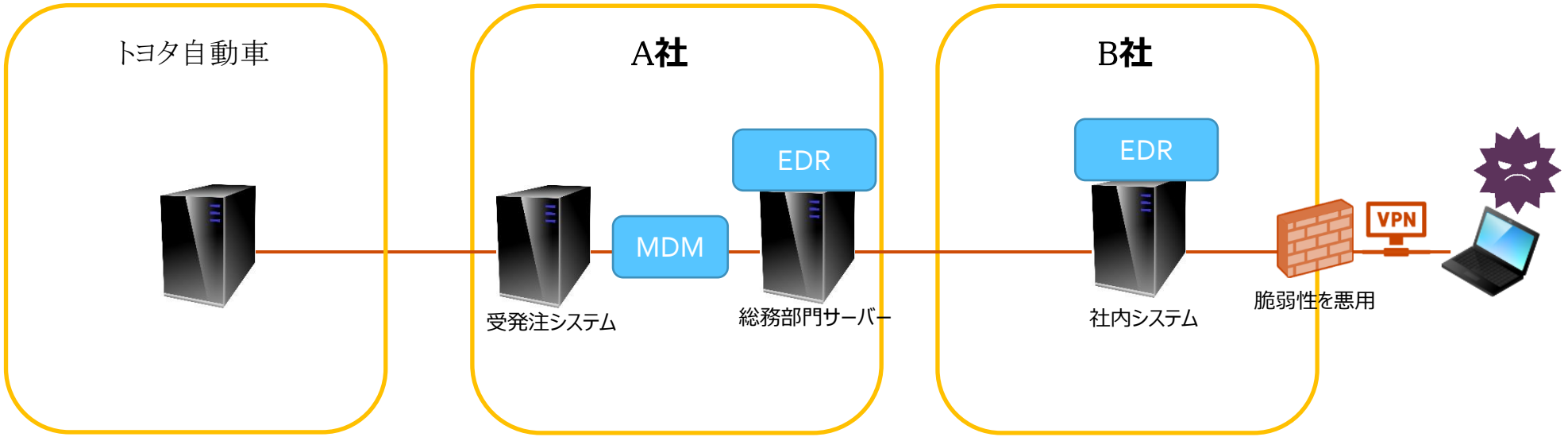
- 最初に攻撃を受けた A 社の取引先である B 社は、 VPN 装置の脆弱性をつかれ、ウィルスに侵入された。
  B社を経由してA社もウィルスに感染し、総務部門のサーバーから受発注システムのサーバーにまで侵入されていた。
  これにより取引先までウィルス被害が及ばないよう、A社は取引先とのネットワークを遮断した。



事例1～アプローチから

- **デバイス保護(MDM)**
  A社にMDMが導入されていれば、アクセス制限により総務部門サーバーから受発注システムサーバーへのウィルスの侵入を防ぐことができた

- **デバイス保護(EDR)**
  B社はVPN装置の脆弱性を突かれてしまったが、EDRが導入されていれば不審な挙動を検知して、端末を自動的に隔離してA社へのウィルスの侵入を防ぐことができた
  同様に、A社にもEDRが導入されていれば、ウィルスの早期発見・隔離により、取引先とのネットワークを遮断せずに済んだ

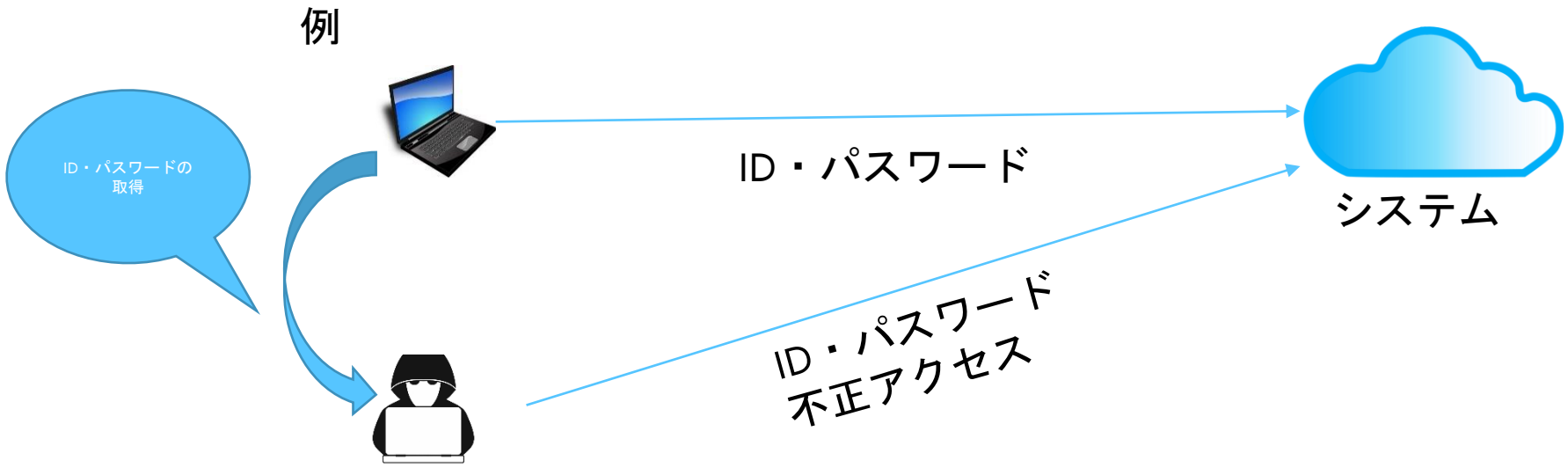


事例2

1，「2022 年 7 月、郡山市、庁内システムに職員が不正アクセス、ポエムなど書き込み」

2，「2022 年 10 月、創価大、教員アカウントに不正アクセス、迷惑メールの踏み台に」

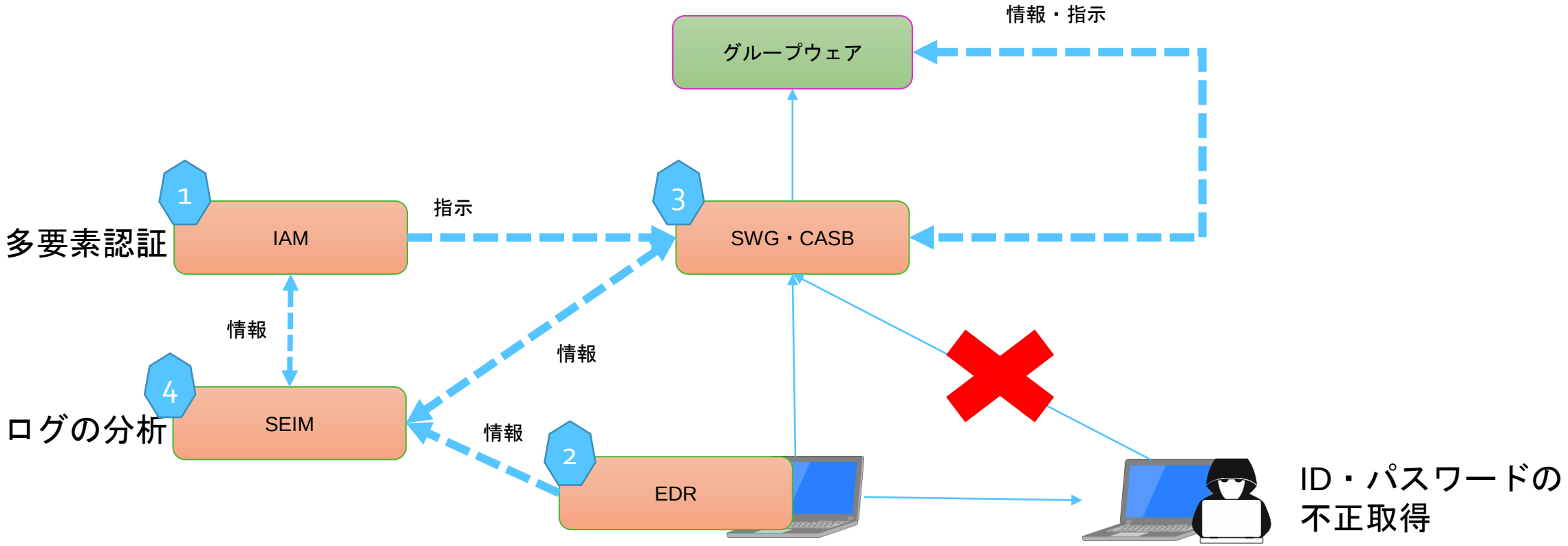
- 問題点としては ID・パスワードのみでのアクセス許可により第三者からアクセスパスワード等を取得されたことが考えられる。この場合どの端末からでもアクセスが可能になるのが想定され、また情報流出や不正アクセスへの踏み台の可能性がある。今回説明するアプローチは IAM などで多要素認証を採用し、またアクセス操作に対する制御やログの解析などを実施して、セキュリティインシデントを低減させる。



