スクエア free セミナー 第１５７回　知っておきたいサイバーセキュリティ対策

「デジタル災害化するサイバー攻撃の変化と企業がとるべき対応」
～デジタル時代の事業防衛とセキュリティ対策～

ニューリジェンセキュリティ株式会社
CTO
仲上竜太,CISSP

nuligen security

本セッションについて

- デジタル化で業務効率UP＆コスト削減！
  しかし、増大するサイバー攻撃への対策も欠かせません。
  サイバー攻撃者の目的や手法を知ることで、サイバー攻撃の被害を抑えられます。
  誰もが被害者になりうるデジタル災害化する昨今のサイバー攻撃トレンドと対策について解説します。

仲上　竜太（なかがみ りゅうた）

ニューリジェンセキュリティ株式会社
CTO
兼 クラウドセキュリティ事業部部長
CISSP, 情報安全確保支援士(登録番号第005254番)

奈良県出身。2001年　電気通信大学卒業後、ソフトウェアオフショアベンチャーでの経験を経て、
株式会社ラックに入社。サイバー・グリッド研究所長、ネットエージェント株式会社取締役、
デジタルペンテストサービス部長ののち、現在は野村総合研究所とラックの合弁企業である
ニューリジェンセキュリティ株式会社にてCTOを務める。
専門分野は先端技術のセキュリティを考慮した安全な利活用方法の研究で、現在は
ゼロトラストセキュリティやメタバースにおけるセキュリティを研究している。

所属団体・委員会等：

・総務省「安心安全のメタバースの実現に関する研究会」構成員(2023-)
・総務省「Web3時代に向けたメタバース等の利活用に関する研究会」構成員(2022-2023)
・内閣官房「デジタル市場競争会議」オブザーバー(2022-)
・日本スマートフォンセキュリティ協会 技術部会 部会長
・日本ネットワークセキュリティ協会社会活動部会海外市場開拓WG
・サイバーセキュリティイニシアチブジャパン 人材教育部会
・クラウドセキュリティアライアンスジャパンチャプター AIセキュリティWG
・日本バーチャルリアリティ学会

nuligen security

サイバー攻撃、質の変化と量の変化

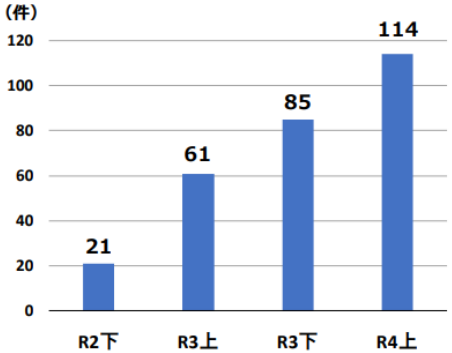
サイバー攻撃、質の変化と量の変化

ランサムウェアによる脅迫被害が多発

過去1年間で日本の組織の61%がランサムウェアの被害にあい、そのうち20%が平均2億5,875万円にのぼる身代金を支払っている。

出典：クラウドストライク、2021年度版グローバルセキュリティ意識調査

近年、日本国内においても医療機関・教育・製造業など様々な業種を狙ったランサムウェア攻撃被害が多発。IT設備の無効化だけでなく、機密情報が窃取され情報公開を盾に脅迫されるケースが頻発している。



企業・団体等におけるランサムウェア被害として、令和4年に都道府 県警察から警察庁に報告のあった件数

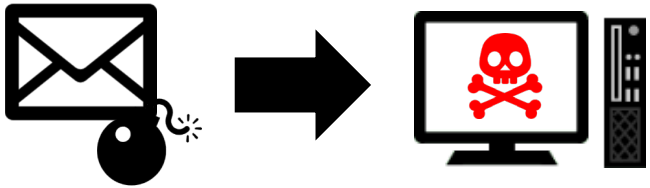
出典：令和4年上半期におけるサイバー空間をめぐる脅威の情勢等について（警察庁）

サイバー攻撃、質の変化と量の変化

標的型攻撃＋ランサムウェア＝二重脅迫(または多重脅迫)

脅迫による金銭の支払いを目的として、標的型攻撃の手法により内部情報を窃取したのち、高性能なランサムウェアで情報を破壊（暗号化）データの復旧を持ち掛け、応じなければ情報を公開

