木更津市教育情報セキュリティ対策基準要綱を次のように定める。

令和６年３月２２日

木更津市教育委員会教育長　　廣　部　　昌　弘

木更津市教育委員会告示第２号

木更津市教育情報セキュリティ対策基準要綱

目次

第１章　総則

（趣旨）

第１条　この要綱は、木更津市立小学校及び中学校管理規則（昭和３９年木更津市教育委員会規則第１号。以下「規則」という。）に基づき、学校（木更津市立小学校及び中学校）を対象とした情報セキュリティ対策を実施するために、教育情報システムを整備及び運用並びに管理する者が遵守すべき事項又はそのシステムを利用する者が遵守すべき基準を定める。

（定義及び適用範囲）

第２条　この要綱において使用する用語の定義及び適用範囲は、別表１のとおりとする。

第２章　推進体制

（推進体制）

第３条　学校における情報セキュリティ対策を統一的な視点で推進する体制については、別表２のとおりとする。

第３章　情報資産の分類及び管理

（情報資産の分類）

第４条　学校における情報資産は、機密性、完全性及び可用性により、別表３のとおり分類し、その分類に応じた取扱いを行う。

（管理責任）

第５条　校長は、その所管する情報資産について管理責任を有する。

２　校長は、情報資産が複製され、又は伝送された場合には、複製等をされた情報資産についても前条の分類に基づき管理する。

（情報資産の分類の表示）

第６条　教職員等は、情報資産について、必要に応じファイル（ファイル名、ヘッダー、フッター等）、格納する電磁的記録媒体のラベル、文書の隅等に、情報資産の分類を表示し、取扱制限についても明示する等適正な管理を行う。

（情報の作成）

第７条　教職員等は、業務上必要のない情報を作成しない。

２　教職員等は、情報の作成時に第４条の分類に基づき、情報を作成する。

３　教職員等は、作成途上の情報についても、紛失、流出等を防止する。また、情報の作成途上で不要になった場合は、当該情報を消去する。

（情報資産の入手）

第８条　情報資産を入手した教職員等は、第４条の分類に基づき、情報を取り扱う。

２　情報資産を入手した教職員等は、入手した情報資産の分類が不明な場合は、校長に判断を仰ぐ。

（情報資産の利用）

第９条　情報資産を利用する教職員等は、業務以外の目的に情報資産を利用しない。

２　情報資産を利用する教職員等は、第４条の分類に応じ、適切に取り扱う。

３　情報資産を利用する教職員等は、電磁的記録媒体に第４条の分類が異なる情報が複数記録されている場合は、最高度の分類に従って、当該電磁的記録媒体を取り扱う。

（情報資産の保管）

第１０条　校長は、第４条の分類に従って、情報資産を適正に保管する。

２　校長は、情報資産を記録した電磁的記録媒体を長期保管する場合は、必要に応じて書込禁止

の措置を講ずる。

３　校長は、機密性２Ｂ以上、完全性２又は可用性２の情報を記録した電磁的記録媒体を保管する場合は、必要に応じて耐火、耐震、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管する。

（情報の送信）

第１１条　電子メール等により機密性２Ｂ以上の情報を送信する教職員等は、必要に応じ、パスワード等による暗号化を行う。

（情報資産の運搬）

第１２条　車両等により機密性２Ｂ以上の情報資産を運搬する教職員等は、必要に応じ鍵付きのケース等に格納し、パスワード等による暗号化を行う等、情報資産の不正利用を防止するための措置を講ずる。

２　機密性２Ｂ以上の情報資産を運搬する教職員等は、校長に許可を得る。

（情報資産の提供又は公表）

第１３条　機密性２Ｂ以上の情報資産を外部に提供する教職員等は、必要に応じパスワード等による暗号化を行う。

２　機密性２Ｂ以上の情報資産を外部に提供する教職員等は、校長に許可を得る。

３　校長は、保護者等に公開する情報資産について、完全性の確保に努める。

（情報資産の廃棄等）

第１４条　機密性２Ｂ以上の情報が記録された用紙の廃棄を行う教職員等は、情報を復元できないように処置する。

２　機密性２Ａ以上の情報が記録された機器の廃棄を行う教職員等は、学校教育課長にその廃棄を依頼する。

３　前項の場合、依頼された学校教育課長は、情報を復元できないように処置する。

第４章　物理的セキュリティ

（サーバ等の管理）

第１５条　学校教育課長は、それぞれ所管するサーバ等の管理について、市長部局に委ねた部分を除き、次の各号に掲げる措置を講ずる。

⑴　サーバ等の機器の取付けを行う場合は、地震、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置する。

⑵　校務系サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が

適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付ける。

⑶　落雷等による過電流に対して、サーバ等の機器を保護するための措置を講ずる。

⑷　通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用するなど、必要な措置を講ずる。

⑸　主要な箇所の通信ケーブル及び電源ケーブルについて、損傷等があった場合、速やかに対応する。

⑹　ネットワーク接続口（ハブのポート等）を、他者が容易に接続することができない場所に設置するなど、適切に管理する。

⑺　可用性２のサーバ等の機器の定期保守を実施する。

⑻　学校教育課長は、機密性２Ｂ以上のデータを含む電磁的記録媒体を内蔵する機器を事業者に修理させる場合は、内容を消去した状態で行わせる。内容を消去できないときは、学校教育課長は、事業者に故障を修理させるに当たり、修理を委託する事業者との間で、秘密保持契約を締結する。

