Cloud Conference 2024
事業停止を伴う大規模なセキュリティインシデント対応の実際

Internet Secure Services

インターネット・セキュア・サービス株式会社

自己紹介

小倉 秀敏（おぐら ひでとし）

インターネット セキュア サービス株式会社　最高サービス責任者

略歴：

- 組み込み機器、組み込みOS開発に約13年従事
- 1999年～、インターネット セキュリティ システム株式会社(ISS) セキュリティ・コンサルティング・ディレクター
- 2007年～、日本IBM セキュリティ・サービス
- 2013年～、日本HP ESP事業部プリセールス・マネージャー
- 2014年～、日本IBM X-Force Incident Responseシニア・マネージング・コンサルタント
- 2022年～、インターネット･セキュア･サービス株式会社最高サービス責任者

得意分野：

- セキュリティインシデント対応
- CSIRT構築支援
- データベースセキュリティ監査および設計、実装
- ネットワークセキュリティ設計、実装
- セキュリティポリシーアセスメント、設計

資格：

- 情報処理安全確保支援士（第24000号）

サイバーセキュリティ侵害の侵入経路の傾向と対策

本日の内容：

昨今サイバーセキュリティに関連する事故や攻撃が報道されることが多くなり、否が応でもサイバーセキュリティを意識させられる機会が増えてきました。特に病院や工場など、被害組織の業務が停止するなどの深刻な影響を与えるランサムウェア被害が大きく取り上げられることも少なくありません。

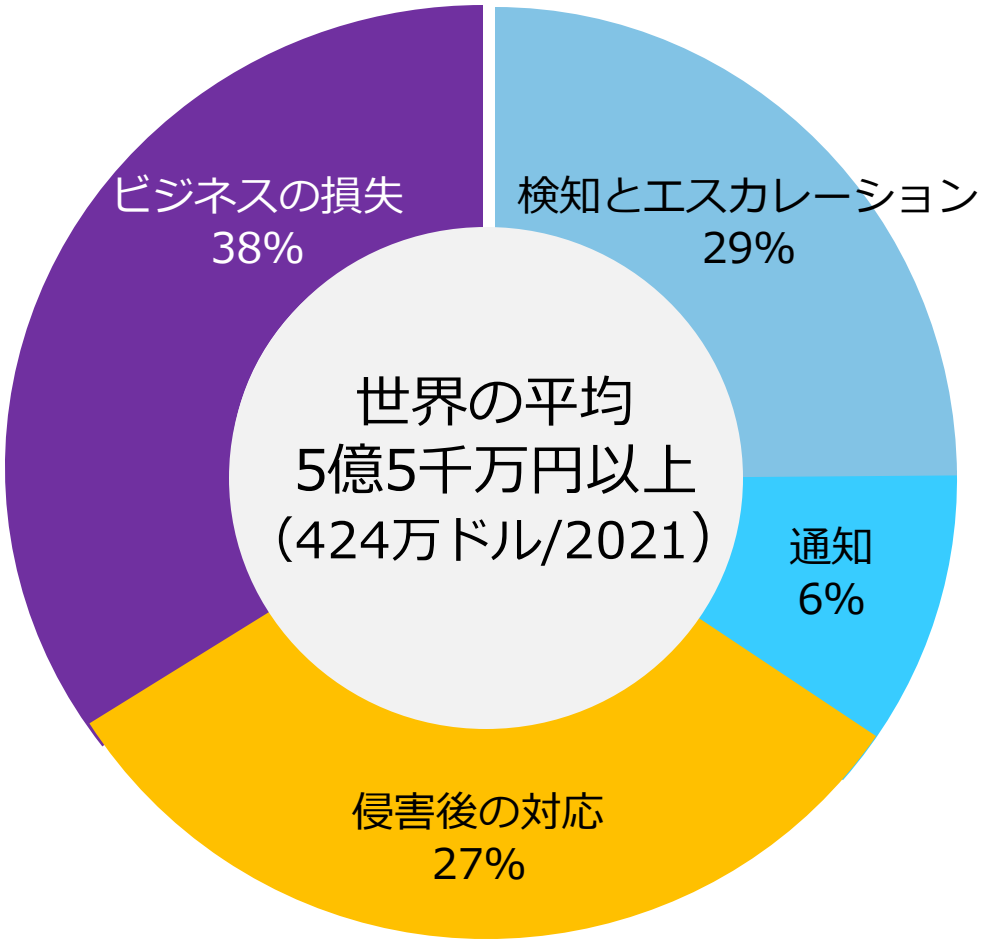
しかし全ての情報が公開されるわけではなく、実際に何が起こっていたのか、知る機会はほとんど得られません。

