情報セキュリティ基本方針

0.92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

情報セキュリティ基本方針

ネットワークコンピュータを利用した経営環境が、当社に導入されて久しい。その間、当社の扱っている情報が、ネットワークコンピュータ上で扱われることが当然のこととなった。ネットワークコンピュータは、その導入による業務効率の影響は甚だしく、また、経営支援ツールとしても今後も大いに活用していくべきものである。インターネットを利用してビジネスチャンスを拡大している当社にとって、「セキュリティの確保」は必須事項である。昨今の度重なるセキュリティ事件は、当社にとっても「対岸の火事」ではなく、問題を発生させないために、早急に対応しなければならない経営課題である。

お客様との関係において、セキュリティ事件が発生した場合の営業機会の損失は甚だしいものになることは想像に難くない。当社は、顧客満足度を向上させるためにも、「セキュア」なブランドイメージを早急に構築しなければならない。

そのために、当社は、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などの情報システム（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』を遵守しなければならない。

情報セキュリティ方針

０．９２a版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3．ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　　E-Mail：sec@jnsa.org

情報セキュリティ方針

１　趣旨

ネットワークコンピュータを利用した経営環境が、当社に導入されて久しい。その間、当社の扱っている情報が、ネットワークコンピュータ上で扱われることが当然のこととなった。ネットワークコンピュータは、その導入による業務効率の影響は甚だしく、また、経営支援ツールとしても今後も大いに活用していくべきものである。インターネットを利用してビジネスチャンスを拡大している当社にとって、「セキュリティの確保」は必須事項である。昨今の度重なるセキュリティ事件は、当社にとっても「対岸の火事」ではなく、問題を発生させないために、早急に対応しなければならない経営課題である。

お客様との関係において、セキュリティ事件が発生した場合の営業機会の損失は甚だしいものになることは想像に難くない。当社は、顧客満足度を向上させるためにも、「セキュア」なブランドイメージを早急に構築しなければならない。

そのために、当社は、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。

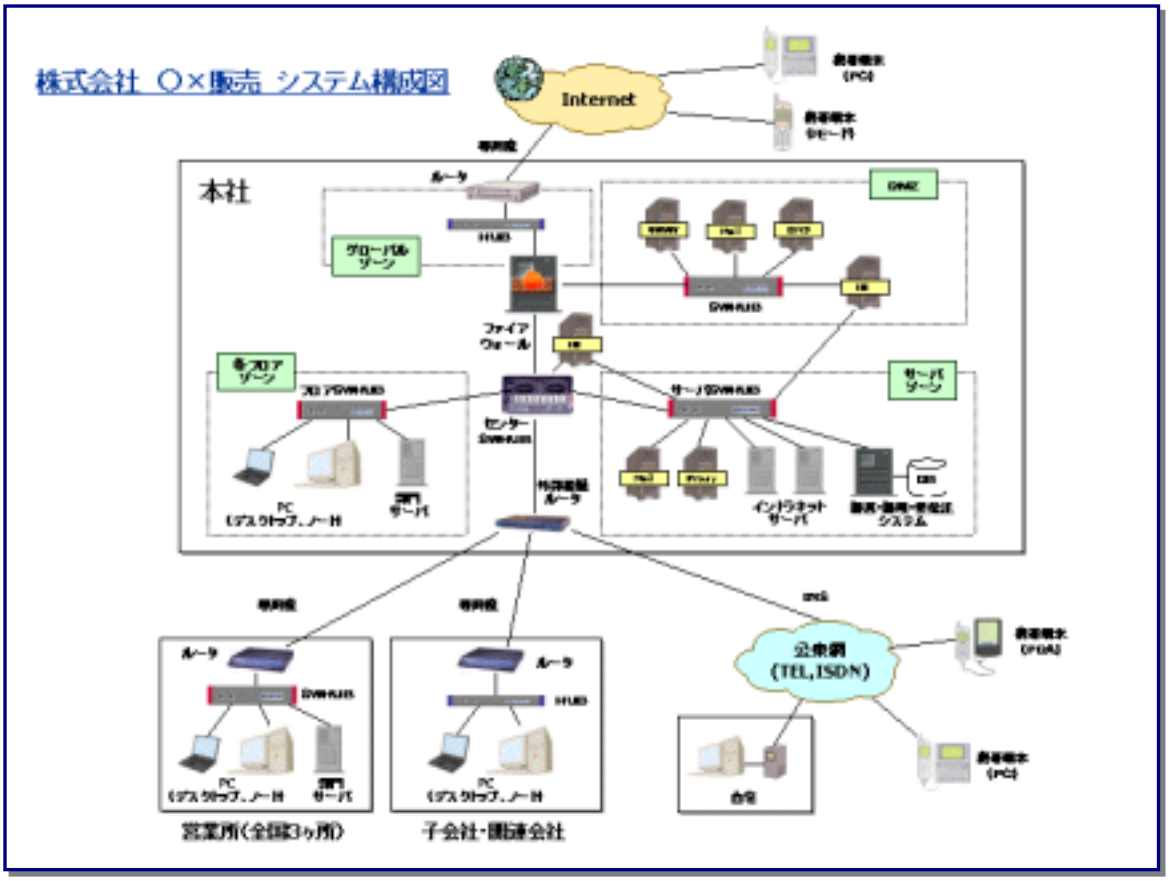
『情報セキュリティポリシー』は、当社の情報資産を、故意や偶然という区別に関係なく、改ざん、破壊、漏洩等から保護されるような管理策をまとめた文書である。

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。

当社の保有するシステムの具体例は、下図で示している範囲とする。



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より具体的に、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。したがって、一般には公表しない機密情報として取り扱わなければならない。以下、方針以外の文書は機密情報である。

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、機密保持契約を締結した上で、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。

７．４　脅威

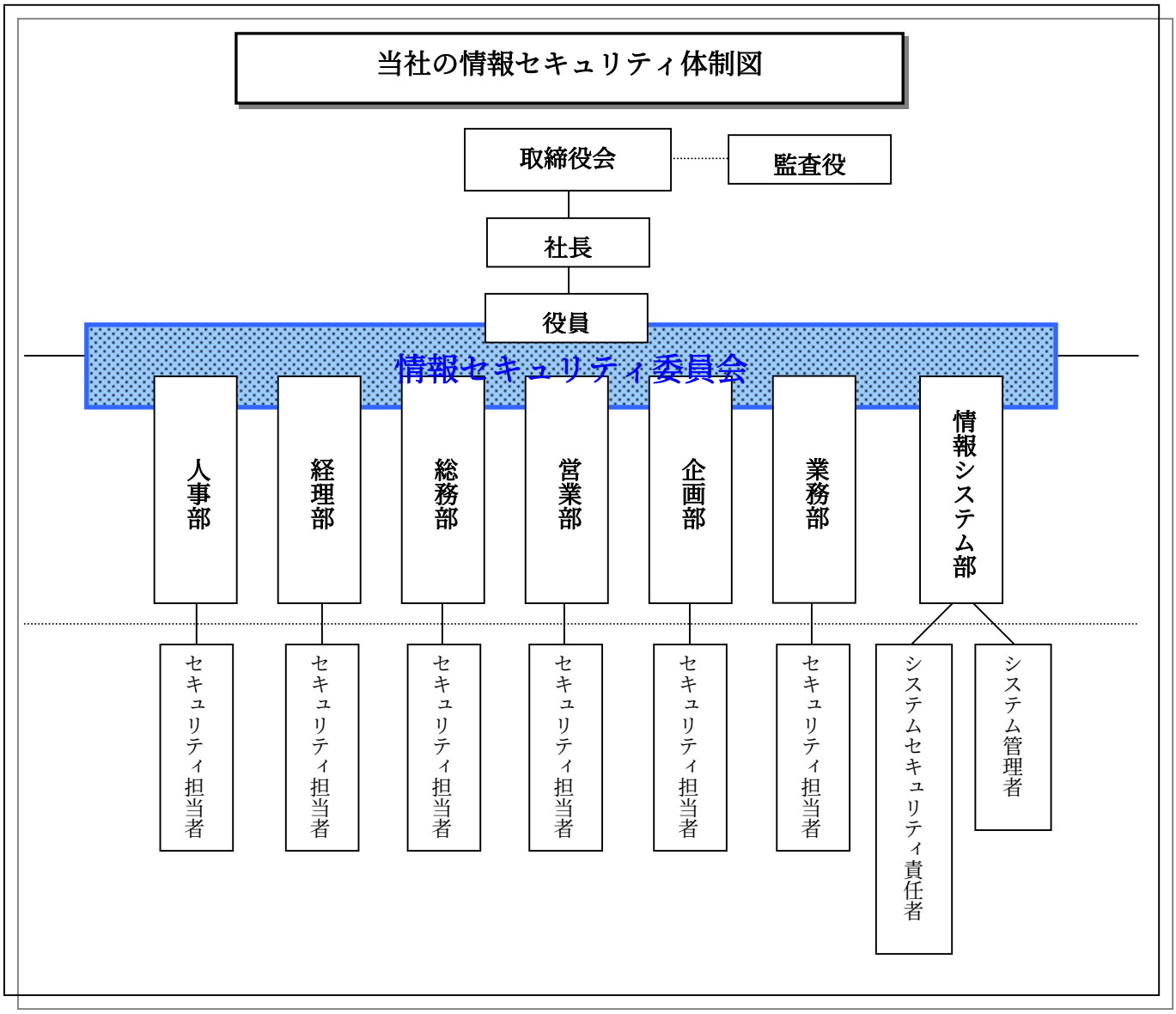
自然災害、機器障害、悪意のある行為等、損失を発生させる直接の要因のこととする。

７．５　脆弱性

建物の構造上の欠陥、定期点検の不備、情報セキュリティ規定・要員教育の不備等、脅威を発生し易くさせる要因、脅威を増加させる要因（脆さ、弱点）のこととする。

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の詳細情報に関しては、情報セキュリティ委員会構成メンバーを参照のこと。

８．２　情報システム部

情報システム部は、情報セキュリティ委員会で決定した対策事項を実施及び推進する担当部署とする。

情報システム部は、当社の情報機器の管理責任を有し、当社に関係するセキュリティ情報収集を行い、社内のセキュリティ対策に反映させなければならない。また、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。

８．３　システムセキュリティ責任者

システムセキュリティ責任者は、情報システム部に属し、システム管理者の作業責任を有する。

システムセキュリティ責任者の役割は、システム管理者への作業指示・管理を行い、システム管理者同士での作業の「相互牽制」及び「職務の分離」が有効に働くように配慮しなければならない。

８．４　システム管理者

システム管理者は、情報システム部に属し、システムセキュリティ責任者より与えられた管理作業の責任を有する。

システム管理者の役割は、管理を依頼された情報機器に対して、セキュリティ対策を実施する現場レベルでの責任者である。

８．５　オペレーター

オペレーターは、情報システム部に属し、システム管理者の管理下のもとで実質的な作業を行う者である。

８．６　セキュリティ担当者

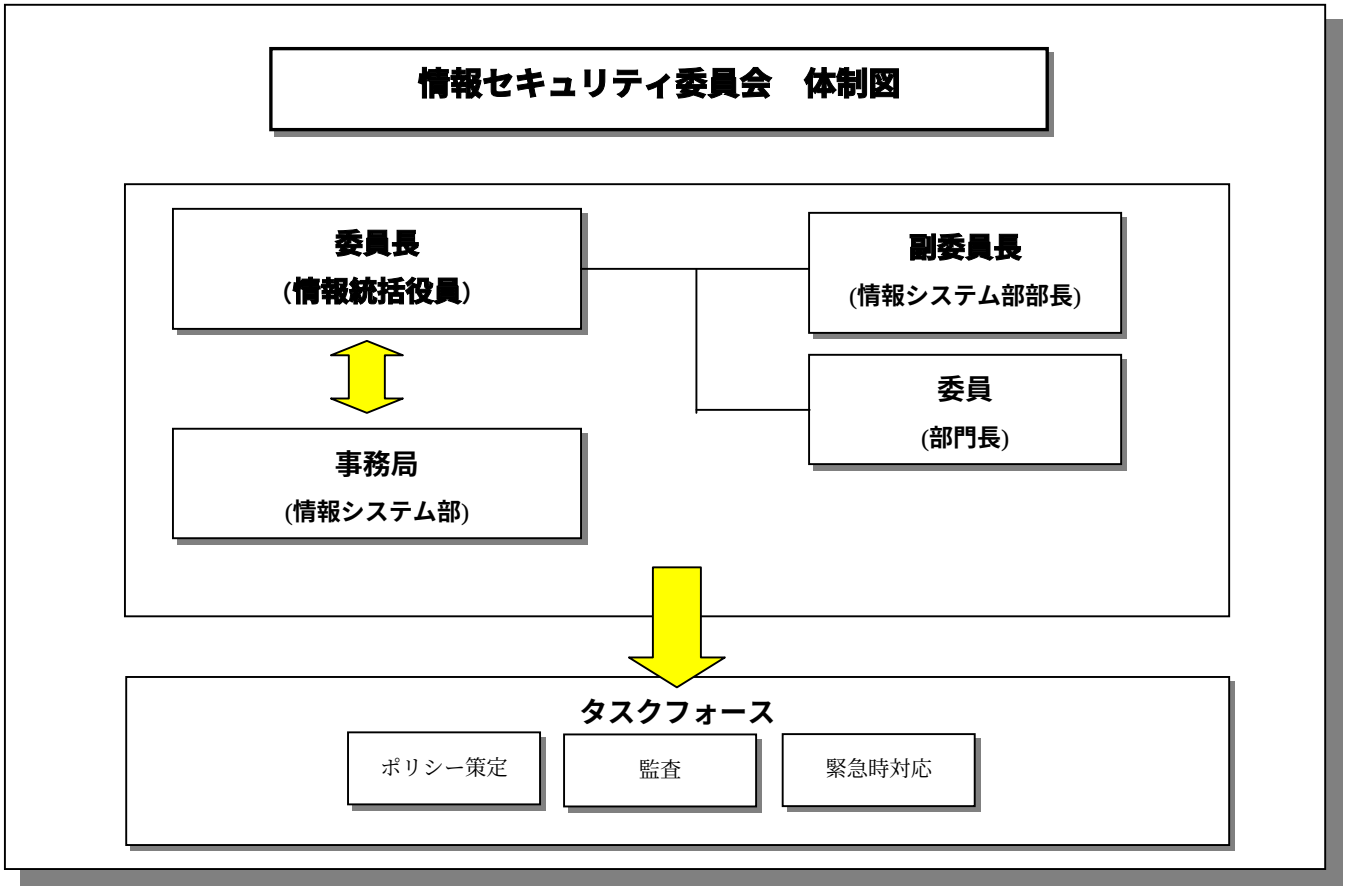
セキュリティ担当者は、情報システム部以外の各部署の部門長によって最低一人は任命され、配置される者である。

セキュリティ担当者の役割は、部門内におけるセキュリティ推進及び情報（社員のセキュリティ対策及び情報セキュリティマネジメントへの不平・不満及び問題点等）の収集担当であり、収集した情報は情報システム部へ報告する。

９　情報セキュリティ委員会の体制図及び構成メンバー

９．１　情報セキュリティ委員会の体制図

委員会の構成は下図の通り定める。



９．２　常勤委員

常勤委員は、委員長、副委員長、委員とする。常勤委員は、委員会が開催されたときは、必ず参加しなければならない。

９．３　非常勤委員

非常勤委員は、外部コンサルタント、法律専門家、システムセキュリティ責任者である。非常勤委員は、委員長によって召集されたときに参加する。

９．４　委員長

委員長は、当社の役員を情報統括役員として取締役会で指名する。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。

９．５　副委員長

副委員長は、情報システム部部長とする。副委員長は、委員長の補佐役である。委員長が万一職務を遂行することが不可能になった場合には、委員長の代理となって、職務を遂行する。

９．６　委員

委員は、各部門長とする。委員は、情報セキュリティ委員会への議題（社内及び社外で起きているセキュリティ事象への対応等）を提示することができる。

９．７　事務局

事務局は、情報システム部とする。事務局は、情報セキュリティ委員会を運営する上での事務作業を行う。

また、情報セキュリティ委員会で作成・策定した情報セキュリティマネジメント計画書や『情報セキュリティポリシー』文書の管理を行う。

９．８　タスクフォース

情報セキュリティ委員会は、各作業を実施するにあたってタスクフォースを設けることができる。このタスクフォースの責任者は、いずれかの委員とする。タスクフォースには、『情報セキュリティポリシー』策定、監査、緊急時対応等の作業を実施する。

１０　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。

１０．１　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。

１０．２　『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。

１０．３　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。

１０．４　『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。

１０．５　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。

１０．６　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。

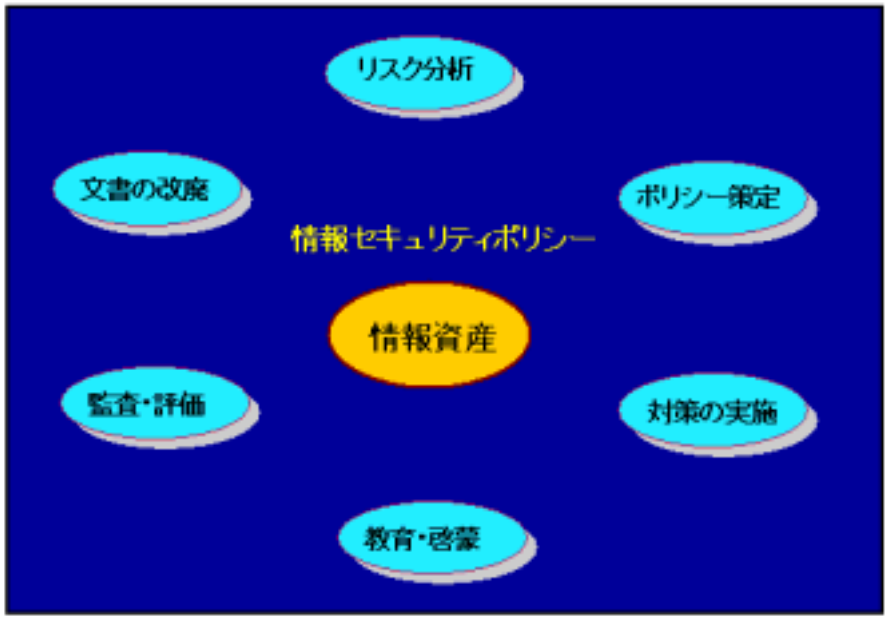
１０．７　『情報セキュリティポリシー』違反者への処罰

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部に申請することとする。

１１　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。

＜情報セキュリティマネジメントサイクル＞



１１．１　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。

１１．２　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。

１１．３　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。

１１．４　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。

１１．５　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。

１１．６　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。

１２　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。

１３　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。

１４　執行期日

本方針は、平成ｘｘ年ｘｘ月ｘｘ日に取締役会にて承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

情報セキュリティ対策標準

0.92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

情報セキュリティ対策標準（概要）

1　趣旨

当社は、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などの情報システム（以下、情報資産）を第４の資産と位置付け、この情報資産を重要な資産とし、保護・管理する「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。

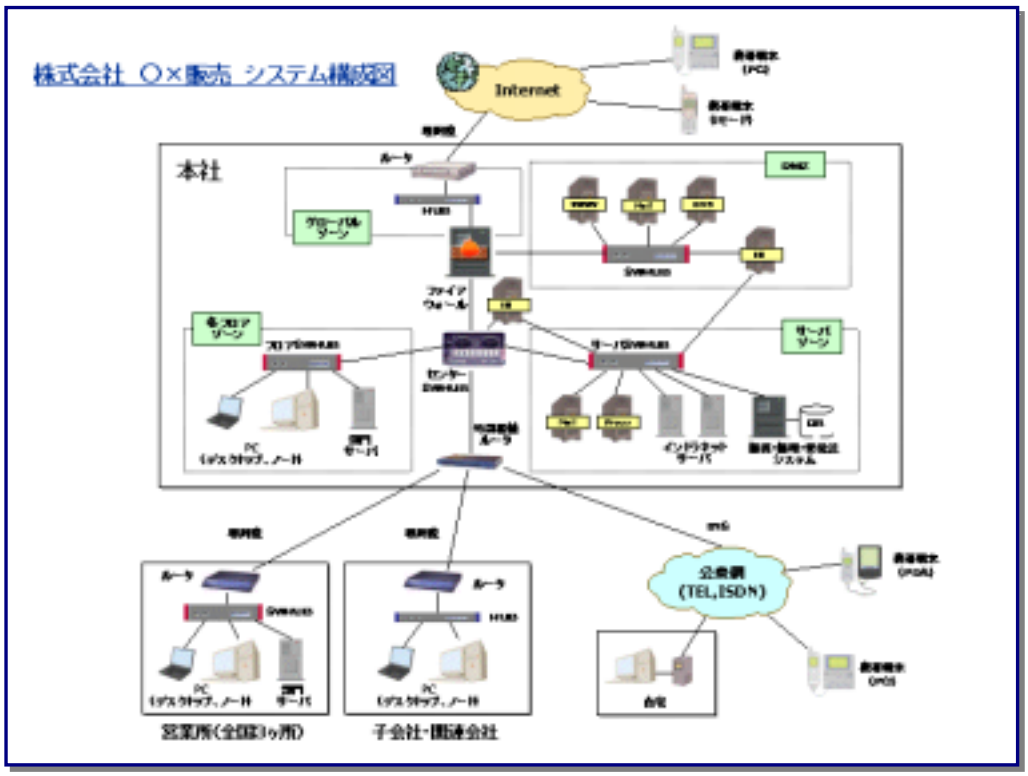
『情報セキュリティポリシー』は、「情報セキュリティ基本方針」＋「情報セキュリティ方針」と「情報セキュリティ対策標準」と「情報セキュリティ実施手順書」の３つの階層で策定・管理する。

