サイバーリスクの可視化に関する調査

第2班
201220588 石川尚樹
201220589 緒方悠人
201220593 北島暢曜
201120644 韓海燕
アドバイザー教員 金岡晃

目次

1. 調査背景
2. 既存研究
3. 調査目的
4. 調査結果
5. 考察
6. まとめと今後の課題

1.1 インターネットの普及による便利なサービス

amazon

オンラインショッピング

E-mail

クラウドコンピューティング

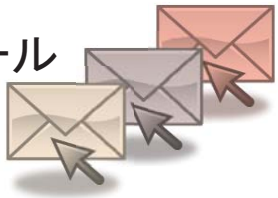
YAHOO! JAPAN

Web検索

SNS
（Social Networking Service）

1.2 便利なサービスに潜むリスク

スパムメール



amazon

データ盗聴

マルウェア

YAHOO! JAPAN

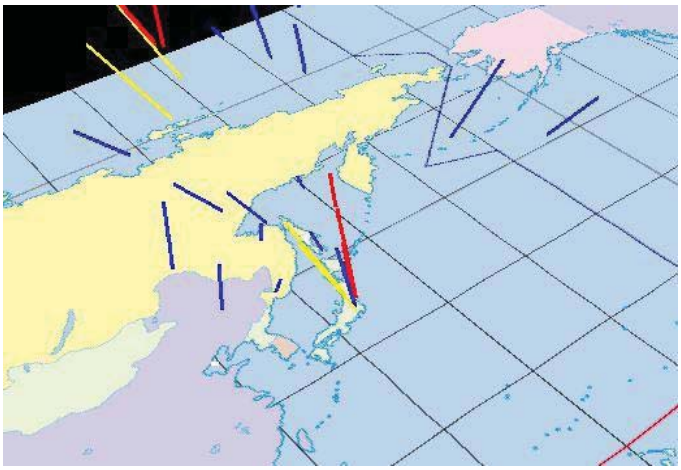
情報漏洩

なりすまし

1.3 日本の現状


衆院にサイバー攻撃
サーバーがウイルス感染
議員パスワード盗難
1カ月盗み見可能状態
震災前の住宅
返済免除
朝日新聞
10月25日
火曜日

出典：朝日新聞朝刊，2011年10月25日

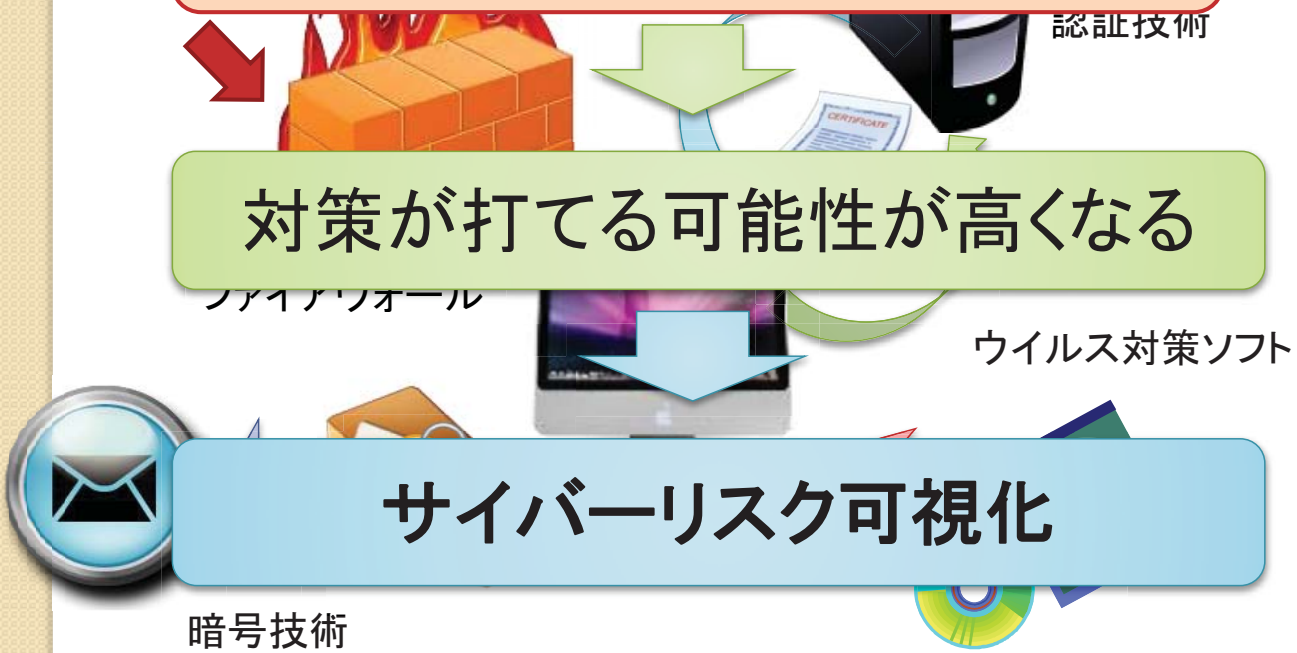


出典：独立行政法人 情報通信研究機構
nicterweb，Atlas URL:http://www.nicter.jp/

常にサイバー攻撃を受けている！

1.4 サイバーリスクに対する技術的アプローチ

サイバーリスクは目に見えないので
目に見えるようにする



対策が打てる可能性が高くなる

サイバーリスク可視化

1.5 現存する可視化技術

・ネット上の無料ツール（オープンソースツール）
・商用製品
・可視化に関する研究論文上のツール

可視化ツールは多種多様
どのツールを使えばいいのか分かりづらい！

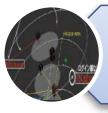
ユーザが選択しやすい分類が必要！

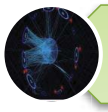
目次

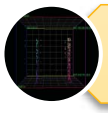
1. 調査背景
2. 既存研究
3. 調査目的
4. 調査結果
5. 考察
6. まとめと今後の課題

