RFC1281　インターネットのセキュアな運用のためのガイドライン

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	
	(1) ユーザには、各自、自身が使用しているシステム(コンピュータとネットワーク)のセキュリティポリシーを理解し遵守する責任があります。ユーザは 、各自、自身の行為に責任を負います。				
	ポリシーのこの部分については、他に、各ユーザには割り当てられたすべての資源の利用に責任があり、それゆえ、アカウントと資源へのアクセスの共有は固く 禁じられていることがあります。しかし、資源へのアクセスは各サイトとネットワーク運用者ごとに割り当てられるので、アカウントの共有を規制する固有の ルールとアクセスの保護は、ローカルなものである必要があります。				
	(2) 各ユーザには、自身のデータを保護するために、入手可能なセキュリティ機構と手順を採用する責任があります。また、使用するシステムの保護を支援する責任もあります。				
	各ユーザには、妥当なやり方でアカウントの権限を扱うことと、サイトで定める、システムのセキュリティのための 手順と、データのセキュリティのための手順に従うことが求められます。パスワードによる保護に依存するシステムについては、各ユーザは適切なパスワードを選択し、定期的に変更する必要があります。				
	(3) コンピュータとネットワーク サービスのプロバイダーには、運用しているシステムのセキュリティを確保する責任があります。さらに、ユーザにセキュリティポリシーと、このポリシーの変更のすべてを知らせる責任もあります。				
	インターネット自身は、集中管理されていませんし、運営されてもいないので、セキュリティについての責任は、インターネットの該当部分の所有者と運営者に あります。さらに、たとえこのインフラストラクチャに中央集権的な監督機関があったとしても、セキュリティは、システムの所有者と運用者の責任である必要があります。そのシステムは、インターネットの主たるデータ資源であり、処理資源であるのです。				
	サイトにおける厳密なセキュリティ手段とシステムの簡易な使用の間には、トレードオフの関係があります。(例: 厳密なセキュリティ手段は、ユーザのインターネットへのアクセスを面倒にしてしまいます。) あるサイトが、システムを保護せずに開けておくようにする場合、攻撃者の身元を隠しながら、他のインターネットホストの攻撃のための足場を提供することに なってしまいます。オープンなシステムを運用しているサイトは、システムのユーザの行為に対して責任があるとともに、必要とあらば他のサイトを支援できるように しておく必要があります。各サイトは、できるかぎりインターネットへのアクセスが認証されているかを確認するようにすべきです。				
	(4) 各ベンダーと各システム開発者には、堅固で、適切なセキュリティコントロールを実装したシステムを提供する責任があります。				
	ベンダーもしくはシステム開発者は、インターネットコミュニティにそのシステムを導入する前に、セキュリティコントロールの観点から 各システムを評価する必要があります。(商用、フリーにかかわらず)各製品は、実装しているセキュリティ機能を記述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	
	(5) 各ユーザ、各サービスプロバイダー、各ハードウエアとソフトウエアのベンダーには、セキュリティを提供するために協力しあう責任があります。				
	(6) インターネットセキュリティプロトコルにおける技術的な改善が、継続的に模索される必要があります。同時に、新しいプロトコル、インターネット用のハードウエアもしくはソフトウエアの開発者には、設計と開発のプロセスにおいて、セキュリティについて考慮することが期待されます。				
	(a)既存の基本的なセキュリティ機構において、改良がなされる必要があります。パスワードセキュリティは通常、インターネットの世界では貧弱であり、パスワード割り当てを管理するツールと、より良い認証技術の使用によって、著しく改善することができます。 同時に、インターネットユーザの人口は、増加しており、 技術的に不慣れなユーザが、より多くの比率を占めるようになっています。配布されるシステムのセキュリティのデフォルトとセキュリティを管理するためのコントロールは、この増加しつつある人々に合わせる必要があります。 (b) プロトコルスーツのセキュリティ拡張が必要です。セキュリティを改善するために追加される必要のあるプロトコルの候補には、ネットワーク管理、ルーティング、ファイル転送、telnet およびメールがあります。 (c) オペレーティングシステムの設計と実装は、よりセキュリティに重点をおくように改善すべきであり、インターネット上のシステムへのセキュリティの実装の質に、もっと注目すべきです。				
	ローカルのセキュリティを改善する際には、5つの分野の対策が必要です。: (1) ローカルのセキュリティポリシーの明確な表明が必要であり、このポリシーは、そのユーザと他の関連する主体に伝達される必要があります。このポリシーは、ファイルとして、ユーザがいつでも入手できるようにする必要があり、システムへのアクセスを提供する際にユーザに伝達される必要があります。 (2) 適切なセキュリティ コントロールが実装される必要があります。これは、つまり最低限、システムへのアクセスをパスワードでコントロールし、まともなパスワード管理を制定し、システム自身とその中の情報を守るようにシステムを設定する、ということです。				

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	
	(3) セキュリティの遵守を監視し、セキュリティの侵害を含むインシデントに対応することができるものが必要です。ログインのログ、ログインの試みなどのセキュリティ関連のイベントは、通常のログの監査と同様、強くお薦めいたします。コネクションや、侵入に対応した他のイベントを追跡することができるものもまた薦められます。しかし、サービスプロバイダーは、収集する情報、それにアクセスできる人、目的について、よく検討された公表されたポリシーをもつことが重要です。このようなポリシーを設ける際には、ネットワークユーザのプライバシーの確保が、考慮される必要があります。 (4) セキュリティ事象を扱うために、コミュニケーションと統制の連携が確立される必要があります。セキュリティの連絡窓口としての責任者が指名される必要があります。セキュリティの連絡窓口への連絡手段は、すべてのユーザに知らせる必要があり、また、公衆のディレクトリに登録される必要があり、さらにコンピュータ 緊急対応センターがいつでも連絡先情報を容易に見つけられるようにすべきです。 セキュリティ連絡窓口は、そのサイトのすべてのシステムの技術と設定に慣れているか、もしくは、いつでもこの知識をもった者と連絡がとることができる必要があります。同様に、セキュリティ連絡窓口は、セキュリティインシデントを扱う最善の努力を行なうことが事前に許可されているか、もしくは、いつでもそれを 承認する者と連絡をとることができる必要があります。				
	(5) セキュリティインシデントを知らされた各サイトとネットワークは、適時に有効なやり方で対応する必要があります。侵入ないし他の侵害が起きた場合、各サイトとネットワークは 、そのインシデントの性格を識別するためと被害を限定するために、資源と対策手段を割り当てる必要があります。適時に、有効にインシデントに対応しないとしたら、サイト／ネットワークは、よいセキュリティをもっているとは考えられないでしょう。 侵害者が特定できる場合、それ以上の侵害が引き起こされないようにするために、適切な行動がとられる必要があります。侵害者に対して課されるべき制裁は、インシデントの性格とサイトの環境によって決まります。例えば、ある大学では学生の侵害者に対して、内部的な処分を行うことを選ぶことでしょう。 同様に、各サイトやネットワークは、システムにセキュリティ上の欠陥があることを知らされた場合、対応する必要があります。各サイトやネットワークには、 修正プログラム（フィックス）が入手可能となり次第、システムにそれらをインストールする責任があります。				