利用者が意図していない操作や改ざん等が行われる

事例2～アプローチ～

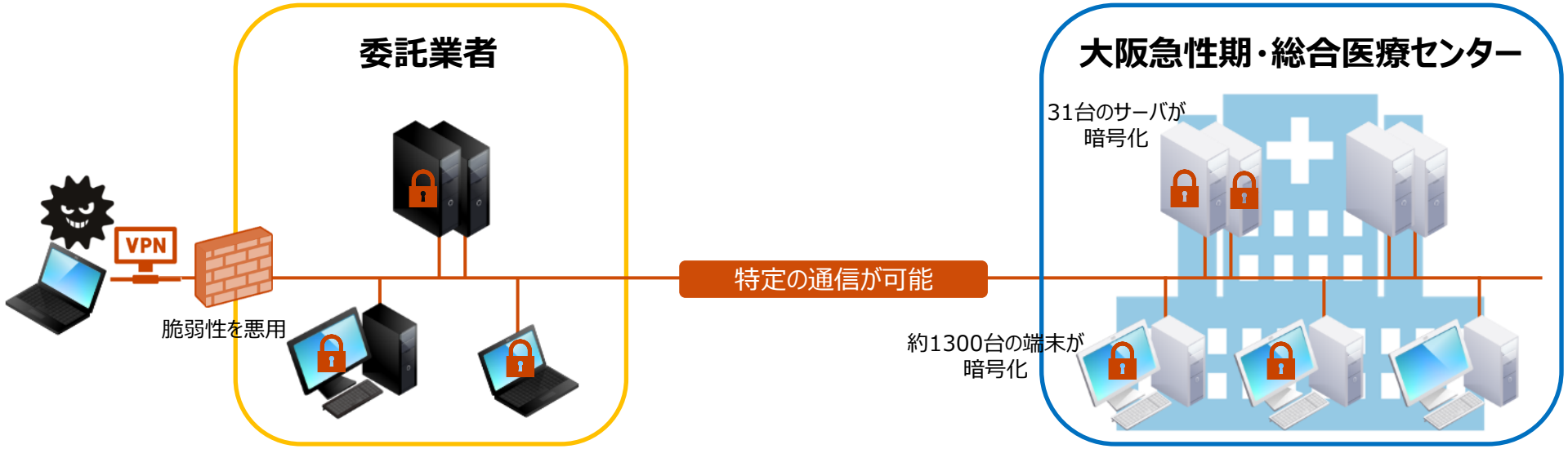
・第三者からID・パスワードの情報取得されると誰でもアクセス可能な状態



事例3

「2022年10月31日、大阪府立病院機構 大阪急性期・総合医療センターで電子カルテシステムがランサムウェアに感染して診療が停止」

- ランサムウェア(Phobos)の攻撃により、31台のサーバと約1300台の端末が暗号化され、電子カルテシステム及び関連するネットワークが完全に停止した
- 攻撃の侵入経路は、委託業者のリモートメンテナンスのVPN接続環境を通じて侵入された可能性がある
- 委託業者のサーバと医療センターのサーバは、オーダリングシステムの連携で繋がっており、委託業者のサーバが被害を受けた後に医療センターのサーバが攻撃を受けるサプライチェーン攻撃の形であった

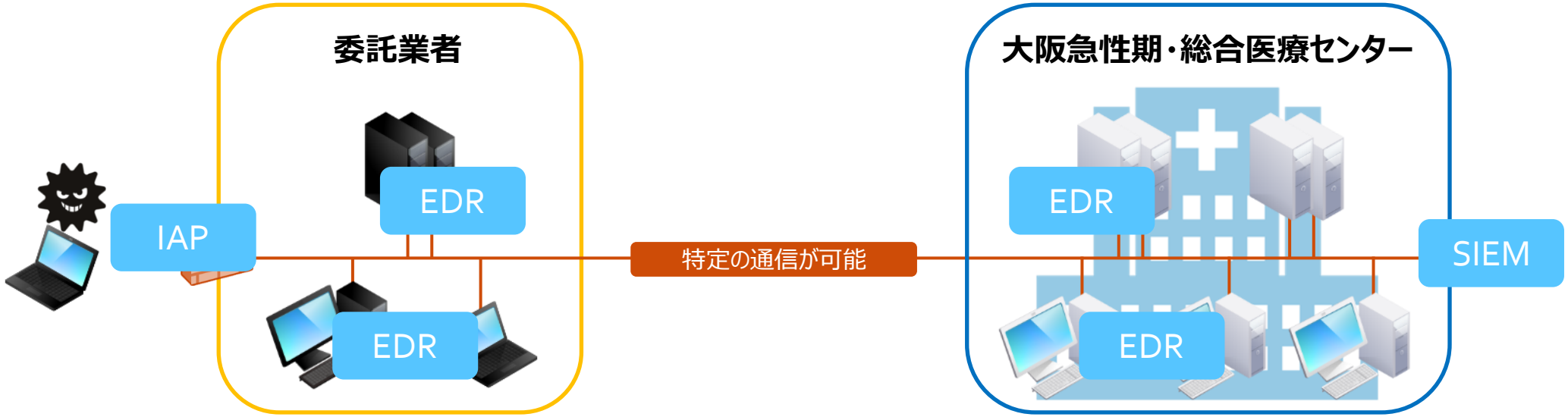


事例3～アプローチ～

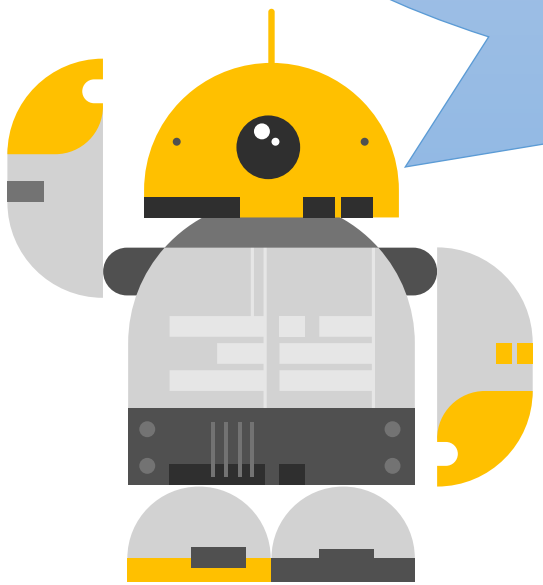
- **ID基盤の整備(IAP)**
  IAPを導入した環境であれば、外部から社内ネットワークに直接アクセスできず、アプリへのアクセスがあるたびに認証・許可が行なわれるため、委託業者のネットワークへの侵入を防ぐことができた

- **デバイス保護(EDR)**
  ウイルス対策ソフトも無効化されたが、EDRが導入されていればウイルス対策ソフトを無効化する挙動を検知して、端末を自動的に隔離して、暗号化を防ぐことができた

- **社内アプリの監視・分析(SIEM)**
  不正アクセスの記録が消え、犯行元の特定が困難な状況となっているが、SIEMが導入されていれば、ログの分析が容易になり、犯行元特定の捜査がもっと進んでいる



全体の流れに対する導入ステップ



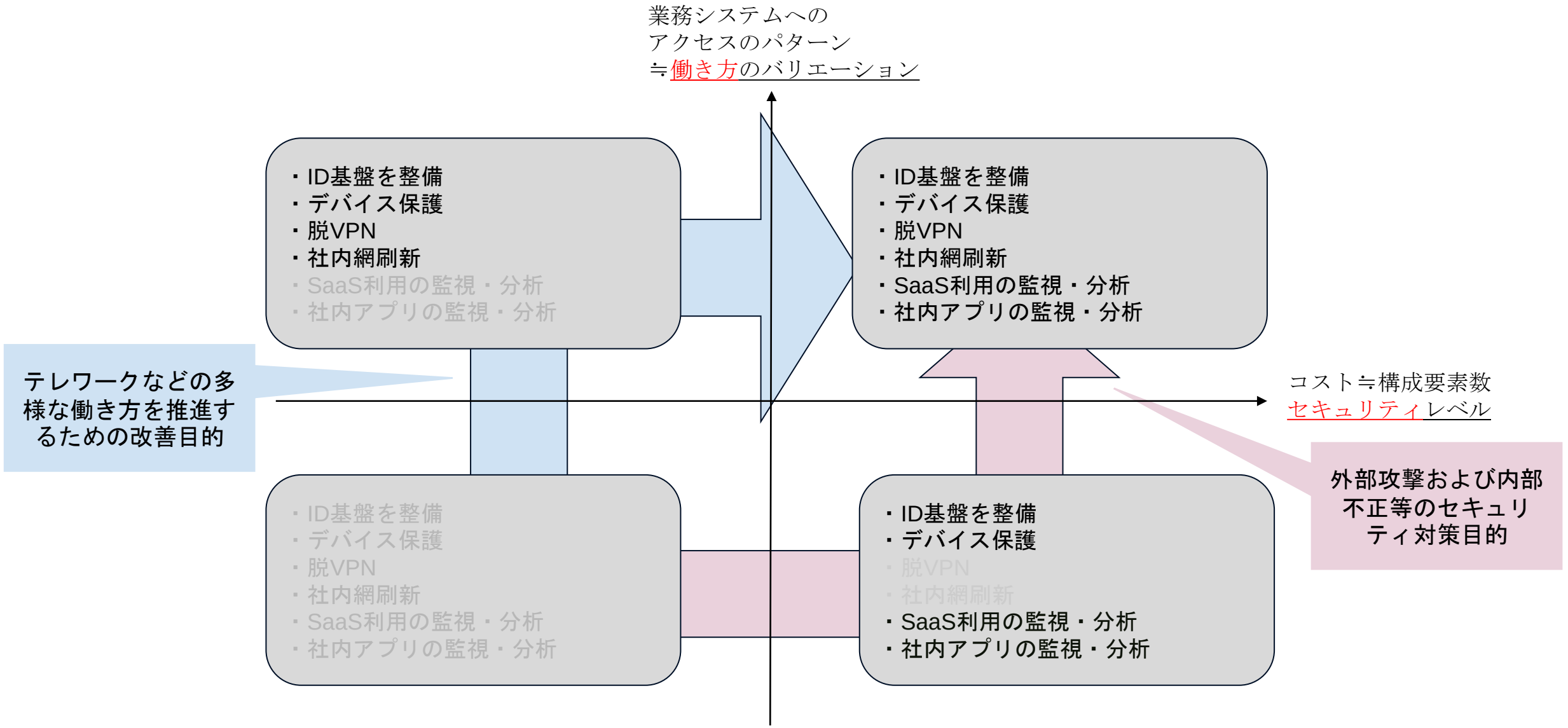
全体の流れに対する導入ステップ

- ソ研分科会参加者に対するアンケートやヒアリングの実施により、**セキュリティインシデント**及び**多様な働き方**がゼロトラスト導入のきっかけとして多いことが分かった
- 今回は下記2パターンの対応契機を例に導入ステップを検討

