宮城県議会における情報セキュリティ要領

（目的）

第１条　この要領は、「宮城県議会における情報セキュリティに関する基本方針」（以下「基本方針」という。）に基づき、宮城県議会（以下「県議会」という。）における情報セキュリティを確保するために、必要な事項を定めることを目的とする。

（定義）

第２条　この要領において、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)　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。

(2)　情報資産　宮城県議会事務局（以下「議会事務局」という。）が調達する電子計算機（印刷装置等の関連機器を含む。）及びこれに付随する基本ソフトウェア並びに情報システムが管理し、及び出力する情報（帳票及び記録媒体を含む。）並びに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）第２条第９項に規定する特定個人情報をいう。

(3)　議会ネットワーク　議会事務局が調達するルーター、無線アクセスポイントその他の通信機器により構成される県議会内における情報通信網（Ｗｉ―Ｆｉを含む。）をいう。

(4)　情報システム　宮城県議会議員（以下「議員」という。）が使用する業務システム及び議会ネットワーク並びに情報システムを適切に管理及び運用するために必要な仕組み及び取決めをいう。

(5)　タブレット端末等　議会事務局が調達するタブレット端末（業務上の必要に応じ、移動させて使用することを目的とした情報端末をいう。）、キーボード、マウス等をいう。

(6)　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。

(7)　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。

(8)　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。

(9)　不正アクセス　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）第２条第４項に規定する不正アクセス行為をいう。

(10)　不正プログラム　情報システムに対して不正かつ有害な動作を行う意図で作成されたプログラムをいう。

(11)　情報セキュリティポリシー　基本方針及びこの要領の総称をいう。

（適用範囲）

第３条　この要領は、議員が利用する情報資産に適用する。

（議員の遵守義務）

第４条　議員は、情報セキュリティの重要性について深く認識し、議会活動及び議員活動に当たっては、情報セキュリティポリシーを遵守しなければならない。

２　議員は、議会活動及び議員活動に必要な範囲で情報資産を利用するものとする。

（対象とする脅威）

第５条　情報資産に対する脅威は、次の各号に定めるところによる。

(1)　情報システムの不正利用、不正アクセス及び不正プログラムの感染

(2)　不正アクセス及び不正プログラムに対する情報システム及びタブレット端末等の脆弱性

(3)　自然災害、機器の故障、操作ミス又は故意による情報資産の滅失、き損又は漏えい

（情報セキュリティ対策の統括）

第６条　宮城県議会議長（以下「議長」という。）は、全議員の情報セキュリティ対策を統括する。

（会派責任者）
第７条　議長を補佐するため、各会派に、会派情報セキュリティ責任者（以下「会派責任者」という。）を置く。
２　会派責任者は、各会派の代表者をもって充てる。
３　会派責任者は、各会派の議員に対し、情報セキュリティの向上に関して必要な支援を行うものとする。

（情報資産の適正管理）
第８条　議員は、個人情報その他の県議会及び県において公にされていない情報（以下「個人情報等」という。）の取扱いに当たっては、個人情報等の流出等の防止に努めるとともに、他者へ公開してはならない。
２　議員は、情報資産の利用及び管理に当たっては、機密性、完全性及び可用性を確保するための適切な措置を講じなければならない。

（情報セキュリティ対策）
第９条　議員は、議会ネットワークに対して、タブレット端末等以外の端末機器を接続してはならない。
２　議員は、タブレット端末等が不正アクセスを感知した場合又は不正プログラムに感染した場合は、議会ネットワークから即時に切り離す等の必要な措置を講じなければならない。
３　議員は、情報セキュリティに関する事故の発生を防止するため、不審なウェブページへのアクセス、不審な電子メールの開封又は不審なリンクへのアクセスを控える等、不正アクセス及び不正プログラム感染への対策を行うものとする。

（研修）
第10条　議長は、情報リテラシー及び情報セキュリティ意識の向上を図るため、議員に対し情報セキュリティに関する研修を実施するものとする。

（情報セキュリティ監査又は自己点検）
第11条　議長は、議員における情報セキュリティポリシーの遵守状況を確認するため、情報セキュリティ監査を実施し、又は議員に対して自己点検を実施させるものとする。
２　議員は、前項の情報セキュリティ監査又は自己点検が行われる場合は、これに協力しなければならない。

（情報セキュリティポリシーの見直し）
第12条　議長は、前条に規定する情報セキュリティ監査又は自己点検の実施結果に基づき、情報セキュリティを侵す脅威に対する脆弱性を検証し、必要に応じて情報セキュリティポリシーの見直しを行うものとする。

（報告）
第13条　議員は、タブレット端末等の紛失、盗難、き損、水漏れ及び滅失について判明したとき又は個人情報等の漏えい、不正アクセスの感知、不正プログラムへの感染その他情報資産の管理に脅威を及ぼす事象について発見したときは、直ちに所属する会派の会派責任者及び政務調査課長に報告しなければならない。ただし、会派に所属しない議員にあっては、政務調査課長への報告をもって足りるものとする。

（違反行為への対応）

第14条　議長は、議員が第８条及び第９条の規定に違反したときは、口頭で注意を与えるものとする。この場合において、違反が改められない場合は、議長は、当該議員による情報資産の利用を停止することができる。

２　前項の規定は、議長自らが第８条及び第９条の規定に違反したときは、「議長」を「副議長」と読み替えるものとする。

（議長への適用）

第15条　第３条、第４条、第８条、第９条及び第13条の規定は、議長たる議員に対しても適用されるものとする。

（その他）

第16条　この要領に定めるもののほか必要な事項は、議長が別に定める。

附　則

この要領は、令和８年４月１日から施行する。