第２０１４-１２号

属性ベース暗号による建設業務のセキュアな情報共有の実現のための研究

株式会社アーク情報システム　ITソリューション部
技師　半田　沙里

平成２７年１１月

平成２６年度
（一財）日本建設情報総合センター
研究助成事業

報告書

研究テーマ
「属性ベース暗号による建設業務の
セキュアな情報共有の実現のための研究」

平成 27 年 8 月 31 日

株式会社アーク情報システム　半田 沙里

研究関係者紹介

■助成研究者紹介　半田（はんだ）　沙里（さり）

■現職：株式会社　アーク情報システム　ＩＴソリューション部　技師

■主な著書

・Two Applications of Multilinear Maps: Group Key Exchange and Witness Encryption Seiko Arita、 Sari Handa、 ASIAPKC 2014/6.

・Seiko Arita、 Sari Handa、 Applications of Multilinear Maps、 2014 年暗号と情報セキュリティシンポジウム、 SCIS 2014、 2E3-1、 2014/1.

・Hiroaki Anada、 Seiko Arita、 Sari Handa、 Yosuke Iwabuchi、 Attribute-Based Identification: Definitions and Efficient Constructions、ACISP 2013、LNCS 7959、pp. 168-186、 2013.

目次

1　研究の背景と目的

建設業では IT の積極的な利用が広まっている。社内だけでなく工事現場でも様々な方面で IT 化が進み、タブレットでの図面の確認や写真の撮影といった PC のシステムから、Web カメラによる監視や IC タグによる入退場管理といった機器まで幅広く IT が活用されている。現場で利用するシステムは、社内や顧客と情報をやりとりするためクラウドのシステムが多く利用されている。
生産性の向上や競争力強化のため、今後も IT 活用は重要になっていくが、顧客情報や設計情報/技術情報のような機密情報を扱うため、十分に安全性を確保する必要がある。

建設業協会はこのような状況を鑑み、建設業特有の生産拠点である建設現場に焦点をあてて、「建設現場における情報セキュリティガイドライン」[1]を発行している。
その中では、インターネットの普及やファイル共有ソフトに介在するウイルス、記録媒体の大容量化により情報漏洩のリスクが増大していて、IT の有効活用には情報セキュリティ対策が必要だが、建設現場固有の要因により情報セキュリティ対策が現場従業員に負担になっていると述べている。

[建設現場固有の要因]
①生産物が単品・個別生産のため作業やルールが標準化しにくい。
②建設現場は工事期間という有期の利用の仮設仕様であるため IT 設備が簡易
③大きな費用をかけられない
④建設現場には元請施工者だけでなく、発注者や設計者、協力会社、資機材メーカー担当者など、多くの関係者が出入りするうえ、工事の進捗状況により関係者が入れ替わるため、情報漏洩のリスクが大きく、情報セキュリティ教育の浸透に手間がかかる
⑤図面や書類等は変更の連続で、原本や最新版の管理の負担が大きい

情報共有に関しては、共有サーバへのアクセスを必要最低限の担当者に限定すべきとし、限定する対策例として、ユーザを会社別・役職別などのグループに分け、「参照」「登録」「変更」「削除」のうち必要な権限のみを付与することを挙げている。また、ユーザの異動や退職、契約終了時にはユーザ ID やアクセス権の変更・削除を速やかに行うこととしている。

建設業協会は、上記④のように協力会社の範囲が広く、施工体制も複層化していることから、ガイドラインの「協力会社編」[2]も発行していて、そのガイドラインでは守るべき情報をまとめ、情報漏洩に対する具体的な対策を示している。

[守るべき情報]
（１）図面、工程表、写真、打ち合わせ記録
（２）発注者、近隣、工事関係者の個人情報
（３）建物の内部や設備の情報（写真等）
（４）工事の技術やノウハウ
（５）関係各社の管理情報

建設業協会発行の「建設現場ネットワークの構築と運用ガイドライン」[3]には外部関係者との情報共有について記載があり、発注者や外部関係者との情報共有にはクラウド等の外部サービスの利用を基本とするとしている。外部サービス選定の際には、データの機密性（ユーザー認証方式、通信とデータの暗号化、アクセス権の設定等）を十分考慮する必要があると述べている。

上記の建設現場固有の課題およびアクセスコントロールによる対策を踏まえ、本研究では、「属性ベース暗号」というアクセスコントロール機能を持つ暗号方式が様々な人が機密情報にアクセスする建設の情報共有の安全性向上に適していると考え、属性ベース暗号をどのように建設業務に利用できるかを研究することにした。そして属性ベース暗号を用いた情報共有のシステムについても研究した。

建設業務の情報共有システムについては、下記の情報を参考にした。

[機能要件]
国土交通省「工事施工中における受発注者間の情報共有システム機能要件　(Rev.4.0)」[4]
情報セキュリティに関する要件で以下を挙げている。
・帳票およびその添付資料と、発議書の保存履歴は、データが不当に消去、改ざんされないように、アクセス制御が実施されること。

[アクセス制御]
アクセス制御の詳細は、国土交通省「土木工事の情報共有システム活用ガイドライン」[5]の中で、工事帳票など資料の種類と、その資料の利用対象者および権限（”登録・変更・閲覧可”と”閲覧のみ”）が定義されている。

2　研究方法

[step1] 建設業務におけるセキュリティ課題と情報共有システムの要件の調査
はじめに、建設業の IT 化、情報共有、情報セキュリティの状況をガイドラインなどで調べ、情報セキュリティの課題を洗い出した。次に情報共有システムのセキュリティ要件を調査した。

[step2] 属性ベース暗号の活用の研究
暗号については、まず属性ベース暗号のタイプごとにできることを考えて整理した。そして、はじめに洗い出したセキュリティの課題と情報共有システムのセキュリティ要件を念頭に置き、属性ベース暗号の建設業務での活用方法を５つ（暗号文ポリシー属性ベース暗号の活用４つ、鍵ポリシー属性ベース暗号１つ）考え出した。

