インターネット広域観測による次世代攻撃検知技術に関する研究開発(051103017)

2008年6月11日

戦略的情報通信研究開発推進制度（SCOPE）成果発表会

研究代表者

後藤 滋樹　早稲田大学 理工学術院 基幹理工学部 情報理工学科

研究分担者

村瀬　一郎　　鈴木　裕信†

早稲田大学 理工学研究所

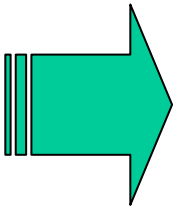
発表内容

1. 背景と目的
2. インターネット定点観測システムの概要
   - センサー配置
   - インシデントの例と不正パケット数の関係
3. インターネット脅威分析手法に関する動向
4. 本研究開発の成果
   - 不正パケットの周期性の存在確認
   - 本手法の基本アイデア
   - 分析適用例
   - 公開ホームページ
5. まとめ

背景と目的

- インターネット上における広域な攻撃には、悪意のある個人やグループによるツールを用いた攻撃だけではなく、ワーム・ウィルスの感染など人間が介在しない攻撃がある。
- 感染・侵入台数をより多くするためにインターネット上に接続されているコンピュータに対し無差別的に攻撃を試みる。
- インターネット上の攻撃は、初期の健在型の愉快犯から、プロフェッショナル化が進み、さらにボットなど遠隔操作による攻撃の高度化が進む。
- インターネット上には、異なる特徴、振舞いを持つ攻撃が同時多発的に存在している。
- インターネット上の不正なパケットを広く観測し振る舞いを分析すると、自サイトのみ観測できないインターネット上の脅威を検知することができる。

