

情報セキュリティポリシー

日東通信株式会社

- 1, 情報セキュリティポリシー基本方針
- 2, 『情報セキュリティポリシー』の適用範囲
- 3, 『情報セキュリティポリシー』の適用者
 3. 1 経営陣の責務
 3. 2 従業員の責務
 3. 3 外部委託業者に対する対応
- 4, 『情報セキュリティポリシー』の構成と位置付け
 4. 1 情報セキュリティ方針 (Policy)
 4. 2 情報セキュリティ規程 (Rule or Guide)
 4. 3 情報セキュリティ手順書 (Operating Procedure)
 4. 4 既存の規程との関連
 4. 5 その他関連法規
- 5, 『情報セキュリティポリシー』の公開対象者
- 6, 基本用語の定義
 6. 1 情報セキュリティ (Information Security)
 6. 2 リスクアセスメント (Risk Assessment)
 6. 3 リスクマネジメント (Risk Management)
 6. 4 脅威 (Security Threat)
 6. 5 脆弱性 (Vulnerability)
- 7, 体制
 7. 1 情報管理委員会
 7. 2 システム管理者
 7. 3 情報セキュリティ責任者
 7. 4 情報セキュリティ監査
- 8, 情報管理委員会の構成図及び構成メンバー
 8. 1 情報管理委員会の構成図

- 8. 2 委員
- 8. 3 非常勤委員
- 8. 4 情報管理委員長
- 8. 5 事務局
- 8. 6 分科会 (Working Group)
- 9, 情報管理委員会の役割と責務
 - 9. 1 情報セキュリティ管理の企画及び計画
 - 9. 2 『情報セキュリティポリシー』文書の配布
 - 9. 3 社内教育の実施
 - 9. 4 監査結果の評価及び改訂
 - 9. 5 幹部会への報告
 - 9. 6 『情報セキュリティポリシー』違反者への対応
- 10, 情報セキュリティ管理
 - 10. 1 リスクアセスメント
 - 10. 2 リスクマネジメント
 - 10. 3 情報セキュリティポリシー及び関連規定の評価・改定
 - 10. 4 対策の実施・確認
 - 10. 5 教育・啓蒙
 - 10. 6 監査・評価
 - 10. 7 規定の更新
- 11, 違反時における罰則
- 12, 情報事故に対する対応
- 13, 改訂

1 情報セキュリティポリシー基本方針

日東通信株式会社（以下、当社）は、お客様情報をはじめとする様々な情報資産を盗難、不正アクセス、事故等様々な脅威や情報漏洩リスクに対し適切な安全管理対策の実施及び、保護を行いお客様ならびに社会に広く信頼される会社となることを目指し

【情報セキュリティポリシー】を制定し、これを遵守する。

1、 情報資産の保護

お客様情報をはじめとする当社応報資産を盗難、不正アクセス、事故等から保護する為、情報セキュリティ方針ならびにそれにまつわる規定を策定し、これに従い業務を行うとともに、関係法令や契約事項を遵守する。

2、 推進体制

情報セキュリティ対策を実施するために、情報管理委員会を組織し情報セキュリティのリスクを軽減することに努める。

3、 教育・研修の実施

契約社員を含む全従業員に対し、情報セキュリティに対する知識と意識を向上させ、情報資産の適正な利用を行うよう、定期的に教育・研修を実施する。

4、 監査体制の整備

情報セキュリティポリシーの遵守状況及び情報資産の取扱いについて、定期的に点検及び監査を行い、発見された不備や改善項目については、速やかに是正処置を講じる。

5, 情報セキュリティインシデントの対応

情報セキュリティに関連するインシデント（事件・事故）の発生に対する適切な処置を講じるとともに、万が一事件や事故が発生した場合、情報管理委員会を中心に必要に応じて関連機関に連絡するとともに、速やかな原因究明、対策を実施し、影響を最小限にするよう努める。また必要に応じて再発防止策を講じる。

