ダウンロードホストに着目したマルウェアの活動傾向分析

石井宏樹† 佐藤和哉† 田端利宏‡

†岡山大学工学部

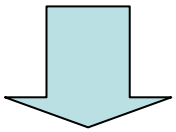
‡岡山大学大学院自然科学研究科

はじめに

- ネットワーク上には多数のマルウェアが存在
- 近年，ボットによる被害が大きな問題

⇒ ボットをはじめとするマルウェアの解析や対策法の検討

ダウンロードホストを重視した研究は少ない



研究用データセットCCC DATAset 2008の攻撃元データの
ダウンロードホストに着目し，マルウェアの特徴を分析

＜目的＞

マルウェアの特徴を明らかにし，マルウェアのダウンロードを抑制するための指標となる情報を示すこと

調査項目

(1) ダウンロードホストの活動期間

・活動期間：調査期間内で初めてダウンロードされた日　～
以降全くダウンロードされなくなる日

(2) ダウンロードホストIPアドレスとマルウェアの種類数の関係

(3) シグネチャファイル配布前後でのダウンロード回数の傾向

(4) マルウェアの1日の平均ダウンロード回数と活動期間の関係

$$1\text{日の平均ダウンロード回数} = \frac{\text{総ダウンロード回数}}{\text{活動期間(日)}}$$

(5) ダウンロードホストIPアドレスとマルウェア名の関係

ダウンロードホストの活動期間

マルウェアの実行ファイルは，ダウンロードホストからダウンロード

⇒ ダウンロードホストの活動期間の特徴の明確化

⇓

ダウンロードホストIPアドレス（258,711個）のうち，調査期間内のダウンロード回数の上位20個を抽出し，１日単位の傾向を分析

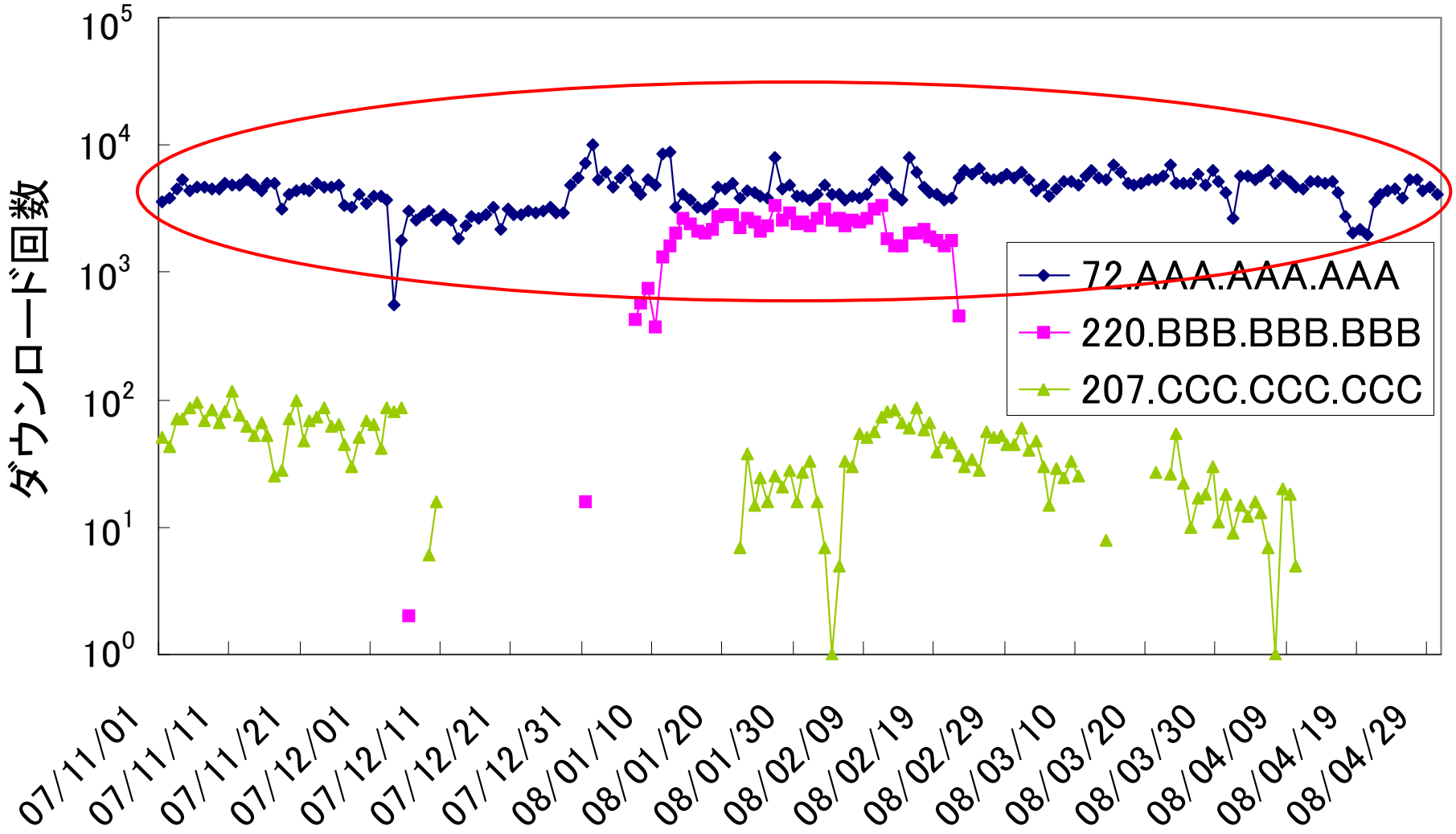
＜抽出したIPアドレスの数が20個である理由＞

- 調査期間内の総ダウンロード回数は，2,942,221回
- 上位20個の総ダウンロード回数は，1,116,347回

⇒ 全体の約38%を占める

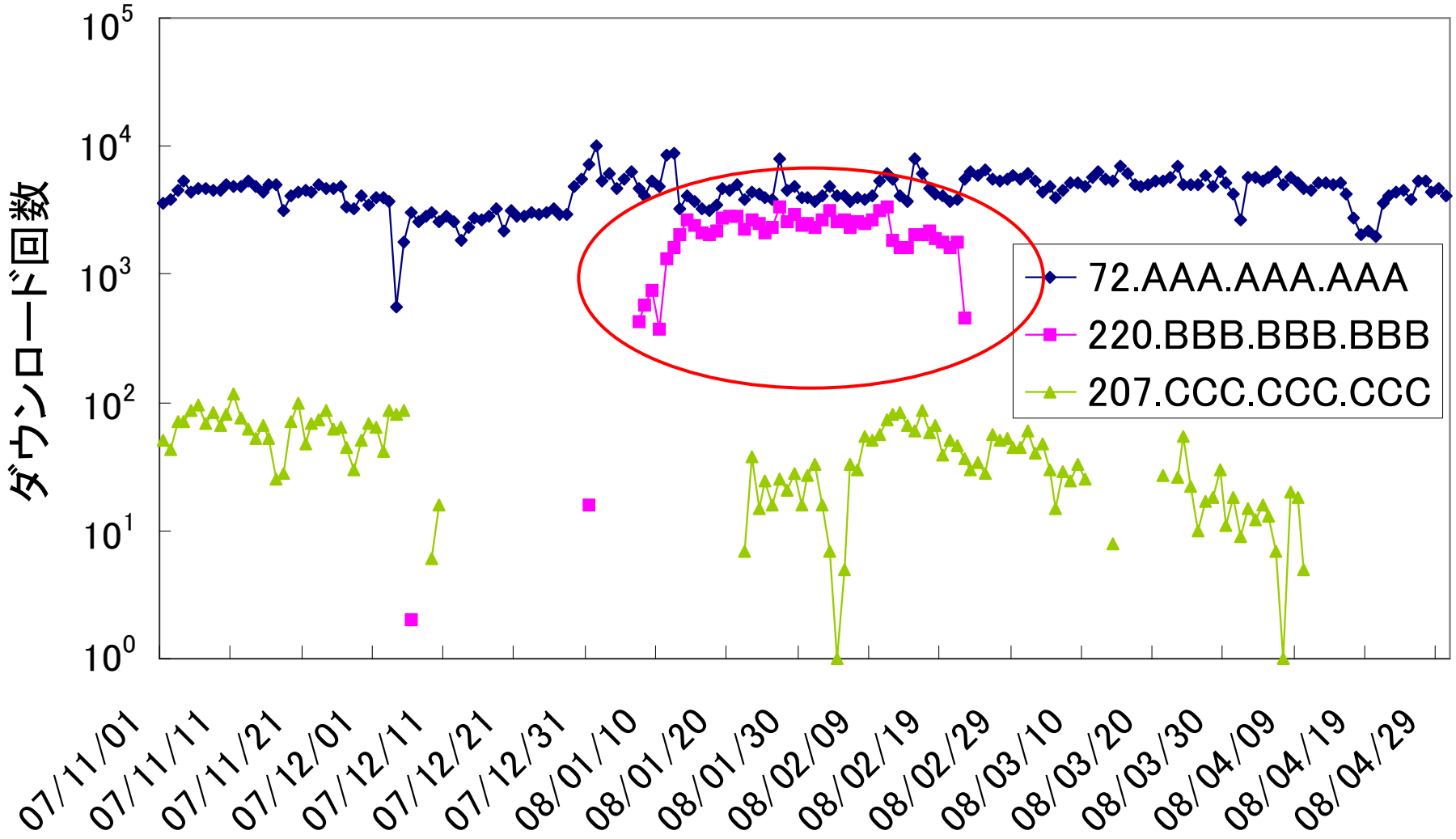
上位20個を調査することで，十分な傾向分析が可能と判断

活動期間の調査結果(1/3)



