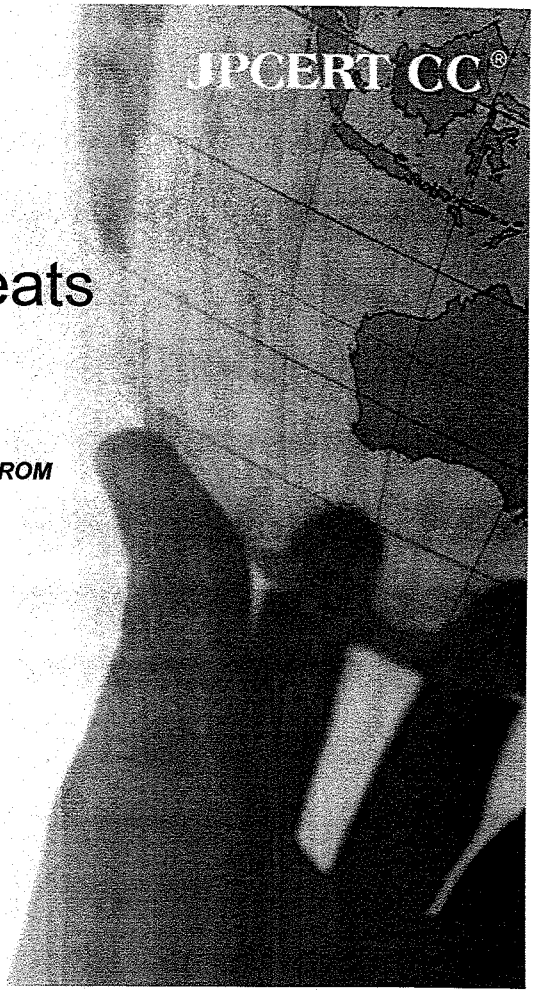



# Information Security Threats Landscape

*2ND APEC SEMINAR ON PROTECTION OF CYBERSPACE FROM TERRORIST USE AND ATTACKS*
*NOVEMBER 18-19, 2008, SEOUL, KOREA*

Koichiro Komiyama, CISSP
JPCERT Coordination Center

## About JPCERT/CC

https://www.jpcert.or.jp/

JPCERT CC®

- JPCERT/CC stands for ...
  - — Japan Computer Emergency Response Team Coordination Center
- Officially established in 1996
- Independent, non-profit organization sponsored by METI (Ministry of Economy, Trade and Industry)
- Coordination and collaboration on Computer Security Incidents with domestic/international organizations
- Issue security bulletins and advisories for Japanese IT professional

## Agenda

JPCERT CC®

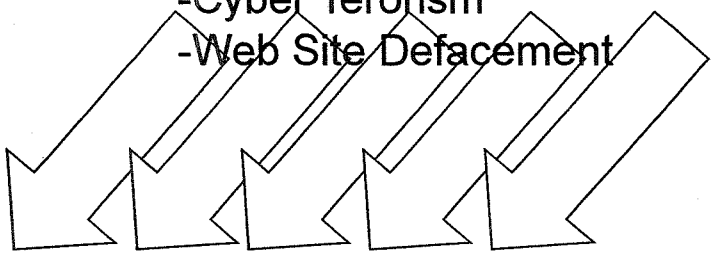
- JPCERT/CC, Who we are.
- Threats
  - —DoS
  - —Bot/Botnet
  - —Targeted Attacks
  - —Vulnerable Control System
  - —New Technology Penetration
    - Twitter
    - BlackBerry
    - Blog
    - Cloud Computing
- Measures
  - —Tsubame (Network Visualizing)
  - —IT Security Inoculation (User Education)




## Change of Tide

JPCERT CC®

We have fought against threats like ...
-Virus/Worm
-DDoS
-Cyber Terorism
-Web Site Defacement

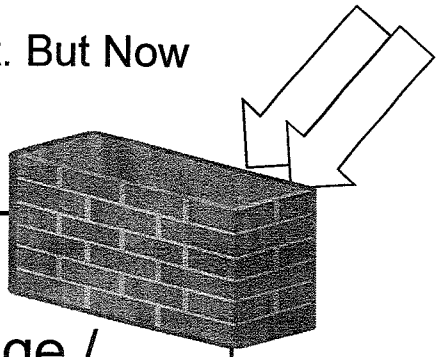


**Government/ Enterprise**

## Change of Tide (cont)

JPCERT CC®

We are protected against external threat. But Now the threats are within us too...



