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	
	インターネットもしくは他のいかなる公共のネットワークに接続する前に、あなたは、アクセスプロバイダーとして利用しようとしているサイトのセキュリティポリシーを入手して、それを読む必要があります。				
	あなたが 1ユーザとして、まず最初に関心をもつべきことは、あなたのコンピュータアカウント（複数もあり得る）の悪用から保護することで、その次にあなたのプライバシーを保護することです。				
	企業のように比較的大きな機関によって通常とられているパスワード盗聴に対する予防措置は、OTP（ワンタイムパスワード）システムを使用することです。				
	＊　誰が、あなたのセキュリティ連絡先かを知る。 ＊　常にパスワードを秘密に保つ。 ＊　机を離れる際には、パスワードロックのかかるスクリーンセイバーを使用するか、または、ログアウトせよ。 ＊　あなたのコンピュータもしくは、あなたのネットワークに誰でも簡単に物理的アクセスができるようにするな。 ＊　どのようなソフトウェア動作させているかを認識し、出所の不明なソフトウェアについて用心深くなれ。ダウンロードしたソフトウェアを実行する前によく考えろ。 ＊　パニックに陥るな。できるならばアラームを鳴らしわたる前に、あなたのセキュリティ連絡先に相談せよ。 ＊　セキュリティ問題を、できるだけ早くあなたのセキュリティ連絡先に報告する。				
	ますます豊富になってきているフリーソフトウェアは、インターネット上で入手可能になりました。このエキサイティングな開発は、公共のネットワークを使用する際の最も魅力的な側面のひとつですが、同時に注意も払う必要があります。				
	ダウンロードしたすべてのファイルを、あなたがそれらの（危険な可能性がある）起源を覚えていられるように保存するように注意してください。				
	あなたがネットワーク越しにとってきた、いかなるファイルも潜在的に危険であると考える必要があります。（ Web ブラウザーのキャッシュの中のファイルもです。）誤ってそれらを実行してはいけません。				
	Web ブラウザーは、プログラムをダウンロードして、あなたの代わりに自動的に、もしくは手動によって実行します。あなたは、これらの機能を実行不能にすることができます。これらを実行可能なままにした場合、あなたがその結果を理解していることを確かめてください。				
	あなたは、あなたの会社のセキュリティポリシーのみならず、Web ブラウザーについてくるセキュリティガイドも読む必要があります。				
	あなたは、ダウンロードしたプログラムをあなたのマシン上で実行するのにはリスクがあることを知っ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	
	フォームをもった Web ページは、よくあります。電子メールと同様、Web ブラウザーから Web サーバーへ送信されたデータは、セキュアでないことを認識してください。				
	その脅威は、SSL を Web ページが本物であることを証明するのに使用することによって護ることができます。				
	あなたが電子メールを使用する際に考慮する必要がある他のセキュリティの論点は、プライバシーです。				
	あなたは、クレジットカード番号や他の慎重を要するデータを決して保護されていない電子メールで送ってはいけません。				
	多くの電子メールユーザが好んで使う他のサービスに、電子メール転送があります。これは極めて慎重に利用する必要があります。				
	仕事で送受信する電子メールは、プライベートなものではないことを銘記してください。雇用者に確認してください。それは雇用者は(場合によっては)法的 に、あなたの電子メールを読んだり利用することができる可能性があるからです。電子メールの法的な位置づけは、各国で施行されている情報のプライバシーに 関する法律によって違います。				
	その添付ファイル自体がプログラムもしくは実行可能なスクリプトである場合には、それを実行する前に特別な注意を払う必要があります。				
	あなたのパスワードは、数字、大文字と小文字、句読点の組み合わせである必要があります。あらゆる言語の実際にある単語や単語の組み合わせ、ナンバープレートの番号、名前等を避けてください。最善のパスワードは、″2B*Rnot2B″のように(ただし、このパスワードは使わないように！)組み立てられた並びです。(例: あなたが忘れないフレーズからの頭文字の組み合わせ)				
	つい、パスワードを書き留めてしまいがちですが、やらないようにしてください。				
	もし書き留める場合には、覚えるまで身につけて、覚えたら裁断してください！決してパスワードを端末の上に貼ったり、ホワイトボードに書きっぱなしにしてはいけません。				
	あなたは、アカウントごとに異なるパスワードをもつ必要があります。ただし、覚えられないほど多くのパスワードであってはなりません。あなたはパスワードを定期的に変更する必要があります。				
