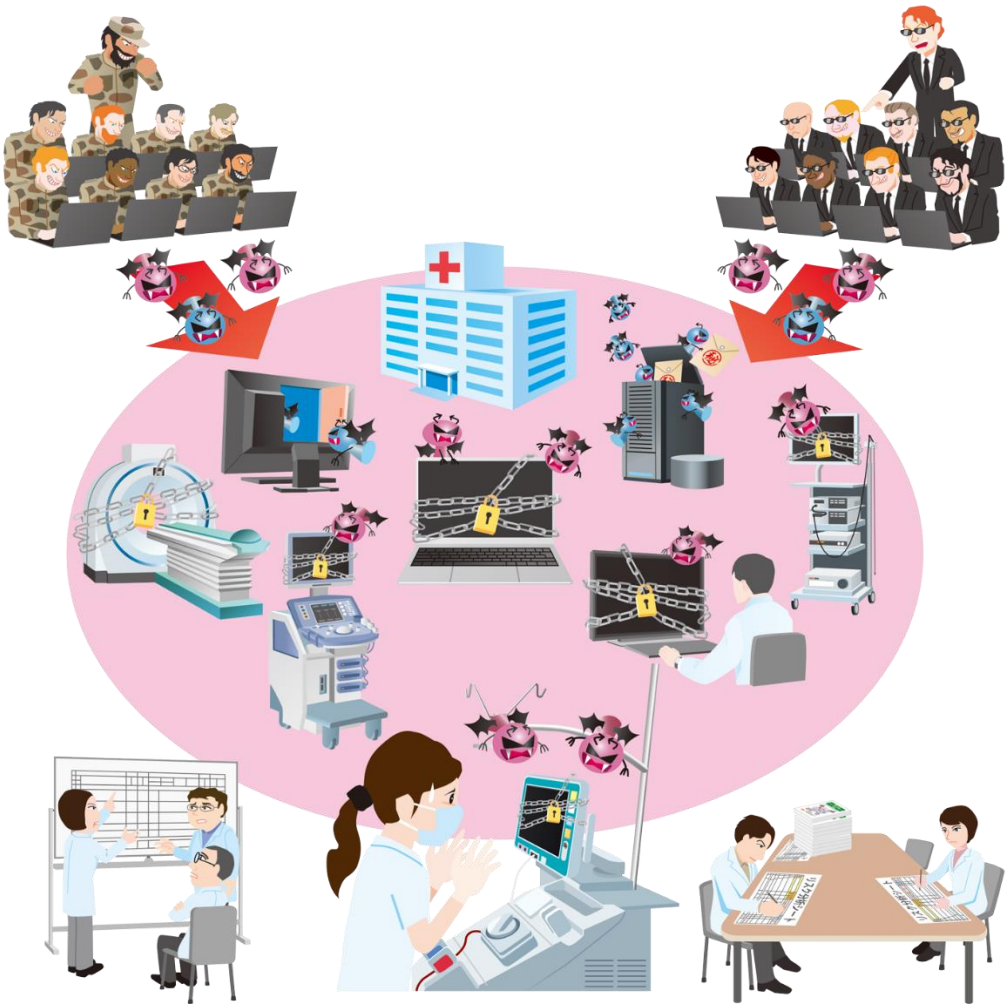
制御システムのセキュリティリスク分析ガイド補足資料

制御システム関連のサイバーインシデント事例7

～2020 年　医療関連企業のランサムウェアによる業務停止～



2020 年 9 月

IPA 独立行政法人情報処理推進機構
セキュリティセンター

目 次

はじめに

「セキュリティ対策を推進する上で、過去の事例に学ぶことは有益です。」

制御システムを保有する事業者にとって、国内外で発生したサイバーインシデント事例の情報をもとに、自社の制御システムに対して同様の脅威が発生した場合のリスクアセスメント（リスクの特定・分析・評価）を実施することは、セキュリティリスク管理の強化につながる。

IPA（情報処理推進機構）は、制御システムにおけるリスクアセスメントの具体的な手順を解説した『制御システムのセキュリティリスク分析ガイド』を公開している。このガイドでは、制御システム保有事業者の事業に重大な被害を与えるサイバー攻撃からの回避に重点を置いた「事業被害ベースのリスク分析手法」を紹介している。自社の制御システムに対して、過去の事例と同様の脅威が発生した場合の事業への影響、脅威の発生可能性、発生した脅威の受容可能性／脅威に対するセキュリティ対策の有効性を分析することは、事業者にとって有益であると考えられる。

「制御システム関連のサイバーインシデント事例」シリーズは、『制御システムのセキュリティリスク分析ガイド』の補足資料として作成した。制御システムのサイバーインシデント事例をもとに、その概要と攻撃の流れ（攻撃ツリー）を紹介している。これらの情報をもとに、事業被害ベースのリスク分析を実施する際に、事例に相当する攻撃ツリーの作成、セキュリティ対策の策定に活用することが出来る。

【参考資料】に関しての内容詳細は、リンクから原文を確認いただきたい。本資料では、脚注は上付き番号（例 1）、巻末の参考資料は[ ]付き番号（例 [1]）で表している。

本資料の位置付け

2020 年ランサムウェア EKANS（Snake）[1][1]が各所でサイバー攻撃を開始 [2]。日本企業を含む複数の企業が被害を受けたとされるが[3][4]、本書では 5 月に起きた世界的な医療関連企業 Fresenius Group[6]におけるサイバーインシデントを取り上げる。

本書では、当該企業やセキュリティベンダ等の公開情報（巻末の【参考資料】）をもとに、サイバーインシデントの概要と攻撃の流れを紹介している。後半では、当該インシデントに関係する情報を整理し、本インシデントをモデルとしたリスク分析を行う際の、攻撃シナリオや攻撃ツリー・ステップの作成例、対策・緩和策への活用例など、リスクアセスメントへのアプローチを紹介している。

対象読者：　制御システムのリスクアセスメント担当者

[1] EKANS は Snake とも呼ばれているが、APT（持続的標的型攻撃:Advanced Persistent Threat）グループにも同名称の Snake（Turla）[5]があり、混乱を避けるために当該ランサムウェアをここでは EKANS（Snake の逆スペル）と呼ぶことにする。

1. 2020 年 医療関連企業のランサムウェアによる業務停止

1.1. インシデント概要

2020 年 5 月に、独に本社のある医療関連企業 Fresenius（フレゼニウス） Group においてランサムウェア EKANS の被害を受け多くのコンピュータが停止し製造や診療に影響を及ぼしたとされ、さらに患者のデータが窃取され公開されるといったインシデントが発生した[7]。
Fresenius Group はドイツに本拠を置く以下の4つの医療関連企業から構成されている。

