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

2007－ＣＳＥＣ－38（１）
2007／7／19

位置認証と情報セキュリティに関する考察

高橋幸雄† 辻井重男‡

† 情報セキュリティ大学院大学 〒211-0835 神奈川県横浜市神奈川区鶴屋町 2-14-1
情報通信研究機構 〒184-8795 東京都小金井市貫井北町 4-2-1

‡ 情報セキュリティ大学院大学 〒211-0835 神奈川県横浜市神奈川区鶴屋町 2-14-1
E-mail: † dgs074102@iisec.ac.jp , takahashi@nict.go.jp ‡ tsujii@iisec.ac.jp

あらまし　現代社会において，カーナビや GPS 携帯によるウォークナビなど位置情報の利用は急速に普及し，また，緊急通報発信時における位置情報通知も開始され，日常生活においてますます重要な情報になってきている．一方，位置情報は，個人個々の情報であり，プライバシーの観点からも，その取り扱いには注意が必要である．そこで，信頼できる位置情報を提供するためのセキュリティや位置認証について述べる．位置情報のセキュリティでは，位置情報管理の手順の一案を示す．また，時刻認証と類似させることで，互換性や時刻認証の枠組みが活用できる位置認証について提示する．位置情報は個々の情報であるという特異性から，その信頼度やプライバシーについて，ユーザが自分で選択し，柔軟な対応ができるようにした．

キーワード　位置情報，位置認証，プライバシー，セキュリティ，時刻認証

The Study for the Position Authentication and the Security of Location Information

Yukio Takahashi† and Shigeo Tsujii‡

† Institute of Information Security, 2-14-1 Tsuruya, Kanagawa-ku, Yokohama, Kanagawa, 211-0835 Japan

National Institute of Information and Communication Technology, 4-2-1, Nukui-kitamachi, Koganei, Tokyo, 184-8795

‡ Institute of Information Security, 2-14-1 Tsuruya-machi, Kanagawa-ku, Yokohama, Kanagawa, 211-0835,Japan
E-mail: † dgs074102@iisec.ac.jp , takahashi@nict.go.jp ‡ tsujii@iisec.ac.jp

Abstract The use of the location information such as walk-navigation by the mobile telephone and car navigations using the GPS spreads rapidly, and the location information notification when the emergency call is started. The location information becomes more important in daily life. The location information is private, and it is necessary to have a high security from the viewpoint of privacy. The security of location information and the positional authentication are so described as to provide the trust location information. One example of the procedure of the location information management is shown. Moreover, the positional authentication similar to the time authentication is presented so that it can utilize the system of the time authentication. Flexible correspondence is made for the user to select the reliability and privacy level.

Keyword Location information, Position authentication, Privacy, Security, Time authentication

1. はじめに

位置情報サービスや GPS 付携帯電話の急激な普及により位置情報を安易に得ることができ，ITS やマンナビ，さらには社会生活における安全や信頼性向上など位置情報の利用が進んでいる．日本版 911 である緊急通報時における発信端末の位置情報を提供するように義務化され（事業用電気通信設備規則 改正：平成 18 年 1 月）[1]，各種情報端末での位置情報取得ができるようになってきている．

また，次世代ネットワーク NGN(Next Generation Network)の検討の中では，サーバの位置や端末の位置情報サービスの提供について考えられている．これが実現すれば，どこでもいつでも位置情報が得られ，ユビキタス位置情報が実現することで，位置情報を使ったアプリケーションが飛躍的に増加していくことが期待される．一方，位置情報に関して，利用促進の面だけで，プライバシー保護が不十分なまま利用されていくと，重大な問題になってくる可能性がある．さらに，個人の位置や行動が，いつのまにか取得され，公開されてしまうことも考えられる．例えば，防犯対策の監視カメラによる個人の行動が，第三者に取得され，カメラ映像が，インターネットなどにより公開されることもでてくる．これは，公然の監視による防犯抑制につながる反面，個人のプライバシーが，保護できなくなる状況になってくる．

