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。

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)*

(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

従来のランサムウエア対策の常套手段であったバックアップは、引き続き有効です。これに加え、2重脅迫ランサムウエアに感染した場合は、組織の機微データや個人情報流出の懸念があることから、「機微データの厳格管理」については、改めて検討する必要があります。

チェックポイント

- 重要なデータに対する定期的なバックアップの設定を確認する。バックアップの検討に当たっては、ランサムウエア感染時でもバックアップが保護されるように留意する。例えば、ファイルのコピーを3個取得したうえで、ファイルは異なる2種類の媒体に保存、コピーのうち、1個はクラウドサービスや保護対象のネットワークからアクセスできない場所等に保管するといった対策等を検討する。
- バックアップデータから実際に復旧できることを確認する。
- 公開された場合、実際に支障が生じるような機微データや個人情報等に対して、特別なアクセス制御や暗号化を実施する。
- システムの再構築を含む復旧計画が適切に策定できていることを確認する。

(3)【検知】不正アクセスを迅速に検知するための対応策

不正アクセスを迅速に検知するための対応策が必要です。迅速な検知を実現するためには、オペレーターとマシンによる自動化を検討する必要があります。

チェックポイント

- サーバー、ネットワーク機器、PC等のログの監視を強化する。
- 振る舞い検知、EDR(Endpoint Detection and Response)、CDM(Continuous Diagnostics and Mitigation)等を活用する。

(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

ランサムウエアによる攻撃の被害を受けた場合でも、冷静で適切な対応ができるように、組織一丸となった対処態勢を構築する必要があります。

チェックポイント

- データの暗号化、公開、インターネット公開サーバーに対するDoS攻撃等を想定した対処態勢、対処方法、業務継続計画等を含むランサムウエアへの対応計画が適切に策定できているか確認する。
- 一部の職員が長期休暇中やテレワーク等であっても、職員がランサムウエア感染の兆候を把握した場合、職員が迅速にシステム管理者に連絡できることを確認する。
- ランサムウエアの感染による被害を受けた場合に、組織内外(業務委託先、関係省庁を含む)に迅速に連絡できるよう、連絡体制を確認する。

参考 URL

- ランサムウエアによるサイバー攻撃について【注意喚起】(NISC)
  https://www.nisc.go.jp/active/infra/pdf/ransomware20201126.pdf
- 【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について(IPA)
  https://www.ipa.go.jp/security/announce/2020-ransom.html
- CISA and MS-ISAC Release Ransomware Guide(CISA)
  https://us-cert.cisa.gov/ncas/current-activity/2020/09/30/cisa-and-ms-isac-release-ransomware-guide
- 大型連休等に伴うセキュリティ上の留意点について(NISC)
  https://www.nisc.go.jp/active/infra/pdf/renkyu20210426.pdf
- 最近のサイバー攻撃の状況を踏まえた経営者への注意喚起(経済産業省)
  https://www.meti.go.jp/press/2020/12/20201218008/20201218008-2.pdf
- 「EMOTET」後のメール脅威状況：「IcedID」および「BazarCall」が３月に急増（トレンドマイクロ）
  https://blog.trendmicro.co.jp/archives/27732
- So Unchill - UNC2198 ICEDID のランサムウェア・オペレーションへの融解(FireEye)
  https://www.fireeye.com/blog/jp-threat-research/2021/02/melting-unc2198-icedid-to-ransomware-operations.html
- 2021 年も増加傾向のランサムウェア、被害に関する共通点とは(LAC)
  https://www.lac.co.jp/lacwatch/report/20210405_002585.html
- UNC2447 SOMBRAT and FIVEHANDS Ransomware: A Sophisticated Financial Threat(FireEye)
  https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html

薬生機審発０７２４第１号
薬生安発０７２４第１号
平成３０年７月２４日

各都道府県衛生主管部（局）長　殿

厚生労働省医薬・生活衛生局医療機器審査管理課長
（　　公　　印　　省　　略　　）

厚生労働省医薬・生活衛生局医薬安全対策課長
（　　公　　印　　省　　略　　）

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

医療機器のサイバーセキュリティの確保に関しては、「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」（平成 27 年４月 28 日付け薬食機参発 0428 第１号、薬食安発 0428 第１号　厚生労働省大臣官房参事官（医療機器・再生医療等製品審査管理担当）、厚生労働省医薬食品局安全対策課長連名通知）において、医療機器の安全な使用を確保するために、医療機器に関するサイバーリスクに対する適切なリスクマネジメントを実施し、必要な対応を行うよう、関係事業者等に対する周知を依頼しているところです。

