

令和8年度 第2回 枚方市病院事業運営審議委員会 資料

情報セキュリティに関する取り組みについて

令和8年9月2日

医事課

近年、医療機関を標的としたランサムウェア（身代金要求型マルウェア）をはじめとするサイバー攻撃が急増・巧妙化しています。特に地方自治体が運営する中核的な急性期病院（200～500床規模）は、地域医療の基幹でありながら、サプライチェーン（委託業者やシステム保守回線）の脆弱性を突かれ、標的とされるケースが全国的に後を絶ちません。ひとたび攻撃を受ければ、電子カルテの暗号化による診療停止、新規救急患者の受入れ制限など、地域医療の崩壊に直結する極めて深刻な事態を招きます。

11病院サイバー被害

救急搬送・手術停止も

「身代金」ウィルス

世界各地で需要インフラがサイバー攻撃にさらされる中で、国内で2010年以降、少なくとも11病院がコンピュータウィルス「ランサムウェア」による被害を受けたことが、読売新聞の取材でわかった。救急搬送の受け入れや手術の停止、外来診療の制限などの被害が出ており、医療機関が攻撃対象になっている実態が浮き彫りになった。

△関連記事7面▽

ランサムウェアシステムに不正侵入し、データを暗号化して使えなくするコンピュータウィルス。ランサムは「身代金」を意味する英語で、攻撃者は、復元する代わりに身代金を要求する。海外で多数の種類が出現し、2015年頃から国内でも確認されるようになった。身代金を支払わなければ、データを公開すると脅す手口もみられる。警察庁によると、警察に寄せられた被害相談は今年1～6月で61件あった。

16年以降

医療機関へのランサムウェア攻撃のイメージ

被害は16年1件、17年3件、18年1件、19年1件、20年0件だったが、21年は5件に急増。身代金を支払った病院は確認されなかった。すでに各病院では対策を講じている。厚生労働省は攻撃を受けた医療機関に報告を求め、発生件数は公表しておらず、ほかにも被害を受けたケースがあると考えられる。

17年までの被害は、病院の業務用パソコンのメールが送受信できなくなった。ファイルが開かなくなった。18年以降は、電子カルテや医療会計、コンピュータ断層撮影法（CT）で撮影した画像の管理といった

①ランサムウェアに感染させる
②データを暗号化
③身代金を要求
④データを公開しない
⑤身代金を支払う
⑥データを利用できず
⑦電子カルテやレントゲンやCTなどの画像データ