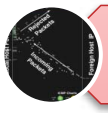
2.1 可視化の分類

- Shiravi, et al.
  “A Survey of Visualization Systems for Network Security”(2011)
  サイバーリスク可視化の対象を5つのクラスに分類


Host/Server Monitoring


Internal/External Monitoring


Port Activity

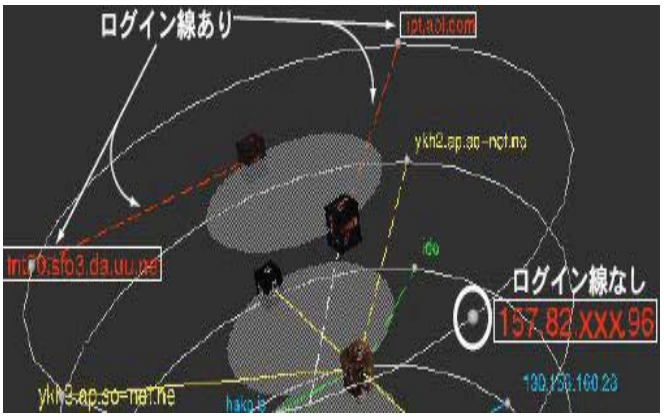

Attack Patterns


Routing Behavior

2.2 5つのクラス(1/3)

Host/Sever Monitoring

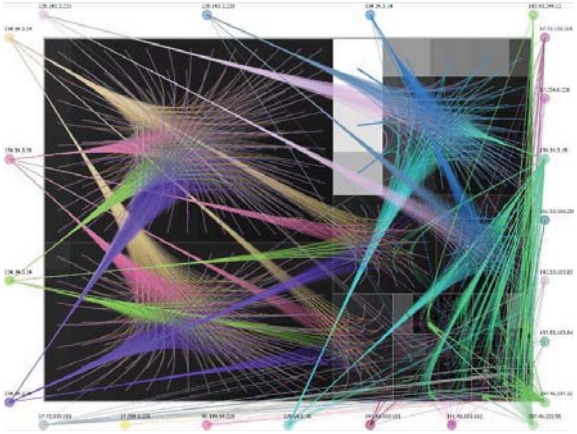
ネットワーク内のホスト・サーバーの状態を可視化するクラス



鼓による可視化

Internal/External Monitoring

外部ネットワークのホスト・サーバーまで可視化するクラス

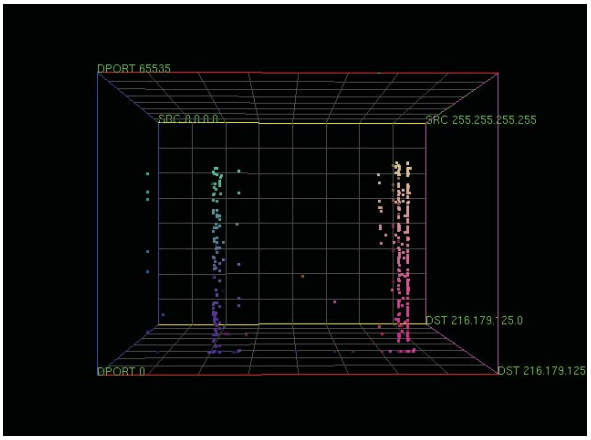


NFlowVisによる可視化

2.2 5つのクラス(2/3)

