Ⅱ－1
サイバーセキュリティの基本概念と脅威

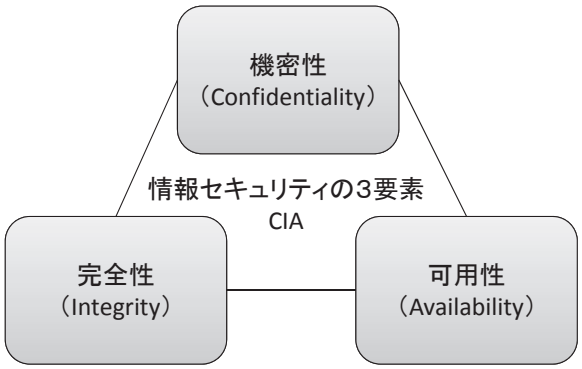
1.1　情報セキュリティの基礎

情報セキュリティとは、JIS Q 27000:2014（ISO/IEC 27000:2014）において情報の機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）を維持することと定義されている。この3つの要素の頭文字をとって情報セキュリティにおける「CIA」と略される。情報セキュリティ対策は、①組織的、②人的、③技術的、④物理的の4つの観点からの対策が、確実かつバランスよく実施される必要がある。

(1)　情報セキュリティの3要素

情報セキュリティとは、JIS Q 27000:2014（ISO/IEC 27000:2014）においては、情報の機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）を維持することと定義されている（図1参照）。なお、完全性は、Completenessにも対応させられる用語であり紛らわしいため、Integrityに対応する用語として、一貫性又はインテグリティが用いられることもある。

図1　情報セキュリティの3要素



（出典）三菱総合研究所作成。

これら3つの要素の頭文字をとって、情報セキュリティのCIAと略される。「CIA」の概念は、情報セキュリティマネジメントに関する英国規格BS7799に1998年に採用されており、それをもとに2000年に国際規格化したISO/IEC 17799:2000（現在のISO/IEC 27002:2006）、さらにこれを2002年に日本工業規格化したJIS X 5080:2002に取り入れられた。その後、ISO/IEC 17799:2005がJIS Q 27002:2006として日本工業規格化された(1)。現在、情報セキュリティマネジメントの国際規格は、ISO/IEC 27000ファミリーとして整備されており、それにあわせてJIS Q 27000ファミリーと名称を変更している。サイバー犯罪に対する国際的な対応を取り決めた「サイバー犯罪に関する条約」（平成24年条約第7号）の前文においても「コンピュータ・システム、コンピュータ・ネットワーク及びコンピュータ・データの秘密性、完全性及び利用可能性に対して向けられた行為並びにコンピュータ・システム、コンピュータ・ネットワーク及びコンピュータ・データの濫用を抑止するために、この条約が必要であることを確信し」として「CIA」の概念に言及している。

この3つの要素はそれぞれ、①機密性：情報へのアクセス（閲覧など）が許可された場合に限定されていること、②完全性：情報への操作（書込み、書換え、消去など）が許可された場合に限定されていて改ざん等がなされないこと、③可用性：許可された場合に情報へのアクセスが

必要に応じて中断することなく利用・制御できることを意味しており、これらが維持できなくなる状況や可能性をセキュリティ上の脅威と見なす。例えば、機密性への脅威としては情報漏えいやなりすまし、完全性については侵入や改ざん、可用性についてはDoS/DDoS攻撃やマルウェア感染などが挙げられる。「CIA」は3要素全てを考慮してバランスよく維持することが求められるが、各要素の重要度の大小は各組織が取り扱う情報や所有する情報システムの特性により異なる。

情報セキュリティには、「CIA」のほかに「真正性（Authenticity）」、「責任追跡性（Accountability）」、「否認防止（Non-Repudiation）」、「信頼性（Reliability）」を維持することを含める場合もある。真正性は情報システムの利用者が確実に本人であることを確認できること、責任追跡性は情報の変更履歴などを辿れること、否認防止は事象又は処置が発生した後で、否認されないように証明できること、信頼性は情報システムの動作や結果が意図どおりであることを意味する。

(2)　情報セキュリティ対策

一般に、情報セキュリティ対策は、①組織的、②人的、③技術的、④物理的の4つの観点から実施される。セキュリティを確保するためにはそれぞれの対策が確実にかつバランスよく実施される必要がある。以下にそれぞれのセキュリティ対策について説明する。

①組織的セキュリティは、組織として取り組むべき情報セキュリティの方針を定め、目的や目標を明確にし、その実現に向けて役職員それぞれの立場に応じた役割や責任を明文化し、組織的な体制や管理の枠組みの定めなどにより、情報セキュリティに組織的に取り組むことである。この中には、情報の重要度に応じた分類やラベル付け、取扱ルールの明確化なども含まれる。また、情報セキュリティに係る事案が発生した場合を想定した計画や対応を行う体制の整備、適切な情報セキュリティを実施するための予算確保等の取組を行うことなども含まれる。

②人的セキュリティは、不正行為、ヒューマンエラー等、人に起因するリスクを軽減するため、適切な人選を行い、必要に応じて機密保持等の守秘義務契約を確実に行い、定期的に教育訓練を実施して、従業員が情報セキュリティを確保しつつ業務を遂行できるようにすることである。人的セキュリティ対策の実施にあたっては、就業中だけでなく、採用時から退職後まで、従業員のライフサイクル全体において、適切な対策を実施することが重要である。例えば採用時には雇用契約、委託契約において、誓約書や同意書といった形で情報セキュリティに関する要求事項への遵守責任を持たせることも効果的な対策となる。また、人的セキュリティの効果を高めるためには自組織のみならず、委託先などサプライチェーン全体を対象とした対策を実施することが重要である。そのため業務委託先の選定基準にセキュリティの取組に関する基準を設けたり、委託先に対する教育や研修、定期的な評価等の取組も重要となる。

③技術的セキュリティは、情報システムを構成するハードウェア、ソフトウェア、データ、ネットワークに対する脅威に対して、適切な技術的対策を実施し、システム全体のCIAを維持することである。技術的セキュリティを実現するものとしては、ユーザ認証やアクセス制御、暗号化、システムの冗長化、バックアップといったものから、ウイルス検知ソフトやファイアウォール、侵入検知システム（IDS）や侵入防止システム（IPS）、メールフィルタ、Webアプリケーション・ファイアウォール（WAF）、さらにそれらの機能を統合した統合脅威管理（Unified Threat Management: UTM）製品やサービスなどが存在する。一方、攻撃者側もこれらの防御策を潜り抜ける手法を日々研究・開発していることから、防御する側には、これらの防御策を単独

で用いるのではなく、様々な製品やサービスなどを組み合わせた多層防御（Defense in Depth）が求められている[(2)]。また、システムを防御するためには、一般的に（a）不要なサービスの停止、（b）サービスを提供する範囲の制限、（c）システムの運用状態の監視、（d）ソフトウェアの安全な（最新の）バージョンへの更新、（e）ユーザアカウントの適切な管理といった5つの対策が必須である[(3)]。

最後に、④物理的セキュリティは建物や設備（コンピュータやサーバ等）に対して物理的な対策を講じることである。ネットワークを介した攻撃から情報システムを防御しても、コンピュータやネットワーク機器などを攻撃者から物理的に守ることができなければ意味がない。企業や組織内に設置しているコンピュータや機密情報が保存された記憶媒体（ハードディスクやUSBメモリなど）が外部からの侵入者によって盗難被害に遭うケースは珍しくない。そのような事態に備えて、監視カメラを設置するだけでなく、執務室やサーバルームなどへの入退室の管理を徹底する必要がある。入退室の管理には、暗証番号やICカードなどを用いた電子キーだけでなく、指紋や虹彩、血管（静脈パターン）、顔などの身体的な（主に静的な）特徴を利用するものも広く使われている[(4)]。また、情報システムにとっては自然災害も大きな脅威であり、災害対策としての耐震設備、防火設備、バックアップ施設の設置、電源・回線の保護なども重要な観点となる。

(3)　情報セキュリティ対策の機能

さらに、前述の情報セキュリティ対策にはそれぞれ、「抑止」、「予防」、「検知」、「回復」等の機能がある。

「抑止」は次に示す「予防」にも含まれる機能であり、情報セキュリティインシデントとなりうる不正行為等の発生自体を未然に防ぐことである。主に組織の内部の人間に対して教育や研修によって情報セキュリティポリシーや規定の遵守を徹底させることや、組織内のネットワークを監視することで、不正行為に対する牽制を働かせること等が該当する。

「予防」は組織、設備、情報システムなどにおける脆弱な部分に対して、対策を実施し、情報セキュリティインシデントの被害を軽減させることである。組織における情報セキュリティ体制の整備や設備、情報システムに対する不正アクセスや攻撃、事故や自然災害等による損害を防止するための物理的・技術的な対策に至るまで、その範囲は多岐にわたる。

「検知」は情報セキュリティインシデントの発生を迅速に発見し、原因究明や影響範囲の特定に必要な情報を取得・保全することである。システムやネットワークの監視、ネットワークログやサーバログの取得などの対策が該当する。情報セキュリティインシデントを迅速に発見することで影響の拡大を防ぎ、被害を最小限に抑えることができる。

「回復」は、情報セキュリティインシデントによって影響や損害を受けた情報システムやネットワークを正常な状態に復旧させることである。

このように、組織的、人的、技術的、物理的な情報セキュリティ対策と、対策の機能を適切に使い分けたり、組み合わせたりすることで、様々な脅威に対して効果的な対策を実施することができる。例えば、不正アクセス対策であれば「予防」・「検知」、内部不正行為対策であれば「抑止」・「検知」等、システムの障害対策であれば、「回復」の機能を高めることが特に重要となる。

●事例研究

■国内における情勢

日本国内では、これまで情報セキュリティを包括的に保護することを目的とした法律が存在していなかった。2000年に制定された「高度情報通信ネットワーク社会形成基本法」（いわゆる「IT基本法」。平成12年法律第144号）の第2条、第22条、第36条第2項第6号は、高度情報通信ネットワークの安全と安心について言及しており、具体的な権利や義務等を定めたものではないが、情報ネットワークを中心とするセキュリティに関する事実上の基本法としての役割を担ってきたと言える。また、個々の法規定中には、部分的に情報セキュリティを保護する機能を担うものもある。「刑法等の一部を改正する法律」（昭和62年法律第52号）によって「刑法」（明治40年法律第45号）に1987年に新設されたコンピュータ犯罪処罰規定（第161条の2、第234条の2、第259条等）を始め、「不正競争防止法」（平成5年法律第47号）の営業秘密の保護に関する規定、「不正アクセス行為の禁止等に関する法律」（いわゆる「不正アクセス禁止法」。平成11年法律第128号）、「個人情報の保護に関する法律」（いわゆる「個人情報保護法」。平成15年法律第57号）の個人データ安全管理措置義務に関する規定（第20条）なども情報セキュリティ保護機能を果たすものとして挙げることができる(5)。さらに、2011年には、「情報処理の高度化等に対処するための刑法等の一部を改正する法律」（いわゆる「サイバー刑法」。平成23年法律第74号）によって、いわゆる「コンピュータ・ウイルス作成罪」（第168条の2）等が刑法に新設されている。

こうした中、2015年1月に新たに施行された「サイバーセキュリティ基本法」（平成26年法律第104号）は、サイバーセキュリティに関する施策を策定及び実施する責務が国にあることを明確にし、行政機関などのサイバーセキュリティを確保するとともに、重要社会基盤事業者などが自主的な取組に努めることを規定している。

