

P2P概論
～DHTとセキュリティを中心に～

2004年11月7日

西谷 智広

自己紹介

1999年 通信系研究所でP2Pのコンテンツ流通、
セキュリティに対する研究を行う。

2002年 Tomo's HomepageにてP2P記事の連載を開始。

2004年 Tomo's HotlineにてP2Pに関するトピックで
集中的に連載開始。

現在：

業務：コンテンツ配信に関するシステム設計の検討を行う。

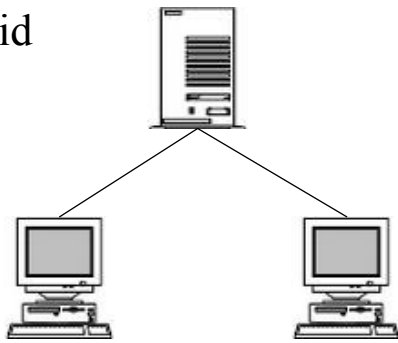
業務外：DHTによるSkypeライクなVoIPシステムを検討中。

DHTを使った新システムの探求。

■趣味：バイオリン、旅行、グルメなどなど。

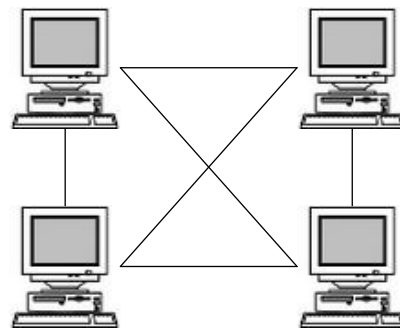
P2Pの種類

Hybrid
P2P



- ・サーバが必要
- ・認証、課金が可能
- ・ノードの管理がし易い
- ・初期コスト高

Pure
P2P



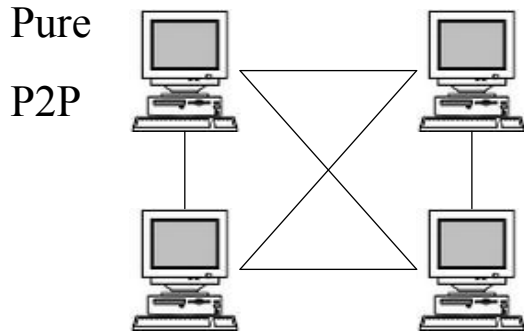
- ・サーバレス
- ・認証、課金が困難
- ・ノードの管理が困難
- ・初期コスト低

P2Pの応用例

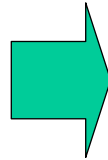
- ・ファイル共有-Napeter,Gnutella,WinMX,Windy
- ・VoIP-Skype
- ・IM-Yahoo,MSN
- ・センサーネットワーク
- ・グループウェア-アリエルAir-one,grove
- ・分散コンピューティング
-