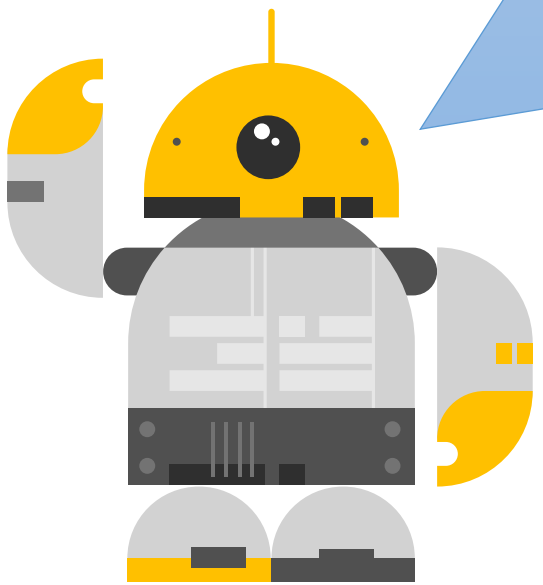
①テレワークなどの多様な働き方を推進するための改善目的
②外部攻撃および内部不正等のセキュリティ対策目的

- 次のスライドで要素の選定に伴う図の説明をする

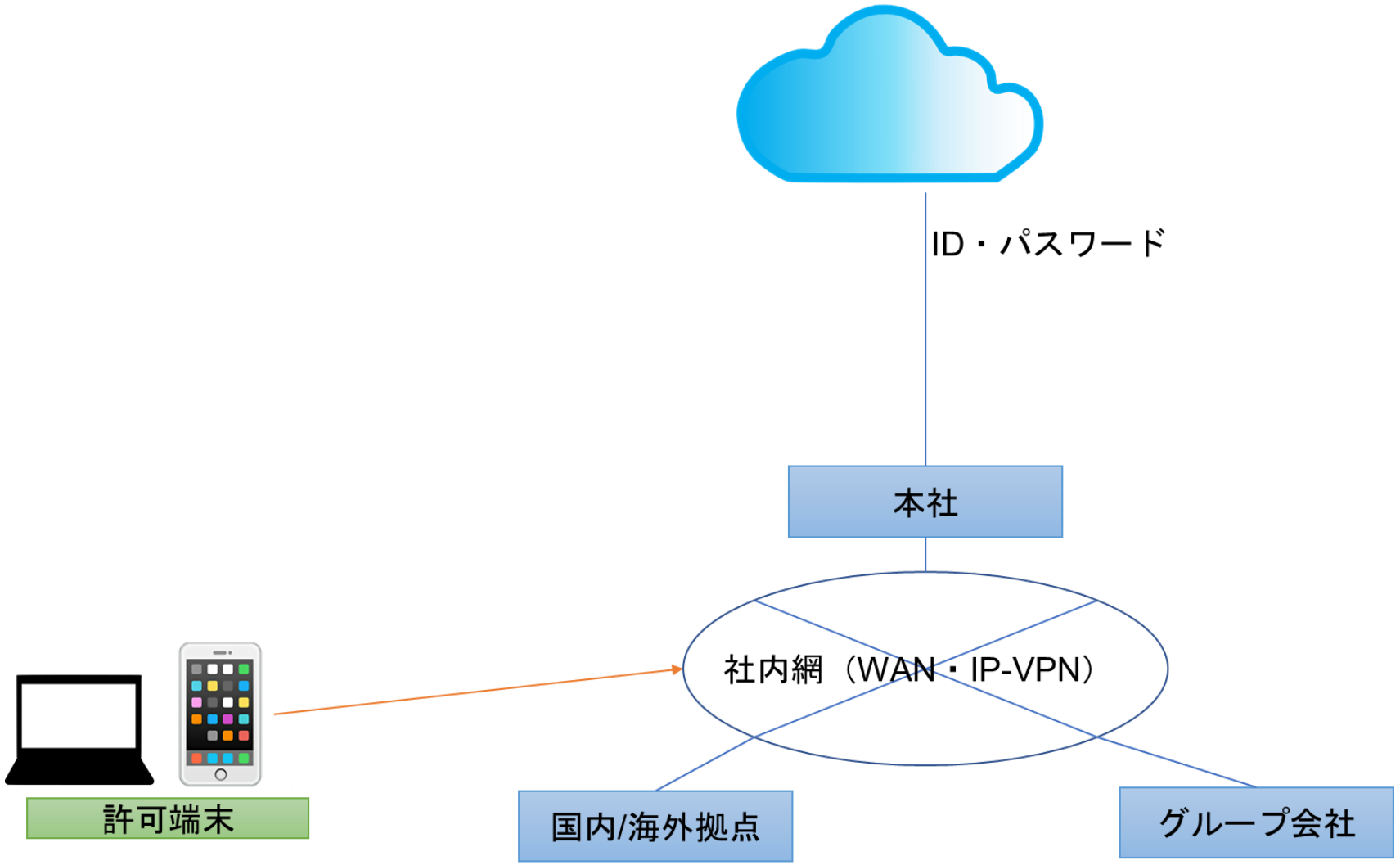
ゼロトラストセキュリティ構成要素の導入とその効果



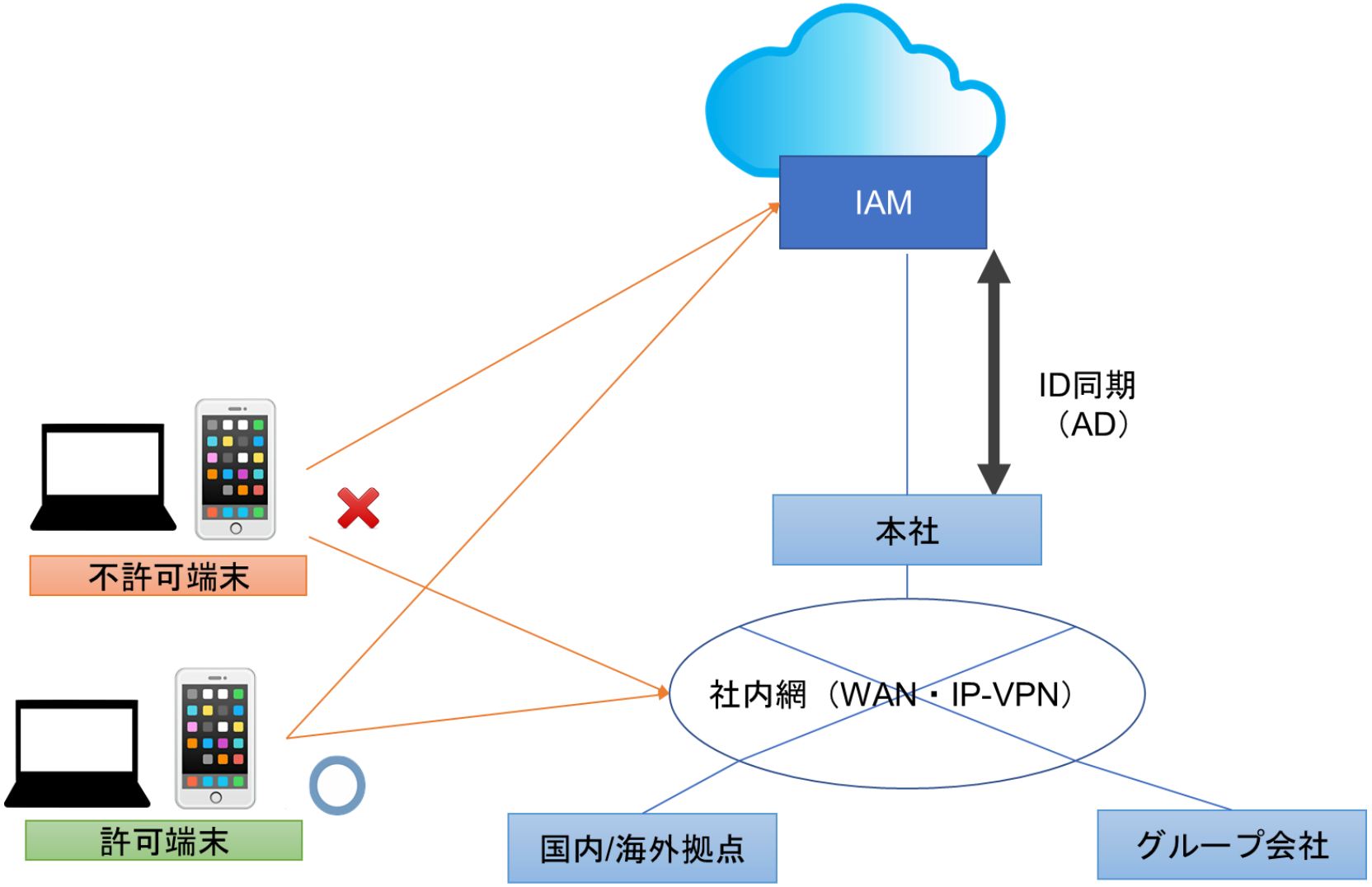
①テレワークなどの多様な働き方を推進するための改善目的



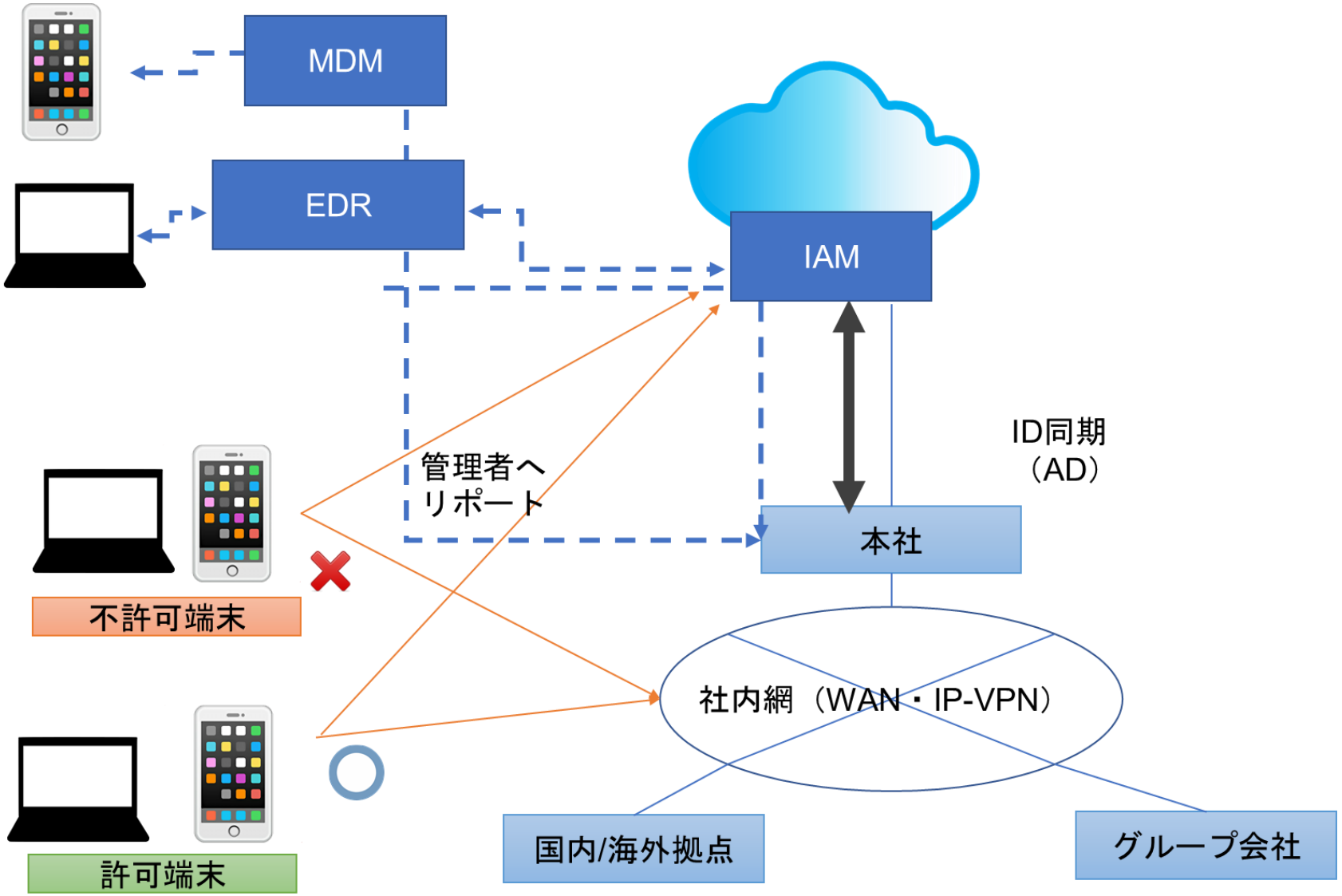
ステップ0 ゼロトラスト導入前のシステム



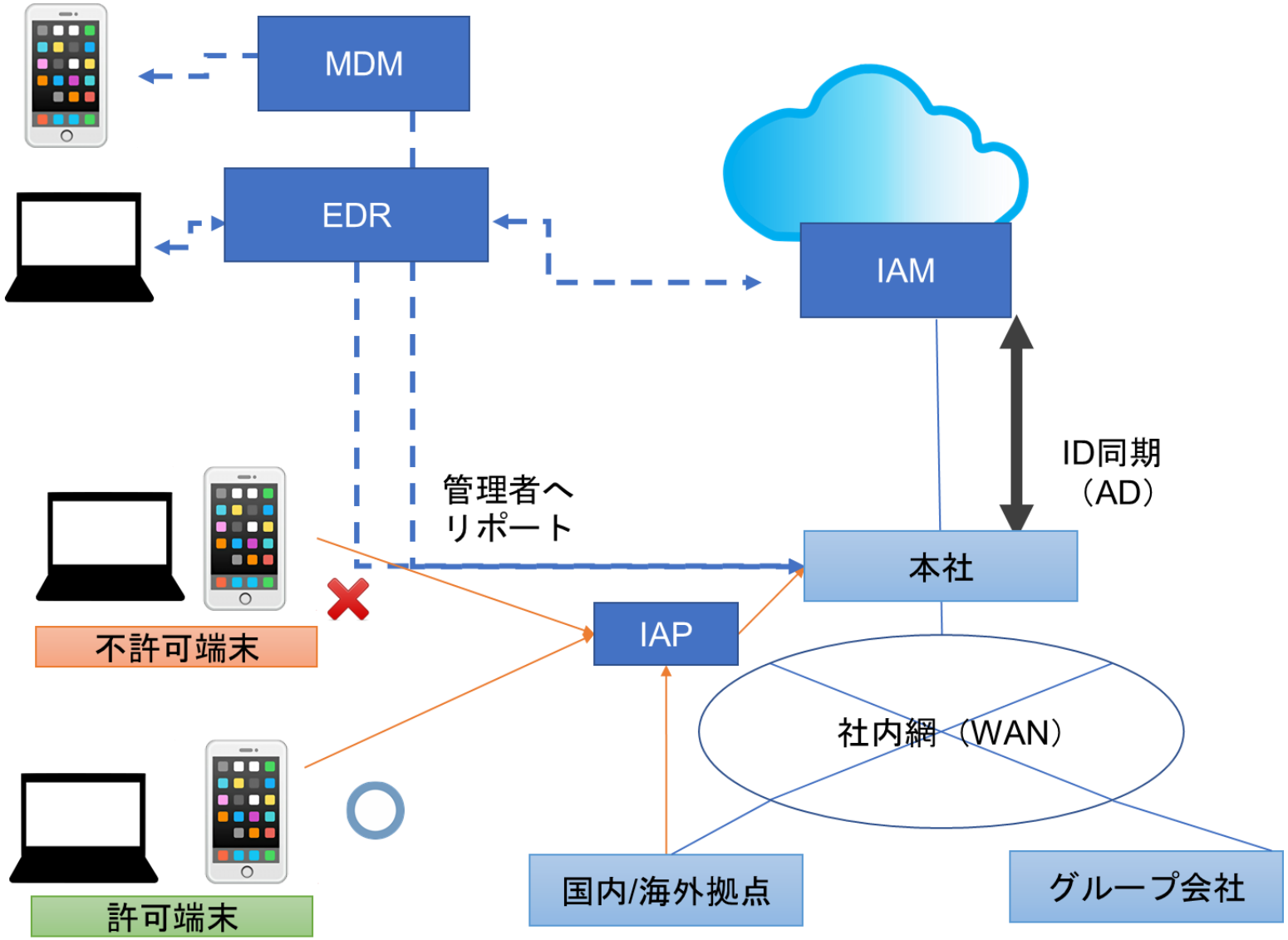
ステップ1 ID基盤の整備



