最近のセキュリティ脅威と対策の方向性

～多角的アプローチから求める最適解

BITS 2016

NIHON UNISYS GROUP BUSINESS & ICT STRATEGY FORUM

Foresight in sight

UNISYS

日本ユニシス株式会社
セキュリティ技術部
真田 大志

1 最近のセキュリティ脅威

- 情報セキュリティからサイバーセキュリティへ
- 情報セキュリティの負の側面
- サイバーセキュリティが重視される背景
- サイバーセキュリティ対策とは
- 社内ネットワークにおけるサイバーセキュリティ対策
- 企業に対する官公庁の対応
- サイバーセキュリティ対策の組み合わせ

2 セキュリティ対策の方向性

- 人的な対策
- 技術的な対策
- 多角的なアプローチと最適な設計の必要性

1 最近のセキュリティ脅威

情報セキュリティからサイバーセキュリティへ

Foresight in sight

- 2000年に発生した官公庁を含む多くのホームページ改ざんや情報漏えいを受けて情報セキュリティ対策が注目されたのち、標的型攻撃の流行等を受けてサイバーセキュリティ対策が注目されている。

情報セキュリティ

- **情報セキュリティとは、情報の機密性完全性および可用性を維持すること**
- **2000年に発生したセキュリティ事件を背景に情報セキュリティポリシーなどを策定する企業が増加**

企業内のセキュリティ維持

サイバーセキュリティ

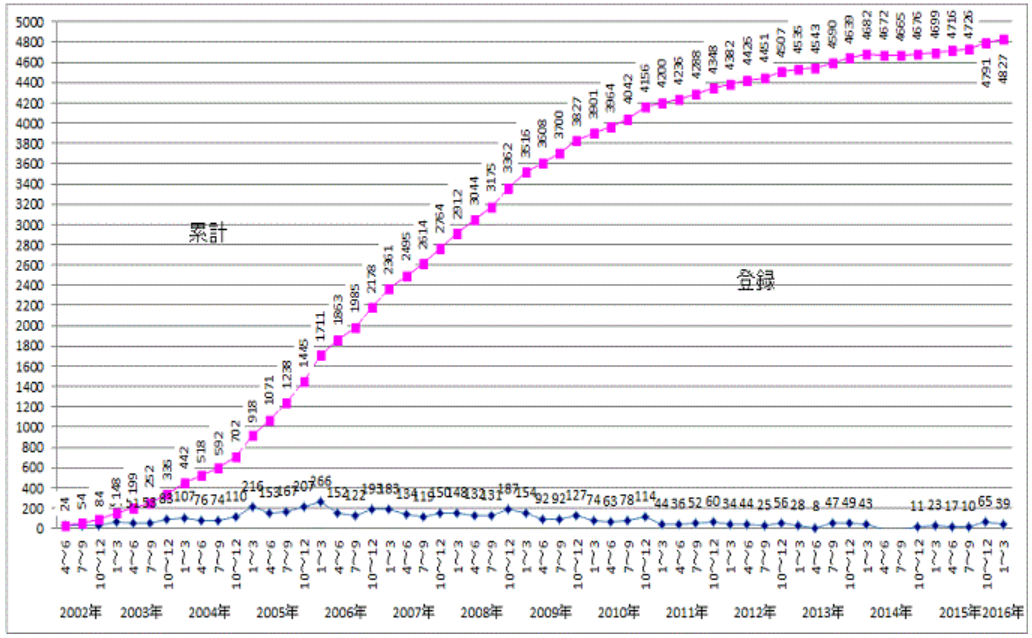
- **サイバーセキュリティとは、データ、システム、ネットワークの安全のために必要な措置がとられ、維持管理されていること**
- **重要インフラを含む標的型攻撃の増加を背景にサイバー空間のセキュリティ対策を国主導で法律として制定**

国策としてのセキュリティ維持

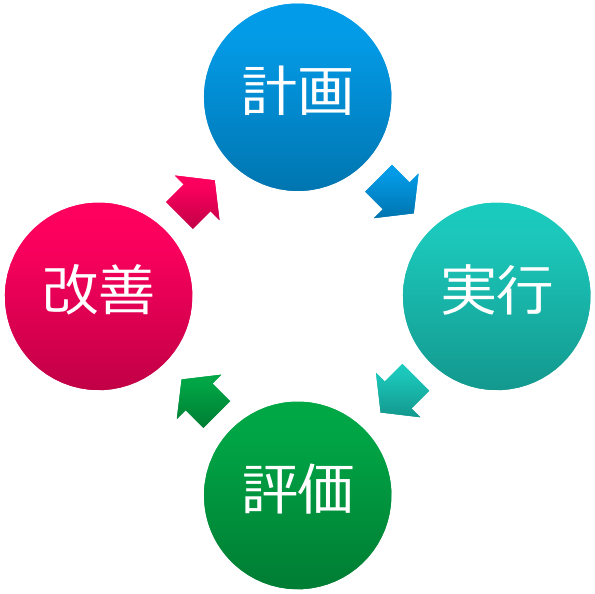
情報セキュリティの負の側面

- 情報セキュリティ対策として注目されたISMS（情報セキュリティマネジメントシステム）の構築・運用であるが、日本国内ではセキュリティポリシー策定やISO/IEC27001認証の取得といった「管理する仕組み」を作ることのみがゴールとする傾向が強くなったと考える。

