新宿区立学校情報セキュリティ対策基準

第1　総則

1　目的

この基準は、新宿区立学校情報セキュリティ要綱（令和８年２月１７日付け７新教指学第787号）に基づく学校情報セキュリティ対策を実施するに当たり、統一的に遵守すべき行為、判断等の基準を定めることを目的とする。

2　用語の定義

この基準において使用する用語の意義は、次に定めるものを除くほか、新宿区立学校情報セキュリティ要綱において使用する用語の例による。

(1)　庁舎　新宿区庁舎管理規則（昭和59年新宿区規則第39号）第2条に規定する庁舎、教育センター、学校をいう。

(2)　コンピュータウイルス　第三者のプログラム又はデータベースに対して、意図的に何らかの被害を及ぼすように作られたプログラム等で、自己伝染機能、潜伏機能又は発病機能を有するものをいう。

(3)　学校情報セキュリティインシデント　学校情報セキュリティに関する障害、事故、故障及びシステム上の欠陥をいう。

3　学校情報資産に対する脅威

学校情報セキュリティ対策を行う上で、特に留意すべき学校情報資産に対する脅威は、次に掲げる事項とする。

(1)　不正なアクセス又は誤操作による学校情報資産の破壊、持ち出し、盗聴、改ざん若しくは消去

(2)　構成機器、記録媒体又は帳票の破壊、紛失若しくは盗難

(3)　故意又は過失による情報の漏えい

(4)　コンピュータウイルス、地震、落雷、火災等による災害、学校情報セキュリティインシデント等による教育等のために用いる情報システムの停止

第2　学校情報資産の管理責任、重要性分類及び管理方法

1　学校情報資産の管理責任

(1)　学校情報資産の管理責任

学校情報資産を作成した学校の学校情報セキュリティ責任者は、当該学校情報資

産を管理する責任を有する。

(2)　管理責任の及ぶ範囲

学校情報資産を複製し、又は伝送した場合においては、当該複製され、又は伝送された学校情報資産を保有することとなった学校の学校情報セキュリティ責任者が管理する責任を有する。

(3)　教職員等の利用責任

学校情報資産を利用する教職員等（以下「利用教職員等」という。）は、当該学校情報資産を３の学校情報資産の重要性分類に基づき利用する責任を有する。

2　リスク管理

学校情報資産を管理し、又は利用する学校の学校情報セキュリティ責任者は、その学校情報資産に対する脅威を分析し、当該脅威に係る影響を評価し、並びに当該脅威の顕在化を予防するための対策及び当該脅威が顕在化した場合に被害を最小化するための手順を定めるものとする。

3　学校情報資産の重要性分類

学校情報資産を作成した学校の学校情報セキュリティ責任者は、当該学校情報資産の機密性、完全性及び可用性（利用教職員等が必要なときに学校情報資産にアクセスできることを確実にすること。）を踏まえ、当該学校情報資産を次に掲げる重要性分類に基づき分類し、目録を作成するものとする。

(1)　重要性分類Ⅰ

ア　教職員等及び児童・生徒の生命、財産、プライバシー等に重大な影響を及ぼす学校情報資産

イ　法令又は区の条例等により守秘されるものと規定されている学校情報資産

ウ　漏えいした場合、個人又は法人その他の団体の利益を害する等教育委員会又は学校に対する信頼を害するおそれのある学校情報資産

エ　滅失し、又はき損した場合、その復元が困難となり、教育委員会の円滑な執行又は学校の円滑な管理運営を妨げるおそれのある学校情報資産

オ　教育等のために用いる情報システムに係るパスワード及び当該情報システムの設定情報

(2)　重要性分類Ⅱ

重要性分類Ⅰに分類される学校情報資産以外の学校情報資産

4　学校情報資産の管理方法

(1)　学校情報資産の重要性分類の表示

学校情報セキュリティ責任者は、学校情報資産の重要性分類の表示をしなければならない。この場合において、第三者が重要性分類の識別を容易にすることができないよう留意しなければならない。

