プレスリリース
2019 年 10 月 29 日

国立研究開発法人情報通信研究機構
日本電気株式会社

生体認証データの高秘匿・高可用性な伝送・保管を量子暗号を用いて実現
～ナショナルチームのスポーツ選手用電子カルテなどへの応用～

【ポイント】

- 個人情報である生体認証データの伝送を量子暗号を用いた高秘匿技術で実現
- 生体認証時の参照データの保管を量子暗号ネットワーク分散ストレージで実現
- スポーツ分野のナショナルチームのデータサーバ管理技術に応用 今後端末にも適応予定

国立研究開発法人情報通信研究機構（NICT、理事長: 徳田 英幸）と日本電気株式会社（NEC、代表取締役執行役員社長 兼 CEO: 新野 隆）は共同で、顔認証システムでの特徴データの伝送と、特徴点などの認証用参照データの保存を、量子暗号[*1]と(k,n)閾値秘密分散[*2]（以下、秘密分散）を用いて構築し、認証時の高い秘匿性・可用性を持ったシステムを開発し、実証に成功しました。

本システムは、量子暗号ネットワーク上にカメラ・サーバ及び秘密分散により分散ストレージされた認証用参照データサーバを設置し、不正アクセスや参照データ消失のリスクが極めて低い安全なシステムです。

生体認証は簡単に本人確認でき、パスワードなどの紛失の危険性もない便利な認証技術ですが、その情報が盗まれた場合は変更できないという課題もあります。この課題を解消するために、認証時のデータ伝送を量子暗号で秘匿化し、認証用参照データを秘密分散で保管・管理することにより、量子コンピュータをもってしても理論上漏えい盗聴が不可能なシステムを開発しました。

我々は、本システムを NICT の量子暗号研究開発用ネットワーク上に構築し、様々な競技団体の日本代表選手が所属するナショナルチームのデータサーバ管理のための試験利用を 10 月から開始しました。このサーバには、日本代表選手のスポーツ選手用電子カルテや分析用映像が保存されているため、極めて厳重に管理する必要があります。今後、各スポーツ競技団体のユーザ端末がサーバにアクセスする際のユーザ認証やデータサーバとの通信にも、今回我々が開発した技術を取り入れる予定です。

【背景】

生体認証は、人間の身体的特徴を抽出し、認証を行うもので、利用方法が簡単で紛失などの問題もない優れた特性を持ち、ユーザに優しいシステムです。

一方、その情報が盗まれた場合、更新できないという課題もあります。また、生体認証用参照データは、個人情報であり、情報セキュリティを担保する上で極めて厳重に管理する必要があり、安全かつ可用性の高い生体認証システムの開発が求められています。

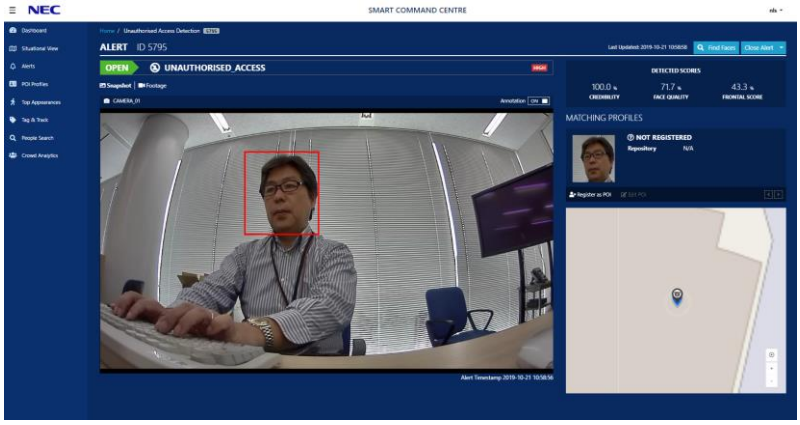


図 1　サーバ室での作業者の顔認証デモの様子

【今回の成果】

NICT は、量子暗号のネットワーク化の研究開発を進め、秘密分散プロトコルを用いた情報理論的安全な[*3]データ保管技術の研究開発を進めてきました。NEC は、情報理論的安全な量子暗号の研究開発を進めてきており、世界 No.1 の認証精度の顔認証技術[*4]を有しています。

