サイバーセキュリティと情報セキュリティの狭間にて

日本サイバーセキュリティ・イノベーション委員会
客員上席研究員　小林正彦

（１）サイバー空間、サイバー攻撃、サイバーセキュリティ

今日、サイバー攻撃、サイバー犯罪という言葉を目にしたことがない日本人にはほぼお目にかかれないだろう。それほど身近になっている「サイバー攻撃」、「サイバー犯罪」などの言葉だが、同時に「サイバーセキュリティ」という言葉もよく使われる用語となってきている。

ずいぶん前からそうだったような気もするかもしれないが、わが国で一般的に目にするようになったのは実はそれほど昔のことではない。米国では 2000 年代の初めころには既に頻繁に使われていたが、日本では概ね 2010 年以降、特に多くなったのは 2014 年以降のことだ。

サイバーセキュリティの用語が一般化してきた過程を見る道具として、グーグル検索を使ってみよう。

『”サイバーセキュリティとは ” before:年月日』を日本語サイトで検索し、オリジナルサイトベース（引用サイトを除外）で件数をみると、2022 年末には 161 件ヒットする。

ところが 2000 年末までは、「検索条件と十分に一致する結果が見つかりません。」となり、2005 年末にようやく 3 件と表示されるまで有意のサイトはないようだ。

その後 2011 年末に 7 件に増えるまで数年間は微増ペースであったのが、2012 年末に突如 12 件となり、その後 2014 年末に 22 件と急増、2015 年末には 39 件、2016 年末には 47 件となって昨年末の 161 件に至っている。

この増加のパターンを見ると、2011 年から 2014 年にかけて顕著な変化があったことが読み取れるが、2014 年 11 月 6 日にサイバーセキュリティ基本法が施行されたことを考えれば納得がいく増加パターンと言えるだろう。

つまり、基本法の施行の更にその前の時代、2010 年頃から世界的にサイバー攻撃のレベルが上って、重要インフラなどに対する脅威が軽視できない状態となってきたという時代の変化が背景にあるのである。

それが基本法制定へとつながったことを、この数字の増加は反映していて、そのような 2010 年代前半の歴史を背景にサイバーセキュリティという用語が一般化した、というのが後付けではあるが筆者の解釈である。

基本法は、「サイバーセキュリティ」に法律上の定義を与えたという点で時代を画するものであるが、それまで法的な根拠を与えられていなかった「情報セキュリティ」に関する政策も、実はこの法律により実質的な裏付けを与えられたということはあまり意識されていない事実である。
むしろ、法律の世界に登場したのが「サイバーセキュリティ」であって、「情報セキュリティ」ではなかったことは、古くからの情報セキュリティ関係者としては若干残念に思うところでもある。

言霊の国である我が国では、いったんサイバーセキュリティが情報セキュリティをオーバーライトしてしまうと、公の文書では情報セキュリティの用語を使うことがはばかられ、情報セキュリティが過去のものにされていくのではないか、と筆者は密かに心配している。
「サイバーセキュリティよ こんにちは」、「情報セキュリティよ さようなら」が国レベルで進行中なのであろうか。そうでなければ良いのだが、どうもその期待は危ういかもしれない・・・そういう残念な気持ちを引きずって書き始める本コラムは、情報セキュリティに対するレクイエムであるかもしれない。

（２）情報セキュリティ政策とサイバーセキュリティ政策

筆者は、内閣官房の組織として 2005 年に発足した内閣官房情報セキュリティセンター（NISC）に、初代の参事官として 2005 年から 2007 年にかけて在職したが、その当時 NISC の英語名称は日本語名称を素直に訳した「National Information Security Center」であり、担っていたのは情報セキュリティ政策であった。
戦略枠組みの策定や政府機関の対策充実などの実務に追われる一方で、大きな目標として目指していたのは、政策の根拠法として「情報セキュリティ基本法」を制定し、NISC をその法律の下に位置付けることであった。
しかし結果として１０年近くその大目標は実現せず、代わりに成立したのは「サイバーセキュリティ基本法」という名称の法律で、NISC の名称も、語呂合わせ努力の結晶として「National center of Incident readiness and Strategy for Cybersecurity」に衣替えすることとなった。
当時のことを知る者として今日目線で振り返って考えると、恐らく「情報セキュリティ」の名称に固執していたのでは、基本法は永久にできなかっただろう、と思うところもある。サイバーセキュリティを看板にすることで、結果として「情報セキュリティに関する政策」にも実質的な裏付けを与える構図となったことは、情報セキュリティ関係者として感慨深くもある。

