サイバー攻撃と情報セキュリティ

杉野　隆

インターネットの普及とは，利用人口の量的拡大だけでなく，利用形態の高度化・深化を意味する．その結果，現在，社会経済や国民生活のさまざまな側面で質的変化が起きている．この質的変化の中に，負の側面としてインターネットを利用した犯罪（サイバー攻撃）の増加がある．本稿では，インターネットが安全・安心・強靭であるべき社会をどのように脅かしているのかについて解説する．まず，企業や組織を対象に，サイバー攻撃とは何か，サイバー攻撃に関する最近の事例，歴史，統計データにみる実態，インターネットの利用形態の多様化に伴う防御方式の変化などを解説し，今後に情報セキュリティを確保するための対策のあり方について卑見を述べる．

キーワード：サイバー攻撃，情報セキュリティ，サイバー空間，標的型攻撃，DDoS 攻撃，境界化，脱境界化

1.　サイバー空間とサイバー攻撃

筆者らは，OR 学会 40 周年記念事業の一環として，2001 年に『ネット情報セキュリティ』という訳本 [1] を出版した．しかし，この本にはサイバー攻撃という用語はまだない．2000 年代の初頭から使われている．

サイバー攻撃はサイバー空間 Cyberspace で行われる．ウィリアム・ギブソンは 1982 年に著した短編小説『クローム襲撃（原題：Burning Chrome)』で，人間の神経系を直接コンピュータに接続し，人間の身体知覚と電子メディアが接合して生まれるメディア環境（電脳空間）に自在に侵入するスーパーハッカーを描いた．さらに，1984 年の『ニューロマンサー（原題：Neuromancer)』でも使用して有名になった．これだけであれば SF の世界で終わるが，インターネットの圧倒的な普及を通じて多くの人が話題にするようになった．われわれは，銀行の ATM のようなメインフレームコンピュータによるオンラインサービスが一般的に提供され始めた 1980 年代からサイバー空間に慣れ親しむようになった．Yahoo!，Google，Facebook などの Web サイトは，インターネット上に形成されたコミュニティであり，サイバー空間が人と人の絆を形成し，個人の疑問・悩みごとや地域問題を解決するなど，実空間 Real space に貢献している．われわれは，メディアによる人間拡張の最終相に近づいた [2] といえる．ただ，サイバー空間における人々の規範意識は未だ実空間よりも低いことも現実である．インターネットの普及は良くも悪くもサイバー空間を質的に変えてしまった．

サイバー攻撃は，情報セキュリティマネジメントシステム (ISMS) に関する用語集である ISO/IEC 27000 における情報セキュリティの定義に従って，「情報資産（情報，ハードウェア，ソフトウェア，物理的施設，無形資産など）の情報セキュリティを損なうコンピュータ同士の攻撃」と定義できる．

「サイバーセキュリティ」という用語が最近急速に広まってきたが，これは 2014 年 11 月に「サイバーセキュリティ基本法」が制定されたことによって政府，自治体がそれに習うようになったからであろう．同法第二条はサイバーセキュリティを，「デジタル情報の安全性及び信頼性の確保のために必要な措置が講じられ，その状態が適切に維持管理されていること」と定義している．一般に，情報セキュリティ概念では，アナログ情報（われわれが直接感知できるのはアナログ情報のみである）もディジタル情報も対象にしているのに対し，サイバーセキュリティではディジタル情報のみを対象としており，対象範囲が狭いと思われる．

主なサイバー攻撃は表 1 のように分類できる．本稿では，このうち，現在多発している標的型攻撃，DDoS 攻撃をとり上げる．

2.　サイバー攻撃の最近の事例

2.1　日本年金機構の情報漏えい事件

日本年金機構（以下，機構）が大量の年金個人情報を流出させた事件は，2015 年 6 月に報道され大きな反響を呼んだ．機構はその前月 5 月 8〜20 日の間に何者かから 124 通の標的型メール攻撃を受け，機構の職員 5 名が添付ファイルを開封した．その結果，機構内で

すぎの　たかし
国士舘大学
〒 154–8515　東京都世田谷区世田谷 4–28–1
takashi@suginosan.net

表 1　サイバー攻撃の種類

対象システム	攻撃対象／攻撃目的	特定	不特定	攻撃目的の例
エンタプライズ系システム	機能妨害・破壊	DoS/DDoS 攻撃	ウイルス感染	組織運営妨害，風評被害，ハクティビズム，テロリズムなど
	データ窃取，破壊・改ざん（不正アクセス）	標的型攻撃，管理者権限乗っ取り	DoS/DDoS 攻撃の準備	愉快犯，ハクティビズム，諜報活動，先端技術・個人情報の窃取
制御系システム	機能妨害・破壊	ウイルス感染	未詳	重要インフラの機能妨害・破壊

