APCERT Activity Updates

Asia Pacific Computer Emergency Response Team

Yurie Ito

JPCERT/CC

Joint Workshop on Security 2008, Tokyo

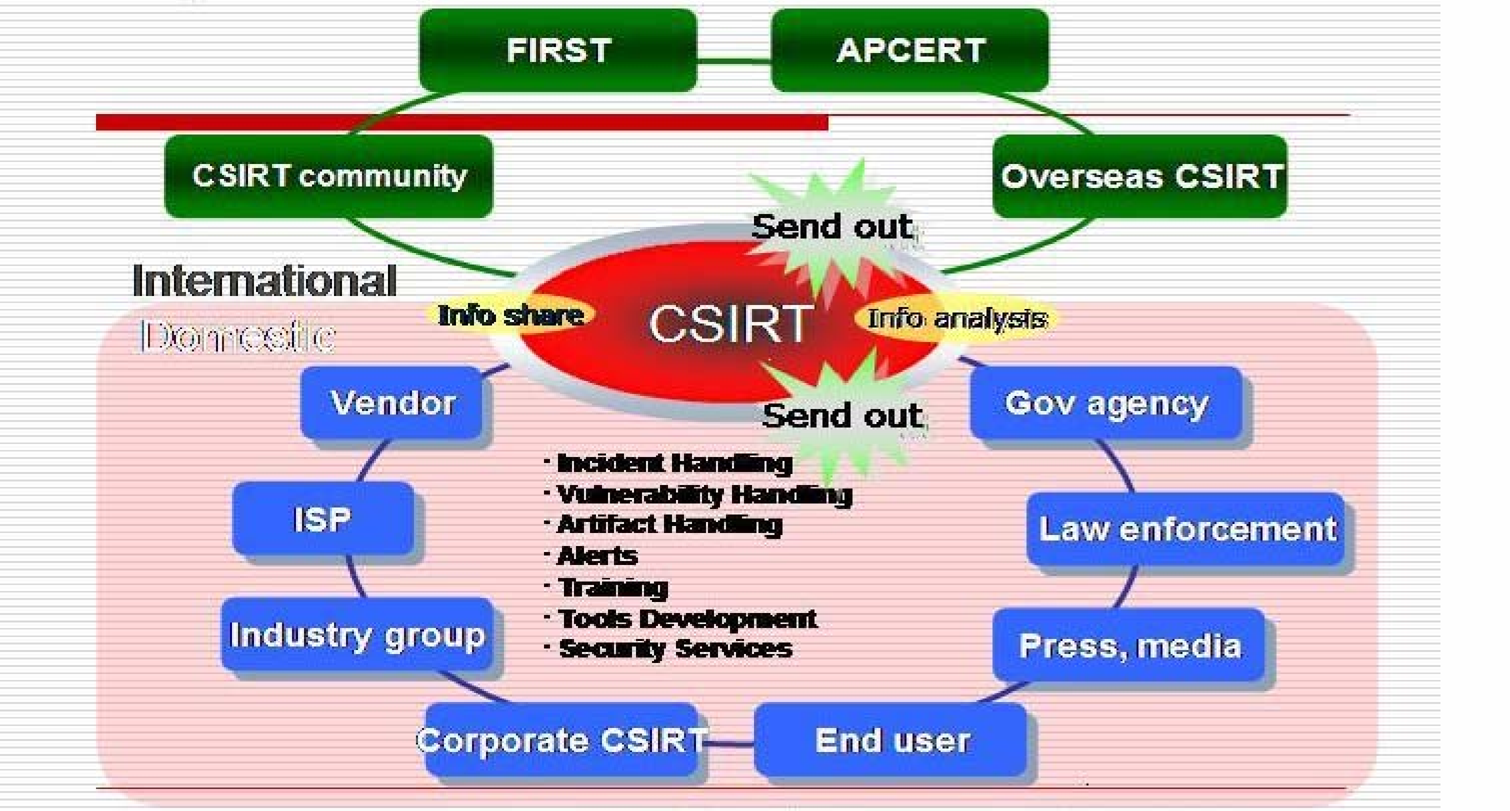
26 March 2008

About APCERT & CSIRT

- **APCERT** (Asia Pacific Computer Emergency Response Team) **is a coalition of the forum of CSIRTs*.**

