TTC技術レポート
Technical Report

TR-1000

セキュリティ要件書
(VPN ユーザ編)

第 1.0 版

2001 年 8 月 30 日制定

社団法人
情報通信技術委員会

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

TTC Telecommunication Technology Committee

目　　次

＜参考＞

１．技術レポート作成の経緯

本技術レポートは、企業内で IP-VPN システムを構築する際にセキュリティ確保の観点からシステム構築者が守るべき要件を整理したものである。

２．国際勧告等との関連

関連する国際勧告はない

３．改版履歴

版数	発行日	改版内容
第 1 版	2001 年　8 月 30 日	制定

４．参照している勧告、標準など

なし

５．技術レポート作成部門

第四部門委員会　第三専門委員会　サブワーキンググループｂ

１．主旨および前提条件

1.1　主旨

本要件書は、企業内で IP-VPN システムを構築する際にセキュリティ確保の観点からシステム構築者が守るべき要件を整理したものである。

1.2　前提条件

本要件書は、下記の前提条件のもとで検討されている。（図1参照）

・同一企業におけるIP-VPNの構築を想定している

・IP-VPN機器は同一機器でかつシステム管理者は同一とする

・VPN機器はIPSecプロトコルを備えており、使用することとする

また、要件の選定にあたって行ったリスク分析は、以下の前提条件のもとで検討されている。

・物理的な範囲：VPN機器間に置かれた機器およびネットワーク

・守るべき資産：VPN間を流れるデータおよび本支店内部のデータ

なお、守るべき資産の「本支店内部のデータ」は、インターネット接続によって発生する新たな脅威に対応している。

リスク分析の前提、条件等

前提

・同一企業におけるIP-VPNの構築

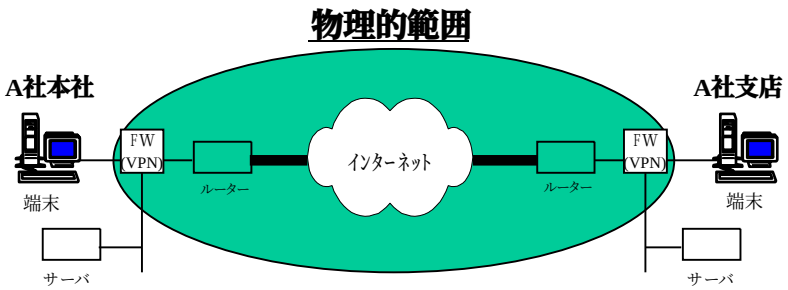
・VPNは同一機器でかつシステム管理者は同一

リスク分析の範囲

・物理的な範囲:VPN-VPN間の機器およびネットワーク

・守るべき資産:VPN間を流れるデータおよび本支店内部のデータ

（後者は、インタネット接続によって発生する脅威に対応）



1.3　用語定義

本書に用いられる主な用語の定義は、以下の通りである。

(1)情報システム関連

①IP-VPN　インターネット上で VPN を実現する技術

②F/W　インターネットに接続された LAN で、外部からは特定の公開されたサービス以外は使えないようにし、内部 LAN のセキュリティを保つためのソフトウェア、またはシステム

③UPS　コンピュータを正常に稼働させ続けるために、電気の供給を雷や地震、火災などによる停電事故などから回避させる装置

④アクセス制御　ハッカーやクラッカーなどからの不当なアクセスを制御するために、前もって決めて

おく規制

⑤追跡・監査機能（ログ）／ログ情報　保護対象資源の処理状況の把握ができ、利用主体が特定できる機能および情報

⑥鍵交換　IPSec で用いられる、セッションキーを VPN 機器間で交換すること

⑦鍵情報　VPN 機器の所持している秘密鍵情報及び、セッションキー情報

⑧業務情報　社内 LAN 内に存在するデータ

(2)設備関連用語

①ネットワーク室　ホストコンピュータ、サーバなどのコンピュータ機器を設置するために専用に設計された、入退室装置を備えている室

②回線　社内 LAN を構築しているネットワーク機器、及びケーブル等

(3)リスク分析関連

①脅威レベル

想定される脅威の発生の起こりやすさにより、以下のように分類する。

・高：　専門の知識および準備がなくとも実行が可能

・中：　それなりの知識があり、それなりの準備があれば達成可能

・小：　達成するためにはかなりの専門知識と周到な準備が必要

②資産レベル

狙われる資産の価値を、以下のように分類する。

・高：　VPNで暗号化すべき情報および内部の機密情報

・中：　上記情報が漏洩、解読するために必要な情報、および不正発見のための情報（EX.設定情報、鍵情報、ログ情報など）

・小：　システム機器、VPNサービス

③リスクカテゴリ

脅威レベル、資産レベルの両面より、以下のように分類する。

・カテゴリA：　脅威もしくは資産レベルの、片方あるいは両方がレベル高のもの

・カテゴリB：　カテゴリAでなく、脅威もしくは資産レベルの、片方あるいは両方がレベル中のもの

・カテゴリC：　カテゴリA、Bに含まれないもの

④対策レベル

各脅威に対する対策を、有効性や費用の面から以下のように分類する。

・必須　　IP-VPN システムを構築する場合、必ず実施もしくは対策を行うべき項目

・強く推奨　IP-VPN システムを構築する場合、実施もしくは対策を行うことが望ましい項目

・推奨　　IP-VPN システムを構築する場合、実施もしくは対策を行うことが推奨される項目

1.4　基準の構成

本基準は、設置基準、技術基準及び運用基準から構成されており、その内容は以下の通りである。

（１）　設置基準（2 項目）

VPN 機器の構成要素の障害、不法侵入者による破壊行為等の危険から、物理的に保護するための設備及び機器の設置環境面の対策

（2）　技術基準（9 項目）

VPN 機器の具備すべき機能を、円滑かつ安全に発揮するための、ハードウェアおよびソフトウェアによる技術面の対策

（3）　運用基準（9 項目）

設置基準、技術基準で示すそれぞれの対策の適切な運用を図り、VPN 機器の安全性および信頼性を確保するための運用面の対策

２．VPN ユーザが守るべきセキュリティ要件

2.1　設備対策要件

項目	対策項目	対策レベル	解説ページ
1 機器の配置	VPN 機器は入退出管理機能があるネットワーク室に設置すること	必須	9
2 電源設備	VPN 機器には UPS 装置を備えること	強く推奨	10

2.2 技術対策要件

項目	対策項目	対策レベル	解説ページ
1 アクセス制御機能	VPN 機器へのアクセス制御機能を有し正しく設定すること	必須	12
2 追跡・監査機能	追跡・監査機能を設けること（ログの収集）	必須	13
3 設定項目	設定項目（ルール）を正しく設定し試験を行うこと	必須	14
4 暗号強度	信頼できる暗号アルゴリズム、鍵長を利用すること	必須	15
5 出荷時の設定	VPN 機器の出荷時の設定を正しく設定しなおすこと	必須	16
6 ハッキング対策	ハッキング対策を行うこと	必須	17
7 暗号鍵の変更	暗号鍵の変更が適切に行われる機能を有すること（鍵交換を行うこと）	強く推奨	18
8 動作監視機能	VPN 機器の動作状況の監視機能を有すること	推奨	19
9 装置の２重化	装置を 2 重化する機能を有すること	推奨	20

2.3 運用対策要件

項目	対策項目	対策レベル	解説ページ
1 運用管理	VPN の運用管理体制を明確にすること	必須	21
2 ログ分析・保管	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること	必須	22
3 バックアップ	VPN のソフトウェアをバックアップすること	必須	23
4 ウイルス対策	ウィルス対策ソフトによりウィルスの発見、駆除を行うこと	必須	24
5 パッチファイル	常に最新のパッチファイルをインストールすること	必須	25
6 パスワードの変更	VPN 機器の定期的なパスワードの変更を行うこと	必須	26
7 機器動作の監視	VPN 機器の動作状況の監視を行うこと	推奨	27
8 クロスチェック	設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること	推奨	28
9 メンテナンス	VPN 機器の定期的なメンテナンスを行うこと	推奨	29

３．VPN ユーザが守るべきセキュリティ要件の解説

3.1　設備対策要件の解説

機器の配置

設-1	対策レベル
VPN 機器は入退出管理機能があるネットワーク室に設置すること	必須

1. **基準の趣旨**

   VPN サービスを継続して提供できるようにするために、以下の行為が行われることを未然に防止する。

   ･VPN 機器そのものに対する、盗難、破壊、停止

   ･VPN のプログラムに対する、破壊、停止

   ･VPN の設定データに対する、盗難、破壊

2. **対策のポイント**

   ・ネットワーク管理者またはネットワーク管理者が認めた者以外の人間が、容易に入室できないようにする。

3. **実施例**

   ・パーティションで仕切られたネットワーク室を用意し、その中に VPN **機器を設置する。同時に、ネットワーク室の出入り口に施錠をする。施錠は、**ID **カードおよび暗証番号入力も必要な電子錠により行う。**

