Brief Overview of CCC Project

--Botnet countermeasures in JAPAN--

JUNKO HAYAKASHI

Board Member; Managing Director

Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)

Steering committee member of “CCC project”

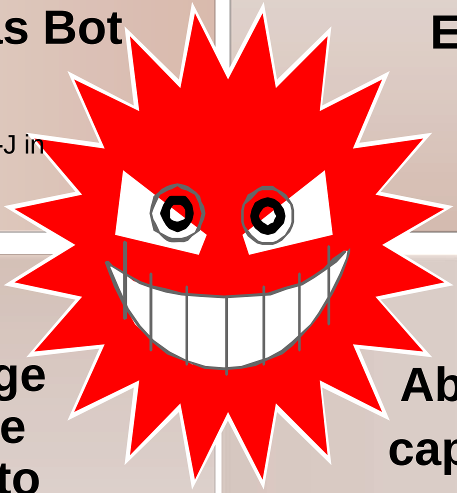
Bots in Japan: current situation

About 80% of malware programs observed on Japanese telecom networks are classified as Bot programs

.Estimate from the results of studies by T-ISAC-J in 2005.

An estimation of infection rates: 2%-2.5%
Equivalent to 400k - 500k people (computers)

.Estimate from the results of studies by JPCERT/CC and T-ISAC-J in 2005.



About 4 minutes on average for a unprotected PC to be infected when connected to Internet.

.From experiments conducted by T-ISAC-J in 2005.

About 100 types of Bots are captured in our honey pot as unknown types per day.

.Number of bot programs with unique hash capturing by CCC.

And

- **Traffic flows caused by Botnet or viruses tops 300Mbps per IP.**
- **A total of around 10Gbps of traffic from Japanese IP addresses are wasted by Botnet. (SPAM mail traffic via Botnet are not included.)**

Liability issue

- Who does have the liability of this Botnet problem?
  - ISPs?
  - End users?
  - Security experts?
  - Service providers?
  - Government?

- Who does take the cost of remediation?

Responsibilities of end users

- Premise

1.Recognition of condition

the users of infected PCs have difficulty in identifying BOT

- notice them
- provide opportunity to check their PCs condition

2.Knowledge of countermeasures

- awareness building

3. Reasonable availability of tools for countermeasures

- Checking and Removal tools

Bot-net Countermeasures

Bot-net countermeasures project was launched in December 2006.

