WCLSCAN

インターネット
早期広域攻撃警戒システム
WCLSCAN

鈴木裕信※1　石黒正輝※2　村瀬一郎※2　大野浩之※3

※1 鈴木裕信事務所

※2 株式会社三菱総合研究所　情報技術研究部

※3 独立行政法人通信総合研究所　情報通信部門非常時通信グループ

概要

- 背景・モチベーション・ゴール
- システム概要
- ベイズ推定による攻撃検知手法
- 評価実験・ケース紹介
- 一般ユーザ利用方法
- 今後の課題
- まとめ
- デモ

背景・モチベーション

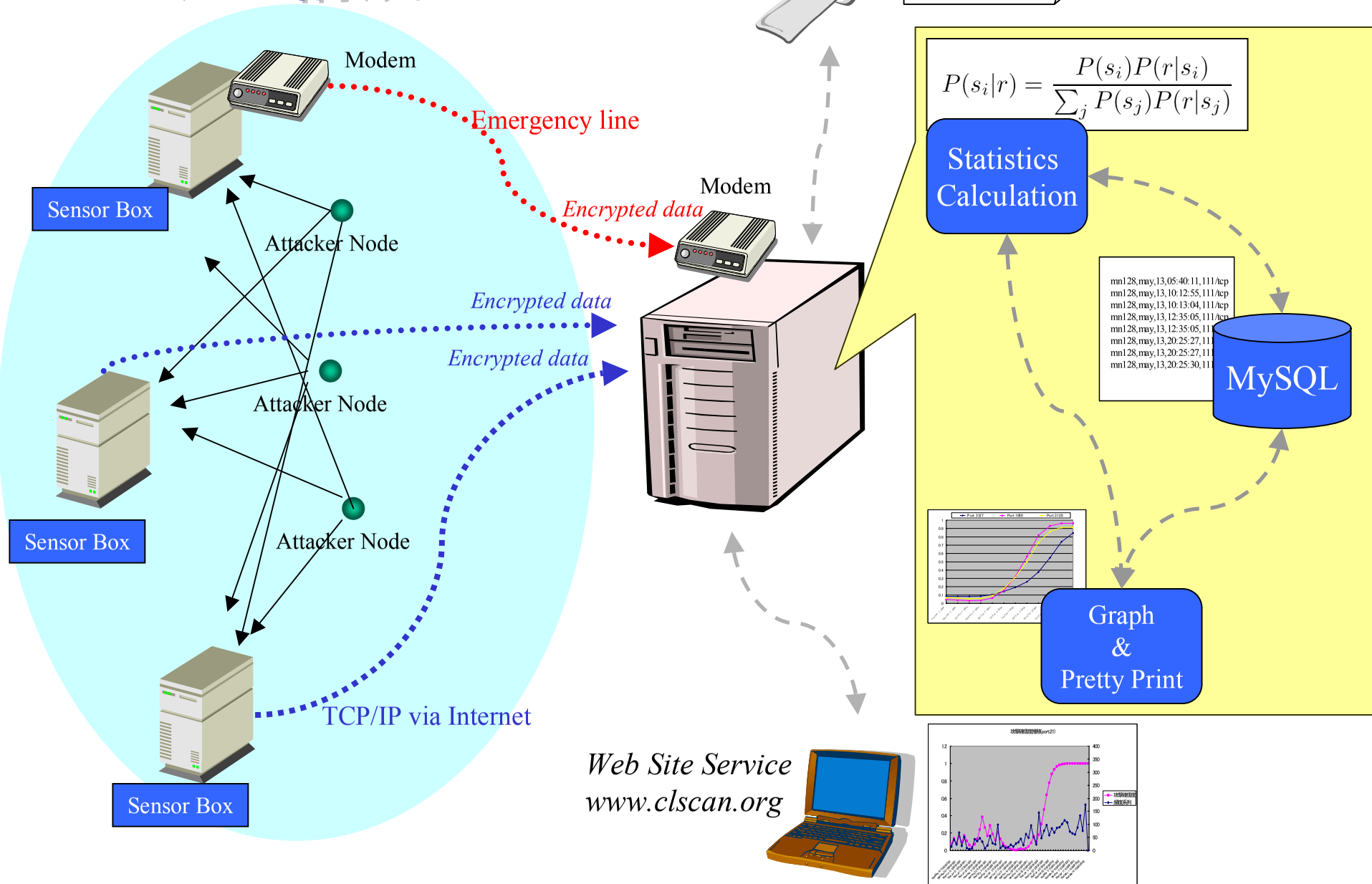
SS2001で
発表

- 広域に影響するインシデント(アタック)では攻撃IPパケットが増える
  - 単体サイトだけだと局所的な偏りがあるかも知れない⇒複数センサーでの検知が必要
- どのような攻撃が行われたかより攻撃が行われた兆候を見つけることが最優先したい
  - セキュリティ組織が警告するのと攻撃にはタイムラグがある⇒知識ベース方式では不十分
  - パケット統計を分析したら0-dayアタックらしきものを発見⇒シグニチャー方式では役にたたない

ゴール

- 24時間365日自動攻撃検知する
  - 状況を診断するような専任オペレータは不要
- 広域なインターネット上で発生している攻撃を自動的に検知する
  - “広域情報収集／データベース化／自動化分析”の3つの機能からなり独立しているので拡張が簡単
- 自動的に解析し危険度を予想する
  - ベイズ推定（推測統計学）を使い危険度を計算させるので確信度が高い
- いつでもどこでも知ることができる
  - パソコンからだけではなく携帯電話からのチェックも可能なのでいつでもどこでもチェックができる
  - デスクトップ上から常時モニタリングができる