さてここで「情報セキュリティに関する政策」にもサイバーセキュリティ基本法が実質的な裏付けを与えた、と述べたが、それは、2014 年に成立したサイバーセキュリティ基本法に基づいて国がサイバーセキュリティ政策やサイバーセキュリティ対策を行う、という法律の建付けのもとで、

NISC が中心となって現実に行ってきた政策は、「情報セキュリティ政策」の要素をかなり併せ持ったものだったからである。

基本法制定以降も NISC が情報セキュリティ的な政策を継続的に行ってきたという事実は、NISC が「情報セキュリティセンター」を母体として発展的に作られた、という歴史的な経緯によって暫定的にそうだったわけではない。NISC はサイバーセキュリティ政策の看板のもとで、実はサイバーセキュリティ政策とともに情報セキュリティ政策も当然のミッションとして行う存在だった、というのが本質的な構図だったのだと筆者は理解している。あえて、「だった」と過去形で書いたことに注意しておいてもらいたい。

情報セキュリティとサイバーセキュリティの違いについて述べているサイトの多くには、「概ね同じ」という記述がある。この理解は大きな間違いではない。しかしながら厳密にいえば違うからこそ名前が違うのであって、そこを意図的にあいまいにして新しい基本法の枠組みのもとで情報セキュリティ政策の要素を残した運用を始めることは、当時の関係者にとっては大きな割り切りだったに違いない。やむを得ない事情と決断と配慮があったのだろう。

サイバーセキュリティ基本法が世に出た 2014 年に、それまで「情報セキュリティ云々」だった多くのものは「サイバーセキュリティ云々」に衣替えをした。しかしながらその際に情報セキュリティの名前を堂々と残した部分がある。NISC の政府機関総合対策グループが行っている「政府機関等の情報セキュリティ対策」である。

NISC 発足と同じ 2005 年に策定された「政府機関の情報セキュリティ対策のための統一基準」及びその後継の基準群は、政府機関自身のための情報セキュリティ対策の基本となるものであるが、基本法が制定されたあとも、つい最近まで堂々と情報セキュリティを名乗りつつ政策展開してきたのだ。この件については書き残したいことがあるので、最後にまた触れることにする。

（３）欧米における情報セキュリティとサイバーセキュリティ

米国と欧州では、日本と違う事情と過去の経緯がある。

＜米国＞

米国においては、2000 年代初めには既にサイバーセキュリティ「cybersecurity」という用語は各所で使われていた。その一方で、情報セキュリティ「information security」「computer security」又は「IT security」の用語も 2000 年代初めから頻繁に使われており、両方の用語は内容によって棲み分けられていた。

例えば、2002 年には「Federal Information Security Management Act：FISMA（連邦情報セキュリティ管理法）」が制定され、各省庁に対して情報セキュリティ対策の自己評価を行い、結果をOMB（合衆国行政管理予算局）に報告する義務が課せられた。

また同法は米国の国家標準を担っている NIST（National Institute of Standards and Technology（米国国立標準技術研究所）に対して、これら各省庁の義務に関する規格やガイドラインの開発を義務付けている。

その NIST が公表してきた様々な公開文書を見てみると、「information security」と「computer security」の用語が、内容に応じて使い分けられてきた一方で、「cyber security」又は「cybersecurity」の用語はなかなか登場せず、ようやく 2009 年に「Cyber Security Standards」という小文書が発行されるまでは公開される文書の上で使われることはなかった。

NIST は、政府機関の情報セキュリティ対策を充実させるために、2005 年に「NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations（米国連邦政府機関の情報システムおよび連邦組織のためのセキュリティ管理策とプライバシー管理策）」を発行し、現在は Rev.5 に至っているが、この最初の版には「information security」の用語が 66 回登場する一方で、cyber の語は全く登場しない。

この文書（Rev.0 に相当）はその後何回か改定されたが、長らく cybersecurity の語とは無縁で、2013 年発行の Rev.4 に至って初めて「cybersecurity」の語が3回登場し、2020 年発行の Rev.5 では遂に 30 回登場することとなる（なお「information security」の語は Rev.5 で 213 回登場）。

行政実務面ではこのように情報セキュリティ対策がずっと表の看板であったが、政治的にはサイバーセキュリティが 2000 年代はじめから喫緊の課題となっていた。

2001 年 9 月 11 日の同時多発テロ事件をきっかけに、同年 10 月に「Executive Order 13231（大統領令 13231）」が発令され、合衆国の重要インフラを守るという政策目的を検討するための組織として PCIPB（大統領重要インフラ保護委員会）が発足した。