今回、NICT と NEC は、これらの技術を統合して、顔認証時の特徴データ伝送を量子暗号で秘匿化するとともに、

認証時の参照データを秘密分散で保管するシステムを開発しました。そして、NICT が 2010 年から運用を続けている量子暗号ネットワーク Tokyo QKD Network[*5] 上にこのシステムを実装・実証することに成功しました。

Tokyo QKD Network は、東京都心にある 2 か所にも量子暗号ネットワークを展開しており、それらの拠点にはネットワークオペレーションセンター（NOC）が配置されています。NOC では、データサーバのサービスも提供しており、様々なユーザのデータが保存されています。日本代表選手が所属する様々なスポーツ分野のナショナルチームは、2013 年から国際競技大会に出場する選手のパフォーマンス向上を目的とした、選手のスポーツ選手用電子カルテや映像解析に本ネットワーク上のサーバを利用しています。

今回、ナショナルチームのご協力により、我々はこのシステムを利用して、このサーバへのアクセスを物理的に管理する試験利用を 10 月から開始しました。都内にある NOC のサーバ室に設置されたカメラ映像から、特徴データが抽出されます。その特徴データは量子暗号で暗号化され、NICT 本部（小金井）の信頼できるサーバ室に設置されている顔認証サーバに送られ、認証が実施されます。なお、この顔認証サーバに保存されている認証用参照データは、Tokyo QKD Network 上に秘密分散でバックアップを行っており、顔認証サーバ等に不具合が発生しても、システムを迅速かつ安全に復旧することが可能です。

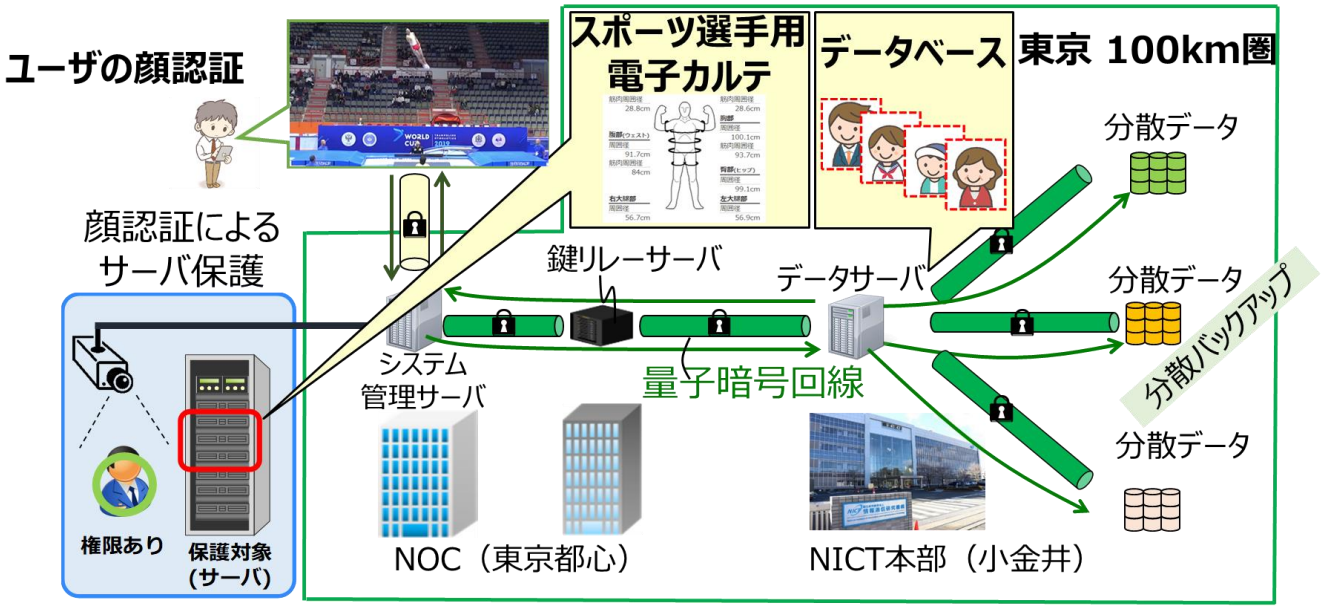


図 2　Tokyo QKD Network 上に設置された顔認証による管理システム概要

【今後の展望】

今後は、各スポーツ競技団体のユーザ端末がサーバにアクセスする際の顔認証のログインによるユーザ認証やデータサーバとの通信にも量子暗号の技術を取り入れ、スポーツ選手用電子カルテの確認や映像解析の際に物・人の安全で強固な認証、安全なデータ伝送及び安全なデータ保存技術の試験利用を、2019 年度末を目途に開始する予定です。

