重要インフラセキュリティセミナー

Telecom-ISAC Japanの最近の取組について

2007.2.14

Telecom-ISAC Japan
企画調整部　部長　有村　浩一

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

Telecom-ISAC Japanとは

- Telecom-ISAC Japanは、2002年7月に7つの国内主要ISP事業者による会員制任意団体として発足
- T-ISAC-Jは、日本で最初のISAC
- T-ISAC-Jは、会員の情報通信サービス、重要インフラをインシデントから守り、またサービスの安定運用ために会員連携のもと速やかな対処活動を行う場を提供することを目指す。

【参考】ISAC　(Information Sharing and Analysis Center)とは

- 発祥地はアメリカ（1998年）
- 米国クリントン政権の国家の重要な情報ネットワークを防護する政策によって、重要インフラを構成する民間の各業種において設置が促されたのが始まり。
- 13の民間業種にISACが発足（金融、電力、運輸、通信等）

組織構成

（2007.1現在）

（財）日本データ通信協会

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

会長：　日本電気
副会長：NTTコミュニケーションズ
構成会社：ニフティ、ソフトバンクテレコム、IIJ、KDDI、
日立製作所、松下電器産業、沖電気工業、
ソフトバンクBB、横河電機、松下電工、
NTTナビスペース、東日本電信電話株式会社、
西日本電信電話株式会社、
エヌ・ティ・ティ・ビジュアル通信、
日本電信電話株式会社

17社

ステアリング・コミッティ

承認

委員長：　NTTコミュニケーションズ
副委員長：ＫＤＤＩ
構成会社：横河電機、日立製作所、ニフティ、IIJ
ソフトバンクBB、日本電気

4社

企画調整部

管理

Working-Group

実行

Working-Group

システム運用部

管理

Working-Group

実行

Working-Group

アライアンスメンバー

ラック、インテック・ネットコア、トレンドマイクロ
インターネットセキュリティシステムズ

オブザーバー

総務省、独立行政法人情報通信研究機構
（社）電気通信事業者協会、
（社）テレコムサービス協会
（社）日本インターネットプロバイダー協会

T-ISAC-J会員に求められる活動参加姿勢

- ”Our security depends on your security”を信じ、win-winの関係構築に貢献する意図をもつこと。
- 1事業者では手に負えない大規模な脅威に一致団結して対処すること。
- 連携活動・情報共有はWorking groupを核におこなう。