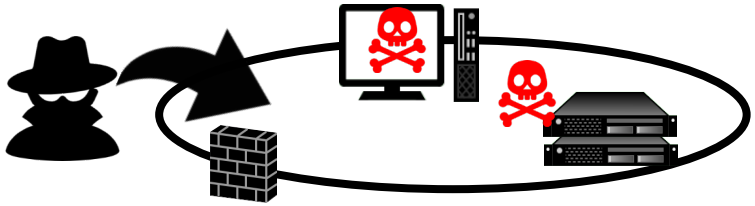
従来型



- 無差別に送信されたメールの添付で感染
- インターネットにつながったPCの脆弱性を悪用して感染、IT環境が破壊

攻撃者が被害者を特定していない

多重脅迫型



- 企業や組織のネットワークに侵入して機密情報を持ち出し
- ランサムウェアによってIT環境を破壊

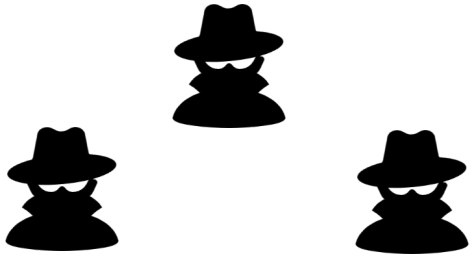
攻撃者が被害者を特定している

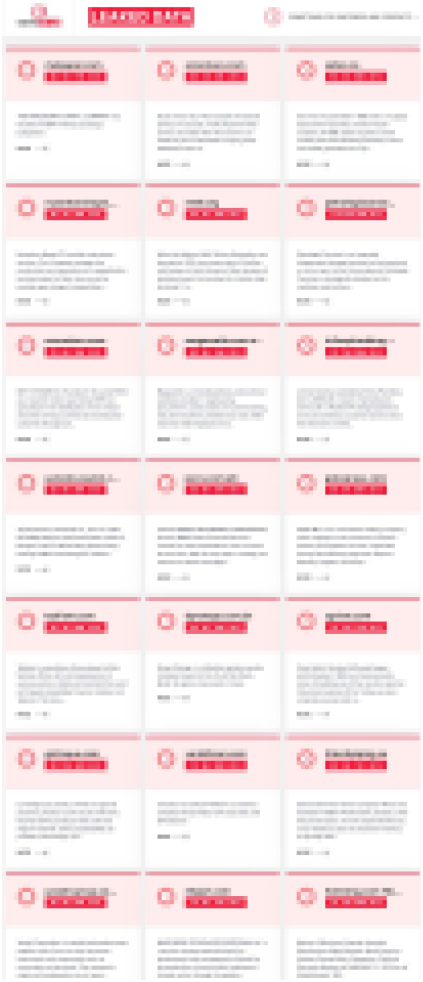
サイバー攻撃、質の変化と量の変化

- **高度なサイバー攻撃ツールに絡んだ、サイバー攻撃のマーケット化・エコシステム化**

Ransomware as a Service：RaaS

- 性能の高いランサムウェアのコードが販売されている
- 侵入能力を持ったサイバー攻撃者が購入することで、ソフト開発力がなくてもランサムウェアによる攻撃が可能





サイバー攻撃、質の変化と量の変化

IPAが発表した10大脅威に見る、昨今のサイバー脅威の現状

ランサムウェアによる被害が2021年以降3年連続1位

サプライチェーンの弱点の悪用が課題

テレワーク等のニューノーマルな働き方を狙った攻撃が継続

NEW：初めてランクインした脅威

順位	組織	昨年順位
1位	ランサムウェアによる被害	1位
2位	標的型攻撃による機密情報の窃取	2位
3位	サプライチェーンの弱点を悪用した攻撃	4位
4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	3位
5位	内部不正による情報漏えい	6位
6位	脆弱性対策情報の公開に伴う悪用増加	10位
7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
8位	ビジネスメール詐欺による金銭被害	5位
9位	予期せぬIT基盤の障害に伴う業務停止	7位
10位	不注意による情報漏えい等の被害	9位

IPA/情報セキュリティ10大脅威2023

サイバー攻撃、質の変化と量の変化

サイバー攻撃の類型

- **意図をもったサイバー攻撃者による情報の窃取や妨害**
  - 敵対企業や組織の情報入手
  - 対外政策による情報入手、混乱、軍事目標の破壊
  - 政治的主張、テロ　など

- **金銭を目的としたサイバー攻撃者による脅迫(増加傾向)**
  - 個人や法人の金融資産を狙った攻撃
  - 暗号通貨を狙った攻撃
  - 企業の情報の窃取と脅迫を狙った攻撃
  - 企業のインフラ無効化と回復を狙った攻撃　など

・デジタル環境が進化・増加し、攻撃しやすい状況＝サイバー犯罪の機会増加
・企業や組織は両方のタイプのサイバー攻撃から資産を防衛する必要がある


災害化する
サイバー脅威

2020年以降のサイバー環境の変化

- リモートワーク・クラウド利用の増加
- ビジネス環境のDX化
- デジタルテクノロジーの進化

サイバー攻撃者にも有利な環境変化

**2020年以降の急激なデジタルへの依存度の高まりと
サイバー攻撃の技術進化により、サイバー脅威が
人為的被害から「デジタル災害」に近い状態になりつつある**

サイバー攻撃技術の進化

デジタル技術の発展によりサイバー攻撃技術が進化

AI
人工知能

RPA
自動化

データベース

災害化するサイバー脅威

AI
人工知能

- **AI（人工知能）や機械学習技術の悪用**
  - 音声や映像の精密な偽造（ディープフェイク）によるなりすまし
  - 侵入した企業内のネットワーク流通データの分析
  - EDRやアンチウイルスに検知されないマルウェアの自動開発　など
- **ChatGPTやStable Diffusionなど生成AIの悪用**
  - 自然なフィッシングメールや偽メッセージの生成
  - 特定の個人を攻撃するための偽画像・映像の生成
  - クラウドサービスやネットワーク機器の脆弱性をつく攻撃コードの自動開発　など