⑼　施設外又は学校外にサーバ等の機器を設置する場合、教育長の承認を得る。この場合においては、当該機器に係る情報セキュリティ対策状況について必要に応じ確認する。

⑽　機器を廃棄、リース返却等を行う場合は、機器内部の記憶装置から全ての情報を消去した上、復元不可能な状態にする措置を講ずる。

（管理区域の管理）

第１６条　管理区域の管理については木更津市情報セキュリティ対策基準に準ずる。

（通信回線及び通信回線装置の管理）

第１７条　学校教育課長は、校内の通信回線及び通信回線装置の管理について、市長部局に委ねた部分を除き、次の各号に掲げる措置を講ずる。

⑴　施設内の通信回線及び通信回線装置を適正に管理する。また、通信回線及び通信回線装置に関連する文書を適正に保管する。

⑵　外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らす。

⑶　機密性２Ｂ以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適正な回線を選択する。また、必要に応じ、送受信される情報の暗号化を行う。

⑷　ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が

生じないように十分なセキュリティ対策を実施する。

⑸　可用性２の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択する。また、必要に応じ、回線を冗長構成にする等の措置を講ずる。

（教職員等の利用する端末や電磁的記録媒体等の管理）

第１８条　学校教育課長及び校長は、それぞれ所管する端末及び電磁的記録媒体の管理について、次の各号に掲げる措置を講ずる。

⑴　学校教育課長は、盗難及び不正アクセス防止のため、必要に応じて、ログイン時のＩＤパスワードによる認証、加えて多要素認証の実施等、使用する目的に応じた適切な物理的措置を講ずる。

⑵　校長は、電磁的記録媒体について、情報が保存される必要がなくなった時点で速やかに記録した情報を消去する。

⑶　学校教育課長は、教育情報システムにアクセスする端末へのログインに際し、パスワードの入力を必要とするように設定する。ただし、災害等の緊急時など、複数の認証情報の入力を行うことが適当でないときを除く。

⑷　学校教育課長は、取り扱う情報の重要度に応じてパスワード以外に生体認証や物理認証等の多要素認証を設定する。特にアクセス制御による対策を講じたシステム構成の場合、校務系情報等の重要な情報資産へのアクセスについては、多要素認証を必須とする。

⑸　学校教育課長は、端末におけるマルウェア感染の脅威に対し、ウイルス対策ソフトの導入等の対策を講ずる。

⑹　校長は、教室等で利用する端末は、盗難防止のため、保管庫による管理等の物理的措置を講ずる。

⑺　校長は、電磁的記録媒体は、情報が保存される必要がなくなった時点で速やかに記録した情報を消去する。

⑻　学校教育課長は、教育情報システムへのアクセスにおけるログインパスワードの入力等による認証を設定する。

第５章　人的セキュリティ

（教育情報セキュリティポリシーの遵守）

第１９条　教職員等は、教育情報セキュリティポリシーを遵守する。

２　教職員等は、情報セキュリティ対策について不明な点、遵守する　ことが困難な点等がある

場合は、速やかに校長に相談し、その指示を仰ぐ。

（業務以外の目的での使用の禁止）

第２０条　教職員等は、業務以外の目的で情報資産の外部への持ち出し、教育情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行わない。

（端末等の持ち出し及び外部における情報処理作業の制限）

第２１条　教職員等は、学校の校務用端末及び電磁的記録媒体記録媒体を外部へ持ち出す場合には、校長の許可を得る。

２　教職員等は、外部で情報処理業務を行う場合には、校長の許可を得る。

（支給以外のパソコン等及び電磁的記録媒体の業務利用）

第２２条　教職員等は、支給以外のパソコン等を原則業務に使用しない。ただし、業務上必要な場合は、校長の許可を得て使用することができる。

２　教職員等は、支給以外の電磁的記録媒体を原則校務用端末で使用しない。ただし、業務上必要な場合は、校長の許可を得て利用することができる。

３　教職員等は、支給以外の電磁的記録媒体を原則学習者用端末で使用しない。ただし、業務上必要な場合は、校長の許可を得て利用することができる。

（校務用端末及び学習者用端末におけるセキュリティ設定変更の禁止）

第２３条　教職員等は、校務用端末及び学習者用端末のソフトウェアに関するセキュリティ機能の設定を学校教育課長の許可なく変更しない。

（机上の端末等の管理）

第２４条　教職員等は、校務用端末及び学習者用端末について、第三者に使用されること又は校長の許可なく情報を閲覧されることがないように、離席時の画面ロックなど、適切な措置を講ずる。

２　教職員等は、電磁的記録媒体、情報が印刷された文書等について、第三者に使用されること又は校長の許可なく情報を閲覧されることがないように、それらを容易に閲覧されない場所に保管するなど、適切な措置を講ずる。

