高対話型おとりシステムの運用経験に関する考察

澁谷芳洋[†1,☆] 小池英樹[†2] 高田哲司[†3]
安村通晃[†4] 石井威望[†5]

インターネット利用人口は拡大しており，今日では個人，組織の双方においてネットワークの使用は欠かせないものとなりつつある．インターネットは多種多様なサービスを提供し，なくてはならないものになっているが，その半面，不正アクセスの問題も急増している．しかし実際の侵入がどのようなものであるかを認知する機会が少なく，見えない世界でのセキュリティに対する認識が難しい．そこで本論文では不正侵入対策の手段の 1 つとなっているおとりシステムに着目し，Honeynet Project が提唱している高対話型として構築した．高対話型おとりシステムの特徴として，OS レベルでおとりを実現し，不正アクセス者に制限なく自由に行動させ，不正アクセス者に気づかれないように行動記録を取得，分析することにより，既知の攻撃方法のみならず，未知の脆弱性や行動を記録することが期待されている．しかし高対話型おとりシステムは概念が新しく，主としてその概念ばかり公開されており，具体的なシステム構築例および，運用結果，問題点についての公開情報が少ない．したがって本論文では高対話型おとりシステムを公開されている情報を参考に実際に構築，運用し，不足する機能を追加したうえでさらに運用を行った．その結果得られたデータおよび知見をもとにおとりシステムの持つ問題点および運用方法の提案を含め今後の課題について述べる．

A Study for Some Experiences of the Operation of Highly Interactive Decoy System

Yoshihiro Shibuya,[†1,☆] Hideki Koike,[†2] Tetsuji Takada,[†3]
Michiaki Yasumura[†4] and Takemochi Ishii[†5]

With the rapid increase of the number of Internet users, now network use is indispensable to individuals and to organization. Although Internet provides us various services and our lives depend on it heavily, we have many problems of suspicious accesses. However, there are few opportunities to recognize what an actual exploit is, and it is difficult to recognize of the security, that is not visible. In this paper, we deployed a decoy system based on the highly interactive level Honeynet Project has defined. This system enables to be decoy on the OS level, making intruders act freely without restriction. It records not only the known activities, but unknown vulnerabilities and activities without being notified by the intruders. Currently, the concept of highly interactive level decoy system is new, the information in these system is not fully available. From these references, we have conducted an operation of the system, while adding some new features that were necessary. By analyzing all the logs from the system, we describe problems and propose the suitable operation methods.

1. はじめに

現在，不正アクセスに対する対策の一手法として，不正アクセス者の行動を記録し，分析することによりその行動を学習する「おとりシステム」の手法が注目されつつある．このシステムでは故意にアクセスしてきた攻撃者をおとり空間に誘導するもの[1)~4)]，アプリケーションレベルで実際にシステムへのアクセスは許可せずにアクセスのイベント記録のみを得るもの[5)]

†1 慶應義塾大学大学院政策・メディア研究科
Graduate School of Media and Governance, Keio University
†2 電気通信大学大学院情報システム学研究科
Graduate School of Information Systems, University of Electro-Communications
†3 ソニーコンピュータサイエンス研究所
SONY CSL
†4 慶應義塾大学環境情報学部
Faculty of Environmental Information, Keio University
†5 東京大学
The University of Tokyo
☆ 現在，海上自衛隊
Presently with Japan Maritime Self Defense Force

等，多様な提案がされている．また，OS レベルでおとりを実現することにより完全にシステムへのアクセスを与える高対話型のおとりシステムの研究に関しては，代表的なものに Honeynet Project[6] がある．Honeynet Project では高対話型おとりシステムとして VMware[7] を使った仮想 OS によっておとりシステムのネットワークを作り，不正アクセス者の各種行動を記録するという方法を web 上で公開している[8),9)]．高対話型おとりシステムは不正アクセス者に制限なく行動させることにより未知の攻撃や脆弱性を発見することが期待されている．しかし，現状ではそのコンセプトの紹介がメインで，公開されている限りでの情報では具体的な運用方法および取得データの把握が難しく，実際に構築し，運用してみなければそれらがどのようなものであるかを認識するのは難しい．

また，同様のコンセプトをもとに実運用し，その体験が公開されているケースもあるが[10)~12)]，実運用回数が 1 回のみで，解析方法も一定時間ごとに VMware のファイルとして残されたおとりシステム自体をコピーし，その内部に残された痕跡の紹介にとどまり，攻撃から侵入，その後の行動の具体的な分析までは触れられていない．そこで本論文では筆者らが実際に計 6 回の運用を実施し，その運用経験により，まだ公開議論されていない問題点および知見を明らかにする．さらに高対話型おとりシステムに必要とされる機能および運用形態について議論する．

2. 高対話型おとりシステム

OS レベルでおとりを実現する高対話型おとりシステムの一般的な目的および要件については以下のとおりである．

2.1 目　　的

高対話型おとりシステムは，OS そのものをおとりとして不正アクセス者に自由に行動させることにより，その行動を逐一記録し，不正アクセスの手法および動機，その他不正アクセス者に関するあらゆる情報を分析，学習することを目的とする．本研究においては，実際に高対話型おとりシステムを構築・運用することにより，まだ公開議論されていない問題点および知見を明らかにし，さらに今後必要とされる機能および運用形態について議論することに重点を置く．