デジタルコンテンツ・プログラムを精密かつ大量に生成できるAI技術の悪用は攻撃機会の増加をもたらす

災害化するサイバー脅威

RPA
自動化

- **RPA(Robotics Process Automation)・自動化の悪用**
  - RPA技術により様々な作業の自動化が可能
  - インターネット上でアクセス可能な範囲に対して機械的に24時間・365日探索が可能
  - スクレイピングによる大量情報の収集
  - RPAを提供するサービスへの攻撃による利用企業の情報への侵害（RPAへの攻撃）
  - 管理者のいない野良ロボットの悪用（RPAへの攻撃）　など

RPAにより24時間365日インターネット全体にハッキングをし続け、脆弱な設定のホストやネットワーク機器を探索。ターゲットの探索を自働化。

災害化するサイバー脅威

データベース

- **サイバー攻撃の端緒となる情報の蓄積と流通**
  - 情報漏洩したサイトやサービスのID、パスワード情報などクレデンシャル情報
  - 公開情報として取得可能な脆弱なIoT機器名やバージョン、IPアドレス、設置された国などの情報
  - Facebook、TwitterなどのSNSから得られるソーシャル情報
  - 攻撃者同士でのデータベースのアンダーグラウンドでの売買　など

AIやRPAが効率よく攻撃対象を選定する情報源として使用。
流出したID、パスワードは別サイトに対してのログインに悪用される。

サイバー攻撃技術の進化

デジタル技術の発展によりサイバー攻撃技術が進化

多くの新技術が一般利用可能な形で提供されており、攻撃者にとってもサイバー攻撃技術への転用は容易。今後も新たな技術の登場を注視する必要がある。


攻撃者優位の
非対称性

サイバーセキュリティにおける非対称性

サイバー攻撃者

**十分な時間をかけて調査し、
脆弱な対象に対して、
好きな時に攻撃すればよい**

セキュリティ担当者

**全領域で対策を行い、いつ来るかわからない攻撃に対し、
24時間備える必要がある**

サイバー攻撃者優位の非対称性

- サイバー攻撃の手法・戦略・情報網は効率的に洗練されエコシステムにより共有されている
- 暗号通貨の流通、デジタルの価値増大などによりサイバー攻撃がビジネス化し、社会情勢を背景として参入者が増加している
- 新たなテクノロジーがオープンに進化し続けている
- 守る側は限られたリソースで対処する必要がある


