サイバーテロリズムに対する不正侵入マネジメントの方法論に関する研究

細　貝　康　夫*

A Study on Methodology of Intrusion Management for Cyber-terrorism

Yasuo Hosogai

The extension of the internet around the world is going to give more chance to cyber-terrorism to attack the computer networks of enterprises and research institutes.

In this paper, the author proposes a methodology of intrusion management for cyber-terrorism. The intrusion management consists of four phases: planning phase, assessment phase, monitoring phase and control phase. Individual tasks involved in these phases are explained concretely in this paper. The tools useful for the intrusion management and the way to get them are also introduced for the practical application of the methodology given in this paper.

1. はじめに

インターネットの急速な普及に伴い、コンピューターネットワークを悪用して企業や研究所の活動に打撃を与え、社会を混乱に陥れる「サイバーテロリズム」の多発が予想される。本研究ではサイバーテロリズムについて、社会問題となった背景、その目的、特性、定義を述べる。次に、海外と国内におけるサイバーテロリズムの脅威を概観するとともに、犯罪行為の手口を分析し、サイバーテロリズムを防止するための「不正侵入マネジメントの方法論」について述べる。

2. サイバーテロリズムとは

(1) サイバーテロリズムの背景

サイバーテロリズムが社会問題となってきた背景は、インターネットの急速な普及により、現実社会を超えたコンピューターによる思考活動空間（電脳空間）が登場したことである。この電脳空間のことをサイバースペースと呼ぶ。サイバーテロリズムは、このサイバースペースにおける情報戦争である。サイバースペースは時間と空間の壁がないため、コンピューター・ネットワークに接続すれば遠隔地との間で情報を双方向で受発信することができるという特徴がある。

このサイバースペースの情報基盤の上に、社会・経済活動の効率化、図民生活の利便性の向上および科学・文化の向上に貢献するであろう活力ある豊かな高度情報化社会が形成された。その一方で、情報化社会の脆弱性も増大してきている。情報への依存度が高い社会や国では、情報が抱える陰の部分も増大してくるのである。インターネットが普及していけばいくほど、利便性が向上すると同時に、サイバーギャングとかサイバーテロリストに狙われる可能性が高くなった。

(2)　情報システムへの脅威とサイバーテロリズムの目的

*経営工学科

情報システムには、自然災害による脅威、偶然の脅威、そして意図的な脅威がある。サイバーテロリズムの脅威は意図的な脅威であり、その目的に対する攻撃目標はそれぞれ、①国家転覆や社会擾乱を行う目的には政府と重要社会基盤、②脅迫や恐喝などの営利目的には政府と企業、③産業スパイなどビジネスの目的には特定企業、④怨恨による復讐目的には重要社会基盤、⑤趣味（達成感、優越感）の目的に対しては不特定企業などがある。

(3) サイバーテロリズムの特性

サイバーテロリズムの特性として次のことがあげられている[3)]。

・サイバーテロリズムは遠隔地から行われるので、攻撃源をたどりにくいし、早期警戒が困難不能、攻撃者はプロや外国政府に雇われたハッカーである。
・サイバーテロリズムは低リスクである
・サイバーテロリズムは低コストである
・サイバーテロリズムの目的は宣伝効果と恐喝
・防護目標は無備である
・先制攻撃の優越性をもつ

(4) サイバーテロリズムの定義

通商産業省の中に、サイバーテロリズム対策のガイドラインを作成するために数年前から「大規模プラント・ネットワーク・セキュリティ対策委員会」という研究会が設置されている。この研究会によると、「サイバーテロリズムとは、ネットワークを通じて政治や産業に対して行われる敵対的な行動であり、大規模で組織的な不正アクセスを試みることである」と定義している[3)]。

サイバーテロリズムは米国等の専門家によって「グローバルな情報戦争」と定義され、一定の政治・経済目的により行政、金融、航空管制、電力などの公共のコンピュータ・ネットワーク・システムに不正侵入し、システム自体の誤動作、停止、破壊及び重要情報の不正取得、改ざん、ウィルス投与等を引き起こすことである。

