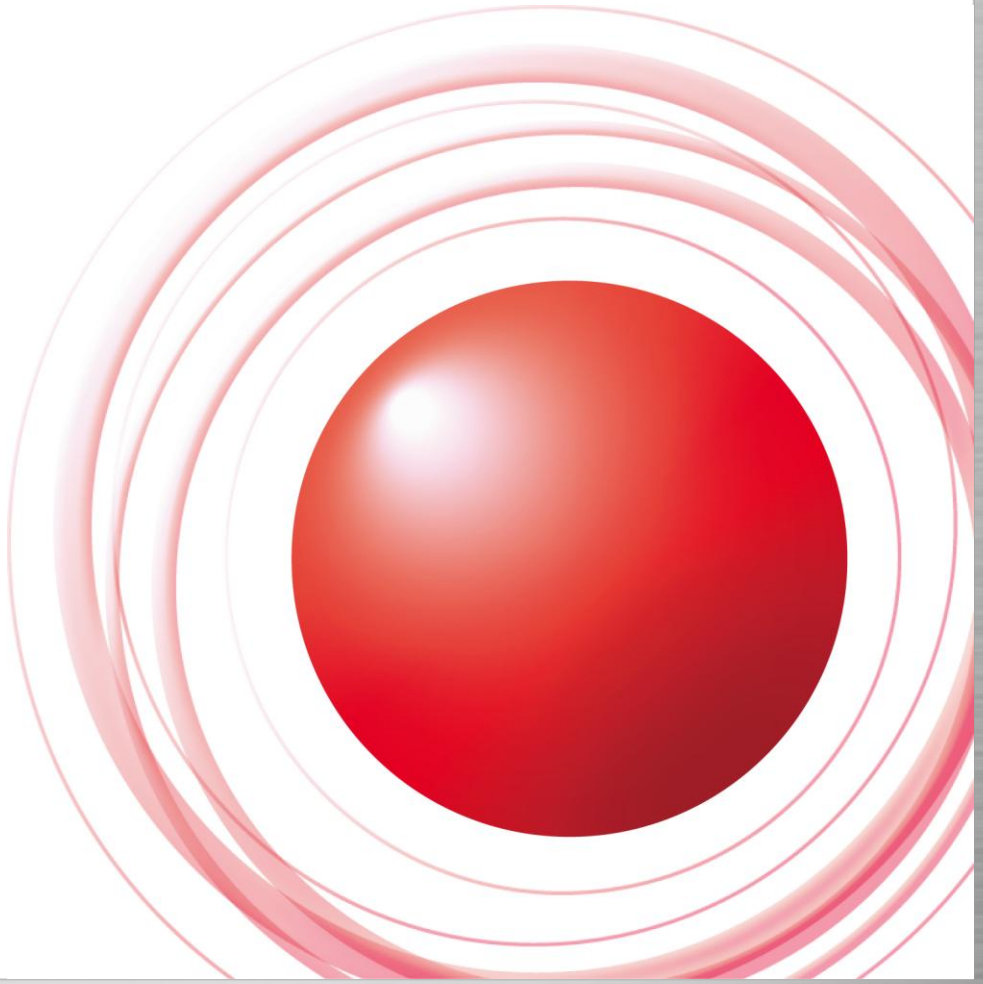
マルウェア対策研究人材育成ワークショップ 2009 (MWS 2009)

観測網の大小に基づく結果の比較とマルウェア対策に関する一考察

IIJ Internet Initiative Japan



2009/10/26

株式会社インターネットイニシアティブ
永尾禎啓　鈴木博志　加藤雅彦　齋藤衛

Ongoing Innovation

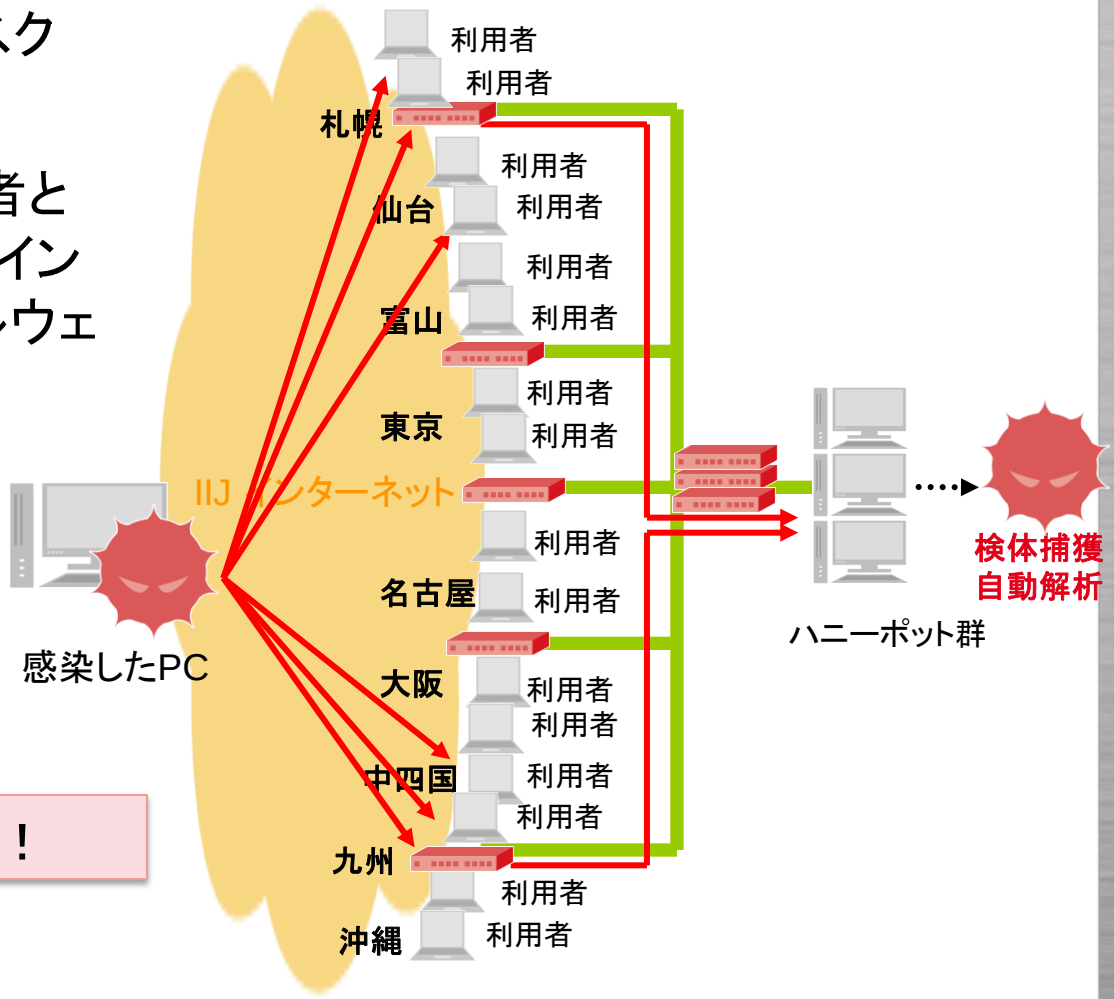
- MITF: IIJ のマルウェア観測
- 観測結果の比較 (MWS2009版)
- 攻撃予測と対策の検討
- まとめ