この委員会で、「サイバースペースのセキュリティ」という問題意識があげられ、2002 年にはサイバースペースのセキュリティについての国家戦略として「National Strategy To Secure Cyberspace：NSSC」が登場したが、この頃には国家防衛に関する話題で「cybersecurity」の用語が頻繁に使われるようになっていた。

その後サイバーセキュリティの所管は PCIPB から国土安全保障省に全面的に移行し、2003 年 6 月、同省内にサイバーセキュリティに取り組むための組織として「National Cyber Security Division：NCSD（国家サイバーセキュリティ部門）」が新設された。連邦政府組織の中に Division 名として cyber security の語が初登場したのである。

このように、米国では 2000 年代の前半から、サイバーセキュリティは政治的な文脈で、情報セキュリティは行政実務分野の文脈で共存しつつ使い分けられていた。

一方欧州における歴史は米国とはかなり様相が違う。

＜EU＞

EU には現在サイバーセキュリティの中心組織として ENISA という機関が存在する。ENISA は日本の NISC に先立つこと1年前の 2004 年に、情報セキュリティのための組織として設立された。名称の ENISA は「European Network and Information Security Agency」[1]の頭文字からできている。つまり、設立当初は「ネットワークと情報セキュリティのための組織」だったわけだ。

ENISA は、2019 年に発効した「The EU Cybersecurity Act」によって Cybersecurity に関する権限を与えられ、EU のサイバーセキュリティの中心機関となった。この点では日本の NISC と似た経緯を辿っており、設置もほぼ同時期で、当初は名称に information security を含んでおり、日本に5年遅れて、ミッションが cybersecurity となったわけである。

ところが、日本では NISC の名称について、語呂合わせ努力の結晶として新たな英語名称を与えたが、EUは、ENISA というこの5文字の組織名をそのまま使い続けながら、cybersecurity に関係させた新たな「当てはめ」を全くしていない。ENISA の名称は新ミッションとなったあとも、英語では「ENISA（The European Union Agency for Cybersecurity）」と称している[2]。官僚経験者である筆者は、英語、仏語、独語のいずれにもあてはまるような良い語呂合わせが見つけられなかったせいではなかろうかと勝手に想像している。

更に見ると、最近書かれた ENISA の関係者コメントなどでは、設立当初の 2004 年から組織名称に情報セキュリティを含んでいるにもかかわらず、ENISA は設立当初からサイバーセキュリティにかかわってきたと言い切っており[3]、2016 年発効の EU の NIS 指令についても、名称が「the EU Network and Information Security directive」であるにもかかわらず、これは EU の 「Cybersecurity strategy」の一部であるという説明をしている。

EU としては ENISA によってこれまで情報セキュリティ政策を推進してきたが、2019 年に「The EU Cybersecurity Act」を発効させたことで、従前から実施していた政策をサイバーセキュリティ政策として看板の付け替えをして、過去の情報セキュリティ政策についてもサイバーセキュリティ政策であった、と強弁して過去をオーバーライトした模様である。

＜欧州各国＞

一方、EU レベルと加盟各国レベルでは多少の温度差があり、2019 年に上述の EU 法が成立したことを横目に見ながらも、国内政策的には情報セキュリティとサイバーセキュリティを区別して扱い続けている国もある。

ドイツの例では、2021 年に発効した新しい IT Security Act 2.0 において、情報セキュリティとサイバーセキュリティを引き続き異なる概念として扱い、それらを両立させた運用が行われている。
欧州諸国は ISO 標準を戦略的に重視して有効に使う政策を取ってきており、場合によっては国際的な場面で欧州以外の地域に対する経済政策の武器としても使ってきた。
これに対して、米国は、多くの場面で ISO 標準を無視まではしないものの軽視する態度が見られ、米国政府や米国企業は「求められれば対応する」程度の対応に終始してきた。
欧州における「情報セキュリティ」の用語に対する態度は、ISO 標準への欧州各国の態度が大いにかかわっているものと考えられる。

（４）情報セキュリティとサイバーセキュリティの関係

米国と欧州における情報セキュリティとサイバーセキュリティの使われ方は、前節に述べたように異なる部分が見られるが、話を日本に戻して、日本における現状、サイバーセキュリティ基本法を踏まえた両者の関係について見てみると、また違った構図が見えてくる。

情報セキュリティとサイバーセキュリティは概ね同じと割り切って、細かいことにはこだわらない、という態度は運用現場では概ね問題ない。情報セキュリティ対策だといって、サイバーセキュリティ対策をすることも、サイバーセキュリティ対策だといって情報セキュリティ対策をすることも、どちらも許容できる。
そうは言うものの、言葉が違うのは違いがあるからで、この分野の関係者であればあるほど、どこが違うのかが気になるところではないか。以下ではその違いの部分に徹底的にこだわって両者の関係を見ることにする。