T-ISAC-Jの機能のイメージ

Telecom ISAC Japan

ISPユーザ

一般のインターネット利用者

（6）広報・セミナー

（5）WG活動

会員企業
オブザーバー

(4)ポータルサイトなど

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

基本情報
・組織紹介
・News
・セミナー情報

DDoS攻撃対応
・ブラックホールIP共同設定
・攻撃状況調査、対策トライアル

BGP経路情報監視
・経路情報
・解析ツール
・障害情報

ボット・Antinny対策
・検体収集
・感染傾向分析
・駆除ツール
・調査、対策結果

CCC運営
・Malware感染者への個別・オーダーメード的な注意喚起

緊急情報交換

(2)センター運用

オペレーションセンター

BGP経路情報監視センター

Cyber Clean Center

企画調整部

(1)情報収集・分析・共有・対策連携

(3) 外部機関連携

NiCT

JPNIC

JPCERT/CC

JPCERT/CC

(0)T-ISAC-J 組織運営・基盤整備

5つの機能で構成
①情報収集
②分析
③共有
④対策連携
⑤（対外的な）告知・啓発

モニタリング用データ

BGP経路情報

Malware系データ

イベント情報
インシデント情報

会員
ISP
ネットワーク

会員

国内外関連情報サイト

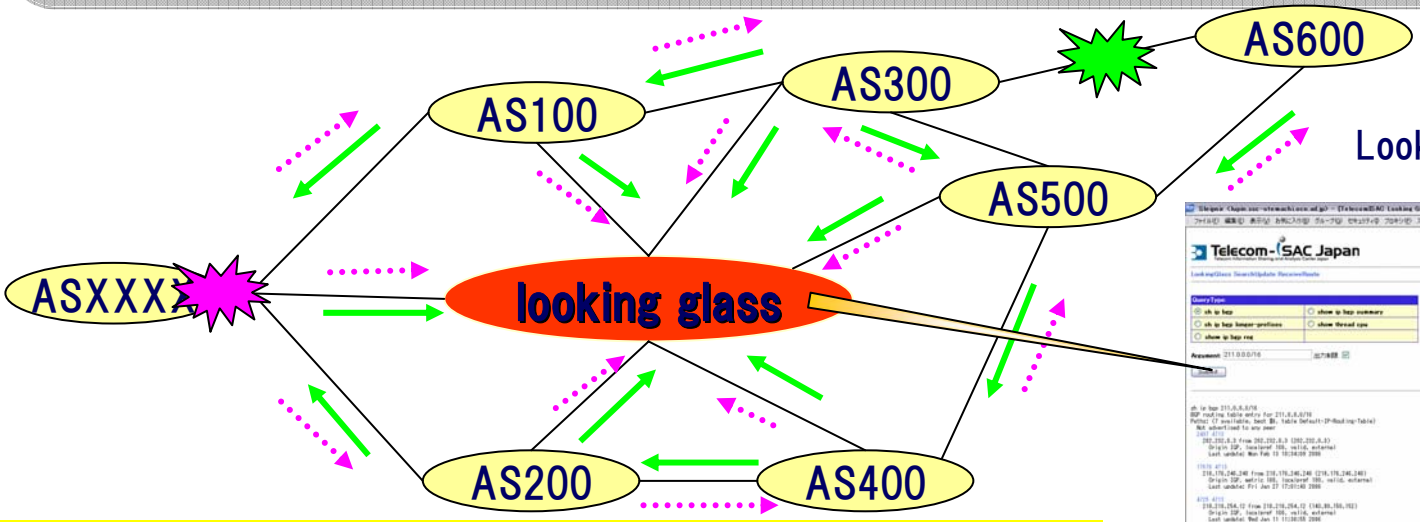
政府関係機関

BGP経路情報共有WGの活動紹介

【WG設置目的】
ISPが行う経路情報運用において発生する脅威（例、BGP経路情報ハイジャック）に、会員が連携して対処するための活動を行う。

【目的実現手段】
T-ISAC-Jの会員ISP(現状7会員）が経路情報を持ち寄り共有することで、複数拠点監視型の経路情報集約ポイント（looking glass）を構築し、運用する。