システム構成

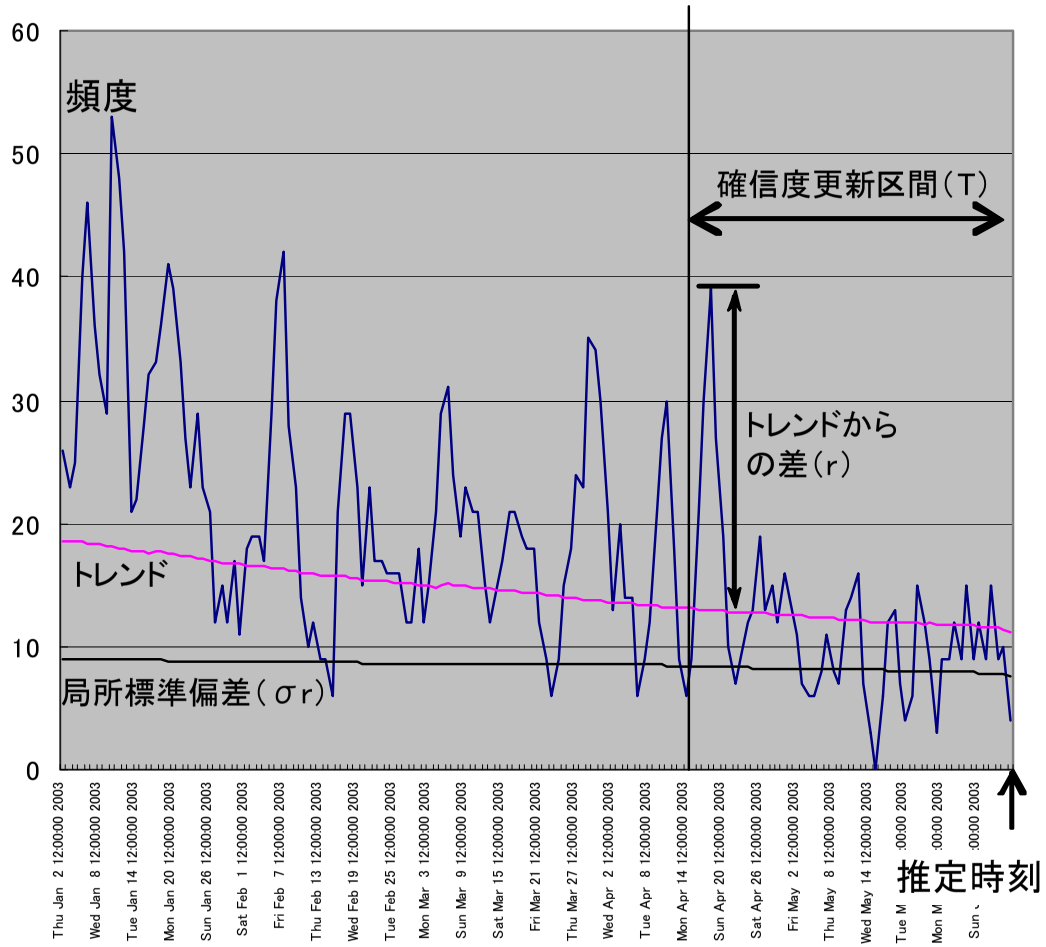

I-mode
EZweb
Alert List
Level : 1
Port:135
....
WCLSCAN
Modem
Emergency line
Sensor Box
Attacker Node
Encrypted data
Modem
Encrypted data
Encrypted data
Attacker Node
Sensor Box
Attacker Node
TCP/IP via Internet
Sensor Box
$P(s_i|r) = \frac{P(s_i)P(r|s_i)}{\sum_j P(s_j)P(r|s_j)}$
Statistics Calculation
MySQL
Graph & Pretty Print
Web Site Service
www.clscan.org

システム構成(2)

- 各々のパート部分が独立性の強いシステムなので拡張・変更が簡単
- プログラム部分の大部分がPerlで書かれている

- センサーボックスシステム
  - インターネット上に存在し到着したパケットを記録した後、集積サーバへその記録を暗号化した後に転送する
- 集積システム
  - センサーボックスから送られてくる記録を受け取り復号化した後MySQLへ格納する
- 計算システム
  - MySQLから必要なデータを取り出し危険度を計算する
- 表示作成システム
  - 計算サーバから結果を受け取り、グラフや見やすい表に加工し、メールで通知したりWebサイトへ掲載する

ベイズ推定による攻撃検知手法



事前確率　尤度関数

$$P(s_i|r) = \frac{P(s_i)P(r|s_i)}{\sum_j P(s_j)P(r|s_j)}$$

事後確率　　証拠

$$\begin{cases} s_0 & : \text{危険状態} \\ s_1 & : \text{安全状態} \end{cases}$$

r: ポートスキャン頻度の
トレンドからの差(観測)