位置情報は，重要な個人情報であり，プライバシー保護，安心・安全確保のためのセキュリティ基本指針の検討が必要

である．

2. 位置情報におけるセキュリティの必要な理由

位置情報において，なぜセキュリティが必要かについて考えてみる．位置情報は，個人情報であり，特に子供，女性，高齢者，著名人の居場所や，貴重品の在りかが判明すると，誘拐やストーカー，追っかけ，詐欺，ひったくり，盗難などの犯罪を助長してしまう恐れがある．また，人に知られたくない位置情報や行動が漏洩され，個人の名誉を著しく損なうことも出てくる．

また，心理的な面においても，位置情報が公に出てしまう．誰かに行動を見られているという意識から，自由に行動ができないため，行動の制約が起きる．

その他，位置情報による行動パターンがわかることにより誹謗中傷・攻撃が増加し，人々が無難な行動をとりがちになると個性の均一化なども心配される．

位置情報対するプライバシー保護といっても，各個人の感情，利用状況に応じて変わってくる．例えば，仕事関係の場合は，多少プライバシーは低くなると考えてもよし，直接的な被害が少ないことから利用者によっては，まったく気にしない人もいるであろう．したがって位置情報を扱う場合は，画一的なプライバシー保護やセキュリティ基準を考えると不便となり，逆に位置情報の利便性を阻害する可能性があるため，利用環境に応じた柔軟な対応ができるものが必要となる．

3. プライバシー問題と対策

位置情報の利用において，プライバシー問題が発生すると考えられる７つの場合を示す．

①個人の位置情報を集約した位置情報管理システム，位置情報提供システムから情報が公開あるいは漏洩されてしまう場合，

②特定の人にしか使用許可していない位置情報が，無意識または故意に，使用許可した人以外に漏れてしまう場合，

③不特定多数（個人を特定しない）位置情報に個人特定情報が付加されて公開されてしまう場合，

④悪意のある第三者が，位置情報を取得し，公開する場合，

⑤ある人の位置情報に無意識に他人の位置情報が含まれて公開されてしまう場合，

⑥個人が，自分または使用許可がある他の人の位置情報を，故意または誤って公開してしまう場合，

⑦第三者が，個人の通信を傍聴して，位置情報を取得・公開する場合．

①，②，③，④に対してはシステム管理者の問題であり，堅固な位置情報管理のセキュリティ対策，個人位置情報利用方法における対策をとるとともに，位置情報管理ポリシーの認定，監視が必要である．位置情報が個人情報としてみなすことができれば個人情報保護法によっても規制されることになる．

⑤に対しては，監視カメラの場合などで，社会制度としての位置情報公開ポリシーなどによる対策となる．

⑥に関しては，個人的な責任であるが，個人の位置情報利用ソフトウエアなどのセキュリティ強化も必要である．また，信頼できる人にしか情報を提供しないことや，法的な罰則規制などの対策を考える．

⑦に関しては，位置情報を通信する場合秘匿性の高い通信手段を使って実施し，暗号などを使うという対策となる．

また，位置情報に関するプライバシー保護のひとつの対策として，位置情報（個人情報）は漏れることを想定したもので，位置情報が公開されても，影響が少なくなるようにする方法がある，利用状況に応じたプライバシーレベルを考え，それに応じた位置情報表示を用いることで，未然に防ぐことが可能である．例えば仕事の場合はレベルを高く，私用の場合はレベルを低くするなどで，位置情報提供者が選択できるようにする．プライバシーレベルの例としては，位置表示において，１０ｋｍ程度以上，１ｋｍ程度，１００ｍ程度，１０ｍ程度などに分けて考える．緯度経度高さ表示では，４分角，２５秒角，２．５秒角，２５０ミリ秒角程度をひとつの区切りとする．また地名では，市・区，町名，番地，号番号等である

