一般財団法人神戸市学校給食会

情報セキュリティポリシー

制定日　平成30年９月１日
改正日　令和３年６月30日
施行日　令和３年７月１日

一般財団法人神戸市学校給食会

１　目的……１

２　定義……１
2.1　ネットワーク
2.2　情報システム
2.3　データ
2.4　情報セキュリティ
2.5　機密性
2.6　完全性
2.7　可用性

３　適用範囲……１

４　職員等の義務……２

５　情報セキュリティに関する権限と責任……２
5.1　常務理事の権限と責任
5.2　総務課長の権限と責任
5.3　課長の権限と責任

６　情報資産の分類と管理……３
6.1　情報資産の管理責任
6.2　情報資産の分類と管理方法

７　物理的セキュリティ……６
7.1　サーバ等の管理
7.2　ネットワークの管理
7.3　端末等の管理

８　人的セキュリティ……９
8.1　職員等の責務
8.2　研修・訓練
8.3　情報セキュリティに関する事件・事故等の報告・分析等
8.4　アクセスのための認証情報及びパスワードの管理

９　技術的セキュリティ……11

9.1　コンピュータ及びネットワークの管理
9.2　アクセス制御
9.3　システム開発、導入、保守等
9.4　コンピュータウィルス等不正プログラム対策
9.5　不正アクセス対策
9.6　セキュリティ情報の収集

10　運用面のセキュリティ……19
10.1　情報セキュリティの監視
10.2　情報セキュリティポリシー等の遵守状況の確認及び対処

11　外部サービスの利用……19
11.1　外部委託に関する管理
11.2　約款による外部サービスの利用

12　情報セキュリティポリシー等に関する違反に対する対応……20
12.1　懲戒処分
12.2　再発防止の指導等

13　評価・改善・見直し……21
13.1　監査
13.2　自己点検
13.3　改善
13.4　情報セキュリティポリシーの見直し

1　目的

一般財団法人神戸市学校給食会（以下「給食会」という。）の情報システムが取り扱う情報には、業務運営上重要な情報が多数含まれており、情報資産を人的脅威や災害、事故等様々な脅威から防御することは、継続的かつ安全・安定的な学校給食事業を確保するほか個人情報の保護の観点からも必要不可欠である。

このため、給食会が保有する情報資産の機密性、完全性及び可用性を維持することを目的として給食会の情報資産に関する情報セキュリティ対策の基本的な考え方と方針を規定するものである。

2　定義

2.1　ネットワーク

コンピュータ等を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）をいう。

2.2　情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

2.3データ

電子計算機処理に係る入出力帳票、磁気ディスク等の記録媒体に記録されている情報又は通信回線により送信される情報をいう。

2.4　情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

2.5　機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

2.6　完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

2.7　可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

3　適用範囲

3.1　組織の範囲

一般財団法人神戸市学校給食会事務分掌規則第２条に定める組織とする。

3.2　情報資産の範囲

情報セキュリティポリシーが対象とする情報資産は次のとおりとする。

3.2.1　物理資産

コンピュータ・ネットワーク・記録媒体等物理的な形状を有する資産でありかつ、情報を利用するのに必要な資産

3.2.2　データ資産

データ及び情報システムの設計等に関する情報

3.2.3　ソフトウェア資産

コンピュータ等の情報機器において稼動するプログラム

3.2.4　サービス資産

電源、メールサービス等契約により提供される情報システムに関連する業務

4　職員等の義務

一般財団法人神戸市学校給食会就業規則第２条第２項に定める職員（以下「職員」という。）及び労働者派遣事業により給食会の事務に携わる者（以下総称して「職員等」という。）は、情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行に当たっては情報セキュリティポリシーを遵守するものとする。

5　情報セキュリティに関する権限と責任

給食会の情報資産について、適切に情報セキュリティ対策を推進・管理するため情報セキュリティに関し権限のある者としての常務理事並びに総務課長及び給食・食育推進課長（以下総務課長及び給食・食育推進課長を総称して「課長」という。）の権限及び責任を規定する。

5.1　常務理事の権限と責任

ア　常務理事は、給食会における全てのネットワーク、情報システム、データ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。

イ　常務理事は、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する専門家をアドバイザーとして置くものとする。

5.2　総務課長の権限と責任

ア　給食会の情報資産に対する情報セキュリティ侵害が発生した場合又は侵害のおそれがある場合に、常務理事の指示に従い、常務理事が不在の場合には自らの判断に基づき、必要かつ十分な措置を行う権限及び責任を有する。

イ　総務課長は、給食・食育推進課長に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

ウ　総務課長は、給食会の共通的なネットワーク、情報システム、データ等の情報資産に関し、次の業務に関し権限及び責任を有する。

⑴　情報資産の開発、設定の変更、運用、見直し等

⑵　情報資産の情報セキュリティ対策

エ　総務課長は、給食会の共通的なネットワーク、情報システム、データ等の情報資産に対する侵害が発生した場合又は侵害のおそれがある場合には、常務理事へ速やかに報告を行い、指示を仰がねばならない。

