2.4 セキュリティー・トラスト

情報サービスや情報システム、さらには人、社会をサイバー攻撃[1]から守るためのセキュリティーと、人や社会が情報サービスや情報システムを安心して利用できるよう信頼を確保するためのトラストという二つの側面から研究開発動向を俯瞰する。情報サービスや情報システムは進歩・発展を続けており、われわれの社会生活に欠かすことができない存在になってきている。これらを悪意ある第三者の攻撃から守るためのセキュリティー、および安心・信頼して利用するためのトラストが重要になってきている。

[セキュリティー・トラストの俯瞰図（時系列）]

本区分の時系列の俯瞰図を図2-4-1に示す。この図では、横軸が年代、縦軸が社会への広がりを表している。通信や制御システムなど「インフラ」が発展し、さまざまなものがつながるようになってきたこと、また多種多様な「プラットフォーム」が登場し人々が利用できるようになってきたこと、さらに社会の中で多岐にわたる「サービス」が展開されてきたことを示している。図中には、その時期に台頭した技術、および攻撃事案やその他のエポックをプロットしている。

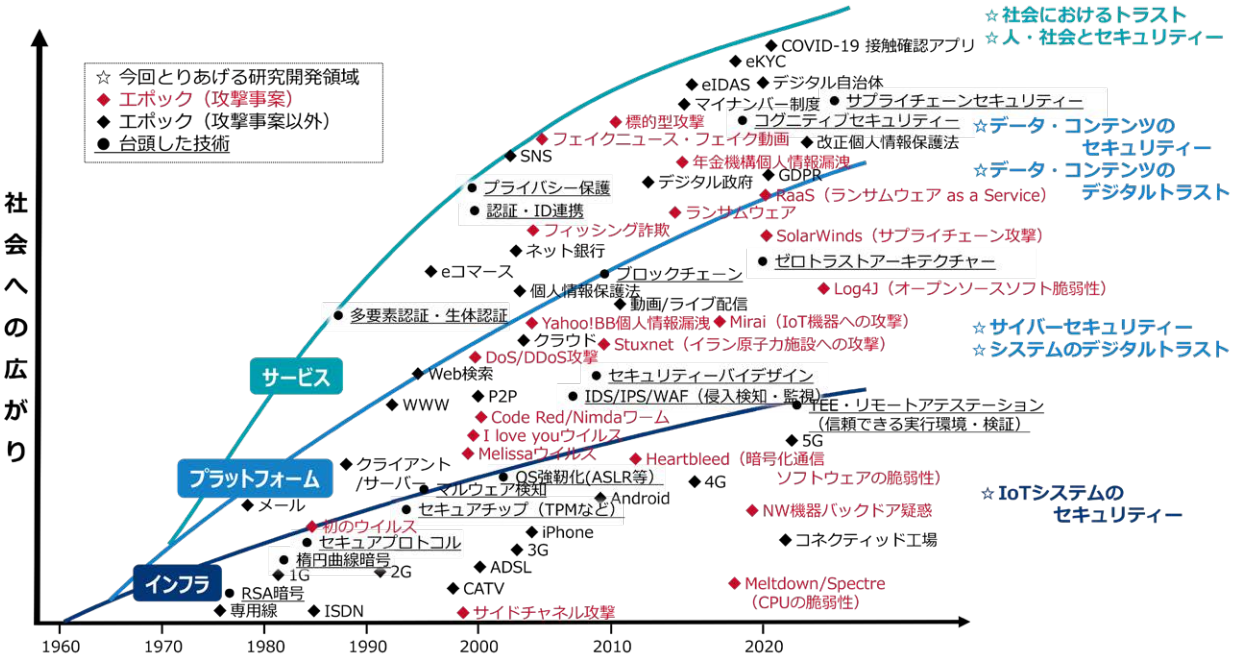

図 2-4-1　　セキュリティー・トラストの俯瞰図（時系列）

以下では、図2-4-1のインフラ、プラットフォーム、サービスの進展と、本区分で扱うセキュリティー、トラストの進展について概観する。

1　サーバーやパソコンなどのコンピューターシステムへの不正なアクセスや、個人、組織をターゲットとした電子メールや偽サイトなどにより、システムの動作妨害・停止・破壊や情報の搾取・改ざん・破壊などを行う攻撃で、標的型攻撃、ランサムウェア攻撃、ビジネスメール攻撃、DDoS攻撃、ソフトウェアの脆弱性を悪用した攻撃、ばらまき型メールによる攻撃、人を狙った攻撃などがある。

