Aグループ　　収集コース担当

とにかく対応のワークシート（ハンドリング担当用）　　2017/8/25

想定教員のPCがランサムウェアに感染しファイルが暗号化され、この情報（相談）が情報センターに届いた。

対応のため

報告が欲しい情報

②

影響ハンイ、他部署へのえいきょう、学外への影響有無、動かないシステムの有無、
復旧までの時間（復旧できるのであれば）
＋情報ううえいの有無、

ハンドリング（上長）担当がテクニカル担当者に行う指示、注意すべき事項

・感染した人を責めないでほしい。
・学外に言いふらさない。
・優先事項（業務停止とか）。
・勝手に判断して処理を進めず、報告をしてほしい。
＋調査範囲（そのPCだけ、NW経由）
＋対応の期限

調査の前にしなければならないこと

・手順の確認。
・インシデント発生者へ、身代金支払の有無、
・PCに対して感染後何かしたか、（感染前も）を聞く。

規程、ルールで明記が必要と思われる事項

・判断できる人。
・報告基準（インシデントの内容によってどこまで報告するか）。
＋・対応者の権限の明記。　＋報告ルールとパス。

調査について

実際に行うべき事項と手段および結果

①

何がほしいか？
初期。いつ、どの端末がウイルス感染したかの確認。（対象の特定）を依頼。
＋保全するか。
＋再発防止策の作成

判断で困った（迷った）事項と理由

上位層への報告（なぜ言わなかったのか、と言われたくない）
↑タイミング。　→程度で判断するのは困難。

その他

法律上、対応や報告が必須となっているものは何か？

とにかく対応のワークシート（ハンドリング担当用）　(B)　2017/8/25

想定教員のPCがランサムウェアに感染しファイルが暗号化され、この情報（相談）が情報センターに届いた。

対応のため

報告が欲しい情報

- 被害の状況（台数、情報流出の有無と内容、ファイル重要度）
- 侵入経路、日時、（ユーザの操作）
- 対策（暫定、長期的）　・加害者像（わかっていれば）（外部の攻撃者）

ハンドリング（上長）担当がテクニカル担当者に行う指示、注意すべき事項

- 保全優先か、復旧優先か
- 調査のための権限付与（入室許可等）

調査の前にしなければならないこと

- 状況保全方法の判断
- 有線、調査のために感染した端末、ネットワークを切断しておく

規程、ルールで明記が必要と思われる事項

- 誰が判断するか　・外部への報告の方法
- 情報の重要度に応じた対応（保全か復旧か）
- 報告、連絡体制

調査について

実際に行うべき事項と手段および結果

- ユーザへのヒアリング（感染経路）　・復旧作業（バックアップ、復元）
- ランサムウェアの特定　・外部への報告
- 優先事項（保全か復旧か）に応じて行う
- ログの確認（情報流出の有無）

判断で困った（迷った）事項と理由

情報流出の有無が確定しない状態で公表するかどうか

その他

とにかく対応のワークシート（ハンドリング担当用）　Cグループ　2017/8/25

想定教員のPCがランサムウェアに感染しファイルが暗号化され、この情報（相談）が情報センターに届いた。

対応のため

報告が欲しい情報

発生の日時，ランサムウェアの要求内容、利用者からの相談内容
当内対応可否，被害内容，バックアップの有無、
原因（分かれ着ば）

ハンドリング（上長）担当がテクニカル担当者に行う指示、注意すべき事項

感染の拡大を止める，予算，保全の要否

調査の前にしなければならないこと

PCの内容の確認
対応の方針（保全を優先するか or 画除を優先するか）

規程、ルールで明記が必要と思われる事項

・対応の方針の内容
・情報資産の重要度
・権限（調査しても良いか！）
　システムの停止・復旧

調査について

実際に行うべき事項と手段および結果

・感染したランサムウェアの種類
・暗号化されたファイルの内容
・復号（旧）できるか？

判断で困った（迷った）事項と理由

・復旧できない場合の対応

その他

グループD

とにかく対応のワークシート（ハンドリング担当用）　2017/8/25

想定教員のPCがランサムウェアに感染しファイルが暗号化され、この情報（相談）が情報センターに届いた。

対応のため

報告が欲しい情報

- ファイルの種類（拡張子、数量、感染したファイルは？）
- 個人情報の有無（重要情報か？）　・共有ファイル、他のPCへの感染状況
- PCの現状（状態）
- 先生に対して、先生の運用状況（何をしたか？）（第1報として）

