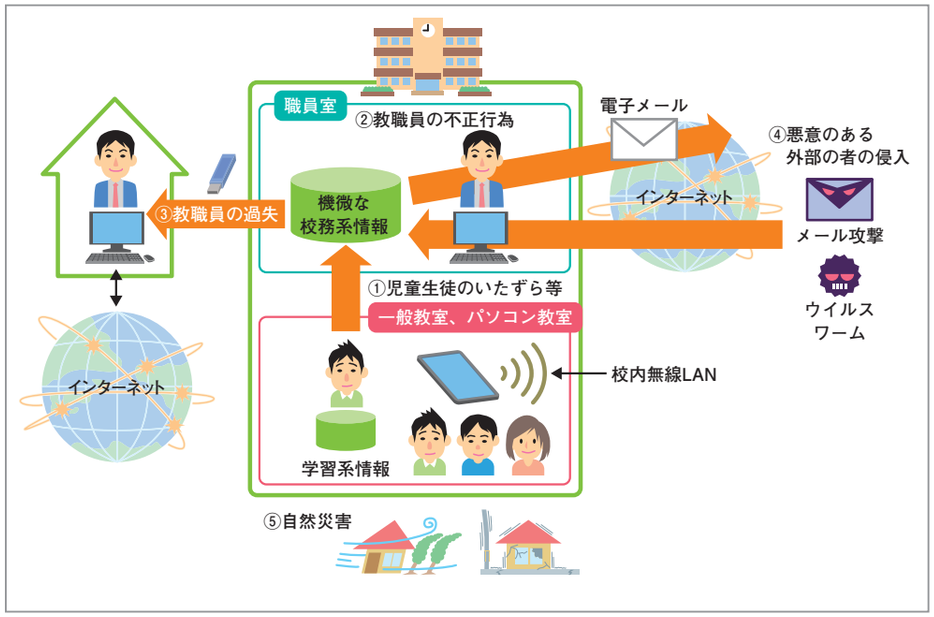
図1.4　学校における情報セキュリティの脅威



(1) 内部脅威

内部脅威とは、学校のなかに潜む情報セキュリティの脅威を指し、3つの脅威が存在します（図1.5参照）。

1　児童生徒のいたずら等による脅威

学校は児童生徒が学ぶ場所であり、児童生徒は学習活動を通して、パソコンやタブレットを使って作品を作り、インターネットにアクセスして調べ学習を行います。

児童生徒は、興味関心の塊ですので、パソコンやタブレットを使ってあらゆるところにアクセスしようとします。そのため、成績情報など児童生徒が見てはいけない機微な情報に対して、児童生徒がアクセスするなどの脅威が存在します。

2　教職員の不正行為による脅威

教職員は、重要な情報資産を取り扱うことが許可された立場です。重要な情報資産を取り扱うことができる内部の人間は、情報資産の外部漏えいや改ざんなどが実行可能なため、教職員による意図的な情報窃取、改ざん脅威が存在します。

また、使用するパソコンのセキュリティ設定を変更するなど、セキュリティレベルを下げる行為も不正行為に該当します。

そのために、情報資産の取り扱いやシステムの利用についてルールを規定する必要があります。

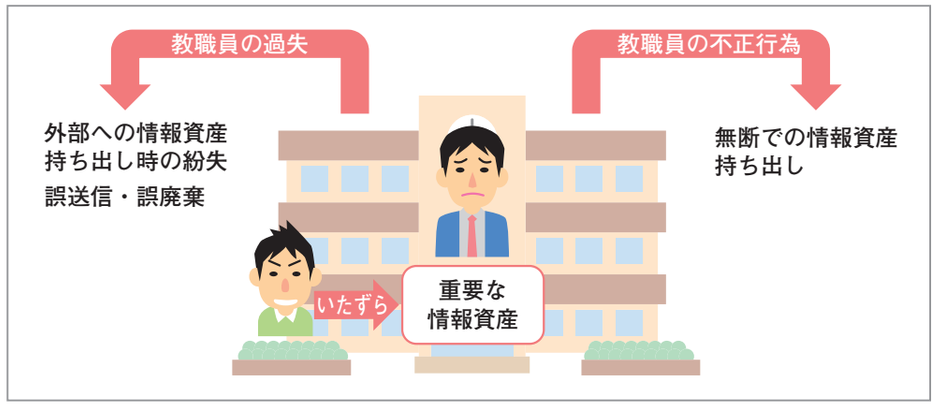
3　教職員の過失による脅威

情報資産への「脅威」は意図的な不正行為だけが原因になるわけではありません。教職員が情報を外部に持ち出し、盗難やうっかりミスにより紛失することで、結果として漏えいしてしまうということも「脅威」です。