（異動及び退職時の遵守事項）

第２５条　教職員等は、異動及び退職により学校を離れる場合には、利用していた情報資産を返却する。その後も業務上知り得た情報を漏らさない。

（非常勤及び臨時の教職員への対応）

第２６条　校長は、非常勤及び臨時の教職員等に対し、採用時に教育情報セキュリティポリシーについて理解させ、また遵守させる。

（教育情報セキュリティポリシーの周知）

第２７条　校長は、教職員等が常に教育情報セキュリティポリシーを閲覧できるように掲示する。

（教育及び訓練）

第２８条　教育長は、教職員等を対象とした情報セキュリティに関する周知、研修等を定期的に実施する。

２　教育長は、必要に応じ新規採用の教職員等を対象とする研修を実施する。

３　教職員等は、定められた研修又は訓練に参加する。

（学校内での情報セキュリティインシデントの報告）

第２９条　教職員等は、学校内で情報セキュリティに係る事故、欠陥等（以下「情報セキュリティインシデント」という。）を認知した場合、速やかに副校長・教頭に報告する。

２　前項の報告を受けた副校長・教頭は、校長及び学校教育課長に報告する。

３　学校教育課長は、当該情報セキュリティインシデントについて、必要に応じて教育長及び教育委員会教育部長に報告する。

（市民等の外部からの情報セキュリティインシデントの報告）

第３０条　教職員等は、管理対象のネットワーク、教育情報システム等の情報資産に関する情報セキュリティインシデントについて、市民等の外部から報告を受けた場合は、副校長・教頭に報告する。

２　前項の報告を受けた副校長・教頭は、校長及び学校教育課長に報告する。

３　学校教育課長は、当該情報セキュリティインシデントについて、必要に応じて教育長及び教育委員会教育部長に報告する。

（情報セキュリティインシデント原因の究明、記録、再発防止等）

第３１条　教育長は、情報セキュリティインシデントについて、教育委員会教育部長、学校教育課長及び校長と連携し、これらの情報セキュリティインシデントの原因を追究し、記録を保存する。また、原因究明の結果から、その再発防止策を検討し、関係者に対して必要な措置を指示する。

２　教育長は、発生した情報セキュリティインシデントの重大性を判断し、必要に応じて市長部局のＣＳＩＲＴ（情報セキュリティに関する統一的な窓口）と連携し、その対応に当たる。

（ＩＤ及びパスワード等の管理）

第３２条　教職員等は、自己の管理するＩＤに関し、次の各号に掲げる事項を遵守する。

⑴　やむを得ない場合を除き、自己が利用しているＩＤを他人に利用させない。

⑵　共用ＩＤを利用する場合は、共用ＩＤの利用者以外に利用させない。

２　教職員等は、自己の管理するパスワードに関し、次の各号に掲げる事項を遵守する。

⑴　パスワードは、他者に知られないように管理する。

⑵　パスワードが流出したおそれがある場合には、速やかに学校教育課に連絡し、パスワードの変更を依頼する。

第６章　技術的セキュリティ

（コンピュータ及びネットワークの管理）

第３３条　学校教育課長は、教育情報システム及びネットワークの管理に当たり、市長部局に委ねた部分を除き、別表４に掲げる措置を講ずる。

（アクセス制御）

第３４条　学校教育課長は、権限のない職員がアクセスできないように、所管するネットワーク又は情報システムごとに、システム上の制限をする。

（利用者ＩＤの取扱い）

第３５条　学校教育課長は、利用者の登録、変更、抹消等の情報管理、教職員等の異動、出向、退職者に伴う利用者ＩＤの取扱い等の方法を定める。

２　教職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、学校教育課長に通知する。

３　学校教育課長は、利用されていないＩＤが放置されないように点検する。

（特権を付与されたＩＤの管理等）

第３６条　学校教育課長は、管理者権限等の特権を付与されたＩＤを利用する者を必要最小限にし、当該ＩＤのパスワードの漏えい等が発生しないよう、当該ＩＤ及びパスワードを厳重に管理する。

２　学校教育課長の特権を代行する者は、学校教育課長が指名した者とする。

３　学校教育課長は、特権を付与されたＩＤ及びパスワードの変更について、委託事業者に行わせない。

４　学校教育課長は、特権を付与されたＩＤのパスワードを初期設定以外のものに変更する。

（外部からのアクセス等の制限）

第３７条　教職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、学校教育課長の許可を得る。

２　学校教育課長は、システム上利用者の本人確認を行う機能を確保し、通信途上の盗聴を防御するために暗号化等の措置を講じる。

３　学校教育課長は、外部からのアクセスに利用する端末を教職員等に貸与する場合は、セキュリティ確保のために必要な措置を講じる。

（自動識別の設定）

第３８条　学校教育課長は、校務系ネットワークで使用される機器について、機器固有情報によって校務用端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定する。

（認証情報の管理）

第３９条　学校教育課長は、教職員等の認証情報を厳重に管理する。

（情報システム等の調達）

第４０条　学校教育課長は、情報システム等の調達に当たり、市長部局に委ねた部分を除き、次の各号に掲げる措置を講ずる。

⑴　情報システムの調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記する。

⑵　機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認する。

（不正プログラム対策）

第４１条　学校教育課長は、不正プログラム対策として、市長部局に委ねた部分を除き、次の各号に掲げる措置を講ずる。

⑴　外部ネットワークから受信したファイルについては、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止する。

⑵　外部ネットワークに送信するファイルについては、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止する。

⑶　コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ教職員等に対して注

意喚起をする。

⑷　所管するサーバ及び端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させる。

⑸　不正プログラム対策ソフトウェアのパターンファイルを常に最新の状態に保つ。

⑹　不正プログラム対策ソフトウェアを、原則として、常に最新の状態に保つ。

⑺　インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合は、コンピュータウイルス等の感染を防止するために、校長が管理している電磁的記録媒体以外を教職員等に利用させてはならない。また、不正プログラムの感染、侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施する。

