当検査センターの情報セキュリティ活動

システム管理課　システム係

はじめに

医療業界においても情報システムを利用した業務のIT化が進められるようになって久しいですが、利便性が増すのと同時に様々な脅威も知られています。例えば、ウイルス感染による機密情報の漏洩、不正アクセスによるデータの改ざん、また昨今ではランサムウェア※1による身代金の要求など、医療業界で実際に被害があった事例もあり社会問題となっています。

そこで今回は、当検査センターで行っている情報セキュリティ対策と、所内の職員向けに行っているITリテラシー※2教育についてご紹介します。

※1 感染したパソコンなどを使用不能にし、その解除と引き換えに身代金を要求するマルウェア（悪意のあるソフトウェア）のことです。

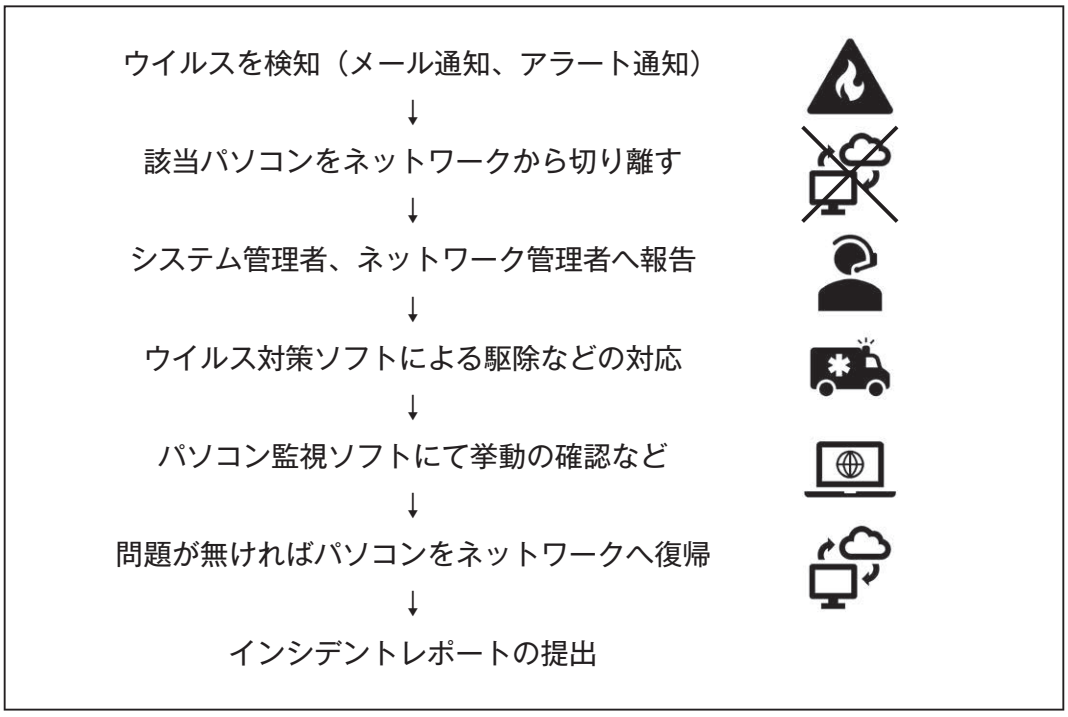
※2 パソコンやスマホなどの情報機器を活用する能力のことです。

1．情報セキュリティ対策

(1)ウイルス対策ソフトの導入

①当検査センターでは全てのパソコンにウイルス対策ソフトを導入しています。また、ウイルス定義は常に最新の状態に更新し、定期的にウイルス検査を行っています。

②ウイルスに感染した場合は、以下の手順で対応しています。



(2)情報資産管理ソフトウェアの導入

①情報資産管理

パソコン、プリンターなどの周辺機器及びソフトウェアのバージョンなどを管理し、所内の情報資産の活用状況を的確に把握することで、各部署の運用状況を監視しています。また、登録されていないパソコンからのネットワーク接続をブロックしています。

②USB メモリ管理

パソコンに接続する USB メモリを管理し、登録されていない USB メモリ（例えば外部から持ち込まれた USB メモリ）の使用を制限しています。使用を制限することで、情報漏洩やウイルス感染のリスクを防いでいます。

③操作ログ管理

パソコン上での職員の操作や、外部との通信、ファイルへのアクセス状況など、さまざまな挙動をログとして記録しています。「いつ」「誰が」「何をしたのか」を正確に把握することで、情報漏洩などのトラブルが発生した際に素早い対応を行います。

