富山市教育ネットワーク利用要領

序

富山市教育ネットワーク利用要領（以下、「利用要領」という。）は、教育ネットワークを利用する全ての者（以下、「利用者」という。）が、教育ネットワークの情報セキュリティを確保するため、教育ネットワークの利用に際し遵守すべき事項を定めるものである。

利用要領は２つの章で構成し、第１章には教育ネットワークの概要を記し、第２章には利用者が遵守すべき事項を記す。

この要領における用語の意味は、富山市情報セキュリティポリシーの例による。

第１章 教育ネットワークの概要

１　教育ネットワークの定義

教育ネットワークとは、学校運営に資するために教育委員会が構築した本市の個別業務ネットワークであり、通信回線とそれを制御する通信機器・コンピュータ群で構成され、教育委員会事務局及び教育センターと市立小中学校等（以下、学校等という）を結んでいる。

教育センターは、このネットワークを介して共通基盤システムや校務支援システムを運用し学校等に提供している。

２　共通基盤システムの定義

共通基盤システムとは、他の情報システムに動作環境を提供するシステムや、全利用者が共通的に業務利用するシステムのことであり、具体的には以下のシステムをいう。

・職員認証システム
・グループウェアシステム（電子メール含む）
・ファイル共有システム
・インターネット閲覧システム
・サーバ仮想基盤

３　教育ネットワークの責任者

教育ネットワークの責任者は、情報セキュリティ責任者とし、教育ネットワークの管理・運用及び情報セキュリティ対策を行う統括的な権限及び責任を有する。

４　教育ネットワークの管理者

情報セキュリティ責任者は、教育ネットワークの管理・運用及び情報セキュリティ対策を教育センター所長に行わせるものとする。ただし、教育センター所長は、必要に応じて情報システム課の助力を要請できることとする。

５　教育ネットワークの利用者

教育ネットワークを利用することができるのは、次に掲げる者とする。

・教育委員会事務局及び教育センター、富山市立小中学校等に所属する教職員
・富山市立小中学校に在籍する児童生徒
・その他、情報セキュリティ責任者が適当と認めた者

６　教育ネットワークの接続範囲

教育ネットワークは、次の部局等を結ぶ。

・教育委員会事務局及び教育センター
・富山市立小中学校等
・その他、統括情報セキュリティ責任者が接続を認めた機関

教育ネットワークは、その役割からインターネットとも接続する。

７　教育ネットワークのセキュリティ

教育ネットワークには、校務系ネットワーク、校務外部接続系ネットワーク、学習系ネットワークの３系統のネットワークが存在する。

これらのネットワークは、それぞれの目的や用途により情報セキュリティに関する要件が異なるため、一律の対策ではセキュリティ強度や使い勝手に大きな支障を生じさせる。

業務効率をできる限り維持しつつ、本市教育ネットワークの情報セキュリティを維持するために、各ネットワークの要件に応じたセキュリティ対策を施すとともに、各ネットワーク間の通信は予め許可された通信のみに制限するホワイトリスト式(※)とすることで最適化を図っている。

