

コンピュータセキュリティインシデントと
その対応に関する調査

調査報告書

平成12年3月

情報処理振興事業協会

目 次

1. はじめに	3
2. 目的	3
3. 調査方法	3
4. 調査期間	3
5. インシデントの分類に関する情報.....	4
5.1 侵入	4
5.1.1 侵入の影響	4
5.1.2 侵入の原因	7
5.2 MTA(Mail Transfer Agent)の予期せぬ第三者利用(SPAM Relay).....	9
5.3 メールアドレスの偽造(Forged E-mail Address SPAM)	10
5.4 サービス運用妨害(DoS).....	11
5.5 プローブ/スキャン	12
5.6 その他のサービスの予期せぬ利用	13
6. インシデントの届け出状況	15
6.1 インシデントの報告件数とインシデントの分類	15
6.2 コンピュータセキュリティインシデントの報告におけるハードウェア、OS	19
6.2.1 ハードウェアの分類	19
6.2.2 OS の分類	20
6.3 コンピュータセキュリティインシデントの報告におけるシステムの役割、どのようにして発見したか、連絡前の対処、対応依頼の分類 ...	21
6.3.1 ホストの役割の分類	21
6.3.2 発見の方法の分類	22
6.3.3 連絡前の対処の分類	22
6.3.4 対応依頼の分類	23
7. インシデント対応に関する情報	24
7.1 インシデント対応のメッセージ	24
7.2 インシデント対応において勧めた対策	27
7.2.1 JPCERT/CC の文書	27
7.2.2 他の CSIRT の文書	28
7.2.3 その他の技術文書	28
7.2.4 その他の機関	29

8.	対策に関する情報 (緊急報告、技術メモ)	30
8.1	技術メモ - サービス運用妨害攻撃に対する防衛.....	30
8.2	技術メモ - Web ページの改竄に対する防衛	30
8.3	技術メモ - 関連サイトとの情報交換.....	30
8.4	技術メモ - コンピュータセキュリティインシデントへの対応	31
8.5	緊急報告 - automountd サーバプログラムを悪用したアタック .	31
8.6	緊急報告 - NFS マウントデーモン mountd を悪用したアタック	31
9.	国際関係に関する情報.....	32
9.1	内外の CSIRT との情報交換	32
9.2	技術トピックス	32
9.2.1	FIRST Conference(於:オーストラリア).....	32
9.2.2	Information Security For New Millemium(於:韓国)	37

1. はじめに

本調査は、情報処理振興事業協会から委託を受けて実施した。

2. 目的

日本におけるネットワークに関するコンピュータセキュリティインシデント(以下、「インシデント」)の届出状況、その対応の状況、および関連する対策技術に関する調査を行ない、我が国のコンピュータセキュリティ対策の促進に資する。

3. 調査方法

JPCERT/CC (コンピュータ緊急対応センター)は、届け出されたデータを整理・分類して、届け出状況に関する分析を行った。また、海外に所在するインシデント対応組織との協調関係や各インシデント対応組織の活動状況などに関する調査も併せて行なった。

4. 調査期間

本調査の対象期間は、平成 11 年 4 月から平成 12 年 2 月である。

次章から、以下の順番でそれぞれについて報告する。

- ・ インシデントの分類に関する情報
- ・ インシデントの届け出状況
- ・ インシデント対応に関する情報
- ・ セキュリティ対策に関する情報(緊急報告、技術メモ)
- ・ 国際関係に関する情報

5. インシデントの分類に関する情報

JPCERT/CC に届け出られるインシデントの分類には、大きく分けて以下の 6 つの分類がある。

- (1) 侵入
- (2) MTA(Mail Transfer Agent)の予期せぬ第三者利用(SPAM Relay)
- (3) メールアドレスの偽造(Forged E-mail Address SPAM)
- (4) サービス運用妨害(DoS)
- (5) プローブ/スキャン
- (6) その他のサービスの予期せぬ利用

なお、(5) のプローブ/スキャンは、未遂に終わったインシデント報告であり、それ以外は、インシデントが起こったものに関する報告である。

以下の項では、この 6 つの分類について説明する。

5.1 侵入

侵入(Intusion)とは、アクセス権限を持たない利用者がなんらかの方法でシステムへのアクセスを可能とし、システムが本来サービスとして意図していない形態で利用されてしまうものである。

この定義を敷衍すれば、いわゆる「不正アクセス」はすべて侵入となってしまうが、一般にはシェル(shell)、あるいはコマンドインタプリタ(command interpreter)と呼ばれるコマンド実行の権限を取られた場合を特別に扱い、これだけを侵入と呼ぶ。

侵入には通常のユーザにおけるコマンド実行の権限が取られるだけの場合と、それを含めて管理者権限(root privilege)を取られる場合がある。管理者権限が取られる場合には、システムの書き換えを含めた最大限の悪用がなされる可能性がある。

CSIRT(Computer Security Incident Response Team)のインシデント対応業務において、侵入は、その影響の大きさから他のインシデントと区別される。以下では、侵入の影響とその原因について述べる。

5.1.1 侵入の影響

一旦、侵入を許してしまうと、その影響は単一のホストに留まらず、サイトの内部、あるいは外部へ大きく拡大する恐れがある。一般に、システムおよびネットワークは内部からの攻撃には弱い。このため、通常のユーザの権限の取

得から、ローカルのシステムを悪用して管理者権限の取得、さらに一ホストの管理者権限の取得からネットワーク全体への悪用へとつながることもあり得る。この様子を図 5.1 に示す。

この図のように、侵入は、小さな一点の弱点から、大きな権限の取得に発展し、大きな影響に及ぶことがある。

一般に影響は単一のネットワークだけにおさまらない。侵入が行なわれると、そのホストを踏台として利用し、別のサイトにさらなる侵入が行なわれることが多い。このような悪用が行なわれる時、攻撃を受けるサイトからは、踏台となっているサイトから攻撃を受けていると見えることとなる。

図 5.2 に示すように、HostA から HostB を経由して HostC が攻撃されている場合、HostC からはあたかも HostB にいるユーザが、HostC を攻撃しているように見える。

また、侵入が行なわれると、通常のアクセス制御を迂回してコマンド実行を可能とする裏口(back door)が設置されることがある。この場合、侵入の原因となる問題を解決しても、悪用は続くこととなる。

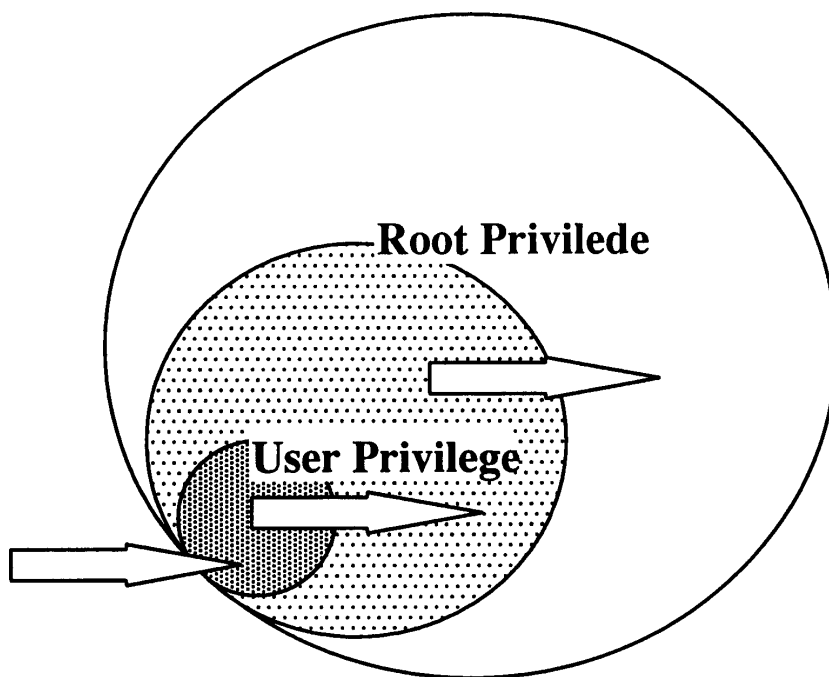


図 5.1: 侵入における権限の広がり

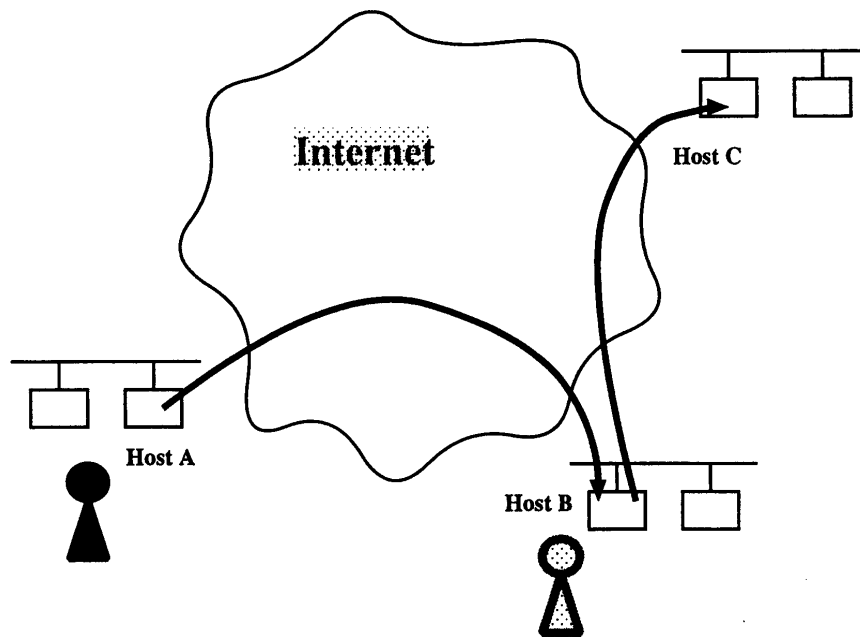


図 5.2: 侵入の連鎖

侵入により管理者権限が取得された場合、システムの改変が行なわれることがある。そしてシステムを改変して、侵入に関連する記録を隠蔽することが行なわれることがある。改変されたシステムで得られる情報はなんらかの形で改竄されていると考えた方がよい。例えば、以下のようなことが考えられる。

