社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2006－DPS－128 (7)
2006－GN－ 61 (7)
2006－EIP－ 33 (7)
2006／9／14

ID爆発における周辺技術調査及びID管理方法に関する一考察

櫛田達也、斉藤典明、山崎哲朗、小林透、金井敦

ＮＴＴ 情報流通プラットフォーム研究所
〒239-0847 神奈川県横須賀市光の丘1-1

ブロードバンド環境の普及に伴い、様々なサービスがオンライン化されネットワーク上で利用可能となってきている。これらのネットワークサービスでは多くのＩＤが利用されているが、サービスの増加に伴いユーザが管理するＩＤも増加しユーザを圧迫しつつある。そこで、我々はこのような利用者自身がＩＤの増加に追随できなくなる状態をＩＤ爆発として問題提起を行っている。本論文では、このＩＤ爆発を解決するために必要となる関連技術の動向を調査した結果を報告し、ＩＤ爆発を解決するための技術要件の見通しについて述べる。

A Study of Technology to Solve The ID Explosion

KUSHIDA Tatsuya, SAITO Noriaki, YAMAZAKI Tetsuro,
KOBAYASHI Toru, KANAI Atsushi
NTT Information-Sharing Labs.
1-1 Hikarinooka Yokosuka-shi, KANAGAWA 239-0847 JAPAN

Various social services are made online as a broadband network environment spreads and our daily life are supported by the network services and became convenient.These services are provided by IDs and users have to manage a lot of IDs to use these services, then it will be felt that users are inconvenient for management of the ID in contradiction to using convenient network services. In this paper, we call this problems The ID Explosion, and the related technologies which are necessary to solve the ID Explosion are investigated and are reported. Moreover, the prospect of a technological requirement to solve the ID Explosion is described.

1 はじめに

ＮＧＮなどブロードバンド環境の普及に伴い、様々な社会サービスがネットワーク上で利用可能になる時代が近づきつつある。このような社会では、利用者を識別し様々なサービスを提供するための様々なＩＤが必要になる。しかしながら提供されるサービスが増加するにともないＩＤが氾濫しユーザを圧迫する状態になることが想定される。

我々は、このようなＩＤの氾濫でユーザを圧迫する状態をＩＤ爆発として提唱している[1]。そこで、本論文では、先の論文で提唱したＩＤ爆発に対する４つのカテゴリについて、解決するための関連の技術動向について調査した結果を報告し、ＩＤ爆発を解決するための技術要件の見通しについて述べる。

2 背景

最近のネットワーク社会では、フィッシングやスパイウェアなどのマルウェアによるオンラインバンキングＩＤの盗難や、クレジット番号の不正使用、迷惑メール問題など、ＩＤにまつわる不安や脅威が広がりつつある。様々な社会サービスがネットワーク上で利用可能にするための試みが推進されている状況において、このような脅威を野放しにしておくことはできない。このようなネットワーク上の社会サービスにおいては、本人識別や権利や状態の保管はＩＤを用いておこなわれており、ＩＤの安全な管理が重要になるが、ＩＤの増加に伴いこの管理に対する負担と脅威は拡大の一途を辿っている。

我々はこのようなＩＤの増加に伴い人間の対応が追随できなくなってしまった状態を”ＩＤ爆発”として定義し、ＩＤ爆発における問題点をＩＤの４つの分類モデルによってあらわした（表1）。

ここで、カテゴリ１は、識別子としてのＩＤであり、例えば、大量のモノや人などにＩＤの付与が必要となるための番号不足や、想定外の利用による想定外の特性を持ったＩＤが出現する問題がある。このカテゴリの問題を解決するために必要な技術分野としては、ＩＤ割り当て方法、ＩＤ生成方法、ＩＤ消去方法、ＩＤ探索方法、ＩＤ記述

