β版

サイバー攻撃を受けた組織における対応事例集
（実事例における学びと気づきに関する調査研究）

※本調査はNISCの委託により、みずほリサーチ&テクノロジーズ株式会社が実施したものです。

2022年3月
内閣官房内閣サイバーセキュリティセンター（NISC）

目次

背景と目的

背景

- サイバー攻撃が巧妙化・複雑化する中、国内ではサイバー犯罪が増加傾向にあり、その脅威は深刻なものとなっています。報道においても、日々、個別のインシデントが取り上げられているものの、風評被害等への懸念から、当事者からは、サイバー攻撃の実情が対外的に公表されないことが多く、サイバー攻撃を受けた際の貴重な経験が共有されがたい状況にあります。
  一方で、我が国のサイバーセキュリティのレベル向上を目的に、経験を共有すべきとの声も聞かれ、一部の企業からは自社の経験も含めて積極的に知見の共有を図りたいとの意見も寄せられています。

目的

- このような状況を踏まえ、内閣官房内閣サイバーセキュリティセンター（NISC）では、サイバー攻撃を受けた企業や研究機関などの協力の下、これらの組織が実際に講じたインシデント対応や、体制強化、人材確保等について、事例調査を実施しました。
- これらの実例を様々な組織でのサイバーセキュリティ対策の検討のヒントとしていただくべく、得られた教訓や気づきを含め、事例集として公開することとしました。（なお、調査にご協力いただいた組織については、特定されないよう匿名化しております。）

本事例集の構成

事例

- 各事例は、以下の構成となっています。

1．概要	サイバー攻撃、それによる被害、サイバー攻撃を踏まえた再発防止策の概要をまとめています。読者のシステム構成や、懸念されるセキュリティのリスクと類似する事例を参照頂けます。
2．状況	攻撃者が、どのようにして該当組織にサイバー攻撃を実施し、どのようにサイバー攻撃の被害が広がり、組織がどのように対処したのか、その概要をまとめています。
3．時系列	組織がサイバー攻撃を検知し、分析、対処した活動を時系列に整理しています。技術的な実施事項だけではなく、対外発表といった組織の各部門の役割を含めています。なお、組織に応じてサイバー攻撃の発生日もしくは検知日を第1日目としています。
4．まとめ	事例に取り上げた組織の得た気付きと取組みをまとめています。  複数組織に共通の気付きと取組みに付与しています。　  組織特有の気付きと取組みに付与しています。 • 受けた背景・国内外の状況： サイバー攻撃発生時点の国内外の状況、および組織固有の状況をまとめています。 • サイバー攻撃による影響： サイバー攻撃による被害をまとめています。 • 発生原因と根本原因の深堀： サイバー攻撃が発生した技術的原因と技術的原因を生み出してた根本原因を整理しています。 • 被害軽減に寄与した対策： 被害を受けたものの、被害の軽減に寄与した対策を整理しています。 • 得られた気付き・教訓： サイバー攻撃を受けて、組織が再発防止を目的に実施した対策を整理しています。 • 今後の課題： 組織がサイバー攻撃への対応力をより高めるために、課題と考える事項を整理しています。

利用方法

- 事例集ヘッダー部の項目の内容は以下の通りです。

想定読者	事例で取り上げられている取組みを実施する想定読者・組織のレベルを示します。 • 基本的取組み：サイバー攻撃への対処の取組みを検討している組織 • 先進的取組み：一定の対策を実施済みであり、更なる対策を検討している組織
組織属性	事例の組織属性。組織の種別や業種等の概要を示します。
要因	発生したサイバー攻撃の主な要因を示します。

これらを参考に、事例集をご利用ください。
例えば、以下の利用シーンが想定されます。

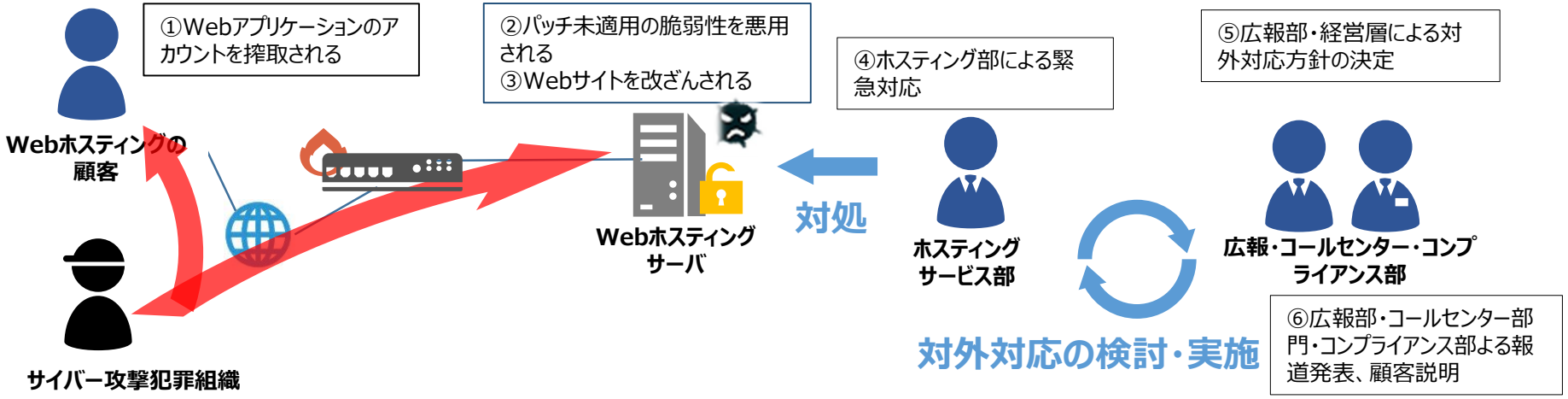
- 経営層の方が、様々な組織の取り組みを概観し、経営課題としてのサイバー攻撃対処への理解を深める
- 戦略マネジメント層の方が、予算確保等、経営層と現場をつなぐ工夫に活用する
- 現場でインシデント対処やセキュリティ対策の実装に携わる実務者・技術者の方が、より、適切かつ効率的に取り組むためのヒントを得る

サイバー攻撃への対応事例

1．概要

- 本事例のA社は、Webホスティングサービスを提供している。
- サービス利用顧客が独自に導入したWebアプリケーションに対して、攻撃者になりすましログインされた後、Webサーバーが稼働するOSの脆弱性を悪用され、Webホスティングサービス上のコンテンツを改ざんされた。
- ホスティングサービスであることから、顧客が導入するWebアプリケーションのセキュリティ対策に関与することが困難であった。また、侵入されたWebサーバのOSには、既知の脆弱性が存在していたが、顧客サービスへの影響を考慮して、パッチ適用を見合わせていた。
- 攻撃の発覚後、ホスティングサービス部による迅速な不正ファイル削除、影響確認作業、広報部による広報活動等により、甚大な顧客被害、経営被害には至らなかった。

2．状況



3．時系列（組織毎の検知・分析・対処）

日時	①経営層	②広報・コンプライアンス部・コールセンター	③ホスティングサービス部
1日目（休）	• Webホスティングサービスの特定顧客が独自に導入したWebアプリケーションのアカウントに正規アカウントで不正ログインされた後、WebサーバーのOSの脆弱性を悪用され、不正なファイルがWebサーバー上に設置される		
1日目（休）夜間			• 運用担当者が、不正なファイルがWebサーバー上に設置されていることを確認 • 攻撃元からのアクセスを遮断 • 攻撃者が配置したファイル削除を開始
2日目（休）早朝			• 攻撃者が配置したファイルの削除完了 • 不正利用されたWebアプリケーションのアカウント停止 • 解析により、該当Webサーバーの正常性、顧客利用環境への影響を確認
3日目	• リスクが高い問題との認識に至り、全社的な問題に格上げし、役員会議にて取り扱いを協議	• コールセンターでの顧客問合わせへの対応 • マスコミからの問合わせへの対応 • 広報部門、コンプライアンス部門にて、サービス事業者としての告知タイミング、告知内容、公表範囲、メディアからの質問への回答方針を検討し、役員承認を得る	
		• JPCERT/CCから問い合わせ	
			• ホスティングサービスの利用顧客に、状況をメール連絡
5日目		• コンプライアンス部、広報部、ホスティングサービス部で対外発表対応を調整	
		• 不正アクセス被害とその対処が完了したことを対外発表 • JPCERT/CCに対応状況を回答	
7日目		• 不正アクセスの詳細を対外発表	

４．まとめ

背景・国内外の状況

- 本事象で悪用されたWebアプリケーションは、オープンソースソフトウェアであり、世界中のWebサイトで幅広く利用されているため、攻撃者の攻撃対象となりやすく、攻撃は、頻繁に行われている。
- 本件で悪用されたOSの脆弱性は、公知の脆弱性であり、設定の不備といった人的なものではない。

発生と検知、エスカレーションと役割分担、対応

- 「２.状況」、「３.時系列」を参照

サイバー攻撃による影響

- Webホスティングサービスの複数顧客のサイト（数千社）に、不正なファイルが配置されたことで、Webサイトの改ざんが発生した。

発生原因と根本原因の深堀り

- 悪用された脆弱性は、OSの既知の脆弱性である。
  - A社が**パッチを適用していれば**、本事象の発生は防止できた可能性が高い
- ホスティングサービス部門においても、原則としてセキュリティパッチ適用が定められているが、現場担当者にパッチ適用判断の裁量が与えられていた。**パッチ適用に関わる作業負担を軽減**できることもあり、各担当者は、当該パッチの緊急度が高くないと判断し、**パッチ適用を見送っていた**。
- 組織としても、**パッチ適用による顧客の利用環境への悪影響を懸念**しており、現サーバにパッチを適用するのではなく、脆弱性を解消した新しいホスティング環境を構築し、顧客に移行を打診していた。しかしながら、**契約上は移行の定めがなく**、新環境への顧客移行が進んでいない状況であった。

