

# ベイズ推定に基づくインターネット攻撃検知システムの開発

---

電子情報通信学会  
暗号と情報セキュリティシンポジウム SCIS 2004

2004年1月27～30日

石黒 正揮<sup>\*1)</sup>   鈴木 裕信<sup>\*2)</sup>   村瀬 一郎<sup>\*1)</sup>   大野 浩之<sup>\*3)</sup>

<sup>\*1)</sup>株式会社三菱総合研究所  
情報技術研究部

<sup>\*2)</sup>鈴木裕信事務所

<sup>\*3)</sup>独立行政法人通信総合研究所  
非常時通信グループ

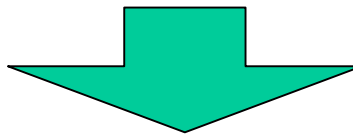
# 発表の概要

---

- 背景と目的
- インターネット攻撃検知システムの概要
- 攻撃検知手法
- 評価実験
- まとめと今後の課題

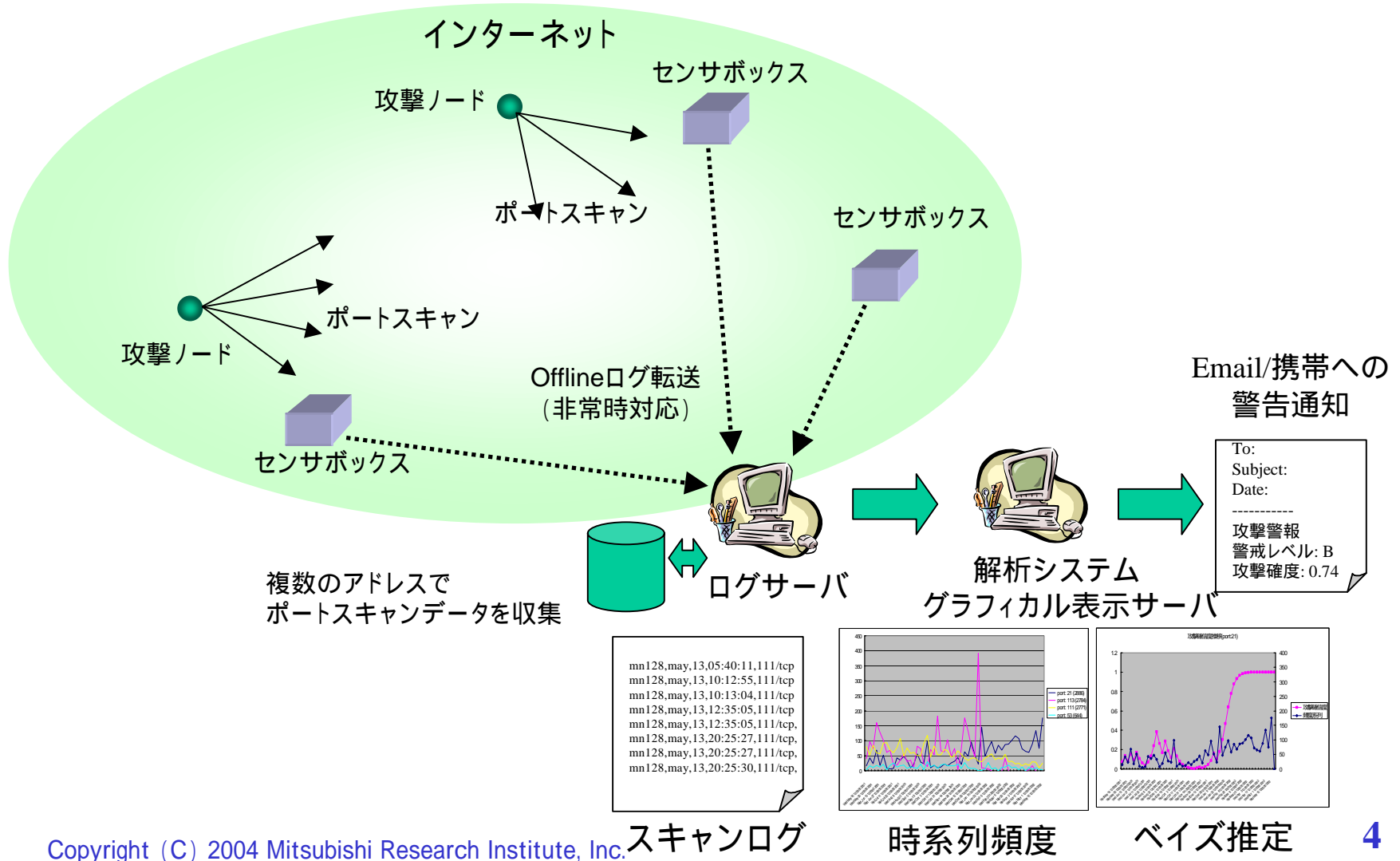
## 背景と目的

- ワーム、自動攻撃ツールなどを用いた攻撃の増加
  - ➔ コンピュータシステムの大規模な被害の発生
- 不正アクセス検出システム(IDS)の開発・稼動は多数
  - ➔ IDSは不正侵入の形跡から検出を行うため先行対応には不十分
- 脆弱性情報に基づく対策意識の高まり
  - ➔ 脆弱性の発見から攻撃の活発化までの時間が短くなり、脆弱性対策の遅れによる被害の拡大傾向
- InternetStormCenter等のアクセスログに基づく警戒情報発信
  - ➔ 人手による分析のため、検出の常時リアルタイム性に欠ける。