4. 具体例における位置情報のセキュリティ

位置情報の利用形態という観点から，位置情報のセキュリティについて考えてみる．位置情報の利用形態は，次の３通りが考えられる．

ア）自分の位置を，自分が必要とする表現で享受する場合（従来のナビゲーションやガイドシステム等），

イ）他の人の位置情報を，自分が検知・活用する場合（待ち合わせナビ，子供監視・老人徘徊，緊急時通報位置情報システム等），

ウ）不特定の人の位置情報を検知・活用する場合（人・車の位置情報を収集した安全ナビ・ITU，行動マーケティング）

現在の位置情報に関して主な利用となっているア）の場合に限れば，位置情報のプライバシーの問題が発生するケースは少ないと思われるが．今後位置情報を活用した位置情報サービス（LBS；Location Based Service）やNGNでの位置情報サービス等，イ）やウ）の利用が活発になることが予測されるので，これらに関するプライバシー保護，セキュリティ対策を主に考える必要がある．

次に，利用形態イ）の場合の具体的な例を用いて，位置情報のセキュリティについて検討してみる．位置情報活用の一般的な利用形態としては，複数の位置情報提供方法で位置情報を取得し，インターネット等を介して他の人が利用することが考えられる．その利用形態の例とて提案された汎用的位置情報基盤[2]をもとに想定した位置情報サービス（図１）について検討した．NGNにおける位置情報サービスも類似したものとなるであろう．位置情報提供者（ここでは“A”とする）は，GPSや位置情報提供携帯電話，SUICAなどのICカードやRFIDタグを用いて得られた位置情報を，登録した位置情報管理機関のシステムに自動的に提供し，蓄積しておく．一方，“A”の位置情報を知りたい位置情報利用者（ここでは”B”とする）は，登録している位置情報サービス機関に，“A”の位置情報を，ある位置情報表示でほしいと要求する．位置情

報サービス機関は，”A”の登録IDをもとに，位置情報サービス機関と契約している位置情報管理機関に，”A”の登録IDの確認後，最新の位置情報を要求し，位置情報を提供してもらう．位置情報の表示の違いは，位置情報変換プラットフォームで変換し，利用者“B”が要求した位置情報を，地図などのマッピングも含めて，提供するするシステムである．異なる位置計測システムを統一的に扱える位置管理構築技術，位置情報提供システム技術，位置情報提供者と利用者の間で位置情報を配信する技術，多様な位置情報を位置変換プラットフォーム技術が必要である．