Our portal site: Cyber Clean Center
https://www.ccc.go.jp/

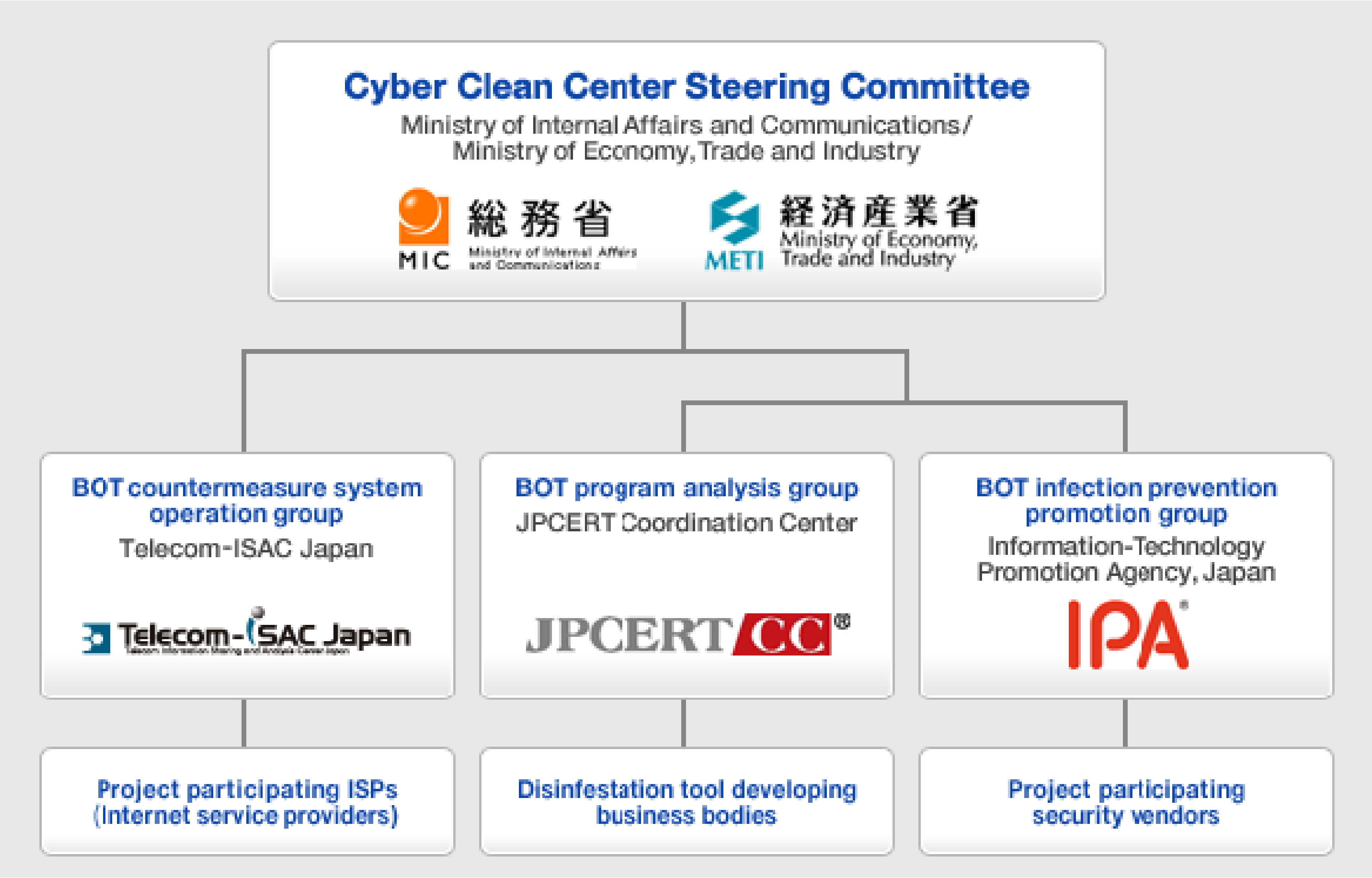
- Promotion and collaboration among 2 ministries (MIC and METI).
- Organized by JPCERT/CC, Telecom-ISAC Japan, and IPA.
- Co-operation with 8 ISPs who are Telecom-ISAC members (now it expands to 65 ISPs including nonmember of ISAC) and antivirus vendors in the Botnet countermeasures Workflow.
- From FY 2006 to 2010
- Main purpose:

  To reduce the number of bot-infected users

  To make removal tool that specializes in Bot that becomes popular in Japan

  To provide bot samples to Project-participating security vendors.

Organization of CCC



Cyber Clean Center Steering Committee

Ministry of Internal Affairs and Communications/
Ministry of Economy, Trade and Industry

