

*Oct. 17, 2005  
Keynote, Black Hat*

# *The Day After* ■ ■ ■

**Institute of Information Security**

Associate Professor

Katsuya Uchida ([uchidak@gol.com](mailto:uchidak@gol.com))

**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.

### 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年近い月日が経過している。その間に多くのインシデントが発生している。

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、中国の思想家孫子も「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。

サイバースペースでのインシデント等を振り返ってみるのも必要な時代ではないだろうか？



*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.

- ジュラシックパーク(? Zerox PARC)での実験
- チューリング賞受賞者Ken Thompsonの裏口(Backdoor)作り
- Bitnetでの悪戯(CHRISTMA exec)



*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.

- 史上最大のDDoS攻撃

- ◆ セキュリティの常識を覆したハッカー
- ◆ 未だに解決しないバッファオーバーフロー
- ◆ 緊急連絡先の欠陥



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.

- ボットネットの先駆け

- ◆ どこまで先をみるのか？
- ◆ Ryan Russell (SecurityFocus) への質問



*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.

- **ロッキード事件とSOX法の意外(?)な関係**
  - ◆ 愚者の経験： 20数年前の状況と同じじゃない！
  - ◆ 内部統制 (Internal Control) の世界への誘い



*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.

- The KnightmareとKevin D. Mitnick

- ◆ 行動心理学を学ぼう
- ◆ 根本対応が必要かも？
- ◆ “Meet the Enemy (ハッカーと語ろう)” by Ray Kaplan at CSI Conference 1994



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.

- 三題噺

- ◆ Nimda/CodeRed
- ◆ September 11
- ◆ エンロン／ワールドコム



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.

## ● DoD(米国国防総省)は真実を語っているのか？

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

### Security First

Howard Schmidt, the former chief security officer at Microsoft, 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**



**Black Hat Japan 2005**

*The Day After ....*

## The Day After ...

### The Day After ...

インターネットを始めとしたサイバースペースでは、サイバーテロ等への対応や堅固なネットワークの構築が必要であるとの議論も言われている。

サイバースペースの未来は.....



## The Day After ...

### 病気とその治療方法

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 ....*

## The Day After ...

- ソーシャルエンジニアリングへの戦い
  - ◆ 根本療法は可能だろうか？



**Black Hat Japan 2005**

## The Day After ...

- 原因療法、根本療法への転換
  - ◆ 対症療法での対応はもう限界ではないだろうか？
    - Anti-Virusソフト
    - 侵入検知システム
    - フィルタリングソフト



*The Day After ...*

*Questions?*

*Comments!*

*Rebuttals...*

***Thank you !***

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

**Black Hat Japan 2005**