被害軽減に寄与した対策

- ホスティングサービス部門では、顧客の誤操作による意図しないコンテンツ改変事象に関する運用手順書を整備済であったため、インシデントによるコンテンツ改変自体への技術的対策を迅速に実施できた。手順書が整備されていなかった場合には、システムの復旧に多大な時間を要したと想定される。

4．まとめ

得られた気付き・教訓

- 脆弱性およびリスク管理が属人的であり、組織として対処する必要があり、対策した。
  - 組織としての脆弱性の対処基準を定めた。
  - 脆弱性情報を社内で共有・展開し、リスク認識を共有した。
- 24h×365d稼働を原則とするWebホスティングサービスのパッチ適用に関して、顧客との事前合意が必要であり、対策した。
  - パッチ適用運用に伴うサービス停止時間を含め、**SLAを明確化**した。
- インシデント発生時には、ホスティングサービス部門による判断と対処が中心となっていたため、全社的なインシデントへの対応体制を強化した。
  - 他サービス部門や管理部門を交えた**組織横断的な、インシデント対応体制を整備**した。
- 経営層と現場担当者とのコミュニケーション不足を改善した。
  - **経営層への報告を定例化**することで、経営層が現状および課題を的確に把握すると共に、現場担当者が経営層の意思決定に基づき迅速にセキュリティ対策に取り組むことができる。
  - セキュリティインシデントを経験し、経営へのインパクトが非常に大きいとの認識に至り、サービス維持よりもセキュリティを重視するように経営層の意識が変化した。
- 実務で利用するために**十分な詳細度で定義されたインシデント対応手順**に基づき、対処するように体制を再整備した。
  - サイバーセキュリティ基本動作を啓蒙、励行する。
  - **部門横断で、演習等を通じてインシデント対処体制を確立**する。

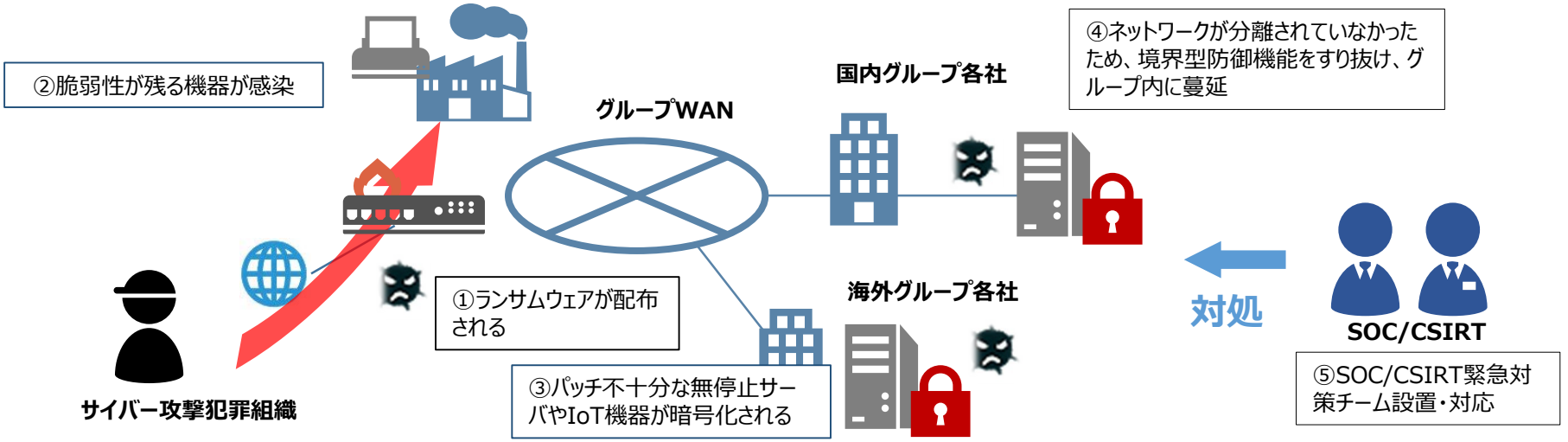
今後の課題

- **運用担当者のパッチ適用に関する作業負荷を低減**し、迅速なパッチ適用やセキュリティリスク分析を実施できる環境整備に取り組む方針である。
- **セキュリティインシデントの対応現場は、各社のノウハウ**そのものであり、インシデント対応にあたって最後に**頼る（は）人材**である。人材確保が難しい状況にあるが、**自社で確保**するように検討を進めている。
- 他部門では、**ISMS認証**を取得済であり、セキュリティマネジメントシステムを有効活用したいが、部門毎にセキュリティ運用の実態が異なっており、組織や手続きの整備と統合を**段階的に進める**よう検討している。
- 高度なサイバー攻撃への対処のために、更なる環境整備が必要である。
  - ログの効率的な取得、分析を属人管理から組織的管理とするため、**様々な機器のログの統合分析、**AIの利用をはじめとするツール選定が課題である。
  - **不審な動きの可視化**の必要性を認識しているが、**不審なふるまいの定義**などが課題である。
- 利用者責任範囲とセキュリティリスクを顧客に周知することが難しく、顧客の獲得と維持が難しくなることを懸念している。**セキュリティリスクを非常に低く認識している顧客に対して、丁寧な説明**とニーズにマッチしたサービスの提供を検討する方針である。

1．概要

- 本事例のB社グループは、多数の海外拠点を有するグループ企業である。
- 海外支店の機器がランサムウェアに感染したことを発端に、グループ企業内全てに攻撃被害が広がった。
- ランサムウェアが悪用した脆弱性は、グループ内でも認識されていたが、無停止が求められるサーバ、パッチ適用の必要性が認識されていなかった、あるいはパッチが適用できないIoT機器に脆弱性が残存していたことから、グループ内にランサムウェアが拡散した。
- ランサムウェアによる破壊活動への対策として、バックアップ含むサイバーBCP対策に、特に重要な気付きがあった。
- 攻撃の発覚後、全社的な組織体制の見直し、サイバー攻撃への耐性を高める取り組みを着実に進めている。

2．状況



3．時系列（組織毎の検知・分析・対処）

日時	①経営・広報	②CISO・SOC・CSIRT	③IT部門・業務部門
1日目　22:00			• サーバ監視でのシステム障害を検知
1日目　22:30			• 運用担当者が、ランサムウェア画面が表示されるとの連絡を受ける
		• セキュリティチームおよびIT運用チームによる緊急対策チーム立ち上げ • 緊急対策チームとITインフラ部門が連携し被害状況収集、攻撃情報収集開始	
2日目（休）1:00		• アンチウイルス、機器のログ分析を開始 • アンチウイルスベンダーに検体の解析を依頼	
		• ITインフラとセキュリティ部門幹部へのエスカレーションと緊急対策本部設置を発動 • 外部への悪影響がないことから、インターネットを切断しないことを判断 • 部分的な社内LANの遮断を実施	
2日目（休）		• 対策方法の立案完了 • 各部門のセキュリティ責任者に、電話連絡にて対策を通知	
2日目（休）9:00	• CIOを中心とした緊急対策本部主導での復旧開始		• 各部門から被害情報を収集・分析
		• 対策ソフトウェアの配置方法の検討と実装開始	
		• ログを収集し、原因究明に着手	
3日目（休）		• 感染元の一次特定が完了し、詳細調査を開始。その他の原因分析も並行して実施。(数日でログ分析終了し、特定終了。その後現地でのフォレンジック調査を実施)	• 復旧作業を継続
4日目	• 広報から、メディアに事案を連絡		
6日目	• 広報から、ニュースリリースを発表		• 被害を受けたシステムの復旧が概ね完了（全面復旧は週内）

４．まとめ

背景・国内外の状況

- 全世界でワーム型のランサムウェアが猛威を振るい始め、日本国内でも、大きな被害の発生が懸念されていた状況であった。
- 本件で悪用されたOSの脆弱性は、公知の脆弱性であり、設定の不備といった人的なものではない。

発生と検知、エスカレーションと役割分担、対応

- 「２.状況」、「３.時系列」を参照

サイバー攻撃による影響

- 被害範囲は、情報システム部門が管理する社内ネットワーク上の業務システム、事務用PCに留まらず、工場に設置された生産システム、入退室管理システムなど、多岐にわたった。

発生原因と根本原因の深堀り

- 悪用された脆弱性は、汎用OSの既知の脆弱性である。
  - PC等に関しては、パッチを適用していれば、本事象の発生は防止できた可能性が高い。
  - パッチが適用できないIoT機器等について、ネットワークに接続するリスクや対策が検討されないまま、利用されていた。
- ワームによるサイバー攻撃を前提としたネットワーク設計がなされていなかった。エンドポイントによるウイルス対策を前提とした、セグメント化されていないネットワークのため、一旦端末がランサムウェアに感染すると、拡散を抑えることが難しい状況にあった。また、ネットワーク状況を、集中監視ができていなかった。
- 自然災害を想定したリアルタイムバックアップと世代管理バックアップを実施していた。**リアルタイムバックアップは、復元には利用できず**、世代管理バックアップから復元した。
- **24hx365d稼働が求められているサーバには、パッチ適用サイクルが短期間で実施できていなかった。**同様に、通常のOA機器と異なり、**IoT機器についてもパッチを適用することの必要性が認識されていなかった。**

被害軽減に寄与した対策

- 各システムのバックアップサイトにランサムウェアが悪用する脆弱性が残存していなかったことから、バックアップデータを利用したシステムの復旧が可能であった。
- インシデント発生時の**一次切り分け時には、過去にワーム被害を経験した人員が関与**できたことから、**過去のノウハウ**に基づき、目の前の事象がワームであることを迅速に把握し、ワームを念頭に置いた対策を迅速に立案することができ、インシデントの早期収拾に寄与した。