「情報セキュリティ対策標準」は、「情報セキュリティ方針」に従い、情報資産を保護・管理するために遵守すべき事項を可能な限り具体的かつ網羅的に記載したものである。

2　対象範囲

「情報セキュリティ対策標準」の適用範囲（対象システム）は、当社の情報資産に関係する人的・物理的・環境的リソースを含むものとする。

当社の対象システムのシステム構成図を下図に示す。



3　適用者

「情報セキュリティ対策標準」は、当社のネットワークコンピュータを利用する全ての利用者に適用する。しかしセキュリティ対策の内容によって適用者が異なるため、各情報セキュリティ対策標準では適用者を明確に記載するものとする。

「情報セキュリティ対策標準」の適用者を、以下に示す。

（1） 当社の経営陣と従業員
（2） 子会社・関連会社の従業員
（3） 外部委託業者の従業員（派遣社員、アルバイトを含）

4　用語

「情報セキュリティ対策標準」で用いられる用語について、以下のように定義する。

(1)　情報セキュリティ方針

情報セキュリティ方針は、『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り、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。

(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は、方針の下層に位置する文書であり、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。

(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は、対策標準の下層に位置する文書であり、この文書は、情報セキュリティ対策標準で記述された文書をより具体的に、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)　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組織であり、全社的なマネジメント体制を整える。

(5)　情報システム部

情報システム部は、情報セキュリティ委員会で決定した対策事項を実施及び推進する担当部署で、当社の情報機器の管理責任を有し、当社に関係するセキュリティ情報収集を行い、社内のセキュリティ対策に反映、また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する。

(6)　システムセキュリティ責任者

システムセキュリティ責任者は、情報システム部に属し、システム管理者の作業指示・管理を行い、システム管理者同士での作業の「相互牽制」及び「職務の分離」が有効に働くように配慮する。

(7)　システム管理者

システム管理者は、情報システム部に属し、システムセキュリティ責任者より与えられた管理作業の責任を有し、管理を依頼された情報機器に対して、セキュリティ対策を実施する現場レベルでの責任者である。

(8)　オペレーター

オペレーターは、情報システム部に属し、システム管理者の管理下のもの実質的な作業を行う者である。

(9)　セキュリティ担当者

セキュリティ担当者は、情報システム部以外の各部署の部門長によって最低一人は任命され、配置される者であり、部門内におけるセキュリティ推進及び情報収集担当であり、収集した情報は情報システム部へ報告する。

上記以外で、各情報セキュリティ対策標準で用いられる用語については、別紙１に記載する。

5　セキュリティ対策標準構成

当社の『情報セキュリティポリシー』の情報セキュリティ対策標準は、その情報セキュリティ対策を２９の項目に分け策定・管理する。

以下に各情報セキュリティ対策標準の記載項目（ドキュメントの単位）を示す。

（１） ソフトウェア／ハードウェアの購入及び導入標準
（２） 委託時の契約に関する標準
（３） サーバルームに関する標準
（４） 物理的対策標準
（５） 職場環境におけるセキュリティ標準
（６） ネットワーク構築標準
（７） LAN における PC（サーバ、クライアント等）設置/変更/撤去の標準
（８） サーバ等に関する標準
（９） クライアント等におけるセキュリティ対策標準
（１０）社内ネットワーク利用標準
（１１）ユーザー認証標準

（１２） ウィルス対策標準
（１３） 電子メールサービス利用標準
（１４） Web サービス利用標準
（１５） リモートアクセスサービス利用標準
（１６） 媒体の取扱に関する標準
（１７） アカウント管理標準
（１８） システム維持に関する標準
（１９） システム監視に関する標準
（２０） プライバシーに関する標準
（２１） セキュリティ情報収集及び配信標準
（２２） セキュリティインシデント報告・対応標準
（２３） 監査標準
（２４） セキュリティ教育に関する標準
（２５） 罰則に関する標準
（２６） スタンダード更新手順に関する標準
（２７） 専用線及び VPN に関する標準
（２８） 外部公開サーバに関する標準
（２９） プロシージャ配布の標準

各情報セキュリティ対策標準（スタンダード）では、以下に示す項目の記載をしなければならない。

（1） 趣旨
（2） 対象者
（3） 対象システム
（4） 遵守事項
（5） 例外事項
（6） 罰則事項
（7） 公開事項
（8） 改訂

6 例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

7 罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『罰則に関する標準』に従う。

８　公開事項

本標準は対象者にのみ公開するものとする。

９　改訂

・本標準は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

アカウント管理標準

0.92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

アカウント管理標準

１　趣旨

アカウントは必要なユーザにのみ発行され、必要最小限の権限が与えられていなければならない。しかし、現実の組織運営においては、組織変更や人員異動などが頻繁に行われることが少なくないので、変化に追従しながらもセキュリティを保つ為に、本標準を遵守しなければならない。

２　対象者

① アカウントを管理するシステム管理者
② アカウントを使用している全利用者
③ 人事管理を行っている人事部
④ 人事権を持っている管理職

３　対象システム

アカウントを使用している全システム

４　遵守事項

４．１　新規アカウントの発行

（１） 新規のアカウントが必要になった場合には、必要な権限と共に人事権を持った管理者に申請する。
（２） 申請を受けた人事権を持った管理者は、必要な権限と必要性を検討し、妥当と判断した場合には、システム管理者に新規アカウントの発行を申請する。
（３） 申請を受けたシステム管理者は、申請を受けたアカウントに必要最小限のアクセス権限を設定する。
（４） アカウントに対応したパスワードは、『ユーザー認証標準』に従って慎重に設定しなければならない。
（５） メール送受信、ファイル共有、インターネットアクセスなど、基本的なアクセス権限については、別途標準的なアクセス権限の表を作って目安にすることが望ましい。

４．２　アカウントの変更

（１）　アカウントに与えられている権限を変更する場合には、新規アカウントの発行と同様に人事権を持つ管理職を通してシステム管理者に申請する。

（２）　人事権を持つ管理職は、現在部下に与えている権限に変更があった場合には、速やかに申請を行うように担当者に指示しなければならない。特に、権限の縮小が行われた場合には、業務上の不都合とは関係なく、セキュリティ上の理由から、速やかにアクセス権限の変更の申請を行わなければならない。

４．３　不要となったアカウントの削除

（１）　人事異動などで不要となったアカウントは、速やかに削除・停止にしなければならない。

（２）　人事部は、退職や休職などでアカウントが不要になったという情報を得た場合には、速やかにシステム管理者に通知し、アカウントを削除・停止しなければならない。

５　例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

６　罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『罰則に関する標準』に従う。

７　公開事項

本標準は対象者にのみ公開するものとする。

８　改訂

・本標準は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

用語：
アカウント
従業員
全ユーザ
社員
正社員
協力会社社員

外部公開サーバに関する標準

0.92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

外部公開サーバに関する標準

１　趣旨

本標準は、当社がシステムをインターネットに接続する場合に、ネットワーク犯罪の被害者や加害者、あるいは踏み台になることなく、円滑かつ効率的なビジネスを継続することを趣旨としている。

インターネットへの接続は、当社の業務効率の向上をもたらす反面、インターネット上の脅威にさらされる可能性もある。そのためインターネットへの接続にあたっては接続そのものの企画から、管理、運用まで慎重に行わなければならない。

当社は、外部へ公開する情報、情報システムに関して、セキュリティレベルの維持、向上、管理を趣旨として、以下の外部公開サーバに関する標準を実施する。

２　対象者

下記を本標準の遵守義務対象者とする。

・外部公開サーバの設置申請者
・システムおよびセキュリティ対策の設計者
・情報セキュリティ委員会
・システム構築担当者
・外部公開サーバのシステム管理者、オペレータ
・利用者（パスワード認証不要のアカウント利用者は除く）

３　対象システム

インターネットに接続し、不特定多数のインターネットユーザにＩＰアドレス及び情報を公開する情報システム、情報機器などを対象とする。対象システムの例としては外部公開サーバ（ウェブサーバ、メールサーバ、FTP サーバ、DNS サーバ、プロキシサーバなど）、ルータ、ファイアウォール及び外部公開サーバに情報を提供するデータベースサーバなどがある。

４　遵守事項

本標準の対象者は次に挙げる事項を遵守しなければならない。

なお、遵守事項は前述の対象手順のうち、セキュリティを考慮する上で特に留意が必要であると考えられる手順についてのみ記載しており、また遵守事項の記載順は対象手順の流れに沿うものとする。

４．１　システムおよびセキュリティ対策の設計に関する遵守事項

（１）　外部公開サーバの目的と公開情報の明確化

システムおよびセキュリティ対策の設計者（以下、システム設計者）は、外部公開サーバの設置の目的と当該サーバにて公開される情報を明確にしなければならない。また公開される情報に「顧客情報、プライバシー情報」などを含む場合は、『プライバシーに関する標準』を遵守しなければならない。

（２）　ネットワークの分離

システム設計者は、外部公開サーバと社内ネットワークの境界点にファイアウォールなどのようにアクセス制御が可能で、通信のログが取得できる機器を設置し、内外のネットワークを分離しなければならない。

（３）　リスク分析の実施

システム設計者は、外部公開サーバのセキュリティ設計を行う上で、必ずリスク分析を行わなければならない。リスク分析を行う上で、以下の項目を明確にしなければならない。

・保護・脅威の対象（守るべき情報）
・脅威
・脅威の原因、プロセス
・対策（予防、防御、検査、対応：回復）

（４）　ルータ及びファイアウォールなどによるアクセス制御

システム設計者は、ルータ及びファイアウォールなど、通信のアクセス制御が可能な機器ではアクセス制御に関して設計書を作成し、情報を公開する上で、必要最低限のアクセスのみ許可するようアクセス制御を実施し厳密に管理しなければならない。アクセス制御は、送信元及び送信先アドレスだけ、プロトコル、通信ポートでなく、時間や通信量などの制限も含まれる。これらのアクセス制御は、外部から外部公開サーバセグメントへのアクセス制御のみならず、外部公開サーバセグメントから外部へのアクセス制御も同様に、実施、管理しなければならない。

これらのアクセス制御の設計書は変更時を含めて、情報セキュリティ委員会に報告し、随時検査を受け、承認を得なければならない。システム管理者は、この変更履歴を保管管理しなければならない。

（５） OS、アプリケーション・サービスのアクセス制御

システム設計者は、OS のアクセス制御とアプリケーションとサービスのアクセス制御に関して、設計書を作成し、厳密にアクセス権を設定しなければならない。この設計書は、変更履歴を含めて保管管理しなければならない。

（６） データのアクセス制御

システム設計者は、データのアクセス制御に関して、設計書を作成し、厳密にアクセス権を設定しなければならない。この設計書は保管管理しなければならない。これらのデータには、OS のシステムファイルやアプリケーション、アプリケーション設定ファイルなども含まれる。これらの設計書は、変更履歴を含めて保管管理しなければならない。

（７） アプリケーション開発

システム設計者は、CGI、API などのアプリケーション開発を行う際、リスク分析を実施し、仕様書の段階から、データの入力チェックなどの、セキュリティ対策の実施を行わなければならない。

（８） 不正アクセス検知システム（IDS）について

システム設計者は、IDS を設置する場合、設計時に以下の作業を行わなければならない。

・適用するシグネチャの選定及び必要なシグネチャの作成
・対応手順の必要なシグネチャの選定と、その対応手順書の作成

（９） 外部公開サーバの推奨プラットホーム

情報システム委員会は、外部公開サーバに関して、推奨プラットホームを規定することが望ましい。システム設計者は外部公開サーバのプラットホームについては、情報セキュリティ委員会が規定する推奨プラットホームを採用することが望ましい。

（１０）設置場所

システム設計者は対象システムの安全な設置場所を検討しなければならない。

安全な設置場所とは、以下の条件を満たす場所を指す。

・施錠されていること
・明示的に許可された者以外の立ち入りが禁止されていること

・ネットワークの盗聴が外部から行えないこと
・監視カメラが設置されていること

（１１）セキュリティ侵害時の対応手順書の作成

システム設計者は、リスク分析で想定されるセキュリティ侵害が発生した場合の対応手順書を設計時に作成しなければならない。対応手順書には以下の項目が含まれていなければならない。

・想定されるセキュリティ侵害の可能性がある事象とその定義
・確認方法
・確認で得られ情報毎の対応方法
・連絡先及び緊急連絡先
・セキュリティ侵害事象の保存方法
・外部公開サーバの運用再開の基準

４．２　設置の申請・設計審査に関する遵守事項

（１）　申請書の提出

外部公開サーバの設置申請者（以下、申請者）は、外部公開サーバの設置の際、必ず情報セキュリティ委員会に「外部公開サーバ設置申請書」を提出し、許可を得なければならない。申請には、申請者の押印だけではなく所属長部長職相当の押印が必要である。

申請を受けた情報セキュリティ委員会は、直ちに審査を開始しなければならない。「外部公開サーバ設置申請書」には次の項目を含まなければならない。

・システム設置の趣旨と扱う情報の内容
・システム構成
・システムの設置場所の住所と組織名称
・システム管理者名とシステムセキュリティ責任者名
・運用開始希望日
・運用管理手順書の添付
・セキュリティ侵害時の対応手順書の添付

（２）　システム構成の明確化

申請者は、外部公開サーバの設置申請時にそのシステム構成を明確にしなければならない。情報セキュリティ委員会により、システム構成の不備もしくは、改善要求を受けたとき、申請者及びシステム設計者は、直ちに

システム構成の再検討を行わなければならない。

（３） 管理体制及びシステム管理者の明確化

申請者は情報及び情報システムの正しく安全な運用を確実にするために、管理体制及びシステム管理者を明確にしなければならない。人的不注意および故意の誤用のリスクを低減するために、システム管理者及びオペレータを２名以上任命しなければならない。

（４） 運用手順書の提出

申請者は、外部公開サーバの設置申請時に運用手順書を情報セキュリティ委員会へ提出なければならない。

（５） セキュリティ侵害時の対応手順書の提出

申請者は、外部公開サーバの設置申請時にセキュリティ侵害時の対応手順書を情報セキュリティ委員会へ提出しなければならない。

（６） 既存の外部公開サーバの申請について

本標準が適用される以前の既存の外部公開サーバについては、３ヶ月以内に本標準に適合するようにしなければならない。３ヶ月以内に、本標準に適合しない場合、情報セキュリティ委員会は情報の公開を強制的に停止させることができる。

４．３　システム構築に関する遵守事項

（１） 提供サービス

システム構築担当者は、外部公開サーバの趣旨、用途に応じた必要最低限のアプリケーション・サービス以外インストールしてはならない。

（２） 安全な設定

システム構築担当者は外部公開サーバに、安全な設定を施さなければならない。安全な設定とは、以下の要件を満たすものである。

・最新のOS
・最新のアプリケーション
・最新のセキュリティパッチの適用
・不要なプログラムやサービスの削除

（3） パスワード強度

ルータ、サーバなど全てのパスワードが利用できる機器には、パスワードを設定しなければならない。特にシステム管理者もしくはシステム管理者に類する権限を持つアカウントのパスワードは、下記のように厳重に設定されなければならない。

・システム管理者自身が設定する
・８文字以上
・大文字小文字の区別がある場合には大文字を１文字以上含める
・記号が含められる場合には１文字以上含める
・数字が含められる場合には１文字以上含める

４．４ 検査に関する遵守事項

・検査実施手順

外部公開サーバは、運用開始前に必ずシステム構築担当者が情報セキュリティ委員会が指定する第三者による検査を受けなければならない。検査には以下の項目を含まなければならない。

・最新の脆弱性情報を含む検査項目
・「外部公開サーバ設置申請書」との整合性
・許可された範囲以外へのアクセスが出来ないこと
・アクセスコントロール定義の確認
・不要なサービス、不要なアカウントが存在しないこと
・推測可能なパスワードが設定されていないこと

検査は、インターネット方向からだけでなく、様々な脅威を想定した方向から実施し、検査に合格するまでは接続試験や検査の目的以外で運用を開始してはならない。また、検査は定期的に実施するが、外部公開サーバが新設された場合及び、ルータ、ファイアウォールの設定変更された場合は随時検査を実施する。検査に不合格になった場合には、１週間以内に対策を行い、再検査を受け、以後これを繰り返す。

４．５ 運用に関する遵守事項

（1） セキュリティレベルの維持

システム管理者は、常に最新のセキュリティ情報を入手し、OS 及びインストールされた、アプリケーション・サービスについて、随時、必要な最

新のアプリケーションのバージョン、セキュリティパッチを適用しなければならない。また、これらの履歴は保管管理しなければならない。OS 及びインストールされたアプリケーション・サービスに関するセキュリティホールのうち深刻なものであると判断され、かつセキュリティパッチが公開されていないものについては、別方法のセキュリティ対策の検討し、その施策を実施しなければならない。検討の結果、セキュリティ対策が無いと判断された場合は、速やかに情報セキュリティ委員会に報告し、情報の公開を停止しなければならない。この停止は、対応のセキュリティパッチの適用もしくは別の施策が実施にて、セキュリティ委員会に報告後、解除できる。

（２） 外部公開サーバのアカウント管理

システム管理者は、外部公開サーバの趣旨、用途に応じた、必要最低限のアカウント以外作成してはならない。また、アカウント毎のアクセス権を規定し、必要最低限のアクセス権のみ付与しなければならない。これらのアカウントは更新履歴を含めて、管理しなければならない。パスワードが必要なアカウントについては、適切なパスワード強度を有しなければならない。

（３） パスワード管理

設定されたパスワードには、以下の運用がなされなければならない。

・１ヶ月に一度必ず更新されなければならない
・同じパスワードを異なる機器、異なる時期に使用してはならない
・設定されたパスワードは、システム管理者が責任を持って携行及び保管する手帳類以外には書き留めてはならない
・緊急時（現場に行くことができない場合等）を除いて、システム管理者以外に教えてはならない。
・パスワードを入力する際は、他人に見られないよう注意しなければならない

（４） 運用業務の委任

システム管理者の運用業務はオペレータに委任することができるが、オペレータは運用手順書以外の操作を行ってはならない。

（５） 運用日誌

システム管理者は、次の項目を含んだ運用日誌を作成し一定期間、保管

管理しなければならない。

・システムへのログイン時間とログオフ時間
・システムの設定変更内容
・ログの保存記録
・バックアップ実施記録
・システムエラーの記録とその是正処置

また情報セキュリティ委員会は、定期的に運用日誌を検査し不適切な記載が発見された場合、適切な是正処置をシステム管理者に指導しなければならない。

（6） 入退室管理

システム管理者は、全ての外部公開サーバの設置場所への入退室記録を保管管理しなければならない。これらの機器のディスプレイ及びコンソールは離席時を含めて、システム管理者及び、オペレータ以外操作、目視できないように必ず、ログアウトもしくはパスワードで保護された状態にしなければならない。

（7） リモートメンテナンス

システム管理者は、外部公開サーバの情報及びデータを、ネットワークを利用し更新・メンテナンスを行う必要がある場合は、その手順を明確に規定しなければならない。システム管理者は、リモートからの情報の更新手順書を作成し、リモートメンテナンスを実施する者に配布、徹底させなければならない。

（8） ログの取得について

外部公開サーバのOS 及びアプリケーション監査ログは次の項目を含めなければならない。

・ユーザID
・ログオン及びログオフの日時
・端末のIP アドレスもしくは端末のID
・OS もしくはアプリケーションへのアクセスを試み、成功したものと、失敗したものの記録
・内部エラー

ファイアウォールおよびルータなど通信経路に設置される機器のログは次の項目を含めなければならない。

・アクセス日時
・プロトコル番号
・ソースIP アドレス
・ソースポート
・ディスティネーションポート
・ディスティネイションIP アドレス
・許可しているアクセス及び、許可していないアクセス

（９） ログの保存

ログは、一時的にハードディスクなどの書き換え可能なメディアに保存されていても良いが、２４時間以内に書き換え不能なメディアに転送され厳重に保管されなければならない。一時的にハードディスクなどの書き換え可能なメディアにログを記録する場合には、十分な記憶容量を確保しておき、異常な量の書き込みが発生した場合においても十分に対処できるように備えておかなければならない。ログは、その取得日から３年間は確実にシステムセキュリティ責任者のみが参照できる場所と方法で厳重に保管されなければならない。

（１０）ログの解析

保存されたログは、システムセキュリティ責任者もしくはシステムセキュリティ責任者からに委任を受けたシステム管理者により解析されなければならない。

ログの解析は少なくとも１ヶ月に１回以上定期的に行わなければならず、セキュリティ侵害や、その可能性がある場合は随時行わなければならない。

ログの解析を行う際は以下の点に注意しなければならない。

・許可されていないIP アドレス
・指定時間外のアクセス
・アクセス頻度
・データ量
・度重なるアクセス失敗

（１１）時間の同期

システム管理者は、ログの精度及び、ログの証拠としての信頼性を確保するために、外部公開サーバの時間の同期を行わなければならない。

（１２）外部公開サーバ情報のバックアップ

システム管理者は、対象システムに保存されるデータとシステムの設定情報をそれぞれ一定期間毎にバックアップをとり、保管管理しなければならない。

（１３）セキュリティ侵害時の対応

システム管理者は、セキュリティ侵害が発生した場合、セキュリティ侵害時の対応手順書に則って対応しなければならない。
またシステム管理者は、セキュリティ侵害時の情報を、できるだけ速やかに、情報セキュリティ委員会に報告しなければならない。
情報セキュリティ委員会は、前述の報告を受けた後、各行政機関への通報を含めて迅速に対応しなければならない。