ハンドリング（上長）担当がテクニカル担当者に行う指示、注意すべき事項

- 復旧、調査どちらを優先させるか、両立できるか？を判断し、方針を指示
- 報告間隔の共有

調査の前にしなければならないこと

報告　テクニカル → ハンドリング → 上層部
判断して、「復旧」「調査」の優先順位を決定

規程、ルールで明記が必要と思われる事項

- 報告の手順、指示系統
- 情報資産の重要度による、対応手順

調査について

実際に行うべき事項と手段および結果

① 教員に対し聞き取り調査
② プロセスとログの解析
③ 共有ファイルの調査
④ ランサムウェアの種類
⑤ バックアップの有無、感染の状況

判断で困った（迷った）事項と理由

回復の手段と環境

その他

グループE

とにかく対応のワークシート（ハンドリング担当用）　2017/8/25

想定教員のPCがランサムウェアに感染しファイルが暗号化され、この情報（相談）が情報センターに届いた。

対応のため

報告が欲しい情報

・情報ろうえいの有無、個人情報の有無

・PCの状況把握

・ランサムウェアの特定、復号化ソフトの有無

ハンドリング（上長）担当がテクニカル担当者に行う指示、注意すべき事項

・証拠保全or現状復旧の選択

調査の前にしなければならないこと

・被害拡大の防止、端末の隔離性

規程、ルールで明記が必要と思われる事項

・初動の対応

調査について

実際に行うべき事項と手段および結果

・感染の事実確認

・事業継続、停止

・被害状況確認

判断で困った（迷った）事項と理由

その他

(F)

とにかく対応のワークシート（ハンドリング担当用）

2017/8/25

成績、入試情報、個人情報など

想定教員のPCがランサムウェアに感染しファイルが暗号化され、この情報（相談）が情報センターに届いた。

対応のため

報告が欲しい情報

発生日時、場所、対象者、被害規模→対象PCに保存されていた情報の内容に業務継続可否、対外公表の有無と（審議内容）。スピード感 よって対処変わりそう。単に暗号化されただけなのか、外部流出があるかと要確認

ハンドリング（上長）担当がテクニカル担当者に行う指示、注意すべき事項

状況調査、被害範囲の特定、暗号化解除の実現可否調査、バックアップ有無の確認 調査体制確立、対象機器の保管指示

ランサムウェアの種類の特定→個人情報、成績の漏えいが判明（代替マシンの用意含む）

調査の前にしなければならないこと

対策と実施するスピード感確定→すぐか、翌朝か、翌営業日まで待ってもよいのか。

証拠の保全、校務・NW経路断（停止までは不要そうだが、影響度による）

規程、ルールで明記が必要と思われる事項

緊急対策本部開設有無と委員の招集、委員会報告資料用意

調査について

実際に行うべき事項と手段および結果

被害状況把握

- 発生したタイミング、現況（終息しているか？途上なのか？）
- 被害範囲→教員単独か、学生の個人情報含まれているか（他大学含む）
- 犯人の目星→学内か学外か、学外の場合、侵入経路特定できるか。
- 対策・再発防止のため、学内のみで対処可能か、委託が必要であれば費用感は？