4．まとめ

得られた気付き・教訓

- 接続するものが多様化し、社内ネットワークへポリシーに準拠できない機器が増加していた。
  - いろいろなものがつながる前提で、社内ITに加えて、**生産製造環境へもサイバーセキュリティ対策徹底**を推進した。
  - 取得可能なログを確認し、検知に有用なものは新たに監視対象に加えた。
  - サイバー攻撃を踏まえた**バックアップ方法**、シナリオ、行動フローを整備した。
- パッチ適用が徹底されていなかった。
  - 「あてなくても大丈夫」から**「あてなければいけない」文化への変革と、適用プロセスを整備**した。
- **サイバーセキュリティを、経営課題としてとらえて対処**をする必要性を再認識した。
  - CISOおよびCISO配下にグループ全体のセキュリティを統括する専門組織を設置し、セキュリティ対策徹底のための複数部署をまたがるバーチャル組織を構成した。
  - 社内モニタリング状況に基づいたサイバー警報ルールを制定し、警報に応じてサイバーBCPを発動する手続きを整備した。
  - 現時点の脅威情報に基づき、サイバー攻撃のシナリオを拡充しつつ、BCPをアップデートしている。**有事に的確に行動をとるための訓練や演習を拡充**・実施した。
- 経営層や社員への説明に、**リスク状況および対策状況等を可視化**することが有効であると考えている。セキュリティに関わる施策や取組結果の定量化の検討に着手している。
- 幅広い分野でセキュリティ人材が不足していた。
  - 人員計画を策定し、教育を進めた。
  - OT現場に蓄積されている多種多様なノウハウを活かし、OT人材にセキュリティ教育を開始した。

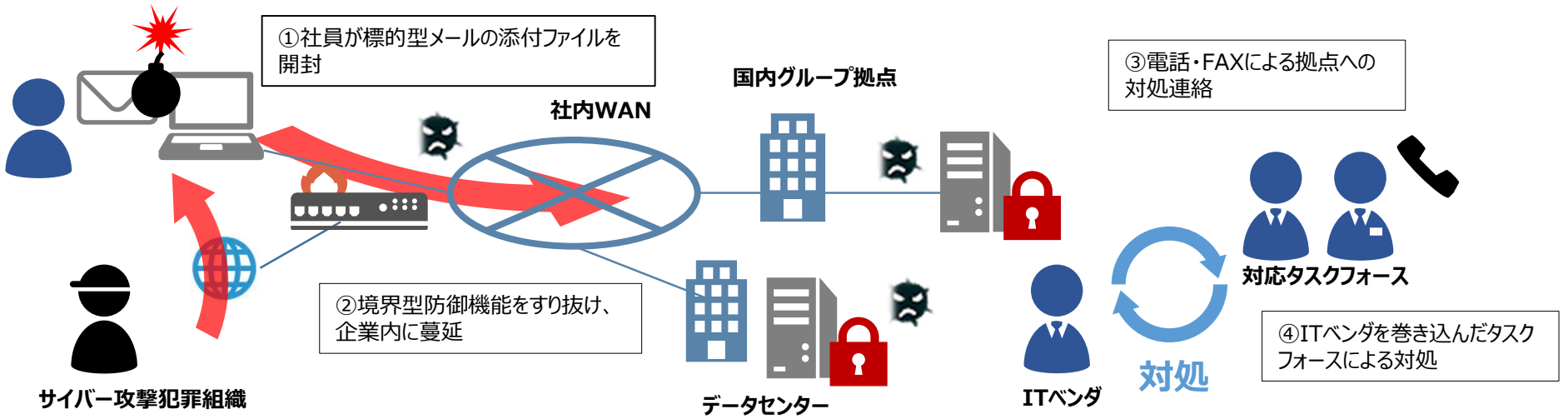
今後の課題

- サイバーセキュリティ体制の成熟度モデルである、Sliding Scale of Cybersecurity の、「Intelligence」レベル相当を目標として検討している。これには、社内で、脅威情報を分析し、実施すべき事項を整理し、各部門に展開・活用する仕掛け、**外部組織と状況を共有**する仕掛けが必要と考えている。
- ゼロトラスト化を進める中で、自前システムとゼロトラストのハイブリット化に取り組む必要がある。
- セキュリティ教育だけではなく、組織構成員の一人一人が、自分の仕事の一要素としてセキュリティが含まれていること、自身に直結することとして認識してもらう「自分ゴト化」に取り組んでいる。
- **資産管理の対象として、OSSやLINUXの管理**が必要と認識している。
- ランサムウェア対策には、重要サーバの堅牢化が不可欠であり、管理が及ばない事業部門**個別のサーバや野良サーバの識別**に取り組む必要がある。
- 自組織のセキュリティ対策の実効性を確認するために、Redチームテストを企画している。

1．概要

- 本事例のC社は、全国に多数の営業拠点を有する企業である。
- 取引先を装ったメールの添付ファイルを従業員が開封したことでランサムウェアに感染し、ファイルサーバや業務サーバの大部分が暗号化された。
- 本ランサムウェアは、既知のウイルス対策ソフトウェアでは検出できない未知のタイプであり、未知のランサムウェアの侵入を想定した、検知システム、バックアップ、サーバ復旧手順や代替システムへの切り替手順などの整備が十分ではなく、復旧までに数か月を要した。
- 公共意識の高い企業風土であり、システム復旧に時間を要しても身代金支払いを拒否することを、インシデント対応の初期段階で意思決定した。
- 攻撃の発覚後、監視システムの強化、全社的な組織体制の見直し、サイバー攻撃への耐性を高める取り組みを着実に進めている。
- 同業他社との勉強会の中で、サイバー攻撃対応の実態を情報公開し、啓蒙活動した社会的貢献は多大である。

2．状況



3．時系列（組織毎の検知・分析・対処）

日時	①経営・広報	②リスク管理委員会	③情報システム部門
1日目			• 取引先を装ったメールを受信し、添付ファイルを開くことでランサムウェアに感染
7日目　未明			• ランサムウェアによりIT機器が暗号化されはじめる
7日目　7:00			• 社内各所より、社内システムが利用できないとの問い合わせが集中
7日目　8:30			• IT担当者が、社内システム上のファイルの暗号化を確認 • 電話で全国の支店およびデータセンターに端末のネットワークからの離線を指示 • セキュリティ担当ベンダおよびサーバ機器のベンダに連絡
7日目　10:00			• サーバ内に、攻撃者への連絡先が記載されたファイルを検出
2週目	• システム障害に関するお知らせ第1報を発表	• 社長を委員長とするリスク管理委員会で攻撃者と連絡を取らないことを意思決定 • インシデント対応のタスクフォースを立上げ	
	• サプライヤー、顧客への状況報告を指示 • サプライヤー、顧客に営業担当者から状況を個別に説明		
			• セキュリティベンダーの調査により、盗まれたデータの一部がダークウェブに公開されていることを確認
			• アンチウィルスソフトの再インストールを開始 • 基幹システムが復旧
3週目以降			• 代替手段としてWebメールを契約
			• ファイルサーバを復旧
	• システム障害に関するお知らせ続報を発表		• メールサーバ復旧

４．まとめ

背景・国内外の状況

- 日本国内においても、ワーム型のランサムウェアが猛威を振るい始め、大きな被害の発生が懸念されていた状況であった。
- 本ランサムウェアは、定義型の既存のウイルス対策ソフトウェアでは検出できない未知のタイプであった。

発生と検知、エスカレーションと役割分担、対応

- 「２.状況」、「３.時系列」を参照

サイバー攻撃による影響

- 大部分の社内サーバが暗号化されたものの、身代金支払いを拒否し、暗号化されたサーバを再構築し、汚染されていないバックアップデータ、顧客等から再度入手したデータにより復旧した。再入手できないデータについては復元を断念した。 復旧まで数カ月を要した。
- 数か月間メールが利用できないことによる現場生産性の低下、顧客信用の失墜といった、金額に算定できない影響も発生した。

発生原因と根本原因の深堀り

- 未知のランサムウェアによる標的型攻撃を受けた。
  - ▶ 攻撃者が侵入した場合の検知および対処のシステム整備が十分ではなかった。**定義型のウイルス対策ソフトウェアに依存**しており、未知のランサムウェアに一旦社内に侵入されると、被害を限定することが難しかった。
- 復旧したサーバのネットワークへの接続手順や、代替システムへの切り替えタイミングなどの整備が十分ではなかったことから、復旧までに長期期間を要した。
- **サイバーセキュリティを考慮しないBCP**であったため、バックアップもランサムウェアに汚染されたため、バックアップからすべてのデータを復旧することが難しかった。

被害軽減に寄与した対策

- 支店のネットワーク等は、本社のネットワークから分離されていたことから、ランサムウェア感染が及ばなかった。また、基幹システムは被害を受けたサーバとはアーキテクチャが異なるため感染を免れた。
- 一部のサーバの**バックアップは、履歴を保持する仕組み**であったため、前日バックアップデータを利用したシステムの復旧が可能であった。
- 本業での**緊急連絡ルートが整備されていたことから、各拠点へのインシデント初動連絡が迅速**であった。

4．まとめ

得られた気付き・教訓

- 定義型のウイルス対策ソフトウェアに依存していたことから、未知のマルウェアへの対策を進めた。
  - ▶ 侵入時の挙動を検知して被害を限定するために、**EDRを導入**した。IT部門だけでは挙動の判断が難しいため、SOCサービスをあわせて契約し、**24hx365dの監視体制**を整備した。
- インシデント発生時の対応計画および関連する準備を進めた。
  - ▶ **インシデント発生時の対応手順を整備し、訓練**を実施した。また、**CSIRT整備**に着手した。
  - ▶ 情報システム部門の**人員を増員し、情報セキュリティ基盤の整備**をすすめた。
  - ▶ 改訂に時間を要する規則ではなくガイドラインを整備して、対応手順や対策ポイントを迅速に更新している。また、エンドユーザーがサイバー攻撃に遭遇した際に、**迷わずどうすればよいのか判断できるように、ポケットブック**を整備した。
- **強いポリシーを持って、情報公開**を進めた。
  - ▶ リスク管理コンサルティング会社と連携しながら、積極的な情報公開を行った。批判的な意見・報道を受けることはなかった。
- セキュリティ対策の必要性を経営層と共有する必要がある。
  - ▶ **公表されている同業他社のセキュリティ投資額といった定量的な情報**やIPAの情報セキュリティ対策ベンチマーク等を活用し、自社のセキュリティ対策状況を可視化し、セキュリティの必要性を、機会がある毎に伝えている。
- 侵害発生時にオンプレミスサーバの被害を軽減するため、**システムのクラウド移行**を進めている。

