# 教育現場におけるセキュリティ対策Ⅲ
（人的セキュリティ）

合同会社KUコンサルティング　高橋 邦夫

National Institute for
School Teachers
and Staff Development

独立行政法人教職員支援機構

# 目次

# 1　人的セキュリティ

## 基本的な考え方

人的セキュリティ対策とは、**情報資産を取り扱う当事者のルール遵守などを通じて情報資産を守る対策**を指します。運用上の過失等からのセキュリティ侵害を最小限に抑え、情報資産の安心・安全な運用を維持するためには、人的セキュリティ対策が効果的です。当事者一人ひとりが、情報セキュリティ意識を高く持ち、それに基づく行動を徹底しなければ、**物理的セキュリティ対策、技術的セキュリティ対策を講じていたとしても、重大な情報セキュリティインシデントにつながりかねません**。様々な立場の人が情報資産を取り扱うという特徴を持つ教育現場では、教職員等のルール遵守を徹底させるとともに、教育現場での事故事例等を踏まえた研修を実施することが重要です。加えて、教育情報セキュリティ管理者(校長)からの働きかけ、児童生徒への指導等を通じて、**一人ひとりに遵守すべき内容とその必要性を浸透させることが重要**です。

## 人的セキュリティの具体例

ルールの遵守

研修の実施

児童生徒への指導

# 2　人的セキュリティ（教育情報セキュリティ管理者（校長）の措置事項）

**【ポイント】**

**教育情報セキュリティ管理者（校長）は、教職員等の情報セキュリティ意識の醸成、情報セキュリティポリシー等の遵守指導、自校の情報セキュリティ対策に関する自己点検を行うなど、自校の情報セキュリティ確保に関する責任を担います。**

## 教育情報セキュリティポリシーに関するガイドライン（抄）

**【例文】**

**＜前略＞**

（２）教職員等の情報セキュリティ意識醸成

① 教育情報セキュリティ管理者は、教職員等に対して、日頃から情報セキュリティに関する話題を積極的に提供し、情報セキュリティ研修を受講させるなど、積極的にセキュリティ認識の向上を図らなければならない。

② 教育情報セキュリティ管理者は、校内でセキュリティ事故につながりかねないヒヤリ・ハット事案を抑止するために、教職員等が事案を発見した際に、ただちに対処し、すみやかに報告が上がるよう、教職員等に対する情報セキュリティ意識の醸成と風通しのよい関係性維持に努めなければならない。

③ 情報セキュリティポリシー等の閲覧容易性確保

教育情報セキュリティ管理者は、教職員等が常に教育情報セキュリティポリシー及び実施手順を閲覧・確認できるように配慮しなければならない。

**【解説】**

**＜前略＞**

（２）教職員等の情報セキュリティ意識醸成

教育情報セキュリティ管理者は、教職員等に対する情報セキュリティ意識の醸成及び風通しのよい関係性維持を行わなければならない。また、教職員等が情報セキュリティポリシーを遵守する前提として、イントラネット等に掲示する方法により、教職員等が常に最新の情報セキュリティポリシー及び実施手順を閲覧できるようにしなければならない。

# 3　人的セキュリティ（教職員等の遵守事項）

## 教育情報セキュリティポリシーに関するガイドライン（抄）

**【例文】**
**＜前略＞**
（3）支給端末の取扱い
① 教職員等は、業務目的以外で支給端末を利用してはならない。
② 教職員等は、外部のソフトウェアを無断で支給端末にインストールしてはならない。
業務上必要な場合には、事前に教育情報セキュリティ管理者の許可を得ること。
③ 教職員等は、支給端末の利用において、下記のカスタマイズを無断でしてはならない。
(ア)セキュリティ機能に関する設定変更 (イ)メモリ増設等の改造
④ 教職員等は、モバイル端末を利用する場合は、盗難・紛失リスクに備えての安全管理をすること。
⑤ 業務端末から離れる時は、端末をロックするなど、他者が閲覧できないようにしなければならない。
⑥ 業務終了後と外出時には、電源を落とさなければならない。

支給されている端末については、業務目的以外で利用してはならず、また、端末から離れる際は端末をロックする等、他者が閲覧できないように留意する必要があります。また、自宅や学校外等での情報処理作業においても支給された端末を利用することとし、支給以外の端末等は原則利用してはいけません。

