本資料について

- 本資料は下記書籍を基にして作成されたものです
- 文書の内容の正確さは保証できないため、正確な知識を求める方は原文を参照してください

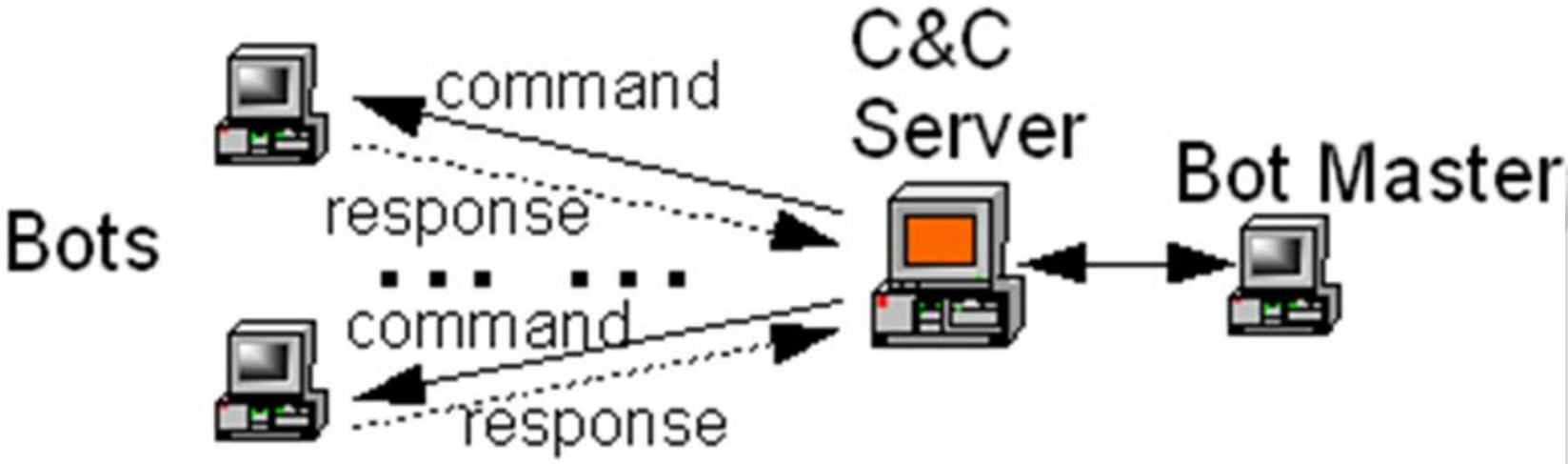
- 文献
  - BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic
- 著者
  - Guofei Gu, Junjie Zhang, and Wenke Lee
- 発行元
  - Georgia Institute of Technology Atlanta
- 発表年
  - 2008年

BotSnifferによるボットネットの検出法

渡邊研究室
染川敦

ボットネットとは

- パソコンやサーバに遠隔操作できる攻撃用プログラム(ボット)を送り込み外部から制御・命令できるネットワーク
- ボットネットはC&C(Command & Control, 命令・制御)チャネルをもつ



研究背景

- ボットネットは最も深刻なセキュリティ問題のひとつ
- ボットネットは一般的に存在するプロトコルを使用する(例 :IRC, HTTP)

