NTTPCCOMMUNICATIONS

資料2－4

次世代情報セキュリティ対策について

啓発だけでは不十分「永遠のビギナー」対策が最大の課題

平成19年12月5日

NTTPCコミュニケーションズ

小山覚

NWセキュリティ対策における官民の役割分担イメージ

NTT PC COMMUNICATIONS

◆インターネットを利用するために必要な知識を持たず、正しい判断と行動が出来ないユーザ（子供などの若年層を含む）の実態に即したセキュリティ対策が必要

国の役割（受動的リスク対策）
- ユーザが選択困難なリスク対策
- 法制度・先導的な研究開発・標準化・情報判断基準　等

インターネットに接続するだけで被害を受ける ①

特定のWebサイトを訪問すると被害を受ける ②

違法・有害情報サイト（著作権等の権利侵害） ③

SPAMメール ウィルス感染 情報漏えい ④

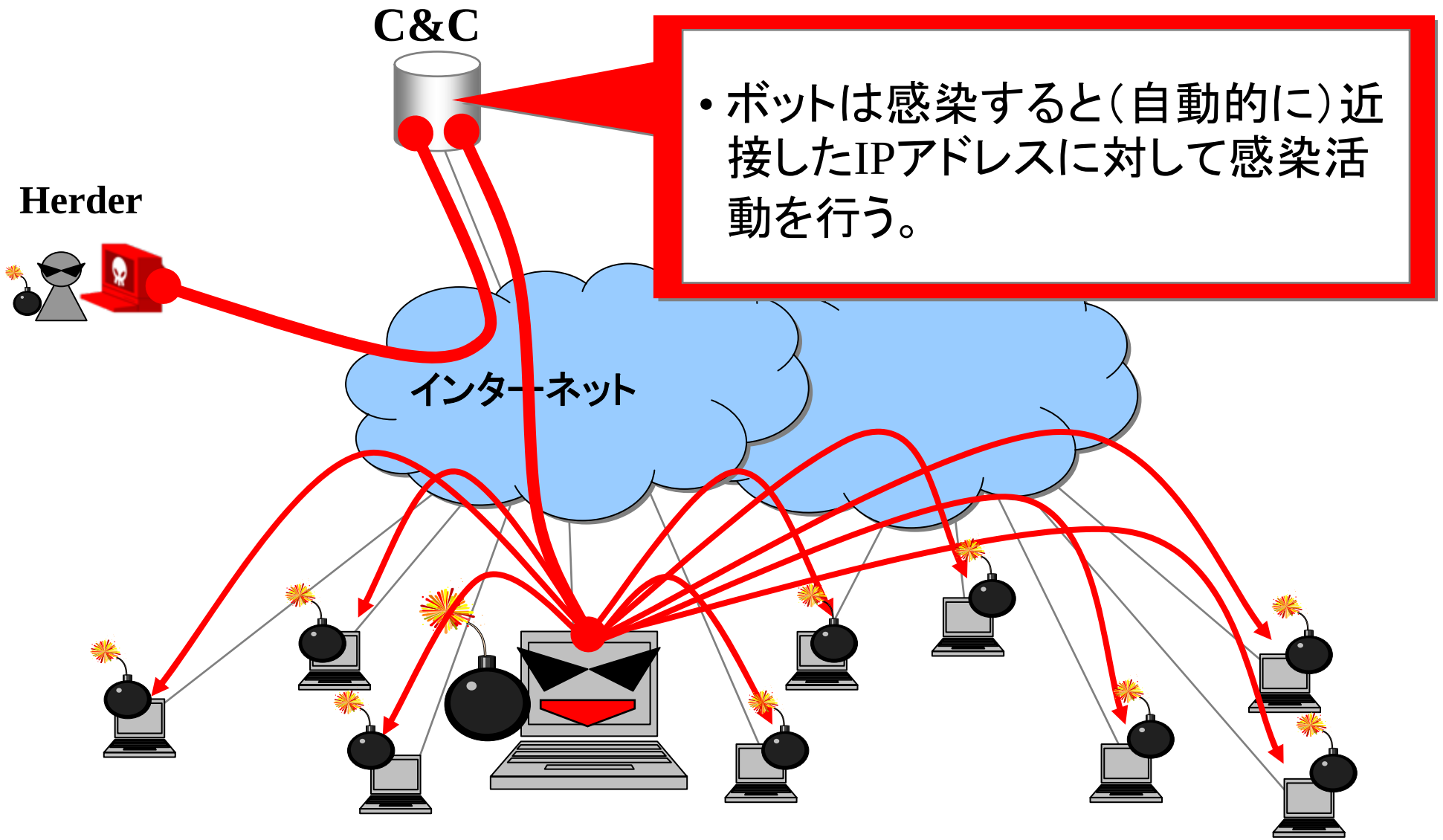
事業者の役割（能動的リスク対策）
- 事業継続のためのリスク対策
- ユーザが選択可能なリスク対策を受益者負担でサービス提供