(2)　学校情報資産の管理

ア　学校情報セキュリティ責任者は、３の学校情報資産の重要性分類に基づき、学校情報資産にアクセスする権限を有する者を定めなければならない。

イ　教職員等は、重要性分類Ⅰに属する学校情報資産を当該学校の学校情報資産が所在する場所から外部へ持ち出し、又は送信してはならない。ただし、当該学校情報資産の内容、使用目的、持出し方法、管理方法等を明確にした上で、当該学校情報資産を管理する学校の学校情報セキュリティ責任者の承認を受けたときは、この限りでない。

ウ　教職員等は、支給されたもの以外の電子計算機、記録媒体等において、重要性分類Ⅰに属する学校情報資産を記録し、又は使用してはならない。

(3)　記録媒体の管理

ア　学校情報セキュリティ責任者は、学校情報資産を記録した媒体を適切に管理しなければならない。

イ　学校情報セキュリティ責任者は、最終的に確定した学校情報資産を記録した媒体については、書き込み禁止措置を講じた上で保管しなければならない。

ウ　学校情報セキュリティ責任者は、重要性分類Ⅰに分類される学校情報資産については、記録した媒体を施錠可能な場所に保管しなければならない。

(4)　学校情報資産の廃棄

教職員等は、重要性分類Ⅰに分類される学校情報資産が不要となった場合は、速やかに廃棄しなければならない。この場合において、当該学校情報資産を記録した媒体を廃棄するときは、学校情報セキュリティ責任者の承認を受け、当該学校情報資産を完全に消去する等復元できないようにした上で、廃棄しなければならない。

第3　物理的な対策

1　サーバ等

(1)　機器等

ア　教育ネットワーク等管理者は、教育ネットワーク等の障害が発生した場合にその教育等のために用いる情報システムの運用が停止しないよう、回線、機器等を冗長構成とする等の措置を講じるように努めなければならない。

イ　学校情報セキュリティ責任者は、教職員等並びに外部委託事業者及びその従業員以外の者が容易に教育ネットワーク等を操作できないような措置を講じなければならない。

ウ　教育ネットワーク等管理者は、サーバ等の重要な機器を設置する場合は、当該サーバ等について、次に掲げる学校情報セキュリティ対策を行わなければならない。

(ア)　設置及び利用場所が確定している電子計算機及び通信回線装置については、所定の設置場所から移動できない措置を講ずること。

(イ)　電子計算機及び通信回線装置については、不正操作されないための措置を講ずること。

(2)　配線

教育ネットワーク等管理者は、配線について、損傷、盗聴、侵入等をされることがないように可能な限り必要な措置を講じなければならない。

(3)　庁舎以外の場所に設置する機器等

ア　教育ネットワーク等管理者は、所管する教育等のために用いるネットワークに係る構成機器及び教育等のために用いる情報システムに係る電子計算機（以下「機器等」という。）を庁舎以外の場所に設置する場合は、新宿区情報化の推進に関する規則（平成20年新宿区規則第92号)第8条第1項の情報化統括管理者（以下「情報化統括管理者」という。）の承認を受けなければならない。

イ　教育ネットワーク等管理者は、定期的に機器等における学校情報セキュリティについて確認しなければならない。

2　管理区域

(1)　管理区域の指定

教育ネットワーク等管理者は、教育等のために用いるネットワークに係る構成機器、重要な教育等のために用いる情報システム及び重要性分類Ⅰに分類される学校情報資産を適正に管理するために、次の表に定めるとおり、事務室等を指定する。

管理区域の区分	管理区域
管理区域Ⅰ	重要な電子計算機、通信回線装置等を設置するために独立して設けられた部屋又は区画で、関係者以外の侵入や自然災害の発生等を原因とする学校情報資産に対するセキュリティ侵害（以下「侵害」という。）に対して、施設及び環境面から対策が講じられているもの
管理区域Ⅱ	事務室等又はその内部であって、関係者以外の侵入や自然災害の発生等を原因とする侵害に対して施設及び環境面から対策が必要な区域で、管理区域Ⅰ以外のもの

