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

安齋 潤[†] 松本 勉[††]

近年，移動体の位置情報を利用したサービスがさかんに研究されている．移動体のような物理オブジェクトの測位方式として複数の方式（GPS や RFID 等）が存在する．異なる測位方式を備えた複数の位置情報（位置トークン）の提供者，その位置トークンを用いて自身の位置を証明する証明者，位置トークンにより証明者の位置を検証する検証者からなる位置トークンモデルを考える．位置トークンモデルでは，測位方式の違い等により位置トークンの形式も異なる場合があり，必ずしも検証者がトークンを検証可能とは限らないという問題がある．本論文では，検証者に代わり位置トークンを検証する位置証明機関を想定することで，このような位置トークン検証問題を解決する．また，位置証明機関による位置トークンの検証方式についても検討する．

On Verifying Location Tokens in Location Certification Infrastructure

Jun Anzai[†] and Tsutomu Matsumoto[††]

Recently, mobile networks are actively studied. The networks provide services depend on mobile node location using various location measurement techniques (GPS, RFID and so on). We assume a model that consists of servers, provers, and verifiers. The server provides prover location data (we call location token) to the prover using the measurement techniques, the prover proves own location to the verifier using the token, and the verifier verifies the token. The verifier may not verify the since the verifier may not have all the corresponding verification methods. For solving this problem, this paper considers a location certification infrastructure that distributes location tokens.

1. はじめに

1.1 背景

近年，移動体端末のような物理オブジェクトの位置情報を利用した位置情報サービス LBS（Location-Based Service）がさかんに研究されている．LBS として，特定位置に存在する移動体端末への情報配信，歩行者のナビゲーション，移動体端末のトラッキング[9),20)]，アクセス制御[15)] 等が存在する．

一方，LBS を実現する測位方式として，GPS（Global Positioning System）方式[7)]，携帯電話等の基地局方式，無線 LAN 方式[10)]，RFID（Radio Frequency Identification）方式[14)]，レーダ方式[6)]，センサネットワーク方式[18)]，および通信遅延方式[1),5),16),19)] が存在する．これらは，有効範囲面では野外の広範囲で使用可能な GPS 方式から主に室内で使用する無線 LAN 方式まであり，安全性面では一般に安全性の低い RFID 方式から特定条件下で安全性が保証される通信遅延方式まで様々である．

LBS の一形態は，移動体端末が自身の位置をサーバに対して位置情報を用いて証明することでサービスを受けるものである．このような位置証明として，論文 19) に 1 種類の位置情報を想定したモデルが提案されている．さらに論文 3), 4) では，位置情報を様々な形式で表現したディジタルデータを位置トークンと呼び，異なる測位方式を備えた複数の位置トークン提供者，提供された位置トークンを用いて自身の位置を証明する証明者（移動体端末等），位置トークンにより証明者の位置を検証する検証者からなる位置トークンモデルを提案している．位置トークンモデルは，たとえば労働者の作業証明，廃棄物の正規位置への廃棄証明，生産物のトレーサビリティ等に利用が可能である．

1.2 従来方式の課題

測位方式は様々な特徴を有するため，システムに応じて適切な方式が選択される．そのため，位置トークンモデル[3),4)] は形式の異なる複数の位置トークンの流通が予想される．位置トークンは形式に応じて安全性や検証法が異なるため，任意の提供者により提供され

† パナソニックモバイルコミュニケーションズ株式会社
Panasonic Moble Communications Co., Ltd.
†† 横浜国立大学
Yokohama National University

た位置トークンは，必ずしも任意の検証者により高い確率では検証できない．たとえばある方式[19]では位置情報に提供者のディジタル署名を付加した位置トークンを提供するために検証者に署名検証を要求する．また，RFID 方式では ID データベースへの接続が必要である．本論文では，この問題を「**位置トークン検証問題**」と呼び，解決を図る．しかし，従来モデル[3),4)]では，この問題が考慮されていない．

一方，位置トークン検証問題と関連する問題[13)]がアプリケーションレベルで扱われている．このモデルは位置情報を含むユーザの様々なコンテキストを複数のアプリケーションが統一的方法により取得することを目的とする．そのため，アプリケーションの要求する形式にコンテキストを変換する機構を設け，コンテキスト形式に応じた取得方法の違いを隠蔽するコンテキスト把握機構 CHANSE[13)]を提案している．しかしながら，位置トークン検証問題は物理的に異なるエンティティ間の通信モデルを扱うため，アプリケーションレベルの CHANSE とは想定が異なる．また，CHANSE は位置を含む複数のコンテキストを想定しているため，具体的に位置を検証する方法は別途用意が必要である．

