3.5 セキュリティー

さまざまな機器や装置、システム、データや情報などを利活用するための技術。現代社会は、ICT システムに深く依存するようになってきており、ICT システムの安全性の確保は非常に重要な課題になってきている。このような問題を解決するために必要となるのが、セキュリティーである。

セキュリティーの研究分野は広く、かつ複雑である。単一の視点から俯瞰するのは困難であるが、図 3-5-1 に示すように、最もベースとなる領域としては教育・人材開発と社会の仕組みとしての法制度が非常に重要な役割を果たしている。さらに適用領域としては、クラウドコンピューティングや IoT（Internet of Things）、次世代ネットワークなど情報系の領域だけではなく、医療や交通サービス、電子政府などありとあらゆる社会システム・サービスに深い影響がある。この両者を結ぶところに技術を位置づけた。

縦軸には下から、装置のレベルであるデバイスのセキュリティー、それらの複合体であるシステムのセキュリティー、さらにデバイスやシステムに格納される情報のセキュリティーという階層で捉え、それらを統合して設計から運用・監視へとつながる横軸で捉えた。また、個別のセキュリティー対策だけではなく、全体を統合管理するための階層を設けた。暗号技術などの基礎的個別要素技術ももちろん重要ではあるが、ここでは応用領域や社会への適用に直接的に関連する七つの研究開発領域に注目する。

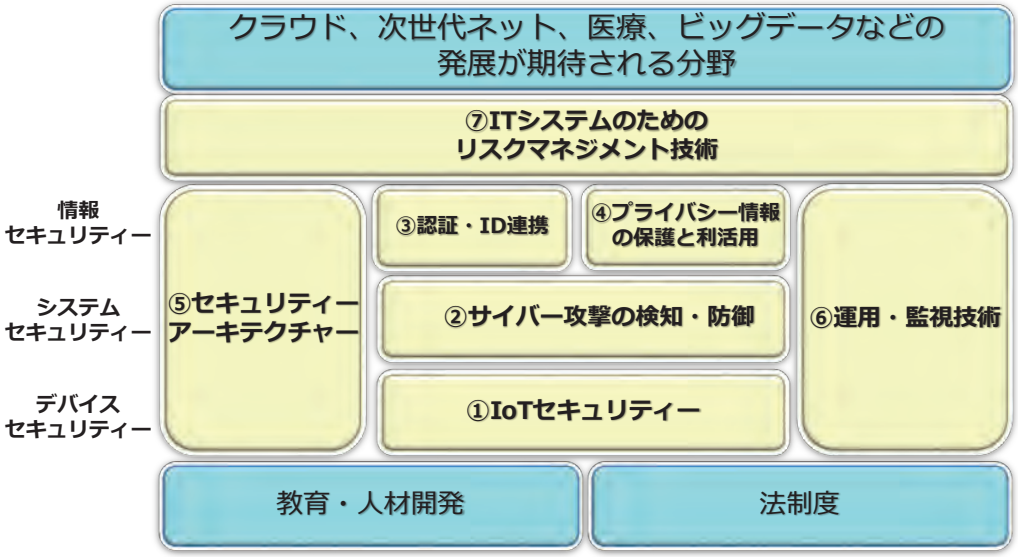

図 3-5-1　セキュリティー区分俯瞰図

① IoT セキュリティー
従来の情報機器だけではなく、家電や玩具、オフィス機器、自動車などのモノがネットワークに接続されつつある。これらのセキュリティー技術について、コンシューマー向けとインダストリー向けの２面性があり、ハードウエアとソフトウエアの両方に対する考慮、業界横断的な取り組みが必要である。

② サイバー攻撃の検知・防御
インターネットを経由したサイバー攻撃が日常的に行われるようになってきた。手口

も巧妙になり、その動機も変化している。国家安全保障と言う意味でもサイバーセキュリティーが重要である。新たな攻撃に対抗するためには、実データに基づいた対策が必須であるが、それらデータの共有が進まないという問題がある。

③ 認証・ID 連携
さまざまなサービスを有機的に連携し、便利で付加価値の高い利用方法が望まれている。そこでは認証、認可、連携が重要になっている。ID、IC カード、生体情報などのさまざまな認証技術と、それらの安全な連携に関する活動があり、ビジネス現場における応用研究・開発が重要であり、実証のための仕組みが必要である。

④ プライバシー情報の保護と利活用
企業や政府、自治体、医療機関などが蓄積する個人情報を活用することは利用者にとっての利便性の向上、提供者の効率向上を実現する。そこでは、プライバシーの保護と利活用を両立する技術が重要になる。課題としては、利用者の同意を得る仕組み、データフォーマット、通信プロトコルの標準化、漏えいデータの失効などがある。

⑤ セキュリティーアーキテクチャー
セキュリティーバイデザインとも呼ばれ、製品やシステム、サービスの設計・開発段階からセキュリティーを作りこんでおこうと言う考えである。脅威の識別、リスク評価、対策の妥当性検証などが技術的課題となる。情報システムだけでなく、組み込み、制御システムなどへの対応が急務である。

⑥ 運用・監視技術
情報システムのセキュアな運用のためには、日々の運用における状況の監視、対策の更新が必要である。対象となるシステムも日々変化し、機器の更新による性能向上にも対応しなければならない。セキュリティーだけでなく、ソフトウエア工学、人工知能、ネットワークなどさまざまな分野の融合が必要である。

⑦ IT システムのためのリスクマネジメント技術
現代社会は IT システムに深く依存し、その安全性の確保は非常に重要である。個別の技術的対策の導入も重要ではあるが、それだけでは不十分であり、リスクマネジメントのためのフレームワーク、リスクアセスメント、リスクコミュニケーションなどのリスクマネジメントのための理論から実務までの体系化、そのための技術の高度化が必要である。

日本においては、暗号要素技術の論文発表や理論的な提案等は活発に行われている。また、顔認証、指紋認証など生体認証においても世界をリードしている。しかし、実システム、実データに基づくセキュリティー対策技術についてはまだ取組が不十分であり、実践的な取組の強化が必要である。特にこれらは国家安全保障にも関わる問題でもあり、技術の国産化が重要な課題となっている。

3.5.1　IoT セキュリティー

（1）研究開発領域の簡潔な説明

情報家電、玩具、自動車、オフィス機器、医療機器、産業用設備・機器、制御システムなど多種多様な「モノ」がネットワークを介してつながる IoT（Internet of Things）が注目を集めているが、つながることで発生する脅威に対するセキュリティー対策を実現するための技術を確立する。

（2）研究開発領域の詳細な説明と国内外の動向

さまざまな分野において IoT 技術の適用が始まっているが、接続により発生する脅威に対するセキュリティー対策の不十分さや責任分界点の曖昧さなど、さまざまな課題がある。脆弱性の露見や設定不備などに起因して、各分野の IoT においてインシデントが発生しており、いまだ重大な被害は発生していないものの、医療機器や自動車などで利用者の生命に関わる問題や、産業用設備・機器や制御システムなどで企業の経営上大きな損害につながる問題が見つかっており、対策技術の確立および対策実施が急務となっている。ここでは、情報家電、医療機器、自動車などをネットワークに接続するコンシューマー向け IoT と、産業用設備・機器、制御システムなどをネットワークに接続するインダストリー向け IoT に分けて、研究開発領域の詳細な説明と国内外の動向を示す。

①　コンシューマー向け IoT のセキュリティー [1)]

［背景と意義］

家電、玩具、自動車、オフィス機器、医療機器など、さまざまな機器が利便性向上や高付加価値化を実現するために、ネットワーク接続機能を備え、新たなサービスの展開が始まっている。ガートナーの調査結果 [2)] によれば、2020 年に IoT 機器は 260 億個に達する見込みであるが、2015 年 11 月に HPE（Hewlett Packard Enterprise）が公開した報告書「Internet of things research study 2015 report」[3)] によると、90% の IoT 機器が少なくとも一つ以上の個人情報を収集しているにも関わらず、80% が脆弱なパスワードを使用しており、70% が通信を暗号化していないなど、十分な対策が実装されないまま製品化やサービス提供が進んでいることを示している。また、複数のベンダーから提供される「モノ」が接続し、サービスを実現するためにはインターネット上のサーバーやクラウドサービスとの連携が必要となるなど、複雑なシステム構成となるため、責任分界点の曖昧さを生じる問題がある。

例えば、情報家電分野では、DVD/HD レコーダーの設定不備や脆弱性が攻撃者によって悪用され、第三者への攻撃（スパムコメント送信の踏み台など）に用いられた事例が報告されている。また、脆弱性を有するホームルータが乗っ取られ、DDoS（Distributed Denial of Service）攻撃の踏み台に悪用される（コンピューターが乗っ取られ、攻撃に使われる）事件が相次いでいる。さらに、情報家電の脆弱性が利用者自身に損害を与える事例も報告されている。インターネット接続機能を有する冷蔵庫における SSL サーバー証明書の検証処理に不備があり、中間者攻撃によって Google サービスへのログイン情報が窃取される危険性が指摘されている。

自動車分野では、2010 年以降、研究者によるさまざまな攻撃成功事例が報告されている。診断用ポートである OBD-II（On-board diagnostics II）への接続による攻撃、車載ネットワークの一つである CAN（Controller Area Network）への攻撃、ファームウエアの改ざんによるブレーキ・ステアリング・エアコンへの干渉、脆弱性を攻撃したエンジンスタートや扉の開閉操作、イモビライザー（電子キーを利用した自動車盗難防止機能）の遠隔操作などである。

医療機器分野では、インターネット接続機能を有するインスリンポンプや心臓ペースメーカーへのハッキングが可能であることが学会で報告されている。また、薬剤ライブラリや輸液ポンプの設定などを管理するサーバーソフトウエアに脆弱性が存在し、患者に投与する薬の種類や量を改ざん可能であることが報告された。

この様に、IoT におけるセキュリティー対策の不十分性や欠落は、対象分野によっては、利用者の生命や資産に関わる恐れがある。また、利用者には被害が発生しないものの、第三者に損害を与えるサイバー攻撃の踏み台になってしまうというリスクを生じる恐れがある。

今後予想される IoT 技術の急速な普及・展開に際して、セキュリティー対策の不十分な製品の出荷やサービス開始を抑止するために、コンシューマー向け IoT における脅威分析と対策検討など、IoT セキュリティー技術の確立が急務となっている。

［これまでの取り組み］

これまで IoT のセキュリティーにつながる検討が各所において進められてきたが、国内では、2016 年に政府機関、関連団体、民間団体から IoT のセキュリティーに関するさまざまなガイドライン、枠組み、手引きが公開された。

経済産業省と総務省は、2015 年 10 月に設立された産学官連携の IoT 推進コンソーシアムにおける検討をもとに、2016 年 7 月に「IoT セキュリティガイドライン ver1.0」[4] を公開した。また、内閣官房サイバーセキュリティセンター（NISC: National center of Incident readiness and Strategy for Cybersecurity）は、2016 年 8 月に「安全な IoT システムのためのセキュリティに関する一般的枠組」[5] を公開した。

情報処理推進機構（IPA: Information Promotion Agency, Japan）は、2006 年以降、現在では IoT と分類されるようになった組み込み機器、自動車、情報家電、医療機器などの情報セキュリティーについて、脅威と対策に関する調査を実施してきたが、2016 年 5 月に「IoT 開発におけるセキュリティ設計の手引き」[6] を公開した。また、IPA が 2016 年 3 月に公開した「つながる世界の開発指針」[7] における検討内容は、先に述べた「IoT セキュリティガイドライン ver1.0」に反映されている。

2016 年は、さまざまな民間団体からも IoT セキュリティーに関する資料が公開された。日本クラウドセキュリティアライアンス（Cloud Security Alliance Japan Chapter）[8] は、2016 年 2 月に「IoT 早期導入者のためのセキュリティガイダンス」（2015 年 4 月公開英語版の翻訳）を、2016 年 4 月に「IoT における ID/ アクセス管理　要点ガイダンス」（2015 年 9 月公開英語版の翻訳）と「Internet of Things（IoT）インシデントの影響評価に関する考察」を公開した。重要生活機器連携セキュリティ協議会（CCDS: Connected Consumer Device Security Council）[9] は、2016 年 6 月に 4 つの「製品分野別セキュリティ

ガイドライン」を公開した。日本ネットワークセキュリティ協会（JNSA: Japan Network Security Association）[10]は、2016 年 6 月に「コンシューマ向け IoT セキュリティガイド」を公開した。

海外では、2015 年 1 月、米国政府機関である連邦取引委員会（FTC: Federal Trade Commission）は、報告書「Internet of Things - Privacy & Security in a Connected World-」[11]を発行し、IoT に潜むプライバシーとセキュリティー上のリスクについて注意喚起した。非営利団体傘下の OWASP（The Open Web Application Security Project）は、「Top 10 IoT Vulnerabilities（2014）」を始めとする複数の技術情報を公開している[12]。業界団体 GSMA（GSM Association）が 2016 年 2 月に「GSMA IoT Security Guidelines」[13]を、非営利団体 OTA（Online Trust Alliance）が 2016 年 3 月に「OTA IoT Trust Framework」[14]リリース版を公開するなど、海外でも IoT セキュリティーに関する資料の公開が相次いでいる。

［今後必要となる取り組み］

IoT のセキュリティー対策としては、従来の情報通信分野の技術を流用可能なもの、組み込み分野の技術を流用可能なものと、新たに IoT 向け固有技術の開発を必要とするものがある。IoT 機器によっては、リソースやコスト上の制限から、従来技術を適用できない場合も考えられることから、この様な制約のもとで適用可能な新規技術の開発が求められる。

また、セキュリティー技術の導入に当たり、脅威分析を行いインシデント発生時の影響を明確化した上で、リソースやコストとの兼ね合いから実装・採用する対策を決定する必要があるが、十分な脅威分析を実施せずに製品開発やサービス運用開始が行われているケースも存在するため、セキュリティーを考慮した IoT 設計技術の確立・普及が求められる。

さらに、脅威の多くはハードウエアおよびソフトウエアに内在する脆弱性に対する攻撃として発生するので、脆弱性対策が重要である。技術的には、製造過程において、内在する脆弱性を出荷前に低減するためのセキュア設計技術やセキュアコーディング技術、未知の脆弱性を発見するファジング技術などの活用が必要となってくる。また、ソフトウエアに関しては、出荷後に新たに発見される脆弱性に備えて、更新機能の実装やパッチ流通技術の確立も不可欠である。

② インダストリー向け IoT のセキュリティー[15),16)]

［背景と意義］

IoT 技術を産業界で活用する IIoT（Industrial IoT）の導入が始まっている。ドイツ政府が推進する戦略的プロジェクト「インダストリー 4.0」においても、製造業などにおける産業用設備・機器や制御システムをネットワークに接続することで、新たな価値やビジネスモデルを創出することを目指している。従来の産業用設備・機器や制御システムは、固有プラットフォーム、専用ソフトウエア、独自プロトコルで構築され、基本的に外部ネットワークと接続しない環境での運用を想定していたため、情報セキュリティーへの懸念は大きくなかった。しかしながら、近年、Windows や UNIX 系の汎用プラットフォームや

標準プロトコルの採用が進み、さらにメンテナンスや管理などの目的で外部ネットワークに接続されるようになったため、サイバー攻撃の対象になりつつある。2010 年に発生したイラン原子力施設におけるマルウエア Stuxnet の感染、2012 年に発生したサウジアラビアの石油会社におけるマルウエア Shamoon の大量感染、2014 年に公開されたドイツ国内の製鉄所に対するサイバー攻撃、2015 年に発生したウクライナの電力会社に対するサイバー攻撃による大規模停電など、インシデントが多数報告されている。社会や組織に対する影響が大きい分野であり、今後ネットワーク接続の拡大とともに脅威の増大が予想されるため、早急に対策の強化が必要である。

サイバー攻撃において、産業用設備・機器や制御システムへの攻撃の糸口となるソフトウエアの脆弱性の報告件数も増加しているが、これらの分野では 24 時間 365 日の稼動（可用性）が重要な要件であるため、セキュリティーパッチの即時適用やアンチウイルスソフトウエアの導入が困難という課題がある。さらに、10 年以上の稼動を前提としているシステムもあるため、長期継続してサポートされるセキュリティー対策製品が入手困難であり、パッチの提供終了など、この分野固有の課題も抱えており、分野の特徴を考慮した脆弱性対策が急務となっている。

こうした中で、重要インフラや製造ラインなどで用いられる産業用設備・機器や制御システムに適用可能なセキュリティー対策、そのための基準や標準の整備と普及、さらには、それに基づく評価認証制度などの必要性が増している。

［これまでの取り組み］

制御システムのセキュリティー基準や標準は欧米を中心に策定が先行しているが、組織・システム・コンポーネントの全てを対象とし、業種に依存せず汎用的な基準・標準として、国際電気標準会議（IEC: International Electro technical Commission）が制御システムセキュリティーについて制定している国際標準規格 IEC 62443（工業用プロセス計測制御のセキュリティー規格）がある。IEC　62443 は 4 階層、合計 13 の規格から構成されており、国際計測制御学会（ISA: International Society of Automation）および WIB（Working-party on Instrument Behaviour）からの提案をもとに標準化中である。

ISA の下部組織である ISCI（ISA Security Compliance Institute）[17] は、制御機器、制御システムおよびセキュリティー開発ライフサイクルプロセスの認証制度である ISASecure を推進しており、IEC 62443 に基づく、

- EDSA 認証（Embedded Device Security Assurance Certification）
  制御機器（組み込み機器）のセキュリティー保証に関する認証、
  IEC 62443-4-2（Technical security requirements for IACS）に対応。
- SSA 認証（System Security Assurance Certification）
  制御システムのセキュリティー保証に関する認証、
  IEC 62443-3-3（System security requirements and security levels）に対応。
- SDLA 認証（Security Development Lifecycle Assurance Certification）
  制御システムの開発ライフサイクルプロセスのセキュリティー保証に関する認証、
  IEC 62443-4-1（Product development requirements）に対応。

の第三者評価認証を実施している。

国内では、2014 年 4 月から制御システムセキュリティセンター（CSSC）[18] 認証ラボラトリーにて、ISCI と相互認証される EDSA 認証業務を開始した。また、2014 年 7 月から日本情報経済社会推進協会（JIPDEC）[19] にて、IEC62443-2-1（Establishing an industrial automation and control system security program）を基本として策定された制御システムを対象とした CSMS（Cyber Security Management System）認証基準に基づく CSMS 適合性評価制度を創設し、認証業務を開始した。

その他としては、米国国立標準技術研究所（NIST: National Institute of Standards and Technology）が「Guide to Industry Control System（ICS）Security」[20] を発行しており、JPCERT コーディネーションセンターがその日英対訳版を作成・公開している。また、インダストリー IoT を推進する業界団体の一つである IIC（Industrial Internet Consortium）は、2016 年 9 月に「Industrial Internet of Things Volume G4: Security Framework」[21] を作成・公開している。

［今後必要となる取り組み］

情報セキュリティー対策が十分でない産業用設備・機器や制御システムに対して、脅威分析を行い、インシデント発生時の事業リスクを明確化する必要がある。導入・適用するためのセキュリティー技術としては、分野の特性から、アンチウイルスソフトウエアを適用できない機器や装置に対するホワイトリスト方式のソフトウエア制御技術、不正侵入に対する検知技術やハードウエアレベルで一方向の通信しかできない様に工夫された特殊なファイアウォールである一方向ゲートウェイ（GW）などが必要である。

コンシューマー向け IoT に対して開発されたセキュリティー技術の流用も考えられるが、完全性や機密性より可用性が求められる分野であることから、高信頼性を確立した上で導入する必要がある。

特に、電力・ガス・水道・化学・石油などといった重要インフラ分野においては、今後の深刻なリスクに備えて、評価認証制度を国内事業者および国産製品に普及させるとともに、分野ごとに固有の要件をまとめていくことが必要である。業界や事業者が主体となり、真に有効となる基準の策定や選定など、その検証を進めていく必要がある。

(3) 注目動向

IoT のセキュリティーに特化した研究が始まっている。例えば、IoT 機器に対する大量のマルウエア感染の実態を調査し、対策としてマルウエアの駆除実験を実施している。[22),23)] この研究では、攻撃観測技術として、ダークネットモニタリング（特定のホストが割り当てられていない IP アドレスを監視すること）やハニーポット（コンピューターウイルスや不正侵入を捕らえるわな）を用いて観測用ネットワークで攻撃が来るのを待つ受動的観測と、インターネット上の攻撃ホスト情報・脆弱性などを自ら探索する能動的観測の二つを組み合わせることによって、IoT 機器のマルウエア感染の実態を明らかにしている。

