経営工学研究所

情報セキュリティ方針

第1版 2006年6月30日

改訂履歴

版	日付	担当者	内容
1	2006/06/30	砂川	新規作成

１ 趣旨

当社はコンピュータシステム開発を主な業務として行っており、ネットワークコンピュータを利用した開発環境は当社にとって必要不可欠である。
一方、世間では度重なる情報セキュリティ事件が発生している。当社において情報セキュリティ事件が発生した場合の信用の損失は致命的であるため、早急に対応しなければならない課題である。
そのために、当社は、個人情報やネットワークコンピュータ上を流通する情報やコンピュータ及びネットワーク等の情報システム（以下、情報資産）を第４の資産と位置付ける。よって、当社は、情報資産を重要な資産とし、保護・管理しなければならない。
当社は、情報資産を保護する「情報セキュリティマネジメント」を実施するために、『情報セキュリティポリシー』を策定する。
『情報セキュリティポリシー』は、当社の情報資産を、故意や偶然という区別に関係なく、改ざん、破壊、漏洩等から保護されるような管理策をまとめた文書である。
当社の情報資産を利用する者は、情報セキュリティの重要性を認知し、この『情報セキュリティポリシー』遵守しなければならない。

２ 『情報セキュリティポリシー』の適用範囲

『情報セキュリティポリシー』の適用範囲は、当社の情報資産に関連する人的・物理的・環境的リソースも含むものとする。

３ 『情報セキュリティポリシー』の適用者

当社の社員・契約社員（一時雇用者を含む）を従業員と定義する。『情報セキュリティポリシー』の適用者は、経営陣、従業員を含めた、当社の情報資産を利用するすべての者である。

３．１ 経営陣の責務

経営陣は、『情報セキュリティポリシー』への支持・支援を表明し、率先して情報セキュリティマネジメントを推進しなければならない。

３．２ 従業員の責務

従業員には、当社の情報資産の使用を認めるが、それは、円滑な業務遂行の手段としての使用を認めることであり、私的利用を許可するものではない。
従業員は、情報資産を扱う上で、企業利益の維持・向上および顧客満足のために、『情報セキュリティポリシー』に同意し、遵守しなければならない。また、これに違反した者は、その結果について責任を負わなければならない。

３．３ 外部委託業者に対する対応

『情報セキュリティポリシー』の適用範囲内で行う作業を、外部委託業者に依頼する場合には、契約上で遵守するべきセキュリティ管理策を明確にし、セキュリティ事故時の責任に関しても明確にしなければならない。

４　『情報セキュリティポリシー』の構成と位置付け

『情報セキュリティポリシー』は、以下の３つの階層に分けて策定・管理される文書とする。

４．１ 情報セキュリティ方針

情報セキュリティ方針（以下、「方針」とする）は、『情報セキュリティポリシー』の最上位に位置する文書である。この文書は、当社の情報セキュリティマネジメントにおける方針を記述したものである。この文書に基づいて下層の文書を策定する。

４．２ 情報セキュリティ対策標準

情報セキュリティ対策標準（以下、「対策標準」とする）は、方針の下層に位置する文書である。この文書は、方針での宣言を受け、項目毎に遵守すべき事項を網羅的に記述する。

４．３ 情報セキュリティ実施手順書

情報セキュリティ実施手順書（以下、「実施手順書」とする）は、対策標準の下層に位置する文書である。この文書は、対策標準で記述された文書を具体的に、配布するべき対象者毎に内容をカスタマイズして記述する。

４．４ 既存の規定との関連

方針は、当社の他の規定（人事規定、就業規則等）と同等の位置付けの文書とする。よって、この文書の改廃は所定の規定に準じて行うものとする。

４．５ その他関連法規

『情報セキュリティポリシー』は、関連法規と照らして違反することの無いようにしなければならない。
また、必要に応じて関連規格に遵守した管理策を導入しなければならない。
関連法規・関連規格としては、以下のものが挙げられる。

国際規格

・ISO/IEC 17799
・ISO/IEC TR 13335（GMITS）

国内規格

・ JIS Q 15001

国内法規

・ 刑法
・ 不正アクセス行為の禁止等に関する法律
・ 建築基準法/同施行令
・ 消防法/同施行令/同施行規則
・ 不正競争防止法
・ 著作権法

５　『情報セキュリティポリシー』の公開対象者

方針は、従業員すべてを公開対象とする。対策標準は、情報セキュリティ委員会メンバーと担当部署の

者を公開対象とする。実施手順書は、該当する業務を行う者を公開対象とする。

６ 『情報セキュリティポリシー』の公開

『情報セキュリティポリシー』は機密文書として扱い、原則として、社外に公開してはならない。ただし、公開しなければ業務を遂行できない場合には、以下で定めるセキュリティ担当者の承認の下で公開を認める場合がある。

７ 基本用語の定義

『情報セキュリティポリシー』における用語は以下の通り定義する。

７．１ 情報セキュリティ（ISO/IEC17799 より抜粋）

情報の機密性、完全性及び利用の可能性の維持。

注）

機密性は、情報にアクセスすることが認可された者だけがアクセスできることを確実にすること、として定義される。

完全性は、情報及び処理方法の正確さ及び完全である状態を安全防護すること、として定義される。

利用の可能性は、認可されたユーザが、必要時に、情報及び関連財産にアクセスできることを確実にすること、として定義される。

７．２ リスクアセスメント（ISO/IEC17799 より抜粋）

情報及び情報処理施設/設備に対する脅威、それらへの影響及びバルネラビリティ並びにそれらがおこる可能性の評価。

７．３ リスクマネジメント（ISO/IEC17799 より抜粋）

許容コストにより、情報システムに影響を及ぼす可能性があるセキュリティリスクを明確にし、制御し、最小限に抑制するか、又は除去するプロセス。

８ 体制

当社の情報セキュリティマネジメントを遂行する体制を以下の通り定める。

８．１ 情報セキュリティ委員会

当社の情報セキュリティを維持していくために、情報セキュリティ委員会を設け、全社的なマネジメント体制を整えるものとする。情報セキュリティ委員会は会社役員および各部門の担当者から構成する。また、当社の役員の一人を情報セキュリティ委員長として取締役会で指名する。情報セキュリティ委員長は、当社における情報セキュリティマネジメントに関しての最高責任者である。