6, 継続的な改善実施

基本方針および関連する諸規則、管理体制を定期的に評価・見直しを行い、情報セキュリティマネジメントシステムの継続的な改善を行う。

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、会社で運営するシステムに限らず、会社が使用するサービスなども含むものとする。

3 『情報セキュリティポリシー』の適用者

当社の経営者・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、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』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、業務遂行上必要な情報資産の使用を認める。

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。

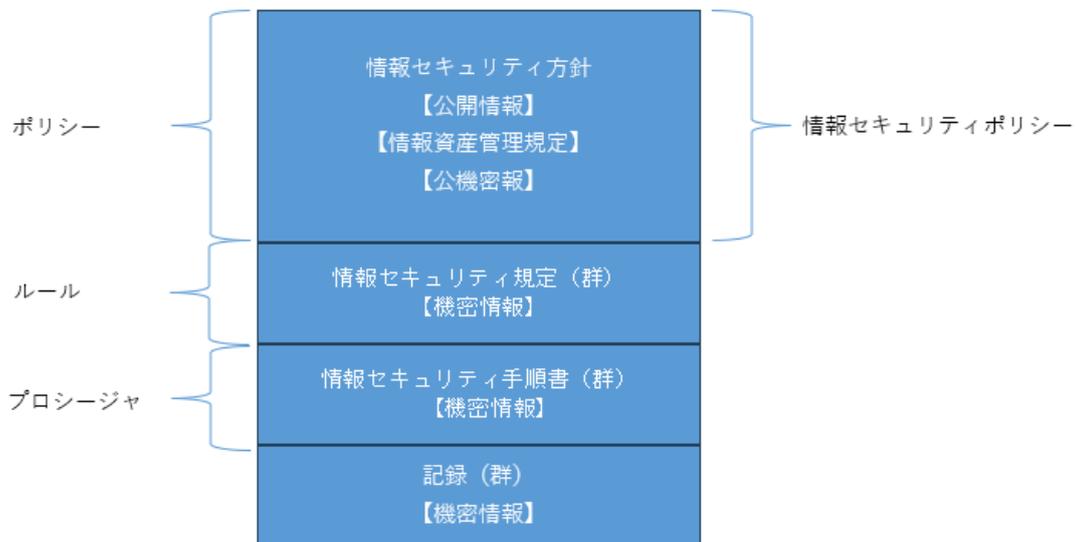
また、これに違反した者は、その結果について責任を負わなければならない。

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、契約上で遵守すべきセキュリティ管理策を明確にし、必要なセキュリティ教育を行い、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「情報セキュリティ基本方針」を含む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 (Policy)

情報セキュリティ方針（以下、「方針」とする）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 情報セキュリティ規程 (Rule or Guide)

情報セキュリティ規程（以下、「規程」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 情報セキュリティ手順書 (Operating Procedure)

情報セキュリティ対策手順書（以下、「手順書」とする）は、規程の下層に位置する文書である。

この文書は、規程で記述された文書をより具体的に、対象となる情報を扱う部門・担当者に応じて記述する。

4. 4 既存の規程との関連

方針は、当社の他の規程（人事規程、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程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、主に以下のものが挙げられる。

国際規格

- ・ ISO/IEC 27001

国内法規

- ・ 刑法
- ・ 不正アクセス行為の禁止等に関する法律（不正アクセス禁止法）
- ・ 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
- ・ 個人情報の保護に関する法律（個人情報保護法）
- ・ 行政手続き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（番号法）
- ・ 労働契約法
- ・ 労働基準法
- ・ 労働安全衛生法（VDT 作業に関するガイドライン含む）
- ・ 会社法
- ・ 電子帳簿保護法
- ・ サイバーセキュリティ
- ・ 刑事訴訟法

5 『情報セキュリティポリシー』の公開対象者

- (1) 情報セキュリティ基本方針は、一般に公開出来るものとする。

6 基本用語の定義

6. 1 情報セキュリティ (Information Security)