災害化する
サイバー脅威に対抗する
セキュリティの考え方

災害化するサイバー脅威に対抗するセキュリティの考え方

アタックサーフェース管理
Attack Surface Management

データ中心
Data Centric

サイバーハイジーン
Cyber Hygiene

ゼロトラストアーキテクチャ
Zerotrust Architecture

今後も進化するデジタル技術、増え続けるデジタル資産に対応可能なセキュリティの取り組みが求められています。

災害化するサイバー脅威に対抗するセキュリティの考え方

アタックサーフェース管理
Attack Surface Management

データ中心
Data Centric

サイバーハイジーン
Cyber Hygiene

ゼロトラストアーキテクチャ
Zerotrust Architecture

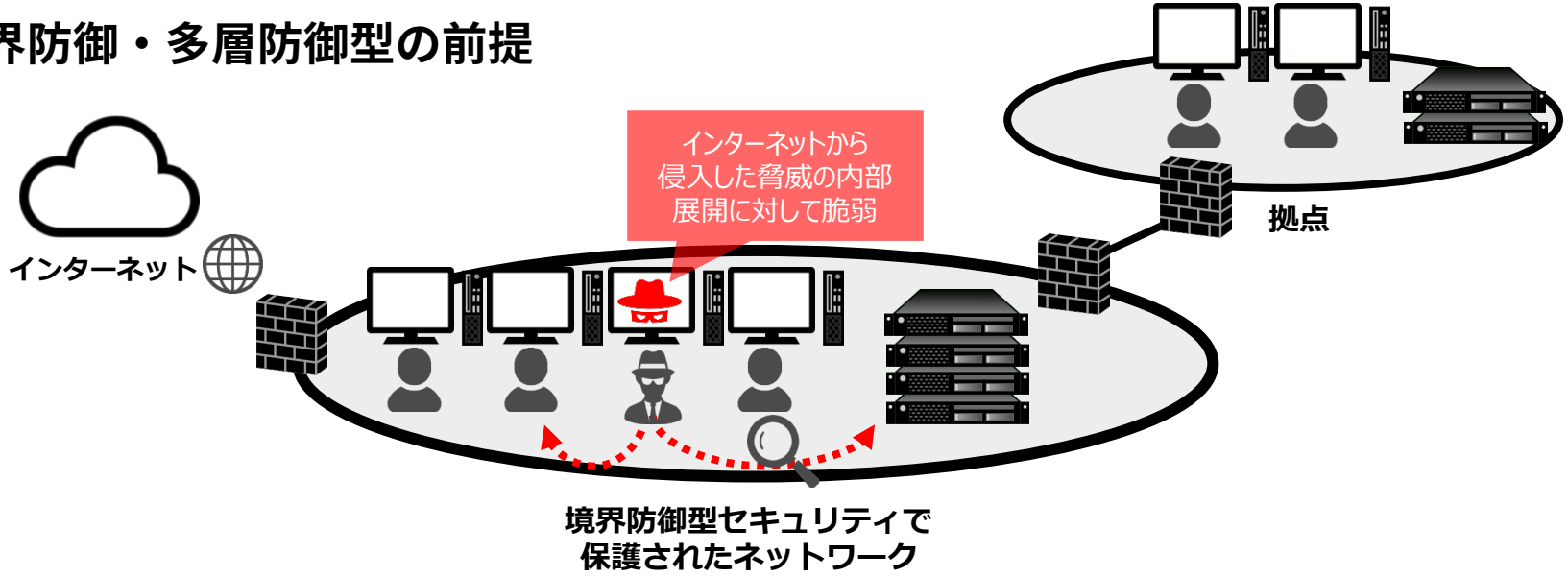
デジタル化で拡大したアタックサーフェース

2020年から2023年で経験した劇的な変化とアタックサーフェース

インターネットへの分散とデジタル化は
アタックサーフェースの増加につながった

デジタル化で拡大したアタックサーフェース

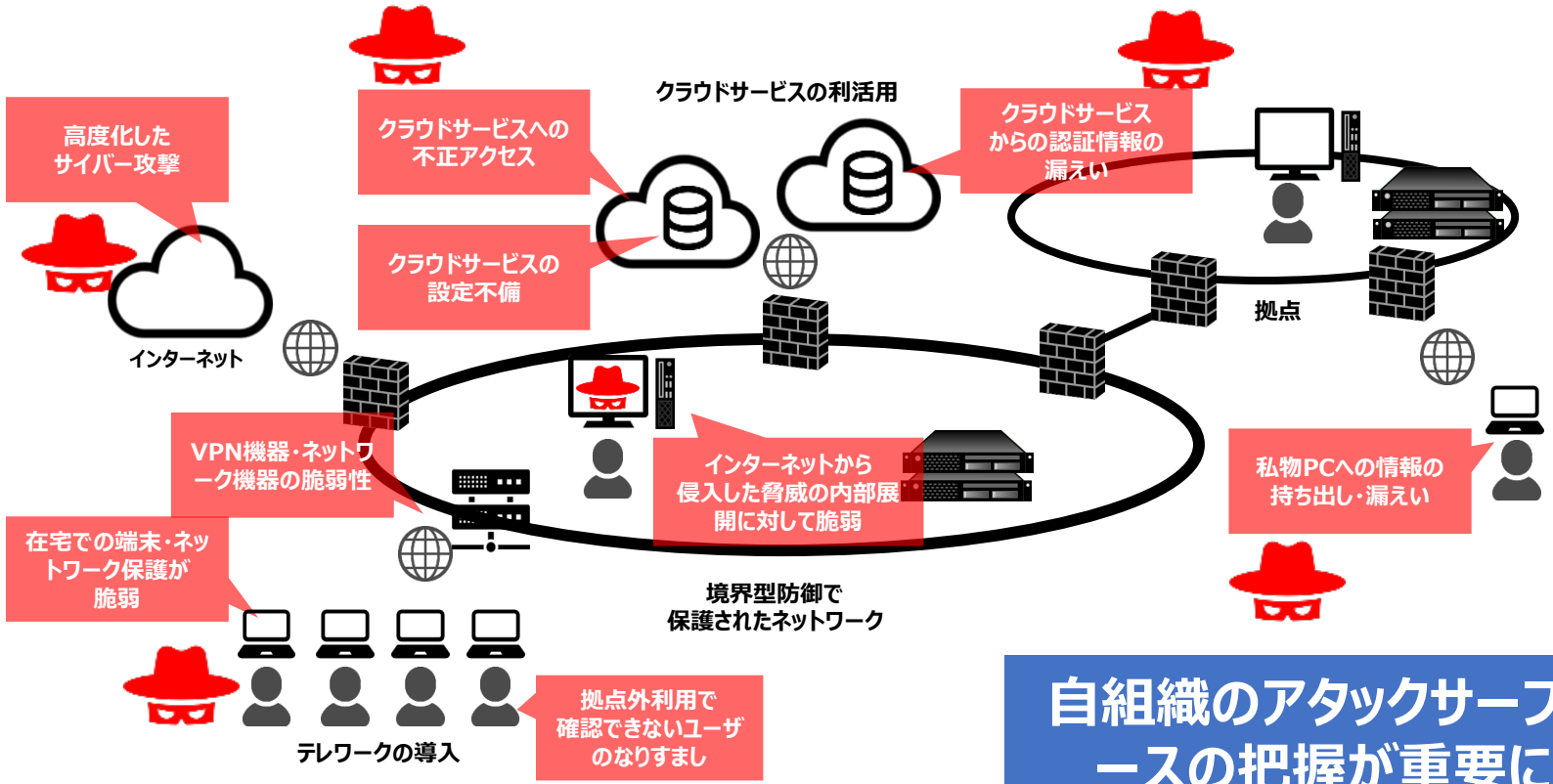
境界防御・多層防御型の前提



- 境界防御・多層防御は物理ネットワーク内にデータと利用者がいることが前提。
- ネットワーク機器の脆弱性の悪用やメールに添付したマルウェアによる侵害などで一度内部に侵害された場合に内部展開に対して脆弱なことが課題。
  これらの課題には、内部の挙動を監視するUEBAなどによる多層防御による対策が試みられている。

デジタル化で拡大したアタックサーフェース

変化した働き方によって生じた**境界外の新たなアタックサーフェースと脆弱性**への対処が課題となっています。



