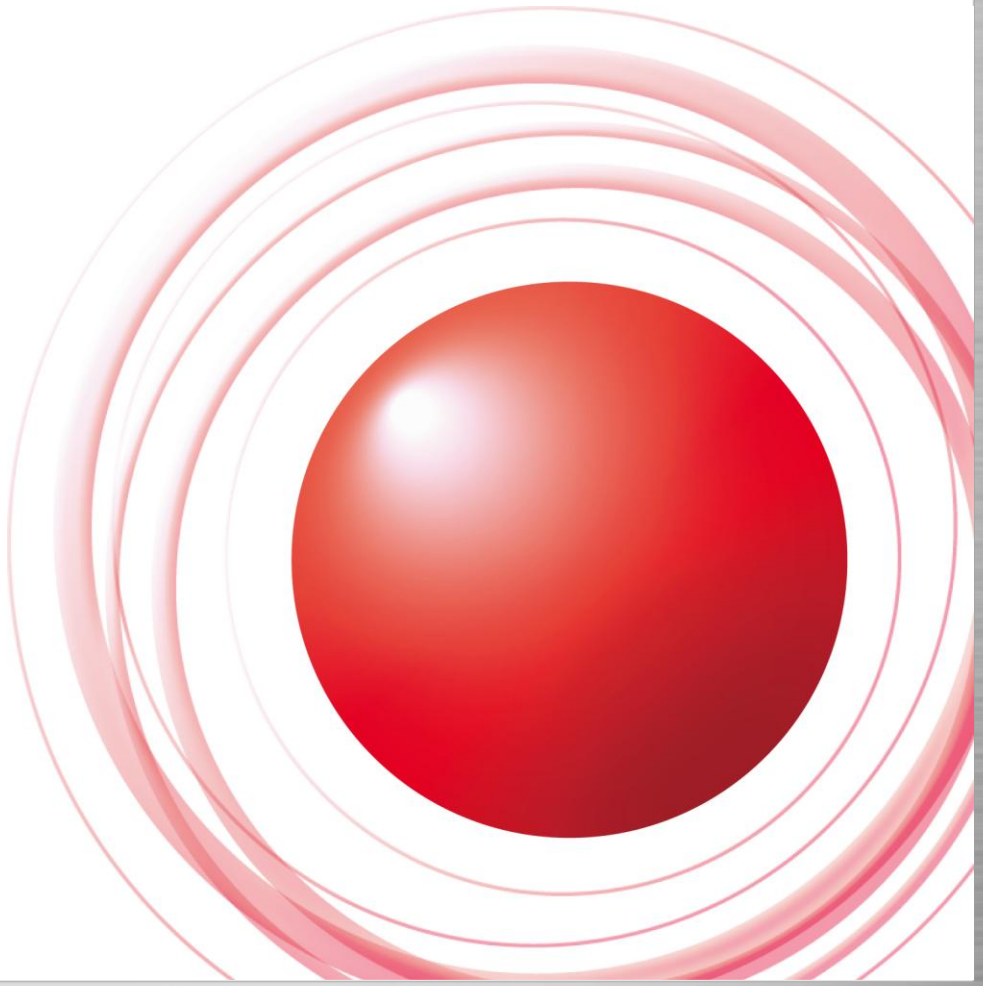
マルウェア対策研究人材育成ワークショップ 2010 (MWS 2010)