Port Activity

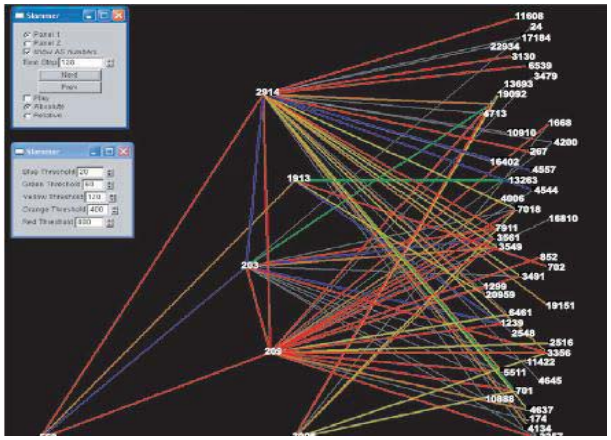
通信ポートの動きを可視化するクラス



Cube of Doomによる可視化

Routing Behavior

ルーティングを可視化するクラス

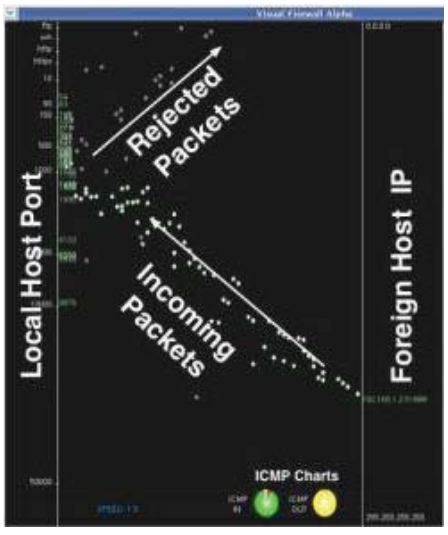


BGP Eyeによる可視化

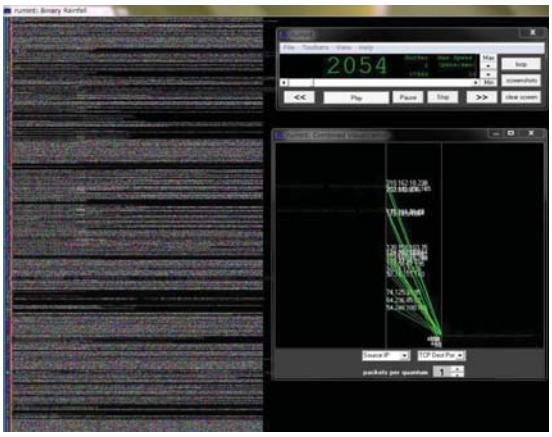
2.2 5つのクラス(3/3)

Attack Patterns

DoS/DDoS攻撃をはじめ、サイバー攻撃を可視化するクラス



Visual Firewallによる可視化



Rumintによる可視化

2.3 既存研究の問題点

目的のクラスに応じたツールを選択しやすくなる

ツールの特徴・ユーザの知識量によっては使えないこともある
→**適切なツールを選択しにくい**

ユーザが適切なツールを選択できる分類法が必要！

Visualization System	Visualization Technique(s)	Data Source(s)	Number of Citations
Host / Server Monitoring			
Erbacher et al. [4][5]	Glyph	Server Logs	106 | 7
Tudumi [6]	3D Node Link	Server Logs	38
NVisionIP [7,8]	Scatter Plot	NetFlows	145 | 20
Portall [9]	Node Link	Packet Traces	21
HoNe [10]	Node Link	Packet Traces	8
Perlman et al. [11]	Node Link | Glyph	Packet Traces	5
Radial Traffic [12]	Radial Panel	Packet Traces	23
Mansmann et al. [13]	Node Link	Packet Traces	2
Internal/External Monitoring			
VISUAL [14]	Scatter Plot | IP Matrix	Packet Traces	93
VizFlowConnect [15]	Parallel Coordinates	NetFlows	111
Erbacher et al. [16]	Radial Panel	Packet Traces	8
TNV [17]	IP Matrix | Color Map	Packet Traces	48
Port Activity			
Abdullah et al. [18]	Histogram	Packet Traces	30
Cube of Doom [19]	3D Scatter Plot	Packet Traces	99
PortVis [20]	Scatter Plot	NetFlows	112
NetBytes Viewer [21]	3D Scatter Plot	NetFlows	7
Existence Plots [22]	Scatter Plot	Packet Traces	3
Attack Patterns			
Giardin [29]	Color Map	Packet Traces	60
NIVA [30]	Node Link | Glyph	Intrusion Alerts	51
Snort View [31]	Scatter Plot | Glyph	Intrusion Alerts	67
IDGraphs [32]	Scatter Plot	NetFlows	29
IP Matrix [33]	Scatter Plot | Color	Intrusion Alerts	21
Visual Firewall [34]	Scatter Plot	Packet Traces	24
IDS Rainstorm [35]	Scatter Plot	Intrusion Alerts	60
Vizalert [36][37][38]	Radial Panel	Intrusion Alerts	38 | 35 | 29
Rumint [39][40]	Parallel Coordinates	Packet Traces	15 | 35
Ren et al. [41]	Flying Term	DNS Traces	10
Xiao et al. [42]	Scatter Plot	Packet Traces	23
Svision [43]	3D Scatter Plot	Packet Traces	9
Mansmann et al. [44]	Treemap	Packet Traces	20
SpiralView [45]	Radial Panel	Intrusion Alerts	5
NFlowVis [46]	Treemap	NetFlows	17
Avisa [49]	Radial Panel	Intrusion Alerts	2
Routing Behavior			
BGPlay [50]	Node Link	BGP Traces	22
Wong et al. [51]	Node Link	BGP Traces	9
LinkRank [52]	Node Link	BGP Traces	16
Teoh et al. [53][54][55]	Histogram | Node Link	BGP Traces	54 | 28 | 35
BGP Eye [56]	Color Map	BGP Traces	8