● 海外の状況、技術動向、制度、規制

■ ISO/IEC 27000ファミリー

ISO/IEC 27000ファミリーは情報セキュリティマネジメントシステム（ISMS）に関する国際規格である。例えば、ISO/IEC 27000は、ISMSファミリー規格の概要、ISMSファミリー規格において使用される用語等について規定した国際規格である。ISO/IEC 27001は組織がISMSを構築するための要求事項をまとめた国際規格である。また、ISO/IEC 27005は、情報セキュリティのリスクマネジメントに関するガイドラインであり、ISO/IEC TR13335（Guidelines for the Management of IT Security: GMITS）を統合し、ISO 31000（リスクマネジメント-原則及び指針）に整合させたものである。具体的にはISO/IEC 27005は資産や脅威を特定するリスク分析、リスク評価、リスク対応といったリスクマネジメントに基づいた情報セキュリティリスク管理プロセスを規定している。

(1)　「情報セキュリティマネジメントとPDCAサイクル」情報処理推進機構ウェブサイト <https://www.ipa.go.jp/security/manager/protect/pdca/standard.html>
(2)　情報処理推進機構セキュリティセンター「脅威と対策―分冊1 イントラネットを利用するための運用上のセキュリティ対策―」（大企業・中堅企業の情報システムのセキュリティ対策）2007.4, p.20. <http://www.ipa.go.jp/security/fy18/reports/contents/enterprise/1.pdf>
(3)　「システムを守るために」2006.7.28. JPCERT コーディネーションセンターウェブサイト <https://www.jpcert.or.jp/tips/2006/wr062802.html>
(4)　馬場重通「物理セキュリティと情報セキュリティの融合」『JNSA Press』19号, 2007.3, pp.9-13.
(5)　経済産業省「情報セキュリティ関連法令の要求事項集」2011.4, p.2. <http://www.meti.go.jp/policy/netsecurity/docs/secgov/2010_JohoSecurityKanrenHoreiRequirements.pdf>

1.2　情報セキュリティの脅威

1.2.1　脆弱性とその取扱い

サイバー攻撃に悪用される可能性のあるソフトウェア等の脆弱性の取扱いに関して、国内では2004年7月から経済産業省告示「ソフトウエア等脆弱性関連情報取扱基準」に基づく「情報セキュリティ早期警戒パートナーシップ」が運用されている。2014年5月に同告示が改正された。

一般的にサイバー攻撃では、攻撃対象が使用しているソフトウェアやハードウェア等のセキュリティ上の欠陥（セキュリティホール）や弱点である「脆弱性」が悪用されることが多い。特に、当該ソフトウェア等の開発者による修正が行われる前に脆弱性が悪用されてしまう、いわゆる「ゼロデイ攻撃」は基本的に防ぐことができないため深刻な脅威となっている。したがって「脆弱性関連情報」は、開発者による修正（修正プログラム「パッチ」の公開等）が完了するまで公にならないように慎重に取り扱われなければならない。

「脆弱性」とは、経済産業省告示「ソフトウエア等脆弱性関連情報取扱基準」（平成16年経済産業省告示第235号）によれば、「ソフトウエア等において、コンピュータ・ウイルス、コンピュータ・不正アクセス等の攻撃によりその機能や性能を損なう原因となり得る安全性上の問題箇所」と定義されている。ウェブアプリケーションに関しては、「ウェブサイト運営者がアクセス制御機能により保護すべき情報等に誰もがアクセスできるような、安全性が欠如している状態」が含まれる。また、「脆弱性関連情報」とは、脆弱性に関する情報であり、①脆弱性の性質及び特徴を示す情報（脆弱性情報）、②脆弱性が存在することを調べる方法（検証方法）、③脆弱性を悪用するプログラム、コマンド又はデータ及びそれらの使用方法（攻撃方法）を指す。

国内における脆弱性への対応体制として、JPCERTコーディネーションセンター（JPCERT/CC）は、1996年の設立以来、米国CERT/CCや英国国家インフラ防護センター（Centre for the Protection of National Infrastructure: CPNI）[(1)]及びフィンランドNCSC-FI（National Cyber Security Centre Finland）[(2)]と連携し、脆弱性関連情報を安全かつ適切に取り扱ってきた。その後、国内においては、2004年7月から、ソフトウェア等脆弱性関連情報取扱基準に基づき、「情報セキュリティ早期警戒パートナーシップ（以下「制度」という。）」の運用が開始され、JPCERT/CCは同制度の調整機関として、脆弱性関連情報の公表日等を当該ソフトウェア製品の開発者と調整する役割を担っている[(3)]。ソフトウェア等脆弱性関連情報取扱基準は2014年5月に改正されている。なお、脆弱性関連情報の報告受付機関としては、情報処理推進機構（IPA）が指定されている[(4)]。

同制度による脆弱性情報の取扱は、ソフトウェア製品とウェブアプリケーションで異なる。ソフトウェア製品に関する脆弱性関連情報は、JPCERT/CCが当該ソフトウェア製品の開発者と調整した上で（基本的に）修正が完了した後に、IPAとJPCERT/CCが共同で運営する脆弱性対策情報ポータルサイトJapan Vulnerability Notes（JVN）を通じて一般に公表される[(5)]。ウェブサイトの脆弱性については、IPAが届出受付だけでなく、当該ウェブサイト運営者に脆弱性関連情報を通知し、対応を促す役割も担う[(6)]。IPAでは、そのほかにも脆弱性対策に関する情報、検査手法・ツール（ファジング（用語集参照）等）、各種普及啓発資料を提供している。

このような公的機関による脆弱性情報の取扱いとは別に、ソフトウェア等のベンダでは、自

社製品の脆弱性を発見・報告した人に報奨金を支払う制度を独自に導入するケースが一般化しつつある。この報奨金制度は、Microsoft、Google、PayPal、Mozillaなどの海外企業のみならず(7)、国内ではサイボウズが実施している(8)。このような状況を踏まえ、脆弱性の発見を専門とする企業も現れるなど、脆弱性情報の売買がすでにビジネスとして成立してきている(9)。

●事例研究

■脆弱性関連情報の届出状況

「情報セキュリティ早期警戒パートナーシップ」に基づく脆弱性関連情報の届出受付開始（2004年7月8日）から2014年第3四半期末までの間に報告受付機関であるIPAに届け出られた件数は10,084件である。その内訳はソフトウェア製品に関するものが1,866件、ウェブサイトに関するものが8,218件であり、ウェブサイトに関する届出が全体の8割を超えている。また、修正を完了した件数は6,703件で、内訳はソフトウェア製品に関するものが925件、ウェブサイトに関するものが5,778件となっている。(10)

●海外の状況、技術動向、制度、規制

■国際標準（ISO/IEC 29147, 30111）

脆弱性関連情報の取扱いに関する国際的な動きとしては、ソフトウェア製品開発者の脆弱性開示に係る対応を規定する国際基準ISO/IEC 29147:2014（Vulnerability Disclosure）や製品開発者の組織内での脆弱性情報取扱手順を規定する国際基準ISO/IEC 30111:2013（Vulnerability Handling Processes）が、それぞれ国際標準化されている。これに伴い、IPA内に設置された「情報システム等の脆弱性情報の取扱いに関する研究会」は、「情報セキュリティ早期警戒パートナーシップ」のこれらの国際標準との整合性に関して調査を行い、その結果を2014年3月に「情報セキュリティ早期警戒パートナーシップにおけるグローバル化の課題と今後の方針調査報告書」として公開した(11)。これを踏まえ、IPAとJPCERT/CCは2014年5月に同パートナーシップのガイドラインを改訂し、2014年版として公開している(12)。

---

(1)　旧名称は、National Infrastructure Security Co-ordination Centre（NISCC）
(2)　旧名称は、Computer Security Incident Response Team CERT Finland（CERT-FI）
(3)　JPCERTコーディネーションセンター「脆弱性関連情報取扱いガイドライン ver.5.0」2014.5.30, p.2. <https://www.jpcert.or.jp/vh/vul-guideline2014.pdf>
(4)　「脆弱性関連情報の届出」情報処理推進機構ウェブサイト <http://www.ipa.go.jp/security/vuln/report/>
(5)　「JVNとは？」Japan Vulnerability Notesウェブサイト <https://jvn.jp/nav/jvn.html>
(6)　情報処理推進機構ほか「ウェブサイト運営者のための脆弱性対応ガイド情報セキュリティ早期警戒パートナーシップガイドライン付録6　抜粋編」2009.7, p.10. <http://www.ipa.go.jp/files/000003033.pdf>
(7)　情報処理推進機構技術本部セキュリティセンター「脆弱性対策の効果的な進め方―深刻度を評価する「CVSS」を利用した脆弱性対策について―」2013.11.22, p.7. <https://www.ipa.go.jp/files/000035701.pdf>
(8)　「サイボウズ、国内商用クラウド初の脆弱性発見コンテスト「cybozu.com Security Challenge」を開催　外部のセキュリティ専門家と協調し、サービスの品質向上を目指す」2013.9.24. サイボウズウェブサイト <http://group.cybozu.jp/news/pdf/2013/130924.pdf>
(9)　情報処理推進機構技術本部セキュリティセンター　前掲注(7)
(10)　情報処理推進機構「ソフトウェア等の脆弱性関連情報に関する届出状況［2014年第3四半期（7月～9月）］」2014.10.23. <https://www.ipa.go.jp/security/vuln/report/vuln2014q3.html>
(11)　「「情報セキュリティ早期警戒パートナーシップにおけるグローバル化の課題と今後の方針調査報告書」などを公開」2014.3.27. 情報処理推進機構ウェブサイト <https://www.ipa.go.jp/security/fy25/reports/vuln_handling/index.html>
(12)　情報処理推進機構ほか「情報セキュリティ早期警戒パートナーシップガイドライン」2014.5. <http://www.ipa.go.jp/files/000039236.pdf>

1.2.2　マルウェア

ウイルス、ワーム、トロイの木馬、バックドア、スパイウェアなど、コンピュータの利用者が意図しない有害な行為を行う不正プログラムを総称してマルウェア（悪意のコード又は悪意のソフトウェア）と呼ぶ。

マルウェア（Malware、Malicious Softwareの短縮形）は、悪意のコード又は悪意のソフトウェアと呼ばれ、利用者の同意を得ずにコンピュータ等にインストールされ（感染）、利用者が意図しない有害な行為を行うプログラムの総称である。マルウェアの代表例としては、ウイルス、ワーム、トロイの木馬等があり、ほかにもバックドア、ルートキット（攻撃者がコンピュータへの侵入や、侵入後に利用するためのツールやソフトウェアのパッケージキット）、キーロガー（キーボードへの入力を記録するソフトウェア）や、スパイウェアとしての追跡クッキーもマルウェアに含まれる(1)。また、アドウェア（広告を表示するソフトウェアやアプリケーション）も悪質な場合はマルウェアと言える。

代表的なマルウェアとして、ウイルス、ワーム、トロイの木馬、ボットに関して説明する。

ウイルスは標的となるファイルやプログラム、コンピュータに自身のコピーを複製（感染）するように設計されており、ファイルを開く、プログラムを実行する等のユーザの操作をきっかけに有害なコードが実行される。ウイルスは単にメッセージを表示するものから、コンピュータ内の個人情報を他人に転送するもの、システムを消去する悪質なものまで多様である。(2)

最近では、インターネットバンキングのウェブサイトから認証情報を窃取し、自動に不正送金を行う高度なウイルスも登場している(3)。

一方、ワームは宿主となるプログラムがなくても標的に感染し、電子メールやUSBメモリ等を介して、又は、悪意のあるウェブサイトから、ユーザがダウンロードすることによって拡散する。ウイルスと異なりユーザの操作が無くても、自己増殖することができる。ワームの多くは、標的のコンピュータに密かにバックドアを仕掛けたり、セキュリティホールを開けたりするため、ハッカー達はワームに感染したコンピュータを悪用して、ほかのコンピュータに対する攻撃等の不正行為を行うことができる。(4)

