序章　那珂市情報セキュリティポリシー

那珂市が取り扱う情報資産には、住民の財産、プライバシー等の個人情報を始め、行政サービスの継続的かつ安全･安定的な運営上重要な情報など､部外に漏洩等した場合、極めて重大な結果を招く情報が多数含まれている。

これらを人的脅威や災害、事故等から防御し、情報資産の機密性、完全性及び可用性（注）を維持するための対策として那珂市情報セキュリティポリシーを定める。

構成は、情報セキュリティ対策に関する統一的かつ基本的な方針の部分である「情報セキュリティ基本方針」と、基本方針を実行に移すための全ての情報資産に共通の対策の部分としての「情報セキュリティ対策基準」の２階層から成り、総合的、体系的かつ具体的に取りまとめるものである。

これにより情報セキュリティ対策を講じるための体制を確立し､那珂市の情報資産を取り扱う全ての職員等に浸透、定着させるものである。

また、これに基づき、情報システム毎に、具体的な情報セキュリティ対策の実施手順として「情報セキュリティ実施手順」を策定することとする。

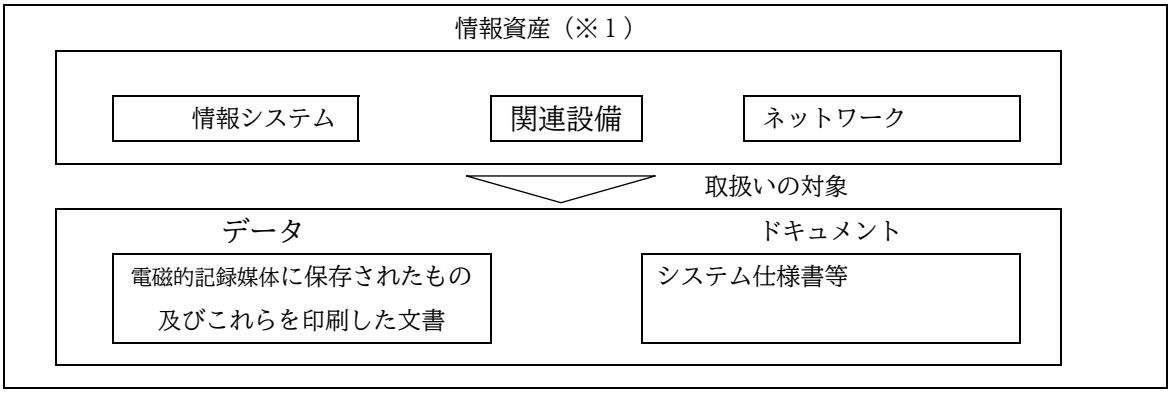
情報資産:情報システム(電子計算機器等及びネットワーク)及びそれが取り扱う情報(電磁的記録媒体に保存されたもの及びこれらを印刷した文書を含む)

（注)：国際標準化機構（ISO）が定めるもの（ISO 7498－2：1989)

機密性（confidentiality)：情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。

完全性（integrity)　：情報及び処理の方法の正確さ及び完全である状態を完全防護すること。

可用性（availability)：許可された利用者が必要なときに情報にアクセスできることを確実にすること。



第１章　情報セキュリティ基本方針

ここでは那珂市の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定める。

１　定義

○電子計算機器等

ハードウェア及びソフトウェアで構成するコンピュータ(クライアントコンピュータ及びサーバ)をいう。

○電磁的記録媒体

サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体と、ＵＳＢメモリ、外付けハードディスクドライブ、ＤＶＤ－Ｒ、磁気テープ等の外部電磁的記録媒体をいう。

○情報センター

那珂市情報センター。ネットワークにより使用する各種サーバを設置する部屋をいう。

○ネットワーク

電子計算機器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。

○情報システム

電子計算機器等で構成され、情報処理を行う仕組みをいう。

○ドキュメント

情報システムの仕様書及びネットワーク図等のシステム関連文書（入出力帳票、システム設計書、ネットワーク仕様書、プログラム仕様書、取扱い説明書等ネットワーク及び情報システムに必要な仕様書類）をいう。

○データ

情報システムで取扱う情報（これらを印刷した文書及び電磁的記録媒体に記録されている情報）をいう。

○情報資産

本基本方針が対象とする情報資産は、次のとおりとする。

①ネットワーク、情報システム、これらに関する設備、電磁的記録媒体

②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)

③情報システムの仕様書及びネットワーク図等のシステム関連文書

○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。

○個人情報

個人に関する情報（事業を営む個人の当該事業に関する情報及び法人その他の団体に関して記録された情報に含まれる当該法人その他の団体の役員に関する情報を除く。）であって、特定の個人が識別され、または他の情報と照合することにより識別され得るものをいう。

○マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

○LGWAN 接続系

LGWAN 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（マイナンバー利用事務系を除く。）。

○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わ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。

○通信経路の分割

LGWAN 接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

○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をいう。

2　情報セキュリティポリシーの位置付け

情報セキュリティポリシーは、本市の情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の最高位に位置するものである。

3　情報セキュリティポリシーの対象範囲

情報セキュリティポリシーの対象範囲は、本市における情報資産に接する許可を受けた全ての者(以下「職員等」という。）とする。

4　職員等の義務

職員等は、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、情報資産の利用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　情報セキュリティ管理体制

