

## P2Pを活用したSNSの提案

西谷 智広

(Tomo's Hotline&Tomo's Homepage)

2005年5月14日

### はじめに

---

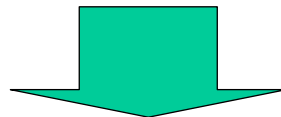
#### □現在のSNSの状況

☆ユーザ数急増

⇒[1]レスポンスタイム等の低下

⇒[2]サーバ、回線の増強

⇒[3]SNS運用企業の設備投資増加



SNSを利用する際ユーザのPCリソースを活用する事で  
SNS運用企業の負担を軽減することはできないか？

それってP2P？

## P2PでSNSはできる？

□P2Pアプリの「Ringooh」「新月」で次のようなことが既に可能。

☆掲示板

☆Blog

☆wiki

☆ファイルアップロード

※Pure-P2P(後述)で動いている

□SNSでは上記の他に

☆公開の制限(友達、友達の友達まで)

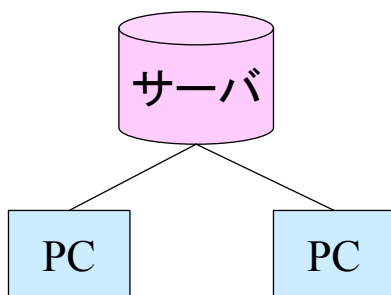
☆招待した人でないと加入できない

という機能が必要かも。

本プレゼンの焦点！

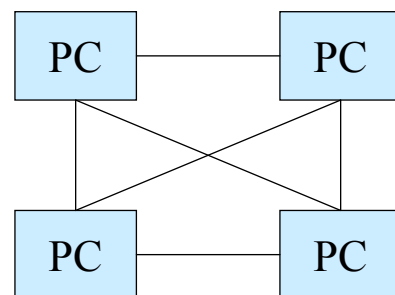
## P2Pの仕組み

Hybrid-P2P



- ・数多くのノードが参加可能
- ・全てのデータの検索可能
- ・初期コストが高い

Pure-P2P

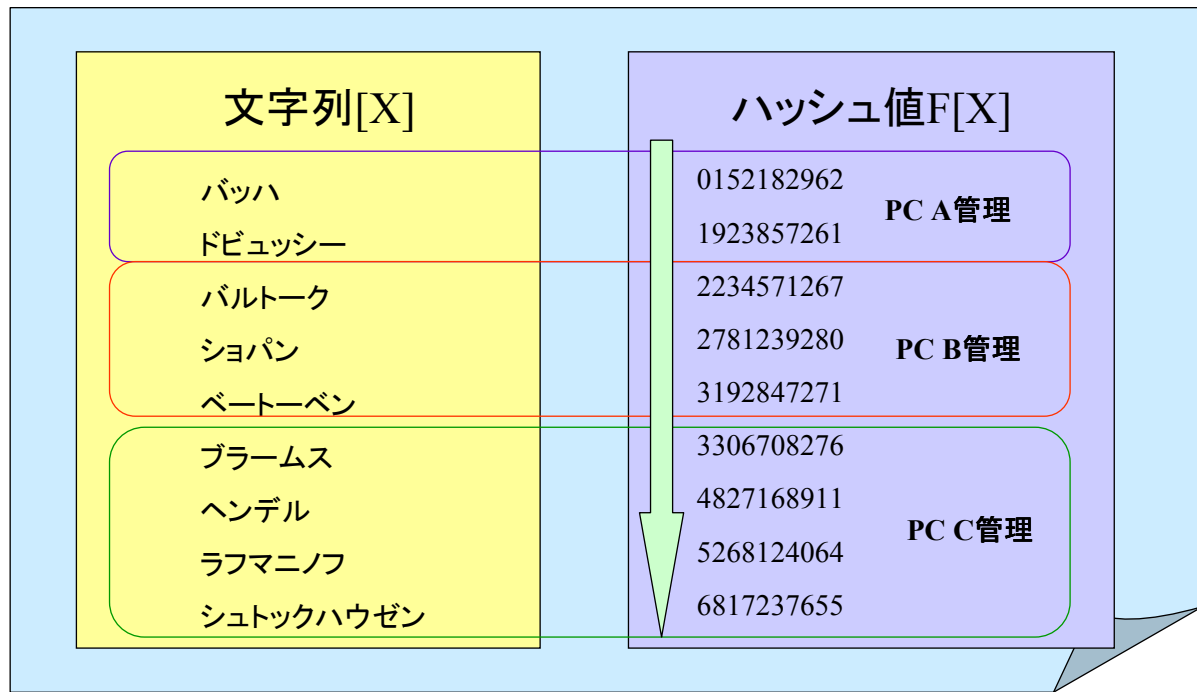


- ・数万程度のノードが参加
- ・検索可能データは一部
- ・初期コストは安い

DHTで解決！

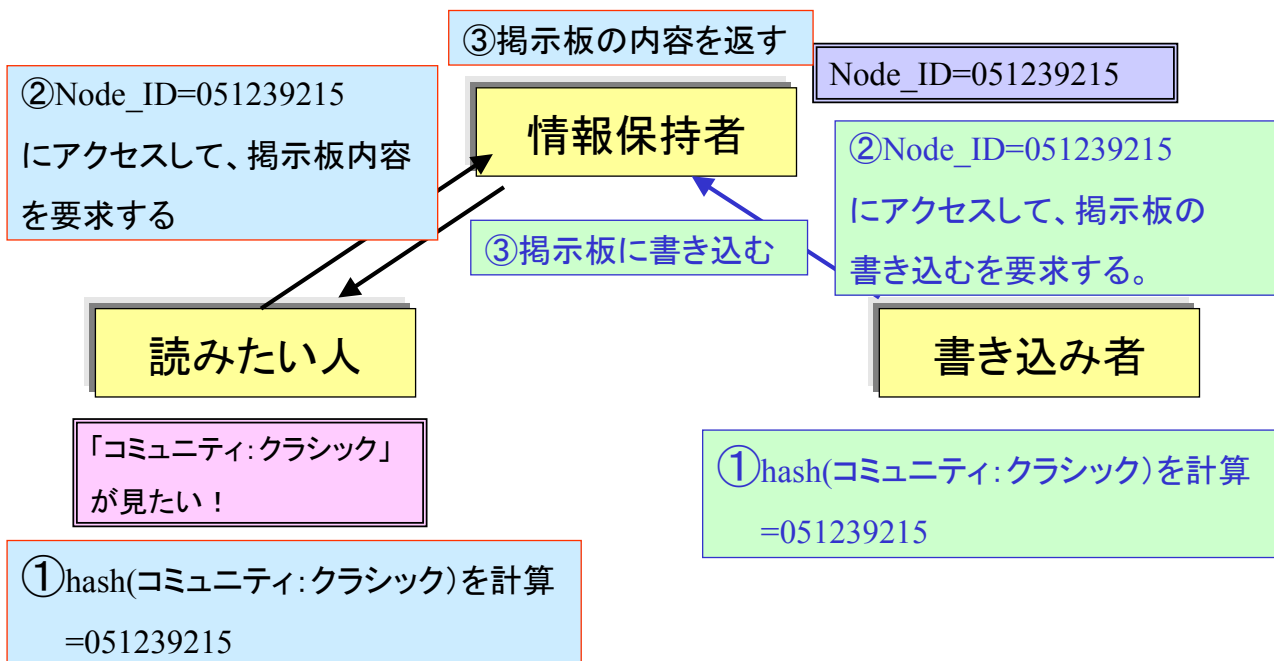
今回は初期・運用コストが少ないPure-P2Pシステムを利用する。

## DHT(分散ハッシュテーブルとは?)



データのハッシュ値でデータ管理するノードを決定する。  
(ノードが頻繁に参加、離脱しても対応可能。)