トロイの木馬は、見かけ上は正規のプログラムを装いながら、システムに侵入し、実際には既存のファイルを置き換えたり、消去したり等の有害行為を行う。ウイルスやワームと異なり、自己増殖することはない。トロイの木馬は元のプログラムの機能を阻害しないように設計されており、侵入してから時間を置いて実行されるものも多く、その検知が難しい傾向にある。(5)

ボットは、標的のコンピュータを、ネットワークを介して外部から操作し、ほかのシステムを攻撃させるなどの目的でシステムにインストールされるプログラムであり、同じ種類のボットに感染しているコンピュータから構成されるネットワークをボットネットと呼ぶ。攻撃者はボットネットを遠隔操作することで、標的に対して組織的な攻撃を実行することができる。(6)

国内では1990年から通商産業省（現：経済産業省）の告示「コンピュータウイルス対策基準」に基づき、コンピュータウイルスを発見した場合、被害の拡大と発生を防ぐために、指定届出機関である情報処理推進機構（IPA）に届出を行う制度が運用されている(7)。同様に、1996年から「コンピュータ不正アクセス対策基準」に基づき、不正アクセスの届出制度が運用されてい

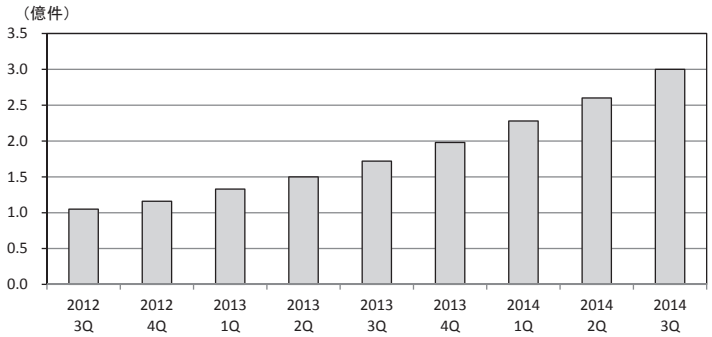
る[8]。さらに、2010年からはIPAにマルウェアや不正アクセスに関する総合的な相談窓口として「情報セキュリティ安心相談窓口」が設置されており、技術的アドバイスを行っている[9]。

●事例研究

■マルウェア登録件数

図1に示すセキュリティベンダ大手のIntel Security（旧：McAfee）が公表している統計情報によれば、2014年第3四半期において同社のマルウェアデータベースに登録されたマルウェアのサンプル数は約3億件となっており、前年同時期と比較し76%増加している（図1参照）。[10]

図1　マルウェアデータベースへの登録サンプル数（全世界）



（注）図中のQは、四半期を示しており、例えば1Qは、第1四半期を表す。
（出典）Intel Security「McAfee Labs脅威レポート」2014.11, p.29. <http://www.mcafee.com/jp/resources/reports/rp-quarterly-threat-q3-2014.pdf>を基に三菱総合研究所作成。

●海外の状況、技術動向、制度、規制

■セキュリティベンダの取組

アンチウイルスソフト等を販売するセキュリティベンダは独自にマルウェアの解析を行っている。セキュリティベンダは独自に配置したハニーポット（Honeypot, マルウェアが進入しやすいおとりサーバやネットワーク）やクローラ（Crawler, ウェブサイト等を巡回してマルウェアを収集するツール）を使って、又はユーザからの提供を受けてウイルスとして疑われるファイル（検体）を収集している。解析の結果マルウェアと判定された検体はパターンファイル（「定義ファイル」とも呼ばれる。）と呼ばれる既知のマルウェアの特徴を記録したデータに追加される。追加されたパターンファイルは、ユーザがアンチウイルスソフト等の製品を更新する際に製品に反映される。アンチウイルスソフトはこのパターンファイルとコンピュータ上のファイルを比較し検出・駆除を行うため、対策ではパターンファイルを最新化することが重要となる。

(1)　Peter Mell ほか（情報処理推進機構・NRIセキュアテクノロジーズ翻訳監修）「マルウェアによるインシデントの防止と対応のためのガイド」2008.9, p.2-1. <https://www.ipa.go.jp/files/000025349.pdf>（原書名: Peter Mell et al.,“Guide to Malware Incident Prevention and Handling,”November 2005. National Institute of Standards and Technology Website <http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf>）
(2)　同上
(3)　「2014年7月の呼びかけ」2014.7.1. 情報処理推進機構ウェブサイト <http://www.ipa.go.jp/security/txt/2014/07outline.html>
(4)　Peter Mell ほか　前掲注(1), p.2-4.
(5)　同上, pp.2-4-2-5.
(6)　同上, p.2-8.
(7)　「コンピュータウイルス対策基準」（平成12年通商産業省告示第952号）<http://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm>
(8)　「コンピュータ不正アクセス対策基準」（平成12年通商産業省告示第950号）<http://www.meti.go.jp/policy/netsecurity/UAaccessCMG.htm>
(9)　「情報セキュリティ安心相談窓口」情報処理推進機構ウェブサイト <http://www.ipa.go.jp/security/anshin/>
(10)　Intel Security「McAfee Labs脅威レポート」2014.11, p.29. <http://www.mcafee.com/jp/resources/reports/rp-quarterly-threat-q3-2014.pdf>

1.2.3　不正アクセス・サイバー攻撃

不正アクセス及びサイバー攻撃が、かつての愉快犯によるものから、金銭目的や政治的なアピールを目的としたものに変化しており、さらに昨今では国家間のサイバー戦争の様相も呈してきている。

マルウェア感染やコンピュータ及びネットワークに対する侵入・改ざん、サービス運用妨害など、いわゆる不正アクセスやサイバー攻撃の発生件数が増えてきている。警察庁が発表した2013年中の不正アクセス行為の発生状況によれば、認知件数は前年比1,700件増の2,951件、検挙数は前年比437件増の980件となっている(1)。

2000年代前半までは、出来合いの攻撃ツールを使うだけの「スクリプトキディ」や「クラッカー」を始めとする愉快犯によるものが多かったが、徐々に金銭を目的とした犯行が増え、クレジットカード情報や銀行などのアカウント情報（IDとパスワードなど）を盗み出すといった直接的なものだけでなく、企業や公的機関から機密情報を盗み出して利害の対立する企業や組織に売るといったケースもある。これらの金銭目的の犯罪行為を行う者たちの中には、背後に犯罪組織が存在し、国際規模で活動しているグループもある。さらに、国の諜報機関が主導的な立場で他国の政府機関を始め、重要インフラに対してサイバー攻撃を行うケースも増えているとみられ、文字どおりの「サイバー戦争」、「サイバーテロ」の様相を呈してきている。

ほかにも、自らの政治的信条をアピールするために、公的機関やメディア、企業のウェブサイトなどに対してDDoS攻撃を行ったり、ウェブサイトの情報を改ざんしたりするといった示威行為も増えてきている。こうした行為を行う者は「ハクティビスト（hacktivist）」と呼ばれ、「Anonymous」や「ラルズセック（LulzSec）」といったグループが世界的に知られている。

近年の脅威とされている主な攻撃の例としては、特定の組織や個人を狙った標的型攻撃や、ウェブサイトの改ざん、不正に取得されたID、パスワード等を悪用した不正ログイン、不正使用、インターネットバンキングにおける不正送金等がある(2)。

侵入・改ざんやマルウェア感染といったサイバー攻撃では、一般的に攻撃対象が使用しているソフトウェアやハードウェアのセキュリティ上の弱点、つまり「脆弱性」を悪用するものが多い。例えば、ウェブサイトを閲覧しただけでマルウェアに感染するドライブバイダウンロード攻撃も端末やアプリケーションの脆弱性が悪用されている。中には、脆弱性の悪用ではなく、文書ファイルなどを装った実行ファイル（マルウェア本体）を開かせる手口による攻撃もある。また、安全なファイルを装った、いわゆる「トロイの木馬」による攻撃は古くから存在している。ほかにも、入力データを適切に処理していないウェブサイトに対する攻撃として、悪意のあるスクリプトやデータベース操作を実行させるクロスサイトスクリプティングやSQLインジェクションなどがある。

また、偽サイトを介してIDとパスワードを盗み出すフィッシング、攻撃者がサイト等から不正に入手したIDとパスワードの組合せを使って、ほかのサイトへのログインを試みるパスワードリスト攻撃（ユーザのIDとパスワードの使い回しを悪用した攻撃）などがある。

新たな攻撃手法は次々に生まれており、最近では正規のインターネットバンキングを利用時に偽の認証画面を表示させ、自動で不正送金を行うマルウェアや、SNSのアカウントを乗っ取

り、マルウェアをダウンロードさせるサイトのリンクを含む投稿を拡散させる攻撃等もある。

●事例研究

■国内の主なサイバー攻撃

2011年10月には衆議院、11月には参議院のコンピュータが外部からの情報窃取を可能とするマルウェアに感染していたことが明らかとなり、特に衆議院に関しては、全議員のIDとパスワードが流出し、最大15日間にわたって電子メールが盗み見られていた可能性があるとの報告書が公開されている(3)。2012年9月には尖閣諸島のいわゆる「国有化」を始めとした一連の情勢を受け、中国のハッカー集団の掲示板等において日本に対するサイバー攻撃が呼びかけられ、裁判所や重要インフラ事業者等のウェブサイトが改ざんされたほか、一部の政府のウェブサイトにアクセスが集中し閲覧が困難になるなど、関連が疑われる被害が発生した(4)。また、2013年4月には宇宙航空研究開発機構（JAXA）のサーバが不正アクセスを受けて国際宇宙ステーションに関する技術情報や関係者の個人メールアドレスが流出したことが判明している(5)。

●海外の状況、技術動向、制度、規制

■中国軍による米国へのサイバー攻撃

2013年2月に米Mandiant社（当時）が発表した「APT1レポート（APT1: Exposing One of China's Cyber Espionage Units）」において、米国の企業や組織に対するサイバー攻撃に中国人民解放軍総参謀部第3部第2局（61398部隊）が関与していると断定された件は、中国からの反発を招いただけでなく、国際的にも注目を集めた。その後、2014年5月には米国司法省が61398部隊の将校らを米国企業にサイバー攻撃を行ったとして起訴したと発表した(6)。

■韓国及びエストニアに対するサイバー攻撃

2013年3月、韓国では複数の金融機関や放送局において、密かに感染させられていたマルウェアが同時多発的に作動し、数万台におよぶコンピュータが機能不全を起こし、社会経済活動に大きな影響が発生した(7)。2007年4月にはエストニアで大規模サイバー攻撃が発生し、ITへの依存度が高かったことから、国家の国民生活インフラ全体が麻痺する事態となった(8)。