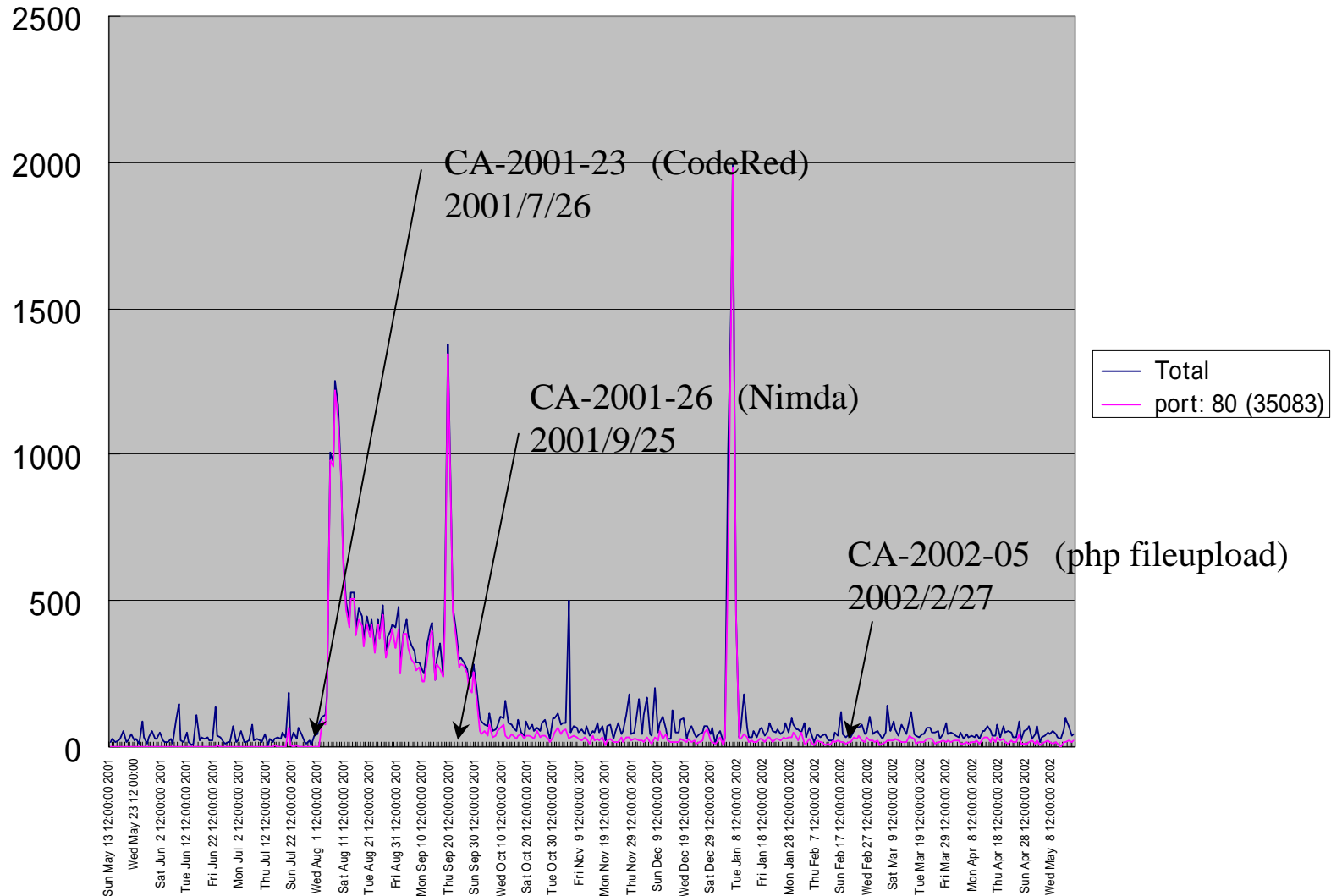


- インターネットの危険度を24時間無人監視する警報システムの提案
  - 周囲のIPアドレスに対するポートスキャン動向を観測
  - アクセスデータの特異性からインターネットの危険度を自動検出
  - 24時間常時無人監視による警報通知