・Fresenius Medical Care： 人工透析装置や関連医療機器の製造と関連サービス（透析治療）を行う

・Fresenius Helios：ヨーロッパを代表する民間病院の運営会社

・Fresenius Kabi： 医薬品・医療機器と関連サービスを提供

・Fresenius Vamed： 医療施設の開発、コンサルティングなどを行う

Fresenius Group の報告[7]と報道[8]によると、5 月はじめに Fresenius Group の IT システムがランサムウェアの被害を受け業務が一時停止[2]、さらにその2週間後に Fresenius Group 傘下の Fresenius Medical Care の透析サービスを受けた一部の患者の個人情報がインターネットに公開されるインシデントが発生した。ランサムウェアによって残された脅迫状（ランサムノート）には、コンピュータ内のデータを暗号化したというメッセージに加え、内部で集めた機密情報を公表するという記載があった[10][11]。

今回、当該事例を紐解くための詳細の報告や記事が少なく、システム構成、攻撃者の侵入方法、攻撃手法等に関しては、事例理解のため IPA の知見に基づく代表的な例示での説明を行う。

前提とするシステム構成に関しては、IEC 62443-2 や NIST SP800-82 Rev.2、経産省の「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」（案）[12]等をもとに作成した仮想システム構成図（図 1-1）を用いる。

なお、同時期に米国国土安全保障省（DHS）と英国の国立サイバーセキュリティセンター（NCSC）が、サイバー作戦の一環として新型コロナウイルス感染症（COVID-19）パンデミックを悪用し医療機関、製薬会社等をターゲットとする脅威グループの共同警告を発しており[13]、攻撃者の攻撃手法として、ウェブサイトの脆弱性の利用とパスワードスプレー攻撃[3]について言及されている。これら攻撃手法が Fresenius Group で用いられたという直接的な記事は見つからないが可能性として参考にし、また EKANS の分析結果の情報や過去のサイバーインシデントの事例を参考に補完・推考する。

---

[2] 報道では Fresenius Kabi の米国拠点とノルウェーの工場の一時的な稼働停止被害[8],[9]、Fresenius Group の報告[6]では Fresenius の IT システムが被害を受けたとされている。情報窃取と暗号化の二重の脅迫による被害と言える[14]。

[3] 不正アクセスを目的とし、同じパスワードで複数の ID にログインを試みる攻撃で、アカウントのロックアウトを回避し、気付かれずにログインすることができる。

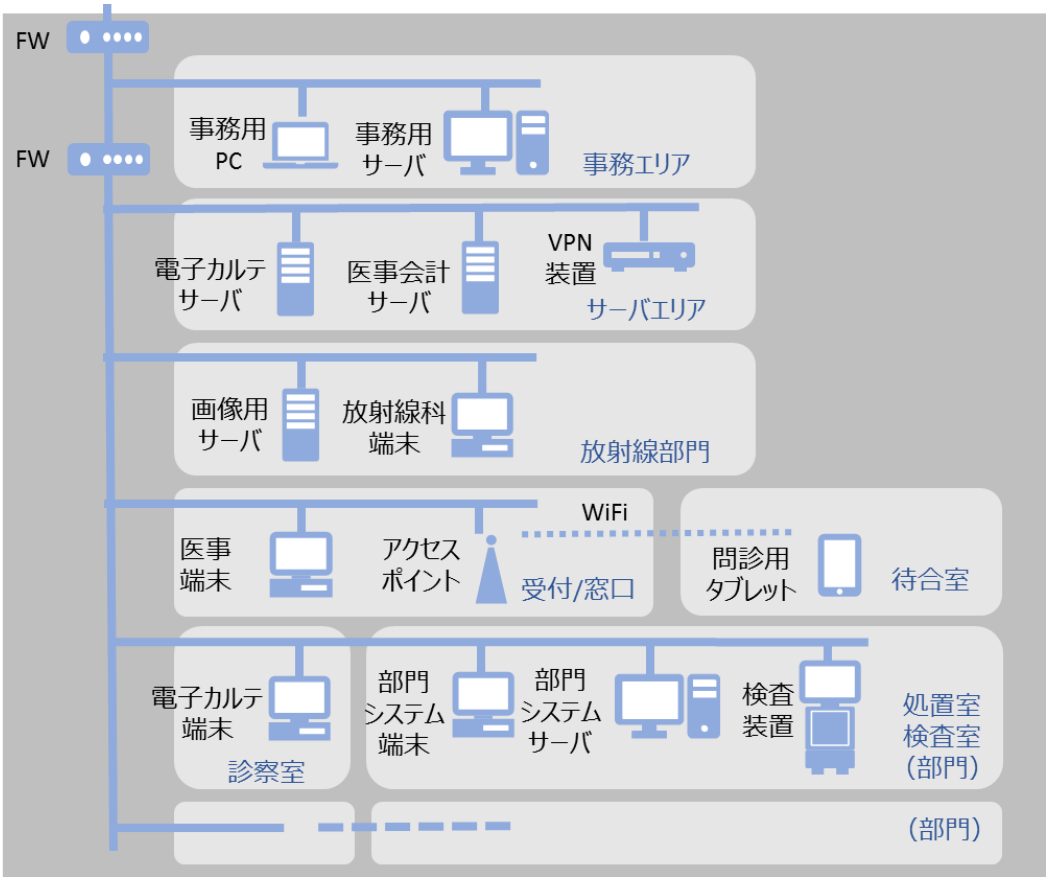


図 1-1 事例理解のための仮想システム構成図(実際のシステム構成とは異なる)

今回紹介するインシデントでは、医療機関だけでなく、医療機器の製造系のシステムでも被害が発生しているが、本システム構成図及び事業被害では割愛する。製造系のシステムに関しては、例えば、IPA の「制御システム関連のサイバーインシデント事例 5」[15]などを参照していただきたい。

【コラム】EKANS の特徴

EKANS は 2019 年 12 月に出現したランサムウェアである。本稿の執筆時点でもさまざまな亜種が作られその特徴は変化し解析が進められているが、特に ICS(産業用制御システム)のプロセスを強制的に停止させるという、ICS も標的とできるランサムウェアという特徴を持っている[1]。また、EKANS には、伝搬・拡散機能は内蔵されておらず対話的に起動するか、スクリプトを使ってホストに感染させる必要がある。つまり、サイバー攻撃のツール群のうち ICS サービスを含む特定プログラムの強制終了とデータの暗号化を担当するツールという位置づけと考えられる。
EKANS はターゲットにより動作が異なるものがある。動作概要については、IPA J-CISP のレポートが参考になる。[11]