自組織のアタックサーフェースの把握が重要に

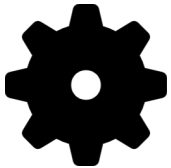
アタックサーフェース管理とは

攻撃者の観点でアタックサーフェースを把握し対処する

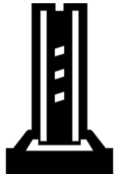
公開

クラウドサービス

公開ウェブサイト



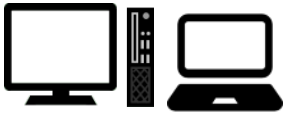
APIサービス



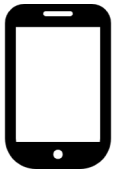
ネットワーク機器

・・・

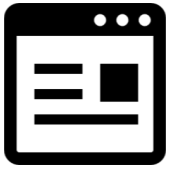
非公開



PC端末



モバイル端末



社内システム

子会社・関連会社ネットワーク

・・・

アタックサーフェースの一例

アタックサーフェース管理とは（ASM：攻撃界面管理）

- **企業や組織のITシステムが抱える課題**
  - 企業が保有するIT資産の爆発的増加
  - 世界に広がるサプライチェーンの広がりとガバナンス
  - テレワークによるモラルハザード
  - 技術進化やサイバー攻撃エコシステムによる、サイバー攻撃の一災害化
- **自組織の攻撃界面を把握し対処するアタックサーフェースマネジメント**
  - 自組織の資産・脆弱性の管理とともに脅威の端緒となる攻撃界面（アタックサーフェース）を管理し、その状態を把握
  - OSINTにより管理認識外の資産を把握し、アタックサーフェースの状態を把握
    - サポート切れ製品、つながったままのテスト機、数年前にキャンペーンで作成したままのウェブサイト、利用者が勝手につないだIoT機器、グループ会社が無許可で取得したドメインなどなど
  - 継続的な資産調査と診断の自動化により攻撃の手がかりを減らす