総務省 MIC Ministry of Internal Affairs and Communications

経済産業省 METI Ministry of Economy, Trade and Industry

BOT countermeasure system operation group

Telecom-ISAC Japan

BOT program analysis group

JPCERT Coordination Center

BOT infection prevention promotion group

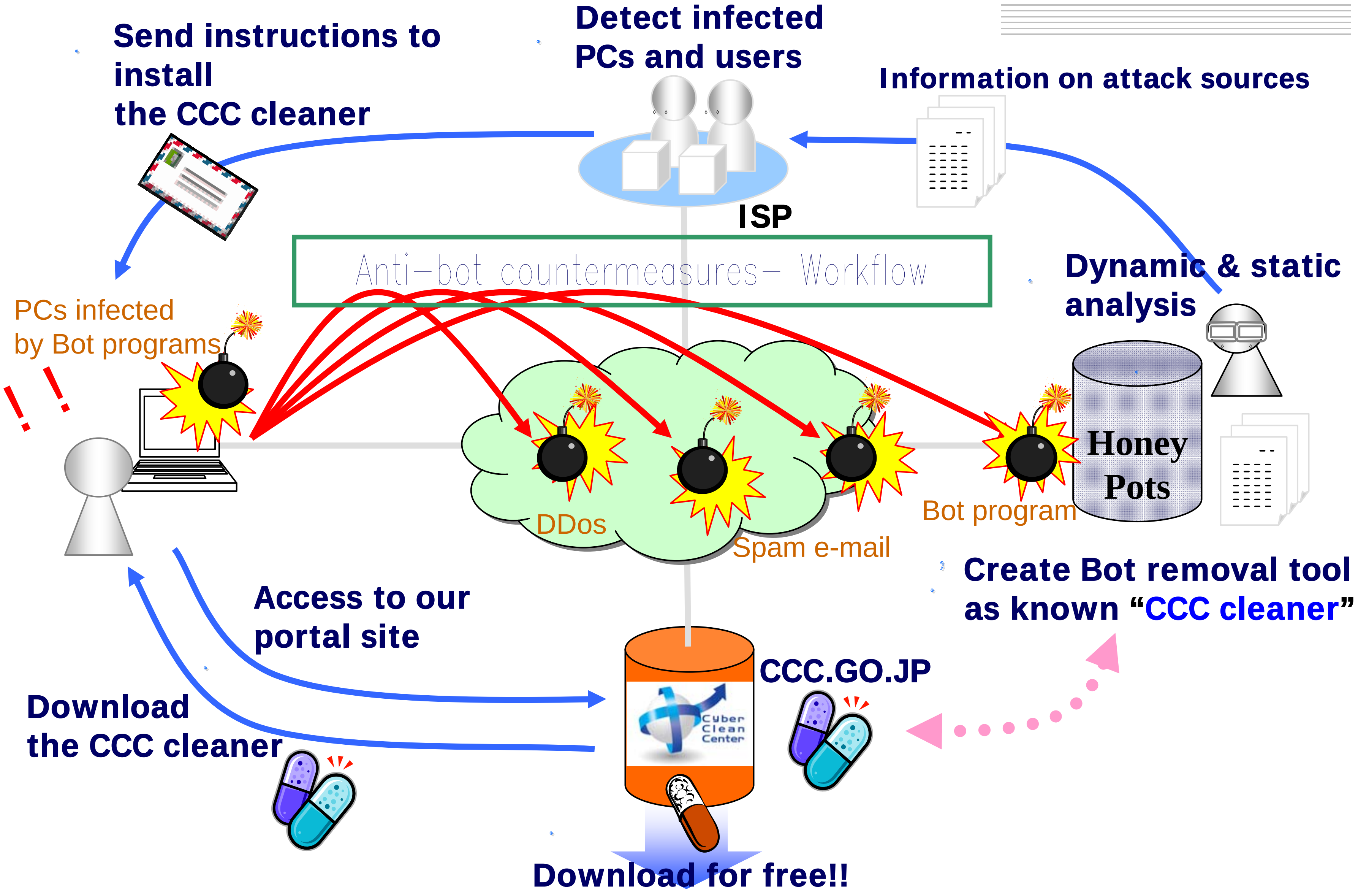
Information-Technology Promotion Agency, Japan

Project participating ISPs (Internet service providers)

Disinfestation tool developing business bodies

Project participating security vendors

How do we handle Bot-infected users?


Send instructions to install the CCC cleaner
Detect infected PCs and users
Information on attack sources
ISP
Anti-bot countermeasures- Workflow
Dynamic & static analysis
PCs infected by Bot programs
!!
Honey Pots
Bot program
DDos
Spam e-mail
Create Bot removal tool as known "CCC cleaner"
Access to our portal site
CCC.GO.JP
Cyber Clean Center
Download the CCC cleaner
Download for free!!

