参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	有効なセキュリティポリシーや手順を作成するには、サイトで多くの意思決定をし、承認を得て、こうしたポリシーについて意見交換 し、実施する必要があります。				
	それぞれの資産についての基本的なセキュリティの目標は、可用性と守秘性とインテグリティです。個々の脅威は、どのようにその脅威が影響を与えうるかを目で検証する必要があります。				
	リスク 分析の手続きとして、守らねばならないすべてのものを識別することがあります。価値のある情報、知的財産権のある情報、すべてのハードウエアのようにわかりやすいものもあります。しかし、システムユーザ自身のように見落とされているものもあります。セキュリティ 問題によって影響を受けうるすべてのものを列記することが重要です。				
	防護すべき資産を識別できたら、次にそれらの資産に対する脅威を識別することが必要です。				
	「セキュリティ ポリシー」と呼ばれる一式のセキュリティのルールについて、あなたの目標は、すべてのユーザ、運用スタッフおよび管理者との間で意見交換される必要があります。				
	セキュリティポリシーの主目的は、ユーザ、スタッフおよび管理者に、技術と情報資産を守るために求められる義務を伝達することです。ポリシーは、このような義務に合うように、その役割を定める必要があります。				
	AUP（ Appropriate Use Policy：適切な使用法のポリシー）も、セキュリティポリシーの一部といえます。これには、ユーザが様々なシステムのコンポーネント上で何をしてよいのか、何をしてはいけないのかが記述される必要があり、これには、そのネットワーク上で許可される通信のタイプが含まれます。AUP は、あいまいさや誤解を防ぐために、可能なかぎり明快である必要があります。				
	セキュリティポリシーを適切で有効なものとするためには、その組織内のすべての階層の従業員の受容と支持が必要です。次にセキュリティポリシーの文書の作成とレビューに参画すべき人々のリストを示します。: (1) サイトのセキュリティの管理者 (2) 情報技術のテクニカルスタッフ（例: コンピュータセンター派遣のスタッフ） (3) その組織内の大きなユーザ グループの管理者（例: 事業部、大学内のコンピュータサイエンス学科等） (4) セキュリティ IRT （Incident Response Team） (5) セキュリティポリシーによって影響を受ける各ユーザグループの代表者 (6) 経営管理者 (7) 法律顧問（それが適当である場合）				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	上記のリストは、多くの組織における典型例ですが、必ずしもこのままである必要はありません。以下のような案も考えられます。 ＊ 重要な株主の代表者 ＊ 予算編成権をもってポリシーに詳しい経営管理者 ＊ 何ができて何ができないかを知っているテクニカルスタッフ ＊ 様々なポリシーの法的な選択肢を知っている法律顧問 組織体によっては、EDP 監査の原則を含めるのが適切であることもあるでしょう。ポリシーの表明が、広く受容されるようになるのであれば、このグループに参画することは重要であるといえます。法律顧問の役割は、国ごとに異なることも述べておきます。				
	よいセキュリティポリシーの特徴を下記に掲げます。: (1) システム管理の実務や実効性のある使用にあたってのガイドラインの発表、もしくは、他の手法において具体化することができるものである必要があります。 (2) セキュリティツールによって、適切に補強することができる必要があり、実質的に技術的な防御ができないときは、認可によって補強する必要があります。 (3) ユーザ、管理者および経営管理者の責任の範囲を明確に定義する必要があります。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	よいセキュリティ ポリシーのコンポーネントは、下記のものから構成されます。: (1) コンピュータ テクノロジー調達ガイドライン これは、要求される、あるいは、よりふさわしいセキュリティの機能の条件を明らかにするものです。これらは 、既存の購買ポリシーとガイドラインを補完するものである必要があります。 (2) プライバシーポリシー これは、下記のような論点についてのプライバシーのあり方を定義するものです。 ＊電子メールのモニタリング（監視） ＊キー ストロークのロギング（履歴） ＊ユーザのファイルへのアクセスのロギング（履歴） (3) アクセスポリシー これは、資産の消失や開示から守るために、ユーザ、運用スタッフおよび経営管理者のための許される使用法についてのガイドラインを作ることによって 、アクセス権限と特権を定義するものです。これは、下記の項目のガイドラインとなっていなければなりません。 ＊外部接続 ＊データ コミュニケーション ＊ネットワークに接続するデバイス ＊システムへの新しいソフトウエアの追加搭載 これは、また、すべての要求される通知メッセージについて記述される必要があります。（例: 接続時のメッセージは、承認された使用法とラインモニタリングについての警告をするものである必要があり、単に"Welcome"といったものであってはなりません。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	(4) 説明責任ポリシー これは、ユーザ、運用スタッフおよび経営管理者の責任を定義するものです。これは、監査する主体を特定するとともに、インシデントに対応するガイドラインを提供するものである必要があります。(つまり、何かそのようなことが検出されたときにはどうしたらよいかということです。) (5) 認証ポリシー これは、信頼を築くもので、有効なパスワードポリシーとリモートからの認証と認証デバイスの使用ガイドラインを設けることによってなされます。(例: ワンタイムパスワードと、それを生成するデバイス) (6) 可用性表明 これは、ユーザに資源の可用性についての計画を示すものです。これは、運用時間と保守のためのダウンしている期間を明らかにするとともに、代理機能と復旧の論点にも言及している必要があります。それには、システムとネットワークの障害を報告する連絡先情報も含まれている必要があります。 (7) 情報システムとネットワークの保守ポリシー これは、テクノロジーをどのように扱ったり、アクセスすることが、内部・外部 の両方のメンテナンス(保守)担当者に認められているか、を記述するものです。ここで示されなければならない重要な論点は、「リモート メンテナンスがみとめられているか」ということと、「そのようなアクセスが、どのようにコントロールされるか」ということです。他にに、ここで検討すべき領域は、アウトソーシングと、いかにそれが管理されるかということです。				
