2011/01/27
ICTテストベッド戦略2011
～JGN2plus・StarBEDジョイント　シンポジウム～

StarBED P2Pオーバーレイネットワーク環境の構築とその活用

株式会社日立製作所　システム開発研究所
寺田　真敏

概要

- Winnyをはじめとする、P2Pファイル交換ソフトウェアから構成されるオーバーレイネットワークにおいて、マルウェア流布や情報漏えいなどの問題は依然として存在しているが、オーバーレイネットワーク自身が持つ潜在的な脅威について言及されることは少ない。

- 本報告では、StarBED上に構築した、多数のWindowsノードから構成される、観測可能なP2Pオーバーレイネットワーク環境のテストベットとしての活用事例を紹介する。

目次

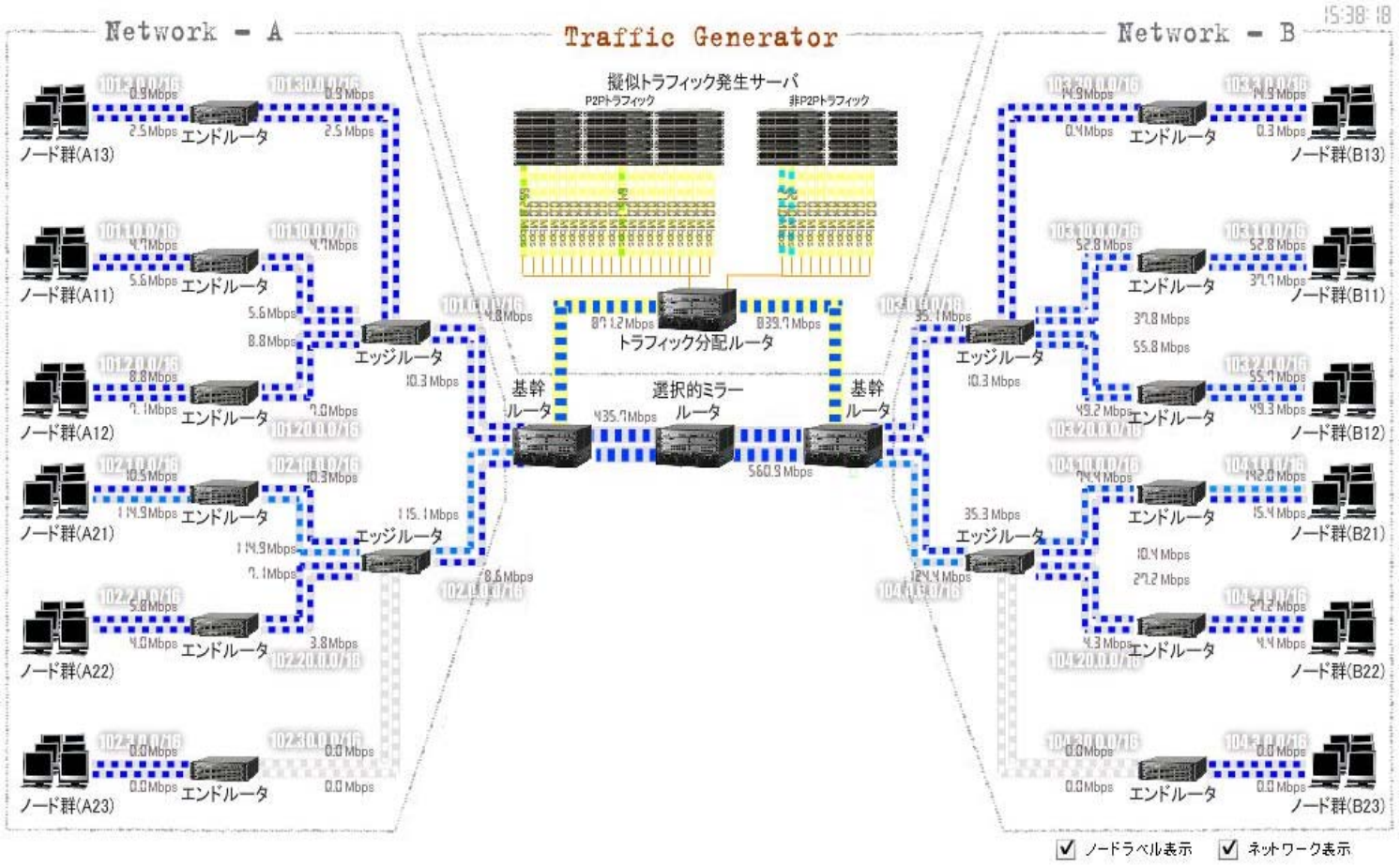
1. StarBED P2Pオーバーレイネットワーク環境の構築
2. 活用事例
   - 事例1. P2P通信の検知・制御システムの有効性検証
   - 事例2. マルウェアダウンロード防止ツールの機能検証
   - 事例3. Shareにおけるファイル保持ノード特定方法
   - 事例4. P2Pネットワーク外に対するサービス運用妨害
   - 事例5. Winnyノードの緊急停止

1. StarBED P2Pオーバーレイ ネットワーク環境の構築

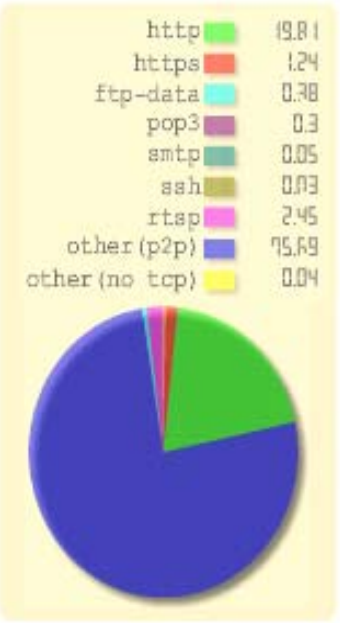
ネットワーク構成とノード構成

- ネットワーク構成
  - 3階層型（バックボーンルータ＋エッジルータ＋エンドルータ）
  - バックボーンでは、インターネットを模擬したプロトコル比率のトラフィックを再現可能
- ノード構成
  - VMware ESXi（6仮想ノード/物理ノード）
    ＋Microsoft Windows XP
    ＋P2Pファイル交換ソフトウェア（Winny、Winnyp、Shareなど）