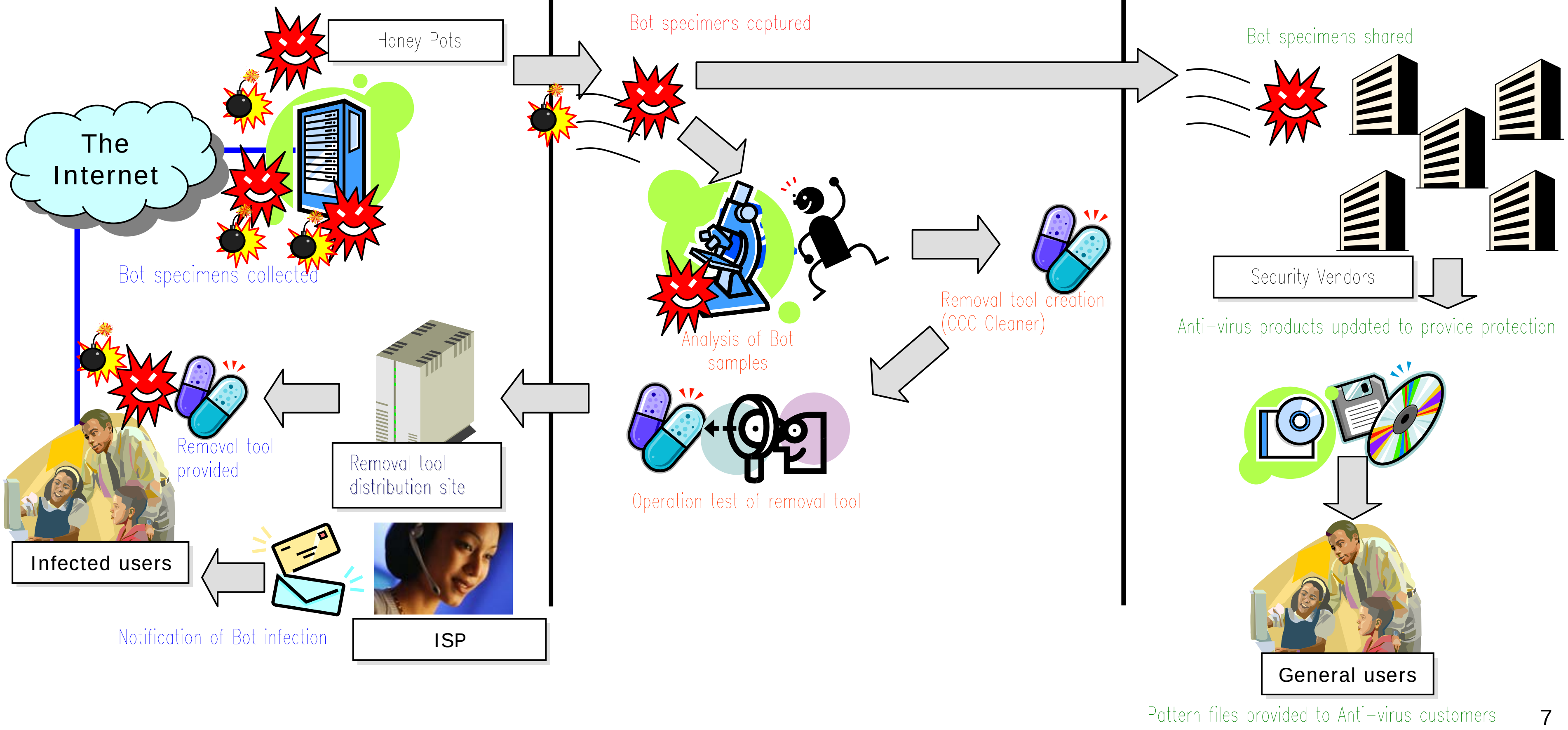
Cyber Clean Center roles

Cyber Clean Center

BOT countermeasure system operation group
Organized by
Telecom-ISAC Japan

BOT program analysis group
Organized by
JPCERT/CC

BOT infection prevention promotion group
Organized by
IPA



Honey Pots

The Internet

Bot specimens collected

Removal tool provided

Removal tool distribution site

Infected users

Notification of Bot infection

ISP

Bot specimens captured

Analysis of Bot samples

Removal tool creation (CCC Cleaner)

