ゼロトラストの本質
～理想と現実のはざまで～

ゼロトラストの本質の研究　分科会
（中日本）

メンバー紹介

リーダー

笹山　晏未

Sasayama Ami

株式会社メイテツコム

メンバー

駒田　信人

Komada Nobuto

株式会社アシスト

事務局

米倉　宏樹

Yonekura Hiroki

株式会社アシスト

サブリーダー

生田　亜裕

Ikuta Ayu

アイカ工業株式会社

メンバー

中村 幸寛

Nakamura Yukihiro

ケー・イー・エルテクニカル
サービス株式会社

アジェンダ

研究のスタート

昨今のセキュリティ事故事例

従来のセキュリティ対策

セキュリティ対策のポイントを考える

ゼロトラストとは

具体的な対策方法

まとめ

研究のスタート

そういえば、、、

コロナ禍でテレワークが増え、
クラウド化の加速もあり、
最近セキュリティ事故が多いなぁ

どうやら・・・

いろいろなセキュリティ対策を
しないといけないらしい

でも、、、

セキュリティ初心者だから
よくわからないな

そこでまずは

昨今のセキュリティ事故を
調べてみた

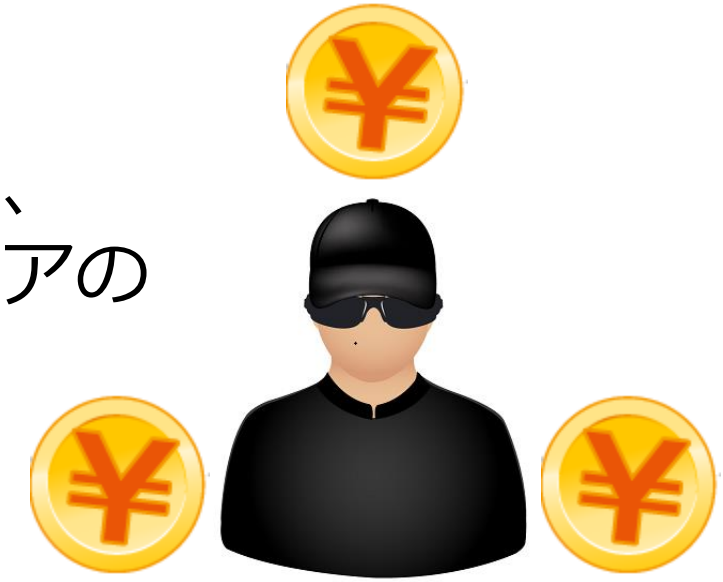
昨今のセキュリティ事故事例

ランサムウェア（マルウェア）感染

ランサムウェアとは、感染したPC上に保存している
ファイルを暗号化して使用ができない状態にし、
復旧させることと引き換えに**身代金**を要求する
マルウェアである。