	あなたは、決してパスワードをスクリプトやログイン手順の中に保存してはいけません。				
	あなたが本当にあなたのシステムにログインしていることを確認してください。それは、ログインプロンプトが現れてあなたのパスワード入力を求めることは、 あなたがそれらを入れなければならないことを意味しないからです。通常でないログインプロンプトは避け、ただちにそれらをあなたのセキュリティ連絡先に報 告してください。ログイン時に何かおかしいことに気づいた場合、あなたのパスワードを変更してください。				

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	
	ネットワーク越しにパスワードを送る場合に暗号化する予防措置がとられていない限り、ネットワーク越しにシステムにログインする場合に可能であれば「OTP（ワンタイムパスワード ）」を使う必要があります。				
	あなたのシステムに、どんなソフトウェアをインストールするかについて慎重であってください。できるならば「信頼できる入手元」からのソフトウェアを使用 してください。いかなるソフトウェアをインストールするときにも、その前にあなたのサイトのポリシーをチェックして下さい。				
	集中管理されたサイトには、ウイルスの脅威を扱うためのポリシーやツールがあります。あなたのサイトポリシーにあたるか、もしくは、あなたのシステム管理者からウイルス問題を解消する正しい手順を聞き出してください。				
	ウイルス検出ツールが、あなたのシステムの問題があることを示している場合、それを報告する必要があります。あなたにそのウイルスを渡したと思われる人にだけでなく、あなたのサイトのシステム管理者にも通知する必要があります。平静であることが重要です。ウイルスに脅えることは、実際のウイルス発生 以上の遅れや混乱を引き起こします。ウイルスについて広くアナウンスする前に、ウイルス検出ツールを使用して、できれば技術的能力のある人物の支援のもと、その存在を確認するようにしてください。				
	あなたはコンピュータに何かを追加する場合においては、常に注意深くある必要があります。特に、データが流れる機器においては注意深くある必要があります。あなたは、集中管理されたコンピューティング環境においては、あなたのコンピュータに何かを接続する前に許可を得る必要があります。				
	モデムは特別なセキュリティ リスクをもたらします。多くのネットワークは、公衆ネットワークからの正面の攻撃を防ぐために設計された一連の予防措置によって保護されています。あなた のコンピュータがこのようなネットワークに接続されている場合でモデムも使用する際には、特に注意しなければなりません。				
	モデムを接続したままにして、あなたのコンピュータをリモートコンピュータにダイアルインできるようにしておいた場合に、どのようなことになるかを理解し てください。すべての適用可能なセキュリティ機能を正しく使用するようにしてください。多くのモデムは、デフォルトで呼び出しに応えます。呼び出しにあな たのコンピュータが応答する準備ができていない限り、あなたは自動応答を OFF にする必要があります。「リモートアクセス」ソフトウェアにはこれを要求するものがあります。あなたのコンピュータを電話でアクセスできるようにする前に、あなたの「リモートアクセス」ソフトウェアのすべてのセキュリティ機能を使用するようにしてください。				
	電話番号を掲載しないことで、誰かが電話回線経由であになたのコンピュータに侵入することを防ぐことができるわけではないことを知っておいてください。モデムを検出するために多くの電話回線を調べて、それから攻撃を放つことは、とても簡単なことなのです。				

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	
	端末もしくはコンピュータにログインしたまま、どこかへ行ってしまうようなことをしてはいけません。できる限りパスワードロックがかかるスクリーンセイバーを使用してください。				
	* 共有ファイル 　　共有ファイルは誰でもが、もしくは、他のユーザの制限されたグループが見ることができるものです。各システムには、これについてそれぞれの方式があります。ファイル共有の権限のコントロール方法を学習して、そのようなコントロールを間違いなく適用してください。 * 保護されたファイル 　　あなただけがアクセスできるようにする必要があるけれども、システム管理者特権をもった人であれば誰でも閲覧可能なファイルが該当します。この例として、電子メールの配信に関連のあるファイルが挙げられます。他人があなたの電子メールを読むことを望まないのであれば、そのように該当のファイルがすべての必要なファイル権限設定をもつようにしてください。				
	ファイルを暗号化する前に、あなたはあなたのサイトのセキュリティポリシーをチェックする必要があります。				
	あなたがファイルを暗号化するのに使用するパスワード、もしくは鍵については注意してください。				
	暗号化プログラムは入手可能な状況にありますが、その品質は、まちまちであることを知っておく必要があります。				
