最近のセキュリティ脅威と対策の方向性 ――多角的アプローチから求める最適解

真　田　大　志

要　約　セキュリティ対策は「情報セキュリティ」から「サイバーセキュリティ」へと変化した。サイバーセキュリティには「技術的な対策」「人的な対策」が必要であり、それぞれの対策は相関関係がある。ネットワーク分離は効果的な技術的対策だが、これのみで脅威を防げるものではなく、多層的な防御が必要になる。多層防御で検知をしなければ、監視ができず、監視をしていてもスキルを持った要員がいなければインシデント時に対応ができない。そのための要員は育成する必要がある。これらの対策はどれかを選択するのではなく、すべてを多角的に組み合わせて実施しないと望む効果は得られない。

1. は　じ　め　に

2010 年代半ばに入り、セキュリティ対策は「情報セキュリティ」から「サイバーセキュリティ」へと変化している。情報セキュリティという言葉は、2000 年 1 月に発生した科学技術庁や総務庁統計局などのホームページ改ざん事件をきっかけに、セキュリティ対策の必要性が注目され、用いられるようになった。情報セキュリティポリシーの構築や ISMS 認証を取得する企業が増え、情報セキュリティ対策の機運が高まったのである。情報セキュリティは、企業内の電子データや紙文書を含む情報を対象とし、人的・物理的・技術的な対策で守ろうという考えで、企業内部の活動を中心としていた。

一方、サイバーセキュリティ対策は、ここ数年の標的型攻撃の増加を背景とした、重要インフラを含むサイバー空間のセキュリティ対策を指す。データ、システム、ネットワークの安全のために必要な措置をとり、維持管理することを、国が主導して法律として制定しているところが、情報セキュリティ対策との相違点である。

本稿では、2 章で情報セキュリティからサイバーセキュリティへの変遷と最新のセキュリティ脅威について、3 章でサイバーセキュリティ対策の概要、4 章で具体的なサイバーセキュリティ対策、5 章で多角的なアプローチについて述べる。

2.　情報セキュリティとサイバーセキュリティ

本章では、情報セキュリティの閉塞とサイバーセキュリティへの変化、最新のセキュリティ脅威について述べる。

2. 1　情報セキュリティの負の側面

2000 年を過ぎたあたりから、継続的に情報セキュリティの対策を維持向上するための仕組みである情報セキュリティマネジメントシステム（ISMS）の認証（ISO/IEC27001）[*1] 取得がブームになった。2016 年現在では約 5000 もの企業が認証を取得しており（図 1）[1]、官公庁事業の入札要件やアウトソーシングの要件にもなっている。ISMS は、セキュリティの管理の仕

組みを作るものである。具体的には、計画・実行・評価・改善の PDCA サイクル、すなわち情報資産の洗い出しとリスクアセスメントをして、対策を考えて実行して、評価（監査）をして、改善していくというような、管理の仕組みを中心とする。この ISMS の流行によって、多くの企業で認証取得やポリシー策定がなされ、セキュリティレベルはある程度まで向上した。

ただ、ISMS 認証は、技術的なセキュリティ対策レベルを求めるものではない。仕組みの構築とそれが機能するかは別問題であるにもかかわらず、ISMS 認証取得＝ゴールという認識が見受けられた。認証は年 1 回の審査を伴うが、そこでは「管理する仕組み」に質問が集中するため、準備の徹底が管理文書や承認プロセスなどに偏り、技術的な対策が疎かになる傾向があったと考えられる。