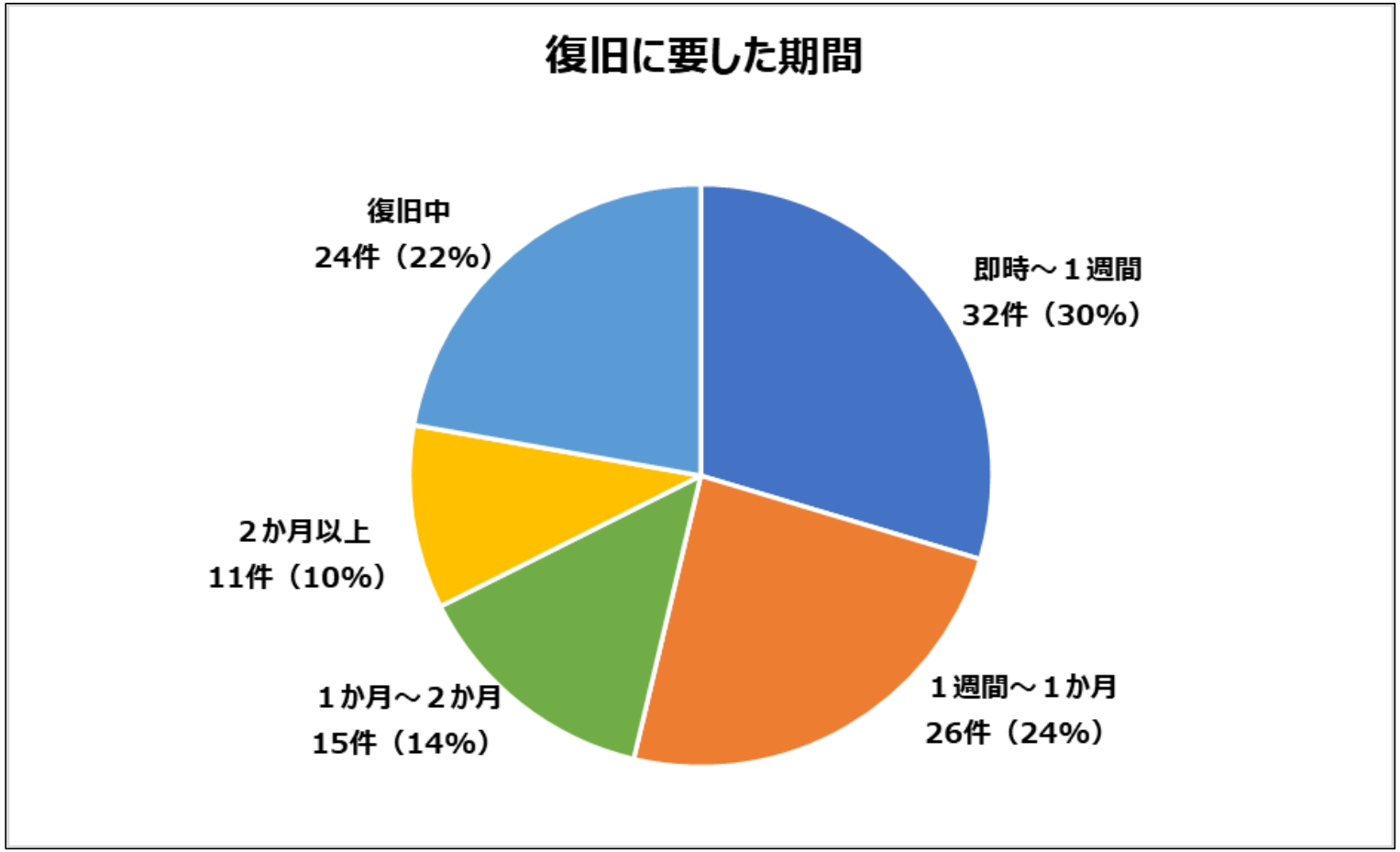
＜事例＞

愛知県の某大手自動車部品サプライヤーや、
大阪府の大規模な病院等で、ランサムウェアの
被害が相次いだ。



ランサムウェア（マルウェア）感染

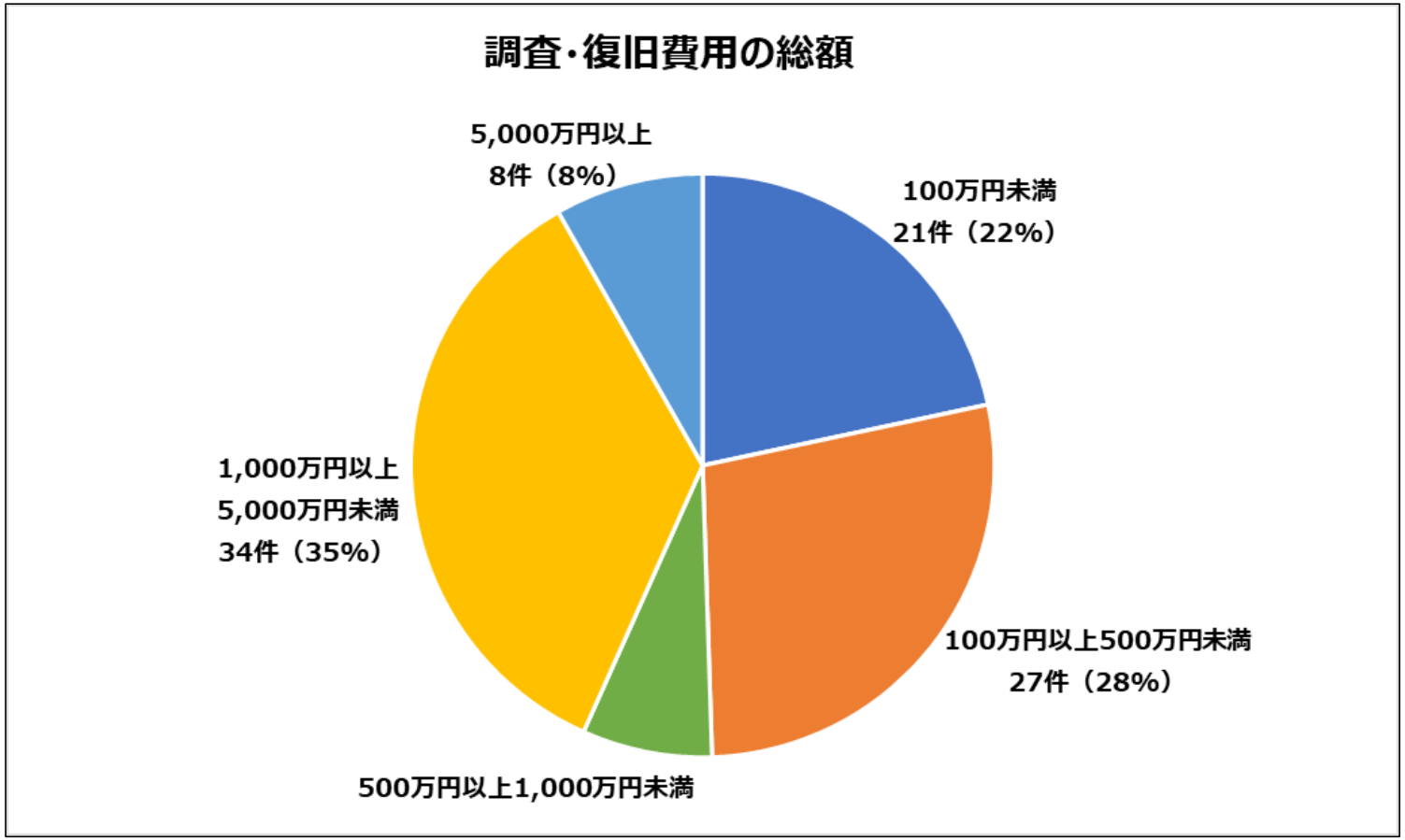
復旧には、かなりの時間を要する。



令和３年におけるサイバー空間をめぐる驚異の情勢等について（警察庁）

ランサムウェア（マルウェア）感染

復旧には、かなりの費用を要する。



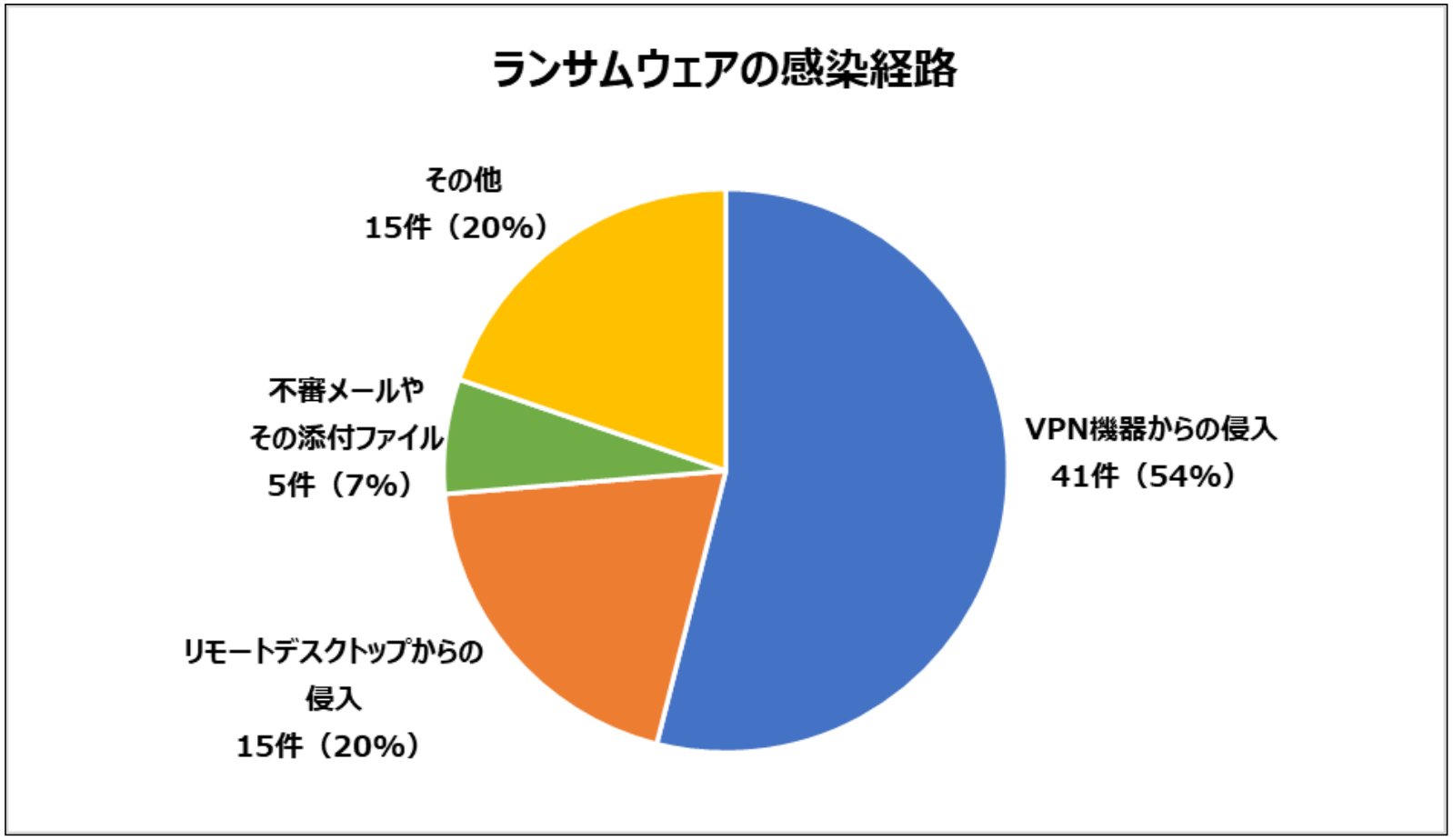
令和３年におけるサイバー空間をめぐる驚異の情勢等について（警察庁）

VPN機器の脆弱性の放置

＜事例＞

テレワーク等による外部から内部ネットワークへの接続が急増し、セキュリティ対策の一環としてＶＰＮ機器を導入する企業等が増加しているが、その**ＶＰＮ機器のぜい弱性等から**組織内部のネットワークに侵入し、ランサムウェアに感染させる手口が被害の多くを占めている。

VPN機器の脆弱性の放置



令和３年におけるサイバー空間をめぐる驚異の情勢等について（警察庁）

無線LAN利用通信の窃取

＜事例＞

ホテルの無線LANネットワークを乗っ取り、
無線LANを利用した宿泊者から情報を窃取する。

内部不正による情報漏えい

＜事例＞

令和３年１月、某大手携帯通信会社Aの元従業員が営業秘密に該当する情報を不正に持ち出していたとして逮捕された。

また、同社は、同従業員の転職先の某大手携帯通信会社Bに対して業務上利用するサーバー内に持ち出した情報が保存され、従業員に開示された。

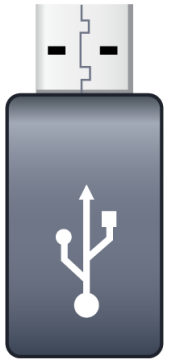
結果として、元従業員は、**懲役2年、執行猶予4年、罰金100万円の有罪判決**を受けた。

USBメモリやPCの紛失

＜事例＞

令和４年6月21日、兵庫県尼崎市にて、住民税非課税世帯等に対する情報を記録したUSBメモリーを鞄へ入れて持ち出した。

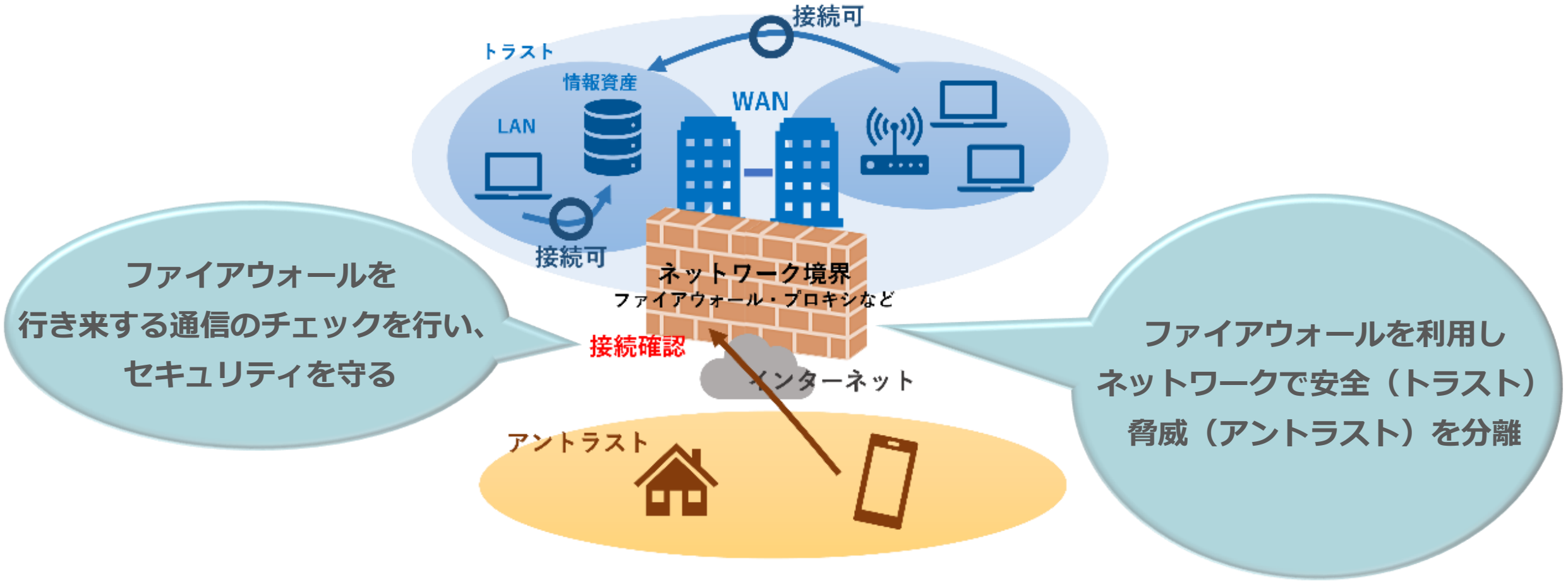
委託者の事業所外でのデータ移管作業終了後、速やかに帰社せず、当該USBメモリーを所持したまま、飲食店に立ち寄り、**食事や飲酒をし**、結果、**USBメモリーが入った鞄を紛失**した。



