マルチメディア通信と分散処理 111－9
コンピュータセキュリティ 20－9
（２００３．２．２７）

ユビキタス環境を想定した超分散認証方式

水野 高宏† 布田 寿康† 林 慶士† 高橋 成文†

ユビキタス社会の到来に伴い，膨大な数の非 PC 機器のネットワーク接続やユーザを介さない機器同士の通信環境の増大が予想される．現在主流となっている認証方式の 1 つに，認証情報を認証サーバで管理するセンタ型認証方式があるが，上記環境に適用した場合，認証サーバへの要求の集中が問題となる．そこで本稿では，ユーザ管理下の機器に認証サーバ機能を分散的に委譲することで，認証サーバへの負荷集中を改善する超分散認証方式の提案を行う．さらに，提案方式が従来方式と比較して高スケーラビリティであることを数値計算により示すと共に，脅威分析により安全に機能するために必要なセキュリティ要件を提示する．

Hyper-decentralized Authentication Architecture for ubiquitous environment

Takahiro Mizuno, Toshimichi Fuda, Takashi Hayashi and Shigefumi Takahashi

With the coming of the Ubiquitous Society, a huge increase in number of non-PC appliances connecting with a network and intercommunication between these appliances without a user are to be expected. One of recent major authentication architecture is Centralized Authentication Architecture in which a server manages authentication data, and this may cause a problem of a load concentration on the server under the above environment. In this paper, we propose Hyper-decentralized Authentication Architecture which eases a load concentration on the server by transferring the server function to a number of appliances under user control. Moreover, we examine the scalability of the proposed architecture in comparison with the conventional architecture based on numerical calculation, and present security requirements for operating securely based on threat analysis.

1. はじめに

近年，コンピュータ／ネットワーク技術の高度化に伴い，いつでもどこでも簡単に安心して利用できるネットワークサービス（以後，ユビキタスサービスと呼ぶ）実現への期待が高まっている．また，情報家電や AV 機器など既に実用化されている機器をはじめ，各種センサや超小型チップ利用によりあらゆるモノがユビキタスサービスとしてネットワーク接続されようとしており[1,2]，「非 PC 機器のネットワーク化」が急速に進んでいる．

一方，EC(Electronic Commerce)の発達や Web サービス技術などによるサービス連携の高度化に伴い，ネットワークセキュリティの重要性が注目されており，認証サービスの必要性はますます高まっている．利用する認証技術は，サービスに要求されるセキュリティレベルやネットワーク環境によって異なるが，主な認証方式は次の 2 つに分けることができる．

(1) センタ型認証方式
(2) EndtoEnd 型認証方式

(1)はパスワード認証や IC カード認証において広く利用されている．認証サーバが一括してセキュリティ管理を行うため，運用面での利便性が高い．また，(2)は PKI(Public Key Infrastructure)技術を利用する方式が代表的であり，SSL／TLS による Web 環境での認証や，IPsec による VPN(Virtual Private Network)の構築などで利用されている．通信を行う機器同士で直接認証を行えるという利点がある．

ところで，「非 PC 機器のネットワーク化」では，従来とは比べものにならない膨大な数（数億から数百億レベル）の機器がネットワークに接続され，ユーザからの能動的なトリガ無しに通信要求が発生する M2M (Machine to Machine)の通信機会が増えていくと予想される[3]．センサや RF-ID タグで取得した情報を利

† 株式会社 NTT データ 技術開発本部
Research and Development Headquarters,
NTT DATA Corporation

用するサービスや情報家電同士の連携サービス[4]がその一例と言える．このようなユビキタスサービスに対して前述の 2 つの認証方式を導入した場合，以下の問題が予想される．

(A) センタ型認証方式では，認証サーバへの負荷集中が発生する．

(B) EndtoEnd 認証方式では，PKI 認証において巨大な CRL(Certificate Revocation List)を膨大な数の機器に配布する仕組みが必要となる．証明書検証機能を VA(Validation Authority)に依頼する場合には，(A)と同様に VA への負荷集中が発生する．

ユビキタスサービスでは PKI 機能を持たない省リソース機器の利用が想定され，加えて膨大な数の機器全ての PKI 証明書を発行･配布することも困難であるため，本稿ではまず(1)の問題に焦点を絞り，負荷集中を改善する超分散認証方式を提案する．本方式は，ユーザ管理下の機器に P2P (Peer to Peer)ネットワークを構成し，認証サーバ機能を Peer に委譲することで，認証サーバへの負荷集中を改善する．

