CYBER INITIATIVE TOKYO | 2022

重要インフラを狙うサイバー攻撃の脅威！「選択」と「集中」で、全拠点を守る

日本アイ・ビー・エム株式会社
セキュリティー事業本部
戦略事業推進部
理事　山下 慶子

IBM Security

IBM

山下 慶子(やました のりこ)

GICSP, CISSP, CISA, CISM

- 外資系ソフトウェアハウスにて、オペレーティング・システム開発
- 国内セキュリティー・ベンダーにて、セキュリティーログ分析業務に従事
- 外資系セキュリティー・ベンダーにて、高度標的型攻撃製品の
  プリセールスを公共組織向けに担当
- コンサルティング・ファームにて、セキュリティー・プロジェクトをリード
- 2018年にIBMへ入社
  戦略クライアント（製造・公共担当）向け
  セキュリティー・サービス・製品の提案・デリバリを推進
- 2022年より現職
  戦略事業推進部にて、IBM Securityの戦略事業を牽引

IBM Security X-Force 脅威インテリジェンス・インデックス 2022

IBM Security X-Force
Threat Intelligence
Index 2022

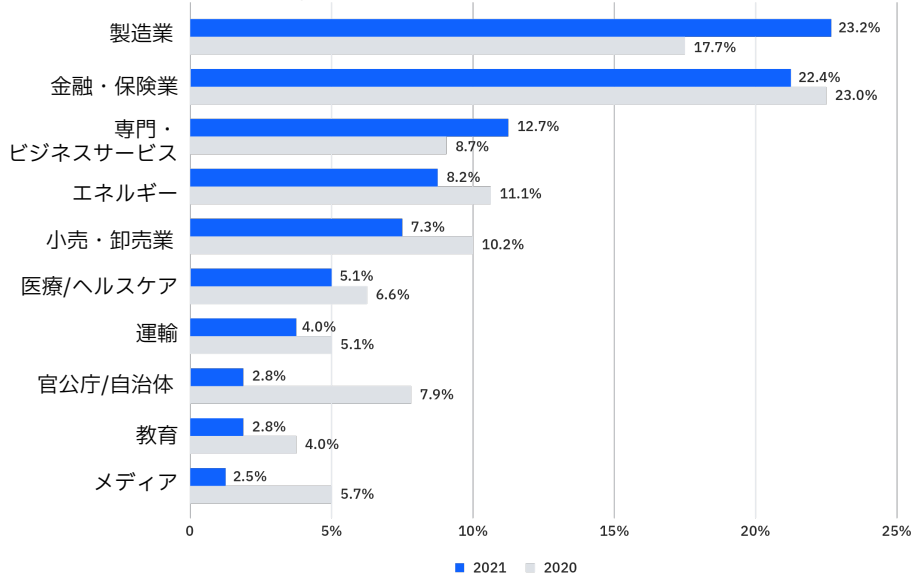
狙われている
重要インフラ・製造業

68.2%

重要インフラ・製造業は
狙われている

2021年のサイバー攻撃を受けた
産業上位10位のうち、
重要インフラと製造業を合せると
7割近くなります。

上位10位の産業への攻撃の内訳、2021年と2020年の比較
(出展：IBM Security X-Force)