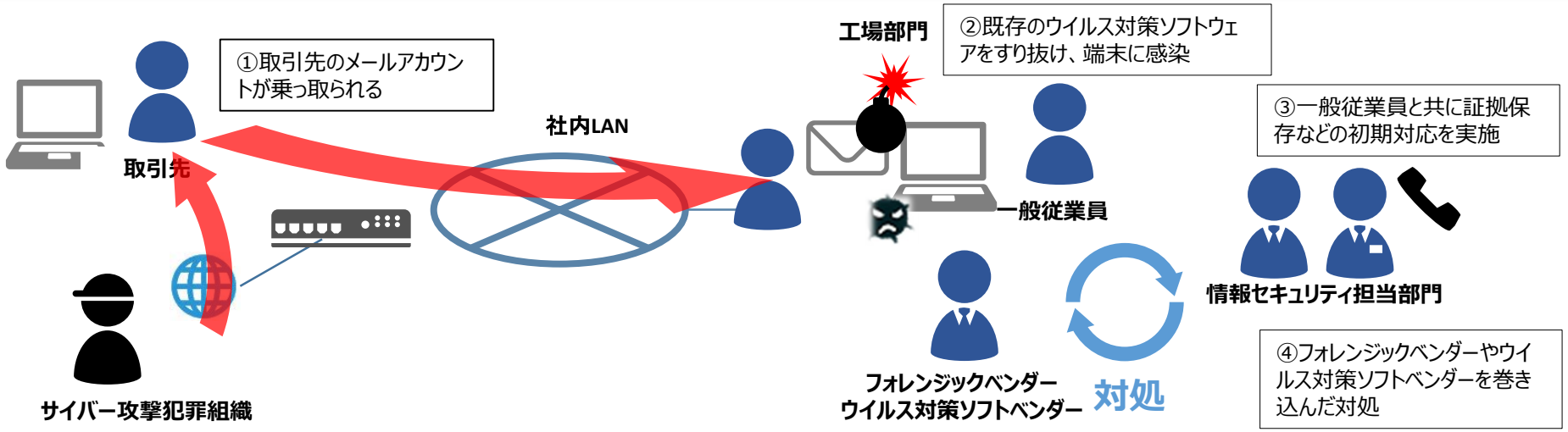
今後の課題

- **DX推進とセキュリティ強化の取り組みを一体**と考えており、同業他社よりも一歩進んだセキュリティの確立を目指している。
- 標的型メール訓練等を実施しているが、メールを開いたりした場合に、何に注意すべきかを、わかりやすく全員に周知徹底することが重要と再認識をした。セキュリティ意識の向上と維持が課題である。
- 顧客の要望等により**個別に導入されるIoT機器は、機器の種別や環境等も異なることから、セキュリティ対策を実現するための個別のルール作り**などが課題となっている。
- システム的な連携が行われると、サプライヤーや下請企業の脆弱性が自社のリスクにも直結するため、**サプライヤーに対するセキュリティ教育や監査が必要**と考えている。
- インシデント時に、バックアップデータからの復元や提供元からの再提供が受けられなかったデータが存在した。迅速な復旧を実現するうえで、**データバックアップに関する見直し**が必要である。
- 定期的に脆弱性診断を実施し、診断結果に基づきシステムをレベルアップする検討に着手した。

1．概要

- 本事例のD社は、サプライチェーンに様々なセキュリティレベルの企業を抱えている。
- D社工場部門の取引先企業のアカウントが攻撃者に乗っ取られた。攻撃者は、取引先企業を装い、D社の工場部門担当者宛にマルウェアをメール送付したことで、D社工場部門の端末2台がマルウェアに感染した。
- ゼロデイ攻撃であったため、既存のウイルス対策ソフトウェアでは検知できなかったものの、導入済のEDRにより検知した。
- 情報セキュリティ担当者が、日常的な情報収集において当該攻撃手法の特徴を把握していたこと、感染現場において情報セキュリティ担当ではない一般従業員と共に迅速かつ適切に証拠を保全できたこと、フォレンジックベンダーやウイルス対策ソフトベンダーとの迅速な連携により、端末2台の感染に留めることができた。

2．状況



３．時系列（組織毎の検知・分析・対処）

日時	①経営・広報	②情報セキュリティ担当部門	③工場部門・人事部門
1日目		• EDRにて、異常なふるまいを検知	
2日目　14:00		• 詳細調査を実施 • EDRで、該当PCの論理隔離を実施	
2日目　16:00		• 社内の掲示板に注意喚起 • グループの全セキュリティ担当者に注意喚起のメールを送付 • ウイルス対策ベンダに検体を提出したところ、マルウェアとの回答を受領	• 工場部門の該当PCの担当者に電話連絡するも、つながらないため、人事部門の上席者に連絡し、ネットワークからの分離とスリープ状態での本社への端末配送を依頼
5日目　8:30		• フォレンジックベンダに、PCの解析を依頼	
6日目		• ウイルス対策ベンダによりシグネチャが作成され、社内に展開 • 他のPCに影響がないことを確認	
2週間目	• 攻撃元となった取引先から状況報告を受領		

４．まとめ

背景・国内外の状況

- D社工場部門が取引する企業が攻撃を受け、取引先企業のアカウントが攻撃者に乗っ取られた。
- 攻撃者が、取引先の正規アカウントを乗っ取っていたことから、メール自体に不審な点をみつけることはできない状態であった。。
- 本マルウェアは、定義型のウイルス対策ソフトウェアでは検出できない未知のタイプであった。

発生と検知、エスカレーションと役割分担、対応

- 「２.状況」、「３.時系列」を参照

サイバー攻撃による影響

- 迅速な封じ込め作業の結果、端末2台の感染に抑えることができた。
  対処が遅れていたらランサムウェアに感染し、事業活動に大きく影響したと思われる。

発生原因と根本原因の深堀り

- 未知のマルウェアによる標的型攻撃を受けた。
  - ▶ 取引先が乗っ取りを受けていることから、自社単独では防ぐことが非常に困難である。**取引先を巻き込んだセキュリティ対策**が必要である。

被害軽減に寄与した対策

- **EDRを導入**していたことから、定義型のウイルス対策ソフトウェアでは検出できなかったマルウェアのふるまいを検出することができた。
  また、**EDRベンダーと良好な関係**を築いており、本事象について迅速な分析を実施することができた。
- インシデント発生を早期に捉えられるよう、平時からIOCや公知の脅威情報等を収集分析していた。
- 平時から、証拠保全の方法などの**具体的なインシデント対応訓練をフォレンジックベンダから受けており**、インシデントの初動が適切であった。
- 平時から、フォレンジックベンダと良好な関係を気付いており、インシデント発生時に、速やかな調査がなされた。
- ウイルス対策ベンダーと良好な関係を築いており、速やかに未知のマルウェアに対するシグネチャーの提供を受けることができ、他の端末の感染を防止することができた。
- サイバー保険に加入しており、インシデント対応の費用を賄うことができた。

4．まとめ

得られた気付き・教訓

- 経営者、非セキュリティ部門の理解を得る必要がある。
  - **リスクコンサル企業やサイバーセキュリティオンライン評価サービス**を活用し、自社の資産とセキュリティリスクの定量化を図り、関係者への説明に活用している。
  - 一部のeラーニングでは、**トレーニング後のテストを止め、家庭でも見れるような短時間の動画を提供**し、受講者が腹落ちして自身の行動が変わるような試みとしている。
  - セキュリティ担当者は、家族にも説明できる程度の平易な用語を用い論理的に説明できるスキルを磨いている。
- 取引先のセキュリティレベルの底上げと管理を実施した。
  - **ヒアリングシートを使用して、取引先のセキュリティ状況をチェック**するようにした。
  - 取引先の増加に伴いアンケートシステムを導入し、効率的に取引先を管理できるよう工夫している。
- セキュリティ部門だけでなく、全社としてサイバー攻撃に対応する体制を整備する必要がある。
  - 身代金の支払い等は、企業リスク管理の範疇あり、セキュリティを経営課題として認識してもらうため、**法務部門や広報部門もセキュリティに関心を持つよう情報共有**し、CSIRT訓練に各部門を関与させることで、雰囲気の醸成を図っている。
  - **セキュリティ部門人材の他部門等への異動、他部門の面接プロセスへの立ち合い等**を通じて、各部門を支援している。
  - 警察をはじめとする外部組織と平時からコミュニケーションを図る。
- インシデント発生時に**キーパーソンと密に連絡**を取る必要がある。
  - インシデント対応計画の中で一斉連絡のプロセスを定義しているが、一斉連絡は混乱を生むケースがあり、キーパーソンとは個別連絡と情報の補足などを行い、密なコミュニケーションを心掛けている。