2.2 要　　件

高対話型おとりシステムを構築するにあたり，最低限必要とされる要件は以下のとおりである．

(1) 不正アクセス者におとりの存在を気づかれないシステム構成
高対話型おとりシステムは，不正アクセス者の行動をありのままに記録し，分析を行うため，極力自然のシステムであるように見せかける必要がある．不正アクセス者におとりであることが見破られてしまうと，ログアウトし，二度とシステムに戻ってこなかったり，痕跡を消去される等，情報収集に致命的な支障を来す．

(2) 外部への攻撃の排除
おとりシステム内で自由に行動させる場合，侵入した不正アクセス者はおとりを踏み台として外部へスキャンや攻撃等を行う可能性がある．しかし，研究目的で運用を行う場合，おとりシステムが犯罪の手段として利用されることを避けなければならない．したがって，システムを構築するうえで，外部への攻撃を最大限に回避するべく，その構成および運用形態に細心の注意を払わなければならない．

(3) 不規則な運用期間および不測事態への対応
不正アクセス者の到来が事前に判明していないため，侵入行為がいつ発生するか分からない．しかし，侵入後，外部への攻撃の対策を回避する等，不測の事態に対応できるよう，時間帯を問わずつねに監視，対処が可能な状態にしておかなければならない．

以上の必要最低限の要件を熟慮したうえで，システム構築を行う．

3. システム構成および試行運用

本研究ではグローバルアドレスを少数保持している SOHO 環境のネットワークにおいて計 6 回の運用を実施した．そして当初 web において公開されていた情報を参考に構築した初期システムから運用を開始し，全 6 回の運用経験を経て得た知見をもとに進化させていった結果，現在運用するシステム構成となったものである．その最終的なハードウェア構成，使用 OS およびツール群を**図 1** に示し，以下その詳細について説明する．

3.1 ハードウェア構成および使用 OS

ハードウェア構成および使用した OS については以下のとおりである．

- おとりシステム
  不正アクセスを行う者に直接アクセスさせ，その行動を分析するためのシステムである．おとりシステムは未知の脆弱性をも発見することができると期待されているが，本実験では，既知の脆弱性および，攻撃法を含め，どれだけ不正アクセス者

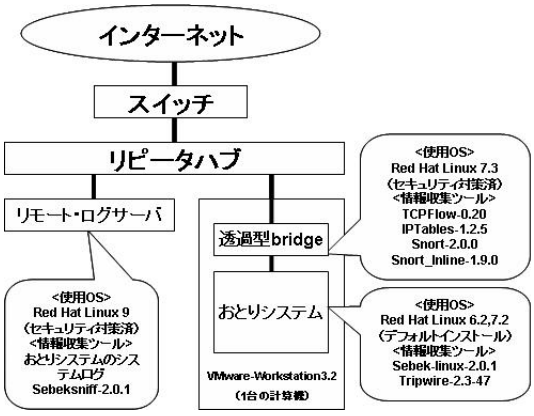

図 1 ハードウェア構成
Fig. 1 Hardware architecture.

に対する情報を得ることができるかをまず検証する必要があった．そのため，故意にシステムに脆弱性を持たせることにより攻撃者が侵入しやすい環境を構築するべく OS にパッチを当てない手法をとった．全 6 回の運用のうち，最初の 3 回は Red Hat Linux 6.2 とし，後半の 3 回はバージョンを上げて Red Hat Linux 7.2 で実施した．なお，起動サービスは，FTP（最後の 1 回を除く），Telnet，SMTP，HTTP，HTTPS とした．

なお，本研究では上記 OS およびサービスで実施したが，今後，不正アクセス者の行動分析をより多く学習するためには，可能な限り多くの OS および多様なサービスを起動させて情報収集を行う必要がある．

- 透過型ブリッジ
  おとりシステムとインターネットとの間にアクセス制御およびデータ収集を行うブリッジを置く．このブリッジ機能は Red Hat Linux 7.3 にデフォルトで組み込まれているため，本実験では当該バージョンを使用した．透過型ブリッジを利用する利点は，IP アドレスを持たず，TTL 値☆の減少もないことから，不正アクセス者に気づかれる可能性が少ないことである．このブリッジにおいておとりシステムに出入りするトラフィックの制御および記録を行う．また，侵入検知システム（Intrusion Detection System，以下 IDS），外部への攻撃を自動的にドロップするツールもこのブリッジにおいて実行した☆☆．
- リモート・ログサーバ
  おとりシステム本体においては，システムの情報を逐一記録するシステムログおよび，キーストロークを記録するツールが実行されている．しかし，攻撃者が侵入に成功した場合，Rootkit と呼ばれるトロイの木馬を設置し，不正アクセス者の行動を隠すのが主流となっている．また，ログの改ざんやシステムの破壊等，おとりシステム上で行われる記録が信頼できないものになると仮定し，リアルタイムでシステムログとキーストロークを転送し安全に保存するリモート・ログサーバを設置した．このことにより，ログを消去されたり，システムを破壊されたりした場合でも事後解析が可能となる．