尤度関数

$$P(r|s_0) = \frac{r}{k\sigma_r + r}$$

$$P(r|s_1) = \frac{k\sigma_r}{k\sigma_r + r}$$

石黒氏作成のSCSI2004発表スライドより

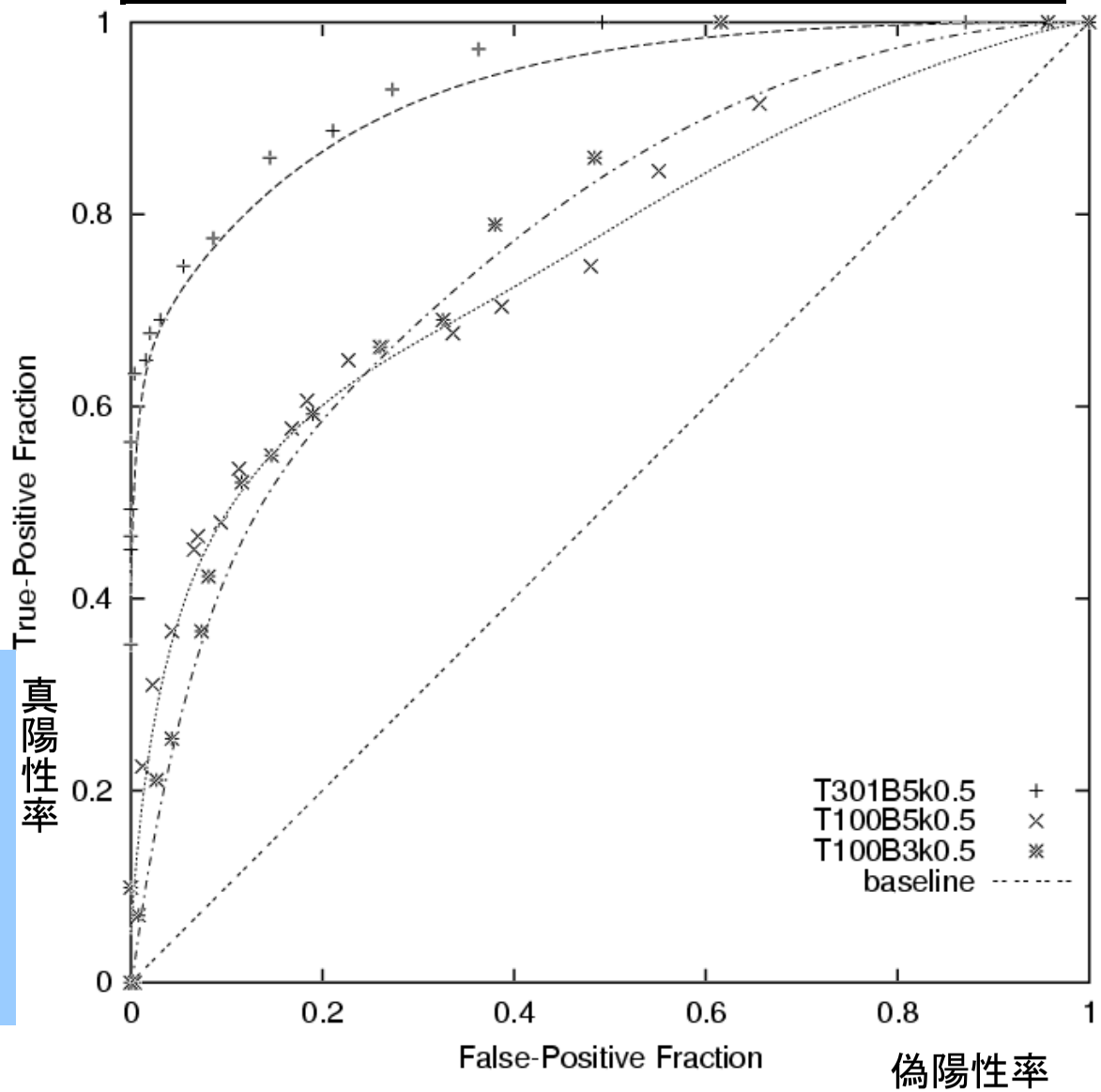
評価実験

- 期間 2003/1/1 ~ 2003/12/1
- ポート25 (smtp) ※変化がダイナミックだったため対象にしてみた
- サイト数　1 ※先行してセンサー単独で動かしていた
- ベイズ推定の結果に対し正しい(真陽性率)と誤り(偽陽性率)のROC (receiver operating characteristic)曲線を作成
- 同じデータで「ベイズ更新区間」「トレンド区間」のパラメータを変化をさせてみた

- y=xよりもROC曲線は上方であるので、有効に危険状態を判別できている
- トレンド区間が大きいほうが精度が出る
- 同じトレンド区間なら更新区間が小さいほうが精度が出る
- 良いパラメータの選び方は職人芸の世界だった！？

石黒によるROC曲線作成結果より

グラフID	ベイズ更新偏差係	ベイズ更新区間	トレンド区間	Az値
T301B5k0	0.5	5	301	0.95
T100B5k0	0.5	5	100	0.79
T100B3k0	0.5	3	100	0.8