---

(1)　警察庁「平成25年中の不正アクセス行為の発生状況等の公表について」2014.3.27. <https://www.npa.go.jp/cyber/statics/h25/pdf040.pdf>
(2)　情報処理推進機構「2014年版情報セキュリティ10 大脅威―複雑化する情報セキュリティあなたが直面しているのは？―」2014.3, pp.12-21. <https://www.ipa.go.jp/files/000037151.pdf>
(3)　警察庁「第1章　特集「サイバー攻撃の情勢と対策」」『焦点』280号, 2012.3, p.4. <https://www.npa.go.jp/archive/keibi/syouten/syouten280/pdf/ALL.pdf>
(4)　警察庁「第5章　サイバー攻撃情勢」『焦点』282号, 2013.3, p.35. <http://www.npa.go.jp/archive/keibi/syouten/syouten282/pdf/99_all.pdf>
(5)　警察庁「第2章　サイバー攻撃情勢」『焦点』283号, 2014.3, p.11. <https://www.npa.go.jp/archive/keibi/syouten/syouten283/pdf/all.pdf>
(6)　Mandiant,“APT1: Exposing One of China's Cyber Espionage Units,”2013.2, pp.3-4. <http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf>; Department of Justice,“U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage,”May 19, 2014. <http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor>; 防衛省編「第1部第2章第5節サイバー空間をめぐる動向」『平成26年版防衛白書―日本の防衛―』日経印刷, 2014, p.110. <http://www.mod.go.jp/j/publication/wp/wp2014/pc/2014/pdf/26010205.pdf>
(7)　警察庁　前掲注(5)
(8)　高山裕司「米国のサイバー戦略とそのインプリケーションについて―国際テロリズム対応の経緯と比較して―」2011.7.25. 海上自衛隊幹部学校ウェブサイト <http://www.mod.go.jp/msdf/navcol/SSG/topics-column/col-002.html>

1.2.4　標的型攻撃

特定の企業や組織を狙った標的型攻撃は､大企業や官公庁のみならず、中小企業も対象とされているが、対象が限定的であるために事前対策が難しく、国内外の企業や政府機関で攻撃の事例が続発している。攻撃の情報をいち早く共有するため、政府や民間の取組が進んでいる。

標的型攻撃とは、特定の企業や組織を狙ったサイバー攻撃である。具体的な手口としては、取引先などの関係のある実在する人物や組織をかたった電子メールを、受信者が関心を持つような件名や内容で送り付けることによって、受信者が添付されたファイルを開いたり、メール本文中に記載されたURLにアクセスしたりすることで、マルウェアに感染させるというものである(1)。例えば、内部の人間をかたって実際に行われた会議の議事録にマルウェアを仕込んだものを送り付けるケースや、監督省庁の実在の職員を装って資料を企業の担当者に送り付けるケースなど、様々なパターンが存在する。このように、標的型攻撃においては、必ずしも技術的に高度な手法が用いられるのではなく、人間の心理的な隙や行動のミスに付け込む「ソーシャルエンジニアリング」が用いられている。対策として、受信者はたとえ実在の相手からのメールであっても、それが本当に本人からのものであるかを慎重に確認する必要がある。また、そのための訓練として「ITセキュリティ予防接種」と呼ばれる演習を実施するケースもある。

国内事例としては、2011年に三菱重工業や衆議院・参議院、外務省の在外公館等に対する標的型攻撃が確認されている(2)。また、近年では手口がより巧妙となってきており、成功するまで粘り強く攻撃し続ける、いわゆる「APT（Advanced Persistent Threat）攻撃」や、何度かのやり取りを繰り返して相手を信用させた後に、マルウェアに感染させるファイルを送り付けるという「やり取り型」攻撃、攻撃対象が頻繁に閲覧する正規のウェブサイトを改ざんしてマルウェアに感染させる「水飲み場型攻撃」などが発生している(3)。

年々巧妙化している標的型攻撃に対し、情報処理推進機構（IPA）では、2008年9月から標的型攻撃メールの届出受付を開始し、2011年10月からは「標的型サイバー攻撃の特別相談窓口」を設置して標的型攻撃メールの情報提供受付や相談対応を実施している(4)。また、標的型攻撃は対象が限定的であるために手口の詳細が共有されにくいとの問題があることから、IPAでは標的型攻撃に使われたメールの分析を行い、対策に役立つ傾向や気づき方のノウハウ、対応方法など関するレポートを公開している(5)。さらにIPAは、2011年10月に経済産業省の協力のもと、サイバー攻撃に関する情報共有と早期対応の場として、サイバー情報共有イニシアティブ（Initiative for Cyber Security Information sharing Partnership of Japan: J-CSIP）を発足させた(6)。2015年1月現在、重要インフラ機器製造業者、電力、ガス、化学、石油の全5業界、51の参加組織による情報共有体制を実運用している。2014年10月から12月の間には、標的型攻撃と見られる不審なメールの情報等、参加組織から158件の情報提供を受け、IPAから参加組織へ46件の情報共有を行っている(7)。IPAはまた、2013年8月には、攻撃者が内部探索しにくいシステム設計策を施すための「「標的型メール攻撃」対策に向けたシステム設計ガイド」(8)を公開し、2014年9月にはその改訂・拡充版として「「高度標的型攻撃」対策に向けたシステム設計ガイド」(9)を公開している。ほかにも、総務省では「国民のための情報セキュリティサイト」で標的型攻撃への対策

を呼びかけている(10)。民間でもJPCERTコーディネーションセンター（JPCERT/CC）が標的型攻撃の実態を調査した報告書を2007年に公開（2008年改訂）している(11)。

●事例研究

■国内における標的型攻撃の事例

2011年9月、三菱重工業が標的型攻撃と見られるサイバー攻撃を受け、最新鋭の潜水艦やミサイル、原子力プラントを製造している工場などで、約80台のコンピュータが外部からの情報窃取を可能とするマルウェアに感染していたことが判明している。さらに同年10月には外務省の在外公館職員が使用するコンピュータなどが情報窃取を目的とするマルウェアに感染していたことが明らかとなり、検出されたマルウェアは外務省のネットワークシステムを標的とした特殊なものであったと報じられている。(12)

●海外の状況、技術動向、制度、規制

■米小売大手Target社からの顧客情報大規模流出事件

2013年11月から12月にかけて、米国の小売大手Target社が不正アクセスを受け、顧客約1億1000万人のクレジットカード情報やデビットカード情報等が流出する事件が発生した。米上院通商・科学・運輸委員会（Senate Committee on Commerce, Science, and Transportation）による報告書「A“Kill Chain”Analysis of the 2013 Target Data Breach」によれば、攻撃はまずTarget社と取引をしている空調業者の認証情報を標的型攻撃で盗み、その認証情報を用いることでTarget社内のネットワークに侵入したとしている(13)。

---

(1)　「あなたを狙う「標的型攻撃メール」「フィッシングメール」被害防止には一人一人の情報セキュリティ対策が重要です」政府広報オンラインウェブサイト <http://www.gov-online.go.jp/useful/article/201202/3.html>
(2)　警察庁「第1章　特集「サイバー攻撃の情勢と対策」」『焦点』280号, 2012.3, p.4. <https://www.npa.go.jp/archive/keibi/syouten/syouten280/pdf/ALL.pdf>
(3)　警察庁「平成26年上半期のサイバー空間をめぐる脅威の情勢について」2014.9.11, p.5. <https://www.npa.go.jp/kanbou/cybersecurity/H26_kami_jousei.pdf>
(4)　「標的型サイバー攻撃の特別相談窓口」2013.6.1. 情報処理推進機構ウェブサイト <https://www.ipa.go.jp/security/tokubetsu/>
(5)　情報処理推進機構「標的型攻撃メールの傾向と事例分析（2013年）―ますます巧妙化、高度化する国内組織への標的型攻撃メールの手口―」2014.1.30. <https://www.ipa.go.jp/files/000036584.pdf>
(6)　「サイバー情報共有イニシアティブ（J-CSIP（ジェイシップ））」2015.1.23. 情報処理推進機構ウェブサイト <http://www.ipa.go.jp/security/J-CSIP/>
(7)　情報処理推進機構技術本部セキュリティセンター「サイバー情報共有イニシアティブ（J-CSIP）運用状況[2014年10月～12月]」2015.1.23, p.1. <http://www.ipa.go.jp/files/000043561.pdf>
(8)　情報処理推進機構セキュリティセンター「「標的型メール攻撃」対策に向けたシステム設計ガイド―攻撃者が“内部探索しづらい（歩きづらい）”システム設計策を施す―」2013.8. <http://www.ipa.go.jp/files/000033897.pdf>
(9)　情報処理推進機構セキュリティセンター「「高度標的型攻撃」対策に向けたシステム設計ガイド―入口突破されても攻略されない内部対策を施す―」2014.9. <https://www.ipa.go.jp/files/000042039.pdf>
(10)「標的型攻撃への対策」国民のための情報セキュリティサイト <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/staff/05.html>
(11)　JPCERTコーディネーションセンター「標的型攻撃について（第二版）」2008.9.17. <https://www.jpcert.or.jp/research/2007/targeted_attack.pdf>
(12)　警察庁　前掲注(2);「外務省にサイバー攻撃、情報流出は確認されず」『日本経済新聞』2011.10.26, 夕刊.
(13)　U.S. Senate Committee on Commerce, Science, and Transportation,“A‘Kill Chain’Analysis of the 2013 Target Data Breach,”March 26, 2014, p.4. <http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=24d3c229-4f2f-405d-b8db-a3a67f183883>

1.2.5　重要インフラに対する攻撃

電力、水道、通信、金融、交通といった社会の基盤を提供する重要インフラへのサイバー攻撃の脅威が高まっている。それらの脅威に対して、内閣サイバーセキュリティセンター（NISC）や所管省庁、制御システムセキュリティセンター（CSSC）等により重要インフラ防護のための取組が進められている。

重要インフラに対するサイバー攻撃が増加している。重要インフラにおけるシステム障害は国民生活及び社会経済活動に多大な影響を及ぼすおそれがある。米国で重要インフラのセキュリティ確保に取り組んでいるICS-CERT（Industrial Control Systems Cyber Emergency Response Team）によれば、重要インフラへのサイバー攻撃等のインシデントの報告件数は2011年の140件から2013年には257件に大幅に増加している(1)。実際に国民生活及び社会経済活動に多大な影響を及ぼした例もある。2010年に発覚したイランのウラン濃縮施設へのサイバー攻撃では、ウラン濃縮に使われる遠心分離機が稼働不能になる被害を受けている(2)。また、2013年3月に韓国で起きたサイバー攻撃では、複数の金融機関及び放送局に対する大規模なサイバー攻撃により、銀行のATMやオンラインバンキングが一時停止するなどの事態に陥っている(3)。

重要インフラへのサイバー攻撃に対して、国内では、NISCや重要インフラ所管省庁、情報セキュリティ関係省庁、CSSC等により重要インフラ防護のための取組が進められている。

情報セキュリティ政策会議は、重要インフラ防護に責任を有する政府と自主的な取組を進める重要インフラ事業者等との共通の行動計画として、2014年5月19日に「重要インフラの情報セキュリティ対策に係る第3次行動計画」を決定している。重要インフラに係る行動計画は、2000年に決定された「重要インフラのサイバーテロ対策に係る特別行動計画」以降、2005年に第1次行動計画、2009年に第2次行動計画が決定されてきており、第3次行動計画は、第2次行動計画において得られた良好事例、要改善事例等の知見を反映し、決定されたものとなっている。同計画では、重要インフラ分野として情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、クレジット、石油、化学の13分野を指定し、「安全基準等の整備及び浸透」、「情報共有体制の強化」、「障害対応体制の強化」、「リスクマネジメント」、「防護基盤の強化」の5つの施策群を掲げている。(4)

また、重要インフラを構成するシステムのうち、水道・ガス・電力などの社会インフラや工場などの設備を管理する制御システムのセキュリティを対象として、2012年にCSSCが経済産業省の支援により立ち上げられている。CSSCでは、制御システムベンダ、セキュリティベンダ、制御システムのユーザ企業、大学、独立行政法人等が参加し、産学官連携により取組が進められている。研究開発、普及啓発、人材育成、国際標準化活動、評価認証等の事業を実施しており、具体的には制御システムのセキュリティを高める技術の研究開発（ホワイトリスト技術の適用、サイバー攻撃の早期認識技術の開発等）、防御技術研究開発のための産業別の模擬プラント構築、実際にインシデントが発生した場合の課題について模擬プラントを用いて検証するサイバーセキュリティ演習、制御システムのセキュリティに関する評価認証であるISASecure EDSA認証の推進などを進めている。(5)

