仮想クラッキングを用いた
サーバ管理能力向上のための実践的トレーニング手法

中村一樹*，小池英樹**，石井威望***
*東京海上日動システムズ　**電気通信大学　大学院情報システム学研究科
***東京海上研究所

企業等において、サーバ管理者の育成は急務である。しかも通常、サーバ管理者を短期間に育成する必要がある。そのための教育手法として教材等を使用した自習や講習実施等が考えられるが、スキルアップに時間を要する場合が多い。また、セキュリティ管理という視点で適当ではないカリキュラムが含まれていることがある。

これに対して、我々は仮想クラッキングの手法を用いて、攻撃者にクラッキングされたサーバを実践的に修復していくことで、セキュリティ管理のために必要な知識やツールを短期間で効率的に修得するという教育手法を提案し、実際に実験を行った。これにより従来と比べて、被験者のセキュリティの意識が向上するという効果が得られたので報告する。

Practical Training Method to Improve Administration Skills by using Simulated Hacking

Kazuki Nakamura*,　Hideki Koike**,　Takemochi Ishii***
*Tokio Marine & Nichido Systems Co., Ltd.
**Graduate School of Information Systems, University of Electro-Communications
***The Tokiomarine Research Institute Co.,Ltd.

In most company or organizations, it is a pressing needs to promote system administrators in a short time. Usually people study by themselves or attend a course. However, such curriculum often takes a long time to get their skills up or contains inappropriate subjects from the aspect of security administration.

We proposed a practical and efficient training method using simulated hacking. In our method, people are asked to fix the server which were cracked and damaged by the simulated hacker. Since they have to use important commands and to see important directories and files, they learn basic knowledge for the administrator much faster.

This paper reports our experiments and their results.

1．はじめに

企業等におけるサーバ管理者の育成は極めて重要であり、できるだけ短期間に業務遂行できるレベルまで能力アップさせることが必要となる。ところが従来の教育手法は、サーバ管理者の育成という観点で必ずしも効果的ではない。例えばサーバ管理者が、ある意味サーバの特定箇所の設定を把握すればよいにも関わらず、あたかも計算機工学の全てを把握しなければならないように記述されている図書が散見されることからも明らかである。

教育スタイルの観点で見るとわかりやすい。一般の職場、セキュリティ関連企業、大学における情報セキュリティ教育のスタイルという観点で捉えると、以下のように整理できる[1]。

- 通常の講義形式で実施
- 実習や実技形式で実施
- 教材やインターネットを使って自習形式で実施
- オンザジョブトレーニング

大学や企業では講義形式が採用されていることが多い。大勢の受講者に対し一般的な知識を与える場合は効率的な方法であるが、一般的に受講者が短期間で知識を修得するのが難しいという問題がある。また自習形式の場合、参考書等をもとに自分のペースで勉強できるというメリットがある。しかしそれに目を通しただけでサーバを理解するのは難しい（なかなか根気が続かず途中で挫折してしまうというケースが多い）。オンザジョブトレーニングは、講師1人に対して受講者1､2人といったように極めて少人数の下で行われることが多く、受講者の理解度に合わせてペースをコントロールできるという点で効果的な教育手法である。しかしながら、講師を担当できるような人材の確保やオンザジョブトレーニング実施に伴う講師の生産性低下という問題が懸念される。従って、実習や実技形式のコンセプトを応用して、例えば「計算機の○○というファイルの□□という箇所を直接参照させる」といった教育を、できるだけ短期間に実施する必要がある。

関連研究として、経済産業省での「セキュリティ

甲子園」の開催が挙げられる。経済産業省では、情報セキュリティに関わる次代を担う青少年の早期育成を図るため、2003年7月に「セキュリティ甲子園」の開催を発表した(同年8月に開催される予定であったが、その後中止となり、翌年「セキュリティキャンプ2004」と名称変更した上で開催された)。「セキュリティキャンプ2004」では、学者・弁護士・警察関係者などの講師による講義、セキュリティと法律に関する事例研究、セキュアなサーバの構築実習、そしてウィルスが蔓延したネットワークの復旧作業などが行われたようであるが、セキュアなサーバの構築に焦点を当てている[2]。