本市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・管理するための体制を確立するものとする。

6　情報資産の分類

情報資産をその重要度に応じて分類し、それに応じたセキュリティ対策を行うものとする。

7　情報資産への脅威

情報セキュリティポリシーを講ずるうえで、情報資産に対する脅威の発生度合いや発生した場合の影響を考慮するものとする。

特に認識すべき脅威は以下のとおりである。

(1)　権限外者による故意の不正アクセスまたは不正操作によるデータやプログラムの持出・盗聴・改ざん・消去、機器及び電磁的記録媒体の盗難等
(2)　職員等及び外部委託者による意図しない操作、故意の不正アクセスまたは不正操作によるデータやプログラムの持出・盗聴・改ざん・消去、機器及び電磁的記録媒体の盗難、規定外の情報システムの機器操作によるデータ漏洩等
(3)　地震、落雷、火災等の災害や事故、故障等によるサービス及び業務の停止等
(4)　大規模・広範囲にわたる疾病による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障害からの波及等

８　情報セキュリティ対策

本市の情報資産を上記７の脅威から保護するため、以下の情報セキュリティ対策を講ずるものとする。

(1)　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、次の三段階の対策を講じる。

ア　マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や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。

イ　LGWAN 接続系においては、LGWAN と接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

ウ　インターネット接続系においては、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。高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

(2)　人的セキュリティ対策

職員等の情報セキュリティに関する権限や責任等を定めるとともに、全ての職員等に情報セキュリティポリシーの内容を周知徹底するため、教育・訓練を行う。

(3)　物理的セキュリティ対策

情報システムを設置する施設等への不正な立入り、情報資産への損傷・妨害等から保護するため、物理的な対策を講ずる。

(4)　技術的セキュリティ対策

情報資産を不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、不正プログラム対策等を実施する。

(5)　運用におけるセキュリティ対策

情報セキュリティポリシーの実効性を確保するため、また、不正アクセスされること及び不正アクセスによって他の情報処理システムに対して被害を及ぼすことを防ぐため、ネットワークの監視、セキュリティポリシーの遵守状況確認等の必要な措置を講ずる。また、障害及び緊急事態が発生した際の迅速な対応を可能とするための対策を講ずる。

９　情報セキュリティ対策基準の策定

本市の情報資産について、上記８の情報セキュリティ対策を講ずるに当たっては、職員等が遵守すべき事項及び判断等の基準を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を行ううえで必要となる基本的な要件を明記した情報 セキュリティ対策基準を策定するものとする。

１０　情報セキュリティ実施手順の策定

情報セキュリティ対策を確実に実施していくためには、個々の情報資産に関する対策の手順を具体的に定めておく必要があることから、情報セキュリティ対策基準に基づき、情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ実施手順は、公開することにより本市の行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

１１　評価・見直し

情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価、情報システムの変更、新たな脅威等情報セキュリティを取り巻く状況の変化を踏まえ、適宜情報セキュリティ対策基準及び情報セキュリティ実施手順の見直しを実施するものとする。

第２章　　情報セキュリティ対策基準

情報セキュリティ対策基準とは、情報セキュリティ基本方針を実行に移すための、那珂市の情報資産に関する情報セキュリティ対策の基準を定めたものである。

１　組織体制

情報セキュリティの管理については、以下の体制とする。

(1)　最高情報セキュリティ責任者（CISO： Chief Information Security Officer、以下「CISO」という）

ア　副市長をCISOとする。

イ　CISOは、那珂市における全てのネットワーク、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。

ウ　CISO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。

エ　CISOは、情報セキュリティインシデントに対処するための体制（CSIRT：Computer Security Incident Response Team、以下「CSIRT」という。）を整備し、役割を明確化する。

(2)　統括情報セキュリティ責任者

ア　情報政策担当部長をCISO直属の統括情報セキュリティ責任者とする。

イ　統括情報セキュリティ責任者は、CISOを補佐しなければならない。

ウ　統括情報セキュリティ責任者は、那珂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。

エ　統括情報セキュリティ責任者は、那珂市の全ての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。

オ　統括情報セキュリティ責任者は、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。

カ　統括情報セキュリティ責任者は、那珂市の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恐れがある場合に、CISOの指示に従い、CISOが不在の場合には自らの判断に基づき、必要且つ十分な措置を行う権限及び責任を有する。

キ　統括情報セキュリティ責任者は、那珂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セキュリティ実施手順の維持・管理を行う権限及び責任を有する。

ク　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、情報システム担当者等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。

ケ　統括情報セキュリティ責任者は、緊急時にはCISOに早急に報告を行うとともに、回復のための対策を講じなければならない。

コ　統括情報セキュリティ責任者は、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に把握し、必要に応じてCISOにその内容を報告しなければならない。

(3)　情報セキュリティ責任者

ア　各部長、会計管理者、議会事務局長、農業委員会事務局長、消防長を情報セキュリティ責任者とする。

イ　情報セキュリティ責任者は、それぞれ所管する情報資産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。

ウ　情報セキュリティ責任者は、その所管する情報資産に係る情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。

エ　情報セキュリティ責任者は、その所管する情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約及び職員等に対する教育、訓練、助言及び指示を行う。

(4)　情報セキュリティ管理者

ア　各課長、出先機関の施設長、会計課課長補佐（総括)、議会事務局次長、農業委員会事務局局長補佐（総括）を情報セキュリティ管理者とする。

イ　情報セキュリティ管理者は、所管する組織内における情報セキュリティ対策に関する権限と責任を有する。

ウ　情報セキュリティ管理者は、所属する課室等において、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のある場合には、情報セキュリティ責任者、統括情報セキュリティ責任者及びCISOへ速やかに報告を行い、指示を仰がなければならない。