ネットワーク構成とノード構成



プロトコル比率



P2Pオーバーレイネットワークの制御と監視

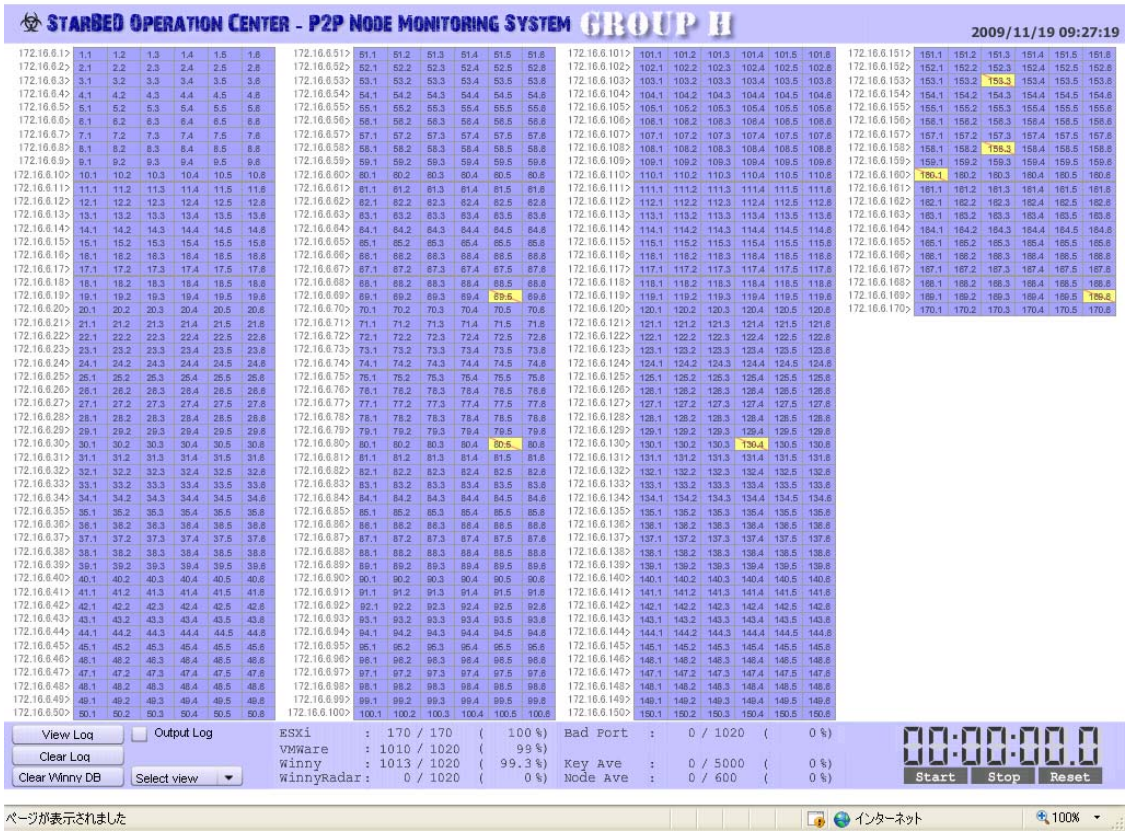
- P2Pファイル交換ソフトウェアのリモート制御
  - Windows SysinternalsのPsToolsを利用して、リモートから仮想ノード上のP2Pファイル交換ソフトウェアを起動あるいは、停止する。

- P2Pファイル交換ソフトウェアのコネクション制御
  - Winnyコマンダ（≒Winnyクライアント）& Winnyサーバ
    Winnyプロトコルを喋り、実Winnyノードと通信する。
  - Shareコマンダ
    Shareプロトコルを喋り、実Shareノードと通信する。

