事　務　連　絡
令和４年 11 月 10 日

各都道府県衛生主管部（局）　御中

厚生労働省医政局特定医薬品開発支援・医療情報担当参事官室
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

医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起）

今般、大阪急性期・総合医療センター（以下「センター」という。）において、ランサムウェアによるサイバー攻撃事案が発生し、電子カルテの閲覧・利用ができなくなる等により、地域の医療提供体制に影響が出ているところです。医療機関を攻撃対象とする同種攻撃は近年増加傾向にあり、その脅威は日増しに高まっています。

厚生労働省では、センターに専門家チームを派遣して、原因の調査と復旧支援を行っていますが、攻撃の侵入経路は、医療機関自身のシステムではなく、院外の調理を委託していた事業者のシステムを経由したものである可能性が高いことが判っています。

医療機関においては、保有する医療情報の安全を確保するため、「医療情報システムの安全管理に関するガイドライン」（以下「ガイドライン」という。）等に基づき、必要な対策を講じていただいているところですが、今般のセンターにおける事案も踏まえると、医療機関自身のシステムにおけるサイバーセキュリティ対策に加え、サプライチェーンとの接続状況や、取引先システムのサイバーセキュリティ対策等をも俯瞰しつつ、必要な対策を講じていくことが求められています。

こうした状況を踏まえ、管内、管下の医療機関に対し、同種のサイバー攻撃に備え、令和３年６月 28 日付事務連絡「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（注意喚起）」（参考）に加え、下記の対策が適切に講じられているか確認を要請するとともに、万が一、サイバー攻撃を受けた場合にも事業継続計画等により地域住民への医療提供体制に支障が出来ることのないよう注意喚起をお願いします。

また、内閣サイバーセキュリティセンターにおいて、ランサムウェア対策に関する特設サイトを作成しているので、必要に応じてご活用下さい。

記

１　サプライチェーンリスク全体の確認

上記の通り、自組織のみならずサプライチェーン全体を俯瞰し、発生が予見されるリスクを医療機関等自身でコントロールできるようにする必要があることから、関係事業者のセキュリティ管理体制を確認した上で、関係事業者とのネットワーク接続点（特にインターネットとの接続点）をすべて管理下におき、脆弱性対策を実施する。

２　リスク低減のための措置

〇パスワードを複雑なものに変更し、使い回しをしない。不要なアカウントを削除しアクセス権限を確認する。多要素認証を利用し本人認証を強化する。

〇IoT 機器を含む情報資産の保有状況を把握する。

〇VPN 装置を含むインターネットとの接続を制御するゲートウェイ装置の脆弱性は、攻撃に悪用される可能性があるので、セキュリティパッチ（最新のファームウェアや更新プログラム等）を迅速に適用する。

〇悪用が既に報告されている脆弱性については、ログの確認やパスワードの変更など、開発元が推奨する対策が全て行われていることを確認する。

〇VPN 機器に対する管理インターフェースのインターネット上の適切なアクセス制限を実施する。

〇メールの添付ファイルを不用意に開かない、URL を不用意にクリックしないこと。不審メールは、連絡・相談を迅速に行い組織内に周知する。

３　インシデントの早期検知

〇サーバ等における各種ログを確認する。(例:大量のログイン失敗の形跡の有無)

〇通信の監視・分析やアクセスコントロールを再点検する。(例：不審なサイトへのアクセスの有無)

４　インシデント発生時の適切な対処・回復

〇サイバー攻撃を受け、システムに重大な障害が発生したことを想定した事業継続計画が策定する。

〇データ消失等に備えて、データのバックアップの実施及び復旧手順を確認する。

〇インシデント発生時に備えて、インシデントを認知した際の対処手順を確認し、外部関係機関への連絡体制や組織内連絡体制等を準備する。

〇インシデント発生時及びそのおそれがある場合には、速やかに厚生労働省等の関係機関に対し連絡する。

５　金銭の支払いに対する対応

厚生労働省としては、サイバー攻撃をしてきた者の要求に応じて金銭を支払うこ

とは、犯罪組織に対して支援を行うことと同義と認識しており、以下の観点により金銭の支払いは厳に慎むべきである。

〇金銭を支払ったからと言って、不正に抜き取られたデータの公開や販売を止めることができたり、暗号化されたデータが必ず復元されたりする保証がないこと。

〇一度、金銭を支払うと、再度、別の攻撃を受け、支払い要求を受ける可能性が増えること。

６　ランサムウェア特設ページ

https://security-portal.nisc.go.jp/stopransomware/

■医療機関等がサイバー攻撃を受けた場合等の厚生労働省連絡先

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

※迷惑メール防止のため、メールアドレスの一部を変えています。

「×」を「@」に置き換えてください。

（ 参 考 ）

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。

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お願いする。

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ったては、「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。

別添１

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。

別添2

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

ランサムウエ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、ランサムウエ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、ランサムウエアの感染により、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：ランサムウエ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

2021 年 4 月 30 日

内閣サイバーセキュリティセンター
重要インフラグループ

ランサムウエアによるサイバー攻撃に関する注意喚起

ランサムウエアによるサイバー攻撃に対する対応策を講じ、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に務めてください。

1. 概要

ランサムウエアによるサイバー攻撃が活発になっており、日本企業や海外子会社で実際に攻撃者にデータが公開される事例が増えており、クライアント端末だけでなくサーバーも被害を受けています。