（１４）想定外のセキュリティ侵害への対応

万が一、想定外のセキュリティ侵害が発生し、セキュリティ侵害時の対応手順書のみでは状況の改善が見込めない場合、システム管理者は即座に情報セキュリティ委員会に報告しなければならない。システム管理者は、情報セキュリティ委員会の指示のもと、手順書外の行為を行うことができる。但し、作業実施記録は詳細に記録しなければならない。

またシステム管理者は、状況の改善後、作業実施記録を元にセキュリティ侵害時の対応手順書を更新しなければならない。

（１５）セキュリティ侵害時の対応手順書の更新

システム管理者は、セキュリティ侵害時の対応手順書の実効性を維持するため、適宜更新しつづけなければならない。

5　例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

6　罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『罰則に関する標準』に従う。

7　公開事項

本標準は対象者にのみ公開するものとする。

8　改訂

本標準は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

サーバ等に関する標準

0.92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

サーバ等に関する標準

１　趣旨

本標準は各サーバのＯＳを含めたソフト、ハード、及び、運用の規定をし、サーバに格納されている情報の保護を目的とする。

２　対象者

当社の全てのサーバ管理者、システム構築者。

３　対象システム

本社・営業所・子会社・関連会社を含む、全てのサーバシステム。

４　遵守事項

４．１ 導入時の規定

（１）サーバ管理者はサーバの設置場所をサーバルームまたは、それに準ずる安全な場所に設置しなければならない。

（２）サーバ管理者はサーバを設置する際はサーバ設置申請書を作成し、情報セキュリティ委員会で認可を受けなければならない。

（３）サーバ管理者は、サーバの設置申請時にそのシステム構成を明確にしなければならない。情報セキュリティ委員会により、システム構成の不備もしくは、改善要求を受けたとき、サーバ管理者は、直ちにシステム構成の再検討を行わなければならない。

（４）サーバ管理者は情報及び情報システムの正しく安全な運用を確実にするために、管理体制及びサーバ管理者を明確にしなければならない。人的不注意および故意の誤用のリスクを低減するために、サーバ管理者及びオペレータを２名以上任命しなければならない。

（５）サーバ管理者はサーバの設置申請時に運用手順書を作成し、情報セキュ

リティ委員会へ提出なければならない。
但し、侵害時対応手順が運用手順書に含まれる事。

（6）本標準が適用される以前の既存のサーバについては、3ヶ月以内に本標準に適合するようにしなければならない。3ヶ月以内に、本標準に適合しない場合、情報セキュリティ委員会は情報の公開を強制的に停止させることができる。

4．2　環境設定の規定

（1） サーバ管理者はサーバで使用するＯＳ及び、ソフトウェア（ウイルス対策ソフト、脆弱性検査ソフトを含む）は情報セキュリティ委員会が規定したものを使用しなければならない。

（2）サーバ管理者はＯＳのアクセス制御、ファイルのアクセス制御、アプリケーション、サービスのアクセス制御に関して、厳密にアクセス権を設定しなければならない。

（3）サーバ管理者、システム構築者はユーザー、ＷＥＢアクセスなどに使用する匿名ユーザーアカウントを含む全てのアカウントのアクセス権限に対して、必要最低限のアクセス権限のみ許可しなければならない。

（4）システム構築者は、CGI、API などのアプリケーション開発を行う者にリスク分析を実施し、仕様書の段階から、データの入力チェック、内部でのデータの処理プロセス、出力されるデータの妥当性などの、セキュリティ対策の実施を義務づけなければなければならない。

（5）システム構築者は、サーバの趣旨、用途に応じた必要最低限のアプリケーション・サービス以外インストールしてはならない。

（6）サーバには、推測困難なパスワードを設定しなければならない。特にサーバ管理者もしくはサーバ管理者に類する権限を持つアカウントのパスワードは、厳重に管理されなければならない。

４．３　運用時の規定

（１）　サーバ管理者はサーバで使用されるソフトウェアは常に最新のＯＳ、最新のアプリケーション、最新のセキュリティパッチの適用、不要なサービスの削除を常に行わなければならない。

（２）　サーバ管理者はウイルス対策として常にウイルス定義ファイル、ウイルス対策システムが最新のものとなるよう情報を収集し、更新があった場合は直ちに反映を行い、サーバのウイルスチェックを行わなければならない。

（３）　サーバ管理者はサーバのパスワードを定期的にこれを変更しなければならない。

（４）　サーバ管理者はサーバのログの取得を行わなければならない。

（５）　サーバ管理者は定期的にサーバのログを一定期間分、媒体に保存を行わなければならない。

（６）　サーバ管理者は定期的にログの解析を行わなければならない。

（７）　サーバ管理者は定期的にサーバ内の情報のバックアップを行わなければならない。

（８）　サーバ管理者は定期的に第三者による検査を受けなければならない。

・脆弱性検査ソフトによる最新の脆弱性情報を含む検査
・「サーバ設置申請書」と実際の設置機器との整合性
・不要なアクセス権が存在しない事
・不要サービスの起動が存在しない事
・不要なアカウントが存在しない事
・推測可能なパスワードが設定されていない事

（９）　第三者による検査結果は必ず記録し、一定期間保管しなければならない。

（１０）第三者による検査によりセキュリティの不備が発見された場合は直ちに不備を是正し、不備の内容と対策状況を情報セキュリティ委員会に報告する。

（１１）セキュリティ侵害が発生した場合、セキュリティ侵害時の対応手順に則って対応しなければならない。
また、サーバ管理者は、セキュリティ侵害の状況を、できるだけ速やかに、情報セキュリティ委員会に報告しなければならない。
情報セキュリティ委員会は、前述の報告を受けた後、各行政機関への通報を含めて迅速に対応しなければならない。

（１２）万が一、想定外のセキュリティ侵害が発生し、セキュリティ侵害時の対応手順のみでは状況の改善が見込めない場合、サーバ管理者は即座に情報セキュリティ委員会に報告しなければならない。サーバ管理者は、情報セキュリティ委員会の指示のもと、手順書外の行為を行うことができる。但し、作業実施記録は詳細に記録しなければならない。

（１３）また、実効性を維持するため、適宜更新しつづけなければならない。

5　例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

6　罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『罰則に関する標準』に従う。

7　公開事項

本標準は対象者にのみ公開するものとする。

８　改訂

・本標準は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

ソフトウェア／ハードウェアの購入及び導入標準

0.92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

ソフトウェア／ハードウェアの購入及び導入標準

1　趣旨

本標準は、当社の業務で使用するソフトウェア／ハードウェアの標準製品を定めて運用管理することにより、全社的に統一されたセキュリティ対策の実現を容易にし、管理の効率化を図り、導入時の設定ミス等を防止することを目的とする。

2　対象者

本標準は、業務で使用するソフトウェア／ハードウェアの購入／導入を行うすべての従業員と、情報システム部、情報セキュリティ委員会のメンバーを対象とする。

3　対象システム

本標準は、当社の業務で使用するために購入／導入する、ソフトウェア／ハードウェア（PC、ネットワーク機器、OS、アプリケーションソフトウェア等）を対象とし、顧客に納品されるものは対象外とする。

本標準は、ハードウェアのうち、情報（機器の設定等を含む）を保管できるものを対象とする。

4　遵守事項

4．1　標準製品リストの作成

（1） 情報セキュリティ委員会は、当社の一般的な業務で使用する以下の標準製品を定め、標準製品リストを作成し、すべての従業員に通知しなければならない。

・PC
　－デスクトップ PC、ノート PC、サーバ機等
・ネットワーク機器
　－ルータ、スイッチングハブ等
・必須導入のソフトウェア
　－OS、OS に付随するユーティリティ
　－文書作成、表計算、プレゼンテーション支援のソフトウェア

－ウィルス対策ソフトウェア
－電子メールソフトウェア、Web ブラウザ
－業務アプリケーション
・選択して導入されるソフトウェア
－暗号化ソフトウェア
－圧縮・解凍ソフトウェア
－文書閲覧ソフトウェア

（２） すべての従業員は、業務上の正当な理由があり、セキュリティ委員会から標準外製品の購入／導入を承認された場合を除き、標準製品リストで定められた製品を購入／導入しなければならない。

（３） 情報セキュリティ委員会は、標準製品を決定するにあたり、必要なセキュリティ機能、スペックを備え、サポート、ライセンス条件、価格、などの条件が適切であることを評価しなければならない。さらに、既存の情報システムと問題なく動作できるものを選択しなければならない。
製品のセキュリティホール情報やその他の不具合に関する情報の提供、パッチ発行等の対応が悪い製品は、標準製品に指定してはならない。

（４） 情報セキュリティ委員会は、標準製品リストを定期的（年一回）に審議し、変更が生じた場合には、速やかにすべての従業員に通知しなければならない。

（５） 情報システム部は、セキュリティ上の問題やその他のトラブルを防止するために、標準製品の適切な設定を検証して決定し、設定ミスを防止するために、設定マニュアルを作成しなければならない。

４．２　標準製品の購入／導入

（１） 情報システム部は、標準製品の発注、保守契約、ライセンス、インストールメディア等を一括して管理する。

（２） 標準製品の購入を行う従業員は、申請書を情報システム部宛に提出しなければならない。

（３） 情報システム部は、申請を受けた標準製品の発注処理を行い、必須導入ソ

フトウェアのインストールと設定、ネットワーク接続の設定、各種ソフトウェアの最新パッチを適用した上で申請者が指定した場所に納品する。
製品購入時にインストールされているものや、OS に付属するソフトウェアであっても、標準製品として認められないものは、排除してから納品する。

（4） 情報システム部は、購入処理を行った製品を管理台帳に登録しなければならない。

（5） 情報システム部は、各部署からの申請により、再インストール等のためにライセンス上問題のないインストールメディアの貸し出しをする。
情報システム部は貸し出し記録を作成し、管理しなければならない。

４．３　標準外製品の購入／導入

（1） 研究、開発、その他業務上の理由で、標準外製品を購入／導入する必要がある従業員は、情報セキュリティ委員会宛に、標準外製品を使用する理由、製品名、製品の種類、管理者等の必要事項を明記し申請を行わなければならない。

（2） 標準外製品の申請を受けた情報セキュリティ委員会は、申請の妥当性を討議し、結果を申請者に通知する。

（3） 情報セキュリティ委員会の承認を得て標準外製品の使用を行う従業員は、標準外製品の使用を停止した場合、情報セキュリティ委員会宛に使用停止の申請をしなければならない。

（4） 情報セキュリティ委員会は、使用許可を行った標準外製品を情報システム部に通知し、情報システム部は、標準外製品を管理台帳に登録しなければならない。

（5） 情報セキュリティ委員会は、標準外のネットワークソフトウェアに対して使用許可を行った場合、セキュリティ関連の情報収集担当者に通知しなければならない。また、当該製品の使用者から使用停止の申請があった場合も通知しなければならない。

（6） 情報セキュリティ委員会は、標準外のネットワークソフトウェアに対して使用許可を与えない場合、情報システム部を通じて、社内ネットワークから切り離した、独立の環境を構築して業務上の要求が達成できるよう指導しなければならない。
情報システム部は、社内ネットワークから切り離した環境で使用されていることを、３ヶ月を超えない期間毎に、使用部署には通知せず確認しなければならない。独立の環境を使用している部署は、その環境が不要になった場合、速やかに情報システム部に通知しなければならない。

（7） 標準外製品の購入／導入を行う部署は、自部署の責任において購入／導入の手続きを行い、ライセンス、インストールメディアの管理を厳密に行わなければならない。

（8） 標準外製品の購入／導入を行う部署は、事前に、既存の情報システムへの影響を検討し、セキュリティ上の安全性を確認し、情報システム部のチェックを受けてから使用しなければならない。

（9） 情報セキュリティ委員会は、既存の情報システムにセキュリティ上やその他のトラブルが発生した場合、標準外製品の購入／導入を行う部署に対し、当該製品の設定変更や社内ネットワークからの切り離し、当該製品の使用停止等を命じることがある。

４．４　ネットワーク機器の購入／導入について

（1） 情報システム部は、本社内のグローバルゾーン、DMZ、サーバーゾーン、各フロアゾーンのフロア SWHUB までのエリアに設置するネットワーク機器（ルータ、スイッチングハブ等）の購入／導入を行い、許可無く各部署にて購入／導入を行ってはならない。

（2） 情報システム部は、『ネットワーク構築基準』に基づき、主要なネットワーク機器の導入を行わなければならない。

（3） （1）で指定する以外のエリアに設置するために、各部署にてネットワーク機器を購入する場合も、標準製品として指定されている製品を使用することが望ましい。各部署にて購入した製品は、管理台帳に登録するため、情報システム部に申請しなければならない。購入した製品は、自部署にて

管理するものとする。

４．５　管理台帳の作成／管理

（１） 情報システム部は、申請された情報を元に PC やネットワーク機器の管理台帳を作成し、新規登録、変更、削除を管理しなければならない。

（２） 管理台帳には、標準製品、標準外製品の両方を登録しなければならない。

5　例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

6　罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については罰則に関する標準に従わなければならない。

7　公開事項

本標準は対象者にのみ公開するものとする。

8　改訂

・本標準は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

ユーザ認証標準

0.92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

ユーザ認証標準

１　趣旨

本標準は、情報を守る為に使用されるユーザ認証に関して、セキュリティを確保しつつ利便性を実現する運用を目的として記述されている。パスワードの長さや文字の種別、更新頻度、対象機器については、実現方法に関する技術の進歩が著しいので、技術動向を見極めた上で、本標準が適宜更新されることが望ましい。

２　対象者

ユーザ認証を行わなければならない全ての従業員

３　対象システム

以下のいずれかの条件を満たす機器、システム及びアプリケーションには、ユーザ認証を用いて情報セキュリティの確保に努めなければならない。

① 汎用的に使われている OS などでネットワーク機能を持つ機器
② ハードディスクなどの記憶媒体を持つ機器
③ ルータ
④ ユーザが用いるメールソフトウェア
⑤ 社内情報共有の為のイントラネットソフトウェア

４　遵守事項

４．１　ユーザ認証を用いたセキュリティ確保

情報セキュリティの維持に影響を与える機器、システム及びアプリケーションで、ユーザ認証を行える機器、システム及びアプリケーションの中で、セキュリティ上重要な意味を持つにも関わらず、ユーザ認証が無い機器、システム及びアプリケーションは使用してはならない。

４．２　対象システムによる認証システムの選定

情報システム部門は、対象システムが関わる重要性と、セキュリティを実現する手法の難易度を勘案してユーザ認証システムを構築しなければならない。情報システム部門は、ユーザ認証の仕組みには、パスワードと生体認証のいず

れかを用いて情報システムを構築しなければならない。

４．３　パスワード

（１） 8 文字以上で記号を 1 文字以上含むことが望ましい。

（２） 一般に使われている単語や本人の趣味、プライベートなどから、他人に推測されやすいパスワードを使用してはならない。

（３） 設定されたパスワードは１ヶ月に一度を目安にパスワードは更新することが望ましい。

（４） パスワードは原則として該当システムの管理者が生成して管理を行うものとする。設定したパスワードは紙などに書き留めてもよいが、対象システムが特定できたり、パスワードの文字列そのものを「あらわに」書き留めたりしてはならない。

（５） パスワードは口外したり、ヒントとなるような物品を身の回りに置いておいてはならない。

（６） 一度使用したパスワードを連続でなくとも使用してはならない。

（７） 一度使用したパスワードを他のシステムなどに使用してはならない。

４．４　初期設定のパスワード

（１） 利用者が最初に使用する初期設定のパスワードは、情報システム部が発行し、口頭もしくは書面で該当者に通知する。

（２） 初期設定のパスワードは、社員番号などの規則性のある予測できるものに設定してはならない。

（３） 利用者はパスワードが発行された後速やかに自らログインしパスワードを変更しなければならない。

（４） システム管理者は、初期設定のパスワードが発行された利用者がログインしパスワードが変更されたことを確認しなければならない。原則として、初期設定のパスワードが発行されてから３日以内に、パスワードの設定変更が確認されない場合には、該当する利用者のアカウントを削除、もしくは無効にしなければならない。

４．５　パスワードを忘れた場合の処置

（１） 利用者がパスワードを忘れた場合には、システム管理者に新規パスワード発行の申請を行わなければならない。

（２） システム管理者は、申請してきた利用者が本当に本人自身であることを何らかの方法で確認しなければならない。

（３） 新規パスワード発行の申請を受けたシステム管理者は、速やかに新規のパ

スワードを発行して、利用者に通知しなければならない。

４．６　ワンタイムパスワード

（１） ワンタイムパスワードは PIN 番号などの認証が必要なものを用いなければならない。

（２） 時刻同期などの認証を必要としない機器は使用してはならない。

（３） ワンタイムパスワードの発生器は、PIN 番号などを推測出来るような状態で携帯してはいけない。

４．７　生体認証

（１） パスワードの記憶と管理が困難な場合には、生体認証を用いても良いが、最新技術動向やコストなどを勘案して、適切な方式を選択しなければならない。

（２） 生体認証を使用する場合には、生体認証のデータそのものが重要な個人情報であるので、厳重に管理しなければならない。

（３） パスワードの利用に対する利便性向上の手段としては、指紋認証などの簡単な生体認証を用いることができる。

（４） サーバルームなどの高いセキュリティを要求される場所への立ち入りの管理には、虹彩認証などの高レベルのセキュリティが期待できる認証システムを用いなければならない。

５　例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

６　罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『罰則に関する標準』に従う。

７　公開事項

本標準は対象者にのみ公開するものとする。

８　改訂

・本標準は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

用語：
ユーザ認証
利用者
情報セキュリティ委員会
PC
ソフトウェア
Web ブラウザ
常時設置型コンピュータ
携帯端末
生体認証
情報システム部

クライアント等におけるセキュリティ対策標準

0.92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

クライアント等におけるセキュリティ対策標準

１　趣旨

本標準は、クライアント PC 上の機密性・完全性を確保し、発生し得る各種問題を未然に防ぐことを目的とする。

２　対象者

PC を利用するすべての従業員

３　対象システム

当社より支給・貸与された PC
※本標準内では、「PC」はノートパソコンを含んだクライアントマシンのことを指し、「ノートパソコン」は、ノートパソコンのみを指します。

４　遵守事項

４．１　私物 PC の使用禁止

（１）　当社の業務において、従業員が使用できる PC は、当社が支給・貸与した PC のみとする。

（２）　いかなる場合でも、当社システム環境に私物 PC を接続・利用してはならない。

４．２　PC に導入するソフトウェア

（１）　当社が支給・貸与する PC は、『ソフトウェア／ハードウェアの購入及び導入標準』で規定されたソフトウェアを導入することとする。したがって、それ以外のソフトウェアを導入してはならない。

（２）　（１）にて指定したソフトウェア以外で、業務上やむを得ず導入しなけれ

ばならないソフトウェアは、情報システム部に申請し、許可を得なければならない。

（3） 導入したソフトウェアは、常に最新の状態で使用することとし、情報システム部が提供するソフトウェア情報をもとに修正プログラム等を導入しなければならない。

４．３　PC の他者への利用の制限

（1） 席を離れる場合、第三者が無断で PC を利用できないように PC にロックを掛けなければならない。

（2） 『ユーザ認証標準』に従い、PC に対するパスワード管理を徹底しなければならない。

（3） ノートパソコンでは、基本認証以外にも BIOS 上での認証を行うようにしなければならない。

４．４　PC での情報の取り扱い

（1） PC で機密情報を取り扱う場合、長期期間その情報を利用する場合には、機密情報を取り扱う許可を情報システム部に申請し、許可を得なければならない。許可を得た機密情報は、万一の漏洩に備え、暗号化等の対策を実施しなければならない。

（2） PC で一時的に機密情報を取り扱う場合、取り扱い後には、不必要となった情報を削除し、いつまでも保持してはならない。

４．５　ウィルス対策の徹底

（1） PC を利用するすべての従業員は、PC を利用する上でウィルス対策を徹底しなければならない。

（2） 『ウィルス対策標準』に規定されている遵守事項を徹底しなければならない。

４．６　PC の移設

（１） PC を利用するすべての従業員は、PC を勝手に移設してはならない。

（２） PC の移設が必要な場合には、情報システム部に申請し、許可を得なければならない。

４．７　ノートパソコンの利用上の注意事項

（１） 社外にノートパソコンを持ち出す場合、盗難・窃盗に注意し取り扱わなければならない。

（２） 社外でノートパソコンを利用する場合、情報の盗み見に注意し利用しなければならない。

５　例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

６　罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『罰則に関する標準』に従う。

７　公開事項

本標準は対象者にのみ公開するものとする。

８　改訂

・本標準は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情

報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

電子メールサービス利用標準

0.92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

電子メールサービス利用標準

１　趣旨

本標準は、電子メールで受け渡される情報の安全性を確保し、電子メール利用にあたって発生し得る各種の問題を未然に防ぐことを目的とする。

２　対象者

電子メールサービスを利用するすべての当社正社員、パート、アルバイト、契約社員とする。

３　対象システム

当社より発行された電子メールアドレスを用いてメールの送受信を行う pc とする。

４　遵守事項

４．１　電子メールサービス利用端末機器のセキュリティ

（１） 電子メールの送受信にあたっては、情報セキュリティ委員会が指定した電子メールソフトウェアを用いなければならない。また、情報セキュリティ委員会の指示に従い、当該ソフトウェアのバージョンアップを行わなければならない。