P2Pオーバーレイネットワークの制御と監視

P2Pオーバーレイネットワークの制御と監視

- ノード監視
  - ポートスキャンを利用して、仮想ノードとP2Pファイル交換ソフトウェアの稼働状況を監視

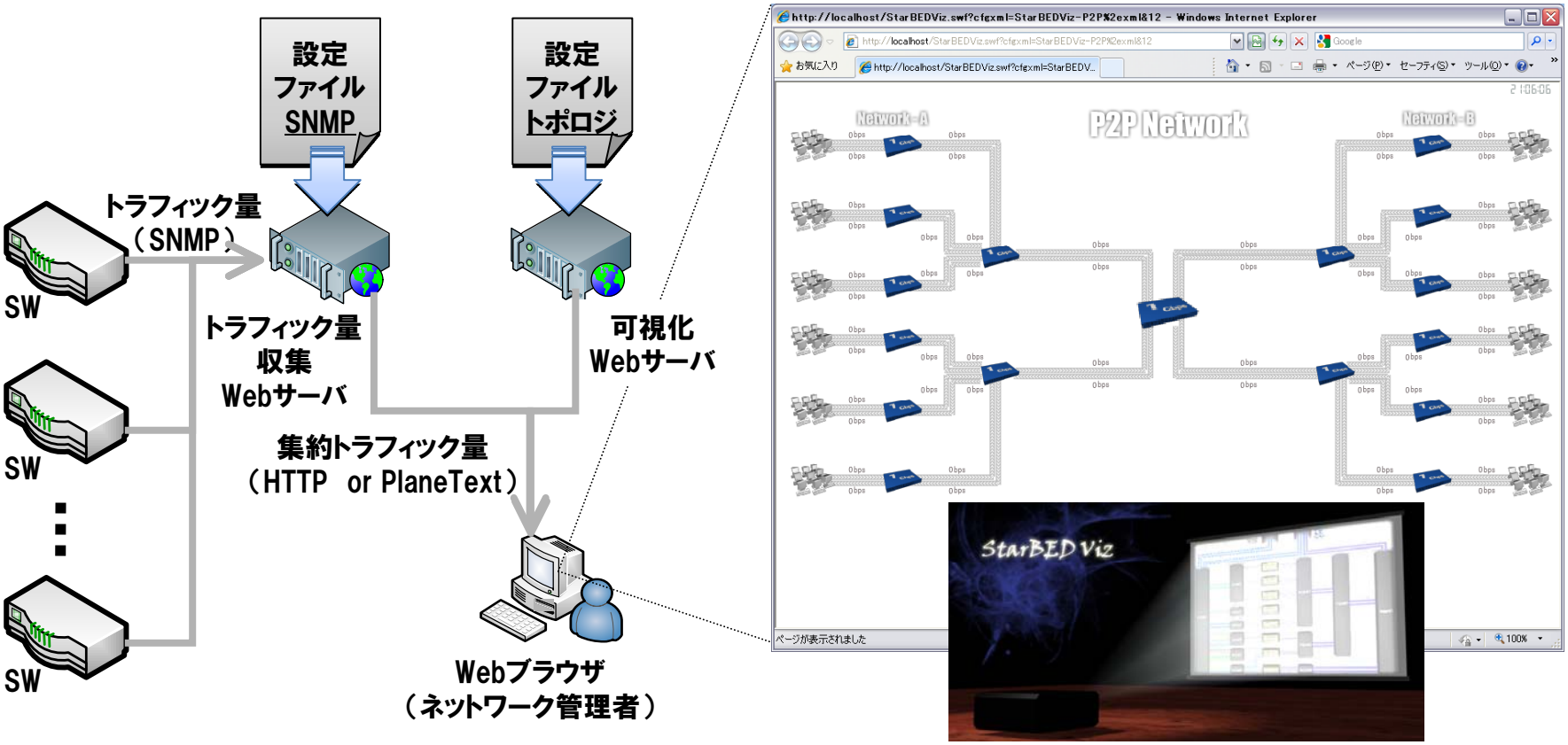


仮想ノード及びP2Pソフト稼動

仮想ノード稼動（P2Pソフト非稼働）

P2Pオーバーレイネットワークの制御と監視

- **ネットワーク構成とトラフィック監視**
  - StarBED Viz：トラフィック量の監視および可視化システム



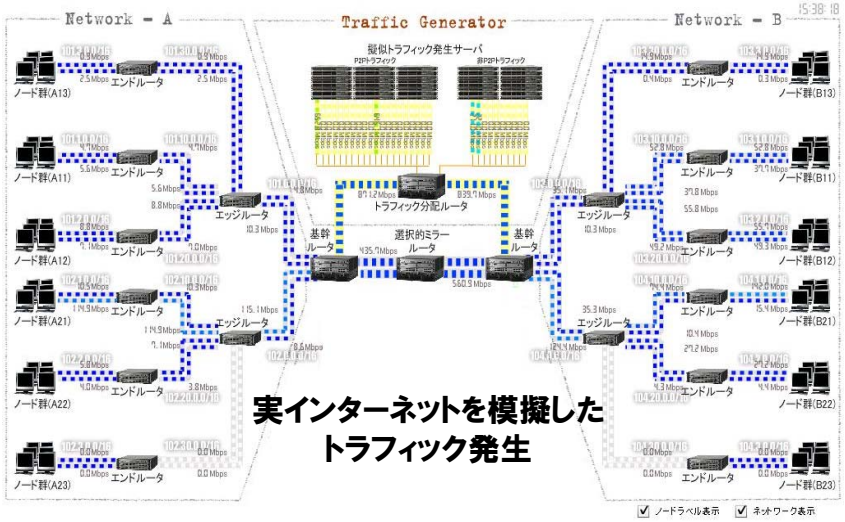
2. 活用事例

- 事例1. P2P通信の検知・制御システムの有効性検証
- 事例2. マルウェアダウンロード防止ツールの機能検証
- 事例3. Shareにおけるファイル保持ノード特定方法
- 事例4. P2Pネットワーク外に対するサービス運用妨害
- 事例5. Winnyノードの緊急停止