1. 集約情報を活用した問題点の早期分析を目指す。
2. 誤った経路情報を出すISPの早期特定手段を開発する。
3. 経路情報の早期復旧方法を確立する。

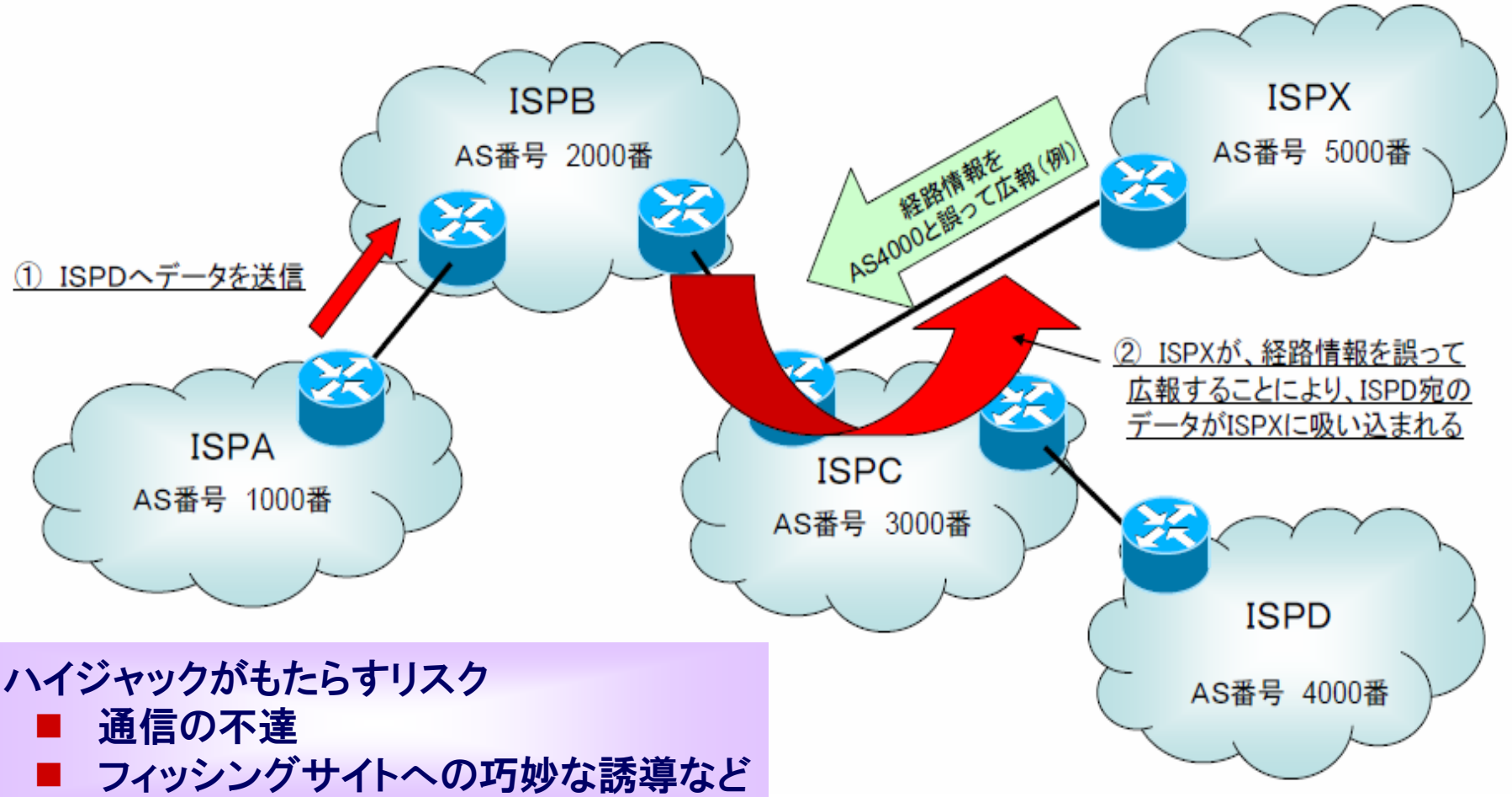


Looking glassシステム画面

【目標】 日本のBGP経路情報の集約ポイントとしたい！

BGP経路情報ハイジャック

・ISPXが経路情報を誤って広報することにより、ISPD宛のデータがISPXに転送される。



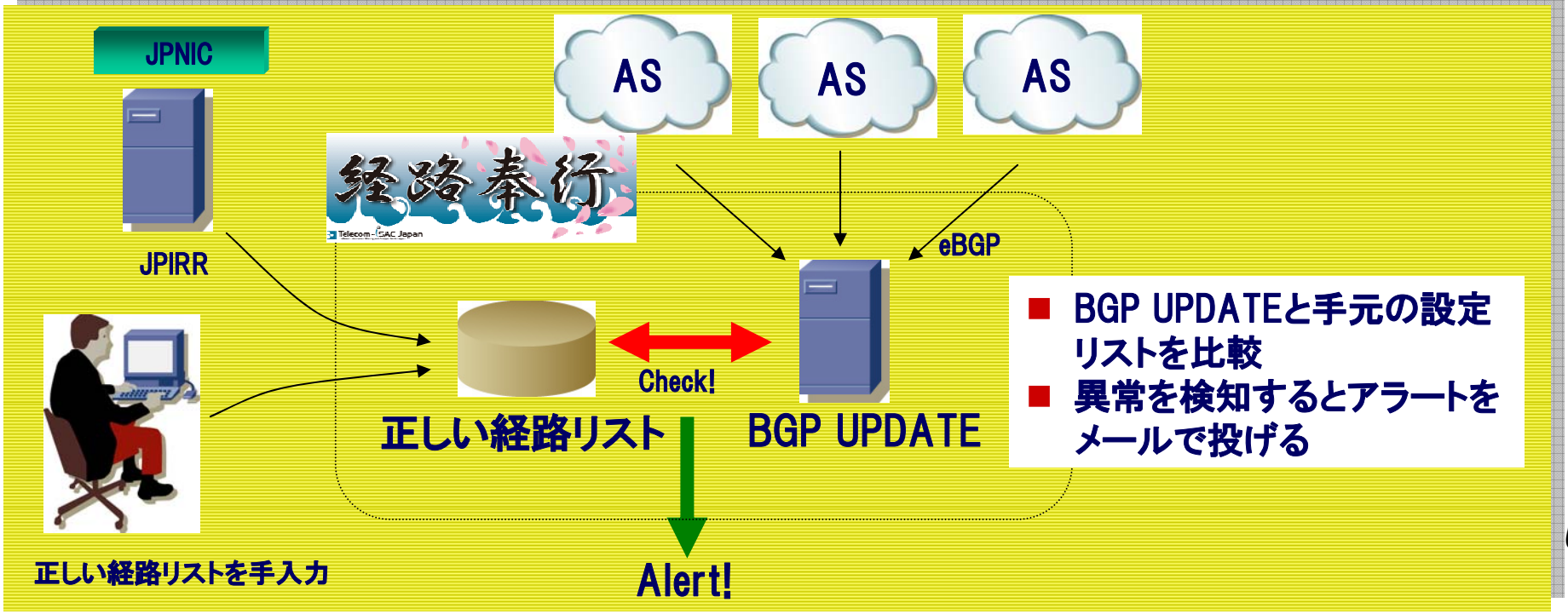
ハイジャックがもたらすリスク
- 通信の不達
- フィッシングサイトへの巧妙な誘導など

【出典】総務省次世代ＩＰインフラ研究会、第２次報告書より

経路奉行(T-ISAC-Jのlooking glass)の仕組み

そもそも、なぜ経路ハイジャックが起こるのか
- どこかで誰かが不正経路の広報を許してる
- 将来的には不正経路が広報できない技術（soBGP, sBGP...)の普及
  （実装を変えるのには時間がかかるけれど...）

そこで、とりあえず目の前にある問題（現状）を見る。
- 不正経路ってどのぐらい流れてるのか？など



経路奉行が検知したアラート状況

2006年

JPIRRを参照開始

	7月	8月	9月	10月	11月	12月
bogon	6	127	9	12	12	14
誤検出	18	38	10	65	7	6
その他 ☹	1		3		7	29

- bogon(駄目)経路
  プライベートブロックやその他bogon経路
  考えられる原因
  - ●実験環境からの漏洩