●事例研究

■国内における情勢

重要インフラの基幹システムを機能不全に陥れ、社会の機能を麻痺させてしまうサイバー攻撃はこれまでに我が国では発生していないが、情報通信技術を用いた諜報活動であるサイバーインテリジェンスは我が国でも頻発している。

2013年1月、農林水産省において不正プログラムへの感染により情報流出の可能性があることが明らかになり、同年4月には宇宙航空研究開発機構（JAXA）において、同機構のサーバが不正アクセスされ、情報流出の可能性があることが明らかになった。これらの情報流出の中で、重要インフラの基幹システムの設計や脆弱性に関する情報が窃取された場合、それらを悪用したサイバー攻撃が実行されるおそれがある。(6)

●海外の状況、技術動向、制度、規制

■Stuxnetによるイランの核燃料施設へのサイバー攻撃

Stuxnet（「スタックスネット」と読む。）は、2010年7月に確認された、産業制御システムを対象としたマルウェアである。イランの核燃料施設のウラン濃縮用遠心分離機のPLC（Programmable Logic Controller）が改ざんされ、8,400台もの遠心分離機が稼働不能となった。Stuxnetは産業制御システムを狙った初のマルウェアとされる。インターネットに接続していないシステムに対しても、USB等のリムーバブルメディアを経由して感染が拡大し、インドネシアやインド、米国、ロシアなど、イラン以外の国でも感染が確認された。(7)

■韓国での大規模サイバー攻撃

2013年3月、韓国の主要な放送局や金融機関において、あらかじめ仕掛けられた時限的に作動する不正プログラムが一斉に作動し、数万台に及ぶコンピュータがダウンした。金融機関ではATMやオンラインバンキングが一時停止し、放送局ではニュース原稿の作成や編集作業に大きな影響が生じるなどの事態に陥った。さらに、6月には複数の韓国政府機関等のウェブサイトが、改ざん及びDDoS攻撃の被害を受け、政府関係者等の個人情報が流出した。韓国政府は北朝鮮の関与を指摘している。(8)

---

(1)　Industrial Control Systems Cyber Emergency Response Team,“ICS-CERT Year in Review 2013,”2014.2.24, p.16. <https://ics-cert.us-cert.gov/sites/default/files/documents/Year_In_Review_FY2013_Final.pdf>

(2)　経済産業省「サイバーセキュリティと経済研究会報告書―中間とりまとめ―」2011.8.5, p.19. <http://www.meti.go.jp/press/2011/08/20110805006/20110805006-3.pdf>

(3)　警察庁警備局「治安の回顧と展望（平成25年版）」2013.12.12, p.86. <https://www.npa.go.jp/keibi/biki/kaiko_to_tenbou/H25/honbun.pdf>

(4)　情報セキュリティ政策会議「重要インフラの情報セキュリティ対策に係る第3次行動計画」2014.5.19, pp.1, 8-10. <http://www.nisc.go.jp/active/infra/pdf/infra_rt3.pdf>

(5)　制御システムセキュリティセンター「制御システムセキュリティの脅威と対策の動向およびCSSCの研究概要について（一般向け）」2015.2.2, pp.10-23. <http://www.css-center.or.jp/pdf/about_CSSC.pdf>

(6)　警察庁警備局　前掲注(3), p.85.

(7)　Nicolas Falliere et al.,“W32.Stuxnet Dossier,”Version 1.4, February 2011, pp.5-7. <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>; JPCERTコーディネーションセンター「Stuxnet―制御システムを狙った初のマルウェア―」2011.3.2. <https://www.jpcert.or.jp/ics/2011/20110210-oguma.pdf>

(8)　警察庁「第2章　サイバー攻撃情勢」『焦点』283号, 2014.3, p.11. <https://www.npa.go.jp/archive/keibi/syouten/syouten283/pdf/all.pdf>; 警察庁警備局　前掲注(3)

1.3　情報セキュリティの要素技術

1.3.1　暗号（暗号化）

暗号とは一定の規則に基づいてデータを変換することでデータの機密性や完全性を守るための手法であり、コンピュータや通信、インターネットサービスの安全性を担保するための基盤となる技術である。コンピュータの能力（解読能力）の向上や数学的な解読方法の改善などのため、暗号アルゴリズムや暗号鍵の長さ（鍵長）は必要に応じて見直す必要がある。

暗号とは一定の規則（アルゴリズム）に基づいてデータを変換することでデータの機密性や完全性を守るための手法である。暗号技術はコンピュータや通信及びインターネットを利用する際には誰でも必ず使用しているといっても過言ではない。例えば、インターネットショッピングやインターネットバンキングのサーバとの通信は暗号化され盗聴を防ぐとともに、サーバが正当なサーバであるかどうかも暗号技術によって検証（認証）されている。コンピュータやインターネットサービスにログインするときのパスワードもコンピュータの中では暗号化（ハッシュ化）されて管理されている。

暗号技術の種類は、共通鍵暗号、公開鍵暗号、一方向性暗号（ハッシュ関数）に大別でき、それぞれ異なる用途で用いられている。暗号の安全性は、用いられている暗号アルゴリズム（暗号プリミティブとも呼ばれる）の強さと暗号鍵の長さ（鍵長）によって規定される。軍事・外交用途などでは暗号アルゴリズムが秘匿されることもあるが、民生用途では相互運用性確保のため暗号アルゴリズムは標準化され公開される場合が多い。

米国では、米国国立標準技術研究所（National Institute of Standards and Technology: NIST）が、米国政府機関の調達時に従う連邦情報処理規格（Federal Information Processing Standards: FIPS）を標準化し、機密情報以外の機微情報向け暗号アルゴリズムとしてAES（Advanced Encryption Standard）等を標準化している。米連邦政府機関は連邦情報セキュリティマネジメント法（Federal Information Security Management Act of 2002: FISMA）に基づきNISTが策定した標準に従うことが求められる。またAES等のNIST標準暗号は民間利用も推奨され、世界中で広く普及している。

日本国内では、「電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討」するため、総務省と経済産業省が共同でCRYPTREC（Cryptography Research and Evaluation Committees）プロジェクトを実施している(1)。CRYPTRECプロジェクトでは「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）」を策定し、リストに掲載されている暗号アルゴリズムについて定期的に評価を行っている。なお、CRYPTRECプロジェクトは根拠法を持たないため、CRYPTREC暗号リストの利用は各省庁の任意であるが、情報セキュリティ政策会議が策定している「政府機関の情報セキュリティ対策のための統一基準」の中で電子政府推奨暗号リストを参照するよう定められている(2)。

暗号の安全性については、コンピュータの能力（解読能力）の向上などにより損なわれることがある（暗号の危殆化）。このため暗号アルゴリズムや鍵長は必要に応じて見直す必要がある。2006年に、政府機関の情報システムにおいて使用されている暗号アルゴリズム（SHA-1及びRSA1024）の安全性が低下したとCRYPTRECにより評価されたことを踏まえ、より強度の高い暗号アルゴリズムへの移行が計画的に進められている(3)。また、近年従来の暗号とは全く異

なる原理に基づく量子暗号通信が注目されている。同技術は伝送速度、伝送可能距離等の面で課題は残っているが、実用化されれば原理的に盗聴不可能とされている(4)。

●事例研究

■CRYPTREC

CRYPTRECとは、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するための総務省及び経済産業省によるプロジェクトであり、CRYPTREC暗号リスト等を策定している。両省が共同で運営する暗号技術検討会、情報通信研究機構（National Institute of Information and Communications Technology: NICT）と情報処理推進機構（IPA）が共同で運営する暗号技術評価委員会及び暗号技術活用委員会で構成される。

■JCMVP

暗号モジュール試験及び認証制度（Japan Cryptographic Module Validation Program: JCMVP）はISO/IEC 19790:2006（JIS X 19790:2007）に基づく暗号モジュールの認証制度である。第三者による試験及び認証により、暗号モジュールが重要情報を適切に保護していることを、暗号モジュールの利用者が確認できる。製品評価技術基盤機構（NITE）により認定された民間の暗号モジュール試験機関が評価を行い、IPAが認証機関として認証を行う。(5)

■電子署名

暗号技術の応用の一つとして電子的な文書やデータの真正性を保証するための電子署名（デジタル署名）がある。電子署名の有効性を保証するため、「電子署名及び認証業務に関する法律」（いわゆる「電子署名法」。平成12年法律第102号）が制定されている。

●海外の状況、技術動向、制度、規制

■米国の標準暗号

1977年に米国政府の標準として採用された暗号方式DES（Data Encryption Standard）は、米国政府機関だけではなく様々な用途に利用されてきたが、コンピュータの能力向上と解読手法の発見などにより1990年代後半にはその安全性が低下（暗号の危殆化）してきた。これに対応するため、NISTではDESに代わる暗号アルゴリズムを策定するプロジェクトを1997年に立ち上げ、公募により優れた方式を選定することとした。公募の結果、世界中から21方式の暗号方式が提案され、安全性と処理効率の観点から最終的にはベルギーの研究者が提案したRijndael（「ラインドール」と読む。）と呼ばれる暗号アルゴリズムが米国標準暗号AESとして選定され、2001年にFIPS-197として標準化された(6)。AESは様々な用途（無線LANの暗号化、PC等とWebサーバ間の通信の暗号化、ブルーレイディスクの著作権保護技術等）で使用されている。

---

(1)　「CRYPTRECとは」CRYPTRECウェブサイト <http://www.cryptrec.go.jp/about.html>
(2)　情報セキュリティ政策会議「政府機関の情報セキュリティ対策のための統一基準（平成26年度版）」2014.5.19, pp.36-37. <http://www.nisc.go.jp/active/general/pdf/kijyun26.pdf>
(3)　情報セキュリティ対策推進会議「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1 及び RSA1024に係る移行指針」2012.10.26. <http://www.nisc.go.jp/conference/seisaku/dai31/pdf/31shiryou0302.pdf>
(4)　東京大学ほか「量子暗号に30年ぶりの新原理」2014.5.22. 国立情報学研究所ウェブサイト <http://www.nii.ac.jp/userimg/press_20140516.pdf>
(5)　「暗号モジュール試験及び認証制度（JCMVP）」情報処理推進機構ウェブサイト <http://www.ipa.go.jp/security/jcmvp/documents/open/jcmvp_pamphlet_201205.pdf>
(6)　National Institute of Standards and Technology, "Federal Information Processing Standards Publication 197: Announcing the Advanced Encryption Standard (AES)," November 26, 2001, p.5. <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

1.3.2　認証・アイデンティティ管理

パソコンやスマートフォンなどで電子メールや各種インターネットサービスを利用する際、個人を特定するためにユーザ認証が行われる。現在はパスワード認証方式が一般的であるが、パスワード漏えいやパスワード類推などにより、不正利用される事案が問題となっている。インターネットバンキング等のサービスでは、より強固な認証方式を導入する事例が増えている。

認証は、通信相手に認証主体が本物であることを証明することが目的であり、証明したい主体の種類の違いにより、ユーザ認証、クライアント認証、メッセージ認証などがあるが、ここではユーザ認証を中心に説明する。