判断で困った（迷った）事項と理由

証拠の保全を優先するか、サービス復旧が優先なのか。

（資産価値に応じて判断してもよい）

原因メールの添付かサイト閲覧か調査に含むべき

その他

アクセスログを残す設定を施せば調査・解析の一助となるが、全PCに強制することは困難ではないか。

調査結果 286名分の氏名、年組・番号・カ氏名、成績が漏えいした

G

とにかく対応のワークシート（ハンドリング担当用）　2017/8/25

想定教員のPCがランサムウェアに感染しファイルが暗号化され、この情報（相談）が情報センターに届いた。

対応のため

報告が欲しい情報

- 感染端末，発覚日時（未定），暗号化されたファイルの特定（ZIP化されたもの？），対象となったデータの種別（成績情報），要求事項（身代金），

ハンドリング（上長）担当がテクニカル担当者に行う指示、注意すべき事項

- PCのログ，通信の履歴（ログ），事務部門からの指示対応？
- 情報センター職員への指示（対応）

調査の前にしなければならないこと

- ネットワークケーブル取外し可否（有無）

規程、ルールで明記が必要と思われる事項

- 判断・指示の出せる部署or管理者？

調査について

実際に行うべき事項と手段および結果

- 該当PCでの不審プログラム確認（プログラム動作）
- イベントログから実行内容確認
- 流出ファイルの特定（アクセスログより確認）

判断で困った（迷った）事項と理由

- 教員の協力が得られない事
- 調査への外部委託の可否

その他

トクブレーブ6

とにかく対応のワークシート（ハンドリング担当用）　2017/8/25

想定教員のPCがランサムウェアに感染しファイルが暗号化され、この情報（相談）が情報センターに届いた。

対応のため

報告が欲しい情報

- いつ漏洩したか
- 漏洩内容
- 影響範囲
- ウイルスの種類
- 復元可否
- 現状

ハンドリング（上長）担当がテクニカル担当者に行う指示、注意すべき事項　情報資産の重要性によって

- 勝手に判断しない
- 定期的な報告をお願いする
- ログを消さない（残す）ようにする
- NW遮断の実施可否を指示する

調査の前にしなければならないこと

- 対象端末PC LANケーブル抜線
- 関係者へ報告
- 連絡網を整備しておく
- 調査ツールでログ取得

規程、ルールで明記が必要と思われる事項

- 指揮命令系統を明確にしておく、
- 報告用フォーマットを作成しておく、
- NW遮断条件を決めておく

調査について

実際に行うべき事項と手段および結果

- プロセス確認ツールを使用する。⇒各種ログを取得して状況を把握（ATTK）（検体を特定する）
- 対象PCの情報資産重要度を分類する
  ⇒高重要の場合、証拠保全する
  ⇒低重要の場合、NW遮断する

判断で困った（迷った）事項と理由

- 証拠保全するか、NW遮断するか判断基準が難しい。
- どこに報告すべきか。

その他

とにかく対応のワークシート（ハンドリング担当用）

2017/8/25

想定教員のPCがランサムウェアに感染しファイルが暗号化され、この情報（相談）が情報センターに届いた。

対応のため

報告が欲しい情報

・事実確認（発覚日、発生日、経緯）、漏えいの有無、人数、原因、二次被害
・不正アクセスのレベル（知的財産の影響含む）、機密情報
・システムの停止、ネットワークの停止（学内LAN、インターネット）停止時間）
・関係施設への影響、保守契約内か、別途費用？

ハンドリング（上長）担当がテクニカル担当者に行う指示、注意すべき事項

・体制の整備
・証拠保全するか、現状復旧するか
・ベンダーへの依頼のタイミング
・重点調査項目

調査の前にしなければならないこと

・関連部署の召集（対策チームを作る）
・インシデントフローの確認
・証拠保全
・ネットワークケーブルの抜線の有無

規程、ルールで明記が必要と思われる事項

・ネットワーク・システム停止の権限の有無
・学内リンギの簡略化
・復旧作業の順番
・報告先（文科省、自治体など）

調査について

実際に行うべき事項と手段および結果

・学内外への広報
・法務部門への法的責任の確認
・プロセスの確認
・ネットワークの通信状況
・イベントログの確認

判断で困った（迷った）事項と理由

・既知のウイルスかどうか
・学内メンバーだけで対応可能？
・教員、代替機（仕事に必要なデータがない）

その他

・学内外への公表（学生、教職員、保護者）公表方法（HP、書面、集会）
2.