	(8) 違反の報告のポリシー これは、 ＊どのようなタイプの違反が報告されなければならないか (例: プライバシーとセキュリティ、内部と外部) ということと、 ＊誰に報告されなければならないか を示すものです。脅かすのではない雰囲気で、匿名での報告を許可することによって、発見された際には、より多くの報告が寄せられるようになるでしょう。 (9) サポート情報 これは、ユーザ、スタッフおよび経営管理者に、それらのタイプのポリシー違反の連絡先情報を知らせるものです。; また、外部へのセキュリティのインシデントについての質問についての扱い方や、機密情報や知的財産権のある情報についてのガイドラインも示します。; さらに、セキュリティの手順や企業(独自)のポリシーや国の法律や規制等の関連情報の参照を示します。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	あなたのセキュリティポリシーに影響を与える制限事項もあります。(例: ラインモニタリング) セキュリティポリシーの作成者は、そのポリシーの作成においては、法的な助言を求めることも考慮すべきです。少なくとも、そのポリシーは、法律顧問によってレビューされる必要があります。				
	あなたのセキュリティポリシーが完成したら、それについて、ユーザ、スタッフおよび管理者との間で意見交換される必要があります。すべての関係者から表明文書にサイン(署名)をもらうことは、それを読み、理解し、そのポリシーに同意するということであり、一連の過程の中でも重要なところです。最後に、あなたのポリシーは、あなたのセキュリティについてのニーズをうまくサポートしているかを確認するために、通常の条件でレビューされる必要があります。				
	セキュリティポリシーが、長期間にわたって柔軟性を持ち続けるようにするためには、骨格をなすセキュリティコンセプトに基づいて、十分に柔軟である必要があります。セキュリティポリシーは、(大部分は)詳細なハードウエアやソフトウエアの環境 からは切り離されているべきです。(それは、特定のシステムとなると、すぐに更新されたり変更されたりするからです。)このポリシーを更新する方式は、明確に文書化される必要があります。これには、手順、参画する人およびその変更について署名すべき人が含まれます。				
	また、すべてのルールには例外があることを認識しておくことも重要です。可能である限り、ポリシーにはどのような一般原則の例外があるのかまで記載される必要があります。				
	すべてのサイトは、わかりやすいセキュリティ計画を立てる必要があります。ここにおける計画は、第 2 節において検討する各論を扱うポリシーより高い位置づけのものである必要があり、各論を扱うポリシーが、その体系の中で整合性をもつ広範なガイドラインのフレームワークとして計画される必要があります。				
	セキュリティ計画において、以下の事項が定められる必要があります。: 提供を受けるネットワークサービスの一覧、その組織体のどの部分がそのサービスを提供するか否か、誰がそうしたサービスにアクセスできるようにするのか、どのようにアクセスできるようにするのか、および誰がそうしたサービスを管理するのか等 。				
	計画には、どのようにインシデントに対応すべきか、ということも盛り込まなければなりません。第 5 章において、この論点について掘り下げた検討を行いますが、個々のサイトでインシデントとその対応についての範囲(クラス)を定義することが重要です。例えば、ファイアウォールのあるサイトでは、対応を実行するまでにファイアウォールを破ろうとした試みの回数で線を引くべきかもしれません。重要性のレベルは、攻撃と対応の両方について定義される必要があります。				
	セキュリティの複雑さは、提供されるサービスの数が増えると、指数関数的に増大しうることを銘記ください。 フィルタリングルーターは、新しいプロトコルをサポートするためにはモディファイ (改造)される必要があります。				
	インフラストラクチャは、人間の過失からも保護されている必要があります。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	このような問題の大部分への対策は、現行のルーティングプロトコル（例: RIP-2、OSPF）で送信されるパケットのルーティング情報の変更を防ぐことです。				
	3 つのレベルの防衛策があります。平文パスワード、暗号技術によるチェックサムおよび暗号化。				
	要するに、そのサービス、プロトコル、サーバーは、不正アクセスや web データベースの改変を防ぐために、いかなるセキュリティが求められようとも、提供されなければならないのです。				
	内部サービスを一式のサーバーホストコンピュータに搭載し、外部サービスを別の一式のサーバーホストコンピュータに搭載するように分離するのが賢明です。				
	つまり、内部サーバーと外部サーバーは、同じホスト コンピュータにいっしょに搭載してはいけないのです。				
	そのようなファイアウォールが、正しく運用されていることを確認するようにする必要があります。				
	（例: 企業の事業部門）この文書では、外部と内部、（公的と私的。）に区別するだけですが、イントラネットを使用しているサイトは、サービスの設計や提供の際には、3つの部分について考慮し、適切な対策をとらなければならないことを、認識する必要があります。				
