サイバーセキュリティ対応の基礎

日本医療情報学会
研修企画委員会

福井大学 University of Fukui

本セミナーでの目的

- 医療機関におけるサイバーセキュリティ対応をする必要がある。
- 医療情報システムに関するガイドラインにあるようにリスク把握するにも、費用がかかる・・・・
- 重要インフラとしての対応として放置できない
- 最低限自らでできることはないのか？

福井大学 University of Fukui

医療系でのセキュリティ問題

- ウイルス感染が広がって端末が利用不能
- ウイルスによる内部サーバへの攻撃
- 電子カルテのデータが乗っ取られた
  - ファイルの暗号化ロックによる使用不能
  - 身代金の要求
  - バックアップも使用不能・戻せない
- 部門システムのデータが乗っ取られた

福井大学 University of Fukui

セキュリティ対策の背景

- 医療情報システムとの密接な連携
  - ネットワーク経由の連携拡大
- リモートメンテナンス等外部接続の増加
- 医療情報システムと外部との関わりの拡大
- クローズドなネットワークが安全とは言い切れない現実
- 意図しない状況からのサイバー攻撃の可能性

福井大学 University of Fukui

背景として

- 医療機関へのサイバー攻撃で実際に被害
  - インターネット経由だけでないことが盲点
- インターネット接続がない筈であるが、リモートメンテナンスはインターネット経由
  - いわゆる管理されていないバックドアがある
  - VPNとはいえVPNルータが管理されている？
    - VPNのファームウエアが古いままで攻撃対象に
- 非常時の運用対応と準備

福井大学 University of Fukui

医療機関への攻撃？

- 政府機関や大手企業への攻撃と同じか？
  - 実は、直接の対象になっているものではない
  - たまたま、外部との接続の機器の脆弱性が狙われた
    - VPN装置の脆弱性から侵入
  - 外部との閉域と思われた接続ネットワークから侵入
  - USBメモリーなどの媒体や持ち込みPCなどから侵入

現段階では直接攻撃よりは、弱点から侵入型が多い
「たまたま」であるが、今後は狙い撃ちにも警戒すべき

福井大学 University of Fukui

サイバー攻撃に対する課題

- 病院は外部と繋がっていないと信じられている
- ランサムウエアによる被害が拡大
  - 侵入経路が想定外
  - 被害拡大に十分なブロックができなかった
  - 復旧方法に盲点があった
- ガイドラインにあるリスク評価
  - インターネット接続がないという過信と未評価
  - ウイルス対策だけでは100%ではない
- 重要インフラとしてのBCP対応

福井大学 University of Fukui

診療報酬改定（案）に含まれるサイバー攻撃対応

改　定　案	現　　行
【診療録管理体制加算】 ［施設基準］ 1　診療録管理体制加算１に関する施設基準 (1)　(略) (2) 中央病歴管理室が設置されており、厚生労働省「医療情報システムの安全管理に関するガイドライン」に準拠した体制であること。 (3)～(9)　(略) (10) 許可病床数が400床以上の保険医療機関については、厚生労働省「医療情報システムの安全管理に関するガイドライン」に基づき、専任の医療情報システム安全管理責任者を配置すること。また、当該責任者は、職員を対象として、少なくとも年１回程度、定期的に必要な情報セキュリティに関する研修を行っていること。さらに、非常時に備えた医療情報システムのバックアップ体制を確保することが望ましい。ただし、令和４年３月31日において、現に当該加算に係る届出を行っている保険医療機関（許可病床数が400床以上のものに限る。）については、令和５年３月31日までの間、当該基準を満たしているものとみなす。 2　診療録管理体制加算２に関する施設基準 (1)　１の(1)から(4)まで、(9)及び(10)を満たしていること。 (2)～(5)　(略) 3　届出に関する事項 (1) 診療録管理体制加算の施設基準に係る届出は、別添７の様式17を用いること。 (2) 毎年７月において、医療情報システムのバックアップ体制の確保状況等について、別添７の様式により届け出ること。	【診療録管理体制加算】 ［施設基準］ 1　診療録管理体制加算１に関する施設基準 (1)　(略) (2) 中央病歴管理室が設置されており、「医療情報システムの安全管理に関するガイドライン」（平成29年５月厚生労働省）（以下、「医療情報システムの安全管理に関するガイドライン」という。）に準拠した体制であること。 (3)～(9)　(略) （新設） 2　診療録管理体制加算２に関する施設基準 (1)　１の(1)から(4)まで及び(9)を満たしていること。 (2)～(5)　(略) 3　届出に関する事項 診療録管理体制加算の施設基準に係る届出は、別添７の様式17を用いること。