情報資産を安全かつ有効的に保護・活用すること。これは、業務の遂行上必要な情報に必要な者だけがアクセスできることを指す。

6. 2 リスクアセスメント (Risk Assessment)

情報資産に対する脅威の重要度及び危険性を特定し、事故発生につながる可能性について評価すること。

6. 3 リスクマネジメント (Risk Management)

上記により特定されたリスクを抑制或いは軽減するための保護の方法。

6. 4 脅威 (Security Threat)

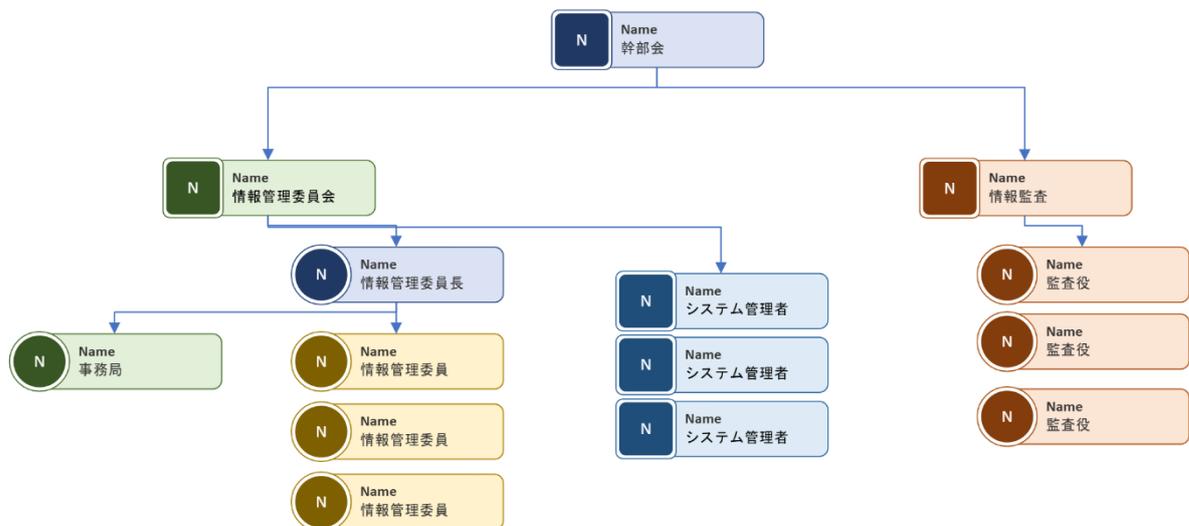
情報資産の損失につながる要因。例えば、情報盗難、自然災害、など。

6. 5 脆弱性 (Vulnerability)

