Japan Information Security
Management Systems User Group

テーマ１
ISMSとゼロトラストセキュリティについての考察

JNSA 標準化部会
日本ISMSユーザグループ　リーダー
インプリメンテーション研究会　主査

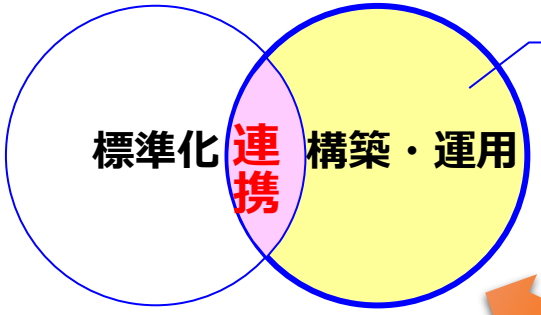
2021年12月17日

魚脇　雅晴

日本ISMSユーザグループの活動紹介　2021年

ISMSの普及・促進

貢献



インプリメンテーション研究会

ISMSの構築・運用におけるベストプラクティクスを検討＆提供

ISOのアドホック会議にリエゾンとして参加

利用するユーザーの意見を反映した規格になるように、27000シリーズの規格作成及び改正に関する討議に参加し、ユーザG代表として意見を述べている。

■27002の改正に関する討議と27001の改正（付属書Aの差し替え等）及び27017の改定に関する討議に参加

ベストプラクティクスを検討＆提供

事例研究として2021年は下記のテーマ深掘り

■ISMSとゼロトラストセキュリティについての考察

標準化されたものをどのようにビジネスの世界に反映＆定着させるか・・・

本テーマを選定した理由

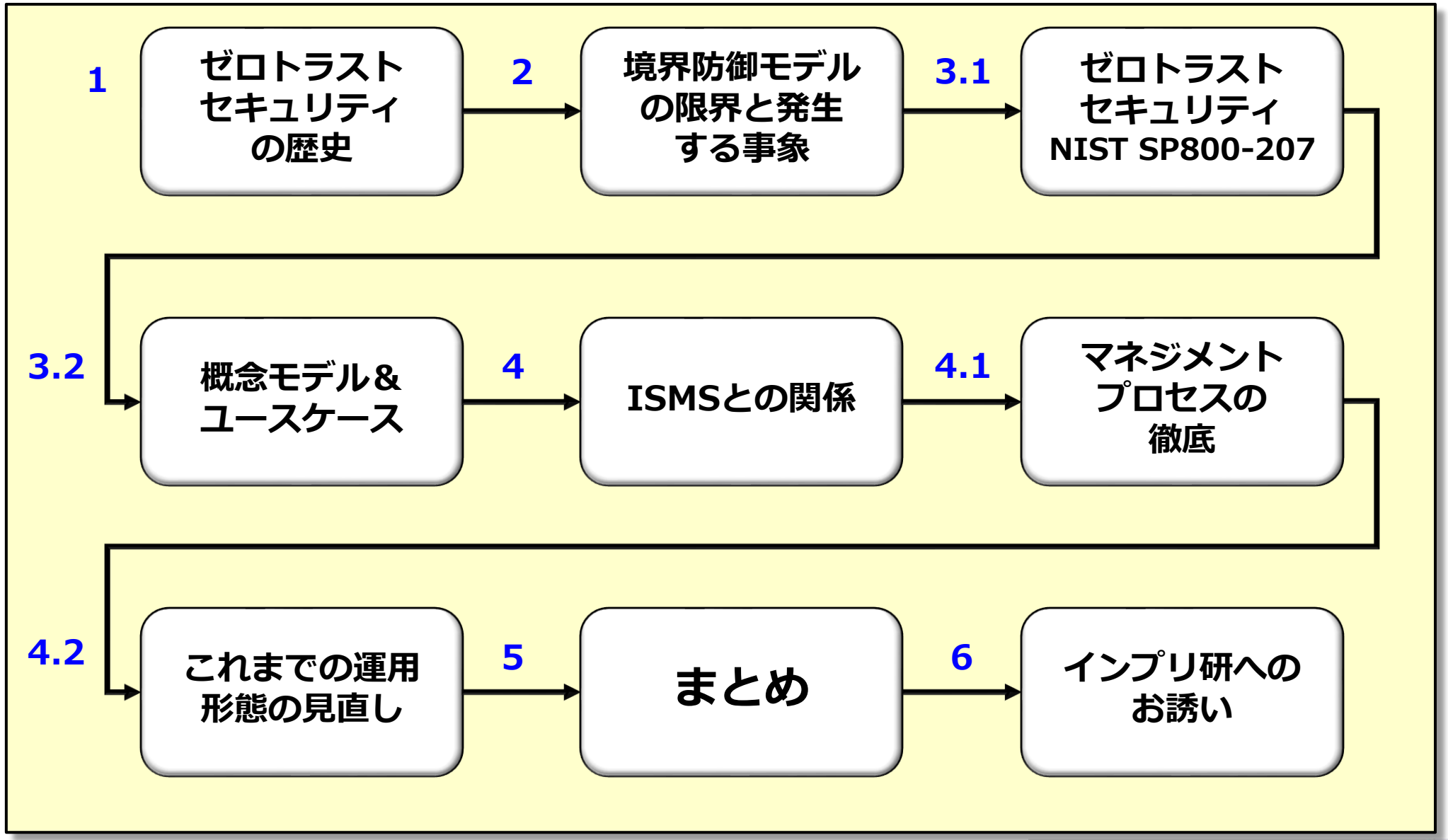
組織を取り巻く環境はクラウドファースト時代（機密情報の社外保管の急増）、サイバー攻撃の多発＆多様化、コロナ禍におけるテレワーク増大といったように大きく変化しています。

そういう背景のなかで今年の検討テーマを選定時には漠然とサイバーセキュリティ関連の話とテレワークを中心にディスカションしていたが、話の中に巷のトレンドキーワード「ゼロトラストセキュリティ」がキーワードとして度々出てくるようになった。メンバーの関心事もゼロトラストセキュリティだが、本質について分かるようで分からない・・・

そこで、

「ゼロトラストセキュリティ」という呪文のようなキーワードではなく、理解出来る内容にブレークダウンすることでゼロトラストの本質を見つめなおすと共にどのように取り込んでいけばよいかについてISMSの視点で整理することしました。

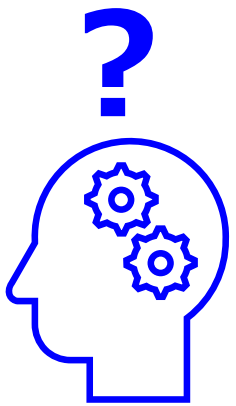
本日の説明の流れ



1. ゼロトラストセキュリティの歴史

ゼロトラスト！ゼロトラスト！

と叫ばれているが、新しい概念？



組織を取り巻く内外の環境の変化とゼロトラスト

2004年　2010年　2017年　2020年　2021年

昔からあるゼロトラストの概念

2004年
Jericho Forum（ジェリコ・フォーラム）
を正式に設立「非境界化」問題の解決に
注力する議論が開始

2010年
Forrester Research, Inc のJohn Kindervag
（ジョンキンダーバーグ）氏よりインフラから
信頼を取り除くことを前提とした考え方である
「ゼロトラスト」というコンセプトが提唱

People, Workloads, Data, の主要軸を追加し、
自動化&オーケストレーション と 可視化&分析
を構成要素全体に関連付けチェース・カニンガム
博士により Zero Trust eXtended (ZTX) とし
て再定義

ゼロトラストというキーワードが頻繁に叫ばれている背景・・・

組織を取り巻く環境の変化

・クラウドファースト時代
（機密情報の社外保管急増）
→SaaS利用の拡大でさらに加速
・サイバー攻撃の多発＆多様化
・コロナ禍におけるテレワーク増大
・内部不正
・DXの加速＆普及

ニーズの高まり

ゼロトラスト対応の
セキュリティプロダクト
相次ぐ発表

技術の追随

NISTのゼロトラストアーキテクチャー
(SP 800-207)

NIST SP 800-207
https://csrc.nist.gov/publications/detail/sp/800-207/final

https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/zero-trust-architecture-jp.html