インターネット接続機器検索サービスとして、以前から存在する検索エンジン SHODAN や、ミシガン大学の研究者が 2015 年 10 月に開発した検索エンジン Censys が提示する検索結果は、脆弱性を有する IoT 機器が多数ネットワークに接続されたままと

なっている実態を示している。[24)]

IoT に適用可能な暗号関連技術としては、二つの対象的な次世代暗号技術の研究が進められている。一つは、リソースに限りのある IoT 機器に実装可能な軽量暗号アルゴリズム[25)]や軽量暗号プロトコルの研究であり、他方は、IoT 機器が収集した個人情報などの機微なデータを一元管理するクラウドサービスにおける情報漏えい対策として、データを暗号化したまま演算・検索を可能とする高機能暗号（検索可能暗号、秘匿検索など）の研究である。[26)]

科学技術振興機構（JST）の戦略的創造研究推進事業（CREST）「ディペンダブル VLSI システムの基盤技術」の成果として報告された、製造段階で生じる LSI の個体差を利用した IoT 機器の秘匿と認証を行うセキュリティー技術[27)]も興味深い。

IoT のセキュリティーを実現する上で、高機能暗号や高度のセキュリティーを実現するハードウエア、耐タンパー性 / 耐クローン性、ハードウエアのトロージャン対策など、ハードウエアセキュリティー技術も注目すべき分野である。

(4) 科学技術的課題

IoT のセキュリティーを実現するためには、多岐にわたるセキュリティー技術の知識が必要である。IoT の構成要素に従って、情報通信分野のセキュリティー技術と組み込み分野のセキュリティー技術を適材適所で使い分ける必要がある。また、ハードウエアセキュリティー技術とソフトウエアセキュリティー技術を組み合わせて実現可能な情報セキュリティー対策も存在する。システム全体のセキュリティーを考察するためには、これら全ての技術の知識を必要とするので、広範囲の知識を有する複数の研究者による連携・共同研究が重要になってくると考えられる。

サイバーセキュリティーの世界では、新たな脅威の出現や攻撃手法の巧妙化が予想されるため、現時点で判明している技術的課題を解決しても、今後想定していなかった新たな課題が発生することが想定される。継続的な技術開発・研究実施が必要不可欠な分野である。

(5) 政策的課題

業界や製品分野によっては、非機能でありコストを要するセキュリティー対策をどこまで実装するか基準が制定されていないため、各業界や各製品分野において、大枠のコンセンサスを形成することが課題である。業界団体が中心となり、各業界におけるセキュリティー脅威の共通認識を形成し、セキュリティー基準を制定していくことが望ましい。

さまざまな「モノ」が相互に接続するため、将来的には、業界横断的な基準が必要となることも考えられる。これらをまとめる上で、国家的な政策のもと、産官学連携や府省連携を行い、検討を進めることが期待される[28)]。重要インフラを形成するインダストリー向け IoT においては、国としての基準やガイドを制定することも必要な時代となってきている。

(6) キーワード

IoT、IoE、IIoT、脆弱性対策、脅威分析、制御システム、重要インフラ、攻撃観測技術、軽量暗号、高機能暗号、ハードウエアセキュリティー

(7) 国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	○	↗	軽量暗号、認証技術ならびにビッグデータ、AI と連携した検知技術の研究を進めている。
	応用研究・開発	○	↗	総務省、経済産業省による IoT 推進コンソーシアムを設立し、ガイドラインを策定、公開している。
米国	基礎研究	◎	↗	製品寿命の長い IoT デバイスに対応する暗号技術やゲートウェイ、アプリケーションのフレームワークを研究するプロジェクトを発足している。
	応用研究・開発	◎	↗	CSA（Cloud Security Alliance）、OTA（Online Trust Alliance）、OWASP（The Open Web Application Security Project）がガイドラインを公開している。IoT 関連ベンダーも並行して、IoT 向けのセキュリティーソリューションを公表している。制御システムに関しては、米国政府によるセキュリティーガイドラインが公開されている。
欧州	基礎研究	○	→	IoT デバイスの研究開発に力をいれている。
	応用研究・開発	◎	↗	ENISA（The European Union Agency for Network and Information Security）によるスマートホームに対するセキュリティーの勧告文書を公開し、GSMA はサービスプロバイダー、製造業、ネットワークオペレーターなどに向けたガイドラインを公開している。また、ドイツ主導によるインダストリー 4.0 プラットフォームは実現戦略におけるセキュリティーの要求事項を公開している。
中国	基礎研究	△	→	IoT のセキュリティーに関する具体的な研究は公開されていない。
	応用研究・開発	○	→	ウイルス検知や防御技術の開発や自動車のハッキング実験を行っているが、IoT/ 制御システムに特化した製品は見当たらない。
韓国	基礎研究	△	→	IoT のセキュリティー関する具体的な研究は公開されていない。
	応用研究・開発	△	→	IoT のセキュリティー要件をまとめる動きはみえるが、国家もしくは標準化団体主導によるガイドライン策定の動きはない。また、具体的は製品も見当たらない。

（注１） フェーズ
基礎研究フェーズ：大学・国研などでの基礎研究のレベル
応用研究・開発フェーズ：研究・技術開発（プロトタイプの開発含む）のレベル
（注２） 現状　※わが国の現状を基準にした評価ではなく、CRDS の調査・見解による評価である。
◎　特に顕著な活動・成果が見えている、 ○　顕著な活動・成果が見えている
△　顕著な活動・成果が見えていない、 ×　活動・成果がほとんど見えていない
（注３） トレンド
↗：上昇傾向、 →：現状維持、 ↘：下降傾向

(8) 参考文献

1）独立行政法人 情報処理推進機構（IPA）, “IoT のセキュリティ”,
https://www.ipa.go.jp/security/iot/index.html（閲覧日 2016-12-16）
2）Gartner, “Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020”,
https://www.gartner.com/newsroom/id/2636073（閲覧日 2016-12-16）
3）Hewlett Packard Enterprise, “Internet of things research study 2015 report”,

https://www.hpe.com/h20195/v2/GetPDF.aspx/4AA5-4759ENW.pdf（閲覧日 2016-12-16）
4）IoT 推進コンソーシアム・総務省・経済産業省 ,“IoT セキュリティガイドライン ver 1.0”,
http://www.iotac.jp/wp-content/uploads/2016/01/03-IoT セキュリティガイドライン ver1.0 別紙 1.pdf（閲覧日 2016-12-16）
5）内閣サイバーセキュリティセンター（NISC),“安全な IoT システムのためのセキュリティに関する一般的枠組”,
http://www.nisc.go.jp/active/kihon/pdf/iot_framework2016.pdf（閲覧日 2016-12-16）
6）独立行政法人 情報処理推進機構（IPA),“IoT 開発におけるセキュリティ設計の手引き”,
https://www.ipa.go.jp/security/iot/iotguide.html（閲覧日 2016-12-16）
7）独立行政法人 情報処理推進機構（IPA),“つながる世界の開発指針 ～安心安全な IoT の実現に向けて開発者に認識してほしい重要ポイント～”,
https://www.ipa.go.jp/sec/publish/tn16-002.html（閲覧日 2016-12-16）
8）一般社団法人 日本クラウドセキュリティアライアンス（Cloud Security Alliance（CSA）ジャパン),
https://www.cloudsecurityalliance.jp/（閲覧日 2016-12-16）
9）一般社団法人 重要生活機器連携セキュリティ協議会（Connected Consumer Device Security council: CCDS),
https://www.ccds.or.jp/（閲覧日 2016-12-16）
10）特定非営利活動法人 日本ネットワークセキュリティ協会（Japan Network Security Association: JNSA),
http://www.jnsa.org/（閲覧日 2016-12-16）
11）Federal Trade Commission（FTC),“Internet of Things – Privacy & Security in a Connected World”,
https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf（閲覧日 2016-12-16）
12）Open Web Application Security Project（OWASP),“OWASP Internet of Things Project”,
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project（閲覧日 2016-12-16）
13）Groupe Speciale Mobile Association（GSMA),“GSMA IoT Security Guidelines”,
http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/（閲覧日 2016-12-16）
14）Online Trust Alliance（OTA),“Internet of Things”,
https://otalliance.org/IoT（閲覧日 2016-12-16）
15）一般社団法人 JPCERT（Japan Computer Emergency Response Team）コーディネー

ションセンター , “制御システムセキュリティとは”,
https://www.jpcert.or.jp/ics/index.html（閲覧日 2016-12-16）
16）独立行政法人 情報処理推進機構（IPA), “制御システムのセキュリティ”,
https://www.ipa.go.jp/security/controlsystem/index.html
（閲覧日 2016-12-16）
17）ISA Security Compliance Institute（ISCI), industrial control systems cybersecurity certification program ISASecure,
http://www.isasecure.org/（閲覧日 2016-12-16）
18）技術研究組合 制御システムセキュリティセンター（Control System Security Center: CSSC),
http://www.css-center.or.jp/ja/info/presentation.html
（閲覧日 2016-12-16）
19）一般財団法人 日本情報経済社会推進協会（Japan Information Processing Development Corporation: JIPDEC),
https://www.jipdec.or.jp/（閲覧日 2016-12-16）
20）National Institute of Standards and Technology（NIST), “NIST Special Publication 800-82 Revision 2,Guide to Industry Control System（ICS）Security”,
http://dx.doi.org/10.6028/NIST.SP.800-82r2（閲覧日 2016-12-16）
21）Industrial Internet Consortium（IIC), “Industrial Internet of Things Volume G4: Security Framework”,
https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf
（閲覧日 2016-12-16）
22）横浜国立大学 情報・物理セキュリティ研究拠点 , “研究成果 IoTPOT - Analysing the Rise of IoT Compromises”,
http://ipsr.ynu.ac.jp/iot/index.html（閲覧日 2016-12-16）
23）吉岡 克成 , “止まらない IoT マルウェア大流行とその対策に向けて”,IoT Security Forum 2016
24）独立行政法人 情報処理推進機構（IPA), “IPA テクニカルウォッチ「増加するインターネット接続機器の不適切な情報公開とその対策」改訂第二版”,
https://www.ipa.go.jp/security/technicalwatch/20160531.html
（閲覧日 2016-12-16）
25）Cryptography Research and Evaluation Committees（CRYPTREC), “CRYPTREC Report 2015 暗号技術評価委員会報告”,
https://www.cryptrec.go.jp/report/c15_eval_web.pdf（閲覧日 2016-12-16）
26）花岡 悟一郎 , “IoT の高度化利活用を促す次世代高機能暗号技術”, IoT Security Forum 2016
27）三菱電機・立命館大学・JST プレスリリース , “LSI の個体差から指紋のような固有 ID を生成し、組み込み機器の安心・安全に貢献「IoT 時代に向けたセキュリティー技術」を開発”,
http://www.jst.go.jp/pr/announce/20150205/（閲覧日 2016-12-16）

28）内閣サイバーセキュリティセンター（NISC）サイバーセキュリティ戦略本部 , “サイバーセキュリティ 2016”
http://www.nisc.go.jp/active/kihon/pdf/cs2016.pdf（閲覧日 2016-12-16）

3.5.2　サイバー攻撃の検知・防御

(1) 研究開発領域の簡潔な説明

本領域の研究開発は、サイバー攻撃を迅速に検知し、有効な防御を行うための次世代技術の確立を目的としている。本分野の研究開発は、実際のオペレーションと強く結びついており、技術の発展により精度の高い分析や対策をより迅速に実現していくことが求められている。なお、本分野の研究開発は各国の政策にも強く結びついており、サイバー犯罪やサイバーテロリズム対策のための研究開発に対しファンディングが積極的になされる可能性が高い点にも留意されたい。

(2) 研究開発領域の詳細な説明と国内外の動向

インターネットの進歩・発展の陰で、インターネットを経由したサイバー攻撃も日々高度化を続けており、重大な社会問題となっている。サイバー攻撃に対抗すべく、サイバー攻撃の観測技術、分析技術、防御技術の研究開発への投資が世界各国で進められている。サイバーセキュリティーの重要性は政策レベルでも強く認識され、それに基づき研究開発の方向性やファンディングの方向性が決められることも多いため、政策面での動向も把握しておくことが重要である。

日本では近年、多数のサイバーセキュリティー関連の法整備が進められている。これは世界的なトレンドであるが、日本では 2014 年 11 月に制定したサイバーセキュリティ基本法からの流れに着目したい。本基本法では、第十九条および第二十条に当該分野における研究開発の重要性がうたわれている。また、本基本法を受けて、内閣サイバーセキュリティセンター（NISC）は サイバーセキュリティー戦略を策定した。その 2016 年の年次計画である「サイバーセキュリティ 2016」[1] には、2016 年度に政府が実施する具体的な取り組みが記載されている。イノベーションの観点からは、第 5 期科学技術基本計画が策定され、2016 年度より本計画に沿った科学技術政策が実施されている。このように、日本ではサイバーセキュリティーの研究開発の重要性が強く認識されてきている。

日本の政府の情報セキュリティーに関する予算も増加傾向にある。サイバーセキュリティ基本法施行後の初の予算編成であった今回は、サイバーセキュリティーに対する姿勢が現れている[2]。ここで、情報セキュリティ政策会議が発行した「情報セキュリティ研究開発戦略（改定版）」[3] を見ると、日本の政府の情報セキュリティー研究開発予算は当初予算ベースでは減少基調にあるようにも読めるが、情報セキュリティーに関わる予算という視点で予算を見ると、着実に増加傾向にある。サイバーセキュリティー分野は実践的な研究開発が多い実態を考えると、サイバーセキュリティーの研究開発プロジェクトへの予算は増加傾向にあると捉えることができる。実際、実践的な研究開発、人材育成、そして実践演習などについては、研究開発という予算の外側の情報セキュリティーに関する予算として、ファンディングがなされるケースも多い。

一方、日本の今後の政策や研究開発への投資動向は、海外の状況に大きく影響されるため、海外の状況も把握しておかなければならない。特に、サイバーセキュリティー分野の研究開発をリードしている米国の動向は重要である。米国の 2017 年大統領予算教書[4] によると、研究開発全体に関する年間予算は約 1520 億ドルであり、これは、2015 年の

1350 億ドル、2016 年の 1460 億ドルに続き、増額されている。オバマ政権は、当初から研究開発への投資を優先する姿勢を打ち出しており、この基本姿勢は 2017 年に向けて揺らいでいない。また、同教書では、サイバーセキュリティーの重要性も強調されている。米国では、今後数十年に直面する課題への対応として、「イノベーション」、「機会創造」、「国家安全保障」という 3 本の柱を掲げているが、この国家安全保障の部分ではサイバーセキュリティーの重要性が強調されており、「サイバーセキュリティ国家行動計画」などへの予算計上が明示される他、対処すべき課題にサイバーセキュリティー関連事案が複数明示されるなど、本分野への重点投資が進められている。

(3) 注目動向

前述のサイバーセキュリティーに関する政策や戦略を知ることで、今後の研究開発への国の投資方針も見えてくる。これらの政策や戦略の中で特筆すべきことの一つに、「人材育成」の重要性があげられる。全世界的に、サイバーセキュリティー人材の重要性とその不足に関する認識が共有されており、それに対応すべく、人材育成に注力することがうたわれている。

日本においても、NISC では新・情報セキュリティ人材育成プログラム[5]（2014 年 5 月策定）、サイバーセキュリティ人材育成総合強化方針[6]（2016 年 3 月策定）に基づき、産学官の連携体制を基本とした施策を展開しており、2016 年度内に次期人材育成プログラムの策定が予定されている。文部科学省でも情報技術を活用して社会の具体的な課題を解決できる人材を育成すべく、複数の大学と産業界による全国的なネットワークを形成し、実際の課題に基づく課題解決型学習等の実践的な教育を実施・普及する enPiT（Education Network for Practical Information Technologies）を展開している[7]。その他、国立研究開発法人 情報通信研究機構（NICT）でも人材育成に本格的に着手している。従来、NICT が保持している演習基盤を活用し、実践的なサイバー防御演習（CYDER）が実施されてきたが、今後は NICT 自身が持つサイバーセキュリティーに関する技術的知見や研究成果等を活かし、NICT 自身が主体的に実践的な演習および関連する教育コンテンツの制作等を実施することとし、NICT の業務に当該演習に係る業務を追加するための法整備を行っている。

政策面ではなくイベント面に着目すると、2020 年開催の東京オリンピックは意識しておきたい。東京オリンピック開催に向けて、情報セキュリティーの確保が最重要課題の一つとなっており、国内企業複数社がセキュリティー事業の強化を表明している。政府としても本腰を入れた対応をしており、サイバーセキュリティー戦略の中でも、「オリンピック・パラリンピック CSIRT（シーサート：Computer Security Incident Response Team）の設置」を明記している。そして、2016 年の伊勢志摩サミットおよび 2019 年の我が国で開催されるラグビーワールドカップにおける取組を踏まえて対応を進めていくこととしている。

一方、ファンディング動向としては、FP7（第 7 次研究枠組み計画）、そしてそれに続く Horizon 2020[8] に着目したい。欧州では EU の FP7 の後継として、2014 年 1 月より Horizon 2020 が開始されており、2014 ～ 2020 年までの 7 年間の研究開発の方向性を示

すとともに約 770 億ユーロの予算が計上されている。Horizon 2020 ではプログラムセクション「Societal Challenges」の中で七つの社会的課題を抽出しており、その中に「Secure societies - Protecting freedom and security of Europe and its citizens」としてセキュリティー関連の課題が挙げられている。この課題の研究予算は、全体予算の 2.2% にあたる約 17 億ユーロを占めている [9]。

この Horizon 2020 の中でサイバーセキュリティーに関してどのような取り組みをしていくべきかを理解することが重要であるが、その参考になるのが FP7 で実施された三つのサイバーセキュリティーロードマップ策定プロジェクトである。FP7 の枠組みの中では、サイバーテロリズムおよびサイバー犯罪に対抗するために必要な研究開発のロードマップを検討するプロジェクトが三つ存在している。具体的には、CyberROAD[10]、CAMINO[11]、そして COuRAGE[12] である。それぞれその検討のアプローチは異なるものの、検討結果として抽出された重点研究課題には大きな齟齬はなく、今後のサイバーセキュリティー研究開発の方向性を理解する大きな手掛かりとなる。

(4) 科学技術的課題

サイバーセキュリティー向上に向けた科学技術的課題のうち、近年特に重要視されているものを以下に紹介する。サイバーセキュリティーは喫緊の課題であるため、概して実践的な研究開発につながる研究課題が重要視される様相を呈している。

- 標的型攻撃対策技術：標的型攻撃は特定組織をターゲットとした長期にわたる執拗な攻撃である。典型的な標的型攻撃では周到に準備された電子メールに添付されたマルウエアによって組織内に侵入する。標的型攻撃では従来型の境界防御技術（入口対策、出口対策）が有効に働かないケースも多い。そのため、組織内部の観測・分析・検知技術（内部対策）の確立が重要となる。また、組織内のログ管理技術や、インシデント発生後のフォレンジック（ネットワークやコンピューターの記録を収集・分析する）技術の高度化も必要となる。
- ドライブ・バイ・ダウンロード攻撃対策技術：Web を介した攻撃であるドライブ・バイ・ダウンロード（DBD）攻撃は、ハニーポット等の受動的観測では捉えられない攻撃である。DBD 攻撃に加担する悪性サイトを Web クローリングで検知する取り組みもあるが、クローリングのシード選択の問題や、数時間で生滅する悪性サイトを捉えられないなど課題が多い。DBD 攻撃対策技術として、ユーザーの Web ブラウザーや組織の Web プロキシー（Web の中継サーバー）等を観測点として取り込んだ大規模観測・分析技術の確立が必要となる。
- DDoS 攻撃対策技術：特定のサーバーに通信を集中させ、外部からのアクセスを不能にする DDoS 攻撃は、サービス提供者や通信事業者にとって依然重要な課題である。2013 年初頭から DDoS ツールやボットネット（乗っ取った攻撃用サーバーの集まり）を利用した従来型の DDoS 攻撃に加え、DNS（Domain Name System）や NTP（Network Time Protocol）等による通信の増幅を悪用したリフレクタ攻撃が台頭しており、対策を一層困難にしている。DDoS 攻撃対策技術として、リフレクタ攻撃観測用ハニーポット技術、大規模ネットワーク観測技術、さらにそれらと被害サーバー側の