（２） 上記ソフトウェアを使用するコンピュータは、『ソフトウェア/ハードウェアの購入および導入標準』に基づいて導入され、『クライアント等におけるセキュリティ対策標準』に基づいたセキュリティ対策を施したものでなければならない。

（３） 電子メールアドレスは初期パスワードとともに発行される。初期パスワードは直ちに変更しなければならない。また、パスワードは最低 3 ヶ月に 1 度、定期的に変更しなければならない。設定するパスワードは、『パスワードに関する標準』に則ったものとする。

（4） 電子メールソフトウェアの利用にあたっては、パスワードを保存してはならない。電子メールソフトウェア起動時にユーザ認証を必要とする設定にしなければならない。

4．2　電子メールで送受信される情報の保護

（1） 当社の事業に関わる情報や、顧客、従業員のプライバシーに関わる情報などの機密情報は、原則として電子メールを用いて送信してはならない。

（2） 業務上やむを得ず機密情報を送受信する場合は、情報セキュリティ委員会の指示に従い、内容に応じて暗号化、電子署名などの処置を施さなければならない。

（3） 電子メールの送信にあたっては、送信先のメールアドレスに間違いがないか、確認の上送信しなければならない。

（4） 当社のセミナー案内や製品ご紹介メールなどのように社外の複数のドメインが混在するメールアドレスに対し、1 通の電子メールで同報送信する場合は、送信先メールアドレスが受信者間で閲覧できないよう、設定しなければならない。また、広告メール等の送信にあたっては、法を遵守しなければならない。

（5） 電子メールを社外の個人的なメールアドレスに自動転送する場合は、情報セキュリティ委員会に申請を行わなければならない。この場合、転送先メールアドレスは原則として携帯電話のメールアドレスとする。

4．3　電子メールサービスとネットワーク保護

（1） 業務目的以外に電子メールサービスを利用してはならない。

（2） スパムメールを受信した場合は、これを転送してはならない。そして、即座に情報セキュリティ委員会に報告しなければならない。

（3） 当社より発行されたメールアドレスを利用して、社外のメーリングリストに参加する場合は、当該メーリングリストの信頼性、および業務への必要性を充分考慮した上で参加しなければならない。また、参加意義の無くな

った場合は、直ちに脱退しなくてはならない。メーリングリストでの発言は、『１３．４．２　電子メールで送受信される情報の保護』を遵守しなければならない。それとともに公序良俗に反する発言をしてはならない。

（４） 電子メールの送信にあたっては、送信するメールサイズを考慮しなければならない。送信可能なメールサイズは、情報セキュリティ委員会にて規定された制限となっている。規定サイズ以上のメールを送信せざるを得ない場合は、分割送信することができる。分割送信時の分割サイズ、送信のタイミングを考慮するものとする。

（５） その他、無用な電子メールを送受信することにより、ネットワークに負荷をかけてはならない。また、電子メール送信時に HTML メールにて送信しないように電子メールソフトウェアを設定しなければならない。

４．４　電子メールを介してのウイルス被害の防止

（１） メールの受信にあたっては、『ウイルス対策標準』に基づき、電子メール保護機能を有効にしなければならない。

（２） 送信元不明のメールに添付されたファイルや、実行形式のまま添付されたファイルなど、不審な添付ファイルに対してはこれに操作を加えてはならない。

（３） ファイルを添付してメールを送信する場合、当該ファイルのウイルス感染が無いことを必ず確認しなければならない。

（４） 電子メールサービスを利用中に、ウイルスの発見や、ウイルスと思われる症状を発見した場合は、『セキュリティインシデント報告、対応標準』に基づき対応しなければならない。

４．５　電子メールの監視許可

（１） 電子メールの利用状況は、当社メールサーバ管理者の協力のもと、情報セキュリティ委員会によって監視されていることを理解しなければならない。

5　例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

6　罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『罰則に関する標準』に従う。

7　公開事項

本標準は対象者にのみ公開するものとする。

8　改訂

・本標準は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

ウィルス対策標準

0.92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

ウィルス対策標準

１　趣旨

本標準は、ウィルス・ワームによって引き起こされる情報漏えいやシステム破壊の被害を未然に防ぐことを目的とする。

２　対象者

PC を利用するすべての従業員

３　対象システム

PC およびゲートウェイサーバ

４　遵守事項

４．１　アンチウィルスソフトの導入

（１） 当社は、PC およびファイルサーバ並びにメールゲートウェイ上にアンチウィルスソフトを導入する。

（２） アンチウィルスソフトは、情報システム部が指定したソフトを導入することとし、PC およびファイルサーバとメールゲートウェイのソフトは、別会社のソフトを使用する。

（３） 選択するアンチウィルスソフトの要件には、以下の機能が含まれていなければならない。

- ✧　定義ファイルの自動更新機能
  （ベンダー→社内サーバ、社内サーバ→PC）
- ✧　常時スキャン機能
  （ファイルシステム、電子メール）

４．２　アンチウィルスソフトの利用

（1）対象者は、PC に導入されたアンチウィルスソフトを常駐設定にし、ファイルへのアクセスおよび電子メールの受信時には、常時スキャンできるように設定しなければならない。

（2） 対象者は、常時スキャンだけではなく一週間に一度、ファイル全体に対するスキャンを実施することとする。

（3） 対象者は、定義ファイルを毎日一度は更新するように設定しなければならない。

４．３　PC およびサーバソフトウェアのセキュリティ対策

（1） 対象者で PC の貸与を受けている者は、PC に導入されているソフトウェアを『PC 等におけるセキュリティ対策標準』に従って、最新状態に維持しなければならない。

（2） 対象者でサーバ管理者の者は、サーバに導入されているソフトウェアを『サーバ等におけるセキュリティ対策』に従って、最新状態に維持しなければならない。

４．４　PC における電子メールを介してのウィルス被害の防止

（1）メールの受信にあたっては、電子メール保護機能を有効にしなければならない。

（2） 送信元不明のメールに添付されたファイルや、実行形式のまま添付されたファイルなど、不審な添付ファイルに対してはこれに操作を加えてはならない。

（3） ファイルを添付してメールを送信する場合、当該ファイルのウイルス感染が無いことを必ず確認しなければならない。

（4） 電子メールサービスを利用中に、ウイルスの発見や、ウイルスと思われる症状を発見した場合は、『セキュリティインシデント報告、対応標準』に

基づき対応しなければならない。

４．５　ウィルス／ワームに関する啓発教育の実施

（１） 当社の PC を利用する場合には、はじめにウィルス／ワームに関する啓発セミナーを受講しなければならない。

４．６　情報システム部におけるウィルス対策窓口の設置

（１） 情報システム部は、社内のウィルス被害状況等を迅速に収集するために、ウィルス対策窓口を設置し周知徹底しなければならない。

（２） ウィルス対策窓口は、社内のウィルス被害状況を掌握し、問題発生時の一次対応を実施する。

４．７　アンチウィルスソフトがウィルスを検知した場合

（１） 対象者は、アンチウィルスの駆除機能を使用してウィルスを駆除しなければならない。

（２） 駆除した結果に関しては、情報システム部に申請書を提出し、報告しなければならない。

（３） ゲートウェイ上で検知した場合は同様に駆除し、情報システム部への報告することはない。

※当社のシステムでは、ウィルスの検知は通常ゲートウェイ上で検知されるが、万一 PC 上で検知できた場合には、ゲートウェイ上のアンチウィルスソフトの性能を再確認し、製品の入れ替え等を検討しなければならない。

４．８　ウィルスに感染した場合

（１） 対象者は、以下の症状が発生した場合には、ウィルス対策窓口に報告し、対応方法を教えてもらわなければならない。

✧　PC の動作が重くなった。

- ✧ ウィルス付のメールが送られたとの連絡があった。
- ✧ 突然、花火がなった。
- ✧ 突然、うずを巻いた。
- ✧ ファイルを開こうとしたら、マクロの警告ポップアップが出た。（このポップアップが何を意味しているかを把握できているなら、報告の必要はない）

（2） 連絡を受けたウィルス対策窓口は、PC からネットワークケーブルをはずすことを指示し、現場に急行しなければならない。

（3） 現場では、アンチウィルスソフトの定義ファイルがいつ更新されているかを確認しなければならない。最新であれば、PC に対してフルスキャンを実行し、ウィルスが検知されるかを確認しなければならない。

（4） ウィルスが検知された場合は、そのウィルスの特性上どのような挙動を示すかを予測し、影響範囲の特定を実施しなければならない。ウィルスが検知されない場合は、ファイアウォールのログを確認し、怪しいログが残っていないかどうかを確認するなどして、原因を特定しなければならない。

（5） ウィルス被害の影響範囲が、社外にまで至っており場合、『セキュリティインシデントに関する標準』に従って、問題の沈静化を図らなければならない。

5 例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

6 罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『罰則に関する標準』に従う。

7 公開事項

本標準は対象者にのみ公開するものとする。

８　改訂

・本標準は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

Ｗｅｂサービス利用標準

0.92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

Ｗｅｂサービス利用標準

１　趣旨

本標準は、Web ブラウザを使用し、社内及び社外のサイトを利用するにあたって発生し得る各種の問題を未然に防ぐことを目的とする。

２　対象者

Web ブラウザを利用するすべての当社正社員、パート、アルバイト、契約社員とする。

３　対象システム

社内ネットワークに接続し、Web ブラウザを使用し、社内外の Web サイトにアクセスするコンピュータ

４　遵守事項

４．１　Web ブラウザ利用端末機器のセキュリティ

（１）対象者は、Web ブラウザの利用にあたって、情報システム部が指定した Web ブラウザを用いなければならない。また、情報セキュリティ委員会の指示に従い、当該ソフトウェアのバージョンアップ及びセキュリティパッチの適用を行わなければならない。

（２） 対象者は、Web ブラウザの利用にあたって、情報システム部が指定した Web ブラウザの設定を施さなければならない。

（３） 上記ソフトウェアを使用するコンピュータは、『ソフトウェア/ハードウェアの購入および導入標準』に基づいて導入され、『クライアント等におけるセキュリティ対策標準』に基づいたセキュリティ対策を施したものでなければならない。

（４） 対象者は、インターネット上のサイトアクセスするときは、必ず情報シス

テム部が指定する Proxy サーバを使用しなければならない。

４．２　Web ブラウザの利用

（１） 対象者は、社内及びインターネット上の Web サーバへのアクセスは、業務上必要な場合のみ利用できる。

（２） 対象者は、リンクをクリックするとき、リンク先の URL を確認してからクリックしなければならない。この場合、リンク先が、信頼できない URL である場合は、クリックしてはならない。また、バナー広告についても同様で、業務上必要のないバナー広告はクリックしてはならない。

（３） 対象者は、業務上不必要なファイルやソフトウェア、不審なファイルなどをダウンロードしてはならない。必要なファイルやソフトウェアであっても、Web サイト上で実行せず、必ずダウンロードし、ウイルスチェックを実施してから表示、実行しなければならない。

（４） 対象者は、署名の無いあるいは信頼できないサイトの ActiveX や Java、JavaScript、VBScript などのコードは実行してはならない。

（５） 対象者は、原則として、SSL（Secure Sockets Layer）などの暗号通信を行ってはならない。但し、特に部門長の申請により、情報セキュリティ委員会が承認した場合において SSL の通信を行うことができる。この場合、利用者は、利用目的、対象サーバ、利用機関を明確にし、情報セキュリティ委員会の報告しなければならない。

（６） 対象者は、インターネット上の Web サーバを利用した電子メールの送受信を行ってはならない。

（７） 対象者は、社内外の Web サーバに対して、攻撃等不正なアクセスを行ってはならない。また、攻撃、不正なアクセスを目的として社内外のシステムを利用してはならない。

４．３　社内ネットワークの Web サーバの利用

（１） 部門サーバにて、業務上必要な情報を公開する場合には、情報自体のアク

セス権限を明確にし、IP アドレスや、ID、パスワードなどを利用したアクセス制御を必ず行わなければならない。このときファイルやアプリケーションをアップロードする場合には、必ずウイルスチェックを実施しなければならない。

（２） 対象者の情報の発信（掲示板などへの書き込み）に関しては、部門長が業務上必要と認めた場合のみ許可される。このとき、情報の正確性を確保し、必要最小限の範囲で発信するものとする。また、下記に該当する情報の発信は禁止する。また、情報の閲覧に関しても同様である。

- 著作権、商標、肖像権を侵害するおそれのあるもの
- プライバシーを侵害するおそれのあるもの
- 他者の社会的評価にかかわる問題に関するもの
- 他者の名誉・信用を傷つけるおそれのあるもの
- 会社の信用・品位を傷つけるおそれのあるもの
- 性的な画像や文章に該当するおそれのあるもの
- 不正アクセスを助長するおそれのあるもの
- 差別的なもの
- 虚偽のもの
- 社内の機密情報

その他公序良俗に反するおそれのあるもの

４．４　アクセス制御された Web サイトの閲覧に関して

（１） 対象者は、パスワードによってアクセス制御された Web サイトの閲覧において、パスワードを Web ブラウザに記憶させるような行為を行ってはならない。

（２） 対象者は、アクセス制御された Web サイトの閲覧時に離籍する場合は必ず、Web ブラウザを終了させるか、OS のパスワード付スクリーンロックを実施しなければならない。

（３） 対象者は、パスワードによってアクセス制御された Web サイトの閲覧において、他人のユーザＩＤやパスワードなどを利用してアクセスしてはならない。

４．５　Web サイトの閲覧状況の監視許可

（１）　Web サイトの閲覧状況は、当社 Proxy サーバ管理者の協力のもと、情報セキュリティ委員会によって監視されていることを理解しなければならない。

（２）　URL フィルタリングを導入する場合、情報セキュリティ委員会は、当社のビジネスを考慮して閲覧禁止サイトを決定できるものとする。業務上必要とされるサイトが閲覧できない場合には、部門長より申請し、情報セキュリティ委員会が承認した場合、申請部門に関してのみ、閲覧できるものとする。

（３）　情報セキュリティ委員会は、業務上必要でない Web サイトや、許可の無い Web サイトなどのアクセスを発見した場合は、該当者の部門長及び人事部長への報告を行う。

５　例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

６　罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については罰則に関する標準に従う。

７　公開事項

本標準は対象者にのみ公開するものとする。

８　改訂

・本標準は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情

報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

ネットワーク構築標準

0.92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

ネットワーク構築標準　　92

ネットワーク構築標準

１　趣旨

本標準は、当社のネットワーク構築をする際に必要なセキュリティに関して記載するもので、インターネット接続環境、社内ＬＡＮ環境、社内ＷＡＮ環境においてネットワーク機器及び各種サーバの構築の条件、及び運用・管理の実施方法の遵守事項を規定する。

２　対象者

ネットワークを運用・管理する全ての従業員。

３　対象システム

インターネット接続環境、社内ＬＡＮ環境、社内ＷＡＮ環境を対象とする社内ネットワーク（ネットワーク機器及び各種サーバ）

４　遵守事項

４．１　全般規定

ネットワーク構築の全般規定を以下に示す。

(1) ネットワーク環境は、以下に示す３つの環境とする。

- インターネットと接続をするインターネット接続環境（グローバルアドレスを利用したネットワークとし、グローバルゾーンとＤＭＺの２つとする）
- 社内環境に設置するＬＡＮを利用した社内ＬＡＮ環境（プライベートアドレスを利用したネットワークとし、サーバゾーンと各フロアゾーンと営業所と子会社・関連会社の３つとする）
- 専用線及び公衆回線を利用した社内ＷＡＮ環境（プライベートアドレスを利用したネットワークとする。

(2) ネットワーク構築のための機器は、以下に示す機器とする。

- ネットワーク機器（ルータ、ハブ、スイッチングハブ、負荷分散装置、ＶＰＮ装置等）
- ファイアウォールサーバ
- インターネットサーバ（ＤＮＳサーバ、WWWサーバ、メールサーバ、Ｐｒｏｘｙサーバ、ウィルス対策サーバ、ＦＴＰサーバ等）
- イントラネットサーバ（WWWサーバ、ＬＤＡＰサーバ、ファイルサーバ、プリンタサーバ、ウィルス対策サーバ、業務システムサーバ）

・ 認証サーバ、不正アクセス監視サーバ、運用監視サーバ、時刻同期サーバ

(3)インターネット接続環境に接続する機器は、ルータ、スイッチングハブ、UNIX系サーバとする。(Windows系サーバについては、アプリケーションを利用するため必要な場合に接続をすることができる)。

(4)インターネット接続環境には、不正アクセスを防止するための仕組みを設置し、不正アクセスを検出した場合には速やかにセキュリティ委員会に報告しなければならない

(5)インターネット接続環境には、不正アクセスを監視できる仕組みを設置し、不正アクセスを検出した場合は速やかにセキュリティ委員会に報告し、システム運用部門と共に適切な対策を講じなければならない。

(6) 主要な機器は、ログ採取とネットワーク監視を実施すること。

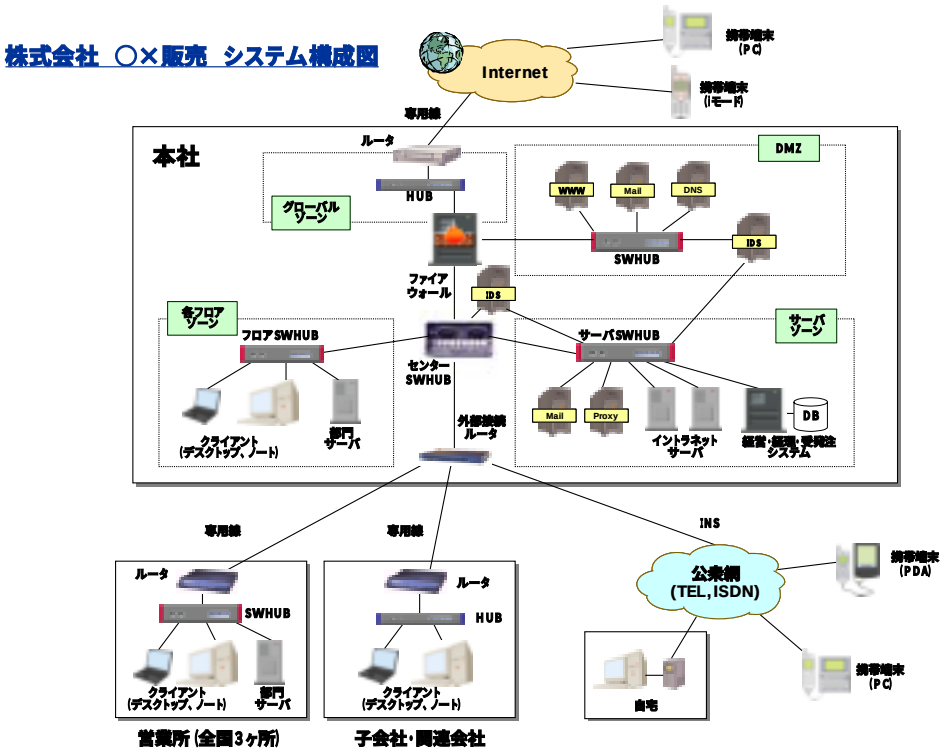
(7) パスワードの設定が可能な機器には、『ユーザ認証標準』に準拠すること。

(8)アクセス制御の設定が可能な機器には、特定の機器からの接続のみ可能な設定をすること

(9) 各機器は、設置場所・接続機器状況・管理者を明確にすること。

(10) 主要なサーバ（インターネットサーバ・イントラネットサーバ）は、サーバルームに構築するサーバ専用セグメントに接続すること。

図６．４－１にシステム構成図を示す。



４．２　インターネット接続環境規定

インターネット接続環境の規定を以下に示す。

(1) ネットワーク接続構成

・ルータによるインターネットプロバイダ接続とし、プロバイダ側のネットワークはグローバルアドレスを利用しなければならない。
・プロバイダと当社の境界には、ファイアウォールサーバを設置し、不正アクセスの対策を実施しなければならない。
・インターネット接続環境に接続できる機器は、インターネットサーバとする。
・ファイアウォールサーバには、ＤＭＺを用意しインターネットサーバを利用できるようにしなければならない。
・ファイアウォールサーバでは、グローバルアドレスとプライベートアドレスの変換を行うことが望ましい。
・外部へのＷｅｂアクセス及びファイル転送は、Ｐｒｏｘｙサーバを経由すること。
・外部とのメールの送受信は、ウィルス対策サーバを経由し最新のパターンデータでウィルス感染チェックすると共に不正中継対策を実施すること。
・インターネットサーバは、情報セキュリティ委員会が指示するＯＳ及びパッチの適用をし、常に最新のセキュリティ対策を実施しなければならない。

(2) 利用できるサービス

・社外ユーザ向けのWWWサービス（情報公開）
・社内ユーザ向けのWWWサービス（情報収集）
・メールの送受信サービス
・ドメインネームサービス
・ファイル転送サービス
・時刻同期サービス