不正パケット数の量や増減といった単純に量として比較



より高度な分析方法を開発し適用する

システムの特徴：多様なデータ収集・多様な分析能力

高度な分析

- ベイズ推定
- 頻度分布偏差スコア
- ポート間相関分析
- ウェーブレット解析
- 自己相関分析
- グラフ構造分析

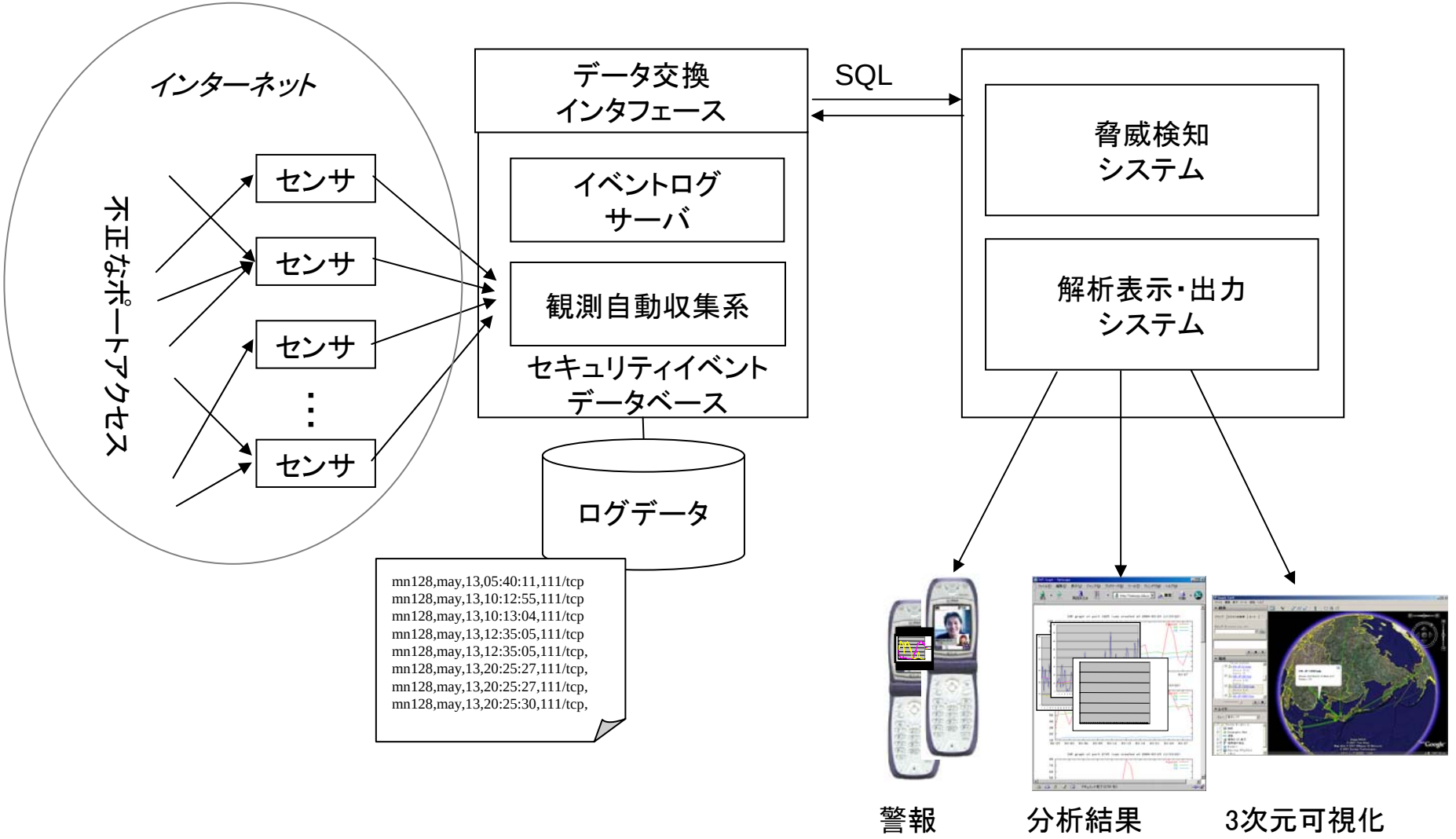
収集先

- 国内ISP
- 国内研究ネットワーク
- 海外研究ネットワーク
- 海外ISP

24/365日稼動

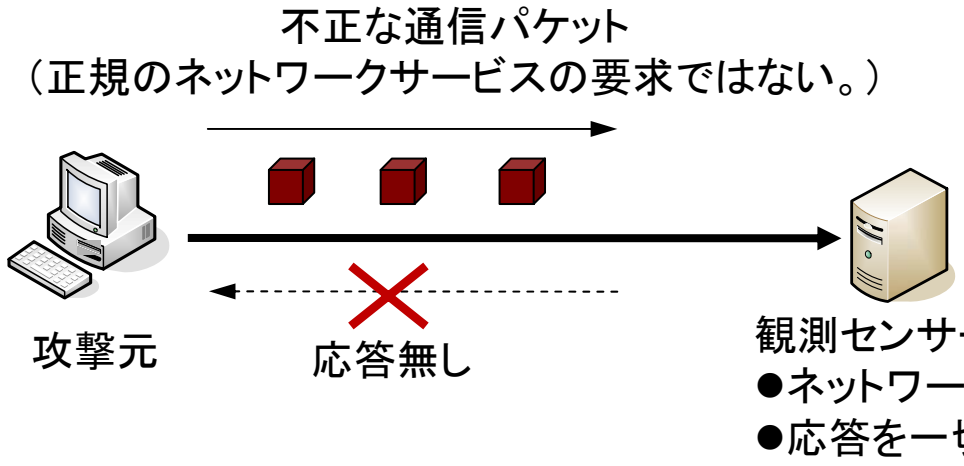
- データ管理システム
- センサーボックス

インターネット定点観測システムの概要

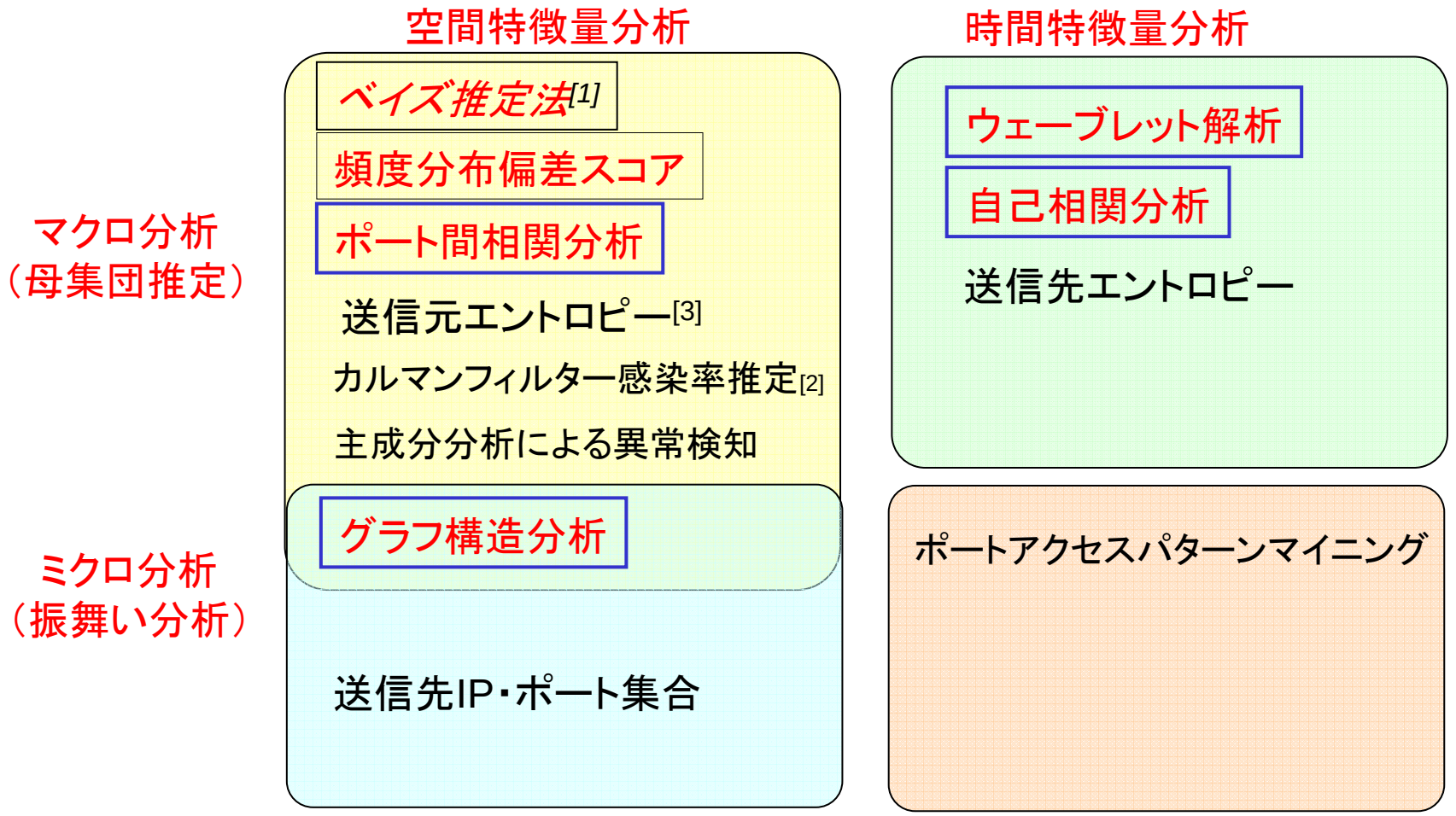


不正パケットの観測センサー

・　受動観測型センサー（Dark IP）



インターネット脅威分析手法の分類体系



青いボックスは本研究開発により加わった能力

[1] Masaki Ishiguro et al, Internet Threat Detection System Using Bayesian Estimation, 16th Annual FIRST Conference on Computer Security Incident Handling, 2004

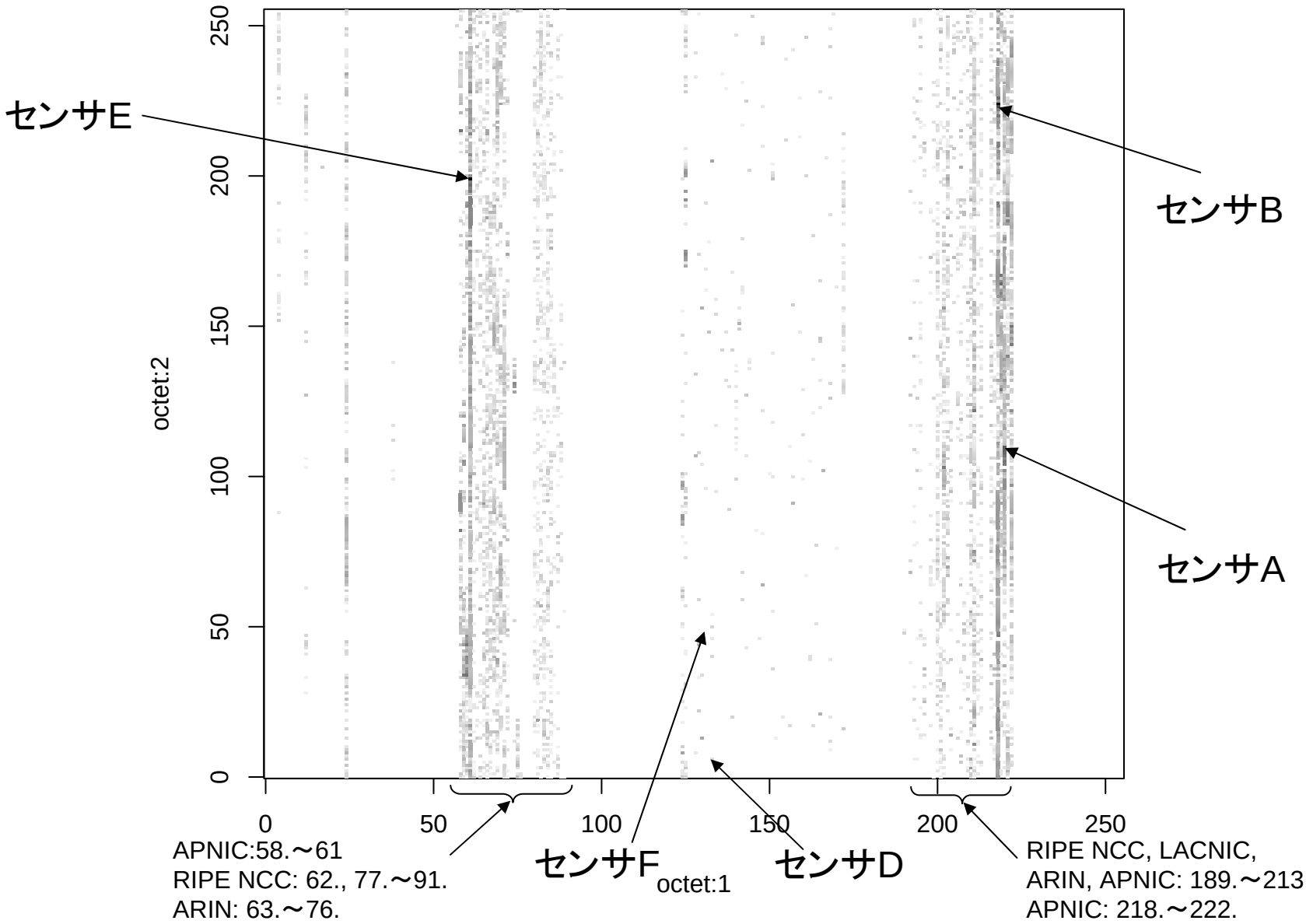
[2] C. Zou et al,"The monitoring and early detection of internet worms",IEEE/ACM Transaction on Networking,

[3] Arno Wagner , Entropy Based Worm and Anomaly Detection in Fast IP Networks,14th IEEE International Workshop on Enabling Technologies