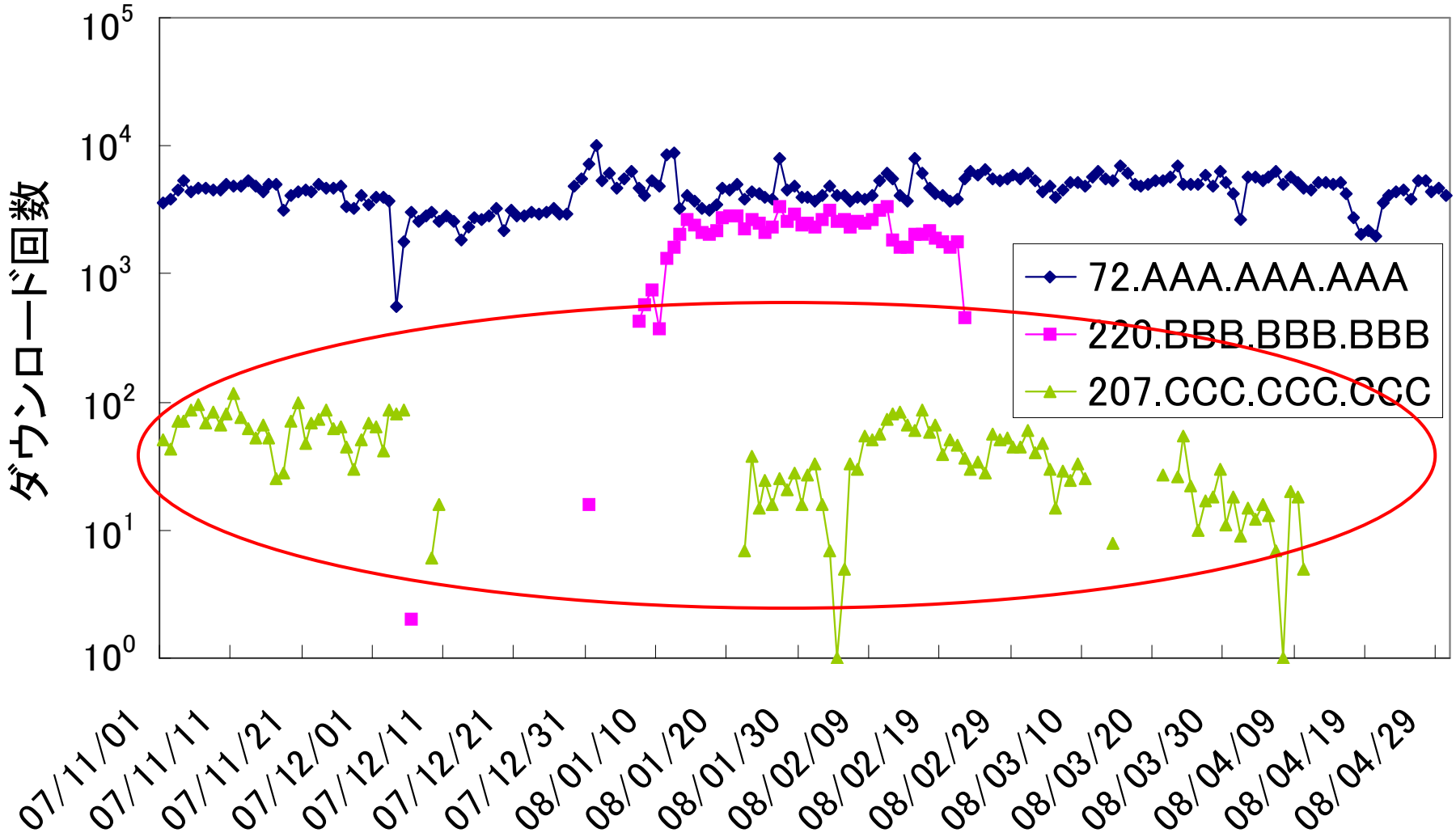
(1) 長期間(3ヶ月以上)ダウンロードホストとして活動しているもの

活動期間の調査結果(2/3)



(2) 短期間(3ヶ月未満)ダウンロードホストとして活動しているもの

活動期間の調査結果(3/3)



(3) 長期間ダウンロードホストとして活動しており，活動期間の間に1ヶ月以上活動していない期間を含むもの(複数期間)

