検証報告書

平成３０年６月２５日

前橋市学校教育ネットワークセキュリティ調査対策検討委員会

前橋市学校教育ネットワークセキュリティ調査対策検討委員会
名簿

委員長	小　暮　俊　子	小暮法律事務所弁護士
委員	横　山　重　俊	群馬大学 総合情報メディアセンター教授
	青　嶋　信　仁	株式会社ディアイティ セキュリティサービス事業部長

目　　次

第１　検証の概要

１　事案の概要

平成３０年３月１６日，前橋市学校教育ネットワークシステム（以下「MENET[1]」という）の公開用サーバへの不正アクセスが確認され，さらにその後の調査により，児童，生徒及び保護者等にかかる，極めて多数の個人情報が流出した可能性が高いことが同月３０日判明した。

このことは，市民に個人情報悪用の可能性に対する深刻な不安を与え，また，市民の前橋市教育委員会（以下「市教委」という）に対する信頼が著しく損なわれるという重大な事態を招いた。

２　本委員会設置の経緯

この事態を受けて，市教委は，MENET 関係者から独立した第三者からなる検証委員会を立ち上げて，上記１の事案（以下「本事案」という）の原因究明とともに，再発防止策を検討させるために，「前橋市学校教育ネットワークセキュリティ調査対策検討委員会」を設置することとした。

３　本委員会に対する委嘱事項

市教委教育長は，平成３０年４月１６日，本委員会委員長に対し，本事案の発生に至るまでの MENET 及び MENET 関係者の問題点，日常におけるシステム運用の経緯 及び本事案発生後の初動における問題点等を検証し，それらを踏まえ，本事案の原因究明とともに再発防止策を検討し，その結果を提言または意見として報告書にまとめることを委嘱した。

４　本委員会の目的

本委員会の検証は，上記３の委嘱の趣旨に従い，MENET 関係者から独立した中立公正な立場から，本事案の原因究明とともに再発防止策を提言することを目的とするものであり，本事案に係る関係者の責任の有無を確定し，これを追及することは目的とはしていない。

５　検証の方法

本委員会は，平成３０年４月１６日以降，規定，各種の契約書，納品物，メール，コンフィグなどの設定情報や１６台分のデジタルフォレンジック調査報告書含む報告書などの関係資料の分析や，関係者のヒヤリング等を

[1] 読み方は　めねっと

実施し，随時必要に応じて合議を重ね，同年６月２０日（以下「本報告書基準日」という）までに入手した情報に基づき，本報告書を作成した。

なお，本報告書基準日までのヒヤリング対象者は，合計延べ３４名であり，また，ヒヤリングは，上記４の目的にのみ利用することを対象者に説明したうえで実施した。

第２　本委員会が認定した事実

１　本事案の不正アクセスの態様

(1)　攻撃者は，平成２９年８月頃から前橋市学校教育ネットワークシステム（MENET）の DMZ ネットワークに設置された教育資料公開サーバに対して，何者かによって作成されたバックドアと呼ばれる裏口を利用して不正アクセスを開始した。教育資料公開サーバに多数存在していた，外部から本サーバを操作可能な脆弱性を利用して，バックドアが複数作成されていた。

その後，攻撃者は，目的を容易にするための不正ツール（認証情報を搾取するツール，ポートスキャンツール及びポートフォワーディングツールなど）を教育資料公開サーバに複数保存し，同年１２月中旬頃から教育資料公開サーバを経由して，適切に設定がされていなかったファイアウォールを通過しながら内部ネットワークに侵入した。内部ネットワーク内の学校系ネットワークおよび個人情報保護ネットワークに存在する端末やサーバにおいても不正ツールが保存された。

平成３０年３月６日，攻撃者は教育資料公開サーバから遠隔操作機能を利用して，個人情報保護ネットワーク内に設置されたドメインコントローラサーバに管理用アカウントで接続し，これを踏み台にして，多数の個人情報が保存されたファイル共有サーバから，各種ファイルを圧縮して教育資料公開サーバに収集・保存した。

その後，外部から教育資料公開サーバに保存された当該圧縮ファイルへのアクセスが多数確認されたことから，個人情報を含むファイルが外部に流出した可能性が高いことが認められた。

