# Short Introduction of Telecom-ISAC Japan
## --- Overview, Current Activities ---

**25 MAR , 2008**

**Telecom-ISAC Japan**

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

# Philosophy

- **The Internet and other telecommunication networks form the base of a social economic structure on a world scale. Ensuring the information security becomes the urgent issue in social economic life.**

- **"Telecom-ISAC Japan aims at the mutual cooperation between wide variety of members, such as those who are in the information and telecommunications industry of our country, presses the information sharing to correspond to these, and the improvement of the information security is pressed by doing the activity to contribute to the start information security measures. And, it acts aiming to contribute to the formation of the advanced telecommunication network society. “**

- **Healthy COMPETITION from lofty COLLABORATION.**

# History

財団法人 日本データ通信協会
NIC : Nippon Information Communications Association

Established by 7 ISP as a private organization.

Joined 5 ISP/SIer, transferred to **NIC**.

**19** ISP/SIer.

*2002 2003 2004 2005 2006 2007 2008*

**Network worm**

**Serious threat to an ISP**

**Coordination for the information sharing**

DDoS analysis & prevention

Anti-Abuse corroborate

BOT analysis

Cyber Clean Center

**Botnet**

**Large scale threat to multiple ISPs**

BGP routing monitoring

经路奉行

**Information sharing for coordination**

TINY monitoring

Trace Back

SoNAR

# Structure (as of Mar 2008)


**Steering Committee**

Approve