以降，2 章で関連技術とその問題点について述べ，3 章で提案方式の具体的なアーキテクチャとメリットについて説明する．また，4 章では数値計算によるスケーラビリティ評価，5 章では脅威分析によるセキュリティ評価について述べる．最後に 6 章で結論を述べる．

2. 関連技術

2.1 Liberty Alliance

2001 年 9 月に米 Sun Microsystems を中心に設立された Liberty Alliance Project により策定中の，インターネット上でのオープンな連携モデルによるユーザ認証サービスの技術標準である[5]．シングルサインオンや個人の属性情報交換に関する検討が行われている．分散型認証システムという点で提案方式に類似しているが，同一認証ドメイン内はセンタ型認証方式で構成されているため，スケーラビリティの問題は解決されていない．

2.2 Grid Computing

ネットワークで接続された多数のコンピュータの資源を活用し，大規模な処理能力を実現するためのアーキテクチャである．SETI@home（地球外生命体発見プロジェクト）をはじめ，物理計算や癌治療薬発見などの事例がある[6,7,8]．サーバ処理の分散という点で提案方式に類似している．しかし，現在の Grid Computing では，通信はサーバと PC の間に限られており，認証もセンタ型認証方式で行っているため，スケーラビリティの問題を解決する手段とはならない．

3. 超分散認証方式の提案

3.1 センタ型認証方式の問題点

センタ型認証方式では，認証サーバにクライアントの認証情報が事前登録され，集中管理される．認証時には，クライアントは自身を証明するデータを認証サーバへ送信し，認証サーバは事前登録済みの認証情報と受信データによりクライアントの正当性を確認する．

Liberty Alliance では，IDP(IDentity Provider)が認証サーバとなり，クライアントである SP(Service Provider)及びユーザに対して相互認証サービスを提供する．IDP には SP 及びユーザの認証情報が事前登録されており，その情報を元に認証が行われる．

図 1 は，自宅の情報家電を外出先からインターネット経由で操作する場合の認証構成例である．センタ型認証方式で実現した場合を図 1-(1)に示す．インターネットを利用して操作する機器（PDA やホットスポット設置の PC）と操作される情報家電（TV や VTR）は，相互認証を行うことで通信が可能となる．図 1-(1)の場合，登録されている全ての機器の認証情報の管理及び認証処理を認証サーバが行う必要があり，機器数の増加に合わせて認証サーバを高性能化する必要がある．しかし，機器数が膨大な数（数億から数百億レベル）に達した場合，ハードウェア技術により対応することは困難であり，何らかの新たな解決手段が必要となる．

3.2 超分散認証方式

超分散認証方式では，認証システムに P2P ネットワークアーキテクチャを採用し，認証を Peer 間で実行することで認証サーバへの負荷集中の問題を解決する．

P2P ネットワークとは，平等な機能を持った構成要素（Peer）同士がブローカレスで直接通信する形態のネットワークで[9,10,11]，Peer が動的にネットワークを構成できるという特徴を持つ．超分散認証方式での認証構成を図 1-(2)に示す．図のように，認証サーバが持つ認証機能をユーザ管理下の Peer（以後，認証 Peer と呼ぶ）に分散的に委譲し，認証 Peer 同士を P2P ネットワークで接続する．この P2P コミュニティを認証サービスコミュニティ（認証 SC）と呼び，認証 SC にセンタ型認証方式における認証サーバと同等の役割を持たせる．また，認証 SC の管理を行うためのセンタとして，サービス提供者は CP (Central Point)を設置･運用する．

各構成要素の役割を以下に整理する．

- **認証 Peer**：自分の配下のクライアント認証情報の管理及び認証処理を行う．クライアントからの要求を受けて，他認証 Peer との相互認証，暗号通信路の提供を行う．
- **CP**：認証 Peer の位置情報，クライアントの接続情報を管理する．IP アドレスや DNS 名などのクライアント ID をキーとした認証 Peer の検索サービスを提供する．
- **クライアント**：認証サービスを利用する機器(人)で，他クライアントのへ認証／通信要求を認証 Peer に送出する．