攻撃者の観点でアタックサーフェースを把握し対処する

（攻撃者にとっての）攻撃的コストの増大

アタックサーフェース管理（アタックサーフェースの例）

ネットワーク
機器

ネットワーク機器

IPアドレス

ドメイン名

メール
アドレス

ネットワーク機器に対するサイバー攻撃の一例

調査活動

- 利用ハードウェアの確認（バナーの取得）
- ファームウェアバージョンの確認
- ネットワーク構成の推定

攻撃の実施

- 企業ネットワークへの侵入
- DoS攻撃によるサービスの停止
- 対応されていない脆弱性を悪用した侵入
- 接続情報の窃取
- bot化　など

アタックサーフェース管理（ASM：Attack Surface Management）

アタックサーフェース管理の問題点

- 多種多様なデジタル資産の把握が困難
- シャドーITの存在
- 変化しつづけるデジタル環境

デジタルの利活用の増加にともないこれらの問題点も深刻化

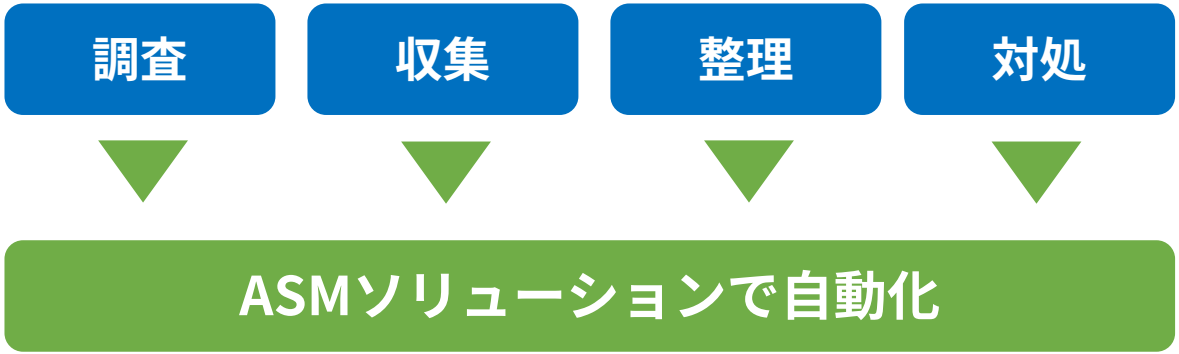
▼

アタックサーフェース管理ソリューションの活用

アタックサーフェース管理（ASM：Attack Surface Management）

アタックサーフェース管理ソリューションの活用

増え続ける企業や組織のアタックサーフェース



攻撃者からは
見えてしまって
いる状態に注意

インターネット上の情報リソースや自動調査機能
により、インターネット上のシャドーITも含め常時
アタックサーフェースの検出および脆弱箇所を特定。

継続的な脆弱性診断や設定不備調査の実施により、
アタックサーフェースの危険個所にすばやい対処が可能。

攻撃コストを
高めて
被害確度を下げる

災害化するサイバー脅威に対抗するセキュリティの考え方

アタックサーフェース管理
Attack Surface Management

データ中心
Data Centric

サイバーハイジーン
Cyber Hygiene

ゼロトラストアーキテクチャ
Zerotrust Architecture

データ中心型セキュリティ (Data Centric Security)

