コンピュータウイルス感染など情報セキュリティに対する脅威

ネットワークや情報システムは、今や日々の業務に不可欠なものとなっており、たった一人のパソコンがウイルス等に感染しただけで、多くの職員の業務に支障が出たり、復旧に多大なコストを要したりするなど、その影響は想像以上に大きいものとなることがあります。

情報の金銭的価値が増している昨今、学校を含め、自治体の組織は日々サイバー攻撃に晒されています。また、その手口も年々巧妙かつ高度なものが増えてきていることから、情報セキュリティポリシーを順守することはもちろん、情報セキュリティに関する知識やその対応策について、日々情報を収集し、アップデートしていくことが求められます。

1　不祥事の事例

※この事例は民間企業等で実際にあった事案を参考に作成

事例　教員Aは、「差出人：文部科学省　件名：至急御回答ください」とのメールに記載されていたURLをクリックし、回答した。後日パソコン上に「お客様のファイルをウイルスによって暗号化しました。」とのメッセージが突然表示され、パソコンや共有フォルダに保存されたデータが開けなくなった。なお、表示された文面は、暗号化解除のために金銭を要求するとともに、要求を受け入れなければ窃取した個人情報を売却するとの脅迫を伴うものであった。

ウイルスは同一のネットワークで繋がっているパソコンにも広がっていたことから、組織全体の業務に大きな支障を生じさせることとなった。

被害の調査を行う中で、感染したパソコン内及び共有フォルダ内に保存されていたデータが外部へ送信されていることが判明し、情報漏洩が明らかになった。暗号化されたデータの復旧には３か月を要し、１００万円を超える費用が発生することとなった。

2　組織で防ぐ

以下のポイントは標準例です。実際には各システム管理者等が定めたものに従ってください。

ポイント１　定められた情報セキュリティ対策の確認・順守

□　情報資産を守るために各職員が順守すべきと定められている内容を知っていますか。
□　定期的に所属内で情報セキュリティ対策に関する研修を実施していますか。
□　職員用パソコン（貸与、許可されているものを含む）を使って業務に関係のないインターネットサイト等を閲覧していませんか。
□　不審なメールが届いた場合、添付ファイルや本文中のURLを開かず削除していますか。また、判断に迷う場合は所属長や情報セキュリティを担当する部署へ相談していますか。
□　私用又は外部の者が所有するUSBメモリ等の電磁的記録媒体について、ウイルススキャンを行うことなく安易に職員用パソコン（貸与、許可されているものを含む）へ接続していませんか。
□　ウイルスへの感染が疑われた場合、自身が取るべき行動を知っていますか（即時ネットワークを切断、所属長へ報告、感染原因とみられるメール等の証拠保全）
□　ウイルス対策ソフト等は常に最新の状態が保たれていますか。
□　パスワードは定期的に変更し、推測されにくいものを使用していますか。

ポイント２　情報セキュリティインシデントの事例や情報の収集・共有

□　情報セキュリティ担当部署が発信する注意喚起情報を定期的に確認していますか。
□　他の自治体や民間企業等で発生した情報セキュリティインシデント事例等について、積極的に情報収集し、所属内で共有が図られていますか。

3　想像してみよう

◎　自分のパソコンがウイルスに感染したことにより、共有フォルダやメール等を介して自所属のみならず他所属の職員のパソコンやシステム全体に障害が発生した場合にどのような結果を招くか想像してみましょう。

