# P2P 掲示板「新月」の プロトコルとデータ構造

Fuktommy

2004 年 9 月 4 日

# 自己紹介

- P2P 掲示板「新月」の作者
- P2P ファイル共有ソフト「pushare」の作者
- 2ch ブラウザ「プッ　ロクシー」の作者
- 掲示板風 Wiki「つ Wiki」の作者
- 掲示板風 Blog「DCard」の作者

# 概要


- はじめに
- ネットワークの生成
- 書き込みの伝播
- データの補完
- アプリケーション
- おわりに

# はじめに

2ch での動物病院名誉毀損裁判

↓

- 発言者が責任を取る
- 管理者が責任を取る

↓

- 発言者が特定されないようにする
- ノード管理者は気軽に発言を削除できる

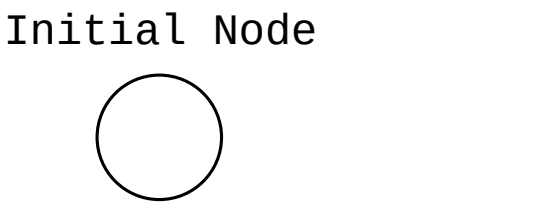
↓

バケツリレー方式

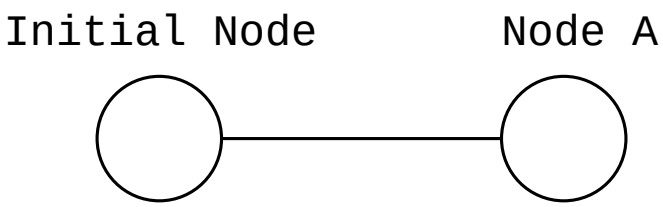
# ネットワークの生成 (1)