各認証 Peer は自分がセキュリティを担保すべき領

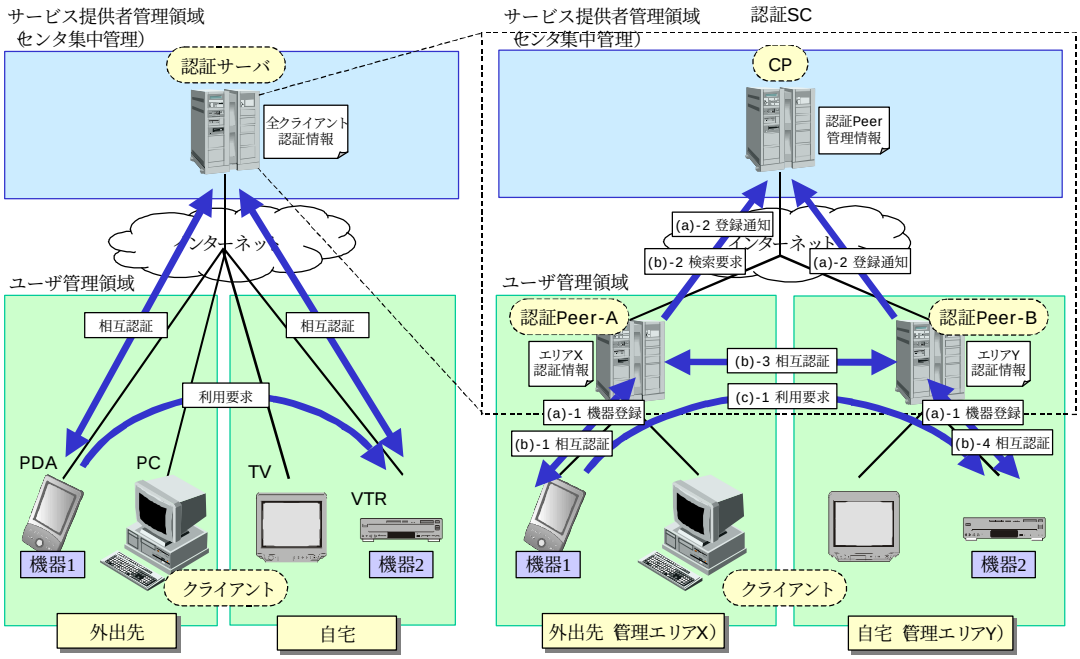

図 1　センタ型認証方式と超分散認証方式の比較

域（以後，管理エリアと呼ぶ）を持つ．各クライアントは少なくとも 1 つの管理エリアに所属し，管理エリアの認証 Peer と相互認証を行う．管理エリアの異なるクライアント同士が認証を行う場合には，各クライアントを管理する認証 Peer 同士が相互認証を行う．

以下に，認証 Peer-A 配下の機器 1 から認証 Peer-B 配下の機器 2 を操作する場合の処理フローを示す．

(a) 初期登録処理

1. 機器 1 を認証 Peer-A に，機器 2 を認証 Peer- B に登録し，認証情報の設定を行う．
2. 認証 Peer-A 配下に機器 1 が，認証 Peer-B 配下に機器 2 が存在することが CP に通知される．

(b) 認証処理

1. 認証 Peer-A は機器 1 からの機器 2 への認証要求を受信すると，まず機器 1 と相互認証を行う．
2. 正しく認証できた場合，認証 Peer-A は機器 2 を管理している認証 Peer を CP に問い合わせる．
3. CP からの問い合わせ結果（認証 Peer-B の所在）を受け，認証 Peer-A は認証 Peer-B と相互認証を行う．
4. 認証 Peer-B は機器 2 と相互認証を行う．正しく認証された場合，認証 Peer-A とセション鍵の共有を行う．

(c) 通信処理

1. 機器 1 は，操作コマンドを記述した電文を認証 Peer-A，認証 Peer-B 経由で機器 2 に送信する．認証 Peer 間の電文は(b)-4 で共有したセション鍵で暗号化される．

超分散認証方式では具体的な認証アルゴリズムは規定しない．従って，従来どおりサービス毎に利用環境に応じた適切な認証アルゴリズムを選択する必要がある．なお，認証 Peer 間の相互認証，クライアント認証は別々の認証アルゴリズムでもよい．例えば，認証 Peer 間認証は SSL を利用し，クライアント認証を MAC アドレス確認により行ってもよい．