大小2つの観測網による結果の時間変化とマルウェア対策に関する一考察

IIJ Internet Initiative Japan



2010/10/19

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

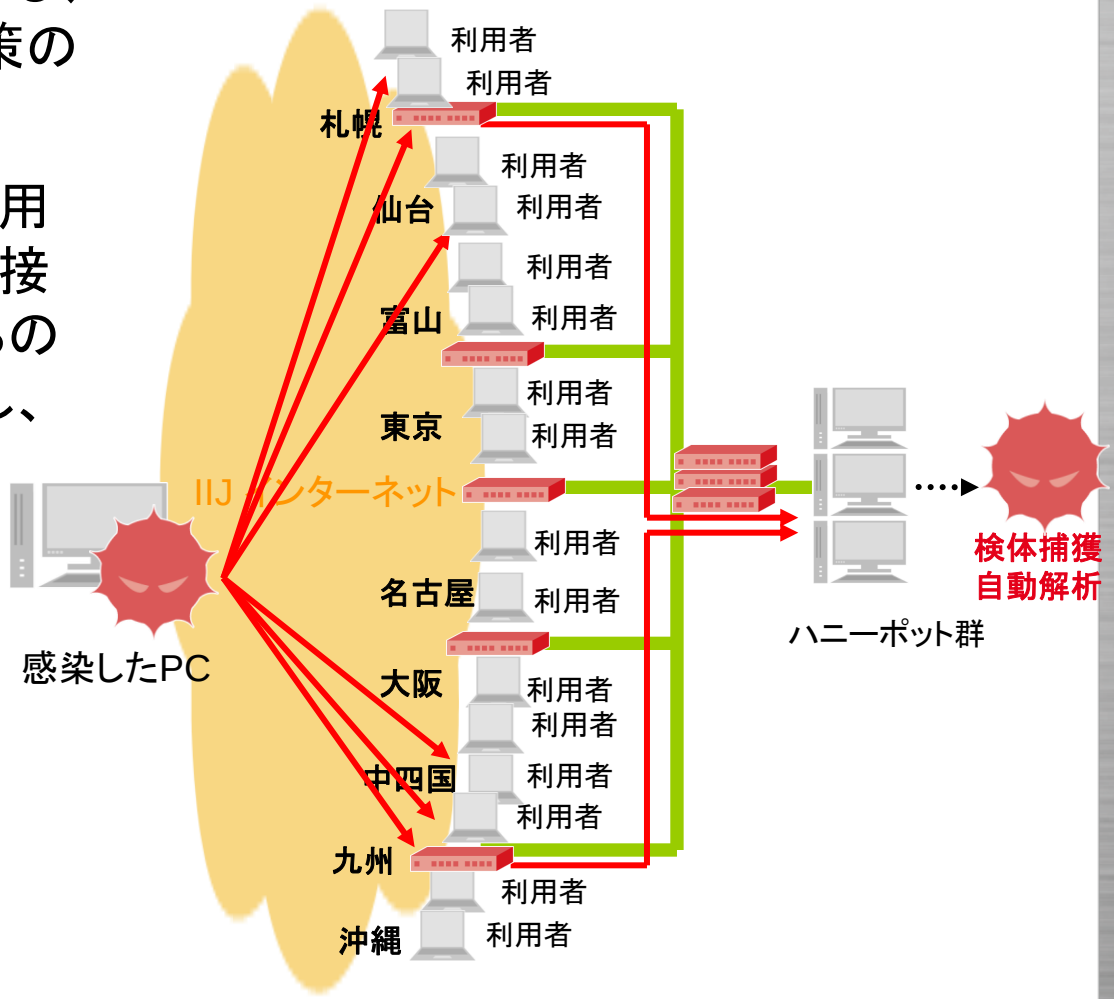
Ongoing Innovation

- MITF: IIJ のマルウェア観測
- 観測結果の比較 (MWS2010版)
- 攻撃への対策の検討
- まとめ

- MITF: IIJ のマルウェア観測
- 観測結果の比較 (MWS2010版)
- 攻撃への対策の検討
- 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



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 77社 (CCCウェブページ https://www.ccc.go.jp/ccc/ より)
- MITFはIIJネットワーク内だけを密に観測
  - 平均して /23 ごとに 1個の観測点

観測結果に違いはあるか?

MWS2008 & MWS2009 での発表:
「近年のマルウェアの活動は局所化している」
を、いくつかの視点で確かめた

定点観測として今年も同じ調査を実施

- MITF: IIJ のマルウェア観測
- 観測結果の比較 (MWS2010版)
- 攻撃への対策の検討
- まとめ

観測結果を見比べる

比較データ項目

CCC DATAset 2010攻撃元データ(CCC2010と略す)と MITF データから項目を抽出して比較

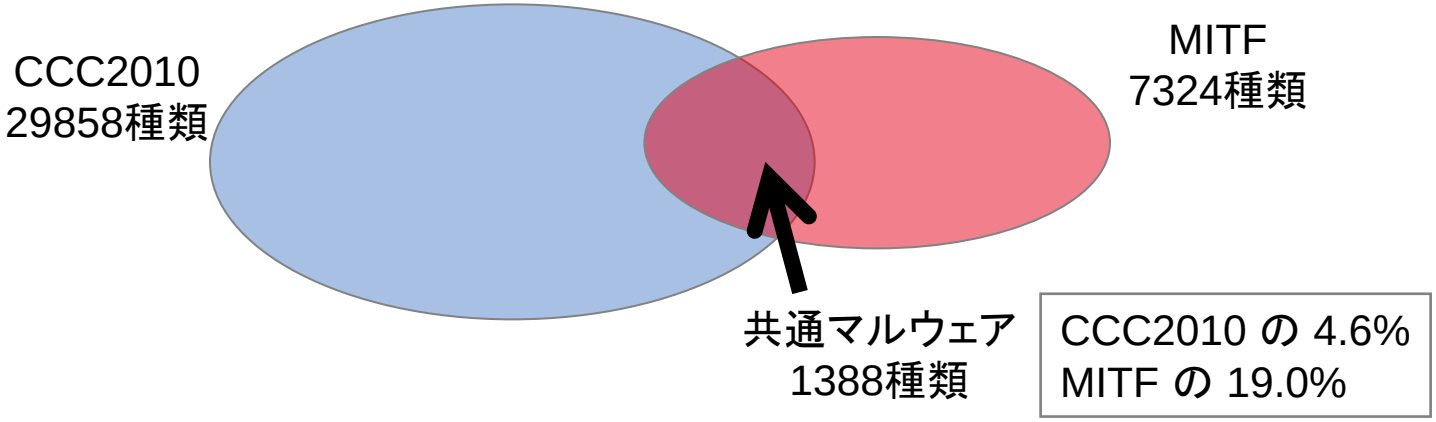
CCC2010 から	MITF から
時刻	時刻
マルウェア取得元 IP アドレス	マルウェア取得元 IP アドレス
マルウェアハッシュ値	マルウェアハッシュ値

対象データの期間

2009/05/01 - 2010/04/30の1年間

観測結果の共通点は? — 共通するマルウェア

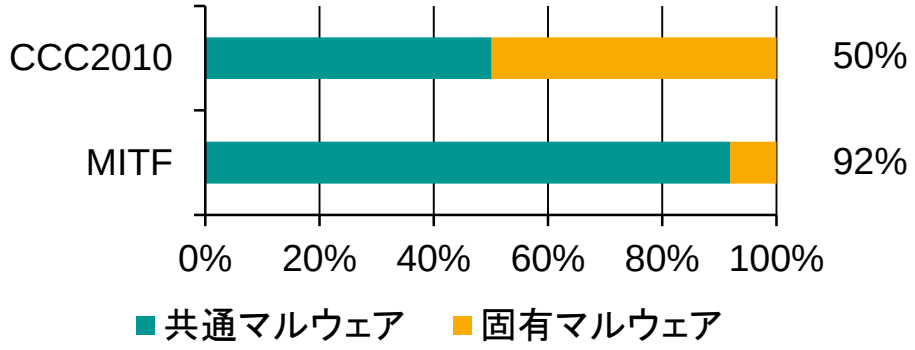
観測されたマルウェアの種類(ハッシュ値ベース)



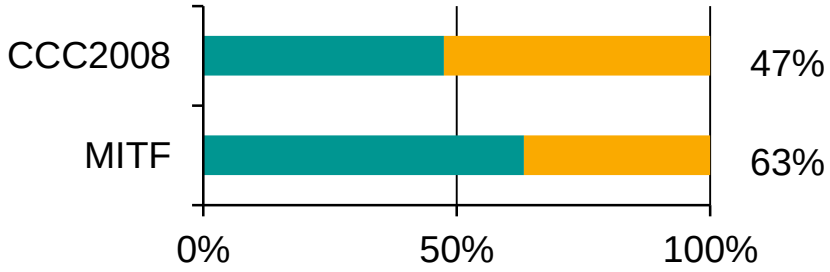
	2008 (6ヶ月)	2009 (1年間)	2010 (1年間)
CCC DATAset	52,465	67,055	29,858
MITF	2,251	27,789	7,324
共通マルウェア	588	1,956	1,388

