Japan Information Security Management Systems User Group

JNSA 標準化部会セミナー

ゼロトラストとISMS

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

2023年8月23日

魚脇　雅晴

【講演2】　「ゼロトラストとISMS」　14:45-15:05〈20分〉

ゼロトラストの歴史

- 2004年くらいから議論されている考え方
- サイバー攻撃の活発化/多発化で時代のニーズとなった

ゼロトラストモデルを現実モデルに実装

- ゼロトラストの概念は抽象化されいるため解りにくい
- 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から現実モデルに落として事例紹介

ISMS（マネジメントシステム）との関係（技術とマネジメントシステムという両輪）

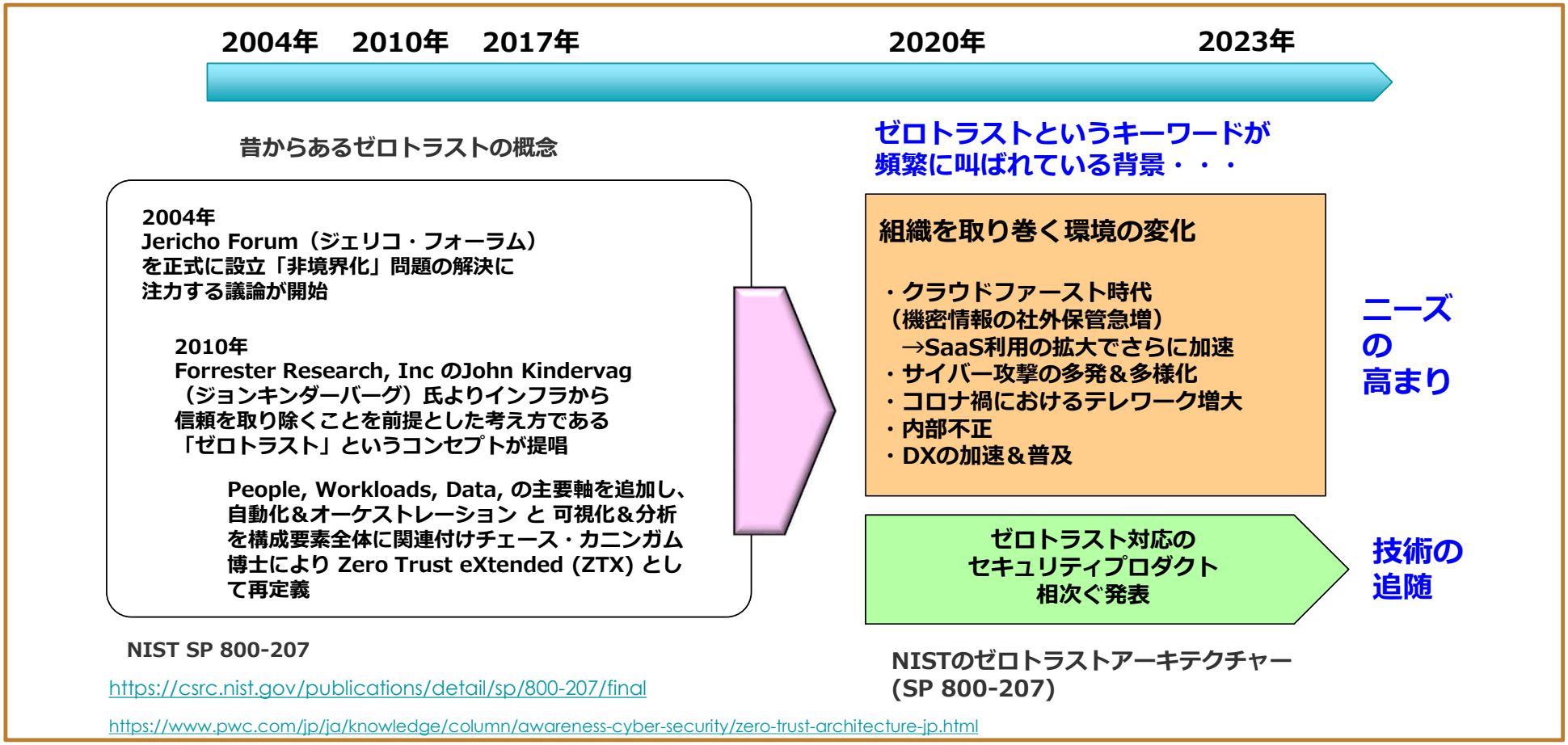
- ゼロトラストのソリューション（技術）とISMS（マネージメントシステム）との関係を整理
- ツールを有効活用するためにはマネジメントシステムとの連携が重要

まとめ
ゼロトラストの本質

- 何を守るか？、どう守るか？、どこまで守るか？
- ビジネスとセキュリティのバランスの両立が大事

ゼロトラストの歴史

ゼロトラストの概念は新しい概念ではなく、2004年くらいから議論されていて、ソリューションありきのものではなかったが、近年のサイバー攻撃の活発化・多発化に対応するための時代のニーズとなった