なお，本件不正アクセスは，平成３０年３月１６日 MENET ヘルプデスクの担当者が，教育資料公開サーバに対する不審なアクセスがなされているログを確認したことから発覚したものである。

(2)　流出した可能性のある個人情報の内容

①　平成２４年度から平成２９年度までに，前橋市（以下「市」という）の公立の小・中・特別支援学校に在籍した全ての児童生徒の給食費に関する４７，８３９人のデータ。個人情報の主な項目は次のとおりである。

学年，組，出席番号，氏名，性別，生年月日，国籍，住所，電話番号，保護者氏名，アレルギー，既往症等

②　同時期に市立公立学校（園）で給食を喫食していた園児児童生徒及び教職員の給食費の引落口座情報２８，２０９件。口座情報の主な項目は次のとおりである。

銀行名，支店名，口座番号，預金者名，引落金額，振替結果

２　前橋学校教育ネットワーク（MENET）の概要等

(1)　MENET は，市内の教育機関が今後の情報化社会の急激な進展を見込み，社会の変化に主体的に対応し，情報の収集や発信ができる児童生徒の育成を目指すことを目的として構築され，平成１０年から運用が開始された市内の小中学校や教育機関を結ぶ情報通信ネットワークである。

MENET は，市教委内で技術力のあった職員（以下「職員協力者」という）や，子ども達の教育に協力したいという意思をもつ，技術力のある民間ボランティア（以下「民間協力者」という）が，市教委の担当者に協力する形で発展してきた。

その後，MENET は平成１７年頃校務支援システムを導入し，個人情報を扱うようになった。また，平成２２年には前橋市総合教育プラザ内にネットワークオペレーティングセンター（NOC）を設けて運用されるようになり，市の行政ネットワークとも接続され，資産評価や学校評価のシステム等が追加され，さらに学校給食管理システムも導入された。このため MENET は，より広範囲かつ大量の個人情報を扱うようになっていった。

また，平成２４年，前橋市総合教育プラザに保管されていた教育資料をデータ化して検索できる教育資料検索システムが導入され，教育資料公開サーバを使って公開された。なお，本事案発生後の解析で，平成２６年１月にバックドアに感染していたことが判明した。ただし，本事案との関連を示す情報はない。

以上のように，MENET には，市教委内の異なる組織により，それぞれが所掌するサーバが置かれるようになった。

(2)　各学校で生じるパソコンのトラブル等に対処するため，市教委は外部に委託して，学校教育課指導係に MENET ヘルプデスクを置いた。

また，MENET の運用に関して，市教委，学校代表者，民間協力者などで構成される MENET 運用委員会が設けられ，平成２９年に MENET 推進委員会と名称が変更された。

３　平成２７年の MENET のデータセンター移管の業務委託

(1)　業務委託の経緯

MENET は，NOC を設けて運用されていたところ，平成２７年が NOC

の設備の更新時期となっていた。

市教委は，設備更新にあたって，MENET を市内の教育施設にとって，さらに使いやすいものにし，安定したサービスの提供や，無駄のない機能的なシステムの構築を目指して，前橋市総合教育プラザ内に設置してあったすべてのネットワーク機器やサーバ等をデータセンターへ移管することとした。

(2) プロポーザルの実施

平成２７年２月，市教委は「MENET データセンター移管業務委託選定審査委員会」を設置し，後に市が本件移管業務を委託した事業者（以下「委託事業者」という）を含む数社に，「MENET データセンター移管提案依頼書」を通知し，企画提案書の提出を求めた。

市教委の作成した仕様書及び仕様書別紙には，主にセキュリティに関連するものとして，次のような記載があった。

① 前橋市教育情報ネットワークの目的
市内の教育機関が安全にインターネットを活用することを目的として，構築すること

② 校務データ等のセンター管理
セキュリティを高めるとともに冗長性のあるシステムとすること

③ 既存サーバ移築/設置機器/内部ファイアウォール
本ファイアウォールに設定するフィルタは，市教委と新校務システムのベンダーと連携のうえ設計・設定すること

④ インターネット/機器/ISP 向けファイアウォール（外部ファイアウォール）
外部・内部・DMZ の３つのセグメントを設定し，レイヤー４レベルまでのアクセス制御を行うこと

⑤ 既存サーバ移築/センター運用/監査対応
前橋市の基準に従ったセキュリティ監査に対応すること。（年１回程度）
ドキュメント作成，ログデータの提出，セルフチェック記録の提出，監査立会を実施すること