  - ●typo、設定ミス
  - ●悪用のための一時的な広報か？
- 誤検知
  - ほとんどが特殊経路制御(マルチプルオリジン、パンチングホールなど)
  - 確認後に設定追加
  - 設定を正しく維持すれば減らせる
  - JPIRR参照開始後、誤検出が減少

経路奉行が検知したアラート（その他編）

- その他 ☹(不正経路として検知して然るべき経路)
  - 他のASが何か広報してる・・・
  - 今のところ、設定ミスか原因不明
    - 直したと連絡がある or 勝手に直ってる
    - PNIのpoint-to-pointアドレスの漏洩？typo?設定ミス？

事例1： 2006年11月　韓国方面から、細かい経路でorigin ASが異なる経路
- 生成元に連絡がとれず経由ASの協力を得て解決
- 経由ASでの経路フィルタを実施しつつ、生成元に連絡して経路広報を停止
- 影響時間は16時間ぐらい

事例2： 2006年11月 インドネシア方面から、prefix長は同じでorigin ASが異なる経路
- 該当経路は直ぐに削除された
- 影響時間は5分ぐらい

事例3： 2006年12月　日本方面から細かい経路でorigin ASが異なる経路
- 広報元に連絡、対応してもらった
- 影響時間は23分ぐらい

事例4:この2ヶ月で3件、経路奉行参加以外のJPIRR Maintainerから検知
- ハイジャックなのか誤検知なのかは不明

経路奉行、システム改善課題

1. 経路情報の収集量を増やす
   - 収集ASを増やす。
   - 大きなネットワークの場合には多くの拠点から経路情報を集める。
   - 検知システムへの経路情報の到達性を改善