我が国における情報セキュリティとサイバーセキュリティの関係について論ずる場合、サイバーセキュリティ基本法が制定されているので、その定義がどういう構造なのかを理解することが出発点となる。
情報セキュリティには国際的に確立した定義が ISO/IEC27000 シリーズのなかにあってそれが使われることが多い。一方で、サイバーセキュリティの定義については現時点で世界共通の明確な定義はなく、国によって文脈によって、意味が異なる使い方がなされているのが実態である。その中で、我が国は明確な定義を有する基本法がある点で、両者の違いを議論しやすい立ち位置にある。
結論的なコメントとなるが、基本法におけるサイバーセキュリティの定義は、一般的に認識されているサイバーセキュリティよりも、かなり情報セキュリティに寄せたものとなっている。

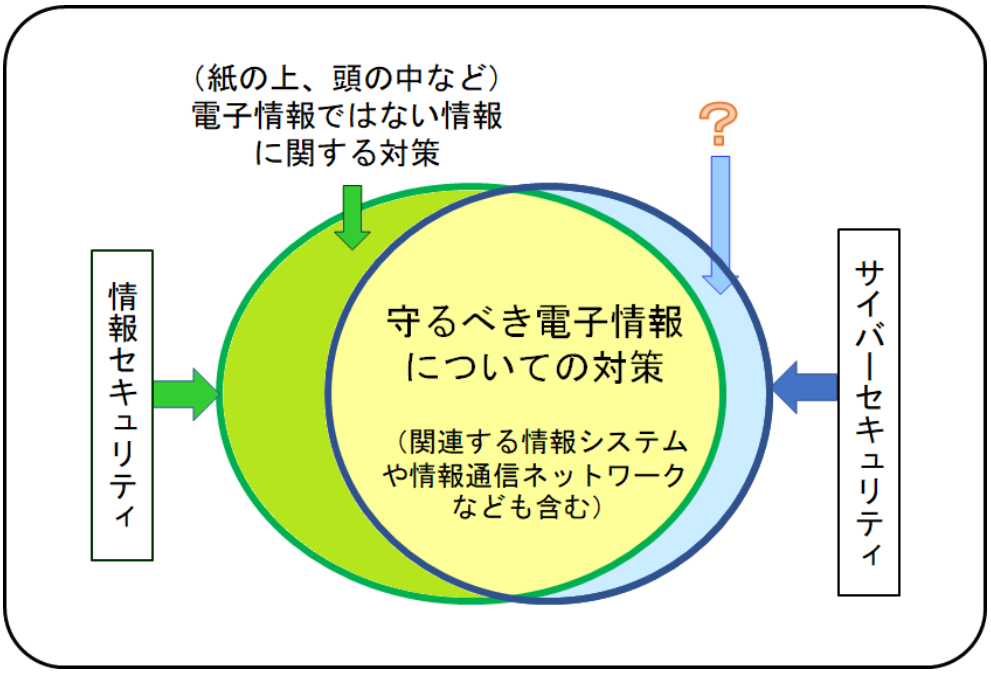
基本法は次のようにサイバーセキュリティを定義している。

（定義）
第二条　この法律において「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(以下この条において「電磁的方式」という。)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（以下「電磁的記録媒体」という。）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。

この定義をざっくり要約して表現すれば、「いわゆる電子的な情報、情報システム、情報通信ネットワークの安全性及び信頼性が、対策を講じることで維持管理されていること」となる。
もう少し細かく見てみれば、「並びに」で2つの対象が並列的に挙げられており、前半の部分は「いわゆる電子的な情報」、後半の部分は「情報システム及び情報通信ネットワーク」について述べるとともに、後半では「安全性及び信頼性の確保のために必要な措置」と表現している部分が、前半の電子的な情報については、より踏み込んで「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」と表現し、両者について「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」となっている。

情報セキュリティは「守るべき情報」を組織自身が特定することが出発点となっており、基本法の定義前半部分は情報を電子的な情報に限定しているものの、安全管理すべき情報を考えることが出発点という構造は同じだ。しかし電子的でない情報、例えば紙の上の情報や、人の頭の中にある情報などが、この定義に入らないことは明白である。

以上の点を意識しながら、両者を対策の集合体として表現したベン図を考えてみれば、大きな共通部分を持つ二つの重なり合う円となる。



共通部分は「守るべき電子的な情報についての対策」であり、この割合は極めて大きい。一方情報セキュリティ側へのはみだし部分には「電子的な情報ではない情報に関する対策」が入っている。そしてサイバーセキュリティ側へのはみだし部分に何が入っているのかであるが、ここは議論の余地があるので、とりあえず「？」と書いておき後段で論ずることにする。