⑥ 既存サーバ移築/センター運用/システム管理業務，依頼作業の実施
障害復旧・バージョンアップ/パッチ作業以外のシステム管理業務及び管理部門からの依頼作業を行う。作業実施後に報告書を提出すること

⑦ ログの保管

ファイアウォール　　５年

(3)　委託事業者の提案書

平成２７年３月１３日付で委託事業者が作成した「前橋市教育情報ネットワーク MENET のデータセンター移管提案書」には，主にセキュリティに関連するものとして次のような記載があった。

①　強固なセキュリティ対策

全社的なセキュリティ向上や仕組みを積極的に導入

②　総合的なセキュリティ対策

経験豊富な専門家を多数擁する技術セキュリティ対策チームによる総合的なセキュリティソリューションを提供することが可能

③　システム構成のコンセプト

外部からの攻撃を防御

④　システム構成の構成

ファイアウォールによる安心・安全な通信

⑤　VPN による安心・安全な通信

⑥　ログの保管

ＩＳＰ接続用ファイアウォール(外部ファイアウォール)　　５年

⑦　管理業務・監査対応・運用レポート

運用イベントの内容及び周期について

監査対応　年１回を想定した前橋市の基準に従った監査対応実施と依頼された場合のアクセスログなどの提供

依頼作業　　随時，実施・報告。

月次レポートの作成

(4)　「データセンター移管業務　要件定義書」について

市教委は，委託事業者の企画提案書を評価し，平成２７年３月２４日委託事業者を優先交渉者として選定した。

同年５月１５日委託事業者は,データセンター移管業務の要件定義書を提出した。要件定義書には，次のような記載があった。

① ISP 接続用ファイアウォール(外部ファイアウォール)

外部からのアクセス制御を行うためプロトコルなどによるアクセス制御を行う

② 内部ファイアウォール

データセンター内に個人情報を含むサーバの情報を保護するための内部ファイアウォールにより，各学校の生徒用セグメントからのアク

セス制御を行う

③ セキュリティ要件

対策内容：ファイアウォールにより，外部からは指定するサーバに対する指定のプロトコルのみにアクセスする

④ ログ管理要件

ISP 接続用ファイアウォール（外部ファイアウォール）　　5 年

⑤ 試験

単体試験，結合試験，総合試験：委託事業者が実施

受入れ試験：市が実施し，委託事業者が立会い

試験項目は基本設計にて協議し決定

⑥ 納品物

納品物一覧→CD-ROM 等で納品

ア　プロジェクト計画書

イ　マスタスケジュール

ウ　変更管理ドキュメント

エ　議事録

オ　要件定義書

カ　基本設計書

キ　詳細設計書

ク　試験成績表

ケ　運用手順書

(5)　契約締結について

平成２７年５月２１日，市と委託事業者は，データセンター移管設計・構築委託契約を締結した。

同契約において，市は委託事業者に，システム設計並びに，上記(4)の「データセンター移管業務　要件定義書」に基づく電気通信機器及びソフトウェアの提供およびその据え付け・調整等の業務を委託した。

納期は平成２７年９月３０日とされた。

なお，委託事業者は，市の承認を得て，システム構築の一部を下請業者（以下「再委託先」という）に再委託した。

(6)　設計方針について

平成２７年６月１９日に，委託事業者が作成した設計方針（案）およびその修正版に記載された「データセンター内論理接続図」と「アクセス制御イメージ(案)」には，ともに DMZ ネットワークと個人情報保護ネット

ワークをつなぐ経路は記載されていなかった。

(7) 基本設計書について

平成２７年６月委託事業者作成の基本設計書には次のような記載があった。

① セキュリティ設計方針

方針内容：ファイアウォールにより，外部からは指定のサーバに対する指定のプロトコルのみにアクセスを限定すること。

② 通信制限

通信制限イメージ図には，DMZ と個人情報保護ネットワークをつなぐ経路は記載されていない。

(8) 詳細設計段階について

詳細設計書は作成されていない。

附属書のネットワーク配置図は，基本設計書に沿ったものとなっていた。しかし，ファイアウォールのコンフィグは，市教委からのサーバの通信条件の情報が不明確であったことに起因して，次のとおりとなっていた。