一方，位置トークン検証問題を解決するために，位置トークン仕様を標準化することが考えられる．筆者らは携帯電話等ある特定システムに限れば現実性はあると考える．ただし，本論文は複数システムを仮定しているため，標準化は困難であると仮定する．

1.3 本論文の目的

本論文は，位置トークン検証問題を解決する位置証明基盤 LoCI（Location Certification Infrastructure）を提案する．LoCI では，検証者に代わり位置トークンの検証を行う位置証明機関 LCA（Location Certificate Authority）を仮定することで，位置トークンの種別に依存した検証方法の差異を吸収する．このコンセプトは CHANSE に近いが，LCA は具体的な位置トークンとその検証法を定義し，かつその安全性を考慮して設計されている点が大きく異なる．

最近，位置トークンモデルの一種といえる商用の位置証明サービス[11)]が開始された．これは証明者である GPS 受信機を搭載したデジタルカメラの位置情報と写真画像から，提供者であるサーバが時刻情報と気象画像から生成した MAC を位置トークンとして提供するサービスである．検証者は MAC をサーバへ送ることで証明者の位置を検証することができる．LoCI では，このような商用位置証明サービスも包含できるような汎用的なフレームワークを目指して設計を行う．

また，LCA がクライアントの代理で位置情報を検証するというコンセプトは，公開鍵証明書の検証を検証サーバが代理する OCSP[12)]と近いが，様々な形式の位置トークンの検証を実現できる点が異なる．

2 章に LoCI の要件を定義し，3 章において LoCI のフレームワークを，4 章において LoCI の拡張方法の説明を行い，5 章において LoCI を評価する．

2. 要　　件

2.1 エンティティの定義

位置証明基盤 LoCI は以下のエンティティからなる：

検証者（V）：位置トークンを検証するエンティティ．

オブジェクト（O）：測位対象となる物理的なオブジェクト．携帯電話やノート PC のような移動体である．O は V が検証可能な位置トークンの形式を既知とする．

位置証明機関（LCA）：位置トークンを検証し，検証結果を通知するエンティティ．全エンティティが信頼する．O は高い確率で LCA を利用可能と仮定する．

提供者（S）：O を測位し，位置トークンを提供するエンティティ．論文 3), 4) の提供者と同じなので，ここでは簡単に説明する．以下に S の種類を示す．

ステーション：基地局やアクセスポイントのような特定位置に固定され，比較的高い計算能力を有する装置である．単体で信頼できると仮定する．

モバイル：ノート PC や携帯電話のような移動体であり，中程度の計算能力を有する装置である．

センサ：センサネットワークのノードや RFID のアクティブ型 IC タグのような，特定の位置に配置され，低計算能力を有し，能動動作可能な装置である．

タグ：RFID のパッシブ型 IC タグのような，計算能力のほとんどない，受動動作する装置である．

ポイント：O が自身の位置を算出する場合に利用する装置である．GPS 衛星や基地局を想定する．

2.2 位置トークンの定義

位置トークン LT（Location Token）は，測位方式より得られた位置情報をディジタル化したデータであり，S の出力を一次 LT，LCA の出力を二次 LT と呼ぶ．

2.2.1 一次位置トークン

位置スタンプ（LS: Location Stamp）：O の位置情報 L，測位時刻 T，O の ID，S の ID およびデータ D から安全なハッシュ関数 H を使用して取得したハッシュ値に対して S または LCA が安全なディジタル署名関数 Sig によりディジタル署名したメッセージである．S としてステーションを想定する．

D は測位時に S が O から取得したデータであり，タイムスタンプ[8] に位置情報を追加したものといえる．本 LT は論文 3)，4) に存在せず，本論文で独自に追加した．

位置証明書（LC: Location Certificate）：O の位置情報 L，測位時刻 T，O の ID，S の ID に対して S が署名したメッセージである．S としてステーションとモバイルを想定する．

位置証拠（LE: Location Evidence）：O が S から取得した位置に関する情報（ID または位置情報）であり，安全な MAC（Message Authentication Code）関数により取得した MAC 値が付加される．S としてセンサを想定する．

仮位置証拠（PLE: Provisional Location Evidence）：O が S から取得した位置に関連する情報（例：IC タグの ID）である．S としてタグを想定する．