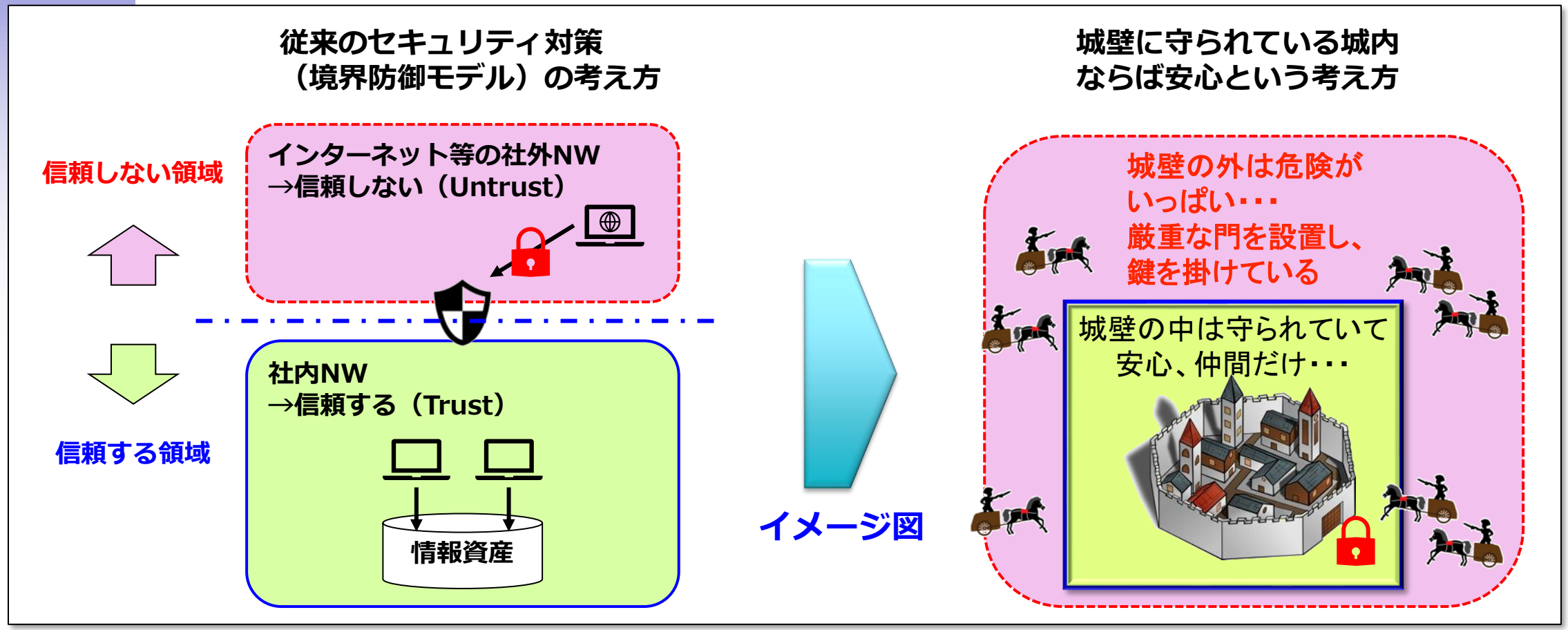
2 境界防御モデルの限界

（イラストで見るゼロトラストが
必要となる背景・・・）

従来のセキュリティ対策（境界防御モデル）

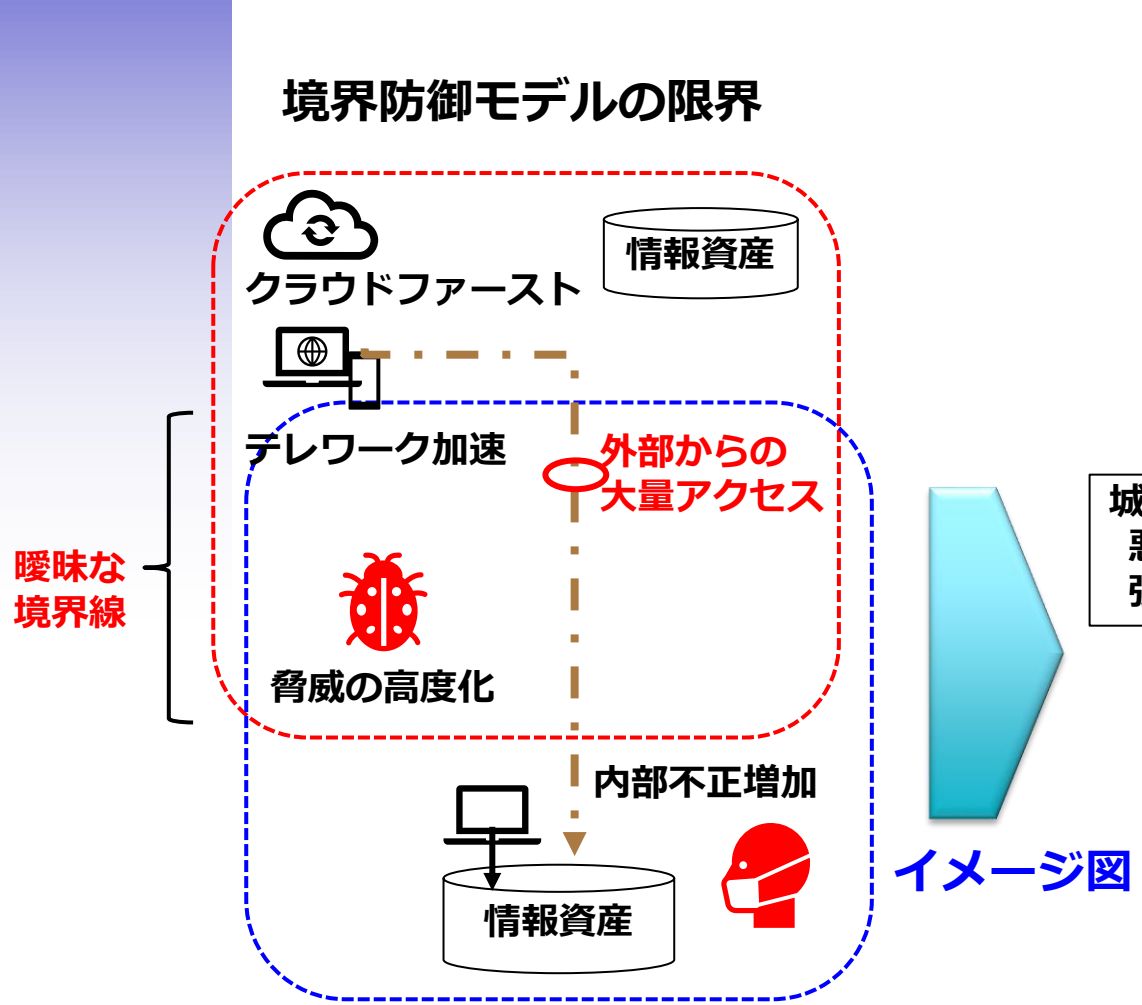
従来のセキュリティ対策（境界防御モデル）

→ 信頼できる「内側」と信頼できない「外側」にネットワークを分け、その境界線で対策を講じる

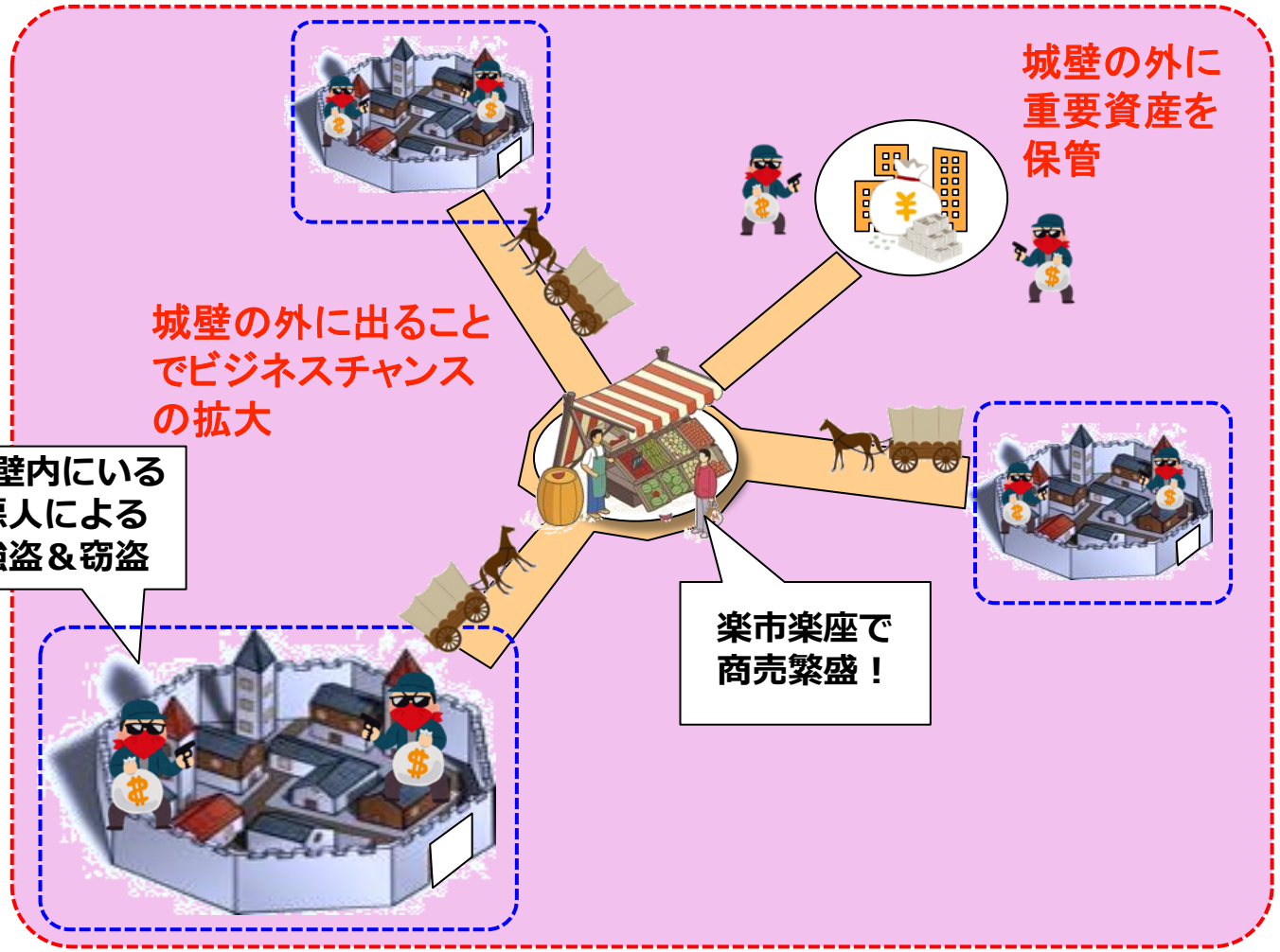


境界防御モデルの限界

→ 信頼できる「内側」と信頼できない「外側」の線引きが曖昧となり**境界防御の前提条件が崩れた・・・**

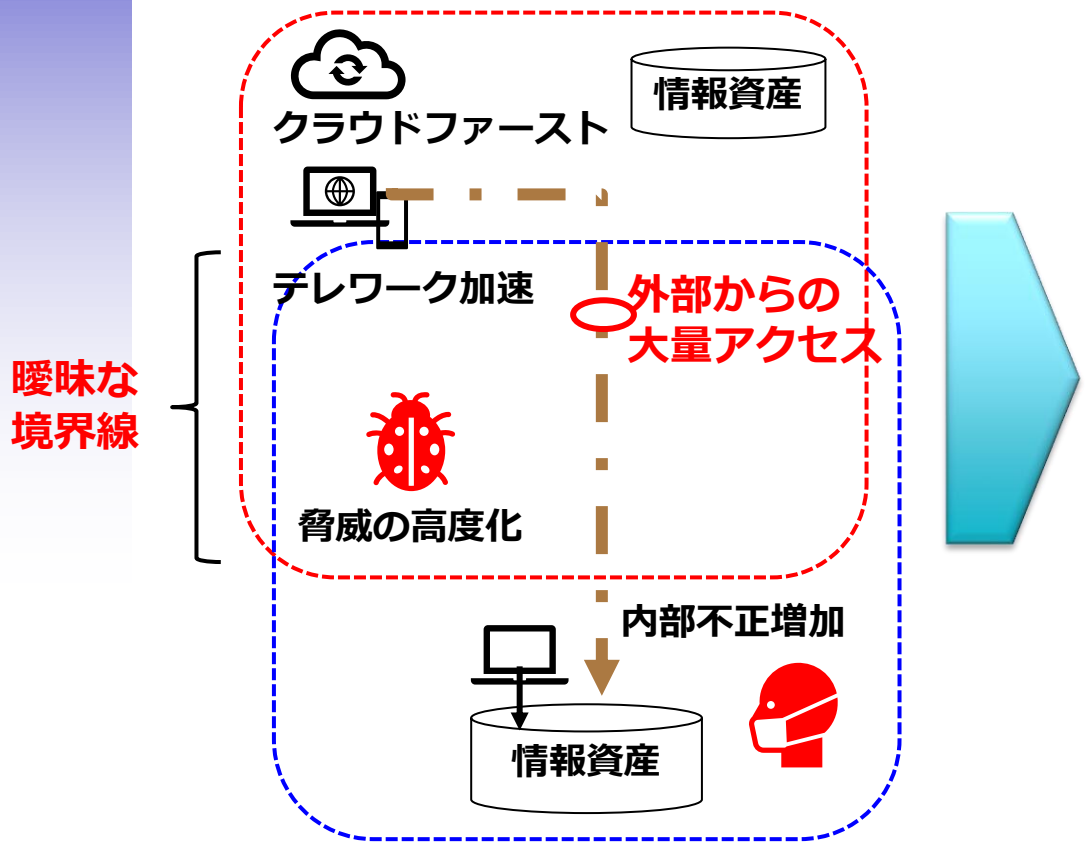


イメージ図



境界防御モデルの限界で発生している事象

境界防御モデルの限界



発生している事象

事象1：クラウド化によりインターネット上に情報資産が大量保管

→社内の情報資産だけ守る境界防御モデルでは対応不可

事象2：テレワーク中心のビジネススタイルで外部から大量のアクセスが発生

→従来のVPNでの対応では帯域不足で適切な業務遂行が困難、外部からのアクセスを適切に認証

事象3：テレワーク中心でオフィスにも自宅にも人がいない

→対面による相互牽制などの運用形態の破綻

事象4：標的型攻撃メールなどにおいて巧妙になり、見分けが付き難く、かつ大量に送られてくる、侵入されたら終わり・・

→従来の人の認識に頼る運用対処の限界

境界防御モデルの限界において発生する事象の深堀と対応方針

事象1：クラウド化によりインターネット上に情報資産が大量保管

→社内の情報資産だけ守る境界防御モデルでは対応不可

課題の深堀	対応方針
・社外保管の情報資産が増加 →境界防御モデルでは対応不可 ・何が保管されているかが不明or棚卸しが出来ていない →増減などの変化が激しく資産台帳の最新化（データ、IT資産など）が出来ていない ・従来の社内ファイルサーバでのアクセス管理では対応不可（クラウド特有の管理が必要）	・インターネット上に保管されている情報の保護について自動暗号化、アクセス制御の徹底 ・クラウドサービスの利用管理と構成管理による実態把握と流動的な情報資産の管理方法の見直しが必要 ・社内/社外のデータを同一に保護する など

事象2：テレワーク中心のビジネススタイルで外部から大量のアクセスが発生

→従来のVPNでの対応では帯域不足で適切な業務遂行が困難、外部からのアクセスを適切に認証

課題の深堀	対応方針
・従来のVPNを張って、社内へのアクセスを安全に確保する方法は現実的ではない →テレワーク中心のビジネススタイルの変化により、大量の送受信データが発生 ・これまで制限していた外部からのアクセスを適切に認証する必要がある	・機密性の高い業務システムはVPN接続での利用 ・通常のオフィス業務はクラウドセキュリティ（Cloud proxy等）の導入で対応、認証後、セキュアな状態で社内を通らずにクラウドサービスへ直接アクセス →社内の帯域圧迫抑制 ・社外からのアクセスを多要素認証などで適切に認証を実施

境界防御モデルの限界において発生する事象の深堀と対応方針

事象3：テレワーク中心でオフィスにも自宅にも人がいない

→対面による相互牽制などの運用形態の破綻

課題の深堀	対応方針
・テレワーク中心の作業で相互牽制が効かないワークスタイルとなった ・オフィスでも出社人数が少ないため、テレワークと同様に相互牽制が効かないワークスタイルとなっている →人が監視するという旧来の考え方では守れない	・相互牽制が必要な業務における確認作業をリモートで実施するためのプロセスを再定義 ・操作ログによる不正操作のモニタリング →何かあった場合のログの保存だけでなく積極的なログ分析で不正操作の確認＆是正 →セキュリティツール導入（ふるまい検知による不正操作の確認）

事象4：標的型攻撃メールなどにおいて巧妙になり、見分けが付き難く、かつ大量に送られてくる、侵入されたら終わり・・

→人の認識に頼る運用対処の限界

課題の深堀	対応方針
・人の注意力だけで防御するのは限界 →サイバー攻撃の高度化、巧妙化、多発化、無差別化 →一定数の開封者がいることを前提にした対策が必要 ※：コロナ禍でいうと必ず一定数の感染者がいることを前提として対応が必要	・巧妙な標的型攻撃メールに対応した訓練＆フィードバックの実施 →開封率の低減 →報告率100%目標（事後対応の徹底＆迅速化） ・EDRやNDRの導入によるふるまい検知による防御 →PCR検査を実施するように感染者を発見し、隔離＆治療する対応が必要

3.1 ゼロトラストセキュリティとは？

NIST SP 800-207*1から読み解く

＊1：米国国立標準技術研究所（NIST）が発行した「Special Publication（SP）800-207 ゼロトラスト・アーキテクチャの解説書

NIST SP 800-207

https://csrc.nist.gov/publications/detail/sp/800-207/final

https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/zero-trust-architecture-jp.html

NIST SP 800-207の要旨

NIST SP 800-207はゼロトラスト・アーキテクチャ（ZTA)の概念定義と情報技術セキュリティ態勢を改善する可能性のある一般的な展開モデルとユースケースを示している（あくまでも考え方）

要旨

ゼロトラスト (ZT) とは、スタティックなネットワークベースの境界線防御から、ユーザ、資産、およびリソースに焦点を当てた防御へと移行する、進化するサイバーセキュリティの一連のパラダイムを指す用語である。ゼロトラスト・アーキテクチャ (ZTA) は、ゼロトラストの概念を利用し、産業や企業のインフラストラクチャとワークフローを計画するものである。ゼロトラストでは、資産やユーザアカウントには、物理的な場所やネットワーク上の位置 (すなわち、ローカルエリアネットワークやインターネット) や資産の所有権 (企業や個人が所有するもの) だけに基づく暗黙の信頼がないことを前提としている。認証と認可 (主体とデバイスの両方) は、企業リソースへのセッションが確立される前に実行される個別の機能である。ゼロトラストは、リモートユーザ、BYOD (Bring Your Own Device) 、企業所有のネットワーク境界内には存在しないクラウドベースの資産等、企業ネットワークの流行に対応したものである。ゼロトラストでは、ネットワークの場所がリソースのセキュリティ態勢の主要な要素とみなされなくなったため、ネットワークセグメントではなく、リソース (資産、サービス、ワークフロー、ネットワークアカウント等) を保護することに焦点を当てている。本文書では、ゼロトラスト・アーキテクチャ (ZTA) の概念的な定義を含み、ゼロトラストが企業の全体的な情報技術セキュリティ態勢を改善する可能性のある一般的な展開モデルとユースケースを示している。