本研究開発における成果

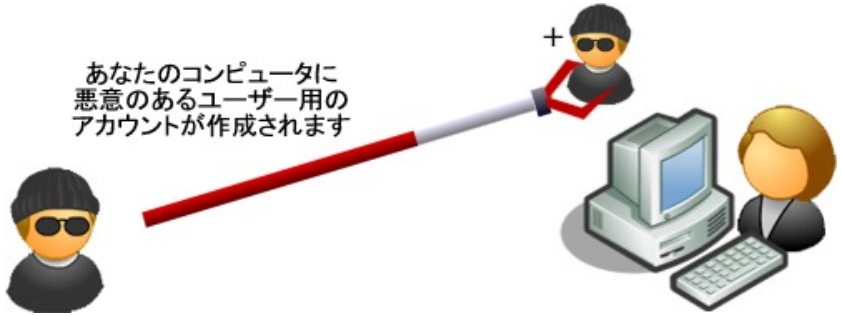
計測系

観測センサーと不正パケット送信元分布



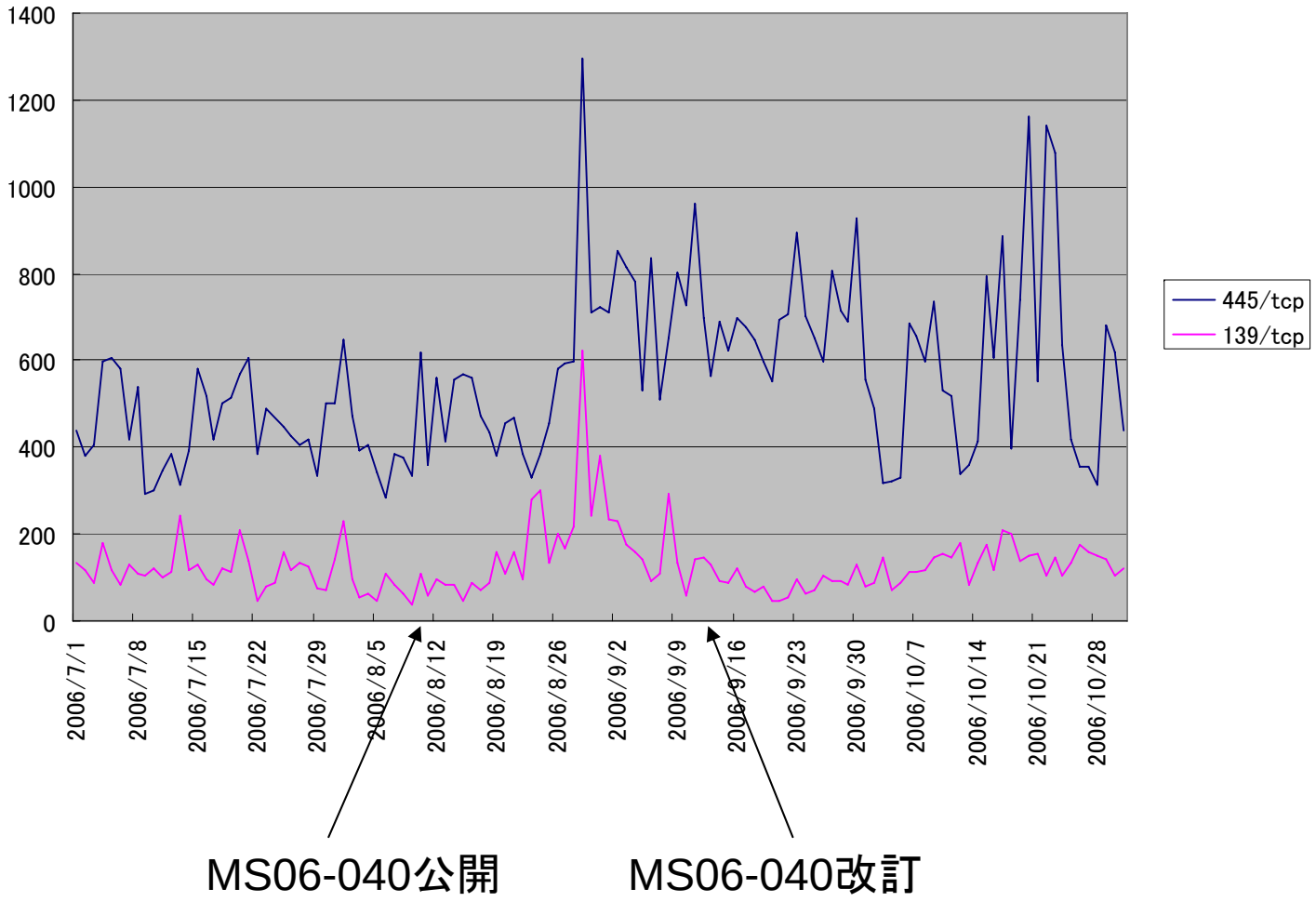
インシデントの例（MS06-040脆弱性の概要）

- Windows RPC, ファイル共有、名前付きパイプなどを提供するServer サービスのバッファオーバーフローの脆弱性により、リモートでコードが実行可能。
- CVE candidate Assigned (20060707) CVE-2006-3439
- MS(米国) 2006/8/8公開、2006/9/12改訂、MS(日本)公開：2006/8/9
- 対象：Windows2000, WindowsXP, Windows Server 2003
- 対象ポート：TCP139, TCP445
- セキュリティ問題の危険性 (深刻度) ：緊急 レベル

