医療機関における サイバーセキュリティへの課題と対応

福井大学
医学部附属病院医療情報部
山下　芳範

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

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

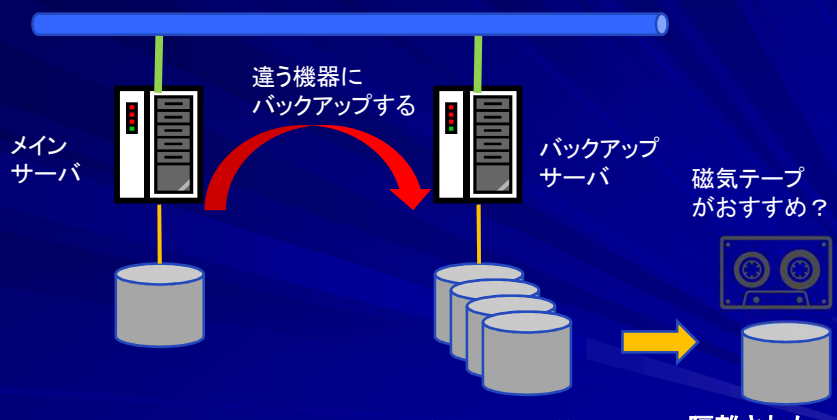
福井大学 University of Fukui

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

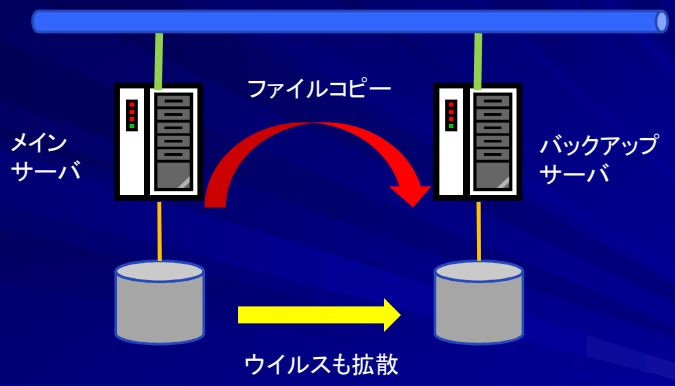
福井大学 University of Fukui

バックアップに求められるもの



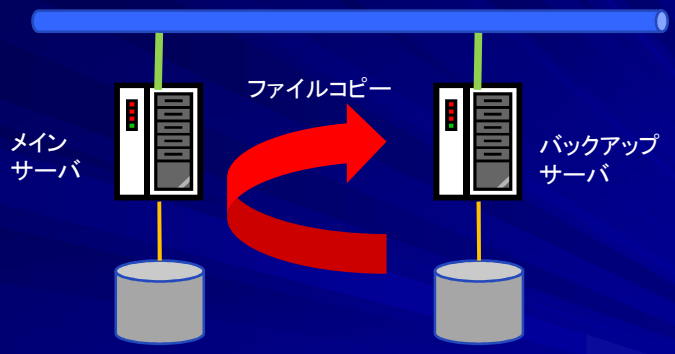
福井大学 University of Fukui

バックアップの課題



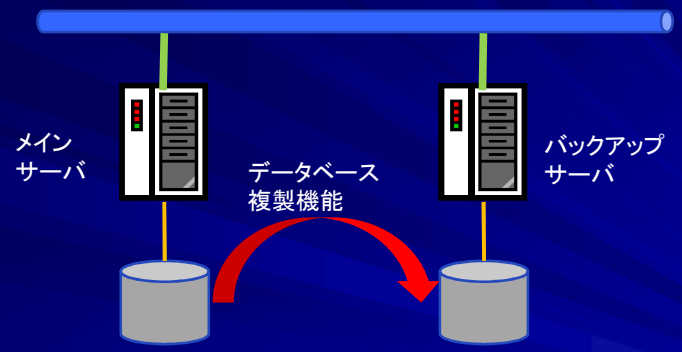
福井大学
University of Fukui

バックアップでの時間稼ぎ（1）