DoS: Denial of Service（サービス妨害），DDoS: Distributed DoS（分散型 DoS）
重要インフラ：情報通信，金融，航空，鉄道，電力，ガス，政府・行政サービス（地方公共団体を含む），医療，水道および物流の各分野における社会基盤をいう．
ハクティビズム：社会的・政治的主張のために行うハッキング行為．「アノニマス」がよく知られている．

計 31 台のパソコン (PC) がウイルスに感染したうえ，5 月 21〜23 日の間に約 125 万件の年金個人情報を流出させた．このうち 55 万件のデータにはパスワードが設定されていなかった．機構は，内閣サイバーセキュリティセンター (NISC[1]) から厚生労働省年金局経由で「不審な通信を検知した」との通報を受けて情報の流出を知り，該当端末を特定して機構 LAN から切り離すことを繰り返したが，5 月 23 日にやっと情報流出が止まった．機構は 6 月 1 日にこの事件を公表した．絵に描いたような標的型攻撃の顛末であった．

その後，厚生労働省や第三者委員会の調査報告書を通して，情報の機密性を確保するために情報系システムから切り離された基幹系システムで管理されている年金個人情報を，機構内の業務手順として，情報系システムの共有フォルダにコピーして使用していたことが，年金個人情報が窃取された直接の原因であることが判明した．業務上の必要性を理由に，当初のシステム設計に反する運用がなされていたわけである．これが情報セキュリティの脆弱性につながった．さらにその背景にある，情報セキュリティインシデントへの幹部の問題意識の甘さ，標的型メールの受信時の対応について具体的なルールが規定されていないなど，運用管理体制，職員の情報セキュリティ意識，組織文化に関する問題点などが指摘された．

標的型攻撃は，2010 年 1 月に，米国の Google 社などに対する Operation Aurora 事件によって大きな話題となった攻撃手法であり，日本でも 2011 年 9 月に，三菱重工業，川崎重工業や，衆参両院などに対する攻撃が報道され，広く知られるに至った．機密情報や個人情報の流出への懸念から，各組織では情報資産の情報セキュリティの確保に向けた対策の強化に乗り出していたはずであった．

機構内では，124 通も送られてきた標的型攻撃メールを開いたのは，わずか 5 名であった．多くの職員は不審なメールであることを見抜き被害を回避していた．問題は，回避した職員がそのことを誰にも告げず，もしくは無視していたこと，その結果，機構内における情報共有ができなかったことである．また，当初のシステム設計に起因する使いにくさを，システムそのものの改善ではなく，運用上の「工夫」によって「使いやすく」する対処が，結果的に情報セキュリティ侵害を手助けすることになった．業務設計，システム設計によって作り上げたルールや仕組み，それに基づくシステム運用環境が業務遂行に合っていない場合などに見られるこのような「工夫」は，リスクとして情報システムに埋め込まれてしまった．

2.2　DDoS 攻撃の集中砲火

2007 年 4 月に，エストニアで，ロシア系住民による暴動の発生に合わせたかのように，大規模な DDoS 攻撃がエストニア政府機関，報道機関，銀行などの Web サイトに仕掛けられ，Web サイトが次々にダウンした．エストニアは電子政府化の最先端を走っているので，それが裏目に出て，国民の生活インフラ全体が麻痺した．国家全体を標的にした大規模サイバー攻撃の世界最初の事例といわれる．

2015 年 10 月に国際的ハッカー集団アノニマスが，日本の古来の風習であるイルカ漁に反対するために，日本の多くの Web サイトに立て続けに DDoS 攻撃を加えてきた．対象となったサイトには，太地町（3 回），The Japan News（読売新聞海外版），成田国際空港および中部国際空港，日本政府観光局，日本郵政，ぷらら，太地漁協，日本捕鯨協会，高野町，九度山町，全日本運輸産業労働組合連合会，日本捕鯨協会，株式会社サイプレス，ASCII.jp などがあった．これらのサイトでは一般のアクセスを受け付けられなくなってしまった．なぜかイルカ漁に関係なさそうなサイトも含まれていた．

