情報事故の種類別の対応事例

ここでは情報事故の種類別の適切な対応について解説します。より迅速な対応が求められるものには初動対応と記載しています。情報事故発生時は、初動対応後に情報セキュリティ事故緊急連絡受付窓口に連絡してください。

マルウェアに感染した場合の対応

マルウェアの感染は、利用者自身は気づかず、他者から指摘されて発見することが多い情報事故ですが、ランサムウェアのように、身代金要求のメッセージが表示されたり、ファイルがロックされたり直接的な被害で気が付くこともあります。マルウェア感染は被害拡大のスピードが速く影響の範囲も大きいため、下記の対応を迅速におこなってください。

対応

1 ネットワークから切り離す 初動対応

遠隔操作、オンラインバンクへの不正送金、外部へのサイバー攻撃、周辺の機器への拡散など、二次被害はネットワークを通じて広がります。そのため、被害を拡大させないために、有線の場合は LAN ケーブルを抜く、無線の場合は無線 LAN（Wi-Fi）の物理スイッチをオフ（ない場合は、OS の設定でオフ）にするなどして感染した機器をネットワークから切り離してください。

2 バックアップ

感染機器に格納されていた情報は、情報自体がマルウェアに感染している場合がありますので取り扱いには注意が必要です。やむをえずバックアップを行う場合は、外部メディアにバックアップしてください。

3 感染機器の復旧

感染した機器を再び利用する際は、OS のクリーンインストール、もしくは工場出荷状態に戻した上で使用してください。

ID・パスワードを窃取された場合の対応

ID・パスワードを窃取された結果、不正アクセスがあったとしても、多くの場合利用者は気づきませんが、サービスによっては、身に覚えのない変更通知メール、不正ログインの警告通知、ログイン履歴を確認できるものなどから、判明することがあります。他者が起こした情報事故により、利用者のID・パスワードが漏えいした可能性があると連絡がある場合もあるかもしれません。

ID・パスワードが窃取された場合は、速やかに下記の対応をおこなってください。

対応

1 パスワードを変更する 初動対応

被害を拡大させないために、パスワードを変更してください。

パスワードが変更されてしまってアクセスできない場合は、システム提供者（管理者）に連絡し、対応を依頼してください。

2 サービスの設定を確認する

ID・パスワードを窃取し不正にログインした攻撃者により、サービスの設定を悪意のあるものに変更されている場合がありますので、サービスの設定を確認してください。

本学のID・パスワードが窃取された場合は、メールシステムなど本学のIDで利用しているサービスの設定を確認してください（メールシステムの場合、攻撃者のメールアドレスに転送されるなど、設定を変更されている可能性があります）。

モバイル端末や外部メディアの紛失、情報の誤送信・誤公開をした場合の対応

スマートフォン、ノートパソコンなどのモバイル端末を紛失し、悪意のある者に拾得された場合、モバイル端末内の個人情報を窃取されたり、ID・パスワードを記憶していたWebサイトに不正アクセスをされてしまう可能性があります。

USBや外付けHDDなどの記憶媒体を紛失した場合も、紛失した外部メディアに格納されていた情報が漏えいする危険性があります。

メールを誤送信してしまったり、オンラインストレージなどで共有範囲を間違って公開してしまった場合も情報漏えいにつながってしまいます。

このような「情報漏えい」の危険性がある情報事故に対しては、下記の対応をおこなってください。

対応

1 （モバイル端末の場合）情報削除またはロック 初動対応

対策7-1「盗難・紛失時も情報にアクセスされない工夫をする」にて述べたリモートワイプ機能を設定していた場合は、速やかに実行しましょう。

また、紛失したモバイル端末がスマートフォンなど、通信契約を結んでいる端末の場合は、携帯キャリアに連絡をおこない、下記の対応ができないか相談してください。

- おおよその位置の検索
- 機器のロック
- 回線の一時停止

2 格納されている情報の確認

格納されている情報の機密性、それらが情報漏えいした場合の影響の範囲や度合いを明確にしてください。

3 情報事故発生の報告

個人情報等の機密性の高い情報が格納されていた場合は、その情報の関係者（教職員については所属長）に速やかに報告してください。