**日本企業も対策待ったなし？　米国のセキュリティ基準「NIST SP800-171」が与える大きなインパクト**

* 大河原 克行

2018年9月18日 06:00

* [リスト](https://twitter.com/search?ref_src=twsrc%5Etfw&q=https%3A%2F%2Fcloud.watch.impress.co.jp%2Fdocs%2Fevent%2F1143350.html)

　NIST（米国標準技術研究所） SP800-171相当のセキュリティ対策を求める新防衛調達基準の試行導入が、2019年度から日本で始まる。

　対象となるのは、防衛省との取引がある約9000社の企業となるが、こうした動きはグローバル展開をしている国内企業全体に波及し、しかも幅広い業種に及ぶことになる。専門家は、「グローバル企業にとどまらず、中小企業を含む日本のあらゆる企業が、NIST SP800-171に準拠したITシステムを導入することが最適である」とさえ指摘する。

　株式会社日本HPが2018年9月14日、東京・後楽の東京ドームホテルで開催した「経営戦略としてのサイバーセキュリティ～米国NIST標準のセキュリティフレームワークとその対応ソリューション～」と題したセミナーでは、この分野に詳しい、多摩大学大学院教授 ルール形成戦略研究所の國分俊史所長のほか、防衛装備庁の藤井敏彦長官官房審議官や、自由民主党 行政改革推進本部本部長である甘利明氏が登壇して、政府を挙げて、この動きに注目し、対応をはじめていることを示すものになった。

[](https://cloud.watch.impress.co.jp/img/clw/docs/1143/350/html/340_o.jpg.html)

日本HPは「経営戦略としてのサイバーセキュリティ～米国NIST標準のセキュリティフレームワークとその対応ソリューション～」と題したセミナーを開催した

[](https://cloud.watch.impress.co.jp/img/clw/docs/1143/350/html/357_o.jpg.html)

講演では自由民主党 行政改革推進本部本部長である甘利明氏も登壇した

　同セミナーの参加対象企業は、防衛省と取引がある企業や自動車産業のIT部門や経営層、国民生活や社会経済活動の基盤を担う重要インフラ産業の関係者としていたが、IoTのビジネス利用を検討中の企業や、Society 5.0をにらんだIT基盤の導入を検討中の企業など、あらゆる産業の顧客も参加。約500人の参加者が、企業が今後取り組むべきサイバーセキュリティの新たな基準について情報を共有するものになった。

　米国では、企業のITシステムの調達が変化するとともに、IT産業全体の成長をけん引するできごとになるとも予測されているだけに、日本においても徐々に関心が高まりつつあることを裏付けたセミナーになったともいえるだろう。

　NIST SP800-171が、IT産業や日本の企業に及ぼす影響を追った。

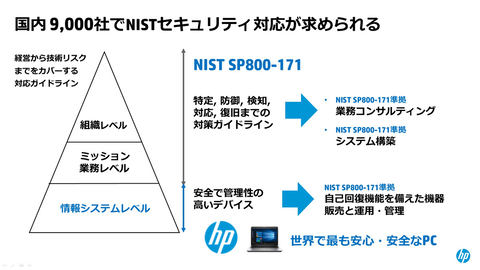
**NIST SP800-171とは？**

　まずは、NIST SP800-171がどういったものなのかを知っておこう。

　NIST SP800-171とは、米国政府機関が調達する製品や技術などを開発・製造する企業に対して、一定のセキュリティ基準に準拠するように求めるガイドラインだ。

　具体的には、保全が必要な情報（Controlled Unclassified Information：CUI）について、調達先企業などが取り扱う際に順守すべきセキュリティ要件を定めており、企業などの非政府機関がCUIを扱う場合において、14分野109項目にわたる具体的なセキュリティ要件を示している。

　これによって、米国政府機関が使用する機器などがハッキングされにくい環境や、取引先からの情報漏えいを阻止することを目指しているというわけだ。

[](https://cloud.watch.impress.co.jp/img/clw/docs/1143/350/html/372_o.jpg.html)

国内9000社でNISTセキュリティ対応が求められる

　実は、ステルス戦闘機である「F-35」の開発において、契約事業者である豪州の防衛企業が脆弱なIDとパスワードを利用していたため、F-35に関する30GB分のデータが盗まれたという事件が発生したことがあった。

　政府機関だけを守るのではなく、こうした取引企業からの情報漏えいが発生しないように、NIST SP800-171では、取引企業においても一定水準のセキュリティ強化を求める内容になっているのだ。