ISMS（ISO/IEC27001）認証取得組織数推移



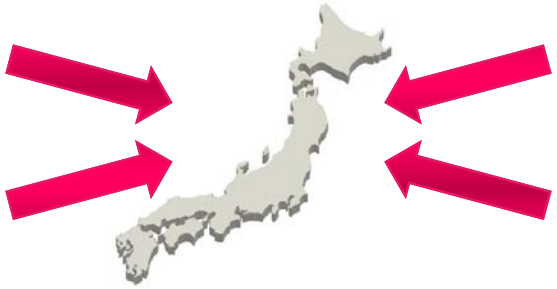
出典：JIPDEC http://www.isms.jipdec.or.jp/lst/ind/suii.html



サイバーセキュリティが重視される背景

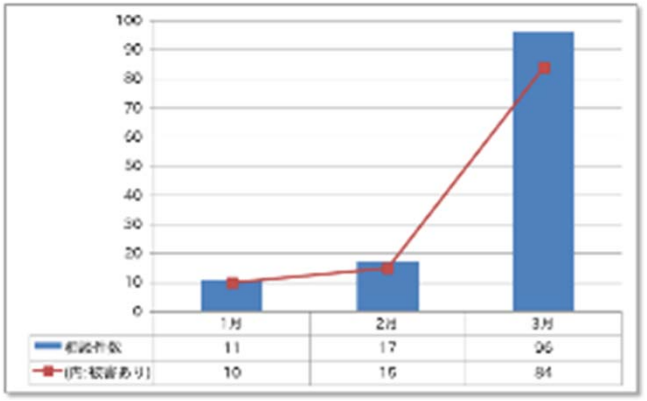
- 近年の高度化されたサイバー攻撃によって、企業でのインシデントが多発したことから、「管理する仕組み」だけではなく実効性の高い技術的な対策を含む対応が求められている。