[1] National center of Incident readiness and Strategy for Cybersecurity

2.3 Tokyo 2020 に向けて

2012 年のロンドン五輪は，「the first digital Olympics」と呼ばれたが，加えて「情報セキュリティの確保」がキーワードとして掲げられ，大会の運営上不可欠な要素として位置づけられた．17 日間の開催期間中に情報セキュリティに関わるインシデントが 1 億 6,500 万回も発生した．その大半はパスワードが変更されるとかログインに失敗するといった軽微なものであったが，オペレーションセンターの最高情報責任者 CIO に報告された重大なサイバー攻撃が 6 件あったという．イギリスはそれまで 6 年がかりで情報セキュリティ対策を実施してきたが，開会式当日の未明になって，オリンピックスタジアムなどの電力供給の監視制御システムが最大のサイバー攻撃を受けた．予備発電機の起動には 30 秒かかるが，開会式最中にこのシステムがダウンすると，わずかの時間でも停電となり大会の評判を大きく損なう．そこで，万が一に備えあらかじめ手動で予備発電機を回し始めた．

日本の情報セキュリティ関係者の現在の最大関心事は，2020 年の東京オリンピック・パラリンピックにおけるサイバー攻撃をいかにして防ぐかということである．

3. サイバー攻撃の歴史

初期のインターネットは，メインフレーム同士をオープンなプロトコルによって接続し，コンピュータ間で情報を交換することのみを目的としていたので，情報セキュリティへの配慮は必要なかった．

しかし，1980 年代半ばから，PC がサーバ（UNIX，Windows などの非メインフレーム系）に接続され，クライアント・サーバ形態を構成するようになった．この形態は，構築の容易さとコストを低減できることから普及した．PC にインストールされているアプリケーションは，データベースサーバなどにアクセスして必要なデータをダウンロードし処理を実行する．しかし，サーバに比べ PC のほうが情報セキュリティの脆弱性が高いので，攻撃を受けるとインシデントを起こしやすい．

マルウェア[2]は，1970 年に初登場したが，1980 年代になってメールを利用したマルウェアが着実に増え，「コンピュータ・ウイルス」という言葉が一般化した．当時は愉快犯による攻撃であったが，1995 年のインターネット元年を境にウイルスによる攻撃が大流行した．2000 年代に入って手口は巧妙化し，さまざまなサイバー攻撃手法が開発されるようになった．守る側の防御技術の強化とのイタチごっこの中でサイバー攻撃は多様化・巧妙化し，また攻撃対象も多様化した．

サイバー攻撃の目的も，初期の知的好奇心や悪ふざけから政治的主張を目的としたハクティビズム，そして 10 年ほど前からは金銭目的のネットバンキング犯罪，情報窃取を目的とする標的型攻撃へと変化した．

従来の犯罪と比較した場合のサイバー犯罪の特徴として，次の 3 点がいわれる．

- 犯罪実行者の特定が困難
  サイバー攻撃の実行者は，第三者のコンピュータを「踏み台」にし，自分の身元を隠して犯罪を敢行することが可能である．
- 被害が潜在化する傾向
  ディジタル情報は不可視であり，不正アクセス行為を受けたり，ウイルスに感染したりしている事実に被害者自らが気づかないことが多く，被害が潜在化する傾向がある．
- 国境を越えて容易に実行が可能
  実行者自身の PC がインターネットにアクセスできれば（現在は常時接続が当たり前），国境を越えて容易にかつ瞬時にサイバー犯罪を敢行することが可能である．

これらは，インターネットの特徴に由来するものである．われわれは，一方でこの特徴を享受しながらも，サイバー空間内ではサイバー攻撃と共存していかねばならない．

4. 統計データにみるサイバー攻撃の実態

サイバー攻撃に関する統計データはさまざまな機関から発表されている．警察庁（犯罪），総務省（情報通信），情報処理推進機構 (IPA)・産業経済省（情報技術），金融庁などは，それぞれの組織の根拠法令ないし事業目的に従って発表している．また，セキュリティベンダも製品販売と関連させ，あるいはより一般的な調査の結果と組み合わせて動向を分析し提供している．このため，サイバー攻撃の全体像はつかみにくい[3]．こ

[2] コンピュータ・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（悪意のコードまたは悪意のソフトウェア）と呼ぶ．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，自動的に不正送金を行う高度なウイルスも登場している．

[3] IPA から毎年発行される情報セキュリティ白書 [3] は，全体像をつかむのに参考になる．

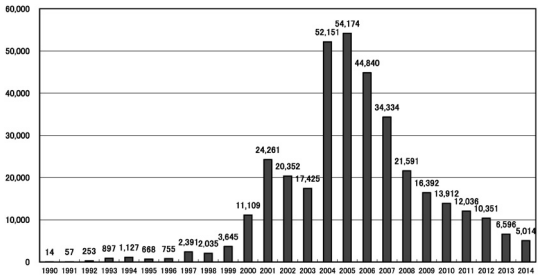

図 1　コンピュータ・ウイルス届出状況 (IPA)