従来のセキュリティ対策って？

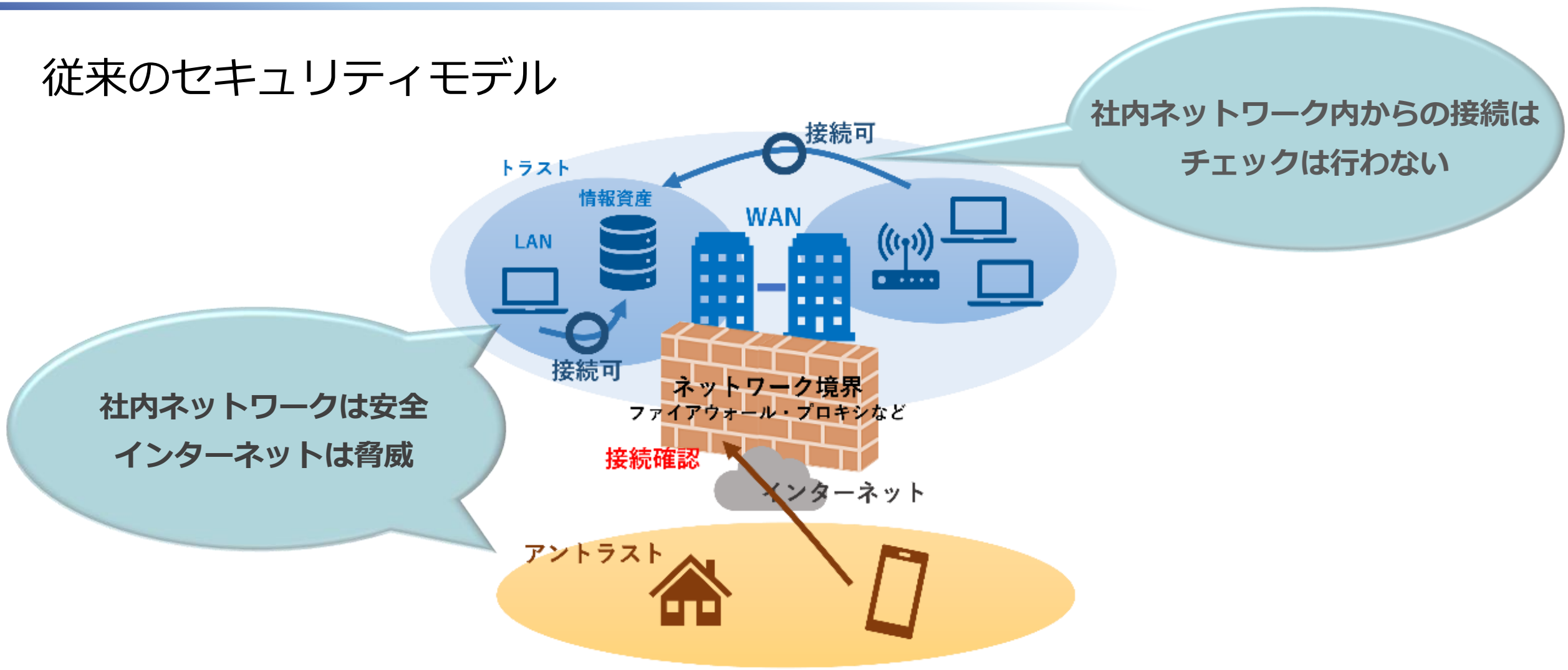
従来のセキュリティ対策

従来のセキュリティモデル「境界防衛モデル」



従来のセキュリティ対策

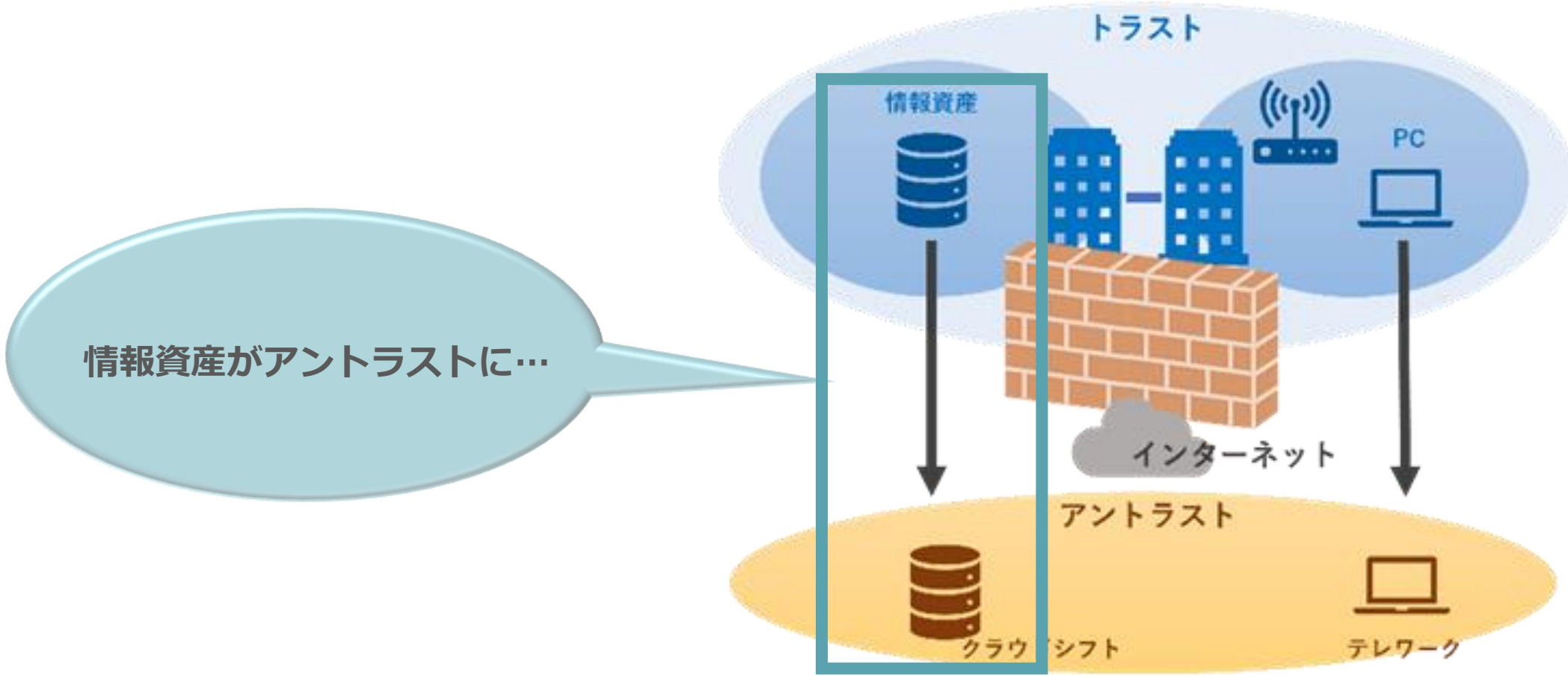
従来のセキュリティモデル



社内で起きてること

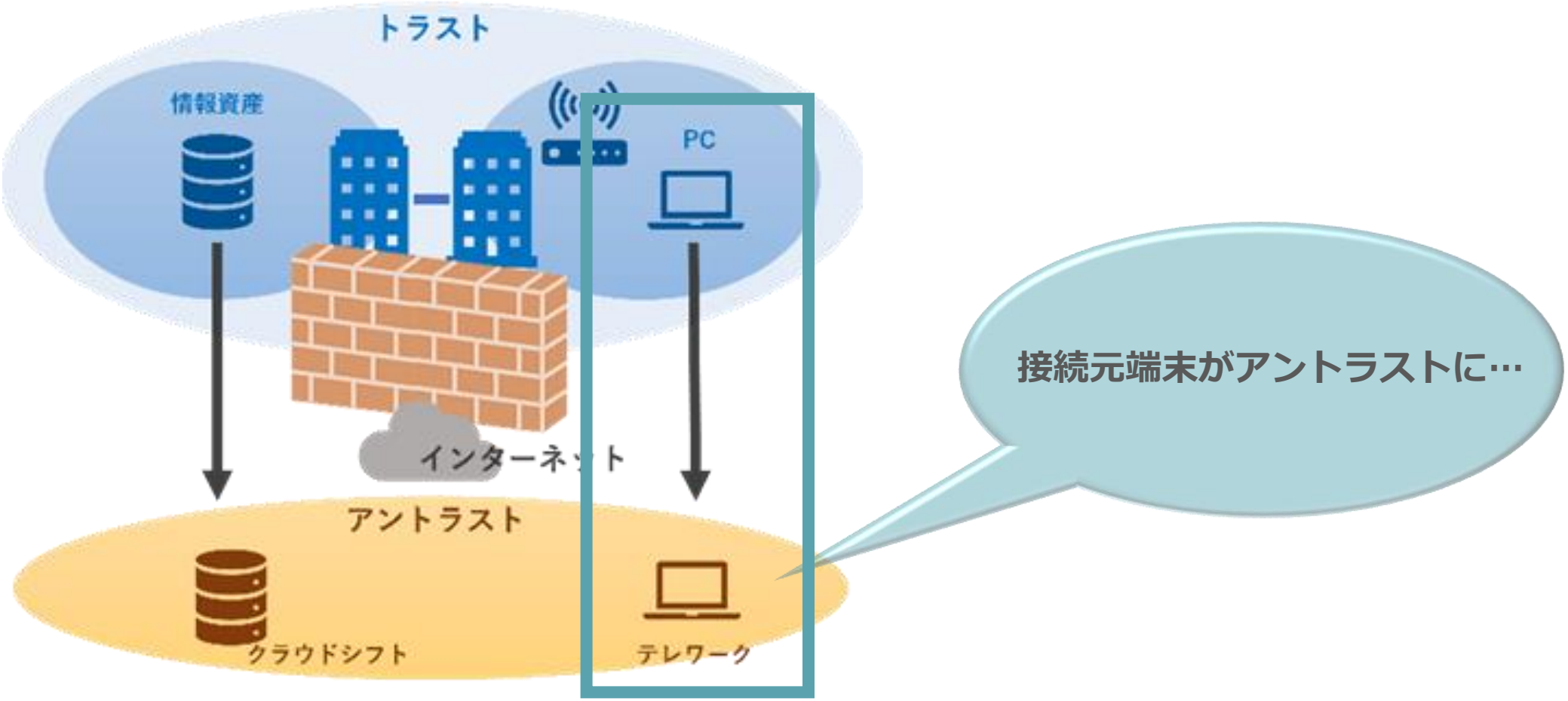
働き方の変化

業務環境のクラウド化（クラウドシフト）



働き方の変化

テレワーク



どうしよう？

今のセキュリティ対策だけでは防げないことが多くなってきた

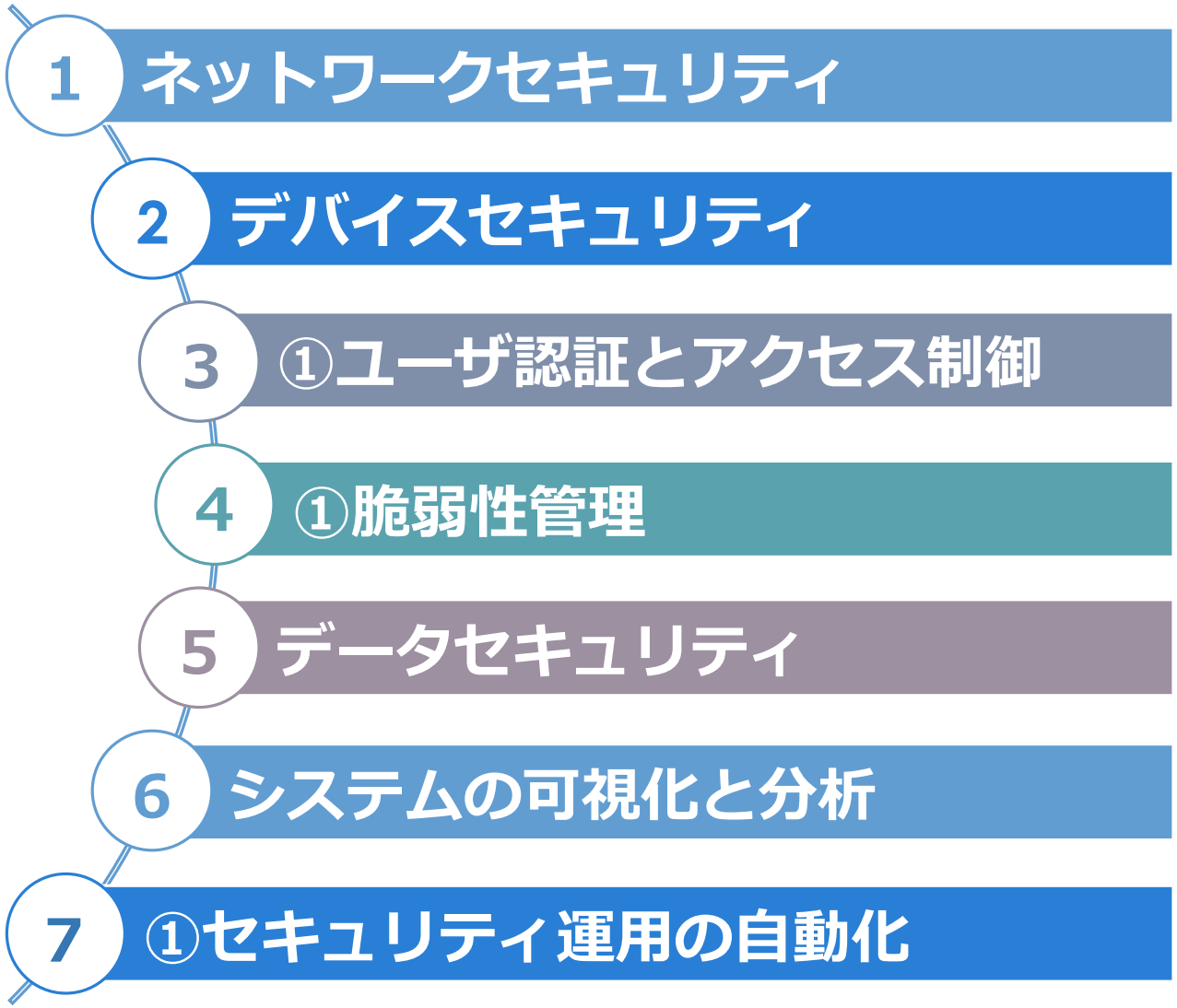
クラウド

テレワーク

守るべき境界があいまいに、、、

どのような
セキュリティ対策が必要？

セキュリティ対策ポイント考えてみた



セキュリティ対策ポイント考えてみた

1 ネットワークセキュリティ

接続元端末も、情報資産も社内ネットワーク/インターネットそれぞれのケースがある
貴重なデータを相手に盗み見られないようにするために通信の保護をする

2 デバイスセキュリティ

接続元端末は外部からの攻撃から保護し、安全な状態であることを監視する
資産管理し、どこの誰が接続元端末を所持しているか管理する

セキュリティ対策ポイント考えてみた

3 ユーザ認証とアクセス制御

・従来のポリシー（接続元端末、人、に応じたアクセス制御）を行う
「ふるまい属性」に応じてポリシーを動的に変動させる
・接続元端末が接続する毎に以下確認をし、
問題がなければアクセスの許可をあたえる
・名乗った通りの本人であることの確認
・接続元端末が企業リソースを利用する権限（ポリシー）があるのか

4 脆弱性管理

所有している機器・システムについて、
外部からの悪意あるアクセスから守るため、脆弱性がないか確認し、
把握、管理、対応する必要がある

セキュリティ対策ポイント考えてみた

5 データセキュリティ

・保有・所有している貴重なデータについて
セキュリティポリシーに基づいたアクセス制御を行い、
アクセス権のあるもののみがデータにアクセスできるようにする
・また、許可されていない情報の持ち出しを検知することで
