

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

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・デリバリーを推進
- 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



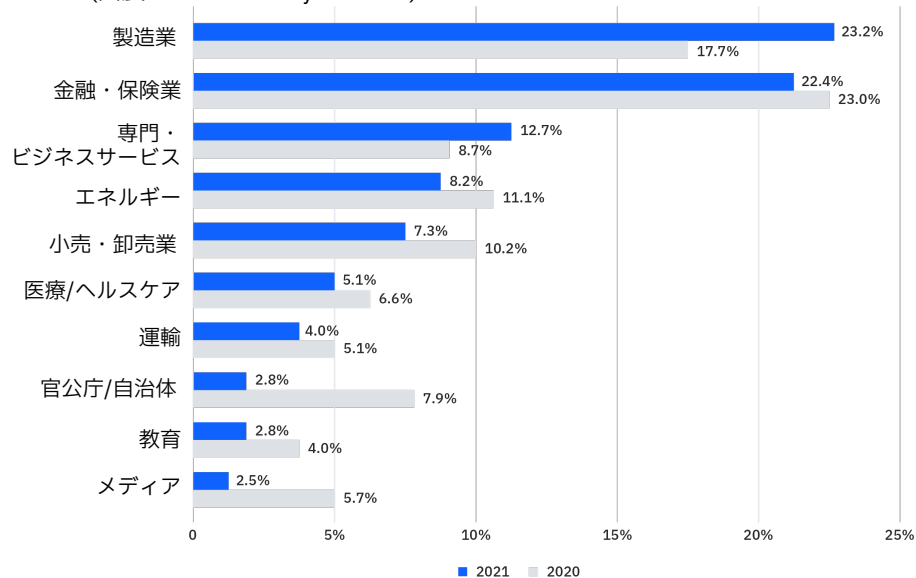
狙われている 重要インフラ・製造業

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すると
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)



