教育情報

情報セキュリティの指導について

－ GIGA 教育の推進をめざして －

拓殖大学名誉教授　山下　省蔵

1．はじめに

文科省は，令和時代の学校教育スタンダードとして，GIGA［Global and Innovation Gateway for All］スクール構想を掲げ，児童・生徒向けの１人１台の端末と，高速大容量の通信ネットワークを一体的に整備する施策に取り組んでいる。これにより多様な子どもたちを，誰ひとり取り残すことなく，個別化・最適化した創造性を育む ICT（Information and Communication Technology）教育を全国の学校現場で持続的に実現させ，また同時に，教員の働き方改革を推進し，充実した学校教育の実現を目指している。

昨年，新型コロナウイルス感染症拡大に伴い緊急事態宣言が発令され，大手企業を中心に多くの企業がテレワークでの在宅勤務となり，政府が働き方改革の一環として主導していたテレワークが，一気に進展した。学校教育においても，ＩＴ化を一層推進し，学び方や教え方を革新する機会にすべきと考える。

今日の経済・社会生活においては，情報通信技術の一層の進展により，生活は便利になり，仕事の効率も上がり，多くの人々にとって，コンピュータやインターネットは，なくてはならないものになっている。

しかし普及に伴い，インターネットを悪用して，ウイルスや迷惑メールをばらまき，コンピュータへの不正侵入をはじめインターネット上での詐欺行為やプライバシーの侵害などの悪質な行為が発生している。

そこで，生徒にコンピュータやインターネットを安全に活用させるには，望ましい活用能力を習得させ，特に情報セキュリティについて適切な対策をとる必要があることを理解させ，そのための対応能力を習得させる必要がある。

昨年ある高校に，海外からと思われる英文の身代金要求型ウイルスが仕掛けられ，サーバ内のすべての教育情報が暗号化されてしまい，あらゆるデータが開けなくなった事例が発生した。

この事例から見ても，これから教育現場でのクラウド化を推進するためには，都道府県教育委員会レベルでサーバーの管理・運営を組織化して，一層厳重な安全管理対策を行うことが求められる。

しかし各学校においても，教育情報セキュリティ対策を一層強化する必要があり，その権限及び責任は管理職である校長にあり，そのための管理能力が必要となる。

2．情報セキュリティポリシーの機能

一般的に情報セキュリティポリシーとは，企業等の組織が取り扱う情報やコンピュータシステムを安全に保つための基本方針や体制・対策などの基準を包括的に定めたものである。

そこで企業においては，実施する情報セキュリティ対策の方針や行動指針が示された組織全

体の規定をつくり，どのような情報資産をどのような脅威から，どのように守るのかといった基本的な考え方をはじめ，具体的な情報セキュリティを確保するための体制づくりと運用規定などを定めている。

各学校については，都道府県の教育委員会が定めている「教育情報セキュリティポリシー」の事例を参考として，各学校も運用規定をつくり，情報機器の安全で有効な活用に努める責任がある。

教育情報セキュリティ対策は画一的なものではなく，各学校においては，校種や規模や体制によって，ネットワークやシステムの構成，保有する情報資産なども異なるので，各学校の組織に見合った情報セキュリティポリシーを作成する必要がある。

教育情報セキュリティポリシーの設定にあたっては，校長の指示のもとに，その担当者だけがネットワークやコンピュータなどに対する情報セキュリティ対策を心がけるのでなく，すべての教職員はもとより，生徒たちにも必要となる適切な情報セキュリティの意識を育成し，情報漏洩やウイルスなどから学校全体の教育組織を防御する体制づくりが必要である。

過去の事例では，情報機器を管理する担当教員が，禁止されているＳＤカードに入試情報を保存し，かつそのカードを校外に持ち出して，紛失した事例がある。

つまり，すべての教職員や生徒たちが情報セキュリティポリシーを遵守することにより，教育情報セキュリティの機能が発揮され，各学校における情報教育推進の基盤となるのである。

