3.13　セキュリティー

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、情報セキュリティーである。情報セキュリティーの研究分野は広く、縦軸に基礎か応用かを、横軸に要素技術的かシステム技術的かをとると図 3.13.1 に示すように整理することができる。ここでは、そのうち特に重要性が高いと考えられる次の 7 つの項目について動向をまとめた。

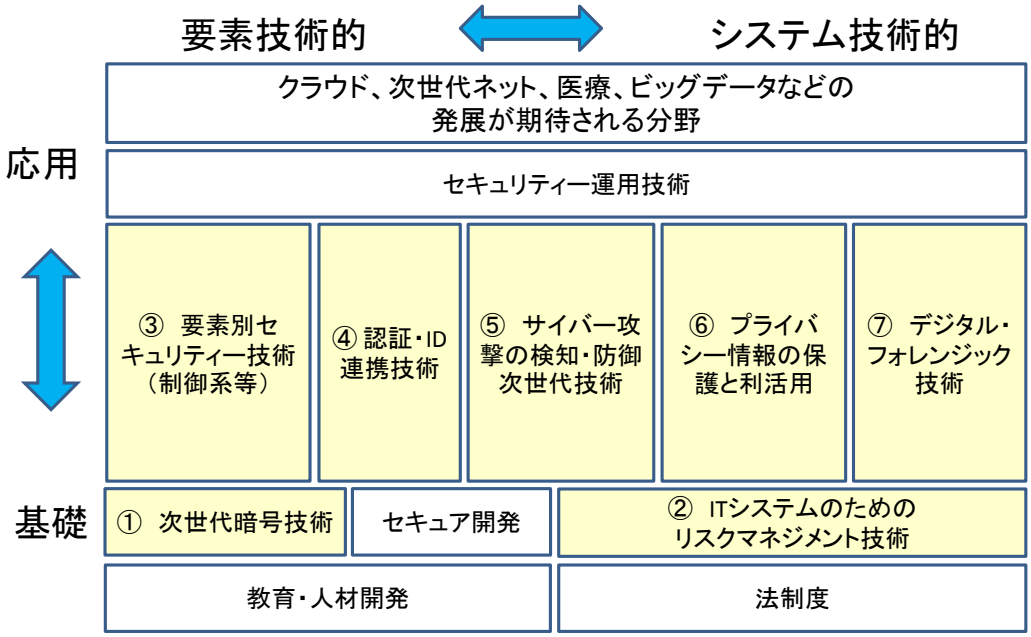

図 3.13.1 セキュリティーの俯瞰図

（１）次世代暗号技術

暗号技術は、データの秘匿性（情報を部外者に見られないこと）、完全性（情報が書き換えられていないこと）、真正性（通信相手やデータの提供元が意図した相手であること）などを確保する上で欠かせない基本技術である。最近では、様々なニーズに応えるための研究開発が重要となりつつあり、具体的には次のような動向が注目されている。

1. データを暗号化したまま演算や情報処理を可能とする暗号化状態処理の研究開発
2. 暗号鍵漏えいからの回復力（レジリエンス）や使い勝手の向上などに関する研究開発
3. 物理的な特性を盛り込んだ暗号技術および暗号プロトコルの研究開発
4. 暗号技術および暗号プロトコルの軽量化の研究開発

この分野の日本の基礎研究・応用研究のレベルは、学会活動の状況などから判断して、十分高く、国際的にもよいポジションにあると考えられる。産官学が協力してうまく産業応用に結び付け、製品競争力の向上に結び付けられるようにしていくことが、大きな課題であると考えられる。

（２）IT システムのためのリスクマネジメント技術

高度化、複雑化する標的型攻撃や、内部犯罪へ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。

この実現のためには、次のような項目の実施が必要になる。

（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

（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。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

これらの技術の開発は、各国において試みられてきているが、まだ十分な成果を上げているとはいえない状況である。今後は、単に情報システム等の脅威を考えたり、技術的な研究をするのみならず、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。

（３）要素別セキュリティー技術（制御系、その他（情報家電、各種機器、自動車等））

セキュリティー対策が必要な対象は、従来の PC やサーバーだけでなく、制御システムや、情報家電、自動車などに拡大している。ここでは、制御系と、その他に分けて動向を整理する。

（ａ）制御系

技術的には、制御分野の特性から、アンチウイルスを適用できない装置に対するホワイトリスト技術、不正侵入に対する検知技術や一方向性ファイアウォールなどが、必要となっている。また今後の深刻なリスクに備えて、評価認証制度を国内の制御システム事業者や重要インフラ事業者および国産製品に普及させるとともに、電力や交通や製造ラインなどの様々ある制御システム分野に固有の要件をまとめていくことが必要である。

（ｂ）その他（情報家電、各種機器、自動車等）

情報家電機器や通信機能を備えた医療機器（インスリンポンプやペースメーカー等）や自動車に対する攻撃による深刻な事故の可能性が指摘されている。また現実に情報家電機器やホームルータを踏み台にした DDoS 攻撃や、これらの機器からの情報漏えいなども多数報告されるようになっている。

技術的なセキュリティー対策は、基本的には、情報通信の分野で培われてきたものを活用していけると考えられるが、対象固有の新たな脅威の出現に対抗する技術開発を続けていくことが必要になる。また、政策的な課題としては、どのレベルの情報セキュリティー対策を各業界や各製品分野で搭載していくのかの基準の確立が重要な課題となっている

（４）認証・ID 連携技術

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、確実な認証と、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（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。

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。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、技術レベルは高く今後もそれを継続していくことが期待される。より高い安全性と使いやすさと低価格を実現できる方式の普及が今後の課題であろう。

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。ＩＤ連携は世界で広く採用される方式の確立が必要であり、応用活動や標準化活動が重要になっていくと考えられる。

（５）サイバー攻撃の検知・防御次世代技術

2014 年ソニー・ピクチャーズエンターテインメントへの攻撃に見られるようにサイバー攻撃はますます巧妙化、悪質化しており、その対策技術はますます重要性を増すと考えられる。このサイバー攻撃の検知・防御次世代技術の研究課題としては下記を挙げることができる。

（ａ）標的型攻撃対策技術
（ｂ）大規模感染型マルウエア対策技術
（ｃ）ドライブ・バイ・ダウンロード攻撃対策技術
（ｄ）DDoS 攻撃対策技術
（ｅ）マルウエア対策技術
（ｆ）サイバー攻撃可視化技術
（ｇ）サイバー攻撃情報共有技術

この分野は、「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が、大学等においてこれらのデータをとるのに日本の公的資金取得・利用の仕組みが適していない等の問題がある。また、学と産の連携も不十分であり、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、非常に限定的であり、米国などに大きく遅れをとっている。今後も新しい技術が必要となる分野なので、状況の改善が期待される。

（６）プライバシー情報の保護と利活用

個人情報保護法の改正時の検討でもっとも重要な課題として検討されているのがプライバシー情報の保護と利活用の両立である。この実現のためには、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が重要となる。大きく分類すると、（ａ）個人を識別不能な様にデータベースを匿名化して公開する技術（Privacy-Preserving Data Publishing)、（ｂ）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の技術（Secure Multiparty Computation)、（ｃ）分散されたサーバーに格納されたデータベースを暗号化してデータマイニングを実施する技術（Privacy-Preserving Data Mining)、（ｄ）抽出された知識からプライベート情報が漏洩しない様に精度を落としたりノイズを加えたりする技術（差分プライバシーなど）がある。

現在、学会レベルでいろいろな研究が実施されているが、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のが実情である。技術の開発とともに、社会的合意形成の努力をする中から、実用性のあるシステムの実現が待たれている。

（７）デジタル・フォレンジック技術

フォレンジック（Forensics）とは本来、法科学などと訳される語であり、科学的な知見を犯罪捜査や法廷の場における法的紛争の解決に役立てることを目的に発達した研究領域を指す。民間でも、巧妙化する標的型攻撃や、2014 年「ベネッセ個人情報流出事件」に見られるような内部からの個人情報の漏洩問題で、ログとデジタル・フォレンジック技術を利用して侵入経路や、情報の流出経路を明確化する努力がなされている。また、警察でもデジタル･フォレンジック技術無しには適切な捜査が行えない時代になってきており、「PC 遠隔操作事件」おける裁判に見られるようにデジタル・フォレンジックの専門用語が法廷で飛び交うようになっている。

また、デジタル・フォレンジック技術は、情報インフラとそれが支える物理的な社会インフラについて、不具合、人的ミス、災害、サイバー攻撃による問題や障害の発生の防止、問題や障害が発生した場合でも影響を最小限に抑えるためにも有用である。

主要な技術動向として以下のようなものがある。

（ａ）ハードディスクの大型化やＳＳＤの普及に対応した電磁的記録の消去や改ざん、偽造の検出や分析技術
（ｂ）インターネットの追跡困難性や通信の暗号化および匿名性に対する対策技術
（ｃ）ウイルス対策ソフトウエアでは検知できないマルウエアの対策技術
（ｄ）主記憶装置など従来は扱えなかった揮発性メモリー領域のデータを利用するライブフォレンジック（メモリーフォレンジック）
（ｅ）大規模データから必要情報の高効率抽出などのための機械学習などの応用

デジタル・フォレンジックに関する製品に関しては、米国などが先行しており、一部を除いて日本の国際競争力は低いといわざるを得ない。また、技術力のある専門家の育成も不十分で今後の重要な課題である。特に、研究人口の不足は深刻で、画像処理や言語処理や人工知能などの分野からの参入を促進していく必要がある。

3.13.1　次世代暗号技術

（1）研究開発領域名

次世代暗号技術

（2）研究開発領域の簡潔な説明

新たに発生する多様な要求に応えるための暗号技術および暗号プロトコルの確立を目的とした研究開発。

（3）研究開発領域の詳細な説明と国内外の動向

暗号技術は現代の ICT 社会においてデータの秘匿性（情報を部外者に見られないこと）、完全性（情報が書き換えられていないこと）、真正性（通信相手やデータの提供元が意図した相手であること）などを確保する上で欠かせない技術となっている。一方、ICT の適用範囲も従来のパソコンやサーバーを中心とする情報処理産業から、周辺機器を含み、より社会に密接した社会インフラ、交通、農業、医療などより多様で多彩な分野に広がりつつある。それに伴い、暗号技術や暗号プロトコルも各応用先の様々なニーズに応えるための研究開発が重要となりつつある。具体的な動向としては以下が挙げられる。

1. データを暗号化したまま演算や情報処理を可能とする暗号化状態処理の研究開発
2. 暗号鍵漏えいからの回復力（レジリエンス）や使い勝手の向上などに関する研究開発
3. 物理的な特性を盛り込んだ暗号技術および暗号プロトコルの研究開発
4. 暗号技術および暗号プロトコルの軽量化の研究開発