エ　情報セキュリティ管理者は、ウに掲げる者がいずれも不在の場合には、自らの判断に基づき必要かつ充分な措置を行う権限及び責任を有する。

(5)　情報システム管理者

ア　各情報システムを所管する課の課室長を当該情報システムに関する情報システム管理者とする。

イ　情報システム管理者は、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と責任を有する。

ウ　情報システム管理者は、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と責任を有する。

エ　情報システム管理者は、所管する情報システムにおける情報セキュリティ実施手順の維持・管理を行う。

(6)　情報システム担当者

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者を、情報システム担当者とする

(7)　情報化リーダー

情報化リーダーは、システムの有効活用と職員等の技能向上及びセキュリティ意識の啓発に関することを行う。

(8) 那珂市情報化推進委員会

ア 情報セキュリティ対策を統一的に行うため、那珂市情報化推進委員会において、情報セキュリティポリシー等、情報セキュリティに関する重要事項を決定する。

イ 那珂市情報化推進委員会は、毎年度、那珂市における情報セキュリティ対策の改善計画を策定し、その実施状況を確認しなければならない。

(9) 兼務の禁止

ア 情報セキュリティ対策の実施において、やむを得ない場合を除き、承認また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。

イ 監査を受ける者とその監査を実施する者は、やむを得ない場合を除き、同じ者が兼務してはならない。

(10) CSIRT の設置・役割

ア CISO は、CSIRT を整備し、その役割を明確化しなければならない。

イ CISO は、CSIRT に所属する職員等を選任し、その中から CSIRT 責任者を置かなければならない。また、CSIRT 内の業務統括及び外部との連携等を行う職員等を定めなければならない。

ウ CISO は、情報セキュリティの統一的な窓口を整備し、情報セキュリティインシデントについて部局等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備しなければならない。

エ CISO による情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等に提供しなければならない。

オ 情報セキュリティインシデントを認知した場合には、CISO、総務省、都道府県等へ報告しなければならない。

カ 情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘案し、報道機関への通知・公表対応を行わなければならない。

キ 情報セキュリティに関して、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わなければならない。

２ データの分類と管理

(1) データの分類

対象となるすべてのデータは、次の重要性分類に従って分類する。

ア 重要性分類Ⅰ

・個人情報の保護に関する法律（平成 15 年法律第 57 号）第２条第１項に規定する個人情報

・行政手続における特定の個人を識別する番号の利用等に関する法律（平成 25 年法律第 27 号。以下「番号法」という。）第２条第８項に規定する特定個人情報

・那珂市情報公開条例第７条に規定する不開示情報

・所管する情報システムに係るパスワード及びシステム設定情報

イ　重要性分類Ⅱ

・外部に公開する情報のうち、行政事務の執行上重要なデータ。

・滅失し、またはき損した場合、その復元が著しく困難となり、行政の円滑な執行を妨げる恐れのあるデータ。

ウ　重要性分類Ⅲ

・上記以外のデータ。

(2)　データの管理方法

ア　データの管理及び取扱い

（ア）　データの重要性分類に従い、パスワード等によるアクセス制限及び暗号等による通信内容の秘匿を行わなければならない。

（イ）　重要性分類Ⅰ・Ⅱのデータの複製や、送付・送信は行ってはならない。ただし、情報セキュリティ管理者の許可を得たものについてはその限りではない。

イ　電磁的記録媒体の管理

（ア）　重要性分類Ⅰ・Ⅱのデータを記録した取り外し可能な電磁的記録媒体は、外部からの脅威にさらされないよう施錠ができるなど特に安全な場所に保管しなければならない。また、保管状況等を記録しなければならない。

（イ）　重要性分類Ⅰ・Ⅱのデータを記録した電磁的記録媒体を送る場合は、職員等または守秘義務を明記した契約を締結した外部業者に行わせるとともに、電磁的記録媒体の物理的な保護措置を講じなければならない。

ウ　電磁的記録媒体の処分

（ア）　電磁的記録媒体が磨耗等により不要となった場合は、当該媒体に記録されている重要性分類Ⅰ・Ⅱのデータをいかなる方法によっても復元できないように処置を行った上で廃棄しなければならない。

（イ）　重要性分類Ⅰ・Ⅱのデータを記録した電磁的記録媒体の廃棄は、情報セキュリティ管理者の許可を得ることとし、廃棄を行った日時、担当者及び処理内容を記録しなければならない。

(3)　データの公開と提供

ア　重要性分類Ⅱ以上のデータを外部へ提供・公開してはならない。ただし、情報セキュリティ管理者の許可を得たもの、または、法令で提供・公開を定められたものに関してはこの限りではない。

イ　情報セキュリティ管理者は、データを外部へ提供する場合、データの重要性分類に応じて、暗号化、パスワードの設定等の適切な保護措置を取らなくてはならない。

ウ　情報セキュリティ管理者はデータを外部へ公開する場合は、改ざん等を防止しデータの完全性を確保しなければならない。

３　情報システム全体の強靭性の向上

(1)　マイナンバー利用事務系

ア　マイナンバー利用事務系と他の領域との分離

マイナンバー利用事務系と他の領域を通信できないようにしなければならない。マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定

（MAC アドレス、IP アドレス）及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。また、その外部接続先についてもインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、インターネット等から LGWAN-ASP を経由してマイナンバー利用事務系にデータの取り込みを可能とする。

イ　情報のアクセス及び持ち出しにおける対策

（ア）　情報のアクセス対策

情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を併用する認証（多要素認証）を利用しなければならない。

（イ）　情報の持ち出し不可設定

原則として、USB メモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。

(2)　LGWAN 接続系

ア　LGWAN 接続系とインターネット接続系の分割

LGWAN 接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータを LGWAN 接続系に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。