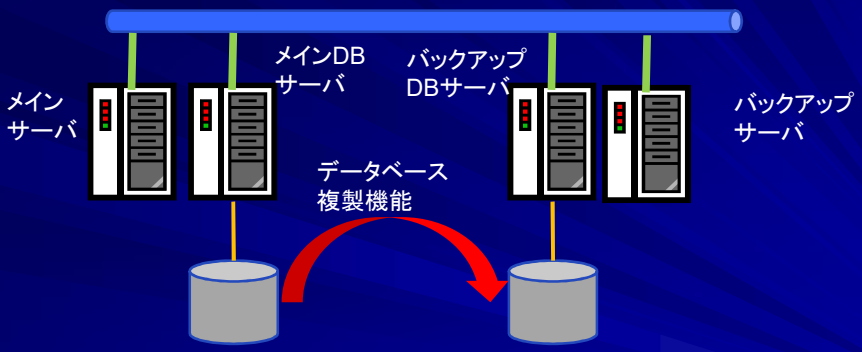
福井大学
University of Fukui

バックアップでの時間稼ぎ（2）



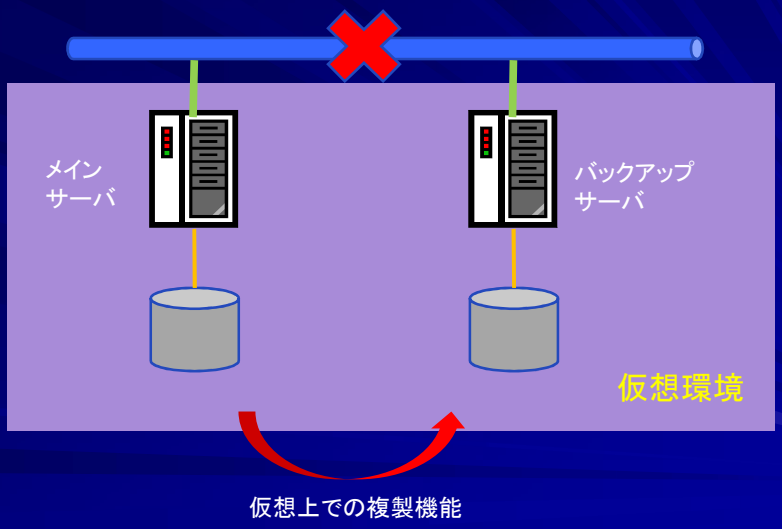
福井大学
University of Fukui

バックアップでの時間稼ぎ（3）



福井大学
University of Fukui

バックアップでの時間稼ぎ（4）



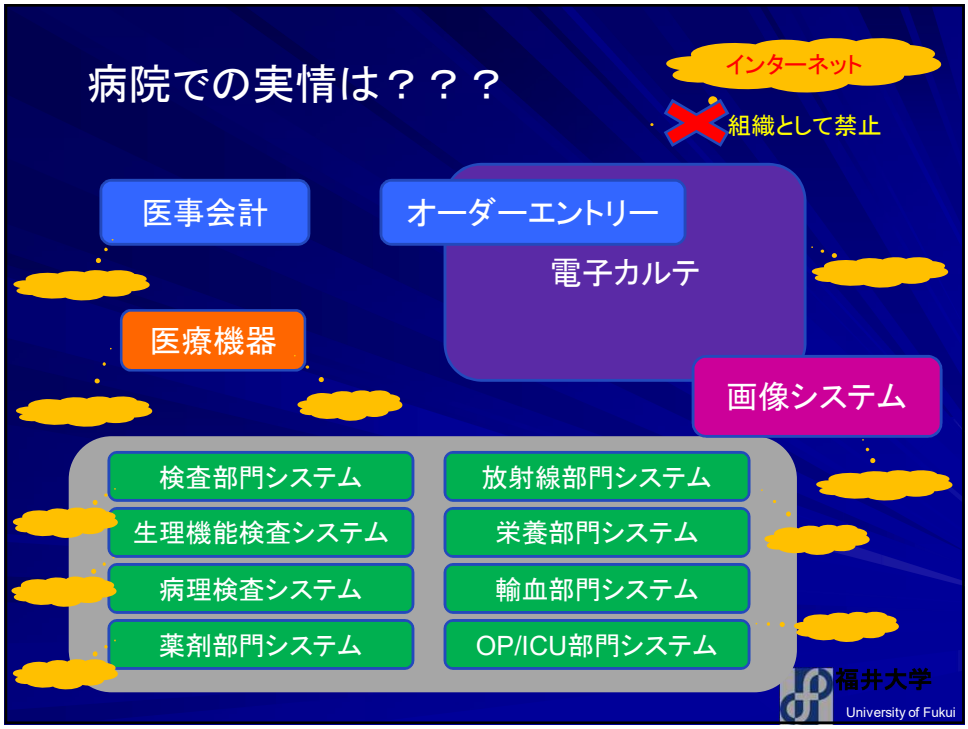
福井大学
University of Fukui

これまでの被害から・・

- 原則インターネット接続はないと思い込んでいないか？
- 各種のリモートメンテナンス用回線が、内部への裏口（バックドア）になっていないか？
  - きっちりと把握できているか？

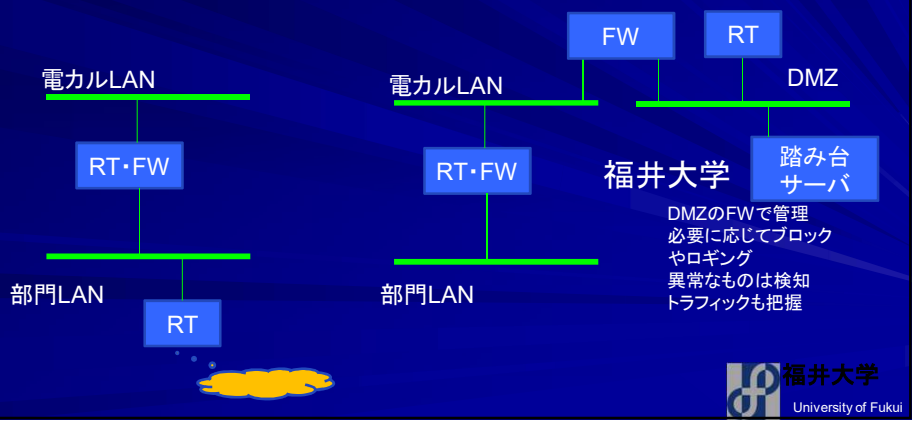
福井大学
University of Fukui


一般的な病院の対応
サーバ
ストレージ
閉域なので安全？
端末
インターネットは
危険なので接続しない
インターネット
福井大学
University of Fukui


病院での実情は？？？
インターネット
組織として禁止
医事会計
オーダーエントリー
電子カルテ
医療機器
画像システム
検査部門システム
放射線部門システム
生理機能検査システム
栄養部門システム
病理検査システム
輸血部門システム
薬剤部門システム
OP/ICU部門システム
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回線を引いている
  - 場合によっては、部門のLANに接続



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

セキュリティ研修の必要性

- 標的型メールから感染が広がる
  - 内部は隔離？？？
    - USB等他の媒体
    - リモートメンテ用回線経由
- 上層部への理解と啓蒙
  - 訓練をすると状況が理解できる

福井大学 University of Fukui

R9から必須の2要素認証

- ID･パスワードは結構漏れる
  - 外部からの攻撃に利用される
  - なしすましへの利用
  - 使いまわしも多い
- 今後の働き方改革で
  - リモートアクセスの実施
    - ID･PASSではダメでしょ
    - 内部が2要素なら、リモートそれ以上？？3要素？？