４．３　社内ＬＡＮ環境規定

社内ＬＡＮ環境の規定を以下に示す。

(1) ネットワーク接続構成

・ スイッチングハブ（レイヤ３、レイヤ２）とハブを使用し、ビル内のネットワークとする。
・ ネットワークの中心となるネットワーク機器は、サーバルームに設置し、他のネットワーク機器はフロアに設置すること。
・ ネットワークセグメント間は、通信サービス毎のアクセス制限を実施し不正アクセスの対策を実施しなければならない。
・ 主要な場所に設置するネットワーク機器には、ネットワーク監視を実施すること。
・ 接続できる機器は、各種サーバと PC とプリンタとする。
・ 使用するアドレスは、プライベートアドレスを利用すること。

(2) 利用できるサービス

・インターネット（WWWサービス）
・イントラネット（社内各業務システム）
・ファイル共有サービス
・プリンタ共有サービス
・メールの送受信サービス

４．４　社内ＷＡＮ環境規定

社内ＷＡＮ環境の規定を以下に示す。

(1) 接続構成

- ルータによる専用回線による専用接続とし、接続先は社内拠点（支店、営業所）及び子会社・関連会社とする。
- ネットワークセグメント間は、通信サービス毎のアクセス制限を実施し不正アクセスの対策を実施しなければならない。
- ネットワーク機器には、ネットワーク監視を実施すること。
- 使用するアドレスは、プライベートアドレスを利用すること。
- 専用線接続が困難な場合においては、情報セキュリティ委員会が認めた場合のみインターネットを利用したＶＰＮ装置を利用した接続を認める。

(2) 利用できるサービス

・インターネット
・イントラネット（社内各業務システム）
・ファイル共有サービス
・メールの送受信サービス

４．５　ネットワーク管理規定

ネットワークに設置するネットワーク機器は、以下に示す手順で管理を行う。

(1) 設置許可申請

ネットワーク機器を設置する場合、別途規定する設置許可申請書を情報システム部に提出しなければならない。

(2) システム管理者の決定

ネットワーク機器を設置する場合、管理者を選出しなければならない。選出は、該当ネットワーク機器を管理する部門とし、選出後には情報システム部に文書で報告しなければならない。

(3) 機器の設置

設置するネットワーク機器は、情報セキュリティ委員会からの指示によるセキュリティ対策がされるように設定を行わなければならない。

設置許可申請の受理及び内部審査での合格がされていないネットワーク機器は、ネットワークに設置を認めない。

(4) 審査・設置許可

セキュリティ対策の施されたネットワーク機器は、速やかに情報セキュリティ委員会が実施する内部審査を行わなければならない。 内部審査は、ネットワークを通じた検証について実施することが望ましい。

内部審査で発見された問題点は速やかに処置を行い、再審査を受けて合格するまで処置と審査を継続しなければならない。

内部審査に合格したネットワーク機器は、許可されたネットワークのみ設置することができる。

(5) 監視

設置したネットワーク機器は、情報セキュリティ委員会から指定された外部機関又は内部組織で監視を行わなければならない。 監視の対象は、ネットワークを流れているデータ（通信パケット）とネットワーク機器の稼動状況とする。

(6) 監査の継続と切り離し

設置したネットワーク機器は、設置後も定期・不定期的に監査を実施しなければならない。監査により発見された問題点の程度によっては、情報セキュリティ委員会の判断により、問題点の処置が完了するまでネットワークから切り離なさなければならない。

5 例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

6 罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『罰則に関する標準』に従う。

7 公開事項

本標準は対象者にのみ公開するものとする。

8　改訂

本標準は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

社内ネットワーク利用標準

0.92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

ネットワーク利用標準

１　趣旨

本標準は、機密保持及び情報資産の保護、有効活用を目的に社内ネットワークの利用管理を行う。利用者は、業務目的以外の理由で、社内ネットワーク及びインターネットを利用してはならない。

２　対象者

社内ネットワークにコンピュータを接続し、社内ネットワーク及びインターネットを利用するユーザ。

３　対象システム

社内ネットワークに接続し、社内ネットワーク及びインターネットへの通信を行うコンピュータ及びシステムを対象とする。

４　遵守事項

４．１　社内ネットワーク及びインターネットの業務目的以外の利用禁止

（１） 社内ネットワークは、会社の情報資産であり、電子メールやＷｅｂサイトの利用などにおいて、業務目的以外の使用を禁止する。インターネットの利用についても同様である。

（２） 情報セキュリティ委員会の許可無く、社内ネットワーク上に、電子メールサーバや、Web サーバ、FTP サーバなどを構築してはならない。

（３） 他人の利用者ＩＤを用いて、社内ネットワーク及び、社外のネットワーク、インターネット上のサイトへアクセスしてはならない。

（４） ネットワーク利用者は、故意もしくは不注意を問わず、社内ネットワーク及び社外ネットワーク、インターネット上のサーバに対して、許可されたアクセス権限以上のアクセスを行ってはならない。

４．２　ネットワークを利用した機密情報の送受信

（１） ネットワーク利用者は、当社の事業に関わる情報や、顧客や従業員のプライバシーに関わる情報などの機密性の高い社内の情報が社外へ漏洩することを防ぐために、ファイルのアップロードや社外へ送信を行ってはならない。

（２） 出所が不明なファイルや内容に確証の持てないファイルをダウンロードや実行してはならない。

（３） 業務上やむを得ず機密情報を社外へ送信もしくは受信する場合は、情報セキュリティ委員会の指示に従い、内容に応じて暗号化、電子署名などの処置を施さなければならない。

４．３　インターネットで利用可能なサービス

（１） ネットワーク利用者は、インターネットの利用において、電子メール及び Web 閲覧以外を使用してはならない。情報セキュリティ委員会は、上記のサービス以外利用できないようなアクセス制御を実施する。

（２） 暗号通信を用いたインターネットへのアクセスは、情報セキュリティ委員会の承認を得たサイトのみ許可するものとする。

（３） Web サービスの利用については、『Web サービス利用標準』を遵守すること。

（４） ネットワーク利用者は、社内ネットワークに接続した PC において、自社の電子メールサービス以外の電子メールサービスを利用してはならない。やむを得ず、社外の電子メールサービスを利用しなければならない時は、情報セキュリティ委員会の承認を得ること。

４．４　社内ネットワークで利用可能なサービス

（１） 電子メールの利用において、本社サーバゾーンにて管理する電子メールサーバを利用しなければならない。その他の電子メールの利用については、『電子メール利用標準』を遵守しなければならない。

（２） インターネット上のサーバに Web ブラウザを用いてアクセスする場合は、必ず、本社サーバゾーンにて管理する Proxy サーバを使用しなければならない。

（３） 本社サーバゾーンにて管理されるシステム（経営、経理、受発注システム、イントラネットサーバ）へのアクセスは、許可された利用者以外利用してはならない。

（４） 各部門サーバは、他部門ネットワーク及び他部門の者が利用する IP アドレスからのアクセスを拒否しなければならない。他部門からのアクセスが業務上必要な場合には、本社サーバゾーンに設置され、アクセス制御可能なイントラネットサーバを利用しなければならない。

（５） 専用線や INS を使用した場合は、Web サービスのプロトコルと電子メールのプロトコル以外を利用してはならない。本社サーバゾーンに配置された重要サーバへのアクセスは、許可されたユーザが許可されたアクセスに限って許可するものとする。

（６） 各部のセキュリティ担当者は、社内ネットワークで利用するサービスを情報セキュリティ委員会に届けなければならない。情報セキュリティ委員会は、届けられた利用サービスにおいて、業務上不必要と判断できるサービスは禁止することができる。また、届けられた利用サービス以外が使用されていないかどうかを検査できるものとする。

（７） 業務上やむを得ず機密情報について、ネットワークを介して扱う場合は、情報セキュリティ委員会の指示に従い、内容に応じて暗号化、電子署名などの処置を施さなければならない。

（８） ネットワーク利用者は、社内ネットワークにおいて、ネットワークモニターなどの、ネットワーク上を流れるパケットを盗聴できる機器及びソフトウェア使用してはならない。但し、情報セキュリティ委員会が承認した調査及び監視目的のネットワークＩＤＳやネットワークモニターなどの利用はできることとする。

（９） ネットワーク利用者は、社内ネットワークサーバへのアクセス用のＩＤ及

びパスワード、証明書は適切に管理しなければならない。特にパスワードの選択および使用については、『ユーザ認証に関する標準』に基づいたものを利用しなければならない。

４．５　社内ネットワークへの接続時の注意事項

（１）　自宅や、他組織のネットワークへ接続した PC は、ウイルス検査とセキュリティ検査を実施し、異常が発見されなかったことを部のセキュリティ担当者が確認した後でなければ、社内ネットワークに接続してはならない。

（２）　ネットワーク利用者は、与えられたＩＰアドレス以外のＩＰアドレスを使用してはならない。

（３）　ネットワーク利用ユーザは、社内ネットワークに接続中のコンピュータを、情報セキュリティ委員会の許可の無い電話回線、携帯電話、PHS、無線ＬＡＮ、専用線などを利用して、社外のネットワークへ接続してはならない。

４．６　監視方針

（１）　我社は、社内から社外、及び社内から社内に対する全ての通信に対して、次の監視を行う。

- 社外への通信権限の有無
- 許可されたサービスの通信状態
- 許可されていない通信先への接続、接続先ＵＲＬ
- 電子メールの本文、添付ファイルの内容
- ダウンロードするファイルの種類
- ウイルスチェック

（２）　情報セキュリティ委員会は、本社サーバゾーンに配置した重要サーバや社内ネットワークへの許可されないアクセス、インターネットへの不審なアクセス等を監視するために IDS を導入する。

（３）　監視内容の決定、追加、変更は情報セキュリティ委員会の承認を得なければならない。監視により、許可されていない通信を検知したシステム管理者及びネットワーク利用ユーザは、情報システム部門長に報告しなければならない。システム管理者及びネットワーク利用ユーザは、監視によって

知りえた情報を情報システム部門長への報告以外に漏洩してはならない。

５　例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

６　罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『罰則に関する標準』に従う。

７　公開事項

本標準は対象者にのみ公開するものとする。

８　改訂

・本標準は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

用語集
社内ネットワーク
電子メール
Web サービス
ネットワーク利用者
コンピュータ

IDS
サイト
アクセス権限
ファイルのアップロード
ダウンロード
Web 閲覧
アクセス

リンク
『Web サービス利用標準』
『電子メール利用標準』
『ユーザ認証に関する標準』

LAN における PC（サーバ、クライアント等）設置/変更/撤去の標準

0.92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

LAN における PC（サーバ、クライアント等）設置/変更/撤去の標準

１　趣旨

本標準は、当社 LAN 環境への PC（サーバ、クライアント等）接続において発生し得る各種の問題を未然に防ぎ、情報資産を保護することを目的とする。

２　対象者

本標準は、当社 LAN 環境に接続する全ての利用者に適用される。当社社員のみならず協力会社社員の利用も対象に含まれる。また、特に認められた場合の、社員ではない者の一時的な利用も対象に含まれる。

３　対象システム

本社各フロア、支社・営業所などの管轄拠点において展開される LAN に接続された全てのシステムを対象とする。

４　遵守事項

４．１　機材の設置

（１） LAN に接続する PC は、『ソフトウェア／ハードウェアの購入および導入標準』に基づいて導入されたものに限る。利用者は個人所有の機材を利用して LAN に接続してはならない。

（２） LAN に接続する PC は、原則として IP 通信のみを利用する事とし、『サーバ等におけるセキュリティ対策標準』または『クライアント等におけるセキュリティ対策標準』に基づいたセキュリティ対策が施されていなければならない。

（３） LAN に接続する PC の設置にあたって利用者は、情報システム部に以下の情報を申請し、承認を受けなければならない。

- 利用者情報（氏名、所属、連絡先等）
- 利用目的

・ 利用形態（設置希望箇所、利用時間帯、利用サービス、予定期間）
・ 利用機器情報（管理者、連絡先、MAC アドレス等ハードウェア情報

（4） 情報システム部は、利用者からの申請に対し、利用目的、利用形態を審査し、結果を申請者に連絡しなければならない。

（5） 情報システム部は、利用申請に対し許諾を与える場合に、一定規則に則って PC 名称（ホスト名）、IP アドレスを決定しなければならない。また、必要に応じて DNS、およびディレクトリへの情報登録を行わなければならない。DHCP など、動的に IP アドレスが変化する利用が発生する場合には、その旨を認識しなければならない。

（6） 情報システム部は、利用申請に対し許諾を与える場合に、接続する HUB・情報コンセント・利用ケーブル番号など、接続箇所を決定しなければならない。

（7） 情報システム部は、利用者に提供する以下の情報一覧（必要に応じて図を利用）を保存し、管理しなければならない。
・ IP アドレス利用一覧
・ PC 名称、DNS 登録一覧
・ 接続箇所利用一覧

（8） 情報システム部は、利用申請に対し許諾を与える場合に、下記情報を保存し、管理しなければならない。
・ 利用者情報（氏名、所属、連絡先等）
・ 利用目的
・ 利用形態（設置箇所、利用時間帯、利用サービス、予定期間）
・ 利用機器情報（管理者、連絡先、MAC アドレス等ハードウェア情報、PC 名称、IP アドレス、アドレス取得形態（固定 IP/DHCP）、接続箇所情報、DNS 登録の有無、ディレクトリ登録情報）

（9） 情報システム部は、利用申請に対し許諾を与える場合に、申請者に対して下記情報を連絡しなければならない。
・ 許諾された利用目的
・ 許諾された利用形態（設置箇所、利用時間帯、利用サービス、予定期間）
・ 利用機器情報（PC 名称、IP アドレス、アドレス取得形態（固定 IP/DHCP）、

接続箇所情報、DNS 登録の有無、ディレクトリ登録情報）

４．２　LAN 接続における留意点

（１） 利用者は、情報システム部が設置している以外の HUB・Router・モデム等を導入してネットワーク形態を変更してはならない。また、それらを利用して他のネットワークに接続してはならない。

（２） 利用者は、変更申請無しに使用機材の機能を変更、あるいは機能の追加を行ってはならない。また、許可されている目的外で LAN を利用してはならない。

（３） 情報システム部は、緊急を要する場合など、必要に応じて利用者の LAN 接続を制限（アクセスの制御、切断など）することができる。利用者は、情報システム部から LAN 接続に関する指示があった場合、その指示に従わなければならない。また緊急時には、情報システム部は利用者に対して指示を与える前に LAN 接続を制限してもよい。

（４） 情報システム部は、利用者の接続形態にあわせ、適切な認証機能・暗号化機能等を提供し、情報の保護に努めなければならない。

- 無線 LAN を利用する場合には、認証および暗号化機能を利用すること
- Switching HUB 等を利用して、利用者間でのパケットキャプチャができない仕組みを用いること
- LAN に接続する機器の通信は、『社内ネットワーク利用基準』に照らして適切な通信のみに限定すること
- リモートアクセスについては、『リモートアクセスサービス利用標準』に照らして適切な通信のみに限定すること
- 各サーバへのアクセス状況については、『監視に関する標準』に基づいて対処すること

４．３　LAN 接続情報の更新、通知手続き

（１） 情報システム部は、利用者に許可した LAN 接続形態が守られているか、許諾後 2 週間以内に、申請内容に照らして確認しなければならない。また半年に一度、部門ごとの LAN 接続状態を確認しなければならない。

（２） 情報システム部は、利用者に許可した LAN 接続について、申請・変更時に予定していた期間が満了する 2 週間前に、利用者に期間の満了について通知しなければならない。また、期間を満了する PC が周辺業務に影響を及ぼす事が無いか、あわせて調査する事が望ましい。

４．４　変更手続き

（１） LAN に接続する PC の利用目的、あるいは利用形態の変更を要する場合、利用者は、速やかに情報システム部に以下の情報を申請し、承認を受けなければならない。

- 利用者情報（氏名、所属、連絡先等）
- 変更事由および変更情報（利用目的、利用形態、PC 設置申請時から変更された情報）
- 変更前機器情報（PC 名称、IP アドレス、アドレス取得形態（固定 IP/DHCP）、接続箇所情報、DNS 登録の有無、ディレクトリ登録情報）

情報システム部は、利用目的・利用形態を審査し、結果を申請者に連絡しなければならない。

（２） 情報システム部は、利用者からの変更申請に対し、利用目的・利用形態を審査し、結果を申請者に連絡しなければならない。変更申請は、変更時の申請に必要な情報（箇所、目的、事由）が明確になっていない場合、および変更前と比較して、同等以上のセキュリティを確保できない場合にはこれを認めない。

（３） 情報システム部は、変更申請に対し許諾を与える場合に、管理している情報（利用者情報、利用目的、利用形態、利用機器情報）を更新しなければならない。

（４） 情報システム部は、変更申請に対し許諾を与える場合に、申請者に対して下記情報を連絡しなければならない。

- 許諾された利用目的
- 許諾された利用形態（設置箇所、利用時間帯、利用サービス、予定期間
- 利用機器情報（PC 名称、IP アドレス、アドレス取得形態（固定 IP/DHCP）、接続箇所情報、DNS 登録の有無、ディレクトリ登録情報）

４．５　機材の撤去

（１）　利用者は、以下に該当する場合、速やかに LAN 接続を終了し、機材をネットワークから切り離さなければならない。あわせて接続終了を情報システム部に報告し、情報システム部の確認を受けなければならない。

- 申請・変更時に予定していた期間を満了した場合
- その他情報システム部からの指示を受けた場合

（２）　情報システム部は、以下に該当する場合、利用者の LAN 接続の終了を確認しなければならない。

- 申請・変更時に予定していた期間を満了した場合
- 緊急時など、情報システム部が必要と判断した場合
- その他接続が不要、あるいは不適当と見なされる場合

（３）　情報システム部は、利用者の LAN 接続終了にあわせ、利用者管理情報を更新（接続終了と判断できる状態に）しなければならない。

（４）　情報システム部は、以下の情報一覧を更新しなければならない。

- IP アドレス利用一覧
- PC 名称、DNS 登録一覧
- 接続箇所利用一覧

５　例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

ただし、ウイルス対策・不正アクセスへの対処など、緊急を要する場合にはこの限りではなく、情報システム部が必要と判断した場合には対処を優先し、情報セキュリティ委員会に対し、事後の報告を行うことを認める。

６　罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『罰則に関する標準』に従う。

７　公開事項

本標準は対象者にのみ公開するものとする。

８　改訂

・本標準は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

リモートアクセスサービス利用標準

0.92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

リモートアクセスサービス利用標準

1 趣旨

本標準は、ダイヤルアップ等により社内ネットワークを利用する、リモートアクセスサービス利用にあたり、当社の情報資産を外部から守ることを目的とする。

2 対象者

下記を本標準の遵守義務対象者とする。
・リモートアクセスを利用する全員
・リモートアクセスを管理するシステム管理者
・リモートアクセスを運用するオペレータ

3 対象機器・対象システム

下記を本標準の遵守義務対象機器・対象システムとする。
・リモートアクセスで利用する機器（PC、PDA、携帯電話など）
・リモートアクセスシステム
・VPN 装置
・リモートアクセスサーバ
・インターネット接続システム
・外部公開サーバ

4 遵守事項

4．1 使用機器に関する遵守事項

（1） 利用者は、ダイヤルアップによる社内ネットワークへのアクセスにおいて、情報システム部が構築した機器を利用しなければならない。

（2） 利用者は、ダイヤルアップルータおよびサーバ・モデムなどによる社内ネットワークへの接続手段を、情報システム部の許可を得ることなく設置してはならない。

（3） その他社内 LAN 環境への接続にあたり、利用機器は、『LAN における PC

（サーバ、クライアント等）設置/変更/撤去の標準』に基づいて設定されなければならない。

４．２ 機器の管理に関する遵守事項

（１） リモートアクセスで使用する PC および携帯電話は、情報セキュリティ委員会が定める利用者のみ利用することができる。

（２） リモートアクセスで使用する PC および携帯電話の管理は、所有する利用者が行わなければならない。

（３） リモートアクセスの管理は、情報システム部（システム管理者およびオペレータ）が行わなければならない。

４．３ 利用環境に関する遵守事項

（１） リモートアクセスで利用できる機器は、情報セキュリティ委員会の定める機器でなければならない。

- ノート型 PC
- PDA
- 携帯電話

（２） リモートアクセスの利用場所は、情報セキュリティ委員会の定める場所でなければならない。

- 外出先（国内、海外）
- 営業所・関連会社等、当社関連施設
- ユーザ先
- 自宅

（３） リモートアクセスによる接続は、情報セキュリティ委員会の定める通信形態でなければならない。

- インターネット経由（PC、携帯電話）
- 公衆回線（電話回線、INS 回線、携帯電話）

（４） リモートアクセスで利用できるサービスは、情報セキュリティ委員会の定めるものでなければならない。

・http・https を利用したサービス
・電子メールサービス
・ファイル転送サービス
・ファイル共有サービス
・業務システムとして導入しているサービス

４．４ アカウント管理に関する遵守事項

（１） 利用者は、『LAN における PC 設置/変更/撤去の標準』に準じ、リモートアクセスサービスの利用において、個人所有の機材を利用してはならない。

（２） リモートアクセスで利用する PC および携帯電話は、利用者（社員）が情報システム部に申請をし、利用者情報（識別番号、パスワード等）を入手しなければならない。
・利用者名
・利用場所
・利用目的
・利用期間
・接続機器（機器種別、OS 種類）
・接続形態