２　教職員等は、不正プログラム対策に関し、次の各号に掲げる事項を遵守する。

⑴　校務用端末及び学習者用端末において、不正プログラム対策ソフトウェアの設定を変更しない。

⑵　外部からデータ又はソフトウェアを取り入れる場合には、不正プログラム対策ソフトウェアによるチェックを行う。

⑶　差出人が不明のもの又は不自然に添付されたファイルを受信した場合は、速やかに削除する。

⑷　インターネットメール又はインターネット経由で入手したファイルを校務系ネットワークに取込む場合は、原則無害化する。ただし、無害化システムが該当ファイルの無害化に対応していない、又は無害化することで必要なファイルが破損する場合には、学校教育課に相談する。

⑸　コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、該当の端末においてＬＡＮケーブルの即時取り外し、通信を行わない設定への変更などを行い、副校長・教頭に報告する。

３　学校教育課長は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家等の支援を受けられるようにしておく。

（不正アクセス対策）

第４２条　学校教育課長は、不正アクセス対策として、次の各号に掲げる措置を講ずる。

⑴　使用されていないポート及びＳＳＩＤ（無線ＬＡＮネットワーク名）を閉鎖する。

⑵　不要なサービスについて、機能を削除し、又は停止する。

⑶　サーバ等に攻撃を受けることが明確になった場合又は攻撃を受けるリスクがある場合は、システムの停止を含む必要な措置を講じるとともに、関係機関と連絡を密にして情報の収集に努める。

⑷　サーバ等に攻撃を受け、当該攻撃が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）違反等の犯罪の可能性がある場合は、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努める。

⑸　教職員等による不正アクセスを発見した場合は、校長に通知し、適切な処置を求める。

（セキュリティ情報の収集）

第４３条　学校教育課長は、セキュリティ情報の収集について、市長部局に委ねた部分を除き、次の各号に掲げる措置を講ずる。

⑴　セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有するとともに、セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施する。

⑵　不正プログラム等に関するセキュリティ情報を収集し、必要に応じ、対応方法を教職員等に周知する。

⑶　情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有する。また、情報セキュリティに関する社会環境、技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講ずる。

第７章　運用

（情報システムの監視）

第４４条　学校教育課長は、セキュリティに関する事案を検知するため、市長部局に委ねた部分を除き、情報システムを常時監視する。

２　学校教育課長は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講ずる。

（遵守状況の確認及び対処）

第４５条　学校教育課長及び校長は、必要に応じて教育情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに教育長及び教育委員会教育部長に報告する。

２　教育長及び教育委員会教育部長は、発生した問題について、適切かつ速やかに対処する。

３　学校教育課長は、ネットワーク、サーバ等のシステム設定等における教育情報セキュリティポリシーの遵守状況について、必要に応じて確認を行い、問題が発生していた場合には、適切かつ速やかに対処する。

（校務用端末、学習者用端末及び電磁的記録媒体の利用状況調査）

第４６条　教育長及び教育長が指名した者は、不正アクセス、不正プログラム等の調査のために、教職員等が使用している校務用端末、学習者用端末及び電磁的記録媒体のログ並びに電子メールの送受信記録の利用状況を調査することができる。

（教職員等の報告義務）

第４７条　教職員等は、教育情報セキュリティポリシーに対する違反行為を発見した場合、直ちに副校長・教頭に報告し、報告を受けた副校長・教頭は、校長及び学校教育課長に報告する。学校教育課長は当該違反行為の内容を精査し、必要に応じて教育長及び教育委員会教育部長に報告する。

２　教育長は、教育情報セキュリティポリシーに対する違反行為について、教育委員会教育部長、学校教育課長及び校長と連携し、これらの原因を追及し、記録を保存する。また、原因究明の結果から、その再発防止策を検討し、関係者に対して必要な措置を指示する。

３　教育長は、教育情報セキュリティポリシーに対する違反行為について、市長部局のネットワークへの影響を判断し、必要に応じて市長部局のＣＳＩＲＴと連携し、その対応に当たる。

（緊急時対応計画の策定）

第４８条　緊急時対応計画については、木更津市情報セキュリティ対策基準に基づき策定された木更津市緊急時対応計画（ＣＳＩＲＴ）実施手順書を準用する。

（業務継続計画との整合性確保）

第４９条　学校教育課長は、自然災害、大規模又は広範囲にわたる疾病等に備えて、業務継続計画と教育情報セキュリティポリシーの整合性を確保する。

（法令遵守）

第５０条　教職員等は、職務の遂行において使用する情報資産を保護するために、関係する法令を遵守し、これに従う。

（教育情報セキュリティポリシー違反時の対応等）

第５１条　校長は、教職員等の情報セキュリティポリシーに違反する行動を確認した場合は、当該教職員等の教育情報セキュリティポリシーに違反する行動を是正するよう指導する。その指

導によっても改善されない場合は、学校教育課長に報告する。

２　報告を受けた学校教育課長は教育長及び教育委員会教育部長に報告する。

３　教育長は、前号の規定により学校教育課長から報告があったときは、当該教職員等の教育ネットワーク又は教育情報システムを使用する権利を停止し、又は剥奪する。この場合において、教育長は、当該職員等の当該権利を停止し、又は剥奪した旨を当該教職員等が所属する学校の校長に通知する。