- ・ 稼働しているプロセスに関する情報を出力するコマンドが改変され、悪用に関連したプロセスの情報が隠蔽される。
- ・ ユーザに関する情報を出力するコマンドが改変され、悪用を行なっているユーザの情報が隠蔽される。
- ・ ファイルシステムに関する情報を出力するコマンドが改変され、悪用に関連したファイルの存在が隠蔽される。
- ・ ネットワークに関する情報を出力するコマンドが改変され、悪用に関連したネットワークの情報が隠蔽される。

また、システムが改変されている場合、システムの修復作業が思わぬ悪影響をもたらすことがあり得る。例えば、以下のようなことが考えられる。

- ・ パスワード設定のコマンドが改変され、情報を傍受するものと置き換えられてしまった場合、侵入の対処としてパスワード変更を行なうと、パ

スワードの情報を漏洩させてしまう。

- ・ ファイル転送のプログラムが改変され、転送されるファイルを別のホストにも送るものと置き換えられてしまった場合、侵入の対処としてファイルの転送を行なうと、情報の漏洩につながる。

このため、管理者権限が取得された場合には、汚染されていないシステムによって修復作業を行なうことが望まれる。

5. 1. 2 侵入の原因

侵入の原因となるものには、アクセス制御の不徹底など、ネットワーク管理上の問題の他に、OS のセキュリティホール(パスワードが付与されていないアカウント、パスワードが知られている管理用アカウントの存在、不十分な標準設定のために悪用可能なネットワークサービスなど)、ソフトウェアの脆弱性(vulnerability)がある。

これまでにすでに原因が発見され、インシデントの報告がされている脆弱性には、以下のものがある。

- ・ IMAP サーバプログラムの脆弱性

IMAP(Interactive Mail Access Protocol)サーバプログラムはメールを取り扱うソフトウェアであり、ユーザのメールリーダと接続し、ホストに配送されたメールをユーザが読むサービスを提供する。IMAP サーバプログラムのある実装には脆弱性があり、ネットワークを通じて侵入される危険性がある。

- ・ statd サーバの脆弱性

statd(ステイタスデーモン)は、NFS(Network File System)サービスを行なうためのサーバのうちの一つで、mountd(マウントデーモン)、nfsd(NFS デーモン)とともに用いられる。statd のある実装には脆弱性があり、ネットワークを通じて侵入される危険性がある。

- ・ Web サーバの cgi-bin プログラムの脆弱性

Web サーバの cgi-bin プログラムとは CGI(Common Gateway Interface)と呼ばれる Web のサービスの拡張機能で、静的な情報をサービスするのではなく、プログラムによって生成されるデータをサービスする仕組みを提供する。これによって、例えばフォームに基づいてユーザからの入力を受け、結果を返すなど、情報のサービスを構築することができる。システムに標準として(誤って)危険な cgi-bin プログラムがインストールされてしまっていたり、セキュリティを十分に考慮せずに cgi-bin プログラムが実装されると、例え

ば、cgi-bin プログラムからパスワードファイルが漏洩するなど、予期せぬ経路で情報が洩れることがある。そして、それを契機として侵入される危険性がある。

- POP サーバプログラムの脆弱性

POP(Post Office Protocol)サーバプログラムは、IMAP と同様にメールを取り扱うソフトウェアであり、ユーザのメールリーダーと接続し、ホストに配送されたメールをユーザが読むサービスを提供する。POP サーバプログラムのある実装には脆弱性があり、ネットワークを通じて侵入される危険性がある。

調査対象の期間において、新たに発見され、侵入の原因となるようになってきている脆弱性には以下のものがある。

- amd サーバプログラムの脆弱性

amd(auto mount daemon)は、4.4BSD で開発されたファイルシステムのデーモンであり、ユーザの利用に応じてファイルシステムを自動的にマウントする機能を提供する。BSD 系の OS や GNU/Linux システムで利用されることが多い。amd のある実装には脆弱性があり、ネットワークを通じて侵入される危険性がある。

- mountd サーバプログラムの脆弱性

mountd は、NFS(Network File System)サービスを行なうためのサーバのうちの一つで、statd(ステータスデーモン)、nfsd(NFS デーモン)とともに用いられる。GNU/Linux システムで用いられている mountd のある実装には脆弱性があり、ネットワークを通じて侵入される危険性がある。

- automountd サーバプログラムの脆弱性

automountd(auto mount daemon)は、amd と同様にユーザの利用に応じてファイルシステムを自動的にマウントする機能を提供する。Sun Solaris などのシステムで利用される。automountd のある実装には脆弱性があり、ネットワークを通じて侵入される危険性がある。

- RPC(rpc.cmsd, rpc.ttdbserverd, rpc.sadmind)サーバプログラムの脆弱性

RPC(remote procedure call)はネットワークサービスの枠組であり、分散ネットワークシステムのサービスを構築する一つのレイヤである。NFS やデスクトップ環境などの実装に利用される。LAN 環境における利用が前提となることが多い。RPC は広域でのネットワークセキュリティがあまり考慮されない形で運用されることが多く、RPC を利用するサーバプログラムのある実装には脆弱性があり、ネットワークを通じて侵入される危険性がある。

- ・ Web サーバプログラムの脆弱性

Web サーバプログラムは Web のサービスを提供するプログラムである。Web サーバプログラムのある実装には脆弱性があり、ネットワークを通じて侵入される危険性がある。

5.2 MTA(Mail Transfer Agent)の予期せぬ第三者利用(SPAM Relay)

MTA(Mail Transfer Agent)とは、メールの配送を行なうプログラムのことである。本来は無関係の MTA を利用して、電子メールを多くのサイトに効率良く配送するということが行なわれる。これは、UCE(Unsolicited Commercial E-mail)、UBE(Unsolicited Bulk E-mail)、あるいは SPAM と呼ばれる大量の不特定多数へのメールの配送に用いられる。

図 5.3 に第三者利用の中継の様子を示す。もともとの送信者(Original Sender)から中継する MTA(Relay)にメールが送信され、多くの受信先(Recipient)にメールが配送される。

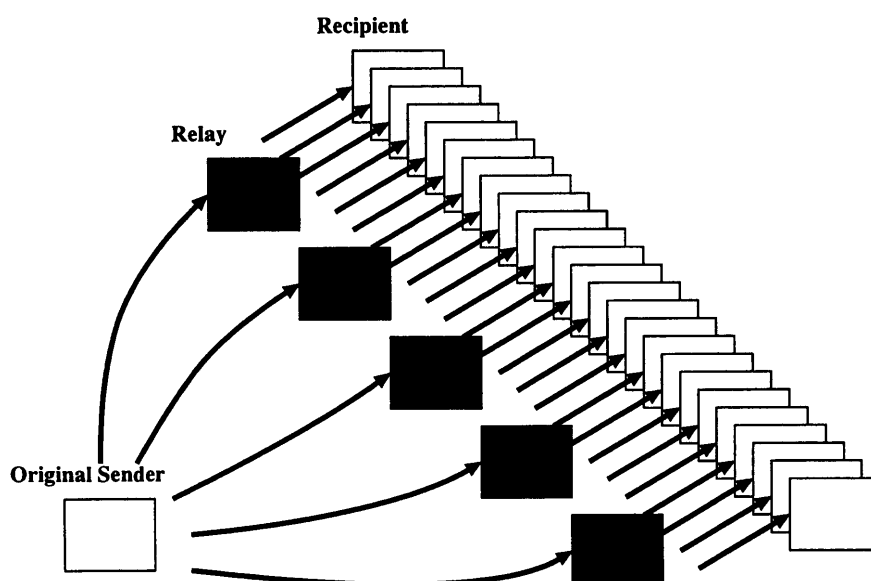


図 5.3: MTA の予期せぬ第三者利用

この配送に MTA が利用される場合、中継しているサイトは不正なメールの発信元であるという疑いをもたれる可能性がある。

このような第三者の利用がなかった時代には、MTA はメッセージの転送を行

なうものとして設計され、また運用されてきた。そして、どのメッセージを配送するのか限定する、接続元の MTA によってその利用範囲を制限するといったアクセス制御には無頓着な部分があった。最近の実装ではアクセス制御の設定により、予期せぬ第三者利用を防ぐことが可能となってきた。しかしながら、多くのサイトが旧来の運用の設定のまま残されており、このインシデントは続いている。