- MITF: IIJ のマルウェア観測
- 観測結果の比較 (MWS2009版)
- 攻撃予測と対策の検討
- まとめ

IIJ MITF (Malware Investigation Task Force)

- 2007年4月より実施している、IIJのマルウェア捕獲、対策のタスクフォース

- IIJの網の内部に、一般利用者と同様にハニーポットを接続し、インターネット側からの攻撃やマルウェアを観測し、解析を行う



IIJ の網をきれいにしたい！

素朴な疑問

2つの観測網

- CCC は国内インターネットを広範に観測

  参加 ISP 76社 （CCC ウェブページ https://www.ccc.go.jp/ccc/ より）

- MITF は IIJ ネットワーク内のみを密に観測

  平均して /23 ごとに 1 個の観測点

観測結果に違いはあるの?

昨年MWS2008での発表:

「近年のマルウェアの活動は局所化している」

いくつかの視点で確かめてみよう！

今年も同じ調査をしてみました

- MITF: IIJ のマルウェア観測
- 観測結果の比較 (MWS2009版)
- 攻撃予測と対策の検討
- まとめ

観測結果を見比べてみよう

比較データ項目

CCC DATAset 2009 攻撃元データ(CCC2009 と略す)と MITF データから項目を抽出して比較

CCC2009 から
時刻
マルウェア取得元 IP アドレス
マルウェアハッシュ値

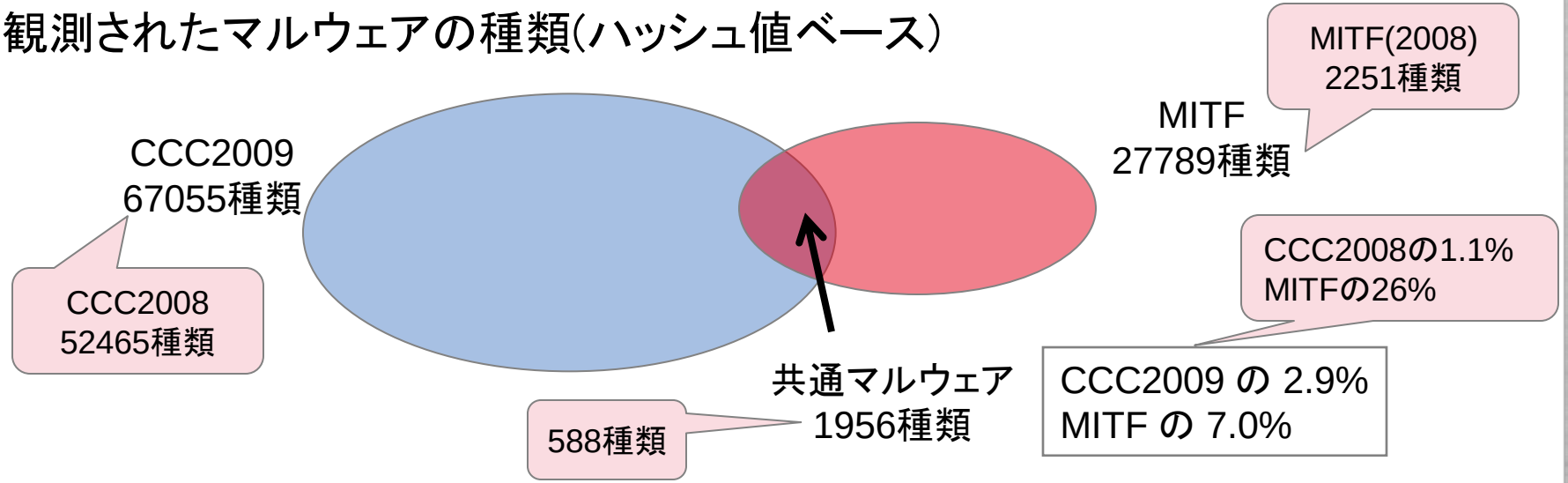
MITF から
時刻
マルウェア取得元 IP アドレス
マルウェアハッシュ値

対象データの期間

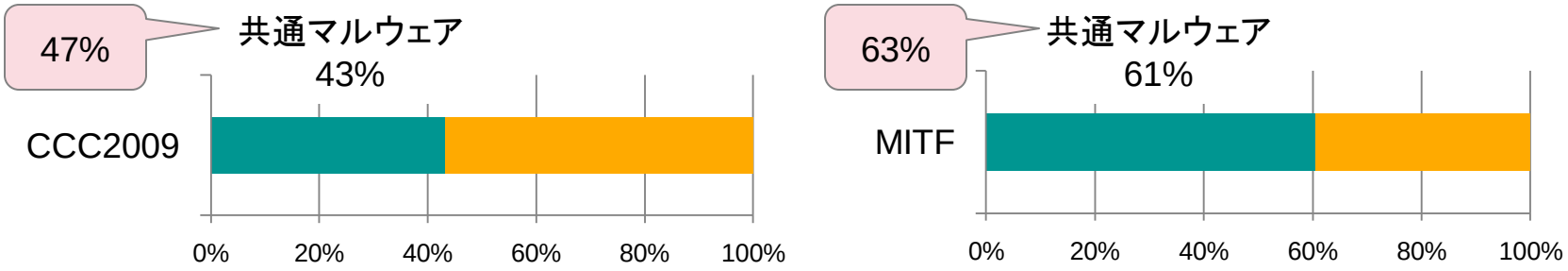
2008/05/01～2009/04/30　の1年間

観測結果の共通点は? — 共通するマルウェア

観測されたマルウェアの種類(ハッシュ値ベース)



マルウェア取得総件数に占める共通マルウェアの割合

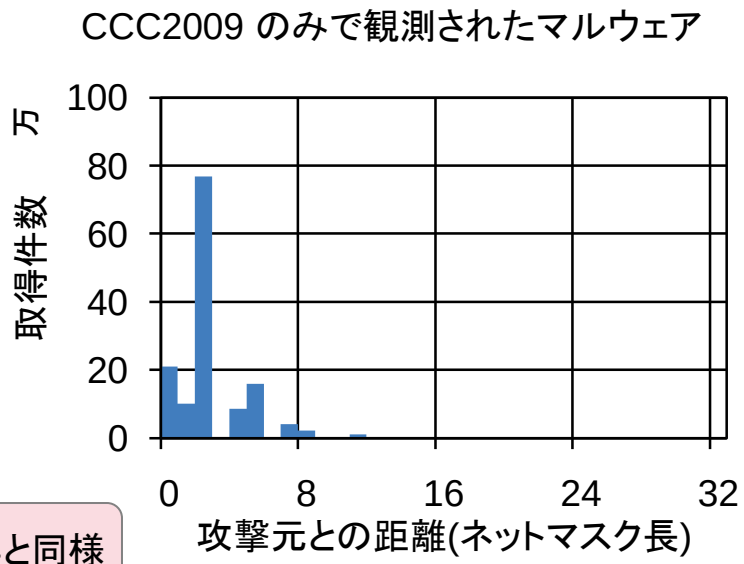


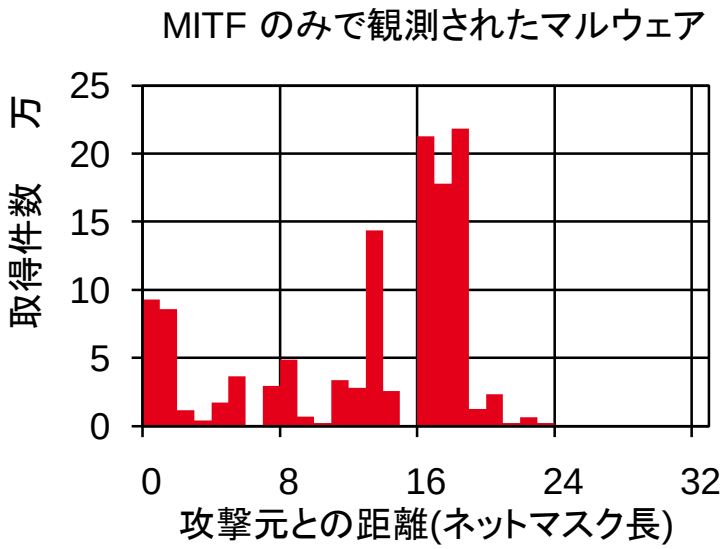
共通マルウェアは IIJ 内外で広く流行しているマルウェア…?