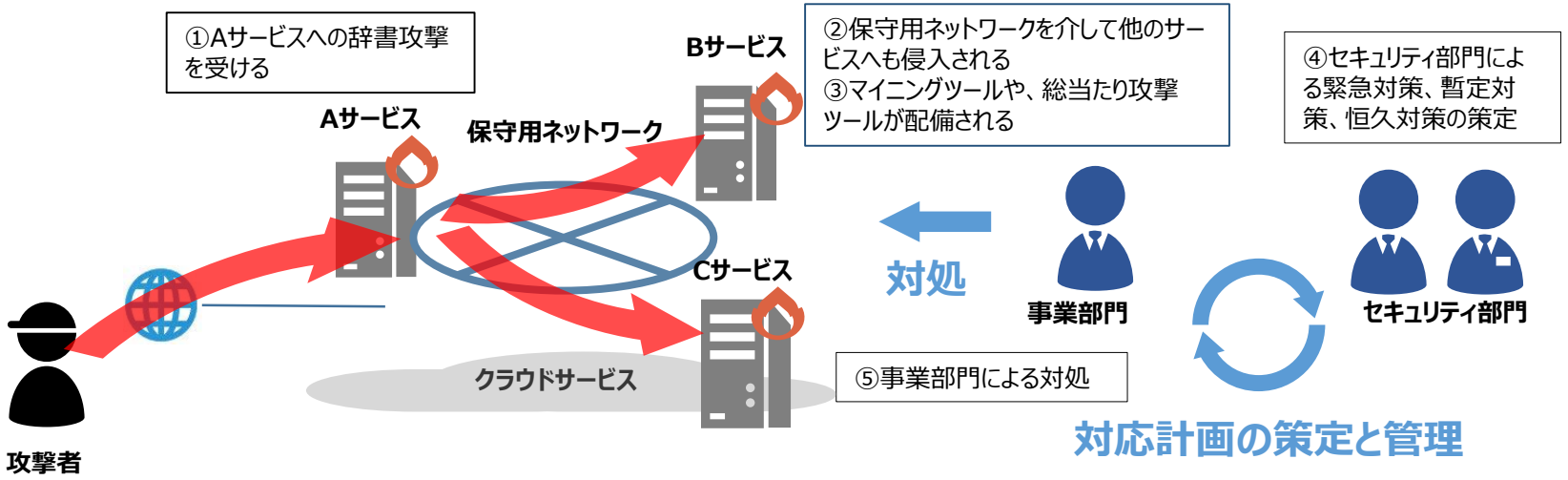
今後の課題

- 今後も取引先の脆弱性に巻き込まれることは懸念されるが、どこまで、取引先をアセスメントするのか、**支援するのか**課題である。**実施コストを自社が負担することに壁**がある。
- **セキュリティ人材が不足**している。
  - 社内にチャンピオンと呼べる専門家を育成し、**先生として人材を育成**することを検討している。更に、モチベーション、プロフェッショナル意識を高めるよう、職務環境の向上に努める必要がある。
- ITとセキュリティ部門が**一体であると、IT部門とセキュリティ部門との適度な緊張関係の維持が難しい**。監査部門が第三者の目線でセキュリティ要求や対策を指摘・管理する体制を検討している。
- **工場のセキュリティを高める**ことが課題である。
  - IT担当者をセキュリティ部門に異動させて、IT担当者が構築したシステムをセキュリティ視点からレビューすることを検討している。
  - 最新の国内工場のシステムを構築したベンダに、自社工場のアセスメントの依頼を検討している。
  - 工場全体に影響が及んだ場合のインシデント対処の役割分担や権限を整備する必要があるが、**工場毎にリテラシーや意識の差があり、一概に定められない**。
- 新しい脅威や技術に対応するためには、情報収集と積極的な新技術の検討と採用が必要であるが、**予算と人員の確保**が課題である。

1．概要

- 本事例のE社は、クラウドサービスを提供する企業である。
- マルチテナントで稼働するクラウド環境で開発及び運用するサービスの一つであるAサービス（構築中）において、従来より実施していたアクセス制限を解除したため、辞書攻撃による不正アクセスが発生。
- 保守用ネットワークの分離が十分ではなく、管理者アカウントに推測容易なパスワードを付与していたことから、Aサービスのサーバを起点に保守用ネットワークを経由して、Bサービス（構築中）、Cサービス（運用中）に不正アクセスされた。
- 攻撃の発覚後、保守用ネットワークの分離、パスワードやファイアウォール規則の管理など、開発から運用までの全ライフサイクルにおける製品セキュリティ確保のための手続きおよび体制の整備に着手している。

2．状況



3．時系列（組織毎の検知・分析・対処）

日時	①自社経営層	②セキュリティ部門	③事業部
検知の11日前			• 構築中のAサービスのテスト用に、誤ってファイアウォールをオープン（これ以降、外部よりログイン試行が開始されていた模様）
検知の1日前	• 後日調査により、外部からの辞書攻撃により管理者アカウントで侵入を受けていたことが判明		
1日目　12:00			• 委託先よりサーバのメモリ異常の報告を受領 • 委託先より、UTMに内部から外部に向けた大量の通信が発生しているとの連絡を受け、サイバー攻撃の可能性を含め対策検討開始 • 委託先に、UTMの通信を強制遮断するよう依頼
1日目　16:00	• インシデントについてCISOが報告を受領	• PSIRTと事業部門による対策会議を開催 • 暫定対策を策定（対象環境の保管、管理者パスワード変更、保守用ネットワークの切り離し、監視強化等）	• Aサービスの管理者パスワードが変更されていることを確認、Bサービス、Cサービスのログが消されている事を確認 • 左記暫定対策の実施
2日目			• 自社およびフォレンジックベンダーによるネットワークフォレンジックを実施
3日目			• Bサービス環境をクローンから復元
4日目			• フォレンジックベンダーへ端末フォレンジックを依頼 • Aサービス環境をクローンから復元
2週目	• 経営連絡会において本インシデントを速報し、他サーバで同様の設定がないか確認を事業部門へ指示		• 接続元IPアドレスを日本に限定する設定を適用
3週目			• フォレンジック結果を受領 • Cサービスの顧客に対し、解析結果、是正報告書を提出
	• 所管官庁へ報告		
		• 品質管理委員会で本インシデント及び注意喚起	• 暫定的な監視強化のため、通信状況解析ツールを設置
4週目以降			• Aサービスの顧客へ本事案を報告 • Cサービスの顧客にサービス復旧計画を説明。Cサービス復旧 • 顧客とのSLAの調整を開始
			• Bサービスの顧客に本事案を報告。Bサービス復旧
	• 社内の安全宣言に向けた対策（暫定対策）についてCISOが承認	• 製品セキュリティ委員会において、経営連絡会で依頼した確認事項を調査し、対応・報告するよう事業部へ依頼	

4．まとめ

背景・国内外の状況

- 辞書攻撃による管理者アカウントの奪取は、古くから行われている攻撃手法である。
- 被害のあったサーバに仮想通貨マイニングツールが埋め込まれていたことから、サーバのリソースを利用して不正に仮想通貨をマイニングさせることを目的としていると考えられる。

発生と検知、エスカレーションと役割分担、対応

- 「２.状況」、「３.時系列」を参照

サイバー攻撃による影響

- Aサービス、Bサービス、Cサービスへの管理者アカウントでの不正ログイン、セキュリティログの消去、仮想通貨マイニングツール及びプロセス隠蔽ツールの埋め込みが行われた。また、AサービスのWebサーバに対してはインターネット上のランダムなIPに対し、ポートスキャン、ブルートフォースを行う不正プログラムを埋め込まれた。
- 被害範囲の特定や暫定対応に4ヵ月程度を要した。

発生原因と根本原因の深堀り

- **リスク評価が十分ではない中で、ファイアウォールをオープン**したことで攻撃を受ける。
  - ファイアウォールをオープンする確認手続きとリスク分析が十分ではなかった。
  - 様々なサービスが同じIaaS上で稼働する環境であるが、ファイアウォールをオープンする計画を、各サービスを所管する関係者間で共有できていなかった。
- 複数サービスで、**保守用ネットワークを分離せずに共用していた。**
- 複数サービスで、**管理者パスワードに辞書攻撃で想定し得るもの**を使いまわしていた。
  - 対象プロジェクトで製品開発および運用に関するセキュリティ規定等が十分に整備されていなかった。

被害軽減に寄与した対策

- **メモリ監視を実施**していた。AサービスのWebサーバから外部へ大量の通信が開始されたことでメモリ異常が発生し、運用保守員がメモリ監視を通じて異常を検知し、本事象が発覚し対処した。結果として、攻撃者が利用を試みたAサービスを踏み台にしたインターネット公開サーバへの攻撃通信を遮断することができた。

4．まとめ

得られた気付き・教訓

- インシデント対応手順、連絡先の整備が不十分であり、事後に整備した。
  - ▶ PSIRTで対応マニュアルを改定し、開発プロジェクトにおけるインシデント対応体制、フォレンジックベンダー等の外部委託先を含む連絡フローをあらかじめ整備した。
- **製品セキュリティの責任分界点が不明確であったため、セキュリティに関するSLAの調整に着手**した。
  - ▶ 製品セキュリティについて、契約範囲を明確化しない中で、顧客から対応を求められるケースがある。顧客との責任分界点を明確にするため、**対処すべき範囲、必要な費用を請求するといったSLAの整理**と調整に着手している。
  - ▶ **委託先ともインシデント時の依頼範囲や対応費用等を契約において明確化**することに着手した。
- 事業部においてインシデント対応費用を社内処理する手続き等で時間を要したことから、**PSIRT部門で費用の振替が行える**といった体制整備を検討している。
- ログ保管期間が短くローテーションで消えており、サイバー攻撃を検知する仕組みが十分ではなく、対処した。
  - ▶ 長期間ログが保管できるように**ログ保管サーバ**を整備した。

