那須塩原市情報セキュリティ規則（令和８年３月９日規則第10号）

最終改正:

改正内容:令和8年3月9日規則第10号［令和8年4月1日］

〇那須塩原市情報セキュリティ規則

令和8年3月9日規則第10号

那須塩原市情報セキュリティ規則

（趣旨）

第１条　この規則は、地方自治法（昭和22年法律第67号）第244条の6第1項の趣旨にのっとり、市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ため、市が実施する情報セキュリティ対策に関し必要な事項を定めるものとする。

（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）実施機関　市長、教育委員会、選挙管理委員会、公平委員会、監査委員、農業委員会、固定資産評価審査委員会及び議会をいう。

（2）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並びにその構成機器であるハードウェア及びソフトウェアをいう。

（3）プログラム　コンピュータを機能させて一つの結果を得ることができるようにこれに対する指令を組み合わせたものをいう。

（4）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、情報を処理する仕組みをいう。

（5）情報資産　次に掲げるものをいう。

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（これらを印刷した文書を含む。）

ウ　情報システムの仕様書、ネットワーク図その他のシステム関連文書

（6）職員　次に掲げる本市の職員をいう。

ア　地方公務員法（昭和25年法律第261号。以下「法」という。）第3条第2項に規定する一般職の職員

イ　法第3条第3項に規定する特別職の職員

（7）部長等　那須塩原市庁議等規則（平成17年那須塩原市規則第8号。以下「庁議等規則」という。）第3条第1号に定める部長等をいう。

（8）課長等　庁議等規則第3条第2号に定める課長等をいう。

（9）機密性　情報にアクセスすることを認められた者のみが当該情報にアクセスできる状態をいう。

（10）完全性　情報が破壊され、改ざんされ、又は消去されていない状態をいう。

（11）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、当該情報にアクセスできる状態をいう。

（12）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。

（13）外部委託事業者等　情報システムの構築、開発、保守又は運用管理その他の情報資産に関する業務を受託する外部事業者若しくは指定管理者又は当該外部事業者若しくは指定管理者の従業者その他の情報資産を取り扱う者をいう。

（14）外部委託　外部委託事業者等に情報資産に関する業務を委託することをいう。

（15）情報セキュリティポリシー　この規則及び第19条に規定する情報セキュリティ対策基準をいう。

（16）マイナンバー利用事務系　個人番号利用事務（社会保障、地方税又は防災に関する事務をいう。）、戸籍事務等に関する情報システム及びデータをいう。

（17）LGWAN接続系　総合行政ネットワーク（Local Ｇｏvernment Wide Area Network）に接続された情報システム及びその情報システムで取り扱うデータ（マイナンバー利用事務系に係るものを除く。）をいう。

（18）インターネット接続系　インターネットメール、ホームページ管理システム等に関するインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

（19）無害化通信　インターネットメール本文のテキスト化、端末への画面転送等により、コンピュータウィルス等の不正プログラムの付着がない等、安全が確保された通信をいう。

（情報セキュリティ対策の対象とする脅威）

第３条　情報セキュリティ対策の対象とする脅威は、次に掲げるものとする。

（1）不正アクセス、ウイルス攻撃及びサービス不能攻撃等のサイバー攻撃並びに部外者の侵入、内部不正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、詐取等

（2）職員又は外部委託事業者等の非意図的要因による情報資産の無断持出し、無許可ソフトウェアの使用その他の内部不正

（3）プログラムの設計、開発及びメンテナンスの不備

（4）外部委託の管理及び情報セキュリティに関する職員によるマネジメントの不備

（5）機器故障その他の非意図的要因による情報資産の漏えい、破壊及び消去

（6）地震、落雷、火災その他の災害による情報システム運用の機能不全

（7）大規模及び広範囲にわたる疾病による要員不足に伴う情報システム運用の機能不全

（8）電力供給の途絶、通信の途絶その他の障害からの影響

（9）その他市が保有する情報資産に影響を与える脅威

（適用範囲）

第４条　この規則は、実施機関及びその保有する全ての情報資産に適用する。

（職員の責務）

第５条　職員は、情報セキュリティの重要性について共通の認識を持ち、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第20条に定める情報セキュリティ実施手順を遵守しなければならない。