CSIRT: Computer Security Incident Response Team*

International Collaboration Model for Information Security



- Incident Handling
- Vulnerability Handling
- Artifact Handling
- Alerts
- Training
- Tools Development
- Security Services

APCERT Member Teams

21 Teams / 15 Economies, as of March 2008

Full Members (14)

- **AusCERT** – *Australia*
- **BKIS** – *Vietnam*
- **CCERT** – *People's Republic of China*
- **CNCERT/CC** – *People's Republic of China*
- **HKCERT/CC** – *Hong Kong, China*
- **IDCERT** – *Indonesia*
- **JPCERT/CC** – *Japan*
- **KrCERT/CC** – *Korea*
- **MyCERT** – *Malaysia*
- **PH-CERT** – *Philippine*
- **SingCERT** – *Singapore*
- **ThaiCERT** – *Thailand*
- **TWCERT/CC** –*Chinese Taipei*
- **TWNCERT** – *Chinese Taipei*

General Members (7)

- **BP DSIRT** – *Singapore*
- **BruCERT** – *Negara Brunei Darussalam*
- **CERT-In** – *India*
- **GCSIRT** – *Philippine*
- **NUSCERT** – *Singapore*
- **SLCERT** – *Sri Lanka*
- **VNCERT** – *Vietnam*

Objectives

- Encourage and support regional and international cooperation on information security in the Asia Pacific region;
- Jointly develop measures to deal with large-scale or regional network security incidents;
- Facilitate info sharing and technology exchange, including info security, computer virus and malicious code, among its members;
- Promote collaborative research and development on subjects of interest to its members;

- Assist other CSIRTs in the region to conduct efficient and effective computer emergency response capability;
- Provide inputs and/or recommendations to help address legal issues related to info security and emergency response across issues regional boundaries;

- Organize annual conference to raise awareness on computer security incident responses and trends.