正規サイト汚染による被害



- ✓ **日本国内から数百万件のアクセスが誘導**
- ✓ **不正広告、標的型メールの標的は日本に**

ランサムウェア感染被害の拡大

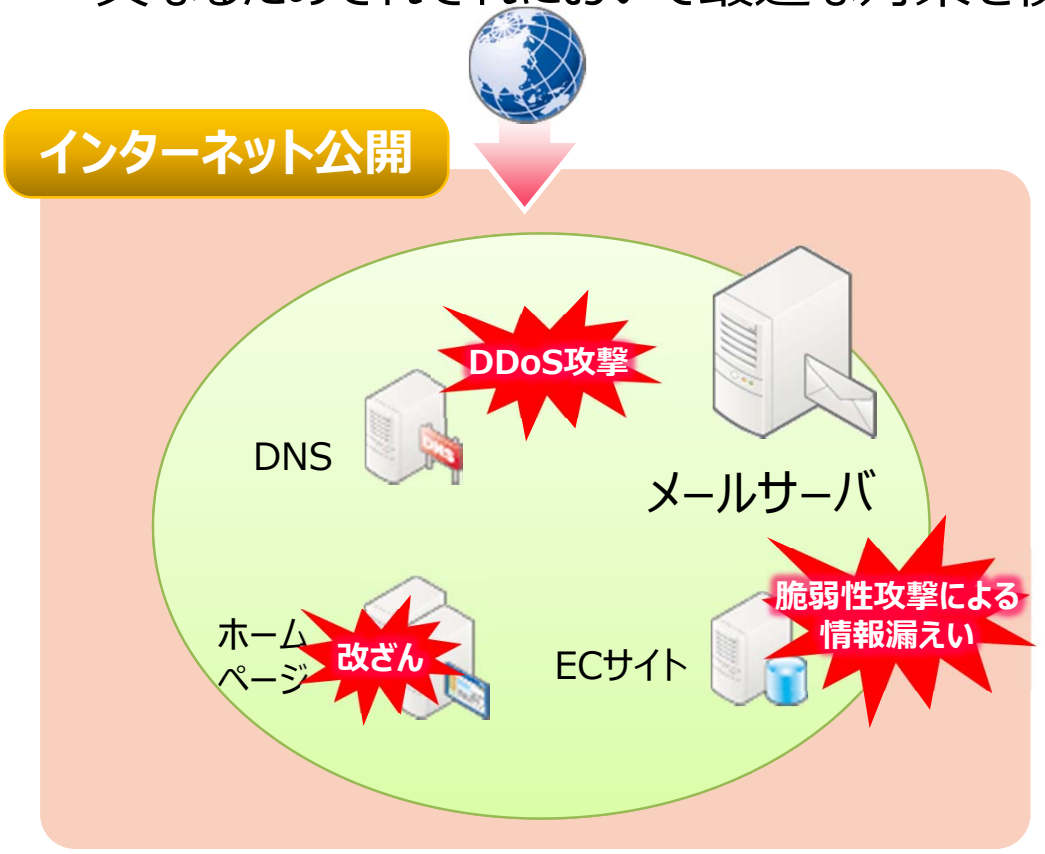


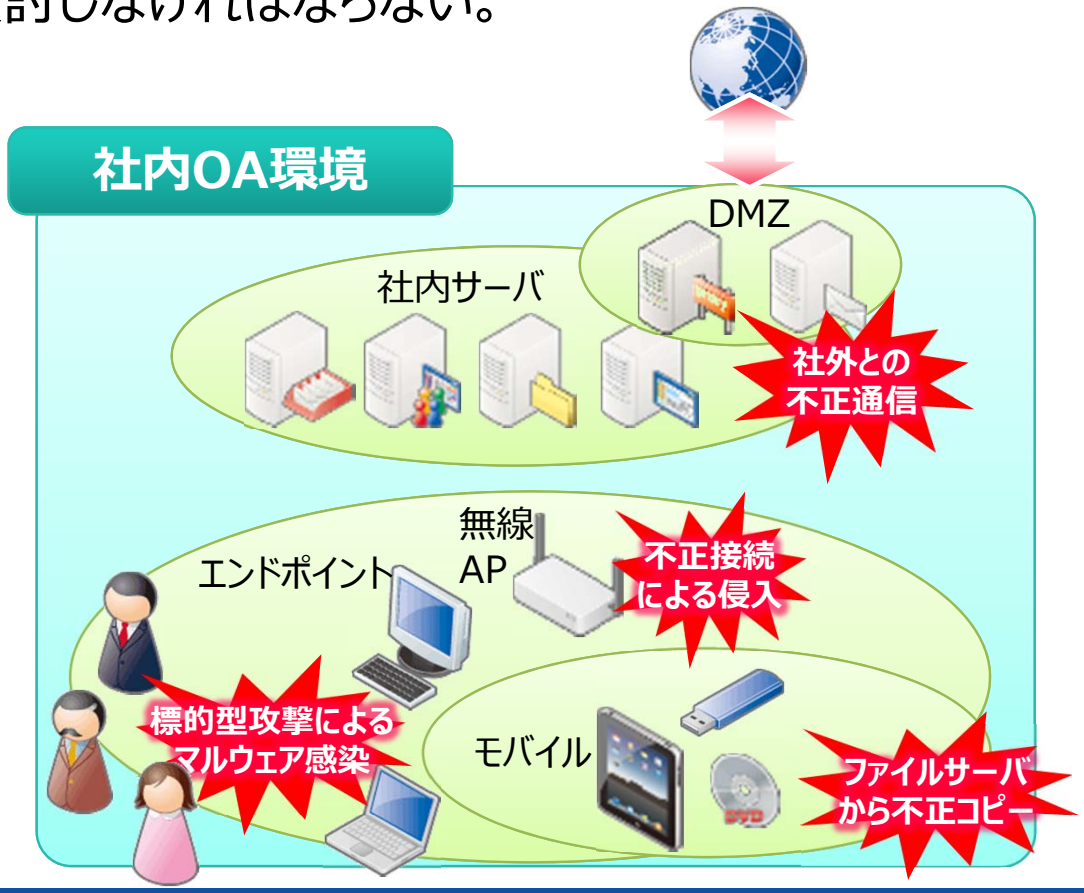
出典：情報処理推進機構　https://www.ipa.go.jp/security/topics/alert280413.html

