Oct. 17, 2005
Keynote, Black Hat

The Day After . . .

Institute of Information Security

Associate Professor

Katsuya Uchida (uchidak@gol.com)

Black Hat Japan 2005

簡単な自己紹介

- **1980年代初** 米系銀行の内部監査部門で、システム監査、業務監査を行った。 セキュリティを本格的考え始めた
- **1990年代**: 損害保険会社で情報セキュリティ関連業務を担当
- **1993年～**: 93年にCSI (Computer Security Institute) Conference 始めて参加 (最近は、6月：NetSec、11月：Annual Conferenceの両方に参加)
- **2002年～**: 中央大学21世紀COE「電子社会の信頼性向上と情報セキュリティ」推進担当者 (2007年3月まで：予定)
- **2003年～**: 中央大学「情報セキュリティ人材育成」プロジェクト (文部科学省) (2008年3月まで：予定)
- **2004年～**: 情報セキュリティ大学院大学

その他

- 日経新聞社デジタルコア：定期コメンテータ
- ISMS審査判定機関：審査判定委員会委員長
- サイバーセキュリティマネジメント (雑誌) 編集委員

この様な経験から情報セキュリティを考えています

Black Hat Japan 2005

The Day After ・・・

愚者は経験から学び、賢者は歴史から学ぶ

Fools say they learn from experience; I prefer to learn from the experience of others.

- ＡＲＰＡＮＥＴが生まれ、既に４０年近い月日が経った。その間に多くの事が起こっている。
- ドイツの宰相ビスマルクは「**愚者は経験から学び、賢者は歴史から学ぶ**」と言っており、中国の思想家孫子は「**敵を知り己れを知らば、百戦して危うからず**」と言っている。
- 最近、サイバースペースにおけるインシデント等を振り返ってみることも大切なのではないかと考えている。

Katsuya Uchida (uchidak@gol.com)
情報セキュリティ大学院大学

The Day After ・・・

Jurassic Park（? Zerox PARC）での実験

- バンパイア（Vampire）プログラムは、昼は活動せず、夜に稼働していないコンピュータを探し、複雑で時間のかかる処理をそのコンピュータで動かし、朝になると処理過程を保存し、活動を休止し、夜が来るまで待った。
- しかし、**プログラムが誤動作**し、朝、全てのコンピュータがクラッシュしており、コンピュータを再起動すると、バグがあるプログラムが**再度コンピュータをクラッシュ**させた
- このプログラムは、ワーム（Worm）とか「**ゼロックス・ワーム**」と呼ばれた。
- 研究者らはこの**ワームの活動を監視する「ワームウォッチャー」プログラムを作成**し、ワームがある限界を超えた場合には、ワームの活動を停止させるプログラムも作成した。

1970末 Katsuya Uchida (uchidak@gol.com)
情報セキュリティ大学院大学

The Day After ・・・

チューリング賞受賞者 Ken Thompsonの裏口 (Backdoor) 作り

- ThompsonはUNIXの ”login” コマンドで、不正なloginコマンドを持つCコンパイラをコンパイルして作成した。 このため、このCコンパイラは、通常のユーザ以外にThompson自身もユーザとしてログインできた
- コンパイラのソースコードから、不正な仕掛けを削除してコンパイルすれば、不正な仕掛けを除去できるが、コンパイラを再コンパイルするにはコンパイラが必要になることを利用し、Thompson は更に新しい仕掛けを作り、コンパイラが自分自身をコンパイルする場合でも、loginコマンドでThompsonがログインできるようにした
- このコンパイラはThompsonの作成した仕掛けを複製していくことになる。実際に初期のCコンパイラには、この機能が残ったものがリリースされ、ログインできたと言われている
- Thompson自身はこのようなプログラムをvirusとは命名しなかったが、自己増殖機能を持ったプログラムを作成した

The Day After ・・・

Bitnetでの悪戯 (CHRISTMA exec)

(Because It's Time Network)