（３） 情報システム部は、利用者情報（利用者、識別番号、パスワード等）の登録・変更・削除を適宜行い、それを管理しなければならない。

４．５ アクセス制御に関する遵守事項

（１） リモートアクセスでは、社内にアクセスできるサーバおよびサービスは必要最低限にしなければならない。

（２） リモートアクセスでは、利用者毎にアクセスできるサーバおよびサービスを決めることとする。

（３） リモートアクセスでは、社内に設置されたサーバのみにアクセスすることができる。ただし、申請により許可された社員についてはインターネットへアクセスすることもできる。

４．６ リモートアクセスサーバに関する遵守事項

（１） リモートアクセスサーバは、専用機器（ルータ、サーバ等）または複数のネットワーク機器で構成されなければならない。

（２） リモートアクセスサーバは、利用者情報を管理することができなければならない。

（３） リモートアクセスサーバは、利用者認証（発信者識別、ワンタイムパスワード）に対応していなければならない。

（４） リモートアクセスサーバは、通信手段としてコールバックと VPN（暗号化）に対応していなければならない。

（５） リモートアクセスサーバは、接続記録を蓄積でき各種データを外部媒体（磁気テープ、ＣＤ－Ｒなど）に保管できなければならない。

・接続成功
・接続失敗
・接続の開始時間と終了時間
・接続時のアカウント名
・発信者識別
・障害情報（エラー情報）

４．７ クライアントに関する遵守事項

（１） クライアントは、利用する社員を識別（利用者識別名・パスワード）し該当者以外の利用をできないようにしなければならない。

（２） クライアントは、ワンタイムパスワードまたはコールバックに対応していなければならず、それを利用しなければならない。

（３） クライアントは、通信手段として発信者識別・VPN（暗号化）に対応していなければならず、それを利用しなければならない。

（４） クライアントは、『クライアント等におけるセキュリティ対策基準』を満たし、かつ『ウィルス対策標準』を満たしていなければならない。

（５） クライアントは、情報セキュリティ委員会が定めたソフトウェアがイントールされ、正常に動作する状態でなければならない。

４．８ 利用手順に関する遵守事項

（１） 利用者は、リモートアクセスを行う場合、クライアントと利用者を識別する情報を入力しリモートアクセスサーバで認証されなければならない。

（２） 利用者は、インターネットを利用してリモートアクセスする場合、ワンタイムパスワードを利用し認証しなければならない。また、VPN を利用する事が望ましい。

（３） 利用者は、公衆電話または携帯電話を利用してリモートアクセスする場合、ワンタイムパスワードを使用し認証しなければならない。

（４） 利用者は、上記以外の通信手段を利用してリモートアクセスする場合、コールバック機能を使用し認証しなければならない。

（５） 利用者は、リモートアクセスしている間に利用者がクライアントから離れる場合に、クライアントを停止するか第三者の利用ができないようにしなければならない。

（６） 利用者は、リモートアクセス利用のための教育を受け一定のレベルになっていることが望ましい。

４．９ 検査と監視に関する遵守事項

（１） 情報システム部は、定期的（年４回）に外部で使用する PC および携帯電話が適切に利用されているか検査しなければならない。

（２） 情報システム部は、定期的（年４回）にダイヤルアップルータおよびサーバ、モデムなどによる社内ネットワークへの接続環境が不正に用意されていないか検査しなければならない。

（３） リモートアクセスサーバは、接続記録を蓄積・管理し、定期的（毎月）に

解析しなければならない。

４．１０ 緊急対応に関する遵守事項

（１） システム管理者は、リモートアクセスサーバに対し、外部から侵害・侵入された場合、リモートアクセスを停止し、原因調査および対策を実施してリモートアクセスを再開始しなければならない。

（２） 利用者は、リモートアクセスで使用する PC および携帯電話を紛失した場合に、速やかにシステム管理者に報告し具体的な指示を受け、対処しなければならない。

（３） 利用者は、リモートアクセスで使用する PC および携帯電話で使用するパスワードを忘れた場合に、システム管理者に連絡し、速やかに新たなパスワードへ変更しなければならない。

（４） 利用者は、リモートアクセスで使用する PC に障害が発生した場合、速やかにシステム管理者に報告し、システムの再構築をしなければならない。

４．１１ 物理セキュリティ遵守事項

（１） リモートアクセスで使用する PC および携帯電話は、所有者の周囲に置き管理できるようにし、使用しない時には、定められた場所で保管しなければならない。

（２） リモートアクセスサーバは、システム管理者以外が利用できなく安全・予防対策がなされた場所に設置されなければならない。

５ 例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

６ 罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合があ

る。罰則の適用については罰則に関する標準に従う。

7 公開事項

本標準は対象者にのみ公開するものとする。

8 改訂

・　本標準は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・　本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・　本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

専用線及び VPN に関する標準

0. 92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

専用線及び VPN に関する標準

１ 趣旨

本標準は、当社とその取引先、或いは当社営業所・関連会社と円滑かつ効率よく業務を遂行するために構築された VPN 及び専用線によるネットワークにおいて、接続される両端の組織のお互いがネットワーク犯罪の被害者や加害者、あるいは踏み台にならないことを目的とする。

２ 対象者

・VPN 及び専用線接続を申請する者
・情報セキュリティ委員会
・VPN 及び専用線接続のシステム管理者、オペレータ

３ 対象システム

・接続される専用線の両端のネットワーク
・VPN 及び専用線接続に用いられるルータ、ファイアウォール、IDS

４ 遵守事項

４．１ 接続手順

（１） VPN 及び専用線接続の新設には、以下の手順を要する。
① 申請
② 完了期限付きシステム工事許可
③ VPN 及び専用線接続契約書の締結
④ システム工事
⑤ 検査合格
⑥ 運用開始

（２） VPN 及び専用線接続を新設するためには「VPN 及び専用線接続申請書」を情報セキュリティ委員会に提出し許可を得なければならない。申請には、担当者の押印だけではなく所属長部長職相当の押印が必要である。

（３） 申請を受けた情報セキュリティ委員会は、直ちに審査を開始しなければならない。

（４） 「VPN 及び専用線接続申請書」には以下の記述が必須である。

① 接続先住所、組織名称
② 接続目的
③ 接続種別（専用線、VPN）
④ 接続開始希望日
⑤ 接続先双方のシステム構成
⑥ 接続先双方のアクセス許可範囲
⑦ 許可されるサービスとその方向性
⑧ 接続先双方のシステム管理者名、システムセキュリティ責任者名
⑨ 接続先双方の異常の定義と異常連絡体制
⑩ 接続先双方の運用管理手順書の添付

（５） 情報セキュリティ委員会は、申請内容を十分に審査し適当であると判断された場合に、「完了期限付きシステム工事許可」を通知する。

（６） 「完了期限付きシステム工事許可」が通知された申請者は、その接続先が社外の場合には「VPN 及び専用線接続契約書」を締結しなければならない。

（７） 「VPN 及び専用線接続契約書」には「VPN 及び専用線接続申請書」に準じた内容が記載され、更に、責任の範囲及び責任者を明確に記載しなければならない。

（８） 「完了期限付きシステム工事許可」が通知された申請者は、指定された期日までにシステム工事を完了し、「VPN 及び専用線接続検査申請書」により検査を申請し、検査を受けなければならない。

（９） 本標準が適用される以前の既存の VPN 及び専用線接続については、速やかに逐次本標準に適合するようにしなければならない。

４．２ 許可するサービス

（1） VPN 及び専用線接続によって利用が許可されるサービスは、必要最小限にとどめられなければならない。

４．３ リモート管理

（1） VPN および専用線接続のシステム管理者が、何らかの理由でリモートアクセスにより、対象システムを管理する場合には、その通信は暗号化されなければならない。

４．４ アクセスコントロール

（1） VPN および専用線接続のシステム管理者は、VPN 及び専用線接続に用いられるルータでアクセスコントロールが施され、サービスの必要なサーバやネットワークのみ通信が行えるようにアクセスが制限されるよう管理しなければならない。ただし、ファイアウォールを用いる場合には、ルータでアクセスコントロールを行う必要はなく、ファイアウォールで適切なアクセスコントロールを行う。

（2） アクセスコントロールは、送信元及び送信先アドレスだけでなく、時間や通信量の制限も含まれ、いずれも必要最小限にとどめられなければならない。

４．５ 安全な設定

（1） VPN 及び専用線接続に用いられるシステムは、安全な設定が施されていなければならない。安全な設定とは、『ネットワーク構築標準』『サーバ等におけるセキュリティ標準』に準じ、以下の要件を満たすことが望ましい。

- 最新の OS
- 最新のアプリケーション
- 最新のセキュリティパッチの適用
- 不要なプログラムやサービスの削除

４．６ パスワード

（1） ルータ、サーバ等全てのパスワードが利用できる機器には、『ユーザ認証標準』に基づいたパスワードが付加されなければならない。

４．７ ログの保存

（１） VPN および専用線接続のシステム管理者は、通信の経路にあるルータ、アクセス対象のサーバおよびファイアウォールでログが保存されるようにしなければならない。

（２） サーバおよびファイアウォールのログには、以下の項目が含まれていなければならない。
- アクセス成功
- アクセス失敗
- 内部エラー
- IP アドレス
- ログインを伴う場合にはアカウント名
- 時間

（３） ルータのログには、以下の項目が含まれていなければならない。
- アクセスコントロール違反
- IP アドレス
- 時間

（４） ログは、一時的にハードディスク等の書き換え可能なメディアに保存されていても良いが、２４時間以内に書き換え不能なメディアに転送され厳重に保管されなければならない。また、一時的にハードディスク等の書き換え可能なメディアにログを記録する場合には、十分な記憶容量を確保しておき、異常な量の書き込みが発生した場合においても十分に対処できるように備えておかなければならない。

（５） ログは、その取得日から３年間は確実にシステムセキュリティ責任者のみが参照できる場所と方法で厳重に保管されなければならない。

４．８ ログの解析

（１） 保存されたルータやサーバやファイアウォールのログは、システムセキュリティ責任者、もしくはシステムセキュリティ責任者の許可を受けたシステム管理者により解析されなければならない。

（２） ログの解析は少なくとも１ヶ月に１回以上定期的に行わなければならず、セキュリティ侵害や、その可能性がある場合は随時行わなければならない。

（３） ログの解析を行う際は以下の点に注意しなければならない。
・許可されていない IP アドレス
・指定時間外のアクセス
・アクセス頻度
・データ量
・度重なるアクセス失敗

４．９ 継続した安全な設定の適用

（１） VPN および専用線接続のシステム管理者は、安全な設定が継続して行われるよう努めなければならない。即ち、新しいセキュリティパッチが公開された場合には、速やかに適用しなければならない。

（２） セキュリティパッチの適用により既存サービスが継続できなくなる場合には、ファイアウォールやルータ、IDS、或いは対象機器自身の設定変更により新しい脅威への対策を確実に講じなければならない。

４．１０ 設定の変更

（１） VPN および専用線接続のシステム管理者は、該当システムの既存の設定を変更する場合において、変更の程度に応じて手続きを行わなければならない。また、以下の点に留意しなければならない。
・重要でないファイルの削除等を行う場合は、業務日誌に記入しなければならない。
・サービスのバージョンアップ等を行う場合は、業務日誌に記入し、情報セキュリティ委員会に報告しなければならない。
・新規アカウントの追加や、新規サービスの追加等の変更を行う場合は、「VPN 及び専用線接続設定変更申請書」を情報セキュリティ委員会に提出して許可を得なければならない。

４．１１ 運用履歴

（1） 設定変更等の運用履歴は、紙もしくは磁気媒体で作成され該当システムのシステムセキュリティ責任者が保管する。

４．１２ バックアップ

（1） VPN および専用線接続のシステム管理者は、該当システムへのセキュリティ侵害に備え、データ、システム設定ファイル等、該当システム上の全情報のバックアップを取らなければならない。

（2） バックアップは１日に１回取得し、バックアップを取ったメディアは、その取得日から３年間は確実にシステムセキュリティ責任者のみが参照できる場所と方法で厳重に保管されなければならない。

４．１３ 設置場所

（1） VPN 及び専用線接続で用いられるルータやファイアウォール等、アクセスコントロールを施している機器、及び、データベースやアプリケーション等重要なデータを扱っている機器類は、全て安全な場所に設置されていなければならない。安全な場所とは、『サーバルームに関する標準』に準じ、以下を満たすことが望ましい。

・施錠されていること
・明示的に許可された者以外の立ち入りが禁止されている
・ネットワークの盗聴が外部から行えないこと
・監視カメラが設置されていること

４．１４ 検査

（1） VPN 及び専用線接続はその運用開始前に、必ず情報セキュリティ委員会の検査を受けなければならない。検査には以下の項目が含まれなければならない。

・最新の脆弱性情報を含む検査項目
・システムの申請書との整合性
・許可された範囲以外へのアクセスが出来ないこと
・アクセスコントロール定義の確認

（2） 検査は、接続両端からお互いの方向に対して行われなければならず、検査

結果はお互いに対して公開する。また、検査に合格するまでは接続は接続試験や検査の目的以外で接続してはならず、検査は２ヶ月ごとに継続して実施されなければならない。もし、検査に不合格になった場合には、１週間以内に対策を行い再検査を受け、以後これを繰り返す。

４．１５ 監視

（１） VPN 及び専用線接続は以下の監視方法で、システムセキュリティ責任者、もしくはシステムセキュリティ責任者の許可を受けたシステム管理者により行われなければならない。

４．１６ 監視方法

（１） ルータやファイアウォール専用機器の監視には NIDS を使用するものとすし、アクセス対象のサーバの監視には HIDS を使用するものとする。

４．１７ 緊急対応(IR)

（１） セキュリティ侵害された場合や、その可能性がある場合は、その事象レベルにより、緊急に適切な対応をしなければならない。（緊急対応の対象となる事象と、その対応方法例は以下のとおりである。）

対象事象：VPN 及び専用線が切断された場合

対応方法：サーバ等への攻撃が行われていないか確認し、原因が見当たらない場合は、プロバイダ等の通信事業者へ切断事由、復旧予定等について確認を行った上、情報セキュリティ委員会に報告し、指示に従わなければならない。

対象事象：アクセスコントロール違反が発見された場合、度重なるアクセス失敗が発見された場合、業務時間外の大量のデータダウンロードが発見された場合

対応方法：接続元の IP アドレスを確認し、該当マシンの利用者に事実関係の有無を確認の上、操作ミス以外の理由による場合は、情報セキュリティ委員会に報告し、指示に従わなければならない。

5 例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリ

ティ委員会に報告し、例外の適用承認を受けなければならない。

6 罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については罰則に関する標準に従う。

7 公開事項

本標準は対象者にのみ公開するものとする。

8 改定

- 本標準は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

- 本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

- 本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

媒体の取扱に関する標準

0.92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

媒体の取扱に関する標準

１　趣旨

本標準は、PC 等の修理時、並びに媒体の処分時に関するルールを定め、機密性の高い情報の漏洩を未然に防ぐことを目的とする。

２　対象者

PC 等の修理を依頼するすべての従業員。
媒体の使用、処分を行うすべての従業員。

３　対象システム

当社の業務で使用するすべての PC 等及び媒体を対象とする。
媒体とは、フロッピーディスク、MO、CD、DVD、磁気テープ、ハードディスク等、取り外しが可能で情報が保存できるものを対象とする。

４　遵守事項

４．１　PC（IT 製品）の修理

（１）　PC 等の修理を依頼する従業員は、機密性の高い情報が読み出し可能な状態で保管されていないことを確認した上で修理を依頼しなければならない。
故障の状況により、保管されている情報の確認や保護が実施できない場合には、ハードディスク等の情報が保管されている装置を取り外して修理を依頼しなければならない。

（２）　『ソフトウェア／ハードウェアの購入及び導入標準』で定められた標準製品の修理を依頼する従業員は、申請書を提出し、情報システム部を通して修理を依頼しなければならない。
情報システム部は、標準製品の代替品を準備し、必要に応じて貸し出しを行う。
標準外製品の修理は、使用部署から直接修理を依頼するものとする。

（３）　情報システム部及び、標準外製品の修理を依頼した従業員は、外部業者が社内に立ち入って修理を行う場合、『サーバルームに関する標準』、『物理的対策標準』に基づいて対応しなければならない。

４．２ 媒体の保管

（１）機密性の高い情報を媒体に保存する者は、権限のない者が保管された情報にアクセスできないよう、暗号化を行うか、媒体を鍵のかかる場所に保管し、鍵は容易に持ち出しが出来ない場所に保管しなければならない。

４．３　媒体の移動

（１）すべての従業員は、機密性の高い情報を保管した媒体を、その情報の管理責任者の許可なく社外へ持ち出してはならない。

（２）すべての従業員は、特定の従業員にのみアクセス権限を限定している情報が保管された媒体を、社内便で送付してはならない。

（３）すべての従業員は、開示範囲を当社内に限定している情報が保管された媒体を、郵送や宅配便等で送付してはならない。
子会社、関連会社、営業所への送付は、社内便などのセキュリティが確保された手段で送付しなければならない。

４．４　媒体の再使用

（１）すべての従業員は、機密性の高い情報が保存されている媒体を再利用する前に、保存されていた情報を、再生できない方法で消去しなければならない。

４．５　PC（IT 製品）と媒体の廃棄

（１）PC（IT 製品）の廃棄を行う者は、情報システム部宛に廃棄申請を提出しなければならない。

（２）PC（IT 製品）の廃棄を行う者は、機密性の高い情報が保管されたハード

ディスク等を取り外してから､指定された場所に廃棄しなければならない。取り外したハードディスク等は、情報システム部が指定する場所に持ち込まなければならない。

（３） 機密性の高い情報が保管された媒体の廃棄を行う者は、情報システム部が指定する場所に持ち込まなければならない。

（４） 機密性の高い情報が保管されているかどうかが確認できない場合には、機密性の高い情報が保管されているものとして取り扱わなければならない。

（５） 情報システム部は、機密性の高い情報が保管されたハードディスク等や媒体を、再生不能な状態に破壊して廃棄しなければならない。

（６） 情報システム部は、機密性の高い情報が保管されたバードディク等や媒体の処分を外部業者に委託する場合、情報セキュリティ委員会の承認を得なければならない。
外部業者に委託する場合、秘密保持及び、処分依頼品の再利用の禁止を契約文書に含めなければならない。

5　例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

6　罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『罰則に関する標準』に従わなければならない。

7　公開事項

本標準は対象者にのみ公開するものとする。

8　改訂

・ 本標準は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平

成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

物理的対策標準

0.92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

物理的対策標準

１　趣旨

本標準は、敷地・建物・機器・設備等を保護し、それらの損傷や利用の妨害、許可されていないアクセスを防止することを目的とする。

２　対象者

敷地・建物・機器・設備等の利用に関わるすべての従業員

３　対象システム

敷地内のすべての情報システム

４　遵守事項

４．１　セキュリティ区画の設定

（１） 重要度の高い機器・設備を設置する場所にはその重要度に応じたセキュリティ区画が設定されなければならない。

（２） セキュリティ区画はその範囲を明確にしていなければならない。

（３） セキュリティ区画の管理については管理責任者を置かなければならない。

（４） セキュリティ区画には施錠設備を設けなければならない。

（５） セキュリティ区画は区画およびそこに設置する機器・設備等に関するセキュリティ上の各種のリスクを評価した上で必要な対策を実施しなければならない。リスクの要素には以下のものがある。

・ 盗難、破壊、地震、火災、水害等の水の事故、ほこり、振動、化学作用、電源事故、電磁波、静電気等

４．２　セキュリティ区画の運用

（１）　セキュリティ区画は従業員不在時には施錠しなければならない。

（２）　セキュリティ区画への入場は、管理責任者の許可を受けて登録した特定のメンバに制限さればならない。

（３）　セキュリティ区画への未登録者の入場については必ず入退場を記録し、登録メンバが同伴しなければならない。

（４）　セキュリティ区画に入場する外部からの来訪者には区画内での注意事項を事前に説明しておかなければならない。

（５）　セキュリティ区画に入場可能な登録メンバは定期的に見直さなければならない。

（６）　セキュリティ区画に入場するものは身分証明となるカードあるいはバッジ等を常に明示しておかなければならない。また従業員は身分証明の明示がない入場者の相互確認を行わなければならない。

４．３　機器・設備の保護

（１）　機器・設備の設置位置については、不正な操作が実施しにくく、不用意な操作ミス（間違いや見落とし）が起こりにくいように配慮しなければならない。

（２）　要度の高い機器・設備は他のものと分離して設置しなければならない。

（３）　機器を設置する場合、落下や損傷の防止措置をとらなければならない。

（４）　機器周辺では飲食・喫煙等を行ってはならない。

４．４　電源・空調の保護

（１）　電源・空調室およびその設備には耐震、耐火、耐水などの防災対策を実施しなければならない。

（２） 電源は、安定化装置の導入、負荷変動機器との配電隔離等によって電源容量と品質を確保しなければならない。

（３） 電源は過電流・漏電等による機器への障害に対する保護措置をとらなければならない。

（４） 電源には避雷設備を設置しなければならない。

（５） 重要度の高い機器・設備に対する電源には、無停電装置、バックアップ電源等を設置しなければならない。

（６） 空調設備は機器・設備を適切に運転するために十分な温度・湿度の調整能力を確保しなければならない。

（７） 重要度の高い機器・設備に対する空調設備については予備装置を確保しなければならない。

４．５　ケーブルの保護

（１） ケーブルは、損傷や回線の盗聴を避けるため、保護用の電線管・カバーの使用や、敷設経路に対する配慮などの対策を行わなければならない。

（２） 干渉防止のため、電源ケーブルと通信ケーブルは分離しなければならない。

（３） 重要度の高いケーブルについては代替経路を準備しなければならない。

（４） ケーブルおよび端子については、未認可の機器・設備の接続や設置に対する監視または定期的チェックを行わなければならない。

５　例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

６　罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『罰則に関する標準』に従う。

７　公開事項

本標準は対象者にのみ公開するものとする。

８　改訂

・本標準は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

＊＊＊ 用語 ＊＊＊
機器と設備：設備は動かせないレベルのものを想定する。
重要度の高い機器・設備、重要度の高いケーブル：「重要度の高い情報資産を取扱う機器・設備およびケーブル」と考える。重要度の高い情報資産については別途定める。
従業員：正社員以外の通常勤務しているスタッフも含むものと考える。