1 の動向はクラウドの普及や情報漏えい対策のためにデータを暗号化してサーバーに保存する機会が増えたことに起因する。通常、暗号化されたデータを処理する際には、復号鍵を持っているノードに一旦データを送り、暗号文を復号し、必要な演算や情報処理を行った後、再び暗号化してサーバーに戻す。そのため、データ復号時の漏えいリスクや、通信量、計算量の増大などの問題がある。この問題に対処するための研究開発として、データを暗号化したまま情報処理可能な暗号化状態処理に注目が集まっている。暗号化状態処理の実現方法には幾つかの方法があるため、各動向について以下でまとめる。

・完全準同型暗号を利用する方法：

完全準同型暗号は、暗号化した状態で平文（暗号化される前のデータ）の加減乗除の四則演算を可能とする暗号方式である。計算量や鍵、暗号文のサイズが大きいという欠点があるが、それらを削減するための基礎理論研究が進められており、主要な研究成果が欧米を中心に創出されている。安全性の根拠となっている格子上 SVP (Shortest Vector Problem) を解くために必要となる計算量の見積もりについては日本からも貢献がある [1)]。研究については、米国のメンバーを中心に完全準同型暗号のライブラリ実装 HElib [2)]が進められている。

・セキュアマルチパーティコンピューテーション(SMC: Secure Multiparty Computation)を応用する方法：

SMC は関係者間で通信を行うことにより互いの入力を相手に秘匿しながら任意の値を計

算する暗号プロトコルである。SMC の基礎理論研究は 1980 年代頃から行われているが、近年、計算能力の増加に伴い実装と応用が進みつつある。例えば欧州では、エストニアの Sharemind を使ったロケットの衝突リスク計算[3]やイタリアの SecureSCM を使ったサプライチェーンマネジメント(SCM: Supply Chain Management)[4]などの応用研究が行われている。日本でも、医療統計分析[5]や化合物検索[6]などの応用研究が行われている他、各社産業化に向けた研究開発を加速させている[7]。SMC の構成要素である準同型暗号や秘密分散、また、その一応用例である匿名エンティティ認証は、それぞれ ISO/IEC 18033-6、19592、20009 として標準化も進められている。

2 は、暗号鍵漏えいへの対処方法や暗号技術をより使い易くするための動向である。前述のとおり暗号技術は現代の産業界にとって欠かせない技術となっており、その解読し難さは当然ながら、それに加えて使い勝手の向上も求められつつある。また、長年の基礎理論研究の結果、解読困難な暗号技術の設計手法もほぼ確立し、解読困難な暗号技術も多数市場に提供されている。そのため、現在においては、暗号アルゴリズムが破られる危険性より、暗号鍵が漏れたり、実装上の問題が突かれたりする危険性の方が高まっており、それらへの対応が求められている。米国では、RKI (Relational Key Infrastructure)[8]という新たな概念が提唱され、産業化が進められている。RKI では、PKI（Public Key Infrastructure）を使いつつ、PKI において運用負荷の大きい証明書発行時や秘密鍵漏洩時における実世界での事務処理の手間を軽減する工夫が加えられている。その概要は以下のとおりである。RKI の各エンティティは、自分の公開鍵 PRK 秘密鍵 PK 対を生成し、PK を GA(Group Authority)に送り、それに対して verinym V というランダムな ID を発行してもらう。GA は V と PK に対する証明書 CERT を発行し、レポジトリ R に登録する。このように、RKI では PK の所有者が誰であるかの確認を省略することにより、実社会での事務処理の手間を省いている。次に、そのエンティティは、V の Ownership Contract (OC) である VOC を生成し、VOC に V の PRK で電子署名を付加し、各認証局 CA に送る。VOC には V に紐づけられている PK を変更する際に必要となる署名鍵などの情報が記述される。各認証局 CA はその V に対する VOC がまだ登録されていなければ、それを保存する。PRK が漏洩した場合には、新たな PRK/PK 対を生成し、新たな PK に VOC の条件を満たす電子署名を付けてもらい CA に渡す。CA は VOC の条件が満たされていることが確認できれば、V に対応する PK が新たな PK であることを示す公開鍵証明書 CERT を発行する。これにより、公開鍵証明書の無効化手続きも自動で行えるため、オフラインでの事務処理を省略することができる。

日本における鍵漏洩へのレジリエンス（回復力）と利便性を両立するための研究開発動向としては、利用者に短いパスワードの利用を許可し利便性を高めながら、鍵漏えいに対して回復力を持たせた相互認証・鍵管理基盤 LR-AKE (Leakage-Resilient Authenticated Key-Establishment)が実用化され産業化が進みつつあることが挙げられる[9]。

3 の物理的な特性を盛り込んだ暗号技術および暗号プロトコルの研究開発動向としては、まず、量子力学の不確定性原理を応用した量子鍵配送が挙げられる。欧米の企業により商用サービスも提供されているが、前述の通り、暗号技術に求められるニーズは一つの側面の高い安全性より、実装や鍵の保護などを含めたトータルでの安全性や利便性とのバランスに移行しつつあり、通信路の盗聴のみに対する高い安全性だけで他の方式との優位性を認めても

らうことが難しくなってきている。一方、不確定性原理を乱数生成器に応用するという新たな展開も出始めている。ここ数年、公開鍵生成時のエントロピー不足による秘密鍵の特定[10)11)]が現実的な社会問題となっており、また、スマートカード、IoT (Internet of Things)、M2M (Machine to Machine)、CPS (Cyber Physical Systems)などにおける乱数生成時のエントロピー確保の問題[12)]もあり、問題解決の一つの方法となる可能性がある。

デバイスから消費電力や漏えい電磁波などのサイドチャネル情報を使って暗号鍵を抜き出す方法の研究開発動向としては、解読コンテスト[13)]が行われており、現実的な側面から解析技術、防御技術の検証が行われている。他には、シリコンチップ用の物理複製困難関数(PUF：Physically Unclonable Function)に関する基礎および応用研究が国際会議 CHES (Workshop on Cryptographic Hardware and Embedded Systems) [14)]などを中心に盛んになりつつあり、欧米では産業化も進みつつある。シリコンチップ用の PUF とは電子回路のパスの微妙な長さの違いや電子素子の不純物の微妙な違いなどに応じて出力が異なるように設計された回路であり、シリコンチップの不正な複製の検出や、暗号鍵の生成や保存の用途としての期待が高まりつつある。

4 は安全性を犠牲にすることなく計算機への負担を軽減するための研究開発である。前述の通り、暗号技術は現在様々な用途で利用されており、中には計算資源が乏しかったり、遅延が許容できなかったり、バッテリーの持ちを長くするため消費電力量を抑えなければならなかったりする場合もある。このような環境に適した暗号技術の研究開発は従来、欧州の Framework Programme において盛んに行われ[15)]、日本からもアルゴリズム提案や安全性評価について貢献が行われていた。現在では、それらの成果も踏まえながら標準化作業が進んでおり、ISO/IEC では 20192 Lightweight cryptography として、そのパート２においてブロック暗号、パート３においてストリーム暗号、パート４において公開鍵暗号技術、パート５においてハッシュ関数の検討が進められている。また、パスワード (weak secret)のみを使ってクライアント、サーバー間で相互認証を行う PAKE (Password Authenticate Key Exchange) の標準規格 ISO/IEC 11770-4 Key management -- Part 4: Mechanisms based on weak secrets の見直しも進められており、より軽量でかつ安全性証明の付いた方式の標準化に向けた検討が行われている。さらに、米国においても 2015 年 7 月に NIST で light-weight cryptography のワークショップ[16)]が計画されており、その重要性が増しつつある。

（４）科学技術的・政策的課題

暗号技術には従来より高い解読困難性が求められていたが、最近では、その高い解読困難性に加えて、産業界からの多様な要求に応えることの重要性が増しつつある。これは、暗号技術が産業を支える要素技術の一つになったことにより、暗号解読耐性以外の価値も重要視され、特定の攻撃のみに対して過度な耐性を追求するより、実装上の安全性や鍵管理、使い勝手、処理速度、消費電力量などが全体として応用先に合致する方が重視されるようになったからである。

したがって、科学技術的・政策的にも、一部の攻撃のみに対してずばぬけた耐性を求めるのでなく、応用先の多様なニーズを先取りしながら、それらに応えるための研究や、そこに新たな科学技術的、学術的な課題を見いだすことが重要である。

（５）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）

従来、暗号技術や暗号プロトコルと連携するには、暗号アクセラレータ、耐タンパーモジュール（TRM：Tamper Resistance Module）、TPM (Trusted Platform Module)、物理乱数生成器などがあったが、新たなハードウエアとしてシリコン PUF (Physically Unclonable Function：物理複製困難関数) が注目されつつある。PUF は忠実なコピーが困難となる物理的な特性のことであり、この特性を用いることによりデバイスや商品などの真贋判定を行える他、方式によっては、乱数生成、サイドチャネル攻撃に強い鍵生成や鍵共有プロトコルなどを構成することが可能となる。欧米では商用展開も始まっており、学会での技術改良の議論も盛んになりつつある。今後、IoT (Internet of Things)、M2M (Machine to Machine)、CPS (Cyber Physical Systems)向けの新たなセキュリティーモジュールとして広がりを見せる可能性がある。

（６）キーワード

暗号化状態処理技術、秘匿検索、秘匿計算、物理複製困難関数、乱数生成、軽量暗号

（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	◎	→	国内会議SCIS (Symposium on Cryptography and Information Security：暗号と情報セキュリティシンポジウム)、 CSS (Computer Security Symposium：コンピュータセキュリティシンポジウム) などを中心に次世代方式の提案、改良、安全性の議論が定常的に行われている。
	応用研究・開発	◎	→	秘匿計算、秘匿統計分析、秘匿検索、量子鍵配送システム、PUFシステムなどのプロトタイプ開発が進む。
	産業化	○	↗	検索可能暗号、秘匿計算、秘匿統計分析、漏えいにレジリエントな認証・鍵管理基盤などの産業展開実績あり。
米国	基礎研究	◎	→	CRYPTOなどの国際会議を中心に次世代方式の提案、改良、安全性の議論が定常的に行われている。
	応用研究・開発	◎	→	Helib など完全準同型暗号の実装と改良が進む。NISTが Lightweight 暗号のワークショップを2015年7月に開催予定。
	産業化	◎	→	量子鍵配送システム、PUFの産業展開実績あり。RKI (Relational Key Infrastructure) の提案と産業展開。
欧州	基礎研究	◎	→	EUROCRYPTなどの国際会議を中心に次世代方式の提案、改良、安全性の議論が定常的に行われている。
	応用研究・開発	◎	→	秘匿計算の応用実績あり。
	産業化	◎	→	秘匿計算、量子鍵配送システム、量子乱数生成器、PUFの産業化実績あり。 Sharemind（エストニア）、量子鍵配送システム（id Quantique (ジュネーブ)、SmartQuantum (フランス)、そしてQuintessence Labs (オーストラリア)）、量子乱数生成器、SRAM PUFが産業展開中。
中国	基礎研究	△	↗	今後増加が見込まれる。
	応用研究・開発	△	↗	従来技術の応用や開発が主。
	産業化	△	→	従来技術の産業化が主。
韓国	基礎研究	△	↗	今後増加が見込まれる。
	応用研究・開発	△	→	従来技術の応用や開発が主。
	産業化	△	→	従来技術の産業化が主。