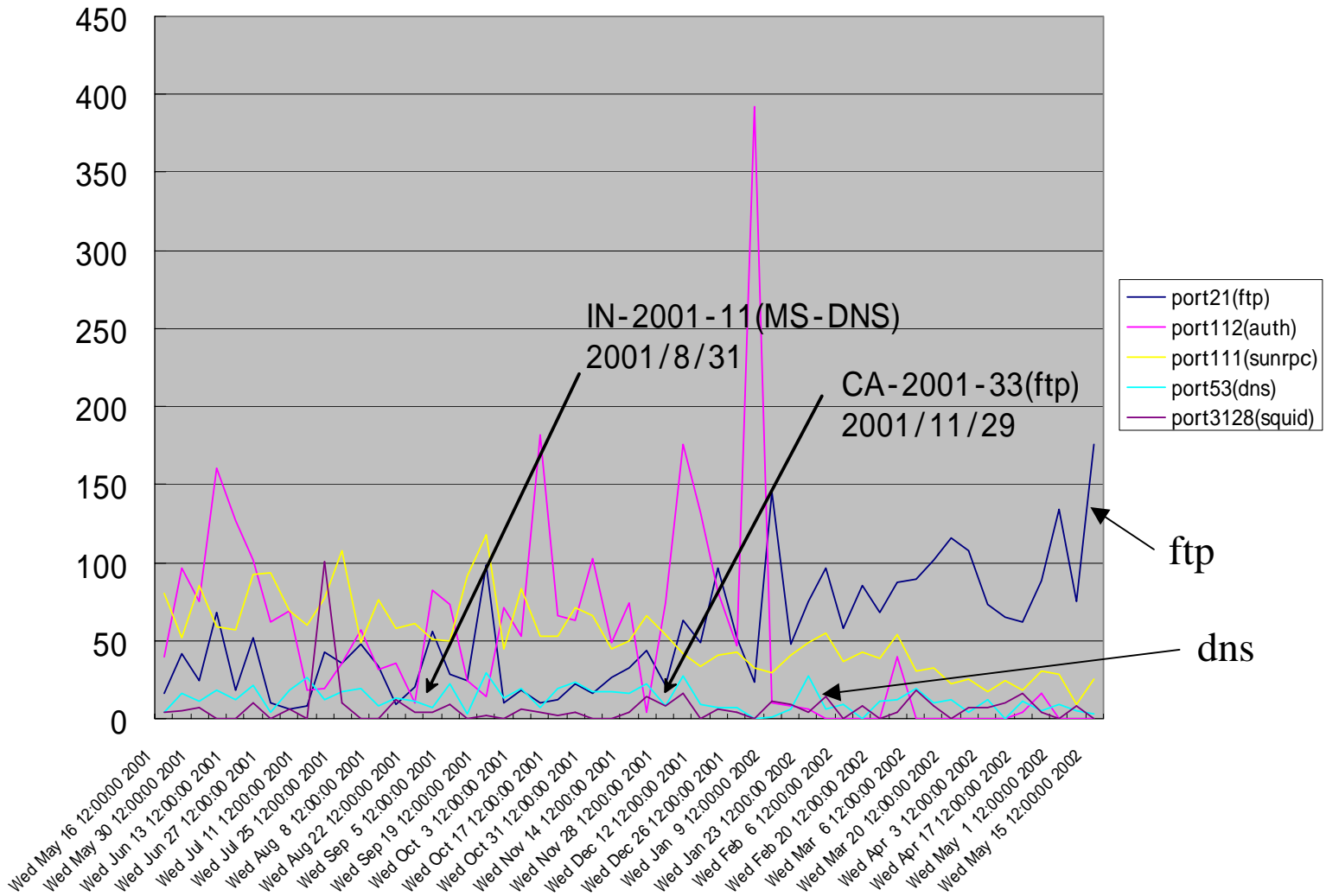
# インターネット攻撃検知システムの概要



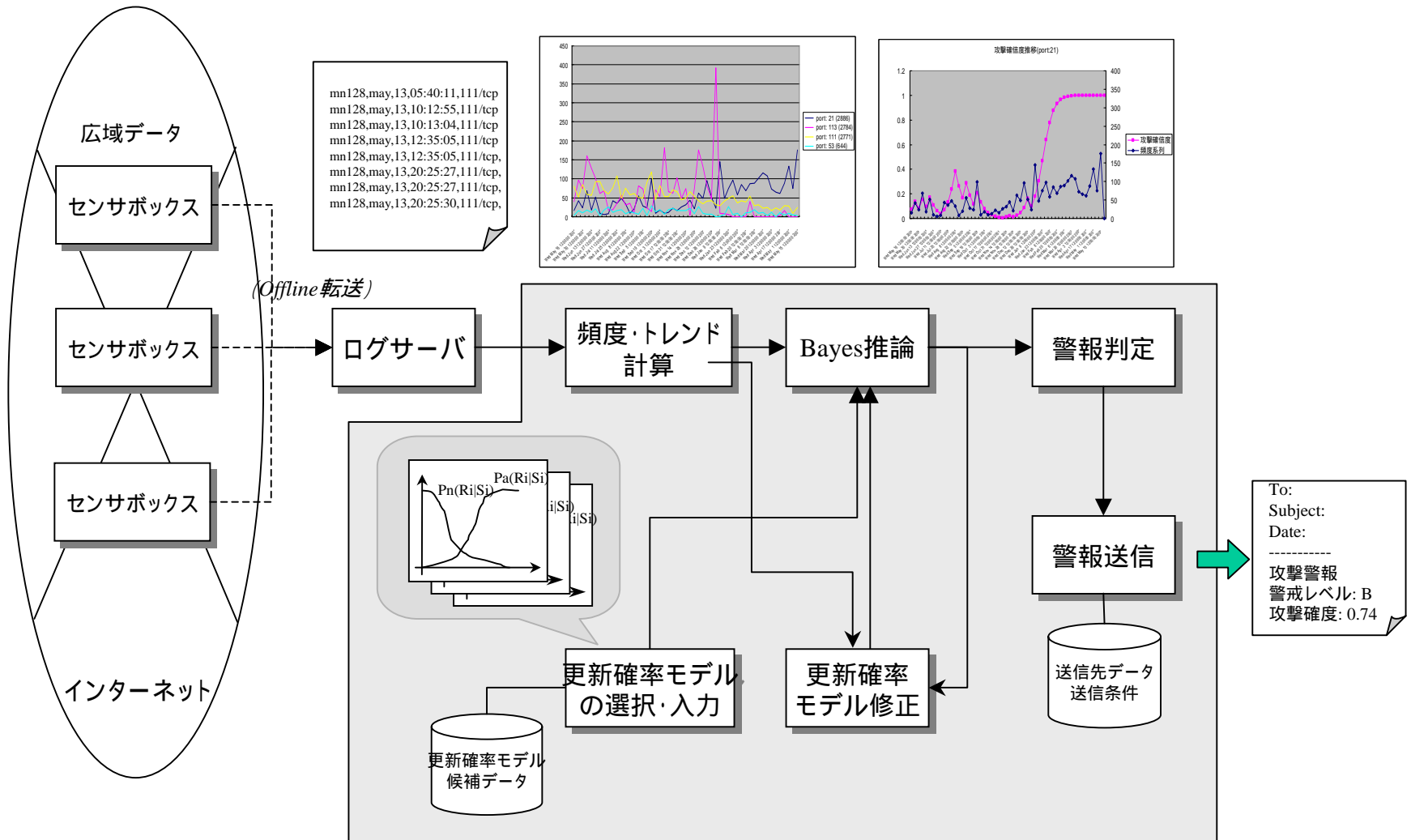
# ポートスキャン頻度の推移とインシデントとの関係(事例1)



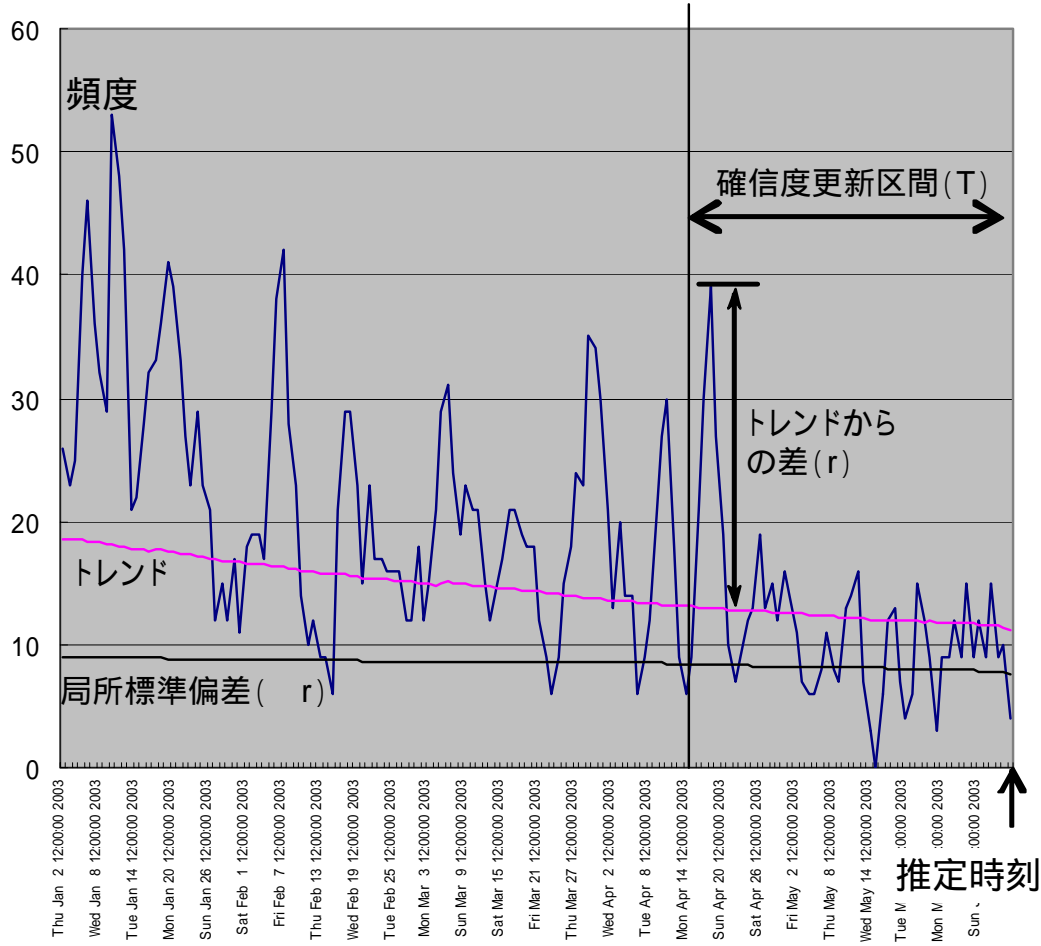
# ポートスキャンの推移とインシデントとの関係(事例2)