目次

1. 調査背景
2. 既存研究
3. 調査目的
4. 調査結果
5. 考察
6. まとめと今後の課題

3.1 調査目的

既存研究の問題点

目的

ユーザが自らの知識量に応じた
可視化ツールを選択できる分類法を提案

手法

1. ツールの理解に必要な知識量を抽出
2. Shiraviらの表を拡張し、
   新たな分類表で知識量の難易度を表現

本調査ではネットワークセキュリティの可視化についての調査を行う

3.2 調査について

調査対象

- 研究論文で発表されている可視化ツール
- ネット上で入手できるオープンソース可視化ツール
- 商用に販売されている可視化ツール

調査項目

- 5つのクラスの所属
- ツールを理解するために必要な知識と量

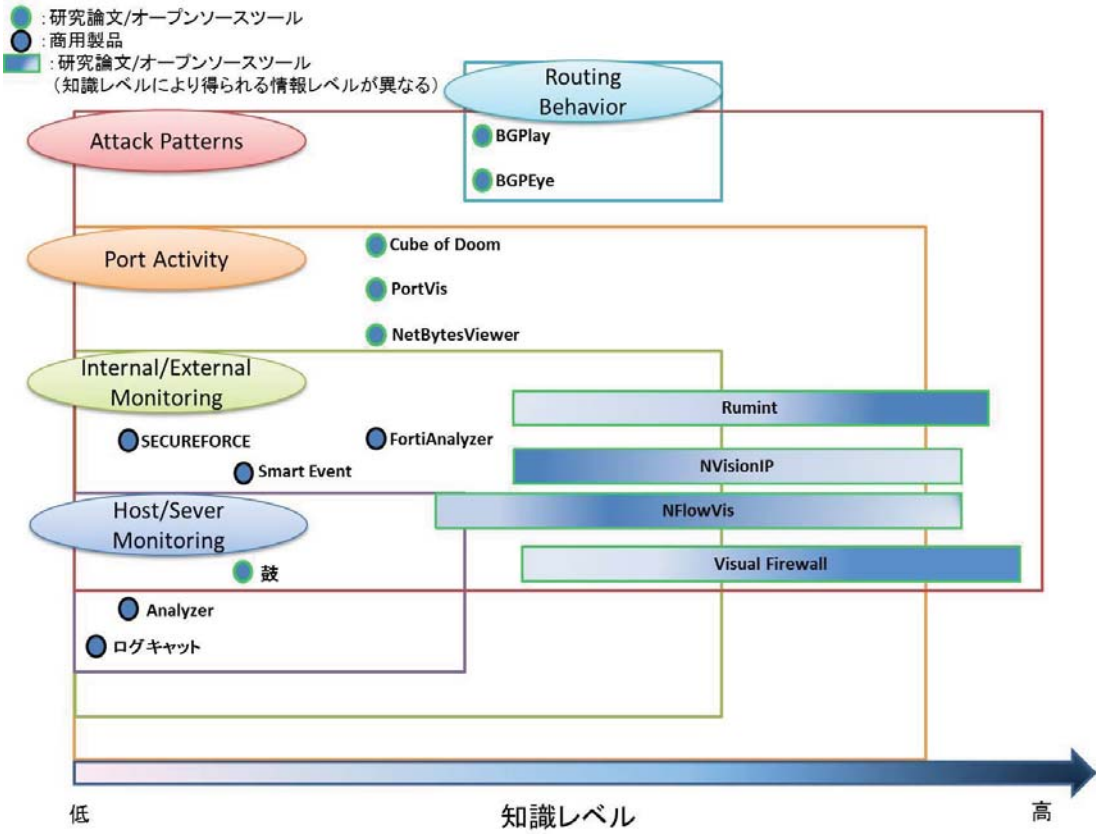
基準

- グループ内で議論し評価

目次

1. 調査背景
2. 既存研究
3. 調査目的
4. **調査結果**
5. 考察
6. まとめと今後の課題

4.1 分類結果



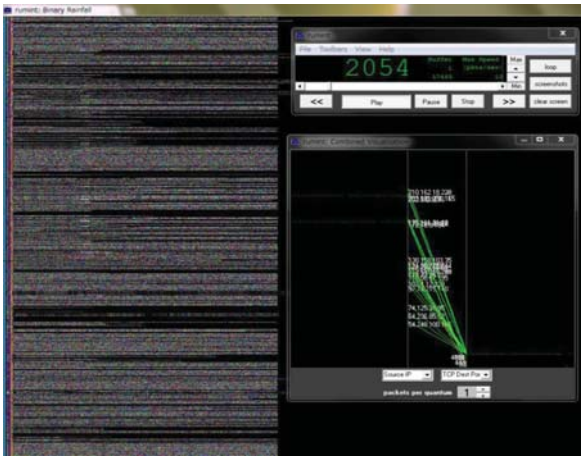
4.2 調査対象の詳細

ツール名	機能	可視化テクニック	要求される知識	分類
鼓[2]	ログ収集 / IDS	3D Node Link	IPアドレス / DNS / IDS	研究論文
Visual Firewall[3]	トラフィック可視化 / シグネチャ可視化 / 通信ポート可視化 / IDS	Scatter Plot / Line Graph	IPアドレス / ポート / IDS / DoS / ウイルス	研究論文
PortVis[4]	通信ポート可視化	Scatter Plot / 3D Line Graph	IPアドレス / ポート	研究論文
NVisionIP[5]	通信ポート可視化 / トラフィック可視化	Scatter Plot / Bar Graph	IPアドレス / ポート / ウイルス / DoS	オープンソース
NFlowVis[6]	トラフィック可視化 / ネットワーク可視化 通信ポート可視化 / IDS	Tree Map / Line Graph / Node Link / Bar Graph	IPアドレス / ポート / DoS / SSHに対する攻撃 / IDS	研究論文
Cube of Doom[7]	通信ポート可視化	3D Scatter Plot	IPアドレス / ポート	オープンソース
BGPEye[8]	ルーティング可視化	Color Map / Node Link / Bar Graph / Pie Graph	AS / BGP	研究論文
NetBytesViewer[9]	通信ポート可視化	3D Impulse Graph	IPアドレス / ポート	研究論文
BGPlay[10]	ルーティング可視化	Node Link	AS / BGP	オープンソース
Rumint[11]	トラフィック可視化 / 通信ポート可視化 / IDS	Parallel Coordinates	IPアドレス / ポート / IDS / DoS / ウイルス	オープンソース
ログキャット[12]	ログ収集・解析	Bar Graph / Line Graph	—	商用製品
SECUREFORCE[13]	ログ収集・解析 / ネットワーク可視化 / IPS	Bar Graph / Pie Graph / Line Graph / Color Map	IPアドレス / (ウイルス / DoS)	商用製品
analyzer[14]	ログ収集・解析 / ネットワーク可視化 / 機器故障検知	Bar Graph / Line Graph / Node Link	IPアドレス	商用製品
Smart Event[15]	ログ収集・解析 / IPS	Node Link / Pie Graph / Bar Graph / Color Map	IPアドレス / (DoS / ウイルス)	商用製品
FortiAnalyzer[16]	ログ収集・解析 / ネットワーク可視化 / IDS / その他脆弱性スキャン	Bar Graph / Pie Graph / Line Graph	IPアドレス / (ポート / ウイルス / DoS)	商用製品