結論だけ先に示しておくと、基本法の定義では、実は「？」には何も入っていない。
このため基本法の定義のサイバーセキュリティは情報セキュリティに包含されることになる。しかし一般的なサイバーセキュリティの認識・用法ではサイバー攻撃に関連した「何か」があると考えられており、基本法以外の場面では、サイバーセキュリティは情報セキュリティに包含されるという主張はなかなかお目にかかれない。

以下、定義の面から両者の比較をしてみる。

国際的な規範となっている ISO/IEC27000 シリーズでの情報セキュリティの定義を噛み砕いて言えば「組織として守るべきとした情報の CIA（機密性・完全性・可用性）を確保すること」のように表現できる。我が国においてもこの定義が使われることが普通である。

基本法の定義は、電子的な情報に限られるものの、「漏えい、滅失又は毀損の防止」を謳っており、ISO における情報セキュリティの定義と比較すると、使っている用語は異なるが、「漏洩」は

「機密性」、「滅失又は毀損」は「完全性と可用性」を表現したものと考えられるので、同じ概念をよりなじみの良い表現で言い換えたものとなっている。
　これは世間一般でのサイバーセキュリティの用語の使われ方、理解のされ方よりも情報セキュリティの定義に歩み寄ったものだと言えるだろう。というのは、構文上サイバー攻撃のような「攻撃」が前提とされておらず、攻撃とは無関係に情報、情報システム、情報ネットワークの保全を内容とする定義であるからだ。従って、災害や事故や過失などによる問題もカバーする定義となっていて、情報セキュリティの定義と基本的に同じである。

　世界共通の明確な定義はないサイバーセキュリティの定義だが、国によってはサイバーセキュリティを法的に定義している国がある。例えばシンガポールには我が国と同様に CIA 確保型のサイバーセキュリティの定義を有する法律があるが、その定義は「不正なアクセス又は攻撃からの保護」を前提としており、災害や事故や過失などによる問題は対象外である。

　一般的なサイバーセキュリティの認識・用法では、サイバー空間、サイバー攻撃そしてサイバーセキュリティという論法でサイバーセキュリティの必要性が理解されているので、基本法の定義における「サイバー攻撃を前提にしていない」というこの特徴は、世の中ではあまり認識されていないように思う。

　一方、「情報」に加えて「情報システム及び情報通信ネットワーク」が定義範囲に明示されていることから、サイバーセキュリティの定義は情報セキュリティの定義より広いという主張がなされることがある。しかし ISO の情報セキュリティ枠組みでの運用を見れば、「情報システムや情報通信ネットワーク」なども、情報を守るために必要であれば対策の対象にするのが当然、とされているので、これら「情報」以外のものがサイバーセキュリティの専管ということはなく、守るべき情報に関係するならば、情報セキュリティはサイバーセキュリティの定義の「情報システム及び情報通信ネットワーク」も対象としているということができる。

　さて、残る問題は先ほどのベン図で「？」とした部分であるが、世間での一般的なサイバーセキュリティの認識・用法では、情報セキュリティに包含されないサイバーセキュリティ独自の要素があって、この部分にはその「何か」が入っていると考えられている。しかし基本法の定義のもとでこの部分を考えてみると、入っているかもしれない「何か」はことごとく除外されていく。

　まず、「守るべき情報と関係がある対策」なら、ここには入っていないから、入っているのは「守るべき情報とは無関係な対策」であって「情報システム及び情報通信ネットワークへの対策であるもの」という属性に該当するものになる。そのようなものとしては何があるだろうか。

この議論で例としてよく挙げられるものとして「攻撃予告段階での脅迫対応」と「踏み台攻撃」がある。その他にもいくつか例示されることがあるが、とりあえずこの2つについて考えてみよう。

攻撃予告段階での脅迫対応は、情報に対する被害は未然の状態での対策だが、もし炸裂すれば情報に被害が生ずるのだから情報セキュリティの所掌範囲に入れていて何らおかしくない。

サーバー機能を不正に利用することで行われる踏み台攻撃についても、自らの情報への被害は通常生じていないので情報セキュリティの対象ではないとの議論があるようであるが、サーバー機能の過負荷により自らの情報と情報システムの可用性に被害が生じかねないと考えて対策をするならば、立派に情報セキュリティ対策でありうる。