① 外部ファイアウォール

内部ネットワークから DMZ ネットワークへの ICMP 通信が許可されている。それに対向する DMZ ネットワークから内部ネットワークへのコンフィグは，ICMP 通信だけでなく，全ての通信を許可する設定となっていた。

② 内部ファイアウォール

信用度の低いネットワークから信用度の高いネットワークへの通信許可ポリシーが設定されている。結果的に DMZ ネットワークから内部ネットワーク内の個人情報保護ネットワークへの通信を許可していた。

(9) 運用前の試験について

委託事業者が実施した運用前のファイアウォールの総合試験記録では，「公開ネットワーク（DMZ ネットワーク）から個人情報保護ネットワークにリクエストが到達しないことを確認」したことになっていたが，実際は確認されないまま，確認結果に「合格」と記載された。

なお，委託事業者側（再委託先を含む）の一部関係者には，試験の際に外部および内部ファイアウォールの設定が上記(8)の設定となっていたことは認識されていたが，委託事業者全体ではその認識は共有されていなかった。

(10) 市による受け入れ試験

委託事業者立会の下，市が行うとされた本番運用前の最後の受け入れ試験も合格とされ，平成２７年９月３０日市教委は委託事業者に検査合格通知書を交付した。

(11) システム構築における市教委の関わり方

市教委においては学校教育課の指導主事が MENET を担当していたが，指導主事の本来の仕事は学校の指導の推進であり，システム構築に十分に関わるのは難しく，また，人事異動により数年で担当者が替わった。このため，委託事業者からの問い合わせ等にも十分には対応できなかった。

平成２７年３月２４日委託事業者が優先交渉者として選定されて以降，同年５月頃までは委託事業者との週１回程度の定例会や分科会等が行われたが，その後は議事録が残っているのは同年６月１９日の打ち合わせが最後である。

４　移設後のシステム運用状況等

(1) 市は委託事業者とシステムにつき，保守契約を締結した。なお，システムには委託事業者以外の業者が導入したサーバもあり，それらは委託事業者の保守範囲には含まれなかった。

同契約書にある定例会は開催されず，月次報告はなされていなかった。

(2) 教育資料公開サーバは市教委の管理対象であったが，セキュリティアップデートはなされていなかった。

(3) 平成２８年８月頃に，委託事業者以外の業者が，学校無線 LAN 構築業務を受注した。

(4) 平成２９年８月，学校給食費管理システムは MENET から市の行政ネットワークに移行された。本事案で流出した可能性のある給食費に関する個人情報のファイルは，移行の際に CSV 形式で抽出されたもので，一部データはメンテナンスもされており，移行が完了となる平成３０年５月まで，移行先システムのトラブルに備えて暗号化せずに置く予定となっていた。

５　前橋市情報セキュリティポリシー

平成１４年市は情報資産を様々な脅威から防御し，市民の財産及びプライバシーを保護するために，情報セキュリティ基本方針等に関する「前橋市情報セキュリティポリシー」を定めた。

この情報セキュリティポリシーでは，「情報セキュリティポリシーの遵守状況を検証するため，必要に応じて情報セキュリティ監査及び自己点検を実施する」と定められている。また，市の最高情報セキュリティ責任者は副市長と定められている。

市の情報政策課は，情報セキュリティの監査の中で，人的セキュリティ（USB，パスワードなど）に関する監査については市教委を含めて実施していた。しかし，技術的セキュリティに関する監査は，行政ネットワークについては順次実施していたが，MENET については実施していなかった。また，市教委は，自身が行う MENET についての自己点検を実施していなかった。

６　不正アクセス発生前に生じていた不具合等

(1)　平成２８年１月，本来学校の教諭は見られないはずであるデータセンターのサーバ経由で各学校のサーバ内にアクセスできることや，センタサーバにおけるプロキシを経由しないインターネットへの通信があったことから，市教委はこの事象を委託事業者に報告した。委託事業者も内容の確認を行い，市教委へ情報の提供を問い合わせたが，応答はなかった。委託事業者もその応答をフォローすることなく，その後本不具合への具体的アクションに至らなかった。

(2)　同年６月，他県で生じた不正アクセス案件に関連し，市教委は委託事業者に不正アクセス対策に関する安全性確認を依頼したが，委託事業者は基本設計書を確認して，問題なしと回答した。