（ア）　インターネット環境で受信したインターネットメールの本文のみを LGWAN 接続系に転送するメールテキスト化方式

（イ）　インターネット接続系の端末から、LGWAN 接続系の端末へ画面を転送する方式

（ウ）　危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式

(3)　インターネット接続系

ア　インターネット接続系においては、通信パケットの監視、ふるまい検知等の不正通信の監視機能の強化により、情報セキュリティインシデントの早期発見と対処及び LGWAN への不適切なアクセス等の監視等の情報セキュリティ対策を講じなければならない。

イ　都道府県及び市区町村のインターネットとの通信を集約する自治体情報セキュリティクラウドに参加するとともに、関係省庁や都道府県等と連携しながら、情報セキュリティ対策を推進しなければならない。

４　人的セキュリティ

(1)　職員等の遵守事項

ア　情報セキュリティポリシー等の遵守

職員等は、情報セキュリティポリシー及び実施手順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等がある場合は、速やかに情報セキュリティ管理者に相談し、指示を仰がなければならない。

イ　業務以外の目的での使用の禁止

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、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ってはならない。

ウ　モバイル端末や電磁的記録媒体等の持出し及び外部における情報処理作業の制限

（ア） CISO は、重要性分類Ⅰ・Ⅱの情報資産を外部で処理する場合における安全管理措置を定めなければならない。

（イ） 職員等は、本市のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持出す場合には、情報セキュリティ管理者の許可を得なければならない。

（ウ） 職員等は、外部で情報処理業務を行う場合には、情報セキュリティ管理者の許可を得なければならない。

エ　支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

（ア） 職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、業務上必要な場合は、実施手順に従い情報セキュリティ管理者の許可を得て利用することができる。

（イ） 職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合には、情報セキュリティ管理者の許可を得た上で、情報処理作業を行う際の安全管理措置を遵守しなければならない。

オ　持ち出し及び持ち込みの記録

情報セキュリティ管理者は､端末等の持ち出し及び持ち込みについて､記録を作成し､保管しなければならない。

カ　パソコンやモバイル端末におけるセキュリティ設定変更の禁止

職員等は、パソコンやモバイル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情報セキュリティ管理者の許可なく変更してはならない。

キ　机上の端末等の管理

職員等は、パソコン、モバイル端末、電磁的記録媒体及び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情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、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。

ク　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。

(2)　非常勤及び臨時的任用職員への対応

ア　情報セキュリティポリシー等の遵守

情報セキュリティ管理者は、非常勤及び臨時的任用職員（以下「非常勤職員等」という。）に対し、採用時に情報セキュリティポリシー等のうち、非常勤職員等が守るべき内容を理解させ、また実施及び遵守させなければならない。

イ　情報セキュリティポリシー等の遵守に対する同意

情報セキュリティ管理者は、非常勤職員等の採用の際、必要に応じ、情報セキュリテ

ィポリシー等を遵守する旨の同意書への署名を求めるものとする。

ウ　インターネット接続及び電子メール使用等の制限

情報セキュリティ管理者は、非常勤職員等にパソコンやモバイル端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

(3)　情報セキュリティポリシー等の掲示

情報セキュリティ管理者は、職員等が常に情報セキュリティポリシー及び実施手順を閲覧できるように掲示しなければならない。

(4)　外部委託事業者に対する説明

情報セキュリティ管理者は、ネットワーク及び情報システムの開発・保守等を外部委託事業者に発注する場合、外部委託事業者から再委託を受ける事業者も含めて、情報セキュリティポリシー等のうち外部委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

(5)　研修・訓練

ア　情報セキュリティに関する研修・訓練

CISO は、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

イ　研修計画の策定及び実施

（ア）　CISO は、幹部を含め全ての職員等に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行い、那珂市情報化推進委員会の承認を得なければならない。

（イ）　研修計画において、職員等は毎年度最低 1 回は情報セキュリティ研修を受講できるようにしなければならない。

（ウ）　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。

（エ）　研修は、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、情報システム担当者及びその他職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

（オ）　情報セキュリティ管理者は、所管する課室等の研修の実施状況を把握しなければならない。

（カ）　CISO は、毎年度 1 回、那珂市情報化推進委員会に対して、職員等の情報セキュリティ研修の実施状況について報告しなければならない。

(6)　緊急時対応訓練

CISO は、緊急時対応を想定した訓練を定期的に実施しなければならない。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、訓練実施の体制、範囲等を定め、また、効果的に実施できるようにしなければならない。

(7)　研修・訓練への参加

幹部を含めた全ての職員等は、定められた研修・訓練に参加しなければならない。

(8)　ID の取扱い

職員等は、自己の管理する ID に関し、次の事項を遵守しなければならない。

ア　自己が利用しているIDは、他人に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。

(9)　パスワードの取扱い

職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

ア　パスワードは、他者に知られないように管理しなければならない。
イ　パスワードを秘密にし、パスワードの照会等には一切応じてはならない。
ウ　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にしなければならない。
エ　パスワードが流出したおそれがある場合には、情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更しなければならない。
オ　複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。
カ　仮のパスワード（初期パスワード含む）は、最初のログイン時点で変更しなければならない。
キ　サーバ、ネットワーク機器及びパソコン等の端末にパスワードを記憶させてはならない。
ク　職員等間でパスワードを共有してはならない（ただし、共有IDに対するパスワードは除く。）。

(10)　接続時間の制限

職員等は、所管する情報システムへの接続については、必要最小限の接続時間で行うように努めるものとする。

(11)　情報セキュリティインシデントの報告

ア　庁内からの情報セキュリティインシデントの報告

（ア）　職員等は、情報セキュリティインシデントを認知した場合、速やかに情報セキュリティ管理者及び情報セキュリティに関する統一的な窓口に報告しなければならない。
（イ）　報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。
（ウ）　情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、CISO及び情報セキュリティ責任者に報告しなければならない。