Government/Enterprise

1. Malicious Insiders(IT Sabotage / Theft of Information)
2. Change of Media Technology (e.g. Twitter)
3. Beginners, Less-Educated




JPCERT CC®

Threat 1:

# MALICIOUS INSIDERS

## Insider Threat 1/2

JPCERT CC®

- What is Meant by "Insider Threat?"

> A current or former employee, contractor, or business partner who
>
> - has or had authorized access to an organization's network, system, or data and
> - intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems
>
> **CERT/CC's definition**


- Is it Really a Threat?
  - —31% of E-crimes were committed by insiders (source: 2007 E-Crime Watch Survey)




## Insider Threat 2/2

JPCERT CC®

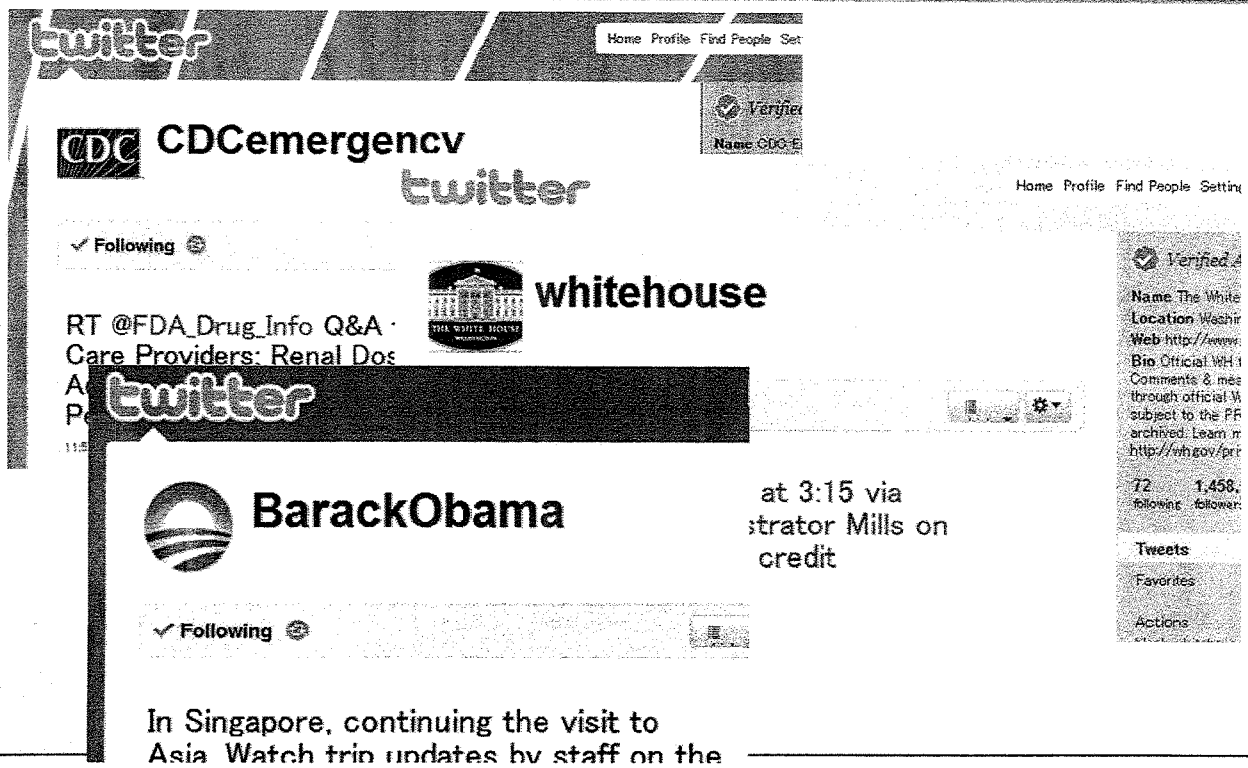
- Category
  - —IT Sabotage
    - Shinsei Bank (2008) : ex-contract employee sneak in corporate network with his credential. Delete more than 2600 files, sneak a peek boss's emails.
  - — Information Theft
    - Japan Ground Self-Defense Force (2009/9) : An officer of JSDF has admitted leaking personal data on 140,000 members, , nearly the entire force, in exchange for 1 million yen($100) in cash.
  - —Misc (Fraud, System misuse)
- Measures
  - —Need to have strict background checks
  - —Consistently Enforce Policies and Controls
  - —Deactivate User Account soon after the termination