安全（安心）・安定・便利・安価

① インターネットに接続するだけで被害を受ける

つなぐと感染しやすいISPと、そうでないISPが存在する？

IPアドレス帯によって攻撃の多寡がある理由

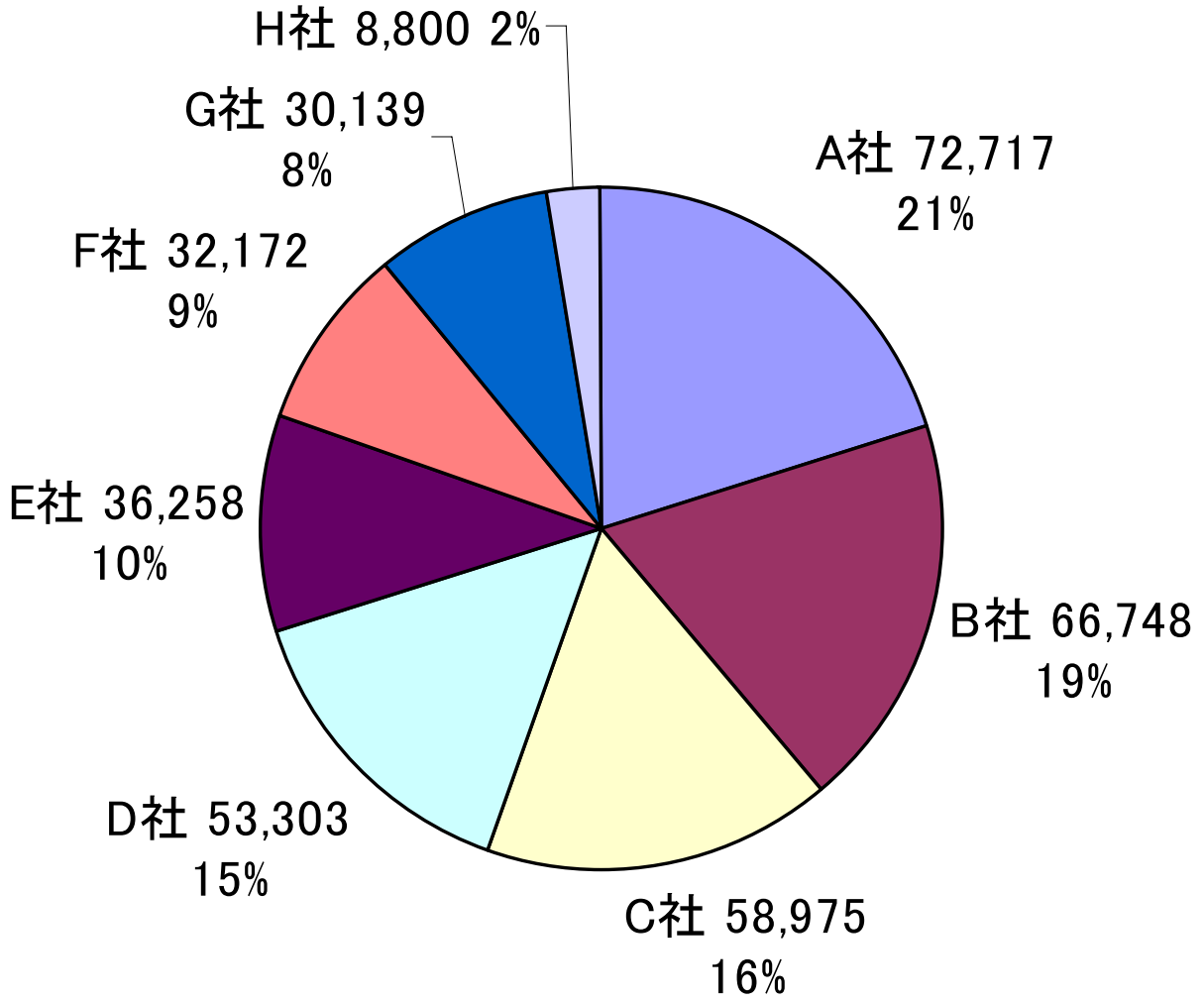


- ボットは感染すると（自動的に）近接したIPアドレスに対して感染活動を行う。

ISP別検体取得数/1台（2007.2.1～8.19）

NTT PC COMMUNICATIONS

OCN, KDDI, Hi-Ho, YahooBB, IIJ, BIGLOBE, @nifty, ODN



感染数にバラつきが出る想定理由

NTT PC COMMUNICATIONS

ISP単位にバラつきが出る理由

◆ マルウェアが感染に使う通信ポートをISPがフィルタリングしている
- マイクロソフトOSの脆弱性を狙う攻撃がよく使う通信ポート
  - TCP 135, 137, 139, 445 等々（過去ワーム蔓延時の救急避難的対策のなごり）

◆ ADSLモデム等でブリッジタイプを利用しているユーザ数の多いISP

◆ 初期型マンションインターネットの多いISP

感染しやすいユーザ（ポートを開けているユーザ）

◆ P2Pファイル交換ソフト利用者

