

セキュリティインシデント対応机上演習 実施マニュアル

目次

1. はじめに	- 1 -
2. 利用規約	- 2 -
3. 机上演習（TTX）について	- 3 -
3-1. 机上演習（TTX）とは	- 3 -
3-2. TTX の目的と対象者	- 3 -
4. 机上演習（TTX）の実施プロセス	- 5 -
5. 事前準備	- 6 -
5-1. 演習計画の策定	- 6 -
5-2. 演習開催準備	- 6 -
6. 演習実施	- 11 -
6-1. 座学	- 11 -
6-2. 演習	- 11 -
6-3. 質疑応答・各種案内・クロージング	- 12 -
7. 事後作業	- 13 -
7-1. アンケート	- 13 -
7-2. 社内報告	- 13 -
7-3. ルール等への反映	- 13 -
8. 一般企業向けランサムウェア感染シナリオの解説とカスタマイズ方針	- 14 -
8-1. 事例企業の概要	- 14 -
8-2. ディスカッションポイント	- 16 -
9. 医療機関向けランサムウェア感染シナリオの解説とカスタマイズ方針	- 22 -
9-1. 事例医療機関の概要	- 22 -
9-2. ディスカッションポイント	- 24 -

1. はじめに

近年、大企業のみならず中小企業においてもサイバー攻撃の脅威にさらされている状況である。組織においてセキュリティインシデントが発生した場合には、被害とその影響範囲を最小限に抑えて事業継続を確保する必要がある。その為には、予めの対応体制と手順を整備したうえで、実際にセキュリティインシデントが発生した場合を想定して演習しておくことが重要であると考えられる。

こうした背景を踏まえ、IPA は中小企業を対象としたセキュリティインシデント対応机上演習の開催およびその支援を行っているが、より多くの組織に机上演習を実施いただけるようにするため、演習教材と演習実施のためのマニュアルを公開することとした。

セキュリティインシデント対応机上演習実施マニュアル（以降、「本マニュアル」という。）は、セキュリティインシデントが発生した際の、初動対応から再発防止策の検討を行うまでのシミュレーションを行う「机上演習」を、IPA が公開する演習教材を利用し実施する上で必要な手順等を記載したマニュアルである。

演習教材および本マニュアルを活用することで、自組織内において机上演習を開催することが可能となる。また、必要に応じてシナリオをカスタマイズすることによって、より自組織の環境に即した内容の机上演習を行うこともできる。

演習実施により、組織のセキュリティ意識の向上とインシデント対応能力向上に貢献することができれば幸いである。

2. 利用規約

■免責事項

本マニュアル及び演習教材の利用に起因または関連して利用者に生じたトラブルや損失、損害等に対し、IPA は一切の責任を負いません。

■注意事項

本マニュアル及び演習教材に登場する組織名は架空のものであり、実際の団体等とは関係ありません。

■利用条件・範囲

本マニュアル及び演習教材は、個人、法人組織における非営利目的でのみ、かつ健全な社会通念に反しないことを条件として、本書面の定めに従って事前連絡せずに無償で使用できるものとします。演習教材については、上記利用条件の範囲において、シナリオのカスタマイズ等の改変を行うことも可能とします。

3. 机上演習（TTX）について

3-1. 机上演習（TTX）とは

TTX は、Table Top Exercise の略で、机上演習のことを指す。主にサイバーセキュリティや危機管理、事業継続計画等にかかるインシデント対応演習で用いられる手法¹である。

演習は、参加者がテーブルに集まり、特定のシナリオに基づいてディスカッションを行い、問題解決や意思決定のプロセスをシミュレーションする。この形式は、コンピューターの操作やログの分析といった技術的なアクションではなく、参加者がインシデント対応に関する計画や戦略の検討、意思決定を体験することに重点を置いているといえる。

セキュリティインシデント対応机上演習の場合、あらかじめ決定されたシナリオをベースに、イベントが発生した際にとる行動（初動対応等）についてグループディスカッションを行う形式で進行する。



図 3-1 TTX の流れ

3-2. 机上演習（TTX）の目的と対象者

TTX は技術的なスキル向上を目的としたものではなく、意思決定のプロセスを体験することを通じ、以下のような目的を達成するために行うものである。

① 理解の促進

サイバー攻撃やリスクに対する組織の対応能力を向上させるため、参加者が自らの役割や責任を理解する。

② コミュニケーションの強化

¹ 本マニュアルにおいては、セキュリティインシデント対応の机上演習のことを TTX と表記している

関係者間の情報共有やコミュニケーションを促進し、チームワークを強化する。

③ 戦略の検証

既存のインシデント対応計画や戦略が効果的であるかを検証し、改善点を見つける。

したがって、TTXは、実際にインシデント発生時の意思決定を行う、組織の経営層を主な対象者と想定しており、**経営層が演習に参加することを強く推奨する**。その上で、組織の管理者、システムやセキュリティの担当者、事業担当者等の情報セキュリティ責任者をサポートする組織の担当者を参加させることにより、インシデント対応に関する組織全体の理解の促進や、チームワークの強化等につなげることが可能となる。