[step3] 属性ベース暗号の活用方法のシステム化検討
前 step で考えた活用方法をシステム化できるか調べるために、オープンソースの暗号ライブラリを調査して秘密分散の属性ベース暗号ライブラリを使うことにした。そのライブラリを組み込んでいる情報共有システムに対して拡張開発を行い、建設業務向け活用方法をシステムに実現した。そして、安全性の考察と性能の評価を行った。

3　暗号方式について

暗号方式について説明する。

(1)　一般的な暗号方式

データの暗号化には、共通鍵暗号や公開鍵暗号がよく使われる。共通鍵暗号は暗号化と復号を同じ鍵で行う暗号方式で、公開鍵暗号は、データの受信者が秘密鍵と公開鍵のペアを作成して公開鍵を公開し、送信者が公開鍵を使用してデータを暗号化して復号者が秘密鍵で復号する方式である。

共通鍵暗号は共通鍵を送信者と受信者がセキュアに共有する必要があるので、送信者が公開鍵暗号で鍵を暗号化して受信者に送るというように、データは計算コストの低い共通鍵暗号で暗号化し、その共通鍵を公開鍵暗号方式で共有するハイブリッド方式が採用されることが多い。

公開鍵暗号方式は受信者の公開鍵で暗号化するため、複数の人に同じ情報を送りたい場合でも、受信者それぞれの公開鍵で暗号化する必要があり手間がかかる。

(2)　属性ベース暗号

属性ベース暗号は公開鍵暗号の一つで、複数の人に同じ情報を送りたいときに暗号文が一つで済むので、組織など複数の人の間での情報共有に向いている暗号方式である。

“属性”とは、部署や役職、名前、年齢のようなユーザ属性で、属性ベース暗号は、暗号化の時に、”営業部 AND 部長” のように復号条件（以下、復号ポリシー）を指定できる暗号方式である。ユーザは、自身の属性をもとに秘密鍵を作り、暗号文を復号する。その際、秘密鍵内のユーザ属性が復号ポリシーを満たしていれば暗号文を復号でき、満たしていなければ復号に失敗する。

このように暗号文に復号ポリシーを設定する属性ベース暗号は、「暗号文ポリシー型」と呼ばれ、逆に暗号文にデータ属性がセットされて、ユーザが持つ秘密鍵に復号ポリシーがセットされるタイプの属性ベース暗号は、「鍵ポリシー型」と呼ばれる。

下表に、暗号文ポリシー属性ベース暗号と鍵ポリシー属性ベース暗号を整理する。

	暗号文ポリシー属性ベース暗号	鍵ポリシー属性ベース暗号
復号ポリシーに用いる属性	復号者の属性	データの属性
セットアップ	公開パラメタとマスタ秘密鍵を生成	公開パラメタとマスタ秘密鍵を生成
暗号化	復号ポリシーと公開パラメタを用	データの属性と公開パラメタを用い

	いて、平文を暗号化する。	て、平文を暗号化する。
秘密鍵の生成	復号者の属性とマスタ秘密鍵から秘密鍵を生成	復号ポリシーと公開パラメタ、およびマスタ秘密鍵から秘密鍵を生成。作られた秘密鍵は、任意の方法で復号者に渡す
復号	秘密鍵と公開パラメタを用いて暗号文を復号する。秘密鍵内の復号者の属性が、暗号文内の復号ポリシーを満たす場合のみ復号できる。	秘密鍵と公開パラメタを用いて暗号文を復号する。暗号文内の属性が、秘密鍵内のポリシーを満たす場合のみ復号できる。

4 章と 5 章で、暗号文ポリシー属性ベース暗号と鍵ポリシー属性ベース暗号の一般的な利用方法を述べ、建設への活用方法を示す。活用方法は、以下のような Web システムを想定して説明する。サーバに鍵生成/暗号化/復号のエンジンが実装されていて、PC またはモバイルのクライアント端末が復号したいファイルを選択してリクエストをサーバに送信すると、サーバが保持しているファイルを復号してクライアントに返す。通信は HTTPS で保護されている想定である。

4　暗号文ポリシー属性ベース暗号の活用方法の研究

(1)　一般的な利用方法

暗号文ポリシー属性ベース暗号は、データに復号ポリシーが設定され、復号者の属性がそのポリシーを満たすと復号できる暗号方式である。この特性を利用して、データへのアクセス制御を実現できる。アクセス制御の活用を a)から d)の 4 つ提案する。

(2)　建設業務への適用

a) ワークフロー

建設の業務では、契約書や仕様書についての協議や報告の書類が発議され、ワークフロー（承認序列）に沿って該当者に回されて承認や差し戻しが行われ、決裁者が最終承認により決裁する。「承認依頼された人は書類を見られる」というアクセス制御を、承認後に復号ポリシーに次の承認者を加えるという操作により実現できる。
ワークフローを個人ではなく部署や役職等の属性で表すと、該当者が異動で不在になってもワークフローを変更する必要がなく利便性が向上する。

請求書の承認フローの例
承認序列：担当営業　⇒　営業部長　⇒　発注者

[暗号文内の復号ポリシー]
担当営業の承認前：
(営業部 AND 顧客 1 担当)
担当営業の承認後：
(営業部　AND　顧客 1 担当) OR (営業部　AND 部長)
営業部長の承認後：
(営業部 AND 顧客 1 担当) OR (営業部 AND　部長) OR 顧客番号 1

[復号者の属性]
社員 A：営業部、顧客 1 担当
社員 B：営業部、部長
顧客 1：顧客番号 1

b) 復号可能期間の制限

建築や土木の工事には多くの段階があり関係会社も多い。そして工事が進むに従って関係者が入れ替わるという特性がある。ユーザが自身の担当フェーズを終えた後も情報にアクセスできる状態にしておくと不正利用や情報漏洩の怖れがあるため、ユーザが情報にアクセス可能な期間を制限する必要がある。
復号ポリシーに復号可能な期間を指定することにより制御を行う。ユーザは、復号可能期間が指定された暗号化ファイルを期間内のみ復号でき、期間外は復号できない。