今般、さらに具体的なリスクマネジメント及びサイバーセキュリティ対策について、平成 29 年度日本医療研究開発機構医薬品等規制調和・評価研究事業「医療機器に関する単体プログラムの薬事規制のあり方に関する研究」の研究報告を基に、「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」として別添のとおり取りまとめました。つきましては、医療機器のサイバーセキュリティの確保に当たって、同ガイダンスを参考として、必要な対応を行うよう、貴管下関係事業者等に周知方お願いいたします。

別添

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

背景

「サイバーセキュリティ基本法」（平成 26 年法律第 104 号）に基づき、内閣に「サイバーセキュリティ戦略本部」、内閣官房に「内閣サイバーセキュリティセンター」が平成 27 年 1 月に設置され、「サイバーセキュリティ戦略」が平成 27 年 9 月 4 日に閣議決定された。

「サイバーセキュリティ」は、サイバーセキュリティ基本法第2条において、「電子的方式、磁気的方式その他人の知覚によっては認識することができない方式により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体）を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていること」と定義されている。またサイバーリスクとは、そうした安全性や信頼性が損なわれ、危害（harm）（※1）が生じるリスクと考えられる。

医療に関するサイバーセキュリティ対応に関しては、医療機関等の医療情報システムについて、平成 17 年3月、厚生労働省から「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、「安全管理ガイドライン」という。）第 1 版を示し、情勢に応じた随時の改定を経て、平成 29 年 5 月の第 5 版に至っている。

また、医療機器のサイバーセキュリティについては、厚生労働省から「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」（平成 27 年 4 月 28 日付け薬食機参発 0428 第 1 号・薬食安発 0428 第 1 号厚生労働大臣官房参事官（医療機器・再生医療等製品審査管理担当）、厚生労働省医薬食品局安全対策課長連名通知。以下、「サイバーセキュリティ通知」という。）にて、医療機器製造販売業者（以下、「製造販売業者」という。）に対し医療機器へのサイバーセキュリティ対応の考え方を示している。

製造販売業者は、有効性及び安全性を確保した医療機器を設計・製造して供給することを責務としており、加えて、医薬品、医薬部外品、化粧品、医療機器及び再生医療等製品の製造販売後安全管理の基準に関する省令（平成 16 年厚生労働省令第 135 号。以下、「GVP 省令」という。）に基づき、販売後の使用における医療機器の有効性、安全性等に関する情報収集・分析、必要に応じた対策等、適切な対応が求められている。このため、製造販売業者は医療機器への悪意を持ったサイバー攻撃に対しても、使用環境を含めた医療機器の特徴に応じて、サイバーセキュリティ対応にも取り組んでいく必要がある。

一般的に、情報セキュリティには、情報の機密性、完全性及び可用性の3つの要素を確保することが求められる。機密性（Confidentiality）とは、正当な権限をもつ限られた者のみ

が、許可された範囲内で情報にアクセスできるよう、保護・管理されていることを指す。完全性（Integrity）とは、データの正当性、正確性及び一貫性が維持され、不適切な変更が行われていないことを意味し、意図された使用方法の下で医療機器の機能や性能が確保され、患者情報や診断結果等の正確性が保たれていることを指す。そして可用性（Availability）とは、必要なときにシステムが正確なサービスを提供できる状態が維持されていることを指す。

これらの要素を満たすべく、サイバーリスクに対するリスクマネジメントを考える際には、従来行われてきた、一次故障や誤操作等をリスク要因として捉えるリスクマネジメントに加えて、悪意を持った攻撃者の存在等もリスク要因として捉えて検討することが必要となる。