方法、ＩＤ変換方法などが挙げられる。具体的な既存技術の例としては、ＩＤの割り当て方法については、統一的な標準化ルールにより生成されたＩＰアドレスを適切な機器に割り当てる仕組みとしてのＤＨＣＰの技術がある。ＩＤ生成方法については、ＩＤを生成するための標準化ルールや仕組みづくりの技術がある。ＩＤ消去方法については、例えばＰＫＩ基盤における証明書の失効管理技術がある。ＩＤ探索方法については、名前解決の仕組みとしてのＤＮＳがある。ＩＤ記述方法としては、グローバルな組織により付与体系が統一された、バーコード、ＱＲコード、ＵＲＬ、ＲＦＩＤなどがある。ＩＤ変換方法としては、プライベートアドレスとグローバルアドレスを変換するＮＡＴやＩＰマスカレードといった機能がある。

表１．ＩＤの分類モデルと対策技術

	分類	必要となる技術
カテゴリ1	識別子としてのID。	ID割り当て方法 ID生成方法 ID消去方法 ID探索方法 ID記述方法 ID変換方法
カテゴリ2	IDに対する存在、能力、権利を示すID	IDの権利付与方法 IDの保存方法 IDの取り出し方法 IDの変更方法
カテゴリ3	権利の行使、認証するためのID。	記憶に基づく認証方法 所有に基づく認証方法 バイオメトリクスに基づく認証方法
カテゴリ4	IDの使用によって生じるID。	履歴IDの保存方法 履歴IDの取り出し方法 履歴IDの信頼性確保方法

カテゴリ２は、ＩＤに対する存在、能力、権利を示すものであり、識別子として付与されたＩＤに意味や利用目的などの属性情報を設定したＩＤである。例えば、覚え切れない、管理しきれないなどの問題がある。このカテゴリの問題を解決するために必要となる技術分野としては、ＩＤの権利付与方法、ＩＤの保存方法、ＩＤの取り出し方法、ＩＤの変更方法などが挙げられる。具体的な既存技術の例としては、ＩＤの権利付与方法については、ＩＣカードによる社員入館証への社員番号の記載（電子的な意味での）方法などがある。ＩＤの保存方法に関しては、個人が覚えきれないＩＤ／ＰＷ（ＰＷ＝ＰａｓｓＷｏｒｄ 以下ＰＷと略す）を管理する場合に、記憶を補助し安全に保存するための技術ある。ＷｅｂサービスのＩＤ管理に限れば、複数のＩＤを整理し暗号化しファイルとして保管するためのＩＤ管理ツールが製品化されている[2]。ＩＤの取り出し方法については、利用場面や、目的に応じて大量のＩＤの中から必要なＩＤを選択する技術である。ＩＤの更新方法については、ＩＤ／ＰＷをＩＤ発行主体と合意のもと数ヶ月に一度更新するものがある。

カテゴリ３は、権利の行使に用いるＩＤであり、例えば、ＩＤ／ＰＷによる不正アクセスという問題がある。このカテゴリの問題を解決するために必要な技術分野は、ＩＤを利用した本人確認のための技術であり、言い換えると本人認証技術である。本人認証技術は本人の記憶に基づくもの（ＩＤ／ＰＷ）、本人の所持に基づくもの（ＩＣカードなど）、本人のバイオメトリクス情報に基づくもの（静脈など）の３つに区分され、各区分によっても様々な方式がある[3]。

カテゴリ４は、ＩＤの使用によって生じるＩＤであり、例えば、履歴ＩＤに対する名寄せや、目的外利用の問題がある。このカテゴリの問題を解決するために必要な技術分野としては、履歴ＩＤの保存方法、履歴ＩＤの取り出し方法、履歴ＩＤの信頼性確保方法が挙げられる。具体的な既存技術の例としては、履歴ＩＤの保存方法としては、サーバでユーザの履歴を保存するログ保管の技術がある。履歴ＩＤの取り出し方法としては、データマイニングの技術などがある。履歴ＩＤの信頼性確保方法については、デジタル・フォレンジックの技術などがある。

３　ＩＤ管理の動向

ＩＤ爆発におけるＩＤ管理技術を検討するために、特に最近の注目すべき技術の動向とその課題について述べてゆく。

３－１．　カテゴリ１の領域における動向

この領域のＩＤはインフラ的な要素が強く、もし、全世界のすべてのものに対するＩＤの付与基準や付与体系が過不足なく統一的に付与されていれば問題にはならいといえる。

ネットワークで利用されるＩＤとしては、ＩＰアドレスあり、ＰＣやルータなどネットワークに接続される機器の識別番号として利用され、様々なサービスが提供されているが、急速なインターネットの普及により、ＩＰアドレスの枯渇が問題となった。