こうした状況を踏まえ、我々はサーバ管理者向けの短期育成トレーニング手法、すなわち仮想クラッキングを用いたサーバ管理能力向上のための実践的トレーニング手法について研究を行った。本論文では、続く第2章で仮想クラッキングを用いたサーバ管理能力向上のための実践的トレーニング概要について述べる。その後考察を行った後で結論を述べ、最後に今後の課題を述べる。

2. 仮想クラッキングを用いたサーバ管理能力向上のための実践的トレーニング概要

本論文に関連して計3回の演習を行ったので、以下に順に説明する。

2.1 第1回目演習

第1回目演習の概要は以下の通りである。

2.1.1 日時

2004年8月30、31日 午前10時～午後11時

2.1.2 被験者

合計4人。2人組のペアを形成し、うち1人がサーバの破壊を担当（以下、「破壊担当者」という）し、もう1人がサーバの修復を担当（以下、「修復担当者」という）するというチームを2つ（便宜的に2チームを、それぞれ「Aチーム」「Bチーム」とする）作った。

破壊担当者は共に学生であり、数ヶ月程度のサーバ管理教育を受けている。一方修復担当者は共に社会人であり、うち1人（Aチーム所属）は企業において約1年半にわたるサーバ管理教育を受けている。もう1人（Bチーム所属）は、計算機にLinuxOSをインストールしウェブサーバを構築した経験があるものの、サーバ管理教育を受けていない。

2.1.3 被験者のタスク

本演習の前提として、修復担当者はOS(RedHat Linux9.0)をサーバにインストールし、HTTP、PHP、MYSQL等からなる簡易アプリケーションを構築しておく(ちなみにAチームはスケジュール管理システム、BチームはXOOPSシステムである)。

破壊担当者のタスクは、正常稼動しているサーバを事前に破壊して正常稼動しない状態にし、演習(サーバ修復）中に、修復担当者からの質問に答えることである（修復担当者の解答に資するようアドバイスするのであり、解答を直接伝えてはいけない)。

一方修復担当者のタスクは、正常稼動していないサーバを正常稼動させ、簡易アプリケーションを正常稼動させることである。修復担当者は参考書等の持ち込みは可であり、また別の計算機を使用してインターネット上の情報を参照することも可であった。しかし、別のサーバの設定ファイルやログの内容を直接参照するのは不可であった。

参考までに、Aチームのサーバの破壊内容を示す。

課題	破壊内容→理由・原因
1	OSが正常に起動しない→/etc/fstabの/（ルート）部分にコメントが付加されたため
2	「ls」コマンドが使用できない→コマンドの内容が改ざんされたため（名前が「wk」に変更された）
3	OSが正常に起動しない→/dev/nullが壊され、そしてパーミッションが変更されてため
4	HTTPが正常稼動していない→httpd.confで、Document Rootが変更されたため
5	スケジュール管理システムが正常稼動しない→/etc/php.iniのパーミッションが変更されたため
6	Document Rootにあるindex.htmlをブラウザで参照することができない→httpd.confで、不要なアクセス権限(.htaccess)が設定されたため
7	インターネットへアクセスすることができない→Eth0がifdownされたため
8	簡易アプリケーションである、スケジュール管理システムが正常稼動しない→DB(mysql)のルートパスワードが初期化されたため
9	コマンドの履歴が表示されない→/etc/profileのHISTSIZEとHISTFILESIZEの数値が変更されたため
10	HTTPが正常稼動していない（ファイルを参照できない）→httpd.confで、 ①デフォルトの80番ポートではなく、8080番ポートを使用するよう変更したため ②Document Rootのパーミッションが変更されたため
11	簡易アプリケーションであるスケジュール管理システムで、ユーザ削除のページに認証がかかっていない→httpd.confで、アクセス権限(.htaccess)の設定が解除されたため
12	簡易アプリケーションであるスケジュール管理システムで、DBにアクセスできない→/etc/php.iniの設定が書き換えられたため（「1」となるべき箇所が、「l」になっていた）
13	HTTPが正常稼動しない→/root/bash_logoutに不要な記述があり、9月になるとlogoutする都度Document Rootのパーミッションが「000」となるため
14	「ps」コマンドを使用すると、サーバが再起動する→/root/bashrcのaliasにreboot処理が追加されたため
15	「su」コマンドを使用できない。一般ユーザでログオンできない→/bin/bashのパーミッションが変更されたため
16	/etc/passwd,/etc/shadowのパーミッションが変更さ