Skypeの登場によってP2Pビジネスモデルの見直しが行われる？

DHT(分散ハッシュテーブル)とは？



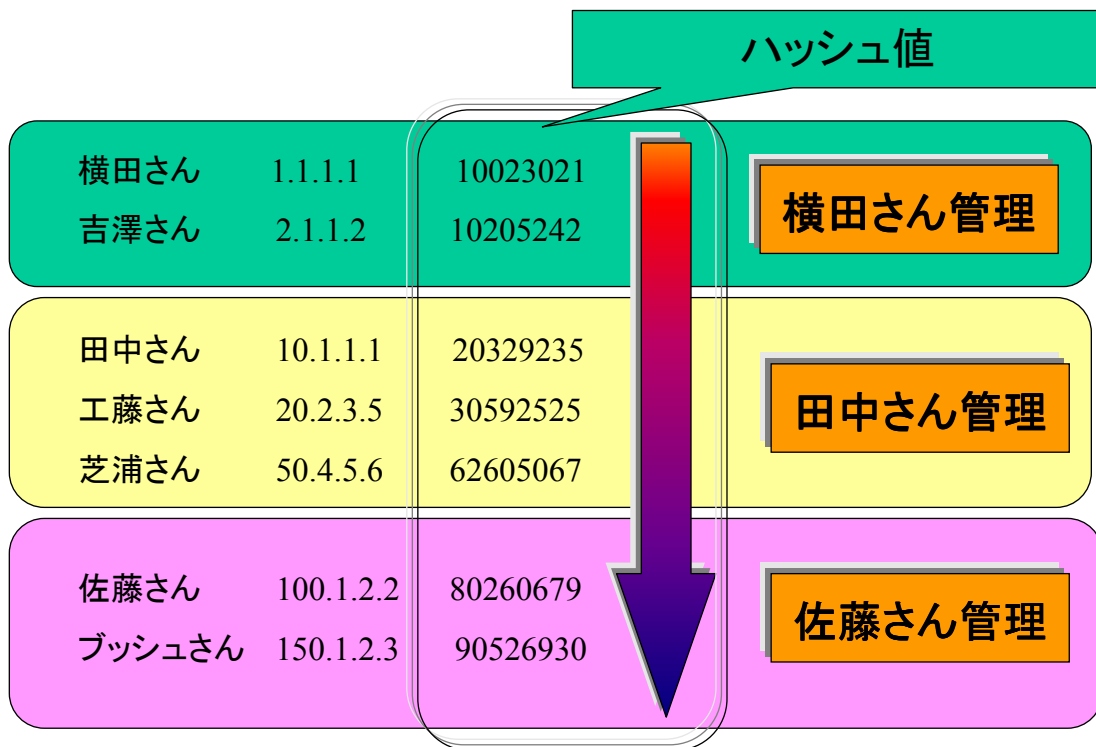
- ・スケーラビリティが乏しい
- ・全てのノードに対する検索が困難
- ・ノード離脱による情報の欠落