一般的なサイバーセキュリティの認識・用法で考えた場合は別な事例があるかもしれないが、基本法第2条のサイバーセキュリティの定義範囲で考えたとき「？」に分類されそうなものは、ISOの情報セキュリティの定義と基本法の定義の枠組みから詰めて考えてれば、守るべき情報との関係が（「風が吹けば桶屋」よりも近い因果関係で）示せるものばかりである。

結局、基本法第2条のサイバーセキュリティの定義範囲では「？」の部分は空集合となる。

このような理解は筆者が法案の立案時の関係者に聞いた話に基づくもので、筆者の勝手な思い込みではない。むしろ、サイバーセキュリティは情報セキュリティの定義から電子的な情報以外の情報の要素を、意図して明瞭にはずしたうえで、用語は噛み砕きつつ、限りなく情報セキュリティをなぞった定義とする、という方針で作られたものだったようである。

このような両者の関係を踏まえれば、サイバーセキュリティが情報セキュリティよりも大きな概念である、というような主張をすることは、基本法の世界では無理があり、基本法のサイバーセキュリティは ISO の情報セキュリティの定義範囲に完全に包含されている、というのが正確な主張である。

包含関係を議論すると、以上のようにサイバーセキュリティは情報セキュリティに包含されているという結論となるが、包含関係や大小論の発想を離れて両者の関係を見てみれば、また違う議論があるだろう。

電子情報は今日爆発的に増加しつつある一方で、非電子情報はゆるやかにしか増加せず、場合によっては過去の文書廃棄などによって減少しているかもしれない。そう考えると、今後必要な対策の大半はサイバーセキュリティ対策の観点から考えれば良いという考えは支持できる。従って、今日的に重要なのはサイバーセキュリティだ、という主張も、そのような論旨からは極めて妥当である。

（５）組織幹部への訴求力の違い

定義から離れて、情報セキュリティ対策とサイバーセキュリティ対策のアプローチの違いを論ずると、包含論とは違う両者の重要な差異が見えてくる。

情報セキュリティ対策を考える際は、「守るべき情報」に主眼を置き、これに対するリスクとそれを防ぐための対策という順番に視点を移していく。守るべき情報はサイバー空間以外にも、例えば紙の上にも頭の中にもある。

しばらく前までは、申請書類など大半紙ベースで運用されていたものが多いので、今もなおそれらの紙情報が様々な場所に大量に保管されているであろう。企業の機密情報を知っている人間の拉致や引き抜きは、ちょっと特殊ではあるが情報セキュリティの観点で言えば意識されるべきリスクである。これらはサイバーセキュリティの定義の中には入らない。定義論で言うとこのような違いを多数列挙することができるので、非電子情報の安全確保は今もなお無視できない。

一方サイバーセキュリティでは、「守るべき情報」が出発点になる情報セキュリティと違って、攻撃やリスクのありようが本質的な課題であり出発点である。これが一般的な使われ方を前提としたサイバーセキュリティの常識的理解であり、サイバーセキュリティは、まず攻撃ありきで考える防衛論である。

昨今ITシステムに対する攻撃の多くは外部から行われ、サイバー空間が攻撃と防御の主たる舞台となっている状況から、このような発想でセキュリティを考えることは極めて現実的であることは間違いない。両者のこのような対策のアプローチの違いから、非専門家への訴求力には大きな違いが生ずる。

情報セキュリティはすべての情報を対象としていて定義範囲は広い。すべてのリスクを幅広く検討して対策を考えることを求めるアプローチである。リスクは広範に存在し、対策を含めて隅々まで配慮しなければならない。このため情報セキュリティは、漠然とした印象のとらえどころないものに感じられることがある。

このような一言では理解を得られにくい性質ゆえ、情報セキュリティ対策の充実を、と訴えても、組織幹部からは必要性を理解してもらえないという嘆きが過去には多くあった。この点が、冒頭にコメントした、『「情報セキュリティ」の名称に固執していたのでは、基本法は永久にできなかったのだろう』と思う理由のひとつでもある。

これに対して、サイバーセキュリティはわかりやすい。まず攻撃ありき、のアプローチで、深刻な被害をもたらす攻撃の存在は今では広く理解されているため、対策の緊急性・必要性が感じられ、刻一刻と進化する攻撃に対して追加の対策も訴えやすく、組織幹部への訴求力も抜群な概念である。

サイバーセキュリティの語の持つ緊急性・必要性の神通力を使って、できる限り情報セキュリティに近い定義で基本法を作るという政策立案者の賢慮が、思惑通り日の目を見て、結果として「情報セキュリティに関する政策」を行ってきた政府の政策についても、その連続性を殆ど損なわずに法的な根拠を事実上得ることになったと筆者は理解している。

