学術研究機関における情報セキュリティ対応

令和４年３月９日

牧野総合法律事務所弁護士法人

弁護士　森　悟史

1　サイバー攻撃・情報漏えい等の実例①

最近話題のサイバー攻撃

・Emotet

悪意ある攻撃者から送られた電子メールにより感染が拡大するマルウェア。

2021年１月、欧州刑事機構による摘発で一旦終息したものの、2021年11月より、再度、感染が急拡大。

他のマルウェアの感染を引き起こす、自己増殖して社内の他の端末にEmotetが感染する、取引先へ正規のメールを装って送信が行われ、さらにEmotetがばらまかれるなどの被害がある。

・ランサムウェア攻撃

コンピュータをロックしたり、暗号化して使用不能にし、元に戻すことと引換えに身代金を要求するマルウェア。また、情報を不正取得し、暴露による脅迫を行うこともある。

実例：米国石油移送パイプラインの操業停止、日本の有名ゲームメーカーの業務停止及び情報漏えい、日本の自動車メーカーの生産停止

2　サイバー攻撃・情報漏えい等の実例②

・ベネッセ・コーポレーションのケース

情報システム構築等の四次委託先会社の従業員で、一次委託先会社の事業所において情報システム開発業務に従事していた者が、顧客情報約3504万件を自分のスマートフォンに複製し、そのうち約1000万件を名簿業者に売却したことから、不正競争防止法（営業秘密侵害罪）に問われた事件。

➡委託先からの漏えい

ベネッセは、おわびとして1人500円の金券を交付するなどしたため、107億円の赤字に。

※委託先からの情報漏えいは非常に多い➡委託先監督の重要性

・半田病院のケース

2022年10月31日、患者の診察記録を預かる電子カルテ等の端末や関連するサーバが暗号化され、身代金を要求された事件。病院内のデータが情報漏えいした可能性がある。

仮想プライベートネットワーク（VPN）装置の脆弱性を悪用して侵入されたものと考えられている。

➡ランサムウェア攻撃

※2023年2月2日、警察庁は、昨年1年間、ランサムウェアの被害を受けたとの申告が、全国の警察に230件寄せられたことを発表（前年より57.5%増））。

3　サイバー攻撃・情報漏えい等の実例③

サイバー攻撃・情報漏えいは企業の話？研究機関や大学は関係がない？

・国立がん研究センター

2022年1月26日、国立がん研究センター東病院において、職員がテレワークに利用していた端末がウイルス感染し、端末が乗っ取られた事件。臨床研究の被験者の個人情報が流出した可能性あり。

・理化学研究所

2021年9月24日、外部事業者提供の学習管理システムのサーバに不正アクセスがあり、ファイルが改ざんされた事件。約1万4000件の個人情報が流出した可能性あり。

・山形大学

2022年10月26日、大学のコンテンツマネジメントシステムの管理者ID及びパスワードが詐取され、不正アクセスを受けた事件。1059人分の個人情報が流出した可能性あり。

※2008年7月から2021年8月までの間、国内801大学を対象に調査したところ、累計漏えい件数が148万7811件（１大学あたり1857件）に上ったとの調査結果もある（株式会社ソースポッドによる調査）。

※大学に対するランサムウェア攻撃も（東海国立大学機構のケースなど）

４　個人情報保護法の建付け

・改正前個人情報保護法

76条（適用除外）　大学その他の学術研究を目的とする機関若しくは団体又はそれらに属する者が、学術研究の用に供する目的で個人情報を取り扱う場合、個人情報取扱事業者が遵守すべき義務に係る規定は適用されない。

➡個人情報保護法上の安全管理措置は直接適用されない。

・改正個人情報保護法

76条（適用除外）規定の削除。大学や研究機関も、原則として、個人情報取扱事業者。ただし、利用目的変更の制限（18条3項5号及び6号）、要配慮個人情報の取得の制限（20条2項5号及び6号）、個人データの第三者提供の制限（27条1項6号及び7号）については、民間企業等とは異なる取扱いが認められている。

➡大学、研究機関であっても、安全管理措置（23条）の規定が適用されるので、情報マネジメントは必須。

5　具体的な安全管理措置①

個人情報保護法23条（安全管理措置）には、具体的な管理措置は明記されていない。
もっとも、前述のとおり、Emotet、ランサムウェア攻撃など情報漏えいの多くは、ネットワーク経由。
したがって、情報管理措置といえば、まずは技術的安全管理措置。

・技術的安全管理措置

①アクセス制御

情報システムにアクセスできる者を限定する

②アクセス者の識別と認証

正当なアクセス権を有する者であることを、ユーザID、パスワード等で識別、認証する

③外部からの不正アクセス等の禁止

ファイアウォール、セキュリティ対策ソフトウェアの導入及びアップデート

ログの定期的な確認

④情報システムの使用に伴う漏えい等の禁止

通信経路又は内容の暗号化、パスワードの利用など

でも、技術的措置だけで十分なのか？

6　具体的な安全管理措置②

「個人情報の保護に関する法律についてのガイドライン（通則編）」では、具体的な安全管理措置の内容として、技術的安全管理措置の他、物理的安全管理措置、組織的安全管理措置、人的安全管理措置を挙げている。