また、多様な気づきを得るために、なるべく複数のグループでディスカッションを行い、互いに結果を共有することを勧める。

4. 机上演習（TTX）の実施プロセス

TTX の効果を最大化するためには、以下のような実施プロセスを基に、計画的に実施することを勧める。

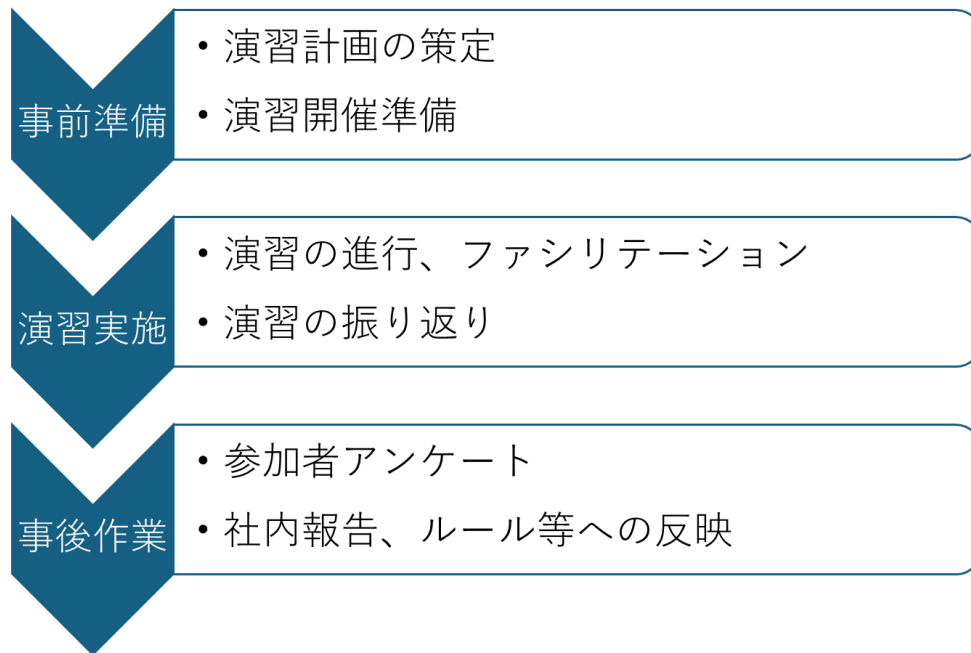


図 3-2 TTX の実施プロセス

① 事前準備

演習の目的を達成できるようにするため、演習計画を策定し、必要な人員、会場、資材の確保等といった演習開催に必要な準備を行う。

② 演習実施

演習における座学部分の解説や、グループディスカッションが円滑に行われるようファシリテーションを行う。

③ 事後作業

参加者へのアンケートや社内報告を実施し、社内ルール等の改善を行うことで組織のインシデント対応能力を向上させる。

各プロセスで実施すべき事項の詳細を、次章以降にて説明する。

5. 事前準備

本章では、TTX 実施にあたり準備すべき事柄について説明する。

5-1. 演習計画の策定

最初に、演習の目的や想定参加者、実施時期等を検討し、演習計画を策定する。

- 演習の目的
 - 3章で記載した内容を参考に、本演習により達成したい目的を設定する。
- 想定参加者
 - 意思決定を行う経営層をはじめ、システムやセキュリティの担当者、インシデントにより影響を受ける事業の担当者等の情報セキュリティ責任者をサポートする組織の担当者から選定する。
 - 1グループあたり4～6名で構成し、なるべく複数のグループを作るようにする。（経営層に加えてシステム関係の実務者が参加する場合、各グループに均等に入るように調整する。）
※チーム分けを主催者事務局に一任する場合、上記を依頼する。
 - 演習を行う講師のほか、必要に応じグループディスカッションのファシリテーションの補助を行う要員や、会場準備等の運営を行う要員を確保する。
- 実施時期
 - 演習の所要時間は3時間程度となるため、想定する参加者（経営層等）が確実に参加できるよう、余裕を持った日時設定を行う。

開催にあたり、参加者のスケジュール調整や部材の確保等が必要となるため、演習の目的等を関係者に説明し、必要な承認を得た上で準備を進める。

5-2. 演習開催準備

(1) 演習シナリオ

2025年4月時点では、以下のシナリオが利用可能である。組織において発生しうるシナリオに近いものを選定し、これをベースとし必要に応じてカスタマイズを行う（シナリオの詳細やカスタマイズについては後述）。

- ① 一般企業においてランサムウェア感染を想定したシナリオ
- ② 医療機関においてランサムウェア感染を想定したシナリオ

(2) タイムスケジュール

本 TTX の標準的なスケジュールを以下の図に示す。所用時間は 3 時間を想定している。

時間	内容
0:00～0:05(5分)	オープニング（主催者挨拶、講師紹介、目的説明等）
0:05～0:25(20分)	講習（座学） 「中小企業のためのセキュリティインシデント対応の手引き」をベースにインシデント対応のポイントを学ぶ。
0:25～1:25(60分) ※説明、発表時間を含む	演習 1 発生した事案の初動対応について、グループディスカッションにより対応方針等を検討する。
1:25～1:35(10分)	(休憩)
1:35～2:35(60分) ※説明、発表時間を含む	演習 2 業務・システムの復旧や再発防止、公表等について、グループディスカッションにより対応方針等を検討する。
2:35～2:50(15分)	振り返り
2:50～3:00(10分)	質疑応答・各種案内・クロージング

図 5-2 TTX のタイムスケジュール例

各セクションにおける実施内容と時間配分の例を以下に示す。あくまで一例であり、実施内容や所用時間をカスタマイズすることは可能であるが、気づきを得るために最も重要となる、グループディスカッションにかかる時間の短縮は推奨しない。

- オープニング（5 分）
 - 主催者による挨拶
 - 講師の紹介
 - 演習の目的やルール、期待される成果等の説明
- 講習（座学）（20 分）
 - 「中小企業のためのセキュリティインシデント対応の手引き」をもとに、インシデント発生時の対応を 3 ステップに分けて説明
- 演習 1（60 分）
 - 演習の進め方や前提条件、インシデントの発生状況、検討課題を説明（10 分）
 - グループディスカッションの実施（30 分）
 - グループ内で簡単に自己紹介を行い、役割分担（リーダー、記録係）を行う。
 - 演習課題に沿って対応策を検討し、グループ内の意見をまとめる。

- ディスカッション内容の発表（15 分）
 - 複数のグループがある場合は、それぞれ発表してもらう（2 グループを目安）。
- 回答例と講評（5 分）
- 休憩（10 分）
- 演習 2（60 分）
 - インシデントの状況や検討課題を説明（10 分）
 - 演習 1 で検討した対応策はグループにより異なるため、講師の説明により対応内容等の状況を揃える。
 - グループディスカッションの実施（30 分）
 - 多くの参加者がディスカッションに参加できるよう、グループ内の役割分担（リーダー、記録係）を変更することを勧める。
 - 演習課題に沿って対応策を検討し、グループ内の意見をまとめる。
 - ディスカッション内容の発表（15 分）
 - 複数のグループがある場合は、それぞれ発表してもらう（2 グループを目安）。
 - 演習 1 で発表していないグループがあれば、優先的に発表させる。
 - 回答例と講評（5 分）
- 振り返り（15 分）
 - 個人毎の振り返り（5 分）
 - 演習を通じて、気づいたことや課題を振り返る。
 - グループ内振り返り（10 分）
 - グループ内容で気づきや課題を共有する。
 - グループ内の振り返り結果を全体に発表する（1、2 名程度）。
- 質疑応答・各種案内・クロージング（10 分）
 - 講師による総評や質疑応答、アンケートの案内等を行い、クロージングする。

（3） 演習に使用する資料や機材類

演習に必要な資料や資材類を以下に示す。会場の大きさや参加人数等により、適宜追加や変更を行う。

- 演習用テキスト（講師用）：1 部/1 ファイル
 - 元ファイルは IPA ウェブサイトからダウンロード
 - 講義に使用する。資料投影用のパソコンにデータファイルを格納
- 演習用テキスト（受講者用）：参加人数分
 - 元ファイルは IPA ウェブサイトからダウンロード

- 参加人数分印刷をして当日配布
- 参加者全員がパソコンで参照できる場合、データによる配布も可
- 演習の回答例：参加人数分
 - テキストとは別に印刷し、グループディスカッション後に配布
- 中小企業のためのセキュリティインシデント対応の手引き
 - IPA ウェブサイトからダウンロード
 - 参加人数分印刷をして当日配布
 - 参加者全員が演習中にパソコンで参照できる場合、データによる配布も可
- アンケート：必要数
 - 演習の理解度、演習を通じて得た気づき（組織の改善点）等に関する項目を盛り込む
 - 演習当日に紙ベースで行う他、後日電子ファイルやウェブから回答させる形式も可
- 資料投影用のパソコン：1 台
- 資料投影用の大画面モニターやプロジェクタ：1 台
- マイク：必要数
 - 会場の大きさを勘案し、必要に応じて準備する
 - 使用する場合、講師用マイクのほか、受講者の発表用のマイクも準備すると良い
- 机と椅子：参加人数に合わせた必要数
- ホワイトボードとマーカー(複数色)：グループ数分
 - ディスカッションの内容の記録とグループ内共有、および発表に使用
 - 用意できない場合は大きめの紙（模造紙等）で代用可
 - パソコンで記録する方式も可能であるが、記録者以外が随時内容を確認できるように、サブディスプレイ等の使用を推奨
- 付箋（大きめのもの）：必要数
 - グループディスカッション時、項目の洗い出し（ブレインストーミング）に使用。
必須ではないが、受講者が使用する可能性があるため、必要に応じて用意しておく
- ネームプレート：必要数
 - 着席場所の指定や、グループ内でのメンバーを把握する目的で使用

