Solution Service Product

大規模なクラウド個人情報管理を実現する「匿名バンク」

対象ユーザー

マイナンバーや個人情報などを安全・安心に利用できるサービスを実現したいお客さま。

特　長

「匿名バンク」の基盤となる検索可能暗号化技術にインデックス機能を実装し、100万人以上の個人情報管理にも対応。セキュアなクラウドサービスの実現に貢献。

クラウド上での安全・安心なデータ管理が課題に

2016年1月から「マイナンバー制度」がスタート。社会保障や税など、これまで分散していた個人情報がマイナンバーにひもづけられることで、確認作業時間のムダやミスが減り、業務効率や利便性が向上していくものと期待されています。将来的には図書館、銀行口座やクレジットカードなどにも適用範囲が広がると予想されており、従業員やお客さまのマイナンバー管理やサービス強化に役立てたいと考える企業にとっては、個人特定情報のセキュリティ強化が今まで以上に重要な課題となります。

近年は、クラウドが広く普及し、企業での活用も増加の一途にあります。クラウドセキュリティの標準を定めているCSA※1は、情報漏えいに特に配慮する必要があるときにはデータの暗号化保存を推奨しています。しかし一般的な暗号方式でデータを暗号化保存する場合、データの検索・照合を行う際に暗号化したデータを一度クラウド上で復号しなければなりません。そのためにはデータを復号するための復号鍵もクラウド上で管理することになります。暗号化データと復号鍵をクラウドで管理すると、クラウド管理者も含めた第三者への情報漏えいリスクが残ることから、機密性の高いデータの利活用への大きな妨げとなっていました。

実際、2015年9月の米国ニューヨーク州の医療保険者へのサイバー攻撃では、保存データは暗号化されていたものの、攻撃者は復号鍵にもアクセスしていたといわれています（2015年10月1日 ITmediaエンタープライズ掲載）。お客さまのセキュリティニーズに応えるためには、単なるデータ暗号化だけではなく、プラスアルファの対策が必要になっています。

※1 Cloud Security Alliance

マイナンバーを活用したセキュアなサービス基盤を実現

日立は、マイナンバーを含めた個人情報を“個人を特定できないように管理”できる匿名化情報管理サービス「匿名バンク」を提供しています。匿名バンクは、オリジナルのお客さま情報を「個人特定情報」（氏名・生年月日・性別など）と「匿名化情報」（趣味、嗜好、購入履歴、健康管理情報など）に分離して管理することで、これら機微な情報を取り扱う事業者側のリスクを軽減することができます。

その基盤技術となる「検索可能暗号化技術」※2は、データの暗号化、復号に加え、暗号化したまま一致検索することができるもので、AES※3レベルの暗号強度に加え、頻度解析に耐えられる暗号化方式を採用しています。

今までのデータベースの暗号化では、データセンター内の特権ユーザー（管

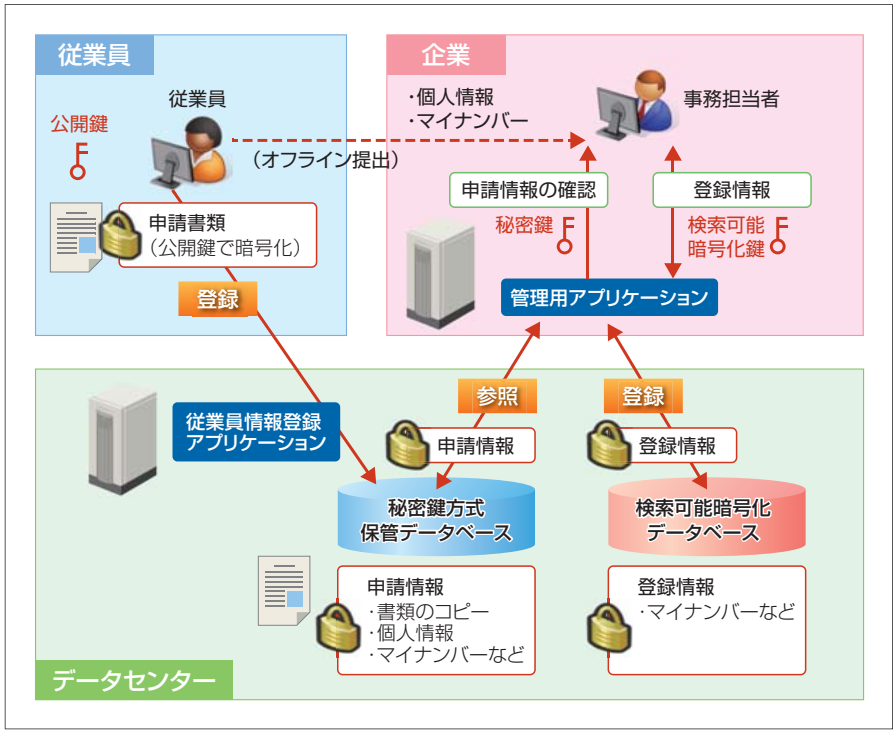


図1 マイナンバーでの活用例

理者、技術者など）による復号が可能であるため、情報漏えいのリスクがありました。これに対し、検索可能暗号化技術があれば暗号化したまま検索できるので、復号の必要がありません。したがって復号鍵をデータセンター側に渡さずにすむので、たとえデータセンター内の特権ユーザーであっても復号は不可能になります。これにより、「個人特定情報」と「匿名化情報」は、同一センター内での分離保管が可能となり、セキュアなサービス運用を実現。さらにクラウドを活用することで、データベースの管理と復号鍵の管理を事業者単位で分離できるため、マイナンバーおよび個人情報の、より安全・安心な管理が可能となります。

