NSP-SEC &

NSP-Security-JP

(NSP-SEC-JP)

Peers Working Together to Battle Attacks to the Internet

JANOG - July 2004

Danny McPherson <danny@arbor.net>
Taka Mizuguchi <taka@ntt.net>

Agenda

- NSP-SECとは？

  ～アメリカでのNSP-SECの活動状況～
- NSP-SEC-JPとは？
- NSP-SEC-JP立ち上げに至った経緯
- 他団体との違い（JPCERT/CC、TelecomISAC、etc.）
- NSP-SEC-JPの活動
- NSP-SEC-JPの参加条件・フロー
- 今後のスケジュール

2002 – *実際にあった*セキュリティ問題

The *Real* Security Problem

- 2002年9月頃、ISP/SP *セキュリティ運用*技術者は以下のことができなかった:

  September 2002 ISP/SP Operations Security Engineers could not:

  – 直接接続されているピア相手の知り合いの *セキュリティ*技術担当者を見つけられなかった

    Find their *security* colleagues in their directly attached peers.

  – 2 Hop 離れているプロバイダだとセキュリティ技術者自体が見つけられなかった

    Find security engineers in providers two hops away.

  – アジア地域だとまったくもってセキュリティ技術者を見つけられなかった

    Find ANY security engineers in the Asian providers.

- 大きなセキュリティ攻撃があった場合、まずそもそも共同に攻撃に対して効果的にアクションをとる以前の問題である、誰と一緒に作業をすればいいのかすらわからなかった

  When big attacks happened, there was no way for the people who needed to work with each other to find/contact one another … let alone work collectively to mitigate the attack.

2003 – 変化が起こった年
A Year of Difference

- 2003年9月　ISP/SPセキュリティ運用者は以下が可能になった

  September 2003 ISP/SP Operations Security Engineers Can:

  – 直接接続されているピアやグローバルISPだと知っているセキュリティ技術担当者を見つけることができる

    Find their *security* colleagues in their direct peers and a huge range of global ISP/SPs

  – メール、チャット、iNOC電話、電話などを用いてインターネット上の攻撃等に共同で対応できるようになった

    Work with each other via email, chat, iNOC Phone, and POTs to collectively mitigate attacks and incidents on the Internet

  – プロバイダ間でTracebackや対応をできる

    Execute inter-provider traceback and mitigation

  – 起こることが予測されている攻撃(Blaster等)に対して事前対応できた

    Apply proactive measures to prepare for projected attacks (e.g., Blaster)

- **What changed?**

NSP-SEC

NSP-SECは一部ISP/SPセキュリティエンジニアによって以下の目的を持って設立されました

NSP-SEC was created by several ISP/SP Security Engineers as a means to meet the following objectives:

1. ISP/SPセキュリティエンジニアに共同で作業ができる相手を見つけること

   Provide a means for ISP/SP Security Engineers to find their colleagues.

2. ISP/SPセキュリティエンジニアにDOS攻撃等に対する対応ができるグループを作ること

   Create a potential forum for ISP/SP Security Engineers to work on DOS attacks, Incidents, and other activities.

対応者を見つけること自体が鍵だった
Finding Colleagues was the Key

- 知ってること:

  We know that:

  – 対応をするにあたって、一人より二人の技術者で対応したほうが効果的

  two engineers working together to mitigate an incident is more effective than one engineer working alone.

  – 対応はエンジニア同士が連絡をしながら行ったほうが早い

  incident mitigation is faster if engineers can communicate with each other during an incident.