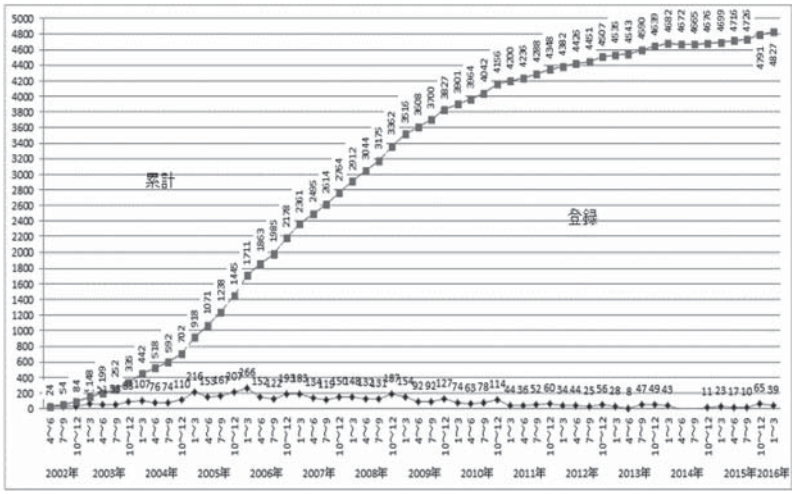

図 1　ISMS（ISO/IEC27001）認証取得組織数推移[1]

2. 2　サイバーセキュリティが重視される背景

セキュリティ脅威は、時代が進むとともに、フロッピーや USB メモリを介したコンピュータウイルス状のものから、インターネットのサイバー空間を介して直接企業に加えられる技術的な攻撃に変化してきた。これらの中には、企業の事業に大きな影響を与えるものもある。

以前は、企業の正規サイトは安全と考えられていたが、最近では企業サイトの表示広告の配信過程でウイルスが仕込まれ、閲覧者が不正サイトに誘導されるという事故が多く起きる*2。さらには企業内の重要なファイルを勝手に暗号化して、復号するのに金銭を要求するランサムウェアも増加している（図 2）[2]。

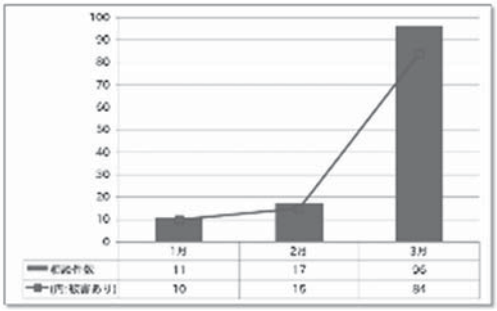

図2　ランサムウェアに関する相談の月別推移（2016年1月～3月）[2]

これらの攻撃は、情報セキュリティのアンチウイルス的な対策では対応が追いつかず、対抗することが難しい。それを背景とした技術的な対策が、サイバーセキュリティ対策である。世界の中で日本におけるサイバーセキュリティ対策が遅れており、攻撃が成功しやすいため標的となっているというレポートもでている[3]。

3.　サイバーセキュリティ対策とは

本章では、サイバーセキュリティ対策の基本となる部分について述べる。企業におけるサイバーセキュリティ対策は、ネットワークの形態とともに二つに分けられる。すなわちインターネット公開サーバの対策と、社内OA環境の対策である（図3）。オールマイティな対策はないため、脅威によって対策を検討する。

インターネット公開サーバは、ホームページやECサイトなど、外部に対してサービスを提供するサーバである。脅威には、DDoS攻撃によるサービス停止、SQLインジェクションなどによる情報漏洩が考えられる*3。

社内OA環境の脅威は、Webサイトやメール閲覧によるマルウェアやウイルス感染、USBメモリなどメディア経由の情報漏洩が考えられる。現在では最も多く標的とされ、企業の対策が進んでいない部分である。