各層ネットワークのポリシーは次のとおり。

※ ホワイトリスト式…通信やアクセスを許可するアドレスなどのリストを作成し、それ以外は拒否・禁止する方式。

■レベル１：学習系ネットワーク

授業等の教育活動に利用するネットワーク。教職員及び児童生徒の両方が利用することを前提としているが、それぞれアクセスできる範囲が異なる。

ただし、情報の毀損や漏洩等が発生した場合に、学校運営に深刻な影響を及ぼす情報資産は保存しない。

パソコンやプリンタ等物理的な機器等を接続しているため、エンドポイント対策(※)及びコンピュータウイルス等の流入を防ぐための入口対策(※)を行う。

■レベル２：校務外部接続系ネットワーク

電子メールや学校ホームページ更新等、インターネット接続が必要な校務のために教職員が利用するネットワーク。

仮想化技術を用いることで校務系ネットワークと論理的に分離している。

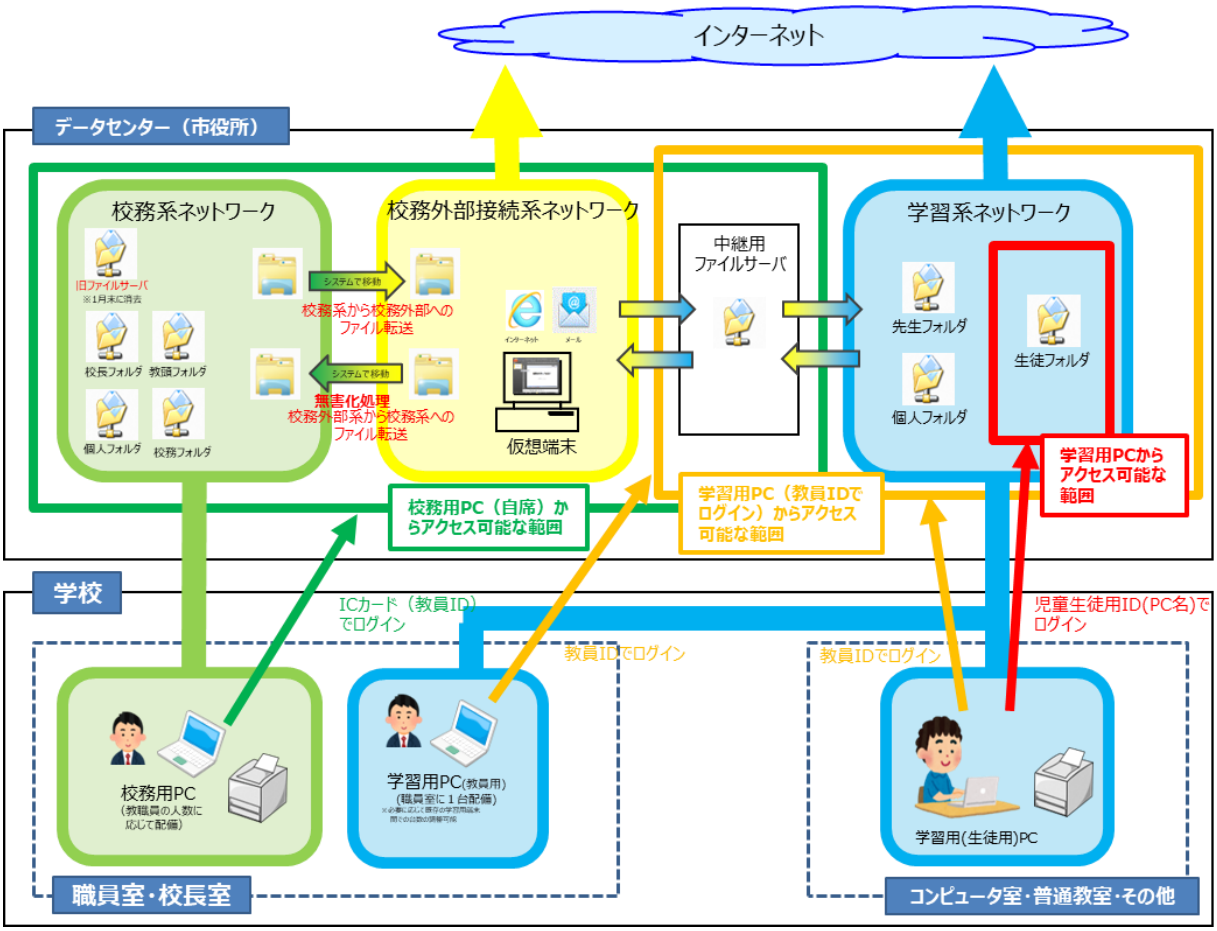
また、インターネットへの接続環境を一か所に集約し、情報セキュリティ上の危険性に対する監視と運用を確実に行う。

■レベル３：校務系ネットワーク

校務用として汎用的に使用するネットワーク。児童生徒の個人情報等、機微な情報を多く扱うことから、出口対策(※)を重点的に施す。あわせて、パソコンやプリンタ等物理的な機器等を接続しているため、エンドポイント対策(※)及びコンピュータウイルス等の流入を防ぐための入口対策(※)を行う。

※エンドポイント対策…教育ネットワークに接続されたサーバ、パソコン、スマートフォンのような末端（エンドポイント）をサイバー攻撃から守るためのセキュリティ対策。
※入口対策…不正アクセス等のサイバー攻撃やマルウェアへの感染を防ぐために、ファイアウォールを構築したり、ウイルス対策ソフトを 導入する等の、内部ネットワークへ外部から侵入されたり、マルウェアが入り込むのを「入口」で防ぐ対策。
※出口対策…内部から外部へ出ていく通信を監視し、重要情報の漏えいを防いだり、マルウェアが外部と通信することを防いだりする「出口」での対策。

ネットワーク構成模式図



第２章 利用者が遵守すべき事項

１　共通

(1)情報端末の取扱い

ア　利用者は、不注意により情報端末が破損、汚損、紛失しないよう、十分に注意すること。また、児童生徒に対しても十分注意して情報端末を取り扱うよう指導すること。万が一、情報端末を破損、汚損、紛失した場合には、速やかに教育センター（教育サポートデスク）に連絡するとともに、「ＩＣＴ機器破損等に係る顛末書」（様式第１１号）を提出すること。

