# 1. 外部ネットワーク接続　セキュリティ基本方針

0.9 版

---------- 取扱注意事項 ----------

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「外部接続に関する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. 既存のネットワークにおける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 作成サンプルポリシー」を明記して下さい。営利目的でも非営利目的の区別はありません。
   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などマスコミ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

## 1　外部ネットワーク接続　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、我社に導入されて久しい。その間、我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。

一方、昨今の度重なるセキュリティに関しての事件は、我社にとっても「対岸の火事」ではなく、被害に遭わないように、早急に対応しなければならない事象である。

このような状況を鑑み、今後は、セキュリティを意識したネットワークコンピュータの利用を行っていかなければならないことは自明である。

我社は、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、我社は、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。

我社は、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、我社の情報資産を、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。

我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。

情報セキュリティポリシーは、組織全体を対象範囲としなければならないものであるが、今回公表する情報セキュリティポリシーは我社の「外部接続ネットワーク」に特化した文書である。