観測結果の共通点は? — 共通するマルウェア

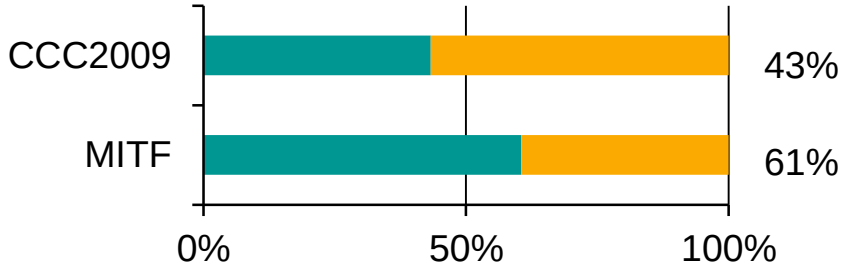
マルウェア取得総件数に占める共通マルウェアの割合



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



2008



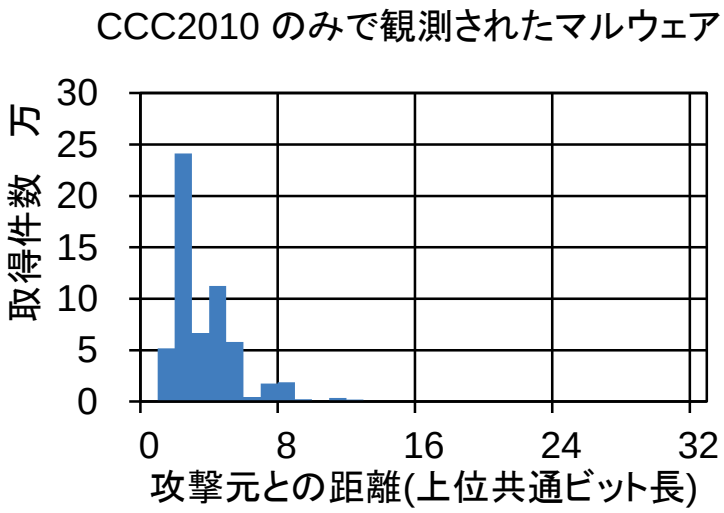
2009

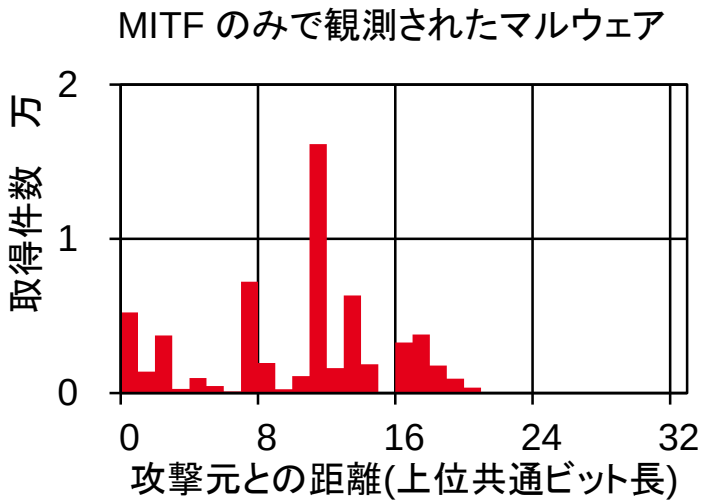
一方のみで観測されたマルウェア

攻撃元とMITF 観測網の距離を調べた

距離の指標:

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



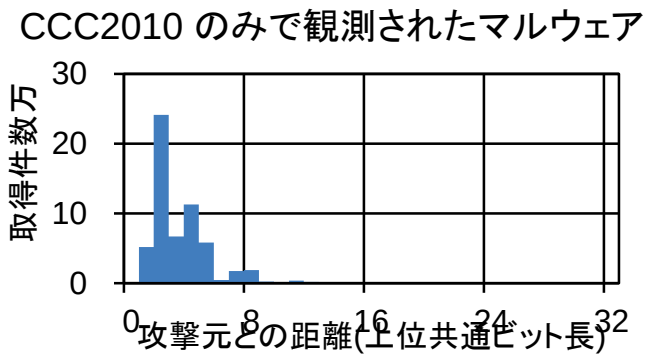


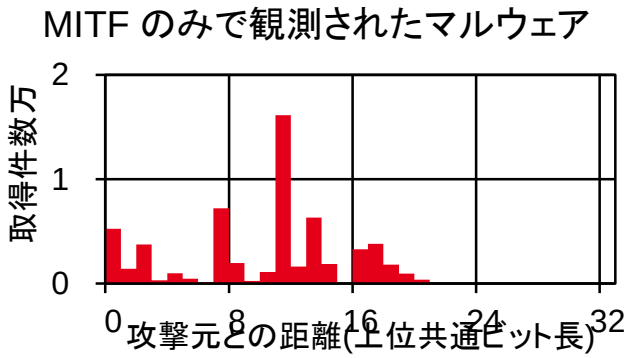
近いところからの攻撃はよく観測される

遠い所からの攻撃はあまり観測されない

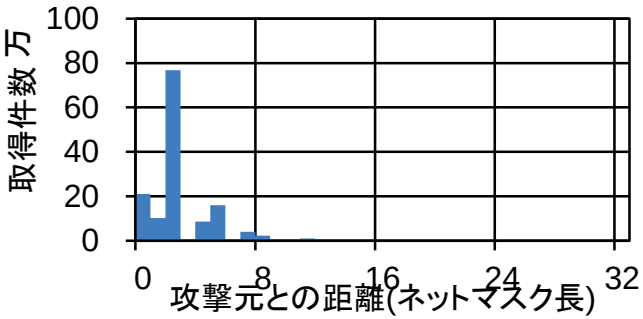
一方のみで観測されたマルウェア

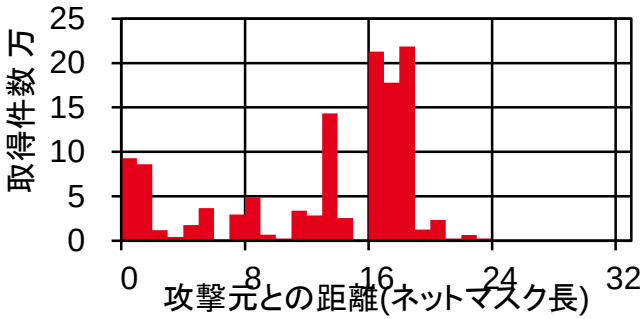
2010



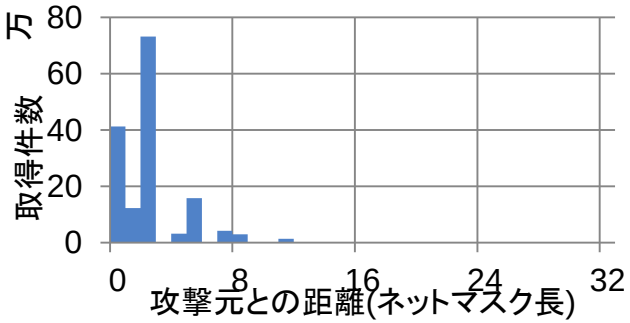