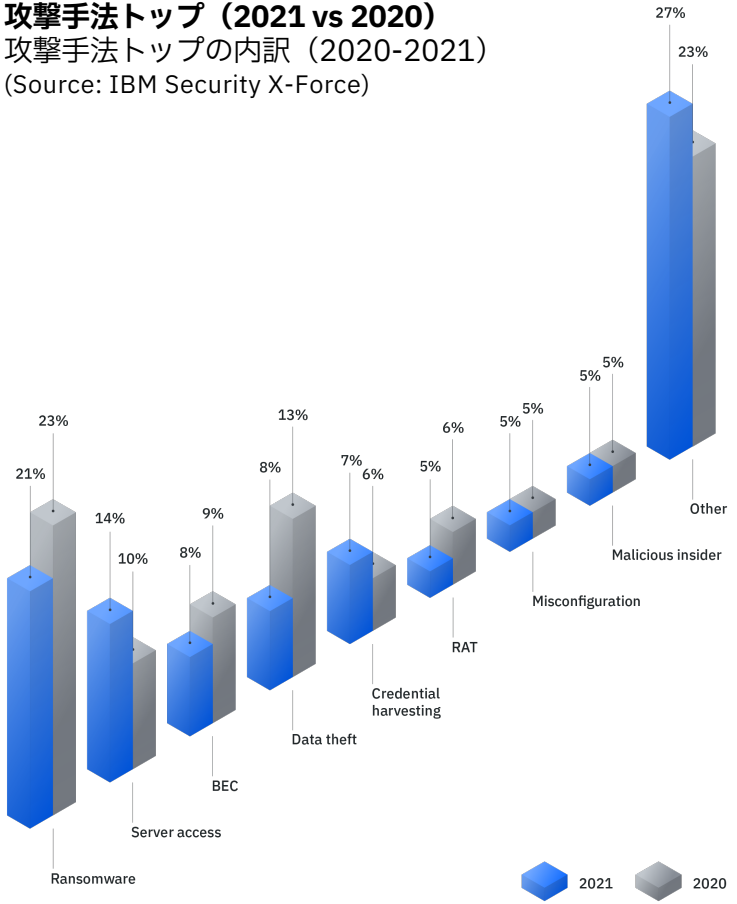
攻撃手法のトップは ランサムウェア

21%

ランサムウェアの攻撃の割合

ランサムウェアはX-Forceが2021年に確認した攻撃手法の第1位で、前年（2020年）の23%から21%に減少しています。

攻撃手法トップ（2021 vs 2020）
攻撃手法トップの内訳（2020-2021）
(Source: IBM Security X-Force)



サイバー攻撃の実例 1: 米国石油パイプライン企業への攻撃

2021年5月に発生した、米国の石油パイプライン企業に対するサイバー攻撃では、
攻撃の影響でパイプラインの操業が約5日間停止しました。

被害にあった会社　：Colonial Pipeline Co.

本社:ジョージア州アルファレッタ　設立:1961年
1日250万バレルの燃料をメキシコ湾岸のテキサス州から北東部のニューヨーク湾まで運ぶ。
東海岸で消費されるディーゼル、ガソリン、ジェット燃料の45%が、コロニアル・パイプラインで運ばれている。

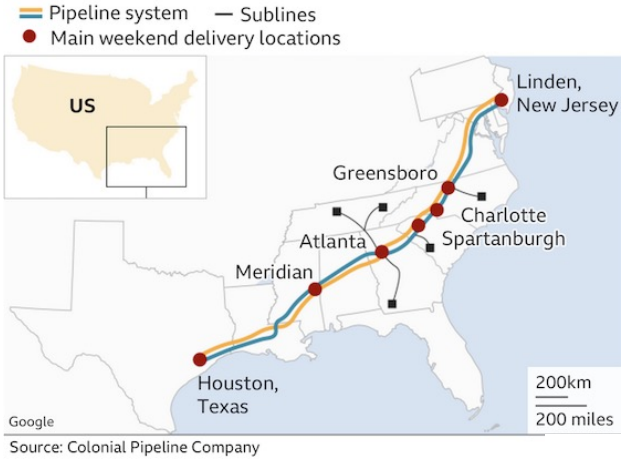
被害の概要

- ✓ 情報システムでランサムウェア感染が発生
- ✓ 100GBデータと引き換えに金銭を要求され支払い、その後FBIがほぼ回収
- ✓ 積極的な隔離を行なったことによりパイプラインが約5日間停止

攻撃の概要

- ✓ VPN装置に不正アクセスをされる
- ✓ 漏えいしたパスワードが利用された
- ✓ VPNは多要素認証が導入済みであったが、
  一部無効にされていたアカウントが悪用される

コロニアル・パイプラインの全体像



出展：https://www.bbc.com/news/business-57050690

サイバー攻撃の実例 2: あいつぐ医療機関への攻撃

2021年10月徳島の医療機関がランサムウェアに感染し、2カ月間診療が停止してしまいました。
2022年10月大阪の医療機関がランサムウェアに感染し、復旧に向けて対応中と報道されています。

