令和6年度医療情報セキュリティ研修 及び
サイバーセキュリティインシデント発生時初動対応支援・調査等事業

# 【システム・セキュリティ管理者向け研修】
# 新規Bコース
# ～ インシデント対応 初動・封じ込め編 ～


**大阪大学　D3センター　教授　CISO**
**猪俣　敦夫**
**Ph.D, RISS, CISSP**


## 自己紹介（いのまたあつお）

**大阪大学　教授**

**D3センター、大学院情報科学研究科**

**情報セキュリティ対策室室長, OU-CSIRT隊長**

- (一社)　公衆無線LAN認証管理機構　代表理事
- (一社)　ライフデータイニシアティブ(LDI)　理事
- (一社)　大学ICT協議会（AXIES）理事
- (一社)　JPCERTコーディネーションセンター　理事
- 京都女子大学、東京薬科大学、慶應義塾大学、NAIST、東京電機大学　他
- 経済産業省　ソフトウェアセキュリティTF委員
- 総務省　公衆無線LANセキュリティ委員会座長
- 2025大阪・関西万博サイバーセキュリティ有識者会議委員
- (株)カプコン　セキュリティ監督委員
- 阪急阪神HD (株)　サイバーセキュリティ顧問
- (株)ベネッセHD　情報セキュリティ監視委員
- NEXCO東日本・中日本・西日本　ETC開発委員、　他多数
- IPA 情報処理安全確保支援士　特定講習講師
- 大阪府警、奈良県警察サイバーセキュリティアドバイザ
- NTT西日本情報漏洩事案内部調査委員会 委員
- 大阪急性期・総合医療センターインシデント調査委員会委員長、他

## 「災害リスク」と「ITリスク」の違いに気づこう

- 事業継続計画（BCP：Business Continuity Plan）
  - テロや災害、システム障害等危機的状況下においても重要な業務が継続できる方策を予め準備しておき、かつその実行に移せる計画のこと
  - その中でも特に情報システム・サービスに関係するのがIT-BCP

- 災害リスク
  - 地震等の発動タイミングは災害発生とほぼ同時→即座に認識、初動へ
- ITリスク
  - 攻撃の種類によってはインシデントの認知が同時に起きるわけではない、暫くしてから気づくパターンや外部からの通報で漸く気づくことが多い

## IT-BCPの難しさ

災害リスクと比較してITリスクはインシデントからの復旧フローを策定しにくい、これはなぜでしょう？

- 発生に気付かない可能性
- BCP発動の判断が困難
- 代替機を使用してデータ復旧するだけでは、再度被害にあう可能性
- 原因を特定しないと容易に復旧出来ない

だからこそ平時からの備え、訓練が大事

# IT-BCPのための「初動」と「封じ込め」

実際にインシデントが発生したら？ということを想定した備えを平時から検討しておこう

1. 体制
2. 対処
3. 初期調査
4. 外部への対応
5. 分析

## 1. 体制

# IT-BCP対策本部

安全管理責任者をとしたIT-BCP 対策本部を設置し、役割分担及び情報共有に基づき

- 方針の決定
- 対策の実施
- フィードバック

により、医療の継続と早期復旧を目指す

- 大規模な病院の場合、医療継続対応の災害対策本部とIT復旧対応のチームが連携しながら相互に情報共有

# IT復旧チームのクロノロ収集

- 初期感染時の事象が確認されたコンピュータ（端末名（ホスト名）、 アドレス、役割）に対する機器の現況
  - 暗号化状況、ランサムノート、ファイル拡張子等、スマホによるスクリーン撮影と実施した作業があればその内容等、確認時刻、確認者名を添えて ITシステム復旧を実施しているチームに報告
- ランサム事案では、同様の症状が多数確認されることも多い
  - 特にサーバーおよびバックアップを中心に調査し、コンピュータ名、IP アドレス等、攻撃範囲の把握を進めること