(2)　管理区域の管理

ア　管理区域Ⅰを定めた教育ネットワーク等管理者は、当該管理区域について、次の各号に掲げる措置を講じなければならない。

(ア)　入退室を、許可を受けた者に制限すること。

(イ)　鍵又は認証装置等により、入退室管理を行うこと。

(ウ)　入退室管理簿等により、入退室の記録を行うこと。

(エ)　その他管理区域の学校情報セキュリティを保つために必要な措置

イ　管理区域Ⅱを定めた教育ネットワーク等管理者は、管理区域に係る教育指導課職員並びに外部委託事業者及びその従業員の出入りを適正に管理しなければならない。

ウ　ア及びイのほか、学校情報セキュリティ責任者は、管理区域内における学校情報資産及び機器等に係る適切な学校情報セキュリティ対策を行わなければならない。

(3)　機器等の取得及び搬入等

ア　教育ネットワーク等管理者は、機器等を取得する場合には、あらかじめ当該機器等のシステムとの適合性に関し、教育指導課職員をもって確認しなければならない。

イ　教育ネットワーク等管理者は、管理区域に機器等を搬入し、又は管理区域から機器等を搬出するときは、教育指導課職員を立ち会わせる等必要な措置を講じなければならない。

3　教育等のために用いるネットワーク

(1)　教育ネットワーク等管理者は、教育等のために用いるネットワーク以外へのネッ

トワークの接続をする場合は情報化統括管理者の許可を得なければならない。この場合において、当該ネットワークの接続は、必要最低限のものにしなければならない。

(2) 学校情報セキュリティ責任者は、教育等のために用いるネットワークを使用して学校情報資産を伝送するとき、その伝送の途上において当該学校情報資産に破壊、盗聴、改ざん、消去等の被害が生じないように学校情報セキュリティ対策を行わなければならない。

第4 人的な対策

1 教職員等の役割及び責任

(1) 教職員等は、使用する端末又は記録媒体を第三者に使用されること及び学校情報セキュリティ責任者の許可なく学校情報資産を第三者に閲覧されることがないように、適切な措置を講じなければならない。

(2) 教職員等は、学校情報セキュリティ責任者の承認を得ずに、機器等を学校外に持ち出してはならない。

(3) 教職員等は、他の組織に異動した場合においても、異動前の組織での業務において知り得た学校情報資産を他に譲渡し、若しくは貸与し、又は使用させてはならない。教職員等が退職等により職を離れた場合においても、同様とする。

第5 技術的な対策

1 教育ネットワーク等及び学校情報資産

(1) 教育ネットワーク等管理者は、重要性分類Ⅰに分類されるログ及び学校情報セキュリティの確保に必要な記録（以下「ログ等」という。）について、必要があると認める場合には、当該ログ等について、盗難、改ざん又は消去等を防止する措置を講じ、適切に保存しなければならない。

(2) 教育ネットワーク等管理者は、記録される媒体の形態にかかわらず、重要性分類Ⅰに分類されるネットワーク構成図及び情報システム仕様書等（以下「ネットワーク構成図等」という。）を適切に保管しなければならない。

(3) 教育ネットワーク等管理者は、重要性分類Ⅰに分類される学校情報資産について、定期的にバックアップ用のデータを作製しなければならない。

2　教育ネットワーク等及び学校情報資産を使用する際の禁止等

(1)　業務目的以外の使用禁止

教職員等は、業務の目的以外のために教育ネットワーク等を使用してはならない。

(2)　学校情報資産の持ち出し及びインターネットによる伝送の禁止等

ア　教職員等は、重要性分類Ⅰに分類される学校情報資産を取り扱う場合には、次に掲げる行為を行ってはならない。

(ア)　学校外の場所への持ち出し（ただし、当該学校情報資産を管理する学校情報セキュリティ責任者が許可したときは、この限りでない。）

(イ)　インターネットによる教育等のために用いるネットワーク以外への伝送（ただし、統括学校情報セキュリティ責任者が許可したときは、この限りでない。）

イ　ア(イ)ただし書の規定による統括学校情報セキュリティ責任者の許可に基づき学校情報資産を教育等のために用いるネットワーク以外へ伝送する場合は、電子署名、通信経路の暗号化、本人認証、パスワード設定等高度なセキュリティ対策を講じなければならない。