情報の漏洩を防ぐ

6 システムの可視化と分析

・デバイスが安全な状態であることを確認・監視
・動的ポリシーを適用するため、ネットワークトラフィック
アクセス要求を継続的にモニタリングを行う

セキュリティ対策ポイント考えてみた

7 セキュリティ運用の自動化

①～⑥のセキュリティ対策と連携、分析し、

インシデント発生を予測

自動対処することで**インシデントの発生を未然に防ぐ**

そういえば、、、

ゼロトラストって最近よく聞くなぁ
なんだろう

ゼロトラストとは

ゼロトラストって何だろう

ゼロトラストとは
セキュリティの概念らしい！

ゼロトラストとは

性悪説のセキュリティモデル

ゼロトラストとは

守るべき**情報資源**への接続を

どこからの接続であっても

接続確認チェックする

ゼロトラストの必要性

接続元端末も、企業リソースも…

ネットワークの**安全領域の外**へ

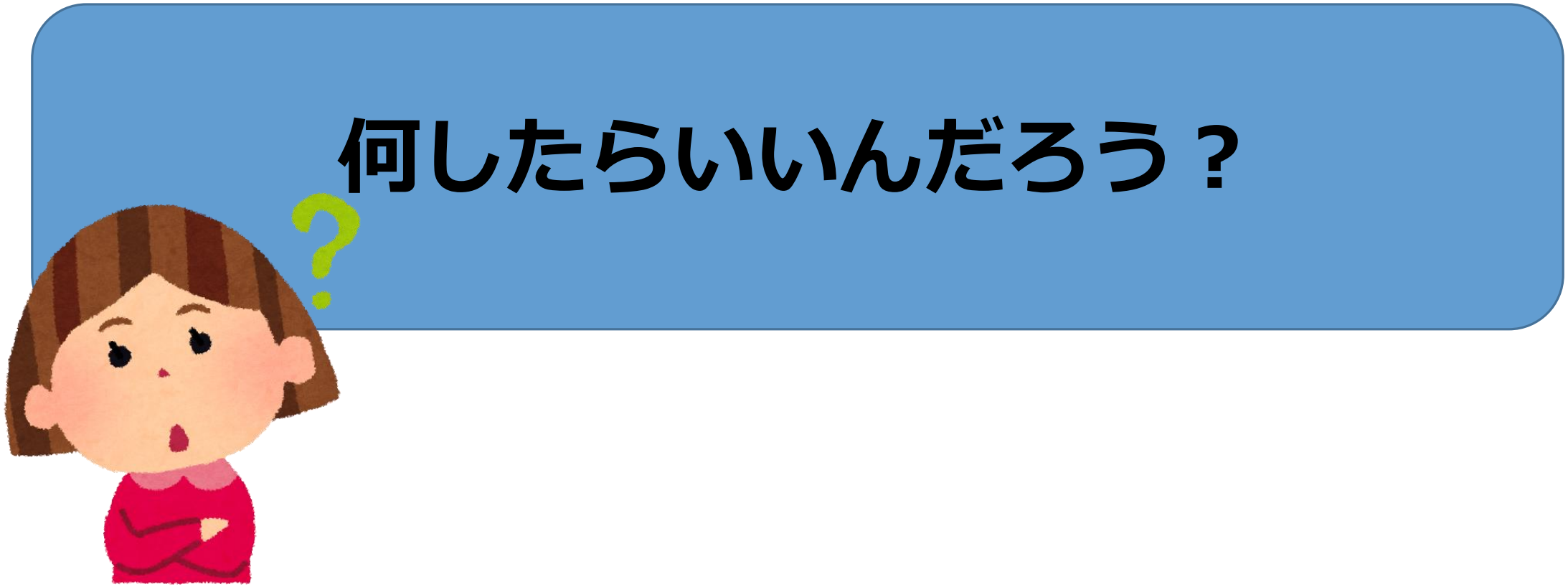
ゼロトラストの必要性

守るべき**情報資源**への接続を
どこからの接続であっても
接続確認チェックする**ゼロトラスト**は

今のセキュリティの考えに
適している！！

ゼロトラストの原則

ゼロトラストって…



ゼロトラストの原則

NIST（米国国立標準技術研究所）
2020年8月発行　Special Publication(SP) 800-207

No.	ゼロトラストの原則
1	すべてのデータソースとコンピューティングサービスをリソースとみなす。
2	ネットワークのロケーションにかかわらず、すべての通信を保護する。
3	企業リソースへのアクセスをセッションごとに許可する。
4	リソースへのアクセスは、クライアントアイデンティティ、アプリケーション/サービス、リクエストする資産の状態、その他の行動属性や環境属性を含めた動的ポリシーにより決定する。
5	すべての資産の整合性とセキュリティ動作を監視し、測定する。
6	すべてのリソースの認証と認可を動的に行い、アクセスが許可される前に厳格に実施する。
7	資産、ネットワークインフラストラクチャ、通信の現状について可能な限り多くの情報を収集し、セキュリティ態勢の改善に利用する。

