

## 6.専用線及びVPN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著作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](mailto: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](mailto:sec@jnsa.org)

専用線及び VPN に関する標準 .....	2
趣旨 .....	2
対象者 .....	2
対象システム .....	2
遵守事項 .....	2
接続手順 .....	2
許可するサービス .....	3
リモート管理 .....	3
アクセスコントロール .....	3
安全な設定 .....	4
運用 .....	4
パスワード .....	4
ログの保存 .....	4
ログの解析 .....	5
継続した安全な設定の適用 .....	6
設定の変更 .....	6
運用履歴 .....	6
バックアップ .....	6
設置場所 .....	6
検査 .....	7
監視 .....	7
監視方法 .....	7
緊急対応 .....	7
例外事項 .....	8
罰則事項 .....	8
公開事項 .....	8
改定 .....	8

## 専用線及びVPNに関する標準

### 趣旨

当社とその取引先、或いは我社の遠隔の工場や事務所と円滑かつ効率よく業務を遂行するために、VPN 及び専用線によってネットワークが接続される場合がある。この場合に、接続される両端の組織のお互いがネットワーク犯罪の被害者や加害者、あるいは踏み台にならないことを目的とする。

VPN 及び専用線接続は、当社及び取引先の業務効率の向上をもたらす反面、接続されるネットワークがお互いに脅威にさらされることにもなるので、接続そのものの企画は十分慎重に行われることが望ましい。

### 対象者

- ・VPN 及び専用線接続を申請する者
- ・情報セキュリティ委員会
- ・VPN 及び専用線接続のシステム管理者、オペレータ

### 対象システム

- ・接続される専用線の両端のネットワーク
- ・専用線接続に用いられるルータ、ファイアウォール、IDS

### 遵守事項

#### 接続手順

VPN 及び専用線接続の新設には、以下の手順を要する。

#### 申請

システム工事完了期限付き許可

VPN 及び専用線接続契約書の締結

#### システム工事

検査合格

運用開始

VPN 及び専用線接続を新設するためには「VPN 及び専用線接続申請書」を情報セキュリティ委員会に提出し許可を得なければならない。申請には、担当者の押印だけでなく所属長部長職相当の押印が必要である。

申請を受けた情報セキュリティ委員会は、直ちに審査を開始しなければならない。

「VPN 及び専用線接続申請書」には以下の記述が必須である。

- ・ 接続先住所、組織名称
- ・ 接続種別（専用線、VPN）
- ・ 接続開始希望日
- ・ 接続先双方のシステム構成
- ・ 接続先双方のアクセス許可範囲
- ・ 許可されるサービスとその方向性
- ・ 接続先双方のシステム管理者名、システムセキュリティ責任者名
- ・ 接続先双方の異常の定義と異常連絡体制
- ・ 接続先双方の運用管理手順書の添付

情報セキュリティ委員会は、申請内容を十分に審査し適当であると判断された場合には、「システム工事完了期限付き許可」を通知する。

「システム工事完了期限付き許可」が通知された申請者は、その接続先が社外の場合には「VPN 及び専用線接続契約書」を締結しなければならない。

「VPN 及び専用線接続契約書」には「VPN 及び専用線接続申請書」に準じた内容が記載され、更に、責任の範囲及び責任者を明確に記載しなければならない。

「システム工事完了期限付き許可」が通知された申請者は、指定された期日までにシステム工事を完了し、「VPN 及び専用線接続検査申請書」により検査を申請し、検査を受けなければならない。

本スタンダードが適用される以前の既存の VPN 及び専用線接続については、速やかに逐次本スタンダードに適合するようにしなければならない。

#### 許可するサービス

VPN 及び専用線接続によって利用が許可されるサービスは、必要最小限にとどめられなければならない。

#### リモート管理

リモート管理の通信は暗号化されなければならない。

#### アクセスコントロール

VPN 及び専用線接続に用いられるルータではアクセスコントロールが施され、サービスの必要なサーバやネットワークのみ通信が行えるようにアクセスが制限されなければならない。ただし、ファイアウォールを用いる場合には、ルータでアクセスコントロールを行う必要はなく、ファイアウォールで適