本講演では、複数の大規模ランサムウェアインシデントに直接対応した経験を元に、実際には何が起こるのか、対策として重要なものは何なのか、ポイントを解説します。

サイバーセキュリティ事故被害額

サイバーセキュリティに関する事故の被害額

- 事故1件当たりの被害金額



参照：IBM X-Forceデータ侵害のコストに関する調査（2021）

攻撃や侵害などを検知（モニタリング）

事故対応（インシデント・レスポンス）

ビジネスの損失

機会損失*によるコストが最も高く、全体の約4割を占める

- システムのダウンタイムによるビジネスの中断や減収
- 顧客喪失と新規顧客獲得のコスト
- 企業評価の低下と業務上の信用の失墜

統計から見るセキュリティ・インシデントの傾向（1/2）

・ インシデント全体における主な傾向

27%
金銭の要求

21%
バックドアが
仕掛けられた

17%
ランサムウェアの
攻撃

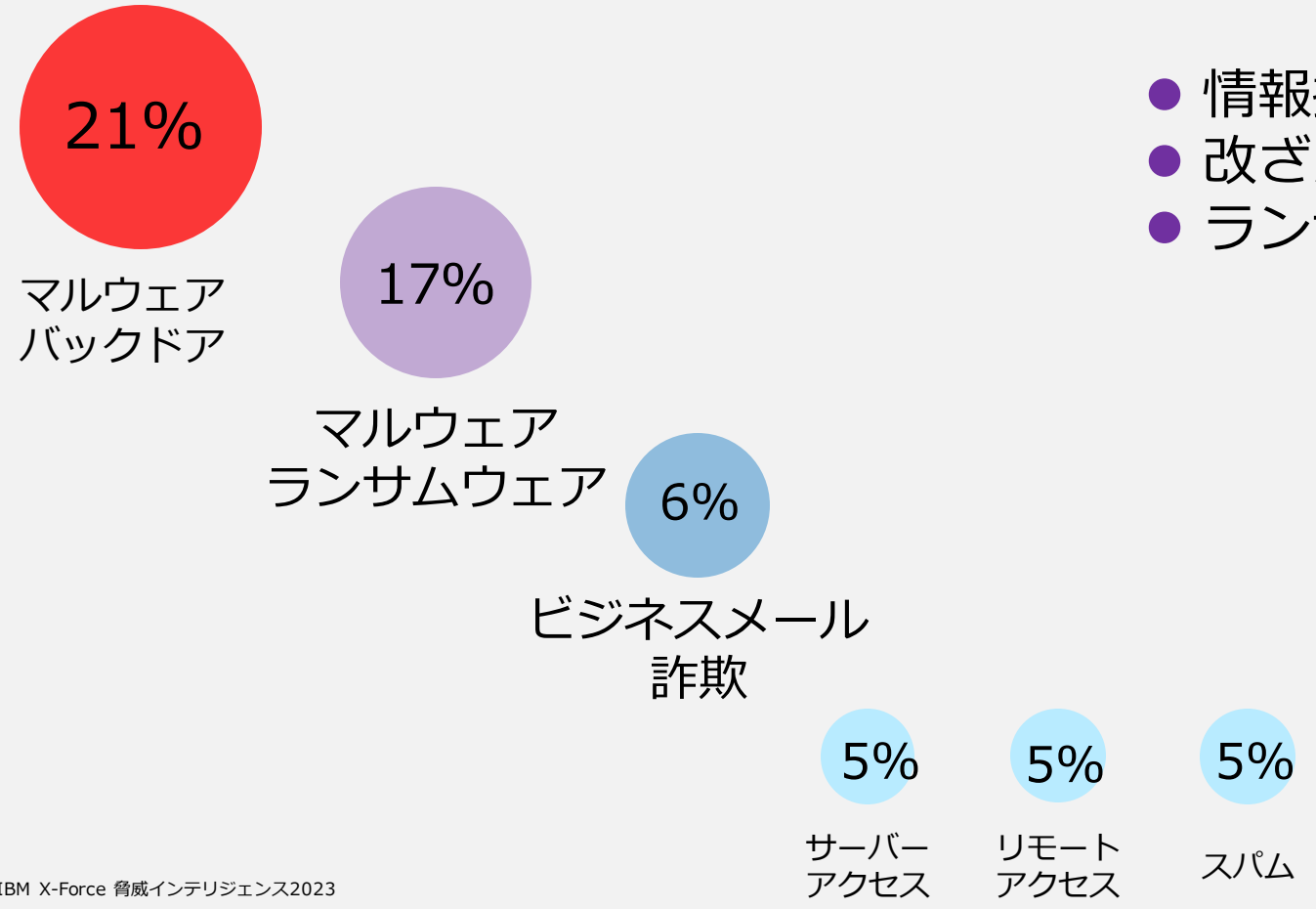
やはり金銭を得ることが目的

- 攻撃者の目的は金銭の奪取
- そのために何ができるか考える
- ランサムウェアは脅迫目的

参照：IBM X-Force 脅威インテリジェンス2023

統計から見るセキュリティ・インシデントの傾向（2/2）

・ インシデント全体でバックドアの仕込みは21%で発生



参照：IBM X-Force 脅威インテリジェンス2023

バックドアを仕掛ければ後で何でもできる

- 情報抜き取り（情報漏えい）
- 改ざん
- ランサムウェアの仕込みなど

サイバーセキュリティインシデントに関連する被害額

- 総務省情報通信白書令和6年版の「10. サイバーセキュリティに関する問題が引き起こす経済的損失」から

調査・分析の実施主体	対象地域	対象期間	経済的損失の概要	損失額