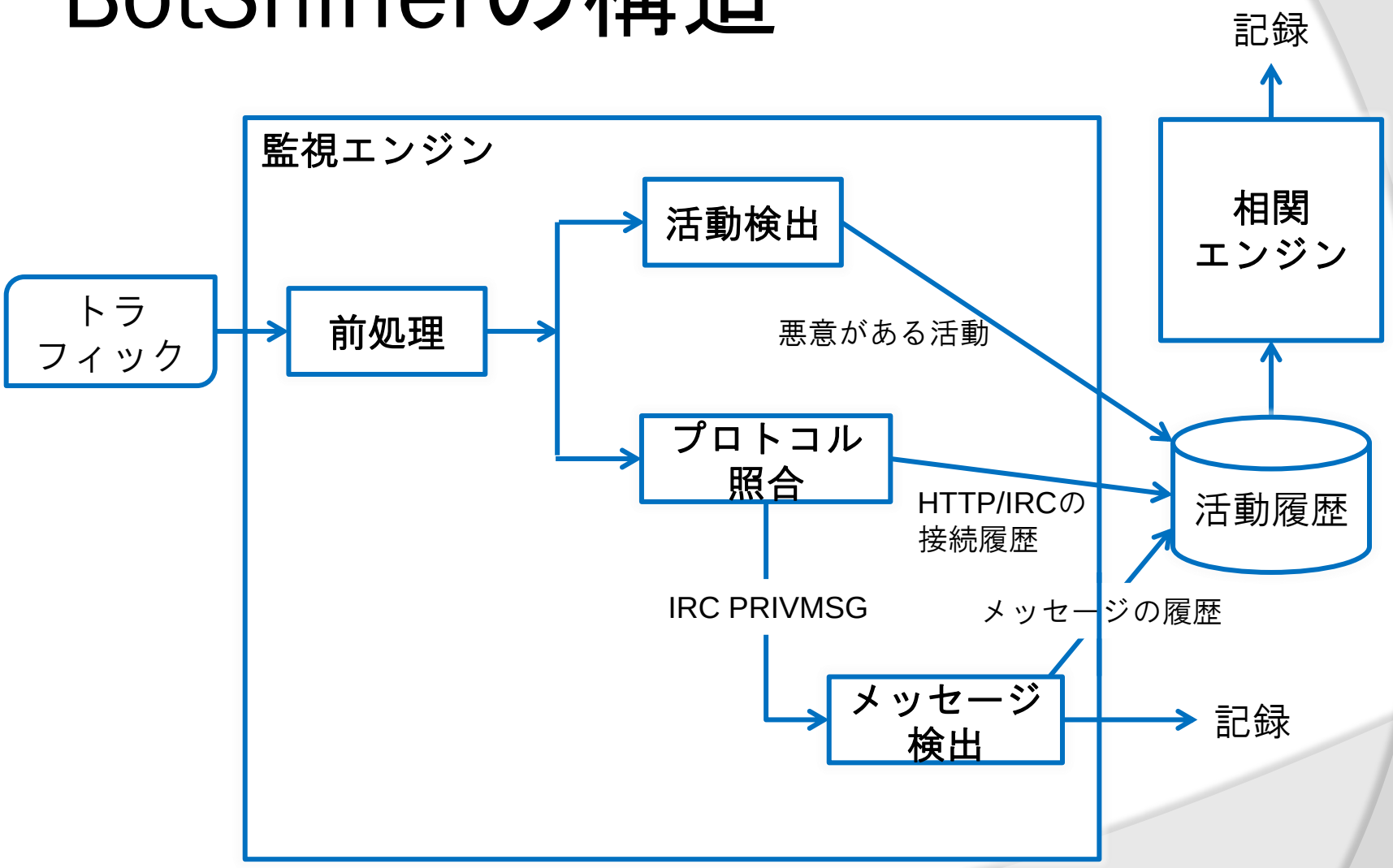
目的

- 事前知識なしでのボットネットの検出システムの開発
- このシステムをBotSnifferと名付ける

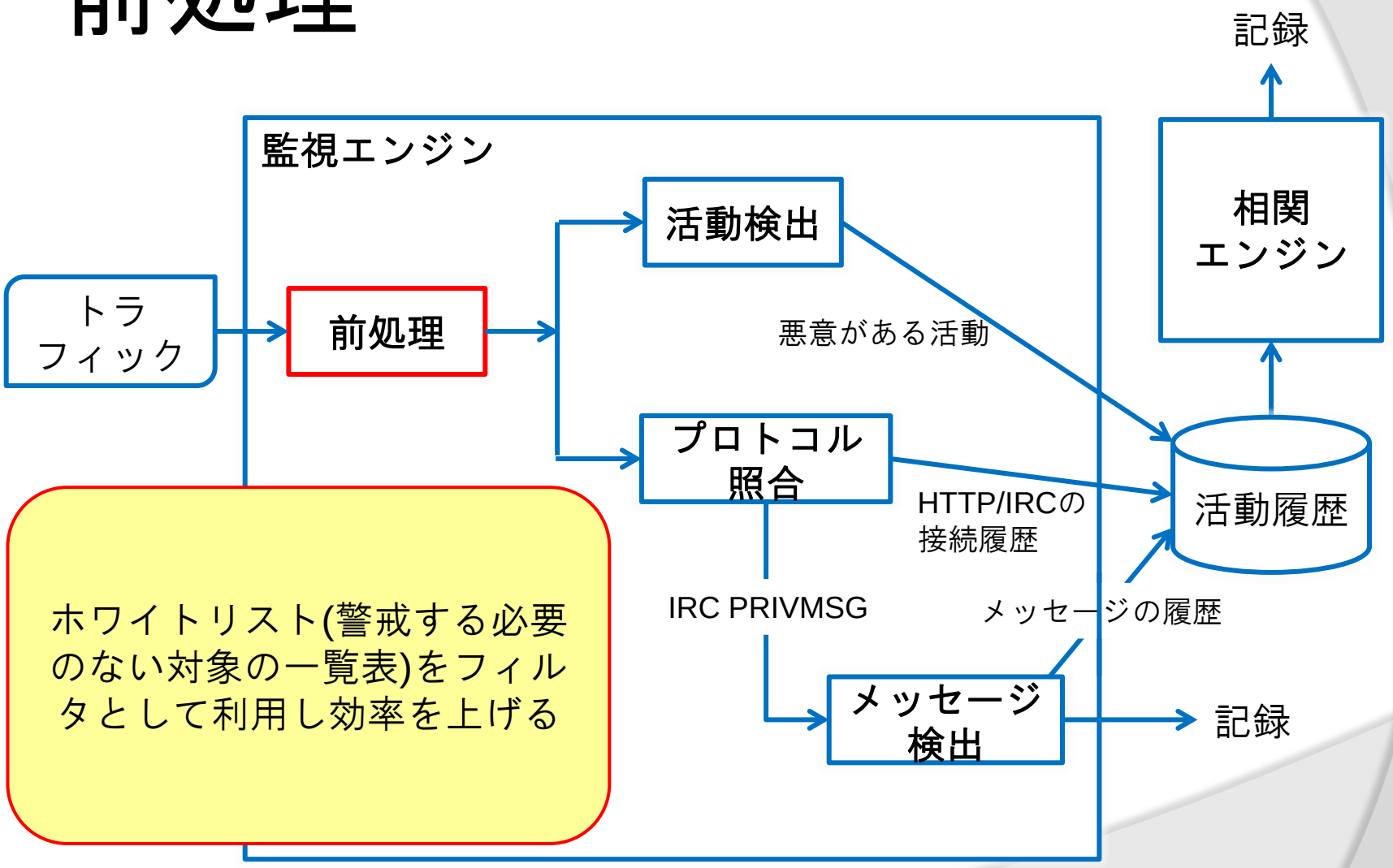
提案方式

- ネットワークの異常を検出し、ボットネットC&Cを識別する
- 同じボットネット内のボットは相関性や類似性があることを利用する

BotSnifferの構造

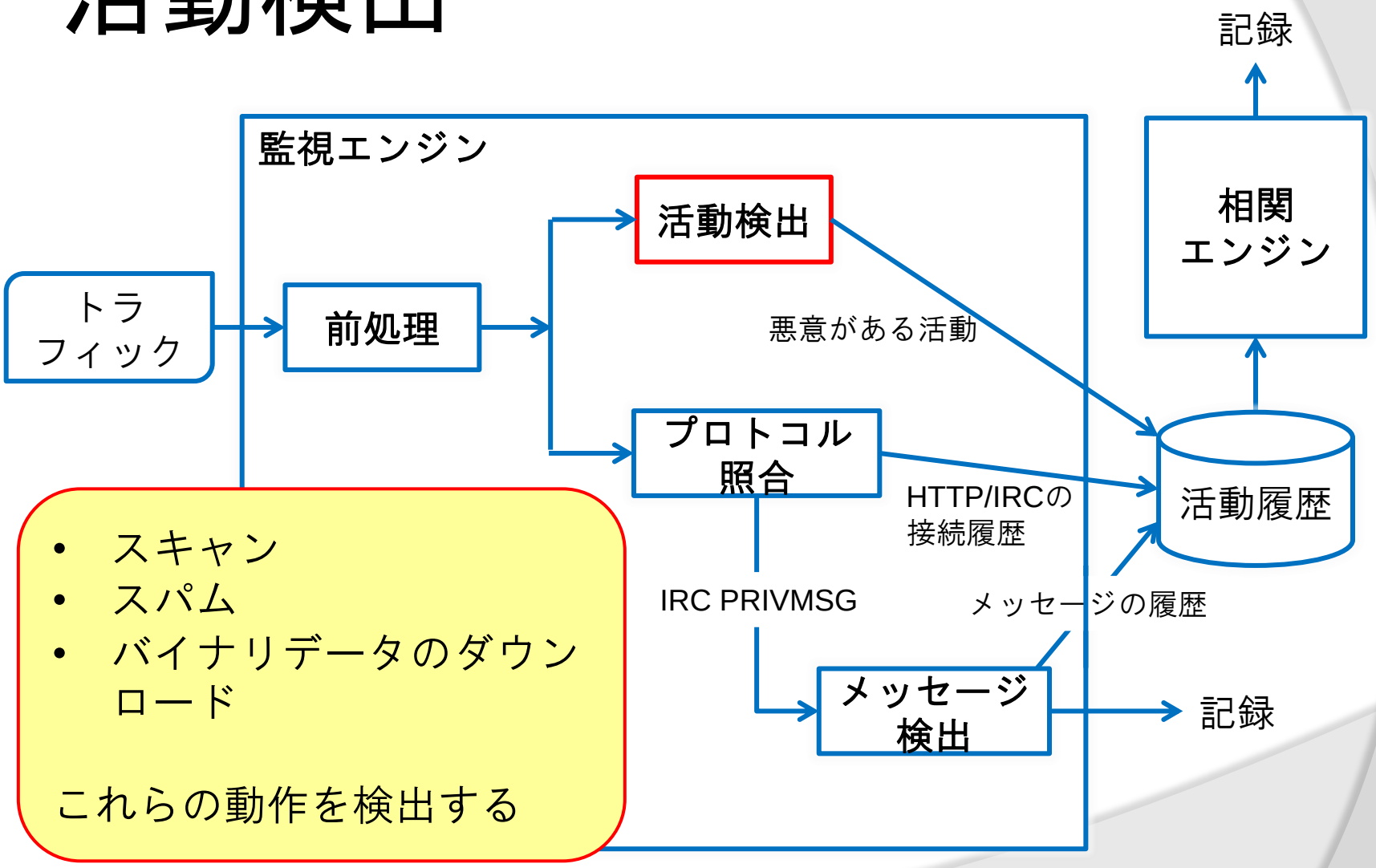


前処理