医師ら

利用できず

電子カルテ レントゲンやCTなどの画像データ

2

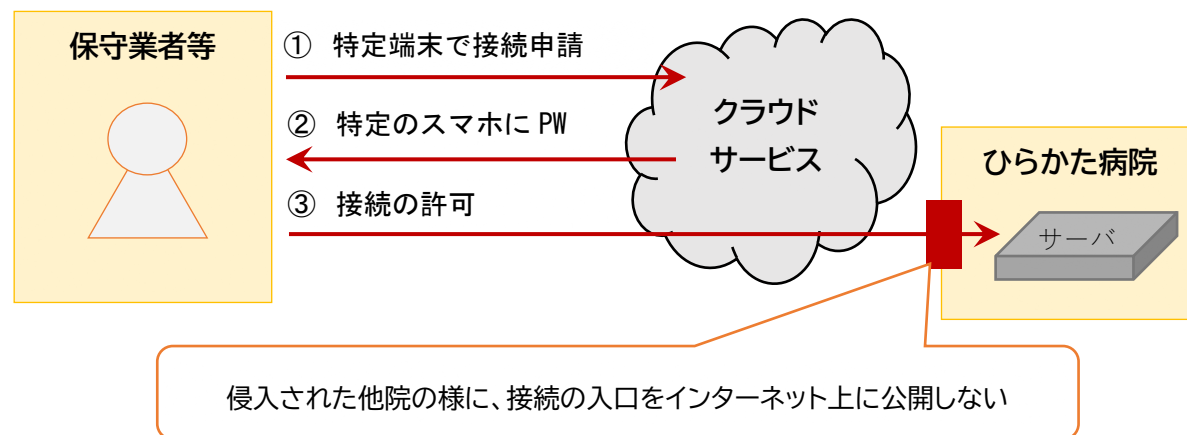
2. これまでの対策（侵入を「防ぐ・早期に気づく」ための多層防御）

当院では、厚生労働省の「医療情報システムの安全管理に関するガイドライン」を遵守し、現在、以下の具体的な対策を講じています。

① 安全な「外部メンテナンス接続」の確立

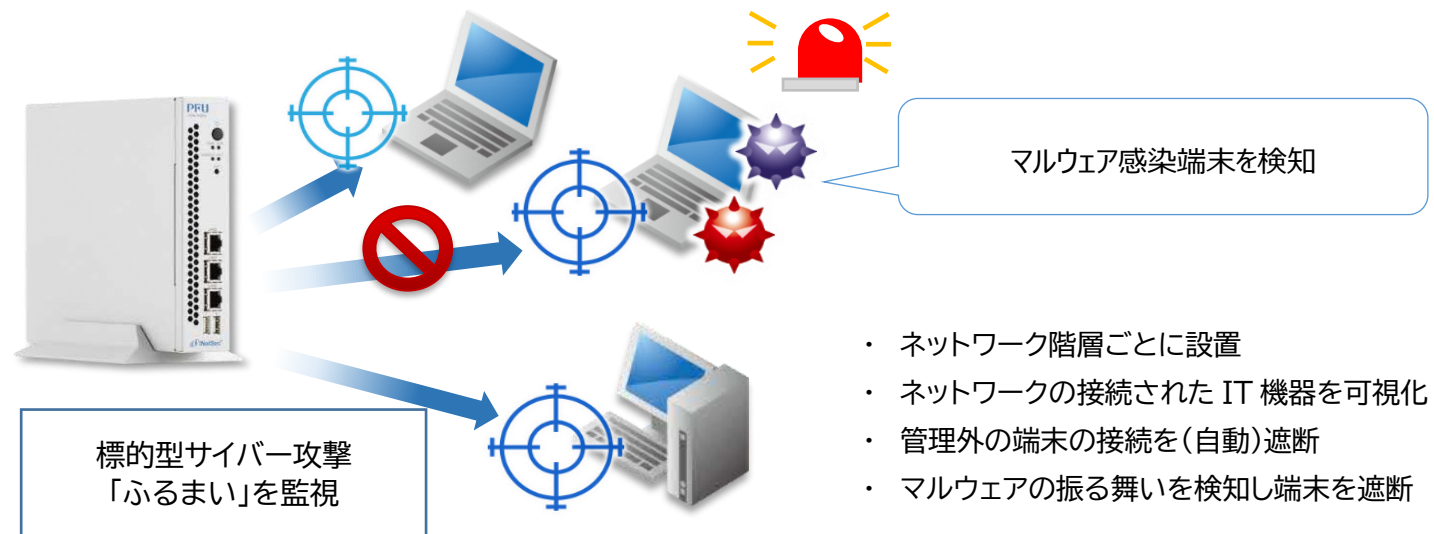
他院で侵入される原因となっていた、システム会社がメンテナンスで院内の電子カルテに接続する際の入口にある「脆弱性」を排除するため、当院は、院外にあるデータセンターのサービス（クラウドサービス）認証プロセスを導入しています。

保守業者等が特定の端末から院外にあるクラウドサービスに接続申請をすると、特定のスマホにパスワード（PW）が送られ、院内のサーバへの接続が許可されます。このように認証や接続端末等の制限を厳格に行うことで、不正侵入の入り口を塞いでいます。



② 通信の「ふるまい検知」による内部監視

万が一、ウイルスがネットワーク内部に侵入した場合を想定し、ネットワーク階層ごとに「普段と異なる通信（不審なふるまい）」をリアルタイムで検知・遮断する仕組みを導入しています。これにより、内部での感染拡大を初期段階で封じ込む仕組みを導入しています。



③ ユーザー認証の高度化（パスワードポリシーの見直し）

総務省等の最新ガイドラインに基づき、形骸化しがちだった「パスワードの定期変更」を廃止し、「13 桁以上の英数記号の組み合わせ」を義務化することで、総当たり攻撃に対する耐性を向上させています。

新	旧
■ 英数字・記号を混在させた<u>13文字以上</u>であること ■ 利用者ID が含まれていないこと ■ 利用者生年月日 が含まれていないこと ■ 利用者カナ氏名のヘボン式ローマ字に変換した英文字（姓と名それぞれ、大小文字区別なし）が含まれていないこと <u>（削除）</u> <u>（削除）</u>	■ 英数字・記号を混在させた<u>8文字以上</u>であること ■ 利用者ID が含まれていないこと ■ 利用者生年月日 が含まれていないこと ■ 利用者カナ氏名のヘボン式ローマ字に変換した英文字（姓と名それぞれ、大小文字区別なし）が含まれていないこと ■ <u>有効期間は60日であること</u> ■ <u>過去3回のパスワードと一致しないこと</u>

3. さらなる防御壁の強化

上記に加え、システム自体を物理的に守る「クラウド化」と、職員の「意識向上」の双方から、有事においても医療が継続できるよう、さらなる防御壁の強化を図ります。

① クラウド型電子カルテの採用

本年 11 月末に稼働を予定している新電子カルテは、システム本体を院内に設置しない「クラウド型」を採用します。これにより現状の院内設置に比べてセキュリティの水準は、以下のとおりさらに強固なものへと向上します。