しかし、現在では、ＩＰｖ６の標準化が済みＩＰｖ４に比べアドレス空間が３２ｂｉｔから１２８ｂｉｔへ大きく広がったため、枯渇の問題は事実上解消されてきた。さらに、この事がトリガーとなりＮＧＮでは今後、電話機や家電製品など従来よりも多くのものにＩＰアドレスの付与が進むと考えられている。そして、この先にはあらゆるモノへＩＤを付与し、ネットワーク上で利用しようというユビキタスの動きがある（図１）。

そこで、ここでは人と人以外に分けて検討を述べる。

（１）人以外のモノへのＩＤ付与

モノへのＩＤ付与するための注目すべき技術としてＲＦＩＤ(Radio Frequency Identification)がある。これは、ＩＣタグ、電子タグとも呼ばれ

るもので、無線を利用してＩＣチップの中のデータを一度に大量に読み取れるＲＦＩＤタグを利用し貼付したモノを１つ１つ識別する事が可能となるもので、ネットワーク上でさらに多くのものを識別する事が可能になると予想される[4]。

代表的なＲＦＩＤに関する技術の標準化団体としては、ＥＰＣＧｌｏｂａｌ[5]やユビキタスＩＤセンター[6]があり、これらの団体では、グローバルでユニークなＩＤを発行／管理するとともに、読み取ったＩＤの名前解決手段や、ＩＤと関連する商品情報などを管理するＤＢなどを含めたネットワーク基盤技術の標準化を目指した取り組み、実験などが行われている。

ここでは対象は単なる固体にとどまらず、さらにより多くの性質のモノに付与が拡大しつつある。

例えば、ＲＦＩＤを用いてモノではなく場所を識別する技術も進展している。視覚障害者の持つ杖にＲＦＩＤのアンテナを内蔵し、点字ブロックへ埋め込まれたＲＦＩＤの情報を取得する事により経路案内や注意喚起などを提供できるシステムが提案されている[7]。

さらに、自然現象をセンシングして識別番号を埋め込み、利用する技術も研究されている。これは、温度、場所、時間などの情報に対してＩＤを付与する事により、自然現象をデジタルデータとして理解し、オンラインシステムで利用しようとするものである。

このように、単なるモノの識別にとどまらず、場所、時間、現象などさまざまなものを識別するためにＩＤが付与され始めている。

（２）人へのＩＤ付与

さらに、人にＩＤを付与する事で様々に利用する方法も検討が進んでいる。

アミューズメント内での迷子探索、医療施設内の患者の位置確認、登下校時の子供の安全管理、高齢者の位置確認などはいずれもＲＦＩＤを持つ人の位置を把握するために利用される例である。

また、人が所有する複数のモノに貼付されたＲＦＩＤタグをリーダに読み込ませる事で、遠隔からの家電制御をおこなう方法についての提案もされている。ここでは、ＲＦＩＤタグを所有する人がＩＤ読ませる順番や読まれた時間、などから異なる機器の制御が可能なっている[8]。

さらには、人間の皮膚に直接ＲＦＩＤを埋めこみ、入室認証や機器の制御を行う研究もなされている[9]。

人にＩＤを付与しネットワークでサービスを利用する場合には、不当にＩＤを読み取られる事による、プライバシー侵害が問題となる。これについては、様々な研究がなされる[10][11]一方で、総務省により“無線タグに関するプライバシー保護ガイドライン”[12]が公表されており、一定の基準があるといえる。しかし、これは対象範囲を“消費者に物品が手交された後も物品に電子タグを装着しておく場合”と限定されたものであり、場所、自然現象などへのＩＤ付与や、人へのＩＤ付与など新たな利用方法が検討されつつある中、新たな問題が発生する可能性が考えられる。

以上のように、ＩＤ付与に関しては、そのルール化や標準化活動により、まずは、あらゆるものにＩＤを付与するにはどうしたらよいかについて先行的に考えられてきたといえる。その結果、様々なモノを識別しネットワークで利用するための基盤技術が構築され、ＩＤをあらゆるものに付与する事が可能になりつつある。