このような仕組みにより、UCE/UBE が配送される場合、中継に利用される MTA は被害者であるという見方もできるが、中継によって配送に加担していると見る向きもある。UCE/UBE を許してしまう運用を改めるといった活動が存在し、第三者の中継を行なう MTA は排斥される可能性が出てきている。このような活動には、RBL(Realtime Blackhole List)、ORBS(Open Relay Blocking System)が有名である。

5.3 メールアドレスの偽造(Forged E-mail Address SPAM)

電子メールの送信ヘッダーを偽造し、メールの配送に関与していないサイトを偽って、大量のメールを配送するということが行なわれる。これは、MTA の第三者利用と同様に UCE あるいは UBE と呼ばれる大量のメールの配送に用いられる。

現在広く利用されているメール配送のプロトコル SMTP(Simple Mail Transfer Protocol)では、メールの送信ヘッダーに関して認証などの仕組みは提供されないため、任意の送信ヘッダーを作り上げることが可能であり、このプロトコルで運用を続ける限り、偽造の問題を避けることはできない。

図 5.4 にアドレスを偽造して配送が行なわれる様子を示す。このようなインシデントの場合、配送できなかったエラーに関してアクセスが来ることになる。

このようなアクセスがあり得ることを想定してネットワークが構成され運用されている場合には、比較的問題は少ない。しかし、メール配送の構成によっては、大量のエラーがサイトの内部で発生することになる。そして、結果としてメールサーバの運用に支障が出ることもある。

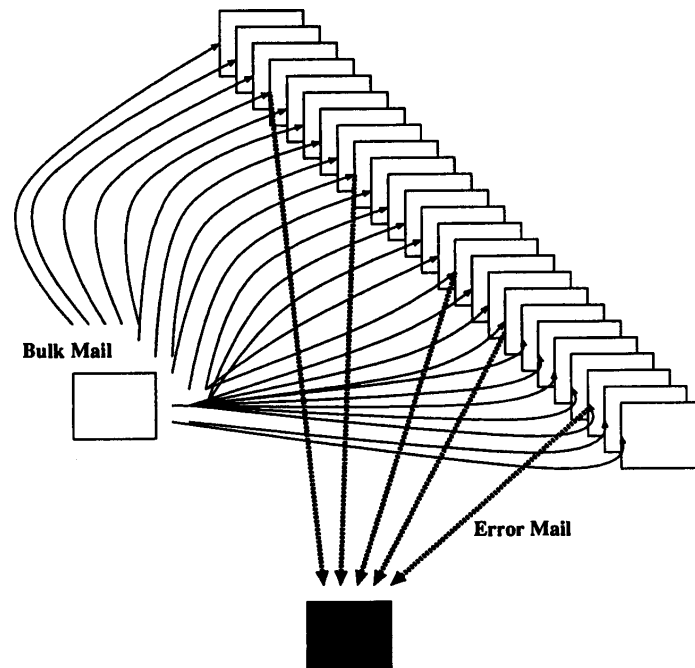


図 5.4: メールアドレスの偽造

5.4 サービス運用妨害(DoS)

サービス運用妨害(DoS, Denial of Service)とは、ネットワークの輻輳や、システムリソースの占有、あるいはシステムのクラッシュによって、運用されているサービスを妨害することである。

DoS には以下にあげるものがある。

- E-mail bomb
- SYN flooding
- Teardrop attack
- Smurf amplifier(UDP, icmp)
- Distributed DoS

このうち、インターネットに典型的な、Smurf amplifier に関して説明する。この攻撃では、複数の中継地点によってパケットが増大され、ネットワークの輻輳が惹起される。

図 5.5 に Smurf amplifier の様子を示す。最初のホスト Originated から(偽造された)ブロードキャストのパケットが各ネットワークに送信される。そして、ブロードキャストに対する返信のパケットが最終的に Victim のホストにすべ

て集中することになり、輻輳がおりサービスの運用が妨害される。

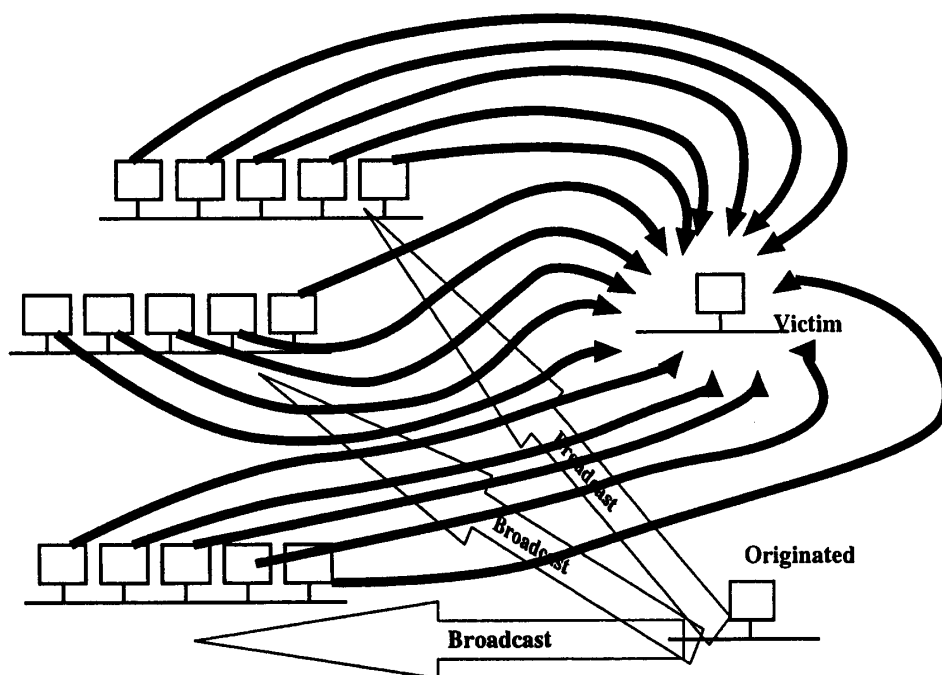


図 5.5: Smurf amplifier によるサービス運用妨害

サービス運用妨害に対しては、これを 100%防ぐことはできないが、より強固にすることはできる。可用性(availability)に関する設計が不十分であるソフトウェアの場合、あるサブシステムの影響が全体に及ぶ、あるいは、可用性に関する設計が不十分であるネットワークの場合、ある一つのホストの影響が全体に及んでしまう。こういった点を改善し、可用性に関して適切な配慮を行なえば、DoS に対して強いシステムとすることができる。

5.5 プローブ/スキャン

ホストあるいはネットワークで運用されているサービスや、それらに含まれるセキュリティ上の弱点の存在をリモートから探査しようとする試みを、プローブ(probe)と呼び、それらがネットワーク上のホストやホスト上のポートに対し走査される場合、これをスキャン(Scan)と呼ぶ。

このような探査は、自動化ツールを用いて大規模かつ無差別的に行なわれることがある。セキュリティ上の弱点を放置して運用を続けていると、弱点の存在を検出され、ホストへの侵入等さまざまなアクセスを受ける可能性がある。

注意が必要なのは、プローブ/スキャンに利用される手法は、従前は単に接続を試みるなどの単純なものだったが、日々進歩を続けてきており、得られる出力や通信の挙動の特性から、利用している OS とサービスを行なうソフトウェアのバージョンの特定を含む探査まで行なわれるようになってきていることである。

探査の空間は、ドメイン名による場合と IP アドレスの場合がある。DNS から情報を取得され、ドメイン名の空間を走査されることを防ぐには、セコンダリ DNS 以外からのゾーン転送を禁止することが有効な対応策となる。

5.6 その他のサービスの予期せぬ利用

その他のサービスの予期せぬ利用には、以下のものがある。

- FTP サービスの予期せぬ利用

FTP によるファイル転送サービスには特定ユーザ向けのものと匿名 (anony-mous) のユーザ向けのものがある。例えば、LAN 環境、あるいは特定のネットワークに限られた利用を前提として FTP サービスの運用を始めたものが、アクセスの制御を行なっていないため、意図していない利用者に利用されてしまうことがある。場合によっては、違法な情報の交換に使われてしまうこともある。原因には、ネットワークサービスとしてのアクセス制御の不徹底、FTP サービスとしてのディレクトリのパーミッションの設定の不備、匿名 (anonymous) FTP サービスの設定の不備などがある。

- Web Proxy サービスの予期せぬ利用

Web Proxy サービスは、インターネットへの Web のアクセスを中継するサービスであり、例えば、内部と外部を分けたネットワークの運用に良く用いられる。自分のサイトの利用のみの利用を前提としてサービスを始めたものが、アクセスの制御を行なっていないため、意図していない利用者に利用されてしまうことがある。

これは、Web サービスを行なっている側からは、アクセスはあたかも Proxy サービスを行なっているサイトから来るように見えるので、アクセス元を隠蔽するために利用されることがある。場合によっては、ディスクやネットワークの帯域などの資源を大量に消費される。

原因には、ネットワークサービスとしてのアクセス制御の不徹底、Proxy サービスとしての設定の不備などがある。

- Web サービスの予期せぬ利用 (情報漏洩、情報書き換え)