# 攻撃検知システムの構成



# 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

- $s_0$  : 危険状態
- $s_1$  : 安全状態

$r$ : ポートスキャン頻度の  
トレンドからの差(観測)

尤度関数

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

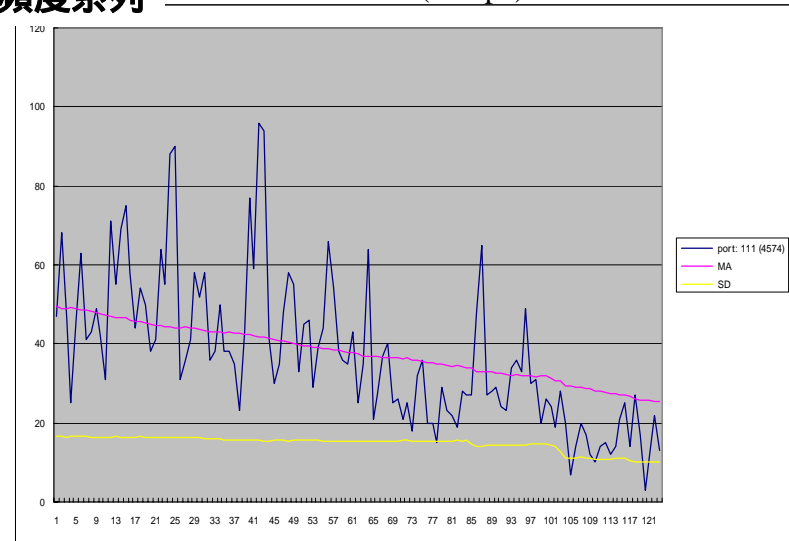
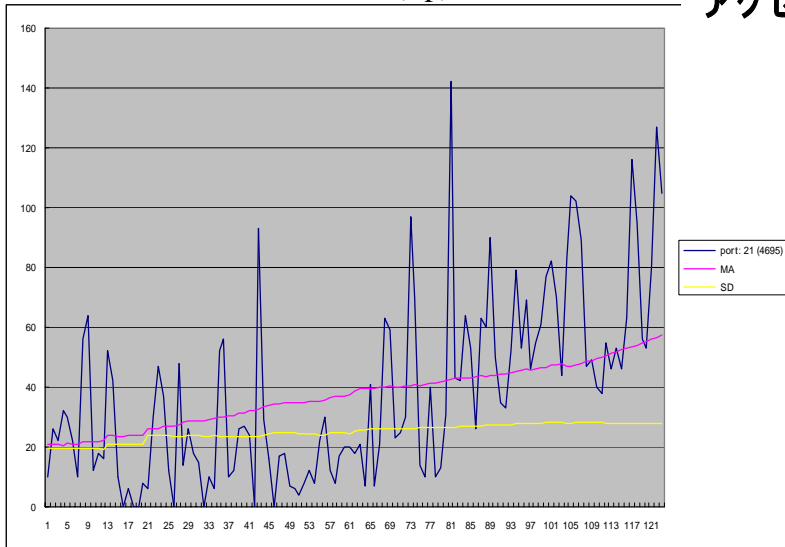
$$P(r|s_1) = \frac{k\sigma_r}{k\sigma_r + r}$$

# 実験1

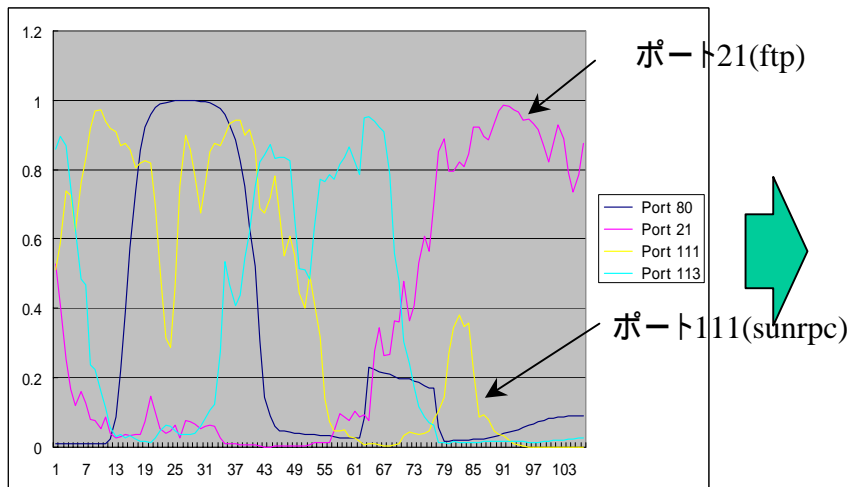
ポート21(ftp)

アクセス頻度系列

ポート111(sunrpc)