サーバルームに関する標準

0.92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

サーバルームに関する標準

１　趣旨

本標準は、サーバルームの設置によってサーバ等を保護し、それらに格納する情報の安全性を確保することを目的とする。

２　対象者

サーバルームの設置と利用に関わるすべての従業員

３　対象システム

サーバルームに設置するサーバ及びその他の機器

４　遵守事項

４．１　サーバルームの定義

（１）　サーバルームの定義は「重要度の高い情報資産が格納されているサーバがまとめて設置される部屋」とする。重要度の高い情報資産については別途定める。

（２）　電子化されたデータとして保存する重要度の高い情報資産は、『クライアント等におけるセキュリティ対策標準』および『媒体の取扱に関する標準』に基づいて管理される場合を除き、サーバルームに設置するサーバでのみ保存されなければならない。

４．２　サーバルームの物理的セキュリティ

（１）　サーバルームは独立した部屋として設置し、一般オフィスとの共用や他社オフィスとの隣接は避けなければならない。

（２）　サーバルームは、危険物保管場所、火気施設、水道設備等、災害のリスクの大きい場所からは遠ざけて設置しなければならない。

（３） サーバルームの外観は目立ちにくいものとし、室名表示等も最小限にとどめなければならない。

（４） サーバルームの出入り口は原則１ヶ所に限定し、施錠設備を設けなければならない。

（５） サーバルームに窓を設けることは極力避け、設ける場合は網付きガラス・強化ガラス等を用いなければならない。

（６） サーバルームには設置する機器・設備の重要度に応じて、防犯カメラ、侵入報知機等の防犯設備の設置を検討しなければならない。

（７） サーバルームには必要に応じて、非常電話、非常ベル等の非常用連絡設備の設置を検討しなければならない。

（８） サーバルームにはコピー・FAX 等、情報の複写や送信のための設備を設置してはならない。

（９） その他のサーバルームの物理的セキュリティについては『物理的対策標準』でのセキュリティ区画の扱いに準ずる。

４．３　サーバルームの運用

（１） サーバルームは従業員不在時には施錠しなければならない。

（２） サーバルームおよびその鍵の管理については管理責任者を置かなければならない。

（３） サーバルームへの入室は、受付または認証装置（入館カード、パスワード入力、生体認証）等によって特定の登録メンバに制限されなければならない。

（４） サーバルームへの未登録者の入室および作業実施については管理責任者の許可と登録メンバの同伴がなければならない。

（５） サーバルームに入室可能な登録メンバは定期的に見直さなければならない。

（６） サーバルームに入室不要となった登録メンバは速やかに登録を解除し、入室のための認証を無効にしなければならない。

（７） サーバルームへの入退室は記録しなければならない。

（８） サーバルーム内で長時間作業を行う場合は一人では実施せず、必ず同伴者を伴わなければならない。

（９） サーバルーム内で管理責任者の許可なく撮影・録音を行ってはならない。

（１０）サーバルームには作業に必要のないものを置いてはならない。もし置いてあった場合は速やかに撤去しなければならない。

（１１）サーバルーム内の環境（機器・設備の有無、配置、利用状況等）は定期的に点検しなければならない。

（１２）その他のサーバルームの運用については『物理的対策標準』でのセキュリティ区画の扱いに準ずる。

5　例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

6　罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『罰則に関する標準』に従う。

7　公開事項

本標準は対象者にのみ公開するものとする。

８　改訂

・本標準は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

＊＊＊ 用語 ＊＊＊
機器と設備：設備は動かせないレベルのものを想定する。
機器・設備の重要度：「機器・設備が取扱う情報資産の重要度」と考える。情報資産の重要度については別途定める。
従業員：正社員以外の通常勤務しているスタッフも含むものと考える。

職場環境におけるセキュリティ標準

0.92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

職場環境におけるセキュリティ標準　153

職場環境におけるセキュリティ標準

１　趣旨

本標準は、職場環境におけるセキュリティリスクを低減し、情報漏えい等のセキュリティ事故を防止することを目的とする。

２　対象者

すべての従業員

３　対象システム

すべての PC、端末およびその他の事務・通信機器

４　遵守事項

４．１　書類・媒体等の取扱いと保管（クリアデスクポリシー）

（１）　従業員は使用していない書類や媒体をキャビネット等へ収納し、机上等に放置してはならない。

（２）　従業員は重要度の高い書類や媒体を施錠保管し、特に必要な場合は耐火金庫・耐熱金庫に保管しなければならない。

４．２　画面に表示する情報の管理（クリアスクリーンポリシー）

（１）　従業員は不正な操作や盗み見防止するため、離席時にはログオフするか、画面・キーボードロック等の保護機能を使用しなければならない。

４．３　事務・通信機器の取り扱い

（１）　従業員はホワイトボード等への書き込み内容を使用後に必ず削除し、放置してはならない。

（２） 従業員はコピー機、FAX、プリンタ等の入出力書類を放置してはならない。特に重要度の高い書類は印刷および送受信の間、従業員が常に機器に（FAX の場合は送受信の両側とも）立ち会うようにしなくてはならない。

（３） 従業員は FAX 送信時には必ず宛先を確認し、誤送信を防止しなければならない。

４．４　搬入物の受渡し

（１） 搬入物の受渡しについては受渡し場所を設置し、『サーバルームに関する標準』で定めたサーバルームおよび『物理的対策標準』で定めたセキュリティ区画とは分離しなければならない。

（２） 受渡し場所への従業員以外のスタッフによるアクセスは、必ず従業員の監視付きで行い、アクセスを記録しなければならない。

（３） 搬入物の受入れを行う従業員は受入れの際に危険物持込や情報漏洩等のリスクがないかどうか点検しなければならない。

（４） 搬入物が登録の必要な情報資産である場合、搬入物の受入れを行う従業員は受入れ後速やかに登録作業を行わなければならない。

（５） 郵便物の受入れ場所には盗み見や抜き取りを防止する対策を行わなければならない。

４．５　盗み聞きによる情報漏えい防止

（１） 従業員は電話や立ち話、オープンな会議スペースでの発言について、盗み聞きを防止するよう配慮しなければならない。

５　例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

６　罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『罰則に関する標準』に従う。

７　公開事項

本標準は対象者にのみ公開するものとする。

８　改訂

・本標準は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本標準の変更を求める者は、情報セキュリティ委員会に申請するしなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

＊＊＊ 用語 ＊＊＊
重要度の高い書類、重要度の高い媒体：それぞれ「重要度の高い情報資産である書類」、「重要度の高い情報資産を格納する媒体」と考える。重要度の高い情報資産については別途定める。
従業員：正社員以外の通常勤務しているスタッフも含むものと考える。

セキュリティインシデント報告・対応標準

0.92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

セキュリティインシデント報告・対応標準

１　趣旨

本標準は、セキュリティインシデントが発生した場合に迅速に対応し、情報システム環境の復旧が円滑になされることを目的とする。

また、当社においてセキュリティインシデントとは次の事態を指す。

（1）情報セキュリティに対する侵害

例：不正アクセスによる情報漏洩、従業員による情報漏洩、ウイルス感染、
なりすまし、使用不能攻撃、ハードウエア紛失　等

（2）システム・ネットワークの故障、損壊

例：電源異常、熱暴走、天災による機器損壊　等

２　対象者

本社・営業所・子会社・関連会社を含む当社のすべての従業員

３　対象システム

当社の従業員が業務上、利用するすべてのシステム

４　遵守事項

４．１　平時の準備

（1） 情報セキュリティ委員会は、『セキュリティ教育に関する標準』に基づいて、セキュリティ教育を実施し、従業員のセキュリティ意識の向上に努めなければならない。

（2） 従業員は業務上、利用するすべてのコンピュータについて、『ウイルス対策標準』に基づいて、適切にウイルス対策を実施しなければならない。

（3） 情報システム部は、『セキュリティ情報収集および配信標準』に基づいて、当社で使用されている製品のセキュリティ情報を収集し、必要なセキュリ

ティ対策を実施することでセキュリティレベルを維持しなければならない。

（4） 情報システム部は、インシデントの検知や原因究明に役立てるために『システム監視に関する標準』に基づいて、適切にログを取得しなければならない。

（5） 情報システム部は、インシデントを検知するため、『システム監視に関する標準』に基づいて、侵入検知システムを利用し、適切にシステムおよびネットワークの監視を行わなければならない。

（6） 情報システム部は、インシデント発生後のシステムの復旧作業に役立てるために『システム維持に関する標準』に基づいて、適切にバックアップを取得しなければならない。なお、バックアップは必要に応じて遠隔地にコピーを保管することが望ましい。

（7） 情報システム部は、インシデント発生後のシステムの復旧作業に必要なリソースを検討し、確保しておかなければならない。

（8） 情報セキュリティ委員会は、各システムの復旧優先度を決定しなければならない。復旧優先度の決定は、対象システムにおいて運用される業務の停止許容時間を観点において行う。
（表１参照）

表１

復旧優先度	業務復旧までの許容時間
3	業務が停止することは許されない
2	24時間以内に復旧しなければならない
1	3日以内に復旧しなければならない
0	インシデント発生時は停止してもよい

４．２　セキュリティインシデント発生時

（1） 従業員はインシデントの発生と疑われる事象を発見した場合、速やかに情報セキュリティ委員会もしくはセキュリティ担当者に報告しなければならない。またクライアント PC において、ウイルス感染や不正アクセスの疑いがある場合、発見後ただちに該当するクライアント PC をネットワークから切り離した上で報告しなければならない。

（2） （1）の報告を受けた情報セキュリティ委員会およびセキュリティ担当者は、下記の観点で状況把握し、対応方法を報告者に指示しなければならない。セキュリティ担当者が報告を受けた場合は、対応方法を報告者に指示するとともに下記事項を速やかに情報セキュリティ委員会に報告しなければならない。
またセキュリティ担当者のみでの作業が困難である場合は、速やかに情報セキュリティ委員会に申し出て、協力を依頼すること。
＜観点＞
・インシデント発生の真偽
・被害を発見した日時
・被害の拡大範囲
・被害内容
・被害原因
・対応方法

（3） インシデントの発生が確認された場合、情報セキュリティ委員会は速やかに関連する部署（情報システム部、広報担当等)、プロバイダー、外部ベンダー等に連絡し、協力を依頼しなければならない。
また、情報セキュリティ委員会は必要に応じて組織横断的なタスクフォースを設け、状況把握や対応方法の指示にあたることができる。

（4） 情報システム部は、インシデントの原因が解消された後、速やかにバックアップテープを用いてシステムを正常な状態に復旧しなければならない。復旧作業にあたっては、４．１（８）で決定した復旧優先度に従って作業すること。

（5） 従業員は、インシデントの 2 次被害防止のため、OS、アプリケーションの入れ替えやクライアント PC の設定変更等の作業が必要になった場合は、情報セキュリティ委員会の指示に従い､速やかに実施しなければならない。

４．３　再発防止計画

（1） セキュリティインシデントへの対応が完了した後、情報セキュリティ委員会および情報システム部は、調査結果をもとに再発防止計画を作成しなければならない。再発防止計画作成時には、技術的側面と組織的側面の両方

に留意すること。

（2） 情報セキュリティ委員会は発生したインシデントのうち、以下の要件を満たすものについては、再発防止計画と共に取締役会に報告しなければならない。

＜要件＞

・社外の第三者からのセキュリティ侵害により当社が被害者となる場合

・顧客や取引先等の社外に対して当社が加害者となる場合

（3） 再発防止計画は、すべての従業員に周知され、適切に実施されなければならない。

（4） 情報セキュリティ委員会は、セキュリティインシデントの発生から再発防止計画作成までの一連の記録を保管・管理しなければならない。

４．４　運用の見直し

４．４（1）　訓練計画

本標準の内容の実効性を担保するため、情報セキュリティ委員会は、定期的にセキュリティインシデントの訓練計画を作成し、従業員参加のもと、訓練を実施しなければならない。

４．４（2）　訓練の評価

・　訓練の結果は情報セキュリティ委員会においてレビューし、セキュリティ対策の運用について改善策の審議を実施しなければならない。

・　訓練の結果は、改善策とともにすべての従業員に周知されなければならない。

４．４（3）　インシデント後の見直し

情報セキュリティ委員会は、セキュリティインシデントの事後に一連の対応を見直し、運用上の改善点を検討しなければならない。検討の結果、運用変更が必要であると認められた場合、速やかに関係する従業員に周知されなければならない。

６　例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

7　罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『罰則に関する標準』に従う。

8　公開事項

本標準は対象者にのみ公開するものとする。

9　改訂

・本標準は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

セキュリティ情報収集及び配信標準

0.92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

セキュリティ情報収集及び配信標準

１　趣旨

本標準は、社内で使用されている製品のセキュリティ情報を収集し、セキュリティレベルを維持する事を目的とする。

２　対象者

当社の情報システム部

３　対象システム

当社に導入されているすべてのソフトウェアおよびハードウェア
“すべて”➔”識別された”がいいなぁ

４　遵守事項

４．１　セキュリティ情報の収集

（１） 情報システム部は『ソフトウェア/ハードウェアの購入標準』で作成された各管理台帳をもとに、社内システムに導入されている全てのハードウェア及びソフトウェアのセキュリティ情報について、定期的に情報を収集しなければならない。

（２） セキュリティ情報は各ベンダーの Web サイトやサポートページなどから収集する。

（３） 情報システム部門（部門⇔部どっち）はセキュリティ関連のメーリングリスト、セキュリティセミナーなどに参加し情報を収集する。

（４） 収集した情報は、重要性、影響範囲などから下記の様に分類する。
危険度　高：サーバの管理権限の剥奪などにより、業務が停止してしまう、または取引先などに影響を与える可能性があり、即座に対応が必要な情報
中：業務が停止するあるいは取引先などに影響は与えないため、

即座に対応する必要はないが、定期メンテナンス時などに対処する必要がある情報

低：特殊な環境/設定でのみ発生し、社内のシステムには関係がないため、特に対処しなくともよい情報

４．２　セキュリティ情報の配布

（１）　情報システム部は、収集した情報を危険度に応じて関係者に対して報告しなければならない。

危険度　高　：発見次第即座に関係者全員に連絡
連絡方法は基本的にはメールを使用。場合によっては社内放送なども利用する。

中　：週１回程度の定例報告を行う。メールにて関係者全員に連絡

小　：週１回程度の定例報告を行う。メールにてシステム管理者に連絡

（２）　情報システム部より通知を受けた者は速やかにその指示に従わなければならない。パッチを適用が必要な場合は『システム維持に関する標準』、ウィルス定義ファイルを更新する場合には『ウィルス対策標準』に基づいて行わなければならない。

（３）　情報システム部は、収集した情報を基に以下のものを作成、公開することが望ましい。

- サーバ設置時の OS の適用パッチ一覧
- サーバ設置時に必要となるサービスなどをまとめたセキュリティ設定チェックリスト
- アプリケーションの適用パッチ一覧
- アプリケーションの実装変更

５　例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

6　罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『罰則に関する標準』に従う。

7　公開事項

本標準は対象者にのみ公開するものとする。

8　改訂

・本標準は、平成 XXXX 年 XX 月 XX 日に情報セキュリティ委員会によって承認され、平成 XXXX 年 XX 月 XX 日より施行する。

・本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

システム監視に関する標準

0.92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

システム監視に関する標準

１　趣旨

本標準は、当社が利用している情報システムの監視について規定し、システム障害、不正アクセスの兆候、情報の流出、不正利用等をいち早く検知し、それらの原因究明が円滑に行われることを目的とする。

２　対象者

当社の情報システム部に所属するすべての社員を適用対象とする。ただし、これに限らず社内においてサーバ、ファイアウォール、主要なネットワーク機器を管理・運用するすべての者について適用する。

３　対象システム

当社の従業員が業務上、利用するすべてのサーバ、ファイアウォールおよび主要なネットワーク機器

４　遵守事項

４．１　対象システムのログによる監視

（１） 情報システム部は､対象システムに関して次にあげるログを取得すること。なお取得されたログは 24 時間以内に書き換え不能なメディアに転送し、3 年間、安全に保管すること。

取得対象：

① ログオン・ログオフの記録
② サーバのアクセスログ
③ ファイアウォールのログ
④ 主要なネットワーク機器のログ
⑤ システムログ

取得内容：

① アクセス時刻

② 発信元/先アドレスとポート番号
③ アクセス成功/失敗
④ 認証成功/失敗

（2） 情報システム部は、許可された処理だけが実行されていることを確認するために、ログを月 1 回解析すること。解析の結果、以下のような事象が確認された場合、情報セキュリティ委員会に報告すること。
① 連続したアクセスの失敗
② 連続した認証の失敗
③ 大量のデータの送受信
④ 権限外の処理の試み
⑤ ユーザアカウントに関する変更（追加、削除、グループ変更等）
⑥ アクセス権の変更

（3） 情報システム部は（2）の事象が、不正アクセスによってもたらされた疑いがある場合には、『セキュリティインシデント報告、対応標準』に基づいて、原因究明、再発防止計画の作成等、適切な対応を実施しなければならない。

（4） 情報システム部は、（1）で取得するログの時間情報を適切に保ち、ログの証拠としての有効性を高めるため、NTP サーバ等を用いてシステム間の時刻同期をとらなければならない。ただし、その場合、NTP サーバ自身のセキュリティ対策にも十分配慮すること。

4．2　侵入検知システムによる監視

（1） 本社のグローバルゾーンおよび DMZ のネットワークにおいては、ネットワーク監視型侵入検知システムを導入し、不正アクセスの発生状況を常時監視すること。

（2） 本社のグローバルゾーンおよび DMZ 上に設置されているサーバにおいては、ホスト監視型侵入検知システムを導入し、不正アクセスの発生状況を常時監視すること。

（3） 情報システム部は、シグネチャベースの侵入検知システムを用いる場合は、

最新のシグネチャにアップデートされた状態を維持しなければならない。

（４） 情報システム部は（１）、（２）の監視によって、不正アクセスの兆候が検知された場合には、『セキュリティインシデント報告、対応標準』に基づいて、速やかに対応しなければならない。

（５） 情報システム部は、侵入検知システムのログを月 1 回分析し、結果を情報セキュリティ委員会に報告しなければならない。

（６） 情報システム部は、侵入検知システムのログを 24 時間以内に書き換え不能なメディアに転送し、3 年間、安全に保管すること。

5　例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

6　罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『罰則に関する標準』に従う。

7　公開事項

本標準は対象者にのみ公開するものとする。

8　改訂

・本標準は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

システム維持に関する標準

0.92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

システム維持に関する標準　175

システム維持に関する標準

１　趣旨

本標準は、当社システムのセキュリティレベルを維持するためのパッチ等の適用ルール及びバックアップルールについて規定する。

２　対象者

当社の情報システム部と各システム管理者及び当社システムを利用する全ての社員

３　対象システム

当社の社員が業務上使用する全てのサーバ、クライアント PC、ネットワーク機器

４　遵守事項

４．１　パッチ適用のルール

（１）　弊社システムの管理者及び使用者は、『セキュリティ情報収集及び配信の標準』に基づいて情報システム部より配信されたパッチ適用の指示に対して、自分が管理または使用している全てのマシンに対して速やかにパッチを適用しなければならない。

（２）　情報システム部は社内全てのマシンに対して、（１）のパッチが指示通り適用されているかを確認する事が望ましい。

（３）　パッチ適用作業によるサービスの停止など他システムへの影響が大きく、速やかに（１）のパッチが適用出来ない場合、システム管理者は情報システム部に連絡しなくてはならない。また、システム管理者はパッチ適用計画を作成し、それに基づいてパッチを適用しなければならない。
（例えば FireWall にパッチを適用するために FireWall を停止しなければならず、その間全ての Web アクセスが出来ないなど）

（４）　システムに対して業務上必要となる修正パッチ等を適用する場合、シス

テム管理者は情報システム部に対して適用したいパッチとその理由について報告しなければならない。

（５） パッチ適用中に何らかのトラブルが発生した場合、作業者はトラブルの内容を情報システム部に報告しなければならない。

（６） 情報システム部は（５）のトラブルの報告を受けた場合、関係各部への連絡を行い今後の対応をする必要がある。

４．２　パッチの取得及び配布方法

（１） WindowsOS 関連のパッチは、システム管理者が MicroSoft のホームページよりダウンロードで取得し、クライアント PC 利用者に対してパッチの置き場所を通知する。