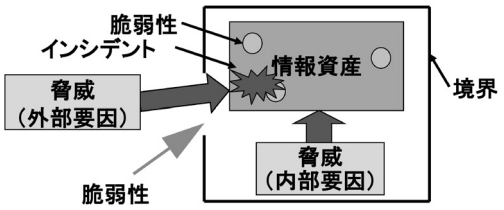

図 2　境界防御モデル

こでは，いくつかの指標について紹介する．これらの統計，報告書は各 Web サイトから入手できる．

(1) サイバー空間の人口（人口普及率）

国勢調査のような全数調査は行われていない．総務省の『通信利用動向調査』が，サンプリング調査を基に，各年 12 月末時点のインターネットの利用者数を推計している．1997 年以来の利用者数，人口普及率，利用企業数，企業当たり利用率の推移がわかる．2014 年 12 月末現在，人口普及率は 82.8%である．

(2) マルウェアの種類

セキュリティベンダ各社は，マルウェアを検知するためにそのパターンや挙動の特徴を抽出してシグネチャとして蓄積している．ウイルス対策ソフトに記録されるウイルス定義ファイルは，これらシグネチャを基に作成される．大手ベンダ Intel Security の McAfee Labs の DB に登録されているシグネチャの種類は，2015 年第 2 四半期において 4 億 3,300 万件を超え，この四半期間に 4,600 万件増加したという．5.9 件／秒の率で発生していることになる．

一方，PC に登録されるウイルス定義ファイル数は，2000 年には新しいシグネチャが 1 日当たり 5 個しか必要ではなかったが，2010 年には 1 日当たり 13,300 個が必要となったという．

(3) コンピュータ・ウイルス

ウイルスに感染した企業から IPA に届けられた件数が発表されている．2005 年にピークを記録した後，2014 年の 5,014 件にまでつるべ落としに減少している（図 1）．しかし，これはウイルス感染を気にする必要がなくなったということではない．自身の複製をメールの添付ファイルとして拡散させるという従来のマスメール型ウイルスから，攻撃者が明確な意図を持ち，特定の組織・個人を狙う「標的型攻撃」の増加が目立つようになったので，届け出件数が減少した．

(4) 情報セキュリティインシデントの発生状況

望まない単独または一連の情報セキュリティ事象の内で，事業運営を危うくするまたは情報セキュリティを脅かす確率が高い事象を情報セキュリティインシデントという（図 2）．一方，情報システムまたは組織に損害を与える可能性があるインシデントの潜在的な要因を脅威（外部要因と内部要因がある）という．脅威が情報資産の脆弱性に付け込み，その結果，可能性に伴ってインシデントが発現し，組織に損害を与える．

IPA は，業種別・従業員数別に無作為に抽出した 13,000 社の企業が認識した情報セキュリティ事象に関する被害状況を調査し，被害発生の原因および有効な情報セキュリティ対策，組織体制，投資額などを含めた実態を『情報セキュリティ事象被害状況調査報告書』として発表している [4]．被害にあった企業が，風評被害を気にして報告しなければ統計には出てこないが，最近は報告される事例が多いという．対象とするインシデントには，コンピュータ・ウイルスおよびサイバー攻撃（ウイルス以外）による被害件数と被害額がある．たとえば，2013 年度では，ウイルスに遭遇（感染または発見）した企業は 70.3%におよび，サイバー攻撃に遭遇（被害の有無を問わず）した経験のある企業は 19.3%，内部者の不正による被害のあった企業は 1.6%であった．サイバー攻撃の手口に関しての調査結果を図 3 に示す．DDoS 攻撃と標的型攻撃が多いことがわかる．サイバー攻撃の手口で最も多いのは，DoS 攻撃 (43.2%) であり，次いで標的型攻撃 (30.4%) である．脆弱性（セキュリティパッチの未適用などが原因）を突かれたことによる不正アクセス (15.8%)，SQL インジェクション (9.2%) がそれに続く [3]．

(5) サイバー事故

警察庁は，事件性のある事象に関心がある．警察庁は，一般の事件と同様に，サイバー犯罪[4]の検挙件数，ネットワーク利用 (93%)，コンピュータ・媒体対象，不正アクセス，標的型メール攻撃，サイバー空間にお