4. **留意事項**

   ・鍵(ID **カード)や暗証番号は、それをネットワーク管理者以外の人間が容易に持ち出せないような場所に保管すること。**

電源設備

設-2 VPN 機器には UPS 装置を備えること	対策レベル 強く推奨

1. **基準の趣旨**

   VPN システムではネットワークの重要度から見て、通常のインターネットを利用したネットワークよりも信頼性向上が求められる。商用電源のトラブル（瞬時停電、電圧降下、電圧変動、過電圧等）から VPN 機器を保護するため、UPS（Uninteruptable Power Supply：無停電電源装置）の設置を推奨する。

2. **対策のポイント**

   UPS の選択は下記２点の項目より決める。

   ① VPN 機器の最大消費電力 W（ワット）と消費 VA を調べる。
   機器の取扱説明書等から電源容量を調べる。

   ② バックアップする時間を決める。
   USP の設置は電源トラブルへの対応が主目的であり、５～３０分程度のバックアップ時間が妥当と思われる。計画停電等長時間の停電への対応まで含めると電源設備として自家発電装置の設置が必要となる。その場合は、停電から自家発電装置からの電源供給までが UPS のバックアップが必要な時間である。

   VPN 機器の消費電力 W と消費 VA を上回る定格容量を持つ UPS で指定したバックアップ時間が得られるものを UPS のカタログ等から選択し使用する UPS を決める。

3. **実施例**

4. **留意事項**

   ・UPS の定格容量以上に VPN 機器等の負荷を UPS に接続した場合、UPS が正常に動作しなくなったり故障したりする可能性があり注意が必要。
   ・UPS では商用電源トラブル時の電力供給源としてバッテリーを使用している。バッテリーには寿命がある（小型シール型鉛畜電池では３～４年）ので、寿命となる前に新しいバッテリーと交換する必要がある。
   ・UPS が商用電源トラブル時に正常に動作することを、UPS 装置の自己診断機能等により定期的に確認する事。

3.2 技術対策要件の解説

アクセス制御機能

技-1	対策レベル
VPN 機器へのアクセス制御機能を有し正しく設定すること	必須

1．基準の趣旨

ＶＰＮ機器はインターネットに接続されているため、外部からアクセスされてパスワードや鍵等の秘密情報を盗まれたり、設定を変更されてＶＰＮの機能を果たさなくなってしまう危険性がある。従って、ＶＰＮ機器へのアクセスを制御する機能を有し、不正にアクセスされないように正しく設定しなければならない。また、外部からだけでなく、内部の管理者以外の利用者が不正にまたは過失でアクセスしてしまう可能性もあり、同様に対応が必要である。

2．対策のポイント

ＶＰＮ機器へのアクセス方法としては、ＦＴＰ、ＴＥＬＮＥＴ、ＨＴＴＰ、コンソールやディスプレイからの設定／操作画面へのアクセス等がある。このような機能に対しての不正なアクセスを防止するためのポイントを挙げる。

・各ＶＰＮ機器によって設定／操作及び管理のための手段として提供しているサービスは同じではないため、使用するＶＰＮ機器に関して、アクセス方法としてどのような機能があるかをまず把握する。実際に運用する上で必要な機能を判断し、不要なサービスはできるだけ停止する。

・ＶＰＮ機器には適切なパスワードを設定し、管理者以外の者がアクセスできないようにする。パスワードは類推されにくいものにし、管理者以外の者が入手できないようにしなければならない。また、不正アクセスの試みを検知し、アクセス元を追跡できるような監視機能を使用することも重要である。

・ＶＰＮ機器にフィルタリング機能が搭載されている場合は、不必要なアクセスをフィルタリングするように設定することも有効である。

3．実施例

例えば、ＶＰＮ機器へのアクセスは、「ＦＴＰ、ＨＴＴＰ、コンソール入力のみ」、「管理者のみ」、「内部からのみ」に限定し、以下の設定を行なう。

- ＶＰＮ機器にアクセス用のパスワードを設定する。パスワードは管理者のみが知り得る情報である。
- ＶＰＮ機器に、その他のアクセス機能があり、機能を停止できる場合は停止するように設定する。
- ＶＰＮ機器に、外部からＶＰＮ機器宛てのデータは遮断するようなフィルタリング機能があれば設定する。

追跡・監査機能

技-2	対策レベル
追跡・監査機能を設けること（ログの収集）	必須

1．基準の趣旨

ログ情報は不正侵入を検出し不正者の追跡するために用いられる重要な手がかりとなる情報である．ログ情報には，イベントに対して次のような項目を記載することが一般的である [1].

イベントが起こった時刻，ユニークな識別子，イベントタイプ，成功したかどうかのフラグ，
要求元 ID，アクセスされたオブジェクトの名前，管理者が作成した履歴情報.

また，不正者を検出した際にリアルタイムにサービスを停止したり，管理者に通知するなどの副産物的な管理も可能となる．さらに未知の攻撃手法を発見するための捜査資料としても活用可能である．

２．対策のポイント

ログ情報が攻撃者により改竄されたり消去されるとログを収集する意味をなさないため，これらを防止する手段が必要である．この手段を講じることで攻撃を抑制する効果も期待されており，ログ情報の改竄・消去が不可能であることを利点とした製品も見受けられる．

３．実施例

ログ情報の改竄・消去の防止手段には CD-R などの Write Once メディアを利用し，一度記録された情報を変更不可能にする方式が最も有効である．その他にもログを暗号化する方式 [2] やログ情報を複数のサーバに分散管理する方式，ログファイル自体を隠蔽しログの削除を考慮した方式などがある．

４．留意事項

[1] A GUIDE TO UNDERSTANDING AUDIT TRUSTED SYSTEMS, NCSC-TG-001VERSION-2, http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-001-2.html

