
Feasibility Study of DoS attack by P2P network.

2009/01/20

**Hitachi Incident Response Team
Masato Terada**

<http://www.hitachi.com/hirt/>



Opening

P2P file exchange software are spreading on the Internet. The requirements of investigation reports such as threats about P2P network are increasing.

In this presentation, we show some experiment results about P2P network enforced in StarBED which is a Large Scale Network Experiment Environment.

- DoS attack by P2P network
- Disable P2P network by P2P own protocol



Contents

1. **Problems of P2P network**
2. **Our activity against the problems**
3. **About P2P file exchange software "Winny" & "Share"**
4. **About StarBED**
5. **DoS attack by P2P network**
6. **Disable P2P network by P2P own protocol operation**
7. **Recovery capability of P2P network**

This presentation shows a solution approach against problems in PURE P2P network.

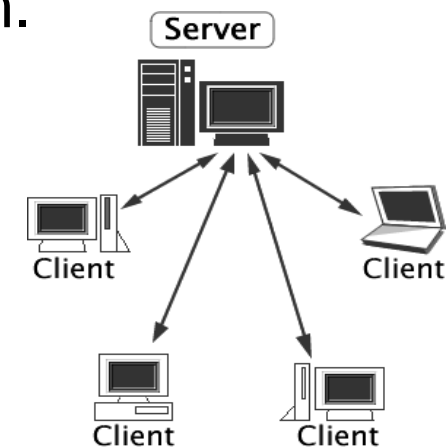


□ P2P file exchange software

A popular technology for file exchange/sharing.
An alternative to client-server network design.

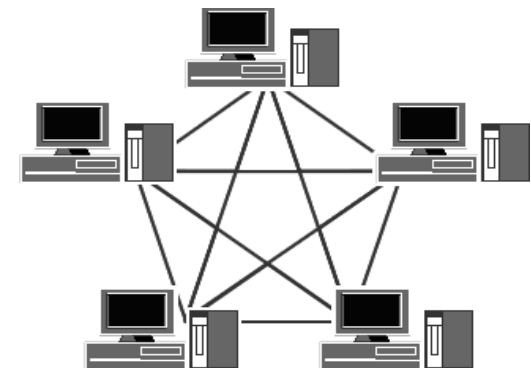
■ Hybrid type

Central server has file and node lists.
Ex. Napster etc.



■ Pure type (Unstructured type)

Without the need for special server devices.
Ex. Winny, Share, Gnutella etc.



□ What are the problems of PURE type P2P network ?

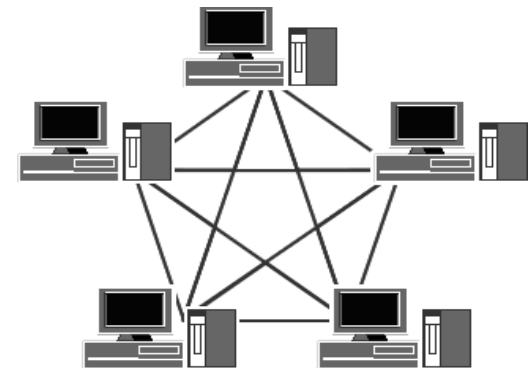
We should have good understanding of the problems of PURE type P2P network.

■ Distribution of files of copyright violation

P2P user downloads computer software, music and movie files etc.

■ Spread of malware

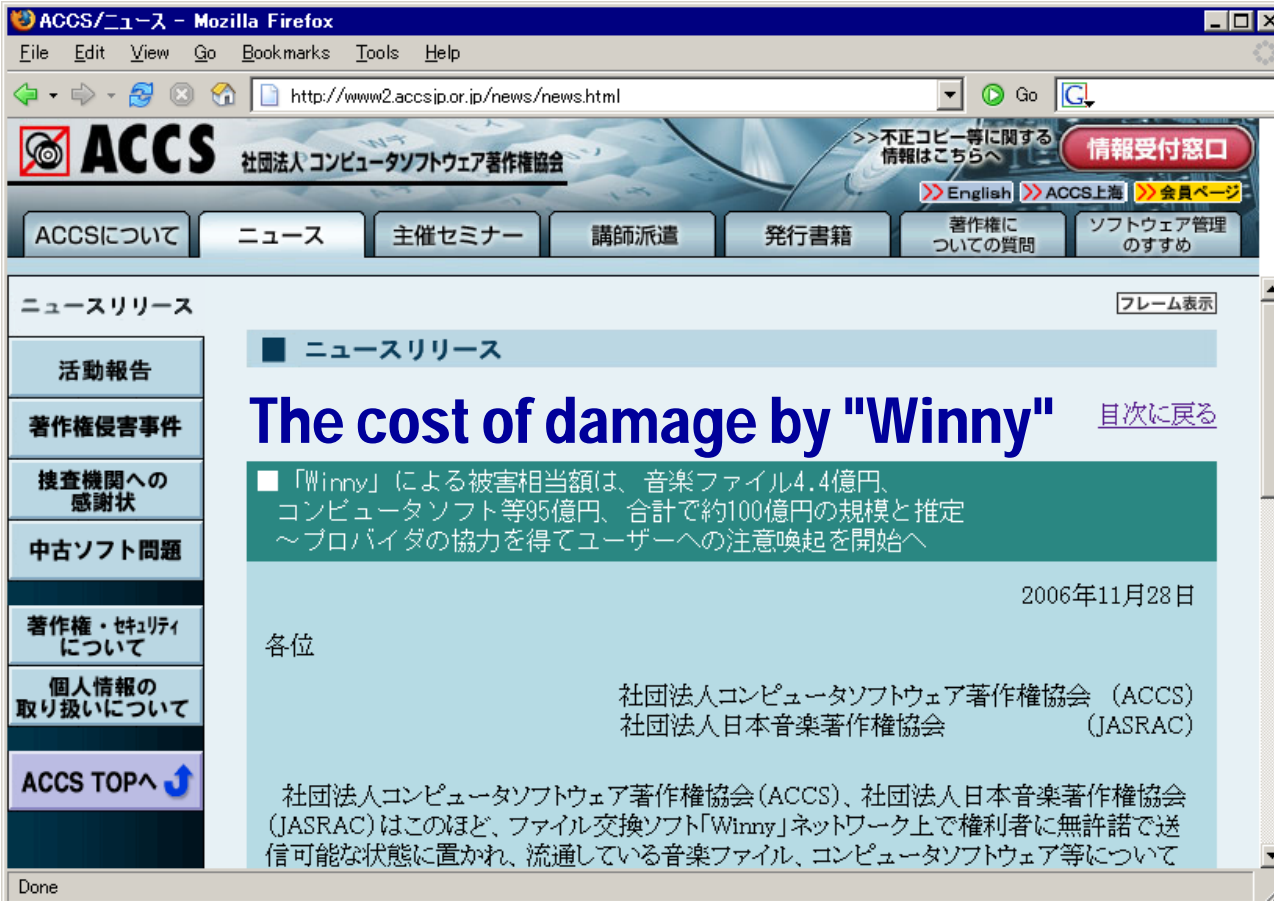
Malware is trigger to leak information, delete files and do DDoS etc.



Anonymity of PURE type P2P seems to cause these problems.

□ Distribution of files of copyright violation

P2P user downloads software applications, music and movies files etc.



The screenshot shows a Mozilla Firefox browser window displaying the ACCS (Association for Copyright Clearance Center of Japan) website. The page is titled "The cost of damage by \"Winny\"". The main content area contains the following text:

■ 「Winny」による被害相当額は、音楽ファイル4.4億円、コンピュータソフト等95億円、合計で約100億円の規模と推定
～プロバイダの協力を得てユーザーへの注意喚起を開始へ

2006年11月28日

各位

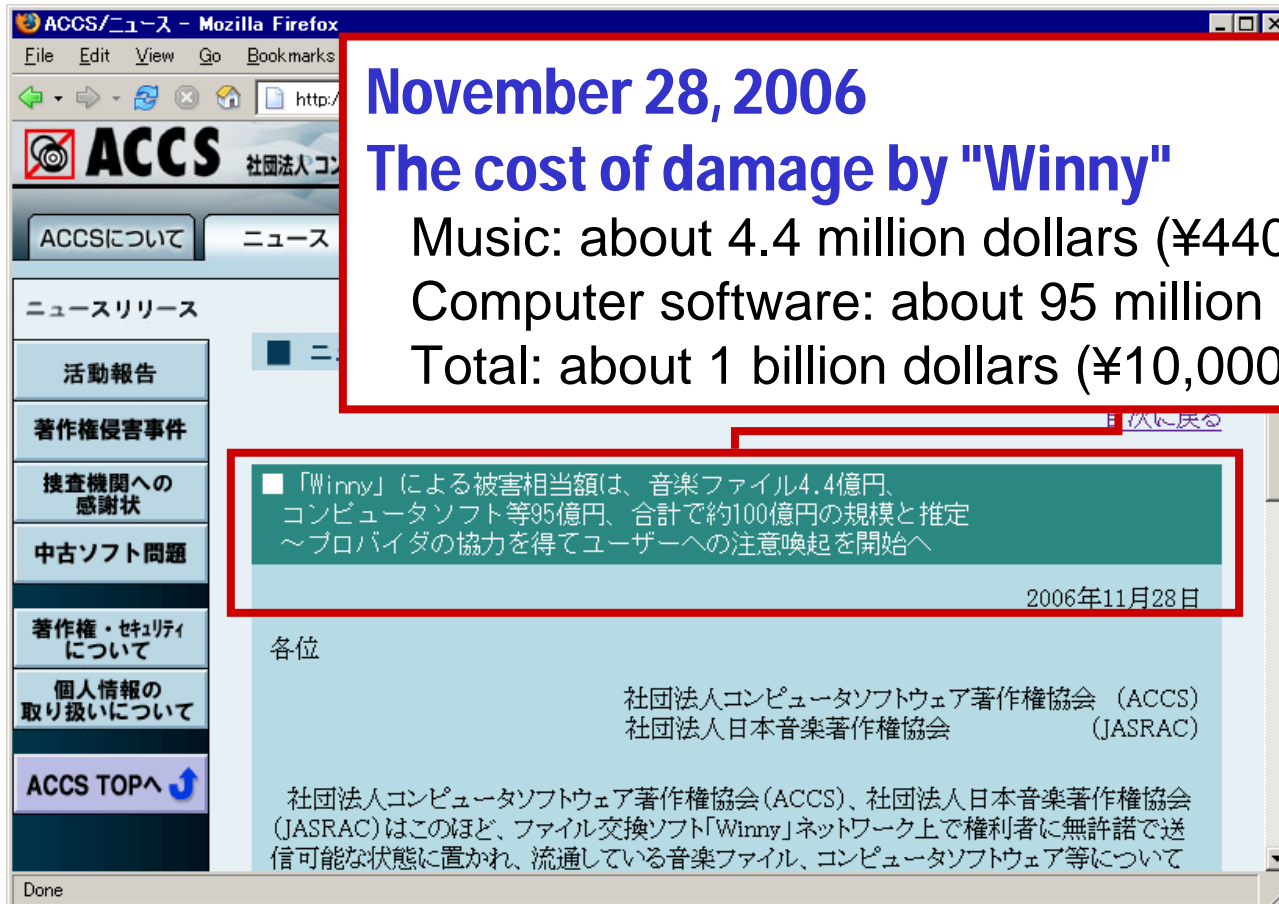
社団法人コンピュータソフトウェア著作権協会 (ACCS)
社団法人日本音楽著作権協会 (JASRAC)

社団法人コンピュータソフトウェア著作権協会 (ACCS)、社団法人日本音楽著作権協会 (JASRAC)はこのほど、ファイル交換ソフト「Winny」ネットワーク上で権利者に無許諾で送信可能な状態に置かれ、流通している音楽ファイル、コンピュータソフトウェア等について

The browser's address bar shows the URL: http://www2.accs.jp.or.jp/news/news.html. The page header includes the ACCS logo and navigation links for "English", "ACCS上海", and "会員ページ". A sidebar on the left contains various menu items such as "活動報告", "著作権侵害事件", and "ACCS TOPへ".

□ Distribution of files of copyright violation

P2P user downloads software applications, music and movies files etc.



November 28, 2006
The cost of damage by "Winny"

Music: about 4.4 million dollars (¥440,000,000).
Computer software: about 95 million dollars (¥9,500,000,000).
Total: about 1 billion dollars (¥10,000,000,000).

「Winny」による被害相当額は、音楽ファイル4.4億円、コンピュータソフト等95億円、合計で約100億円の規模と推定
～プロバイダの協力を得てユーザーへの注意喚起を開始へ

2006年11月28日

各位

社団法人コンピュータソフトウェア著作権協会 (ACCS)
社団法人日本音楽著作権協会 (JASRAC)

社団法人コンピュータソフトウェア著作権協会 (ACCS)、社団法人日本音楽著作権協会 (JASRAC)はこのほど、ファイル交換ソフト「Winny」ネットワーク上で権利者に無許諾で送信可能な状態に置かれ、流通している音楽ファイル、コンピュータソフトウェア等について

□ Spread of malware

Malware is trigger to leak information, delete files and do DDoS etc. **JPCERT/CC reported this problem at 18th FIRST Annual Conference (June 2006).**

18th Annual FIRST Conference
June 25-30, 2006
Renaissance Harborplace Hotel
Baltimore, Maryland USA

JPCERT/CC

Threats of P2P File Sharing Software

-- a Japanese Situation About "Winny"--

JPCERT/CC is an independent non-profit organization, acting as a national point of contact for the other CSIRTs in Japan. Since its establishment in 1992, the center has been gathering computer incident and vulnerability information, issuing security alerts and advisories, and providing incident responses as well as education and training to raise awareness of security issues.

Keisuke Kamata
Yuichi Miyagawa

JPCERT Coordination Center
Japan

Copyright© 2006 JPCERT/CC All rights Reserved 1

□ Spread of malware

Malware is trigger to leak information, delete files and do DDoS etc. **Antinny spreads via Winny network and is included in ZIP file etc.**

JPCERT/CC™

Summary of Antinny

- Spread in mid 2003.
- A “Trojan horse” virus that spread via Winny.
- Leaks information, deletes files, does DDos, etc.
- Over 50 similar derived viruses.
 - Viruses are designed to be executed by the user, therefore does not require special knowledge (such as designing attacks on vulnerabilities) and is easily created.
- Over a 170,000 PCs were confirmed to be infected.
- Information leaked from companies, autonomies, and individuals causing serious social problem.

Contents

1. Problems of P2P network
2. Our activity against the problems
3. About P2P file exchange software "Winny" & "Share"
4. About StarBED
5. DoS attack by P2P network
6. Disable P2P network by P2P own protocol operation
7. Recovery capability of P2P network

This presentation shows a solution approach against problems in PURE P2P network.



- Some organizations have started to cooperate, to solve these problems since summer of 2006.



HITACHI



- **1st step (2006-2007)**

Feasibility study of Winny & Share P2P network observation

- **2nd step (2008-)**

Encouragement of malware incident prevention on P2P network

- 1st step

Feasibility study of Winny & Share P2P network observation

- How many nodes exist over Winny and Share network ?

Winny

180,000 nodes/day

Share

200,000 nodes/day

□ 2nd step

Encouragement of malware incident prevention on P2P network.