初期ノードの 1 つの枝に注目する

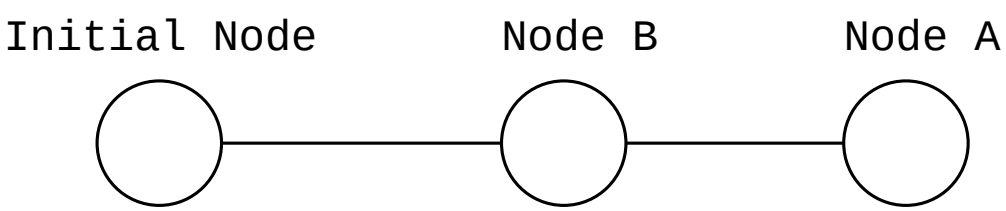
最初の状態




1 つ目のノードが接続する

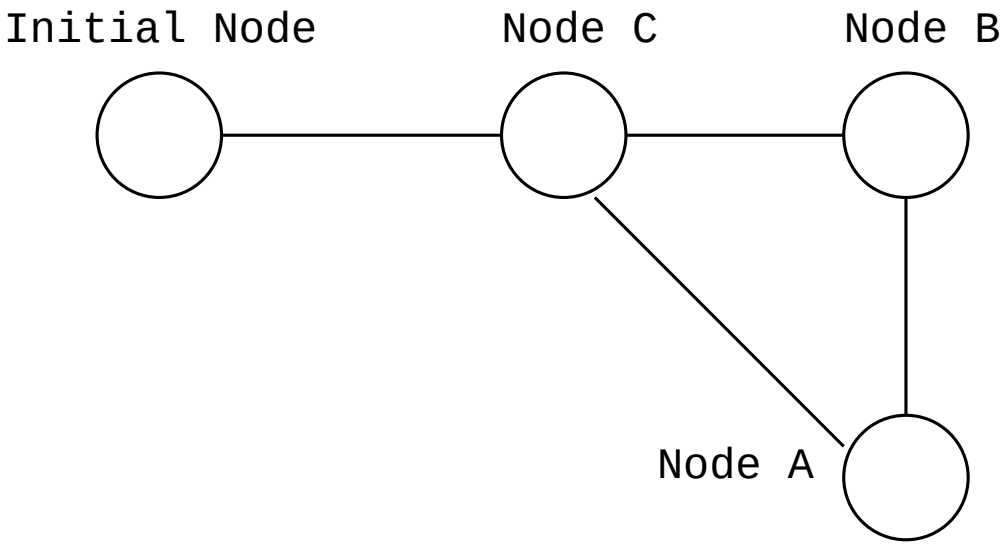



2 つ目のノードが接続する



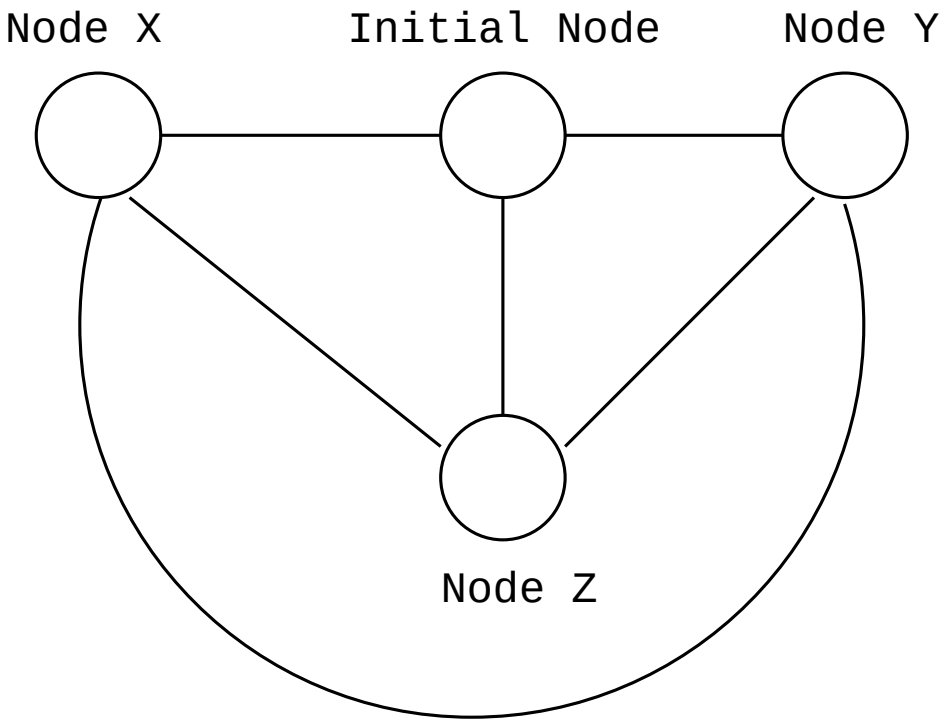
# ネットワークの生成 (2)