切なアクセスコントロールを行う。

アクセスコントロールは、送信元及び送信先アドレスだけでなく、時間や通信量の制限も含まれ、いずれも必要最小限にとどめられなければならない。

#### 安全な設定

VPN 及び専用線接続に用いられるシステムは、安全な設定が施されていないなければならない。安全な設定とは、以下の要件を満たすものである。

- ・最新の OS
- ・最新のアプリケーション
- ・最新のセキュリティパッチの適用
- ・不要なプログラムやサービスの削除

#### 運用

##### パスワード

ルータ、サーバ等全てのパスワードが利用できる機器には、パスワードが付加されなければならない。特に管理者もしくは管理者に類する権限を持つアカウントのパスワードは、下記のように厳重に設定されなければならない。

- ・システム管理者自身が設定する
- ・8文字以上
- ・大文字小文字の区別がある場合には大文字を1文字以上含める
- ・記号が含められる場合には1文字以上含める
- ・数字が含められる場合には1文字以上含める

設定されたパスワードには、以下の運用がなされなければならない。

- ・1ヶ月に一度必ず更新されなければならない
- ・同じパスワードを異なる機器、異なる時期に使用してはならない
- ・設定されたパスワードは、システム管理者が責任を持って携行及び保管する手帳類以外には書き留めてはならない
- ・現場に駆けつけられない止むを得ない非常の場合を除いて、システム管理者以外に教えてはならない
- ・パスワードを入力する際は、他人に見られないよう注意しなければならない

##### ログの保存

通信の経路にあるルータやアクセス対象のサーバやファイアウォールで

は、ログを保存しなければならない。

サーバやファイアウォールのログには以下の項目が含まれていなければならない。

- ・アクセス成功
- ・アクセス失敗
- ・内部エラー
- ・IP アドレス
- ・ログインを伴う場合にはアカウント名
- ・時間

ルータのログには以下の項目が含まれていなければならない。

- ・アクセスコントロール違反
- ・IP アドレス
- ・時間

ログは、一時的にハードディスク等の書き換え可能なメディアに保存されていても良いが、24時間以内に書き換え不能なメディアに転送され厳重に保管されなければならない。

一時的にハードディスク等の書き換え可能なメディアにログを記録する場合には、十分な記憶容量を確保しておき、異常な量の書き込みが発生した場合においても十分に対処できるように備えておかななければならない。

ログは、その取得日から3年間は確実にシステムセキュリティ責任者のみが参照できる場所と方法で厳重に保管されなければならない。

#### ログの解析

保存されたルータやサーバやファイアウォールのログは、システムセキュリティ責任者、もしくはシステムセキュリティ責任者の許可を受けたシステム管理者により解析されなければならない。

ログの解析は少なくとも1ヶ月に1回以上定期的に行わなければならない。セキュリティ侵害や、その可能性がある場合は随時行わなければならない。

ログの解析を行う際は以下の点に注意しなければならない。

- ・許可されていないIP アドレス
- ・指定時間外のアクセス
- ・アクセス頻度
- ・データ量
- ・度重なるアクセス失敗

#### 継続した安全な設定の適用

安全な設定は継続して行われなければならない。即ち、新しいセキュリティパッチが公開された場合には、速やかに適用しなければならない。

セキュリティパッチの適用により既存サービスが継続できなくなる場合には、ファイアウォールやルータ、IDS、或いは対象機器自身の設定変更により新しい脅威の対策を確実に講じなければならない。

#### 設定の変更

該当システムの既存の設定を変更する場合には、変更の程度に応じて手続きを行わなければならない。

- ・重要でないファイルの削除等を行う場合は、業務日誌に記入しなければならない。
- ・サービスのバージョンアップ等を行う場合は、業務日誌に記入し、情報セキュリティ委員会に報告しなければならない。
- ・新規アカウントの追加や、新規サービスの追加等の変更を行う場合は、「VPN及び専用線接続設定変更申請書」を情報セキュリティ委員会に提出して許可を得なければならない。