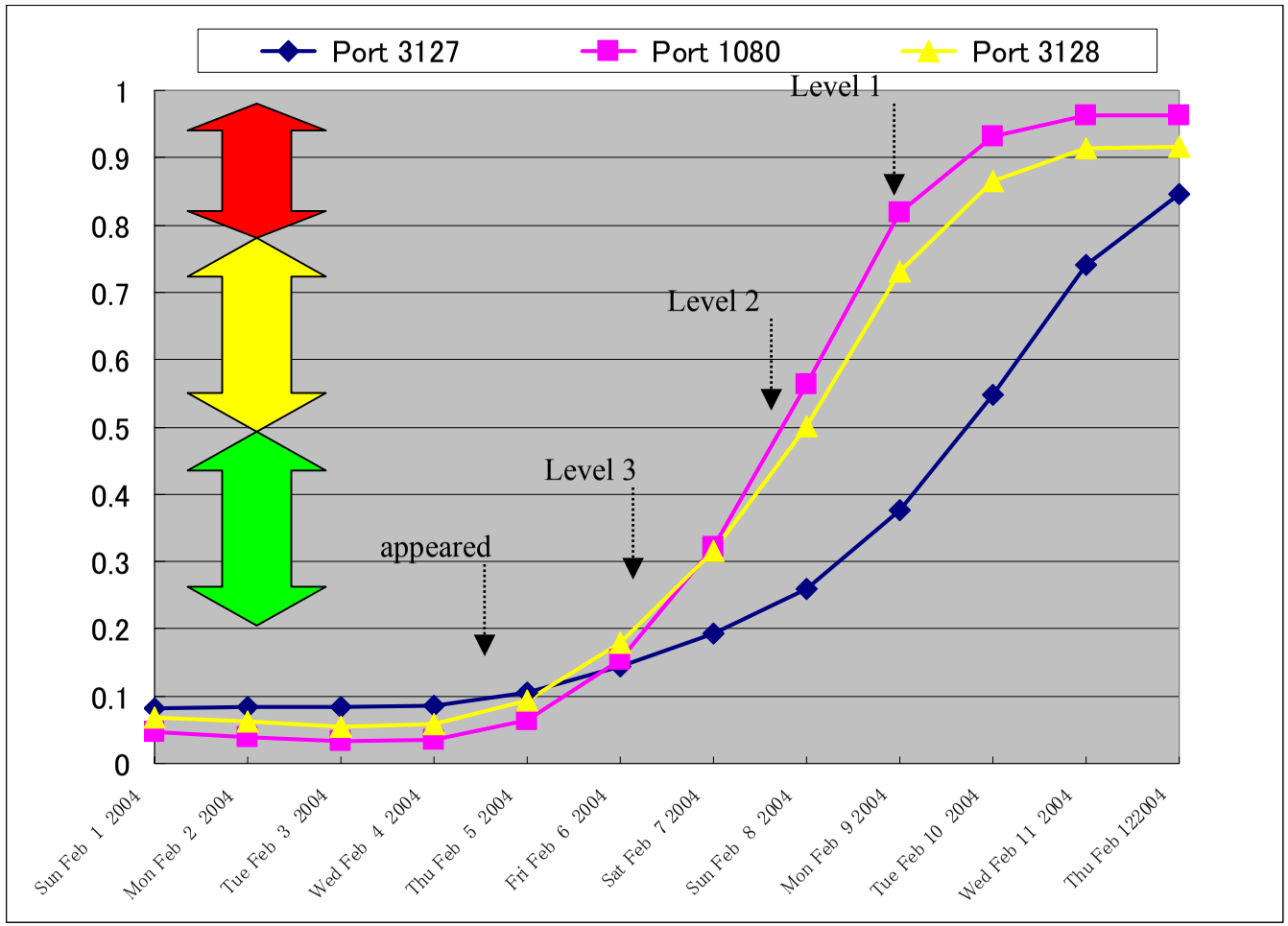


Doomjuiceケース

まったく新しい攻撃が発生した場合

- 2004/2/7 (昼ごろ)レベル3に見たことのないポートへのアクセスが増加したとあった
- 2004/2/7 (午後4時) IWR研究者間メーリングリストへMydoomバックドア狙いのポートスキャンが増えていることを報告
- 2004/2/9(日本時間)ウィルスベンダによるアナウンス
- 2004/2/10 (日本時間)メディアによるアナウンス
- 2004/2/11 @pliceによる注意喚起掲示