1.2. 被害発生にいたる攻撃の流れ

1.2 節では、サイバー攻撃から被害発生にいたるまでの流れを次の 2 つの局面に分けて解説する。1.2.1～1.2.4 までの攻撃の流れに冠しては事実詳細が公表されていないため、事象理解のため、IPA の知見に基づき推測した代表的な攻撃の流れを示す。

1.2.1【攻撃局面 A1（1）】攻撃者の侵入

攻撃者が、標的型攻撃メール等によって内部に侵入する。
同時に、侵入した PC にバックドアを設置し、インターネット上の C&C サーバとの通信を確立する。

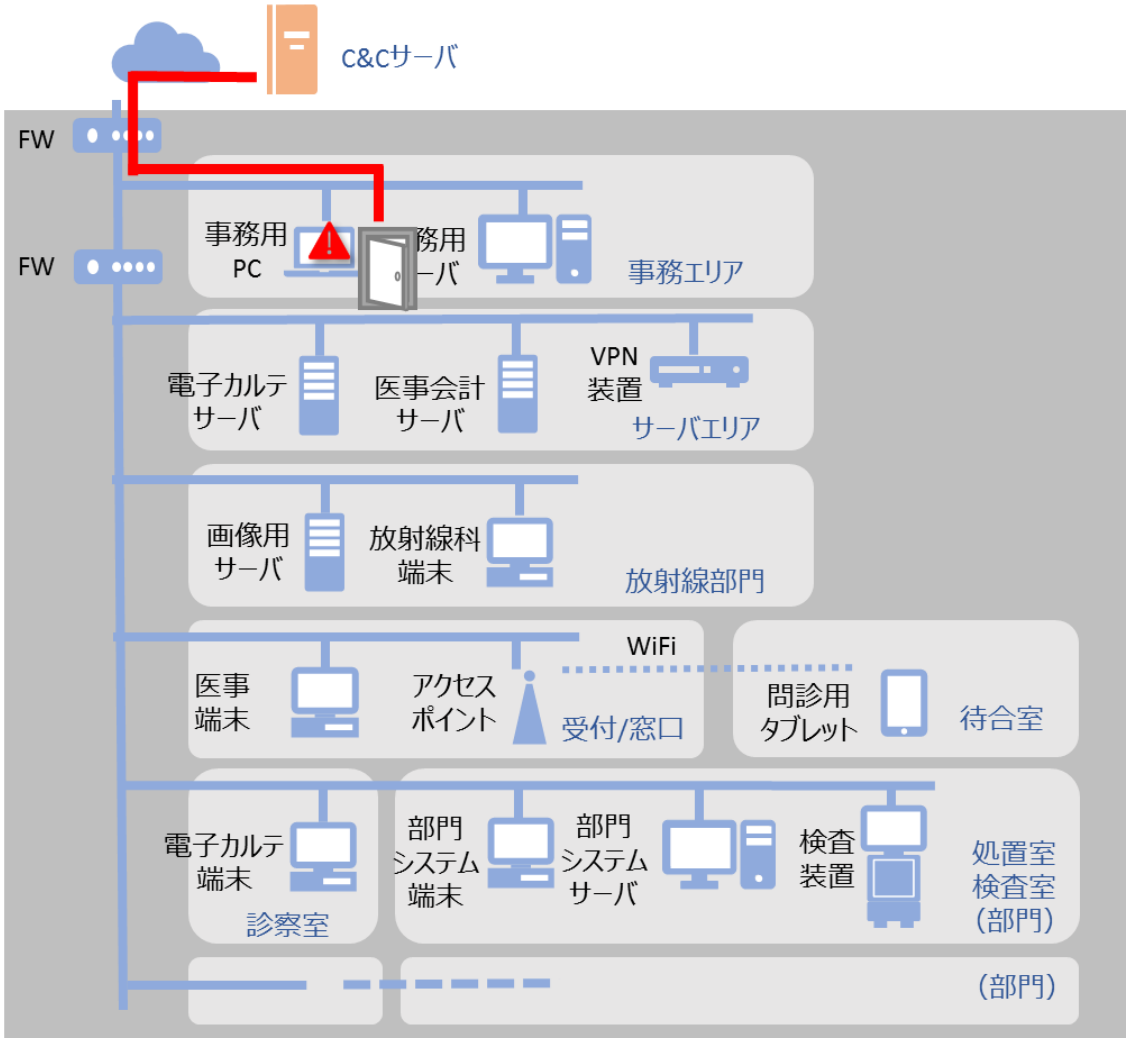


図 1-2 対象企業への侵入

1.2.2【攻撃局面 A1（2）】権限昇格による内部ネットワークの掌握