データ中心型セキュリティの背景

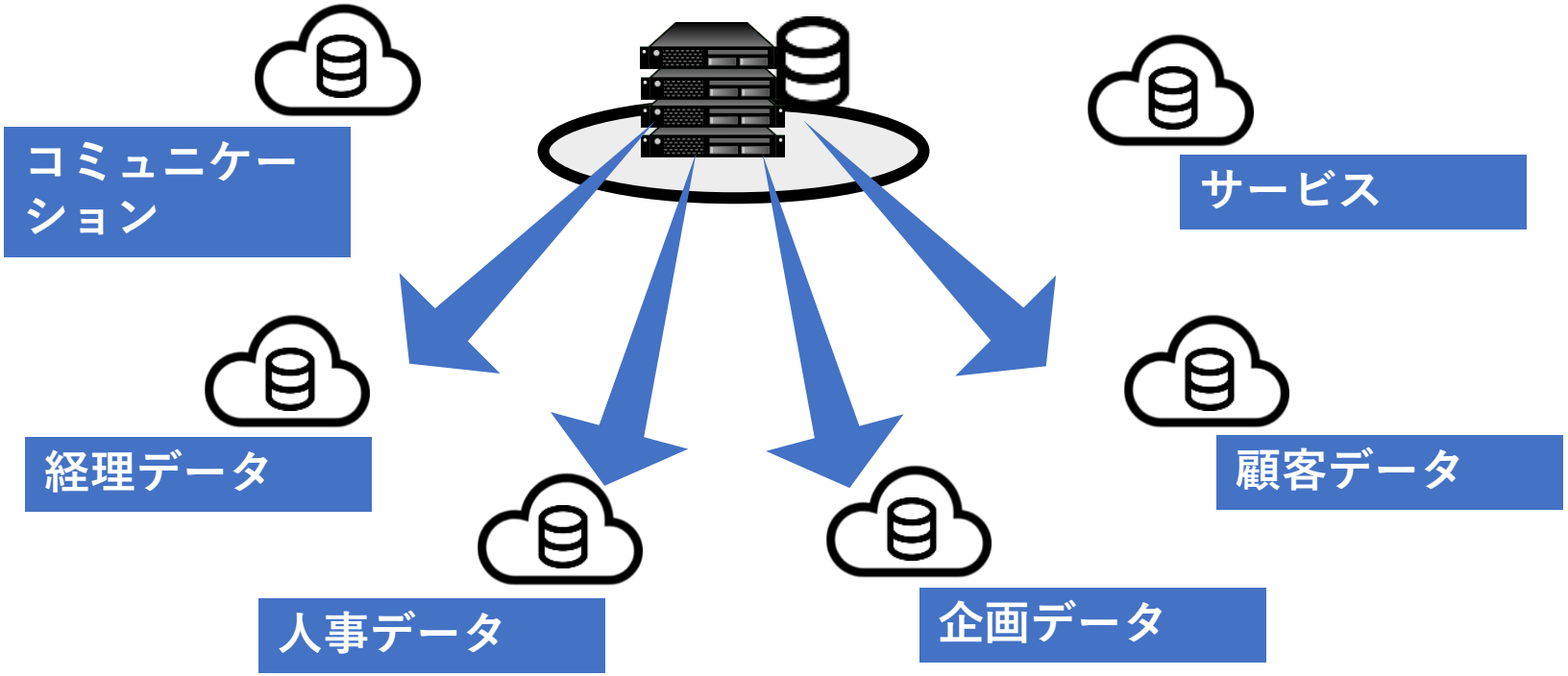
IT化／DXによって組織が取り扱うデータの量と重要度が増大

データの価値　＞＞＞＞＞＞　ハードウェアの価値

機密データ保護に関するコンプライアンスの強化

データはどこにありますか？

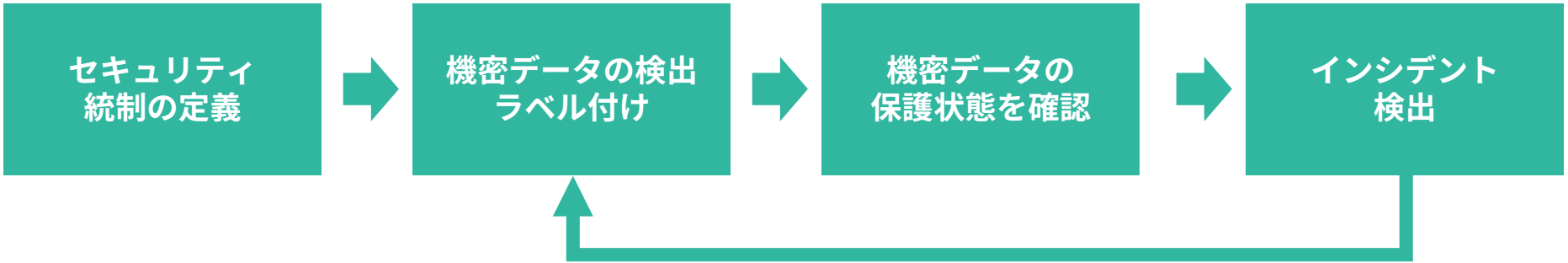
複数のクラウドサービスに分散する組織のデータ



SaaSやIaaS/PaaSの活用推進により、企業や組織の重要データが**複数のサービスに分散**。
社内外のコミュニケーションやサービスそのものも**クラウド上に蓄積**される状態。

クラウド×データ中心セキュリティの新たな考え方：DSPM

- **DSPM（Data Security Posture Management）**
  - クラウドやオンプレミスに保存されている膨大なデータから機密データや重要データを検出し、データが適切に保護されているかを管理する仕組み



- **DSPMとは**
  - データが膨大化しており、すべてのデータを人間が管理し適切に保護設定が行われているかを確認するセキュリティソリューション
  - クラウド上のデータの保護はSaaSなどCSP（クラウド・サービス・プロバイダ）の提供する保護方法をサジェストする
  - 不適切な操作や利用により不規則にコピーや配置された機密情報を見つけ出す

災害化するサイバー脅威に対抗するセキュリティの考え方

アタックサーフェース管理
Attack Surface Management

データ中心
Data Centric

サイバーハイジーン
Cyber Hygiene

ゼロトラストアーキテクチャ
Zerotrust Architecture

サイバーハイジーン＝サイバー衛生

情報システムに対してかかる脅威に対して、
脆弱性を即時に最小化し、脅威の顕在化を防ぐ取り組み。

サイバーハイジーンの取り組み

- 資産管理とデータの棚卸
- 脆弱性管理とパッチマネジメント
- ID管理と多要素認証
- ネットワークセグメンテーション
- アタックサーフェースの管理
- ログの監査　など