## DHTを使った例: 掲示板



□ Blog、Wikiも同様の手法で実現可能

## P2Pでの信頼性の保障

---

「ユーザの身分」を誰が保証するか？

□方法は大きく分けて2つ。

案1) 信頼できる人(SNS運用会社)などがその人の身分を保証

⇒PKI的なアプローチ

案2) 他人あるいは自分自身がその人の身分を保証

⇒PGP的なアプローチ

企業ベースで運用するには案1で望ましいと考えられる。

⇒非営利、個人ベースの運用であれば案2という解もある。

## SNSに加入する時のユーザ作業

---

□P2P-SNSアプリをPCにインストール

□SNS運用会社から電子証明書をもらう

⇒ユーザの「身分証明書」と同様。SNS運用会社からの「お墨付き」

⇒秘密鍵はユーザのPC内に閉じる。

□電子証明書をDHT(P2P)で公開。

※証明書内容の変更、SNSからの脱退等もSNS運用会社に通知。

# 友達を証明する仕組み「FOAF」

```
<rdf:RDF ....>
  <foaf:PersonalProfileDocument rdf:about="">.....
  </foaf:PersonalProfileDocument>
  <foaf:Person rdf:nodeID="me">
```

TomoがP2P Todayを友人と  
記述する場合

```
<foaf:name>Tomohiro Nishitani</foaf:name>
<foaf:givenname>Tomohiro</foaf:givenname>
<foaf:family_name>Nishitani</foaf:family_name>
<foaf:nick>Tomo</foaf:nick>
<foaf:mbox rdf:resource="mailto:aaa@bbb"/>
```

自分の情報  
=Tomo

```
<foaf:knows>
  <foaf:Person>
    <foaf:name>P2P Today</foaf:name>
    <foaf:mbox rdf:resource="mailto:ccc@ddd"/>
  </foaf:Person>
</foaf:knows>
```

友人の情報  
=P2P Today

```
</foaf:Person>
</rdf:RDF>
```

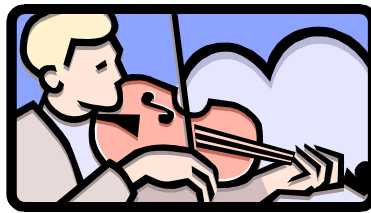
<http://www.ldodds.com/foaf/foaf-a-matic.ja.html>で生成（一部編集）

□電子署名をして、改ざんを防止する。

## 友達の友達（2次の繋がり）を証明しよう！ [概要]



Nao



Tomo



P2P Today

①NaoがP2P Todayを認証（チャレンジ・レスポンス方式）[P2P Todayの電子証明書を活用]

②NaoにTomoと友達である事を通知



③NaoのFOAFにTomoが含まれている事を確認



④TomoのFOAF、電子証明書をDHTから検索し、検証。FOAFにP2P Todayが含まれる事を確認。

⑤NaoはP2P Todayに自分の情報を公開

N次の繋がりまでの公開も理論的には可能

ご清聴ありがとうございました。

西谷 智広 tnishita@yahoo.co.jp

Mixi,Greeに「Tomo」で参加しています。

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

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

[お知らせ]今後のイベントの開催予定:

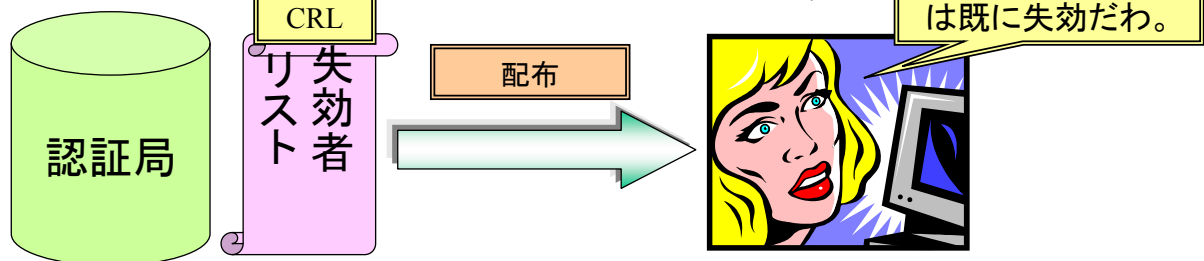
DHTオフ会 6月中旬～下旬頃

Skype勉強会 8月～9月頃

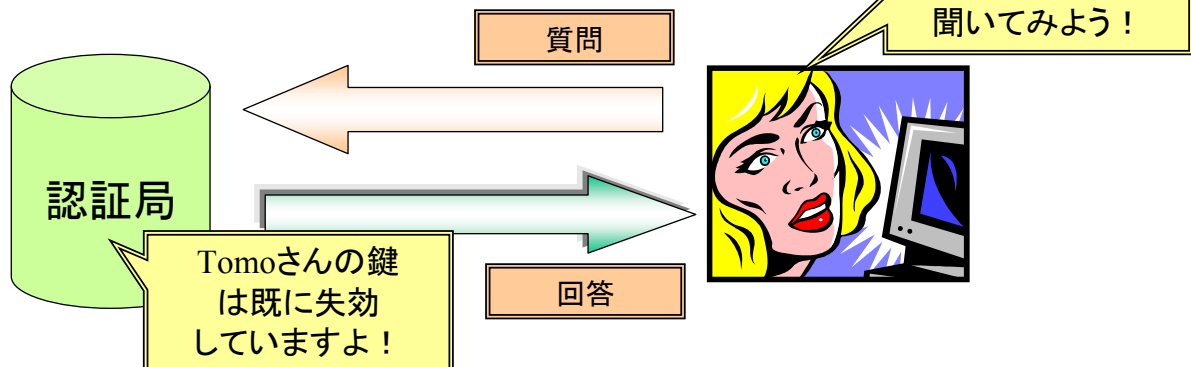
P2P勉強会 今年度中

## [補足]電子証明書の失効確認

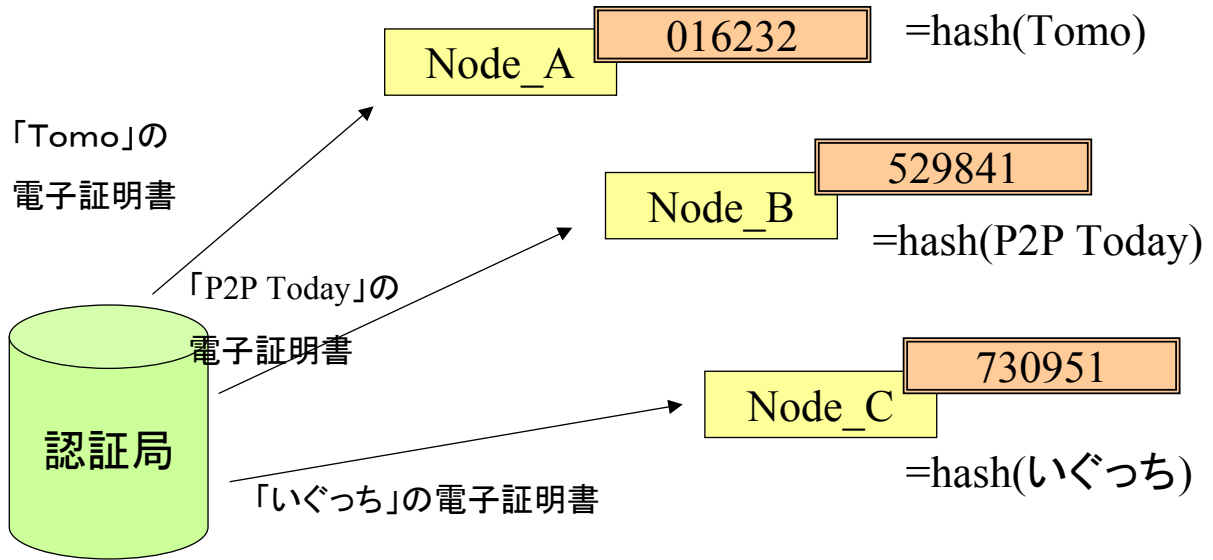
### ①CRL方式



### ②OCSP方式



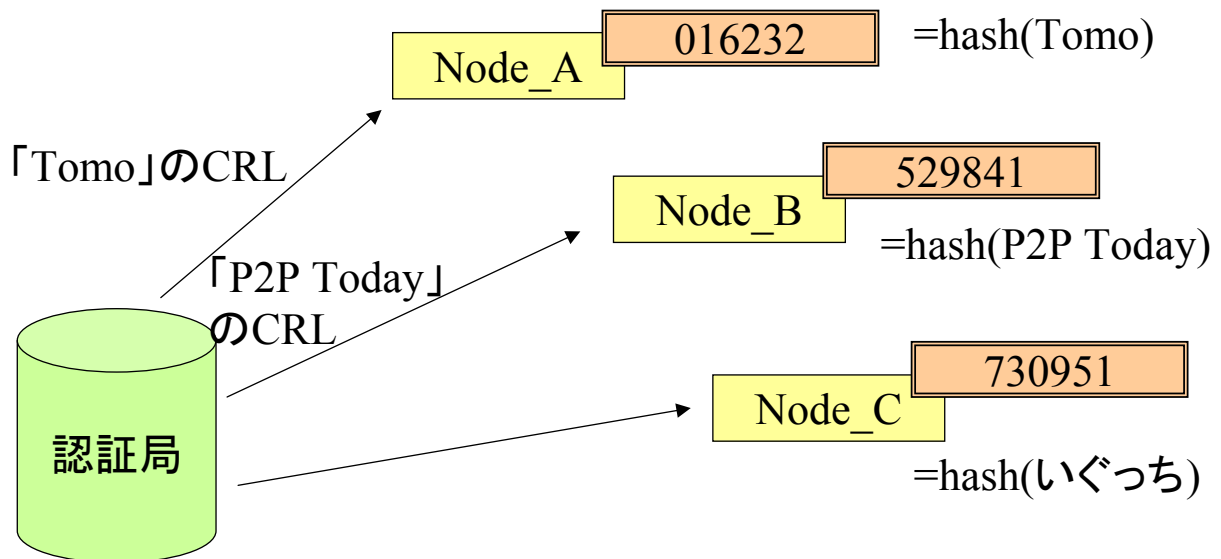
