MITSUBISHI ELECTRIC
Changes for the Better

NEWS RELEASE

（開発 No.1605）

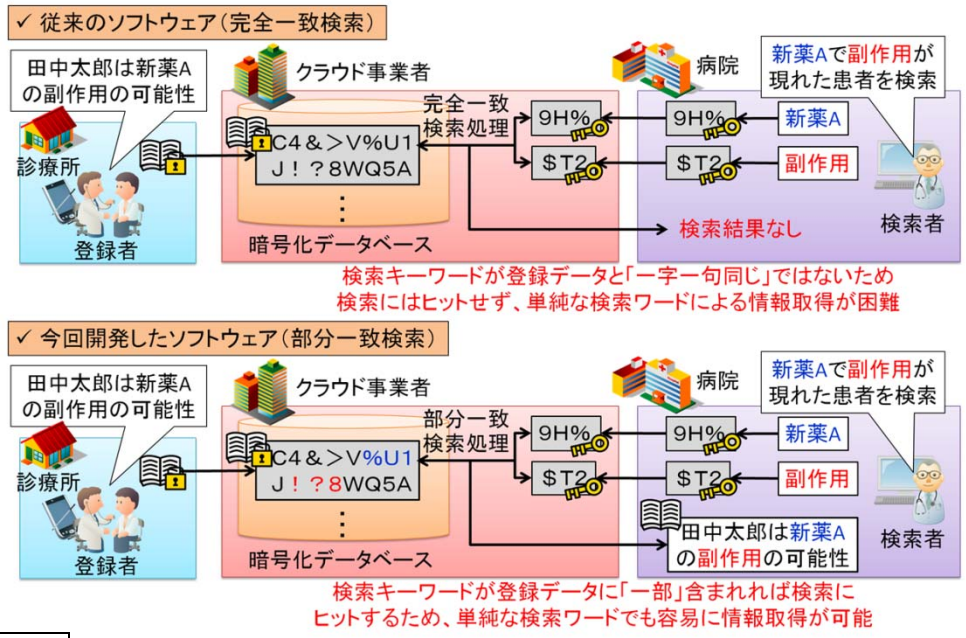
2016 年 2 月 4 日
三菱電機株式会社

クラウド上での暗号化データ検索の利便性向上に貢献

「部分一致対応秘匿検索基盤ソフトウェア」を開発

三菱電機株式会社は、クラウドサービス（以下「クラウド」）において、機密保護のために暗号化した情報を復号せずに検索できる秘匿検索技術に、「部分一致検索機能」を付加した「部分一致対応秘匿検索基盤ソフトウェア」を世界で初めて※1 開発しました。従来の「完全一致検索」と同等の安全性を確保したまま、検索者の利便性向上に貢献します。

※1　2016 年 2 月 4 日現在（当社調べ）



開発の特長

1. キーワードを暗号化した状態で「部分一致検索」を可能にし、利便性向上に貢献

・登録データや検索キーワードの各文字を暗号化するだけでなく、各文字が先頭から何文字目かを表す「文字位置」を各暗号文に埋め込み、検索キーワードの「文字位置」を暗号化したままスライドさせて検索することで、検索キーワードの「部分一致検索」を実現
・「部分一致検索機能」により、長い文字列に対するキーワード検索が可能となり、用途が拡大

2. 強固な暗号化技術により、クラウドの機密保護環境を構築

・登録データの暗号化時にキーワード検索可能な部署や利用者を限定し、より強固な機密保護を実現
・同じ検索キーワードでも毎回暗号文の値が変わるため、検索キーワードの類推を防止可能
・検索キーワードの各文字を分離させない暗号化技術により、文字の出現頻度分析を防止

開発の概要

	検索機能	安全性
今回	暗号化したまま、完全一致検索に加えて、部分一致検索が可能	暗号化したままキーワード検索可能 検索するユーザーを限定可能
従来※2	暗号化したまま、完全一致検索のみ可能	同上

※2　2013 年 7 月 3 日に当社が発表した「秘匿検索基盤ソフトウェア」

今後の展開

2017 年度に、本技術を当社製品に適用する予定。

報道関係からのお問い合わせ先	〒100-8310 東京都千代田区丸の内二丁目 7 番 3 号　TEL 03-3218-2359　FAX 03-3218-2431 三菱電機株式会社　広報部

開発の狙い

機器のネットワーク接続や様々なデータの集約を行うため、クラウドの需要は拡大しています。また、マイナンバー制度の導入により、医療費削減のためにカルテに記載されているプライバシー情報の共有・利活用が想定されるなど、異なる場所で収集・管理されてきた個人情報がつながります。そのため、機密情報やプライバシー情報をクラウドで管理して利活用する際には、情報の暗号化による機密保護やプライバシー保護を行うとともに、利便性にも優れたセキュリティー対策が求められています。