特に、情報資産を外部に持ち出すケース、たとえばUSBメモリ等記録媒体に情報資産をコピーして持ち出す場合や、外部メールに情報資産を添付して送信する場合や廃棄行為において起こりがちです。

学校内部で情報資産を取り扱う限りにおいては、比較的安全ですが、外部に情報資産を持ち出す場合は、セキュリティ対策を施したシステムの外側に持ち出した人間の安全管理に委ねられるため、セキュリティレベルが低下し、セキュリティ事故が起こりやすい状態になります。

図1.5　情報資産に対する内部脅威



(2) 外部脅威

インターネット上には授業で活用したい様々な写真や動画などが存在する一方で、重要な情報資産を盗みだしてやろうと企む悪意のある人間が存在し、インタ

(2) 学校の情報セキュリティを管理する側

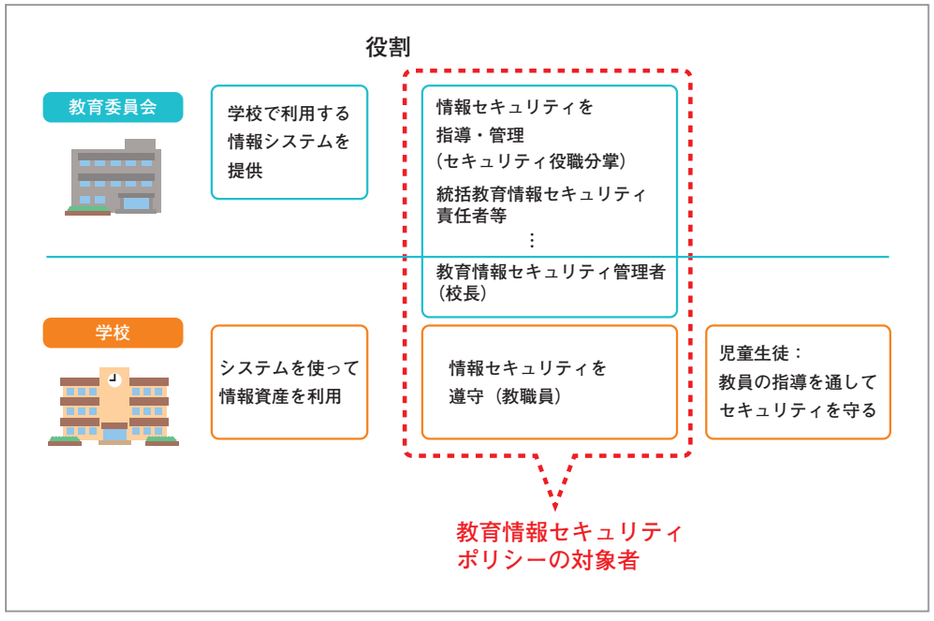
教職員のセキュリティ面を管理する「教育情報セキュリティ管理者」が配置され、学校におけるセキュリティ管理を実行します。さらに、学校の情報セキュリティを管理する実務者として、「学校教育情報セキュリティ・システム担当」が校務分掌で配置され、システム面でのセキュリティ対策の現場対応や教育情報セキュリティ管理者を補佐します

4-3 教育委員会と学校の役割分担

教育委員会と学校で役割分担をして情報セキュリティを維持する組織体制を作ります（図1.12参照）。

児童生徒は、学習活動を通して、学習系システムで作品を作ったり、ワークシートに考えを記入したりしますので、情報システムの利用者といえますが、まだ責任能力を問える立場にはないため、教育情報セキュリティポリシーの対象者としないで、教員の指導を通して、情報セキュリティポリシーを守ることとしています。