オ　総務課長は、給食会における緊急時等の連絡体制の整備並びに職員等に対する指示を行う。

カ　総務課長は、情報セキュリティ監査の計画、実施、報告等を行う権限及び責任を有する。

5.3　課長の権限と責任

ア　課長は、所管する課における情報セキュリティ対策に関する統括的な権限及び責任を有する。

イ　課長は、所管するデータ等の情報資産の情報セキュリティ対策に関する権限及び責任を有する。

ウ　課長は、総務課長の指示に従い給食会の所管課内のネットワーク、情報システム、データ等の情報資産及びパーソナルコンピュータ等についての物理的セキュリティに関する管理を行う。

エ　課長は、所管課内におけるデータ等の情報資産に対する情報セキュリティ侵害が発生した場合又は侵害のおそれがある場合には、総務課長へ速やかに報告を行い、指示を仰がねばならない。

6　情報資産の分類と管理

6.1情報資産の管理責任

6.1.1　管理責任

課長は、所管する情報資産についての管理責任を有する。また、課長は、当該情報資産の利用範囲を定めなければならない。

6.1.2　情報取扱者の責任

職員等は、情報資産の作成・入手・利用等に際しては、十分にその責任を自覚したうえで行わなければならない。

6.1.3　複製等の管理

データが複製又は送信された場合には、当該複製等も原本と同様に管理しなければならない。

6.2　情報資産の分類と管理方法

6.2.1　情報資産の分類

ア　対象となる情報資産は、各々の情報資産の機密性、完全性及び可用性を踏まえ、次の重要性分類に従って分類する。

機密性

3	給食会事務で取り扱う情報資産のうち、特に機密性を要するもの（次のデータだけではなく、それらが含まれる記録媒体、パーソナルコンピュータ、システム等も同様） ・個人情報に関するデータ ・法令の規定により秘密を守る義務を課されているデータ ・部外に知られることが適当でない法人その他団体に関するデータ ・部外に漏れた場合に給食会の信頼を著しく害するおそれのあるデータ ・公開することでセキュリティ侵害が生じるおそれがあるデータ
2	機密性３には当てはまらないが、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
1	機密性２又は機密性３の情報資産以外のもの

完全性

2	給食会事務で取り扱う情報資産のうち、改ざん又は破損により、給食会事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産
1	完全性２以外の情報資産

可用性

2	給食会事務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、給食会事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産
1	可用性２以外の情報資産

イ　情報資産の機密性、完全性、可用性のいずれかの重要性分類２以上に分類される情報資産は、この対策基準の対象とする。また、重要性分類１の情報資産も、必要なものはできる限りこの対策基準に準じた対応を講じるものとする。

6.2.2　情報資産に対するリスク分析の実施

総務課長は、給食会が保有する情報資産に対して、リスク分析を行い、適切なリスク管理を行わなければならない。

6.2.3　情報資産の管理方法

ア　情報資産の管理

⑴　情報資産について、第三者が重要性の識別を容易に認識できないよう適切な管理を行わなければならない。

⑵　すべての情報資産を明確に識別し、重要な情報資産に対しては必要に応

じて目録を作成して管理しなければならない。

イ　データの作成

⑴　業務上必要のないデータを作成してはならない。

⑵　データの作成時に重要性分類に基づき、当該データの分類を定めなければならない。

⑶　作成途上のデータについても、紛失や流出等を防止しなければならない。また、データの作成途上で不要になった場合は、当該データを消去しなければならない。

ウ　情報資産の入手

⑴　給食会外の者が作成した情報資産を入手した職員等は、重要性分類に基づき、当該情報の分類を定めなければならない。

⑵　情報資産を入手した職員等は、入手した情報資産の分類が不明な場合、課長に判断を仰がなければならない。

エ　情報資産の利用

⑴　情報資産を利用する職員等は、情報資産を業務上の目的以外に利用してはならない。

⑵　情報資産の利用においては、情報資産の分類に応じ、利用者並びにアクセス権限を定めなければならない。

⑶　機密性３のデータは、課長の許可を得た場合、複写、複製、送付、送信を行うことができる。ただし、パスワード等による情報漏えい対策を施さなければ電子メールによる送信を行ってはならない。

⑷　電子メールにより機密性２のデータを送信する職員等は、必要に応じパスワード等による情報漏えい対策を施さけれればならない。

⑸　情報資産を利用する職員等は、記録媒体又は紙媒体に情報資産の分類が異なるデータが複数記録されている場合、最高度の分類に従って、当該記録媒体を取り扱わなければならない。

オ　情報資産の保管

⑴　課長は、情報資産の重要性分類に従って、所管する情報資産の保管を適切に行わなければならない。

⑵　職員等は、最終的に確定したデータを記録した記録媒体については書込禁止措置を行ったうえで保管しなければならない。

⑶　課長等は、持ち運び可能な記録媒体を、耐火、耐熱、耐水及び耐湿対策を講じたうえ施錠可能な場所への保管をする等適切な管理を行わなければならない。

⑷　課長は、情報システムのバックアップで取得したデータを記録する記録媒体を長期保管する場合は、自然災害を被る可能性が低い地域への保管を

考慮しなければならない。

⑸　機密性２以上の情報資産が保管された記録媒体の搬送に当たっては、必要に応じ鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置を施さなければならない。