  また，10 分おきにキーストロークとシステムログをメールで通知することにより，キーストローク事象の発生から侵入の事実を知ることができ，侵入以後は，極力リアルタイム解析ができるように工夫した．

3.2 情報収集ツール

不正アクセス者の行動を記録する情報収集ツールは，インターネット上で多数公開されている．目的によって複数のツールを使用することが可能であるが，ログの量が多すぎると重要な記録を見落とす等，解析に不備が生じる可能性があることを考慮し，必要十分な情報収集をするべく本研究では最終的に以下に述べるツールを使用した．

(1) ブリッジ

透過型ブリッジに設置したツール群は以下のとおりである．

- TCPFlow
  TCPFlow[14] は，確立した TCP セッションの全記録を行うツールである．このことにより，平文におけるセッション内容の解析が可能となり，また，キーストローク記録のみでは解析不可能なスクリプトの内容の分析にも役立つ．さらに，ダウンロードしたファイルのバイナリも記録することができ，ヘッダ部分を取り除くことである程度のバイナリの事後展開も可能である．Honeynet Project では IDS によってすべてのトラフィックダンプを記録しているように書かれているが，それ以外の具体的な情報収集の方法については触れられていない．そこで，本研究では独自に解析を容易化することおよび，セッションの状況が具体的に平文で記録される利点を考慮し，当該ツールを使用した．
- IPTables

☆ パケットがネットワーク上を巡回し続けられる時間
☆☆ ブリッジの起動スクリプトが Honeynet Project から公開されている[13]．

IPTables は，Linux Kernel 2.4 以降で標準装備となった Firewall である．このツールはアクセス制御のほか，出入りするトラフィックの記録をシステムログに記録する機能を有している．本研究では，当該ツールがおとり OS に標準装備であり，オープンソースであることと，このツールにより，本研究に必要なアクセス制御，ロギング等の機能が満たされているために他の Firewall ツールを用いることなく活用した．また，本研究では，外部からおとりシステムへのトラフィックをすべて許可し，おとりシステムから外部へのトラフィックは回数制限を行った．すなわち，おとりシステム発の DoS 攻撃を回避するため，1 日あたり，TCP を 9 回，UDP を 20 回，ICMP を 50 回，その他 10 回に制限した．制限回数に至ったらそれ以降のパケットは自動的にドロップされる．

- Snort [15]
  Snort は，オープンソースの IDS である．トラフィックをシグネチャと比較し，一致した場合に警告を発する．本実験では，侵入時における攻撃パターンの抽出のために使用した．
- Snort_Inline [16]
  おとりシステムが侵入された後に気遣わなければならないのがおとりシステムを踏み台とした外部への攻撃である．当該ツールは，おとりシステムから出たパケットで，シグネチャと一致したパケットを無効化する．このことにより，上記 IPTables における外部への攻撃の回数制限による回避の補完をなす．

(2) リモート・ログサーバ

リモート・ログサーバに設置したツール群は以下のとおりである．

- Sebeksniff [17]
  Honeynet Project が独自に開発したツールであり，後述する Sebek-linux とはサーバ・クライアントの関係をなす．このツールは，おとりシステムにおいて設置された Sebek-linux がネットワーク上に流した UDP によるキーストローク記録を取得し，ログに記録するものである．このツールはシステムログを介さずに記録を行うため，ログを改ざんされたり，システムログを停止されたりしても機能する．

(3) おとりシステム

おとりシステム本体に設置したツール群は以下のとおりである．

- Sebek-linux [18]
  Loadable Kernel Module を組み込む形でキーストロークの記録を行い，特定の IP アドレスおよび MAC アドレスの計算機に記録を UDP パケットとして送る．改造型の bash のような，システムログに依存する記録方法の場合，侵入後にシステムログを停止されるとその後の行動分析ができなくなるが，当該ツールはシステムログを停止されても引き続き記録が行えることと，Loadable Kernel Module 組み込み型で，その存在に気づかれにくい利点に鑑み，本運用において採用した．
- Tripwire [19]
  ホスト型 IDS であり，初期の状態でシステムのファイルの属性，容量等をすべてデータベース化し，記録する．改ざんされたファイルの有無をチェックする際，このデータベースと比較する．事後解析において，改ざんされたり追加されたりしたファイルの検証に使用することができるが，本研究では基本的に情報収集をおとりシステムの外部で行う運用方針であるため，当該ツールは事後解析時の補助として用いた．

また，本研究では，おとりシステムおよびブリッジは VMware Workstation 3.2 [7] を使用することにより，1 台の計算機で済ませ，リモート・ログサーバを含め合計 2 台の計算機で実現した．VMware の利点は，Guest OS としてインストールしたおとりシステムをファイルの形で保存することができるため，運用終了後のリカバリが数分で可能となることである．

4. 運用結果

おとりシステムをネットワーク上に設置し，全 6 回の実験を行った．そして最終的な形での運用形態は前項で述べたとおりである．また，6 回分の変更履歴を**表 1** に示し，以下，運用結果について述べる．

4.1 実験期間

実験期間を**表 2** に示す．本研究では，おとりシステムをネットワーク上に設置してから攻撃，侵入に至り，解析上の問題点が発見されるまでの間，繰り返し行った．

表 1 システムの変更履歴
Table 1 System changed history.