- Malware spread and information leakage problems exist in the overlay network such as P2P network including Winny. Recently, there is many observation data of nodes/files, but there is not quality data about the threat such as DoS of the P2P network (overlay network) itself. We examine the control possibility of P2P network (overlay network) by P2P network (overlay network) in this experiment.

□ 2nd step

Encouragement of malware incident prevention on P2P network.

□ Experiment ONE

Winny: Index poisoning DDoS Attacks

□ Experiment TWO

Winny: Disable P2P network by P2P own protocol operation

- Sending many close connection requests
- Sending one message with exploit the vulnerability (JVN#74294680)

□ Experiment THREE

Winny: Recovery capability of P2P network

Contents

1. Problems of P2P network
2. Our activity against the problems
3. About P2P file exchange software "Winny" & "Share"
4. About StarBED
5. DoS attack by P2P network
6. Disable P2P network by P2P own protocol operation
7. Recovery capability of P2P network

This presentation shows a solution approach against problems in PURE P2P network.



□ Characteristics of Winny and Share

■ PURE P2P type

No index/central server to manage the network

■ Simple GUI

Word Search and Search results

■ Anonymity

Multi-hop proxies or re-publish of cached contents

Encrypted communication channel

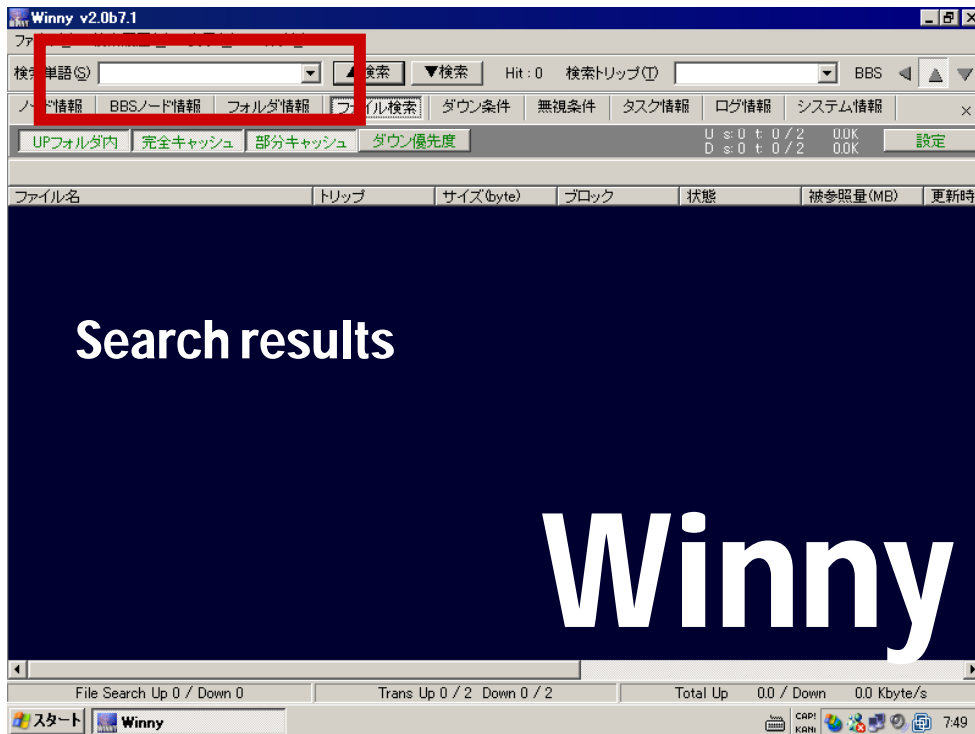
□ Characteristics of Winny and Share

■ PURE P2P type

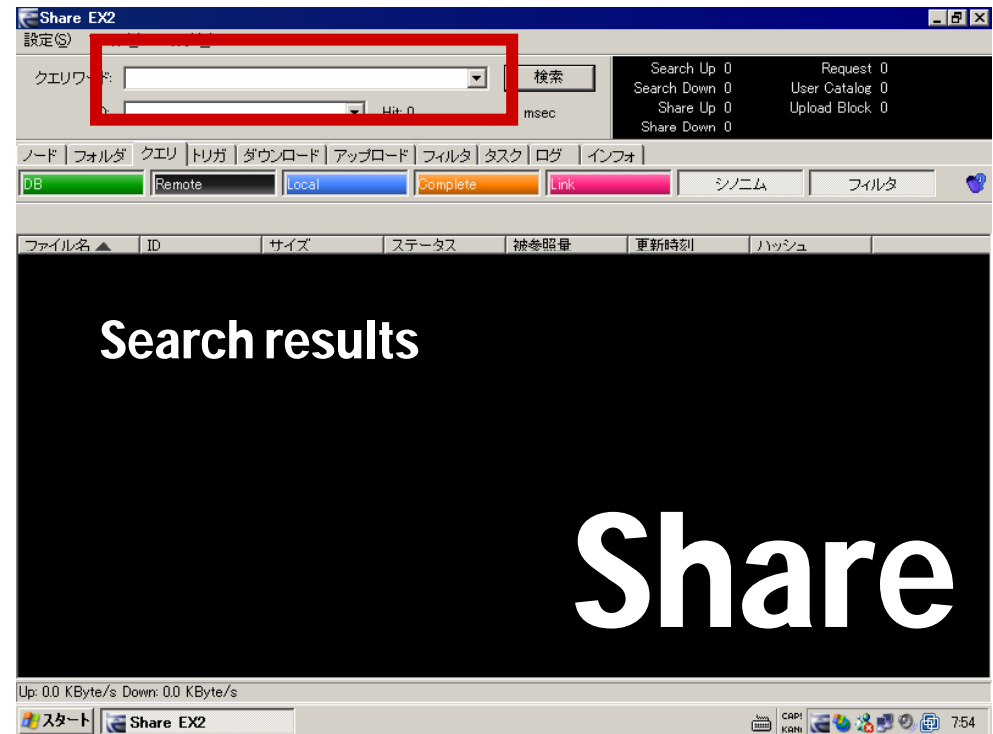
No index/central server to manage the network

■ Simple GUI

Word Search



Word Search



3.

About P2P file exchange software "Winny" & "Share"



Characteristics of Winny and Share

- PURE P2P type
No index/central server to manage the network
- Simple GUI

Word Search

The screenshot shows the Winny v2.0b7.1 interface. A search for '仁義なき' has been performed, resulting in 180 hits. The search results are displayed in a table with columns for filename, drop, size, block, and status. The word 'Search results' is overlaid on the table. A red box highlights the search input field.

ファイル名	ドロップ	サイズ(byte)	ブロック	状態
仁義なきのドキュメント.zip	Kxm9pWJTh	937,046,219		仮想ファイル
仁義なきのドキュメント.zip	xMmmFN2o0y	32,328,432		仮想ファイル
仁義なきのドキュメント.zip		1,559,340		仮想ファイル
仁義なきのドキュメント.zip		3,112,092		仮想ファイル
(0011)のデスクトップ(060214-1028).jpg	Zav69nAG0h	263,929		仮想ファイル
仁義なきのドキュメント.zip	3urtLL611u	95,948,790		仮想ファイル
仁義なきのドキュメント.zip	soKkXtuNh0	6,229		仮想ファイル
仁義なきのドキュメント.zip	gDzHfRNvR	170,779		仮想ファイル
仁義なきのドキュメント.zip	jd7heIok6k	791,940,977		仮想ファイル
仁義なきのドキュメント.zip		451,009,903		仮想ファイル
仁義なきのドキュメント.zip	OyuZRHsHof	559,392,882		仮想ファイル
仁義なきのドキュメント.zip		593,811,204		仮想ファイル
仁義なきのドキュメント.zip		101,208		仮想ファイル
仁義なきのドキュメント.zip		17,825,792		仮想ファイル
仁義なきのドキュメント.zip	0FRM0JC#B	4,291,728		仮想ファイル
仁義なきのドキュメント.zip	nkn84BPod5	1,627,951,111		仮想ファイル
仁義なきのドキュメント.zip		1,626,861,503		仮想ファイル
仁義なきのドキュメント.zip		176,825		仮想ファイル
仁義なきのデスクトップ(051001-1652).jpg	YuWGJVm876	185,560		仮想ファイル
仁義なきのデスクトップ(041126-0150).jpg	FrM8R0Frdw	185,560		仮想ファイル
仁義なきのデスクトップ(060204-2030).jpg	Rfb7vTOT8	5,200		完全キャッシュ
仁義なきのデスクトップ(050822-2157).jpg	z7es4phjds	5,200		仮想ファイル
Ownerのドキュメント.zip	olyaGOSQV6	15,200		仮想ファイル
Ownerのドキュメント.zip	xl605bT3z	104		仮想ファイル
Ownerのドキュメント.zip	WdISElIP0x	631		仮想ファイル
Ownerのドキュメント.zip	3vm030lbXp	645		仮想ファイル
Ownerのドキュメント.zip	00TdbIeqTj	456		仮想ファイル
Ownerのドキュメント.zip	kyWvcAht8N	34,477,600		仮想ファイル
Ownerのデスクトップ(060205-1041).jpg	j9pmfQmz0q	190,524		仮想ファイル
Ownerのデスクトップ(051219-0441).jpg	7ny5Rz2B	407,943		仮想ファイル
Ownerのデスクトップ(051017-0750).jpg	00TdbIeqTj	139,672		仮想ファイル
Ownerのデスクトップ(051016-0813).jpg	00TdbIeqTj	25,284		仮想ファイル

Winny

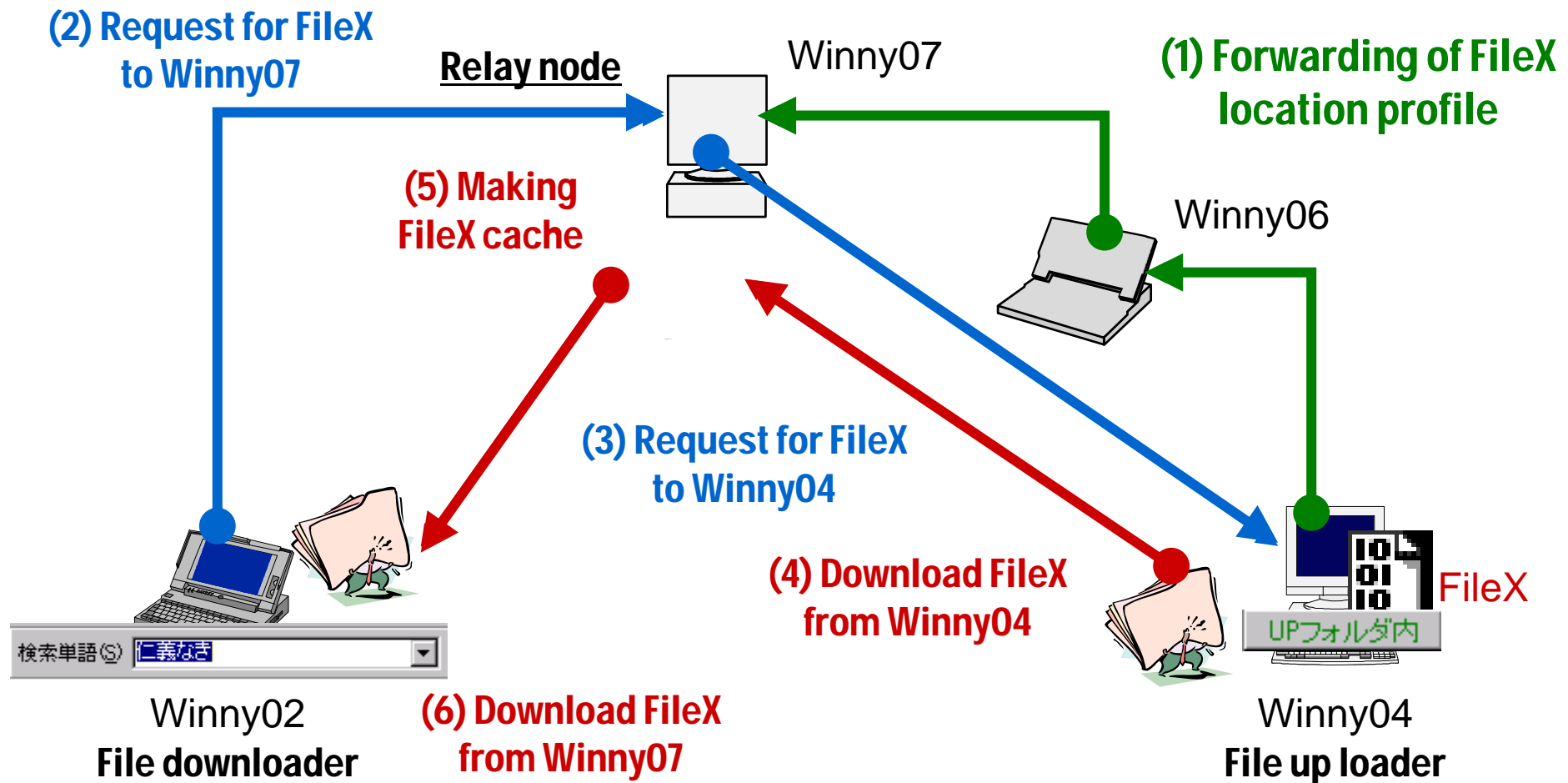
Word Search

The screenshot shows the Share EX2 interface. A search for '仁義なき' has been performed, resulting in 0 hits. The search results are displayed in a table with columns for filename, ID, size, status, reference number, update time, and hash. The word 'Search results' is overlaid on the table. A red box highlights the search input field.

ファイル名	ID	サイズ	ステータス	被参照数	更新時刻	ハッシュ
-------	----	-----	-------	------	------	------

Share

□ P2P mechanism of Winny to accomplish anonymity



Contents

1. Problems of P2P network
2. Our activity against the problems
3. About P2P file exchange software "Winny" & "Share"
4. About StarBED
5. DoS attack by P2P network
6. Disable P2P network by P2P own protocol operation
7. Recovery capability of P2P network

This presentation shows a solution approach against problems in PURE P2P network.



- ❑ **StarBED --- A Large Scale Network Experiment Environment**
 - In StarBED, there are many actual computers, and switches which connect these computers.
 - There are 680 actual PCs in StarBED, in order to realize a large-scale topology. Furthermore, each node on StarBED can run 10 virtual machines with VMware, which enables constructing a large-scale experiment topology.