(3)　同年１２月，学校生徒系ネットワークから管理サーバ経由で個人情報保護ネットワークに入れるとの指摘があり，市教委は委託事業者に報告したが，その後具体的なアクションに至らなかった。

(4)　本事案において，平成２９年８月に不正アクセスを受けてから，ウイルス対策ソフトのアラートの管理はされていなかった。

７　不正アクセス確認後の初動

(1)　平成３０年３月１６日不正アクセスが確認され，市教育長や MENET

推進委員会に報告された。市教委は，委託事業者に不正アクセスの調査を依頼した。また，インターネットを一時的に遮断し，公開用サーバをネットワークから切断するとともに，外部ファイアウォールの設定の不備を修正するよう依頼した。なお，この過程で委託事業者からの報告により，ファイアウォールの通信ログは半日分しか保管されていないことが判明した。

また，市の情報政策課は，市教委からの報告を受けた後，ただちに市教委と市の行政ネットワークをつなぐ回線を遮断した。

(2) 同月１７日，市教育長は，市の最高情報セキュリティ責任者の副市長に本事案の状況について報告した。

(3) 同月１８日，市教委は委託事業者の機器故障時の問い合わせ窓口を訪問し，外部・内部ファイアウォールの設定内容の確認および制限の強化を指示した。

(4) 同月１９日，委託事業者を交えて対策会議を開催した。また，前橋警察署に連絡し，今後の対応について相談した。

(5) 同月２０日，群馬県警察本部職員が来庁し，詳細な状況を確認するとともに，今後の対応について相談した。

(6) 同月２１日，委託事業者の協力を得ながら，公開用サーバの複製をとり，簡易解析作業を開始した。

(7) 同月２２日，委託事業者から一次調査結果の報告を受けたが，さらにセキュリティ専門業者の詳細分析を依頼することとした。

(8) 同月２３日，群馬県警察本部に簡易解析の結果を送付した。
委託事業者の解析により，外部の不正なサイトへの通信記録が確認され，インターネットを完全に遮断した。

(9) 同月２６日セキュリティ専門業者から，現時点では個人情報の流出は確認できてないとの報告を受けた。

(10) 同月２８日，不正アクセスについて，記者発表を行った。

(11)　同月２９日，校務用サーバを正常化するため，サーバの解析や危険なファイルを取り除く作業の実施に向け，具体的な手順を検討した。

(12) 同月３０日，セキリィティ専門業者から，個人情報が不正に持ち出されていた可能性が高いとの報告があった。
セキュリティ専門業者は，流出した可能性が高いファイルがインターネット上に公開されていないかの調査を開始した。

(13)　４月３日，前橋警察署および群馬県警察本部に公開用サーバの解析情報を提供し，本事案について不正アクセス禁止法違反の疑いで捜査が開始された。

(14) 同月４日，個人情報流出の可能性が高いことにつき，記者発表をするとともに，市教委内に市民のためのコールセンターを設置した。
なお，流出した可能性が高いファイルがインターネット上に公開されていることは確認されていない。

(15) 同月５日，同日付け書面で，口座情報流出の可能性に関し，金融機関に対して，注意喚起を促した。

(16) 同月９日，同日付け書面で，保護者に個人情報流出問題について謝罪するとともに，注意喚起を促した。

(17) 同月１８日，セキリィティ専門業者から，新たに不正に持ち出された可能性がある情報が見つかったこと及びこれ以上の情報の流出は確認できないことの報告があった。

(18) 同月１９日，同月４日に記者発表を行った個人情報流出の件数が増えたこと記者発表をした。

(19) 同月３０日，市教委は情報流出の可能性の対象者で連絡先が判明した保護者あてにお詫び状を送付した。

第３　本事案における問題点とその原因

以上の本委員会が認定した事実を検証した結果，本委員会は不正アクセスがおきたのは教育資料公開サーバの脆弱性放置に，また個人情報へのアクセスにいたったのはファイアウォールの設定不備に原因があり，その背景には関係者全体の MENET およびセキュリティに対する理解不足があったと判断する。