（適用除外）

第５２条　校長は、木更津市教育情報セキュリティポリシーに基づく対応が困難な事務等が発生する場合は、学校教育課長に適用除外を申請する。

２　申請を受けた学校教育課長は、経営改革課と協議の上、教育長の承認を得る。

第８章　業務委託及び外部サービスの利用

（委託事業者の選定基準）

第５３条　学校教育課長は、委託事業者の選定に当たり、市長部局に委ねた部分を除き、委託内容に応じた情報セキュリティ対策が確保されることを確認する。

２　学校教育課長は、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を事業者選定の際の参考にする。

（契約項目）

第５４条　情報システムの運用、保守等を業務委託する場合には、委託事業者との間で必要に応じて次の各号に掲げる情報セキュリティ要件を明記した契約を締結する。

⑴　教育情報セキュリティポリシーの遵守

⑵　委託事業者の責任者、委託内容、作業者の所属及び作業場所の特定

⑶　提供されるサービスレベルの保証

⑷　委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法

⑸　委託事業者の従業員に対する教育の実施

⑹　提供された情報の目的外利用及び委託事業受託者以外の者への提供の禁止

⑺　業務上知り得た情報の守秘義務

⑻　再委託に関する制限事項の遵守

⑼　委託業務終了時の情報資産の返還、廃棄等

⑽　委託業務の定期報告及び緊急時報告義務

⑾　市による監査、検査

⑿　市による情報セキュリティインシデント発生時の公表

⒀　教育情報セキュリティポリシーが遵守されなかった場合の規定（損害賠償等）

（確認、措置等）

第５５条　学校教育課長は、委託事業者において必要なセキュリティ対策が確保されていることを必要に応じて確認し、前条の契約に基づき措置を実施する。また、その内容を教育長に報告する。

（外部サービスの利用）

第５６条　学校教育課長は、木更津市教育外部サービス利用手順書を整備する。

２　学校教育課長は、木更津市教育外部サービス利用手順書に従って、外部サービス（クラウドサービス、Ｗｅｂ会議サービス、ＳＮＳ等のインターネットを介して利用するサービスのことをいう。）を利用する。

第９章　学習者用端末におけるセキュリティ

（学習者用端末のセキュリティ対策）

第５７条　学校教育課長は、学習者用端末のセキュリティ対策について、別表５に掲げる措置を講ずる。

（児童生徒におけるＩＤ及びパスワード等の管理）

第５８条　学校教育課長は、児童生徒におけるＩＤ及びパスワード等の管理について、別表６に掲げる措置を講ずる。

第１０章　評価及び見直し

（監査）

第５９条　教育長は、必要に応じて、学校教育課の職員のうちから情報セキュリティ監査員を指名し、教育ネットワーク及び教育情報システム等の情報資産における情報セキュリティ対策状況について、これに監査を行わせる。

２　情報セキュリティ監査員は、可能な限り、監査及び情報セキュリティに関する知識を有する者とし、必要に応じて経営改革課に協力を要請する。

３　情報セキュリティ監査員は、監査を行うに当たって、監査実施計画を立案し、教育長の承認を得る。

４　被監査部門は、監査の実施に協力する。

５　学校教育課長は、事業者に業務を委託している場合は、委託事業者（再委託事業者を含む。）に対して、教育情報セキュリティポリシーの遵守について、必要に応じて監査を行う。

６　学校教育課長は、監査を実施したときは、監査結果を取りまとめ、教育長に報告する。

７　学校教育課長は、監査報告書等を適正に保管する。

８　教育長は、監査結果を踏まえ、課題及び問題点を所管する校長に対し、当該事項への対処を指示する。また、指摘事項を所管していない校長に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させる。

（自己点検）

第６０条　校長は、所管する学校における本基準及び手順書に沿った情報セキュリティ対策状況について、学校教育課長からの指示に基づき、自己点検を行い、その結果を学校教育課長に報告する。

２　学校教育課長は、校長から報告された自己点検結果と自己点検結果に基づく改善策を取りまとめ、教育委員会教育部長及び教育長に報告する。

３　校長及び教職員等は、自己点検結果に基づき情報セキュリティ対策について改善に努める。

（教育情報セキュリティポリシーの見直し）

第６１条　教育長は、教育情報セキュリティポリシーについて、情報セキュリティ監査及び自己点検並びに情報セキュリティに関する状況の変化等を踏まえ、必要があると認めた場合は、その見直しを図る。