回次	変更箇所
2	IDS の設置（Snort） リモート・ログサーバの設置 キーストローク記録（Syslog 依存）
4	キーストローク記録（Syslog 非依存-Sebek）
5	外部への攻撃の無効化（Snort_Inline）

表 2 システムの運用期間
Table 2 Term of operation.

回次	期間
1	2003/4/21 11:32-5/2 7:22
2	2003/5/9 18:54-5/21 7:52
3	2003/5/31 20:20-6/2 10:02
4	2003/6/10 17:19-6/11 9:45
5	2003/7/3 16:00-7/14 8:24
6	2003/7/14 9:27-7/30 9:33

表 3 運用開始から侵入までに要した時間，起動サービス
Table 3 Time and opening services until attacked.

回次	侵入までに要した時間	起動サービス
1	9 日 4 分	FTP,Telnet,SMTP,HTTP HTTPS
2	10 日 23 時間 26 分	FTP,Telnet,SMTP,HTTP HTTPS
3	16 分	FTP,Telnet,SMTP,HTTP HTTPS
4	13 時間 7 分	FTP,Telnet,SMTP,HTTP HTTPS
5	5 時間 14 分	FTP,Telnet,SMTP,HTTP HTTPS
6	10 日 33 分	Telnet,SMTP,HTTP HTTPS

4.2 運用の指針

運用の指針としては，構築したおとりシステムの情報収集能力を検証するため，未知の脆弱性および攻撃方法のみならず，不正アクセス者のすべての行動を収集するべく実施した．したがって，当初は不正アクセス者の攻撃，侵入そしてその後の行動を可能な限り多く，短期間で収集するため，セキュリティホールがある状態での OS で運用した．

4.3 攻撃情報の取得

全 6 回において，IDS が作動不良であった第 1 回を除き，攻撃情報の取得に成功した．その内容は，FTP の脆弱性に対する攻撃が 4 件，HTTPS の脆弱性に対する攻撃が 1 件であった（**表 3**，**表 4**）．なお，第 2 回次から第 5 回次までの攻撃，侵入方法がすべて FTP の脆弱性に対するものであったため，第 6 回次では FTP サービスを停止した結果，HTTPS に対する攻撃となったものと考えられる．

また，既知の脆弱性に対する攻撃は，ウィルスやワーム等の自動化された攻撃が多いことが考えられる．それらの自動化による攻撃についてもおとりシステムで多数記録されたが，本運用で実際に侵入に成功し，その後連鎖的に行動が記録されたものは手動のものであった．

このうち，FTP の脆弱性を狙ったものについては，IDS のシグネチャに合致しており，IDS の警告ログに記録が残されていたが，HTTPS の脆弱性を狙ったものについては IDS には記録されていなかった．そこで，ブリッジの IPTables における出入りする IP アドレスおよびポート番号の記録と，TCP セッションの全記録とを照合した結果と，起動していた HTTPS サービスはすでにバッファオーバフローに対する脆弱性が指摘されていたことから，この攻撃は特殊な文字列を送り続けた結果生じたバッファオーバフロー攻撃であると判断した．このように，シグネチャと合致しない未知の攻撃や，亜種と思われる攻撃法については，IDS の記録には残らないため，トラフィックの記録やセッション記録から探る必要がある．なお，IDS のシグネチャについてはつねに最新のものを使用している．

表 4 攻撃先，攻撃方法，ダウンロードしたツール
Table 4 Attack and downloaded tools.

回次	攻撃先	攻撃方法	ダウンロードしたツール
1	不明	-	Rootkit IRC 関連ツール
2	FTP	RNFR ././攻撃	Rootkit
3	FTP	RNFR ././攻撃	Rootkit IRC 関連ツール
4	FTP	RNFR ././攻撃	Rootkit スキャンツール (ftp,DNS 脆弱性)
5	FTP	RNFR ././攻撃	Rootkit
6	HTTPS	バッファオーバフロー攻撃	(試みたが失敗)

また，攻撃内容で，FTP RNFR././攻撃の記録では，すべての記録において，“. /./” のコマンドが 73 回繰り返された結果，管理者権限の取得に至るというものであった．

第 1 回次において IDS が作動不良であり，攻撃に対する記録が取得できなかったため，第 2 回次以降ではシステム起動時のみならず，定期的にシステム全体の機能チェックを行い，情報洩れがないよう心がけた．

さらに，全 6 回の運用における，おとりシステム設置から侵入までに要した時間は表 3 のとおりである．

4.4 侵入後の行動

侵入に成功した後，不正アクセス者は必要なツールを外部からダウンロードし，おとりシステムの利用を開始した（表 4）．ダウンロードは FTP セッションまたは，HTTP セッションにより行われるため，ダウンロード先，ファイル名，インストール先の状況は逐一記録される．その記録は透過型ブリッジを通過する際に行われるため，不正アクセス者に気づかれることはない．また，TCPFlow により，ダウンロードしたツールの全バイナリも記録されるため，おとりシステム上でツールをインストール後にダウンロードしたバ

```
From: root root@localhost.localdomain
To: xxxxxx@yahoo.com
Subject: Linux localhost.localdomain 2.4.18-3 #1 Thu Apr 18 07:31:07 EDT 2002 i686 unknown

*** Uname –a:
Linux localhost.localdomain 2.4.18-3 #1 Thu Apr 18 07:31:07 EDT 2002 i686 unknown
*** Inet Info
      inet addr:xxx.xxx.xxx.xxx Bcast:xxx.xxx.xxx.xxx Mask:255.255.255.248
      inet addr:127.0.0.1 Mask:255.0.0.0
--- 中略 ---
***Passwd:
root:x:0:0:root:/root:/bin/bash
--- 中略 ---
***Shadow
root:HBbpsx02dN4WXGlK.a3iu0:12212:0:99999:7:::
--- 以下省略 ---
```