<http://www.starbed.org/>



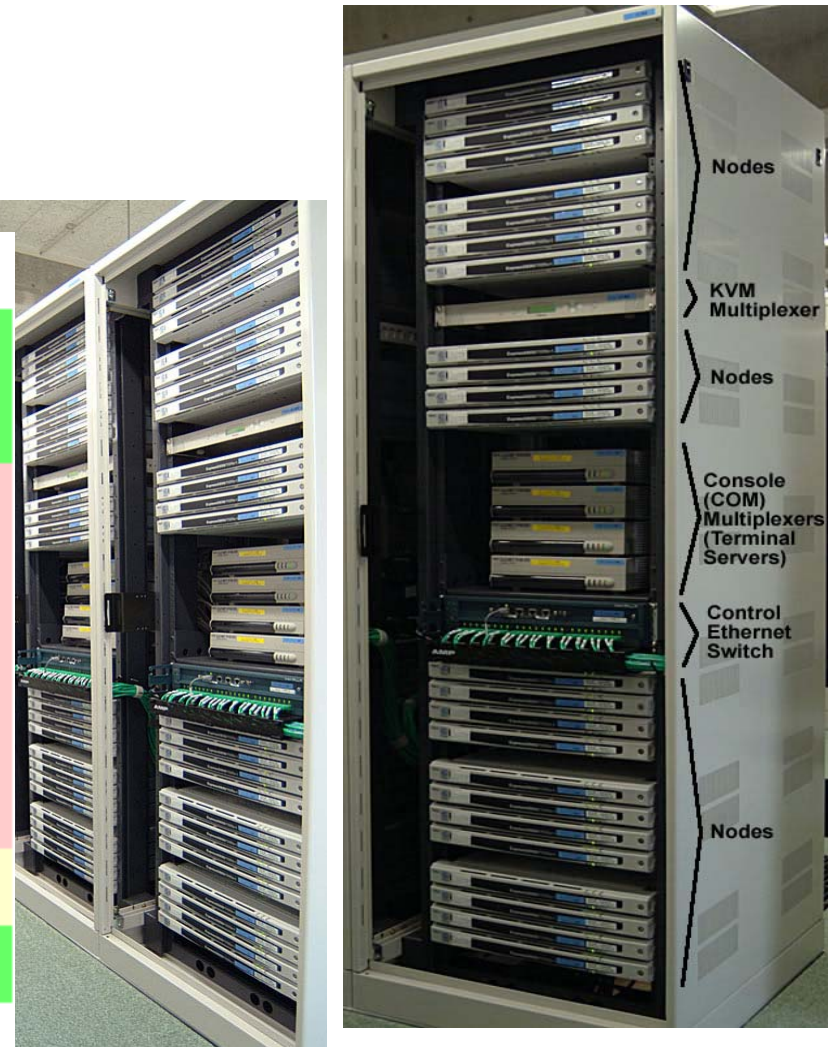
□ StarBED --- A Large Scale Network Experiment Environment



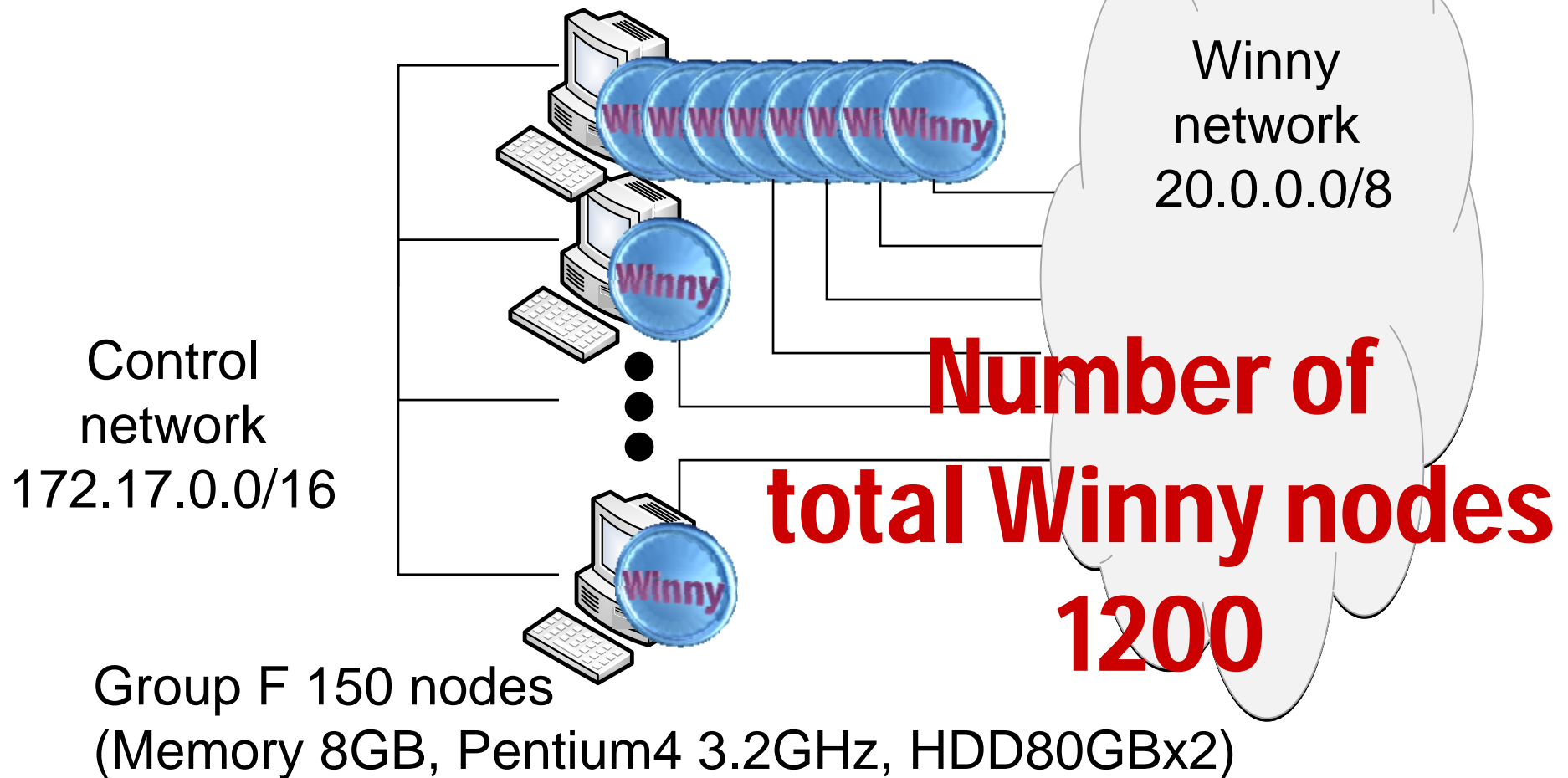
NICs of PC-node groups

group name	# of PCs	experiment networks	disk type	installation date	
		ATM	FE*	GbE**	
A	208	0	0	1 ATA	2002
B	64	1	1	0 ATA	
C	32	1	4	0 SCSI	
D	144	0	1	0 ATA	
E	64	0	4	0 ATA	
F	168	0	0	4 SATA	2006
total	680				

*FE means FastEthernet, **GbE means Gigabit Ethernet

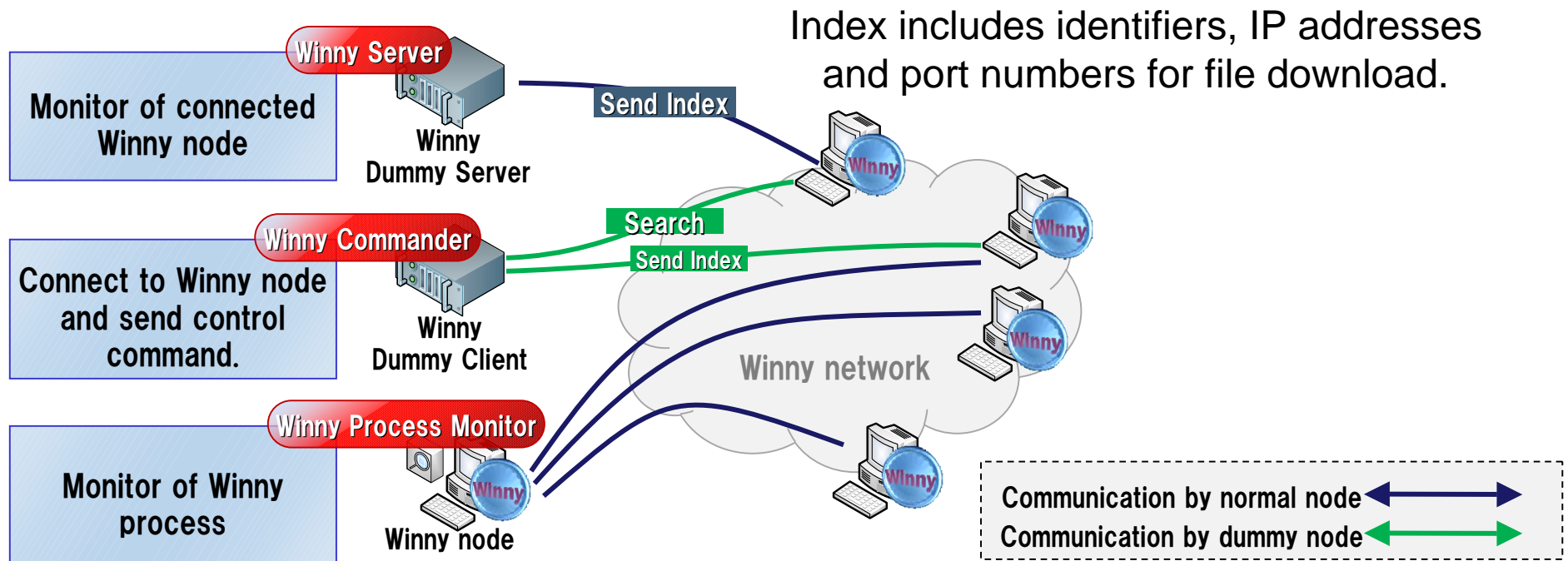


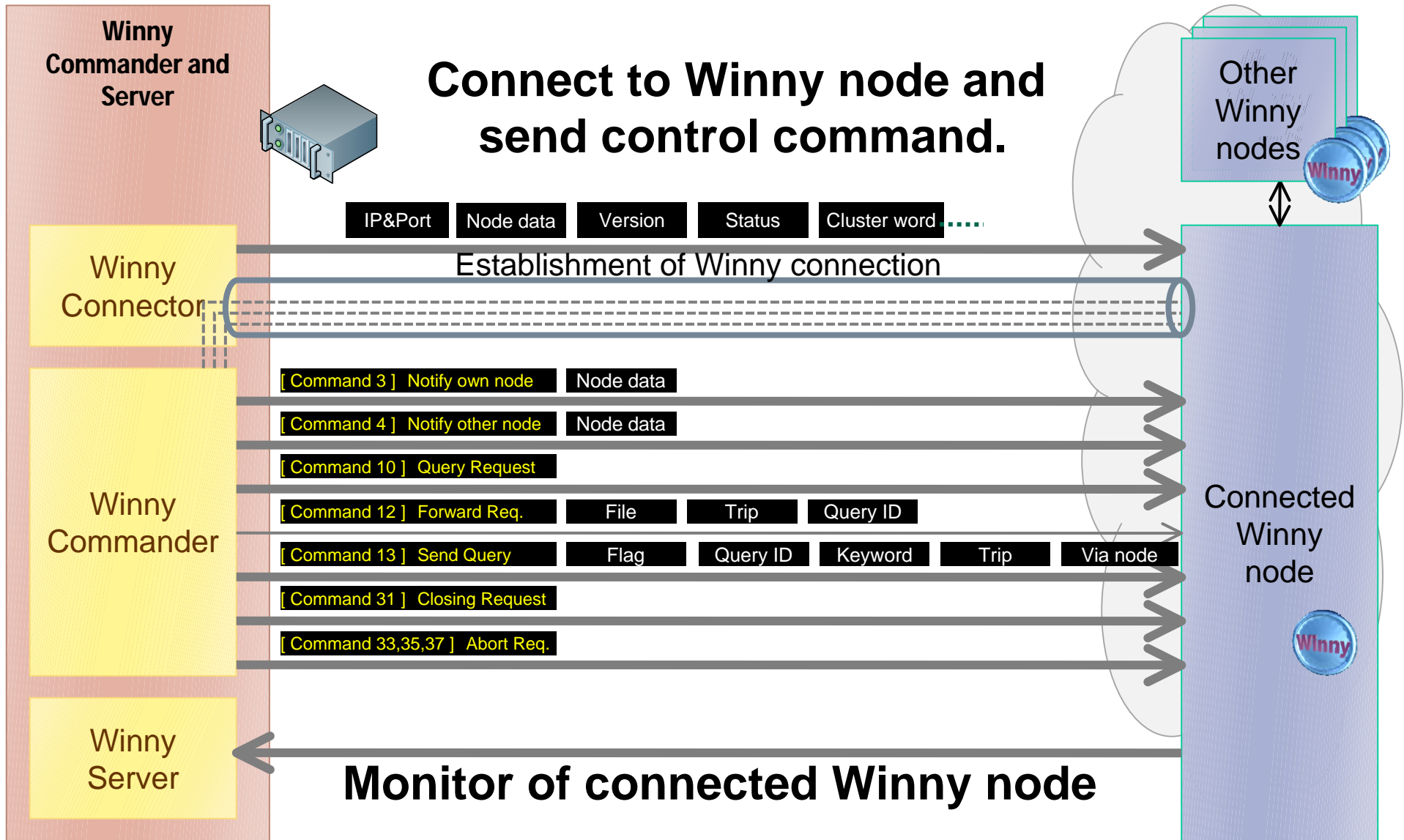
8 VM nodes/physical node by VMware ESXi
Windows + Winny2.0 b7.1/VM node



Group F 150 nodes
(Memory 8GB, Pentium4 3.2GHz, HDD80GBx2)

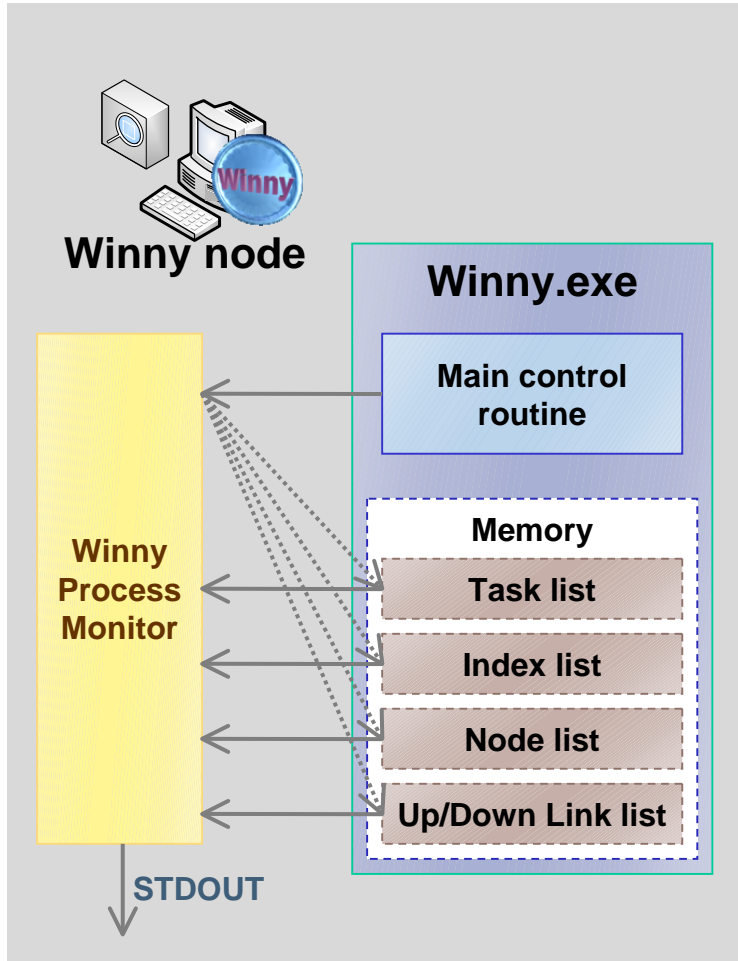
- **Winny Commander and Server**
 - It talks about the Winny protocol, and communicates with the actual Winny nodes.
- **Winny Process monitor**
 - It is a real time monitor which outputs a status of Winny.