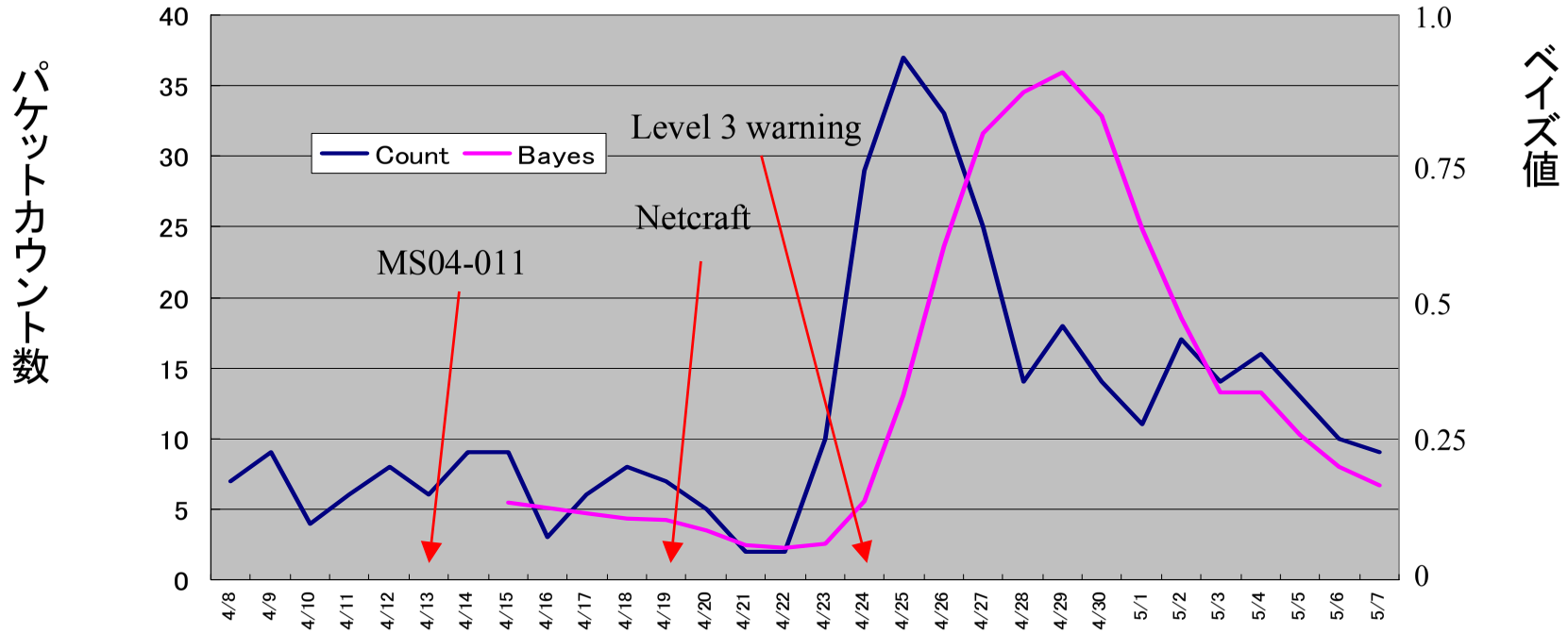
Graph of Bayesian Estimation Curve



Time Zone is JST

Detected activity of “Doomjuice”

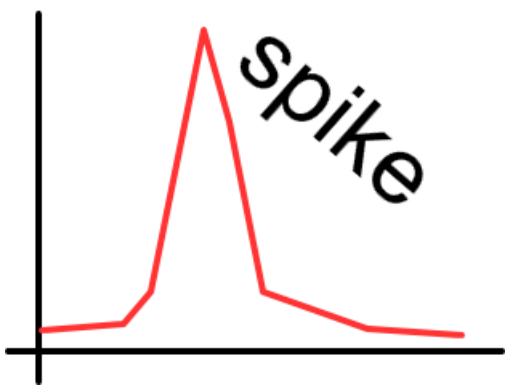
SSL BOMBケース たぶん来るだろうと待ち構えていた場合

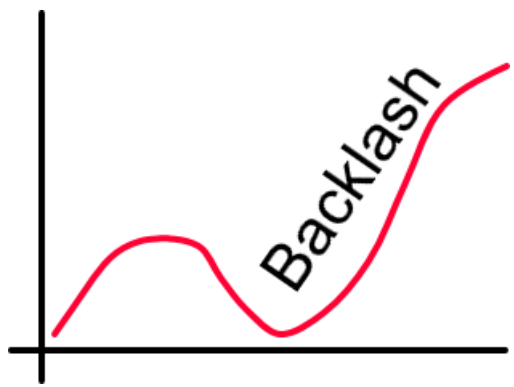


- SSL BOMB --- MS-IISへのDoSアタック
  - 2004/4/13 MS04-011でTCP/SSLの脆弱性を公表
  - 2004/4/19 Netcraftがexploitコードが公表されていると警告
  - 2004/4/24 IWRでlevel 3にリストアップされる
    - 予想通りの攻撃をセンサーが捕らえた

