参考

○久留米市情報セキュリティ規則

令和４年１月１１日
久留米市規則第２号

久留米市情報セキュリティ規則（平成１５年久留米市規則第５０号）の全部を改正する。

（目的）

第１条　この規則は、情報セキュリティ確保のための体制及び方策に係る基本的な事項を定めることにより、本市が保有する情報資産の機密性、完全性及び可用性の維持を図り、もって本市の行政サービスを安全かつ効率的に提供することを目的とする。

（定義）

第２条　この規則において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(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、その構成機器（ハードウェア及びソフトウェア）をいう。

(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。

(3)　情報資産　本市の保有する次に掲げるものをいう。ただし、地方教育行政の組織及び運営に関する法律（昭和３１年法律第１６２号）第３０条に基づき本市に設置された教育機関において教育の用に供するものを除く。

ア　ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

イ　ネットワーク及び情報システムで取り扱う情報

ウ　情報システムの仕様書、ネットワーク図等のシステム関連文書

(4)　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。

(5)　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。

(6)　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。

(7)　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。

(8)　情報セキュリティポリシー　この規則及び第４条第１項の情報セキュリティ対策基準の総称をいう。

（想定する脅威）

第３条　情報資産の機密性、完全性及び可用性を維持するため、次に掲げる脅威を想定し、情報セキュリティに関するあらゆる方策を実施する。

(1)　不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃、部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

(2)　情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

(3)　地震、落雷、火災等の災害によるサービス及び業務の停止等

(4)　要員不足に伴うシステム運用の機能不全等

(5)　電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

（規範）

第４条　情報セキュリティに関する方策は、この規則を最上位の規範とし、具体的な遵守事項及び判断基準等を定めた情報セキュリティ対策基準（以下「情報セキュリティ対策基準」という。）並びに情報セキュリティ対策基準を実施するための具体的な手順を定めた情報セキュリティ実施手順（以下「情報セキュリティ実施手順」という。）に基づき実施するものとする。

２　情報セキュリティ実施手順は、公にすることにより本市の行政運営に重大な支障を及ぼすおそれがあることから、非公開とする。

（職員の遵守義務）

第５条　本市に勤務する全ての職員は、情報セキュリティの重要性を理解し、業務の遂行に当たっては、情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

２　職員は、職務の遂行において使用する情報資産を保護するため、次に掲げる法令のほか関係法令を遵守し、これに従わなければならない。

(1)　地方公務員法（昭和２５年法律第２６１号）

(2)　著作権法（昭和４５年法律第４８号）

(3)　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）

(4)　個人情報の保護に関する法律（平成１５年法律第５７号）

(5)　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）

(6)　サイバーセキュリティ基本法（平成２６年法律第１０４号）

(7)　久留米市個人情報の保護に関する法律施行条例(令和5年久留米市条例第1号)

（令5規則11・一部改正）

（組織体制）

第６条　本市における情報セキュリティの確保を推進する全庁的な組織体制を確立するため、次の各号に掲げる職を置き、当該各号に定める職にある者をもって充てる。

(1)　最高情報セキュリティ責任者　総務部を担当する副市長

(2)　統括情報セキュリティ責任者　情報政策を担当する部長

(3)　情報セキュリティ責任者　次のアからキまでに掲げる部門の区分ごとに当該アからキまでに定める者

ア　久留米市行政組織条例（昭和４３年久留米市条例第４６号）第２条に規定する部及び室　各部長及び秘書室長

イ　会計室　会計管理者

ウ　久留米市企業局　上下水道部長

エ　執行機関として法律に定めるところにより本市に置かれる委員会（この号オに掲げるものを除く。）若しくは委員の事務局又は委員会の管理に属する事務を掌る機関　各事務局長及び機関

オ　教育委員会　教育部長

カ　議会に置かれる事務局　事務局長

キ　久留米市総合支所設置条例（平成１６年久留米市条例第４３号）別表左欄に掲げる各総合支所　各支所長

(4)　情報セキュリティ管理者　前号アからキまでに掲げる部局室等に組織される課及び室（以下「課等」という。）ごとに当該課等の長

(5)　情報システム管理者　情報システムを所管する課等ごとに当該課等の長

(6)　情報システム担当者　情報システムを所管する課等ごとに当該課等の担当者

（最高情報セキュリティ責任者）

第７条　最高情報セキュリティ責任者（以下「CISO」という。）は、本市における情報セキュリティ確保のためのあらゆる方策に関し、最終決定権限及び責任を有する。

（最高情報セキュリティ副責任者の指名）

第８条　CISOは、必要に応じ、CISOの命を受けてその事務の一部を総括整理し、CISOのつかさどる職務を助ける者として、最高情報セキュリティ副責任者（以下「副CISO」という。）を１人指名することができる。