DDoS 攻撃観測情報を用いた DDoS 攻撃の予測・早期検知・早期対策技術の確立が求められている。

・マルウエア分析・解析技術：膨大な亜種マルウエアや解析回避機能を有するマルウエアの出現により、シグネチャベースのマルウエア検知手法（マルウエアに特有のパターンに基づく検知手法）の効果が低下している。マルウエア対策技術として、サンドボックス解析技術（保護された領域で動作を解析する技術）の高度化や、カーネルモードで動作するマルウエア解析技術、マルウエアの長期動的解析技術、マルウエアの解析回避機能への対策技術の確立が必要である。

・大規模感染型マルウエア対策技術：大規模感染型マルウエア（ワーム等）はインターネット上で依然猛威を振るっている。大規模感染型マルウエア対策技術として、大規模ネットワーク観測・分析の高度化と、その観測結果を活用した対策技術の開発が求められている。また P2P（Peer to Peer）型の通信を行うマルウエアも多く存在しており、P2P 型マルウエアの観測・分析技術も重要である。

・サイバー攻撃可視化技術：サイバー攻撃は元来不可視であるが故に検知や防御が難しく、また対策の重要性を組織のトップマネジメントが正しく理解することを阻んでいる。サイバー攻撃可視化技術はセキュリティーオペレーションの迅速化・効率化や、トップマネジメント層を含めたセキュリティーアウエアネスの向上を図る上で重要となっている。

・サイバー攻撃情報共有技術：サイバー攻撃は容易に国境をまたいで行われるため、サイバー攻撃対策には国際的な情報共有が有効であるが、多くの場合、人手による情報共有が主流となっており、また機微な情報の共有は困難となっている。サイバー攻撃情報共有技術として、共通のデータフォーマットやインターフェースを定義することは非常に重要であり、そのための国際標準化活動も行われてきている。同時に、サイバー攻撃に関連した情報のグローバルなリポジトリの構築、機微情報のサニタイズ技術、高速な検索技術、異なる攻撃キャンペーン間の相関分析技術等の確立が重要となっている。

・脆弱性の自動管理技術：脆弱性の存在は、インシデント発生の主要因となる。そのため脆弱性の存在を監視し、必要な対策を必要な時に実施することが重要であるが、人的リソースの制約から対応が困難なケースが多数存在する。そのため、脆弱性の検知・対応を自動化する技術の研究開発が望まれている。既に、IT 資産リストと脆弱性情報レポジトリ内情報の更新を監視することで脆弱性を検知する技術や、SDN（Software Defined Network）を用いて脆弱性検知後の対応を自動化する技術などが検討されている。また、脆弱性の自動管理のみならず、各種のセキュリティーオペレーションの自動化に関する研究開発も強く求められている。

・モバイルデバイスのセキュリティー管理技術：モバイルデバイスへのサイバー攻撃の可能性は昔から指摘されてきていたが、近年、Android や iOS などを対象としたランサムウエアなどのマルウエアの脅威が増大してきている。モバイルデバイスへの人々の依存度は増加してきており、また、モバイルデバイスの数は膨大であるため、マルウエアの大規模感染などによるパンデミックが起きた際の被害は甚大である。そのため、モバイルデバイスのセキュリティーを評価・可視化するなどの技術の研究開発が必要である。

・IoT 向けセキュリティー技術：数年前より、Windows 端末だけではなく、Linux 組み

込み機器であるブロードバンドルータや Web カメラなどをはじめとする IoT 機器がマルウエア感染する事例が多く見られている。IoT 機器は、リソースの制約があるものや、常日頃から管理者による適切な管理を受けることが難しいものなども存在し、従来のセキュリティー技術をそのまま活用することが困難なケースが多数存在する。そのため、各種 IoT 機器のセキュリティーを担保するための研究開発が望まれている。また、IoT 機器やモバイル機器に感染するマルウエアを想定した新しいハニーポット技術の確立、および収集したマルウエアの分析技術も課題となっている。

(5) 政策的課題

サイバーセキュリティーは「データオリエンテッド」な研究分野であり、研究の成否は、いかに大規模な“実データ”を定常的に収集できるかにかかっていると言っても過言ではない。実データを定常的に収集するためには、収集技術の開発のみならず、システムの安定稼働や長期運用体制の構築、関係組織（例えば大学の場合は学内情報センター）との折衝等々、人的コストの非常に高い作業を継続的に行う必要があり、有用なデータの収集が始まるまでに数年単位の時間を費やす事も珍しくない。しかしながら、公的な競争的資金は数年程度の年限で設定されており、大規模なデータ収集基盤の構築に多くの時間を割くことが難しく、そのためオリジナルな“実データ”を用いた研究環境を構築できている国内大学は数えるほどしか存在しない。また、公的な競争的資金では研究の新規性やデマケーション（他の研究との差別化）が重視されるため、既に構築したデータ収集基盤の長期運用という重要な項目に予算計上することが難しい。

また、サイバーセキュリティーは実践的な研究分野であり、常に実用化を目指した研究開発が重要である。米国の例をみると、ミシガン大学の研究グループが設立した Arbor Networks 社（DDoS 対策製品でトップシェア）や、カリフォルニア大学サンタバーバラ校等の研究グループが設立した Lastline 社（標的型攻撃対策製品で成長株）など、大学の学術研究が実用化に直結している。さらに、それら企業の製品が集めた実データを学術研究にフィードバックすることで、新たな研究を生み出しており、実データを中心とした研究のライフサイクルが確立している。一方、サイバーセキュリティー分野において国内大学の研究成果が実際の製品やサービスに結びついた例はほぼ皆無であり、産業界と学術界の間で大きなギャップが存在している。

さらに、日本の公的な研究資金ではデマケーションが重要視されるため、類似の研究課題に関して複数の研究グループが研究資金を獲得して同時並行的に研究開発を進めることは、ほぼ起こり得ない（そして、研究資金獲得後は競争が発生しない）。米国では、複数の省庁がサイバーセキュリティーに関する研究予算を計上しており、その全体調整は NITRD（The Networking and Information Technology Research and Development）が受け持つものの、省庁間のデマケーションを行うのではなく、ある程度の重複は許容しつつ、年度ごとの評価を厳正に行い、高い研究成果を上げている研究グループが生き残る仕組み（つまり資金獲得後の競争の仕組み）を構築している。そのために、研究資金提供側の組織も各分野の専門家を擁しており、技術的な評価を行える体制を敷いている。

(6) キーワード

サイバーセキュリティー、サイバー攻撃、標的型攻撃、ドライブ・バイ・ダウンロード攻撃、DDoS 攻撃、マルウエア、サイバー攻撃可視化、サイバー攻撃情報共有、脆弱性対策、モバイルセキュリティー、IoT セキュリティー

(7) 国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	○	↗	・国内シンポジウム等でのサイバーセキュリティーやマルウエア解析に関する発表件数は大学、企業とも増加傾向。一方、著名な国際会議での発表件数については、暗号系分野においては以前から Crypto, Eurocrypt, Asiacrypt などにおいて一定の存在感を維持。サイバーセキュリティー分野では従来は存在感に乏しかったものの、近年、RAID 2013/2015/2016 や ACM CCS 2015 に採録されるなど、国際的な成果も伸びつつある。 ・日欧連携が積極的に行われている。例えば、総務省戦略的国際連携型研究開発推進事業と FP7 との日欧 ICT 協調課題である「サイバー脅威に対する回復性強化のためのサイバーセキュリティ」（NECOMA プロジェクト）は終了したものの、本コミュニティを中心に、日欧の研究機関が集結して国際共同研究を行っている。
	応用研究・開発	○	→	・総務省が主導する「国際連携によるサイバー攻撃予知・即応プロジェクト」（PRACTICE, 2015 年度末まで）や、「官民連携による国民のマルウエア対策支援プロジェクト」（ACTIVE）、「実践的サイバー防御演習」（CYDER）の中で、実践的な応用研究が進められている。 ・情報通信研究機構は日本最大規模のサイバー攻撃観測・分析・対策システム NICTER を中心とした研究開発を推進しており、特にそのリアルタイム分析・可視化技術は世界をリードしている。
米国	基礎研究	◎	→	・米国の大学・公的研究機関による基礎研究レベルは非常に高く、著名な国際会議でのプレゼンスも高い。 ・NSF、DoD、DHS 等からの豊富な研究資金に基づく大小のプロジェクトが継続的に実施されている。
	応用研究・開発	◎	→	・大学での研究が実用を目指した応用研究であるものが多く、ミシガン大学発祥の Arbor Networks や、カリフォルニア大学サンタバーバラ校発祥の Lastline 社等、起業につながっている例も多い。 ・情報共有のフォーマットを規格化する動きが活発化しており、特に STIX や TAXII と呼ばれる脅威情報の交換のための規格は DHS から OASIS（Organization for the Advancement of Structured Information Standards, 構造化情報標準促進協会）へ移管して検討が進められている。
欧州	基礎研究	○	→	・ウィーン工科大学（オーストリア）や Eurecom Institute（フランス）等、マルウエア解析技術やサイバー攻撃観測技術等で高い研究成果実績有。 ・一方で、優秀な研究者が米国等の研究機関に移籍する事例も多く、研究人材の確保は容易ではないようにうかがえる。
	応用研究・開発	○	↗	・FP7 の後継の Horizon 2020 で、セキュリティーは七つの社会的課題の一つにあげられており、応用研究はさらに進むものと思われる。 ・EC は 14 カ国 28 組織（ISP、CERT、Law Enforcement、IT プロバイダー、学術ネットワーク、学術機関、重要インフラ事業者）で構成される ACDC（Advanced Cyber Defense Center）を設立。応用研究から実運用まで情報共有が進んでいる。

中国	基礎研究	△	↗	・中国国内トップクラスの大学の学生が米国等に留学し、研究成果を上げているが、中国国内の大学における研究成果が著名な国際会議に採録されるまでには至っていない。
	応用研究・開発	△	↗	・これまで国際的に注目される大規模研究プロジェクトは公表されているレベルでは見られない。 ・サイバーセキュリティー分野における国際標準化活動に徐々に注力。例えば IETF では Alibaba や Huawei のエンジニア、もしくは雇用した欧米のコンサルタントなどが chair の役職を務めたり、規格を提案してくるようになってきている。同様の傾向は ITU-T やその他の標準化団体でも見られる。
韓国	基礎研究	○	↗	・KAIST や POSTECH 等トップクラスの大学の研究成果が ACM CCS や NDSS 等の著名な国際会議に採録される等、基礎研究の国際的な評価は上がりつつある。
	応用研究・開発	○	→	・国家的なセキュリティーインシデントを多数経験しており、政府主導のセキュリティー対策を実践。 ・KISA、ETRI、KISTI といった公的機関が、サイバーセキュリティー技術の研究開発や、モニタリング、インシデント対応を行っており、特に政府機関に導入されているセキュリティー機器は 100% 国産と言われている。

（注１） フェーズ
基礎研究フェーズ：大学・国研などでの基礎研究のレベル
応用研究・開発フェーズ：研究・技術開発（プロトタイプの開発含む）のレベル
（注２） 現状 ※わが国の現状を基準にした評価ではなく、CRDS の調査・見解による評価である。
◎ 特に顕著な活動・成果が見えている、 ○ 顕著な活動・成果が見えている
△ 顕著な活動・成果が見えていない、 × 活動・成果がほとんど見えていない
（注３） トレンド
↗：上昇傾向、 →：現状維持、 ↘：下降傾向

(8) 参考文献

1）内閣サイバーセキュリティセンター（NISC）サイバーセキュリティ戦略本部 , “サイバーセキュリティ 2016（案）”, http://www.nisc.go.jp/active/kihon/pdf/cyber-security2016.pdf（閲覧日 2016-12-16）
2）井出 一仁 , “政府予算はサイバーセキュリティ分野が急伸”, http://itpro.nikkeibp.co.jp/atcl/watcher/14/334361/011400462/（閲覧日 2016-12-16）
3）内閣サイバーセキュリティセンター（NISC）情報セキュリティ政策会議 , “情報セキュリティ研究開発戦略（改定版）,” http://www.nisc.go.jp/active/kihon/pdf/kenkyu2014.pdf（閲覧日 2016-12-16）
4）Barack Obama, “The Budget Message of the President,” https://obamawhitehouse.archives.gov/sites/default/files/omb/budget/fy2017/assets/message.pdf（閲覧日 2017-3-1）
5）内閣サイバーセキュリティセンター（NISC）情報セキュリティ戦略会議 , “新・情報セキュリティ人材育成プログラム ,” http://www.nisc.go.jp/active/kihon/pdf/jinzai2014.pdf（閲覧日 2016-12-16）
6）内閣サイバーセキュリティセンター（NISC）サイバーセキュリティ戦略本部 , “サイバーセキュリティ人材育成総合強化方針 ,” http://www.nisc.go.jp/conference/cs/jinzai/dai03/pdf/ 03sankoushiryou01.pdf（閲覧日 2016-12-16）
7）文部科学省 , “情報技術人材育成のための実践教育ネットワーク形成事業”,

http://www.mext.go.jp/a_menu/koutou/kaikaku/itjinzai/index.htm（閲覧日 2016-12-16）
8）European Commission, “Horizon 2020,”
http://ec.europa.eu/programmes/ horizon2020/（閲覧日 2016-12-16）
9）European Commission, “Factsheet: Horizon 2020 budget,”
http://ec.europa.eu/research/horizon2020/pdf/press/fact_sheet_on_horizon2020_budget.pdf（閲覧日 2016-12-16）
10）CyberROAD（Development of the CYBER crime and CYBER terrorism research ROAD map）
http://www.cyberroad-project.eu/（閲覧日 2016-12-16）
11）CAMINO（Comprehensive Approach to cyber roadMap coordINation and develOpment）
http://www.fp7-camino.eu/（閲覧日 2016-12-16）
12）COuRAGE（Cybercrime and cyberterrOrism（E）Uropean Research AGEnda）
https://www.courage-project.eu/（閲覧日 2016-12-16）

3.5.3　認証・ID 連携

（1）研究開発領域の簡潔な説明

ユーザーが安全かつ簡便に、さまざまなサービスを利用するためには、確実な認証を行う必要がある。限られた利用環境における認証だけでなく、さまざまな情報デバイスを利用し、さまざまな地点・時間においても確実な認証を行う柔軟で強固な認証技術が必要である。一方、クラウドコンピューティングを含むインターネット環境においては、サービスを提供するサイト間での情報連携を確実に行う必要がある。そのためには、複数サイト間での認証と、認証の対象となるユーザーが持つ属性情報の集合体（ID: アイデンティティー）を連携（フェデレーション）して利用するためのフレームワークであるアイデンティティー連携（ID 連携）が必須である。また連携した際、認証されたユーザーが利用可能となる範囲、例えば利用可能時間帯や利用可能アプリケーションを厳格に認可することが必要である。本領域では、このような多様な利用環境とサービス連携への対応に必要となる認証・ID 連携のアーキテクチャーの研究開発を行う。

（2）研究開発領域の詳細な説明と国内外の研究開発動向

PC だけでなく、スマートフォンやウエアラブル・デバイス等のさまざまなデバイスをユーザーが利用する環境が進化する一方、インターネット上での単独運用によるサービス提供サイトだけでなく、複数のクラウドコンピューティング環境上で、さまざまな情報を連携したサービスが増加している。連携されるさまざまな情報の中には、漏えいしてはならない機微な属性情報も数多くあり、サービスを利用しようとするユーザーを確実に特定することが必要である。すなわち、さまざまなデバイスに対応した高度な認証技術が必要である。また、認証技術の範囲は、人やモノの特定と確認だけではない。人の場合、本人の存在性の確認に加えて、本人に対する権限付与も必要である。例えば、「社員として認められる（本人の存在性確認）が、一般社員なので機密情報にはアクセスできない（権限付与）」といった認証プロセスが必要である。一般に、存在確認のための行為を狭義の「認証」（Authentication）と呼び、権限付与行為を「認可」（Authorization）と呼ぶ。認証と認可は、本人が保有するさまざまな属性情報（Attribute）すなわちアイデンティティーによって決定される。

一方サービスにおいては、インターネット上の単一のサイトのみによって提供されるのではなく、直接サービスを提供するサイト以外で認証を行うような複数のサイト間における認証連携が増加する。そのために、サービスを提供するにあたっても複数のサイトに散在する属性情報を流通させる技術が必要となっている。ID 連携技術は複数サイト間で認証情報を連携させ、属性情報を流通させるために必要な技術である。

［認証技術の世界的動向］

世界各国で頻発するサイバー攻撃や ID 窃盗等に対処するため、さまざまな認証方式が研究開発されている。インターネット上で提供されるサービスにおいては、ユーザー ID とパスワードの単純な組み合わせによる認証方式から、ハードウエアトークンを用いた認証方式、複数の要素を組み合わせた多要素認証、過去の利用環境等との差分を分析するリ

スクベース認証等、さまざまな認証方式が研究開発されている。

IC カードを利用した認証は全世界的に非常に幅広く適用されている。接触型だけでなく NFC のような非接触型も適用が進んでいる。

スマートフォンを中心としたモバイルデバイスでは、内蔵のカメラや音声を利用した認証方式が研究・開発されている。指紋認証は、iOS のようなスマートフォン OS では、標準認証方式としても実装されている。また、NFC を内蔵したスマートフォンも多く出荷され、一部では IC カードの代替としても利用が広がっている。

一方、大量の情報を処理可能なコンピューティング環境が整備され、従来では不可能であった機械学習や AI と呼ばれる技術分野、グラフ理論を適用した技術分野、ブロックチェーンを利用した技術分野等の新しい技術研究を認証と組み合わせる最先端の研究開発が進んでいる。

［ID 連携技術の世界的動向］

複数のサイトを連携しサービスを提供するために ID を連携し、一度のサイトへのログインで複数のサイトが利用可能になるシングルサインオン（Single Sign On：SSO）の技術が開発され、ブラウザーベースの SSO だけでなく、スマートフォン等のデバイスや、ブラウザーを利用しない方式も開発・実装されている。SOAP（Simple Object Access Protocol）を利用し XML で記述されたセキュリティー情報を複数サイト間で交換する SAML（Security Assertion Markup Language）の技術[1)]は、SSO 機能を実装することが可能であり、2000 年代前半に標準化団体 OASIS（Organization for the Advancement of Structured Information Standards）で開発された。現在は高い信頼性を必要とする企業間 ID 連携やクラウド間 ID 連携において、多くのクラウドベンダーが SAML をサポートしている。また、REST（Representative State Transfer）ベースのプロトコルを利用した実現技術としては、2000 年代後半に登場した OpenID[2)] や OAuth[3)] を利用した方法、さらには OAuth をベースに発展させた OpenID Connect はここ数年で研究・開発され、コンシューマー向けサービスやソーシャルアプリケーションを中心に、クラウド上でも実装されている。

また、ID 連携を発展させ、複数のサイトに散在するユーザーの属性情報を流通する技術も研究・開発され、サービスへの実装も行われている。

［認可技術の世界的動向］

サービスを提供するにあたって、必要な情報を構成する複数のサイト間で認可情報をやりとりする技術は、2000 年代の早いうちに標準化が図られ、SOAP プロトコル上に XACML（eXtensible Access Control Markup Language）[4)] として仕様が策定され今日でも引き続き拡張が行われている。一方、ネットサービスが広がるにつれ、REST 方式で認可情報のやり取りが必要になり、策定された技術仕様が OAuth である。OAuth の仕様を組み合わせることによって、認証を行うことも可能となっている。 認可を与えるには認証を受けたユーザーに関連した属性値を利用して判断する。

(3) 注目動向

［FIDO（Fast Identity Online）］[5)]

認証デバイス間での相互運用性や、パスワード管理の煩わしさを排除すべく、パスワード認証に代わる新たな認証方法の開発に取り組む組織として、2012 年 7 月に設立された非営利団体。UAF（Universal Authentication Framework）、U2F（Universal 2nd Factor）の 2 種類のプロトコルが開発されている。

［トラストフレームワーク］[6)]

