

# Ventures on the Internet- From Academy to Industry



*Glenn Mansfield Keeni*

 株式会社 サイバー・ソリューションズ  
*Cyber Solutions Inc.*

[www.cysol.co.jp](http://www.cysol.co.jp)

# Swing with the waves

I adore the medical profession

I love Physics

Ended up doing Computer Science

**The Internet Wave arrived !**



# The time-line (1)

- ◆ 1957年 スプートニクショック. 米高等研究計画局 (**ARPA**)を編成する.
- ◆ 1969年 **ARPANET**接続実験に成功.
- ◆ 1973年 Vint CerfとBob Kahn、**TCP**を提案.
- ◆ 1981年 日本でN1 ネット(**UUCP**=UNIX to UNIX Copy)スタート.
- ◆ 1982年 **TCP/IP**米国防総省標準に採用.
- ◆ 1983年 TCP/IPが**UNIX**(4.2BSD版)に装備.
- ◆ 1984年 **DNS**(Domain Name System)導入.
- ◆ 1986年 第一回**IETF**ミーティング
- ◆ 1988年 **CERT**(Computer Emergency Response Team) 設立  
**TAINS in Tohoku University**

# The time-line (2)

- ◆ 1991年 ティム・バーナーズリー, **WWW** (World-Wide Web)登場.
- ◆ 1993年 Mosaicの登場. WWWトラフィック**341,634%**の急増.
- ◆ 1993年 **JPNIC** (ネットワークセンター)発足.
- ◆ 1995年 ドメイン名登録が**有料化**.
- ◆ 1995年 Sun Microsystemsによって**JAVA**が発表される.
- ◆ 1996年 米政府サイト(CIA、司法省、空軍等)が**不正侵入**をうける.
- ◆ 1998年 **2,000,000**件目のドメイン名が登録される.

# The Internet Wave

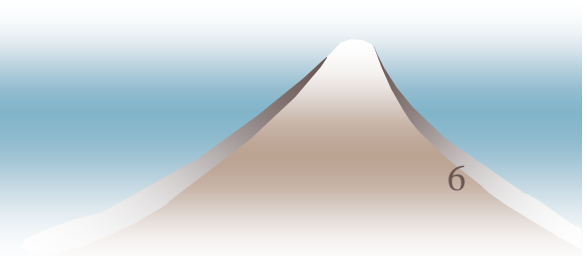
*情報の民主化*

*Self Expressionの民主化*

*ネットワーク活動の民主化*

*Democratization/Universalization of  
Information/SelfExpression/Network activity*

*End of part one*



# サイバー・ソリューションズについて

- ◆ Since 1997
    - 世界に通用する
    - 社会に貢献する
- 技術を生み出す**

IDEA → ACTION → TECHNOLOGY → PRODUCT

**PacketChaser**

**Cp Monitor SMART**

**NetSkate Visualizer**  
Network Visualization & Management System  
ネットスケツト

**NetSkate Koban**  
イントラネットをターゲットとしたセキュリティシステム

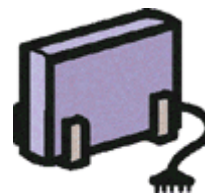
**BUSINESS**

# Cyberが出来る事！

- ◆ 「イントラネットセキュリティ/ネットワーク見」ソリューションの販売



- ◆ ネットワーク検証サービス



- ◆ 共同研究開発



- ◆ 受託研究開発



# NetSkateKoban

## 不正PCの検知 & 接続阻止

◇不正PC接続による、

常時監視

リアルタイム検知

即座に遮断

いつでも操作

もれなく記録

どのような  
ネットワーク  
にも対応可  
能

ネットワークの構成把握

ネットワークのトラフィック把握

Kobanなら  
一元管理が  
可能です！





異常発生時  
管理者へ通知

CpMonitor  
SMART

検知

Winny通信

インターネット

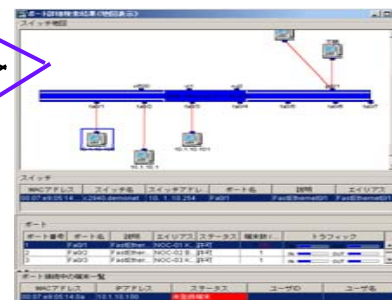
New!!

NetSkateKoban  
サーバ

監視

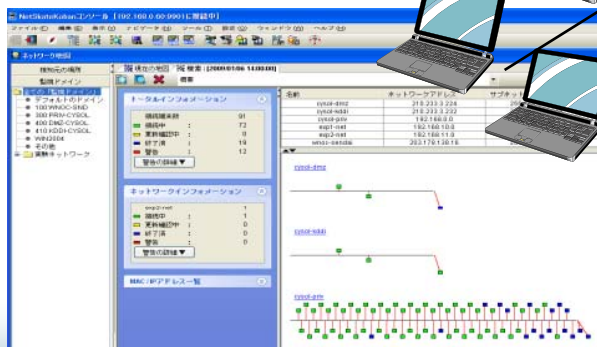


+ NMSモジュール



NetSkateKoban  
センサ

検知



遮断

遮断

Winny

持込

# NetSkateKoban®導入実績

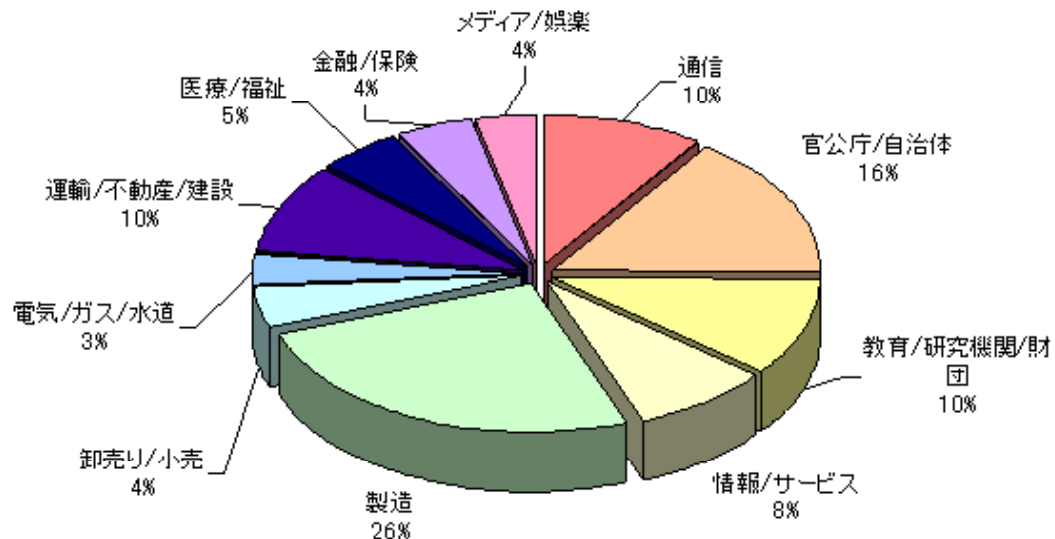
大手電力会社  
数万台の端末を監視

大手製造メーカー  
数千台の端末を監視

官公庁・自治体  
数千台の端末を監視

監視センサ数  
5,000台を突破

150社を超える導入実績



# 大規模事例

No	導入企業	業種	構成例	監視端末数
1	東北電力	電力	SW型	15,000台
2	B	官公庁	ルータ型	10,000台
3	C	官公庁	1Segセンサー	5,000台
4	D	その他製造	SW型	4,000台
5	E	小売業	VLANセンサ	3,000台
6	F	病院	1Segセンサー	1,500台
7	G	電気機器	1Segセンサー	4,000台
8	H	製造	VLANセンサ & 1Segセンサ	7,000台
9	I	電気通信事業社	VLANセンサ	50,000台
10	J	キャリア系SIer	1Segセンサー	20,000台