危険度推移



警報情報

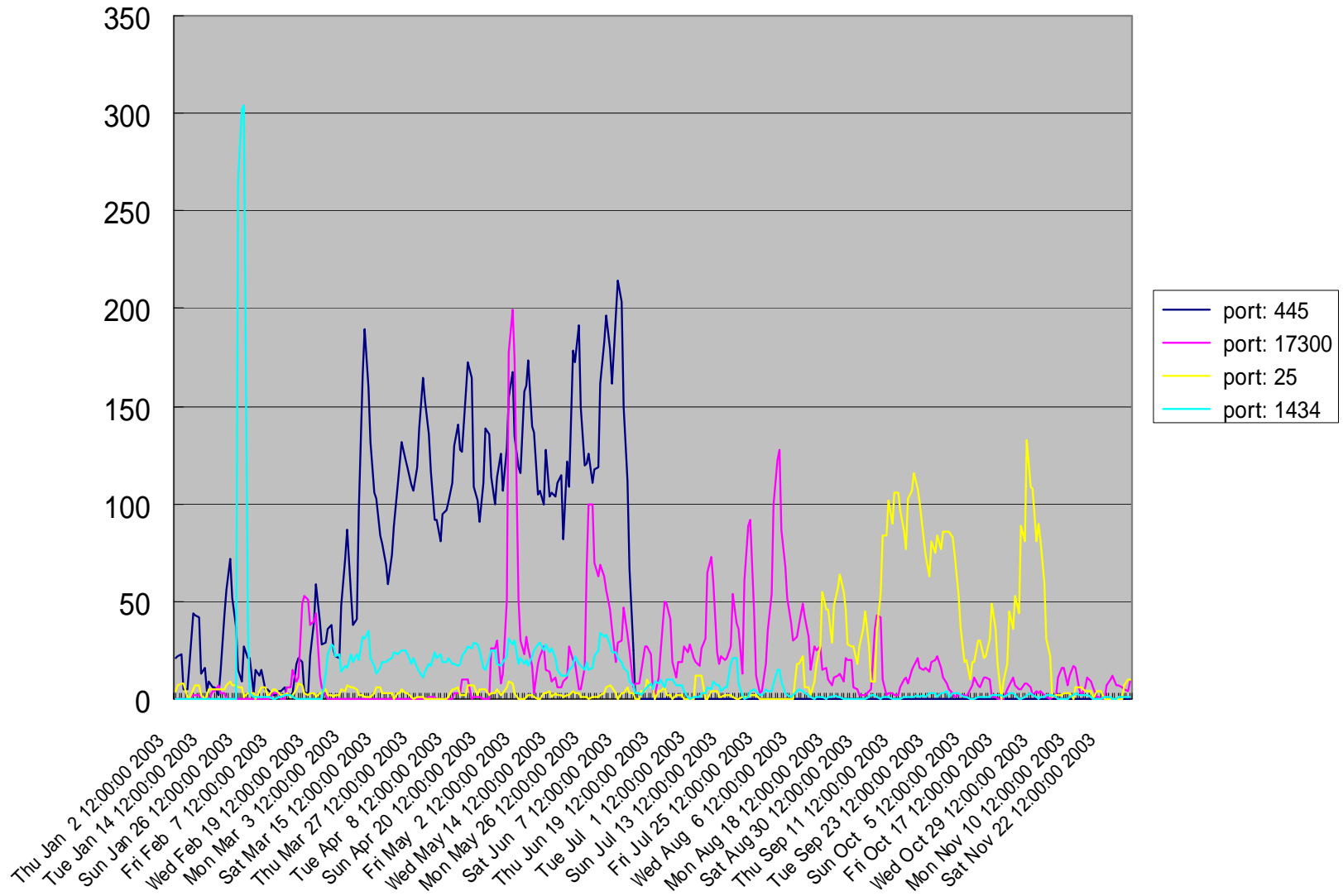
**Port No.: 21**  
**Warning Level: Severe (Level 2)**  
**Bayes Confidence: 0.8741**  
**Latest Access Amount: 105**  
**Latest Moving Average: 57.2**  
**Latest Standard Deviation: 27.8**  
**(Latest Term: [Tue May 14 00:00:00 2002**  
**-- Sun May 19 00:00:00 2002])**