	それゆえ、そのサービスには、外部と内部のサービスやネットワークとは別の独自のサポートシステムが必要となります。				
	組織体は、よく知られているようにセカンダリネームサーバーとしてふるまう保護されたサイトを築き、DNS マスターを、フィルタリングルーターを使ってサービス妨害攻撃から守る必要があります。				
	それゆえ、これらのサーバーが、そのサービスには使う予定がなかったホストからはアクセス不能であることと、予定していたホストだけがそのサービスにアクセス できることをも確認する必要があります。（つまり、Telnet や FTP のような一般的なサービスは、管理者以外の者には許されない。）				
	一般的な、アクセスをそのサービスを必要とするホストに制限するルールと、そうしたホストによるアクセスをそのサービスに制限するルールが、最初の1歩として お薦めできます。				
	電子メールサーバーは、外界とのアクセスを必要とします。				
	Web サーバーが、インターネットコミュニティにつながっている場合、機密情報が、そのサーバーのホスト機にはないことが特に重要です。 実際、そのサーバーは、他の内部ホスト機によって「信頼」されていない、専用ホスト機に搭載されることが推奨されています。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	多くのサイトでは、FTP サービスと WWW サービスをいしょに搭載しようとすることでしょう。しかし、これは情報を提供するだけの匿名 ftp サーバー(ftp-get)だけにすべきです。匿名 ftp の put を WWW と組み合わせて使うのは危険です。(例 あなたのサイトが web で公開している情報が、改ざんされる可能性があります。) それぞれのサービスごとにセキュリティを検討してください。				
	しかし、FTP では認証が要求される一方、TFTPでは要求されません。よって、できるだけ TFTP は避けなければなりません。				
	FTP サーバーは、専用のホスト機に搭載される必要があります。				
	薦められません。特に、FTP サービスがファイルの送り込みを認めている場合にはお薦めできません。(上記の WWW の節をご覧ください。)				
	TFTP は、FTP ほどの機能はサポートしていませんし、セキュリティ機能をもっていません。このサービスは、内部使用だけを想定すべきであり、このときには、(システム上のすべての読み取り可能なファイルではなく、)そのサーバーが 事前に定められたファイルにだけアクセスできるように、制限的に設定すべきです。 おそらく、典型的な TFTP の使用法は、ルーター設定ファイルをルーターにダウンロードするのに使うことでしょう。 TFTP は専用ホスト機に搭載されるべきで、FTP もしくは Web の外部アクセスを サポートするホストにインストールしてはなりません。				
	それゆえ、NFS サーバーは、サービスを使用しているホストによってのみアクセス可能である必要があります。これは、どのホストに、そのファイル システムはエクスポートされているかと、どのように権限を与えるか、(例: read-only、read-write 等)を設定することによってできます。ファイルシステムは、ローカルネットワーク外部のホストには、エクスポートされてはなりません。これでは NFS サービスが外部からアクセス可能である、ということになってしまうからです。理想的には NFS サービスへの外部アクセスは、ファイアウォールによってくい止めるべきです。				
	サイト上のユーザの認証機能以外は、最低限のアクセスに限定すべきです。				
	また、他のいかなるサーバーとも共同のホスト機に搭載してはなりません。				
	さらに、サービス自身へのアクセスを含むすべてのノードへのアクセスは、セキュリティが突破されるときに備えて、「紙の証跡」が出せるように、ログを採るようにしなければなりません。				
	その難しい部分は、そのパケットが、その扉を通じたアクセスを許可ないし拒否されるかを定めるクライテリア(基準)を作ることです。				
	よりよいセキュリティのためには、通常、フィルタは、2 つのネットワークの間に 1つだけ設置れる要塞ホストと呼ばれるホスト機に置かれ、アクセスを制限します。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	正規のユーザが、このファイアウォール越しに資源を入手できるようにするためには、サービスは、要塞ホストによって転送される必要があります。				
	この設定により、外部ルーターが、IP 層でのセキュリティを突破する攻撃（ IP スプーフィング、ソースルーティング、パケットフラグメント）の試みをブロックする一方で、プロキシサーバーが上位層のプロトコルのセキュリティ ホールの可能性についてを扱えるようになります。その内部ルーターの目的は、プロキシサーバー宛て以外のすべてのトラフィックをブロックすることです。 もし、この設定が厳密に実装されていれば、高いレベルのセキュリティが達成できます。				
	ファイアウォールを購入するときには、そのファイアウォールの物理的要素の費用に加えて、このような追加的費用が考慮される必要があります。				
	結局、セキュアでないと後で気づくよりも、セキュリティを知覚できる方がよいので、気軽に挑戦すべきではありません。				
	すべてのセキュリティ手段と同様、脅威、守るべき資産の価値、セキュリティを実装するのにかかる費用に基づいて意思決定することが重要です。				
	既に述べたように、現在のネットワーク環境において、システムとネットワークのセキュリティとインテグリティ（完全性）に関心のあるサイトには、標準的で手軽なパスワードではない方法 への移行を検討することを薦めます。				
	このような技術のひとつとして、チャレンジレスポンス技術があり、これは 1回だけ使用できるパスワードを提供するものです。（通常「ワンタイムパスワード（OTP）」と呼ばれています。）				
	その製品を使用する決定は、各組織体の責任においてなされることであり、各組織体は、独自に試用 ・選択すべきです。				