構成例：センサ型、VLAN型、SW型、ルータ型





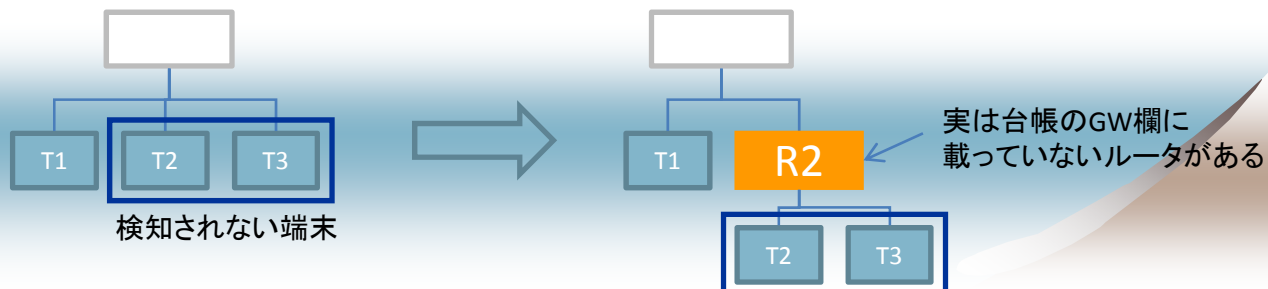
- ◆ もはや**社会的な義務**となっている、情報セキュリティの為組織内ネットワークの把握を簡単に行えるサービス
- ◆ 以下の**重要な基礎情報**をご提供する。



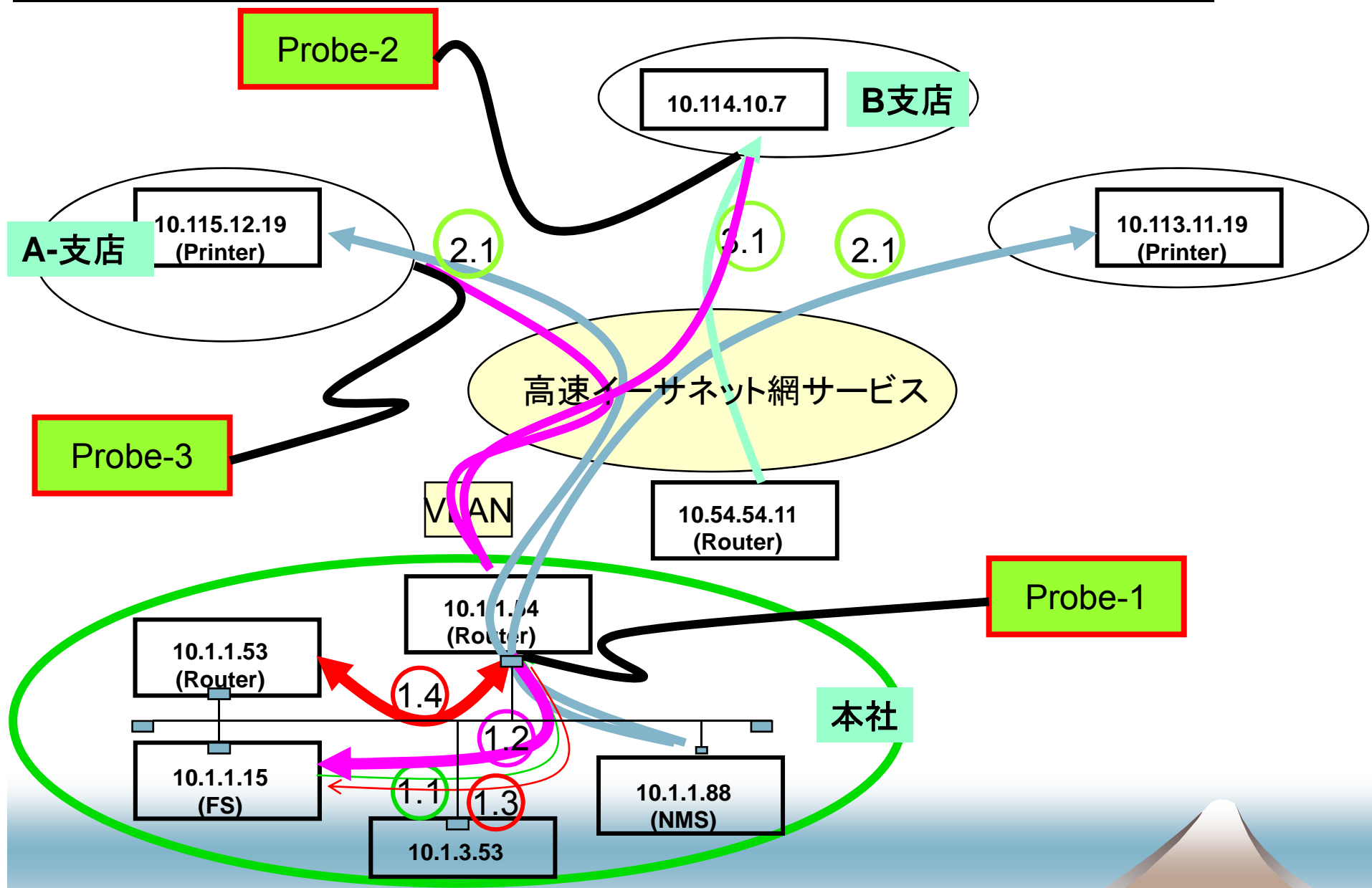
- ★ ネットワーク利用端末一覧 → 想定外の持ち込みPCがないか？
- ★ 内部サーバ・サービス一覧 → 想定外の情報漏洩の危険は？
- ★ ネットワーク帯域利用の多い端末 → 想定外のインターネット利用？
- ★ その他注意すべき端末情報 → 想定外の異常な端末？



- ◆ NetSkateKoban監視結果と機器台帳の比較が行えた
- ◆ 以下の事項を指摘ができた
  - 機器台帳の記載漏れ
  - 機器台帳の記載ミス
    - MACアドレスの入力がなくIPアドレスも正しく記載されていない  
Input RecNo: 3881 <10.201.1.x2>
    - IPアドレスが重複して記載されている
    - 機器台帳上でのMACアドレスとIPアドレスの対応が実際検知されたものと異なる  
Input RecNo: 769      00-00-4c-29-f1-12 10.24.1.204  
Koban Rec :            00-00-4c-e9-f1-12 10.24.1.204
  - 単一のIPアドレスに対して複数のMACアドレスが検知されている  
e.g. Duplicate Koban IP RecNos 177: 00-00-74-e9-cf-67 10.18.1.225  
120: 00-00-74-d6-b9-3a 10.18.1.225
- 台帳記載端末のIPアドレスに到達性がない
- 台帳未記載のGWの検出