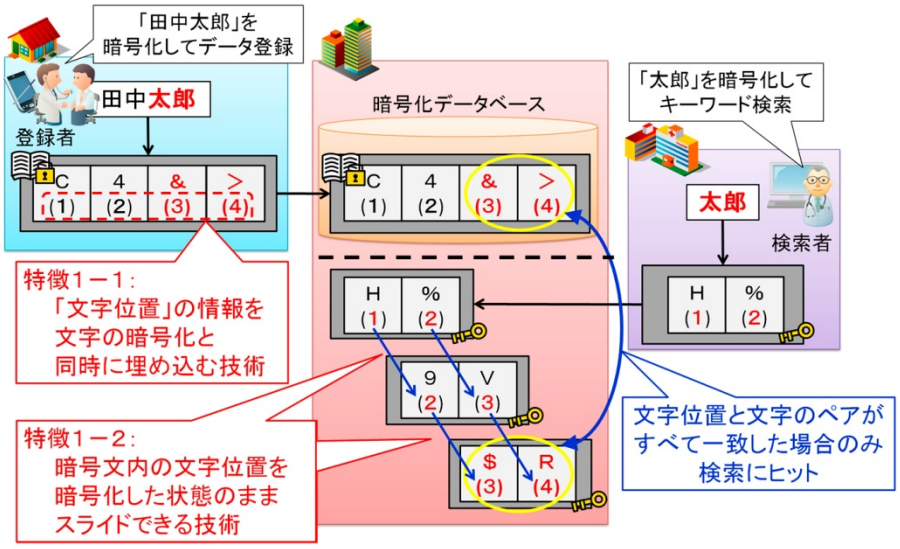
当社は、2013 年 7 月 3 日に、企業側でデータ暗号化および鍵管理を行い、クラウドでのコンピューターウイルス感染による情報漏洩や、管理者の内部不正による暗号化データの復号を防ぎつつ、クラウド側のデータ検索を可能とする「秘匿検索基盤ソフトウェア」を発表しました。一方、このソフトウェアは「完全一致検索」のみに対応しており、一般的なウェブ検索で用いられているような柔軟な検索はできず、利便性を高めることが課題でした。

特長の詳細

1. キーワードを暗号化した状態で「部分一致検索」を可能にし、利便性向上に貢献

今回開発したソフトウェアでは、登録データや検索キーワードの各文字を暗号化するだけではなく、各文字が先頭から何文字目の位置にあるかを表す「文字位置」の情報を各文字の暗号化と同時に埋め込む技術と、埋め込まれた「文字位置」を暗号化したままスライドさせる技術を実現しました。従来のソフトウェアでは、「文字位置」の情報を埋め込めず、登録データと検索キーワードが一字一句一致しなければ検索にヒットしませんでしたが（完全一致検索）、今回開発したソフトウェアでは、暗号化された検索キーワードを復号せずに、埋め込まれている「文字位置」をスライドさせて登録データの文字列と検索キーワードの一致判定を実施できます。このような「文字位置」の情報を用いることで、暗号化したまま「部分一致検索」を可能としました。

また、従来の「完全一致検索」のソフトウェアでは、必要な情報を容易に検索できるように登録データを短くすることや、使える検索キーワードを事前に決定しておくなどの制約がありましたが、今回の「部分一致検索」ではそのような制約なく容易に検索できるため、様々な用途に適用できます。



2. 強固な暗号化技術により、クラウドの機密保護環境を構築

本ソフトウェアは、既に当社から発表済みの「秘匿検索基盤ソフトウェア」と同様に、登録データの暗号化時にキーワード検索が可能な部署・利用者を限定できるため、企業のような組織に適したアクセス制御機能を備えています。また、同じ検索キーワードでも暗号化する度に毎回異なる値に変化するため、検索キーワードの類推を防ぐことができます。

また、登録データや検索キーワードの各文字の暗号文を抜き出して検索処理を実行できると、各文字の出現頻度が分析可能となり、たとえ暗号化されていてもその頻度から文字を推定できる恐れがあります。これを防ぐため、暗号文の各文字を分離不可とする暗号化も実現しました。これらにより、これまで通りの機密保護環境レベルを保ちながら、より柔軟な「部分一致検索」を実現します。

特許

国内 4 件、海外 4 件　出願中

開発担当研究所

三菱電機株式会社　情報技術総合研究所
〒247−8501　神奈川県鎌倉市大船五丁目 1 番 1 号
FAX 0467-41-2142
http://www.MitsubishiElectric.co.jp/corporate/randd/inquiry/index_it.html