ウ　教職員等は、原則として、支給されたもの以外の記録媒体を管理区域Ⅰに持ち込んではならない。

(3)　無許可ソフトウェアの導入の禁止

ア　教職員等は、自己に供用された端末等に対し、教育ネットワーク等管理者が認めるソフトウェア以外のソフトウェアを導入してはならない。

イ　教職員等は、教育ネットワーク等管理者が認めるソフトウェアを導入する場合においても、その提供元の信頼性が確保できることを確認した上で、ソフトウェアを入手しなければならない。

(4)　構成機器の変更の禁止

教職員等は、自己に供用された端末等について、構成機器の増設又は改造を行ってはならない。

(5)　教育等のために用いる情報システムに関するネットワーク構成図等及びソフトウェアの貸与

教育ネットワーク等管理者は、所管する教育等のために用いる情報システムに関するネットワーク構成図等又はソフトウェアを他の課等の情報セキュリティ責任

者に貸与する場合には、当該貸与が著作権法その他の法令に抵触しないことを確認した上で行わなければならない。この場合において、教育ネットワーク等管理者は、当該ネットワーク構成図等又はソフトウェアの取扱に関し、当該他の課等の情報セキュリティ責任者と協議の上、必要な事項について定めなければならない。

3　アクセス制御等

(1)　利用教職員等の登録

学校情報セキュリティ責任者は、所管する利用教職員等の登録、変更又は抹消を記録した学校情報資産を適切に管理しなければならない。

(2)　教育等のために用いるネットワークに対するアクセスの制限

教育ネットワーク等管理者は、教育等のために用いるネットワークを利用する権限を有しない教職員等によって不正に教育等のために用いるネットワークのサービスが利用されることがないよう適切に教育等のために用いるネットワークの管理を行わなければならない。

(3)　適切な教育等のために用いるネットワークの経路の制御

教育ネットワーク等管理者は、不正アクセス行為の禁止等に関する法律（平成11年法律第128号。以下「法」という。）第２条第４項に規定する不正アクセス行為を防止するため、教育等のために用いるネットワークの経路を適切に制御しなければならない。

(4)　教育等のために用いるネットワーク以外からのアクセス

教育ネットワーク等管理者は、教育等のために用いるネットワーク以外からのアクセスの許可を必要最低限にしなければならない。

(5)　教育等のために用いるネットワーク以外のネットワークとの接続

教育ネットワーク等管理者は、教育等のために用いるネットワーク以外のネットワークと接続しようとする場合には、当該ネットワークの構成、学校情報セキュリティのレベル等を詳細に検討し、学校情報資産及び機器等に影響が生じないことを確認しなければならない。

(6)　パスワード

学校情報セキュリティ責任者は、教職員等が使用するパスワードを、想像することが困難な文字列にする等適切な措置を講じなければならない。

(7)　特権を付与されたID

教育ネットワーク等管理者は、特権を付与されたIDについて、可能な限り初期設

定以外のものに変更しなければならない。

4　教育等のために用いるネットワークの導入、開発、保守等

(1)　教育等のために用いるネットワークの導入

ア　教育ネットワーク等管理者は、教育等のために用いるネットワークを新たに拡張し、又は他のネットワークに接続しようとする場合には、既存のネットワークに影響が生じないよう拡張又は接続する前に十分な試験を行わなければならない。

イ　教育ネットワーク等管理者は、アの試験による結果の記録のうち重要なものを厳重に保管しなければならない。

(2)　ソフトウェアの導入及び変更

ア　教育ネットワーク等管理者は、ソフトウェアを計画的に導入するとともに、導入に当たっては、当該ソフトウェアの適格性及び他のネットワークとの適合性について確認しなければならない。

イ　教育ネットワーク等管理者は、ソフトウェアについて学校情報セキュリティに重大な影響を及ぼすおそれのある不具合が発見された場合には、速やかに当該ソフトウェアの変更を行う等適切に対応しなければならない。

ウ　教育ネットワーク等管理者は、イの場合のほか、ソフトウェアの変更については計画的に行わなければならない。

(3)　教育等のために用いるネットワークの学校情報セキュリティインシデント及び不正行為への対策

教育ネットワーク等管理者は、教育等のために用いるネットワークの開発若しくは保守時の学校情報セキュリティインシデント又は不正行為に対する対策のため、必要な事項を別に定めなければならない。