3.　海外と国内におけるサイバーテロリズムの脅威の動向

(1)　海外におけるサイバーテロリズムの脅威の動向を図表1に示す[3), 5)]。

図表1　海外におけるサイバーテロリズムの脅威

項番	発生年月	発生場所、犯罪内容
1	1994.3	米ローム空軍研究への侵入
2	1994.6	シティバンクへの侵入・資金移動
3	1996.6	米国、英国の銀行からサイバーテロリストの脅迫により5億ドル強奪
4	1998.2	米軍コンピュータへの侵入
5	1998.9	NYタイムズのホームページがハッカーに乗っ取られた

(2)　国内におけるサイバーテロリズムの脅威の動向を図表2に示す[3), 5)]。

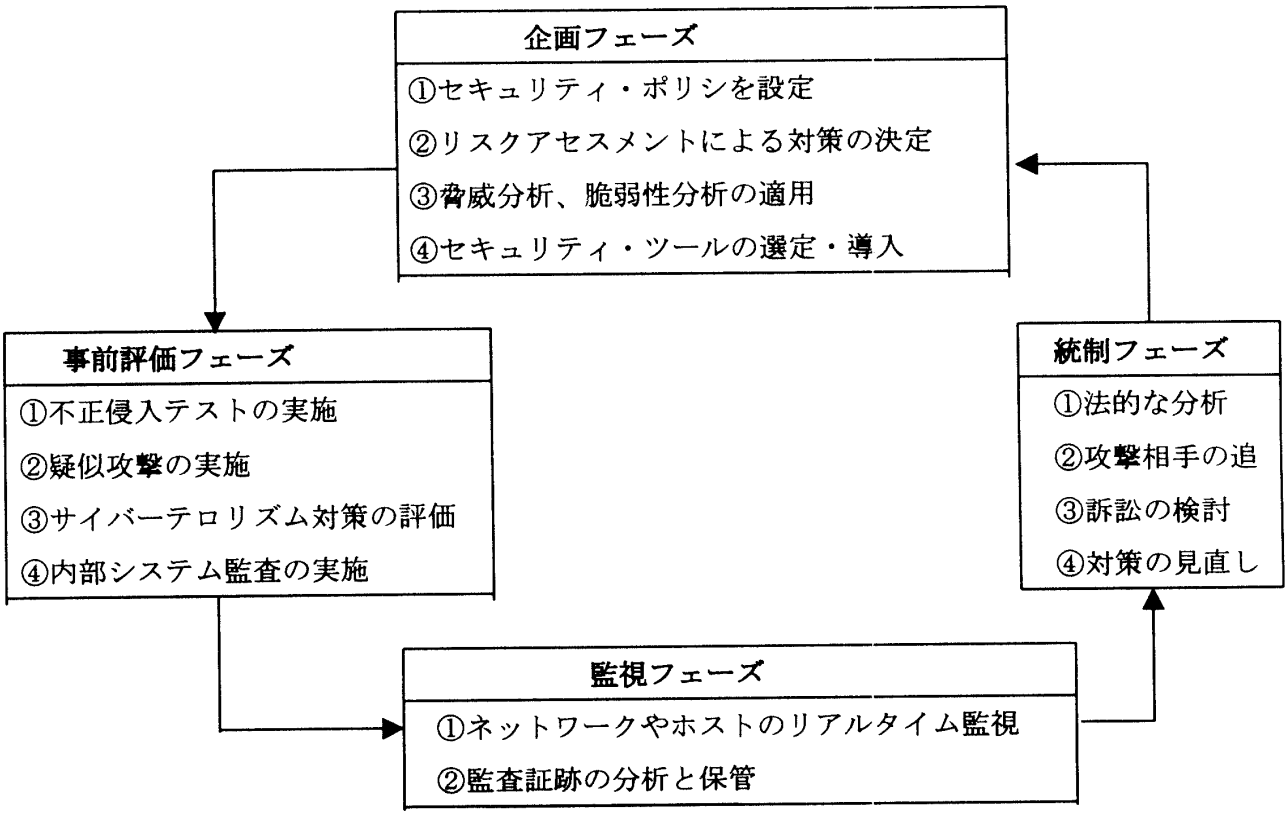
図表2　国内におけるサイバーテロリズムの脅威

項番	発生年月	発生場所、犯罪内容
1	1995.12	東海銀行における資金移動
2	1996.4	大分県プロバイダへの侵入
3	1996.12	sendmail アタック事件
4	1997.4	Email 爆撃
5	1997.6	httpd アタック事件
6	1998.4	通商産業省の入札説明用フロッピーディスクにウイルスが感染

4. サイバーテロリズムに対する不正侵入マネジメントの管理手順

サイバーテロリズムを企業リスクの一つとして管理していくための方法論にについては、確定的なものは無いのが現状である。そこで、不正侵入防止システムの開発・導入・運用の管理手順が新兵器システムのそれと類似していることから、米空軍で用いられているシステム・エンジニアリングの方法論（AFSCM375-5）[1] を参考にサイバーテロリズムに対する不正侵入マネジメントの管理手順を研究した。図表３で示すように不正侵入マネジメントサイクルは、４つのフェーズに分かれており、企画フェーズ、事前評価フェーズ、監視フェーズ、統制フエーズから構成される。各フェーズでの主要な目的と作業の概要は次のとおりである。

図表３　不正侵入マネジメント・サイクル



4.1　企画フェーズ

企画フェーズでの目的は、サイバーテロリズム不正侵入（intrusion）を回避（avoidance）するシステムを企画し、導入することである。作業の概要としては、セキュリティの概念に基づいてセキュリティ・ポリシを設定し、リスクアセスメントを行って防止対策を決定する。その際、