Network Security Cooperation

Emergency Response

Computer Security Awareness

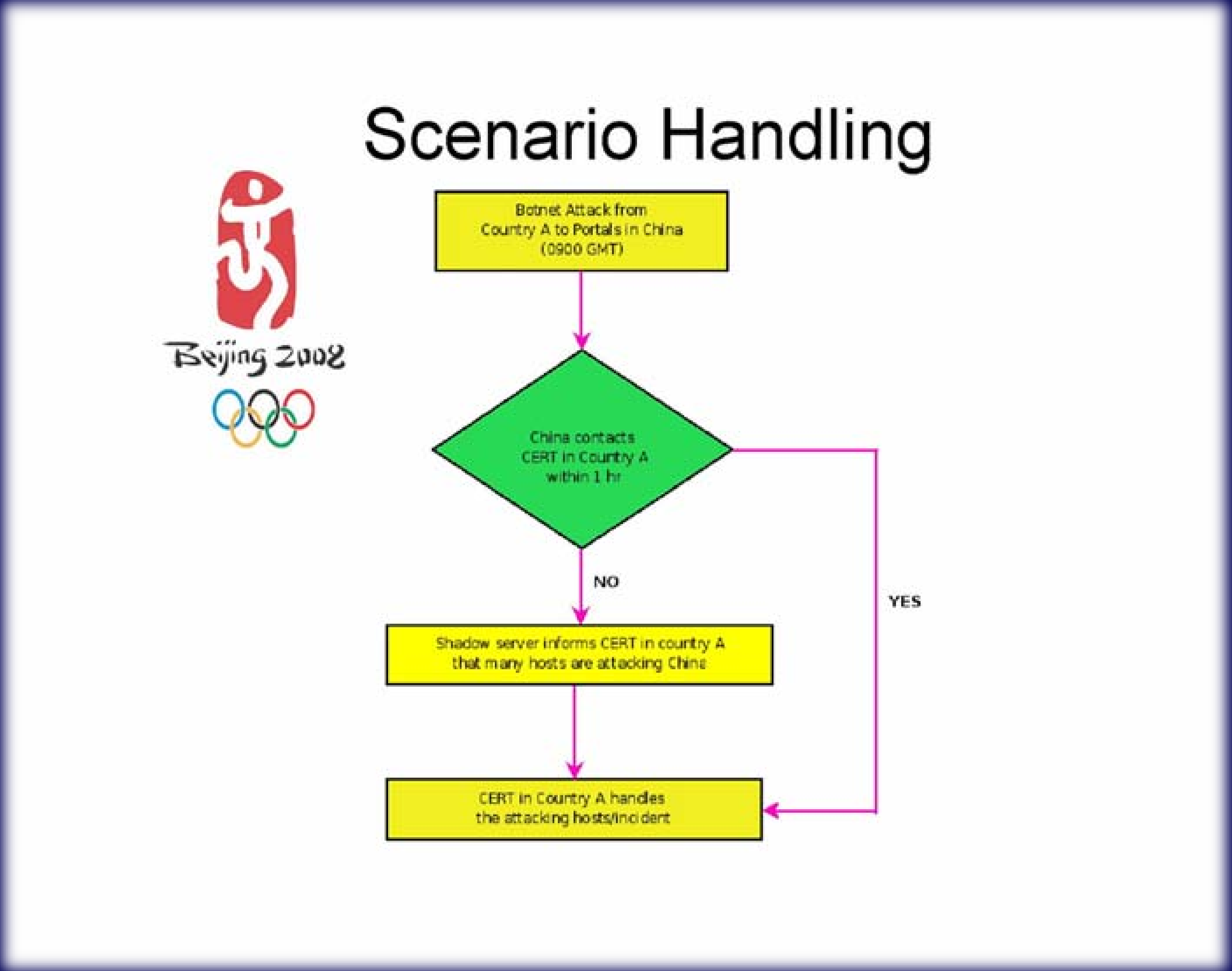
APCERT DRILL 2007

Beijing 2008
CNCERT/CC
KrCERT/CC
JPCERT/CC
HKCERT
TWNCERT
CERT-In
ThaiCERT
BKIS
BRUCERT
MyCERT
SingCERT
AusCERT
APCERT
Asia Pacific Computer Emergency Response Team

- Date : 22nd December 2007
- Participation teams:
  - Malaysia – MyCERT
  - Australia – AusCERT
  - Brunei – BruCERT
  - China – CNCERT
  - Singapore – SingCERT
  - Thailand – ThaiCERT
  - Hong Kong – HKCERT
  - India – CERT-In
  - Japan – JPCERT
  - Korea – KRCERT
  - Chinese Taipei – TWNCERT
  - Vietnam -BKIS

Timeline

- **0700** Lord of Armageddon (LoA) declare cyber war on Beijing Olympics
- **0900** Co-ordinated botnet attacks from AP region causing media sites and government portals inaccessible
- **1100** Spam containing malware that turns PC into zombies were filling up mailboxes in AP economies
- **1300** Border and Core routers crashing and rebooting frequently. 0-day exploit for Cisco IOS rumoured to be available. Cisco promise to release fix in a few hours
- **1430** – Cisco released patch and advisory on critical IOS vulnerability
- **1600** – Security analysts announced that bots automagically removed themselves, no more attacks



Scenario Handling

Botnet Attack from Country A to Portals in China (0900 GMT)