【 事例1. StarBEDを用いた実験紹介 】

P2P通信の検知・制御システムの有効性検証

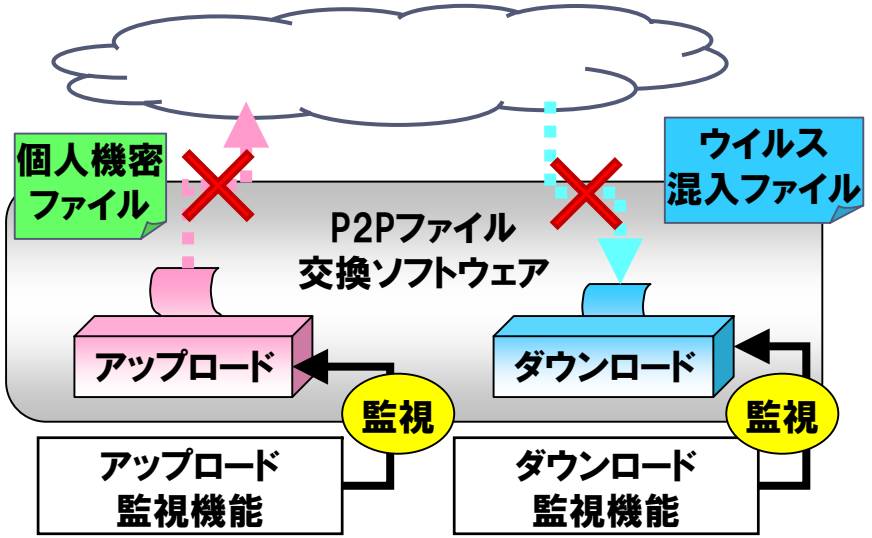
- **概要**
  - 総務省から受託した「ネットワークを通じた情報流出の検知及び漏出情報の自動流通停止のための技術開発」において開発したP2P通信の検知・制御システムの有効性（ファイルのダウンロード阻止率）を検証する。
- **実験環境**
  - トポロジ：3階層ネットワーク
  - P2Pソフト：P2Pソフト構成：7種類（計1,000台）（6仮想ノード／物理ノード）
  - 利用ツール：P2P通信の検知・制御システム
- **結果**
  - P2P通信検知・制御なしの場合、25分間のファイルダウンロード数は269個。制御ありの場合には17個。⇒94%のファイルのダウンロードを阻止



【 事例2. StarBEDを用いた実験紹介 】

マルウェアダウンロード防止ツールの機能検証

- **概要**
  - P2Pネットワーク向け開発したマルウェアダウンロード防止ツールの機能テストを実施する。
  - アップロード監視機能
    意図しないファイルアップロードを防ぐ。
  - ダウンロード監視機能
    ウイルスの疑いのあるファイルのダウンロードを防ぐ。

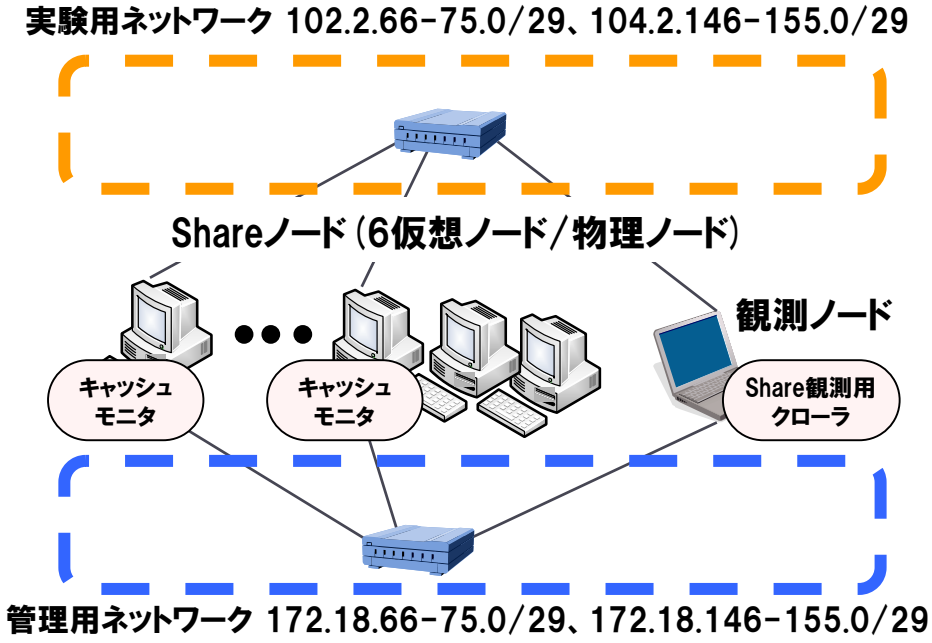


- **実験環境**
  - トポロジ：1階層ネットワーク
  - P2Pソフト：Winny（250台）、
    Share（250台）（6仮想ノード/物理ノード）
  - 利用ツール：マルウェアダウンロード防止ツール、Winny/Share観測用クローラ
- **結果**
  - Winny、Share共に、阻止対象／対象外のファイルをアップロード／ダウンロードした際に、アップロード／ダウンロード監視機能が有効に動作することを確認した。

【 事例3. StarBEDを用いた実験紹介 】

Shareにおけるファイル保持ノード特定方法

- **概要**
  - ファイル保持ノードを特定できれば、(匿名性の低下による) 適切ではないファイル流通の抑止、(IPアドレスの特定による) ファイル削除依頼の実現が可能となる。
  - ファイルの所在情報が記載されたキーを取得する際に、ファイル保持フラグに関連する(と思われる)フラグが存在することに着目した、Shareネットワークの監視手法を検証する。
- **実験環境**
  - トポロジ:3階層ネットワーク
  - P2Pソフト:Share (120台)
  - 利用ツール:Share観測用クローラ
    キャッシュモニタ
- **実験手順**
  - 開始と終了時にキャッシュモニタで
    キャッシュファイル種別を取得する。
    その間、クローラでキー情報
    (ファイル保持フラグ) を取得する。



【 事例3. StarBEDを用いた実験紹介 】

Shareにおけるファイル保持ノード特定方法

- **結果**
  - フラグがファイル保持に関連していること、ファイル保持フラグとキャッシュファイル種別との関係を調査した結果、ファイル保持フラグがONである場合、キャッシュブロック保有率=100%（完全キャッシュ）に関するファイルであることを示した。