過去を振り返って、情報セキュリティの CIA の概念（機密性・完全性・可用性）を法律的に条文化することができただろうか、と考えてみると、恐らく立法技術的に難度が極めて高く、官僚経験者の立場で考えれば法制局などを通すことは困難であっただろうと感じられる。

内閣立法で「情報セキュリティ基本法」の法案を通すなどというチャレンジは誰もが躊躇する高いハードルであったに違いない。それが「情報セキュリティ基本法」という名称のものが10年間できなかった理由の一つであると後知恵で思うところである。

情報セキュリティの CIA の概念を法律に書き込むことの困難さだけでもハードルは高かったであろうが、むしろすべての情報を対象とする情報セキュリティの定義を基本法に持ち込もうとすると、紙の上の情報ならまだしも頭の中の情報まで入れるのか、という話になってしまうことのほうが問題だったかもしれない。

頭の中の情報は、企業の知的財産保護の観点でのニーズはあるかもしれないが、国レベルで考えると他の法律との整理ができただろうか？　・・・そんなことはどんなに頑張ってもできない相談であったかなと、筆者は今にして思う。

（６）政府自身にとっての情報セキュリティ

本当は入れたかったのではないかと推測する「電子情報」以外の情報を、大胆に割り切って成立させたサイバーセキュリティ基本法だが、それまで NISC が行ってきた政策は情報セキュリティ政策であったので、定義から外れてしまう電子情報以外の情報を含めた情報セキュリティ対策をどう扱うかという問題が当然ながら生じたであろう。しかし 2014 年当時の関係者たちは、この問題をうまくかわしながら、概ね連続的に政策展開してきた。

当時の関係者の割り切りを筆者なりに推測すれば、情報セキュリティ対策は、それまで法律の裏付けがなくてもやってきたのだから、これからもその延長で淡々と続ければ良いではないか、という判断であったのかもしれない。

そういう態度を取っても問題ない程度には、政府内の情報セキュリティ対策のレベルが上っていることが前提であるが、情報セキュリティ政策が産声を上げた 2000 年、NISC が発足した 2005 年当時に比べれば、20 年近くの年月を経て、概ね枠組みの出来上がった政府自身の情報セキュリティ対策の取り組みは、その前提を満たす程度になっていたことだろう。

このように、サイバーセキュリティセンターの中に情報セキュリティ対策を実施するグループ（政府機関総合対策グループ）が存在する、という構図は、サイバーセキュリティがカバーしない非電子情報を含めた対策をサイバーセキュリティ対策である、と無理やりこじつけるようなことはせずに、素直に情報セキュリティ対策として扱ってきたことを意味している。

情報セキュリティ政策や政府の情報セキュリティ対策は必要性がなくなったわけではなく、引き続き必要であるので基本法の裏付けがなくてもそのまま継続すれば良い、という整理だったのだとすれば、「サイバーセキュリティは重要だが、一般的な組織においては情報セキュリティ対策が引き続き必要なのだ」ということを政府自身が身をもって示していたわけだ。

この判断と態度は、一般社会や情報セキュリティとサイバーセキュリティの取り扱いに悩んでいるかもしれない企業に対して大いに意味あるメッセージだったと思う。2014 年当時の関係者の懐の深さを感じるところである。

実際に、2014 年の基本法施行とともに多くの「情報セキュリティ云々」が「サイバーセキュリティ云々」に衣替えした中で、（2）で触れたように、NISC の政府機関総合対策グループが行っている「政府機関等の情報セキュリティ対策」は、基本法施行後つい最近まで堂々と情報セキュリティを名乗りながら政策展開してきた。

（７）残念に思うこと

ところが、基本法施行以降も堂々と使ってきた「政府機関等の情報セキュリティ対策のための統一基準群」が 2018 年版[4]から 2021 年版[5]に改定される際「政府機関等のサイバーセキュリティ対策のための統一基準群」に衣替えされてしまうという事件が起こった。

筆者にとってこれはまさに事件であった。この改名によって、サイバーセキュリティセンターの看板のもとで情報セキュリティ対策も行うし、それが当然、ということを許した 2014 年の懐の深い賢明な割り切りを、制度上は半ば否定してしまったようなものだからだ。

政府機関の対策範囲は、基本法のサイバーセキュリティの定義範囲では不足するので、従前どおり情報セキュリティは残し、もしサイバーセキュリティ的に考えると不十分と考えられる部分があるなら、情報セキュリティ対策のサイバーセキュリティ補完分として行えば良いものと筆者は考えてきたところであり、NISC も 2014 年以来そのような対応をしてきたと考えていたからだ。