侵入の節でも cgi-bin プログラムの脆弱性として述べたが、Web サービス

が予期せぬ利用をされ、情報漏洩、情報書き換えが起こることがある。
原因としては、システムの標準設定をセキュリティの評価なしに導入した結果、外部からのアクセスを意図していない情報が取得されるなど、設定の不徹底、cgi-bin プログラムなど拡張の仕組みの利用において、セキュリティを弱める利用を行なってしまうなどがある。
特に、掲示版などのプログラムには、予期せぬ利用を許してしまうものが多い。

6. インシデントの届け出状況

本節では、JPCERT/CC へのインシデント届け出状況について述べる。

なお、以降の数値は JPCERT/CC へ届け出られた情報であり、データの偏りや網羅性も充足していないと考えられるため、実際のインシデントの発生状況をこれらのデータから考察することは、現実的ではない。よって、各データの分布などに関する考察は、JPCERT/CC へ届け出られた情報の客観的な数値の分布状況などを述べることとする。

6.1 インシデントの報告件数とインシデントの分類

インシデントの報告の報告件数と分類を表 6.1 に示す。ここで括弧内は、報告様式にしていなかったがインシデントとして処理されたものである。

表 6.1: インシデントの報告件数とその分類

	総数	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	JAN	FEB
侵入	91 (9)	15	6 (2)	6 (1)	8	9	7 (1)	6 (1)	8	7 (1)	7 (1)	12 (2)
中継	68 (3)	7 (1)	6	5	5	5	5	1 (1)	8	5	13 (1)	8
偽造	37 (7)	2 (1)	3	2 (1)	2 (1)	1	5 (1)	5	3 (2)	2 (1)	6	6
DoS	22 (6)	2	(1)	3 (1)	5 (2)	2 (1)	1 (1)		1	1	4	3
悪用	13 (8)	1 (2)	4 (1)	2	1	(1)	(1)	3	1	(1)	1 (1)	1 (1)
プローブ/ スキャン	285 (22)	48 (5)	35 (5)	33	34 (2)	23	18	13 (1)	25	6	25 (4)	25 (5)
その他	17 (22)	2 (3)	4 (3)	(1)	(5)	(1)	3 (2)	1 (3)	1	4	1 (3)	1 (1)
計	533 (77)	77 (12)	58 (12)	51 (4)	55 (10)	43 (3)	37 (6)	28 (6)	47 (2)	25 (3)	57 (10)	55 (9)

件数の推移をグラフにしたものを、図 6.1 に示す。また、総数の割合を円グラフにしたものを、図 6.2 に示す。

なお、プローブ/スキャンは他の報告とは違う性格を持っていることが、報告件数の傾向から推測することができる。届け出状況を分析すると、他のインシデントと異なり、報告者の「忙しさ」の影響が大きく現れるインシデントであると考えられる。すなわち、報告者の時間的余裕がある時期には報告が集まるが、それ以外は集まりにくいという特殊性であり、顕著な例は、12月に現れて

いる。

この月に、プローブ/スキャンが極端に少なくなっているのは、Y2K 問題対応による関係各方面における業務負荷の増加があったためと考えられる。

プローブ/スキャンとその他の分類を除いて、その増減を見ると、4 月より若干減ってきて、それから安定し、1 月、2 月と増えているという傾向になっている。

また、報告様式に準拠せずに届けられるインシデントには、CSIRT として取扱の対象ではないもの（例えば、行為者の特定についての要望等）が多く含まれている。

セキュリティインシデントは、悪意に基づく行為によってのみ起こるのではないし、行為者を特定し、追い詰めるという対応は、多くの場合望ましい結果をもたらさないものだが、そのような捜査や犯人追求という姿勢に陥ることが多くあり、これらの捜査や犯人の追求を CSIRT に依頼することが時々見られる。

よりよい結果を得るためには、捜査や犯人追求といった姿勢で事象に望むのではなく(このことが優先する場合は、司法機関への相談が有効)、再発の防止を優先し、技術的な事象の特定や影響を受けたシステムの復旧など、事後対策に注力することの方が有用である。

一方、昨年法律制定などの影響から「不正アクセス = 侵入」ととらえ、インシデントを「侵入行為」だけと考える面も見られるようである。実際に侵入される行為以外にも、システム運用者の意図しない利用や、予定外のサービスの停止など、インシデントにはいろいろな行為パターンがあることを、理解しておく必要がある。

また、管理者と利用者とのコミュニケーションの問題もいくつか見られる。ネットワークの運用においては、インシデントに関して、管理者と利用者の連絡/問い合わせを円滑に行なうような体制を整えておくことが望ましい。

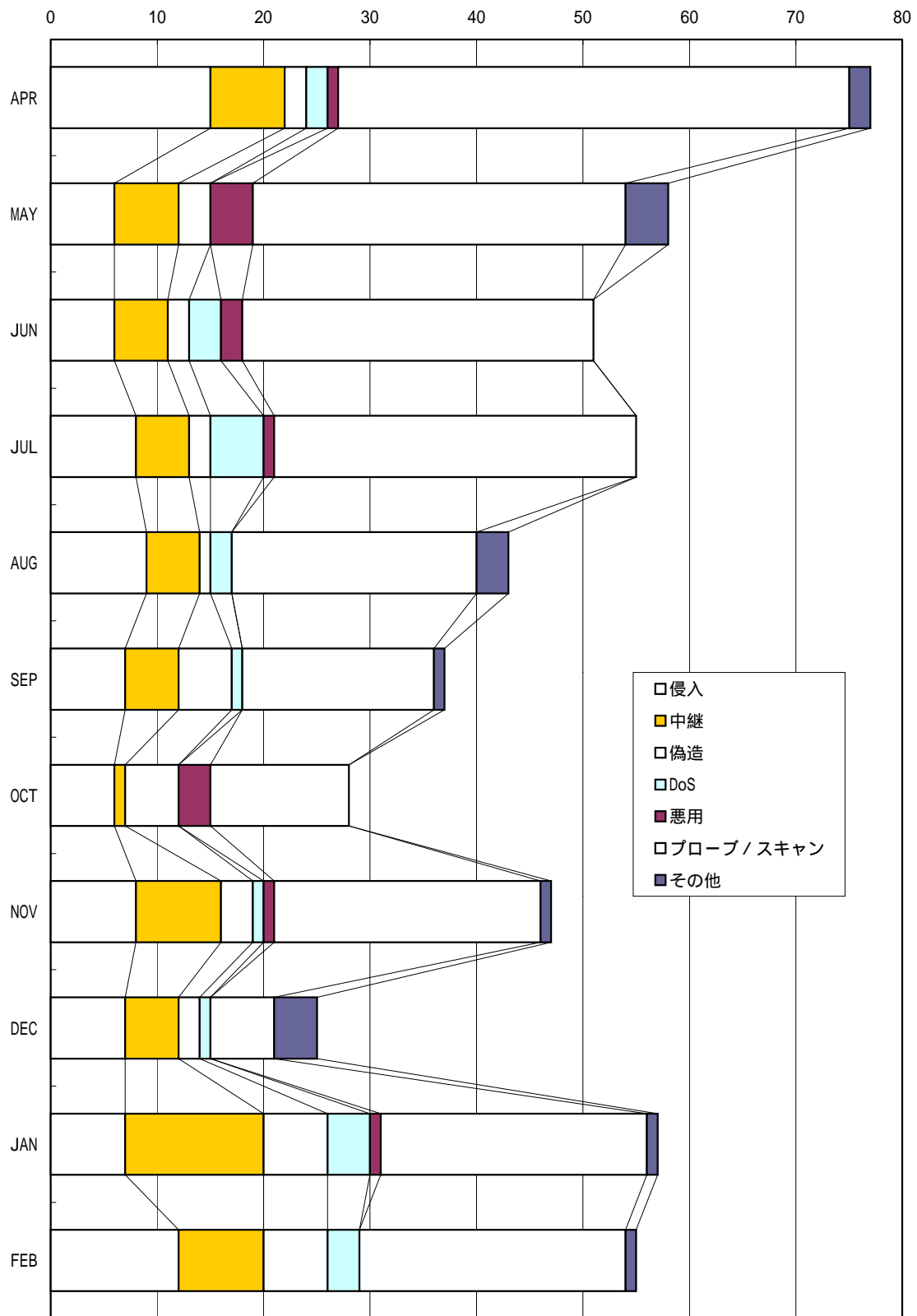


図 6.1: インシデントの報告件数とその分類(1)