4.

Tools for experiment of P2P network Winny Process monitor



Index

ファイル名	トロップ	サイズ(byte)	ブロック	状態
		42,669		仮想ファイル
		75,852		仮想ファイル
		208,915		仮想ファイル
		60,816,389		仮想ファイル
		213,234		仮想ファイル
		302,900		仮想ファイル
		128,873		仮想ファイル
		142,991		仮想ファイル
		142,542		仮想ファイル
		342,788,506		仮想ファイル

Node

状態	方向	回線速度	接続	接続時間	無通信時間	バージョン	接続優先度
検索リンク	上流	120	Raw	5:47	0:03	b7.1	0 (-8)
検索リンク	上流	120	NAT	0:22	0:03	b7.1	0 (-8)
待機		1000	Raw				0 (0)
待機		120	Raw				0 (0)
待機		120	Raw				0 (0)
待機		300	Raw				0 (0)
待機		1000	Raw				0 (0)
待機		120	Raw				0 (0)
待機		1000	Raw				0 (0)
待機		50	Raw				0 (0)
待機		120	Raw				0 (0)
待機		1000	Raw				0 (0)

Task

ファイル名	タスク内容	カウント	進行状況
@エム)にらまん)カタンム.txt	キャッシュから変換済み	590 / 590	ファイル変換正常終了
Fewt2013.TXT	キャッシュから変換済み	631 / 631	ファイル変換正常終了

File Search Up 2 / Down 0 Trans Up 0 / 2 Down 0 / 2 Total Up 108 / Down 4.1 Kbyte/s

Monitor data of each List

```
== Link =====
"U s: 2 t: 0 / 2 16.2K", "D s: 0 t: 0 / 2 7.1K"
```

```
== Node =====
0,0.0.0.0,0.0.0.0,219.114.217.39,32485,0,0,0,5,0,-1,0,,,0 ( 0 ),,,
1,0.0.0.0,0.0.0.0,58.159.23.77,8896,0,0,0,5,0,-1,0,,,0 ( 0 ),,,
2,0.0.0.0,0.0.0.0,203.88.184.153,4869,0,0,0,5,0,-1,0,,,0 ( 0 ),,,
3,0.0.0.0,0.0.0.0,118.4.162.101,30125,0,0,0,5,0,-1,0,,,0 ( 0 ),,,
```

```
== Task =====
君よ、優しい風になれ (とらいあんぐるハート3 リリカルおもちゃ箱).txt, キャッシュから変換済み,
1,706 / 1,706, ファイル変換正常終了, -35791394:-8,,0.0.0.0:0
信長の野望 革新 シナリオ天下布武お願いします.txt, キャッシュから変換済み, 118 / 118, ファイル変
換正常終了, -35791394:-8,,0.0.0.0:0
聖なるかな シリアル希望.txt.jpg, キャッシュから変換済み, 9,152 / 9,152, ファイル変換正常終了, -
35791394:-8,,0.0.0.0:0
```

```
== Index =====
11756, "(C73) (同人誌) [THIRD BRAND] イリヤルート攻略!新婚編
2.zip", "", 5407059, 5B3E2BF7388BABA67EE4723AADEC8E83, 61.205.48.174, 11250, 2008/1/24 20:13:43, 990
11757, "(B'z)今夜月の見える丘に
[PV].mpg", "", 43858528, CB7663F736B5FEFA1BF0F0028CE96F0E, 210.146.164.86, 7745, 2008/2/12
21:27:45, 205
11758, "(シングル) [Mizuho] It's my precious time! (FORTUNE ARTERIAL イメージテーマ)(mp3 lame
192k+鮭).rar", "", 39575498, E44E6CF7A68871214A14FC9F1ABF2641, 219.126.190.45, 5850, 2008/1/31
22:34:56, 607
```

identifier IP port

Up/Down Link

Contents

1. Problems of P2P network
2. Our activity against the problems
3. About P2P file exchange software "Winny" & "Share"
4. About StarBED
5. DoS attack by P2P network
6. Disable P2P network by P2P own protocol operation
7. Recovery capability of P2P network

This presentation shows a solution approach against problems in PURE P2P network.



□ Index poisoning Attack

The attacker inserts massive numbers of bogus records into the index for a set of targeted titles. As a result, when a user searches for a targeted title, the index returns bogus results, such as bogus identifiers, bogus IP addresses, or bogus port numbers.

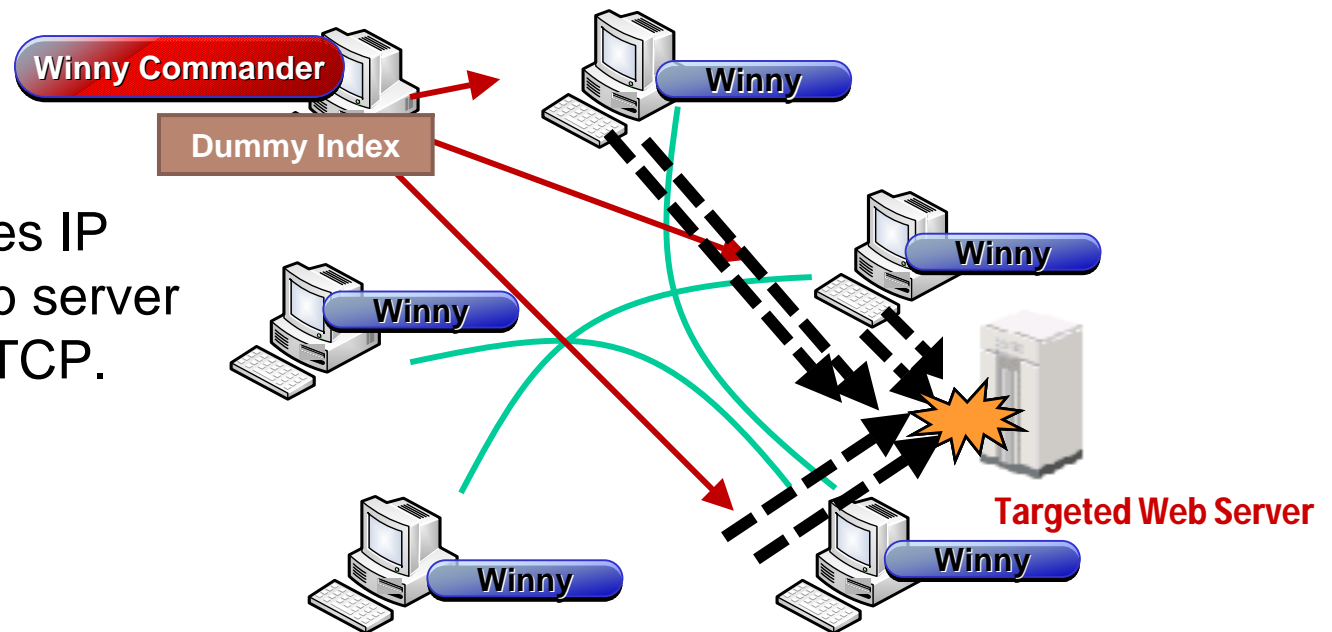
□ Related works

- Xiaosong Lou, et.al: "Prevention of Index-Poisoning DDoS Attacks in Peer-to-Peer File-Sharing Networks", IEEE Transactions on Multimedia, special issue on Content Storage and Delivery in P2P Networks, Nov.9, 2006.
- J. Liang, N. Naoumov, and K. W. Ross, "The Index Poisoning Attack in P2p File-Sharing Systems," Infocom, 2006.
- N. Naoumov and K. W. Ross, "Exploiting P2p Systems for Ddos Attacks," International Workshop on Peer-to-Peer Information Management (keynote address), Hong Kong, May 2006.

□ Index poisoning DDoS Attack

The attacker inserts massive numbers of bogus records into the index for a set of targeted titles. As a result, when a user searches for a targeted title, the index returns result, such as bogus identifier, IP address of targeted Web server, and port number 80/TCP.

Dummy Index includes IP address of targeted Web server and port number 80/TCP.



□ Experiment procedures

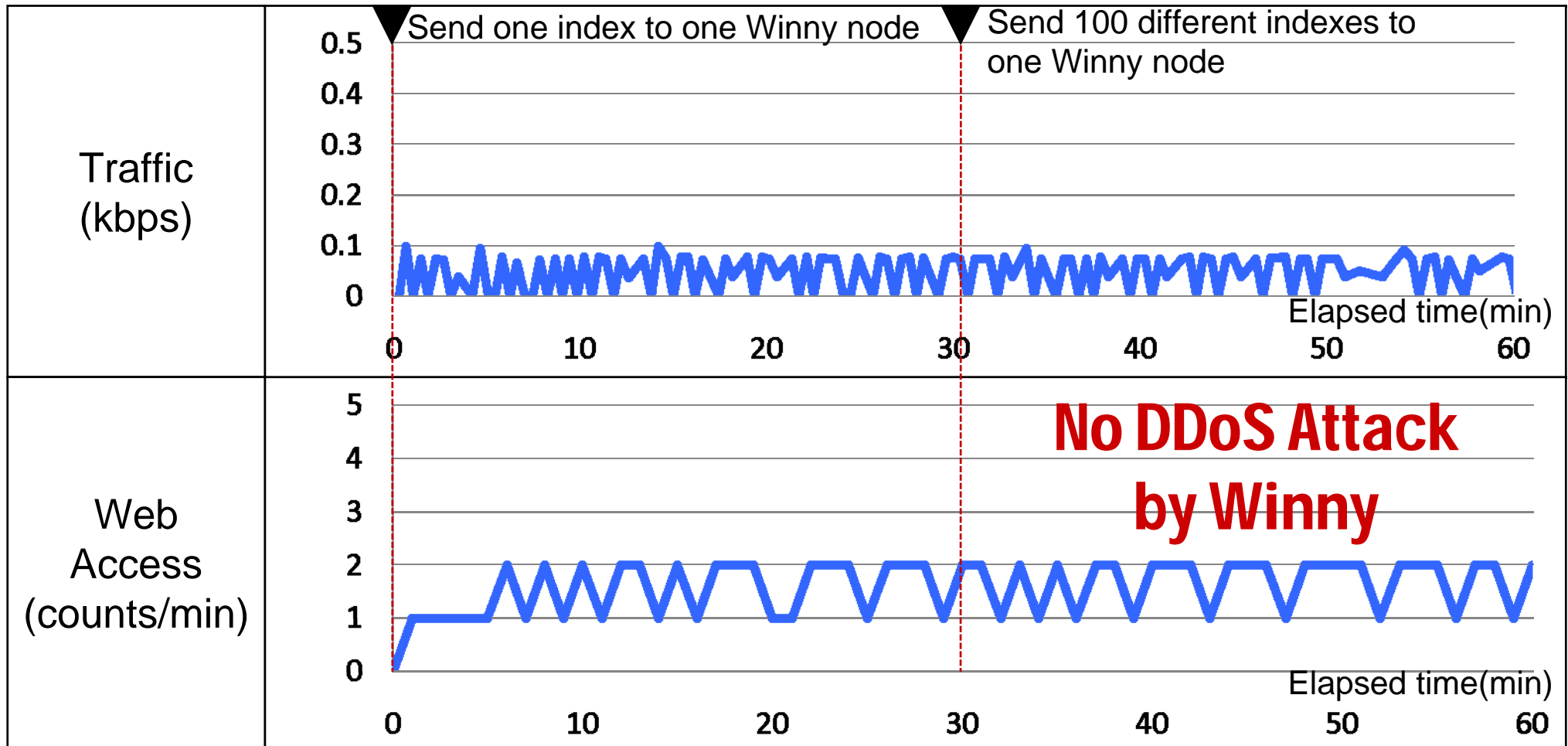
- 1200 Winny nodes are started, and P2P network for Winny is constructed.
- Make an index which includes IP address of targeted Web server.
- The index is poured into one Winny node in P2P network for Winny from one Winny Commander node.

5.

DoS attack by P2P network Result from experiment



Index distribution without download operation of each node (1200 nodes)

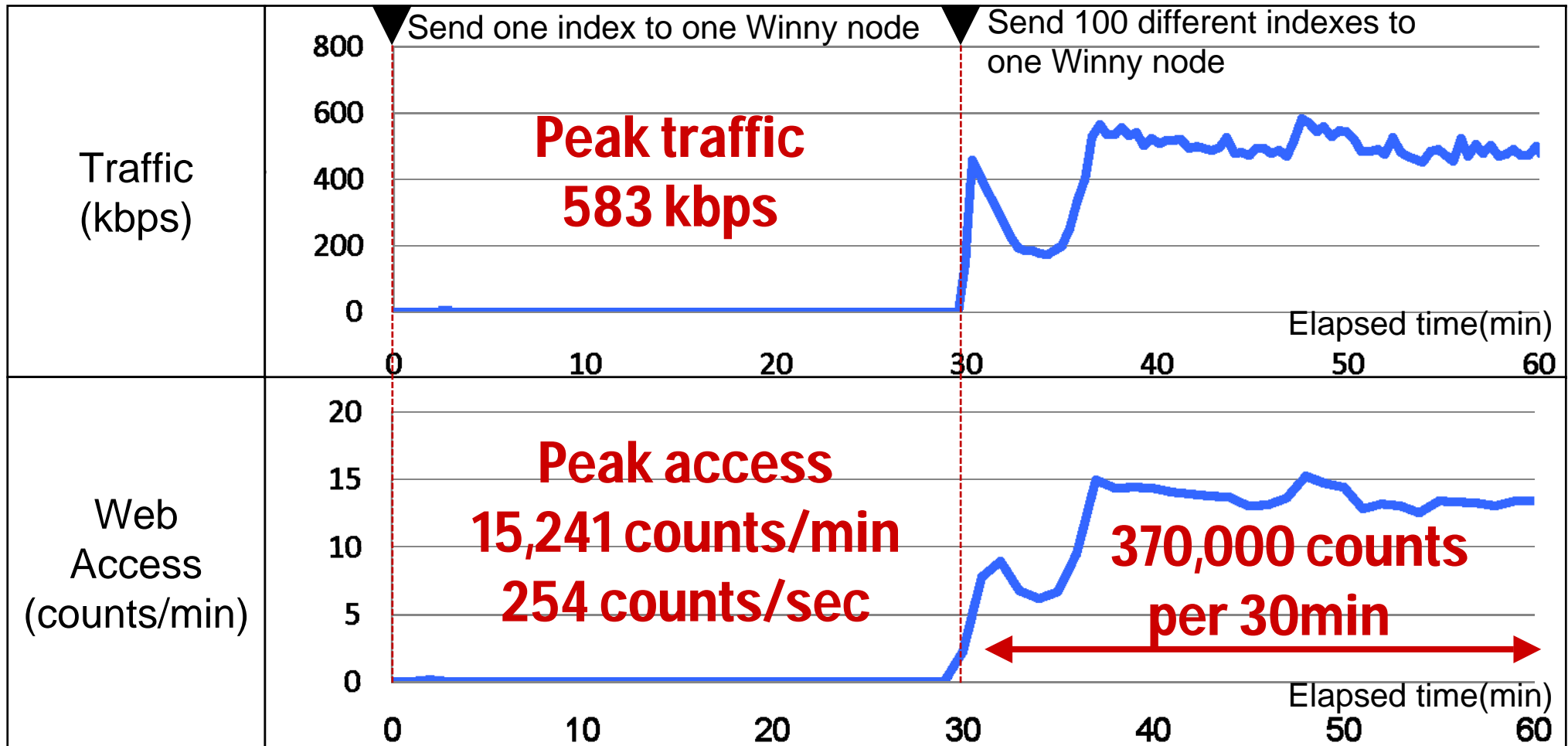


5.

