

事務連絡
令和3年6月28日

各都道府県衛生主管部（局） 御中

厚生労働省政策統括官付サイバーセキュリティ担当参事官室

厚生労働省医政局研究開発振興課医療情報技術推進室

厚生労働省医薬・生活衛生局医療機器審査管理課

厚生労働省医薬・生活衛生局医薬安全対策課

医療機関を標的としたランサムウェアによるサイバー攻撃について(注意喚起)

近年、国内外の医療機関を標的とした、ランサムウェアを利用したサイバー攻撃による被害が増加している（別添1参照）。ランサムウェアによるサイバー攻撃は国境を超えて実行されており、我が国においても、世界各国と同様にリスクが高まっているところである。医療機関の情報システムがランサムウェアに感染すると、保有する情報資産（データ等）が暗号化され、電子カルテシステムが利用できなくなって診療に支障が生じたり、患者の個人情報などが窃取されたりする等の甚大な被害をもたらす可能性がある。

また、新型コロナウイルスに関連した医療機関へのサイバー攻撃や7月から開催されるオリンピック・パラリンピック東京大会においても、大会関係機関等を狙ったサイバー攻撃等が予見されるところである。

については、4月30日付けで発出された内閣官房内閣サイバーセキュリティセンターからの注意喚起（別添2参照）について、改めて、貴管内の医療機関に対し周知するとともに、下記に示したランサムウェアによるサイバー攻撃の解説及び対策例を参考に、関係医療機関に対し注意喚起をお願いする。

また、医療機関と医療機器製造販売業者の連携によって、医療機器に係る必要なサイバーセキュリティ対応が円滑に行われるよう、下記のうち「医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律」（昭和 35 年法律第 145 号）に
関係する各種手続き（以下「薬事手続き」という。）について、改めて貴管下関係製造販売業者等に周知方願います。

記

1 ランサムウェアについて

ランサムウェアはコンピュータに感染すると、コンピュータ内のデータを暗号化、もしくはシステムをロックして使用不可の状態にし、元に戻すための身代金（仮想通貨であることが多い。）を払うことを要求（脅迫）するコンピュータウイルスである。

2 最近の攻撃の手口

最近は、次のような2つの攻撃手口が多く見られる。

(1) 二重脅迫

暗号化したデータを復旧するための身代金要求に加え、暗号化する前にデータを窃取し、窃取したデータの一部をインターネットに公開してデータの所持を誇示し、身代金を支払わなければ残りのデータを全て公開する、といった二重脅迫の被害が確認されている。

(2) 人手によるランサムウェア攻撃

従来のランサムウェアは、ランサムウェア本体がダウンロードされたコンピュータ内の情報を暗号化したり、ランサムウェアを添付したメールを組織内にばらまいたりするような単純な感染拡大であったが、最近では攻撃者から遠隔でコントロールされたランサムウェアが、組織内のネットワークを探索し、ドメインコントローラ（LAN 内にあるコンピュータや利用者アカウントなどを集中管理するサーバ）やセキュリティパッチやソフトウェア等の配信サーバなどの重要なサーバをランサムウェアの管理下に置き、それらから一斉に組織内の端末やサーバ、特にバックアップサーバにランサムウェアを感染させるような攻撃が確認されている。

3 ランサムウェア攻撃への対策

主な対策としては、次のようなものが挙げられる。

(1) 組織のネットワークへの侵入対策

① 攻撃対象領域の最小化

インターネットからアクセス可能な、あるいは公開するサーバやネットワーク機器を最低限にするとともに、インターネット経由で利用するアプリケーションも最低限にする。さらに、それらが乗っ取られる場合を考慮し、そこからアクセス可能な範囲を限定する。

② なりすまし、不正ログイン対策

組織外からの認証・認可の対象や範囲を特定し、限定する。多要素認証等の強固な認証方式を採用するとともに、アクセスや認証のログを取得し、監視する。

③ 脆弱性対策

端末及び利用ソフトウェア、ファームウェア（ハードウェアを直接操作するソフトウェアでハードウェア内にある）等を常に最新の状態に保つ。最近は、脆弱性が公開されてから、その脆弱性を悪用する手法が出回るまでの期間が短いため、迅速に対応できるよう体制や計画を整備する。