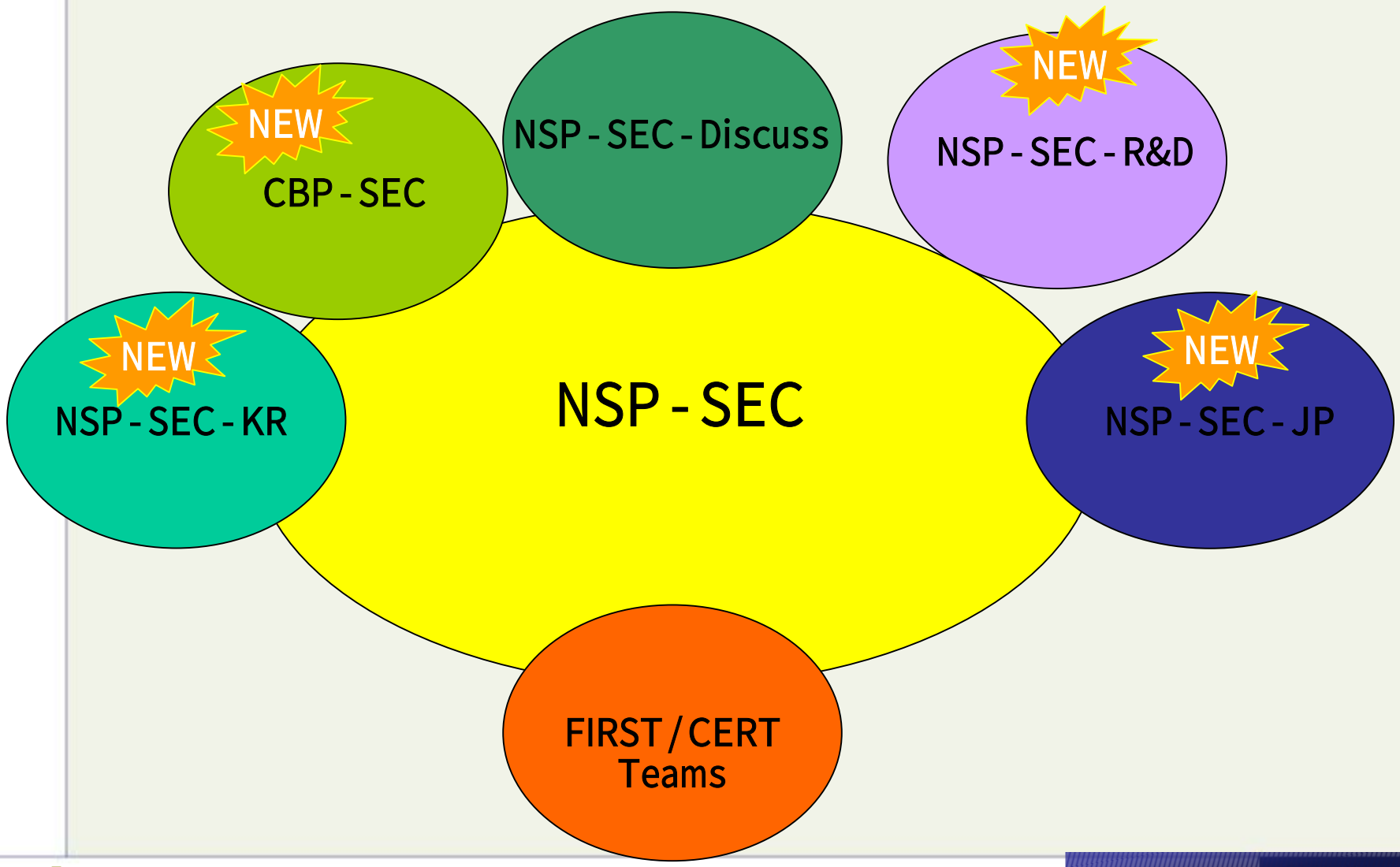
- NSP-SECはその対応者を探して、もしかして対応を共同に行える人を探す手段を与えます

  NSP-SEC provides that means to find colleagues and perhaps – work on the incidents.

  – 共同作業がNSP-SEC上でやらなくてはいけないわけではなくて、“1対1”のNSP-SEC外の共同作業は起こっているし、その方が推薦されている

  It is not the exclusive mode of collaboration. “Point to Point” collaboration outside of NSP-SEC does happen and is strongly promoted.

Mitigation Communities



NSP-SEC – The Details

- NSP-SEC ー NSP/ISPで働いていて、セキュリティインシデントに対して実際に対応をしている技術者に対する*閉じたオペレーションフォーラム*

  NSP-SEC – *Closed* Security Operations Forum for engineers actively working with NSPs/ISPs to mitigate security incidents.

- 参加している個人の参加資格･信頼度をチェックするために複数のレイヤでの確認作業

  Multiple Layers of sanity checking the applicability and trust levels of individuals.