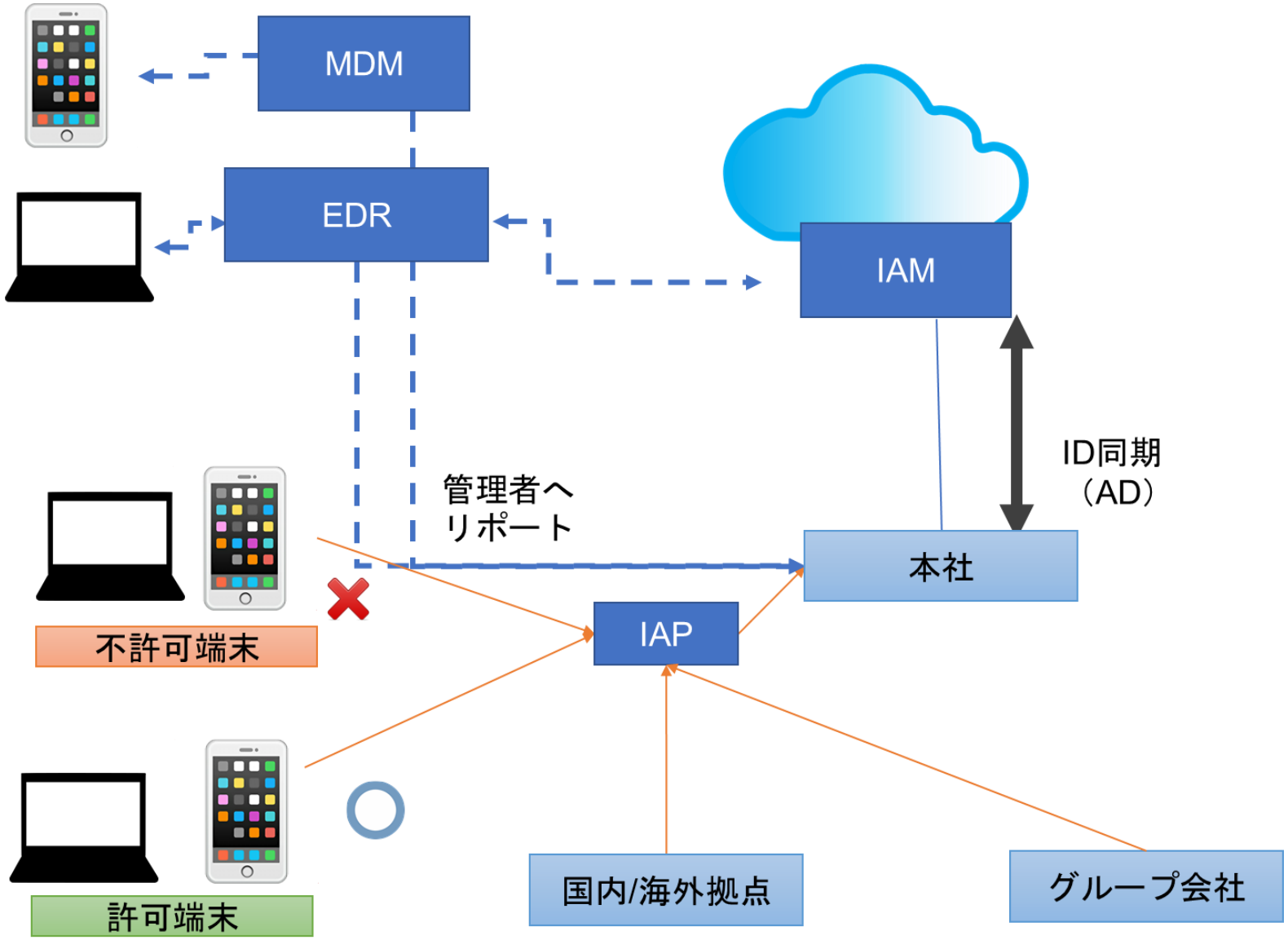
ステップ2 デバイス保護



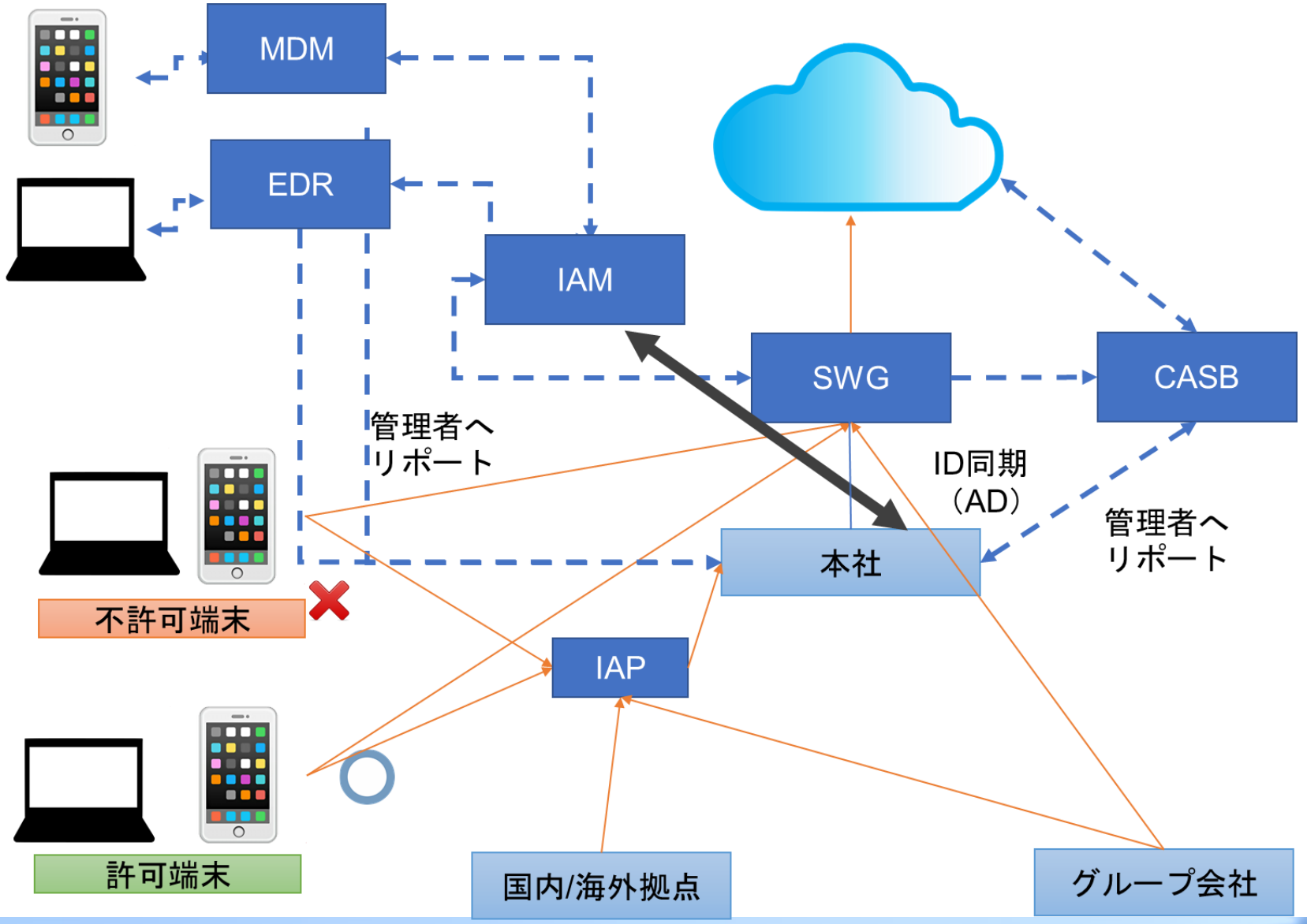
ステップ3 脱VPN


MDM
EDR
IAM
ID同期
（AD）
管理者へ
リポート
本社
IAP
不許可端末
社内網（WAN）
国内/海外拠点
グループ会社
許可端末

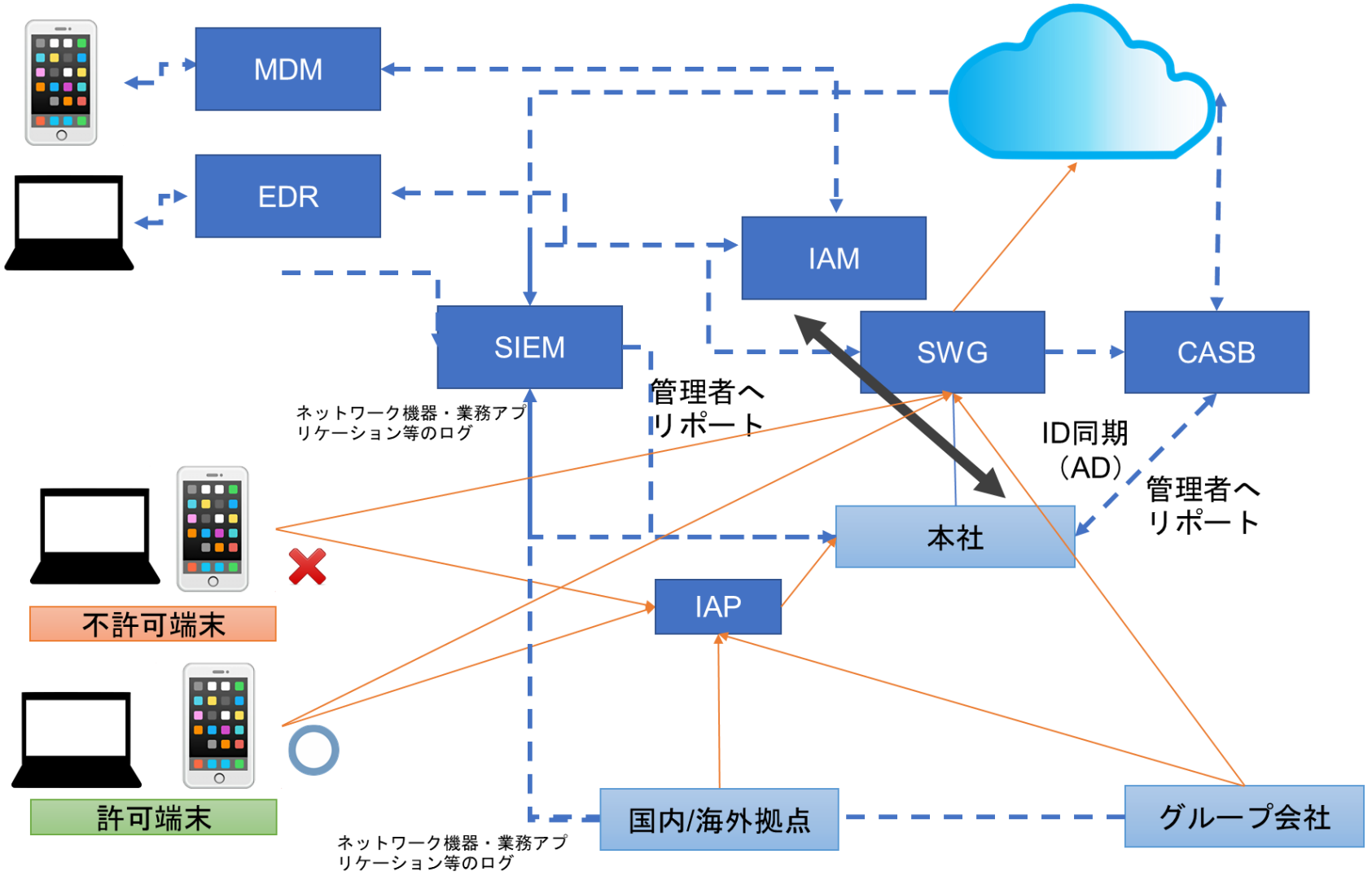
ステップ4 社内網刷新



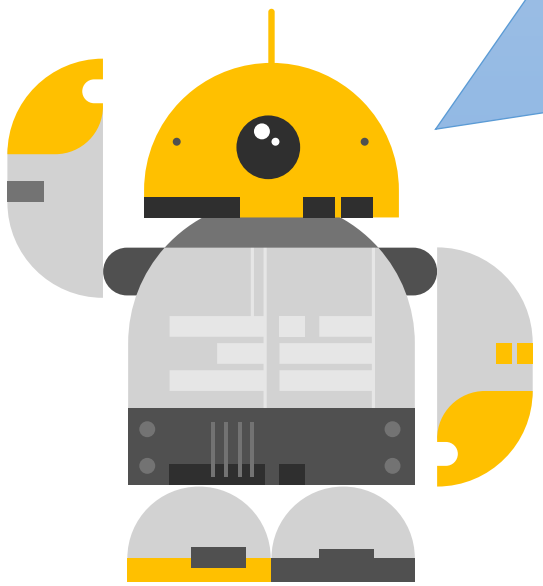
ステップ5 SaaSアプリの監視・分析



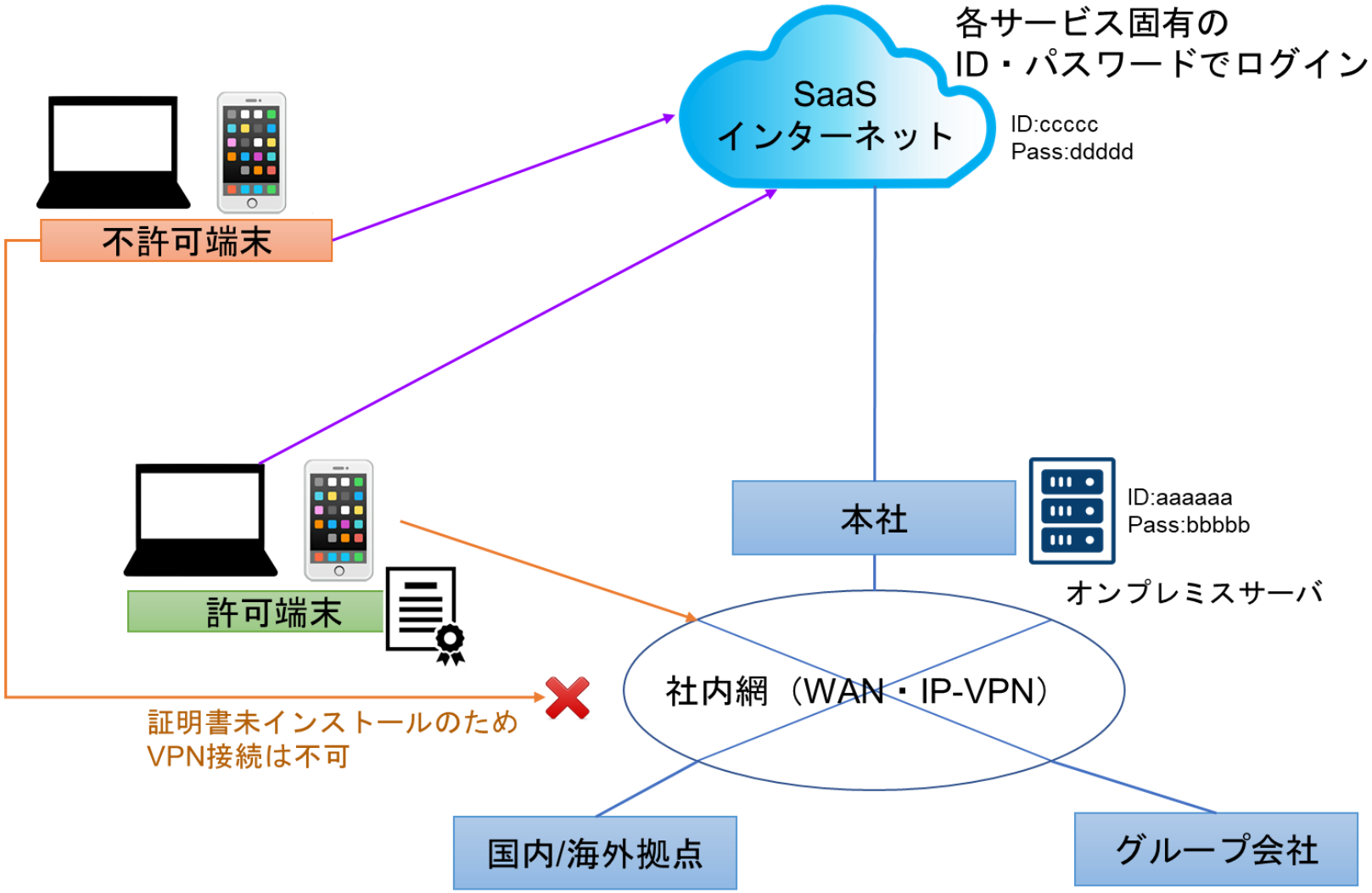
ステップ6 社内アプリの監視・分析