図 3 システムデータのメール送信
Fig. 3 Mail of system data.

```
18:03:12-2003/07/24 [501:bash:16213:pts:0]w
18:03:22-2003/07/24 [501:bash:16213:pts:0]skill -kill pts/0
18:03:32-2003/07/24 [501:bash:16213:pts:0]w
18:03:38-2003/07/24 [501:bash:16213:pts:0]ls
18:03:41-2003/07/24 [501:bash:16213:pts:0]cd /var/tmp
18:03:45-2003/07/24 [501:bash:16213:pts:0]cd 1
18:03:47-2003/07/24 [501:bash:16213:pts:0]./x
```

図 2 ログインアカウントの確認と強制ログアウト
Fig. 2 Checking login account and forcing log-out.

イナリ本体を消去されても事後解析することが可能である．

さらに，これら解析可能なセッションは，平文で行われるものに限られ，不正アクセス者はツールのダウンロードに失敗し続け，結局何も行わなかった第 6 回次を除き，毎回 SSH バックドア付きのツールをダウンロードし，利用していたため，それ以降の行動は暗号化されており解析することができなかった．このため，暗号化される前にキーストロークを記録する必要が生じ，第 2 回次以降はキーストロークの記録を行った．この時点ではキーストロークをおとりシステムのシステムログに記録し，それをリモート・ログサーバに転送する方策をとった．しかし，第 3 回次において，おとりシステムの Syslogd を改ざん，サービスの再起動をするといった問題が発生したため，データの信頼性がなくなったことから，第 4 回次以降は前述の UDP パケットとしてリモート・ログサーバに送るシステムログに依存しない方式をとった（表 1）．

また，侵入後は毎回 w コマンドで他のログインアカウントの有無を調査しており，筆者が試しにログインしてみたところ，強制的にログアウトさせられた（**図 2**）．

このキーストローク記録と保存したツールとを照合することにより，ダウンロードした新たなツールと考えられるコマンドがどのような働きをするのかを検証し，暗号化されているセッションでの不正アクセス者の行動を解析した．その結果，外部へ発しようとしたスキャンコマンド等の記録を認めることができた．

4.5 おとりシステムの利用

全 6 回運用した結果，おとりシステムを外部への攻撃に利用した記録はなかった．そのかわり，ダウンロードしたツールの中に，侵入したおとりシステムが脆弱であることを他の攻撃者仲間にメール通知をするスクリプトが組み込まれており，それを利用した外部へのメール送信や（**図 3**），IRC セッション関連のツールをダウンロードし，外部との会話に使用するというものが目立った．ただし，IRC 関連ツールは，不正アクセス者がリモートからの管理を容易にする Backdoor タイプのワームもあり，また，記録内容が英語での会話のほか，解読不明な文字列も存在し，実際の IRC かワームであるかの確認には至らなかった．

第 2 回次から第 4 回次までは，定期的にリモート・ログサーバをチェックし，10 分おきに転送されたログとキーストロークをメール通知した．しかし，第 4 回次に外部へのスキャンコマンドを数個打った記録があり☆，リアルタイムで監視していても，コマンドを発するのは一瞬の出来事であり，手動で阻止することができなかったという反省から，第 5 回次以降は時間あたりの回数制限および侵入後のリアルタイム解析に加え，前述した Snort_Inline を導入した．

また，第 3 回次には，おとりシステムのログイン機能が改ざんされてしまい，解析のためおとりシステムにログインできないという不具合が生じ，やむをえず

☆ IPTables の記録から，外部に出た形跡はなく，コマンドの実行は失敗していた．

不正アクセス者の設置した Backdoor からログインしてシステムを停止するという場面もあった．この対策として，常時何らかのアカウントをログインさせておくことも考えたが，不正アクセス者に気づかれることを考慮し，それは行わなかった．

5. 考　　察

以上に述べたとおり，高対話型おとりシステムのコンセプトを Honeynet Project の公開情報を参考に確実なデータ収集ができるようシステムに機能を付加することにより，攻撃から侵入，利用までの一連の流れを記録として残すことができた．ここでは，試行運用の結果得られた，新たな知見等についてまとめる．