ゼロトラストの原則

NIST（米国国立標準技術研究所）
2020年8月発行　Special Publication(SP) 800-207

No.	ゼロトラストの原則
1	すべてのデータソースとコンピューティングサービスをリソースとみなす。
2	ネットワークのロケーションにかかわらず、すべての通信を保護する。
3	企業リソースへのアクセスをセッションごとに許可する。
4	リソースへのアクセスは、クライアントアイデンティティ、アプリケーション/サービス、リクエストする資産の状態、その他 境属性を含めた動的ポリシーにより決定する。
5	すべての資産の整合性とセキュリティ動作を監視し、測定する。
6	すべてのリソースの認証と認可を動的に行い、アクセスが許可される前に厳格に実施する。
7	資産、ネットワークインフラストラクチャ、通信の現状について可能な限り多くの情報を収集し、セキュリティ態勢の改善に利用する。

ゼロトラストの原則

ゼロトラストの原則に
我々が考えたセキュリティ対策ポイントを
あてはめてみよう

ゼロトラストの原則

NIST（米国国立標準技術研究所）
2020年8月発行　Special Publication(SP) 800-207

No.	ゼロトラストの原則	
1	すべてのデータソースとコンピューティングサービスをリソースとみなす。	デバイスセキュリティ　データセキュリティ
2	ネットワークのロケーションにかかわらず、すべての通信を保護する。	ネットワークセキュリティ
3	企業リソースへのアクセスをセッションごとに許可する。	ユーザ認証とアクセス制御
4	リソースへのアクセスは、クライアントアイデンティティ、アプリケーション/サービス、リクエストする資産の状態、その他の行動属性や環境属性を含めた動的ポリシーにより決定する。	ユーザ認証とアクセス制御
5	すべての資産の整合性とセキュリティ動作を監視し、測定する。	システムの可視化と分析　脆弱性管理
6	すべてのリソースの認証と認可を動的に行い、アクセスが許可される前に厳格に実施する。	ユーザ認証とアクセス制御
7	資産、ネットワークインフラストラクチャ、通信の現状について可能な限り多くの情報を収集し、セキュリティ態勢の改善に利用する。	セキュリティ運用の自動化