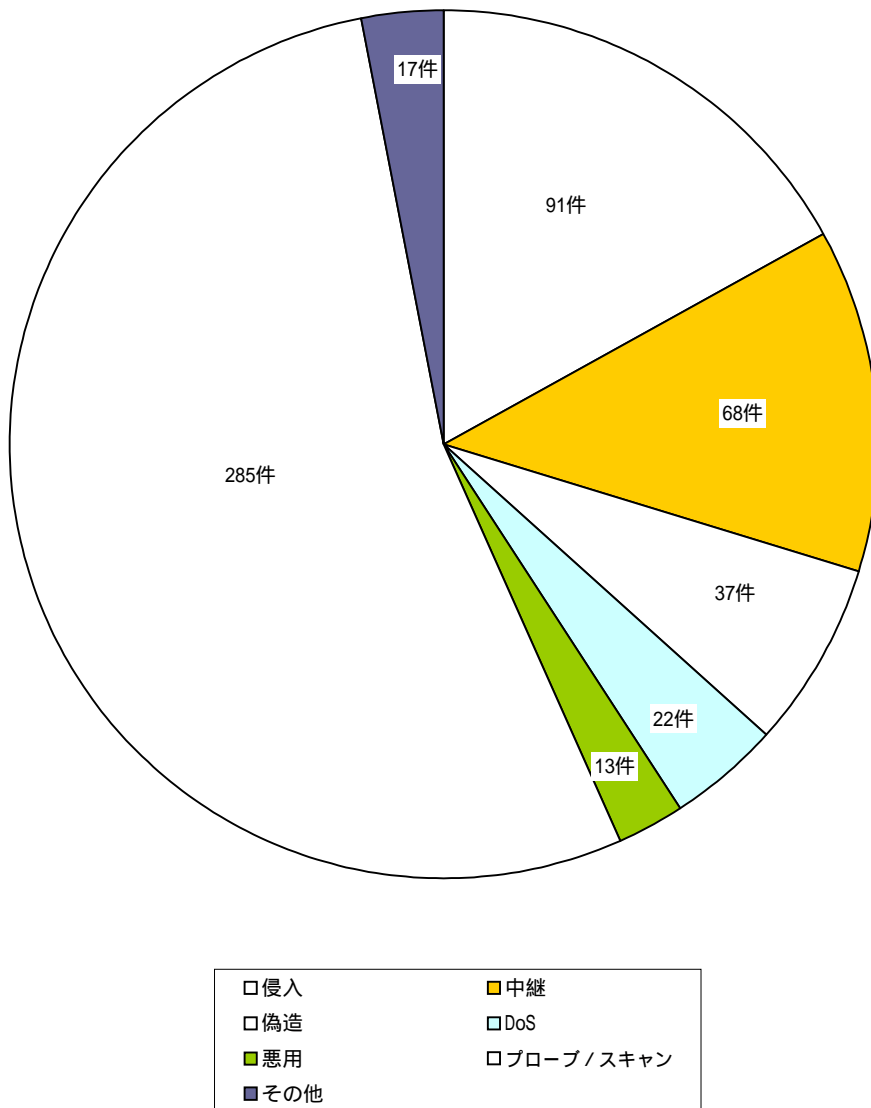


図 6.2: インシデントの報告件数とその分類(2)

6.2 コンピュータセキュリティインシデントの報告におけるハードウェア、OS

インシデント報告におけるハードウェアとOSに関して述べる。

インシデント報告において、OSとハードウェアに関する記述があり、この分類の対象となる報告件数とマシンの数を表6.2に示す。一つの報告に複数のマシンが記述されることがあるためマシンの数は対象となる報告の数よりも多い。

表6.2: 対象となる報告件数とマシンの数

	総数	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	JAN	FEB
報告件数	199	25	15	15	16	14	15	13	19	12	28	27
マシンの数	243	33	16	16	16	14	19	15	22	12	42	39

単一のホストだけでなくネットワーク全体がインシデントの対象になった場合などはマシンの数が増える。

傾向としては、全体のインシデントと同様に、4月より若干減ってきて、それから安定し、1月、2月と増えているという状況になっている。1月、2月は影響の大きなインシデントが増えていると考えられる。

6.2.1 ハードウェアの分類

ハードウェアの分類について表6.3に示す。

表6.3: ハードウェア

種類	総数	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	JAN	FEB
PC	120	12	6	7	7	11	11	10	11	5	25	15
WS	113											
Sun	101	18	6	6	6	1	7	5	9	4	16	23
HP	5		4	1								
SGI	3	2			1							
NeXT	1								1			
Rs/6000	1	1										
DEC	2							1			1	
Macintosh	8			1	1	2			1	2	1	
ルータなど	3			1	1							1

6.2.2 OS の分類

OS の分類について表 6.4 に示す。

表 6.4:OS の種類

	総数	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	JAN	FEB
Solaris2	84	17	5	3	5		6	5	7	3	12	21
Linux	106	10	3	5		8	5	6	6	4	2	4
FreeBSD	31	1	2	2	4		3	2	3		10	4
WindowsNT	27	1	1		2	3	2	1	3	2	6	6
SunOS4	11	1		2	1	1	1				3	2
MacOS	7			1		2			1	2	1	
HP-UX	5		4	1								
BsD/os	3						1	1			1	
IRIX	3	2			1							
Windows98	2				1						1	
DigitalUNIX	1						1					
AIX	1	1										
NeXTSTEP	1								1			
MkLinux	1				1							
該当なし	3			1	1							1
不明	11		1	1					1	1	6	1

6.3 コンピュータセキュリティインシデントの報告におけるシステムの役割、どのよう

にして発見したか、連絡前の対処、対応依頼の分類

インシデント報告における、システムの役割、どのようにして発見したか、連絡前の対処、および対応依頼の分類に関して述べる。

記述があって対象となる報告の件数を表 6.5 に示す。

表 6.5:対象となる報告件数

	総数	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	JAN	FEB
報告件数	231	27	19	18	21	17	18	15	21	15	31	29

傾向としては、全体のインシデントと同様に、4月より若干減ってきて、それから安定し、1月、2月と増えているという状況になっている。

以下、それぞれの分類について述べる。

6.3.1 ホストの役割の分類

ホストの役割の分類について表 6.6 に示す。ここで、ホストの役割の分類複数回答があるので合計は報告件数よりも多い。

表 6.6:ホストの役割

	総数	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	JAN	FEB
Mail	146	19	12	13	9	11	12	10	13	10	21	16
Web	96	12	12	6	7	5	8	4	5	11	11	16
DNS	72	11	7	8	3	4	7	5	7	5	8	7
FTP	48	6	3	4	6	4	5	3	2	4	4	7
Proxy	11	1	0	1	0	1	0	3	2	0	1	2
FW	9	1	0	0	0	2	1	1	2	1	0	1
POP	5	1	2	1	0	0	0	0	1	0	0	0
Other	32	5	2	4	5	1	1	0	4	1	6	3

ここで、メールサーバが多いが、メールサーバがすなわち危険ということではない。役割と危険性に何らかの相関があるということはいえない。

6.3.2 発見の方法の分類

発見の方法の分類について表 6.7 に示す。ここで、「保守作業で」、「外部から」、「サービス停止」の3つの分類がある。

「保守作業で」というのは、保守作業の一貫においてログを見て発見したり、監視していて発見するという分類である。

「外部から」というのは、外部のユーザあるいは管理者などからの連絡により発見するという分類である。

「サービス停止」というのは、サービスが停止したことにより、発見するという分類である。

表 6.7: 発見の方法

	総数	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	JAN	FEB
保守作業で	132	11	11	9	9	7	13	9	15	7	21	20
外部から	53	7	5	6	4	6	3	3	4	6	5	4
サービス停止	36	8	1	2	7	4	1	3	2	1	4	3

保守作業でわかる場合が多く半数以上を占めるが、外部からの連絡でわかる場合も多いと言える。

6.3.3 連絡前の対処の分類

連絡前の対処の分類について表 6.8 に示す。ここで複数回答があるので合計は報告件数よりも多い。

分類には、「復旧」、「修正」、「停止」、「制御」、および「連絡」がある。

「復旧」は、インシデントの発生からシステムを復旧し、通常の運用に復旧したことを示す分類である。

「修正」は、インシデントの発生の原因を特定し、修正を行なったことを示す分類である。

「停止」は、システムあるいはサービスを停止しているという分類である。

「制御」は、アクセス制御によりサービスの対象を限定しているという分類である。

「連絡」は、関連サイトに連絡を行なっているという分類である。

表 6.8: 連絡前の対処

	総数	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	JAN	FEB
復旧	105	16	8	12	8	9	7	4	9	4	15	13
修正	56	3	7	6	3	7	3	3	8	0	10	6
停止	53	9	0	2	4	4	4	2	7	5	4	12
制御	50	2	6	4	7	2	5	4	4	2	10	4
連絡	13	0	3	1	1	1	2	1	1	1	2	0

何らかの対処を行なっている場合が多いが、問題を特定し修正を行なうというのはできていない場合が多い。また、関連サイトに連絡を行なうことはあまり行なわれていないことがわかる。インシデントの広がりを防ぐためには関連サイトに連絡を行なうことが望ましい。

6.3.4 対応依頼の分類

対応依頼の分類について表 6.9 に示す。ここで複数回答があるので合計は報告件数よりも多い。

分類には、「連絡」、「質問」、「支援」、「情報」、および「FYI」がある。

「連絡」は、CSIRT から「関連サイトに連絡して欲しい」という依頼である。

「質問」は、インシデントに関する質問に答えて欲しいという依頼である。

「支援」は、インシデントの対応の支援の依頼である。

「情報」は、インシデントに関する情報を教えて欲しいという依頼である。

「FYI」は、依頼ではなく、CSIRT に対する情報提供である。

表 6.9: 対応依頼

	総数	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	JAN	FEB
連絡	102	11	9	6	6	10	9	12	11	9	10	9
質問	79	9	5	6	7	6	6	5	7	4	12	12
支援	77	8	5	8	9	8	5	5	8	6	6	9
情報	51	4	2	2	3	2	4	4	6	5	8	11
FYI	39	4	2	2	4	3	2	2	3	5	8	4

