

2019. 10. 19

畑 啓之

HTTPSではなくHTTPで始まるホームページは消え去る運命にあるのか？

最近以下のようなメールがよく入ってくる。このメールによると、通信の安全を確保するためのSSL証明書の導入がなされていないHTTPで始まるホームページは閲覧できなくなる可能性があるようである。正確にはHTTPSとHTTPが混在するホームページにおいてHTTPが閲覧不可能になる。しかし、世の中には通信の秘密の必要がない情報も多く、この措置にはいささか疑問が残る。世の中、確かに通信の秘密が破られると困るサイトも多くあるが、全てがすべてそのようなサイトであるとは限らない。SSL認証を取りそれを維持し続けるためには、年間数万円の費用が発生する。秘密保持を前面に押し出した新たな事業分野の創造（商売）を目指していると思えない。

本日の日本経済新聞には量子コンピュータの問題解決速度の速さが示されていた。スーパーコンピュータで1万年かかる計算が実に3分で終わるとのこと。量子コンピュータが汎用的に用いられるようになった時、SSL認証を受けたHTTPSはどうなっているのか、楽しみである。そんな時代となっても、HTTPは十分に役目を果たしているものと思うのだが。

【HTTPS化対応をしないとWebサイトが正常に表示されなくなります】

2019年12月から2020年2月にかけて、Google Chrome に対してWebサイト内の「HTTP」コンテンツがブロックされるよう段階的な仕様変更が行われることが公表されました。

■概要

▽対象ブラウザ

Google Chrome 79.0以降

▽変更内容

HTTPS/HTTP混在ページにおけるHTTPをデフォルトでブロック対象とする

▽想定影響

Webサイト上に「http」で記述されているコンテンツが正常に動作しなくなる

本仕様変更に伴い、コンテンツがブロックされると、Webサイトに訪問されたお客様に伝えたい情報を正しく伝えることができなくなります。

SSL 証明書の導入がお済みでない場合、2019 年 12 月の上記仕様変更前にご対応いただくことを強くお勧めいたします。

日本経済新聞 2019.10.19

量子コンピュータ グーグル実証か

人工知能（AI）などに続く革新的技術として期待される量子コンピュータ（3面きょうのこと）が「スーパーコンピュータを越える日」が近づいてきた。米グーグルは、理論上の概念だった性能を実証し、最先端のスパコンで1万年かかる問題を瞬時に解く実験に成功した。米IBMなども研究に力を入れる。急速な進歩はいずれ人類にこれまでにない計算パワーをもたらす。AIの活用や金融市場のリスク予測などを通じ、社会にディスラプション（創造的破壊）を起こす可能性を秘める。

グーグルが「量子超越」を達成したもう一つ。英フィナンシャル・タイムズは9月、この報じた。日本経済新聞が入手した資料によると、最先端のスパコンでおよそ1万年かかる計算問題を、同社の量子コンピュータが3分20秒で解いたという。

量子超越は、従来のコンピュータでは困難な計算問題を量子コンピュータが解く性能を指す。理論上はスパコンを上回ると思われる。世界で初めて実証したとみられる。同社は「コントロールできない」としているが、事実なら「教科書に載るレベル。歴史に重要な成果（科学技術振興機構の嶋田義昭フェロー）だ。近く正式発表するもようだ。

「超計算」人類の手中に

量子コンピュータは「量子力学」という物理法則に従って動く。従来のコンピュータは「0か1」で情報を表すが、量子力学の世界は「0であり、かつ1でもある」という特殊な状態が起りえる。

この仕組みを利用した「量子ビット」と呼ぶ計算単位を使うことで、膨大な情報をもとめて処理できる。計算の回数が大幅に減り、時間が劇的に短くなる。グーグルは今回、53個の量子ビットを実現し、乱数をつくる計算でスパコン超えの性能を実証した。グーグルなどが量子コンピュータの研究に乗り出したのは、半導体の微細加工による従来のコンピュータの性能向上に限界が見え始めたためだ。AIなどの登場を受け、膨大なデータを扱えるコンピュータが求められている。

50〜100量子ビットに到達し、開発はNISQと呼ばれる中規模の量子コンピュータに移りつつある。また幅広い計算に使えるわけではないが、経済や産業、社会を変えると期待が膨らむ。

計算能力が足りないため、解決しにくい問題は多い。例えば都市部の渋滞解消。現在は無数の車がそれぞれ1台ずつ進む道を短時間で計算するのは困難だ。量子コンピュータを使い、

スパコン1万年分、3分で

車ごとに「渋滞を起ささない最適ルート」を指定できれば渋滞は解消に役立つ。AIによる画像や言語などの処理も短時間、省エネになる。計算力を生かし、個人の体質に合わせて薬を作り分けるような新たな医療の誕生も後押しできる。

量子コンピュータの「使い道の開拓に力を入れるのがIBMだ。16年に量子コンピュータを外部の利用者にクラウド経由で公開した。世界で16万人を超過登録利用者のほか独アイムラーや米JPMorgan・チェアーズなど90近い企業など研究を進める。

日本では慶応義塾大学に連携拠点が有り、銀行や化学大手が参加する。画期的な薬や材料の開発、金融市場のリスク予測などの研究が熱を帯びる。

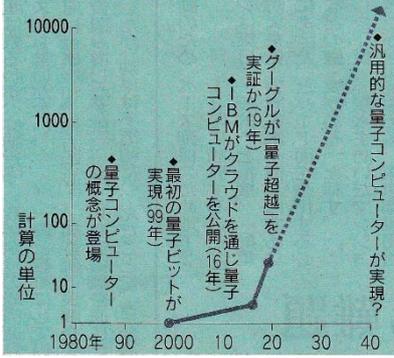
暗号破る恐れ

ただし、量子コンピュータがもたらすのは「光」だけではない。革新的技術は時に脅威となる。ささやかれるのが、ネット社会が根底から揺るリスクだ。現在は通信の際にパスワードなどの情報を暗号化している。最新のスパコンでも解読に時間がかかることから「安全」とみなす。量子コンピュータはこの暗号を破る恐れがある。新しい暗号技術の検討も進む。

IBMのメインフレーム（汎用機）の発売は1964年。従来のコンピュータもその前に20年ほどの黎明（れいめい）期があった。

量子コンピュータの歴史と今後の見通し

- 将来はスパコンでも難しい問題を短時間、省エネで解く
- AIによる画像、音声、言語の処理
 - 金融市場のリスク予測
 - 画期的な薬や材料の開発
 - 物流効率化や都市部の渋滞解消



日本IBMの森本典繁執行役員は「量子コンピュータもそのフェーズにある」と指摘する。

量子コンピュータの歴史で、およそ70年ぶりに起き始めた革新の動き。本格的な量子コンピュータの実用化には課題が多いが、米インテルや中国のアリババ集団なども開発に参入し、今後もアレックススルが生まれる見通しだ。

(生川暁、張耀宇)

開発が進む量子コンピュータの方式		
量子ゲート方式	従来のコンピュータのように、汎用性が高く様々な計算ができる	米グーグルやIBM
量子アニーリング方式	最適な組み合わせを見つけ出す計算に特化した方式	Dウェーブ・システムズ（カナダ）