８．２ 情報セキュリティ管理者

情報セキュリティ管理者の役割は、情報セキュリティに関する作業指示・管理を行う現場レベルの責任者である。情報セキュリティ委員会によって指名される。

当社に関係する情報キュリティ情報収集を行い、社内の情報セキュリティ対策に反映させ、従業員から

収集した情報を、必要に応じて情報セキュリティ委員会に報告しなければならない。

９ 情報セキュリティ委員会の役割と責務

情報セキュリティ委員会の主な役割を下記の通り定める。

９．１ 情報セキュリティマネジメントの企画及び計画

情報セキュリティ委員会は、当社における情報セキュリティマネジメントを実施していく企画及び計画を作成し、その計画通り情報セキュリティマネジメントを実施しなければならない。
この企画及び計画には、情報セキュリティマネジメントを遂行する為のリスクアセスメント、リスクマネジメントはもちろんのこと、『情報セキュリティポリシー』の見直しや従業員への普及・啓発も考慮に入れなければならない。

９．２ 『情報セキュリティポリシー』文書の配布責任

情報セキュリティ委員会は、『情報セキュリティポリシー』を策定又は改訂した場合には、迅速に対象従業員へその文書を配布しなければならない。

９．３ 社内教育の実施

情報セキュリティ委員会は、情報セキュリティに関する継続的な社内教育を行う。この社内教育は、意識向上と技術向上の両面から実施しなければならない。

９．４ 『情報セキュリティポリシー』の遵守状況の評価及び改訂

情報セキュリティ委員会は、従業員の『情報セキュリティポリシー』遵守状況を定期的に調査し、『情報セキュリティポリシー』のレビューを行うこととする。
また、従業員の『情報セキュリティポリシー』に対する意見や要望を収集し、その妥当性を評価するとともに必要に応じて内容の改訂を行うこととする。

９．５ 監査結果の評価及び改訂

情報セキュリティ委員会は、監査の結果を受けて、『情報セキュリティポリシー』の妥当性を評価すると共に、必要に応じて、内容の改訂を行わなければならない。

９．６ 取締役会への報告

情報セキュリティ委員会は、情報セキュリティの維持・管理状況や『情報セキュリティポリシー』の改定状況、及び情報セキュリティに関する事故や問題の発生状況を取締役会へ報告しなければならない。

９．７ 『情報セキュリティポリシー』違反者への処罰

情報セキュリティ委員会は、従業員の『情報セキュリティポリシー』に違反した行為等が判明した場合、該当従業員に対して適切な処置を講じることとする。場合によっては、人事規定に基づいた処罰を人事担当者に申請することとする。

１０ 情報セキュリティマネジメント

当社は、情報資産を保護するために、情報セキュリティマネジメントを以下の通り進めることとする。

１０．１ リスク分析

当社の情報資産に関するリスクアセスメント、リスクマネジメント全般は、情報セキュリティ委員会が行うこととする。

１０．２ ポリシー策定

『情報セキュリティポリシー』の策定･評価･レビューは情報セキュリティ委員会が行うこととする。
情報セキュリティ委員会では、方針および対策標準を策定することとする。
対策手順書に関しては、情報セキュリティ委員会より指名された各情報システムの担当者が策定し、運用しなければならない。

１０．３ 対策の実施

当社で策定した『情報セキュリティポリシー』に記述した対策は、計画的に実装しなければならない。
情報システム部は、セキュリティ対策実装のための計画書を策定し、情報セキュリティ委員会の承認を得なければならない。

１０．４ 教育・啓蒙

当社は、情報資産を扱うすべてのものに対し、意識向上と技術レベルの向上の両面から、積極的に情報セキュリティの教育を行うこととする。
当社の情報資産に関わるすべて者は、会社が提供する情報セキュリティの教育を受けなければならない。
同時に、当社の情報資産に関わる者は、情報セキュリティに関する最新の情報について、自発的に情報セキュリティ委員に提言することが望ましい。

１０．５ 監査・評価

情報セキュリティ委員会は、定期的あるいは発見の可能性のあるときに情報セキュリティに対する脅威、脆弱性を洗い出し、その対策を検討し、『情報セキュリティポリシー』に反映させなければならない。
それらは、監査の結果、情報資産の利用者から届けられた情報、情報セキュリティの脆弱性に関する情報の収集等の活動から得られる情報をもとに行われる場合もある。

１０．６ 文書の改廃

『情報セキュリティポリシー』の改廃は、方針は、取締役会の承認を必要とする。対策標準及び実施手順は、情報セキュリティ委員会が決議する。

１１ 違反時における罰則

当社は、『情報セキュリティポリシー』の違反者に対し、厳格な措置をとることとする。
情報セキュリティ委員会は、『情報セキュリティポリシー』に違反した事項の重要度を評価し、適切な処置を講じることとする。

１２ 情報セキュリティ侵害時の対応

当社の情報セキュリティが侵害されたと思われる事象が判明した場合は、速やかに準備された対応方法に従って対応しなければならない。

１３ 執行期日

本方針は、２００６年6月３０日に取締役会にて承認され、２００６年7月１日より施行する。