カ　情報資産の提供・公表

⑴　機密性３の情報資産を外部に提供する者は、必要に応じ暗号化又はパスワードの設定を行わなければならない。

⑵　機密性３の情報資産を外部に提供する者は、常務理事に事前に許可を得たうえで、日時・担当者及び提供概要を記録しなければならない。

⑶　課長は、市民に公開する情報資産について、完全性を確保しなければならない。

キ　情報資産の廃棄

⑴　記録媒体が不要となった場合は、当該媒体に含まれるデータの消去を行ったうえで焼却、裁断又は溶解等により復元不可能な状態にして廃棄しなければならない。

⑵　情報資産の廃棄を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。

⑶　情報資産の廃棄を行う者は、課長の許可を得なければならない。

6.2.4　文書の管理

ア　情報セキュリティポリシーを実施していくうえで必要とされる文書は、一般財団法人神戸市学校給食会法人文書管理規程の定めに従い管理しなければならない。

イ　情報セキュリティに係る文書（以下「文書」という）を作成又は更新する場合は、あらかじめ課長による承認を受けなければならない。

ウ　文書は、定期的に見直しを行い、必要に応じて更新しなければならない。

エ　文書を廃棄する職員等は、廃棄文書が誤って使用されないようにしなければならない。ただし、廃棄文書を保持する必要がある場合には、廃棄文書と分かるように適切な識別を施さなければならない。

6.2.5　記録の管理

情報セキュリティポリシーの効果的運用の証拠を示すために、記録を作成し、適切な管理をしなければならない。

7　物理的セキュリティ

7.1　サーバ等の管理

7.1.1　基幹機器の管理

ネットワークの基幹機器については、施錠した収納設備内で厳重な管理を行

わなければならない。

7.1.2　装置の取付け等

ア　総務課長は、ネットワーク機器及び情報システム機器の取り付けを行う場合、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し、容易に取り外せないよう適切な固定を行う等必要な措置を施さなければならない。

イ　総務課長は、システムの停止により、給食会事務の執行等に重大な影響を及ぼすおそれがあるものについて二重化等を行い、同一データを保持し、システムの運用が停止しないように努めなければならない。

ウ　権限のある職員等以外の者が容易に操作できないように、総務課長は、利用者のID、パスワードの設定等の措置を施さなければならない。

7.1.3　配線

ア　配線の変更、追加については、総務課長の権限とする。

イ　総務課長は、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等必要な措置を施すほか、損傷等があった場合には、迅速に対応しなければならない。

ウ　総務課長は、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できない場所に設置する等適切に管理しなければならない。

7.1.4　機器等の定期保守及び修理

ア　課長は、所管の可用性２のサーバ等の機器は、定期保守を実施しなければならない。

イ　課長は、記憶装置を内蔵する所管の機器を外部の業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、外部の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、守秘義務契約を締結する他、秘密保持体制の確認などを行わなければならない。

7.1.5　事務所外への機器の設置

課長は、給食会事務所の敷地外にサーバ等の機器を設置する場合、常務理事の許可を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

7.1.6　機器の廃棄等

課長は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、すべてのデータを消去の上、復元不可能な状態にする措置を施さなければならない。

7.1.7　機器等の搬入出

ア　課長は、所管の機器等を搬入する場合、あらかじめ当該機器等の既存情報

システムに与える影響について、所属職員等に確認を行わせなければならない。

イ　機器等の搬入出には職員等が同行する等の必要な措置を施さなければならない。

7.2　ネットワークの管理

7.2.1　事務所内の通信回線等の管理

総務課長は、事務所内の通信回線及び通信回線装置を関係機関と連携し、適切に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適切に保管しなければならない。

7.2.2　外部ネットワークへの接続

総務課長は、通信回線による外部へのネットワーク接続は必要最低限のものに限定し、できる限り接続ポイントを減らさなければならない。

7.2.3　ネットワークで使用する回線

ア　ネットワークに使用する回線は送信途上においてデータの破壊、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が実施されたものでなければならない。

イ　総務課長は、ネットワークで使用する回線を選択するに当たって、必要な可能性を考慮しなければならない。

7.3　端末等の管理

7.3.1　端末等の盗難防止策

課長は、所管する事務室等の端末等について、ワイヤーによる固定等の盗難防止のための措置を講じなければならない。

7.3.2　ログインパスワード

総務課長は、情報システムへのログインパスワードの入力を必要とするように設定しなければならない。また、必要に応じてＢＩＯＳパスワード、ハードディスクパスワード等を併用しなければならない。

7.3.3　認証の併用

総務課長は、パスワード以外に必要に応じてIDカード等による認証の併用を行うものとする。

7.3.4　暗号化機能の利用

総務課長は、端末のデータの暗号化等の機能を有効に利用しなければならない。

7.3.5　タブレット端末等の持ち運び可能な端末（モバイル端末）のセキュリティ

モバイル端末を事務所外で利用する場合は、端末の紛失・盗難対策として普段からパスワードによる端末ロックを設定しておかなければならない。また紛

失・盗難にあった際の対応として、遠隔消去（リモートワイプ）や自己消去機能などを活用できるときは、それらの機能を活用し、モバイル端末内のデータを消去しなければならない。