- 完璧を目指していないが、今まではよい状況を目指しています

  Not meant to be perfect – just better than what we had before.

http://puck.nether.net/mailman/listinfo/nsp-security

NSP-SECメンバー参加資格
NSP-SEC Membership Requirements

NSP-SECへの参加資格は実際にNSPセキュリティ事件に対して主体的に対応を行っている人間に限られています。よって、参加資格としてはオペレータ、ベンダー、研究者、FIRSTの人等NSPセキュリティインシデントを止めるために対応している人間になっています。これが何を意味をしているかというと、報道関係者は無しですし、”悪者”も除いています。

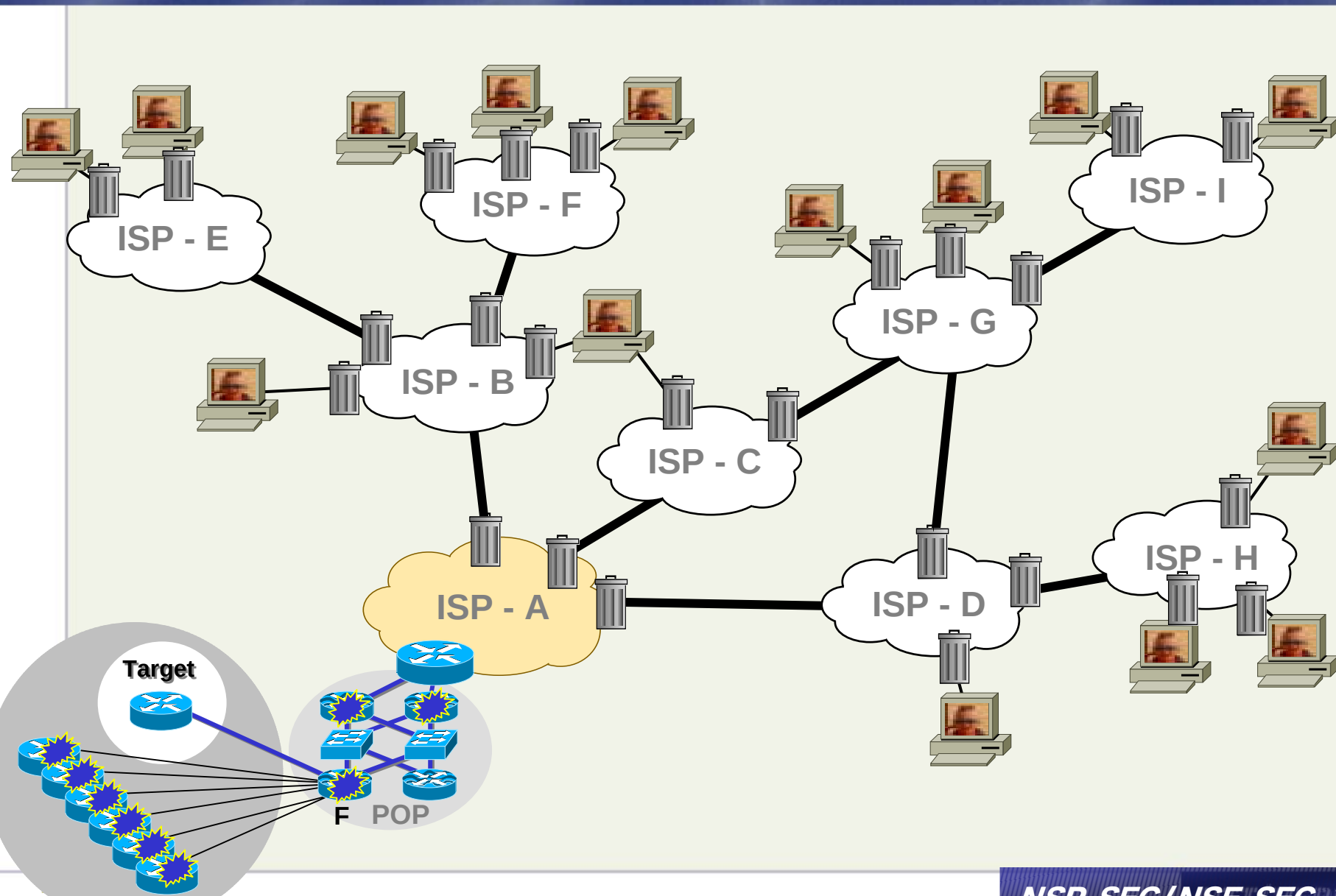
Membership in nsp-sec is restricted to those actively involved in mitigation of NSP Security incidents. Therefore, it will be limited to operators, vendors, researchers, and people in the FIRST community working to stop NSP Security incidents. That means no press and (hopefully) none of the "bad guys.“