そして，このような事態に至るまでの，MENET の体制や技術および運用面における問題点とその原因として次のような点を指摘できる。

１　市教委

(1) MENET に対する組織としての理解不足

MENET は，職員協力者や民間協力者が MENET 担当者に協力する形で発展してきた。

MENET は，発足時は個人情報を扱っていなかったが，その発展の中で，校務支援システムや学校給食管理システムなどの個人情報を扱うようになった。新しいシステムの追加に伴い，必然的に MENET の規模は大きくなり，管理の難易度は上がったにも関わらず，従来の職員協力者や民間協力者という善意ある人の貢献により成り立つ運営責任体制のままで進められてきた。

また，それぞれのシステムはいろいろな組織が独自に管理をしており，MENET の全体を理解できている人がいるとは言い難い状況の中で運営されてきた。このような運営体制は責任の所在の曖昧さにつながり，また情報やシステムの管理ができない状況を生んだ。

結果的に MENET は大きく発展したが，その発展内容は十分には理解されず，全体が把握されないままであったことに組織として気付いていなかった。

このため，データセンター移管業務委託時には市教委側は MENET 担当者と職員協力者で委託事業者に対する対応を行っていたが，その対応は委託事業者側から見ると，MENET の通信条件などの情報提供が不十分で，かつ依頼した質問への回答も滞るなど，不満を抱かざるを得ないものとなった。

(2) 組織としての担当業務および人員配置における配慮がなかったこと

市教委においては，学校教育課の指導主事が MENET 担当者となっていたが，同人は学校の指導の推進という仕事に加えて MENET の担

当を任され，しかも人事異動により数年で人が替わった。

このため，MENET では学校教育課以外の組織がシステムを設置して利用する中，担当者には各システムを理解し管理するための十分な技術，時間及び権限もなく，移管されるサーバの通信条件などの情報などは知る由もなかった。

このような状況でも MENET を運用しなければならなかったが，MENET 担当者の直属の上司は学校の指導の推進が本来の仕事であるため手助けはできず，必然的に当初から職員協力者や民間協力者によるできる範囲での支援中心で運用せざるを得なかった。

(3) セキュリティの重要性の認識不足

教育資料公開サーバの管理は，市教委の中の前橋市総合教育プラザという組織であり，データセンター移管業務の中では，同サーバの移管はサーバだけをデータセンターに物理的に移設するだけで，委託事業者による運用などはないという認識で進められた。しかし，この認識は同サーバの管理者に十分に周知されていなかったことから，管理者に同サーバにつきバージョンアップが必要という認識はなく，結果的に移設後は，追加，変更や確認は行われなかった。このような状況のまま同サーバが放置された結果，同サーバは脆弱性の問題を多く抱えたままで運用され，その脆弱性が利用されてバックドアが作られた。

また，MENET 内の端末やファイル共有サーバには，本件での原因に限らず，以前から複数のウイルスが存在し，ウイルス対策ソフトで検知されたものもあった。異常に気が付いた利用者からの連絡によって MENET ヘルプデスクで対処されたこともあるが，検知されたことをシステム的に MENET 関係者に通知し，組織的に対処することは行われていなかった。

本事案の攻撃者が持ち込んだ不正ツールが，ウイルス対策ソフトで検知された痕跡もあり，もしこれに適切に対処できていれば，個人情報の流出の可能性は低かった。

これらは日常のセキュリティ意識の低さを露呈するものである。

(4) システムの管理体制が確立されていないこと

データセンター移管業務の委託先業務のフェーズ毎のチェックや，納品物の検収および納品後の保守作業において，具体的にどのようなチェックを行ったか等の記録がなく，関係者に記憶も残っていなかった。さらに，不正アクセス発覚時には設計書関係の納品物自体も行方不明とい

う状況であり，システムに対する管理体制が確立されていなかったと言わざるを得ない。

２　市の監査

市は，MENET については技術的セキュリティ面を監査の対象としてこなかったことが認められ，市のセキュリティ管理施策の中で，MENET が全体との整合性がないまま別扱いされている。

３　委託事業

本事案では，市教委からのサーバについての通信条件が不明確であることに起因して，本システムが試験時及び運用開始時に基本設計に従わないセキュリティ上の重大な問題を持つネットワークであるまま本事案発生まで放置された。