4.3 ツールの二分類

研究論文上の可視化ツール/
オープンソースツール

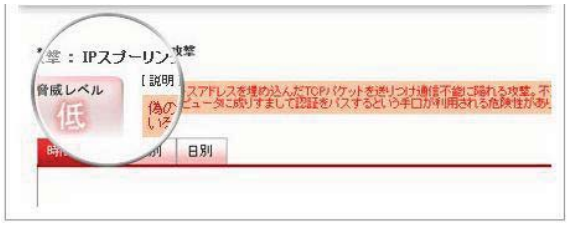
- ユーザの知識量に依存
- 問題解決のための支援が**無い**



Rumintによる可視化

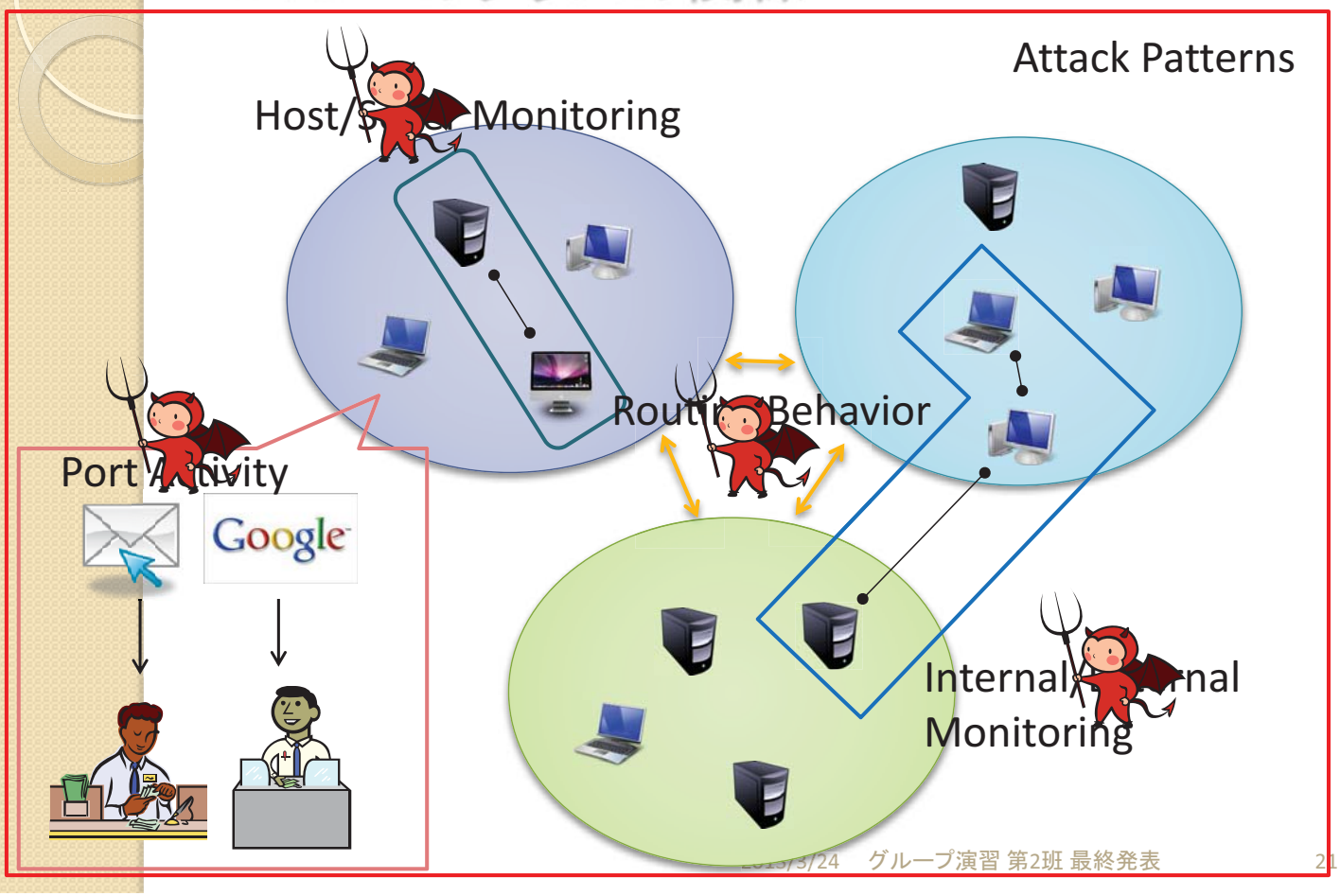
商用製品

- 分かりやすいグラフィック
- 問題解決のための支援が**ある**

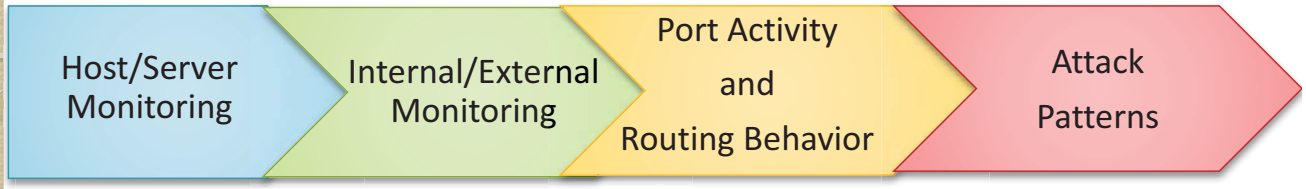


SECUREFORCEによる可視化

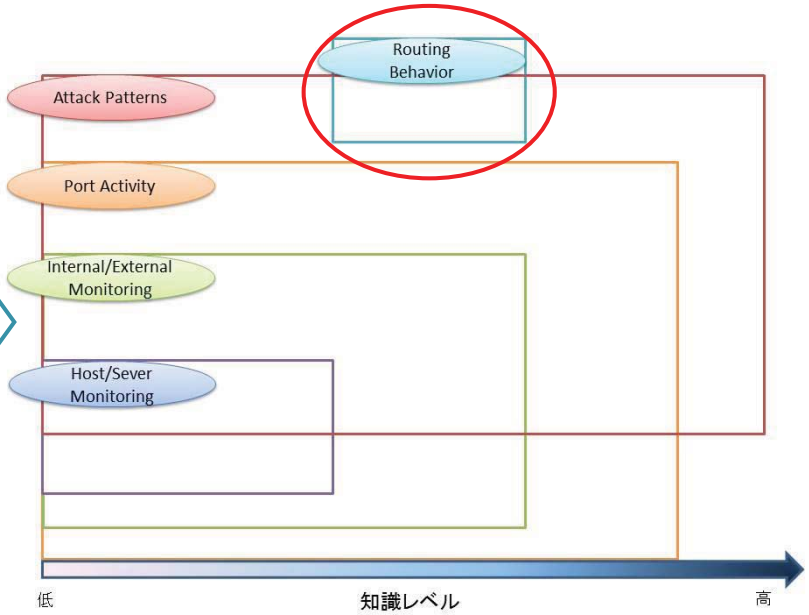