http://puck.nether.net/mailman/listinfo/nsp-security

NSP-SEC 参加資格
NSP-SEC Membership Requirements

- “セキュリティに詳しい人”ではNSP-SECの参加資格を満たしているとはいえません
  - **Being a “Security Guru” does not qualify for NSP-SEC Membership.**
- “*国や地方自治体*”ではNSP-SECの参加資格を満たしているとはいえません
  - **Being “from the *Government*” does not qualify for NSP-SEC Membership.**
- 実際にISP/SPバックボーンのルータの設定ができる人、誰かに設定を指示できる人、フォーラムに貢献できる人、やグループにBCPを提供できる人である必要があります
  - **You need to be someone who *touches* a router in a ISP/SP backbone, can tell someone to *touch* a router, offer some service to the forum, or develop BCPs for the community.**
- ROMはお断りです。貢献できない人はリストから外されます
  - **NO LURKERS! If you do not contribute, you get punted off.**

NSP-SEC: Daily DDOS Mitigation Work



運用上の信頼関係
It's all about *Operational Trust*

- プロバイダ間の対応には、運用上の信頼関係が必要なんです
  - **Inter-Provider Mitigation Require Operations Trust.**

情報の守秘、営業活動等に利用しない、報道関係者には教えない、一般のCERT等には伝えないようにするために、共同対応した仲間を、信頼する必要があります

You need to trust your colleagues to keep the information confidential, not use it for competitive gain, not tell the press, and not tell the commercial CERTS and *Virus* circus.

よって、すべての参加要求はNSP-SEC管理者によってチェックされて、そしてほかの人たちの投票によって決められます

So all membership applications are reviewed by the NSP-SEC Administrators and Vetted/Approved by the membership.

すべてのメンバーは6カ月おきに参加資格について見直しが入ります

All memberships are reviewed and re-vetted every 6 months – letting the membership judge their peer's actions and in-actions.

NSP-SECが違うもの・・・
NSP-SEC is not ….

- 完璧じゃない
  - NSP-SEC is not perfect
- 全てのISP間のセキュリティ調整を解決するものではない
  - NSP-SEC is not to solve all the challenges of inter-provider security coordination
- 究極の解決策ではない
  - NSP-SEC is not the *ultimate solution.*
- *でも、今までのインターネット上のセキュリティ問題に対して有効であったこともあった*
  - *But NSP-SEC does impact the security of the Internet:*
    - Example: Slammer

Slammerの時のNSP-SECの対応
NSP-SEC's Role during Slammer

- ISPが最初に何かが起こっていることに気づいた

  The ISPs were the first to notice something was happening.

  – 回線が輻輳し、ルータが飛び、BGPセッションがFlapし、お客様が文句を言い出した

    –Circuits saturated, routers spiking, BGP sessions flapped, and customers complained.