ここにはバックアップへの対応と
研修の強化が入っている

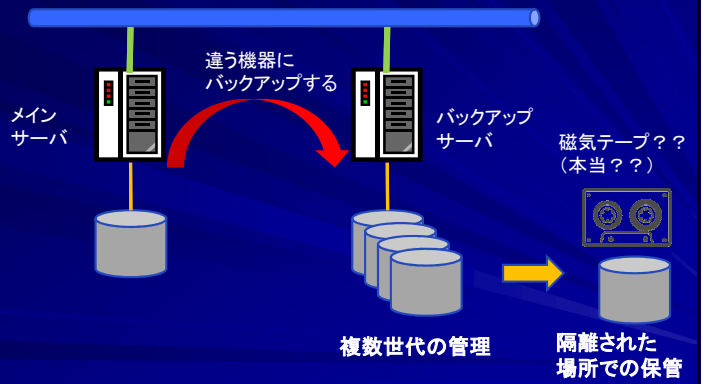
福井大学 University of Fukui

なぜバックアップか？

- 元に戻す唯一の方策
  - 滅多になくてもやはり必要
- ランサムウエアやウイルス対策だけでなく、システムのBCP対応としても重要
  - サイバー攻撃のためだけではない
  - 災害等非常時対応として考える

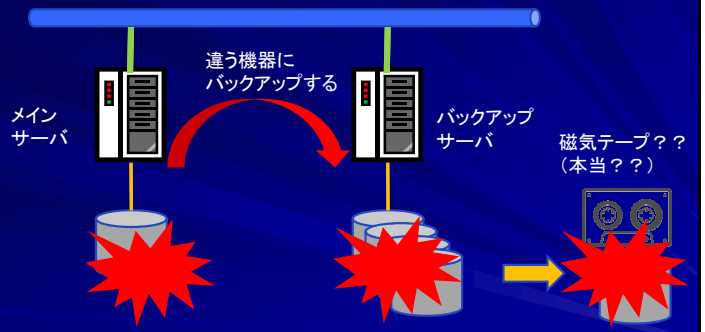
福井大学 University of Fukui

バックアップに求められるもの



福井大学 University of Fukui

バックアップもやられた（連鎖した）



福井大学 University of Fukui

セキュリティ対策がなぜ重要か？

- 医療情報システムとの密接な連携
  - ネットワーク経由の連携拡大
- リモートメンテナンス等外部接続の増加
- 医療情報システムと外部機関等との関わりの拡大
- クローズドなネットワークが安全とは言い切れない現実
- 意図しない状況からのサイバー攻撃の可能性

福井大学 University of Fukui

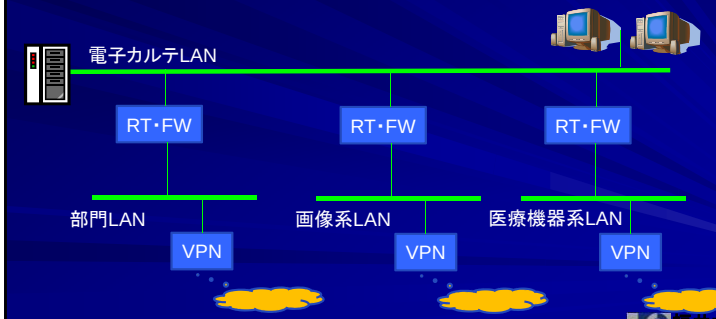
なぜVPN？？

- VPNは安全
  - 通信の暗号化が前提なので、データ保護としては有効
- しかし、VPN装置の穴が狙われている
  - 家庭用ルータでも問題になったことと同じ
  - 最新のバージョンに更新しているか？
    - 内部のソフトウエアの脆弱性を狙われる
  - ユーザー情報を装置に保持？？