今後は、ＩＤが付与される事により、どういった事が問題となるか、またその解決方法についての技術的、制度的議論が重要となると考えられる。

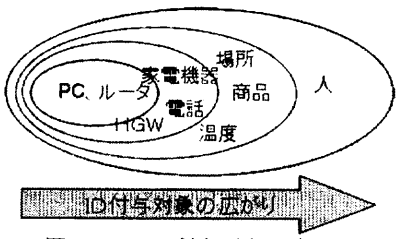

図１．ＩＤの付与対象の広がり

３－２．　カテゴリ２の領域おける動向

この領域のＩＤはＩＤに意味や利用目的などの属性情報を設定したＩＤであり、権限や権利の証明に利用されるＩＤである。例えば、Ｗｅｂサービスや企業内システムを利用する際のＩＤ、ＰＷからなるアカウントは、そのサービスの利用権利を表すＩＤといえる。

現在では、アクセス権に限らず、様々な権利がネットワーク上で利用可能となってきている。ここでは、権利を発行する観点と、個人が権利を保護する観点に分けて動向について述べる。

（１）　電子的な権利の発行

従来よりデジタルデータの真正性を保障するための技術として公開鍵暗号を利用したデジタル署名やＰＫＩ基盤などの研究が進んでいる。さらに、電子署名法（2001年施行）、e-文書法（2005年施行）など電子化文書に対する法整備が進み、ＧＰＫＩなどの政府による認証基盤の整備もすすんできている。

このような流れの中、従来紙で行われた各種の電子申請が可能になり、個人においても、住民票の取得や、パスポート申請などがオンラインで可能となっている。

さらにこれらに追随するように、様々な権利や、

存在を証明し活用するためのＩＤが電子化されネットワーク上で利用されはじめている。

例えば、従来紙で管理されていた株券に対して、2004年に“社債、株式等の振替に関する法律”が公布された。これにより、株券発行や券面保有のコストやリスクの削減を目的に、株券が電子化され2009年以降すべての紙による株券が廃止され電子的なデータによる管理に以降する予定となっている。

また、商業的な音楽や映像などのデジタルコンテンツの著作権の保護技術としてＤＲＭ技術がある。また、コンテンツに付与するＩＤについては、まだ、全世界的な統一は取れていないが、日本ではコンテンツＩＤフォーラム[13][14]が標準化に向けた活動を行っている。デジタルコンテンツの著作権を侵害する、Ｐ２Ｐによるファイルの交換は依然として大量に行われている現状をかんがみるとこれらの技術の効果はまだ限定的ともいえるが、ステークホルダの圧力もあり、盛んに研究がなされており、今後の発展、普及が十分に期待できる。

（２） 個人が権利を保護

電子的な権利を発行するための技術的、制度的基盤の整備が進むことで、ネットワーク上で扱える権利や存在を証明するためのＩＤは増加している。それに伴い個人のＩＤ管理の負荷は増大すると考えられるが、統一的な基準も技術もなく、個人のＩＤ管理はユーザの管理任せになっているのが現状であろう。

ＰＫＩ基盤を利用し証明書により本人確認が厳重になったとしても、ユーザ個人の管理がずさんで盗難された場合には、正当な証明書でアクセスされるため不正の判断が困難となる。また、ＩＤ／ＰＷの不正アクセスでは、ユーザを狙ったものがほとんどであるといったデータもあり。すでに一部では、権利に関するユーザにおけるＩＤ管理が破綻しているとも言える。

またブログやポッドキャスティング、ＳＮＳなど、個人がデジタルコンテンツをネットワークへ簡単に発信できるような形態が次々とサービスとして提供されている。

このような状況の中、電子化される権利が増加した場合に個人がその権利を保護し適切に利用するためのＩＤ管理の仕組みつくりが早急に必要となると考えられる。

３－３． カテゴリ３の領域における動向

この領域のＩＤは権利の行使に用いるＩＤのことで、特にＩＤによる本人確認方法に関わる技術が重要となる。（表２）

（１）記憶に基づく認証

ＩＤ／ＰＷやパスフレーズによるもので、サービス提供者側にとっては安価に導入可能であるが、ユーザにとっては各サービス毎に異なるＰＷやパスフレーズを頭の中に記憶しておく事ができないため、メモ帳やHDに保存する事となり、その結果盗み見や盗難といった危険性を高めたり、覚えやすいＰＷ（誕生日など）を設定するといった事により人的なセキュリティの穴が開くこととなる。