④ ウイルス対策ソフト

ウイルス対策ソフトを導入し、定義ファイルを最新の状態に保つ。

⑤ 拠点間ネットワークのアクセス制御

ランサムウェア攻撃に限らず、複数の拠点をネットワークで接続している場合、対策の弱い拠点から侵入され、そこから侵入される事例が散見されるため、拠点間のアクセス制御を見直す。

⑥ 攻撃メール対策

攻撃メールへのセキュリティ装置等による対策や、職員の啓発や訓練を行う。

⑦ 内部対策

攻撃者による侵害を早期に検知するため、統合ログ管理、内部ネットワーク監視、コンピュータの不審な動作を監視する仕組み（製品等）を導入する。

⑧ ログの取得と保存

感染経路、他の端末、サーバへの感染拡大の有無の確認等を行うため、各種のログを取得し、一定期間（1年以上を推奨）保存する。

⑨ その他

夜間等に活動し、感染を広げるランサムウェアの被害を防止するため、使用していないパソコンの電源を切る。

(2) インシデント対応体制の構築

実被害を抑制するために、ウイルス等の不審な活動を検知した際に素早く対応できるインシデント対応体制を構築する。特に、迅速に意思決定を下すためには組織の意思決定層を含めた体制を構築することが必要である。

次の事項は、事前に決めておくべき項目の例となる。

- ① インシデント発生が疑われる不審な事象が確認された場合の対処の手順や報告手順の整理
- ② 調査対象システムの保全方法(メモリダンプ、ディスクイメージの取得等)の整備
- ③ システム停止やネットワーク遮断など、業務に大きな影響を与える対処の判断方法の明確化

(3) データ・システムのバックアップ

事業継続のため、データやシステムのバックアップを行う。ランサムウェアの影響は、感染端末のみならず、感染端末からアクセス可能な別の端末やクラウド上のデータにも及ぶ可能性があるため、データをバックアップする際には、次の点に留意する必要がある。

- ① 重要なファイルは、定期的にバックアップを取得する。
- ② バックアップに使用する装置・媒体は、バックアップ時及びバックアップデータの戻し時のみ対象機器と接続する。
- ③ バックアップ中に感染する可能性を考慮し、バックアップに使用する装置・媒体は複数用意する。
- ④ バックアップの妥当性(バックアップが正常に取得できているか、現状のバックアップ手法が攻撃に対して有効か)を定期的に確認する。
- ⑤ データのみならず、システムの再構築を含めた復旧計画を策定する。

(4) 情報窃取とリークへの対策

情報が窃取され、公開される脅威については、次のような対策が考えられる。

- ① IRM (Information Rights Management) 等の情報漏えい対策(情報が窃取されても被害を限定的な範囲に留める対策)を導入する。
- ② 重要データを取り扱うコンピュータを接続するネットワークと一般職員が扱うパソコンを接続するネットワークを別のネットワークアドレスにするなどによりネットワーク経由での侵害範囲拡大に対するハードルを上げる。

(5) 医療情報システム等のセキュリティ対策

医療情報システム等では、安定稼働が優先され、閉域ネットワークであることを理由に、端末やアプリケーションへのセキュリティパッチの適用が見送られることがある。しかし、過去には、業務上の必要性により持ち込んだUSBメモリを介した感染事例や保守のために持ち込んだ端末が既にコンピュータウイルスに感染していて、そこから感染が拡大した事例がある。

また、医療情報システムを閉域ネットワークで運用している場合においても、医療機器業者が緊急保守等のために用意したリモートアクセス回線を限定的に使用させたこと等により、そこから感染した事例もある。

このため、医療機器の製造販売業者やシステムの保守業者にセキュリティパッチの適用による影響を確認し、セキュリティパッチを適用する。

(6) その他医療機器のサイバーセキュリティ対応に係る留意点

医療機器のサイバーセキュリティ対応については、医療機器の製造販売業者向けに、「医療機器のサイバーセキュリティの確保に関するガイダンスについて」

(平成 30 年 7 月 24 日付け薬生機審発 0724 第 1 号、薬生安発 0724 第 1 号厚生労働省医薬・生活衛生局医療機器審査管理課長、医薬安全対策課長連名通知)(別添 3 参照) 及び「国際医療機器規制当局フォーラム(IMDRF)による医療機器サイバーセキュリティの原則及び実践に関するガイダンスの公表について」(令和 2 年 5 月 13 日付け薬生機審発 0513 第 1 号・薬生安発 0513 第 1 号厚生労働省医薬・生活衛生局医療機器審査管理課長、医薬安全対策課長連名通知)(別添 4 参照)が発出されている。