(4)　教育等のために用いるネットワークに関する外部委託事業者

ア　教育ネットワーク等管理者は、新たに教育等のために用いるネットワークの開発を事業者に委託する場合は、情報の機密性に応じたセキュリティレベルが確保されていることを確認した上で、総務部契約管財課契約係に対し、当該事業者の経営状況等の調査を依頼し、当該開発の契約を適正に履行することが可能であるかどうかを確認しなければならない。

イ　教育ネットワーク等管理者は、外部委託事業者の従業員が委託した業務に従事するときには、当該外部委託事業者の従業員であることを証する身分証明書を事

前に提示させなければならない。

(5)　教育等のために用いるネットワークの変更

教育ネットワーク等管理者は、教育等のために用いるネットワークに重要な変更を加える場合は、情報化統括管理者の承認を得なければならない。

(6)　構成機器の廃棄、返却及び修理

ア　教育ネットワーク等管理者は、学校情報資産を記録した媒体が含まれる構成機器を廃棄する場合は、当該媒体に記録された学校情報資産を完全に消去する等復元できないようにした上で行わなければならない。賃貸業者に対し、賃貸した構成機器を返却する場合も、同様とする。

イ　教育ネットワーク等管理者は、学校情報資産を記録した媒体が含まれる構成機器の故障について、事業者に委託して修理させる場合は、可能な限り当該媒体に記録された学校情報資産を消去するものとする。

(7)　管理記録

教育ネットワーク等管理者は、教育等のために用いるネットワークについて行った変更及び修理等の作業については、それらの作業記録を作成し、適切に管理しなければならない。

5　教育等のために用いる情報システムの導入、開発、保守等

(1)　教育等のために用いる情報システムの導入

ア　教育ネットワーク等管理者は、既存の教育等のために用いる情報システムを新たに拡張し、又は他の情報システムに接続しようとする場合には、既存の情報システムに影響が生じないよう拡張又は接続する前に十分な試験を行わなければならない。

イ　教育ネットワーク等管理者は、アの試験による結果の記録のうち重要なものを厳重に保管しなければならない。

(2)　ソフトウェアの導入及び変更

ア　教育ネットワーク等管理者は、ソフトウェアを計画的に導入するとともに、導入に当たっては、当該ソフトウェアの適格性及び他の情報システムとの適合性について確認しなければならない。

イ　教育ネットワーク等管理者は、ソフトウェアについて学校情報セキュリティに重大な影響を及ぼすおそれのある不具合が発見された場合には、速やかに当該ソフトウェアの変更を行う等適切に対応しなければならない。

ウ　教育ネットワーク等管理者は、イの場合のほか、ソフトウェアの変更については計画的に行わなければならない。

(3)　教育等のために用いる情報システムの学校情報セキュリティインシデント及び不正行為への対策

教育ネットワーク等管理者は、教育等のために用いる情報システムの開発若しくは保守時の学校情報セキュリティインシデント又は不正行為に対する対策のため、必要な事項を別に定めなければならない。

(4)　教育等のために用いる情報システムに関する外部委託事業者

ア　教育ネットワーク等管理者は、新たに教育等のために用いる情報システムの開発を事業者に委託する場合は、情報の機密性に応じたセキュリティレベルが確保されていることを確認した上で、総務部契約管財課契約係に対し、当該事業者の経営状況等の調査を依頼し、当該開発の契約を適正に履行することが可能であるかどうかを確認しなければならない。

イ　教育ネットワーク等管理者は、外部委託事業者の従業員が委託した業務に従事するときには、当該外部委託事業者の従業員であることを証する身分証明書等を事前に提示させなければならない。

(5)　電子計算機の廃棄、返却及び修理

ア　教育ネットワーク等管理者は、学校情報資産を記録した媒体が含まれる電子計算機等を廃棄する場合は、当該媒体に記録された学校情報資産を完全に消去する等復元できないようにした上で廃棄しなければならない。賃貸業者に対し、賃貸した構成機器を返却する場合も、同様とする。

イ　教育ネットワーク等管理者は、学校情報資産を記録した媒体が含まれる電子計算機の故障について、事業者に委託して修理させる場合は、可能な限り当該媒体に記録された学校情報資産を消去するものとする。