（※1　医療機器のリスクマネジメントの規格である JIS T 14971:2012 では、危害（harm）を「人の受ける身体的傷害若しくは健康障害、又は財産若しくは環境の受ける害」と定義している。本ガイダンスでは、患者や医療機器の使用者に対する安全性に係る危害を第一に想定しているが、医療機器の製造販売業者は個人情報の漏洩等の危害についても十分な対応をすることが社会的に求められていることに十分に留意すべきである。）

1.目的

本ガイダンスの目的は、サイバーセキュリティ通知により示された製造販売業者が行うべきサイバーセキュリティへの取組について、医療機器への開発・設計（市販前）及び市販後の対応をより具体的にするための情報を提供することである。製造販売業者が本ガイダンスを参考に適切な対応を実施することによって、サイバーセキュリティに関するリスクの低減、医療機器本来の有効性及び安全性の確保が図られ、患者へのリスクの低減に繋がる。

なお、サイバーセキュリティの分野は攻撃方法の多様化・巧妙化等の状況の変化が著しいことから、サイバーセキュリティの対策は、本ガイダンスに示したものに限らず、技術動向等を踏まえて適切な対策を取るべきことに十分留意することが必要である。

2.検討が必要となる医療機器及び使用環境の特定

本ガイダンスは、サイバーセキュリティに関するリスクが想定される医療機器を対象とするものであり、医療機器の全てを対象とするものではない。サイバーセキュリティに関する対応が必要な医療機器に該当するかは、機器の特性及びその使用環境等を特定し検討することが必要である。

医療機器におけるサイバーリスクのうち、医療機器を用いた診療を受ける者（患者）及び医療機器の使用者に対する障害に係るリスクは、優先的に対応することが必要である。

2.1 対象となる医療機器

本ガイダンスの対象は、医療機器のうちプログラムを使用したもの（医療機器プログラムを含む。）及び付属品等にプログラムを含むものである。医療機器のクラス分類（Ⅰ～Ⅳ）を問わない。

基本的に、医療機器と接続して使用する又は併用される IT 機器等（単体で医療機器に該当しないもので、プログラム単体の場合を含む。）を医療機器の構成品（付属品等）として提供する場合は、本ガイダンスの対象となる。

2.2 医療機器の使用環境の特定

各医療機器に係るサイバーリスクを想定するためには、当該医療機器の使用環境を特定することが必要となる。また、使用環境だけでなく、医療機器を構成するユニット間又は複数の医療機器で構成されるシステムにおいて、医療機器間でインターネット等（無線等含む）を利用し、制御信号あるいはデータ交換を行う場合についても考慮することが必要となる。

医療機関等においては、「安全管理ガイドライン」を踏まえた安全管理が求められていることに留意すること（例えば、アクセス管理、通信の暗号化等。）。

なお、特定した使用環境に関する情報は、使用者等へ情報提供する必要がある（5．参照）。

2.2.1 医療機関での使用環境

多くの医療機器は医療機関内で使用されており、また、医療機関の医療情報システムに関しては「安全管理ガイドライン」を踏まえた安全対策及び管理が求められている。したがって、医療機関での使用を意図する医療機器の場合は、「安全管理ガイドライン」で求められる環境での使用を基本とする。

2.2.2 医療機関の管理が及ばない使用環境

例えば、在宅医療で使用される医療機器の場合、医療機関による管理が十分に及ばない環境で使われることに留意する必要がある。

在宅医療で使用する医療機器や家庭用の医療機器の開発においては、当該医療機器の使用環境を明確化し、医療機関の管理が及ばない使用環境での使用を意図した場合は、「安全管理ガイドライン」を踏まえた管理の及ばない環境であることを考慮する必要がある。

2.2.3 その他の使用環境（特定が困難）

体内植込み機器や装着機器等の多くは、患者の移動に伴い様々な場所に移動する。こ

のため、想定される多様な環境での使用時におけるサイバーリスク等を評価し、その危険性等についても留意すること。

2.3 医療機器のネットワーク等への接続

医療機器における通信機能・ネットワークへの接続や USB 等のポートの利用に応じたサイバーリスクの検討が必要となる。

2.3.1 ネットワーク等への接続機器

医療機器が接続されるネットワークを踏まえた検討が必要である。医療機関内に限定され、インターネット回線と分離された環境で使用される機器と、インターネット回線への接続を意図する機器では、使用環境が異なっており、接続環境に応じた対応が必要となる。