	それゆえ、Kerberos クライアントとサーバーは、安全な時間の情報源をもつ必要があり、正確な時間を維持する必要があります。				
	秘密のトークン選択するときには、それらを慎重に選ぶようにして下さい。パスワードの選択と同様、それらを推測しようと企む者に対して、強いものである必要があります。つまり、それらはいかなる国語のひとつの単語であっても、いかなる業界用語、隠語などであってはいけません。理想的には、それらは、短いよりも長い方が望ましく、前部と後部に、文字とデジットと他の文字を組み合わせたパスフレーズから成るものが望まれます。				
	秘密のトークンが選択されたら、これらの保護が非常に重要です。（トークンカードのように、）ハードウエアデバイスへの PIN として使用されるものもあり、これらは、関連付けられているデバイスと同じ場所に書かれたり、置かれたりしてはなりません。他には、PGP（ Pretty Good Privacy ）の秘密鍵のようなものも、不正アクセスから保護される必要があります。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	標準的で手軽なパスワードの使用をやめる必要性については強調しすぎることはないのですが、組織体によってはそれらを使用し続けるところもあるでしょう。				
	こうした組織体は、より良い技術の使用に移行することが推奨されるのですが、暫定的に、我々は伝統的なパスワードの選択と保守を助けるのために、 次のアドバイスをします。ただし、これらの手段も盗聴プログラムによる開示に対しては有効な保護ではないことを覚えておいてください。				
	(1) 強いパスワードの重要性 - (すべてではないにしろ)システムの突破の多くの場合、侵入者は、システム上のアカウントへのアクセスを得る必要があります。 その目的を達する典型的なやり方は、正規のユーザのパスワードを推測することによるものです。これはしばしば、システムのパスワードファイルに対して非常に大きな辞書を 使用する、自動化されたパスワード解析プログラムを実行することによって行われます。パスワードがこのようなやり方であばかれるのを防ぐ唯一の方法は、慎重に、容易には推測されないパスワードを選択することです。(つまり 、字数、綴り、厳守すべき文字の組み合わせです。)パスワードはまた、システムがサポートしていて、ユーザが扱える範囲で、できるだけ長くすべきです。 (2) デフォルトパスワードの変更 - 多くのオペレーティング システムとアプリケーション プログラムは、デフォルトのアカウントとパスワードをもつようにインストールされます。これらは直ちに、推測されたりクラックされないものに変更しなければなりません。 (3) パスワードファイルへのアクセス制限 - サイトは特に、潜在的な侵入者がそれらをクラッキングのために手に入れないようにするために、ファイルの暗号化されたパスワードの部分を守ろう とすることでしょう。効果的なテクニックのひとつとして、シャドウ パスワードの利用があげられれます。これは、標準ファイルのパスワードのフィールドが、ダミーもしくは偽のパスワードをもつ、というものです。正規のパスワードを納めたファイルは、システム上の別の場所に保護せれます。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	(4) パスワードエイジング（計画的陳腐化） – いつ、どのようにパスワードを発行するかは、セキュリティコミュニティにおいて今でも論争のある論点です。アカウントが使用されなくなったら、パスワードは保持されてはならないことは一般に受け入れられていまが、ユーザが現在使用中のよいパスワードを変更することについては白熱した議論がなされています。パスワード変更の主張は、破られたアカウントの使用継続の防止との関連があります。しかし反対論は、定期的なパスワード変更によって、ユーザはパスワードを見えるところに書くようになってしまったり、（例えば端末に貼り付けること。）推測が容易な非常に単純なパスワードを選ぶようになってしまう、と主張します。侵入者は、捕捉もしくは推測されたパスワードを後ではなくすぐに使用する可能性が高いことも述べておく必要があります。この場合、パスワードエイジングは 、ほとんど保護策になりません。 このジレンマに対する決定的な回答はありませんが、パスワードポリシーは、この論点に直接的に対応し、どれ位の頻度でユーザがパスワードを変更しなければならないかについてのガイドラインを提供すべきです。確かにパスワードの定期的な変更は 、通常、大部分のユーザにとっては さほど困難ではありませんので、あなたはその導入を検討すべきです。パスワードは、少なくとも、特権アウントが変更されたとき、 個人において重要な変更がなされたとき（特に、これが管理者の場合には！） アカウントが変更されたときには変更されることが推奨されています。さらに、もし特権アカウントのパスワードが変更されたときには、システム上のすべてのパスワードが変更される必要があります。				
	(5) パスワード／アカウントのブロッキング – 事前に定義された認証の失敗の回数の後に、アカウントを使用不能にすることの有用性を見出しているサイトがあります。もし、あなたのサイトでこのメカニズムを採用するのでしたら、このメカニズムを「宣伝」しないことを薦めます。使用不能にした後に、たとえ正しいパスワードが入力されても、表示されるメッセージは、失敗したログインのときのままにしておかなければなりません。このメカニズムを実装することによって、正規のユーザが、彼らのアカウントが再度使用できるようにシステム管理者に要求するようにすることが必要になります。 (6) finger デーモンについて – デフォルトで、finger デーモンは、システムとユーザについての かなりの情報を表示します。例えば、これはすべてのユーザの現在使用中のシステムのリストや、 特定のユーザの .plan ファイルのすべての内容を表示することができます。この情報は侵入者によって、ユーザ名を特定し、彼らのパスワードを推測するのに利用される可能性があります。サイトでは、finger を、表示される情報を制限するようにすることを 検討するよう、お薦めいたします。				