China contacts CERT in Country A within 1 hr

NO

YES

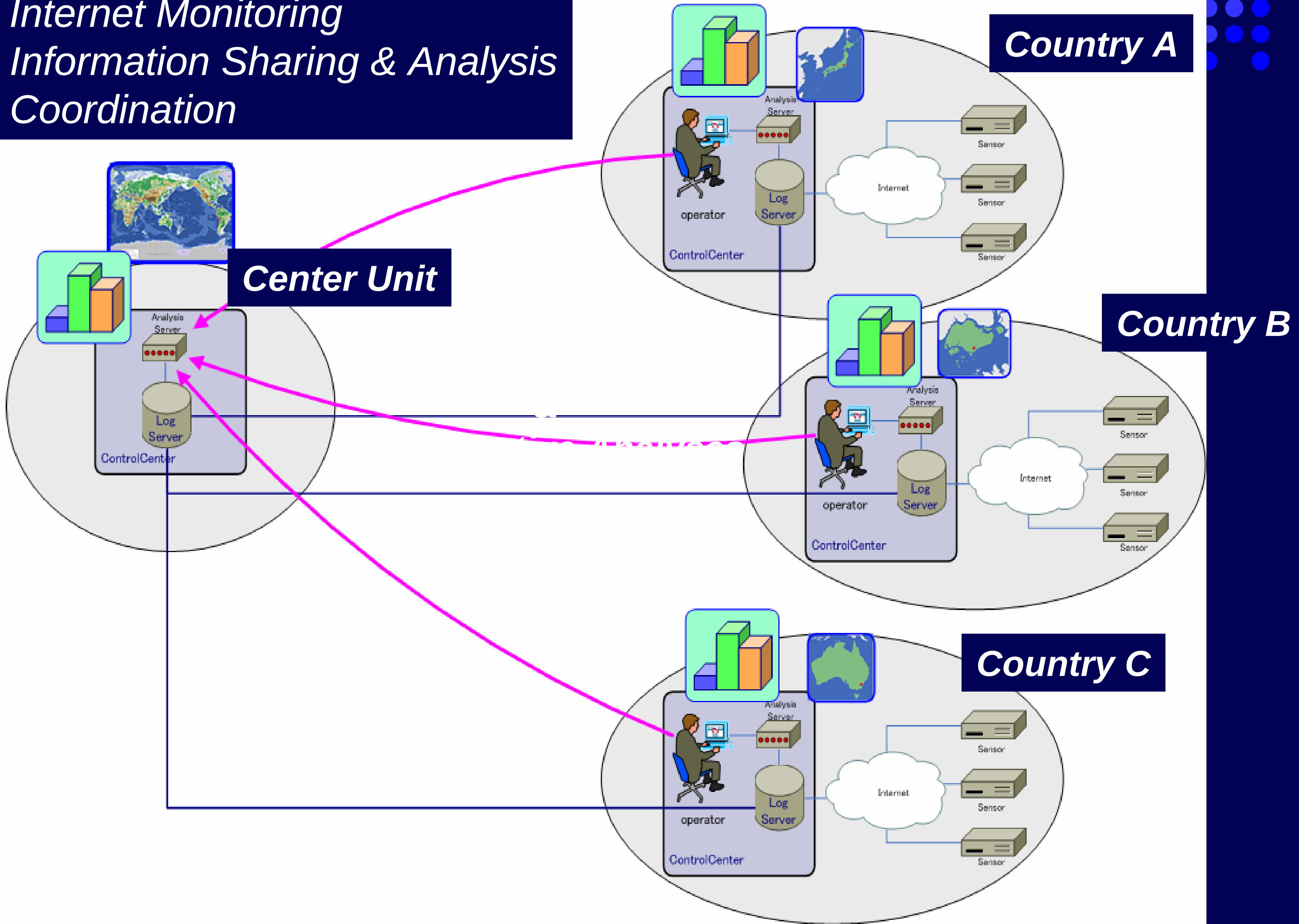
Shadow server informs CERT in country A that many hosts are attacking China

