(34) 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

半田　沙里[1]

[1]非会員　株式会社アーク情報システム（〒102-0076 東京都千代田区五番町４－２）
E-mail:shanda@ark-info-sys.co.jp

建設の業務では施主や受注側管理者，各施工の現場技術者など様々な関係者の間で情報を共有する必要があるが，工程ごとに技術者が入れ替わる，下請け構造の多層化により情報セキュリティ教育が浸透しにくいという特性があり，情報の漏洩が懸念される．そこで，アクセスコントロール機能を持つ"属性ベース暗号"を利用して建設の情報共有をどのように安全にできるかを研究した．属性ベース暗号には，"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２種類ある．それぞれの構成と特性を整理し，建設の情報共有における活用例を示した．また，暗号文ポリシー属性ベース暗号の情報共有システムに緯度経度によるエリア制限の機能を追加し，属性ベース暗号のシステム化について検討した．

Key Words : *data share，security，crypto systems，Attribute-Based Encryption*

1. 研究の背景

建設の業務では，打合せ資料や契約書，工事の設計図，写真などの情報を発注者，受注者，工事の管理者や作業者など様々な人達の間で共有する必要があり，情報の中には，個人情報や契約の金額，社外秘の技術情報など，関係者以外に知られてはならないものもある．それらの情報を扱う人を考えてみると，建設の業務の特色から以下のようなセキュリティ問題が懸念される．

①工程ごとに作業者が入れ替わり，多くの関係者が出入りする．
②下請け構造が階層化していて，情報セキュリティの教育が行き届きにくい．
③ITリテラシがさまざまで，自宅PCからの情報漏洩などのリスクがある．

本研究では，属性ベース暗号(Attribute-Based Encryption : ABE)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活用できるかを研究した．また，その方法のシステム化も検討した．

2. 属性ベース暗号とは

属性ベース暗号は公開鍵暗号の一つである．公開鍵暗号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．この課題を解決した暗号方式が属性ベース暗号である．属性ベース暗号は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適している．

“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 かつ 部長”のように復号条件（以下，復号ポリシーと呼ぶ）を指定できる暗号方式である．受信者は，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「暗号文ポリシー属性ベース暗号」と呼ばれ，逆に暗号文にデータ属性がセットされて，受信者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「鍵ポリシー属性ベース暗号」と呼ばれる．表-1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してまとめる．

表-1　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整理

	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いて，平文を暗号化する.	データの属性と公開パラメタを用いて，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.

３章と４章では，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、次に建設への適用の例を示す．適用例は，Webシステムを想定している．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.

3. 暗号文ポリシー属性ベース暗号の利用例

(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．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.

(2) 建設への適用

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．ユーザがその情報を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/経度をサーバーに送り，サーバー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

サーバー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．

4. 鍵ポリシー属性ベース暗号の利用例

(1) 一般的な利用方法

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) 建設への適用

・ 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

5. システム化での検討事項

建設の情報共有における属性ベース暗号の様々な活用ケースを検討した．なかでも建設では特に"位置情報によるエリア制限"に特色があると考え，情報共有システムに実現することにした．

属性ベース暗号は，様々な機能や安全性を達成した多

くの方式が提案されている．その中でも，John Bethencourt，Amit Sahai，Brent Watersが提案した秘密分散を利用した方式[1]は基本的な方式で，他の方式のベースとなっているものである．彼らは，提案方式を実装したライブラリをWeb上で提供している[2]．（以降，このライブラリをBSW CP-ABEと呼ぶ）

本研究では，情報セキュリティ大学院大学が研究開発で作成したBSW CP-ABEを用いた情報共有システム[3]に対して，"位置情報によるエリア制限"機能を実現した．その際の課題を以下に記す．

①緯度経度で利用エリアを制限するには，暗号スキームが数値を範囲（<，<=，>，>=）扱えなければならない．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，ライブラリを実行すると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，処理性能が低下するという問題を抱えている．

②Androidには現在地の緯度経度を偽装するアプリが存在し、偽装に対してシステムで別途対策を講じる必要がある．

謝辞：本研究は，（一財）日本建設　情報総合センターの研究助成を受けて実施したものです．

参考文献

1) Bethencourt, J，Sahai, A，and Waters, B：Ciphertext-Policy Attribute-Based Encryption，*SP '07 Proceedings of the 2007 IEEE Symposium on Security and Privacy*, p.321-334，2007.
2) Bethencourt, J，Sahai, A，and Waters, B：Ciphertext-Policy Attribute-Based Encryption , <http://acsc.cs.utexas.edu/cpabe/ >，(入手 2015.6.30).
3) 情報セキュリティ大学院大学：「組織内情報共有プラットフォーム」，<https://www.iisec.ac.jp/news/20140530angonews.html> ，(入手 2015.6.30).