福井大学 University of Fukui

リモートメンテのバックドア問題

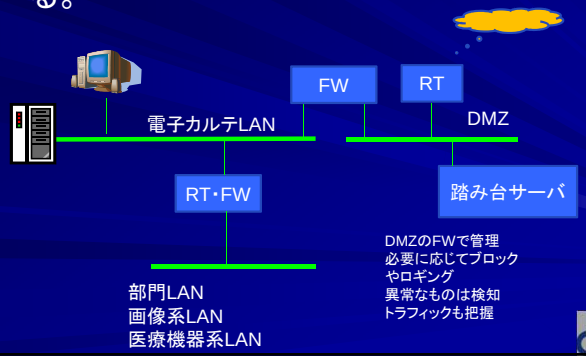
- リモートメンテ用に個別に回線を引いている
  - 部門のLANに接続されている



福井大学 University of Fukui

リモートメンテをまとめて管理

- リモートメンテの入口を1か所にまとめたり、踏み台サーバ経由でないと入れないようにする。



福井大学 University of Fukui

医療情報システムや医療機器システムでの課題

福井大学 University of Fukui

医療系システムで必要なこと

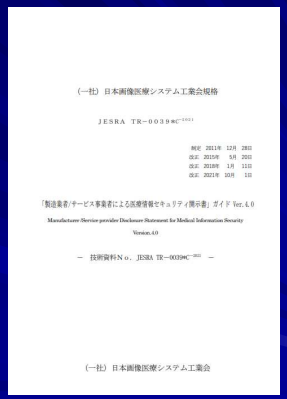
- OSのセキュリティパッチ
- アプリケーションや利用コンポーネントにおける脆弱性への対応
- システムとしての脆弱性の確認
- 継続的な脆弱性への対応
- ベンダーから運用に関わる内容への告知

福井大学 University of Fukui

でも、現状をどう把握する

- 専門家に依頼するには時間もかかるし・・・
- できることだけでもしてっみよう！

福井大学 University of Fukui



福井大学 University of Fukui

「製造業者/サービス事業者による医療情報セキュリティ開示書」（MDS/SDS）の入手と利用

医療機関等は製造業者/サービス事業者に対し、医療機器を含む対象とするシステム/サービス毎にMDS/SDSを要求し入手してください。対象とするシステム/サービスのMDS/SDSが未作成の場合は、作成するよう要求してください。

医療機関等は「安全管理ガイドライン」の遵守が求められており、医療機関等全体としては医療機関等が主体となって、医療情報システムの製造業者/サービス事業者の協力を受けつつ、安全管理ガイドラインに則って機密性・完全性・可用性を確保するために対象とするシステム/サービスの安全管理を行う必要があります。

一方、医療機器に関しては、薬機法における製造販売業者が厚生労働省通知「医療機器におけるサイバーセキュリティの確保について」に則ってサイバーセキュリティの確保を行う必要があります。

このように医療機関等は対象とするシステム/サービスのリスクアセスメントを行うことが必要となります。MDS/SDSはリスクアセスメントを行う際に利用でき、「安全管理ガイドライン」に対する準拠性が確認できます。対象とするシステム/サービスの情報セキュリティに関する情報を入手することによって、効果的にリスクアセスメントを実施し、有効な技術的対策や運用的対策を立てることができます。