異なる組織間での ID 情報の交換は、個人情報の悪用や漏えいのリスクがある。そこでポリシーやルールを明確にした上で、信頼できる組織を認定し、それらを連携させることによって、企業ごとのユーザーの登録・認証を別々に行うことなく、アイデンティティー情報を異なる組織や機関間で交換することを可能にする。

［マイナンバー］[7)]

わが国において、社会保障と税の一体改革を実現する手段として、国民に唯一無二の個人番号を付与し、行政手続きの効率化を行う。さらに将来の民間との連携等を視野に入れた制度である。個人番号を利用するために、耐タンパー性の高い IC カードの配布が予定されている。将来的には IC カードのみならず、スマートフォン内臓の NFC（Near Field Communication）による認証手段や、トラストフレームワークによる民間等他の認証フレームワークとの相互接続も課題としている。

［学術認証フェデレーション］[8)]

我が国において、学術 e- リソースを利用する大学、学術 e- リソースを提供する機関・出版社等から構成された連合体。米国で開発された Shibboleth をベースに連携ネットワークの構築・運用を行う他、ID 連携に関する技術の研究・開発を行い、国際学会での発表も活発である。

［クラウドコンピューティング］

さまざまなサービスがクラウドベースで提供され始めている中で、クラウド間やオンプレミスの企業との ID 連携が必要である。また、認証・認可・属性管理等のサービスを提供するクラウドである IDaaS（IDentity as a Service）も広がり、日本でも提供する企業がでてきている[9)]。

［機械学習・AI］

以前より認証分野では特徴量計算による認証技術の研究開発が行われてきた。最近では廉価で汎用的なデバイスを利用した音声認識、画像認識によって特徴量計算が身近なものになっている。大量の情報を用いて複数のアルゴリズムにより、高速で正確な特徴量計算を行う機械学習の研究開発が進んでおり、例えばリスクベース認証には機械学習の研究開発結果が反映されている。代表的なアルゴリズムとして SVM（Support Vector Machine）があり海外では 2000 年代初頭から研究が行われている[10)]。

［グラフ技術］

1999 年に W3C が Semantic Web の標準化技術として RDF（Resource Description Framework）の策定を行った。テキストだけでなく画像等さまざまなリソースのメタ情報を記述することが可能となっただけでなく、リソース間の関係性も網羅、つまりグラフ表現できるようになった。一方、グーグルの創業者らが研究開発した Page Rank や、Facebook が提供する Graph API は人やモノの属性情報を持つノードとノード間の関係を示すエッジで構成されるグラフ表現（RDF と対比しこれらをプロパティグラフと呼ぶ）である。「平均 6 人『知人の知人』を介していけば全ての人とつながることができる」という「6 次の隔たり」もグラフで表現することができる。RDF やプロパティグラフは機械学習と密接に関わることもあり、グラフ技術を取り入れ認証技術が発展することが期待される。

［ブロックチェーン］

ビットコインで一躍有名になったブロックチェーンであるが、その適用範囲はさまざまな分野で研究されている。複数のノード間のトランザクションの正当性に注目し、認証への適用も考案されている [11]。一部では実際に特許を取得し先行者利益を得ようとする動きもある [12]。

（4）科学技術的課題

認証技術は、モバイルデバイスの進化による技術的進展がさらに期待できる。特に日本では、静脈認証や顔認証といった生体認証は実用化されており、より高精度な認証を行うべく技術の深みの追求をすべきであろう。また、スマートフォン内蔵のカメラを利用した虹彩による認証技術の研究等も行われており、モバイルデバイスを利用した認証技術は、国際的にも先を走り続けることが期待される。

一方、ID 連携技術の場合、技術的目標は「他のサービスと連携できること」であり、独自技術仕様を提供できる企業や機関は「他を凌駕した当該サービス市場において占有率（シェア）を持つこと」にある。しかし最近では、Facebook や Twitter 等でも、ID 標準技術をベースに拡張する傾向にあり、全く新しい技術をゼロから基礎研究して開発を行っていない。従って、ID 連携技術の場合は、短期においては、応用研究・開発に重点を置く方向にある。

機械学習・AI、グラフ技術、ブロックチェーンの分野は、日本の取り組みは十分とはいえない。より高度な認証技術を研究開発する場合、これらの技術に対する取り組みは必須であると考えるが、セキュリティー分野とこれら機械学習等の分野の両方の技術を持ち合わせている研究者や技術者は日本には非常に少ないと思われる。その中で、例えばブロックチェーン技術を認証に組み入れる取り組みが日本でもいくつかでてきている [13),14)]。セキュリティー分野は最近では学際的な分野として取り扱われる機会が増えて来たと思われるが、最新の機械学習やグラフ技術は、数学や統計学に対する理解力と応用力が必須であり、国際的な技術力向上のためにはその対策を講ずることは避けて通れないと思われる。

(5) 政策的課題

機械学習やグラフ技術を取り入れた認証技術を小さな実証を重ねて研究することは、クラウドや OSS、企業が提供する実験環境等を利用することによって可能であるが、実用化には本格的な実証が不可避であり、それには多量な実験データが必要である。しかし、昨今のプライバシー / 個人情報保護が叫ばれる中、実験に必要な大量のデータを入手しにくくなっている。一方、ブロックチェーンの場合、ビジネスによる利益期待が大きいため、十分な実証と検証を行わずに本番サービスに導入され、後のトラブルに繋がる可能性も危惧されている。社会への適用時の信頼性・安全性確保のために、十分な技術研究開発を行う必要があり、法制度的な扱いや特区のような政策的なサポートも必要と考える。

(6) キーワード

アイデンティティー、認証連携、フェデレーション、強固な認証、生体認証、プライバシー、マイナンバー、機械学習、AI、グラフ、ブロックチェーン

(7) 国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	△	→	・認証分野：生体認証では顔認証等の研究のように、世界に先んじて進んでいる分野がある。また国内外への論文投稿も活発であり研究が進んでいるとみられる。 ・機械学習、グラフ技術の技術を認証技術へ適用する研究は少ない。ブロックチェーンは幾つかの例が散見される [13]。 ・ID 連携分野：日本独自の基礎研究は進んでいない。
	応用研究・開発	△	↗	・認証分野：顔認証の実証実験等、認証精度向上・問題点克服のための研究・開発・実証が進んでいる。IPA では生体認証の導入・運用についてのガイドラインを公開している [15]。 ・機械学習、グラフ技術等の技術を認証技術へ適用する基礎研究が進んでいないため応用研究に結びつかない。ブロックチェーンは基礎研究から応用研究・開発のフェーズでの十分な実証を行われず実用試行のケースもある [14]。 ・ID 連携分野：学術認証ネットワーク（学認）による ID およびサービス連携のための応用研究・開発が進んでおり、国際学会での発表も多く行っている。学認が開発した uApprove.jp は本人同意による属性提供を実装している。 ・認証と ID 連携の広範囲の適用として期待されるものに、将来医療等を含み、広範囲の用途が考えられているマイナンバーとそれを支えるシステムがあり、さまざまな実証が行われている [16]。
米国	基礎研究	◎	↗	・認証分野：国防関連を含め生体認証の研究が進んでいる。 ・ID 連携分野：ネット企業を中心に民間での研究が進んでいてる。 ・機械学習、グラフ技術、ブロックチェーン等の技術を認証技術へ適用する多くの研究が行われている。[11]
	応用研究・開発	◎	↗	・認証分野：官民の重要施設や安全保障対策を優先として、応用研究・開発を行っている。 ・機械学習、グラフ技術、ブロックチェーン等の技術を認証技術へ適用し、応用も進みいくつかは実用化の域に達している。米国特許取得の例もある [12]。 ・ID 連携分野：ネット企業を中心に民間での応用研究が進んでいて、積極的に技術標準化のイニシアチブをとる。IETF や W3C のようなインターネット中心の規格に大きな影響力を行使している。

欧州	基礎研究	△	→	・認証分野：欧州の通信会社を中心とした研究が以前は多かったが、最近は特筆すべき顕著な研究成果が見受けられない。 ・機械学習、グラフ技術、ブロックチェーン等の技術を認証技術へ適用する研究は少ない。 ・ID 連携分野 :EU のプライバシー保護の動きと併せ、プライバシーと併せた関連研究が散見される。
	応用研究・開発	○	→	・認証分野 :EU の eID や EU 諸国の電子政府を中心としたシステムのための認証技術に関する応用研究・開発が進んでいる [17]。 ・機械学習、グラフ技術、ブロックチェーン等の技術を認証技術へ適用する基礎研究が進んでいないため応用研究に結びつかないと思われる。 ・ID 連携分野 :EU の TAS3 プロジェクトでは 2011 年までに大規模な ID 連携実証実験を行った [18]。
中国・韓国	基礎研究	△	→	・特筆すべき顕著な研究成果が見受けられない（公開されていない）。
	応用研究・開発	△	→	・特筆すべき顕著な研究成果が見受けられない（公開されていない）。

（注１） フェーズ
基礎研究フェーズ：大学・国研などでの基礎研究のレベル
応用研究・開発フェーズ：研究・技術開発（プロトタイプの開発含む）のレベル
（注２） 現状　※わが国の現状を基準にした評価ではなく、CRDS の調査・見解による評価である。
◎　特に顕著な活動・成果が見えている、 ○　顕著な活動・成果が見えている
△　顕著な活動・成果が見えていない、 ×　活動・成果がほとんど見えていない
（注３） トレンド
↗：上昇傾向、 →：現状維持、 ↘：下降傾向

(8) 参考文献

1）OASIS（Organization for the Advancement of Structured Information Standards）, “OASIS Security Services（SAML）TC”
https://www.oasis-open.org/committees/security/（閲覧日 2016-12-16）
2）OpenID Foundation, http://openid.net/developers/specs/（閲覧日 2016-12-16）
3）Dick Hardt, “The OAuth 2.0 Authorization Framework”
http://tools.ietf.org/html/rfc6749（閲覧日 2016-12-16）
4）OASIS eXtensible Access Control Markup Language（XACML）
https://www.oasis-open.org/committees/xacml/（閲覧日 2016-12-16）
5）FIDO（Fast IDentity Online）Alliance Consortium, “FIDO Alliance”
https://fidoalliance.org/（閲覧日 2016-12-16）
6）経済産業省 , “ID 連携トラストフレームワーク”
http://www.meti.go.jp/policy/it_policy/id_renkei/（閲覧日 2016-12-16）
7）内閣官房 , “社会保障・税番号制度”
http://www.cas.go.jp/jp/seisaku/bangoseido/（閲覧日 2016-12-16）
8）学術認証フェデレーション , “学認（GakuNin）”
https://www.gakunin.jp/（閲覧日 2016-12-16）
9）山田 高 , “法人向け IDaaS「KDDI Business ID」提供開始 !”（KDDI Cloud Blog 2014.07.29 記事）
http://cloudblog.kddi.com/idaas/230/?v=block（閲覧日 2016-12-16）
10）Kenneth Jonsson, Josef Kittler, Yong Ping Li, and Jiri Matas, “Support vector machines for face authentication”, Image and Vision Computing Vol. 20, No. 5-6,

pp. 369-375（2002）.
11）David Shrier, Weige Wu, and Alex Pentland, “MIT Blockchain & Infrastructure（Identity, Data Security）Report”（MIT, 2016）.
http://cdn.resources.getsmarter.ac/wp-content/uploads/2016/05/MIT_Blockchain_Infrastructure_Report_Part_Three_May_2016.pdf（閲覧日 2016-12-16）
12）Justin Fisher, Maxwell H. Sanchez, “Authentication and verification of digital data utilizing blockchain technology”（U. S. Patent 20160283920 A1: 2016-09-29）.
http://www.freepatentsonline.com/y2016/0283920.html（閲覧日 2016-12-16）
13）東京大学大学院情報理工学系研究科附属ソーシャル ICT 研究センター , “次世代個人認証技術講座 実証実験 ～ MITHRA Project ～”
http://www.sict.i.u-tokyo.ac.jp/news/mithra/（閲覧日 2016-12-16）
14）Keychain Pte. Ltd., “分散型認証プラットフォーム Keychain”,
http://keychain.jp/one-page/index.html（閲覧日 2016-12-16）
15）独立行政法人 情報処理推進機構（IPA）, “生体認証導入・運用の手引き”
https://www.ipa.go.jp/files/000024404.pdf（閲覧日 2016-12-16）
16）総合科学技術会議 科学技術イノベーション政策推進専門調査会 ICT 共通基盤技術検討ワーキンググループ , “日本の医療を取り巻く状況と医療 ICT の利活用 医療健康共通基盤”（第 6 回会合資料）
http://www8.cao.go.jp/cstp/tyousakai/innovation/ict/6kai/siryo2-3.pdf（閲覧日 2016-12-16）
17）European Commission, “Trust Services and eID（electronic IDentification）”
http://ec.europa.eu/digital-agenda/en/trust-services-and-eid
（閲覧日 2016-12-16）
18）Trusted Architecture for Securely Shared Services（TAS^3）Consortium, “The TAS^3 Integrated Project”
http://vds1628.sivit.org/tas3/（閲覧日 2016-12-16）

3.5.4　プライバシー情報の保護と利活用

（1）研究開発領域の簡潔な説明

プライバシーを保護したままでデータベースから共通の傾向や固有のパターン等の有益な知識を抽出する。技術を大きく分類すると、(1) 個人を識別不能にする匿名化技術、(2) プライベートなデータを暗号化したままで任意の計算を実行する秘匿計算技術、(3) プライバシー保護した上でデータマイニングを実施する技術、(4) 抽出された知識からプライベート情報が漏えいしない様に精度を落としたりノイズを加えたりする差分プライバシー技術がある。

（2）研究開発領域の詳細な説明と国内外の動向

［背景と意義］

多くの企業が顧客の情報や購買履歴を管理して、ビジネスに活用する動きが加速している。いわゆる、ビッグデータと呼ばれる、大規模で機械的に収集される多量のデータがあらゆる分野で注目を集めている。例えば、わが国において特定機能病院を対象に導入されている、疾患と治療の記録からなる DPC（Diagnosis Procedure Combination）データセットは、700 万人の患者のデータを格納し、急性入院の約 50% を電子化している。多量で多様な電子化データに基づいて、疾病や債券市場の動向の予測、都市計画や防災対策などの従来考えられなかった新しい価値が創造されようとしている。

その一方で、ビッグデータの活用から生じるプライバシーの課題も浮き上がってきた。2013 年 7 月には、JR 東日本が交通系 IC カード Suica4300 万枚の乗降履歴を市場調査を目的として利用者の同意なく日立製作所に販売していたことが報道されて、大きな批判を浴びた。氏名や連絡先などの個人を特定する情報は除外されていたが、カードに割り当てられた ID は一月単位で保存されており、乗降駅の履歴を積み上げることで個人を識別されるリスクが残っていた。自分の情報が再識別されることを懸念した多くの利用者が利用停止を求めることとなった。2014 年 7 月には、ベネッセホールディングスが、「進研ゼミ」や「こどもちゃれんじ」などで知られる教材の受講者の氏名や生年月日などの 760 万件の個人情報を外部に流失したことを明らかにした。データベースの管理をしていた委託先の技術者がスマートフォン経由で情報を抜き出して、名簿業者に販売していた。漏えい対策のための倫理教育やマネジメントシステムを整備しても、悪意のある内部者による不正行為を防止することが困難であること、そして、漏えいした顧客情報を流通させるマーケットが存在していることが認識された事件であった。

2003 年に制定された個人情報保護法は、制定当時は存在していなかったスマートフォンや Suica の様なデバイスから個人が識別されることを想定していなかった。従来の仕組みでは個人情報ではないが、ビッグデータの普及に伴って、個人が識別されたり利用者が意図しない追跡が行われたりする可能性のある情報、いわゆる、グレーゾーンの存在が顕在化してきた。そこで、2015 年、保護法が改正され、2016 年から個人情報の監視や検査権限を有する個人情報保護委員会が発足し、2017 年から全面施行を予定している。改正された大きな項目は次の通りである [1]。

1） 個人情報の定義の明確化
個人識別符号（第 2 条 2 項）、要配慮個人情報（第 2 条 3 項）
2） 個人情報の有用性確保
匿名加工情報（第 2 条 9 項）、認定個人情報保護団体による個人情報保護指針（第 53 条）
3） 個人情報の保護を強化
個人情報データベース等提供罪（第 83 条）
4） 個人情報保護委員会の新設と権限（第 5 章）
5） 個人情報の取り扱いのグローバル化
国境を越えた適用（第 75 条）、外国執行局への情報提供（第 24 条）
6） オプトアウトの扱い
届出厳格化（第 23 条 2 項）、利用目的の変更禁止（第 15 条 2 項）

問題となっていたグレーゾーンとされていた身体の特徴に関する情報や携帯電話や免許証などのデバイスの番号なども取り扱いの対象として広げる一方で、個人を再識別するリスクを低減するためのプライバシー保護技術の活用も想定している。

海外でもビッグデータの活用のための法整備は進んでいる。ビッグデータという概念を産んだ米国では、2012 年に企業が行う個人情報の収集に対して、利用者が主張できる権限をまとめた「消費者プライバシー権利章典」を公表している。企業が収集している情報の種類やその活用方法の情報は、消費者に正しく提供されるべきである。企業に追跡されることを拒否できる Do-Not-Track 原則などの権利も認められるべきことがうたわれている。欧州では、データが国境を越えて流通する時は、データの保護が十分であるかどうかを認定することを定めた EU データ保護規則（GDPR）が 2016 年に成立した。

このように、プライバシーを保護することと、ビッグデータを活用するという二つの大きな要請があり、国内外の法整備は着々と進んでいる。しかし、技術的には両者を完全に満足することはそれほど容易ではない。ビッグデータとひとくくりにするにはデータは多様であり、その粒度、頻度、アクセスの方法はさまざまである。個人を識別しようとする攻撃者にもさまざまなタイプがあり、匿名化されたデータと照合できるどんな情報を持っているかを事前に決めることはできない。例えば、クレジットカード運用会社にとって、カード番号から個人を特定することは容易であるように、照合性の容易性には一様な基準はない。さらに、単に乗車駅と利用日時を知られても気にしない利用者もいれば、ストーカーに追われている利用者にとっては深刻な情報であったりするように、プライバシーの感じ方には主観的な曖昧さが避けられない。

［これまでの取り組み］

ここでは、プライバシー保護技術を（1）匿名化技術、（2）秘匿計算技術、（3）プライバシー保護データマイニング技術、（4）差分プライバシー技術に分類して、それぞれの取り組みを示す。

1） 匿名化技術

匿名化の処理は、ISO/TS 25237（Health informatics – Pseudonymisation）の中で、

データとデータ主体（所有者）との間の相関を取り除くプロセス、と定義されている。最も簡単なものは、氏名などの情報を仮の疑似 ID と置き換える仮名化である。しかし、2001 年に Samarati が、氏名を削除しても、性別や年齢、郵便番号などの本人に関する静的な属性情報を束ねることで、本人を識別する疑似 ID（QI:Quasi Identifier）として利用できることを指摘し、集合として評価した個人識別の度合いを与える *k*- 匿名性（k-anonymity）[2] の概念を初めて提唱し、その後のさまざまなアルゴリズムの研究が行われた。Sweeney による定式化 [3] が行われ、QI の数で定義した *k*- 匿名性を発展させ、最頻度のアイテムが 1/l の確率でしか識別できないことを保証した *l*- 多様性（l-diversity）[4]、それに加えてセンシティブ属性が閾値 t より離れていることを保証した t- 近似性（t-closeness）などの研究が行われた。

匿名化の評価指標にはいくつもの定義があるが、それらを保証する匿名化の方法は一意ではない。属性を削除したり、値を一般化したりする組み合わせがあり、Yao らによりその匿名化問題は NP- 完全問題に属する困難な問題であることが証明されている [5]。従って、大規模な問題に対して誤差を最小化する匿名化を求めることは現実的ではなく、事前に閾値を用意して枝刈りを施したり、トップダウンにデータセットを分割したり、ボトムアップに分割されたデータセットを統合することで匿名性の保証を得るアルゴリズムがいくつか開発された。Incognito[6] や Anatomy[7] などが知られている。製品の開発も盛んであり、オープンソースにも、例えば University of Texas, Dallas 校の UTD Anonymization Toolbox[8] などが知られている。ここでは、前述の Incognito に加えて、Datafly, Mondrian Multidimensional k-Anonymity, l-diversity, t-closeness, Anatomy の 6 つの代表的なアルゴリズムが実装されている。