既存の対策では防げない攻撃への技術的な対策として、
サイバーセキュリティ対策が重要となる。

サイバーセキュリティ対策とは

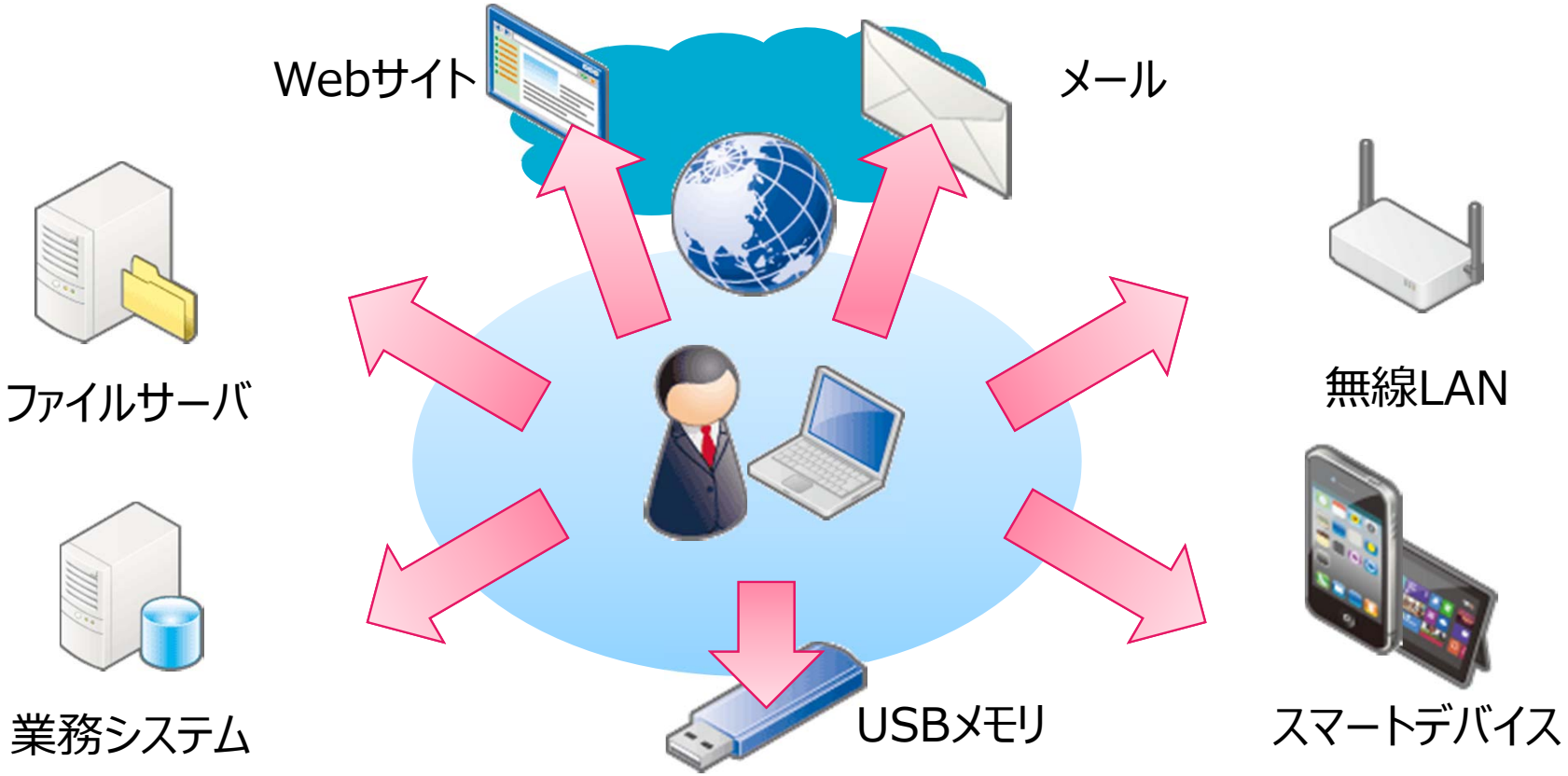
- 企業におけるサイバーセキュリティ対策はネットワーク形態により２つに分けられ、脅威が異なるためそれぞれにおいて最適な対策を検討しなければならない。