（外部委託事業者等に対する措置）

第６条　実施機関は、外部委託事業者等に情報資産を取り扱わせる場合には、情報セキュリティポリシーを遵守させるための必要な措置を講ずるものとする。

（情報セキュリティ対策）

第７条　市長は、市が保有する情報資産の管理及び運用に当たり、次に掲げる情報セキュリティ対策を講ずるものとする。

（１）　情報セキュリティに対応する全庁的な組織体制の確立

（２）　情報資産の重要度に応じた区分の設定及びその区分に応じた管理の徹底

（３）　情報システム全体に対し、次に掲げる情報システムの区分に応じ、それぞれに定める対策

ア　マイナンバー利用事務系　原則として、マイナンバー利用事務系の情報システムとこれ以外の情報システムとの通信ができないようにした上で、端末からの情報の持出しができない設定、端末への多要素認証の導入等により、住民情報の流出を防ぐこと。

イ　LGWAN接続系　LGWAN接続系の情報システムとインターネット接続系の情報システムとの間における通信環境を分離した上で、安全が確保された通信のみを許可できるようにすること。この場合において、両情報システム間で通信する場合には、無害化通信を実施すること。

ウ　インターネット接続系　不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施すること。

（４）　情報システムを設置する施設への不正な立入りの禁止及び情報資産の損傷の防止その他の物理的な侵害からの保護

（５）　職員及び外部委託事業者等に対する情報セキュリティに関する教育及び啓発

（６）　情報システムの誤操作、不正操作、不正アクセス等からの情報資産の保護

（７）　情報セキュリティの監視及び例外措置の適用

（８）　クラウドサービスその他の外部サービスの適正な利用

（最高情報セキュリティ責任者）

第８条　市の全て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を有する責任者としてChief Information Security Officer（最高情報セキュリティ責任者をいう。以下「CISO」という。）を置く。

２　CISOは、企画部に関する事務を所掌する副市長をもって充てる。

３　CISOは、市の情報セキュリティに関する事務についてCISOを補佐し、CISOの命を受けて本市の情報セキュリティに関する事務を統括するDeputy Chief Information Security Officer（最高情報セキュリティ副責任者をいう。以下「DISO」という。）を一人任命することができる。

（各実施機関の代表者）

第９条　各実施機関（市長を除く。以下この条及び次条において同じ。）の代表者は、情報セキュリティポリシーを遵守し、その所管する情報資産及び情報セキュリティを管理しなければならない。

２　各実施機関の代表者は、CISO及びDISOとの連携を密にし、第12条第１項に規定する各実施機関の情報セキュリティ責任者とともに、情報セキュリティ対策を推進しなければならない。

（統括情報セキュリティ責任者）

第10条　CISO及びDISOを補佐するため、統括情報セキュリティ責任者（以下「統括責任者」という。）を置く。

２　統括責任者は、企画部長をもって充てる。

３　統括責任者は、市の全ての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。

４　統括責任者は、市の情報資産に対する情報セキュリティインシデントが発生し、又はそのおそれがある場合において、CISO又はDISOの指示に従うとともに、CISO及びDISO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。

５　統括責任者は、市の共通的なネットワーク、情報システム及び情報資産に関する情報セキュリティ実施手順の維持及び管理を行う権限及び責任を有する。

６　統括責任者は、情報セキュリティインシデントが発生したときは、直ちにCISO及びDISOに報告を行うとともに、情報資産の回復のための対策を講じなければならない。

７　統括責任者は、第12条第１項に規定するセキュリティ責任者、第13条第１項に規定するセキュリティ管理者に対して、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。

８　統括責任者は、情報セキュリティインシデント発生時等の円滑な情報共有を図るため、CISO、DISO、統括責任者、次条第１項に規定する統括管理者、第12条第１項に規定するセキュリティ責任者及び第13条第１項に規定するセキュリティ管理者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。この場合において、各実施機関の代表者に対しても必要に応じて適切に情報の共有が図ることができるよう、各実施機関のセキュリティ責任者に対し連絡体制の構築を求めなければならない。

９　統括責任者は、情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時把握し、必要に応じてCISO及びDISOにその内容を報告しなければならない。