3．情報セキュリティについて

インターネットの活用にあたっては，インターネットは誰もが利用できる公共のインフラであり，それぞれの生徒が家族や友人たちとつながっており，一人ひとりが自分が利用するコンピュータの情報セキュリティを守ることが，インターネットに接続している他の多くの利用者の安全にも関わっていることを自覚させる必要がある。

つまり，みんなで利用するのであり，各自の正しい知識と対策によって，安心してインターネットが活用できることをしっかり理解して身に付けさせたい。

学校のコンピュータは，ウイルス対策が施されているが，自宅のパソコンを利用する場合は，ウイルスセキュリティソフトがインストールされていることを確認するよう指導する。

次に，情報セキュリティに関しておもな指導すべき事例について以下にまとめた。

⑴　情報セキュリティ三原則の指導

コンピュータやインターネットを安心して利用するには，「情報セキュリティ対策」が不可欠であることを強調して指導する。

インターネットに関する脅威が多様化する中で，さまざまな情報セキュリティ対策が必要となっているが，初心者のための情報セキュリティ３原則を次に示した。

①　ソフトウェアの更新

OS（基本ソフト）や Web ブラウザなどのソフトウェアでは，修正プログラムが提供された場合には必ず更新する。

②　ウイルス対策ソフトの導入

ウイルスの感染防止のために，対策ソフトやパーソナルファイアウォールやフィルタリングなどの機能を備えた総合セキュリティ対策ソフトを導入する。

③　ID とパスワードの適切な管理

パスワードは他人に容易に想像されないものを作成し，同じパスワードを使い回さないように指導する。

過去，パスワードの定期的な変更が推奨されていたが，2017 年に，米国国立標準技術研究所

からガイドラインとして，サービスを提供する側がパスワードの定期的な変更を要求すべきではないとし，日本でも内閣サイバーセキュリティセンターから，パスワードを定期変更する必要はなく，流出時に速やかに変更すればよいとされている。

最近 ID とパスワードの代わりに，身体的な特徴である指紋，顔，静脈，虹彩（瞳孔周辺の渦巻き状の文様）などや声紋（音声），署名（手書きのサイン）などを利用する生体認証の実用化が進められている。

生体認証は，パスワードによる認証と比較して，記憶が不要なため利便性が高く，記憶忘れによるトラブルもないという長所がある。しかし生体認証の種類によっては，以下の課題がある。

a） 人の成長，老化などによる身体的特徴の変化によって認証が正しく行われない。

b） サインなどの行動的特徴を盗み見られてなりすまされる危険がある。

c） 双子など身体的特徴が似ている人を誤認識することがある。

d） 認証情報の変更の課題としては，パスワードや IC カードと異なり，身体的特徴は意図的に変更できない。

しかし最近では，これらの課題に対策を施した製品も開発されつつある。

⑵ 詐欺行為にあわないように指導する

① フィッシング（phishing）詐欺

フィッシング詐欺とは，送信者を詐称した電子メールを送りつけたり，にせの電子メールからにせのホームページに接続させ，クレジットカード番号やアカウント情報（ユーザ ID，パスワード）などの重要な個人情報を盗み出す詐欺行為である。

最近では，パソコンだけでなく，スマートフォンでも同様に電子メールからフィッシングサイトに誘導する手口もあるので注意させる。その手口は，クレジットカード会社や銀行からのお知らせメールに似せて，リンクをクリックさせ，偽装したサイトに利用者を誘導し，クレジットカード番号や口座番号などを盗み取る手法である。

また，電子掲示板や SNS（Social Networking Service）の投稿サイトに，URL を記載してアクセスさせ誘導する手口としては，アルファベットの一文字の o（オー）を数字の 0（ゼロ）にしたり，アルファベットの大文字の I（アイ）を小文字の l（エル）にしたりして，閲覧者に見まちがえをさせる手口が使われるので注意する。