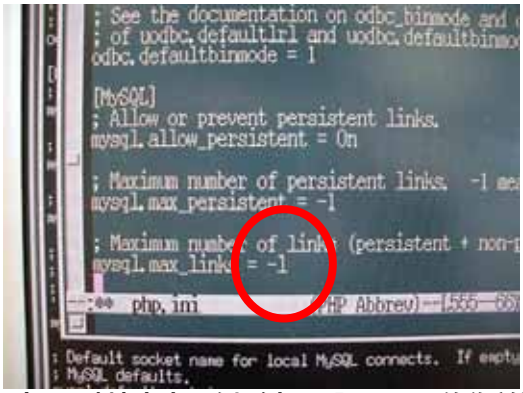
	れていることを発見→同左
17	HTTPが正常に稼動していない→crontab上に不必要な設定があり、9月中16時になると、httpdがストップしていたため
18	CDROMをマウントすることができない→/etc/fstab上の設定が変更されたため
19	80番等、主要なポートへのアクセスが拒否されている→FirewallがHighに変更されたため
20	メモリを128Mとして認識しているため、処理が遅くなる→/boot/grub/grub.confが変更されたため
21	サーバを再起動するたびに、HTTPが正常稼動しなくなる→9月に計算機再起動の都度、/etc/init.d/httpdのパーミッションを書き換えるよう、/etc/rc.sysinitへスクリプトを埋め込んだため

(表1、Aチームのサーバの破壊内容とその理由・原因)

2.1.4 結果

2日間の演習を通じて、Aチームの修復担当者は21問中、課題19～21を除く18問の破壊箇所を発見し修復した。Bチームの修復担当者は、15問中13問の破壊箇所を発見し、そのうち12問を修復した。

A・Bチーム共、短時間のうちに複数の破壊箇所を発見して修復するという局面もあったが、一つの破壊箇所の発見と修復に長時間を要するケースが散見された。例えばAチームの修復担当者は、課題3・12の発見と修復に、それぞれ数時間ずつ要した。



(写真1、破壊内容の例(表1の課題12。修復前))

2.2 第2回目演習

第2回目演習ではサーバを破壊する上でのコンセプトを明確にし、より短時間で破壊箇所の発見や修復が可能となるよう課題設定を工夫した。また演習を2部構成とし、破壊・修復担当者を総入れ替えすることで(従って2部いずれにも参加した者は、破壊担当と修復担当を1回ずつ経験することになる)、被験者のスキルアップにどのように繋がるか調査した。

第2回目演習の概要は以下の通りである。

2.2.1 日時

第1部：2004年9月30日 午前10時～午後7時
第2部：2004年10月27日 午前10時～午後5時

2.2.2 被験者

第1部の被験者は8人。4人組を形成し、うち2人が破壊担当者となり、残りの2人が修復担当者となるチームを2つ作った(便宜的に2チームを、それぞれ「Aチーム」「Bチーム」とする)。破壊担当者4人は学生2人と社会人2人であり、学生は共に数年程度のサーバ管理教育を受けている。社会人は、約1年半にわたるサーバ管理教育を受けている者1人と、サーバにLinuxOSをインストールしてウェブサーバを構築した経験があるものの、サーバ管理教育を受けていない者1人である。修復担当者は共に学生であり、1年程度のサーバ管理教育を受けている。

一方、第2部の被験者は6人。2人組を形成し、うち1人が破壊担当者となり、残りの1人が修復担当者となるチームを3つ作った(便宜的に3チームを、それぞれ「Cチーム」「Dチーム」「Eチーム」とする)。破壊担当者はいずれも学生であり、皆、1～2年程度のサーバ管理教育を受けている。修復担当者は学生2名と社会人1名であり、学生については数年程度のサーバ管理教育を受けている。そして社会人については、約1年半にわたるサーバ管理教育を受けている。

2.2.3 被験者のタスク

第1部については、修復担当者数と解答数との関係について整理するため、原則として上記2.1と同一の課題を設定した(ただし、一部省略した課題あり)。ただしOSインストールと簡易アプリケーション構築は行っていない(代わりに、サーバの設定を修復担当者に事前に見てもらうという機会を設けた)。

次に第2部であるが、演習の前提として、OS(FedoraCore2)インストール済の計算機があり、HTTPが稼動している。破壊担当者のタスクは、上記2.1同様、正常稼動しているサーバを事前に破壊して正常稼動しない状態にすると共に、演習(サーバ修復)中に修復担当者からの質問に答えることである。