4.4 5つのクラスの関係



4.5 5つのクラスの包含関係



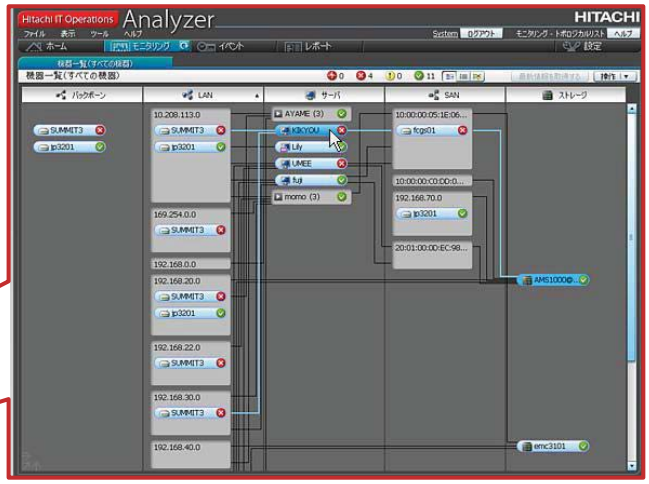
全ての可視化ツールにおいてこの関係が成り立つわけではない

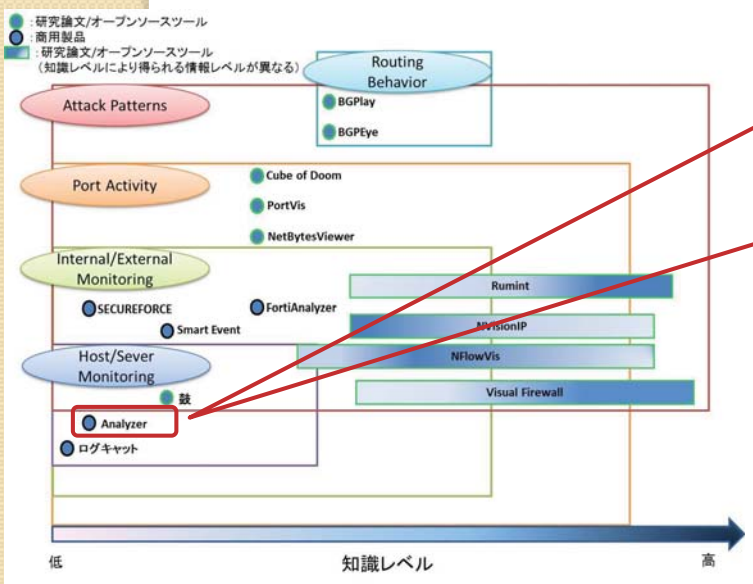


4.6 Analyzer（商用製品）

分類：Host/Sever Monitoring

機能：ネットワーク内の機器の状態を把握することができる
稼働監視ツール



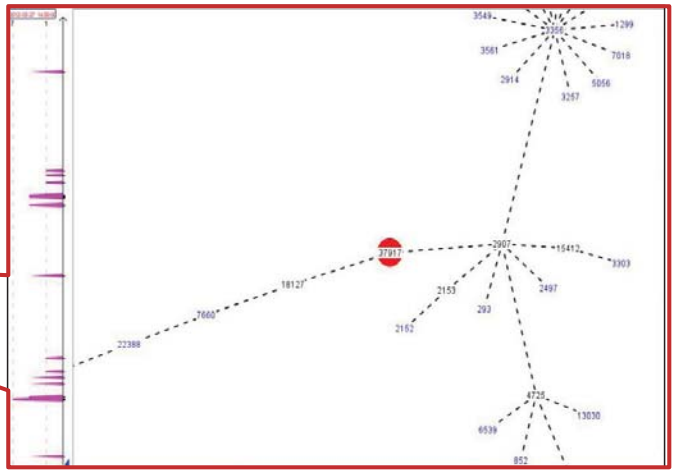