何が起きた？

- はじまりは、VPNの脆弱性をついた不正アクセス
- ランサムウェアによるデータ暗号化→システム利用不可

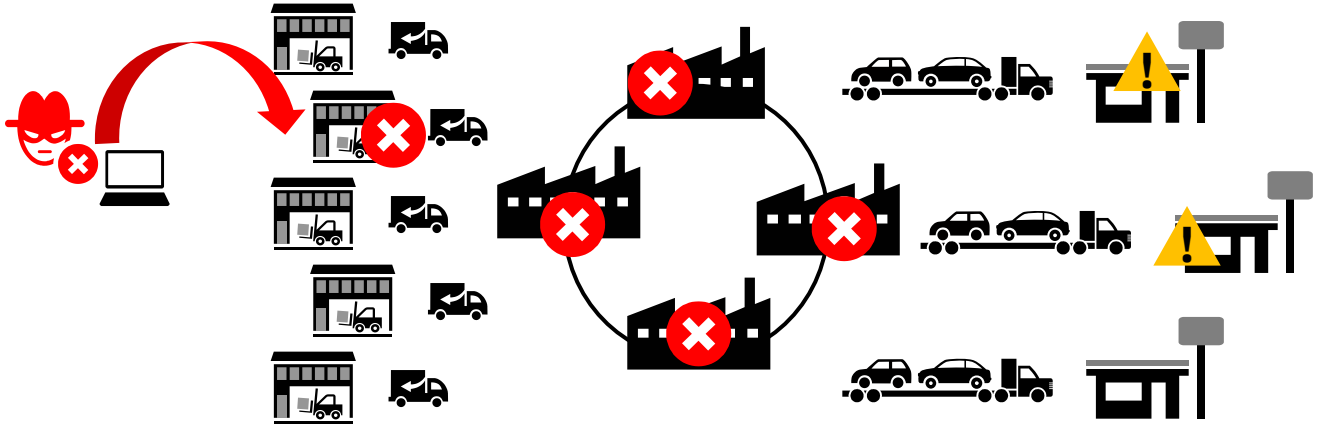
なぜ起きる？

- 電子カルテ導入が進み、インターネットにつながる
- IT担当者不在だったり、行き届かない運用・保守

サイバー攻撃の実例 3: 増加するサプライチェーンへの攻撃

2022年3月日本の自動車メーカーが生産ラインを停止することで、明らかになった取引先のサイバー攻撃。

- 取引先・関係会社とのConnectivityが進み、自組織のセキュリティーだけに注力すればよい時代ではなくなってきた
- 取引先や関係会社、子会社などを含んでの「Weakest Link」を把握することが重要