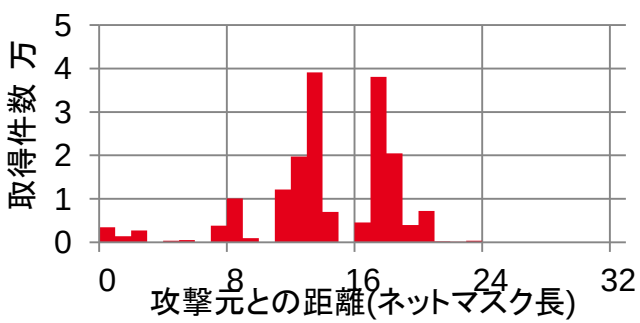
2009



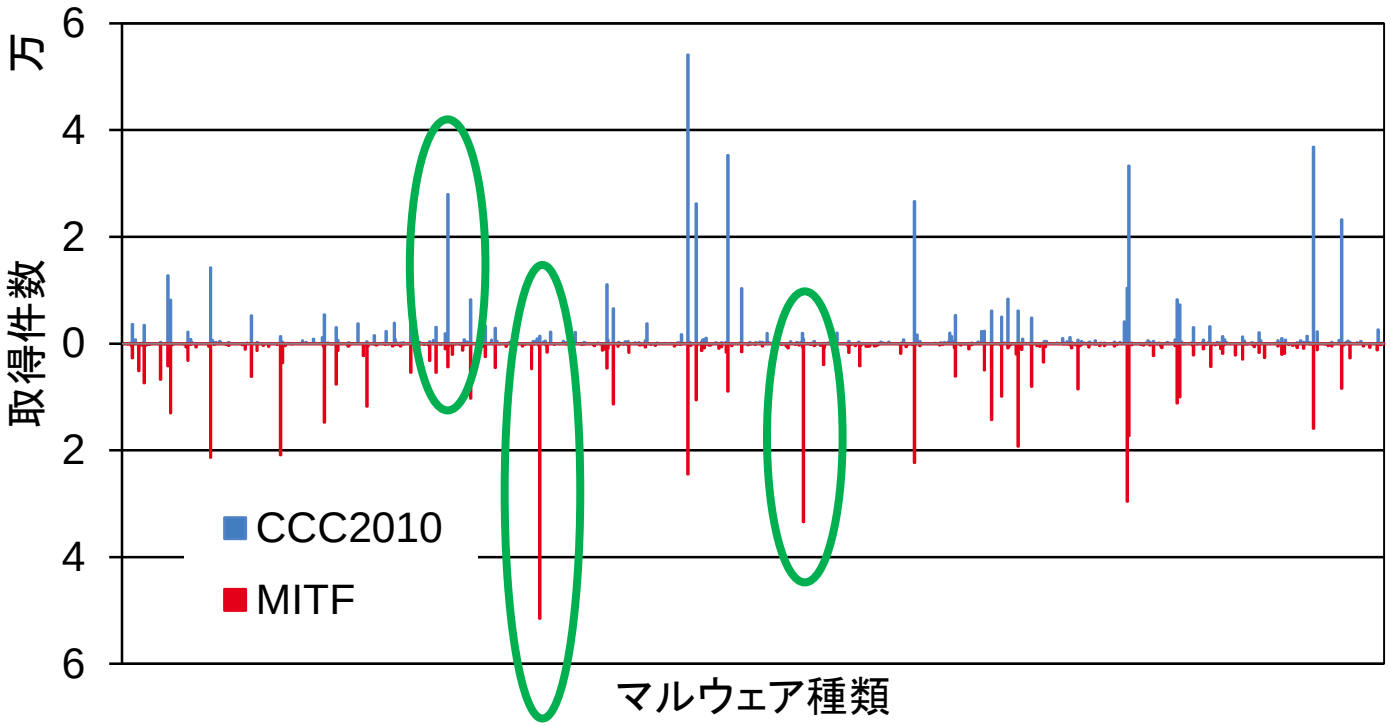


2008





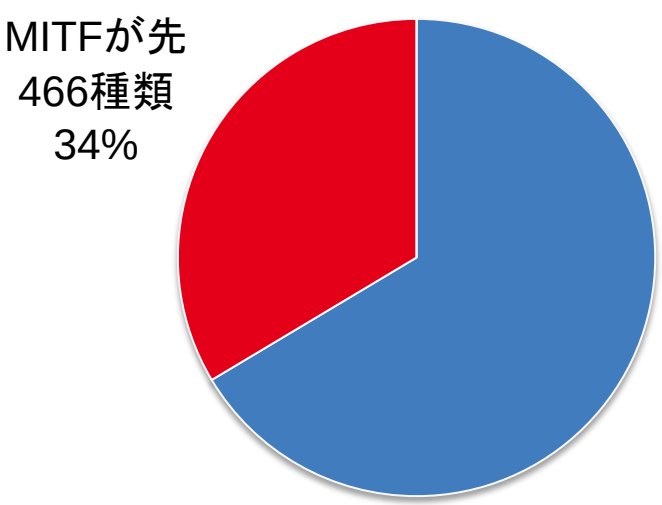
共通マルウェアの取得件数

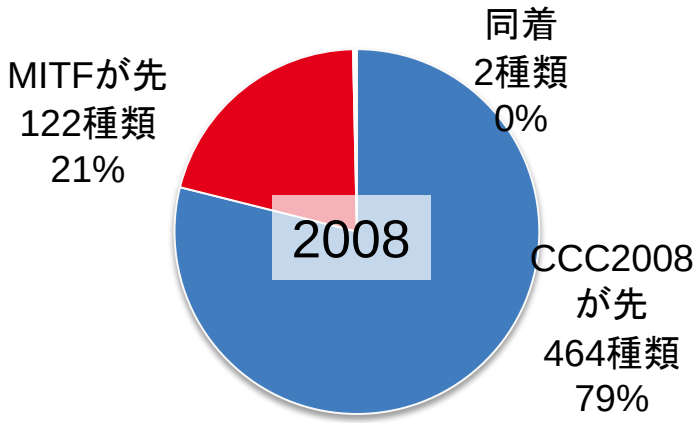


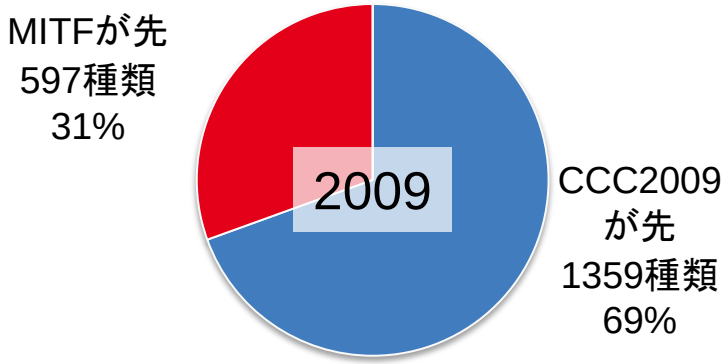
CCC, MITFに共通して活発に観測されているマルウェアもあるが、
一方だけで活発なものもある

