プレスリリース
平成 26 年 6 月 4 日

世界初、量子鍵配送・スマートフォンを用いた認証・データ保存システムの開発に成功

～安全な鍵をスマートフォンに転送、重要情報へのアクセス権の設定、安全な情報保存を可能に～

【ポイント】

- 量子暗号とスマートフォンを組み合わせた、個人データの効率的・安全な管理システムを開発
- スマートフォンに個人認証用の鍵などを保存することで、個人データアクセス権の厳格な管理が可能
- 医療機関での電子カルテなどへの応用が期待

独立行政法人 情報通信研究機構（以下「NICT」、理事長: 坂内 正夫）は、量子鍵配送装置[*1] からの安全な鍵（共通乱数）をスマートフォンに転送・保存することで、個人データへのアクセス権の設定とデータの安全な保存を可能とするシステムの開発に世界で初めて成功しました。本技術の開発により、従来、量子鍵配送で実現していた伝送路上での情報理論的に安全な通信だけでなく、データ管理においても高い安全性を確保することが可能になりました。例えば、クラウド上のデータ・サーバに保存された電子カルテなど高度に秘匿すべき個人データを、スマートフォンに転送した鍵で暗号化・復号化することにより、高度に秘匿すべき個人データへのアクセス権を容易に設定でき、本人の承認なしに個人データが閲覧されることがない重要データの効率的かつ安全な管理が可能になります。

【背景】

現在、個人情報を多く含むデータをネット上や関係機関のサーバに保存するケースが多くなっています。一方、データ伝送路やネットワークを通しての情報漏えいが様々なレベルで脅威になっています。伝送路上での盗聴に対しては、量子鍵配送装置と one-time-pad[*2] 暗号を組み合わせることで、情報理論的に安全（絶対安全）[*3] な通信の実現が可能ですが、伝送されたデータを安全に保存することや保存したデータへの不正アクセス行為への対策は十分になされていませんでした。

【今回の成果】

今回新たに開発したシステムは、量子鍵配送装置で情報理論的に絶対安全なデータ暗号化用と個人認証用の２つの鍵（共通乱数）を生成し、量子暗号とスマートフォンを組み合わせることで、個人データ等の高い秘匿性が求められるデータの安全な伝送と伝送後のデータの絶対安全な保存を可能にします。また、データを暗号化する範囲や運用条件に応じて暗号化用の鍵の設定を変えることができるため、データへの多様なアクセス管理を実現することができます。

スマートフォンに転送された鍵による復号

【今後の展望】

今回開発したシステムを用いて、個人情報への不正アクセスを防止できる電子カルテ[*4] などへの応用を検討するとともに、その他の応用についての共同研究開発を広く募集する予定です。

＜ 本件に関する 問い合わせ先 ＞
未来 ICT 研究所
量子 ICT 研究室
藤原 幹生、佐々木 雅英
Tel: 042-327-7552, 6524
E-mail: fujiwara@nict.go.jp, psasaki@nict.go.jp

＜ 広報 ＞
広報部 報道担当
廣田 幸子
Tel: 042-327-6923
Fax: 042-327-7587
E-mail: publicity@nict.go.jp

＜用語解説＞

*1 量子鍵配送装置

量子鍵配送装置では、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こん跡が残り、この原理を利用して盗聴を見破る。

*2 one-time-pad

通信量と同じ長さの乱数を 1 回だけ使用し暗号化する暗号方式。乱数は送信者と受信者であらかじめ共有され、データの送受信時に 1 ビットごとに排他的論理和を行うことにより、暗号化・復号化を行う。この暗号化方式については、情報理論的安全性が証明されている。

*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。

*4 電子カルテ

電子カルテとは、従来、医師・歯科医師が診療の経過を記入していた紙のカルテを電子的なシステムに置き換え、電子情報として一括してカルテを編集・管理し、データベースに記録したもの。カルテは、医師・歯科医師が医師法第 24 条・歯科医師法第 23 条に基づいて記載、5 年間の保存が義務付けられている準公式書類にあたるため、不用意に電子化できるものではなく、電子カルテには法的な裏づけが必要だった。

それに対し、1999 年に厚生省（当時）は診療録の電子媒体による保存を認める通達を発表し、その際、電子カルテのガイドラインとして知られる以下の 3 つの条件を満たすよう求めた。

（1） 保存義務のある情報の真正性が確保されていること。
- ・故意または過失による虚偽入力、書換え、消去及び混同を防止すること。
- ・作成の責任の所在を明確にすること。

（2） 保存義務のある情報の見読性が確保されていること。
- ・情報の内容を必要に応じて肉眼で見読可能な状態に容易にできること。
- ・情報の内容を必要に応じて直ちに書面に表示できること。