活動期間の調査結果まとめ

ダウンロードホストIPアドレスと活動期間の関連の分類

(1) 長期間（3ヶ月以上）ダウンロードホストとして活動

(2) 短期間（3ヶ月未満）ダウンロードホストとして活動

(3) 複数期間ダウンロードホストとして活動

抽出した上位20個についての分析結果

特徴	個数
（1）長期間	5個
（2）短期間	12個
（3）複数期間	3個

→ 短期間活動しているものが多い

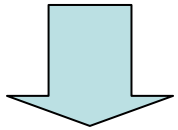
＜考察＞

- 攻撃者は，ダウンロードホストが停止させられた場合にも，マルウェアの頒布続行
- そのために，ダウンロードホストIPアドレスを頻繁に変更

ダウンロードホストIPアドレスとマルウェアの種類数の関係

＜予想＞

複数のマルウェアがダウンロードされるダウンロードホストIPアドレスからの通信を遮断



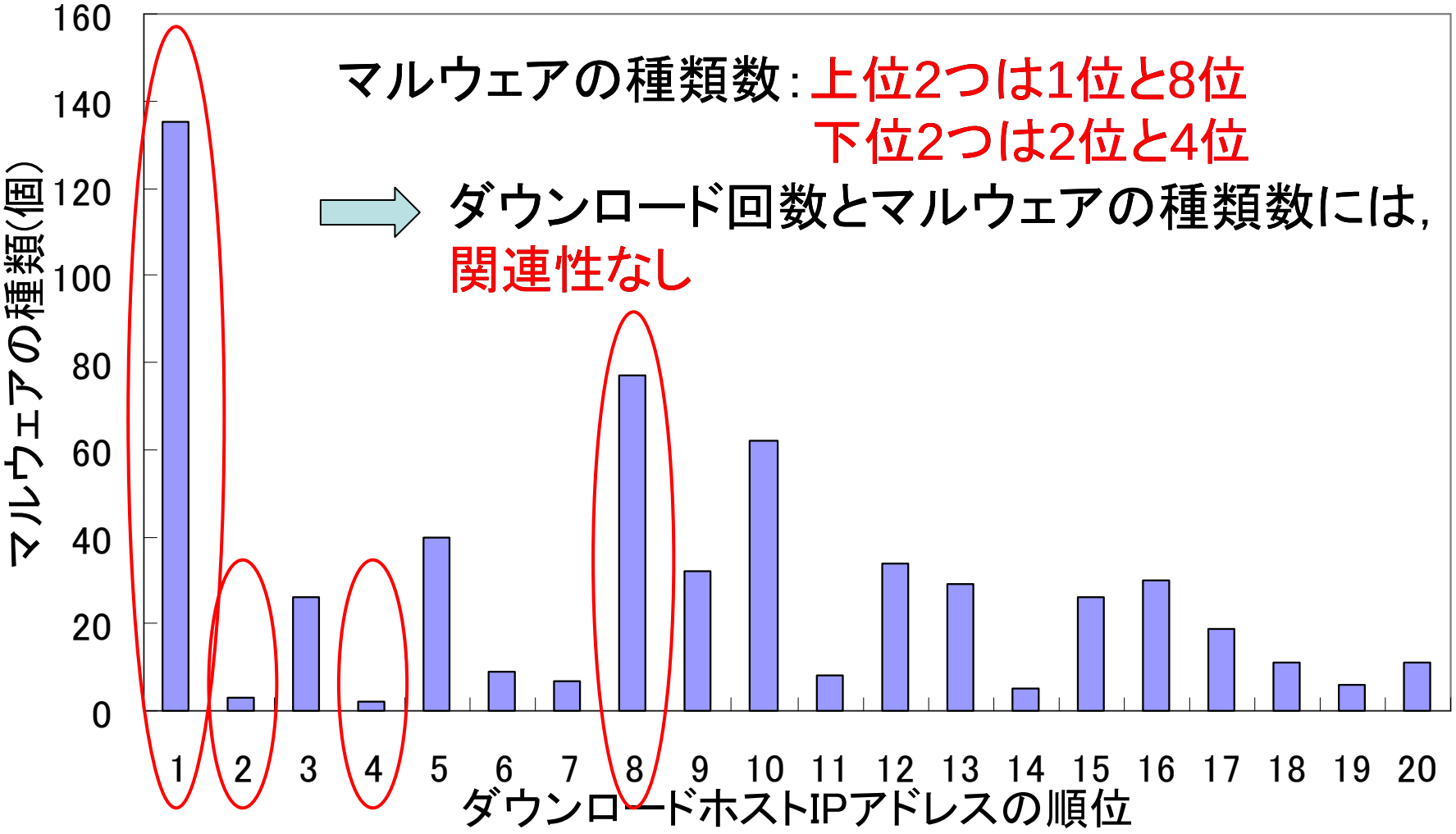
複数のマルウェアの感染防止が可能

総ダウンロード回数の多いダウンロードホストIPアドレスから，ダウンロードされるマルウェアの種類数の傾向を調査

＜使用したダウンロードホストIPアドレス＞

調査期間内のダウンロード回数が上位20位まで

ダウンロード回数とマルウェアの種類数の関係の調査結果(1/2)



ダウンロード回数とマルウェアの種類数の関係の調査結果(2/2)

順位	平均ダウンロード回数	標準偏差	種類数