C&C サーバからの操作で各種のツールを利用しながら、標的のネットワーク内部を探索し事務用サーバ（＝ドメインコントローラ）の管理者権限を取得する。

＊以降の図では、事務用サーバ＝ドメインコントローラとしている

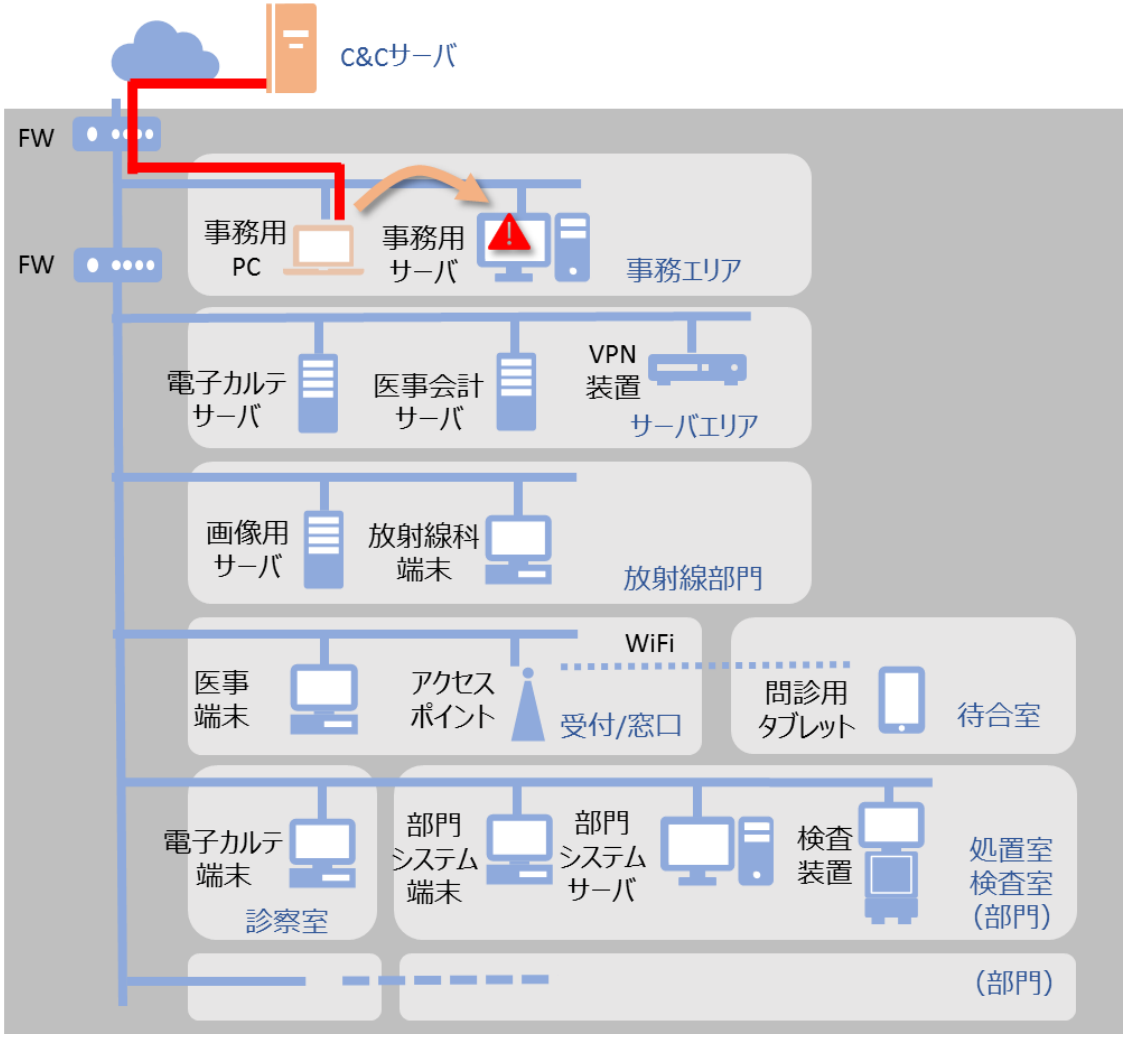


図 1-3 権限昇格による内部ネットワークの掌握

1.2.3【攻撃局面 A2】情報の窃取

電子カルテサーバの管理者権限を取得、電子カルテサーバにアクセスし、患者の個人情報を C&C サーバに送る。

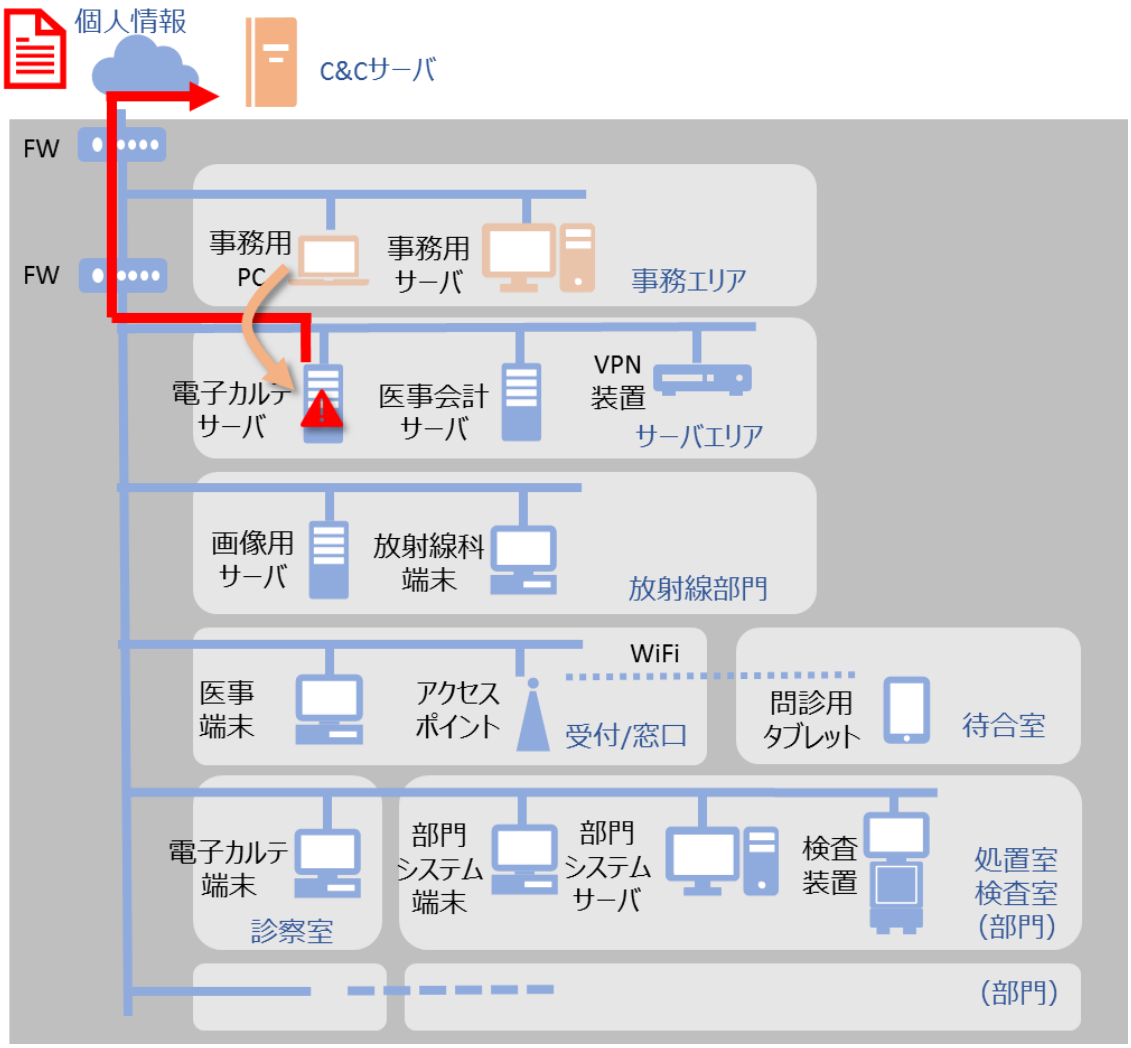


図 1-4 情報の窃取

1.2.4【攻撃局面 A3（1）】ランサムウェアの展開

ドメインコントローラの管理者権限を利用して、管理権限のあるコンピュータにランサムウェアを配布する[11]。

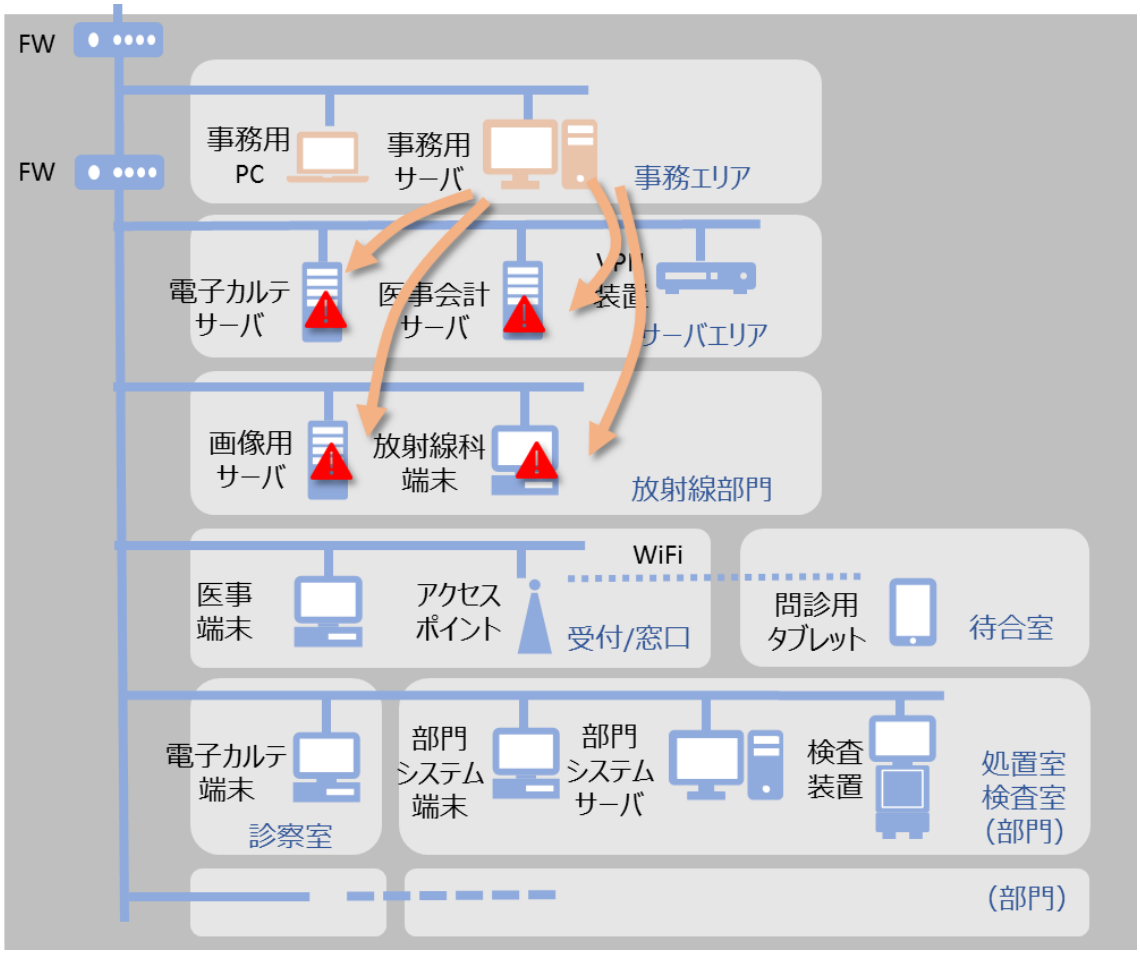