参考

ゼロトラストモデル（全て信頼しない、常に検証）

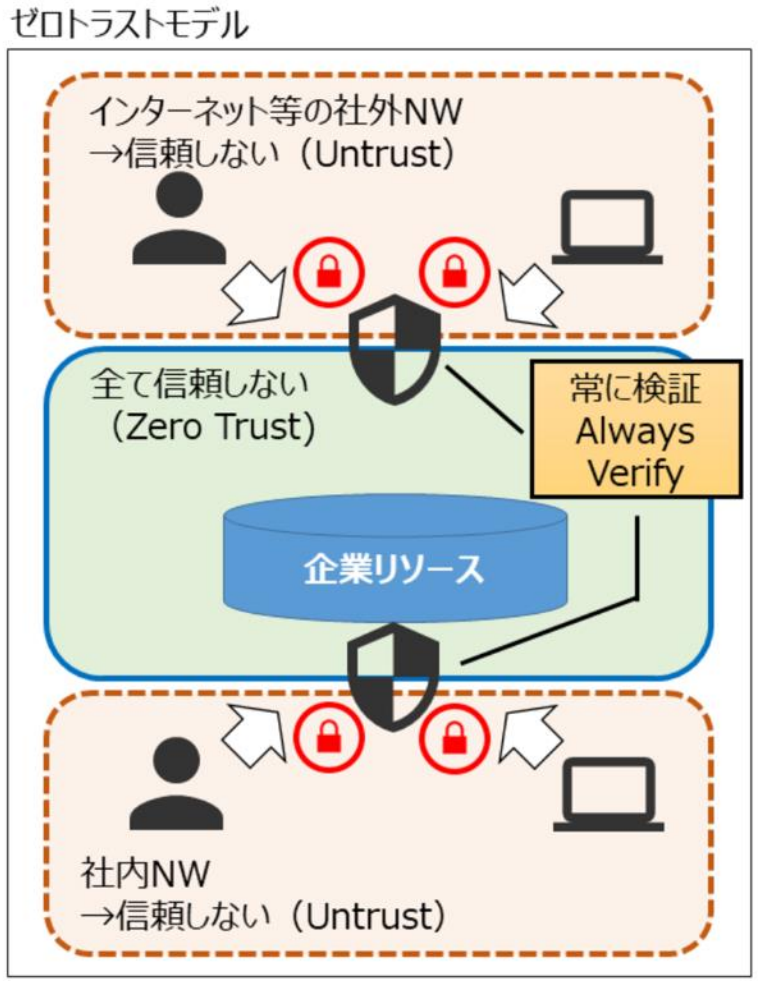


図2. ゼロトラストモデル

ゼロトラストモデル（全て信頼しない、常に検証）

→ 信頼しない（Untrust）とは？

→ 常に検証（Always Verify）とは？

具体的にどういうことをすればゼロトラストモデルを実装したことになるのか？

企業所有のネットワーク境界内に配置されていないリモートユーザーやクラウドベースの資産を含めて、ユーザー、資産、およびリソースを保護することに焦点を当てた、新しい進化したサイバーセキュリティの考え方

https://www.intellilink.co.jp/column/security/2020/052000.aspx

参考

NISTのゼロトラストアーキテクチャー(SP 800-207)

(3) ゼロトラストの原則

ゼロトラストに関する多くの議論では、FW等による境界防御は不要だという誤った印象が強調されてしまうことがありますが、境界防御の要素もゼロトラストの概念の一部として引き続き定義され続けています（例としてマイクロセグメンテーション等の考え方が挙げられます）。ここでは、何を除外するかではなく、何が必要かという観点で原則を挙げます。
なお、理想としてはすべての原則が実装されることが望ましいですが、すべての原則がそのままの形で適用できない可能性があることに注意が必要です。

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見なす。** *All data sources and computing services are considered resources.*
2	**ネットワークのロケーションに関わらず、すべての通信を保護する。** *All communication is secured regardless of network location.*
3	**すべてのリソースの認証と承認を、動的に、アクセスが許可される前に厳密に実施する。** *All resource authentication and authorization are dynamic and strictly enforced before access is allowed.*
4	**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。** *Access to individual enterprise resources is granted on a per-session basis.*
5	**企業リソースへのアクセスを、要求者の身元や利用アプリ、要求する資産などの監視可能な状態やその他ふるまいの属性を含めた動的ポリシーによって決定する。** *Access to resources is determined by dynamic policy—including the observable state of client identity, application, and the requesting asset—and may include other behavioral attributes.*
6	**企業は、所有および関連付けられているすべてのデバイスが可能な限り最も安全な状態にあることを確認、資産を監視し、それらが可能な限り最も安全な状態にあることを確認する。** *The enterprise ensures that all owned and associated devices are in the most secure state possible and monitors assets to ensure that they remain in the most secure state possible.*
7	**動的に適切なポリシーの割り当てを行うため、ネットワークトラフィックやアクセス要求の可視化・収集を行い、継続的にモニタリングする。** *An enterprise should collect data about network traffic and access requests, which is then used to improve policy creation and enforcement. This data can also be used to provide context for access requests from subjects.*

アクセス要求の信頼の実現

アクセス要求の信頼のために必要なインプットを提供

https://www.intellilink.co.jp/column/security/2020/052000.aspx

参考

「ゼロトラストセキュリティ」の考え方を読み解く？

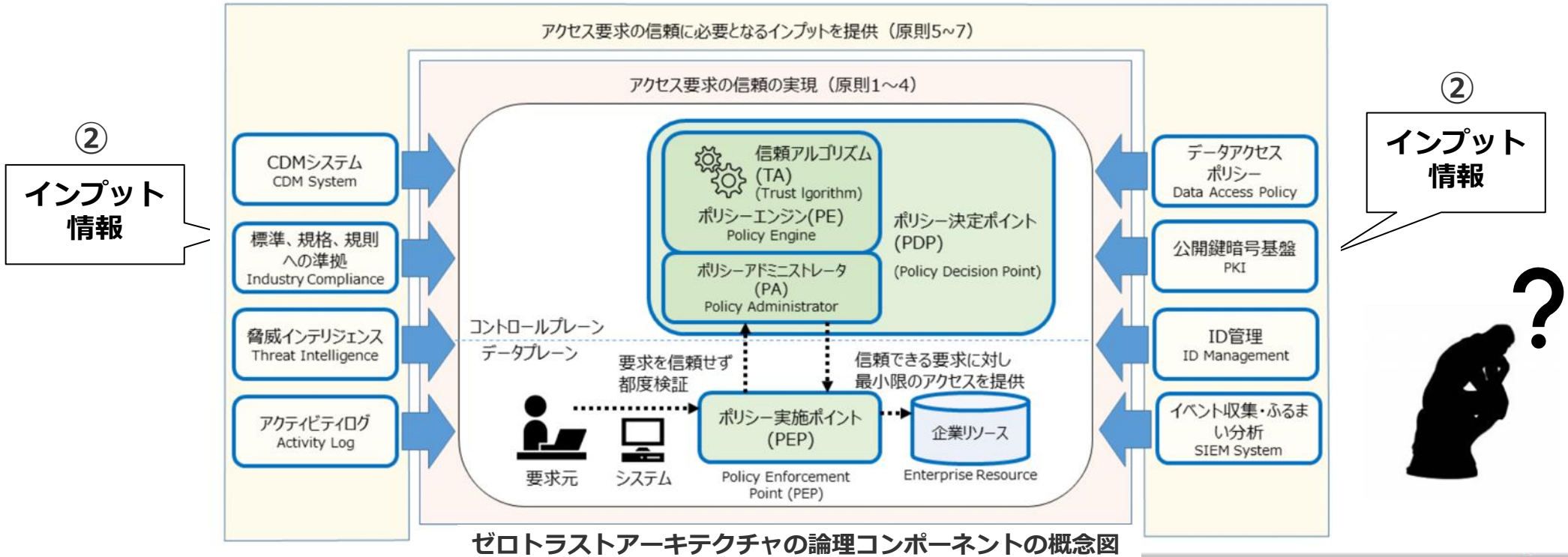
①アクセス要求の信頼の実現

→信頼アルゴリズム（TA）とは？、ポリシーエンジン（PE）とは？
→ポリシーアドミニストレーター（PA）とは？
→ポリシー決定ポイント（PDP）とは？
→ポリシー実施ポイント（PEP）とは？