[2] Secure Syslog, http://www.core-sdi.com/

設定項目

技-3 設定項目（ルール）を正しく設定し試験を行うこと	対策レベル 必須

1．基準の趣旨

VPN 機器を用いた暗号通信を適切に行うため、通信相手ごとに暗号化手段を決定し、正常に暗号化されているか確認するための試験を行うこと。

2．対策のポイント

（1） 暗号化するべき相手と暗号化方式を決定し、ルールテーブルを作成すること。

（2） 作成したルールテーブルに基づき、VPN 機器を正しく設定すること。

（3） 設定後テストデータを送信し、パケットキャプチャー装置により適切に暗号化が行われているか、確認すること。

3．実施例

（1） ルールテーブルの設定例

図 1 に示すような、本社、支社 X、支社 Y 間で VPN 機器を用い暗号化通信を行う場合の、ルールテーブルの設定例を表１に示す。

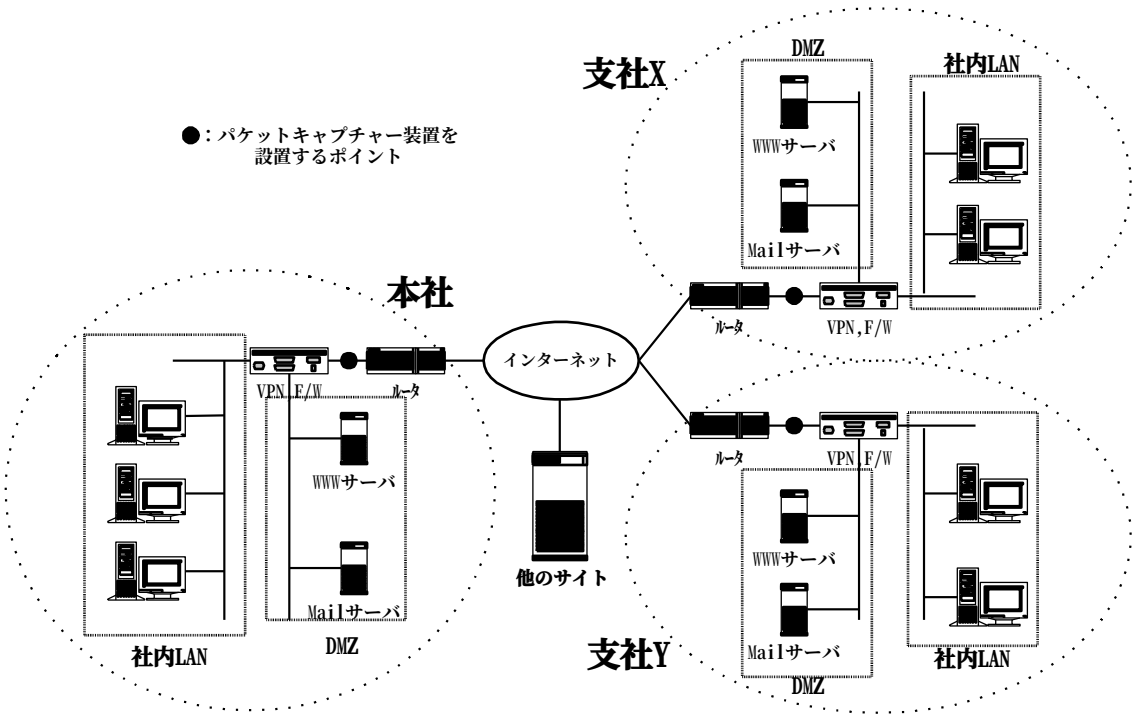


図１　システム構築例

From \ To			本社			支社 X			支社 Y			他のサイト
			DMZ		内部 LAN	DMZ		内部 LAN	DMZ		内部 LAN	
			WWW サーバ	Mail サーバ		WWW サーバ	Mail サーバ		WWW サーバ	Mail サーバ		
本社	DMZ	WWW サーバ		-	-	×	×	×	×	×	×	×
		Mail サーバ	-		-	×	○	○	×	○	○	×
	内部	LAN	-	-		×	○	○	×	○	○	×
支社 X	DMZ	WWW サーバ	×	×	×		-	-	×	×	×	×
		Mail サーバ	×	○	○	-		-	×	○	○	×
	内部	LAN	×	○	○	-	-		×	○	○	×
支社 Y	DMZ	WWW サーバ	×	×	×	×	×	×		-	-	×
		Mail サーバ	×	○	○	×	○	○	-		-	×
	内部	LAN	×	○	○	×	○	○	-	-		×
他のサイト			×	×	×	×	×	×	×	×	×	

○ ： 暗号化を行う

× ： 暗号化を行わない

表 1 ルールテーブル

（2） 試験項目の例

ルールテーブルの設定が正しく行われているか、テストデータを送信し、パケットキャプチャー装置を図 1 に示した場所へ接続し以下に示す試験を行う。

・暗号化を行う全ての通信相手に対し、テストデータ送信し、パケットキャプチャー装置により暗号化されているか確認する。

・他のサイトのインターネット接続サーバに対し、テストデータを送信し、パケットキャプチャー装置により暗号化が行われていないことを確認する。（複数のサーバに対しテストを行う）

4．留意事項

（1） 通信相手の変更があった際や、ソフトウェアの更新を行った際は、改めて見なおすこと。

（2） 暗号技術は標準に準拠していること。

暗号強度

技-4 信頼できる暗号アルゴリズム、鍵長を利用すること	対策レベル 必須

1．基準の趣旨

ＶＰＮ機器を利用するにあたって必要となる暗号アルゴリズムの選択基準について示す。

2．対策のポイント

暗号化アルゴリズムを選定するにあたっては以下のポイントが重要となる。

①暗号強度

②性能

①の暗号強度については暗号アルゴリズムが持つ鍵の長さに依存する。鍵長が長ければ強度に優れる。ただし、鍵長が長くなるとＶＰＮ機器が暗号データを解読する際に時間を要すことになり②の性能に関わってくる。従って、①と②の関係を踏まえた上で選択する必要がある。

3．実施例

ＶＰＮ機器で一般的にサポートされる暗号化アルゴリズムは以下の通り。

名称	鍵長	補足
DES	56bit	1977 年、米ＮＩＳＴにて標準化
Triple DES	168bit	DES 暗号化を３回行う。
RC2	可変長（0～2048bit）	米 RSA 社で開発
RC5	可変長(0～2048bit)	米 RSA 社で 1995 年に提案
CAST	可変長(1～128bit)	RFC2144 として公開されている。

4．留意事項

ＶＰＮ機器でサポートされる暗号化アルゴリズムは上で挙げたようなものが採用されている。鍵長については固定であったり可変長であったりするが、選択にあたってはなるべくＶＰＮ機器でサポートされる最長の鍵長を採用する。

出荷時の設定

技-5	対策レベル
VPN 機器の出荷時の設定を正しく設定しなおすこと	必須

１．基準の趣旨

出荷時のデフォルト設定は公知であるため，その状態のまま運用されている機器に対しては公知の攻撃が存在する可能性がある．つまり，正しい管理権限を持つ者以外がログの閲覧や設定変更などの操作が可能な状態で出荷されている製品もあると考えられる．このような攻撃は VPN 製品に特化したものではなく WWW サーバ，FTP サーバにも存在する脅威であり，ベンダーからの最新情報を常に得ておくことも必要になる．

２．対策のポイント

正しい管理者を機器が認識するためにパスワード認証を行うことが多い．出荷時のデフォルトのパスワードをそのまま利用することにより攻撃の対象となりうるため，パスワード変更は必須である．

また，複数のユーザで管理を行う場合には，設定を変更・操作できる権限を正しく設定しているかどうかを確認する必要がある．特にネットワーク経由での設定変更が可能かどうかか重要なポイントとなる．外部からの設定変更を禁止することがセキュリティ的観点からは最善であるが，運用の簡便性とのトレードオフになるため実運用とのバランスが必要である．

３．実施例

本運用に入る前に，外部のネットワークと接続していないテストベットでのテスト運用を行い，設定のミスを発見するフェーズを持つことが推奨される．

ファイアウォールとの併用で，外部からの（設定変更やログ閲覧などの）管理プロトコルを通過させるか否かを正当に設定する必要がある．場合により通信路の暗号化も推奨される．

４．留意事項

特になし．

ハッキング対策

技-6 ハッキング対策を行うこと	対策レベル 必須

1．基準の趣旨

WWW ページの改竄やサーバへの不正アクセスなどハッキング行為への対策について示す。

2．対策のポイント

ハッキング行為への対策として次の２点がポイントとなる。

① 防御対象のサーバ自身の対策

② 防御対象のネットワーク全体の対策

①については、サーバ自身に対策を施しセキュリティレベルを高めることでハッキング行為から防衛する目的で行う。

②については、サーバが置かれているネットワーク全体へのセキュリティ対策でアクセス制限やハッキング行為の追跡および監視を目的で行う。

3．実施例

①の実施例について

ハッキング行為はサーバで動作するサービスやＯＳのセキュリティホールを狙って行われるケースが多い。従って、以下のような対策を施す必要がある。

・サービス、ＯＳを最新バージョンにする。

・サービス、ＯＳに対する最新パッチの適用

・用途以外のサービスを立ち上げないようにする。

②の実施例について

インターネットへ公開され不特定多数からのアクセスが行われるサーバを設置する場合、F/W導入によるサーバへのアクセス制限が必要となる。ＩＰアドレス、サービスなどで制限を行い、公開サーバ以外のアクセスを防止する。またこの場合、公開セグメントをDMZ化し内部ネットワークへのアクセスを防ぐことも重要となる。

また、ハッキング行為が行われた場合に直ちに管理者に警告し、どのようなハッキング行為が行われたか追跡するためにＩＤＳ（Intrusion Detection System）を導入する必要がある。

4．留意事項

最近のハッキング行為は正当なＷｅｂアクセスを装ったり、アドレスを詐称するなど手口が高度化しており、F/W導入だけではハッキング対策に不十分な場合が多い。ＩＤＳの導入やサーバ自身の対策を行うなどして、より強固なセキュリティ対策を実施する必要がある。また、対策にあたっては通産省のコンピュータ不正アクセス対策基準に遵守する必要がある。

暗号鍵の変更

技-7 暗号鍵の変更が適切に行われる機能を有すること（鍵交換を行うこと）	対策レベル 強く推奨

１．基準の趣旨

現在の暗号通信においては、強力な暗号アルゴリズムを使用していても莫大な計算能力を提供できればいつかは暗号が解読できてしまうものであるため、暗号鍵が見破られる可能性はゼロとは言い切れないが、暗号鍵を定期的に変更していれば、万が一ある時点での暗号鍵が見破られてしまった場合でも、他の鍵で暗号化された情報は解読されないので安全といえる。従って、運用上の何らかの問題で暗号鍵が漏洩してしまった場合の対策のためにも、暗号鍵の変更が適切に行なわれることを推奨する。

２．対策のポイント

ＶＰＮ機能として IPsec を使用している場合を考える。

IPsec の場合、自動鍵交換プロトコル（ＩＫＥ）が規定されており、現在では多くの IPsec 装置がＩＫＥをサポートしているので、これを使用する。暗号鍵の有効期間（ライフタイム）を決定し、IPsec 装置に設定しておくことにより、鍵のライフタイムに従って自動的に相手装置と鍵交換を行なって鍵が変更される。IKE では、鍵交換メッセージ用に、実際のデータ通信を暗号化する鍵とは別の鍵を使用するので、鍵交換用の鍵もライフタイムを決めて定期的に変更されるようにする。

