経営レベルで考える最低限知っておくべきサイバーセキュリティ
～DXにおけるサイバーリスクとゼロトラストネットワーク～

GSX
GLOBAL SECURITY EXPERTS

グローバルセキュリティエキスパート株式会社

取締役　西日本支社長

兵庫県警察サイバーセキュリティ対策アドバイザー

三木　剛

2020年度までの実績一覧

GSX
GLOBAL SECURITY EXPERTS

脆弱性診断

20年に渡る業歴
3,000件以上
の診断実績
(業界を問わず)

標的型メール訓練サービス

年間約2,000組織
への実施実績
(業界を問わず)

セキュリティ監査

1,500件以上
の実施実績
(業界を問わず)

教育関連

中央省庁・独立行政法人・製造業
医療・エンタメを中心に、
実績多数

標的型攻撃対策ソリューション

証券・保険・消費者金融・
製造業・エンタメ・独法・メディア
・防衛・人材・会計・Sierなどを
中心にサンドボックス・SIEMの導入

CSIRT関連

証券・カード・消費者金融・
石油・Sier・医療・電力・
スーパーゼネコン・製造業

インターネットの脅威

IPA情報セキュリティ10大脅威　2021年度版

■「情報セキュリティ10大脅威 2021」

NEW：初めてランクインした脅威

昨年順位	個人	順位	組織	昨年順位
1位	スマホ決済の不正利用	1位	ランサムウェアによる被害	5位
2位	フィッシングによる個人情報等の詐取	2位	標的型攻撃による機密情報の窃取	1位
7位	ネット上の誹謗・中傷・デマ	3位	テレワーク等のニューノーマルな働き方を狙った攻撃	NEW
5位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	4位	サプライチェーンの弱点を悪用した攻撃	4位
3位	クレジットカード情報の不正利用	5位	ビジネスメール詐欺による金銭被害	3位
4位	インターネットバンキングの不正利用	6位	内部不正による情報漏えい	2位
10位	インターネット上のサービスからの個人情報の窃取	7位	予期せぬIT基盤の障害に伴う業務停止	6位
9位	偽警告によるインターネット詐欺	8位	インターネット上のサービスへの不正ログイン	16位
6位	不正アプリによるスマートフォン利用者への被害	9位	不注意による情報漏えい等の被害	7位
8位	インターネット上のサービスへの不正ログイン	10位	脆弱性対策情報の公開に伴う悪用増加	14位