3 つ目のノードが接続する



# ネットワークの生成 (3)

初期ノードには複数の枝がある




全てのノードはこのように接続している

# 書き込みの伝播 (1)

原理はブロードキャスト

- あるノードで発生した書き込みは全てのノードに伝播する
- 転送量を減らす工夫が要る

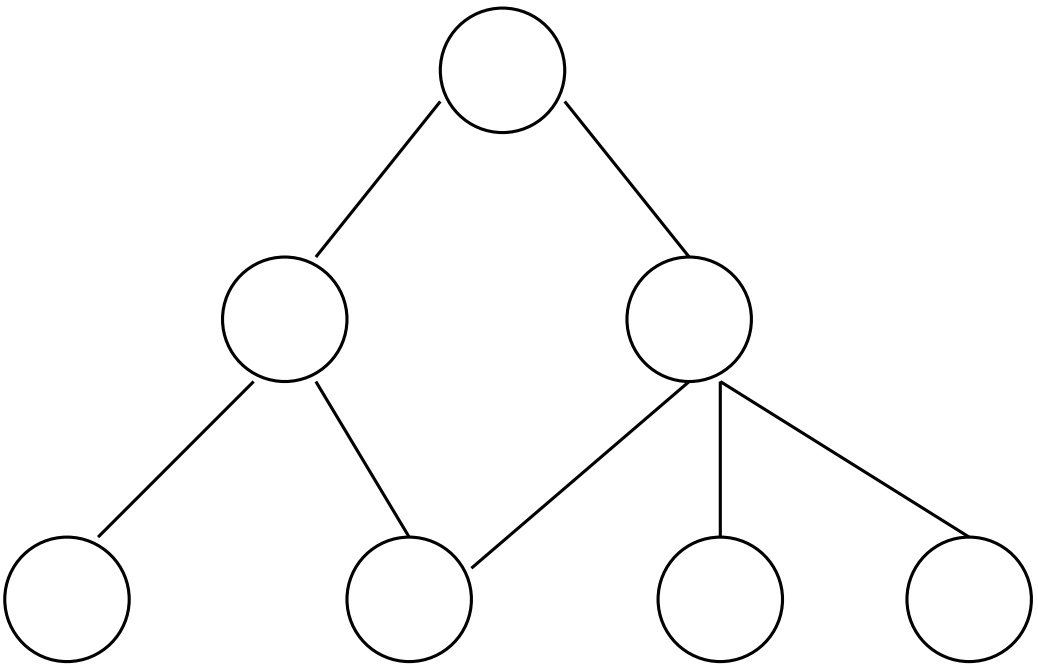
↓

情報を $2$ つに分ける

- 書き込みがあったという情報
- 書き込みの中身

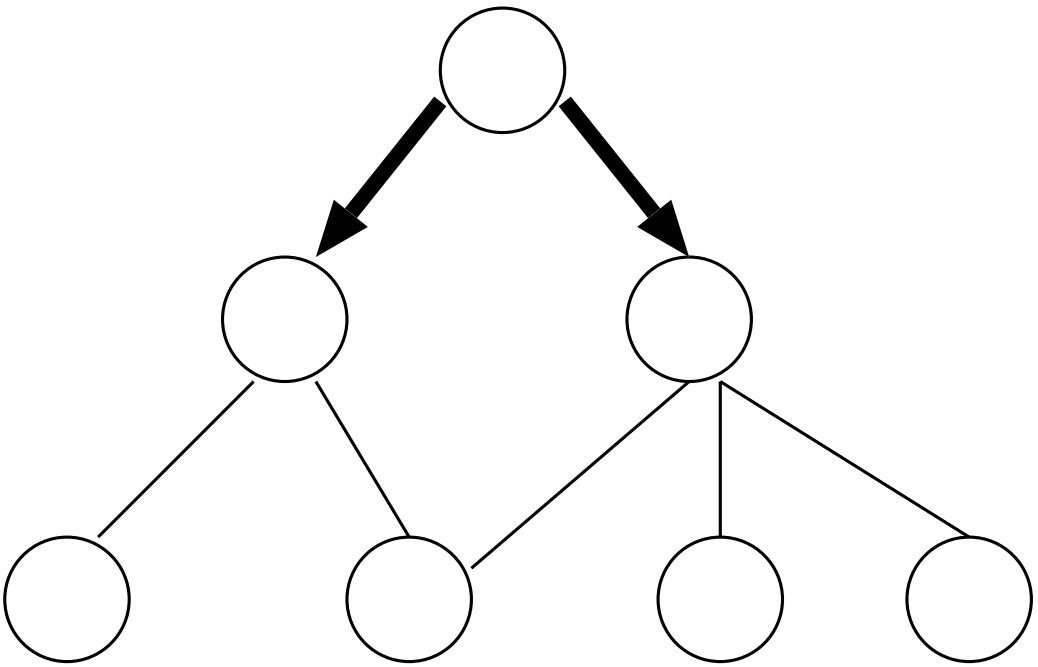
# 書き込みの伝播 (2)

ネットワークの例



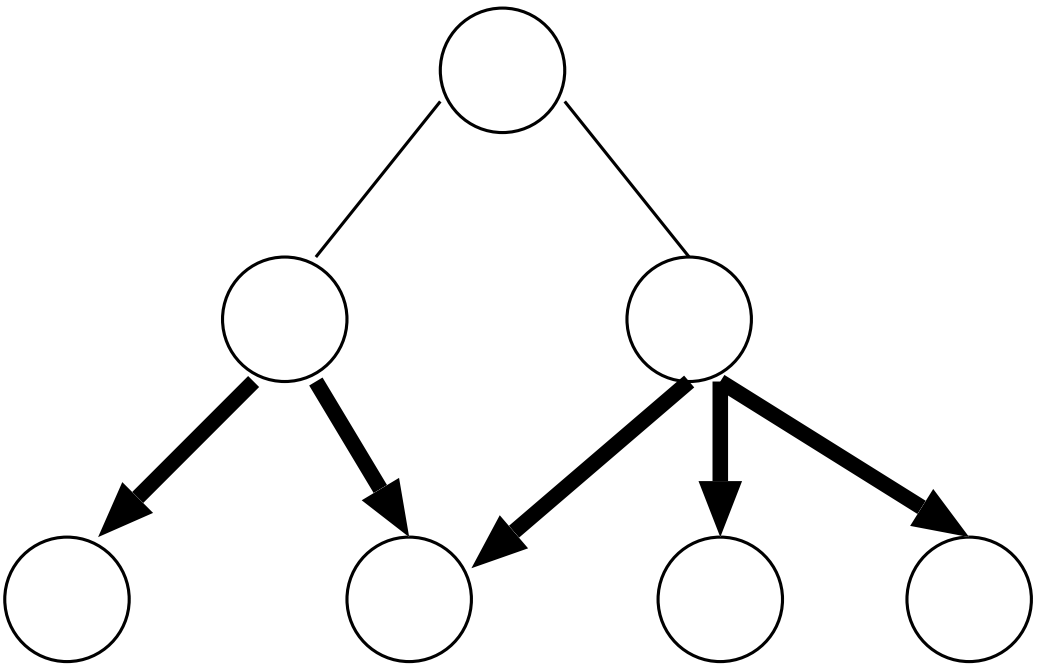
# 書き込みの伝播 (3)