理論的な匿名化の指標やアルゴリズムの定義、それらの効率的な実装が行われ、今後はそれらをさまざまなビッグデータに適用する際に生じるさまざまな応用研究が進むとみられる。例えば、GPS などの位置情報の時系列データである、いわゆる trajectory data（移動経路データ）から個人が特定されないようにする要求は大きく、ITS の普及と相まってこれから盛んになることが予想される。Peloponnese 大学のグループは、多次元になる GPS の時系列データを匿名化する閾値ベースの研究 [9] を行い、疑似位置データを用いた実験を重ねている。Facebook などのソーシャルネットワークサービスにおけるプライバシー保護も重要な課題である。多くのサービスではアカウント作成が無料で行われるために、偽の利用者を容易に許してしまい、それらを用いた個人情報の抜き取りが深刻な脅威になっている。これらに対して、自然言語処理を用いて投稿に対して匿名化のレベルを制御したりする研究が今後盛んになるとみられる。Illinois 大学 Chicago 校（米）の Yu らのグループはグラフ理論を用いて、仲介者の数を制御することで、そういった脅威を抑制する研究 [10] を試みている。

2015 年には我が国において個人情報保護法が改正された。この改正法において、従来の個人情報に加え、匿名加工情報と呼ばれる新しい取扱いのスキームが新設されたことは注目に値する。個人情報に特定の個人を識別することができないように個人情報を加工したものを匿名加工情報と定義し、その加工方法を定めるとともに、事業者による公表などその取扱いについての規律を設けている。具体的な加工方法については、現在も検討が行われている。「特定の個人を識別することができないように個人情報を加工すること」に

は *k*- 匿名性の達成も含まれると考えられ、今後我が国における個人情報の加工方法として、*k*- 匿名化やそれに関連する匿名加工技術は実務的に重要な技術となる可能性が高い。

2） 秘匿計算技術

データを開示することなく、複数のデータの統計処理を行えれば、プライバシー漏えいの危険性が減る。これを秘密計算と言うが、秘密計算にはこれまでに大きく分けて、秘匿計算、準同型性暗号系による暗号プロトコル、秘密分散に基づく秘密計算、の三種類の実現方式が知られており、それぞれの方式には計算効率性や計算モデルの自由度の観点において、長所と短所がある。

ここでは、秘匿計算、あるいは秘匿回路計算（SFE:Secure Function Evaluation）について述べる。秘匿計算は、入力値を秘匿したままで任意の関数（回路）を評価する技術である。入力の一部を持つ複数の入力者と回路評価者との間で関数評価が行われるので、マルチパーティープロトコル（Multi Party Protocol）とも呼ばれる。1）の匿名化には、匿名性の強さに応じた再識別のリスクが残っていたのに対して、この技術では暗号化や秘密分散を用いて平文の情報を 1 ビットも漏えいさせないことを試みる。プライバシー情報を秘匿したままで、いかなる解析アルゴリズムも実行することができる理想の技術である。

後に Turing 賞受賞者となる Andrew Yao がこの理論を最初に提案したのは、まだ公開鍵暗号が提案されて間もない 1986 年のことであった [11]。しかし、任意の回路を秘匿計算できるというその自由度の代償として、ビットレベルで信号を暗号化しなくてはならず、膨大な計算コストのために実用性はなく、長い間理論研究者の興味の対象であった。この間、暗号化の代わりに秘密分散を用いるプロトコルなどの多くの理論整備が行われた。

計算機技術の発達とプライバシー保護の強い要請に押されて、ようやく実装されたのは当初の提案より 18 年後の 2004 年、イスラエルの Malkhi らによる研究グループが Usenix Security で発表した Fairplay[12] である。Fairplay は高級言語レベルで記述されたプログラムソースをゲートレベルの回路記述言語にコンパイルし、それらを 2 台の仮想マシンの間で暗号化と復号化を繰り返して回路での実行をする。基本的な算術計算と限定された条件分岐機能しかなく、例えば乗算でさえ加算の繰り返しを用いて自分で実装しなくてはならなかった。それでも、試験実装したシステムを公開しており、その後の本分野の研究を活性化する原動力となった。

Fairplay 以降も多くのシステム開発が続いている。Fairplay の 2 者を複数プレーヤー間で実行するような拡張 Fairplay-MP や、SEPIA, TASTY, VIFF などの多くの SFE 実装系が発表されている。置換ネットワークと呼ばれる専用回路のアイデアを用いて高速に秘匿積集合を計算するシステムの開発 [13] や、Virginia 大学のグループによる新しいコンパイラー（Billion-gate）は従来のメモリーの制約を取り除き、SFE の技術をより実用レベルに近づけた [14]。中でも、Tartu 大学（エストニア）の Dan Bogdanov が開発した Sharemind [15] は、秘密分散を要素技術にした汎用の SFE コンパイラであり、ソフトウエア開発キット（SDK:Software Development Kit）を提供したりライセンシングを進めたりしており注目されている。ソートや統計処理などの Sharemind ベースの研究にもつながっている。Sharemind プロジェクトのウェブ [16] からデモンストレーションを行って

いる。

国内の秘匿計算の試みとして、NTT セキュアプラットフォーム研究所の MEVAL[17] がある。MEVAL は、秘密分散型の秘匿計算の処理系であり、100 万件の加算、乗算、大小比較、ソートをそれぞれ、1.5 ミリ秒、135.1 ミリ秒、286.8 ミリ秒、6875 ミリ秒で実行できることが報告されている。2013 年のデータで、乗算は Sharemind の 10 倍高速である。

3） プライバシー保護データマイニング技術

プライバシー保護データマイニング（Privacy-Preserving Data Mining, PPDM）は利用者のプライバシーを保護してビッグデータの活用を実現する技術である。

PPDM 研究の原典は、2000 年に発表された二つの全く同名の論文である。一つは、イスラエルの Lindel と Pinkas によって暗号理論のトップカンファレンスである CRYPTO で発表された "Privacy Preserving Data Mining"[18] であり、もう一つも機械学習のやはりトップ会議の一つである ACM SIGMOD で発表された "Privacy-preserving data mining"[19] である。前者は公開鍵暗号を用いて秘匿しながら対数計算を実行し、後者はランダムなデータを入力に加えてマイニング処理を行い、ベイズの定理に基づいてノイズを除去する再構築アルゴリズムを提案している。興味深いことに、両者とも同一の情報エントロピーに基づく決定木学習アルゴリズム ID3 を秘匿しながら実行するものであった。

この二つの論文を出発点として、多くの研究が行われ、一つの分野の様に発達している。データマイニングアルゴリズムにはさまざまな種類があるので、そのそれぞれをプライバシー保護する試みが 2000 年代初頭には行われた。ナイーブベイズ学習、決定木学習、クラスタリング、相関ルール抽出[20]、情報推薦、協調フィルタリングなどである。これらのアルゴリズムの解説については、Aggarwal と Yu によるサーベイ "Privacy-Preserving Data Mining: Models and Algorithms"[21] が良書である。

PPDM の主な要素技術には、加法準同型性を満たした公開鍵暗号アルゴリズムとそれを用いた秘匿内積プロトコル[22] や 2）で述べた秘匿回路計算 SFE がある。条件を満たす準同型性暗号として、Paillier 暗号[23] や楕円曲線暗号がよく知られている。デファクト標準の RSA 公開鍵暗号は、乗法の準同型性を満たしているが、平文が同じならば暗号文も同じになる性質を持っているために利用できない。一般に、秘匿計算部分はビット長に応じて大きなコストがかかるので、秘匿内積で計算できるところは極力そちらで行い、比較や等号処理等の準同型性暗号を用いると困難なところだけを SFE で行うことが多い。このスタイルの代表例に、Vaidya と Clifton の相関ルール抽出[20] がある。一方、秘匿内積を使わないで、分散管理された複数の集合の積集合を秘匿して求める問題もよく用いられる。積集合の大きさを求めれば、クロス集計や頻出アイテムの評価を与えるからである。この秘匿積集合には、入力する値と多項式の係数をそれぞれ異なるパーティーが保有し、秘匿したままで関数の出力値のみを求める秘匿多項式評価プロトコルが要素技術として構成される。Freedman らによるプライベートマッチングプロトコル[24] が代表例であり、Camenisch らによってさらなる効率化[25] が行われている。

これらの要素技術の研究開発や安全性評価は 2000 年代にほぼ完成していて、実現可能性は確認されている。しかし、ビット長に比例してかかる暗号化のコストが大きく、実用

化のレベルには至っていない。改良されたアルゴリズムや小規模のデータセットに、適用範囲は限定されている。この技術的な困難さを改良するために、加法準同型性だけでなく乗法の準同型性も保証する環準同型性暗号などの暗号要素技術の改良が重ねられている。

暗号要素技術のブレークスルーを待つ間は、たとえ大きな処理コストと時間をかけても見合うだけの、極めてプライバシーの要求が強い分野から PPDM の適用が進むものと予想される。あるいは、*k*- 匿名性などで失われる精度が許容できないほど高い精度を必要とする分野にも適用の可能性がある。これらの例には、ゲノムデータの解析や臨床疫学などの医療分野があげられる。文献 [26] では、健康診断の結果により得られたピロリ菌に感染した患者リストと、地域がん登録で得られた胃がん患者のリストを秘匿したままマッチングすることで、ピロリ菌のがん罹患に関する相対危険度を求める実験が行われた。

クラウドに委託したデータの漏えいを防止してそのサービスを活用するために、さまざまな検索可能暗号方式が提案されている。Boneh らは、データ所有者が公開鍵を用いてデータを暗号化してクラウドに保管し、秘密鍵を持つ利用者が検索用のタグを生成して、クラウドに検索を実行させる公開鍵検索可能暗号（Public Key Encryption with keyword Search: PEKS）を提案した [27]。これを元にして、キーの連言検索や範囲検索を可能とする方法 [28] などいくつもの改良が試みられている。松田らは、階層型 ID ベース暗号を用いてマルチユーザーへの対応を可能とする方式を提案し、ブラウザーと Web サーバー間で SQL 文による検索を可能とするシステムを実装している [29]。

4） 差分プライバシー技術

差分プライバシー技術とは、データベース問い合わせとその応答に関わる情報漏えいを理論的に評価し、その対応策を与える技術である。多数の個人に関するデータが蓄積されたデータベースに対して、統計的な問い合わせを行い、その応答値から、問い合わせ対象としたデータベースに、ある個人が含まれているか否かが判定可能であるというリスクを低めるために、統計値を雑音によって摂動させ、開示することによりプライバシーを保護する。与えられた母集団数と対象クエリについて、その応答値に加えるべき雑音の分散の上限が理論的に求められる。

差分プライバシーの研究は 2006 年の Dwork らの研究 [30] に端を発し、以降、理論計算科学、暗号理論、データ工学、機械学習等、多数の理論分野にわたり、主に理論的アプローチの下で複合的に発展しつつある。差分プライバシーのモデルは、暗号理論における標準的な安全性定義として用いられている「識別不可能性」の議論を下敷きとしていることから、以前から積み上げられてきた理論的な安全性解析との親和性が高い。また、その安全性が攻撃者の背景知識によらないことから、*k*- 匿名性等に比べより強力な安全性を保証できる。ただし、差分プライバシーを達成するためには、クエリ応答値に非常に分散の大きい確率分布から得た雑音による摂動を与えることが必要な場合があることから、実用に耐えない場合もあるが、以下のような実用化も始まっている。Google は Web ブラウザーである Chrome に RAPPOR（randomized aggregatable privacy-preserving ordinal response）と呼ばれる差分プライバシーを用いたユーザー統計の収集フレームワークを実装している。Chrome を利用する多数のエンドユーザーから数値や文字列の情報を受け

取り、これを集約して統計情報を得るときに、集計者はユーザー個別の情報を得ることになり、プライバシー上の懸念がある。RAPPOR では、chrome から情報送信する際に、ユーザーの手元で情報をランダム化した上で情報提供し、集計者側からはユーザー個別の情報が特定されないことを差分プライバシーの定義において保証している。また、Apple は iOS10 において多数ユーザーの利用パターンの解析において、個別データの Privacy を保護するために差分プライバシーを利用していると公表している。

［今後必要となる取り組み］

現在のプライバシー保護技術を実サービスに適用するにあたって、今後次のような取り組みが求められると考える。

・利用者の同意を取る仕組み
データの所有者とデータをひもづけて、利用目的の変更や第三者提供に対して同意や利用停止などの制御を可能とする仕組み。

・匿名化されたデータを交換するためのフォーマットの標準化
XML や JSON などの標準的なフォーマットの上で、データの種類と形式、匿名化措置の方法や程度、利用条件などのポリシーなどを記述する標準フォーマット。

・要求する匿名化レベルや提供するためのポリシー記述言語の標準化
プライバシー情報の所有者が自分の情報を誰にどこまで提供するかを定めたり、第三者に情報提供のための条件、提供先において受け取るための条件など、さまざまな論理的な条件を十分に表現するための記述言語。ポリシーを宣言することで、機械的な条件の判断や交渉を可能にする。

・PPDM（Privacy-Preserving Data Mining）でデータを交換するための通信プロトコルの標準化
プロトコルに従って暗号文を交換するためのデータ形式や制御メッセージの交換のための汎用的なプロトコル。暗号鍵や公開鍵証明書などの既存のフォーマットや TLS など通信プロトコルを応用して、PPDM で必要なマルチパーティーで行われる非同期通信を可能とする枠組みが必要である。

・匿名化されたデータやその提供者に対して、評判や信頼の度合いを提供するためのトラストフレームワーク
匿名化によって低減された個人識別のリスクやその情報発信者の評判などを交換するためのプロトコルや表現形式の標準化。

・漏えいしたデータを早期に検出する技術
P2P などで公開されているデータに違法なものや漏えいしている情報がないかを機械的に判断して、検出する技術の開発。

・SNS などへ情報を発信する際に、ポリシーに応じてプライバシー情報の検査をする機構
不用意な個人情報の公開を防止するために、自身で設定したポリシーに整合しない情報を発信する前に警告を与えるサービスや技術の開発。

・漏えいした情報を失効させる仕組み
やむなく漏えいしてしまったプライバシー情報や個人情報に対して、認証された管理者

のもとで迅速に失効させる技術とその制御プロトコル等の開発。

（3）注目動向（新たな知見や新技術の創出、大規模プロジェクトの動向など）

［注目すべきプロジェクト］

・Geographic Privacy-aware Knowledge Discovery and Delivery（GeoPKDD）[31)]
車や人等の動きのデータ（trajectory data）をプライバシーに配慮して現実的な知識抽出サービスを実現しようとするプロジェクト。イタリア Pisa 大学、スイス EPFL、ベルギー Hasselt 大学などの共同プロジェクト。

・MIT, CryptDB [32)]
SQL データベースにおけるクエリーとデータそのものを暗号化することで、不正なサーバー管理者に対して格納されているデータのプライバシーを保障するシステムの開発プロジェクト。通常の非暗号化された SQL データベースと遜色ないほどのパフォーマンスを実現している。

・University of Texas Dallas 校、UTD Anonymization Toolbox [8)]
匿名化アルゴリズムのツールボックスの開発プロジェクト。*k*- 匿名性などの多くのアルゴリズムをサポートして、Windows 版、Linux 版のツールボックスを公開している。

・独立行政法人産業技術総合研究所セキュアシステム研究部門「プライバシー保護データベース検索技術」プロジェクト [33)]
化合物データ、ゲノムデータ、地質データなどのデータベース提供者に対して、検索クエリーを知らせないで検索を実現するプロジェクト。生命情報工学研究センターと共同して、製薬開発分野における応用を検討している。

・JST CREST プロジェクト、自己情報コントロール機構を持つプライバシー保護データ収集・解析基盤の構築と個別化医療・ゲノム疫学への展開 [34)]
暗号技術を適用して、ゲノム塩基配列中の塩基の変異（SNP）とその影響を秘匿したままで評価する技術の研究プロジェクト。ゲノムの影響を考慮した個人に特化した治療等への応用を目標としている。筑波大学、東京大学、名古屋工業大学、三重大学、産業技術総合研究所による共同プロジェクト。

（4）科学技術的課題

秘匿計算技術の課題には次のようなものがある。

・計算コスト、通信コストの削減
計算とともに生じる大きな処理時間が最大の問題である。また、1 ビットの情報でも暗号化するとその暗号文の大きさに拡大することとなり、一般的な公開鍵暗号として数千ビットを想定すると、1000 倍近くの容量を消費する。

・秘匿したまま処理を行う要素技術の拡大
従来は加算のみ、乗算のみに限られていた演算をそれらの両方とも実現したり、指数計算などのより複雑な計算へと拡大すること。

・実現するデータマイニングなどの処理の複雑化、多様化

ロジステック回帰の様に逐次的に係数を変化させて、収束を必要とするアルゴリズムなどを効率的に実現する方法の開発。

・高機能暗号の研究開発
関数型暗号や完全準同型性暗号などの高機能暗号の基礎研究は、近年発展の速度が速く、今後も継続した取り組みが必要である。高機能暗号に関連する研究は理論の構築に比して実装技術やライブラリの構築 、現実的なユースケースに即した応用技術が追いついていないため、その整備が必要である。

・秘密計算の研究開発
秘密計算を利用したプライバシーデータの活用については、準同型暗号や Garbled circuit の活用については多くの研究例がすでにあるが、高機能暗号の活用はこれまでにほとんどない。データ解析と暗号理論分野の両方に精通した研究者・技術者が少ないことがその理由の一つであると考えられ、分野間の交流等人材開発が必要である。また「ビッグデータ解析」と「個人データのセキュリティ・プライバシー保護」を個別的な研究開発課題でなく、両者を両輪としたソリューション型の研究開発を進める必要がある。

・差分プライバシーの研究開発
差分プライバシーは理論計算科学分野ではすでにデファクトスタンダードのプライバシーモデルとして定着した感がある。実応用を目指した試みも米国では出始めている。この分野に精通した研究者・技術者は諸外国に比べ日本には極めて少なく、少なくとも研究者レベルではこの分野の専門家の養成が必要であろう。

(5) 政策的課題

我が国の個人情報保護法においては、プライバシー保護レベルとしては最も低い仮名化や匿名化などを想定しており、単純な匿名加工データとするだけで本人同意不要の第三者提供が行われる可能性がある。匿名化は現実的なプライバシー保護技術の一つではあるが、措置の手順や加工の履歴を知る悪意のある攻撃者による内部犯行に対しては十分ではない。一方、安全性の高い PPDM などの暗号化によるプライバシー保護はその存在が知られてはいるが、計算コストや技術が成熟していないことを理由にまだ普及の兆しが見えない。匿名化だけで十分であるという制度が定着すると、暗号化を用いる動機付けが低下してしまい、この技術の普及が一段と遅れてしまうことが懸念される。

個人データ活用におけるプライバシー保護は、法制度との整合性を維持しつつ両技術を適切に組み合わせる複合的なソリューション開発が必要であり、そのための人材育成、組織の構築が必要である。

デバイス・通信技術の発展や、新種のサービスの普及に伴い、プライバシー保護のあるべき姿は急速に変容していくとともに、個人情報活用に対する個人の受容度も変化していく。技術の進歩に柔軟に対応できる法制度の整備も重要な課題である。

(6) キーワード

匿名化、仮名化、*k*-匿名性、*l*-多様性、マルチパーティー計算、Secure Function Evaluation、加法準同型性暗号、水平分割、垂直分割、プライバシー保護データマイニング、プライベートマッチング、差分プライバシー

(7) 国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	○	↗	・暗号理論に関する基礎研究は、企業、大学、国立研究所ともに高いレベルにある。国際的にも競争力があり、優れた成果を挙げている。 ・プライバシー保護技術・システムセキュリティーについての基礎研究は、トップ国際会議等での発表は数が多くなく、国際的に競争力があるとは言えない。
	応用研究・開発	○	→	・ゲノムのプライバシー保護プロジェクト等、応用を意識したプロジェクトが増えてきている。NTT や三菱等は実装を発表している。
米国	基礎研究	◎	↗	・多くの学術論文が発表されている。いずれの研究領域においても、差分プライバシー、完全準同型暗号など多くの理論的アイデアはほとんど米国の大学・企業の研究者から提案されている。
	応用研究・開発	◎	↗	・MIT の CryptDB や SFE の実装等、高い技術力で提案された概念の実装が先行している。 ・高速秘密計算の開発環境 ObliVM, JustGarble などの秘匿回路開発フレームワークが発表されている。
欧州	基礎研究	○	→	・論文レベルではコンスタントに発表が続いている。差分プライバシーや暗号理論の研究も強い。
	応用研究・開発	○	→	・EU のプロジェクトなどで、ユビキタスネットワーク等の多くの分野を統合する動きが見られる。EU データ保護指令などの法整備も先行している。
中国	基礎研究	○	→	・秘匿回路評価の提案者を排出するなど学者を生み出しているが、活躍の場は米国などが主である。
	応用研究・開発	○	↗	・データ工学分野を中心に、複数名のデータプライバシー研究者が活動している。
韓国	基礎研究	○	→	・各種の暗号アルゴリズムの基礎的な研究を行い、国際標準に提案活動を行っている。
	応用研究・開発	△	→	・特に目立った活動は見られない。

（注１） フェーズ
基礎研究フェーズ：大学・国研などでの基礎研究のレベル
応用研究・開発フェーズ：研究・技術開発（プロトタイプの開発含む）のレベル
（注２） 現状　※わが国の現状を基準にした評価ではなく、CRDS の調査・見解による評価である。
◎　特に顕著な活動・成果が見えている、 ○　顕著な活動・成果が見えている
△　顕著な活動・成果が見えていない、 ×　活動・成果がほとんど見えていない
（注３） トレンド
↗：上昇傾向、 →：現状維持、 ↘：下降傾向

(8) 参考文献

1）個人情報保護委員会
http://www.ppc.go.jp/personal/preparation/（閲覧日 2016-12-22）
2）Pierangela Samarati, “Protecting respondents’ identities in microdata release,” IEEE Transactions on Knowledge and Data Engineering, Vol. 13, No. 6, pp. 1010-1027 (2001).

