神奈川県情報セキュリティポリシー（要綱）

神奈川県デジタル戦略本部

（※）本要綱の「第２章情報セキュリティ対策基準」については、情報セキュリティの確保に支障を及ぼす恐れのある情報を含むことから、記載しておりません。

＜目　次＞

神奈川県情報セキュリティポリシー（要綱）

序　神奈川県情報セキュリティポリシーの構成

神奈川県情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）とは、神奈川県（以下「県」という。）が所管する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をいう。情報セキュリティポリシーは、県が所管する情報資産に関する業務に携わる全ての職員等に情報セキュリティへの取組みを浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化に柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分である情報セキュリティ基本方針と情報セキュリティを取り巻く状況の変化に依存する部分である情報セキュリティ対策基準により構成することとした。

また、情報セキュリティポリシーに基づき、コンピュータ、ネットワーク及び情報システム（以下「情報システム等」という。）又は局、部若しくは室課所ごとの情報セキュリティに係る具体的な実施手順を、情報セキュリティ実施手順として策定することとする。

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構成

<table>
<tr><th>分類</th><th>文　書　名</th><th colspan="2">内　　容</th></tr>
<tr><td rowspan="2">情報セキュリティポリシー</td><td rowspan="2">神奈川県情報セキュリティポリシー</td><td>情報セキュリティ基本方針</td><td>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。</td></tr>
<tr><td>情報セキュリティ対策基準</td><td>情報セキュリティ基本方針に基づき定める情報システム等に共通の情報セキュリティ対策の基準。</td></tr>
<tr><td>情報セキュリティ実施手順</td><td>情報セキュリティ点検に関する基準　等</td><td colspan="2">情報セキュリティポリシーに基づいて、局、部又は室課所ごとに定める具体的な実施手順。</td></tr>
</table>

第１章　情報セキュリティ基本方針

１　目的

県の情報システム等が取り扱う情報には、県民等の個人情報のみならず行政運営上重要な情報など、外部に漏えい等した場合に重大な結果を招く情報も含まれている。

したがって、これらの情報及び情報を取り扱う情報システム等を様々な脅威から防御することは、県民等の財産、プライバシー等を守るためにも、また、業務の安定的な運営のためにも必要不可欠であり、さらに県に対する県民等からの信頼の維持向上に寄与するものである。

本基本方針は、県が所管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、県が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

２　定義

この要綱において、次に掲げる用語の意義は、以下の各号に定めるところによる。

(1) コンピュータ	汎用コンピュータ、サーバ、ワークステーション、パーソナルコンピュータ及びこれらに類するもの並びにこれらの運営に必要な機器をいう。
(2) ネットワーク	コンピュータを接続してデータ通信するための情報通信網並びにこの運営に必要な設備及び機器をいう。
(3) 情報システム	コンピュータ及びネットワークを用いて業務処理を行うために必要な体系をいう。
(4) データ	コンピュータ又は記録媒体に記録されている電磁的記録をいう。
(5) 情報資産	コンピュータ、ネットワーク、情報システム及びこれらが取り扱う情報（当該情報を印刷した文書を含む。）をいう。
(6) 記録媒体	データを記録するための媒体をいう。例えば、磁気テープ、フロッピーディスク、ハードディスク、ＵＳＢメモリ、ＣＤ－Ｒ、ＤＶＤ－Ｒ、ボイスレコーダ、デジタルカメラ、ＳＤメモリカードなど。
(7) モバイル端末	コンピュータのうち、自席にとどまらず、庁舎内外に携帯し、利用できる端末をいう。
(8) IoT 機器を含む特定用途機器	テレビ会議システム、IP 電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システム特有の構成要素であって、ネットワークに接続されている又は電磁的記録媒体を内蔵しているものをいう。
(9) 外部サービス	事業者等の庁外の組織が情報システムの一部又は全部の機能を提供するものをいう。ただし、当該機能において県が所管する情報資産が取り扱われる場合に限る。