自社セキュリティー対策の見直し

- ✓ VPN装置・FW等外部接続機器のセキュリティー設定確認
- ✓ ランサムウェア対策の棚卸

取引先セキュリティー・ガバナンスの強化

- ✓ 契約・監査プロセスの整備
- ✓ セキュリティー対策の提供

サプライチェーン・セキュリティー

VPN

ランサムウェア対策

DX

OTセキュリティー

クラウド・セキュリティー

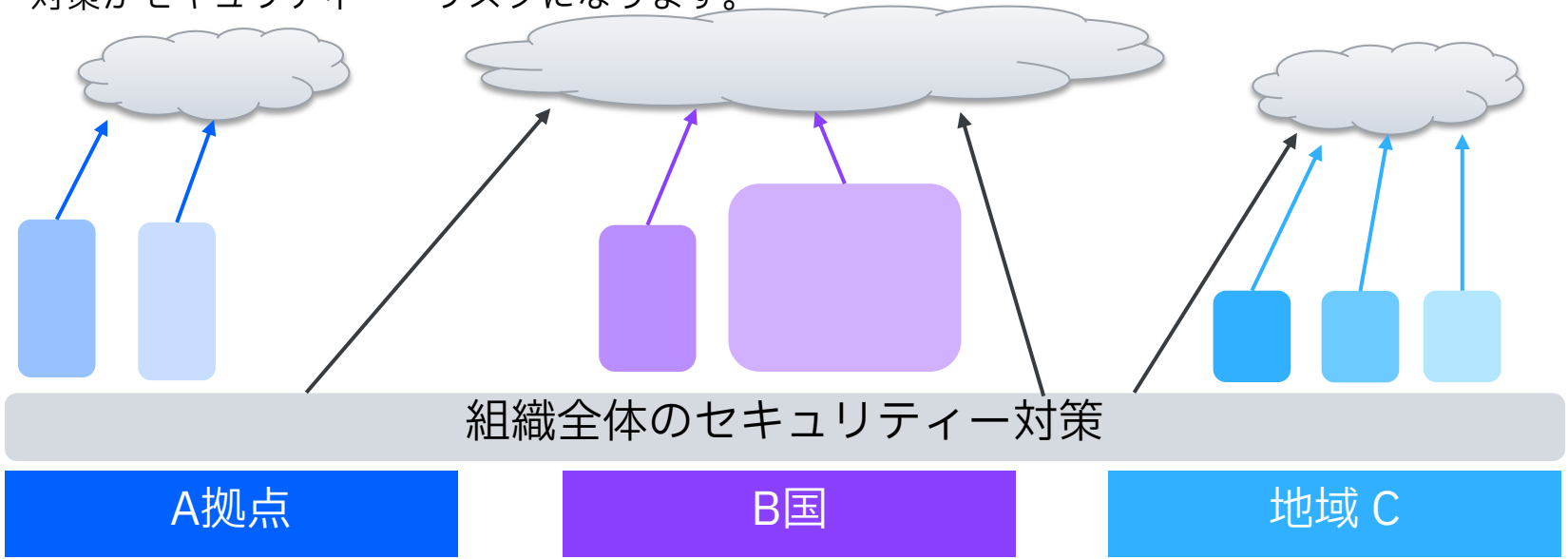
ゼロトラスト・セキュリティー

AI

いったい何を
どこまで？

攻撃者はWeakest Linkを狙う→グローバル企業の例

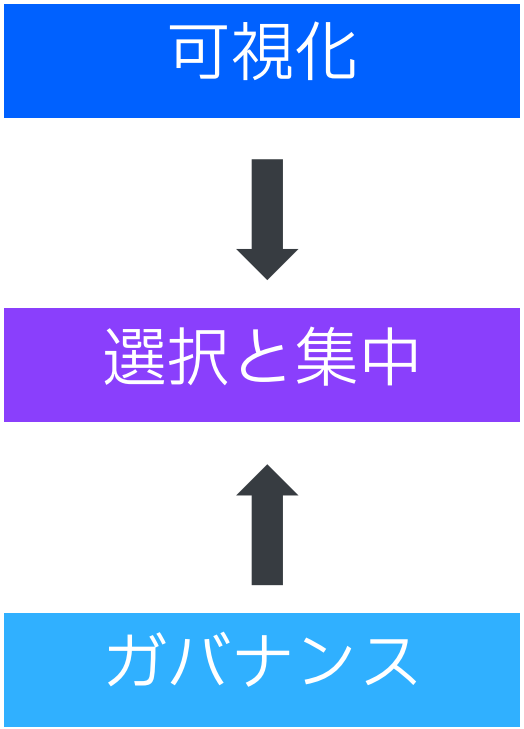
多くの海外拠点、異なる業態の事業を束ねるグローバル企業となると、事業部毎、地域（拠点）毎に、セキュリティー対策を実施しているお客様は少なくありません。乱立する事業部毎・拠点毎のセキュリティー対策がセキュリティー・リスクになります。



攻撃者は、
セキュリティー・レベルの最も低い場所（拠点・ネットワーク・サプライチェーン）
＝Weakest Link を狙いサイバー攻撃を仕掛けます。

ではWeakest Link をどうすればいいのか...

セキュリティーに費やせる予算には限りがあるのに、セキュリティー対策は次々を新しいものを提案され、何をどこまでやったらいいのかわからないというお客様に多くお会いします。



Weakest Linkを把握することが重要

選択と集中：すべてに同じレベルを求めない

拠点・部門まかせにしない組織統一の対策

可視化：Weakest Linkを把握する

Weakest Linkを把握するということは、自組織のセキュリティー・リスクを適切に認識することです。

Weakest Link を把握しているが、
対策にまで辿り着いていない

そもそも自組織のWeakest Linkが何なのか
把握できていない

可視化：Weakest Linkを把握する

Weakest Linkを把握するということは、自組織のセキュリティー ・リスクを適切に認識することです。

そもそも自組織のWeakest Linkが何なのか
把握できていない

机上アセスメント

- 守るべきデータはどこにあるのか？
- 守るべきライン（常時稼働システ
- すでに漏えいしている社内情報はないか？
- 対応していない脆弱性はないのか？
- インターネットにつながってるシステムは？
- ーク上つながってる？
- 子会社とはネットワーク上つながってる？
- 協力会社とはネットワーク上つながってる？