(4) 会場の確保とレイアウト

演習に使用する会場のレイアウト例（20 名参加を想定）を以下の図に示す。机をグループ毎（島型）に配置するほか、ホワイトボード等の資材も設置する必要があるため、十分な広さを確保すること。

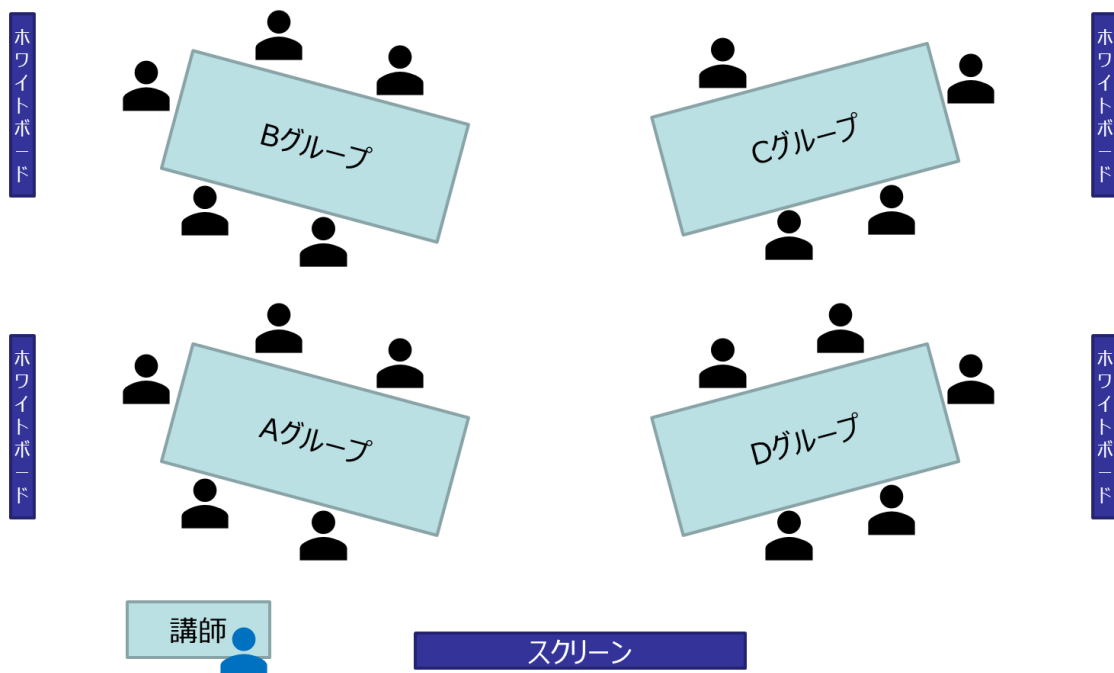


図 5-2 会場レイアウト例

(5) 事前学習

参加者の情報セキュリティに関する前提知識を揃えるために、必要に応じ事前学習を実施する。学習にあたっては、IPA の映像コンテンツ²等を活用していただきたい。

一例として、ランサムウェア感染を想定したシナリオで実施する場合、IPA が公開している「今、そこにある脅威～組織を狙うランサムウェア攻撃～」の映像コンテンツ³を事前に視聴させるといったことが考えられる。

演習当日に学習の時間を設けることも可能であるが、グループディスカッションの時間が短くならないよう、タイムスケジュールに留意すること。

² IPA:映像で知る情報セキュリティ

<https://www.ipa.go.jp/security/videos/list.html>

³ YouTube (IPA チャンネル) : 今、そこにある脅威～組織を狙うランサムウェア攻撃～

<https://www.youtube.com/watch?v=TWqJ5P8oaUM>

6. 演習実施

演習は、前章で作成したタイムスケジュールをもとに進行する。

6-1. 座学

講師用のファイルのノート部分に補足事項を記載しているため、これを参考に説明を行う。受講者の知識等に合わせて、適宜用語の説明等を入れながら進めること。

6-2. 演習

演習の進行にあたり、各フェーズでの注意事項を説明する。

(1) グループワーク

- その時点で判明している被害状況や影響範囲を加味して、組織として行うべき対応を議論いただくこと（その時点で不明なものは、必要に応じて調査を行うという対応として挙げていただく）。
- 参加者が自由に意見を述べられるような雰囲気をつくり、参加者から出た意見に対し、建設的な議論がなされる（批判的・否定的なコメントに偏らない）ように誘導すること。
- 挙げた意見は、まとまってから記録するのではなく、随時ホワイトボード等に記入してもらうようにすること。
- 議論が発散、ないしは停滞している場合、助言や軌道修正を行い、各課題に対し時間内に一定の結論が出るように誘導すること。
- 助言を行う場合、考慮すべき観点等のヒントを与えることにとどめ、回答例を教えるのは控えること（正解を導き出すことではなく、考えていただくことが重要であるため）。
- 講師やファシリテーターが、グループ討議中に各テーブルを回った際に、後で取り上げたい意見をメモしておき、発表時に紹介する。

(2) 発表

- 結論だけではなく、その結論に至った理由についても話していただくようにする。
- 複数グループに発表をさせる場合、残り時間に留意する（他のグループと重複する内容は説明を省略する等）。
- 発表を行ったグループと異なる視点で検討を行ったグループがいる場合、挙手を求めて簡単に話していただく時間を設ける。

(3) 講評

- 回答例をベースに説明を行う。この時に、回答例で示している内容がインシデント対応ステップのどこにあたるのか、また、何故この段階で必要なのかを説明するように努める。
- 回答例はあくまで一例であるので、各グループから異なる回答が出た場合でも、明確に誤っている部分があればポジティブなコメントを行うように努める。
- 明らかに誤った回答があった場合は、その理由を丁寧に説明し、受講者にネガティブな印象を抱かれないように配慮すること。

(4) 振り返り

- 回答内容の正誤（できたこと、できなかったこと）を評価するのではなく、今後のインシデント対応に活かすことのできる「気づき」を重視すること。
- 可能であれば、自組織の問題と具体的な改善策等についても考えていただくこと。

6-3. 質疑応答・各種案内・クロージング

質疑応答にあたっては、可能な範囲で対応することとし、その場で答えられない内容は持ち帰って後日回答することとする。

また、その場で質問しづらい場合があると想定されるため、別途アンケートやメール等で質問を受け付けるようにすることが望ましい。

7. 事後作業

演習の効果を最大化するためには、演習結果をもとに、組織の体制やインシデント対応手順等を見直していく必要がある。

7-1. アンケート

受講者に対してアンケートを実施し、演習の改善点や、組織において見直しが必要な事柄についての情報を得る。

- アンケート項目の例
 - 座学や演習内容の理解度
 - 満足度
 - 実際のインシデント対応に活かせるか
 - 自組織におけるルール等の改善点
- 等

7-2. 社内報告

アンケートの結果や、組織における改善事項等をまとめた報告書を作成する。報告書の内容を経営層に説明し、改善策の実施の許可や予算措置等につなげる。

7-3. ルール等への反映

前項で取りまとめた内容をもとに、インシデント対応体制の見直し、対応手順の整備、インシデント発生時の報告先の再確認といった改善を行う。

必要に応じ、他のシナリオでの演習や、従業員教育を計画する。

8. 一般企業向けランサムウェア感染シナリオの解説とカスタマイズ方針

本章では、一般企業向けランサムウェア感染シナリオの詳細解説とカスタマイズについて説明する。

8-1. 事例企業の概要

本演習シナリオで用いている仮想の企業の情報を以下に記す。変更せずそのまま使用できるような設定としているが、自組織内の要員のみで演習を実施する場合は、実態に合わせてカスタマイズすることで、演習の効果を高めることができる。