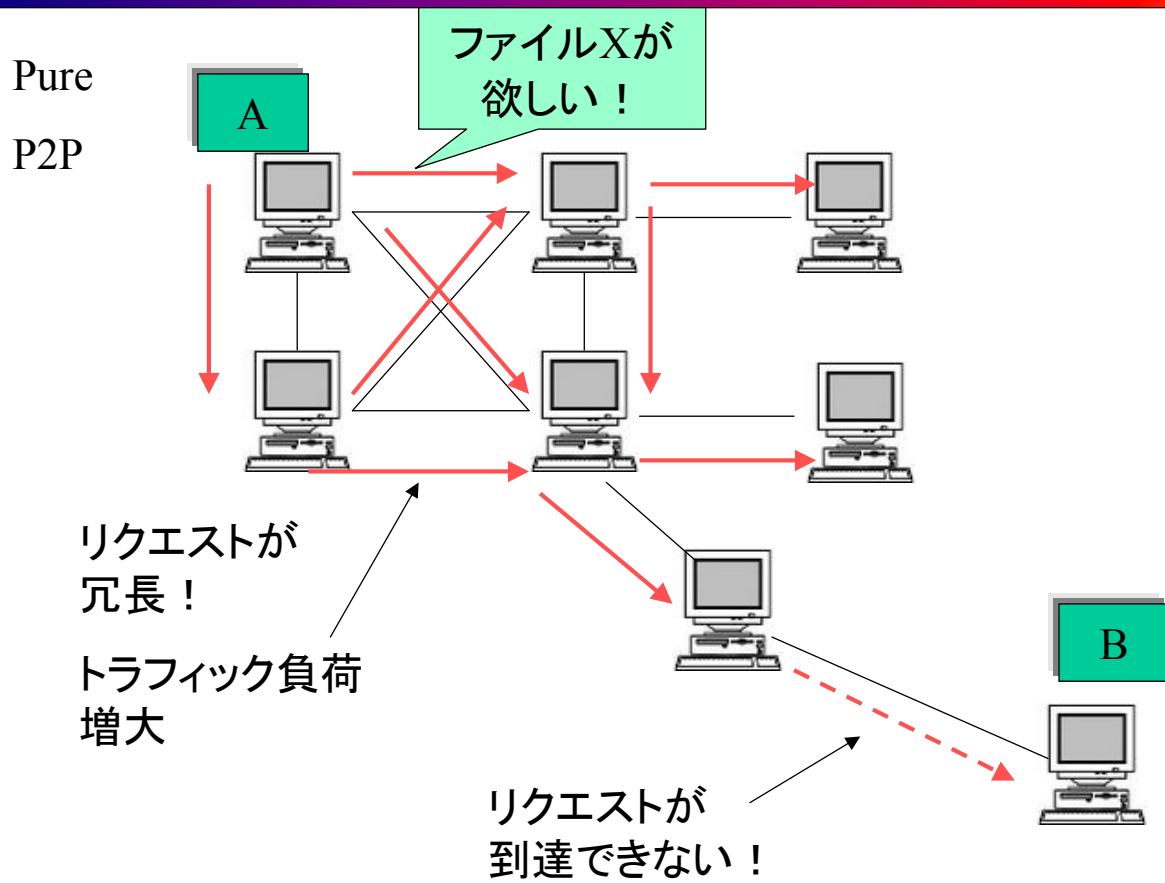
DHTの特徴

- ・スケーラビリティが良好
- ・全てのノードに対する検索が可能
- ・ノード離脱でも情報は引継ぎ
- ・様々アプリケーションの実現が容易に可能

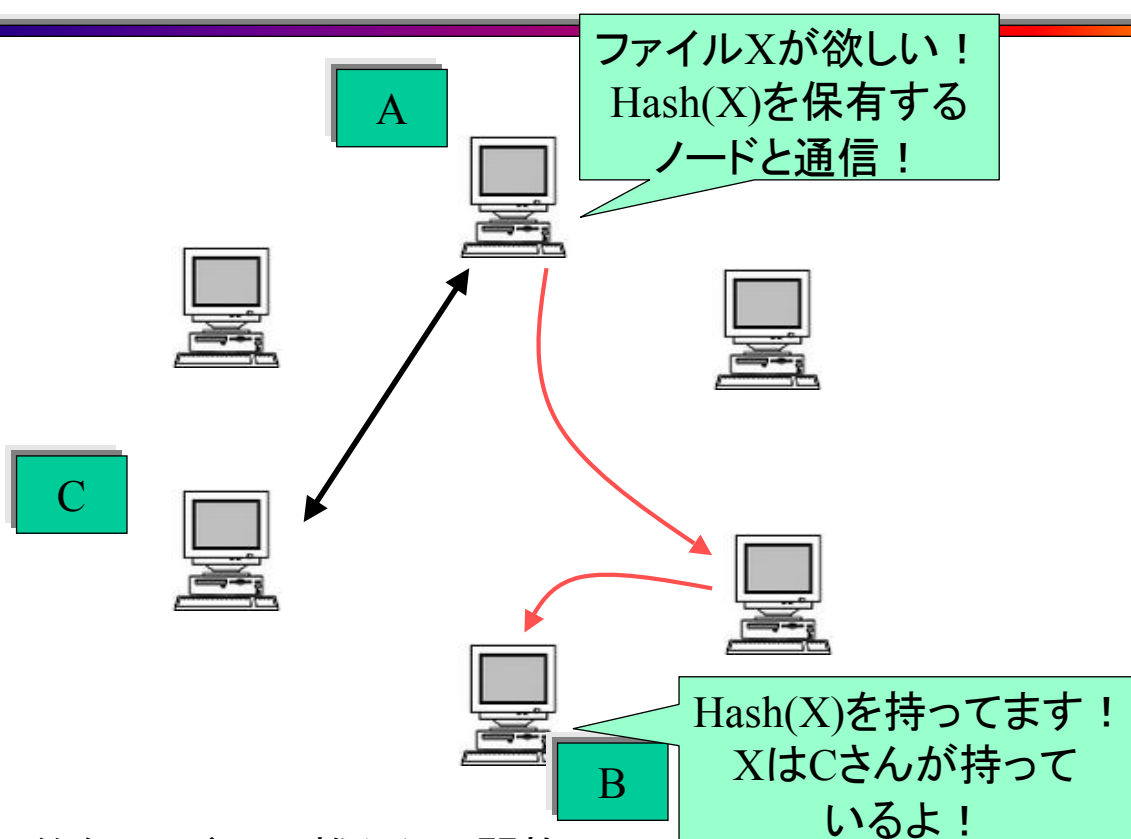
DHT(分散ハッシュテーブル)の仕組み