イ　住民等外部からの情報セキュリティインシデントの報告

（ア）　職員等は、本市が管理するネットワーク及び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、住民等外部から報告を受けた場合、情報セキュリティ管理者に報告しなければならない。
（イ）　報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。
（ウ）　情報セキュリティ管理者は、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CISO及び情報セキュリティ責任者に報告しなければならない。
（エ）　CISOは、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、住民等外部から報告を受けるための窓口を設置し、当該窓口への連

絡手段を公表しなければならない。

ウ　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

（ア）　統括情報セキュリティ責任者は、情報セキュリティインシデントを引き起こした部門の情報セキュリティ管理者、情報システム管理者及び情報セキュリティに関する統一的な窓口と連携し、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明結果から、再発防止策を検討し、CISO に報告しなければならない。

（イ）　CISO は、統括情報セキュリティ責任者から、情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

５　物理的セキュリティ

(1)　サーバ等の管理

ア　機器の取付け

情報システム管理者は、サーバ等の機器の取付けを行う場合、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正に固定する等、必要な措置を講じなければならない。

イ　機器の電源

（ア）　情報システム管理者は、施設管理部門と連携し、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、当該機器が適正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なければならない。

（イ）　情報システム管理者は、施設管理部門と連携し、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じなければならない。

ウ　通信ケーブル等の配線

（ア）　情報システム管理者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルが損傷等を受けないよう可能な限り必要な措置を施さなければならない。

（イ）　主要な箇所の配線は、損傷等についての定期的な点検を行わなければならない。

エ　機器の定期保守及び修理

（ア）　情報システム管理者は、重要情報を格納しているサーバ等の機器の定期保守を実施しなければならない。

（イ）　情報システム管理者は、電磁的記録媒体を内蔵する機器を外部の事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、情報システム管理者は、外部の事業者に故障を修理させるにあたり、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ほか、秘密保持体制の確認等を行わなければならない。

オ　庁外への機器の設置

情報システム管理者は、庁外にサーバ等の機器を設置する場合、CISO の承認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。

カ　機器の廃棄等

情報システム管理者は、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、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

(2)　管理区域（情報センター等）の管理

ア　管理区域（情報センター等）の管理

（ア）　管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理及び運用を行うための部屋（那珂市情報センター）や電磁的記録媒体の保管庫をいう。

（イ）　情報システム管理者は、管理区域を外部からの侵入が容易にできないようにしなければならない。

イ　管理区域の入退室管理等

（ア）　情報システム管理者は、管理区域への入退室を許可された者のみに制限し、入退室管理簿の記載による入退室管理を行わなければならない。

（イ）　職員等及び外部委託事業者は、管理区域に入室する場合、身分証明書及び入出証を携帯し、求めにより提示しなければならない。

ウ　機器の搬入出

（ア）　情報システム管理者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員又は委託した業者に確認を行わせなければならない。

（イ）　情報システム管理者は、情報センターの機器等の搬入出について、職員を立ち会わせなければならない。

(3)　通信回線及び通信回線装置の管理

ア　情報システム管理者は、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さなければならない。

イ　情報システム管理者は、行政系のネットワークを総合行政ネットワーク(LGWAN)に集約するように努めなければならない。

ウ　情報システム管理者は、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、適正な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

エ　情報システム管理者は、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しなければならない。

オ　情報システム管理者は、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しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

(4)　職員等の利用する端末や電磁的記録媒体等の管理

ア　情報システム管理者は、盗難防止のため、執務室等で利用するパソコン等のワイヤーによる固定など、施錠管理等の物理的措置を講じなければならない。電磁的記録媒体については、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しなければならない。

イ　情報システム管理者は、マイナンバー利用事務系では「知識」、「所持」、「存在」を利用する認証手段のうち二つ以上を併用する認証（多要素認証）を行うよう設定しなければならない。

6　技術的セキュリティ

(1)　所管する情報システムの管理

ア　所管する情報システム管理記録の作成と管理

情報システム管理者及び情報システム担当者は、所管する情報システムにおいて行ったシステムの変更作業を記録し、適切に管理しなければならない。

イ　所管する情報システム仕様書の管理

（ア）　情報システム管理者及び情報システム担当者は、所管する情報システムの仕様書を最新の状態にしなければならない。また、システムの仕様変更等の処理を行った場合は、その記録を作成しなければならない。

（イ）　情報システム管理者及び情報システム担当者は、所管する情報システムの仕様書を業務上必要とする者のみが閲覧できる場所に保管しなければならない。

ウ　アクセス記録の取得

情報システム管理者及び情報システム担当者は、所管する情報システムのアクセス記録及びセキュリティ関連障害に関する記録を取得し、窃取、改ざんまたは消去されないよう に必要な措置を講じたうえ、一定の期間保存しなければならない。また、可能な範囲で分析しなければならない。

エ　障害記録の作成

情報システム管理者及び情報システム担当者は、可能な範囲で障害記録を作成し、一定の期間保存しなければならない。

オ　バックアップの取得

情報システム管理者及び情報システム担当者は、所管する情報システムの重要性分類Ⅰ・Ⅱのデータについては、定期的に外部電磁的記録媒体へのバックアップを取り、施錠等のできる安全な場所へ保管しなければならない。