（註 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
産業化フェーズ ：量産技術・製品展開力のレベル

（註 2）現状
※我が国の現状を基準にした相対評価ではなく、絶対評価である。
◎：他国に比べて顕著な活動・成果が見えている、 ○：ある程度の活動・成果が見えている、
△：他国に比べて顕著な活動・成果が見えていない、×：特筆すべき活動・成果が見えていない

（註 3）トレンド
↗ ：上昇傾向、 →：現状維持、 ↘：下降傾向

（８）引用資料

1) "SVP Challenge" http://www.latticechallenge.org/svp-challenge/index.php
2) "HElib" https://github.com/shaih/HElib
3) "Sharemind" https://sharemind.cyber.ee/
4) "SecureSMC" http://sesar.di.unimi.it/Sesar/securescm
5) NTT "秘密計算システム" http://www.ntt.co.jp/inlab/blabo/forum2014/pdf/C-1.pdf
6) AIST "秘密計算による化合物データベースの検索技術" http://www.aist.go.jp/aist_j/press_release/pr2011/pr20111101/pr20111101.html
7) 清藤、四方 "高機能暗号を活用した情報漏えい対策「暗号化状態処理技術」の最新動向" http://www.imes.boj.or.jp/research/papers/japanese/14-J-10.pdf
8) ENT Foundation "Entity Network Translation (ENT) + Relational Key Infrastructure (RKI)" http://www.ent.net/mcms_site/images/pages/20140906_mapping_full.png
9) 今井 秀樹 "情報セキュリティと「想定外」" https://www.jstage.jst.go.jp/article/essfr/5/3/5_3_198/_pdf 電子情報通信学会 基礎・境界ソサイエティ Fundamentals Review, Vol. 5, No.3, pp.198-204, 2012.01
10) Nadia Heninger, Zakir Durumeric, Eric Wustrow and J. Alex Hlderman "Mining your Ps and Qs: Detection of Widespread Weak Keys in Network Devices" In Proc of the 21st USENIX Security symposium, 2012.8
11) Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung and Christophe Wachter "Public Keys" Advances in Cryptology - CRYPTO 2012, LNCS 7417, pp 626-642, 2012.8
12) Daniel J. Bernstein, Yun-An Chang, Chen-Mou Cheng, Li-Ping Chou, Nadia Heninger, Tanja Lange, Nicko van Someren "Factoring RSA Keys from Certified Smart Cards: Coppersmith in the Wild" Advances in Cryptology - ASIACRYPT 2013, LNCS 8270, pp 341-360, 2013.12
13) "DPA contest" http://www.dpacontest.org/home/
14) "Workshop on Cryptographic Hardware and Embedded Systems" http://www.chesworkshop.org/
15) "European Network of Excellence in Cryptology II" http://www.ecrypt.eu.org/index.html
16) NIST " Lightweight Cryptography Workshop 2015 " http://www.nist.gov/itl/csd/ct/lwc_workshop2015.cfm

3.13.2　IT システムのためのリスクマネジメント技術

（1）研究開発領域名

IT システムのためのリスクマネジメント技術

（2）研究開発領域の簡潔な説明

重要性を増す 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ために、(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、(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、（ｃ）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技術の高度化などを行う。

（3）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、複雑化する標的型攻撃や、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。

この実現のためには、次のような項目の実施が必要になる。

（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

（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。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

これらの技術の開発は、各国において試みられてきているが、まだ十分な成果を上げているとはいえない状況である。

［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：

近代の組織では、マネジメントシステムによりいろいろな対象を、適正に管理をしようと試みてきた。1960 年代には米国のエドワーズ・デミング（Edwards Deming）による PDCA サイクル（plan-do-check-act の略で計画、実行、評価、改善を繰り返す）の概念を用いて、事業の生産管理や品質管理が効果的に行われるようになった [1)]。

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)。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、次の 3 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扱ってきた。

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 3.13.2 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けられるようになった。また ISO/IEC27001 の 2013 年改定では情報資産でなく、広く無体物としての情報を対象とするようになった [3)]。

このように概念としては整理されてきたが、リスクコミュニケーションを図 1 において具体的にどのように扱うかの検討は（ｃ）で述べるように不十分のままである。

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 [4)5)6)]。現在も小規模ではあるがいろいろな研究がなされており、さらなる研究の進展が期待されている。

また、ＩＴシステムのリスクマネジメントの概念をさらに広くとらえ、整理していくことも必要となっている。

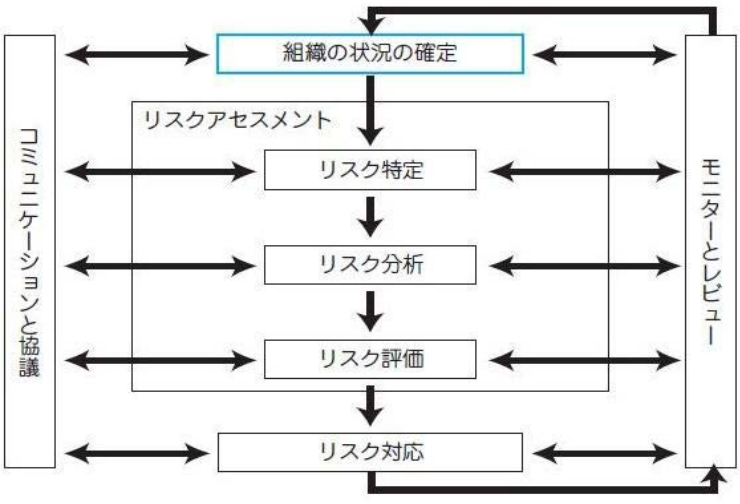

図 3.13.2　リスクマネジメントのプロセスの流れ（ISO31000）

（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２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

上記の①に対しては、下記のようにすでにいろいろな方法が提案されている[6]。

（イ） ブレーンストーミング法（非形式的アプローチ）

（ロ） チェックリスト利用法（ベースラインアプローチ）

（ハ） ランク値付けマトリックス法（詳細リスク分析アプローチ）

（ニ） フォールトツリー分析法（詳細リスク分析アプローチ）

ランク値付けマトリックス法に関しては、EU においてクラウドのセキュリティー等に対し、優れた適用が行われている[7]。また、Bruce Schneier がセキュリティー評価に適するようにフォールトツリー分析法を改良したアタックツリー分析法[8]の適用などもいろいろ行われている（例えば引用資料 9)）。

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）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。

上記の②のどのような対策をとるべきかを明確にするため、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 Attack）を用いた最適な対策選定手法を提案している[10]。

また、標的型攻撃のように複雑で種々の方法を組み合わせた攻撃に対し、イベントツリー分析法とフォールトツリー分析法を組み合わせ、派生リスクやコストを考えたうえで最適の対策案の組み合わせを求める方法の提案と適用が実施されている[11]。

しかし、いずれも大規模な問題に、容易に適用できるものにはなっていない。

（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

リスクコミュニケーション自体の研究は１９８０年代から本格的に実施されるようになってきており、米国のナショナル･リサーチ・カウンシルは１９８９年にリスクコミュニケーションを、「個人とグループ、そして組織の間で情報や意見を交換する相互作用的過程である」と定義しており、リスクのタイプとレベルに加えて、リスクマネジメントの方法に関する議論が必要であるともいう[12]。しかし、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[13]。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。

現状の MRC は、モデリングに専門知識を必要とし、しかも、時間がかかるという問題がある。

［今後必要となる取り組み］

（ａ）ＩＴシステムの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

従来のリスクマネジメントは経験に基づく手順の提示が中心で、理論に基づく技術の体系化がなされておらず、ＩＴ分野以外のリスク管理と連携した、統合的なリスク管理も不十分であった。このような状況は国内だけでなく海外でも同様であると考えられる。

このため、佐々木らは「ＩＴリスク学」[14] 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たが進展は限定的であり、さらに多くの研究者が参加した上でのこのような研究の深化が期待される。

また、情報セキュリティ大学院大学ではＩＴリスクに対し、経済学・経営学・法学などを総合的に組み合わせた研究を行ってきたが（引用資料 14）の 7 章）、さらに多くの研究者が参加して、研究を行うべきテーマであると考えられる。

（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、ＩＴシステムの各種サービスを対象としたリスクアセスメントが重要となってくると考えられる。例えば、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おり、一部実施されているが、リスクアセスメント技術を向上させる中からさらに高度な分析ができるようにしていく必要がある。

また、リスクの本質である、1 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選ぶ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。

（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。

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。

（４）科学技術的・政策的課題

内閣サイバーセキュリティーセンター（NISC）が指摘するように、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、単に情報システム等の脅威を考えたり、技術的な研究をするのみならず、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[15]。

（５）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）

（ａ）セキュリティー経済学については、ENISA(European Union Agency for Network and Information Security)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[16]。最近では、プライバシーの経済学の研究もおこなわれるようになってきた[18]。

（ｂ）米国のミシシッピー州立大学では将来のセキュリティー研究の方向を検討し、①Separating insider deviant behavior from insider misbehavior、②Unmasking the mystery of the hacker world、③Improving information security compliance、④Cross-cultural InfoSec research を含むものになるだろうと推定している[17]。

（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、リスク対リスク

（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。
	産業化	―	↗	―
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。
	産業化	―	↗	―
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、ENISAで2011年より、WGが作成され研究が強化されている。また、クラウドのセキュリティー評価などが適切に実施されている。
	産業化	―	↗	―
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るが目立たない。
	応用研究・開発	△	→	目立った動きが見えない
	産業化	―	→	―
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。
	産業化	―	→	―

（註 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
産業化フェーズ ：量産技術・製品展開力のレベル
（註 2）現状
※我が国の現状を基準にした相対評価ではなく、絶対評価である。
◎：他国に比べて顕著な活動・成果が見えている、 ○：ある程度の活動・成果が見えている、
△：他国に比べて顕著な活動・成果が見えていない、×：特筆すべき活動・成果が見えていない
（註 3）トレンド
↗ ：上昇傾向、 →：現状維持、 ↘：下降傾向