一方、修復担当者のタスクは、正常稼動していないサーバを正常稼動させ、HTTPからなる簡易アプリケーションを正常稼動させることである。参考書等の持ち込みを許可すること等の修復担当者の制約については、上記2.1.3と同様である。

(写真2、第2回目演習の様子(その1))

2.2.4　結果

まず第1部であるが、Aチームの修復担当者は19問中18問の破壊箇所を発見して修復し、Bチームの修復担当者は12問全ての破壊箇所を発見して修復した。

一方第2部であるが、C・D・Eチームの修復担当者は、それぞれ14問中13問・14問全て・10問全ての破壊箇所を発見して修復することができた。

2.3 第3回目演習

これまでは主として学生を対象にした演習を行った。彼らは皆、研究目的でサーバ管理者業務を行っているわけであるが、社会人、すなわち実務の一環としてサーバ管理者業務を行っている（又は、今後行う可能性がある）者を対象にすると、これまでとは異なった結果が出る可能性がある。そこで、主として社会人を対象にした演習を行うこととした。

また過去2回の演習では、修復担当者へのアンケートを行っていない。彼らの定性的な意見を把握するため、今回アンケートを配布して回答してもらった。

第3回目演習の概要は以下の通りである。

2.3.1 日時

2005年6月29日 午後6時30分～午後9時

2.3.2 被験者

合計7人。本演習では1人が破壊担当者となり、残りの6人が修復担当者となった。修復担当者は2人組のペアを形成し、チームを3つ作った（便宜的に3チームを、それぞれ「Aチーム」「Bチーム」「Cチーム」とする）。3チームとも同一の破壊内容とし、破壊担当者が3チーム全ての破壊作業を担当した。

破壊担当者は学生であり、1～2年程度のサーバ管理教育を受けている。修復担当者は社会人5人と学生1人であり、それぞれ以下のような教育を受けている。

Aチーム：サーバ管理教育5年以上の社会人1人とサーバ管理教育1年未満の社会人1人
Bチーム：サーバ管理教育を受けていない社会人2人
Cチーム：サーバ管理教育を受けていない社会人1人とサーバ管理教育1年未満の学生1人

ちなみに、サーバ管理教育の未経験者がいること等も考慮し、事前に2時間半をかけてOSやUNIXコマンドに関する講義を行った。

2.3.3 被験者のタスク

演習の前提として、OS(RedHat Linux9.0)がインストールされた計算機があり、HTTPが稼動している。

破壊担当者のタスクは、上記2.1、2.2と同様、正常稼動しているサーバを事前に破壊（具体的には、ウェブページの改ざん）して正常稼動しない状態にすると共に、演習（サーバ修復）中に修復担当者からの質問に答えることである。

一方、修復担当者のタスクは、正常稼動していないサーバを正常稼動させ、そして改ざんされたウェブページを正しく表示することである。参考書等の持ち込みを許可すること等の修復担当者の制約については、上記2.1.3、2.2.3と同様である。

2.3.4 結果

全部で8問の課題を設定したが、各チームが発見し修復した破壊箇所は、以下の通りである。

Aチーム：8問、Bチーム：5問、Cチーム：5問

2.3.5 修復担当者へのアンケート結果

本演習では、修復担当者6人へのアンケートを行った。主な結果は以下の通りである。

2.3.5.1 Linuxやネットワークの理解への寄与

アンケートの結果は、以下の通りである。修復担当者の83%が、本演習が「役立った」と回答している。

（質問）演習は、Linuxやネットワークに関する理解を深めるために役立ちましたか？
（回答）役立った　　4人（66%）
　　多少役立った　　1人（17%）
　　何ともいえない　1人（17%）

主な理由は以下の通りであるが、修復担当者のサーバ管理に関するスキルが様々であったことを考慮すると、本演習はサーバ管理教育の未経験者だけではなく、経験者にも一定の効果を与える演習であるといえる。

