SQAT® SECURITY REPORT

2019 年 9 月号

株式会社ブロードバンドセキュリティ
セキュリティサービス本部
東京都新宿区西新宿 8-5-1 野村不動産西新宿共同ビル 4F
TEL：03-5338-7417　FAX：03-5338-7435
https://www.bbsec.co.jp/

知る・守る
続ける

BBSec は内閣サイバーセキュリティセンターの
「サイバーセキュリティ普及啓発」に賛同しています

はじめに

株式会社ブロードバンドセキュリティ
セキュリティサービス本部 本部長
齊藤 義人

本レポートは、株式会社ブロードバンドセキュリティ（以下、BBSec）の脆弱性診断サービス「SQAT®」における2019 年上半期（1 月～ 6 月）の膨大な診断結果からデータを抽出し、集約したものを、当社のエンジニアらの感性も交えてアウトプットしたレポートです。主にサイバーセキュリティのトレンドや展望についてお楽しみいただくことができる内容となっております。

次世代コンピュータとして様々な国の政府が重点分野に指定、企業も開発競争に参入するなど、近年国内でも関心が高まってきている量子コンピュータ。現在使われている暗号技術は、約 10 年後に実装される見込みの量子コンピュータによって破られる可能性が高いとされています。「まだまだ先の話だから、この件は後回しにしておこう」では、済まなくなるでしょう。耐量子暗号の標準化動向やセキュリティの観点も交えて、有識者とともに語らいます。

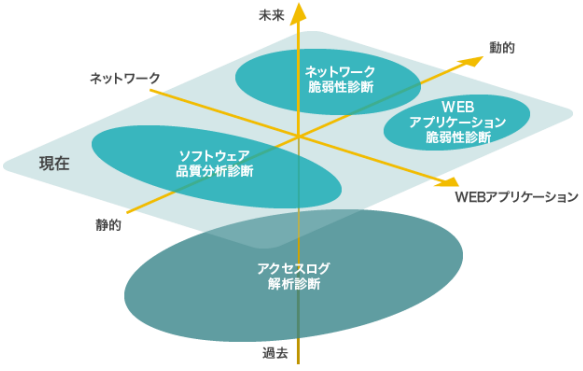
想像してみてください。外部ネットワークに繋がれ自動運転機能が搭載された自動車が普及し、事故の確率がゼロに等しくなった社会を。逆も想像してみてください。セキュリティ対策が不十分なせいで制御不能になった車が、事故の確率を上げてしまった社会を。今後の動向が気になる自動車業界のトレンドやハッキングに焦点を当てました。

脆弱性診断を受ける目的やきっかけ、診断後の対策の優先順位付けなどは、保有する資産やセキュリティポリシー、組織の経営方針によって異なるでしょう。多岐に渡る業種、ひとつとして同じ環境はない様々なシステムの診断を多数実施し、お客様とも密に接する当社診断員だからこそ知り得る「秘訣」を集約しました。

本レポートが、読者の皆様のセキュリティ対策における有益な情報としてご活用いただけることを願ってやみません。それこそが「便利で安全なネットワーク社会を創造する」をモットーに掲げる BBSec の使命であると考えております。

SQAT®（Software Quality Analysis Team）とは
～スペシャリスト集団が組織の脆弱性対策をトータルに支援～

「SQAT®」は、BBSec がご提供する脆弱性診断サービスです。エンジニア、コンサルタント、ホワイトハッカー等から編成された精鋭チームが、あらゆる側面から網羅的な診断を実施。スペシャリストのノウハウを結集して組織の情報システム強化をお手伝いします。お客様は金融機関・インターネット事業者などの民間企業から、官公庁をはじめとする公共機関まで幅広く、これまでに延べ 4,300 組織、22,300 を超えるシステムで利用されています。



CONTENTS

量子コンピュータの実用化と耐量子暗号の標準化動向
～未来は遠く、それでいて近い～

通信の安全性に特化した技術として普及している暗号技術。コンピュータの進化によって、そう遠くない未来には現在普及している暗号技術は破られてしまう可能性がある。このシナリオに抗うため、日夜研かれし頭脳を駆使して挑戦を続ける研究者たちがいる。その中のひとりである、東京大学の縫田 光司氏をお招きし、当社セキュリティサービス本部でアナリストを務める芦原聡介と様々な角度から暗号技術の可能性を語り合っていただいた。

量子暗号と耐量子暗号の違いについて

芦原：まずは対談の企画段階で、量子コンピュータの実用化の話題が候補に挙がり、そこから派生して米国政府の耐量子暗号の標準化動向などにも触れたい、となったのですが、社内で検討していくうちに「そもそも量子暗号と耐量子暗号を混同している方もいるのでは？」という疑問が生まれました。