構成要素の必要性までは理解できるが、どういう仕組みなのか、SP 800-207を読み込んでも理解しにくいので次ページ以降で解説をする・・・

②アクセス要求の信頼のために必要となるインプットを提供

→インプット情報についてはどう使うか別として何となく理解できる



ゼロトラストアーキテクチャの論理コンポーネントの概念図

https://www.intellilink.co.jp/column/security/2020/052000.aspx

3.2 ゼロトラストセキュリティとは？
（概念モデルとユースケース）

ゼロトラストにおけるアクセスの抽象的モデル
についてユースケースを設定して考え方を解説

ゼロトラストの概念の整理の試み

下記のアプローチにより、判り難いゼロトラストの概念のフレームワークを理解しやすく整理を行う

1. ゼロトラストの概念のフレームワーク簡略化

2. 概念のフレームワークをユースケースにて説明

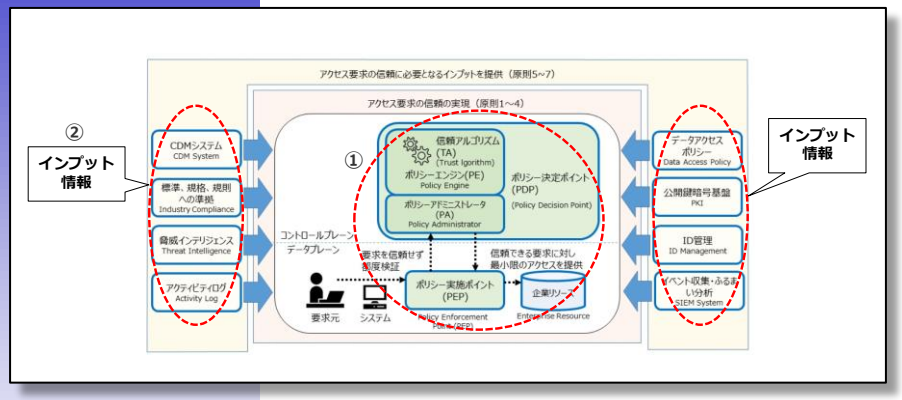
①本人性の確認＆アクセス許可を判断するためのインプット情報

②経路情報及びログ分析による整合性チェック

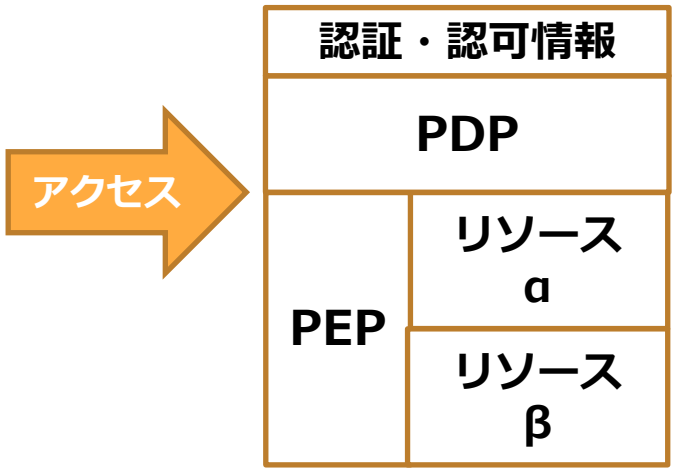
③認可されたアクセスの監視

ゼロトラストセキュリティにおける認証・認可の考え方

ゼロトラストアーキテクチャの論理コンポーネントの概念図

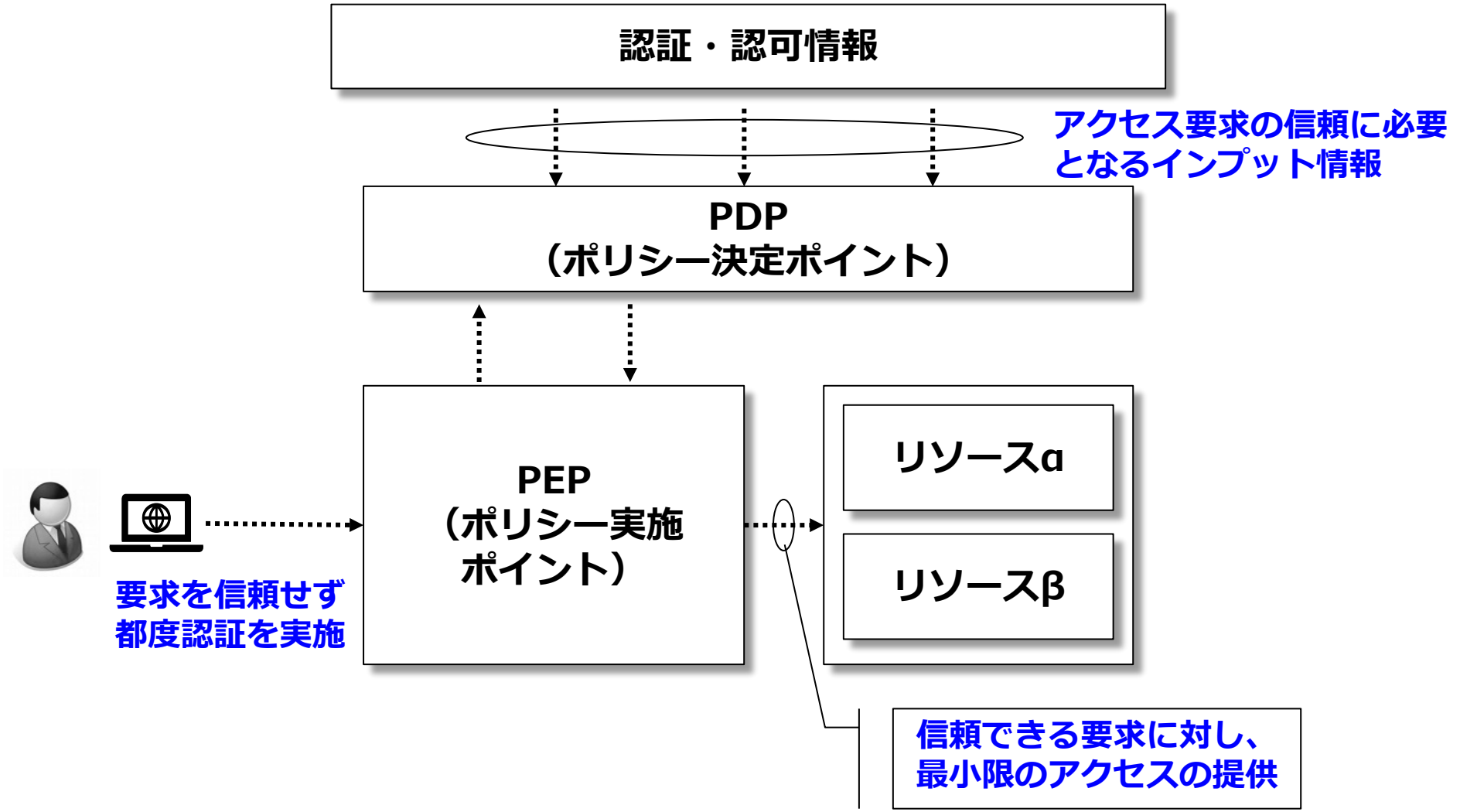


簡略化

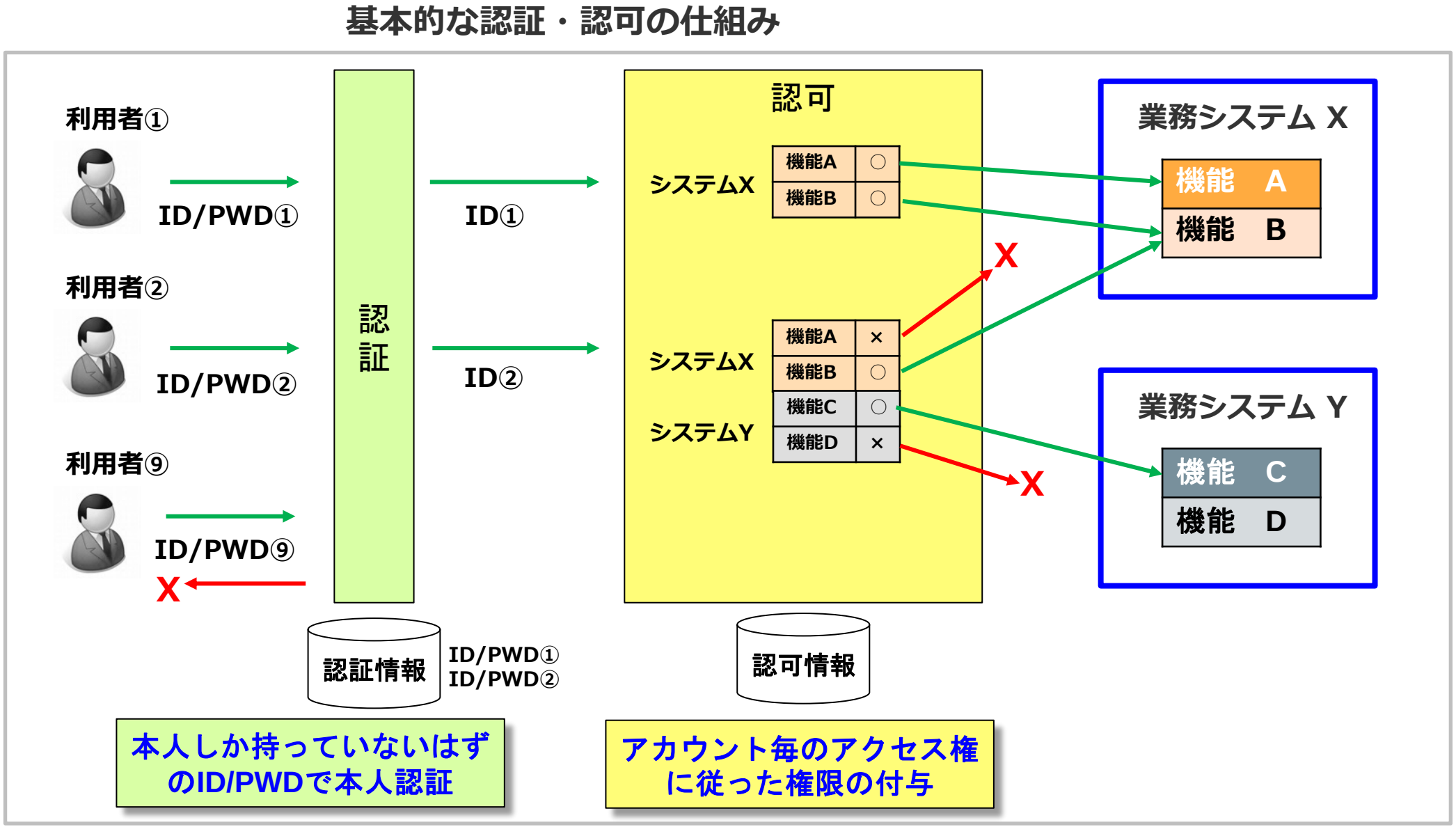


構成要素	説明
PDP(ポリシー決定ポイント)	**認証情報・認可情報に基づいて、アクセス可否（ポリシー）を決定する場所。** ※SP800-207では、PDPをさらに「PA(ポリシーアドミニストレータ)」「PE(ポリシーエンジン)」に分割して記載しているが、当文書では分割記載しない。
PEP(ポリシー実施ポイン)	**決定されたアクセス可否を強制する場所**（Firewallやサーバのログインプロセスなど）
リソース	**組織が業務に使う資源**：システムサービスや情報
認証・認可情報	単純なモデルではPDPが内包しているが、発展形ではPDPに外部から供給されることもある。 以下の図では、特に議論対象にならない限り省略する。