8　人的セキュリティ

8.1　職員等の責務

8.1.1　情報セキュリティポリシー等の遵守義務

職員等は、情報セキュリティポリシー及びこれに基づく文書に定められている事項を遵守しなければならない。また、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がある場合には、課長に相談し、指示を仰がなければならない。

8.1.2　法令等の遵守義務

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、次の法令等を遵守し、これらに従わなければならない。

ア　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）

イ　著作権法（昭和45年法律第48号）

ウ　個人情報の保護に関する法律（平成15年法律第57号）

エ　行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）

オ　神戸市個人情報保護条例（平成９年10月条例第40号）

カ　一般財団法人神戸市学校給食会法人文書管理規程（平成30年８月規程第２号）

キ　一般財団法人神戸市学校給食会個人情報保護規程（平成30年８月規程第４号）

8.1.3　指示に基づいた情報資産の利用等

職員等は、所管の課長の指示等に従い、情報資産を利用するとともに、開発、設定の変更、運用、更新等の作業を行う。

8.1.4　支給以外の情報資産の持ち込み禁止

職員等は、支給以外のパーソナルコンピュータ及び記録媒体等の持ち込みをしてはならない。

8.1.5　情報資産の持ち出し禁止

職員等は、課長の許可を得た場合に限り、事務所外に情報資産を持ち出すことができる。

8.1.6　業務目的外の利用禁止

職員等は、業務目的外でのパーソナルコンピュータ等の利用、情報システムへのアクセス、電子メール利用及びインターネットへのアクセス等を行っては

ならない。

8.1.7　端末等の利用

ア　職員等は、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課長の許可なく変更してはならない。

イ　職員等は、端末や電磁的記録媒体、データが印刷された文書等について、第三者に使用されること、又は課長の許可なく情報を閲覧されることがないように、離席時の端末のロックや記録媒体、文書等の容易に閲覧されない場所への保管等、適切な措置を講じなければならない。

8.1.8　事務室外における情報処理作業の制限

ア　職員等は、事務室外で情報処理作業を行う場合には、課長の許可を得なければならない。

イ　職員等は、事務室執務室外で情報処理作業を行う際、支給以外のパーソナルコンピュータによる情報処理を行ってはならない。

8.1.9　異動、退職時等の遵守事項

職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産を、返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

8.2　研修・訓練

8.2.1　職員等に対する研修の実施

ア　総務課長は、職員等を対象とする情報セキュリティに関する研修を毎年度最低１回実施しなければならない。

イ　新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。

ウ　総務課長は、毎年度情報セキュリティに関する研修の実施状況を記録しなければならない。

8.2.2　緊急時対応訓練

総務課長は、緊急時対応を想定した訓練を定期的に実施させなければならない。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の内容等を定め、また、効果的に実施できるようにしなければならない。

8.2.3　研修等への参加

職員等は、情報セキュリティに関する意識を深め情報セキュリティ上の問題が生じないようにするため、定められた研修・訓練に参加しなければならない。

8.3　情報セキュリティに関する事件・事故等の報告・分析等

8.3.1　情報セキュリティ関する事件・事故の報告

ア　職員等は、情報セキュリティに関する事件・事故、システム上の欠陥及び

誤動作を発見した場合、若しくは外部から報告を受けた場合、速やかに課長に報告しなければならない。

イ　総務課長は、報告のあった事故等について、必要に応じて神戸市教育委員会等の業務上の関係機関に連絡を行うとともに常務理事に報告しなければならない。

8.3.2　事故等の分析・記録等

ア　情報セキュリティに関する事件・事故等を引き起こした課の課長は、総務課長と連携し、当該情報セキュリティに関する事件・事故等を分析し、記録を保存し、常務理事に報告するものとする。