## 実験2 (ROC分析)

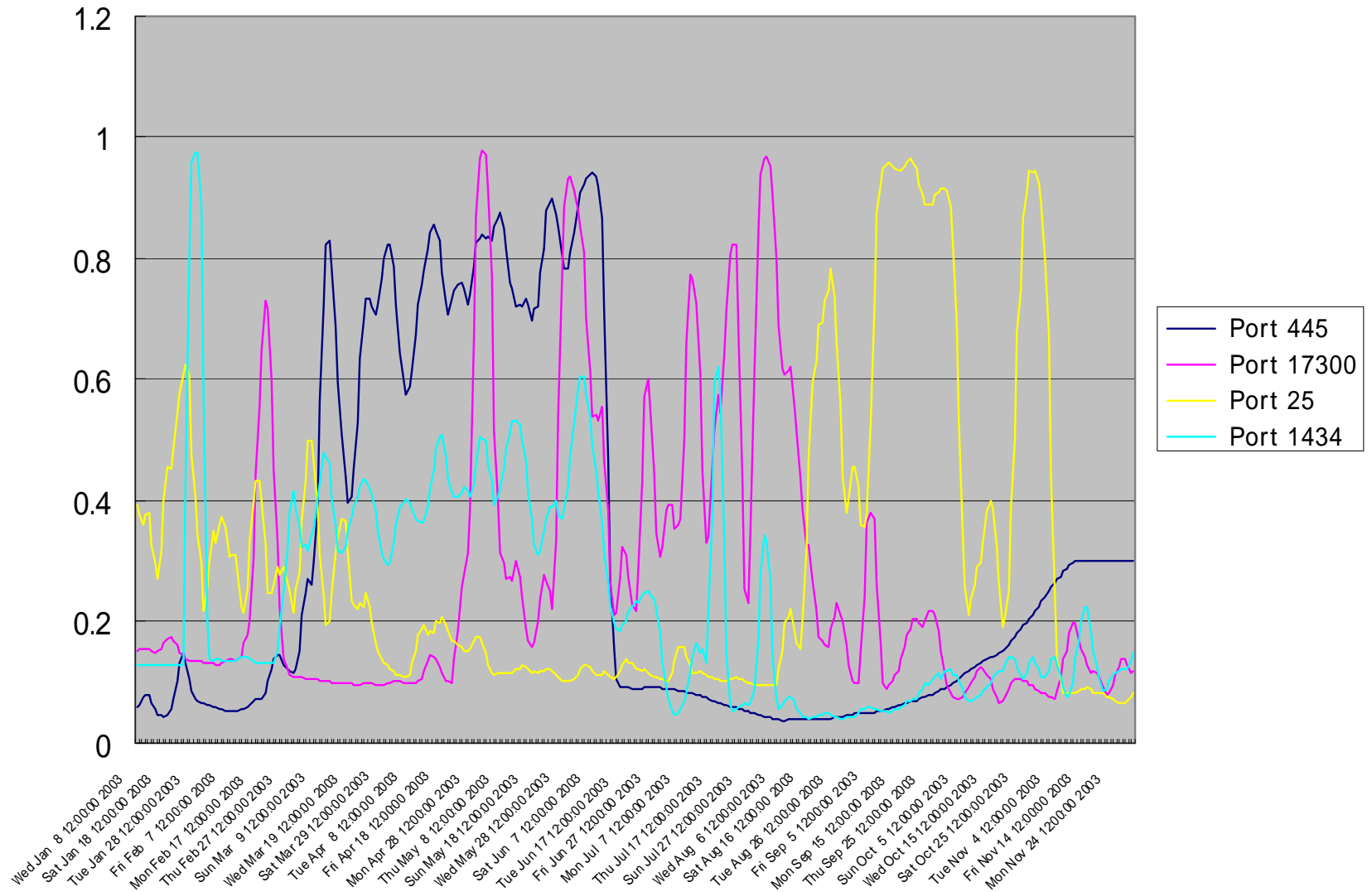
---

- 対象データ: 2003年1月1日 ~ 2003年12月1日
- JPCERTの注意喚起の例
  - **ポート80** は httpサーバで使用され、2003年3月18日に ``Microsoft IIS 5.0 の脆弱性に関する注意喚起"(JPCERT-AT-2003-0003)
  - **ポート135**は、Windows RPCサービスで使用されるもので、2003年8月15日に、**W32/Blaster** **ワーム**によって大規模な被害を生じた ``TCP 135番ポートへのスキャンの増加に関する注意喚起"(JPCERT-AT-2003-0006)
  - **ポート25**は、メールサーバで使用されるもので、2003年3月31日に ``新たな **sendmail** の脆弱性に関する注意喚起"(JPCERT-AT-2003-0004)
  - **ポート1434**は、**Microsoft SQL Server 2000**で使用されるもので、2003年1月27日に ``UDP1434番ポートへのスキャンの増加に関する注意喚起"(JPCERT-AT-2003-01-27)