(3)サーバー室の入退室管理

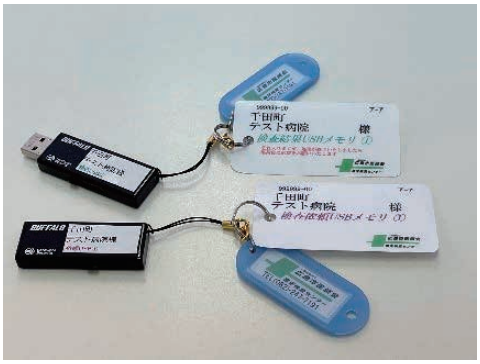
「静脈認証装置」をサーバー室の入口に設置し、入退室を制限・監視することにより物理的な面からセキュリティを確保しています。また、監視カメラを設置しています。

(4)利用者情報の管理

ユーザーやファイルへのアクセス権限、メールアドレス、各種システムの利用者情報（アカウント）を管理しています。定期的に情報を更新し、異動や退職があった場合の権限の変更や利用の停止を行い、情報へのアクセスを制限しています。

(5)パスワード付き USB メモリの使用

所内ではパスワード及びウイルス対策ソフト付きの USB メモリを使用しています。また、医療機関とのデータ受け渡しについても、従来のフロッピーディスクからパスワード付き USB への切替えを行っています。これにより紛失などが起きた場合の情報漏洩を予防しています。



2. IT リテラシー教育

当検査センターでは年に一度、全職員を対象にした研修会を行っています。また、情報処理推進機構（IPA）などの情報から緊急性の高い内容については随時､所内で情報共有を行っています。

(1)情報セキュリティ研修会

毎年、全職員を対象に近年のサイバーリスクの実態や、実際に起こった医療機関へのサイバー攻撃の実例などを踏まえて、情報セキュリティについての研修会を行っています。同時に個人情報に関する研修会も行い、情報漏洩などの危険性と、扱っている情報の重要性を学ぶことで、情報セキュリティに対する意識を高めています。

(2)IT リテラシーについての情報展開

昨今の IT に纏わる社会的な出来事や傾向・流行などを所内の職員向けに情報展開しています。また､IPA などから緊急性の高いセキュリティの脆弱情報が発表された場合、新聞記事などで注意するべき情報が公開された場合にも所内で展開しています。

＜情報展開したテーマの例＞

・情報セキュリティの基本対策

攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消し攻撃によるリスクを低減する
ウイルス感染	セキュリティソフトの利用	攻撃をブロックする
パスワード窃取	パスワードの管理･認証の強化	パスワード窃取によるリスクを低減する
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導（罠にはめる）	脅威･手口を知る	手口から重要視するべき対策を理解する

・フィッシングメールや SMS からの脅威と対策

実在する金融機関や各種インターネットサービスなどをかたり、**「不正ログインされた可能性があります」「口座再開の手続きを行ってください」**などのメールやSMS（携帯のショートメール）を送り、偽サイト（フィッシングサイト）へ利用者を誘導し、そこで入力させた個人情報（クレジットカード、ID、パスワード）などを盗み出す手口。
2019年上半期（1月～6月）の被害件数は183件、被害額は約1億6,600万円にとどまったものの、同年9月だけで被害件数は436件、被害額は約4億2,600万円に膨れ上がった。

新型コロナの10万円給付も同じような詐欺が横行しています。注意しましょう

＜対策＞

1. 情報収集し、フィッシング詐欺の手口を知る
2. メールやSMSなどで誘導されるURLを不用意に開かない
3. **ログインや情報の入力は、送られてきたURLからではなく、正規サイトもしくは正規アプリから行う**
4. OSやセキュリティソフト、セキュリティアプリを最新の状態に保って利用する

おわりに

近年の情報資産に対する外部からの攻撃は、巧妙かつ進化し続けており、ウイルス対策ソフトなどを導入し、どんなに「技術的」な対策を行っても、100% 脅威を防ぐことは不可能だといわれています。そこで、当検査センターでは職員個々の IT リテラシーの向上が重要と考え、情報セキュリティ研修や IT リテラシー教育を行い「人的」な情報セキュリティ対策を行うことで、「組織的」なセキュリティの水準を高めることを目指しています。

また、所内の職員だけに留まらず、ご要望のある医療機関へ情報セキュリティ対策についての出前勉強会なども、今後は企画していきたいと考えております。もし、情報セキュリティに関する勉強会にご興味があるようでしたら、下記までお問合せください。

担当：システム管理課　システム係
前崎　憲一
（情報処理安全確保支援士）
TEL：082-247-7198（直通）
第019949号

＊ウェブサイトでもご覧いただけます。　http://www.labo.city.hiroshima.med.or.jp/