参考資料２

ICT サイバーセキュリティ政策分科会（第８回）議事要旨

１．日　時）令和６年５月 27 日（月）14：00～16：00

２．場　所）WEB 開催

３．出席者）
【構成員】
後藤主査、新井構成員、上原構成員、栗原構成員、小山構成員、辻構成員、蔦構成員、盛合構成員

【オブザーバー】
内閣官房内閣サイバーセキュリティセンター、内閣官房サイバー安全保障体制整備準備室、デジタル庁、経済産業省、地方公共団体情報システム機構

【総務省】
山内サイバーセキュリティ統括官、豊嶋大臣官房審議官（国際技術、サイバーセキュリティ担当）、小川サイバーセキュリティ統括官室参事官（統括担当）、酒井サイバーセキュリティ統括官室参事官（政策担当）、佐藤サイバーセキュリティ統括官室企画官、道方サイバーセキュリティ統括官室企画官、牧野サイバーセキュリティ統括官室統括補佐、井上サイバーセキュリティ統括官室参事官補佐

【発表者】
篠原直行（国立研究開発法人情報通信研究機構（NICT））、清本晋作（株式会社 KDDI 総合研究所）、
四方順司（国立大学法人横浜国立大学）、高江洲勲（三井物産セキュアディレクション株式会社）、
沖本彰（KDDI 株式会社）

４．配布資料
資料８－１　耐量子計算機暗号（PQC）と NICT の研究開発（NICT）
資料８－２　「安全な無線通信サービスのための新世代暗号技術に関する研究開発」について（KDDI 総合研究所、横浜国立大学）（一部非公開資料）
資料８－３　生成 AI はサイバーセキュリティ領域にどのような影響を及ぼすか（新井構成員）（非公開資料）
資料８－４　生成 AI とセキュリティ（三井物産セキュアディレクション）
資料８－５　KDDI のサイバーセキュリティ対策と AI 活用（KDDI）
参考資料１　ICT サイバーセキュリティ政策分科会第５回　議事要旨
参考資料２　ICT サイバーセキュリティ政策分科会第６回　議事要旨

5．議事概要
（１）開会

（２）議題
◆議題「新技術の進展に応じたサイバーセキュリティ対策の取組について」、「（１）量子計算機の進展に応じた対量子計算機暗号の研究開発」、NICT 篠原氏より資料８－１、KDDI 総合研究所清本氏、横浜国立大学四方氏より資料８－２を説明。

◆構成員の意見・コメント
後藤主査）
全体の考えとして、現時点では量子コンピューターの脅威は生じていないとのことだったが、今後量子コンピューターの性能が向上していく中で耐量子計算機暗号、高機能暗号の作成のキャッチアップの度合いに関してはどのようにお考えか、暗号技術が進展すればどのような量子コンピューターが出てきても問題がないのか、あるいは常に追いかけ合いが必要なのかについて伺いたい。

NICT　篠原氏）
暗号技術開発は基本的にいたちごっこが続くことはやむを得ない。量子コンピューターを使うと RSA 暗号や楕円曲線暗号が Shor のアルゴリズムで高速に解かれることは知られているが、今のコンピューターで高速に解ける方法が存在しないかということも分かっておらず、量子コンピューターを使わなくても速く解けてしまうこともあるかもしれない。これは現在の暗号だけでなく、耐量子計算機暗号にも言えることである。

格子問題は量子コンピューターで高速に解ける可能性があるとされた論文が出たこともあり、今後もこういったものは出てくるため、継続的な研究開発と検証は必要になると考える。

