7.リモートアクセスに関する標準

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

リモートアクセスに関する標準

趣旨

我社は、ダイヤルアップで社内ネットワークに接続するリモートアクセスから、社内の情報資産を守るために、セキュリティ対策を実施する。

本標準は、リモートアクセスを利用することによる、我社の情報資産を外部から守るために、必要な対策を継続的に実施するものである。

対象者

下記を本標準の遵守義務対象者とする。

・リモートアクセスを利用する全員
・リモートアクセスを管理するシステム管理者
・リモートアクセスを運用するオペレータ

対象機器・対象システム

下記を本標準の遵守義務対象機器・対象システムとする。

・リモートアクセスで利用する機器（ＰＣ、ＰＤＡ、携帯電話など）
・リモートアクセスサーバ
・ＶＰＮ装置
・リモートアクセスシステム
・インターネット接続システム
・外部公開サーバ

遵守事項

・ダイヤルアップによる社内ネットワークへのアクセスは、情報システム部門が構築したものを利用しなければならない。
・ダイヤルアップルータおよびサーバとモデムなどによる社内ネットワークへの接続手段を、情報システム部門の許可を得ることなく設置してはならない。

管理に関する遵守事項

・リモートアクセスで使用するＰＣおよび携帯電話は、情報セキュリティ委員会が定める利用者のみ利用することができる。
・リモートアクセスで使用するＰＣおよび携帯電話の管理は、所有する利用者が行わなければならない。

・リモートアクセスの管理は、情報システム部門（システム管理者およびオペレータ）が行わなければならない。

利用環境に関する遵守事項

・リモートアクセスで利用できる機器は、情報セキュリティ委員会の定める機器でなければならない。

・ノート型ＰＣ
・ＰＤＡ
・携帯電話（ｉモード）

・リモートアクセスの利用場所は、情報セキュリティ委員会の定める場所でなければならない

・外出先（国内、海外）
・支社・支店・営業所・工場
・ユーザ先
・自宅

・リモートアクセスによる接続は、情報セキュリティ委員会の定める通信形態でなければならない。

・インターネット経由（ＰＣ、携帯電話）
・公衆回線（電話回線、ＩＮＳ回線、携帯電話）

・リモートアクセスで利用できるサービスは、情報セキュリティ委員会の定めるものでなければならない。

・ｈｔｔｐ・ｈｔｔｐｓを利用したサービス
・電子メール
・ファイル転送
・ファイル共有
・業務システム

アカウント管理に関する遵守事項

・リモートアクセスで利用するＰＣおよび携帯電話は、利用者（社員）が情報システム部門に申請をし、利用者情報（識別番号、パスワード等）を入手しなければならない。

・利用者名
・利用場所
・利用目的
・利用期間
・接続機器（機器種別、ＯＳ種類）

・接続形態

・　情報システム部門は、利用者情報（利用者、識別番号、パスワード等）の登録・変更・削除を適時行い管理しなければならない。

アクセス制御に関する遵守事項

・リモートアクセスでは、社内にアクセスできるサーバおよびサービスは必要最低限にしなければならない。

・リモートアクセスでは、利用者毎にアクセスできるサーバおよびサービスを決めることとする。

・リモートアクセスでは、社内に設置されたサーバのみにアクセスすることができる。

・リモートアクセスでは、申請時に許可された社員のみインターネットへのアクセスをすることができる。

リモートアクセスサーバに関する遵守事項

・リモートアクセスサーバは、専用サーバまたはNW機器でなければならない。

・リモートアクセスサーバは、利用者情報を管理することができなければならない。

・リモートアクセスサーバは、利用者認証（発信者識別、ワンタイムパスワード）に対応していなければならない。

・リモートアクセスサーバは、通信手段としてコールバックとＶＰＮ（暗号化）に対応していなければならない。

・リモートアクセスサーバは、接続記録を蓄積でき各種データを外部媒体に保管できなければならない。

・接続成功

・接続失敗

・接続の開始時間と終了時間

・接続時のアカウント名

・発信者識別

・障害情報（エラー情報）

クライアントに関する遵守事項

・クライアントは、利用する社員を識別（利用者識別名・パスワード）し該当者以外の利用をできないようにしなければならない。

・クライアントは、ワンタイムパスワードまたはコールバックに対応していなければならない。

・クライアントは、通信手段として発信者識別・ＶＰＮ（暗号化）に対応していなければならない。
・クライアントには、情報セキュリティ委員会が定めたソフトウェアをイントールし動作しなければならない。

利用手順に関する遵守事項

・リモートアクセスする場合、クライアントと利用者を識別する情報を入力しリモートアクセスサーバで認証をしなければならない。
・インターネットを利用してリモートアクセスする場合には、ワンタイムパスワードを利用し認証をしなければならない。
・公衆電話または携帯電話を利用してリモートアクセスする場合には、ワンタイムパスワードを使用し認証しなければならない。
・上記以外の通信手段を利用してリモートアクセスする場合には、コールバックを使用し認証しなければならない。
・リモートアクセスしている間に利用者がクライアントから離れる場合、クライアントを停止するか第三者の利用ができないようにしなければならない。

検査と監視に関する遵守事項

・リモートアクセスの利用者は、リモートアクセス利用のための教育を受け一定のレベルになっていることが望ましい。
・リモートアクセスで使用するＰＣは、十分なセキィリティ対策を実施後システム管理者の検査を受け承認されたＰＣのみ接続することができる。
（利用者認証、ワンタイムパスワード、ウィルス対策、ＶＰＮ、スクリーンセーバ等）。
・情報システム部門は、定期的（年４回）に外部で使用するＰＣおよび携帯電話が適切に利用されているか検査しなければならない。
・リモートアクセスサーバは、接続記録を蓄積・管理をし定期的（毎月）に解析しなければならない。

緊急対応に関する遵守事項

・システム管理者は、リモートアクセスサーバに対し、外部から侵害・侵入された場合、リモートアクセスを停止し、原因調査および対策を実施しリモートアクセスを再開始しなければならない。
・リモートアクセスで使用するＰＣおよび携帯電話を紛失した場合には、速やかにシステム管理者に報告し具体的な指示を受けな対処しなければならない。
・リモートアクセスで使用するＰＣおよび携帯電話で使用するパスワードを忘れ

た場合には、システム管理者に連絡をし新たなパスワードへの変更をしなければならない。
・リモートアクセスで使用するＰＣが障害になった場合には、速やかにシステム管理者に報告しシステムの再構築をしなければならない。

物理セキュリティ遵守事項

・リモートアクセスで使用するＰＣおよび携帯電話は、所有者の周囲に置き管理できるようにし、使用しないときはきちんと管理された場所で保管しなければならない。
・リモートアクセスサーバは、システム管理者以外が利用できなく安全・予防対策のされた場所に設置されなければならない。

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。

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ことがある。罰則の適用については罰則に関する標準に従う。

公開事項

本標準は対象者にのみ公開するものとする。

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すること。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すること。
・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すること。