Threat 2:

# CHANGE OF MEDIA TECHNOLOGY



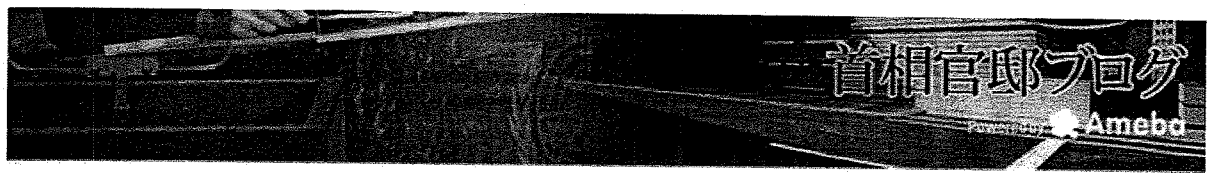


## New Technologies Coming in: Blog Service

JPCERT CC®

- PM starts blogging!




■プロフィール

[ルームを見る]

ニックネーム:首相官邸ブログ

[記事作成・編集]

このブログの読者になる(チェック)

1 | 2 | 3 | 4 | 5 [最初 次ページ≫

2009-11-12

**メコン地域諸国との信頼と絆**

テーマ:鳩山内閣総理大臣

天皇陛下御在位20年を、国民のみなさまとともに、心よりお慶び申し上げます。

いついかなるときも、国民と共に歩み、心をお寄せになられておられる天皇陛下、皇后陛下のご健康と皇室のご繁栄を心からお祈り申し上げます。

＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊

■最近の記事一覧

メコン地域諸国との信頼と絆
中小企業金融円滑化法案について
天皇・皇后両陛下からいただいた勲し
編集部から
強固な日米関係をめざして
行政の大掃除で、コンクリートから人へ
触れ合い、慰霊、勲し…… 全力で取り組まれた20年
編集部から
新しい国づくり
新型インフルエンザ対策について

[一覧を見る]





## New Technologies Coming in: Youtube

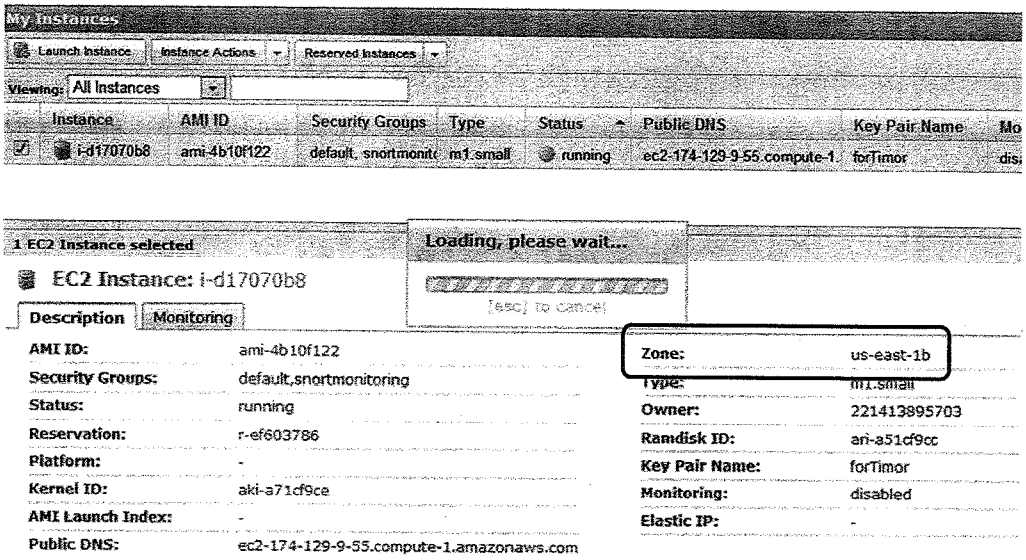
JPCERT CC®

- MoFA minister's press briefings are uploaded on Youtube immediately after.
- Ministry of Health, Labour and Welfare , Ministry of Defense , Ministry of Justice , Ministry of Foreign Affairs