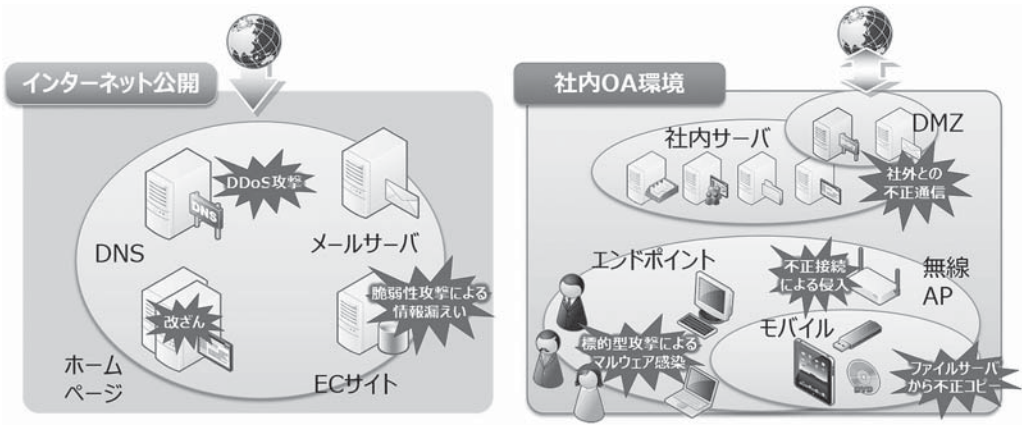

図3　ネットワーク形態による脅威

3. 1　社内 OA 環境のサイバーセキュリティ対策

社内 OA 環境は、インターネットへ単一のサービスを提供する公開系のサーバと違い、クライアントに様々な利用方法があるため防御（対策）することが難しい。インターネットへ接続し、Web サイトを閲覧することもあれば、メールで添付ファイルのやり取りをすることもある。業務システム、ファイルサーバ、中にはインターネットストレージを利用する企業もあるだろう（図 4）。これらのやり取りを安全に行うためには、それぞれに監視する機能が必要になる。

ファイルサーバには数千数万のデータが格納され、様々なユーザが使うため管理が複雑化する。また、クライアントにスマートデバイスをつないだり、無線 LAN につないだりするやり取りについても、アクセス制限や暗号化などが必要になる。このように様々な利用用途があるので、それぞれのところでそれぞれに対策をするのが難しい。

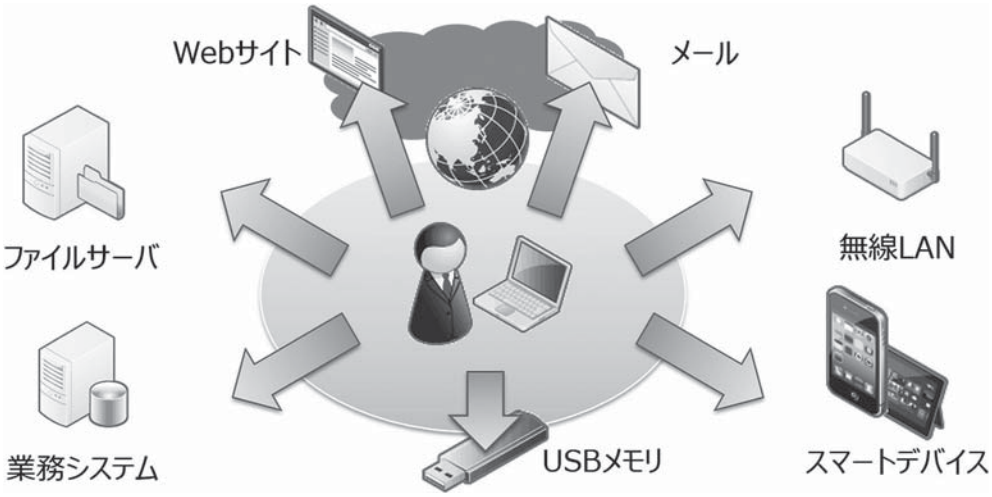

図 4　社内ネットワークのサイバーセキュリティ対策

3. 2　企業に対する官公庁の対応

対策が難しい OA 環境を持つ企業に対し、監督官庁はサイバーセキュリティ基本法に基づくサイバーセキュリティ戦略を受けたガイドラインを提示している。経済産業省は「サイバーセキュリティ経営ガイドライン」として、必要最低限の実施項目に絞って提示している。金融庁は金融検査マニュアル改正とともに、FISC[*4] の安全対策基準も改訂した。総務省からも情報通信白書においてサイバーセキュリティの重要性が述べられている。

3. 3　サイバーセキュリティ対策の組み合わせ

サイバーセキュリティ攻撃の特徴や、官公庁から提示されている対策を踏まえ、サイバーセキュリティ対策は、「人による対策（人的な対策）」と「技術的な対策」に分けられる。すなわち、新しい脅威に対応するためには、「人が行う対策」と「専用の機械などによる対策」を多角的に組み合わせて実施する必要がある（図 5）。

