１５ リモートアクセスサービス利用標準

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

１５ リモートアクセスサービス利用標準......2
１５．１ 趣旨......2
１５．２ 対象者......2
１５．３ 対象機器・対象システム......2
１５．４ 遵守事項......2
１５．４．１ 使用機器に関する遵守事項......2
１５．４．２ 機器の管理に関する遵守事項......3
１５．４．３ 利用環境に関する遵守事項......3
１５．４．４ アカウント管理に関する遵守事項......4
１５．４．５ アクセス制御に関する遵守事項......4
１５．４．６ リモートアクセスサーバに関する遵守事項......5
１５．４．７ クライアントに関する遵守事項......5
１５．４．８ 利用手順に関する遵守事項......6
１５．４．９ 検査と監視に関する遵守事項......6
１５．４．１０ 緊急対応に関する遵守事項......7
１５．４．１１ 物理セキュリティ遵守事項......7
１５．５ 例外事項......7
１５．６ 罰則事項......7
１５．７ 公開事項......8
１５．８ 改訂......8

１５ リモートアクセスサービス利用標準

１５．１ 趣旨

　本標準は、ダイヤルアップ等により社内ネットワークを利用する、リモートアクセスサービス利用にあたり、当社の情報資産を外部から守ることを目的とする。

１５．２ 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

１５．３ 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）
・リモートアクセスシステム
・VPN 装置
・リモートアクセスサーバ
・インターネット接続システム
・外部公開サーバ

１５．４ 遵守事項

１５．４．１ 使用機器に関する遵守事項

（１） 利用者は、ダイヤルアップによる社内ネットワークへのアクセスにおいて、情報システム部が構築した機器を利用しなければならない。

（２） 利用者は、ダイヤルアップルータおよびサーバ・モデムなどによる社内ネットワークへの接続手段を、情報システム部の許可を得ることなく設置してはならない。

（３） その他社内 LAN 環境への接続にあたり、利用機器は、『LAN における PC（サーバ、クライアント等）設置/変更/撤去の標準』に基づいて設定されなければならない。

１５．４．２ 機器の管理に関する遵守事項

（１） 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。

（２） 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。

（３） リモートアクセスの管理は、情報システム部（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。

１５．４．３ 利用環境に関する遵守事項

（１） 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）

（２） 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）
・営業所・関連会社等、当社関連施設
・ユーザ先
・自宅

（３） 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）

（４） 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
・電子メールサービス
・ファイル転送サービス
・ファイル共有サービス
・業務システムとして導入しているサービス

１５．４．４ アカウント管理に関する遵守事項

（1） 利用者は、『LAN における PC 設置/変更/撤去の標準』に準じ、リモートアクセスサービスの利用において、個人所有の機材を利用してはならない。

（2） 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

（3） 情報システム部は、利用者情報（利用者、識別番号、パスワード等）の登録・変更・削除を適宜行い、それを管理しなければならない。

１５．４．５ アクセス制御に関する遵守事項

（1） 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。

（2） 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。

（3） 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。

（４） 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。

１５．４．６ リモートアクセスサーバに関する遵守事項

（１） リモートアクセスサーバは、専用機器（ルータ、サーバ等）または複数のネットワーク機器で構成されなければならない。

（２） 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。

（３） 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。

（４） 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。

（５） 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）

１５．４．７ クライアントに関する遵守事項

（１） 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。

（２） 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ず、それを利用しなければならない。

（３） 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ず、それを利用しなければならない。

（4） クライアントは、『クライアント等におけるセキュリティ対策基準』を満たし、かつ『ウィルス対策標準』を満たしていなければならない。

（5） 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。

１５．４．８ 利用手順に関する遵守事項

（1） 利用者は、リモートアクセスを行う場合、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されなければならない。

（2） 利用者は、インターネットを利用してリモートアクセスする場合、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。また、VPN を利用する事が望ましい。

（3） 利用者は、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、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。

（4） 利用者は、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、コールバック機能を使用し認証しなければならない。

（5） 利用者は、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に、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。

１５．４．９ 検査と監視に関する遵守事項

（1） 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。

（2） 情報システム部は、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。

（3） リモートアクセスサーバは、接続記録を蓄積・管理し、定期的（毎月）に解析しなければならない。

１５．４．１０ 緊急対応に関する遵守事項

（1） 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てリモートアクセスを再開始しなければならない。

（2） 利用者は、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、速やかにシステム管理者に報告し具体的な指示を受け、対処しなければならない。

（3） 利用者は、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、システム管理者に連絡し、速やかに新たなパスワードへ変更しなければならない。

（4） 利用者は、リモートアクセスで使用する PC に障害が発生した場合、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。

１５．４．１１ 物理セキュリティ遵守事項

（1） 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、使用しない時には、定められた場所で保管しなければならない。

（2） 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・予防対策がなされた場所に設置されなければならない。

１５．５ 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。

１５．６ 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。

１５．７ 公開事項

本標準は対象者にのみ公開するものとする。

１５．８ 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。