カ　ソフトウェアの交換

職員等間で、所管する情報システムに関するソフトウェア等を交換する場合は、情報システム管理者の許可を得るとともに、著作権等に配慮しなければならない。

キ　ソフトウェアの導入に関する注意

（ア）　職員等は、新たにソフトウェアを導入する場合は、情報システム管理者の許可を得なければならない。

（イ）　職員等は、正規のライセンスのないソフトウェアを導入してはならない。

（ウ）　職員等は、業務上不必要なソフトウェア及び安全性が確認されないソフトウェアをインストールしてはならない。

（エ　)職員等は、導入されているソフトウェアを適切に運用管理しなければならない。

ク　メールの送受信等

（ア）　職員等は、メールの自動転送機能を用いて、業務上不必要な者へ職場のメールを転送してはならない。

（イ） 職員等は、チェーンメールや不審なメールを他者に転送してはならない。
（ウ） 職員等は、重要性分類Ⅱのデータに該当する添付ファイルのあるメールを送信する必要がある場合には、事前に情報セキュリティ管理者の承認を受けなければならない。
（エ） 職員等は、差出人が不明な、または不自然なファイルが添付されたメールを受信した場合は、直ちに廃棄しなければならない。

ケ　暗号化

（ア） 暗号化については、統括情報セキュリティ責任者が定める方法を用いなければならない。
（イ） 暗号のための鍵は、重要性分類Ⅰのデータとして厳重に管理しなければならない。

コ　職員等以外の者が利用できる情報システム

統括情報セキュリティ責任者は、所管する情報システムのうち職員等以外の者が利用できるものについては、情報セキュリティ対策について特に強固な対策を取らなければならない。

サ　情報システムの入出力データ

（ア） 情報システム管理者及び情報システム担当者は、所管する情報システムに入力されるデータの適切なチェック等を行い、それが正確であることを確実にするための対策を施さなければならない。
（イ） 情報システム管理者及び情報システム担当者は、所管する情報システムから出力されるデータの処理が正しく行われていることを確認しなければならない。

シ　業務目的以外の使用の禁止

職員等は、業務目的以外での情報システムへのアクセス及びメールの使用を行ってはならない。

(2)情報システムアクセス制御

ア　利用者登録

（ア） 情報システム管理者及び情報システム担当者は、所管する情報システムの利用者の登録、変更、抹消等については、所管する情報システム毎に定められた方法に従って行わなければならない。
（イ） 利用者登録、変更等は、情報システム管理者に対する申請により行わなければならない。
（ウ） 利用者に付加される情報システム及びデータへのアクセス権限は業務内容等を勘案し必要最低限のものとしなければならない。

イ　インターネット以外のネットワークへのアクセス制御

情報システム管理者及び情報システム担当者は、所管する情報システムのネットワークにアクセスできる者を定め、それ以外の者がアクセスできないよう措置を講じなければならない。

ウ　外部からのアクセス

外部からのアクセスの許可は、必要最低限にしなければならない。

エ　外部ネットワークとの接続

（ア） 情報システム管理者及び情報システム担当者は、外部ネットワークとの接続に際しては、当該外部ネットワークのネットワーク構成、機器構成及び情報セキュリティレベル等を詳細に検討し、那珂市の情報資産に影響が生じないことを明確に確認したうえで、統括情報セキュリティ責任者の許可に基づき接続しなければならない。

（イ） 情報システム管理者及び情報システム担当者は、外部ネットワークとの接続を行うことで内部ネットワークの安全性が脅かされることの無いようにセキュリティ対策に努めなければならない。

（ウ） 情報システム管理者及び情報システム担当者は、接続した外部ネットワークの情報セキュリティに問題が認められた場合、または内部ネットワークの情報セキュリティに問 題が認められた場合には、速やかに当該内部ネットワークを外部ネットワークから物理的に遮断しなければならない。

オ　パスワード等の管理

（ア） 情報システム管理者及び情報システム担当者は、情報機器の ID、パスワードを厳重に管理しなければならない。

（イ） 統括情報セキュリティ責任者は、ネットワーク並びにネットワーク上で利用する各種サービスの ID、パスワードを適切に管理しなければならない。

(3) 情報システムの開発・導入・保守

ア　情報システムの開発・導入

（ア） 情報システム管理者及び情報システム担当者は、所管する情報システムのソフトウェアを開発・導入する場合は、情報セキュリティ上問題にならないかどうか、確認しなければならない。

（イ） 情報システム管理者及び情報システム担当者は、所管する情報システムのソフトウェアを開発する場合は、ソフトウェアの仕様書、ネットワーク構成図等を整備しなければならない。

（ウ） 情報システム管理者及び情報システム担当者は、開発したソフトウェアを既に稼動している所管する情報システムに導入する場合は、接続する前に十分な試験を行わなければならない。

イ　情報システムの変更管理

情報システム管理者及び情報システム担当者は、重要なシステムを追加、変更、廃棄等した場合は、その際の設定・構成等の履歴を記録・保存し、必要な場合には復旧できるようにしなければならない。

ウ　ソフトウェアの保守及び更新

（ア） 情報システム管理者及び情報システム担当者は、情報セキュリティに重大な影響を及ぼすソフトウェアについては、適切な保守が行われるようにし、その不具合については、 速やかに修正等の対応を行わなければならない。

（イ） 統括情報セキュリティ責任者は、所管する情報システムのソフトウェアの更新等については、計画的に実施しなければならない。

エ　機器の修理及び廃棄

（ア） 職員等は、電磁的記録媒体の含まれる機器を外部の業者に修理させる場合、ま

たは貸借期限終了等により廃棄もしくは返却する場合、可能な範囲でバックアップを取り、電磁的記録媒体内のすべてのデータを消去しなければならない。

（イ） 職員等は、故障を外部の業者に修理させる際、データを消去することが難しい場合は、修理を委託する業者と守秘義務を明記した契約を締結しなければならない。

オ　機器構成の変更

（ア） 職員等は、情報システムの機器について改造または機器の増設・交換を行ってはならない。

（イ） 職員等は、情報システムの機器について業務を遂行するため機器の増設・交換を行う必要がある場合には、当該情報システムの情報システム管理者の許可を得なければならない。