通常Pure-P2Pの通信



DHTの通信



※物理的なノードの距離からの開放

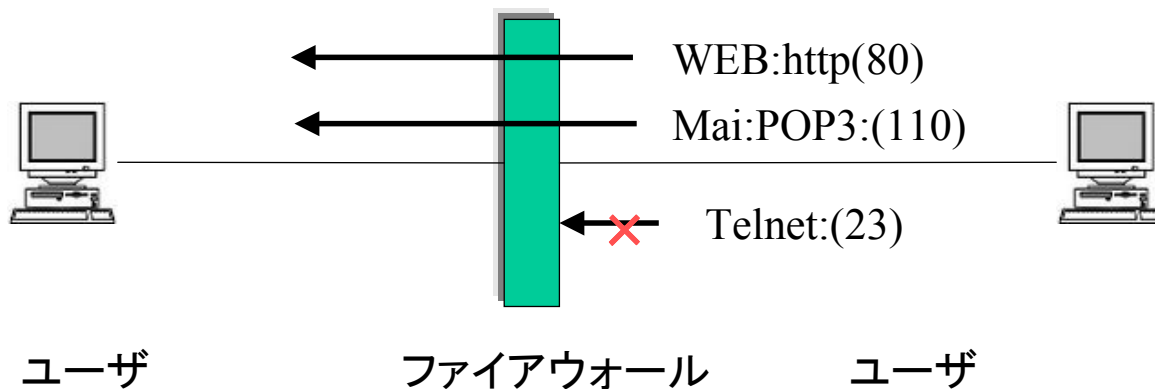
DHTの応用例

- ・ファイル共有
- ・IM
- ・掲示板,Blog
- ・VoIP
- ・匿名プロキシ
-

同じ仕組みで様々なアプリケーションに応用可能。