資産の定義から脅威分析と脆弱性分析を行いリスクを定義する。また、防止対策をとるための技術として暗号技術、ファイアウォール、アクセス制御技術などの調査やテストを行い、防止システムを選定・決定する。

(1) セキュリティ・ポリシの設定

セキュリティ・ポリシのチェックリストを用いて作成する。守るべき目標、客体（たとえばライフライン）の中で防御すべき項目を洗い出し、重要度をだいたい3段階に区分することによって、どこを守るかを決する。重要度は全員により評点法で決定する。そしてセキュリティ・ポリシを設定した中で、脅威分析を用いて、安全対策の妥当性を検討するために分析を行う。

(2) リスクアセスメントによる防止対策の決定

リスク・アセスメントとは、セキュリティ上のリスクおよびそれに対する対策の効果を数値化することによって、基準に照らしたリスク管理を実施することである。同時に費用対効果や現状のセキュリティ・レベルが、どのように改善されてきたかを数値によって評価する。なお、リスクアセスメントのツールとして、TDSの「Trident Information Protection Toolbox」がある。

(3) 脅威分析、脆弱性分析の適用

①HAZOP（Hazard and Operability Studies）：プラント（化学プロセス）の安全性を評価する手法。設計意図からの「ずれ」を想定し、その原因、影響を検討することにより、安全対策の妥当性を検討する。

②FTA（Fault Tree Analysis）：障害・事故事象とその原因を想定し、事象と原因の因果関係を木構造に図式化して表現することにより、事象を避けるために除去すべき原因集合を抽出する手法である。

③ 脆弱性テスト：脆弱性テストは、既存の制御における脆弱な領域を発見し、潜在的脅威を特定するものである。これはクラッカがシステムへの無認可アクセスを得るために使用するツールが模倣され、利用される。主なチェック項目には、次のものがあげられる[4]。

- ●強度が不十分なパスワード、もしくはパスワードの未設定
- ●パスワードファイルを入手する試み
- ●保護されていないシステムバイナリとファイル
- ●機密データへのアクセスの試み
- ●既知のバグの利用
- ●不適切に実装された制御