[4] インターネットを利用した犯罪やコンピュータまたは電磁的記録を対象とした犯罪などの情報技術を利用した犯罪をいう．

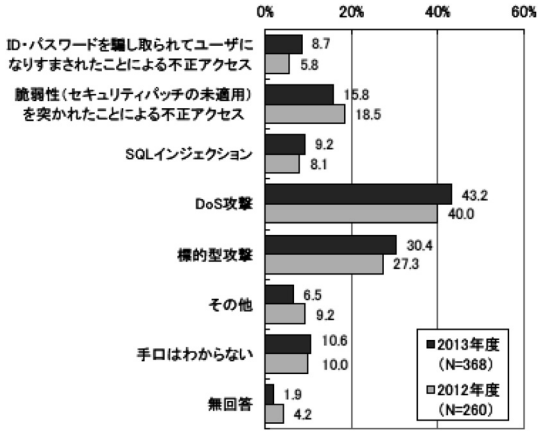

図 3　サイバー攻撃の手口（2012 年度調査との比較）

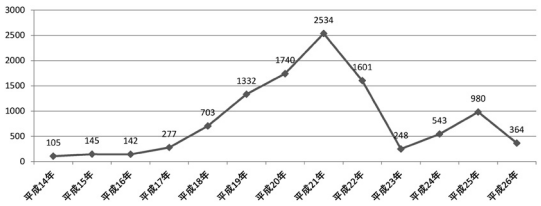

図 4　不正アクセス禁止法違反検挙件数（警察庁）

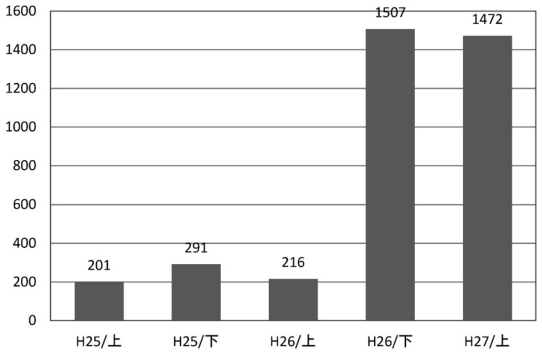

図 5　標的型メール攻撃の件数（警察庁）

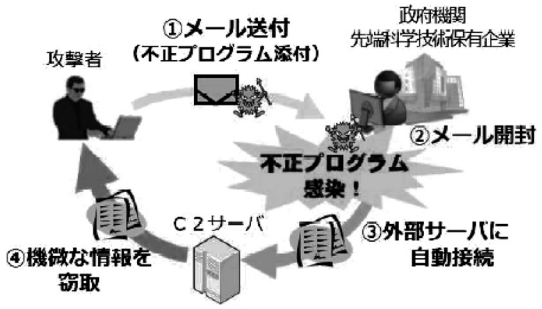

図 6　標的型メール攻撃の仕組み[6]

ける標的候補の探索行為（不審なアクセス[5]）などの統計を『サイバー空間をめぐる脅威の情勢について』として半期ごとに発表している．

① 不正アクセス

不正アクセスの目的は，機密情報・個人情報を窃取するか，パスワードなどの個人認証情報を窃取して，ショッピングサイトでの不正購入や (6) に述べる預金の不正引き出しを行うことである．元の勤務先の社内ネットワークにアクセスして，あるいは自身の本来の権限を超えてアクセスして機密情報を盗み出す，といった手口も多い．2009（平成 21）年には，ユーザ ID ／パスワードをフィッシングサイトから入手したケースが 2,084 件も発生し，ピークを記録した（図 4）．

IPA も，不正アクセスの被害を受けた場合の届出を受け付けている．

② 標的型攻撃

2014（平成 26）年下期に急激に増加した（図 5）が，日本年金機構を始め，多数の団体，機関，事業者などでサイバー攻撃による情報窃取などの被害が発生している．2015（平成 27）年上期に 1,472 件発生した．

標的型メール攻撃のプロセスを図 6 に示す．

標的型攻撃では，攻撃者は，攻撃準備―初期潜入―攻撃基盤構築―システム調査―攻撃最終目的の遂行，というように潜在化したプロセスを経て，ウイルス付きのメールを送付する（図 6 中①）．標的のメールアドレスは，インターネット上で公開されていないものが全体の約 9 割を占めている．攻撃者は攻撃対象の組織や職員について調査し，探索行為を行って，本物と見紛うようなメールを非公開アドレスに対して送付する．標的はその巧みさに騙されてメールを開封してしまい，ウイルスに感染する（図 6 中②）．ウイルスは標的に気づかれずに外部サーバに接続し（図 6 中③），機微／機密情報を攻撃者に送付する．このようにして情報が窃取される（図 6 中④）．