# 教育情報セキュリティポリシーに関するガイドライン（抄）

**【例文】**

**＜前略＞**

（19）児童生徒への指導事項

教職員等は、児童生徒に学習者用端末等を利用させるに当たり、以下の事項について指導を行わなければならない。

① 学習用途の利用限定
学習者用端末及び学習系クラウドサービスは学習目的で利用すること。

② 利用者認証情報の秘匿管理
ID及びパスワードは他の人に知られないようにすること。

③ ウイルス対策ソフトウェアの管理
ウイルス対策ソフトウェアは常に最新の状態に保つこと。

④ 端末のソフトウェアに関するセキュリティ機能の設定変更禁止
利用する端末のセキュリティ機能の設定を、許可なく変更してはならないこと。

⑤ 学習系情報は学習系クラウドに保管
端末で生成した情報の保存先を学習系クラウドに指定できる機能がある場合には、この機能を利用して原則学習系クラウドに保管し、学習者用端末にローカル保存は必要最小限とすること。

⑥ 無断で外部ソフトウェアをインストール禁止
無断で外部ソフトウェアをインストールしないようにすること。

⑦ コミュニケーションツールの利用制限
学校から許可されたコミュニケーションツール（SNS,チャット等）のみを利用すること。

⑧ ウイルス感染が疑われる場合の報告
学習用端末が動かない、勝手に操作されている、いつもと異なる画面や警告が表示されるなどの症状がでた場合、すぐに担任教員に報告すること。

⑨ 端末の安全な取扱い
学習用端末は大事に取り扱い、盗難・紛失・破損等に注意すること。

**【解説】**
**＜前略＞**
（19）児童生徒への指導事項
　学校における情報の取扱いは、教職員等のみならず、児童生徒も含まれる。GIGAスクール整備以降、児童生徒による学習活動のデジタルシフトが加速化しており、児童生徒による情報セキュリティの確保は、学校の情報セキュリティ確保のなかで大きな比重を占めるものとなってきた。その意味で児童生徒に情報モラル・セキュリティ指導を通して情報セキュリ ティ意識を醸成させる教員の役割は大きい。本項では、児童生徒に指導いただきたい内容について記載している。

教職員等のみならず、児童生徒も学校の情報を取り扱う主体となることから、教職員等は児童生徒に学習者用端末等を利用させるに当たり、十分に指導を行う必要があります。

# ４　人的セキュリティ（研修・訓練）

## 教育情報セキュリティポリシーに関するガイドライン（抄）

【例文】
＜前略＞
（２）研修計画の策定及び実施
① CISOは、教職員等に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行い、情報セキュリティ委員会の承認を得なければならない。
② 研修計画において、教職員等は、毎年度最低１回は情報セキュリティ研修を受講できるようにしなければならない。【推奨事項】
③ 新規採用の教職員等を対象とする情報セキュリティに関する研修を実施しなければならない。
④ 研修は、統括教育情報セキュリティ責任者、教育情報セキュリティ責任者、教育情報セキュリティ管理者、教育情報システム管理者、教育情報システム担当者及びその他教職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。
⑤ CISOは、毎年度１回、情報セキュリティ委員会に対して、教職員等の情報セキュリティ研修の実施状況について報告しなければならない。

情報セキュリティを適切に確保するためには、情報セキュリティ対策の必要性と内容を全ての教職員等が十分に理解していることが必要不可欠である。また、情報セキュリティインシデントの多くは、教職員等の規定違反に起因している場合もある。さらに、情報セキュリティの向上は、利便性の向上とは、必ずしも相容れない場合がある。教職員等が業務を優先することが、情報セキュリティ対策の軽視につながることもある。また、情報セキュリティに関する脅威や技術の変化は早いことから、教職員等に対しては、常に最新の状況を周知することが重要である。

# 5　人的セキュリティ（情報セキュリティインシデントの連絡体制の整備）

## 教育情報セキュリティポリシーに関するガイドライン（抄）

**【例文】**
（１）学校内からの情報セキュリティインシデントの報告
① 教職員等は、情報セキュリティインシデントを認知した場合、速やかに教育情報セキュリティ管理者に報告しなければならない。
② 報告を受けた教育情報セキュリティ管理者は、速やかに統括教育情報セキュリティ責任者、教育情報システム管理者及び情報セキュリティに関する統一的な窓口に報告しなければならない。
③ 教育情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、必要に応じてCISO及び教育情報セキュリティ責任者に報告しなければならない。
＜略＞

情報セキュリティインシデントやその発生の予防が重要なことは言うまでもないが、実際に情報セキュリティインシデントを認知した場合に、責任者に報告を速やかに行うことにより、被害の拡大を防ぎ、早期に回復を図れるようにしておく連絡体制を整備することも必要である。

# 6　まとめ

セキュリティ対策を講じるに当たっては、物理的セキュリティや技術的セキュリティもさることながら、情報資産を取り扱う当事者のルール順守などを通じた人的セキュリティが徹底されていなければ、意味をなしません。

このため、教職員一人ひとりが、情報セキュリティ意識を高く持つだけでなく、児童生徒も情報資産に触れる可能性があることを踏まえ、児童生徒への指導等を通じて、**学校現場一人ひとりが順守すべき内容とその必要性を浸透させることが重要**です。