第１節　情報セキュリティを取り巻く状況

日本大学危機管理学部　教授　美濃輪　正行

Ⅰ　情報セキュリティの規格

「情報セキュリティ」という言葉は、ISO/IEC 27001:2013[1] なる国際規格に記載されている。ISO/IEC 27001:2013 は 1995 年に英国で制定された BS7799-2(情報セキュリティ管理システム仕様) を元に国際規格である ISO/IEC27001-2005、ISO/IEC 27001:2013 に発展し、現在に至っている[2]。この規格は情報セキュリティ管理に関する認証制度である ISMS の要求事項であり、国内ではこの認証制度は 2002 年から運用が開始されている[3]。本国際規格は JIS Q27001:2014[4] として日本語化されている。

情報セキュリティが維持できている状態とはどのような特性を満たすのか、この規格から読み取ることができる。主に３つの特性で説明されるが、それらは機密性 (Confidentiality)、完全性 (Integrity)、可用性 (Availability) からなる[5]。昨今の情報セキュリティに関連する危機的な事案も、多くのケースでこれらの特性によって説明することができる。機密性を犯す事案としては個人情報の漏洩や通信データの覗き見、同様に完全性についてはホームページの改竄や既存ファイルの不正な書き換え、更に可用性については DDoS 攻撃やランサムウェアによるデータ利用不可等が該当する。

ISO/IEC 27000 シリーズとして、ISO/IEC 27001:2013 以外に、ISO/IEC 27002:2013 には情報セキュリティ管理策の実践のための規範、ISO/IEC 27003:2010 には情報セキュリティマネジメントシステムの実践の手引き等、関連する規格が存在する。

尚、「情報セキュリティ」に関するガイドラインや監査制度は存在するものの、この用語を含む国内法は存在しない。情報セキュリティに関連する法律には､サイバーセキュリティ基本法、通信事業法、個人情報の保護に関する法律、刑法等が存在する。

Ⅱ　サイバーセキュリティ

「セキュリティ」の言葉を含む「サイバーセキュリティ基本法」[6] は 2015 年に施行された。この法律では「サイバーセキュリティ」を次のように定めている。

「サイバーセキュリティ」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必

要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていることをいう。

「サイバーセキュリティ基本法」で指すところの「サイバーセキュリティ」は、情報システムに関連する事案に重点を置いたものであり、ISO/IEC27001 の「情報セキュリティ」は情報システムに関連しない事案も対象とすると捉えて良いであろう。例を挙げて考えると、学生の名前と成績情報を含む印刷物は適正に管理されるべき個人情報であるが、もしこの印刷物が窃取されたとしたら、これは個人情報の漏洩となり、情報セキュリティの特性が侵されたことになる。サイバーセキュリティの定義からすると「電子的方式、磁気的方式その他人の知覚によっては認識することができない方式により記録」の条件は満たさず、これは該当しない。「サイバーセキュリティ基本法」の第一章　総則　第一条には

インターネットその他の高度情報通信ネットワークの整備及び情報通信技術の活用の進展に伴って世界的規模で生じているサイバーセキュリティに対する脅威の深刻化その他の内外の諸情勢の変化に伴い、情報の自由な流通を確保しつつ、サイバーセキュリティの確保を図ることが喫緊の課題となっている状況に鑑み（以下省略）

との記述があり、昨今のサイバー攻撃による被害の甚大さに対応しようとする意図が窺える。実際に、昨今発生しているサイバー犯罪には、経営や社会的な評価に多大な影響を及ぼす事案が発生している。

サイバーセキュリティの用語について 2008 年に発令された本土防衛のための米国大統領令 [7] では次のように言及している。

サイバーセキュリティとは、コンピュータ、電子通信システム及びサービス、有線通信、電子通信、及びその中の情報を含めて、これらの被害を防止、保護、復旧し、これらの可用性、完全性、認証の的確さ、機密性、否認不可を確実にすることである。

その他、NIST(National Institute of Standards and Technology) 提供の年間レポートやフレームワークにも本用語は頻出している。また、英国政府が国家的な情報セキュリティに関する戦略を策定した文書の題名も “National Cyber Security Strategy 2016 to 2021” となっており、この中でもサイバーセキュリティについて次のように言及している。