一方でのみ観測されたマルウェア

攻撃元とMITF 観測網の距離を見てみた

攻撃元アドレスと MITF の観測点アドレスとの上位共通ビット長を、距離の指標とした



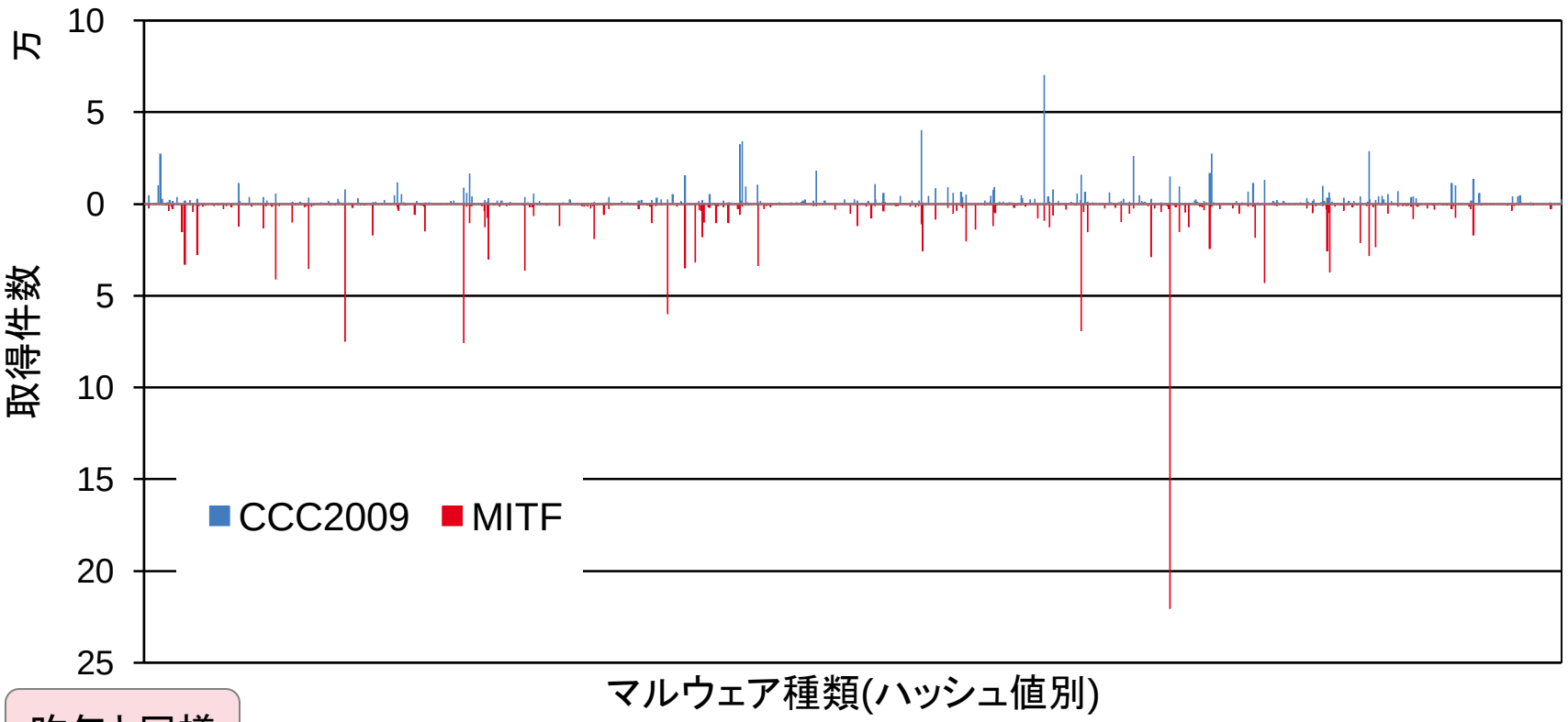


昨年と同様

近いところからの攻撃はよく観測される

遠い所からの攻撃はあまり観測されない

共通マルウェアの取得件数



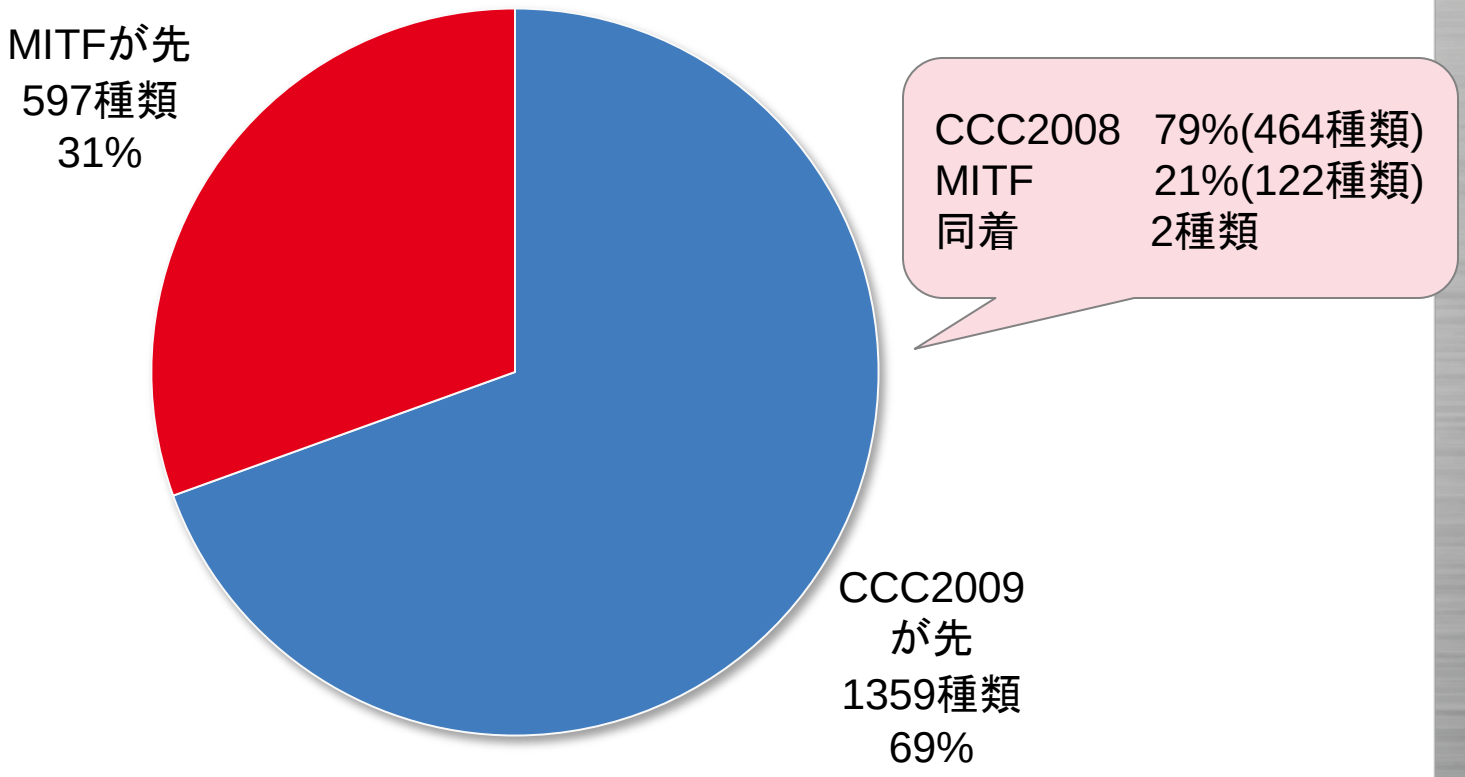
昨年と同様

CCC で活発に観測されても、MITF では必ずしも活発でない

共通マルウェア: どちらで先に観測されていたか