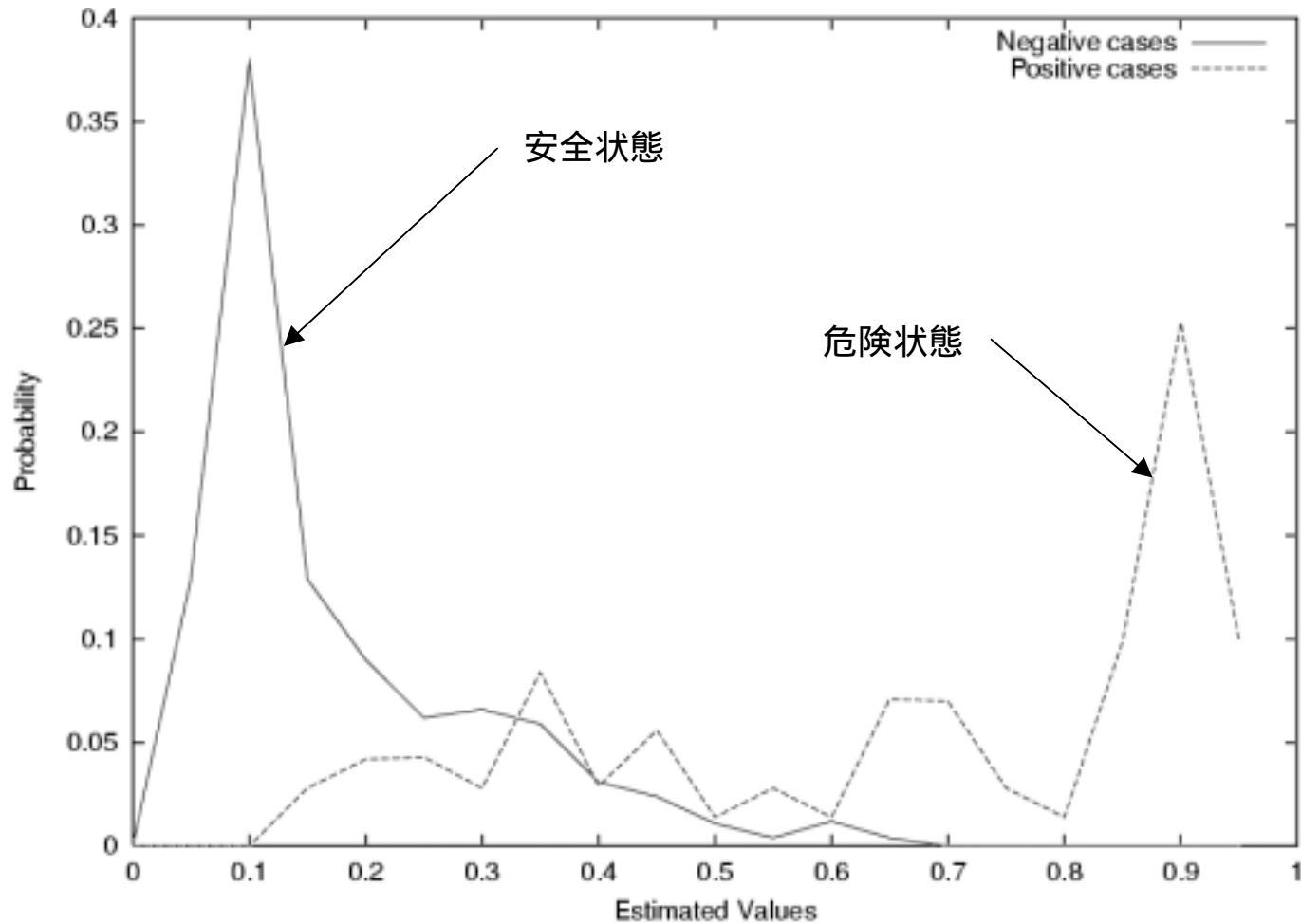
# ポートスキャン頻度の時系列推移



# 危険度推定値の推移

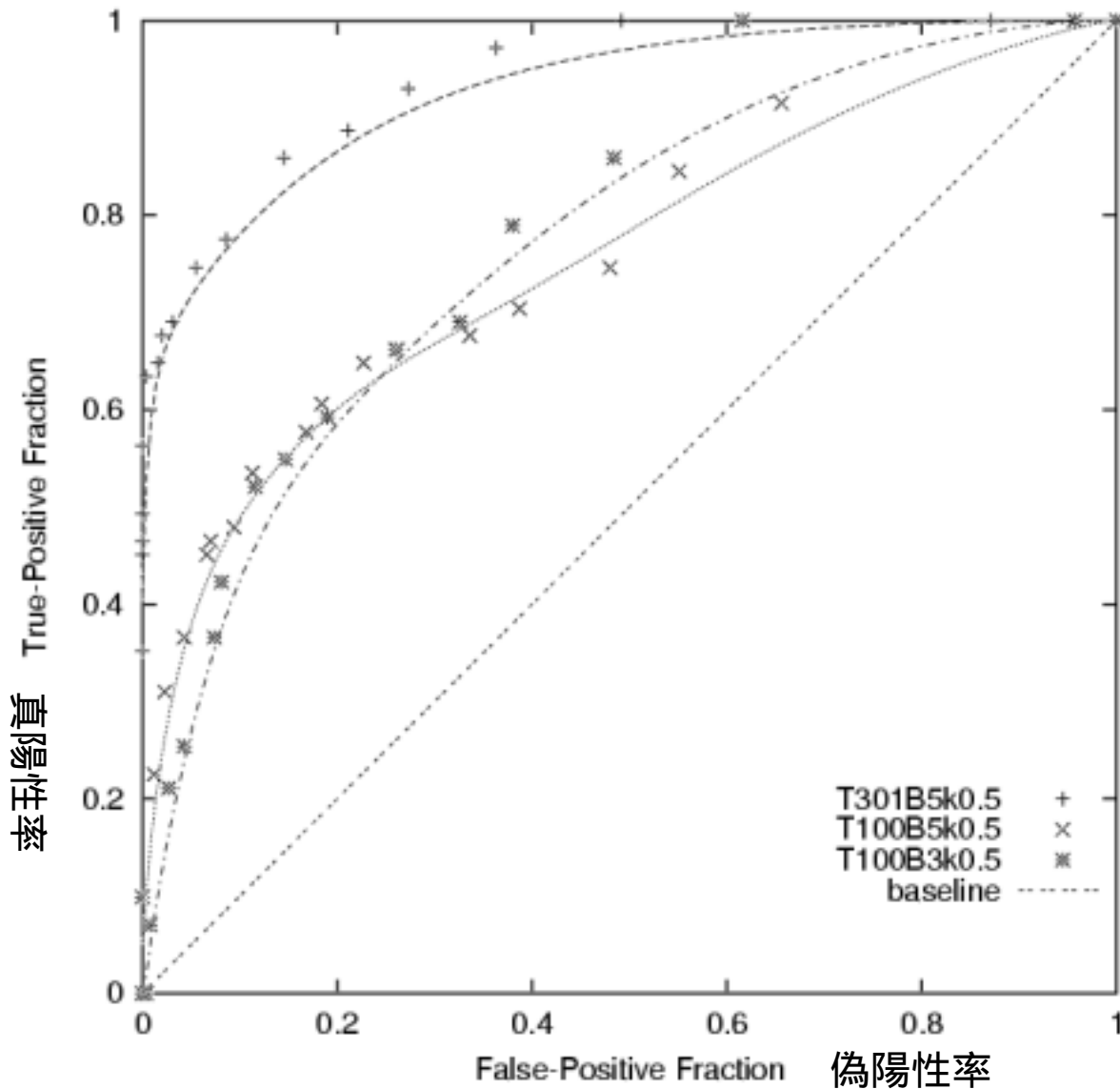


# 状態区別のベイズ推定値分布



ポート25に関して、目視による危険状態真偽に対する自動検知のベイズ推定値の分布

## ROC曲線



グラフID	ベイズ更新 新偏差係	ベイズ更新 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

# まとめと今後の課題

---

## まとめ

- ポートスキャン頻度の時系列変化を観測し、ベイズ推定に基づきネットワーク攻撃の危険度を推定するシステムを開発
- 24時間常時無人監視による警報システムを稼動
- 実データによるROC分析により、性能を比較