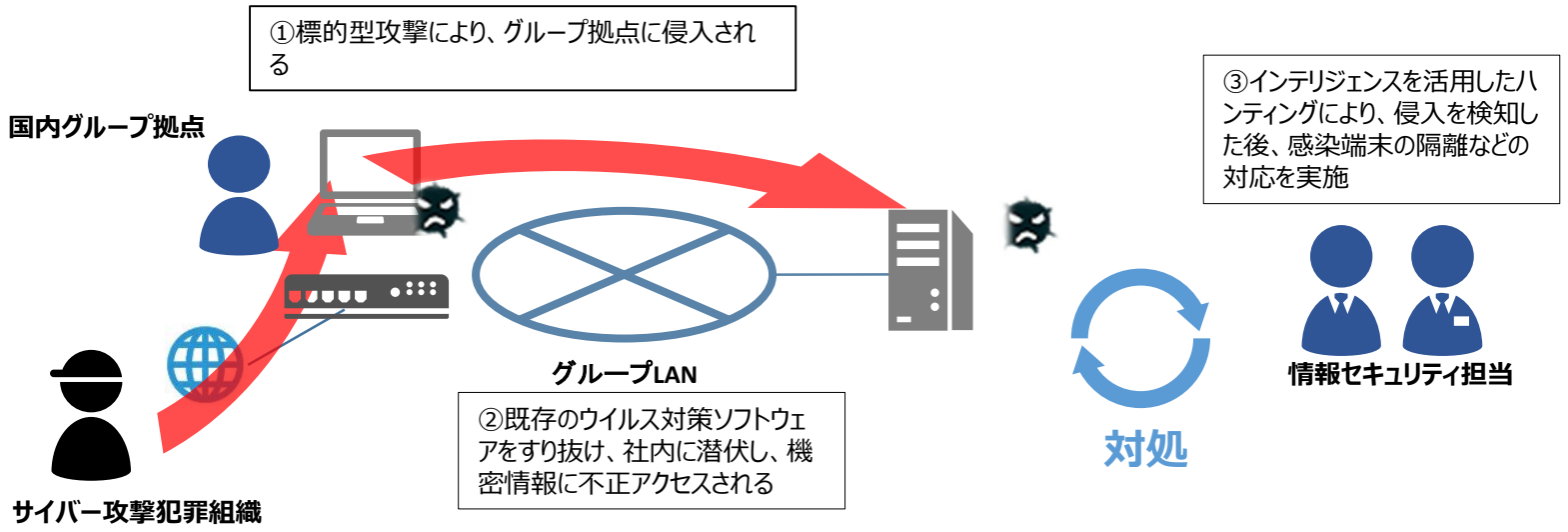
今後の課題

- 全てのプロジェクトにおいて、CSIRTとPSIRTが定めるセキュリティ対策を漏れなく実施することを目標としている。また、出荷後に極力インシデントが発生しないように**開発時から脆弱性を意識した作りこみ**をする等、セキュリティを考慮した製品ライフサイクルを構築することを目標としている。
- 資産管理の方法は社内で定義できていないため、フォーマットを定め、状況を把握できるようにする必要がある。

1．概要

- 本事例のF社は、ITソリューション企業である。
- 国内グループ拠点に標的型攻撃を受け社内へ侵入された。高度標的型攻撃であったため、既存のウイルス対策ソフトウェアでは検知できず、社内深くに侵入された。
- その後、インテリジェンスに基づくハンティングを実施していたことから、侵入を検出することができ、侵害範囲の調査、侵害端末の隔離等のインシデント対応を実施することができた。
- 高度な攻撃への対応能力を高めるため、重要度に応じた情報の管理・防御態勢の整備、サプライチェーンの管理、EDRの導入等を進めている。

2．状況



３．時系列（組織毎の検知・分析・対処）

日時（※）	①経営・広報	②CISO・CSIRT・危機管理	③事業部門
			• 外部より不正アクセスを受け、侵入を開始
		• 社内PCより不正通信の発生を検出し、調査を開始 • 感染PCの隔離・調査、不正通信先の検知・遮断を実施	
	• 当該ファイルに関連する顧客へ個別に状況説明	• 社内サーバに保存されたファイルに対して不正アクセスが行われていたことを確認	
	• 不正アクセス被害を発表		

※日時はマスクしています。

4．まとめ

背景・国内外の状況

- 本攻撃には、定義型のウイルス対策ソフトウェアでは検出できない、本組織向けにカスタマイズされたツールが使用されていた。そのため、ウイルス対策ソフトウェアを基盤とした、初動、不正通信検知および感染拡大防止の仕組みが機能しなかった。

発生と検知、エスカレーションと役割分担、対応

- 「２.状況」、「３.時系列」を参照

サイバー攻撃による影響

- 社内サーバへの不正アクセスが行われていた。

発生原因と根本原因の深堀り

- 本組織向けにカスタマイズされた高度標的型攻撃を受けた。
  - ▶ 日々進化するサイバー攻撃に合わせて、被害軽減対策や検知技術をアップデートする必要がある。
- 不正アクセスされた機密情報は、攻撃を受けたファイルサーバでの**保管を禁止していたが守られなかった**。
  - ▶ セキュリティ対策の周知不足や、ファイルサーバの特権管理漏れ等のセキュリティ策が不十分な箇所や部門が狙われており、組織やサーバ等のセキュリティ対策の範囲に**漏れがないよう取り組む**必要がある。

被害軽減に寄与した対策

- 侵入当初からしばらくの間は、侵入及び被害状況を把握することができなかった。ただし、当時から**統合ログ管理ツールを導入し、ログ解析の環境を整備**していたことから、不正通信の調査、フォレンジックを実施することができた。
- 更に、ログ解析時の侵入痕跡についても、当時から**ハンティング**していたことから、侵入検出につながった。ハンティングに取り組んでいなければ、発見が遅れる、もしくは侵入が明らかにならなかったと考えられる。

また、**同じ侵入を受けた組織が、その痕跡情報を公開していた**ことが寄与した。自社でも、サイバー攻撃への取り組みに関する他の組織からの講演依頼を受け、情報の共有に努めている。

4．まとめ

得られた気付き・教訓

- 攻撃動向に合わせて、システムを随時改良する必要がある。
  - グループ全体で**EDR, NDRの導入**、リモートアクセス認証の導入、ファイルサーバの監視強化、特権管理、最重要情報の独立ネットワークへの保存等を実施した。
  - **社内および顧客向けシステムの構成情報をあらかじめ登録し、公開された脆弱性情報に対するリスクを自動的に通知**する仕組みを整備した。
- 現場業務を意識したセキュリティ対策を導入する必要があり、対策した。
  - 多要素認証を経て、暗号保護した状態のまま編集できるファイルサーバを導入した。
  - **事業部門や経営層がセキュリティ情報を簡易に閲覧するためのダッシュボード**を整備した。
  - 迅速なインシデント報告のため、Web報告フォームを整備した。
- 情報管理の手続きを強化した。
  - 事業部単位で情報の重要度を判断できるように、組織としての情報の管理基準・考え方を策定し、**優先して保護すべき情報を決定**した上で、重要度に応じたセキュリティ対策を導入した。
  - 重要なシステムを識別し、バックアップとBCPに重点を置いた机上演習を実施した。
  - 情報の重要度を踏まえた上で、**社内認定済クラウドへの社内システムの移行**を進めている。
- 非セキュリティ部門との連携を進める必要がある。
  - セキュリティ対策として法務部門の規定を変更する際に、セキュリティ教育に法務コンテンツを含めるなど、**法務、調達部門など管理部門との連係**を進めている。
  - 取引先が自ら対策状況を点検し、点検結果をWebシステムに入力するようにシステムを整備した。**「理解度テスト」を配布**し、社内教育と自社の位置付け把握に活用してもらった。

今後の課題

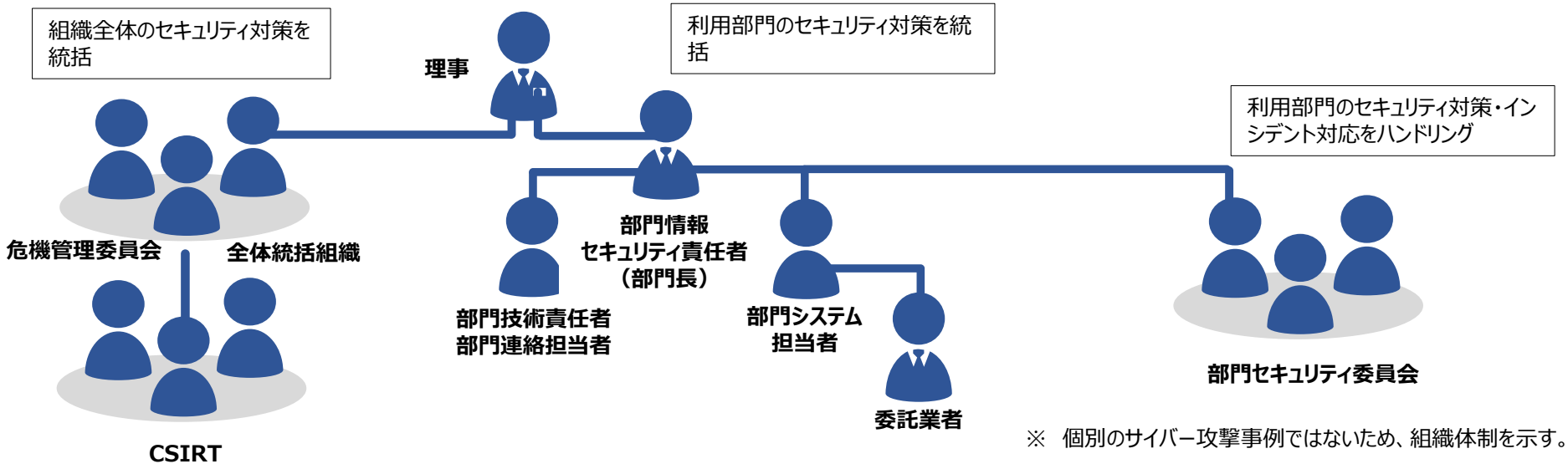
- 顧客や株主など関係者への説明責任を果たすこと、観察した高度な攻撃にも対応できるレベルを目指したセキュリティ対策の実施を目標としている。
  - **第三者による定量評価**を尺度としてセキュリティ対策を実施することで、経営層へのアピールも容易になるが、**適切な指標の設定が課題**である。
  - 第三者が定めた指標だけではなく、**自らKPIを定めて**取組みを進める必要がある。
  - **指標だけに依存することなく、攻撃者の攻撃レベルをウオッチして、必要な取り組みを選定**して実施する必要がある。
- 所管するシステムの**構成とその脆弱性を網羅的に把握**する必要がある。
  - 新規システム導入時の業務プロセスに、脆弱性情報通知システムへの構成情報の登録手続きを含めているが、未登録の稼働済システムは、個別に人海戦術で登録しなければならない。
  - **取引先から調達するシステム・ソフトウェアの構成要素（SBOM）を管理**する必要がある。
- 限られた予算内でセキュリティのパフォーマンスを向上させるため、インシデント発生時の本社、関係会社、調達先の影響を迅速に把握することが課題である。
  - 技術や手続き等の**セキュリティ対策状況を一覧・マップ化**することで、インシデントが発生した組織と自組織の影響を迅速に判断することを検討している。
- **限られた予算内でセキュリティのパフォーマンスを維持するため、先進的な技術の導入とともに、維持コストを抑えるための合理化**が課題である。