福井大学 University of Fukui

「製造業者による医療情報セキュリティ開示書」チェックリスト

（医療情報システムの安全管理に関するガイドライン第 5.1 版対応）

製造業者　：	作成日　：			
製品名称　：	バージョン　：			
医療機関における情報セキュリティマネジメントシステムの実践(6.2)				
1　扱う情報のリストを提示してあるか？(6.2.C1)	はい	いいえ	対象外	備考＿＿
物理的安全対策(6.4)				
2　個人情報が入力・参照できる端末の覗き見防止の機能があるか？(6.4.C5)	はい	いいえ	対象外	備考＿＿
技術的安全対策(6.5)				
3　離席時の不正入力防止の機能があるか？(6.5.C4)	はい	いいえ	対象外	備考＿＿
4　アクセス管理の機能があるか？(6.5.C1)	はい	いいえ	対象外	備考＿＿
4．1　アクセス管理の認証方式は？(6.5.C1)				
・記憶（ID・パスワード等）	はい	いいえ	対象外	備考＿＿
・生体認証（指紋等）	はい	いいえ	対象外	備考＿＿
・物理媒体（IC カード等）	はい	いいえ	対象外	備考＿＿
・その他（具体的な方法を備考に記入してください）	はい	いいえ	対象外	備考＿＿
・上記のうちの二要素を組み合わせた認証（具体的な組み合わせを備考に記入してください）	はい	いいえ	対象外	備考＿＿
4．1．1　パスワードを利用者認証手段として利用している場合、パスワード管理は可能か？(6.5.C13(1)～(5))	はい	いいえ	対象外	備考＿＿
4．1．2　セキュリティ・デバイスを用いる場合に破損等で本人の識別情報が利用できない際の代替機能があるか？(6.5.C3)	はい	いいえ	対象外	備考＿＿
4．2　利用者の職種・担当業務別の情報区分ごとのアクセス管理機能があるか？(6.5.C6)	はい	いいえ	対象外	備考＿＿
4．3　アクセス記録（アクセスログ）機能があるか？(6.5.C7)	はい	いいえ	対象外	備考＿＿

福井大学
University of Fukui

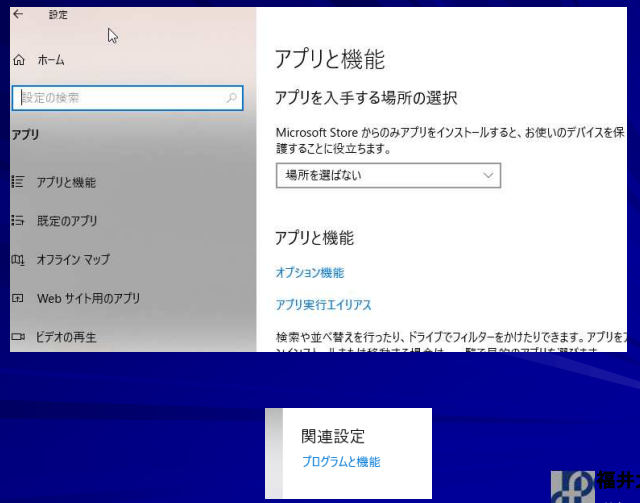
脆弱性診断の基本

- システム基本的な問題がないかの確認
  - 期待している動作だけでなく、予期しないトラフィックでの問題の有無
  - 設計通りの通信の状態の確認
- 意図しない（利用しない）出入口の有無
- OSとしての安全性確認
  - パッチの適用状態
- アプリケーションの安全性確認
  - 不要サービスなどの有無
  - 異常通信時の対応状況
  - アクセス権の妥当性