## 今後の課題

- 多地点の観測データを用いることによる推定精度の向上
- 地点間、ポート間の変動差、相関を利用した攻撃検出
- 警報通知法の検討

# 参考情報

- WCLSCANホームページ

www.clscan.org

- 分析

www.clscan.org/iwr/iwr.html

- グラフ

www.clscan.org/iwr/g.html

- i-mode

www.clscan.org/iwr/i.html

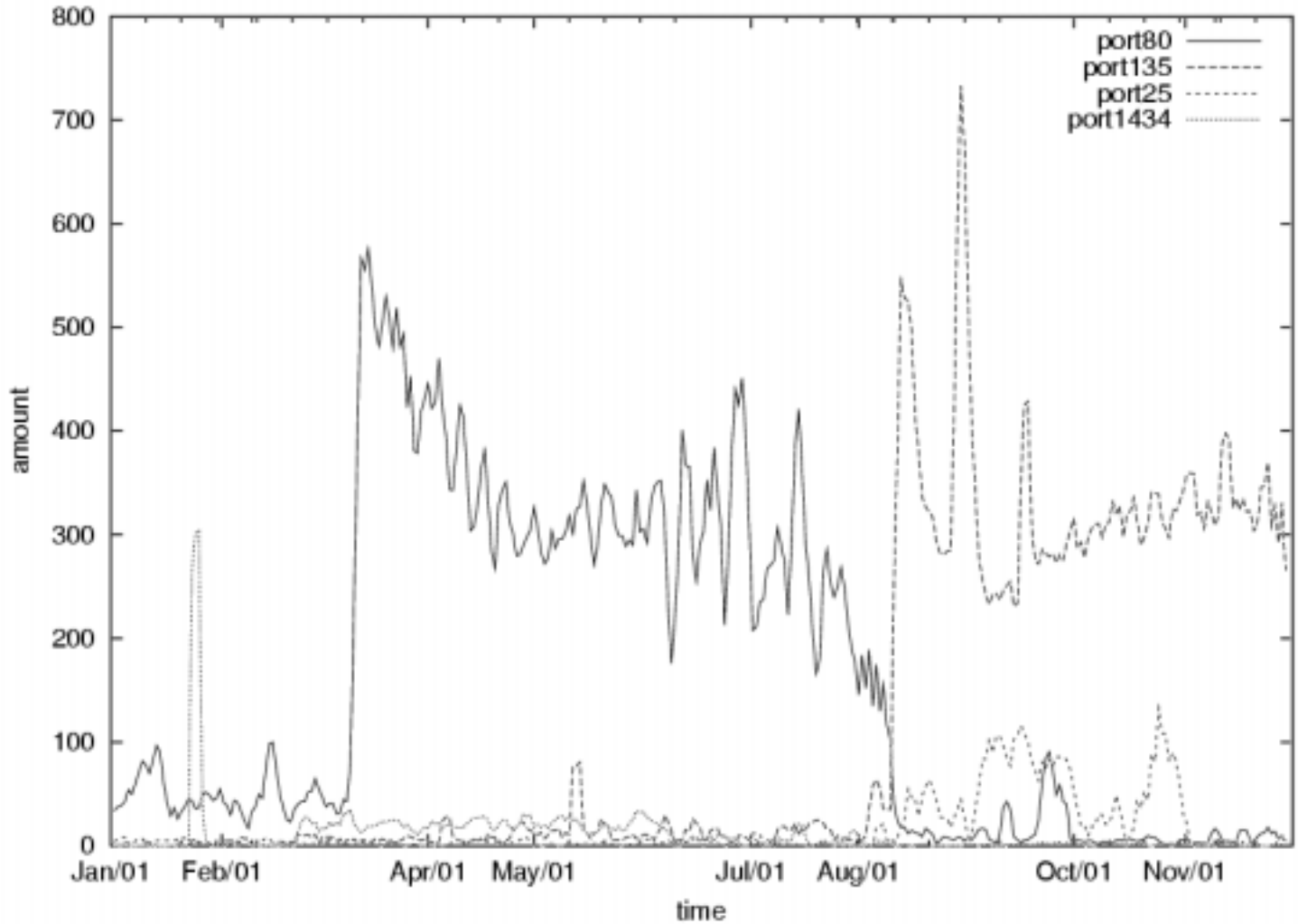
- Ez web

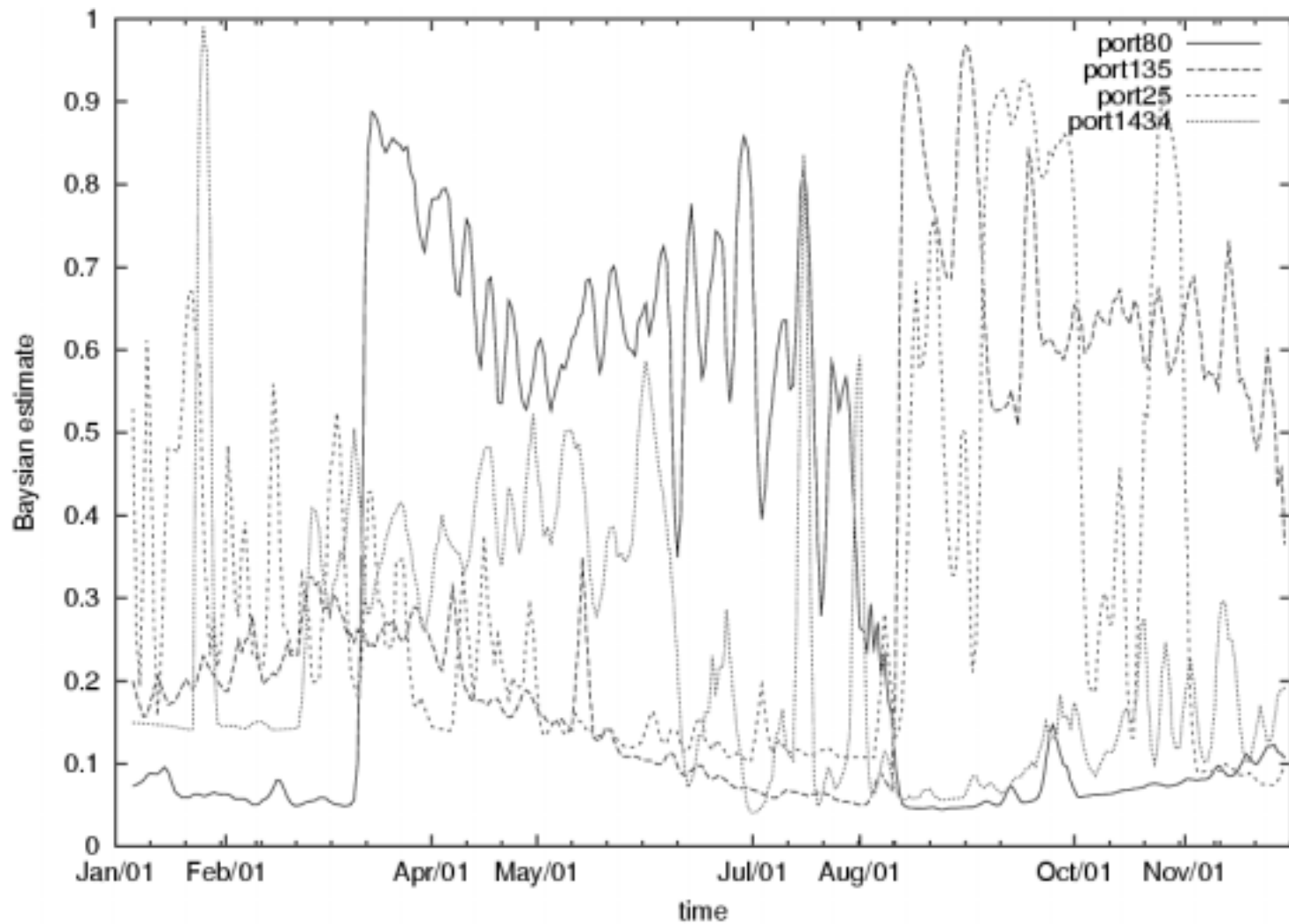
www.clscan.org/iwr/ez.html





以上



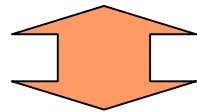


## 一般的な不正アクセス検出との比較

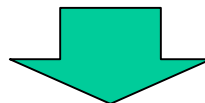
- ホスト型IDS ... ホスト上の各種サーバのログを解析
- ネットワーク型IDS ... LAN内のトラフィックを解析



実際に侵入を受けた場合しか検出の対象となり得ない



- 本手法: 周囲のポートスキャン頻度の活発化などの変化の特異性からインターネットの広域的な危険度の変化を検知



周囲の観察から、自サイトへの攻撃を事前に警戒できる