横浜国立大学　四方氏）

公開鍵暗号やその高機能暗号に対して、いつ何が出てくるか分からない量子コンピューターの脅威に対して、何を根拠に暗号の開発をするかというと、量子コンピューターで効率的に解けないとされている問題のクラスである NP 困難問題あるいはその関連問題を基盤に構成されている点である。NP 困難問題は今のコンピューターでも多項式時間では解けないと予想されており、量子コンピューターにおいても量子多項式時間で解くことができないという学術的な強い予想がある。一方で、NP 困難問題でも暗号の構成との相性があり、相性が良くないものを選ぶと実用性に欠ける。現在、格子問題は暗号構成と相性がよく、学会でも盛んに用いられている。なお、暗号構成の効率性を良くするのに特殊な構造を入れたり、パラメーターをできるだけ小さくしないと実用的にはならないが、そのような場合には新たな攻撃が出てくる可能性もある。つまり、暗号開発の大きな方向性については問題ない（追いかけっこはない）と考えられるが、実用性を考慮に入れる構成では継続的な解析とパラメーター更新は必要であると考える。

KDDI 総研　清本氏）

ある日突然研究のブレークスルーが起きる可能性も否定できないため、継続した安全性の評価や監視は当然必要である。その上で、実際の運用の場合には、十分なセキュリティマージンを取ったパラメーター（鍵の長さ、アルゴリズム等）にしていれば、兆候が出てから破られるまでの置き換えについての猶予期間はある程度担保できる。こういったセキュリティマージンをしっかり取る考え方と、今後の課題としてクリプトアジリティ等の議論があり、なるべく置き換えをしやすいような構成にしておくことも考えの一つにある。例えば、ハッシュ関数や複数の暗号の部品がプロトコルの中で使われていると、一つ一つ置き換える必要が生じるため、一つのアルゴリズムでシンプルにしていくようなアプローチも検討が盛んになっている。

盛合構成員）

PQC の高機能暗号の標準化について、知財に関しては、ロイヤリティーをいただいて産業の育成につなげていく戦略もあれば、オープンにすることで普及を優先し、日本の PQC に係る人材育成の方で勝ちを取りに行くなど色々あると思うが、どのような戦略をお考えか伺いたい。

横浜国立大学　四方氏）

PQC の基礎技術（鍵共有、公開鍵暗号、デジタル署名）の標準化は米国（NIST）が中心的に進めているが、今後、日本は高機能暗号の分野で標準化を含めて産業界で積極的に展開していくべきと思う。標準化の際には、3GPP、ISO、ITU-T など内容に応じた国際標準化に持っていく必要がある。
知財に関しては、標準化を進めるうえで敢えてパテントを取らずに普及を優先して推進する場合や、パテントをとってフリーにする戦略等、色々と考えられると思うが、大学、企業、コンソーシアム等、組織のポリシーにも影響されるため、どれが良いのか一概に言うのは難しい。ただ、セキュアな社会構築には、質の高い暗号技術をできるだけフリーで使える状況に持っていかないといけないと思う。儲けるのはそれが付随するサービスをメインとするのが良いのではないか。これまで暗号技術で儲けることの難しさは実感しているところであり、世界の中で日本の産業技術力を主体としたアピールとし、暗号技術はそれら産業と連携しながら広く展開していくことが良いと考える。

小山構成員）

大変頼もしく、将来が明るいなと思いながらお話を聞いていた。ところで、暗号化した保護情報が危殆化する場合に、過去に通信傍受等で保存された情報についても、可能な限り情報漏洩リスクの最小化を行いたい。特にインターネット通信は国外経由の通信も多く、共通鍵を 2 倍以上の長さにする対策を打つまでの間に取られていた情報保護の対策について、何か良い方法はあるのか、量子コンピューター対策の観点等から助言をいただきたい。

KDDI 総研　清本氏）

いわゆるストアゼンデクリプトのような、将来解読が可能になるまで保存しておくという脅威は昔から指摘されている。例えば、ヨーロッパなどではガイドラインの作成に取りかかっているが、その中でも早期に PQC を用いる方針とされている。ただ、PQC はできて間もない技術であるため、従来の暗号化とのハイブリッドで運用して将来の脅威に備えるアプローチになると考えられる。共通鍵暗号については、今のうちから鍵を 2 倍にしておくというのは一つの選択肢であるが、対策を行う分だけコストは発生するため、情報資産の価値に鑑みての対策が必要となる。例えば、20～30 年後には無価値になる情報であれば通常の対策とする、その頃であっても解読されては困るのであれば今から鍵を長くするという対策にならざるを得ない。

