情報処理学会論文誌 Vol. 52 No. 2 680–689 (Feb. 2011)

安全な地図情報配信システムに関する一考察

秦野康生[†1] 宮崎邦彦[†1] 鈴木邦康[†2]
高橋由泰[†1] 山田隆亮[†1] 本多義則[†1]

近年，たとえば測位手段の多様化などにともない，屋外だけでなく，屋内空間を対象とした地図情報サービスが注目されてきている．屋内地図情報では，屋外地図だけでは表現できなかったより詳細な情報を含むため，屋外地図情報と比較し，施設・建物の利用者・管理者などに関するプライバシや機密情報がより多く含まれる．また，1つの施設・建物に対して，複数の所有者・管理者が存在することが想定される．したがって，屋内地図の配信においては，屋内地図に含まれる機密情報を，各地図情報の所有者・管理者の意思（誰にどの部分を見せることを許すかなど）を適切に反映して配信することが重要である．本稿では，上記の課題を解決するため，暗号技術を用いた地図情報配信システムを提案し，その実験結果について報告する．

A Study on Secure Geographic Information System

Yasuo Hatano,[†1] Kunihiko Miyazaki,[†1]
Kuniyasu Suzuki,[†2] Yoshiyasu Takahashi,[†1]
Takaaki Yamada[†1] and Yoshinori Honda[†1]

Recent development of various positioning technologies like a global positioning system (GPS) promotes geographic information services using not only outdoor but also indoor map information. However, on indoor map information services, it is desired that service providers manage indoor map information carefully, because indoor map information often contains sensitive information, e.g., layout in exclusion zone. In addition, there are many administrators in commercial complex, office building for rent and so on. Therefore, if a service provider uses indoor map information, it must protect sensitive information in the indoor map according to instructions from each of the administrators. In this paper, in order to achieve this, we propose a novel distribution system for indoor map information and report a prototype development of the proposal system.

1. はじめに

1.1 背景・目的

近年，たとえば測位手段の多様化などにともない，屋外だけでなく，屋内空間を対象とした地図情報サービスが注目されてきている．屋内地図には，屋外地図だけでは表現できなかったより詳細な情報が含まれる．このため，広く共有されることにより，あらたなサービスや利用形態が生まれることが期待される．しかしながら，屋外の情報はもともと誰でも入手可能な公の情報であると考えられることが多かったのに対し，屋内の情報は，施設・建物の利用者・管理者などの私の情報であるといえる．そのため，屋外地図と比較すると，プライバシや機密情報がより多く含まれることになる．

また，屋内の地図情報では，1つの施設・建物に対して，複数の所有者・管理者が存在する場合がある．たとえば，ショッピングモールや百貨店などの複合商業施設，あるいは，オフィス用の賃貸ビルなどでは，1つの屋内空間に複数の管理者が存在し，個々の管理者が各担当区画内の地図情報を作成，所有することが考えられる．屋内地図に含まれるプライバシや機密情報を保護するためには，屋内地図の配信者が，それぞれの管理者の意思（誰にどの部分を見せることを許すかなど）を適切に反映することが重要となる．

従来技術を用いて，地図情報の配信制御を行う場合には，地図情報を平文の状態で配信サーバ上に保管し，地図情報を閲覧する利用者を認証したのち，開示可能な地図情報のみを利用者に配信することが一般的である．そのため，従来技術では，複数存在する地図の管理者からの個別の要求に応じ，適切に開示先の設定を行うことが必要となる．また，配信時のログ生成などにより，その設定が正しく実行されていることを，それぞれの管理者に示すことが必要となる．

本稿では，暗号技術を用いた地図情報配信システムについて提案する．本稿で提案する地図配信システムでは，屋内地図情報の保護のため，公開鍵暗号を用い，それぞれの管理者が地図情報の開示先の設定を行い，設定に基づき暗号化を行う．地図を配信する地図情報配信者は，暗号化された状態で地図情報を保管し，利用者に応じて復号に必要な秘密鍵を選択，復号することによって，利用者ごとに地図情報の制限的な開示を行う．

†1 株式会社日立製作所システム開発研究所
Hitachi Ltd., Systems Development Laboratory
†2 株式会社日立アドバンストシステムズ
Hitachi Advanced Systems Corporation

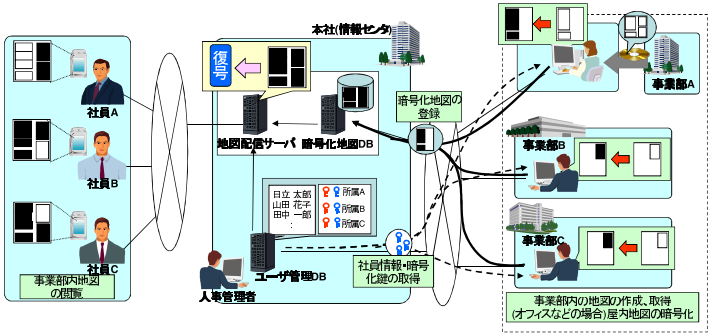


図 1　提案システムを利用したサービス例
Fig. 1　Example service of the proposal system.