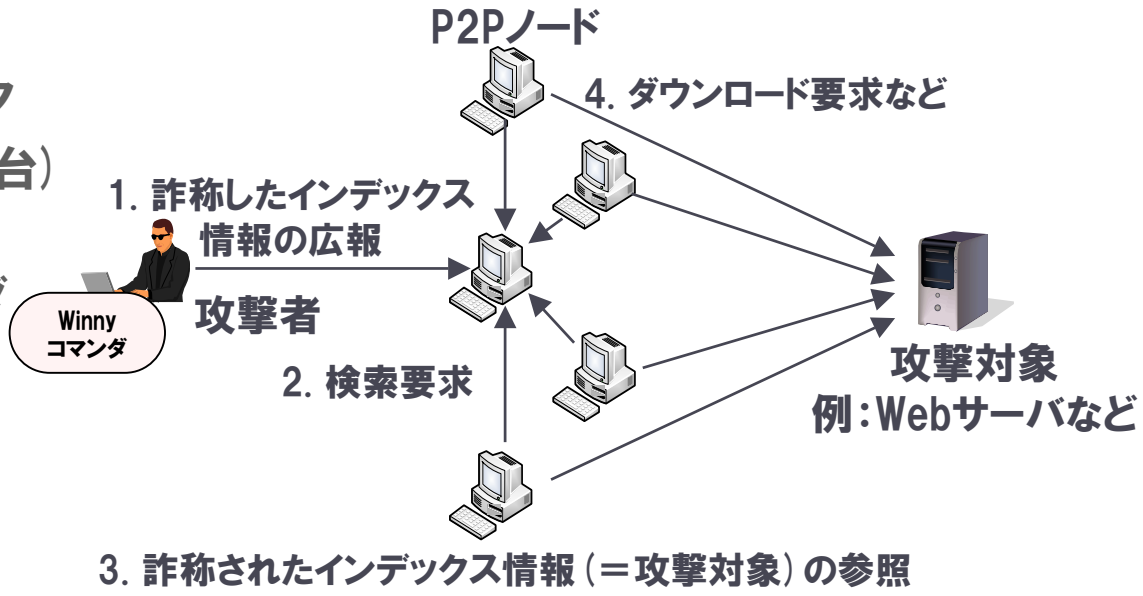
ファイル保持フラグとキャッシュファイル種別との関係

ファイル保持フラグ	件数	内訳（件数）		
		開始時	終了時	
ON	2,272	アップロードファイル	アップロードファイル	430
		完全キャッシュ	完全キャッシュ	357
			インデックス消失	2
		部分キャッシュ	完全キャッシュ	1,465
		非保持		
			インデックス未作成	18
OFF	147	拡散キャッシュ（部分）	拡散キャッシュ（部分）	14
		非保持	完全キャッシュ	2
				12
			拡散キャッシュ（部分）	119

【 事例4. StarBEDを用いた実験紹介 】

P2Pネットワーク外に対するサービス運用妨害

- **概要**
  - Winnyノードが保有する特定のファイル所在情報（キー情報）をリモートから制御することにより、ファイルの流通抑制や、ファイルのダウンロードノードを特定できる。しかし、制御の方法によっては、Webサーバなどの特定のノードに対するサービス運用妨害攻撃に悪用される可能性がある。
  - WebサーバのIPアドレスを格納した キー情報を配布し、ダウンロード操作を組合せた状態において、 Webサーバへのトラフィックの発生を定量的に示す。
- **実験環境**
  - トポロジ：1階層ネットワーク
  - P2Pソフト：Winny（1,000台）（6仮想ノード/物理ノード）
  - 利用ツール：Winnyコマンダ