2. 経路の判別方法の改善
   - 判別に使用する属性（パス属性、状態変化など）を増やす。

3. 通知方法の工夫

など

ボットネット実態調査

１．感染状況の調査（2005年3月～5月に調査）

- 日本のISPユーザの 2～2.5% がボットプログラムに感染していることが判明（およそ40万～60万台の感染PCが存在）
- おとりに一日約80種類のボット検体がひっかかる。そのうち70種類は未知な検体

２．マイボット飼育・攻撃能力調査

- 試験環境下でボットネットを構築
- ノートPC１台でもインターネット上で200Mbps以上だせることが判明
- PCからの情報漏洩、巧妙なスパム他、多機能を満載

仮にこれら全てのPCをサイバー攻撃に同時に悪用すれば、世界中のインターネットを破壊することすら可能。

ボット対策プロジェクトスタート！

経済 >> 記事一覧

▼トップ　景気ウオッチ

http://www.nikkei.co.jp/news/keizai/20061128AT3S2700M27112006.html

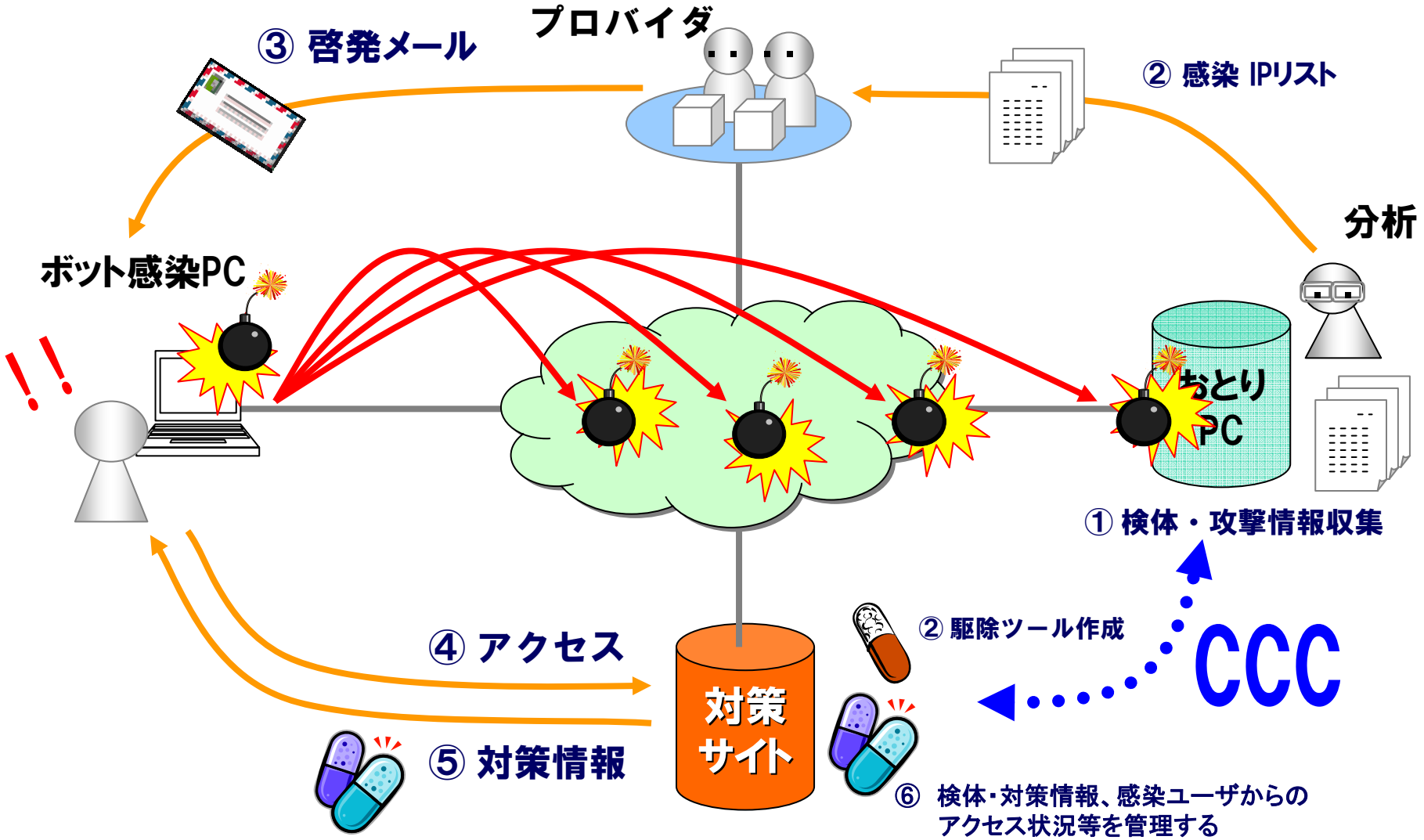
新型コンピューターウイルス「ボット」、政府が撲滅に着手

総務省は経済産業省と共同で、他人のパソコンに命令して特定のホームページを攻撃したり、大量の迷惑メールを送りつける新型のコンピューターウイルス「ボット」を撲滅するための対策に着手する。国内で「ボット」による被害とみられる事例が増えているためだ。駆除ソフトを開発して無償で配布する。

「ボット」は他人のパソコンを無断で操作するのを目的に作られたプログラムで、感染すると外部に乗っ取られてしまう。利用者が気づかないうちに個人情報を盗んだり、特定のホームページに数百万台で攻撃を仕掛けたりする。国内でインターネットに接続しているパソコンのうち40万―50万台が感染しているとみられ、被害は年々拡大している。(07:01)