## [補足]DHTによる電子証明書の管理



※電子証明書は随時発行

各ノードが電子証明書の分散的なレポジトリとなる

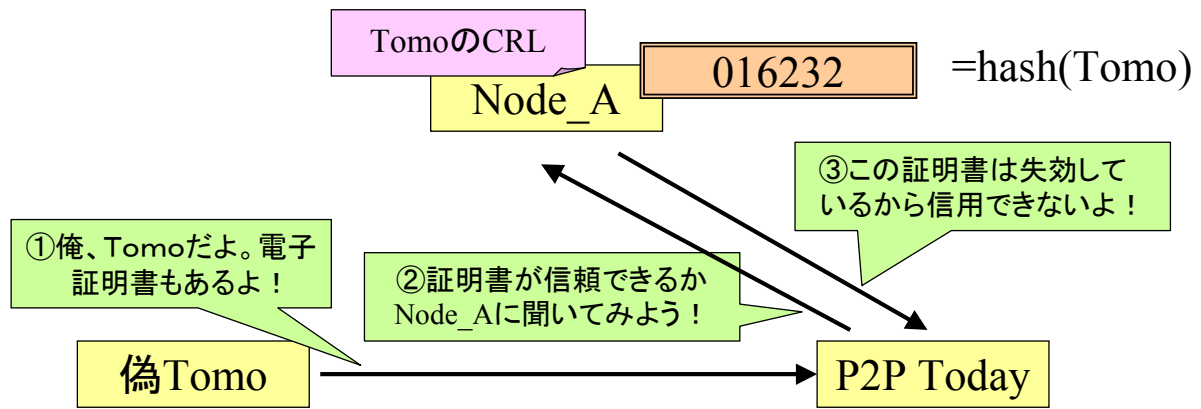
## [補足]DHTによるCRLの管理



※CRLは随時発行

各ノードがCRLの分散的なレポジトリとなる

## [補足]DHTにおける認証方法



### メリット

- ①認証のための負荷が分散される
- ②即時に電子証明書が失効かどうか判断できる