Jグループ

とにかく対応のワークシート（ハンドリング担当用）　2017/8/25

想定教員のPCがランサムウェアに感染しファイルが暗号化され、この情報（相談）が情報センターに届いた。

対応のため

報告が欲しい情報

感染日時、端末情報、対応した内容（時系列で）
感染範囲
共有フォルダ等の有無
個人情報などの流出の有無

ハンドリング（上長）担当がテクニカル担当者に行う指示、注意すべき事項

・手順をふんで、落ち着いて対応する
・随時・状況の報告
・周囲に情報を漏らさない
・判断に困る場合は相談

調査の前にしなければならないこと

・ネットワークケーブルの抜線
・端末の隔離

規程、ルールで明記が必要と思われる事項

調査について

実際に行うべき事項と手段および結果

・端末の状況把握（OS、パッチの適用の有無）
・感染ファイル、マルウェアの特定、プロセスの石座認、被害状況

判断で困った（迷った）事項と理由

ネットワークのケーブルの抜線
状況によるため判断が難しい

その他

とにかく対応のワークシート（テクニカル担当用）　(K)　2017/8/25

想定教員のPCがランサムウェアに感染しファイルが暗号化され、この情報（相談）が情報センターに届いた。

対応のため

報告が求められると思われる情報

感染日時、場所、有無、人、機器、範囲（状況）
マルウェアの種類
業務への影響　情報ろうえいの有無、ろうえい先、復旧方法、見込み

ハンドリング（上長）担当から、受けたい指示、注意

・状況確認 → 報告 → 保全、隔離の指示
・対応人数、役割分担
・感染範囲、状況調査

調査の前にしなければならないこと

・しかるべき人への報告（CISO）
・保全
・調査方法の報告
・セアリング
・ベンダーへの相談
・取線

規程、ルールで明記が必要と思われる事項

・インシデント発生時の対応、報告手順
・強制力を発動するための規程
・端末のセキュリティ対策

調査について

実際に行うべき事項と手段および結果

・証拠保全
・マルウェアの特定
・情報流出の詳細
・感染範囲
・感染経路
・ファイルの復旧

判断で困った（迷った）事項と理由

・手順通りの対応ができない場合（例．教員が拒否した）
・情報ろうえいの有無の判断
・外部公表の判断
インシデントレベル
調査への協力が得られない場合

その他

とにかく対応のワークシート（ハンドリング担当用）　グループ：L　2017/8/25

想定教員のPCがランサムウェアに感染しファイルが暗号化され、この情報（相談）が情報センターに届いた。

対応のため

報告が欲しい情報
感染している台数、現在までにとった対応、いつ感染したか？、現在の状況（暗号化されているかどうか）、影響はないか、知られているウイルスか？、データの重要性、復旧可能性、いつまでに復旧する必要があるか？、バックアップ取っているか、個人情報の有無
感染経路（ログ解析、NW解析）、被害範囲、暗号化以外の被害

ハンドリング（上長）担当がテクニカル担当者に行う指示、注意すべき事項
被害を最小限に留めるそち（ネットから切りはなす等）、マルウェアの特定、データ保全、適宜報告するよう指示、ダウンタイムの許容範囲、復号を試みてもらう。

調査の前にしなければならないこと
調査員の確保、上長へ報告（CISO）、関連部署への連絡、学外調査の仮確保（冒）

規程、ルールで明記が必要と思われる事項
「感染時にネットワークから切りはなす」「すみやかな報告と報告先」
「てんぷファイルに注意」
インシデントレベルの確定、報告ルート

調査について

実際に行うべき事項と手段および結果
上記全て

判断で困った（迷った）事項と理由
身代金を払うかどうかで、削除のタイミング
公表すべきかどうか、公表のタイミング
個人情報の範囲.（講習会名簿はどうする？）

その他
・年間インシデント分類の報告（予算取りの為）を行う必要性.

グループM

とにかく対応のワークシート（ハンドリング担当用）　2017/8/25

想定教員のPCがランサムウェアに感染しファイルが暗号化され、この情報（相談）が情報センターに届いた。

対応のため

報告が欲しい情報

- 発生した日時，気がついた日時
- 被害状況と重要度（対象のデータは何か？）（ログなどがあるか）
- 調査にかかる時間
- 他PCへの影響有無（共有フォルダ）
- 復旧の方法

ハンドリング（上長）担当がテクニカル担当者に行う指示、注意すべき事項

- 現状を保全する（証拠の保存）
- 影響範囲
- 報告（中間）のタイミングと調査と復旧（調査）それぞれの指示指示
- 原因の特定

証拠
- 保全 or 調査？
- 調査 or 復旧？

どちらを優先すべきか？

調査の前にしなければならないこと

- （IOAの報告タイミング）の決定
- 拡大防止（関連部署ネットワーク停止 etc…）
- 全社への共有

規程、ルールで明記が必要と思われる事項

- 重要度の切り分け
- 報告時間フォーマット
- 連絡のルーチン
- ネットワークを止める，etc 初動のルール

調査について

実際に行うべき事項と手段および結果

- 感染の原因（経路 etc…）
- ランサムウェアによるデータの感染の調査
- 他PCへの影響の調査
- 対象ファイルの特定
- プリセットハッカー（不正通信調査）
- イベントビューアログ（ファイル流出調査）