・物理的安全管理措置

①個人データを取り扱う区域の管理

管理区域と取扱区域を分けて、入退室管理及び持ち込む機器等の制限等を行う

間仕切り等の設置、座席配置の工夫、のぞき込み防止措置の実施

②機器及び電子媒体等の盗難等の防止

個人データを取り扱う機器、個人データが記録された電子媒体や書類を、施錠できるキャビネット等へ保管

セキュリティワイヤ等で固定

③電子媒体等を持ち運ぶ場合の漏えい等の防止

持ち運ぶ個人データの暗号化、パスワード設定

④個人データの削除及び機器、電子媒体等の廃棄

書類については、焼却、溶解等適切なシュレッダ処理等を行う

電子媒体については、専用のデータ削除ソフトウェアの利用又は物理的に破壊

7　具体的な安全管理措置③

・組織的安全管理措置

①組織体制の整備

個人データ取扱いに関する責任者の設置及び責任の明確化

従業者が取り扱う個人データの範囲の明確化

個人データを複数の部署で取り扱う場合の各部署の役割分担及び責任の明確化

②個人データの取扱いに係る規律に従った運用

個人データ利用状況、持ち運び状況、削除・廃棄状況の確認

個人データが蔵置されている情報システムの利用状況の確認

③個人データの取扱状況を確認する手段の整備

個人データ取扱状況の把握

④漏えい等事案に対応する体制の整備

個人データの漏えい等の事案の発生又はその兆候を把握した場合の報告連絡体制（エスカレーション）

⑤取扱状況の把握及び安全管理措置の見直し

個人データの取扱状況について定期的に点検又は監査

8　具体的な安全管理措置④

・人的安全管理措置

従業者教育

従業者に定期的に研修を行う

秘密保持に関する事項を就業規則に盛り込む、又は秘密保持契約を締結する

9　安全管理措置のまとめ

上記の措置はあくまで例に過ぎない。

したがって、これらができていないからといって、安全管理措置が不十分となるわけでもないし、逆に、これらをすべて行っていたからといって、安全管理措置が十分となるわけでもない。

個人情報保護委員会ガイドライン（通則編）

「安全管理措置を講ずるための具体的な手法については、個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容とすべきものであるため、必ずしも次に掲げる例示の内容の全てを講じなければならないわけではなく、また、適切な手法はこれらの例示の内容に限られない。」

➡各組織の実情に合わせた安全管理措置を講ずることが必要。

多くの組織では、技術的安全管理措置や物理的安全管理措置に主眼を置いており、組織的安全管理措置や人的安全管理措置が軽視されている傾向が・・・

➡組織的安全管理措置や人的安全管理措置も重要。

組織的安全管理措置、人的安全管理措置を講じていない場合、適切な管理がされていないと評価されてしまうことも・・・

どのようなケースでどのような対応をすべきかを判断するためには➡リスクマネジメント

10　リスクマネジメント①

リスクを組織的に管理し、組織の損失の回避・低減を図るプロセス。

事業を遂行するに際しリスクがあることは当然➡リスクをいかにコントロールするかが問題

・リスクマネジメントのプロセス（手法）

①情報資産の洗い出し・棚卸し（どのような情報がどこにあるのか）

②リスクの発見及び特定

③リスクの評価及び算定

定性的分析（金額以外の値を用いて、リスクの大きさを算定する方法）

定量的分析（金額を用いて、リスクの大きさを算定する方法）

④リスク対応策の決定及び実施

リスク回避、リスク低減、リスク移転・共有、リスク受容

⑤モニタリング及び改善

※上記プロセスをPDCAで回すことが重要

※営業秘密を中心に説明している「大学における秘密情報の保護ハンドブック」（平成28年10月全面改訂・経済産業省）でも、秘密情報の分類、分類に応じた情報漏えい対策の選択などが規定されている。