[暗号文内の復号ポリシー]
内装会社 A　AND
（ 現在日 >= 20150102　AND　現在日<= 20150304 ）

[復号者の属性]
現在日=20150102、所属=内装会社 A
復号時に、サーバがシステム日付をユーザ属性に追加する。

c) 位置情報によるエリア制限

近年は、現場にタブレットなどのモバイル端末を持ち込み、情報を参照したり入力したりするケースが増えている。モバイルから得られる GPS の緯度/経度を利用して、指定したエリア内にある端末のみが暗号化された情報を復号できるように制限することで、原子力発電所の作業など機密性の高い情報を扱う場合に、そこでだけ情報にアクセスできるように制御する。
暗号化時に、復号ポリシーに現場の緯度の範囲と経度の範囲を指定する。ユーザが復号しようとした時にモバイル端末の緯度経度を取得して、指定されたエリア内なら暗号化された情報を復号できる。

[暗号文内の復号ポリシー]
(緯度 >= 35.681000　AND　緯度<= 35.682000)
AND
(経度>= 139.766000　AND　経度<= 139.767000)

[復号者の属性]
緯度= 35.681382
経度= 139.766084
復号時に、モバイルのアプリケーションが GPS の緯度/経度をサーバに送り、サーバが属性にセットする。

d) 接続元を制御

建設の業務では工事の現場や関連企業など複数の場所から情報にアクセスするためクラウドの情報共有システムが便利である。しかし、自宅などからシステムにアクセスして情報を入手できてしまうと不正利用される危険が高まり、また、その個人端末にセキュリティ対策がなされていなかったりファイル共有ソフトが入っていたりすると情報漏洩の危険もある。

情報にアクセスする端末の IP アドレスを復号ポリシーに指定することによりアクセス元を制限できる。例えば、復号ポリシーに現場事務所や自社、関連企業のネットワークのグローバル IP アドレスを設定しておけば、指定されたネットワーク内の業務端末は暗号化された情報を復号できるが、自宅など指定外のネットワークの端末では復号できず、情報の不正利用や情報漏洩を防ぐことができる。

[暗号文内の復号ポリシー]

IP アドレス = 192168001002

[復号者の属性]

IP アドレス=192.168.001.002

サーバはリクエストのヘッダから送信元の IP アドレスを取得し、属性にセットする。

5　鍵ポリシー属性ベース暗号の活用方法の研究

(1)　一般的な暗号方式

鍵ポリシー属性ベース暗号は、復号ポリシーがデータの属性で表現されるので、データのフィルタリングとして利用できる。フィルタリングの条件が含まれている秘密鍵を復号者に渡す方法は任意であるため、データのアクセスを制御するオーナーの存在を想定し、オーナーは広い範囲を復号できる鍵を高価、狭い範囲しか復号できない鍵は安価というようにレベルを付けて鍵を販売する利用モデルが考えられる。このモデルは、映画や音楽などのコンテンツ配信に応用できる。

(2)　建設業務への適用

a) センサー測定値の配信制御

近年構造物の老朽化が問題となっていて、構造物にセンサーを取り付けて計測値を収集する技術が開発されている。ここでは、センサーから収集した計測値を利用者に提供するケースを考える。

計測会社はセンサーの計測値を無線センサーネットワーク(WSN)で収集するが、WSN は悪意のあるセンサーノードがネットワークに介入しやすく、情報漏洩やデータの改ざんの脅威が存在するため、通信するデータは暗号化されていることが望ましい。各センサーノードは計測値を暗号化する時に、データの属性を暗号文にセットする。計測会社は、それらの属性を組み合わせて様々な復号ポリシーを構成し、その復号ポリシーの秘密鍵を生成して計測値を希望するユーザに配布または販売する。秘密鍵を受け取ったユーザは、復号ポリシーでフィルタリングされた計測値のみを知ることができる。

[秘密鍵内の復号ポリシー]
(計測日 >= 20150101 AND　計測日<= 20150131)
AND
構造物=橋梁

[データの属性]
構造物=橋梁、計測種別=歪み、センサーID=12345、計測日=2015/01/02

6　提案方法のシステム化検証

提案した建設業務への属性ベース暗号の活用方法を情報共有システムに実現する方法を検討した。暗号のプログラムと情報共有プログラムをゼロから作るのではなくオープンソースの既存のプログラムを利用することで、開発コストを抑え、品質も確保することができる。そこで、オープンソースの属性ベース暗号のプログラムを調査した。

(1)　属性ベース暗号のライブラリの調査

属性ベース暗号は、復号ポリシーに指定できる制約が色々あり、例えば NOT 条件が使えたり使えなかったり、属性数に制限がある方式/ない方式が存在する。安全性を高めた方式や機能を追加した方式もあり、多様な方式が提案されている。暗号の構成に用いる部品もペアリングと呼ばれる双線形写像も用いるものや格子暗号ベースのものがある。それらの方式の中には実装プログラムを提供しているものもあるので、求める用途や安全性に合ったライブラリを利用するとよい。ここでは、オープンソースの属性ベース暗号のライブラリを４つ紹介する。

a) 秘密分散を利用した属性ベース暗号

【Ciphertext-Policy Attribute-Based Encryption】[7]

秘密分散の代表的な方法である「(k,n)閾値秘密分散法」を説明する。(k,n)閾値秘密分散法は多くの属性ベース暗号で利用されている仕組みである。

秘密分散法は、ある秘密の値をツリー構造に沿ってツリーのルートからリーフに分散させる手法である。(k,n)閾値秘密分散法は、ツリーの各ノードに閾値の条件（分散させる数：n と復元に必要な数：k）を設定する。各ノードで、閾値の個数以上の分散値を持っていると親ノードの値を計算できる。リーフに分散した値をツリーの各ノードに設定された閾値を満たす個数持っていれば、リーフからルートまで計算することができ、ルートの秘密の値を復元できる。

属性ベース暗号では、まず復号ポリシーを論理ツリーの形で表現する。復号ポリシーの AND/OR が論理ツリーのノード、復号ポリシーの属性が論理ツリーのリーフである。暗号化処理で、秘密の値をツリーのルートからリーフに分散させ、リーフに分散された値を暗号文に含める。復号時は、秘密鍵に復号者が持つ属性から計算された値が含まれていて、その値と暗号文内のリーフに分散された値を用いて論理ツリーをリーフからルートに向かって辿る。秘密鍵内の復号者の属性が論理ツリーの条件を満たす場合のみ、ツリーをルートまで辿ることができ、ルートに設定された秘密の値を復元できる。そして、それをもとに暗号文を平文に復号できる。