- 1987年12月に広がったワームは、構造化プログラミング言語レックス (REXX) を利用し、「CHRISTMA execワーム」と呼ばれた
- 全世界を繋いでいたIBM社内のネットワークやIBMの大型コンピュータを利用していた大学や研究機関のネットワーク BITNETを混乱させた
- このワームは本来の機能である自分自身を電子メールを送る機能を隠し、電子版のクリスマスカードであると偽ったプログラムで、実際は「トロイの木馬」プログラムである
- このプログラムが添付されていた電子メールを受け取り、クリスマスツリーを画面上に描くプログラムを実行すると、このユーザのアドレス帳にある全ての人にこのメッセージを送った。
- 多くの人がこのプログラムを実行したため、多くのユーザがこのワームを受け取り、ネットワークに多大な負荷をかけた

The Day After ・・・

史上最大のDDoS攻撃
Internet Worm *or* Morris Worm

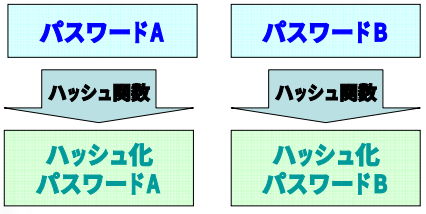
事件の概要

- 1988年11月2日 当時、コーネル大学の大学院生であったロバート・タッパン・モーリス・ジュニア (Robert T. Morris Jr.) は、SUN-3とVAXコンピュータのBSD 4.2及び4.3版の脆弱性を利用したプログラム (ワーム) を作り、インターネットに流した
- UNIXのユーザID／パスワードファイル (/etc/passwd) を利用してパスワード解読した。当時のUNIXでは、パスワードファイルは誰でも見る (読み出す) ことができた。 このファイルは暗号化されていたため、パスワードを推測することは不可能であると考えられていた。 パスワードを暗号化には、一方向関数 (ハッシュ関数) が使われており、暗号化されたパスワードから元のパスワードを復元 (解読) できないと考えられていた
- UNIXのfingerdプログラムはバッファ・オーバーフローを引き起こすgets()関数を使っており、バッファ・オーバーフローを利用して、管理者 (ルート) 権限を得ることができた
- sendmailのDEBUGコマンドを利用し、他のコンピュータにプログラムを送付
- インターネットの接続されていたコンピュータの約10%、6000台が被害を受けた

The Day After ・・・

史上最大のDDoS攻撃
Internet Worm *or* Morris Worm

- ハッカーの常識 (セキュリティ専門家の非常識？)
  - ハッシュ関数では、ハッシュ化後のパスワードを元のパスワードに戻せない
  - あるパスワードをハッシュ化し、ハッシュ化後のパスワードと同じものであれば、パスワードは同じ！



ハッシュ化パスワードAと
ハッシュ化パスワードBが
同じならば

パスワードAとパスワードB
は同じ

The Day After・・・

史上最大のDDoS攻撃
Internet Worm or Morris Worm

パスワード攻撃に対する考察：Morris Jr.のパスワード攻撃からの教訓

金融機関のキャッシュカードは、盗難カードを利用してATM等でパスワードを類推しても、数回誤った暗証番号を入力するとカードが利用できなくなります。 この方法はATM等の機器を利用する場合には、非常に有効な方法ですが、ネットワーク上では常に有効でしょうか。

- ネットワーク上では、口座番号等とパスワードを入力しなければなりませんが、当然ながら口座番号とパスワードが正しくなければログイン等ができません。
- この方法では、同一口座番号に対して、ATMと同様パスワードを数回誤って入力した場合、ログインをロックする方法を採用している場合があります。 しかしながら、ログインをロックする方法は、ロック解除のため、コールセンター等で対応する必要があるため、時間・費用の問題があり、金融機関・利用者とも避ける傾向があります。
- 口座番号とパスワードを間違えたら、一定時間ログインをできない方法で安全を確保していますとおっしゃる方がおります。
- もし、ある金融機関の口座番号の仕組みがある程度推測できた場合、口座番号を変化させ、同一のパスワードを入力する方法で、口座番号とパスワードを推測する攻撃者がいたらどうでしょうか。 一定時間ログインできない仕組みが適用できるでしょうか？