3）Latanya Sweeney, “k-Anonymity: A Model for Protecting Privacy”, International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, Vol. 10, No. 5, pp. 557-570（2002）.
4）Ashwin Machanavajjhala, Daniel Kifer, Johannes Gehrke, and Muthuramakrishnan Venkitasubramaniam, “L-diversity: Privacy beyond k-anonymity”, ACM Transactions on Knowledge Discovery from Data, Vol. 1, No. 1, Article No. 3（2007）.
5）Chao Yao, X. Sean Wang, and Sushil Jajodia, “Checking for k-anonymity violation by views”, In Proceedings of the 31st international conference on Very Large Data Bases（Trondheim, Norway, 2005）, pp. 910-921（VLDB, 2005）.
6）Kristen LeFevre, David J. DeWitt, and Raghu Ramakrishnan, “Incognito: efficient full-domain k-anonymity”, In Proceedings of the 2005 ACM SIGMOD（SIGMOD’05）international conference on Management of data（Baltimore, USA, 2005）, pp. 49-60（ACM, 2005）.
7）Xiaokui Xiao and Yufei Tao, “Anatomy: simple and effective privacy preservation”, In Proceedings of the 32nd international conference on Very large data bases（Seoul, Korea, 2006）, pp. 139-150（VLDB, 2006）.
8）UTD（The University of Texas at Dallas）Data Security and Privacy Lab, “UTD Anonymization Toolbox”
http://cs.utdallas.edu/dspl/toolbox/（閲覧日 2016-12-16）
9）Giorgos Poulis, Spiros Skiadopoulos, Grigorios Loukides, Aris Gkoulalas-Divanis, “Apriori-based algorithms for km-anonymizing trajectory data”, Transactions on Data Privacy Vol. 7, No. 2, pp. 165-194（2014）.
10）Chongjing Sun, Philip S Yu, Xiangnan Kong, and Yan Fu, “Privacy Preserving Social Network Publication Against Mutual Friend Attacks”, Transactions on Data Privacy Vol. 7, No. 2, pp. 71-97（2014）.
11）Andrew C. Yao, “How to generate and exchange secrets”, In Proceedings of the 27th IEEE Symposium on Foundations of Computer Science（Toronto, Canada）, pp. 162–167（IEEE, 1986）.
12）Dahlia Malkhi, Noam Nisan, Benny Pinkas, and Yaron Sella, “Fairplay – a secure two-party computation system”, In Proceedings of the 13th USENIX Security Symposium（San Diego, USA, 2004）, pp. 287–302（USENIX, 2004）.
13）Yan Huang, David Evans, Jonathan Katz, and Lior Malka, “Faster secure two-party computation using garbled circuits”, In Proceedings of the 20th USENIX Security Symposium（San Francisco, USA, 2011）, pp. 35-35（USENIX, 2011）.
14）Benjamin Kreuter, Abhi Shelat, and Chih-Hao Shen, “Billion-gate secure computation with malicious adversaries”, In Proceedings of the 21st USENIX Security Symposium（Bellevue, USA, 2012）, pp. 14-14（USENIX, 2012）.
15）Dan Bogdanov, Sven Laur, and Jan Willemson, “Sharemind: A framework for fast privacy-preserving computations”, In Proceedings of the 13th European

Symposium on Research in Computer Security（Málaga, Spain, 2008）, pp. 192-206（Springer-Verlag, 2008）.
16）Cybernetica, “Sharemind project”
https://sharemind.cyber.ee/（閲覧日 2016-12-16）
17）濱田 浩気 , 五十嵐 大 , 菊池 亮 , 千田 浩司 , 諸橋 玄武 , 冨士 仁 , 高橋 克巳 , “実用的な速度で統計分析が可能な秘密計算システム MEVAL”, コンピュータセキュリティシンポジウム（高松 , 2013）論文集 , pp. 777-784（情報処理学会 , 2013）.
18）Yehuda Lindell and Benny Pinkas, “Privacy Preserving Data Mining”, Advances in Cryptology – CRYPTO 2000: 20th Annual International Cryptology Conference（Santa Barbara, USA, 2000）, Lecture Notes in Computer Science, Vol. 1880, pp. 36-54（Springer-Verlag, 2000）.
19）Rakesh Agrawal and Ramakrishnan Srikant, “Privacy-preserving data mining”, In Proceedings of the 2000 ACM SIGMOD international conference on Management of data（Dallas, USA, 2000）, pp. 439-450（ACM, 2000）.
20）Jaideep Vaidya and Chris Clifton, “Privacy preserving association rule mining in vertically partitioned data”, In Proceedings of the 8th ACM SIGKDD international conference on Knowledge discovery and data mining（Edmonton, Canada, 2002）, pp. 639-644（ACM, 2002）.
21）Charu C. Aggarwal and Philip S. Yu, “A General Survey of Privacy-Preserving Data Mining, Models and Algorithms”, Privacy-Preserving Data Mining, Vol. 34, pp. 11-52（2008）.
22）Bart Goethals, Sven Laur, Helger Lipmaa, Taneli Mielikäinen, “On private scalar product computation for privacy-preserving data mining”, In Proceedings of the 7th Annual International Conference in Information Security and Cryptology（Seoul, Korea, 2004）, pp. 104-120（Springer-Verlag, 2004）.
23）Pascal Paillier, “Public-Key Cryptosystems Based on Composite Degree Residuosity Classes”, Advances in Cryptology – EUROCRYPT 1999: International Conference on the Theory and Application of Cryptographic Techniques（Prague, Czech Republic, 1999）, Lecture Notes in Computer Science, Vol. 1592, pp. 223-238（Springer-Verlag, 1999）.
24）Michael J. Freedman, Kobbi Nissim, and Benny Pinkas, “Efficient Private Matching and Set Intersection”, Advances in Cryptology – EUROCRYPT 2004: International Conference on the Theory and Applications of Cryptographic Techniques（Interlaken, Switzerland, 2004）, Lecture Notes in Computer Science, Vol. 3027, pp. 1-19（Springer-Verlag, 2004）.
25）Jan Camenisch and Gregory M. Zaverucha, “Private intersection of certified sets”, Financial Cryptography and Data Security, Vol. 5628, pp. 108-127（2009）.
26）Hiroaki Kikuchi and Jun Sakuma, “Bloom Filter Bootstrap: Privacy-Preserving Estimation of the Size of an Intersection”, Journal of information processing, Vol. 22, No. 2, pp. 388-400（2014）.

27）Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Guiseppe Persiano, “Public key encryption with keyword search”, Advances in Cryptology – EUROCRYPT 2004: International Conference on the Theory and Applications of Cryptographic Techniques（Interlaken, Switzerland, 2004）, Lecture Notes in Computer Science, Vol. 3027, pp. 506-522（Springer-Verlag, 2004）.
28）Dan Boneh and Brent Waters, “Conjunctive, subset, and range queries on encrypted data”, In Proceedings of the 4th Theory of Cryptography Conference（Amsterdam, The Netherlands, 2007）, Lecture Notes in Computer Science, Vol. 4392, pp. 535-554（Springer-Verlag, 2007）.
29）松田 規 , 伊藤 隆 , 柴田 秀哉 , 服部 充洋 , 平野 貴人 , “検索可能暗号の高速化と Web アプリケーションへの適用方式に関する提案”, マルチメディア、分散、協調とモバイル（DICOMO2013）シンポジウム（十勝川温泉 , 2013）論文集 , pp. 2067-2074（情報処理学会 , 2013）.
30）Cynthia Dwork, “Differential privacy”, In Proceedings of the 33rd international conference on Automata, Languages and Programming（Venice, Italy, 2006）Part II, Lecture Notes in Computer Science, Vol. 4052, pp. 1-12（Springer-Verlag, 2006）.
31）Geographic Privacy-aware Knowledge Discovery and Delivery（GeoPKDD）
http://www.geopkdd.eu/（閲覧日 2016-12-16）
32）MIT Computer Science and Artificial Intelligence Laboratory（CSAIL）Computer Systems Security Group
http://css.csail.mit.edu/cryptdb/（閲覧日 2016-12-16）
33）国立研究開発法人 産業技術総合研究所（AIST）「プライバシー保護データベース検索技術」プロジェクト
https://www.risec.aist.go.jp/project/dbscoop-ja.html
（閲覧日 2016-12-16）
34）国立研究開発法人 科学技術振興機構（JST）戦略的創造研究推進事業 Genome Privacy CREST（プロジェクト統括・佐久間 淳）
http://www.jst.go.jp/kisoken/crest/project/45/45_02.html
（閲覧日 2016-12-16）

3.5.5　セキュリティーアーキテクチャー

（1）研究開発領域の簡潔な説明

セキュリティーアーキテクチャーとは、ソフトウエア製品やシステムの開発において、安全な（セキュリティー上の脆弱性のない）製品、システムを構築するための構造、技法を指す。特に、プログラミング工程における脆弱性修正ではなく、分析、設計工程などの早期段階から安全に構築することが必要とされるため、セキュリティー・バイ・デザイン（セキュア・バイ・デザイン）と呼ばれることもある。

（2）研究開発領域の詳細な説明と国内外の動向

システムやソフトウエアの脆弱性を除去する手法として、従来「セキュア・プログラミング」が主な関心の対象であった。しかし、セキュア・プログラミングの対象は開発工程におけるプログラミング（実装）工程に限定されている。このような、ソフトウエアの欠陥修正を実装段階に置く手法は、ソフトウエアの開発プロセス、特にウォーターフォール型開発では手戻りのコストがかかるということは既に知られていた[1)]。セキュリティー上の欠陥である脆弱性修正においても状況は同じであり、テストや完成後の脆弱性検査において脆弱性が発見されても、修正に多大なコストと期間がかかり、開発プロジェクトの事情によっては修正せずに放置せざるを得ないという事態が頻発するようになった。そこで、他のソフトウエア開発同様、分析工程や設計工程など、開発の早期段階からセキュリティーの問題点を発見し対処するというセキュリティーアーキテクチャー技術研究の必要性を生んだ。また、セキュリティーに近いプライバシー保護研究の分野では、同様の概念が既にプライバシー・バイ・デザイン[2)]として存在していた。そのため、本研究領域はそれに倣い、セキュリティー・バイ・デザインとも呼ばれることになる。

以上の歴史的経緯をふまえ、セキュリティーアーキテクチャーの研究の多くは、既存のソフトウエア工学における問題解決の手法をセキュリティーに拡張するアプローチがとられている。従来のソフトウエア工学的手法と、セキュリティーに適用する場合の大きな相違点は、悪意の想定の有無にある。例えば、分析工程における要求工学は要求の獲得に関する技術であるが、要求の獲得においては、他の要求については利害関係者が開発対象に要求する内容を対象とするのに対し、セキュリティーの要求獲得では、まず第三者または利害関係者による、悪意に基づく要求（脅威）を認識し、その要求により、対象のソフトウエアやシステム、サービス等が被害を受けないように、対策を施す必要がある。このように、まず脅威を認識し、続いてその対策を検討するというプロセスは従来の開発プロセスにはないセキュリティー特有のものである。このようなプロセスのうち、要求獲得段階で行われる技術のことをセキュリティー要求工学と呼び、一般に分析、設計工程で行われるプロセスを脅威分析と呼ぶ。

セキュリティー要求工学技術は、ゴール指向分析や、エージェント指向分析、ユースケース分析など、既存の要求工学の技術をセキュリティーに応用したものが多く提案されている[3)]。一方、脅威分析については、アタックツリー分析[4)]や脅威モデリング[5)]など、セキュリティー分野独自の必要性から発展したものが多い。

(3) 注目動向

近年、サイバー攻撃の対象が ICT システム、機器にとどまらず、ソフトウエアが搭載されている組み込み機器や制御システムなどにも広がりを見せている。現実に、車載システムや航空システム、工場などへのサイバー攻撃手法の公開や、攻撃による被害が発生している[6)-8)]。また、近年さまざまな機器がインターネットに接続することで、さまざまなサービスを提供する Internet of Things（IoT）が急速に発展しているが、IoT システムもまた、構築時にセキュリティーが十分に考慮されていないために脆弱性が存在していることが多く、現実のサイバー攻撃により情報漏えいなどの被害が問題化している。そこで、近年では組み込み、IoT や制御システムを対象としたセキュリティーアーキテクチャーについての研究も活発になってきている。

(4) 科学技術的課題

セキュリティー要求工学、および脅威分析において、必要な技術要素は下記の通りであるが、それぞれの要素において、技術的課題が存在する。

［脅威の識別］

対象のソフトウエア、システムにどのような脅威が存在するかを、開発者が識別できることが重要になる。しかし、現状では、脅威の識別に必要な情報は、脅威モデリングにおける STRIDE 脅威分類などに限定されている。また、アタックツリー分析における下位ノードの識別（ある脅威を可能にする攻撃や条件の識別）についても、十分なセキュリティー知識がないと困難な、属人性の高い作業になってしまっている。知識の欠如を補完するために、Common Attack Pattern Enumeration and Classification（CAPEC）[9)] や Common Vulnerabilities and Exposures（CVE）[10)] など、既知の攻撃や脆弱性がパターン化、データベース化されているが、脅威抽出において十分に活用されていないのが現状である。

また、脅威の識別には、対象となるソフトウエア、システムのモデル化、ないしモデルとしての把握が必要になる。ソフトウエアのふるまいの中で、データがどのように流れるかが明確になることで、そのデータに対する攻撃のポイントが明確になる。しかし、このモデル化は、開発工程が上流にさかのぼるにしたがって、詳細化が困難になる。この課題はセキュリティー要求工学における脅威抽出の障害となる。

［リスク評価］

識別された脅威に対する対策を検討する前に、脅威が引き起こす影響のリスクを評価する必要がある。セキュリティーにおけるリスク評価の方法には議論が存在していたが、近年 ICT 以外の組み込みや制御システムにセキュリティーを適用する際により明確になった。自動車などの製造においては、安全性（機能安全、セーフティ）のリスク分析として Fault Tree Analysis（FTA）[11)] が用いられる。FTA では故障の事象の原因をアタックツリーのように細分化した上で、各基本事象の発生する確率と影響の積によりリスクを求めている。機能安全において扱う事象はこれまで、自然現象やヒューマンエラーなど、蓋然性に基づく確率の予測が容易であった。しかし、サイバー攻撃ではその事象が人為によって操作可能であるため、FTA をセキュリティーに適用する場合、事象のリスク評価の発生確率の算出が問題となる。そこで、セキュリティーにおけるリスク評

価には、確率の変わりに攻撃の発生頻度を用いる手法、攻撃の容易さ、攻撃者のスキルを用いる手法などが提案されている。

［対策の妥当性検証］

対策の妥当性は、最終的にテスト段階で確認する手法と、分析、設計それぞれの工程が終わった段階で確認する手法の二つがある。それぞれの技術的課題について述べる。

・セキュリティーテストの十分性、網羅性の確認

セキュリティーテストについては、第三者による確認が容易である理由からブラックボックステストやその一種であるファジングがよく用いられるが、これらのテストは十分性、網羅性の確保には適していない。十分性や網羅性の確認には、静的コード解析技術が用いられることが多い。

・要求仕様、設計仕様の検証

ソフトウエアの検証をレビューによる確認以外で行う手法としては、形式手法を用いる方法がある。形式手法は定理証明を用いる手法と、モデル検査による手法がある。定理証明を用いる手法は、ソフトウエアの正しさを数学的に証明することができるが、証明には数学的知識を必要とし、かつ自動化が進んでいないため、応用は暗号アルゴリズムやプロトコルの証明にとどまっている。一方、モデル検査はツールによる自動化が進んでいるが、モデルの記述に知識を要するなどの問題があり、一般のソフトウエアへの普及は進んでいないのが現状である。

(5) 政策的課題

セキュリティーアーキテクチャーに関わる標準としては、ISO IEC 15408（コモンクライテリア、CC）[12] がある。CC はソフトウエア製品、システムのセキュリティーを保証する認証制度になっている。しかし、CC の適用は CC 認証を要求されている一部の製品に限定されており、一般の製品やシステムの開発には、追加で必要なドキュメントや工数、費用面の問題から普及が進んでいない。

近年、組み込み、制御システムに対するサイバー攻撃の脅威が高まっていることもあり、機能安全による開発の規格、標準がある業種では、機能安全規格、標準をセキュリティーに拡張することで対応しようとしている。しかし、業種にまたがる共通のセキュリティー構築のための規格、標準はまだ確立していない。また、組み込みや制御システムにおいては、セキュリティーの認識不足、知識不足による安全性の欠如が問題視されており、2020 年の東京オリンピック、パラリンピックを控え、特に重要インフラ分野におけるセキュリティー人材育成の必要性が指摘されている。

(6) キーワード

セキュリティー・バイ・デザイン、セキュリティー要求工学、脅威分析、リスク評価、形式手法、機能安全、セーフティ、IoT、組み込み

(7) 国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	○	→	要求工学分野において、ゴール指向を中心に研究がされてきた。
	応用研究・開発	△	↗	また十分ではないが、IoT など具体的な応用分野を中心に活発化しつつある [13]。
米国	基礎研究	◎	→	CMU（Carnegie Mellon University）、FAU（Florida Atlantic University）を中心にあらゆる領域において先行している。
	応用研究・開発	◎	→	ツールやサービス提供、業界ごとの規格やガイドラインなどの開発が活発である。
欧州	基礎研究	◎	→	各種要求工学手法の応用や、プライバシーを含めた研究が各国で活発である。
	応用研究・開発	◎	↗	近年では Industrie 4.0[14] での CPS へのセキュリティーの組み込みも進む。
中国	基礎研究	○	→	要求工学をセキュリティーに応用する研究など、いくつかの事例が見られる。
	応用研究・開発	○	↗	IoT、ビッグデータなど特定の分野における応用研究が見られる。
韓国	基礎研究	×	→	国際会議等で顕著な研究成果が見られない。
	応用研究・開発	×	→	上に同じ。

（注１） フェーズ
基礎研究フェーズ：大学・国研などでの基礎研究のレベル
応用研究・開発フェーズ：研究・技術開発（プロトタイプの開発含む）のレベル
（注２） 現状 ※わが国の現状を基準にした評価ではなく、CRDS の調査・見解による評価である。
◎ 特に顕著な活動・成果が見えている、 ○ 顕著な活動・成果が見えている
△ 顕著な活動・成果が見えていない、 × 活動・成果がほとんど見えていない
（注３） トレンド
↗：上昇傾向、 →：現状維持、 ↘：下降傾向