図5　サイバーセキュリティ対策の組み合わせ

4.　サイバーセキュリティ対策の方向性

本章では、サイバーセキュリティ対策の組み合わせとして挙げた「人的な対策」と「技術的な対策」の具体的な内容について述べる。

4.1　人的な対策

人的な対策とは、機械化できない対策であり普遍的なものである。「監視・分析」「インシデント対応」「人材育成」の三つが挙げられる。

4.1.1　監視・分析とインシデント対応

監視・分析は、次節で述べる多層防御による検知機能を用いて攻撃を監視し分析することで、攻撃の兆候や痕跡を発見することである。具体的にはファイアウォールやIPS[*5]、アンチウイルスによる検知とSEIM[*6]などによるログ分析を指す。検知機能は変遷するが、それを監視しないとアクションが起こせないため、監視する仕組みは変わらず絶対的に必要なものである。またアラートのひとつひとつを分析することも重要である。一定期間のアラートを相関的に見ることによって、インシデントの形跡や予兆を見つけることができる。

インシデント対応は、監視でアラートが発生した場合に誰がどのように対応するのかを決めておくことである。対応にあたる組織を最近ではCSIRT（Computer Security Incident Response Team、シーサート）と呼ぶ。

4.1.2　人材育成

人材育成には大きく「経営向け」「一般社員向け」「CSIRT要員向け」の三つがあり、対象によって人材育成の内容が変わってくる。経営向けは、経営資源の投入を判断するためのセキュリティ情勢や業種・業界動向など、一般社員向けは必要最低限のセキュリティ知識、CSIRT要員向けには少しレベルの高いセキュリティ知識、経験、能力が必要になる。

これらをすべて一企業の中で実現するのはコストがかかるので、高度な判断を行うCSIRT要員の社員数名を育成し、アウトソーシングをサポートの位置づけで利用することで、サイバーセキュリティ対策を無理なく実施することができる。例えば、単純な監視部分に使うSOC（Security Operation Center）や、高いスキルが必要とされるインシデント時のフォレンジック、要員育成時の講師などが代表的なアウトソーシング対象である。

4. 2　技術的な対策～多層防御

技術的な対策には二つあり、一つめは多層防御である。セキュリティ脅威には様々な種類があるため、それらを入り口、内部、出口にて多層的に防御する必要がある（図 6）。入り口ではファイアウォールや侵入検知システム（IPS）、各種フィルタ、内部ではクライアントのエンドポイントでのウイルス対策や情報漏洩対策（DLP：Data Loss(Leak) Prevention）の製品およびソリューション、出口では誤送信防止や標的型攻撃への対策を施す。対策を無力化する新たな攻撃が生まれ、さらに新たな対策が必要となる、いわばイタチごっこの様相だが、検知しないことには攻撃や感染の有無さえ分からない。脅威の種類を把握し、効果的な対策に重点を置くのが、多層防御のポイントである。