ニューノーマルな状況から
サイバー犯罪被害が爆発的に広がっている

なぜ、サイバー犯罪被害が急速に広まり、止められないのか？

１．状況が変わった

２．犯人が変わった

３．変わったことに気づいていない

１．状況の変化

- **企業が急速にITの利活用**を始めた
- その結果、**価値のあるデータが散在**するようになった
- **テレワーク**で端末の管理が緩くなった

ネット環境とシステムが急拡大し、価値あるデータが散在

DXデジタルトランスフォーメーション

業務効率化
情報集約化
意思決定の迅速化
新規ビジネス創出

ネットの相互接続
システムの爆発的な拡大

価値あるデータ
が一気に精錬される

出入口の増加と
テレワークによる
端末の手薄な管理

2．犯人像の変化

- 攻撃手法や手口が一般化：犯罪インフラの発展
- **サイバー攻撃を「犯罪者」が金銭目的で行う**

日本を取り巻く脅威

サイト改ざん

不正ログイン

不正アクセス

ランサムウエア

不正送金

内部犯行

負荷攻撃

標的型攻撃

攻撃手法が多様化しており、企業、個人として
どこまで対策すべきか頭を抱えている・・・

ニュースに出てこないインシデント（事故）

ランサムウエア
ビジネスメール詐欺
システム、工場停止

これらは自社被害のためニュースになり難い
しかし情報漏洩よりもインパクト、企業リスクが大きい

さらにテレワークで何が問題になっているか？

在宅ワークなどを含むテレワークでは、次の様な脅威が増えます。

端末の紛失/盗難
誤操作
不正行為
マルウエア感染

気持ちの緩み x 攻撃者のターゲット

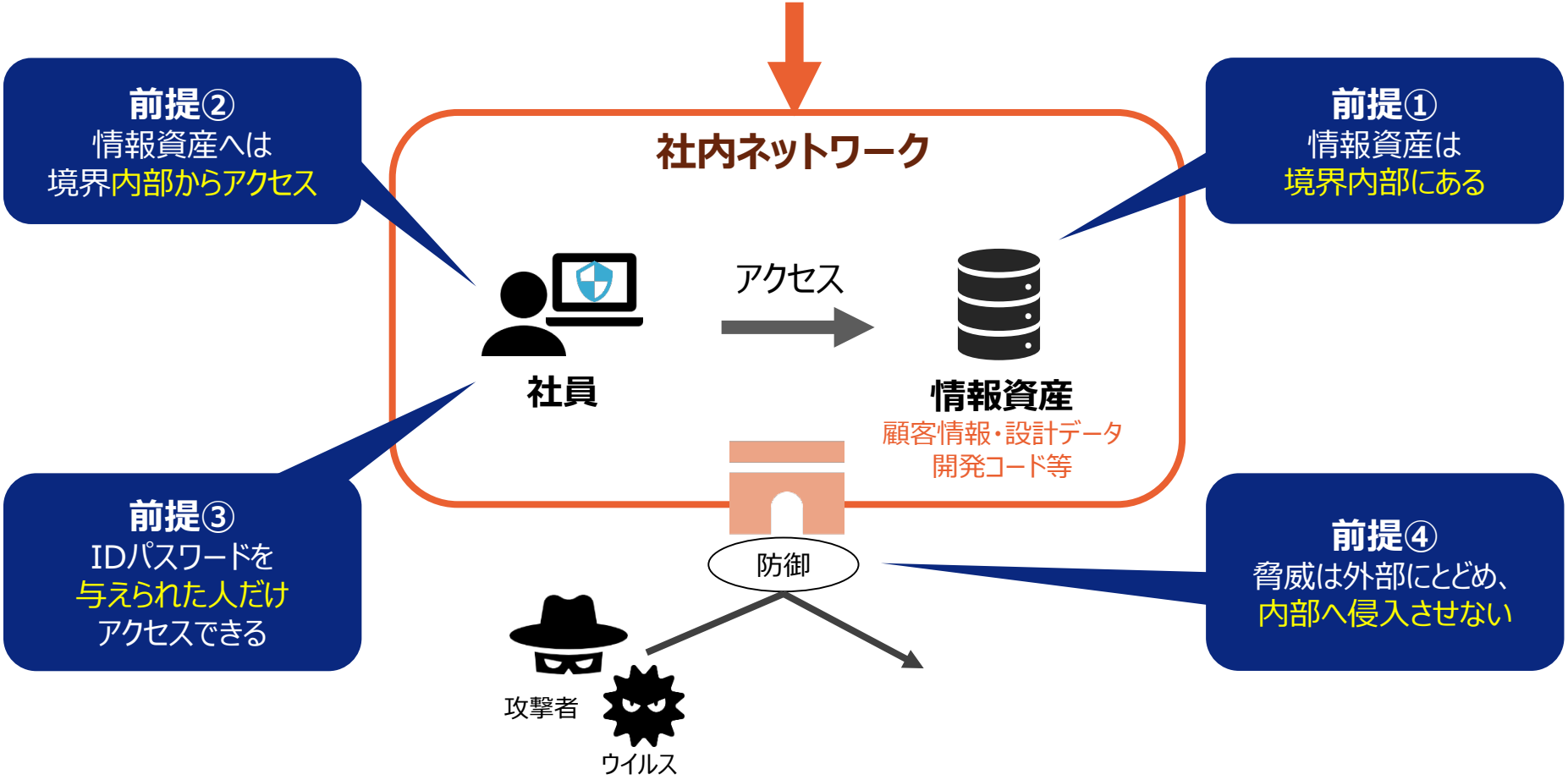
サイバーセキュリティにおける企業の最大のリスクは
「情報漏洩」よりも「事業継続の妨げ」にある