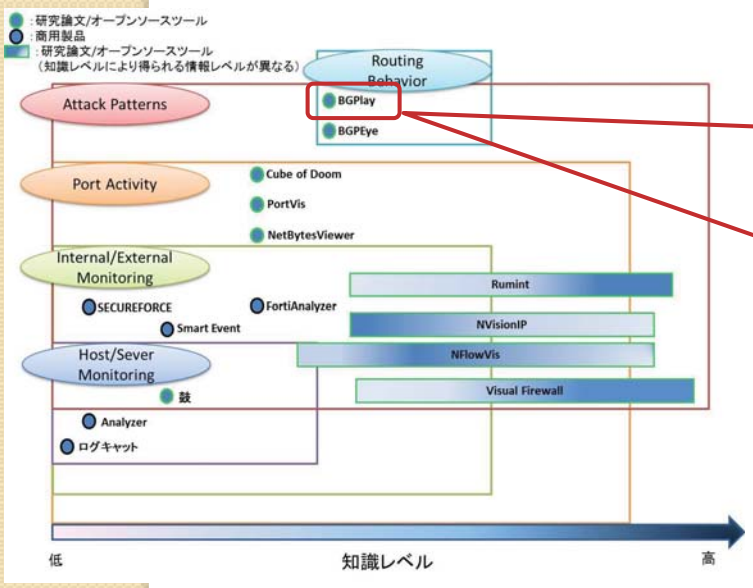
グループ内評価：
- 機器の繋がり視認しやすい
- ユーザに知識が無くても、ツールの支援により理解できる

4.7 BGPlay（オープンソースツール）

分類：Routing Behavior

機能：Prefixと日時を設定することで、その期間内のルーティングを表示する



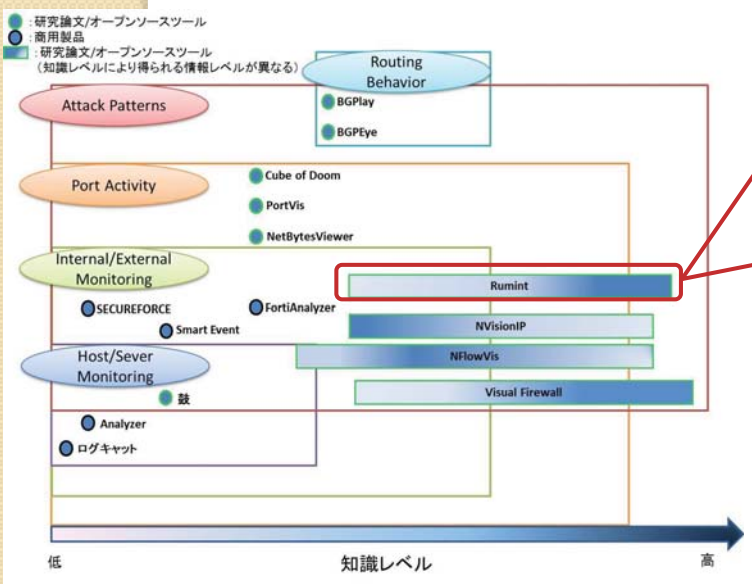


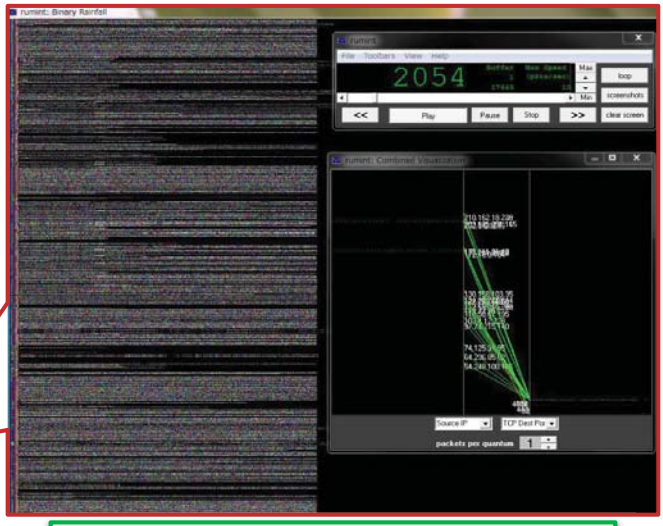
グループ内評価：
- ASという応用知識が必要
- 他のクラスの知識は特に必要としない