- （「役立った」と回答した者）忘れていたコマンドなどを再認識できたから
- （同上）自社のサーバの現状について、とても不安を覚える程役にたった

2.3.5.2 実務への応用の可能性

アンケートの結果は、以下の通りである。修復担当者の83%が、「本演習で得られた知識を、実務（業務・研究）に応用できる」と回答している。

（質問）演習で得られた知識を、実務に応用できると思いますか？

（回答）思う　　5人（83%）
　　思わない　1人（17%）

主な理由は以下の通りであるが、本演習を通じて、システムやネットワークに関する勉強を継続したいとの回答が寄せられたので、本演習は学習意欲を高める効果があるものと考える。

- （「思う」と回答）自社でウェブサーバを数十台管理しており、類似した作業を行っているため
- （同上）現在学生で、自分の研究には直接応用できないが、システムやネットワークの仕組みに興味が湧いたので、是非勉強を継続したい

2.3.5.3 企業や教育機関における情報セキュリティ教育の一環として、本演習を取り入れることの是非

選択肢として「賛成」「反対」「何ともいえない」の3つを用意したが、修復担当者全員が「賛成」と回答した。その理由としていくつか意見が寄せられたが、要約すると「周辺システムに緊急事態が発生した際の対処法を修得できた」ということであった。

続く第3章では、3回の演習を踏まえた考察を行う。

3．考察

3.1 修復担当者の立場

3.1.1 修復担当者数と解答数との関係

第1回目演習では修復担当者は1人であったが、第2回目演習（第1部）では修復担当者が複数存在していた。修復担当者が複数存在すると、お互い相談して修復したり、作業を分担することができる。第2回目演習での正解率はほぼ100%となったが、修復担当者が複数存在したことがその理由として考えられる。

3.1.2 サーバ管理上必要な「勘所」の体得

最近のOSは、インストール用のCDROMを計算機に差し込み、そしてグラフィカルモードを使用して初心者でも簡単にインストールすることができる。グラフィカルモードでの操作が増えると、相対的にテキストモードでの操作が減少する。最近は設定ファイルですらグラフィカルモードで参照・変更できるものが多い。本演習により、設定ファイルが物理的にどのディレクトリに存在するか、どのような設定ファイルから調査に着手すればよいかという、いわゆるサーバ管理上の「勘所」を体得できると考える。

3.1.3 普段使用しないコマンドを使用すること

サーバ上で何らかの処理を行う時、その方法は必ずしも一つとは限らない。例えばUNIXでファイル参照するコマンドで考えても、「more」「cat」「tail」を使用するという選択肢がある。従って、ある特定のコマンドを憶えた場合類似するものを憶えようとせず、既知のものを代替することが考えられる。

しかし表1の課題2・14のようにコマンドが使用不能となった場合、必然的に類似するコマンドの有無を調査し、存在すればそれを使用することになる。こうした作業を繰り返すことにより、普段あまり使用しないコマンドを憶えることができる。

3.2 破壊担当者の立場

3.2.1 破壊担当者と修復担当者の入れ替え

従来の教育手法では、教える側と教わる側が固定するケースが多い。第2回目演習では、破壊担当者と修復担当者を入れ替えるという実験を行ったが、本手法では、教える側と教わる側を臨機応変に入れ替えることができる。これにより、お互いに相手がどのようなファイルの改ざんに関心を持っているのか理解できる。またサーバの修復を担当するだけでなく攻撃を担当する機会を与えることで、「自分ならどのように行動するか」ということを意識するようになり、結果として各種設定ファイルやログの重要性を認識することに繋がったと考える。インターネット経由での攻撃・侵入者の行動を事前に予測して対処することに繋がるので、非常に実践的なトレーニング手法である。

従来の一方的な講義形式や、教材やインターネットを使った自習形式ではなく、本演習のように立場を随時入れ替えてお互い刺激し合いながら学ぶという方式も、トレーニング手法として重要である。

3.2.2 攻撃担当者のスキルの再確認

第2回目演習の第1部で修復を担当し第2部で破壊を担当した者から、「事前準備が大変であったが、非常に勉強になった」との意見が寄せられた。この理由として考えられることは、次のようなことである。

攻撃担当者は事前に破壊内容を検討してその作業を行い、そして意図通りに修復することができるか検証する。しかし演習本番中に修復担当者から様々な質問が寄せられるので、そのための対策として、サーバに関する知識をリマインドするための事前学習、すなわち想定問答を行ったということである。