ゼロトラストの歴史を振り返る・・・ゼロトラストの考え方の背景

昔でも絶対に守らなければならない情報を手間隙かけて守る必要があったので、ツール前提ではなく非境界化や信頼を取り除くという議論がされていた

外部　**外部は危険がいっぱい**

内部　**<内部も安全ではない>**

- 内部は仲間だけ→不正を働くかも？
- 重要な作業は2mansルールで相互牽制
- 作業ログを必ず取得し、すぐにチェック（作業申請との付き合わせ）
- 特殊エリアは監視カメラかガラス張り
- 特権アカウントは1～2名に限定
- 機密情報には徹底的に近づけさせない
- 定期的な監査を随時実施

わかるようでよくわからない
ゼロトラストモデルを紐解く

ゼロトラストモデルを現実モデルに実装（概念/論理モデルから現実モデル）

概念モデル

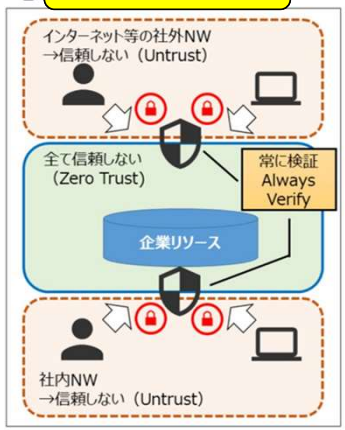
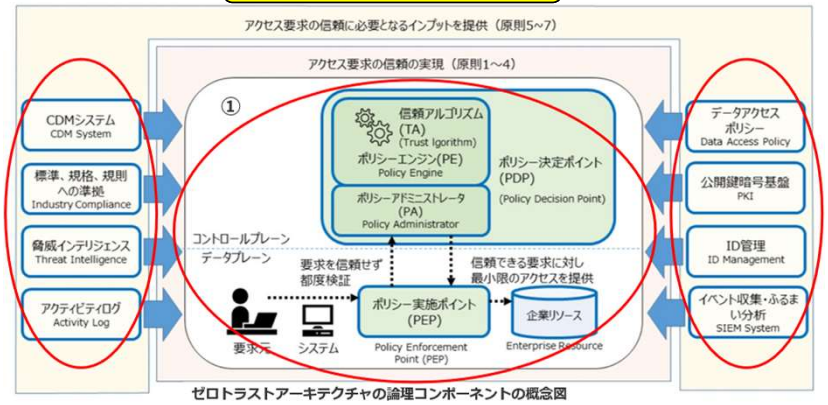