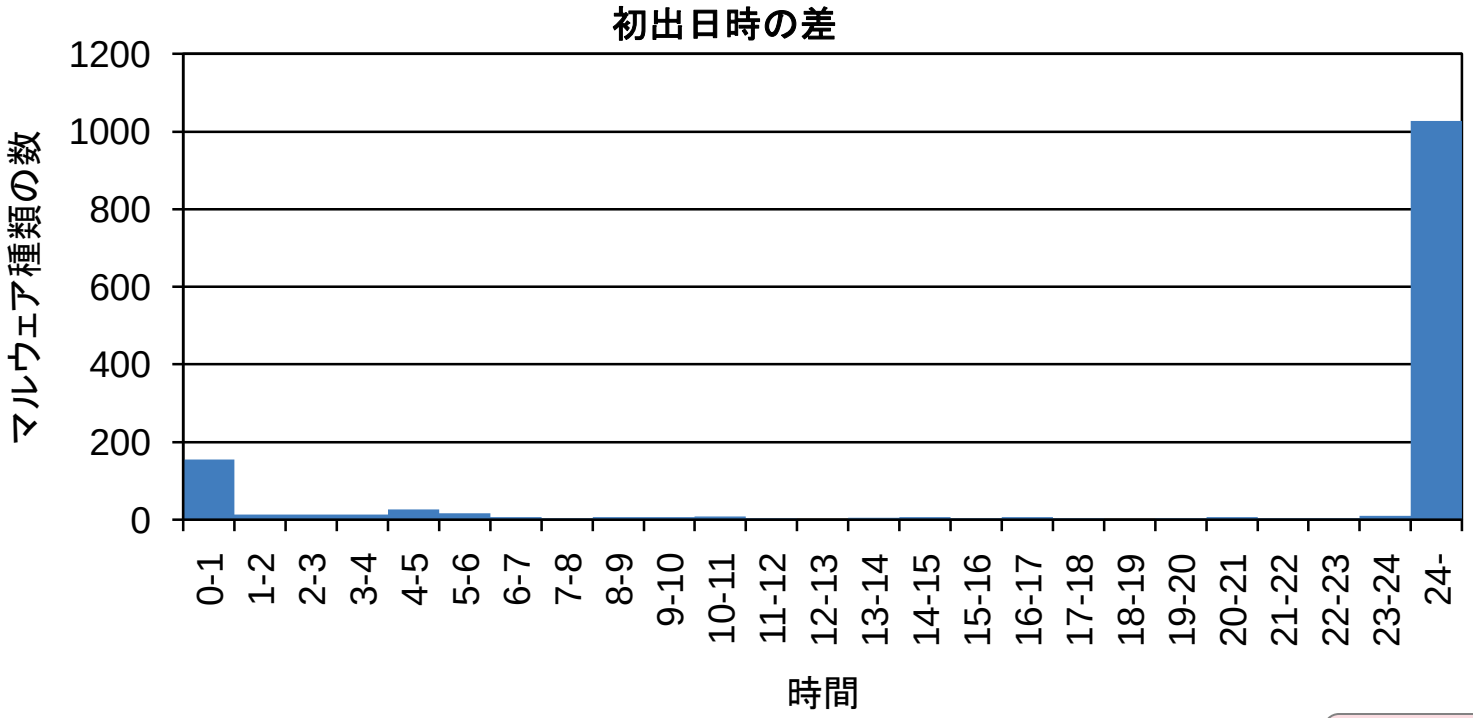
マルウェアの種類(ハッシュ値ベース)ごとに初出日時を比較

全体: 共通マルウェア　1956種類



共通マルウェア: どちらで先に観測されていたか

CCC2009 で先に観測されたマルウェア



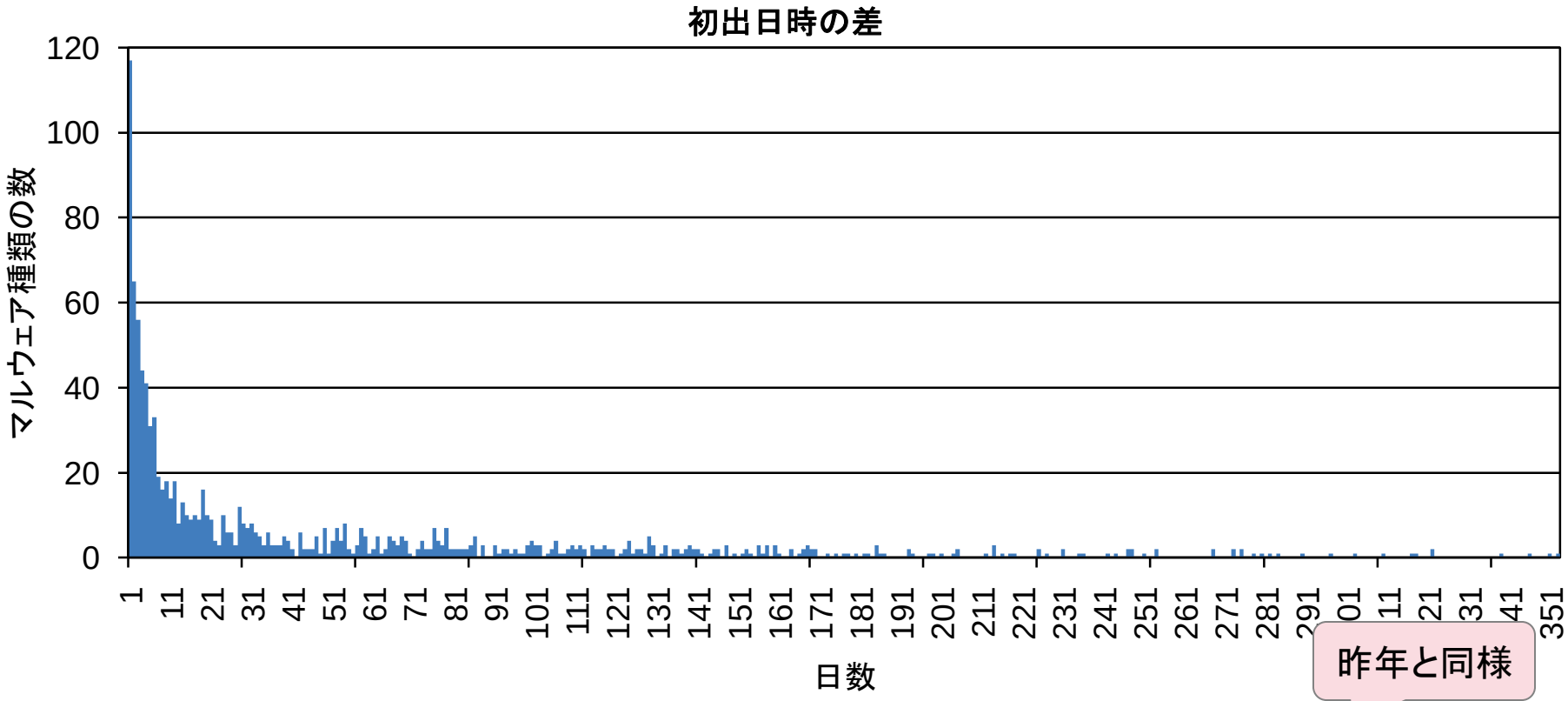
共通マルウェア 1956種類のうち

53%は CCC2009 で 24時間以上先行して観測

昨年と同様

共通マルウェア: どちらで先に観測されていたか

CCC2009 で先に観測されたマルウェア