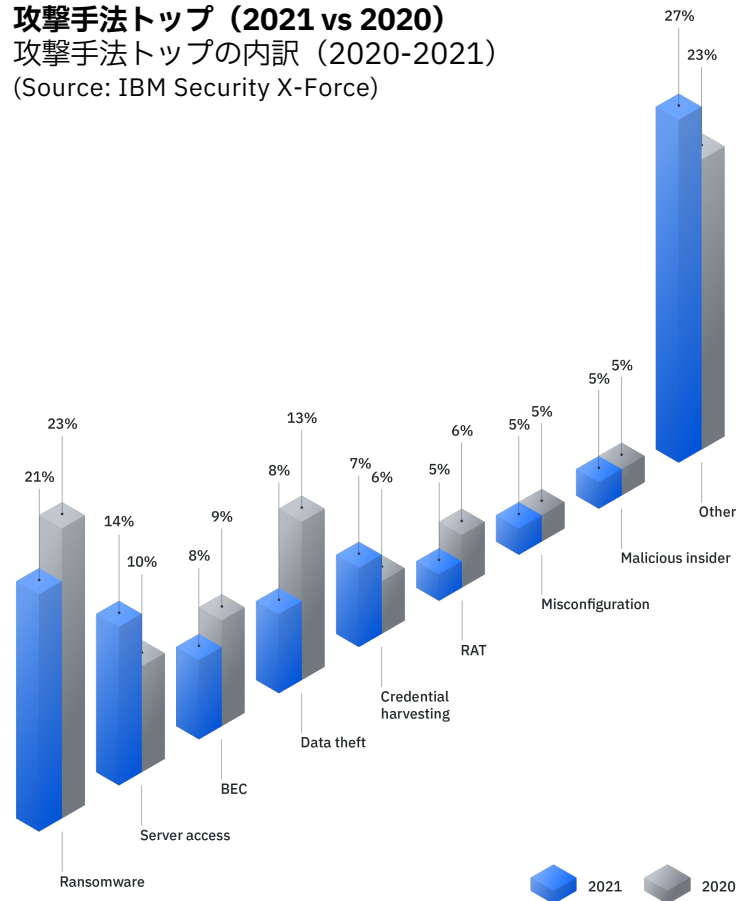
攻撃手法のトップは ランサムウェア

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

— Pipeline system — Sublines
● Main weekend delivery locations



Source: Colonial Pipeline Company

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？

はじめは、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

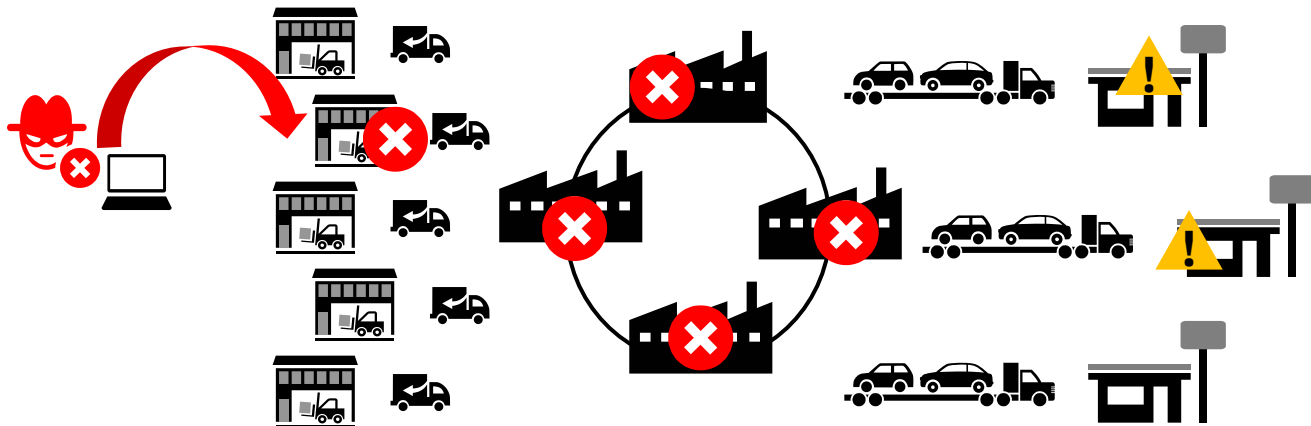
IT担当者不在だったり、行き届かない運用・保守



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



自社セキュリティ対策の見直し

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

取引先セキュリティ・ガバナンスの強化

- ✓ 契約・監査プロセスの整備
- ✓ セキュリティ対策の提供

サプライチェーン・セキュリティ VPN

DX ランサムウェア対策

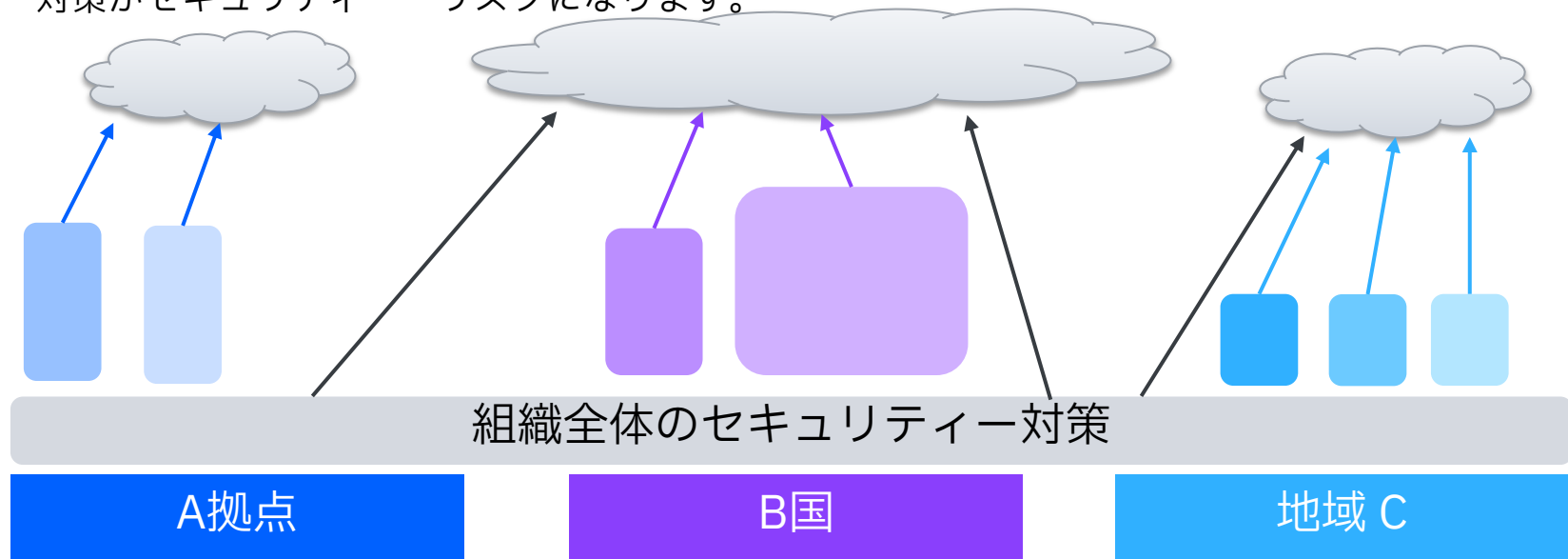
OTセキュリティ
クラウド・セキュリティ

ゼロトラスト・セキュリティ 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対策がセキュリティ・リスクになります。



**攻撃者は、
セキュリティ・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...