本稿で提案する地図情報配信システムでは，地図の管理者自身が暗号化を行うため，地図情報配信時に管理者の意思を適切に反映することが可能となる．これにより，たとえば複合商業施設や大規模企業における事業部地図の管理，あるいは，オフィス貸出におけるビル内の地図管理など，1 つの施設内に複数の管理者が存在する場合に有用な地図情報配信システムの実現が可能となる．**図 1** に，その一例として大規模企業における事業部地図管理のイメージ図を示す．

1.2　従 来 技 術

従来技術では，たとえば Web サービス上のセキュリティ機構や DRM（Digital Right Management）を利用し，配信者（サーバ）側で認証を行い，開示する地図情報へのアクセスを制限する方法が知られている[2),9)]．特に，DRM を利用した方式[9)] では，詳細地図の情報を暗号化して保管し，認証結果に基づき復号鍵（ライセンスキー）の取得の可否を判断することで，利用者ごとに地図情報へのアクセスを制限する方法が示されている．しかしながら，これらの方式では，同一の地図情報を，利用者ごとに異なる地図表示を行う方法については示されていない．たとえば，機密エリアを含むフロアを閲覧させる場合に，権限のある利用者には機密エリア内の間取りを含む地図を表示し，権限のない利用者に，同一の地図表示において，機密エリアを非開示の状態で表示する方法については示されていない．

本稿では，地図情報の配信者が暗号化された地図情報を保管し，利用者の認証結果に応じて復号に必要な秘密鍵を選択，地図情報を復号する．この際，表示する地図領域に応じて適切な暗号化データを取得し，認証結果から得られた秘密鍵を利用して，利用者ごとに異なる地図表示を行う．また，各地図管理者が利用者ごとにきめ細かな開示設定を行うことによって，屋内地図に適した地図情報配信が可能となる．

2.　地図情報配信システムの基本検討

2.1　エンティティ

本稿では地図情報配信システムの利用者として，以下の三者を考える．

（1）配信（サーバ）側
　（a）地図管理者
　（b）地図配信者
（2）受信・閲覧（クライアント）側
　（a）地図閲覧者

地図管理者は，地図情報管理の主体である．地図管理者は，自身の管理下にある地図の作成や，最新状況に合わせた更新などのメンテナンスを行う．屋外地図を中心とした従来の地図は，適切な対価の下で広く一般に提供される，公開情報であることが多いが，屋内地図には，私的な情報が多く含まれる．そのため，屋内地図では，閲覧可能な利用者（地図閲覧者）を限定すべき情報を含んでいる場合には，どの地図閲覧者がどの情報を閲覧できるかの設定は，地図管理者が行う．たとえば屋内地図において，施設・建物の管理者が地図管理者に相当する．

地図配信者は，各地図管理者が設定した地図情報を集約し，地図閲覧者に提供する主体である．通常，地図閲覧者からの要求を受け，必要な地図情報を取得し，その結果を提供する．地図配信者が提供するサービス自体は，インフラとして，広く一般に提供されることが望ましいが，情報源となる地図情報に屋内地図などの私的な情報が含まれるため，その取扱いには注意が求められる．

地図閲覧者は，地図を閲覧する主体である．地図閲覧者は，現在位置や目的地などの情報を地図配信者に送信し，その結果としての周辺地図などの情報を取得する．地図閲覧者の利用する端末としては，携帯電話などの携帯端末が想定される．なお以下では，地図閲覧者の利用する端末として，携帯電話などのリソースの制限された携帯端末を想定する．そのため，地図閲覧者が閲覧する地図の描画処理などは，極力地図配信者が行うものとする．

2.2　セキュリティ要件の検討

前節で述べた地図情報配信システムの利用者の各役割を考慮すると，セキュリティ要件は以下のようにまとめられる．なお，一般の情報システムに共通的に必要とされる要件（例：

セキュリティパッチを適用する，マルウェア対策ソフトを導入するなど）は含めていない．

要件 1　地図管理者が設定した地図情報へのアクセス制御ポリシ（i.e. どこをだれが閲覧可能か）に従いアクセス制御が実施されること

要件 2　地図配信者が地図管理者によってアクセス制限された地図情報などを知りうる場合，地図配信者は，当該情報の他への漏えいを防止する対策を講じること

2.3　配信制御方針

2.3.1　基 本 方 針

前節のセキュリティ要件を満たすための配信制御方針として，本稿では公開鍵暗号技術を利用する．まず，地図配信者は地図閲覧者ごと（あるいは，地図閲覧者の種別（役割，権限など）ごと）に公開鍵・秘密鍵の組を生成し，公開鍵を地図管理者に配布する．地図管理者は，配布された公開鍵を用いて，地図情報を開示先ごとに暗号化し，その結果（暗号化地図情報）を地図配信者に送付する．地図配信者は，暗号化された状態で地図情報を保管し，地図閲覧者からの要求に応じて，復号に必要な秘密鍵を適切に制御することによって，屋内地図のセキュリティを確保する．

従来技術では，たとえば地図情報を平文の状態でデータベースに保管し，データベースに具備されたアクセス制御機構を用いることが一般的である．すなわち，地図閲覧者が地図配信者にアクセスを行い，地図情報を取得する際，地図配信者は地図閲覧者の種別を判断し，その種別に応じて適切な情報を選択，配信を行う．このようなデータベースのアクセス制御を利用した従来技術では，地図情報は平文の状態で保管されているため，地図配信者は，地図情報を無条件で閲覧することが可能である．そのため，前節の要件 1 を達成するためには，地図配信者は，複数いる地図管理者それぞれの指示に応じ，適切にデータベースのアクセス制御の設定を行うことが必要である．また，要件 2 を達成するためには，その設定が正しく実行されていることを，それぞれの地図管理者に示すことが必要となる．なお，地図配信者が適切なアクセス制御を行っていることを示すための施策としては，たとえば，ログの生成や設定変更の通知などがあげられる．