## New Technologies Coming in: Cloud Computing

JPCERT CC®

- I have my own server on Amazon EC2!
- Though I don't know where my confidential information is …



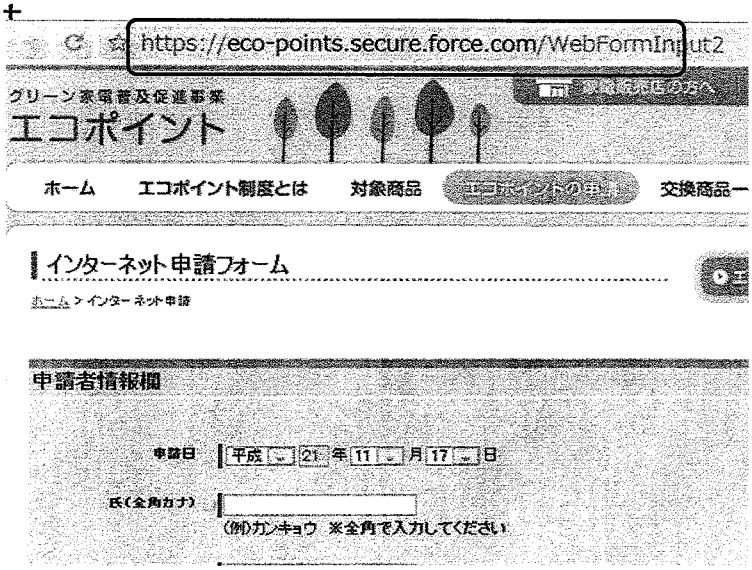




## New Technologies Coming in: Cloud Computing

JPCERT CC®

- First government web service which powered by Salesforce.com was launched (2009/7)
- Ask users to input
  - Name
  - Address
  - Phone number



- Government/CIP need services like twitter, blogs and Cloud Computing Service
  - relatively low in price
  - Better performance, functions, usability
- We should consider about risks arise with them.
  - Those services are not under our control
  - Where those server are located? (Does Japanese Law have any effect there?)

- Measures
  - Keep up to new technologies/services
  - Update policies






Threat 3:

# BEGINNERS, LESS-EDUCATED

# Beginners, Less-Educated

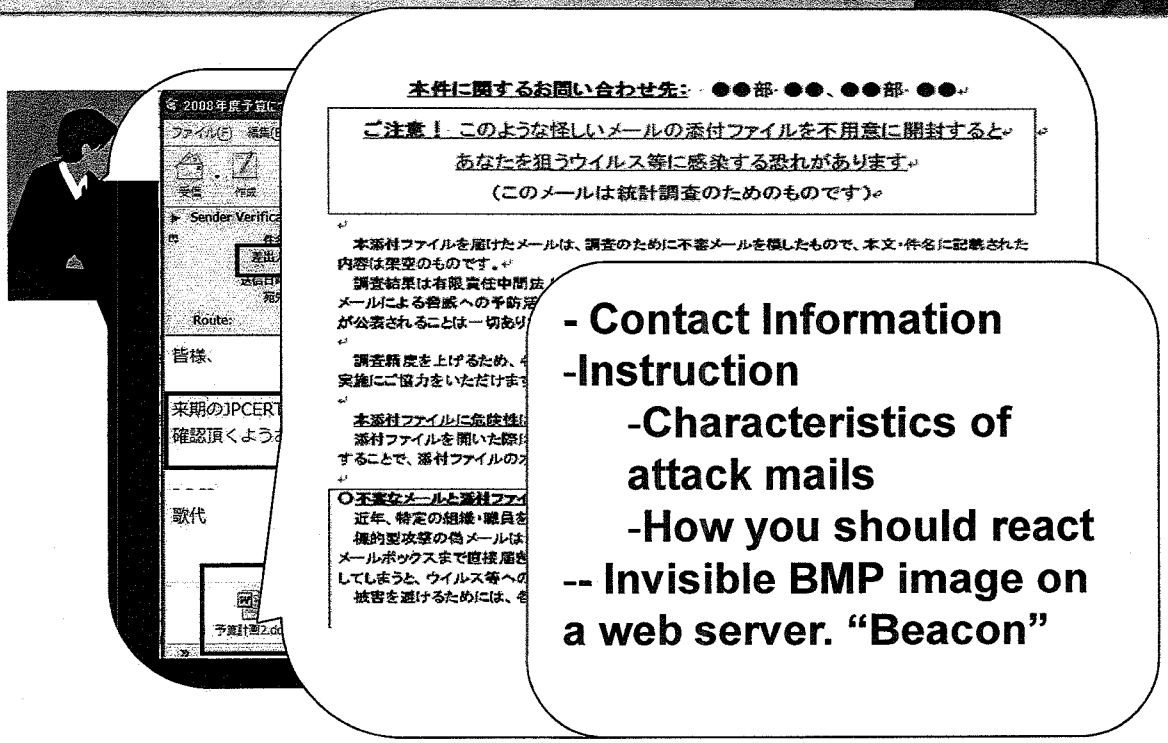
JPCERT CC®

- Target Trojan Attacks are steadily increasing
  - customized message for few recipients
- How to prevent employee opening those malicious attachment?
- Inoculation!
  - What is Inoculation?
  - An exercise to raise awareness toward mail attacks such as targeted attacks/phishing. Users receive fake targeted attack mails with attachment which does not harm their computer.



# Inoculation How it works.

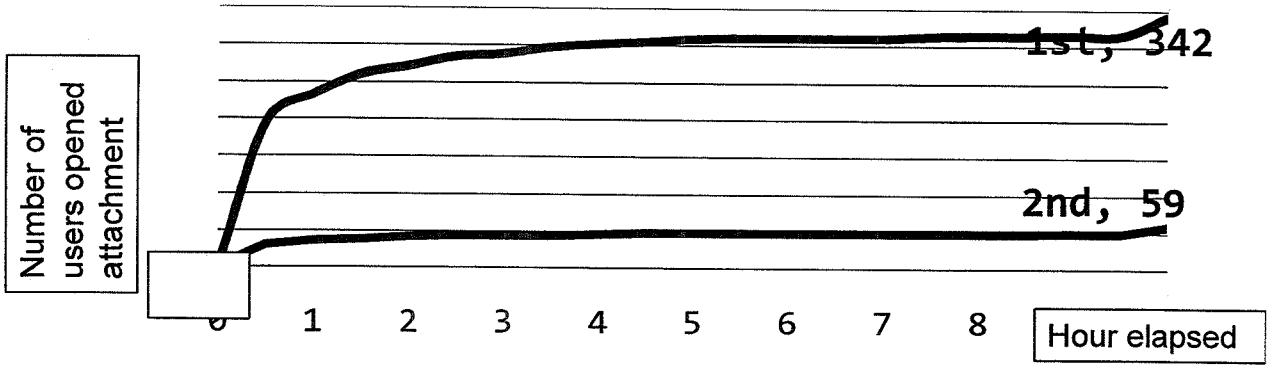
JPCERT CC®



## Inoculation: What we learned

JPCERT CC®

- 14 Companies from 8 industries, 2600 recipients
- 44.0% of users opened suspicious attachments the 1st time. The rate went down to 13.0% in the 2nd time.
- More than 50% of users who opened the attachment responded within 30 minutes of the beginning.






## Summary

JPCERT CC®

1. Threats exist inside our organization as well.
2. Economic crisis accelerated government/CIP using twitter, Youtube, cloud computing.
   - Used to be conservative to adopt new tech.
3. User education is key to build secure organization. The inoculation raised user awareness against targeted attack/phishing. IT reduced rate of suspicious mails being opened.

- Email : office@jpcert.or.jp
- Tel: +81-3-3518-4600
- Fax: +81-3-3518-4602
- https://www.jpcert.or.jp

## Incident Report

- Incident Reporting Form
  *https://www.jpcert.or.jp/english/ir/form.html*
- Email : info@jpcert.or.jp
  PGP Fingerprint : FC89 53BB DC65 BD97 4BDA D1BD 317D 97A4 69EC E048