セキュリティに費やせる予算には限りがあるのに、セキュリティ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。

可視化

Weakest Linkを把握することが重要



選択と集中

選択と集中：すべてに同じレベルを求めない



ガバナンス

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

守るべきデータはどこにあるのか？

インターネットにつながってるシステムは？

守るべきライン（常時稼働システム）

机上アセスメント

ネットワーク上につながってる？

すでに漏えいしている社内情報はないか？

子会社とはネットワーク上につながってる？

対応していない脆弱性はないのか？

協力会社とはネットワーク上につながってる？

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 **脆弱性診断** につながってる？

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。



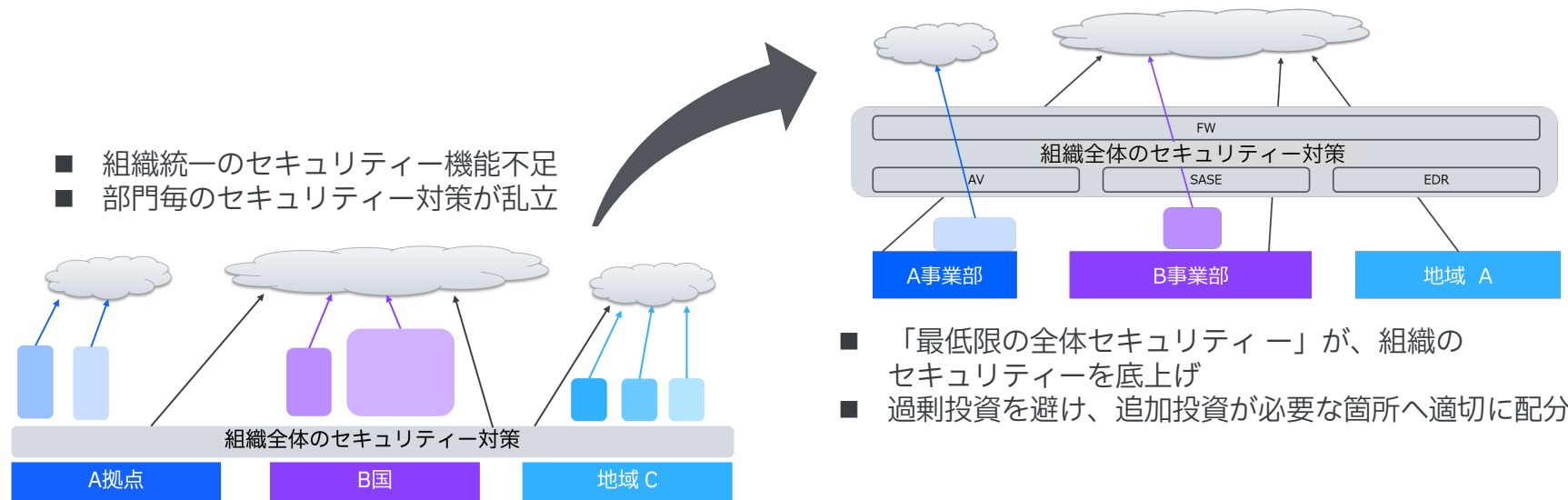
型	集約	連邦 (統制型)	連邦 (ガイド型)	分散
方針	セキュリティー部門がツール等で対策を集約 ※外部委託を含む	各社にて対応を実施し、セキュリティー部門に対応状況を報告	- セキュリティー部門はガイドを展開 - ガイドに従い各社にて実施	各社に対応を一任
事例	- 境界防御対策 - 脆弱性診断 - 脅威分析 等	- バックアップ - 管理者アカウントの管理 - 通信の暗号化 等	- ネットワーク機器セキュリティー設定 - Webアプリケーションのセキュアコーディング 等	規定類で定められたベースラインを超える追加のセキュリティー対策 等

