特集
Special Feature

ハードウェアセキュリティの最新動向

編集にあたって

松本　勉 | 横浜国立大学／産業技術総合研究所
佐々木貴之 | NEC／横浜国立大学
石黒正揮 | 三菱総合研究所

近年，Industrie 4.0 や Society 5.0 の実現に向けて，IoT（Internet of Things）やサイバーフィジカルシステムが重要となってきている．このようなシステムのセキュリティを担保するには，ソフトウェアに加えて，ソフトウェアが動作するプラットフォームであるハードウェアについても，セキュリティが担保されなければならない．なぜなら，ハードウェアはソフトウェアよりも低いレイヤで動作するため，ソフトウェアでは，ハードウェアレイヤの脅威への対応が難しいためである．ハードウェアレイヤの脅威の例として，ハードウェアチップから漏れ出る電磁波の物理的な観測による暗号鍵の解析（1 章）や，意図的な機能の停止や情報漏えいを引き起こすハードウェアトロージャン（3 章），センサに対する攻撃（4 章）が報告されており，これらのハードウェアレイヤの脅威はシステムの安全性に大きな影響を与える．一方，ハードウェアを活用したシステムの堅牢化として，暗号化処理の高速化（2 章），セキュリティ機能の保護（4 章）や，ハードウェアを含むシステム全体のセキュリティ，たとえば，自動車のセキュリティの検討（6 章）が進められている．

また，世の中の動向を見ると，アメリカのセキュリティ機関である NIST がハードウェアセキュリティのベストプラクティスの検討を開始したり，日本においても経済産業省が発行しているサイバー・フィジカル・セキュリティ対策フレームワークにおいてハードウェアの信頼性が言及されたりと，ハードウェアセキュリティの重要性の認識が広まっている．

システムの基盤となるハードウェアのセキュリティの知見は，セキュリティ分野の読者に限らず，幅広い読者に有用であると考え，本特集を企画した．本特集では，ハードウェアに対する攻撃やハードウェアを利用したシステムの堅牢化など，ハードウェアセキュリティに関する最新動向を広く俯瞰する．本特集の構成は以下のようになっている．

(1) ハードウェアに対する物理攻撃

ハードウェアはシステムの信頼の起点であり，安全なシステムを設計し運用するために，ハードウェアに対する攻撃を理解する必要がある．
東北大学 本間尚文氏と上野嶺氏が，ハードウェアへの物理的なアクセスによる攻撃手法について整理を行い，具体的な攻撃手法について解説している．

(2) ハードウェアを用いた暗号処理の高速化

ハードウェアを用いたセキュリティ機能の強化として，複数の署名を集約して署名サイズを削減する

集約署名やデータを暗号化したまま検索が可能な秘匿検索などの高機能暗号の高速化が挙げられる．

横浜国立大学 坂本純一氏と吉田直樹氏が，高機能暗号に用いられる数学的操作のハードウェアによる高速化について，ハードウェアの実装例を基に解説している．

(3) ハードウェアトロージャンの脅威と検出

ハードウェアを用いてシステムを堅牢化するためには，ハードウェア自体が信頼できなければならない．この際，IC 製造のサプライチェーンにおいて，チップ設計者が意図しない機能（ハードウェアトロージャン）の混入が脅威として指摘されている．

奈良先端科学技術大学院大学／産業技術総合研究所 林優一氏と産業技術総合研究所 川村信一氏が，ハードウェアトロージャンの全体像を整理し，その発見手法について解説している．

(4) 計測セキュリティ

IoT システムやサイバーフィジカルシステムは，センサから情報を収集し，その情報に基づいてアクチュエーションを行う．よって，測定の妨害やセンサや認識アルゴリズムをだますような攻撃が行われると，システム全体に影響を与える．

横浜国立大学／産業技術総合研究所 松本勉（本特集のゲストエディタ）と産業技術総合研究所 鈴木大輔氏が，センサを用いたシステムモデルを解説するとともに，攻撃対象となるセンサやシステムに与える影響について整理している．加えて，問題解決に向けた複数のアプローチを挙げている．

(5) Trusted Execution Environment によるシステムの堅牢化

暗号化などのクリティカルな機能を保護するために，それらの機能と一般的なアプリケーションの実行空間を CPU によって分離する技術（Trusted Execution Environment, TEE）の活用が期待されている．

産業技術総合研究所 須崎有康氏と本特集のエディタである NEC／横浜国立大学 佐々木貴之が，TEE のコンセプト，複数の実装とその特性について整理している．加えて，TEE の活用が見込まれるユースケースの紹介がなされている．

(6) 自動車サイバーセキュリティの基本

通信機能を備えたコネクテッドカーが普及し始めているが，自動車が攻撃を受け，自動車の制御システムに異常が発生すると，重大な事故につながる可能性がある．

産業技術総合研究所 Camille Gay 氏が，車載ネットワークの概要や，実際の攻撃事例，自動車業界特有の課題について解説している．

以上のように，ハードウェアセキュリティの分野では攻撃と防御の両方の観点からの検討や，IC チップレベルからシステムレベルまでの検討が行われており，日々技術が進歩している．本特集で紹介したハードウェアセキュリティに対する取り組みが，安全・安心な社会の実現に貢献することを期待したい．

（2020 年 3 月 2 日）