◆ ネットゲームソフト利用者
- OSのアップデートは止めている
- ウィルス対策ソフトもインストールしていない
- P2P/ゲーム専用端末のためマルウェアに感染しても気にしない

ISPがポートを閉じれば問題は解決する？

NTT PC COMMUNICATIONS

◆ マルウェアが感染攻撃等に利用する通信ポートを閉じれば、暫定的には感染活動を抑制し、マルウェアの脅威を一桁下げることが可能。

- SPAMメールやDDoS攻撃の温床となっているボットなどのマルウェア対策には有効
- Windowsアップデートを怠るユーザ、ウィルス対策ソフトを購入しないユーザや更新しないユーザの対策として有効
- ファイル共有等をインターネットで平文通信しているユーザはサービスが利用できなくなる。
- 全ISPが同じ対策を打つと、脅威の手法が変化し、より困難な状況に陥る可能性がある。

- ISPが自社ネットワークにおいて、マルウェアが感染活動に常態的に利用する通信ポートを閉じることが、受動的リスク対策として相当であり「正当業務行為」と認められることが望ましい。
- ISPがOP25B/IP25Bやマルウェア感染ポートを閉じることで、日本のインターネットのセキュリティ水準が上がると思われるが、その実施判断はISPの経営判断に委ねられるべきである。