位置リファレンス（LR: Location Reference）：O が S（例：GPS 衛星）を利用して計算した位置情報，または S から取得した位置計算に用いるプレ位置情報である．位置情報を計算する負荷を低減させるため，携帯電話ではプレ位置情報を基地局に送り，代理計算を依頼する Assisted-GPS 方式を利用する場合がある．そのため，本論文では独自に LR にプレ位置情報を含めた．

2.2.2 二次位置トークン

拡張位置証明書（ELC: Extended LC）：一次 LT の検証結果として得られる O の位置情報 L，時間 T，O の ID，S の ID，データ D のハッシュ値，存在フラグ F（存在/不在），一次 LT 種別 C，一次 LT のハッシュ値に対して LCA が署名したメッセージである．ただし，位置トークンの種別により，T，S の ID，データ D のハッシュ値は含めない．なお，F は通常は存在を設定し，不在検証の場合のみ不在を設定する．本 LT は論文 3)，4) に存在せず，本論文で独自に追加した．

2.2.3 位置トークンに関する処理

LT に関する処理として，以下を定義する：

生成：測位の結果（位置情報）を入力とし，一次 LT（LS，LC，LE，PLE，LR）を出力する．S が実行できる．

検証：単数または複数一次 LT を入力とし，検証結果を出力する．LCA が実行できる．詳細を 4 章に示す．LCA は以下の全基本検証法を利用できる．

LS/LC 検証法：記載された位置情報と発行者のディジタル署名を検証する．

表 1 提供者と測位方式に対応した一次位置トークン
Table 1 Primary location tokens corresponding to providers and measurement methods.

提供者＼測位方式	申告型	推測型	直接型
ステーション	ー	ー	LS/LC
モバイル	ー	ー	LC
センサ	ー	LE	ー
タグ	ー	PLE	ー
ポイント	LR	ー	ー

LE 検証法：LCA は発行者の MAC も検証し，正しい場合に ID データベースにアクセスして，ID 情報を位置情報に変換する．

PLE 検証法：LCA は ID データベースにアクセスし，ID 情報を位置情報に変換する．

LR 検証法：プレ位置情報の場合，基地局にアクセスし，プレ位置情報を位置へ変換する．

また，LCA は以下の全応用検証法を利用できる．

経路検証法：複数の一次 LT から O の移動経路を判断する．

範囲検証法：複数の一次 LT から O の存在する範囲を判断する．

不在検証法：単数または複数一次 LT から O が特定の位置に存在しないことを判断する．

変換：前記検証の出力を入力とし，一次 LT のハッシュ値と検証結果とを含む二次 LT（ELC）を出力する．LCA が実行できる．

2.3 測位方式の定義

O の位置を計測または位置情報を得る測位方式は論文 3)，4) と同じであり，ここは簡単に説明する：

申告型：O が LCA に自身の位置を自己申告する方式（例：GPS 方式）．一次 LT として LR を想定する．

直接型：O の位置を S が測位する方式（例：通信遅延方式）．一次 LT として LS/LC を想定する．

推測型：LCA が O の位置を証拠から推測する方式（例：RFID 方式）．一次 LT として LE，PLE を想定する．

表 1 に提供者と測位方式に対応した位置トークンを示す．現在はハイフンに相当する測位方式は存在しないと考えられるため，そのような測位方式が出現した場合は対応する位置トークンを定義すればよい．

2.4 セキュリティモデル

システムの安全性に関する仮定を示す：

- LS/LC 対応の S は PKI（Public Key Infrastructure）によるディジタル署名の生成が可能である．
- 認証情報がディジタル署名である二次 LT に対応の V は，PKI によるディジタル署名の生成，検