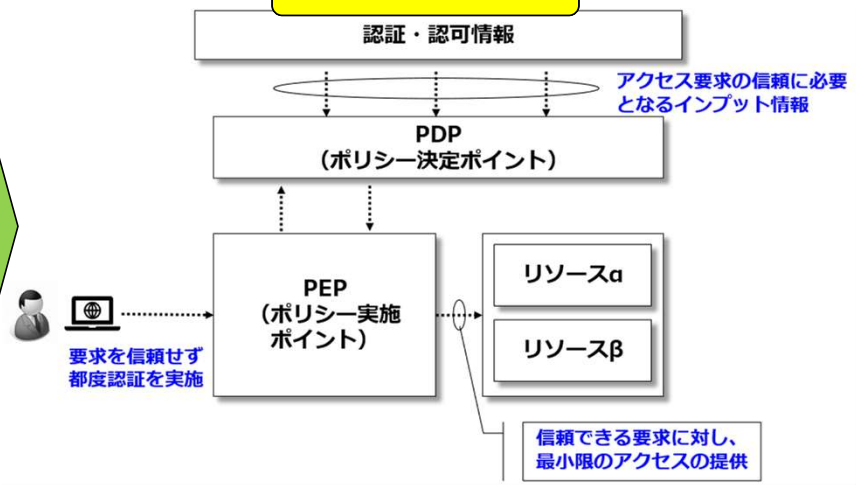
図2.ゼロトラストモデル

論理モデル

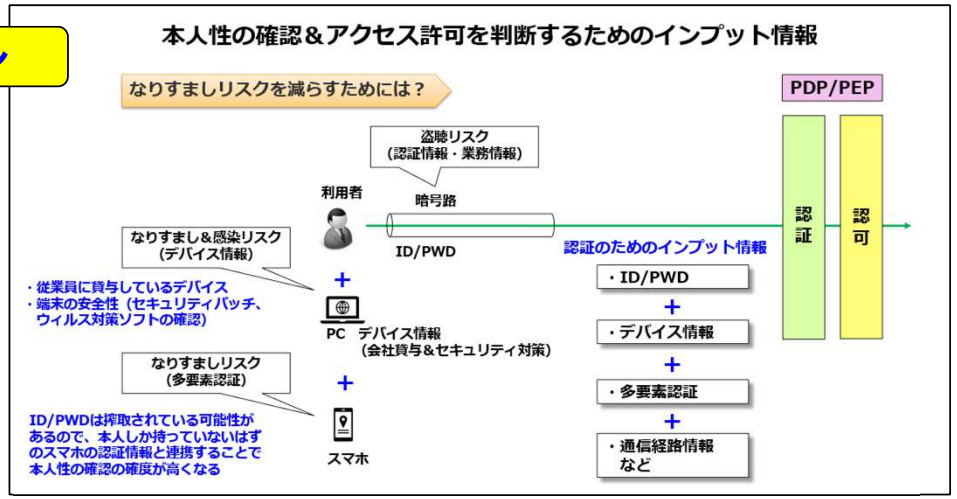


ゼロトラストアーキテクチャの論理コンポーネントの概念図

簡略モデル



現実モデル



ゼロトラストモデルを
現実モデルに実装

概念モデル
論理モデル
簡略モデル
現実モデル

ゼロトラストモデル（全て信頼しない、常に検証）の概念

ゼロトラストモデル

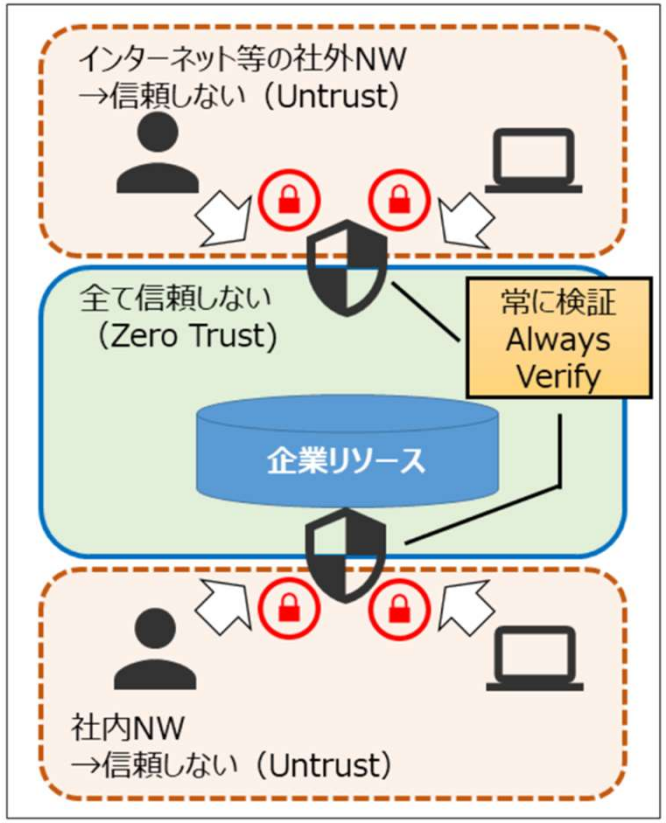


図2.ゼロトラストモデル

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？

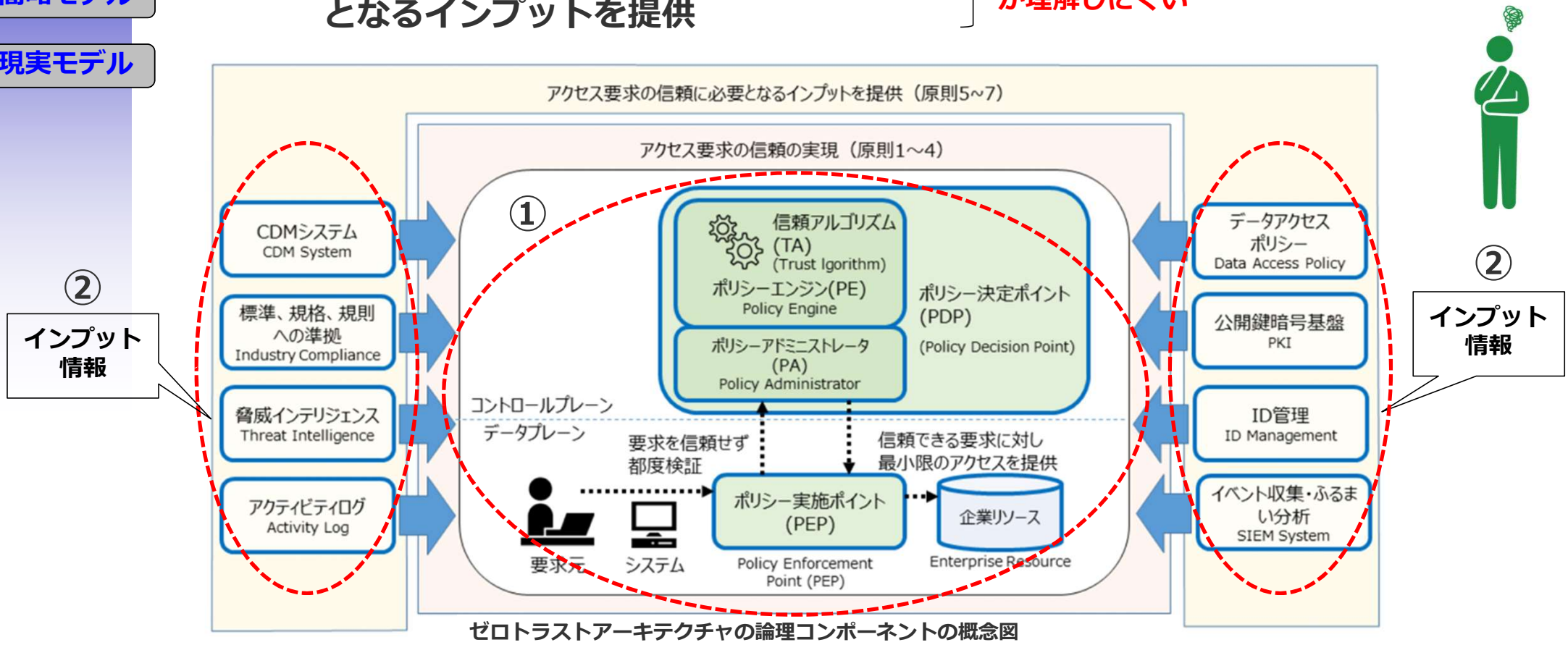
https://www.intellilink.co.jp/column/security/2020/052000.aspx