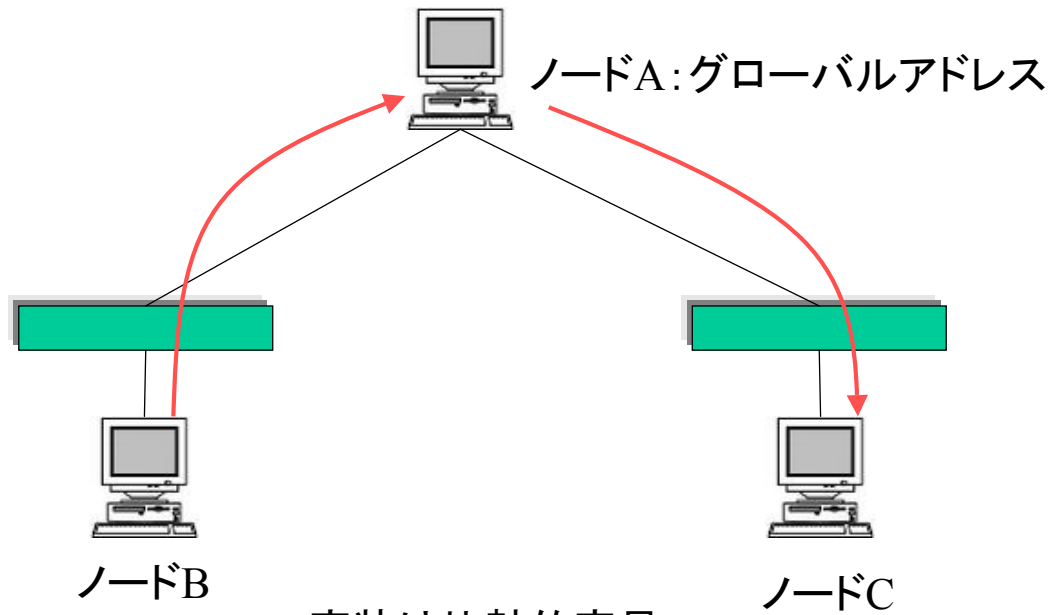
ファイアウォール越え通信

- ・Skypeによって大きく注目された技術



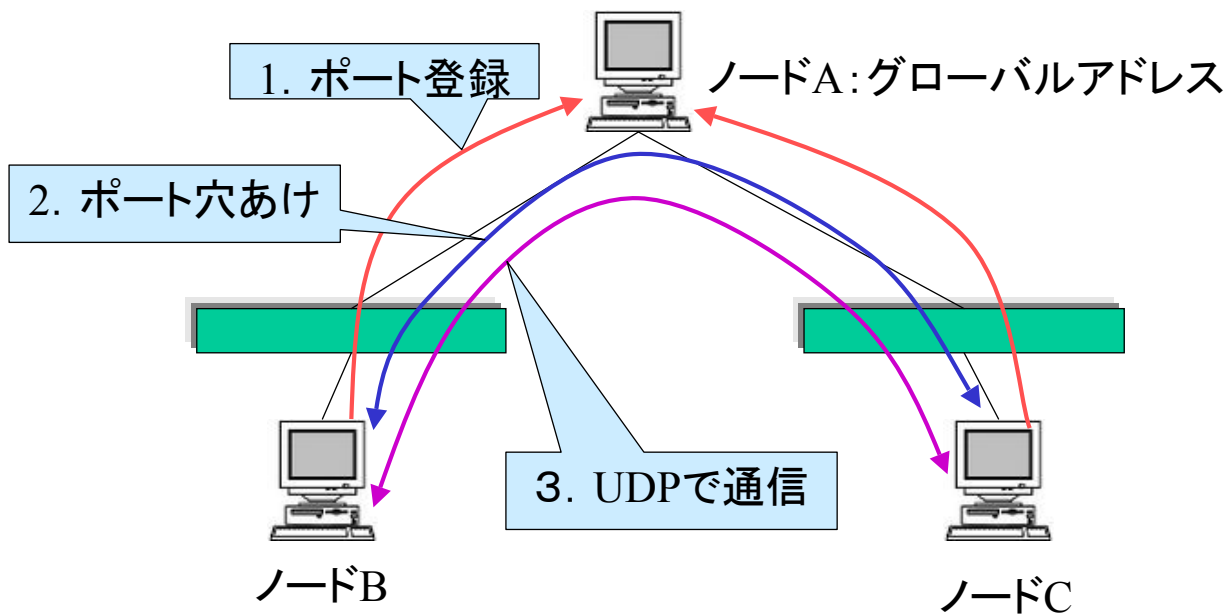
ファイアウォールは unnecessaryな通信を遮断する。
⇒P2P通信をする時には「穴あけ」をする必要がある。