(1) 企業概要

テンプレートでは、都内の中小企業を想定した設定としている。

社 名：アイピーエー製造株式会社

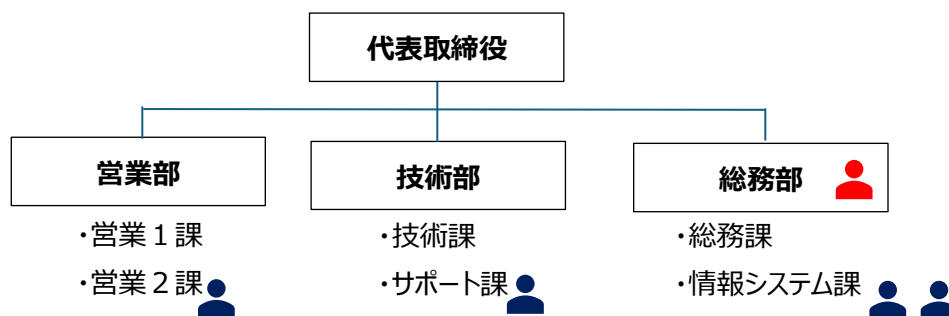
拠 点：東京都文京区本駒込

決算月：3月

従業員：60名

取引先：中小企業

業 務：事務機器、ネットワーク機器の販売、付随する営業及び管理業務



(2) セキュリティ管理

以下のように基本的な情報セキュリティに関する体制整備や教育等が行われている設定となっている。

- ・ 総務部長（取締役）が情報セキュリティ担当者を兼務
- ・ 情報システム課2名と各部1名からなる情報セキュリティ委員会を発足（月に1

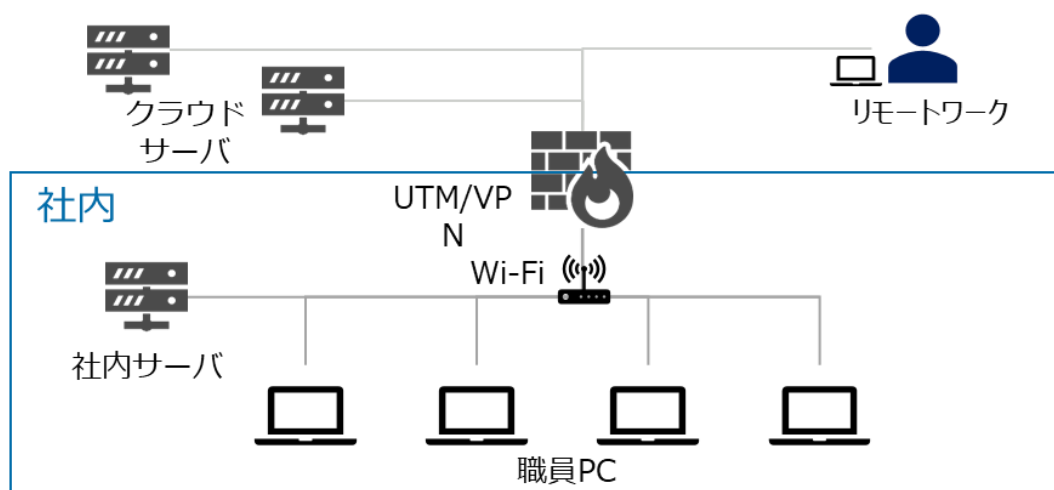
回委員会を定期的に開催)

- ・ 「中小企業の情報セキュリティ対策ガイドライン」を参考に情報セキュリティ規程を整備
- ・ 情報セキュリティに関する従業員教育（e-learning）を年1回実施

(3) 社内システム・ネットワーク環境

クラウドサービスと社内サーバに構築されたシステムを併用する典型的な構成としている。

- ・ メールサーバ、Webサーバはクラウド上にあり、情報システム課にて管理・運用している。
- ・ 業務で利用している販売管理システム、会計システムはクラウドサービス(SaaS)として提供され、ユーザのデータは、各サービスのクラウドサーバ上に保存されている。
- ・ 社内インフラにある社内サーバは、ファイル共有サーバであるが、ActiveDirectoryサーバ（ADサーバ）⁴も併用しており、業務システム等のデータを保有している。
- ・ PCのOSはWindows11を利用、ウイルス対策ソフトを導入、リモートワーク時は持出し可能
- ・ UTMを導入してネットワーク上の脅威に対応、VPN機器でリモートワークを実施
- ・ 部署毎にL3 switchでアクセス制限



⁴ Windows のサーバに搭載されたディレクトリサービス機能で、ユーザやコンピュータの管理を行うサーバ

(4) 補足事項

原則として、演習資料で提示している情報をもとにディスカッションを行っていただくが、受講者から質問があった場合は、以下のような情報を補足説明する。それ以外の前提条件は、グループ内で仮定して良い。

a) 取り扱い商品

- 複数ブランドの PC と周辺機器、事務所用什器（机、椅子、キャビネット等）、ネットワーク機器はルータ、HUB、Web カメラ等

b) 業務詳細

- 上記機器に関して、お客様環境において最適な機器を提案し、導入から保守サポートまで提供

c) 社内システム・ネットワーク環境

- 社内インフラには、AD サーバが構築されており、ID 管理を行う。AD サーバの管理者権限は、情報システム課の特定の従業員のみ保有している
- 部署間のアクセスは L3 スイッチで制御しており、他部署へのアクセスは不可としている。
- ファイルサーバ内のフォルダにアクセス権を付与しており、他部署のフォルダにはアクセスできないように制御している
- 各従業員が使用している PC は Windows11 のみで、規程上各自で Windows Update を実施することになっている。
- 新型コロナウイルス流行以降、在宅勤務を可能とし、社内 PC を持出し自宅から VPN 経由で社内ネットワークにアクセス可能としている。
- UTM から通知されるアラート対応は情報システム課で対応している。ログの取得はしているが、チェックはしていない。

8-2. ディスカッションポイント

(5) 状況(1)の内容と回答例

【状況(1) (3/27 9:30)】

- 営業部の従業員が朝 PC を起動したら、赤い画面が表示され、暗号化されて操作不能となっていた
- 発見した従業員から情報システム課に連絡がはいり、情報セキュリティ責任者へその旨の報告があった

→【課題】状況(1)において、誰に対し、どのように対応を指示・報告しますか

インシデント検知時の初動対応の基本的な考え方については、教材スライドの P.9「ステップ1 検知・初動対応」を参照。

状況から、ランサムウェアに感染した可能性があるとは推定できるが、この時点では従業員からの申告のみであり、ランサムウェアが原因と断定することはできない。したがって、まずは事実確認を行う必要があると考えられる。