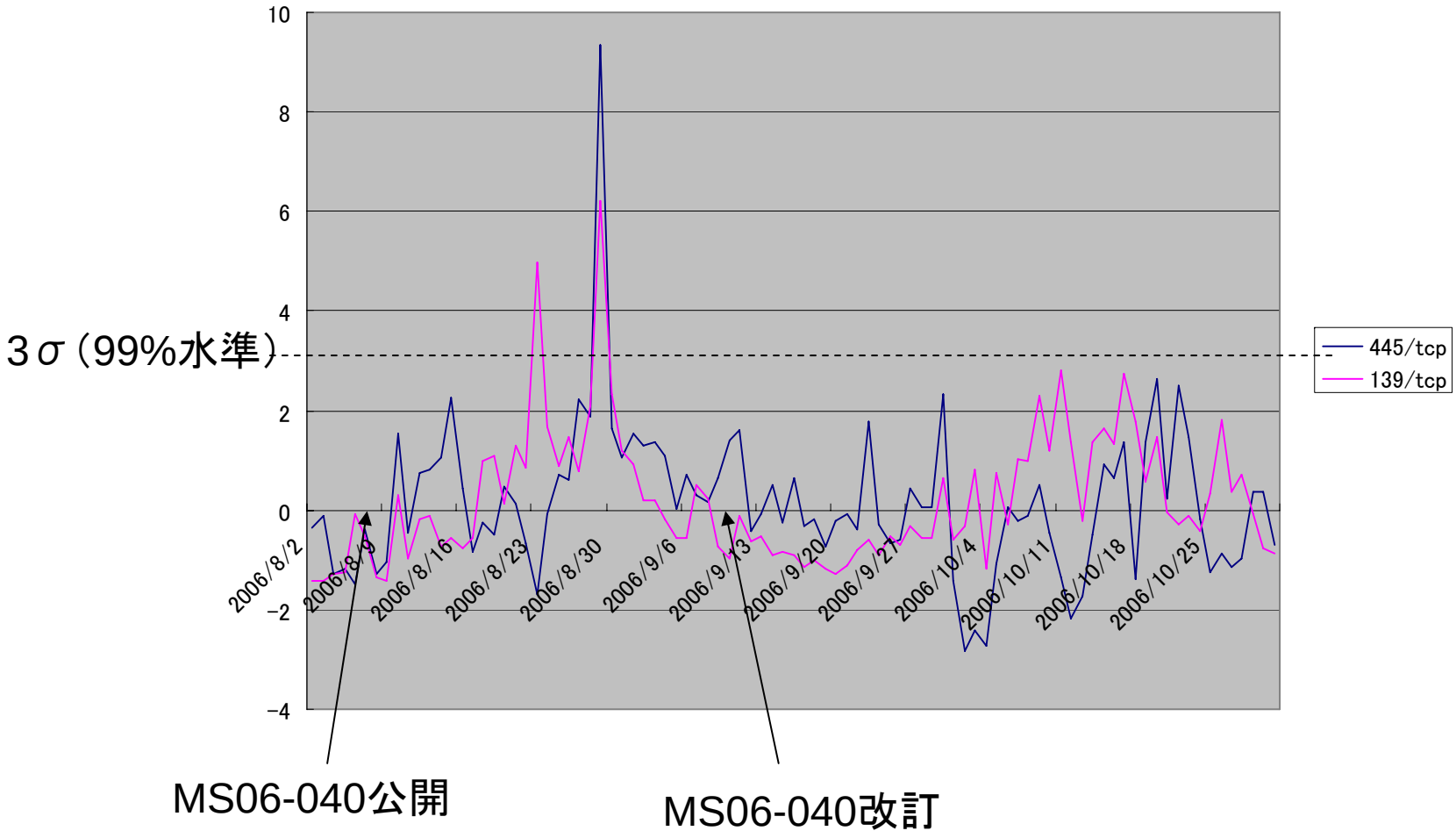


- 情報源：
  http://www.microsoft.com/technet/security/bulletin/ms06-040.mspx

MS06-040前後の関連ポートの動向（センサー合計）



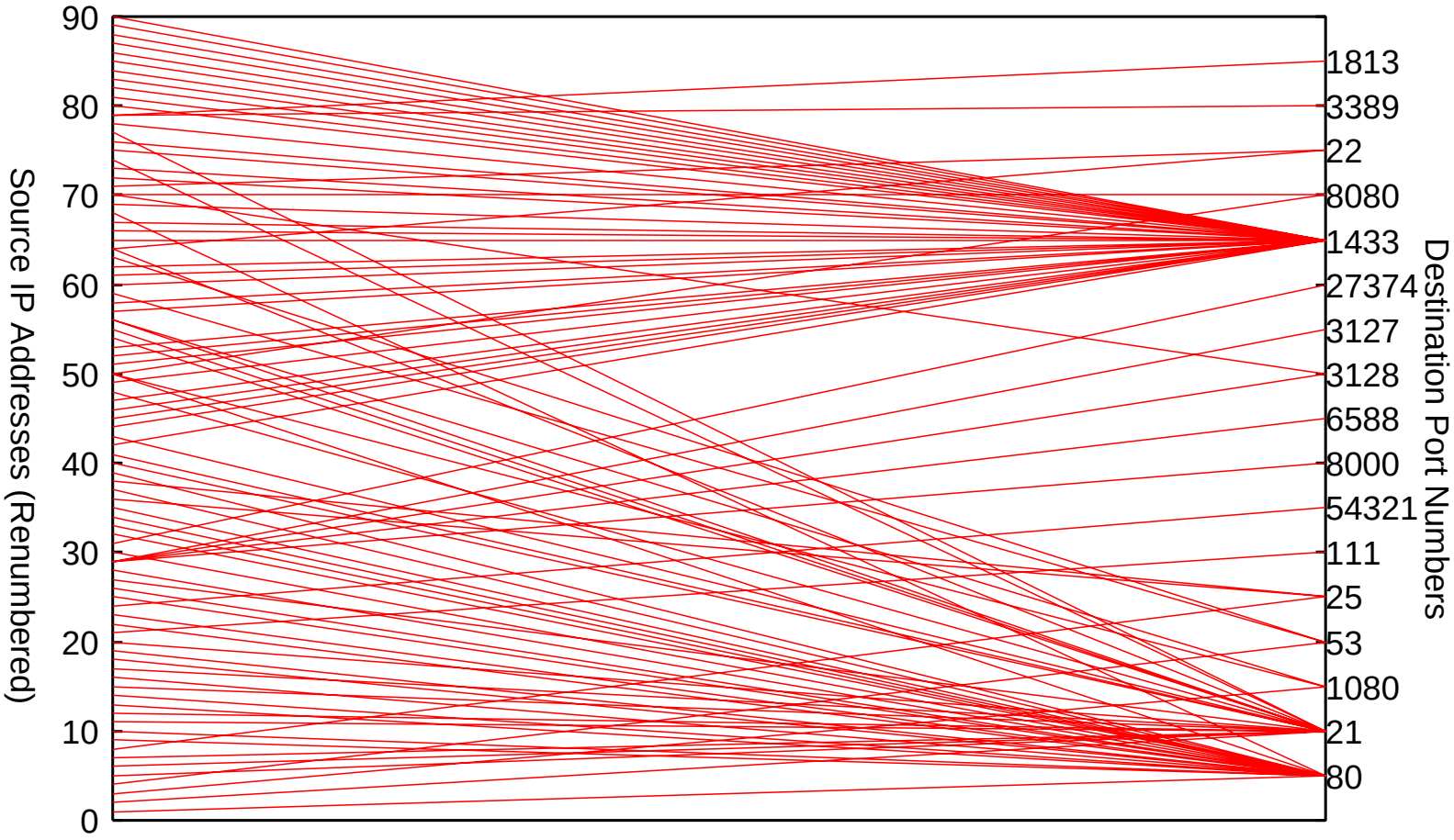
MS06-040前後の分布偏差(Zスコア)(28日分布偏差)



分析系

グラフ構造分析

- 攻撃パケット発信元、攻撃パケット送信先を使ってグラフ構造を作り、それにより脅威度をランキングする

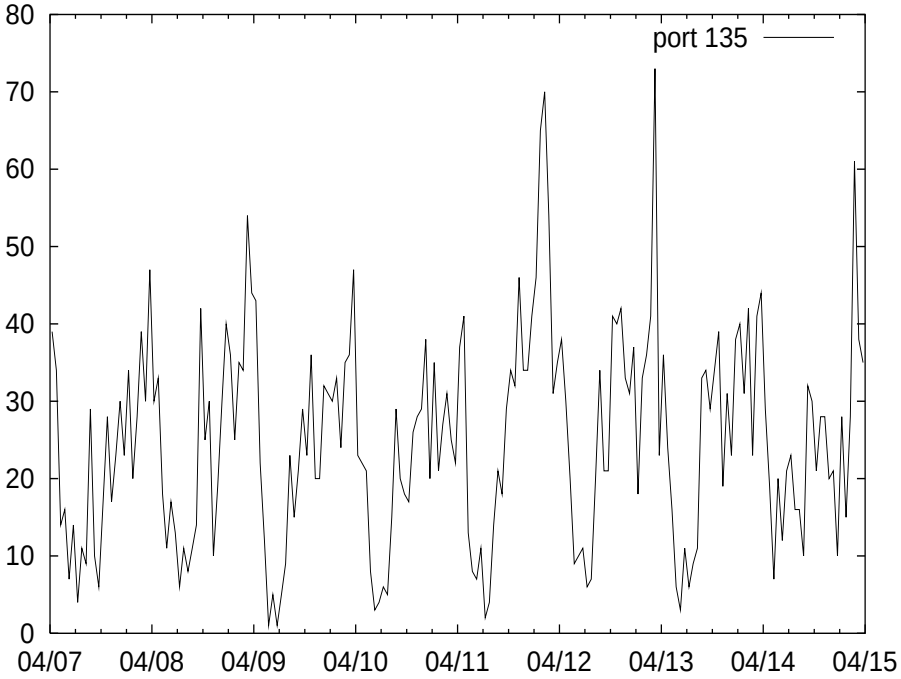


グラフ構造分析例

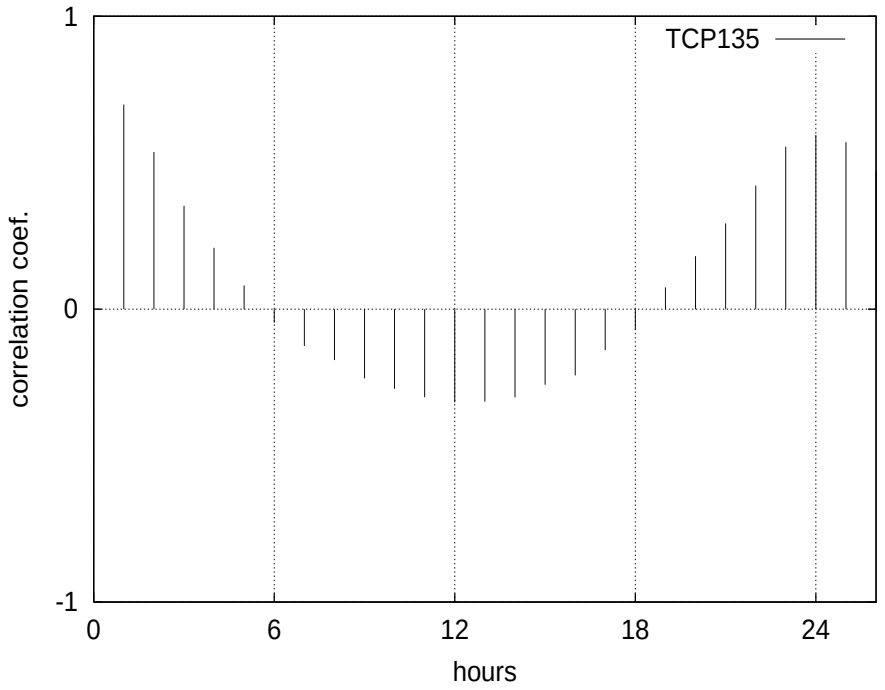
・ 2005年7月に発生したポート1443への攻撃の脅威度を分析しランキングした結果