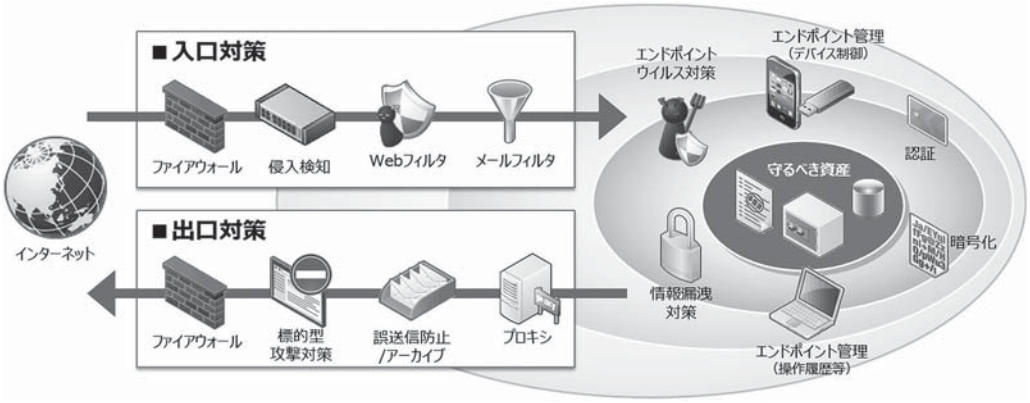

図 6　多層防御

4. 3　技術的な対策～ネットワーク分離

技術的な対策の二つめはネットワーク分離である。インターネットから入ってくる脅威をやみくもに排除するよりも、インターネット側に重要な情報を置かないことで、被害を最小限に留めるという発想である（図 7）。官公庁、地方自治体、独立行政法人や金融機関は、インターネットを分離し、決定的な対策とすることを打ち出している。これは重要なデータを含む基幹ネットワークと、インターネットを利用するネットワークを分離することで侵入を防ぐことを目的としている。攻撃の高度化によりインターネット接続されている部分は侵入されることを前提とし、その場合に重要なデータを守ることを最優先とする考えである。ネットワーク分離にはいくつかの方式がある。

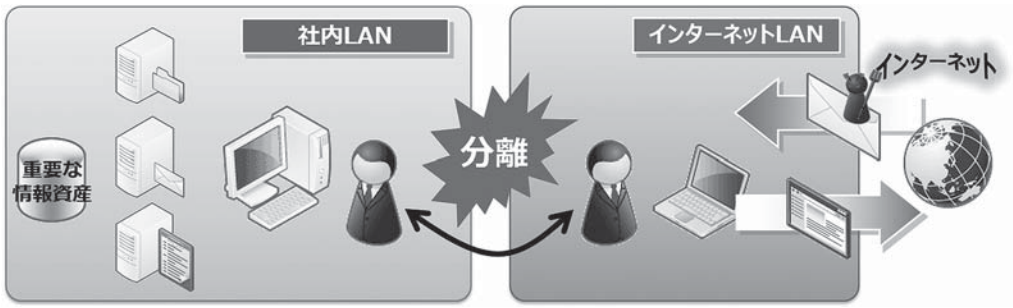

図7　ネットワーク分離

4.3.1　物理分離と論理分離

一般的なインターネット接続環境では、業務システムやファイルサーバにアクセスできる端末がインターネットにも接続可能で、Web サイトの閲覧やメールの送受信ができる状態である（共存。図8左）。それに対し、インターネット接続側と社内 LAN を物理的に分離すれば、確実にネットワーク分離が実現できる（図8中央）。しかしこの方式では社内の基幹ネットワークとインターネット（社外）とのデータ交換ができなくなるし、社内外の両方を見ようとすると端末が2台必要になるため、限られた業種にしか適用できない。そこで、これを緩和した方式が論理分離である（図8右）。ネットワークを論理的に分離し、基本的には相互の通信をできなくするが、一部の限定された通信は許可し、セキュリティと利便性のバランスをとる。

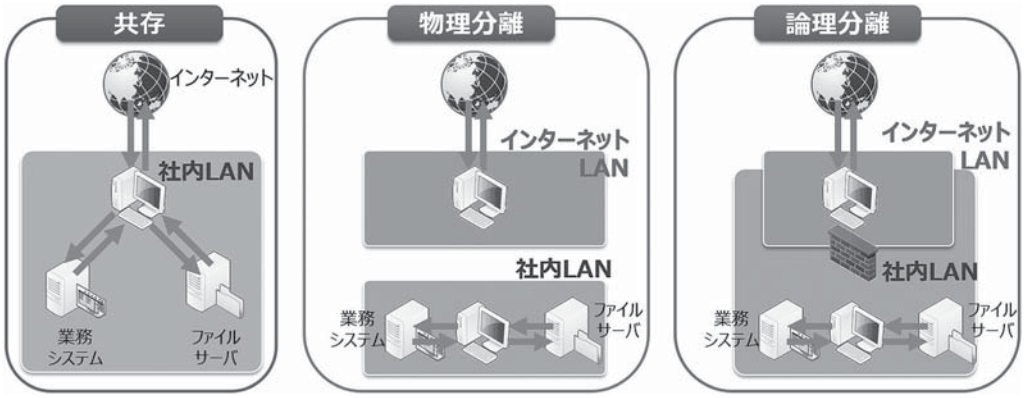

図8　物理分離と論理分離

4.3.2　論理分離の例

論理分離の例を二つ挙げる。一つめはインターネット分離である（図9左）。インターネット側の LAN と社内 LAN の間の通信を限定し、インターネット LAN にある仮想クライアントの画面のみを社内 LAN 端末に転送することで、ウイルス感染や侵入を防ぐことができ、端末も1台で賄える。ただし、ファイル交換については無害化対策が必要になる。交換するファイルフォーマット（データ部、プロパティ領域などの位置）を限定し、それにそぐわない（怪しい）スクリプトなどを削除する。こういった操作を加えることで、外からのデータを安全に社内に持ち込むことができる。