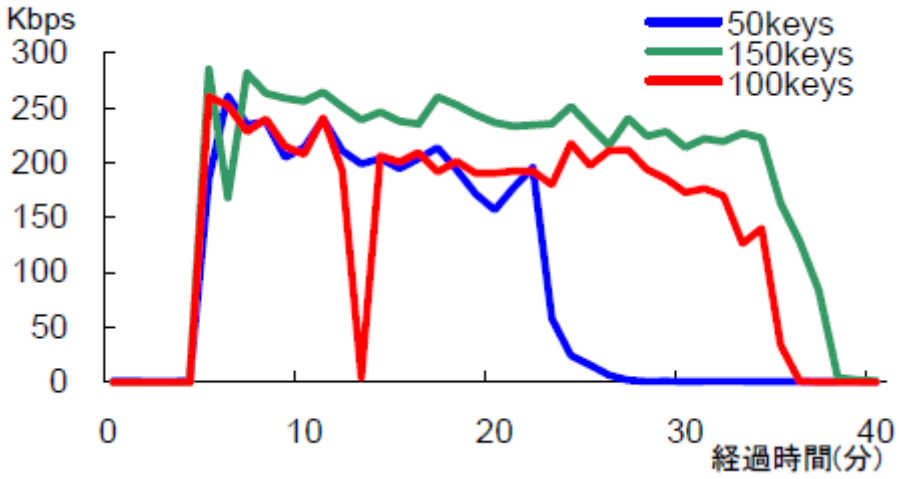


【 事例4. StarBEDを用いた実験紹介 】

P2Pネットワーク外に対するサービス運用妨害

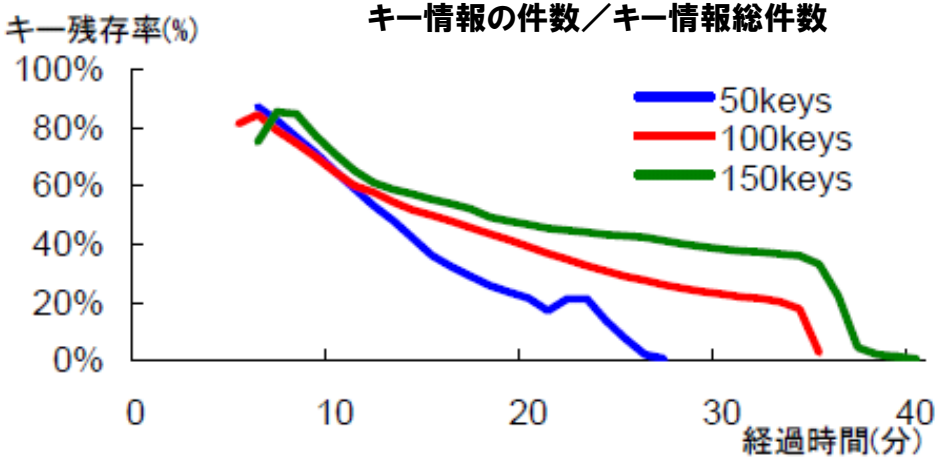
- **実験手順**
  - キー情報にWebサーバのIPアドレスと自動ダウンロード設定のトリガ対象となるファイル名を設定した50個のキー情報をWinnyコマンダ経由で配布する。同様に、ハッシュ値の異なるキー情報を100個、150個とした場合について観測する。
- **結果**
  - 誘導によって発生するトラフィック量
    データ転送速度（ピーク時のデータ）：約260Kbps（パケット量は約540pps）

誘導されたトラフィック量



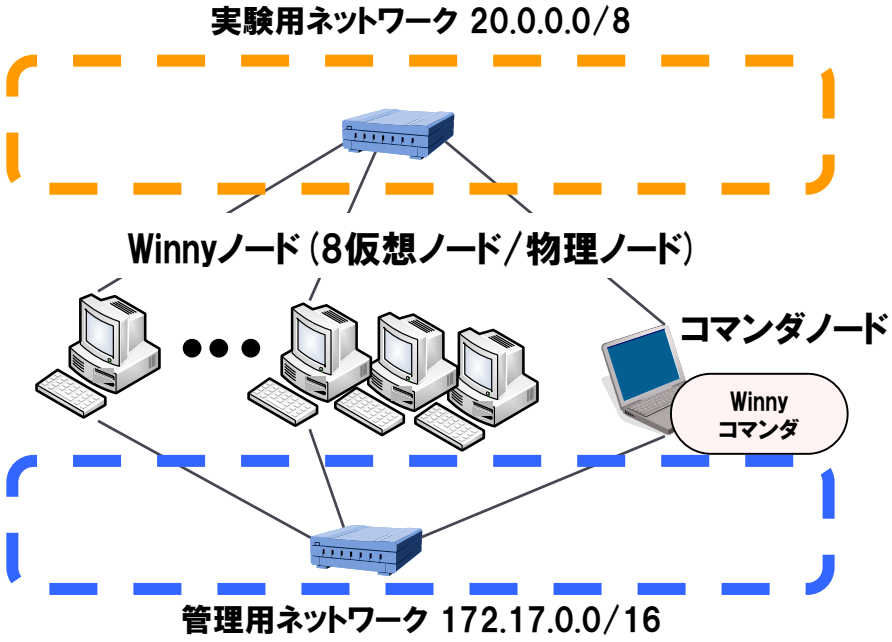
キー残存率

Webサーバの IP アドレスが格納されたキー情報の件数／キー情報総件数



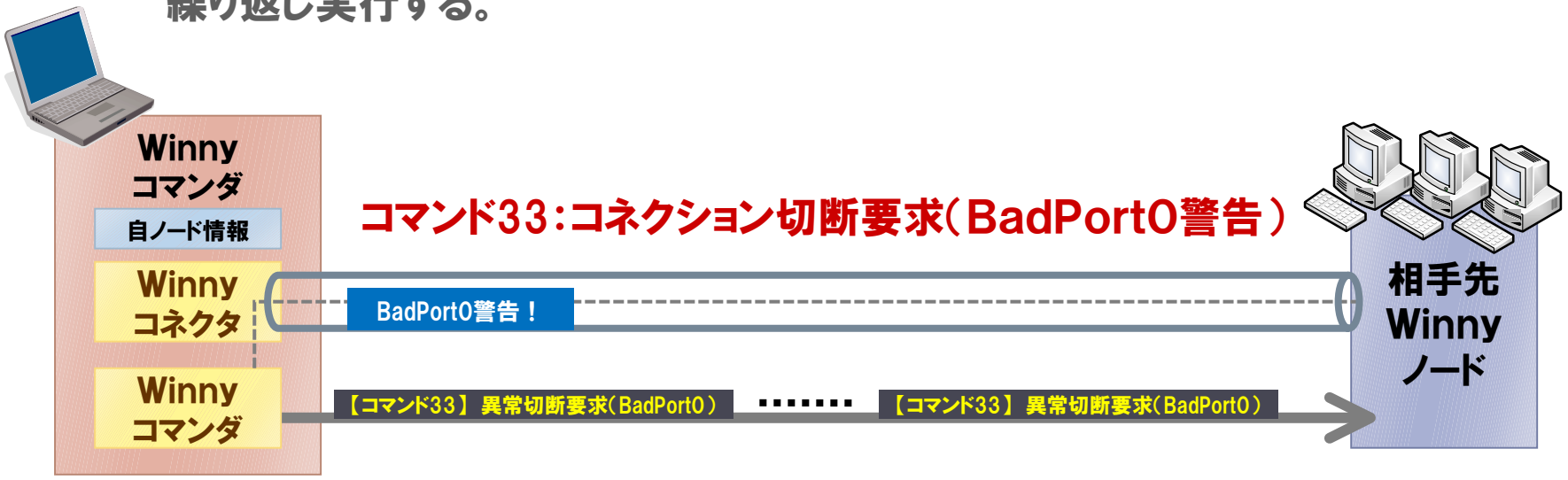
【 事例5. StarBEDを用いた実験紹介 】
Winnyノードの緊急停止

- **概要**
  - 任意のWinnyノードを停止（Winnyレベルでの停止状態）させることができるならば、緊急事態時に、Winnyネットワークをマヒさせる（Winny緊急停止ボタン構想）、情報漏えいを起こしているノードや、漏えい情報の流通を助長しているノードの活動抑止に応用できる。
  - ポートゼロ警告の大量送付ならびに、JVN#74294680を利用して、停止までの動作を観測する。
- **実験環境**
  - トポロジ：1階層ネットワーク
  - P2Pソフト：Winny（1,200台）
  - 利用ツール：Winnyコマンダ