ライフタイムは、短くする程一つの暗号鍵で暗号化するデータ量が少なくなるため見破られた際のリスクは低くなるが、逆に自動鍵交換を行なう頻度が多くなるため IPsec 装置への負荷が
大きくなってしまい、データ通信の性能に影響する。従って、ライフタイムはむやみに短くしたりせず、暗号通信する情報の価値や使用する暗号アルゴリズムのほか、実際に通常の運用に与える影響等を考慮して決定する。検証試験を行なってみることも有効である。

もしも、装置が対応していない等の理由で自動鍵交換を行なわない場合は、手動で定期的に暗号鍵の設定変更を行なう。

３．実施例

IKE では以下のフェーズが存在し、異なる暗号鍵を生成する。

Phase 1 --- 鍵交換プロトコル（ＩＫＥ）メッセージ用の暗号鍵

Phase 2 --- 実際のデータ通信用の暗号鍵

多くの IPsec 装置では各々のライフタイムを設定でき、また相手 IPsec 装置毎に異なる値を設定することも可能である。自動鍵交換の際に、設定された値に従ってネゴシエーションを行ない、生成された鍵のライフタイムが決定するが、お互いで異なる値を設定している場合に実際にどちらのライフタイムが使用されるかは装置の仕様に依存してしまうので、お互いで設定値を合わせておくのが望ましい。

動作確認機能

技-8 VPN 機器の動作状況の監視機能を有すること	対策レベル 推奨

1．基準の趣旨

VPN 機器の動作状況等を遠隔監視し、機器の異常、障害等を検知し被害の拡大を防止する機能を備えること。

2．対策のポイント

（1） SNMP や CMIP などのプロトコルが実装してあり、遠隔監視のできる VPN 機器を導入する。

（2） SNMP マネージャなどを導入し、VPN 機器の監視を行う。

3．実施例

（1） SNMP を実装した VPN 機器の遠隔監視構成例

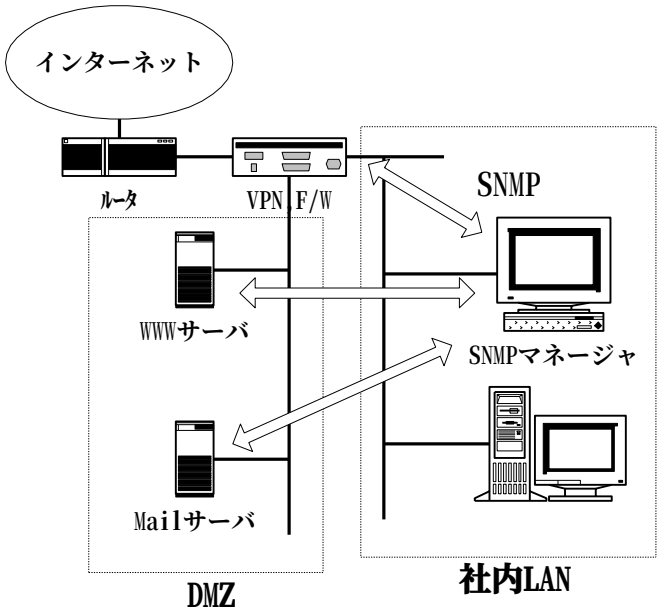


図１　システム構成例

（2）　監視項目例

- VPN 機器（OS、AP）が動作しているか
- 負荷がどの程度生じているか
- トラフィック状態は正常であるか
- VPN 機器の温度は適切であるか

4．留意事項

（1）　遠隔監視は２４時間行うことが望ましい。

装置の２重化

技-9 装置を 2 重化する機能を有すること	対策レベル 推奨

１．基準の趣旨

通常のサービスにおいては一定間隔ごとに，深夜などのサービス利用者が少ない時間帯に保守のためにサービスを停止することがあるが，VPN **サービスにおいてはサービス停止を防止する可用性**（Availability）**を確保することが必要である．可用性は**[1] **において，機密性**（Confidentiality）**・完全性**（Integrity）**と並びセキュリティ保持のための重要な柱の一つである．**

２．対策のポイント

可用性を高める方法には代替機器を置き，装置を２重化しておく手法が一般的である．機器の故障などの要因で通常時には利用される機器から自動的に代替機器に置き換わる方式と，手動で移行する方式の２つが考えられるが，いずれもサービス停止の事態が起こったことを監視する体制との連携が重要である．特に災害時の復旧においては，運用規定において代替機器の準備は必須事項である．

３．実施例

機器の２重化だけでなく，運用時における設定情報のバックアップを取っておくことでスムーズな機器移行を行うことができる．

４．留意事項

[1] OECD「**情報セキュリティのためのガイドライン**」

3.3 運用対策要件の解説

運用管理

運-1 VPN の運用管理体制を明確にすること	対策レベル 必須

１．基準の趣旨

ＶＰＮ機器を導入してシステムを構築し、実際にＶＰＮを運用していくにあたっては、ＶＰＮ機器を盗難されてしまったり、誤った設定／操作をしてしまう等、障害や故意または過失による脅威を未然に防止し、また、何らかの脅威が発生してしまった場合の損害を最小にしてシステムが迅速に回復されるようにするために、ＶＰＮの運用に関する規程を整備し、運用管理体制を明確にする。

２．対策のポイント

ここでは、リスク分析の結果に従って対策のポイントを挙げる。

- **セキュリティ運用組織を整備し、各管理者や運用担当者を定め、それぞれの責任と権限／役割を明確にする。ＶＰＮ機器の破壊や盗難に対しては管理された場所に設置するとともに、そこに入室可能な者を特定し、責任者が入退室の管理を行なう。また、管理者や担当者は常に知識の習得と技術向上を図る必要があり、人材の育成／教育についても明確にする。**
- **ＶＰＮの運用方針に基づいてＶＰＮ機器の操作／設定方法を整備、策定し、操作ミスや設定ミスによる脅威を未然に防ぐ。**
- **機密データに関しては、重要度に応じて保有、利用、配布、消去等の管理規程を整備する。ＶＰＮ機器のパスワードもこれに属し、厳重に管理して盗まれないようにする。また、類推されないようなパスワードにするため、生成の際の規定を整備する。**

その他、障害や漏洩等脅威が発生した場合の対応法を整備してマニュアル化しておき、速やかに通常運用に復旧できるようにする。また、環境の変化や技術の進歩による新たな脅威に対応していくために、継続的に監査を行なって整備を判定し、管理体制の見直しを図ることも重要である。

３．実施例

規定項目の詳細については、「情報システム安全対策」参照。

４．留意事項

セキュリティ対策を重視するあまり複雑で厳しい規定を作成してしまうと、実際には守られなかったり、業務が非効率になる可能性がある。実現性の高い現実的な体制を整え、利用者全体に浸透させることも重要である。

ログ分析・保管

運-2	対策レベル
VPN の追跡・監視情報（ログ）を定期的に保管、分析すること	必須

１．基準の趣旨

VPN 機器は動作に異常が発生した場合、あるいは外部からの不正なアクセスが検知された場合、原因等を記述したログをファイル、または外部のログ収集装置に記録する。管理者は定期的にログを監視することで、システムダウンや不正アクセスを未然に防止することが必要であり、実際に不正アクセスによる被害が発生した場合には、実行者の特定、手法の解析、被害状況の把握等のためにログは不可欠なものとなる。また分析にあたっては過去にわたってログを参照する必要も多々あるため、適切なログの保管が必要である。

2.　対策のポイント

(1)　ログファイルの出力場所

多くのネットワーク機器およびワークステーションは、ログ出力方法として SYSLOG プロトコルを利用する。SYSLOG では各機器ごとの設定によりログ出力先をローカルファイル、あるいはネットワーク上の他機器上の任意ファイル等にするなどの選択が可能である。ログ出力先の決定は、想定されるログファイルのサイズ、ログ生成に伴うトラフィック量等を勘案して行うべきである。また不正アクセスに対しては、機器への侵入者の多くが、侵入の検知を困難にするためにログ記録内容の操作を行うことを考慮にいれ、ログ発生元とログ記録先を物理的に異なる機器に分割するといった対策も必要である。

(2)　**ログファイルの管理**

ログは過去に記録されたものに対しての追記で記録されるため、ログファイルの容量は常に増加する。したがってログ分析を現実的なコストで行うためにはログファイル容量を適切な大きさに保つ必要がある。また機器に異常が生じた場合、不正アクセスを受けた場合は、兆候としてログファイルの容量が短時間に急激に増加することが多いため、管理者は常にファイル容量に注意を払う必要がある。