(4) セキュリティ・ツールの選定・導入

特定した潜在的脅威を回避するために暗号技術、ファイアウォール、アクセス制御技術などを選定・導入する。具体的には、セキュリティ・スイート製品を選定・導入する。

4.2　事前評価フェーズ

このフェーズでの目的は、防止システムを運用する前に事前評価（アセスメント）を行うことである。作業の概要としては、企画フェーズで導入した防止システムが要求どおりに役立つもの

かどうか、事前評価することである。セキュリティ・ポリシに基づいて、システムの安全度をチェックする不正侵入テストや定期的なシステム監査があって、初めてシステムに「保証」が与えられる。疑似攻撃を実施するために、米国政府や一部の大企業の中には専門のタィガー・チーム（不正侵入テストなどを専門に手掛けるチーム）を組織内に抱えるところまである。

(1) 不正侵入テストの実施

インターネットや電話回線から企業ネットワークへの不正侵入テストを行うために、ペネトレーションテストを実施する。

(2) 疑似攻撃の実施

防止システム（防衛側）に対して、タィガー・チーム（攻撃側）が Tiger、COPS、SATAN などを用いてシミュレーションにより疑似攻撃を行う。つまり、セキュリティ・ホールを見つけて不正アクセスを行う。このような2サイドゲーミング・シミュレーションにより、運用前に導入する防止システムのどこが悪いのかを事前に評価することが可能となる。

(3) サイバーテロリズム対策の評価

セキュリティの評価基準に照らして、防止システムを評価する。

(4) 内部システム監査の実施

監査チームを組んで内部システム監査を行う。監査の視点は、主に内部統制全般の点検、安全性及び不正・詐欺の点検・摘発の監査を実施する。

4.3 監視フェーズ

このフェーズでの目的は、防止システムを実施・監視することである。万一に備えて不正侵入や内部不正の存在を常時監視する仕組みが必要となる。作業の概要は、事前評価後のネットワークやホストのリアルタイム監視と、監査証跡の分析と保管を行う。

(1) ネットワークやホストのリアルタイム監視

ネットワーク監視ツールや不正侵入検出プログラムを用いて、不正をリアルタイムで監視し発見する。

(2)監査証跡の分析と保管

変更検出ツールを用いて監査証跡を分析するとともに監査証跡を保管する。

4.4 統制フェーズ

このフェーズでの目的は、サイバーテロリズムに対処するために法的な分析を検討して攻撃相手を追跡していき、訴訟を行うことである。作業の概要は、監査証跡に基づいて法的な分析を行い、攻撃相手の特定し、訴訟を検討し、実行する。

(1) 法的な分析

監査証跡を調べてサイバーテロリズムに対処するために訴訟が可能かどうか、必ず有能な弁護士に相談すること。

(2) 攻撃相手の追跡

不正侵入検出プログラムを用いて不正侵入の証跡がないかどうかを調べる。

(3) 訴訟の検討

攻撃相手が特定できたら訴訟を検討する。法的な手段には難しさや危険な側面があるため、十分考えてから実行することが肝要である。

(4) 対策の見直し

最終的には、対策の見直しを図ってまた最初の企画フェーズに戻る（ローリング）ことが重要である。これらの管理には多くのコストがかかるので、費用対効果のトレードオフにもとづいて対策を練るとことが肝要である。

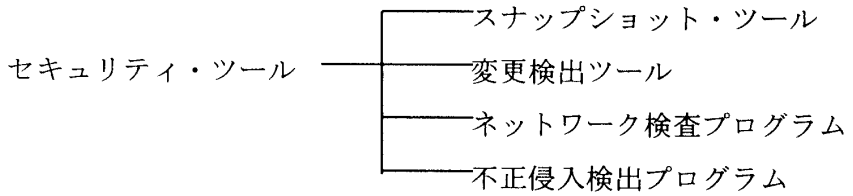
5. セキュリティ・ツールの利用動向

ここでは、不正侵入マネジメントで利用可能なセキュリティ・ツールについて概観する。

5.1　セキュリティ・ツールの体系化

セキュリティ・ツールは、サイトでセキュリティの評価や強化を行う専用プログラムのことである。セキュリティ・ツールは、図表4で示すように4種類に大別される[2)]。

図表4　セキュリティ・ツールの体系化



(1) スナップショット・ツール

これは、静的監査ツールとも呼ばれ、システムに弱点がないどうかを調べてその報告をするツールのことである。スナップショットプログラムは定期的に実行することが望ましい。少なくとも毎月1回、できれば毎週1回実行するのがよい。このプログラムからの出力結果を慎重に分析し、確認作業を実施する。この出力データを秘匿することも大切である。