書き込みがあったという情報が流れる



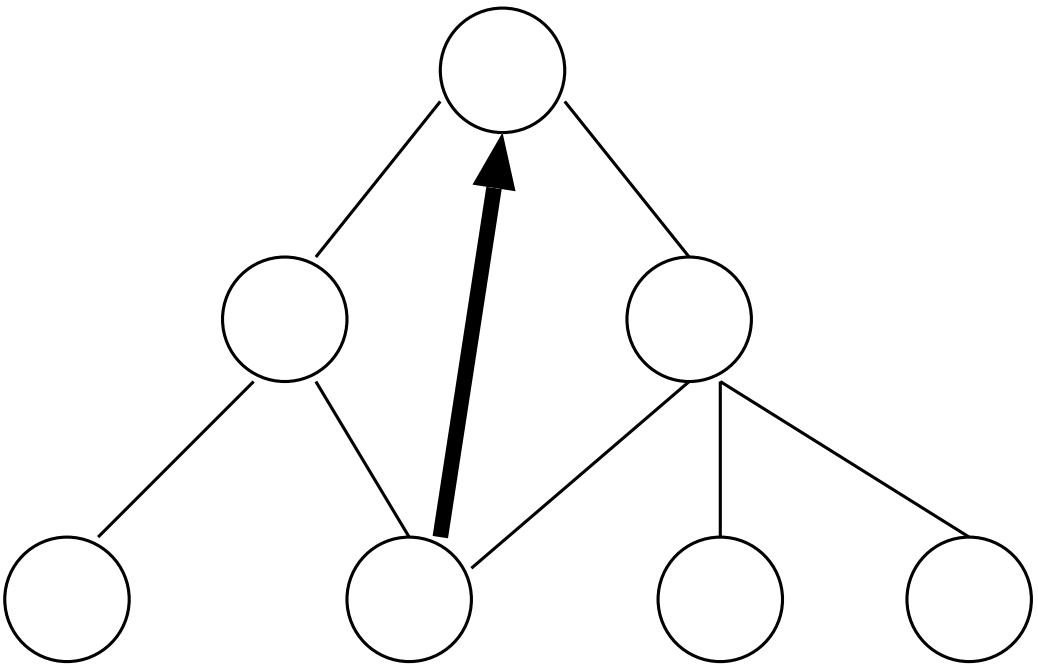
# 書き込みの伝播 (4)

書き込みがあったという情報の伝播



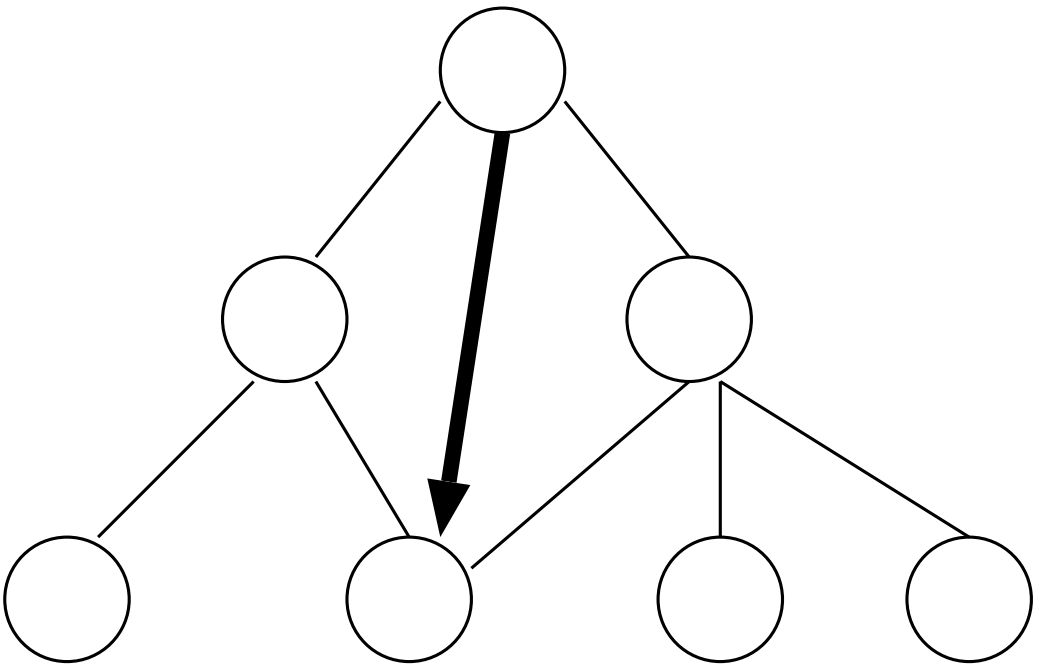
# 書き込みの伝播 (5)