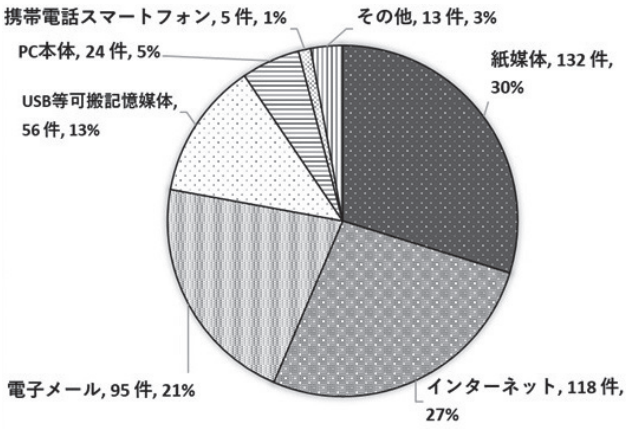
サイバーセキュリティとは情報システム (ハードウェア、ソフトウェア、関連する基盤構成)、その中のデータ、提供サービスを不正なアクセスや危害、誤使用から守るものである。ここでは意図的に引き起こされるシステムオペレータによる危害や偶発的に

セキュリティ手順を間違えた結果も含む。

Ⅲ　情報セキュリティ管理の保護対象

私たちが滞りなく情報を有効活用するためには、情報セキュリティ管理が前提となる。情報セキュリティの保護の対象を明確にして、それら各々が情報セキュリティの要求基準が満たされるように規約や管理手順を作成または体制を確立して、運用局面ではそれに従う。問題発生時は、回復措置によって問題解消に努めるが、法的拘束力の影響を受けることもある。これらは静的な管理サイクルではなく、環境条件や情報システムのサービス、関係する組織体制や人員構成によって動的な管理サイクルとしての対応が求められる。

図表１　媒体・経路別の個人情報漏洩件数



保護の対象となる情報は、個人情報や認証情報等を含む電子データ、印刷物の他に経営戦略上の資源となりうるようなIoTデータやAIの学習データ等の情報も対象となり得る。図表１は日本ネットワークセキュリティ協会がインターネットニュースなどで報道されたインシデントの記事、組織からリリースされたインシデントの公開記事などをもとに集計した媒体・経路別の個人情報の漏洩件数と割合である[8]。情報セキュリティから容易に電子データが連想されるが、個人情報については紙データを介した漏洩件数の割合が最も高く、電子メールやインターネットを介した漏洩は半数にも満たないことも留意すべきである。保護すべき対象の情報は個人情報保護法の改定[9]があれば変動するし、営業活動に有益な人の移動に関するデータが販売の対象となる[10]こともある。コールセンター等で顧客とのやり取りを音声データとして残す場合も個人が特定できるような内容であれば個人データになり得るし、音声による認証が一般的になると音声データ自体が個人情報として扱われる可能性も残る。何が保護の対象となるかは、法的な視点や組織の事業内容から常に見直しが必要である。

Ⅳ　情報セキュリティ管理の基本

情報セキュリティ管理は、保護の対象を選定した後、管理の方針と目標をセキュリティポリシとして明文化し、それに従い保護対象のレベルや組織単位の責任範囲をセキュリティスタンダードとして規定、セキュリティ管理を実現するための具体的な手順をセキュリティプロシジャとして文書化して[11]、それに従い日常の運用管理業を行う。セキュリティ

スタンダードやセキュリティプロシジャを策定する際には、サイバー攻撃の情勢を勘案して自組織の業務との関連性について注意する必要がある。

現代は情報社会から情報過剰社会と言われるが[12]、大量の情報から特に注意を要するものを選択する必要に迫られている。情報セキュリティ管理では機密レベルを設定して文書データを峻別することは一般的だが、包括的な認識だけでは問題が発生するケースがある。2017 年に国内の航空会社がビジネスメール詐欺によって、3 億 8400 万円の被害を受けた。当該メールの発信アドレスを確認すると、過去の発信メールアドレスと 1 文字異なっていた[13]。この変異に気付いていれば被害は防げたのである。当件とは反対に、南アジアの国立銀行が被害を受けたサイバー攻撃では経由銀行の銀行職員が振込先のスペルミスを発見することにより 10 億ドルの被害を免れたケースもある[14]。メールの発信元や振込先の指定の確認は日常的な定型業務であるが、事務処理量が膨大であったとしても、状況に応じて精査が望まれる。どの様なセキュリティ管理の規約・手順を定めるか、またそれが順守されているかによって被害状況は変わってくる。