また，認証 SC は認証サーバの代替の位置付けであり，認証ドメイン毎に形成される．従って，異なる認証ドメインや認証システムと相互接続する場合には，新たにブリッジを設置する必要がある．

超分散認証方式をセンタ型認証方式と比較した場合の利点を以下にまとめる．

- 認証サーバを認証 Peer として分散配置しているため，特定のサーバへの負荷集中を改善できる．さらに，グリッドコンピューティングと同様，Peer の設置／運用をユーザが行うため，センタ型認証方式と比較して設備投資費や運用コストを低減できる可能性がある．
- インターネット接続される区間については認証 SC がセキュリティを担保するため，クライアントは自らを登録した認証 Peer との接続環境に応じたセキュリティ機能のみを持てばよい．従って，ユビキタスサービスで想定されるセンサなどの省リソース機器での利用も可能である．
- クライアント認証情報がインターネット上を流れず，認証サービス提供者にも知られないことから，認証情報漏洩の危険性が低い．

4. 数値計算によるスケーラビリティ評価

4.1 提案方式のモデル化

超分散認証方式のスケーラビリティを数値計算により検証する．検証の方針として，提案方式をモデル化し，概算値を元にしてセンタ型認証方式との比較を行う．以下に，モデル化におけるアプローチを示す．

(1) サーバへの負荷集中

Webサーバは FIFO 待ち行列及びプロセッサシェアリングによりモデル化が可能である[12]．本検討では，概算値による比較評価が目的なので，ランダム到着／処理時間一定である M／D／1 型待ち行列モデルを用いて簡略的にモデル化を行った．M／D／1 モデルでは，待ち時間 Wq は式(1)で表わされる．ここで，μは平均到着率(単位時間に要求が到着する確率)，λは平均サービス率(単位時間に処理が終了する確率)を示す．

$$Wq = \frac{r}{1-r}\frac{1}{2m} \quad (\rho = \lambda/\mu \text{とする}) \quad (1)$$

(2) 認証処理

認証 Peer 間認証･クライアント認証共に PKI で行うものとし，証明書失効のチェックは各機器が CRL を用いて行うこととした．また，相互認証処理は証明書検証と暗号演算処理から構成され，証明書検証処理では公開鍵演算を，暗号演算処理では公開鍵演算と秘密鍵演算を 1 回ずつ行うことを仮定した．

(3) 検索処理

CP における認証 Peer 検索処理，証明書検証での CRL チェック処理では，検索に二分探索法を使用することを仮定した．

4.2 前提条件の設定

4.1 節で定義したモデルを数値計算により検証するときの前提条件を以下に示す．

(1) 認証処理内訳

(a) センタ型認証方式
- クライアントとサーバ間の相互認証

(b) 超分散認証方式
- 通信元クライアントと認証 Peer 間の相互認証
- CP での認証 Peer 検索
- 認証 Peer 間の相互認証
- 通信先クライアントと認証 Peer 間の相互認証

(2) 評価対象外とする項目
- 通信時間及びネットワークの輻輳
- OS やソフトウェア実行時のオーバヘッド
- CPU リソースの制限

(3) 処理時間

処理構成の前提条件を元に，実計測時間を基本とした処理時間の設定を行った．
- 証明書検証処理時間：0.5 (msec／件)
- 相互認証処理時間：10 (msec／件)
- 検索に伴う比較処理時間：0.05 (msec／回)

上記処理時間は，Pentium Ⅲ 700MHz (RAM: 512MB)の機器で計測された値の概算である．評価ではこの性能を 1 として機器性能を表現する．

4.3 評価結果

(1) 要求数増加に対する応答時間の変動

クライアント数の増加に伴う要求数の増加に対する応答時間の変化を検証した．

パラメータ設定及び結果を図 2 に示す．限界要求数がセンタ型認証方式で約 4300 万件／日，超分散認証方式で約 6.6 億件／日となり，超分散認証方式の方がセンタ型認証方式よりも約 15 倍限界要求数が大きいことがわかる．ここで，一般には上限の無い待ち行列では呼損が発生しないため，ρが 1 に近づくと待ち時間が∞に発散するが，本評価ではρ=1 のときの要求数を特に「限界要求数」と呼ぶこととした．