もう一つは重要システムの分離である（図9右）。マイナンバーを始めとする個人情報や経営情報など、社内でも機密性の高いシステムのサーバとクライアントに、特殊なネットワークドライバを導入して論理的に隔離し、他の端末からは見えなくする方法である。ランサムウェアやウイルスが社内に侵入しても、保護対象システムのデータ破壊や漏洩を防ぐ。

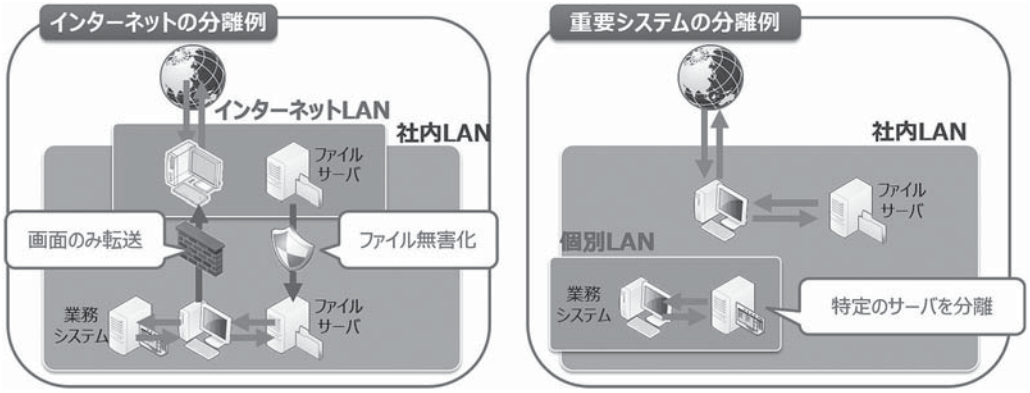

図9　インターネット分離と重要システム分離

4.3.3　ネットワーク分離のまとめ

ネットワーク分離の各方式のメリット・デメリットを表1にまとめた。

表1　ネットワーク分離の各方式のメリット・デメリット

分離方式		メリット／デメリット
物理分離		■ インターネットからの侵入を完全に防ぐことが可能 ■ 社内LAN側のOS/APのパッチ更新、ウイルスパターンファイル更新を考慮する必要あり
論理分離	インターネットの分離	■ 端末統合による利便性向上（1人一台の端末でよい） ■ 構成の複雑化による運用負荷の増大 ■ 業務形態によってはクライアント仮想化の導入コスト増大
	重要システムの分離	■ インターネットからの侵入をほぼ完全に防ぐことが可能 ■ 現状のネットワーク構成からの移行が容易 ■ システム間連携がある場合には考慮が必要

物理分離は当然一番安全であり、インターネットからの脅威は完全に防ぐことができるが、OSやアプリケーションのパッチ更新ができないなど考慮すべき事項は多く、業務に少なくない影響を与える。インターネットとは完全に分離されていても、USBメモリやCD-ROMから感染する恐れもある。

インターネットの分離については、安全性が向上し利便性も保つが、新しい仕組みの導入によるコストが発生し、構成の複雑化による情報システム部門の負荷が増える。

重要システムの分離は、現状のネットワーク構成から移行が容易という特徴があり、重要データだけを守るには効果的な方法である。ただし他のシステムとのシステム間連携がどの程度あるのか、等の要件を整理する必要がある。