概念モデル
論理モデル
簡略モデル
現実モデル

ゼロトラストセキュリティの論理コンポーネントの概念図

①アクセス要求の信頼の実現
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

構成要素の必要性は理解できるが、SP 800-207を読み込んでも全体像が理解しにくい

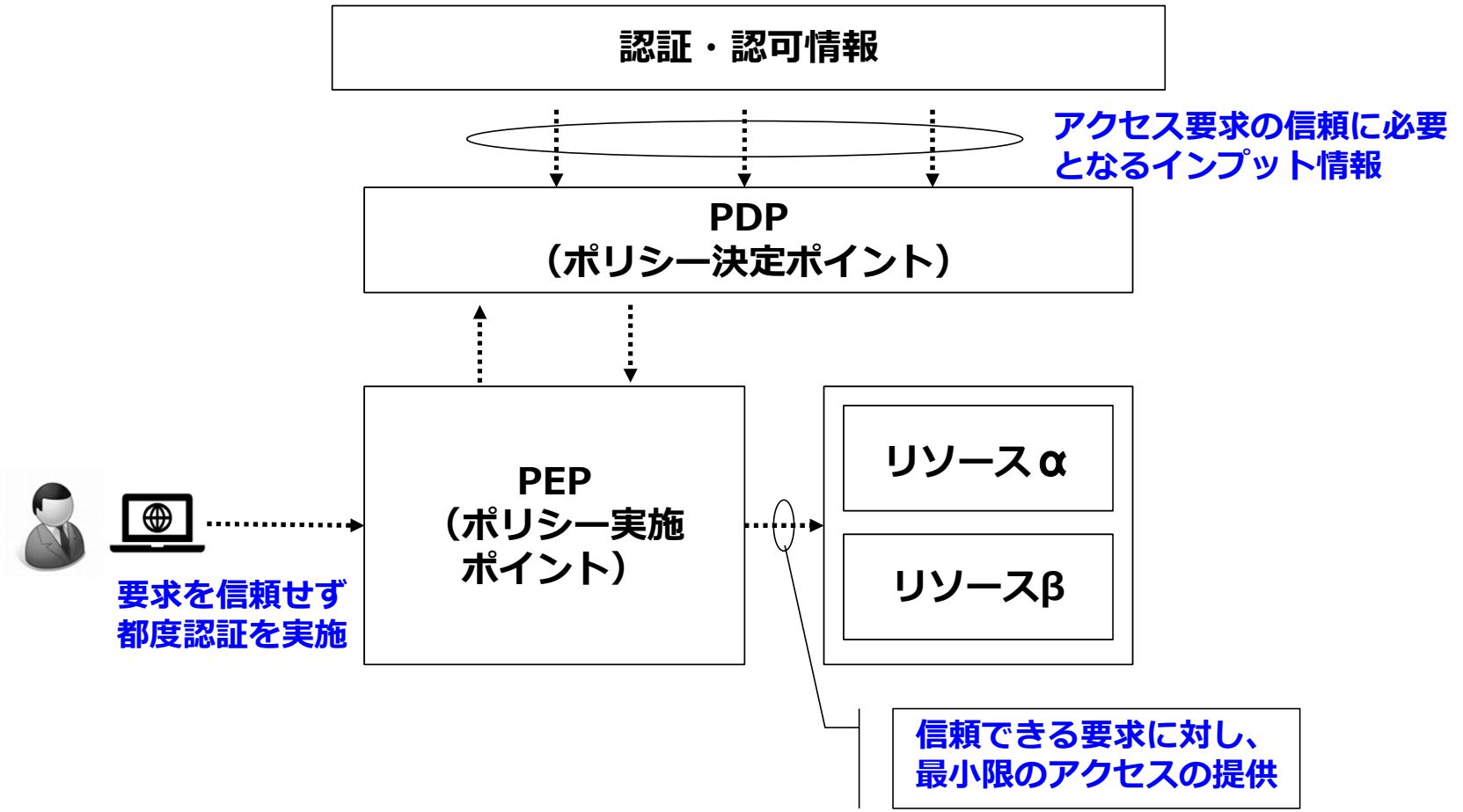


ゼロトラストアーキテクチャの論理コンポーネントの概念図

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

概念モデル
論理モデル
簡略モデル
現実モデル

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）



概念モデル
論理モデル
簡略モデル
現実モデル