① COPS (Computer Oracle and Password System)：パッケージは、小さなシェルファイルやCプログラムを集めたものである。このパッケージを利用すると、システムに弱点がないかどうかをチェックすることができる。ファイルやディレクトリごとにアクセス許可権が適切に設定されているかどうか、構成ファイルに問題がないかどうかなどがチェックできる。COPS は、コードを読み出すことによって検証を簡素化し、それぞれの特殊な環境に合わせた修正も簡単にできるようになっている。

② Tiger：Tiger の開発者は、テキサスA&M大学（TAMU）の Doug Schales 氏である。Tiger は、前述の COPS とよく似た方法で、UNIX システムにセキュリテイ上の問題がないかどうかを調べる一連のスクリプトで構成される。当初の目的は、大学外からアクセスを希望するユーザに許可を与えたことに伴い、大学内の UNIX システムをチェックすることだった。ファイアウォールのパケットフィルタリングを修正して大学外からのアクセスを許可するようになるまでは、システムは Tiger でチェックしなければならなかった。

(2) 変更検出ツール

システムを定期的に監視し、不正な改ざんがないかどうかを調べるツールである。不正侵人者

が再侵入しやすいように細工を施したり不正侵入の足跡を消したりすることを調べるためである。このことは、不正侵入があったという事実を知る手がかりをつかむためである。不正侵入は通常ひそかに行われるので、変更検出ツールを使用しなければ、不正侵入があったという事実を確認して適切な対策を講じることはできない。

① Tripwire：Tripwire は UNIX のホスト上で、ファイルの改ざんを検出するチェックサム・ツールである。チェックサム・ツールは、各ファイルの正常な状態における特徴的な値を求めて登録しておき、定期的にこれらの特徴的な値を求め直して両者の値の一致を検証する。Tripwire はアメリカの Purdue 大学の COAST プロジェクトて開発された。

(3) ネットワーク監視ツール

これはネットワークを監視し、ネットワークに弱点がないかどうかを調べる自動ツールである。ネットワークを検査するための自動ツールは、sendmail や ftpd などのネットワークプログラムに既知のセキュリティ関連バグがないかどうかをチェックするプログラムのことである。

① SATAN (Security Administrator Tool for Analyzing Network) は、Wietse Venema 氏と Dan Fammer 氏が開発したものである。SATAN はシステム管理者向けのツールである。SATAN は、ネットワークに関連した共通のセキュリティ問題を検出し、問題点をそのまま報告する。COPS や Tiger などのツールはシステムの内部から動かすが、SATAN はシステムの外部から動かす。これは外部からの攻撃に悪用されやすい。すでに侵入したことのあるシステムだけではなく、ほかのシステムへも SATAN で侵入できる。

② ISS (Internet Security Scanner) の開発者は Christopher William Klaus 氏である。ISS をほかのシステムから実行し、それを自分のシステムに向けて利用してみることで、クラッカーに悪用されやすいバグや構成エラーがないかどうかを調べることができる。

(4) 不正侵入検出プログラム

システムとネットワークの両方を監視し、不審な振る舞いがないかどうかを調べるツールである。不正侵入者は、いったんシステムに忍び込むことに成功すると、今後再び入りやすいような細工を施す。そしてひそかに築いた拠点を足がかりにして組織の内部やインターネット上のほかのコンピュータへと侵入していく。現在市販されているのは次の 3 種類である。

①Gauntlet Force Field：システムを監視し、不正侵入の痕跡がないかどうかを調べる。

②Net Ranger：ネットワークを監視し、不正侵入がないかどうかを調べる。

③ Real Secure：さまざまな不正アクセスのパターンをデータベースとして持ち、それと社外からの侵入や社内のアクセスを照らし合わせることで不正をリアルタイムで発見する。

