防衛取得研究「情報セキュリティの現状と趨勢について」

研究員　上野　登

はじめに

2018 年 2 月 9 日付の日本経済新聞の第 1 面に「サイバー対策 米基準要求 防衛省、調達先 9000 社に」という記事が掲載された。記事の内容は、防衛省が米国基準の包括的なサイバー防衛策を取引企業に義務付ける調整に入ったというもので、米国の「秘密ではないがその取扱いに注意を要する重要な情報（CUI：Controlled Unclassified Information）」の取扱いについて定めた連邦基準（NIST SP800-171）に準じた（盛り込んだ or 同程度の）基準を導入するというものである。

その先には、現在、急速に拡大している情報ネットワークの「クラウド」化を見据えることができる。「クラウド」とは、簡単な言い方をすれば、企業や個人が、自らのサーバーに情報データを保存するのではなく、クラウドサービスを提供する企業等が管理するデータサーバー等を利用して、インターネット上に情報データを保存し、（場合によってはアプリケーションの使用も含めて）利用すること、あるいはそのサービスのことである。「クラウド」という言葉は、「雲」そのもので、ネットワーク図を作成する際に、ネットワーク上のどこかにあるものを雲の絵を使って表わすことに由来するものである。

防衛省では、秘密の情報（特別防衛秘密、特定秘密、省秘等）の取扱いについては、防衛省・自衛隊においても、関係する防衛関連企業においても、情報システム上では、他の情報とは別の独立したシステムあるいはスタンドアローンで取り扱うよう厳格に規定している。

一方、防衛省で定める「保護すべき情報（『注意』や『部内限り』に相当：後述）」の取扱いについては、防衛関連企業に対し、「装備品等及び役務の調達における情報セキュリティの確保に関する特約条項（防経装第 9246 号 21.7.31 別紙）」いわゆる「情報セキュリティ特約」において規定されている。今回の報道は、この「保護すべき情報」の防衛関連企業における取扱いについて、セキュリティが確保されたクラウド環境を利用するよう推奨され、あるいは義務化が予想されることから、各企業には大きな影響を与えるものと認識するので、欧米や我が国における関連する動向について、小論で取り扱うこととする。

1　欧米の動向

(1) 米国の動向

米国では、現在、官民挙げての情報システムのクラウド化が加速している。2010 年 11 月、当時のオバマ大統領が大統領令（Executive Order） 13556 を発出し、「保護すべき情報」または「管理すべき重要情報」あるいは「取扱い注意情報」と呼ばれる CUI について、どのように取扱わねばならないかを体系的規定を定めるよう指示した。そして、その結果、NIST（米国商務省国立標準技術研究所（National Institute of Standards and Technology））は、NIST SP800-171「連邦政府機関外の組織及び情報システムに対する CUI の保護について」の基準（ガイドライン）を策定し、連邦政府機関外の組織に対し、CUI についてどのように管理するかの基準を定めた。

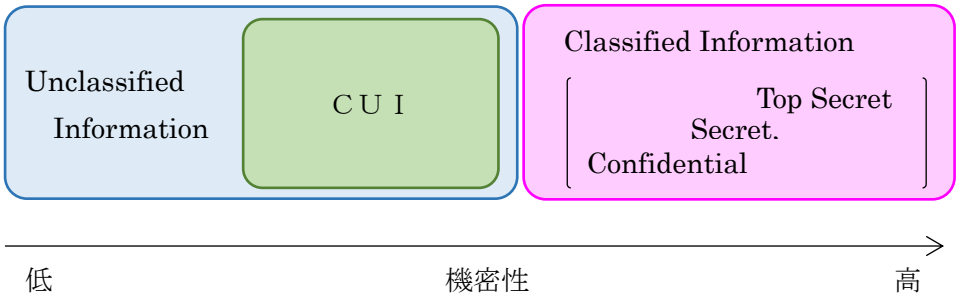
また、国防省（DoD：Department of Defense）は、2016 年 10 月に国防省調達規則補足（DFARS：Defense Federal Acquisition Regulation Supplement）252.204.-7012「軍事上の CUI の保護とサイバーインシデント報告」を発簡し、国防省との調達契約に関わるすべての企業とそのすべてのサプライヤー（下請け）に対して、2017 年（昨年）12 月 31 日までに NIST SP800-171 への対応を義務付けた。

そして、さらに、米国政府は、その他の業界に対しても、その適用を計画しており、現在実施時期を検討していると聞く。今後、連邦調達基準（FAR：Federal Acquisition Regulation）において、他の業界に対する NIST 適用を指示する見込みであり、多くの業界が 2019 年上期までに対応することになると予想されている。