可視化：Weakest Linkを把握する

Weakest Linkを把握するということは、自組織のセキュリティー ・リスクを適切に認識することです。

そもそも自組織のWeakest Linkが何なのか
把握できていない

守るべきデータはどこにあるのか？

守るべきライン（常時稼働システム）？

すでに漏えいしている社内情報はないか？

対応していない脆弱性はないのか？

インターネットにつながってるシステムは？

脅威インテリジェンス・サービス

子会社とはネットワーク上つながってる？

協力会社とはネットワーク上つながってる？

可視化：Weakest Linkを把握する

Weakest Linkを把握するということは、自組織のセキュリティー ・リスクを適切に認識することです。

そもそも自組織のWeakest Linkが何なのか
把握できていない

守るべきデータはどこにあるのか？

守るべきライン（常時稼働システム）？

すでに漏えいしている社内情報はないか？

対応していない脆弱性はないのか？

インターネットにつながってるシステムは？

海外拠点とはネットワーク上つながってる？

子会社とはネットワーク上つながってる？

協力 ながってる？

脆弱性診断

ガバナンス：全てを集約する必要はない

国内関係会社、海外拠点・関係会社のセキュリティー管理態勢を検討する上で、どのようなガバナンスを効かせていくか。自社にとって最適なセキュリティー・ガバナンス体系の検討が重要なカギです。

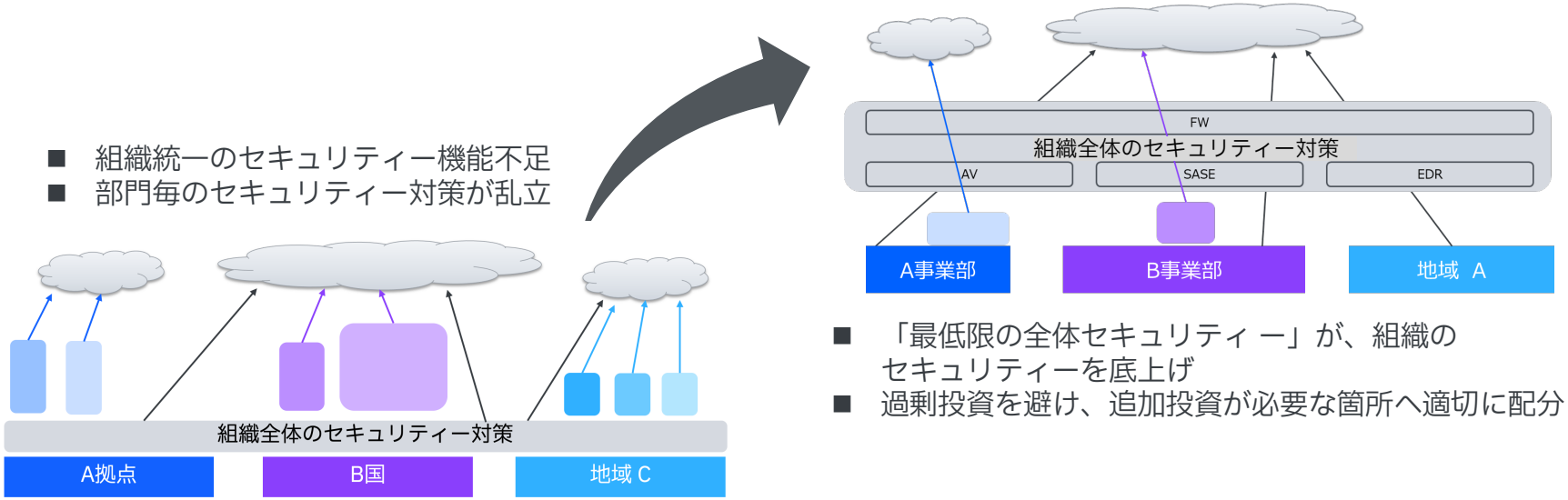
型	集約	連邦（統制型）	連邦（ガイド型）	分散
方針	• セキュリティー部門がツール等で対策を集約 ※外部委託を含む	• 各社にて対応を実施し、セキュリティー部門に対応状況を報告	• セキュリティー部門はガイドを展開 • ガイドに従い各社にて実施	• 各社に対応を一任
事例	• 境界防御対策 • 脆弱性診断 • 脅威分析 等	• バックアップ • 管理者アカウントの管理 • 通信の暗号化 等	• ネットワーク機器セキュリティー設定 • Webアプリケーションのセキュアコーディング 等	• 規定類で定められたベースラインを超える追加のセキュリティー対策 等