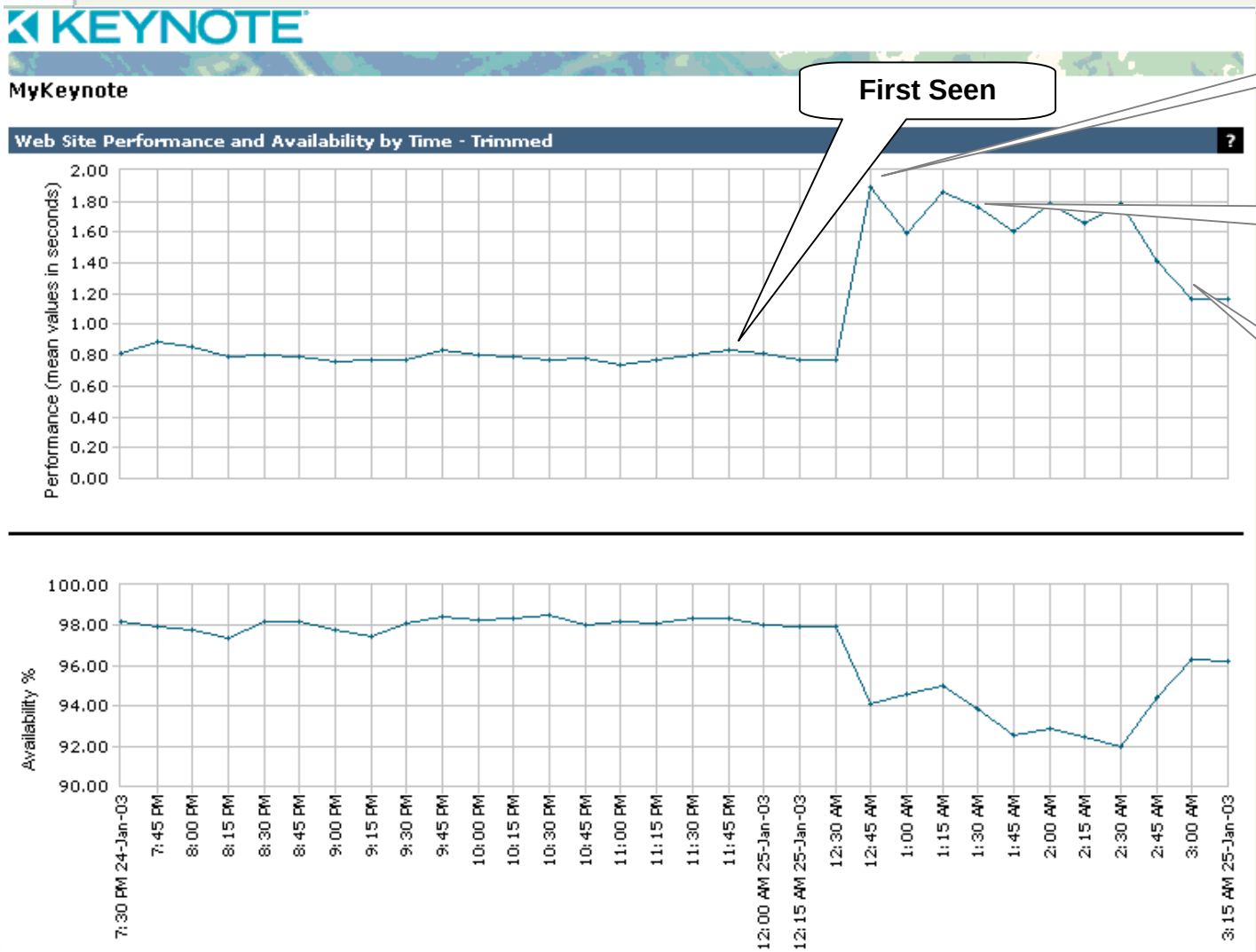
- NSP-SECが最初にWormについて報告した。CERT/FIRST TeamはNSP-SECからアラームを得た

  NSP-SEC was the first reporter of the worm. CERT/FIRST Teams got their alert from NSP-SEC.

- NSP-SECメンバーがパケットダンプしたり、Wormを解析したりして、どのようにWormを閉じ込めるか考えた人達だった

  - NSP-SEC members were the ones who dump the packets, analyzed the worm, characterized its spread, and came up with a way to contain the worm.

Impact of NSP-SEC's Containment



First Seen

Real Impact

Containment Starts

Containment Takes Effect

4:00 a.m. PST Containment

In the Skitter Core

NSP-SEC-DISCUSS

- NSP-SEC上は対応が実際に行われるところで、そこで何かを学んだりするところではない。知っていることが期待されている
  - NSP-SEC is where the mitigation takes place. You do not learn anything, you are already expected to know.
- NSP-SEC-DISCUSS(NSP-SEC-D)で色々と学んだり、新しい対応方法を学んだりするところである
  - NSP-SEC-DISCUSS (NSP-SEC-D) is the place to learn, consult, work on new mitigation techniques, and lurk (if you want to).

http://puck.nether.net/mailman/listinfo/nsp-security-discuss

NSP-SEC-D Membership

- **NSP-SECでは参加資格が無くても、NSP-SEC-Dには参加資格がありえることもある**
  - **People who would not qualify for NSP-SEC MAY qualify for NSP-SEC-D.**
  - **セキュリティ製品を開発しているベンダーなど**

    Vendors with Security Engineers developing products.
  - **ISPで仕事をしているセキュリティコンサルタント**

    Security *Consultants* working with ISPs.
  - **セキュリティ調査をしている人**

    Security Researchers.
  - **FIRST/CERT等の担当者**

    The masses of FIRSTs/CERTs

NSP-SEC-D Topics

- Best Common Practice(BCP)の開発- 新しいツールやテクニックなどを使って、コミュニティで役に立つものを模索
  - Best Common Practice (BCP) Development – working on new tools and techniques that will work in the community.
- プロバイダ間での共同作業対応フローの模索 ー 経験から学んで、よりよくしていく
  - Inter-Provider Coordination Procedures – learning from experience and moving forward.
- Proactive対応に向けた調査 ー 何が将来起こるかを起こる前に検討して、Proactiveに対応を準備する
  - Proactive Forensic Analysis – Looking at what is going to happen, before it happens, and prepare proactive mitigation.