（統括情報セキュリティ責任者）

第９条　統括情報セキュリティ責任者は、CISO及び副CISOを補佐し、次に掲げる事項について統括的権限及び責任を有する。

(1)　本市の全てのネットワークの開発、設定の変更、運用、見直し等

(2)　本市における情報セキュリティ対策の実施状況の監督、見直し等

(3)　情報セキュリティインシデントが発生した場合（セキュリティ侵害が発生するおそれがある場合を含む。以下同じ。）における措置の実施等

(4)　情報セキュリティポリシー及び情報セキュリティ実施手順の遵守状況の監督、行動規範の違反への対応等

(5)　その他本市における情報セキュリティ全般に関する助言、指導、指示等

（情報セキュリティ責任者）

第１０条　情報セキュリティ責任者は、次に掲げる事項について、その所管する部局室等における統括的権限及び責任を有する。

(1)　その所管する部局室等における情報システムの開発、設定の変更、運用、見直し等

(2)　その所管する部局室等における情報セキュリティ対策の実施状況の監督、見直し等

(3)　その所管する部局室等において情報セキュリティインシデントが発生した場合における措置の実施等

(4)　その所管する部局室等における情報セキュリティポリシー及び情報セキュリティ実施手順の遵守状況の監督、行動規範の違反への対応等

(5)　その他その所管する部局室等における情報セキュリティに関する助言、指導、指示等

（情報セキュリティ管理者）

第１１条　情報セキュリティ管理者は、次に掲げる事項について、その所管する課等における権限及び責任を有する。

(1)　その所管する課等における情報セキュリティ対策の実施、見直し等

(2)　その所管する課等において情報セキュリティインシデントが発生した場合における措置の実施等

(3)　その所管する課等における情報セキュリティポリシー及び情報セキュリティ実施手順を遵守した情報セキュリティの実施、行動規範の違反への対応等

（情報システム管理者）

第１２条　情報システム管理者は、次に掲げる事項について、その所管する情報システムにおける権限及び責任を有する。

(1)　その所管する情報システムの開発、設定の変更、運用、見直し等

(2)　その所管する情報システムに関する情報セキュリティ実施手順の策定

(3)　その所管する情報システムにおける情報セキュリティ対策の実施、見直し等

(4)　その所管する情報システムにおいてセキュリティ侵害が発生し、又は発生するおそれがある場合における措置の実施等

(5)　その所管する情報システムにおける情報セキュリティポリシー及び情報セキュリティ実施手順を遵守した情報セキュリティの実施、行動規範の違反への対応等

（情報システム担当者）

第１３条　情報システム担当者は、情報システム管理者の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う。

（情報セキュリティ対策）

第１４条　脅威から情報資産を保護するため、次の各号に掲げる区分に応じ当該各号に定める情報セキュリティ対策を行うものとする。

(1)　情報資産の分類と管理　本市の保有する情報資産を、その重要性及び事故等が起きた場合の影響範囲に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

(2)　情報システム全体の強靭性の向上　情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、対策を講じる。

(3)　物理的セキュリティ　サーバ、情報システム室、通信回線及び職員のパソコン等の管理について、物理的な対策を講じる。

(4)　人的セキュリティ　情報セキュリティに関し、職員が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

(5)　技術的セキュリティ　コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

(6)　運用　情報システムの監視、情報セキュリティポリシー及び情報セキュリティ実施手順の遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティ

の運用面の対策を講じるとともに、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

(7)　業務委託と外部サービスの利用　業務委託、外部サービスの利用、ソーシャルメディアサービスの利用等の場合には、必要なセキュリティ対策を講じる。

（緊急時の連絡及び報告体制）

第１５条　統括情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、CISO、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者及び情報システム担当者間の緊急連絡網を整備しなければならない。

２　情報セキュリティ責任者は、緊急時等に必要な情報を報告させるため、その所管する部局室等における緊急時の報告体制を整備しなければならない。

（CSIRTの設置）

第１６条　情報システムに対するサイバー攻撃等の情報セキュリティインシデントが発生した場合において、当該情報セキュリティインシデントの把握及び分析を正確に行い、被害の拡大防止、復旧、再発防止等を迅速かつ的確に行うため、情報セキュリティインシデント対応チーム（以下「CSIRT」という。）を置く。

２　CSIRTの体制及び役割については、別に定める。

（情報セキュリティに関する監査等）

第１７条　情報セキュリティポリシー、情報セキュリティ実施手順その他の情報セキュリティに関する遵守状況を検証するため、定期的又は必要に応じ、監査及び自己点検を実施するものとする。

２　情報セキュリティに関するあらゆる方策においては、最新の情報に注意を払い、適宜、適切な見直しを行い、常に情報セキュリティの適正な運用の確保に努めなければならない。

（補則）

第１８条　この規則に定めるもののほか必要な事項は、別に定める。

附　則

この規則は、令和４年４月１日から施行する。

附　則(令和５年３月３１日規則第１１号)

この規則は、令和５年４月１日から施行する。