DoS attack by P2P network Result from experiment

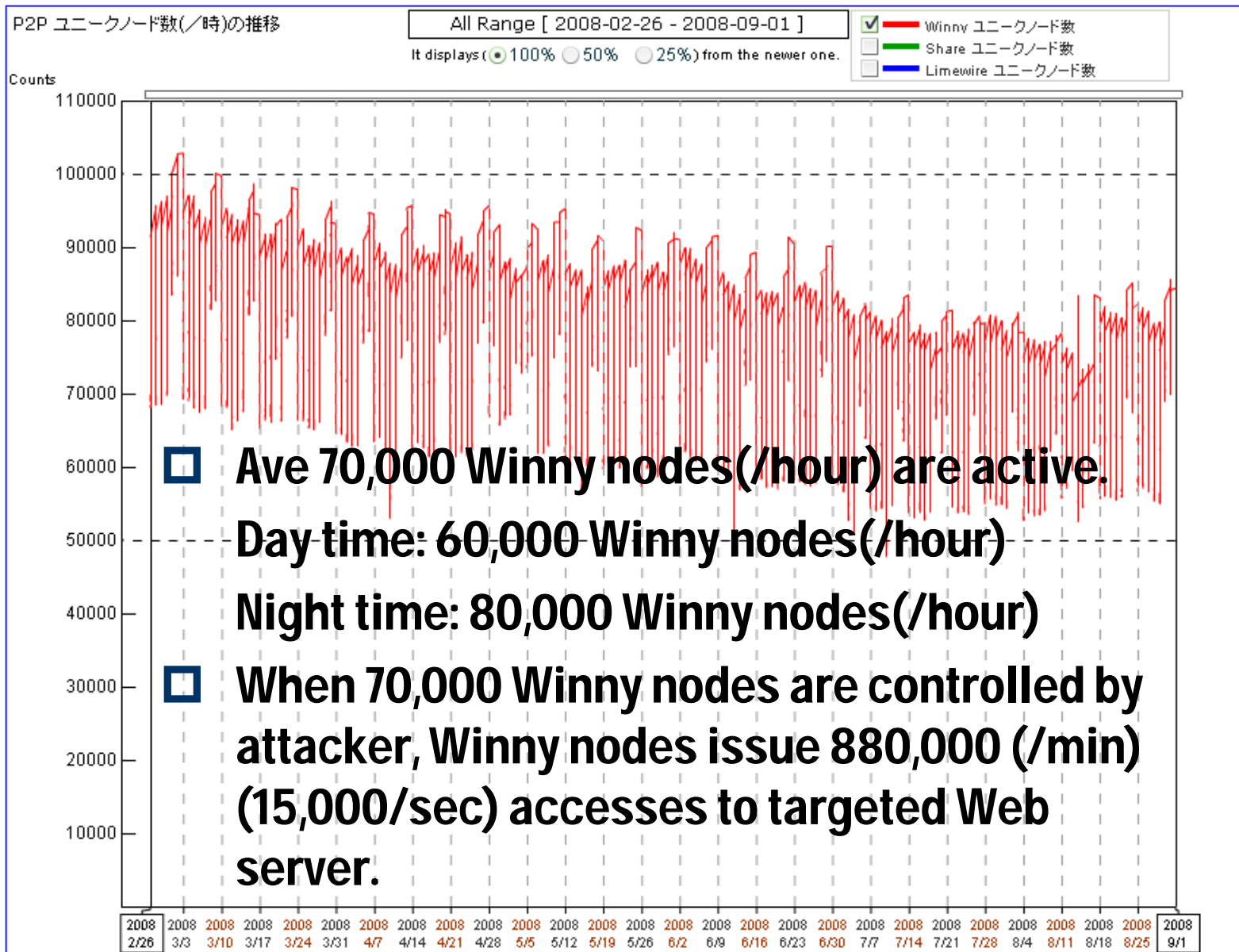


Index distribution with download operation of each node (1200 nodes)



5.

DoS attack by P2P network Consideration from experiment



Contents

1. Problems of P2P network
2. Our activity against the problems
3. About P2P file exchange software "Winny" & "Share"
4. About StarBED
5. DoS attack by P2P network
6. Disable P2P network by P2P own protocol operation
7. Recovery capability of P2P network

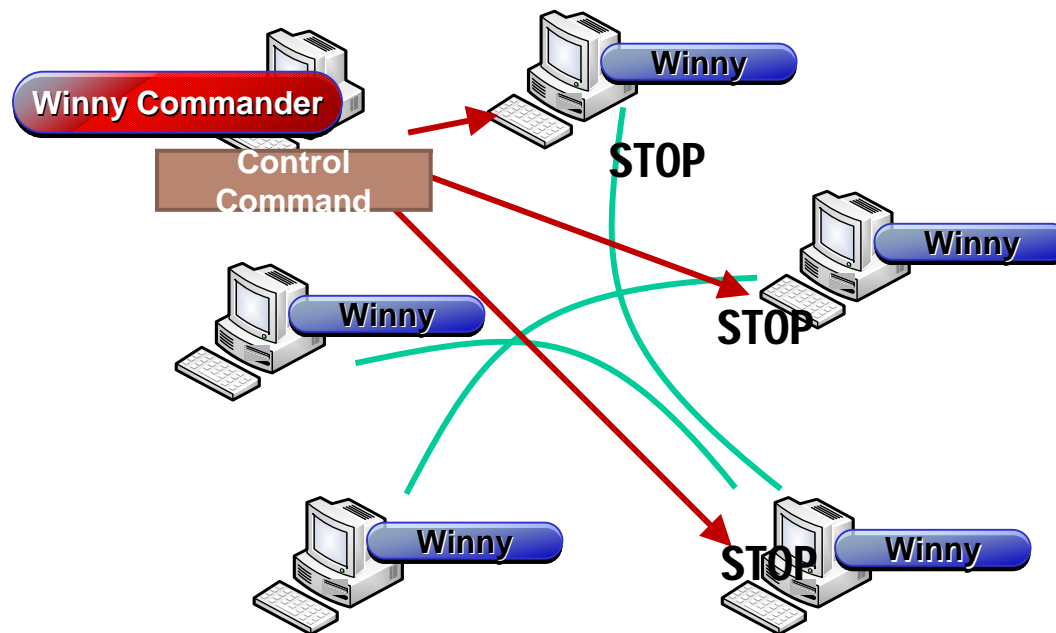
This presentation shows a solution approach against problems in PURE P2P network.



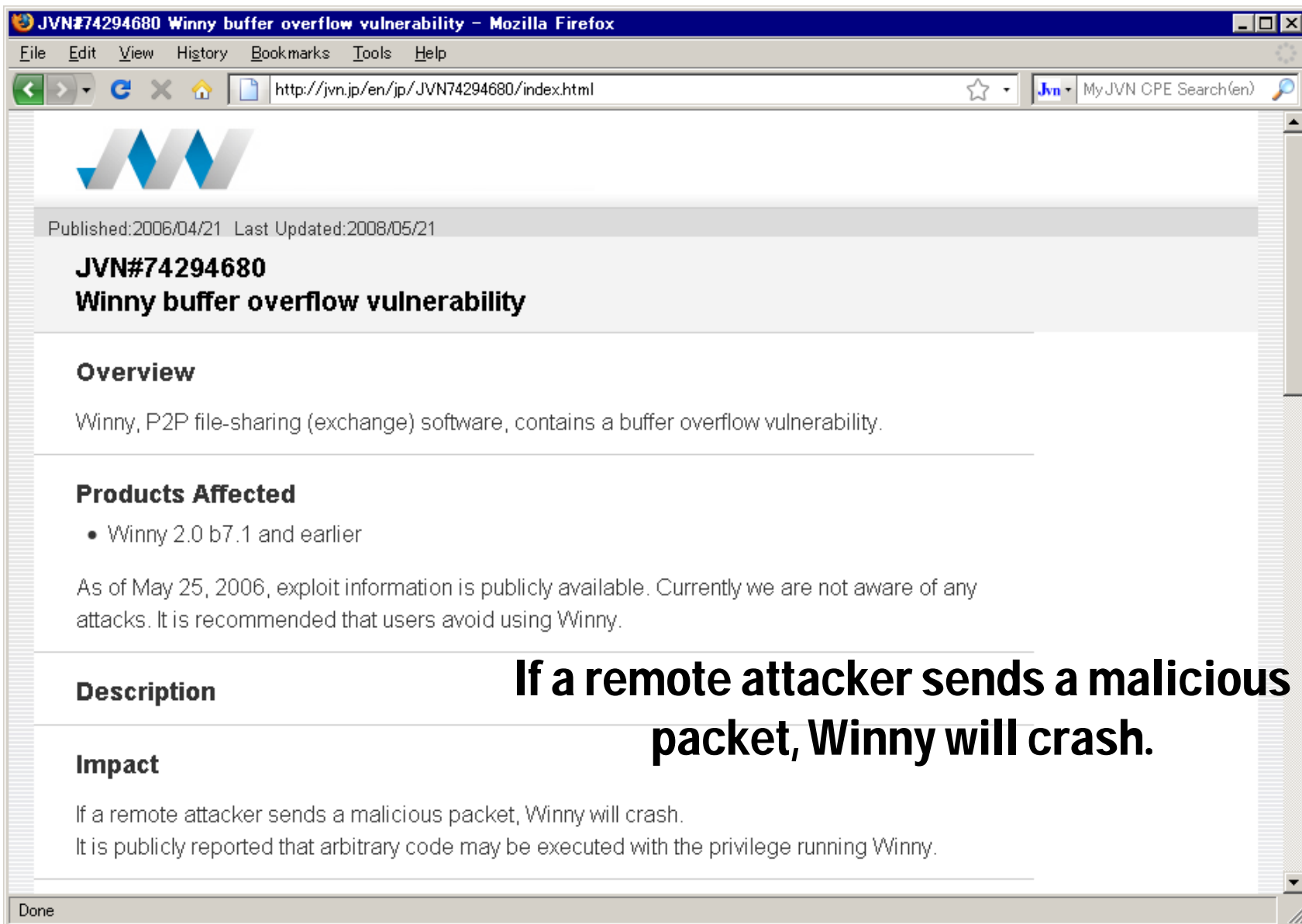
❑ Disable P2P network by P2P own protocol operation

If it lets active Winny nodes stop, at the time of the emergency, it can be applied to disable Winny network, and to prevent the leakage information circulation.

- Sending many “Close connection request” messages
- Sending one message with exploit the vulnerability (JVN#74294680)



Disable P2P network by P2P own protocol operation Winny buffer overflow vulnerability (JVN#74294680)



The screenshot shows a Mozilla Firefox browser window with the title "JVN#74294680 Winny buffer overflow vulnerability - Mozilla Firefox". The address bar shows the URL "http://jvn.jp/en/jp/JVN74294680/index.html". The page content includes the JVN logo, publication and update dates, the title "JVN#74294680 Winny buffer overflow vulnerability", and sections for "Overview", "Products Affected", "Description", and "Impact".

Overview
Winny, P2P file-sharing (exchange) software, contains a buffer overflow vulnerability.

Products Affected

- Winny 2.0 b7.1 and earlier

As of May 25, 2006, exploit information is publicly available. Currently we are not aware of any attacks. It is recommended that users avoid using Winny.

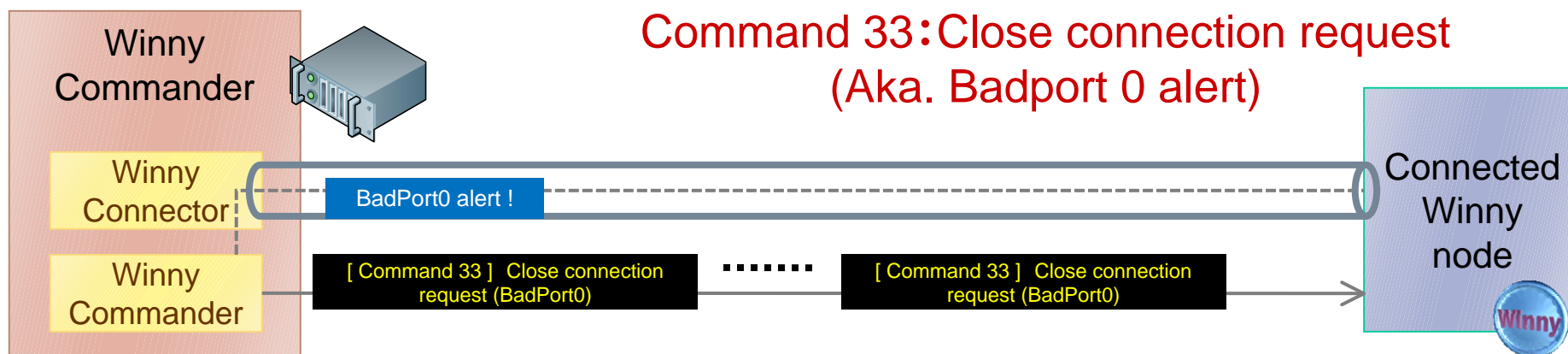
Description

If a remote attacker sends a malicious packet, Winny will crash.