判断で困った（迷った）事項と理由

- 調査の続行や復旧の判断

「調査」or「復旧」どちらを優先するか？

その他

とにかく対応のワークシート（ハンドリング担当用）　2017/8/25

想定教員のPCがランサムウェアに感染しファイルが暗号化され、この情報（相談）が情報センターに届いた。

対応のため

報告が欲しい情報

▨先生に対して
- backupをとっているか
- メールを開いた時の詳しい状況（時間など）

▨テクニカル担当者に対して
- ~~ファイルに個人情報が含まれているか。入っていた場合~~
- NWから切り離す手立てがあるか、離れていなければ、切り離す。
- 何をもって感染したと判断したのか。
- 感染経緯の現状
- 他のPCや共有フォルダへのとび火の有無

ハンドリング（上長）担当がテクニカル担当者に行う指示、注意すべき事項

指示
- NWから又感染端末を切り離す。
- いつまでに復旧すべきか
- ランサムウェアを停止する依頼をする。

注意すべき事項
- 復旧を優先するのか、証拠保全を優先させるのか。→ 結果、今回のインシデントでは…まずは、復旧（暗号化をとめる）を優先する。

調査の前にしなければならないこと
- フローの確認
- 現地のPCの状態とLANがつながっているのか、セキュリティーワイヤなどが設置されているか
- CISOに報告（一次報告）。

規程、ルールで明記が必要と思われる事項
- ウイルス感染した際は、対象の端末を情シスに預けるという規程を作成もりこむ。
- LANを抜く等の初動対応の権限付与。

調査について

実際に行うべき事項と手段および結果

▨事項と手段
- 証拠保全 … Fast IRツールによる保全
- 復旧 … ランサムウェアの動作と停止、削除、暗号化されたファイルの復旧。
- 痕跡調査 … PCのプロセスの同査、イベントログの同査⇨RATへの感染とファイル名の特定 ファイル内容の不審点（個人情報の有無、件数等）公表の研究データの有無

▨結果
- ファイルの復旧と、流出ファイルの特定。

判断で困った（迷った）事項と理由
- 情報資産の価値判断
- 暗号化と流出が重なり、復旧と保全のどちらを優先すべきか難しい。
- 個人情報の流出をいつ、どうやって公表するのかの判断
- 流出した被害者への対応　・とび火したPCをどこまで調査するのかの判断

その他

グループ：○

とにかく対応のワークシート（ハンドリング担当用）　2017/8/25

想定教員のPCがランサムウェアに感染しファイルが暗号化され、この情報（相談）が情報センターに届いた。

対応のため

報告が欲しい情報

- 実際にランサムウェアに感染しているのか 拡大傾向か
- 重要度 機密度
- 影響範囲
- 気付いた経緯（外部・内部）
- ランサムウェアだけの感染か？
- 停止可能か
- 復旧までにどれだけかかるか
- 復旧にかかる費用

ハンドリング（上長）担当がテクニカル担当者に行う指示、注意すべき事項

- 証拠保全 優先
- 3日後までに調査・復旧を完了していること

調査の前にしなければならないこと

- PC調査することを教員（感染者）と合意すること
- 停止可能期間・復旧期限の確認
- 工数調整
- 必要な情報の整理
- 成績データの復旧を優先
- 公表・報告の必要性の確認
- 関係者への第1報
- 協力ベンダーの確認

規程、ルールで明記が必要と思われる事項

- 感染（疑い含む）時 事前連絡なく
  - 即停止する
  - PC調査
  - データ消去する場合あり
- データのバックアップ
- 個人の判断で身代金を払わない
- 業務停止が復旧か判断フロー

調査について

実際に行うべき事項と手段および結果

- 感染の確認：ファイルを開けない、身代金要求画面の表示
- ランサムウェアの特定：ファイルの拡張子の確認
- 証拠保全：Fax訳で取得
- 流出ファイルの確認：イベントログからファイル名を確認

判断で困った（迷った）事項と理由

- NW停止

その他