ホワイトリスト(警戒する必要のない対象の一覧表)をフィルタとして利用し効率を上げる

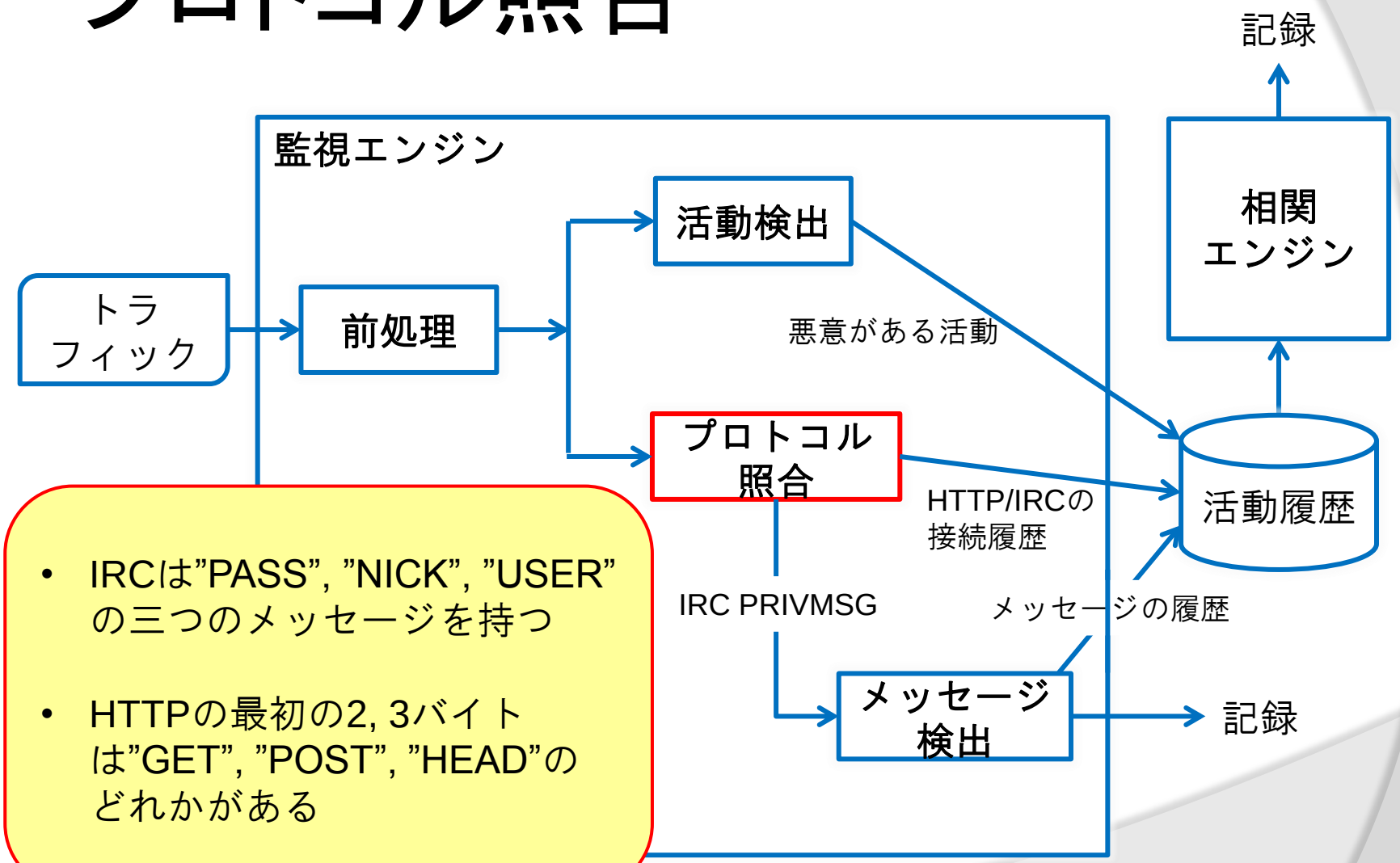
活動検出



- スキャン
- スパム
- バイナリデータのダウンロード

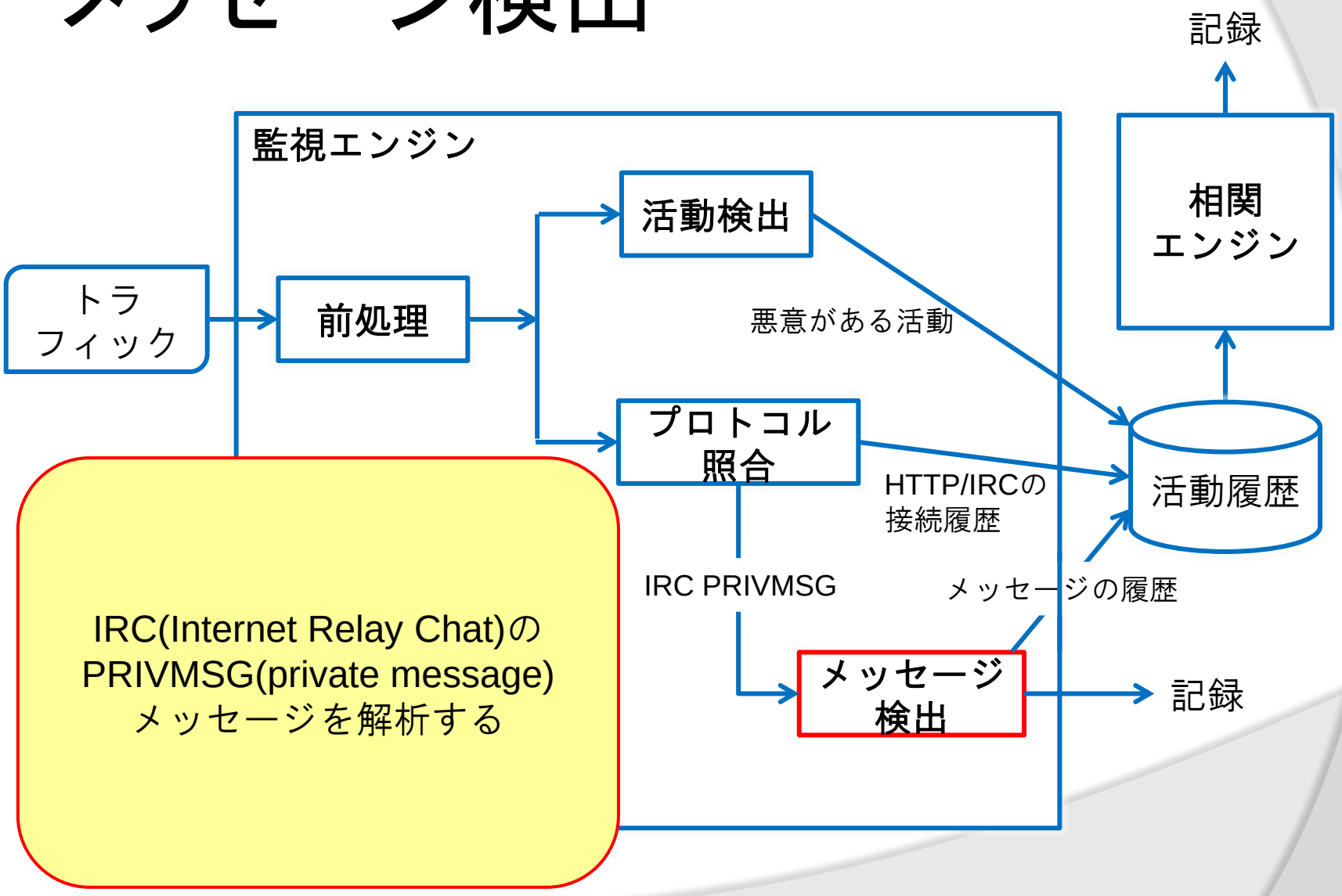
これらの動作を検出する

プロトコル照合

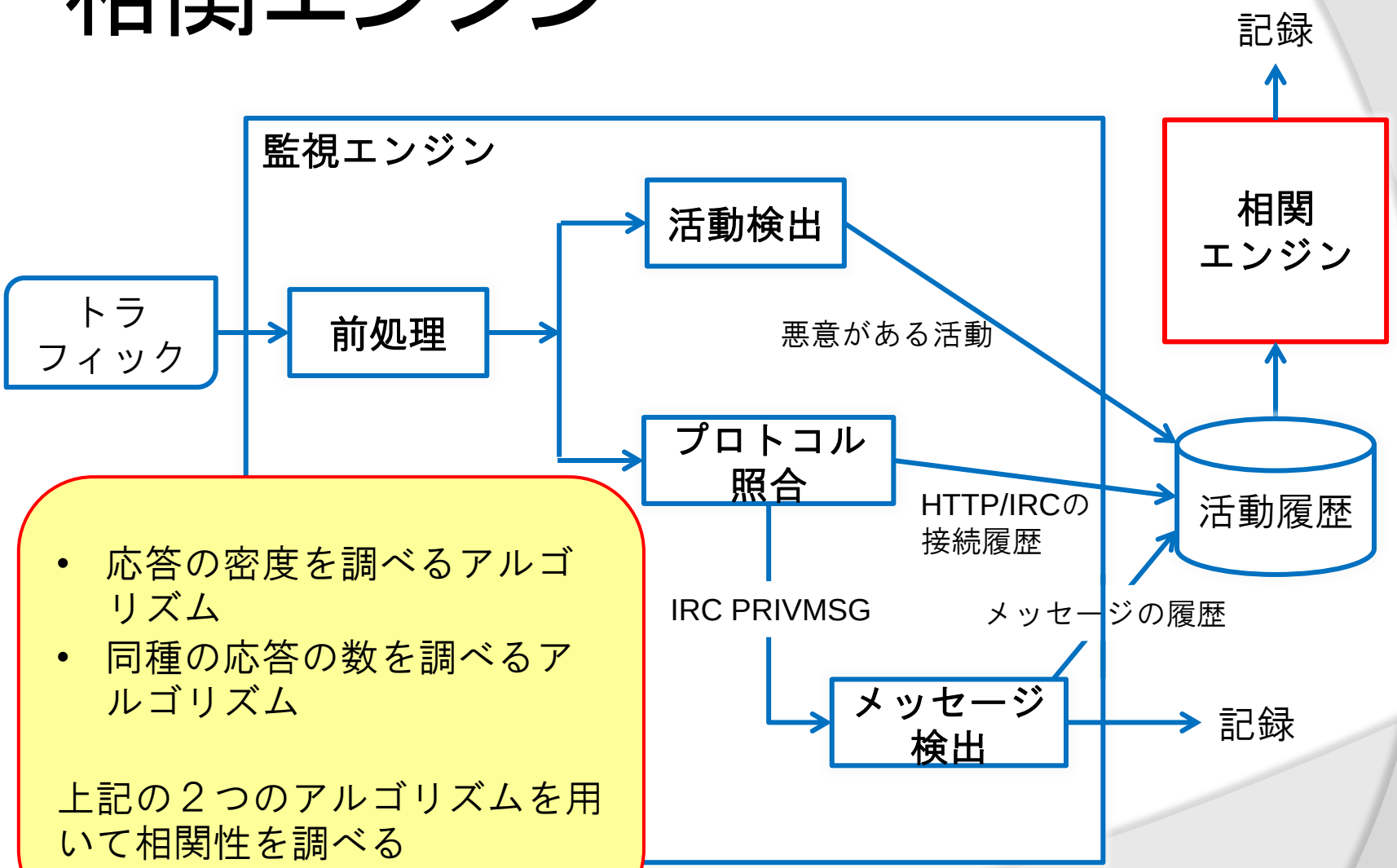


- IRCは”PASS”, ”NICK”, ”USER”の三つのメッセージを持つ
- HTTPの最初の2, 3バイトは”GET”, ”POST”, ”HEAD”のどれかがある