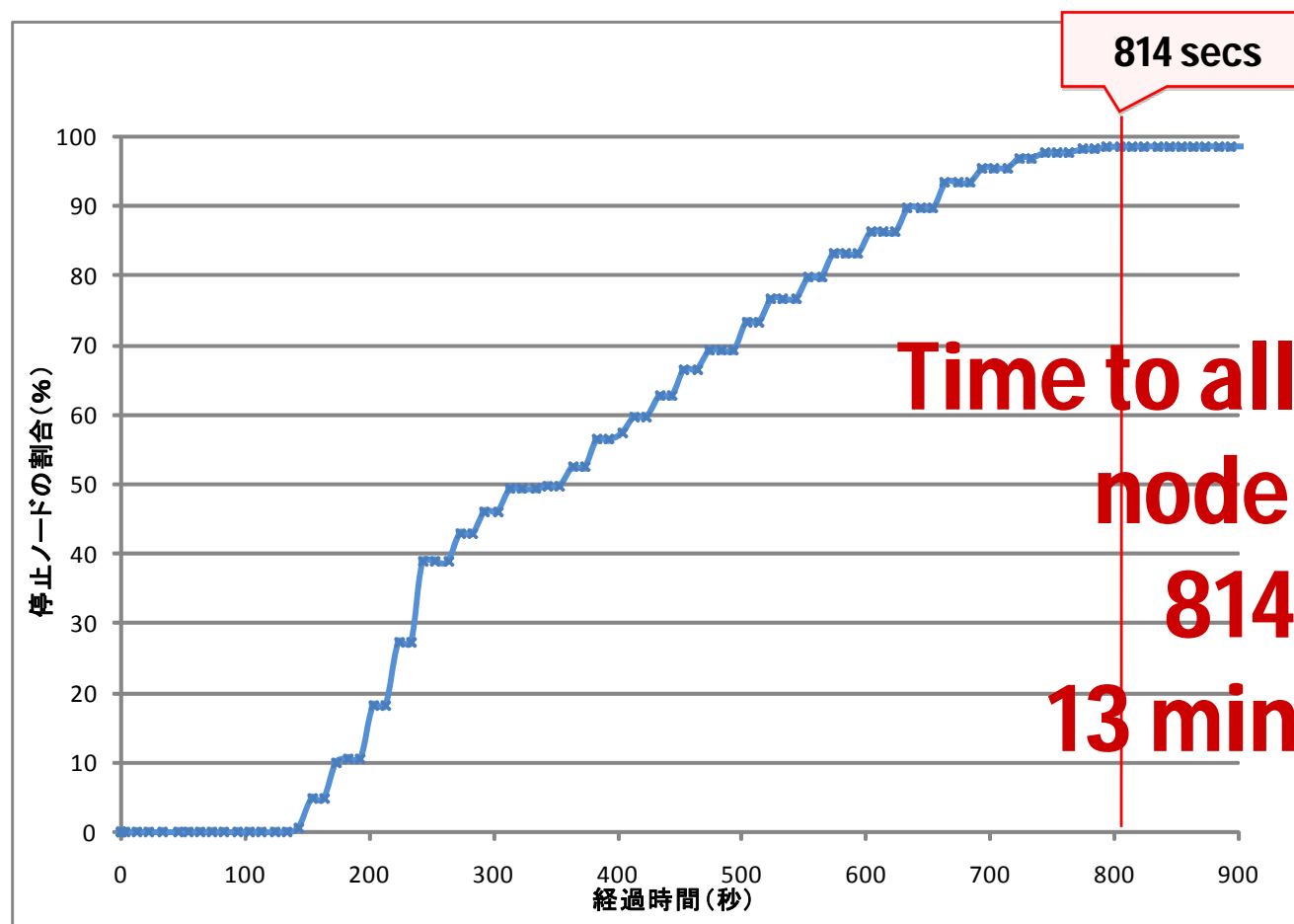
Impact

If a remote attacker sends a malicious packet, Winny will crash.
It is publicly reported that arbitrary code may be executed with the privilege running Winny.

- ❑ **Experiment procedures - Sending many “Close connection request” messages**
 - 1200 Winny nodes are started, and P2P network for Winny is constructed.
 - Winny Commander node sends 200 “Close connection request” messages (Command 33) to 12 Winny node.
 - Above procedure is carried out repeatedly.



□ Time to all the Winny node stops



**Time to all the Winny
node stops
814 sec
13 min 34 sec**

6.

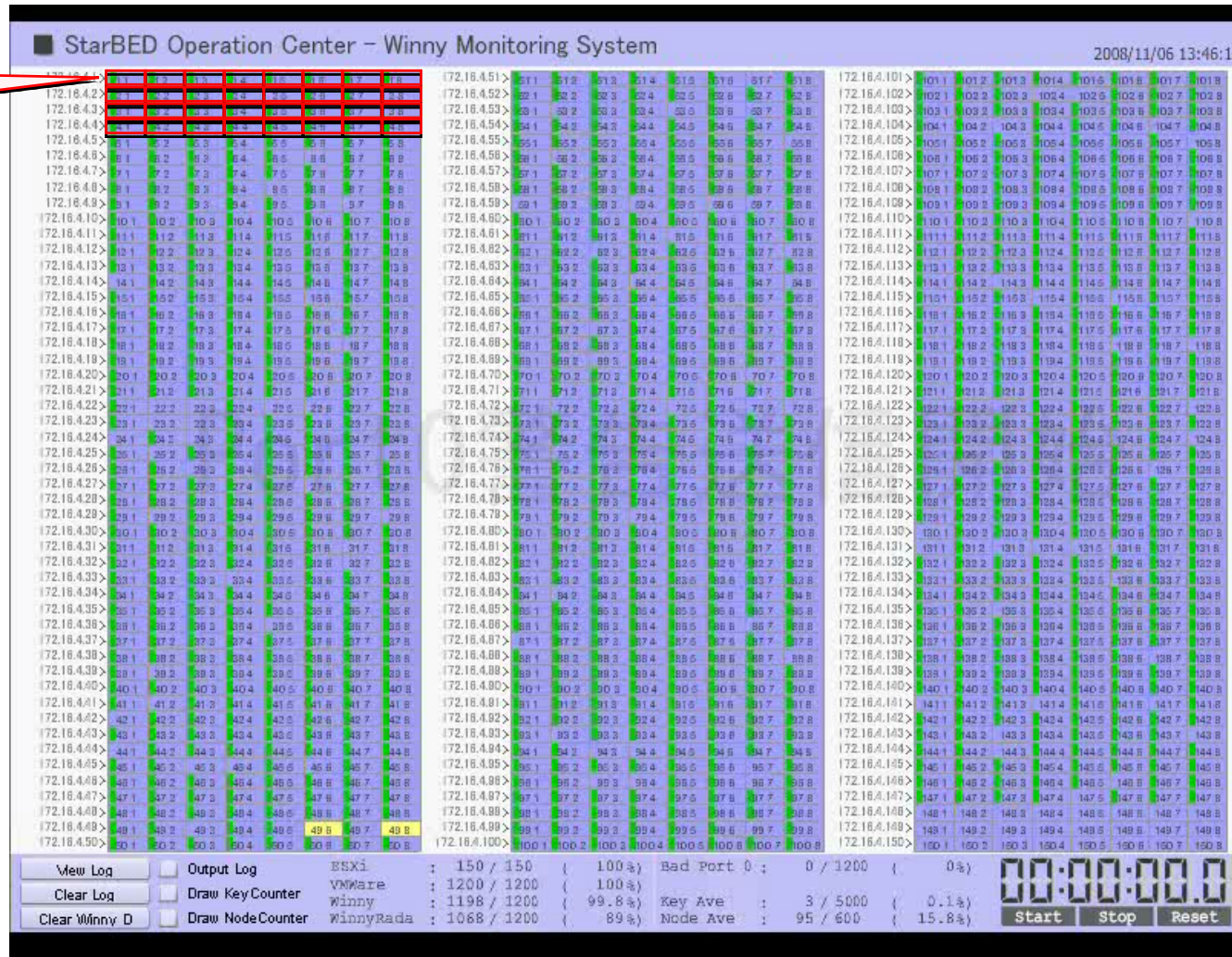
Disable P2P network by P2P own protocol operation Result from experiment



Winny node status

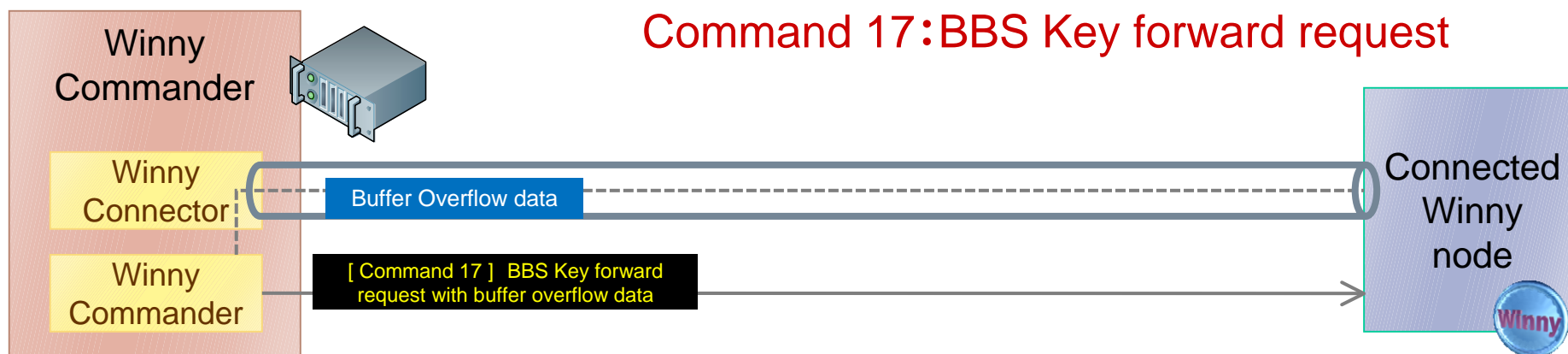
Red circle: Winny node stop

1 cell is
1 Winny node



1200
nodes

- ❑ **Experiment procedures - Sending one message with exploit the vulnerability (JVN#74294680)**
 - 1200 Winny nodes are started, and P2P network for Winny is constructed.
 - Winny Commander node sends 1 “Buffer overflow data request (JVN#74294680)” message (Command 17) to 12 Winny node.
 - Above procedure is carried out repeatedly.

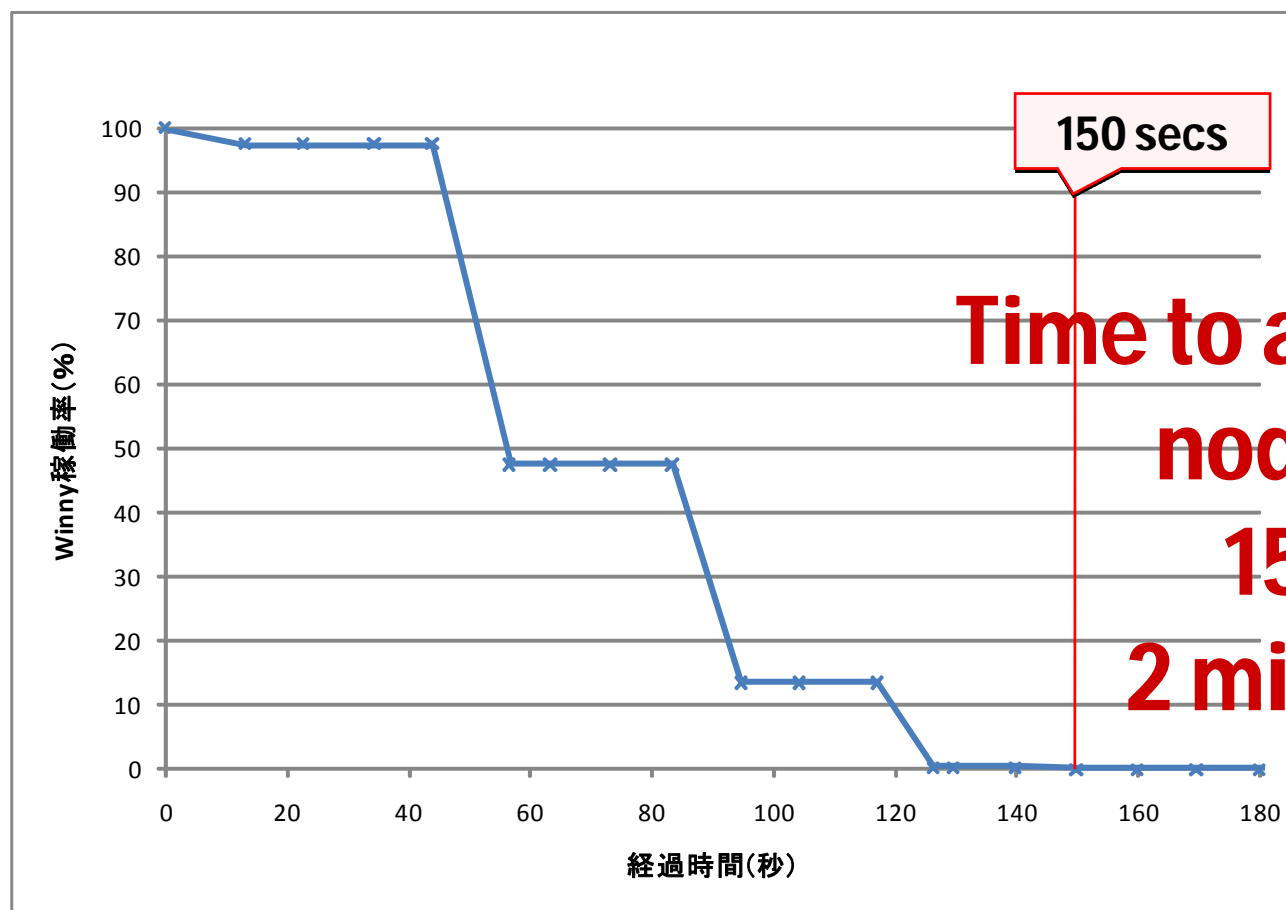


6.

Disable P2P network by P2P own protocol operation Result from experiment

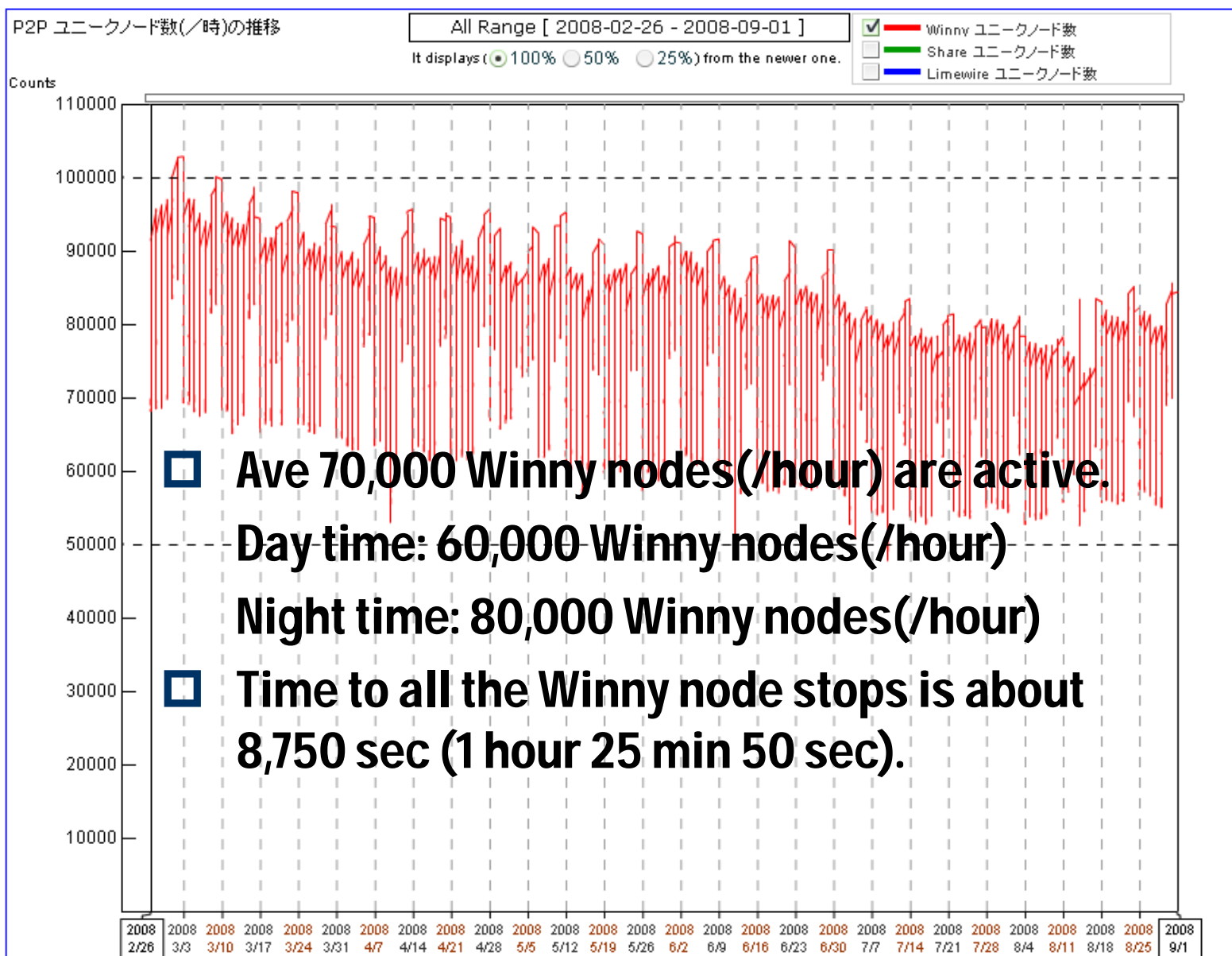


□ Time to all the Winny node stops



6.