一方，本稿で述べる暗号化を利用した方式では，地図管理者自身がアクセス制御ポリシを設定し，地図情報を暗号化することでアクセス制御が実現される．そのため，秘密鍵の適切な管理を前提とすれば，地図配信者は地図管理者のアクセス制御ポリシを意識することなく，前節の要件 1 を満たすことができる．

なお，本稿で述べる暗号化を利用した方式では，復号に必要な秘密鍵の地図配信者による適切な管理を前提としている．すなわち，復号に必要な秘密鍵は地図配信者が保管しており，地図配信者は秘密鍵を用いて地図情報を復号することにより，従来技術と同様，地図配信者自身が地図情報を閲覧することが可能である．しかしながら，地図情報そのものが暗号化されているため，要件 2 についても従来技術と比較すれば，達成はより容易であると考える．

2.3.2　基本方針の改良について

本稿では，地図閲覧者が，たとえば携帯電話など，リソースの限られた端末を利用することを想定している．そのため，上記の基本方針の検討では，地図配信者が復号に必要な秘密鍵の管理を行い，復号，および，復号後の地図情報の描画処理を行うことを前提とした．しかしながら，地図閲覧者が利用する端末上で十分なリソースを確保できる場合には，あらかじめ復号に必要な秘密鍵を地図閲覧者に配布し，地図閲覧者が直接復号と地図情報の描画処理を行うことも可能である．この場合には，地図閲覧者からの要求を受けた地図配信者は，地図管理者より取得した暗号化された地図情報の中から，該当する地図情報をそのままの（暗号化されたままの）状態で地図閲覧者に提供する．地図閲覧者は，取得した（暗号化された）地図情報を自身が保持する鍵を使って復号を試み，その結果を閲覧する．これによって，地図配信者が知りうる地図情報は，すべて暗号化されているため，要件 2 を満たすための特別な対策（閲覧者の認証，通信路の暗号化など）は不要となる．すなわち，地図閲覧者が利用する端末で十分なリソースが確保できる場合には，要件をより容易に実現できるという利点がある．

また，本稿では，地図配信者を 1 つのエンティティとして扱っている．しかしながら，本稿で提案する地図情報配信システムでは，地図情報そのものが暗号化されているため，たとえば，地図情報の保管場所として外部のオンラインストレージを用いるなど，地図情報を第三者に預けることも可能である．

3.　暗号技術を用いた地図情報配信システムの提案

3.1　システム構成

前章の配信制御方針による地図情報配信システムを**図 2** に示す．地図情報配信システムの構成は以下のとおりである．

- 地図閲覧端末：地図情報配信サーバにアクセスし，地図の閲覧を行う．なお，本稿では地図閲覧端末として携帯電話を想定する．
- 地図配信サーバ：閲覧端末から閲覧要求を受け取り，地図格納 DB から該当する地図情報の取得，復号，描画処理を行い，地図閲覧端末での閲覧画面を生成する．
- 地図格納 DB：暗号化地図情報を格納する．また，地図配信サーバからの要求に応じて該当する地図情報を地図配信サーバに送付する．

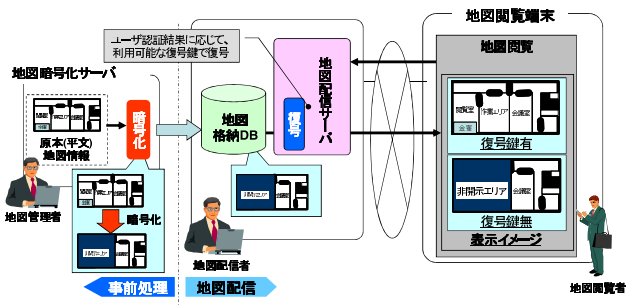


図 2　地図情報配信システム
Fig. 2　Distribution system for map information.

- 地図暗号化サーバ：平文地図情報（原本）に対し開示先の設定を行い，暗号化処理を行う．暗号化結果（暗号化地図情報）を地図格納 DB に格納する．

なお，上記地図格納 DB 内には，地物に関する情報が個別に保管されているものとし，各地物は付随する属性情報（名称など），および，形状情報（ジオメトリ）が格納されているものとする．

上記のうち，地図閲覧者が地図閲覧端末を，また地図配信者が地図配信サーバと地図格納 DB を，また，地図管理者が地図暗号化サーバを利用する．また上記のとおり，地図情報の暗号化，復号はそれぞれ以下で行う．

- 暗号化：地図格納 DB に格納する以前に，地図暗号化サーバ上で暗号化を行う．
- 復号：地図情報配信サーバ上で，地図閲覧者に応じて必要な鍵を取得し，復号する．

なお，復号に使用する秘密鍵は地図閲覧者（あるいは，地図閲覧者の種別）ごとにあらかじめ地図配信サーバ上で生成・格納しておき，地図閲覧者は地図配信サーバへのアクセスに際し，認証処理を行うことによって，地図配信サーバが地図閲覧者の利用可能な秘密鍵を制限する．

3.2　地図情報の暗号化・復号について

3.2.1　地物の暗号化・復号方法

前述のとおり，地図情報には，地物を表現するため，地物に付随する属性情報（名称など）と形状を表すジオメトリが格納されている．本稿では，屋内の地図情報のプライバシエリアの情報を隠蔽するため，地物に関する全情報（すなわち，属性情報，ジオメトリ）を暗号化する方法について述べる．

