○国立市情報セキュリティに関する規則

平成18年３月23日規則第５号

改正

令和２年３月25日規則第18号

令和５年３月22日規則第13号

令和８年３月23日規則第14号

国立市情報セキュリティに関する規則

前文

近年の情報技術の目覚しい進展は、情報流通の高速化とネットワーク化によって、国際的ボーダレス化とともに社会構造をも変える勢いになっている。

ＩＴの進展は、社会に大きな恩恵をもたらし、今後の社会発展にとってなくてはならないものとなっている。しかし一方、技術の進化は、情報の流出やデータ改ざんの可能性も同時に広げることになり、新たに深刻な社会問題にもなっている。

地方自治体の使命は、第一義に住民の生命、財産を守ることにある。その目的のために、自治体では、常にあらゆる部署で実に多様な住民の個人情報を保有し、活用している。その個人情報も紙情報である限り、管理責任の範囲は明確であったが、いったん情報が電子化されることでネットワーク化が可能となれば、管理の範囲がボーダレス化して自治体の管理の範疇（ちゅう）を超えてしまうことになる。このことは、自治体にとって、サービス提供のために必要な個人情報等の情報資産が、正当な使われ方がされず、漏えい等の危険が高まり、逆に住民の生命、財産を脅かすことになりかねないことをも意味する。しかも、電子情報としてネットワーク化することにより、情報は拡散し、修復が極めて困難になるおそれがある。昨今、個人情報の流出事件が多発しており、そのときの情報量は莫大で被害も甚大となっている。

このような、電子情報の流出を見ると、２つの要因がある。１つは、外部からの侵入によるものである。日常的な技術革新は、世界規模でのコンピュータウィルスの蔓延やサイバー犯罪の増加等を招き、セキュリティに万全はないに等しい。２つ目は、内部による、意図的漏えいと無意識、怠慢による人為的ミスである。このような事態を発生させないために、継続的なチェックシステムと継続的な職員の意識改革が不可欠である。

このように、電子自治体への移行やＩＴ社会は、住民にとっても利便性をもたらし、今後も一層進展していくであろう。しかし、ＩＴの進歩は目覚ましく、万全を期したセキュリティ対策も、それをもって終了とはならない。常にセキュリティが破られることを認識したリスク管理と、継続的なセキュリティ体制の見直しが重要である。

以上のことを認識した上で、国立市は、住民の生命、財産につながる個人情報等の情報資産、行政運営上重要な情報を守るため、情報資産のリスク管理の規範となるべき国立市情報セキュリティポリシーを定める。この情報セキュリティポリシーは、基本方針となる本規則及び国立市情報セキュリティ対策基準で構成し、市の情報資産を扱うすべての者の情報セキュリティに対する意識の向上を図り、情報資産を取り扱う個人の裁量で情報セキュリティが判断されることのないよう統一的な基準を定めるものである。このことにより、国立市は、国立市の情報管理システム及び職員の意識が、常に高いセキュリティ水準で維持できるよう努めるものとする。

（目的）

第１条　この規則は、国立市（以下「市」という。）の情報資産を取り巻く物理的及び人的な脅威等に対し、情報セキュリティを確保するため、基本的な考え方及び統一的な方策について定め、市の情報資産を取り扱うすべての者がこれを理解し、遵守することにより、市民からの情報資産に対する継続的な信頼を獲得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、それぞれ当該各号に定めるところによる。

（１）　情報　市が保有する電子データ及び書類等のすべての情報をいう。

（２）　情報システム　ネットワーク、ハードウェア、ソフトウェア及び記録媒体で構成され、市の業務を処理するための仕組みをいう。

（３）　情報資産　情報及び情報システムをいう。

（４）　ネットワーク　コンピュータを相互に接続するための通信網及びその構成機器をいう。

（５）　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。

（６）　機密性　情報にアクセスすることを許可された者のみアクセスでき

ることを確実にすることをいう。

（７） 完全性　情報及びその処理の方法が正確及び完全であることをいう。

（８） 可用性　許可された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をいう。

（９） 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。

(10) 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。）。

(11) 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。

(12) 職員　地方公務員法（昭和25年法律第261号。以下「法」という。）第３条に規定する一般職及び特別職の職員並びに法第22条の３第４項に規定する臨時的に任用する者であって、市が保有するすべての情報資産に関する業務に携わるすべてのものをいう。

(13) 受託者　市の事務事業の委託を受けた者及び当該業務に従事している者をいう。

（対象とする脅威）

第３条　情報資産に対する脅威として、次の脅威を想定し、情報セキュリティ対策を実施する。

（１） 不正アクセス、ウイルス攻撃、業務を不能とする攻撃等のサイバー攻撃、部外者の侵入その他の意図的な要因による情報資産の漏えい、破壊、改ざん又は消去、重要情報の詐取、内部不正等

（２） 情報資産の無断持ち出し、情報セキュリティ統括責任者の許可を受けていないソフトウェアの使用等の規定違反、設計又は開発の不備、プログラム上の欠陥、操作ミス又は設定ミス、情報システムの維持管理の不備、内部監査又は・外部監査の機能の不備、委託管理の不備、事業の遂行の管理の欠陥、機器の故障等の非意図的な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業務の停止等