Operation test of removal tool

Bot specimens shared

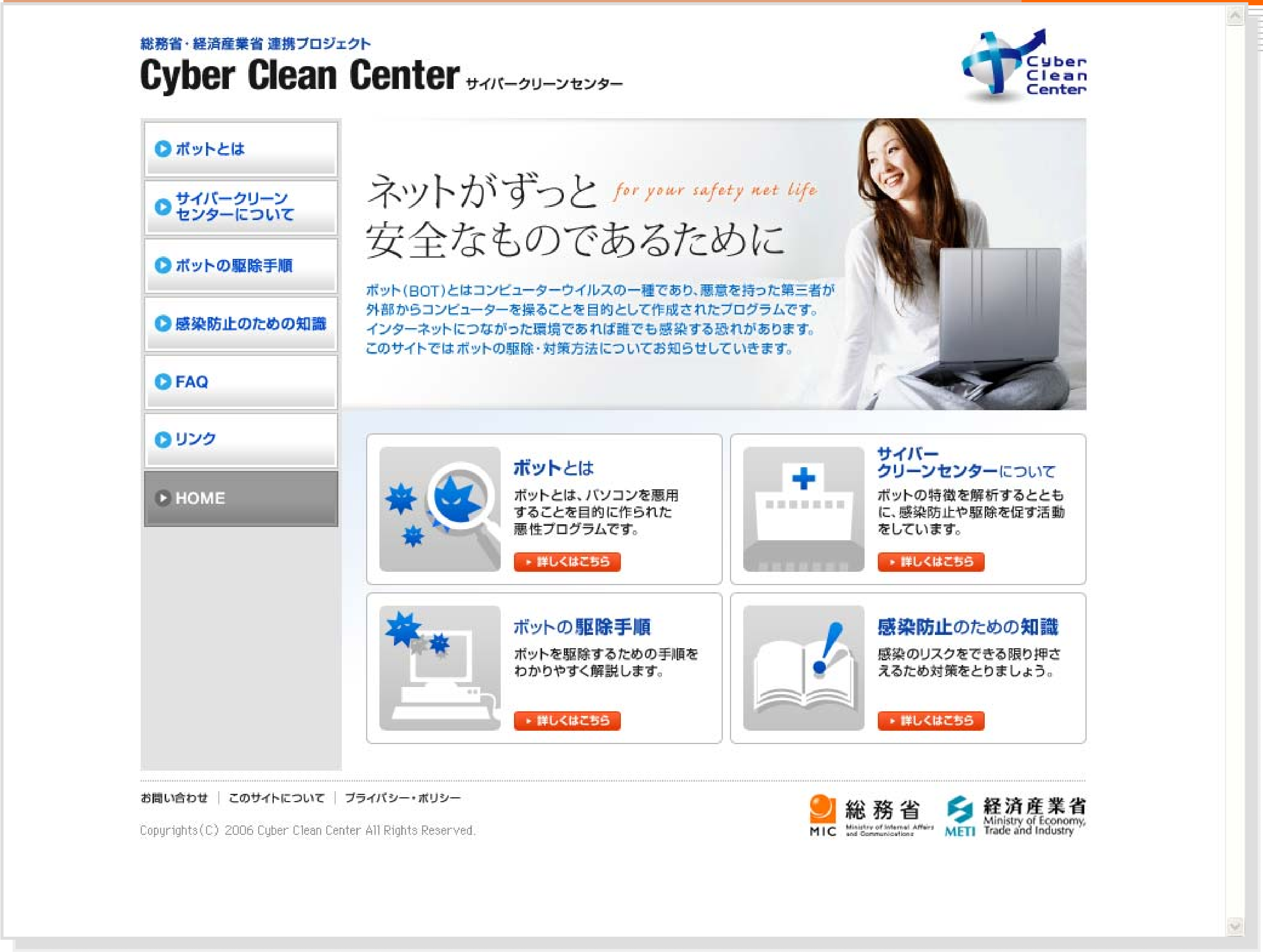
Security Vendors

Anti-virus products updated to provide protection

General users

Pattern files provided to Anti-virus customers

GENERAL FRONT PAGE: https://www.ccc.go.jp/



総務省・経済産業省 連携プロジェクト

Cyber Clean Center サイバークリーンセンター

- ボットとは
- サイバークリーンセンターについて
- ボットの駆除手順
- 感染防止のための知識
- FAQ
- リンク
- HOME

ネットがずっと *for your safety net life*
安全なものであるために

ボット(BOT)とはコンピューターウイルスの一種であり、悪意を持った第三者が外部からコンピューターを操ることを目的として作成されたプログラムです。インターネットにつながった環境であれば誰でも感染する恐れがあります。このサイトではボットの駆除・対策方法についてお知らせしていきます。

