大分市立学校における情報セキュリティの基本方針

大分市教育委員会

1　趣旨

大分市立小中学校（以下、「学校」という。）において取り扱う情報には、市民の個人情報や教育行政及び学校の運営上重要な情報等、改ざんや外部への漏えい等が発生した場合に極めて重大な影響を及ぼす情報が多数含まれています。また、その情報を処理し、業務や事務を行う情報システムにおいても、システム停止や不正動作等があった場合には、同様に市や市民及び市の教育行政に対し重大な影響を及ぼすこととなります。学校は、保有する「情報（注１）や情報システム（注２）（以下、「情報資産」という。）」を適切に保護し、責任を持って管理する義務があります。

さらに、近年の情報・通信技術の発達とそれにともなう高度情報化社会の出現は、教育における情報化に対して構造的変革をもたらしており、情報セキュリティ対策においても、情報化に対応した対策の実施が要求されています。特に情報ネットワークを介した情報システムの比重が高まるにつれ、市民や学校、他の教育機関等との情報交換や連携処理が広く行われるようになり、情報セキュリティにおいて従来の「情報を保有し処理することにより生じる直接的責務」に加え、「情報化社会の一構成員としての社会的責務」を果たす必要があります。

本市教育委員会は、学校における情報資産の情報セキュリティ要件である機密性、完全性、可用性（注３）を確保･維持すると共に、情報化社会における社会的責任を果たすため、統一的・体系的な情報セキュリティ対策を実施することとし、ここに「大分市立学校における情報セキュリティの基本方針（以下、「基本方針」という。）」及び「大分市立学校情報セキュリティ対策基準（以下、「対策基準」という。）」を定めます。

（注１）

「情報」：学校の業務に携わる全ての教職員及び委託事業者（以下「教職員等」という。）が業務上作成し、又は取得したすべての文書等のうち電磁的に記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録をいう。）されたもの及び電子計算機処理に係る入出力帳票をいう。

（注２）

「情報システム」：ハードウエア、ソフトウェア、通信網、記録媒体等及びこれらで業務処理を行う仕組み並びにこの仕組みを開発、運用及び保守するために作成された資料等をいう。

（注３）JIS X 5080:2002 による定義

「機密性」：アクセスを認可された者だけが情報にアクセスできることを確実にすること。

「完全性」：情報及び処理方法が、正確であること及び完全であることを保護すること。

「可用性」：認可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること。

2　適用範囲

教職員等及び情報資産

3　対抗する脅威

本市教育委員会が学校の情報セキュリティ対策の策定及び実施にあたり、情報資産への脅威として認識するものは以下のものです。

（1）　教職員等によらない物理的及び論理的侵入・窃盗・妨害・破壊・盗聴・なりすまし、改ざん等

（2）　教職員等による操作ミス、破壊、紛失、物理的及び論理的侵入・窃盗・妨害・盗聴・なりすまし、改ざん、著作権違反、業務目的外使用等

（3）　コンピュータウイルス、ワーム等の悪意のあるプログラム

（4）　地震、雷、火災、風害、水害等の災害及び停電、回線断、故障、異常動作、容量超過等

本市教育委員会はこれら脅威に対抗し、学校の情報資産の機密性、完全性、可用性を確保･維持する対策を実施します。

4　基本的な考え方

本市教育委員会は学校における情報セキュリティ対策の基本的な考え方を以下に示します。

（1）　情報セキュリティ対策の構成

学校における情報セキュリティ対策は次のものにより構成され、それに基づき実施します。

①「基本方針」：情報セキュリティ対策に関する統一的かつ基本的な方針を定めたもの。

②「対策基準」：基本方針に基づき情報セキュリティを確保するために遵守すべき行為等の基準について定めたもの。

なお、個々の情報資産の情報セキュリティ対策においては、「基本方針」「対策基準」に基づき、情報資産毎に、より具体的な「情報セキュリティ実施手順」を策定し、実施することになります。

（2）　教職員等の責務

学校の情報資産を利用する者は、情報セキュリティの重要性を認識するとともに、この基本方針を指針とする情報安全対策を実践します。

教職員等は、基本方針及び対策基準を理解し、遵守することで、学校が保有する情報資産を適切に保護します。

（3）　組織・体制

学校における情報セキュリティ対策は、責任や役割を明確にした組織・体制のもとに行うものとします。

（4）　情報の分類と管理

学校の情報システムにおいて取扱う情報について、重要な情報を重点管理する考え方から重要度に応じた情報分類の定義を行い、情報の管理責任及び管理方法を明確にします。

（5）　人的セキュリティ

情報セキュリティに関する役割や責任を明確化し、教職員等に基本方針及び対策基準の内容を周知徹底するため、研修等の必要な対策を講ずるものとします。

（６） 物理的セキュリティ

情報システムの設置場所について、不正な立入り、損傷及び妨害から情報資産を適切に保護するため、入退室管理等の物理的な対策を講ずるものとします。

（７） 技術的対策及び運用管理

学校の所有する情報資産を不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等の必要な対策を講ずるものとします。

（８） コンピュータウイルス等の不正プログラム対策

学校の情報資産をコンピュータウイルス等の不正プログラムから適切に保護するため、また、自らが加害者にならないために必要な対策を講ずるものとします。

（９） 媒体の取扱及び管理

学校の情報システムにおける取り外し可能な記録媒体について、適正な管理をするための対策を講ずるものとします。

(10) 情報システムの開発・導入・保守

学校の業務に使用する情報システムの開発・導入・保守においては、情報資産を適切に保護するために必要な対策を講ずるものとします。

(11) 委託

学校の情報システムの開発、運用、保守等を外部に委託する場合は、情報セキュリティに関する必要な対策を講ずるものとします。

(12) 情報セキュリティに関する事案への対応

情報セキュリティに関する事案が発生した場合の対応をあらかじめ定めるとともに、情報セキュリティに関する事案が発生した際には、定められた対応を迅速かつ円滑に実施し、その影響を最小限にするとともに、再発防止のために必要な対策を講ずるものとします。

(13) 評価・見直し

新たな脅威等を踏まえ、定期的に基本方針、対策基準及び情報セキュリティ対策の評価を行い、情報システムの変更、基本方針及び対策基準の見直しを実施します。

５ 公開範囲

本「基本方針」は、教職員等に対して学校の情報セキュリティ対策への指針を示すため、また市民・団体等に対して学校の情報セキュリティ対策への理解を得るため、広く公開を行うものとします。

附 則

この基本方針は、平成２２年４月１日から施行する。

附 則

この基本方針は、平成２６年４月１日から施行する。