地図の閲覧に際し，地物の暗号化にかかわる問題は以下の 2 点である．

問題 1　隠蔽領域の適切な地図表示ができなくなる．

問題 2　隠蔽した地物の位置に基づく検索ができなくなる．

上記の問題 1 は，暗号化した地物のデータを地図格納 DB 上から削除した場合に生じる．この場合，地図閲覧者が閲覧を行う際，該当する領域内の暗号化された地物ははじめからないものとして扱われる（地図表示上では，たとえば吹き抜けのように，何もない空間として表示される）．また，問題 2 はジオメトリを暗号化することによって，地物の位置に関する情報も暗号化されることにより生じる．復号時には，地図閲覧者の閲覧要求に応じて，適切な暗号化データを取得し，復号することが必要となる．しかしながら，位置情報が失われることによって，該当する地図情報内に隠蔽した地物があったとしても，復号対象となる暗号化データを取得することが困難となる．

上記を解決するため，本稿では地物の暗号化に際し，以下の処理を施す．

解決策 1　隠蔽領域を墨塗り表示するための仮想地物（墨塗り領域）を生成し，隠蔽領域が非開示時の場合には仮想地物（墨塗り領域）を表示する．

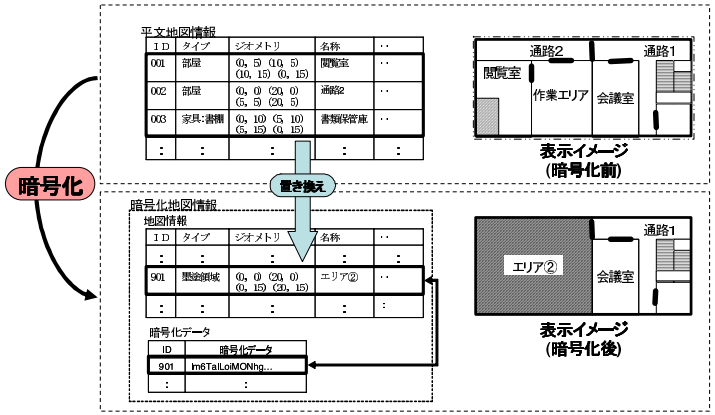
解決策 2　墨塗り領域と暗号化データを関連付けて保管し，表示領域内の隠蔽した地物に対応する暗号化データを取得できるようにする．

上記の解決策 1 によって，問題点 1 が解決できる．また，復号時に，地図閲覧者が閲覧する領域内に隠蔽領域（墨塗り領域）があった場合に，関連付けられた暗号化データを調べることで容易に復号対象となる暗号化データを得ることができる．これによって，問題点 2 が解決できる．以上の暗号化方式の概略を**図 3** (a) に示す．

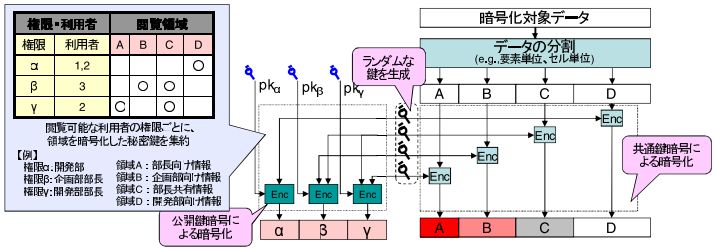
なお，上記では地物そのものを隠蔽化する場合について述べたが，ジオメトリのみ，一部の属性情報のみ，など地物内の一部を隠蔽化することも可能である．その場合には，暗号化した属性情報，ジオメトリを NULL などの事前に定めた値で置き換え，暗号化結果を地物と関連付けて保管すればよい．

3.2.2　地物暗号化のための暗号化方式

本稿では，地図管理者が地物単位で暗号化を行うことにより，地図閲覧者への地図情報の開示制限を行う．一般的な公開鍵暗号を利用して複数の地図閲覧者への開示を許可する場合には，単一の地物をそれぞれの地図閲覧者の公開鍵で個別に暗号化を行うことが必要となり，データサイズなどの観点からは効率が悪い．そのため，たとえば MRES（Multi-Recipient Encryption Scheme）[3),12)] や放送型暗号[5),8)] などの同報通信向けの暗号化方式を用いることが有用となる．



(a) 地図情報の暗号化



(b) 個別データ（地物）の暗号化

図 3　地図情報の暗号化方法
Fig. 3　Encryption method for map information.

本稿では，地物内の属性情報，ジオメトリごとにきめ細かな開示先の設定を行うため XMRES（eXtended Multi-Recipient Encryption Scheme）[11] を用いる．XMRES では，あらかじめデータをブロックに分割したうえで，各ブロックにランダムに生成した共通鍵暗号の共通鍵を用いて暗号化を行い，さらに，生成された共通鍵をアクセス権に応じた適切な地図閲覧者の公開鍵で暗号化する．これによって，ブロックごとに開示先を制限することが実現可能となる．図 3 (b) に XMRES の暗号化処理の概略を示す．なお，本稿では，図 3 (b) 内の A，B などの各ブロックが地物内の属性情報，あるいは，ジオメトリに相当する．