1	6125.6	9226.9	135
2	33793.7	47778.7	3
3	1296.6	1933.9	26
4	9701.0	9693.0	2
5	478.2	752.6	40
6	1523.8	1464.3	9
7	1701.7	1665.9	7
8	139.4	147.1	77
9	326.8	559.4	32
10	158.1	170.6	62
11	1178.6	1867.0	8
12	254.6	602.7	34
13	277.5	539.4	29
14	1267.0	1021.6	5
15	187.5	111.6	26
16	154.7	201.4	30
17	241.2	409.7	19
18	409.5	302.6	11
19	723.0	833.7	6
20	338.8	265.1	11

ダウンロード回数とダウンロードされたマルウェアの種類の特徴

(1) ダウンロード回数の大部分が1から数種類の特定のマルウェア
例:2位, 17位

(2) ダウンロード回数の大部分を占めるマルウェアが存在しない
例:8位, 15位

＜考察＞

(1):特定のマルウェアの拡大防止可能

(2):多種のマルウェアの拡大防止可能

シグネチャファイル配布前後でのダウンロード回数の傾向

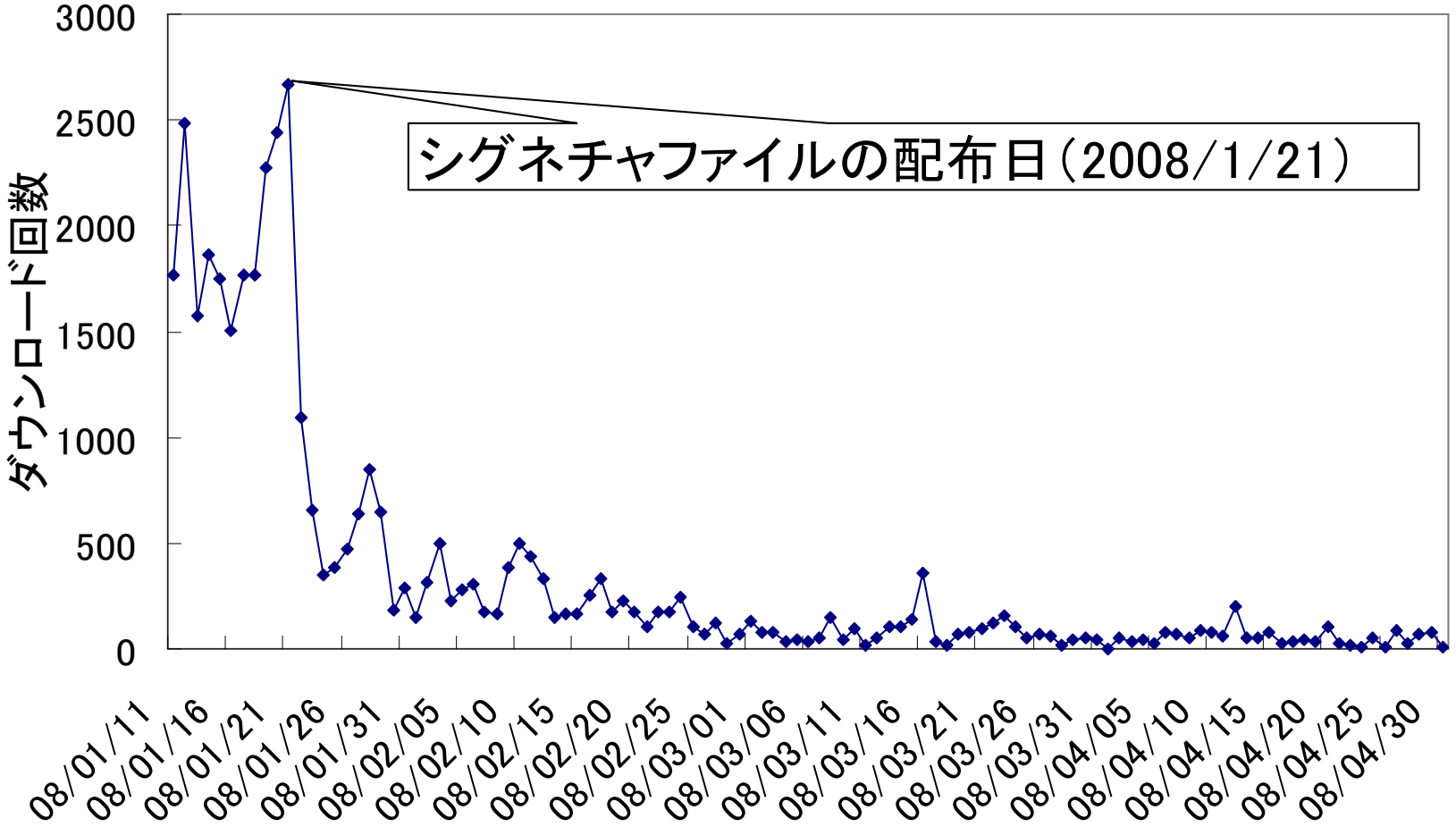
- シグネチャファイルの配布により，マルウェアの駆除が可能
- 攻撃者は，解析されたマルウェアの使用中止，もしくは使用困難に