トレンドマイクロ	日本	2023年【調査時期】	過去3年間でのサイバー攻撃の被害を経験した法人組織の累計被害額の平均	1億2,528万円
警察庁	日本	2023年上半期	ランサムウェア被害に関連して要した調査・復旧費用の総額	26%が100万円未満 19%が100万円～500万円未満 25%が500万円～1,000万円未満 23%が1,000万円～5,000万円未満 8%が5,000万円以上
FBI	米国	2022年	サイバー犯罪事件による被害報告総額	102億ドル
NFBI	英国	2023年	サイバー犯罪による被害報告総額	560万ポンド
Sophos	世界14か国	2023年	直近のランサムウェア攻撃の修復に要した１組織あたりの年間平均コスト	182万ドル
IBM	世界16か国	2023年	組織における１回のデータ侵害にかかる世界平均コスト	445万ドル
Cybersecurity Ventures	世界	2025年【予測】	サイバー犯罪によるコスト	10兆5,000億ドル
Fastl	北米、欧州、アジア、太平洋地域	2023年	サイバー攻撃を受けた企業の損失	過去12ヶ月間収益の9%

参照：https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r06/image/f00302.png

被害発生企業に生じる実際の損害

- 株式公開企業ではIR情報をチェックすることで実際の影響を推測することが可能
  - 四半期決算報告の特別損失を確認
  - 一見総務省の情報通信白書の数字との乖離が大きいが、緊急で実装したセキュリティ対策費用などが含まれていると考えられる。
    - 前ページの表に記載されたIBM調査の損失額平均445万ドルは、日本においても決してかけ離れた数字ではない