3.3　提案システムの構築

以上の検討結果に基づき，開発した地図情報配信システムの概要を示す．なお，本地図情報配信システムでは，以下を用いて地図配信サーバ，地図格納 DB の構築を行った．

［実装環境］

- GIS サーバ，GIS Web インタフェース：GeoMation(R) 4.0
- データベース：Microsoft(R) SQL Server(TM) 2008 Express Edition
- Web サーバ：Apache Tomcat(TM) 5.5.26
- 実行環境：J2SE(TM) Runtime Environment 5.0 Update 16

(1) 地図暗号化サーバ（暗号化ツール）

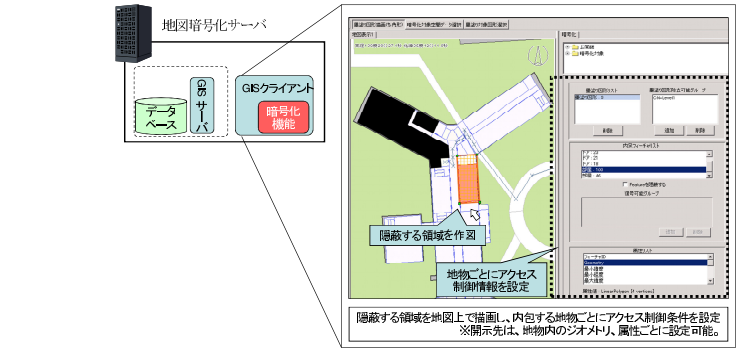
地図暗号化サーバでは，地図閲覧者（あるいは，地図閲覧者の種別）ごとに割り当てられた公開鍵暗号を用いて，地図情報の開示先の設定，および，暗号化を行う．**図 4** (a) に，作成した地図暗号化サーバの概略を示す．図示したように，地図暗号化サーバ上での暗号化は，GIS サーバ内に格納された平文の地図情報を閲覧し，隠蔽化する領域を暗号化ツール（GIS クライアント）上で指定する．暗号化ツールは，指定された領域上に墨塗り領域を生成する．次に，墨塗り領域内に含まれる地物ごとにアクセス制御情報（開示先）の設定を行う．すべての隠蔽領域に対して開示先の設定を終了した後，設定情報に従い，暗号化が実行され，暗号化地図情報が生成される．

(2) 地図情報配信システム（地図配信サーバ，地図格納 DB，地図閲覧端末）

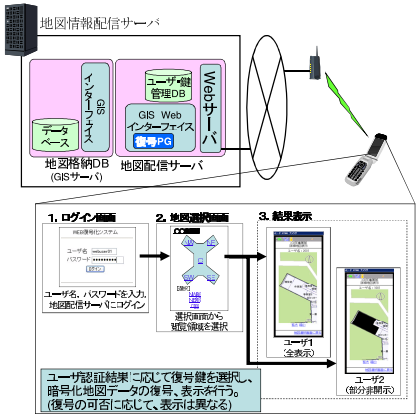
図 4 (b)，(c) に作成した地図情報配信システムと地図情報配信における処理シーケンスの概略を示す．なお，図 4 (b) 内の地図情報配信サーバの地図格納 DB（GIS サーバ）内には，前述の地図情報暗号化サーバで暗号化された暗号化地図情報が格納されている．また，地図配信サーバには，あらかじめ地図閲覧者（あるいは，地図閲覧者の種別）ごとに割り当てられた秘密鍵が格納されている．

地図閲覧者は，携帯電話から地図配信サーバにアクセスを行いユーザ認証を行う．次に地図閲覧者は，建屋の中から地図を閲覧する領域を選択する．地図情報配信サーバは，地図閲覧者からの要求に対し，図 4 (c) の処理シーケンスに従い，描画に必要な地図情報を取得し，さらに前記のユーザ認証結果に基づき必要な秘密鍵を取得し，暗号化データの復号を行う．このとき，ステップ 5 の事前処理として，描画する地図情報の中に墨塗り領域が含まれているか否かを判別する（墨塗り領域が含まれている場合にのみ，ステップ 5 からステップ 8 の処理が行われる）．地図情報配信サーバは，復号後，得られた地図情報から携帯電話に送付する画面を生成し，携帯電話に結果を送付する．

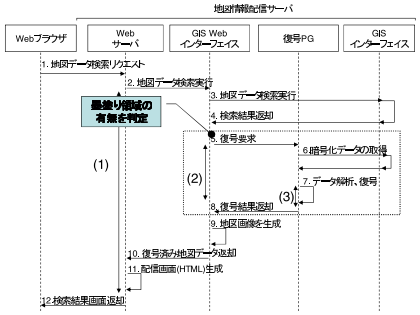
上記の処理において，復号の際，必要な秘密鍵が取得できない場合には，墨塗り領域をそのまま表示し，取得できた場合には，墨塗り領域を削除した後に復号結果を用いて地図の描



(a) 地図暗号化サーバ



(b) 地図情報配信システム



(c) 地図情報配信の処理シーケンス

図 4　開発プログラムの概略
Fig. 4　Development of proposal system.

画を行う．これにより，地図閲覧者ごとに開示される地図が異なる．

4. 実　　験

4.1 開発・実験環境

前章の地図情報配信システムに関し，地図表示に関する実験を行った．なお，実験に利用した環境は，以下のとおりである．また，最終的に送信される地図は携帯端末向けの 31 KB（200 × 400 ピクセル）の JPEG ファイルである．

［実験環境］

- PC：Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00 GHz，1.95 GB RAM
- OS：Microsoft(R) Windows Server(R) 2003 Standard Edition SP2

［暗号アルゴリズム］

- 公開鍵暗号：1024-bit key RSA with OAEP padding [13)]
- 共通鍵暗号：128-bit key AES with CBC mode [6),7)]

表 1　実験結果
Table 1　Experimental result.