② 特定のWebサイトを訪問すると被害を受ける

Googleの調査：ユーザーが閲覧しただけで知らないうちにマルウェアに感染させるサイト

- 数十億ページから**450**万**URL**を詳しく分析→**約45万ページが黒**
- **マルウェア配布サイトは検索結果に警告を表示**

ウィルス対策ソフトの検知率の変化

NTT PC COMMUNICATIONS

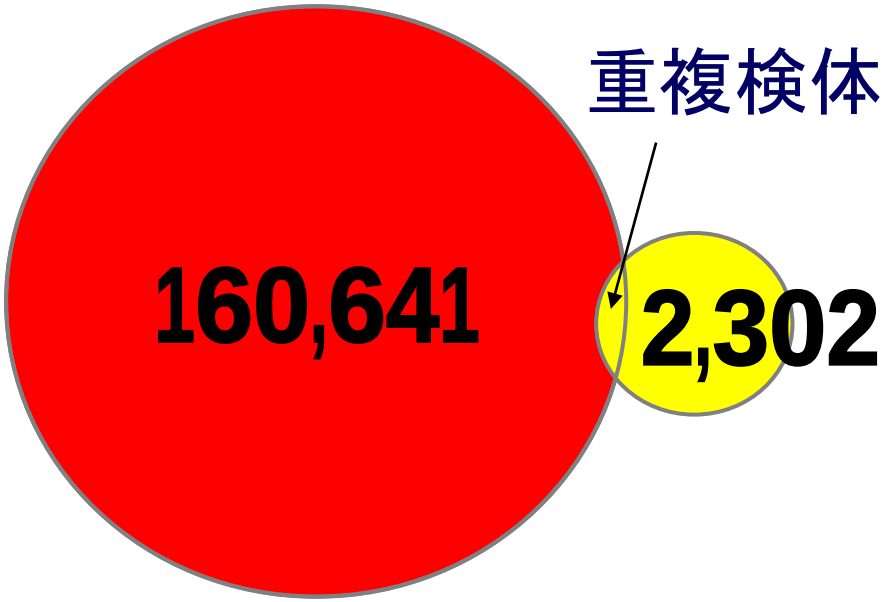
調査期間	未知/既知	収集検体		割合(%)	記 事
		収集数	種類		
2005年 4月1日～5月12日	既知	28,309	767	21	
	未知	3,537	2,938	79	
	合計	31,846	3,705		
2007年 9月1日～9月30日	既知	540,255	10,026	94	ジェネリック対応により検知率が飛躍的に向上
	未知	5,984	639	6	
	合計	546,239	10,665		
2007年 月日～月日 (LAC様調査結果)	既知	18,835	596	31	ジェネリック検知できないマルウェアがWeb経由でDLされている
	未知	8,920	1,325	69	
	合計	27,755	1,921		

BlackList指定されている約10万URLを巡回（約2週間）した結果、8.5%のURLで何らかのマルウェアに感染することを確認し1,921種類27,755検体を取得。1921種類の検体の中で69%が未知検体