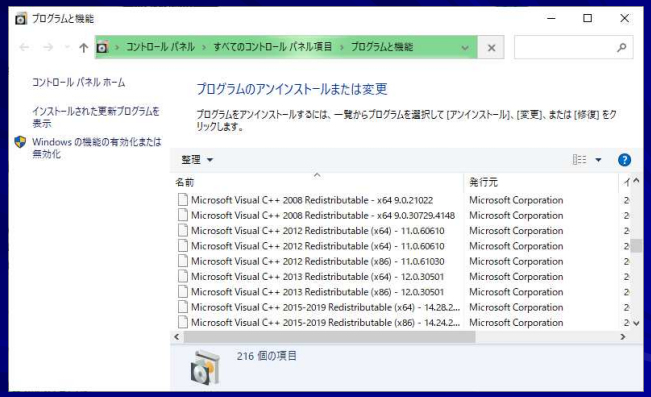
福井大学
University of Fukui

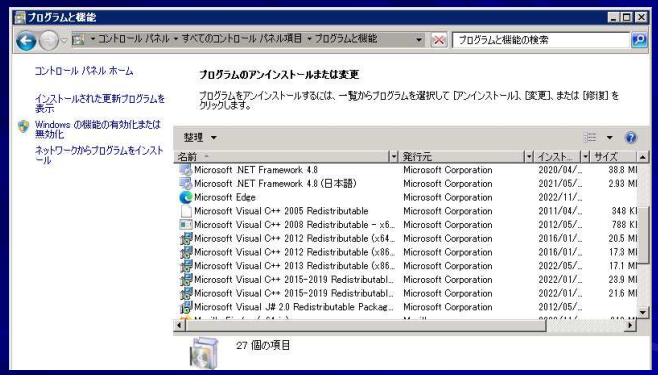
どんなアプリを使っている？

福井大学
University of Fukui



福井大学
University of Fukui





サーバの構成に機能の追加の状況がわかる

いわゆる追加コンポーネント

通信の確認

NETSTATというコマンド

- 現在のPCがどこに通信しているかを見る


```
C:¥Users¥admin>
C:¥Users¥admin>netstat

アクティブな接続

  プロトコル  ローカル アドレス          外部アドレス          状態
  TCP         127.0.0.1:1890         yyamapcm8:62522        ESTABLISHED
  TCP         127.0.0.1:2368         yyamapcm8:40000        ESTABLISHED
  TCP         127.0.0.1:5354         yyamapcm8:20703        ESTABLISHED
  TCP         127.0.0.1:5354         yyamapcm8:20704        ESTABLISHED
  TCP         127.0.0.1:9569         yyamapcm8:9570         ESTABLISHED
  TCP         127.0.0.1:9570         yyamapcm8:9569         ESTABLISHED
  TCP         127.0.0.1:9571         yyamapcm8:9572         ESTABLISHED
  TCP         127.0.0.1:9572         yyamapcm8:9571         ESTABLISHED
  TCP         127.0.0.1:9573         yyamapcm8:9574         ESTABLISHED
  TCP         127.0.0.1:9574         yyamapcm8:9573         ESTABLISHED
  TCP         127.0.0.1:9575         yyamapcm8:9576         ESTABLISHED
  TCP         127.0.0.1:9576         yyamapcm8:9575         ESTABLISHED
  TCP         127.0.0.1:9577         yyamapcm8:9578         ESTABLISHED
  TCP         127.0.0.1:9578         yyamapcm8:9577         ESTABLISHED
  TCP         127.0.0.1:20703        yyamapcm8:5354         ESTABLISHED
  TCP         127.0.0.1:20704        yyamapcm8:5354         ESTABLISHED
  TCP         127.0.0.1:40000        yyamapcm8:2368         ESTABLISHED
  TCP         127.0.0.1:62522        yyamapcm8:1890         ESTABLISHED
  TCP         172.30.0.182:1065      ufproxy01:8080         CLOSE_WAIT
```



```
  TCP         [::1]:23935            yyamapcm8:23937        ESTABLISHED
  TCP         [::1]:23937            yyamapcm8:23935        ESTABLISHED
  TCP         [2001:2f8:1f:930:2935:8046:8c9e:f619]:1083  ufproxy02:8080         ESTABLISHED
  TCP         [2001:2f8:1f:930:2935:8046:8c9e:f619]:1084  ufproxy02:8080         ESTABLISHED
  TCP         [2001:2f8:1f:930:2935:8046:8c9e:f619]:1218  ufproxy02:8080         ESTABLISHED
  TCP         [2001:2f8:1f:930:2935:8046:8c9e:f619]:1224  ufproxy02:8080         CLOSE_WAIT
  TCP         [2001:2f8:1f:930:2935:8046:8c9e:f619]:2707  ufproxy03:8080         CLOSE_WAIT
  TCP         [2001:2f8:1f:930:2935:8046:8c9e:f619]:2717  ufproxy03:8080         CLOSE_WAIT
  TCP         [2001:2f8:1f:930:2935:8046:8c9e:f619]:9113  ufproxy02:8080         CLOSE_WAIT
  TCP         [2001:2f8:1f:930:2935:8046:8c9e:f619]:9114  ufproxy02:8080         CLOSE_WAIT
  TCP         [2001:2f8:1f:930:2935:8046:8c9e:f619]:9116  ufproxy02:8080         CLOSE_WAIT
  TCP         [2001:2f8:1f:930:2935:8046:8c9e:f619]:9118  ufproxy02:8080         CLOSE_WAIT
  TCP         [2001:2f8:1f:930:2935:8046:8c9e:f619]:9119  ufproxy02:8080         CLOSE_WAIT
  TCP         [2001:2f8:1f:930:2935:8046:8c9e:f619]:9120  ufproxy02:8080         CLOSE_WAIT
  TCP         [2001:2f8:1f:930:2935:8046:8c9e:f619]:9121  ufproxy02:8080         CLOSE_WAIT
  TCP         [2001:2f8:1f:930:2935:8046:8c9e:f619]:9122  ufproxy02:8080         CLOSE_WAIT
  TCP         [2001:2f8:1f:930:2935:8046:8c9e:f619]:9123  ufproxy02:8080         CLOSE_WAIT
  TCP         [2001:2f8:1f:930:2935:8046:8c9e:f619]:11128  ufproxy02:8080        ESTABLISHED
  TCP         [2001:2f8:1f:930:2935:8046:8c9e:f619]:11156  ufproxy01:8080        ESTABLISHED
  TCP         [2001:2f8:1f:930:2935:8046:8c9e:f619]:11187  ufproxy02:8080        ESTABLISHED
  TCP         [2001:2f8:1f:930:2935:8046:8c9e:f619]:11221  ufproxy02:8080        ESTABLISHED
  TCP         [2001:2f8:1f:930:2935:8046:8c9e:f619]:11915  ufproxy02:8080        ESTABLISHED
  TCP         [2001:2f8:1f:930:2935:8046:8c9e:f619]:11922  ufproxy02:8080        ESTABLISHED
  TCP         [2001:2f8:1f:930:2935:8046:8c9e:f619]:11924  ufproxy02:8080        ESTABLISHED
  TCP         [2001:2f8:1f:930:2935:8046:8c9e:f619]:11933  ufproxy02:8080        ESTABLISHED
```