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・レベルに合わせることであり、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」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、セキュリティ統制の必要性を認識

●：主体的に実施
○：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	●	○
4		教育	●	○
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	△	○
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、
買取済み会社

取り組みのきっかけ

- 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

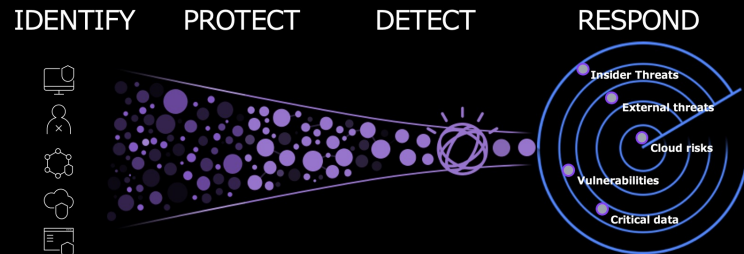
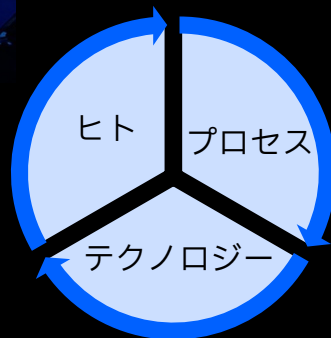
- 規制産業がゆえに、各国で別々の法令が設けられ、日本本社からすべてを把握するのは困難と判断
- 展開する国・地域が多岐にわたり、日本から一括監視することが必ずしもコストメリットにはつながらない

IBMが構築するセキュリティー組織：Fusion Center



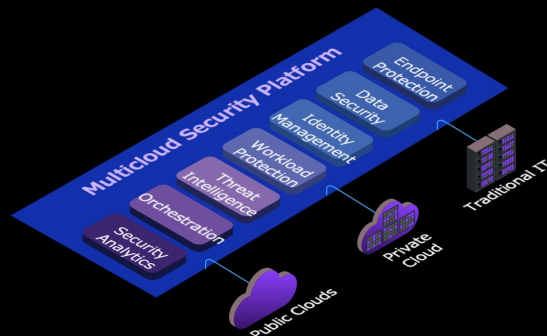
セキュリティー組織の統合

- 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



運用の標準化と高度化

- 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



ツールの連携

- 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

サービス

IBM Security Consulting and Managed Security Services			
Strategy, Risk & Compliance Governance, Risk, and Compliance, and Active Governance Services	Threat Management Managed Detection and Response, X-Force, and OT/IoT/IoMT Services	Zero Trust SASE, Data Security, Network Security, and IAM Services	Cloud Security Cloud Strategy, Cloud Native, and Cloud Workload Protection Services

テクノロジー

QRadar XDR Threat Management	Guardium Data Security	Verify Identity Management	Trusteer Fraud Protection	MaaS360 Unified Endpoint Management	Open Ecosystem 3rd party solutions
--	----------------------------------	--------------------------------------	-------------------------------------	---	--