選択と集中：すべてに同じレベルを求めない

すべてのセキュリティー対策を本社機能に統一すると、多種多様な事業体の場合、最も高いセキュリティー・レベルに合わせることとなり、部署・拠点によっては、過剰投資ともなりえてしまいます。

選択：部門毎に重要度が異なる「守るべき資産」は各部門にて対策実施

集中：組織として統一して底上げする「最低限の全体セキュリティー」の推進



他のお客様は
どうしてる？

お客様事例紹介：A社～EDRで全拠点を可視化～

弊社でご支援している製造業のお客様の取り組み事例をご紹介します。

社員規模：～5万人
海外拠点規模：20数か国
海外拠点：子会社、直営工場、関連会社、買収済み会社

取組みのきっかけ

- 従来は「分散」型のガバナンス体制、
  各社、各地域にセキュリティーはゆだねていた
- 20xx年海外拠点でインシデント発生
- 本社側で詳細を把握するにも時間を要し、
  セキュリティー統制の必要性を認識

お客様事例紹介：A社～EDRで全拠点を可視化～

弊社でご支援している製造業のお客様の取り組み事例をご紹介します。

IBMがご支援開始時の状況

- 全社共通資産管理ソリューションを全世界で導入中2年目
- それまでの連邦（ガイド）型では、海外のインシデント収まらず、集約型への移行を社長判断で決定
- VPNソリューションの移行を全社共通ソリューションで実施するべく計画中

お客様の抱える課題

- 全体監理を行う本社リソースの欠如
- トップダウン方針を各社のトップに説明、担当者との作業調整にさらに時間がかかる
- 拠点のIT担当者のセキュリティー知識不足

お客様と目指した姿

- 各拠点の自律的セキュリティー運用体制の確立
- 全体状況を本社側で把握しつつも、実際の対応や対策は現地で実施
- 本社が運用管理を行うEDRを導入

お客様事例紹介：A社～EDRで全拠点を可視化～

弊社でご支援している製造業のお客様の取り組み事例をご紹介します。

社員規模：～5万人
海外拠点規模：20数か国
海外拠点：子会社、直営工場、関連会社、買収済み会社

取組みのきっかけ

- 従来は「分散」型のガバナンス体制、
  各社、各地域にセキュリティーはゆだねていた
- 20xx年海外拠点でインシデント発生
- 本社側で詳細を把握するにも時間を要し、
  セキュリティー統制の必要性を認識

●：主体的に実施
〇：要請ベース・部分的に実施
X：未実施・未導入
△：導入中か、不完全な状態で運用中
赤字：現在取組み中

#	対策領域	代表的な対策例	本社	海外
1	統制・全体監理	戦略ロードマップ策定	△	X
2		規程・ガイド作成	△	X
3		監査	●	〇
4		教育	●	〇
5	脅威管理	ログ統合監視	X	△
6		EDR/MDR エンドポイント脅威監視・対応	△	〇
7		インシデント対応	●	X
8	衛生管理	資産管理	X	●
9		脆弱性管理	△	X
10	ID管理	ID管理	X	X

お客様事例紹介：B社～ガバナンス組織の構築～

弊社でご支援している規制産業お客様の取り組み事例をご紹介します。

社員規模：～5万人
海外拠点規模：40数か国
海外拠点：子会社、直営店、関連会社、買収済み会社

取組みのきっかけ

- 従来は「分散」型のガバナンス体制、各社、各地域にセキュリティーはゆだねていた
- 20xx年海外拠点でインシデント発生
- 本社側で詳細を把握するにも時間を要し、セキュリティー対策一新の必要性を認識