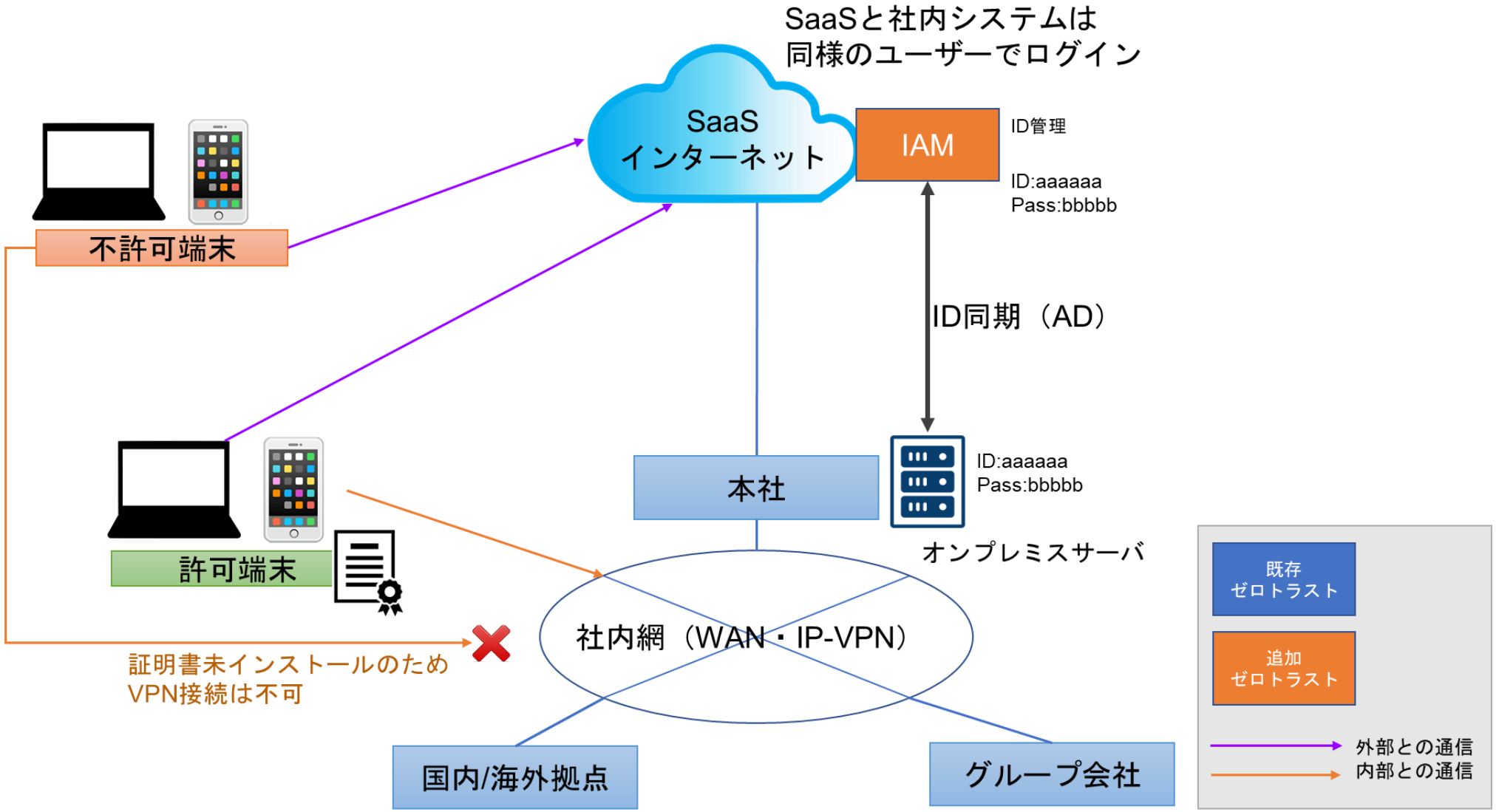
②外部攻撃および内部不正等のセキュリティ対策目的



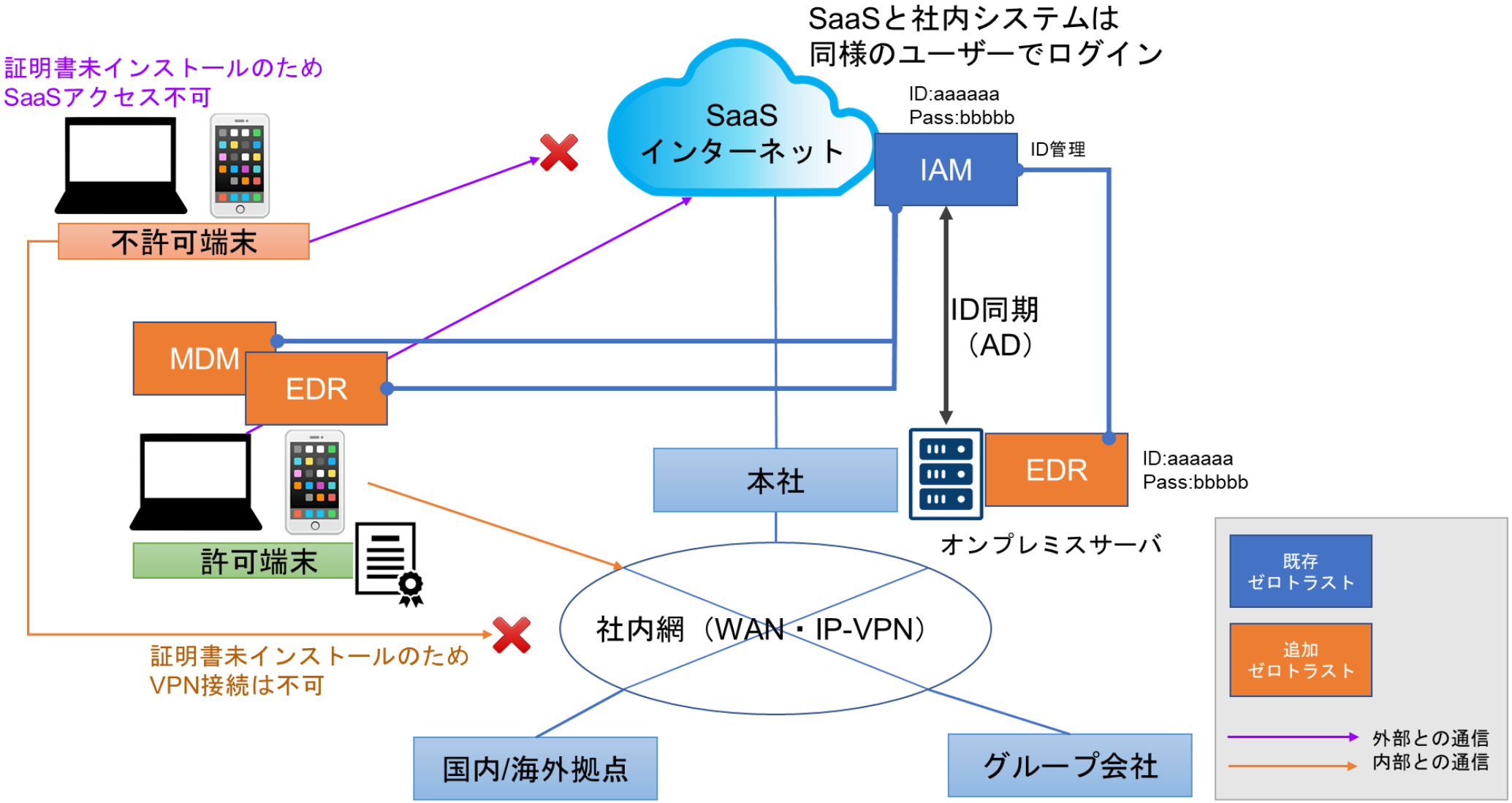
ステップ0 ゼロトラスト導入前のシステム



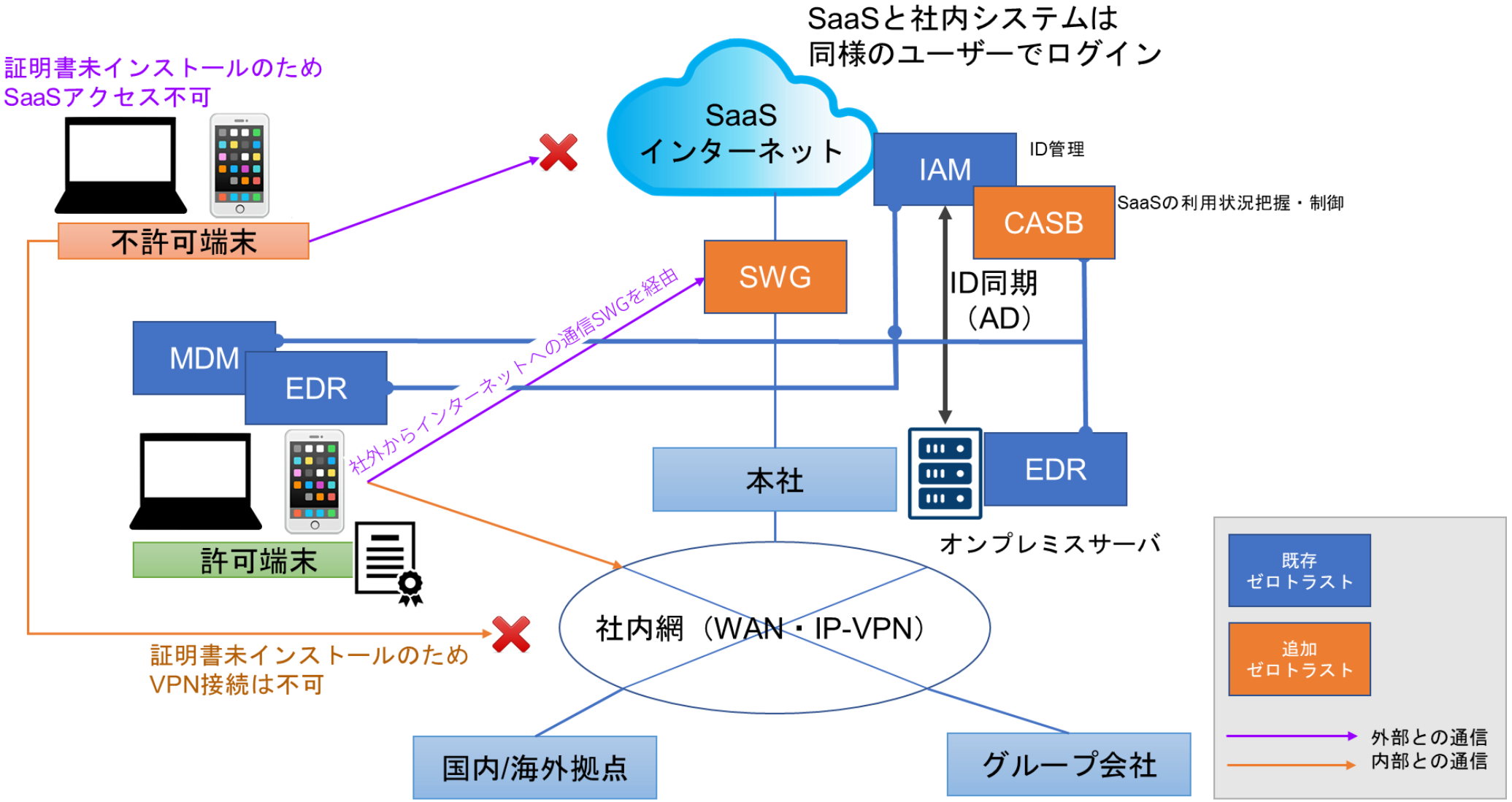
ステップ1 ID基盤の整備



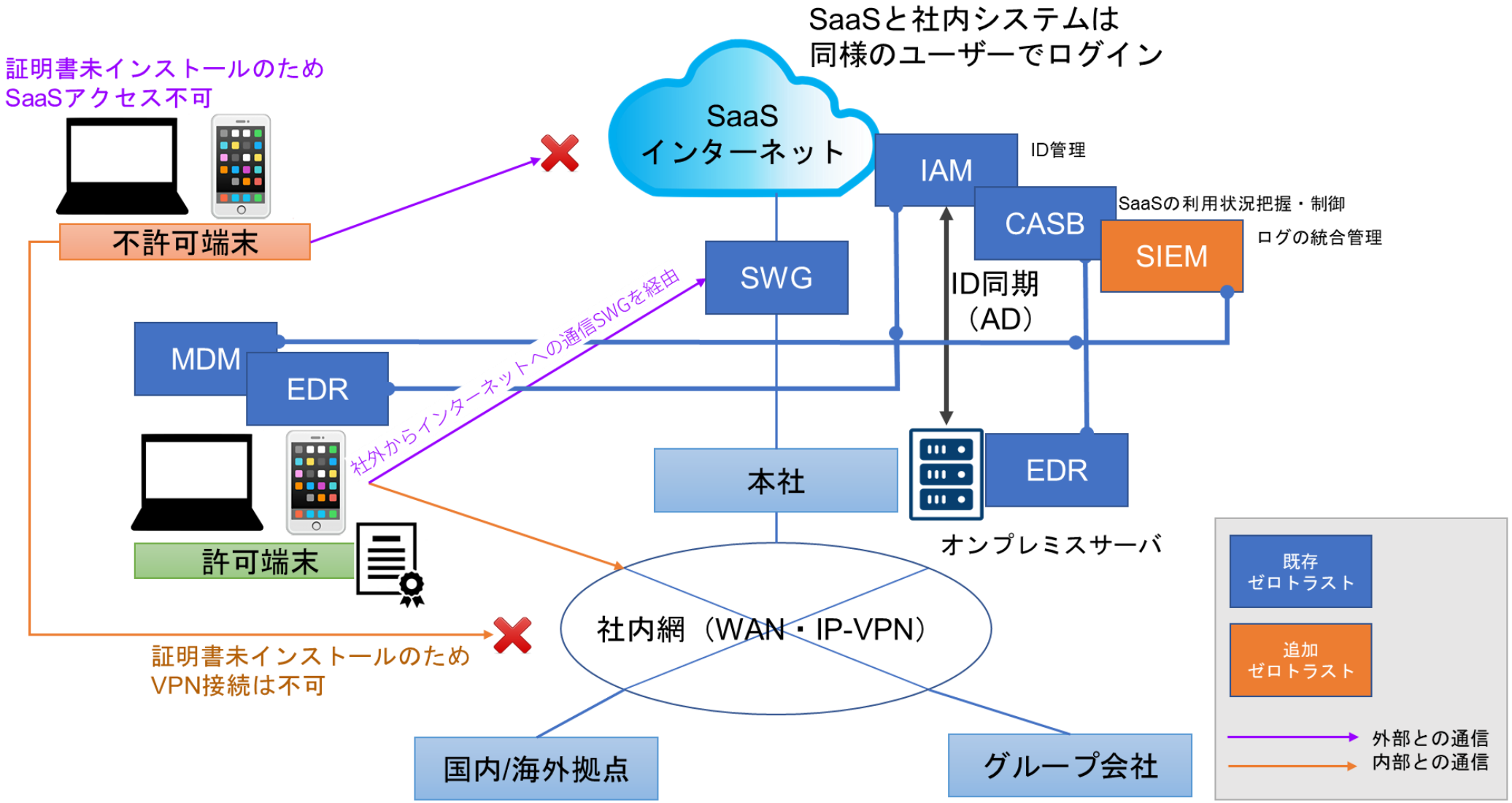
ステップ2 デバイス基盤



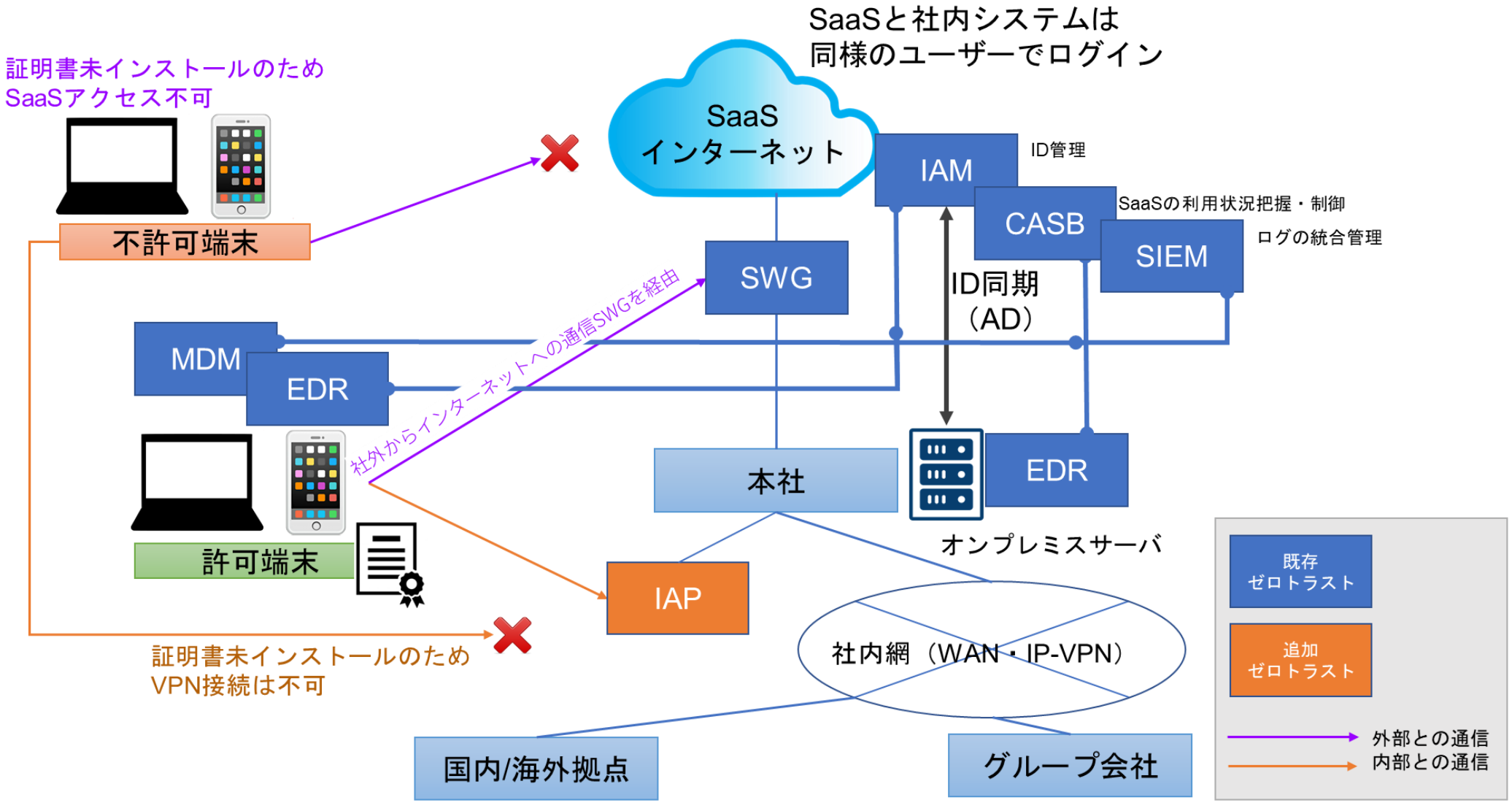
ステップ3 SaaSアプリの監視・分析



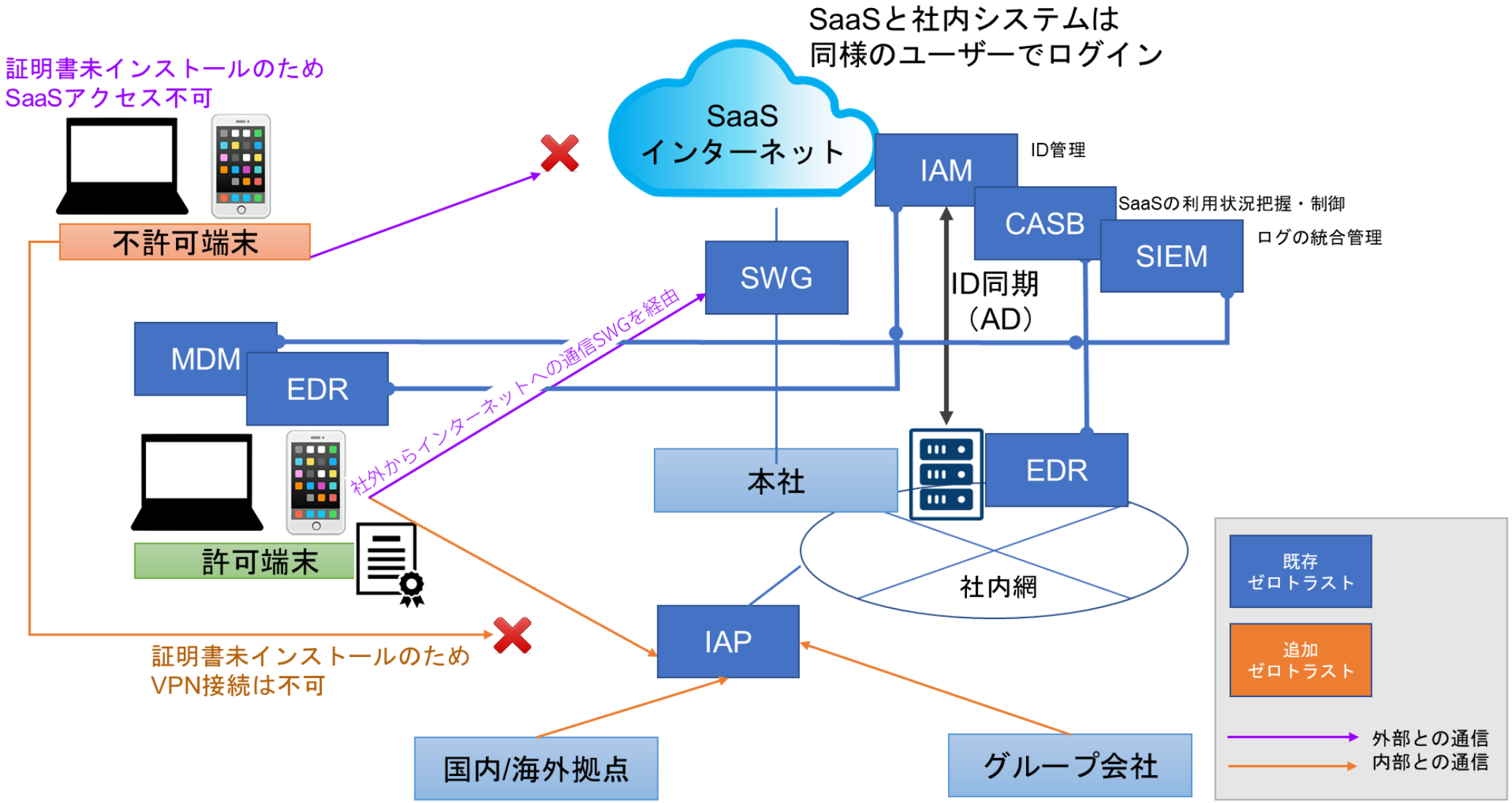
ステップ4 社内アプリの監視・分析



ステップ4 社内網刷新


SaaSと社内システムは