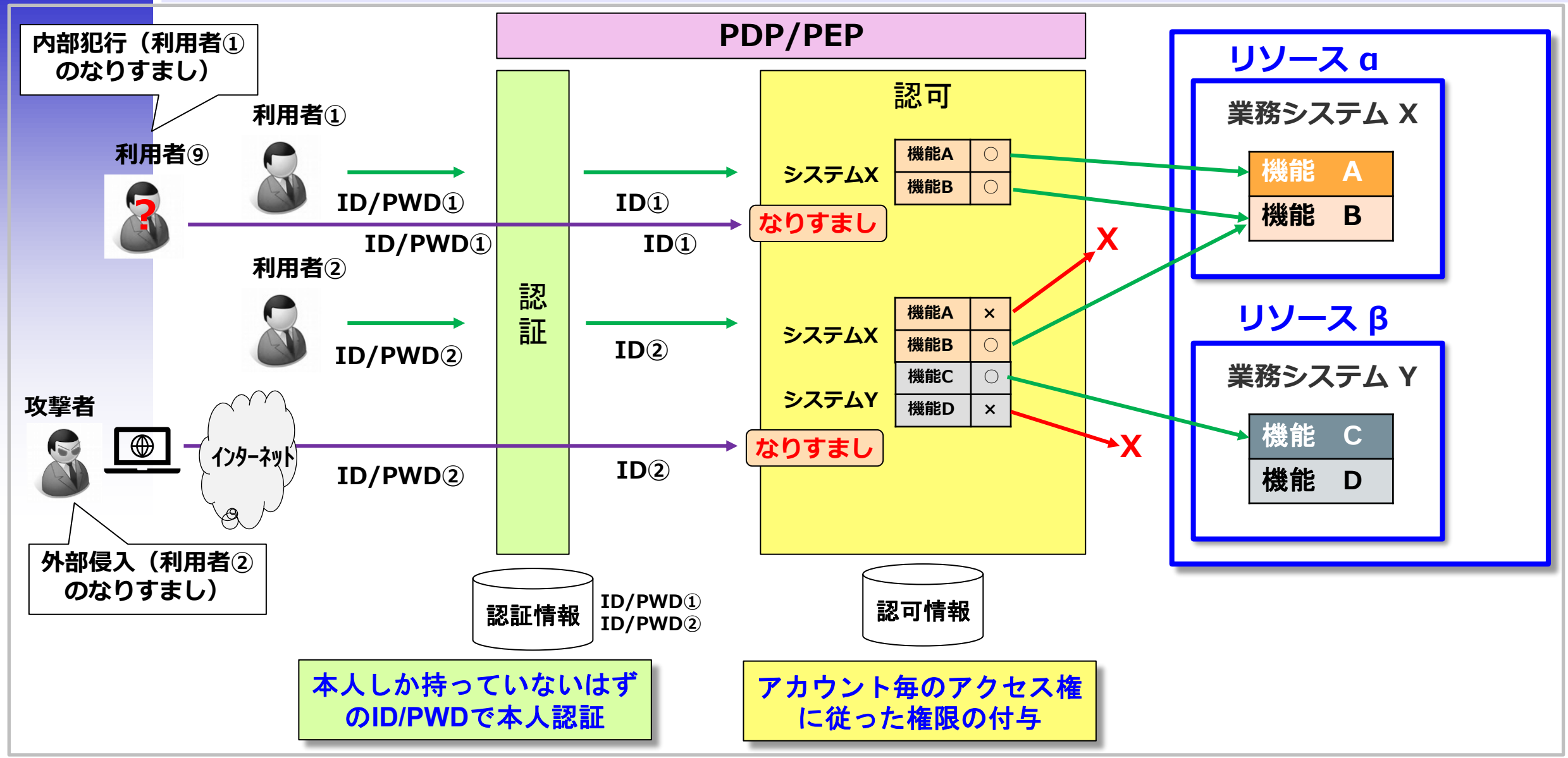
ゼロトラストアーキテクチャの論理コンポーネントの概念図（簡略版）



基本的な認証・認可の仕組み（従来の考え方）



基本的な認証・認可の仕組み（従来の考え方）・・・なりすまし侵入の可能性大



本人性の確認＆アクセス許可を判断するためのインプット情報

なりすましリスクを減らすためには？

PDP/PEP

盗聴リスク
（認証情報・業務情報）

利用者

暗号路

ID/PWD

なりすまし＆感染リスク
（デバイス情報）

・従業員に貸与しているデバイス
・端末の安全性（セキュリティパッチ、ウィルス対策ソフトの確認）

＋

PC　デバイス情報
（会社貸与＆セキュリティ対策）

なりすましリスク
（多要素認証）

＋

スマホ

ID/PWDは搾取されている可能性があるので、本人しか持っていないはずのスマホの認証情報と連携することで本人性の確認の確度が高くなる

認証のためのインプット情報

・ID/PWD

＋

・デバイス情報

＋

・多要素認証

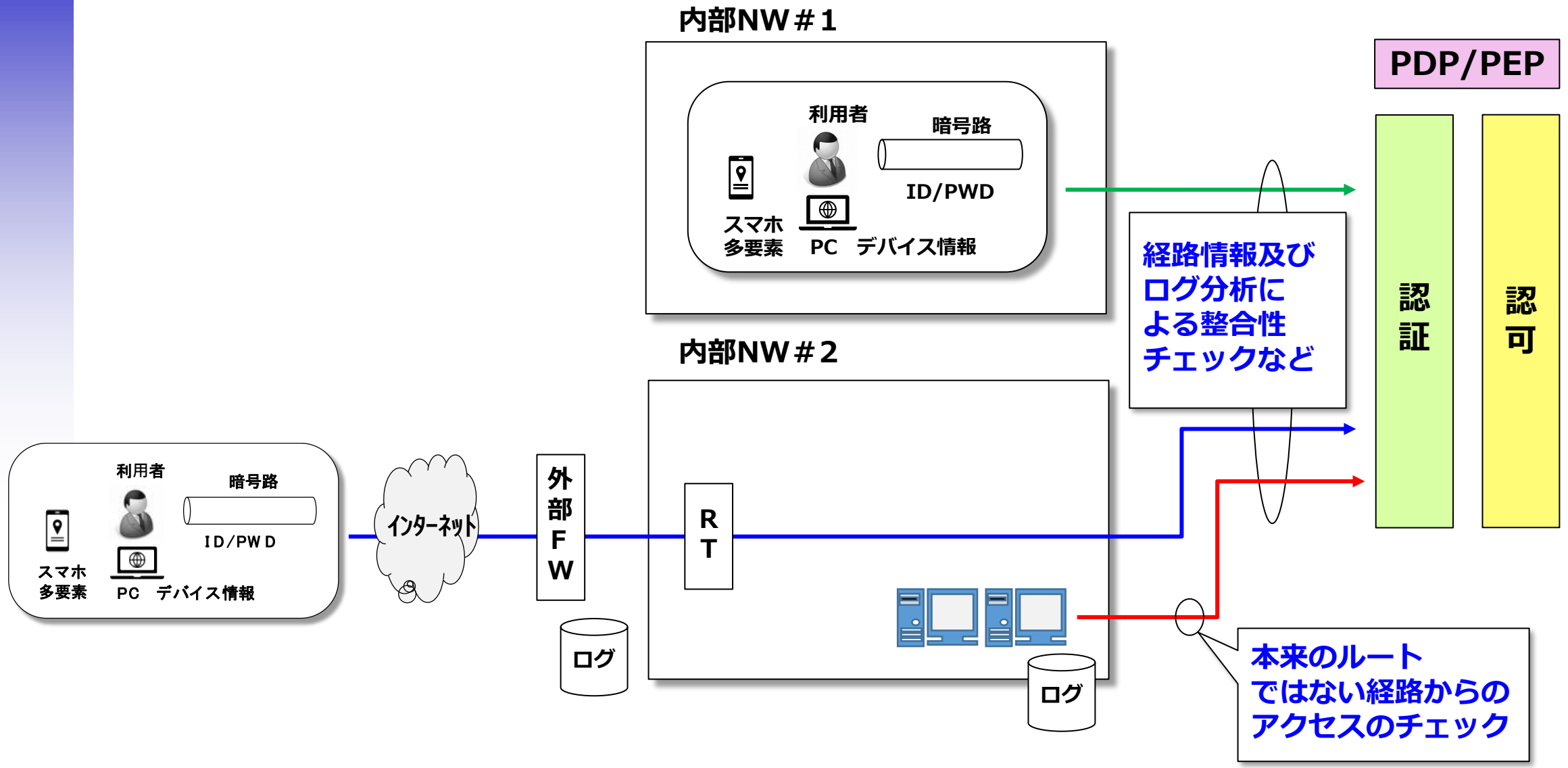
＋

・通信経路情報
など

認証

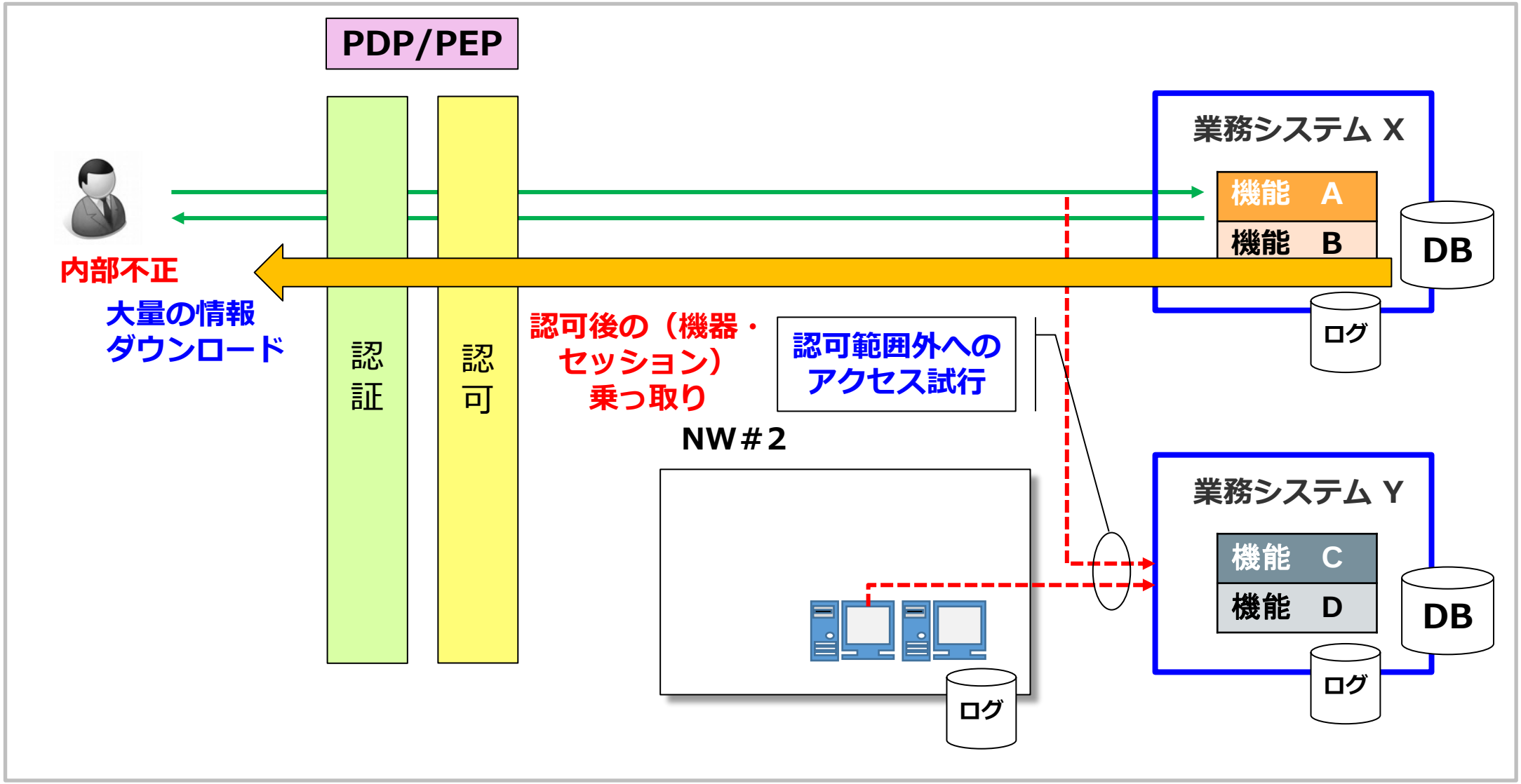
認可

経路情報及びログ分析による整合性チェック



認可されたアクセスの監視

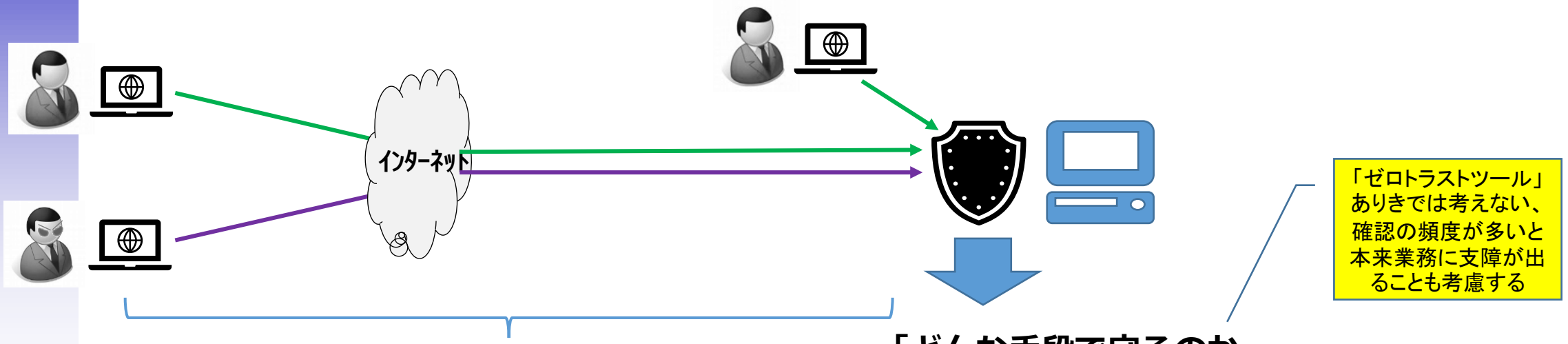
通常と異なる活動の監視（モニタリング）



ゼロトラストの考え方を要約すると・・・無条件には信じない、確認する

→ネットワーク越しの情報は信じられない（社内だからといって無条件には信頼しない）

課題：「ゼロトラストを前提に自組織のアクセス許可条件を明確にする」



「何を疑うのか、どこまで疑うのか」

「どんな手段で守るのか（確認するのか）」

「ゼロトラストツール」ありきでは考えない、確認の頻度が多いと本来業務に支障が出ることも考慮する

疑う事（例）	手段（例）
通信経路（盗聴・なりすまし・通信経路詐称）	専用線、VPN、経由してきた機器のログ
通信相手	ワイタイムパスワード/デジタル証明書
通信相手のパソコン	検疫システム、エージェント導入
アクセス許可した相手の行動	行動監視(SIEM,CDMなど)

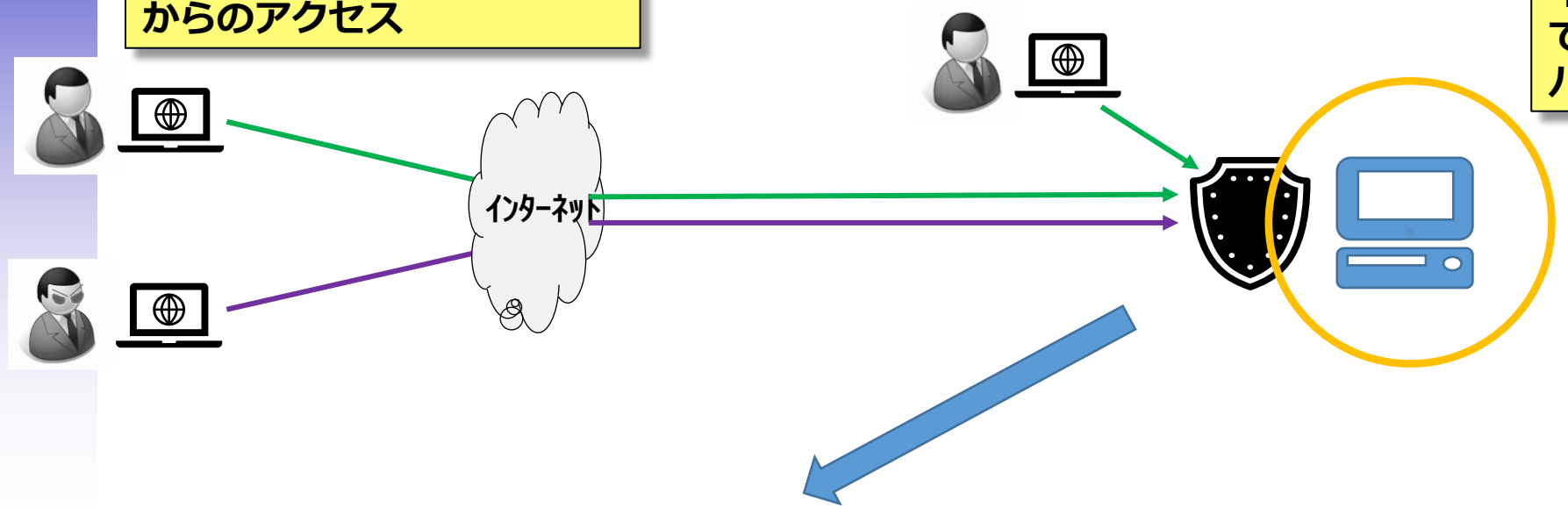
対象組織の事業分野、持っている情報資産の特性、採用しているシステム/NW構成・技術、かけられるコストによって最適解は異なる

（組織の状況に合わせたチューニングが必要）

組織の状況に合わせたリスク分析と対応策の決定（判断）が必要

事例（その１）

テレワーク中心のビジネススタイルで80%以上が外部からのアクセス



事例（その２）

インターネット上に公開しているシステムで常にサイバー攻撃に晒されている

脆弱性情報に基づいてセキュリティアップデートも実施し、定期的にペネトレーションテストやアクセスログの分析を実施しているが過去に侵入されたことがある

EDR導入による振る舞い検知などの対応策も検討の視野に入れる

多要素認証の導入

インターネット越しのアクセスだとID/PWDが盗まれるとなりすましリスクが高いので多要素認証を導入することで本人しか持っていない要素と組み合わせる

4.　ISMSとの関係

ISMSとの関係についての整理

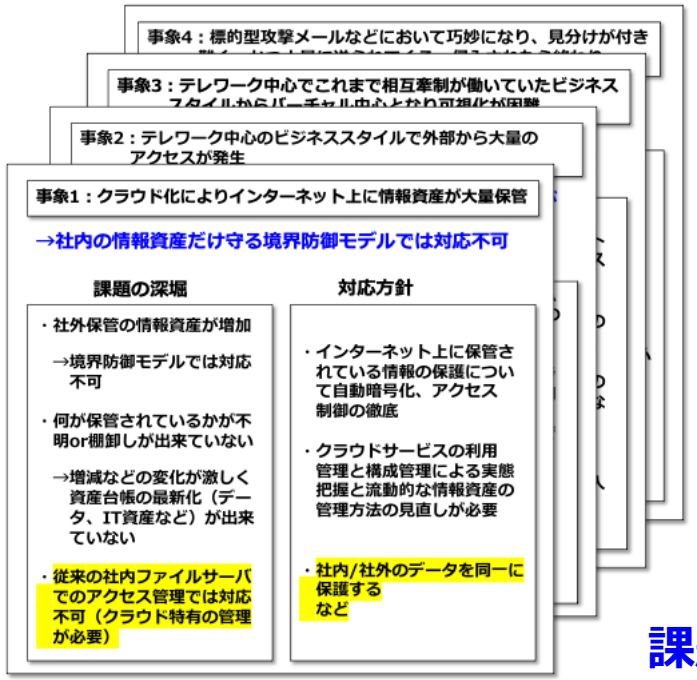
4.1 組織の状況及びその状況の理解

組織は、組織の目的に関連し、かつ、そのISMSの意図した成果を達成する組織の
の能力に影響を与える、**外部及び内部の課題を決定**しなければならない

組織を取り巻く環境の変化

- クラウドファースト時代
（機密情報の社外保管急増）
→SaaS利用の拡大でさらに加速
- サイバー攻撃の多発＆多様化
- コロナ禍におけるテレワーク増大
- 内部不正
- DXの加速＆普及

事象群

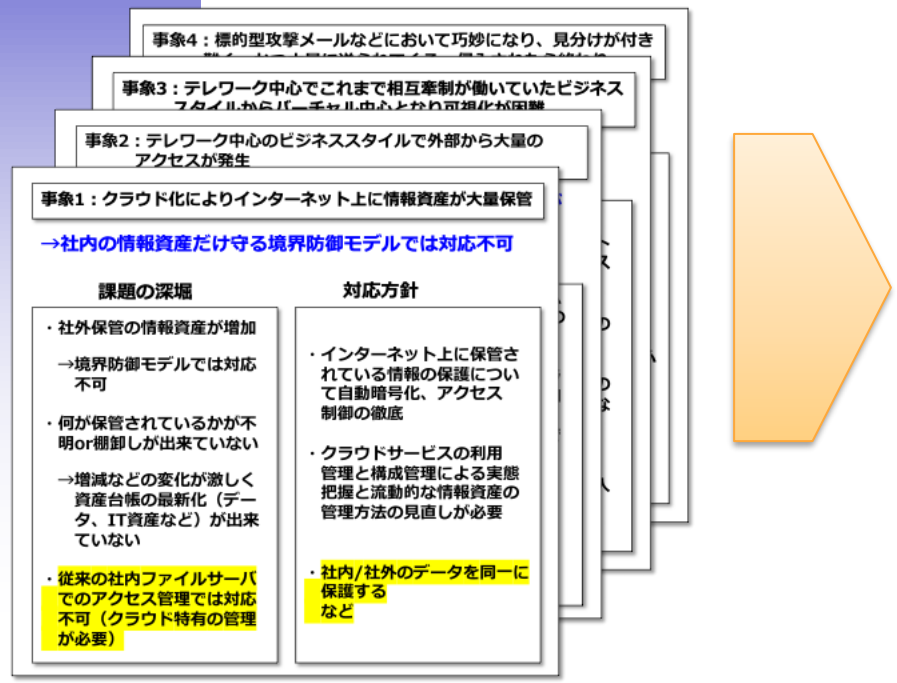


外部及び内部の課題を決定

課題の一つの境界防御モデルの限界から解決策の一つとしてゼロトラストを検討項目の一つとして考慮

ISMSとの関係についての整理

外部及び内部の課題を決定



規格要求事項の「4.1 組織の状況及びその状況の理解」を正しく認識＆実行を行うことでリスクアセスメントに繋げることが重要！

組織で実施してきたセキュリティ管理策で十分（リスク受容範囲）と考えてきた前提条件が崩れた

事例１：情報資産は社内のファイルサーバ内に保管されているはずだった
（社外と社内のNWを分離し、境界防御モデルでセキュリティ対策を厳重に実施）

→社外保管の情報資産が増加（クラウド中心）
→社内ファイルサーバの管理策では守れない？

事例２：外部からのアクセスは一部に制限し、VPNを張って社内へのアクセスの安全に確保していたはずだった
（外部NWからのアクセスを一部に制限し、リモートアクセスの利用者を把握出来ていてID/PWD認証で十分だと思っていた）