# ネットワーク検証サービス Case Study



## ◆ 研究開発実績

### ● IPA, SCOPE, NiCT, 官公庁 等の公募案件の研究開発

- セキュリティ確保を目指したネットワークイベント記録の高信頼な収集と管理技術の開発(総務省)－東北大学との共同提案
- ネットワークモビリティをサポートする新世代ユビキタスネットワーク監視フレームワークに関する研究開発(総務省)－東北大学との共同提案
- 広域インシデント情報共有および分析技術の開発(ICODEF) (IPA)
- ユビキタス時代の介護サービス向上に寄与するIPv6 応用技術の研究開発(NiCT)
- セキュアSYSLOGプロセス監視・管理フレームワークの技術、製品開発(宮城県 地域中核IT企業支援事業)
- 地域医療の高度化に資するセキュアな無線ネットワーク実現に関する調査研究、実証実験ネットワークモニタリング及びセキュリティ評価(総務省)
- 健康福祉のための先進的エージェント・ネットワークに関する研究(総務省)
- 超高速ネットワーク上におけるトラフィック解析に基づいたネットワーク管理のためのイベント検知に関する研究開発(JGN2東北リサーチセンタ)
- 高トラフィック観測・分析法に関する技術調査(IPA)
- 次世代ユビキタスネットワークの監視フレームワークに関する研究(総務省)
- ユビキタス時代の介護サービス向上に寄与するIPv6応用技術の研究開発(NiCT)
- 次世代ネットワーク(JGN IPv6)の管理に関する研究(総務省)
- インテリジェントネットセキュリティ管理(文部科学省 知的クラスタ創成事業)
- インターネット情報インフラ防護のための技術調査(IPA)
- 広域セキュリティ管理のためのセンサレイシステムの技術開発(IPA)
- 高齢者・障害者のための情報カウンセリングセンターのモデル化と介護・福祉情報の取り扱い技術(NiCT)
- JANIシステム開発(NiCT)
- 不正アクセスの高感度検出およびグローバル警戒機構に関する研究(IPA)
- 研究開発用ギガビットネットワークに係る共同研究(NiCT)
- 不正アクセス高感度検出及びグローバル警戒機構研究に関する業務委託(IPA)
- インターネットオリエンテーリング可能な地図構成法に関する研究(IPA)

### ◆ その他受託開発実績

- 大手電力会社様向けイントラネットセキュリティシステムの開発
- 大学向けポータルサイトの開発
- 自治体向け地震センサからのSOAP/XML受信サーバの開発
- 大学向けSNSサイトの開発
- 通信キャリア向けトラフィック情報提供システムの開発
- ホスティングサービスプロバイダのためのサーバ自動監視システムの開発

成果

多数の標準  
多数の技術  
多数の商品

# 国際研究・標準化活動

## International Research and Standardization Activities

### IETF (Internet Engineering Task Force) Activities

- ◆ RFC1567 “X.500 Directory Monitoring MIB.”  
G. Mansfield, S. Kille.
- ◆ RFC1608 “Representing IP Information in the X.500 Directory.”,  
G. Mansfield. et.al.
- ◆ RFC1609 “Charting Networks in the X.500 Directory.”,  
G. Mansfield. et.al.
- ◆ RFC1804 “Schema Publishing in X.500 Directory.”,  
G. Mansfield, et.al.
- ◆ RFC4295 “Mobile IPv6 Management Information Base”,  
G. Mansfield, et.al.
- ◆ RFC4498 “Managed Object Aggregation MIB”,  
G. Mansfield.
- ◆ RFC5427 “Textual Conventions for Syslog Management”,  
G. Mansfield.
- ◆ RFC5488 “Network Mobility (NEMO) Management Information Base”,  
S. Gundavelli, G. Mansfield et.al.

*IETF-netlmm-wg: draft-ietf-netlmm-pmip6-mib-00.txt*

G. Mansfield et.al

## 「共同研究開発」

- ◆ ネットワーク運用・管理・セキュリティ関連課題
- ◆ モバイル端末・モバイルネットワーク情報収集
- ◆ 認証および分散情報管理(LDAP)技術
- ◆ 大規模分散, データベース, アプリケーション

### <共同研究開発事例>

大手通信会社様とのセキュリティ関連共同研究

#### ◆ 成果



10件の国内特許を申請

国内特許取得

6件特許を取得

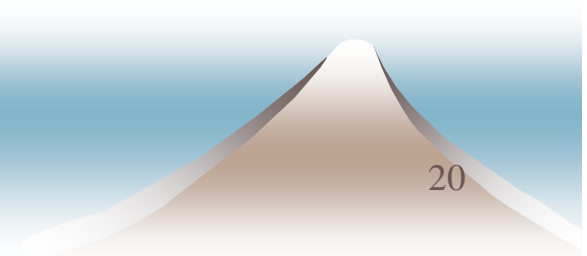
2件の海外特許申請中

海外特許取得

# Awards and Citations

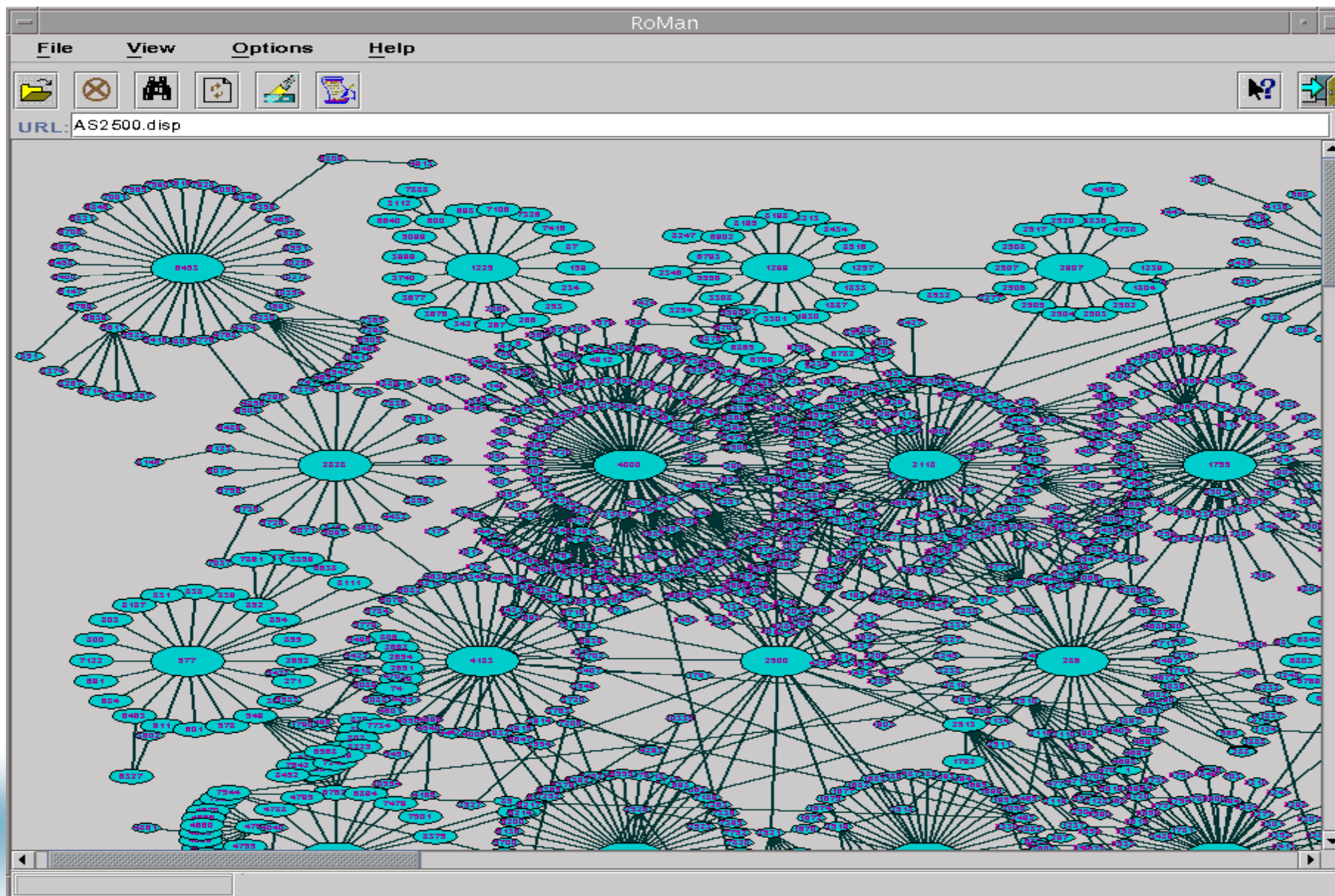
- ・ 平成17年7月 宮城県「新商品特定随意契約制度認定」
- ・ 平成17年9月 セキュリティ商品100選に掲載
  - ・ 株式会社メディアセレクト 2005年9月1日発行 swpr mook pp.113-114に掲載
- ・ 平成17年11月 第8回 七十七ニュービジネス助成金受賞
  - ・ 財団法人七十七ビジネス振興財団
- ・ 平成18年4月第18回「中小企業優秀新技術・新製品賞」において「優秀賞」および「産学連携特別賞」を受賞
  - ・ リそな中小企業振興財団、日刊工業新聞社共催
- ・ 財団法人電気通信振興会発行「情報通信ジャーナル」Vol.24、No.7 (2006.7)、「ICTベンチャー全国十選」に掲載
- ・ 平成18年9月 NiCT研究開発採択
  - ・ 移動体と超大規模ネットワークのためのNetSkateKoban
- ・ 平成18年10月 第10回みやぎものづくり大賞「優秀賞」受賞
- ・ 平成19年5月 マイクロソフトITベンチャー支援事業採択
  - ・ 安全なファイル持ち出し技術
- ・ 平成19年10月「情報化月間」表彰
  - ・ 経済産業省をはじめとする関係6府省が定めた「情報化月間」において、国の情報化促進に貢献したことが認められ表彰されました。
- ・ 平成21年3月 NEDOのイノベーション推進事業(産業技術実用化開発費補助事業)に 当社提案の「安全でオープンな組込みソフトウェアのライフサイクル管理技術」が採択されました。