	我々は、各サイトに、守秘性を確保し、価値ある情報を守るために、暗号を使用することを薦めます。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	暗号の使用は、政府とサイトの規制によってコントロールされていることがあるので、我々は管理者に、それらを採用する前に、その使用そ制限している法 もしくは政策について勉強することを強くお薦めいたします。 この目的で入手可能な様々なアルゴリズムやプログラムについて検討することは、この文書の範疇外ですが、UNIX の暗号プログラムは簡単に破られることが 分かっているので、我々は、その安易な使用に対して警告いたします。我々は、みなさんに、すべてのアルゴリズム／製品を使用する前に、その暗号の強度を理解する時間をとることも強くお薦めします。				
	あなたがインテグリティの保証のためにチェックサムをとるために使うのには、メッセージダイジェスティングプログラム MD5 [ref] のように暗号的に強いプログラムを使用することを提案します。				
	ホストへの物理的アクセスを、そのホストを使用することが想定されている人々にのみアクセスを許すように制限してください。				
	オリジナルとバックアップのデータのコピーとプログラムを安全に保管してください。それらをバックアップ目的で良い保管状態に保つこととは別に、それらは盗難から守られている必要があります。ダメージ（破壊）についての考慮ばかりでなく、盗難防止のためにも、 バックアップを、オリジナルとは別の場所に保存することが重要です。				
	（ノート PC などの）ポータブルホストには、特にリスクがあります。たとえあなたのスタッフの PC が盗難にあっても、問題が起きないようになっているかをご確認ください。PC 上でどのようにデータが保護されるべきか （例 ： 暗号化）とともに、PC のディスク上に 保存することが許されるべきこの種のデータのためのガイドラインを作成することをご検討ください。				
	ウォークアップホストは、そのユーザがあなたのネットワーク上の資源にアクセスすることを許可される前に、認証される必要があります。				
	空室のオフィスのような、監視されていないネットワークへのアクセスがあるところすべてに目を配ってください。配線室でそのような領域を切断するのが見識であり、セキュアハブの使用と、承認されていないホストを接続する試みを監視することをご検討ください。				
	正規の承認なしに、ユーザにモデム回線につなぐことを許してはいけません。これには、臨時の接続も含まれます。（例: 一晩だけモデムを FAX もしくは電話回線のプラグに挿す。）				
	すべてのあなたのモデム回線のレジスターの保守を行い、あなたのレジスターを最新に保つようにしてください。定期的に（理想的には自動的に）サイトに承認されていないモデムがないかをチェックしてください。				
	あなたのネットワーク上の何かにユーザがアクセスできる前に、ユーザ名とパスワードのチェックがなされる必要があります。通常のパスワードセキュリティの考慮事項が特に重要です。				
	この理由により、可能であればワンタイムパスワードを使用すべきです。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	すべてのユーザが同様に認証されるように、ひとつだけのダイアルインポイントを設けることが有益です。				
	ユーザは、たまにパスワードを誤って入力することがあります。初回と 2度めの失敗ログインの後に、短時間の遅れ（例えば 2秒）を設定し、3度めの後に切断するようにしてください。				
	ダイアルインサーバーには、コールバック機能を提供するものがあります。（つまり、ユーザがダイアルインして認証されると、そのシステムはそのコールを切断し、特定の番号でコールバックします。）この機能は注意して使う必要があります。				
	すべてのログインは、成功であろうと失敗であろうとログを採る必要があります。しかし、ログの中に正しいパスワードを残してはいけません。				
	各サイトは、必要な情報だけをもつように注意して、自らの専用のログインバナーを作成すべきです。				
	短いバナーを表示するようにしてください。ただし、「気をそそる」名前を表示してはいけません。				
	ダイアルアウトユーザも認証される必要があります。				
	認証されていないダイアルインコールからのダイアルアウトを許可してはいけません。				
	最低限、同一のモデムと電話の回線を、ダイアルインとダイアルアウトの両方に使用することを許してはいけません。				
	最低限、同一のモデムと電話の回線を、ダイアルインとダイアルアウトの両方に使用することを許してはいけません。				
	モデムは、使用中にはプログラム変更できないことを確認してください。最低限、3つのプラスサインがあなたのダイアルインモデムをコマンドモードにしないことをご確認ください！				
	あなたのモデムが完全にコールを切断することをチェックしてください。ユーザがアクセスサーバーからログアウトするときに、そのサーバーが電話回線を正し くハングアップさせるかを検証してください。そのサーバーが、ユーザが予期せずハングアップしたときに、どこからのセッションが活動状態にあったか、ログ アウトを監視することも同等に重要です。				
	監査データには、すべての人々、プロセス、もしくはネットワーク中の他の主体によって異なるセキュリティ レベルを達成しようとする、すべての試みが含まれる必要があります。				
	特に、公開サーバーに対する「匿名（anonymous）」もしくは「ゲスト」アクセスに注意することが重要です。				