朝日新聞デジタル 2022/10/31より
大阪急性期・総合医療センターでのクロノロジー事例

# 2. 対処



## バックアップシステムのLAN抜線 FIREWALL, VPN等外部接続点の遮断

- 優先度の高い LAN ケーブル、光ファイバーケーブルに順位タグ等を明示
  - 定期的に管理者とともにサーバールームでどのLANケーブル、光ファイバーケーブルが重要であるのかを確認すること

## 全サーバーセグメントの遮断 、全サーバーのLAN抜線
## クライアントセグメントの遮断

- コアスイッチのサーバーセグメントの LAN ケーブルを抜線
- コアスイッチのクライアントセグメントの LAN ケーブルを抜線
- 優先度の高い LAN ケーブル、光ファイバーケーブルに順位タグ等を明示
  - 定期的に管理者とともにサーバールームでどれがサーバーないしクライアントのセグメントであるのかを確認することが重要

## 全クライアントのLAN抜線及び初期保全

- クライアントの LAN ケーブルないし光ファイバーケーブルの抜線、及びコンピューターウイルス対策ソフトの稼働をさせず保全するよう平時から職員に対しての周知
  - 定期的にセキュリティ研修で伝えることが大切
- 館内放送などインシデント発生時のアナウンスについて検討
  - インシデント発生時には電子メールをはじめ全ての情報システム・サービスが利用できなくなることを改めて認識すること

# 3. 初期調査



## SYSLOGサーバーの保全

- syslog サーバーで収集しているsyslogを書き換え不能なメディア(CDRやBD等）に定期的にバックアップを実施
  - USBメモリやハードディスクなどへのバックアップは、攻撃者によって削除されるリスクもある、ということを認識しておくこと

## 脅威情報の収集

- ランサム事案の場合、ランサムノートなど脅迫状に記載された情報、ウイルスによって出力されたメッセージ等から、脅威情報を収集し関係者に共有
  - なお、脅威情報の調査に当たっては攻撃を受けたネットワークとは完全に別のネットワークから実施すること
- 侵入手口、復号化の可能性、使用するツール、ウイルスの傾向と、リークされたサイトの存在可能性、窃取された情報の公開に対する脅迫もありうるため、状況の公開には留意すること
  - 安易に全ての情報を公開することが攻撃者にとって都合の良いことにもなるため、その対応には関係者で綿密に検討すること

## ファーストフォレンジック

Windowsサーバーやドメインコントローラーのセキュリティログから

- Event ID 4624ログオン成功
- Event ID 4625 ログオン失敗
- Event ID 4776 NTLM 認証
- Event ID4672 特権割り当て

等、RDP 関連のログ、ないしsyslogサーバーのsyslogから外部とのSMB、RDP、HTTP、HTTPS、SSH、TELNET、FTP 等の異常と思われる記録を検索

# 4. 外部への対応



## ステークホルダーへの連絡、広報体制の確立

- 緊急連絡網を作成し、年に1回以上は電話番号等の更新を実施
  - なお、緊急連絡網に個人情報を記載する場合には取り扱いに留意すること
- 平時にてプレスリリースの様式を整えておき、メディア等の連絡先を取得しておくと良い
  - 情報公開という視点でもあるが、患者へのコンタクト手段が失われた際にメディアは周知方法の1つにもなりうる

## 被害範囲の特定

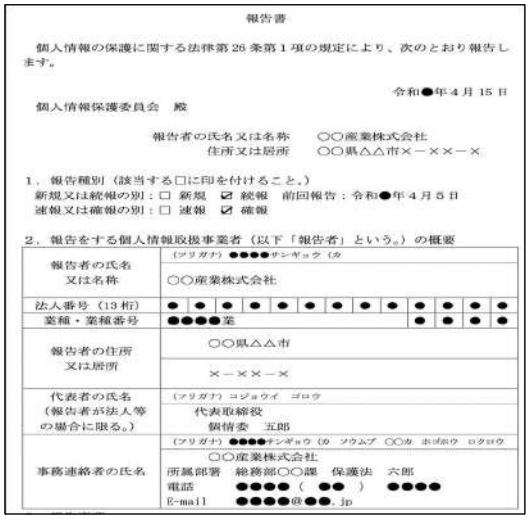
- 攻撃者によって暗号化されたと思われる判断
  - 拡張子が変更されている
  - 脅迫状（ランサムノート）が表示されている
- 侵入後、攻撃者によってバックドアが設置されることも多く、管理者権限やBuilt-In Administrator（OS標準のID）のパスワードが共通化されている場合、特に、ルーター、ファイアウォールのsyslog等の証跡を確認する。なお、syslogで確認できない場合には全数被害を前提に検討したほうが良い
  - ビルトインアカウントであるadministratorの管理が適切になされているかどうか今一度確認すること