NSP-SEC Techniques & Tools

- Remote Triggered Black Hole
- Sink Holes configured as scan analyzers
- Sink Holes configured as backscatter collectors.
- BGP Prefix Filtering
- ACLs

NSP SEC Meetings

- **NANOG Security BOFs (www.nanog.org)**
  Chaperons/Facilitators:
  Merike Kaeo - kaeo@merike.com
  Barry Raveendran Greene bgreene@senki.org
  Danny McPherson danny@arbor.net

- **RIPE Security BOFs (www.ripe.net)**
  Coordinator:
  Hank Nussbacher - hank@att.net.il

- **APRICOT Security BOFs (www.apricot.net)**
  Coordinators/Facilitators:
  Derek Tay - dt@agcx.net
  Dylan Greene - dylan@juniper.net

- **JANOG 14 (www.janog.gr.jp)**
  Danny McPherson - danny@arbor.net
  Taka Mizuguchi - taka@ntt.net

NSP-SEC Action List

- Back-Up E-mail Servers (response to the US N. East Black Out)
- Secure Chat Areas that are on all the time.
- iNOC Phone Based Conference Calls
- NSP-SEC Contact List

What can you do to help?

- もしあなたがルータを設定していて、オペレーションにいて、ISPセキュリティ対応をしている場合は、nsp-secへの参加をしてください
  - If you configure routers, are in operations, and handle ISP Security, then apply for nsp-sec membership:

    http://puck.nether.net/mailman/listinfo/nsp-security
- NSP-SECは各ISPから2，3名のルータを設定できて、セキュリティ事件に対する対応ができる技術者を探しています
  - NSP-SEC is looking for two or three engineers from each ISP who has the authority to configure routers and handle security incidents.

NSP-SEC-JPとは？

- NSP-SECのSub-communityとして立上げ（NSP-SECと連携）
- MLのメンバは、ISP / ICP及びベンダのセキュリティ関連のオペレータの有志
- 非公開（クローズドなconfidential情報交換も有）
- リアルタイムでのセキュリティインシデント対応ML
- セキュリティに関する啓蒙活動も考慮

NSP-SEC-JP立ち上げに至った経緯

- NSP-SECの課題
- 日本のセキュリティインシデントの状況
- セキュリティの担当者がいない
- 言葉の高い壁

NSP-SECの課題

- アジアにおけるセキュリティ発生率は高い
- アジアからの参加者が少ない
- 言語（エリア）毎のNSP-SECが必要かも…
- スケールの技術的な挑戦？

エリア別、国別、言語別なNSP-SEC-xx

ってあると便利かも

日本のセキュリティインシデント

～感染しているホストが存在するASの数～

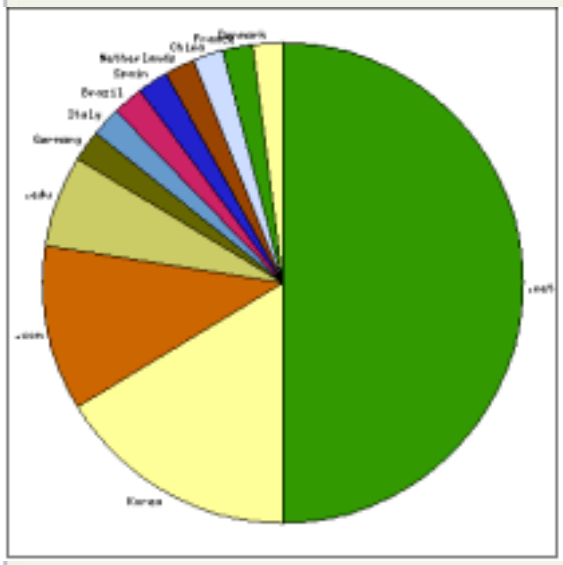
- Beagle に感染しているAS: 69 (約14％)
- Blasterに感染しているAS: 76 (約15％)
- Mydoomに感染しているAS: 26 (約5％)
- Nachiに感染しているAS: 28 (約5％)
- Slammerのホストが存在するAS: 68 (約14％)
- SPAMのホストが存在するAS: 130 (約26％)

JPNICによるAS割り当て数：494 (2004/06/18現在)