この攻撃は，現在は一層巧妙化しており，警察庁は「不審なメールを安易に開けず，最新のセキュリティ対策を講じてほしい」と呼びかけている．しかし，攻撃者は受信者がつい開いてしまうような巧妙なだましの手口を使ってくるので，完全に防ぐのは不可能であろう．

[5] 脆弱性をもつ Web サイト，不正アクセスの踏み台に使えるサーバなどを発見するためにさまざまな Web サイトにアクセスを繰り返す行為．

[6] http://www.nishinippon.co.jp/nnp/national/article/195718

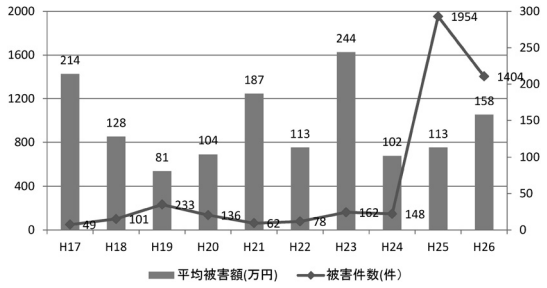

図 7　インターネット・バンキングによる預金等不正払戻しの件数と平均被害額（金融庁）

(6) インターネット・バンキングによる預金等不正払戻し

金融分野に関しては，金融庁も統計を発表している（図 7）．犯人がインターネット・バンキング利用者のユーザ ID やパスワードなどの認証情報を何らかの手口で窃取し，窃取した認証情報を利用して，預金者本人の預金口座から資金を移動させるものである．手口としては，スパイウェア，フィッシング，Man-in-the-Middle (MID) などが使用されている．

5.　サイバー攻撃の防御方式の変化

5.1　境界防御

江戸時代に，幕府は，関東の江戸まわり関所（箱根，新居，気賀など）を設け，西国からの敵の侵入を防いだ「入り鉄砲出女」という入口／出口対策をとっていた．鎖国政策でも，長崎出島という一点に絞った入口／出口対策が成功していた．

従来の情報セキュリティ対策の基本も，インターネットとの境界（図 2）にファイアウォールなどのセキュリティ製品を設置し，インターネットと組織内ネットワークを非武装地帯 (DMZ) で分離するという境界防御であった．アクセス制御，パスワードによって外部脅威からの脅威を防止（さらには抑止）し，万が一この防御線を破られたら早期に検知し回復させる予防―検知―回復モデルを前提する予防中心の対策によって内部に存在する情報の CIA（機密性，完全性，可用性）を確保できた．ISMS の概念が確立した 2000 年前後においては，外部（あるいは内部）からの脅威は，せいぜいマルウェア，不正アクセス程度であったので，これで対策としては足りていた．

5.2　脱境界化

企業情報システムは，地理的に拡大した取引先，顧客と情報ネットワーク接続を行っている．あるいは，従業員が出先において，モバイル PC からインターネットを介して本社のサーバにリモートアクセスする，従業員が私用のモバイル機器（スマホやタブレット端末）をオフィスに持ち込んで，社外／社内の制約なく自社のサーバにアクセスする BYOD (Bring Your Own Device) などが普及してきた．また，USB メモリなどの可搬型デバイスの社内への持ち込みもある．クラウドサービスでは，境界がどこに存在するか不明な状況にある．結果として，企業情報ネットワークのシステム境界は常に流動して，Borderless System となる．

境界防御により情報資産へのアクセスを保護していても，そこに至る侵入経路と手段を知られてしまえば，従来のような対策で攻撃の影響を回避することは難しい．また，内部不正によって従業員・業務受託者が情報資産のコピーを持ち出すという攻撃を受けることも多くなっている．現在では，Internet Data Center，クラウドサービスを利用するなど，情報資産が自らの管理下の施設から飛び出し，企業ネットワークの物理的境界をないものにしている．このため，情報セキュリティのリスクに対する考え方を改める必要が生じてきた．

このような状況を考慮すると，組織内のあるレベルまでの侵入は許しつつも，情報資産へアクセスの手前で攻撃を検知したり，情報資産の持ち出しを阻止する多段防御のような仕組みが必要になってくる．これが脱境界化 De-perimeterization と呼ばれる考え方である．