ユーザ認証では、個人に固有のIDを割り当て、それにパスワードなど本人しか知らない（持たない）要素を組み合わせて、本人であることを証明する。IDと組み合わせる要素としては、記憶を頼りにするパスワード、所持するものを頼りにするICカード、本人の身体的特徴を頼りにするバイオメトリクス（指紋、虹彩など）などがある。ユーザ認証に使われるIDとパスワードなどの組合せは、各種サービスが本人を特定するための重要な基盤となるため、IDの機密性、完全性、可用性を厳格に管理すること（アイデンティティ管理）が重要となる。電子メールやSNSなどのインターネットサービスを利用する際、現在は多くのサービスでIDとパスワードによる認証（パスワード認証方式）が使用されている。

パスワード認証方式は、本人が記憶しているパスワードを利用するため、特別な装置を用意する必要が無く、実装や運用が容易なために広く用いられているが、ひとたびパスワードが第三者に知られてしまうとすぐになりすましができてしまうという欠点がある。このためインターネットバンキング等のサービスでは、①ワンタイムパスワード方式や②2段階認証方式、③ICカード認証方式などのより強固な認証方式を導入する事例も増えている。

①ワンタイムパスワード方式とは、利用するたびに異なるパスワード（使い捨てパスワード）を使って認証を行う方式であり、パスワード漏えいに対する防御力が強い。代表的な使い捨てパスワードの生成方式としては、専用機器（トークン等）を使って使い捨てパスワードをユーザに知らせる方式や、携帯電話等に電子メールやショートメッセージで使い捨てパスワードを知らせる方式がある。

②2段階認証方式とは、IDとパスワードによる認証に加えて、追加の情報（セキュリティコード等）を入力させることで認証を行う方式である。セキュリティコードは、携帯電話のショートメッセージや電子メールなどに認証の都度送信されるため、携帯電話の盗難や電子メールアカウントの乗っ取りなどを防ぐことで認証強度を高めることができる。不正アクセスが疑われる場合（通常利用と異なる地域（海外など）からのアクセス、通常使われていない端末からのアクセスなど）にのみセキュリティコードを求める運用とすることで、利用者の手間を少なくする工夫をするケースが多い。

③ICカード認証方式とは、ICカードに組み込まれた電子証明書を用いて、ユーザ認証を行う方式である。ICカードに組み込まれた電子証明書は偽造が困難であるため、物理的な盗難を防ぐことで認証の強度が保たれるという特徴がある。国内では、インターネットを通じて行政手続きを行う公的個人認証サービスに利用されている。

●事例研究

■パスワード認証方式のリスク

パスワード認証方式において、パスワードが第三者に知られてしまう原因には、類推が容易なパスワードを使ってしまうこと（例：暗証番号に0000や誕生日など）もあるが、パスワードによく使われる一般的な文字列をリスト化（辞書化）して、それを使った総当たり攻撃（辞書攻撃）によってパスワードが知られてしまうこともある。加えて、IDとしてメールアドレスを使う場合に、複数のサービスに同一のIDとパスワードを設定してしまうケースが多い（パスワード使い回し）。この場合に、あるサービスで使っていたID・パスワードが何らかの理由で漏えいしてしまったために、別のサービスに不正にアクセスされてしまうケース（パスワードリスト攻撃）が継続して発生している(1)。

情報処理推進機構（IPA）が2013年12月に公表した「2013年度 情報セキュリティの脅威に対する意識調査―調査報告書―」によると、全国の13歳以上のインターネット利用者のパスワードの設定について、「サービス毎に異なるパスワードを設定している」と答えた回答者は全体の27.2%にとどまっており、パスワード使い回しの実態が明らかになっている(2)。また、2014年には、国内の物流事業者や航空事業者のメンバーサイトや、ECサイト（ネットショップ）に対するパスワードリスト攻撃とみられる不正アクセスが多数発生した(3)。

こうした状況をうけて、IPA及びJPCERTコーディネーションセンター（JPCERT/CC）では、2014年9月にパスワードリスト攻撃による不正ログイン防止に向けた呼びかけ「STOP!! パスワード使い回し!!」を開始した(4)。

●海外の状況、技術動向、制度、規制

■米国著名人のプライベート写真の流出事件

2014年8月末に、米Apple社のクラウドサービスiCloudから、そこに保存されていた米国著名人のプライベート写真が流出する事件が発生した。同社の調査結果によると、これは当該著名人のID、パスワード、セキュリティのための質問（パスワードを忘れた時のための質問）に的を絞った攻撃（標的型攻撃）であり、その結果IDとパスワードが類推されて不正アクセスが起こったとのことであった。この事件を受けて、同社では類推されにくい「強力なパスワード」を設定するとともに、2段階認証を有効にすることをユーザに推奨している。(5)

---

(1)　情報処理推進機構・JPCERTコーディネーションセンター「STOP!! パスワード使い回し!! パスワードリスト攻撃による不正ログイン防止に向けた呼びかけ」2014.9.17. 情報処理推進機構ウェブサイト <https://www.ipa.go.jp/files/000041753.pdf>

(2)　情報処理推進機構「2013年度情報セキュリティの脅威に対する意識調査―調査報告書―」2013.12, p.53. <https://www.ipa.go.jp/files/000035983.pdf>

(3)　「クロネコメンバーズWebサービスへの不正ログインに関するお知らせ」2014.9.26. ヤマトホールディングスウェブサイト <http://www.yamato-hd.co.jp/news/h26/h26_43_01news.html>;「JALマイレージバンク特典「Amazonギフト券への交換サービス」の一時停止ならびに、JMBパスワード変更のお願い」2014.2.3. 日本航空ウェブサイト <https://www.jal.co.jp/info/jmb/140203.html>;「ANAマイレージクラブ特典「iTunesギフトコードへの交換サービス」一時停止と会員パスワード変更のお願い」2014.3.17. 全日本空輸ウェブサイト <https://www.ana.co.jp/topics/notice140311/>;「「なりすましログイン」への対応に関して（9月11日更新）」2014.9.11. リクルートホールディングスウェブサイト <http://www.recruit.jp/news_data/notification/20140908_7754.html>

(4)　情報処理推進機構・JPCERTコーディネーションセンター　前掲注(1)

(5)　“Apple Media Advisory: Update to Celebrity Photo Investigation,”September 2, 2014. <https://www.apple.com/pr/library/2014/09/02Apple-Media-Advisory.html>

1.3.3　アクセス制御

個人情報や金融情報、企業の重要情報などの情報は、その重要性に応じてアクセス制御を行う必要がある。電子ファイルなどの情報資産を不正アクセスから守るためには、物理的、ネットワーク、サーバ、電子ファイルのアクセス制御などを、適切に行うことが重要である。

情報セキュリティの3要素（機密性、完全性、可用性）のうち、特に機密性を確保するためには、対象とする情報資産（電子ファイルなど）の重要性に応じてラベル付けを行い、そのラベルに応じたアクセス制御を行うことが重要である。

情報資産の中には、広く一般に公開されているもの（公開情報）や、一部の関係者のみに公開されているもの（関係者外秘）、特に重要で取扱いを限定するもの（極秘）のように、求められる機密性が異なるものがあるため、まずは対象とする情報資産の洗い出しを行い、それらの重要度に応じたラベル付けを行う必要がある。例として、情報セキュリティ政策会議の「政府機関の情報セキュリティ対策のための統一基準」では、政府の情報をラベル付けするための基準を定めている(1)。

アクセス制御は様々な箇所や方法で行うことが求められるが、情報資源（電子ファイルなど）へのアクセス制御の代表的な方法として、「物理的なアクセス制御」、「ネットワークのアクセス制御」、「サーバのアクセス制御」、「電子ファイルのアクセス制御」がある。

「物理的なアクセス制御」とは、情報資産を管理するサーバを設置したオフィスやデータセンターに適切な人のみが入室できるように管理することである。具体的には、物理的な鍵や暗証番号、ICカードなどを使って入退室管理を行う。

「ネットワークのアクセス制御」とは、情報資産を管理するサーバに対して、LANやインターネットを経由してパソコンなどからアクセスする場合に、適切なパソコンのみが通信できるように管理することである。具体的には、サーバにアクセスするネットワークの経路上にルータやファイアウォールなどを設置して、不必要な通信を遮断する。

「サーバのアクセス制御」とは、サーバにアクセスするパソコンを識別したり、パソコンを使う利用者を識別したりすることで、適切なパソコンや利用者のみがサーバにアクセスできるように管理することである。具体的には、電子証明書をインストールすることでパソコンを識別したり、利用者ごとに異なるIDとパスワードを付与したりすることで認証を行う。

「電子ファイルのアクセス制御」とは、個別の電子ファイルの機密レベルに応じて利用者や利用者属性（グループなど）ごとにアクセス権を付与して、適切な利用者のみが当該電子ファイルにアクセスできるように管理することである。具体的には、サーバのOSの機能を利用して、ファイルごとにアクセス可能な利用者と、その利用者に許可する権限（読み取り可や書込み可など）を設定する。

企業などが社内LAN上に設置したサーバや、インターネット上のファイル共有サービスで電子ファイルを扱う場合は、前述の様々なアクセス制御の方法を適切に組み合わせて管理することが重要である。例えば、ネットワークのアクセス制御を厳格に行ったとしても、物理的なアクセス制御が不十分であれば、不正な侵入等による情報漏えいのリスクが高まることになる。最近では、複数のサーバやサービスを、一人の利用者が同時に使用するケースも増えてき

ている。この際にサーバやサービスごとに認証を行わずに、最初の1回だけ認証を行い、その後はその認証情報を使って認可を行うシングルサインオンの仕組みの導入も進んでいる。

●事例研究

■国内における不正アクセスの事例

情報処理推進機構（IPA）が2014年3月に公表した「2014年版 情報セキュリティ10大脅威」によると、2013年において社会的影響が大きかったセキュリティ上の脅威として、第2位に「不正ログイン・不正利用」、第8位に「紛失や設定不備による情報漏えい」が示されている。不正ログイン・不正利用としては、IDとパスワードによる認証方式に対して、パスワードリスト攻撃（複数のウェブサイトで同一のIDとパスワードを使い回している利用者に対して、管理が不十分なウェブサイトからIDとパスワードの情報を不正に取得し、別のウェブサイトに利用者を偽って不正アクセスを行う攻撃手法）による不正アクセスが多数発生した。紛失や設定不備による情報漏えいとしては、アクセス制限や認証のない設定のままで機器やサービスを使用したために、重要な情報が意図しない第三者に公開されて情報漏えいしたケースが発生した。(2)

また、2014年6月には、ベネッセコーポレーションにおいて、個人情報を格納したデータベースにおけるアクセス権限設定の不備により、約3500万件の個人情報漏えい事件が起きた。システム開発・運用を行っているグループ会社の業務委託先の社員が全ての個人情報を閲覧可能な権限を持っており、その権限を濫用して不正に個人情報を社外に持ち出し、名簿業者に売却したことにより被害が拡大した。(3)

●海外の状況、技術動向、制度、規制

■シングルサインオンに関する技術動向

シングルサインオンを実現する方式としては、「エージェント（プログラム組込み）型」、「リバースプロキシ（代理応答）型」、「フェデレーション（認証連携）型」などの方式がある。「エージェント型」や「リバースプロキシ型」は、主に企業内システムで利用されている。一方、「フェデレーション型」は、主にインターネット上のサービス間で多く利用されている。

「フェデレーション型」のシングルサインオンについては標準化が進められており、現在は非営利組織である米国のOpenID財団（OpenID Foundation）が標準化したOpenID（オープン・アイディ）と、国際的な非営利組織であるOASIS（Organization for the Advancement of Structured Information Standards,「オアシス」と読む。）が標準化したSAML（Security Assertion Markup Language,「サムル」と読む。）が広く使われている(4)。