サーバだと通信先が限られるので少ない

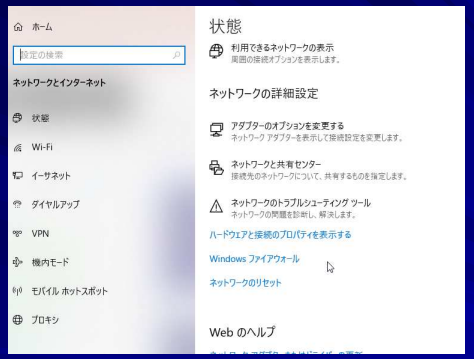
```
Z:¥>netstat

アクティブな接続

  プロトコル  ローカル アドレス          外部アドレス          状態
  TCP    127.0.0.1:60686        FHSVMG01:60687         ESTABLISHED
  TCP    127.0.0.1:60687        FHSVMG01:60686         ESTABLISHED
  TCP    127.0.0.1:60688        FHSVMG01:60689         ESTABLISHED
  TCP    127.0.0.1:60689        FHSVMG01:60688         ESTABLISHED
  TCP    192.168.144.10:3389    yyamapcm8:12220        ESTABLISHED
  TCP    192.168.144.10:20426   fhcsad02:49671         ESTABLISHED
  TCP    192.168.144.10:21053   ufproxy01:8080         ESTABLISHED
  TCP    192.168.144.10:22861   ufh-ft3-mtml-1:https   ESTABLISHED
  TCP    192.168.144.10:24815   ufh-ft3-mtml-1:ssh     ESTABLISHED
  TCP    192.168.144.10:24817   ufh-ft3-mtml-1:ssh     ESTABLISHED
  TCP    192.168.144.10:63578   ufh-ft3-mtml-1:ssh     ESTABLISHED
  TCP    [2001:2f8:1f:844:c936:2d72:2c1d:67b8]:18025  [2001:2f8:1f:860::162:109]
:microsoft-ds  ESTABLISHED
```

