

ム)によって、モバイル端末がコンピューターと同様にインターネットに接続され、さまざまなサービスが利用可能になると、モバイル端末からインターネットにアクセスする利用者が増加した。iPhoneやAndroidの登場によって、スマートフォンが急速に普及するとともに、モバイル向けの通信規格も4G、そして5Gへと進みつつあり、より高速・大容量な通信がモバイル端末でも実現できるようになった。モノがインターネットの多様なサービスに接続され、相互に情報が交換されるIoT (Internet of Things) も広がりつつある。従来は人やコンピューターがインターネットを介して接続され、情報やサービスを交換してきたが、自動車や家電などの個人の身の回りの物、あるいは電気やガス、交通設備などの社会インフラもネットワークに接続され、あらゆる情報が交換されるようになってきた。また、通信インフラの発展・普及に応じて、電子メールやウェブ検索、クラウド、動画やライブ配信などのプラットフォームや、eコマースやネット銀行、SNS (Social Networking Service)、電子政府などの多様なサービスが登場するようになった。これまでの文字ベースの情報から、画像や映像を含むさまざまな情報のやりとりが可能になり、これによって一方向の情報提供から、双方向のユーザー参加型のコミュニケーションへと、サービスが変遷してきた。インターネットを含むさまざまな情報システムやサービスの利用者は拡大し、同時にセキュリティやトラストの問題が認識されるようになってきた。

サイバー攻撃は、その目的や手法を変えつつ、社会に大きな被害と影響を与えてきている。マルウェア (不正プログラム) によるウェブサイトやデータの改ざんなど、個人や企業へのいたずら行為として始まった攻撃は、インターネットの普及に伴い深刻化してきた。攻撃の目的は、企業・組織への妨害や、個人情報や金銭の搾取へと悪質化し、攻撃手法もDoS (Denial of Service)・DDoS (Distributed Denial of Service) 攻撃や標的型攻撃、フィッシング詐欺など多様化した。近年では、スパイやテロ、国の重要インフラを狙った攻撃など、国家の関与が疑われる組織的な攻撃へと発展している。IoTや制御システムに対する攻撃は、情報漏えいやプライバシー侵害などにとどまらず、物理的な被害に直結し、時には人命にも大きな被害を与える可能性がある。しかも、ネットワークに接続されるモノの寿命は、これまで接続されてきたコンピューターなどに比べると格段に長くなり、そのセキュリティの確保は一層困難になりつつある。このような課題に対抗すべく、暗号技術やマルウェアの検知、認証技術をはじめとする、さまざまなセキュリティ技術による強化対策に加え、個人情報保護法などの制度面での対策が同時に進展してきている点も、セキュリティにおける重要な流れである。

また近年、社会への影響度の点で無視できないのは、情報システムや情報サービスにおける安心・信頼である、トラストである。情報技術がますます高度化し、情報システムや情報サービスへの社会の依存度が高まる中、フェイクニュースによる情報サービスや情報そのものへの不信感や、COVID-19の接触確認アプリによる個人情報漏えいへの懸念や国の監視・管理への不信感など、人々のトラストを揺るがす事態が生じている。情報技術の活用は社会と密接な関係があり、技術的な信用の担保だけではなく、人間の心理的な要素や、制度による保証などもあわせて、多面的に考慮することが重要になってきている。

[セキュリティ・トラストの俯瞰図 (構造)]

本区分の俯瞰図 (構造) を図2-4-2に示す。この図では、本区分の全体像を、基盤層、情報・システム・デバイス層、人・社会層の3層に分けている。基盤となる領域としては、心理学・経済学・人文社会学、数学・暗号技術・コンピューターサイエンス、教育・人材開発、法制度があり、これらがセキュリティ・トラスト分野において重要なベースとなる役割を果たしている。この土台の上に、悪意ある第三者の攻撃からの保護である情報システムや情報サービスのセキュリティ、およびそれらの想定する機能が安定して維持されると