→テレワーク中心のビジネススタイルの変化により大量のアクセスが発生し、インターネット経由で不正利用（なりすましなど）の確認が困難

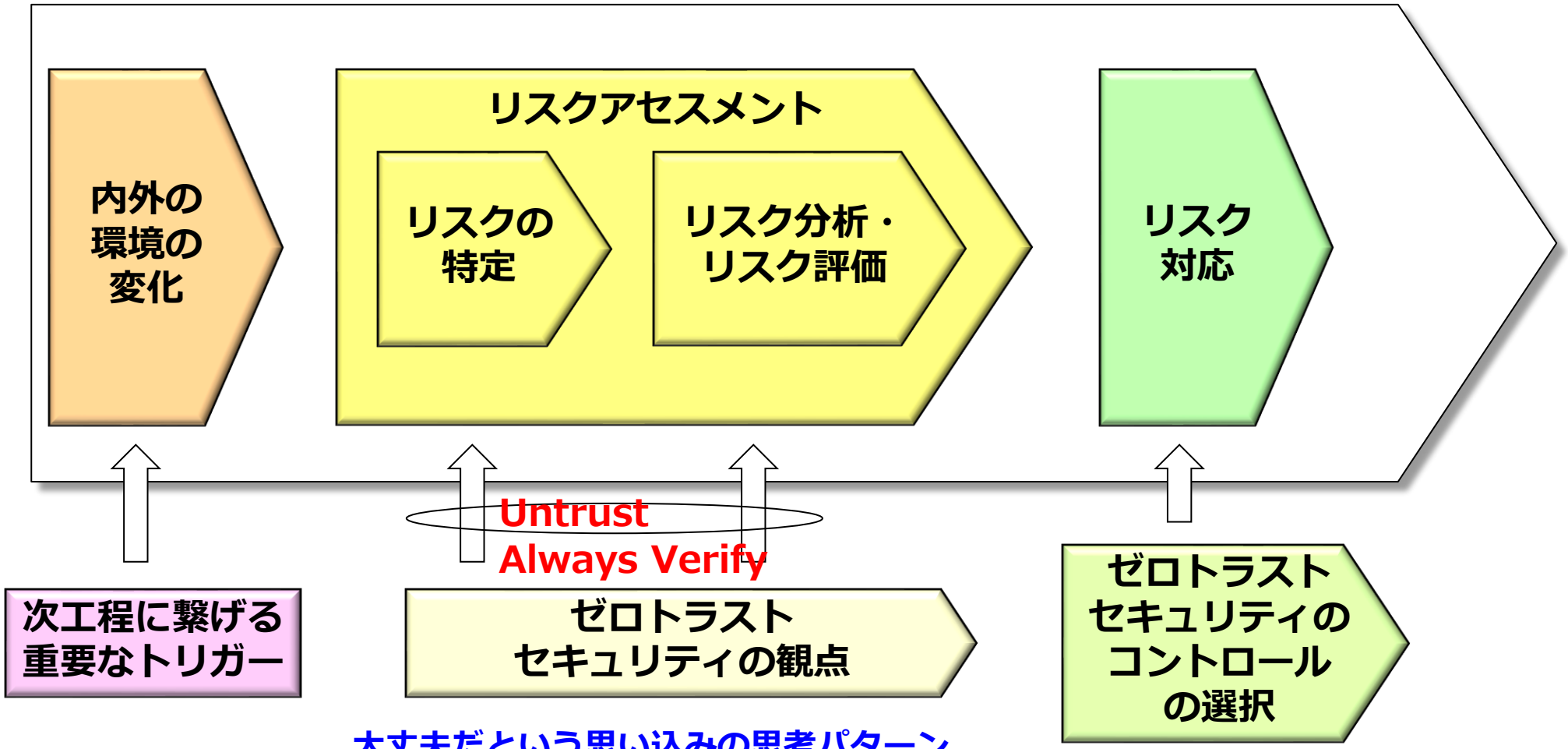
事例３：重要な情報資産を持っていないので、うちは狙われないはず
（対岸の火事として傍観していた）

→現在は無差別攻撃でこれまで重要な情報資産がないから内は大丈夫といっていた企業がランサムウェアの攻撃を受けて、すべてのシステム＆PCを暗号化された結果として業務停止に追い込まれるような状況

環境の変化に伴うリスクの変化が発生

ISMSとの関係についての整理

ISMSの枠組みでの営み



大丈夫だという思い込みの思考パターン
を変えるためのツールとして取り入れる

ISMSとの関係についての整理

ゼロトラスト対応

ゼロトラスト対応ツール

・リアルタイム
・大量データ
・相関分析など

ツール事例

・EDR
・NDR
・SASE
・UEBAなど

ツールの導入で完了ではなく、運用プロセスとの連携が重要（事例①）

ゼロトラスト運用対処

・オフライン
・選択と集中
・マンパワーに左右

運用対処事例

・PWD更新
・利用ログと業務日報との突合
・サーバ/NWの異常ログ分析

＋

セキュリティマネジメントの徹底

・台帳管理
・構成管理
・モニタリングなど

従来の対応

これまでの運用形態の見直し
（信頼しない、常に検証）

・マイクロセグメント
・アクセス制限の徹底
・アカウントの棚卸し

従来の運用プロセスのなかにも信頼しないという精神を反映（事例②）

4.1 管理プロセスの徹底

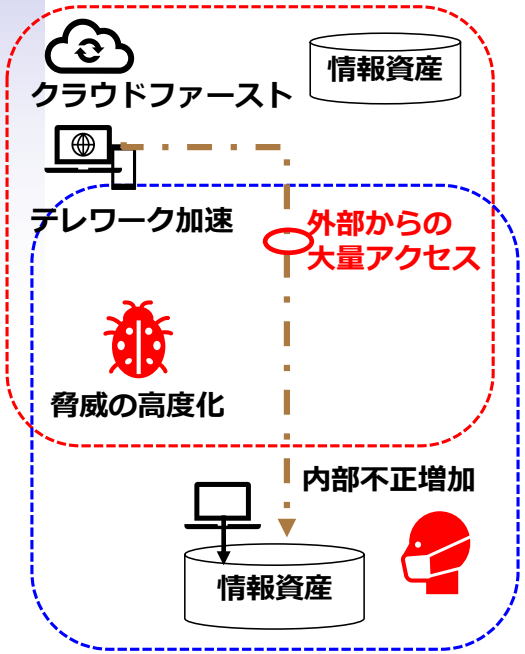
**ツールの導入で完了
ではなく、運用プロセスと
の連携が重要（事例①）**

ゼロトラストとは？　・・・　コロナ禍の状況と似ている？

・ゼロトラストはコロナの状況と似ている、ウィルスを持っている人が一定数いる状況で
どのように暮らしていくか？

→ 発熱やPCR検査などで検出後に隔離処置（コロナ）
→マルウェア感染による挙動の変化や振る舞い検知による発見＆隔離処置（ゼロトラスト）

境界防御モデルの限界

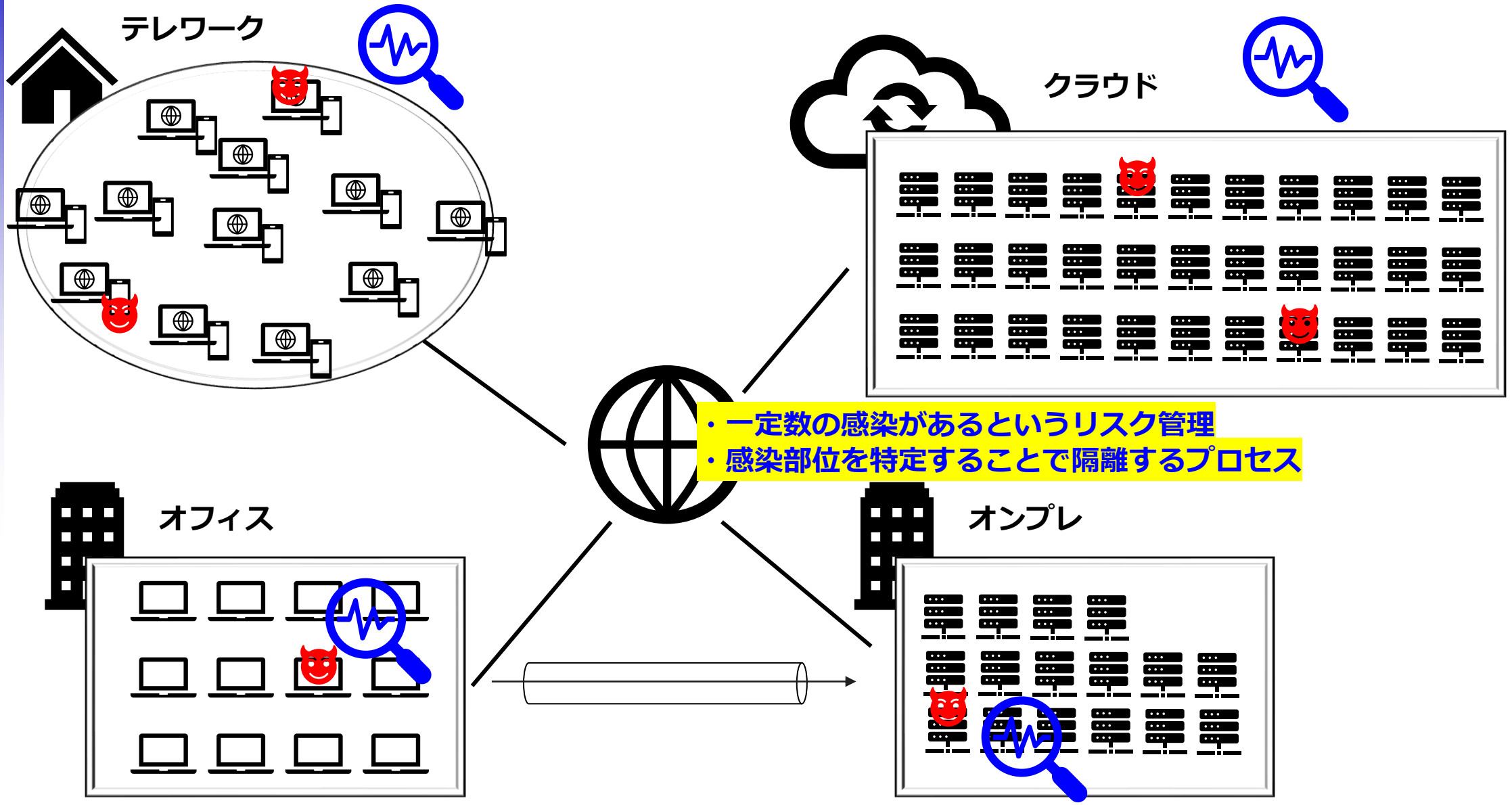


感染しないように境界線で防御していたが、感染しているかもしれないという前提条件での対応が必要
（一定数の感染があるというリスク管理）

→各ブロック単位（サーバ群、PC群）でEDRなどによる振る舞い検知を実施することで感染部位を特定することで隔離するプロセスを構築することが重要

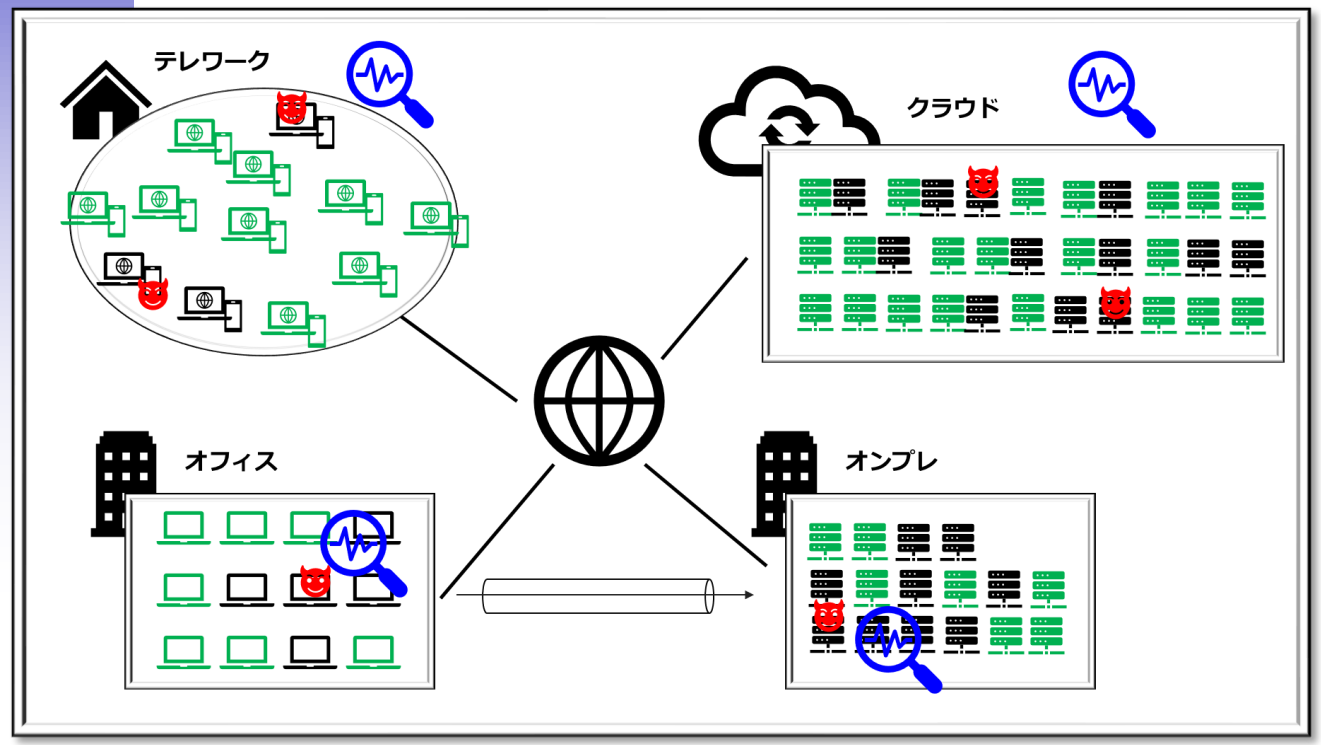
→多要素認証や都度認証により、システム内への侵入リスクを出来るだけ制限することも重要（但し、複数の入り口やシステムを網羅的に設計＆構築するには時間とリソースが掛かるので、EDRから導入する判断がなされていると推定