6.　脱境界化セキュリティ対策の試み

標的型攻撃のような人間の行動心理に付け込む攻撃に対しては，境界で一括して防御するという二項対立的セキュリティモデル（図 2）では完全に境界で防御することは不可能である．本来的に分散させた多項連携型セキュリティモデルを定義し，アプリケーション個別，文脈個別にセキュリティ対策を行うモデルを探索することになった．

6.1　多重防御

攻撃者の境界からの侵入を許さざるを得ない場合（たとえば，SSL を使用しない Web 通信中のセッションを HTTP セッションハイジャックによって乗っ取られる），万が一許してしまった（たとえば，ゼロデイ攻撃を受けたり，利用者の不注意によって PC がウイルス感染する）場合に備えて，不測事態対応として，予期される攻撃への多段階の対応策（すなわち複数の境界）を用意しておくことである．

6.2　第三者との連携による認証

情報セキュリティを確保するためには，ユーザ認証

（ユーザの本人確認），認可（ユーザのアクセスを許可）とアイデンティティ (ID) 管理（アカウント情報の管理）が重要である．境界化状況ではドメイン（自社の管理下の対象ネットワーク）内では一定の情報セキュリティポリシ（企業や組織において実施する情報セキュリティ対策の方針や行動指針）が確保されているという前提があった．しかし，脱境界化状況では，企業自らが構築する自社ネットワークやクラウドサービスは，それぞれがドメインを構成し，データは，流動的に組み合わされたドメイン間を流通していく．しかも，各ドメインの情報セキュリティポリシは相違するということを考慮しなければならない．これに対して，現在次の二つのアプローチが提案されている．

① ユーザ中心アプローチ

ドメインの情報セキュリティポリシに応じて情報セキュリティを分担（認証と認可を分散）させ，ユーザの意思に基づいてドメイン間のデータの流通を制御するという考え方である．たとえば，Claim-based security 方式では，境界外からのアクセスに対して，第三者による信頼保証に基づいてアクセスを受け入れる．

② データ中心アプローチ

究極的に守るべき資産は情報（データ）であるという立場に立ち，ドメイン間で当該データに関して一貫した情報セキュリティポリシを適用すればよいという考え方であり，たとえば，Selective intelligent encryption が提案されている．これは，公開鍵暗号方式で使用される暗号化鍵，復号鍵それぞれにパラメータを組み込み，復号時に両パラメータの持つアルゴリズムによって復号可否を決定することによって，送信者がデータの受け手を「自由に指定」できるという方式である．

本稿では，これらの詳細の説明は割愛する．

7. 情報セキュリティを確保するために（まとめに代えて）

サイバー攻撃という脅威から個人，企業，社会の情報活動を完全に守ることができないのであれば，技術的対策だけでなく，組織的，人的対策を含めて多重防御型で情報セキュリティ対策を実施する必要がある．

そのための課題として次のことが考えられる．

(1) 入口対策を見直す

価値の高い情報資産（重要資産）を峻別し，システム設計に立ち返って，この重要資産へのアクセス権を見直し，またインターネットや電子媒体からこの重要資産を隔離する．

(2) 出口対策を加える

境界内は安全であるとの前提から，ウイルスなどの脅威が境界内に入り込むことはやむを得ないという前提の下に，脅威の境界内での活動を最小限に抑え，万一重要資産が感染しても，情報を外に持ち出させない仕組みを施す．

(3) 脆弱性対策を徹底する

従来から，ソフトウェアのセキュリティパッチの適用，最新バージョンへの更新，パスワードの強化などの基本的な脆弱性対策の必要性は言われてきたが，関連するセキュリティ対策が費用や手間を要することから，後回しにされることが多い．CISO（Chief Information Security Officer：最高情報セキュリティ責任者），情報セキュリティ管理者などが具体的な対策の確実な実施を推進する．

(4) 監視の強化と発見時の対応手順を整備する

重要資産へのアクセスログを長期にわたって継続して採取し，ログの内容分析によって不審な動きを検知するとともに，その場合の対応手順をあらかじめ作成しておき，その手順を実行できるように，定期的に訓練を行う．

(5) 情報セキュリティ人材を育成する

情報システムの開発，運用のための要件定義の中で情報セキュリティは非機能要件（情報システムの対象業務に求められる要件以外の要件）とされてきた．しかし，2 節に見たように，現在では，情報セキュリティが損なわれると，企業経営にも直接影響する事態になりかねず，業務を遂行するうえで欠かせない要件，すなわち機能要件として取り組むことが必要である．