Webダウンロード検体とCCC検体は一致？

NTT PC COMMUNICATIONS

● CCCで取得した検体とWebダウンロードで取得した検体を各々比較した（SHA1ユニーク）

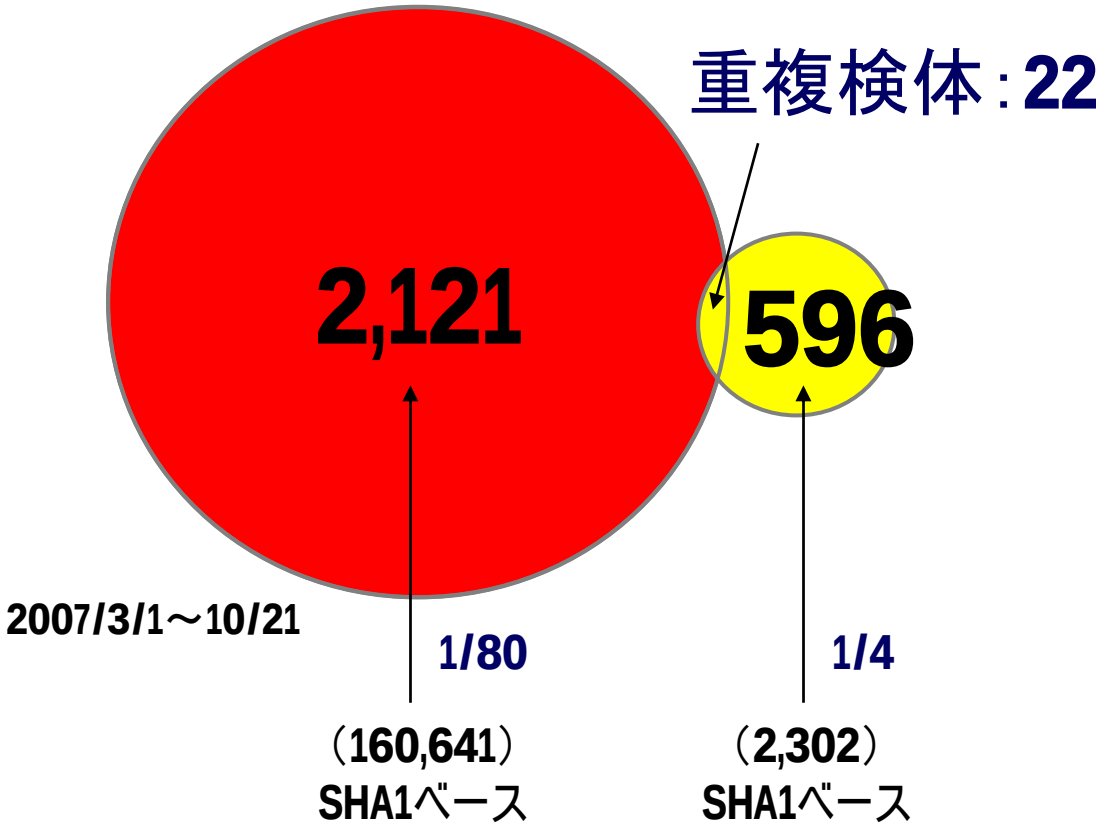


重複検体：11

2007/3/1～10/21

・0e2b5d8b0142b8256ee885df993b1112f8af5996
・12115ebfe69b28c27d6425ee41dc1009f4e73133
・23e6185b859637ba14f60d4ba30177b35c9e5431
・2aa613b7e3f67c37b5c4e558d7e93b1cbdc2bcd5
・56e838436fcea7840600f1ebc16406e7c0898f92
・62a2ec31877497b054c966db47e6c826eecdbedd
・a56b46c140ca21b565bccfc9ff6d01a07afedc47
・b47287290a253926661d7685f968e41a5c127bc8
・d7ca32e4bd1d337a2975fb91a5a25aefa250a046
・e5fcde2ced6190d224570679fc6d259a24682fae
・eeeed44d45236f900cfedb4926865d7e52566d69

● CCCで取得した検体とWebダウンロードで取得した検体を各々比較した（ウィルス名比較）



- BKDR_Generic
- BKDR_IRCBOT.GEN
- PE_Generic
- PE_PARITE.A
- Possible_MLWR-1
- Possible_MLWR-5
- Possible_SMLDL-1
- Possible_Strat-6
- TROJ_BHO.LU
- TROJ_DLOADER.CCT
- TROJ_DLOADER.IRQ
- TROJ_DLOADER.PSH
- TROJ_Generic
- TROJ_Generic.A
- TROJ_Generic.MRS
- TROJ_OBFUSCAT.RE
- TROJ_SMALL.HTM
- TROJ_SPAMBOT.B
- TROJ_TIBS.ARL
- WORM_Generic
- WORM_NUCRYPT.GEN
- WORM_ZHELATIN.IR

Web経由のマルウェアの実態と対策

NTT PC COMMUNICATIONS

◆ Web経由で感染するマルウェアは、CCCで対応中のネットワーク感染型のマルウェアとは異ったものが大半

◆ ウィルス対策ソフトも追いついていない（2-3年前のボットと同じ状況）

◆ 2-3年前と比較し攻撃側が有利な状況にさらに遷移している

- ネットワーク感染型のボットは待っていれば飛んできてくれたが、Web経由で感染するマルウェアは積極的に探さなければ見つからない
- 攻撃側は常にダウンロードできる状況にしておく必要はない
  - ➢ SPAMメール送信タイミングと組合わせた、低リスクで効率的な運用が可能