オープン
プラットフォーム

IBM Cloud Pak for Security						
Unified Data Service Global Threat Intelligence Shared Analytics Risk Service Centralized Case Management Common UX SaaS / On Prem						
Red Hat Hybrid Cloud Platform						
SIEM tools	EDR tools	Cloud repositories	Data lakes	Database protection	Network protection	Additional point solutions

エコシステム

IBM Security	AWS	Palo Alto	Azure Sentinel	Microsoft Defender(Windows Defender)			SentinelOne	
CrowdStrike	Splunk	ServiceNow	Cisco	Office 365	ArcSight	SAP	Trend Micro	Cybereason
Netskope	illumio	Carbon Black	Zscaler	Cloudflare	Symantec	CyberArk	akta	Workday
SailPoint	Salesforce	Tenable	VirusTotal	Fortinet	RiskLens	IBM OpenPages	RSA Archer	Elastic
Proofpoint	Juniper	Onapsis						

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動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・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

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

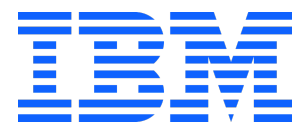
ibm.com/blogs/security/jp-ja/

video.ibm.com/channel/kfww5QcT925

© Copyright IBM Corporation 2022. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others.

No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.



ワークショップ、セッション、および資料は、IBMまたはセッション発表者によって準備され、それぞれ独自の見解を反映したものです。それらは情報提供の目的のみで提供されており、いかなる参加者に対しても法律的またはその他の指導や助言を意図したものではなく、またそのような結果を生むものでもありません。本講演資料に含まれている情報については、完全性と正確性を期するよう努力しましたが、「現状のまま」提供され、明示または暗示にかかわらずいかなる保証も伴わないものとしします。本講演資料またはその他の資料の使用によって、あるいはその他の関連によって、いかなる損害が生じた場合も、IBMは責任を負わないものとします。本講演資料に含まれている内容は、IBMまたはそのサプライヤーやライセンス交付者からいかなる保証または表明を引きだすことを意図したもので、IBMソフトウェアの使用を規定する適用ライセンス契約の条項を変更することを意図したものでなく、またそのような結果を生むものでもありません。

本講演資料でIBM製品、プログラム、またはサービスに言及していても、IBMが営業活動を行っているすべての国でそれらが使用可能であることを暗示するものではありません。本講演資料で言及している製品リリース日付や製品機能は、市場機会またはその他の要因に基づいてIBM独自の決定権をもっていつでも変更できるものとし、いかなる方法においても将来の製品または機能が使用可能になると確約することを意図したものではありません。本講演資料に含まれている内容は、参加者が開始する活動によって特定の販売、売上高の向上、またはその他の結果が生じると述べる、または暗示することを意図したもので、またそのような結果を生むものでもありません。パフォーマンスは、管理された環境において標準的なIBMベンチマークを使用した測定と予測に基づいています。ユーザーが経験する実際のスループットやパフォーマンスは、ユーザーのジョブ・ストリームにおけるマルチプログラミングの量、入出力構成、ストレージ構成、および処理されるワークロードなどの考慮事項を含む、数多くの要因に応じて変化します。したがって、個々のユーザーがここで述べられているものと同様の結果を得られると確約するものではありません。

記述されているすべてのお客様事例は、それらのお客様がどのようにIBM製品を使用したか、またそれらのお客様が達成した結果の実例として示されたものです。実際の環境コストおよびパフォーマンス特性は、お客様ごとに異なる場合があります。

IBM、IBM ロゴ、ibm.com、QRadar®、MaaS360®、IBM Security®、IBM Services®、X-Force® は、世界の多くの国で登録されたInternational Business Machines Corporationの商標です。他の製品名およびサービス名等は、それぞれIBMまたは各社の商標である場合があります。現時点での IBM の商標リストについては、www.ibm.com/legal/copytrade.shtmlをご覧ください。

Microsoft、Windows、Windows NT および Windowsロゴは Microsoft Corporationの米国およびその他の国における商標です。

Red Hat、OpenShiftは、Red Hat Inc.または子会社の米国およびその他の国における商標または登録商標です。