　2016年10月、米国防総省は取引を行うすべての企業に対して、NIST SP800-171に準拠したITシステムを利用し、機密情報およびCUIを扱わなければならないとの通達を出している。そして2017年12月31日までに、これを順守するように徹底した。

　こうして2018年1月以降、米国政府調達にかかわるすべてのサプライヤーと納入される製品、技術、サービスは、NIST SP800-171の条件を満たす必要が生じているのだ。これは米国内の企業だけでなく、米国防省と取引がある全世界の企業が対象になる。

　しかも、米国政府だけの取り組みにとどまらず、米国政府は国際標準化することも検討しているほか、主要国でもこの動きに追随する流れがすでに出始めている。

　そのひとつが日本である。

　日本政府は2017年2月に、防衛調達における情報セキュリティ強化に関する官民検討会設置し、防衛調達における新情報セキュリティ基準策定の検討を開始。2018年9月までに7回の検討会を開催して、ここで設ける基準をNIST SP800-171と同等にすることを決定した。

　防衛装備庁 長官官房審議官の藤井敏彦氏は、「海外との共同研究、開発が多い防衛調達においては、同盟国と同等のセキュリティレベルを維持することが重要な課題となっている。NISTのサイバーセキュリティの標準に対応した新しい調達基準はそのためのものである」とし、「防衛省や防衛装備庁のなかを守ればいいというわけではない。調達に関しては、一般企業を含むサプライチェーン全体において、機微な情報を守る必要がある。そのためには、防衛調達における契約企業に適用されるセキュリティ基準を、米国の新たな基準と同程度まで強化する必要がある」と語る。

　日本においても、防衛省と取引があるすべての企業は、2019年度以降、NIST SP800-171と同等のセキュリティレベルを持つ必要がある。対象となる企業は約9000社と見られている。

[](https://cloud.watch.impress.co.jp/img/clw/docs/1143/350/html/369_o.jpg.html)

防衛装備庁 長官官房審議官の藤井敏彦氏

**CUIは「米国にとっての重要情報」**

　NIST SP800-171の動きに関して、注目しておきたいポイントがいくつかある。ひとつは、CUIの定義だ。

　CUIは非秘密情報ではあるが、「米国にとっての重要情報」という意味を持つ。機密情報そのものではないが、これらを広範囲に集めれば機密が特定される可能性がある情報といった意味合いでとらえることができるだろう。しかもそれが、米国政府が持つ情報だけでなく、一般企業が生成したり、保持したりする情報も含まれる。

　そして重要なのは、企業側の意図とは別に、政府側がそれらの情報がCUIである、ということを定義する点だ。

　米国では、2010年のオバマ大統領による大統領令によって、各省庁がCUIに該当する情報を定義した。2016年9月には連邦規則で、CUIを処理、格納、通信する民間企業に対して、ITシステムを特定の技術体系で構築して、CUIを保護することを義務づけた。

　定義されたCUIのなかには、ヘルスケア企業が持つ個人情報、自動車メーカーが持つ自動走行のテストデータ、通信事業における基地局の通信データなどが含まれる。

　多摩大学大学院教授 ルール形成戦略研究所の國分俊史所長は、「米国政府と取引をするのであれば、NIST SP800-171に準拠したITシステムに移行しなくてはならないのとは当然だが、北米事業を行う日本の企業は当該情報を取り扱っている可能性が高く、グローバル展開をしている企業であれば、米国政府と直接的に取引していなくても、NIST SP800-171に準拠する必要が出てくる」と指摘する。

[](https://cloud.watch.impress.co.jp/img/clw/docs/1143/350/html/388_o.jpg.html)

多摩大学大学院教授 ルール形成戦略研究所の國分俊史所長

**情報システムの調達・運用に対して影響を及ぼす？**

　2つめのポイントは、NIST SP800-171が、多くの企業にとって、情報システムの調達・運用に対して影響を及ぼす可能性があるという点だ。

　米国政府においては、現在、国防総省が先行してNIST SP800-171を徹底しているが、すでに一部省庁でも、NIST SP800-171を前提にした調達を開始している例が出ている。国防総省以外と取引する企業にも波及し始めており、政府全体にこの仕組みが広がる前に、早期に対応する必要が出ているのだ。

　さらにNIST SP800-171は、政府調達において直接取引する企業だけでなく、それらの企業とサプライチェーンでつながる企業にも影響を及ぼす。

　「政府と直接取引する企業にとっては、調達先もNIST SP800-171になっていなければ、問題が発生する可能性がある。しかも、それが製品や技術を生産、開発する企業だけでなく、政府に納入する物流を行う企業に対しても用いられることになる。多くの企業において、NIST SP800-171への準拠が求められることになる」と、多摩大学の國分所長は語る。