社内ネットワークのサイバーセキュリティ対策

- インターネットへ単一のサービスを提供しているサーバと違い、OA環境のクライアントは様々な利用方法があり制限をかけにくいため、防御することが難しい。



企業に対する官公庁の対応

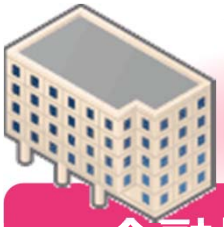
Foresight in sight

- サイバーセキュリティ基本法に基づくサイバーセキュリティ戦略を受けて官公庁、関連機関からは対策のガイドラインが提示されている。

経済産業省

サイバーセキュリティ経営ガイドライン

- サイバーセキュリティ経営の3原則
- サイバーセキュリティ経営の重要10項目



金融庁

金融検査マニュアル

- サイバーセキュリティ対策の強化

総務省

情報通信白書

- サイバーセキュリティ対策の推進

サイバーセキュリティ対策の組み合わせ

- サイバーセキュリティ対策は、その特性上「人的な対策」「技術的な対策」にわけられる。

セキュリティ事件・事故は増加の一途

- 従来のセキュリティ対策では通用しない事案が増えてきており、見直しが必要

サイバーセキュリティ対策

人的な対策

- 人材育成
- 監視・分析
- インシデント対応

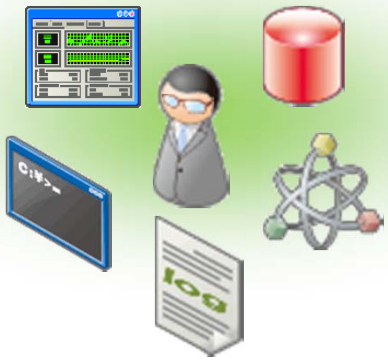
技術的な対策

- ネットワーク分離
- 多層防御

2 セキュリティ対策の方向性

人的な対策

- 「人による対策」とは機械化できない対策であり、技術的な対策のように攻撃手法によって実施しなければならない対策が変わるようなものではなく、普遍的なセキュリティ対策である