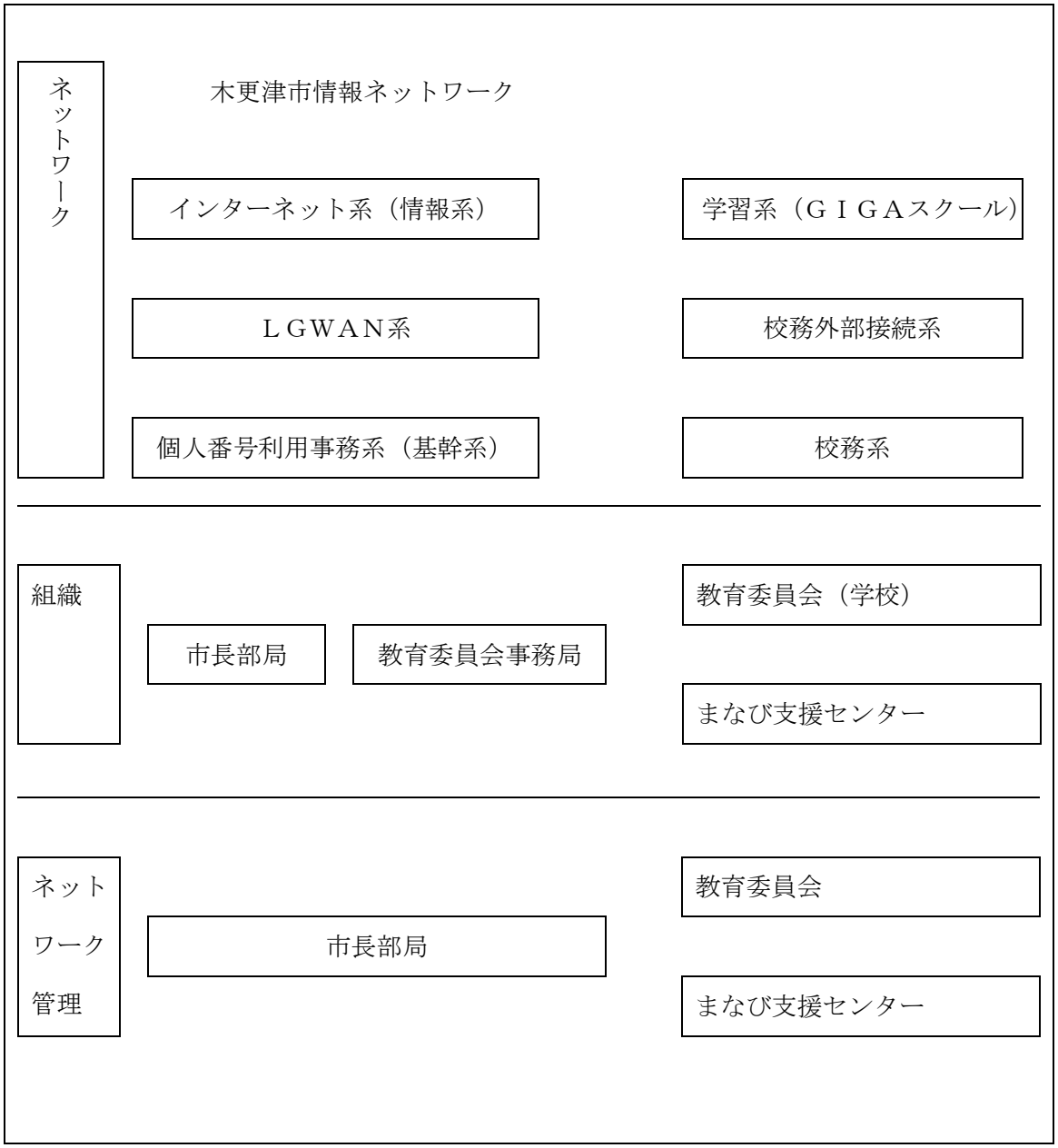
別表１（第２条）

定義

用語	定義
ネットワーク	端末、サーバ、セキュリティ機器等を相互に接続するための通信網
教育ネットワーク	学習系ネットワーク（ＧＩＧＡスクール）
情報システム	ネットワーク、端末、サーバ及びソフトウェアで構成され、情報処理を行う仕組み
情報資産	ネットワーク、情報システム及びそれらで取り扱う情報（用紙に出力したものを含む。）
学習系情報	児童生徒のワークシート、作品など、学校が保有する情報のうち、学校における教育活動において活用することを想定している情報であって、教員及び児童生徒がアクセスすることが想定されている情報
学習者用端末	学習系情報にアクセス可能な端末
学習系サーバ	学習系情報を取り扱うサーバ
学習系システム	学習系ネットワーク上に構成される情報システム
校務外部接続系情報	校務系情報のうち、学校ホームページに掲載する情報等、インターネット上に公開又は伝送することを想定している情報
校務外部接続用端末	校務外部接続系情報にアクセス可能な端末
校務外部接続系サーバ	校務外部接続系情報を取り扱うサーバ
校務外部接続系システム	校務外部接続系ネットワーク、ホームページ運用サーバ（ＣＭＳ）等から構成される校務外部接続系情報を取り扱うシステム
校務系情報	児童生徒の成績、出欠席及びその理由、健康

	診断結果、指導要録、教員の個人情報など、学校が保有する情報のうち、学校及び学級の管理運営、学習指導、生徒指導、生活指導等に活用することを想定している情報であって、児童生徒がアクセスすることが想定されていない情報
校務用端末	校務系情報にアクセス可能な端末
校務系サーバ	校務系情報を取り扱うサーバ
校務系システム	校務系ネットワーク上に構成される情報システム
教育情報システム	校務系システム、校務外部接続系システム及び学習系システムを合わせた総称
無害化通信	インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信

適用範囲


ネットワーク
木更津市情報ネットワーク
インターネット系（情報系）
学習系（ＧＩＧＡスクール）
ＬGWAN系
校務外部接続系
個人番号利用事務系（基幹系）
校務系
組織
市長部局
教育委員会事務局
教育委員会（学校）
まなび支援センター
ネットワーク管理
市長部局
教育委員会
まなび支援センター