ボットとは

ボットとは、パソコンを悪用することを目的に作られた悪性プログラムです。

▸ 詳しくはこちら

サイバークリーンセンターについて

ボットの特徴を解析するとともに、感染防止や駆除を促す活動をしています。

▸ 詳しくはこちら

ボットの駆除手順

ボットを駆除するための手順をわかりやすく解説します。

▸ 詳しくはこちら

感染防止のための知識

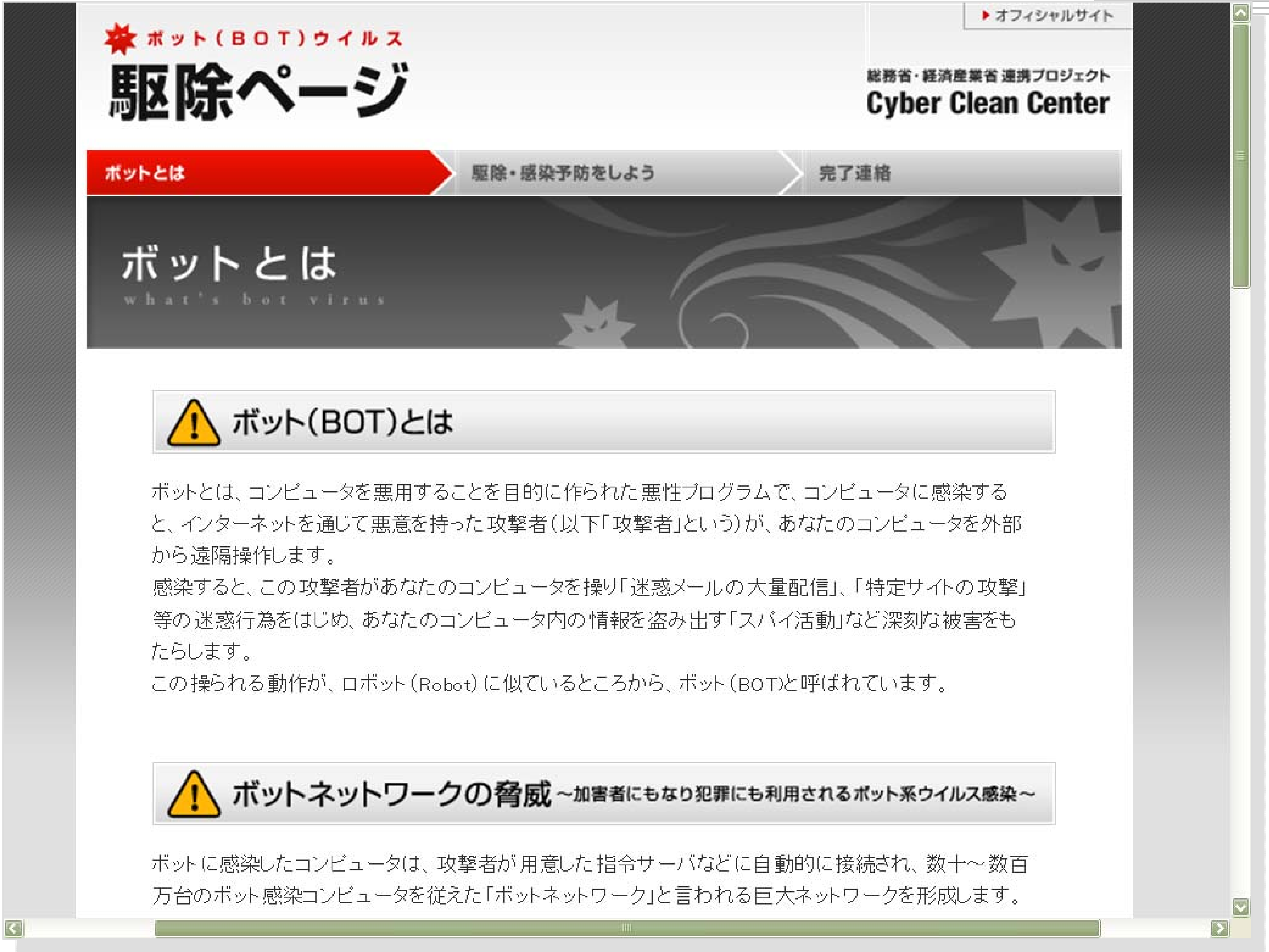
感染のリスクをできる限り押さえるため対策をとりましょう。

▸ 詳しくはこちら

お問い合わせ | このサイトについて | プライバシー・ポリシー

総務省
MIC Ministry of Internal Affairs and Communications
経済産業省
METI Ministry of Economy, Trade and Industry

For Bot Infected Users.https://www.ccc.go.jp/



ボット(BOT)とは

ボットとは、コンピュータを悪用することを目的に作られた悪性プログラムで、コンピュータに感染すると、インターネットを通じて悪意を持った攻撃者（以下「攻撃者」という）が、あなたのコンピュータを外部から遠隔操作します。