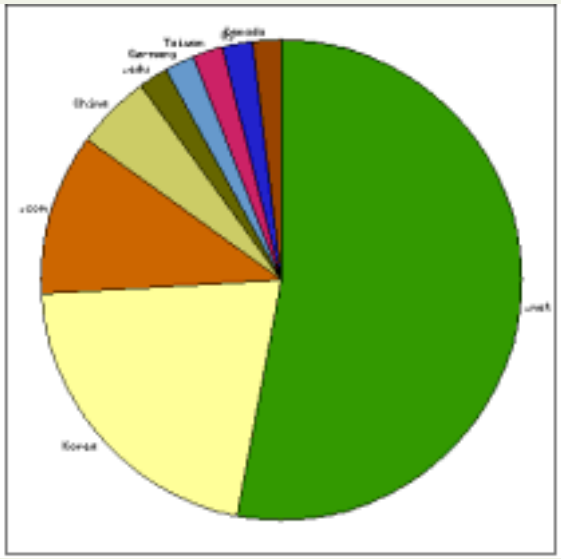
Data from Team Cymru project

Worm Demographics

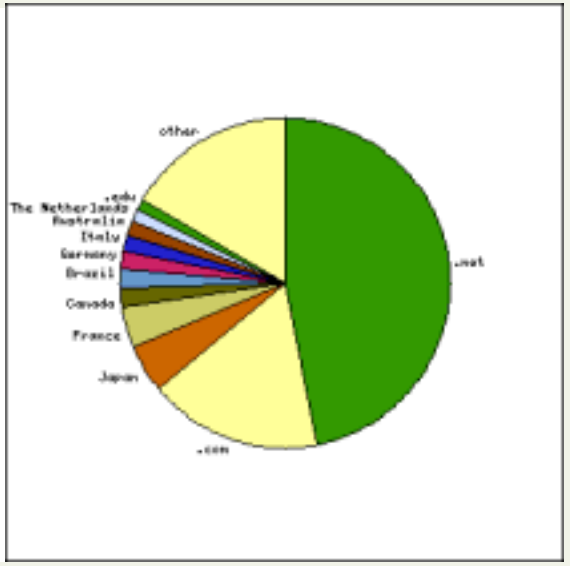
Code Red



Nimda



Blaster



#Data from Arbor Networks Inc.

NSP-SECの状況

- NSP-SECに参加している日本ISPのオペレータの数（.jpドメインのアカウントを持っている）
  - 2497　　2人
  - 4713　　3人
  - 2914　　2人

日本のISPのセキュリティインシデントは多いが、参加ISPが圧倒的に少ない・・・

ISPのセキュリティ担当

アメリカでは、多くのISPにセキュリティ担当者（security@）を配置して、リアルタイムセキュリティ対応等を実施している。

仕事内容：

- リアルタイムセキュリティインシデント（DDoS,hacking,不正アクセス等）時の緊急対応
- インシデントのレポーティング
- SPAM対応
- 捜査当局（FBI、州及びローカルの警察）との対応

日本のISPにセキュリティ担当者は居るのだろうか？

言葉（English）の高い壁

日本人には英語の壁は高いのでは？

- メールの読み書きは出来てもスピードは数倍…
- 英語のメールは取りあえず飛ばす
- アメリカンジョークでは笑えない
- 英語を見ると虫唾が走る
- 体が受け付けない…
- 英語って何？

他の団体との違いは？

- 無料のML登録
  - ー会員制ではない
- ML参加者の審査による参加承認フロー
  - ーでもクローズなMLだから、confidential
- クローズなMLだからできるセキュリティ情報交換
- リアルタイムなセキュリティインシデントの対応
- ISP全体での大規模セキュリティインシデント（DDoS等）対処方法の相談（DNS, black holing）？

ISPの、ISPによる、ISPのためのML

＃将来的には他団体との連携は必要だろうと考えています

NSP-SEC-JPの活動

- リアルタイムセキュリティインシデント対応
- NSP-SECとの連携（模索中…）
- セキュリティ情報の発信
- 他プロジェクトとの連携

  Team Cymru

  IMS(Internet Motion Sensor)

リアルタイムセキュリティインシデント対応

- セキュリティアタックが発見された場合、MLに対応依頼をする。各ISPのメンバは自ASに関係するセキュリティインシデントに対して即座に対応を実施する

例:

DDoS attack against x.x.x.x.