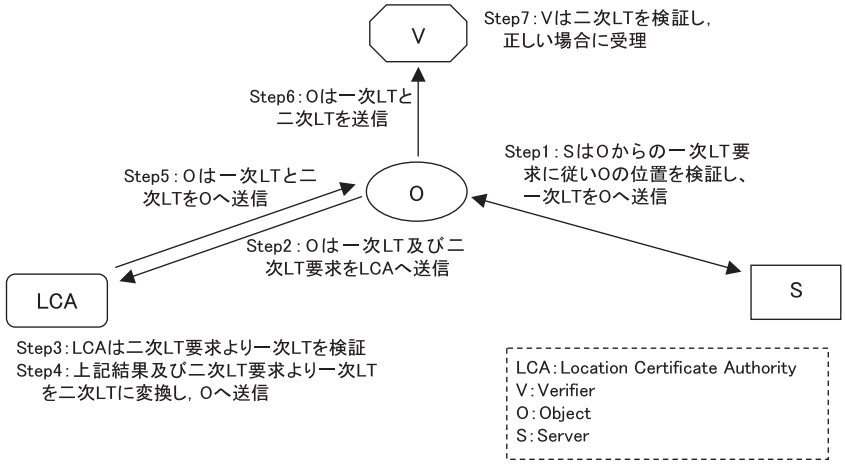

図 1 提案機構のシーケンス
Fig. 1 The sequence of our proposed mechanism.

証，利用する公開鍵の証明書の検証が可能である．

- LCA は PKI によるディジタル署名の生成，検証，利用する公開鍵の証明書の検証が可能である．
- LS/LC/LE のいずれかを発行可能な S，LCA，V は，O を認証できる．認証方法は PKI を前提とした公開鍵暗号または共通鍵暗号を用いた方式を用いる．

LoCI に対する攻撃および攻撃者の定義を行う：

- 攻撃の目的は，V に偽の LT を受理させること．
- 攻撃者は O または第三者である．
- 攻撃のため第三者と O は結託する可能性がある．具体的には，第三者が取得した一次 LT を O のものであると偽り LCA に受理させる場合を想定する．

2.5 位置証明基盤 LoCI の要件

LoCI は，以下の要件を満たさなければならない．

検証性：LCA が生成した二次 LT が，任意の検証者により高い確率で検証できること．

保存性：一次 LT に対して二次 LT の安全性が低下しないこと．具体的には，二次 LT から対応する一次 LT を特定可能であり，かつ二次 LT が含む一次 LT の検証結果があらかじめ定義された正しい手順で LCA により実施されていることを意味する．

3. 位置証明基盤 LoCI の詳細

3.1 LoCI のフレームワーク

図 1 を用いて LoCI のフレームワークを説明する．

Step1：提供者 S は，O からの一次 LT 要求に応じてオブジェクト O の位置を計測する．なお，LS/LC/LE のいずれかに対応する S は O を認証し，正しい場合，O の位置を測位する．測位の結果より，一次 LT を生成し，O へ送信する．O が攻撃者なら，一次 LT を改ざんし，LCA に偽の LT を受理させる攻撃が想定され，その耐性は一次 LT の種別に依存する．

Step2：O は位置証明機関 LCA へ一次 LT と二次 LT 要求を送る．二次 LT 要求は，二次 LT に付加する認証情報種別（ディジタル署名，MAC，なし），応用検証の種別（経路，範囲，不在，なし），検証対象位置（経路，範囲，不在範囲），検証対象期間を含む．

Step3：LCA は O を認証し，正しい場合，二次 LT 要求を受け入れる．二次 LT 要求より一次 LT を検証する．検証方法の詳細を 3.2 節に，**図 2** に流れを示す．

Step4：LCA は Step3 の検証の出力と一次 LT の種別（LS/LC/LE/PLE/LR）を含む二次 LT に変換する．変換方法の詳細を 3.3 節に，図 2 に流れを

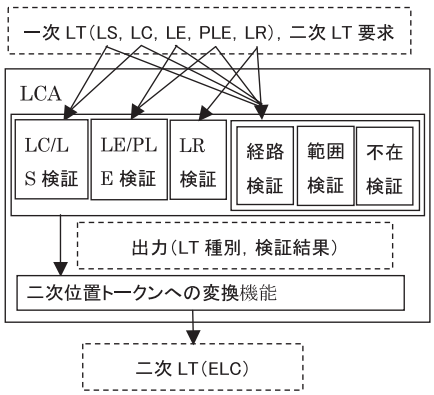

図 2 LCA の機能ブロック
Fig. 2 The function block of LCA.