これにつき，システムを構築した委託事業者側の原因としては次のようなことが考えられる。

・詳細設計以降の再委託先への委託において，管理確認が不十分であった。

・プロジェクト管理の一つである，市教委側とのコミュニケーションを自らが担っているという認識が不足していた。

・運用開始後も，運用業務の中のプロジェクト管理の一つであるコミュニケーションを自ら担っているという認識が不足していたことから，市教委側からの不正アクセス前に生じていた不具合等の調査依頼を受けたことを契機に，ネットワーク上の不備を修正する機会が複数回あったにもかかわらず，活用できなかった。

・個人情報を取り扱うシステムにふさわしい高セキュリティなシステム構築を自らが担っているという認識が不足していた。このため，提案書，要件定義書および基本設計書に高セキュリティと記載し，これを実施する姿勢をうち出していたにも関わらず，セキュリティ設計における当然の注意（due care）を果たすことができなかった。

４　本事案発生後の初動

本事案発生後の初動については，ファイアウォールの通信ログが半日分しか保管されていなかったため，解析に手間取ったという事態は生じたが，関係各所への報告や積極的な全容解明への行動や被害者となりうる市民への連絡対応などは速やかであり，初動対応はほぼ適切になされたものと判断する。

第４　再発防止策の提言

以上の本事案の問題点とその原因の検証を踏まえて本委員会は次のとおり提言する。

１　情報システムの企画・設計・構築・運用を担える体制作り

市教委側に，システム全体を統括でき，発注者の責任（委託事業者の管理・監督を含む）を果たせる体制を作ることが必要である。

このためには，委託事業者側と専門的な会話ができる人材の確保・育成が必要となる。人材の確保・育成には通常時間を要するため，暫定的にはこの業務自体を外部委託することも有効であり，これらを実現するための予算措置が必須であろう。

管理する組織としては，権限と責任をもち，現状の組織に属さない組織またはそれに類するものを作ることが望ましい。また，その組織は従来以上に，市の情報政策課と連携しながら情報セキュリティの確保に取り組むことが必要である。

２　市全体としてセキュリティ施策徹底

(1)　教職員のセキュリティ意識向上への取り組みへの関与

教職員のセキュリティ意識向上への取り組み内容として，現状の利用者作業に関する扱いだけではなく，情報基盤運用におけるセキュリティ意識向上を対象分野として取り上げることを考慮する。

(2)　市のシステム全体のセキュリティ監査の実施体制

セキュリティ監査対象として，MENET に属するデータサンター内のサーバやネットワーク機器類を市のシステム全体のセキュリティ監査の実施対象とすることを考慮する。

３　MENET 情報セキュリティポリシーの改訂

平成２９年１０月に発表された文部科学省が公表した「教育情報セキュリティポリシーに関するガイドライン」（以降，文科省ガイドライン）に準拠しつつ，MENET に適した形に改訂して進めていくことが必要である。そして，それに沿って，今後の対応を進めていくことが望ましい。

情報セキュリティポリシーは，定期的に見直しを行うことが必要であるが，変更された都度，その内容を教職員だけではなく，委託事業者にも周知することが望ましい。

4　MENET の運用を強化

(1)　組織で理解できるシステム

校務系システムは機微な情報を扱うため，他システムとネットワークの分離を基本とすることなど，文科省ガイドラインに準拠した形ですすめることが望ましいが，管理面を含めてすぐにできない部分は MENET に合った代替案を出すなど，組織で管理できる範囲ですすめることが望ましい。

(2)　外部委託

市教委と委託事業者とで，実施されていなかった MENET を安全に運用するための定期的な打合せや報告などを行い，密にコミュニケーションを図り，齟齬のない運用を行うことが望ましい。また，委託事業者による再委託を認める場合は，再委託先に委託事業者と同水準を担保させることが望ましい。

(3)　自己点検

MENET 全体について，接続機器の管理状況，システムのセキュリティアップデート管理状況，ログは規定通り取得できているかなどもあわせて自己点検を行い，問題がある点は組織的に対応を行い，問題解決まで確認することが望ましい。

(4)　ウイルス対策管理

ウイルス対策ソフトの通知管理を行い，原因と対策を組織的に行うようにすることが望ましい。

第５　終わりに

今日情報システムが, 児童生徒の教育環境や教育管理の場で果たしている役割は非常に大きくなって来ているとともに, 今後ますますその重要度は増していくと考えられる。この背景のもと，MENET をさらに改善・拡充する活動は学校教育活動の中で注目されるべきである。