1．概要

- 本事例のG機関は、数万人規模の学術研究機関である。
- 当該機関では、端末のランサムウェア感染、使いまわしパスワードを要因とする不正アクセスなど、様々なインシデントに対処している。
- 発生する様々なインシデントへの対処を通じて、VLANによるネットワーク分割、全体統括組織によるICT管理を通じた利用者部門のICT管理運用コストの低減、組織全体のセキュリティ教育等の技術的および組織運用的なサイバー攻撃対策を整備している。

ここでは、個別のサイバー攻撃事例ではなく、学術研究機関における対応体制の整備状況全般について整理した。

2．状況



※　個別のサイバー攻撃事例ではないため、組織体制を示す。

３．時系列（組織毎の検知･分析･対処）

日時	①経営･広報	②CISO･CSIRT･危機管理	③事業部門
個別のサイバー攻撃事例ではないため、省略。			

４．まとめ

背景・国内外の状況

- G機関は、数万人規模の学術研究機関である。
- 多数の職員、研究者、学生を抱えており、セキュリティ対策を各部門が担う体制をとっている。

発生と検知、エスカレーションと役割分担、対応

- 「２.状況」、「３.時系列」を参照

サイバー攻撃による影響

- ランサムウェアに関しては、大規模な被害は発生しておらず、影響が学生の端末に限定される感染事例が発生している。
- より影響が大きなケースとして、SNSから漏洩した使い回しのパスワードにより、不正侵入される事例も発生している。

発生原因と根本原因の深堀り

- ランサムウェア感染および不正侵入に関しては、パスワードの開示や不審メールの開封など利用者の不適切な運用が影響している。

被害軽減に寄与した対策

- 研究機関内のネットワークは、**VLANで非常に細かく分割**し、VLAN間の通信を遮断するよう制御していることから、ランサムウェア等に感染したとしても、特定のVLAN内に感染の影響が留まるよう設計している。
- 無線LAN接続された端末間の通信を遮断することで、無線LANを経由した感染を抑えるよう設計している。
- 研究機関内のシステムは、Active Directoryに偏っておらず多様なシステムから構成しており、Active Directory経由の感染リスクはある程度低減される。

４．まとめ

得られた気付き・教訓

- 情報資産とIT資産を管理する必要がある。
  - 情報資産の位置付け及び重要性は、**オーナーが判断**できるとの方針のもと、統括組織が規定を設け、重要度判定を支援している。
  - 研究者が、独自にネットワークや機器を導入するケースに対応するためのセキュリティ対策基準を定め、導入には手続きの順守を必要とするように制御している。
- 技術的対策が必要である。
  - 多要素認証を導入するとともに、**クラウドサービスを積極的に活用**している。
  - 不審メール対策として、通報窓口を整備するとともに、サンドボックスを活用し安全性を確認している。
  - メール・ファイルサーバ等の基本的なITサービスを統括組織が組織全体に提供することで、各部門が独自運用する必要がなく、個別サービスを手放すように誘導している。
  - 脆弱性診断サービスを各部門に提供し、各部門がチェックするようにしている。
- 情報セキュリティ意識の向上が必要である。
  - 標的型メール攻撃対策として、メール訓練、ウイルス感染の疑似体験型訓練、情報セキュリティのeラーニング講習を実施している。
  - 組織全体委員会、技術担当者レベルの連絡会などの会議や教員向け、事務担当向け等の講習会を開催している。
  - 名刺入れ等に入れて持ち歩くことができる**要約版ガイド**を作成し、全員に配布している。

今後の課題

- 何か起こらないとセキュリティ対策の必要性が認識されず、**費用対効果の説明が難しい**。予算削減の流れの中で、単年度予算だけでなく、**継続的活動の予算確保が課題**である。
- 組織や研究の独立性とセキュリティ役割のバランスが課題である。
  - 研究の独立性等の観点から、**エンドポイントを含めてどこまで統一的にITサービスを提供管理すべきか**議論と方針策定が必要である。組織での統一的対策を優先すると、先進的ICT技術の採用を止めてしまう懸念があり、一方で先進技術の利用を優先すると、その利用範囲やセキュリティ対策とのトレードオフなどを整理・合意する必要がある。
  - 人事権限は部門にあり、統括組織からセキュリティ対策の徹底を指示することは、構造的に難しい。一方、部門においても、研究責任者が各々研究領域と人員を抱える中で、**部門としてセキュリティ対策を1つに定めること、同意の確保が難しい**。
  - 部門がインシデント対応を担うが、スキルに懸念のある部門では適切に実施できていない可能性があり、**組織全体としての状況把握**が課題である。
  - 部門がIT資産を管理しており、組織全体としての管理状況の把握が課題である。
- クラウド化が進む中で、利用状況の把握とリスク管理が課題である。

研究データについても、重要度の基準を含む管理手続きを制定する必要がある。

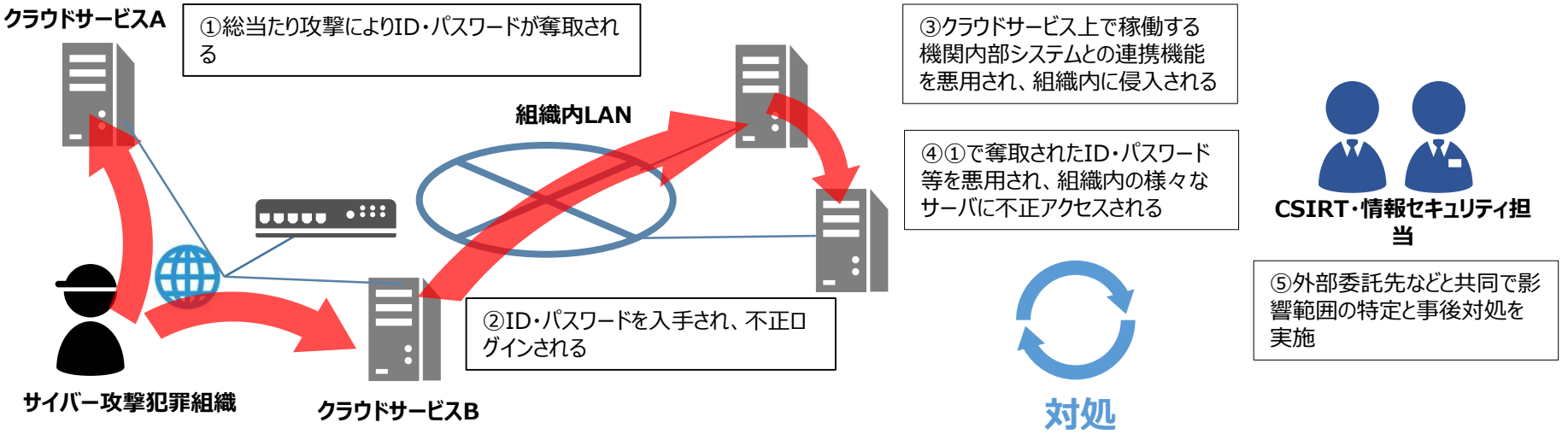
- セキュリティを考慮した人員のローテーションや配属ができていないケースもあり、ノウハウ蓄積が難しい。また、外部からセキュリティに興味のある人材の応募があればよいが、採用条件のよい企業に流れてしまう。**セキュリティ専門人材の育成が課題**である。

産業スパイを想定した対策をどの程度実施すべきか判断が難しい。

1．概要

- 本事例のH機関は、数万人規模の学術研究機関である。
- 利用しているクラウドサービス（A）に、パスワード総当たり攻撃により、不正にアクセスされた。
- 一方、機関内部システムと連携するクラウドサービス（B）に不正にログインされた後、連携機能を悪用され、内部システムへの侵入を許した。機関内部システムでは、クラウドサービス（A）と同じID・パスワードを利用している利用者がおり、侵入された機関内部システムを踏み台に、その他の内部システムに不正アクセスされ、未公表の研究情報、職員の個人情報などが外部へ漏えい又は外部から閲覧された可能性がある。
- 再発防止のため、認証システムの高度化、組織内ネットワークの再構成、運用手続きの見直しなど、管理・防御態勢の整備を進めた。