なお，限界要求数以下の区間では，認証 Peer のオーバヘッドにより，超分散認証方式の方が数十ミリ秒程度応答速度が遅くなるが，実運用時に問題となる差ではないと判断した．

(2) 認証 Peer の要求性能

超分散認証方式における処理限界の要因分析によってボトルネックとなる処理の特定を行い，認証 Peer の要求性能について検討した．

認証 Peer と CP について，個別の限界要求数を図 3 に示す．認証処理時間に影響を与える認証 Peer 性能に対する限界要求数を計算した．なお，クライアント数は 1000 万，認証 Peer 数は 10 万で固定とした．図 3 より，認証 Peer 性能がある一定値よりも低い場合には認証 Peer 上での認証処理が，高い場合には CP での検索処理がボトルネックとなり，限界要求数が決まることがわかる．この例では，CP 性能が 10 の場合，最も効率的な認証 Peer 性能は約 0.0017 となる．これは性能が 1 の PC の数百分の一の性能しか持たない機器が認証 Peer として効率良く稼動することを示しており，例えば，ADSL ルータやホームゲートウェイなどの処理性能の低い機器に認証 Peer を組み込めることを示唆している．

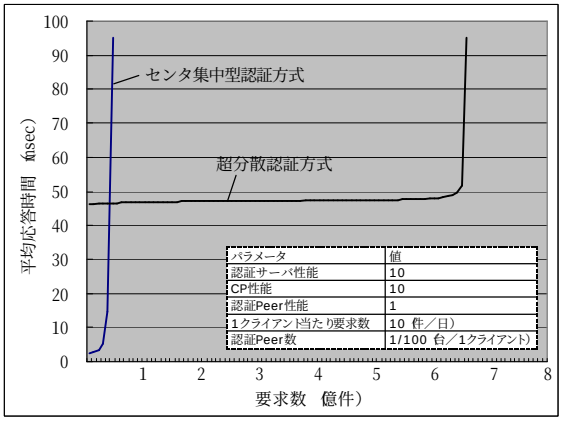

図 2 要求数と応答時間の関係

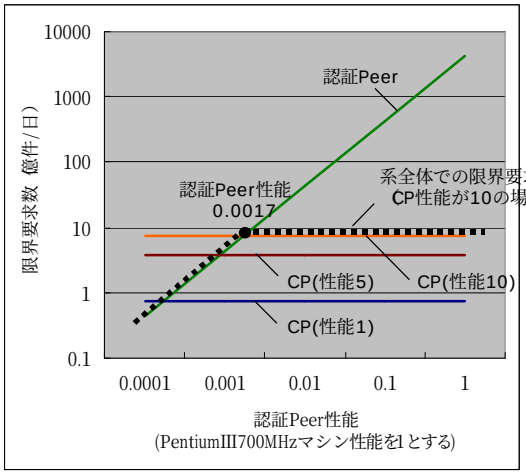

図 3　認証 Peer 性能と限界要求数の関係

表 1　各種ネットワークサービスと限界要求数

		ホーム ネットワーク	オフィス ネットワーク	センサ ネットワーク
パラメータ	認証サーバ性能	10	10	10
	CP性能	10	10	10
	認証Peer性能	0.1	0.5	1
	認証Peer数（台/1クライアント）	1/10	1/100	1/10000
	1クライアント当たり要求数（件/日）	1	10	100
限界要求数	センタ型認証方式（億件/日）	0.43	0.43	0.43
	超分散認証方式（億件/日）	5.9	6.6	7.6

(3) 各種ネットワークサービスへの適用

各種ネットワークサービスへの適用を想定した場合の評価例を示す．ホームネットワーク／オフィスネットワーク／センサネットワークの 3 つの利用シーンを想定し，各ネットワークサービスで考えられる一数値例を設定した．

表 1 に，パラメータ設定及び評価結果を示す．表 1 の例では，いずれの利用シーンにおいても，センタ型認証方式と比較して 13～17 倍の限界要求数となっており，提案方式の方が種々のネットワークサービスで高いスケーラビリティを持つことがわかる．