情報資産の流出、漏洩につながる要因。ソフトウェア、ハードウェアの不備、情報教育の不備など。

7 体制

情報セキュリティ管理を遂行する体制を以下の通り定める。



7. 1 情報管理委員会

当社の情報セキュリティを維持していくために、情報管理委員会を設け、全社的な管理の体制を整えるものとする。ポリシー及び関連した規定の策定を行う。

7. 2 システム管理者

システム管理者は、情報管理委員会で決定した対策事項を実施及び推進する。

システム管理者は、情報機器の管理責任を有し、情報セキュリティに関する情報の収集を行い、必要に応じて情報管理委員会に報告する。

7. 3 情報セキュリティ責任者

情報管理委員長を情報セキュリティ責任者とする。

7. 4 情報セキュリティ監査

情報セキュリティ監査は、情報管理委員会とは独立した組織であり、幹部会によって必要に応じて任命される。外部の監査人を含むのが望ましい。

幹部会

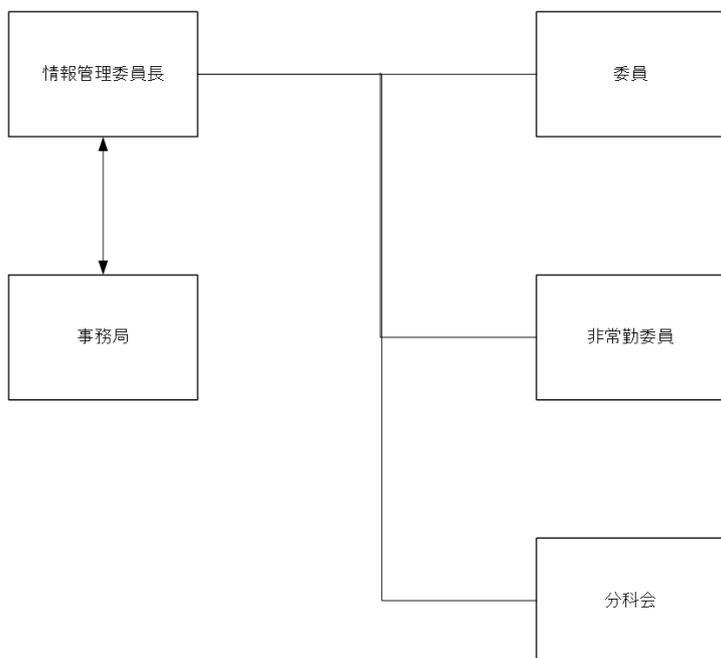
会社の最高決定機関として、情報セキュリティポリシーを承認する。

8 情報管理委員会の構成図及び構成メンバー

8. 1 情報管理委員会の構成図

委員会の構成は下図の通り定める。

情報管理委員会 構成図



8. 2 委員

各部門、拠点の代表者で構成される。委員は、情報セキュリティに関する方針・施策等を

検討し、従業員に対する周知・徹底を行う。

8. 3 非常勤委員

情報管理委員会は、外部の専門家（セキュリティコンサルタント、法律専門家など）を、非常勤委員として必要に応じて招集することが出来る。

8. 4 情報管理委員長

情報委員長は、情報セキュリティ責任者である。

8. 5 事務局

事務局は、情報管理委員会を運営する上での事務作業を行う。

8. 6 分科会（Working Group）

情報管理委員会は、各作業を実施するにあたって分科会を設けることができる。

9 情報管理委員会の役割と責務

情報管理委員会の主な役割を下記の通り定める。

9. 1 情報セキュリティ管理の企画及び計画

情報管理委員会は、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する。

この企画及び計画には、情報セキュリティ管理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及び本ポリシーの見直しや従業員の教育・啓発も含まれる。

9. 2 『情報セキュリティポリシー』文書の配布

情報管理委員会は、『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

従業員へ通知し、周知徹底させる。

9. 3 社内教育の実施

情報管理委員会は、経営陣、従業員に対し情報セキュリティに関する継続的な社内教育を行う。

9. 4 監査結果の評価及び改訂

情報管理委員会は、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、内容の改訂を行う。

9. 5 幹部会への報告

情報管理委員会は、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』の改訂状況、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幹部会へ報告する。