再発防止策の提言として述べたように, 今回のようなセキュリティ上の問題を発生せないために「情報システムの企画・設計・構築・運用を担える体制作り」は必須であると考える。しかしながら，体制を再構築する際に注意すべきは, 単にセキュリティ上の問題を回避するという情報システムの企画・設計・構築・運用における「影」の部分のみを体制構築の目的とすべきでないことである。

MENET をさらに改善･拡充するために必要な教育の情報化により学びのイノベーションを起こそうという「光」の部分にも同様に注力すべきである。別の言い方をすれば，今回は「影」の部分の問題点が露呈したわけであるけれど,「光」の部分に関する問題がなかったのかについても同時に検証すべきであると考える。つまり,「光」と「影」の両面で，MENET の改善・拡充がさらに効率的に実施できる方法はないのかを継続的な情報システムの企画・設計・構築・運用のサイクルの中で検証し続けて行く必要があると考える。

前橋市の MENET の取り組みは，冒頭で述べた学校教育における情報システムの果たす役割を予見した先駆的なものであったと同時に, 発足後も関係者の継続的な努力・貢献により発展してきている。

本報告書で扱った, 本事案における目に見える被害に対する対応と再発防止策の実施は当然進めなくてはならないものであるとともに, 以下のような目にみえにくい被害を防ぐことにも留意することも肝要である。

１　セキュリティ上の脅威を避けるために, 現在失われている児童生徒に向けての教育の機会

２　MENET のこれまでの活動に根ざす，先駆的でもリスクを取って児童生徒の利益のためであれば積極的に動くという伝統の喪失

本委員会は MENET が, MENET の持つ伝統とコミュニティを活かし, 将来にわたって学校教育の質の向上のために発展していくことを祈念する。

参考　IT 用語の説明

CSV 形式	カンマでデータを区切ったテキストファイルである。 異なる環境や異なるアプリケーションの間でデータをやり取りする際に利用されることが多い。
DMZ ネットワーク	外部ネットワーク(インターネット)及び内部ネットワークの双方からの接続が許可され，「公開ネットワーク」や「非武装地帯」とも呼ばれている。DMZ ネットワークは外部ネットワークへの接続は許可されるが，内部ネットワークへの接続は許可されない。DMZ ネットワークのサーバが攻撃を受け侵入された場合でも，内部ネットワークへの侵入を保護する役割として設置される。
ICMP	「通信の不具合に係わる通知」や「ネットワークに接続された機器の動作確認」等を行うために使用する技術。
VPN	通信を暗号化して論理的に専用線であるかのように扱うネットワーク。
遠隔操作機能	「インターネット」上のコンピュータ等から，他のコンピュータのデスクトップ画面を表示するとともにキーボードやマウスの操作を行う機能。
情報セキュリティポリシー	組織がどのような情報をどのような方法で保護するのかなどの情報セキュリティ対策に対する取り組み姿勢や具体的なルールなどをまとめたもの。
脆弱性	ソフトウェアの不具合，設計ミス等によってできるセキュリティ上の欠陥。攻撃者は，脆弱性を悪用してサーバ等に侵入することがある。
コンフィグ	ネットワーク機器，セキュリティ機器やコンピュータなどがどのように動作するかが記載された設定情報。
デジタルフォレンジック	コンピュータやネットワーク等の資源から保全，調査・分析を行うための科学的調査手法・技術をさす。犯罪捜査や法的紛争に際し使われることが多い。
バックドア	コンピュータの機能を無許可で利用するための侵入口。
ファイアウォール	管理者等が定めたルールに基づいて，ネットワークの間の通信を「許可」したり「拒否」する機能を有するセキュリティ機器。ネットワークの「防火壁」とも呼ばれている。
外部ファイアウォール	本件においては，「インターネット」「DMZ ネットワーク」「内部ネットワーク」に接続されたファイアウォールを指

	し，「ISP 接続ファイアウォール」とも呼ばれる。
内部ファイアウォール	本件においては，内部ネットワーク内に設置されたファイアウォールを指す。内部ネットワーク内でより重要な情報を取り扱うネットワークへの通信を制限する目的で設置される。
ポートスキャンツール	特定のコンピュータやネットワークが許可している通信の出入口（ポート）を確認するためのツール。
ポートフォワーディングツール	特定のコンピュータへの遠隔操作を橋渡しする機能をもつツール。