これらの技術検証は完了しており、これらの技術について、ハンドフリーでの本人認証が必要とされるスマート製造現場や医療現場での導入を目指し、より利便性の高いシステムの実現を目指した研究開発を進めていきます。

各機関の役割分担

- NICT: 量子暗号ネットワーク及び秘密分散の開発
- NEC: 量子暗号、量子鍵配送リンク及び顔認証装置の開発

研究支援

なお、本研究の一部は内閣府総合科学技術・イノベーション会議の戦略的イノベーション創造プログラム（SIP）「光・量子を活用した Society5.0 実現化技術」（管理法人：国立研究開発法人量子科学技術研究開発機構 https://www.qst.go.jp/）によって実施されました。

戦略的イノベーション創造プログラム（SIP） https://www8.cao.go.jp/cstp/gaiyo/sip/

＜用語解説＞

***1 量子暗号通信技術**

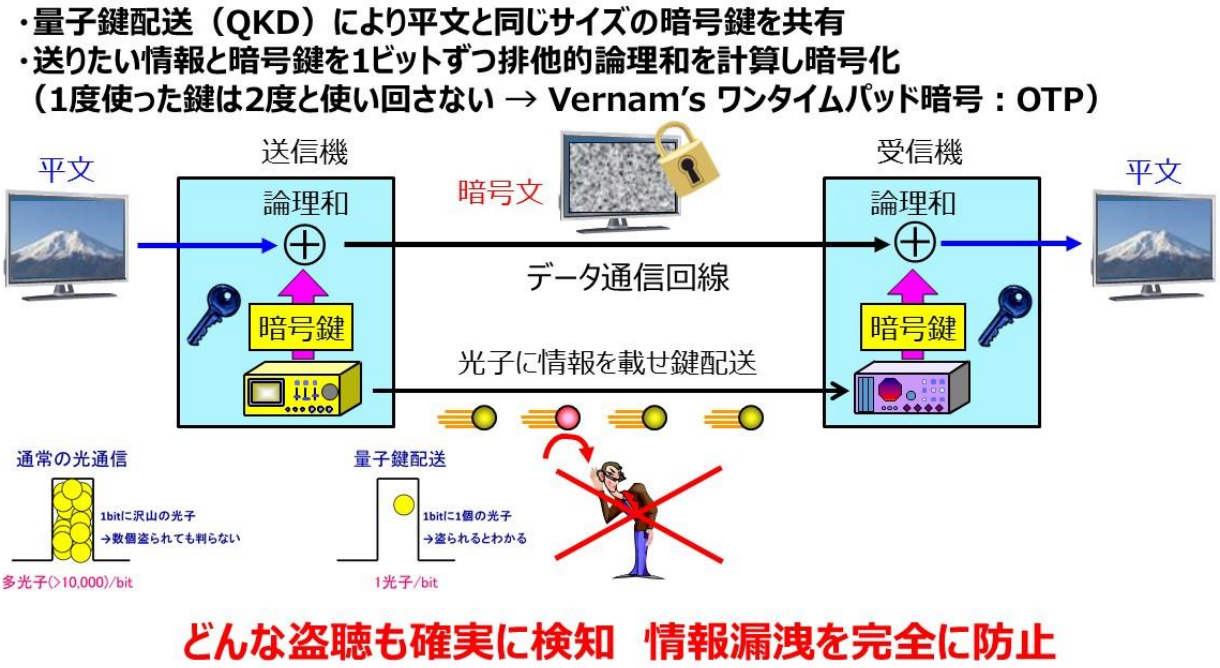
量子鍵配送（QKD）[*6] 装置から供給された暗号鍵を種鍵（たねかぎ）として使用する共通鍵暗号（ワンタイムパッド[*7] 又は AES）装置のことで、データレイヤ上の重要通信を直接、高速暗号化（100 Mbps～1 Gbps）する統合型暗号化システム