（3） 保存義務のある情報の保存性が確保されていること。
- ・法令に定める保存期間内、復元可能な状態で保存すること。

さらに、電子カルテに対し、医療情報システムの安全管理に関するガイドラインに個人情報保護法＋JISQ15001:2006 による個人情報の保護が推奨されている。

補足資料

量子鍵配送・スマートフォンを用いた認証・データ保存システム

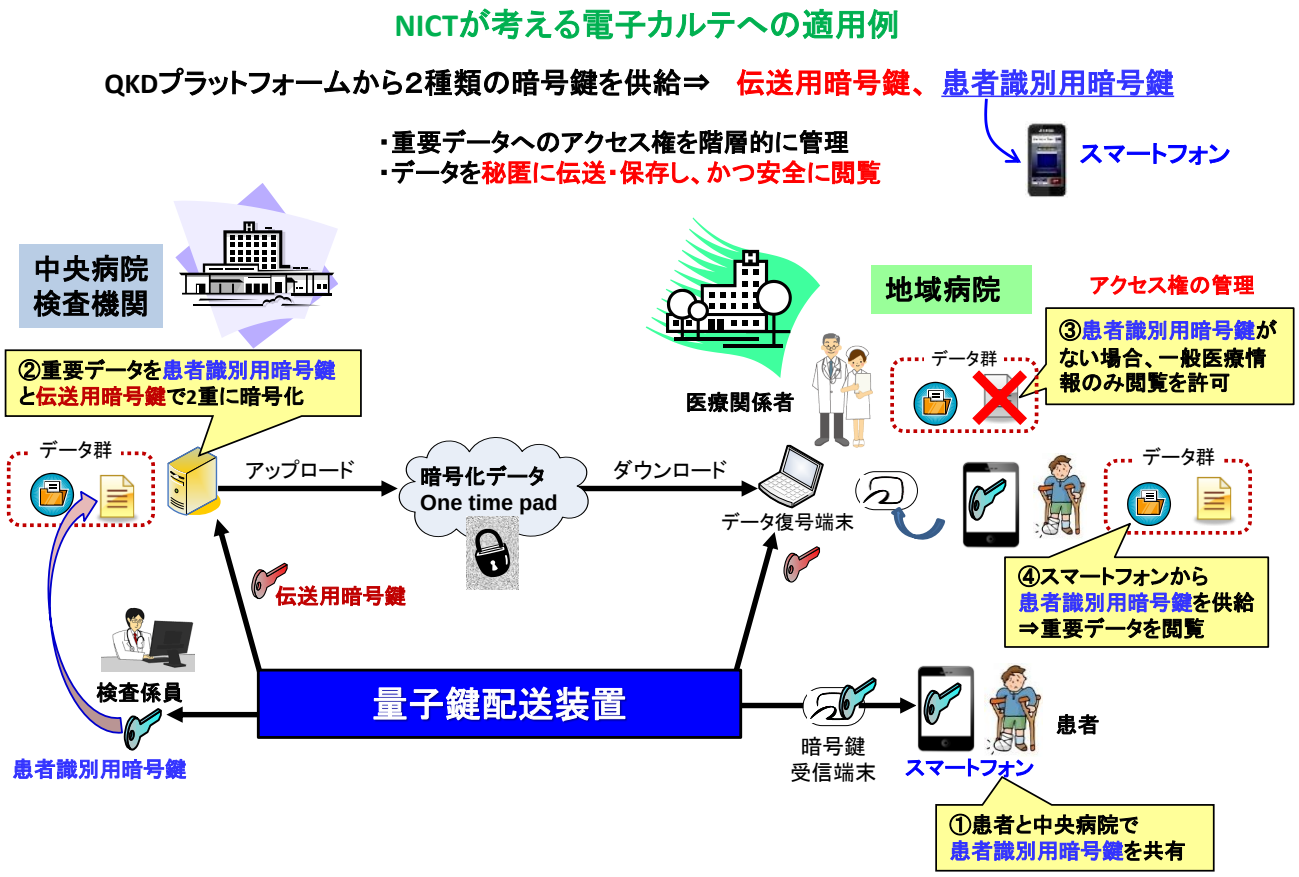

図 1: 量子鍵配送(QKD)装置とスマートフォンを用いたデータの安全な保存・閲覧システムの例

図 1 に、量子鍵配送装置とスマートフォンを用いたデータの安全な保存・閲覧システムの概要を示します。最初に、スマートフォン所有者は、データの送信者と量子鍵配送装置を用いて安全な鍵を共有します。データ送信者は、各ユーザに対してデータへのアクセス権を設け、各ユーザのスマートフォンに保存した鍵のブロックに対応し、データブロックごとに暗号化します。さらに、データ送信者は、送信用にも量子鍵配送装置からの鍵を使用して暗号化し、受信端末に伝送します。受信端末で復号化されたデータは、スマートフォンに格納された鍵で暗号化されているため、保存時にも不正アクセスによるデータの流失の心配がありません。ユーザがデータの閲覧をする際には、スマートフォンに格納された鍵をフェリカリーダーなどのインターフェースを通して、データ復号端末に転送します。データ復号端末では、鍵に基づいてデータを復号します(図 2 参照)。その際、データ送信者が設定したアクセス権が反映されるため、データ閲覧権限の設定が可能になります。

