黒磯那須公設地方卸売市場事務組合情報セキュリティ基本方針

１．目的

本基本方針は、地方自治法（昭和２２年法律第６７号）第２４４条の６第１項の趣旨にのっとり、本組合が保有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、本組合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

⑴　実施機関
　管理者、監査委員及び議会をいう。

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並びにその構成機器であるハードウェア及びソフトウェアをいう。

⑶　情報システム
　コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

⑷　プログラム
　コンピュータを機能させて一つの結果を得ることができるようにこれに対する指令を組み合わせたものをいう。

⑸　情報資産
　次に掲げるものをいう。

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、ネットワーク図その他のシステム関連文書

⑹　機密性
　情報にアクセスすることを認められた者のみが当該情報にアクセスできる状態をいう。

⑺　完全性
　情報が破壊され、改ざんされ、又は消去されていない状態をいう。

⑻　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、当該情報にアクセスできる状態をいう。

⑼　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。

⑽　外部委託事業者等
　情報システムの構築、開発、保守又は運用管理その他の情報資産に関する業務を受託する外部事業者若しくは指定管理者又は当該外部事業者若しくは指定管理者の従業者その他の情報資産を取り扱う者をいう。

⑾　外部委託
　外部委託事業者等に情報資産に関する業務を委託することをいう。

⑿　情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

⒀　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す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。

⒁　無害化通信

インターネットメール本文のテキスト化、端末への画面転送等により、コンピュータウィルス等の不正プログラムの付着がない等、安全が確保された通信をいう。

３．対象とする脅威

情報セキュリティ対策の対象とする脅威は、次に掲げるものとする。

⑴　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並びに部外者の侵入、内部不正等の意図的な要因による情報資産の漏えい、破壊、改ざん、消去、詐取等

⑵　情報資産の無断持出し、無許可ソフトウェアの使用その他の内部不正

⑶　プログラムの設計、開発及びメンテナンスの不備

⑷　外部委託の管理及び情報セキュリティに関するマネジメントの不備

⑸　機器故障その他の非意図的要因による情報資産の漏えい、破壊及び消去

⑹　地震、落雷、火災その他の災害による情報システム運用の機能不全

⑺　大規模及び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

⑻　電力供給の途絶、通信の途絶、その他の障害からの影響

⑼　その他本組合が保有する情報資産に影響を与える脅威

４．適用範囲

本基本方針は、実施機関及びその保有する全ての情報資産に適用する。

５．職員等の遵守義務

実施機関に属する全ての特別職、一般職員及び非常勤職員（以下「職員等」という。）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、業務の遂行に当たっては、情報セキュリティポリシーを遵守しなければならない。

６．外部委託事業者等に対する措置

外部委託事業者等に情報資産を取り扱わせる場合には、情報セキュリティポリシーを遵守させるための必要な措置を講ずるものとする。

７．情報セキュリティ対策

本組合が保有する情報資産の管理及び運用に当たり、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　情報セキュリティに対応する組織体制の確立

⑵　情報資産の重要度に応じた区分の設定及びその区分に応じた管理の徹底

⑶　情報システム全体に対し、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こと。

⑷　情報システムを設置する施設への不正な立入りの禁止及び情報資産の損傷の防止その他の物理的な侵害からの保護

⑸　職員等及び外部委託事業者等に対する情報セキュリティに関する教育及び啓発

⑹　情報システムの誤操作、不正操作、不正アクセス等からの情報資産の保護
⑺　情報セキュリティの監視及び例外措置の適用
⑻　クラウドサービスその他の外部サービスの適正な利用

８．情報セキュリティ監査及び自己点検

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、情報セキュリティ監査を実施するとともに、職員等に自己点検を行わせるものとする。

９．情報セキュリティポリシーの改訂

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合又は情報セキュリティに関する状況の変化に対応するため新たに対策が必要となった場合には、情報セキュリティポリシーを改訂する。

10．情報セキュリティ対策基準の策定

本基本方針に定めるもののほか、情報セキュリティ対策を実施するために、具体的な遵守事項、判断基準等を定める情報セキュリティ対策基準を策定する。なお、情報セキュリティ対策基準は非公開とする。