(1)　情報セキュリティ政策会議「政府機関の情報セキュリティ対策のための統一基準（平成26年度版）」2014.5.19, pp.2-4. <http://www.nisc.go.jp/active/general/pdf/kijyun26.pdf>
(2)　情報処理推進機構「2014年版情報セキュリティ10大脅威―複雑化する情報セキュリティあなたが直面しているのは?―」2014.3. <https://www.ipa.go.jp/files/000037151.pdf>
(3)　「事故の経緯」ベネッセコーポレーションウェブサイト <http://www.benesse.co.jp/customer/bcinfo/01.html>
(4)　OpenID Foundation <http://openid.net/foundation/>;“OASIS Security Services (SAML) TC.”<https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security>

1.3.4　監視

ネットワークや各種ネットワークサービスの可用性を確保するためには、様々な方法で異常が発生していないかを監視することが重要である。監視カメラなどの物理的な監視に加え、サーバやネットワーク機器等に対する「ハードウェア監視」、「サービス監視」、「ネットワーク監視」などを組み合わせて行うことで、異常を迅速に発見することが可能となる。

ネットワークや各種ネットワークサービスについて、情報セキュリティの3要素（機密性、完全性、可用性）のうち、特に可用性を確保するためには、異常を迅速に発見するための監視が重要である。監視の方法としては、オフィスやデータセンターで監視カメラなどを使って物理的に人や物の出入りを監視する方法に加えて、サーバやネットワーク機器に対する①ハードウェア監視、②サービス監視、③ネットワーク監視などが行われる。

①ハードウェア監視では、主に障害監視が行われる。サーバ機器のCPUやメモリ、HDD（ハードディスクドライブ）やその他の周辺機器について、サーバ機器内に備え付けられた監視機能が状態を常時監視し、異常時には警告を管理者等に通知する。

②サービス監視では、そのサービスが利用可能か否かの「サービス死活監視」と、必要十分な性能が確保できていることを確認する「サービス性能監視」が行われる。

「サービス死活監視」では、そのサービスを提供するサーバに対する通信が可能であることを確認するping（「ピン」あるいは「ピング」と読む。特定の相手とサーバ、PC等のネットワーク上で通信が可能であることを確認するためのコマンドであり、OSに標準搭載されている。）監視がよく使われる。また、ネットワークサービスを構成するソフトウェアの状態を監視するケースも増えている。ソフトウェアの状態を監視する場合、ウェブサービスや電子メールサービスで使用する通信プロトコル（HTTPやSMTPなど）を使って、サービスからの返答の内容を確認することで監視を行う（サービスからの返答が全くない場合には到達性がないこと、返答が一部ある場合にはパケットロスがあること、返答があっても返答が遅い場合にはネットワークに遅延があることを確認する）。

「サービス性能監視」は、対象ネットワークサービスの利用者が急増して反応が遅くなったり、サーバのメモリ不足やHDD容量不足などで性能低下が起きていたりすることを発見するために行う。

③ネットワーク監視では、LANやインターネットを構成するネットワークスイッチやルータ、ファイアウォールなどの通信機器に対する「ネットワーク性能監視」と、ネットワーク上を流れる通信内容に対する「ネットワーク不正アクセス監視」が行われる。

「ネットワーク性能監視」では、各通信機器に備え付けられた監視機能を使い、一定時間当たりの通信処理量（スループット）などを収集し、ネットワーク上にボトルネックが発生していないことを監視する。通信機器の監視機能では、SNMP（Simple Network Management Protocol）やRMON（Remote network MONitoring,「アールモン」と読む。）などの標準化された監視用プロトコルが広く使われている。

「ネットワーク不正アクセス監視」では、不正な端末による通信やウイルスを含んだ通信、機密情報などを不正に持ち出ししようとする通信などを監視する。ネットワーク不正アクセス監視を行うツールとしては、ファイアウォールに加えて、IDS（侵入検知システム）やIPS（侵入

防止システム）などの専用ネットワーク装置を用いることが多い。最近は通信を使用しているアプリケーションの種類を識別して監視する次世代型ファイアウォールの導入も増えている。

なお、各種監視機能を通じて収集されたデータは膨大になるため、管理者が的確に状況を把握できるように、統合監視ツールに収集され、集計やグラフ化などが行われる。企業の情報システムやネットワークの監視に使われる統合監視ツールとしては、OpenView（ヒューレット・パッカード（HP））、Tivoli（IBM）、JP1（日立製作所）などが多く用いられる。オープンソースソフトウェアとしては、NagiosやHinemosなどが多く用いられる。

●事例研究

■インターネット上の監視

サイバー攻撃の増加を背景に、国内でも様々な形でインターネット上の監視が行われている。

情報通信研究機構（NICT）では、インシデント分析システムnicter（Network Incident analysis Center for Tactical Emergency Response,「ニクター」と読む。）[(1)]やサイバー攻撃統合分析プラットフォームNIRVANA（nicter real-network visual analyzer,「ニルバーナ」と読む。）[(2)]を開発・運用し、インターネット上の攻撃トラフィック（攻撃のための通信）の可視化を行っている。

警察庁では、サイバー犯罪対策の一環として、「リアルタイム検知ネットワークシステム」を運用し、インターネット上にセンサを設置して不審な通信を監視している[(3)]。2014年9月に警察庁が発表した「平成26年上半期のサイバー空間をめぐる脅威の情勢について」によると、2014年上半期では、①各種リフレクター攻撃（攻撃対象のIPアドレスを送信元IPアドレスとして詐称して、攻撃対象に大量のデータを送信する攻撃手法）の踏み台となる機器の探索行為、②通信の暗号化に用いられるセキュリティプロトコルである、SSL及びTLSのためのオープンソースソフトウェアである「OpenSSL」の脆弱性（通称「Heartbleed（ハートブリード）」）を標的としたアクセスの増加、③ビル管理システムに対する探索行為などの特徴的かつ不審な通信が観測された[(4)]。

●海外の状況、技術動向、制度、規制

■米国NSAによるネットワーク監視とスノーデン事件

米国国家安全保障局（National Security Agency: NSA）は、PRISM（「プリズム」と読む。）と呼ばれる通信監視プログラムを運用していると言われている[(5)]。PRISMは、国際的に著名なインターネットサービス（GoogleやFacebookなど）の情報を収集・分析して監視することで、テロ対策などに活用することを目的としているとされている。PRISMの存在は、2013年6月に、NSA及び米国中央情報局（Central Intelligence Agency: CIA）の元職員であるエドワード・スノーデン（Edward Joseph Snowden）の告発により明らかになった。同時に、日本を含む他国大使館に対するNSAによる盗聴行為も明らかになり[(6)]、各国から批判が相次いだ。

(1)　「研究紹介」情報通信研究機構ウェブサイト <http://www.nict.go.jp/nsri/cyber/research.html>
(2)　「ネットワークリアルタイム可視化システムNIRVANA」情報通信研究機構ウェブサイト <http://www.nict.go.jp/publication/NICT-News/1109/01.html>
(3)　「サイバーテロ対策」警察庁ウェブサイト <http://www.npa.go.jp/hakusyo/h23/honbun/html/1-toku2_2_6.html>
(4)　警察庁「平成26年上半期のサイバー空間をめぐる脅威の情勢について」2014.9.11, pp.13-15. <http://www.npa.go.jp/kanbou/cybersecurity/H26_kami_jousei.pdf>
(5)　「米当局、GoogleなどIT大手のサーバーからデータ収集」『ロイター』2013.6.7. <http://jp.reuters.com/article/jpUSpolitics/idJPTYE95603Q20130607>
(6)　「米、日本大使館を盗聴、38大使館・代表部対象、韓国なども、英紙報道」『日本経済新聞』2013.7.1, 夕刊.

1.3.5　インフォメーションハイディング

「情報を隠す」セキュリティ技術であるインフォメーションハイディングの代表的な例として、秘匿通信を目的としたステガノグラフィと著作権管理、情報誘導及び改ざん検出等を目的とした電子透かしがある。

1990年代中頃から米国において著作権管理の新たなメカニズムや秘匿通信に対するニーズの高まりに伴い、インフォメーションハイディング分野の研究開発が急速に進展した(1)。インフォメーションハイディングとは、直接的には「情報を隠す」セキュリティ技術全般を指すが、情報の改ざん検出や追跡の手段等に用いられるウォーターマーキング（Watermarking、いわゆる「透かし」。）、秘匿通信に用いられるステガノグラフィ（Steganography）や、さらにその他の技術を含む裾野の広い技術領域を指す言葉でもある(2)。

電子的な技術を用いる透かしは電子透かし（Digital Watermarking）と呼ばれる。電子透かしは人間には知覚できない微小な変更をデジタルメディア（データ、画像データ、映像データ、音楽データ、テキスト、プログラム等。以下「メディア」という。）に加えることで、メディアの属性情報をメディア自体に不可分に埋め込み、その情報を検出する技術である(3)。

電子透かしはさらにロバスト（強い）電子透かしとフラジャイル（弱い）電子透かしに分類される。ロバスト電子透かしはメディアに圧縮や編集等の加工を施しても透かし情報の検出が可能な高い耐性を持っており、著作権管理や情報誘導等に用いられる。著作権管理においては、デジタルメディアに著作権者のIDや配布先ID等の属性情報を埋め込むことで、著作権情報を提供したり、不正に流通したメディアを検出したりすることができる。また、メディアにコピー等に関する制御情報を埋め込み、コピー制御（例：コピー可／一回までコピー可等）や視聴回数制御を行うこともできる。ほかにもメディアを特定するためのメタ情報や識別IDを埋め込むことによりメディアと対応するメタ情報を一体化して管理する用途がある。情報誘導については、メディアにURL等の情報を埋め込むことで関連情報の表示や誘導を行うものである。例えば、電子透かしが入ったキャンペーンに関するポスターを、電子透かしを検出するアプリが入ったスマートフォンで撮影することで、そのままキャンペーンサイトに誘導されるような利用がされている。(4)

一方、フラジャイル電子透かしはメディアの変更に対して電子透かしが壊れやすく敏感に応答する特徴を持っているため、編集・加工により透かしが変化していることを検知することで、改ざんを検知することができる(5)。

ステガノグラフィは第三者に情報の存在を気づかれずに当該情報を通信・伝達する秘匿通信の技術である。ステガノグラフィは、埋め込みデータを秘匿することを目的とした技術であるため、埋め込むメディアの種類は問わない。メディアに情報を埋め込むという基本的な機能は電子透かしと同様であるが、情報を埋め込む目的が違うため技術要件が異なる。電子透かしではメディアそのものにできるだけ変更を加えず情報を埋め込むこと目的であるため、埋め込む対象となるメディアの品質劣化を最小限にすることが望ましいが、ステガノグラフィでは、あくまで情報を隠すことが目的であり、情報の存在を第三者に気づかれない程度であれば、メディアに品質劣化・改変が生じても構わない。(6)

●事例研究

■ハイビジョン映像向け「電子透かし」

NHK及び三菱電機はハイビジョン映像向けの電子透かし技術を共同で開発し、高画質なハイビジョン映像に対して、高速で情報を埋め込み／検出する技術を実用化し、2013年11月からNHKインターナショナル及びNHKエンタープライズにおいて本格運用されている(7)。

NHKインターナショナルは海外、NHKエンタープライズは国内向けにNHKの映像素材等の提供を行っており、電子透かしにより映像にID情報を埋め込むことで、不正にコピー・使用されたNHKの映像の検出や、違法アップロードの行為者の特定と追跡が可能となる。そのほかにも電子透かしが埋め込まれた映像を、対応するアプリケーションが入った携帯端末で撮影することで映像に関連する情報を表示したり、映像にカメラの撮影情報を埋め込むことで放送時に利用する映像の特定を容易にしたりする等の著作権保護以外の機能も実現する。(8)