（２）所持品に基づく認証

ユーザにとっては記憶する必要はなくなるが、誤って紛失・盗難される危険性や貸し借り可能な問題がある。そのため実際には他の何らかの方式と組み合わせる対処がされている。例えば、銀行ＡＴＭの磁気カードの場合は４桁のＰＷとの組み合わせである。

（３）バイオメトリクス情報に基づく認証

バイオメトリクス情報に基づく認証では、静脈などの人間の身体情報を利用しているため、ユーザは記憶する必要も紛失する心配も、貸し借りの問題もない。しかし、一方で、システム的な認識率に起因する誤認の問題や、身体的特徴はＰＷなどの変更可能な論理的な関連付けとは異なり“代わりの指紋を生成する事ができない”あるいは、身体情報は個人と直接関連付いた情報であるため、“身体情報から逆に本人を特定することができる“といった問題も指摘されている[15]。

さらに、これらの分類であげた例以外にも、前述の課題を補完するためのさまざまな方式が提案されている。

表２．認証技術の分類

分類	例	利点	課題
記憶に基づくもの	パスワード、パスフレーズ	安価に導入可能	記憶忘れする 漏洩しやすい
所持物に基づくもの	ICカード、ワンタイムパスワードトークン 銀行のカード	覚える必要ない	紛失・盗難 機器の貸し借り
バイオメトリクス情報に基づくもの	指紋、静脈、虹彩	覚える必要ない 貸し借りできない	誤認の危険性 取替えが利かない 心理的抵抗感

（４）その他の補完技術

例えば、ひとつのＰＷで多くのサービスに安全に認証できるメカニズムでシングルサインオン（以下ＳＳＯ）技術がある。もっとも、普及しているＳＳＯはＷｅｂサーバに対するもので、Cookieや、LibertyAllianceProject[16]による方式などがある。

また、あわせ絵による認証やニーモニック認証では、既存の記憶に基づく認証方式において最大の問題点であった「人間に起因する問題」つまり人間が簡単に遂行できない「意味のない文字列を覚える」「定期的にまったく新しいＰＷに変更する」といった問題を回避するため。意味のない文

字列を「思い出す」から「画像を認識する」という行為に変換する事により、ユーザに課せられる記憶の負担を軽減している[17][18]。

リスクの大小によりパッシブ認証とアクティブ認証を使い分けるという考え方もある。ここで、リスクの大小とは、例えば、金額の小さな商取引と大きな商取引などのことである。ユーザが認証時にＩＤ／ＰＷの入力など、なんらかのアクションを必要とするものをアクティブ認証と位置づけ、アクセスしてきたデバイスの種類やＩＰアドレス、サイトにおけるユーザの行動パターンなどのプロファイルを過去のユーザ・プロファイルと比較して、正当なユーザであるかどうかを判断する事で、ユーザに認証のための操作を必要としないものをパッシブ認証と位置づけている。パッシブ認証の場合は、サービスの提供時に確実に認証できない場合もあり、ある程度のリスクには目をつむり、ユーザの利便性を最優先させる方法と言える [19]。ただし、リスクをどう判断するかについての議論の余地はある。

もし、ユーザがたった一つのＩＤを管理するだけで、あらゆるサービスの認証が安全に行われるのであれば問題にはならないが、そのようなことは現実にはありえないため、結局は各サービスにより要求される方式によるＩＤが氾濫することとなる。

所持物に基づくものの場合、個人の財布を圧迫しているが、定期券や少額決済機能、カード決済などの複数のＩＣカードの機能が携帯電話のようなひとつのデバイスで実現できるように、ＩＣカードによりＩＤを１枚に統一することも今後可能であろう。

バイオメトリクスは、誤認やユーザの心理的な抵抗感もあるため、現在は銀行ＡＴＭや携帯電話などのように選択的に利用されたり、他の区分の補助的な役割となっている。しかし、盛んに研究されている分野であり、今後の成果に期待できる。