2．状況



3．時系列（組織毎の検知・分析・対処）

日時	①経営・広報	②CISO・CSIRT・情報セキュリティ対策本部	③事業部門
1か月以上前			• クラウドサービスAにて、100名のアカウントへ不正ログイン
			• クラウドサービスBと内部サーバとの連携機能を悪用され、内部サーバへ侵入
			• 内部サーバを踏み台に、クラウドサービスAの不正ログインに使用された ID・パスワードを流用し、更に内部システムに不正ログインされる。内部サーバに保管されていた他の内部システムのパスワードが窃取され、他のシステムへと侵入
1日目		• CSIRT から理事長、CISO及び幹部へ連絡 • 所管官庁、外部委託業者、外部機関（JPCERT/CC等）へ連絡	• 情報システム担当者が、自身のサービス利用履歴に不審な点を発見し、不正アクセスを受けたアカウントを発見 • 不正ログインされたアカウントのパスワードを強制変更 • 内部ネットワーク以外からのクラウドサービスAのアクセスを遮断
2日目		• 情報セキュリティ対策本部を設置し、対策会議を開催	
3日目	• 外部機関（NISC、警察等）と連携		• 調査により、内部システムへの不正なアクセスを確認 • 全職員の内部システム用パスワードを強制変更 • 内部システムおよび、クラウドサービスAの機能を停止 • 被害の範囲、侵入経路等について分析を開始
6日目	• Webサイトにて本事案を公表		• 被害の拡大防止のため、外部へのインターネット接続を遮断
2週目			• 外部接続している研究部門のサーバに、内部システムへの不正なアクセスの足掛かりと思われる不正な通信記録確認 • クラウドサービスAの更なる不正ログインと情報漏洩を確認
1か月目			• ファイアウォールの監視強化のため、別ベンダーによる監視を追加 • インターネット接続を日中のみ再開 • 主要な内部システムを再開
2か月目	• 警察に被害届を提出		

４．まとめ

背景・国内外の状況

- アカウント奪取に用いられた総当たり攻撃は、古くから行われている攻撃手法である。
- 匿名通信が駆使されており、侵入者がどの国又は地域から攻撃を行っていたか、どのような目的を持っていたかは明らかになっていない。

発生と検知、エスカレーションと役割分担、対応

- 「２.状況」、「３.時系列」を参照

サイバー攻撃による影響

- 未公表の研究情報、個人情報等が奪取された。
- インターネットが利用できなくなったことから、経理等を含む業務が停止した。
- インターネットやシステムの停止判断と各部門との調整に時間を要したことが、被害拡大につながった。

発生原因と根本原因の深堀り

- **情報等の重要度に応じて内部ネットワークが分離されておらず**、一旦侵入を受けると、広範囲に不正アクセスが可能であった。
- **なりすましが容易な認証システム**であった。
  - クラウドサービスに多要素認証が適用されていなかった
  - パスワードの運用規則を制定していたが、形骸化していた。
  - パスワード強度診断ツールを導入していたが、全員に適用されていなかった上、強度も十分ではなかった。
- インターネットと内部システムの停止を決定する体制・手続き整備が不足していたため、部門との調整および判断に時間を要し、被害の拡大につながった。
- 委託先が実施するセキュリティ監視において、**アラートとする閾値が誤って設定**され、事態の把握が出来なかった。また、本研究機関としても監視状況に問題ないと判断しており、**委託先管理が十分ではなかった**。
- クラウドサービスと内部サーバを連携する機能のリスク認識が十分ではなかった。

被害軽減に寄与した対策

- 情報セキュリティ規程や研修を通じて、セキュリティ対策を周知しており、**パスワード管理等の適切な対策**がなされていたシステムは、**内部ネットワークへの侵入後の不正アクセスの影響を受けなかった**。

4．まとめ

得られた気付き・教訓

- インシデント発生時に迅速にシステム停止等を判断できるようにした。
  - ▶ **インシデント対応計画として、BCP的な検討を追加**し、業務が立ち行かなくなった状況を含めて、エスカレーションのタイミング・対象者、意思決定者等をルール化し、迅速な意思決定を行えるようにした。
- 一度内部に侵入を許すと、拡散を防止できなかったため、**情報の重要度等に応じたネットワーク分離**を行った。
  - ▶ 職員の属性に応じて、利用できるネットワークを限定するようにシステムを改修した。
- 機関内のIT資産の把握が必要であり、対策を進めた。
  - ▶ **資産管理システムを導入**し、資産管理状況を把握し、IT機器の機能制御を行うようにした。
- 利用者への丁寧な説明が必要である。
  - ▶ **なぜ対策するのかを伝えなければ、対策を取ったことで不便になったという不満ばかりが募る。**過去のインシデントの原因、必要な対策を取らないとインシデントが再発することをeラーニングで伝える、意見交換会で対策の必要性をあらためて伝えている。対策の必要性をシステム利用者へ丁寧に説明し、地道に理解してもらうことが必要である。
  - ▶ 職員に情報をわかりやすく提示するために、**組織内の情報サイトの再構築や掲示板構成の見直し**、外国籍研究員のための和英併記等を実施した。
- 委託先の適切な管理が必要であり、対策した。
  - ▶ 適切なスキルを有する委託先が選定できるよう、要求仕様書と選定基準を見直し、**委託先との定期会議**を設けて改善要望を提示すると共に、定期的に運用実態を実地監査・レビューしている。

今後の課題

- Windows以外の機器や、センサー系の機器などの管理に取り組む必要がある。
- 情報の重要度などから、特に守るべきもの、そうでないものは利便性を優先するなどのメリハリのある対策が必要と認識している。
  - ▶ **経営層、セキュリティ所管部署、データを保持する研究部門と、保護資産の重要度、利便性、優先度とセキュリティ対策の関係を合意**して、対策を考えていく必要がある。また、ルールを整備するとともに、現場が適切に情報の重要度を評価できるツールが必要と考えている。
  - ▶ **いきなり全資産を分別するのではなく、特に守るべき情報をピックアップ**し、アクセス制御、ネットワーク分離や監視強化などを行い、守るという考え方を検討している。
- セキュリティ専門家が各部門に数名張り付き、部門のセキュリティ管理状況をチェックする、意図を伝えるのが望ましいが、**人材確保が課題**となっている。
- セキュリティと利便性はトレードオフの関係になりがちなので、経営層と現場がコミュニケーションを密にしてセキュリティ対策に関する理解を共有し、セキュリティと利便性のバランスの取れたセキュリティ対策を実施することが重要。
- NDR等の検出対象として、日常的な研究活動のふるまいと異なるものを検知するとなると、**費用・人手がかかる**ことが懸念される。

付録

- 本書で使用した用語を紹介します。

用語集

用語	意味
インシデント	サイバー攻撃により発生した、セキュリティに影響を及ぼす事故のこと
オンプレミス	ネットワーク機器、サーバ、ソフトウェアなどのITシステムを、自組織の施設構内に設置して運用する利用形態のこと。
サイバー攻撃	悪意を持った攻撃者が、コンピュータシステムに不正侵入し、不正なプログラムの実行、情報の奪取、破壊等を行うこと
脆弱性診断	システムやネットワーク上の脆弱性などのセキュリティリスクを診断すること
セキュリティパッチ	プログラムのセキュリティ上の弱点や欠陥を部分的に修正する追加プログラムのこと
ダークウェブ	匿名性が高く、特別な閲覧ソフトウェアでアクセスできる特別なサイトのこと
ハンティング	セキュリティ情報、ネットワーク機器のログ等を活用及び分析して、自組織の潜在的な脅威や侵害を洗い出す活動のこと
標的型攻撃	特定の組織を狙ったサイバー攻撃のこと　ばらまき型のメール攻撃等と異なり、特定組織に対して攻撃を繰り返す特徴がある
フォレンジック	不正アクセスや情報漏えい等の原因究明や捜査に必要なデータ等を収集および分析する方法のこと
マルウェア	不正かつ有害に動作させる意図で作成されたソフトウェアの総称のこと　ランサムウェアやワームなどが含まれる
ランサムウェア	感染したコンピュータに保存されているデータを使用出来ないように暗号化し、元に戻す対価として身代金を要求するプログラムのこと

用語集

用語	意味
ログ	コンピュータの利用状況や通信等の記録のこと
ワーム	マルウェアの一種で、自身を複製して他のシステムに拡散させるプログラムのこと
BCP （Businees Continuity Planning）	緊急事態に遭遇した際に、中核業務を早期復旧あるいは継続するための計画のこと
CISO （Chief Information Security Officer）	最高情報セキュリティ責任者と呼ばれ、組織が実施するセキュリティ対策を統括する責任者のこと
CSIRT （Computer Security Incident Response Team）	インシデント発生に対応する組織のこと
EDR （Endpoint Detection and Response）	パソコンやサーバ上のファイル操作等を記録、分析し、インシデント対応を支援する製品のこと
IaaS （Infrastructure as a Service）	情報システムを稼働するために必要なネットワーク、ストレージなどの基盤を、インターネットを介してサービスとして提供すること
IDS （Intrusion Detection System）	ネットワークや端末上の不正な動作を検知し、管理者に知らせる製品のこと
IoC （Indicator of Compromise）	サイバー攻撃などの侵害痕跡や指標のこと
IoT （Internet of Things）	センサー機器などの「モノ」をインターネットに接続する仕組みのこと
JPCERT/CC	日本国内におけるインシデントの報告受付、対応の支援等を行う中立組織のこと
MSS （Managed Security Service）	セキュリティ監視などの運用を請け負うサービスのこと

用語集

用語	意味
OSS （Open Source Software）	ソースコードが公開され、改変等が認められているソフトウェアのこと
PSIRT （Product Security Incident Response Team）	自社で開発する製品およびサービスのセキュリティ向上やインシデントに取り組む組織のこと
SLA （Service Level Agreement）	サービスを提供する事業者とサービス利用者間で、サービスの範囲、内容、達成目標等について合意した内容のこと
SOC （Security Operation Center）	ネットワーク機器やサーバのログ等を監視し、サイバー攻撃やその予兆を検知、分析する組織のこと
UTM （Unified Threat Management）	ウイルス対策等の複数のセキュリティ機能を統合し、セキュリティ上の脅威を管理する機器のこと