図 2: データ復号端末の例
右側にスマートフォンがつながれている。

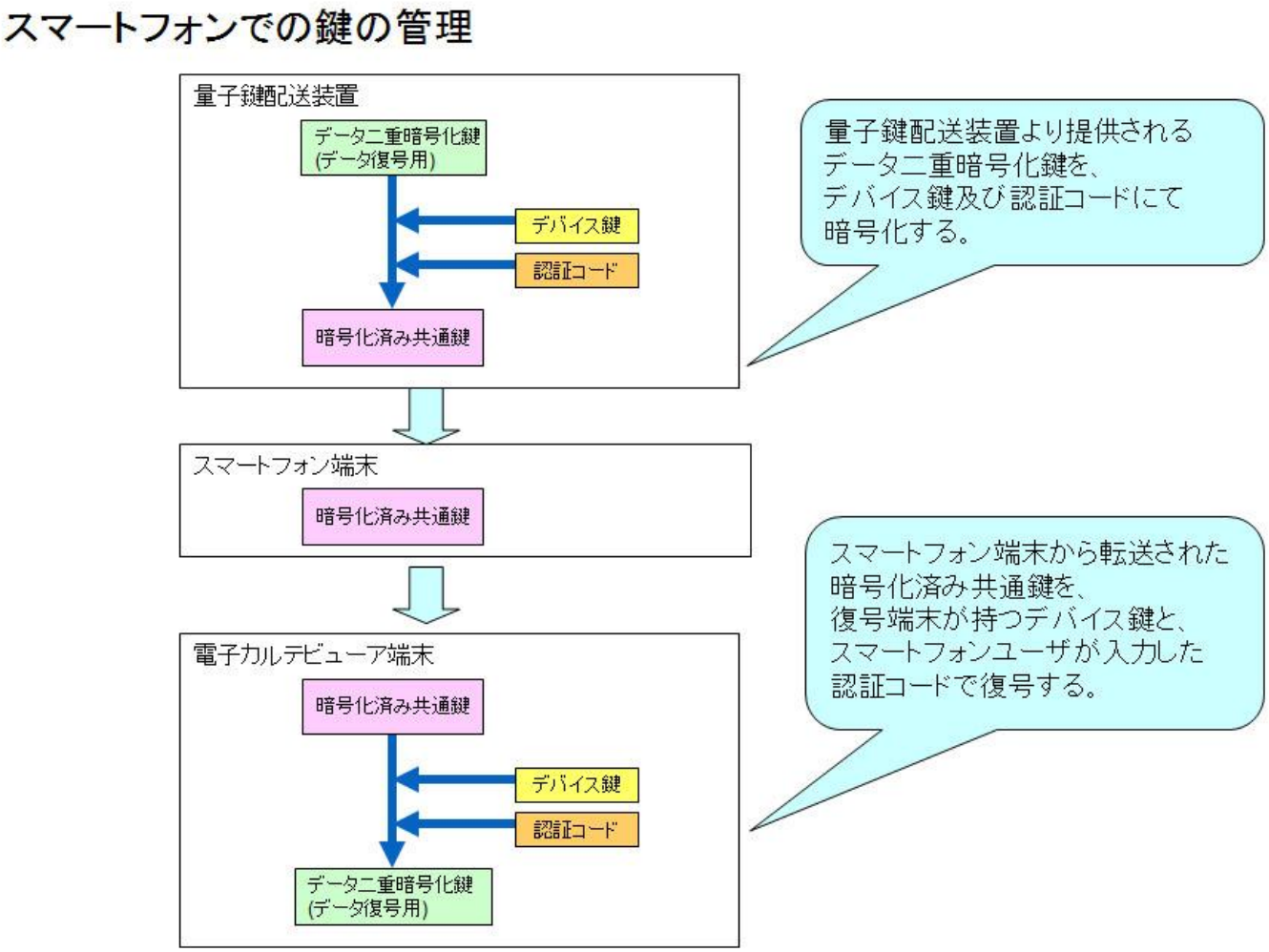

図 3: スマートフォンでの鍵管理の流れ

図 3 では、量子鍵配送装置からの鍵の受け取りと、データ復号時の鍵の流れを示しています。スマートフォンの個体とユーザ認証機能が本システムには組み込まれており、スマートフォンを紛失した際に、データの不正流出を防ぐためにユーザのみが知る認証コードにて復号用の鍵を暗号化しています。