*End of part two*





# Cyber Technology: Network Cartography-2 (全世界規模のグローバルネットワーク地図)



# Cyber Technology: Tracking Attacks across the Internet

## *Packet Prints (1)*

- ◆ Requirement: Packet print must be Invariant along hops      some header fields change (RFC1812)
  - ◆ Use Invariant part of Packet Header
  - ◆ Optionally use all or part of data

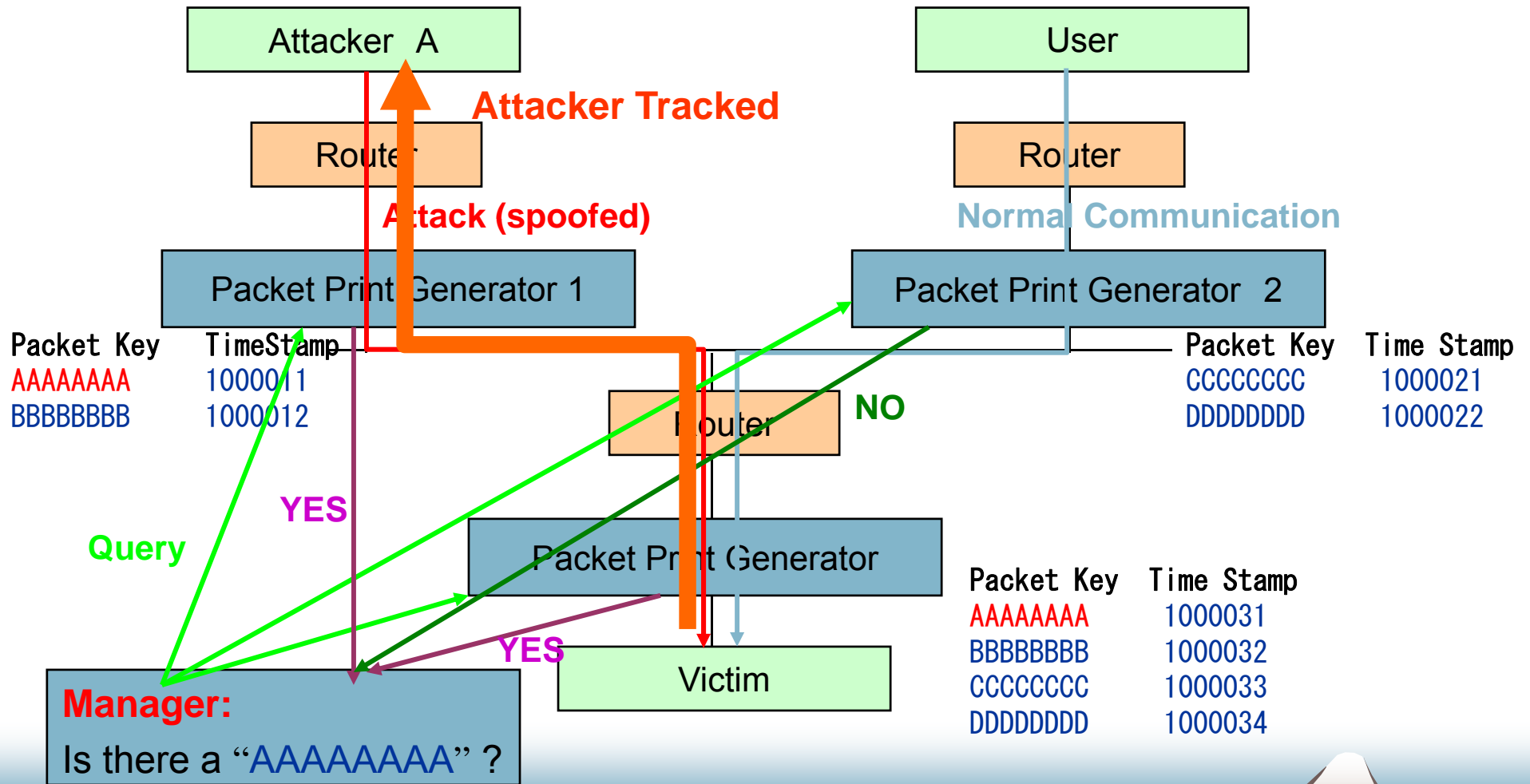
Versions	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time to Live		Protocol	Header Checksum	
Source Address				
Destination Address				