サイバークリーンセンター（CCC）の設置運営による
ボット駆除に向けた地道な取り組みを行う

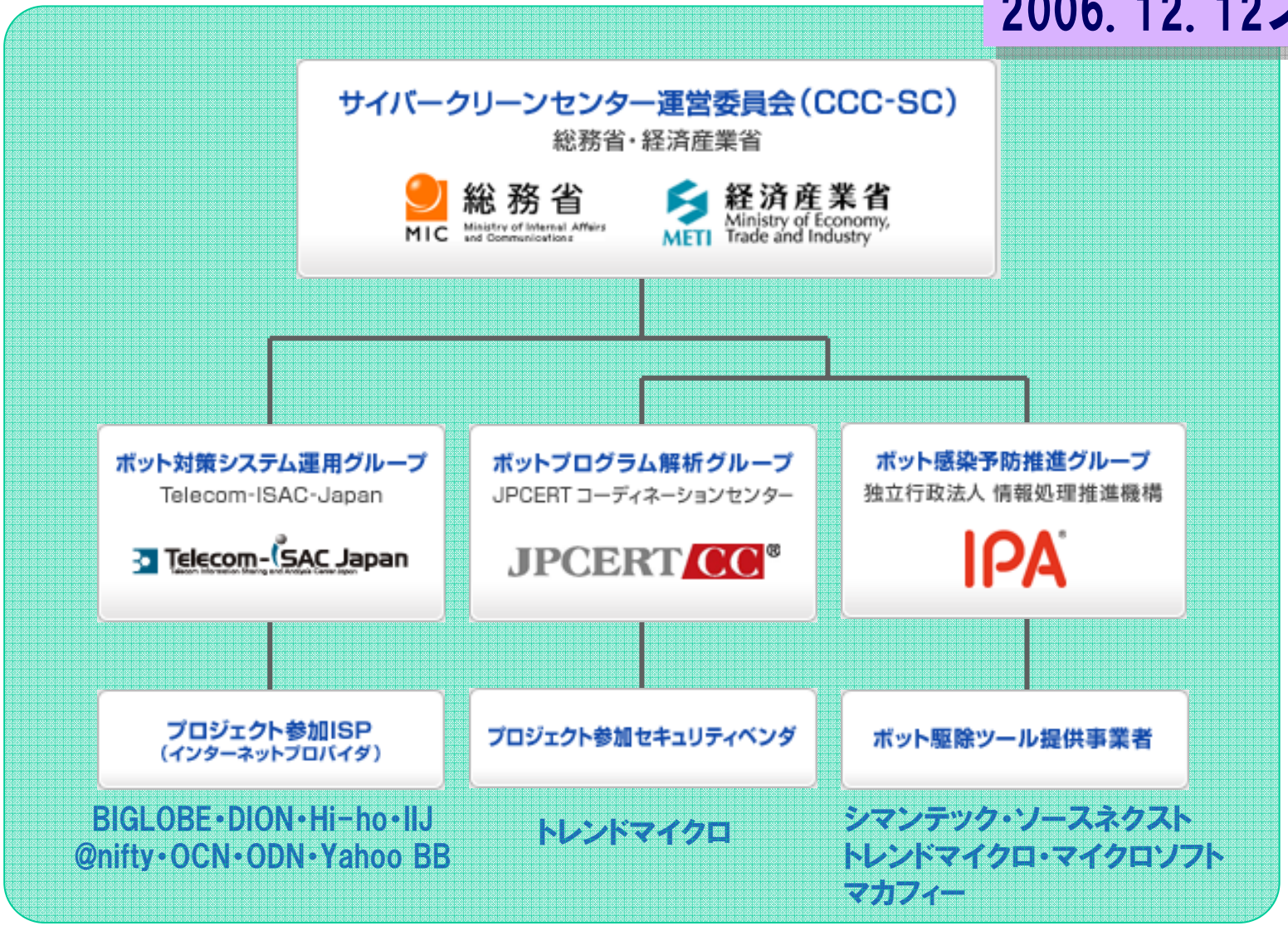
ボット感染者対策ワークフロー



● 実際の感染者に対し注意喚起するとともに、確実に対策情報を届け「オーダーメイド治療」を実施

サイバークリーンセンター運営体制

2006.12.12スタート



サイバークリーンセンター専用ポータルサイト

- 一般ユーザ向け啓発サイト

- ボット感染者向け対策サイト

https://www.ccc.go.jp/

対策完了連絡【ボット感染者向け対策サイト】

注意喚起実施状況

注意喚起実施	ハニーポット取れ高		注意喚起対象者の反応			
	IPアドレス数（ユニーク数）	検体数（Hashユニーク数）	①TOPページ	②ツールDL	③Win UP	④結果報告アンケート回答
テスト実施						
2006.12.15	約100	約300	30%	26%	12%	17%
2007.1.25	約600	約350+α	24%	20%	8%	13%
【参考】Antinny対応	約12000	――――	39%	36%	23%	34%
本格実施（2007.2～）	約1000/日	約600/日	?	?	?	?

・アンケート結果比較（駆除結果）

	第1回	第2回
駆除成功	57%	72%
駆除失敗	0%	5%
検出しない	43%	23%