(3)　**重要イベント発生時の管理者への通知**

記録内容に定常状態以外で発生するイベントが記録された場合、速やかにシステム管理者に認識される必要がある。このため必要に応じてログ出力中に特定の文字列等が出現した場合に、管理者に対して電子メールやポケットベルによる警報を送信するしくみ等を併用するなどの考慮が必要である。

３．実施例

市販のネットワーク管理ミドルウェアでは、ログの収集機能、およびログ内容の監視機能を備えている。このようなソフトウェアを利用することで、例えば複数の VPN 機器から発生したログを、単一のログ管理サーバ（ネットワーク管理ソフトを搭載したワークステーション等）で集中管理しつつ、ログファイル中に異常をあらわす文字列が現れた場合、管理者が携帯するポケットベルへメッセージを送信するといったことが可能である。

４．留意事項

特になし。

バックアップ

運-3 VPN のソフトウェアをバックアップすること	対策レベル 必須

１．基準の趣旨

VPN は VPN 機器と VPN ソフトウェアで構成される。VPN ソフトウェアは、既定の設定のまま使用されることは少なく、運用に合わせて最適な効率が出るように詳細に設定される。ソフトウェアが事故や外部からの侵入により、破壊または停止された場合、VPN ソフトウェアを以前の状態に速やかに復旧するのに、ソフトウェアのバックアップは必要である。また、事故や外部の侵入の原因調査においても状況把握や分析をする上で有用である。

２．対策のポイント

（１）構成ソフトウェアの設定の保存

設定状態をどのように保存するかがポイントとなる。設定方法は各ソフトウェアによって、テキストファイルを編集するものから、GUI の操作のみで行えるものまで様々である。被害を受けた時に、VPN ソフトウェアの状態を再現することができるように、設定方法に合わせて設定状態を保存する必要がある。設定方法が容易であっても、設定のバックアップが容易であるとは限らない点に注意する。

３．実施例

設定を再現できる設定ファイルが存在する場合は、その設定ファイルのコピーをバックアップとして保存する。設定ファイルが存在しない場合は、設定画面のハードコピーを保存するなど、設定の再現に必要な情報をバックアップしておくこと。

４．留意事項

ウイルス対策

運-4 ウイルス対策ソフトによりウイルスの発見、駆除を行うこと	対策レベル 必須

内容.　（汎用 OS 利用の機器の場合）推奨

１．基準の趣旨

本基準は、システムの正常な動きを維持するために、コンピュータウイルス（コンピュータの記憶媒体やネットワークを通じて、プログラムなどに侵入し、ファイル破壊などの被害をもたらす繁殖型のプログラムのこと）の感染を防止するワクチンソフトの導入を推奨する。

２．対策のポイント

コンピュータウイルスを発見、駆除するには、抗ウイルスソフト（以下、ワクチンソフト）の導入し外部より入手したファイル及び媒体は必ず検査する必要がある。ワクチンソフトを導入するためのポイントを挙げる。

- ワクチンソフトで使用するウィルスパターンファイルは定期的に更新し､最新のものを利用することが重要である。
- 複数のワクチンソフトを利用すると効果が高い。
- 出所が不明なプログラムは導入しない。
- ダウンロードしたファイルは必ずウィルスチェックを行う。
- オリジナルプログラムにはライトプログラムをかける。

コンピュータウイルス対策の中では感染の防止が一番大事なことである。
ユーザには最低限次のことを遵守するように教育を行う。

【感染防止七箇条】

① 最新のワクチンソフトを使いウイルス検査を行う。
② 万一のウイルス被害に備えるため、データのバックアップを行う。
③ ウイルスの兆候を見逃さないようにし、ウイルス感染の可能性が考えられる場合は、ウイルス検査を行う。
④ メールの添付ファイルはウイルス検査後開く。
⑤ ウイルスが感染している可能性のあるファイルを扱う時はマクロ機能の自動実行は行わない。
⑥ 外部から持ち込まれたフロッピーディスク及びダウンロードしたファイルはウイルス検査後使用する。
⑦ コンピュータの共同利用時の管理を徹底する。

３．実施例

1. 情報処理振興事業協会（IPA）セキュリティセンター

１９９０年４月に通商産業省（※）よりコンピュータウイルス対策基準が告示され、その中で、ＩＰＡが届出を受け付ける公的な機関として指定され、届出の受付、対策の普及啓発を行っている。

４．留意事項

特になし

パッチファイル

運-5 常に最新のパッチファイルをインストールすること	対策レベル 必須

１．基準の趣旨

システム導入時に、既知のセキュリティ問題を解決していると期待できている最新版を用いることは重要である。しかし、開発時に十分に検討した製品においても、セキュリティ上の問題が内在していることが多い。そのため、OS やアプリケーションの提供元からセキュリティなどの問題点を修正するためのパッチファイルが提供される場合がある。パッチファイルが提供されるということは、問題点が公になったことであり、早急に適用し問題を取り除かなければならない。

２．対策のポイント

OS にパッチファイルを適用する際には、その OS 上で動作している全てのアプリケーション（サービス）を停止しなければならない。そのため、適用する際は事前に関係者に広く周知し、混乱のないよう手配を整える必要がある。また、適用するパッチファイルに重大な欠陥がないとも限らないため、可能であれば、バックアップやそのソフトウェアの機能により、適用前の状態に戻すことが可能な状態にしておくこと。アプリケーションに関しても同様である。

３．実施例

OS におけるパッチファイル適用例

Microsoft Windows NT のサービスパック 3 適用システムに、サービスパック 4 が提供されたため適用する。

アプリケーションにおけるパッチファイル適用例

Microsoft Internet Explorer 4.0 にサービスパックを適用し、5.0 にする。

４．留意事項

使用している OS やソフトウェアのセキュリティ機能に関する最新の情報に関し、積極的に収集する必要がある。情報収集先として、使用しているソフトウェアベンダーのほか、以下のような公的機関も有効である。

・通産省　情報処理振興事業協会（IPA）

コンピュータ不正アクセス対策、被害届についての窓口

http://www.ipa.go.jp/security/ciadr/index.html

・警察庁（情報システム安全対策研究会　ネットワーク・セキュリティ対策室）

http://www.npa.go.jp/hightech/index.htm

・JPCERT/CC（コンピュータ緊急対応センタ）

http://www.jpcert.or.jp

パスワードの変更

運-6	対策レベル
VPN 機器の定期的なパスワードの変更を行うこと	必須

１．基準の趣旨

本基準は、ＶＰＮシステムを利用する者が実施すべき運用対策において、ＶＰＮ機器のパスワードおよびユーザＩＤの管理者が守るべき事項としてまとめたものである。尚、基本的には、「コンピュータ不正アクセス対策基準」（平成８年８月８日制定　通商産業省告示第３６２号）（平成９年９月２４日改正　通商産業省告示第５３４号）に従い、その中でシステムユーザ基準においてのパスワード及びユーザＩＤ管理に該当する内容を記載している。

２．対策のポイント

システムユーザまたは管理者自身が使用するパスワード及びユーザＩＤを管理する際に実施すべき対策についてまとめたものである。

３．実施例

システムユーザまたは管理者基準の実施すべき対策で、パスワード及びユーザＩＤについての内容を以下に示す。

（１）ユーザＩＤは、複数のシステムユーザで利用しないこと。
（２）ユーザＩＤは、パスワードを必ず設定すること。
（３）複数のユーザＩＤを持っている場合は、それぞれ異なるパスワードを設定すること。
（４）悪いパスワードは、設定しないこと。
（５）パスワードは、随時変更すること。
（６）パスワードは、紙媒体等に記述しておかないこと。
（７）パスワードを入力する場合は、他人に見られないようにすること。
（８）他人のパスワードを知った場合は、速やかにシステム管理者に通知すること。
（９）ユーザＩＤを利用しなくなった場合は、速やかにシステム管理者に届け出ること。
（10）パスワードの入力を省略する機能は、システム管理者の指導の下で使用すること。
（11）ユーザＩＤは、個人単位に割り当て、パスワードを必ず設定すること。
（12）長期間利用していないユーザＩＤは、速やかに停止すること。
（13）ユーザＩＤの廃止等の届出があった場合は、速やかに登録を抹消すること。
（14）パスワードは、当該システムユーザ以外に知らせないこと。
（15）パスワードのチェックを随時行い、悪いパスワードは、速やかに変更させること。
（16）パスワードが当該システムユーザ以外に知られた場合又はその疑いのある場合は、速やかに変更させること。

