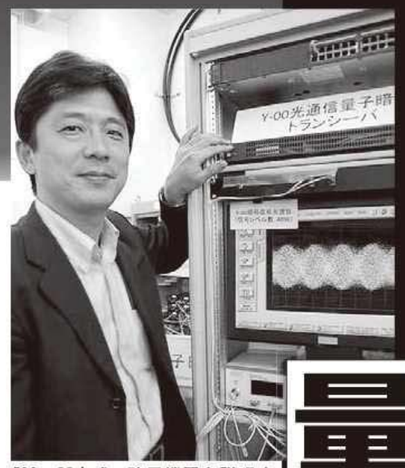
厳選ワイド 一日千秋

何かが始まる、何かが変わる――そんな期待感もふくらむ秋、である。どんな世界であれ、ずっと変わらず同じでいられるはずもない。ならば一日千秋の思いで時機をうかがう、そんな各界のニュースをお届けしよう。

実用化に向け日米が大競争 量子暗号って何だ？



「Y―00方式」暗号機器を説明する玉川大の二見准教授

東芝は「5年以内に実用化」とするが…

「量子」が情報通信を革命的に変えようとしている。『日本経済新聞』は8月31日付朝刊の1面トップに「東芝、究極の安全通信 量子暗号で実用化へ」と載せ、米CNNは9月4日、「グーグル、量子コンピューターを開発」と伝えた。

『量子コンピュータとは何か』（ジョージ・ジョンソン著、ハヤカワ文庫）によると、普通のコンピューターはデータを0と1に置き換えて計算するのに対して、量子コンピューターは0と1に加え「同時に0であり1である状態」の3通りに置き換える。その結果、「世界最速のスーパーコンピュータを使っても何十億年とかかる」（同書）数百桁の数の因数分解が量子コンピューターには素早く計算できる可能性があるという。

グーグルは2013年、カナダのDウェーブ・システムズ社から「世界初の商用量子コンピューター」を購入した。CNNによれば、Dウェーブ社とは別に、米カリフォルニア大サンタバーバラ校と共同で量子コンピューターの研究を進めることになったという。内閣府の科学技術・IT戦略担当参与の齋藤ウィリアム浩幸氏は、量子コンピューターの可能性をこう見る。

「今の性能を例えるなら、1970年代の半導体。しかし、ものすごい勢いで進化しており、いずれ桁数が大きい数の素因数分解が一気に解けるようになる可能性があります。そうなれば、〝国家的な大問題〟になるのは確実です」

世界中の暗号が解読可能になるからだ。齋藤氏によれば、銀行の多くが採用する「2048ビットのRSA暗号」を解読するには何千年もかかる。しかし、今より進化した量子コンピューターは一瞬で解いてしまう可能性がある。犯罪集団が量子コンピューターを入手すれば、あらゆる個人情報は筒抜けになってしまう。そこで研究が進んでいるのが「量子暗号」だ。

前出記事には、〈東芝は「理論上破られない」究極の暗号とされる量子暗号通信の実用化にめどをつけた〉とある。より正確には、「量子暗号鍵配信（QKD）」と呼ばれる方式。暗号処理されたデータを解読するための「暗号鍵」を光ファイバー経由で送信する際、何者かが盗み見しようとすると「鍵」は壊れ、データは解読されない仕組みだ。

東芝の発表によれば、〈東京の大手町―小金井間を結ぶ全長45キロメートルの既設光ファイバーを用い、1日あたりの平均鍵配信量25・8ギガビット（総鍵配信量878ギガビット）で34日間の安定した稼働を確認しました〉。これは1日当たりの鍵配信量としては「世界最大」という。

「川崎市の研究開発センターと英国の東芝欧州研究所で研究を続けており、5年後の実用化を目指しています」（東芝広報部）

しかし、QKDには難題がある。前出の齋藤氏は「光ファイバーの特性上、距離がネックになる」と言う。

「光ファイバーの信号は距離が長くなると弱まる性質があり、約50キロごとに信号を増幅する装置の設置が必要です。増幅するには信号を読み取るのですが、そうするとQKDの仕組み上、暗号が壊れてしまいます。結局、QKDは約50キロ以上の通信に使えないと一般的に理解されています」

もっと辛辣な見方をするのは、玉川大の広田修・量子情報科学研究所長だ。

「QKDは理論上、『100％安全』とされていましたが、近年、従来の数理暗号より優れた暗号は作れないと明らかになりました。現に米国は2003年にQKDの研究を断念しました」

ロシアの専門家が10年、学術誌に載せた論文、それにインターネットを開発した米国防総省の国防高等研究計画局（DARPA）が12年に発表した内容は、いずれもQKDに否定的な結論だったという。しかし、QKD以外の方式もある。

「鍵を配送するQKDとは異なり、通信文をそのまま量子効果を使って暗号化する方式です。00年に米ノースウエスタン大と玉川大で開発が始まりました。玉川大の『Y―00方式』は、量子暗号化したデータを毎秒100ギガビットの速度で120キロ伝送することに成功し、今年7月に対外発表しています」（広田氏）

毎秒100ギガビットは24時間に換算すると864万ギガビット。東芝の25・8ギガビットより約33万倍速い。同研究所の二見史生准教授は、次のように力説する。

「通信の世界では1秒当たりのビットで表示するのが常識です。遠くへ大容量のデータを安全に送る点で我々の方が圧倒的に優れているのは明らかです」

実験室に案内されると、ルーターのような外観の機器が置かれていた（149ページ写真参照）。データを量子暗号化するのだという。

「ノースウエスタン大の技術は米国で軍事用に使われると思いますが、我々は複数のデータセンターを持つ企業をユーザーに想定しています。技術的に実用段階にあります」（二見氏）

最近、ベネッセ、アップル、日本航空など個人情報の漏えいが相次ぐ。Y―00方式の導入が増えれば抑止効果があるはずだが、普及で困る組織があるという。

「米国の情報機関です。国家安全保障局（NSA）のスノーデン元職員が暴露した内部資料によれば、NSAは光ファイバーからデータを盗み見ています。Y―00方式は情報収集の妨げになるでしょう。まさかとは思いますが、夜道は気をつけています」（同）

米国の情報独占に挑戦すれば危ない……。スパイ映画のような話なのだ。

ジャーナリスト・谷道健太