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

事例

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

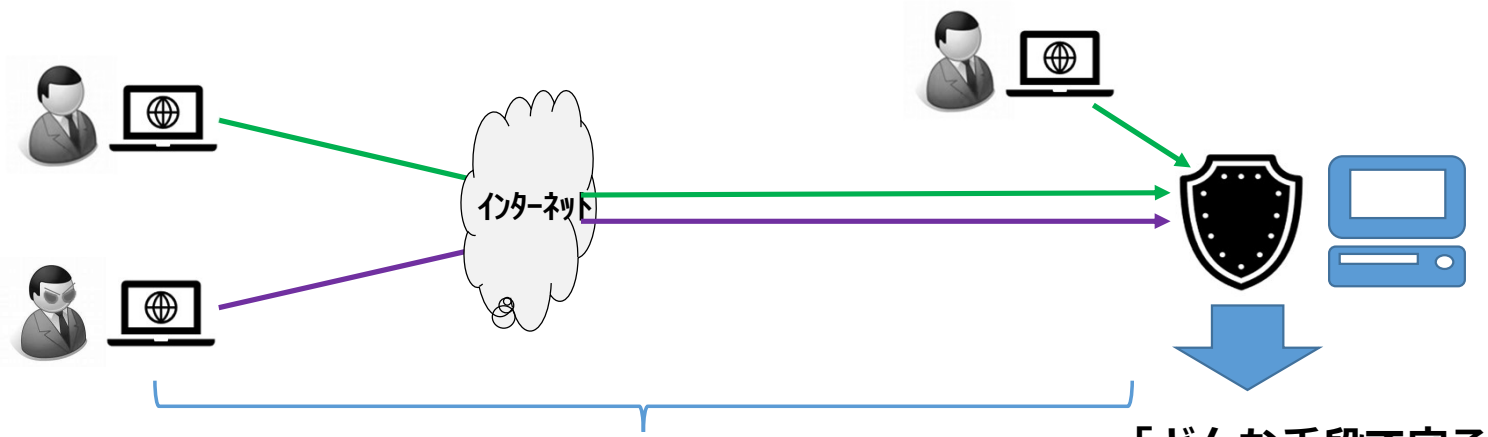
・ID/PWD
＋
・デバイス情報
＋
・多要素認証
＋
・通信経路情報
など

認証

認可

事例

疑うことと守る手段（確認方法）について



「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）」

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）

ゼロトラストとISMSの関係

技術とマネジメントシステム

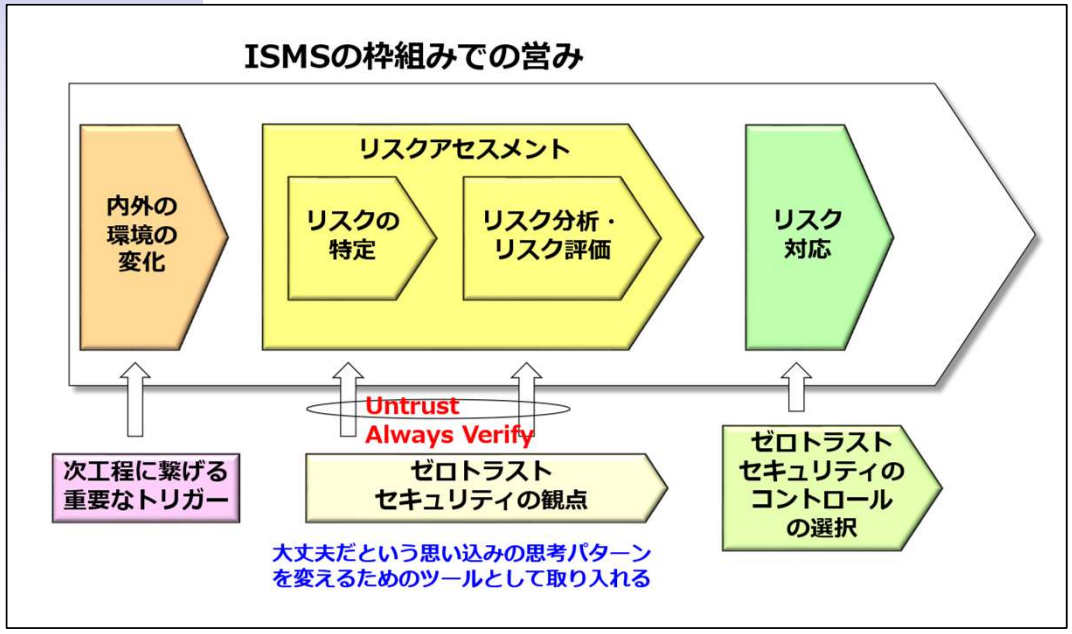
両輪の関係