修復担当者から寄せられた質問に対し、攻撃担当者が即答するのはいとも簡単であり、解答を導くような「上手な」ヒントを提供するのは案外難しい。無意味にサーバの設定ファイルを参照することを防ぎつつ破壊箇所に辿り着くまでに何をしてもらうべきかを考えることは、攻撃担当者自身のサーバスキル向上に無意識に繋がっているものと考える。これ

は大変興味深く、本手法の本質を表している。
　修復担当者だけでなく、攻撃担当者のスキルを再確認できるという点でも本手法は効果的である。

3.3 その他

3.3.1 演習時間と予習

　これまで3回の演習を行ってきたが、演習時間は2時間半から2日間まで様々であった。破壊担当者からのヒントの提示は必要最小限にすべきであり、できるだけ修復担当者が独力で破壊箇所を発見し修復するのが望ましい（その方が、達成度・理解度共に大きい）。従って、可能であれば1日程度の時間をかけて演習すべきである。
　また、できれば演習に先立ちOSやUNIXコマンド等に関する予習を行うのが望ましい。サーバ管理教育未経験者の場合、演習の理解度が高まると考える。

3.3.2 本物の攻撃者の視点取り入れの必要性

　サーバ管理に関する初心者の場合はともかく、一定レベル以上の者を演習対象とする場合、すぐに破壊箇所が発見されるような設定は避けるべきである。
　またこれまでの演習では、重要なコマンドを分かり易く置き換えたような、いわゆる「間違い探し」的な課題が多かった。今後はより本物の攻撃者の視点での内容にすると、サーバの破壊・修復担当者双方にとってスキル向上につながるものと考える。

（写真3、第2回目演習の様子（その2））

3.3.3 破壊箇所に関する調査方法

　第2回目演習の第1部では、サーバの設定を修復担当者に事前に見てもらう機会を設けた。ところが修復担当者の中にデジタルカメラを持参して、ディスプレイに表示されたサーバ内の様々な設定ファイルに関する画面キャプチャを取得する者がいた。破壊前後の画面キャプチャを比較して、どのファイルのどの部分が破壊されたかを容易に把握できるようにするのが目的であるが、これは当初我々が予想していなかった方法である。演習の都度新たな発見があるのも、本手法の特徴である。

　続く第4章で本論文の結論を述べ、その後第5章で今後に向けた課題を述べる。

4．結論

　何者かにサーバを攻撃された場合、「サーバを一度停止し、初期化した上で再設定すればよいではないか」ということになるケースがある。しかし企業の場合、同様の対応を取るのは難しい。
　今回、仮想クラッキングを用いたサーバ管理能力向上のための実践的トレーニング手法について提案した。言い換えれば、サーバが仮想的にクラッキングされた状態を作り出してその修復を図るというものであるが、これによりサーバ管理能力が向上したという定性的効果が得られたので、非常に実践的な教育プログラムであるといえる。
　また本手法を通じて、サーバ管理教育未経験者だけでなく、経験者にも一定の効果があるという結果が得られた。また、「面白い」という好意的反応も寄せられた。情報セキュリティに関する人材育成並びにサーバ管理教育の一環として、本手法を取り入れることを提案する。

5．今後の課題

　今後の課題として大きく2点挙げられる。
　1点目は、「破壊内容」の体系化である。これまで演習を重ねてきたことにより、大量の「破壊内容」が存在している。これを整理し、例えば「ログ参照方法に関する項目」「基本コマンドの使用に関する項目」というような「破壊内容」の体系化を図りたい。これにより、被験者の弱点部分だけを重点的に補強することも可能になる。
　2点目は、アンケートの充実である。第3回目実験において修復担当者からのアンケートを行ったが、絶対数が少ない。今後も演習を重ねてアンケート数を増やしていくほか、被験者のスキル向上の達成度合いを捉えるため、同一被験者を対象にして演習を複数回実施していくことにも挑戦したい。
　最後に、演習実施にあたりご協力頂いた岐阜県立国際情報科学芸術アカデミーの吉田茂樹教授と神成淳司講師に厚く御礼申し上げる。

参考文献

[1]佐々木良一,“情報セキュリティハンドブック”,電子情報通信学会,pp477-487(2004.11)
[2]“セキュリティ甲子園の開催について”,経済産業省(2003.7),
http://www.meti.go.jp/kohosys/press/0004211/0/030702seculity.pdf
“PCWEB総合ニュース”,MYCOM(2004.6),
http://pcweb.mycom.co.jp/news/2004/06/15/012.html