　例えば、米政府と直接取引を行う企業から見て“孫孫請け”という、かなり離れた立場の会社であっても、導入するPCがNIST SP800-171の基準を満たしたPCであることはもちろん、そのPCを搬入する物流会社の選定においても、NIST SP800-171を満たしたITシステムを導入している企業でなくてはならない、といったことが発生することになる。すでに、米国の大手物流会社はそれへの対策を実施済みだという。

　多摩大学の國分所長は、「NIST SP800-171のガイドラインを満たしていなければ、取引から除外される可能性がある。日本の企業は、NIST SP800-171に準拠することに対して強い危機感がない。これに準拠しなければ『調達先対象から外れてくれ』と言われる危険性を持った経営体制であることを、知らなくてはならない。企業経営を左右するできごとである。これを無視して、グローバル経営を推進することはできない。危機感を持たないことは、市場環境を誤認した状態で経営をしているのと同じだ」と、警笛を鳴らす。

　NIST SP800-171によって示されたセキュリティ要件を満たさない事業者や製品、サービスはグローバルサプライチェーンからはじき出される恐れがあるというわけだ。

　「米国政府機関が調達する製品や技術だから、『当社には関係がない』とか、『影響があるのは防衛関係だけ』という考え方は通用しなくなる」と語る。

　米国においては、業界団体が率先してNIST SP800-171への対応を推進しているところだ。

　全米自動車産業協会（AIAG）では、2018年5月から参加企業に向け、NIST SP800-171のガイドラインに対応する姿勢を明らかにするとともに、それを支援する体制を構築。北米電力信頼度協議会（NERC）や官民連携R＆Dセンター（NCCoE）でも、同様の動きを開始している。

　また、マイクロソフトやHP.incなどの主要IT企業は、製品やサービスが準拠していることを明確に示すといった動きも加速している。

　HP inc. セキュリティリサーチ＆イノベーション担当フェロー兼バイスプレジデントのBoris Balache氏は、「デバイスの調達において、セキュリティ要件を含むべきであり、その最低限のレベルは、NIST SP800-171への準拠になる」とする。

　日本HPでは、NIST SP800-171に準拠し、自己回復機能を備えたデバイスを投入しているほか、NIST SP800-171に対応するための業務コンサルティングやシステム構築を用意していることを強調してみせた。

[](https://cloud.watch.impress.co.jp/img/clw/docs/1143/350/html/410_o.jpg.html)

HP inc. セキュリティリサーチ＆イノベーション担当フェロー兼バイスプレジデントのBoris Balache氏

[](https://cloud.watch.impress.co.jp/img/clw/docs/1143/350/html/345_o.jpg.html)

日本HPでは、NIST SP800-171に準拠した製品を用意。新たな政府調達基準に対応していることを強調した

　ちなみにクラウドサービスにおいては、Federal Risk and Authorization Management Program （FedRAMP）への準拠が、政府の活用において前提となっており、AWSやAzure、GCPが対応していることが、各社のサイトで公表されている。

　日本においては、現時点では防衛省の調達においてのみ、この基準が採用されるという段階であり、米国ほど多くの企業に影響を及ぼす段階ではない。しかし、今後の流れを考えると、国内のすべての企業がNIST SP800-171を視野に入れておいた方がいいだろう。

　防衛装備庁の藤井長官は、「防衛産業にかかわる企業以外も、こうした調達基準を用いることが、日本全体のセキュリティ環境を高めることにつながる」とする。

　経済産業省の産業サイバーセキュリティ研究会において、ワーキンググループ1では、制度・技術・標準化を検討。標準モデルとして、サイバー・フィジカル・セキュリティ対策フレームワークを策定しているが、そのなかで、今後は分野横断型サブワーキンググループを設置し、防衛産業だけでなく、ビル、電力、自動車産業、スマートホームなどの分野にも適用。「防衛産業の取り組みが、ほかの産業の道しるべになることを想定している」とする。

　「防衛産業だけが堅牢性を上げていくだけでなく、広い産業において、さまざまな企業が守らなくてはならいものは何かということを知り、自社のセキュリティ強化だけでなく、サプライチェーン全体でのセキュリティ強化に取り組んでほしいと考えている。パートナーから信頼されるセキュリティを構築する必要があるとした」とした。