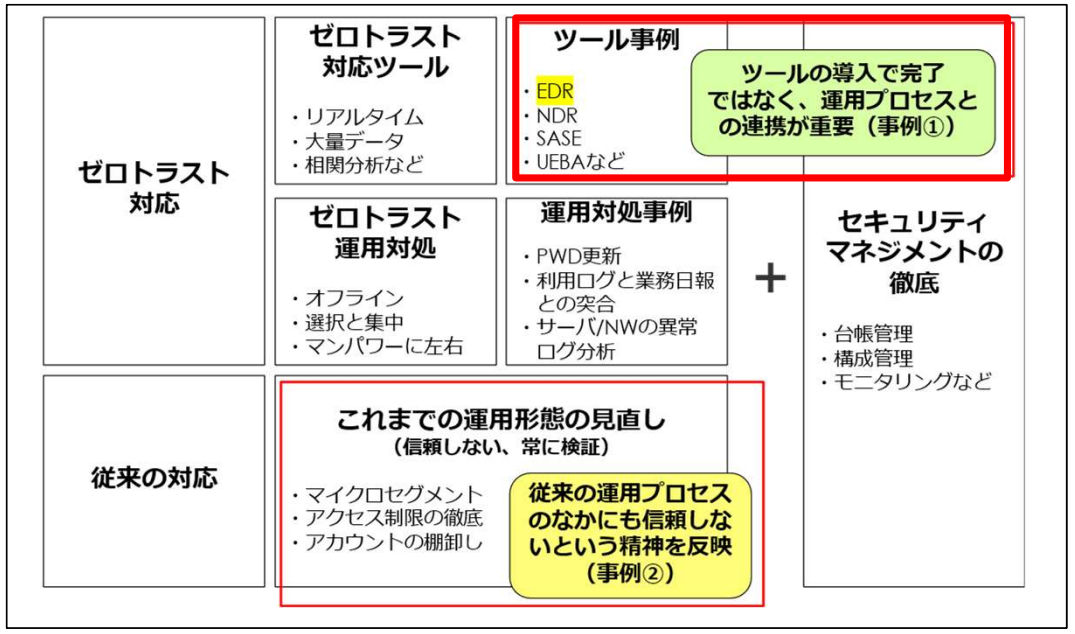
ゼロトラストのソリューションとISMSとの関係（連携）

①何を守るのか？、どのように守るのか？

②技術とマネジメントシステムという両輪

技術
運用
＋
マネジメント



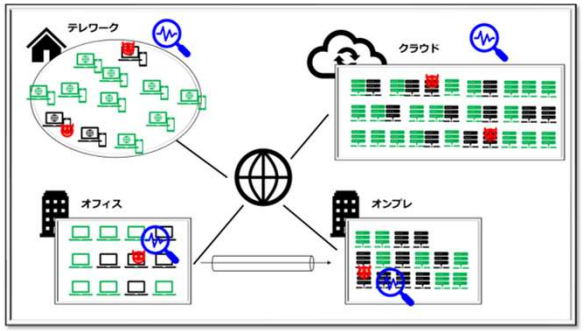


ISMS（マネジメントシステム）との関係（技術とマネジメントシステムという両輪）

ツールを有効活用するためには

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（サーバ、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

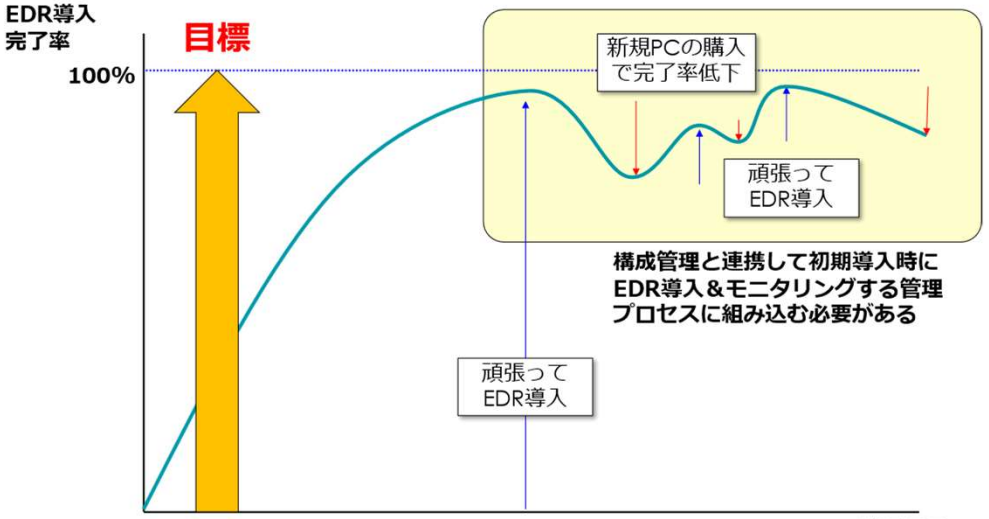
EDRなどのシステムを導入したら終わりではなく、それらを機能させるためのプロセス作りが重要！