**Planning and Coordination Division**

Manage

**Working groups**

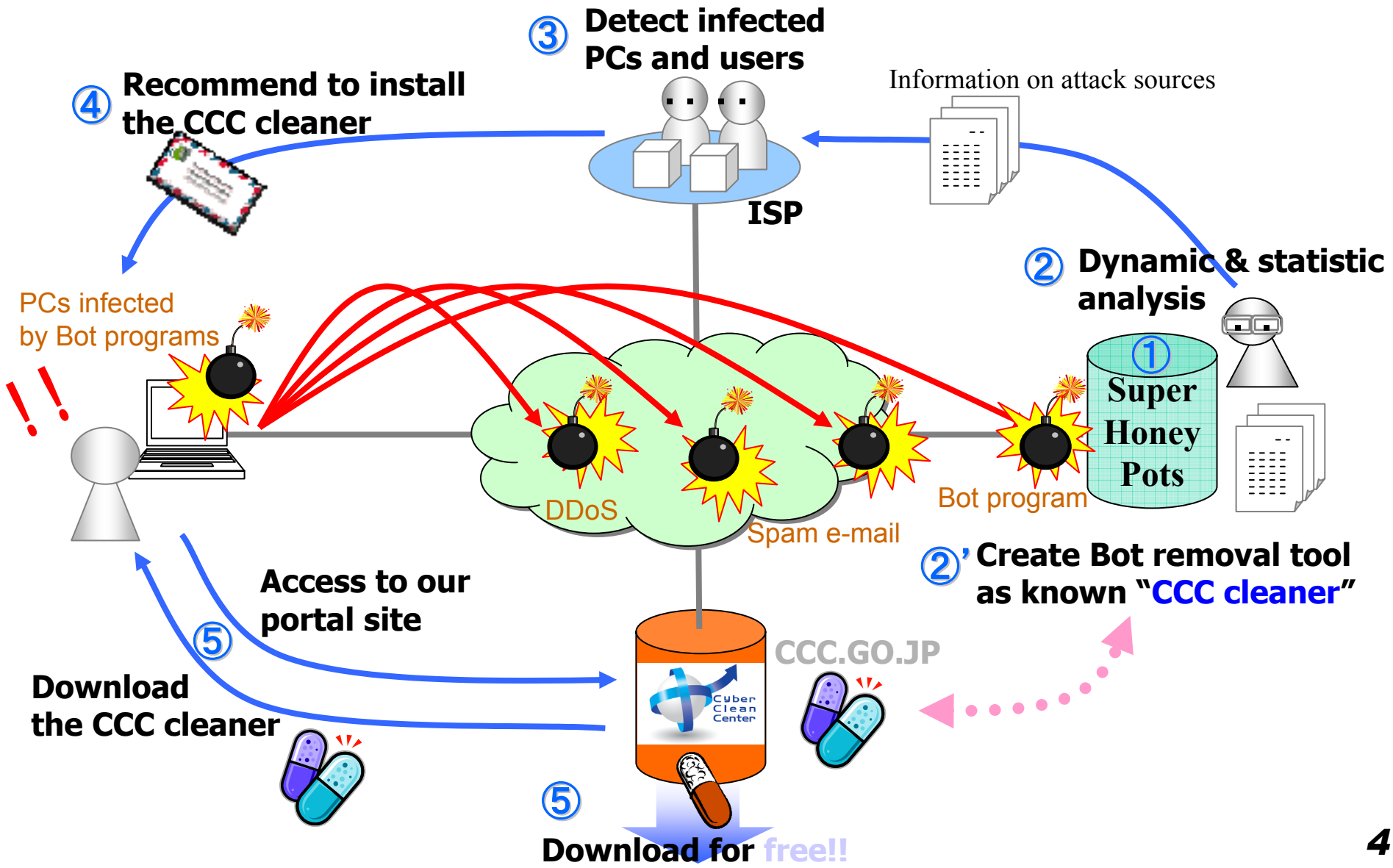
Execute

*CCC-WG*
*BGP-WG*
*TB-WG*
*SoNAR-WG*

19 members

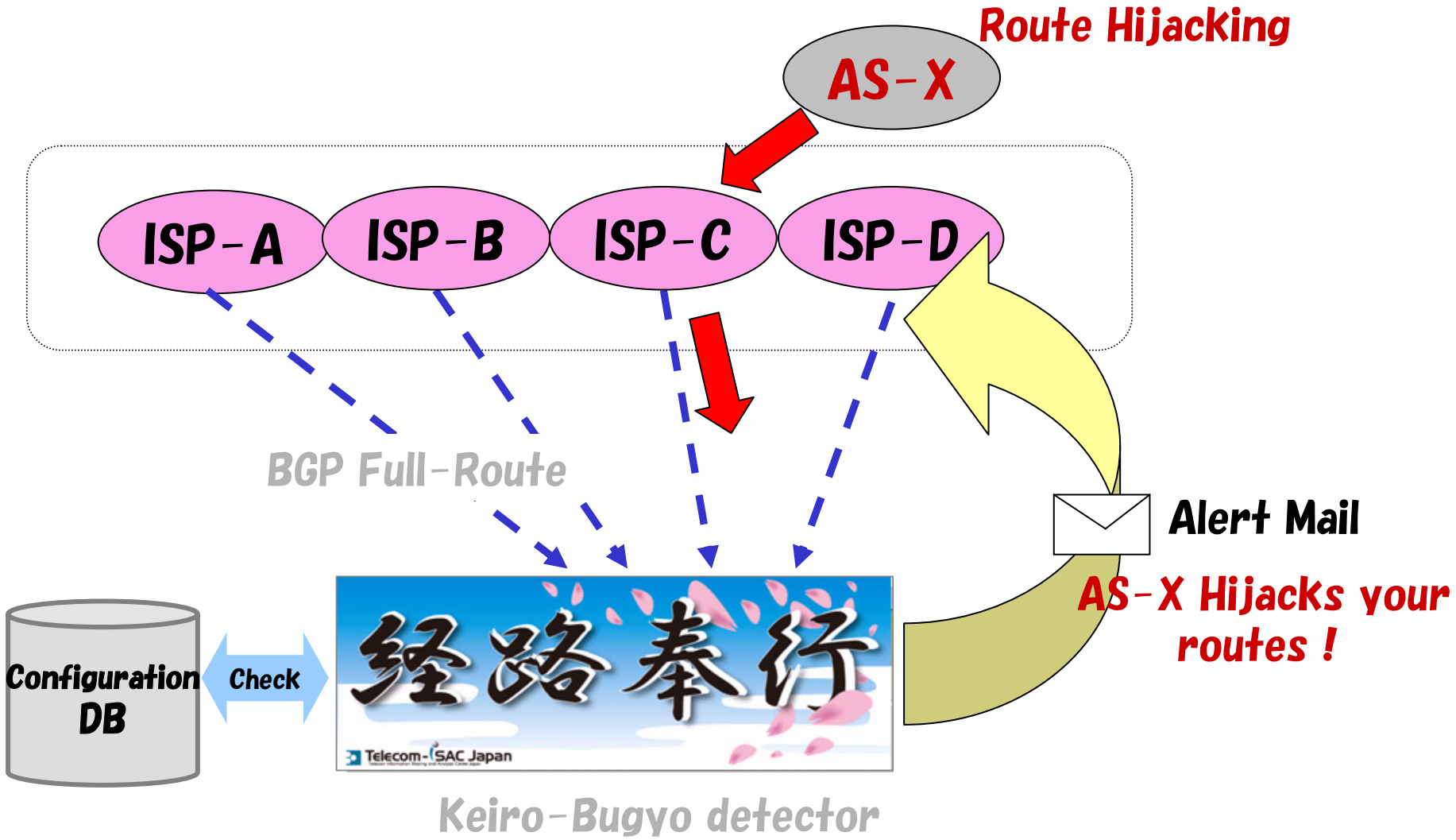
**KDDI CORPORATION**
**NEC Corporation**
**NTT Communications Corporation**
**NIFTY corp.**
**SOFTBANK TELECOM Corp.**
**SOFTBANK BB Corp.**
**Internet Initiative Japan Inc.**
**Hitachi, Ltd.**
**Matsushita Electric Industrial Co., LTD.**
**Oki Electric Industry Co., Ltd.**
**Yokogawa Electric Corp.**
**Matsushita Electric Works, LTD.**
**NTT Navispace Corp.**
**NIPPON TELEGRAPH AND TELEPHONE EAST CORPORATION**
**NIPPON TELEGRAPH AND TELEPHONE WEST CORPORATION**
**Nippon Telegraph and Telephone Corporation**
**NTT Visual Communication Corporation**
**KDDI R&D Laboratories**
**NEC BIGLOBE, Ltd.**

