特集

理科大のセキュリティ研究

安全なネットワーク社会を支えるセキュリティ技術

東京理科大学 工学部 情報工学科 准教授 藤沢（ふじさわ） 匡哉（まさや）

ネットワーク技術が発展し，様々なものがネットワークに接続して，お互いに情報をやりとりできるようになっている．このようなネットワーク社会において安全に様々な活動をするためには，セキュリティ技術は欠かせない技術となっている．

セキュリティの基本的な考え方として，機密性・完全性・可用性の３つを維持することが重要であると，国際標準 ISO/IEC 27000 によって定義されている．機密性とは，「情報へのアクセスを認められた者だけが，その情報にアクセスできる状態を確保すること」であり，その達成のためには，認証技術，アクセス制御，暗号化技術等が利用される．完全性は「情報が破壊，改ざん又は消去されていない状態を確保すること」であり，その達成のためには，ディジタル署名技術，電子透かし技術，アクセス履歴管理等が利用される．また，可用性は「情報へのアクセスを認められた者が，必要時に中断することなく，情報及び関連資産にアクセスできる状態を確保すること」であり，その達成のためには，システムの多重化や，クラウド化が必要となる．

このように情報セキュリティの中核となる技術には，暗号化技術，認証技術，ディジタル署名技術，電子透かし技術，アクセス制御技術があり，暗号化技術の基本原理の発展として残りの技術も発展してきた．

多様なシステムが構築されるようになると，セキュリティの概念として新たな要素の追加が必要となってきた．国際標準 ISO/IEC 27002 では，前述の情報セキュリティの３要素に加えて，真正性「システムの利用者が，確実に本人であることを確認し，なりすましを防止する」や責任追跡性「ある実体の動作が，その動作から動作主の実体まで一意に追跡できることを確実にすること」が求められる．これらについては，ディジタル署名技術や零知識証明技術によって達成可能となる．このように，暗号技術，ディジタル署名技

術，認証技術，電子透かし技術等は，多様なシステムにおいて生じる様々な用途におけるセキュリティに対応できるように高機能な技術へと発展している．

ここまで情報セキュリティにおける暗号技術と関連する技術について概説してきたが，以降では本学の各分野の研究者によって研究されている様々な角度からのセキュリティ研究について簡単に紹介する．

まず，特集記事の紹介の前に，本研究室における研究について簡単に紹介する．量子計算機の研究が近年急速に発展しており，十数年後～数十年後には，十分に大きなビット数の量子計算機が実現すると予想されている．現在主要に利用されている公開鍵暗号技術やディジタル署名技術は，十分大きな量子計算機を用いることによって解読されることが報告されている．そのため，次世代の暗号方式として耐量子計算機暗号が注目されており，NIST において標準化の検討が進められている．本研究室では，耐量子計算機暗号の 1 つである誤り訂正符号を用いた McEliece 暗号について研究しており，処理の効率化やサイドチャンネル攻撃に強い方式の検討を行っている．

以降では本特集記事で取り上げたセキュリティ研究の 5 つの各記事について簡単に紹介する．詳細については各記事を参照していただき，セキュリティ研究の面白さや社会的な貢献について読み取って欲しい．

① 漏洩に強いセキュリティ

情報セキュリティの基本的な概念について平易に紹介している．ネットワーク上では正しい利用者なのかを判定（認証）する必要があり，それらの情報は重要で漏らさないようにしなければならない．多くの人が複数のサービス，システムを利用しているが，それらの内の一部に関する情報が漏れたとしても，連鎖して他への被害を増大させない仕組みについて考える内容となっている．

② 視覚復号型秘密分散法と組合せデザイン

組合せデザインは，実験計画法，ソフトウェアテスト，符号化技術等に応用されている数理的な概念であり，その構成には有限幾何や代数幾何学が用いられている．この概念は暗号の分野でも応用されており，本記事では，応用例の 1 つとして視覚復号型秘密分散法への適用について解説している．視覚復号型秘密分散法は秘密分散法の 1 つである．秘密分散法は秘密を複数に分散することによって安全に扱えるようにする技術である．分散した値のうち，ある個数までであれば攻撃者に盗まれたとしても秘密が漏れることはないという性質を持っている．通常，秘密分散法の暗号化や復号には計算機が必要となるが，視覚復号型秘密分散法は視覚的に秘密情報を復元でき，計算機が不要な方法となっている．そのために工夫が必要となるが，組合せデザインを上手く利用することにより，この問題を解決している．

③ 暗号に対する攻撃法

暗号方式の安全性は考え得るすべての攻撃に対して評価する必要がある．そのようなことから，攻撃法の研究が発展するが，より安全に利用できる暗号方式も発展することに繋がるので，非常に重要な研究テーマである．本記事では共通鍵暗号の攻撃法として知られている差分攻撃について具体的な例を示しながら解説している．

④ 秘密計算

ネットワーク上から膨大なデータを収集できるようになっており，それらを用いて分析することで有益な情報を得ることができるようになっている．しかし，このような計算を 1 つの組織で実施するのはコスト的に厳しく，計算資源を共有化できるクラウド上で委託計算を行うことが増えてきている．この際に，プライバシー保護のために情報を暗号化していても，計算の際に復号して元の情報に復元すると，クラウドの内部不正者によって情報を盗まれる危険が残っている．そこで，暗号化したまま任意の計算ができる技術である秘密計算が近年注目されている．本記事では，それらの技術について応用事例なども含めて解説している．

⑤ AI セキュリティ

コンピュータの目覚ましい発展によって AI（Artificial Intelligence）が人間に代わって出来る仕事が増えてきており，多岐にわたる分野において様々なシステムへの導入が進んでいる．AI では，現実の大量のデータを用いて深層学習させることで，優れた推定精度を得ている．これに対して，学習データに不正なデータを混入させて学習モデルを操作する攻撃（データポイズニング）や AI の出力を基に逆に学習に用いたデータを推定する攻撃（モデル反転攻撃）等の AI 特有の攻撃が存在し，それらに対応した方法についての研究が必要となっている．本記事では AI 特有の攻撃のうち，モデル反転攻撃について具体例を示しながら，その対応について解説している．