福井大学 University of Fukui

認証基盤もインフラ

- 認証基盤はネットワークと同様に、全てのシステムで利用するものである
- 認証やPKIは共通でないと意味がない

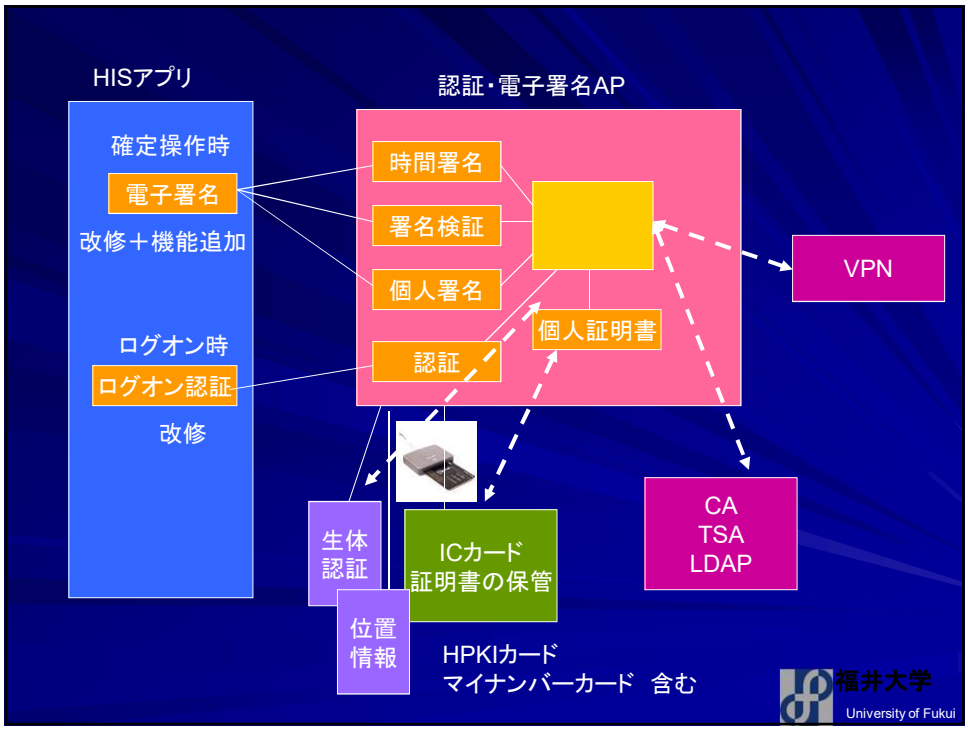
- どこかのおまけでは、認証基盤やPKIは投資価値がない
  - コストだけかかってしまう
- 全体の役割を考慮した構成が重要