＜予想＞

解析されていない状態と解析後の状態の比較から，ダウンロード回数の減少などの傾向有り

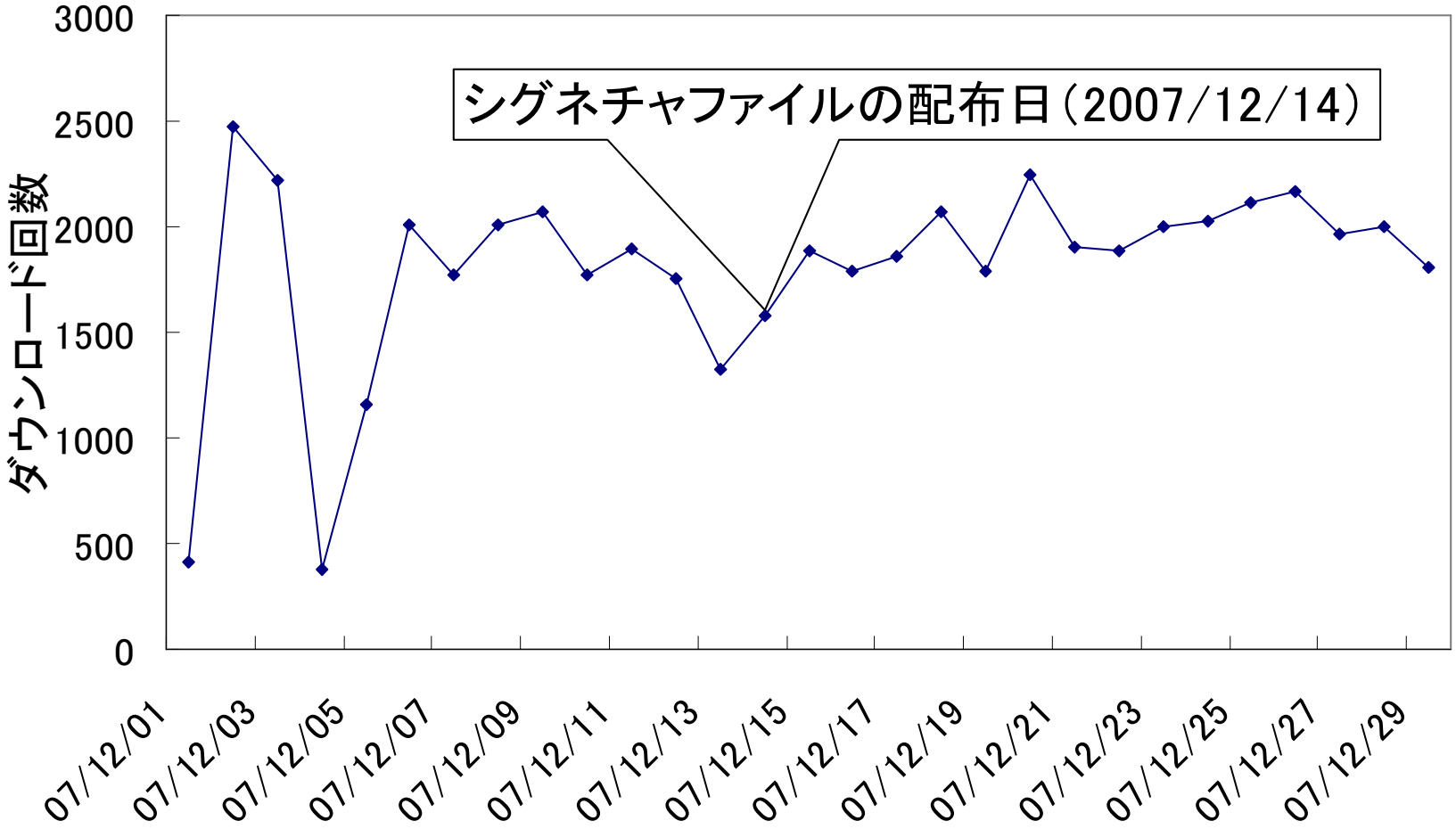
マルウェアのハッシュ値ごとのダウンロード回数の変化とシグネチャファイルの配布日の関連を調査

シグネチャファイル配布前後の傾向調査結果(1/3)