メッセージ検出


記録
監視エンジン
相関
エンジン
活動検出
トラ
フィック
前処理
悪意がある活動
プロトコル
照合
HTTP/IRCの
接続履歴
活動履歴
IRC PRIVMSG
メッセージの履歴
メッセージ
検出
記録
IRC(Internet Relay Chat)の
PRIVMSG(private message)
メッセージを解析する

相関エンジン



- 応答の密度を調べるアルゴリズム
- 同種の応答の数を調べるアルゴリズム

上記の２つのアルゴリズムを用いて相関性を調べる

結果

トレース	パケット	検出
B-IRC-1	4447	成功
B-IRC-2	143431	成功
B-IRC-3	262878	成功
V-Rbot	347153	成功
V-Spybot	180822	成功
V-Sdbot	474	成功
B-HTTP-1	65695	成功
B-HTTP-2	395990	成功

ボットネットのトレース

トレース	パケット	誤検出
IRC-1	189421	0
IRC-2	33320	0
IRC-3	2073587	6
IRC-4	4071707	3
IRC-5	19190	0
IRC-6	1033318	1
IRC-7	393185	0
IRC-8	2818315	1
ALL-1	4706803	0
ALL-2	6769915	0
ALL-3	16523826	0
ALL-4	21312841	0
ALL-5	43625604	0

通常のトレース

関連研究

- Honeypot
  - 不正アクセスを受けることに価値を持つシステム
  - 正規の通信が発生しないため検出漏れをなくすことができる
  - 実際に不正アクセスを受けるため踏み台にされる恐れがある

まとめ

- ボットネットは最も深刻なセキュリティ問題のひとつ
- 同じボットネット内のボットの制御には相関性がある
- ボットネットは事前知識なしに検出することができる

今後の課題

- 分析でより多くの特徴を組み合わせる
- インターネット上に分散して配置する

参考資料

- Cyber Clean Center
  (URL :https://www.ccc.go.jp/bot/)

- @IT -ハニーポットを利用したネットワークの危機管理
  (http://www.atmarkit.co.jp/fsecurity/special/13honey/honey01.html)

- ハニーポット -Wikipedia
  (URL: ja.wikipedia.org/wiki/ハニーポット)