(a) 暗号化処理

暗号化対象の平均データサイズ［byte］	処理時間［ミリ秒］
132	20.04

(b) 地図情報配信処理（復号）

	(1)	(2)	(3)
処理時間［ミリ秒］	577.93	287.38	145.28

4.2 実 験 結 果

前章の地図情報配信システムにおいて，地図情報の暗号化処理，および，地図情報配信に関して性能評価を行った．測定結果を**表 1** に示す．ここで，表 1 内の (1)〜(3) は，図 4 (c) の (1)〜(3) に対応する．すなわち

(1)　地図表示のための Web サーバ内での全処理時間．
(2)　復号のために追加された処理の全処理時間．
(3)　(2) のうち復号処理そのものにかかる処理時間．

である．

実験は屋内地図を対象とし，1 フロア（18 部屋）のうち 4 つの部屋を暗号化し，地図配信（復号）では，1 フロア分すべてを表示するのにかかる処理時間を測定した．また，測定は 10 回行い，その平均値を示している．なお，表 1 (a) は，暗号化対象の地物の平均データサイズ，平均処理時間を表し，地図配信（復号）処理は，地物の復号処理にかかる処理時間の合計を示している．本実験により，地物 1 つあたりにかかる暗号化処理時間は，およそ 20 ミリ秒である．また，復号にかかる処理全体 (2) は約 300 ミリ秒，そのうち復号処理そのものの処理時間の合計 (3) は 145 ミリ秒程度であった．なお，同じ地図に対して復号する地物の個数を 16 に増やした場合でも，地図配信全体では 600 ミリ秒，復号にかかる処理全

体 (2) は 300 ミリ秒，また復号そのものの処理時間の合計 (3) は 170 ミリ秒であった．これは，復号にかかる処理では，データの復号そのものの処理ではなく，ステップ 6 の暗号化データ取得のためのデータベースへの接続やステップ 7 内の復号鍵の取得などがオーバヘッドとなっているためである．

上記の実験において，実際に携帯電話[⋆1]から携帯電話回線を用い地図データ検索リクエストから地図表示が完了するまでの平均時間を測定したところ，8.8 秒という結果を得た．

4.3 考　　察

暗号化処理は，開示先の設定変更が行われた場合に，対象となる地物のみを再暗号化すればよいが，復号処理は地図閲覧者からの要求ごとに処理を行う必要がある．そのため，以下では，復号処理に関し考察を行う．

実験結果より，地図配信全体で 600 ミリ秒に対し，復号にかかる処理全体が 300 ミリ秒であるため，復号処理にかかる割合が大きい．しかしながら，復号する地物の数を 4 から 16 に増やした場合でも，復号にかかる処理全体 (2) の処理時間が 300 ミリ秒程度であり，復号する地物の個数の増加による復号にかかる処理時間の増加は少ないことが分かる．また，本実験では，携帯電話上での地図表示全体に対し，サーバでの処理そのものが占める割合は小さいことから，実験システムは有効であると考える．

5. システム拡張性の検討

実験システムでは，地図閲覧者に規定の領域を選択させ，該当する地図情報を地図格納 DB から取得し，地図閲覧者に応じた復号処理を行い，その結果を配信する．しかしながら，一般的な地理情報システムでは，キーワード検索機能や経路探索機能がサポートされていることが一般的である．したがって，より高機能な地図情報配信システムの構築にあたっては，これらの機能への対応が不可欠である．以下に，これらの機能への対応方法に関する検討結果を述べる．

5.1 キーワード検索機能への対応

キーワード検索機能を実現するための 1 つの方法としては，検索機能付き暗号[1] を利用することである．検索機能付き暗号では，あらかじめ指定したキーワードに対して，暗号化された状態のまま検索を行うことが可能である．キーワード検索機能は，たとえば部屋名称など，地物の属性情報に対して実行される．したがって，本提案システムでは，属性情報の暗号化に，汎用的な暗号化方式の代わりに検索機能付き暗号を利用すればよい．

また，汎用的な暗号化方式で上記のキーワード検索機能を実現するためには，たとえば以下のようにする．まず，利用者（あるいは，利用者種別ごと）に検索に利用するキーワードと地物の座標を関連付けたキーワードリストを作成し，これを公開鍵暗号を用いて暗号化する．利用者がキーワード検索を実行する場合には，上記の暗号化されたキーワードリストを復号，キーワード検索を実行し，得られた座標情報をもとに地図を表示する．以上のように利用者ごとにキーワードリストを作成することによって，利用者ごとに検索可能なキーワードを制限することが可能となる．

5.2 経路探索機能への対応

経路探索機能はラベル付きの有向グラフを用いて行われる．グラフを構成する各ノードは地図上の座標と対応付けて管理され，さらに地図上の移動可能な経路をノード間のリンクを用いて表現する．また，経路間の距離，あるいは，移動に要する時間や料金をリンクのラベル（以下，コストと呼ぶ）によって表現する．一般的な経路探索では，上記の有向グラフを用いて，出発地から目的地までの経路をダイクストラ法に基づき，最短経路を探索する[4),10)]．ダイクストラ法[4)] の中核処理は，起点ノードに隣接する全ノードに対し，出発地ノードからの合計コストを算出し，隣接ノードまでのコストが最小となる経路を評価することである．ダイクストラ法は，この中核処理を出発地ノードから開始し，目的地ノードまで繰り返すことによって，出発地から目的地への最小経路を探索する幅優先アルゴリズムである．