今後4K、8Kと映像の高度化が進み、映像コンテンツの価値が高まる中で、電子透かし技術の重要性が増すものと考えられる。

●海外の状況、技術動向、制度、規制

■デジタルシネマ

映画の撮影～編集～上映までをデジタルデータで行うデジタルシネマの普及が進む中で、上映中のデジタルシネマの盗撮防止のため電子透かしの技術が利用されている。ハリウッド映画の6大スタジオのDisney、Fox、Paramount、Sony Pictures Entertainment、Universal、Warner Bros.が構成する業界団体Digital Cinema Initiativesは、デジタルシネマの要求仕様書としてDCSS（Digital Cinema System Specification）(9)を策定しており、この中でコンテンツの盗撮防止対策の1つとして上映装置において上映時間と場所を特定できる情報を電子透かし（DCSSではForensic Markingとして規定）として埋め込むことが要求されている。(10)

(1)　ロス・アンダーソン（トップスタジオ訳）『情報セキュリティ技術大全』日経BP, 2002, p.426.（原書名: Ross Anderson, *Security Engineering*, 2001.）
(2)　松本勉「インフォメーションハイディングの概要」『情報処理』vol.44 no.3, 2003.3, p.227.
(3)　瀬戸洋一ほか『情報セキュリティ概論』日本工業出版, 2007, p.169.
(4)　中村高雄・高嶋洋一「知っておきたいキーワード　第19回　電子透かし」『映像情報メディア学会誌』vol.61 no.7, 2007.7, pp.948-950.
(5)　同上, p.949.
(6)　瀬戸ほか　前掲注(3), pp.180-181.
(7)　「ハイビジョン映像向け「電子透かし」本格運用開始のお知らせ」2013.11.18. 三菱電機インフォメーションシステムズウェブサイト <http://www.mdis.co.jp/news/topics/2013/1118.html>
(8)　「ハイビジョン映像向け電子透かしソリューション」三菱電機インフォメーションシステムズウェブサイト <http://www.mdis.co.jp/products/digital-watermark/index.html>
(9)　Digital Cinema Initiatives, Member Representatives Committee,“Digital Cinema System Specification: Version 1.2 with Errata as of 30 August 2012 Incorporated,”October 10, 2012. <http://dcimovies.com/specification/DCI_DCSS_v12_with_errata_2012-1010.pdf>
(10)　*ibid*., pp.118-122.

1.3.6　トラステッドコンピューティング

トラステッドコンピューティングとはCPUと独立したハードウェアベースのセキュリティ基盤を構築することによりシステムの高信頼性を担保する仕組みである。PCやモバイル端末、組込み機器を中心に、この仕組みを実現するセキュリティチップが内蔵されている。セキュリティチップには暗号鍵を安全に保管することができ、例えば、PCからハードディスクドライブだけを取り出しても暗号鍵がなく復号できないため漏えいしない。また、システム構成を検証することができ、システムの安全性を維持することができる。

トラステッドコンピューティング（Trusted Computing）とは、OSやソフトウェアの動作に使われるCPUとは独立したハードウェアを利用したセキュリティ対策基盤により、不正なソフトウェアの動作や保存されたデータに不正なアクセスができないようにしたシステムの高信頼性を担保する仕組みである。仕組みを実現するハードウェアはセキュリティチップと呼ばれており、OSやほかのハードウェアから独立して機能するため、外部からの攻撃に強い（耐タンパー機構）。通常、ハードディスクドライブ（HDD）、ソリッドステートドライブ（SSD）、フラッシュメモリに格納された暗号鍵などの重要な情報は簡単に読み出しできるため暗号鍵の安全は担保されないが、セキュリティチップに格納された暗号鍵は外部に取り出せないため、安全に格納・管理することが可能である。

2003年にセキュリティチップメーカーやPCメーカーなど14社が中心となり組織された国際的な標準化団体であるTrusted Computing Group（TCG）がセキュリティチップの仕様をTrusted Platform Module（TPM）として標準化している(1)。TPMは暗号鍵を安全に保管する暗号化機能、機器やソフトウェアが変更されていないことを確認する機能、改ざん検出機能、暗号処理機能を備えている(2)。TPMが標準化されたことによりセキュリティチップを搭載するPCが増加した。これらのPCでは、HDDのデータを暗号化するための暗号鍵がPC内のセキュリティチップに格納されているため、HDD単体を盗まれてもデータを解読できない仕組みとなっている(3)。

現在、TPMチップは暗号鍵の安全な保管場所としての利用が主になっているが、TPMの機能を利用することでストレージの暗号化や、電子メールの暗号化、クライアント認証など、様々な分野で信頼できる環境や接続を保証することができるようになる。

すでにTMPチップを組み込んだPCは6億台以上出荷されている。近年ではOSレベルでのTPMへの対応が進み、サイバーセキュリティの脅威に対する危機意識が高まっていることから、特に企業での普及が進んでいる(4)。一方で、TCGでは、PC以外にもストレージ、認証機能などの仕様も定めており、ストレージ、認証機能を持った組込み機器であるPOS端末やATM、デジタル複合機、携帯電話などにもTPMが搭載可能となっている(5)。

●事例研究

■TPM活用事例

デジタル複合機（Multi Function Printer: MFP）には、HDDが内蔵されており、HDDが抜き取られ、一時的に保存されたデータが漏えいしないよう暗号化機能が実装されている。TPMが搭載されたMFPでは、HDDの暗号化の暗号鍵はTPM内部に保管され、さらにTPM内部の暗号鍵（ルート暗号鍵）でも暗号化されており、HDDデータの機密性を確保している(6)。

また、TCGでは、2012年2月にストレージセキュリティの最新仕様TCG Opalを発表しており、HDD自身で暗号化と暗号化したデータを元に戻す復号を安全に行う技術を標準化している(7)。この仕様を遵守すれば、HDD自体にディスク全体を暗号化するボリューム暗号機能を持ち、PCが盗難にあっても、ファイルの内容を見ることができないため、HDDから情報が漏えいしない。

●海外の状況、技術動向、制度、規制

■TCGによるTPMの標準化

2003年4月に組織されたTCGはTPMと呼ばれるセキュリティチップの仕様の策定及び各種デバイス（PC、サーバ、携帯電話等）への搭載による「信頼できるコンピューティング」技術（システムが意図した状態で動くこと）の普及促進を目的としている。

TPM 1.2(8)では、公開鍵暗号（RSA）、ハッシュ機能（SHA-1）、メッセージ認証符号MAC（HMAC）、真性乱数生成器といった暗号化機能を始め、RAMメモリ、フラッシュメモリ、カウンタ、タイマの機能が標準化されている。PC内部のデータの漏えいを防ぐために、データ（鍵）の暗号化機能やデータが改ざんされるのを防止するためのデータの署名機能、機器が正当なものかどうか確認するためのハッシュ機能が使われる。

2014年にTPM 2.0(9)が公開された。変更点としては、高度な暗号化アルゴリズムをサポートしていることや、将来利用される暗号アルゴリズムにも対応可能な柔軟性のある仕組みを持つ。TPM 2.0は、サーバ、デスクトップPC、組込みシステム、モバイル機器、ネットワーク機器など、多様なプラットフォームに対応している。例えば、PC用には、PCクライアント・プラットフォームTPMプロファイル（PC Client Platform TPM Profile: PTP）仕様を標準化している。

チップメーカー各社がTPMに準拠したセキュリティチップを製造しており、それらのチップを搭載したPCが主に企業向けに販売されている。また、Windows Vista以降、OSもTPMに対応したストレージ暗号化機能であるBitLockerを提供している(10)。

---

(1)　Trusted Computing Group,“Trusted Computing Group (TCG) Timeline,”October 2012. <https://www.trustedcomputinggroup.org/files/resource_files/03B78F71-1A4B-B294-D0AF4D3092FD9C75/TCG%20timeline%20rev%20Oct%202012.pdf>
(2)　電子情報技術産業協会TCG専門委員会「TPMを活用したセキュリティ最前線」2007.10.3, p.10. <http://home.jeita.or.jp/is/committee/infopolicy/tcg/d20071003.pdf>
(3)　情報処理推進機構「分冊3企業内情報システムを企業外から利用するシステムの運用上のセキュリティ対策」『大企業・中堅企業の情報システムのセキュリティ対策―脅威と対策―』2007.4, p.27. <http://www.ipa.go.jp/security/fy18/reports/contents/enterprise/3.pdf>
(4)　Warwick Ashford,“Enterprise finally embraces TPM-based security,”*ComputerWeekly.com*, July 30, 2014. <http://www.computerweekly.com/news/2240225813/Analyis-Enterprise-finally-embraces-TPM-based-security>
(5)　電子情報技術産業協会TCG専門委員会　前掲注(2), pp.41-44.
(6)　情報処理推進機構「デジタル複合機のセキュリティに関する調査報告書 V2.1」2014.6.9, pp.24-26, 110-113. <http://www.ipa.go.jp/files/000027285.pdf>;「セキュリティ機能の紹介」リコーウェブサイト <http://www.ricoh.com/ja/security/products/mfp/function/>
(7)　Trusted Computing Group,“TCG Storage Security Subsystem Class: Opal,”Specification Version 2.00 Revision 1.00, February 24, 2012. <http://www.trustedcomputinggroup.org/files/resource_files/B15F1F8F-1A4B-B294-D03F09D5122B21F6/Opal_SSC_2%2000_rev1%2000_final.pdf>
(8)　Trusted Computing Group,“TPM Main: Part 1 Design Principles,”Specification Version 1.2 Revision 116, March 1, 2011. <http://www.trustedcomputinggroup.org/files/static_page_files/72C26AB5-1A4B-B294-D002BC0B8C062FF6/TPM%20Main-Part%201%20Design%20Principles_v1.2_rev116_01032011.pdf>
(9)　Trusted Computing Group,“Trusted Platform Module Library Part 1: Architecture,”Family“2.0”Level 00 Revision 01.16, October 30, 2014. <http://www.trustedcomputinggroup.org/files/static_page_files/8C56AE3E-1A4B-B294-D0F43097156A55D8/TPM%20Rev%202.0%20Part%201%20-%20Architecture%2001.16.pdf>
(10)「BitLockerドライブ暗号化のハードウェア要件」Microsoftウェブサイト <http://windows.microsoft.com/ja-jp/windows-vista/hardware-requirements-for-bitlocker-drive-encryption>

主要事項執筆者一覧

執筆者所属：三菱総合研究所

執筆者	主要事項
情報通信政策研究本部主席研究員　村野（むらの）　正泰（まさやす）	1.3.1, 4.1, 4.2, 4.3, 4.4, 4.6, 5.1.1, 5.1.2, 5.1.3, 5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.3.1, 5.3.2, 6.2.1
情報通信政策研究本部主席研究員　澤部（さわべ）　直太（なおた）	1.3.2, 1.3.3, 1.3.4
情報通信政策研究本部主任研究員　谷田部（やたべ）　智之（ともゆき）	1.1, 1.2.1, 1.2.3, 1.2.4, 1.3.6, 2.4, 6.2.6, 6.2.7
情報通信政策研究本部主任研究員　清水（しみず）　友晴（ともはる）	6.1.1
情報通信政策研究本部研究員　松本（まつもと）　尭（たかし）	1.2.5, 2.1, 2.2, 2.3, 3.1, 3.2, 3.3, 4.5
情報通信政策研究本部研究員　丸田（まるた）　佳織（かおり）	1.2.2, 1.3.5, 5.1.4, 5.2.5, 5.2.6, 6.1.2, 6.2.2, 6.2.3, 6.2.4, 6.2.5, 7.1, 7.2, 7.3

＊ 本稿におけるインターネット情報の最終アクセス日は、原則として、2015年1月13日である。