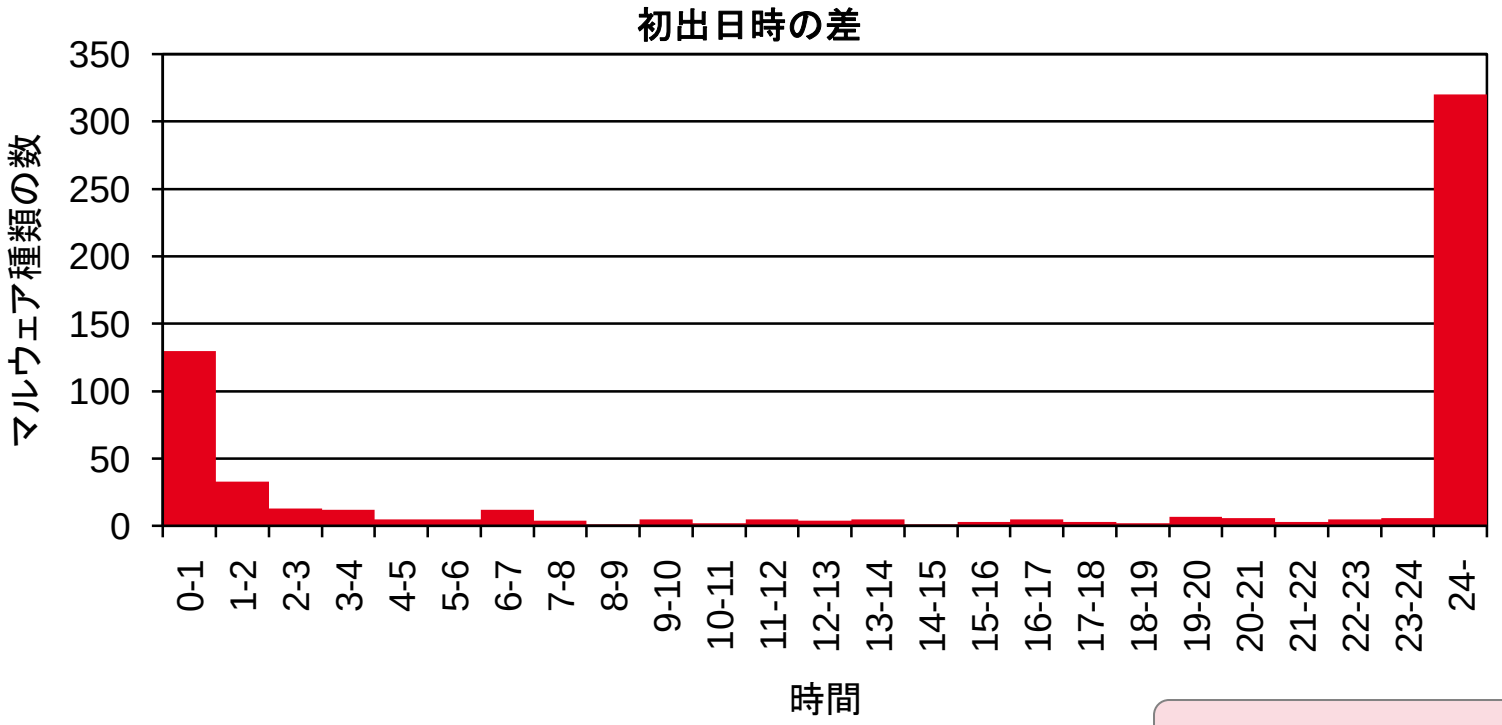


昨年と同様

数週間～1年近く遅れてようやく MITF に観測されるものも

共通マルウェア: どちらで先に観測されていたか

MITF で先に観測されたマルウェア



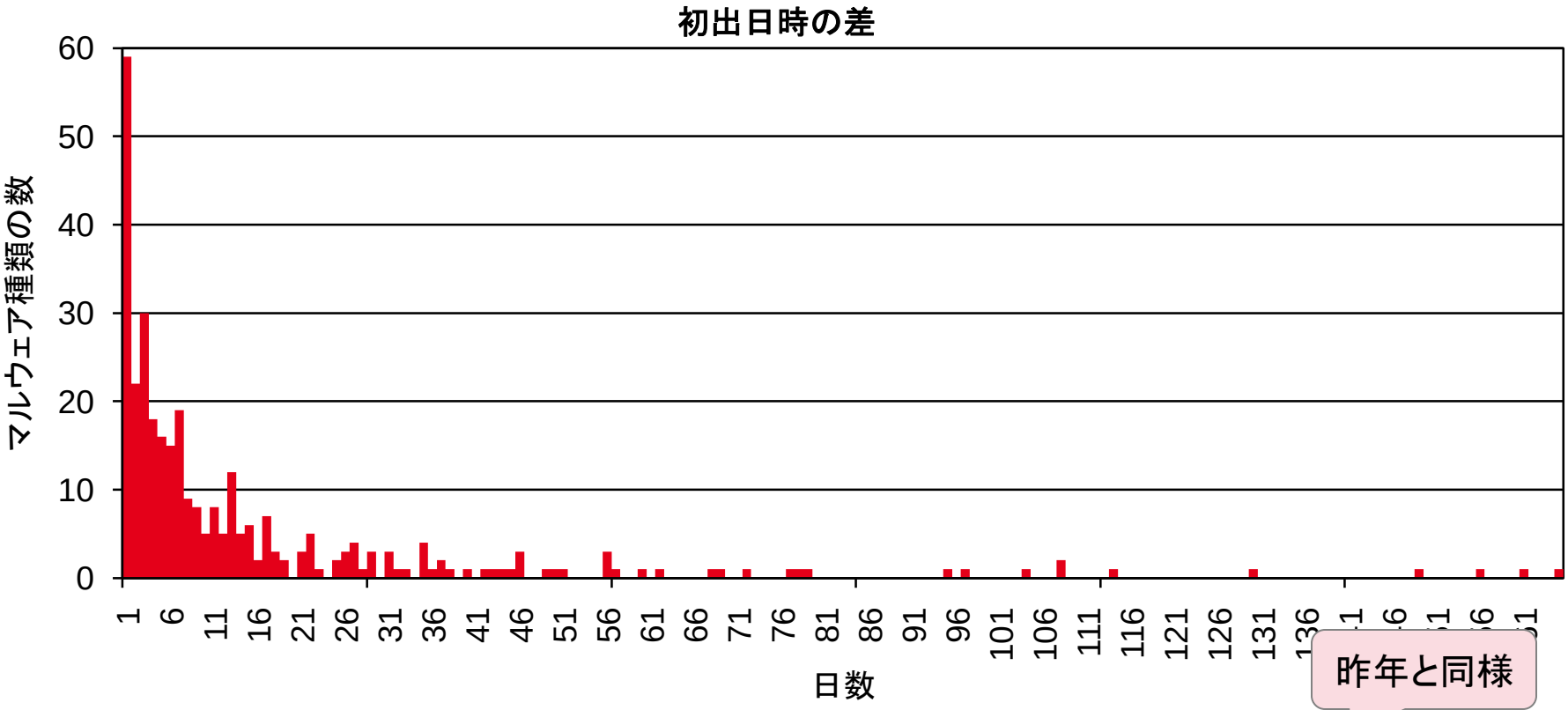
共通マルウェア 1956種類のうち

昨年の8%より少し増加

16%は MITF で 24時間以上先行して観測

共通マルウェア: どちらで先に観測されていたか

MITF で先に観測されたマルウェア



数日～5か月以上遅れて CCC2009 で観測されるものも