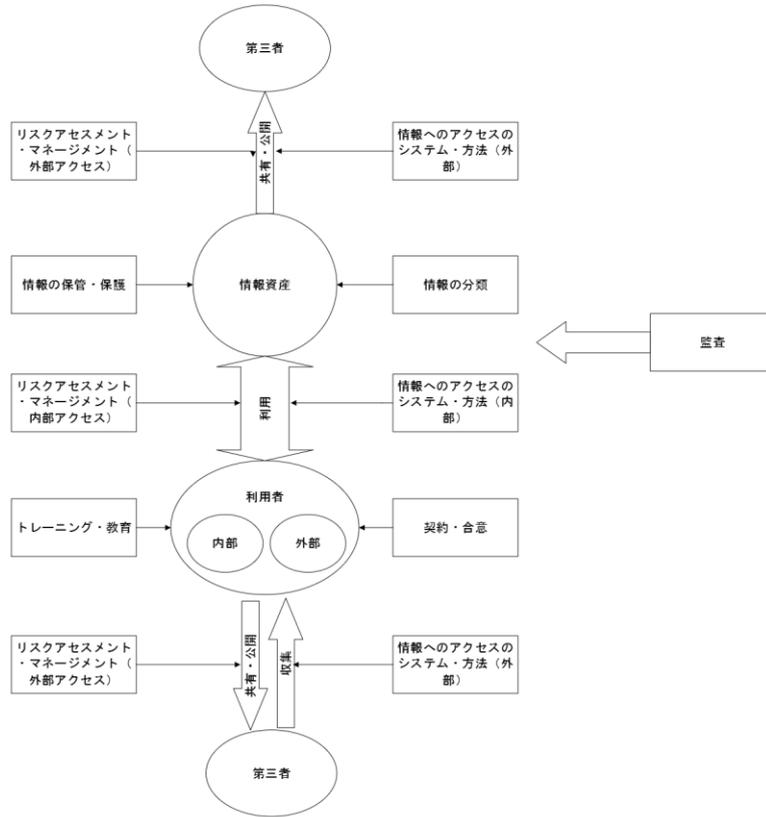
9. 6 『情報セキュリティポリシー』違反者への対応

情報管理委員会は、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、幹部会に報告し、適切な処置を講じてもらうことが出来る。

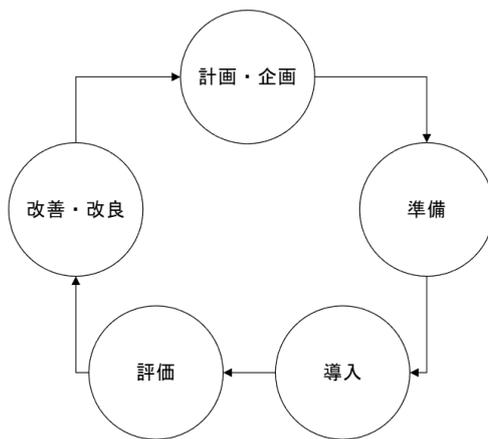
10 情報セキュリティ管理

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。

情報セキュリティ管理



情報管理ライフサイクル



計画・企画:

- ポリシー、規則、手順の作成・変更。
- 必要な資源の確保 (人・物・時間)。

準備:

- 必要なものの同定。
- 導入時期の決定。
- 導入の周知。

導入:

- 新しい規則、手順の導入。
- 使用者のトレーニング・教育。

評価:

- 規則、手順の評価。
- 監査。

改善・改良:

- 改善・改良に必要な規則・手順のリスタップ。
- 変更による影響の評価。

10.1 リスクアセスメント

情報資産に関するリスクアセスメントは、情報管理委員会が行う。

10.2 リスクマネジメント

リスクアセスメントに基づくリスクマネジメントは、情報管理委員会とシステム管理者が共同で行う。

10.3 情報セキュリティポリシー及び関連規定の評価・改定

『情報セキュリティポリシー』及び関連規定の評価・改定は情報管理委員会が行う。
情報管理委員会は、手順書の策定・評価・改定にあたり、システム管理者の協力を要請できる。

10.4 対策の実施・確認

情報管理委員会は、情報セキュリティ関連の初規定が実施されていることを、システム管理者の助けを得て確認する。

10.5 教育・啓蒙

情報管理委員会は、情報セキュリティ教育を行う。
全従業員は、定期的に必ず情報セキュリティ教育を受けなければならない。

10.6 監査・評価

情報管理委員会は、情報セキュリティ監査の結果のなどにに基づき、定期的に『情報セキュリティポリシー』の見直しを行い、必要に応じて更新する。

10.7 規定の更新

『情報セキュリティポリシー』の更新は、幹部会によって承認される。

1 1 違反時における罰則

『情報セキュリティポリシー』の違反者に対する措置は、情報管理委員会の助言に基づき、幹部会が決定する。

1 2 情報事故に対する対応

情報管理員会は、別途定められた手順に従い情報事故に対応する。

1 3 改訂履歴

2025年8月 初版