## 攻撃グループの特定

- 個人情報漏洩の有無により、個人情報保護委員会への報告等、その後の対応が大きく変わるため、医療継続を最優先とした上で攻撃グループの特定調査を開始し、情報漏洩や２重脅迫などの傾向を把握するのが望ましい
  - フォレンジック専門の業者が多くの知見を有していることから、サポートを得ることも選択肢の一つにするのも良い
- 脆弱性を持つOSのバージョン及びアプリケーション、VPN機器など可能性として考えられる侵入経路を早期に特定を目指す
  - 脆弱性を明確にできなければ再度侵入される危険性は高いものと考えたほうが良い

# 情報漏洩の調査及び個人情報保護委員会への報告書提出

- 地方独立行政法人における、要配慮個人情報が含まれる保有個人情報の漏えい等（又はその恐れ）については、速報（新規：発覚日から3～5日以内）と確報（続報：発覚日から30日以内、不正な目的で行われた恐れがある場合は発覚日から60日以内）の提出
- 報告書書式
  - https://www.ppc.go.jp/personalinfo/legal/leakAction/



報告書

個人情報の保護に関する法律第 26 条第１項の規定により、次のとおり報告します。

令和●年４月 15 日

個人情報保護委員会　殿

報告者の氏名又は名称　○○産業株式会社
住所又は居所　○○県△△市×－××－×

１．報告種別（該当する□に印を付けること。）
新規又は続報の別：□ 新規　☑ 続報　前回報告：令和●年４月５日
速報又は確報の別：□ 速報　☑ 確報

２．報告をする個人情報取扱事業者（以下「報告者」という。）の概要

| | |
|---|---|
| 報告者の氏名又は名称 | （フリガナ）●●●●サンギョウ（カ<br>○○産業株式会社 |
| 法人番号（13 桁） | ● ● ● ● ● ● ● ● ● ● ● ● ● |
| 業種・業種番号 | ●●●●業 ● ● ● ● |
| 報告者の住所又は居所 | ○○県△△市<br>×－××－× |
| 代表者の氏名（報告者が法人等の場合に限る。） | （フリガナ）コジョウイ　ゴロウ<br>代表取締役<br>個情委　五郎 |
| 事務連絡者の氏名 | （フリガナ）●●●●チンギョウ（カ　ソウムブ　○○カ　ホゴホウ　ロクロウ<br>○○産業株式会社<br>所属部署　総務部○○課　保護法　六郎<br>電話　●●●●（　●●　）　●●●●<br>E-mail　●●●●@●●．jp |

# 厚生労働省への報告書提出

- 「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）場合等の際には、厚生労働省等の所管省庁への連絡も必要

- 厚生労働省連絡先
- 医政局特定医薬品開発支援・医療情報担当参事官室
- TEL:　03-6812-7837
- MAIL:　igishitsu@mhlw.go.jp

- 厚生労働省のHPも適宜確認しておくと良いでしょう
- https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html