ファイアウォール通過技術～ノード介在型



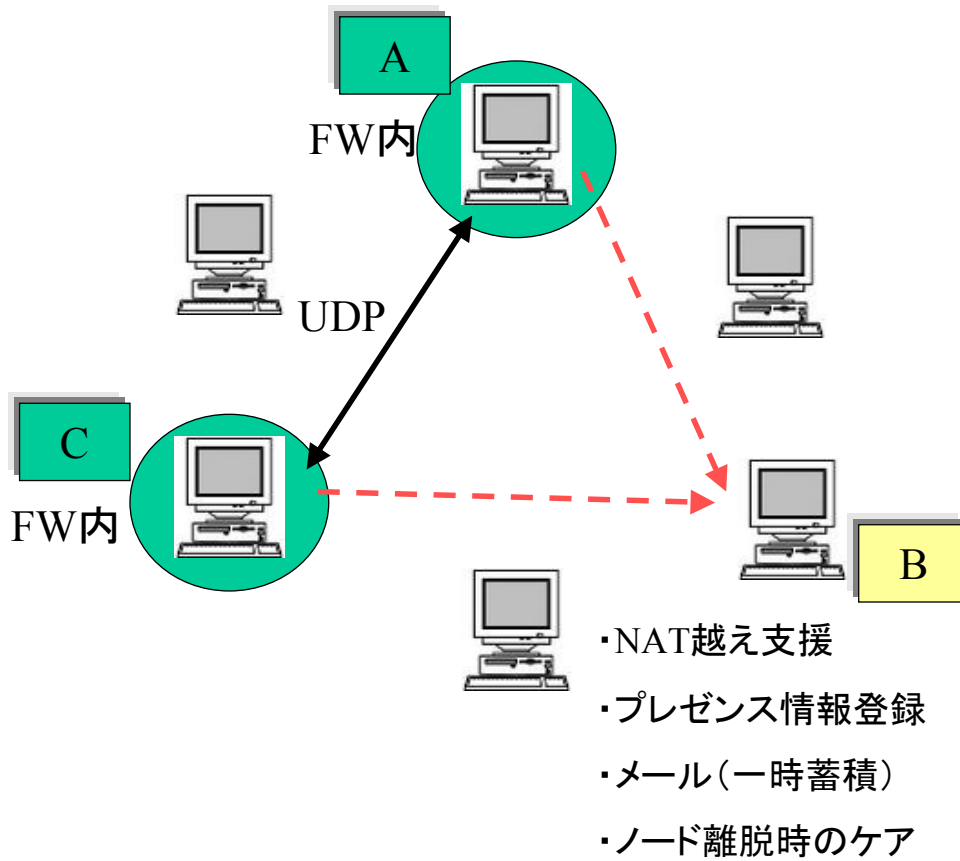
- ・実装は比較的容易
- ・セキュリティは？
- ・ノードAの負担大きい

ファイアウォール通過技術～UDP HolePunching



- ・実際の通信はP2P、ノード介せず
- ・全てのファイアウォールを通過できるとは限らない。

DHT+UDP HolePuncingでSkypeを超える？



P2Pとセキュリティ

- ・匿名性 ⇒MIX-net,秘密分散法
- ・認証 ⇒PGP,PKI
- ・ウィルス、ワーム対策 ⇒ウィルス対策ソフト、IDS
- ・情報流出 ⇒セキュリティポリシ

.....

P2Pと認証

■サーバレスで認証をするのは困難。

1) PGP

⇒本当に信頼できるのか曖昧。

気軽なコミュニティを形成するには良いかも。

2) PKI

⇒課金などをする上では必要不可欠？

証明書のライフサイクルをどうケアするか？

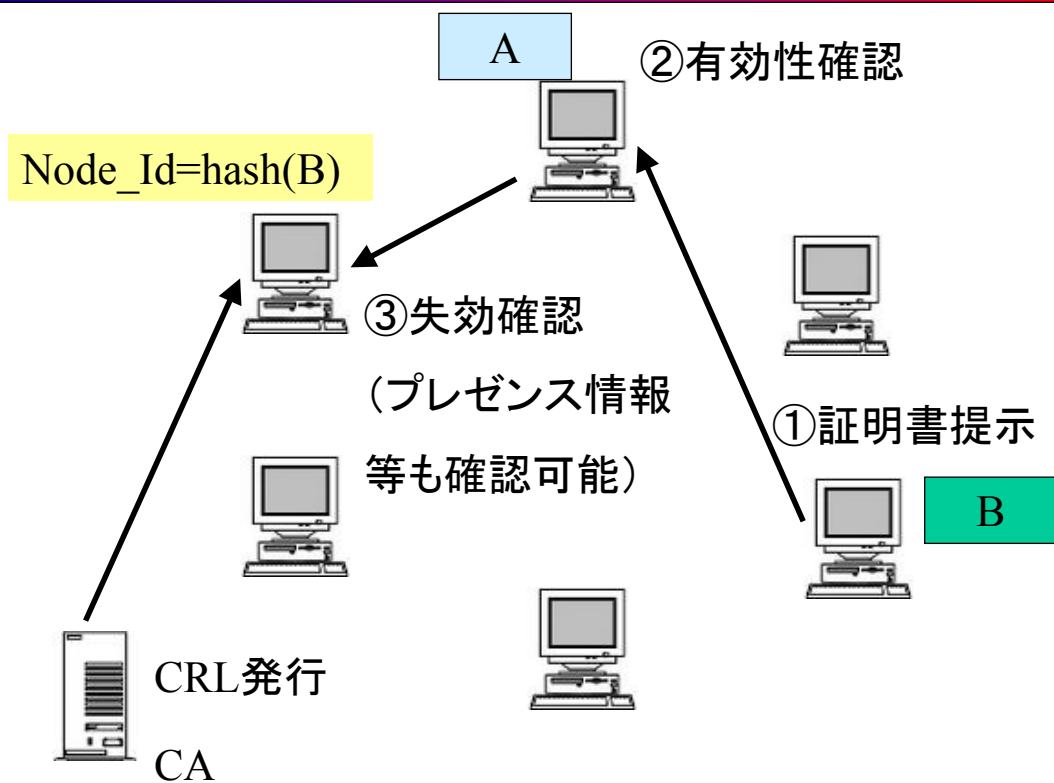
・証明書発行、証明書有効性停止(CRL?)