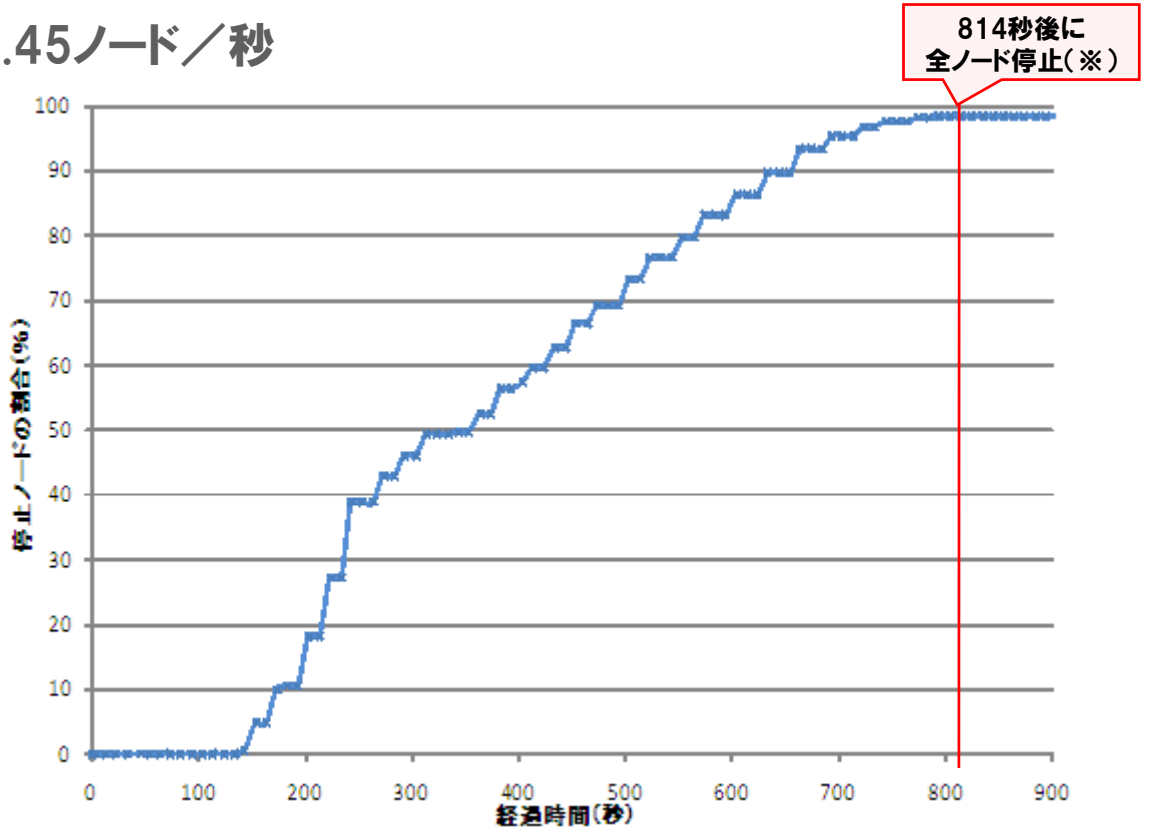
【 事例5. StarBEDを用いた実験紹介 】
Winnyノードの緊急停止

- **実験手順**
  - Winnyコマンダノード1台からWinnyノード12台にコマンド送信（ポートゼロ警告の場合200件/JVN#74294680の場合1件）する。全Winnyノードが停止するまで繰り返し実行する。