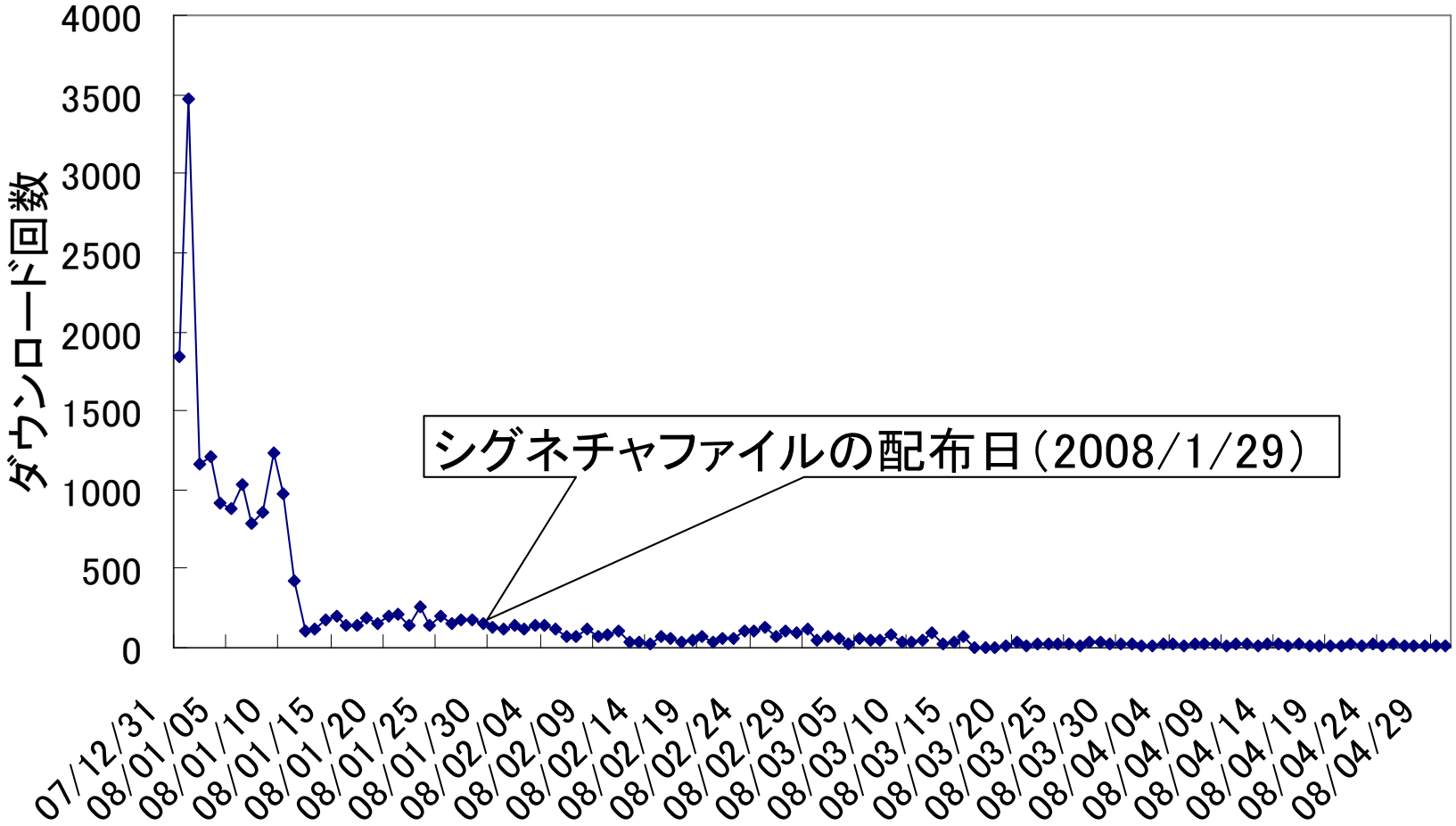
(1) シグネチャファイル配布後にダウンロード回数が減少

シグネチャファイル配布前後の傾向調査結果(2/3)



(2) ダウンロード回数の変化がほぼ一定

シグネチャファイル配布前後の傾向調査結果(3/3)



(3) 活動開始日付近のみダウンロード回数が多い

シグネチャファイル配布前後の傾向調査結果のまとめ

シグネチャファイル配布前後でのダウンロード回数の傾向分類

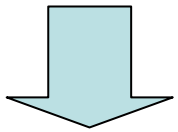
(1) シグネチャファイル配布後にダウンロード回数が減少

(2) ダウンロード回数の変化がほぼ一定

(3) 活動開始日付近のみダウンロード回数が多い

＜分類結果＞

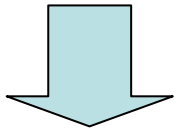
- (2)と(3)に該当するマルウェアがほとんど
- (1)はシグネチャファイルの配布日が(3)の急激に減少する時期に偶然重なっただけ