示す．

Step5：LCA は一次 LT と二次 LT を O へ送信する．

Step6：O は検証者 V に一次 LT と二次 LT を送信する．

Step7：V は O を認証し，正しい場合，二次 LT を検証する．検証結果が正しい場合，二次 LT に含まれる位置情報を受理する．

上記説明では O が LCA に二次 LT への変換を依頼しているが，V が O または S から得た一次 LT を二次 LT 要求とともに LCA に送り，二次 LT へ変換してもよい．

3.2 位置トークンの検証

LCA による一次 LT の基本検証法を以下に示す．

LS/LC 検証法：記載された位置情報に矛盾がないことを確認，および PKI の手順によりディジタル署名を検証する．

LE/PLE 検証法：LCA は ID データベース（IDB）にアクセスし，ID に関連付けされた位置情報を取得する．なお，LCA が ID データベースを兼ねてもよい．MAC の検証法は一般的な MAC と同じである．MAC の検証に必要な共通鍵は IDB が有するものとする．

Step1：LCA は一次 LT に含まれる ID をクエリとして IDB に送信する．

Step2：IDB は ID リストから一致する ID を検索する．

Step3：IDB は ID に関連付けられた位置情報（IC タグの埋め込まれた地理的な位置等）をアンサとして LCA へ送信する．

タグの出力が固定値の場合，ID を一度取得すれば再度そこに行く必要がないため，ID は時間等に依存して毎回変化し，かつその値が S と LCA 以外に予想困難なことが望ましい．これを実現するため，タグと IDB で共有する共通鍵をシードとして安全な擬似乱数生成器 PRG によりワンタイム ID を生成する．

LR 検証：位置情報の場合，検証処理は実施しない．プレ位置情報の場合は基地局にアクセスして位置情報への変換を行う．LCA が基地局を兼ねてもよい．

次に LCA による一次 LT の基本検証法を以下に示す．

経路検証：複数の一次 LT から O の移動経路（**図 3**）を検証する方法である．論文 17) に紹介されたリンク型タイムスタンプ法を参考に，一次 LT および S に対する攻撃耐性の向上を図るリンク方法を提案する．

a) **経路リンク**：S_i は S_j（$i \neq j$）が生成した一次位置トークン LT_j を O から取得し，LT_j に依存して新しい LT_i を生成する方式である．たとえば LT 生成関数を Gen（S の秘密鍵 P，位置情報 L_i），$\|$ を連接記号とし，$LT_i = \mathrm{Gen}(P_i, L_i \,\|\, H(LT_j))$ と実現できる．

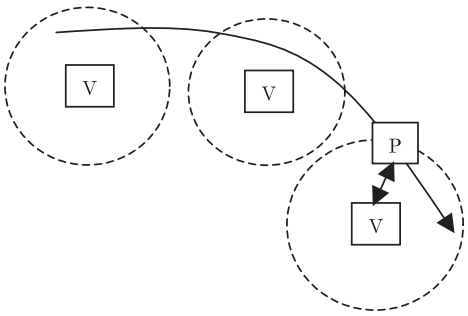

図 3 経路検証
Fig. 3 The route verification.

b) **時刻リンク**：S_i は自身が前回生成した一次 LT_{i_1} に依存して新しい LT_{i_2} を生成する方式である．S は生成した全一次 LT を履歴として保持する．たとえば $LT_{i\_2} = \mathrm{Gen}(P_i, L_i \,\|\, H(LT_{i\_1}))$ と実現できる．

c) **経路・時刻リンク**：S_i は O から得た S_j（$i \neq j$）が生成した LT_j と，前回生成した一次 LT_{i_3} に依存して新しい一次 LT_{i_4} を生成する方式である．S は生成した全一次 LT を履歴として保持する．たとえば $LT_{i\_4} = \mathrm{Gen}(P_i, L_i \,\|\, H(LT_j \,\|\, LT_{i\_3}))$ と実現できる．

LCA は上記リンクによる一次 LT を，次の手順により検証し，検証結果を出力する：

Step1：基本検証法により複数一次 LT を検証する．

Step2：次のように複数一次 LT のリンクを検証する．

経路リンクの検証：経路リンクが各 S の位置と矛盾しないことを確認できた場合は検証成功と判断する．たとえば，ある経路上に順に S_1，S_2，S_3，S_4 が存在する場合，S_3–S_1–S_4–S_2 と実際と異なる順序に一次 LT がリンクされていないこと．

時刻リンクの検証：時刻リンクが各 S の履歴と矛盾しない場合は検証成功と判断する．

経路・時刻リンクの検証：経路リンクおよび時刻リンクの検証を両方とも実施する．

Step3：S_i–S_j 間距離から予想される O の移動時間，LT_i と LT_j から算出された移動時間の差が，許容範囲以内と確認できた場合は検証成功と判断する．S_i–S_j 間経路を考慮する場合のみ実施する．