5.1 問題点と本研究で講じた対策

本研究において明らかになった問題点および，運用過程で講じた対策について述べる．

(1) IDS では検知できない攻撃への対策

IDS は，シグネチャとのパターンマッチングにより攻撃のインシデントを検出するが，攻撃手法がそのシグネチャとは異なる「亜種」攻撃であった場合には検出されない．本研究では 4 度の FTP に対する攻撃は IDS により検出されたが，最終回次の HTTPS に対する攻撃は検出されず，TCPFlow が取得したデータを解析することによりシグネチャとは異なるパターンのバッファオーバフロー攻撃であることを確認した．しかし，TCPFlow は攻撃に限らずすべての確立されたコネクションを記録するためにログの量が膨大となり，IDS として使用することは困難である．また同様の理由で侵入された瞬間の通知も難しい．そこで，本研究では定期的にキーストロークのログをメール通知することにより，キーストローク事象の発生をもって侵入の事実のアラートと考え，その後の厳密な監視活動を行った．

同様に，シグネチャとのパターンマッチングにより外部への攻撃を無効化する Snort_Inline についても，外部への攻撃が「亜種」攻撃であった場合には検出されず，そのまま外部へと発されてしまう．これはおとりシステムに限らず IDS の持つ課題とされていることであり，この問題点を考慮のうえで運用しなければならない．本研究ではそれを手動で補うため，侵入の事実を確認したらただちにおとりシステムの監視体制へと移行し，以後はリアルタイムで不正アクセス者の行動をログおよびキーストロークから追跡することにより，外部への未知または亜種の攻撃等，不慮の事態に対し常時対応できるようにした．

(2) 未知のコマンドが暗号化通信である場合の問題と対策

不正アクセス者は，バックドア付き SSH によりログインしていた．したがって，キーストロークは記録することができるが，そのコマンドが連鎖的なスクリプトであった場合にはそのコマンド名からは行動を把握できない．本研究では未知のコマンドは主にダウンロードしたツールのコマンドであり，あらかじめ保存しておいたダウンロードツールを解析用の計算機で展開し，検証することによりその内容を把握した．仮におとりシステム内に SSH がインストールされていなくても，不正アクセス者は外部からダウンロードしてそれを用いるため，おとりシステムを運用する際には暗号化通信が主に利用されるということを念頭に置いておく必要がある．

(3) ダウンロードツールの消去に対する問題と対策

不正アクセス者は，ツールをインターネットからダウンロードした後，そのバイナリを展開，インストールするが，インストール後は毎回そのバイナリを rm コマンドで消去していた．そのため，透過型ブリッジにおける TCPFlow によりダウンロードしたバイナリを保存しており，その保存されたバイナリを解析する方策をとった．しかし，ソースファイルがあればそのソースコードを解読することによりツールの機能を分析することが可能であるが，本研究において取得したバイナリの大半はコンパイル済の実行形式ファイルで提供されており，コマンド名だけではそのツールの機能を分析することができなかった．したがって，本研究における運用解析では，ツール機能検証のための計算機をさらに 1 台用意し，その計算機上でツールを実行させることにより機能を検証した．

(4) 未知の脆弱性の確認には莫大な運用期間が必要

今回，おとりシステムを実運用したのは合計 6 回，期間にして約 4 カ月であったが，その期間においては未知の脆弱性の発見には至らず，すべてにおいて，既知の脆弱性からの侵入によるものであった．未知の脆弱性を発見するには，その解析評価に至るまで，莫大な運用期間が必要であると考える．さらに，未知の攻撃についても，本実験における HTTPS に対する攻撃については，IDS の記録に残されなかったため，キーストローク事象の発生後，約 4000 以上にも及ぶ TCPFlow のログを 2 日がかりで解析することで既知の攻撃であると判断した．したがって，有期における実験で未知の脆弱性を取得することは困難であり，また，未知の攻撃についてもおとりシステムの設置から侵入の事実を認めるまでの期間が長い場合には，

TCPFlow のログの量が莫大なものとなり，解析にさらなる時間を要するため，おとりシステムの設置目的をこの 1 点に絞ることは難しく，未知のものに限らず不正アクセス者の行動全般について学習することに焦点を当てるのが適当であると考える．

(5) 単独または少人数での長時間連続監視の問題

本研究における行動監視は単独で行った．シグネチャとのパターンマッチングで外部への攻撃を無効化するという手法が完全でない以上，おとりシステムを土台にした外部への攻撃を極力防ぐためには侵入後のリアルタイム監視が必要不可欠である．しかし，複数の人数でチームを組む等，当直制で監視を続けない限り，単独での連続監視には生活活動等の制約がある．本研究においても長期間の連続監視が困難であったため，踏み台とされる前に，不正アクセス者がログアウトする等のタイミングを見計らって運用を停止した．しかし，これではバックドア等から再びおとりシステムに戻ってきた場合の情報収集活動が困難である．

5.2 不正アクセス者の特性と情報収集に留意するべき点

本運用結果を分析して明らかになった不正アクセス者の特性および，情報収集に留意するべき点について述べる．

(1) おとりシステム上での解析が困難

本研究において，不正アクセス者は侵入後に毎回 w コマンドで他のログインアカウントの有無を確認し（図 2），必要であれば強制ログアウトさせてまで単独行動を好んだ．このことは，運用中は安易におとりシステムにログインできないことを示している．したがって，運用中はおとりシステム上での解析ができない．VMware の特性を生かし，ファイルとして保存されているおとりシステムのコピーをとり，検証用の計算機を設けて解析し，それを定期的に行うことによりその差分を比較することにより解析するという方法もあるが[11),12)]，運用期間中においては，不正アクセス者はダウンロードしたツールのソースファイル，コマンド履歴を消去することはもちろん，パスワードファイルを何度も改ざんしたりしていた．したがって，おとりシステムをファイルとして定期保存しても，その時間間隔に発生した事象がすべて記録されているわけではない．以上のことからおとりシステム内のデータに依存するのではなく，透過型ブリッジおよびリモート・ログサーバ等のおとりシステム外部において極力多くの情報を収集する必要がある．