シグネチャファイル配布前後でのダウンロード回数に明確な変化なし

マルウェアの1日の平均ダウンロード回数と活動期間の関係

- マルウェアの存在が明らかになると，解析が行われる
- 攻撃者は，解析されたマルウェアの使用中止，もしくは使用困難に



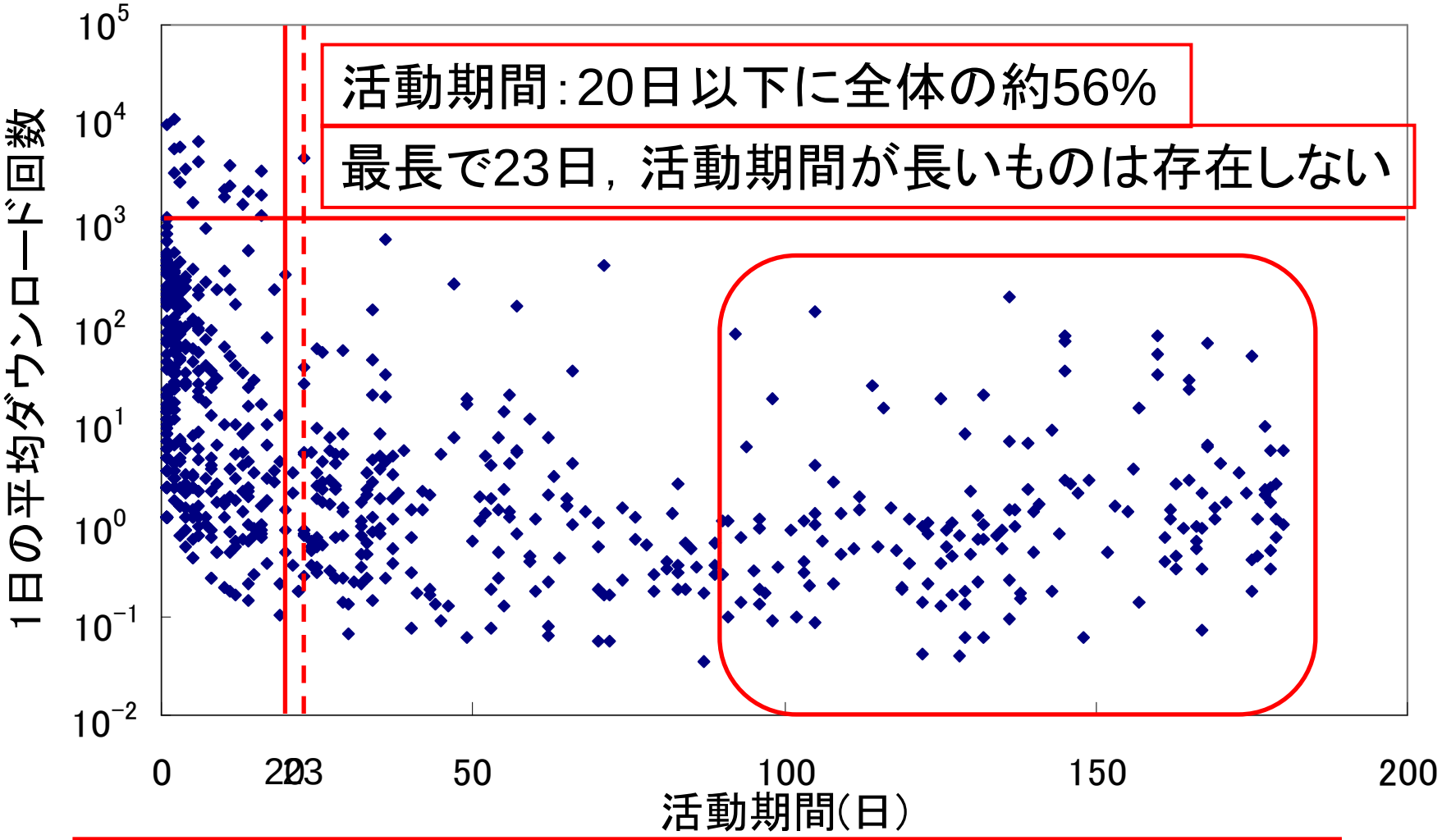
＜予想＞

(1) 1日の平均ダウンロード回数が多いマルウェア
⇒ 存在が明らかになりやすいため，活動期間が短い

(2) 1日の平均ダウンロード回数が少ないマルウェア
⇒ 活動期間が長い

マルウェアごとの1日の平均ダウンロード回数とそのマルウェアの活動期間について調査

平均ダウンロード回数と活動期間の調査結果



活動期間長：平均ダウンロード回数の少ないものが多い

平均ダウンロード回数と活動期間の調査結果のまとめ

1日の平均ダウンロード回数と活動期間の関係

(1) 平均ダウンロード回数の多いマルウェア：活動期間が短い

⇒ マルウェアの早期解析，シグネチャファイル配布等の対策が有効

(2) 平均ダウンロード回数の少ないマルウェア：活動期間が長い

⇒ ダウンロードホストの早期停止等のマルウェア拡散への対策が有効

ダウンロードホストIPアドレスと マルウェア名の関係

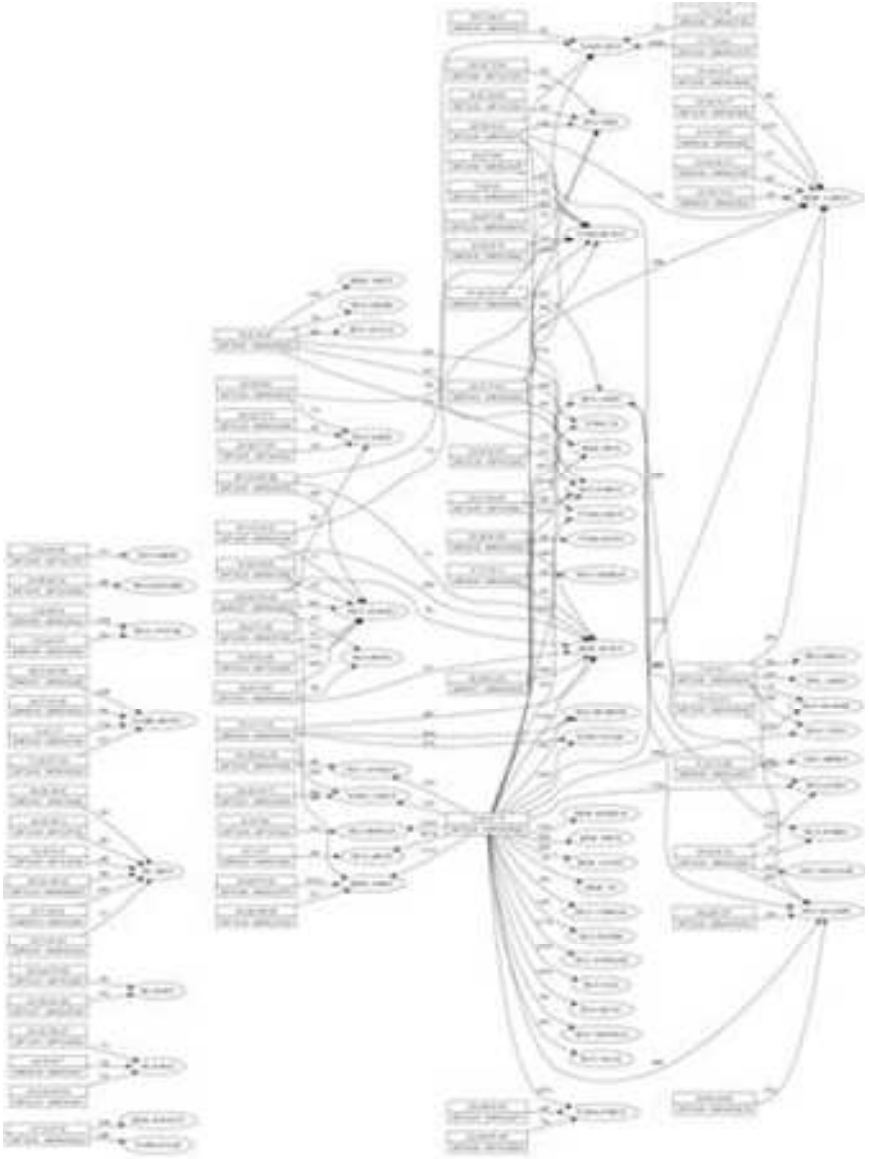
- マルウェアの実行ファイルはダウンロードホストからダウンロード
- 用いられるIPアドレスは，攻撃者により指定