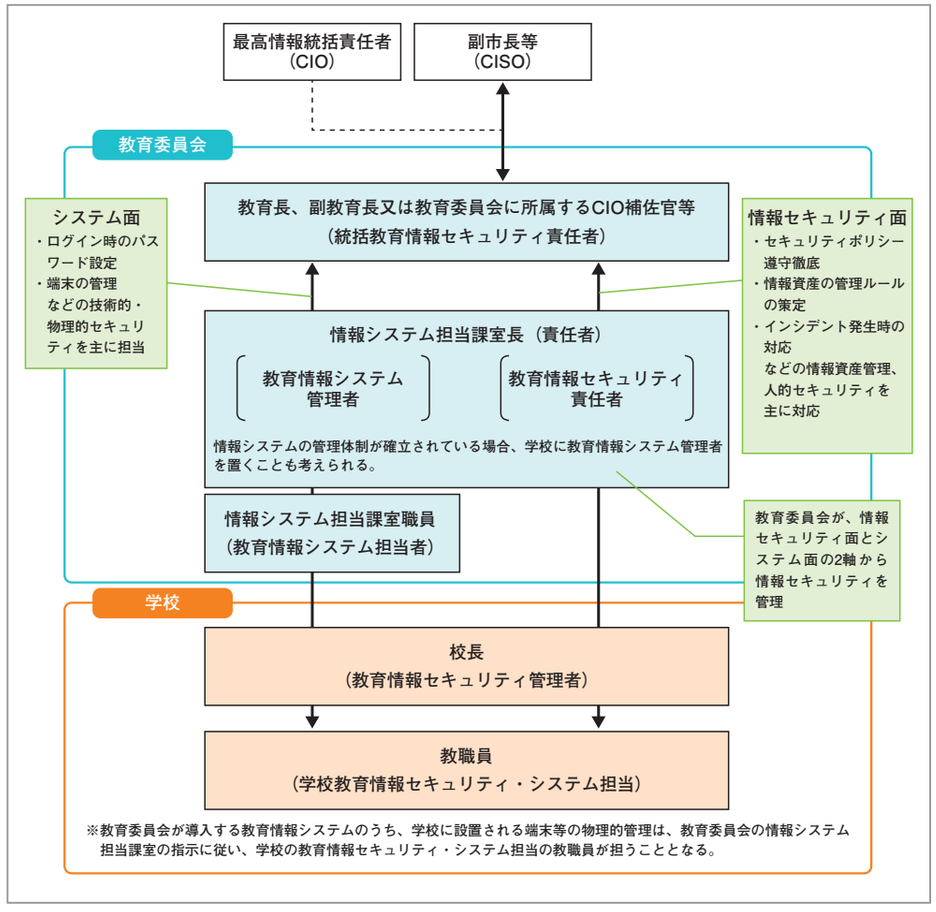
図1.12　教育委員会と学校の役割分担



4-4 組織体制の基本的考え方

教育委員会と学校の役割分担を踏まえて、ガイドラインでは図1.13に示すように、教育委員会と学校をまたがる組織体制の基本系を提示しており、学校から見ると、システム面と情報セキュリティ面の2軸で教育委員会と対応する形になります。

図1.13　情報セキュリティ推進の組織体制例



以上がガイドラインの考え方ですが、地方公共団体では個々に事情が異なるため、必ずしも組織体制の考え方に沿っていない場合もあります。ただ、情報セキュリティを守る体制として、学校だけでは無理で、システムを構築する教育委員会と、利用して教育活動に取り組む学校で、役割分担した体制構築が必要であり、

1 情報資産の取扱い

学校において、重要な情報資産を取り扱うことができる人は、その情報資産に対して許可された人に限定しています。許可された人は、そうでない人に対して情報秘匿する義務があります。

1-1 秘匿すべき情報が容易に目に入る状況の放置禁止

児童生徒からの校務系情報の秘匿については、児童生徒が学習系端末から校務系情報にアクセスできないよう、技術的なセキュリティ対策が必要ですが、職員室等では、児童生徒が教職員の傍らに近寄って、校務系情報の盗み見をする危険性が残ります。特に教職員のID/パスワードが盗まれた場合には、非常に危険な事態になりますので注意が必要です。