もはや経営課題でしかない

境界防御の限界

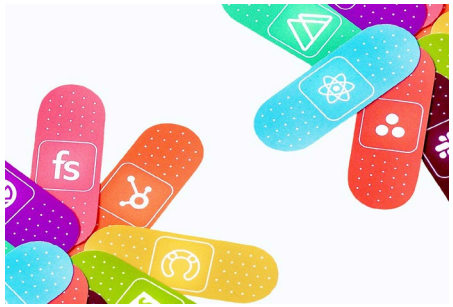
これまでのセキュリティ対策

これまでのセキュリティ対策は、**境界防御**でした。

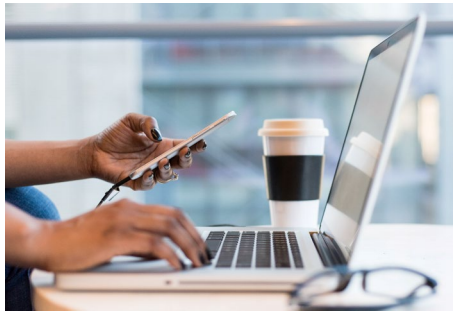


「社内ネットワークの中は安全であり、信頼できる」という考え方

IT環境の3つの変化と今直面している課題



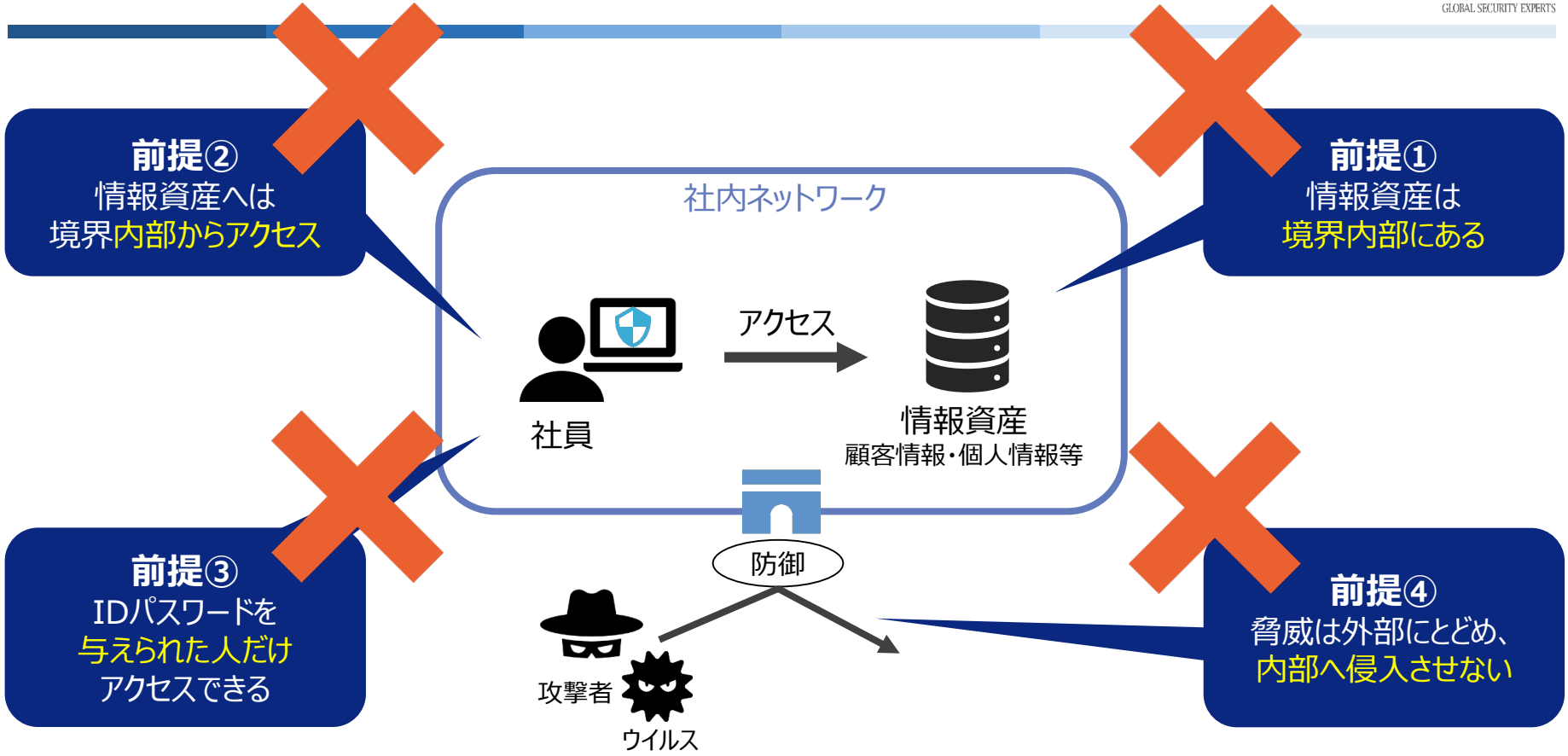
1. システムのクラウドサービスへの移行



2. テレワークへの移行

3. サイバー犯罪の高度化/頻発化

境界防御だけで脅威に立ち向かうには限界がある



「社内ネットワークの中は安全であり、信頼できる」という考え方から
「信頼できるネットワークは存在しない」という考え方へ。
これがゼロトラストの根本となる考え方です。

全ての会社に必要なセキュリティ対策

GSX
GLOBAL SECURITY EXPERTS

全社員の意識啓発と事故を想定した訓練

情報資産の棚卸し と 対策のロードマップ

多層防御からゼロトラストへの仕組み化

セキュリティ担当、専門部署の設置

上記4項目は全て **厚労省**の**監督指針・還元資料**や**報告書**
また経産省のサイバーセキュリティ経営ガイドライン に明記

セキュリティ対策の進め方

防犯意識とリスク認識を共有 ①

守る情報を特定 ②
リスクアセスメント
何を守るか？を明確にしリスクを見える化

対策ロードマップ

組織体制 ③
脅威を早期に分析し、対処する仕組の構築(社内体制)

仕組み化 ④
驚異を可視化する仕組の導入
(センサー/分析基盤/監視基盤)

教育・訓練による、意識と運用の定着 ①

①教育＆アウェアネス向上
階層別研修
標的型メール訓練
E-Learning
インシデント対応演習

②アセスメント
リスクアセスメント
脆弱性診断/AD診断
ペネトレーションテスト
ロードマップ策定支援
セキュリティ監査

③組織構築＆改革
セキュリティ人材育成
CSIRT/PSIRT構築
ポリシー作成/更新
脆弱性管理体制構築
（内製化）
運用チーム構築/要員派遣

④システム導入＆運用
EDR/MDR
SWG/CASB/SASE
SIEM/UEBA
各種開発/導入/運用
緊急対応（フォレンジック）

最後に

Ｆ１は早さを極めるために、エンジンの研究開発と共に、ブレーキ性能の開発も重点的に行っています。
企業も同様、DXを進めると同時にセキュリティへの投資を同じくして行う必要があります。
ブレーキ性能を高めて、大事故にならないように。

GSX

GLOBAL
SECURITY
EXPERTS