7. インシデント対応に関する情報

本節では、インシデント対応に関する情報について述べる。

7.1 インシデント対応のメッセージ

インシデント対応に関するメッセージのやりとりの数を以下に示す(これには、海外とのやりとりは含まれていない)。

表 7.1 にインシデント対応に関するメッセージの分類を示す。

表 7.1: インシデント対応に関するメッセージの分類

分類	方向	説明
RP	CSIRT 外	Report(報告)
NR	CSIRT 外	Not Report but a Incident(RPではないがインシデント))
NT	CSIRT 外	Notify(連絡派生通知)
QT	CSIRT 外	Question(問い合わせ(広報以外))
AT	CSIRT 外	After that(その後,先方から来たメールの数)
OG	CSIRT 外	Outgoing(先方に対する返事)

ここで、RP(Report)は、報告である。NR は(not Report)報告様式にしたがってないため、RP に分類できないがインシデントとして対応されたものである。NT(Notify)は、CSIRT から出された連絡派生通知である。QT(Question)は、CSIRT に対する問い合わせである。AT(After that)は、先方から来た 2 通め以降のメールである。OG(Outgoing)は、CSIRT から出される返答である。

表 7.1 の分類によるインシデント対応に関するメッセージの数を表 7.2 に示す。

表 7.2: インシデント対応に関するメッセージの数

総数	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	JAN	FEB
RP 533	77	58	51	55	43	37	28	47	25	57	55
NR 77	12	12	4	10	3	6	6	2	3	10	9
NT 284	27	17	16	19	33	20	19	68	5	31	29
QT 62	4	5	2	2	9	4	4	4	4	9	15
AT 1164	123	364	69	91	90	40	43	72	52	98	122
OG 2268	350	235	165	190	174	148	147	185	138	270	266

件数の推移をグラフにしたものを、図 7.1 に示す。また、総数の割合を円グラフにしたものを、図 7.2 に示す。

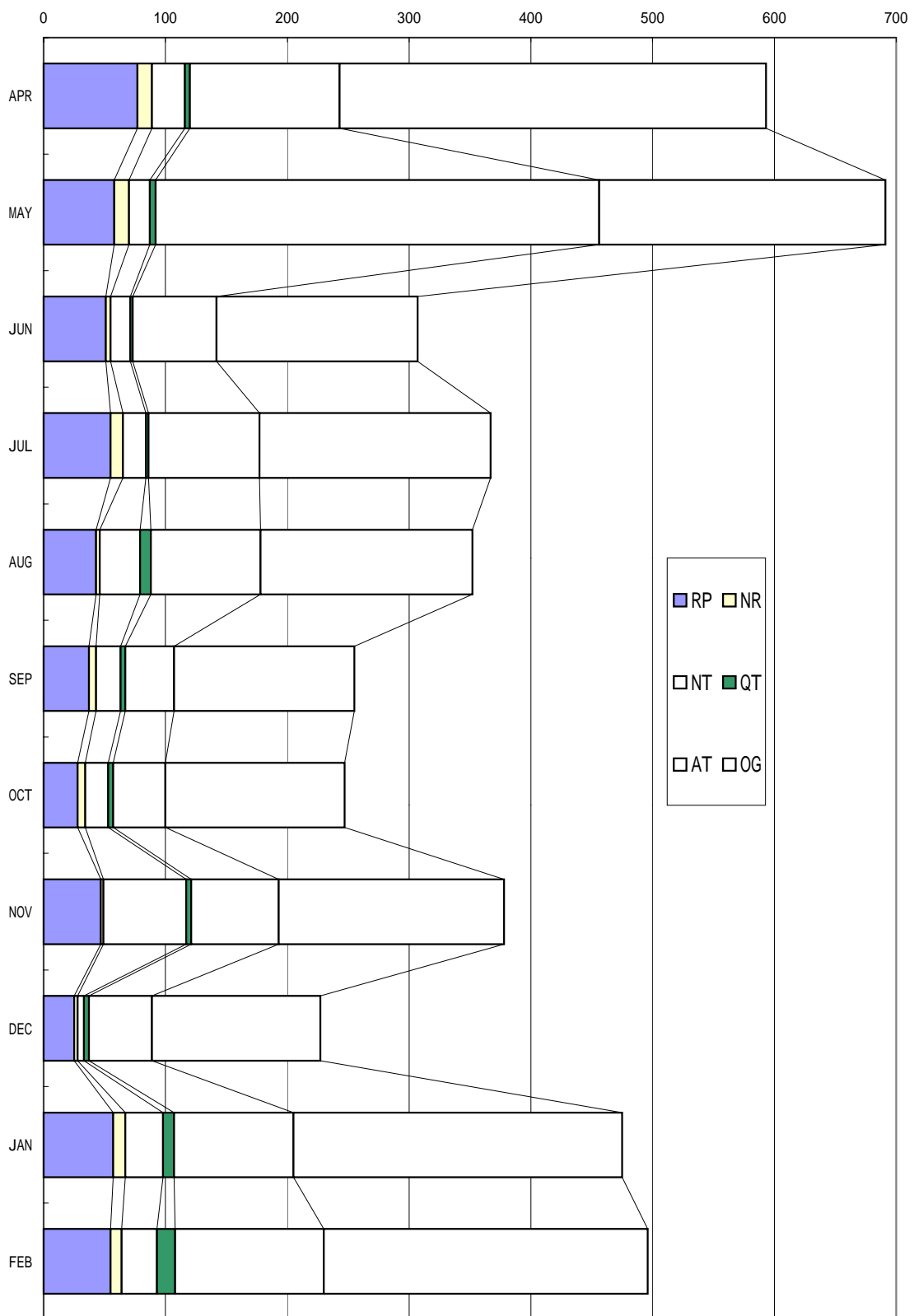


図 7.1: インシデント対応に関するメッセージの数(1)

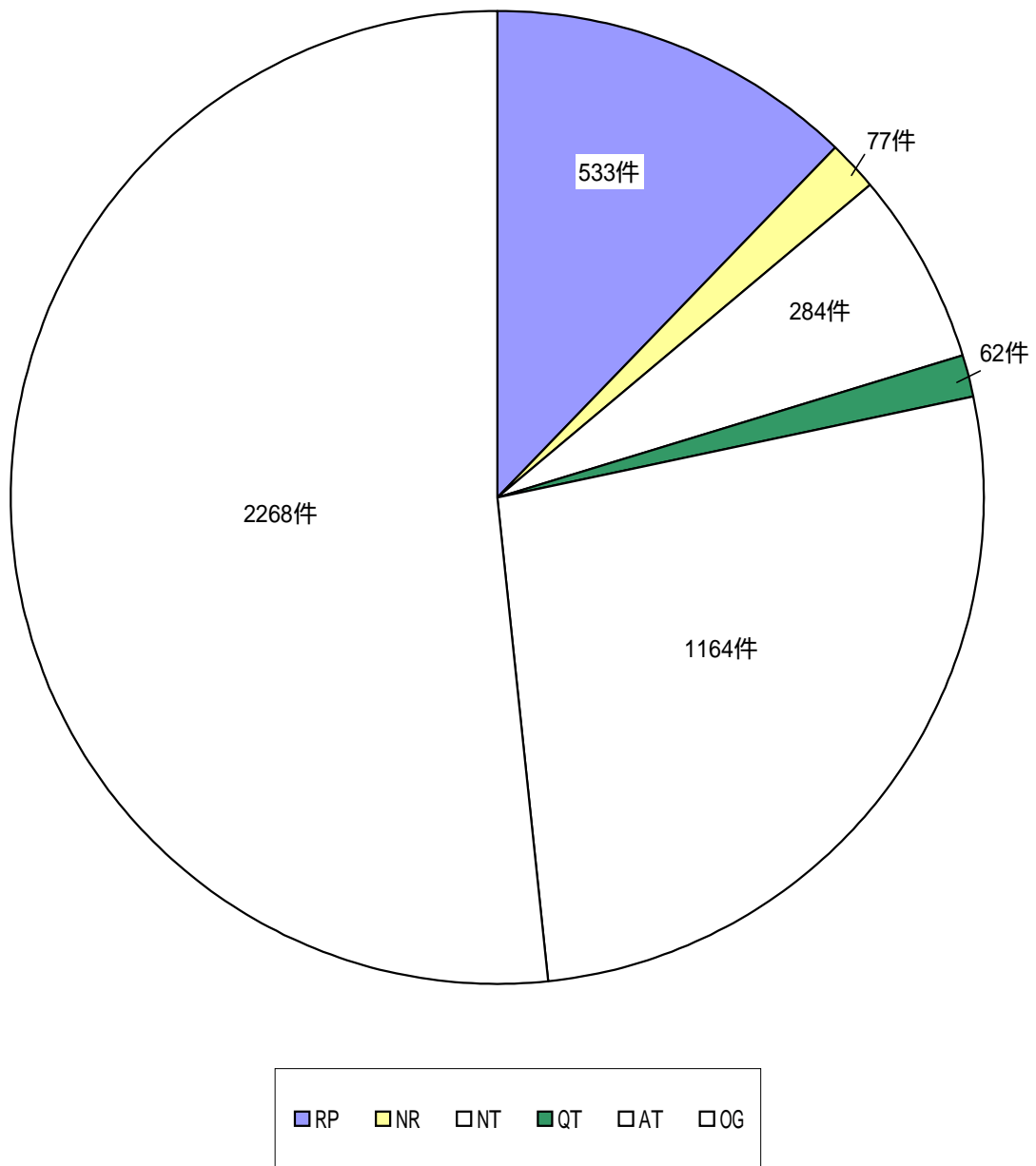


図 7.2: インシデント対応に関するメッセージの数(2)

