１４．Ｗｅｂサービス利用標準

0.91 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(0.91 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(0.91 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

１４．Ｗｅｂサービス利用標準

１４．１　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。

１４．２　対象者

Web ブラウザを利用するすべてのネットワーク利用者

１４．３　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

１４．４　遵守事項

１４．４．１　業務目的以外の利用禁止

（１） 社内ネットワーク利用者は、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。対象者は、業務上必要でない Web サーバへアクセスしていることを発見した場合、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。

（２） 社内ネットワーク利用者は、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。

（３） 社内ネットワーク利用者は、信頼できない Web サーバにアクセスしてはならない。

（４） 社内ネットワーク利用者の情報の発信（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

（５） 社内ネットワーク利用者は、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。

（６） 社内ネットワーク利用者は、社内外の Web サーバに対して、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。

１４．４．２　Web ブラウザ利用端末機器のセキュリティ

（１） 社内ネットワーク利用者は、Web ブラウザの利用にあたって、情報セキュリティ委員会が指定した 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） 上記ソフトウェアを使用するコンピュータは、『PC 購入/導入（IT 製品購入/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） 社内ネットワーク利用者は、インターネット上のサイトアクセスするときは、必ず情報セキュリティ委員会が指定する Proxy サーバを経由しなければならない。

１４．４．３　インターネット上の Web サーバへのアクセス

（１） 社内ネットワーク利用者は、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。

（２） 社内ネットワーク利用者は、インターネット上のサイトへのアクセスにおいて、Cookie の設定をオフにしなければならない。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。

（３） 社内ネットワーク利用者は、署名の無い ActiveX や Java、JavaScript、VBScript などのコードは実行してはならない。但し、信頼できるサイトに登録されていない場合でも、システム管理者より通知があった場合には、実行してもよい。

（４） 社内ネットワーク利用者は、システム管理者の許可のないソフトウェアもしくはファイルをインターネット上からダウンロードして、実行、閲覧してはならない。

（５） 社内ネットワーク利用者は、リンクをクリックするとき、リンク先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。できれば、バナー広告ブロックのソフトウェアを導入することが望ましい。

１４．４．４　社内ネットワークでの Web 閲覧

（１） 社内ネットワーク利用者は、情報システム部の許可を得なで Web サーバや情報を他部門や子会社へ情報を公開する目的のサーバは立ち上げではならない。不審な Web サーバを発見した場合は、速やかに情報システム部に報告しなければならない。

（２） 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。

（３） 社内ネットワーク利用者は、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は、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。

１４．４．５　アクセス制御された Web サイトの閲覧に関して

（１） 社内ネットワーク利用者は､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） 社内ネットワーク利用者は、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） 社内ネットワーク利用者がクライアント証明書を必要とする場合は、情報セキュリティ委員会の承認後取得申請できるものとする。これらの証明書は各自厳密に管理しなければならない。

１４．４．６　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、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

長への報告を行わなければならない。

１４．５　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。

１４．６　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。

１４．７　公開事項

本標準は対象者にのみ公開するものとする。

１４．８　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
Web ブラウザ
サイト
Web サーバ
掲示板
不正なアクセス
攻撃
Proxy サーバ

SSL