目指したのは…

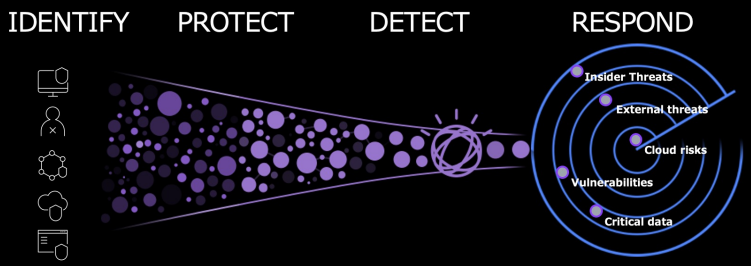
各国で自立運用する
セキュリティー組織体制の構築

お客様の抱える課題

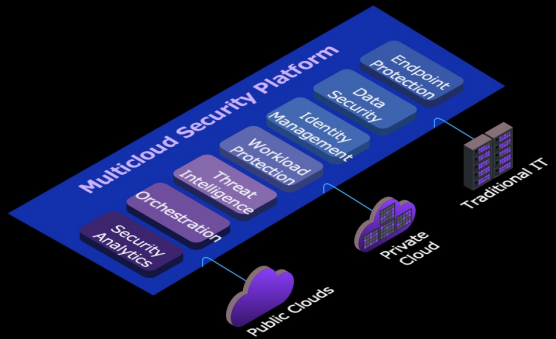
- 規制産業がゆえに、各国で別々の法令が設けられ、日本本社からすべてを把握するのは困難と判断
- 展開する国・地域が多岐にわたり、日本から一括監視することが必ずしもコストメリットにはつながらない