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

マネジメントシステムとの連携が重要

EDR導入完了率100%を目指すためには？



まとめ（伝えたいこと）

Point1

・何を守るのか？、どう守るのか？、どこまで守るのか？
・考え方については今も昔の変わらない
・ただ、置かれた環境が変わったことを認識する必要がある
（境界線の中は安心という常識は非常識となった→安全神話の崩壊）

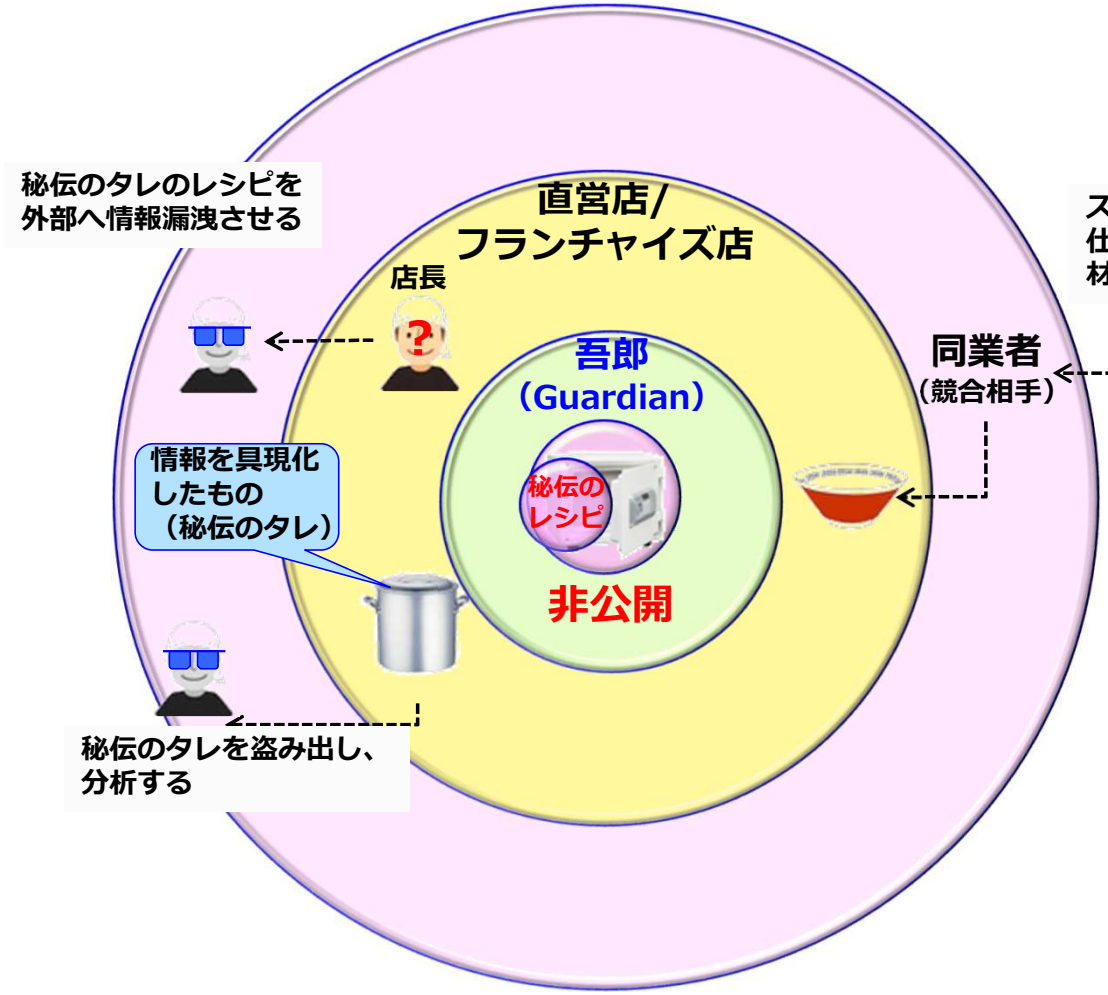
Point2

・昔は手間ひま掛けていたことが現在はツールで対応可能
・ツールを利用することでセキュリティ対策が実施出来るだけでなく
ビジネスの利便性を確保出来る
→ビジネスとセキュリティのバランスが両立させるポイントを
調整することが可能（次スライドで説明）

事例①

何を守るのか？、何から守るのか？　・・・　秘伝のタレ（営業秘密）

守るべき資産の特定とステークホルダーの関係を下記に整理する



**従業員、取引先など
システム面では守れ
ない側面も意識する
必要がある！**

まとめ（伝えたいこと）

Point1

・何を守るのか？、どう守るのか？、どこまで守るのか？
・考え方については今も昔の変わらない
・ただ、置かれた環境が変わったことを認識する必要がある
（境界線の中は安心という常識は非常識となった→安全神話の崩壊）