ベイズ推定の癖

- Spike effect
  - 一部センサーにスパイクが観測されたとき、それが全体の総数をひっぱってしまい、影響が後々まで出てしまう
- Backlash effect
  - 一度ベイズ値が上昇した後に減少した状態からは、ベイズ値の上昇が早い





一般ユーザの利用方法

- Web Brower from PC/PDA
  - www.clscan.org
- I-mode (NTT DoCoMo)
  - www.clscan.org/iwr/i.html
- Ezweb (KDDI)
  - www.clscan.org/iwr/ez.hdml

携帯電話の
画面イメージ

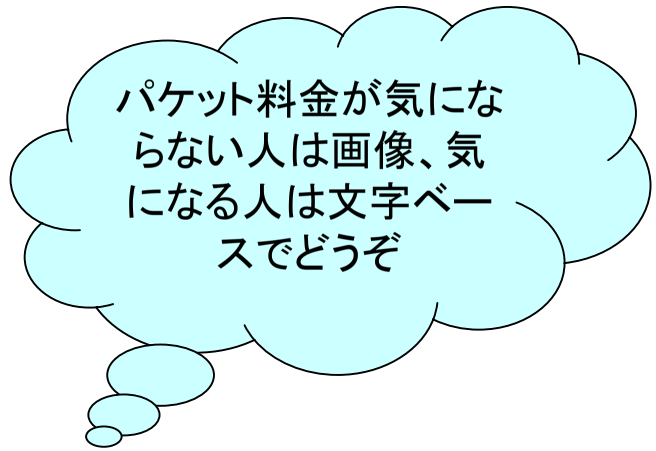
```
2004/2/19 19:31
IWR:
L P      B    C
1 80     0.88 117
1 135    0.84 287
2 901    0.69 9
2 443    0.50 2
3 1080   0.50 128
3 3128   0.49 130
3 12345  0.45 4
3 3127   0.42 209
```

- ほとんど場合、携帯電話からのチェックで十分
- レベル1発生時に携帯へメール通知する機能は“ウザイ(煩わしい)”ので中止

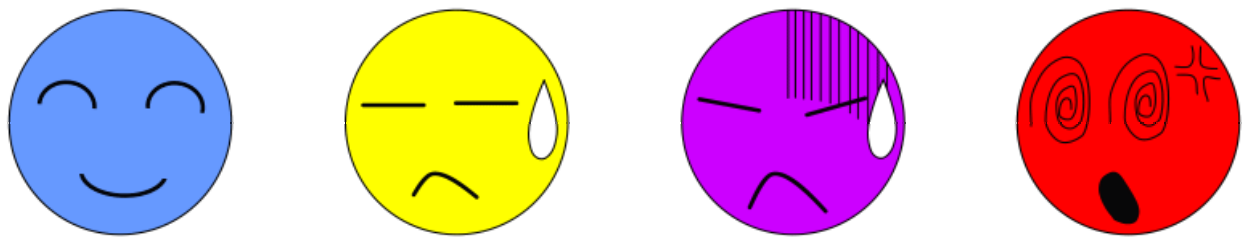
一般ユーザの利用方法

Update!

- Facial indicator
  - GNOME アプレットを開発
    - デスクトップ上から常時モニタ
  - Webサイト上のアイコン
    - パソコン上から
    - 携帯電話から



Smiley　Uneasy　Distress　Panic



(^_^)v　(-_-;)　(-_-T)　(@o@#)

今後の課題

- 基本システム作成及び評価終了しセンサー設置台数の拡大へ
  - データとして意味のあるものを検知するために独立した専用センサマシンを配置中（現在４台）
- データベースに格納されているログを使ってさらに色々な分析を検討中
  - www.sco.comへのDoSアタックの痕跡をみつけることもできた
- 本プロジェクト参加間でのコミュニケーション
  - 独立行政法人（１）、大学（２）、企業（３）が本プロジェクトに参加

まとめ

- インターネット早期広域攻撃警戒システムの開発と運用を行っている
- ベイズ推定による危険度を計算し、その結果を一般に公開している
- パソコンからだけではなく、携帯電話からも確認できる
- 評価実験では有効であることが確認され、実際のケース紹介のように役に立っている
- さらに充実したシステムにするために現在活動中
  - 共同研究提案Welcomeです！！

デモ

http://www.clscan.org