❶ インフラ・プラットフォーム・サービスの進展

1970年代のデータ通信は、主に専用線を利用して行われた。専用線は、企業や組織におけるコンピューターを直接つなぐ接続方式であり、利用者間でクローズドなデータのやりとりが行われていた。この状況を劇的に変えたのが、インターネットの登場である。ISDN（Integrated Services Digital Network）やケーブルテレビ（CATV）、ADSL（Asymmetric Digital Subscriber Line）、光回線の普及により、より高速・大容量なインターネット接続が可能になると、さまざまなサービスやコンテンツがインターネットを介して利用できるようになっていった。2000年代中頃になると、モバイル化の流れが加速していく。3G（第3世代移動通信システム）によって、モバイル端末が本格的にインターネットに接続され、メールなどのコミュニケーションサービスが利用可能になった。 iPhoneやAndroidの登場によって、スマートフォンが急速に普及し、スマートフォンからインターネットにアクセスする利用者が増加した。モバイル通信は4G、そして5Gへと進み、生活に必要不可欠な社会インフラとなっている。従来、スマートフォンやコンピューターがインターネットに接続されていたが、近年、モノがインターネットに接続される IoT（Internet of Things）が広がり、家電などの個人の身の回りの物から自動車や電気、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、サイバー空間とフィジカル空間の融合が進展している。さらに、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し、われわれの生活に必要不可欠なものとなっている。一方で、インターネットを介したサイバー攻撃による被害も増加しており、情報サービスや情報システムをサイバー攻撃から防御するためのセキュリティーや、人や社会が情報サービスや情報システムを安心・信頼して利用するためのトラストが重要視されるようになってきた。

❷ セキュリティー

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いる。マルウェア（不正プログラム）を使った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）攻撃や標的型攻撃など多様化した。データを暗号化し復元の見返りに身代金を要求するマルウェア（ランサムウェア）による被害が多発している。さらに、近年のランサムウェアは、データを搾取した上で攻撃先のデータを暗号化し身代金を支払わない場合には搾取したデータを公開すると脅す二重脅迫や、ランサムウェアの開発と実行が分業化されたランサムウェアサービス（RasS：Ransomware as a Service）に進化している。個人や企業を狙ったフィッシング詐欺も頻発しており、その件数は、毎年、過去最高を更新している[2]。

サイバー攻撃が多様化する中で、近年、人の脆弱性を狙った攻撃への対策の重要性が高まっている。これまでのサイバー攻撃では、デバイスやOS、システム、ネットワーク、データが狙われてきた。一方で、フィッシング詐欺では、フィッシングメールや偽サイトを用いて人をだまして重要な情報を搾取しようとしている。システムへの不正侵入でも、従来はシステムの脆弱性が狙われることが多かったが、フィッシングメールにより人をだましてパスワードを奪いシステムに侵入する事例も発生している。もう一つ重要性が高まっているものが重要インフラ施設やサプライチェーンなどを狙い、社会に大きな影響を及ぼす攻撃への対策である。例えば、2021年、米国の石油パイプライン施設のシステムがマルウェアに感染し、米国東海岸のガソリン価格が高騰するなど社会に大きな影響を与えた。サプライチェーンを狙った攻撃には、ある企業が攻

2 フィッシング対策協議会（https://www.antiphishing.jp/）を参照いただきたい。

撃を受けることにより、サプライチェーンに関係する他の企業にまで被害が及ぶケースと、マルウェアなどに感染したソフトウェアなどがサプライチェーンを介して広く配布されて、そのソフトウェアを利用する多くの企業にまで被害が及ぶケースがある。前者のケースでは、2022年に、自動車部品会社がランサムウェアの攻撃を受け、自動車製造会社にまで影響が及んだ。後者のケースでは、2020年に、ネットワーク監視ソフトウェアを提供する米国企業がサイバー攻撃を受け、ウイルスに感染したソフトウェアがサプライチェーンを介して世界中で利用されている同社のシステムに配信され、世界中の多くの企業に影響を与えた。オープンソースソフトウェア（OSS：Open Source Software）でもサプライチェーンを介した被害のリスクが顕在化してきている。2021年に発見されたOSSの脆弱性では、脆弱性を持つOSSが、さまざまな製品に導入されていたため、世界中の製品がサイバー攻撃のリスクに晒された。このように、重要なインフラ施設やサプライチェーン、OSSの脆弱性を狙った攻撃のリスクは増加しており、その被害は、攻撃を受けた施設や企業にとどまらず、二次被害、三次被害と大規模化し、社会に影響を及ぼしている。