具体的な対策は？

セキュリティ対策ポイントに対する具体的な対策

①ネットワークセキュリティ

・SWG ・SDP

・インターネット分離

②デバイスセキュリティ

・EPP ・EDR

・MDM ・IT資産管理

③ユーザ認証とアクセス制御

・多要素認証

・シングルサインオン

・特権ID管理 ・統合ID管理

④脆弱性管理

・CSPM

・脆弱性管理

⑤データセキュリティ

・DLP

・ファイルアクセス制御

・システムバックアップ

⑥システムの可視化と分析

・CASB

・統合ログ管理

・SIEM

⑦セキュリティ運用の自動化

・SOAR

それぞれどのような機能？

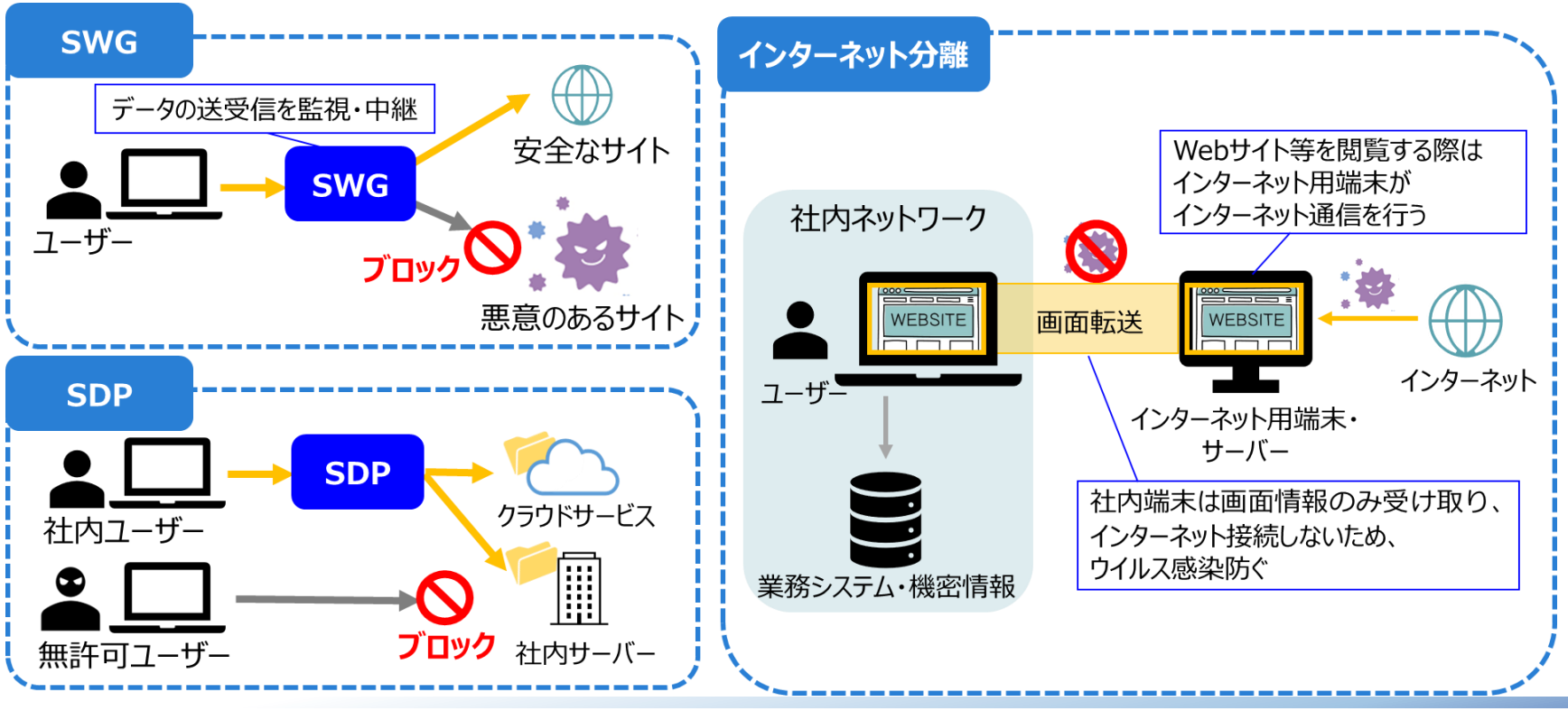
①ネットワークセキュリティ

SWG　SDP　インターネット分離

SWG：インターネット通信をチェック・安全でないサイトへのアクセスを遮断

SDP：システムの間通信を制御、認証された場合に通信経路を確立

インターネット分離：インターネット接続した仮想ブラウザから業務端末に画面情報のみを転送



②デバイスセキュリティ

EPP　EDR

EPP：組織内に侵入したマルウェアを検知し、自動的に駆除

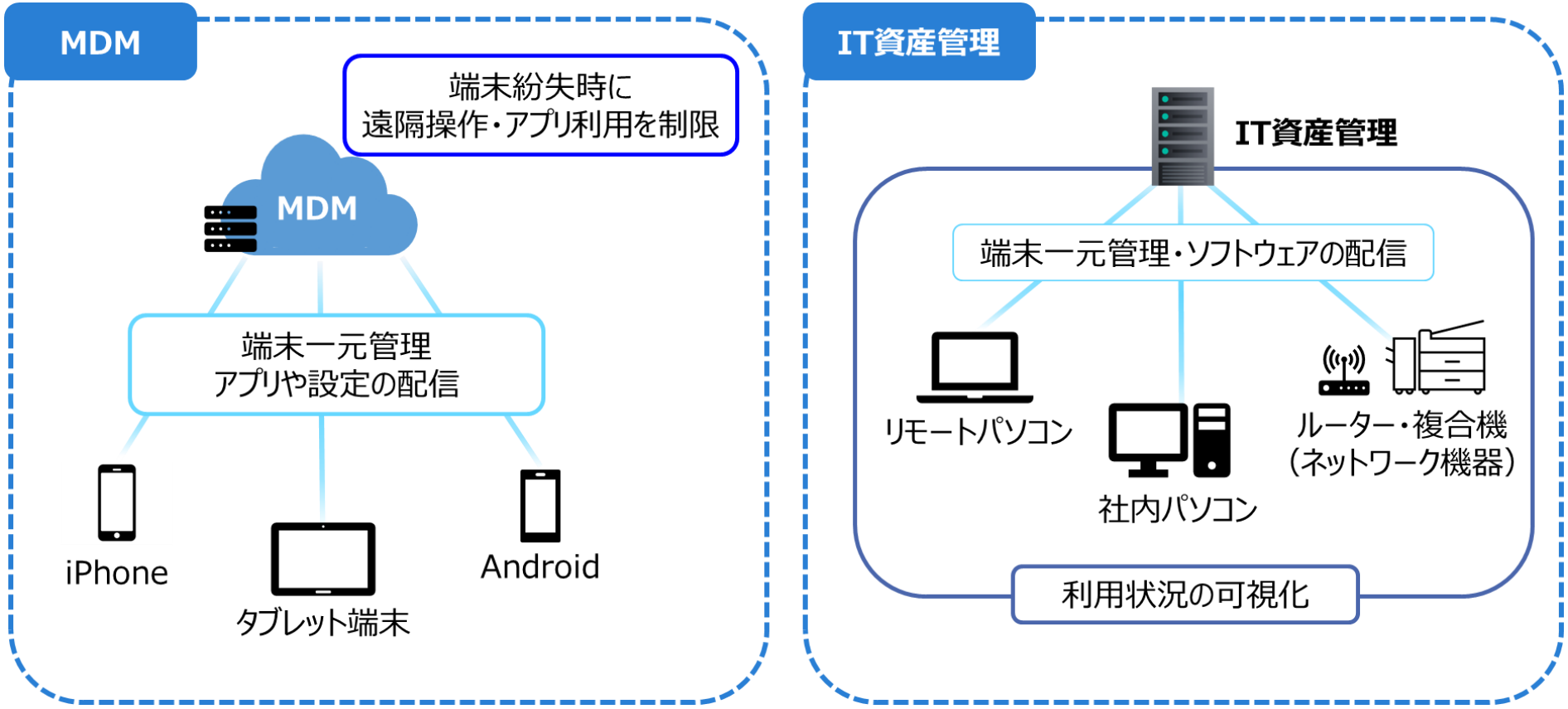
EDR：不審な動きを常時監視・被害を迅速に可視化

②デバイスセキュリティ

MDM　IT資産管理

MDM：複数のモバイル端末を、企業で統一したポリシー下で管理

IT資産管理：企業におけるIT資産の保有状況・利用状況を可視化

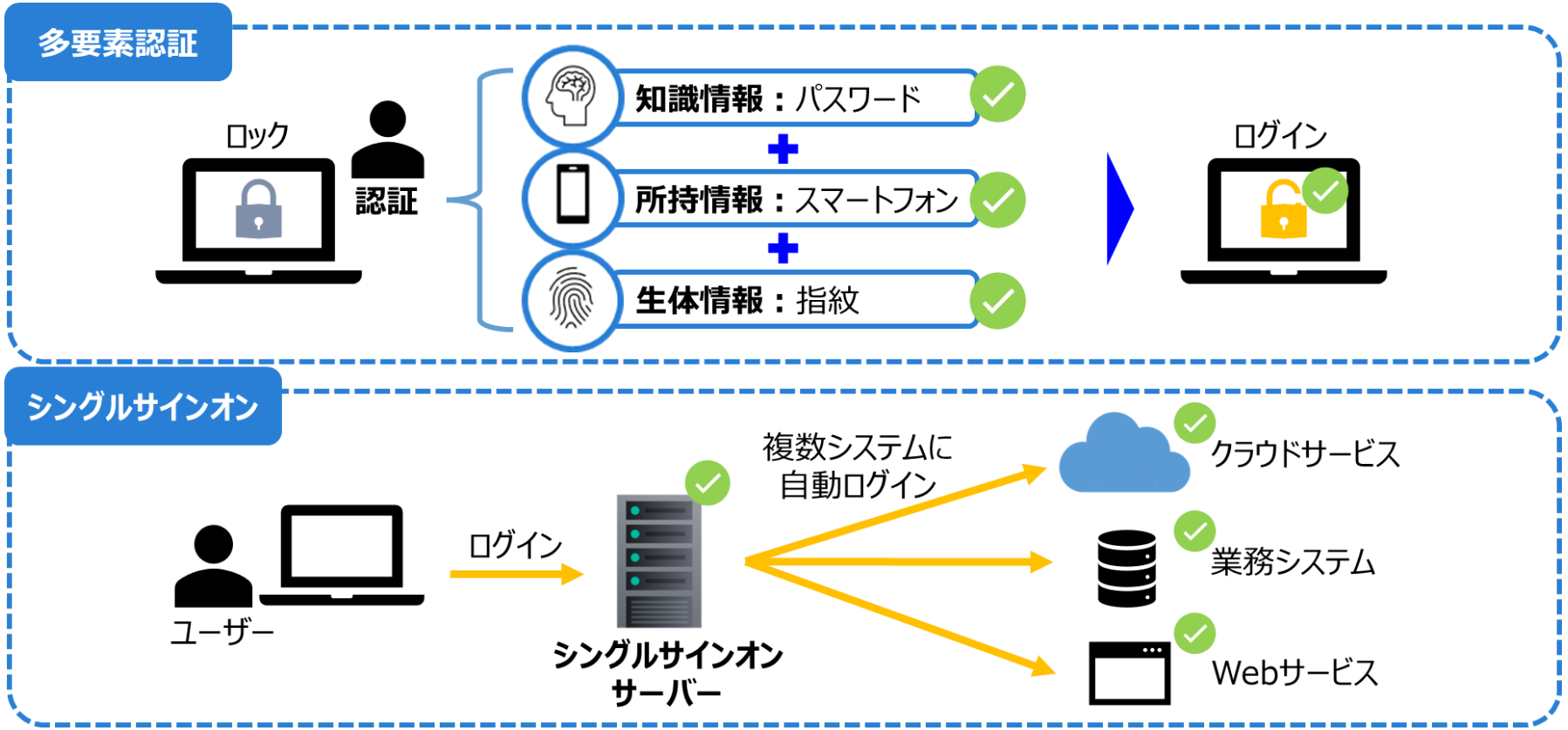


③ユーザ認証とアクセス制御

多要素認証　シングルサインオン

多要素認証：IDとパスワードの他に、所持情報や生体認証と組み合わせて認証

シングルサインオン：一度のユーザ認証処理により複数システム上で
パスワードを入力することなくログインさせる

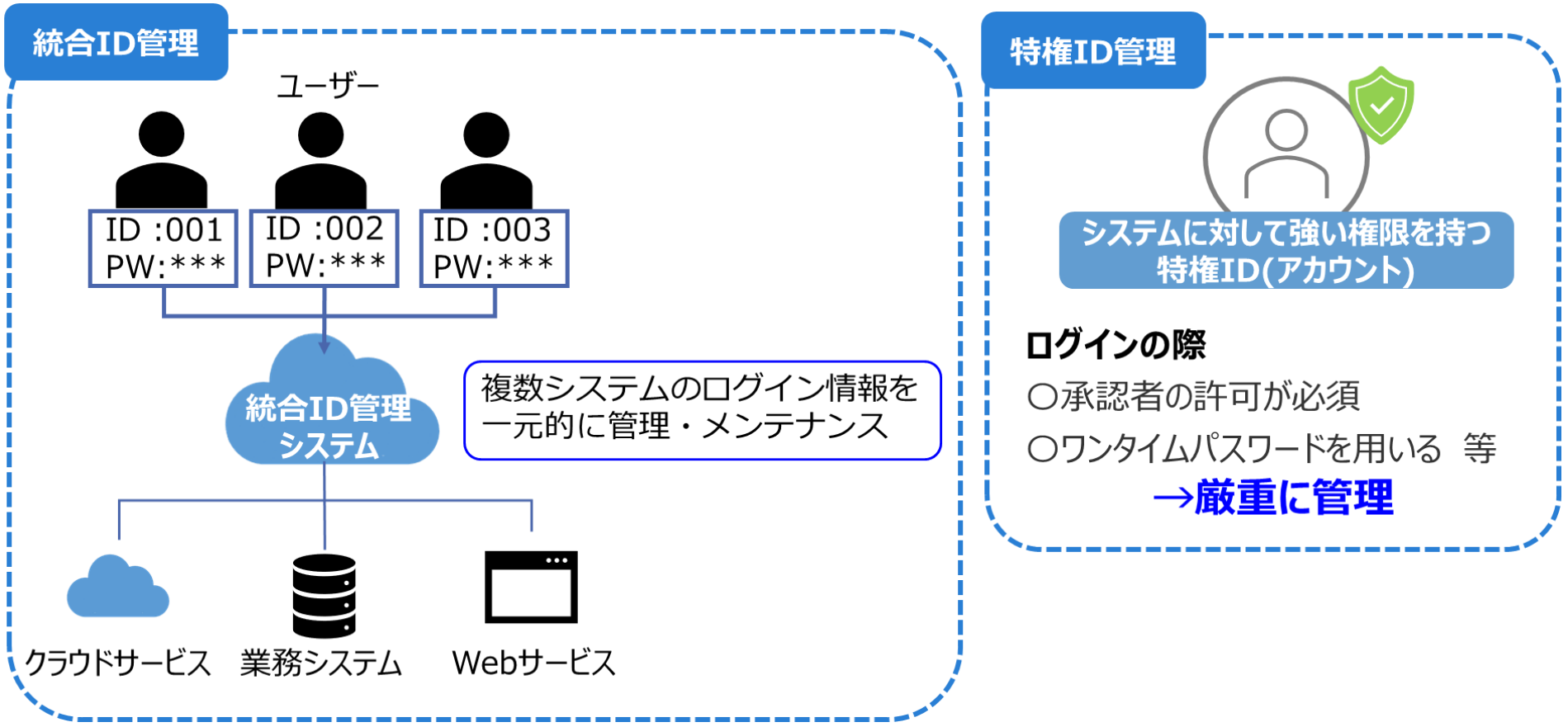


③ユーザ認証とアクセス制御

特権ID管理　統合ID管理

統合ID管理：複数システムのユーザーIDを一元的に管理・メンテナンス

特権ID管理：強い権限を持っているユーザのログインを厳重に管理