Disable P2P network by P2P own protocol operation Consideration from experiment



Contents

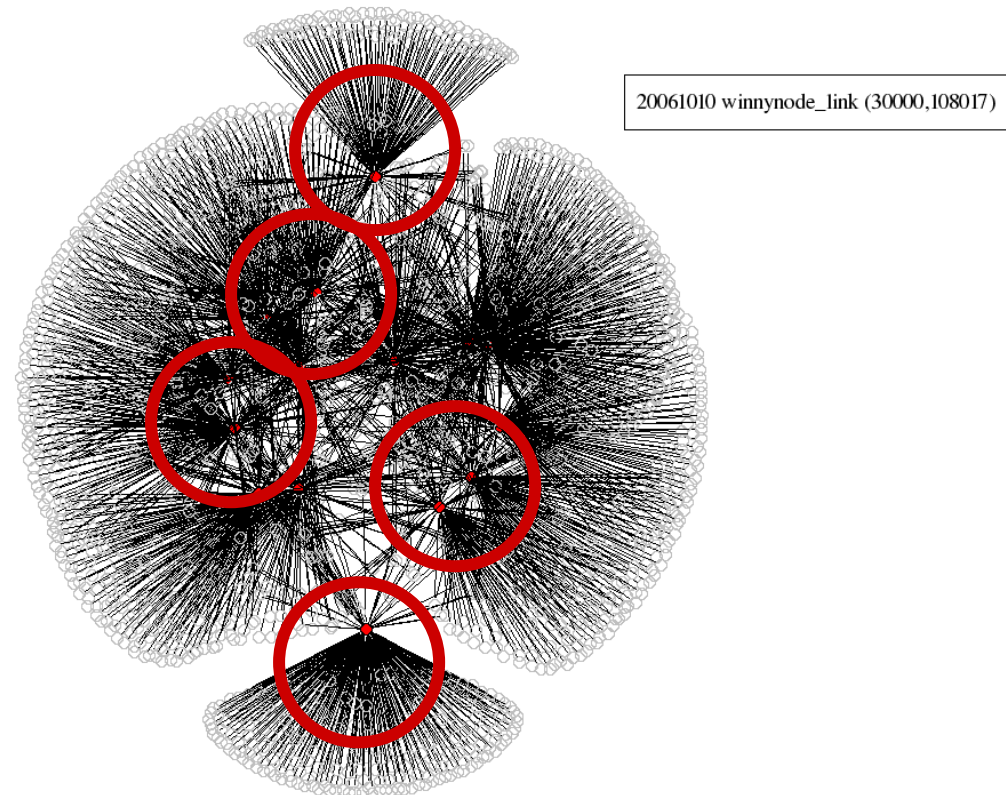
1. Problems of P2P network
2. Our activity against the problems
3. About P2P file exchange software "Winny" & "Share"
4. About StarBED
5. DoS attack by P2P network
6. Disable P2P network by P2P own protocol
7. Recovery capability of P2P network

This presentation shows a solution approach against problems in PURE P2P network.



□ Recovery capability of P2P network

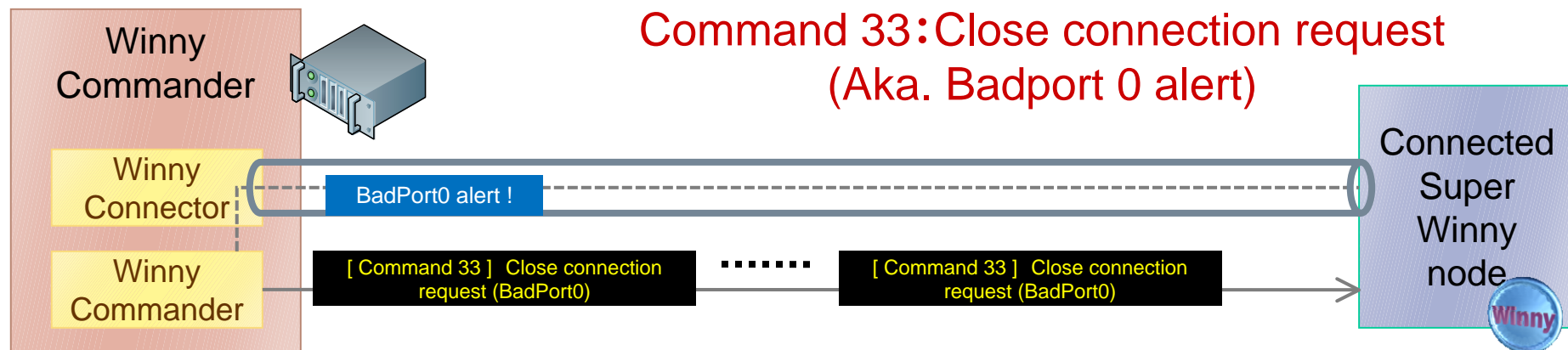
In Winny network , there are some “Super” P2P node which is most active node and reference node .When some active Winny nodes stop, other Winny nodes will recover own network.



□ Experiment procedures

- 1200 Winny nodes are started, and P2P network for Winny is constructed.
- Winny Commander node sends 200 “Close connection request” messages (Command 33) to 5 “Super “ Winny node.

“Super” Winny node is most active node and reference node in Winny network.



7.

Recovery capability of P2P network Result from experiment

#node:1818

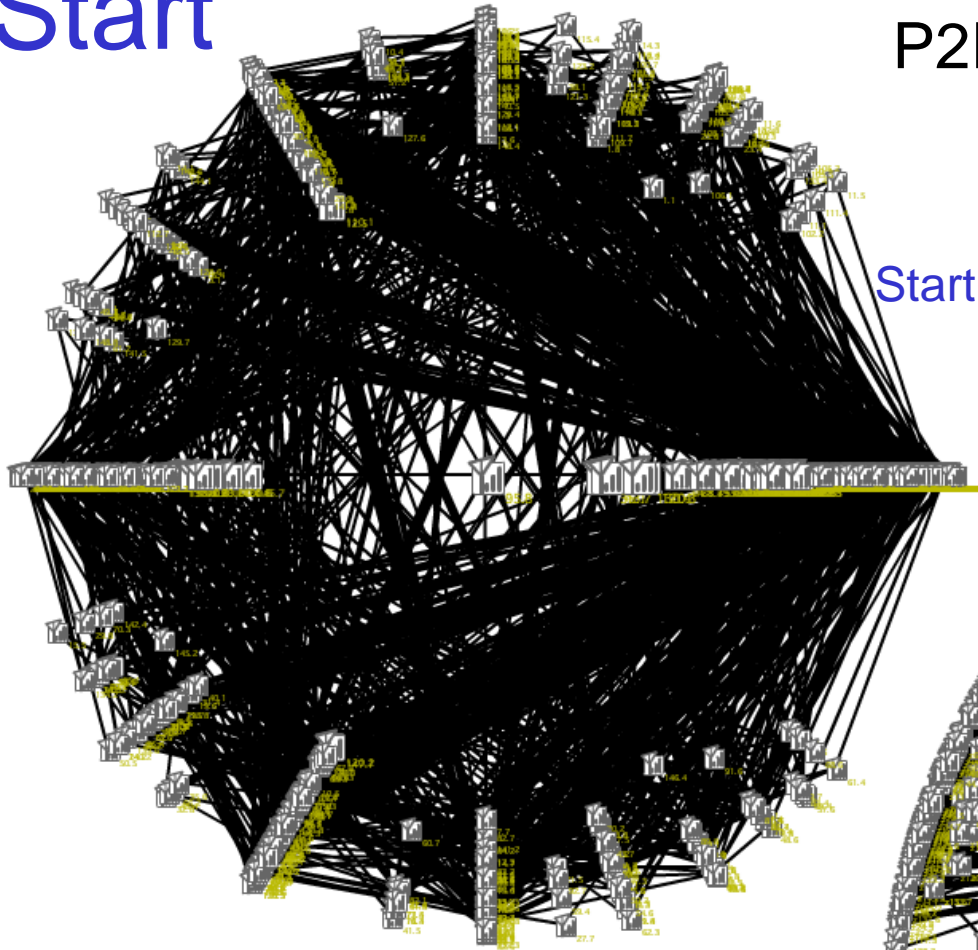
processing time(ms):96479

Start

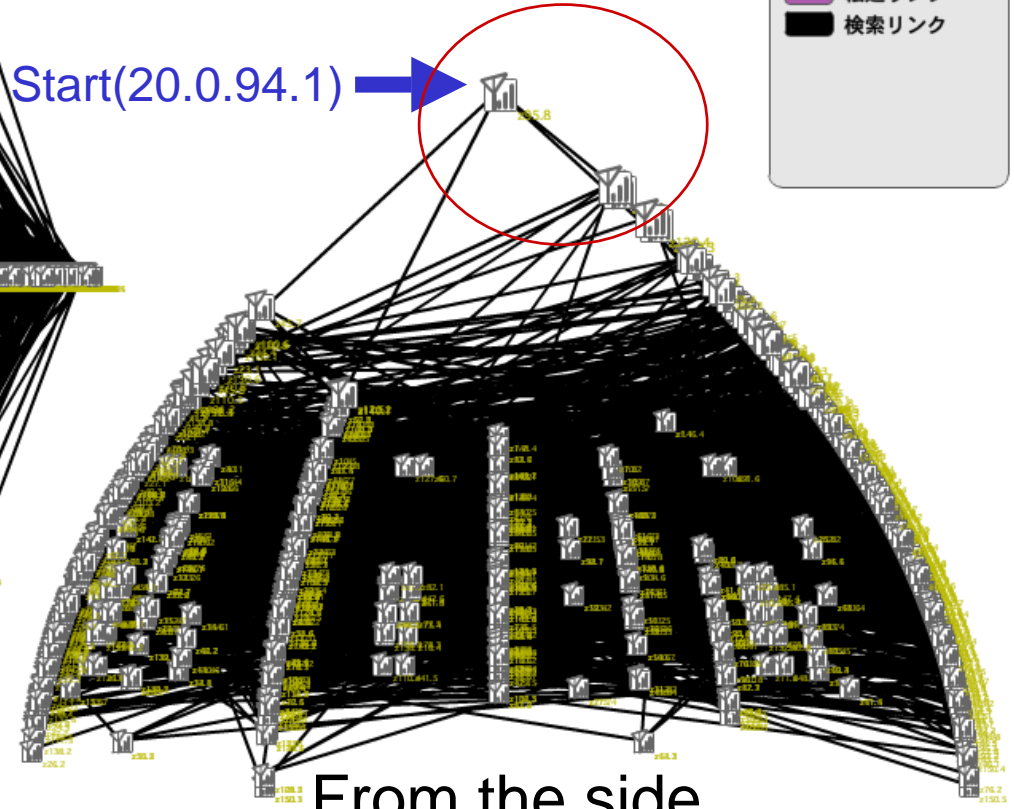
P2P link relation map

“Super” Winny nodes

Start(20.0.94.1) →



From the top



From the side

7.

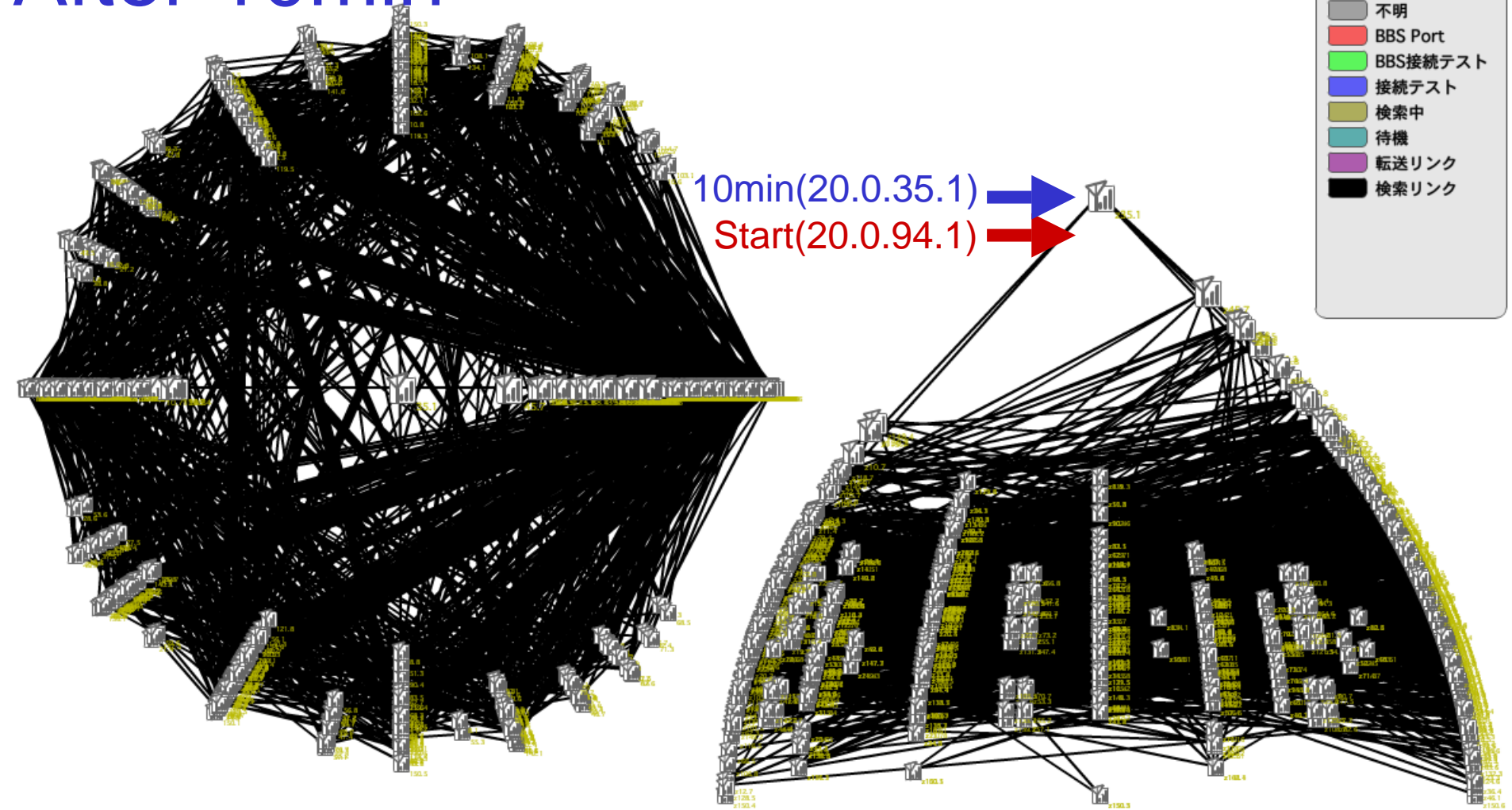
Recovery capability of P2P network Result from experiment



#node:1824

processing time(ms):96327

After 10min



7.