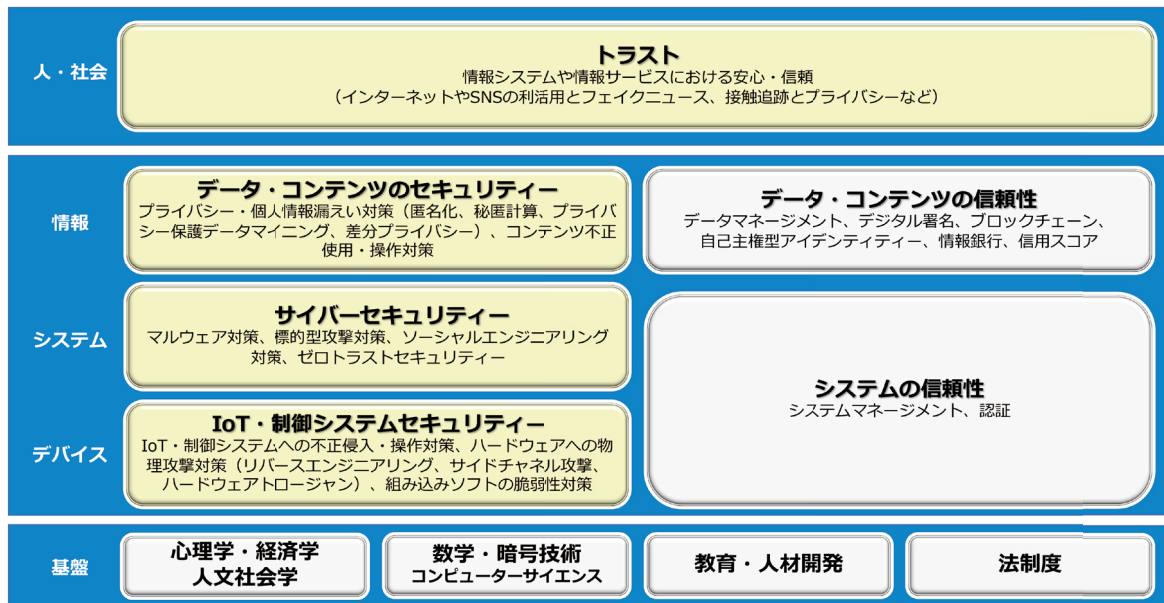


図2-4-2 セキュリティー・トラストの俯瞰図（構造）

いう広義の信頼性（ディペンダビリティ）に関する技術群を位置づけた。ここでは横軸を、セキュリティ技術と、信頼性を確保するための技術に分け、縦軸を、守る対象であるデバイス、システム、および情報に分けて示している。最上位の層としては、人・社会との関係に注目する層として、トラストを位置づけた。

本区分においては、以下の①から④までを研究開発領域として取り上げる。

① IoT・制御システムセキュリティ

パソコンやスマートフォンなどの従来の情報端末に加え、家電、医療、工場・インフラなどの産業用途、自動車・宇宙航空など、更なるIoT化の進展が見込まれている。一方、セキュリティのリスクは増大しており、ソフトウェアやハードウェア、ネットワークなど、広範かつ縦断的なセキュリティ確保が必要となってきた。

② サイバーセキュリティ

インターネットの進歩・発展の影で、インターネットを経由したサイバー攻撃は日々高度化を続けている。一方、既にインターネットは生活や産業など多くの社会活動が依存する社会インフラとなっており、そのサイバー攻撃への対策は、安心・安全な社会を実現する上で必要不可欠である。

③ データ・コンテンツのセキュリティ

パーソナルデータの活用は、「インターネットにおける新しい石油」とも評され、インターネット経済の発展の鍵となっているが、同時に、欧州を中心にプライバシー保護への要求も高まっている。また近年では、フェイクニュースと呼ばれる悪意を持った情報操作が社会問題化している。データ経済の発展には、セキュリティやプライバシーの保護とデータ利活用を両立する技術が重要である。

④ トラスト

近年、情報システムのセキュリティーに加え重要になってきているのが、情報システムや情報サービスにおける安心や信頼の概念の総称である「トラスト」である。情報技術がますます高度化し、情報システムや情報サービスへの社会の依存度が高まる中、注目が集まるトラストを、人間の心理、制度、および技術の側面から捉える。

本区分ではとりあげていないが、情報システムや情報サービスの想定する機能が安定して維持されるという広義の信頼性（ディペンダビリティ）に関する技術や仕組みも重要である。個別の内容については、ブロックチェーン、および自己主権型アイデンティティー（SSI:Self-Sovereign Identity）は「2.5.7 ブロックチェーン」を、情報銀行、および信用スコアは「2.1.9 社会におけるAI」、および「2.5.5 IoTアーキテクチャー」を参照されたい。

2.4

俯瞰区分と研究開発領域 セキュリティー・トラスト