被害会社（業界）	被害時期	被害額 （特別損失額）	被害内容
KADOKAWA グループ	2024年6月	36億円	250,000件の情報漏洩（個人情報含む）
株式会社イズミ	2024年2月	10億円	7,702,009件の会員情報の閲覧、メールサーバ被害
セイコーグループ	2023年8月	4.５億円	60,000件の情報漏洩（個人情報含む）
株式会社エムケイシステム	2023年8月	1.03億円	情報漏洩件数については公表なし
株式会社オリエンタルコンサルタンツホールディングス	2021年9月	7.5億円	情報漏洩件数については公表なし

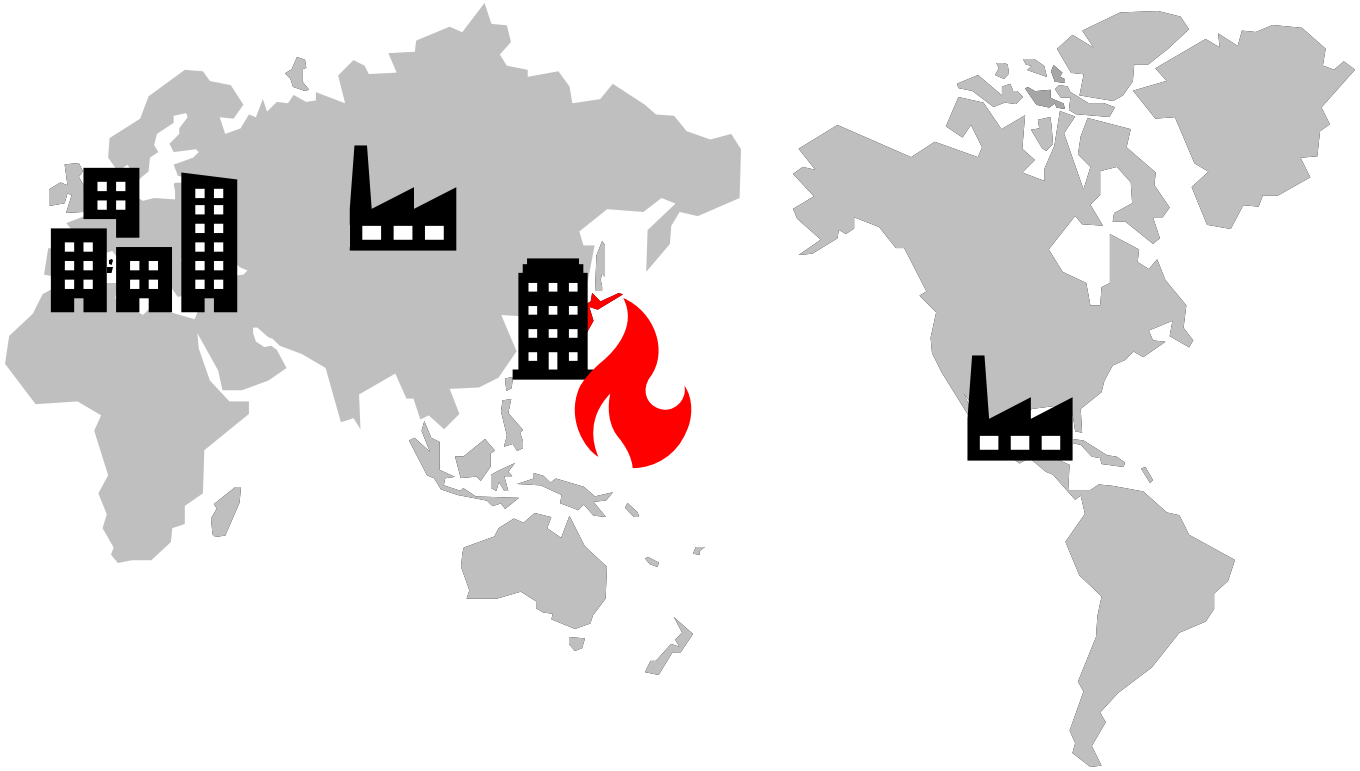
主なランサムウェア被害事例（2021年9月 – 2024年6月）

ISSが対応した
事業停止に陥った大規模ランサムウェア感染事例

Internet Secure Services

インシデントの概要

- 事象
  被害組織グループのデータセンターのサーバー群が暗号化され停止し、工場、販売関係を含むグループ全体の業務が停止。
  攻撃者グループからデータの持ち出しと金銭支払を要求する脅迫メールが届いた。



攻撃のタイムライン