- MITF: IIJ のマルウェア観測
- 観測結果の比較 (MWS2009版)
- 攻撃予測と対策の検討
- まとめ

攻撃予測と対策の検討

CCC2009とMITFのデータを照合することで、今後の攻撃予測・先回り防御に役立てられないか

攻撃予測できたなら

- MITFで先に見つけたら予測に基づき(CCC経由で)近隣アドレスで防御
- CCCで先に見つけたら予測に基づきMITF側で防御開始

近隣ISPを踏み台にしてIIJの顧客を守る☺

KDDI　－　IIJの、とあるCIDR　－　マカオのISP

攻撃予測と対策の検討

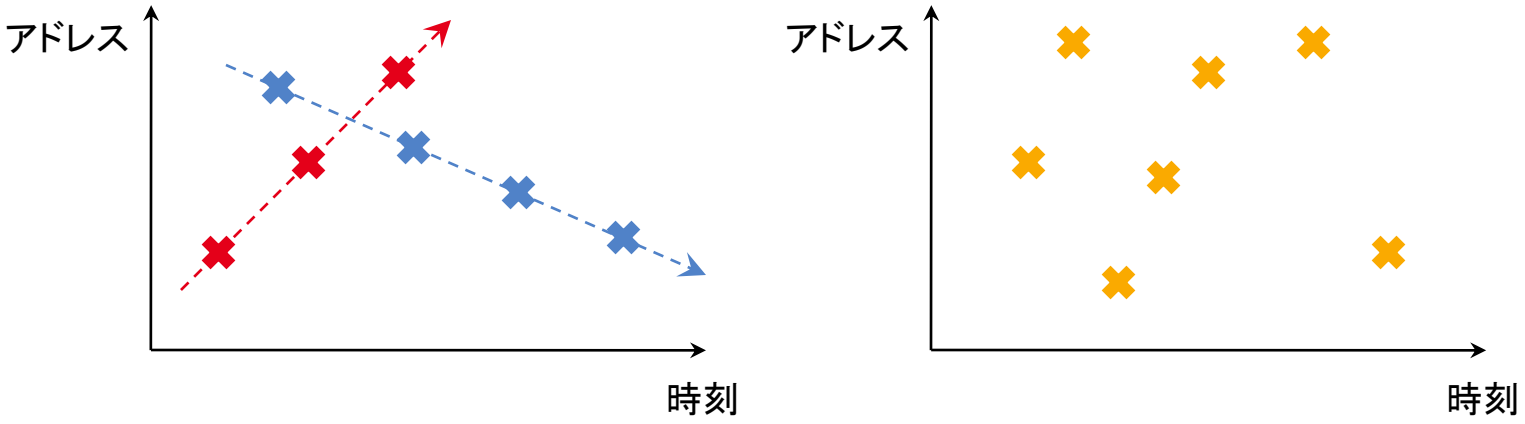
ISPによる一次防御

- •ISP ルータでフィルタリングで感染拡大を防止
  - （注：実現には技術的課題だけでなく、法的課題もある）
- •あくまでも一時回避策
  - •すでに感染しているホストは救えない
  - •CCCの注意喚起活動やウィルス対策ソフトなど、より本質的な対応がとられるまでの一次対応

攻撃予測と対策の検討

予測にむけた攻撃パターン分類

- IPアドレスを昇順・降順に攻撃していくパターン
  - → スキャン速度から到達予測
- IPアドレスをランダムに攻撃していくパターン
  - → 何かできないものだろうか?