2014 年に発覚した国内の教育サービス会社の個人情報流出事件では、環境上対策は施されていたが、不正検知のためのデバイス制御ソフトのバージョンが最新でなかった[15]が故に、システム開発に携わっていた関連会社の社員が大量の個人情報を含む PC に接続したスマートフォンを接続し、持ち出し可能であることを偶発的に発見することを発端とした事件であった[16]。名簿業者を介して他の教育サービスの会社に流出し、被害者からの通報で事態が発覚、事件によって会社の業績は落ち込み、2019 年も裁判は継続している。情報漏洩対策のソフトが各 PC に導入されており、組織として対策の意図はあったと考えられるが、一部の管理が徹底していなかったことや、関連会社の社員への過剰な信頼によるものか、情報システム環境の不備により結果的には経営に大きな損害を与えることになった。

情報セキュリティ管理は、その管理の対象も広範に亘るものであるが、些細な管理上の拙さが大きな影響を生むことがある。また、技術の変化や業務内容によって、管理対象や管理手順は変わってくる。以降の節では、情報セキュリティを管理する上で何が課題となるのか、いくつかの事例と共に考察を進める。

◆さらに学ぶための参考文献

・サイバーセキュリティと経営戦略研究会 編（2014 年）『サイバーセキュリティ』（NTT 出版）
・三宅功（2016 年）『CxO のための情報セキュリティ』（ダイヤモンド社）
・羽田卓郎・山﨑哲（2014 年）『ISO/IEC 27001 情報セキュリティマネジメントシステム構築・運用の実践』

[1] ISO (2013) "*ISO/IEC 27001:2013*" https://www.iso.org/standard/54534.html (2019 年 04 月 30 日アクセス)
[2] 情報処理推進機構「情報セキュリティマネジメントの規格や標準」
https://www.ipa.go.jp/security/manager/protect/pdca/standard.html (2019 年 08 月 27 日アクセス)
[3] 一般社団法人である情報マネジメントシステム認定センターが認定業務を行っている。「センター概要」 https://isms.jp/about/overview.html (2019/08/2 アクセス)
[4] 一般社団法人情報マネジメントシステム認定センター 「ISOIEC 27000 ファミリーについて」 https://www.jipdec.or.jp/smpo/u71kba000000jjgv-att/27000family_20190520.pdf (2019 年 08 月 27 日アクセス)
[5] 日本規格協会編 (2014) 「対訳 ISO/IEC 27001:2013 (JIS Q 27001:2014) 情報セキュリティマネジメントの国際規格」P.20
[6] e-Gov (2014)「平成二十六年法律第百四号 サイバーセキュリティ基本法」第一章 総則
[7] THE WHITE HOUSE(2008) " *NATIONAL SECURITY PRESIDENTIAL DIRECTIVE/NSPD-54 HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD-23"P.3 "Definitions*"
[8] 日本ネットワークセキュリティ協会 セキュリティ被害調査ワーキンググループ (2019 年)「情報セキュリティインシデントに関する調査報告書【速報版】」P.9「3.3 媒体・経路別漏えい件数」より引用
[9] 個人情報保護委員会事務局 (2016)「改正個人情報保護法について」 https://www.meti.go.jp/committee/kenkyukai/sansei/daiyoji_sangyo_chizai/pdf/003_02_00.pdf (2019 年 08 月 27 日アクセス)
[10] 市嶋 洋平 (2018)「データは隠さず売る 人流データは月 100 万円から」日経 XTREND
https://xtrend.nikkei.com/atcl/contents/technology/00003/00001/ (2019/09/21 アクセス)
[11] IPA「情報セキュリティマネジメントと PDCA サイクル」
https://www.ipa.go.jp/security/manager/protect/pdca/policy.html (2019 月 09 月 24 日アクセス)
[12] 秋山隆平 (2007) 「情報大爆発 コミュニケーションはどう変わるか」宣伝会議 P.11「第 01 章何が起きているのか」
[13]「アドレス 1 字違い見逃す 日航 3.8 億円メール詐欺被害」日本経済新聞 2017/12/22
[14] "*How a hacker's typo helped stop a billion dollar bank heist*" REUTERS (2016/03/10)
[15] 浅川 直輝 (2014)「ベネッセ事件容疑者はなぜスマホでデータを持ち出せたか、IT 部門は設定の再点検を」 日経 XTECH https://tech.nikkeibp.co.jp/it/atcl/news/14/072800239/ (2019/09/20 アクセス)
[16] 下級裁裁判例 「事件番号 平成 27(ワ)2486 事件名 損害賠償請求事件 裁判年月日 平成 30 年 12 月 27 日」東京地方裁判所