政府機関総合対策グループのウェブページを見ると、例えば 2021 年 7 月付で発行された「政府機関等の対策基準策定のためのガイドライン」[6]の中には、情報セキュリティの語が今も多数使われており、現時点では対策範囲をサイバーセキュリティに限定するというような態度を取っているわけではなさそうだ。

しかしサイバーセキュリティセンターのお膝元で情報セキュリティ政策を続けることの居心地の悪さに耐えられない関係者がいたための名称変更だとすると、今後上述のガイドラインなどもサイバーセキュリティに上書きされていくことになるのかもしれない。

「言霊の国」の習わしとして、最初は違いを割り切って名前を付けたものの、時間の経過とともに名前に実態が引きずられてくる、ということはしばしば起こることである。情報セキュリティとサイバーセキュリティとの間でもこれが起きて、統一基準群の名称をサイバーセキュリティに置き換えたのだとすれば、この日本社会の無言の「言霊圧力」は侮れない。情報セキュリティにかかわってきた筆者としては胸騒ぎが収まっていない。

（８）結語：両者との実務的な望ましい付き合い方

国の政策については、上述したとおりこれまでは「サイバーセキュリティ政策」の名前のもとに、実務的には「情報セキュリティ政策＆サイバーセキュリティ政策」が行われてきたわけであるが、一般論としても、情報セキュリティ対策の裏打ちのない純粋サイバーセキュリティ対策のようなものは有効性に疑問符が付くだろう。

企業においても、仮にサイバーセキュリティ対策（CS）という説明を経営幹部にしていたとしても、実際に行う対策は情報セキュリティ対策（IS）と併せて「CS on IS」又は「CS with IS」であると思われる。

これまで情報セキュリティ対策を丁寧に行ってきた多くの組織の立場で考えてみると、サイバーセキュリティ対策の観点から見て必要となる対策の大半は、既に実施済みのはずである。一方で、毎年 PDCA を回して新規に直面する新たな要素は、殆どがサイバー空間で発生していると思われる。従って情報セキュリティ対策の側面から対策メニューを考えた場合であっても、新たな課題はサイバー空間対応が最重要となって、新規の対策要素は大半がサイバーセキュリティ対策と位置付けても良いであろうことも容易に想像できる。

つまりこういうことだ。

「サイバーセキュリティ対策の充実は現代社会が直面する大きな課題である。」
「情報セキュリティ対策を丁寧に実施すれば、サイバーセキュリティ対策も大半カバーされている。」
「情報セキュリティ対策の裏打ちのないサイバーセキュリティ対策は画餅。」
「実のあるサイバーセキュリティ対策は必ず情報セキュリティ対策の土台の上にある。」

そこで実務的観点から両者との望ましい付き合い方を考えてみたい。これが今回のこのコラムの結語である。

対策立案にあたって重点をサイバーセキュリティに置くことは今日的には自然な選択である。しかし、情報セキュリティを怠って良いわけではなく、実務的には情報セキュリティ対策的なアプローチで考えたほうが対策洩れは少ないはずである。

組織のセキュリティ対策は、情報セキュリティ対策的な下地をきちんと作ったうえで、サイバーセキュリティ対策的に点検してみる、という段取りで行うことが効果的であり、その上で組織幹部への説明には情報セキュリティでもサイバーセキュリティでもどちらでも通りやすい方ですれば良い。このような対応が両者との望ましい付き合い方ではないだろうか。

いずれにしても理解しておくべきことは、「情報セキュリティの時代が終わってサイバーセキュリティの時代になったのではなく、**情報セキュリティが一定の水準に確保できているならサイバーセキュリティに重点を置くことが可能であり現実的である**」という両者の関係である。

---

[1] https://www.enisa.europa.eu/about-enisa/accounting-finance/files/annual_accounts_2005.pdf --- enisa.europa.eu の現在の公表資料の中で「英語の旧名称」を確認できる文書（最古ではないかもしれない）

[2] https://www.enisa.europa.eu/about-enisa

[3] https://www.enisa.europa.eu/news/enisa-news/enisa-15-years-of-building-cybersecurity-bridges-together

[4]政府機関等の情報セキュリティ対策のための統一基準群（平成 30 年度版）
https://www.nisc.go.jp/policy/group/general/kijun.html　の改訂履歴　統一基準群（平成 30 年度版）

[5]政府機関等のサイバーセキュリティ対策のための統一基準群（令和3年度版）
https://www.nisc.go.jp/policy/group/general/kijun.html

[6]政府機関等の対策基準策定のためのガイドライン（令和3年度版）
https://www.nisc.go.jp/pdf/policy/general/guider3.pdf