【 事例5. StarBEDを用いた実験紹介 】
Winnyノードの緊急停止

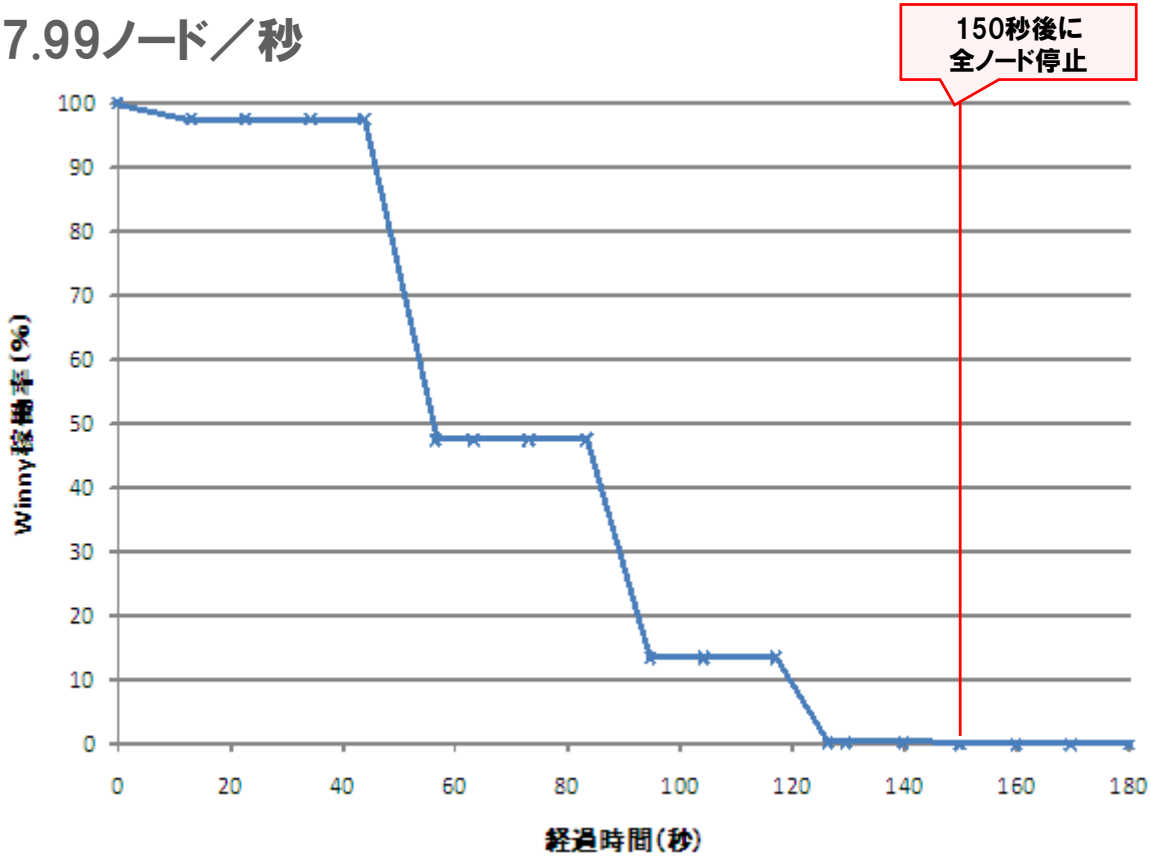
- **結果**
  - ポートゼロ警告により、全Winnyノードが停止するまでに要した時間
    814秒（13分34秒）
  - 単位停止ノード数＝1.45ノード／秒



※ Winnypノードが2％程度含まれているため100％にはならない。

【 事例5. StarBEDを用いた実験紹介 】
Winnyノードの緊急停止

- **結果**
  - JVN#74294680により、全Winnyノードが停止するまでに要した時間
    150秒（2分30秒）
  - 単位停止ノード数＝7.99ノード／秒



参考情報

事例1. P2P通信の検知・制御システムの有効性検証

- Winnyp通信検知機能の実装および評価
  情報処理学会論文誌 Vol.52 No.1, p.2-13 (2010)
- 初期パケットの乱数性に着目したP2P通信検知方式
  情報処理学会 コンピュータセキュリティ 研究報告 Vol.2010-CSEC-50 No.38 (July 1-2, 2010)
- P2P ファイル交換ソフトウェアを対象としたトラヒック解析・制御システムの基本アーキテクチャの提案
  情報処理学会 コンピュータセキュリティ 研究報告 Vol.2009-CSEC-46 No.35 (July 2-3, 2009)
- コネクション解析による P2P 通信端末検知手法
  情報処理学会 コンピュータセキュリティ 研究報告 Vol.2008 No.71 (July 24-25, 2008)
- 端末内の動作監視に基づく情報漏えいウイルスの検知手法に関する検討
  情報処理学会 コンピュータセキュリティ 研究報告 Vol.2008 No.71 (July 24-25, 2008)
- IP マーキングによる不正活動ホストの広報機能の開発
  情報処理学会 コンピュータセキュリティ 研究報告 Vol.2008 No.71 (July 24-25, 2008)
- P2Pファイル交換ソフトウェア環境における情報流通対策アーキテクチャの検討
  情報処理学会 コンピュータセキュリティ 研究報告 Vol.2008 No.21, pp.243-248 (Mar. 6-7, 2008)

事例2. マルウェアダウンロード防止ツールの機能検証

- P2Pファイル交換ソフトウェア環境における クライアント型情報流通対策システムの提案
  情報処理学会論文誌 Vol.51 No.9, p.1645-1658 (2010)
- P2Pファイル交換ソフトウェア環境における情報流通対策向けデータベースの検討
  情報処理学会 コンピュータセキュリティ 研究報告 Vol.2008 No.71, pp.123-128 (Jul. 24-25, 2008)

参考情報

事例3. Shareにおけるファイル保持ノード特定方法

- P2Pファイル交換ソフトウェア環境Shareにおける効率的なファイル保持ノード特定手法
  情報処理学会 コンピュータセキュリティ 研究報告 Vol.2010-CSEC-49 No.5 (May 11, 2010)

事例4. P2Pネットワーク外に対するサービス運用妨害

- P2Pファイル交換ソフトウェアWinnyを対象としたオーバーレイネットワークの制御実験
  情報処理学会 コンピュータセキュリティ 研究報告 Vol.2009-CSEC-45 No.22 (May 28-29, 2009)

その他

- P2Pファイル交換ソフトウェア環境向け注意喚起メッセージングシステムの提案
  情報処理学会 コンピュータセキュリティ シンポジウム 2009 (Oct.26-28, 2009)
- クローリング手法を用いた P2P ネットワークの観測
  情報処理学会 コンピュータセキュリティ 研究報告 Vol.2007 No.48 (May 25, 2007)

END

StarBED P2Pオーバーレイネットワーク環境の
構築とその活用

2011/01/27

(株) 日立製作所

本内容は、総務省から受託した「ネットワークを通じた情報流出の検知及び
漏出情報の自動流通停止のための技術開発」の成果の一部です。