イ　常務理事は、報告を受けた情報セキュリティに関する事件・事故等について再発防止策の策定、実施のための必要な措置を指示しなければならない。

8.4　アクセスのための認証情報及びパスワードの管理

8.4.1　IDの管理

ア　職員等は、他人に自己が利用しているIDを利用させてはならない。

イ　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てはならない。

8.4.2　パスワードの管理

ア　職員等は、自己のパスワードに関し、次の事項を遵守しなければならない。

⑴　パスワードは秘密にし、パスワードの照会等には一切応じない。

⑵　情報システム又はパスワードに対する危険のおそれがある場合には、課長に速やかに報告し、パスワードを速やかに変更する。

⑶　パスワードを記載したメモを作成する場合は、特定の場所に施錠して保存する等により、他人が容易に見ることができない措置をとる。

⑷　パスワードは十分な長さとし、文字列は想像しにくいものとする。

⑸　複数の情報システムを扱う場合は、同一のパスワードを複数のシステムで用いない。

⑹　仮のパスワードは、最初のログイン時点で変更する。

⑺　パーソナルコンピュータ等のパスワードの記憶機能を利用しない。

⑻　職員等の間でパスワードを共有しない。

イ　課長は、パスワードの照会等には一切応じてはならない。

ウ　給食報告サイトのログインID・パスワードの管理

⑴　食数報告のために整備された給食報告サイトについて、学校ごとに付与するログインID・パスワードは、毎年、変更する。

⑵　パスワードは十分な長さとし、文字列は想像しにくいものとする。

9　技術的セキュリティ

9.1　コンピュータ及びネットワークの管理

9.1.1　データの保存

データの保存については、課長の定める方法により保存を行わなければならない。

9.1.2　ファイルサーバの設定

特定の職員等のみが取扱う権限を持つデータについては、同一所属であっても、権限のない者が閲覧及び使用できないよう設定しなければならない。

9.1.3　アクセス記録の取得等

ア　課長は、所管するシステムにおいて、アクセス記録及び情報セキュリティの確保に必要な記録を取得し、窃取、改ざん、誤消去等を防止する措置を施したうえで一定期間保存する。また、不正アクセスの兆候を発見するために定期的にそれらを分析することとする。

イ　課長は、システムから自動出力したアクセス記録等について、必要に応じ、外部記録媒体にバックアップしなければならない。

9.1.4　仕様書等の保管

課長は、所管するシステムのネットワーク構成図、情報システム仕様書等に関し、記録媒体の形態に関わらず、業務上必要とする者以外の者が閲覧したり、紛失したりすることがないよう、適切な保管をしなければならない。

9.1.5　情報資産のバックアップ

総務課長は、所管する必要なものはサーバの二重化対策実施の有無に関わらず、定期的に情報資産のバックアップのための対応を行うものとする。

9.1.6　通信回線によるデータの送信

総務課長は、所管するシステムにおいて、通信回線によりデータを送信する場合、専用通信回線を使用する、送信するデータを必要最小限にする等データの保護のために適切な措置を講じなければならない。

9.1.7　外部の者が利用するシステム

総務課長は、インターネット等により外部の者が利用できるシステムにおいては、必要に応じ他のネットワーク及び情報システムと物理的に分ける等、情報セキュリティ対策について特に強固に対策をとらなければならない。

9.1.8　Webサイトでの情報公開時の注意事項

総務課長は、Webサイトにより情報を公開・提供する場合に、当該サイトに係るシステムにおいて情報の漏えい・改ざん・消去、踏み台、DoS攻撃等を防止しなければならない。また、メールシステムを含め各業務システムにおいても、他のシステムに対する攻撃の踏み台とならないようにコンピュータウィルス対策など適切な管理をしなければならない。

9.1.9　無許可ソフトウェアの導入等の禁止

ア　職員等は、各自に供与された端末に対して、無断でソフトウェアを導入し

てはならない。

イ　職員等は、業務を円滑に遂行するために必要なソフトウェアがある場合、総務課長の許可を得た場合に限り、利用することができる。

ウ　職員等は、不正にコピーしたソフトウェアを導入又は使用してはならない。

9.1.10　機器構成の変更の禁止

職員等は、ネットワーク及び各自に供与された端末等に対して、端末及びその他機器の増設又は改造を行ってはならない。軽微な機器の増設の場合は、課長の許可を必要とする。

9.1.11　電子メール

ア　課長は、電子メールに添付されるファイルについて、セキュリティ上問題があると思われるファイルについては、送受信を制限できるようにしなければならない。

イ　職員等は、業務上必要のない送信先に電子メールを送信してはならない。

ウ　職員等は、複数の宛先に電子メールを送信する場合、必要がある場合を除き他の送信先の電子メールアドレスがわからないようにしなければならない。

エ　職員等は、重要な電子メールを誤送信した場合、課長に報告しなければならない。

オ　職員等は、自動転送機能を用いて、電子メールを転送してはならない。

9.1.12　電子署名・暗号化

職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、総務課長が定める電子署名、暗号化又はパスワード設定等の方法を用いて、送信しなければならない。

9.1.13　無許可端末の接続禁止

職員等は、課長の許可なく端末等をネットワークに接続してはならない。

9.1.14　障害記録

課長は、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体系的に記録し、適切に保存しなければならない。

9.2　アクセス制御

総務課長又は課長は、所管するネットワーク又はシステムにおいて、次の事項を実施しなければならない。

9.2.1　利用者の識別及び認証

課長は、所管するネットワーク又は情報システムに権限がない職員等がアクセスすることが不可能となるように、利用者の識別及び認証等適切な対応を行わなければならない。

9.2.2　利用者登録

ア　総務課長は、利用者の登録、変更、抹消、登録した情報資産の管理、異動、

出向及び退職時における利用者IDの取扱い等については、定められた方法に従って行わなければならない。必要な利用者登録・変更・抹消は、総務課長に対する申請により行う。

イ　総務課長は、利用されていないIDが放置されないようしなければならない。

9.2.3　ネットワークにおけるアクセス制御

総務課長は、アクセス可能なネットワーク又はネットワーク上のサービス毎にアクセスできる者を定めなければならない。また、ネットワークサービスを利用する権限を有しない職員等が当該サービスを利用できるようにしてはならない。

9.2.4　強制的な接続制御、経路制御

ア　課長は、不正アクセスを防止するため、適切なネットワーク経路制御を施さなければならない。

イ　課長は、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、ルータ等に搭載されている通信ソフトウェア等を設定しなければならない。