#### 運用履歴

設定変更等の運用履歴は、紙もしくは磁気媒体で作成され該当システムのシステムセキュリティ責任者が保管する。

#### バックアップ

該当システムへのセキュリティ侵害に備え、データ、システム設定ファイル等の該当システム上の全ての情報のバックアップを取らなければならない。

バックアップは1日に1回取らなければならない。

バックアップを取ったメディアは、その取得日から3年間は確実にシステムセキュリティ責任者のみが参照できる場所と方法で厳重に保管されなければならない。

#### 設置場所

VPN及び専用線接続で用いられるルータやファイアウォール等、アクセスコントロールを施している機器、及び、データベースやアプリケーション等重要なデータを扱っている機器類は、全て安全な場所に設置されていなければならない。安全な場所とは、以下のことをいう。

- ・施錠されていること
  - ・明示的に許可された者以外の立ち入りが禁止されている
  - ・ネットワークの盗聴が外部から行えないこと
- ・監視カメラが設置されていること

## 検査

VPN 及び専用線接続はその運用開始前に必ず検査を受けなければならない。検査には以下の項目が含まなければならない。

- ・最新の脆弱性情報を含む検査項目
- ・システムの申請書との整合性
- ・許可された範囲以外へのアクセスが出来ないこと
- ・アクセスコントロール定義の確認

検査は、接続両端からお互いの方向に対して行われなければならない、検査結果はお互いに対して公開する。検査に合格するまでは接続は接続試験や検査の目的以外で接続してはならない。また、検査は2ヶ月ごとに継続して実施されなければならない。もし、検査に不合格になった場合には、1週間以内に対策を行い再検査を受け、以後これを繰り返す。

## 監視

VPN 及び専用線接続は以下の監視方法で、システムセキュリティ責任者、もしくはシステムセキュリティ責任者の許可を受けたシステム管理者により行われなければならない。

### 監視方法

- ・ルータやファイアウォール専用機器の監視には NIDS を使用するものとする。
- ・アクセス対象のサーバの監視には HIDS を使用するものとする。

### 緊急対応(IR)

セキュリティ侵害された場合や、その可能性がある場合は、その事象レベルにより、緊急に適切な対応をしなければならない。

緊急対応の対象となる事象と、その対応方法例は以下のとおりである。

対象事象：VPN 及び専用線が切断された場合

対応方法：サーバ等への攻撃が行われていないか確認し、原因が見当たらない場合は、プロバイダ等の通信事業者へ切断事由、復旧予定等について確認を行った上、情報セキュリティ委員会に報告し、指示に従わなければならない



らない。

対象事象：アクセスコントロール違反が発見された場合、

度重なるアクセス失敗が発見された場合、

業務時間外の大量のデータダウンロードが発見された場合

対応方法：接続元の IP アドレスを確認し、該当マシンの利用者に事実関係の有無を確認の上、操作ミス以外の理由による場合は、情報セキュリティ委員会に報告し、指示に従わなければならない。

#### 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。

#### 改定

- ・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。

#### 付録

VPN 及び専用線接続申請書

VPN 及び専用線接続契約書

VPN 及び専用線接続設定変更申請書

## 用語

VPN：インターネットを介した仮想専用線

専用線：通信事業者と契約により固定的に接続される回線

専用線接続：専用線により両端のネットワークが接続されること

システムセキュリティ責任者：VPN 及び専用線接続によるネットワークの監督責任者

システム管理者：システムセキュリティ責任者の監督の下に、VPN 及び専用線接続における実際の設定や、運用管理を行う者

オペレータ：システム管理者の指示により設定等の操作を行う者

ルータ：通信経路を制御する機器

ファイアウォール：内部ネットワークと、外部ネットワークを隔て、内部から、もしくは外部からのパケット、及びサービスをフィルタリングする機器

IDS：ネットワーク上を流れるパケットを監視するための機器

NIDS：ネットワーク型 IDS

HIDS：ホスト型 IDS

セキュリティパッチ：OS、アプリケーションのセキュリティホールを塞ぐための修正プログラム