(8) 参考文献

1) Richard H. Thayer（Editor）, Merlin Dorfman（Editor）, Software Requirements Engineering, 2nd Edition,（Wiley-IEEE, 2000）.
2) Peter Hustinx, “Privacy by design: delivering the promises”, Identity in the Information Society, Vol. 3, No. 2, pp 253–255（2010）.
3) 吉岡 信和 , 田口 研治 , “セキュリティ要求工学の実効性”, 情報処理 Vol. 50, No. 3, pp. 185-186（2009）.
4) Bruce Schneier and Adam Shostack, “ Breaking Up Is Hard to Do: Modeling Security Threats for Smart Cards”, In Proceedings of the 1st USENIX Workshop on Smart Card Technology（Chicago, USA, 1999）, pp. 175–185（USENIX, 1999）.
https://www.schneier.com/academic/paperfiles/paper-smart-card-threats.pdf（閲覧日 2016-12-15）
5) Adam Shostack, Threat modeling: designing for security（Wiley, 2014）.
6) Forbes, “Digital Carjackers Show Off New Attacks”（2013/07/24 公開 Youtube 動画）
https://youtu.be/oqe6S6m73Zw（閲覧日 2016-12-15）
7) Charlie Miller and Chris Valasek, “Remote Exploitation of an Unaltered Passenger Vehicle（August, 2015）”

http://illmatics.com/Remote%20Car%20Hacking.pdf
（閲覧日 2016-12-15）
8）Reuters, “Polish airline, hit by cyber attack, says all carriers are at risk”, （2015/06/22 公開 technology news 動画）
http://www.reuters.com/article/us-poland-lot-cybercrime-idUSKBN0P21DC20150622（閲覧日 2016-12-15）
9）Sean Barnum, “Common Attack Pattern Enumeration and Classification”, https://capec.mitre.org/documents/documentation/CAPEC_Schema_Description_v1.3.pdf（閲覧日 2016-12-15）
10）Mitre, “Common Vulnerabilities and Exposures（CVE）”, https://cve.mitre.org/（閲覧日 2016-12-15）
11）International Electrotechnical Commission（IEC）, “Fault Tree Analysis Edition 2.0”, (IEC, 2006).
12）独立行政法人 情報処理推進機構（IPA）, “ISO/IEC 15408: valuation criteria for IT security, ver.3.1 release 4”, https://www.ipa.go.jp/security/jisec/cc/prevcc.html（閲覧日 2016-12-15）
13）独立行政法人 情報処理推進機構（IPA）, “つながる世界の開発指針～安全安心な IoT の実現に向けて開発者に認識してほしい重要ポイント～”, http://www.ipa.go.jp/files/000051411.pdf（閲覧日 2016-12-15）
14）Bill Lydon, “Industry 4.0 - Only One-Tenth of Germany’s High-Tech Strategy（Automation.com2014/04/04 記事）”, http://www.automation.com/automation-news/article/industry-40-only-one-tenth-of-germanys-high-tech-strategy（閲覧日 2016-12-15）

3.5.6　運用・監視技術

（1）研究開発領域の簡単な説明

サイバー攻撃に備えた各種セキュリティー装置やネットワークの運用･監視技術の確立。

（2）研究開発領域の詳細な説明と国内外の動向

サイバー攻撃に用いられる手法は日々進化を続けており、通常のサイバー攻撃であっても、攻撃の検知や攻撃による被害発生を未然に阻止することは難しくなりつつある。2016 年も、JTB、日本経済団体連合会など、十分なサイバー攻撃対策を施していると思われる組織でさえも、サイバー攻撃による侵入や重要な情報の流出を阻止することができなかった [1)-3)]。

このような被害発生を前提とした対策手法として、情報処理推進機構は 2014 年に『高度標的型攻撃』対策に向けたシステム設計ガイド [4)] を公開している。本ガイドでは、マルウエア感染などの初期潜入は防ぎきれないことを前提に、その後に発生する組織内ネットワークでの盗聴やバックドア開設（基盤構築）や端末間での感染拡大やサーバーへの侵入（内部侵入・調査）を発見し封じ込めることを求めている。同様の考え方は米国 National Institute of Standards and Technology（NIST）が公開した Computer Security Incident Handling Guide[5)] でも採用されている。

また、マルウエア Mirai が公開された結果、工場出荷時のままなど脆弱なパスワードを設定された IoT 機器による 10 万台規模のボットネット（botnet: 悪意のあるプログラムにより乗っ取られた多数のゾンビコンピュータで構成されるネットワーク）が構築され、1Tbps を超える DDoS 攻撃が発生するようになっている [6)]。このほか、フィンランドにおいては、DoS 攻撃によりマンションの暖房が停止するというサイバー攻撃も観測されている [7)]。

McAfee Labs の予測 [8)] によれば、2015 年時点で、タブレット機器、ウエアラブル機器、IoT 機器の台数は、それぞれ 2.48 億台、2 億台、150 億台と推定されている。現時点ですら、IoT 機器はその他機器と比べ台数が桁違いに多い。今後、タブレット機器は 2019 年までに 2.69 億台、ウエアラブル機器は 2018 年までに 7.8 億台に増加すると予想されている一方、IoT 機器は 2020 年までに 200 億台に増加するとされており、IoT 機器のセキュリティー対策は重要な課題となりつつある。

また、世界的な IPv4 アドレス枯渇と IP アドレスの使用機器の爆発的な増加を受けて、IPv6 アドレスの利用が加速される兆候がある。Linux 系、BSD 系、Windows 系といった主要 OS は既に IPv6 に対応している。さらに、Apple 社は、2016 年 6 月 1 日以降に同社 App ストアに提出される iOS 用アプリケーションでは、IPv6 のみのネットワークに対応すること必須化すると発表した [9)]。このよう流れを受けて、今後、多くの OS やアプリケーションは IPv6 に対応するようになることになると推定される。

しかし、これは、従来とは桁違いな多くの情報機器が IPv6 によってインターネットに直結される可能性、一つの組織に数億台の情報機器が存在する可能性があることを意味している。このような背景を受けて、国内外で、新たな考え方によるセキュリティー対策やネットワーク運用の手法が開発され始めている。

［サイバー攻撃検知技術］

前述の通り、初期感染による被害発生を前提としたサイバー攻撃対策が必須となった。これは、一般的な対策であるインターネットとの接続点におけるセキュリティー対策（入口・出口対策）に加え、組織内のネットワークでのセキュリティー対策（内部対策）が必要になることを意味する。

一般に、対外接続回線の回線速度（帯域幅）に比べ、組織内 LAN の総回線速度は数桁大きく、100Gbps を超えることも珍しくない。Intrusion Detection System などのセキュリティー製品の価格は監視対象の回線速度に比例するため、入口・出口対策と同様に全ての通信を漏れなく監視することはコスト面から非現実的になる。このため、組織内ネットワークの状況を俯瞰し、異変を察知した場合にその発生箇所を集中的に精査してサイバー攻撃の有無を確認し、必要に応じた対策を講じるという手法の確立が必要となる。

［被害緩和技術］

初期感染、基盤構築、内部侵入・調査の各段階では、組織内の情報機器でマルウエア感染などの被害が既に発生している。この状況の悪化を回避するためには、被害が発生している機器への対処が求められる。従来は、マルウエア感染機器を隔離（ネットワークからの切離）し、マルウエアの駆除や駆除ができない場合のクリーンインストールを施して安全性を確認したのちに再接続する手順が一般的であった。

しかし、情報技術の応用範囲が広がるにつれ、単体で稼働する情報機器というものはほぼ存在しない状況となっている。また、情報機器をプラント制御などに活用している場合、制御対象であるプラントが停止する前に情報機器を隔離することは極めて危険な行為であると言える。さらに、海外においては、マルウエアの駆除活動を攻撃側が察知すると、発見されていない感染機器を用いて、データの消去など破壊活動に転じる事例も確認されている。

標的型サイバー攻撃などでは、対処しても執拗に侵入を繰り返すだけでなく、対処を繰り返すことで攻撃側が防御側の体制を学習しステルス化することも懸念される。攻撃の存在を確認できる状況であれば、観測により攻撃側の目的などを推定する方が望ましいこともある。つまり、感染を継続させることによるリスクを軽減させる技術、あるいは、感染機器を攻撃者に察知されることなく監視下に置く手法の確立が必要となる。

［ネットワーク構成技術］

前述の俯瞰監視 / 集中監視、および、被害緩和を実現するためには、サイバー攻撃の状況に応じて監視対象のネットワーク構成を動的に変更する技術が必要となる。例えば、サイバー攻撃による被害を受けているネットワークセグメントを隔離する、制限付きで組織ネットワークへの接続を継続する、集中監視用のセキュリティー装置に当該セグメントの通信を転送するなどが考えられる。また、攻撃側の目的（狙っている情報など）が推定できた場合、その情報が存在するサーバーやネットワークセグメントを隔離する、アクセス制限を強化するなどの保護策を講じることも考えられる。これにより、業務を継続しつつ、かつ、サイバー攻撃に対処するレジリエントなネットワークが実現される。

例えば、Software Defined Networking（SDN）を応用し、攻撃の通信のみをハニーポッ

トなどのおとりシステムに誘導し、攻撃側の活動を監視する手法は製品化が進みつつある。さらに、最近は仮想化技術の活用が広がっており、情報の持ち出しができないように細工を施した本物のシステムの仮想イメージをおとりシステムとして活用するという手法も採用可能になりつつある。

［脆弱性自己検証および対策技術］

ソフトウエアに対する検証やサイバー攻撃の観測によりソフトウエアの脆弱性を発見し、この脆弱性を狙った攻撃を無害化する対策を生成する技術である。

例えば、脆弱性の発見手法としては、検証手法の一種であるファジング（fuzz testing）を用いてソフトウエアに例外処理を発生させ、脆弱性が存在する箇所を特定する。サイバー攻撃により被害が発生した際の攻撃プログラムや攻撃セッションを解析し、攻撃側が狙っている脆弱性、あるいは、攻撃セッション中の shellcode や exploit code といった情報を特定する。

無害化の手法としては、Intrusion Prevention System（IPS）に当該脆弱性を狙った攻撃を検知する暫定パターン（signature）を生成し、セッションを観測した時点で通信を遮断する。脆弱性が発生する機械コードを変更する暫定パッチを作成するというものがある。

現在、これらの一連の処理に加え、暫定 signature や暫定パッチ適用による副作用の有無の検証までを全て自動化する技術の研究開発が進みつつある。

［被害機器特定技術］

現代のサイバー空間の利用では、モバイル機器の存在が大きくなってきている点に特徴がある。IoT 機器の普及に伴い、その傾向はさらに加速されることは自明と言える。サイバー攻撃によって被害を受けたモバイル機器は、その状態を抱えたまま現実世界を移動することなる。当然、当該機器は、現実世界の位置などに応じてサイバー空間も移動することになる。また、車車間通信のように、時間や場所といった環境に応じて機器同士がアドホックネットワークを構成する利用も増えると想定される。

このような状況下でのサイバー攻撃対策を講じるためには、当該機器の地理上の位置に加えサイバー空間上での位置（IP アドレスや接続ネットワーク等）を短時間で特定する技術が必要になる。特にアドホックネットワークの場合、従来のように固定されたポイントを通過する通信を監視する集約型監視が行いにくく、ネットワーク構成の変更に追従する動的な監視の仕組みが必要となる。

ただし、既にさまざまな機器がサイバー空間に存在する現在、これらを新たな機器に置き換えることは非現実的であるため、ネットワーク監視などにより、不審な挙動を示す機器を発見する技術の研究開発が必須となる。

［セキュリティー情報イベント管理（Security Information Event Management: SIEM）］

各種セキュリティー機器が発する警報やサーバー等のログ情報の相関分析により、単体の機器の警報では見つけられないサイバー攻撃や同時多発するサイバー攻撃の中から危険度や緊急度の高いものを抽出し、セキュリティー技術者に提示する技術である。

ただし、多くの場合、相関分析のルールの定義、パラメータの調整は観測対象のネットワークごとに行う必要があり、そのためにセキュリティー技術者に求められる背景知識も幅広いものが求められる。

現在、これら設定等の処理を自動的に行う技術の研究がなされている。

(3) 注目動向

国内においては、総合科学技術・イノベーション会議による戦略的イノベーション創造プログラム（SIP）において、「重要インフラ等におけるサイバーセキュリティの確保」に関する研究開発が進行中であり、研究費は 2015 年度 5 億円、2016 年度 25.5 億円となっている [10)]。また、文部科学省が実施する国立大学法人等における情報セキュリティー体制の基盤構築において、俯瞰 / 集中型監視技術や当該技術を活用する人材育成の研究開発が進行中であり、実施費用は 2016 年度 7.8 億円となっている [11)]。

一方、米国においては、国防高等研究計画局（DARPA　Defense Advanced Research Projects Agency）による脆弱対策技術を完全自動化した CTF 大会 DARPA Cyber Grand Challenge が 2015 年から 2016 年にかけて実施され、総予算は 5500 万ドル（約 56 億円）であった [12)]。なお、このチャレンジで用いられたプログラムは全て無償公開されており、その成果を活用したと思われるセキュリティー製品のコンセプト発表が始まっている。

また、被害機器特定技術については、MITER による 5 万ドル（約 5 百万円）の賞金をかけたチャレンジ [13)] が 2016 年 11 月現在開催中である。このほか、2012 年より NIST がメリーランド大学に National Cybersecurity Center of Excellence を設置し、組織のセキュリティー向上のための監視手法の開発を開始している。

そのほか、韓国や台湾においては、研究機関や学校（台湾の場合は幼稚園から大学まで）のセキュリティー監視を一括して行う Security Operation Center（SOC）が運用を開始しており、膨大な情報を俯瞰的に処理する手法の研究開発が進みつつある。

(4) 科学技術的課題

サイバー攻撃の手口が高度化するにつれ、その検知および対策技術も高度化が求められており、そのためには IDS/IPS（侵入検知・防御システム :Intrusion Detection System/ Intrusion Prevention System）を始めとする各種セキュリティー機器の高性能化が必須要件となる。IDS/IPS を例とすれば、以前は 1 パケットごとに解析処理すれば良かったが、現在はセッション全体を解析、さらには、複数のセッションの相関性、SIEM（Security Information Event Management）の場合は複数のログ間の相関性まで解析する必要が生じている。

しかし、ネットワーク技術の進歩はいまだ著しく、5 年ほど前であれば、高性能なものでも大規模組織で 10Gbps、一般家庭も 100Mbps、モバイル機器単体で 10Mbps 程度だったものが、それぞれ、100Gbps、1Gbps、200Mbps を超える時代となり、10 倍以上の伸びとなっている。これに対し、CPU やメモリ量の増加は頭打ち状態から数倍程度となっている。

セキュリティー機器の高度化のためにはこれらハードウエア資源の高性能化、および、限られた資源を効果的に活用する手法の開発が求められている。

(5) 政策的課題

他国と比較した場合の相違点として、米国との比較であれば、これまでも指摘されている通り予算規模の違いが挙げられる。さらに、米国においては、さまざまな技術開発に幅広く投資し、その中の一部が実を結べば良いと考えており、集中投資によるリスク発生を回避している。前述の DARPA Cyber Grand Challenge を例とすれば、決勝に進んだチームはサイバーセキュリティーを専門とする者だけで構成されておらず、ソフトウエア工学、形式言語理論、機械学習理論、知識ベース技術などさまざまな研究分野の人材が参加していた。わが国では、これらの研究分野は急速に人材が減少している状況にあるのと対照的である。

また、決勝に進んだチームを監督する教員、DARPA（国防高等研究計画局）関係者らとの情報交換から、人工知能によるサイバー攻撃防御の完全自動化は遠い未来に実現すべき究極の目標ではあるが、今後 10 年程度の人工知能研究分野およびハードウエアなどの周辺技術の進歩を鑑みると、サイバーセキュリティー技術者の補佐役の実現を当面の目標と考えているようであった。この考え方は、韓国の学術研究機関のセキュリティー監視を行っている Korea Institute of Science and Technology Information のセキュリティー監視チームとの合同ミーティングでも同様であった。

国家予算が厳しいわが国ではあるが、人工知能学会などが人工知能に対する過度の期待に警鐘を鳴らし始めているように、極度の一極集中とならない政策が必要になっていると考える。

また、他国と比べ、わが国においてサイバーセキュリティー研究を行う際に壁となるのが、通信の秘密の扱いである。前述のように諸外国では、一定の条件下でセキュリティー監視センターによる通信解析を認めているが、わが国では、憲法、有線電気通信法などにより通信解析自体が違法であるとされている。この問題は、極めてセンシティブなものであり、拙速な解決は望ましくないが、何らかの対応が求められている。

(6) キーワード

サイバーセキュリティー、サイバー攻撃対策、標的型サイバー攻撃、レジリエントネットワーク、セキュリティー情報イベント管理（Security Information Event Management）

(7) 国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	△	→	監視運用に携わる研究者が極めて少ないが、大学情報センター系の教員などを中心に基礎研究は行われている。ただし、自校の通信であっても実データを研究に利用できる大学は少ないのが現状である。
	応用研究・開発	△	→	製品化では実データによる検証および機能強化が必須であるが、実データの入手が極めて困難であることもあり、外国製品との差を埋めることに苦労している。このため、アンチウイルスソフトなどを除けば、監視運用の製品化まで至った例はごく少数に止まっている。
米国	基礎研究	○	↗	DoD（DARPA）、DHS、NSF などにより潤沢な研究資金が幅広く投資されており、かつ、研究に必要な実データの入手も一定条件のもとで可能となっている。
	応用研究・開発	○	↗	大学で生まれたアイデアを元に起業化する流れがうまく循環している。ただし、すべての起業化が成功しているわけではなく、実際にはごくわずかである。 また、実データを活用した製品の性能検証や高機能化が有効に働いている。極端な事例として、実際に Botnet を乗っ取って運用してみた実事例を論文で発表するなど、わが国を含めた諸国では違法性が問われる活動まで容認されている。
欧州	基礎研究	○	↗	サイバーセキュリティー全般として基礎研究は活発であり、国際会議での発表も数多くなされている。
	応用研究・開発	△	→	欧州も個人情報保護や通信の秘密の制限が厳しくかけられているため、実用化段階の検証が行いにくいのが現状である。5 年ほど前であるが、フランス Eurecom の研究者が大挙して渡米し、米国のセキュリティー企業や大学に転職するという事態も発生している。
中国	基礎研究	−	−	監視運用に関する情報はほとんど公開されていないため評価が難しい。
	応用研究・開発	−	−	Golden Firewall（金盾）と言われる通信監視が極めて効果的に機能していることから、かなりのレベルの技術開発が行われていることは推定できるが、監視運用に関する情報はほとんど公開されていない。
韓国	基礎研究	○	↗	北朝鮮が関与したとされるサイバー攻撃を受け重要情報が流出するなどの被害が年に数回の頻度で発生しているため、監視運用に必要な基礎技術の開発は比較的活発である。
	応用研究・開発	△	→	基礎技術の製品化は、政府機関等での採用必須化などもあり、アンチウイルスソフトや IDS など一定の分野で進んでいる。ただし、米国やイスラエル製品と競合する分野では、厳しい競争にさらされ、製品化が難しいのが現状である。
イスラエル	基礎研究	○	↗	サイバーセキュリティーに直結しないものであっても、国防に関連する可能性がある基礎理論分野については、大学や研究機関において活発に研究されている。
	応用研究・開発	△	→	国家による支援制度もあり、数多くのベンチャー企業が立ち上がっている。また、大学等の研究機関との連携も国家が後押しする体制が整っている。ただし、製品化に関するノウハウが十分にないこともあり、他国企業と共同で製品化する事例も多い。また、米国製品と競合することが多いのも実情である。

（注１） フェーズ
基礎研究フェーズ：大学・国研などでの基礎研究のレベル
応用研究・開発フェーズ：研究・技術開発（プロトタイプの開発含む）のレベル
（注２） 現状 ※わが国の現状を基準にした評価ではなく、CRDS の調査・見解による評価である。
◎ 特に顕著な活動・成果が見えている、 ○ 顕著な活動・成果が見えている
△ 顕著な活動・成果が見えていない、 × 活動・成果がほとんど見えていない
（注３） トレンド
↗：上昇傾向、 →：現状維持、 ↘：下降傾向