IBMが構築するセキュリティー組織：Fusion Center

<u>セキュリティー組織の統合</u>
- セキュリティー人材の共有
- グループ横断的な知見共有
- 経営者とのコミュニケーション



<u>運用の標準化と高度化</u>
- Playbookを活用したプロセス標準化
- リスクに応じたプロセス高度化
- ツールを活用した自動化と効率化



<u>ツールの連携</u>
- レポートによる可視化
- SIEMによるリアルタイム相関分析
- SOARによるオーケストレーション

そうは言っても、

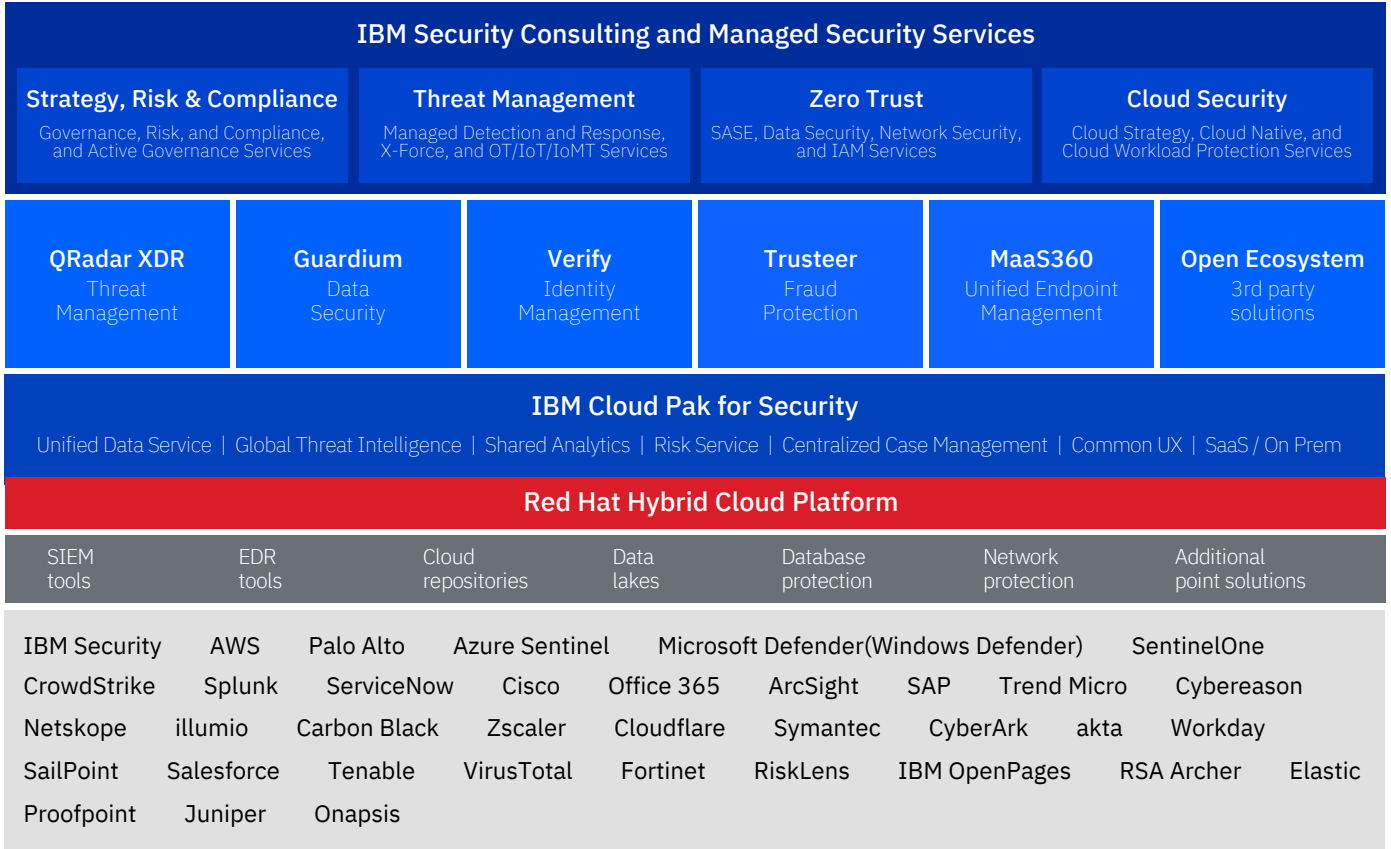
やっぱり誰かに相談したい

はい！！！

私達、IBM Security が皆様のご相談をおまちしています。

あらゆるニーズに対応可能なセキュリティー・ポートフォリオ

業界で最も幅広いサイバーセキュリティーのオープンな統合アプローチ



IBM Security のサービス

お客様が事業を開始するために必要な技術や専門知識の確固たる基盤を提供

IBM Security Consulting Services

- セキュリティー成熟度を向上させ、リスクとコンプライアンスに対応するための協調的かつ全体的なアプローチ
- ロードマップ戦略の定義とその効果的な伝達を支援

IBM Security Expert Labs

- IBMとエコシステムの技術を既存のインフラに統合し、セキュリティー・アドバイザリーおよびマネージド・サービスを利用して、お客様のビジネスに最も重要な成果を提供

真のビジネス成果を実現するために設計された技術的専門知識を持ったIBMにお任せ

IBM Managed Security Services

- グローバルな専門知識とAIや機械学習による統合技術に支えられた、24時間365日の継続的な監視、管理、脅威インテリジェンスにより、セキュリティーとリスクを合理化
- 組織内のスキルを向上、チームのセキュリティー能力を強化

専門家から学ぶ

ハッカー主導の攻撃、研究主導の防御、脅威から身を守る。

X-Force Red

- ペネトレーション・テスト
- 脆弱性管理
- 攻撃的シミュレーション
- アプリケーション セキュリティー

X-Force Incident Response

- インシデント・ レスポンス体制整備サービス
- 24時間365日の緊急 インシデント対応サポート
- 脅威ハンティング

X-Force Threat Intelligence

- 脅威インテリジェンスと 共有プラットフォーム
- 脅威プログラム評価
- ダークウェブ分析
- マルウェア・リバース・ エンジニアリング

IBM Security Cyber Range

- サイバー攻撃演習
- 危機管理・ デザイン思考ワークショップ
- エグゼクティブ・ ブリーフィング

ありがとうございました

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube/user/ibmsecuritysolutions

ibm.com/blogs/security/jp-ja/

video.ibm.com/channel/kfww5QcT925