# Activities (1) Cyber Clean Center work flow

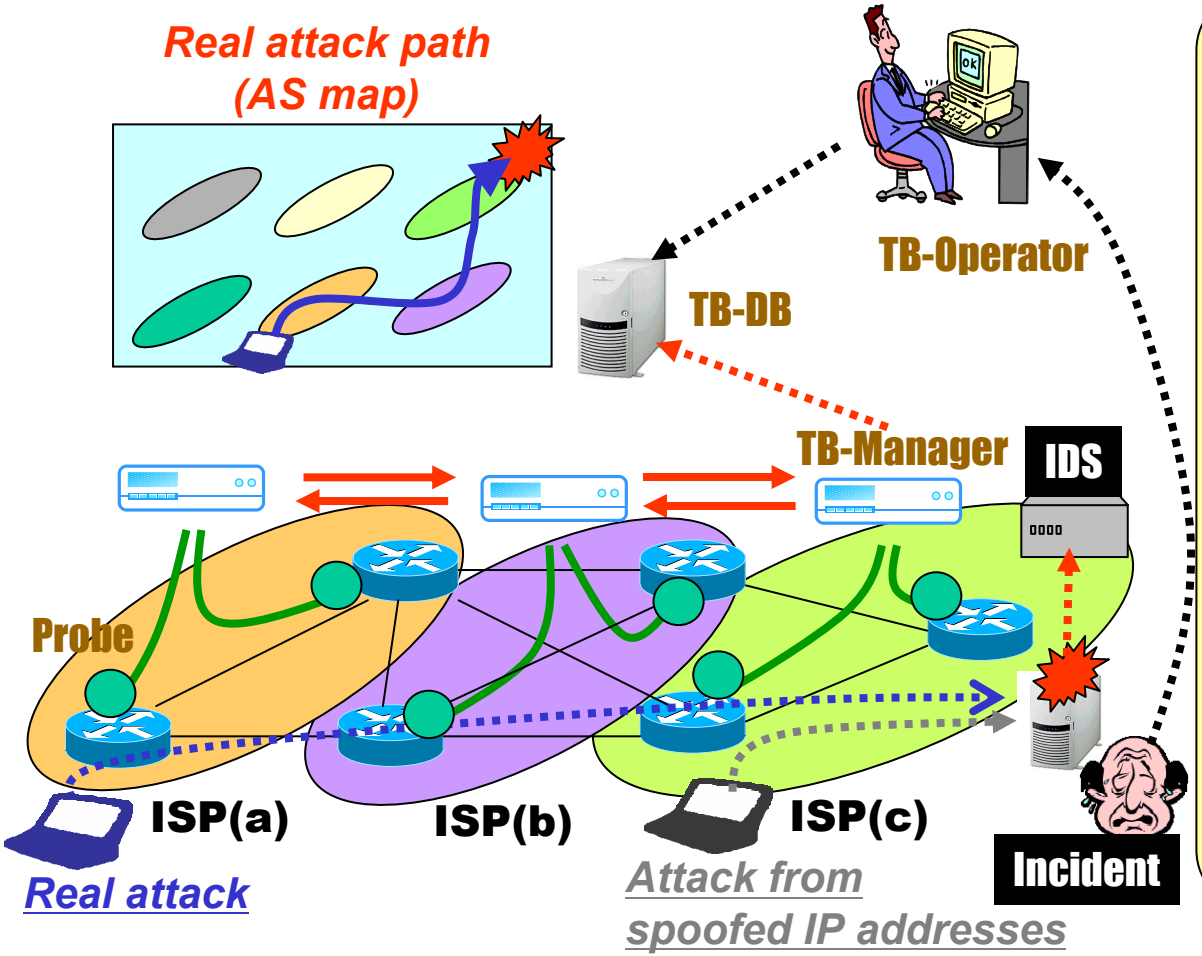


# Activities (2) BGP monitoring

·**BGP prefix hijacking is a real threat.**
- ISPs need a solution based on today's technology.



# Activities (3) Trace Back Project (R&D)




Outline of Trace Back system under development.

**0. Store HASH data temporary.**

Each probe convert PKT to HASH, and store own cache automatically.

**1. Store suspicious information.**

Whenever IDS notify suspicious attacks, TB manager calculate the attack PKT's HASH, and automatically recursive analyze it's AS map with neighbor AS's TB manager, and store it to TB-DB.

**2. Detect the real attack path**

After an incident be recognized, TB-Operator analyze TB-DB by attack PKT's HASH, and detect the real attack path.

**Role of T-ISAC-J**

A: Propose a legitimate operation model.
B: Propose an operational contract among ISP.
C: Establish the Trace Back platform in the participating ISP. (FY2008～FY2009)

# Activities (4) SoNAR-WG

**S**ociety **o**f **N**etwork **A**buse **R**esponse

- **ネットワークを利用した不正・不法行為対応（ABUSE対応）に関する情報を共有し、利用者に与える被害の拡大を抑止するフレームワークを策定することを第一の活動目的とする。**
- **インシデント対応を分析することによって得られた知見を社会に展開することも視野に入れた活動を展開する。**
- **また、通信サービスにおける危機管理業務のひとつとして存在するABUSE対応プロセスを定着させるため、業態・業界を超えた交流から有意義な手法を吸収する活動も実施する。**

## SoNAR-WG

**①ABUSE憲章の策定**

ABUSE対応に関する原則を明文化し共有する試み。ABUSE対応の輪郭を浮彫りにし、範囲を再定義する目的。

**②事例共有と分析**

各社にて対応中の案件を事例として紹介し、他社での事例との比較や対応方針を共有することで対応効率化を狙う。

**③勉強会**

他業種・業態の事業者との交流により、新しい事案に関する情報の入手と対応手法の洗練を目指す。

**④ツール類の検討**

事例集積データベースや連携・連絡のためのツールの仕様等について検討する。