7.2 インシデント対応において勧めた対策

インシデント対応において勧めた対策の集計を表 5.3 に示す。

表 7.3 JPCERT/CC の文書

JPCERT/CCの文書	1127
他のCSIRTの文書	811
その他の技術文書	256
その他の機関の紹介	245
計	2439

7.2.1 JPCERT/CC の文書

インシデント対応において勧めた対策のうち JPCERT/CC の文書に関して表 7.4 に示す。ここで「at」とあるのは緊急報告、「tec」は技術メモ、「beginners」は初心者向けの技術文書である。

表 7.4: JPCERT/CC の文書

	総数	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	JAN	FEB
at-97-0003	45	12	8	3	4	5		6	3	3		1
at-97-0004	47	14	7	3	4	4		7	5	2		1
at-98-0001	54	23	6	4	5	2	1	8	3	2		
at-98-0002	44	15	7	3	4	4		6	3	2		
at-98-0003	49	12	10	5	4	5		6	3	2	1	1
at-98-0004	19	7	2	3	2		1	1	1			2
at-99-0001	55	27	8	4	1	5		6	3	1		
at-99-0002	48	29	5	7	3	1	1	2				
tec-97-0001	73	13	2	9	7	1	8	5	6	8	7	7
tec-98-0001	54	12	2	8	5	1	5	2	3	6	5	5
tec-99-0001	287								6	19	125	137
tec-99-0002	272									22	131	119
beginners	16	1	5	2	2	1	2	1			2	
その他	64	23	5		1	5	5	2	5	9	2	7

7.2.2 他の CSIRT の文書

インシデント対応において勧めた対策のうち他の CSIRT の文書に関して表 7.5 に示す。

ここで、CA は Cert Advisory, Bulletins は CERT Bulletins, SIM は Security Incident Module である。その他の文書については、7.2.5 節を参照のこと。

表 7.5:他の CSIRT の文書

	総数	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	JAN	FEB
CERT	124											
CA-96.21	5				2	3						
CA-98.01	10	2	1	1	2	2					1	1
CA-98.12	24	20	3						1			
CA-99.08	9				4	1	1	3				
CA-others	76	10	10	5	3	14	6	5	3	11	2	7
Bulletins	30	5	2		2	9		2	2	3	2	3
SIM	26	1	4	1	2	4		2	10	1	1	
IN	12	4	7								1	
techtips	12	2	5			3						1
Summaries	8		2							6		
侵入検知	162	39	21	12	13	14	5	15	28	13	2	
権限詐取	149	28	22	11	13	14	5	13	28	13	2	
CIAC	146	27	21	10	13	14	5	13	28	13	2	
UNIX設定	72	12	10	6	5	10		6	6	10	6	1
Security	70	12	10	4	5	10		6	6	10	6	1

7.2.3 その他の技術文書

インシデント対応において勧めた対策のうち、その他の技術文書文書に関して表 7.6 に示す。7.2.5 節を参照のこと。

表 7.6:その他の技術文書

	総数	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	JAN	FEB
Relay Check	58	11	2	8	5	1	5	3	3	7	7	6
Antispam	52	10	2	8	5	1	5	2	3	6	5	5
SunSOLVE	44	26		4			5	3	2		1	3
TCP-wrapper	22	9	6	3	2	2						
Microsoft	22		1	1	1	11		2				6
SGI	10	2	5		1		2					
Linux Mountd	9	9										
RedHat	8	2				3	1	2				
Resonate	7			6	1							
RBL	8	1						3		2	2	
RFC	6	2	1	1	1						1	
WWW security	5			3	1			1				
ORBS	5	1						3		1		

7.2.4 その他の機関

インシデント対応において勧めた対策のうち、その他の機関の紹介文書に関して表 7.7 に示す。

表 7.7: その他の機関の紹介

	総数	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	JAN	FEB
IPA(セキュリティセンター)	19	6	1	2		1	1	1	2	3	2	
JPNIC	7			1			1	4	1			
日弁連	36	4	3	1	3	5	3	1		1	3	12
日本消費者協会	34		2		1	2	7	4		1	6	11
法律相談	25	4	3	1	3	5	3	1		1	3	1
国民生活センター	23		1		1	3	3			1	3	11
警察	14			1		1						11
その他	87	4	18	10	2	3	19	6	10	5	2	8

8. 対策に関する情報 (緊急報告、技術メモ)

本節では、セキュリティ対策に関する情報(緊急報告、技術メモ)について述べる。

対象期間において、以下の4つの技術メモ、および2つの緊急報告が発行された。

- ・ 技術メモ - サービス運用妨害攻撃に対する防衛
- ・ 技術メモ - Web ページの改竄に対する防衛
- ・ 技術メモ - 関連サイトとの情報交換
- ・ 技術メモ - インシデントへの対応
- ・ 緊急報告 - automountd サーバプログラムを悪用したアタック
- ・ 緊急報告 - NFS マウントデーモン mountd を悪用したアタック

それぞれについて以下で簡単に解説する。

8.1 技術メモ - サービス運用妨害攻撃に対する防衛

サービス運用妨害について解説し、どのようなサービス運用妨害攻撃があるか、それに対してどのような防衛が考えられるか、インシデントが発生した時にはどのように対処したら良いかを解説した文書である。

8.2 技術メモ - Web ページの改竄に対する防衛

Web ページの改竄について解説し、どのようにして Web ページの改竄が起こるか、それに対してどのような防衛が考えられるか、インシデントが発生した時にはどのように対処したら良いかを解説した文書である。

8.3 技術メモ - 関連サイトとの情報交換

インシデントが発生した時には、その拡大を防ぎ、影響範囲を小さくするために、関連サイトと連絡を取ることが望ましい。

サイトのネットワーク管理者がインシデントの発生に際して、どのように関

連サイトと連絡を取ったらいいか、その際に気をつける点はなにかを具体的に解説した文書である。

8.4 技術メモ – コンピュータセキュリティインシデントへの対応

コンピュータセキュリティインシデントについて解説し、インシデントが起こった時の対応を具体的な手順、チェックリストともに解説した文書である。

8.5 緊急報告 – automountd サーバプログラムを悪用したアタック

So1aris2 のシステムで用いられる automountd サーバプログラムの脆弱性を突く攻撃について解説した文書である。

8.6 緊急報告 – NFS マウントデーモン mountd を悪用したアタック

GNU/Linux システムで用いられる NFS マウントデーモン mountd の脆弱性を突く攻撃について解説した文書である。

9. 国際関係に関する情報

本節では、国際関係に関する情報について述べる。

9.1 内外の CSIRT との情報交換

調査の対象の機関では、国内には JPCERT/CC 以外の CSIRT がなかった。このため、国内 IRT との情報交換件数は 0 である。

海外組織との情報交換件数を表 9.1 に示す。

表 9.1: 海外組織との情報交換件数

	総数	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	JAN	FEB
海外から	288	30	14	11	22	37	23	19	22	16	59	35
海外へ	95	29	9	7	7	15	1	5	8	6	3	5

情報交換をした CSIRT について、表 9.2 に示す。

表 9.2: 海外の CSIRT

CSIRTの名称	国あるいは地域
CIAC	米国エネルギー省
AusCERT	オーストラリア
CERT/CC	米国
CERTCC-KR	韓国
CERTRENATER	フランス
DFNCERT	ドイツ
JANET	イギリス
DoD-CERT	米国国防総省
CERT-NL	オランダ

9.2 技術トピックス

9.2.1 FIRST Conference(於:オーストラリア)

第 11 回 FIRST(Forum of Incident Response and Security Teams)の Annual Conference が 1999 年 6 月 13 日から 6 月 18 日の期間でオーストラリアで行なわれた。

Y2K 問題やネットワークに影響を与えるウィルスなど多岐に渡る議論が行な

われた。

- Black Hats Session

ソフトウェアの脆弱性や攻撃/侵入のための技術やツールについての調査を行っているグループがいくつかあり、このチュートリアルの講師もそのような活動を行っている技術者の一人である。脆弱性や攻撃方法についての知識を得ることにより身を守るとというのが彼らのスタンスである。したがって、チュートリアルの内容も攻撃の方法や侵入の仕組み、攻撃のためのツールの紹介にまで至っていた。また、最後に攻撃のデモンストレーションも行ったが、NFSを使った改竄/侵入のデモンストレーションが失敗に終わり、会場に助けを求める場面もあった。

- Computer Forensics (Advanced Tutorial Track)

オーストラリアにおける Computer Forensic の概論。残念ながら CSIRT の業務には直接関係しないが、Law Enforcement の側にも、Law Enforcement の立ち入り捜査を受ける被攻撃サイトにも有益な議論であると思われる。

- Forensic Computing Tools

Forensic用のツールについて、ノウハウの紹介。データの replication, ex-amination, integrity, recovery 用の各ツール、暗号関連ツール、システム分析用のツール等、市販の製品で不十分なものは開発している。

- Moment of Truth: The admissibility and Weight of Computer Forensic Evidence in the Australian Legal System

Computer Forensic に関する概説と case、問題点の紹介。

- Intrusion Investigation and Post-Intrusion Computer Forensic Analysis

Computer Forensic の実際の作業と留意点について。

- Computer Virus Operation and New Directions

会場の都合により短縮され、CIAC のマテリアル(昨年と同内容と思われる)を元にウィルスに関する概論が展開された。

- Will the real owner of this IP address please stand up?