その書き込みが欲しいノードがある



# 書き込みの伝播 (6)

書き込みの内容の送受信



書き込み内容を受信したら、そのノードは書き込みがあったノードと同じように振舞う。

# 書き込みがあったという情報の内容

/server.cgi/update/ファイル名
  /タイムスタンプ/ID/ノード名

/server.cgi/update
  /thread_52696E474F6368E7B78FE59088
  /1091938245
  /0bd020008077fdd9c594c613aacaa738
  /192.168.1.1:8000+server.cgi

GET メソッド→ shinGETsu

# 書き込みを取得する命令の内容

/server.cgi/get/ファイル名
  /タイムスタンプ/ID

/server.cgi/get
  /thread_52696E474F6368E7B78FE59088
  /1091938245
  /0bd020008077fdd9c594c613aacaa738

GET メソッド→ shinGETsu

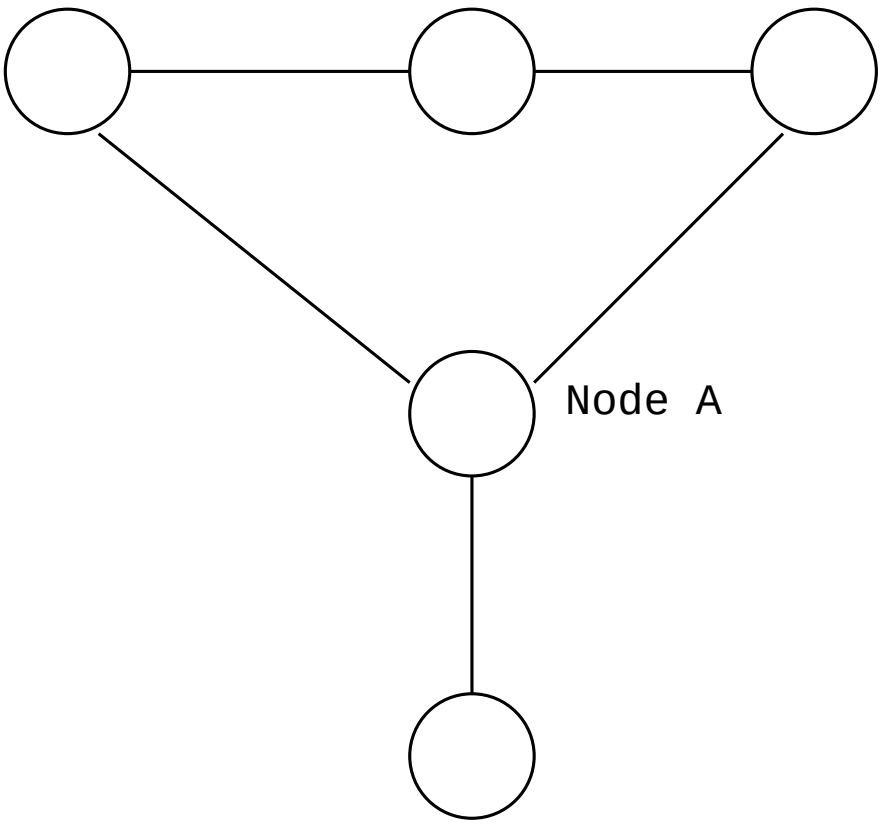
# 書き込みの内容

1091938245<>

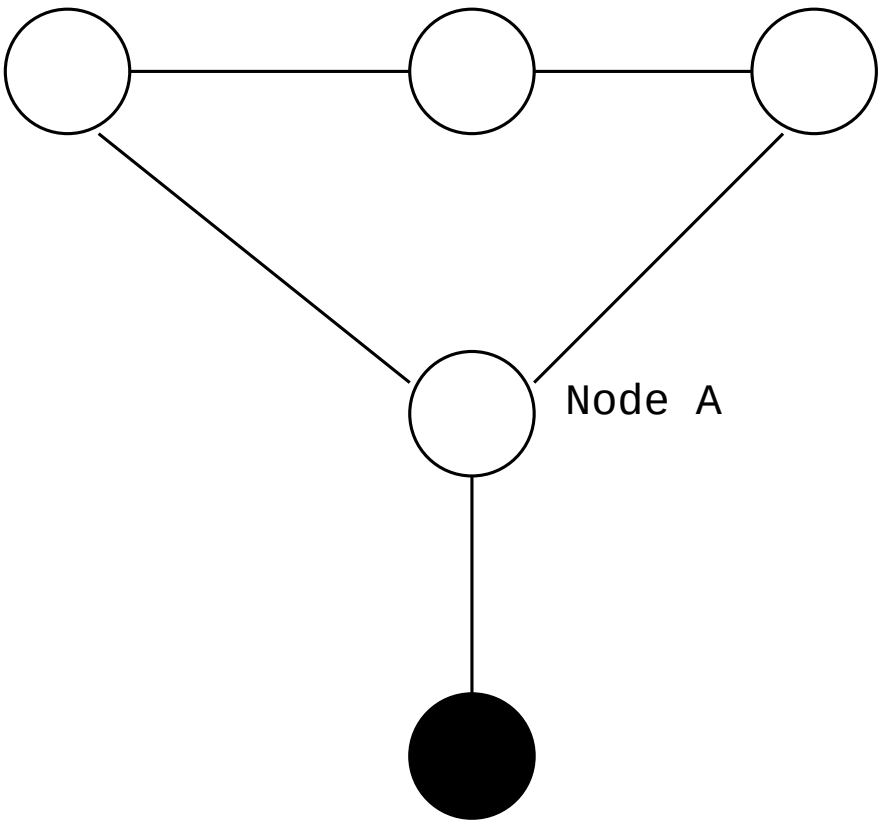
0bd020008077fdd9c594c613aacaa738<>

body:RinGOch がんばれ<br>超がんばれ

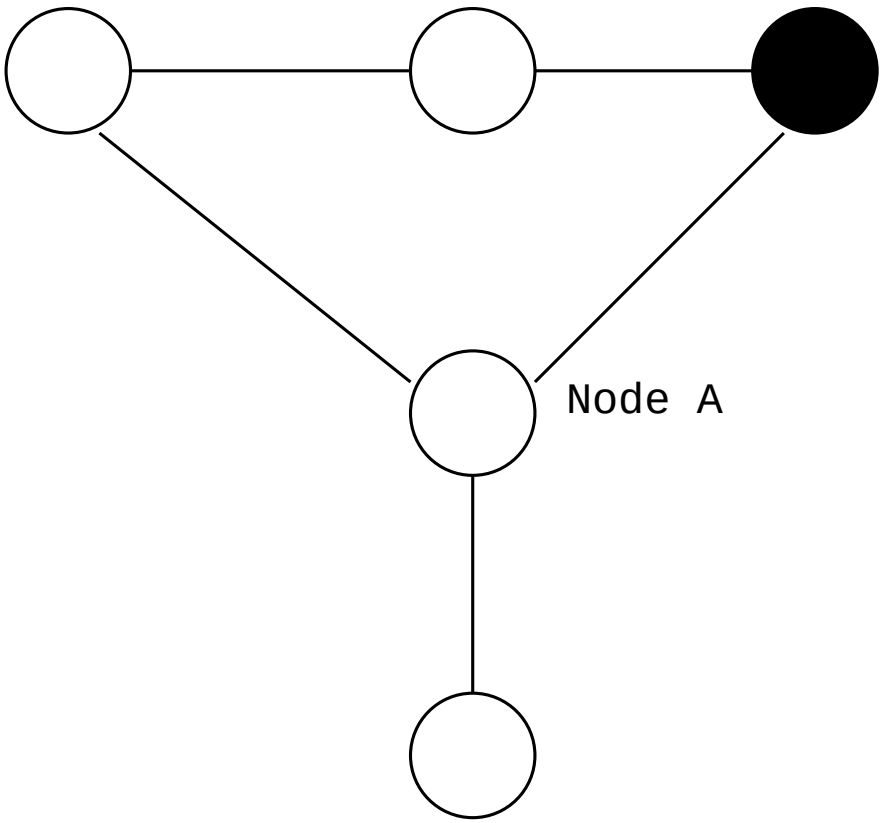
# データの補完 (1)