***6 量子鍵配送（Quantum Key Distribution: QKD）**

量子鍵配送では、送信者が光子を変調（情報を付加）して伝送し、受信者は届いた光子 1 個 1 個の状態を検出し、盗聴の可能性のあるビットを排除（いわゆる鍵蒸留）して、絶対安全な秘密鍵（暗号化のための乱数列）を送受信者間で共有する。変調を施された光子レベルの信号は、測定操作をすると必ずその痕跡が残り、この原理を利用して盗聴を見破る。量子鍵配送による鍵生成と、それを用いた暗号技術の総称は量子暗号技術と呼ばれることもある。

***7 ワンタイムパッド暗号化**

送受信者が暗号化通信する際、送信する情報（平文）のデジタルデータと同じ長さの乱数を暗号鍵として用意し、はぎ取り式メモ（パッド）のように 1 回ごとに使い捨てる暗号化方式。異なる平文ごとに、異なる暗号鍵を使う方式をいう。平文と暗号鍵データの排他的論理和によって暗号文を生成して伝送し、受信側で再び暗号文と暗号鍵データの排他的論理和によって平文を復号する。この暗号化方式は、どんなに高い計算能力を持つ盗聴者であっても、暗号文から平文を永遠に解読できないことが証明されている最も安全で強固な暗号化方式である。



***2 (k,n)閾値秘密分散**

(k,n)閾値秘密分散法では、最初に、秘密情報 S（整数）の保有者が S から n 個のシェアと呼ばれる値を生成する。次に、秘密保有者は、シェア保有者（1～n）に各シェアを秘密裏に渡す。秘密保有者は、この後、秘密情報を消去する。秘密情報の復元には、k 人のシェア保有者が協力して k 個のシェアを収集し、所定の計算をすることにより、秘密データ S を復元できる。このとき k を閾値と定義する。(k,n)閾値秘密分散法の詳細な説明や NICT での活動については以下を参照。

NICT 報道発表「将来にわたり情報漏えいの危険のない分散ストレージシステムの実証に成功」（2016 年 7 月 1 日）
https://www.nict.go.jp/press/2016/07/01-3.html

***3 情報理論的安全性**

情報理論に基づいた暗号解読の可能性についての概念。公開情報から暗号文の復号に必要な鍵を推定できないこと。将来どれだけ計算機が発達しても盗聴の危険性がない。

***4 NEC 世界 No.1 の認証精度の顔認証技術**

NEC、米国国立機関による顔認証の精度評価で第 1 位を獲得
https://jpn.nec.com/press/201910/20191003_01.html

***5 Tokyo QKD Network**

NICT が 2010 年から東京圏に構築・運用を続けている量子鍵配送（QKD）ネットワークのテストベッド。NEC、東芝、NTT-NICT、学習院大学等の様々な産学機関で開発された QKD 装置が導入され、装置改良の研究開発、長期運用試験、相互接続やネットワーク運用試験など、QKD ネットワーク技術の実用化に向けた研究開発のほか、QKD ネットワークを現代セキュリティ技術と融合した新しいセキュリティアプリケーションの研究開発などを進めている。
http://www.tokyoqkd.jp/

＜ 本件に関する問い合わせ先 ＞
国立研究開発法人情報通信研究機構
未来 ICT 研究所
量子 ICT 先端開発センター
藤原 幹生
Tel: 042-327-7552
E-mail: fujiwara@nict.go.jp

日本電気株式会社
ナショナルセキュリティ・ソリューション事業部
飯塚 浩巳
Tel: 042-333-5591
E-mail: qkd-inquiry@nss.jp.nec.com

＜ 広報 ＞
国立研究開発法人情報通信研究機構
広報部 報道室
廣田 幸子
Tel: 042-327-6923
E-mail: publicity@nict.go.jp

日本電気株式会社
コーポレートコミュニケーション本部広報室
浜田 毅士
Tel: 03-3798-6511
E-mail: press@news.jp.nec.com