5. 脅威分析によるセキュリティ評価

5.1 評価方針

超分散認証方式では認証サーバ機能をユーザ機器に委譲することから，実用にあたりセンタ型認証方式とは異なるセキュリティ要件が必要になることが予想される．そこで，脅威分析によるセキュリティ評価を行い，必要となるセキュリティ要件を設定する．一般的に，脅威分析で抽出された全ての脅威に対して対抗手段を持つことがセキュリティ要件となるが，センタ型認証方式と同等のセキュリティレベルを確保すればよいとの考え方から，センタ型認証方式における脅威との差分に注目して要件を抽出した．以下に評価手順を示す．

(1) 前提条件／環境設定の設定を行う．
(2) センタ型認証方式の脅威分析を行う．
(3) センタ型認証方式と超分散認証方式の分析結果を比較し，同等な脅威のマッピングを行う．
(4) マッピングされなかった差分項目を新たな脅威として設定し，その対策を超分散認証方式のセキュリティ要件とする．

5.2 評価結果概要

(1) 前提条件の設定

脅威分析の前提条件／環境設定を以下に示す．

- **業務範囲**：認証サーバ･CP･認証 Peer･クライアントの設置／初期化／運用
- **攻撃者**：認証サーバ･CP 管理者，ユーザ，第三者
- **守るべき資産**:認証 Peer･クライアントの管理情報，プログラムコード，認証情報（秘密鍵などの秘匿性の高いデータ及びそこから算出されたデータ）
- **脅威**：資産の不正照会／改竄／消失，事実否認
- **範囲外事象**：CA (Certificate Authority)のセキュリティ破綻，アプリケーションレイヤの脅威
- **利用環境**：社会的責任を持たないユーザ自身が認証 Peer を管理する環境，クライアントに不特定多数が物理的にアクセス可能な環境

(2) センタ型認証方式の分析

攻撃者，資産，脅威について全組み合わせ(274 通り)を想定し，そこから脅威となる組み合わせ(109 通り)を抽出した．次に，それらの脅威を実行する具体的方法を設定し，それに対して現システムで実施されている対抗手段の洗い出しを行った．

(3) 脅威項目のマッピング

超分散認証方式についても，全組み合わせ(652 通り)の中から脅威となる組み合わせ(219 通り)を抽出した．その 219 の組み合わせに対してセンタ型認証方式の分析結果をマッピングしたところ，217 の脅威はマッピングされ，2 項目のみがマッピングされなかった．

(4) 脅威の設定

マッピングされなかった以下の 2 項目を新たな脅威として設定する．

(a) ユーザが認証 Peer 内のクライアント管理情報を改竄して不正なクライアントを接続する脅威
(b) ユーザが初期設定時に認証 Peer へ不正なクライアントを登録する脅威

5.3 セキュリティ要件

超分散認証方式では，上記 2 つの脅威に対する対策案を，センタ型認証方式でのセキュリティ要件に追加すべき要件として提示する．

(1) 認証 Peer の耐タンパ性

ユーザによる認証 Peer 内の情報の改竄を防ぐためには，ユーザ管理下にあってもユーザが自由にデータを操作できない環境が必要になる．

実現方法の 1 つとしては，セキュリティ機能を持った耐タンパ性の高い IC チップ（以後，セキュアチップと呼ぶ）を認証 Peer に搭載し，認証 Peer 内情報へのアクセスを制御する方法がある．セキュアチップに

はあらかじめ認証鍵を埋め込んでおき，認証された正当なプログラム又は管理者のみが情報へのアクセスを許可される．これは，ユーザが保有する IC カード内の電子マネー金額は，ユーザであっても自由に書き換えられないのと同様の仕組みである．PC にセキュアチップを組み込むという取り組みは，TCPA(Trusted Computing Platform Alliance)が検討を進めている[13]．TCPA では PC のセキュリティ機構に関する標準仕様の策定に取り組んでおり，ハードウェアレベルのセキュリティ機構を利用した PC の安全性確保の実現を目指している．この取り組みは提案方式の実現に重要な位置付けであると言え，今後の展開が注目される．

また，ハードウェアに依存しない手法としては，耐タンパソフトウェア技術の利用が考えられる．

(2) 第三者によるクライアント認証の必要性

認証 Peer への不正クライアントの登録を防ぐためには，ユーザ以外の第三者によってクライアントが認証される必要がある．実現方法としては，PKI 認証や CP との認証をクライアント登録時に実施する方法がある．また，クライアント認証は環境によっていくつかのレベルが想定できるため，各サービスの特性に応じて適切な第三者認証の方式を選択する必要がある．