縫田：たしかに、混同されることも多いです。単純に字面だけでいうと、日本語には“耐”が付いているだけ、英語でも Quantum cryptography と Post - Quantum cryptography でして、「“耐”“Post”が付いているほうが改良版」と捉えてしまう方も結構見受けられます。実際は全くの別物で、量子暗号というと量子コンピュータを使った暗号化技術を指すこともありますが、実際には量子鍵配送、つまり量子力学の原理を利用して暗号化に使用する秘密鍵を安全に相手に送り共有するための技術を指す場合が多いです。

芦原：そうですね。量子鍵配送に関しては、ITU-T で Y.3800 勧告として承認され、国際標準の骨格に日本の技術が強く反映されていることが先日ニュースになりましたね。それに対して、耐量子暗号のほうは、量子力学の原理が実装された新しい型のコンピュータ、すなわち量子コンピュータに対抗するための技術のことですよね。つまり、暗号を使用する自分は量子コンピュータを使っていなくても、攻撃者のほうは量子コンピュータを使えるという攻撃モデルを想定しています。そんな条件でも、解読することができない暗号技術のことを耐量子暗号といいます。ですので、耐量子暗号は、現在普及しているコンピュータを使って実装するものです。

高機能暗号、耐量子高機能暗号について

芦原：次にセキュリティの観点からすると、暗号はあくまでセキュリティを実現するためのひとつの手段であり、コストがかかるものというイメージがあります。こういったネガティブなイメージを払拭できる話をしたくて。そうですね…、まずは高機能暗号について話をしていきたいと思うのですが。

縫田：普通の暗号技術は、暗号化や認証技術など通信の安全性を守るのに特化したものです。高機能暗号と呼ばれる技術は、比較的新しい技術でして、安全性はもちろんあるのですが付加的な機能も充実させようという技術です。高機能暗号の例を挙げますと、準同型暗号[*1]（次ページ図１参照）というものがありまして、暗号文がふたつ与えられた際に平文や秘密鍵なしで計算できる技術です。これは平文が仮に数値だったとすると、暗号化を解いて足して暗号化しなおすのではなく、暗号文のままで中身を加算できます。単なる安全性だけではなく、機能としてもより便利なものになっているということになりますね。これは一例であって、他にも検索可能暗号[*2]、関数型暗号[*3]などといった技術もあります。

芦原：高機能暗号を企業で利用するという話ですと、自社でだけ使うようなシステムなら暗号化の必要はないと思いますが、例えばクラウド上のシステムなど、データ処理を外部委託するような環境の場合ですよね。不正だったり、事故だったりがあったとしても、安全性が保たれるようにしたい。暗号化技術はこういった状況で必要になってくる。

縫田：おっしゃるとおりで、クラウドの利用者側としては安全だと思いたいけれども、必ずしも言い切れないと思う人もいる。ですが、暗号化した状態でクラウドにデータを預けておいて、統計的な処理をするとして、暗号化したままで実現できるようになるなら完全には信用できないと思われるクラウド環境だったとしても、見られることはないだろう、と思える。

芦原：もし具体例を挙げるとしたら、どのような高機能暗号の利用の仕方がありますか？法的な理由などで、データ処理を外部委託したくても平文では外に出せない場合も考えられますよね？

縫田：そうですね…。例えばビッグデータ解析をするとき、個人の活動の履歴や、病歴、企業秘密、特許のアイデアなど、あまり外部に見せたくないようなデータを分析します。こういうときに先ほど言ったような準同型暗号を使えば、暗号化したままで分析を行うことができる。情報の利活用とプライバシーを守ることの両立になりますね。

芦原：準同型暗号ですと、既に実装されているものもありましたよね。準同型暗号を使ったソフトウェアが出ていて、使い始めている企業もあったと記憶しています。

縫田：この“高機能暗号”に先ほどまでお話をしていた“耐量子技術”が合わさると、安全性がより強固なものになります。それが“耐量子高機能暗号”というものですね。耐量子暗号と高機能暗号には、数学的な仕組みに共通点が多いという相性の良さもあります。

量子コンピュータの起源と研究について

芦原：耐量子暗号は、“量子コンピュータが実装されたときに対抗するための技術”といったことを話しましたが、ともすると量子暗号やこれを搭載した量子コンピュータが悪者であるかのように捉える方もいるかもしれません。そうではなくて、高性能なものを駆使して世の中を便利なものにしたいといった前向きな動機で研究が始まったわけですよね。