（ウ） 職員等は、他のネットワークへ接続を行う場合及び他のネットワークからアクセスを可能とする仕組みを構築する場合には、当該情報システムの情報システム管理者の許可を得なければならない。情報システム管理者及び情報システム担当者は、許可に当たって所管する情報システム及び他の情報システムにセキュリティ上の問題を生じさせてはならない。

(4)　不正プログラム対策

ア　情報システム管理者、情報システム担当者は所管する情報システムのサーバ及び必要な機器に 不正プログラム対策ソフトを導入しなければならない。

イ　情報システム管理者、情報システム担当者は不正プログラムチェック用のパターンファイルを常に最 新のものに保たなければならない。

ウ　情報システム管理者、情報システム担当者は定期的に新種の不正プログラムに関する情報収集や所管する情報システム内部の感染状況等について情報収集しなければならない。

エ　情報システム管理者、情報システム担当者は不正プログラム情報について、職員等に対する注意喚起を行なわなければならない。

オ　情報システム管理者、情報システム担当者は不正プログラムについて、職員等に対して必要な啓発活動を行わなければならない。

カ　職員等は、外部からデータまたはソフトウェアを取り入れる場合及び外部に持ち出す場合に必ず不正プログラムのチェックを行わなければならない。

キ　職員等は、添付ファイルのあるメールを送受信する場合は不正プログラムのチェックを行わなければならない。

ク　職員等は、情報システム管理者及び情報システム担当者が提供する不正プログラム情報を常に確認しなければならない。

(5)　不正アクセス対策

ア　情報システム管理者及び情報システム担当者は、所管する情報システムのセキュリティホール等の情報収集に努め、メーカー等から修正プログラムの提供があり次第、速やかに対応するとともに、その修正履歴を記録・保存しなければならない。

イ　情報システム管理者及び情報システム担当者は、所管する情報システムに不正な侵入や利用が あった場合に探知等できるよう、適切な対策に努めなければならない。

ウ　職員等により内部ネットワーク及び外部ネットワークに対して不正なアクセスがあった場合は、関係する情報システムを所管する情報セキュリティ責任者または情報システム管理者は当該職員等が属する課等の長に通知し、適切な処置を求めなければならない。

エ　職員等は、外部ネットワークより不正アクセスがあった場合は、情報システム管理者に報告し、適切な措置を講じなければならない。

(6)　セキュリティ情報の収集

ア　情報システム管理者及び情報システム担当者は、重要なシステムの設定に係るファイル等について、定期的に当該ファイルの改ざんの有無を検査しなければならない。

イ　統括情報セキュリティ責任者は、セキュリティに関する情報について、国及び関係団体、民間事業者等から適宜情報を収集しなければならない。

7　運用

(1)　情報システムの監視

情報システム管理者及び情報システム担当者は、所管する情報システムの運用にあたっては、常に情報システムを監視するとともに情報セキュリティ障害に対して注意を払わなければならない。

(2)　情報セキュリティポリシーの遵守状況の確認

統括情報セキュリティ責任者及び情報セキュリティ管理者、那珂市情報化推進委員会は、情報セキュリティポリシーの遵守状況について、また、運用上支障が生じていないかについて確認を行わなければならない。

(3)　侵害時の対応等

ア　緊急時対応計画の策定

CISO 又は那珂市情報化推進委員会は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により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発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適切に対処しなければならない。

イ　緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

（ア）　関係者の連絡先

（イ）　発生した事案に係る報告すべき事項

（ウ）　発生した事案への対応措置

（エ）　再発防止措置の策定

ウ　業務継続計画との整合性確保

自然災害、大規模・広範囲にわたる疾病等に備えて別途業務継続計画を策定し、那珂市情報化推進委員会は当該計画と情報セキュリティポリシーの整合性を確保しなければならない。

エ　緊急時対応計画の見直し

CISO 又は那珂市情報化推進委員会は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

８　例外措置

(1)　例外措置の許可

情報セキュリティ管理者及び情報システム担当者は、情報セキュリティ関係規定を遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し又は遵守事項を実施しないことについて合理的な理由がある場合にはCISOの許可を得て、例外措置を取ることができる。

(2)　緊急時の例外措置

情報セキュリティ管理者及び情報システム担当者は、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避の時は、事後速やかにCISOに報告しなくてはならない。

(3)　例外措置の申請書の管理

CISOは、例外措置の申請書及び審査結果を適切に保管し、定期的に申請状況を確認しなければならない。

９　法令等の遵守

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、次の法令のほか関係法令を遵守し、これに従わなければならない。

- 地方公務員法（昭和 25 年法律第 261 号）
- 著作権法（昭和 45 年法律第 48 号）
- 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）
- 個人情報の保護に関する法律（平成 15 年法律第 57 号）
- 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）

１０　懲戒処分等

(1)　懲戒処分

情報セキュリティポリシーに違反した職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて地方公務員法による懲戒処分等の対象とする。

(2)　違反時の対応

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には、速やかに次の措置を講じなければならない。

ア　統括情報セキュリティ責任者が違反を確認した場合は、統括情報セキュリティ責任者は当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適切な措置を求めなければならない。

イ　情報システム管理者等が違反を確認した場合は、違反を確認した者は速やかに統括情報セキュリティ責任者及び当該職員等が所属する課室等の情報セキュリティ管理者

に通知し、適切な措置を求めなければならない。

ウ　情報セキュリティ管理者の指導によっても改善されない場合、統括情報セキュリティ責任者は、当該職員等のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、統括情報セキュリティ責任者は、職員等の権利を停止あるいは剥奪した旨をCISO及び当該職員等が所属する課室等の情報セキュリティ管理者に通知しなければならない。