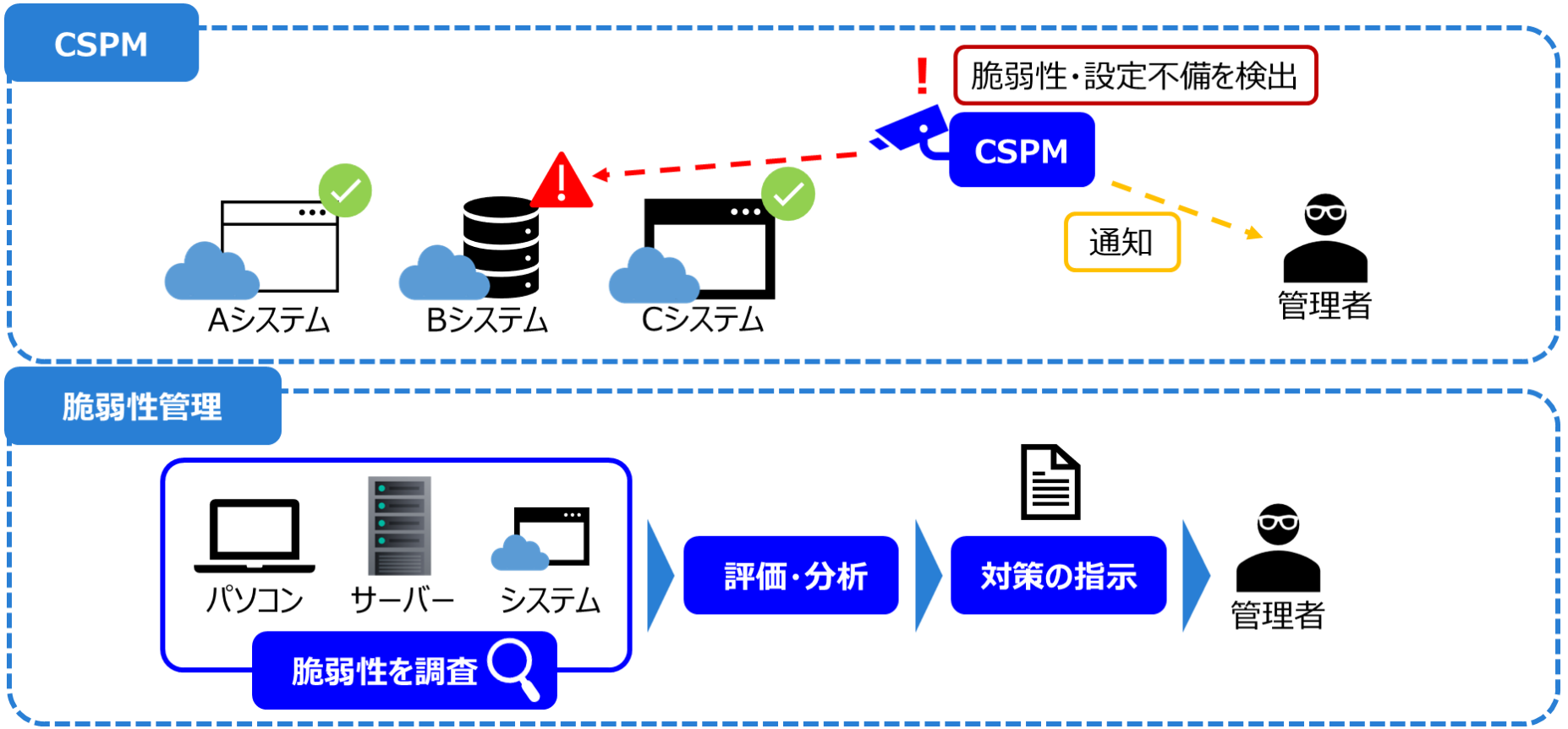


④脆弱性管理

CSPM　脆弱性管理

CSPM：システムやサービスのセキュリティ設定を監査

脆弱性管理：組織内のセキュリティ脆弱性を特定、評価、処理、報告



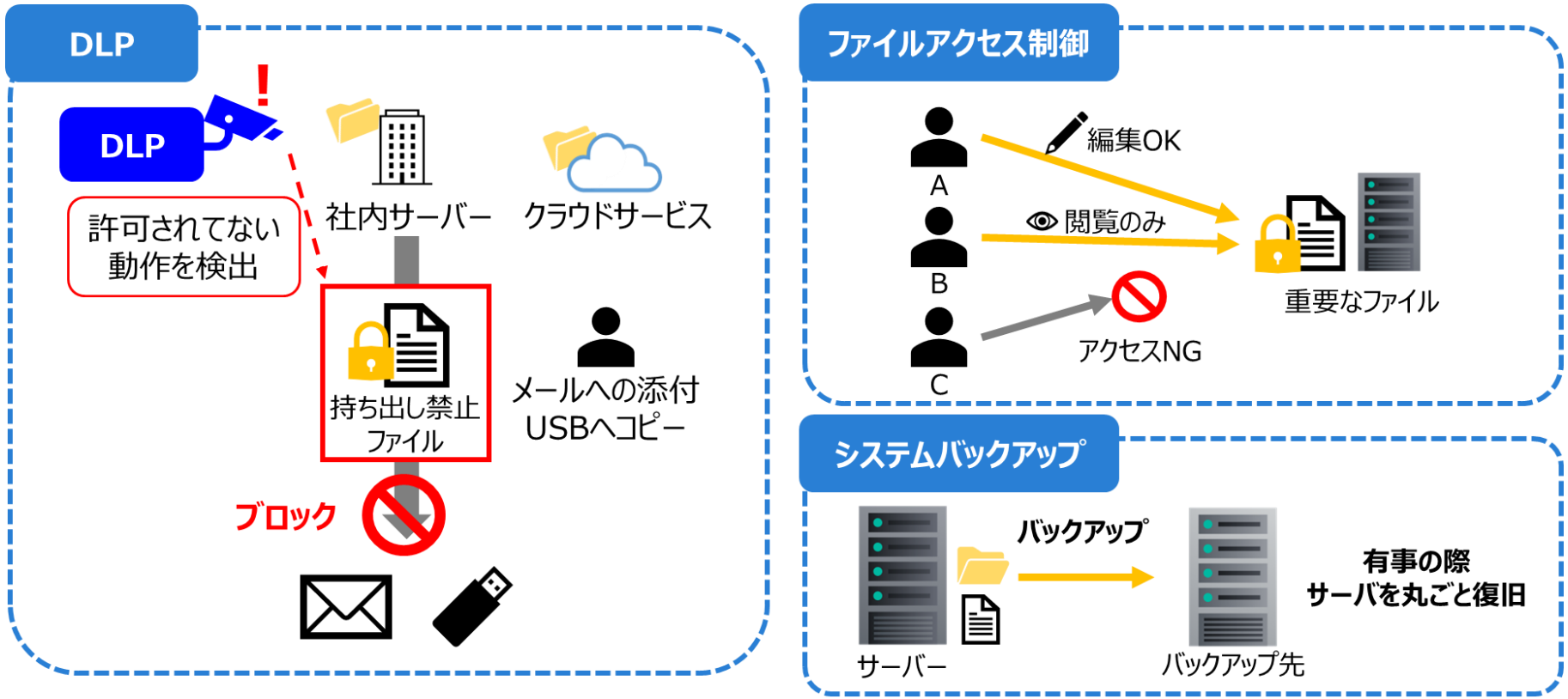
⑤データセキュリティ

DLP　ファイルアクセス制御　システムバックアップ

DLP：データの監視・不正な動作をブロック

ファイルアクセス制御：権限分掌によりデータを保護

システムバックアップ：データをバックアップし、有事の際に備える

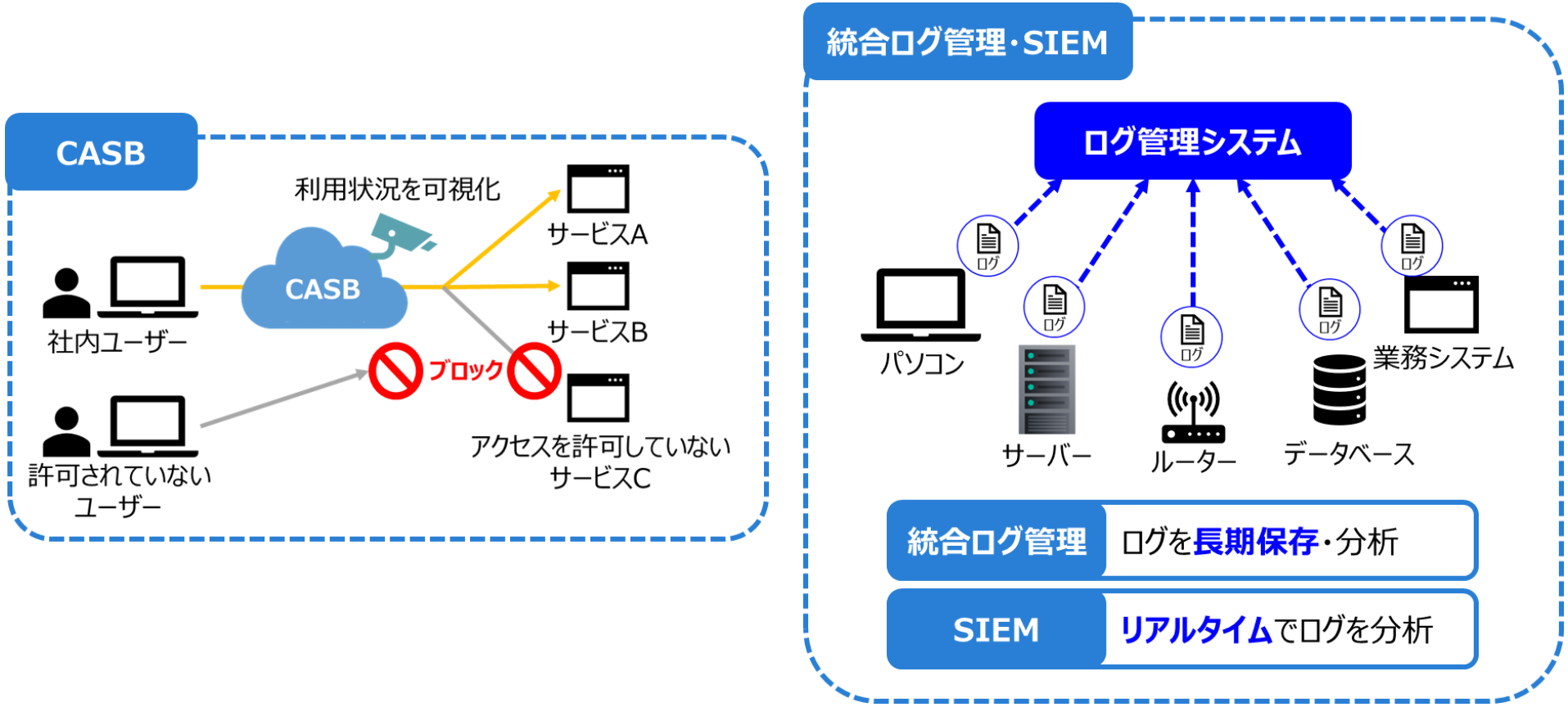


⑥システムの可視化と分析

CASB　統合ログ管理　SIEM

CASB：クラウドサービスの利用状況を可視化･制御

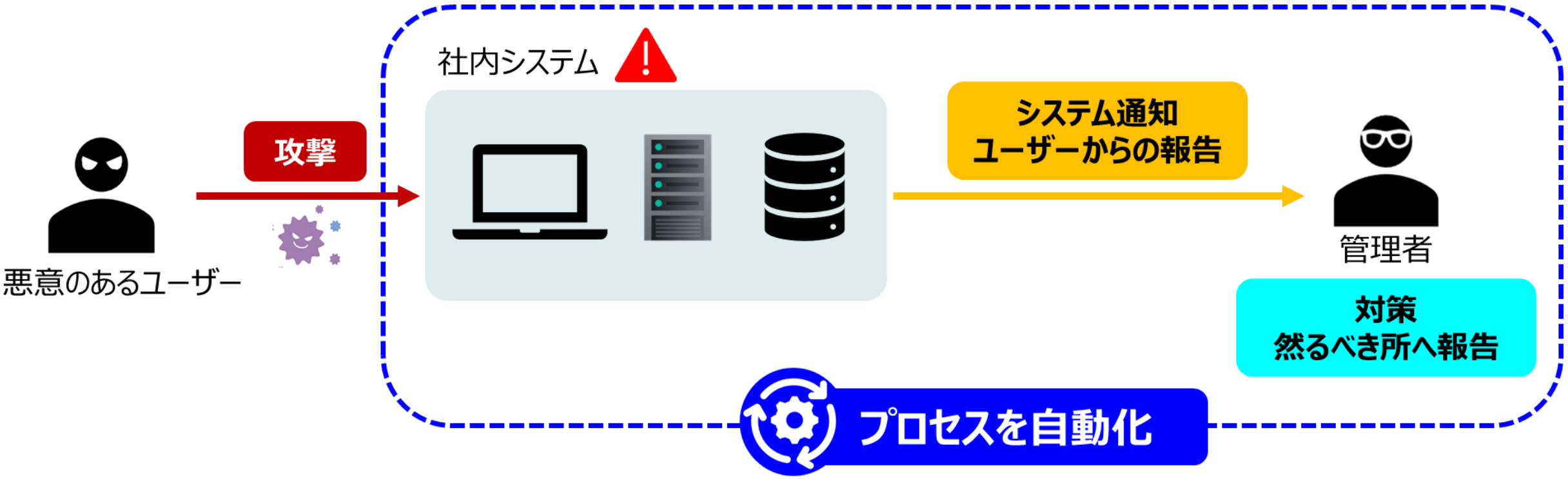
統合ログ管理･SIEM：複数システムのログを一元管理・分析



⑦セキュリティ運用の自動化

SOAR

SOAR：インシデントの発生から処理までの流れを自動化



ソリューション入れるだけで？いいんだろうか？

ソリューション以外の方法（システム管理者）

- システム操作ログの監視。また、**監視していることを従業員に周知**することで不正を予防する
- 紛失した場合の影響度について、従業員に**教育・啓発**を定期的に行う
- VPN機器やリモートデスクトップアプリケーション等について、**最新のアップデートやパッチ適用**を定期的に行う
- ユーザに付与する**アクセス権限は最低限の権限**とする
- **特権ユーザを管理し**、異動者・退職者があった場合速やかに対応すること

ソリューション以外の方法（従業員）

- 不審なメールを受信したときは、**添付ファイルは開かず、リンク先もクリックせず**、システム管理者へ速やかに報告すること
- ウイルス感染を検知した場合は**PCをLANから速やかに切断**すること
- ホテルや喫茶店などの**公衆Wi-Fiは利用せず**、自宅以外の場所からテレワークをしない
- 会社のパスワードポリシーに沿った、**複雑なパスワードを設定**すること
- パスワードを使い回さず、**システム毎に異なるパスワード**を設定すること