Ciphertext-Policy Attribute-Based Encryption は、属性ベース暗号研究の初期に提案された(k,n)閾値秘密分散法を利用した暗号文ポリシー属性ベース暗号で、ベーシックな方式であり他の多くの属性ベース暗号のベースとなっている。

[開発元]　John Bethencourt, Amit Sahai, Brent Waters
http://acsc.cs.utexas.edu/cpabe/
[言語] C 言語
[ライセンス] GPL

b) 内積による述語暗号

【Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption】[8]
暗号文ポリシー属性ベース暗号における暗号文内の復号ポリシーや、鍵ポリシー属性ベース暗号における暗号文内のデータ属性は、秘密情報ではなく暗号文から分かる情報である。これらを知られたくない場合に使える暗号として「述語暗号」が考えられた。述語暗号は、暗号文内のパラメタ x と秘密鍵内のパラメタ v が定められた関係 R を満たす、つまり R(x、v)=true となる場合のみ復号できる暗号方式である。本ライブラリは関係 R に"内積"を使用した鍵ポリシー属性ベース暗号である。以下に詳細を述べる。
送信者はデータを暗号化する時にデータの属性をベクトル x として暗号文に埋め込む。このとき、暗号文からは x の値が分からないようにする。復号者が持つ秘密鍵には復号ポリシーのベクトル v が埋め込まれていて、復号者は、暗号文と秘密鍵が "x と v の内積が 0" という関係 R を満たしている場合のみ平文に戻すことができる。復号ポリシーベクトル v には AND、OR 論理式を設定できる。
この方式は鍵ポリシー属性ベース暗号のため、建設業務への活用方法の鍵ポリシー型の提案（センサー測定値の配信制御）の実現に利用できる。この方式を使えば暗号文である測定値に設定する属性を隠すことができる。

[開発元]　JPBC (The Java Pairing-Based Cryptography Library)
http://gas.dia.unisa.it/projects/jpbc/
[言語] Java
[ライセンス] LGPL

※JPBC の補足
2000 年以降、ID ベース暗号や属性ベース暗号、関数型暗号などの機能を持った暗号が盛んに研究されている。それらの暗号はペアリングと呼ばれる楕円曲線上の 2 点から有限体への双線形写像が考えられたことにより構成可能になった。暗号は C 言語で実装されること

が多く、ペアリングの部分は C 言語のフリーライブラリ「PBC (Pairing-Based Cryptography)」がよく使われる。JPBC は PBC の Java 実装であり、ペアリングを用いた暗号方式や格子ベースの暗号方式の実装も提供されている。

c) 格子ベースの多重線形写像で構成された回路で表現する属性ベース暗号

【Attribute-Based Encryption for Circuits from Multilinear Maps】[9]

復号ポリシーを論理ツリーではなく AND/OR ゲートを用いた回路で表現できる属性ベース暗号である。暗号の構成要素に従来のペアリングではなく、より安全性の高い格子暗号ベースの多重線形写像を採用している。

暗号文ポリシー属性ベース暗号と鍵ポリシー属性ベース暗号の両方の実装がある。

[開発元]　JPBC (The Java Pairing-Based Cryptography Library)

http://gas.dia.unisa.it/projects/jpbc/

[言語] Java

[ライセンス] LGPL

d) 複数のドメインが管理する属性を使用できる属性ベース暗号

【Decentralizing Attribute-Based Encryption】[10]

従来の属性ベース暗号では、扱う属性は一つのドメインが管理している属性だが、本ライブラリの属性ベース暗号方式では複数のドメインが管理する属性を使用することができる。この属性ベース暗号は暗号文ポリシー型で、ユーザは別々のドメインが発行した属性を持つことができ、復号ポリシーにも別々のドメインが発行した属性を混在させられる。

各ドメインは、復号者に付与する属性を決め、それらの属性からその復号者の秘密鍵を生成する。復号者は複数のドメインから秘密鍵を受け取り、それらの秘密鍵で暗号文を復号する。

[開発元]　Charm (暗号プログラムを手早く実装ためのフレームワーク)

http://charm-crypto.com/index.html

[言語] Python

[ライセンス] LGPL

(2)　属性ベース暗号のシステム

本研究では、ベーシックな属性ベース暗号方式であり復号ポリシーを数字の範囲で指定できる 【Ciphertext-Policy Attribute-Based Encryption】ライブラリを採用して、提案した暗号文ポリシー属性ベース暗号の活用方法 a)～d)をシステムで実現できるかの検証およびシステム化するにあたり考慮すべきことの検討を行った。(以降、このライブラリを BSW CP-ABE ライブラリと呼ぶ)

BSW CP-ABE ライブラリは、情報セキュリティ大学院大学が 2011 年に文部科学省の支援を受けて実施した属性ベース暗号を用いた情報共有の研究開発「暗号技術の導入による機密情報の適切な保護方式の研究～グローバル社会における持続的な経済発展のための基盤技術として～」で使われている。本研究では、この研究開発のシステム（以降、ABE 情報共有システムと呼ぶ）を用いて、建設業務向けの属性ベース暗号の活用方法 a)～d)が実現できるか調べ、できない点に関しては拡張開発を施して実現できるようにした。

・ABE 情報共有システムの概要

ABE 情報共有システムは、属性ベース暗号で暗号化したファイルをクラウドストレージに保存する Web システムである。ファイルを登録するユーザは、登録時に復号ポリシーを指定する。すると、復号ポリシーを含んだ暗号化ファイルがストレージに保存される。ファイルを取得するユーザは、自身の属性から秘密鍵を生成し、その鍵に含まれる属性が暗号化ファイルの復号ポリシーを満たす場合のみ暗号化ファイルを復号できる。