11　リスクマネジメント②

・<u>リスク対応策</u>

①リスク回避

リスクを生じる原因を除去したり、別の方法に置き換えることにより、リスクを取り去る。

デメリットが多い（最悪の場合、当該業務や研究を中止するということ）。

②リスク低減

リスクの発生確率を低下させたり、被害の影響度を低減させる。

リスク対応策の基本は、このリスク低減。

③リスク移転・共有

リスク自体を外部機関に移転したり、保険をかける。

リスクの発生確率は低いが、発生した時の影響が大きい場合に用いる。

④リスク受容

対応策をとらず、そのままにする。

リスク対応策をとるだけのコストに見合わない場合に用いる対応策。

12　学生の管理①

調査研究・教育目的で、学生にも、情報・データを利用させることが考えられる。その中には、個人情報やセンシティブ情報が含まれていることも。

➡学生の管理も重要

・学生の立ち位置・・・従業者と同等か？

　従業者とは、企業・組織のメンバーとして、企業・組織の目的（営利・事業継続など）のために、企業・組織と同じ方向を向いて、企業・組織の手足となり業務を遂行する者

　　※従業者に対しては、従業者監督（個人情報保護法24条）が定められている。

　これに対して、学生は、大学における不可欠の構成員ではあるが、大学のサービスを利用する者

➡お客様のようなもの？

➡とすると、学生と従業者とは別の立ち位置

➡学生に従業者監督は及ばない？

　cf 大学の自治　人事の自治の他、施設・学生の管理の自治があるとされている。

　　学生は、大学自治の主体ではない（最高裁昭和38.5.22東大ポポロ事件）

13　学生の管理②

学生は大学の設備・資産（情報を含む。）を利用する以上、管理者の指示に従う必要がある。

従業者監督（個人情報保護法24条）が直接適用されるわけではないが、従業者監督と同じように考えることができるのでは。

実際には、安全管理措置の内容に従った対策が必要。

・組織的安全管理措置の側面

情報管理に関しての責任者の設置及び責任の明確化

学生が取り扱うことのできるデータの範囲の限定（本当に個人情報やセンシティブ情報を取り扱わせる必要があるか？）

インシデント発生時、誰に報告するのかを予め決めておくこと

・人的安全管理措置の側面

学生に対する情報セキュリティ教育・研修

秘密保持合意書の取得

・物理的安全管理措置の側面

情報にアクセスできる機器の限定

※「大学における秘密情報の保護ハンドブック」では、学生が秘密情報を取り扱う研究に参加することで生じるメリットと、学生に課せられる義務等とのバランスに応じて、研究への参加の是非について予め検討しておく必要があるとしている。

14　学生の管理③

・パスワード管理の重要性

情報システムにアクセスする際のパスワード設定の不十分さにより、情報漏えいしているケースが多い。

・具体的なパスワード管理策

①パスワードポリシーの策定及び学生への周知

②デフォルト（初期設定）でのパスワードを利用しない

③英字・数字を組み合わせて、10桁以上などの制限

（可能であれば、適切なパスワードを設定しないと情報にアクセスできないような技術的措置）

④同じパスワードを複数のサービスで使い回さない（他のサービスから漏えいしたパスワード情報を使って、別のサービスのアカウントに不正アクセスするケースがある）

⑤以前は、定期的にパスワードを変更することが推奨されていたが、現在では推奨されない。

※定期的にパスポート変更すると、いちいち覚えられないため、似たようなパスワードを設定しがち

➡かえって、推知されやすいパスワードになってしまうことがある

15　情報漏えい時対応

・情報漏えいが疑われる場合の対応

①個人情報保護委員会への報告（個人データ漏えい等の場合、個人情報保護法26条1項）

②本人への通知（個人データ漏えい等の場合　個人情報保護法26条2項）

その他にも

③関係部署（監督行政庁、IPA、JPCERT/CC、警察等）への連絡・報告

④事実関係の調査及び原因の究明

⑤外部専門機関・専門家の招へい（フォレンジック調査）

⑥事実関係等の公表

⑦再発防止策の検討及び決定

➡やることはたくさんある

時間がない

初動対応が重要

そこで・・・

16　IT-BCP・情報セキュリティBCP

BCP（事業継続計画）の情報システム・情報セキュリティ版。
BCPには、その他にも自然災害BCPや感染症BCPなどがある。
予め、インシデントが発生した場合に必要な情報システムの運用を維持する目的等で作成されるもの。

・具体的な対策内容
①責任者の指名及び権限の明確化（責任者が対応できない場合の補助責任者の指名）
②データ保管・バックアップ
③代替機の準備、冗長化
④インシデントの判断基準・BCP発動基準（誰がどのような要件を考慮しBCPを発動するか）
⑤インシデント発生時のエスカレーションの方法（2ルートあるとよい）
⑥インシデント発生時の情報共有の範囲（内部犯行の可能性はあるか）
⑦リカバリ方法（想定される被害状況から見た優先度の設定）
⑧教育・訓練（ディザスタリカバリ訓練）
⑨IT-BCPの定期的チェック及び見直し

17　身代金の支払いは許されるのか？（参考）

・犯罪による収益の移転防止に関する法律

　金融機関等に対して、本人確認等が義務付けられている➡身代金支払いとは無関係

・暴力団排除条例

　利益供与を禁止しているが、その対象は暴力団員等一定の限定がある上、提供した側は刑罰の対象ではない。

・企業が反社会的勢力による被害を防止するための指針（犯罪対策閣僚会議・2007年）

　「反社会的勢力への資金提供は、絶対に行わない」→法律ではないため拘束力なし

・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・2020年）

　「ランサムウェア攻撃を助長しないようにするためにも、金銭の支払いは厳に慎むべきものである」

　→法律ではないため拘束力無し

➡身代金の支払いは勧められるものではないが、法律上は違法ではないと考えられる。

事実、情報システムがロックされているような状況で、他の代替手段が考えられるのか？

業務遂行できない状況が続くことは許されるのか？

半田病院の例では、犯人側は、半田病院から３万ドル（約450万円）を受け取ったと主張している。