図 1-5 ランサムウェアのネットワーク内への配布

1.2.5【攻撃局面 A3（2）】プロセスの強制終了と暗号化

ランサムウェアを配布されたコンピュータでは、暗号化の妨げとなるアプリケーションが強制終了し[1]、データの暗号化が行われ、診療サービスが停止する。

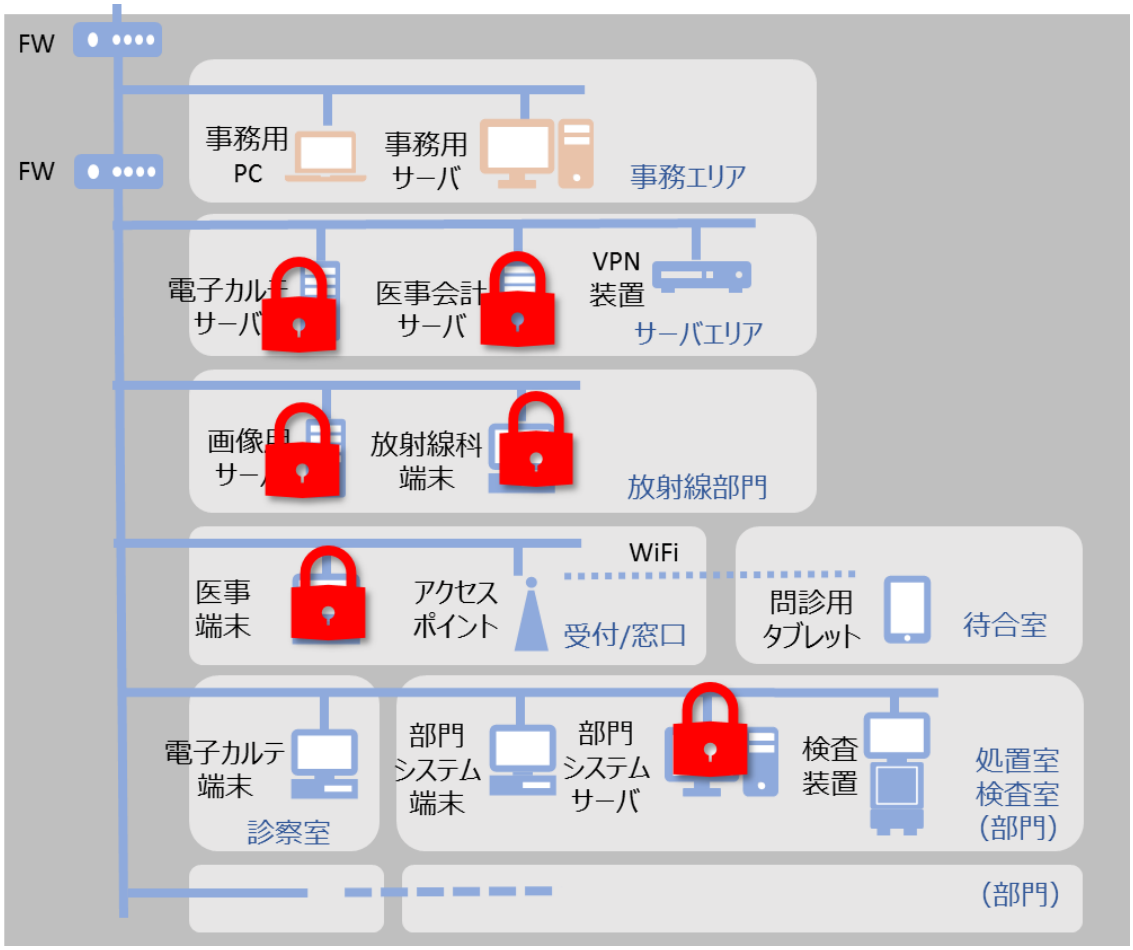


図 1-6 重要プロセスの強制終了とコンピュータの暗号化

2. リスク分析（事業被害ベース）の素材としてのインシデント情報の整理

2.1. 事業被害と攻撃シナリオの検討

本インシデントを参考に、検討した事業被害の例を表 2-1 に示す。
事業被害は2つあるため、項番 1,2 と分けて記載している。
2.2 節では、この事業被害と攻撃シナリオに至る攻撃ツリーを検討する。