NIST SP800-171 はそもそも、情報システムの利用について、民間企業の知的財産を保護し安全保障に不可欠な米国経済の強さを発揮するために、技術的にセキュリティの効いたシステム環境の中で CUI を管理し、取扱い、広く情報を共有するとの発想で、米国政府のクラウド調達のセキュリティ基準である FedRAMP（Federal Risk and Authorization Management Program：オバマ政権が 2011 年 12 月に定めたクラウドサービス及び関連商品のセキュリティをコントロールベースラインで評価する標準）に準拠したクラウドサービスの利用を推奨しているものである。これが、米国では、現在、官民挙げての情報システムのクラウド化が加速している所以である。

また、米国がクラウド化を推進している背景の１つには、サイバーセキュリティ人材を企業ごとに集めることが困難な事情があるという。そのため、サイバー攻撃に対処する人材をクラウドサービスの提供会社に集約し、セキュリティレベルの高いサービスを普及させることで民間企業への攻撃にも対処できる体制づくりが可能になることを期待しているものである。

ところで、米国における情報として機密性の観点から分類すると、機密性の高い順に、機密（Top Secret）、極秘（Secret）、秘密（Confidential）などのいわゆる秘密情報（Classified Information）と、秘密に格付けされない一般情報（Unclassified Information）に分類される。ただし、その一般情報の中の一部の重要な情報に、「保護すべき情報」または、「管理すべき重要情報」あるいは「取扱い注意情報」と呼ばれる CUI（Controlled Unclassified Information）が存在している。図示すると次のようなイメージとなる。



秘密情報は、国防省が規定し、民間においては、国家産業保全プログラム（NISP：National Industrial Security Program）、国家産業保全プログラム運用規則（NISPOM：National Industrial Security Program Operation Manual）に基づき管理されている。

CUI については、前述の大統領令 13556 に、「such as information that involves privacy, security, proprietary business interests, and law enforcement investigations」すなわち「個人情報、安全保障、企業の占有情報及び捜査情報を含むような情報」と定義されており、「秘密」ではないものの、企業における従業員名簿やスケジュール管理表、仕様書や設計図などもその対象となる。集積すると秘密を類推することができたり、企業の競争力を損なうこととなったり、さらには軍事外交等、安全保障に関わるような広範囲なもの（情報）とみなすことができる。従前の国防省の SBU（Sensitive But Unclassified ）や FOUO（For Official Use Only）は、この CUI に包含されたものであると考えられる。

この CUI については、米国立公文書記録管理局（NARA：National Archives and Records Administration）が一括して管理しており、「CUI Registry - Categories and Subcategories」において、農業、重要技術情報、重要インフラ、非常事態管理、輸出管理、金融、地政学的情報、移民政策等、多方面の２３のカテゴリーに分類されている。

NIST SP800-171 と ISO 基準の情報セキュリティマネジメントシステム

である ISMS（ISO/IEC27001:2014）を比較すると、NIST の要求事項は 110 項目、ISMS の要求項目は 114 項目であるが、NIST はより具体的な指針であると考えられており、ISMS を包含していると見做されている。例えば、ISMS は、情報システムや組織そのもののサイバーセキュリティを向上させるフレームワークとして、サイバーセキュリティを「特定」、「防御」の２段階で考える枠組みであるのに対し、NIST は、「特定」、「防御」、「検知」、「対応」、「復旧」の５段階とし、ISMS の「特定」、「防御」のあとに「検知」、「対応」、「復旧」の概念とそれぞれの要求項目に対して技術的な推奨事項が存在する点にある。NIST の要求事項と ISMS の要求事項を比較すると、NIST は ISMS より約３０％ほど広い概念（より具体的）との見方もある。

なお、NIST SP800-171 については、米国防省との調達契約に関わるすべての企業とそのすべてのサプライヤー（下請け）に対して、2017 年（昨年）12 月 31 日までにその対応を義務付けられたと述べたが、米国防省調達契約に我が国の法人が参画した場合も適用になることは当然視されているものの、現時点では、米国政府と我が国政府ほか、数か国の政府とその適用を巡って交渉の途上にある。