（８）引用資料

1) W. デミング、NTT データ品質保証研究会訳、デミング博士の新経営システム論、NTT 出版 1996
2) ISO, ISO31000:2009, Risk Managemeent – Principles and guidelines, 2009
3) ISO/IEC27001:2013, Information technology -- Security techniques -- Information security management systems -- Requirements

4) R. Anderson: “Why information security is hard---An economic perspective,” Proc. 17th Annual Computer Security Appliations Conference, 2001.
5) L. A. Gordon and M. P. Loeb: “The economics of information security investment,” ACM Trans. Info. Sys. Security, vol.5, no.4, pp.438-457, 2002.
6) ISO/IEC TR 13335-1~5, Guidelines for the Management of IT Security(GMITS)
7) ENISA： Cloud Computing: Benefits, risks and recommendations for information security, 2009
8) Bruce Schneier, "Attack trees," Dr. Dobb’s journal, vol. 24, pp. 21-29, 1999.
9) Pinchinat, Sophie, 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.
10) S. Bistarelli, F. Fioravanti, and P. Peretti, "Defense trees for economic evaluation of security investments," in Availability, Reliability and Security, 2006.
11) 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 論文集,4号,pp 147-154
12) National Research Council (U.S.). “Improving Risk Communication”, The National Academies Press,1989
13) 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
14) 佐々木良一編著「ＩＴリスク学　情報セキュリティを超えて」共立出版，２０１３
15) 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）」2014
16) ENISA , Working Group on Economics of Security https://www.enisa.europa.eu/activities/risk-management/working-group/WG%20EoS
17) Robert E. Crosslera, Allen C. Johnstonb, Paul Benjamin Lowryc, Qing Hud, Merrill Warkentina, Richard Baskervillee; Future directions for behavioral information security research, Computers & Security, Volume 32, February 2013, Pages 90–101
18) S. Romanosky, D. Hoffman, A. Acquisti. "Empirical Analysis of Data Breach Litigation." WEIS2012. http://weis2012.econinfosec.org/papers/Romanosky_WEIS2012.pdf
19) K. Matsuura. “A Derivative of Digital Objects and Estimation of Default Risks in Electronic Commerce.” LNCS 2229, pp.90-94, Springer, 2001.

3.13.3　要素別セキュリティー技術

（1）研究開発領域名

要素別セキュリティー技術（制御系、その他（情報家電、各種機器、自動車等））

（2）研究開発領域の簡潔な説明

これまでの情報通信系システムだけでなく、組込み系システムという分野に象徴されるように、あらゆる「もの」が、ソフトウエアで制御されるようになり、更にネットワークと接続する時代となってきている。それに伴って、これまでは情報セキュリティーへの脅威を考慮してこなかった分野でもその対策が不可欠となっている。しかも近年、標的型サイバー攻撃と呼ばれる攻撃対象や目的（機密情報窃取やシステム破壊等）を特定した攻撃が深刻な脅威となってきている。それぞれの分野固有の情報セキュリティー上の脅威の明確化と、それに対する技術面や運用管理面での対策、参照する基準や標準、ガイドなどの整備に加え、業界ごとにおける普及啓発が重要となっている。

（3）研究開発領域の詳細な説明と国内外の動向

①制御系システムのセキュリティー[1)]

［背景と意義］

制御系システムは、従来、固有のプラットフォーム、固有のソフトウエア、固有のプロトコル、更に、基本的には外部とのネットワーク接続はなされない環境で使われるものと考えられ、情報セキュリティー的な配慮はほとんどなされてこなかった。しかし、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んでおり、更にメンテナンスや管理、上位の情報系システムとの連携などの目的で外部ネットワークに接続され、サイバー攻撃の対象になってきているという課題に直面している。2010 年にはイランの原子力施設へ侵入し誤動作を起こさせたマルウエア Stuxnet は大きな衝撃を与えたが、以降も、石油会社での多数のワークステーションのディスク破壊や交通制御装置の誤動作など、サイバー攻撃による事件、事故が多数報告されている。社会や組織にとって影響の非常に大きい分野であり、この４、５年大きな脅威となってきている標的型サイバー攻撃の対象となって大きな混乱や被害を招かないように、早急に備えていく必要がある。

一方で、サイバー攻撃の糸口となる産業用制御システムのソフトウエアの脆弱性の報告件数も大幅に増加しており、その対策や対応も急務である。しかし制御系システム分野では、24 時間 365 日の稼働（可用性）が重要な要件であるためアンチウイルスワクチンの使用の制約やセキュリティーパッチの適用が困難といった課題がある。しかも 10 年以上の稼働が前提のシステムのためセキュリティーパッチが提供されないなど、この分野固有の課題も抱えている。

こうした中で、重要インフラや製造ライン等で用いられる制御系システムの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が必要となってきている。

［これまでの取り組み］

制御系システムのセキュリティーの基準や標準は欧米を中心に策定が先行しているが、そ

のカバー範囲は、組織やシステムや装置等の各セキュリティーレイヤに対応したもの、業種や業界に対応したもの等、様々な基準や標準が提案されている。このような状況下において、全てのセキュリティーレイヤをカバーし、業種に依存せず汎用的な基準・標準であるIEC62443（工業用プロセス計測制御のセキュリティ規格）が注目されてきており、一部の事業者の調達要件に引用する動きもでてきている。

IEC62443 は以下の 4 階層、13 の基準から構成されている：

IEC62443-1：用語、コンセプト、モデルの定義について記した技術仕様

IEC62443-2：事業者や運用者の組織管理を対象としたセキュリティ要求事項等の規格

IEC62443-3：制御システムを対象としたセキュリティ要求事項等の規格

IEC62443-4：制御システムを構成する個別装置のセキュリティ要求事項等の規格

一方で、制御系システム分野では、ある団体によって策定された基準を用いた第三者評価認証が ISCI [2]、WIB [3]等で実施されている。ISCI では 2010 年より制御系システムを構成する個々のコントローラ等の装置製品の認証制度を運用しており、重要な要件となる装置の通信機能に対する堅牢性（ロバストネス）のテスト技術を実用化している。WIB では、事業者によるシステムの調達の際のセキュリティー要件を広く規定しており、石油・化学等一部の業界でその認証が利用されてきている。一方で、この評価認証で先行していた ISCI や WIB の要求事項（評価基準）が、IEC62443 のシリーズ(-4 と-2 のレイヤ)に標準案として提案されてきている。換言すると、組織から装置やコンポーネントまでのレイヤをカバーする汎用の制御系システムセキュリティーに対する国際標準が、評価認証スキームを兼ね備えることになり、その適用や普及が進むものと考えられる。

国内では、2011 年より、制御系システムセキュリティーにおける基準や評価認証の検討に着手し、IEC62443 の審議中のドキュメントに対しての寄書を行うとともに、発行済みのパートに対して日本語訳を（財）日本規格協会より発刊し、また、評価認証として、2014 年に、CSSC [4]にて装置やコンポーネントに対して ISCI と相互承認される評価認証スキームを立ち上げ、更に JIPDEC [5]にて IEC62443-2-1 に準拠した組織のセキュリティーマネジメントの評価認証スキームを世界に先駆けて立ち上げた。

［今後必要となる取り組み］

技術的には、制御分野の特性から、アンチウイルスワクチンを適用できない装置に対するホワイトリスト技術、不正侵入に対する検知技術や一方向性ファイアウォールなどが必要となっている。

また今後の深刻なリスクに備えて、評価認証制度を国内の制御系システム事業者や重要インフラ事業者および国産製品に普及させるとともに、電力や交通や製造ラインなどの様々ある制御系システム分野に固有の要件をまとめていくことが必要である。例えば、電力業界ではスマートグリッドの敷設が進んでおり、その基準として、NIST7628 や IEC61580 他、様々提案されているが、業界や事業者として、真に有効となる基準の選定や拡張など、その検証を進めていく必要がある。

②その他のシステムのセキュリティー（情報家電、各種機器、自動車等）

［背景と意義］

情報家電をはじめとして、IoT や IoE という用語に象徴されるように、利便性や高付加価値化を実現するために、様々な機器にネットワーク機能やサービスが備えられてきている。その反面、情報家電機器やホームルータを踏み台にした DDoS 攻撃や、逆に機器からの情報漏えいなども多数報告されるようになっている。

また将来的な攻撃の可能性として、通信機能を備えた医療機器（インスリンポンプやペースメーカー等）に対して、研究ベースではあるが、無線からの攻撃の可能性が 2011 年より学会で発表されてきている。[6)]

更に、現在の自動車は 100 近い CPU を内蔵し、ソフトウエア制御が中心となってきている。また、車体内部の診断情報を外部に取り出すためのデバイスの接続口を備え、ネットワークを経由した情報の授受なども可能になり、さらにスマートフォンと情報をやり取りすることもできるようになってきている。その一方で、2010 年には、研究ベースであるが、ネット経由での攻撃が可能である事例が学会で公表される、引き続いて毎年新たな攻撃の試行実験例が発表されるようになってきている。[7)]

このように、機能の高付加価値化や利便性の向上のもとで、想定される脅威に対しての検討が急務となってきている。

［これまでの取り組み］

情報家電においては、基準等が国際的に定まっていない中で、日本においては 2010 年に、先行する主要な家電メーカーが参画し、IPA においてガイドを策定した [8)]。ガイドにおいては、搭載する情報機能、外部との接続口、提供されるネットサービスを前提に、想定される脅威と対策を抽出したものである。技術的には、これまで PC や情報通信で培ったセキュリティー技術の適用が可能である。しかし業界における利用は各社に委ねられたレベルにとどまっている。

自動車においては、欧州が先行して業界を束ねた基準作り（リスク分析手法など）や技術開発（セキュリティーチップ等）のプロジェクトを推進してきている。国内においては、業界の中にセキュリティー部会等を設置して検討を進めているとのことだが、詳細については公開されていない。2012 年に、IPA において自動車関連各社の参画の下、ガイドを策定した [7)]。ガイドは、自動車の仮想的なネットワーク構成の下で、情報家電のアプローチと同様に、想定される脅威と対策を抽出したものである。ただ、業界における利用は各社に委ねられたレベルにとどまっている。

両者とも難しい側面は、セキュリティーは製品の機能やサービスと表裏一体となっており、各社の事業戦略に深く関わってくるため、縦横な議論や合意が進まないという背景がある。

［今後必要となる取り組み］

技術的には、ソフトウエアに内在する脆弱性をいかに出荷前に低減するかが重要で、そのためのコーディング規約やセキュアコーディング技術、また、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、出荷後の利用時に発見される脆弱性のパッチの流通技術の確立も不可欠である。

業界団体が中心となって、業界におけるセキュリティー脅威の共通認識の下で、セキュリティー基準やレベルを定めていくことが望ましい。様々なものが相互に接続する中で、業界横断的な基準も将来的に必要になってこよう。また、特に人命に関わる自動車等においては、機能安全（セーフティ）の基準は先行して国際標準 ISO26262 となっていることを受け、機能安全も左右するセキュリティーをそこに取り入れていくことが重要である。