表 2-1 事業被害の例（下線はリスク分析をする上での IPA による想定）

項番	事業被害			
1	患者の個人情報の漏えい			
	攻撃シナリオ	攻撃拠点	攻撃対象	最終攻撃
	患者のカルテのサーバが攻撃され保存してある個人情報が窃取される。	*事務用 PC*	*電子カルテサーバ*	電子カルテの窃取
2	診療サービスの停止			
	攻撃シナリオ	攻撃拠点	攻撃対象	最終攻撃
	診療サービスを支援するコンピュータが暗号化され業務が停止する。	全ての感染したコンピュータ	全ての感染したコンピュータ	感染したコンピュータの暗号化

また、事業被害に至る攻撃ルートの例を表 2-2 に示す。本表の項番は表 2-1 に対応している。

表 2-2 攻撃ルートの例（下線はリスク分析をする上での IPA による想定）

項番	誰が	どこから	どうやって	どこで		何をする
	攻撃者	侵入口	経由	攻撃拠点	攻撃対象	最終攻撃
1	悪意ある外部者	*事務用 PC*	*管理サーバの特権アカウントの利用*	*事務用 PC*	*電子カルテサーバ*	電子カルテの窃取
2	悪意ある外部者	*事務用 PC*	*管理サーバ（特権アカウント）*	全ての感染したコンピュータ	全ての感染したコンピュータ	暗号化

2.2. 攻撃ツリーの作成

今回のインシデント事例を、リスク分析における攻撃ツリー・ステップの枠組みにあてはめ整理した内容が表 2-3、表 2-4 となる。分析対象の範囲などによっては切り出し方のパターンは考えられるが、一例として参照いただきたい。

表 2-3 事業被害 1: 情報窃取の例

攻撃局面	攻撃ステップ項番	攻撃シナリオ 攻撃ツリー・ステップ ＜患者の個人情報の漏えい＞
【A1】	S1	侵入口= 事務用 PC 攻撃者が標的型攻撃メールによりイントラネットに侵入し、事務用 PC にバックドアを設置する
【A1】	S2	内部ネットワークを調査し、ドメインコントローラの管理者権限を取得する
【A2】	S3	電子カルテサーバの管理者権限取得し電子カルテサーバにアクセスする
【A2】	S4	電子カルテサーバから個人情報を抜き出し外部へ送信する

表 2-4 事業被害 2：診療サービスの停止の例

攻撃局面	攻撃ステップ項番	攻撃シナリオ 攻撃ツリー・ステップ ＜工場の操業を制御する役割のコンピュータが暗号化され操業停止となる。＞
【A1】	S1	侵入口= 事務用 PC 攻撃者が標的型攻撃メールによりイントラネットに侵入し、事務用 PC にバックドアを設置する
【A1】	S2	内部ネットワークを調査し、ドメインコントローラの管理者権限を取得する
【A3】	S5	ドメインコントローラの管理下のコンピュータにランサムウェアを配布し感染させる
【A3】	S6	各コンピュータでランサムウェアが起動され、ランサムウェア内に記述されているリストにあるプロセスを停止させる
【A3】	S7	ランサムウェアが各コンピュータ内のデータを暗号化し、業務が停止する。

2.3. 事業被害ベースのリスク分析の分析要素のまとめ

本インシデントをリスク分析の際の素材として活用するために、1.2 節で紹介した攻撃局面を分析ガイドで説明している事業被害ベースの分析要素毎にまとめた結果が表 2-5,表 2-6 となる。

表 2-5 各種情報をもとにした分析要素のまとめ（事業被害1）

分析要素		内容
攻撃用途		
	侵入口	事務用 PC
	攻撃対象	電子カルテサーバ
	攻撃拠点	事務用 PC
	経由	管理サーバの特権アカウントの利用
攻撃者		悪意ある外部者
事業被害		患者の個人情報の漏えい
攻撃シナリオ		患者の電子カルテが保存されているサーバに侵入され、保存してある個人情報が窃取される。
最終攻撃（目的）		機微情報の窃取
攻撃ルート		表 2-2 を参照
攻撃ツリー		表 2-4 を参照
攻撃手法		ネットワーク上のコンピュータのスキャンと特権昇格 データのコピー

表 2-6　各種情報をもとにした分析要素のまとめ（事業被害 2）

分析要素		内容
攻撃用途		
	侵入口	事務用 PC
	攻撃対象	全てのコンピュータ
	攻撃拠点	全てのコンピュータ
	経由	管理サーバ
攻撃者		悪意ある外部者
事業被害		診療サービスの操業停止
攻撃シナリオ		医療サービスを支援するコンピュータが暗号化され業務が停止する。
最終攻撃（目的）		コンピュータの暗号化
攻撃ルート		表 2-2 を参照
攻撃ツリー		表 2-3 を参照
攻撃手法		ネットワーク上のコンピュータのスキャンと特権昇格 ランサムウェアのコピー ランサムウェアによる暗号化

2.4. 対策・緩和策の整理

対策・緩和策の検討を進める上で、一般的なランサムウェアの観点からは、英国の国立サイバーセキュリティセンター（NCSC）の「Mitigating malware and ransomware attacks」[16]、CIS[4]から公開されている Security Primer – Ransomware[17]、標的型攻撃に関しては、IPA から公開された、「高度標的型攻撃」対策に向けたシステム設計ガイド[18]に記載されている緩和策等を参考にして、リスク分析作業に活用するための緩和策を整理した。表 2-7 は、代表的な対策・緩和策をまとめたものとなる。