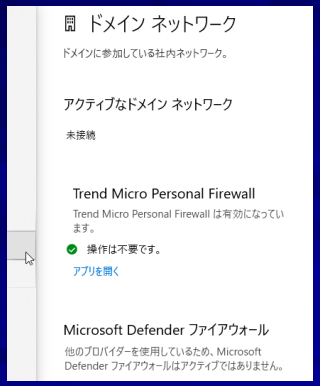
ファイアウォールの状態確認

福井大学
University of Fukui



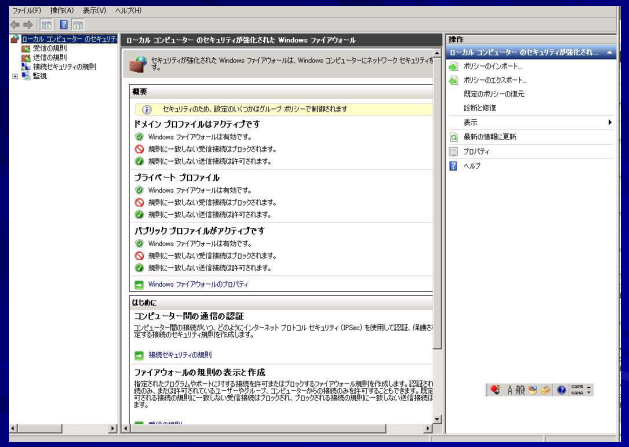
福井大学
University of Fukui

ウイルス対策ソフトなどので一括管理になっている場合もある

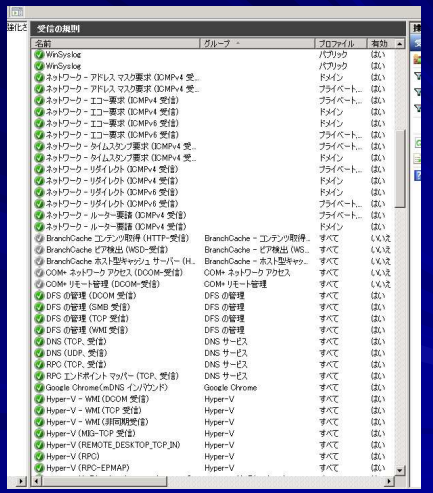


福井大学
University of Fukui

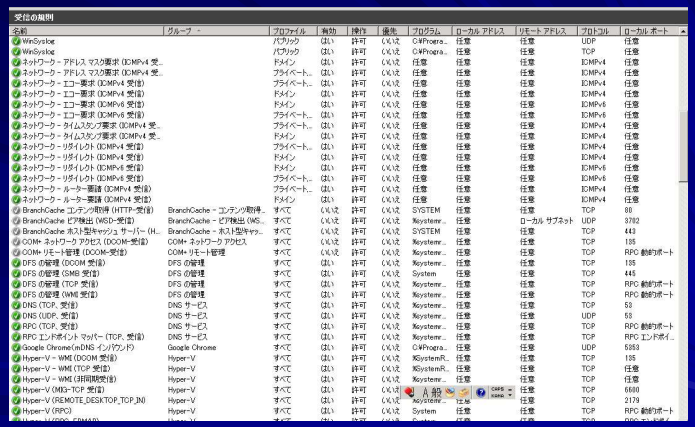
福井大学
University of Fukui



福井大学
University of Fukui



福井大学
University of Fukui



福井大学
University of Fukui

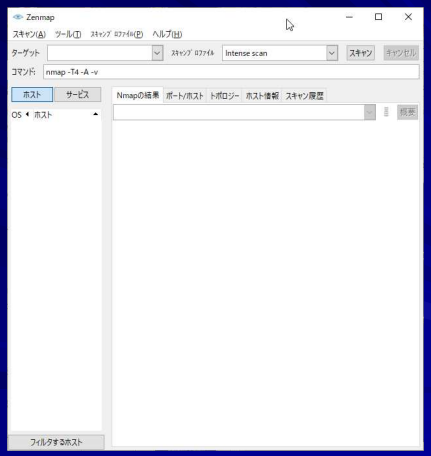
もう少し詳しく見る

福井大学
University of Fukui

- ちょっとハッキングツールに近いかな？
- どのような通信を待っているかを確認する
  - Pingが通らないものでも見つける

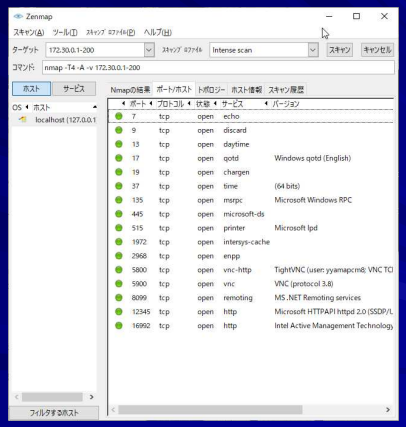
福井大学 University of Fukui

NMAP　というツール



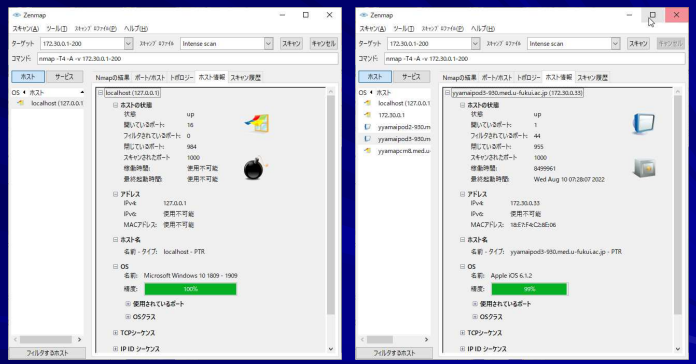
福井大学 University of Fukui

スキャンを行った結果



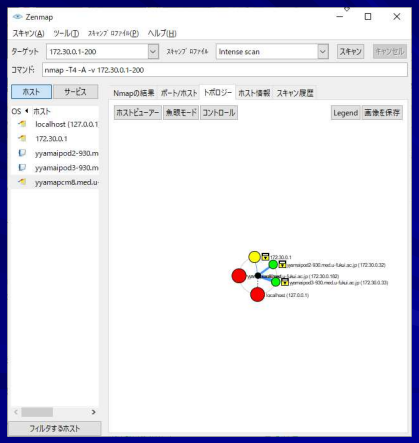
福井大学 University of Fukui

OSの種類なども探索してくれる