なお、情報端末に液体類をこぼした場合は、情報端末の動作の可否に関わらず、すぐに電源を落としたうえでバッテリーを取り外し、教育センター（教育サポートデスク）へ連絡すること。

イ　利用者は、Windows10 アップグレードや脆弱性対策等、情報端末に実施すべき作業について教育センターから指示があった場合は、速やかに対応しなければならない。

ウ　情報セキュリティ管理者（学校長） は情報端末を管理するための台帳を整備する等して、常に情報端末の所在を把握しておかなければならない。また、教育センター所長が求めた場合、情報セキュリティ管理者は情報端末の所在を報告しなければならない。

(2)ソフトウェアの導入、更新等

業務上必要なソフトウェアの導入、更新又は教育ネットワークの構成機器の設定変更（プリンタドライバの導入等）を行う場合は、「管理者権限使用申請書」（様式第２号）により教育センター所長に申請し、承認を得なければならない。

(3)パソコン、プリンタ及びサーバ等の接続、移動、更新及び廃止

パソコン、プリンタ及びサーバ等を、教育ネットワークに接続、移動、更新及び廃止する場合は、「教育ネットワーク接続申請書」（様式第３号）により教育センター所長に申請し、承認を得なければならない。

(4)パソコンの機器増設又は改造の禁止

貸与されたパソコンに対するメモリやハードディスク等の機器の増設又は改造は認めない。

(5)ネットワーク配線及び通信機器の変更禁止

無断でネットワーク配線を動かしてはならない。

なお、情報セキュリティ管理者（学校長）は、ネットワーク配線及び通信機器への接続を変更、廃止及び追加する場合は、事前に教育センター（教育サポートデスク）と協議すること。

(6)通信機器の電源

利用者は、教育センターが設置したルータやハブ等の電源を許可なく落としてはならない。また、児童生徒に対しては、不要に通信機器を触らないよう指導すること。

(7)校務データの取り扱い

校務遂行のために作成した文書や資料等のデータは、原則として学校用フォルダに保存すること。

2　校務系情報端末の使用

(1)職員認証

利用者は、校務系ネットワークに接続する情報端末（以下、「校務系端末」という。）を利用する場合、本人確認のために、教育センター発行の IC カード（以下、「IC カード」という。）とパスワードの二要素認証により、職員認証システムの認証を受けなければならない。

(2)校務系情報端末の取扱い

ア　利用者は、職員室等、定められた場所でのみ校務系端末を使用すること。

イ　校務系ネットワークの不正利用防止のため、下記のどちらかを行った場合は校務系端末をロックする。

①IC カードを IC カードリーダから取り外したとき。

②一定時間（10 分）操作しないとき。

ウ　ロックを解除する場合は、当該校務系端末を使用していた利用者が自身の IC カードでログオンし直す。

エ　利用者は、帰宅時等、校務系端末を長時間使用しないときは、校務系端末の電源を切り、IC カードを IC カードリーダから取り外すこと。

オ　利用者は、校務系端末使用時、使用権限のない者から校務系端末の画面を覗き見されないよう周囲に注意を払うこと。

3　IC カード等の取扱い

(1)IC カードの管理

利用者は、業務上必要のないときは、教育ネットワークの不正利用を防止するため、IC カードをカードリーダから取り外し、適切に管理しなければならない。

なお、紛失又は盗難により IC カードをなくした場合は、不正使用防止のため直ちに教育センター（教育サポートデスク）へ連絡しなければならない。

(2)代用コードの発行

IC カードを不携帯状態の利用者が、業務上校務系端末の利用が必要な場合、利用者は教育センターへ IC カードの代用コードの発行を依頼することができる。

なお、教育センター（教育サポートデスク）は本人確認の上、代用コードを発行する。

(3)会計年度任用職員等の IC カードの利用

ア　申請

情報セキュリティ管理者は、会計年度任用職員等に校務系端末を利用させる場合、「IC カード貸与及びシステム等利用申請書」（様式第４号）を教育センター所長に申請し、承認を得なければならない。

イ　情報セキュリティ研修実施

情報セキュリティ管理者は、校務系端末を利用させる会計年度任用職員等に対し、情報セキュリティ研修を実施しなければならない。

会計年度任用職員等は情報セキュリティ管理者に「誓約書」（様式第５号）を提出し、情報セキュリティ管理者はこれを保管するものとする。

また、情報セキュリティ管理者は「情報セキュリティ研修実施報告書」（様式第６号）を教育センター所長へ提出しなければならない。

(4)IC カードの返却・Google アカウントの廃止

情報セキュリティ管理者は、人事異動等により IC カード、Google アカウントが不要となった場合は、IC カードと「IC カード返却・Google アカウント廃止届」（様式第７号）を速やかに教育センターへ提出しなければならない。