CERT in Country A handles the attacking hosts/incident

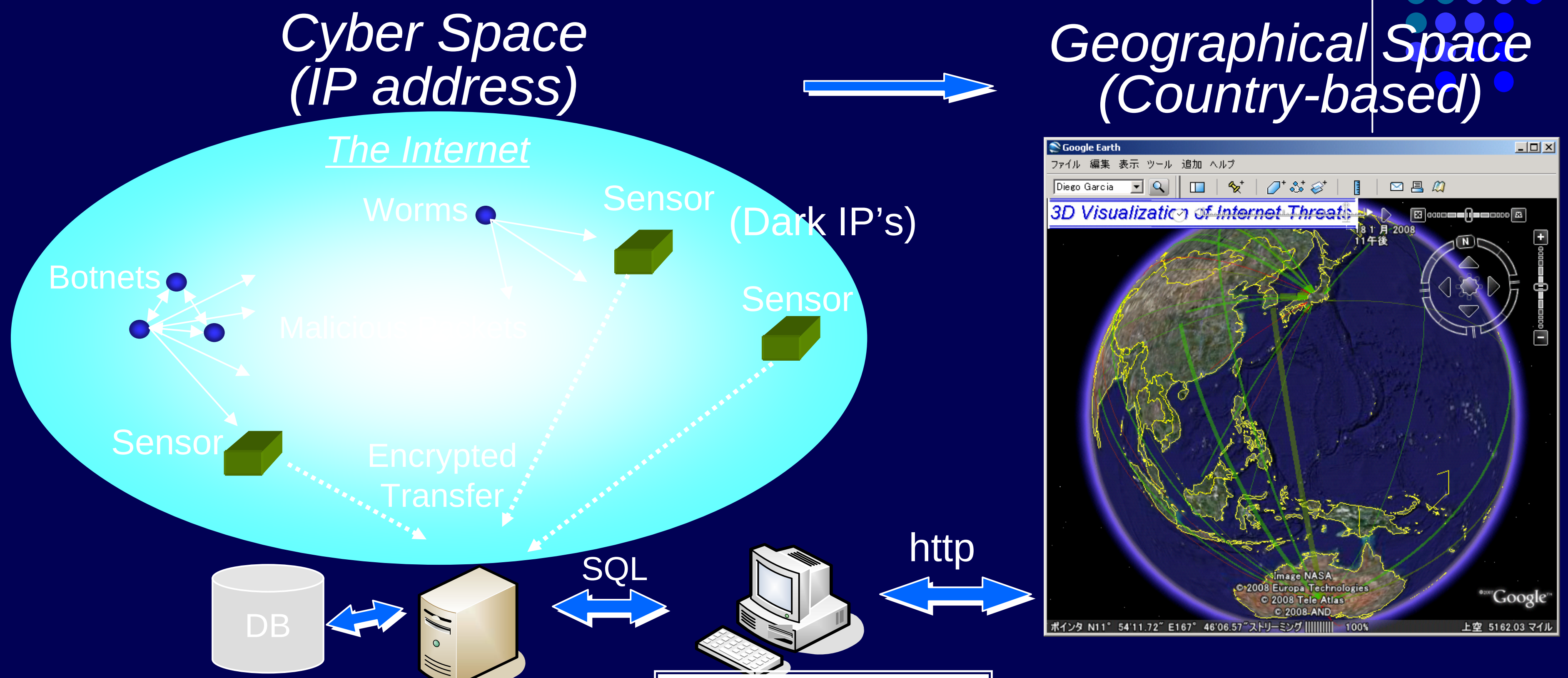
Objectives

- Establish a common platform for Internet threat monitoring, information sharing & analyses in Asia-Pacific region.
- Promote collaboration among CSIRT in Asia-Pacific region by using the common platform.
- Enhance capability of global threat analyses by incorporating 3D Visualization features to the common platform

(1) Internet Monitoring
(2) Information Sharing & Analysis
(3) Coordination



System Overview



```
mn128,may,13,05:40:11,111/tcp
mn128,may,13,10:12:55,111/tcp
mn128,may,13,10:13:04,111/tcp
mn128,may,13,12:35:05,111/tcp
mn128,may,13,12:35:05,111/tcp,
mn128,may,13,20:25:27,111/tcp,
mn128,may,13,20:25:27,111/tcp,
mn128,may,13,20:25:30,111/tcp,
```