ただし、より安全側に倒す判断として、この時点で当該 PC をネットワークから切り離すことを否定しない。

また、近年のランサムウェアは、複数の PC やサーバに対し感染範囲を広げていくことから、当該の PC 以外に影響が広がっていないかを確認することも重要である。

【回答例】 ※括弧書きは、回答例のスライドに記載していない内容

- ・ 情報システム担当に対して、報告した従業員と事実関係や影響範囲の確認を指示する
- ・ 情報セキュリティ委員会に属する各部の担当者に対して、同様の事象が発生していないか確認を指示する
- ・ (情報システム担当に対して、報告した従業員にヒアリングを行い、発見に至った経緯や実施した操作内容について確認するよう指示する)
- ・ (情報システム担当に対して、当該の PC をネットワークから切り離すように指示する)

(6) 状況(2)の内容と回答例

【状況(2) (3/27 10:00)】

- ・ 情報システム担当が確認したところ、営業部の PC 2 台、社内サーバ 1 台が暗号化されて操作不能となっていた
 - 営業部の PC には顧客（取引先）からの預かり情報などが保存されている
 - 技術部の PC では顧客（取引先）への遠隔保守サービスも行っている
 - 総務部のパソコンには従業員の個人情報なども保存されている
 - 社内サーバ（ファイル共有）には業務全般のデータが保存されている
- ・ 情報システム担当は発生している現象からランサムウェアに感染したと判断して情報セキュリティ責任者に報告し、相談のうえ対応を進めることにした

→ 【課題】 状況（2）において、誰に対し、どのように対応を指示・報告しますか

ランサムウェアに感染し、複数の PC やサーバに影響が広がっており、業務に支障が出ているものと考えられる。状況(1)の解説で述べた通り、影響範囲がさらに広がる恐れがあることから、被害拡大を抑えるために、機器をネットワークから切り離す等の処置が必要である。ネットワークから切り離す範囲については、その範囲を広くするほど被害の拡大を防止することができるが、切り離された PC で業務を行うことができなくなる。回答例において切り離し範囲を例示しているが、一律の正解を示しているものではない。業務継続と影響範囲拡大防止のどちらを優先するかにより判断が変わってくることに留意していただきたい。

また、個人情報等を保存している PC やファイルサーバも既に影響を受けている、あるいは今後影響を受ける恐れがある。近年のランサムウェア攻撃は、データを暗号化するだけでなく、データを窃取して脅迫を行うケースが目立っていることから、個人情報等が漏えいしている恐れがあることも念頭におきつつ対応する必要がある。

以上を踏まえると、企業の事業継続に影響する重大インシデントが発生したものと判断し、対策本部を設置するなどして必要な対応が速やかに行える体制に移行することが必要と考えられる。

【回答例】 ※括弧書きは、回答例のスライドに記載していない内容

- 経営者に対して、重大インシデントの発生を報告し、対策本部の設置を提案する。
- 情報システム担当に対して、感染拡大を防ぐために感染パソコンの隔離を指示する。
- 情報システム担当に対して、L3 switch で総務部と営業部のネットワークの隔離を指示する。
- 情報システム担当と保守担当者に対して、遠隔保守用のネットワークの接続制限を検討させる。
- 全従業員に対して、インシデントの発生を報告し、同様の事象が発生した場合速やかに報告するよう指示する。
- 外部セキュリティベンダに対して、緊急対応を相談する。
- (ネットワークや該当 PC、ファイルサーバ、AD サーバ、VPN 機器のアクセスログを取得する)
- (代替 PC の手配を行う)

(7) 状況(3)の内容と回答例

【状況(3) (3/27 13:00)】

- 外部セキュリティベンダが到着し、初動対応支援と調査を開始した
- 感染したパソコンには10万ドルの仮想通貨を要求するメッセージと、残り72時間
を示すカウントダウンタイマーが表示されていた

→【課題】状況(3)において、身代金を支払いますか。その判断理由は何か。

状況(2)において、感染拡大に対する一次対応は完了しているため、原因究明と暫定対応を行う状況にある。

セキュリティベンダによる初動対応支援として、感染範囲の特定や封じ込めが行われる。その後、ログの分析やフォレンジック調査などにより、侵入原因の特定等が行なわれる。

身代金の支払いについては、回答例に記載している理由から、原則として支払いに応じないことを推奨する。実際の攻撃においては、標的組織の規模等を勘案して支払い可能な金額を推定し、提示してくる場合があるが、金額の大小を問わず、身代金の支払いを行うべきではない。可能な限り、身代金を支払う以外の方法（バックアップからの復旧等）でデータの復旧を行うべきである。一部のランサムウェアについては、暗号化されたデータを復号するためのツールがウェブサイト上に公開⁵されている場合もあるため、確認することを勧める。ただし、人命等にかかわるケースを想定し、身代金を支払うという経営判断を行う可能性や、その判断基準について議論することは妨げない。

また、データ復旧業者に作業を依頼する場合は、料金や復旧方法等のトラブルを避けるため、日本データ復旧協会が公開している「ベンダー選定チェックシート⁶」を活用し、業者選定を行うことを勧める。

【回答例】

- 以下の理由により身代金の支払いは応じない
 - 暗号化されたファイルが復元される保証がない
 - 被害原因などが不明なため再度同じ攻撃を受ける可能性がある
 - 支払ったことで別の攻撃を受ける恐れがある

⁵ NO MORE RANSOM : 復号ツール

<https://www.nomoreransom.org/ja/decryption-tools.html>

⁶ 日本データ復旧協会：日本データ復旧協会ガイドライン

<https://www.drajp.or.jp/guideline/>

(8) 状況(4)の内容と回答例

【状況(4) (3/27 17:00)】

- 外部セキュリティベンダの調査の結果、営業部の PC4 台と社内サーバ（業務システム）1 台への侵害拡大を確認した。尚、リークサイトを確認したが、現時点では自社が保有するデータに関する投稿は確認されていない
- さらなるサイバー攻撃や外部への影響拡大を防ぐために、すべてのネットワーク切断を実施することにした

→【課題】状況（4）において、インシデントについて誰にどのような形で報告や相談を行いますか。

報告・公表の基本的な考え方については、教材スライドの P.11「ステップ2 報告・公表」を参照。

ランサムウェア感染により漏えいしたおそれのあるデータに個人情報（個人データ）が含まれる場合、個人情報保護委員会規則で定める「不正の目的をもって行われたおそれがある個人データの漏えい等（又はそのおそれ）」の要件に該当するため、個人情報保護委員会への報告が義務となる⁷。

個人情報保護委員会へ報告は、発覚から3～5日以内に「初報」を、発覚日から30日以内（上記③に該当する場合は60日以内）に「確報」を提出する必要がある。あわせて、個人データが漏えいした本人に対する通知も、明確な期限は定められていないが、「状況に応じて速やかに」「概要、個人データの項目、原因などの内容を」「本人にとって分かりやすい方法」で行う必要がある。詳しくは、個人情報保護委員会のウェブサイト⁸を参照いただきたい。

その他、特定の業界を対象とした法令や規則等により、必要な報告先が異なるため、事前に関連法規等を確認し、報告先を整備しておくことを勧める。

本事案では、「すべてのネットワーク切断を実施」しているため、社内に設置されているパソコンやサーバ、ネットワークを使用した業務ができなくなることを意味している。したがって、業務の停止により影響を受ける顧客や取引先等に状況報告を行う必要があると考えられる。報告の方法は、ウェブサイトによる公表、電話、メール等が考えられるが、ラン