9.2.5　外部からのアクセス

ア　総務課長は、外部からのアクセスの許可は、合理的理由を有する必要最低限のものに限定しなければならない。

イ　内部ネットワーク及び情報システムへのアクセス方法及び利用方法等は、通信途上の機密性及び利用者の真正性が確保できるものでなければならない。

ウ　課長は、事務所外で利用する端末を職員等に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。

9.2.6　外部ネットワークとの接続

ア　総務課長は、外部ネットワークとの接続にあたり、当該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、給食会の情報資産に影響が生じないことを確認したうえで、常務理事の許可に基づき接続しなければならない。

イ　総務課長は、接続に際して情報セキュリティの確保できるネットワーク構成を採らなければならない。課長は、当該外部ネットワークの瑕疵により給食会のデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対応するため、必要に応じて当該外部ネットワークの管理責任者による損害賠償責任を契約上担保するよう努めなければならない。

ウ　接続した外部ネットワークのセキュリティに問題が認められ、給食会の情報資産に脅威が生じるおそれがある場合には、総務課長は当該外部ネットワークとの接続を物理的に遮断することができるものとする。

9.2.7　ログイン試行回数の制限等

課長は、学校が使用する給食報告サイト等において、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ教職員等がログインしたことを確認することができるようにシステムを設定するよう考慮しなければならない。

9.2.8　パスワードに関する情報の管理

ア　総務課長は、職員等のパスワードに関する情報を厳重に管理しなければならない。また、職員等のパスワードを発行する場合において、仮のパスワードを発行する場合、ログイン後直ちに仮のパスワードを変更させなければならない。

イ　総務課長は、仮のパスワードも含めパスワードを発行する場合、パスワードの長さは十分な長さとし、文字列は想像しにくいものとする。

ウ　総務課長は、パスワードは定期的に変更し、古いパスワードを再利用しないものとする。

9.3　システム開発、導入、保守等

9.3.1　情報システムの調達

ア　課長は、情報システムの調達に当たっては、一般に公開する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しなければならない。

イ　課長は、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しなければならない。

9.3.2　情報システムの開発等

ア　課長は、ネットワーク及び情報システムの開発、導入、更新及び運用保守に当たっては、次の事項を定める。

⑴　責任者及び監督者
⑵　作業者及び作業範囲
⑶　開発するシステムと運用中のシステムとの分離
⑷　開発・保守に関する設計仕様などの成果物の提出
⑸　セキュリティ上問題となり得るおそれのあるハードウェア及びソフトウェアの使用禁止
⑹　アクセス制限
⑺　機器の搬入出の際の許可及び確認
⑻　記録の提出義務
⑼　仕様書・マニュアル等の定められた場所への保管
⑽　情報システムに係るソースコードの適切な方法での保管
⑾　開発・保守を行った者の利用者ID、パスワード等の当該開発・保守終了後に不要となった時点での速やかな抹消

イ　課長は、ネットワーク情報及び情報システムの開発、導入、更新及び運用保守に当たって、不正にコピーしたソフトウェア及び支給以外のソフトウェアの導入又は使用等、問題のある行為が発生しないようにしなければならない。

ウ　課長は、ネットワーク情報及び情報システムの開発、導入、更新及び運用保守に当たって、コンピュータウィルス等対策ソフトウェアを導入する等、ウィルス感染やサイバー攻撃による情報漏えい等が発生しないようにしなければならない。

9.3.3　情報システムの移行

ア　課長は、所管するシステム開発・保守計画の策定時に情報システムの移行手順を明確にしなければならない。また、移行の際、情報システムに記録されているデータの保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

イ　課長は、新たに情報システムを導入する際には、既に稼働している情報システムに接続する前に、十分な試験を行わなければならない。また、既存の情報システムを更新する際には、既に稼働している情報システムとの連携において、十分な試験を行わなければならない。

ウ　課長は、擬似環境による動作確認後に情報システムの移行を行わなければならない。また、作業については、作業経過を確認しながら実施するとともに、作業内容を記録しなければならない。

エ　課長は、原則として個人情報及び機密性の高い生データを、試験データに使用してはならない。ただし、合理的な理由がある場合で、常務理事が許可した場合は、この限りではない。

オ　課長は、試験に使用したデータ及びその結果を一定期間厳重に管理しなければならない。

9.3.4　情報システムの入出力データ

ア　課長は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を必要に応じて組み込むように情報システムを設計しなければならない。

イ　課長は、内部処理において誤ったデータに書き換えられる等の可能性がある場合に、書き換え等を検出するチェック機能を組み込むように情報システムを設計しなければならない。

ウ　課長は、情報システムから出力されるデータは、保存された情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

9.3.5　ソフトウェアの保守及び更新

課長は、ソフトウェア等を更新、又は修正プログラムを導入する場合、不具

合及び他のシステムとの相性の確認を行い、計画的に更新し又は導入しなければならない。

また、情報セキュリティに重大な影響を及ぼす不具合に対する修正プログラムについては、課長は、速やかに対応を行わなければならない。

9.3.6　作業管理記録

課長は、担当するシステムにおいて行ったシステム変更等の作業については、作業記録を作成しなければならない。作成した作業記録は、窃取、改ざん等をされないように適切に管理を行わなければならない。