その機能要件の実現を担う情報セキュリティ技術者は約 26.5 万人いるが，うち 16 万人はスキル不足であり，実質 8 万人ほどの技術者が不足しているという調査結果 [3] もあり，企業における情報セキュリティ人材の育成は喫緊の課題といえる．情報セキュリティは，物理的，技術的，管理的，人的と広範囲に及ぶこと，従来はベンダ任せにしてきたことから，自社での育成は難しいといわれる．まずは自社の情報資産の保護とリスクマネジメントに権限を持つ CISO を任命し，自社にとって不足している人材（コンピタンス）は何かを見極め，アウトソーシングと自社での育成を積み重ねていくことが必要である．

(6) 脆弱性情報を共有し事故を予防する

サイバー攻撃では，ICT の脆弱性に付け込んで攻撃を加えるといったインシデントが非常に多い．しかし，ICT 関連技術・製品はほとんどがベンダの所有で

ある．ベンダが保有する社会インフラ（Microsoft の Windows OS も現在では社会インフラである）の脆弱性[7]に関してユーザ企業の情報セキュリティ管理者ないし利用者個人の自己責任に訴えるのは限度がある．ソフトウェアは無体物であるゆえ，現行の製造物責任法は適用対象外としているので，ベンダの責任を追求できない．ソフトウェア製品の開発・販売者自らが脆弱性を公表（たとえば，Windows OS の Windows Update）することも必要であろう．現在は，脆弱性の発見者（ユーザ個人・企業，ソフトウェア製品を組み込んだ情報システムの開発・販売者など）が IPA に届出し，IPA と JPCERT/CC が脆弱性の修正に向け，Web サイト運営者やソフトウェア開発者と調整を行い，その結果を基に IPA が開発者の対応状況を公表する（開発者の同意が条件）ソフトウェア等脆弱性関連情報届出制度がある．経済産業省は，脆弱性の解決をさらに加速させるために，ソフトウェア開発者の同意がなくても脆弱性を公表できるような制度を 2016 年度に定める予定という．

(7) サイバー安全教育によって情報セキュリティ意識を醸成する

情報社会では，サイバー空間の住人はすべて ICT の利用者である．インターネットの利用には自己責任の原則が適用されているが，たとえば高齢者にもスマホを使ってもらおうとする場合に，自己責任の原則を貫けるだろうか？ 人間は手続きの順守について緩いところがある．物理学者でありロゲルギストの一人であった高橋秀俊は，計算機と付き合わねばならない人間の特性として次の八つを挙げ [5]，計算センターの壁に貼っていたという：

1. 人間は気まぐれである，
2. 人間はなまけものである，
3. 人間は不注意である，
4. 人間は根気がない，
5. 人間は単調をきらう，
6. 人間はのろまである，
7. 人間は論理的思考力が弱い，
8. 人間は何をするかわからない．

情報セキュリティを確保するためにも，人間のこの特性を忘れてはならない．ではどうするか？

中央省庁では，職員の情報セキュリティ意識の向上，インシデント発生時の対応手順を習得させるために，2015 年 3 月から NISC と総務省が主催してサイバー防御演習を行っている．同様に，企業でも疑似攻撃を自社サイトに加え，これらの攻撃に対する従業員たちの対応を定量的に評価し，必要な教育を継続的に（業務内容の変化，ICT の変化に伴い，情報セキュリティ対策も変化する）行うところが現れている．

今後，サイバー攻撃は実空間における交通事故と同じような現象になっていくのではないか．日本では，幼稚園，小学校で交通安全教育を行ってきたが，これからは，同様に小学校からサイバー安全教育を継続的に行って情報セキュリティ意識の醸成を図っていく必要がある．

参考文献

[1] D. Denning, *Information Warfare and Security*, Addison-Wesley, 1998.（杉野隆監訳，『ネット情報セキュリティ』，オーム社，2002.）
[2] M. McLuhan, *Understanding Media*, McGraw-Hill, 1964.（栗原裕，河本仲聖訳，『メディア論』，みすず書房，1987.）
[3] IPA，情報セキュリティ白書 2015，2015.
[4] IPA, 2014 年度情報セキュリティ事象被害状況調査, 2015.
[5] 高橋秀俊，“時分割方式設計の哲学，”『数理と現象』，岩波書店，1975.

[7] Web サーバで認証や暗号に広く利用されているオープンソースの OpenSSL に 2014〜2015 年にかけて三つの脆弱性が発見され多くのインシデントが発生した．たとえば，三菱 UFJ ニコスでは，延べ 894 名のクレジットガード番号その他の個人情報が不正に閲覧された．