Katsuya Uchida (uchidak@gol.com)
情報セキュリティ大学院大学

The Day After・・・

史上最大のDDoS攻撃
Internet Worm or Morris Worm

- **バッファーオーバーフロー**
  - 未だに完全には解決していない (かなり対応ができてきたが・・・)
  - 根本的な解決方法を考える必要があるのでは？
- **緊急連絡先**
  - この事件を契機にCERT/CCが作られた
  - 電子メールだけで、連絡が可能だと思っていたが、電子メールが利用できなかった。 CERT/CCは、4つの手段で連絡を取れるようにしている。
  - 緊急時対応では、どの手段が利用できなくなるか分からないとしたら・・・

CERT/CC Contact Information
- Email: cert@cert.org
- Phone: +1 412-268-7090 (24-hour hotline)
- Fax: +1 412-268-6989
- Postal address:
  CERT Coordination Center
  Software Engineering Institute
  Carnegie Mellon University
  Pittsburgh PA 15213-3890 U.S.A.

Black Hat Japan 2005
Katsuya Uchida (uchidak@gol.com)
情報セキュリティ大学院大学

The Day After・・・

どこまで先を読むのか
CodeRed Worm

- 2001年はワームが数多く出現した年
- Nimdaは史上最悪のワームと言われた・・・
- Code Red
  - Windowsの脆弱性を利用して感染を広げる
  - ＤＤｏＳ攻撃を目的とし、感染コンピュータはDDoS攻撃用の兵隊になった
  - 攻撃目標は米国ホワイトハウスと決められていた
  - 今までは、DDoS攻撃の兵隊は手作業で作成していた
  - DDoS攻撃の兵隊を自動化した点は今後非常に大きな問題になるのではないか？
  - 攻撃目標を外部から与えることができれば、非常に大きな脅威になるのでは？
  - 現時点の脅威より、今後の脅威を考える必要があるのではないか？

2001年の主なワーム
- 3月 - Lion
- 4月 - Lpdw0rm
- 6月 - Adore
- 6月 - Leaves
- 7月 - SirCam
- 7月 - Code Red
- 8月 - Core Red II
- 9月 - X.c
- 9月 - Code Blue
- 10月 - Nimda

Trends and Predictions of Worm Techniques
By Ryan Russell (Security Focus)

Katsuya Uchida (uchidak@gol.com)
情報セキュリティ大学院大学

The Day After・・・

ロッキード事件とＳＯＸの以外な関係

- ロッキード事件
  - 全日空の新型旅客機導入選定に絡み、1976年2月に明るみになった戦後の日本を代表する大規模な汚職事件で、前内閣総理大臣 田中角栄が受託収賄と外国為替・外国貿易管理法違反の疑いで逮捕された
  - この事件により、1980年代初めに、米国大手銀行は主要支店に内部統制 (Internal Control) 部門が作られ、コンピュータ監査、業務監査が監査部門 (Audit Dept.) とは別に行われた
- ＳＯＸ (Sarbanes-Oxley Act) 法 (2002年)
  - エンロン、ワールドコム等の米国企業の会計不祥事の続出に対して、米国政府が制定した企業改革のための法律で、「内部統制」の整備・評価を経営幹部に義務づけている

ロッキード事件から２０年経って、
また「内部統制」が必要と言われている

Katsuya Uchida (uchidak@gol.com)
情報セキュリティ大学院大学

The Day After ・・・

Social Engineering
The Knightmare & Kevin Mitnick

- **システム侵入方法**
  - 非常に強固なセキュリティシステムに侵入するのに、最良な方法は従業員に賄賂を贈ることである。(BS7799 Lead Auditor Courseより)
  - 情報システムの最大のセキュリティホールは人間である
  - “Meet the Enemy (ハッカーと語ろう)” by Ray Kaplan at CSI Conference 1994　ハッカーとセキュリティ会議参加者の電話会議で、何気なく入ってきた電話会社のオペレータがハッカーから、自分のユーザID／パスワードを聞き出されてしまった事件が発生
  - IDやパスワードなどのセキュリティ上重要な情報を日常生活の中での盗み聞きやなりすましなどにより不正に入手する