Event Log
Records

Event Log Database

(1) Secure
(2) 24 × 7 Operation
(3) Robust

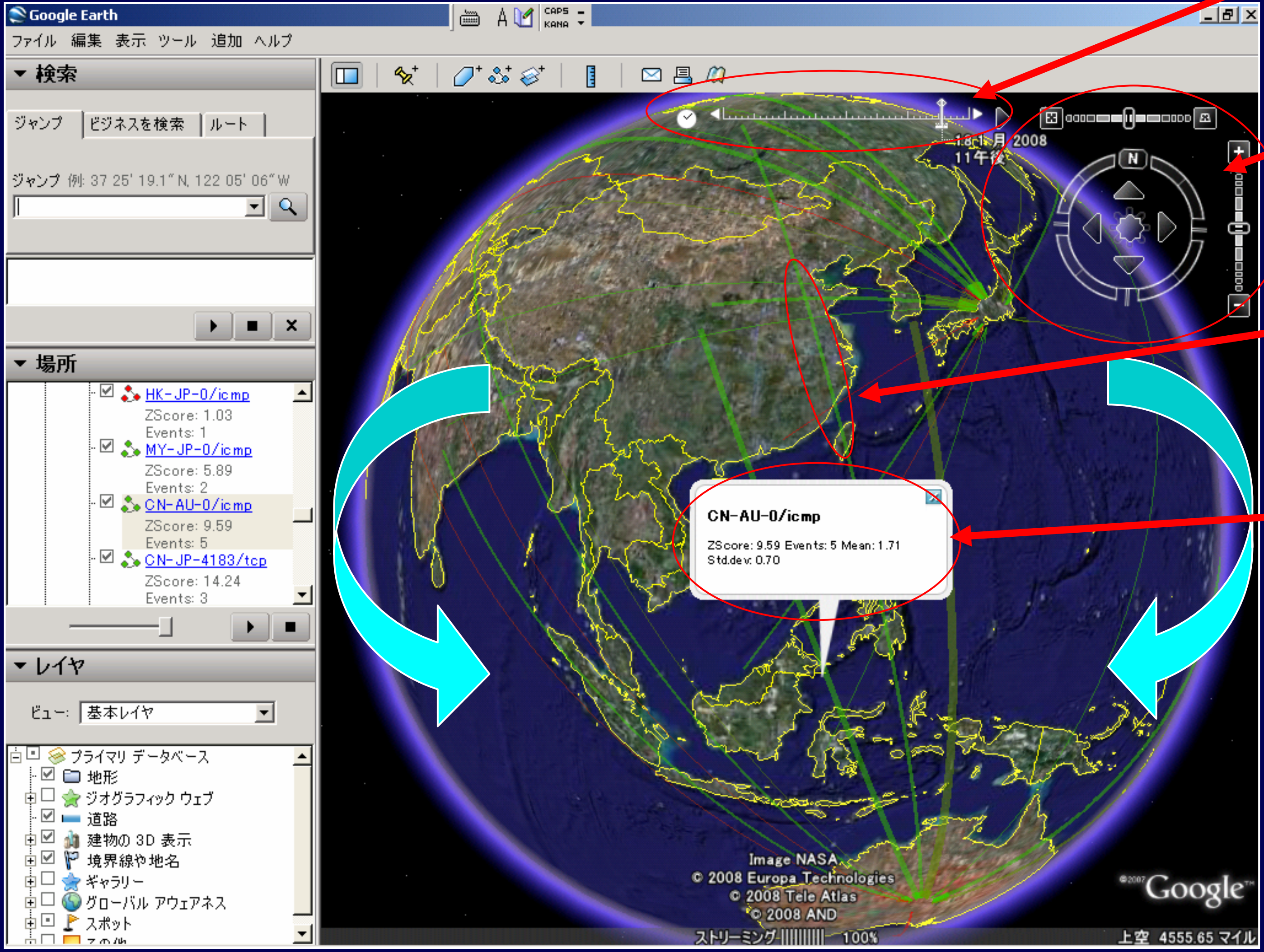
Analysis & 3D Visualization Server

(1) Trend Analysis
(2) Statistical Analysis
(3) Threat Screening

3D Visualization Client (on GoogleEarth)