(2) ＥＵの動向

一方、ＥＵにおいても米国同様、各企業のクラウド化促進の様相を呈している。2016 年 7 月、欧州ネットワーク情報セキュリティ庁（ENISA：European Network and Information Security Agency）は、米国 NIST と連携し、法的拘束力を持つ NIS Directive を施行した。内容については、①加盟国ごとのサイバーセキュリティ能力の確立、②加盟国間の具体的協調強化、③重要なサービスとデジタル・サービスプロバイダーの明確化、④これらの運用者のために特別な義務を課す、等であり、すなわち、ＥＵ市場で活動する企業に対して、すべての情報データを取扱うシステムについて、前述の米国 NIST 基準に事実上準じた標準で指定された技術体系の採用を義務付けるものである。実施期日は、2018 年 5 月 10 日までであり、各企業には早急な対応が迫られているものである。

さらにＥＵにおいては、従前の EU データ保護指令（Data Protection Directive 95）に代わり、2016 年 4 月に EU 一般データ保護規則（GDPR：General Data Protection Regulation）が制定された。これは、ＥＵ域内における新しい個人情報保護の枠組みであり、個人データ（personal data）の処理と移転に関するルールを定めた規則である。厳しい罰則規定があり、EU 加盟諸国に対して直接効力が発生するばかりでなく、現地で事業を展開する日本法人にも適用される。これは、この GDPR を遵守しなければ、ＥＵ内での企業活動が実施できないことを示す非常に厳しい規定である。本規

則は、2 年間の移行期間を経て、2018 年 5 月 25 日より適用されることとなっている。

2　我が国の動向

(1)　日本政府等の取り組み

政府与党である自由民主党は、2017 年 5 月、政務調査会 IT 戦略特命委員会における「データ立国による知的社会への革新に向けた提言『デジタル・ニッポン 2017』」の中で、「日本がサプライチェーンマネジメントの最下層までサイバーセキュリティの国際標準技術を搭載（適用）するには、変化し続ける国際標準に対応する“日本版 FedRAMP”クラウドを創設し、これを企業が利用していれば国際標準に準拠していると言える IT インフラを提供していくべき」と提言している。

学会レベルにおいては、多摩大学において、多摩大学大学院教授國分俊史氏を中心にルール形成戦略研究所を立ち上げ、上記取り組みを推進している。

(2)　経済産業省の取り組み

経済産業省は、2017 年 3 月に、「製造産業における重要技術情報の適切な管理に関する基準となる考え方の指針（通称、『重要技術情報ガイドライン』）」を策定し、その中で、国際的産業競争力維持の観点から、「①製品を分析するだけでは模倣が難しく、技術流出による影響が大きい重要技術に関する情報や②その重要技術に関する情報を権利化した場合でも、権利侵害の探知や立証が難しいものの情報」を「重要技術情報」と定義し、その適切な管理について基準となる考え方を示した。さらに、2017 年 9 月 6 日付の日経新聞などの情報によると、経済産業省は、今年 2018 年 9 月を目途に「産業競争力強化法改正案」を国会に提出し、重要技術情報の管理の法制化を目指しており、「重要技術情報」の細分化と管理技術の管理要求事項の義務化、そして新たな認証制度の制定に向けて検討中であると言われている。

(3)　防衛省の取り組み

防衛省では、「装備品等及び役務の調達における情報セキュリティの確保について（通達）」（防経装第 9246 号 21.7.31）において、「防衛省の職員以外の者にみだりに知られることが業務の遂行に支障を与えるおそれのある情報（『部内限り』）や「当該事務に関与しない職員にみだりに知られることが業務の遂行に支障を与えるおそれのある情報（『注意』）」を「保護すべき情報」と規定している。その「保護すべき情報」の取扱いについては、前述したとおり、防衛関連企業に対して、「情報セキュリティ特約」において、規定しているが、この「保護すべき情報」が、米国における「CUI」

に近い概念と考えてよい。

防衛省は、来年度（平成 30（2018）年度）予算案において、「防衛調達における官民双方での保全体制の強化」の項目の中で、「標的型によるサイバー攻撃等に対し、官民間において安全な情報共有を行うため、既存の電子メールに信頼性の高い電子証明書を整備するとともに、今後のクラウド環境を見据えた官民情報共有環境のあるべき姿に関する調査研究」を行う事業を計上している。

その具体的な取り組みとしては、来年度下期を目途に、「情報セキュリティ特約」等を改訂し、その中で「保護すべき情報」について再定義し、現在の「部内限り」に相当する情報を伴う契約については、防衛省と防衛関連企業間、あるいは防衛関連企業間のインターネット上の情報交換について、まずは、成りすまし防止と改ざん防止の観点から S/MIME（Secure / Multipurpose Internet Mail Extensions：カプセル化した電子メールの公開鍵方式による暗号化とデジタル署名に関する標準規格）を導入し、2018 年度下期に試行、2019 年度から本格運用に移行する方針である。そして、「注意」に相当する情報については特に触れられていないが、おそらく、これから述べるクラウドの中で取り扱われるものと推察する。