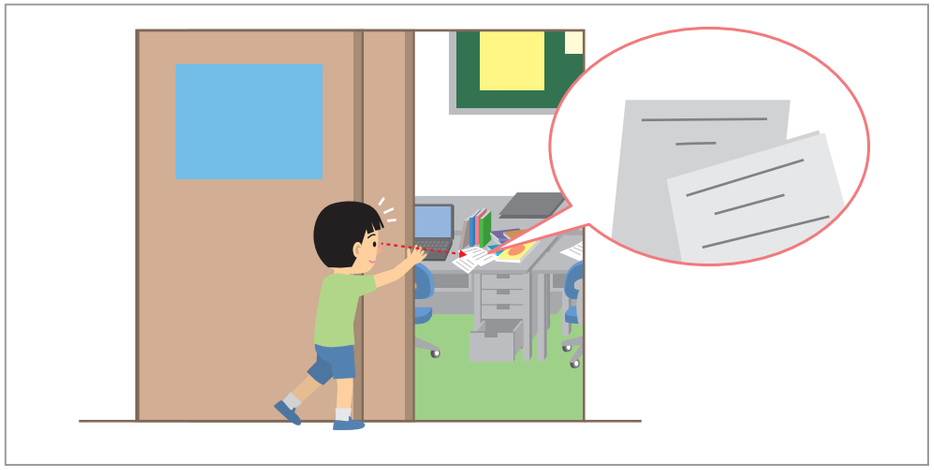
事例 11

ある学校で、同校生徒が教職員サーバに接続して情報を持ち出し、多数の生徒個人情報がインターネット上に流出する事故が発生した。この生徒は、教職員が管理するサーバにログインして情報を盗んでおり、ログインに必要なパスワードを見て記憶し、アクセスしていた。

気をつけたいポイント

1. ID、パスワードをメモしたファイルが、インターネットに接続できるパソコンやサーバに、そのまま保管されていないか
2. ID、パスワードが書かれた付箋紙やメモがパソコンの傍らに貼られていないか
3. 教職員用パソコンが表示されたまま放置されていないか
4. 重要書類が机上に放置されていないか

図2.1：秘匿すべき情報が容易に目に入る状況イメージ



事例 12

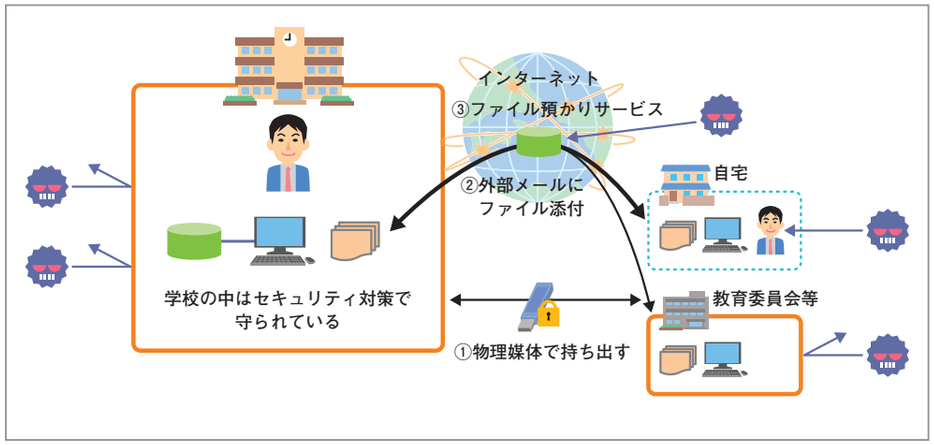
2015年から2016年にかけ、聞き出したID/パスワードを使い、外部の者が無線LAN経由で公立高校の校内LANに侵入した。一般の生徒がアクセス可能な学習用サーバを経由して校務系サーバに入り、成績を含む個人情報を窃取した。校内の学習系ネットワークにアクセスして、そこで校務系サーバのパスワードのヒントを得ていたことが、情報漏えい事故につながった。

気をつけたいポイント

パスワードとは、本人のみが知っている前提で、本人であることを証明する情報です。そのため、他者に漏えいしないようにパスワードを記憶しておくことが求められます。一方で、生年月日や氏名をベースにしたパスワードは容易に推定できるため、個人認証のセキュリティレベルが低いと指摘されています。

パスワードは推測困難なものとするために、8ケタ以上、英大文字小文字、数字、記号などから3種類以上の文字種を組み合わせたものが安全とされています。しかし、他者が推測困難なものは本人も記憶が難しいことも事実です。その場合には、手帳等にパスワードを記入して、それを横机等の施錠保管できる棚で保管管理してください。重要なのは、他者に知られないことです。

図2.2：情報資産の外部持ち出し形態（3種類）



2-2 USBメモリによる情報資産の外部持ち出し

外部に情報資産を持ち出す際のセキュリティ事故は後を絶たず、平成27年度に起きた教職員よる個人情報漏えい数では、全体の1/3がUSBメモリによる情報資産の外部持ち出し関連でした。