サービス停止により影響が明らかになった日を１日目としたタイムライン

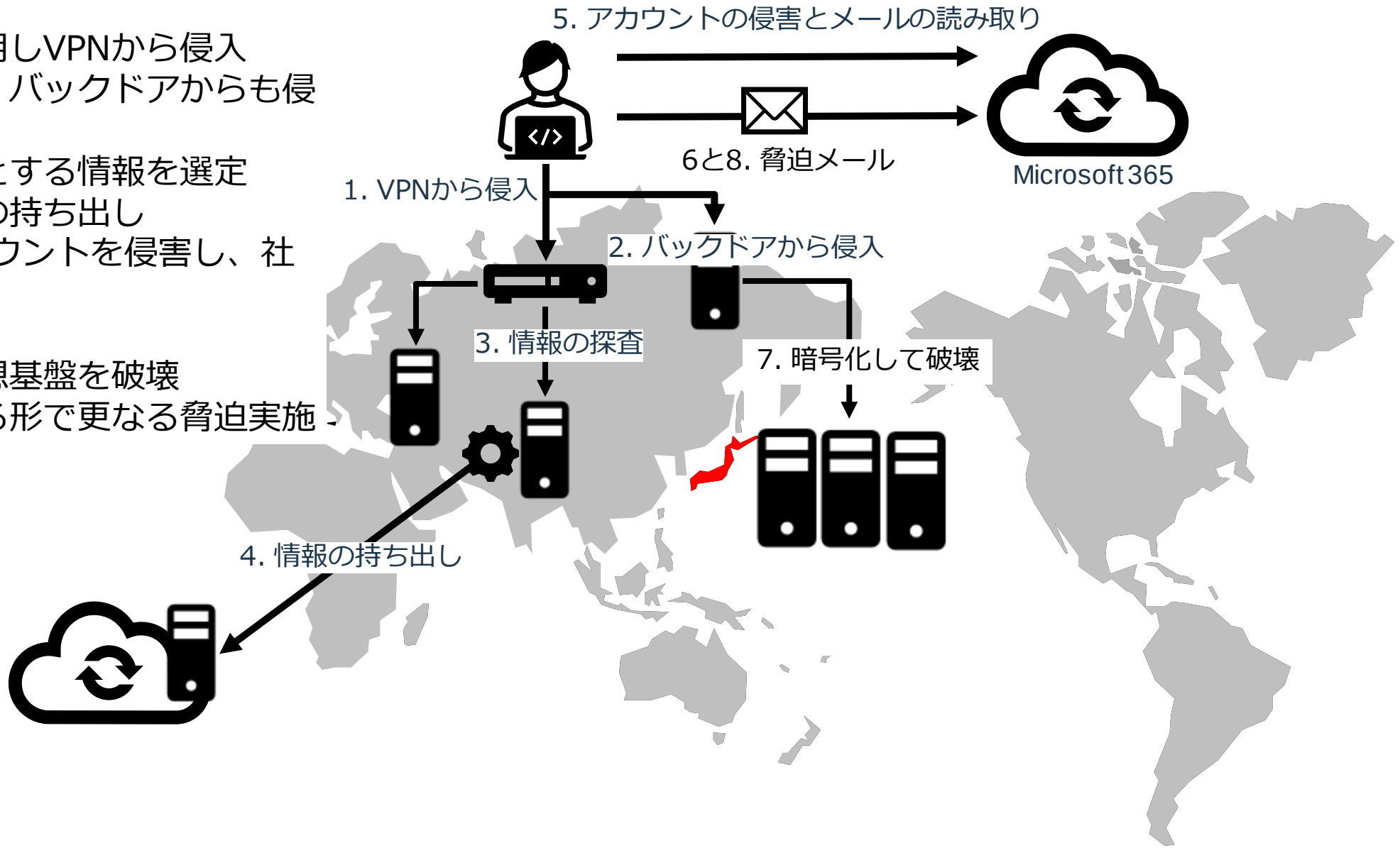
攻撃	攻撃内容	攻撃者の活動	影響範囲
10日前	VPNへのログオンと侵入	VPNから侵入後、Active Directory環境の調査を実施すると共に、複数の管理者権限アカウントの認証情報を収集	日本
5日前	Windowsドメインなど内部環境情報の取得 重要情報の所在確認 データ持ちだしツールの展開	Windowsドメイン環境の情報を収集 管理者権限アカウントの認証情報を収集 持ち出し対象とする重要情報を確認するため、複数のファイルサーバーを閲覧 データ持ち出しツールを複数のサーバーに展開	日本
4日前～前日	情報の持ち出し	データ持ち出しツールを使い持ち出しを実施。持ち出し先は攻撃者が設置したクラウド上のLinuxホスト	日本
1日目	データセンター内仮想環境の破壊	データセンター内の仮想環境が攻撃され仮想OSが暗号化されサービス停止	全世界
2日目	Microsoft 365の侵害 最初の脅迫メール	社員のアカウントを侵害しMicrosoft 365にアクセス。メールを盗み読む 脅迫メールの送付	日本