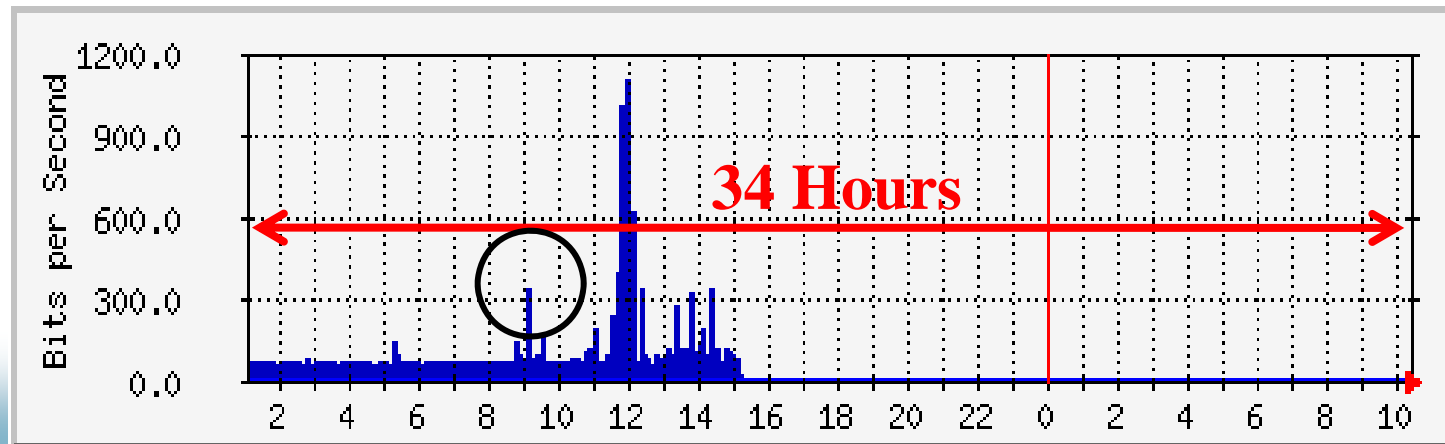
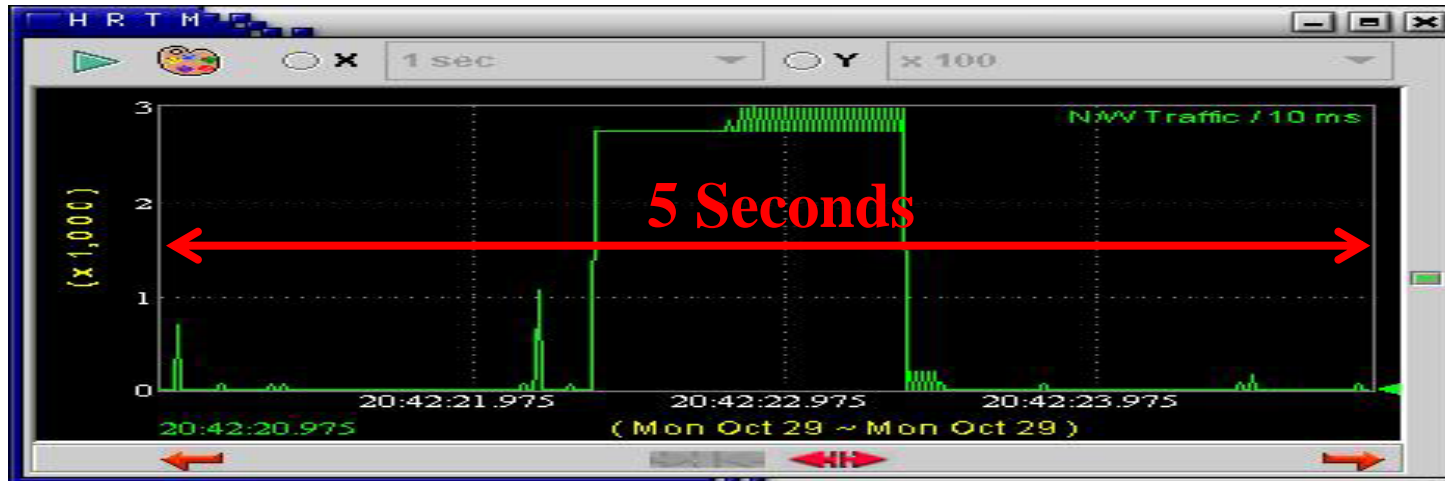
Masked field of IP Header when operating hash function

# Cyber Technology: Tracking Attacks across the Internet

## Packet Prints (2)

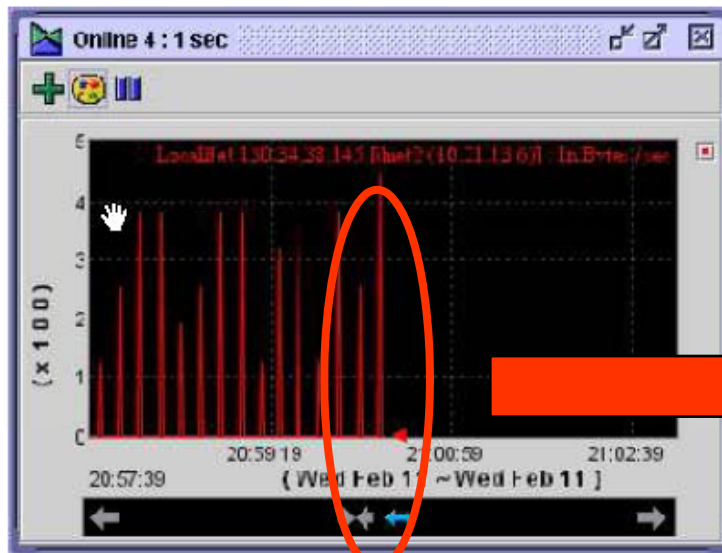


# Cyber Technology: High Resolution Traffic monitoring-1

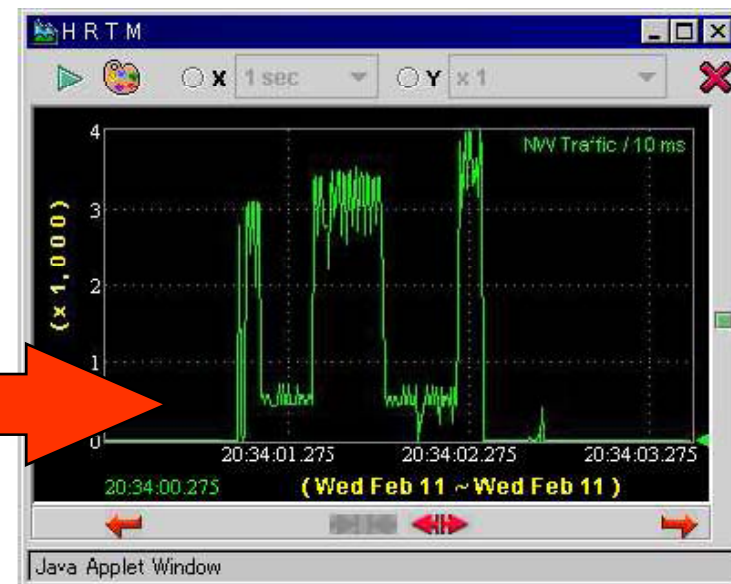


# Cyber Technology: HighResolution Traffic monitoring-2

- ◆ Example) Effect of TAgMO (Time Aggregated MO)
  - (1 sec interval) Only impulse
  - (10ms interval) Clear pattern can be shown



(a) Traffic seen at 1sec interval by RMON polling

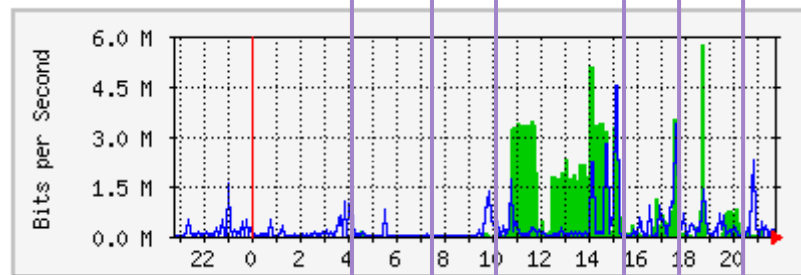


(b) Traffic seen at 10ms intervals by aggregation technique

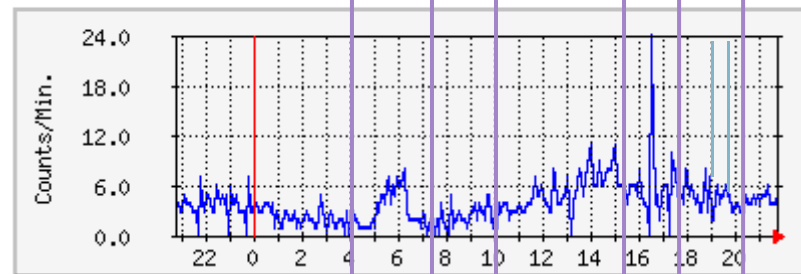
# Cyber Technology: New Statistic for Traffic monitoring

## Category transform

**IPv4 IpOctets**



**IPv4 Dst.Addresses**



### ◆ *Category Transforms*

- *Amplification of symptoms*
- *Easier to correlate/interpret*

Case(1): Only Addresses increases

Case(2): Only Octets increases

Case(3): There is a DoS attack?