⁷ 個人情報保護委員会：漏えい等の対応とお役立ち資料

<https://www.ppc.go.jp/personalinfo/legal/leakAction/>

⁸ 個人情報保護委員会：漏えい等報告・本人への通知の義務化について

https://www.ppc.go.jp/news/kaiseihou_feature/roueitouhoukoku_gimuka/

サムウェア感染によりシステムが利用できなくなっている状態であることを踏まえて、方法を決定する。サンプルの事例においては、ウェブサーバやメールサーバがクラウド上に設置されているため、代替の通信手段やパソコン等を手配すれば、ウェブサイトやメールを使用した報告・公表は可能と考えてよい。

相談窓口への相談は必須ではないが、インシデント対応にかかる支援や情報提供を受けられる可能性があるため、必要に応じて利用する（相談窓口の例は教材スライドの P.11 を参照）。特に警察は、被害届の提出だけではなく相談も受け付けているため、事案発生時に早めに相談を行っていくことで、インシデント対応や被害届の提出を円滑に行えるようになると思われる。

【回答例】 ※括弧書きは、回答例のスライドに記載していない内容

- ・ 遠隔保守を行っている顧客（取引先）に対して、遠隔保守が行えない旨を個別に報告する（可能であれば代替手段の提示も行う）
- ・ 警察のサイバー犯罪相談窓口に対して、相談する
- ・ ネットワーク切断による影響が広範囲に及ぶ可能性がある場合は、Web サイトを通じた公表を検討する
- ・ 個人データの漏えい等により個人の権利利益を害する恐れが確認された場合は、個人情報保護委員会への報告と本人への通知を行う
- ・ （情報漏えいの可能性がある場合は、業種により所轄官庁へ届け出が必要な場合もある）

なお、本シナリオでは時間の都合上、教材スライド P.13「復旧・再発防止」はディスカッションの対象外としている。再発防止策のフェーズについてディスカッションを行う場合は、以下のような状況を想定して実施する。

- ・ 代替機の調達、バックアップからデータ復元により数日で業務復旧
- ・ ランサムウェアの侵入原因は、VPN 機器の既知の脆弱性を悪用されたもの（脆弱性修正プログラムを適用していなかった）。
- ・ VPN 機器の脆弱性修正プログラム適用は情報システム課で実施すべきところ、脆弱性に関する情報を入手していなかった。

9. 医療機関向けランサムウェア感染シナリオの解説とカスタマイズ方針

本章では、医療機関向けランサムウェア感染シナリオの詳細解説とカスタマイズについて説明する。

9-1. 事例医療機関の概要

本演習シナリオで用いている仮想の医療機関の情報を以下に記す。変更せずそのまま使用できるような設定としているが、自組織内の要員のみで演習を実施する場合は、実態に合わせてカスタマイズすることで、演習の効果を高めることができる。

(1) 企業概要

テンプレートでは、都内の中規模病院を想定した設定としている。

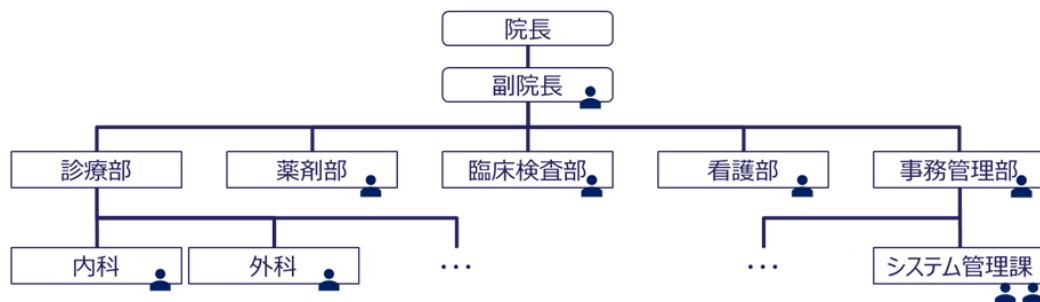
社 名：アイピーエー病院

拠 点：東京都文京区本駒込

病床数：140 床

職員数：165 名

診療科目：内科、消化器内科、循環器内科、外科、整形外科、リハビリテーション科



(2) セキュリティ管理

以下のように基本的な情報セキュリティに関する体制整備や教育等が行われている設定となっている。

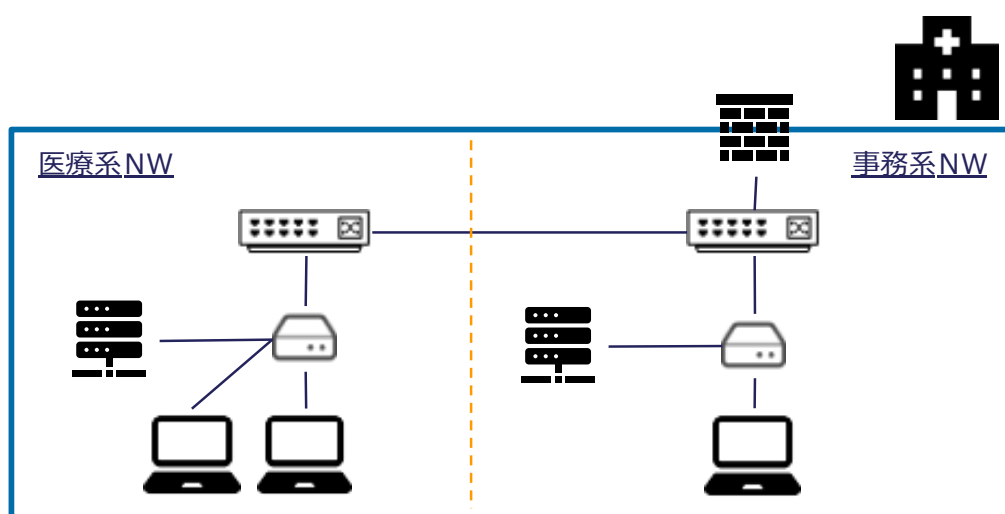
- ・ 副院長が情報セキュリティ責任者を兼務
- ・ 情報システム課2名と各部1名以上からなる情報セキュリティ委員会を組織
- ・ 医療情報システムの安全管理に関するガイドライン第5.0版を参考に情報セキュリティ規程を整備

- ・ 情報セキュリティに関する職員教育(e-Learning)を年 1 回実施
- ・ 情報セキュリティ対策の実施状況は各部の管理者が年 2 回確認し、情報セキュリティ委員会へ報告

(3) 社内システム・ネットワーク環境

医療系ネットワークと事務系ネットワークを論理的に分離した典型的な構成としている。
 なお、状況付与をシンプルにするため、クラウドサービスは構成から外している。

- ・ ネットワークは医療系ネットワークと事務系ネットワークで論理的に分割、医療系ネットワークは原則インターネットに接続禁止
- ・ 医療系ネットワークは基幹システム（電子カルテ、オーダリング、医事会計、看護支援等）、部門システム（検体検査、医用画像情報、給食管理等）から構成され、診療部門毎に L3 switch⁹でアクセス制限
- ・ 基幹システムはバックアップを取得（バックアップサーバに毎週末、LTO テープ¹⁰に毎月末）
- ・ 各システム・ネットワークは構築したシステム会社が保守