同様のユーザーでログイン
証明書未インストールのため
SaaSアクセス不可
SaaS
インターネット
IAM
ID管理
CASB
SaaSの利用状況把握・制御
SIEM
ログの統合管理
不許可端末
SWG
ID同期
（AD）
MDM
EDR
社外からインターネットへの通信SWGを経由
本社
EDR
オンプレミスサーバ
許可端末
IAP
証明書未インストールのため
VPN接続は不可
社内網（WAN・IP-VPN）
国内/海外拠点
グループ会社
既存
ゼロトラスト
追加
ゼロトラスト
外部との通信
内部との通信

ステップ5 脱VPN


SaaSと社内システムは
同様のユーザーでログイン
証明書未インストールのため
SaaSアクセス不可
不許可端末
SaaS
インターネット
IAM
ID管理
CASB
SaaSの利用状況把握・制御
SIEM
ログの統合管理
SWG
ID同期
（AD）
MDM
EDR
社外からインターネットへの通信SWGを経由
本社
EDR
許可端末
社内網
IAP
証明書未インストールのため
VPN接続は不可
国内/海外拠点
グループ会社
既存
ゼロトラスト
追加
ゼロトラスト
外部との通信
内部との通信

まとめ

『働き方改革』により**多様な働き方への対応**が必要に

多様な働き方の実現 ≒ 多様アクセス方法への対応

⟷ **セキュリティリスクとのトレードオフ**

サイバー攻撃の**高度化・巧妙化**

ビジネスへ大きな影響を及ぼすサイバー攻撃の発生

- トヨタ供給網へのサイバー攻撃、全工場稼働停止
- 大阪急性期・総合医療センターへのサイバー攻撃、電子カルテシステム障害

⟷ **サイバー攻撃の経営問題化**

ゼロトラストセキュリティへの対応が急務

まとめ