一般的に経路探索用データを暗号化する場合には，その周辺の地図は非開示領域であることが想定される．3 章で述べた地図情報の暗号化では，非開示領域に対して仮想地物（墨塗り領域）を生成し，非開示領域内の地物に関する暗号化データを墨塗り領域に関連付けて管理した．これにより，表示領域内の墨塗り領域の有無を調べることによって，閲覧権限のある利用者に対して，墨塗り領域を開示した地図を提供することが可能となる．

経路探索用データも同様にして，暗号化対象となったノードやリンクを墨塗り領域と関連付けて管理することによって，利用者に応じて適切な経路探索用データを用いて経路探索を行うことが可能である．すなわち，事前に経路探索範囲が自明である場合，探索範囲内の墨塗り領域の有無を調べ，墨塗り領域がある場合には，対応する暗号化された経路探索用データを取得し，復号する．これにより，暗号化に対応した経路探索処理が可能となる．また，墨塗り領域と関連付けることによって，出発地や目的地を座標情報から指定することも可能となる．しかしながら，探索範囲が明示的に与えられない場合には，上記の方法は適用でき

⋆1 FOMA(R) 用携帯電話 N-06A（日本電気株式会社製）を利用した．

ない．また，探索領域が大きい場合には，探索不要な経路探索用データを復号する必要が生じるため効率が悪くなる．そこで以下では，暗号化された経路探索用データを用いて経路探索を行う方法を述べる．

経路探索の基本処理では，起点ノードから隣接ノードを探索し，そのコストを評価する．そこで，以下のようにすることによって暗号化に対応した経路探索機能を実現する．まず，暗号化対象となるノードに接続されたリンクから隣接ノードを取得する．次に，隣接ノードに，経路探索用データが暗号化されていることを示すフラグ（以下，暗号化フラグと呼ぶ）を設定する．最後に，暗号化対象となるノードと暗号化対象のノードに接続されたリンクを暗号化し，経路探索用データから削除，暗号化データを前記の隣接ノードと関連付けて保管する．これによって，経路探索の中核処理における隣接ノードの探索時に暗号化フラグを調べることで，隣接ノード内に暗号化された経路探索用データの有無を知ることが可能となる．

経路探索時には，始点ノード内に暗号化フラグが設定されている場合，関連付けられた暗号化データを取得，復号する．暗号化データが復号できた場合には，復号結果を用いて経路探索用データの復元を行い，復元結果を含めた経路探索処理を継続する．復号できなかった場合には，暗号化された経路探索用データがなかった場合と同様に，従来の開示状態の経路探索用データのみを用いた経路探索を実施することができる．**図 5** に経路探索用データの暗号化方法の概略を示す．また，**図 6** (a) にダイクストラ法の処理フローを示し，図 6 (b) にダイクストラ法への復号処理の適用方法を示す．なお，図 6 (a) はダイクストラ法の概略であり，図 6 点線内がダイクストラ法の中核処理となっている．また，図 6 (b) の破線内が復号処理適用のために追加した処理である．

6. ま と め

屋内の地図情報には，たとえば金庫などの機密領域など，地図そのものにプライバシや機密情報が含まれる．また，1 つの施設・建物に複数の管理者が存在することが想定される．本稿では，暗号化を用いることによって，屋内地図にかかわる機密情報，プライバシを保護する地図情報配信システムを提案し，地図情報の暗号化・復号方法を示した．また，地図表示方法について実験結果を示し，さらにキーワード検索や経路探索機能への対応方法について示した．暗号技術を用いることによって，各地図情報の管理者の意思を適切に反映した地図情報の開示制御が可能となる．

キーワード検索，経路探索機能の実現，および，実サービスにおける処理性能の妥当性検

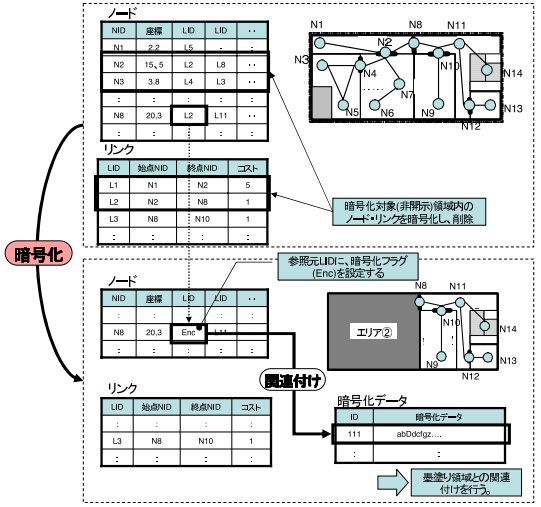
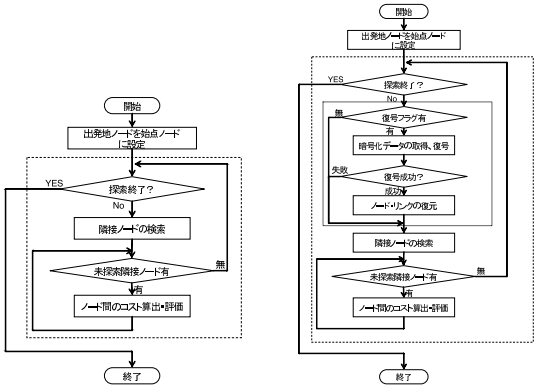


図 5　経路探索用データの暗号化
Fig. 5　Encryption for route search data.



