長崎県立大学
UNIVERSITY OF NAGASAKI

シーボルト校　研究紹介 Vol.12

長与町に立地する長崎県立大学シーボルト校。
すぐ近くの大学でどのような研究が行われているかをシリーズで紹介していきます。

星野文学　教授

暗号の理論と実装の研究

－情報システム学部　情報セキュリティ学科－
https://sun.ac.jp/researchinfo/hosh-fumi/
星野文学　教授紹介ページ▶

技術が目まぐるしく進歩している現代では10年前の常識が現在ではほとんど通用しないという事が良くあります。実は暗号技術のトレンドもこの10年で大きく変化しています。

例えば2012年にOnline Trust Allianceという団体によって常時SSL/TLS化という概念が提言されました。現在ではほとんど全ての主要ウェブサイトがこの提言を採用しており、Googleの透明性レポートによると85%～95%のページがHTTPSで読まれている事が分かります（図1）。

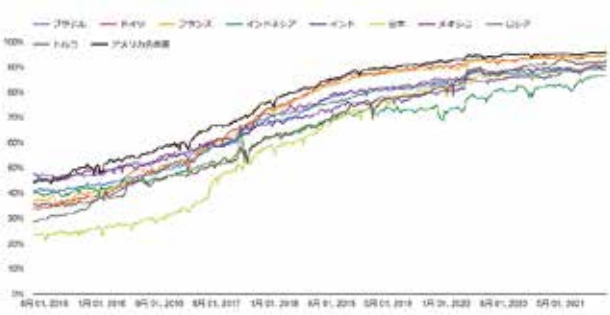

図1　HTTPS経由で読まれたページの割合（Windows Chrome）
出典　https://transparencyreport.google.com/https/overview

つまり、ほとんどのインターネット上の通信に公開鍵暗号とデジタル署名が使用されており、こうした技術は既に必要不可欠なインフラの一部になっています。

また、ビットコインに代表される暗号資産の隆盛も暗号技術を取り巻く状況に強い影響を及ぼしています。ビットコインには主にデジタル署名とハッシュ関数という暗号技術が用いられますが、イーサリアムやジーキャッシュのような後発の暗号資産ではより高度な技術が使用されます。

それから、それまで難しいと思われていた完全準同型暗号と呼ばれる暗号技術が2009年に理論的に実現可能である事が分かり、この10年で実用化に向けた研究が沢山行われています。

さらに、特定の計算において従来の計算機の能力を遥かに凌駕する量子計算機の実現が近づいていると言われています。量子計算機によって、現在使用されている公開鍵暗号やデジタル署名の幾つかは破られることが知られています。量子計算機に対して強い公開鍵暗号やデジタル署名を設計する事が最近の暗号研究のトレンドとなっており、米国標準技術研究所（NIST）が標準化を行っています（図2）。

現在の標準化候補		
ベースとなる技術	公開鍵暗号／鍵交換	デジタル署名
格子暗号	CRYSTALS-KYBER NTRU/SABER FrodoKEM/NTRU Prime	CRYSTALS-DILITHIUM FALCON
多変数多項式暗号		Rainbow GeMSS
符号	Classic McEliece HQC/BIKE	
同種写像	SIKE	
ゼロ知識証明		Picnic
ハッシュ関数		SPHINCS+

図2　耐量子計算機暗号の標準化動向

星野研究室では、こうした最新の暗号技術について理論から実装まで幅広く研究しています。暗号の研究には多少数式を使うので、煙たがられている傾向があるかもしれませんが、暗号が必要不可欠なインフラだという事が理解されてきているので10年後にはこのトレンドは変わるかもしれません。