ゼロトラストとは？　・・・　コロナ禍の状況と似ている？



EDR*1を導入すれば安心か？　→ NO！

①振る舞い検知は完全ではない
②EDRを導入対象（オンプレ、クラウド、PC)すべてに入れる必要がある
③検知した後の対応プロセスの構築が必要



：EDRの導入済み
：EDRの未導入

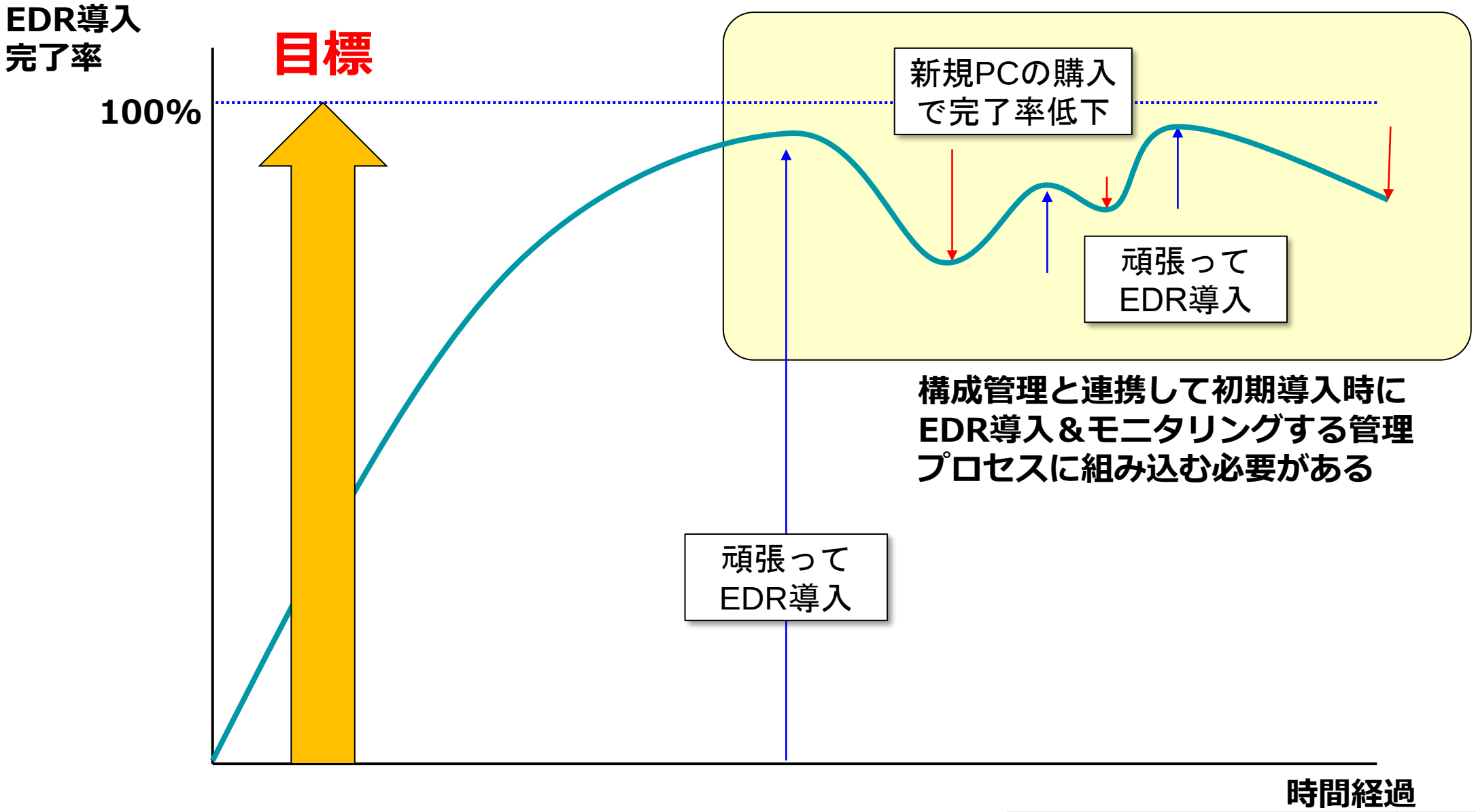
EDRなどのシステムを導入したら終わりではなく、それらを機能させるためのプロセス作りが重要！

例）

・IT資産の導入プロセスへの組み込み
・野良クラウドの防止
・モニタリングによる可視化など

＊1：EDR（Endpoint Detection and Response）とは、ユーザーが利用するパソコンやサーバー（エンドポイント）における不審な挙動を検知し、迅速な対応を支援するソリューション

EDR導入完了率100%を目指すためには？



EDRなどのゼロトラストを機能させるためには・・・

EDRなどのゼロトラストシステムを機能させるための管理プロセス作りとは？

事例	コントロール対象	コントロール	補足説明
IT資産の導入プロセス	OA用PC	増減するIT資産に追随してEDRの導入をもれなく実施するためのプロセス作り →導入漏れがリスクにつながる	情シスが全体コントロール
	プロジェクト用PC		各部門が中心となるため統一的な対応が取りにくい
	オンプレミス		対象の特定を契約決裁から確認することで抜け漏れを防ぐ
	クラウド		インスタンスを自由に増減出来るので管理するためのプロセス作りが難しい
野良クラウド	個人契約の無認可クラウド	管理面、情報漏洩の観点からも野良クラウドの発生を管理プロセスから防止	操作ログのスクリーニングや内部監査のヒアリングで確認する
モニタリングによる可視化	各種セキュリティログ	ログインの失敗や時間外でのアクセス、不正操作などの確認を実施	通常の運用プロセスの中に定期的なイベントとしての組み込みが重要

4.2 これまでの運用形態の見直し

従来の運用プロセスの
なかにも信頼しない
という精神を反映
（事例②）

ゼロトラストの考えで運用形態の見直し

無条件に信頼していたものを信頼しないことを前提条件にする

①認証・認可を通過したとしても、常に正しいエンティティだと限らない

→入口を通過しても、自由にアクセス出来ないように設計する（マイクロセグメント）

→アクセス制御の徹底（必要最小限のアクセス権付与）＆定期的な棚卸し
・アカウントの乗っ取りがあったとしても最低限の権限で被害を最小化

→都度認証の徹底、多要素認証の導入

②システム内には常に正規のメンバーだけでなく、第三者が存在する可能性がある

→不正侵入された形跡を常に確認する（アクセス拒否のログに着目＆アクセス時間帯の確認）

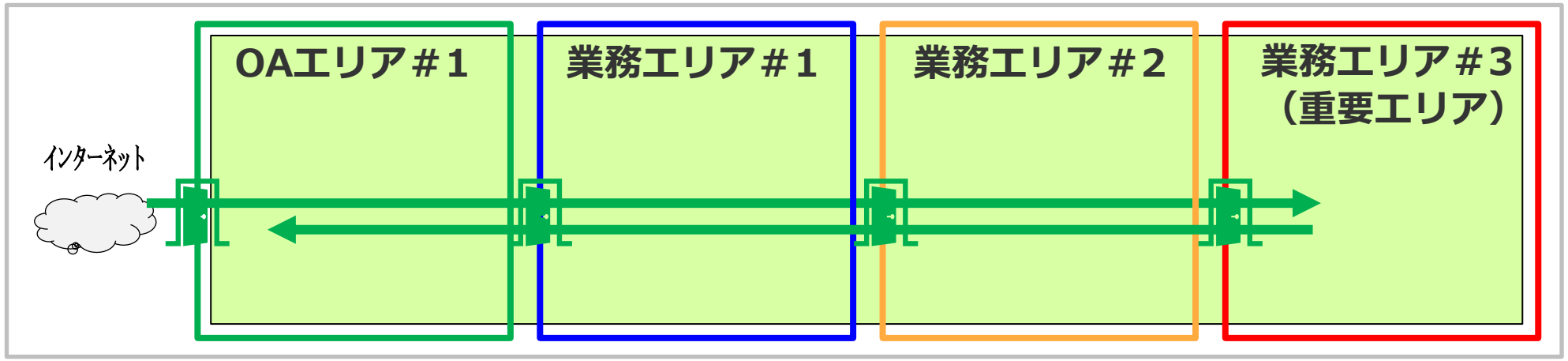
→異動等でアクセス権が無い利用者のアカウントが放置されていないか確認する
非正規メンバーがアクセスをしていないか（内部メンバーによる不正アクセス）