上原構成員）

コメント

NISTにおいて、PQCの特に基礎的な部分の標準化が進められ、ある意味決着がついているような空気もあるが、いくつか最終ラウンドにまで残ったアルゴリズムが破られる事件もあった。こうしたことも踏まえると、PQCに関する研究は、未だ予断なく様々な面から検討を続けなければならないフェーズにあって、安全性評価に関する研究開発投資を怠ることはできないと感じた。

また、四方氏への御質問として、基礎の部分での新規提案は厳しく、高機能暗号で戦うことは1つの戦略であると思うが、これまでの高機能暗号の普及の仕方・され方を見ると、キラーアプリケーションがあったと思う。この取組は非常に先進的な研究であると承知しているが、一番実用に近いアプリケーションに対して、今どのくらいの位置にいるのかについて伺いたい。

横浜国立大学　四方氏）

高機能暗号は、基礎技術に比べて機能が付加されている分のオーバーヘッドが生じるため、アルゴリズムレベルの改良、ソフトウェア設計やハードウェア設計からの改良も、今後、実用性を高めていく上でまだまだ必要である。キラーアプリケーションについては、高機能暗号にも様々な種類があるため、一概には言えないが、無線通信の5G、Beyond 5G（6G）の観点からいえば、その特徴である高速大容量通信、多数接続通信、低遅延・高信頼通信の3つの特徴から整理するのが良いと思う。高速大容量通信や低遅延・高信頼通信はリアルタイムでは共通鍵暗号に頼らざるを得ないアプリケーションが多いと思うが、共通鍵暗号の柔軟な鍵配送に関しては、PQCの鍵配送や高機能暗号が有効ではないかと思う。一方、共通鍵暗号は基本的に一対一通信であるため、多数接続通信分野に関しては公開鍵暗号や高機能暗号のアプリケーションの出番が多いと思う。私の研究プロジェクトでも、アグリゲート署名や放送型の認証系など複数間での通信を同時に扱うことへの応用に注目しており、こうした応用分野に今後Society5.0やAI、クラウドなどが絡むと、PQCの高機能暗号のキラーアプリケーションとなっていくのではないかと考える。

蔦構成員）

一般論として量子コンピューター技術が発達すると、現在の暗号が危殆化するという話をよく耳にする。重要性が非常に高い基礎研究を行っている中、マネタイズが難しいとの話もあったが、予算不足で研究ができなくなるようなことがないように、国の方でもしっかりと予算措置をするなど支援しながら引き続き進めていただきたい。

◆議題「（2）AIの進展に応じたサイバーセキュリティ対策」、新井構成員より資料8－3、三井物産セキュアディレクション高江洲氏より資料8－4、KDDI沖本氏より資料8－5を説明。

◆構成員の意見・コメント

小山構成員）

生成AIに「橋渡し人材」的な役割や、分野横断の課題共有の役割を担わせたいと考えている。生成AIにサイバー攻撃のログや解析結果をインプットし、何が行われていたかを文書化し、更に攻撃元を探索するような試みが始まってと理解している。弊社のCSIRTでも一部で活用を模索している。更に一歩進めて、セキュリティが専門ではない一般の方々に対して、サイバー攻撃の状況を図示して解説したり、映像化したりすることで、自分や自社への脅威を理解しやすくし、サイバーセキュリティの普及啓発が進められると良いなと考えている。