（４） 大規模又は広範囲にわたる疾病による要員の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社会基盤の障害からの波及等

（適用範囲）

第４条　この規則の適用範囲は、次に掲げるとおりとする。

（１）　行政機関の範囲　この規則が適用される行政機関は、市長部局とする。

（２）　情報資産の範囲　市長が管理する次のアからウまでに定めるものその他すべての情報資産とする。

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及びネットワーク図等のシステム関連文書

（３）　対象者　前条第12号に規定する職員及び同条第13号に規定する受託者とする。

２　前項第３号に規定する職員及び受託者は、情報資産に係る業務に携わらなくなった後又は当該委託業務が完了した後も、適用範囲から外れるものではない。

（対策基準の策定）

第５条　この規則に基づき情報セキュリティ対策を実施するに当たり、遵守すべき事項及び判断等の統一的な基準として、国立市情報セキュリティ対策基準（以下「対策基準」という。）を定めるものとする。

（実施手順の策定）

第６条　この規則及び前条の対策基準に基づき、情報セキュリティ対策を具体的に実施するために、国立市情報セキュリティ実施手順（以下「実施手順」という。）を定めるものとする。

（情報セキュリティの管理体制）

第７条　情報セキュリティ対策を適切に管理推進するため、別に定めるところにより推進する全庁的な組織及び管理体制を確立する。

（職員及び受託者の義務）

第８条　職員及び受託者は、情報セキュリティの重要性について共通の認識

をもつとともに関係法令、条例及びこの規則等を遵守しなければならない。

（情報資産の評価及び管理）

第９条　情報セキュリティ管理者は、情報の機密性、完全性及び可用性等による情報資産の定期的評価を行い、その重要性に応じて分類し、適切な管理をしなければならない。

（情報セキュリティ対策）

第10条　情報資産を故意（盗聴、不正アクセス、改ざん、破壊、窃盗等）、過失（入力間違い、操作間違い等）、災害（火災、地震等）、故障等の脅威から守るため、次に掲げる対策を定める。

（１）　人的セキュリティ対策　情報セキュリティに関する権限や責任及び遵守すべき事項を定め、職員及び受託者に対する周知徹底を図るとともに、十分な教育・啓発を行うこと。

（２）　物理的セキュリティ対策　情報システムの設置場所及び情報の保管場所等への不正な立入り並びに情報資産への損害及び利用の妨害等から情報資産を保護すること。

（３）　技術的セキュリティ対策　情報資産を不正アクセス等から保護するため、情報資産へのアクセス制御及びネットワーク管理を行うこと。

（４）　運用等における対策　情報システムの監視及び情報セキュリティ対策の遵守状況の確認等を行うこと。

（５）　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て業務の効率性及び利便性の観点を踏まえ、情報システム全体をマイナンバー利用事務系、ＬＧＷＡＮ接続系及びインターネット接続系の３段階に区切り、それぞれの段階で適切な対策を講じる。

（６）　業務委託と外部サービス（クラウドサービス）の利用　業務委託を行う場合には、委託事業者を選定し、情報セキュリティの要件を明記した契約を締結し、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確認し、必要に応じて契約に基づき措置を講じる。

（７）　評価及び見直し　情報セキュリティポリシーの遵守状況を検証するため、定期的に又は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し、運用の改善を行うことにより、情報セキュリティの向上を図るとともに、情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

（８）　緊急時におけるセキュリティ対策　緊急事態が発生した場合に、迅速かつ適切な対応がとれるよう危機管理を行うこと。

（情報セキュリティ監査及び自己点検の実施）

第11条　内部監査責任者及び情報セキュリティ委員会は、この規則に基づく情報セキュリティ対策が適切に運用されているか検証するため、定期的に、又は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ものとする。

（評価及び見直し）

第12条　情報セキュリティ委員会は、前条の監査結果及び次に掲げる状況に基づき、この規則、対策基準及び実施手順に定める事項並びに情報セキュリティ対策について定期的に評価及び見直しを実施する。

（１）　社会環境の変化及び市民からの要請

（２）　情報セキュリティ対策技術の変化

（３）　市又は国若しくは他の地方公共団体の情報セキュリティ事故情報

（４）　市内部の環境の変化

（５）　関連法令及び条例等の改正

（文書及び記録の管理）

第13条　職員及び受託者は、この規則に定める情報セキュリティ対策を実施する上で必要な文書等を国立市文書管理規程（平成９年３月国立市規程第１号）又は受託に係る契約書により適切に管理しなければならない。

（違反者への対応）

第14条　この規則に基づく情報セキュリティ対策に違反した職員及び受託者の対応については、その重大性及び発生した事案の状況等に応じ、法令、条例、契約書等に定めるところによるものとする。

付　則

この規則は、平成18年４月１日から施行する。

付　則（令和２年３月25日規則第18号抄）

（施行期日）

１　この規則は、令和２年４月１日から施行する。

付　則（令和５年３月22日規則第13号抄）

（施行期日）

１　この規則は、令和５年４月１日から施行する。

付　則（令和８年３月23日規則第14号抄）

（施行期日）

１　この規則は、令和８年４月１日から施行する。