監視・分析

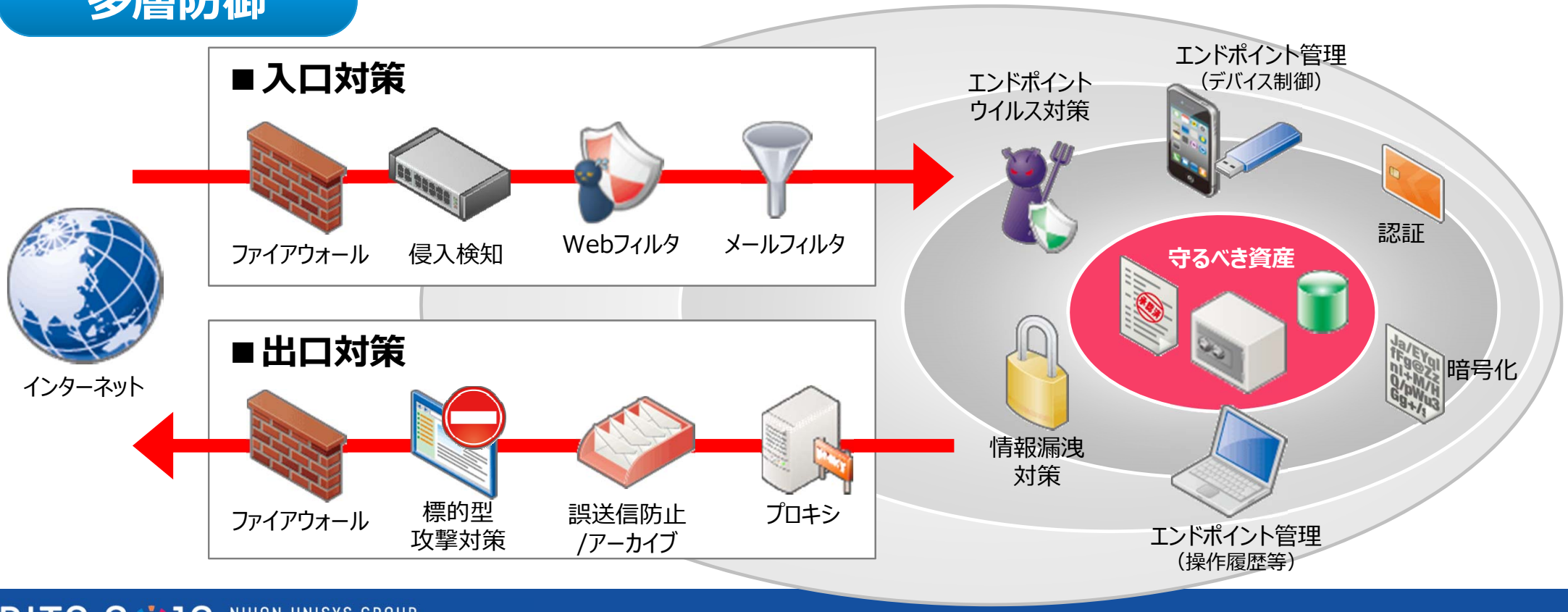
インシデント対応

人材育成

技術的な対策　－多層防御－

- 多層防御の目的は、重要なデータの漏洩やシステム停止を防ぐために多層の防御によって攻撃を検知し、影響を抑えることにある。

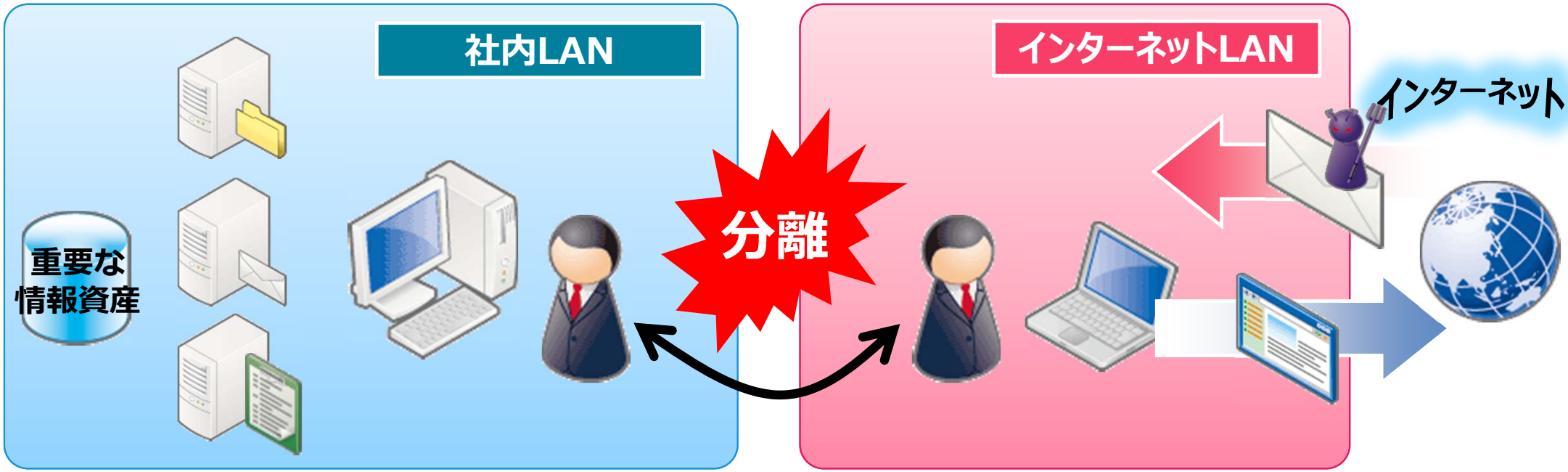
多層防御



技術的な対策　－境界防御①－

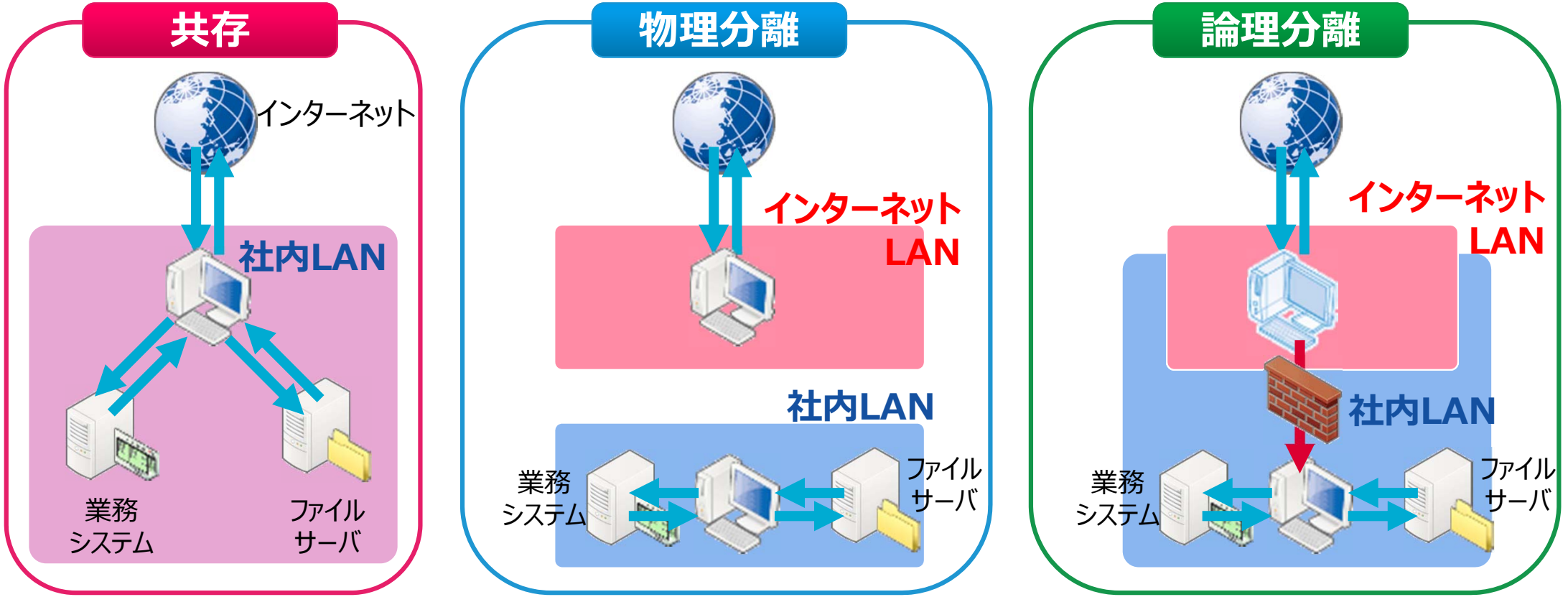
- 境界防御とはネットワークの「分離」である。脅威の大多数はインターネットを経由して侵入されるケースが多いため、これを根本的に排除するのが狙いとなる。