4　巧妙化・高度化するサイバー攻撃の手口

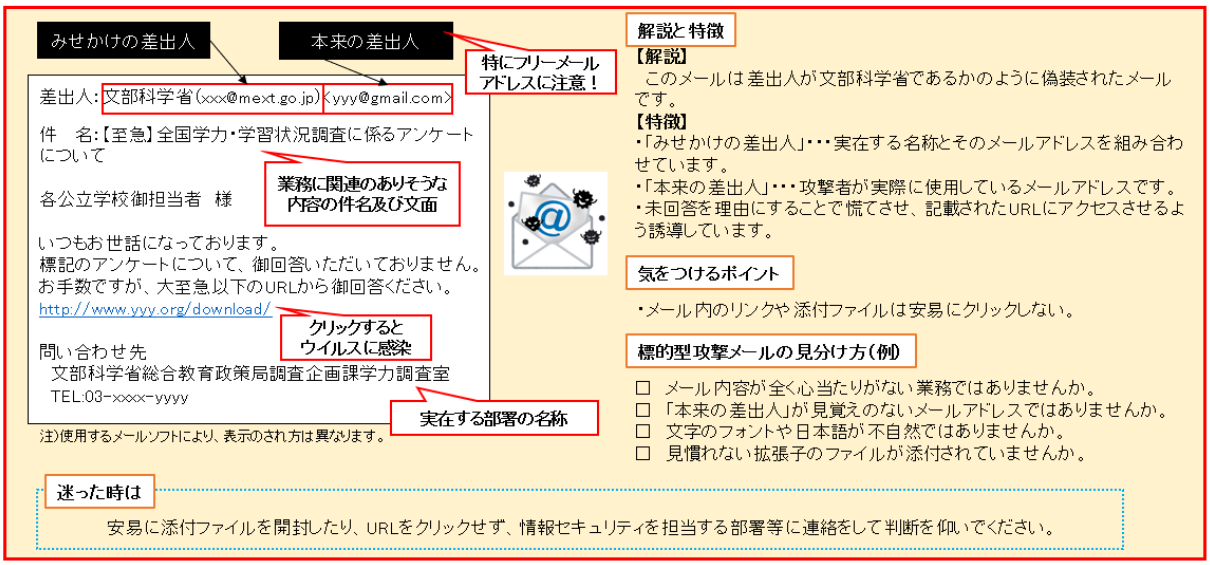
（1）標的型攻撃メール

重要な情報を盗むことなどを目的として、組織の担当者が業務に関係するメールだと信じて開封してしまうよう巧妙に作り込まれたウイルス付きのメールのことです。最近では地方公共団体もそのターゲットとなっています。

標的型攻撃メールのウイルスは、ウイルス対策ソフトでは検出されないものが多いため感染に気づきにくく、知らぬ間に被害が拡大しているケースがあり、深刻な問題となっています。

※出典：　総務省『国民のためのサイバーセキュリティサイト』
（https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/index.html）

【標的型攻撃メールの例】



（2）ランサムウェア

ランサムウェアとは、身代金という意味を持つ英単語の「Ransom（ランサム）」と、コンピュータウイルス等を含むコンピュータに何らかの処理を行うプログラムなどを指す「Software（ソフトウェア）」を組み合わせた造語です。（出典：警視庁 HP）

感染すると、パソコンやサーバに保存しているデータが暗号化され使用できなくなり、データを復元する対価として金銭を要求されることがあります。さらには、データを盗み取った上、「対価を支払わなければデータを公開する」などと金銭を要求するダブルエクストーション（二重恐喝）という手口も発生しています。

近年は、法人や自治体を標的とした攻撃手法が主流となっており、感染したパソコンが接続する内部ネットワーク全体に感染を拡大させる手口が登場しています。この種のマルウェア（悪意のあるソフトウェア）に感染すると、組織内での業務の停滞や情報漏洩、情報漏洩による県民からの信頼喪失等、被害が広範かつ深刻化する恐れがあり、特に注意が必要です。

5　問われる責任

（1）行政上の責任・・・懲戒処分（免職、停職、減給、戒告）（2）刑事上の責任・・・懲役、罰金等
（3）民事上の責任・・・損害賠償等　　（4）社会的な責任・・・報道等

【参考】

懲戒処分の基準　第２　　１（７）秘密漏えい

ア　職務上知ることのできた秘密を故意に漏らし、公務の運営に重大な支障を生じさせた職員は、免職又は停職とする。この場合において、自己の不正な利益を図る目的で秘密を漏らした職員は、免職とする。

イ　具体的に命令され、又は注意喚起された情報セキュリティ対策を怠ったことにより、職務上知ることのできた秘密が漏えいし、公務の運営に重大な支障を生じさせた職員は、停職、減給又は戒告とする。

懲戒処分の基準　第２　　１（９）個人情報の盗難、紛失又は流出

過失により個人情報を盗まれ、紛失し、又は流出させ、公務の運営に支障を生じさせた職員は、減給又は戒告とする。この場合において、公務の運営に重大な支障を生じさせた職員は、停職又は減給とする。