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

医療機関等がサイバー攻撃を受けた際の厚生労働省連絡先

サイバー攻撃等により個人情報等が漏洩したおそれが発生した場合

# 5. 分析

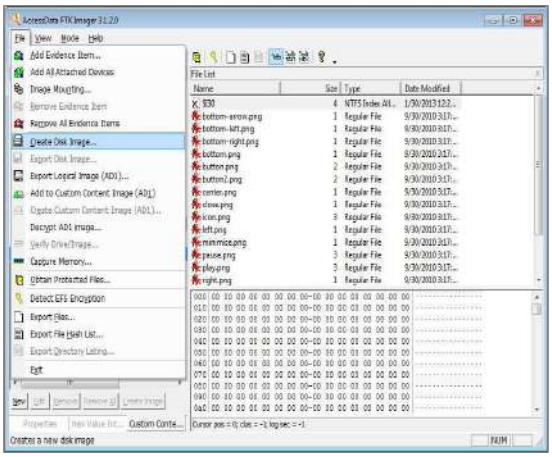


## すべての資格情報のリセット

- あくまでも平時からBuilt-In Administrator(ビルトインされている特権ユーザー）のパスワードについては個々のシステムごとに設定されているか確認しておく必要があるが、もしインシデントが発生した場合には分析においてパスワード設定の再確認が重要
  - 同一パスワードを用いていて攻撃者に全て乗っ取られた事案が多数
- 桁数は長ければ長いほど良い
  - パスワードの定期変更は不要
- 多要素認証など二要素認証の実施
  - 攻撃者によってパスワードがもし破られたとしても、さらに別の認証が提供されていることで侵入が非常に困難になる

# 保全

- exterro社FTK Imager Liteを使用し、被害を受けたPCの保全を実行
  - FTK Imager Liteはインストール不要で外付けSSD等から起動可能
- サーバーのハードディスクサイズ以上の保全用ハードディスクが必要
  - FTK Imagerでは、1TByteあたり4時間程度かかるため保全対象を慎重に選択
- FTK Imager：
- https://www.exterro.com/ftk-imager



# フォレンジック調査

- **フォレンジック調査費用は年々上昇傾向であり、現在ではPC1 台あたり100 万円以上**、サーバーは数百万円かかる場合がある
  - リスク移転を前提に、サイバーセキュリティ損害保険の加入により、フォレンジック費用を保険でカバーできることも多い

# 侵入経路の特定

- VPN装置、ネットワーク機器、電子メール、記憶媒体等の侵入経路を特定
  - ドメインコントローラなど重要なサーバーとの経路を持つ箇所など
- 脆弱性・設定ミスの悪用、脆弱な実装・運用、全体として脆弱箇所を抽出
  - 基幹ルーターなど運用上アップデートが困難な箇所が存在していないかを再度確認すること
- 要求仕様や仕様書での検討不足やセキュアコーディングの欠落、ハードニング（堅牢化）の未適用などの、上流工程におけるセキュリティ仕様の不備の洗い出し
  - セキュリティバイデザインとも呼ばれる

# サイバー攻撃への対応事例

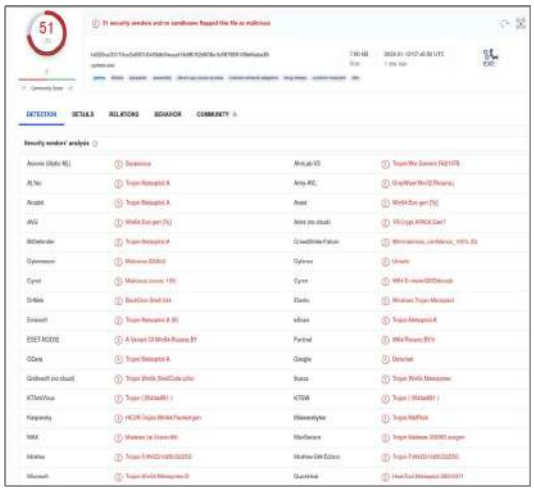
- 攻撃テクニックや要素技術を分析し、攻撃（脅威）ベクトル（侵入・攻撃方法）を作成し、再感染の防止や攻撃の局所化のための設定等を検討
  - BIOS、UEFI（システムのブート部分）の確認
  - ウイルス等不正プログラムのAuto Run（自動起動）の削除
  - 最新ウイルス対策ソフトのパターンの配布方法
- 再利用禁止ファイル、再利用許可ファイルの一覧の作成
  - 再利用禁止：.exe .dll
  - 目視確認条件付き再利用許可：.txt .bat
- PowerShell、Windowsスクリプトホストの停止
  - PowerShellを悪用した事案が多いことから不要であれば停止も検討
- PowerShell使用においてはログ取得は必須
- RDPを使用するのであればポート変更なども検討