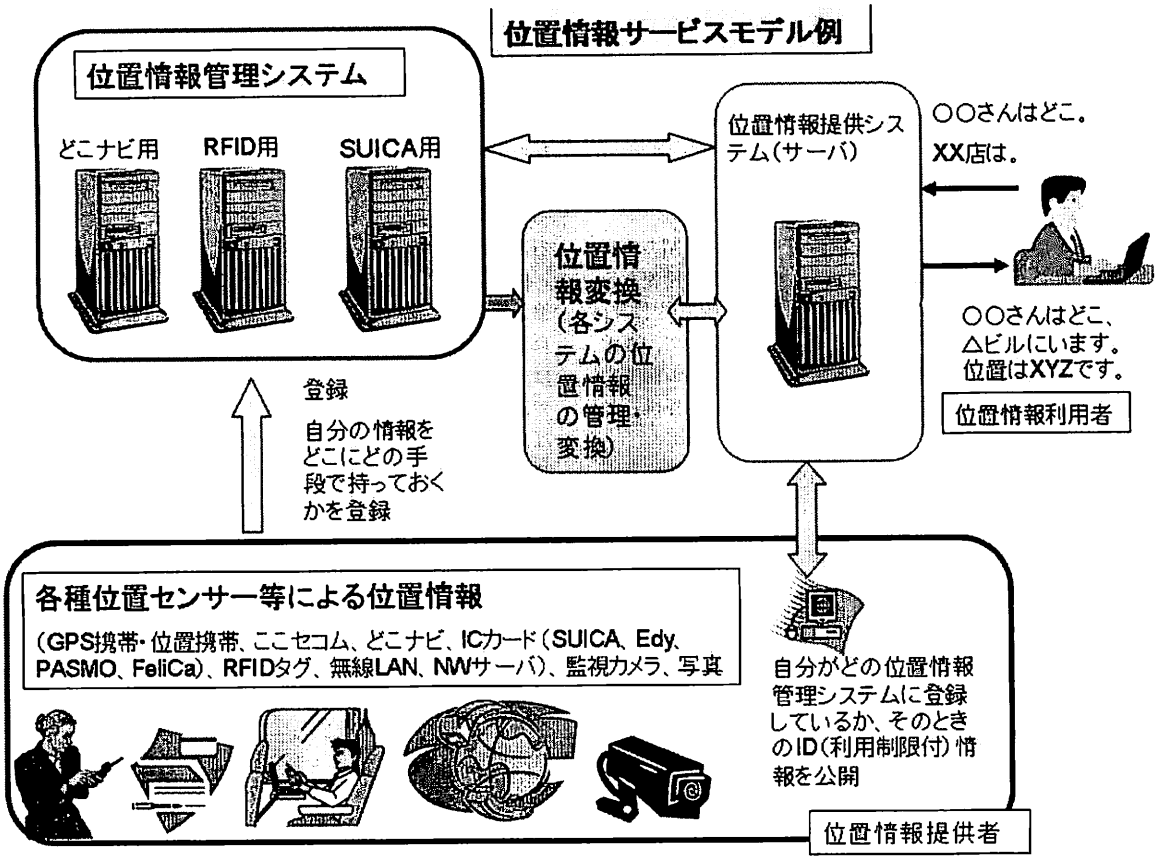

図1　位置情報サービスの例

まず，位置情報管理システム及び位置情報提供システムにおける位置情報管理は厳格に行う必要がある．管理システムは外部からの攻撃に強いシステムを導入するとともに，厳格な管理を行うために管理指針を各システムで設定し，公開しても問題とならない形で公表または監査機関に監査してもらう．管理指針は，OID（オブジェクトID）番号でリンクが取れることとする．利用者は，OIDが示す管理指針を見て選択することで，管理者の公然の監視ができる．位置情報は，犯罪やプライバシー関係するものであることから，管理機関は登録制にしたほうが望ましい．

次に，個人の位置情報を位置情報管理システムが集約する時に，個人の位置情報が勝手に位置情報管理システムに行かないような制限をつける必要がある．気づかないうちに，位置情報が集められていたという事態にならないように，登録意思を確認しながら実施していくことが必要である．特に，位置情報提供者が，誰にどのようなレベルの情報を知らせていいかなどの情報利用に関する制約をつけられるようにしておく．また，グループ単位で利用可能とするなど，セキュリティを確保しながら利便性の確保も考える必要性がある．位置情報利用者が，直接アクセスする位置情報提供システム運用時のセキュリティ確保も重要である．個人を特定した位置情報取得については，位置情報利用者・要求者に応じて，プライバシーレベルを情報提供者が選択できるようにしておく．

このシステムにおけるセキュリティを確保した手順の具体的な例を以下に示してみた．

①位置情報サービス機関に対する登録時

1）利用者の本人登録し，位置情報サービス機関の発行する番号・IDを受ける．

2）次に，どんな位置情報が活用できるかの情報登録（随時変更可能）を行う．

3）位置情報サービス機関が契約している位置情報管理システム機関の中から，自分が関係するものに関する情報提供

（位置情報管理システム機関の名前，登録番号等）をしてもらう．

4）自分の位置情報を教えていいメンバーの登録（随時変更可能）を行う．

5）自分が位置情報を知りたい人のメンバー登録（随時変更可能）を行う．

6）位置情報を享受してもいい仲間・グループの設定も可能とする．

②位置情報利用時

1）“A”（個人）またはグループ“a”（仲間）のメンバーの居場所を要求する．

2）“A”または“a”のメンバーが，その人に教えていい人かどうかの確認を行う．

3）確認できたら，その人の位置情報サービス機関の登録IDから，契約している位置情報管理システム機関の情報を元に，位置情報管理システム機関に位置情報提供の依頼を行う．