（４）科学技術的・政策的課題

技術的なセキュリティー対策は、これまで情報通信の分野で培われてきたものを活用していける。ただ、もちろん新たな脅威の出現や攻撃手法も巧妙化していくので、それに対抗する技術開発を続けていくことになる。サイバー攻撃の検知技術、防御技術、攻撃情報の共有フレームワークなどの確立が核になってくる。

政策的な課題としては、どのレベルの情報セキュリティー対策を各業界や各製品分野で搭載していくのかの基準が制定されていない点にある。非機能でありコストのかかるセキュリティー対策をどのレベルまで対応するかは、業界や製品分野に応じて、大枠のコンセンサスを作っていくのが重要な課題である。社会インフラとなっている制御系システム分野においては、国としての基準やガイドを制定していくことも必要な時代になってきていると考える。

（５）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）

技術的な動向としては、サイバー攻撃自体をいかに入り口で検知するかという技術として、アプリケーションレイヤでの高度なファイアウォールや仮想実行するサンドボックスタイプのツールの開発で各社しのぎを削る。ホワイトリスト方式でマルウエアを実行させないツールの開発も、組込み系での用途を視野に進んでいる。ますます巧妙化するマルウエアの挙動解析研究を通して、システムでの不審な動きを検知する技術の研究開発も続いている。標的型サイバー攻撃間の相関分析から、攻撃者像の特定などの研究開発も重要となっている。更に、ネットワークの仮想化技術（SDN: Software Defined Network）のセキュリティー対策への活用の研究が期待されている。

運用管理面での動向としては、攻撃者に対して、業界や集団で対抗する手段の一つとして、攻撃情報やインシデント情報の組織間での情報共有の重要性が主張されている。組織の事業上の機密や個人情報の取り扱いの壁があるが、そこを解決するスキームが各国や業界分野ごとで取り組まれている。また、その情報を共有・交換するためのデータ形式やフレームワーク（STIX、CyBox など）の提案や議論も進んでいる。[9)]

国の施策として重要インフラシステムの情報セキュリティー向上を図ろうとする動きも一部では進んでいる。米国では、国家の安全保障、経済活動維持等の一環として重要インフラシステムのサイバーセキュリティー向上を目的に、2013 年 2 月 12 日に大統領令（Executive Order）第 13636 号「Improving Critical Infrastructure Cybersecurity（重要インフラのサイバーセキュリティーの向上)」を発布し、2014 年 2 月 12 日に NIST より「Framework for Improving Critical Infrastructure Cybersecurity」の第一版が公開され、各重要インフラ業界に、このフレームワークに沿ったセキュリティー対策のレビューや業界ガイドラインを作ることを提言している。[10)]

（６）キーワード

脆弱性、サイバーセキュリティー、サイバー攻撃、標的型攻撃、情報家電、IoT、IoE、組込み系、制御システム、重要インフラ

（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	○	↗	認証技術や検知技術を進めている
	応用研究・開発	◎	↗	業界や国研で分野を特定して進めている
	産業化	◎	↗	事業で先行している分野では、セキュリティーの必要性を業界団体内で議論を進めている。セキュリティー評価認証制度の確立や普及で先行している
米国	基礎研究	◎	↗	検知技術や防御技術、脅威情報流通技術など、先行的にすすめている
	応用研究・開発	◎	↗	NISTや業界団体を中心に、基準やガイドを策定して公開している。国家施策として、取り組みをけん引している
	産業化	◎	↗	先端的なセキュリティーツールの製品投入や、調達要件となる評価認証などで先行している。スマートグリッド事業などでも先陣を切っている
欧州	基礎研究	○	↗	カードやチップなど、特定分野で頭角を現している
	応用研究・開発	◎	↗	業界のガイドや、国際標準化委員会で活躍がみられる
	産業化	◎	↗	カードや、自動車やスマートグリッド分野などで、戦略的に進めている
中国	基礎研究	△	→	表立って、基礎研究は見えてこない
	応用研究・開発	○	↗	ウイルス検知やフィルタリング技術などを実施しているレベルで、先行製品はほとんど出てきていない
	産業化	△	→	制御や重要インフラで、情報収集を進めているレベルで、国際的な発信はほとんど確認できない
韓国	基礎研究	○	→	検知技術を進めている
	応用研究・開発	○	→	一部のセキュリティー分野で先行的な製品が出されているが、市場を獲得するにはいずれも至っていない
	産業化	△	→	余りセキュリティーを考慮されていない情報家電製品などが市場投入されており、産業界のセキュリティーへの取り組みはみえていない

（註 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
産業化フェーズ ：量産技術・製品展開力のレベル

（註 2）現状
※我が国の現状を基準にした相対評価ではなく、絶対評価である。
◎：他国に比べて顕著な活動・成果が見えている、 ○：ある程度の活動・成果が見えている、
△：他国に比べて顕著な活動・成果が見えていない、×：特筆すべき活動・成果が見えていない

（註 3）トレンド
↗ ：上昇傾向、 →：現状維持、 ↘：下降傾向

（８）引用資料

1）制御システムの情報セキュリティに関する調査（2012 年度）
http://www.ipa.go.jp/security/fy24/reports/ics_sec/ics_report.pdf

2）ISCI：ISA Security Compliance Institute（米国の ISA セキュリティー適合性協会）
http://www.isasecure.org/

3) WIB：http://www.wib.nl/
4) CSSC（制御システムセキュリティセンター）：http://www.css-center.or.jp/
5) JIPDEC（日本情報経済社会推進協会）：http://www.jipdec.or.jp/
6) 医療機器における情報セキュリティに関する調査（2013 年度）
http://www.ipa.go.jp/files/000038223.pdf
7) 自動車の情報セキュリティ動向に関する調査 （2012 年度）
http://www.ipa.go.jp/files/000027274.pdf
8) 情報家電におけるセキュリティ対策 検討報告書（2010 年度）
http://www.ipa.go.jp/files/000014114.pdf
9) STIX、CyBox： http://stix.mitre.org/
10) Framework for Improving Critical Infrastructure Cybersecurity：
http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

３.13.４　認証・ＩＤ連携技術

（１）研究開発領域名

認証・ＩＤ連携技術

（２）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。また、インターネット上では、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（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。

（３）研究開発領域の詳細な説明と国内外の動向

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、漏洩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、本人が保有する様々な属性情報（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 の最新版では、標準認証方式としても実装されている。一方、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。

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 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のにあたって、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。

（４）科学技術的・政策的課題

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」である。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。

（５）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。執筆時点（2014 年 12 月）で 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洩のリスクがある。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 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)]。

（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

（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。 ・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 ・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[10)]。
	産業化	○	↗	・認証分野：ATMでの指紋認証・静脈認証[11)] 等をはじめとして、先端認証技術の実社会への適用が進んでいる。 ・ID連携分野：米国が中心となって標準化された技術の適用によるネットサービスが提供されている。日本独自の仕様による産業化はほとんど見受けられない。
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。
	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。 ・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。
	産業化	◎	↗	・認証分野：官民の重要施設や安全保障対策を優先して、応用研究・開発を行った技術や製品を積極的に導入している。 ・認証分野：民間のネットサービスにおいても、生体認証だけでなくリスクベース認証等も導入のスピードが非常に速い。 ・ID連携分野：ネット企業が最新の技術を非常なスピードで実サービスに実装・提供している。他国の追随を許さない。
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。 ・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[12)]。 ・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[13)]。
	産業化	○	→	・認証分野：EU諸国の電子政府進展に伴い、ICカード等を中心とした社会生活における活用は広範囲に広がっている。 ・ID連携分野：EU諸国同士のID連携によるサービスが提供されている。主に社会生活を補助するEU諸国を通しての情報提供等が特徴と思われる[14)]。
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。 ・中国に関しては軍需、サイバー攻撃の両面から調査が必要。
	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。 ・中国に関しては軍需、サイバー攻撃の両面から調査が必要。
	産業化	△	→	・特筆すべき顕著な産業化が見受けられない。 ・中国に関しては軍需、サイバー攻撃の両面から調査が必要。

（註 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
産業化フェーズ ：量産技術・製品展開力のレベル
（註 2）現状
※我が国の現状を基準にした相対評価ではなく、絶対評価である。
◎：他国に比べて顕著な活動・成果が見えている、 ○：ある程度の活動・成果が見えている、
△：他国に比べて顕著な活動・成果が見えていない、×：特筆すべき活動・成果が見えていない
（註 3）トレンド
↗ ：上昇傾向、 →：現状維持、 ↘：下降傾向

（８）引用資料

1) OASIS Security Services (SAML) TC
https://www.oasis-open.org/committees/security/
2) OpenID http://openid.net/developers/specs/
3) OAuth http://tools.ietf.org/html/rfc6749
4) XACML https://www.oasis-open.org/committees/xacml/
5) FIDO Alliance https://fidoalliance.org/
6) ID 連携トラストフレームワーク
http://www.meti.go.jp/policy/it_policy/id_renkei/
7) 社会保障・税番号制度 http://www.cas.go.jp/jp/seisaku/bangoseido/
8) 学術認証フェデレーション https://www.gakunin.jp/
9) 法人向け IDaaS http://cloudblog.kddi.com/tag/idaas/?v=block
10) 医療健康共通基盤
http://www8.cao.go.jp/cstp/tyousakai/innovation/ict/6kai/siryo2-3.pdf
11) 静脈認証技術
http://itpro.nikkeibp.co.jp/article/Active/20131128/521244/?ST=activesmart
12) Trust Services and eID
http://ec.europa.eu/digital-agenda/en/trust-services-and-eid
13) Trusted Architecture for Securely Shared Services
http://vds1628.sivit.org/tas3/
14) CLARIN http://www.clarin.eu/

3.13.5　サイバー攻撃の検知・防御次世代技術

（1）研究開発領域名

サイバー攻撃の検知・防御次世代技術

（2）研究開発領域の簡潔な説明

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

（3）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るため、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。

米国の 2015 年大統領予算教書[1)]によると、研究開発全体に関する年間予算は約 1350 億ドルであり、国防総省、エネルギー省、国立科学財団、商務省、国土安全保障省等の予算概要の中でセキュリティーあるいはサイバーセキュリティーに関する言及がある。それに加え「OGSI: Opportunity、 Growth and Security Initiative」と呼ばれる 560 億ドルの追加予算案が盛り込まれているなど、セキュリティー分野への重点投資が進められている。

