［創立 60 周年記念特集：2050 年の情報処理］

9 2050年の情報処理（セキュリティ編）

菊池浩明 | 明治大学　須賀祐治 | IIJ
コンピュータセキュリティ研究会（CSEC）

X デーと量子コンピュータ

ついにこの日がきてしまった．2049 年 X 月，**RSA 公開鍵暗号 1024 ビットが H 社の量子コンピュータ QC-10 に解かれる**ニュースが世界を駆け巡った．量子コンピュータが開発されれば，離散対数問題や素因数分解問題の困難さにその安全性の根拠を持つ，今日の公開鍵暗号がことごとく使い物にならなくなることは 2000 年初頭から言われていることだった．しかし，「あと十年で開発される」という噂が繰り返されるだけで，なかなか実現には至っていなかった．

その流れが変わったのは，私が生まれた 2020 年．旧 Google 社が発表した量子コンピュータが現実的な規模の問題を解いたところからだったろうか．各社の開発競争が激化し，それに対応するように，次世代の耐量子暗号の開発も盛んになっていったのだった．

1979 年，RSA 暗号が生まれてすぐに，Scientific American 誌において Martin Gardner 氏の記事で懸賞金を出した 129 桁（428 ビット）の素因数分解問題が世界中の分散処理で解けたのはその 17 年後の 1994 年．1024 ビットの RSA 暗号は，2015 年の古書[☆1]によると，世界トップ 10 のスーパーコンピュータがあれば 2015 年に，汎用の PC であれば 2020 年に解かれると言われていたのに，2020 年に 829 ビットの素因数分解が成功した後は，記録も伸び悩んでいたのだった．

うむむ，量子コンピュータができた今，私が勤めているオンラインの暗号資産会社と新型ブロックチェーンによる公開鍵暗号基盤はどうなってしまうのだろう？

生体認証とビッグブラザー

私[☆2]の生まれた 2020 年は，2 回目の東京オリンピックが新型肺炎で延期された年として記憶されている．この年から急速に普及したものは，キャッシュレス決済と次世代生体認証基盤だった．それまでは指紋や顔画像を無断で取られることは，監視社会を恐れる人々によって強く反対されていたものだったらしいけど，スマホに生体認証が必須になり，全世界の空港での入国審査の標準となり，ラウンジの入退出で体験するにつれてみんな抵抗がなくなってきたものだ．特に私が小学校の頃から，学校に入るのにカメラでチェックするのが普通だったし，テストや受験のときにも顔認証されていたからね．

えっ?,「ビッグブラザー」は心配じゃなかったのかって？

確かに，George Orwell は，「1984 年」で人々の思想と行動を監視する社会における独裁者の象徴として描いていた．でも，私たちの生体情報は政府が管理するわけではない．公開鍵基盤 PKI が複数のルート証明書をトラストの起点とするように，**生体情報もそれぞれ自分が信用する民間の認定情報銀行に預け入れ，オープンな ID 連携の機構により全域的での認証が実現**されている．情報銀行同士の競合の中，ガバナンスの不十分な情報銀行は認定を取り消され淘汰が生じ，結果的に互いの不正を監視しあう競合信頼基盤ができあがっていた．

一方で 1990 年代の暗号規制に対抗すべくサイファーパンクと呼ばれる草の根運動の再来が起きた．地理的に狭いコミュニティだけで通用する私的なスコアリング制度が過疎化した地域で広がりを見せたけど，昭和前半の村社会が再建されることになってしまった．一斉を風靡した地域通貨はいまや中四国の山間部だけで

☆1 CRYPTREC Report 2017 暗号技術評価委員会報告，図 3-2: 素因数分解の困難性に関する計算量評価（1 年間でふるい処理を完了するのに要求される処理能力の予測，2018 年 2 月更新）．

☆2 2020 年生まれの 30 歳の IT 技術者．

ひっそりとやりとりされているだけだ．

日々のヘルスケア情報や診察，検査，治療，投薬などの**医療情報も，十分に匿名化されて医療，介護ビッグデータとして広く交換されている**．ゲノム解析に基づく免疫治療や治験なども一般的になっていて，30 年前は人々を苦しめた花粉症も，オーダメイド治療によりチフスなどと同様のもはや過去の病気なのさ．