クラウド型電子カルテシステムの採用

現状：オンプレミス

- ⚠ **物理的脆弱性**
院内のサーバの物理的破損や通信障害、災害のリスク
- ⚠ **セキュリティ対策の遅延**
脆弱性修正の適用が遅れ、攻撃被害のリスクが増加
- ⚠ **限定的な防御体制**
院内の職員のみによる脅威からの監視・対応に限界



採用後：クラウド

- ✓ **強固なインフラセキュリティ**
堅牢なデータセンターで稼働、物理的破損や災害から保護
- ✓ **最新セキュリティ対策の即時適用**
クラウド側で常に自動で最新対策が適用
- ✓ **多層防御体制**
24時間体制の監視と自動対応が実現

✓ クラウド移行による3つの主要な改善

1 強固なインフラセキュリティ

院外の**堅牢なデータセンター**でシステム稼働。院内のサーバの物理的破損や通信障害・災害のリスクから切り離され、安全性が担保されます。

2 最新のセキュリティ対策の即時適用

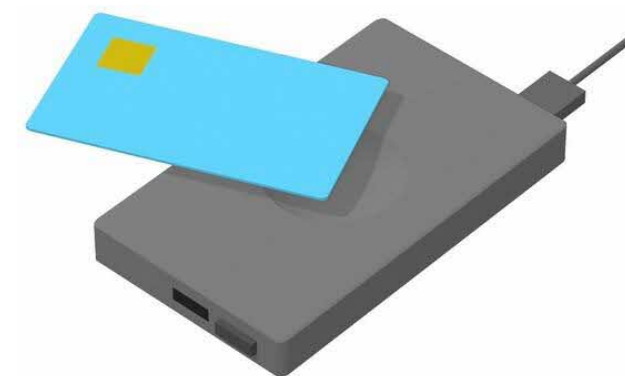
オンプレミスの課題だった**対策の適用の遅れ**が解消。クラウド側で常に**最新のセキュリティ対策が自動適用**され、脆弱性への対応が迅速化します。

3 クラウド接続と既存対策の相乗効果

当院の**外部メンテナンス接続統制**と**強力なパスワード認証**が、クラウド接続時の強固な認証の仲介役として機能。多層防御が実現します。

② ログイン方法の強化

電子カルテの入れ替えに合わせ、電子カルテへのアクセス時のログインにおいて、パスワード(自分しか知りえない記憶)に加え、ひこカード(自分だけの所持物)を用いた二要素による認証を新たに導入します。これにより、ID・パスワードが万が一漏洩した場合でも、外部からのなりすましや不正侵入ができないようになります。



③ 職員の意識向上と全職員セキュリティ研修の実施

技術的な対策（システム）を施すだけではセキュリティは完成しません。現場でシステムを扱う「職員一人ひとりの意識（人）」が脅威に対する最大の防御壁となります。

セキュリティの最大の防御壁：「人の意識」

技術的対策（システム）

認証・監視・バックアップなどのシステム基盤を構築。ただしこれだけでは不十分。

人的対策（職員の意識）

職員一人ひとりのセキュリティ意識向上が最大の防御壁となります。

そのため当院では、全職員を対象に「IPA（独立行政法人情報処理推進機構）の情報セキュリティ 10 大脅威」を切り口として、情報セキュリティの底上げを図る職員研修を今年度実施しています。外部からの攻撃やAIに潜むリスクなど、脅威に対する全員が実施すべき対策や心構えを周知徹底することで、組織全体の「セキュリティ文化」の醸成に努めています。