日本の情報セキュリティ政策会議が 2014 年 7 月に公表した情報セキュリティ研究開発戦略（改定版）[2)]よると、米国の情報セキュリティー研究開発予算は大幅な増加傾向にある一方、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全体としては減少基調にあり、情報セキュリティー研究開発予算の GDP 比率は、2007 年度においては約 1.2 倍、2014 年度では約 12 倍と拡大している。

欧州では EU の FP7（第 7 次研究枠組み計画）の後継として、2014 年 1 月より Horizon 2020 [3)]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 7 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 [4)]。

サイバー攻撃の検知・防御次世代技術の研究課題としては下記が挙げられる。

標的型攻撃対策技術：

特定組織をターゲットとした長期に亘る執拗な攻撃であり、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。したがって、標的型攻撃対策技術として、組織内部の観測・分析・検知技術（内部対策）の確立が重要となっている。さらに、組織内のログマネジメント技術や、インシデント発生後のフォレンジック技術の高度化も必要となっている。

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。また、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 カメラなどがマルウエア感染する事例も多くみられる。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重要となっている。また、P2P 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・分析技術も重要となっている。さらに、組み込み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も課題となっている。

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っている。

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となっている。2013 年初頭から DDoS ツールやボットネットを利用した従来型の DDoS 攻撃に加え、DNS や NTP 等による通信の増幅を悪用したリフレクター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、リフレクター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重要となっている。

マルウエア対策技術：

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って、シグネチャベースのマルウエア検知手法の効果が低下している [5]。マルウエア対策技術として、サンドボックス解析技術の高度化や、カーネルモードで動作するマルウエアの解析技術、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求められている。また、組み込み機器やモバイル機器に感染するマルウエアの収集・解析技術の確立も重要となっている。

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ー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、トップマネージメント層を含めたセキュリティーアウェ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跨いで行われる。したがって、サイバー攻撃対策には国際的なサイバー攻撃情報の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、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（そのための国際標準化）、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。

（４）科学技術的・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、わが国においては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、前述の通り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）が受け持っているが、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。

（５）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）

・海外のセキュリティー関連予算の動向は前述の通り。
・国内では 2014 年 11 月にサイバーセキュリティ基本法が成立。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推進について定められている。
・2020 年の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。

（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

（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、企業とも増加傾向にある。一方、著名な国際会議での発表件数は多くはないものの、RAID 2013ではNTTからの投稿が複数件採録される等、国際的な成果も伸びつつある。 ・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）では、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）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。
	産業化	△	↗	・国産のセキュリティー製品は非常に少なく、大部分を海外ベンダに依存している。大手企業の多くも、海外製品のSI業に徹しており、自社製品が普及している例は少ない。 ・その中でもFFRI社のアンチウイルス製品（Yarai）等、国産製品の普及が徐々に進んでいる事例が出て来ている。 ・情報通信研究機構が開発した対サイバー攻撃アラートシステムDAEDALUSは、クルウィット社により商用サービス化（SiteVisor）される等、公的機関の研究開発が産業化される事例も出て来ている。
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。
	産業化	◎	→	・Palo Alto Networks（ファイアウォール）、Sourcefire（IDS）、FireEye（サンドボックス）等のセキュリティー企業による製品や、CiscoやJUNIPER NETWORKS等のネットワーク機器ベンダによる製品等、セキュリティー市場における支配的立場にある。 ・航空機製造で有名なBoeing社は収益の4割を防衛事業で得ており、その一翼としてCyber Engagement Centerを立ち上げ、サイバーセキュリティーサービスを展開している。

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を上げている。 ・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伺える。
	応用研究・開発	○	↗	・FP7の後継のHorizon 2020で、セキュリティーは7つの社会的課題の1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ACDC（Advanced Cyber Defense Center）を設立。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）で構成されており、応用研究から実運用まで情報共有が進んでいる。
	産業化	○	→	・Kaspersky（ロシア）、F-Secure（フィンランド）、Sophos（イギリス）、Panda Security（スペイン）等、アンチウイルスやセキュリティー製品で国際的に高いシェアを有している。
中国	基礎研究	△	↗	・中国国内の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。
	産業化	△	↗	・金山毒霸、瑞星殺毒軟件、江民瑞星殺毒軟件等のアンチウイルスソフトの国内シェアが高いが、国際的な普及には至っていない。
韓国	基礎研究	○	↗	・KAISTやPOSTECH等の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している。 ・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。
	産業化	○	↗	・Ahnlabをはじめ大小の情報セキュリティー関連企業が数百社存在し、国産のセキュリティー技術の研究開発および産業化を行っている。

（８）引用資料

1) The White House, “FISCAL YEAR 2015 BUDGET OF THE U.S. GOVERN-MENT,” http://www.whitehouse.gov/sites/default/files/omb/budget/fy2015/assets/budget.pdf
2) 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
3) European Commission, “Horizon 2020,” http://ec.europa.eu/programmes/horizon2020/
4) European Commission, “Factsheet: Horizon 2020 budget,” http://ec.europa.eu/research/horizon2020/pdf/press/fact_sheet_on_horizon2020_budget.pdf
5) The Guardian, “Antivirus software is dead, says security expert at Symantec,” http://www.theguardian.com/technology/2014/may/06/antivirus-software-fails-catch-attacks-security-expert-symantec

３.13.６　プライバシー情報の保護と利活用

（１）研究開発領域名

プライバシー情報の保護と利活用

（２）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。大きく分類すると、(1) 個人を識別不能な様にデータベースを匿名化して公開する技術(Privacy-Preserving Data Publishing)、(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の技術 (Secure Multiparty Computation)、(3) 分散されたサーバーに格納されたデータベースを暗号化してデータマイニングを実施する技術(Privacy-Preserving Data Mining)、(4) 抽出された知識からプライベート情報が漏洩しない様に精度を落としたりノイズを加えたりする技術（差分プライバシーなど）がある。

（３）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。また、Facebook では一日 30 億回の「いいね」がクリックされ、Twitter のツィートは日に 4 億を超えるという。これらの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。漏洩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。

現行の個人情報保護法は、2003 年に制定されたものであり、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 年の法改正を目標として、政府の IT 総合戦略本部に「パーソナルデータに関する検討会」が組織され、ビッグデータを活用するためのルール作りが進められた。2014 年の 6 月に発表された大綱では、個人情報の監視や検査権限を有する第三者機関を設けることを条件として、利用者の同意を得なくても別の目的に利用できるようにする道筋が示された。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。欧州委員会は、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 データ保護規制を 2012 年に提案し、2015 年の成立を目指している。

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、アクセスの方法は様々である。個人を識別しようとする攻撃者にも様々なタイプがあり、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。更に、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) 出力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)[5]の概念を初めて提唱し、その後の様々なアルゴリズムの研究が行われた。Sweeney による定式化[1]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)[2]、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 [3]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、今後はそれらを様々なビッグデータに適用する際に生じる様々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(英)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 Social Network 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。

(2) 秘匿計算技術

秘匿計算、あるいは秘匿回路計算（SFE: Secure Function Evaluation)とは、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 ビットも漏洩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 Turning 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 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。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、暗号ではなく、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

プライバシー保護データマイニング (Privacy-Preserving Data Mining, PPDM)は、水平または垂直に分割されたデータセットを保有する複数の組織が、それぞれのデータを漏らすことなく協力し、各種のデータマイニングを実行する技術である。加法準同型を満たす公開鍵暗号などを用いて、それぞれのデータを暗号化して送りあい、暗号化したまま内積計算などを繰り返すことで、決定木学習や相関ルールなどのデータマイニングされた結果だけを共有する。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最も有力な技術であるといえよう。

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様々な種類があるので、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[25]、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" [20]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[27]や(2)で述べた秘匿計算 SFE がある。条件を満たす準同型性暗号として、Paillier 暗号[26]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[25]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[28]が代表例であり、Camenisch らによって更なる効率化[29]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[21]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、様々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[22]。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[23]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[24]。

(4) 出力プライバシー

データマイニングされた知識から漏洩するプライバシー情報を秘匿するために、マイニング出力の結果に対して必要十分なだけのノイズを追加することが研究されている。Dwark によって提唱された差分プライバシー (Differential Privacy)は、加えるべきノイズの確率分布とその大きさを決める技術である。提供されるプライバシーの度合いを理論的に保障している点で多くの注目を集めている。

［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紐づけて、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、様々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 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。

・漏洩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洩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。

・漏洩した情報を失効させる仕組み
やむなく漏洩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元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。

（４）科学技術的・政策的課題

2015 年度には我が国の個人情報保護法の改定を計画している。しかしながら、そこで検討されているのは、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。

（５）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内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 [33)]
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 [34)]
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、産業総合研究所による共同プロジェクト。

（６）キーワード

匿名化、仮名化、集合匿名化、k-匿名性、l-多様性、 マルチパーティー計算、Gabbled Circuit、 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、ラプラスノイズ

（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。
	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。
	産業化	×	↘	・企業におけるプライバシー技術開発はそれほど盛んではない。
米国	基礎研究	○	→	・多くの学術論文が発表されている。差分プライバシーやビッグデータに対する試みも多い。
	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。
	産業化	△	→	・調査不十分。プライバシー保護を目的としたベンチャーはまだ盛んではない。
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。
	産業化	○	↗	・Sharemindなどの商用ベースのプロジェクトの登場。高い技術力、強い法整備、大きな市場などがかみ合ってきている。

（註 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
産業化フェーズ ：量産技術・製品展開力のレベル

（註 2）現状
※我が国の現状を基準にした相対評価ではなく、絶対評価である。
◎：他国に比べて顕著な活動・成果が見えている、 ○：ある程度の活動・成果が見えている、
△：他国に比べて顕著な活動・成果が見えていない、×：特筆すべき活動・成果が見えていない

（註 3）トレンド
↗ ：上昇傾向、 →：現状維持、 ↘：下降傾向

（８）引用資料

1) LATANYA SWEENEY, Int. J. Unc. Fuzz. Knowl. Based Syst., 10, 557 (2002)
2) Ashwin Machanavajjhala, Daniel Kifer, Johannes Gehrke, and Muthuramakrishnan Venkitasubramaniam. 2007. L-diversity: Privacy beyond k-anonymity. ACM Trans. Knowl. Discov. Data 1, 1, Article 3 (March 2007).
3) Kristen LeFevre, David J. DeWitt, and Raghu Ramakrishnan. 2005. Incognito: efficient full-domain K-anonymity. In Proceedings of the 2005 ACM SIGMOD international conference on

Management of data (SIGMOD '05). ACM, New York, NY, USA, 49-60.