Step4：Step1–3 のすべての検証に成功した場合経

路検証が成功したと判断する．

範囲検証：k 個の一次 LT を用いて，二次 LT 要求に含まれる検証対象範囲 L_R と期間 T_R に O が存在したことを検証する．位置と時間の観点で検証する．

a) 位置の検証
- k 個の一次 LT が示す位置 $L_1, L_2, \cdots, L_k$ が検証対象範囲 L_R に含まれる場合（$\{L_1, L_2, \cdots, L_k\} \subseteq L_R$），検証に成功したと判断する．

b) 時間の検証
- k 個の一次 LT が示す時刻 $T_1, T_2, \cdots, T_k$ が検証対象期間 T_R に含まれる場合（$\{T_1, T_2, \cdots, T_k\} \subseteq T_R$），検証に成功したと判断する．

  ただし，個々の LT が示す時刻 $T_1, T_2, \cdots, T_k$ のうち連続する時刻間の差があらかじめ定められた時間を超える場合は検証失敗とする．

不在検証：k 個の一次 LT を用い，二次 LT 要求に含まれる不在範囲 L_A と不在期間 L_A に O が存在しないことを検証する．位置と時間の観点で検証する．

a) 位置の検証
- k 個の一次 LT が示す位置 $L_1, L_2, \cdots, L_k$ が検証対象範囲 L_A の補集合に含まれる場合（$\{L_1, L_2, \cdots, L_k\} \subseteq \overline{L_A}$），検証に成功したと判断する．

b) 時間の検証
- k 個の一次 LT が示す時刻 $T_1, T_2, \cdots, T_k$ が検証対象期間 T_A に含まれる場合（$\{T_1, T_2, \cdots, T_k\} \subseteq T_A$），検証に成功したと判断する．

  ただし，個々の LT が示す時刻 $T_1, T_2, \cdots, T_k$ のうち連続する時刻間の差があらかじめ定められた時間を超える場合は検証失敗とする．

不在検証では，O は L_A に不在であることを証明したいが，自身の位置は開示したくない場合がある．その場合，LCA は二次 LT へ一次 LT および $L_1, L_2, \cdots, L_k$ を含めず，不在のみを保証してもよい．

3.3 二次位置トークンの変換

LCA は 3.2 節に示した検証法より得た一次 LT の検証結果と一次 LT 種別 C と一次 LT のハッシュ値に対して，二次 LT 要求の認証情報種別に指定された方法により認証情報を付加し，拡張位置証明書 ELC を生成する．

4. 拡　　張

本章では，LoCI のフレームワークの拡張方法を示す．

4.1 履歴・刻印

位置証明機関 LCA，提供者 S，検証者 V またはオブジェクト O は個々の処理の履歴を保存する．また，O は一次位置トークン LT の発行を受ける際，LCA，S，V に対して刻印（自身の ID 等）を送信し，LCA，S，V はそれを記録する．もし，正当な要求があった場合，可能ならば署名または MAC を，履歴または刻印に付加し，履歴または刻印を開示する．これにより検証精度の向上，および紛争時の調停を可能とする．

履歴・刻印を V，S，P，V のエンティティ間で流通させることにより，履歴・刻印の信頼性を高める．具体的には，一定時間または処理ごとに履歴・刻印を他のエンティティに送信し，他のエンティティはそれを履歴として記録する．O は，他のネットワークへ移動する際に送信してもよい．また，履歴・刻印を保存する専用エンティティとして履歴・刻印データベース HSDB を設け，すべてのエンティティの履歴・刻印を HSDB に集めてもよい．

4.2 複数オブジェクトの位置証明

S は複数 O の測位した結果を含む LT を提供可能である．LS/LC の場合は，発行先として複数 O の ID を記載すればよい．複数 O の位置を検証するには，測位方式をそれぞれの O に対して使用するほか，複数 O を同時に検証可能な通信遅延利用方式[2] を利用することができる．また，RFID のリーダは複数タグの ID を同時に読み込めるため，それらの ID を発行先に含めた LE/PLE を発行することも可能である．

5. 評　　価

LoCI が 2.5 節に示した要件を満たすことを示す．

5.1 検 証 性

LoCI は，既存の測位方式を 3 種類に分類し，それらに 5 種類の一次 LT をマッピングし，かつすべての LT に検証法を定義したことにより，LCA は既存の複数の測位方式に対応できる．また，2.1 節の定義より O は高い確率で前記 LCA を利用可能であり，かつ O は V が実施可能な検証法を既知である．したがって，LCA を用いて O は一次 LT を二次 LT 要求で指定した形式の二次 LT へ変換できる．さらに，V は既知の検証法で二次 LT を検証できる．以上により，LoCI は検証性を満たす．