蔦構成員）

AIについては、著作権、データ保護、ガバナンスについて重要性も高く盛んに議論されているが、セキュリティの文脈でも本格的な議論が必要になってきている印象。本分科会の成果物を見据えた話として、セキュリティ関連の文書ではAIも脅威がある旨簡潔に書かれる印象があるが、本日の話を踏まえるともう少し具体的に様々な脅威等に触れてもよいのではないか。

質問として、AI vs AIのサイバー攻撃・防御のシミュレートもできるようになっているという印象があるが、例えば将棋などでは、AI同士を対戦させて人間が普通思いつかない戦術が考案され、かつそれを人間が活用してきていると認識している。サイバー攻撃、サイバーセキュリティについても同じ事が言えるか。同じ事が言えるとして、バッドアクターは制約なくAIを利用して研究をするが、一般の研究者はそうした制約なく研究を進められるのか、それによる差が更なる脅威となる恐れはあるのかについて伺いたい。

新井構成員）

制約のないAIを攻撃者が使用する一方で、研究者は制限のあるAIを使用する差はあり、例えば、フィッシング

やフェイクニュースの検出目的に AI が使えないかという研究をすると、攻撃者は偽動画を生成できるが、研究者は倫理上問題のある動画生成はできないため、訓練データを自ら作るといった活動に制約ができてしまうことになる。その事によって、検出の精度が下がってしまうといった影響がおよぶ可能性があり、言い換えると AI vs AI を実現させても能力差が出てしまうことも十分考えられる。

上原構成員）

AI を使ったセキュリティ技術(AI for Security)と AI を使うことによるリスクや AI そのものを守るためのセキュリティ(Security for AI)が両方語られたと思うが、今は AI for Security を強力に推すべき場面であって、Security for AI は最低限のリスクヘッジを除いては後回しで良いのではないかと思う。AI を攻撃に活用する動きが進むと守る側はどんどん不利になるため、AI を活用して守りを固める方向に目一杯アクセルを踏んでおくべきだという認識を持っている。

蔦構成員）

AI も活用した不正検知について、最近規模が大きい内部不正が報道されることも多いため、不正検知による未然防止、事後対応の重要性がますます高まっていると感じる。一方で、そこに AI を活用すると、どうしても従業員に対する強めの監視や、AI による評価（プロファイリング）に繋がるよう思うので、プライバシーとの兼ね合いも改めて整理する時期に来ているのではないか。

盛合構成員）

高江洲様へ質問
AI セキュリティに関するガイドラインが既に各国から出ているが、日本の国益を守るという観点でどのような点に配慮し、何を留意すべきか。

三井物産セキュアディレクション　高江洲氏）

今後、LLM を使わないという選択肢はなく、うまく利活用をして様々な業務を自動化していくことになる。LLM のセキュリティ自体を過度に気にすることで、利用促進を阻害するようなことは起きてはならない。
ただ、重要なリスクを放置すると甚大な影響を及ぼす可能性があるため、LLM に係るリスクに濃淡をつけた上で、特に攻撃を受けるリスクやインシデントが発生するリスクなどに順位的に対策していくといったように、実態に即したガイドラインの整備が重要。

後藤主査）

沖本様に質問。ネットワーク監視という実務に AI を活用されているとのことだが、その具体的な効果や課題、その他の見込みや状況について教えていただきたい。

ＫDDI 沖本氏）

2016 年から自動化についてプレスで公表している。人的な部分での作業の効率化は 4〜5 割となり、人員が半分で済むということになる。作業時間も人手で行う場合の半分となったが、AI のルールベースに新規の追加が生じたことにより運用が少し複雑になってしまった。また、検知精度に関しては５〜８割上昇しているが、ある意味クリーニングした後のデータであるため精度は高くなるもので、通信事業者の課題としては、精度を高く保ち、かつ、検知漏れが無いようにする必要がある。抜け漏れなく早く検知するには、まだ人の手が必要である。AI の進歩とともに完全自動化を部分的にであれ、いかに入れていくかが課題。

(3)閉会

以上