感染すると、この攻撃者があなたのコンピュータを操り「迷惑メールの大量配信」、「特定サイトの攻撃」等の迷惑行為をはじめ、あなたのコンピュータ内の情報を盗み出す「スパイ活動」など深刻な被害をもたらします。

この操られる動作が、ロボット（Robot）に似ているところから、ボット（BOT)と呼ばれています。

ボットネットワークの脅威 ～加害者にもなり犯罪にも利用されるボット系ウイルス感染～

ボットに感染したコンピュータは、攻撃者が用意した指令サーバなどに自動的に接続され、数十～数百万台のボット感染コンピュータを従えた「ボットネットワーク」と言われる巨大ネットワークを形成します。

Activity results of CCC

From 2006 Dec.12.2007.jul.31
(A part of data is excluded.)

.Number of total collected samples. 3,198,796

Among the countless attacks to the "honey pot," collect the samples, such as Bot programs (binary files).

.Number of Unique samples.83,240

Since a number of same samples will be collected, remove the ones that are identical in size and external characteristics, then separate the unique specimens (binary files).

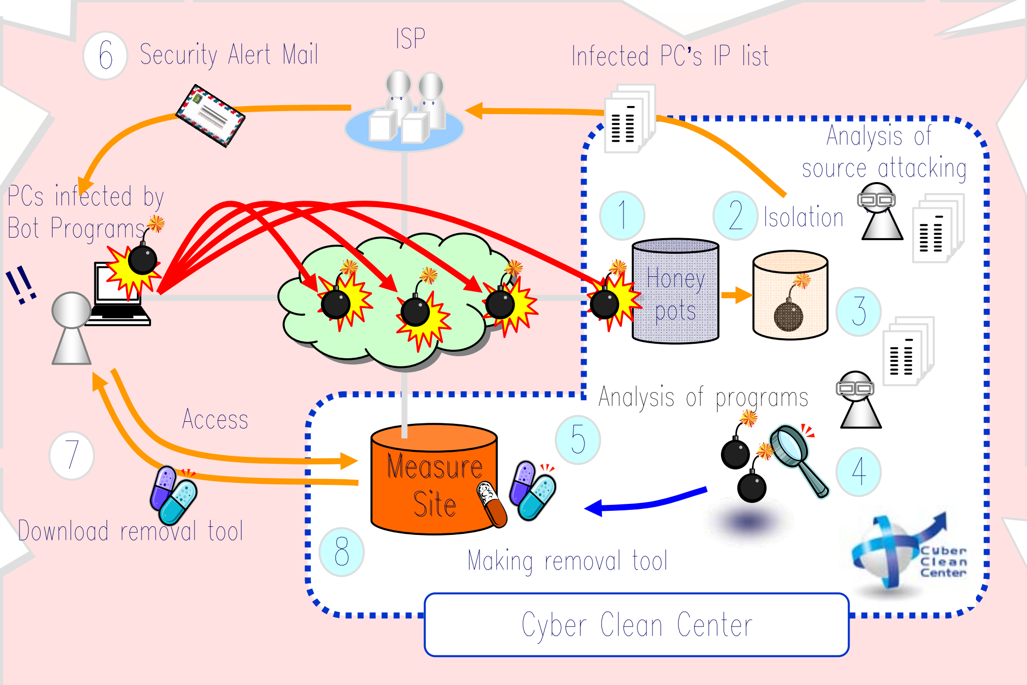
. Number of Unknown samples. 4,854

Examine unique samples using commercial anti-virus software, then separate those that were undetectable.

. Alerts to identified users: Provided 93,026 times

This is the number of security alerts that cooperative ISPs provided to infected users.

Number of recipients: **28,009**



.Number of samples materials reflected in removal tool.4,046

Analyze unknown samples and create the Bot removal tools for those that are high-risk and currently infecting PCs.

. Percentage of alert recipients to download Bot removal tools: **30%**

.Bot Removal Tool

Updated:**26** times

Bot removal tools are updated every week.

Total Frequency of Removal Tool Download . 164,561

Next step in enhancing CCC project

- Change the composition of honeypots

- Broaden the reach of ISPs

- Improving ratios of visiting the removal tool distribution
- Inform the public about anti-malware measures

- Build a closer relationship with global partners