July 10			July 11			July 12			July 13		
port	count	threat	port	count	threat	port	count	threat	port	count	threat
135	1031	0.627	135	1038	0.789	135	885	0.792	135	1057	0.636
445	1121	0.472	445	822	0.378	445	820	0.432	1433	346	0.331
12345	10	0.163	139	208	0.160	1433	222	0.233	445	739	0.305
139	232	0.159	1433	159	0.130	139	219	0.195	2745	6	0.148
1433	115	0.132	12345	13	0.109	9898	7	0.089	139	204	0.135
3410	8	0.123	901	14	0.109	1024	2	0.085	2100	3	0.111
901	9	0.123	3410	11	0.087	4899	64	0.078	8080	3	0.111
22	12	0.112	3389	6	0.087	3306	19	0.064	8535	3	0.111
3090	7	0.112	3306	18	0.087	2100	1	0.064	25	6	0.111

不正パケットの時間周期性の存在確認



不正パケット数時系列変化
（2007/4/7～2007/4/15）

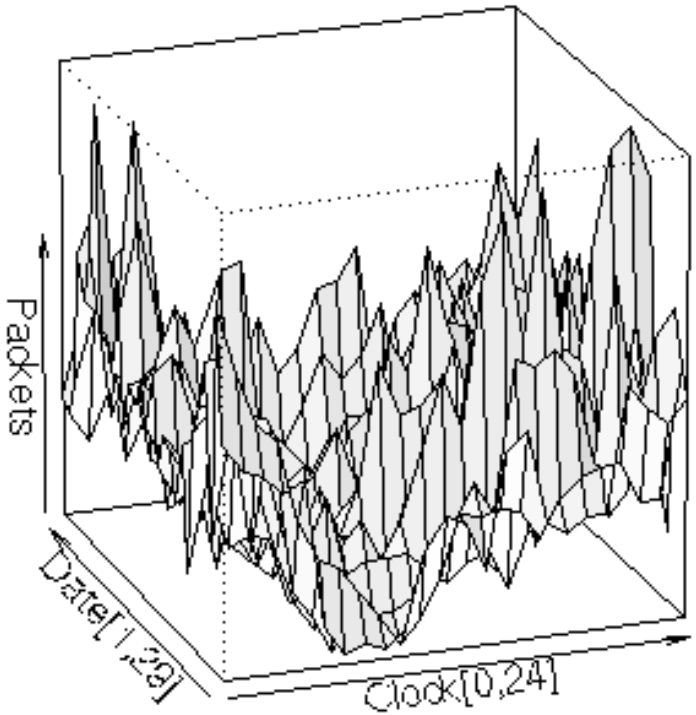


自己相関関数
（ラグ：0～25時間）

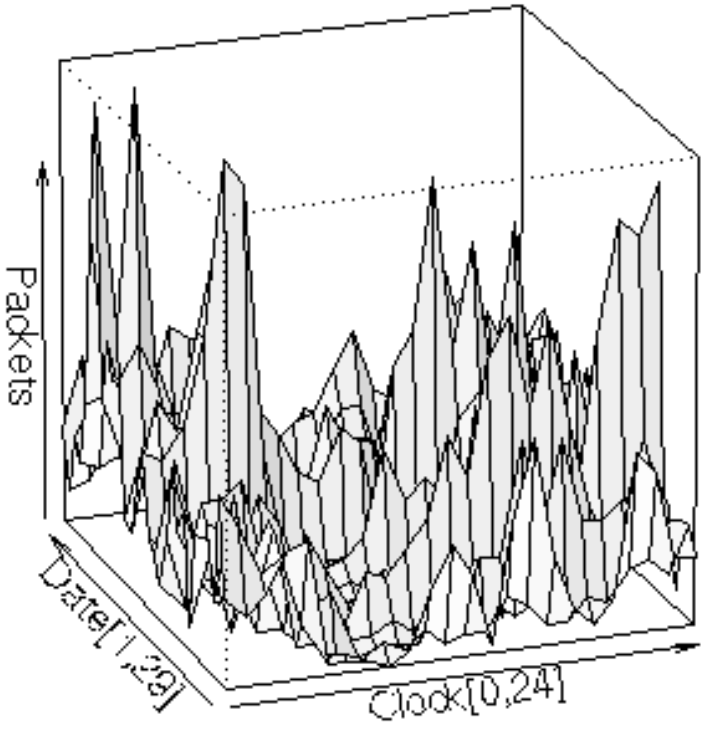
日本　→　時間周期性
米国　→　フラット

3D頻度表示による周期性の存在確認

X135.tcp



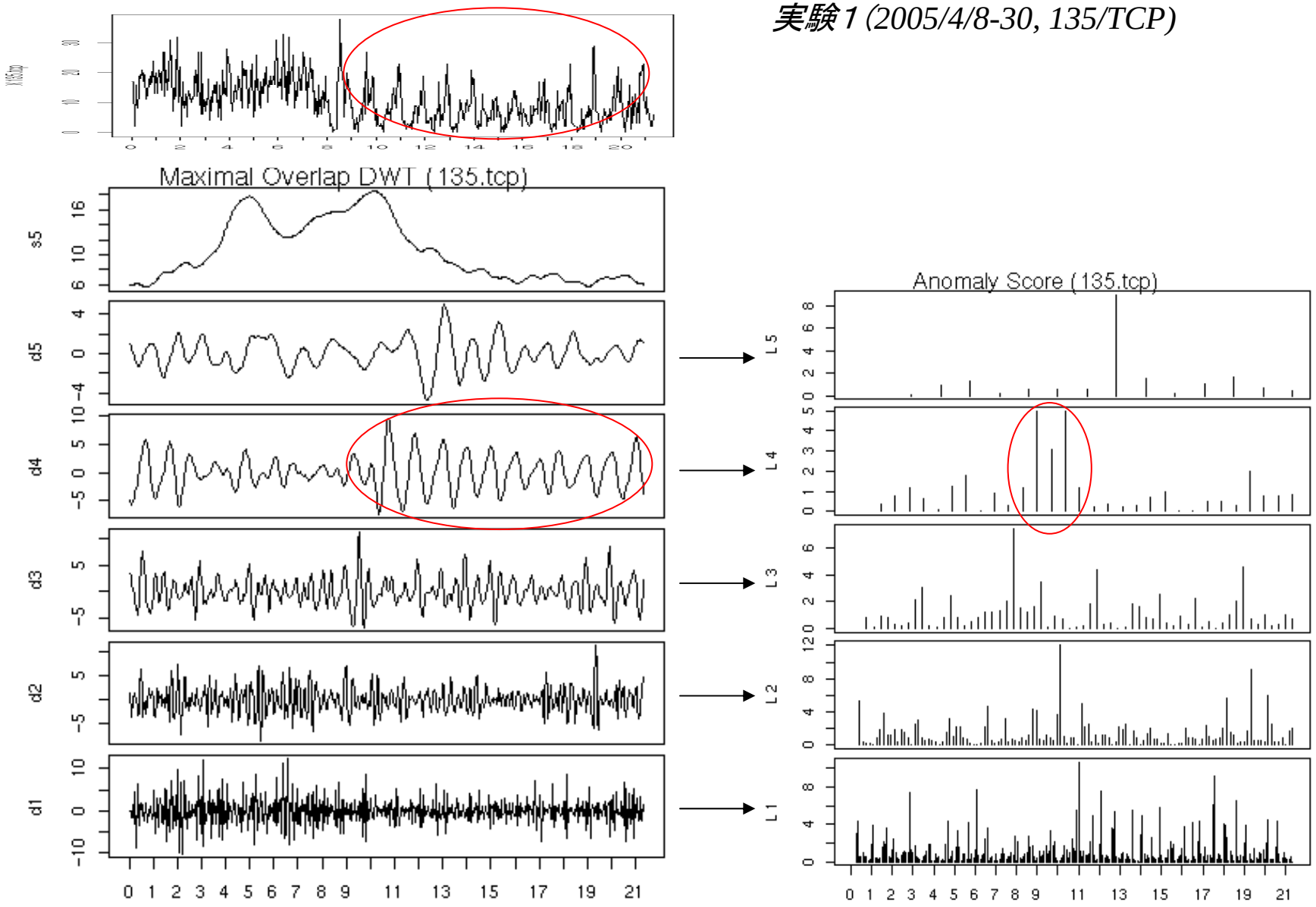
X445.tcp



2007/1/25～2/26

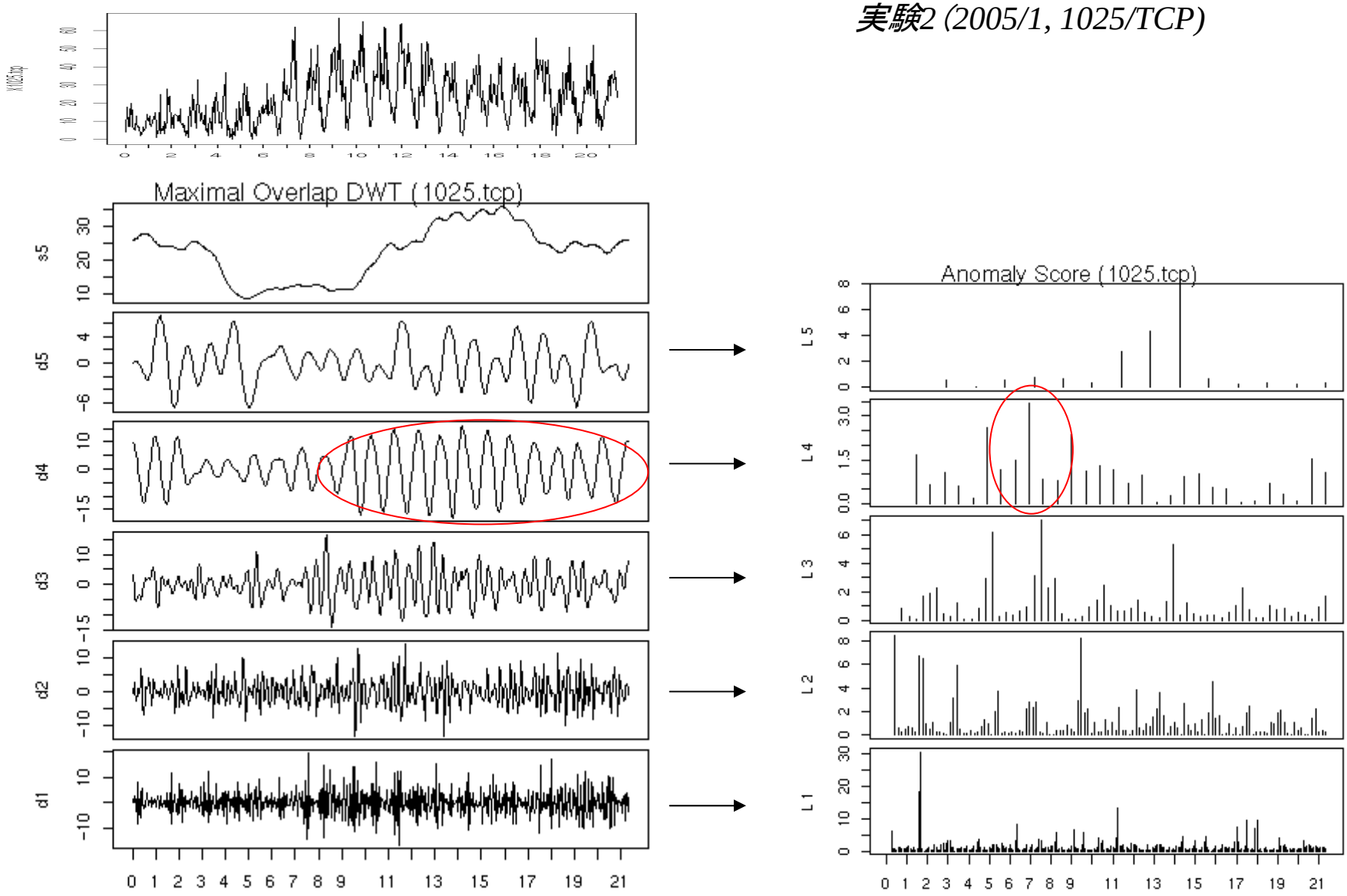
ウェーブレット解析による周期性の確認

実験1 (2005/4/8-30, 135/TCP)



ウェーブレット解析による周期性の確認

実験2 (2005/1, 1025/TCP)

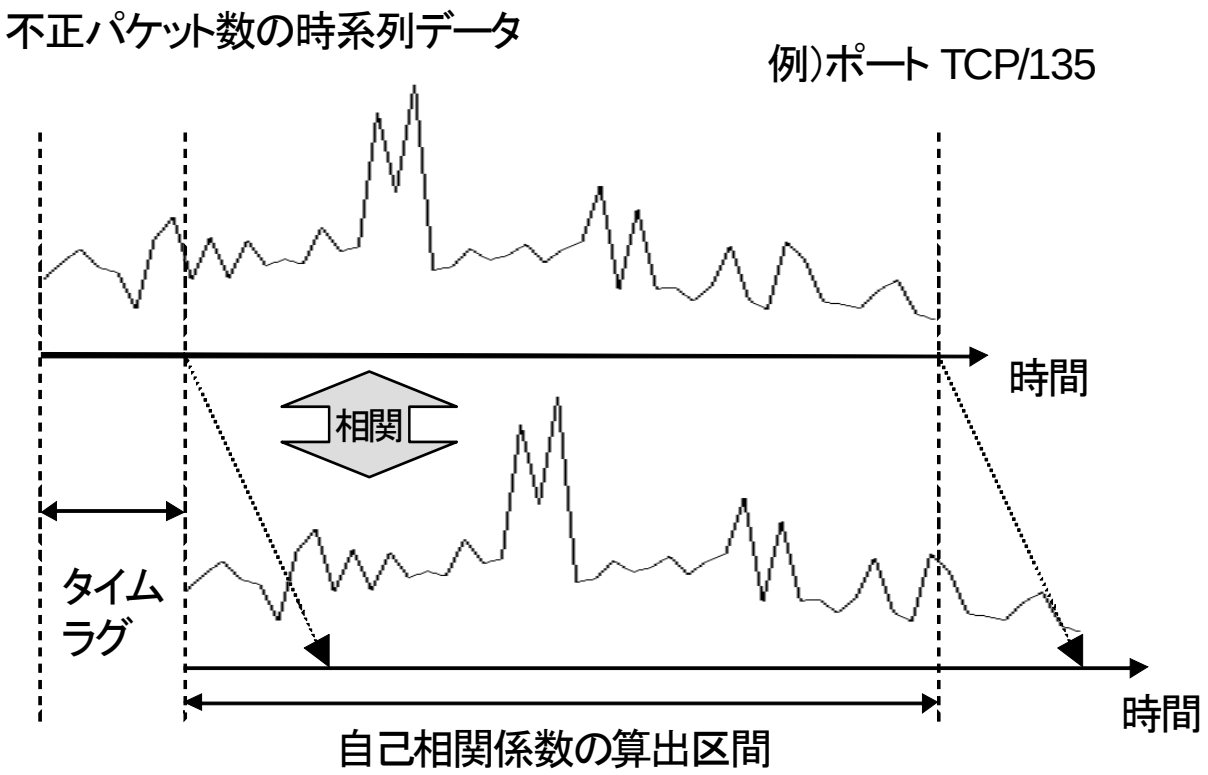


新種のワームの発生・変化の検出手法

- コンピュータ・ワームの種類により、時間、曜日、日にち等による動作周期性が存在
- コンピュータ・ワームの種類により、複数のポートを組合わせたアクセスパターンが存在