6. おわりに

6.1 結論

本稿では，認証サーバ機能を P2P コミュニティ上に分散し，各 Peer に認証処理を委譲することで負荷集中を改善する超分散認証方式の提案を行った．また，本方式の有効性を数値計算によって検証し，センタ型認証方式と比較して約 15 倍のスケーラビリティを持つことを示すと共に，要求性能の分析から，ADSL ルータやホームゲートウェイなどの処理性能の低い機器に認証 Peer を組み込むことが可能であることを示した．さらに，安全に機能するために必要なセキュリティ要件として，認証 Peer の耐タンパ性，クライアントの第三者認証の必要性を提示した．これにより，センタ型認証方式と同等のセキュリティレベルを保持したまま，膨大な数のクライアントに対応できる認証システムの構築が可能になることを示した．

6.2 今後の課題

(1) プロトタイプによるスケーラビリティの検証

スケーラビリティの評価では，モデル化による数値計算を用いて提案方式の有効性を検証した．しかし，実システムでは，評価で考慮していない様々な要因がスケーラビリティに影響することが予想される．従って，本検証結果の信頼性をプロトタイプにより検証する必要がある．

(2) CP への負荷集中の改善

本方式においても，クライアント数が極度に増加した場合に CP への負荷集中が発生する．これの解決策の一つとして，CP を持たない pure 型 P2P ネットワークで認証 SC を構成する方法がある．現在，pure 型における Peer の効率的な検索手法に関する研究が進められており[14,15]，これらの成果を適用することで実現できる可能性がある．

(3) EndtoEnd 認証方式の問題の解決

本方式は認証サーバへの負荷集中の改善を検討しており，EndtoEnd 認証方式の問題については考慮していない．現状の SSL／TLS の運用では証明書の厳密なチェックは行われていないが，インターネットに接続された多数の機器が M2M 通信を行うユビキタスサービスでは，証明書の正当性確認が重要となる．本検討では，ユーザ管理下の耐タンパ機器にセンタ機能を分散することで負荷集中の改善を実現したが，この構成は認証以外のサービスにも展開することが可能なことから，例えば CRL の分散配置や VA への負荷集中の改善への適用を検討する予定である．

参 考 文 献

[1] Auto-ID Center : http://www.autoidcenter.org/

[2] 高橋 史忠, 蓬田 宏樹, “センサがネットにつながれば”, 日経エレクトロニクス, 2002.7.15, pp.99-129, 2002.

[3] 総務省「ユビキタスネットワーク技術の将来展望に関する調査研究会」報告書 : http://www.soumu.go.jp/s-news/2002/020611_4.html

[4] JEITA HOUSE: http://www.eclipse-jp.com/jeita/index2.html

[5] Liberty Alliance Project : http://www.projectliberty.org/

[6] SETI@home : http://setiathome.ssl.berkeley.edu/

[7] United Devices : http://www.ud.com/home.htm

[8] (株)NTT データ Cell Computing Project : http://www2.cellcomputing.jp/

[9] 小柳 恵一, 星合 隆成, 梅田 英和, “P2P ネットワーキング技術の提案と紹介”, 信学論(B) vol.J85-B, no.3, pp.319-332, March 2002.

[10] P2P Conference in Japan 2002 Spring http://www.p2pconf.com/

[11] Jnutella : http://www.jnutella.org/

[12] 藤田 靖征, 村田 正幸, 宮原 秀夫, “Web サーバシステムのモデル化と性能評価”, 信学論(B) vol.J82-B, no.3, pp.347-357, March 1999.

[13] TCPA (Trusted Computing Platform Alliance) : http://www.trustedcomputing.org/

[14] Ion Stoica, Robert Morris, David Karger, Frans Kaashoek, Hari Balakrishnan, “Chord: A Scalable Peer-To-Peer Lookup Service for Internet Applications”, In Proceedings of ACM SIGCOMM, pp.149-160, August 2001.

[15] Sylvia Ratnasamy, Paul Francis, Mark Handley, Richard Karp, Scott Shenker, “A scalable content addressable network”, In Proceedings of ACM SIGCOMM, pp.161-172, August 2001.