ゼロトラストセキュリティへの対象事項を洗い出し「**働き方改革**」、「**セキュリティ対策**」の２つの導入目的を元に導入方法を検討・提案。

自社状況や導入目的を把握した上で自社に適したゼロトラストセキュリティ対応を行うことが重要

【ゼロトラスト対象事項】

- ID 基盤を整備
- デバイス保護
- 脱 VPN
- 社内網刷新
- SaaS 利用の監視・分析
- 社内アプリの監視・分析

テレワークなどの多様な働き方を推進するための改善目的

外部攻撃および内部不正等のセキュリティ対策目的

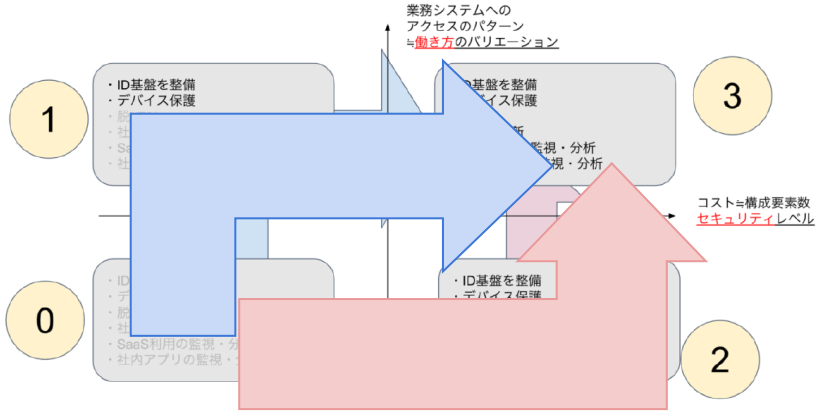
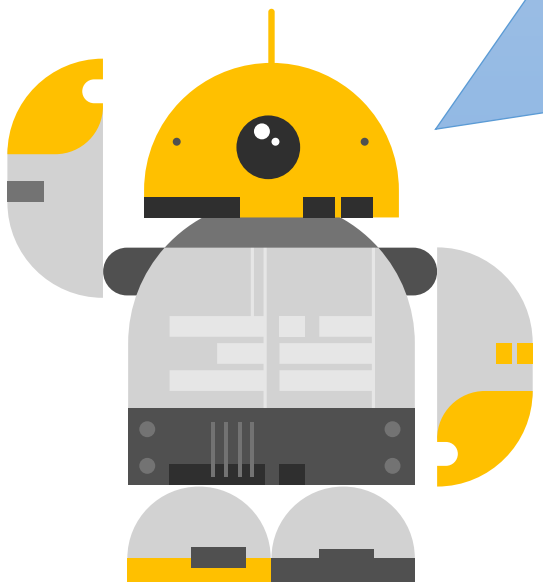


図 23 ゼロトラストセキュリティ構成要素の導入とその効果

発表内容は以上です。ご清聴ありがとうございました。



【-END-】