このようにネットワーク分離は効果が高いものの、守りたい対象や現状のネットワーク構成等を踏まえて導入を検討する必要がある。

5. サイバーセキュリティ対策のまとめ

ここまでサイバーセキュリティに必要な「技術的な対策」「人的な対策」を述べたが、それぞれの対策は相関関係がある。ネットワーク分離は効果的な対策だが、これのみで脅威を防げるものではなく、多層的な防御が必要になる。多層防御で検知をしなければ、監視ができず、監視をしていてもスキルを持った要員がいなければインシデント時に対応ができない。そのための要員は育成する必要がある。したがって、これらの対策はどれかを選択するのではなく、すべてを多角的に組み合わせて実施しないと望む効果は得られない（図 10）。

また、業種・業界・企業規模・ワークスタイルによって最適なセキュリティ対策は変わってくる。在宅勤務、外回りが多い業務、IoT を実践している、PCIDSS[*7] や ISO27001 ガイドラインに沿う必要があるかなど、さまざまな環境がある。在宅勤務やモバイル機器の社外持ち出しが多い企業であれば、ネットワーク分離に加えて VPN を考慮したネットワーク設計が必要になる。取り扱うデータの重要度からより厳密な管理が求められる業種であれば、ネットワーク設計も相応して厳密になる。また、金融機関であれば金融検査マニュアルや FISC 安全対策基準に対応する設計が、流通業界であれば PCIDSS に対応する設計が必要になる。

図 10　多角的アプローチ

6. お わ り に

本稿は、2016 年 6 月に東京で開催された日本ユニシスグループの総合展示講演会「BITS2016」の講演内容を文書化したものである。日本ユニシスグループは、様々な業種、業界の顧客へのセキュリティ対策の支援の中で、多くの知見を得てきた。その知見を基に、顧客に最適なセキュリティ対策をこれからも提案していく所存である。

＊1　ISMS（Information Security Management System）適合性評価制度とは、情報資産を様々な脅威から守り、リスクを軽減させるための総合的な情報セキュリティ・マネジメントシステムである。2005年10月にISMS認証基準として国際規格ISO/IEC 27001：2005が発行された。
＊2　Webサイトの右端などに表示される広告は、サイト自体が提供しているのではなく、広告代理店や業者が作っている場合が多い。その広告は様々なサイトに配信されるため、それにウイルスを仕込むことによって、感染被害の発生が拡大している。
＊3　インターネット公開サーバは、外部データセンタへ預けたり、クラウドサービスを利用するなどアウトソーシングすることが多くなったため、セキュリティ対策もアウトソーシング先で実施することが多くなった。特にDDoS攻撃などは企業側での対応が難しいため、ISP側での対策が必要となる。
＊4　公益財産法人金融情報システムセンター（FISC：Center for Financial Industry Information Systems）。
＊5　IPS：Intrusion Prevention System/侵入防止システム。サーバやネットワークの外部との通信を監視し、侵入の試みなど不正なアクセスを検知して攻撃を未然に防ぐシステムのこと。
＊6　SIEM：Security Information and Event Management.サーバーやネットワーク機器、セキュリティ関連機器、各種アプリケーションから集められたログ情報に基づいて、異常があった場合に管理者に通知する仕組み。
＊7　PCIDSS：Payment Card Industry Data Security Standard.クレジットカード情報および取り引き情報を保護するための国際的なセキュリティ基準。

参考文献　［1］　認証取得組織数推移グラフ，情報マネジメントシステム認定センター（JIPDEC），2017年2月，https://www.isms.jipdec.or.jp/lst/ind/suii.html
［2］【注意喚起】ランサムウェア感染を狙った攻撃に注意，独立行政法人情報処理推進機構（IPA），2016年4月，https://www.ipa.go.jp/security/topics/alert280413.html
［3］　2016年第3四半期　セキュリティラウンドアップ，ドレンドマイクロ株式会社，2016年11月，P26，
http://www.trendmicro.co.jp/jp/security-intelligence/sr/sr-2016q3/index.html

執筆者紹介　真　田　大　志（Hiroshi Sanada）
大手データセンタにおいてネットワークの構築・運用業務に従事後、セキュリティ専門企業にて情報セキュリティ脆弱性診断業務・不正アクセス監視業務を経て2006年に日本ユニシス入社。現在は、企業におけるCSIRT構築支援、セキュリティアセスメント、セキュリティ監査等のコンサルティング業務に従事。公認情報セキュリティ主任監査人。