さらに、記述した欧米の動向を視野に入れ、また、かつ、自由民主党政務調査会 IT 戦略特命委員会における「デジタル・ニッポン 2017」の提言の後押しを受けて、国内防衛産業が防衛関連業務を履行する際の現行セキュリティ基準を NIST 標準と同程度まで強化し、FedRAMP レベルのクラウドサービスの利用を見据えた新セキュリティ基準を策定するとともに、当該新基準を政府部内の関係機関と共有する方向で検討が進められている。

新たな国際標準に対応した新セキュリティ基準の策定は来年度末に、また、その準備期間に 2019 年度の 1 年間があてられ、2020 年度には本格運用が開始されるものと見込まれている。

この動きが冒頭で引用した新聞記事の内容であり、国内防衛産業におけるクラウド化を推進する大きなうねりのひとつと捕らえることができる。

(4) J-Bridge 構想

既述したように、欧米ではすでに、官民を挙げて、セキュリティの確保された、アクセス権限を保有する者の間で、CUI レベルの重要な情報を共有できる環境を担保できる、NIST SP800-171 や FedRAMP の基準を満足したクラウドサービスの導入に拍車がかかっている。我が国においても、大手銀行が米国系クラウドサービスを利用を開始したことが話題になった。防衛省が NIST SP800-171 と同レベルのすなわち世界レベルの新基準を策定して同レベルのクラウドサービスが導入することについては既に既定路線

化し、検討を進めていることは既述のとおりである。しかし、国（防衛省等）が主体的に整備するシステム環境を指定することは可能であろうが、国が民間業者に対して民間ブランドのクラウドを指定してその利用を義務化したり、強制したりすることは、我が国の国情として、極めてハードルの高いものであると思われる。

一方、既に我が国の一部大手 IT 関連企業において、NIST 基準を満足するクラウド環境を先取りした形で自主的に整備して、特に、防衛関連企業に向けたサービスを開始しようとする動きがある。「J-Bridge 構想」というプロジェクトがこれに該当する。

この「J-Bridge 構想」の最も注目すべき点は、クラウドと言いつつ、特に防衛産業関連の重要な情報を日本国内のデータセンターで管理することにより、我が国の知的財産の維持を担保でき、非常時等の安全保障上の担保が得られることになる。また、NIST 基準（＝世界基準）を満足する（≒数年後に予想される防衛省の新基準）情報システムを利用するということは、企業自身の世界的ブランド力を高め、ひいては産業競争力向上に寄与できるものと認識している。

さらに、NIST 基準に要件を満足させるためにはクラウドの利用なしではセキュリティ確保に膨大なコストがかかる恐れがある。そのため、防衛省契約のサプライチェーンの第２層、第３層…の多くは中小企業であり、コンピュータシステムの通信監視、安全性の確保に対するコスト等の低減対策としては極めて有効である。

この“日本版 FedRAMP”の嚆矢（こうし）である「J-Bridge 構想」については、特に防衛産業がクラウド化の牽引役として、是非、成功させなければならないと認識している。

おわりに

小論においては、主に NIST SP800-171 をめぐる欧米、我が国における動向について触れてきた。

我が国の政府担当者や官庁、企業経営者の多くはいまだに「クラウド」に不信を抱いているかもしれないし、サイバーセキュリティの視点からの有効性に関する認識が低いのではないかとも思われる。それが、我が国が NIST などの世界標準の導入に出遅れている理由かもしれない。NIST 基準（≒今後予定されている防衛省の情報セキュリティ新基準）を満足しなければ、クラウドが利用できないのではなく、クラウドを利用するということがすなわち、NIST 基準の管理策の要求事項の多くの部分を満足することと認識している。

我が国における新セキュリティ基準の策定と履行は、諸情勢から判断すると今まで述べてきたとおり、急務である。また、クラウドの利用者からの視点で考えると、そのクラウドを利用すれば、「セキュリティを確保しつつ、使いたい情報が不自由なく入手できる」ことが重要であり、そのためには、まずは防衛関連企業が率先して、そのクラウド利用に対して資本投下（トータルコストは低減される。）をし、関連する情報を（例えば、プロジェクトごとに）集積することがその成功の秘訣であると考える。

全世界的な NIST レベルの新基準の適用とクラウド化は進むべくして進まざるを得ない大きな流れである。それを牽引するのは、防衛産業界、防衛関連企業であることは間違いない。