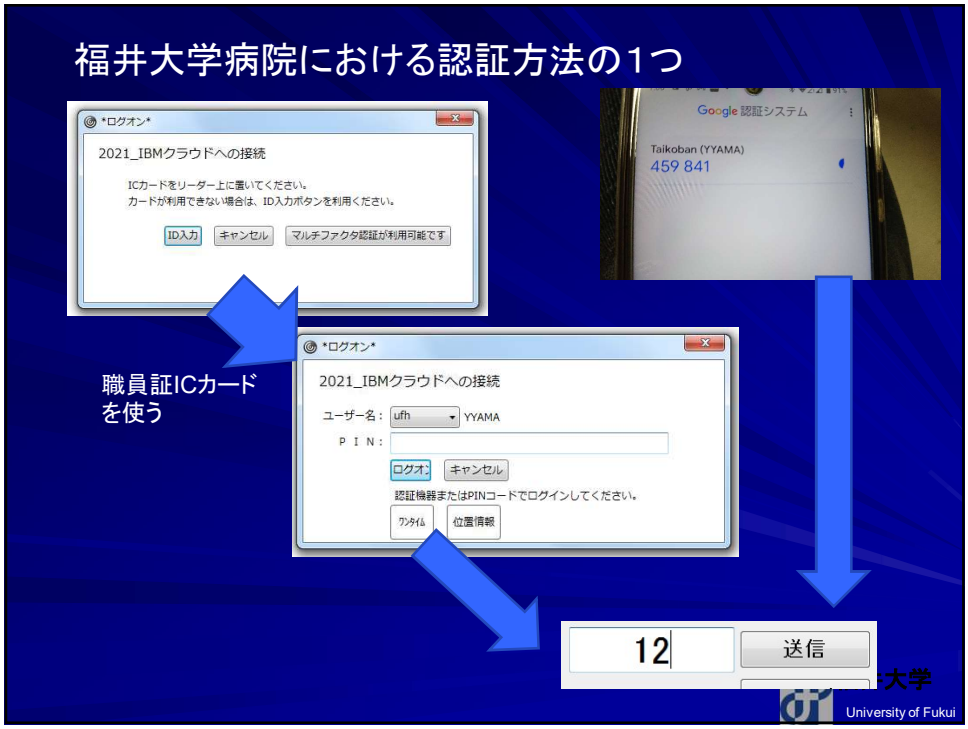
福井大学 University of Fukui

福井大学病院での多要素認証

- ガイドラインでは2要素認証とあるが・・・
  - 基本はID+パスワードは避けることが目標
  - 生体認証はコスト高
    - ICカード＋PINコードやワンタイムパスワード
  - 生体認証が利用できない場合は？
  - 内部は2要素認証　外部からの利用も2要素？？
    - 外部からのVPN接続も同じでいいのか？福井では3要素に
- 将来を見据えて複数への対応
- 認証基盤として独立

福井大学 University of Fukui


HISアプリ
確定操作時
電子署名
改修＋機能追加
ログオン時
ログオン認証
改修
認証・電子署名AP
時間署名
署名検証
個人署名
認証
個人証明書
VPN
CA
TSA
LDAP
生体
認証
位置
情報
ICカード
証明書の保管
HPKIカード
マイナンバーカード　含む
福井大学
University of Fukui


福井大学病院における認証方法の1つ
ログオン
2021_IBMクラウドへの接続
ICカードをリーダー上に置いてください。
カードが利用できない場合は、ID入力ボタンを利用ください。
ID入力
キャンセル
マルチファクタ認証が利用可能です
Google 認証システム
Taikoban (YYAMA)
459 841
職員証ICカード
を使う
ログオン
2021_IBMクラウドへの接続
ユーザー名：
ufh
YYAMA
ＰＩＮ：
ログオン
キャンセル
認証機器またはPINコードでログインしてください。
ワンタイム
位置情報
12
送信
大学
University of Fukui

この先必要なセキュリティ対策とは

福井大学
University of Fukui

あらかじめ問題を把握する

- 機器の動作試験は当たり前
- 意図しないセキュリティ事象の確認
- 特にネットワークでの接続については、ネットワークとしての安全性や安定性の確認

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

対策はすべき課題

- 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
- 運用に関わる内容への告知

福井大学 University of Fukui

OSのパッチ問題

- 医療機器に限らず、医療情報システム全体で、導入時の時点で塩漬けされている場合が多くある
  - 理由1：動作確認が必要
  - 理由2：薬機法で改造になるのでできない

福井大学
University of Fukui

セキュリティ対策問題

- 医療機器にPCが含まれていて、ネットワーク接続があっても、不正プログラム対策もない
- USBが使えるものもあるが、不正プログラム対策もない
- 別途不正プログラム対策をしようとしても、薬機法を盾に抵抗される

福井大学
University of Fukui

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

福井大学 University of Fukui

防御としての効果

- 挙動不審なトラフィックの排除
- 重要サーバ群の保護
  - BYODなど多彩な端末からの防御
  - 重要サーバ入口での防御
- 仮想化のメリットとの組み合わせ
  - 仮想化の特徴を生かせる
- 医療機器サーバのように対策が不十分なものへの対策強化が行える
- IoTデバイスへの対応