(a) 経路探索処理の概要　　(b) 経路探索処理への復号処理の適用

図 6　経路探索用データの復号
Fig. 6　Decryption for route search data.

証は今後の課題である．

謝辞　本研究は，平成 21 年度総務省委託研究「ユビキタス・プラットフォーム技術の研究開発（ユビキタス空間情報基盤技術の研究開発）」の研究成果の一部です．

参 考 文 献

1) Abdalla, M., Bellare, M., Catalano, D., Kiltz, E., Kohno, T., Lange, T., Malone-Lee, J., Neven, G., Paillier, P. and Shi, H.: Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions, *Advances in Cryptology – CRYPTO 2005*, Lecture Notes in Computer Science, Vol.3621 (LNCS 3621), pp.205–222 (2005).
2) An, N., Chatterjee, R., Horhammer, M. and Ravada, S.: Securely Implementing Open Geospatial Consortium Web Service Interface Standards in Oracle Spatial, *Proc. 18th International Conference on World Wide Web*, pp.1179–1180 (2009).
3) Bellare, M., Boldyreva, A. and Staddon, J.: Multi-Recipient Encryption Schemes: Security Notions and Randomness Re-Use, available form http://www-cse.ucsd.edu/˜mihir/papers/bbs.html (2003).
4) Dijkstra, E.W.: A note on two problems in connexion with graphs, *Numerische Mathematik*, Vol.1, pp.269–271 (1959).
5) Dodis, Y. and Fazio, N.: Public-Key Broadcast Encryption for Stateless Receivers, *ACM Workshop in Digital Rights Management* (*DRM 2002*), LNCS 2696, pp.61–80 (2003).
6) Federal Information National Institute of Standards and Technology (NIST): Specification for the Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197 (FIPS-197) (Nov. 2001).
7) Federal Information National Institute of Standards and Technology (NIST): Recommendation for Block Cipher Modes of Operation: Methods and Techniques, NIST Special Publication 800-38A (Nov. 2001).
8) Fiat, A. and Naor, M.: Broadcast Encryption, *Advanced in Cryptology*: *CRYPTO'93*, LNCS 773, pp.480–491 (1993).
9) Gabillon, A. and Capolsini, P.: DRM policies for Web Map Service, *Proc. SIGSPATIAL ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS*, pp.20–29 (2008).
10) Hart, P.E., Nilsson, N.J. and Raphael, B.: A Formal Basis for the Heuristic Determination of Minimum Cost Paths, *IEEE Trans. Systems Science and Cybernetics*, Vol.4, No.2, pp.100–107 (1968).
11) Hatano, Y., Miyazaki, K. and Kaneko, T.: A Study on Multi-Resipient Encryption for Selective Disclosure, *Proc. 2009 International Conference on Security & Management* (*SAM 2009*), Vol.II, pp.570–575 (2009).
12) Kurosawa, K.: Multi-Recipient Public-Key Encryption with Shortened Ciphertext, *Public Key Cryptography – PKC'02*, pp.48–63, Springer-Verlag (2002).
13) RSA Laboratories: PKCS #1: RSA Cryptography Standard, Public-Key Cryptography Standards (PKCS) (2002).

(平成 22 年 5 月 14 日受付)
(平成 22 年 11 月 5 日採録)

秦野　康生

2004 年東京理科大学大学院理工学研究科修士課程修了．同年（株）日立製作所入社．同社システム開発研究所にて，暗号，情報セキュリティの研究に従事．2010 年東京理科大学大学院理工学研究科博士課程修了．博士（工学）．2002 年暗号と情報セキュリティシンポジウム（SCIS2002）論文賞受賞．電子情報通信学会会員．

宮崎　邦彦（正会員）

1998 年東京大学大学院数理科学研究科修士課程修了．同年（株）日立製作所入社．現在に至るまで，同社システム開発研究所にて，暗号，情報セキュリティの研究に従事．2006 年東京大学大学院情報理工学系研究科博士課程修了．博士（情報理工学）．2004 年暗号と情報セキュリティシンポジウム（SCIS2004）論文賞受賞．電子情報通信学会会員．

鈴木　邦康

1992 年（株）日立アドバンストシステムズ入社，入社より伝送装置および情報通信システムの開発に携わり，現在，暗号・情報セキュリティの研究に従事．

高橋　由泰（正会員）

2001 年東京大学大学院工学系研究科電子情報工学専攻博士課程単位取得中退．東京大学先端科学技術研究センター協力研究員を経て，2003 年（株）日立製作所入社．現在，同社システム開発研究所所属．主にセキュリティ，著作権保護，電子透かし，およびその応用技術に関する研究に従事．博士（工学）．電子情報通信学会会員．

山田　隆亮（正会員）

1988 年京都大学工学部資源工学科卒業．同年（株）日立製作所に入社．大森ソフトウェア工場を経て，現在，システム開発研究所第 7 部主任研究員．マルチメディア応用，空間情報システム，情報セキュリティシステムの研究に従事．情報処理学会論文賞（2005 年）．博士（情報科学）．

本多　義則

1991 年九州大学大学院工学研究科修士課程修了．同年（株）日立製作所入社．同社システム開発研究所にて，情報セキュリティの研究開発に従事．