情報セキュリティポリシー策定指針
（臨海ホールディングスグループ）

平成 20 年 3 月 31 日
代表取締役社長決定

（目的）

第１条　本指針は、株式会社東京臨海ホールディングス（以下、「当社」という。）及びグループ各社等が構成する企業集団（以下、「当社グループ」という。）が保有する情報資産の機密性、完全性及び可用性を維持し、当社を含むグループ各社が情報セキュリティポリシーを策定する際のガイドラインとなる基本的事項を示すとともに、情報セキュリティに係る基本的理念の共有化を図ることで、当社グループの業務の適正さを確保、維持することを目的として定める。

（定義）

第２条　この指針において、次の各号に掲げる用語の定義は当該各号に定めるところによる。

(1) グループ各社（又は「各社」）
当社と「業務運営に関する協定」（以下「業務運営協定」）を締結している会社をいう。

(2) 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、その構成機器(ハードウエア及びソフトウエア) をいう。

(3) 情報処理システム
コンピュータ、端末装置、通信回線等により、電子情報を処理するシステムをいう。

(4) 情報資産
以下のものをいう。
ア　会社において職務上作成し、又は取得した文書、図画及び電磁的情報
イ　ネットワーク、情報処理システム及びこれらに関する設備、電磁的記録媒体（以下「情報システム等」という。）

(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。
ア　機密性とは、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。
イ　完全性とは、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。
ウ　可用性とは、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。

(6) 情報セキュリティポリシー
本指針及び当社、グループ各社それぞれが情報セキュリティ対策について本指針第６条の規定に準じて総合的、体系的にまとめたもの。

（対象とする脅威）

第３条　当社グループが想定し、情報セキュリティ対策を講じるべき情報資産に対する脅威は、次の各号に掲げるものとする。

(1) 部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃等の要因による情報資産

の漏えい、破壊、改ざん、消去及び不正な操作等

(2) 情報資産の盗難、紛失、無断持ち出し、ウイルス感染、無許可ソフトウエアの使用等の規定違反、プログラム上の欠陥、人為的なミス、故障等の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、風水害等の災害や突発的な停電によるサービス及び業務の停止、情報資産のき損、喪失等

（基本的役割）

第４条　当社及びグループ各社は、連携を取りながら、本指針並びにそれぞれの内部統制に関する基本方針等に基づき、情報セキュリティポリシーの策定や必要な環境整備を進めるなど総合的、体系的な情報セキュリティ対策を実施する。

２　当社及びグループ各社の基本的役割は、次の各号に定めるとおりとする

(1) 当社（グループ本社）

当社は、当社グループにおいて必要な情報セキュリティが確保されるよう、策定指針を整備し、本指針に基づきグループ会社のモデルとなる情報セキュリティポリシーを策定し、グループ各社の情報セキュリティポリシー策定の支援を行う。

さらに、業務運営協定に基づく内部監査等により、グループ各社に対する指導・監督を行うとともに、グループ各社間での情報資産の取扱いの調整など、当社グループの情報セキュリティの確保に関する総合的調整を行う。

(2) グループ各社

グループ各社は、策定指針に基づき各社における情報セキュリティポリシーを策定する。また、具体的対策のための実施手順の策定や自己点検の実施など、情報セキュリティポリシーを適切に運用することにより、必要な情報セキュリティの確保に努める。

（社員等の遵守義務）

第５条　当社及びグループ各社は、それぞれの役員及び社員（嘱託、派遣契約等に基づき当社で勤める者を含む。以下「社員等」）に対し情報セキュリティの重要性及び情報資産への脅威に関する共通認識の醸成に努め、それぞれが定める情報セキュリティポリシー及びその他情報セキュリティの確保に必要な事項を遵守させなければならない。

（情報セキュリティポリシーのガイドライン）

第６条　当社及びグループ各社が、本指針並びにそれぞれが定める内部統制に関する基本方針等に基づき、第３条に掲げる脅威から情報資産を保護するため策定する情報セキュリティポリシーには、次の各号に定める基本的事項を明記するものとする。

(1) 組織体制の確立

ア 会社における総合的な情報セキュリティ対策を推進するため、情報セキュリティ担当取締役、情報セキュリティ管理者、情報セキュリティ責任者等を置き、各職層における役割、権限及び責任を明確にすること。

イ 当社及びグループ各社において、必要な場合には社内にそれぞれ情報セキュリティ委員会を設置することとし、役割、権限等について明確にすること。

(2) 情報資産の分類と管理

業務上保有、管理する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類

に基づき、情報資産の管理及び取扱い方法等について具体的に定めること。

なお、それぞれが文書管理規程等に既に文書等の情報資産に特段の定めをし、これを優先させる必要がある場合は、当該規定を優先する旨規定すること。

(3) 物理的セキュリティ

サーバ、通信回線及びパソコン等の情報処理機器類の管理について、物理的な対策を定めること。

(4) 技術的セキュリティ

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な対策を定めること。

(5) 人的セキュリティ

ア 情報セキュリティに関し、社員等が遵守すべき事項について明確かつ具体的に定めること。

イ 社員等に対する教育及び啓発の実施について定めること。

ウ 外部委託事業者等への対応について定めること。

(6) 情報セキュリティポリシーの運用

ア 情報システム等の監視、情報セキュリティポリシーの遵守状況の確認、外部委託等を行う際のセキュリティ確保、自己点検の実施等、情報セキュリティポリシー運用上の対策について定めること。

イ 情報資産への侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応体制の整備について定めること。

ウ 情報資産への侵害に係る事項は、業務運営協定第３条第６項に規定する事項とする。したがって、グループ各社は、情報資産への侵害が発生した場合等には当社へ報告を行う旨明記する。当社は、報告を受けた事項についてグループ全体で対応が必要な場合には、体制を整備する旨明記すること。

(7) その他、策定の目的、用語の定義、対象となる脅威など総則的事項

２　前項に係らず、グループ各社の情報資産や環境整備の状況、取引先との関係、その他情報セキュリティ対策を実施するため必要と認められる場合には、当社グループ全体の利益を損なわない範囲において、一部を省略し又は別の事項を定めることができる。

（本指針等の見直し）

第７条　第４条第２項各号に定める情報セキュリティに関する内部監査や自己点検の結果、本指針の見直しが必要となった場合及び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な対策が必要となった場合は、本指針を見直す。

２　当社及びグループ各社は、前項に基づき本指針が見直された場合及び前項の規定に準じて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には、それぞれの情報セキュリティポリシーを見直す。

（雑則）

第８条　本指針については、当社のインターネットホームページにおいて公開する。

附則

この指針は、平成２０年４月１日から施行する。