SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

Web PKI 業界が耐量子計算機暗号への移行を急がなくて良い 3 つの理由
Three Reasons why Migration to PQC is not an urgent issue for Web PKI

伊藤　忠彦 *　　肖　俊廷 *
Tadahiko Ito　　Junting Xiao

キーワード Web PKI、耐量子計算機暗号、Cryptographic agility

あらまし

Web PKI 業界においては、かねてより Cryptographic agility の向上に取り組んでおり、証明書有効期間の短縮や、ソフトウェアアップデートの迅速化などに取り組んできた。これらの取り組みの結果、Web PKI 業界においては、耐量子計算機暗号への移行をそれほど急がなくても良い状況となっている。本書では、その状況を説明し、また他業界における注意点について考察を述べる。

本書においては PKI を「公開鍵暗号を利用するためのインフラ」とし、また Web で公開鍵暗号を利用するためのインフラを Web PKI とする。より正確には、Web PKI は、CA/BForum による Baseline Requrements [1] を満たし、多くの代表的な web ブラウザのトラストプログラムが要求する基準を満たし、web サーバを認証するために利用可能な PKI とする。

量子コンピュータへの研究開発に伴い、従来のコンピュータで解けない大きな合成数の素因数分解問題や楕円曲線上の離散対数問題を解くことが可能となることが予想されている。それにより、それらの問題を安全性の根拠とする暗号技術が安全でなくなる可能性が指摘されている。そこで、大規模な量子コンピュータが実用化される時代においても安全な、耐量子計算機暗号技術 (Post-Quantum Cryptography, PQC) の研究開発が盛り上がりを見せている。

一方で、耐量子計算機暗号の標準技術が選定された後に、どのようなプロセスを経て既存暗号から耐量子計算機暗号へ移行するかという課題に対しては、課題整理の途上となっている。現在の課題整理においては、レトロスペクティブディクリプション (retrospective decryption) の脅威 [1] [2] が中心となり検討されており、なんらかの優先付けをした上で移行をするべきだと考えられている [3]。

本書では、ライフサイクルの長いデータや（秘匿目的の）暗号化データについては優先して耐量子計算機暗号等への移行を検討する必要がある一方、Web PKI 業界における認証目的の公開鍵暗号においては移行の優先度を下げることが可能であるとの分析を、3 つの理由とともに述べる。

加えて、他の暗号アプリケーションを利用する業界に向けて、長期的及び短期的な提言を述べる。

参考文献

[1] CA/Browser Forum, “Baseline Requirements for the Issuance and Management of Publicly - Trusted Certificates (Version 1.8.0)”, August 2021.

[2] W. Beullens, J.-P. D’Anvers, A. Hülsing, T. Lange, L. Panny, C. de Saint Guilhem, and N. P. Smart, “Post-Quantum Cryptography - Current state and quantum mitigation”, ENISA Report, vol. 2, pp. 3-29, May 2021.

[3] W. Barker, and M. Souppaya, “Migration to Post-Quantum Cryptography”, White paper, NIST NC-CoE, June 2021.

* セコム株式会社, 〒 181-8528 東京都三鷹市下連雀 8-10-16. SECOM CO., LTD., 8-10-16, Shimorenjaku, Mitaka, Tokyo 181-8528, Japan.

[1] 攻撃者は現存するデータをとりあえず保管しておき、将来において暗号解読可能な量子コンピュータを用いてそのデータに対して攻撃するというようなもの。