次ページ以降に事例を紹介

ゼロトラストに関する考察（その1）・・・マイクロセグメント

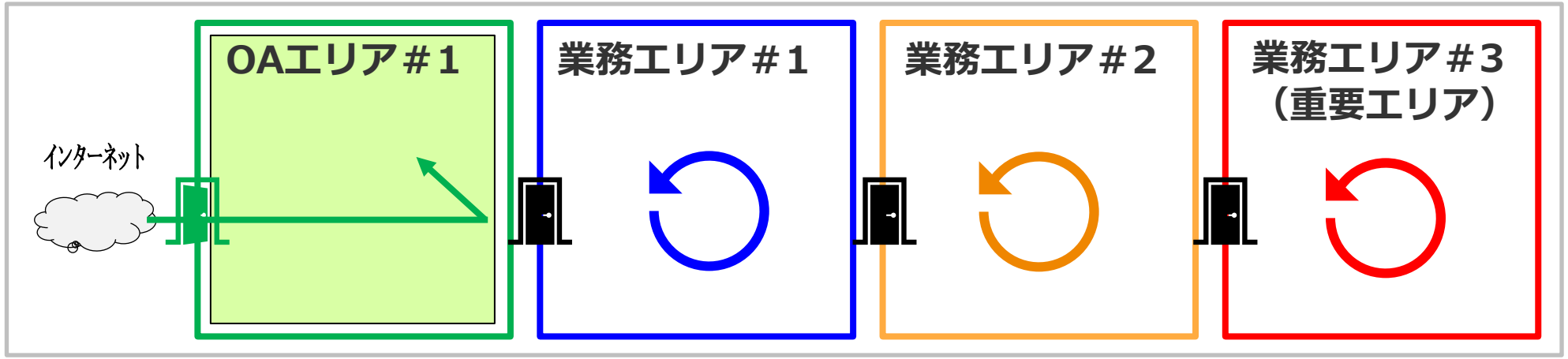
NGな
パターン

入口を通過したら、どこへでも自由にアクセス可能（侵入されたら自由に移動可能）



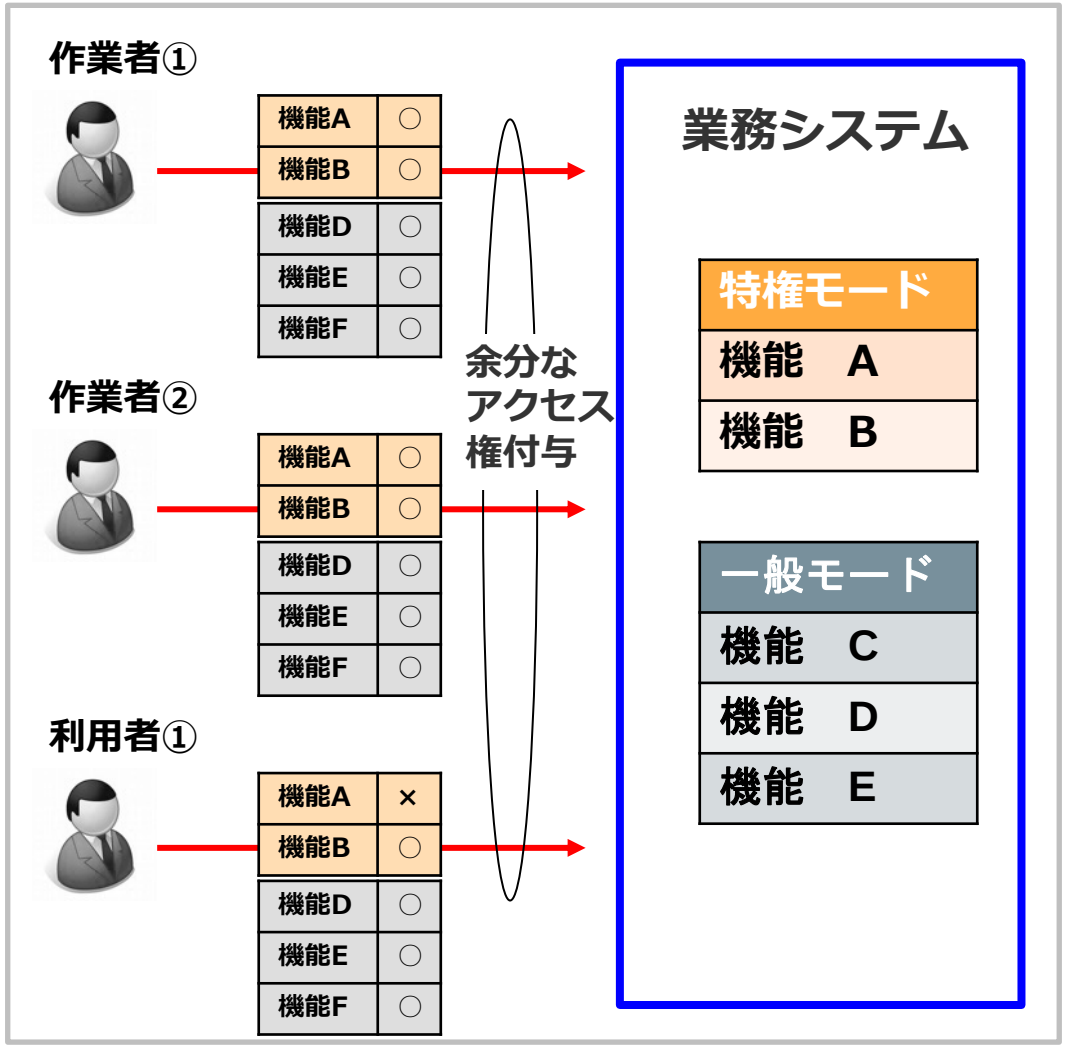
Goodな
パターン

入口を通過しても、自由にアクセス出来ないように設計する（マイクロセグメント）

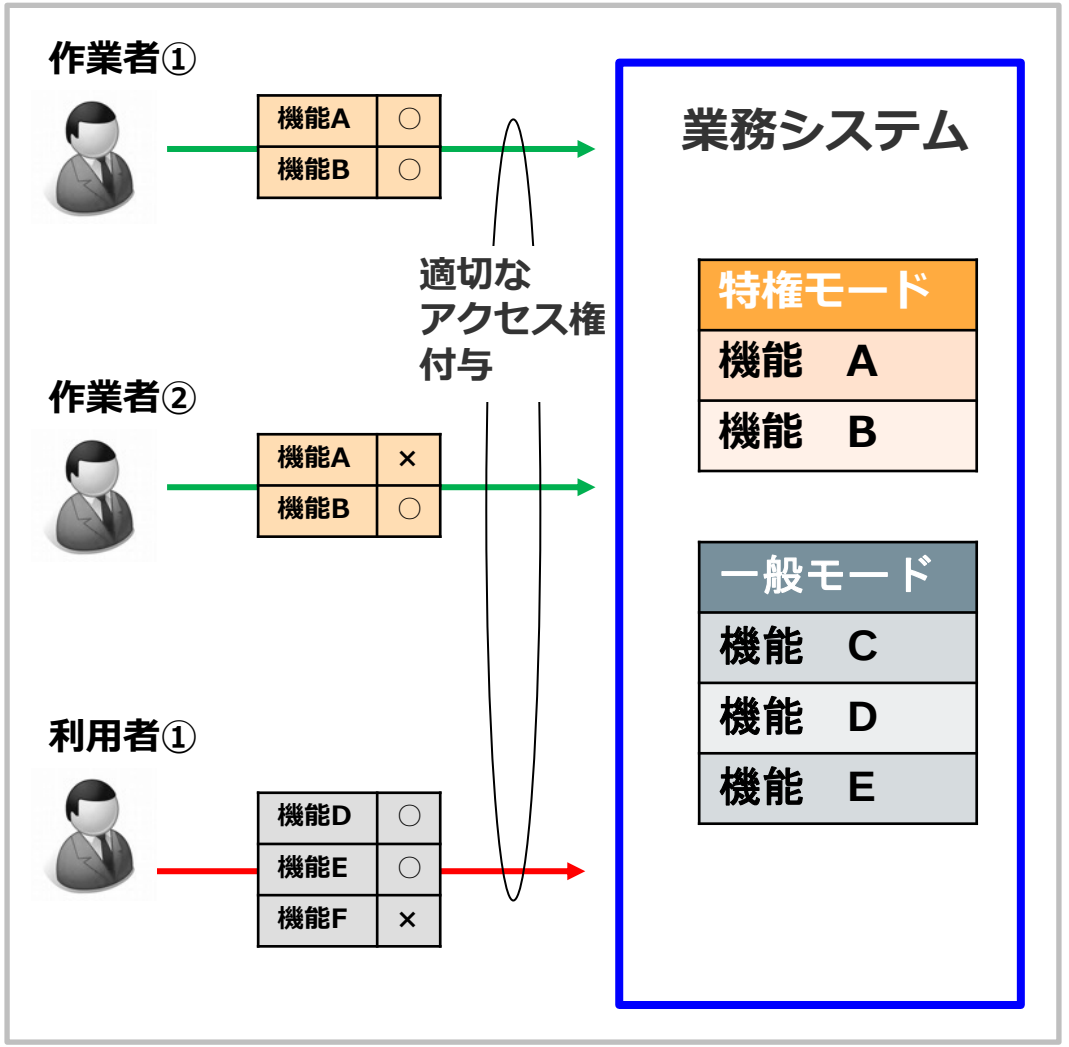


ゼロトラストに関する考察（その2）・・・アクセス制限の徹底

NGなパターン
（アクセス権の特売状態）



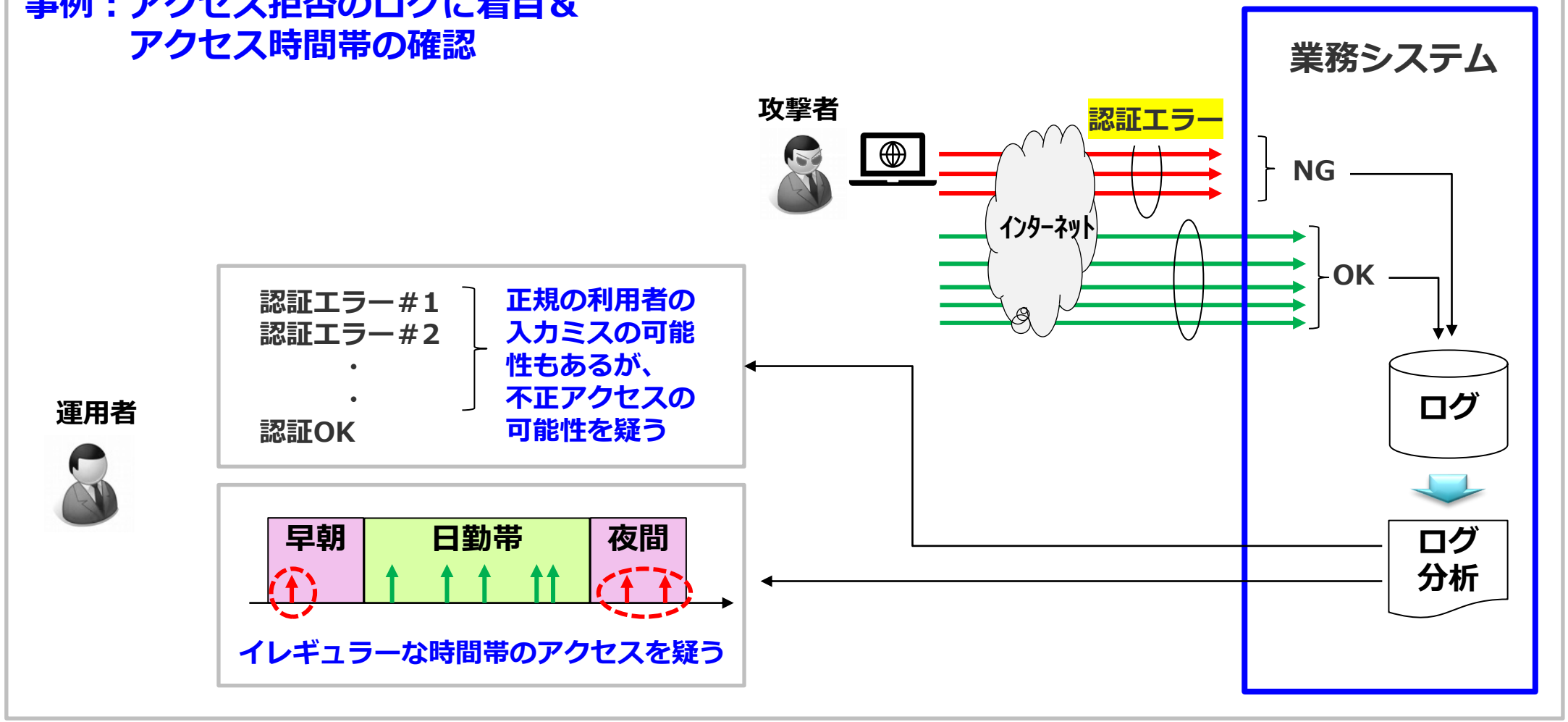
Goodなパターン
（必要最低限の払い出し）



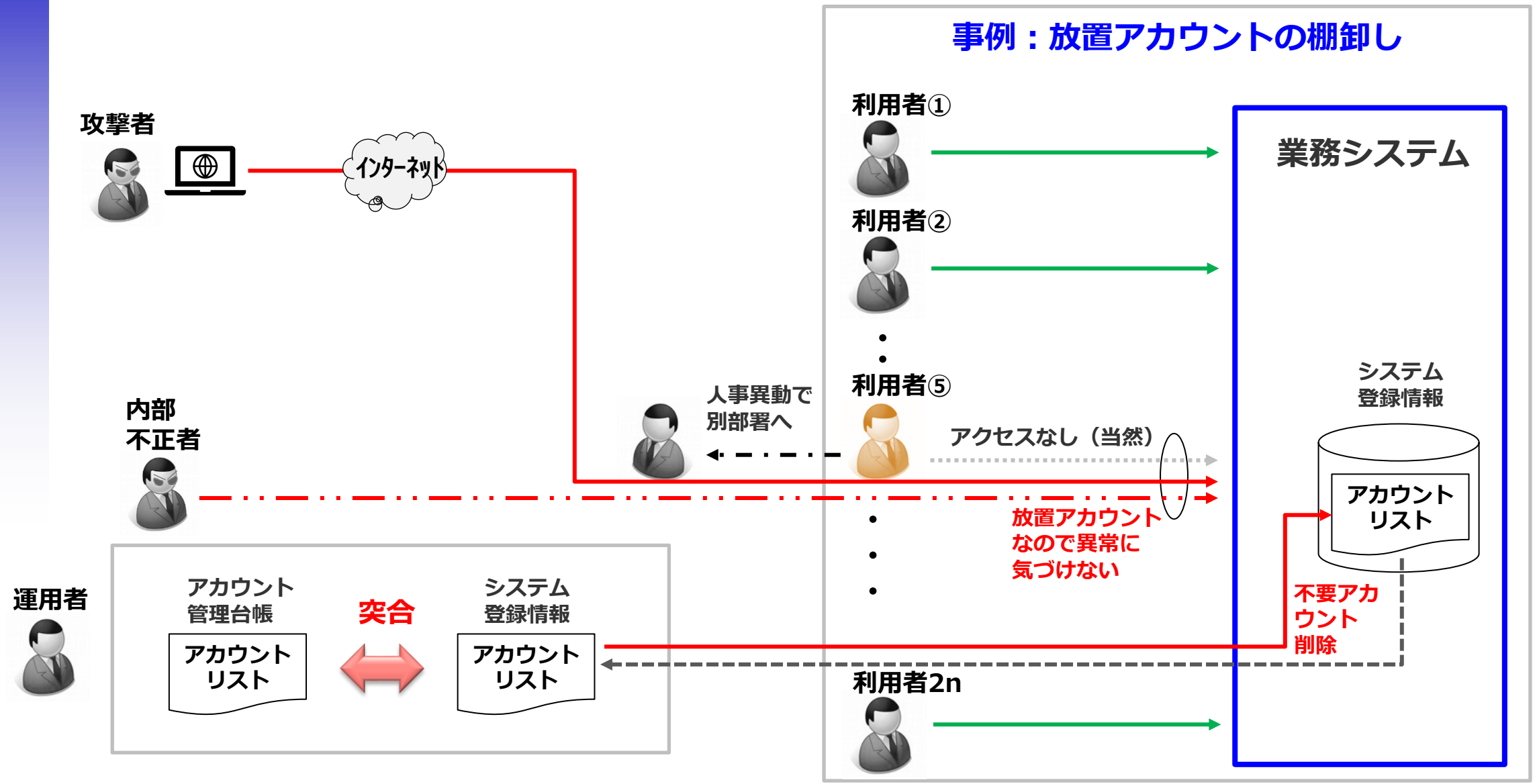
ゼロトラストに関する考察（その3）・・・不正侵入

不正侵入されているという前提条件で
侵入された形跡を常に確認する

事例：アクセス拒否のログに着目＆
アクセス時間帯の確認



ゼロトラストに関する考察（その4）・・・危険な放置アカウント



5. まとめ

ゼロトラストセキュリティとISMSとの関係
→協調しながら、リスク対応を行う両輪

ゼロトラストセキュリティの勉強をしてみて少し理解したこと

・新しい概念ではないが時代にマッチした考え

・ツールありきではなく各組織状況＆特性に合わせた検討が必要

・スクラッチ開発ではなく既存のシステムとの整合を考慮

・ツールの導入がゴールではなく管理プロセスも一緒に考慮

・リスクアセスメントが重要なことを改めて認識

仮説（独り言）

ウィルス対策ソフトの導入が一般的でなかった時代には導入効果について費用対効果で判断していたが、現在では入れることは常識、必須条件となっている（空気のような状態）
ゼロトラスト関連のツール類も同じ状況になりつつある？？？

■インプリメンテーション研究会へのお誘い

2021年は下記の2テーマに取り組んできました。
毎年、**組織を取り巻く環境の変化に対応したテーマに挑戦**しています。
ご興味のある方は一緒に検討に参加頂ければ幸いです。
冷やかしも大歓迎ですので、気軽に事務局へご連絡ください。

テーマ1：　ISMSとゼロトラストセキュリティについての考察

テーマ2：　ISMS要求事項の解釈と運用の実態
（箇条4について）

現在、Web会議（zoom）
で討議しています！
毎月最終木曜日18:00～21:00

ご清聴ありがとうございました。

本日のセミナーではISMSとゼロトラストセキュリティを題材に企業を取り巻くリスクに対してISMS＋αでどのように可視化＆対応すべきかについてご紹介させて頂きました。

今回ご紹介した内容は一つの事例にすぎませんが、今後皆さまの職場へ持ち帰って検討頂ければ幸いです。

ルンダーレ宮殿の中庭