福井大学 University of Fukui

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

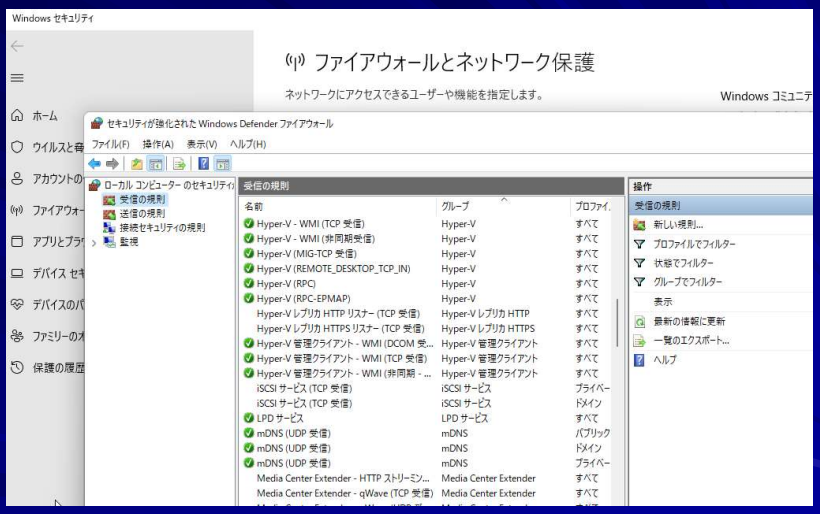
福井大学 University of Fukui

コストをあまりかけずに・・・

- 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

福井大学 University of Fukui

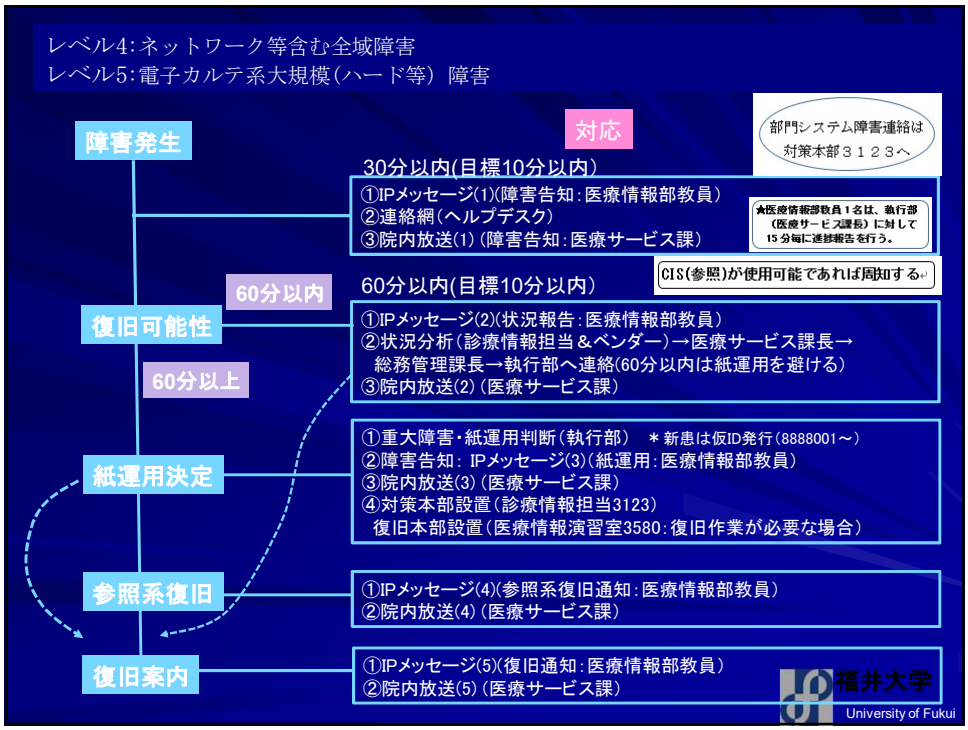
PCやサーバ単位での、通信の制限は標準機能となっている

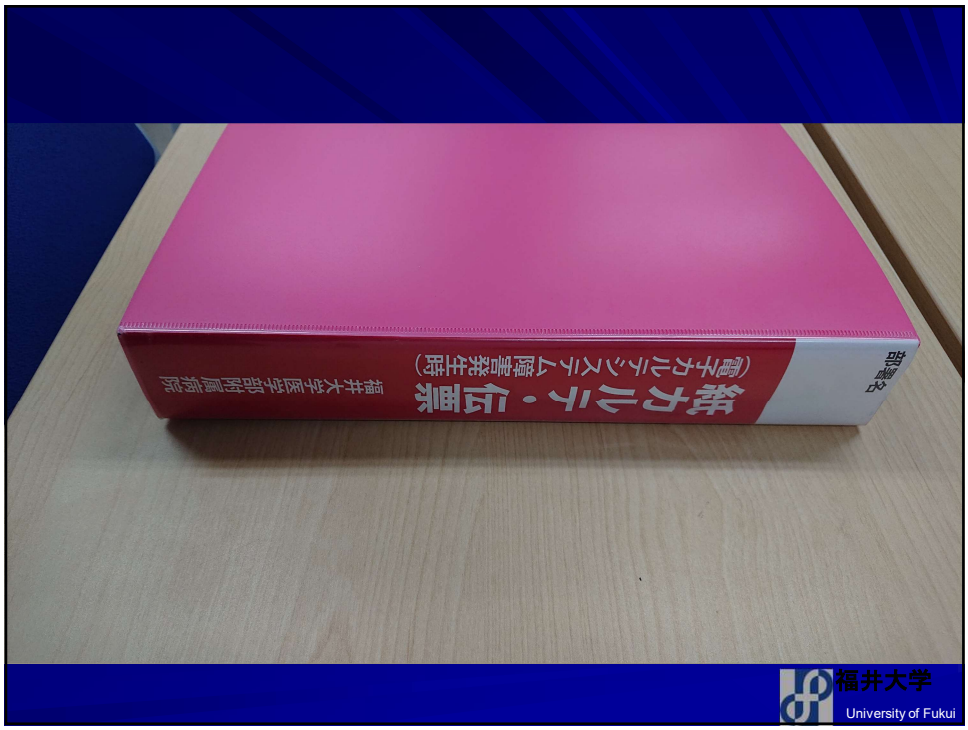


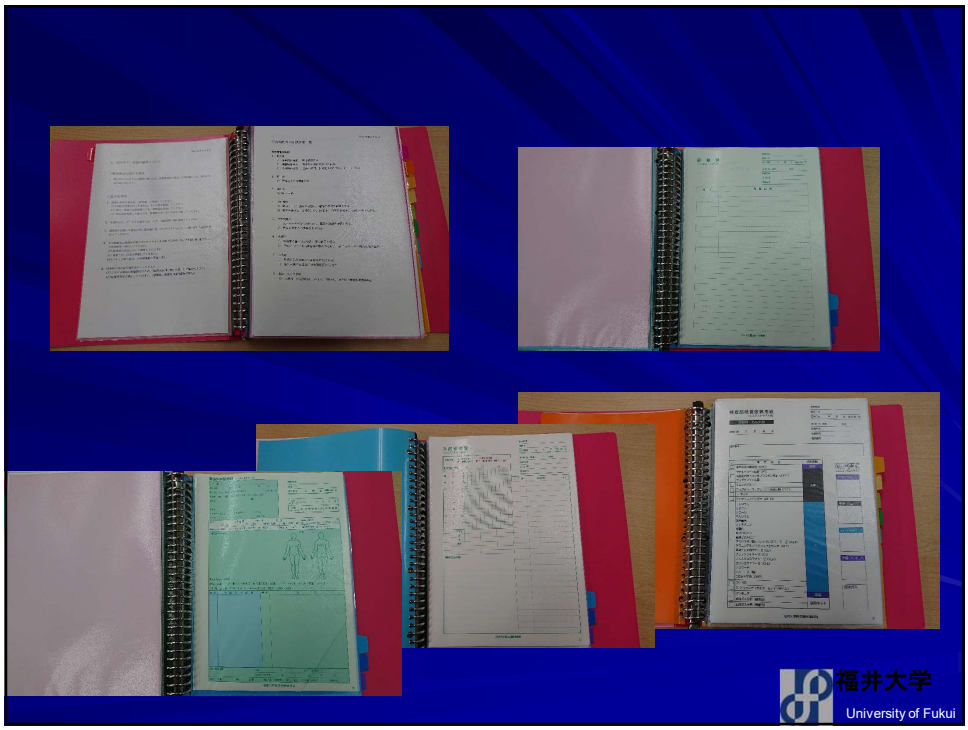
福井大学
University of Fukui

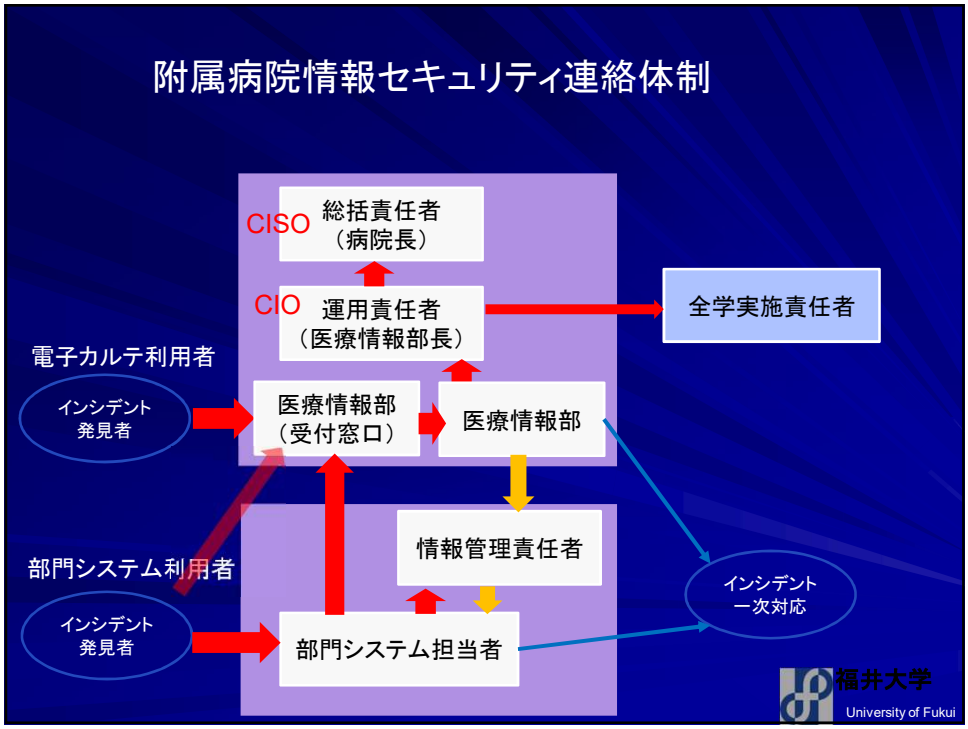