４．留意事項

システムユーザ基準は、「コンピュータ不正アクセス対策基準」（通商産業省告示第３６２号、５３４号）に従うこと。

機器動作の監視

運-7	対策レベル
VPN 機器の動作状況の監視を行うこと	推奨

１．基準の趣旨

本基準は、 ＶＰＮシステムを利用する者が実施すべき運用対策において、ＶＰＮ機器の動作監視のユーザーが守るべき事項としてまとめたものである。

２．対策のポイント

外部からの異常アクセスや装置の故障といった運用上の異常の早期発見と対策をおこなうために、ＶＰＮ機器の監視についてまとめたものである。

３．実施例

ＶＰＮ機器の動作状況の監視として、管理体制の整備について以下にまとめる。

（１）システムのセキュリティ方針を確立し、周知・徹底すること。

（２）システムの管理体制、管理手順を確立し、周知・徹底すること。

（３）緊急時の連絡体制及び復旧手順を確立し、周知・徹底すること。

（４）システム管理の業務上知り得た情報の秘密を守ること。

（５）システム管理者の権限は、業務を遂行する上で必要最小限にすること。

（６）システム管理者は２人以上かつ必要最小限の管理者で、その業務は定期的に交代すること。

（７）システム管理者の資格を喪失した者の権限は、速やかに停止すること。

不正アクセス及びその予備行為を発見するための対策を以下にまとめる。

（１）ルーター又はファイアウォールにログ収集機能がある場合には、ログに不正アクセスの試みの痕跡がないか確認していること。

（２）サーバーのログに不正アクセスの痕跡がないか確認していること。

（３）システム管理者及びユーザーのパスワードが不正に更新されていないか確認していること。

（４）システムの運用に係る設定ファイルが不正に更新されていないか確認していること。（５）不正なデーモン／サービス／エージェント／アカウントが稼働されていないか確認していること。

（６）ｃｒｏｎ／ａｔ等指定した時間にプログラムを実行するコマンドによって実行される全てのファイルについて問題がないか確認していること。

（７）ｕｉｄ／ｇｉｄ等アクセス権限の設定が不正となっているファイルがないか確認していること。

（８）不正なファイルが格納されていないか確認していること。

（９）侵入検出システム（ＩＤＳ）を設置するとともに、ＩＤＳからの警告の有無とその内容を確認していること。

（10）ディレクトリやファイルの改ざんに係るチェックを行うツールを利用して設定情報の不正な変更が行われていないことを確認していること。

（11）上記の確認項目(1)～(10)のうち、実施している項目全ての確認頻度について、適切な期間を設けていること。

４．留意事項

システムユーザー基準は、「コンピュータ不正アクセス対策基準」（通商産業省告示第３６２号、５３４号）に従うこと。

クロスチェック

運-8	対策レベル
設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること	推奨

1．基準の趣旨

担当者 1 人だけで作業を実施すると、不具合を見逃す場合がある。それを未然に防止する。

2．対策のポイント

・複数の専任者を置くのが難しい場合、ごく少数の専任者の他に多数の兼任者を置くことでリソース不足をカバーするのもよい。

3．実施例

・VPN 機器の設定作業を、以下の要領で実施する。

1) 1 人の担当者が設定項目の内容を検討し、設計する。
2) 他の複数の担当者が、内容をレビューする。
3) 1 人の担当者が設定内容を VPN 機器に入力する。
4) 他の複数の担当者が、入力内容を確認する。

4．留意事項

・担当者のスキルを常に向上させるのが望ましい。

メンテナンス

運-9 VPN 機器の定期的なメンテナンスを行うこと	対策レベル 推奨

1．基準の趣旨

（目的）

・VPN 機器の故障、動作不良、誤動作の発生を未然に防止するため、定期的なメンテナンスを行うことが必要である。

・メンテナンスの対象には、VPN 機器のハードウェアと、VPN に搭載されるソフトウェアの 2 種類がある。（ソフトウェアのバージョンアップについては、2-5 参照のこと）

（対象）

・ハードウェアのメンテナンスとは、まず VPN 機器自体の診断を行い、永年劣化などによる VPN 構成機器の動作不良個所を早期に発見する。もしも不良個所が発見された場合には、機器または部品の交換および再起動を行う。

・ソフトウェアのメンテナンスは、VPN に搭載される（OS を含む）すべてのソフトウェアに関して、不要タスクの発生、動作や OS バグなどの影響による、VPN アプリケーション誤動作の排除を目的として、VPN 機器のシステムリセットおよび再起動を行う（リブートする）。

2．対策のポイント

（脅威の発生と対処）

・一時的または恒常的に機器障害、ネットワーク障害が発生する場合は、不必要なあるいは不正なタスクが生成、進入し稼動していることが考えられる。

（チェック方法と手順）

・メンテナンスは VPN 機器をいったん停止させるため、システム全体に影響をおよぼさない時間帯に行うことが望ましい。

・ハードウェアの診断は、定期的な動作ログの分析や VPN 機器に内蔵される（簡易な）自己診断プログラムの実行だけでなく、外部の診断装置を使用したより詳細な診断プログラムの実行が必要である。

・VPN アプリケーションは、VPN 機器に搭載される OS を含むすべてのソフトウェアからの誤動作、動作不良により影響を受ける可能性があるため、VPN 機器全体のソフトウェアリセット（システムリセット）を行う事が望ましい。

3．実施例

（タイムスイッチによる自動システムリセット）

・企業活動の最閑散期となる毎週日曜日の昼間、タイムスイッチにより定刻（たとえば、14 時）にいっせいに、VPN 機器の電源を OFF し、再度、タイムスイッチにより電源 ON する。

（オペレータによるいっせいリセット）

・企業活動の最閑散期となる毎週日曜日の昼間の定刻（たとえば、14 時）に、各拠点に設置された VPN 機器を、オペレータがマニュアルでいっせいにリセットする。

4．留意事項

（システム全体への影響）

・VPN 機器のリブートは、初期化完了およびネットワークシステムでの動作確認までに 30 分程度はかかるためと予想されるため、なるべくシステム全体の最閑散時間帯に実施する必要がある。

（同期したメンテナンス）

・ソフトウェアの変更があった場合には、該当ソフトウェアを搭載するすべての VPN 機器のリセットを行う必要があるため、システム全体でリブートする時間帯の事前調整が必要となる。

４．参考情報

（１）資産、脅威一覧

資産

分類	詳細
ハードウェア	ＶＰＮ機器
	回線
ソフトウェア	ＯＳ
	アプリケーション（VPN、Firewall）
サービス	VPN サービス
情報	業務情報
	VPN 機器設定情報
	鍵情報
	ログ情報

脅威

対象	脅威
ハード	破壊
	盗難
	故障
ソフト	破壊
	停止
	（不正利用）今回対象外
情報	漏洩
	改竄
	削除
サービス	サービス妨害

なお、次に示すリスク分析表内の項目である資産の存在場所において、「VPN 機器」「サーバ」は以下のように定義する。

・VPN 機器：VPN 装置、Firewall
・サーバ：内部で業務に使用しているもの（ex.ファイルサーバ）

（２）リスク分析表

NO	資産	攻撃者			存在場所	脅威評価					対策			
		管理者	内部者	第三者		脅威	脅威の発生方法	資産レベル	脅威レベル	カテゴリ分類（別紙参照）	設備対策	技術対策	運用対策	
1	VPN 機器		○		ネットワーク室	装置の破壊	物理的に装置を破壊	低	高	A	VPN 機器は入退出管理機能があるネットワーク室に設置すること（設-1）	VPN 機器の動作状況の監視機能を有すること（技-8）	VPN の運用管理体制を明確にすること（運-1）	
											―	装置を 2 重化する機能を有すること（技-9）	VPN 機器の動作状況の監視を行うこと（運-7）	
2				○			設置場所へ侵入して装置を破壊	低	低	C	VPN 機器は入退出管理機能があるネットワーク室に設置すること（設-1）	VPN 機器の動作状況の監視機能を有すること（技-8）	VPN の運用管理体制を明確にすること（運-1）	
											―	装置を 2 重化する機能を有すること（技-9）	VPN 機器の動作状況の監視を行うこと（運-7）	
3							自然災害	低	低	C	―	―	―	注 1）自然災害は考慮しない
4			○			装置の盗難	装置（の一部）を外部に持ち出す	低	中	B	VPN 機器は入退出管理機能があるネットワーク室に設置すること（設-1）	VPN 機器の動作状況の監視機能を有すること（技-8）	VPN の運用管理体制を明確にすること（運-1）	
											―	装置を 2 重化する機能を有すること（技-9）	VPN 機器の動作状況の監視を行うこと（運-7）	
5				○			設置場所へ侵入して装置を外部に持ち出す	低	低	C	VPN 機器は入退出管理機能があるネットワーク室に設置すること（設-1）	VPN 機器の動作状況の監視機能を有すること（技-8）	VPN の運用管理体制を明確にすること（運-1）	
											―	装置を 2 重化する機能を有すること（技-9）	VPN 機器の動作状況の監視を行うこと（運-7）	
6						装置の故障	装置の故障によりサービスが不可能になる	低	―	C	VPN 機器は入退出管理機能があるネットワーク室に設置すること（設-1）	VPN 機器の動作状況の監視機能を有すること（技-8）	VPN の運用管理体制を明確にすること（運-1）	
											―	装置を 2 重化する機能を有すること（技-9）	VPN 機器の動作状況の監視を行うこと（運-7）	