ネットワーク分離



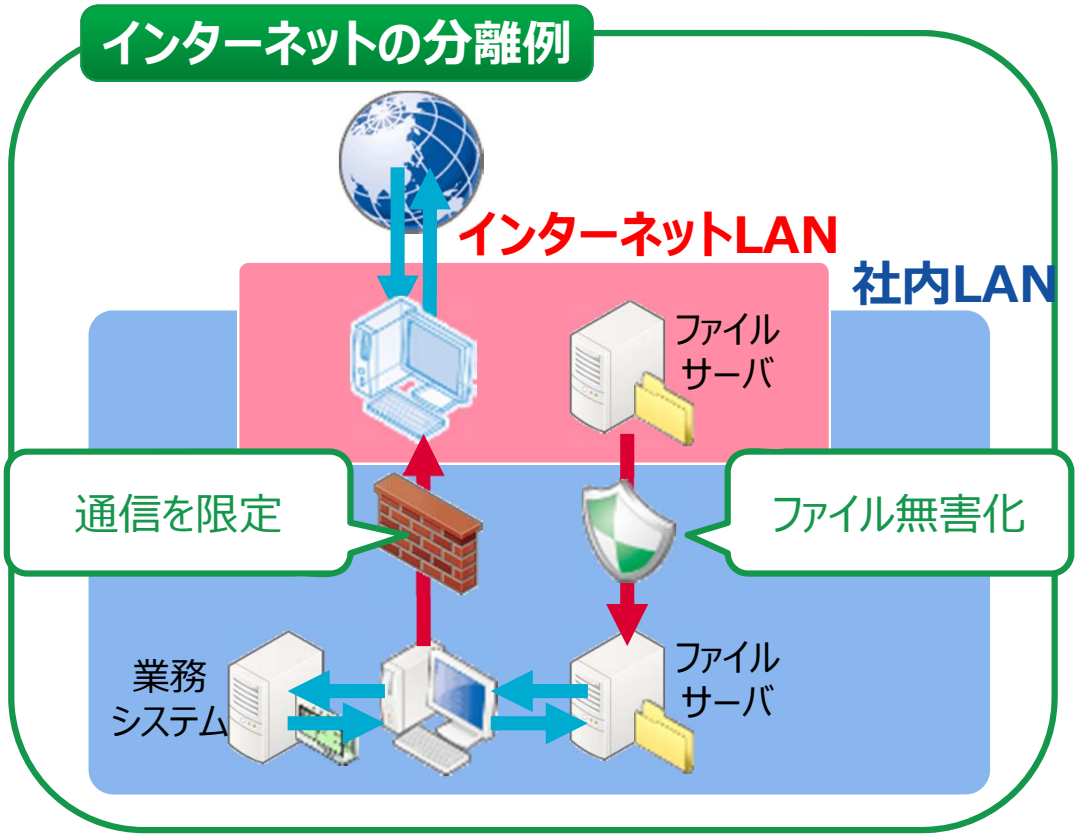
技術的な対策　－境界防御②－

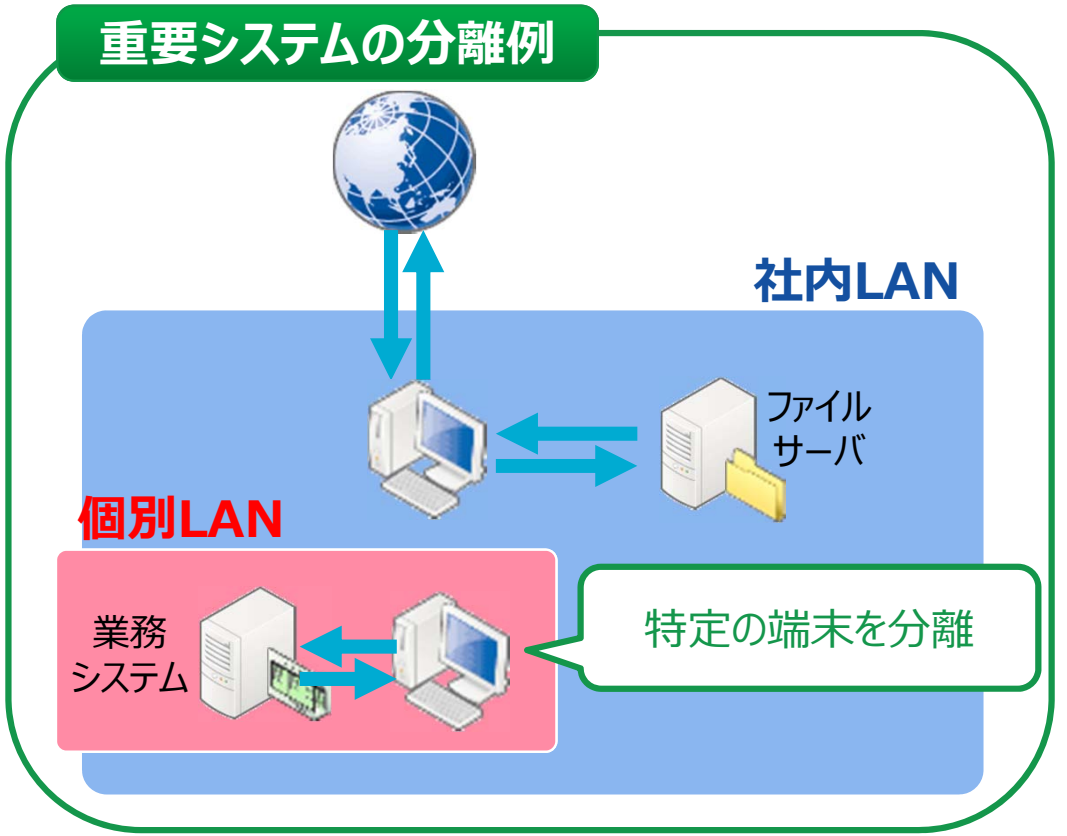
- インターネットへ接続可能なネットワーク環境を分離する方式としては、「物理分離」と「論理分離」に分けられる。