	多くの場合、ファイルの削除では実際には消えないことも知っておく必要があります。古いハードディスクに価値ある情報が残らないようにする唯一の方法は、それを再フォーマットすることです。				
	あなたは、プラグインするプログラムに親しんでいるという理由だけでプラグインを使用してはいけません。				
	繰り返しになりますが、アプリケーションコンポーネントをダウンロードすることには気をつけてください。				
	ソーシャルエンジニアリングの被害者にならないようにする方策として覚えておかなければならない重要なことは、パスワードは秘密にするものであるということです。あなたの個人的なアカウント用のパスワードは、あなただけが知っているようにする必要があります。あなたのアカウントに何かをする必要のあるシステム管理者は、あなたのパスワードを要求する事はありません。管理者がもっている権限では、あなたのパスワードを知るまでもなく、あなたのアカウント上の作業を行うことができます。管理者があなたのパスワードを聞き出す必要はないのです。				
	ユーザは、自身のアカウントの使用を守り、自分自身の使用のために使うようにする必要があります				
	サイトに来るシステム保守技術者は、（あなたが知っている）現地サイトの管理者と同伴でなければなりません。				

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	
	あなたの会話している相手が名乗っている通りの人であると確信を持てるのでない限り、そのような人に秘密情報を明かしてはなりません。				
	人の識別を 2重にチェックすることは、常に良いことです。				
	あなたがそのようにできない場合に最も賢明なことは、秘密を明かさないことです。				
	あなたがシステム管理者である場合、パスワードのユーザへの割り当てと再割り当てのためのセキュリティの手続きがあるはずであり、あなたはそのような手続きに従う必要があります。				
	あなたがエンドユーザである場合には、システムの秘密を誰にも明かす必要は全くありません。				
	会社によっては複数の ユーザに共通アカウントを割り当てているところがあります。あなたが、そのようなグループに含まれてしまった場合、グループのメンバーであると名乗る人が本当であることがわかるように、グループの全員を知っておくようにしてください。				
	*セキュリティ機能を ON にする方法を学ぶためにマニュアルを読み、それらを ON にする。 *あなたのデータや電子メールのプライバシーを、どの程度確保する必要があるかを考えよ。あなたは、プライバシーソフトウェアを調べて、その使い方を学んだことがあるか？ *あらかじめ最悪の事態に備える。 *どのような脅威があるかについて最新の情報を知っておく。				
	あなたは、事前に許容できるリスクを判断し、この判断に依拠する必要があります。				
	あなたの判断を、定期的に、また必要性が生ずるごとに、レヴューするのも賢明です。				
	単に、ネットワークからいかなるソフトウェアをも、ダウンロードすることを避けるようにするのも賢明です。				
	複数のユーザによって共有されている場合、コンピュータ上にプライバシーソフトウェアをインストールすることには価値があります。				
	あなたのファイルが改ざんされたことに気がついた場合、もしくは、何らかの方法であなたの承諾なしにアカウントが使用されていたことを突き止めた場合、ただちにあなたのセキュリティ連絡先に通知する必要があります。				
	すべてのユーザ向け文書を注意深く読んで下さい。あなたのコンピュータ上でサービスを動作させている場合、これが明確であるようにしてください。ネットワークサービスが活動している場合、それらが正しく設定されているようにしてください。（すべてのパーミションを、匿名、もしくはゲストログイン等を防ぐように設定してください。）多くのプログラムにネットワーク機能が組み込まれるようになってきています。このような機能の正しい設定方法と、安全な使用方法を学んでください。				

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	
	ユーザのデータをバックアップしてください。これは常に重要です。バックアップは、通常、ハードディスクが壊れた場合、もしくは誤ってファイルを削除してしまった場合、あなたの作業を失わないようにする考え方です。バックアップすることも、コンピュータセキュリティインシデントによってデータを失われないようにするために重要です。最も悪徳で、残念ながら卑近な脅威には、コンピュータウイルスやトロイの木馬プログラムによってもたらされる、コンピュータのハードディスクの消去があります。				
	ウイルス検出ソフトウェア、もしくはセキュリティ監査ツールを入手してください。公衆ネットワークに接続する前に、それらの使用法とインストール方法を学んでください。多くのセキュリティツールは、現状と元の状態を比較できるようにするために、「クリーン」なシステム上で動作させることを要求します。それゆえ、事前にいくつかの作業が必要です。				