表 2-7 代表的な対策・緩和策の例

項番	対策・緩和策
D1	電子メールのフィルタ[16][17][18]
D2	アンチウィルス、マクロ無効化などのマルウェア対策を行う[16][18]
D3	システムが最新のパッチで更新されていることを確認する[16]
D4	システムのバックアップを作成し、リストアの確認を行う[16][17]
D5	ファイル共有やリモートデスクトップのポートが不要であれば塞ぐ[17]
D6	ネットワークのセグメンテーションを行い、アクセス制御を適用する[18]
D7	パスワード、アカウントの強化[17]
D8	多要素認証の使用[16]
D9	インシデントレスポンスプランを策定し、トレーニングを行う[15][16]
D10	検知すべきイベントの特定と迅速な対応[15]

「D1. 電子メールのフィルタ」は、悪意あるメールやマクロ付のメールなどサイバー攻撃の起因となるようなメールを除去するという意味である。

「D2. アンチウィルス、マクロ無効化などのマルウェア対策を行う」は、マルウェアや悪意のあるマクロを動作させないようにするためのもので、既知のマルウェアを検出可能なシグネチャ型のアンチウィルスだけではなく、ふるまい検知型の導入など未知のマルウェアに対しても対策を講じることが望ましい。

「D3. システムが最新のパッチで更新されていることを確認する」は、脆弱性を利用したランサムウェアに対する一般的な対応策となる。

[4] Center for Internet Security https://www.cisecurity.org/

「D4. システムのバックアップを作成し、リストアの確認を行う」は、ランサムウェアによって暗号化された場合は、あらかじめバックアップしたデータからリストアするしか確実な対応策が無い。ランサムウェアによっては、共有フォルダや接続されたクラウド、外部記憶媒体のバックアップやボリュームシャドウコピー[5]を削除するものもあるため、バックアップデータをオフラインで保管するのが望ましい。また、定期的にバックアップが取得できているか、スムースにリストアできるかの確認も定期的に行う必要がある。

「D5. ファイル共有やリモートデスクトップのポートが不要であれば塞ぐ」は、リモートデスクトッププロトコル port3389、ファイル共有（SMB） port445 などのサービスを利用していないのであれば、ファイアウォールなどでマルウェアが利用できないように設定をしておく。

「D6. ネットワークのセグメンテーションを行い、アクセス制御を適用する」は、ネットワークの適切なセグメンテーション（VLAN 等）を行い、セグメント間に境界 FW を設置して必要最小限の通信のみ許可する事を意味する。

「D7. パスワード、アカウントの強化」は、推測しにくく十分に長いパスワードを使用、アカウントのロックアウトを検討するという意味である。

「D8. 多要素認証の使用」は、認証にパスワード以外の要素による認証システムを導入する事を意味している。

「D9. インシデントレスポンスプランを策定し、トレーニングを行う」は、緊急時にすぐに対応が可能となるようにすべきことをまとめ、組織の体制を構築し、日常から備えておくという意味である。

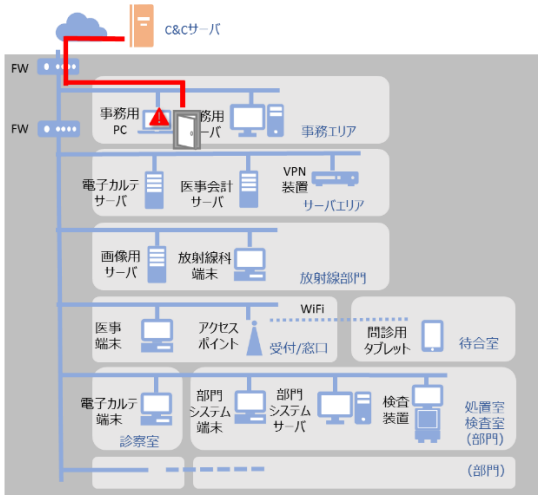
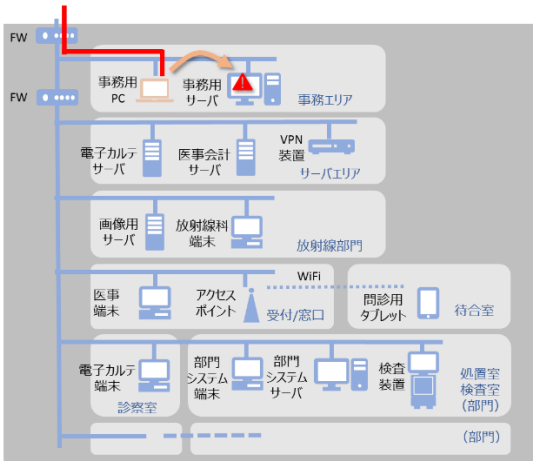
「D10. 検知すべきイベントの特定と迅速な対応」は、検知すべきイベント（意図していないアクセスや通信）を特定し、当該イベントを迅速に検知するためのシステム・手順・体制（手順書など）を構築するという意味である。

5 アプリケーションやシステムを稼働したままバックアップできる Windows の機能

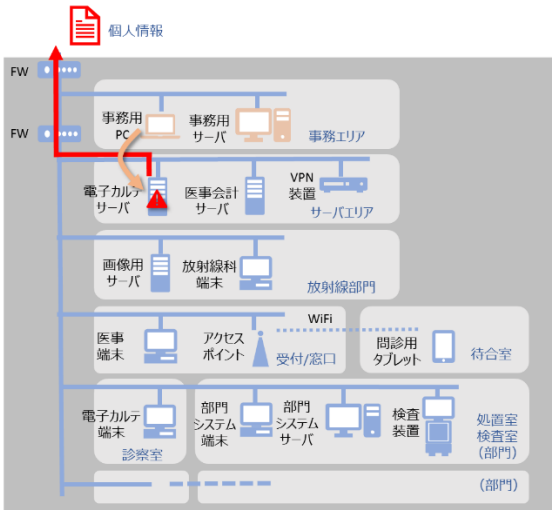
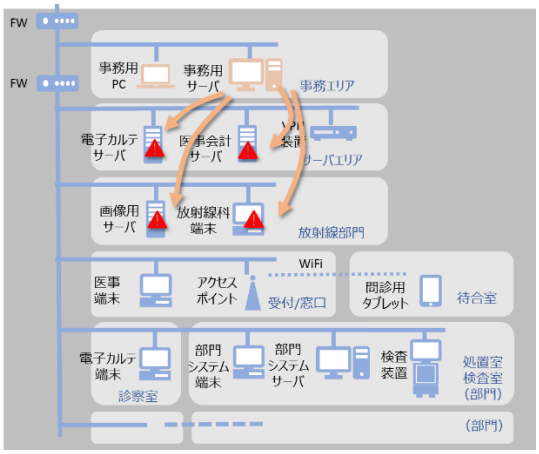
2.5. 攻撃ステップと対策・緩和策の関連付け