4) Samarati, P., "Protecting respondents identities in microdata release," Knowledge and Data Engineering, IEEE Transactions on , vol.13, no.6, pp.1010,1027, Nov/Dec 2001
5) Chao Yao, X. Sean Wang, and Sushil Jajodia. 2005. Checking for k-anonymity violation by views. In Proceedings of the 31st international conference on Very large data bases (VLDB '05). VLDB Endowment 910-921.
6) Vanessa Ayala-Rivera, Patrick McDonagh, Thomas Cerqueus, Liam Murphy, A Systematic Comparison and Evaluation of k-Anonymization Algorithms for Practitioners, Transactions on Data Privacy 7:3 (2014) 337 – 370.
7) Xiaokui Xiao and Yufei Tao. 2006. Anatomy: simple and effective privacy preservation. In Proceedings of the 32nd international conference on Very large data bases (VLDB '06), Umeshwar Dayal, Khu-Yong Whang, David Lomet, Gustavo Alonso, Guy Lohman, Martin Kersten, Sang K. Cha, and Young-Kuk Kim (Eds.). VLDB Endowment 139-150.
8) UTD Anonymization Toolbox (http://cs.utdallas.edu/dspl/toolbox/)
9) Giorgos Poulis, Spiros Skiadopoulos, Grigorios Loukides, Aris Gkoulalas-Divanis, Apriori-based algorithms for km-anonymizing trajectory data, Transactions on Data Privacy 7:2 (2014) 165 – 194.
10) Chongjing Sun, Philip S Yu, Xiangnan Kong, Yan Fu, Privacy Preserving Social Network Publication Against Mutual Friend Attacks, Transactions on Data Privacy 7:2 (2014) 71 – 97.
11) Andrew C. Yao. How to generate and exchange secrets. In Proc. of the 27th IEEE Symposium on Foundations of Computer Science, Toronto, Canada, pages 162-167. IEEE Computer Society, 1986.
12) Dahlia Malkhi, Noam Nisan, Benny Pinkas, and Yaron Sella. Fairplay - a secure two-party computation system. In In USENIX Security Symposium, pages 287-302, 2004.
13) Y. Huang, D. Evans, J. Katz, and L. Malka. Faster secure two-party computation using garbled circuits. In Proceedings of the USENIX Security Symposium, 2011.
14) B. Kreuter, a. shelat, and C. Shen. Billion-gate secure computation with malicious adversaries. In 22nd USENIX Security Symposium USENIX Association, Proceedings of the USENIX Security Symposium, 2012.
15) D Bogdanov, S Laur, J Willemson, Sharemind: A framework for fast privacy-preserving computations, Computer Security-ESORICS 2008, 192-206.
16) Sharemind プロジェクト (https://sharemind.cyber.ee/)
17) 濱田 浩気, 他, 実用的な速度で統計分析が可能な秘密計算システム MEVAL, 3C2-1, 情報処理学会, コンピュータセキュリティシンポジウム CSS 2013.
18) Lindell, Y., Pinkas, B., Privacy Preserving Data Mining Advances in Cryptology -, CRYPTO 2000 Lecture Notes in Computer Science 1880, Springer, pp. 36-54, 2000.
19) Rakesh Agrawal and Ramakrishnan Srikant. 2000. Privacy-preserving data mining. In Proceedings of the 2000 ACM SIGMOD international conference on Management of data (SIGMOD '00). ACM, New York, NY, USA, 439-450.
20) C.C. Aggarwal and P.S. Yu. A General Survey of Privacy-Preserving Data Mining, Models and

Algorithms. Privacy-preserving data mining, pages 11–52, 2008.

21) Hiroaki Kikuchi, Jun Sakuma, Bloom Filter Bootstrap: Privacy-Preserving Estimation of the Size of an Intersection. JIP 22(2): 388-400 (2014).

22) Boneh, D., Crescenzo, G.D., Ostrovsky, R. and Persiano, G., “Public key encryption with keyword search”, EUROCRYPT 2004, LNCS, vol.3027, pp. 506-522 (2004).

23) Boneh, D. and Waters, B., “Conjunctive, subset, and range queries on encrypted data”, TCC 2007, LNCS, vol.4392, pp. 535-554 (2007).

24) 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, pp. 2067 - 2074, 2013.

25) Vaidya, J. and C. Clifton, “Privacy preserving association rule mining in vertically partitioned data”, The Eighth ACM SIGKDD Intl. Conf. on Knowledge Discovery and Data Mining, SIGKDD, ACM Press, Edmonton, Canada, pp. 639-644, 2002.

26) Paillier, P.: Public-key cryptosystems based on composite degree residuosity classes, IN ADVANCES IN CRYPTOLOGY – EUROCRYPT 1999, Springer-Verlag, pp. 223–238 (1999).

27) Goethals, B., Laur, S., Lipmaa, H. and Mielikainen, T.: On private scalar product computation for privacy-preserving data mining, Proceedings of the 7th Annual International Conference in Information Security and Cryptology, Springer-Verlag, pp. 104–120 (2004).

28) Freedman, M. J., Nissim, K. and Pinkas, B.: Efficient private matching and set intersection, Advances in Cryptology–EUROCRYPT, Springer-Verlag, pp. 1–19 (2004).

29) Camenisch, J. and Zaverucha, G.: Private intersection of certified sets, Financial Cryptography and Data Security, pp. 108–127 (2009).

30) Cynthia Dwork. Differential privacy. In ICALP, pages 1–12. Springer, 2006.

31) https://www.risec.aist.go.jp/project/dbscoop-ja.html

32) http://css.csail.mit.edu/cryptdb/

33) http://cs.utdallas.edu/dspl/cgi-bin/toolbox/

34) https://www.risec.aist.go.jp/project/dbscoop-ja.html

35) http://www.jst.go.jp/kisoken/crest/project/45/45_02.html

3.13.7　デジタル・フォレンジック技術

（1）研究開発領域名

デジタル・フォレンジック

（2）研究開発領域の簡潔な説明

デジタル・フォレンジック（Digital Forensics）とは、情報セキュリティー上の事故や不正行為・犯罪行為（これらをインシデントと呼ぶ）への対応、および情報システム上での人の行為に関する法的紛争・訴訟時に行われる電磁的記録の証拠保全および調査・分析、電磁的記録の改ざん・毀損等についての分析、情報収集を行う技術の総称である。狭義にはインシデントの発生後や訴訟時の対応に使われる技術を指すが、より広義には平時の情報システム運用時の各種記録（ログ）の確実な保管等の予防的技術や、不正行為等の発見のための電磁的記録分析技術等も含めることが多い。さらに近年では、画像や文書、電子メールの分析の自動化など、より広い意味でのセキュリティー対応のための電磁的記録の処理技術も含む概念と捉えられている。

（3）研究開発領域の詳細な説明と国内外の動向

フォレンジック（Forensics）とは本来、法科学などと訳される語であり、科学的な知見を犯罪捜査や法廷の場における法的紛争の解決に役立てることを目的に発達した研究領域を指す。我が国では法医学や法化学、鑑識学などが良く知られている。近年では人々の生活や産業活動、経済活動が情報通信技術に依拠するようになったため、犯罪捜査や法的紛争の解決においても電磁的記録の収集、証拠保全と調査分析が不可欠となっており、デジタル・フォレンジックはそのような社会的要請に呼応する形で発達してきた。最近ではカタカナ表記のフォレンジックがデジタル・フォレンジックを指す例も多い。

デジタル・フォレンジックは当初、情報通信技術の発達が早く、かつ訴訟や法的紛争の多い米国で発達してきた。米国では、民事訴訟において相手方に証言や証拠の提出を求めることができる「ディスカバリー」と呼ばれる制度があり、請求された側は連邦民事訴訟規則に沿って余さず証拠を開示したことを示すことが求められる。この証拠に電磁的記録が該当することが増加するとともに、訴訟対応のためのデジタル・フォレンジック技術や製品、そして関連事業が拡大した。また、特に企業間の訴訟においてはディスカバリーの過程で文書ファイルをはじめとする膨大な電磁的記録を効率的に分析することが求められるため、関連する技術開発が進んでいる。さらに、サイバー犯罪の高度化に伴い、不正アクセスやマルウエアの供用による犯罪が急速に増加しており、これらの犯罪行為の早期検出と対応、追跡・分析そして捜査の技術の研究開発が盛んである。

我が国では、2000 年に警察庁に専門の組織が置かれるなどサイバー犯罪への対応力が強化されてきたことに伴い、デジタル・フォレンジックへの需要が高まり、民間部門における研究開発も進んできた。2004 年頃から頻発した企業からの個人情報持ち出し事件、およびマルウエアによる P2P ファイル共有システムへの情報流出事件は、内部不正行為、セキュリティーポリシー等への違反行為の調査に必要な技術の研究開発を盛んにした。近年では、マルウエアを用いた官公庁や企業に向けた高度標的型サイバー攻撃が急速に増加しているため、これらの組織における通信ログやファイアウォール・IDS (Intrusion Detection System

不正アクセス監視システム / 侵入検知システム)のログの相関分析から迅速に不正アクセス行為や内部に侵入したマルウエアの活動を検出する技術の研究開発が進み、事業展開も進んでいる。さらに、発見されたマルウエアの解析、検出された犯罪行為・不正行為の詳細の分析、事故原因を調査分析するための技術の需要が大きく、研究開発が盛んである。

（４）科学技術的・政策的課題

デジタル・フォレンジックが対象とする電磁的記録は、文書や写真、音声記録のように従来物理媒体として生成、流通されていたものがデジタルデータとして流通するようになったものと、情報通信機器のオペレーティングシステムやアプリケーション等が生成する動作記録（ログ）や通信記録などの情報通信機器固有のもの、そしてプログラムに大別できる。これらの情報は消去や改ざん、偽造、暗号化などによる隠蔽が容易であること、情報量が膨大になり分析が困難であること、インターネットの匿名性により行為者の追跡が困難になる場合が多いこと、プログラムに関しては特にバイナリ形式において静的な動作解析が困難であることが共通かつ本質的な技術課題である。

デジタル・フォレンジックでは企業文化、市民感情および社会制度や法制度が実装の障害になる例も多い。例えば情報システムにおいてはインシデントに備えて通信内容や利用記録、操作履歴を記録し保存しておくことが望ましいが、記録は通信の秘密やプライバシーを含むことから厳重な管理を要すると考えられるため、一般化していない。通信記録等の保存を制度的に義務付ける場合には、保存期間や安全管理に関して電気通信事業法や個人情報保護法との関係整理が必要である。また、デジタル・フォレンジックにはインシデントの経緯を詳細に分析し公表することにより原因を明らかにし、再発防止策を社会に共有させる効果があるが、現時点では情報システムのインシデントの際に原因を調査した結果を進んで公表する企業や組織は一部にとどまっている。このインシデント事例の公表が進まず事例の収集が十分行えないことは、デジタル・フォレンジックの研究開発の上での障害ともなっている。

サイバー犯罪は国境を跨いで行われる場合が多いことや、企業活動の国際化によって法的紛争も海外の裁判所で行われることも増加化しているため、捜査や裁判において証拠となる電磁的記録の取得プロセスや分析技術などについて国際的な共通認識の確立も重要である。