＜予想＞

(1) マルウェア名とダウンロードホストIPアドレスには，関連性有り

(2) 特定のマルウェアに着目したとき，用いられるダウンロードホストIPアドレスの活動期間には，特徴有り

IPアドレスとマルウェアの関係の調査結果（1/4）



＜ダウンロードホストの分類＞

(1) 多種のマルウェアがダウンロードされるホスト

(2) 1，2種類のみのマルウェアがダウンロードされるホスト

＜マルウェアの分類＞

(1) 多数のダウンロードホストからダウンロード

(2) 1，2個のダウンロードホストからのみダウンロード

IPアドレスとマルウェアの関係の調査結果(2/4)

多種のマルウェアがダウンロードされるダウンロードホスト

活動期間が比較的長い

72.AAA.AAA.AAA
活動期間:2007/11/01-2008/04/30(182日)

IPアドレスとマルウェアの関係の調査結果(3/4)

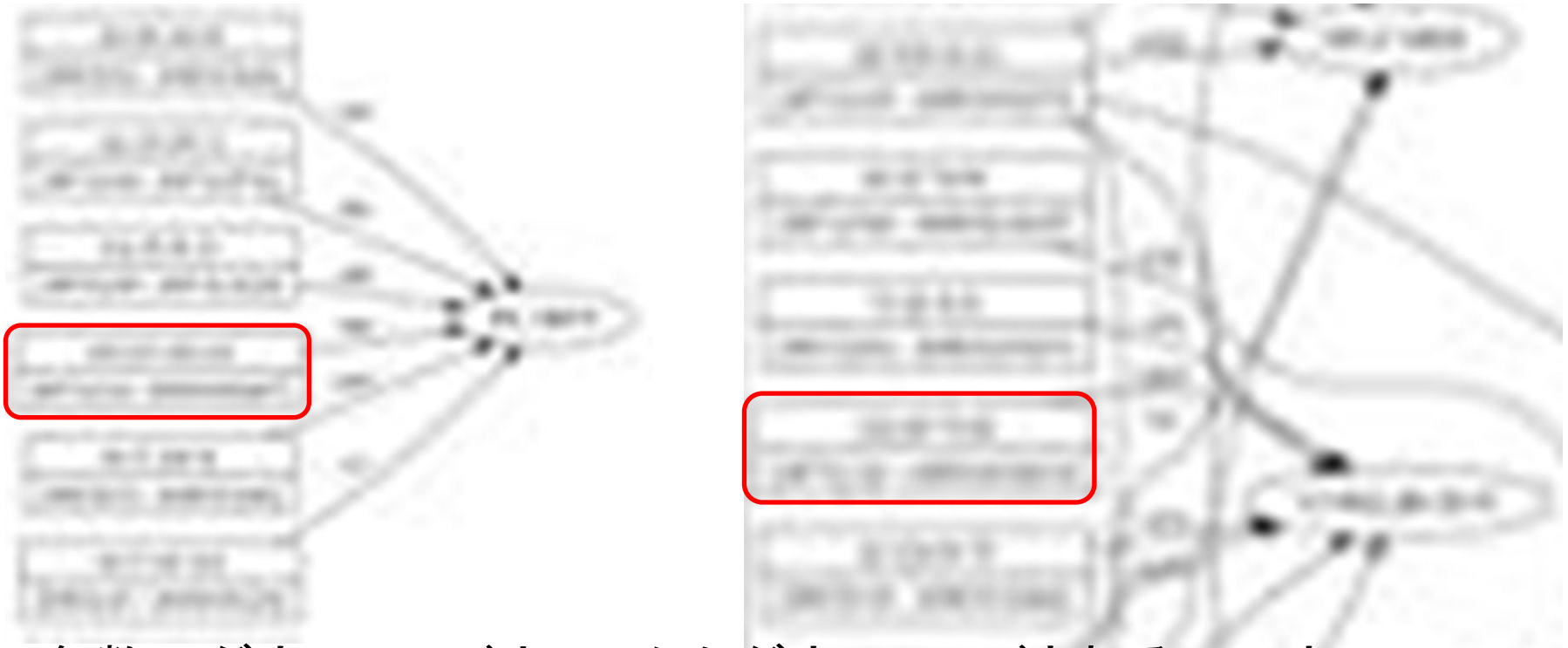
220.DDD.DDD.DDD
活動期間:2007/12/08-2008/02/12(57日)

125.EEE.EEE.EEE
活動期間:2008/01/26-2008/01/29(4日)

ダウンロードされたマルウェアが1，2種類しかないダウンロードホスト

活動期間が比較的短い

IPアドレスとマルウェアの関係の調査結果(4/4)



多数のダウンロードホストからダウンロードされるマルウェア

利用するホストには，長期間(3ヶ月以上)活動するダウンロードホストが含まれる

IPアドレスとマルウェアの関係の調査結果の考察

活動期間の長いダウンロードホストの特定

⇒ (1) 多種のマルウェア感染の拡大防止

(2) 長期間のダウンロードによる，特定のマルウェアの感染の拡大防止

まとめ

＜調査内容＞

攻撃元データのダウンロードホストに着目し，マルウェアの特徴を分析

＜調査結果＞

(1) ダウンロードホストの活動期間
長期間，短期間，および複数期間の3種類に分類可能

(2) ダウンロード回数とマルウェアの種類数の関連性は薄い

(3) シグネチャファイル配布前後でダウンロード回数の変化は小さい

(4) 1日の平均ダウンロード回数が多いマルウェアの活動期間は短い

(5) ダウンロードホストの活動期間が長いものほど，ダウンロードされるマルウェアの種類数が多い