別表２（第３条）

推進体制

職	任務
教育長	⑴　教育長は、本市における全ての教育ネットワーク、教育情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。 ⑵　教育長は、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高情報セキュリティアドバイザーとして置き、その業務内容を定めるものとする。
教育部長	⑴　教育ネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。 ⑵　教育ネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。 ⑶　学校教育課長及び校長に対して、情報セキュリティ対策に関する指導及び助言を行う。 ⑷　情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、必要かつ十分な措置を実施する権限及び責任を有する。 ⑸　教育ネットワーク、教育情報システム及び情報資産に関する情報セキュリティ対策実施手順の維持及び管理を行う権限及び責任を有する。 ⑹　緊急時の円滑な情報共有を図るため、教育長、教育部長、学校教育課長、校長及びまなび支援センター所長を網羅する連絡体制を含めた緊急連絡網を整備する。
学校教育課長	まなび支援センター所長に対して、次に掲げる作業の指示及び管理を行う。 ⑴　教育ネットワークにおける開発、設定の変更、運用、見直し等 ⑵　教育ネットワークにおける情報セキュリティ対策 ⑶　教育ネットワーク、教育情報システム及び情報資産に関する情報セキュリティ対策実施手順の維持及び管理

まなび支援センター所長	学校教育課長の指示に従い、次に掲げる作業を行う。 ⑴　教育ネットワークにおける開発、設定の変更、運用、見直し等 ⑵　教育ネットワークにおける情報セキュリティ対策 ⑶　教育ネットワーク、教育情報システム及び情報資産に関する情報セキュリティ対策実施手順の維持及び管理
校長	当該学校に所属する教職員等に対して、情報セキュリティ対策に関する指導及び助言を行う。
副校長・教頭	⑴　校長を補佐し、当該学校における情報セキュリティ対策の実務に当たる。 ⑵　当該学校において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、速やかに校長より学校教育課長に報告を行い、指示を仰ぐ。
情報セキュリティに関する統一的な窓口	情報セキュリティに関して、木更津市 CSIRT と協調して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、外部の事業者等との情報共有を行う。

別表３（第４条）

⑴機密性による情報資産の分類

<table>
<tr><th>分類</th><th>分類基準</th><th>分類に応じた取扱い</th></tr>
<tr><td>機密性３</td><td>学校で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産</td><td rowspan="2">・機密性３の情報資産に対しては、支給以外の端末での作業の原則禁止とする。
・業務以外の目的での利用を禁止する。
・必要以上の複製及び配付を禁止する。
・必要に応じ、耐火、耐震、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管する。
・保管場所への必要以上の電磁的記録媒体等の持ち込みを禁止する。
・必要に応じ、情報の送信又は情報資産の運搬若しくは提供時に暗号化又はパスワード設定する。
・復元不可能な処理を施して廃棄する。
・業務上必要な場合を除き、外部に持ち出さない。</td></tr>
<tr><td>機密性２Ｂ</td><td>学校で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産</td></tr>
<tr><td>機密性２Ａ</td><td>学校で取り扱う情報資産のうち、直ちに一般に公表することを前提としていないが、児童生徒がアクセスすることを想定している情報資産</td><td>・業務以外の目的での利用を禁止する。
・必要以上の複製及び配付を禁止する。</td></tr>
<tr><td>機密性１</td><td>機密性２Ａ、機密性２Ｂ又は機密性３の情報資産以外の情報資産</td><td>-</td></tr>
</table>

⑵完全性による情報資産の分類

分類	分類基準	分類に応じた取扱い
完全性２	学校で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、学校関係者の権利が侵害される又は学校事務及び教育活動の適確な遂行に支障を及ぼすおそれがある情報資産	・バックアップする。 ・業務上必要な場合を除き、外部に持ち出さない。 ・必要に応じ、耐火、耐震、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管する。
完全性１	完全性２の情報資産以外の情報資産	-

⑶可用性による情報資産の分類

分類	分類基準	分類に応じた取扱い
可用性２	学校で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、学校関係者の権利が侵害される又は学校事務及び教育活動の安定的な遂行に支障を及ぼすおそれがある情報資産	・バックアップする。 ・必要に応じ、耐火、耐震、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管する。
可用性１	可用性２の情報資産以外の情報資産	-

別表４（第３３条）

コンピュータ及びネットワークの管理

	管理の対象	措置
1	ファイルサーバの設定等	住民の個人情報、人事記録等、特定の教職員等しか取り扱えないデータについて、別途ディレクトリを作成する等の措置を講じ、同一学校等であっても、担当職員以外の教職員等が閲覧及び使用できないようにする。
2	バックアップの実施	ファイルサーバ等に記録された情報について、定期的にバックアップを実施する。
3	情報システム仕様書等の管理	ネットワーク構成図、情報システム仕様書について、記録媒体に関わらず、業務上の関係者以外の者に閲覧される、又は紛失することがないよう、適正に管理する。
4	ログの取得等	ア　各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存する。 イ　取得したログについて、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について確認する。
5	障害記録	教職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適正に保存する。
6	ネットワークの接続制御、経路制御等	ア　フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定する。 イ　不正アクセスを防止するため、ネットワークに適切なアクセス制御を施す。 ウ　フィルタリング機能により閲覧することができないインターネットサイトについて、業務上必要と認めた場合は、当該サイトのフィルタリングを解除する。