3) 認証サーバ

⇒サーバに集中して負荷がかかるけども良い？

ただし、きめ細かい認証ポリシーは実現可能。

PKI+DHTの親和性



P2Pのウィルス、ワーム対策について

P2Pソフトは基本的には必要ポートを空ける必要あり。

■ポートフィルタリング以上の対策が必要。

⇒FW、ルータ:ステートフルインスペクション

⇒PC:パーソナルファイアウォール

ウィルス対策ソフト

■懸念点

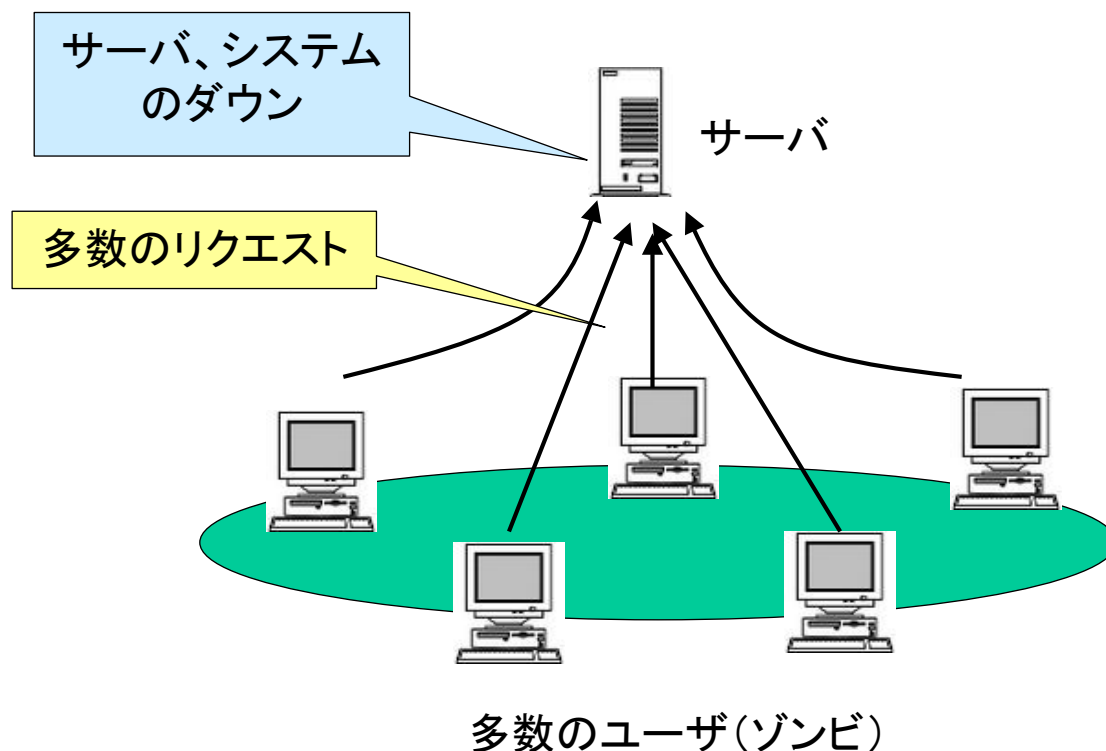
・P2Pソフト(特に和製)に対するセキュリティベンダのケアが遅い!