現場で分かったこと

攻撃者側	内容
VPNから侵入していた攻撃者	• 有効な社員のアカウントが悪用された
様々な攻撃行為	• PowerShellを使った情報収集、権限昇格の試み • Cobalt Strikeバックドアの設置 • リモート同期ツールを使用したファイルの持ち出し • Microsoft 365アカウントへの侵害とメールの読み出し • 仮想基盤上で動作している仮想OSの破壊 • LAN内でのブルートフォース攻撃によるアカウントの侵害 • 様々な脆弱性の悪用行為
特徴的なこと	• ランサムウェアプログラムが仕掛けられていない！ • 社内メールを逐次監視し、社内メールへの返信で新たな脅迫をしてくる
被害者側	**内容**
指揮命令系統が皆無	• 中心人物はいるがファシリテーター的な振る舞い。だれが意志決定を担っているのか分からない
ログが致命的に不足	• そもそもログ取得の設定がされていないなど、調査対象が決定的に不足している
複数のセキュリティベンダーやコンサルファームの参画	• 組織関係者が自分の知っているセキュリティベンダーやコンサルファームにやたら声を掛けたため、一時はベンダーが複数入ってしまい、役割分担もできていなかった

攻撃者の動き

1. 社員アカウントを悪用しVPNから侵入
2. バックドアを設置し、バックドアからも侵入
3. 持ち出しターゲットとする情報を選定
4. ツールを使って情報の持ち出し
5. 社員のMicrosoftアカウントを侵害し、社内メールの読み取り
6. 脅迫メールの送付
7. データセンターの仮想基盤を破壊
8. 社内メールに返信する形で更なる脅迫実施



現場の雰囲気

- インシデント対策室（War room）は映画シン・ゴジラの「巨災対」：巨大不明生物特設災害対策本部のような様相
- 50人～60人程度の人がインシデント対策室で対応を実施（ISSもその一部）
- 急ごしらえのネットワーク（接続ホストが多すぎて遅延が生じるほど）
- 朝・夕のビデオ会議（関係会社なども参加し、何人参加しているのか、分からないほど）
  - システムの復旧を早くしてほしいという現場からのリクエストが殺到
  - 技術的な分析結果に基づく判断や次の調査ポイントなどを具体的に提示できるインシデント対応ベンダーが重要。各所からの状況共有だけでは対応が何も進まない
- 夕方の関連経営者会議
  - 各グループ会社社長が参加（インシデント対策室の一角で実施）