このような脅威に対して、セキュリティーは、情報サービスや情報システム、さらには人・社会をサイバー攻撃から守る重要な役割を持っている。進化するさまざまなサイバー攻撃に対抗すべく、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ー技術による対策強化が進められてきている。技術的な対策以外にも、製品の企画や設計のフェーズからセキュリティー対策を組み込むことでサイバーセキュリティーを確保しておくセキュリティーバイデザインの考え方や、各種ガイドラインによる運用面での対策も進められている。重要インフラ施設やサプライチェーンを狙ったサイバー攻撃により被害が大規模化する中で、サイバー攻撃の防御の考え方も、システムがインターネットとつながる境界で防ぐ境界防御から、すべてのシステムへのアクセスを検証するゼロトラストアーキテクチャーの考え方に変化している。また、セキュリティーの研究開発では、実際のサイバー攻撃のデータが対策を講じる上で重要な役割を持つため、サイバー攻撃の観測基盤を拡充してデータを蓄積していくことが望まれている。人への攻撃に対抗するためには、人の認知（コグニティブ）を考慮したセキュリティーの研究開発が重要になってきている。近年、問題となっているSNSに拡散したフェイク情報による世論の誘導などについても、人の認知や社会・行動科学などを含めた研究開発が必要となってきている。人や社会に関するセキュリティーは、今後、重要となる研究開発領域であり、心理学、社会学、経済学、法学などを含めた学際的アプローチによる総合的なセキュリティー対策の研究が望まれている。さらに、セキュリティー分野に共通する課題が人材育成である。セキュリティーは、ハードウェアからソフトウェア、システムなどの分野横断的な幅広い知識や、さまざまな守る対象に対するサイバー攻撃を分析・対策する技術、最近では機械学習などの隣接分野の技術も必要となっている。その一方で、このような知識や技術を持つ研究者の数は限られている。また、インシデント対応を行う現場のセキュリティー人材も不足している。重要インフラやサプライチェーンのセキュリティーなど、セキュリティー分野の重要性は年々増しており、セキュリティー分野の研究者や高度なスキルを持つ実務者を育成していくことが必要となっている。

❸ トラスト

情報サービスや情報システムをサイバー攻撃から守り安全性を確保するのが「セキュリティー」の役目であるのに対して、それらを安心して利用できるよう信頼を確保するのが「トラスト」の役目である。「旧来のトラスト」は、顔が見える人間関係や人々の間のルールに支えられたが、デジタル化の進展につれて、バーチャルな空間にも人間関係が広がり、複雑な技術を用いたシステムへの依存が高まり、また、だます技術も高度化している。例えば、最新のAI技術により巧妙に偽装されたフェイクなどによる情報サービスや情報そのものへの不信感や、ユーザーにとってブラックボックスであるAI技術を用いた自動運転車に安心して乗車できるのか、さらには、メタバースなどのバーチャル空間での活動において、生身の人間や物理的な実体が必ずしも確認できなくても相手を信用できるか、など、さまざまな問題が想定される。このような不信・警戒を過度に持つことなく幅広い協力・取引・人間関係を作り、デジタル化によるさまざまな可能性・恩

恵がより広がるようなデジタル社会を実現するものがトラストであり、デジタル社会におけるトラスト形成の仕組みを構築することが重要となっている。トラストを考える上では、対象真正性（本人・本物であるか?）、内容真実性（内容が事実・真実であるか?）、振る舞い予想・対応可能性（対象の振る舞いに対して想定・対応できるか?）の「トラストの3側面」を考慮する必要がある[3]。さらに、トラストの3側面のそれぞれについて、技術的な担保に加えて、人間の心理的な要素や、制度による保証なども併せて、多面的に考慮することが重要である。このトラストの3側面の中の対象真正性を担保する役割を持つのが以下で説明するデジタルトラストである。本書では、デジタルトラストを、データ・コンテンツの信頼性を保証するためのデータ・コンテンツのデジタルトラストと、システムの信頼性を保証するためのシステムのデジタルトラストに分けて扱う。