4.8 Rumint（オープンソースツール）

分類：Internal/External Monitoring, Port Activity,**Attack Patterns**

機能：pcapデータセットをロードすることで送受信された
パケットを可視化する





グループ内評価：
- 計20種の可視化が可能、多彩
- ユーザに対する支援はない
- 異常が発生しているか否かの判断はユーザの知識次第

目次

1. 調査背景
2. 既存研究
3. 調査目的
4. 調査結果
5. 考察
6. まとめと今後の課題

5.1 可視化対象に対する考察

調査対象において大きな違いが見られた

商用製品

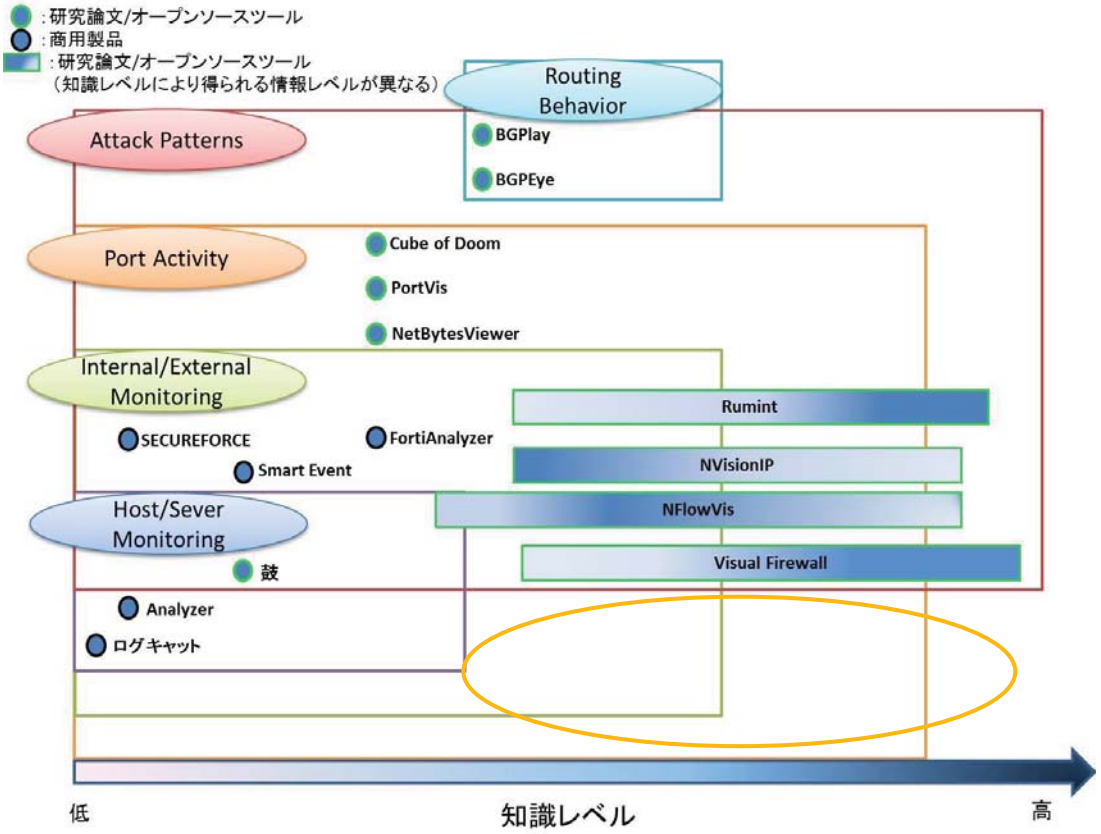
- 企業向けのツールが大多数
- 個人向けに可視化を提供するものはほとんどなかった
- 誰でも問題を発見することができるような支援

研究論文/オープンソースツール

- ハイレベルなユーザ向けのツールが大多数
- 実際に使用できる環境を整えることも難しいものが多数
- 新規の攻撃の発見や対策の検討に使用

5.2 可視化レベル表に対する考察

- 現存する可視化手法を全体的に把握できた
- 可視化ツールが自らの知識で選択しやすくなった
- ツールの見当たらないエリアの存在が判明した
- 目的とユーザのレベルにあった可視化ツールが必ず存在するとは断言できない



・実際にツールが必要であるのに存在しない
・必要が無くて存在しない

5.2 可視化レベル表に対する考察

- 現存する可視化手法を全体的に把握できた
- 可視化ツールが自らの知識で選択しやすくなった
- ツールの見当たらないエリアの存在が判明した
- 目的とユーザのレベルにあった可視化ツールが必ず存在するとは断言できない

目次

1. 調査背景
2. 既存研究
3. 調査目的
4. 調査結果
5. 考察
6. まとめと今後の課題

- まとめ
  - 現存する可視化ツールを調査
  - ユーザの知識レベルで分類する新たな手法を提案
    - この分類手法は初めての試みである
- 今後の課題
  - 調査の拡大
    - さらに多くの可視化ツールを調査
    - ツールの見当たらないエリアに入り込むツールが存在する可能性の検証
  - 可視化レベルのより明確な境界を定義
    - レベルをさらに明確に定義し、適宜変更する必要