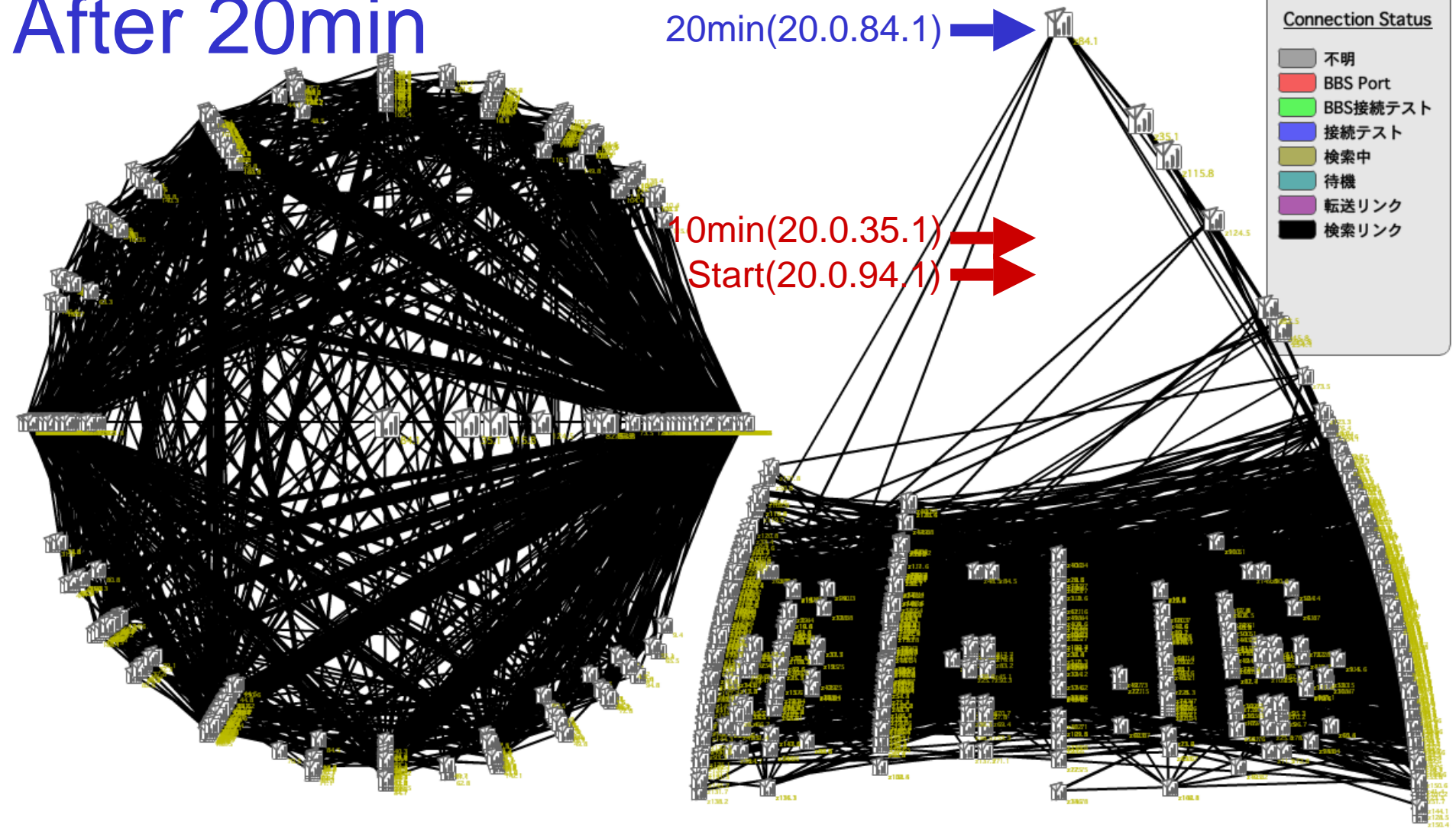
Recovery capability of P2P network Result from experiment



#node:1816

processing time(ms):95640

After 20min



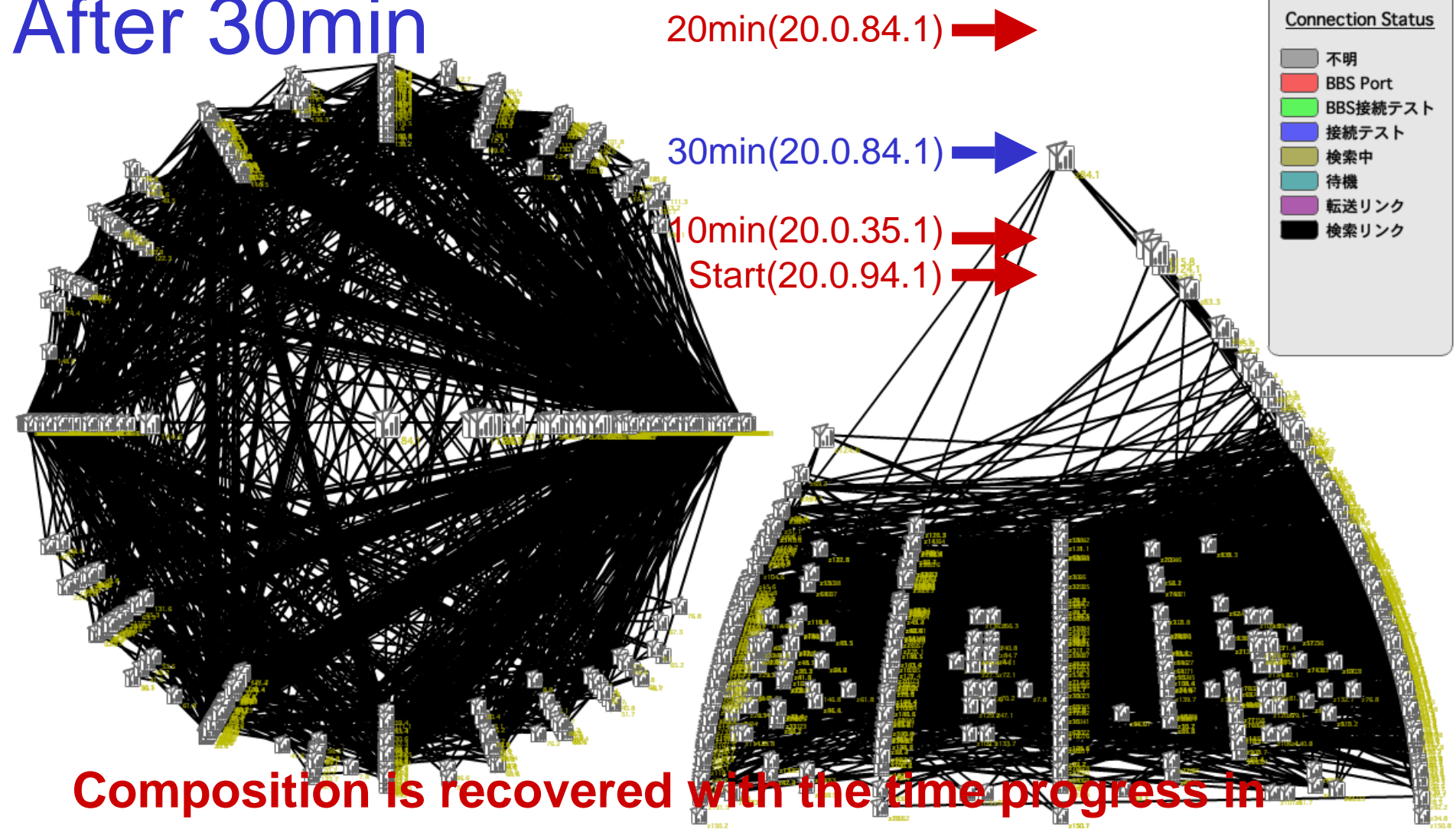
7.

Recovery capability of P2P network Result from experiment



#node:1808 processing time(ms):94344

After 30min



Composition is recovered with the time progress in the condition of the degree experiment start time.

Questions ?

We continue this feasibility study of DoS attack by P2P network. Next month, we will do 3rd experiment trial on StarBED.



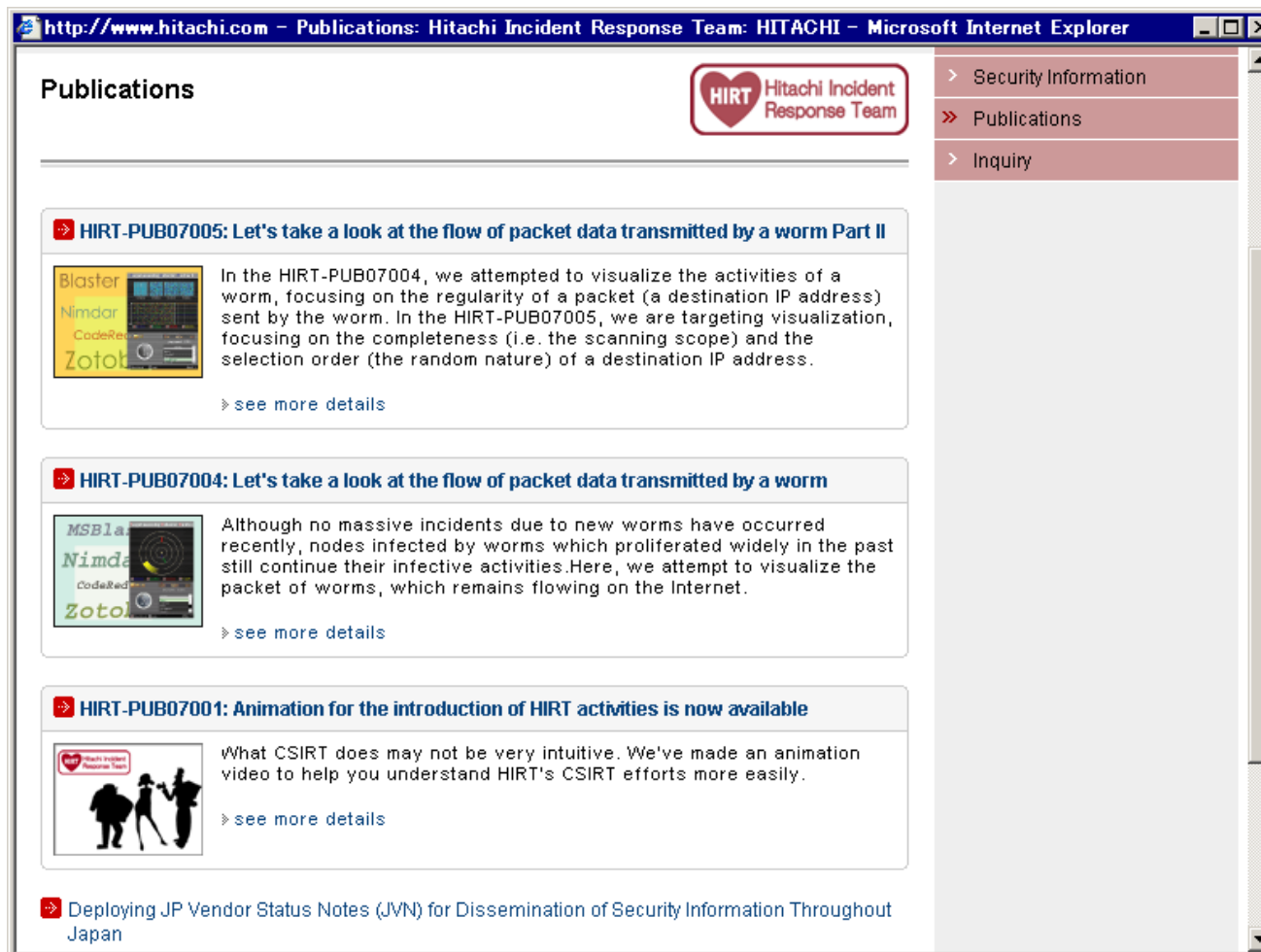
About HIRT

- **HIRT (Hitachi Incident Response Team)**
 - <http://www.hitachi.com/hirt/>
 - <http://www.hitachi.com/hirt/publications/>
- **JVNRSS Feasibility Study Site**
 - <http://jvnrss.ise.chuo-u.ac.jp/jtg/>

HIRT (Hitachi Incident Response Team) was established in 1998 as an in-house project, and was organized to act as CSIRT (Computer Security Incident Response Team) for the Hitachi group in October 2004. To promote better vulnerability handling (support activity to eliminate security vulnerabilities) and better incident responsiveness (support activity to avoid and recover from the latest security violations and related incidents), HIRT is the CSIRT point of contact that coordinates the Hitachi group and liaisons with external entities.



About HIRT



The screenshot shows a web browser window with the address bar displaying "http://www.hitachi.com - Publications: Hitachi Incident Response Team: HITACHI - Microsoft Internet Explorer". The page title is "Publications". A navigation menu on the right includes "Security Information", "Publications" (which is selected), and "Inquiry". The main content area features a "Hitachi Incident Response Team" logo and a list of publications:

- HIRT-PUB07005: Let's take a look at the flow of packet data transmitted by a worm Part II**
In the HIRT-PUB07004, we attempted to visualize the activities of a worm, focusing on the regularity of a packet (a destination IP address) sent by the worm. In the HIRT-PUB07005, we are targeting visualization, focusing on the completeness (i.e. the scanning scope) and the selection order (the random nature) of a destination IP address.
[see more details](#)
- HIRT-PUB07004: Let's take a look at the flow of packet data transmitted by a worm**
Although no massive incidents due to new worms have occurred recently, nodes infected by worms which proliferated widely in the past still continue their infective activities. Here, we attempt to visualize the packet of worms, which remains flowing on the Internet.
[see more details](#)
- HIRT-PUB07001: Animation for the introduction of HIRT activities is now available**
What CSIRT does may not be very intuitive. We've made an animation video to help you understand HIRT's CSIRT efforts more easily.
[see more details](#)
- Deploying JP Vendor Status Notes (JVN) for Dissemination of Security Information Throughout Japan**



Ending

This presentation has showed some experiment results about P2P network enforced in StarBED which is a Large Scale Network Experiment.

- DoS attack by P2P network
- Disable P2P network by P2P own protocol

Acknowledgement

This work was supported by a consignment research from the Ministry of Internal Affairs and Communications, Japan.



END

Feasibility Study of DoS attack by P2P network.

2009/01/20

Hitachi Incident Response Team
Masato Terada