	ネットワーキングソフトウェアを定期的にアップグレードしてください。新しいバージョンのプログラムが出たら、アップグレードするのが賢明です。セキュリティ脆弱性は、解消されている可能性が高いといえます。これをやらずにいる期間が長いほど、製品のセキュリティ脆弱性が知られて、どこかのネットワーク攻撃者によって攻撃されるリスクが大きくなります。「アップトゥデート」に保って下さい！				
	あなたがトラブルを懸念する場合に連絡する相手を見つけてください。あなたの ISP（インターネットサービスプロバイダー）は、セキュリティ連絡先、もしくはヘルプデスクをもっているでしょうか？トラブルが起きてから、それらを探そうとして時間を無駄にしないように、トラブルが起きる前にこれを調べておいてください。簡単に連絡できるように、オンラインとオフラインの両方の連絡先情報をもつようにしてください。				
	ウイルスの問題を避ける方法が 3つあります。: 1. ごちゃ混ぜにしない できる限り、どんなソフトウェアをあなたのシステムにインストールするかについて注意してください。出所が不明、もしくは不確かなプログラムを動作させてはいけません。あなたが再フォーマットしたのでない限り、古いフロッピーディスクを使って、特にその古いフロッピーディスクがソフトウェアを展示会などから持ち帰った媒体であった場合には、プログラムを実行したり、再起動してはいけません。 あなたのコンピュータにどのようなファイルが保存されているかについて、細心の注意を払うならば、ほとんどすべてのウイルス感染のリスクは、なくすことができます。詳細については「ダウンロードする際の危険」をご覧ください。				

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	
	3. 異常に注意する 「異常を検出できないから異常がない」というのは真ではありませんが、これはよいルールであるといえます。あなたのシステムの動きに親しんでおく必要があります。説明のつかない異常がある場合、(例えば、あるべきはずのファイルがない、見慣れない新しいファイルがある、ディスクの空きスペースが「なくなっている」場合、)ウイルスの存在をチェックする必要があります。				
	あなた自身のコンピュータを維持管理する責任がある場合、あなたのコンピュータの機種用のコンピュータ ウイルス検出ツールに慣れ親しんでおく必要があります。あなたは、最新のツール(すなわち 3ヶ月以内のもの)を使う必要があります。既に報告されているウイルスが、あなたの組織で「発生」している場合、あるいは、あなたがフリーウェアを使用していた場合、他人が使用したフロッピーディスクをファイルを運ぶのに使用していた場合などには、あなたのコンピュータをテストすることが非常に重要です。				
	あなたのホームコンピュータにウイルスがあるとか、悪意を持ったプログラムが動作したとか、システムが侵入されたといった懸念がある場合、最も賢明な行動は、まずそのシステムをすべてのネットワークから切断することです。入手可能であれば、ウイルス検出ソフトウェア、またはシステム監査ソフトウェアを使用する必要があります。				
	ホームシステムが攻撃されたことが明らかになったら、それはクリーンアップするときです。理想的には、システムをスクラッチから再構築する必要があります。これはハードディスク上のすべてを消去することを意味します。次に、OS(オペレーティングシステム)をインストールし、次にそのシステムが必要と するすべての追加的なソフトウェアをインストールしてください。その OS(オペレーティングシステム)や追加的なソフトウェアをバックアップストレージからではなく、オリジナルの配布フロッピーディスク、もしくは CD-ROM からインストールするのが最良といえます。この理由は、システムはしばらく前に侵入されたことがあり、そのバックアップ システム、もしくはプログラムファイルには、改ざんされたファイル、もしくはウイルスがある可能性があるからです。システムをスクラッチからリストアする ことは退屈ですが、やる価値があります。セキュリティインシデントの前にインストールしていた、すべてのセキュリティ関連のフィックスを再インストールすることを忘れてはいけません。これらは、確認された確かな源泉から入手してください。				

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	
	ホームコンピュータ上でサービスを動作させることのセキュリティに関する限り、覚えておくべき 4つの非常に重要なことがあります。 ＊最初に最も重要なことですが、サーバーが正しく設定されていない場合、ネットワーク上での攻撃に対して非常に脆弱であるといえます。あなたがサービスを動作させている場合、正しい設定に慣れておくことが決定的に重要です。これは、しばしば容易ではなく、トレーニング、もしくは技術的経験を要求する可能性があります。 ＊すべてのソフトウェアには欠陥があり、発見された欠陥は、不正にコンピュータセキュリティを突破するのに利用される可能性があります。あなたのホームマシン上でサーバーを動作させている場合、知って おく必要があります。これは作業を要求します。: あなたはセキュリティアップデートを入手するために、ソフトウェアの供給者と連絡がとれるようにしておく必要があります。オンラインのセキュリティフォーラムを通じて、セキュリティの論点を知っておくことが強く推奨されます。参考文献のリストについては [RFC2196] をご覧ください。				