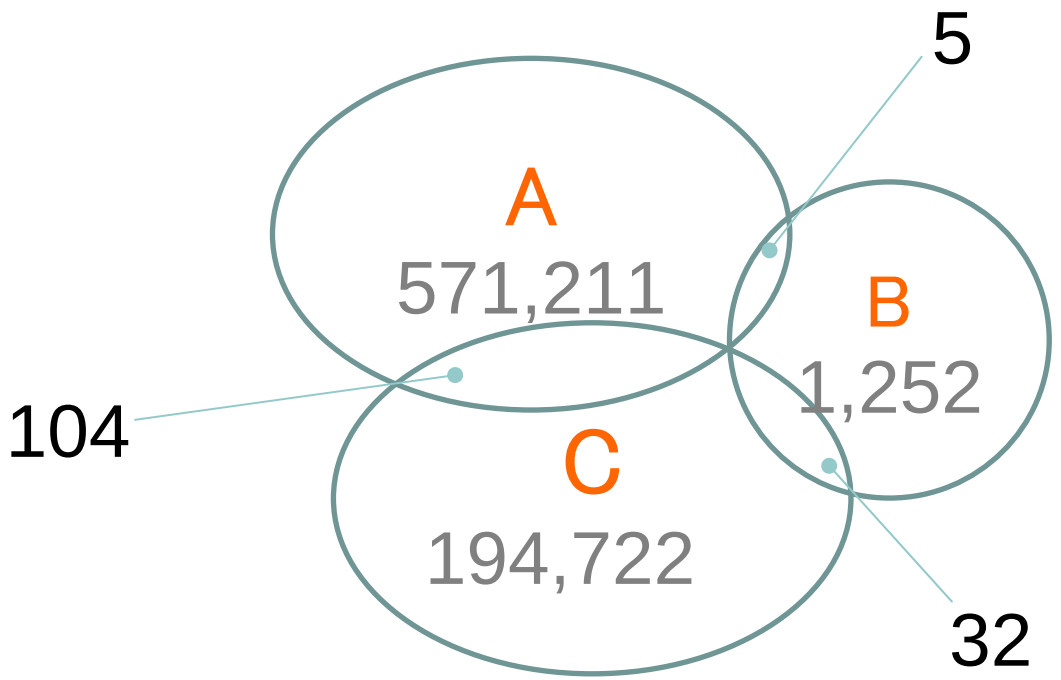
◆ 疑うことをしない「永遠のビギナー」が騙され連れて行かれるサイトの情報共有が必要。特に日本のユーザにとって有効なDB構築が必要。

研究者が見ている世界は必ずしも一致していない

BL乱立の一因？

A	URLBlacklist.com	http://urlblacklist.com/
B	Malware Block List	http://www.malware.com.br/
C	Google Safe Browsing API	http://code.google.com/apis/safebrowsing/

2007/09/13 10:00



④ SPAMメール・ウィルス感染
情報漏えい

SPAMメール誘導型マルウェア等の調査

NTT PC COMMUNICATIONS

- SPAMメール収集専用メールアドレスを準備
- コンピュータ内のメールアドレスを外部に漏洩させる機能を持つマルウェアを利用して、メールアドレスをSPAMメール送信者？に通知
- 目的
  - マルウェアによるメールアドレス収集
  - 悪性サイトへ誘導してマルウェアに感染させる脅威も調査

スパムメール収集期間	8/21～8/23（3日間）
スパムメール収集数	47,945通
抽出URL数	53,522
ユニークURL数	9,307（IPアドレス形式のURL: 6,691）
悪性判定URL数	466（5%）
処理時間[min]	4,893 8/24 12:08～8/27 21:41