データ・コンテンツのデジタルトラストは、データを扱う人やモノが本人、本物であることと、データが改ざんされていないことを技術的側面と法的側面の両面から保証する。例えば、行政活動や経済活動のデジタル・トランスフォーメーション（DX）は人々の生活や企業活動にさまざまな恩恵を与えている。マイナンバーカードは、コンビニエンスストアでの各種行政証明書の取得やe-Taxによる確定申告、健康保険証としても利用することが可能で、その利便性が拡大している。一方で、マイナンバーカードが他人によって利用されたりデータが改ざんされたりすると、利用者に不安や不信を与えるだけでなく犯罪にもつながる。このような問題に対処するために必要となるのがデータ・コンテンツのデジタルトラスト（トラストサービス[4]とも呼ばれる）である。システムのデジタルトラストは、システムのハードウェアやソフトウェアが不正に改変されていないことを検証しシステム間の信頼関係を確立する。例えば、システム間の信頼関係を確立することなくシステムが構築・運用されると、自動運転車が不正なシステムにつながり不正操作により人命に影響が及ぶ危険性が生じる可能性がある。また、近年の情報システムは、複数のステークホルダーが役割に応じてシステムを構築し、ステークホルダーのシステムを接続して運用する場合が多く、ステークホルダーのシステム間を接続するためには、膨大な数のシステム間の信頼関係を確立することが必要となる。システムのデジタルトラストは、ステークホルダーのシステム間の信頼関係を、人を介さずにダイナミックに確立でき、サービスを迅速に提供することができる。

［セキュリティー・トラストの俯瞰図（構造）］

以下では、図2-4-2に示す本区分の俯瞰図（構造）について説明する。この図では、本区分の全体像を、基盤層、デバイス・システム・情報層、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、経済学などの人文・社会科学と、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、セキュリティー・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情報サービスや情報システムを守るセキュリティー、および情報サービスや情報システムの信頼性を保証するためのデジタルトラストに関する技術群を位置付けた。セキュリティー、デジタルトラストの縦軸は、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。最上位の層は、人・社会との関係に注目する層として、人・社会を守るための人・社会とセキュリティーと社会におけるトラストを位置付けた。