また、医療機器プログラムにおけるセキュリティアップデートやセキュリティパッチ対応等を実施するにあたっては、「医療機器プログラムの一部変更に伴う軽微変更手続き等の取扱いについて」(平成 29 年 10 月 20 日付け薬生機審発 1020 第 1 号厚生労働省医薬・生活衛生局医療機器審査管理課長通知)(別添 5 参照)等において、医療機器としての使用目的又は効果及びその性能に影響を与えない範囲においては、簡略化した薬事手続きにより迅速に対応できるとされており、医療機器プログラム以外の医療機器の薬事手続きにおいても参考にすることができる。

なお、個別の医療機器のサイバーセキュリティ対応に係る薬事手続きについては、必要に応じ、独立行政法人医薬品医療機器総合機構又は登録認証機関に相談すること。

近年の医療機関を標的としたランサムウェア攻撃の状況

＜国内の事例＞

- ① 2018年10月16日、宇陀市立病院で、ランサムウェアにより電子カルテシステムが使用不可能となった。電子カルテシステムは同月18日に復旧したが（この間、紙カルテにより診療継続）、一部患者（1,133名）の医療情報が参照できない状態となった（2019年3月に復旧）。
また、発生月の診療報酬請求に影響を及ぼし、福祉医療費助成制度等に基づく償還に遅れが生じた。
なお、システム復旧を優先する一方、証拠保全を行わないまま医療情報システムの再セットアップが行われたことで、正確な原因究明ができない状況となった。
- ② 2020年12月2日、福島県立医科大学付属病院は、2017年にランサムウェアによる放射線撮影装置の不具合で放射線画像の再撮影に至った事案が2件あったことを公表した。

＜海外の事例＞

- ① 2021年3月17日、オーストラリアのメルボルンの医療機関イースタンヘルスは、ランサムウェアに起因するインシデントで、ITシステムが一時停止したことを公表した。
イースタンヘルスは、総病床1,514のメルボルン地域最大の医療機関である。同医療機関のCIOは3月16日のインシデント認知時に、全てのITシステムをシャットダウンした。同時に緊急度の低い手術は延期された。3月末までにかけて徐々にシステムを復旧したが、それまでは紙と手作業により業務を進めていた。
- ② 2021年5月1日、米国サンディエゴの病院で、ランサムウェアにより、ITシステムが使用できなくなり、重症患者は近隣の病院への転院を余儀なくされた。6月1日同病院は、14万7千人の患者、職員、医療関係者の個人情報と機密情報の漏洩の可能性を公表した。同日時点で、復旧は完了していない。
- ③ 2021年5月14日、アイルランドの医療サービスを行う会社で、ランサムウェアにより、医療記録が閲覧できなくなった。当該企業は影響が拡大することを懸念して、全ITシステムを停止した。6月4日時点で復旧は完了していない。この間、患者の治療への影響が発生している。
- ④ 2021年5月18日、ニュージーランドのワイカト地区保健局で、ランサムウェアにより通信回線が使えなくなり、X線写真の伝送に不具合が発生した。同保険局は、身代金を払わないと判断し、システムの復旧作業を開始したが、6月2日時点のデータの復旧は半分程度である。

2021年4月30日

内閣官房内閣サイバーセキュリティセンター

ランサムウェアによるサイバー攻撃に関する注意喚起について

2021年4月30日、内閣サイバーセキュリティセンターは、重要インフラ事業者等に向けて、ランサムウェアによるサイバー攻撃について注意喚起を行いました。

本件は、日本国内においても、ランサムウェアの感染により、データが暗号化されたり、業務情報や個人情報などが窃取されたりする事例が相次いで確認されていることから、重要インフラ事業者等の十全なサイバーセキュリティ確保のための注意喚起ですが、広く一般にも活用していただけるよう公開するものです。

なお、万が一被害に遭った場合は、被害拡大防止の観点から、一人で解決しようとせず、警察など関係機関に御相談ください。

資料：ランサムウェアによるサイバー攻撃に関する注意喚起

本件に対する問い合わせ先
内閣サイバーセキュリティセンター(NISC)
電話：03-5253-2111(代表)
重要インフラ第2グループ