（２） UNIXOS のパッチについては、システム管理者が各ベンダーよりダウンロード取得し、サーバの管理者に対してパッチの置き場所を通知する。

（３） 各アプリケーションのパッチに関しては、システム管理者が各ベンダーより取得する。クライアント PC にインストールが必要な場合はシステム管理者が配布する。

（４） ネットワーク機器のパッチについては情報システム部がベンダーより取得し、ネットワーク管理者にパッチの置き場所を通知する。

４．３　ウィルス定義ファイルの更新

（１） 『ウィルス対策標準』に基づいてウイルス定義ファイルを更新しなければならない

４．４　サーバのバックアップについて

（１） 業務上重要なサーバ（WWW サーバ、mail サーバ、経営・経理・受発注システムなど）については、そのデータ及び log を定期的にバックアップしなければならない。

（２） パッチの適用など、サーバのシステムに対して何らかの変更を行う場合、変更後の不具合が発生する可能性がある。その為、サーバに対して変更を行う前にサーバのシステムバックアップを取らなければならない。

（３） パッチの適用など、サーバのシステムに対して何らかの変更を行った場合は、安定動作確認後にサーバのシステムバックアップを取らなければならない。

（４） バックアップ作業は業務に影響が及ばないように作業時間は十分に配慮しなければならない。

４．５　バックアップ媒体の取り扱いについて

（１） バックアップ媒体はテープとする。

（２） システムバックアップは過去２回分のバックアップデータを保持することが望ましい。

（３） バックアップに使用する媒体は、鍵付きの保管場所に置くなど、サーバ管理者が責任をもって管理しなければならない。

（４） バックアップに使用した媒体の破棄については、『媒体の取り扱いに関する標準』に基づいて処理をしなくてはならない。

４．６　システムの監視について

（１） サーバ管理者及びネットワーク管理者は、システム障害等の兆候をいち早く見つけるために、サーバ及びネットワークの監視を行わなければならない。監視については『システム監視に対する標準』に基づいて行わなければならない。

５　例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

6　罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『罰則に関する標準』に従う。

7　公開事項

本標準は対象者にのみ公開するものとする。

8　改訂

・本標準は、平成 XXXX 年 XX 月 XX 日に情報セキュリティ委員会によって承認され、平成 XXXX 年 XX 月 XX 日より施行する。

・本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

委託時の契約に関する標準

0.92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

委託時の契約に関する標準

１　趣旨

本標準は、当社の業務を外部の業者に委託し、実施する場合の契約における問題および委託作業時の問題を未然に防ぐことを目的とする。

２　対象者

委託を行うすべての従業員

３　対象システム

委託業務で使用するすべてのもの

４　遵守事項

４．１　委託先の選定に関する遵守事項

（１）委託を行う者は、委託先として信頼できる業者を選ばなければならない。

４．２　委託契約に関する遵守事項

（１）委託を行う者は、委託業務の仕様以外に、機密保持に関する以下の契約事項を盛り込まなければならない。

- ✧　委託業者は、当社の業務で知り得た情報を第三者に開示してはならない。

（２）委託を行う者は、委託業務の仕様以外に、情報管理に関する以下の契約事項を盛り込まなければならない。

- ✧　委託業者は、当社の業務を行うにあたって情報管理責任者を明確にしなければならない。
- ✧　委託業者は、当社の業務を行うにあたって入手した情報を適切に管理

しなければならない。

- ✧ 委託業者は、入手した情報をリストアップし、常に授受の状況を明確にしなければならない。
- ✧ 委託業者は、入手した情報を閲覧・利用できる者を特定し、明示しなければならない。
- ✧ 委託業者は、電子媒体で納品する場合、ウイルスが含まれていないことを確かめなければならない。

（3） 委託を行う者は、委託業務の仕様以外に、品質管理に関する以下の契約事項を盛り込まなければならない。

- ✧ 委託業者は、スケジュールに従った作業を実施し、途中経過における進捗状況を明確にしなければならない。
- ✧ 委託業者は、品質管理のために実施する事項を明確にしなければならない。

（4） 委託を行う者は、委託業務の仕様以外に、再委託に関する以下の契約事項を盛り込まなければならない。

- ✧ 委託業者が、再委託を行うためには、当社に事前の承認を得なければならない。

5　例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

6　罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『罰則に関する標準』に従う。

7　公開事項

本標準は対象者にのみ公開するものとする。

８　改訂

・本標準は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

監査標準

0.92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

監査標準　186

監査標準

１　趣旨

本標準では、マネジメントシステムの内部監査にかかわる事項を規定する。

２　対象者

本標準は、情報資産を扱うすべての人を対象とする。権限および責務は以下のグループによって区別される。

・情報セキュリティ委員会およびその構成メンバ

・情報セキュリティ委員会から任命された監査組織、およびその監査人

・被監査組織および被監査人

３　対象システム

本標準は監査に関するものであり、情報システムや情報機器を対象としない。

４　遵守事項

４．１　共通事項

（１）　情報セキュリティ委員会は、監査組織を構成し、定期的に監査を実施しなければならない。監査の周期は、１年に１回とする。監査の周期を変更する際には、情報セキュリティ委員会での承認を得なければならない。

（２）　情報セキュリティ委員会は、監査の対象、目的について、監査組織と協議した上で合意しなければならない。情報セキュリティ委員会は、合意した内容が監査の目的に合致しているかについての責任をもつ。

（３）　監査組織は、合意された内容に基づいて監査を実施し、その結果を情報セキュリティ委員会へ報告しなければならない。情報セキュリティ委員会は、監査の結果を受けて、必要に応じて適切な是正措置を行わなければならない。

（４）　監査組織は、被監査組織、対象に対して独立していなければならない。もし独立した監査組織を構成できない場合には、相互監査体制をとることでできる限り独立性を維持しなければならない。監査組織は、客観的に監査を行わなければならない。

（５）　監査組織は、監査の実施にあたり専門の知識や技能を必要とする場合、専門家の協力を得ることができる。監査組織は、監査の目的について専門家に説明し、専門家による作業の結果について最終的な判断を下すことができなければならない。

（６）監査組織は、監査の過程において知りえた情報を、監査目的以外に公開してはならない。

（７）被監査組織および被監査人は、監査の円滑な実施のために、スケジュール調整、資料の提示、監査立会い等、監査組織の活動に協力しなければならない。

４．２　監査の計画

（１）監査組織は、合意された監査内容に基づいて、監査の計画を立てなければならない。監査組織は、監査の目的として以下を含めなければならない。

・内部統制が正しく規定されているか

・規定された内容にしたがって組織が効率的に実行しているか

（２）監査組織は、監査の計画にあたり以下の内容を検討または実施しなければならない。

・内部統制として実施されている活動内容

・資産およびそれらへのリスクの分析

・セキュリティ方針や標準等の規定の分析

・組織を取り巻く環境の変化

・内部統制を理解するためのヒアリングや観察

（３）監査組織は、監査項目に以下の内容を含めなければならない。

・セキュリティ方針および標準

・情報セキュリティ委員会の構成および実行

・情報資産を含む財産の管理

・社員、契約社員等の扱い

・物理セキュリティ

・通信および運用

・アクセス制御

・システム開発

・事業継続計画

・法律、規制等への準拠

（４）監査組織は、計画した監査項目のそれぞれについて、問題点が内在する可能性について検討し、予測される内部統制リスクを判断した上で、実施手

続きや監査のサンプリング密度を決定しなければならない。

（５） 監査組織は、監査の実施手順および項目について、主要な内容を文書化しておかなければならない。

４．３　監査の実施

（１）監査組織は、各監査人に対して監査の実施を指示する。

（２）監査人は、あらかじめ決められた手続きに基づいて監査を実施する。監査手続きは以下を含む。

・インタビュー

・行動の観察

・証拠等の検閲

・監査人による作業手順の実施

（３） 監査人は、組織内で提供されているサービスの可用性を考慮しなければならない。

（４） 監査人は、システム監査ツールを使用するとき、システムへの影響に細心の注意を払わなければならない。監査時には、一般へのサービスは停止していることが望ましい。

（５） 監査人は、セキュリティ方針と、実際のマネジメント活動を比較して、有効性についての判断をしなければならない。判断する観点としては以下を含む。

・組織の存在意義とセキュリティ方針との整合性

・セキュリティ方針と標準の整合性

・標準の実行に関して使用している設備費用および運用費用等のコストとそれらの妥当性

・PDCA サイクルの適切な実施

（６） 監査人は、監査結果を裏付けるために、監査によって得られた情報を記録しなければならない。

（７） 監査人は、監査によって得られた情報を元に、内部統制リスクが予測範囲内であるかを評価し、実施手続きの妥当性を判断しなければならない。

（８） 監査組織は、監査人からの報告を受けて、発見された問題の量や質が予測範囲を超えており、実施した手続きが妥当でないと判断した場合には、再度監査計画を立案して実行しなければならない。

４．４　監査結果の報告

（1）監査組織は、監査結果を元に監査報告書を作成し、情報セキュリティ委員会へ報告しなければならない。監査組織は、対象者の不在、機密情報に関する閲覧の拒絶など、さまざまな理由によって実施できなかった監査項目を監査報告書に含めなければならない。
（2）監査組織は、監査結果の裏付けとなる十分な根拠を提示できなければならない。
（3）監査組織は、問題点の指摘事項を報告する場合、問題点の重大性に応じて分類しなければならない。監査組織は、問題点を解決するための改善策について、可能な限り監査報告書に含めることが望ましい。
（4）監査報告書は、開示範囲を情報セキュリティ委員会のみとする。

4．5　是正措置

（1）情報セキュリティ委員会は、監査組織からの報告を受けて、是正措置の計画立案をし、実行の判断をしなければならない。
（2）情報セキュリティ委員会は、実行することになった是正措置について、緊急性、および重要性を考慮して、適切な時期に行う。
（3）是正措置の指示を受けた被監査組織または被監査人は、速やかに是正措置を行い、実施した是正内容および時期を情報セキュリティ委員会に報告しなければならない。

5　例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

6　罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『罰則に関する標準』に従う。

7　公開事項

本標準は対象者にのみ公開するものとする。

８　改訂

・本標準は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

＊＊＊用語集＊＊＊
内部統制リスク
システム監査ツール
PDCA サイクル

罰則に関する標準

0.92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

罰則に関する標準

１　趣旨

本標準は、当社のセキュリティ違反に対する罰則の適用手順及びそれに関わる遵守事項を規定する。

２　対象者

本標準は、セキュリティ方針および標準が適用されるすべての人を対象とする。罰則事項の執行は、セキュリティ違反に対する罰則の適用に関わる委員会のメンバー、部門長及び人事部門の担当者を対象とする。

３　対象システム

本標準は罰則に関するものであり、情報システムや情報機器を対象としない。

４　遵守事項

４．１ 罰則案件の届出

部門長は罰則に相当すると思われる社員のセキュリティ違反を確認した場合、委員会に罰則の適用について審議を求める案件の届出を行わなければならない。なお、部門長のセキュリティ違反に関する罰則案件の届け出は委員会のメンバーが行うものとする。

４．２ 委員会での審議及び決定

委員会は届出が行われた罰則案件について審議を行い、罰則の適用と再教育についてその要否と程度または内容を決定しなければならない。

４．３ 人事部門での罰則手続き

人事部門の担当者は委員会での決定に基づき、該当者に対する就業規則に従った罰則の決定及び適用に関する手続きの実施をしなけれならない。

４．４ 再教育

委員会は罰則案件の審議結果で再教育が必要と決定した該当者に対して再教育

を実施しなければならない。

5　例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

6　罰則事項

本標準は、罰則について規定したものであり、遵守事項に違反した者への対応は、情報セキュリティ委員会にゆだねる。

7　公開事項

本標準は対象者にのみ公開するものとする。

8　改訂

・本標準は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

用語集
セキュリティ違反

プライバシーに関する標準

0.92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

プライバシーに関する標準

１　趣旨

本標準は、顧客の個人情報（以下「顧客情報」とする）を適切に収集・維持・破棄における取り扱い時に注意するべき事項をまとめ、発生しうる問題を未然に防ぐことを目的とする。

２　対象者

顧客情報を取り扱うすべての従業員

３　対象システム

顧客情報を取り扱うすべてのコンピュータ

４　遵守事項

４．１　顧客情報を取り扱う部門の特定

（１）　情報セキュリティ委員会は、当社内にて顧客情報を取り扱う部門を特定し、その部門長に対して、以下の遵守事項を徹底されなければならない。

（２）　特定されていない部門においては、顧客情報を取り扱ってはならない。

４．２　顧客情報管理責任者の設置

（１）　顧客情報の収集・維持・破棄を行う部門の部門長は、顧客情報管理責任者を設置し、部門内の責任者を明確にしなければならない。

４．３　顧客情報保護方針の公開

（１）　顧客情報管理責任者は、顧客情報を広く一般から収集する場合、当社の Web サイトや広告等に当社の顧客情報保護方針を公開しなければならない。

（２） 顧客情報保護方針には、下記に記載される遵守事項の内容および当社への連絡先を明確にしなければならない。

４．４　顧客情報の収集

顧客情報の収集を行う者は、以下の事項を遵守しなければならない。

（１） 顧客情報の収集時には、顧客に対して利用目的を明示し、顧客から同意を得なければならない。なお、収集以外の形で得た顧客情報を利用する場合は改めて顧客から同意を得なければならない。

（２） 顧客に示した利用目的に関する情報以外を収集してはならない。

（３） 収集した情報を顧客に提示した利用目的以外の利用をしてはならない。

４．５　顧客情報の維持

顧客情報管理責任者は、以下の事項を遵守しなければならない。

（１） 顧客情報に対する登録・参照・変更・削除の実施可能な者を明確にし、顧客情報へのアクセス制限を実施しなければならない。

（２） 顧客情報を利用する場合、正確な情報を利用しなければならず、そのための保護策を実施しなければならない。

（３） 顧客情報のバックアップを実施しなければならない。バックアップした媒体は、顧客情報と同様の管理策を設けなければならない。

（４） 顧客から当該顧客の顧客情報に関する開示・訂正・削除の要求があった場合、これに対応しなければならない。

４．６　顧客情報の破棄

顧客情報管理責任者は、以下の事項を遵守しなければならない。

（１） 客情報を破棄する場合、第三者の目にさらされないように注意して破棄しなければならない。

（2）電子媒体等の破棄においては、『媒体の取り扱いに関する標準』に基づいて実施しなければならない。

４．７　顧客からクレーム処理

顧客情報管理責任者は、以下の事項を遵守しなければならない。

（1） 当社の業務において顧客からクレームを受けた場合には、速やかに対応しなければならない。

（2） 顧客情報が漏えいしてしまったなど必要がある場合、情報セキュリティ委員会を開催し、当社の見解を迅速に明確にしなければならない。

（3） どのようなクレームが発生した場合でも、第一報を 12 時間以内に報告し、その後の対応状況に関しても適宜連絡しなければならない。

5　例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

6　罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『罰則に関する標準』に従う。

7　公開事項

本標準は対象者にのみ公開するものとする。

8　改訂

・本標準は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速

やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

プロシージャ配布の標準

0.92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

プロシージャ配布の標準

１　趣旨

本標準は、規定された、または更新されたプロシージャを、対象者に適切に配布し周知することを目的とする。

２　対象者

プロシージャの開示を許可されたすべての従業員

３　対象システム

本標準はプロシージャ配布に関するものであり、情報システムや情報機器を対象としない。

４　遵守事項

４．１　対象者への周知

（１） 情報セキュリティ委員会は、プロシージャの制定、および更新を実施した場合、迅速に開示が許可された対象者へ周知しなければならない。

４．２　配布の手段

（１）情報セキュリティ委員会は、プロシージャを Web 上で公開する。
（２）Web サーバへのアクセスは、開示が許可された対象者のみが閲覧できるように正しく制御されなければならない。
（３）情報セキュリティ委員会は、ネットワーク上の問題等によってプロシージャの閲覧ができなくなることを避けるために、一定数の紙媒体によるプロシージャを保有していなければならない。

４．３　対象者の確認

（１）情報セキュリティ委員会は、Web ベースによる理解度チェック問題など、

対象者の理解度を確認するための手段を用意しなければならない。

（２）対象者は、情報セキュリティ委員会からの周知を受けてから、速やかにプロシージャの内容を確認し、理解しなければならない。

（３）対象者は、情報セキュリティ委員会が用意した理解度確認用の手段を、周知後１週間以内に実施しなければならない。

４．４　実施の確認

（１）情報セキュリティ委員会は、対象者が理解度確認の手段をすべて実施し、必要な条件を満たすことにより、プロシージャを受け取り正しく理解したとみなすことができる。

（２）各部署のセキュリティ責任担当者は、各担当者の実施状況を Web のツールで確認することができる。セキュリティ責任担当者は、未実施者を識別し、未実施者に対して実施を促さなければならない。セキュリティ責任担当者は、やむを得ない理由で対象者の実施が困難な場合、速やかに情報セキュリティ委員会に報告しなければならない。

5　例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

6　罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『罰則に関する標準』に従う。

7　公開事項

本標準は対象者にのみ公開するものとする。

8　改訂

・本標準は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

用語集

（特になし）

セキュリティ教育に関する標準

0.92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

セキュリティ教育に関する標準

１　趣旨

本標準では、セキュリティ教育、訓練に関わる事項を規定する。

２　対象者

教育、訓練の対象者は、当社のコンピュータに携わっているすべての人、またはそれを運用、管理し、業務に携わっているすべての人を対象とする。
（例）
教育対象者、経営者、システム管理者、オペレータ、利用者、第三者利用者、訓練対象者、システム管理者、オペレータ

３　対象システム

本標準はセキュリティ教育に関するものであり、情報システムや情報機器を対象としない。

４　遵守事項

４．１ 教育の計画立案

教育部門ならびに、各部署のセキュリティ責任担当者は、対象者およびタイミング、もしくはその内容について、各教育を計画し、立案しなければならない。

一般説明会
教育部門は、年に１回、コンピュータに携わるすべての人に対して、セキュリティに関する説明会を実施しなければならない。

再教育
教育部門は、セキュリティ違反者に対して、セキュリティの再教育を実施し、違反の再発防止に努めなければならない。

新入社員、中間採用者への教育
教育部門は、新入社員、中間採用者に対して、入社時にセキュリティ教育を実施

しなければならない。

社内異動者への教育
各部署のセキュリティ責任担当者は、社内異動者に対して、異動時に、その部署の情報セキュリティに関して教育を実施しなければならない。

契約社員および協力会社への教育
各部署のセキュリティ責任担当者は、契約社員および協力会社に対して、部署の情報セキュリティに関して、許可された権限と責務に応じた教育を実施しなければならない。

４．２ 教育の実施

教育部門ならびに、各部署のセキュリティ責任担当者は、コンピュータに携わるすべての人に対し、以下の教育内容について、教育資料を使用し、セキュリティの教育を実施しなければならない。

教育内容

- ・情報セキュリティの問題のもつ意味を理解
- ・組織や個人の情報セキュリティの重要性
- ・セキュリティ対策
- ・情報セキュリティ計画
- ・データ所有者の責任
- ・モラル教育
- ・禁止行為に関しての教育他
- ・啓発

４．３ 訓練の実施

教育部門ならびに、各部署のセキュリティ責任担当者は、セキュリティに責任をもつ対象者に対し、定期的に、以下の訓練内容について、訓練資料を使用し、セキュリティの訓練を実施しなければならない。

訓練内容
・リスク分析
・セキュリティ対策についての導入、管理、運用、利用等
・セキュリティ問題の検出、検知、報告、復旧等

４．４ 教育、訓練資料

教育、訓練資料は、適切な教育、訓練を行うため、定期的な見直し行う。

教育、訓練資料には、以下のものがある。
・一般説明会教育資料
・再教育資料
・新入社員教育資料
・中間採用者教育資料
・社内異動者教育資料
・協力会社および契約社員教育資料
・セキュリティ対策訓練資料
・セキュリティ問題訓練資料

４．５ 教育実施記録

教育部門は、教育、訓練の実施状況に関して以下の記録を行わなければならない。

記録項目
・教育の実施日
・教育実施者（部署）
・教育の受講者
・教育の内容

４．６ 教育運用実施報告、確認

教育部門は、情報セキュリティ委員会に教育、訓練の実施状況を報告しなければならない。
情報セキュリティ委員会は、セキュリティの教育、訓練が適切に行われているかを把握するため、教育部門から提出されるセキュリティ実施報告書を確認しなければならない。実施されていない場合、教育部門に対して、適切な指導を行わなければならない。

５　除外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

６　罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『罰則に関する標準』に従う。

７　公開事項

本標準は対象者にのみ公開するものとする。

８　改訂

・本標準は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

用語集

スタンダード更新手順に関する標準

0.92a 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.92 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.92 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

スタンダード更新手順に関する標準

１　趣旨

本標準は当社のスタンダードを更新する場合の手順及びそれに関わる遵守事項を規定する。

２　対象者

本標準はスタンダードの更新に関わる委員会のメンバーを対象とする。

３　対象システム

本標準はスタンダード更新手順に関するものであり、情報システムや情報機器を対象としない。

４　遵守事項

４．１ 更新案件の提案

委員会のメンバーはスタンダード更新の必要性を認識した場合、そのスタンダードの更新について提案することができる。

４．２ 委員会での審議及び決定

委員会は提案された更新案件について審議を行い、更新を実施するかどうかを決定しなければならない。

４．３ 更新結果の反映と記録

委員会は実施することが決定した更新案件についてスタンダードの文言の変更を行うとともに、変更内容の記録を残さなければならない。

４．４ 担当役員に対する報告

委員会は実施することが決定した更新案件について担当役員に報告しなければならない。

５　例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

6　罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『罰則に関する標準』に従う。

7　公開事項

本標準は対象者にのみ公開するものとする。

8　改訂

・本標準は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

用語集
（特になし）