(1) Flexible View
(2) Manipulation
(3) 3D Animation

Capabilities of 3D Visualization System



☑ HK-JP-0/icmp
ZScore: 1.03
Events: 1

☑ MY-JP-0/icmp
ZScore: 5.89
Events: 2

☑ CN-AU-0/icmp
ZScore: 9.59
Events: 5

☑ CN-JP-4183/tcp
ZScore: 14.24
Events: 3

CN-AU-0/icmp

ZScore: 9.59 Events: 5 Mean: 1.71
Std.dev: 0.70

Animation Controller
(Time-Slide Bar)

View Navigation Controller

Threat Status(Arrows)
(1) Color: Threat Level
(2) Width: Traffic

Threat data
(1) Traffic
(2) ZScore
(3) Std.Dev

APCERT Recent Activity Updates 1

- **PacINET 2007, 14-22 August 2007, Solomon Islands**
  http://www.picisoc.org/tiki-index.php?page=PacInet+2007
  - **AusCERT interacted with Pacific Islanders', who are willing to start discussions about CERT capability developments.**

- **ITU Regional Workshop, 28-31 August 2007, Hanoi, Vietnam**
  http://www.itu.int/ITU-D/cyb/events/2007/hanoi/
  - **MyCERT, AusCERT, CNCERT/CC, JPCERT/CC attended the "Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection".**
  - **Indonesia and Mongolia are also willing to discuss CERT capability developments.**

APCERT Recent Activity Updates 2

- **APEC TEL 36, 21-26 October 2007, Santiago, Chile**
  http://www.apectel36.cl/prontus_apectel/site/edic/base/port/home.html

  - **CNCERT/CC, JPCERT/CC, KrCERT/CC, MyCERT attended the "Workshop on Cyber Security Exercises" and shared experience of the APCERT Incident Handling Drill.**
  - **CNCERT/CC is forwarding a project on "Guide on Policy and Technical Approaches Against Botnets".**

  * As a Security Expert Group, APCERT provides recommendation, situation awareness and trend to AP regional intergovernmental initiatives. APCERT is a General Guest of APEC TEL.

- **CICTE (Inter-American Committee Against Terrorism) 5-9 November 2007, Miami, USA**
  http://www.cicte.oas.org/Rev/EN/Events/Cyber_Events/II_Workshop_MIAMI-2007.asp

  - **MyCERT attended and had interactions with OAS (Organization of American States) and APWG (Anti-Phishing Working Group).**

APCERT Recent Activity Updates 3

- Visiting New CSIRTs in Asia Pacific
  - APCERT SC members visited several CSIRTs and relevant government departments, to support and cooperate in incident handling and information sharing.

- Other International Relationships & Engagements
  - FIRST Director & SC Member: Yurie Ito, JPCERT/CC
  - APEC TEL SPSG Deputy Convenor: Jinhyun Cho, KrCERT/CC

APCERT Recent Activity Updates 4

- **APCERT AGM & Conference 2008, 10-12 March 2008**

  http://apcert2008.hkcert.org/

  InterContinental Grand Stanford Hong Kong

  Hosted by HKCERT

  - ***The 7th APCERT Annual Conference, providing a valuable opportunity for APCERT Teams, CSIRTs of the AP region, and other closely related organizations to come together and share different experiences, perspectives and best practices on information security.***
  - ***Most importantly, it provides an opportunity to help improve Internet security throughout the Asia Pacific and beyond, through cross border cooperation and information sharing.***

APCERT
Asia Pacific Computer Emergency Response Team

Thank you

APCERT General Contact:

apcert-sec@apcert.org

APCERT Website:

http://www.apcert.org