龍ケ崎市議会告示第２号

龍ケ崎市議会情報セキュリティ規程を次のように定める。

令和８年３月２７日

龍ケ崎市議会議長　後　藤　敦　志

龍ケ崎市議会情報セキュリティ規程

（目的）

第１条　この規程は、情報セキュリティに関する基本的な指針を定め、龍ケ崎市議会（以下「議会」という。）が管理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する。

（定義）

第２条　この規程において、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。

⑴　情報　職務の遂行に伴うコンピュータ及び記録媒体に記録されたデータをいう。

⑵　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。

⑶　情報システム　ハードウェア、ソフトウェア、ネットワークその他の電磁的記録媒体等で構成され、情報処理を行う仕組みをいう。

⑷　情報資産　情報、情報システム、行政情報を含む紙媒体、端末、アカウント、認証情報、設定情報、ログその他これらに付随する媒体及び記録をいう。

⑸　脅威　次に掲げるもので、議会が管理する情報資産に損失を与えるものをいう。

ア　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、改ざん及び消去、重要情報の詐取並びに内部不正等

イ　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、設計及び開発の不備、プログラム上の欠陥、操作及び設定ミス、メンテナンス不備、内部及び外部監査機能の不備、外部委託管理の不備、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

ウ　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

エ　大規模かつ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

オ　電力供給、通信及び水道供給の途絶等のインフラの障害からの波及等

⑹　情報セキュリティ　脅威から議会が管理する情報資産を保護し、次に定め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いう。

ア　機密性　情報資産にアクセスすることを認められた者だけが、これにアクセスできる状態をいう。

イ　完全性　情報資産が破壊、改ざん又は消去されていない状態をいう。

ウ　可用性　情報資産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、これにアクセスできる状態をいう。
⑺　情報セキュリティ対策　情報セキュリティを維持するための管理策をいう。
⑻　議員　龍ケ崎市議会議員をいう。
⑼　職員　龍ケ崎市議会事務局の職員をいう。
⑽　外部要員　議会と業務委託先の業者との社員派遣等契約に基づき、議会で作業する前号に掲げる職員以外の者をいう。

（適用範囲）

第３条　この規程を適用する対象者及び資産の範囲は、次のとおりとする。
⑴　対象者の範囲　議員、職員及び外部要員とする。
⑵　資産の範囲　議会が管理する全ての情報資産とする。

（議員及び職員の義務）

第４条　議員及び職員は、情報セキュリティの重要性について共通の認識を持ち、議会活動又は業務の遂行に当たってこの規程を遵守しなければならない。

（外部要員の管理）

第５条　外部要員を使用する職員は、契約等において、外部要員に対し前条に規定する義務と同様の義務を課し、適正に管理するものとする。

（情報の区分）

第６条　議会は、第８条の情報セキュリティ対策基準に基づき、その管理する情報資産を重要度に応じて区分し、当該区分に応じた次条の情報セキュリティ対策を講ずるものとする。

（情報セキュリティ対策）

第７条　議会は、議会が管理する情報資産を脅威から保護するため、次に掲げる情報セキュリティ対策を講ずるものとする。
⑴　情報システム全体の強靭性の向上　インターネットに接続する情報システム及び外部サービスにおける不正通信の監視機能の強化その他の高度な情報セキュリティ対策
⑵　物理的セキュリティ対策　サーバ等、情報システム室等、通信回線等及び議員に貸与する端末並びに職員が業務上使用する端末の管理について行う、物理的な対策
⑶　人的セキュリティ対策　情報セキュリティに関する議員、職員及び外部要員が遵守すべき事項の制定並びに十分な教育及び啓発その他の人的な対策
⑷　技術的セキュリティ対策　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
⑸　情報システム運用セキュリティ対策　情報システムに対する運用ミスや情報漏えい等から情報資産を保護するために必要な情報システムの運用、保守及び監視等に関する対策

⑹　ネットワークセキュリティ対策　ネットワーク障害、不正アクセス等から情報資産を保護するために必要なネットワークの可用性の確保及び監視等に関する対策

⑺　外部サービス利用対策　情報システムに関する業務を外部委託する場合に行う、次に掲げる対策

ア　情報セキュリティ対策要件を明文規定した契約を締結すること。

イ　必要に応じて契約に基づく措置を講じさせること。

ウ　相手方の契約約款による外部サービスを利用する場合に、別途利用に係る規定を整備し、必要なセキュリティ対策を講じさせること。

（情報セキュリティ対策基準）

第８条　議会は、想定される脅威に対応するため、議会における情報セキュリティ対策の統一基準となる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。

（情報セキュリティ実施手順）

第９条　議会は、前条の対策基準に従い、情報セキュリティ対策に関する手法、手順の詳細を規定した情報セキュリティ実施手順を策定するものとする。

（情報セキュリティの管理体制）

第10条　議会は、情報セキュリティ対策を推進し、管理するため、最高情報セキュリティ責任者及び情報セキュリティ管理者並びに情報セキュリティ委員会を置くものとする。

２　議会は、情報資産に関する事件及び事故に適切かつ迅速に対応するため、情報セキュリティ緊急対策会議を置くことができる。

（情報セキュリティ監査の実施）

第11条　議会は、第８条の対策基準の遵守状況等を検証するため、定期的に情報セキュリティ監査を実施するものとする。

（法令等の遵守）

第12条　第３条第１号に規定する対象者は、職務の遂行に際しては、関連法令等を遵守しなければならない。

（見直し）

第13条　議会は、第１１条の情報セキュリティ監査又は自己点検の結果その他情報セキュリティを取り巻く状況の変化を踏まえ、必要があると認めるときは、この規程を見直すものとする。

付　則

この告示は、公布の日から施行する。