	非常に重要な注意事項: パスワードを収集しはいけません。これは、仮に監査記録が不正にアクセスされたときには、甚大なセキュリティ問題を引き起こす可能性があります。誤ったパスワードも収集し てはいけません。その理由は、それらは正しいパスワードとたった 1文字違いということがよくあるからです。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	収集のプロセスは、ホスト、もしくはアクセスされる資源ごとに定められる必要があります。データの重要性と、例えばサービスが妨害されているときなどに身近にそれをもつ必要性に応じて、データは、それが必要とされるまでローカルに保存したり、もしくは、個々のイベントが起きた後で保存場所に転送することができます。				
	1度だけ書き込めるデバイス上に監査データを収集することは、単なるファイルの方法よりも設定に少し労力を要しますが、これには、大きくセキュリティを強化する明らかな利点があります。それは、侵入者が、侵入が起きたことを示すデータを改ざんすることができないからです。この方法の欠点は、保存メディアを用意し続ける必要性があることと、そのメディアの費用です。				
	ラインプリンターにログをとることは、永続的なログと、緊急のログが必要とされるシステムでは有用です。リアルタイムシステムは、失敗や攻撃の瞬間が記録されるこの一例です。レーザープリンターもしくは、データを貯める他のデバイス（例 ： プリントサーバー）は、バッファが重要な瞬間に必要なデータを含んでいるときには、データの消失に悩むことでしょう。「紙の記録」を書き出すことの欠点は、プリンターを維持管理する必要があることと、記録を手で検索する必要があることです。また、印刷される莫大な量の紙の保管場所の論点もあります。				
	監査データの収集は、急速にバイト数を消費することになるので、この情報の保存可能性についてはあらかじめ検討される必要があります。				
	監査データは、サイトで最も慎重に保全されるデータとして扱われて、バックアップを採る必要があります。				
	監査データは、また、調査、検知、インシデントに備えての準備の鍵となりえます。この理由で、どのように監査データが扱われるかを決定するときに、法律顧問の助言を求めることを助言します。これはインシデントが起きる前になされる必要があります。				
	監査データの内容によっては、数多くの法的な疑問があります。これは、あなたの法律顧問に対応願う必要がある問題を提起します。もし、あなたが監査データを収集、保存するならば、その存在とその内容の両方による結果に備える必要があります。				
	上記の例を、わかりやすく話し、監査データに関連した法的な論点を考慮するように、あなたの組織体を促す必要があります。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	バックアップを作成する手続きは、コンピュータシステムの運用についての古典的な領域です。本書の文脈において、バックアップは、サイトのセキュリティの全体計画の一部として扱っており、バックアップには、この文脈において重要な観点がいくつかあります。: (1)　あなたのサイトがバックアップを作成しているかを確認してください。 (2)　あなたのサイトがバックアップに、サイト以外のストレージ（保存）を使用しているかを確認してください。ストレージ（保存）サイトは、そのセキュリティとその可用性の両方の観点から慎重に選択される必要があります。 (3)　あなたのバックアップがサイト以外にあるのでしたら、さらなる情報の保護のために、それを暗号化することを検討してください。しかし、将来、いつでもデータを復元できるように、よい鍵管理スキームが必要となることを認識してください。また、将来、復号する必要があるときに必要な復号プログラムへのアクセスができることを確認してください。 (4)　あなたのバックアップは良くできているとは限りません。サイトがインシデントを認知するまでに長い時間がかかった、多くのコンピュータセキュリティのインシデントの例があります。このような場合、被害を受けたシステムのバックアップも侵されています。 (5)　定期的に、あなたのバックアップの正確性とインテグリティ（完全性）を検証してください。				
	上記のような起こりうる各イベントについては、あらかじめ適切な緊急時対応計画 (コンティンジェンシープラン）に対応を示しておく必要があります。				
	いかなる事前に計画された手続きに際しても、インシデントへの対応の目的に注意が払われる必要があります。				
	しかしすべての関連主体は、分析しないと、同様のインシデントが再発する可能性があることを認識する必要があります。				
	インシデントに際してうまく行動できるように、事前に行動の優先順位をつけておくことも重要です。				
	他の重要な関心事は、インシデントが起きたシステムやネットワーク以外の他者の被害です。政府規制の範囲内で、できるだけ早く被害を受けた主体に通知する ことは、常に重要です。この論点の法的な教訓として、これ以上の遅れや、管理者にとっての不確実性を避けるために、これは計画された手続きに含まれている必要があります。				
	セキュリティ インシデントに対応するすべての計画は、ローカルのポリシーと規制に従ったものである必要があります。				
	インシデントに対応することは、 退屈で、多くのルーティン（定型的）業務を必要とします。これらは、サポートする人材で対応することができます。 技術者を解放するためには、次のような仕事を補助するスタッフを任命すること が有用です。: コピー 、FAX 等。				
	各種の連絡先のために、特定の「連絡窓口（POC:Points of Contact）」が定められる必要があります。				
	対照的に、連絡窓口は、そのイベントへの対応に参画しているすべての主体の労力を調整する必要があります。				
	唯一の連絡窓口はまた、証拠収集の責任を負う唯一の主体である必要があります。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	インシデントへの対応のプロセスは、場合によっては規模拡大のメカニズムも提供すべきです。そのようなメカニズムを定めるために、サイトは、インシデントのための内部的な機密スキームを築く必要があります。				
	連絡窓口の変更があった場合、旧連絡窓口はすべての提供元情報の中で新しい連絡窓口を知らせる必要があります。				
	最後にユーザは、気づいたインシデントの報告のし方を知っておく必要があります。				