7	外部の者が利用することができるシステムの分離等	外部の者が利用することができるシステムについて、必要に応じ他のネットワーク及び教育情報システムと物理的に分離する等の措置を講じる。
8	異なるネットワークとの接続制限等	ア　教育ネットワークを外部のネットワークと接続しようとする場合には、教育長の許可を得る。ただし、校務系又は個人番号利用事務系ネットワークと接続してはならない。 イ　接続しようとする外部ネットワークのネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、庁内及び学校の全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認する。 ウ　ウェブサーバ等をインターネットに公開する場合は、教育ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続する。 エ　接続した外部ネットワークのセキュリティに問題があると認められ、情報資産に対する脅威が生ずることが想定される場合には、教育長の判断に従い、速やかに当該外部ネットワークを物理的に遮断する。
9	重要性が高い情報に対するインターネットを介した外部からのリスク、児童生徒による重要性が高い情報へのアクセスリスクへの対応	ア　校務系システム及び学習系システム間の通信経路の論理的又は物理的な分離をするとともに、ウェブ閲覧やインターネットメールなどのインターネットを介した外部からのリスクの高いシステムと重要性が高い情報（特に校務系）を論理的又は物理的に分離する。 イ　校務系システムとその他のシステムとの間で通信する場合には、各システムにおけるアクセス権管理の徹底や無害化通信を行う等の適切な措置を講ずる。
１０	複合機のセキュリティ管理	複合機の調達、運用及び廃棄等のライフサイクルの各段

		階に応じて適正に管理する。
１１	特定用途機器	特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を講ずる。
１２	無線ＬＡＮに対する不正アクセス対策	ア　無線ＬＡＮを使用する場合、解読が困難な暗号化及び認証技術を使用する。 イ　機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講ずる。
１３	電子メールに関するセキュリティ管理	ア　権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行う。 イ　スパムメール等が内部から送信されていることを検知した場合は、メールサーバの運用を停止する。 ウ　電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にする。 エ　教職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を教職員等に周知する。 オ　システム開発、運用、保守等の委託事業者の作業員による電子メールアドレス利用について、委託事業者との間で利用方法を取り決める。
１４	無許可ソフトウェアの導入の禁止等	ア　教職員等が校務用端末及び学習者用端末に無断でソフトウェアを導入することを禁止する。ただし、業務上の必要がある場合は、これを許可し、当該ソフトウェアのライセンスを管理する。 イ　不正にコピーしたソフトウェアの利用を禁止する。
１５	機器構成の変更の制限	教職員等が校務用端末及び学習者用端末に対し機器の改

		造及び増設並びに交換を行うことを原則として禁止する。ただし、業務上の必要がある場合は、これを許可する。
１６	無許可でのネットワーク接続の禁止	教職員等が許可なく支給以外のパソコンをネットワークに接続することを禁止する。
１７	業務以外の目的でのウェブ閲覧の禁止	ア　教職員等が業務以外の目的でウェブを閲覧することを禁止する。 イ　教職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、校長に通知し適正な措置を求める。

別表５（第５７条）

学習者用端末のセキュリティ対策

	措置	内容
1	授業に支障のないネットワーク構成の選択（帯域や同時接続数など）	クラウドサービス提供事業者側のサービス要件基準を満たしたネットワーク構成を設計する。また、運用開始前には十分検証し、利用状況に応じて定期的に改修計画を行う。
2	不適切なウェブページの閲覧防止	児童生徒が端末を利用する際に不適切なウェブページの閲覧を防止する対策を講ずる。
3	マルウェア感染対策	ウイルス対策ソフトウェアの導入又はＯＳ等のバージョンの最新化など、学校内外での端末の利用におけるマルウェア感染対策を講ずる。
4	端末を不正利用させないための防止策	端末のセキュリティ状態の監視に加えて、不適切なアプリケーションやコンテンツの利用を制限し、常に安全で児童生徒が安心して利用できる状態を維持する。
5	セキュリティ設定の一元管理	端末のセキュリティ設定やＯＳアップデート、ウェブブラウザのアップデート、学習用ツールのインストール、端末の利用履歴も含めた状態確認などの作業を一元管理する。
6	端末の盗難及び紛失時の情報漏洩対策	児童生徒が端末を紛失しても、遠隔操作でロックをかける、あるいはワイプ（データ消去）することで第三者による不正操作や情報漏洩を防ぐ等の安全管理措置を講ずる。
7	運用及び連絡体制の整備	学校内外での端末の運用ルールを制定し、情報セキュリティインシデント発生時の児童生徒又は保護者からの連絡及び対応方法を各学校において整理する。

別表６（第５８条）

児童生徒におけるＩＤ及びパスワード等の管理

	措置		内容
1	ＩＤの登録、変更及び削除	⑴入学又は転入時のＩＤ登録処理	ＩＤについては、シンプルかつ一意であり、進級又は進学時に変更が必要とならないものを設定するよう努める。
		⑵転出、卒業又は退学時のＩＤ削除処理	転出や卒業退学時に学習用ツールのサービス利用期間が終了する場合は、あらかじめ児童生徒本人によるデータ移行をサービス利用期間内に実施し、ＩＤの利用停止後、最終的にはＩＤ及び関連するデータの完全削除を行う。ただし、本人同意や法令等に従った適切な管理の下、一部のデータを活用することは可能とする。
2	多要素認証等によるなりすまし対策		本人確認を厳格に行う必要がある場合は、多要素認証等のなりすまし対策を講ずる。

附　則

この要綱は、令和６年４月１日から施行する。