攻撃のパターン

ハニーポットのIPアドレスがわかっているMITFデータを対象に調査

期間内に同一アドレスから 3回以上観測されたマルウェア 1543種類の、一連のスキャン　30032個

- IPアドレスを昇順に攻撃していくパターン
  - 190個、例えばおよそ125アドレス/秒
- IPアドレスを降順に攻撃していくパターン
  - 143個、大半が数アドレス/秒
- IPアドレスをランダムに攻撃していくパターン(残り)
  - 29699個

攻撃のパターン

パターン集計から除外されたマルウェア

- 期間内に同一アドレスから 2回以下しか観測されなかった
- 26246種類も！
- すべてが本当に単発(or 2発)攻撃なのか…?
- MITF のハニーポットは /23 単位
  - 攻撃スキャン範囲が /24 以下だとパターンまでは捉えられない
  - ハニーポットを増やすにも予算などの都合もある

MITF観測網でも密度が足りていない可能性

十分な密度とは?

→ 今後の研究課題

昇順・降順パターンからの攻撃予測の検証

MITF昇順・降順パターンからの攻撃予測

- CCC2009にも同一スキャンの前後部分が観測されていないか調査

目的

- 近隣アドレス到達までの時間的猶予から対策の実効性を推定したい

結果

CCC2009から該当する観測ログは見つからず・・・

- CCC2009のデータからは検証できず
- MITFアドレスの近隣にハニーポットがいなかったのか
- ただ、MITFアドレス内のハニーポットは数個発見☺

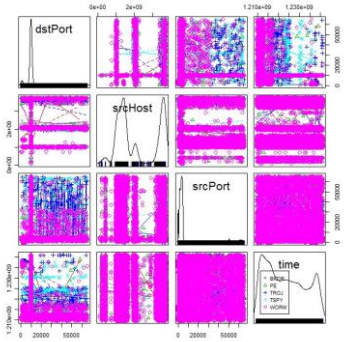
ランダムパターンに対する攻撃予測可能性の検討

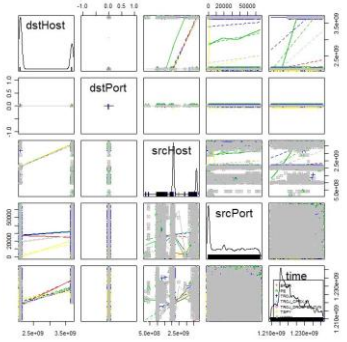
統計処理によるマルウェア種別(Bot, Worm, Backdoor, …)ごとの傾向分析

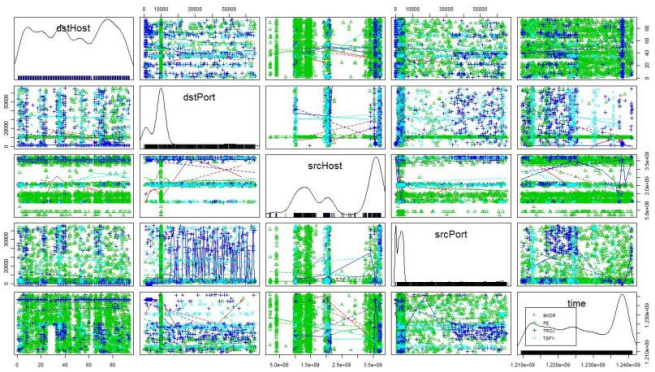
- CCC2009, MITF それぞれを対象に

目的

- 予測のための傾向把握
- どの程度の密度でハニーポットがあれば早期発見できて対策できるか







結果

特徴見いだせず・・・ (時間切れ)

ランダムパターンへの対策の検討

- 予測をせず、一斉にフィルタして拡大を防ぐことを考えてみる

- IPアドレスをランダムに攻撃していくパターン： 29699個
  - うち、15分以上かけている攻撃： 18209個 (61%)
  - この15分間でフィルタを実施して、その後の攻撃を止められたら?
    - → 一連のランダム攻撃のうち 45% (平均)の攻撃を止められる

- MITF: IIJ のマルウェア観測
- 観測結果の比較 (MWS2009版)
- 攻撃予測と対策の検討
- まとめ

まとめ

1. 観測結果の比較
    - •CCC DATAset2009 攻撃元データと MITF の攻撃元データを比較
    - •MWS2008発表と同様の結果が得られた
        - •マルウェアの感染活動は局所的
        - •観測網によって観測結果に違いがある
    - •今年もこの傾向に変化なし
2. 攻撃予測と対策の検討
    - •CCC,MITFの観測から相互に攻撃予測・即時対策ができないか検討
    - •昇順・降順の攻撃パターン
        - •125アドレス/秒　→ 150C離れていれば 5分の対策時間
    - •ランダムな攻撃パターン
        - •予測方法は考えられなかったが、一斉フィルタで 45%ブロック

(本当の?) まとめ

- IIJ も MITF によるハニーポットのデータを持っています。
- ですが、それを使った研究に注げる能力、労力はご覧のとおりです。
  - ISP現場における、その他の日常業務に忙殺されています。
    （言い訳 兼 悲鳴）

つきましては…

協力者募集！☺

実務現場で IIJ のネットワークをきれいにしてやろうという方、大歓迎

ご連絡お待ちしております☺

IIJ Internet Initiative Japan

ご清聴ありがとうございました

お問い合わせ先 IIJ セキュリティ情報統括部 永尾、鈴木、加藤、齋藤
TEL：03-5259-6450
nagao@iij.ad.jp, hiroshi-suzuki@iij.ad.jp, masa@iij.ad.jp, msaito@iij.ad.jp
http://www.iij.ad.jp/

Ongoing Innovation