10　統括責任者は、情報セキュリティ監査に関する計画の策定、その実施及び結果の承認について権限及び責任を有する。

（統括情報セキュリティ管理者）

第11条　情報セキュリティ及び情報システムに関する専門的な観点から統括責任者を補佐する者として、統括情報セキュリティ管理者（以下「統括管理者」という。）を置く。

２　統括管理者は、企画部デジタル推進課長をもって充てる。

３　統括管理者は、市のセキュリティ対策の実施状況を取りまとめなければならない。

４　統括管理者は、市のネットワーク及び情報システムの適正な管理及び運営を取りまとめなければならない。

５　統括管理者は、職員に対しセキュリティ教育を実施しなければならない。

６　統括管理者は、情報セキュリティインシデント等に関する情報を収集し、必要に応じて関係する組織に周知しなければならない。

（情報セキュリティ責任者）

第12条　各実施機関の部及び事務局（会計課を含む。以下「部局等」という。）におけるセキュリティ対策を実施する者として情報セキュリティ責任者（以下「セキュリティ責任者」という。）を置き、部長等及び会計管理者をもって充てる。

２　セキュリティ責任者は、その所掌する部局等の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。

3　セキュリティ責任者は、その所掌する部局等において所管している情報システムの導入、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。
4　セキュリティ責任者は、所掌する部局等において所有している情報システムについて、情報セキュリティインシデント発生時等における連絡体制の整備並びに職員に対し、情報セキュリティに関する教育、訓練、助言及び指示を行うものとする。
（情報セキュリティ管理者）
第13条　セキュリティ責任者を補佐する者として課長等を情報セキュリティ管理者（以下「セキュリティ管理者」という。）とする。ただし、施設にあっては施設長をセキュリティ管理者とする。
2　セキュリティ管理者は、その所掌する課、室又は施設（以下「課等」という。）におけるセキュリティ対策に関する権限及び責任を有する。
3　セキュリティ管理者は、その所管する情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。
4　セキュリティ管理者は、その所管する情報システムにおける情報セキュリティに関する権限及び責任を有する。
5　セキュリティ管理者は、その所管する情報システムに係る情報セキュリティ実施手順の維持管理を行う。
6　セキュリティ管理者は、その所掌する課等において使用している情報システムについて、情報セキュリティインシデント発生時等における連絡体制を整備する。
7　セキュリティ管理者は、その所掌する課等において、情報資産に対する情報セキュリティインシデントが発生し、又はそのおそれがある場合には、速やかにCISO、DISO、統括責任者、統括管理者及びセキュリティ責任者に報告を行い、指示を仰がなければならない。
（情報セキュリティタスクフォースの設置）
第14条　市の情報セキュリティに関する重要事項を協議し、総合的な調整を行うため、情報セキュリティタスクフォース（以下「対策本部」という。）を設置する。
2　対策本部には、本部長、副本部長を置き、部長等及び会計管理者をもって組織する。
3　本部長はCISOが兼ねるものとし、副本部長は本部長が指名する。
4　本部長は、対策本部を統括し、会議の結果を市長へ報告する。
5　本部長に事故があるとき、又は本部長が欠けたときは、副本部長がその職務を代理する。
6　対策本部の庶務は、企画部デジタル推進課が行う。
（兼務の禁止）
第15条　情報セキュリティ対策の実施において、特にやむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。
2　第17条の情報セキュリティ監査を受ける者とその監査を実施する者は、特にやむを得ない場合を除き、同じ者が兼務してはならない。
（CSIRTの整備）
第16条　CISOは、セキュリティ侵害に対処するための体制（Computer Security Incident Response Team。以下「CSIRT」という。）を整備し、その役割を明確化するものとする。
2　CSIRTの体制及び役割は、CISOが定める。
（情報セキュリティ監査及び自己点検）
第17条　市長は、情報セキュリティポリシーが遵守されていることを検証するため、情報セキュリティ監査を実施するとともに、職員に自己点検を行わせるものとする。
（情報セキュリティポリシーの改訂）
第18条　市長は、情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合又は情報セキュリティに関する状況の変化に対応するため新たに対策が必要となった場合には、情報セキュリティポリシーを改訂する。
（情報セキュリティ対策基準の策定）
第19条　市長は、この規則に定めるもののほか、情報セキュリティ対策を実施するために、具体的な遵守事項、判断基準等を定める情報セキュリティ対策基準を策定する。
2　情報セキュリティ対策基準は、非公開とする。
（情報セキュリティ実施手順の策定）
第20条　市長は、情報セキュリティ対策基準に基づき、情報セキュリティ対策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を策定する。
2　情報セキュリティ実施手順は、非公開とする。
（その他）
第21条　この規則に定めるもののほか、情報セキュリティに関し必要な事項は、実施機関が定める。

附　則

この規則は、令和8年4月1日から施行する。