USBメモリは小さい中にたくさんの情報を収納し、携帯に便利で手軽に利用できます。しかし、情報資産を外部に持ち出すときは、持ち出す人に管理責任をゆだねなくてはならない時点でセキュリティレベルが下がり、情報資産を持ち出す際のセキュリティ事故は後を絶ちません。

ガイドラインでは、大多数の学校において、情報資産の外部持ち出しにUSBメモリを利用しており、そこでのセキュリティ事故が多発していることを重視して、セキュリティ対策の考え方を規定しています。

事例 13

USBメモリを持ち出してから自宅に戻る間に、懇親会があり、酔いすぎて帰宅最中に、電車のなかに大事な情報が入ったカバンを置き忘れた。

事例 14

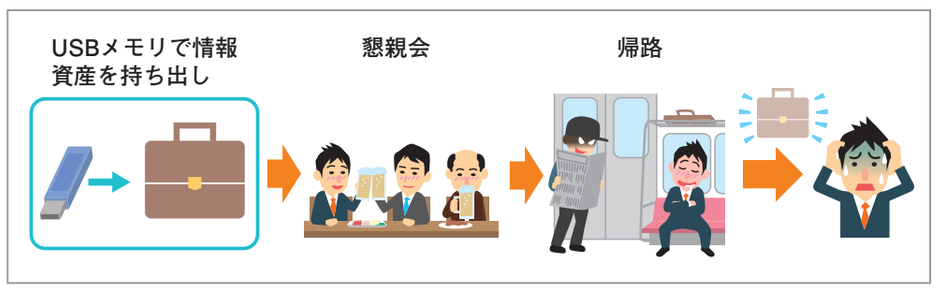
車でUSBメモリを持ち帰る途中で、コンビニに立ち寄り、買い物をして車に戻ったら、車上荒らしに合って、カバンごと盗まれた。

気をつけたいポイント

重要な情報資産を収納したUSBメモリをカバンごと置き忘れるケースは毎年多数発生しています。

学校からUSBメモリを持ち出し、途中で懇親会や別の用事があると、紛失、置忘れが起きます。自宅など目的地まで直行することが欠かせません。車通勤の場合は、駐車中の車上荒らしの被害も後を絶たっていませんので、大事な情報を持ち歩く際には寄り道をしないことが鉄則です。

図2.3：USBメモリ持ち出し中の紛失例



事例 15

教員が私物のUSBメモリを持ち込み、校務用パソコンに接続して、情報資産を持ち帰ったが、このUSBメモリはウイルスに感染しており、自分の教務用パソコンに感染し、ネットワークを介して学校のほとんどのパソコン、サーバがウイルス感染した。その結果、大規模な情報漏えいが起きた。

気をつけたいポイント

USBメモリはウイルス感染を媒介する危険性もあり、セキュリティ対策が施された環境で安全なものだけを利用してください。

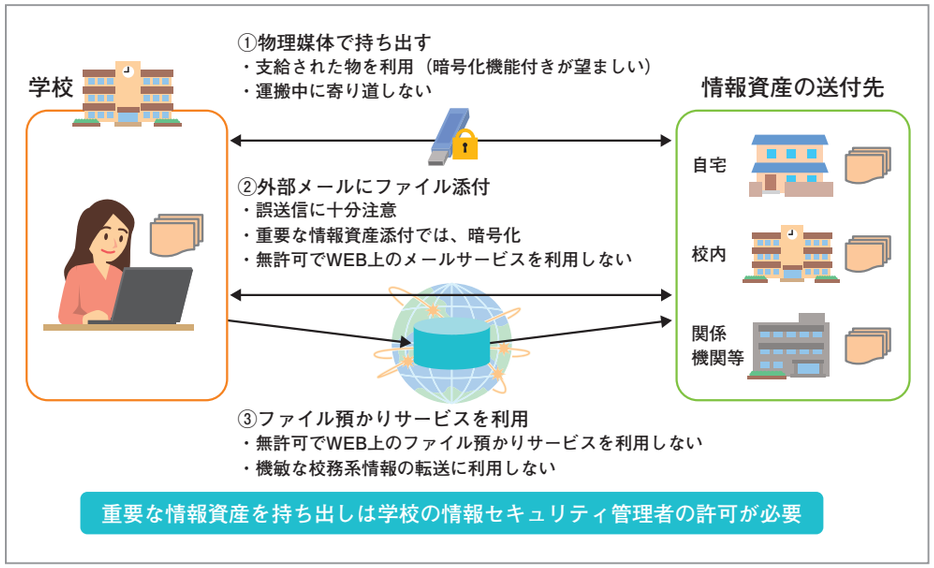
私物のUSBメモリを無許可で校務に利用することは、ウイルス感染を引き起こす危険な行為です。持ち出す情報資産によっては外部情報漏えいに相当しますので、絶対にしてはいけません。