・ポートを空けると、そのポートに対してケアできない

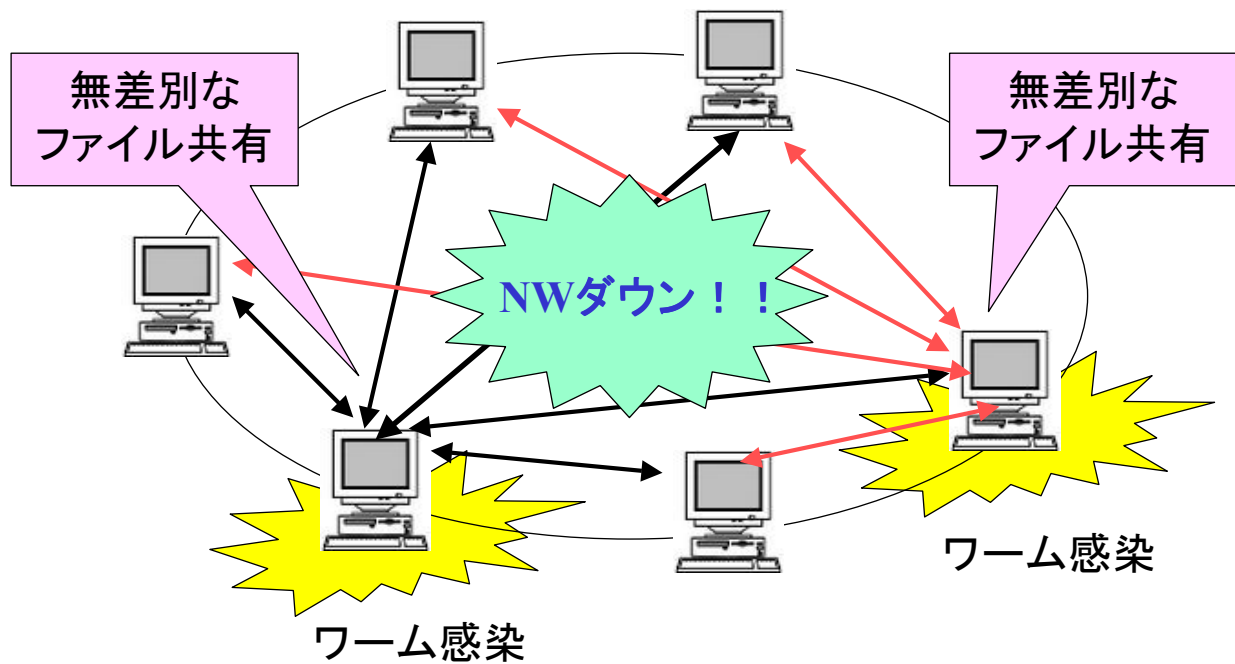
ルータ、パーソナルFWが存在する。

⇒早期に大規模なワーム、ウィルス感染の可能性

DDoS攻撃とは?



新たなDDoS攻撃の可能性



■トラフィック型DDoS攻撃がいずれ出現する？

まとめ

- DHT(分散ハッシュテーブル)でPure-P2Pの問題点をクリアできる場合がある
- P2Pユーザはセキュリティ情報に対して常にウォッチする必要がある。

お知らせ

◇P2P勉強会

- ・2月～3月の土or日に開催予定
- ・会場は都内を予定
- ・P2Pに関連した講演＋懇親会

⇒講演者 & 参加者募集中！！

ご清聴ありがとうございました！

西谷 智広

tnishita@yahoo.co.jp

Tomo's Homepage (HP)

<http://homepage3.nifty.com/toremoro/index.html>

Tomo's Hotline(Blog)

<http://toremoro.tea-nifty.com/>