→ 考察① 駆除精度の向上

・アンケート結果比較（駆除ソフト）

	第1回	第2回
AV導入済み	29%	50%
AV導入なし	71%	50%
AV期限切	0%	0%

→ 考察② 対策完了報告データの信頼性

整理学： T-ISAC-Jの取組事項

1. 通信実態(問題)の可視化と対策の試行
   - ■対策情報等の試行結果を情報共有する
   - ■欲しい情報は自分で見つけないと手に入らない
     - 「経路奉行(会員ISPから提供されるBGP経路情報を蓄積・共有するLooking glassシステム)」によるBGP経路情報の監視
     - ハニーポット運用を通じたボット感染実態調査

2. T-ISAC-Jの名前による警鐘や啓発
   - Antinny感染ユーザへの注意喚起

3. 汚れたインターネットを浄化するための試行
   - Antinny等のウィルス対策の試行
   - サイバークリーンセンターによるMalware感染者へのオーダーメード治療
   - 適法性を確保したトライアルの展開(例、DDoS攻撃対応)

T-ISAC-J会員に求められる活動参加姿勢
- ”Our security depends on your security”を信じ、win-winの関係構築に貢献する意図をもつこと。
- 1事業者では手に負えない大規模な脅威に一致団結して対処すること。
- 連携活動・情報共有はWorking groupを核におこなう。