技術的な対策　－境界防御③－

- 論理分離を行うにあたっては、業種・業態等によって脅威の元である「インターネット」を分離するか、守る対象である「重要システム」を分離するかを検討する。





技術的な対策　－境界防御④－

- 各分離方式にはそれぞれ特徴があるため、求める「安全性」「コスト」「インターネット利用形態」によって最適な方式を選択する必要がある。

分離方式		メリット／デメリット
物理分離		■ インターネットからの侵入を完全に防ぐことが可能 ■ 社内LAN側のOS/APのパッチ更新、ウイルスパターンファイル更新を考慮する必要あり
論理分離	**インターネットの分離**	■ 端末統合による利便性向上（1人一台の端末でよい） ■ 構成の複雑化による運用負荷の増大 ■ 業務形態によってはクライアント仮想化の導入コスト増大
	重要システムの分離	■ インターネットからの侵入をほぼ完全に防ぐことが可能 ■ 現状のネットワーク構成からの移行が容易 ■ システム間連携がある場合には考慮が必要

多角的なアプローチと最適な設計の必要性

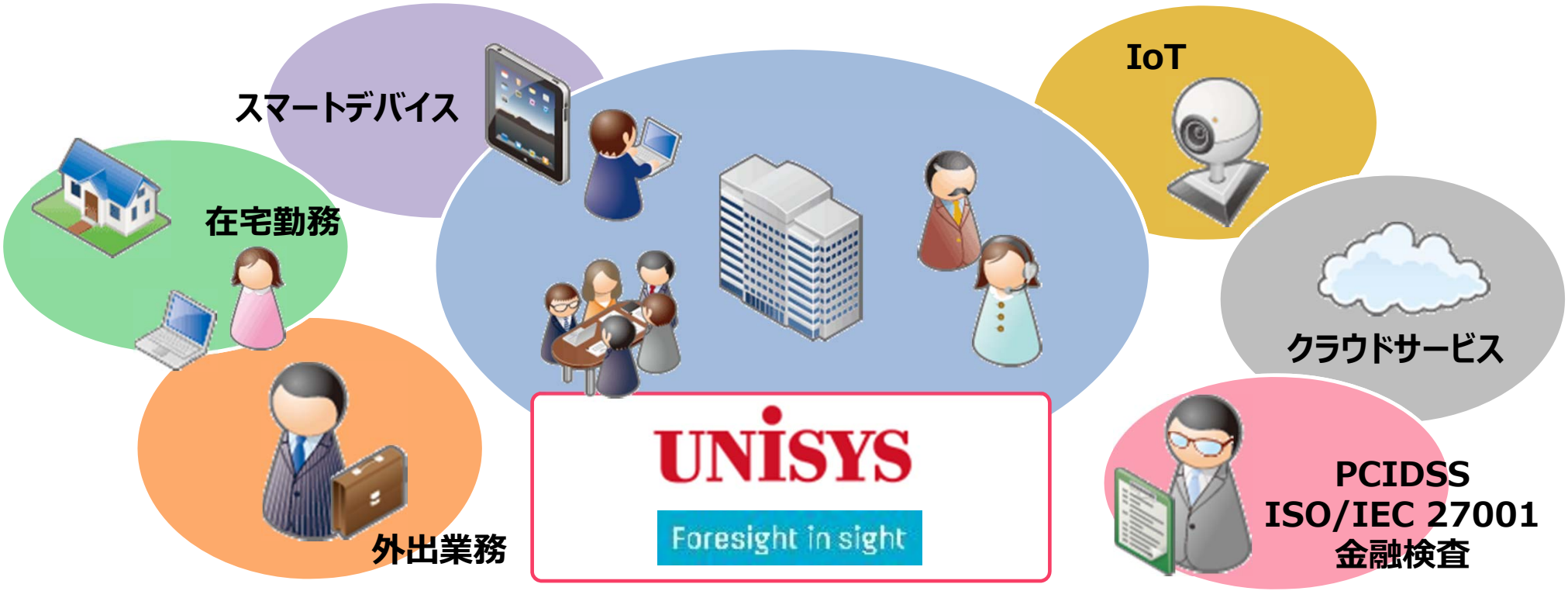
Foresight in sight

- これらの対策は相互に関連があり、技術的な対策と人的な対策のどちらが欠けても期待する効果を得ることはできないため、多角的にアプローチする必要がある。

多角的なアプローチと最適な設計の必要性

Foresight in sight

- 対策の実施においては現状の業種・業態、ワークスタイル、企業規模等、様々な要素を勘案したうえで最適な方式の選択、プロダクトの組み合わせを検討する必要がある。



Unisys Stealth　セキュリティの新しいカタチ

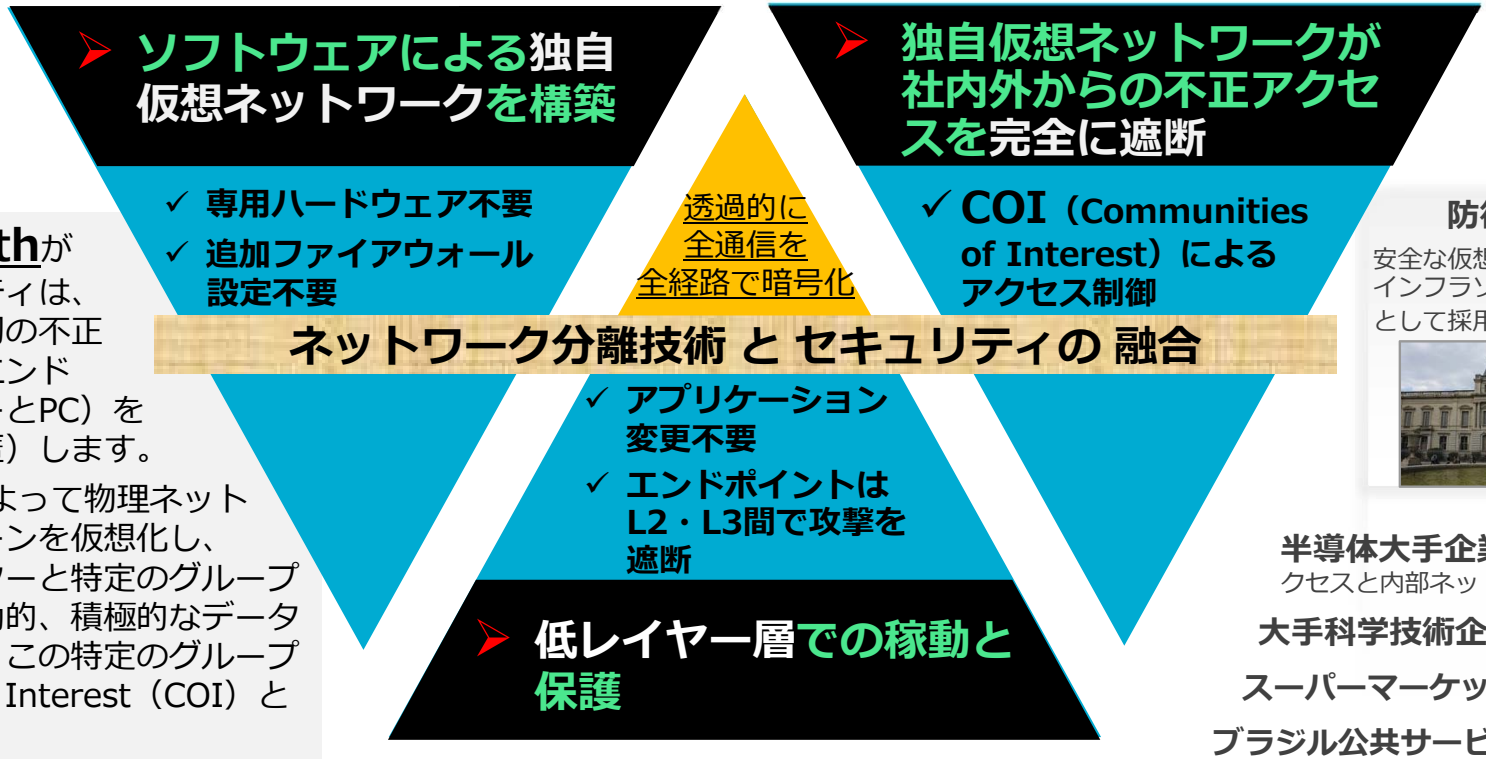
Foresight in sight

STEALTH by UNISYS

米国防総省の要請で開発されたUnisys Security
見えないものはハッキングできない

Unisys Stealthが提供するセキュリティは、暗号化によって一切の不正トラフィックからエンドポイント（サーバーとPC）をクローキング（隠匿）します。

Stealthは暗号化によって物理ネットワークのバックボーンを仮想化し、通信をデータセンターと特定のグループのみに制限して能動的、積極的なデータ保護を提供します。この特定のグループはCommunities of Interest（COI）と呼ばれます。



米国政府機関

Stealthで通信を保護。

防衛機関

安全な仮想デスクトップインフラソリューションとして採用。

医療機関

複数の病院間のデータ送信の安全性確保を実現。

半導体大手企業：仮想デスクトップへのリモートアクセスと内部ネットワークの分離で機密データを保護。

大手科学技術企業：工程管理環境と知的財産を保護。

スーパーマーケット：POS環境のPCI DSS順守に活用。

ブラジル公共サービス：各拠点間システム連携で安全にディスク・イメージ転送。

BITS 2016

NIHON UNISYS GROUP BUSINESS & ICT STRATEGY FORUM

Foresight in sight

UNISYS