

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

Webサービス利用標準	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 Web ブラウザ利用端末機器のセキュリティ	1
4.2 Web ブラウザの利用	2
4.3 社内ネットワークの Web サーバの利用.....	2
4.4 アクセス制御された Web サイトの閲覧に関して	3
4.5 Web サイトの閲覧状況の監視許可.....	4
5 例外事項.....	4
6 罰則事項.....	4
7 公開事項.....	4
8 改訂.....	4

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××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。