員が自宅で安全に情報資産を扱うことについて事前に確認を取ることが求められます。

　また、情報資産は持ち出す段階から、パスワード設定し、自宅での事務処理が終わったら、USBメモリ等から該当の情報資産をすみやかに消去し、コピーを残さないことを誓約させることも必要です。

図3.1に情報資産の外部持ち出しで注意点を示します。

図3.1：情報資産の外部持ち出しにおける注意点



(2) 情報資産の持ち出しの記録

　情報資産の管理については、学校内部で取り扱う分には問題は起こりにくいのですが、リスクが高いのが情報資産の持ち出し及び廃棄です。廃棄の場合も、学校から外部に情報資産を持ち出す行為ですので、現況管理の観点から、重要性の高い情報については管理簿で記録を残すことが必要になります。

　学校からの情報資産の出入りについて記録が残らないと保管管理が不徹底になり、情報セキュリティ事故において原因究明に支障をきたします。

(3) 情報資産の持ち出し管理簿等

　学校からの情報資産を持ち出す場合に必要と思われる管理簿を下記に示します。

❶情報資産の持ち出し管理簿

　USBメモリ等記録媒体による外部持ち出しは、持ち出し・持ち帰りで記録を付け、返却を確認することが必要です。また、記録媒体紛失の観点から記録媒体の使用管理も併せて行います

　外部メールやCD-ROM等での持ち出しも含めて、学校から外に持ち出せない情報資産を例外として持ち出す場合には、記録を残すことが必要です（参考　別紙1参照）

❷情報資産の廃棄管理簿

　情報資産の廃棄も、外部持ち出しに相当します。廃棄の記録を残すことで誤廃棄であるかどうかの判別や、紛失・盗難との区別を明確にすることができます（参考　別紙2参照）

❸自宅作業のための私物パソコン使用申請書

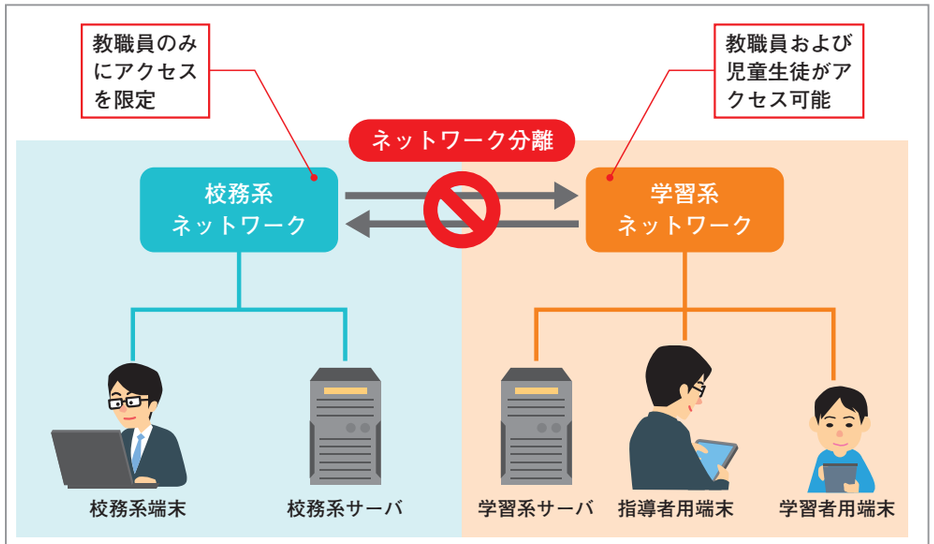
　教職員の自宅のパソコン環境のセキュリティ対策を確認することが目的です。サポート切れのOS使用やウイルス対策ソフトが入っていないようなケースでは、自宅パソコンでの業務処理は認められませんので自宅での情報資産の取り扱いにおいては、事前に確認することが必要です（参考　別紙3参照）