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)ごとに初出日時を比較

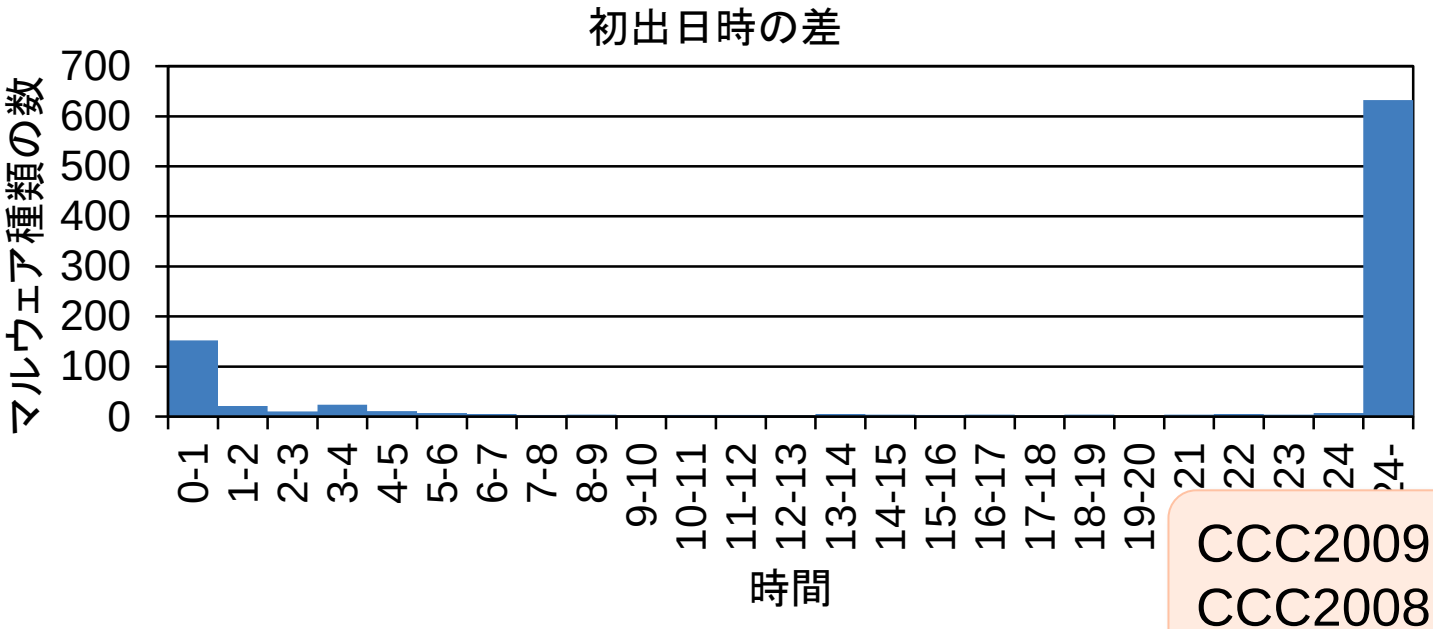






共通マルウェア: どちらで先に観測されていたか

CCC2010 で先に観測されたマルウェア



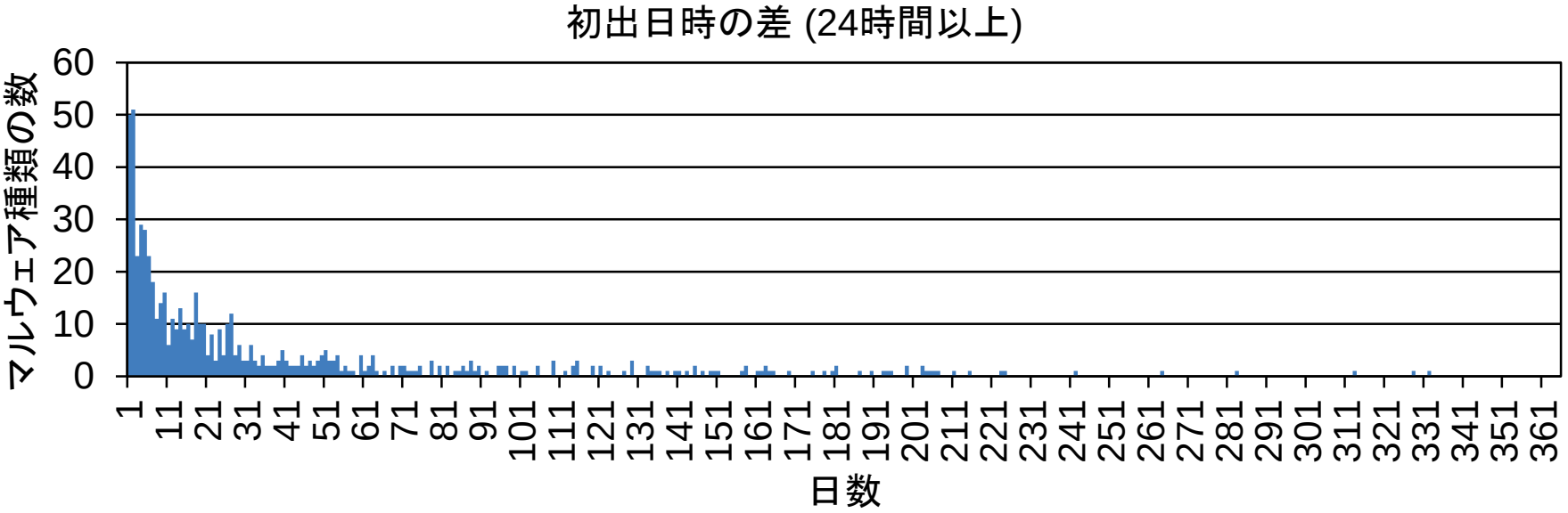
CCC2009: 53%
CCC2008: 59%

共通マルウェア 1388種類のうち

46%は CCC2010 で 24時間以上先行

共通マルウェア: どちらで先に観測されていたか

CCC2010 で先に観測されたマルウェア

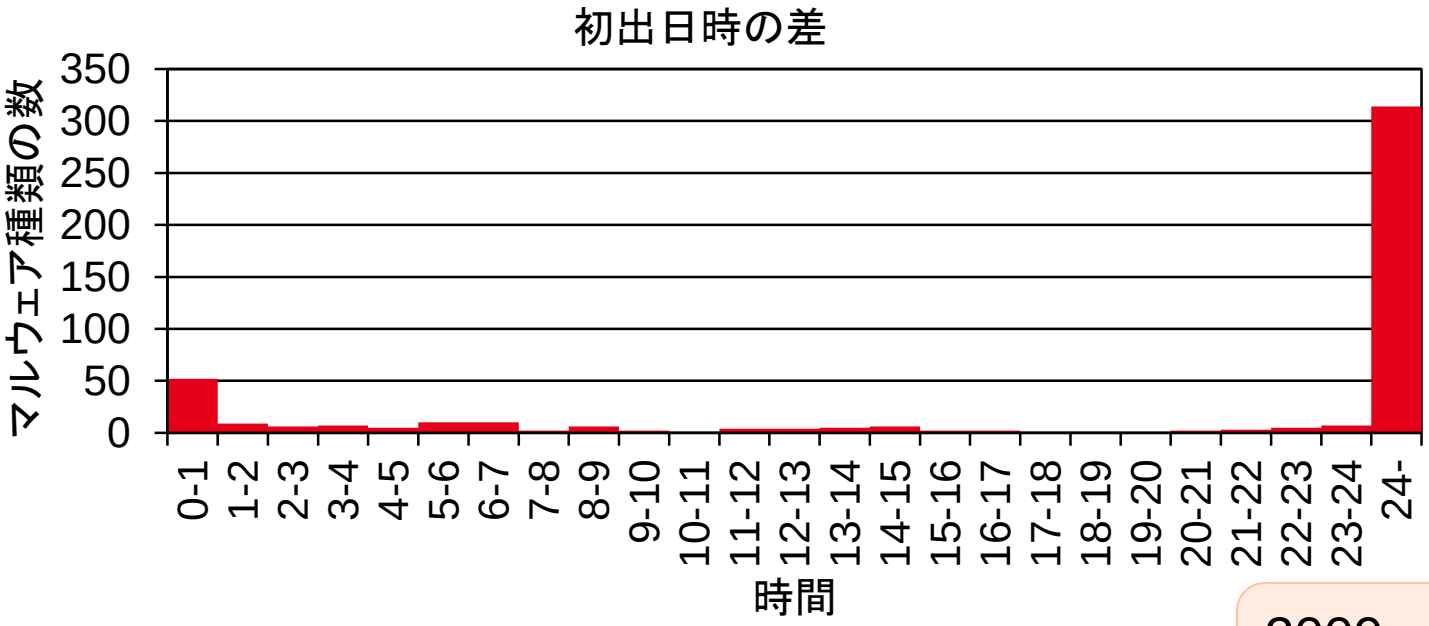


数週間～1年近く遅れてようやくMITFで観測されるものも

(平均27日、最大332日)