BCP対応に関して

福井大学
University of Fukui


レベル4:ネットワーク等含む全域障害
レベル5:電子カルテ系大規模(ハード等) 障害
対応
部門システム障害連絡は
対策本部３１２３へ
障害発生
30分以内(目標10分以内)
①IPメッセージ(1)(障害告知:医療情報部教員)
②連絡網(ヘルプデスク)
③院内放送(1)(障害告知:医療サービス課)
★医療情報部教員１名は、執行部
(医療サービス課長)に対して
15分毎に進捗報告を行う。
CIS(参照)が使用可能であれば周知する
60分以内
60分以内(目標10分以内)
復旧可能性
①IPメッセージ(2)(状況報告:医療情報部教員)
②状況分析(診療情報担当＆ベンダー)→医療サービス課長→
総務管理課長→執行部へ連絡(60分以内は紙運用を避ける)
③院内放送(2)(医療サービス課)
60分以上
紙運用決定
①重大障害・紙運用判断(執行部) ＊新患は仮ID発行(8888001～)
②障害告知: IPメッセージ(3)(紙運用:医療情報部教員)
③院内放送(3)(医療サービス課)
④対策本部設置(診療情報担当3123)
復旧本部設置(医療情報演習室3580:復旧作業が必要な場合)
参照系復旧
①IPメッセージ(4)(参照系復旧通知:医療情報部教員)
②院内放送(4)(医療サービス課)
復旧案内
①IPメッセージ(5)(復旧通知:医療情報部教員)
②院内放送(5)(医療サービス課)
福井大学
University of Fukui


福井大学
University of Fukui


福井大学
University of Fukui


附属病院情報セキュリティ連絡体制
CISO
総括責任者
（病院長）
CIO
運用責任者
（医療情報部長）
全学実施責任者
電子カルテ利用者
インシデント
発見者
医療情報部
（受付窓口）
医療情報部
情報管理責任者
部門システム利用者
インシデント
発見者
部門システム担当者
インシデント
一次対応
福井大学
University of Fukui