(6)　管理記録

教育ネットワーク等管理者は、教育等のために用いる情報システムについて行った変更及び修理等の作業については、それらの作業記録を作成し、適切に管理しなければならない。

6　コンピュータウイルスの対策

(1)　教育ネットワーク等管理者は、コンピュータウイルスをチェックするパターンファイルを常時、最新のものに保たなければならない。

(2)　教育ネットワーク等管理者は、所管する教育等のために用いる情報システムに対し、コンピュータウイルスの対策のためのソフトウェア等を導入しなければならない。

(3)　教職員等は、データ又はソフトウェアを取り入れる場合及び執務室外にデータ又はソフトウェアを持ち出す場合には、必ずコンピュータウイルスのチェックを行わなければならない。

(4)　教職員等は、コンピュータウイルスに関する情報については、常時、確認しなければならない。

(5)　教職員等は、自己の端末等において差出人の不明なメール又は不自然に添付されたファイルを発見したときは、速やかにそれらを削除しなければならない。

(6)　教職員等は、ファイルが添付されたメールを送信し、又は受信する場合は、コンピュータウイルスのチェックを併せて行わなければならない。

(7)　教職員等は、特に必要な場合を除き、コンピュータウイルスのチェックを中断してはならない。

7　不正なアクセスの対策

(1)　教育ネットワーク等管理者は、情報セキュリティホール（ソフトウェアに関する学校情報セキュリティ上の抜け穴をいう。以下同じ。）の発見に努め、教育ネットワーク等の運用保守を受託する事業者等から修正ソフトウェアの提供があった場合には、業務に支障がないことを確認の上、速やかに当該情報セキュリティホールを除去しなければならない。

(2)　教育ネットワーク等管理者は、情報セキュリティホールが発見された場合において、(1)の修正ソフトウェアの提供がない段階においても、サーバ、端末及び通信回線上で採り得る対策を可能な限り講じなければならない。

(3)　教育ネットワーク等管理者は、重要な教育等のために用いる情報システムの設定に係るファイルの改ざんの有無について定期的に検査しなければならない。

(4)　教育ネットワーク等管理者は、侵害を受ける可能性がある場合には、教育等のために用いる情報システムの停止等必要な措置を講じなければならない。

(5)　教育ネットワーク等管理者は、侵害が法に違反する可能性がある場合、当該侵害の記録の保存並びに警察署及び関係機関との緊密な連携に努めなければならない。

(6)　教育ネットワーク等管理者は、教育等のために用いる情報システムにおいて、標的型攻撃による内部への侵入又は外部への情報漏えいを防止するために必要な人的

対策及び技術的対策を講じるとともに、内部に侵入した攻撃を早期探知し、通信をチェックする等の内部対策を講じなければならない。

(7)　教育ネットワーク等管理者は、実施している不正なアクセス対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられる体制の整備に努めなければならない。

8　学校情報セキュリティに関する情報の収集等

(1)　教育ネットワーク等管理者は、学校情報セキュリティに関する情報を収集し、教育ネットワーク等について、学校情報セキュリティ対策上必要な措置を講じなければならない。

(2)　統括学校情報セキュリティ責任者は、(1)の情報を定期的に取りまとめ、学校情報セキュリティ責任者にその結果を通知しなければならない。

(3)　教育ネットワーク等管理者は、新宿区情報システム緊急時対応計画（平成16年3月18日付け15新企情第783号 ネットワーク管理者決定）（以下「緊急時対応計画」という。）に掲げる緊急に連絡すべき情報を入手した場合は、当該緊急時対応計画に定める連絡先に連絡しなければならない。

第6　運用

1　教育等のために用いる情報システムの監視

(1)　教育ネットワーク等管理者は、学校情報セキュリティを確保するため、常時、教育等のために用いる情報システムの監視を行わなければならない。

(2)　教育ネットワーク等管理者は、(1)の監視により得られた結果を記録した媒体について、盗難、改ざん、消去等を防止するために必要な措置を講じ、安全な場所に保管しなければならない。