福井大学 University of Fukui

ネット上の一覧を図示してくれる



ペネトレーション・テスト

- 現実的なサイバー攻撃での耐性試験
  - 既知の脆弱性を検出するための特徴的なパターンでの疑似攻撃
  - 既知の侵入パターンによる不正侵入の試行
  - 既知の攻撃パターンによるサービス妨害の試行
  - 外部からのコマンド実行、情報操作、データ取得の試行
  - Web系の弱点への総攻撃

何を考えるべきか

- 院内におけるセキュリティのリスクを考える
  - セキュリティ対策の基本
- どうしても、リスク評価は100%とはならない
  - 考えうる対策はするが、「お守り」という認識で
  - エンドポイントだけでは限界
- 何かが起こる可能性を考える
  - 起こった時の対応を考慮する
  - そのためにも、検知のための「網を張る」
    - パターンだけでなき「不審なふるまい」も対応する
  - 万一の時のブロック手段を考慮する

コストをあまりかけずにできることから・・・

- まず、現状でできることをする
  - ウイルス対策ソフトでできることを生かす
    - 異常動作（ふるまい）の検知と集約化
    - セキュリティパッチの代わりの機能
      - 病院システムは、アップデートができない場合が多いので
  - OS機能によりできることを生かす
    - 不要な通信を遮断しておく
      - サーバとの通信以外はブロックする
    - 不要なファイル共有やアクセス権の制限
    - 実行権限の制限やドメイン管理での制限

Fukui Prefectural Dinosaur Museum

御清聴ありがとうございました。

福井大学
University of Fukui