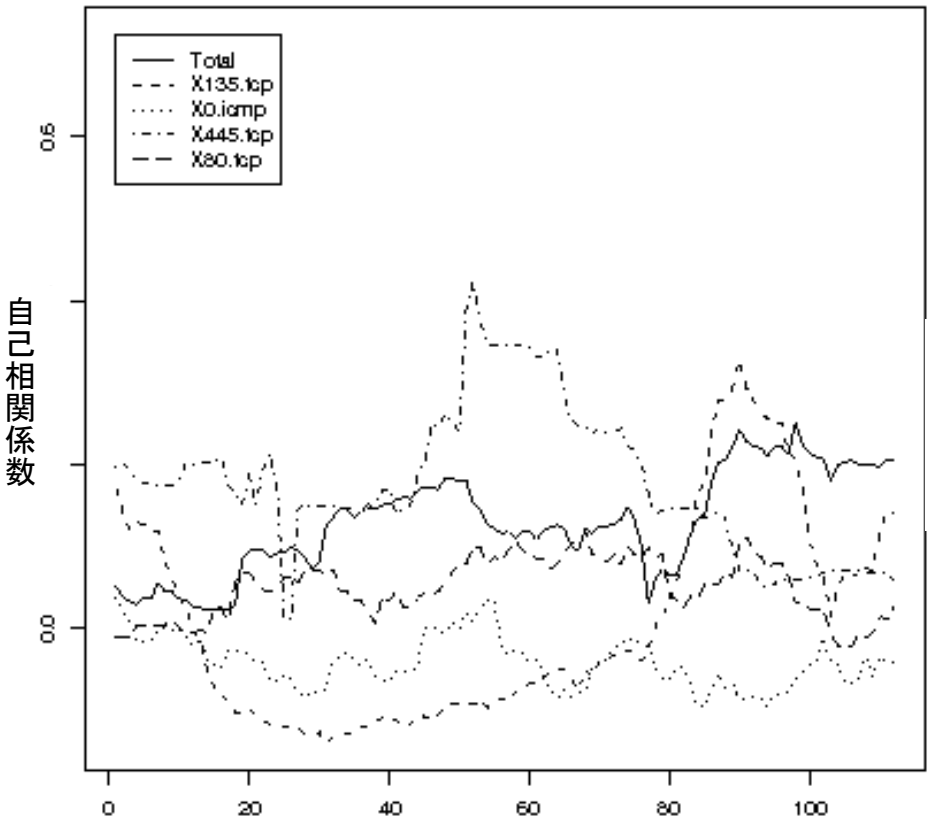
- ポート別の自己相関分析により、新種のワームの発生、ワームの構成比率の変化による時系列パターンの変化を検出
- ポート間の相関分析により、複数のポートへの攻撃を行うワームの変化を検出

ポート別の自己相関分析



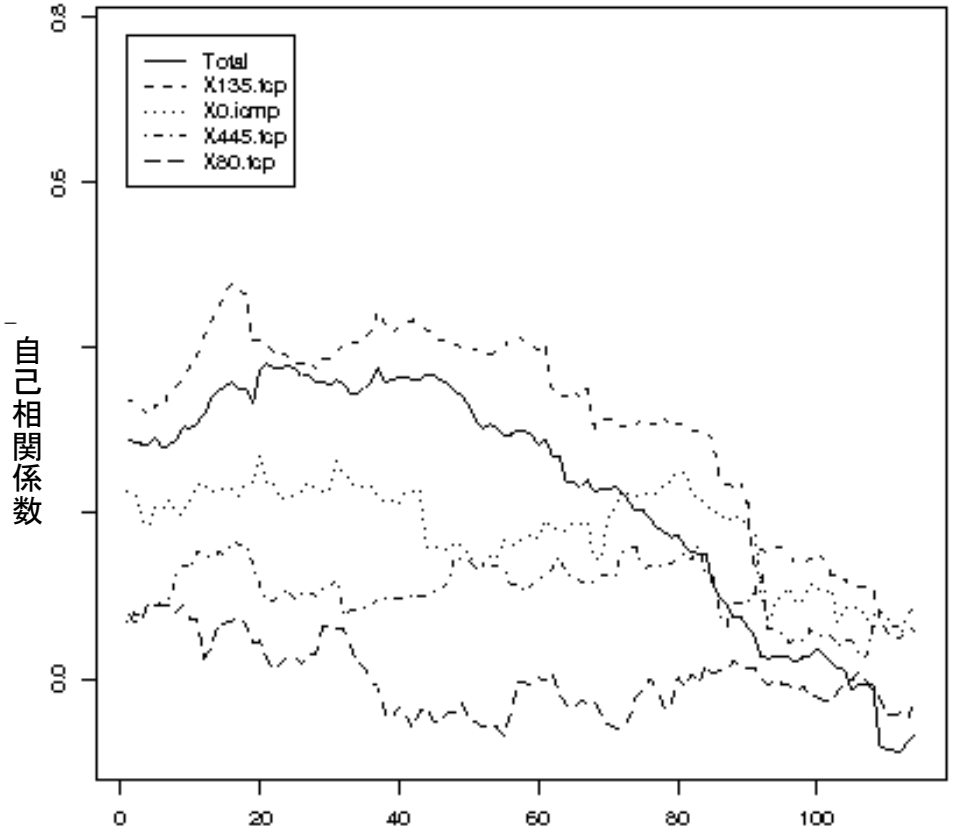
適用結果（自己相関分析、ラグ24時間）

2008年5月16日～22日



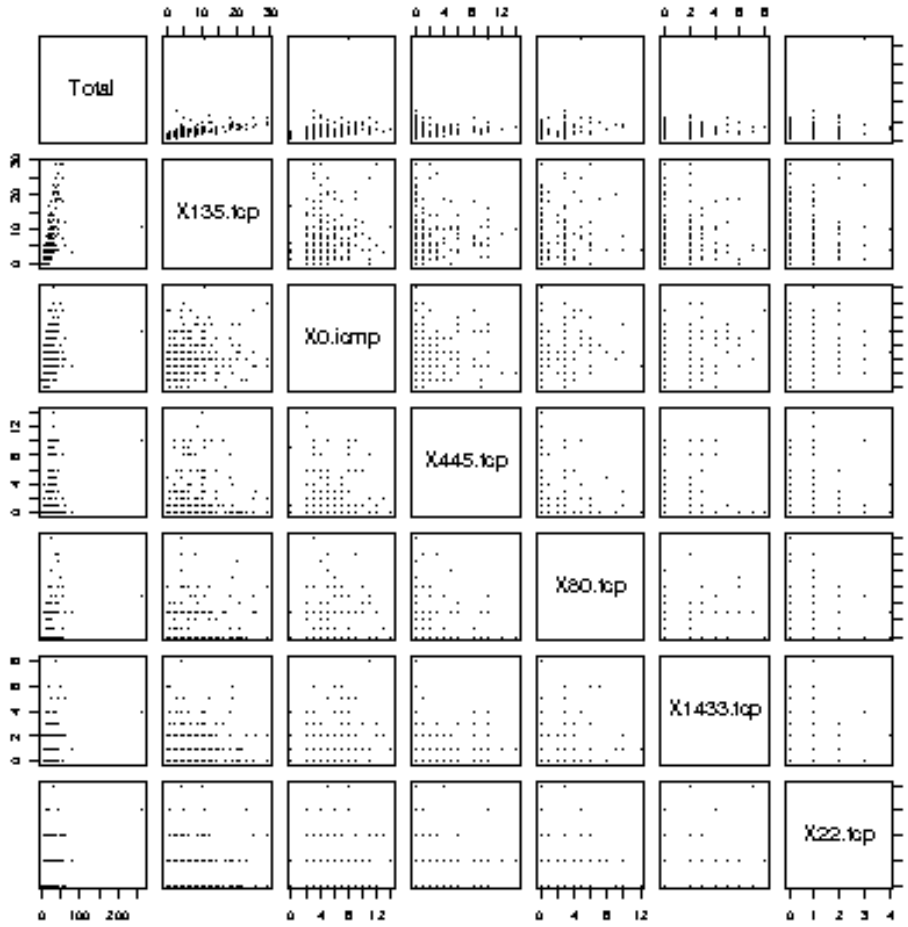
ポート	トータル	135/TCP	IMCP	445/TCP	80/TCP
Zスコア	1.23	1.05	0.0080	−1.32	−0.63