*End of part three*

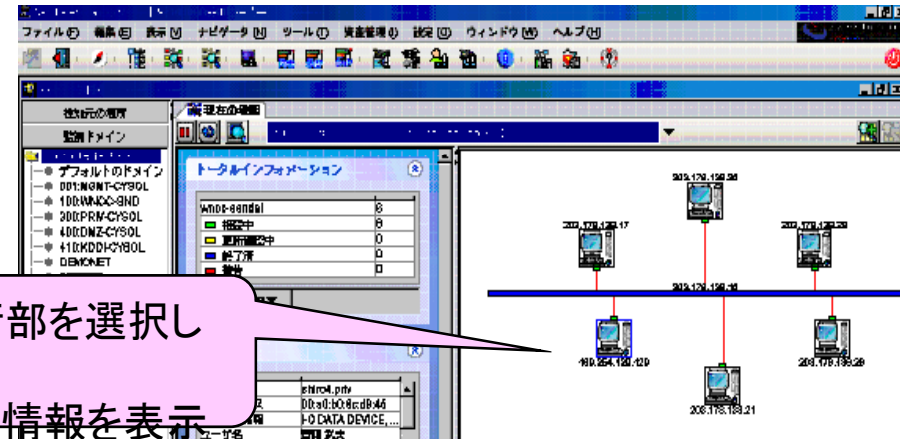
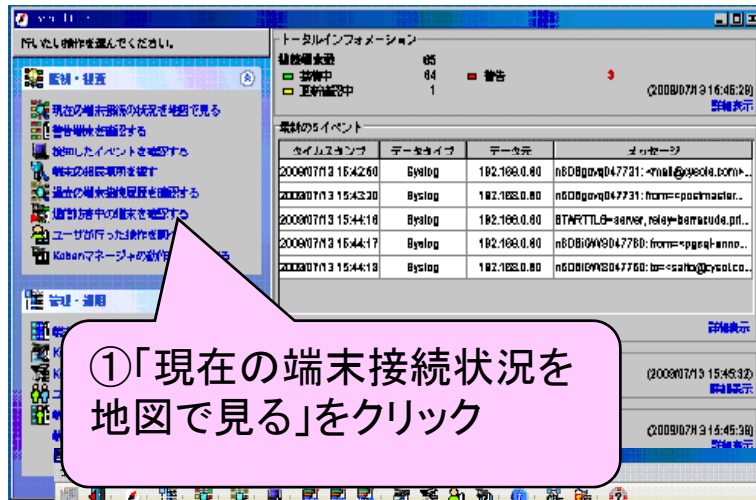
# 運用例①「どこに、何が接続されているか？」を簡単に把握」

PCの検知 & 不正接続阻止

ネットワークの構成把握

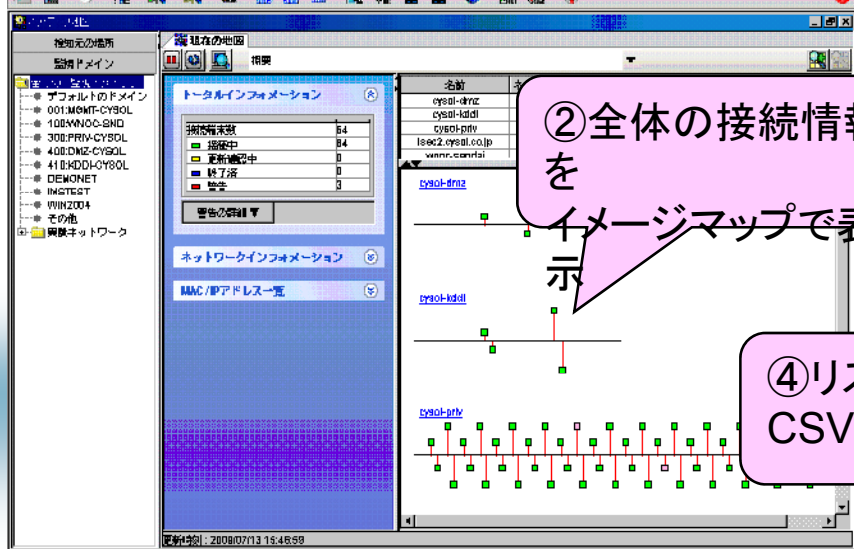
ネットワークのトラフィック把握

Case Study: 企業Aにおいて、技術部ネットワークに現在何台の端末が接続していて、どんな端末が接続しているかを確認したい！

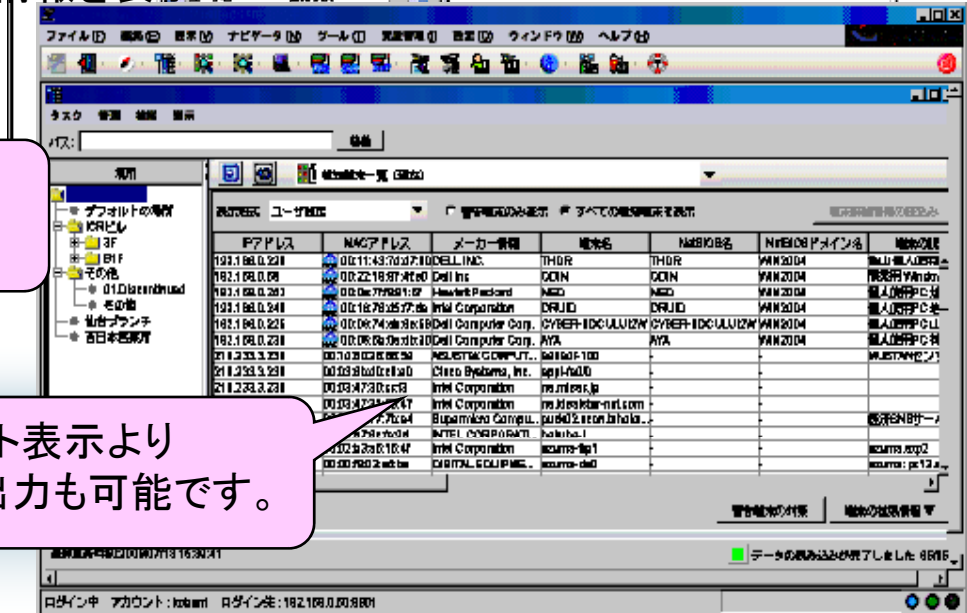


①「現在の端末接続状況を地図で見る」をクリック

③技術部を選択して 詳細な情報を表示



②全体の接続情報を イメージマップで表示



④リスト表示より CSV出力も可能です。

# 運用例②「未登録PCの接続阻止」

PCの検知 & 不正接続阻止

ネットワークの構成把握

ネットワークのトラフィック把握

Case Study: 研究所において社員の不正持込PCの接続を確認して接続を阻止したい

The screenshot shows the NetSkateKoban console interface. The main window displays a network map with a red box highlighting a device at IP 10.1.10.103. A context menu is open over this device, with the option 「接続の遮断」 (Disconnect) selected. Below the map is a table of detected endpoints. A log window at the bottom shows several alarm messages, with the most recent one stating: 「未登録端末(00:02:b3:a6:15:63/10.1.10.100)を検知しました。」 (Detected unregistered device (00:02:b3:a6:15:63/10.1.10.100)).