4）位置情報管理システム機関のポリシーに従って，要求された人の契約条件を考慮し，位置情報管理システム機関に蓄積されている位置情報をその記録時刻と合わせて提供してもらう．

5）位置情報サービス機関は，提供された幾つかの位置情報から，最新時刻や位置精度をもとに要求レベル，要求表現に合わせて位置情報を提供する．

③セキュリティ・信頼性確保の方法

1）位置情報管理，位置情報サービス等の管理・サービスに関するポリシーを公開し，公然の監視による信頼性を確保する．

2）位置情報管理機関，位置情報サービス機関等がポリシーにそった運営をしていることや，そのサービスの質などをチェックする任意（指定）調査機関による認定制度を確立し，適合マークなどを用いて，その信頼度を公開できるようにする．

3）任意（指定）調査機関の認定基準を，公的な立場の組織で議論し，設定し，公開する．

4）座標変換方法を公開し，その信頼性の確保を行う．

5. 位置認証の提案

位置情報をより信頼性を持たすため，位置情報が信頼できるものとするための検証法方法などが検討されている[3]．本報告では，信頼される位置情報を確保する方法として位置認証の概念を提案する．

位置情報を持った存在証明をするものであり，証明するものと証明は1対1対応することとする．位置認証を必要とする項目としては，製造（産地）特定，行動管理，アリバイ，作業証明，廃棄物管理証明，証拠写真の信憑性，記念写真・アルバム，利用制限，情報確認，データ証明，偽装防止，実空間情報の付加価値等があげられる．

位置認証の定義をする場合において，広く一般にタイムスタンプサービスとして利用され，日本でも平成17年4月からサービスが開始した信頼される“タイムビジネス”[4]を考慮して考える．タイムビジネスでは，情報通信研究機構が配信している高信頼の日本標準時を基にし，4社の時刻配信機関と，5社の時刻認証機関が実施している．2005年4月1日から施行された「e-文書法」において，法律により義務付けられている文書保存について，電子文書での保存が容認され，その電子文章の時刻管理・時刻証明をタイムスタンプによりできるようになる．国税関係の書類等については，電子文書保存の要件として，電子署名とタイムスタンプを付すことが義務付けられているなど，その重要性が，急速に高まってきている．

この時刻認証と類似させながら定義や手順を設定することで，時刻認証で用いられている文章の長期保存や信頼性の確保などの仕組みを利用できる．また，位置は変化することから位置認証・位置情報提供において，時刻も合わせて証明する使い方が一般的であるので，同時に結合して認証を実施することができる．

位置認証において代表的な位置情報提供方法である衛星測位システムGNSS（米国GPS；既運用，欧州Galileo；計画中，ロシアGLONASS；既運用，日本準天頂衛星QZSS；計画中など）は，簡便に高い精度での位置情報を提供することができ，急速に普及している．一方，衛星測位用シミュレータを用いれば，偽装した位置での偽装信号を容易に発生できるため，偽装かどうかを判別することは難しく，位置認証の位置情報としては不十分である．GPS付携帯電話のように単に位置情報を得る場合は偽装しやすいが，測位衛星からの信号の観測データを位置認証機関に送付し，解析して位置認証機関が位置情報を提供する方法[5]では，偽装はしにくくなり，位置認証における位置情報としては，信頼度は高まるが，完璧には成りすましを防ぐことはできない．偽装を判別するには，その場所近辺でしか得られない偽装されない特別な信号を受信する必要がある．そこで，例えばQZSSを使って，リアルタイムでは非公開であるが後に公開される特殊信号を付加することで，成りすましをしにくくし，GPSだけでは不十分な証明性を高めることができるものと考える．