以下のホストから“x.x.x.x”に対して443ポートの大規模なアタックがあります。

対処願います。

ASN	IP address	Name
2914	61.120.xxx.yy	VRIO Verio, Inc.
2914	210.175.xxx.zz	VRIO Verio, Inc.
4713	210.145.xxx.yy	OCN NTT Communications Corpora
4713	210.154.xxx.yy	OCN NTT Communications Corpora

NSP-SECとの連携

- 基本的にお互いのMLのConfidentialityを確保
- リアルタイムセキュリティインシデント対応時の連携
- セキュリティに関するML間の情報のトランスファ
- 将来的なNSP-SECとのsub-communityとしての技術的な連携（compromised hostを分離しての対応）
- NSP-SEC-DISCUSSの持つ、新しい技術の習得、コンサル機能も持ち合わせる

セキュリティ情報の発信

- ベンダさんからのセキュリティ情報の発信
- ISP間のセキュリティ情報の共有 / 交換
- セキュリティ対策に関する議論

他プロジェクトとの連携(Team Cymru)

- Team Cymruへの協力
  - Virus/Attackに関するWeekly report

例:

“The weekly Mydoom report”が出ました。“21 JUN 2004"の週のリストでは、“624”ASN中、“5106”のホストがあります。

251x

251x

471x

:

  - Team Cymruドキュメントの日本語化のサポート(予定)

管理者（NSP-SEC-JP-OWNER）の役割

- NSP-SECにも参加し、NSP-SEC-OWNERとの連携
- NSP-SEC-JPに関する以下の各種作業をボランティアベースで実施
- 加入・脱退等の作業

  加入依頼が来たときの、初期審査および、MLでの審査（48時間以内にML参加者二人以上による保証が条件）の依頼

- 除名

  管理者の半数以上の同意により、参加者の除名や参加志願者の拒否を決定する時があります。

- 管理者：

AS2497	IIJ	松崎　吉伸
AS2914	NTT/VERIO	水口　孝則
AS4713	OCN	吉田　友哉

NSP-SEC-JPの求める参加者

- ISPやそれに準ずるネットワークを運用している
- セキュリティ対応が仕事に含まれる
- NSP-SEC-JPに対して無償で観測、分析したデータ等やその他協力を提供できる
- ルータや機器に実際にログインして操作することが組織内で許されていて、しかもアタックが発生している際には何らかの対応ができる。もしくは、誰か 適切な人に指示してこれらの対応させることができる
- NSP-SEC-JPの活動に時間を使える
- 国際のPOPやリンクを持つISPはNSP-SECに加入することをお奨めします。

NSP-SEC-JP参加までのフロー

- 参加資格を満たしている場合（NSP-SEC-JP OWNERにて判断）

- 下記の「自己紹介」をメールでnsp-security-jp-owner@puck.nether.net宛てに送信し た上で、WEBのフォームからnsp-security-jpの購読を申し込んでください。

  名前:
  e-mail:
  Tel(日中):
  Tel(夜間休日):
  iNOC Phone:
  組織名:
  対応可能なAS番号:
  職務内容:
  信用照会先(名前、e-mail):
  PGP鍵の登録先:

  職務内容はできるだけ詳しく教えて下さい。信用照会先にはインターネット業界であなたの身元を保証できる人を記載して下さい。

- 審査（48時間以内にML参加者二人以上による保証が条件）

- nsp-security-jpの世界へようこそ!!

NSP-SEC-JPの活動と今後の予定

2004/1	NSP-SEC-OWNERメンバとメール交換が始まる
2004/2	APRICOTでのNSP-SEC BoF参加
2004/5	NANOGにてNSP-SEC moderatorと飲む
	nsp-security-jpスタート
2004/6	FIRST@budapestでの紹介
	Team cymru Weeklyレポート開始
2004/7	JANOGでの周知
2004/10	NANOGでまた飲む (予定)

参考URL:

http://puck.nether.net/mailman/listinfo/nsp-security

http://puck.nether.net/mailman/listinfo/nsp-security-discuss

http://puck.nether.net/mailman/listinfo/nsp-security-jp

http://www.cymru.com/

Special thanks to

日本語翻訳:	NTT-Com	森信 拓 様
Team Cymru:		Mr.Dave DEITRICH
NSP-SEC:		Mr. Barry GREENE
NSP-SEC-JP owner:	IIJ	松崎 吉伸 様
	OCN	吉田 友哉 様