(4) 補足事項

原則として、演習資料で提示している情報をもとにディスカッションを行っていただくが、受講者から質問があった場合は、以下のような情報を補足説明する。それ以外の前提条

⁹ レイヤ3スイッチ：ネットワークを論理的に分割できるネットワーク機器

¹⁰ Linear Tape-Open テープ：大容量データを保管できる磁気

件は、事前にファシリテーター側で設定しておくか、グループ内で仮定して良い。

a) 社内システム・ネットワーク環境

- ・ システム管理課は、プライムベンダである A 社と連携して院内のシステム構成を管理している。しかし、部門システムの中には当該部門で独自に構築・導入されたものがあり、システム管理課において構成やセキュリティ対策の実施状況等の詳細を把握できていない可能性がある。
- ・ 事務系ネットワーク配下のパソコンやサーバは、ウイルス対策ソフトの導入や OS のセキュリティ更新プログラムのインストールといった基本的なセキュリティ対策が実施されている。
- ・ 基幹システムや部門システムの一部は、システムの都合上、ウイルス対策ソフトの導入や OS のセキュリティ更新プログラムのインストール等が行えていないものがある。

b) 体制等

- ・ 地震等の災害発生を想定した BCP（事業継続計画）は策定されているが、セキュリティインシデントを想定した BCP は策定されていない。

9-2. ディスカッションポイント

(5) 状況(1)および(2)の内容と回答例

【状況(1) (3/27 9:30)】

- ・ 病院内に設置されていたプリンタから、データを窃取および暗号化した旨の文書の大量印刷を内科の看護師が発見した
- ・ 発見した看護師から情報セキュリティ責任者へその旨の報告があった。

【状況(2) (3/27 10:00)】

- ・ 情報セキュリティ責任者から指示を受けたシステム管理者が確認したところ、電子カルテサーバが暗号化されて操作不能となっていた
- ・ システム管理者は発生している現象からランサムウェアに感染したと判断して情報セキュリティ責任者に報告し、相談のうえ対応を進めることにした

→【課題】状況(2)において、情報セキュリティ責任者として、誰に対し、どのように対応を指示・報告・相談しますか

インシデント検知時の初動対応の基本的な考え方については、教材スライドの P.10「ステップ1 検知・初動対応」を参照。

プリンタから脅迫文書が大量印刷される事象は、徳島県つるぎ町立半田病院のランサムウェア感染事案で実際に発生したものである¹¹。状況(2)まで速やかに報告や調査が行われており、ここまでの初動対応は的確である。

電子カルテサーバがランサムウェアに感染してしまったため、既に診療に影響が出ているものと想定される。また、ランサムウェアが感染を拡大し、影響範囲がさらに広がる恐れがあることから、被害拡大を抑えるために、機器をネットワークから切り離す等の処置を行うべきである。したがって、情報セキュリティ責任者の立場としては、院長に対策本部設置を提案するなど、必要な対応が速やかに行える体制への移行を促す必要があると考えられる。

ネットワークから切り離す範囲については、その範囲を広くするほど被害の拡大を防止することができるが、切り離されたパソコンやシステムで業務を行うことができなくなる。回答例においては、電子カルテシステムと、部門システム毎の切り離し範囲を指示しているが、一律の正解を示しているものではない。例えば、患者の生命維持に関わる医療機器が繋がっている部門システムを隔離する場合、隔離により当該部門システム内の機器の動作（患者の生命）に影響を与えないことが前提条件となる。患者の生命維持を最優先としつつ、次に業務継続と影響範囲拡大防止のどちらを優先するかにより判断が変わってくることに留意していただきたい。

ユーザ側で実施できないシステムへの対応については、システムの運用・保守を行っている会社に対応を依頼することが最初の選択肢となる。自組織のみで十分な対応が行えないと想定される場合は、他の相談窓口等を活用する。医療機関向けの初動対応支援を行う窓口として、厚生労働省の委託事業により設置されている相談窓口¹²や日本医師会が設置しているサイバーセキュリティ対応相談窓口¹³がある。都道府県警では、被害届だけではなくサイバー攻撃に関する相談も受け付けている。

また、近年のランサムウェア攻撃は、データを暗号化するだけでなく、データを窃取して脅迫を行うケースが目立っていることから、既に個人情報等が漏えいしている恐れがあることも念頭におきつつ対応する必要がある。

出題上は、情報セキュリティ責任者としての対応を検討いただくものとしているが、病院としての対応（BCP等）について、議論が行われても問題ない。

¹¹ 徳島県つるぎ町立半田病院：コンピュータウイルス感染事案 有識者会議調査報告書

https://www.handa-hospital.jp/topics/2022/0616/report_01.pdf

¹² 厚生労働省：医療機関向け セキュリティ教育支援ポータルサイト

<https://mist.mhlw.go.jp/incident/>

¹³ 日本医師会：サイバーセキュリティ対応相談窓口（緊急相談窓口）

<https://www.med.or.jp/doctor/sys/cybersecurity/001566.html>

【回答例】

- ・ 院長に対して、重大インシデントの発生を報告し、対策本部の設置を提案する
- ・ システム担当に対して、感染拡大を防ぐために感染パソコンの隔離を指示する
- ・ システム担当に対して、診療部門毎のネットワークの隔離を指示する
- ・ 全職員に対して、インシデントの発生を報告し、同様の事象が発生した場合速やかに報告するよう指示する
- ・ 外部システムベンダに対して、緊急対応を相談する
- ・ 入院患者の対応、外来・救急の制限等を検討する

(6) 状況(3)の内容と回答例

【状況(3) (3/27 13:00)】

- ・ 外部システムベンダ A 社が到着し、初動対応支援と調査を開始した
 - ・ 感染したパソコンには 10 万ドルの仮想通貨を要求するメッセージと、残り 72 時間を示すカウントダウンタイマーが表示されていた
- 【課題】状況（3）において、身代金を支払って復元しますか。その判断理由は何か

身代金の支払いについては、回答例に記載している理由から、原則として支払いに応じないことを推奨する。実際の攻撃においては、標的組織の規模等を勘案して支払い可能な金額を推定し、提示してくる場合があるが、金額の大小を問わず身代金の支払いを行うべきではない。可能な限り、身代金を支払う以外の方法（バックアップからの復旧等）でデータの復旧を行うべきである。本事例においては、電子カルテを含む基幹システムのバックアップを LTO テープに保存（毎月末）している。LTO テープは、原則としてネットワークから隔離された場所に保管されており、ランサムウェアにより暗号化される可能性は低い。このため、少なくとも 1 か月前のデータに復元可能と見込まれる。ただし、人命等にかかわるケースを想定し、身代金を支払うという経営判断を行う可能性や、その判断基準について議論することは妨げない。

また、一部のランサムウェアについては、暗号化されたデータを復号するためのツールがウェブサイト上に公開されている場合もあるため、確認することを勧める。データ復旧業者に作業を依頼する場合は、料金や復旧方法等のトラブルを避けるため、日本データ復旧協会が公開しているベンダー選定チェックシートを活用し、業者選定を行うことを勧める。

【回答例】

- ・ 以下の理由により身代金の支払いは応じない

- ・ 暗号化されたファイルが復元される保証がない
- ・ 被害原因などが不明なため再度同じ攻撃を受ける可能性がある
- ・ 支払ったことで別の攻撃を受ける恐れがある

(7) 状況(4)の内容と回答例

【状況(4) (3/27 17:00)】

- ・ 外部システムベンダの調査の結果、医療系ネットワークのパソコン 2 台と部門サーバ 1 台への侵害被害を確認した。尚、リークサイトを確認したが、現時点では自社に関する投稿は確認されていない。
- ・ 外来診療を停止、救急を制限、さらなるサイバー攻撃を防ぐため、すべてのネットワークを切断して対応することとした。