	あなたのサーバーソフトウェアにセキュリティ上の欠陥が見つかった場合、そのソフトウェアの使用を止めるか、もしくは、脆弱性をなくす「パッチ」もしくは「フィックス」を適用する必要があります。ソフトウェアの供給者は、礼儀正しい会社、もしくはフリーウェアの作者であれば、セキュリティの欠陥を修正する情報やアップデートを提供します。このような「パッチ」もしくは「フィックス」を、できるだけ早くインストールしなければなりません。 ＊よく言われるルールとして、古いソフトウェアほど既知の脆弱性をもつ可能性が大きいといえます。これは、あなたは素直に真新しいソフトウェアを信頼する必要がある、ということではありません！しばしば、サーバーにある明らかなセキュリティの欠陥でさえ、発見するのに時間がかかります。 ＊サーバーには、何の警告もなしに起動するものがあります。Web ブラウザーや telnet クライアントには、明示的に禁止する設定をしない場合、自動的に FTP サーバーを起動するものがあります。このようなサーバー自体が正しく設定されていない場合、ホームコンピュータのファイルシステム全体がインターネット上の誰からでも入手可能となりえます。				
	一般的に、どんなソフトウェアでもネットワーク デーモンを起動することができます。安全であるための方法は、あなたが使用している製品を知ることです。あなたが製品を使用することによって実際にサービ スを動作させているかを見出すために、マニュアルを読んでください。そして何か疑問がわいたときには、その会社に問い合わせるか、フリーソフトウェアの作 者にメールしてください。				

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	
	できるならば、あなたのサーバーソフトウェアにあるセキュリティに関連するすべての「ログをとる」オプションを活動させてください。このログをとることによる恩恵を得るためには、あなたは、このようなログを定期的にレヴューする必要があります。ログがしばしば非常に速く膨張するので、あなたは、ハードディスクが満杯にならないように注意する必要があることを知っておく必要もあります！				
	ユーザはリモートログインするとき、非常に注意深くある必要があります。				
	あなたがリモートログインサービスの使用を望む場合、その接続がセキュアに行うことができることをチェックし、セキュア技術／機能を使用するようにしてください。				
	接続は、OTP（ワンタイムパスワード）、SSH（Secure Shell）、SSL（Secure Sockets Layer）のような技術を使用することによって、セキュアにすることができます。OTP（ワンタイムパスワード）は、パスワードを盗むことを無意味にし、SSH は 、接続上を転送されるデータを暗号化します。SSL の検討については「Web で風邪をひかないように」をご覧ください。このようなセキュアサービスは、リモートでログインしようとするシステム上で利用できるようにする必要があります。				
	あなたがコンピュータ上にビジネスの記録や、他の慎重を要するデータを保存している場合、暗号化機能が安全に保存するのに役立ちます。				
	しかし、いかなるシステム上で動作するあらゆる暗号化機能についていえることですが、鍵やパスワードを最初に安全に保存する必要があります！				
	変化する我々が住んでいる世界の中で、ちょうど住宅をもっている人が、利便性や、その家をセキュアにするための支出に注目するようになってきているのと同様に、コンピュータネットワークのユーザは、セキュリティを無視してはいけません。				
	Default Account（デフォルトアカウント） 　システムやサーバーソフトウェアには、事前に設定されたアカウントをもって提供されるものがあります。このようなアカウントは、あらかじめ定められた（ユーザ名と）パスワードで設定されていることがあり、誰でもアクセスできるようになっていたり、しばしばユーザが最初にログインするのに便利なように添えられていたりします。デフォルトアカウントは OFF にする、もしくは、システムの濫用のリスクを低減するために事前設定されたパスワードを変更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	
	Systems Administrator（システム管理者） 　システムを保守管理し、システム管理者特権をもっている個人をいいます。管理者としてではない作業中は、この個人によるエラーやミスを避けるために、（そのシステムの）管理者として行為する時間を最小限に制限する必要があります。				