技術的な復旧

被害組織で実施された主要な技術的な対応を列挙します。侵入の根本原因が特定できたことは非常に大きいと言えます。ビジネスパートナーとのビジネス再開のため、原因を特定し正しく対処できたことは重要なポイントとなり得ます。

項目	内容
侵入原因の排除	全社員のパスワード変更と多要素認証の強要 VPNとMicrosoft 365アカウントの両方
内部侵害行為の抑止	悪用に使用された管理者アカウントを無効化 全管理者アカウントのパスワード変更
復旧	別のデータセンターに構築中の仮想基盤上に新たにサーバーを構築 インターネット接続の要・不要によりネットワーク分離を実施
追加セキュリティ施策 （時間を要する対策）	EDR：Endpoint Detection and Responseソフトウェアの導入 SOCの強化 VPNをSASE：Secure Access Service Edgeに移行 各種ログをSIEM：Security Information and Event Managementシステムに集約

発生した非技術的な対応

カテゴリ	項目	内容
意志決定	グループ各社への復旧優先順位の設定	状況の変化で優先順位自体を変更しなければならないことが生じる。事例では社長間で合意していたため、優先順位の変更決定は社長間の合意を要した。
届出	管轄警察署への被害届提出	警察署への通報を検討。被害届の提出などは警察より案内されるのでしたがう。通報を行う際にはセキュリティ会社にアドバイスを受けるとよい。 警察庁のサイト：https://www.npa.go.jp/bureau/cyber/pdf/r50419cpal.pdf
	損害保険会社への届出	保険会社から公表等に係わるアドバイスを受けることが可能。ただしインシデント対応を実施したセキュリティ会社も同席させた方がよい
報告	監督官庁への報告	報告内容はインシデント対応を実施したセキュリティ会社にアドバイスを受けるべき。注意点としては、監督官庁は具体的な質問を受けた際には回答する義務があるため、場合によっては監督官庁への質問などから、セキュリティインシデントの発生が開示されてしまう可能性があること。
	個人情報保護委員会への報告	報告内容はインシデント対応を実施したセキュリティ会社にアドバイスを受けるべき。直接報告ではなく監督官庁経由での報告経路に変更されている。
情報開示	一般への情報開示	開示方法、開示のタイミング、内容、そもそも開示すべきかどうかはインシデント対応を実施したセキュリティ会社にアドバイスを受けるべき。
	ビジネスパートナーへの情報開示	ビジネスパートナーによっては、所定の書式による報告を要求されることがある。根本原因、影響範囲の特定と対策を含める必要がある。インシデント対応を実施したセキュリティ会社に報告書の作成など依頼するとよい。
	株主への情報開示	株主の視点から、インシデントの影響などを説明できるような情報の開示が必要。株主総会で質問されることもあるため、適切な回答を準備しておく。

ランサムウェア被害から得た対策ポイント

技術的対策	入口の強化	VPN、RAS、保守用接続などインターネットからの接続点は、接続可能なIPアドレスを制限する
	認証の強化	パスワードの強化（16文字推奨）、アカウント管理強化、多要素認証の利用
	検知の強化	EDRの導入、ログ管理の強化とSIEMを利用したログ相関分析による早期検知
	初動対応の強化	バックドアや情報持ち出しを迅速に遮断するための、インシデント初動時通信遮断設定の準備
組織的対策	インシデント対応計画の策定	ランサムウェア攻撃が発生した場合の対応手順を定め準備します。大規模インシデントの場合、特別対策部屋の設置、経営陣、法務、広報、インシデント対応責任者の連携が必須
	セキュリティポリシーの強化	特にアクセス制御ポリシーがポイント。最低限のアクセス権限付与、特に管理者権限を持つアカウントの管理厳格化。多要素認証の導入
	サプライチェーンセキュリティ強化	サードパーティやベンダーとのやり取りにおけるセキュリティ対策を強化し、間接的な攻撃のリスクを低減
教育的対策	アカウント取り扱い教育	組織のユーザーIDは極力社外サービスには使用しない、パスワードの使い回し禁止、強力なパスワードの利用など、アカウントの運用に関する教育の強化
	訓練による習熟度向上	シナリオベースのテーブルトップエクササイズなど、シミュレーション型の訓練を実施し、実際のインシデント発生時にスムーズな対応ができるよう習熟度の向上を計る