IPアドレス	端末名	MACアドレス	ステータス	ログオン名	端末の説明	メーカー情報	ユーザID	ユーザ名	開始時刻	更新時刻	割り当てIP
10.1.60.221		00:10:c2:04:11:64	未登録端末			WILLNET, INC.	不明	不明	2009-11-06 14:49:44	2010-01-14 11:30:17	
10.1.60.201		00:10:c2:04:09:0c	未登録端末			WILLNET, INC.	不明	不明	2009-11-06 14:49:44	2010-01-14 11:30:17	
10.1.10.103		00:a0:b0:6c:e8:e9	未登録端末			I-O DATA DEVIC...	不明	不明	2010-01-14 11:30:59		
10.1.10.100		00:02:b3:a6:15:63	未登録端末			Intel Corporation	不明	不明	2010-01-14 11:30:47		

Log messages:

- 2010/01/14 11:17:20 Koban通知 アクション(自動): データ収集成功-イベント監視アラーム(閾値): 10.1.10.100, ポリシー名: Disk space
- 2010/01/14 11:18:50 イベント監視アラーム (Ping) 警告! ルール違反が起きました [Ping到達性監視] イーサネットスイッチ一覧: 全ての「場所」
- 2010/01/14 11:18:50 イベント監視アラーム (Ping) 警告! ルール違反が起きました [Ping到達性監視] イーサネットスイッチ一覧: 全ての「場所」
- 2010/01/14 11:30:47 Koban アラーム 未登録端末(00:02:b3:a6:15:63/10.1.10.100)を検知しました。
- 2010/01/14 11:30:59 Koban アラーム 未登録端末(00:a0:b0:6c:e8:e9/10.1.10.103)を検知しました。

①「未登録端末」が接続

②営業部ネットワークで警告が出ていることを確認!

③「接続の遮断」をクリックして不正端末の排除!

# 運用例③ - 「どこに、何が接続されているか？」が簡単に検索できます。

PCの検知 & 不正接続阻止

ネットワークの構成把握

ネットワークのトラフィック把握

Case Study: 大学Bにおいて、端末(10.1.10.202)の接続位置を特定したい!

The screenshot shows the NetSkateKoban console interface. A search window is open, and the search results are displayed in a table. The search criteria are IP address 10.1.10.202. The results show that this IP is connected to port Fa0/7 of switch c2940.demonet. The traffic volume for this connection is 100 kbps.

① IPアドレス(10.1.10.202)を入力して「ポートの特定」をクリック

② どのスイッチ

③ 何番ポート(研究室)

④ トラフィック量

⑤ 10.1.10.202の端末

MACアドレス	スイッチ名	スイッチアドレス	ポート名	説明	エリアス
08:00:46:4d:ed:78	c2940.demonet	10.1.10.254	Fa0/7	FastEthernet0/7	NOC-PP-03

ポート名	説明	エリアス	ステータス	端末数 / 警告...	トラフィック
1	Fa0/1	FastEthernet... NOC-01 Kob...	許可	1 (1)	IN [ ] OUT [ ]
2	Fa0/2	FastEthernet... NOC-02 BB...	許可	0	IN [ ] OUT [ ]
3	Fa0/3	FastEthernet... NOC-03 Kob...	許可	1	IN [ ] OUT [ ]
4	Fa0/4	FastEthernet... NOC-04 Wir...	許可	1	IN [ ] OUT [ ]
5	Fa0/5	FastEthernet... NOC-PP-01	許可	0	IN [ ] OUT [ ]
6	Fa0/6	FastEthernet... NOC-PP-02	許可	0	IN [ ] OUT [ ]
7	Fa0/7	FastEthernet... NOC-PP-03	許可	1	IN [ ] OUT [ ]
8	Fa0/8	FastEthernet... NOC-PP-04	許可	0	IN [ ] OUT [ ]
9	Gi0/1	GigabitEther... UP Link	許可	5 (1)	IN [ ] OUT [ ]
10	Nu0	Null0	許可	0	IN [ ] OUT [ ]
11	Vl1	Vlan1	切断	0	IN [ ] OUT [ ]
12	M500	Vlan500	許可	0	IN [ ] OUT [ ]

MACアドレス	IPアドレス	ステータス	ユーザID	ユーザ名
08:00:46:4d:ed:78	10.1.10.202	正常	kadota	門田健二

# 運用例④ - どこに、何が接続されているか？」が簡単に把握できます。(物理構成)

PCの検知 & 不正接続阻止

ネットワークの構成把握

ネットワークのトラフィック把握

NetSkateKobanコンソール [192.168.0.60:9901に接続中]

ファイル(F) 編集(E) 表示(V) ナビゲータ(N) ツール(T) 設定(O) ウィンドウ(W) ヘルプ(H)

ポート詳細検索結果

MACアドレス	スイッチ名
00:a0:de:06:c7:fa	catalyst35-2.priv.cysol...

ポート情報一覧

ポート番号	ポート名	説明
6	Fa0/5	FastEthernet0/5
7	Fa0/6	FastEthernet0/6
8	Fa0/7	FastEthernet0/7
9	Fa0/8	FastEthernet0/8
10	Fa0/9	FastEthernet0/9
11	Fa0/10	FastEthernet0/10
12	Fa0/11	FastEthernet0/11
13	Fa0/12	FastEthernet0/12
14	Fa0/13	FastEthernet0/13

ポート接続中の端末一覧

MACアドレス	IPアドレス
00:a0:de:06:c7:fa	192.168.0.1

ポート詳細検索結果(地図表示)

スイッチ地図

c2940.demonet:10.1.10.254

fa0/1 fa0/2 fa0/3 fa0/4 fa0/5 fa0/6 fa0/7

10.1.10.100 10.1.10.101

どの研究室

スイッチ

MACアドレス	スイッチ名	スイッチアドレ...	ポート名	説明	エリアス
00:07:e9:05:14:...	c2940.demonet	10.1.10.254	Fa0/1	FastEthernet0/1	FastEthernet0/1

ポート

ポート番号	ポート名	説明	エリアス	ステータス	端末数/...	トラフィック
1	Fa0/1	FastEther...	NOC-01 K...	許可	1 (1)	IN OUT
2	Fa0/2	FastEther...	NOC-02 B...	許可	1	IN OUT
3	Fa0/3	FastEther...	NOC-03 K...	許可	1	IN OUT

ポート接続中の端末一覧

MACアドレス	IPアドレス	ステータス	ユーザID	ユーザ名
00:07:e9:05:14:0a	10.1.10.100	未登録端末		

トラフィック量

*End of part four*

# The Keywords

*Simple is beautiful*

*Nurture your ideas*

# The Keywords

*We reject kings, presidents and voting. We believe in*

*Rough Consensus &  
Running Code*

# The Keywords

みんながやってることはやるな！

*Do Not Follow the crowd!!*

当時、インターネットはだれもやってなかった  
インターネットがやってきて、その波に乗った

At that time no one was doing Internet  
We rode on the Internet wave

# The Keywords

。。。やるなら

at the right time

at the right place

do the right thing

# The Keywords

Know Thyself :

