# ２７．専用線及び VPN に関する標準

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

# ２７．専用線及び VPN に関する標準

## ２７．１ 趣旨

本標準は、当社とその取引先、或いは当社営業所・関連会社と円滑かつ効率よく業務を遂行するために構築された VPN 及び専用線によるネットワークにおいて、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。

## ２７．２ 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

## ２７．３ 対象システム

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

## ２７．４ 遵守事項

### ２７．４．１ 接続手順

（１） VPN 及び専用線接続の新設には、以下の手順を要する。
① 申請
② 完了期限付きシステム工事許可
③ VPN 及び専用線接続契約書の締結
④ システム工事
⑤ 検査合格
⑥ 運用開始

（２） 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はなく所属長部長職相当の押印が必要である。

（3） 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。

（4） 「VPN 及び専用線接続申請書」には以下の記述が必須である。

① 接続先住所、組織名称
② 接続目的
③ 接続種別（専用線、VPN）
④ 接続開始希望日
⑤ 接続先双方のシステム構成
⑥ 接続先双方のアクセス許可範囲
⑦ 許可されるサービスとその方向性
⑧ 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
⑨ 接続先双方の異常の定義と異常連絡体制
⑩ 接続先双方の運用管理手順書の添付

（5） 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、「完了期限付きシステム工事許可」を通知する。

（6） 「完了期限付きシステム工事許可」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。

（7） 「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。

（8） 「完了期限付きシステム工事許可」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。

（9） 本標準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、速やかに逐次本標準に適合するようにしなければならない。

### ２７．４．２ 許可するサービス

（１） 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。

### ２７．４．３ リモート管理

（１） VPN および専用線接続のシステム管理者が、何らかの理由でリモートアクセスにより、対象システムを管理する場合には、その通信は暗号化されなければならない。

### ２７．４．４ アクセスコントロール

（１） VPN および専用線接続のシステム管理者は、VPN 及び専用線接続に用いられるルータで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るよう管理しなければならない。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。

（２） 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。

### ２７．４．５ 安全な設定

（１） 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ければならない。安全な設定とは、『ネットワーク構築標準』『サーバ等におけるセキュリティ標準』に準じ、以下の要件を満たすことが望ましい。

・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

### ２７．４．６ パスワード

（１） 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、『ユーザ認証標準』に基づいたパスワードが付加されなければならない。

### ２７．４．７ ログの保存

（１） VPN および専用線接続のシステム管理者は、通信の経路にあるルータ、アクセス対象のサーバおよびファイアウォールでログが保存されるようにしなければならない。

（２） サーバおよび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

（３） 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

（４） 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。また、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ければならない。

（５） 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。

### ２７．４．８ ログの解析

（１） 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。

（２） 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ず、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。

（３） 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

### ２７．４．９ 継続した安全な設定の適用

（１） VPN および専用線接続のシステム管理者は、安全な設定が継続して行われるよう努めなければならない。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。

（２） 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への対策を確実に講じなければならない。

### ２７．４．１０ 設定の変更

（１） VPN および専用線接続のシステム管理者は、該当システムの既存の設定を変更する場合において、変更の程度に応じて手続きを行わなければならない。また、以下の点に留意しなければならない。
・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。

### ２７．４．１１ 運用履歴

（１） 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。

### ２７．４．１２ バックアップ

（１） VPN および専用線接続のシステム管理者は、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、該当システム上の全情報のバックアップを取らなければならない。

（２） バックアップは１日に１回取得し、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。

### ２７．４．１３ 設置場所

（１） 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、『サーバルームに関する標準』に準じ、以下を満たすことが望ましい。

・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

### ２７．４．１４ 検査

（１） VPN 及び専用線接続はその運用開始前に、必ず情報セキュリティ委員会の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れなければならない。

・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

（２） 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ず、検査結果はお互いに対して公開する。また、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ず、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。

### ２７．４．１５ 監視

（１） 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。

### ２７．４．１６ 監視方法

（１） 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し、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。

### ２７．４．１７ 緊急対応(IR)

（１） 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。

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。

### ２７．５ 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。

### ２７．６ 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。

### ２７．７ 公開事項

本標準は対象者にのみ公開するものとする。

### ２７．８ 改定

- 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。