NTT PC COMMUNICATIONS

http://IPアドレス 6,691の調査結果

件名：Honey I miss you. let me show you how much. I took some pictures for you, see?
From：xxx
To：xxx

click http://xxx.xxx.16.228

Sample

- 同期間にサイバークリーンセンターの検体収集用ハニーポットで観測していた攻撃元IPアドレス7075とつき合わせた結果

  重複したIPアドレスは1件のみ

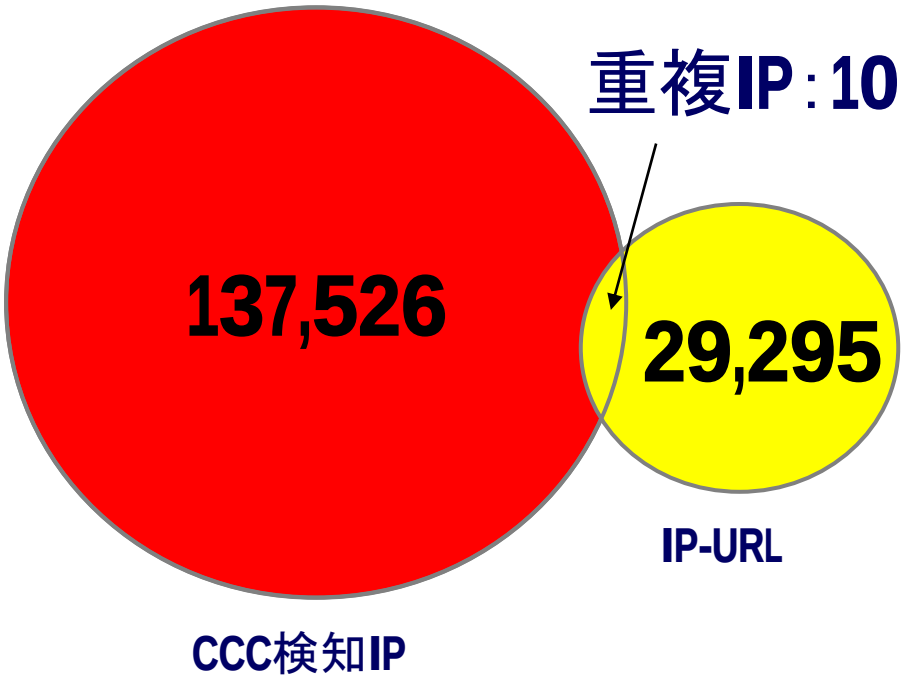
- 6,691件のIPアドレスの中で国内は26件

  26件にアクセスしたところ、1件からマルウェアがダウンロードし感染

調査期間を2ヶ月に拡大してみても

NTT PC COMMUNICATIONS

- 2007年7～8月にCCCで検知した攻撃元IPと、同期間にSPAMメールから検知した誘導先IPを調査



つまりは、乗っ取られたホストに傾向があるか調査してみたが、

まとめ．．

ISPネットワークでの
フィルタリングは必要か？

永遠のビギナの脅威を低減する受動的リスク対策

NTT PC COMMUNICATIONS

◆ポイントはWebダウンロード型マルウェアへの取り組み
- インターネットのリスクの全容を把握することは困難

◆厄介な存在「永遠のビギナー」とどう付き合うか
- インターネットの存在を意識せず、PCをTVのように操作するユーザが、かなりの割合で存在する
  - ウィルス対策ソフトをインストールしても契約更新しない
  - 契約更新していても、PCを時々使うときにパターンファイルを最新にせずに利用するユーザ
  - ウィルス対策ソフトを意図的に止めるユーザ

◆ SPAMやマルウェアを撒き散らす悪性サイト等の情報共有が必要
- セキュリティベンダにとっては大事な商売道具 →非公開
- 研究者は範囲限定でサンプリング調査 →公開
  - BLを突合しても心配になるだけ…

◆ BLを積極的に共有しDB登録リストの信頼性を高める工夫が必要。
- 腕を競うのはリストを作ることではなく、リストを活用するノウハウで競うべき

健全な競争のため高邁な連携が必要

Thank you!