													VPN 機器の定期的なメンテナンスを行うこと（運-9）	
7							停電する	低	低	C	VPN 機器には UPS 装置を備えること（設-2）	―	―	
8							自然災害	低	低	C	―	―	―	注 1）自然災害は考慮しない
9	回線（通信路）		○	○	社内	通信路の破壊（切断）	物理的に通信路を切断	低	高	A	―	―	―	注２）VPN 装置に特有な問題でないため、情方システム安全対策基準解説書などを参考のこと
10							ネットワーク機器の故障	低	高	A	―	―	―	注２）VPN 装置に特有な問題でないため、情方システム安全対策基準解説書などを参考のこと
11							劣化による切断	低	中	B	―	―	―	注２）VPN 装置に特有な問題でないため、情方システム安全対策基準解説書などを参考のこと
12							自然災害	低	低	C	―	―	―	注２）VPN 装置に特有な問題でないため、情方システム安全対策基準解説書などを参考のこと
13	VPN 機器のソフトウェア(OSとアプリケーション)	○			VPN 機器	ソフトウェアの破壊	操作を誤ってシステムファイルなどを削除	低	低	C	―	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の運用管理体制を明確にすること（運-1）	
											―	―	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
											―	―	VPN のソフトウェアをバックアップすること（運-3）	
14			○				ファイル消去などの方法でソフトウェアを破壊	低	中	B	VPN 機器は入退出管理機能があるネットワーク室に設置すること（設-1）	VPN 機器へのアクセス制御機能を有し正しく設定すること（技-1）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
											―	追跡・監査機能を設けること（ログの収集）（技-2）	VPN のソフトウェアをバックアップすること（運-3）	
15				○			ウイルスなどによるソフトウェアの破壊	低	中	B	―	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
											―	ハッキング対策を行うこと（技-6）	VPN のソフトウェアをバックアップすること（運-3）	

												—	—	ウイルス対策ソフトによりウイルスの発見、駆除を行うこと（運-4）	
												—	—	常に最新のパッチファイルをインストールすること（運-5）	
16		○				ソフトウェアの停止	操作の誤りによるソフトウェアの停止	低	低	C	—	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の運用管理体制を明確にすること（運-1）	
												—	—	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
												—	—	VPN のソフトウェアをバックアップすること（運-3）	
17			○	○			ソフトウェアのセキュリティホールを突いた攻撃によるソフトウェアの停止	低	中	B	—	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
											—	ハッキング対策を行うこと（技-6）	VPN のソフトウェアをバックアップすること（運-3）	
											—	—	常に最新のパッチファイルをインストールすること（運-5）	
18							OS のバグによる停止	低	—	—	—	—	VPN のソフトウェアをバックアップすること（運-3）	
											—	—	常に最新のパッチファイルをインストールすること（運-5）	
											—	—	VPN 機器の定期的なメンテナンスを行うこと（運-9）	
19			○	○			停電する	低	低	C	VPN 機器には UPS 装置を備えること（設-2）	—	—	
20	VPN サービス			○		サービスの妨害	外部からの攻撃（DoS 攻撃など）によるサービスの妨害	低	中	B	—	—	—	注３）対処法無し
21	業務情報		○	○	インターネット上	漏洩	VPN 設定ミスにより暗号化されておらず漏洩	高	低	A	—	VPN 機器の出荷時の設定を正しく設定しなおすこと（技-5）	設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること（運-8）	

22				○			データを盗聴し解読され、漏洩する	高	低	A	－	信頼できる暗号アルゴリズム、鍵長を利用すること（技-4）	設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること（運-8）	
											－	暗号鍵の変更が適切に行われる機能を有すること（鍵交換を行うこと）（技-7）	－	
23			○	○			停電し、暗号化が行われない	高	低	A	VPN 機器には UPS 装置を備えること（設-2）	－	－	注４）起こり得るか不明
24						改竄	データを盗聴しデータ中身を改竄される。		低		－	信頼できる暗号アルゴリズム、鍵長を利用すること（技-4）	設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること（運-8）	
			○	○							－	暗号鍵の変更が適切に行われる機能を有すること（鍵交換を行うこと）（技-7）	－	
25			○	○	VPN 機器	漏洩	出荷時設定のセキュリティレベルが低く、VPN 機器に侵入され情報が漏洩	高	高	A	－	VPN 機器へのアクセス制御機能を有し正しく設定すること（技-1）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
											－	追跡・監査機能を設けること（ログの収集）（技-2）	VPN 機器の定期的なパスワードの変更を行うこと（運-6）	
											－	設定項目（ルール）を正しく設定し試験を行うこと（技-3）	設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること（運-8）	
											－	VPN 機器の出荷時の設定を正しく設定しなおすこと（技-5）	－	
											－	ハッキング対策を行うこと（技-6）	－	
26			○	○			VPN 機器のパスワードが盗まれ、ユーザになりすまし、データが漏洩	高	低	A	－	VPN 機器へのアクセス制御機能を有し正しく設定すること（技-1）	VPN の運用管理体制を明確にすること（運-1）	
											－	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	

												―	ハッキング対策を行うこと（技-6）	VPN 機器の定期的なパスワードの変更を行うこと（運-6）	
27		○					管理者の操作ミス等によりセキュリティーレベルが低く設定され、データが漏洩	高	低	A	―	VPN 機器へのアクセス制御機能を有し正しく設定すること（技-1）	VPN の運用管理体制を明確にすること（運-1）	
											―	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
											―	ハッキング対策を行うこと（技-6）	設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること（運-8）	
28			○	○		改竄	出荷時設定のセキュリティレベルが低く、VPN 機器に侵入され情報を改竄	高	高	A	―	VPN 機器へのアクセス制御機能を有し正しく設定すること（技-1）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
											―	追跡・監査機能を設けること（ログの収集）（技-2）	VPN 機器の定期的なパスワードの変更を行うこと（運-6）	
											―	設定項目（ルール）を正しく設定し試験を行うこと（技-3）	設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること（運-8）	
											―	VPN 機器の出荷時の設定を正しく設定しなおすこと（技-5）	―	
											―	ハッキング対策を行うこと（技-6）	―	
29			○	○			VPN 機器のパスワードが盗まれ、ユーザになりすまし、データを改竄	高	低	A	―	VPN 機器へのアクセス制御機能を有し正しく設定すること（技-1）	VPN の運用管理体制を明確にすること（運-1）	
											―	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
											―	VPN 機器の定期的なパスワードの変更を行うこと（技-6）	VPN 機器の定期的なパスワードの変更を行うこと（運-6）	
30		○					管理者の操作ミス等によりセキュリティレベルが低く設定され、VPN 機器に	高	低	A	―	VPN 機器へのアクセス制御機能を有し正しく設定すること（技-1）	VPN の運用管理体制を明確にすること（運-1）	

							侵入され情報を改竄					―	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
												―	ハッキング対策を行うこと（技-6）	設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること（運-8）	
31			○	○		削除	出荷時設定のセキュリティレベルが低く、VPN 機器に侵入され情報を削除	高	高	A	―	VPN 機器へのアクセス制御機能を有し正しく設定すること（技-1）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
												―	追跡・監査機能を設けること（ログの収集）（技-2）	VPN 機器の定期的なパスワードの変更を行うこと（運-6）	
												―	設定項目（ルール）を正しく設定し試験を行うこと（技-3）	設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること（運-8）	
												―	VPN 機器の出荷時の設定を正しく設定しなおすこと（技-5）	―	
												―	ハッキング対策を行うこと（技-6）	―	
32			○	○			VPN 機器のパスワードが盗まれ、ユーザになりすまし、データを削除	高	低	A	―	VPN 機器へのアクセス制御機能を有し正しく設定すること（技-1）	VPN の運用管理体制を明確にすること（運-1）	
												―	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
												―	ハッキング対策を行うこと（技-6）	VPN 機器の定期的なパスワードの変更を行うこと（運-6）	
33		○					管理者の操作ミス等によりセキュリティレベルが低く設定され、VPN 機器に侵入され情報を削除	高	低	A	―	VPN 機器へのアクセス制御機能を有し正しく設定すること（技-1）	VPN の運用管理体制を明確にすること（運-1）	
												―	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
												―	ハッキング対策を行うこと（技-6）	設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること（運-8）	