次に，位置の測定精度は低いが，証明性は高い位置情報提供方法の例を示す．

1）携帯電話など，利用者を1対1で特定できる通信方式とあわせた通信の電波源強度の減衰や信号の遅れから求められる位置情報，2）RFIDやICカードによる位置情報，3）監視カメラの映像による位置情報，4）無線LAN，UWB等のネットワーク通信端末による位置情報，5）ランドマークなどの目印を一緒に写したカメラ映像にタイムスタンプを押したものによる位置情報などを活用した方法などが考えられる．また，将来的にはNGNで考慮されている位置情報サービスを活用することで，ネットワーク管理会社から位置情報を容易に得ることができるようになると考えられる．

また，これら，証明性の高いが位置精度が低いものと，高精度で容易な衛星測位とを組み合わせて利用することも考える必要がある．

図2に位置認証を実行する場合の，基本的な位置認証の手順の例を示す．コンテンツは，そのハッシュ値を用いて，ユーザまたは第三者が提供した位置情報を含めて，位置認証機関の秘密鍵で暗号化し，位置認証スタンプを作る．この位置認証スタンプを利用者に送り返して，その位置認証スタン

プを，必要に応じて公開鍵で復元し，もとのコンテンツのハッシュ値と確認して，同じであることを確認し，そこについている位置情報を，そのコンテンツの位置情報として用いる仕組みで，時刻認証と類似させている．時刻と位置は，その信頼性を除けば，同等に扱うことが可能と考えられる．時刻情報は，普遍で誰もが共通に刻むものであるから，ネットワークと処理の遅れを除けば，認証機関の時刻で証明でき，時刻の信頼性はきわめて高い．一方，位置情報は個別の情報のため，時刻のように簡単に証明性の高いものを提供できにくいという特殊性を持つので，信頼性は異なる．また，もうひとつの大きな違いは，時刻の表現は簡単であるが，位置情報は，きわめて多種多様である．提供できる位置情報と，要求される位置情報の表現が，大きく異なることもある．その変換が必要であるが，４章で述べた位置情報変換プラットフォームなどを活用して変換できるものと考える．

このように位置情報の信頼性や表現が，提供方法や状況に応じて異なるため，位置情報信頼性レベルを定義し，位置情報提供者の表現と位置認証利用者が必要とする表現の両方を含むことが可能な位置認証スタンプとする．また，４章で述べたプライバシーレベルも含めることで，利用者や位置情報提供者の必要性に応じて，位置の信頼度やプライバシーを使い分けることができるようにする．