ABE 情報共有システムは、復号ポリシーに復号者の ID や属性を複数指定するというシンプルな使い方を想定した画面になっている。

[ABE 情報共有システムで活用方法を実現できるかの検討]

a) ワークフロー

復号ポリシー：個人の ID や属性

秘密鍵：　属性

⇒ABE 情報共有システムの既存入力項目および既存の属性で実現可能である。

b) 復号可能期間の制限

復号ポリシー：日付の期間指定

⇒　日付の期間の入力フォームと復号ポリシーへの設定が必要。

秘密鍵：現在日時

⇒　システムが現在日時を属性に追加して秘密鍵を作る必要がある。

c) 位置情報によるエリア制限

復号ポリシー：緯度経度

⇒　緯度および経度の範囲を入力するフォームと復号ポリシーへの設定が必要。

秘密鍵：現在地の緯度経度

⇒　復号時に、モバイル端末で GPS の緯度経度を取得してユーザの属性に追加して秘密鍵を作る必要がある。

d) 接続元を制御

復号ポリシー：IP アドレスの範囲

⇒　IP アドレスの範囲を入力するフォームと復号ポリシーへの設定が必要。

秘密鍵：

⇒　復号時に、接続元の IP アドレスを取得してユーザの属性に追加して秘密鍵を作る必要がある。

(3)　システムの拡張内容

検討内容をもとに、ABE 情報共有システムのファイル登録 Web 画面、暗号化/復号のサーバ処理に対して項目を追加し、暗号ライブラリに対しては数値の範囲指定を有効にした。また、モバイル端末で緯度経度情報を取得するようにした。

a) Web 画面

ABE 情報共有システムで建設業務向けの復号ポリシー（復号可能期間制御、位置によるエリア制御、接続元制御）を入力できるようにするため、ファイル登録画面の復号ポリシーを設定する箇所に、各入力フォームを追加した。

以下がファイル登録画面に建設業務向けの復号ポリシー入力フォームを追加した画面である。

この画面で各項目に条件を入力した場合に作られる復号ポリシー文字列の例を示す。

■ユーザの復号ポリシーの入力
宛先：宛先１　宛先２　　（既存項目）
復号可能期間：　2015/01/02　～　2015/03/04
IP アドレス：192.168.001.002　～　192.168.003.004
緯度：　　111.10000　～　111.12345
経度：　　99.00000　～　101.00000

■設定される復号ポリシー
```
(  ( 宛先１　OR　宛先２　)
   AND
   ( CurrentDate >= 20150102　AND　CurrentDate <= 20150304 )  // 復号可能期間
   AND
   (　 (IP >= 192168001002　AND　IP <= 192168003004)　　// IP アドレス
OR
    (　 (latitude >= 12345000　AND　latitude <= 12345111)　　// 緯度
          AND
          (longitude >= 9900000　AND　longitude <= 10100000)  // 経度
       )
   )
)
OR 登録者 OR 例外属性
```

※既存のポリシーの説明
・(宛先１　OR　宛先２　OR　・・・ OR 宛先 n)　：復号可能なユーザ
・OR 登録者　　：ファイルの登録者。自身が登録したファイルは常に復号可能。
・OR 例外属性　　：全てのファイルに設定される属性。特別な事態が発生して復号権限を持たないファイルを復号する必要が発生したら、管理者にこの属性を持たせて復号可能にする。

b) サーバー処理

システムでは復号前にユーザの属性を元に秘密鍵が生成される。今回追加した復号ポリシーに適用するために、鍵生成時にユーザ属性にシステムが自動的に現在日/ IP アドレス / 緯度経度を追加するようにした。

・現在日[CurrentDate]は、サーバ日付

・IP アドレス[IP]
復号する端末が固定 PC の場合、サーバはリクエストのヘッダから IP アドレスを取得し、属性にセットする。

・緯度/経度 [latitude / longitude]
復号する端末がモバイルの場合、クライアントはモバイルの GPS の緯度/経度サーバに送り、サーバが属性にセットする。

例）
■ユーザ属性
CurrentDate=20150102　IP=192168001002　latitude=12345000　 longitude=7890000

c) 暗号ライブラリ

BSW ライブラリ自体は数値の範囲指定機能を持つが、ABE 情報共有システムはこの機能を利用しないためライブラリから除外している。そこで今回、ライブラリの数値の範囲指定機能を使えるようにした。これにより、ファイル登録画面で入力された範囲条件（日付、緯度経度、IP アドレス）を含む復号ポリシーでファイルを暗号化できるようになり、復号時には数値の属性（日付、緯度経度、IP アドレス）で秘密鍵を生成できるようになった。

d) モバイル端末での緯度経度の取得

このシステムは Android モバイル端末でも利用できる。ユーザがモバイルでファイルを復号しようとするとシステムはモバイルの位置情報をサーバに送信する。復号対象のファイルの復号ポリシーに位置の条件が含まれている場合、サーバはユーザの位置がその条件を満たすかどうかチェックし、満たす場合のみ復号する。

・モバイル端末での位置情報の取得
モバイル端末での位置情報の取得には、Geolocation API を使用した。Geolocation API は W3C が定めた位置を扱うための標準仕様で、スマートフォンやタブレットのブラウザが実装している。Geolocation API は GPS や Wi-Fi、IP アドレスなどからモバイル端末の位置（世界測地系）を取得していて、測位の精度は測位の方法により異なる。GPS の測位の精度とエリア制御の利用検討については後述する。

(4)　GPS を用いたエリア制御の利用方法の検討

測位精度については本研究のスコープから外れるため、ここでは測位精度に関する調査文献（「平成２４年度情報セキュリティ対策推進事業（位置情報の精度・信頼性に関する調査事業）調査報告書」日本情報経済社会推進協会）[6]を参考にして、スマートフォンの GPS の測位精度について簡単に述べる。

・スマートフォンの GPS の測位精度

この調査文献では、キャリア・メーカーなどが異なる Android スマートフォンを用いて、以下の測定場所の晴天時と雨天時における GPS 測位精度を試験している。

測定場所の環境：①通しの良い屋外、②見通しの悪い屋外、③屋内

[調査文献の試験結果]

晴天時の GPS 測位試験の結果は、①見通しの良い屋外⇒②見通しの悪い屋外⇒③屋内の順に誤差が大きくなり、①見通しの良い屋外は誤差がほとんど 20m 以内で、ビルの陰など②見通しの悪い屋外は誤差が 40m 以内に収まっているものは 6 割程度である。