2.3 節までの情報をもとに、【攻撃局面 A1】や【攻撃局面 A2】と代表的な対策・緩和策を紐づけた例が表 2-となる。セキュリティ対策の基本である「多層防御」を考慮し、緩和策を立案することがポイントとなる。

表 2-8 制御システムにおける攻撃ステップと対策・緩和策の紐づけ例

攻撃局面	攻撃ステップ[6]	対策・緩和策	対象システム・資産
【攻撃局面 A1】 	[S1] 対象企業への侵入と攻撃のバックドア確保	電子メールのフィルタ[D1] アンチウィルス、マクロ無効化などのマルウェア対策を行う[D2] システムが最新のパッチで更新されていることを確認する[D3] パスワード、アカウントの強化[D7]	•事務用 PC
【攻撃局面 A1】 	[S2] 特権昇格とネットワークのスキャンと管理サーバへの侵入	システムが最新のパッチで更新されていることを確認する[D3] 不要ポートを塞ぐ[D5] ネットワークのセグメンテーションを行い、アクセス制御を適用する[D6] パスワード、アカウントの強化[D7] 多要素認証の使用[D8]	•事務用ネットワーク、管理サーバ(事務用サーバ)

6 [S]は表 2-3、表 2-4 の項番と対応。 [D]は表 2-7 の項番と対応。

攻撃局面	攻撃ステップ[7]	対策・緩和策	対象システム・資産
【攻撃局面 A2】 	[S3][S4] 電子カルテサーバへのアクセスとデータの窃取	・ネットワークのセグメンテーションを行い、アクセス制御を適用する[D6] ・多要素認証の使用[D8] ・インシデントレスポンスプランを策定し、トレーニングを行う[D9] ・検知すべきイベントの特定と迅速な対応[D10]	電子カルテサーバ
	[S5] [S6] [S7] ランサムウェアの配布とランサムウェアによる攻撃	・システムのバックアップを作成し、リストアの確認を行う[D4] ・インシデントレスポンスプランを策定し、トレーニングを行う[D9] ・検知すべきイベントの特定と迅速な対応[D10]	各種コンピュータ、診療装置等

[7] [S]は表 2-3、表 2-4 の項番と対応。 [D]は表 2-7 の項番と対応。

【補足説明】

すでに暗号化されてしまったケースへの対応は、一部のランサムウェアに対してではあるが、ID Ransomware[19]、No More Ransom Project[20] 等のランサムウェアデータベースサイトでランサムウェアの特定や暗号化の解除キー（復号キー）を提供しており、本解除キーが使えるケースもあり得る。

おわりに

本資料では、制御システムにおけるインシデント事例を紹介すると共に、セキュリティリスクアセスメントへの活用方法について一つのアプローチを紹介した。

事業被害ベースのリスク分析においては、自社の制御システムにとって回避すべき事業被害を明確化し、被害に至る攻撃シナリオと攻撃ルートを漏れなく洗い出すことが重要である。攻撃シナリオは、過去に発生した制御システムのインシデント事例を含む各種の公開情報を参考にしつつ、自社の制御システムに生じ得る脅威とその影響を検討するが、具体的な攻撃ルート・攻撃手順を想定することで、セキュリティ対策を効率的に進めることが可能となる。

本資料が各社の制御システムのセキュリティ向上に活用されることを期待する。

参考資料

[1] [DRAGOS] EKANS Ransomware and ICS Operations
https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/

[2] [SECURITY WEEK] New Snake Ransomware Targets ICS Processes
https://www.securityweek.com/new-snake-ransomware-targets-ics-process

[3] [BBC] ホンダにサイバー攻撃　海外工場で操業停止も
https://www.bbc.com/japanese/52989059

[4] [SC] Snake ransomware attack hits power company Enel Group
https://www.scmagazineuk.com/snake-ransomware-attack-hits-power-company-enel-group/article/1686199

[5] [Mitre ATT&CK] Turla
https://attack.mitre.org/groups/G0010/

[6] FRESENUS SE &KGaA
https://www.fresenius.com/

[7] [FRESENIUS] Fresenius Medical Care confirms illegal publication of patient data in Serbia subsequent to recent hacker attack
https://www.fresenius.com/8307

[8] [KrebsonSecurity] Europe's Largest Private Hospital Operator Fresenius Hit by Ransomware
https://krebsonsecurity.com/2020/05/europes-largest-private-hospital-operator-fresenius-hit-by-ransomware/

[9] Legemiddelfabrikk rammet av datavirus – får følger i Halden
https://www.digi.no/artikler/legemiddelfabrikk-rammet-av-datavirus-far-folger-i-halden/491475

[10] [Malware Hunter Team]
https://twitter.com/malwrhunterteam/status/1258080951101468673

[11] [IPA] サイバー情報共有イニシアティブ(J-CSIP) 運用状況 [2020 年 4 月～6 月]
【付録】EKANS ランサムウェアの解析事例
https://www.ipa.go.jp/files/000084401.pdf

[12] [経済産業省] 医療情報を取り扱う情報システム・サービスの 提供事業者における安全管理ガイドライン (案)
https://www.meti.go.jp/press/2019/03/20200305001/20200305001-2.pdf

[13] [US-CERT] APT Groups Target Healthcare and Essential Services
https://www.us-cert.gov/ncas/alerts/AA20126A

[14] [IPA] 事業継続を脅かす新たなランサムウェア攻撃について
https://www.ipa.go.jp/files/000084974.pdf

[15] [IPA]「制御システム関連のサイバーインシデント事例 5」
https://www.ipa.go.jp/files/000080702.pdf

[16] [NCSC] Mitigating malware and ransomware attacks
https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

[17] [CIS] Security Primer – Ransomware
https://www.cisecurity.org/white-papers/security-primer-ransomware/

[18] [IPA]「高度標的型攻撃」対策に向けたシステム設計ガイド
https://www.ipa.go.jp/files/000046236.pdf

[19] ID Ransomware
https://id-ransomware.malwarehunterteam.com/

[20] No More Ransom Project
https://www.nomoreransom.org/ja/index.html

更 新 履 歴

2020 年 9 月 8 日	初版	ー

制御システムのセキュリティリスク分析ガイド補足資料

制御システム関連のサイバーインシデント事例 7

～2020 年 医療関連企業のランサムウェアによる操業停止～

[発　　行]　2020 年 9 月 8 日　第 1 版

[著作・制作]　独立行政法人情報処理推進機構　セキュリティセンター
編集責任　辻　宏郷
執筆者　福原　聡
協力者　桑名　利幸　木下　仁　高見　穣　小助川　重仁