5.2 保 存 性

一次 LT から二次 LT へ変換されるまでに安全性が保存されていることを確認するため，一次 LT の流通時の安全性，LCA における一次 LT の検証，および二次 LT への変換の安全性の観点から保存性の検証を行う．これらの考察の結果より，LoCI は保存性を満たす．

位置トークンの流通：一次LTは，仮位置証拠PLEと位置リファレンスLR，ディジタル署名またはMACが付加された位置スタンプLSと位置証明書LC，および位置証拠LEのグループに分けられる．
- LS/LCおよびLEの流通時の安全性はディジタル署名方式またはMAC方式に帰着する．
- PLEおよびLRは，偽造や改ざんが原理的に可能であるため，VはPLEとLRをベースとする二次LTであることを確認した場合，安全性の保証がないことを認識して利用する必要がある．

なお，PLEは，タグのIDが時間や取得回数により変化し，かつその値が安全なPRGにより生成される場合，攻撃者によりIDが予想困難なため，偽造や改ざんを検出することが可能である．

また，第三者の一次LTをOの一次LTであるとLCAへ偽る結託攻撃の耐性に関しても，Sが信頼可能と仮定したとき，一次LT自体の安全性に帰着する．

位置トークンの検証・変換：VはLCAを信頼すると仮定するため，Vは二次LTに含まれる検証結果も信頼する．よって，LTの検証・変換の安全性はLCAが利用する検証・変換法の安全性に帰着する．
- LC/LS検証法の安全性は，PKIにおけるディジタル署名の安全性に帰着する．
- LE検証法の安全性は，MACの安全性に帰着する．
- PLE検証法の安全性は，前述したようにタグが出力するIDの変更法の安全性に帰着する．
- LR検証法の安全性は，保証困難である．ただし，LRは発行時点から安全性が保証困難であるため保存性とは矛盾しない．
- 経路検証法は，リンク型タイムスタンプのリンキングプロトコルに近い手法のため，安全性はタイムスタンプ方式とほぼ等しい．例外として，Oが特定の移動先において一次LTを取得しないことで経路を改ざんするタイムスタンプに存在しない攻撃を想定する場合，経路検証法Step3に示したOの移動時間を利用した攻撃検出手法を利用できる．
- 範囲検証は，単純に検証対象範囲 L_R と検証対象期間 T_R にそれぞれ複数の一次LTが示す位置 $L_1, L_2, \cdots, L_k$ と時刻 $T_1, T_2, \cdots, T_k$ が含まれるかどうかを確認しているだけであるため，T_R 内でかつ $T_1, T_2, \cdots, T_k$ 以外の時刻にOが L_R 外に存在する可能性がある．そのため，$T_1, T_2, \cdots, T_k$ のうち連続する時刻間の差があらかじめ定められた時間を超える場合は検証失敗とすることで不正を検知する．
- 不在検証は，範囲内か範囲外かを検証するのが異なるのみで範囲検証の安全性と同様である．
- 二次LTへの変換は，検証結果に加えて一次LTのハッシュ値を含ませるため，二次LTから対応する一次LTを特定することが可能である．

6. まとめ

本論文では，複数種類の測位方式と複数種類の位置トークンを想定した位置トークン流通モデルにおける位置トークン検証問題を指摘し，位置証明機関LCAの仮定により解決する位置検証基盤LoCIを提案した．