雨天時は①見通しの良い屋外②見通しの悪い屋外ともに測位精度が低下する結果となっている。

端末による違いは、①見通しの良い屋外ではさほど差はないが、②見通しの悪い屋外では差が生じている。

・エリア制御の利用方法の検討

この調査研究より、GPS 測定値の誤差の範囲は GPS 衛星からの受信のしやすさや天候の影響を受けることが分かる。復号ポリシーに緯度経度の範囲を指定してエリアによるアクセス制御を実施する場合は、GPS の測定値には誤差があり、現場の周りの障害物（建物など）の有無により誤差の大きさに違いがでることを考慮して復号ポリシーの緯度経度の範囲を決める必要がある。

2010 年に技術検証のための準天頂衛星初号機「みちびき」が打ち上げられ、2017 年から 2019 年までに 3 基が追加され 4 基体制で運用されることが決まっている。GPS 衛星の信号と準天頂衛星の信号を組み合わせることで誤差範囲 2m～数 cm で測位でき、信号捕捉の時間も短くなる。ASUS の ZenFone 2 など、みちびき対応のスマートフォンやタブレットもいくつか発売されている。今後の実用化に向けた動きに期待したい。

(5)　安全性の検討

属性ベース暗号は、属性から秘密鍵を生成し、その秘密鍵内の属性が暗号文の復号ポリシーを満たす場合のみ復号できる暗号方式のため、属性が偽造されると本来復号できないはずの暗号文を復号できてしまう。そこで、悪意を持ったユーザが、自身の属性では復号ポリシーを満たしていない暗号文に対して、属性を偽造して復号しようとするケースを検討した。

a) 復号可能期間指定

ユーザ属性にセットする現在日は、サーバのマシン日付を使用している。攻撃者がサーバに侵入してマシン日付を復号可能期間内の日付に変更してしまうと、本来復号できない暗号文が復号されてしまう。
本システムでは、攻撃者によるマシン日付変更は想定していない。

b) IP アドレス指定

ユーザ属性にセットする固定端末の IP アドレスは、サーバで HTTP リクエストヘッダの送信元 IP アドレスから取得している。この IP アドレスが偽造されると、復号ポリシーに指定された端末/ネットワーク IP アドレスではない端末で、復号できてしまう。
本システムでは、攻撃者による HTTP リクエストヘッダの送信元 IP アドレスの偽造は想定していない。

c) 緯度/経度指定

ユーザ属性にセットする緯度と経度の値は、モバイル端末側で HTTP リクエストの Body にセットしてサーバに送信される。本システムはセッション管理をしているためログインしていないユーザのリクエストは処理されないが、ログインしているユーザが悪意を持っている場合は、HTTP Body に実際の緯度経度とは異なる値をセットしてサーバに送信することが可能である。サーバ側は、リクエストの緯度経度が偽装されたものかどうか、判断することができない。

また、Android 端末では GPS の位置情報を疑似の位置情報にする Android アプリも存在し、緯度経度を偽装することが可能である。

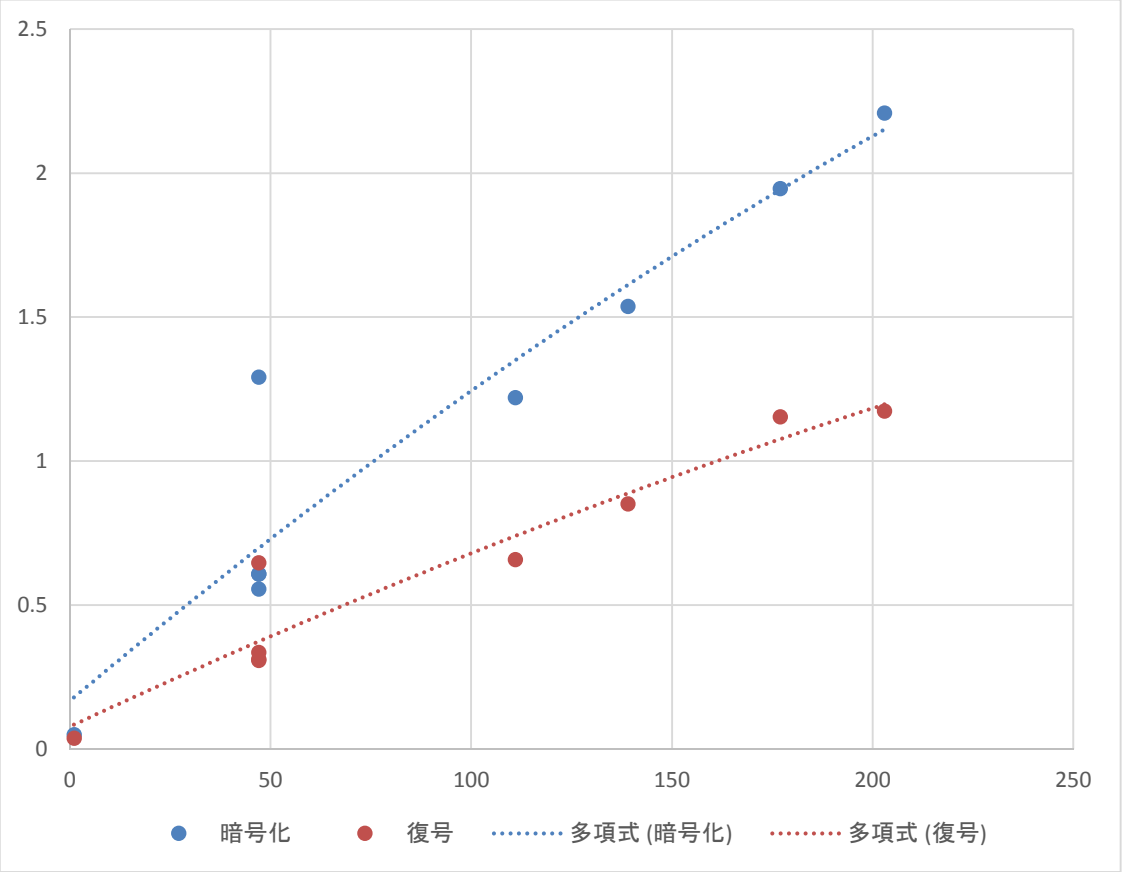
本システムには GPS 位置情報偽装の対策はまだとられておらず、今後の課題である。
対策としては、定期的にモバイルの位置情報をサーバに送信し、位置情報の大幅な変更があった場合は位置情報の偽装を疑い、管理者に警告する方法が考えられる。