# 検討すべき対応策

- ロックアウト設定および UAC（ユーザアカウント制御）の実施
  - 管理者権限の厳格な限定使用
- Built-In Administratorのパスワードのユニーク化と十分な長さの確保
- アプリケーション自動起動の停止
  - 再起動しても再度繰り返されるリスク
- Remote Registry、Win-RMの停止
  - リモートでのレジストリ編集をはじめリモート管理はリスクになりやすい
- DB 再利用の方針
  - データベース再構築はコストも時間もかかることからどのように復旧させるべきか、平時にベンダーと検討を進めておくことが望ましい
- パスワードの変更記録
  - ログを参照し、変更が記録されているかシステム完全性を担保すること

# 検体の取得と情報収集

- BIOS・UEFIリスク
  - Windows OSより先にBIOS、UEFI起動によりウイルスが動作開始するため、単なる初期化だけでは再感染する恐れが生じることもある
  - この場合、復旧手順にBIOS、UEFIの初期化が必要。検体が取得出来たら検体の性質、特徴を早期に把握すること
- Virus Totalにて検体に対応するウイルス対策ソフトの情報を取得するのが望ましい
- 特に、ほぼ同一の名称である場合においても同じウイルスとして認識するのではなく、ハッシュ値が異なれば同種ウイルスの亜種が存在していたことに注意すること



# コンピューターウイルス対策ソフトのパターン作成

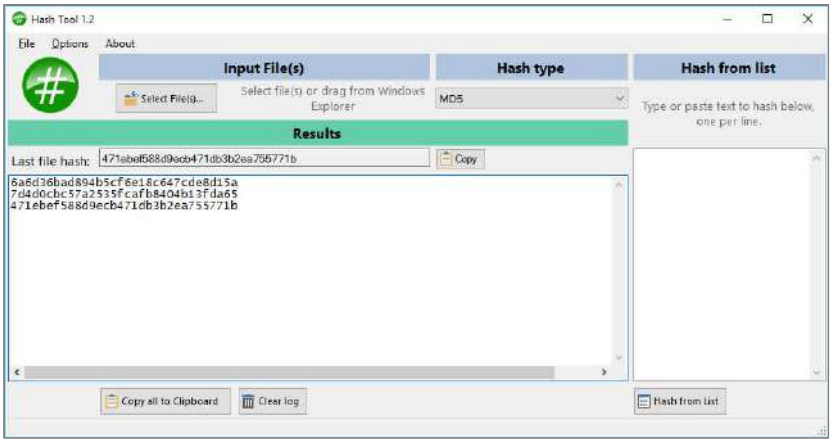
- ウイルス対策ソフトが検体を削除しないように、USBメモリのドライブを除外設定した上で検体をUSBメモリ等の可搬ストレージに保管
  - 稼働するストレージには検体をコピーしないこと
- 検体のHash値をHash Tool等を用いて取得し、Virus Totalサイトにてウイルス対策ベンダー対応等の検索、調査を実施
  - 検体を直接アップロードする方法もあるが、セキュリティコミュニティとの共有に同意したこととなるため、個人情報が含まれている場合なども含め情報漏洩リスクの観点からアップロードは実施しないこと
- ウイルス対策ソフトベンダーが検体に対して未対応の場合、ベンダーに検体を送ることも望ましい
  - 検体アップロードの際には注意しながら実施すること

# コンピューターウイルス対策ソフトのパターン作成

- Virus Total：
- https://www.virustotal.com/gui/home/search

# コンピューターウイルス対策ソフトのパターン作成

- Hash Tool：
- https://apps.microsoft.com/detail/9NBLGGH4RRR2?hl=ja-JP&gl=US




# コンピューターウイルス対策ソフトのパターン作成

- Microsoft Defender 検体提出先：
- https://www.microsoft.com/en-us/wdsi/filesubmission

## おわりに



サイバー攻撃は決して他人事ではない

自分たちの組織でも起こることを前提とした
備えがとても大事

今あなたの周りに何人相談出来る人はいますか？

# ありがとうございました。