*Strengths & Weaknesses*

# A Model for Business



**Small world !!**

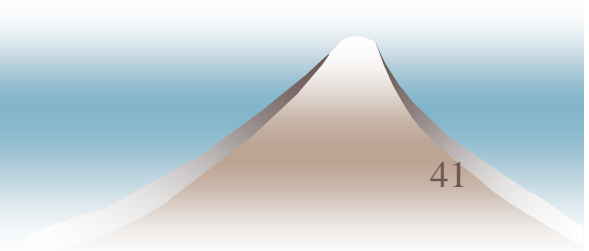


# The delta principle

Step wise refinement

Small (delta ) steps

Quasi-static equilibrium



# Moving Target

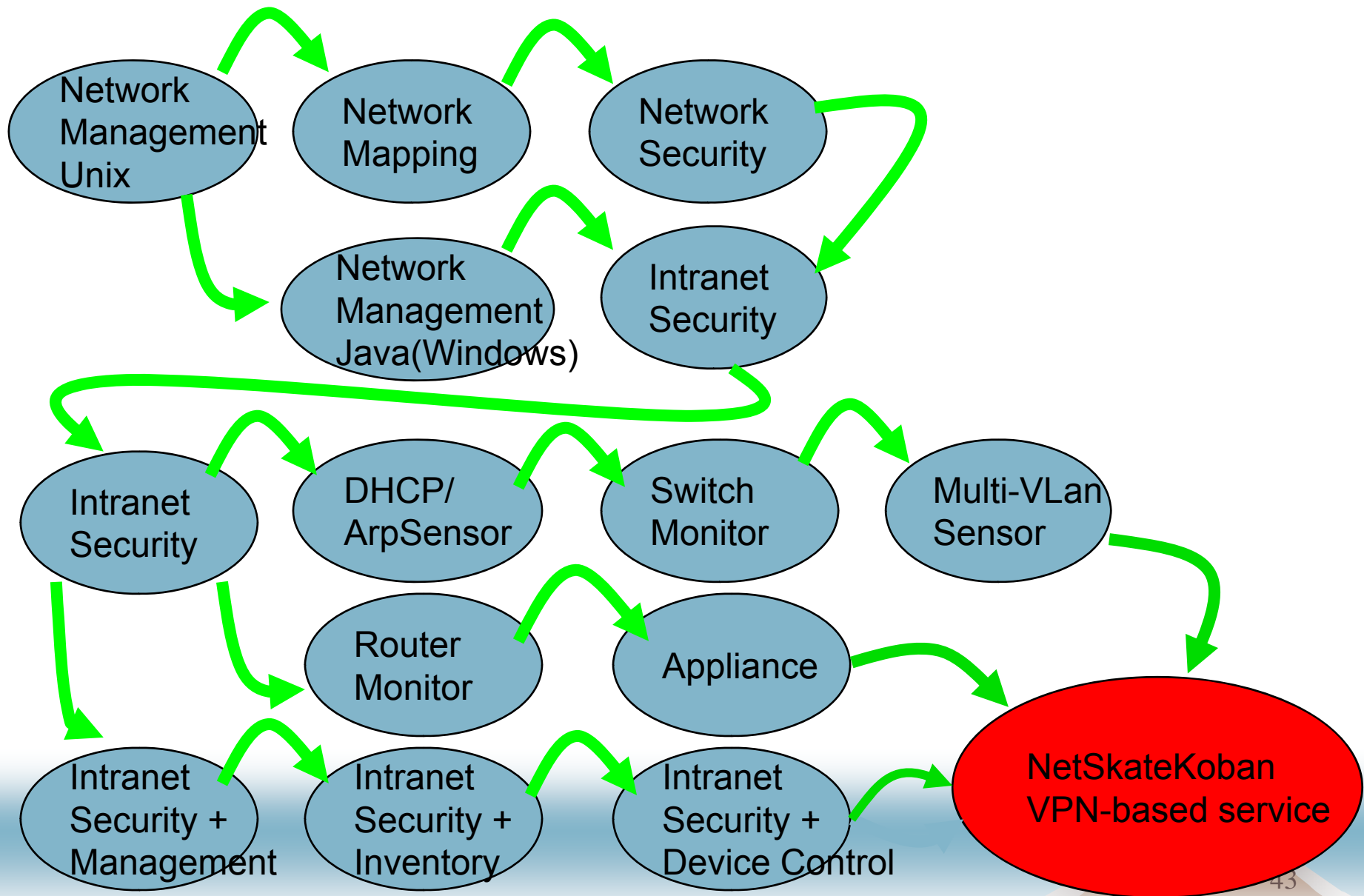
Technology is changing

Market is changing

Requirements are changing

***You must change! ADAPT !***

# The Evolution



# 大学 勉強 ベンチャー

*There is no end to learning*

*You can learn from anyone*

Marriage of ideas/potential/possibilities  
才能の融合

Network vs Software

Age and wisdom vs Youth and energy

Japan vs India

Perfection vs Optimism



*End of part five*

# About software

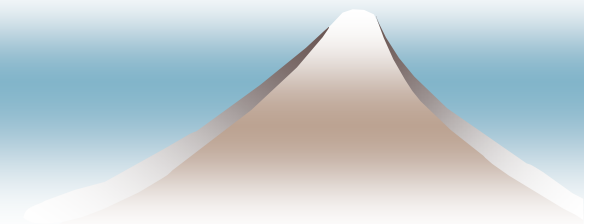
Software: Art *not* Science

Information *vs* data [garbage]



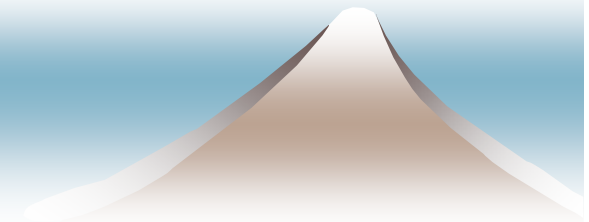
# About Software Project Planning

- ◆ Understand the beast.
  - Confirm and reconfirm the understanding is correct
  
- ◆ Resource Management and planning
  - Software projects are difficult to plan and manage.  
(Estimation is impossible.)  
Back-calculation in general!  
Given time, Given budget,
  
- ◆ System design the 80-20 rule
  - *"if anything can go wrong, it will!"* Murphy's laws
  - Figure out the 80%
  - Exception cases
  
- ◆ The next life: Problem shooting/Debugging Effective logging
- ◆ Scalability of system



# About Software projects : *Team-work & communication*

- ◆ Software development is teamwork
- ◆ Members will come and go but the team remains!
- ◆ For good team work – use *common* sense  
*don't be original !*  
*Common* sense = *Conventions*
- ◆ Use *Conventions* to work *efficiently* in teams
  - working language (for international teams)
  - coding conventions
- ◆ ***Be liberal in what you accept, be conservative in what you send!***
- ◆ And meet deadlines !!



# About Software: *Criteria for well written program*

## 1. Easy to understand **by others**

*Common Sense, Conventions*

*Comments*

*Size of a block- visible within one window*

## 2. Easy to maintain:

*Modularized*

3. Correct/Meets the requirements

4. Easy to use

5. Error handling is done well

6. Efficiency/Performance