(8) 参考文献

1）Piyokango, “JTB への不正アクセスについてまとめてみた”, http://d.hatena.ne.jp/Kango/20160614/1465925330（閲覧日 2016-12-15）
2）Piyokango, “経団連事務局端末の不審な通信発生についてまとめてみた”, http://d.hatena.ne.jp/Kango/20161110/1478795281（閲覧日 2016-12-15）

3）Piyokango, “2016 年 6 月に複数の組織で確認されたマルウエア感染インシデントについてまとめてみた”,
http://d.hatena.ne.jp/Kango/20160626/1466954474（閲覧日 2016-12-15）
4）独立行政法人 情報処理推進機構（IPA), “『高度標的型攻撃』対策に向けたシステム設計ガイド」の公開”,
https://www.ipa.go.jp/security/vuln/newattack.html（閲覧日 2016-12-15）
5）National Institute of Standards and Technology（NIST), “Computer Security Incident Handling Guide”,
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
（閲覧日 2016-12-15）
6）西脇 春名 ,“大規模 DDoS 攻撃を引き起こした IoT ボットネット :「Mirai」ソースコード徹底解剖 - その仕組みと対策を探る”,
http://www.atmarkit.co.jp/ait/articles/1611/08/news028.html
（閲覧日 2016-12-15）
7）Piyokango, “フィンランドで発生した DoS 攻撃の影響による家庭用管理システムの障害についてまとめてみた”,
http://d.hatena.ne.jp/Kango/20161126/1480177786（閲覧日 2016-12-15）
8）McAfee Labs, “2016 年の脅威予測”,
http://www.mcafee.com/jp/resources/reports/rp-threats-predictions-2016.pdf
（閲覧日 2016-12-15）
9）Apple, “Supporting IPv6-only Networks”,
https://developer.apple.com/news/?id=05042016a（閲覧日 2016-12-15）
10）内閣サイバーセキュリティセンター（NISC), “サイバーセキュリティの概要”,
http://www.nisc.go.jp/conference/cs/kenkyu/dai05/pdf/05shiryou0304.pdf
（閲覧日 2016-12-15）
11）内閣サイバーセキュリティセンター（NISC), 政府のサイバーセキュリティに関する予算 ,
http://www.nisc.go.jp/conference/cs/dai06/pdf/06shiryou05.pdf
（閲覧日 2016-12-15）
12）Defense Advanced Research Projects Agency（DARPA), “DARPA Cyber Grand Challenge”,
https://cgc.darpa.mil/（閲覧日 2016-12-15）
13）Miter, “MITER Challenge IoT”,
https://www.mitre.org/research/mitre-challenge/mitre-challenge-iot
（閲覧日 2016-12-15）

3.5.7　IT システムのためのリスクマネジメント

（1）研究開発領域の簡潔な説明

重要性をます IT システムの安全を確保するためのリスクマネジメント（リスクアセスメント、リスクコミュニケーションを含む）技術の高度化を行う。

（2）研究開発領域の詳細な説明と国内外の動向

［背景と意義］

現代社会は、IT システムに深く依存するようになってきており、IT システムの安全性の確保は非常に重要な課題になってきている。そのような中で、高度化、複雑化する標的型メール攻撃やランサムウエア、さらには内部犯罪のための対策を適切に実施するためには、ハードウエアやソフトウエアの導入などの個別の技術的対策だけでは不十分で、リスクアセスメント、リスクコミュニケーションを含むリスクマネジメントのための理論から実務までの体系化やそのための技術の高度化が不可欠となってきている。

特に、最近では、次のような対応が必要となっている。

（a） 新しい状況に適応したリスクマネジメントのためのフレームワークの確立と、それに伴い必要となる技術の確立。

重要インフラや IoT もサイバー攻撃の対象となりつつあり、攻撃により重要インフラや IoT が誤動作した場合やそのサービスが失われた時の脅威は非常に大きな問題となることが予想されることからこれらを含めた新しいフレームワークが必要となる。

（b） リスクマネジメントの基礎となるリスク分析やリスク評価を含むリスクアセスメント技術の高度化。

攻撃手段が高度化・複雑化しており、従来のフォルトツリーやアタックツリーのようなリスク分析法では、適切なリスク分析が行えず、適正な現状のリスクやリスク対策効果の把握が困難になっている。また、リスクの時間推移に伴う動的変化への対応も必要となる。さらに、ここでは、リスク対策が必要かどうかだけでなく、どのような対策の組み合わせが望ましいのかの検討も可能とする必要がある。

（c） リスクに関与する人たち（例えば経営者、従業員、顧客など）がいろいろいる中で、提案された対策案やその組み合わせを実行するに当たってのリスクコミュニケーションに基づく関与者間の合意形成。

損害額・対策費用の増大等の問題が生じており、セキュリティー担当者の判断だけで対策を決定するのは困難になってきている。このため、経営者との間の適切なリスクコミュニケーションが大切になっている。経営者とのリスクコミュニケーションは時間がかかりすぎないようにするとか技術的な知識が十分でなくとも判断しやすくする等の難しい条件が要求される。

［これまでの取り組み］

（a） リスクマネジメントのためのフレームワークの確立と、それに伴い必要となる技術の確立：

IT 分野では、2000 年に情報セキュリティーマネジメントが標準化の対象となってい

る（ISO/IEC27001）[1]。しかし、この段階で情報セキュリティーのリスクマネジメントで扱う対象は、下記の三つの階層のうち第 2 階層が中心で、情報資産をマネジメントの対象としてあつかってきてきた。

第 1 階層　IT システムそのものの安全
第 2 階層　IT システムが扱う情報の安全
第 3 階層　IT システムが行うサービスの安全

そして、第 1 階層の IT システムそのものの安全性のうちハードウエアの安全性はほとんど扱われてこなかった。またネットショッピングの安全などの第 3 階層の IT システムが行うサービスの安全問題もほとんど対象外であった。さらに、この段階では、関与者間のリスクコミュニケーションの問題も明示的には扱われてこなかった。

2009 年になると一般化されたリスクやリスクマネジメントの定義が標準化された（ISO 31000）[2]。ここでは、図 3-5-2 に示すようなリスクマネジメントプロセスが提案され、リスクマネジメントの中に、リスクアセスメントだけでなく、リスクコミュニケーションが位置づくようになった。このような中で、重要インフラや IoT を含めてリスクマネジメントのためのフレームワークという動きがみられるようになってきた。企業全体のリスクの中に情報システムのリスクをどう位置づけるかなどの検討のため情報セキュリティーのリスクを経済学的に扱う試みが 21 世紀になって行われ始めた[3]。セキュリティー経済学については、ENISA で 2011 年より、WG が作成され、必要なアプローチ方法に関する分析結果が 2012 年に報告されている[4]。

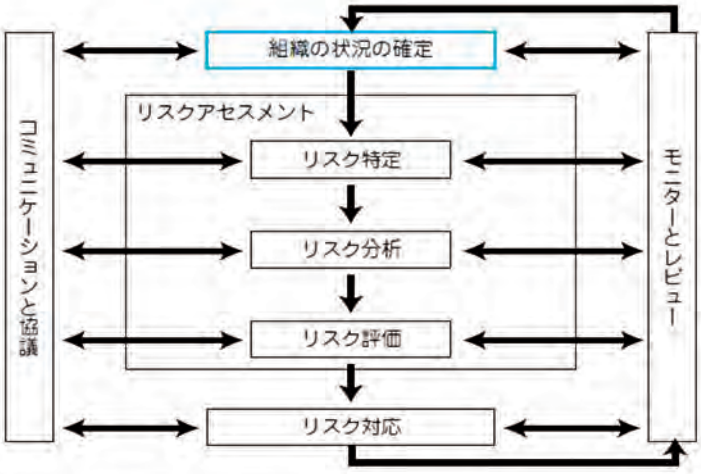

図 3-5-2　リスクマネジメントのプロセスの流れ

(b)　リスクマネジメントの基礎となるリスクアセスメント技術の高度化。

リスクマネジメントの中心となるリスクアセスメントは、次の二つのフェーズに分けて考えることができる。

（1）　対策を必要とするリスクの明確化
（2）　そこで必要となる対策の検討とそのプライオリティ付け

（1）のために実施されるのがリスク分析である。従来は定性的分析や準定量的分析法が中心であったが定量的分析の試みも行われてきた。例えば、Bruce Schneier がセキュリティー評価に適するようにフォルトツリー分析法を改良したアタックツリー分析

法[5] の適用なども行われている（例えば、文献 6)）。また、高度化･複雑化するサイバー攻撃の対策のリストアップと対策効果の推定を容易にするために、侵入後の種々のシーケンスの記述が可能なイベントツリー分析法と各シーケンスの分岐時点における対策効果の記述が容易なディフェンスツリー分析法を組み合わせる方式も提案されている[7]。

このようなモデル化を行ううえで脅威分析の方法に関する研究が進み始めている[8]。重要インフラや IoT を対象にすることにより、機密性の喪失だけでなく、完全性や可用性の喪失が重要になり、制御対象を含めたリスク評価が重要になってきているからだと考えることができる。このため、セキュリティーとセイフティーを統一的に扱おうとする試みが行われている[9]。

(c) リスクに関与する人たちがいろいろいる中で、提案された対策案やその組み合わせを実行するに当たってのリスクコミュニケーションに基づく関与者間の合意形成

IT システムに関するリスクコミュニケーションの研究は、国内外でほとんど行われてこなかった。佐々木良一らは、IT システムのリスクコミュニケーションの目的を①個人的選択、②組織内合意形成、③社会的合意形成の 3 つに分けられることを示すとともに、組織内合意のために多重リスクコミュニケータ MRC の開発を行った[10]。これは、リスク間の対立や、関与者間の意見の相違を考慮しつつ、リスクコミュニケーションにより対策案の最適な組み合わせを求められるようにするものである。MRC については種々の発展が図られている。しかし、IT システムのリスクコミュニケーションの検討はまだまだ不十分であり、今後研究の加速が期待される。

［今後必要となる取り組み］

(a) 重要インフラや IoT なども含めたリスクマネジメントのためのより広いフレームワークの確立

サイバー攻撃の激化や、いろいろなものがインターネットに接続されたことから、既に述べたように、リスクマネジメントの新しいフレームワークの検討が少しずつではあるが進みつつある。このような検討は「産」だけでも「学」だけでも不可能で産官学が協力した推進が必要となる。

(b) リスクアセスメント技術の適用範囲の拡大と適用容易化

今後、クラウドのリスクアセスメント、サプライチェインのリスクアセスメント、制御システムのリスクアセスメント、内部犯罪のリスクアセスメントなどが重要になると考えられているが、その研究はまだまだ不十分である。脅威分析の深化や、セキュリティー分析と安全分析の関連付けと統一的扱いも重要な課題となる。

また、リスクの本質である、一つのリスク対策が新たなリスクを生み出す問題や、リスク対策により、攻撃側が動的に変化する問題などを考慮した新しいリスクアセスメント技術の開発が期待される。

さらに、対策案の組み合わせを求めるためのリスクアセスメント技術については、大規模なシステムに適用できるようにするとともに、多くの人が適用できるようにしていく必要があると考えており、さらなる改良が期待されている。

また、重要インフラや IoT を対象にすると、セキュリティー分析だけでなく安全分

析も必要になってきており、これらをどのように組み合わすべきかということも課題となってきている。

(c) IT システムのためのリスクコミュニケーションに関する研究の深化

IT システムの適用に関する社会的合意形成（例えば、青少年のための情報フィルタリング）のためのリスクコミュニケーション技術が重要になっていくと考えられる。また、組織内合意形成においても多くの人が容易に適用できるようにする方向での改良が期待されている。特に、今後はリスクコミュニケーションに経営者の参加が不可欠となるが、経営者はリスクコミュニケーションに多くの時間をかけるわけにいかず、技術的理解も限界がある中で適切な合意形成をできるようにしていく必要がある。

さらに、合意形成を可能にする要因等の分析等の理論化を通じた、リスクコミュニケーション手段の高度化なども重要なテーマになっていくと考えられる。

(3) 注目動向

リスクマネジメントのためのフレームワークの確立と、それに伴い必要となる技術の確立については、2008 年ごろより佐々木良一らが「IT リスク学」[11] の名のもとに IT リスクを広くとらえたうえで、学の確立を図ってきている。

2014 年 2 月には米国の NIST(国立標準技術研究所)が「重要インフラのサイバーセキュリティーを向上させるためのフレームワーク」を策定し、リスクに関する目標と現実のギャップを特定・分析し、優先順位付けを行う方法を提案した[12]。経営層とのリスクコミュニケーションの方法についても考慮しているのが大きな特徴であり、注目に値する。

また、Jack Freund と Jack Jones は 2015 年に “Measuring and Managing Information Risk: A FAIR Approach”[13] という本を出版し、Information Risk のフレームワークの見直しと Information Risk の測定法や管理法の検討を試みている。FAIR というのは Factor analysis of information risk の略である。ここでは、定量的リスク分析を積極的に扱い発生確率の不確実性を考慮し、モンテカルロ法を用いてリスクの分布を求めるような方法も提案されている。FAIR Institute という非営利組織も設立され、FAIR に基づくリスクマネジメントの普及活動を行っているようである。

リスクマネジメントの基礎となるリスクアセスメント技術の高度化については、2012 年には、米国の NIST（National Institute of Standards and Technology）より SP800-30 Rev.1（リスクアセスメントの実施の手引き）[14] が出版され、リスクアセスメントのための具体的手順が示された。しかし、一般的な方法であり、目的や対象によっていろいろな手法が必要とされるが、これらに関する研究は限定的である。

必要となる対策の検討とそのプライオリティ付けは図 3-5-2 におけるリスクの評価に対応し、どのような対策をとるべきかを明確にするため、Stefano Bistarelli らは , アタックツリーに脆弱性への対策を適用したディフェンスツリーを定義し , 対策のリスク低減率と運用コストを考慮した ROI（Return On Investment）と , 攻撃者が再攻撃を仕掛ける割合を考慮した ROA（Return on Assets）を用いた最適な対策選定手法を提案している[15]。

また、事故シーケンスの発生確率を下げる対策と、損害の大きさを低減する対策を組み合わせて最適な対策案の組み合わせを求める方式の研究も増えてきている。2016 年には

“Risk Analysis and Security Countermeasure” という本[16)]が出版され定量的評価に基づく対策案の選定を行う方法も提案された。最近、このような定量的分析に基づく対策の検討が注目を浴びているように見える。このため、リスク関連のデータをどのように集めるかにも関心が行くようになり、セキュリティーインテリジェンス技術と結びつけるような動きも出てきている。

(4) 科学技術的課題

情報セキュリティーや IT リスクの問題を考えるにあたっては、科学技術的な研究はもちろん重要であるが、国際政治、法律、安全保障、危機管理、経済学、心理学等の社会科学的視点も含めさまざまな領域の研究とも連携して行われることが求められる。しかし、これらの研究は個別かつ小規模におこなわれているに過ぎない。

(5) 政策的課題

今後の脅威の増大を考えるなら、政府はこの問題を重要課題として取り上げ、大きなプロジェクトの設立を検討すべきであると考える。このプロジェクトにおいては、セキュリティー保険とのリンク等社会実装の関係も含めて研究課題としておくべきだろう。

(6) キーワード

リスクアセスメント、リスクコミュニケーション、リスクマネジメント

(7) 国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	○	↗	IT システムに関するリスクコミュニケーションなどの研究が大学などで積極的に進められているが層は薄い。
	応用研究・開発	○	↗	IPA 等でセキュリティー経済学やリスク心理学的アプローチが進み始めているが層は薄い。
米国	基礎研究	◎	↗	リスクアセスメントに関する大学における研究は多い。また、理論的研究に関するアプローチが開始されている。
	応用研究・開発	◎	↗	NIST を中心に、リスクマネジメントに関する基準やガイドを策定して公開している。国の組織の安全性評価に積極的に適用している。
欧州	基礎研究	○	→	ディフェンスグラフを用いる対策案選定法などのリスクアセスメント技術が大学などで積極的に進められている。
	応用研究・開発	◎	→	セキュリティー経済学については、ENISIA で 2011 年より、WG が作成され研究がおこなわれてきたが、最近は目立った新しい動きは見られない。
中国	基礎研究	○	↗	大学などにおいてリスクアセスメントに関する研究は行われているようであり、論文などは増えつつある。
	応用研究・開発	△	→	目立った動きが見えない。

韓国	基礎研究	○	→	大学などにおいてリスクアセスメントに関する研究は行われている。
	応用研究・開発	○	→	政府機関などにおいてリスクアセスメントが実施されている。

（注１） フェーズ
基礎研究フェーズ：大学・国研などでの基礎研究のレベル
応用研究・開発フェーズ：研究・技術開発（プロトタイプの開発含む）のレベル
（注２） 現状 ※わが国の現状を基準にした評価ではなく、CRDS の調査・見解による評価である。
◎ 特に顕著な活動・成果が見えている、 ○ 顕著な活動・成果が見えている
△ 顕著な活動・成果が見えていない、 × 活動・成果がほとんど見えていない
（注３） トレンド
↗：上昇傾向、 →：現状維持、 ↘：下降傾向

(8) 参考文献

1) International Organization for Standardization（ISO）, “ISO/IEC27001:2013,Information security management”, http://www.iso.org/iso/home/standards/management-standards/iso27001.htm（ 閲覧日 2016-12-15）
2) International Organization for Standardization（ISO）, “ISO31000: 2009, Risk Management,” http://www.iso.org/iso/home/standards/iso31000.htm（閲覧日 2016-12-15）
3) Ross Anderson, “Why information security is hard---An economic perspective,” In Proceedings of the17th Annual Computer Security Appliations Conference（Louisiana, USA, 2001）, pp. 358-364（IEEE, 2001）.
4) European Union Agency for Network and Information Security（ENISA）, Working Group on Economics of Security https://www.enisa.europa.eu/activities/risk-management/working-group/WG%20EoS（閲覧日 2016-12-15）
5) Bruce Schneier, “Attack trees,” Dr. Dobb’s journal, Vol. 24, pp. 21-29（1999）.
6) Sophie Pinchinat, Mathieu Acher, and Didier Vojtisek, “Towards Synthesis of Attack Trees for Supporting Computer-Aided Risk Analysis” Workshop on Formal Methods in the Development of Software（co-located with SEFM）2014（Grenoble, France, 2014）.
7) 石井 亮平 , 佐々木 良一 , 金子 紀之 , “イベントツリーを用いたリスク評価ツールの実装と標的型攻撃最適組み合わせ問題への適用”, コンピュータセキュリティシンポジウム 2013（高松 , 2013）論文集 4 号 , pp 147-154（情報処理学会 , 2013）.
8) 大久保隆夫 , “脅威分析法 組み込みの安全性とセキュリティを保証するために”（情報セキュリティ大学院大学講義資料） https://www.ipa.go.jp/files/000046476.pdf（閲覧日 2016-12-15）
9) Kenji Taguchi, et. al., “Meta-modelling approach to standardizing Safety-Sensitive Consumer Devices,” Asia-Pacific Council on Systems Engineering Conference（APCOSEC）2013（Yokohama, Japan, 2013）.
10) 佐々木 良一 , 日高 悠 , 守谷 隆史 , 谷山 充洋 , 矢島 敬士 , 八重樫 清美 , 川島 泰正 , 吉

浦 裕 , “多重リスクコミュニケータの開発と適用”, 情報処理学会論文誌 Vol. 49, No. 9, pp. 3180-3190 (2008).
11）佐々木 良一 (編),「IT リスク学 情報セキュリティを超えて」(共立出版 ,2013).
12）National Institute of Standards and Technology (NIST), “Framework for Improving Critical Infrastructure Cybersecurity Ver.1.0 (February 2014)”, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf（閲覧日 2016-12-15）
13）Jack Freund and Jack Jones, Measuring and Managing Information Risk: A FAIR Approach (Elsevier, 2015).
14）National Institute of Standards and Technology (NIST), “Guide for Conducting Risk Assessments (September 2012)”, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf（閲覧日 2016-12-15）
15）Stefano Bistarelli, Fabio Fioravanti, and Pamela Peretti, “Defense trees for economic evaluation of security investments,” In Proceedings of the 1st International Conference on Availability, Reliability and Security (Vienna, Austria, 2006), pp. 416-423 (IEEE. 2006).
16）Thomas L. Norman, Risk Analysis and Security Countermeasure (CRC, 2016).