2008年2月25日～3月1日

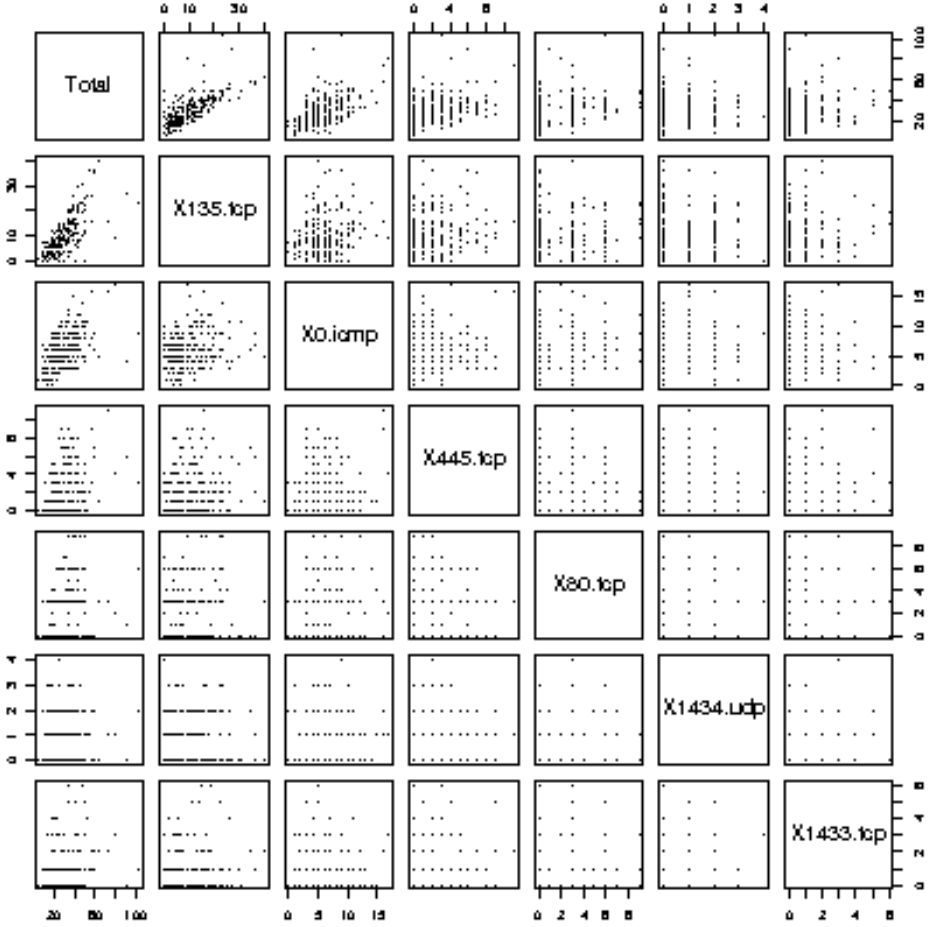


ポート	トータル	135/TCP	IMCP	445/TCP	80/TCP
Zスコア	−2.05	−2.21	−2.03	−0.58	−0.64

適用結果（ポート間相関）



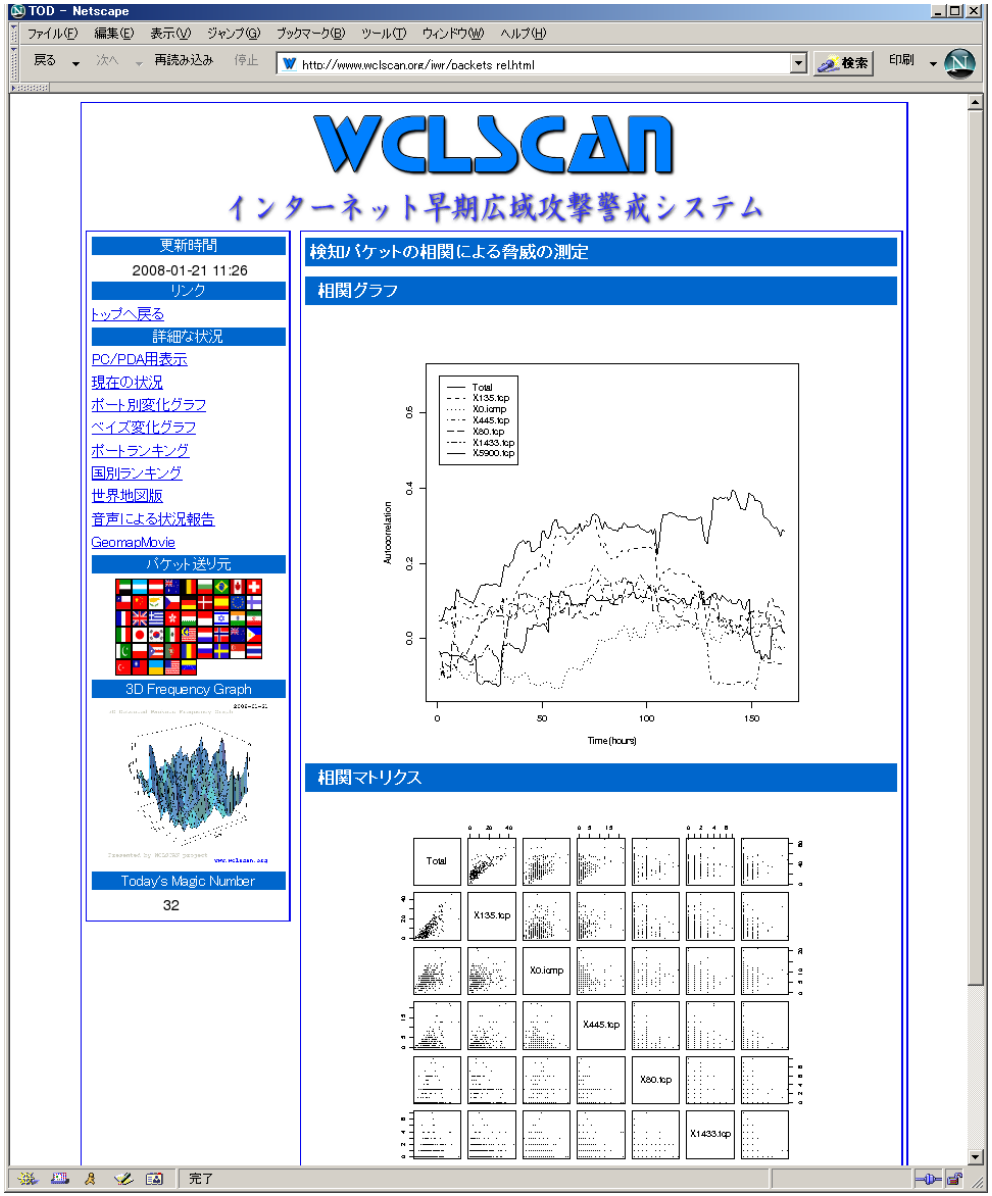
2008年5月16日～22日



2008年2月25日～3月1日

成果の公開ホームページ

http://www.wclscan.org



まとめ

- インターネット上においてワームなどから送信される不正なパケットを複数のIPアドレスでかつ広域的に観測可能とした観測網の構築
- 従来のような不正パケット数の増減のみからでは検出が困難なアクセスパターンの変化に基づく脅威を早期に検出することが可能な技術を開発
  - グラフ構造に着目し、攻撃の脅威がどのように変化し、またどれくらい注意しなければいけないかがわかる脅威度ランキングが作成できる分析技術を開発
  - 不正パケットのポート間の相関およびポートごとの自己相関係数の時間変化を検出することにより、インターネット上の脅威を早期に発見する検出技術を開発
- 分析結果をWEBによりリアルタイムで表示する機能や携帯電話に警報を通知する機能により、サーバ管理者が迅速に脅威に対応できる環境を提供