(6)　ライブラリの性能の検討

今回、BSW CP-ABE ライブラリの数値の範囲指定機能を利用できるようにしたが、暗号では数値を剰余で扱っていて、数値の大小を比較することが困難である。この点を BSW CP-ABE では、数値を bit 展開して文字列として比較することで解決している。しかし、復号ポリシー中のある一つの比較条件が数値の bit 数分の文字列一致条件に変換されるため性能への影響が懸念されたが、複数の比較条件を含む復号ポリシーを測定したところ暗号化が 2 秒ほど、復号が 1 秒ほどであったため、実用に耐えられると判断した。

暗号化と復号の処理時間の復号条件数による違い

復号条件の文字列	展開後の 復号条件数	暗号化	復号
policy = CurrentDate = 20151230#27	1	0.051	0.038
policy = (CurrentDate >= 20151230#27 and CurrentDate <= 20151231#27)	47	0.556	0.336
		1.292	0.647
		0.608	0.312
		0.608	0.308
policy = (CurrentDate >= 20151230#27 and CurrentDate <= 20151231#27)　and (IP >= 192999999999#38 and IP <= 199999999999#38)	111	1.220	0.658
policy = (CurrentDate >= 20151230#27 and CurrentDate <= 20151231#27) and (latitude >= 12312345#27 and latitude <= 99999999#27) and (longitude >= 99999999#27 and longitude <= 99999999#27)	139	1.537	0.851
policy = (CurrentDate >= 20151230#27 and CurrentDate <= 20151231#27) and (latitude >= 12312345#27 and latitude <= 99999999#27) and (longitude >= 99999999#27 and longitude <= 99999999#27) and (IP >= 192999999999#38)	177	1.946	1.154
policy = (CurrentDate >= 20151230#27 and CurrentDate <= 20151231#27) and (latitude >= 12312345#27 and latitude <= 99999999#27) and (longitude >= 99999999#27 and longitude <= 99999999#27) and (IP >= 192999999999#38 and IP <= 199999999999#38)	203	2.208	1.174



[詳細]　復号可能期間指定と緯度経度、IP アドレスをすべて指定すると、復号条件の文字列は約 200 個の復号条件に展開される。その最大条件での暗号化の処理時間は 2 秒強、復号の処理時間は 1 秒強であった。

7　研究の成果と今後の課題

(1)　研究の成果

本研究では、建設業務特有の情報セキュリティの課題を明らかにして、暗号でその課題を解決する方法を研究した。特に、工程ごとに関係者が入れ替わるという性質と、オフィスではなく工事現場で機密情報が扱われるという点に注目した。人の入れ替わりに対しては、アクセス可能な期間を限定する方法を提案した。現場での機密情報へのアクセスに対しては、現場にいるときだけアクセスできる方法と、アクセス元を制限する方法を提案した。これら論理レベルの提案を、暗号ライブラリを使って実際にシステムにできることを示した。

本研究では、日付・位置情報・IP アドレスをアクセスコントロールの対象項目にしたが、これらの項目はシステムが自動的にユーザの属性に追加していて、値が偽造されると復号権限を持たずとも復号できてしまう危険があることが分かった。

(2)　今後の課題

・属性値の偽造対策

日付・位置情報・IP アドレスの中で位置情報は特に偽造できる可能性が高いうえに偽造を検知することが難しい。スマートフォンの位置情報の偽造は研究課題になっていて、電子署名により真正性を担保する方法やアクセスの URL を隠ぺいする方法などが考えられている。実用化に向け、それらの研究を参考にして位置情報の偽造防止と検知の仕組みを考え、システムに組み込む必要がある。

・グループウェアへの応用

本研究では、建設の業務への属性ベース暗号の活用をシンプルな情報共有システムで検証したが、実際の業務で使うシステムには、国土交通省「工事施工中における受発注者間の情報共有システム機能要件」に書かれている掲示板やスケジュール管理などの機能も求められ、グループウェアの利用が適している。

グループウェアにもオープンソースのシステムがあるため、今後はオープンソースのグループウェアに今回開発したプログラムを移植して、建設業の関係者の間で便利に安全に情報をやりとりできるようにしたい。

オープンソースのグループウェアの代表的なものを２つ挙げる。

① Alfresco

[開発元] Alfresco Software Inc.

[機能] 文書管理がメイン

・バージョン管理（チェックイン、チェックアウト）
・ワークフロー
・アクセス証跡
・モバイル対応
・クラウド環境とオンプレミス環境のコンテンツを常に同期
など
[ライセンス] コミュニティ版（オープンソースライセンス、LGPL）
エンタープライズ版（サブスクリプションライセンス）
[システム環境] Spring Framework (Java/J2EE フレームワーク)

② Aipo
[開発元] 株式会社エイムラック　（日本企業）
[機能] グループウェア
・スケジュール管理
・ワークフロー
・Web メール
・ファイル共有
・モバイル対応
など
[ライセンス] AGPLv3
[システム環境] OpenSocial を採用、Java

いずれも Java 実装のため、Java の属性ベース暗号ライブラリも候補に入れて考える。

謝辞
私はこれまで暗号の理論を研究してきましたが、今回、建設業という具体的なケースを想定した利用方法を考えそれをシステム化したことで、暗号が理論的に安全でも暗号を使うシステム側に問題があれば脆弱になるため、ユーザの使い方やシステム全体の総合的な情報セキュリティを考える必要があると実感しました。このような貴重な機会をいただけたことに大変感謝しています。
また会合の際には、建設の業務や現場に明るくない私のために、現場のセキュリティ事情を教えてくださったり貴重なアドバイスをいただきました。協力してくださった JACIC の方々にお礼申し上げます。ありがとうございました。

■参考文献

[1]建設現場における情報セキュリティガイドライン（第１版）
建築業協会、日本土木工業協会
http://www.nikkenren.com/kenchiku/bcs_it/report/security/index.html