全職員対象セキュリティ研修の実施

IPA（独立行政法人情報処理推進機構）の「情報セキュリティ10大脅威」を切り口として、組織全体の意識向上を図る職員研修を今年度実施しています。

教育テーマ1

外部からの攻撃やAIに潜むリスクなどの脅威

教育テーマ2

脅威に対する全員が実施すべき対策や心構え

目的

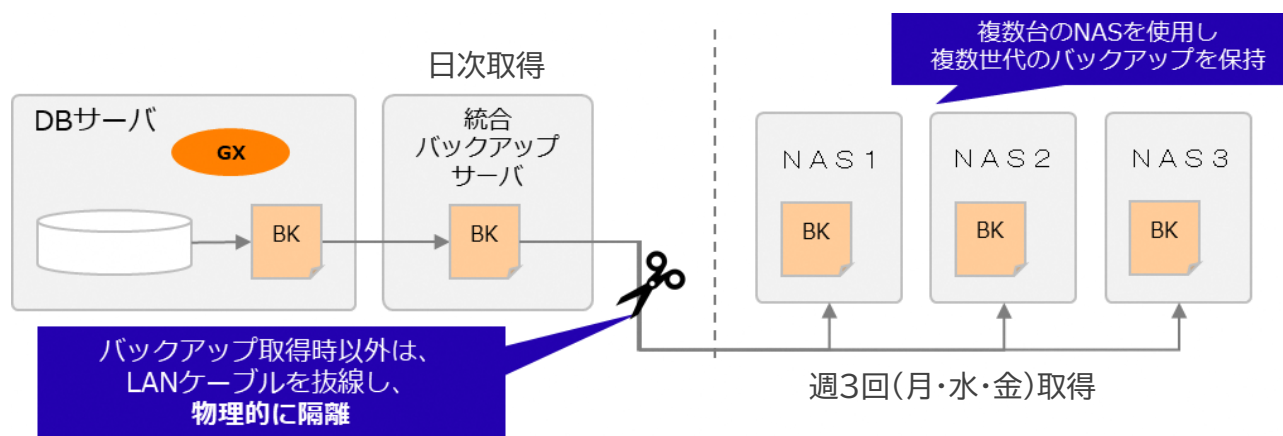
組織全体の「セキュリティ文化」の醸成

4. 有事への備え（それでも防ぎきれないインシデントを想定する重要性）

これら最新鋭の防御策を講じて、日々進化するサイバー攻撃を「100%防ぎきる」ことは不可能です。そのため、当院では「侵入される、あるいはシステムが停止する」ことをあらかじめ前提とし、もしそのような事態が発生した場合にあっても被害を最小限に抑え、医療を継続するための「万が一に備えた対策」に力を入れています。

① 「オフラインバックアップ」の確保

当院では、日次で診療情報のバックアップを取得していますが、万が一ランサムウェア等のウイルスに攻撃されれば、そのバックアップデータも使い物にならず（暗号化）になります。そこで、ウイルスからデータを守るため、ネットワークから物理的に隔離された「オフラインバックアップ」を週に3回、保存用ハードディスク（NAS）に取得することで、最悪の事態が発生した場合でも、データを復旧させるためのデータを守る体制を整えています。



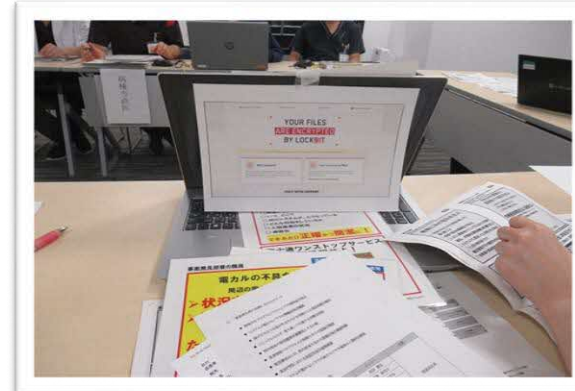
② 医療継続のための「業務継続計画（ICT-BCP）」策定と「初動対応訓練」

当院では、システム障害やサイバー攻撃があった場合に、各部署、各職員の取るべき行動を示した「情報システム部門業務継続計画（ICT-BCP）」を策定しています。

また、この計画に基づき、初動対応を主題として多職種の職員が参加するインシデント訓練を年に1回実施し、万が一の事態に備えています。



昨年度の訓練の様子
(2026/3/11)



本年11月末に稼働するの新システムへ移行時は電子カルテを一定時間停止させます。具体的には、金曜日夜間から日曜日午後までの間「紙カルテ運用（旧システムは参照のみ可能）」を予定しています。電子カルテが使えず、紙カルテで運用せざるを得ないこの状況は、大規模インシデント発生時における「課題の洗い出しができる機会」でもあると捉えています。

5. まとめ

当院では、「事前防御（認証・セグメント監視）」、「万が一の備え（クラウド化・二要素認証・オフラインバックアップ）」、そして「事後対応（訓練・BCP）」がシームレスに連携したセキュリティ対策となるよう、取り組んでいます。

情報セキュリティ対策の全体像

技術的対策と人的対策のシームレスな連携

3層の構えによるシームレス（途切れの無い）セキュリティ防御

事前防御

第1層：侵入阻止

- 安全な外部接続
- ふるまい検知
- パスワードの高度化

万が一の備え

第2層：被害最小化

- クラウド化による安全強化
- ログイン方法の強化
- オフラインバックアップ

事後対応

第3層：早期復旧

- BCP（業務継続計画）策定
- インシデント訓練
- 迅速な復旧体制

安心・安全で途切れない医療の提供

以上を踏まえ、認証・監視・バックアップと「3層の技術的防御」に加え、「職員全体のセキュリティ意識向上」を図ることでセキュリティ体制を盤石なものとするを、情報セキュリティに関する取り組みの基本方針に据えています。

基本方針

3層の技術的防御 + 職員全体のセキュリティ意識向上 = 盤石のセキュリティ体制

今後とも、新しい電子カルテの安定稼働を視野に、地域の皆様に「安心・安全で途切れない医療」を提供し続けてまいります。