記憶に基づく認証においては、前述のように代替手段が実用化されているにもかかわらず、ユーザの記憶に頼っているのが現状で、ユーザにとっては年々記憶すべきＰＷなどが増加している現状にある。また、スパイウェアやフィッシングなどにより個人のＩＤを盗み出し、不正アクセスする場合には、正当な情報を利用するため、見破るのは現在不可能に近く、サービス側にとっては、落ち度がないのに被害を受ける状況にある。

記憶に基づくものについては、現在抜本的な解決技術がなく、今後さらに深刻化する可能性が高いといえる。

３－４．　カテゴリ４の領域における動向

この領域のＩＤはＩＤの使用によって生じるＩＤで、主にＩＤの履歴記録とその利用に関する技術が重要となる。

履歴ＩＤの保存方法に関しては、例えば、センサーやカメラを用いて個人の日常生活の行動履歴を網羅的に生涯通じて保存し、様々に利用しようとするライフログの研究が行われている。ここでは網羅的に記録される情報は、大量にデータが保存されることになるが、有用な情報量の割合は低いと考えられており、情報の検索や活用を如何に効率化するかということが課題となっている。この問題を解決するために、重要性、同一性を判断し、クラスタリングする方式の研究や、データが取得された際のコンテキスト解析して取得情報に対してコンテキスト情報を与える手法の研究などが行われている[20]。

一方このようなＩＤの別の利用研究もあり、デジタルデータを法的問題解決に用いるためのデジタル・フォレンジックについての検討も進んでいる[21][22]。ここでは、デジタルデータの信頼性の確保のための技術、法制度の両面からの検討がされている。

これらの技術の進歩により、人間の行動履歴ＩＤが信頼性の高いデジタルデータとして保存され、それが簡単に分析されるようになることで、今後ますます様々な用途で利用されるようになると予想される。その一方で、様々な個人の行動や嗜好が名寄せにより簡単に分析されることで、新たなリスクが発生するとも考えられ、プライバシの問題などがさらに深刻化するであろう。

４　考察

ここでは、先に挙げた関連技術を概観し、ＩＤ爆発を解決するために必要となる技術についての考察を試みる。

カテゴリ１のＩＤについては、あらゆるモノへＩＤを付与するための基盤技術が整備されつつある。これにより、ＩＤを付与するためにはどうするかという課題から、あらゆるものへＩＤが付与された場合の問題点の抽出とその解決技術の検討へとシフトすることが重要となっている。

カテゴリ２のＩＤについては、権利発行側の法的、技術的基盤が整うことで、今まで紙で扱われた権利や、デジタルデータの権利などのＩＤ化が進み電子的な権利ＩＤが増加している。その一方で、個人におけるＩＤの管理については、ユーザ任せになっており、個人がその権利を保護し適切に利用するためのＩＤ管理の仕組みつくりが急務となっている。

カテゴリ３のＩＤについては、さまざまな本人確認のための技術が検討され実用化されているにもかかわらず、覚えるべき認証要素が年々増加する傾向にあり、ネットワークにおける脆弱性の根

源となっている。しかし、これについては、現在抜本的な解決方法がないといえる。

カテゴリ４のＩＤについてはネットワーク上だけでなく現実世界での個人の行動までもが、信頼性の高いデジタルデータとして保存され、それが簡単に分析される技術が整ってきている。これにより、便利になる一方で、個人の行動や嗜好が丸見えとなるリスクも増大している。

今まではネットワーク機器や固体のモノをネットワークで利用するためにＩＤが付与され、ユーザは自分を取り巻く数個の単一ＩＤを管理すればよかった。しかしながら、今後さらにＩＤが場所や、価値や人などあらゆるモノにＩＤが付与され、権利や能力や存在までもがデジタル化される一方で、ＩＤが別のＩＤにバンドルされＩＤの関係までもが複合的で複雑となっていき、新たなリスクや新たな負担が増大していくこととなる（図２）。