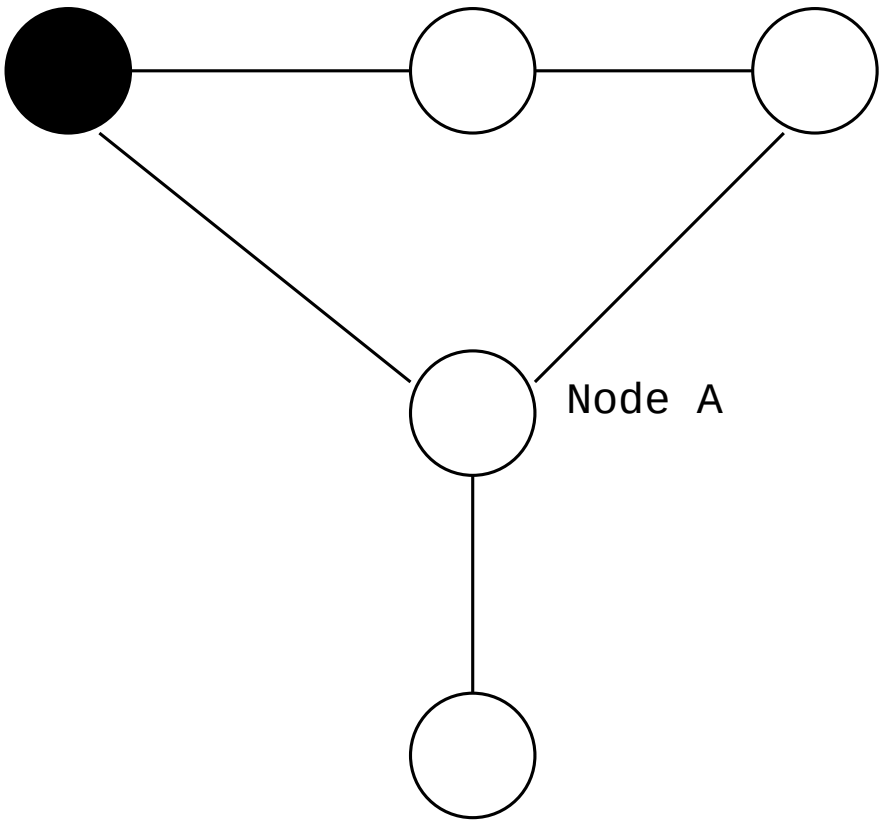
# データの補完 (2)



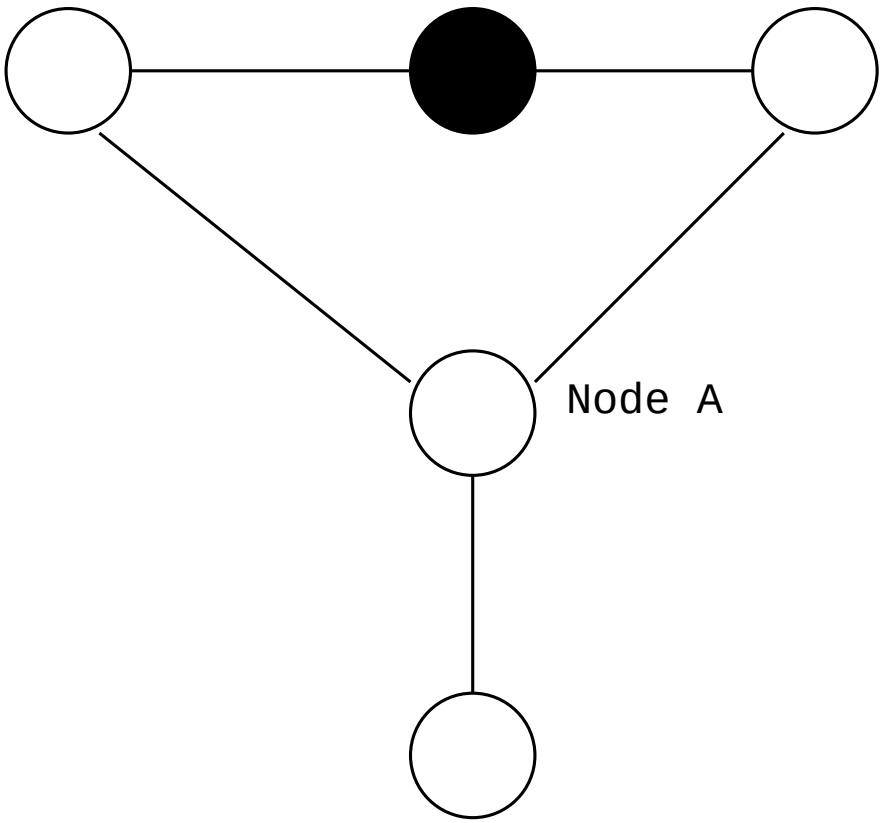
# データの補完 (3)