ソーシャルエンジニアリング手法としては、以下のようなものがある

- 電話で利用者や管理者になりすまして、緊急事態を装いIDやパスワードを聞き出す。
- 会話を盗み聞きしたり、システムの利用時に利用者が入力する情報を背後から盗み見る。
- Eメールに記された偽りのURLをクリックさせて、個人情報を入力させる(フィッシング)。
- 廃棄された紙ゴミから情報を読み取る。

The Day After ・・・

Social Engineering
The Knightmare & Kevin Mitnick

国内でのソーシャルエンジニアリング！？

- **昭和56年 (1981年) 10月　H相互銀行事件**
  犯人は、H相互銀行の某支店に「”コムセン”の者だが機械のテストをするからS支店の口座へ3500万円の入金操作をして欲しい」と指示し、預金係主任が本店からの指示と信じて操作を行った。共犯の女性が事前に開設してあった口座に入金がされた時間頃に別のS支店で3000万円を引き出し、騙し取った。
  典型的な「ソーシャルエンジニアリング」手法で、犯人の男は電話で行内で使われる言葉(行内用語)で指示をしたため、支店の預金主任は完全に騙された。
- **昭和60年 (1985年)　某郵便局**
  発生した。郵便局の窓口の係員に「すぐにお金を持ってくるので、この通帳の口座に入金しておいて欲しい」と頼み、それを信じて入金手続きを端末機で行わせ、他の郵便局のATM端末から現金1100万円余りを引き出した。　忙しかったり、顧客が忙しそうにしていると、つい親切に対応することが良いと錯覚してしまう。どんなに切迫している状況の場合でも、どこまでは対応してもよいかを判断できる教育・訓練が必要になる。

The Day After ・・・

米国国防総省の情報
True or Not True

2002年7月、当時の米国大統領重要インフラ保護委員会 の副委員長 ハワード・シュミットは、インタビューで、「米国国防総省（DOD）が行った2001年の調査では、国防総省への攻撃の97～98%の攻撃はパッチ適用をしなかったか、設定ミスである」と述べている。

http://www.govtech.net/magazine/sup_story.phtml?id=18492

Security First

Howard Schmidt, the vice chairman of the president's Critical Infrastructure Protection Board, speaks about the national plan and other cyber security issues. (July 2002)

Q: What kinds of technology will be needed to stave off electronic attacks? Do we need bigger anti-virus programs?

A: The common misconception is this is a technology issue. But it's not a technology issue. For example, the DOD did an analysis last year and it's somewhere in the high 90s, like 97 [percent] to 98 percent of things that have hit the DOD systems have been the result not of some new piece of technology but exploitation of people that have not had processes in place to install patches or to configure their systems properly.

Government Technology

Unauthorized DoD Intrusions
(314 Category 1 & 2 Intrusions as of 1 Jan 2003)

97% Preventable

492 Unauthorized DoD Root- Level Intrusions (as of 31 Dec 2001)

96% Preventable

Katsuya Uchida (uchidak@gol.com)
情報セキュリティ大学院大学

The Day After ・・・

三大噺
CodeRed/Nimda、September 11、Enron/WorldCom

The Past Year - Shaping InfoSec
米国における情報セキュリティへの方向性

参考：企業会計審議会：日本版SOX法（草案）
http://www.fsa.go.jp/news/newsj/17/singi/f-20050713-2.html

Katsuya Uchida (uchidak@gol.com)
情報セキュリティ大学院大学

The Day After ・・・

病気とその治療法

病気に対する治療方法には、通常以下の3つの方法がある。

- **根本療法**： 病気にならないようにすることが大切で、身体を鍛えたり、身体に抵抗力をつけることである。
- **原因療法**： 万一、病気になってしまった場合、病気の原因を取り除くことにより、病気を治す方法である。
- **対症療法**： この方法は、症状を和らげることによるもので、根本的な治療方法とは言えない。あくまでも一時的な方法であり、原因療法、根本療法を行うことができない状況においてのみ利用する方法であり、繰り返し対症療法を行うことは、身体にとって有害なものになる可能性が高い。

The Day After ・・・

情報セキュリティの治療法は？

- 現在の多くの情報セキュリティ対策は、病気治療でいえば、対症療法でしかない。
- AntiVirusソフト、侵入検知システム（IDS）等は、その典型であろう。
- 侵入防止システム(Intrusion Prevention System)等の原因療法的なものも一部でてきているが、根本療法的なものを求めるのは無理だろうか？
- もし、そうだとすると・・・・

The Day After . . .