システムの堅牢化

継続的な脆弱性管理

システム状態の可視化

サイバーハイジーン＝情報システムの健康維持

歯に例えると？

- 虫歯治療→インシデント対応
- 日々の歯磨きによる予防
- 定期健診での徹底調査

歯科衛生士=Dental Hygienist

災害化するサイバー脅威に対抗するセキュリティの考え方

アタックサーフェース管理
Attack Surface Management

データ中心
Data Centric

サイバーハイジーン
Cyber Hygiene

ゼロトラストアーキテクチャ
Zerotrust Architecture

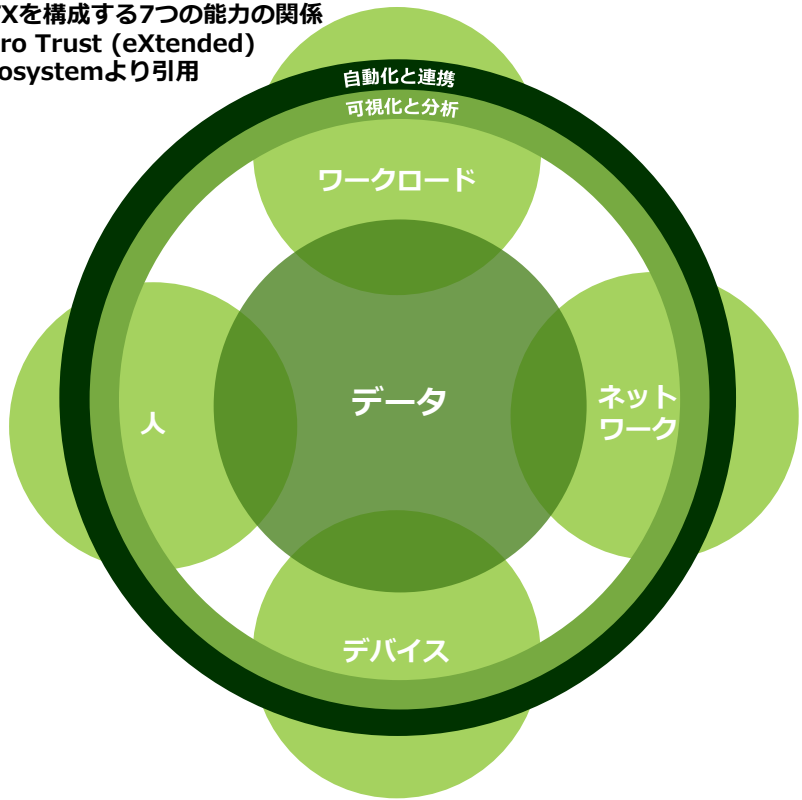
ゼロトラストに共通する基本的な考え方と特長

Always Verify, Never Trust.

常に検証し、信用しない。

拡張ゼロトラスト Zero Trust eXtended (ZTX)

ZTXを構成する7つの能力の関係
Zero Trust (eXtended) ecosystemより引用



- クラウドやモバイル、IoT等の近年の情報通信技術の変化に対応したゼロトラストの拡張コンセプト
- 7つの能力を基にゼロトラストに取り組むためのベンダーを含めた実現のための相互連携であるエコシステムを定義
- 最も保護すべきデータを中心に、人・デバイス・ワークロード(アプリ／システム)・ネットワークのコンポーネントがあり、これらを可視化と分析、自動化と連携の能力で接続することでゼロトラストによる保護が行われた状態を目指す

ゼロトラストの構成要素

ゼロトラストを構成する7つの要件とセキュリティ対策

アイデンティティ	デバイス	データ	ワークロード	ネットワーク	可視化と分析	自動化と連携
アイディンティティ連携 既存ディレクトリとの統合管理	侵入検知・自動防御 マルウェア対策 デバイス管理 デバイス制御 アプリ制御	漏えい防止 改ざん防止 データ分類 クラウドセキュリティ ・設定管理 ・利用状況管理	脆弱性検査	ID認識プロキシ セグメント化による分離 仮想化 安全なインターネットアクセス	可視化・分析基盤 セキュリティオペレーションセンター	APIによる自動連係 マネージドサービス

これらの個別のセキュリティ対策を連携させ、全体でゼロトラストが適用された状態であるゼロトラスト・アーキテクチャの実現を目指します。

変化するワークスタイル

急激なデジタル化とコロナ禍によりワークスタイルが短期間で大幅に変化

オフィス出社

オフィスネットワークのセキュリティを中心に、人・情報資産を保護する方法として境界防御・多層防御がセキュリティの中心。

テレワーク中心

コロナ禍におけるテレワーク強制に始まり可用性中心のテレワーク設計。オンライン会議によるVPN渋滞やネットワークスピード課題が発生し、可用性向上の方法としてゼロトラストによる社内アクセス（アクセスプロクシ）注目のきっかけにもなった。

ハイブリッド

オンラインミーティングと会議室ミーティング、テレワークと出社の混合などリアルとリモートが混在する。データのやり取りはクラウドが中心に。

設備刷新タイミングにおける情報システムのクラウド化とともにビルトインセキュリティによるゼロトラストの実現が加速。

まとめ

アタックサーフェース管理
Attack Surface Management

データ中心
Data Centric

サイバーハイジーン
Cyber Hygiene

ゼロトラストアーキテクチャ
Zerotrust Architecture

DX・デジタルワークプレースの変化による恩恵を最大化するため、
新たなセキュリティの考え方が求められています

ご紹介）Cloudscort サービス概要

- Cloudscortは、クラウドネイティブ機能を強化する(使いやすくする)サービスです
- 機能群はSaaS型でご提供します。また、プロフェショナルサービスは部分的なMSSとしてご提供します
- https://cloudscort.com

	クラウド機能	Cloudscortのサービス
検知・対応	Web Application Firewall Webファイアウォール	WAFやNWFWの運用で求められるタスクを支援 • 最新攻撃パターンの自動適用 • 検知した攻撃通信の自動分析 • 被害拡大防止のための通信先遮断 • ユーザ要望によるカスタムIPルールの設定
	Network Firewall Networkファイアウォール	
未然防御	CSPM クラウド設定管理	CSPMやVMの運用で求められるタスクを支援 • 検知した脆弱性の解説・対策情報付与 • クラウド資産価値×脆弱度に応じた対応優先順位の判定 • セキュリティサービスの自動最適化
	VM 脆弱性管理	

--- 共通機能 ---

- 高度脅威インテリジェンス（NRIセキュア、ラック）
- CISOダッシュボード
- プロフェッショナルサービス（MSS:セキュリティ運用支援）

※ 実装見込みの情報を一部含みます。

nuligen
security