# データの補完 (4)



# データの補完 (5)



# アプリケーション層と通信層

通信層の上にアプリケーション層が載っている。

- アプリケーション層
- 削除関係
- 署名関係
- 通信層

## 署名

1. 秘密鍵を用意しておく
2. 本文 (書き込み本文や名前など) を連結する
3. MD5SUM を計算する
4. Apollo トリップルーチンで署名と公開鍵を計算する
5. それぞれ Base64 エンコードする

```
1077012086<>
7889e7dbe2efbc7d0d0eb9e7445c21c5<>
pubkey:nR+44NHyRSLTLZxDeHv5NENcnLDILuClhXe3H4tb
hyLNDjO543DGdJF6PbYUnX86/rCcCOAS0eZO3zH5SlYsAA<>
sign:IVscZ3IGvlbZQT/UM8isu6Th7KrX0SnO3Ipkcz6zaf
ClDkwR18SdpOHUYTw4GFRf3KxOqc/BULkky1sBFyWVAA<>
target:body<>body:key=hoge
```

## Apollo トリップルーチン

WinnyBBS のトリップが基になっている。WinnyBBS のトリップは RSA 公開鍵暗号を利用したもので、鍵長が 64bit。

Apollo の鍵長は 256bit。トリップ=公開鍵そのもの、トリップ元の文字列=秘密鍵そのもの。

鍵生成では素数の判定をしているが、精度を落として速度を重視している。

## 削除信号

remove_stamp と remove_id で削除対象のレコードを指定する。

署名と組み合わせると自動削除もできる (実装依存)。

免罪符的な意味合いが強いが . . .

1090630743<>
a99749da658ba1fbb437682604171 3a6<>
name:管理人の中の人などいな (ry<>
body:偽造ファイルとの報告あり、削除情報を伝播させてみた<>
remove_stamp:1086970730<>
remove_id:362bb56f9aec5618cbef2b9abcb1af74

# 複数のアプリケーション

- 旧式ゲートウェイ
- 新型ゲートウェイ (Wiki 風ゲートウェイ)
- 新型ゲートウェイ+ノート
- 新型ゲートウェイ+ノート+P2PWeb
- 別のゲートウェイ

↓

- リスト
- スレッド
- ノート
- P2PWeb
- 別のアプリケーション

## アプリケーション＝プラグイン

Perl 版ではアプリケーションは 1 つづつの CGI として実装されている。概念的なものであるから、必ずしも実装とは対応しない。

アプリケーションはアプリケーション層の機能であり、キャッシュファイルのデータ形式に対応する。

# おわりに

今後の課題

- 用語の統一
- 仕様と実装の明確な区分
- 仕様書の作成
- RFC にする野望

# 著作権表示

この文章はクリエイティブ・コモンズ・ライセンスの下でライセンスされています。

```
<?xml version="1.0" encoding="euc-jp" ?>
<rdf:RDF
  xmlns="http://web.resource.org/cc/"
  xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
  xmlns:dc="http://purl.org/dc/elements/1.1/">

<Work rdf:about="http://fuktommy.s64.xrea.com/p2p/shingetsu.ps.gz">
  <dc:title>P2P 掲示板「新月」のプロトコルとデータ構造</dc:title>
  <dc:creator><Agent><dc:title>Fuktommy</dc:title></Agent></dc:creator>
  <dc:date>2004-09-04</dc:date>
  <dc:rights><Agent><dc:title>Fuktommy</dc:title></Agent></dc:rights>
  <license rdf:resource="http://creativecommons.org/licenses/by/2.0/jp/" />
</Work>

<Work rdf:about="http://fuktommy.s64.xrea.com/p2p/shingetsu.pdf">
  <dc:title>P2P 掲示板「新月」のプロトコルとデータ構造</dc:title>
  <dc:creator><Agent><dc:title>Fuktommy</dc:title></Agent></dc:creator>
  <dc:date>2004-09-04</dc:date>
  <dc:rights><Agent><dc:title>Fuktommy</dc:title></Agent></dc:rights>
  <license rdf:resource="http://creativecommons.org/licenses/by/2.0/jp/" />
</Work>

<License rdf:about="http://creativecommons.org/licenses/by/2.0/jp/">
  <permits rdf:resource="http://web.resource.org/cc/Reproduction" />
  <permits rdf:resource="http://web.resource.org/cc/Distribution" />
  <requires rdf:resource="http://web.resource.org/cc/Notice" />
  <requires rdf:resource="http://web.resource.org/cc/Attribution" />
  <permits rdf:resource="http://web.resource.org/cc/DerivativeWorks" />
</License>
</rdf:RDF>
```