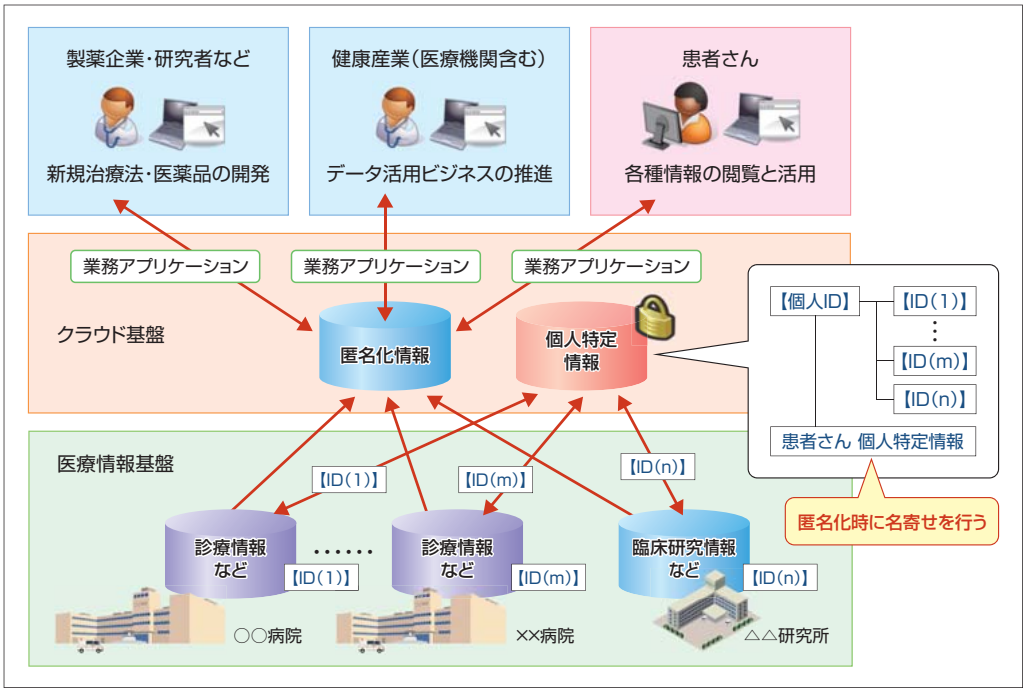


図2 医療・ヘルスケア分野での活用例

※2 特許第5412414号
※3 Advanced Encryption Standard：米国の国立標準技術研究所によって制定された暗号化規格

機能強化で100万人以上の個人情報管理にも対応

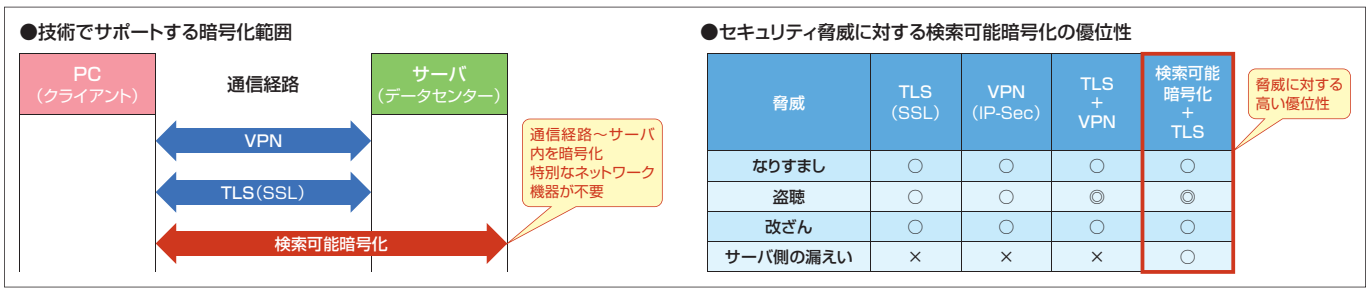
このたび、検索可能暗号化技術にインデックス（索引）機能を実装することで、100万人以上の個人情報管理にも対応できるサービス能力の向上を図りました。これにより、クラウド環境における大規模なマイナンバー管理や各種行政手続き、個人特定情報を利用した電子申請やヘルスケアサービス、医療・臨床研究情報などの安全な収集・共有・公開基盤としての活用が可能となりました（図1、図2）。

また匿名バンクは、PC（クライアント）とサーバ（データセンター）の間でも、特別なネットワーク機器を必要とせず二重に暗号化することが可能なため、専用線に相当するセキュアな通信経路を確保できます。匿名バンクとTLS※4を組み合わせることで、通信路におけるなりすましや盗聴、改ざんを防ぐだけでなく、データセンター側でも情報にアクセスすることが困難となるため、セキュリティ性の高い共有システムをクラウド上に構築可能となるのです（図3）。

例えば、名寄せに本サービスを利用すれば、複数システム間の情報を統合的に取り扱い、複数機関で共有・活用するプラットフォームを構築することができます。

※4 Transport Layer Security：データを暗号化して送受信する方法

今後も日立は、匿名バンクの継続的なサービス強化と、検索可能暗号化技術を活用した安全・安心な社会インフラの構築に貢献していきます。



脅威	TLS（SSL）	VPN（IP-Sec）	TLS＋VPN	検索可能暗号化＋TLS
なりすまし	○	○	○	○
盗聴	○	○	◎	◎
改ざん	○	○	○	○
サーバ側の漏えい	×	×	×	○

図3 匿名バンクによるセキュリティ脅威への対応

お問い合わせ先

（株）日立製作所 スマート情報システム統括本部
https://www8.hitachi.co.jp/inquiry/it/healthcare-it/form.jsp

■ 情報提供サイト
http://www.hitachi.co.jp/tokumeibank/