2　学校情報セキュリティポリシーの遵守状況等

(1)　教育ネットワーク等管理者は、学校情報セキュリティポリシーの遵守状況及び学校情報資産の管理に関する問題の有無について、常時、確認を行わなければならない。

(2)　教育ネットワーク等管理者は、(1)の確認により、学校情報セキュリティポリシーの遵守状況又は学校情報資産の管理に関する問題が発生していた場合には、速やかに統括学校情報セキュリティ責任者にその旨を報告しなければならない。

(3)　統括学校情報セキュリティ責任者は、(2)の報告があった場合は、速やかに当該

問題に対する適切な措置を講じなければならない。

3　学校情報セキュリティ障害

(1)　学校情報セキュリティ障害の調査

ア　教育ネットワーク等の障害又は侵害（以下これらを「学校情報セキュリティ障害」という。）を確認した教職員等は、その内容を速やかに学校情報セキュリティ責任者に報告しなければならない。

イ　アの報告を受けた学校情報セキュリティ責任者は、その内容を速やかに統括学校情報セキュリティ責任者及び教育ネットワーク等管理者に報告しなければならない。

ウ　統括学校情報セキュリティ責任者は、イの報告があった場合は、当該学校情報セキュリティ障害に関して詳細に調査を行い、その調査結果を新宿区情報化の推進に関する規則第2条に規定する情報化戦略本部（以下「情報化戦略本部」という。）へ報告しなければならない。

(2)　学校情報セキュリティ障害の拡大の防止

ア　教育ネットワーク等管理者は、次に掲げる場合には、教育ネットワーク等及び学校情報資産の保護のために教育等のために用いるネットワークを切断する措置を講じるものとする。

(ア)　教育等のために用いる情報システムの運用に著しい支障が生じる等異常なアクセスが継続しているとき、又は不正なアクセスが判明したとき。

(イ)　コンピュータウイルス等不正なプログラムが教育等のために用いるネットワークを経由して拡大しているとき。

(ウ)　災害等により、教育等のために用いるネットワークを稼動させる電力の供給を受けることが危険又は困難であるとき。

(エ)　コンピュータウイルス等の不正なプログラムに感染したとき、又は感染が疑われるとき。

(オ)　その他教育ネットワーク等及び学校情報資産に係る被害が想定されるとき。

イ　教育ネットワーク等管理者は、次に掲げる場合には、教育ネットワーク等及び学校情報資産の保護のために所管する教育等のために用いる情報システムを停止する措置を講じるものとする。

(ア)　コンピュータウイルス等不正なソフトウェアが学校情報資産に危害を及ぼ

しているとき。

(イ) 災害等により、教育等のために用いる情報システムを稼動させる電力の供給を受けることが危険又は困難であるとき。

(ウ) コンピュータウイルス等の不正なプログラムに感染したとき、又は当該感染が疑われるとき。

(エ) その他教育ネットワーク等及び学校情報資産に係る被害が想定されるとき。

ウ 教職員等は、自己の端末等を教育等のために用いるネットワークから離脱させる場合には、事前に教育ネットワーク等管理者の許可を受けなければならない。ただし、教育ネットワーク等及び学校情報資産への危害を防止するため、直ちに離脱させる必要がある場合には、事後において、教育ネットワーク等管理者にその旨を報告するものとする。

(3) 学校情報セキュリティ障害への対応

教育ネットワーク等管理者は、学校情報セキュリティ障害が発生した場合には、次に掲げる措置を迅速かつ円滑に講じなければならない。

ア 緊急時対応計画により定められた連絡先への連絡

イ 学校情報セキュリティ障害に係る現状及び対処した経過の記録

ウ 学校情報セキュリティ障害に係る証拠保全の実施

エ 学校情報セキュリティ障害の再発を防止するための暫定的な措置

オ エの暫定的な措置を講じた後の復旧作業

カ オの復旧作業後必要と認められる期間内における学校情報セキュリティ障害の再発に関する監視

(4) 学校情報セキュリティ障害の再発防止の措置

ア 教育ネットワーク等管理者は、学校情報セキュリティ障害に関するリスクを分析し、学校情報セキュリティ障害の再発を防止するために必要な措置を検討し、統括学校情報セキュリティ責任者にその旨を報告しなければならない。