(2) 多様な言語構成

不正アクセス者の行動心理を分析するのに IRC による外部との会話は貴重な資料となるが，その会話が必ずしも主要言語であるとは限らない．本研究で得た IRC の会話においてもその例に漏れず，東欧系の言語であることまでは判明したが，全会話の内容分析には今後も多大な時間を要する．このように，不正アクセス者の身元は世界レベルであり，計算機やネットワーク関連の知識のみならず，語学関連の知識が要求されることもある．

5.3 今後の課題と展望

以上の知見をふまえ，より安全かつ実用化に向けた高対話型おとりシステムに必要と考える運用形態および機能について以下のとおり提案する．

5.4 侵入と同時に対処できる正確な通知機能

本研究では，おとりシステムから離れている際，発生したキーストローク事象のメール通知を持って侵入の事象を確認していたが，通知間隔を広げた場合には不測の事態への対処が遅れる可能性がある．また，間隔を狭めるとメールサーバの負荷の増大にもつながる．したがって，侵入と同時に対処するためには常時おとりシステムを自動監視し，侵入を表す特定のトラフィックあるいはシステムコールが呼ばれた時点で自動的に管理者にアラートを発する機能があればより迅速な対応ができるものと考える．

5.5 監視態勢への移行までの自動的対応

管理者不在時に侵入を受けた際，管理者が監視態勢へ移行するまでの間，自動的に不正アクセス者を足止めしつつ適切な対処ができることが望ましい．それを実現するための具体的なシステム考案については今後の課題である．

5.6 行動状況解析の可視化

本研究では行動分析をリアルタイム，事後とを問わず地道な手動によるログの照合に任せている．ログの量は膨大であり，リアルタイム解析においては重要な情報を見落とす可能性があるため，不正アクセス者の行動を理解しやすく可視化することにより，現在の状況を瞬時に判断できるようにし，解析の手を緩和させる機能があればより確実な状況対応がとれるものと考える．

5.7 各研究分野の統合プロジェクト化

おとりシステムは，既存の情報収集ツール等の組合せであるが，それらのツールについて，個々の開発分野における専門家が集い，システムと同調することができ，かつ要件を満たすツールの開発，実装に携われば現在かかえている問題点の解決への近道となるものと考える．

6. おわりに

本研究では，不正アクセス者の行動分析から，未知の脆弱性や行動を学習することが期待されているおとりシステムを OS レベルで実現する高対話型おとりシステムとして構築，実運用した．高対話型おとりシステムはその概念については公開されているが，具体的なシステム構築例および，実運用における結果とその解析については公開例がきわめて少ないため，本研究では公開例を参考に情報収集のためのツールや，侵入の際のアラート手段等，公開例だけでは不足していた機能を順次追加しながら実際に構築，運用することによりその問題点および知見等を得ることを目的に実施したものである．

そして，不正アクセス者の攻撃から侵入，利用までの一連の流れを記録した．また，全 6 回にわたる実運用によって得られたデータを基に解析し，得られた知見等について述べた．本研究で得られた結果が不正アクセス者の行う行動のすべてではないが，ネットワークに接続されているシステムがさらされている脅威についての概要について示すことができたと考える．

セキュリティには，侵入検知に代表されるような技術的な面と，その技術を活用する人的な面との 2 通りがあると考えられるが，特に後者については，セキュリティが「見えない」世界であるために啓発が難しい．しかし本研究によって，おとりシステムが不正アクセス者の行動を具体的に記録することができるということが分かり，それはおとりシステムの運用を検討していくうえで貴重なデータであると考える．また，不正アクセス者の行動は，IDS 等，単独のツールだけでは情報収集が不可能であり，おとりシステムの運用，すなわち不正アクセス者の行動分析に必要な情報は多岐にわたることを示している．

本研究により，高対話型おとりシステムによって不正アクセス者の一連の行動を把握できることは検証することができたが，考察の項で述べたとおり，今後は不正アクセス者がおとりシステムからいったんログアウトし，その後また戻ってくる事象の記録等を含めたさらなる長期運用および，外部に対する攻撃へのより確実な対処方法の考案，IRC セッションの解読による不正アクセス者の心理分析の評価等の課題を解決するべく，さらに安全かつ十分なデータ収集が可能なシステムについて議論および評価していきたいと考える．

謝辞 本研究を進めるにあたり，森ビル（株）文化事業部・アカデミーヒルズリサーチネットワークには快適な研究環境を提供いただいた．また，電気通信大学大学院小池研究室のセキュリティ研究チームの皆様には，運用を進めるうえで細部ネットワーク環境の整備および論文を書き進めるうえで有用なアドバイスをいただいた．ここに，深く謝意を表する．