（５）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）

以下、個別の技術要素に関する動向や課題、近年のトピックについて述べる。

① 電磁的記録の消去や改ざん、偽造の検出や分析技術

削除ファイルの復元はかつてデジタル・フォレンジックの中心的技術だったが、情報漏洩対策を目的とした完全消去技術の普及や、ハードディスクを代替しつつある SSD における Trim 技術（消去してもよい領域をあらかじめ通知することによって書き込み速度の低下を抑える技術)の普及、記憶媒体に直接アクセスできないクラウドサービスの普及で困難になりつつあり、対応技術の研究開発が望まれる。写真や動画、音声データの自然な改ざんは市販のツールで容易に行えるようになったため不正行為にも使われる例が増えており、信号処理などの技術を駆使して改ざんの痕跡を検出する技術の研究開発も進んでいる。

② インターネットの追跡困難性、通信の暗号化および匿名性に対する対策技術
IPv4 における CGN (キャリアグレード NAT)の普及、IPv6 における匿名 IP アドレス導入、Tor や Freenet などの匿名強化技術の普及により、今後 IP アドレスによる通信元追跡は不可能になるため、その対応技術の研究開発が求められている。また、米国 NSA による国際的な通信傍受活動が明らかになって以来急速に各種通信が暗号化される傾向が強まり、ウイルス対策やフィルタリング、IDS をはじめとする通信監視の障害になる例が増えているため、対応するための技術が求められている。しかしこれらの技術は本質的に対応が困難であり、暗号化・匿名化された通信を検出して状況に応じて禁止するなどシステム的な対策技術の提案が多い。さらに、我が国では通信の秘密を遵守する立場から法制度との関係の整理が必要である。

③ マルウエア対策の高度化とマルウエア分析の自動化
企業や組織に対するサイバー攻撃では、ウイルス対策ソフトウエアでは検知できないマルウエアが中心的役割を果たしている。このため、マルウエアの挙動、特に通信に着目した検出手法や、難読化されたマルウエアの分析技術の高度化が求められる。前者に関しては、企業情報システム内の機器からの情報セキュリティーに関する警告や通信ログなどを一元管理し分析することによってインシデント検出を行うセキュリティー情報イベント管理（SIEM）が普及しているが、そのインシデント検出の自動化、高精度化に関する研究開発が進んでいる。マルウエア分析については VM を活用した動的解析の効率化・自動化技術の開発と標的型攻撃対応ファイアウォールとしての製品化も進んでいるが、攻撃側の進化により検出できない例も少なくないため引き続き開発が必要である。

④ ライブフォレンジックとファストフォレンジック
フォレンジック関連事業者からは、不正行為に使われたアプリケーションやマルウエアがまだ動作中に主記憶を含め電磁的証拠を収集して分析するライブフォレンジックや、さまざまな時間的制約を受ける環境内でできるだけ迅速にインシデント対応を行うファストフォレンジックの必要性が高まっており、関連技術の開発が求められている。前者に関しては、機器で動作中のアプリケーションが未知である場合にいかに迅速に主記憶上のデータの意味を解析するかが研究課題であり、暗号鍵の自動検索などについての研究がある。後者は、従来記憶媒体を完全に複製してからその内容の解析を行うことが一般的であったのに対し、記憶媒体の大容量化に伴いそれが困難となってきたことから、必要最小限の複製と解析で済ませるための研究が求められている。

⑤ 大規模データへの対応のための機械学習などの応用
一般に情報システム内における電磁的記録の量は膨大になっており、全てを人力によって分析することは現実的ではない。そこで詳細な分析が必要でない部分をあらかじめ選り分けるため、機械学習など人工知能分野の研究成果を応用する研究が盛んである。特に、大量の文書ファイルに対し、インシデントとの関係の有無を機械学習技術を利用して選り分ける予測コード付技術（Predictive Coding）は実用化され、米国においては民事裁判でディスカバリーにおける証拠の分析を大幅に効率化した。東アジア圏の言語に対しても同技術が応用され、日本企業による事業化がなされている。この他、前述の SIEM におけるインシデント分析自動化も機械学習の応用例が多い。ま

た、監視カメラの映像や大量の写真画像などからインシデントに関わるものを検出する際には、顔認識や物体認識などのロボットビジョン関連技術の応用研究が行われており、一部は製品化されている。さらに、近年ビッグデータ関連研究によって盛んになった大規模データに対する傾向分析技術も応用されている。

⑥ 新たなデバイスやクラウドへの対応

タブレットやスマートフォンの利用が広がってきたこと、制御機器、パソコン周辺機器のコントローラなどがマルウエアに感染する例などが発見されたことから、これらにおける電磁的記録もインシデント対応において収集、分析が必要となり、関連技術の研究開発が盛んに行われるようになった。さらに、クラウドサービスの普及への対応の研究も盛んである。IaaS 型クラウドサービスに対しては仮想計算機に直接アクセスできる場合が多いため、従来の電磁的証拠の収集技術を生かすことができるが、SaaS 型クラウドサービスでは一般には困難であるため、クラウド事業者にどのような電磁的記録の証拠保全を求め、その真正性をどのように確保するかのフレームワークに対する研究提案が多い。

⑦ デジタル・フォレンジックの人材育成

デジタル・フォレンジックは法曹関係者や実務者との連携が欠かせない学際的領域であり、研究活動や産業化には技術と法律の両方に通じた人材が必要となることから、人材育成カリキュラムや両分野の相互の啓蒙活動が米国や英国を中心に多く見られる。大学や大学院修士課程における人材育成も米国、カナダ、英国、オーストラリアなどでは盛んであり、Computer Forensics Program などの名称でコースを設ける例が多い。しかしそのカリキュラムについてはまだ議論があるようで、カリキュラムそのものを扱う研究論文がいくつか見られる。

我が国では、大学におけるデジタル・フォレンジックの人材育成プログラムはそれほど盛んではないが、東京電機大学が 2014 年度から文科省「高度人材養成のための社会人学びなおし大学院プログラム」として社会人向けに科目を開講する。また、政府の支援を受けた一般の人材育成プログラムとしてはコンテスト形式を取るものがいくつかあり、総合的インシデント対応力を競う「危機管理コンテスト」（サイバー犯罪に関する白浜シンポジウム実行委員会主催）や、脆弱性検査やインシデント対応に必要な知識や技術を競う SECCON 全国大会（SECCON 実行委員会）などがある。

（6）キーワード

デジタル・フォレンジック、証拠保全、マルウエア解析、機械学習、ビッグデータ、通信の秘密、プライバシー、サイバー犯罪、サイバー刑法

（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	△	→	関連研究は行われているが分野に特化した国内研究集会がなく、セキュリティー研究やサイバー法研究、法科学研究に付随した存在という位置づけ。
	応用研究・開発	△	↗	アジア語圏向け予測コード付技術の開発、マルウエア解析技術の開発などを一部企業が先導。
	産業化	○	↗	セキュリティー監視事業、インシデント対応事業は一定の産業に。全通信を記録する企業内情報システム向け証拠保全機器や、端末管理ソリューションも国産製品が普及。ディスカバリー対応のための予測コード付技術は海外展開も行われているが、監視の自動化技術は海外に先行されている。主要地域で唯一世界的マルウエア対策ソフトウエア会社が存在しない。
米国	基礎研究	◎	→	主要な国際学会と論文誌は米国に集中しており、最も層が厚い。
	応用研究・開発	◎	↗	暗号応用技術は大学で研究が行われており、ディスカバリー対応をはじめとするシステム応用研究開発は企業が主導。
	産業化	◎	↗	ディスカバリーやシステム監査などは大きな産業に。マルウエアの動的解析技術を応用した次世代ファイアウォールやSIEM製品はほぼ独占。
欧州	基礎研究	◎	↗	大学では英国を中心に研究が盛ん。英国計算機学会が各大学にコースを提供し人材育成も行う。英国外ではドイツ、フランス、スイスなど暗号研究が盛んな地域で関連研究が行われている。 NATOがサイバー防衛の基礎研究部門をエストニアに置き、同分野の世界的中心地に。Interpolでも関連する調査研究。
	応用研究・開発	○	→	携帯電話の規格化の中心であることから関連応用研究が先行。暗号応用も強み。マルウエア関連やVPN技術などの研究開発も盛ん。
	産業化	◎	→	世界的マルウエア対策企業がドイツ、ルーマニア、スペイン、フィンランド、ロシアなどにありインシデント対応産業は盛ん。
中国	基礎研究	○	→	セキュリティー研究者の層の厚さを背景に国際学会でも活動は活発。香港大学を中心にこの分野で研究コミュニティを形成、警察とも協働。しかし分野特化した国際学会ICDFIは2013年、2014年と開催したが一旦休止に。
	応用研究・開発	○	↗	文化的背景から企業の学会研究発表は少ない。しかしハッカーコミュニティの活動が盛んで技術者の層の厚さを伺わせる。
	産業化	○	↗	政府が情報セキュリティーに関する企業への規制を急速に進めた結果、企業を中心に製品導入が進んでいる模様。国内に複数のマルウエア対策企業も持つ。
韓国	基礎研究	○	→	高麗大学や順天郷大学が専門の研究所を設置。関連国際会議でも活発に発表。しかし研究者人口規模は大きくはない。
	応用研究・開発	○	↗	情報セキュリティー産業が発達しているのを背景に研究は盛んだが、独自技術に基づくものが少ない。
	産業化	◎	↗	多くの関連企業があり、製品を展開。大規模な事故の発生を背景にインシデント対応の重要性も認知されてきている。

（８）引用資料

1）デジタル・フォレンジック事典（日科技連）
2）Digital Forensic Research Workshop（DFRWS）http://www.dfrws.org/
3）IFIP WG 11.9 Annual Conference on Digital Forensics
http://www.cis.utulsa.edu/ifip119
4）The Association of Digital Forensics, Security and Law http://www.adfsl.org/
5）デジタル・フォレンジック研究会 http://www.digitalforensic.jp
6）情報処理学会コンピュータセキュリティ研究会 http://www.iwsec.org/csec/
7）株式会社 UBIC「Predictive Coding」
http://www.ubic.co.jp/technology/predictive-coding.html
8）高麗大学校 Digital Forensic Lab http://forensic.korea.ac.kr/
9）Journal of Digital Investigation (Elvevier)
10）IEEE Trans. on Information Forensics and Security
11）Guidance Software Encase Forensics https://www.guidancesoftware.com/forensic.htm
12）AccessData E-discovery and Forensics http://accessdata.com/
13）Purdue Cyber Forensics http://cyberforensics.purdue.edu/
14）Hong Kong Legal Information Institute http://www.hklii.hk/eng/