	サイトでは、業務時間内でも時間外でも機能する報告手続きを確立する必要が あります。				
	法的な決着をはかるようなインシデントが起きたときには、できるだけ早く 捜査機関（例 アメリカ合衆国における FBI とシークレット サービス） と連絡をとることが重要です。現地の法執行機関、現地のセキュリティ事務所、学内の警備部門にも、適切に知らさせる必要があります。この節では、直面する多くの論点を記述しますが、各組織体には、どのように法執行機関や捜査機関とやり取りをするかに影響を与えるそれぞれの（ローカルと） 政府の法や規制があることは、周知のとおりです。最も重要な点は、各サイトはこれらの論点について検討しておく必要があるということです。				
	あなたの組織体もしくはサイトに法律顧問がいれば、あなたはインシデントが進行中であることを知り次第、この事務所に知らせる必要があります。 最低限、あなたの法律顧問は、あなたのサイトもしくは組織体の法的、財務的な 利益を守るために参画する必要があります。				
	捜査活動の支援と、可用性の制限の間のバランスは、微妙です。あなたは、いかなるインシデントにおいても何をすべきかについての意思決定を するときには、あなたの法律顧問のアドバイスと、その侵入者が 引き起こしているダメージ（ある場合には）を考慮する必要があります。				
	最後に、あなたの法律顧問は、あなたのサイトのインシデントに対応するために記述された手続きを試す必要があります。あなたが実際にこれらの手続きを実行する前に、法的な見通しをもって「問題のない健康診断書」を入手することが重要です。				
	システムのハードウエアもしくはソフトウエアの欠点によってその突破が起きたと判断されたときには、そのベンダー（ないし販売代理店）や コンピュータ セキュリティ インシデントへの対応を行うチームに、できるだけ早く通知する必要があります。				
	特定の個人についての情報 は、特に慎重を要するもので、プライバシーの法規との関係があります。この領域の問題を避けるために、関係のない情報は削除されるべきであり、残る情報の扱い方の表明が含められる必要があります。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	大きなインシデントにおいて、なぜある行動がとられるのかや、どのようにユーザ（もしくは部門）がふるまうことが期待されているか についてコミュニケーションすることは決定的に重要です。 特に、（他の部門を含む）外界に何をしゃべることが許されているのか、（あるいはいけないか）をユーザに明確に示す必要があります。				
	顧客や連絡先とのコミュニケーションは、気をきかせ、かつ慎重に対応する必要があります。				
	アメリカ合衆国においては、メディアにおけるコンピュータセキュリティインシデントの占める量がすさまじく伸びてきています。 このようなプレス（報道）のし方は、今、諸外国に拡大しようとしています。それはインターネットが成長を続け、国際的に拡大しているからです。そのようなメディアの注目がまだ起きていない国の読者は、 アメリカ合衆国の経験から学ぶことができ、警戒して準備しておく必要があります。				
	広報室がない場合、プレスに発表される情報は、慎重に検討される必要があります。				
	本当にインシデントであるのか を識別するのを補助するために、通常、入手可能な検知ソフトウエアを入手し、利用することは有益です。				
	誰かが何かがおかしいと疑ったらすぐに、システムのスナップショットをとることが極めて重要です。				
	持つべき視野と影響を識別するために、そのサイトに適切で、接続形式に適切な 基準が定められる必要があります。				
	オリジナルのベンダー配布メディアが入手可能であれば、すべてのシステムファイルの分析を開始し、すべての異常事項は注目される必要があり、インシデントの対応に 参画しているすべての主体に問い合わせる必要があります。				
	インシデントへの対処においては、一定の手続きを踏むことが必要不可欠です。すべてのセキュリティ関連活動で最も重要なことは、すべてのサイトが現にポリシーを持っていることです。ポリシーと目的を定めない場合にとられる行動は、方向性のないままとなります。その目的はあらかじめ、経営管理者と法律顧問によって定められる必要があります。				
	あなたがインシデントの発生を確認したら、適当な人に通知する必要があります。どのようにこの通知がなされるかは、技術的な観点と、感情的な観点の両方からイベントを管理下におくために、非常に重要です。その状況は、その問題の通知と理解を助けるためにできるだけ詳細に記述される必要があります。その通知において、どの主体に詳細な技術情報を提供するかを決定する際には、十分に注意する必要があります。				
	まず最初に、現地の人宛てと、サイト外の人宛てのどちらのいかなる通知も、明瞭である必要があります。				
	もし、インシデント対応チームが参画した場合、情報交換のために雛形（報告様式）の項目を埋めることが必要となります。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	もし、情報が第3者に渡るのでしたら、下記の最低限の情報だけが提供されるべきです。 (1) ログのタイムゾーン 世界標準時間(GMT)または現地時間で。 (2) リモート システムについての情報 ホスト名、IP アドレス(とユーザ ID)を含む。 (3) そのリモート サイトに関連したすべてのログ エントリ (4) インシデントの種類 (何が起きたのか、なぜ問題とする必要があるのか。)				
	最低限、あなたは下記の事項を記録する必要があります。: (1) すべてのシステムイベント(監査記録) (2) あなたがとったすべての行動(時間を付して) (3) すべての外部との会話(誰と話したか、日付と時間、会話のないようを含む)				
	それゆえ、法的なフォローアップが可能である場合、準備されている手続きに従って、証拠の誤った対応によって、その法的なフォローアップを危機に陥れることを避ける必要があります。				