Point2

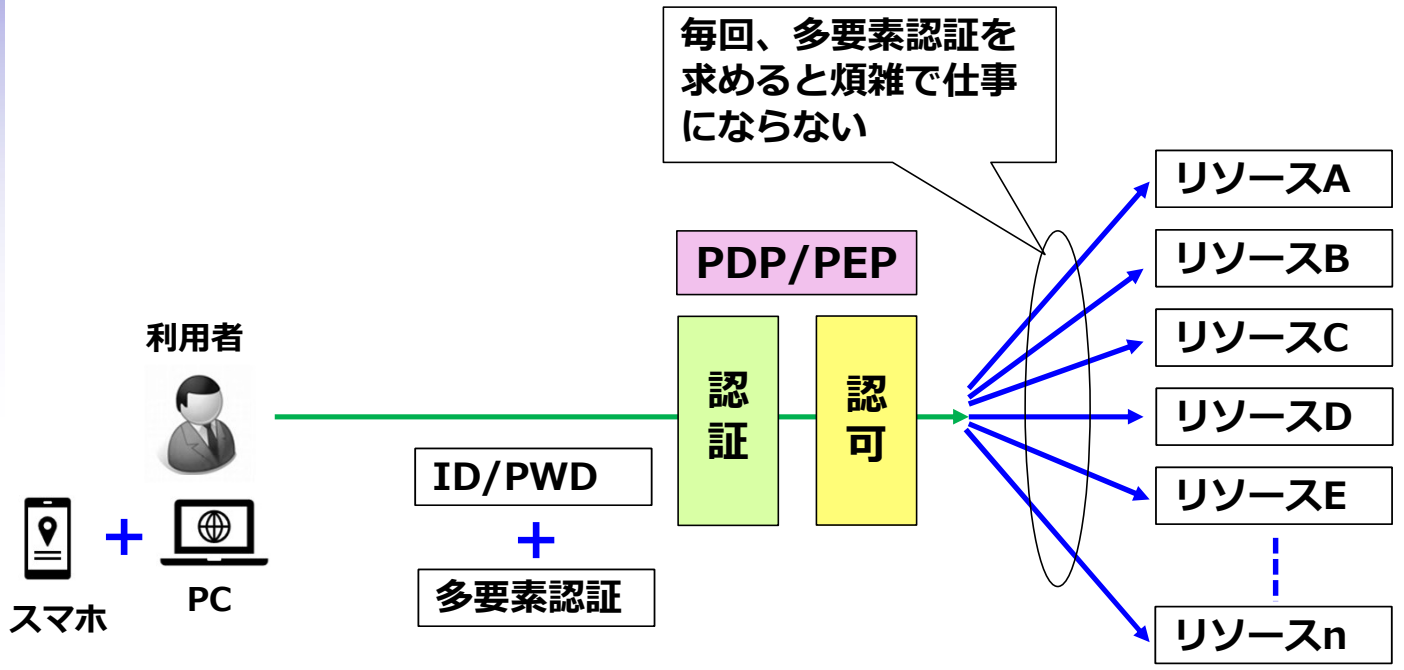
・昔は手間ひま掛けていたことが現在はツールで対応可能
・ツールを利用することでセキュリティ対策が実施出来るだけでなく
ビジネスの利便性を確保出来る
→ビジネスとセキュリティのバランスが両立させるポイントを
調整することが可能（次スライドで説明）

Point2：ビジネスとセキュリティのバランスの両立が大事

ビジネスとセキュリティとのバランスについて多要素認証を事例に確認する

✕：厳密性を求めて毎回、多要素認証を求めて煩雑にする？

◍：一定の法則（レーティングなど）でビジネスを阻害しない範囲で認証情報を求める

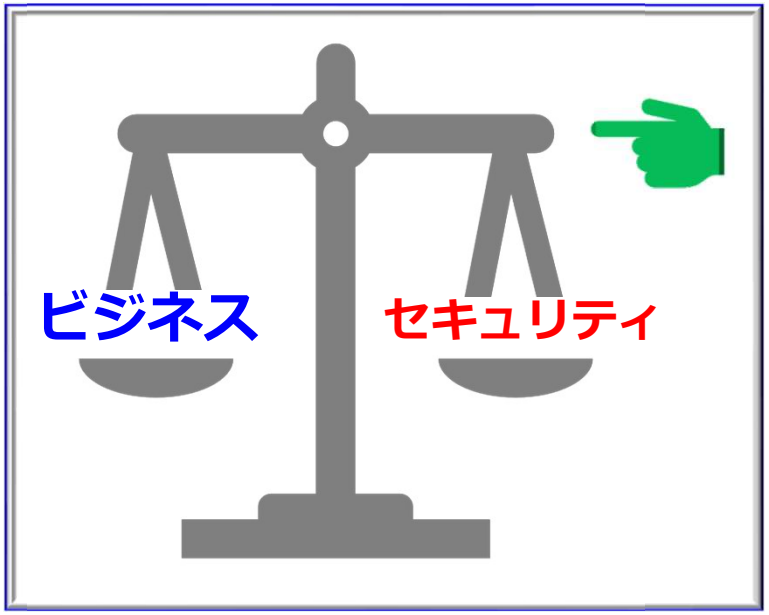


ビジネスとセキュリティのバランスを両立させるポイントを調整することが必要

最後に伝えたいこと

バランスと協調

ビジネスを阻害しない



技術とマネジメント

ご清聴ありがとう
ございました