DARPA(the Defense Advanced Research Projects Agency)の依頼でRAND研究所が実施した研究

http://www.rand.org/publications/MR/MR797/

The Day After . . .

The Day After . . .

The Day After

- 1996.03 DARPA (米国国防総省高等研究計画局) が実施
- 米国の情報セキュリティ基盤を拡充するために必要となる研究開発課案への提言作成
- 約60名の政府、大学、報道などの情報インフラ関係者による約半日の机上演習
- 西暦2000年に起こると仮定された中東危機を背景とし、重要インフラに対してサイバー攻撃の発生を想定

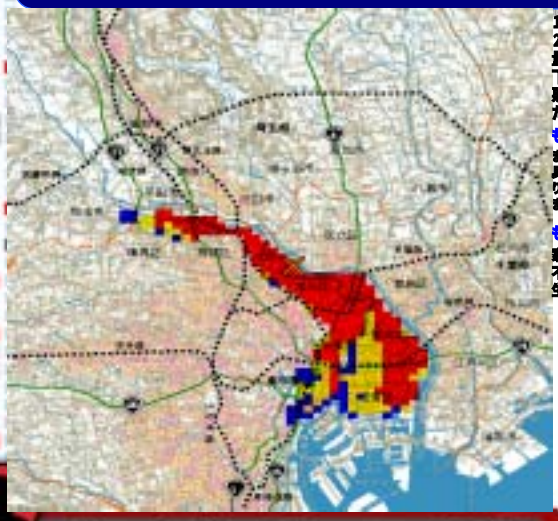
Eligible Receiver

- 1997.06月 NSA (国家安全保障局) が、3カ月の準備期間の後に約2週間の攻撃を実施
- アメリカ国内のすべての電力システムおよび電話のシステムのスイッチを切る方法を見つけること。 国防省の中にあるコンピュータシステムに不正侵入を試みること
- コンピュータネットワークの24時間監視体制の確立。 800あるネットワーク全てにIDSおよびファイアウォールを設置。

Digital Pearl Harbor

- 2002.07 ガートナー／US Naval War Collegeが実施
- 重要インフラへのサイバー攻撃の実行可能性とそれによるダメージの程度を見極める
- 仮想シナリオに基づいて、電力網システム、通信インフラストラクチャ、インターネット、金融サービスのそれぞれに対して、コンピュータセキュリティの専門家が4つのチームに分かれて攻撃手法をを机上で考察

The Day After . . . 自然災害による問題も



1993年に当時の建設省が荒川下流地域で200年に1回程度発生すると考えられる降雨量：「3日間に548mm」があった場合、荒川下流域で破堤が発生すると想定した中の最悪のものが、荒川右岸16．75Kmが破堤した時で、左図はその時の浸水区域を示した

もし2m以上浸水したら・・

まず家屋の1階がすべて水につかってしまい、家財道具などに重大な被害が出ます。また、2階も水につかり、国民の社会・経済活動が壊滅的なダメージを受けます。

もし50cm以上浸水したら・・

家屋が床上浸水します。また、自動車の走行が不可能となるばかりか歩くことも困難になり、市民生活に重大な影響がでます。

浸水深
赤：2．0メートル以上
黄：0．5 ～ 2．0メートル未満
青：0．5メートル以下

全被害状況	
浸水面積	82．8 Km²
浸水区域内人口	1,163,031 人
床下浸水戸数	18,085 戸
床上浸水戸数	456,052 戸
被害額	384,947 億円

阪神大震災の被害金額
10兆円の約4倍に相当

The Day After . . .

次に来るのは、

- The Day After . . . in Cyberspace だろうか？
- 映画「The Day After Tomorrow」で言われているような自然災害だろうか？
- それとも・・・

The Day After ・・・

Questions?

Comments!

Rebuttals・・・

Thank you ！

著作権の関係でプレゼンの
内容と同じではありません。

Institute of Information Security
Katsuya Uchida (uchida@iisec.ac.jp)