ユーザ認証標準

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

ユーザ認証標準

１　趣旨

本標準は、情報を守る為に使用されるユーザ認証に関して、セキュリティを確保しつつ利便性を実現する運用を目的として記述されている。パスワードの長さや文字の種別、更新頻度、対象機器については、実現方法に関する技術の進歩が著しいので、技術動向を見極めた上で、本標準が適宜更新されることが望ましい。

２　対象者

ユーザ認証を行わなければならない全ての従業員

３　対象システム

以下のいずれかの条件を満たす機器、システム及びアプリケーションには、ユーザ認証を用いて情報セキュリティの確保に努めなければならない。

① 汎用的に使われている OS などでネットワーク機能を持つ機器
② ハードディスクなどの記憶媒体を持つ機器
③ ルータ
④ ユーザが用いるメールソフトウェア
⑤ 社内情報共有の為のイントラネットソフトウェア

４　遵守事項

４．１　ユーザ認証を用いたセキュリティ確保

情報セキュリティの維持に影響を与える機器、システム及びアプリケーションで、ユーザ認証を行える機器、システム及びアプリケーションの中で、セキュリティ上重要な意味を持つにも関わらず、ユーザ認証が無い機器、システム及びアプリケーションは使用してはならない。

４．２　対象システムによる認証システムの選定

情報システム部門は、対象システムが関わる重要性と、セキュリティを実現する手法の難易度を勘案してユーザ認証システムを構築しなければならない。情報システム部門は、ユーザ認証の仕組みには、パスワードと生体認証のいず

れかを用いて情報システムを構築しなければならない。

４．３　パスワード

（１） 8 文字以上で記号を 1 文字以上含むことが望ましい。

（２） 一般に使われている単語や本人の趣味、プライベートなどから、他人に推測されやすいパスワードを使用してはならない。

（３） 設定されたパスワードは１ヶ月に一度を目安にパスワードは更新することが望ましい。

（４） パスワードは原則として該当システムの管理者が生成して管理を行うものとする。設定したパスワードは紙などに書き留めてもよいが、対象システムが特定できたり、パスワードの文字列そのものを「あらわに」書き留めたりしてはならない。

（５） パスワードは口外したり、ヒントとなるような物品を身の回りに置いておいてはならない。

（６） 一度使用したパスワードを連続でなくとも使用してはならない。

（７） 一度使用したパスワードを他のシステムなどに使用してはならない。

４．４　初期設定のパスワード

（１） 利用者が最初に使用する初期設定のパスワードは、情報システム部が発行し、口頭もしくは書面で該当者に通知する。

（２） 初期設定のパスワードは、社員番号などの規則性のある予測できるものに設定してはならない。

（３） 利用者はパスワードが発行された後速やかに自らログインしパスワードを変更しなければならない。

（４） システム管理者は、初期設定のパスワードが発行された利用者がログインしパスワードが変更されたことを確認しなければならない。原則として、初期設定のパスワードが発行されてから３日以内に、パスワードの設定変更が確認されない場合には、該当する利用者のアカウントを削除、もしくは無効にしなければならない。

４．５　パスワードを忘れた場合の処置

（１） 利用者がパスワードを忘れた場合には、システム管理者に新規パスワード発行の申請を行わなければならない。

（２） システム管理者は、申請してきた利用者が本当に本人自身であることを何らかの方法で確認しなければならない。

（３） 新規パスワード発行の申請を受けたシステム管理者は、速やかに新規のパ

スワードを発行して、利用者に通知しなければならない。

４．６　ワンタイムパスワード

（１） ワンタイムパスワードは PIN 番号などの認証が必要なものを用いなければならない。

（２） 時刻同期などの認証を必要としない機器は使用してはならない。

（３） ワンタイムパスワードの発生器は、PIN 番号などを推測出来るような状態で携帯してはいけない。

４．７　生体認証

（１） パスワードの記憶と管理が困難な場合には、生体認証を用いても良いが、最新技術動向やコストなどを勘案して、適切な方式を選択しなければならない。

（２） 生体認証を使用する場合には、生体認証のデータそのものが重要な個人情報であるので、厳重に管理しなければならない。

（３） パスワードの利用に対する利便性向上の手段としては、指紋認証などの簡単な生体認証を用いることができる。

（４） サーバルームなどの高いセキュリティを要求される場所への立ち入りの管理には、虹彩認証などの高レベルのセキュリティが期待できる認証システムを用いなければならない。

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：
ユーザ認証
利用者
情報セキュリティ委員会
PC
ソフトウェア
Web ブラウザ
常時設置型コンピュータ
携帯端末
生体認証
情報システム部