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



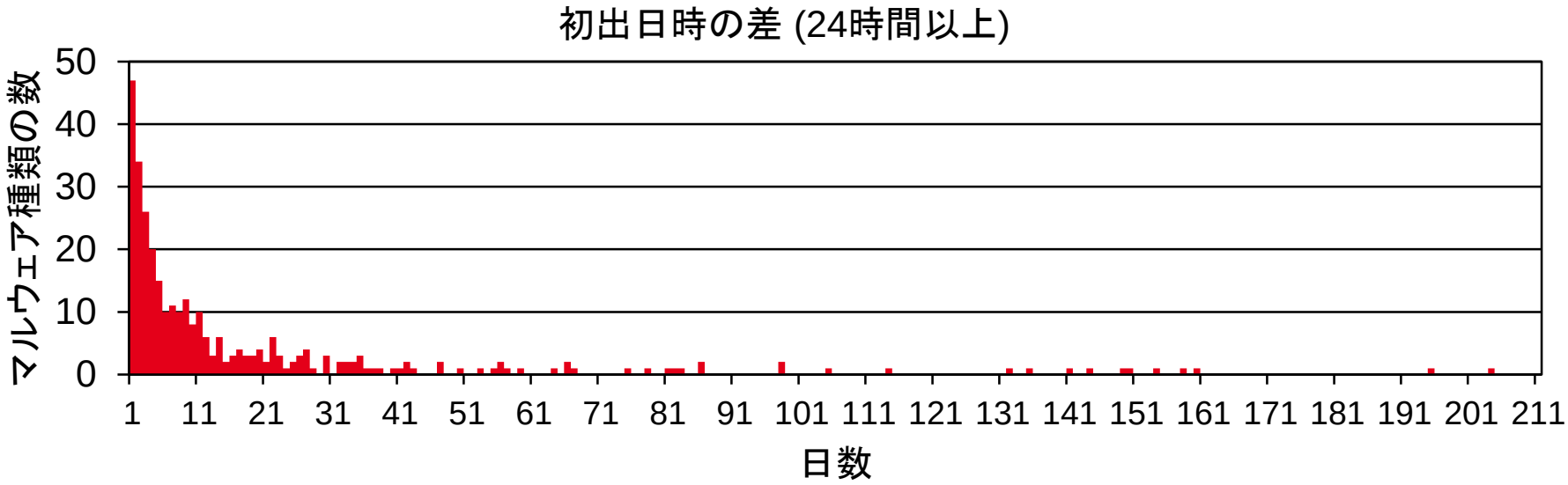
2009: 16%
2008: 8%

共通マルウェア 1388種類のうち

27%は MITF で 24時間以上先行

共通マルウェア: どちらで先に観測されていたか

CCC2010 で先に観測されたマルウェア



数週間～半年以上遅れてようやくCCC2010で観測されるものも

(平均14日、最大204日)

- MITF: IIJ のマルウェア観測
- 観測結果の比較 (MWS2010版)
- 攻撃への対策の検討
- まとめ

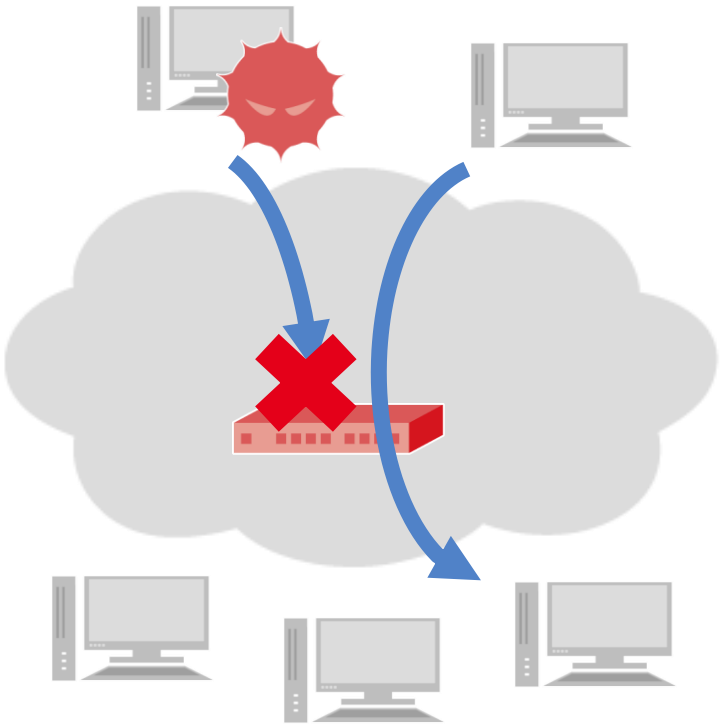
攻撃への対策の検討

ISPによる一次防御

- ISP ルータでIPアドレスによるフィルタリングを実施して感染拡大を防止

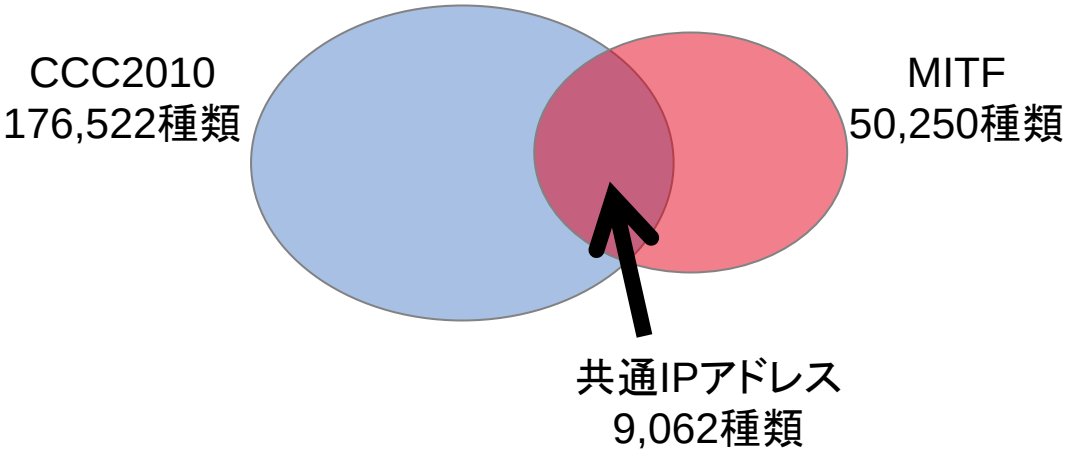
  (注意：実現には技術的課題のほか、法的課題もある)

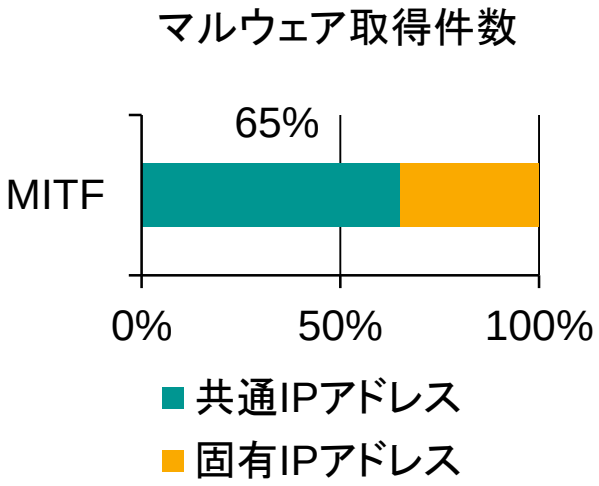
- あくまでも暫定的な回避策
  - すでに感染しているホストは救えない
  - CCCの注意喚起活動やウィルス対策ソフトなど、より本質的な対応がとられるまでの一次対応



攻撃への対策の検討 ― 共通IPアドレス

マルウェア取得元 IP アドレスを軸に検討





CCC2010からマルウェア取得元IPアドレスの情報をもらい

フィルタリングを実施したら

IIJアドレスへの攻撃の65% (のかなりの部分)を防げるのではないか?