一般にインターネットバンキングでは，クレジットカード番号などの重要な情報の入力画面では，SSL（Secure Sockets Layer）という暗号化技術が利用されている。

重要な情報を入力する Web ページでは，SSL が採用されているかを確認することが大切である。

SSL で通信が行われていることは，Web ブラウザの URL 表示部分（アドレスバー）や運営組織名が緑色の表示になっているか，鍵マークが表示されているかなどで確認することができる。

重要な情報の入力を求めるページで，SSL が使用されていない場合は，まずはフィッシング詐欺を疑ってみる必要がある。

金融機関などの名前で送信されてきた電子メールの中で，通常と異なる手順を要求された場合には，内容を鵜呑みにせず，金融機関に確認することも必要である。

フィッシング詐欺であるかどうか判断が難しい場合には，必ず正規の Web サイトや金融機関からの郵便物などで連絡先の電話番号を調べて再確認する必要がある。

② ワンクリック詐欺

ワンクリック詐欺とは，Webサイトや電子メールに記載されたURLを一度クリックしただけで，一方的に，サービスへの入会などの契約成立が宣言され，多額の料金の支払いを求められるという詐欺である。

ワンクリック詐欺の手口は，契約してしまったように思わせ，期限内に利用料金を支払わない場合，延滞料が加算されるとか，法的措置を講ずるといった脅迫的な内容で，利用者に支払いを迫ってくる。

アダルト系，出会い系などを装った内容であることが多い。

間違ってクリックした場合や，意図せずこうしたWebサイトを閲覧して，料金を請求された場合は，解約手続きや返信メールなどで連絡はせずに無視することが大切である。つまり，こちらから支払理由などを確認するために業者に連絡を取ると，相手に自分の個人情報を渡すことになるので，決して連絡をとらないことが大切である。

先方からは，何度も利用料を請求してくるが，返信や問い合わせなどせず，無視し続けるとメールが送られてこなくなる。

「電子消費者契約及び電子承諾通知に関する民法の特例に関する法律」では，「電子消費者契約に関する民法の特例」として，消費者がコンピュータの操作ミスなどで，契約する意志がなく申し込んだ場合における救済措置がとられている。

不安がある場合は，支払いをする前に，総務省電気通信消費者相談センターや消費生活センター，警察などに相談させるように指導する。

⑶ ＳＮＳ利用上の注意点

友人同士がメッセージや写真などを共有してコミュニケーションを取ったりする，いわゆるSNSが普及している。SNS利用時に想定される脅威と対策について指導する。

① プライバシー情報の書き込みに注意する

友人間のコミュニケーションを目的としてSNSを利用していても，書きこんだ情報はインターネット上に公開されていることに変わりはないので，書き込む内容には十分注意して利用することが大切である。

最近のGPS機能のついたスマートフォンやデジタルカメラで撮影した写真には，目に見えない形で，撮影日時，撮影した場所の位置情報などが記録されている。

そこで，写真から場所が他人に特定されてしまう危険性があり，迷惑行為やストーカー被害などの犯罪の被害にあうこともあるので，注意が必要である。また，SNSは誰でも投稿することができることから，ワンクリック詐欺，フィッシング詐欺などに誘導される危険性もあり，情報の発信元の信頼性に注意する必要がある。

4．IoTのセキュリティ対策

インターネットに接続できる機器が普及し，日常生活の中でもIoT［Internet of Things］機器が普及してきている。IoT機器を適切に利用し管理し，インターネット経由で自宅等の機器が外部から操作され，不正利用されたり，プライバシーが漏れたりしないように以下の点に注意させる。

① サポートがない機器は導入しない

② 初期設定に気をつける

インターネットに接続する導入機器には，必ずID，パスワードの設定をする。

③ 機器の廃棄時にはデータを消去する

参考資料

文部科学省「教育情報セキュリティポリシーガイドライン」，総務省・経済産業省「クラウドサービスに関する検討会」関係資料