ネットワーク通信により医療機器内の情報を送受信したり、操作したりすることが可能な医療機器については、より慎重にサイバーセキュリティ対応を考慮すべきである。なお、ネットワーク接続を利用するリモートメンテナンス等の保守機能を持つ医療機器についても同様である。

2.3.2 無線通信等利用の医療機器

無線通信（医療用無線周波数帯域、Bluetooth、Wi-Fi 等）を利用し、医療機器のユニット間又は医療機器間で制御信号や情報交換をする機能を有する機器に関しては、利用している技術及び使用する機器の種類におけるリスクに応じた配慮が必要となる。

2.3.3 USB 等の外部入出力ポート

USB ポートや CD/DVD ドライブ等を備え、使用可能な状態にある医療機器に関しては、これらを使用した場合のリスクへの対応が必要となる。

3.サイバーセキュリティ対応

医療機器に係るサイバーセキュリティへの対応については、製造販売業者による対応はもちろんのこと、使用者側における当該医療機器の適切な使用、維持管理、「安全管理ガイドライン」に基づく情報システムの維持管理等日常の適切な管理が重要である。

なお、サイバーセキュリティへの対応に当たっては、関連のガイダンス、規格、技術文書、その他の方法等の最新の情報を参考にしながら、医療機器の使用環境を踏まえ実施する必要がある。（巻末の「参考資料等」及び「規格、規格文書等」を参照。）

3.1 製造販売業者によるサイバーセキュリティ対応

製造販売業者は、意図される使用環境におけるサイバーリスクに対するリスクマネジメントを実施し、必要な対策を行い、その結果リスクが受容可能になることを説明できるようにすること。リスクマネジメントを行うに当たっては、医療機器の意図される使用方法、使用者、使用環境等を考慮したベースラインを定めて実施、検証することが望ましい。

特に、医療機器の開発・評価時に使用されるデータベースや、実使用時に利用される OS 等の既製品ソフトウェアについても、医療機器のライフサイクル(※2)を通じ考慮する必要がある。なお、これら既製品ソフトウェアを用いた医療機器のライフサイクルと搭載した当該既製品ソフトウェアのライフサイクルについては、整合させることが望ましいが、困難である場合には、その対応について検討を行い、必要に応じて使用者へ必要な情報を提供する(5項参照)。

なお、製造販売業者は、供給する製品のサイバーセキュリティ対応に関する社内の方針・体制を品質システム等の一部として確立することが求められる。また、サイバーセキュリティに関連する問合せ窓口及びサービスに係る取組について、使用者へ開示することが望ましい。

(※2 ライフサイクルとは、開発から使用を終了し破棄されるまでが本来の期間ではあるが、これとは別に医療機器の設計・製造時には耐用期間が特定されている。各医療機器の耐用期間については、通常、添付文書に「保管方法及び有効期間等」として記載されており、製造販売業者は、少なくともこの期間は、当該医療機器についてサイバーセキュリティへの対応を行うことが必要となる。また、既出荷製品について適切な脆弱性管理ができない場合、製造販売業者は、製品の扱いに関する情報を使用者へ速やかかつ適切に伝えるとともに、使用者と連携して対応することも必要となる。)

3.2 使用者によるサイバーセキュリティ対応

製造販売業者から出荷された医療機器は、販売業者・貸与業者を経て、医療機関等の使用者に納入される。納入後の医療機器のサイバーセキュリティに関する日常の管理は、医療機関等の使用者にて実施する必要があることから、製造販売業者は、必要に応じて医療機関と連携を取り、保守契約等に基づきサイバーセキュリティの確保を支援することが重要である。なお、医療機器から医療機関等の情報システムへ転送されたデータに関するサイバーリスクについては、システムの管理者である医療機関による対応が必要である。

サイバーリスクに伴う医療機器の不具合等の情報も、GVP省令における安全管理情報の一つであるため、製造販売業者は、医療機関と連携を取り、こうした情報を収集する必要がある。

また、独立行政法人情報処理推進機構(IPA)セキュリティセンターでは、「コンピュータウ