参考文献

1) 竹森敬祐，田中俊昭，清本晋作，中尾康二：不正侵入者に検知されることなくおとりのデータ領域へと誘導するおとりシステムの実装評価，マルチメディア通信と分散処理 101-14，コンピュータセキュリティ 12-14，pp.79–84 (2001.2.21).
2) 宮川明子，稲田 徹，後沢 忍：不正侵入者を外部ネットワークに設置したおとりサーバへ誘導するセキュリティシステムの検討，信学技報，ISEC2001-49, pp.225–230 (2001.7).
3) 河内清人，藤井誠司，木下洋輔，芦沢 賢，勝山光太郎：おとり誘導装置の試作，情報処理学会第 64 回全国大会，2H-03, pp.3-371–3-372 (2003).
4) 藤井誠司，大越丈弘，河内清人，北澤繁樹，勝山光太郎，芦沢 賢，木下洋輔：おとり誘導による不正アクセス対策システム，情報処理学会第 64 回全国大会，2H-04, pp.3-373–3-374 (2003).
5) Niels Provos: Honeyd. http://www.citi.umich.edu/u/provos/honeyd/
6) The Honeynet Project. http://project.honeynet.org/
7) VMware. http://www.vmware.com/
8) Know Your Enemy: Learning with VMware. http://project.honeynet.org/papers/vmware/
9) Know Your Enemy: GenII Honeynets. http://project.honeynet.org/papers/gen2/
10) ハニーポットプロジェクト，日経 BP 社，日経ネットワークセキュリティ,「無線 LAN パニック」，pp.130–137 (2003.4).
11) ハニーポットプロジェクト，日経 BP 社，日経ネットワークセキュリティ,「自己防衛マニュアル」，pp.146–155 (2003.8).
12) ハニーポットプロジェクト，日経 BP 社，日経ネットワークセキュリティ,「プロが薦める！最強ツール」，pp.174–187 (2003.12).
13) Tools for Honeynets. http://project.honeynet.org/papers/honeynet/tools/index.html
14) tcpflow—A TCP Flow Recorder. http://www.circlemud.org/˜ jelson/software/tcpflow/
15) Snort. http://www.snort.org/
16) Project: snort_inline: Summary. http://sourceforge.net/projects/snort-inline/
17) sebeksniff-2.0.1. http://project.honeynet.org/papers/honeynet/tools/index.html
18) sebek-linux-2.0.1. http://project.honeynet.org/papers/honeynet/tools/index.html

19) home tripwire.org. http://www.tripwire.org/
20) Spitzner, L.: *Honeypots*, Addison-Wesley, pp.167–192 (2002).

(平成 15 年 12 月 1 日受付)
(平成 16 年 6 月 8 日採録)

澁谷　芳洋

1997 年防衛大学校本科理工学専攻（地球科学科）卒業．2004 年慶應義塾大学大学院政策・メディア研究科修士課程修了．現在海上自衛隊勤務．情報セキュリティ，特に不正アクセス者の行動を分析するおとりシステムに関心を持つ．

小池　英樹（正会員）

1991 年東京大学大学院工学系研究科情報工学専攻博士課程修了．工学博士．同年電気通信大学電子情報学科助手．1994 年同大学院情報システム学研究科助教授．現在に至る．1994 年〜1996 年，1997 年 U.C.Berkeley 客員研究員．2003 年 University of Sydney 客員研究員．情報視覚化の研究に従事．特に視覚化へのフラクタルの応用，Perceptual User Interface，情報セキュリティへの視覚化の応用に興味を持つ．1991 年日本ソフトウェア科学会高橋奨励賞，2000 年情報処理学会 DICOMO2000 最優秀論文賞，2001 年 IEEE VR2001 Honorable Mention for the Outstanding Paper Award 受賞．ACM，IEEE/CS，日本ソフトウェア科学会各会員．

高田　哲司（正会員）

2000 年電気通信大学大学院情報システム学研究科情報システム運用学博士課程修了．工学博士．同年電気通信大学サテライトベンチャビジネスラボラトリ研究員．2003 年ソニーコンピュータサイエンス研究所入所．現在に至る．情報視覚化の研究に従事．情報視覚化，情報セキュリティに関心を持つ．IEEE/CS，ACM 各会員．

安村　通晃（正会員）

1947 年生．1971 年東京大学理学部物理学科卒業．1975 年〜1977 年 UCLA 留学．1978 年東京大学理学系大学院博士課程（情報科学専攻）満了．（株）日立製作所中央研究所主任研究員を経て，1990 年 4 月より慶應義塾大学環境情報学部助教授．現在，同教授．理学博士．実世界指向インタフェース，マルチモーダルインタラクション，ユニバーサルデザイン等の研究に従事．ヒューマンインタフェース学会，日本ソフトウェア科学会，日本認知科学会，日本教育工学会，ACM 各会員．

石井　威望

1963 年東京大学大学院工学研究科博士課程修了．工学博士．1991 年より東京大学名誉教授，東京電力株式会社開発本部顧問．1999 年より慶應義塾大学客員教授．2001 年より株式会社東京海上研究所理事長．