9.4　コンピュータウィルス等不正プログラム対策

9.4.1　総務課長の実施事項

総務課長は、次の事項を実施しなければならない。

ア　コンピュータウィルス等の情報について職員等に対する注意喚起を行う。

イ　所管するサーバ及び端末に、コンピュータウィルス等対策ソフトウェアを常駐させる。

ウ　情報システムにおいてフロッピィディスク等の記録媒体を使用する場合、給食会が管理しているものを職員等に使用させるとともに、当該媒体の使用にあたり、ウィルスチェックを行わせる。

エ　コンピュータウィルス等対策ソフトウェア及び定義ファイルは常に最新のものに保たなければならない。インターネットに接続していないシステムにおいても、定期的に当該ソフトウェア及び定義ファイルの更新を実施しなければならない。

オ　業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを原則として利用してはならない。

カ　コンピュータウイルス対策ソフトウェア等の設定変更権限については、一括管理し、総務課長が許可した職員を除く職員等に当該権限を付与してはならない。

9.4.2　職員等の遵守事項

職員等は、次の事項を遵守しなければならない。

ア　端末において、コンピュータウィルス等対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更しない。

イ　外部ネットワーク及びフロッピィディスク等の記録媒体からデータ又はソフトウェアを取り入れる際には、必ずコンピュータウィルス等対策ソフトウェアによるチェックを行う。

ウ　外部ネットワーク及びフロッピィディスク等への記録媒体へデータ又はソフトウェアを送信・書き込みする際には、必ずコンピュータウィルス等対策ソフトウェアによるチェックを行う。

エ　差出人が不明な電子メール又は不自然なファイルが添付された電子メールを受信した場合は速やかに削除する。

オ　端末に対して、コンピュータウィルス等対策ソフトウェアによる完全スキャンを定期的に行い、スキャンの実行を途中で止めない。

カ　提供されたコンピュータウィルス等の情報を常に確認する。

キ　添付ファイルのあるメールを送受信する場合は、コンピュータウィルス等対策ソフトウェアでチェックを行う。

ク　コンピュータウィルス等に感染したおそれのある場合には、速やかに課長に報告するとともに、その指示に従い、ＬＡＮケーブルの即時取り外しや端末の通信機能の停止等、他への感染を防止する指示を講じる。

ケ　端末には、業務に必要なソフトウェアのみをインストールするとともに、端末に導入されているソフトウェアについて、課長から最新版へのアップデートの指示等があったときは、速やかにその指示に従う。

9.4.3　専門家の支援体制

常務理事は、実施しているコンピュータウィルス等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ようにしておかなければならない。

9.5　不正アクセス対策

9.5.1　使用されていないポートの閉鎖等

課長は、不正なアクセスによる影響を防止するための必要な措置を講じなければならない。

ア　使用されていないポートを閉鎖する。

イ　不正アクセスによるデータの書換えを検出し、Ｗｅｂサイトの改ざんを防止する。

ウ　ソフトウェアにセキュリティホールが発見された場合は、速やかに修正プログラムを適用する。

9.5.2　攻撃の予告

課長は、攻撃の予告等サーバ等に不正アクセスを受けることが明白な場合には、システムの停止、他のネットワークとの切断などの必要な措置を講じなければならない。

また、関係機関との連絡を密にして情報の収集に努めなければならない。

9.5.3　記録の保存

常務理事は、不正アクセス行為の禁止等に関する法律違反等犯罪の可能性がある不正アクセスを受けた場合、不正アクセスの記録の保存に努めるとともに、関係機関との緊密な連携に努めなければならない。

9.5.4　内部からの不正アクセスの監視

課長は、職員等が使用している端末からの事務所内のサーバ等に対する不正アクセスや外部のサイトに対する不正アクセスを監視しなければならない。

9.6　セキュリティ情報の収集

総務課長は、セキュリティホール等のセキュリティに関する情報を収集し、必要に応じ職員等で情報を共有しなければならない。

10　運用面のセキュリティ

10.1　情報システムの監視

10.1.1　事象の検知

総務課長は、セキュリティに関する事象を検知するため、情報システムの監視を行わなければならない。

10.1.2　時刻同期

総務課長は、重要なアクセスログ等を取得するサーバの正確な時刻設定又はサーバ間の時刻同期ができる措置を施さなければならない。

10.1.3　常時監視

総務課長は、外部と接続するシステムを稼働中、常時監視しなければならない。

10.2　情報セキュリティポリシー等の遵守状況の確認及び対処

総務課長は、所管の範囲において情報セキュリティポリシー及びこれに基づく文書の遵守状況について常に確認を行い、問題を認めた場合には速やかに常務理事に報告しなければならない。

常務理事は、発生した問題について、適切かつ速やかに対処しなければならない。

11　外部サービスの利用

11.1　外部委託に関する管理

11.1.1　委託先事業者の選定

ア　特定個人情報を扱う業務又はネットワーク及び情報システムの開発・保守並びにデータ処理その他情報処理に係る外部委託をする場合は、委託先の選定にあたり、委託内容に応じたセキュリティレベルが確保されなければならない。

イ　クラウドサービスを利用する場合、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サービスを利用しなければならない。