→【課題】状況（４）において、外部に対しどのように報告・公表しますか

報告・公表の基本的な考え方については、教材スライドの P.11「ステップ２ 報告・公表」を参照。

「医療情報システムの安全管理に関するガイドライン」では、医療機関等がサイバー攻撃を受けた（疑い含む）際に、厚生労働省等の所管省庁への連絡等を行う必要があるとされている。医療機関独自の連絡先としては、教材に記載の通り、厚生労働省の医政局¹⁴が挙げられる。

ランサムウェア感染により漏えいしたおそれのあるデータに個人情報（個人データ）が含まれる場合、個人情報保護委員会規則で定める「不正の目的をもって行われたおそれがある個人データの漏えい等（又はそのおそれ）」の要件に該当するため、個人情報保護委員会への報告が義務となる。

個人情報保護委員会へ報告は、発覚から３～５日以内に「初報」を、発覚日から 30 日以内（上記③に該当する場合は 60 日以内）に「確報」を提出する必要がある。あわせて、個人データが漏えいした本人に対する通知も、明確な期限は定められていないが、「状況に応じて速やかに」「概要、個人データの項目、原因などの内容を」「本人にとって分かりやすい方法」で行う必要がある。詳しくは、個人情報保護委員会のウェブサイトを参照いただきたい。

この時点で外来診療の停止や救急の制限が行われているため、患者を受け入れられないことについて、一般の方や地域の医療機関等に広く周知する必要があると考えられる。周知

¹⁴ 厚生労働省：医療分野のサイバーセキュリティ対策について

https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryuu/iryuu/johoka/cyber-security.html

の方法は、ウェブサイトによる公表、電話、メール等が考えられるが、ランサムウェア感染によりシステムやネットワークが利用できなくなっている状態であることを踏まえて決定する。

その他、セキュリティインシデントの観点ではなく、医療提供が停止しているという観点から必要な報告先についても議論いただく。

【回答例】

- ・ 厚生労働省等の所管省庁（医政局、警察、個人情報保護委員会）への連絡
- ・ 内部（患者、医療関係者）に対して今後の対応方針や案内方法を提示
- ・ 外部（外来、マスコミ）に対してウェブ等を通じた対応方針の提示
- ・ 地域の医療機関と支援体制を相談

→【課題】状況（4）において、医療の継続のため、早期復旧や暫定対応に向けてどのような指示を出しますか

システムの復旧にあたっては、バックアップデータの他、代替となるパソコンやサーバ等の確保が重要となる。ランサムウェアに感染してしまったパソコンやサーバはそのままでは利用できないため、代替機を確保し、新たに設定作業やデータの復元等を行う必要がある。

紙カルテ運用等により患者の生命維持に必要な最低限の医療を提供しつつ、システム復旧に向けての問題点を把握し、優先度をつけて対応を実施していく必要がある。

【回答例】

- ・ バックアップからデータの復旧の指示、代替機の手配
- ・ 紙カルテの使用等の暫定運用
- ・ 入院患者に対する院内診療を優先するための問題点の把握及び対応

（8）状況(5)の内容と回答例

【状況(5)（4/27 17:00）】

- ・ システムが全面復旧した。外部ベンダの調査の結果、以下のことが分かった
 - 医療系ネットワークの一部の部門システムに、外部システムベンダ B 社のリモート保守のためのインターネット接続が存在していたが、外部システムベンダ A 社は認識していなかった
 - リモート保守のための VPN 装置はアップデートが行われておらず脆弱性が残っていた
 - 部門システムの都合上、サポート切れ OS の利用やウイルス対策ソフトが未導

入の端末があった

- 院内のバックアップサーバもランサムウェアに感染し、LTO テープからデータ復旧したため、約 1 か月間のデータが復旧できなかった
- インシデント発生の一週間後に記者会見を開いたが、会見内容について説明責任が果たされていないとの指摘が起きていた
- ・ 以上をもとに、情報セキュリティ委員会で再発防止策を検討することにした

→【課題】状況（5）において、どのような再発防止策を策定しますか。また、その優先度はどうしますか。

状況から、ランサムウェア攻撃を行った攻撃者は、外部システムベンダ B 社が設置した VPN 装置に残っていた脆弱性が悪用し、医療系ネットワークに侵入したものと推定される。さらに、セキュリティ対策が不十分な端末やサーバが存在していたため、ランサムウェアによる被害範囲が広がってしまったとみられる。被害の直接的な原因となった脆弱性対応を行った後、再発防止のために根本的な原因を突き止めて対策する必要がある。

事例組織においては、医療情報システムの安全管理に関するガイドライン¹⁵を参考にした情報セキュリティ規程の整備や、情報セキュリティに関する職員教育が行われていた。しかし、本事例のようなインシデントが発生してしまったことを鑑みると、規程が形骸化し、職員が守るべきことが徹底されていなかったことが、根本的な原因の一つと考えられる。

また、医療機関内では様々なシステムが利用されており、各システムが異なるベンダにより導入・運用されているケースは珍しくない。事例組織においては、組織としてシステムの全体像を認識し、管理できていなかったことが問題である。各部門が独自にシステムを導入する場合においても、情報システム部門等がそれを一元的に把握し、ベンダ任せにせず必要なセキュリティ対策等を実施させるためのルールと体制の構築が必要である。

以上のことから、優先度の高い再発防止策として、内部規程やベンダとの契約内容を実効性のある内容へ見直しを行うことに加え、順守の状況を定期的に確認(必要に応じて、第三者による監査も検討)することが挙げられる。

さらに、事案が発生した際の影響を小さくするために、セキュリティインシデントを想定した BCP の策定や、セキュリティインシデントに関する教育や訓練の実施が有効である。

¹⁵ 2025 年 3 月現在、同ガイドラインの最新版は、2023 年 5 月に発行された第 6.0 版である。したがって事例企業が参考にした同ガイドラインの第 5.0 版は、2017 年 5 月に発行された古いものであることに注意が必要である。

インシデント発生から一週間後に開かれた記者会見では、事象の原因や再発防止策等を説明できていなかったため、本事象について詳細な説明が求められている状況である。広報にあたっては、その対応を誤ると信頼を大きく損なう事態になりかねない。したがって、広報マニュアルや弁護士等の第三者に相談できる体制を整備しておくことで、有事の際に的確な説明責任を果たせるようにしておく必要がある。

再発防止策の優先度については、以下の考え方で整理すると良い。

① 事案の直接的な原因の特定と対処

同様の手口で攻撃を受けないようにするため、直接的な原因となった事象に対処する（空いている穴をふさぐ）。

② 事案の根本的な原因の特定と対策

引き金となった事象が二度と発生しないようにするため、根本的な原因を特定し対策する（穴が空かないようにする）。

③ 事案発生時の影響を低減する対策

万が一、類似の事案が発生した時に備え被害を防止・低減する対策を行う（穴から落ちてもけがをさせない、または軽減する）。

【回答例】

- ・ 発見された脆弱性への対処
- ・ 内部規程の順守状況の確認及び是正、外部監査も検討
- ・ 内部規程を見直して実効性を高める（インターネット接続、バックアップの間隔と手法等）
- ・ セキュリティ対応能力も考慮したベンダ選定
- ・ ベンダとの契約内容の妥当性確認
- ・ セキュリティインシデントを想定した BCP の整備
- ・ インシデント内容を踏まえたセキュリティ教育、訓練
- ・ 説明責任を果たせる仕組みの構築（広報マニュアル整備、弁護士への相談等）

以上