3 詳細は「2.4.7 社会におけるトラスト」を参照いただきたい。

4 総務省トラストサービスの概要（https://www.soumu.go.jp/main_content/000684847.pdf）を参照いただきたい。

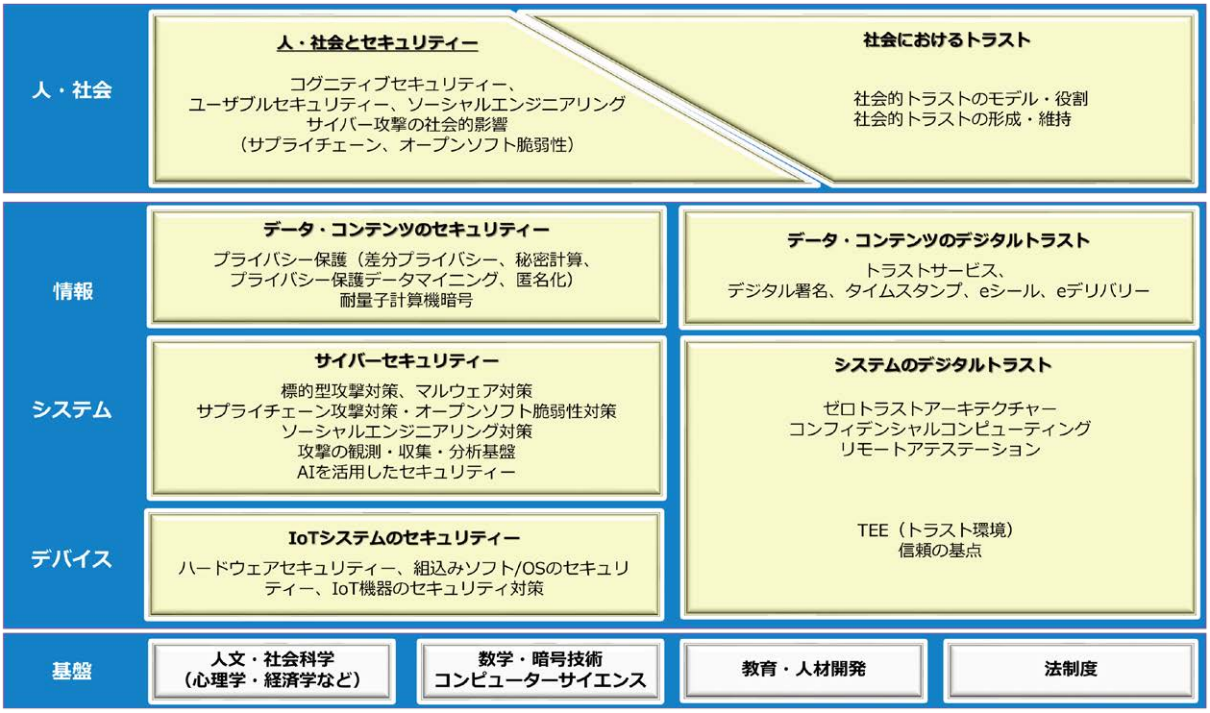

図 2-4-2　　セキュリティー・トラストの俯瞰図（構造）

以下では、本区分において取り上げる❶から❼までの研究開発領域について概観する。

❶ IoTシステムのセキュリティー

家電から、医療機器、工場・インフラなどの産業用途、自動車・宇宙航空など、幅広くIoT化が進展している。一方、近年、自動車、センサーなどに対するセキュリティーのリスクも増大している。 IoTシステムの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ーを扱う。

❷ サイバーセキュリティー

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いる。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おり、サイバーセキュリティーは、安心・安全な社会を実現する上で必要不可欠である。近年、身代金を要求するマルウェア（ランサムウェア）の攻撃による被害が拡大しており対策が必要である。ユーザーの端末を含む情報サービス・情報システムをサイバー攻撃から守るためのセキュリティーを扱う。

❸ データ・コンテンツのセキュリティー

データは「インターネットにおける新しい石油」とも評され経済の発展の鍵となっており、データ活用の重要性が高まっている。一方で、欧州を中心にプライバシー保護への要求やAIの拡大に伴い学習データのプライバシー保護など、プライバシー保護の重要性も高まっている。また、近年、量子コンピューターの研究開発が活発に進められており、十分な性能を持つ量子コンピューターが実用化されると、現在利用されている暗号が解読されてしまうことが懸念されている。データ活用とプライバシー保護を両立するための技術と、将来、量子コンピューターが実用化されたとしてもデータ・コンテンツの保護を維持するために必要な耐量子計算機暗号技術を扱う。

❹ 人・社会とセキュリティー

サイバー攻撃の拡大に伴い、これまでのシステムの脆弱性を狙った攻撃に加えて、フィッシングメールによる人への攻撃や、フェイクニュースやデマによる世論の誘導などが社会に影響を及ぼしている。情報サービスを利用するユーザー（人）の認識や行動に着目して、セキュリティー技術単体に加えて、心理学、経済学などの人文・社会科学を含めた学際的アプローチによるセキュリティーを扱う。

❺ システムのデジタルトラスト

サイバー空間とフィジカル空間を高度に融合したシステムによるSociety5.0では、そこに参加するステークホルダーが増加し、システムの数も膨大となる。システム間の信頼関係を確立することなくシステムが構築・運用されると、システムが不正なシステムにつながり不正操作を受ける危険性が生じる。ステークホルダーのシステム間の信頼関係を、人を介さずにダイナミックに確立、および維持するシステムのデジタルトラストを扱う。

❻ データ・コンテンツのデジタルトラスト

行政活動や経済活動など、われわれの生活の中のさまざまな活動がデジタル化（DX）されていく中で、本人のなりすましや電子文書の改ざんなどの行為を防止することは、情報サービスを提供していく上で必要不可欠である。データ・コンテンツを扱う人、組織、ものが本物であることや、データが改ざんされていないことを保証するデータ・コンテンツのデジタルトラストを扱う。

❼ 社会におけるトラスト

近年、情報サービスや情報システムをサイバー攻撃から守り安全性を確保するセキュリティーに加え重要になってきているのが、それらを安心して利用できるよう信頼を確保するトラストである。デジタル化の進展につれて、バーチャルな空間にも人間関係が広がり、複雑な技術を用いたシステムへの依存が高まり、だます技術も高度化した。不信・警戒を過度に持つことなく幅広い協力・取引・人間関係を作ることができ、デジタル化によるさまざまな可能性・恩恵がより広がるような社会を実現するための社会におけるトラストを扱う。

セキュリティー・トラストは、人々の生活や社会に密接に関係する重要な研究開発領域である。セキュリティーでは、近年、人を狙った攻撃が増加し、その影響は社会へ拡大している。トラストでは、AIやデジタル技術の進化で従来とは大きく異なる信頼に関係する問題が発生している。今後、安心・安全なデジタル社会を実現する上では、これまでのセキュリティーやデジタルトラストに関する研究開発に加えて、人・社会の層に位置付けた「人・社会とセキュリティー」や「社会におけるトラスト」に関する研究開発の推進が求められている。