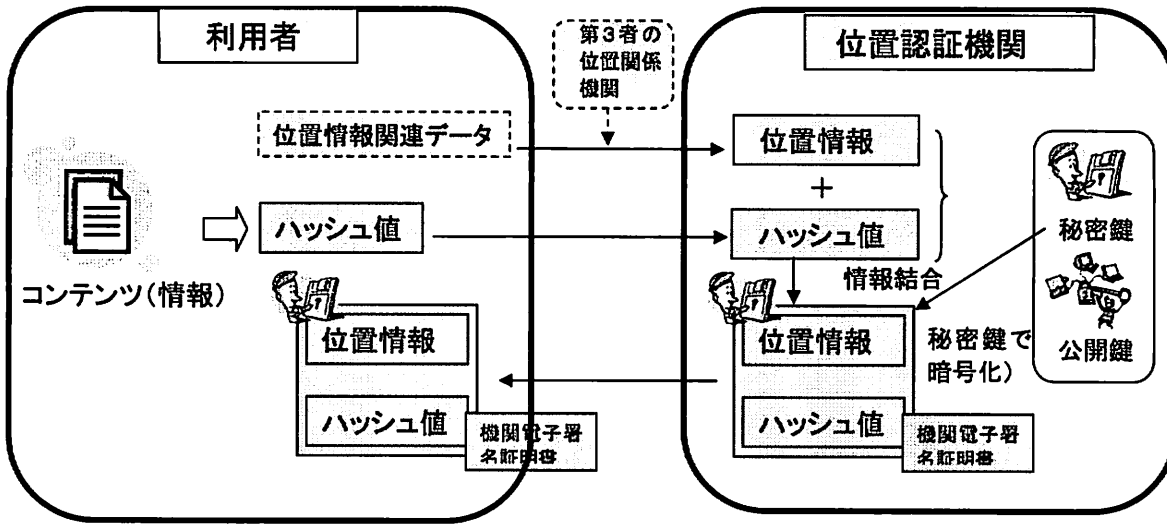

図２　位置認証の概要

6. 位置認証におけるプライバシー

位置認証で証明する位置情報は，重要な個人情報として，犯罪行為やプライバシー問題に絡む可能性があり，位置情報の秘匿性の考慮が必要である．また，認証は，一般的には位置認証をさせる人は，不特定多数というよりは，制限された人にしか許可しないこともあり，通常の位置情報ほど，プライバシーを保護しやすいが，位置認証自体が認証を行いたいと思う第三者が位置情報を知ることは避けられないので，注意は必要である．また，位置認証では，過去のある時点での位置情報が正しいかを確認することが多いので，リアルタイムでの位置情報が関係する犯罪行為に直結する危険性は，比較的低いのではと考える．

7. ３W認証

時刻認証との互換性をもった位置認証を用いることで，既にサービスが行われている時刻認証（When），個人認証・電子署名（Who）と，今回示した位置認証（Where）を組み合わせた３W認証を提案する．３W認証を用いることで，セキュリティを高めることができる．例えば，情報元，相手がわからないときに，どこから送られてきたかを確認することで，未然に被害を防いだり，情報を排除したりできる．成りすまし画面や迷惑メールに関しても，実際ありえない外国サイトや場所から配信された場合排除できるし，本人確認の助けにもなりうる．また，情報発信もとの場所が明確になれば，取締りの助けになるとともに，犯罪行為を行っている場所が多くの人の目に触れることで公然による監視となり，犯罪の抑止効果となる．

8. まとめ

今回，位置情報は個人情報で，そのプライバシー保護が必要な観点から，将来の位置情報サービスの例などを，用いて位置情報のプライバシー保護に関する考察を行った．

また，位置情報の重要性やその信頼のよりどころになるものとして，既にサービスを開始している時刻認証と類似した位置認証を提案した．時刻認証と互換性を持つことにより，その蓄積された仕組みを最大限に活用でき，効率的に構築することができるほか，位置と時刻という切り離せない情報を一緒にした３W認証もできる．

また，本報告で提案した位置認証は，位置情報の信頼度をレベル等で表示することで，ユーザが取得できる位置情報の信頼度の違いを含めた柔軟な利用が可能となる．位置情報で重要なプライバシーも，ユーザが状況に応じて選択して利用

できるシステムである．このように，ユーザの利用環境に応じて，適応できるものとなっている．

今後は，これらの位置情報のプライバシー保護の具体的な手法を，今後の位置情報サービスの中で，どのように実施するのがいいかの具体的な検討を行うとともに，今回提唱した位置認証を実施するために必要な具体案を提案して行く．

文　献

[1] 朝生雅人，中尾昌照，祖慶良実，“緊急通信発信時における位置情報通知機能の開発”，NTT DoCoMo テクニカル・ジャーナル，15巻1号，pp34-39，2007

[2] 原史明，沼田雅美，植原啓介，砂原秀樹，寺岡文男，“Universal Location Platform：汎用的位置情報基盤の設計と実装（位置情報サービス，＜特集＞ユビキタス時代を支えるモバイル通信と高度交通システム）”，情報処理学会論文誌，47巻12号，pp 3112-3123，2006

[3] 安齋潤，松本勉，”位置証明基盤における位置トークン検証問題とその解決方法（モバイルコンピューティング，＜特集＞ユビキタス社会を支えるコンピュータセキュリティ技術）”，情報処理学会論文誌，47 巻 8 号，pp 2344-2351，2006，

[4] 小宮山牧兒，“タイムビジネス信頼・安心認定制度業務開始”，日本データ通信協会，通号 142 巻，pp1-5，2005

[5] 小山康弘，市川隆一，神崎政之，丹野貴之，西村史隆，熊敏，”位置認証技術試験システムの開発”，日本地球惑星科学連合大会，D123-004，2006 年 5 月 16 日