34				○	サーバ	漏洩	パスワードの類推や解読により、権限者になりすまして侵入	高	中	A	－	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
											－	－	VPN 機器の定期的なパスワードの変更を行うこと（運-6）	
											－	－	設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること（運-8）	
35				○			サーバOSのセキュリティホールをついて侵入	高	中	A	－	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
											－	ハッキング対策を行うこと（技-6）	常に最新のパッチファイルをインストールすること（運-5）	
											－	－	設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること（運-8）	
36				○			VPN・FWのセキュリティホールをつき、かつパスワードの類推や解読により、権限者になりすまして侵入	高	中	A	－	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
											－	ハッキング対策を行うこと（技-6）	常に最新のパッチファイルをインストールすること（運-5）	
											－	－	VPN 機器の定期的なパスワードの変更を行うこと（運-6）	
											－	－	設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること（運-8）	
37				○			VPN・FWのセキュリティホールをつき、かつサーバOSのセキュリティホールをついて侵入	高	中	A	－	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
											－	ハッキング対策を行うこと（技-6）	常に最新のパッチファイルをインストールすること（運-5）	
											－	－	設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること（運-8）	

38				○		改竄	パスワードの類推や解読により、権限者になりすまして侵入	高	中	A	－	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
											－	－	VPN 機器の定期的なパスワードの変更を行うこと（運-6）	
											－	－	設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること（運-8）	
39				○			サーバOSのセキュリティホールをついて侵入	高	中	A	－	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
											－	ハッキング対策を行うこと（技-6）	常に最新のパッチファイルをインストールすること（運-5）	
											－	－	設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること（運-8）	
40				○			VPN・FWのセキュリティホールをつき、かつパスワードの類推や解読により、権限者になりすまして侵入	高	中	A	－	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
											－	ハッキング対策を行うこと（技-6）	常に最新のパッチファイルをインストールすること（運-5）	
											－	－	VPN 機器の定期的なパスワードの変更を行うこと（運-6）	
											－	－	設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること（運-8）	
41				○			VPN・FWのセキュリティホールをつき、かつサーバOSのセキュリティホールをついて侵入	高	中	A	－	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
											－	ハッキング対策を行うこと（技-6）	常に最新のパッチファイルをインストールすること（運-5）	
											－	－	設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること（運-8）	

42				○		削除	パスワードの類推や解読により、権限者になりすまして侵入	高	中	A	－	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
											－	－	VPN 機器の定期的なパスワードの変更を行うこと（運-6）	
											－	－	設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること（運-8）	
43				○			サーバOSのセキュリティホールをついて侵入	高	中	A	－	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
											－	ハッキング対策を行うこと（技-6）	常に最新のパッチファイルをインストールすること（運-5）	
											－	－	設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること（運-8）	
44				○			VPN・FWのセキュリティホールをつき、かつパスワードの類推や解読により、権限者になりすまして侵入	高	中	A	－	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
											－	ハッキング対策を行うこと（技-6）	常に最新のパッチファイルをインストールすること（運-5）	
											－	－	VPN 機器の定期的なパスワードの変更を行うこと（運-6）	
											－	－	設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること（運-8）	
45				○			VPN・FWのセキュリティホールをつき、かつサーバOSのセキュリティホールをついて侵入	高	中	A	－	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
											－	ハッキング対策を行うこと（技-6）	常に最新のパッチファイルをインストールすること（運-5）	
											－	－	設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること（運-8）	

46	設定情報		○	○	VPN 機器	漏洩	VPN 機器のパスワード設定を誤り、不正にアクセスされる	中	低	B	－	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の運用管理体制を明確にすること（運-1）	
											－	－	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
											－	－	VPN 機器の定期的なパスワードの変更を行うこと（運-6）	
											－	－	設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること（運-8）	
47			○	○			VPN 機器の設定ミスにより第三者に権限が与えられている	中	低	B	－	VPN機器へのアクセス制御機能を有し正しく設定すること（技-1）	VPN の運用管理体制を明確にすること（運-1）	
											－	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
											－	－	設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること（運-8）	
48			○	○			パスワードが類推され不正にアクセスされる	中	低	B	－	VPN機器へのアクセス制御機能を有し正しく設定すること（技-1）	VPN の運用管理体制を明確にすること（運-1）	
											－	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
											－	－	VPN 機器の定期的なパスワードの変更を行うこと（運-6）	
											－	－	設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること（運-8）	
49			○				ハードディスクが不正に持ち出される	中	中	B	機能があるネットワーク室に設置すること（設-1）	－		
50			○	○			コンピュータウイルスによる、不正プログラムの実行	中	中	B	－	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	

												―	ハッキング対策を行うこと（技-6）	ウイルス対策ソフトによりウイルスの発見、駆除を行うこと（運-4）	
												―	―	常に最新のパッチファイルをインストールすること（運-5）	
51			○	○			VPN 機器のセキュリティホールを突き、管理者権限を奪われる	中	中	B	―	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
												―	ハッキング対策を行うこと（技-6）	常に最新のパッチファイルをインストールすること（運-5）	
			○	○			パスワードファイルを盗まれ、パスワードが解読され、ユーザになりすまされる	中	低	B	―	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
												―	ハッキング対策を行うこと（技-6）	常に最新のパッチファイルをインストールすること（運-5）	
52			○	○		改竄	VPN 機器のパスワード設定を誤り、不正にアクセスされる	中	低	B	―	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の運用管理体制を明確にすること（運-1）	
												―	―	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
												―	―	VPN 機器の定期的なパスワードの変更を行うこと（運-6）	
												―	―	設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること（運-8）	
53			○	○			VPN 機器の設定ミスにより第三者に権限が与えられている	中	低	B	―	VPN機器へのアクセス制御機能を有し正しく設定すること（技-1）	VPN の運用管理体制を明確にすること（運-1）	
												―	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
												―	―	設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること（運-8）	

54			○	○			パスワードが類推され不正にアクセスされる	中	低	B	－	VPN機器へのアクセス制御機能を有し正しく設定すること（技-1）	VPN の運用管理体制を明確にすること（運-1）	
											－	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
											－	－	VPN 機器の定期的なパスワードの変更を行うこと（運-6）	
											－	－	設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること（運-8）	
55			○	○			コンピュータウイルスによる、不正プログラムの実行	中	中	B	－	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
											－	ハッキング対策を行うこと（技-6）	ウイルス対策ソフトによりウイルスの発見、駆除を行うこと（運-4）	
											－	－	常に最新のパッチファイルをインストールすること（運-5）	
56			○	○			VPN 機器のセキュリティホールを突き、管理者権限を奪われる	中	中	B	－	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
											－	ハッキング対策を行うこと（技-6）	常に最新のパッチファイルをインストールすること（運-5）	
57			○	○			パスワードを解読され、ユーザになりすます	中	低	B	－	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
											－	ハッキング対策を行うこと（技-6）	常に最新のパッチファイルをインストールすること（運-5）	
58		○				削除	VPN 機器のパスワード設定を誤り、不正にアクセスされる	中	低	B	－	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の運用管理体制を明確にすること（運-1）	
											－	－	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	

												—	—	VPN 機器の定期的なパスワードの変更を行うこと（運-6）	
												—	—	設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること（運-8）	
59			○	○			VPN 機器の設定ミスにより第三者に権限が与えられている	中	低	B	—	VPN機器へのアクセス制御機能を有し正しく設定すること（技-1）	VPN の運用管理体制を明確にすること（運-1）	
												—	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
												—	—	設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること（運-8）	
60			○	○			パスワードが類推され不正にアクセスされる	中	低	B	—	VPN機器へのアクセス制御機能を有し正しく設定すること（技-1）	VPN の運用管理体制を明確にすること（運-1）	
												—	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
												—	—	VPN 機器の定期的なパスワードの変更を行うこと（運-6）	
												—	—	設定の見直し（初期設定時も含む）、ログの分析等は複数でチェックすること（運-8）	
61			○				ハードディスクの不正持ち出し	中	中	B	機能があるネットワーク室に設置すること（設-1）	—		
62			○	○			コンピュータウイルスによる、不正プログラムの実行	中	中	B	—	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
												—	ハッキング対策を行うこと（技-6）	ウイルス対策ソフトによりウイルスの発見、駆除を行うこと（運-4）	
												—	—	常に最新のパッチファイルをインストールすること（運-5）	

63			○	○			VPN 機器のセキュリティホールを突き、管理者権限を奪われる	中	中	B	―	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
											―	ハッキング対策を行うこと（技-6）	常に最新のパッチファイルをインストールすること（運-5）	
64			○	○			パスワードを解読され、ユーザになりすます	中	低	B	―	追跡・監査機能を設けること（ログの収集）（技-2）	VPN の追跡・監視情報（ログ）を定期的に保管、分析すること（運-2）	
											―	ハッキング対策を行うこと（技-6）	常に最新のパッチファイルをインストールすること（運-5）	