[2]建設現場における情報セキュリティガイドライン【元請会社編／協力会社編】
建築業協会、日本土木工業協会
http://www.nikkenren.com/kenchiku/bcs_it/report/security/index3.html

[3] 建設現場ネットワークの構築と運用ガイドライン
日本建設業連合会
http://www.nikkenren.com/publication/pdf/97/2013_NW_GL.pdf

[4]工事施工中における受発注者間の情報共有システム機能要件　（Rev.4.0）
国土交通省
http://www.cals-ed.go.jp/mg/wp-content/uploads/kinoyoken_rev40_kaisetsu.pdf

[5]土木工事の情報共有システム活用ガイドライン
国土交通省
http://www.mlit.go.jp/common/001068234.pdf

[6] 平成２４年度情報セキュリティ対策推進事業（位置情報の精度・信頼性に関する調査事業）調査報告書
日本情報経済社会推進協会
http://www.meti.go.jp/meti_lib/report/2013fy/E003535.pdf

■暗号の参考文献

[7]Ciphertext-Policy Attribute-Based Encryption
John Bethencourt, Amit Sahai, and Brent Waters.
28th IEEE Symposium on Security and Privacy (Oakland) , May 2006.

[8]Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption
Allison Lewko, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, Brent Waters
Advances in Cryptology – EUROCRYPT 2010
Lecture Notes in Computer Science Volume 6110, 2010, pp 62-91

[9] Attribute-Based Encryption for Circuits from Multilinear Maps
Sanjam Garg Craig Gentry Shai Halevi Amit Sahai Brent Waters
http://eprint.iacr.org/2013/128.pdf

[10] Decentralizing Attribute-Based Encryption
Allison Lewko, Brent Waters
Advances in Cryptology – EUROCRYPT 2011
Lecture Notes in Computer Science Volume 6632, 2011, pp 568-588

様式－３－３

HOW TO UTILIZE ATTRIBUTE-BASED ENCRYPTION FOR SECURE INFORMATION SHARING ON CONSTRUCTION SERVICES

Handa,S.
ARK Information Systems

Construction job has particular work style:
1. Workers are replaced by another frequently according their job period.
2. Workers access sensitive data at outside like construction site.

These would be factor of information leak, so it needs to control user access. Attribute-based encryption(ABE) is cryptosystem that can control access. User sets decryptional condition in ciphertext or secretkey. I study how to utilize ABE for secure data sharing of construction work.

I propose 5 method:

1.Workflow
2.Limitation of period
3.Limitation of area
4.Limitation of IP address
5.Control of distribution of sensor data

I achieved these methods on an information sharing system that uses an attribute-based encryption library and evaluated security of the method.

KEYWORDS**:** *security, information sharing, attribute-based encryption*

様式－３－２

研　究　成　果　の　要　約

助成番号	助　成　研　究　名	研 究 者・所 属
第2014-12号	属性ベース暗号による建設業務のセキュアな情報共有の実現のための研究	株式会社アーク情報システム 半田　沙里

建設の業務では、工程ごとに関係者が入れ替わる、オフィスではなく工事現場で機密情報を扱うなどの特有の要因により、情報漏洩のリスクが懸念されている。この問題をアクセスコントロールが可能な属性ベース暗号(Attribute-Based Encryption：ABE）で解決できるのではないかと考え、属性ベース暗号の建設業務への活用方法の研究を行った。

属性ベース暗号のタイプ（暗号文ポリシー属性ベース暗号：CP-ABE、鍵ポリシー属性ベース暗号：KP-ABE）ごとにできることを整理すると、暗号文ポリシー属性ベース暗号は情報へのアクセスを制御することができ、鍵ポリシー属性ベース暗号は情報配信を制御することができることが分かった。これを建設に適用し、課題を解決する方法をCP-ABEで４つ、KP-ABEで１つ提案した。

[CP-ABEによるアクセスコントロールの建設での活用方法]

１．ワークフロー

承認順にアクセス権を付与する。承認者以外に情報を見られないようにできる。

２．復号可能期間の制御

工事関係者に担当の工期の間だけアクセス権を付与する。工期が過ぎると自動的にアクセスできなくなる。

３．位置情報によるエリア制御

モバイル端末が現場エリア内にあるときのみ情報にアクセスできる。

４．接続元を制御

接続元のIPアドレスを制限することで、自宅など職場以外からのアクセスをブロックし、情報漏洩のリスクを軽減する。

[KP-ABEによる情報配信制御の建設での活用方法]

・センサー測定値の配信制御

様々な復号ポリシー設定した秘密鍵を準備してユーザに渡すことで、ユーザがアクセスできるデータをコントロールできる。

理論ベースのこの活用方法をシステムに実現できるか確かめるため、属性ベース暗号を組み込んでいる既存の情報共有システムに対して拡張開発を行い、活用方法が実現できることを示した。

活用方法２～４は、復号ポリシーに日時・緯度経度・IPアドレスを数字の範囲で指定する必要があるため、数値の範囲指定の機能を持つ暗号ライブラリを使ったが、１つの数値範囲条件を多数の文字列一致条件に変換するため性能への影響が懸念されたが、実測の結果２秒ほどだと分かり実用レベルであると判断した。

暗号文ポリシー属性ベース暗号は、ユーザの属性から復号の秘密鍵を生成する。今回提案した活用方法は、復号時にシステムが自動的に現在日時・現在位置の緯度経度・接続元のIPアドレスを復号者の属性に追加するため、それらの値が偽造できると本来復号できないはずの暗号化ファイルを復号できてしまう危険があることが分かった。特にモバイルの位置情報は偽造できる可能性が高いので、偽造防止および偽造検知の研究を参考にして、システムに対策を施す必要がある。このようにシステムが自動追加する属性の偽造対策が今後の課題である。

本研究では、建設業務への属性ベース暗号の活用をシンプルな情報共有システムで検証したが、実際の業務では掲示板やスケジュール管理等の機能を持つグループウェアの利用が適している。今後はオープンソースのグループウェアに対して今回開発したプログラムを移植して、建設に携わる関係者が便利に安全に情報を共有できるようにしたい。