5.2 役立つソフトウェア

セキュリティを維持するのに役立つソフトウェアを紹介する[2)]。

(1) Internet Scanner：ファイアウオールや WWW サーバなどに含まれるセキュリティ・ホールを登録してあるデータベースを参照して穴を発見し、パッチ・プログラムが公開されている WWW サイトなどを知らせる機能をもつ。

(2) TCP Wrapper：これは、ホスト（UNIX）上で、フィルタリング機能とロギング機能を提供するツールである。すなわち、FTP や Telenet 等の TCP のインターネットサービスを提供するプログラムを利用する要求があった場合に、一定のアクセスを制限する機能と、そのアクセスについての情報を蓄積（ロギング）する機能を持つ。想定されていない IP アドレスないしドメインからのアクセスがあった場合に、それを検知することができる。

(5) Kerberos：これは、共有鍵暗号方式に基づいたネットワーク認証システムである。Kerberos のソースコードとマニュアルは、MIT（マサチューセッツ工科大学）から入手できる。

5.3 セキュリティ・スイート製品の動向

セキュリティ・ツールも体系化・統合化されたセキュリティ・スイート製品が市場に出回っている。したがって、この管理手順においてセキュリティ・サービスやスイート製品を実績のあるベンダーから購入または委託すると良い[6]。

図表 5　セキュリティ・スイート製品

製品カテゴリ	ｱｸｾﾝﾄ・ﾃｸﾉﾛｼﾞｰ	ｲﾝﾀｰﾈｯﾄ・ｾｷｭﾘﾃｨ・ｼｽﾃﾑｽﾞ	ｼｽｺｼｽﾃﾑｽ
ｾｷｭﾘﾃｨ・ﾎｰﾙの検出	NetRecon	Internet Scanner	NetSonar
不正侵入の監視	Intruder Alert	Real Secure	NetRanger
ﾌｧｲｱｳｫｰﾙ	Eagle		PIX Firewall , CentriFirewall
ｾｷｭﾘﾃｨ・ｽｲｰﾄ製品	AXENT product suite	SAFE suite	

製品カテゴリ	ｾｷｭﾘﾃｨ・ﾀﾞｲﾅﾐｯｸｽ・ﾃｸﾉﾛｼﾞｰｽﾞ	ﾈｯﾄﾜｰｸ・ｱｿｼｴｰﾂ	ﾄﾚﾝﾄﾞﾏｲｸﾛ
ｾｷｭﾘﾃｨ・ﾎｰﾙの検出	Kane Security Analyst	Ballista	
不正侵入の監視	Kane Security Monitor	CyberCop	
ﾌｧｲｱｳｫｰﾙ		Gauntlet	*トレンドＶＣＳ
暗号	RSA 暗号	RGP 暗号	
ｾｷｭﾘﾃｨ・ｽｲｰﾄ製品	Secure Sight	NetTools Secure	
ウイルス検知			*トレンドＶＣＳ

参考文献

1) Norman L. Gelbwakns. “AFSCM 375-5 as Methodology for System Engineering” IEEE Transactions on Systems Sience and Cybernetics Vol.SSC.3 No.1 June 1967

2) Simson Garfinke, Gene Spafford, 安藤進（訳）：“Web セキュリティ&コマース”, オライリー・ジャパン（1998－03）

3) 通商産業省：“大規模プラント・ネットワーク・セキュリティについて”, 大規模プラント・ネットワーク・セキュリティ対策委員会（1998－03）

4) Glen Bruce, Rob Dempsey, さとうよしひろ（訳）：“分散コンピューティングセキュリティ”, 株式会社プレンティスホール出版、p 435～p 436、(1998－05)

5) 江畑謙介：“情報テロ”, 日経 BP 社, (1998－05)

6) 日経コンピュータ：“不正侵入はこう防げ”（1998－07）

（平成10年12月14日受理）