今後は，具体的に提案した位置トークンの検証法の安全性を詳細に検討していく必要がある．

参考文献

1) 安齋 潤，松本 勉：位置検証（1）：中継攻撃に耐性を有する位置検証方式，暗号と情報セキュリティシンポジウム（SCIS2005）予稿集，2B4-3 (2005).
2) 安齋 潤，松本 勉：位置検証（2）：複数証明者を検証可能な位置検証方式，暗号と情報セキュリティシンポジウム（SCIS2005）予稿集，2B4-4 (2005).
3) 安齋 潤，松本 勉：安全な暗号位置情報サービスの構成方法，情報セキュリティ研究会，2B4-4 (2005).
4) Anzai, J. and Mastumoto, T.: How to Construct Cryptographic Location-Based Services, *Proc. SecUbic-05* (2005).
5) Brands, S. and Chaum, D.: Distance-Bounding Protocols, *Proc. Eurocrypto'93*, pp.344–359, Springer-Verlag (1993).
6) Capkun, S. and Hubaux, J.P.: Securing position and distance verification in wireless networks, Technical report EPFL/IC/200443, submitted to *ACM MobiCom04* (2004).
7) Gabber, E. and Wool, A.: How to prove where you are: Tracking the location of customer equipment, *Proc. 5th ACM Conf. Computer and Communications Security* (*CCS*), pp.142–149 (1998).
8) Haber, S. and Stornetta, W.S.: How to Time-Stamp a Digital Document, Journal of Cryptology, *The Journal of the International Association for Cryptologic Research*, Vol.3, No.2, pp.99–111 (1991).
9) Izumi, M., Takeuchi, S., Watanabe, Y., Uehara, K., Sunahara, H. and Murai, J.: A Proposal on a Privacy Control Method for Geographical Location Information Systems, *Proc. INET'00* (2000).

10) Kitasuka, T., Nakanishi, T. and Fukuda, A.: Indoor Location Sensing Technique using Wireless Network, *Proc. Computer System Symposium'02*, pp.83–90 (2002).
11) 位置時間証明情報提供サービス．http://www.mitsubishielectric.co.jp/coco-dates/
12) Myers, M., Ankney, R., Malpani, A., Galperin, S. and Adams, C.: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP, RFC2560, IETF Network Working Group (1999).
13) 中村哲也，松尾真人，板生知子：適応型通信サービスにおけるコンテクスト把握機構 CHANSE，情報通信学会論文誌，Vol.43, No.2, pp.593–604 (2002).
14) Nakanishi, K., Nakazawa, J. and Tokuda, H.: LEXP: Preserving User Privacy and Certifying the Location Information, *2nd Workshop on Security in Ubiquitous Computing Ubicomp'03* (2003).
15) 榮樂恒太郎，新城 靖，樋爪真紀，中田吉法，板野肯三：高い情報生存能力を実現するラッパ SysGuard におけるガード・モジュールの開発環境，日本ソフトウェア科学会第 4 回プログラミングおよび応用のシステムに関するワークショップ (2001).
16) Sastry, N., Shankar, U. and Wagner, D.: Secure Verification of Location Claims, Report No.UCB//CDS-03-1245, University of California, Berkekey.
17) 宇根正志，松浦幹太，田倉 昭：デジタルタイムスタンプ技術の現状と課題，金融研究，日本銀行金融研究所 (2004).
18) Vora, A. and Nesterenko, M.: Secure Location Verification Using Radio Broadcast, *Proc. OPODIS 2004: 8th International Conference on Principles of Distributed Systems* (2004).
19) Waters, B.R. and Felten, E.W.: Secure, Private Proofs of Location, Princeton University Computer Science Technical Reports, TR-667-03 (2003).
20) Watanabe, Y., Takeuchi, S., Teraoka, F., Uehara, K. and Murai, J.: The Geograhical Location Information System with Privacy Protection, *IPSJ Journal*, Vol.37, No.6 (1996).

(平成 17 年 11 月 24 日受付)
(平成 18 年 6 月 1 日採録)

安齋 潤

1996 年 3 月東海大学工学部通信工学科卒業．同年 4 月松下通信工業（株）入社（現パナソニックモバイルコミュニケーションズ（株））．1997 年 4 月から 2001 年 9 月まで（株）高度移動通信セキュリティ技術研究所へ出向し，情報セキュリティの研究に従事．現在，携帯電話のセキュリティソフトウェアの開発に従事．2005 年 9 月横浜国立大学大学院環境情報学府博士後期課程修了．博士（工学）．電子情報通信学会会員．

松本 勉

1986 年 3 月東京大学大学院博士課程（電子工学）修了，工学博士．同年横浜国立大学工学部専任講師．現在，同大学大学院環境情報研究院教授．1981 年より，暗号・電子署名のアルゴリズムとプロトコル，ディジタル証拠性，耐タンパソフトウェア，情報ハイディング，ネットワークセキュリティ，認証方式，バイオメトリクス，人工物メトリクス等の各種情報セキュリティ技術の研究教育とその実応用に力を注ぐ．1982 年に「明るい暗号研究会」を数人の仲間とともに創り研究をはじめた．国際暗号学会 IACR 理事．CRYPTREC 暗号モジュール委員会委員長．電子情報通信学会より「情報セキュリティの基礎理論」への貢献に関して業績賞を受賞．