イ 教育ネットワーク等管理者は、次に掲げる事項を情報化戦略本部に報告するとともに、教職員等に周知しなければならない。

(ア) アの学校情報セキュリティ障害の概要

(イ) 学校情報セキュリティポリシーが見直された場合における見直し後の学校情報セキュリティポリシー

4　学校情報セキュリティに関する違反への対応

(1)　教育ネットワーク等管理者は、教職員等の学校情報セキュリティポリシーに違反する行為を確認した場合には、当該教職員等が所属する学校の学校情報セキュリティ責任者にその旨を通知しなければならない。

(2)　(1)の通知を受けた学校情報セキュリティ責任者は、当該教職員等に対し適切な措置を講じなければならない。

(3)　教育ネットワーク等管理者は、(2)の措置によっても当該教職員等の学校情報セキュリティポリシーに違反する行動が改善されない場合には、当該教職員等による教育ネットワーク等の使用を停止させることができる。

(4)　教育ネットワーク等管理者は、(3)により使用を停止させた場合には、統括学校情報セキュリティ責任者及び当該教職員等が所属する学校の学校情報セキュリティ責任者にその旨を通知しなければならない。

5　外部委託に関する管理

事業者に学校情報業務を委託する場合には、次に掲げる事項を契約書に明記しなければならない。

(1)　学校情報セキュリティポリシーの主旨の遵守に関すること。

(2)　受託した学校情報業務上知り得た情報の守秘義務に関すること。

(3)　受託した学校情報業務上提供された情報の目的外利用又は第三者への提供の禁止に関すること。

(4)　受託した学校情報業務上提供された情報の適切な管理に関すること。

(5)　受託した学校情報業務上提供された情報の複写等の禁止に関すること。

(6)　受託した学校情報業務の再委託の禁止に関すること。

(7)　受託した学校情報業務上提供された学校の情報の返還義務に関すること。

(8)　区の求めにより受託した学校情報業務に関する報告を定期的に行うこと。

(9)　区の監査に応じること。

(10)　当該事業者の従業員に対する学校情報セキュリティに関する教育の実施に関すること。

(11)　学校情報セキュリティインシデント発生時等における報告に関すること。

(12)　前各号に掲げる事項に違反した場合の措置に関すること。

6　派遣労働者に学校情報業務を行わせる場合

派遣労働者に学校情報業務を行わせる場合には、労働者派遣事業の適正な運営の確

保及び派遣労働者の保護等に関する法律（昭和60年法律第88号）第26条第1項に規定する労働者派遣契約に係る書面に、次に掲げる事項を明記しなければならない。

(1)　当該派遣労働者の学校情報セキュリティポリシーの遵守に関すること。

(2)　学校情報業務上知り得た情報の守秘義務に関すること。

(3)　区の監査に応じること。

(4)　前3号に掲げる事項に違反した場合の措置に関すること。

7　例外措置

(1)　教育ネットワーク等管理者は、学校情報セキュリティ関連規程を遵守することが困難な状況下において、業務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し、又は遵守事項を実施しないことについて合理的な理由がある場合は、統括学校情報セキュリティ責任者の許可を得て、例外措置を採ることができる。

(2)　教育ネットワーク等管理者は、業務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかに統括学校情報セキュリティ責任者に報告しなければならない。

(3)　統括学校情報セキュリティ責任者は、例外措置の申請及び審査結果を適切に保管し、必要に応じて、申請状況や例外措置実施状況を確認しなければならない。

第7　監査、点検、評価及び見直し

1　監査

教育ネットワーク等管理者は、監査の結果を統括学校情報セキュリティ責任者へ報告しなければならない。

2　点検

学校情報セキュリティ責任者は、所管する学校情報資産について学校情報セキュリティポリシーに沿った学校情報セキュリティ対策が行われているかどうか点検を行い、統括学校情報セキュリティ責任者に当該点検の結果を報告しなければならない。

3　評価及び見直し

(1)　統括学校情報セキュリティ責任者は、１の監査及び２の点検の結果並びに学校情報セキュリティに関する状況の変化等を踏まえ、学校情報セキュリティ対策の実効性を定期的に評価しなければならない。

(2)　統括学校情報セキュリティ責任者は、その評価に基づき学校情報セキュリティ対策の必要な見直しを行うものとする。

附則

この基準は、令和８年２月１７日から施行する。