このチュートリアルではログ等からドメイン名や IP アドレスを抽出し、そこから適切な連絡先を調べる方法の説明が行われた。ログ等に記録された情報の見方や信憑性、得られた情報から適切なコンタクト先を探す方法 (<http://www.cert.org/te> 等)等の技術的な話の他にも移動体通信や TLD の売買により適切なコンタクト先の特定が難しくなっているという話もあっ

た。

前半は昨年のセッションと同内容と思われる。IP address spoofing 等までは解説が及ばなかったようだ。

- KeynoteAddress

Prof. William Caeli (Queensland University of Technology) による講演。セキュリティ対策を施された製品が普及するか、そうでない製品がさらに急速に出回るか、現在は岐路に立っている。前者に向けて CERTs/FIRST コミュニティの役割が重要であり、実際にはロビー活動を行なっていく必要もある、という内容。

- CSIRT Foundation: gaining and operation "Trust"

- Teams in Asian/pacific Area (パネル)

Maritn Coe (SingCERT) による APSIRC と各チーム (含 SingCERT) の概説、Chaeho Lim (CERT-CC/KR) による CERT-CC/KR の概説、鈴木裕信氏による JPCERT/CC の概説。SingCERT でも default のままの Linux 等が問題になっているらしい。

- Setting up a Policy Certification Authority

SURFnet PCA, DFN-PCA による PCA 設立に関する概説。PCA の概要、PCA に対する requirement、ポリシーの必要性、ランニングコスト等。パブリックサービスの運営上参考になる点も多いと思われる。

- Vulnerability Prevention and Insurance

- Assessing Network Security for Insurability

保険のためのセキュリティ評価基準についての話。保険の対象はダウンタイムであるため、denial of service と system compromise は同等に評価すべきである、といった内容。

- On the Management of Secure Gateways

ゲートウェイ (ルータ/ファイアウォール?) の運用のアウトソースを請け負っている業者からの発表。リスク等々について顧客に如何に伝えていくか等、顧客との関係をどうしていくかという話。実践に基く知見の紹介。

- Bugs per Amount of Code

プログラムに含まれるバグをどのように減らしていくか、あるいは減っていくかという話は従来からある。この発表では、見る角度を変えて「このくらいのコードならこのくらいのバグが含まれている」という話であった。基準として、ステップ数だけでなく種類 (カーネル、ライブラリ、アプリケーション等) や新しいコードの含有率等も挙げ、バグの量の評

価を行っていた。

- A Case Study in Incident and Vulnerability Handling Coordination
 - Bind Activity
Jeff carpenter(CERT/CC)による。BIND のセキュリティホールを例に 1998 年の 3 ~ 6 月に CERT/CC が行った vulnerability handling の過程が紹介された。一般向けのプレゼンテーションなので、バッファオーバフローの説明などもあり、どのようなことが起こり、どのような対応をしたかという話が週単位で進められた。

- BoF session BoF として 5 つのテーマが用意された。
 - (A1)FIRST's role in the International Infrastructure Issues for Global Incident Response
 - (A2)Voice over IP-Security Issues and Concerns
 - (A3)Robert's Rules of Order
 - (B1)Norms for Disclosure Scheduling and Credit in Advisories
 - (B2)FIRST Pre-conference follow-up meeting

- Vulnerability Handling
 - Vulnerability Assesment Using SAINT
アウトソースを受けたネットワークに対し、SAINT を使って assesment を行ない、セキュリティ対策状況の改善を行なっていくという話。実践に基づく知見の紹介。

 - Security Issues for "Always On" Devices
AT&T Worldnet においてケーブルモデムや xDSL, fixed wire1ess といった常時接続サービスを提供した折のリスクアセスメントの話。ケーブルモデムでは隣接世帯と同一のブロードキャストドメインになるため、Windows のファイル共有などが見える。

 - A Tiger Team Approach to resolving vulnerability cases
火曜日の "BIND Activity"CSIRT 業務の視点から vulnerability handling の流れを紹介する内容だったのに対して、この発表は vulnerabilityhandling の過程を時間を軸にモデル化しようというややアカデミックな話であった。プレゼンテーションの中ではモデルに対して実際のデータを投入して図表化し、考察を行っていたが、残念ながらそのデータは配布されなかった。研究者の視点であり、すべてが実際の CSIRT 業務に有効であるとは思えない。しかしながら、情報公開の時期や手順などを考えるうえで大変興味深い発表であった。

- What Incident Response Personnel need to know about today, shacker world
会場からの質問によるパネルセッション。「ハッカー」の行動様式等に関する知見や、Law Enforcement 関係者が defcon 等に出席した折の話。
- Intrusion Detection
 - The Implementation of IDA
 - Lessons Learned in the Implementation of a Multi-Location Network Based Real-Time Intrusion System
IBM ERS のサービスについての紹介。実際の運用に基く知見が紹介されており、有益であった。
- Y2K Panel
コーディネーションセンターには一般的な質問が寄せられる傾向があるため、(1) センターとして Y2K に関するレポートが大量に寄せられるおそれがある、(2) FAQ の整備や情報収集により備えるべきである、(3) オーストラリアは先に 2000 年になるので AusCERT は状況を他のチームにレポートするつもりである、といった話題が出た。また、(4) セキュリティパッチが Y2K compliance と衝突する可能性があるという指摘があった。
- Incident Handling
CERT-CC/KR と CERT/CCc(+ISS)から、インシデントハンドリングに必要な情報をいかに効率良く抽出するかという話題で発表があった。
- Ask the Experts
会場からの質問によるパネレセッション。以下のような話題があった。
 - Explorer.Zip について(ユーザ教育が重要である)
 - 参加者の比率(大学/政府機関/IT 産業/他)
 - メール自動応答のセキュリティ
 - パケットのトレース(DoS Tracker のような)
 - coordinated な attack はどれくらいあるか
 - UDP を使う意味はあるか(プロトコルデザインの問題、TCP よりも軽い再送メカニズムを実装しやすい)
 - 大学に情報セキュリティを教える学科を作るべきでは。
 - Multicast について(フィルタリングが難しい)
 - 自動システムの秘密鍵について(注意せよ、ガードを固くせよ)
 - オープンソースソフトウェアのセキュリティについて
- Secure Shell (SSH) Tutorial
registration 時には "Incident Response-Threats and Responses" というタイトルになっていたチュートリアルレ粹である。SSH バージョン 1 に関

する導入ガイド的な内容であった。我々にとって SSH は既に馴染みの深いソフトウェアであり、技術的な収穫はなかった。

- Risk Avoidance and Risk Management (Advanced Tutorial Track)
Protect, Detect, React にかかるコストを時間の関数と捉えてアセスメントせよ という内容。 $P(t) > D(t) + R(t)$ とせよという主張。会場とのディスカッションを重視しており、途中から話が逸れていった感がある。
- Creating an Incident Response Team
IR 業務を実現するための HOWTO 的なチュートリアルと、FedCIRC の活動報告的な話であった。人材や環境など IRC (Incident Response Capability) として必要なものや、様々なプロシジャの確立や教育などについての説明が行われた。

9.2.2 Information Security For New Millemium(於:韓国)

第3回 Anti-Intrusion Workshop が韓国で、1999年11月8日から11月9日の期間で行なわれた。

アジアパシフィックの CSIRT として、CERTCC-KR(韓国)を始め、TW-CERT(台湾), AusCERT(オーストラリア), SUNSET(スタンフォード大学)と議論を行なった。

韓国におけるセキュリティインシデントの組織 CONCERT(大学, 研究機関, 企業, および ISP など 150 以上の組織から構成される)の第3回のワークショップ。特に今回は海外の CSIRT を迎え、海外に韓国の現状を紹介するとともに、情報交換を行なわれた。

主催:

MIC(Ministry of Information and Communication)

KISA(Korea Informaiton Security Agency)

CONCERT(Consortium of CERTs)

協賛:

KISIA(Korea Information Security Industry Association),

Chosunilbo, E1ectronic Newspaper, Information Security 21,

LG-EDS Systems, Samsung SDS, SK Telecom, Inet Inc.

Sun Micro Systems Korea

- Tutorial "Secure Administration of Campus Networks" : Stephen E.Hansen, Security Officer, Stanford University.

Stanford University の CSIRT(SUNSET)に関する紹介とその取り組み, インシデントに関する分析など。

- SessionA-1 "Security Organizations of Korea"
韓国におけるセキュリティ関連の組織に関する発表(6つ)。KISA, コンピュータ犯罪対応組織, CERTCC-KR, Korea Root CA, KISIA について。
- SessionA-2 "AP Countries Session"
AusCERT, JPCERT, TW-CERT 各組織の紹介。TW-CERT に関しては初めてだったので, 勉強になった。
- 展示
アンチウイルス関連, ファイアウォール関係, データリカバリ関係のサービスなどの説明を見た。残念ながらほとんどの資料が韓国語。
CIH ウィルスは韓国ではかなり猛威をふるったようである。
- Panel Discussion "Y2K and Information Security, Virus and Crack"
日本の Y2K の取り組みを(個人的意見として)話した。