マルウェアは撲滅するか

昔はアンチウィルスソフトウェアというのがあって，ソフトウェアの脆弱性を悪用してコンピュータに感染するのを防いでいたそうだね．もうないよ．もちろん脆弱性は決してなくならないけれど，ベンダにより安全性が証明されたアプリを管理された OS に入れて使うことがほとんどになってしまって久しい．今や，ごく一部の専門家しか任意のソフトウェアがインストールできる環境を使わなくなってしまった．**アンチウィルスソフトが売れなくなってしまった**セキュリティベンダはどんどんプラットフォーマー[☆3]に身売りをしてしまった．

同様に，**自動車はコネクテッドカーばかり**になってしまった．Car PKI による新型 CAN によって，外部からエンジンをかける車はもう車検を通らない．トラス省お墨付きじゃない自家用車で公道走れるのはガソリンで動くトヨマツの旧車くらいじゃないかな？

では，マルウェアの危険性はもうないのかって？

もちろん，不正行為はなくならない．2050 年になっても標的型フィッシングとオーダメイドスパイウェアは手を変え，品を変えて不正を続けている．機械が安全になっても，人間は予測不能で不正確で脆弱だからね．組織の内部犯行は，やはりなくならない．エージェントによる機械操作を防止するために，30 年前はよく使われていた**人間をテストする Captcha は廃れてしまった**．人工知能の発達に伴い解読精度が上がってしまい，高度化のインフレが止まらなくなって廃れてしまったからだ．代わりに，生体認証基盤による匿名の ID 連携により，誰だか分からないけれど，今生きている人間であることは確実に分かるようになってしまったというわけ．

生き残るのは誰か

さて，ポスト量子コンピュータの社会はどうなったのかって？

人類の中で最も脳容量が大きく，頑強な体躯を有して高度な石器を使いこなしたネアンデルタール人は 4 万年前に絶滅し，代わりに力も弱く狩りも下手なホモ・サピエンスが生き残った[☆4]．強いものや優れたものが生き残るとは限らないのだ．

結局のところ，2050 年，なんと **RSA 署名による公開鍵証明書は今も現役**である．量子コンピュータの需要は，一部のプラットフォーマーと真理省，愛情省などの省庁にとどまっていて，まだ一般のユーザが手にするほど市場価値が高まってはいない．耐量子技術として期待されていた格子暗号は，すでに技術的には成熟していたけれど，コストとそれに見合う市場価値がまだ認められないでいる．RSA 暗号だけではないよ，**電子メールも FAX も Fortran[☆5] も Java もまだ残っている**．高い技術や優れたアルゴリズムが必ずしも生き残るとは限らない．

いいじゃないか，そして，2050 年の今日も，私はいつものスローガンを三唱して 1 日を始めるのだった．

「戦争は平和なり
自由は隷従なり
無知は力なり」[☆6]

（2020 年 1 月 14 日受付）

☆3 2050 年のプラットフォーマー Baidu（百度），Alibaba（阿里巴巴），Tencent（テンセント）．

☆4 更科　功「絶滅の人類史　なぜ「わたしたち」が生き延びたか」（NHK 出版，2018）によるとネアンデルタール人の脳容量は約 1550cc，現代のホモ・サピエンスは約 1350cc．

☆5 竹内郁雄「当たらぬも八卦」（情報処理，Vol.1，1991）では，30 年前にソフトウェアというのは文化だから，Fortan は 2020 年にも残る，と予言して的中させている．

☆6 ジョージ・オーウェル「一九八四年［新訳版］」（ハヤカワ epi 文庫，高橋和久（翻訳），2009）

■菊池浩明（正会員）　kikn@meiji.ac.jp

2013 年明治大学総合数理学部先端メディアサイエンス学科教授．国立研究開発法人理化学研究所革新知能統合研究センター客員研究員．電子情報通信学会，日本知能情報ファジィ学会，IEEE, ACM 各会員．本会フェロー．

■須賀祐治（正会員）　suga@iij.ad.jp

（株）インターネットイニシアティブ セキュリティ情報統括室 シニアエンジニア．博士（工学）．CSEC 研究会幹事．CELLOS 幹事．CRYPTREC TLS 暗号設定ガイドライン WG 主査．2004 年度山下記念研究賞．SUG founder.