(10) クラウドサービス	ネットワークに接続されたコンピュータを運営する事業者等が提供する様々なサービス・機能を利用する形態をいう。
(11) ソーシャルメディア	インターネット上において不特定多数の者が情報を交換・共有する仕組みをいう。例えば、ブログ、ソーシャルネットワーキングサービス、動画共有サイトなど。
(12) ソーシャルメディアサービス	インターネット上において不特定多数の者が情報を交換・共有する仕組みを提供するサービスをいう。
(13) 機密性	情報にアクセスすることを認められた者が、情報にアクセスできる状態を確保することをいう。
(14) 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。
(15) 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。
(16) 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。
(17) 情報セキュリティ対策	情報セキュリティを確保するための対策をいう。
(18) 情報セキュリティインシデント	望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、業務の遂行を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。
(19) 職員等	地方公務員法（昭和 25 年 12 月 13 日法律第 261 号）第４条第１項に規定する職員及び労働者派遣事業の適正な運営の確保及び派遣労働者の就業条件の整備等に関する法律（昭和 60 年７月５日法律第 88 号）第２条第２項に規定する派遣労働者をいう。
(20) 庁舎	県がその事務を処理する目的で所有する建物及び敷地（ただし、デジタル戦略本部室長が管理するネットワークに有線ＬＡＮ又は無線ＬＡＮで接続できない区画を除く。）並びに賃借する建物内の区画（フロア内すべてを県の機関のみで借用している場合はそのフロア全体）をいう。

３　情報セキュリティポリシーの位置付けと職員等の義務

情報セキュリティポリシーは、県が所管する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指針となるものである。

したがって、県が所管する情報資産に関する業務に携わる全ての職員等は、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、業務の遂行に当たって

情報セキュリティポリシーを遵守するものとする。

4　情報セキュリティ管理体制

県は、県が所管する情報資産について、情報セキュリティ対策を推進及び管理するための体制を確立するものとする。

5　情報の分類

県は、情報をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

6　情報資産への脅威

情報セキュリティ対策基準を策定する上で、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と、特に情報セキュリティ対策を講ずべき脅威は以下のとおりである。

(1) 部外者による故意の不正アクセス、ウイルス攻撃、サービス不能攻撃等の意図的な要因による情報又はプログラムの持出し、盗聴、改ざん及び消去、機器及び媒体の盗難等

(2) 職員等及び委託事業者の従業員による誤操作、故意の不正アクセス又は不正操作による情報若しくはプログラムの持出し、盗聴、改ざん及び消去、機器及び媒体の盗難、正規の手続きによらない端末及び媒体の接続による情報漏えい等

(3) 地震、落雷、火災等の災害及び事故、故障等による業務の停止

(4) 大規模・広範囲にわたる疾病による職員等の要員不足に伴う情報システム運用の機能不全

7　情報セキュリティ対策

県は、上記６で示した脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じるものとする。

(1) 情報システム全体の強靭性の向上

情報システム全体に対し、次の三段階の対策を講じるものとする。

ア　個人番号利用事務を取り扱うネットワークにおいては、原則として、外部ネットワーク及び他の内部ネットワーク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パスワード以外の生体認証等を加えた二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。また、インターネット接続口は、原則として、神奈川情報セキュリティクラウドに集約する。

(2) 物理的対策

情報システム等を設置する執務室等への不正な立入り及び情報資産への損傷、妨害等から保護するための物理的な対策

(3) 人的対策

情報セキュリティに関する役割等を定め、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等、十分な教育及び啓発を講じるための対策

(4) 技術的対策

情報資産を不正なアクセス等から適切に保護するための情報資産へのアクセス制御、ネットワーク管理等の技術面の対策

(5) 運用における対策

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、委託を行う際の情報セキュリティ確保等の運用面の対策及び緊急事態が発生した際に迅速な対応を可能とするための危機管理対策

8　情報セキュリティ対策基準の策定

県が所管する情報資産について、上記７の情報セキュリティ対策を講じるに当たっては、遵守すべき行為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。このため、情報セキュリティ対策を行う上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第２章に定めるものとする。

9　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基準を遵守して情報セキュリティ対策を実施するために、個々の情報資産の情報セキュリティ対策の手順等をそれぞれ定めていく必要がある。このため、情報資産に対する脅威及び情報資産の重要度に対応する情報セキュリティ対策基準の基本的な要件に基づき、局、部及び室課所の長は、所管する情報資産の情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ対策基準及び情報セキュリティ実施手順は、公にすることにより情報セキュリティの確保に重大な支障を及ぼす恐れがあるため取扱いに注意するものとする。

10　情報セキュリティ監査の実施

県は、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、定期的に監査を実施するものとする。

11　評価及び見直しの実施

県は、情報セキュリティ監査の結果等により、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を行うとともに、情報セキュリティを取り巻く状況の変化に対応するために、情報セキュリティポリシーの見直しを実施するものとする。