

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きな把握

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著作権は、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ェ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
1 趣旨.....	1
2 対象者.....	1
3 対象システム.....	1
4 遵守事項.....	1
4.1 私物 PC の使用禁止.....	1
4.2 PC に導入するソフトウェア.....	1
4.3 PC の他者への利用の制限.....	2
4.4 PC での情報の取り扱い.....	2
4.5 ウィルス対策の徹底.....	2
4.6 PC の移設.....	3
4.7 ノートパソコンの利用上の注意事項.....	3
5 例外事項.....	3
6 罰則事項.....	3
7 公開事項.....	3
8 改訂.....	3

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××年××月××日に情報セキュリティ委員会によって承認され、平成××年××月××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。