(5)再交付

情報セキュリティ管理者は、紛失、汚損により IC カードが使用不能になった場合は、「IC カード再交付申請書」（様式第８号）を教育センター所長に申請し、再交付を受けなければならない。

４ 学習系情報端末の使用

(1)利用者認証

学習系情報端末（以下、「学習系端末」という。）を利用する利用者は、本人確認のために、ID とパスワードにより、利用者認証を受けなければならない。

ただし、児童生徒が WindowsOS の学習系端末を利用する場合に限り、端末に紐づく共有アカウントによるログインを認める。

(2) 校外への持ち出し

児童生徒が家庭学習等のため ChromeOS の学習系端末を校外に持ち出す場合、情報セキュリティ管理者は該当の端末を管理する者（以下、「端末管理者」という。）を指名し、その者に端末の所在を把握させなければならない。また、情報セキュリティ管理者が求めた場合、端末管理者は端末の所在を報告しなければならない。

なお、WindowsOS の学習系端末の校外への持ち出しは原則禁止とする。

(3)情報端末の借用

情報セキュリティ管理者は、院内学級の授業等を行うために、一時的に学習系端末を増設する必要がある場合、「パソコン借用申請書」（様式第１号）により教育センター所長に申請し、承認を得たうえで貸出専用パソコンを借用すること。

また、借用期間中は、教育センターの指示に従いウイルス対策パターンの更新作業等を行うこと。

５　電磁的記録媒体の利用

電磁的記録媒体（以下、「記録媒体」という。）の取扱いについては、別に定める「富山市情報セキュリティ共通実施手順」による。ただし、教育ネットワークで電磁的記録媒体を利用する場合は、以下の取扱い制限も実施しなければならない。

(1)校務系ネットワークにおいて、記録媒体をデータ書き込みのために接続することは、原則禁止とする。ただし、業務上必要な場合は次の各号を満たす場合に行うことができる。

ア　当該記録媒体がUSBメモリ又はUSB外付けハードディスク等の場合は、「記録媒体登録申請書」（様式第９号）を教育センター所長へ申請し、承認を得ていること。

イ　当該記録媒体がUSBメモリ又はUSB外付けハードディスクの場合は、ハードウェア暗号化機能を有していること。ただし、USB外付けハードディスクに限り、教育センター所長が適当と認める場合には当該機能のないものも認める。

ウ　書き出すデータについて、情報セキュリティ管理者の許可を得ていること。なお、データの書き出しは情報資産の複製であることに留意すること。

(2)情報セキュリティ管理者は、(1)アにて登録した記録媒体を廃棄する場合は、「記録媒体廃止届」（様式第１０号）により教育センター所長へ申請し、承認を得なければならない。

なお、データ消去については、消去ソフトウェアや物理的破壊等により記録内容が復元不可能となるよう処置しなければならない。

６　個人の保存データの開示

(1)メールの開示

教育センターが付与した個人メールアカウントに届いたメールについて、以下の全ての事由を満たす場合は、情報セキュリティ管理者は、該当するメールを取得することができる。

ア　業務に必要なメールであること。

イ　メールを受信した本人の退職等により、所属内で他の者が取得することができないメールであること。

ウ　情報セキュリティ管理者が、メールを受信した本人の同意書又はメール開示理由書を教育センター所長に提出し、承認を得ていること。

(2)デスクトップ、マイドキュメント等を含む個人用ドライブの開示

業務に必要な文書等を個人用ドライブに保存した利用者が退職等した場合、教育センター所長は、情報セキュリティ管理者からの申請に基づき、情報セキュリティ管理者に当該職員の個人用ドライブ内のファイルを取得させることができる。

７　パスワードの初期化

利用者は、教育センターが管理する共通基盤システムにログインするためのパスワードを失念した場合、教育センターにパスワードの初期化を依頼することができる。

なお、教育センター（教育サポートデスク）は本人確認の上、パスワードの初期化を行う。

また、利用者は、教育センター（教育サポートデスク）からのパスワード初期化連絡後、初期化されたパスワードを即時に変更しなければならない。

附 則

この要領は、令和２年４月１日から施行する。

附 則

この要領は、令和２年１２月８日から施行する。

附 則

この要領は、令和３年４月１日から施行する。

附 則

この要領は、令和４年４月１日から施行する。