11.1.2　契約書の記載事項

ア　特定個人情報を扱う業務又はネットワーク及び情報システムの開発・保守並びにデータ処理その他情報処理に係る業務を外部委託する場合は、当該委

託先事業者との間で、下記事項を明記した契約を締結しなければならない。

⑴　データその他業務上知り得た情報（以下「データ等」という）の秘密の保持に関する事項

⑵　第三者への委託（以下「再委託」という。）の禁止又は制限に関する事項

⑶　データ等の目的以外の目的のための使用及び第三者への提供の禁止に関する事項

⑷　データ等の複写及び複製の禁止に関する事項

⑸　データ等の取扱いに関する事故の発生時における報告義務に関する事項

⑹　データ等の取扱いに関する検査の実施に関する事項

⑺　契約に違反した場合における契約の解除及び損害賠償に関する事項

⑻　委託業務終了時の資産の返還、廃棄等に関する事項

⑼　情報セキュリティポリシー及びこれに基づく文書の遵守に関する事項

⑽　事故時等の公表に関する事項

⑾　委託先の責任者、委託内容、作業者、作業場所の特定に関する事項

⑿　委託先の責任者及び従事者に対する研修の実施に関する事項

⒀　情報セキュリティ確保への取り組みの実施状況に係る報告義務に関する事項

イ　アに加えて、次に掲げる事項を必要に応じて契約書等に明記するよう努めるものとする。

⑴　提供されるサービスレベルの保証に関する事項

⑵　委託業務の定期報告及び緊急時報告義務に関する事項

⑶　外部施設等への情報資産の搬送時における紛失、盗難、不正コピー等の防止に関する事項

11.1.3　情報セキュリティ確保への取組み状況等の調査

課長は、契約締結後においても、当該委託先事業者のセキュリティ確保への取組み実施状況等について、定期的若しくは随時、調査を行い、安全の確保に努めなければならない。

11.1.4　再委託

再委託（再々委託を含む。）を受ける事業者がある場合、11.1.2及び11.1.3に定める事項は再委託を受ける事業者にも適用する。

11.2　約款による外部サービスの利用

利用規約等に同意して利用する外部サービスでは、機密性2以上の情報を扱ってはならない。

12　情報セキュリティポリシー等に関する違反に対する対応

12.1　懲戒処分

情報セキュリティポリシー及びこれに基づく文書に違反した職員及びその監督責任者は、その重大性、発生した事象の状況等に応じて、懲戒処分の対象となる。

12.2　再発防止の指導等

職員等に情報セキュリティポリシー及びこれに基づく文書に違反する行為がみられた場合には、課長は、速やかに次の措置を講じなければならない。

12.2.1　再発防止の指導その他適切な措置

当該職員等に対して違反する行為の事実を通知し、再発防止の指導その他適切な措置を行う。

12.2.2　使用権の停止・剥奪

指導等によっても改善されない場合、当該職員等の情報資産の使用権を停止あるいは剥奪する。

12.2.3　報告

違反する行為が生じた場合、違反する行為の内容、指導内容その他措置の状況について常務理事に報告する。

13　評価・改善・見直し

13.1　監査

13.1.1　実施方法

総務課長は、情報セキュリティ対策状況について、必要に応じて監査を行わせなければならない。

13.1.2　監査実施計画の策定

総務課長は、監査を行うに当たって、監査実施計画を策定しなければならない。

13.1.3　監査結果の報告

総務課長は、監査を実施した場合は、当該監査結果を取りまとめ、常務理事に報告しなければならない。

13.1.4　監査調書等の保管

総務課長は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適切に保管しなければならない。

13.1.5　指摘事項への対処

常務理事は、監査結果を踏まえ、指摘事項に関係する課長に対し、当該事項への対処を指示しなければならない。

13.1.6　監査結果の活用

常務理事は、情報セキュリティポリシー等情報セキュリティ対策の見直し時に監査結果を活用しなければならない。

13.2　自己点検

13.2.1　実施方法

ア　課長は、所管するネットワーク及び情報システムの情報セキュリティ対策状況について、定期的及び必要に応じて自己点検を実施しなければならない。

イ　課長は、所管する所属の情報セキュリティ対策状況について、定期的及び必要に応じて自己点検を行わなければならない。

13.2.2　自己点検結果等の報告

課長は、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、常務理事に報告しなければならない。

13.2.3　自己点検結果の活用

ア　職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

イ　常務理事は、情報セキュリティポリシー等情報セキュリティ対策の見直し時に点検結果を活用しなければならない。

13.3　改善

13.3.1　是正措置

課長は、業務上発見された問題、外部から指摘された問題、監査及び自己点検において指摘された問題等に対する再発防止のため、その原因を除去するための措置を施さなければならない。

13.3.2　予防措置

課長は、業務上予見される問題、他の機関で発生したものと同種の情報セキュリティ事件・事故、監査及び自己点検において指摘されうる問題等の発生を未然に防止するため、その原因を除去するための措置を施さなければならない。

13.3　情報セキュリティポリシーの見直し

常務理事は、監査及び自己点検の結果、改善の状況、残留リスク、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、情報セキュリティポリシー等情報セキュリティ関連文書の見直しを行う。