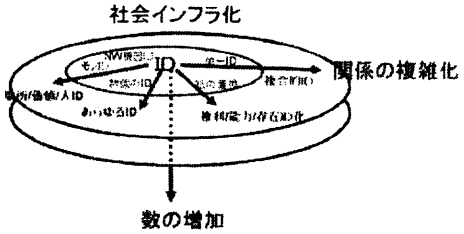

図２．ＩＤ爆発による管理負荷の加速

このような状況の中、ユーザが安全かつ効率的にＩＤ管理を実現するための技術が必要であり、ＩＤの関係を解きほぐし、ユーザ主体で統合、変更、削除などができる仕組みづくりが急務と考えられる。そのためには、サービス提供側に閉じた観点でのＩＤ管理システムではなく、蓄えられた情報をユーザとともに統合的に利用するような社会システムの構築を考える事が望ましい。

５　まとめ

本論文では、様々なネットワークサービスを提供するためのＩＤが氾濫し、返ってユーザを圧迫している状態であるＩＤ爆発において、先の論文で提示した４つのカテゴリに基づいて、ＩＤ爆発を解決するために必要となる関連技術動向を調査し報告した。

また、その上で、ＩＤ爆発を解決するための技術要件の見通しについて述べた。

今後の課題は、今回の調査結果を踏まえて、ＩＤ爆発でまず課題となる、”覚えきれない、管理しきれない”という問題を解決するための技術要件を明らかにしてゆく予定である。

【参考文献】

[1]斉藤典明, 櫛田達也, 山崎哲朗, 小林透, 金井敦：ネットワーク社会におけるＩＤ氾濫の課題分析, 情処技研, 2006-GN61-6(2006)
[2]gooID メモリー：http://idmemory.goo.ne.jp/
[3]”本人認証技術の現状に関する調査報告書”, IPA, http://www.ipa.go.jp/security/fy14/reports/authentication/(2003)
[4]岸上順一監修：ＲＦＩＤ教科書, アスキー出版(2005)
[5]http://www.dsri.jp/company/epc/intro.htm
[6]http://www.uidcenter.org/
[7]鵜沼宗利：RFID タグを用いた歩行者の経路誘導ー視覚障害者向け道案内システムー, 情報処理, Vol.45, No9, pp.918-922(2004)
[8]関良明：RFID を用いた遠隔制御手法：ID-Linker の検討, 信学技報, OIS2006-1, pp.1-6(2006)
[9]http://www.kevinwarwick.org/
[10]木下真吾, 星野文学, 小室智之, 藤村明子, 大久保美也子：RFID プライバシー保護を実現する可変秘匿 ID 方式, Computer Security Symposium 2003(CSS2003), Oct(2003)
[11]三重野友紀：ＩＣタグの利用に際して消費者のプライバシーを守るには, 知的資産想像, 2005 年 9 月号(2005)
[12]http://www.soumu.go.jp/s-news/2004/040608_4.html
[13]http://www.cidf.org/
[14]岸上順一：電子化知的財産とコンテンツＩＤ, 情報処理学会研究報告, Vol2001, No.17, pp.1-4(2001)
[15]瀬戸洋一：バイオメトリックセキュリティ認証技術の動向と展望, 情報処理, Vol.47, No6, pp.571-576(2006)
[16] http://www.projectliberty.org/jp/
[17]高田哲司, 小池英樹：あわせ絵：画像登録と利用通知を用いた正候補選択方式による画像認証方式の強化法, 情報処理, Vol44, No8, pp, 2002-2012(2003)
[18]徐強, 西垣正勝：ニーモニックに基づくワンタイム・パスワード型画像認証の実現可能性に関する検討, 情処研報, 2006-DSP-126, pp.317-322(2006)
[19]”ユーザー認証は『パッシブ』と『アクティブ』の両方で”, http://itpro.nikkeibp.co.jp/article/NEWS/20060426/236362/ (2006 年 8 月確認)
[20]井上知洋, 中村元紀:センサーとユーザフィードバックを用いたライフログアノテーション手法の提案, 信学総大講演論文集, Vol2006, D-4-6, pp.23(2006)
[21]http://www.digitalforensic.jp/C-F.html
[22]“デジタル・フォレンジックとは”, 辻井重雄, Computer&NetworkLAN, オーム社, No.257, 2005
複合的な脅威