	下記の手続きが、適当な場合にはとられます。 (1) 定期的に(つまり毎日)、あなたのログ日誌のコピーをとり、サインされたコピーを(システム イベントを記録するのに使用されるメディアとあわせて) 文書の保管人に渡す。 (2) 保管人は、これらのコピーされたページを安全な場所(つまり金庫)に 保存する必要がある。 (3) 情報を蓄積するために実施するとき、あなたは署名と日付の付された受領書を文書の保管人から入手する必要がある。				
	この段階には、あらかじめ定められた手続きを実行することが含まれている必要があります。あなたの組織体ないしサイトは、例えば、インシデントに対応する際に、許容可能なリスクを定義する必要があり、とるべき行動と戦略もあらかじめ記述しておく必要が あります。これは、迅速な意思決定が必要で、決定するための検討を行うために、すべての参画している主体と連絡をとることが不可能なときには特に重要です。				
	ひとたびインシデントが包囲されたら、今度はその起源を根絶する番です。ただしその起源を根絶する前に、被害を受けたシステムと、そのインシデントの起源 についての、必要なすべての情報を収集することは、システムをクリーンにする際にそれらは失われがちなので、十分注意する必要があります。				
	ひとたびインシデントが起きると、すべての脆弱性をなくすことは困難です。脆弱性を除去する鍵は、その突破の知識と理解です。 当初の版のメディアを再度使用して、再度システムをカスタマイズすることが必要不可欠となります。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	この最悪の事態のシナリオを回避するために、当初のシステムの設定記録と、各カスタマイズのための変更が、保持されている必要があります。ネットワークに基づいた攻撃の場合、攻撃された各オペレーティング システムの 脆弱性のためパッチをインストールすること重要です。				
	理想的には、自動化されて、定期的に、セキュリティインシデントの検知に使用されたのと同じテストを適用する必要があります。				
	フォローアップの段階においてシステムは、クリーンアップの段階において 失われている可能性がある要素について監視される必要があります。				
	また、できるだけ早くそのインシデントが引き起こしたダメージの金額的な 見積もりを入手することも重要です。この計算には、すべてのソフトウエアやファイルの損失に関連した費用、（特に、すでに開示されている知的財産権のあるデータの価値）ハードウエアのダメージ、変更されたファイルを復元する人件費、 被害を受けたシステムの再設定などが含まれる必要があります。				
	インシデントの後、いくつかの行動をしなければなりません。 これらの行動は、下記のようにまとめることができます。: (1) そのシステムの資産の目録を作る必要があります。（つまり、慎重な検査によって、そのインシデントによって、どのように システムが影響を受けたかを判断する必要があります。） (2) そのインシデントの結果として学んだ教訓は、インシデントの再発を防止する ために、改訂されたセキュリティ計画に含められている必要があります。 (3) インシデントを前提に、新たにリスク分析がなされる必要があります。 (4) もし必要と判断されれば、そのインシデントを引き起こした人間の、 捜査と訴訟を始める必要があります。				
	もしインシデントが、貧弱なポリシー、そしてそのポリシーが変更されなかった ことに起因するものである場合、過去を繰り返すことになっています。 ひとたびサイトがインシデントから復旧したら、サイトのポリシーと手続きは、 同様のインシデントを防止するための変更を絞り込むために、レビュー（見直し） される必要があります。 たとえインシデントが起きなくても、ポリシーと手続きを定期的にレビュー（見直し） するのが賢明です。				
	「自分のネットワークを守ること」と「他人のネットワークまで守る必要があると考えること」は、全く別のことです。インシデントへの対応において、自分のシステムと他人のシステムについて特定の脆弱性が明らかになります。侵入者を追跡することは簡単で、足跡をたどってその侵入者を追跡してみたくなることさえあるでしょう。よい意図であっても、ある時点で「一線を踏み越えて」しまう可能性があり、侵入者以外の何者でもないことになることを銘記しておいてください。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	セキュリティインシデントにおいては、2つの選択肢があります。まず、サイトは、その侵入者を捕らえることができることを期待して監視することを選択することができます。;また、サイトは、そのインシデント後にクリーンアップして、侵入者をそのシステムから締め出すことができます。これは、非常に思慮深くなされる必要がある意思決定です。				
	セキュリティインシデントにユーザが関係している場合、そのサイトのセキュリティポリシーは、どのような行動がとられるべきかを記述する必要があります。違反については、深刻に受け止める必要があります。				
	あなたのシステムとネットワークは、静的な環境ではないので、あなたは、定期的にポリシーと手順を見直す必要があります。 (1)　CERT/CC のような、様々なセキュリティインシデント対応チームによって発表されるアドバイザリに登録し、あなたのサイトの技術に該当する脅威に対抗してあなたのシステムをアップグレードする。 (2)　あなたの備品のベンダーによって制作されたセキュリティパッチの動向に注目し、該当のものすべてを入手し、インストールする。 (3)　あなたのシステムの設定について発生するすべての変更を識別するために、監視する活動を行い、すべての異常事項を調査する。 (4)　すべてのセキュリティポリシーと手順を(最低限)定期的にレビュー(見直し)する。 (5)　最新情報についていくために、関連のメーリング リストと USENET のニュースグループを読み、上級システム管理者の間で情報を共有する。 (6)　定期的にポリシーと手順の遵守の状況をチェックし、この監査は、ポリシーと手順を定めたり、実装した人以外の者によって行われる必要がある。				