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

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。