コラム 22

無許可で重要な情報資産を持ち出す行為がもたらすこと

　無許可で学校から持ち出せない重要な情報資産を持ち出す場合や、学校が教職員による情報資産の持ち出し全般を放置している場合、これらは何を意味するのでしょうか？

図4.4：学習系システムと校務系システムの通信経路の分離



出典：「教育情報セキュリティポリシーに関するガイドライン」ハンドブックP17 図表17

(2) 児童生徒が教職員になり代わって機微な校務系情報にアクセスするリスクへの対策

児童生徒が先生のパソコンにアクセスしてもログインできないように管理する必要があります。これは校務用パソコンだけではなく、教室で先生が利用する指導者用パソコンでも同じです。

端末のログインはID・パスワードで行うケースが多数だと思いますので、教職員はくれぐれもID・パスワード情報が流出しないように気を付けてください。

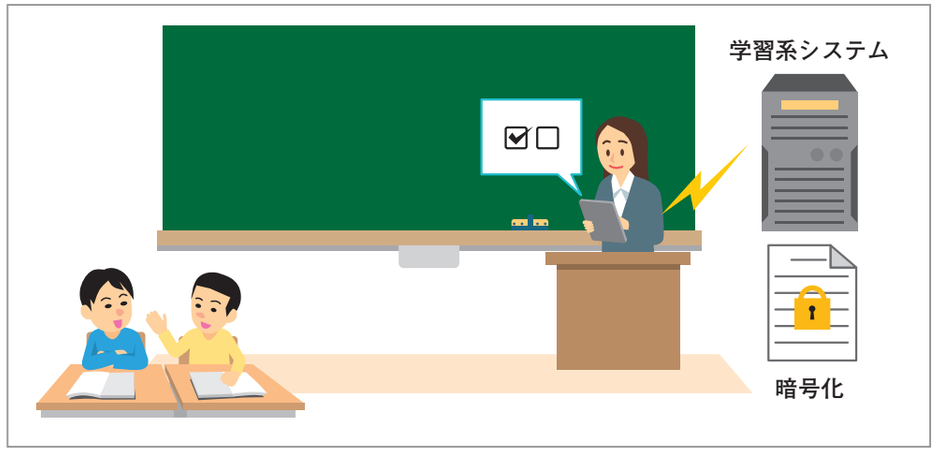
(3) 学習系システムへの機微な校務系情報保管の禁止

校務系システムが扱う情報と学習系システムで扱う情報とでは、重要性分類が違います。重要性分類に明らかな差異があると、情報資産のセキュリティ対策が異なるため、システムを分けて管理することが有効となります。

機微な校務系情報とは、重要性分類Ⅰ、Ⅱに相当する児童生徒に関する成績情報、学籍情報、出欠情報、保健観察情報など児童生徒及び保護者に関する機微な個人情報が含まれているもので、外部漏えいがあった場合には、個人のプライバシーや教育活動に重大な支障を及ぼすため、教職員しか扱えない情報として、厳重な安全管理が必要です。

この機微な校務系情報のなかには、教室でしか取得できない情報があります。児童生徒の出欠情報、健康観察情報、学習所見情報です。これらの情報は、教員が教室で手帳などに記録し、職員室で校務用パソコンにデータ投入しますが、図4.5に示したように、教室で直接データ投入できると非常に便利です。

図4.5：学習系システムへの機微な校務系情報保管の禁止



しかし、この場合には、教室でつながるのは学習系システムになりますので、学習系システムに機微な校務系情報を保管する形態となります。学習系システムは児童生徒がアクセスできますし、機微な校務系情報と学習系情報では、重要性分類が違うため別システムで管理する原則に反してしまいます。

ガイドラインでは、機微な校務系情報は学習系システムには保管せずに校務系システムに保管することを求めています。ただし、この場合のように機微な校務系情報を学習系システムに保管せざるを得ない場合には、保管する機微な校務系情報を暗号化するなど情報が外部漏えいしてもすぐには解読されないように安全措置を講ずることを求めています。

ここで注意いただきたいのは、全ての学習系情報まで暗号化などの安全措置は求めていないことです。学習系情報は、児童生徒が活用しやすい環境であることが必要ですので、機微な情報は扱わないことで活用を優先しようとしています。