ランサムウエア感染によるデータの暗号化、業務情報や個人情報の窃取等の被害は、経済・社会に大きな影響を与えることを踏まえ、予防策、感染した場合の緩和策、対応策等を検討してください。

対策は、予防、検知、対応、復旧の観点から行う必要があります。以下、具体的な対応策の例を示すので、参考にしてください。

① 【予防】ランサムウエアの感染を防止するための対応策
② 【予防】データの暗号化による被害を軽減するための対応策
③ 【検知】不正アクセスを迅速に検知するための対応策
④ 【対応・復旧】迅速にインシデント対応を行うための対応策

2. 具体的対応策

(1) 【予防】ランサムウエアの感染を防止するための対応策

最近のランサムウエアの侵入経路は以下のようなものがあり、これらを踏まえた予防策が必要です。

① インターネット等の外部ネットワークからアクセス可能な機器の脆弱性によるもの
② 特定の通信プロトコル(RDP や SMB)や既知の脆弱性を悪用した攻撃によるもの[1]
③ 新型コロナウイルス感染症対策として急遽構築したテレワーク環境の不備によるもの
④ 海外拠点等セキュリティ対策の弱い拠点からの侵入によるもの
⑤ 別のマルウエアの感染が契機となるもの

[1] *US-CERT(Twitter)「US-CERT(@USCERT_gov)の投稿(2021/4/29)」、https://twitter.com/USCERT_gov/status/1387435697037094919 (2021/4/30 閲覧)*

チェックポイント

- インターネット等外部ネットワークからアクセス可能な機器については、外部ネットワーク公開の必要性を十分検討したうえで、セキュリティパッチを迅速に適用する、外部からの管理機能、不要なポート(137(TCP/UDP)、138(UDP)、139(TCP)、445(TCP/UDP)、3389(TCP/UDP)など)やプロトコルを外部に開放しない等の対応策等、IT資産管理を改めて確認する。特に、通信プロトコル「SMB」や「RDP」については、これまでも必要最小限のポートの開放やSMBv1の無効化等を呼びかけているところ、ファイアウォールを含む各機器の設定を改めて確認する。
- ソフトウエアや機器等の脆弱性については、ランサムウエアを用いる攻撃者グループによる悪用が報告されているものを含む以下の脆弱性に十分留意する。
  - Fortinet製Virtual Private Network(VPN)装置の脆弱性(CVE-2018-13379)[2]
  - Ivanti製VPN装置「Pulse Connect Secure」の脆弱性(CVE-2021-22893、CVE-2020-8260、CVE-2020-8243、CVE-2019-11510)[3]
  - Citrix製「Citrix Application Delivery Controller」「Citrix Gateway」「Citrix SD-WAN WANOP」の脆弱性(CVE-2019-19781)[4]
  - Microsoft Exchange Serverの脆弱性(CVE-2021-26855等)[5]
  - SonicWall Secure Mobile Access (SMA) 100シリーズの脆弱性(CVE-2021-20016)[6]
  - QNAP Systems製NAS(Network Attached Storage)製品「QNAP」に関する脆弱性(CVE-2021-28799、CVE-2020-36195、CVE-2020-2509等)[7]
  - Windowsのドメインコントローラーの脆弱性(CVE-2020-1472等)[8]
- テレワーク等に関連し、職場から持ち出したPCについて、休暇中に長期間、十分な管理下になかったPCを職場で再び利用する際は、パッチの適用やウイルススキャンの実施など必要に応じて実施する。
- 最近では、マルウエア「Emotet」に代わり、マルウエア「IcedID」に感染させる不正なメール等も確認されていることから、ウイルス対策ソフトの導入及び最新化、定期スキャンの実施、メール環境に対するセキュリティ対策等、通常のマルウエア対策も実施する。

---

[2] *NISC「Fortinet製VPNの脆弱性(CVE-2018-13379)に関する重要インフラ事業者等についての注意喚起の発出について(2020/12/3)」、https://www.nisc.go.jp/active/infra/pdf/fortinet20201203.pdf (2021/4/30閲覧)*

[3] *Ivanti「Pulse Connect Secure Security Update(2021/4/20)」、https://blog.pulsesecure.net/pulse-connect-secure-security-update/ (2021/4/30閲覧)*

[4] *Citrix「CVE-2019-19781 - Vulnerability in Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP appliance(2020/10/23)」、https://support.citrix.com/article/CTX267027 (2021/4/30閲覧)*

[5] *Microsoft「On-Premises Exchange Server Vulnerabilities Resource Center(2021/3/25)」、https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/ (2021/4/30閲覧)*

[6] *SonicWall「CONFIRMED ZERO-DAY VULNERABILITY IN THE SONICWALL SMA100 BUILD VERSION 10.X(2021/4/30)」、https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001 (2021/4/30閲覧)*

[7] *QNAP Systems「Response to Qlocker Ransomware Attacks: Take Actions to Secure QNAP NAS(2021/4/22)、https://www.qnap.com/en/security-news/2021/response-to-qlocker-ransomware-attacks-take-actions-to-secure-qnap-nas (2021/4/30閲覧)*

[8] *Microsoft「CVE-2020-1472 Netlogon の特権の昇格の脆弱性(2021/2/9)」、https://msrc.microsoft.com/update-guide/ja-jp/vulnerability/CVE-2020-1472 (2021/4/30閲覧)*