ランサムウェア被害から得た対策ポイント：技術

- 防御の要は認証強化と高権限アカウントの保護
  - 認証情報保護を第一優先とした方がよい
    - たとえ脆弱性を悪用した攻撃であっても、そのまま攻撃を継続するのではなく次に「高権限アカウント（管理者アカウントなど）を奪取する」ことを目標とする傾向が強い。
    - 多要素認証やゼロトラストアーキテクチャの利用が効果が高い
- 検知能力の強化
  - 社内ネットワークに侵入後攻撃者が実施する行為は検知できないケースが多い。EDRによる検知や、ログ相関分析による検知などを強化

技術的対策	入口の強化	**VPN、RAS、保守用接続などインターネットからの接続点は、接続可能なIPアドレスを制限する**
	認証の強化	**パスワードの強化（16文字推奨）、アカウント管理強化、多要素認証の利用**
	検知の強化	**EDRの導入、ログ管理の強化とSIEMを利用したログ相関分析による早期検知**
	初動対応の強化	**バックドアや情報持ち出しを迅速に遮断するための、インシデント初動時通信遮断設定の準備**

ランサムウェア被害から得た対策ポイント：組織的対応

- 事前準備が重要
  - CSIRT(Computer Security Incident Response Team)またはそのような機能を持つチームが活動できるように準備しておく。
  - 初動の方法、初期隔離手段の開発
  - 厳格なアカウントポリシーの策定と適用
    - アカウントへの権限付与の厳格化、多要素認証の利用など
  - サプライチェーンのセキュリティ規程の作成
    - 日本の企業で本丸のネットワークから直接侵入されるケースより、サプライチェーンで接続された他社経由で侵入されるケースが目立つようになってきた。

組織的対策	インシデント対応計画の策定	**ランサムウェア攻撃が発生した場合の対応手順を定め準備します。大規模インシデントの場合、特別対策部屋の設置、経営陣、法務、広報、インシデント対応責任者の連携が必須**
	セキュリティポリシーの強化	**特にアクセス制御ポリシーがポイント。最低限のアクセス権限付与、特に管理者権限を持つアカウントの管理厳格化。多要素認証の導入**
	サプライチェーンセキュリティ強化	**サードパーティやベンダーとのやり取りにおけるセキュリティ対策を強化し、間接的な攻撃のリスクを低減**

ランサムウェア被害から得た対策ポイント：教育

- 組織に所属する全員への基本的なセキュリティ教育の実施
  - 組織内部アカウントの取り扱いの注意点を具体的に説明することは重要。社内アカウントを外部サービスのユーザーIDとして極力使用しない、パスワードの使い回しはしないなど周知徹底が重要
- CSIRTなどの対応チームに対するインシデント対応時の訓練
  - インシデントシナリオを元に、チームとしてどのような判断をしなければならないか、などを議論することで、チーム自体の習熟度を向上させる。

教育的対策	アカウント 取り扱い教育	**組織のユーザーIDは極力社外サービスには使用しない、パスワードの使い回し禁止、 強力なパスワードの利用など、アカウントの運用に関する教育の強化**
	訓練による習熟度 向上	**シナリオベースのテーブルトップエクササイズなど、シミュレーション型の訓練を実施し、 実際のインシデント発生時にスムーズな対応ができるよう習熟度の向上を計る**

Internet Secure Services