１１　外部サービスの利用

(1)　外部委託

ア　外部委託事業者の選定基準

（ア）　情報セキュリティ管理者は、外部委託事業者の選定にあたり、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しなければならない。

（イ）　情報セキュリティ管理者は、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参考にして、事業者を選定しなければならない。

（ウ）　情報セキュリティ管理者は、クラウドサービスを利用する場合は、取り扱う情報の重要度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。

（エ）　情報セキュリティ管理者は、クラウドサービスを利用して重要性分類Ⅱ以上のデータを取り扱う場合は、該当サービスのデータセンターを日本国内に設置し、国内法の適用される事業者を選定しなくてはならない。

イ　契約項目

情報システムの運用、保守等を外部委託する場合には、外部委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

- 那珂市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
- 外部委託事業者の責任者、委託内容、作業者、作業場所の特定
- 提供されるサービスレベルの保証
- 外部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
- 外部委託事業者の従業員に対する教育の実施
- 提供された情報の目的外利用及び受託者以外の者への提供の禁止
- 業務上知り得た情報の守秘義務
- 再委託に関する制限事項の遵守
- 委託業務終了時の情報資産の返還、廃棄等
- 委託業務の定期報告及び緊急時報告義務
- 市による監査、検査
- 市による情報セキュリティインシデント発生時の公表
- 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)

ウ　確認・措置等

（ア）　情報セキュリティ管理者は、外部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定期的に確認し、前項の契約に基づき措置しなければならない。また、その内容を統括情報セキュリティ責任者に報告するとともに、その重要度に応じてCISOに報告しなければならない。

また、ネットワークを利用する外部委託業務については情報主管課長に報告しなければならない。

（イ） 統括情報セキュリティ責任者並びに情報主管課長は、委託業務の内容について検討し、情報セキュリティ上の問題があると判断した場合は、情報セキュリティ管理者に対し問題の是正を求めるものとする。

(2) 約款による外部サービスの利用

ア 約款による外部サービスの利用に係る規定の整備

情報セキュリティ管理者は、以下を含む約款による外部サービスの利用に関する規定を整備しなければならない。また、当該サービスの利用において、重要性分類Ⅱ以上の情報が取扱われないように規定しなければならない。

（ア） 約款によるサービスを利用してよい範囲

（イ） 業務により利用する約款による外部サービス

（ウ） 利用手続及び運用手順

イ 約款による外部サービスの利用における対策の実施

職員等は、利用するサービスの約款、その他提供条件から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適切な措置を講じた上で利用しなければならない。

(3) ソーシャルメディアサービスの利用

ア 情報セキュリティ管理者は、本市が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

（ア） 本市のアカウントによる情報発信が、実際の本市のものであることを明らかにするために、本市の自己管理ウェブサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を行うこと。

（イ） パスワードや認証のためのコード等の認証情報を適切に管理するなどの方法で、不正アクセス対策を行うこと

イ 重要性分類Ⅱ以上の情報はソーシャルメディアサービスで発信してはならない。

ウ 利用するソーシャルメディアサービスごとの責任者を定めなければならない。

１２ 評価・見直し等

(1) 自己点検

ア 実施方法

（ア） 統括情報セキュリティ責任者及び情報システム管理者は、所管するネットワーク及び情報システムについて、毎年度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） 情報セキュリティ責任者は、情報セキュリティ管理者と連携して、所管する部局

における情報セキュリティポリシーに沿った情報セキュリティ対策状況について、毎年度及び必要に応じて自己点検を行わなければならない。

イ　報告

統括情報セキュリティ責任者、情報システム管理者及び情報セキュリティ責任者は、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、那珂市情報化推進委員会に報告しなければならない。

ウ　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）　那珂市情報化推進委員会は、この点検結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

(2)　監査

ア　実施方法

CISO は、情報セキュリティ監査統括責任者を指名し、ネットワーク及び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、毎年度及び必要に応じて監査を行わせなければならない。

イ　監査を行う者の要件

（ア）　情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

ウ　監査実施計画の立案及び実施への協力

（ア）　情報セキュリティ監査統括責任者は、監査を行うにあたって、監査実行計画を立案し、那珂市情報化推進委員会の承認を得なければならない。

（イ）　被監査部門は、監査の実施に協力しなければならない。

エ　外部委託事業者に対する監査

（ア）　情報セキュリティ監査統括責任者は、監査を行うにあたって、監査実行計画を立案し、那珂市情報化推進委員会の承認を得なければならない。

（イ）　被監査部門は、監査の実施に協力しなければならない。

オ　報告

情報セキュリティ監査統括責任者は、監査結果を取りまとめ、那珂市情報化推進委員会に報告する。

カ　保管

情報セキュリティ監査統括責任者は、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。

キ　監査結果への対応

CISO は、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し当該事項への対処を指示しなければならない。また、指摘事項を所管していない情報セキュリティ管理者に対しても、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なければならない。

ク　情報セキュリティポリシー及び関係規程等の見直し等への活用

那珂市情報化推進委員会は、監査結果を情報セキュリティポリシー及び関係規定等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

(4)　情報セキュリティポリシー等の見直し

那珂市情報化推進委員会は、情報セキュリティ監査及び各部署の自主点検の結果、並びに情報セキュリティ環境の変化等を踏まえ、情報セキュリティポリシー等について毎年度評価を行い、必要があると認めた場合には改善を行うものとする。

【改定】
・平成１５年９月策定
・平成２８年３月７日一部改定
・令和６年３月１８日一部改定