会社としてのセキュリティルール

- パスワードルール
- PC持ち出しルール
- 個人所有PCを使わない
- USB等、外部記憶媒体の利用ルール
- テレワーク時のルール

こまったときのIPA(※回し者ではありません)

IPA Better Life with IT

第6期中核人材育成プログラム（令和4年7月開講）
カリキュラムご案内資料

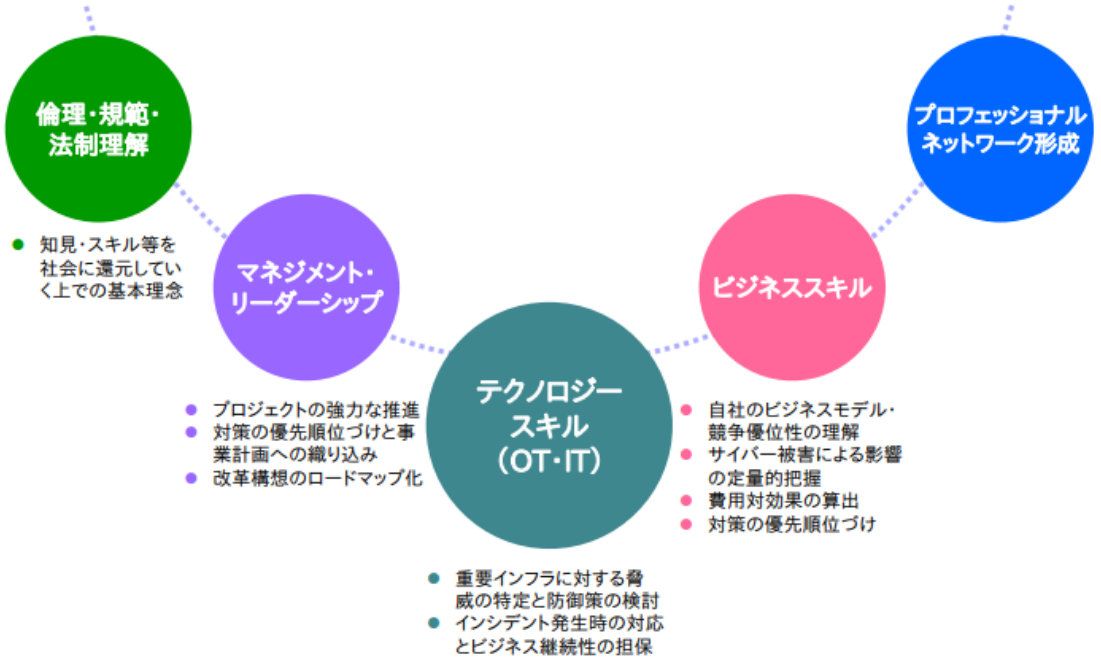
独立行政法人情報処理推進機構（IPA）

サイバーセキュリティ人材の定義もされている

育成する産業サイバーセキュリティ人材

IPA

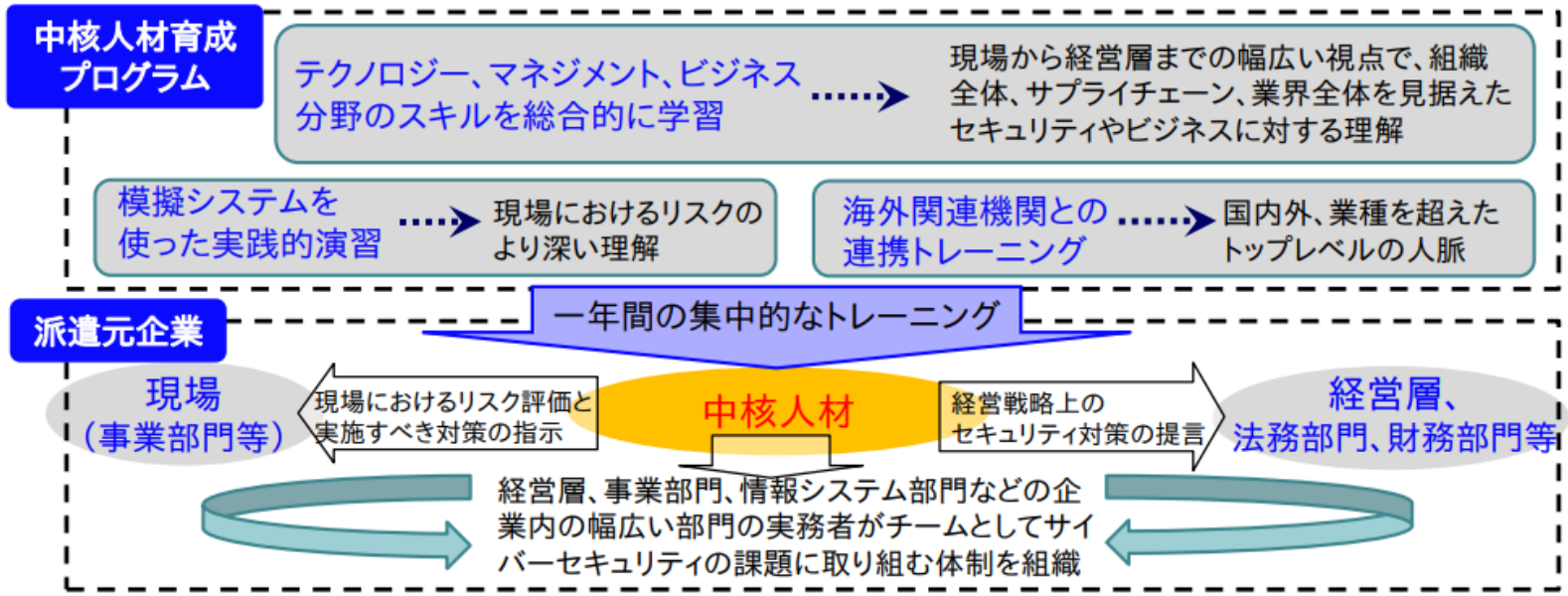
- OT（制御技術）とIT（情報技術）双方にわたる技術的なスキルを核として有し、リーダーシップなどの業務推進能力、セキュリティ専門家などとの人脈も有する、組織全体のサイバーセキュリティ対策の中核となる人材



概要

概要

- 将来、企業などの経営層と現場担当者を繋ぐ**中核人材**を担う方を対象
- テクノロジー（OT・IT）、マネジメント、ビジネス分野を総合的に学ぶ1 年程度のトレーニング
- 開始当初3ヶ月の初歩的なレベル合わせからハイレベルな卒業プロジェクトまで実施
- 受講者が自社に近い環境での演習を体験できるよう、各業界のシステムを想定した模擬システムを使用
- 海外のトップレベルのセキュリティ対策のノウハウの獲得等を目的に、海外関連機関との連携トレーニングを実施



参考としたサイト

- IPAのページに中核人財の定義だけではなく、有償無償のコンテンツがありました。

https://www.ipa.go.jp/security/index.html

まとめ

まとめ

- コロナ禍でテレワークが増え、クラウド化の加速もあり、
  最近セキュリティ事故が増加してきた

- ゼロトラストとは昔からある概念だが、**昨今の働き方にも適した**
  外部も内部も区別なく疑ってかかる**性悪説**のセキュリティモデル

- セキュリティ対策として以下が有効
  - ゼロトラストに則した**製品の導入**
  - 会社としての**セキュリティルール**を設定
  - **教育・啓発**を実施して**セキュリティリテラシーを向上**

ご清聴
ありがとうございました。