攻撃への対策の検討 ― フィルタリングの効果

CCC2010のマルウェア取得元 IP アドレスに対して、その近隣ネットワークをフィルタリングした場合の、IIJネットワーク上での効果を検討

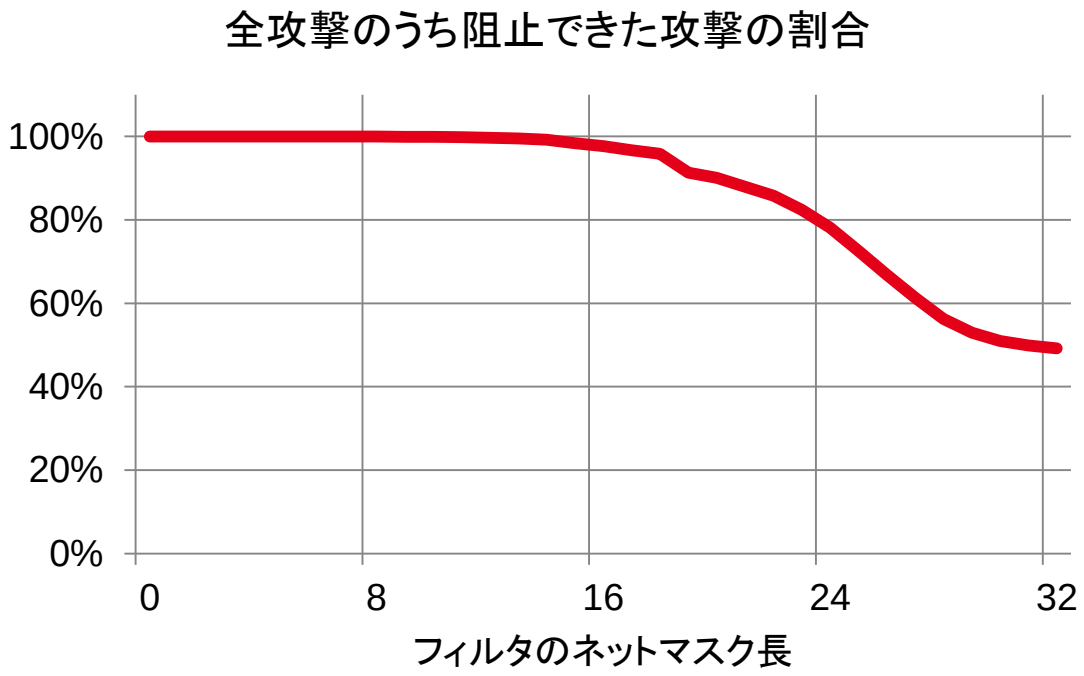
- MITFのデータを「一般利用者PCへの攻撃」とみなして計算することでシミュレート
- アドレス発見からフィルタ適用まで15分のタイムラグを想定

フィルタのネットマスク長は /16? /24? どのくらいが適切?

様々なネットマスク長でシミュレートして比較

攻撃への対策の検討 ― フィルタリングの効果

シミュレーション結果

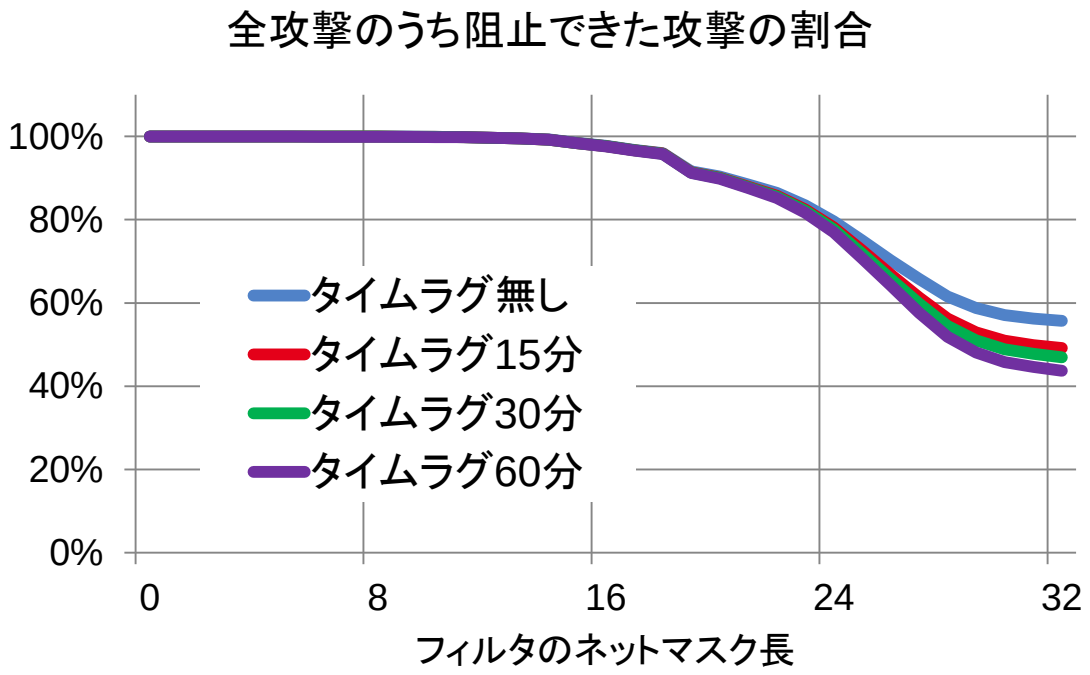


/32の場合、攻撃の49%を未然にブロック

/24なら78%を未然にブロック

攻撃への対策の検討 ― フィルタリングの効果

タイムラグ15分は妥当？



タイムラグが大きくても、効果にはあまり影響しない

- MITF: IIJ のマルウェア観測
- 観測結果の比較 (MWS2010版)
- 攻撃への対策の検討
- まとめ

まとめ

1. 観測結果の比較
   - CCC DATAset2010 攻撃元データと MITF の攻撃元データを比較
   - MWS2008, MWS2009発表と同様の結果
     - 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
   - 今年もこの傾向は継続
2. 攻撃への対策の検討
   - CCC2010の攻撃元IPアドレスをもとにISPルータでフィルタリングした場合を検討
   - フィルタのネットマスク長ごとの効果を評価

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
TEL：03-5259-6450
nagao@iij.ad.jp
http://www.iij.ad.jp/

Ongoing Innovation