

【別冊②】 初動対応時の想定対応手順

対応者	目的	☐	対応手順
発見者	感染拡大の防止と可及的かつ速やかな報告を行う。	☐ ☐ ☐ ☐	コンピュータの動作が不調な場合は、当該コンピュータの LAN ケーブルを抜線する。これには、サーバ、PC、NAS、医療機器のコントローラーなどが含まれる。速やかにシステム管理者に報告する。 脅迫状等が確認された場合は、即座に病院長、システム管理者に報告する。周辺のすべての LAN ケーブルを抜線する。 対象のコンピュータが感染していることが分かるように、目印となるシール等を貼り、電源を切らないように保全を行う。 システムの表示画面をスマートフォン等で撮影し、システム管理者に共有する。
対策本部長・対策副本部長	的確な判断をするための情報の収集、関係者の健康の維持、混乱した状況での新たなインシデント誘発の防止	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	対策本部の設置を宣言し、事務局に対してクロノロジーの作成を指示する。 システム管理者の報告に基づき、被害範囲を特定し、診療行為への影響度を確認する。 外来、救急の受入、手術、検査実施の可否を判断し、対外連絡と広報方針を決定する。 医療担当と紙カルテ運用の可否を判断し、医師、看護師、スタッフに指示をする。 転院が必要な入院患者を確認し、地域医師会、地域病院会との連携を要請する。 当日以降、手術、検査が予定されていた患者・家族への説明方針を決定し、診療科、部門での対応を指示する。 翌日以降の外来患者への対応方針を決定し、診療科、部門での対応を指示する。 紙カルテ運用を開始した場合は、課題やインシデントについて調査を指示し、対応を検討する。 特定の従事者に過負荷がかからないよう、ローテーションと休憩に配慮するよう、診療科、部門に指示をする。またメンタルには十分に留意する。 対策本部長と副本部長は適宜、交代する。 外来手術等の再開に向けた、必要な情報の収集と指示
総務課 広報担当	積極的な情報公開に基づく取材攻勢の鎮静化、患者・家族の不安を	☐ ☐ ☐	救急受入停止の場合は、消防本部に連絡する。 厚生労働省医政局に初動対応支援の依頼を連絡する(必要時)。 所轄官庁、自治体、医師会、地域連携等に診療制限の状況を連絡する。

	取り除くためのコミュニケーションとイメージダウンの最小化	☐ ☐ ☐ ☐	・救急、外来、手術の受入可否 ・地域連携の停止状況 入院患者、入院予定者、手術予定者、外来患者、家族向けの案内文を作成し、病院スタッフへ周知する。特に、入院予定者、手術予定者へは、医師からの説明が納得感がある事に留意する。 第1報を大学本部にプレスリリースを要請する。 記者会見の会場を確保する。 想定問答集を作成する。
システム管理者・担当者 (サイバー事象対応担当)	復旧にかかる期間を算定するための材料を収集する。 そのため、被害範囲の特定と、復旧時にコンピュータを初期化する必要があるかの状況を把握する。	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	【留意事項】 市販のVPNソフト等のバックドアソフトを設置するケースが散見される。市販製品の場合、ウイルス対策ソフトでの検知は不可能となるため、再び侵入され攻撃される可能性が残る。 セグメント間でのSyslogや、Windows SMB関連ログを分析すれば、通信のなかったセグメント、コンピュータに関しては、初期化等の作業が不要となる。 一方で、作業員とツールが確保できれば、初期化して復旧が早くなる場合もある。意思決定にあたっては、セキュリティベンダーの助言を得て、対策本部として意思決定できる情報を多く得ることが重要である。 インターネット接続を停止する。 基幹スイッチでセグメントごとに抜線し、セグメント間の拡大拡散を防止する。 脅迫状(ランサムノート)を確認し攻撃者集団を特定する。可能な場合、脅迫状のスクリーンショットを書き換え困難なCD-R、DVD等、もしくはUSBメモリに保存する。 可能であれば、Enterprise Admin、Domain Admin、Administrators及びBuilt-In Administratorのパスワードを16桁以上の長いパスフレーズに変更する。プログラムがAdmin「administrator」アカウントとパスワードを使用している場合、影響が及ぶ可能性があるため、留意する。 可能な範囲で、Active Directory、病院情報システムサーバーのWindowsログ(C:\Windows\System32\winevt以下のファイル全て)とFirewall、ルーターのSyslogを書き換え困難なCD-R、DVD等、もしくはUSBメモリに保存する。 オフラインバックアップの伏況を確認し、汚染等がない事を確認し、何時時点でのデータから復旧できる事を確認し、関係者に共有する。

		☐ 脅迫状の表示されたコンピュータ(暗号化されたシステム)を特定する。この際、サーバや PC、NAS の共有フォルダ等に暗号化ツール、ウイルスが潜んでいる可能性に十分に留意する。感染コンピュータ一覧表を作成し、コンピュータ名 IP アドレス、役割、ウイルス対策ソフトの稼働状況を一覧にする。 ☐ ウイルス対策ソフトの停止やアンインストールされているならば、攻撃ツール、暗号化ウイルスはウイルス対策ソフトで駆除できる可能性が高くなる。 ☐ 反面、管理者権限が取得されている証左となるため、RDP 等を使用した水平展開が容易となるため、RDP が許可されているコンピュータは、基本的に感染していることを想定し調査を進める。 ☐ 脅迫状の表示されたサーバ、PC のデスクトップ、Documents を調査し、不審なフォルダ、ファイル暗号化ツール、ウイルスの存在を確認する。ツールやウイルスが発見された場合は、他の機器にも同様に設置されている可能性が高いため、感染コンピュータ一覧表に、ツールやウイルスの保存先を追加記入する。 ☐ 可能な場合は、ツールやウイルスのプロパティを確認し、タイムスタンプ、ファイルサイズを取得し一覧に記入する。 ☐ セキュリティベンダーや警察と協力し、保全を開始する。 医療機器のコントローラーには、脆弱な OS で稼働している場合があるため、医療機器ベンダーの協力を得て、感染の有無を調査する。Linux や組み込み OS であっても感染しないという保証は一切ない事に留意する。 ☐ セキュリティベンダーの協力のもと、被害にあった機器の BIOS、UEFI の汚染の有無を確認する。 ☐ 初動を終え、復旧に向けた計画を策定する。 ・サーバ PC の初期化(BIOS、UEFI の初期化) ・モダリティの初期化(BIOS、UEFI、ファームウェアの初期化) ☐ バックアップからの復旧(サーバ、PC の再構築に時間がかかる場合は、参照系の復旧を優先する) 紙カルテ運用となった場合は、早期に医療現場向けのワープロ機能の提供を実施する。この際、プリンタートナー、用紙が大量に消費されることから、維持に留意する。 ☐ セキュリティベンダーの協力のもと、ランサム集団が窃取した情報を基にした 2 次脅迫を行うかを確認する。2 次脅迫の恐れがある場合は、ダークウェブの調査を開始する。
--	--	---