　日本では、これまで、国際標準であるISO27001に準拠することが政府入札の条件になっていたが、多摩大学の國分所長は、「ISO27001は、情報セキュリティマネジメントシステムであり、精神論といえるものしか示されていない。NIST SP800-171は技術フレームワークであり、7割の項目が技術面から、何をどうすべきか、ということが細かく示されている。まったく異なる要件をクリアすることが、今後の政府入札に用いられる可能性がある」と指摘する。

　防衛装備庁の藤井長官は、今後の新たな調達基準の導入に向けて、「新基準に対して、コスト増にならないようにするための課題解決、国内事業者のクラウドサービスにおいて、NIST SP800-171に準拠したクラウドサービスが現時点ではないことの課題、下請けとなる中小企業に対するケアをどうするのかといった課題がある」と指摘した。

**NIST SP800-171に準拠しただけでは不十分？**

　そして3つめのポイントは、実は、NIST SP800-171に準拠しただけでは不十分であるという点だ。

　米国では、米国防省と取引がある企業は、2017年12月末までにNIST SP800-171への準拠を完了したが、この監査において、多くの企業が未対応であるとの判定を受ける事態が発生した。

　これには理由があった。米国防省は監査において、NIST SP800-53の基準を用いて監査を実施したからだ。

　NIST SP800-53とは、連邦政府情報システムおよび連邦組織を対象にしたセキュリティ管理およびプライバシー管理を定めたものであり、政府との取引先を対象に制定したNIST SP800-171よりも厳しい内容となっている。

　「NIST SP800-171では、CUIの管理においてパスワードをかけていることが示されているだけだが、NIST SP800-53では256ビット以上のパスワードであることが示されている。また退職した社員の情報についても、NIST SP800-53では自動的に削除されることが定められているが、NIST SP800-171の範囲では手作業でも構わない。こうした違いが、未対応との判定を下される要因になった」と、多摩大学の國分所長は説明。

　「NIST SP800-171に対応する際には、むしろ、NIST SP800-53に対応するという姿勢で取り組む必要がある。NIST SP800-171のガイドラインは忘れてもらった方がいい」とする。

　米国政府は、NIST SP800-171というガイドラインを示しながらも、政府と同等水準のセキュリティレベルを持つNIST SP800-53への対応を求めているのが実態だといっていい。

**これまでと異なる考え方が必要に**

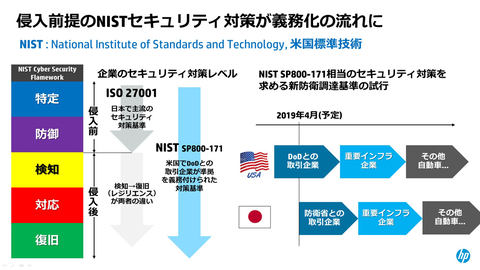
　なおNIST SP800-171は、IT産業におけるモノづくりの考え方や、ITを利用する企業の調達の仕方、運用の仕方に変化を及ぼす点も、見逃せない要素だ。

　モノづくりの観点では、NIST SP800-171においては、従来の「壊れない」、「防御すればいい」という考え方は通用せず、侵入されることを前提としたモノづくりを行い、ハッキングされたあとリブートするまでのシナリオを提示することが必要であると、多摩大学の國分所長は指摘する。

　「これは、単にログを取っておけばいいというIT産業的な考え方ではなく、製品の設計思想として、ハッキングされたことを前提とし、その解決に向けたシナリオを明確に示すことが大切になる。それを世界に対して説明することが必要である。壊れないモノづくりを目指してきた日本の企業には、発想の転換が必要になる」とする。

　日本は、IoT分野において、リーダー的存在の一角を担っているが、そのモノづくりにおいても、壊れないモノづくりからの発想を変えないと、調達から外れる可能性があるというわけだ。

　「IoT機器の設計段階で、考慮すべきサイバー攻撃のシナリオ数が、品質指標となってくる。その場合、日本のメーカーは劣位になる可能性がある」と指摘する。

[](https://cloud.watch.impress.co.jp/img/clw/docs/1143/350/html/371_o.jpg.html)

侵入前提のNISTセキュリティ対策が義務化の流れに

**ITシステムの調達・運用におよぼす影響**

　一方で、ITシステムの調達・運用においても、NIST SP800-171の影響は大きいという。

　米国政府では、調達における製品、技術、サービスの推奨リストを公開。その一方で、ブラックリストも公開している。そのなかには、「日本の製品もブラックリストに相当乗っている」と、多摩大学の國分所長は語る。

　NIST SP800-171においては、スマートフォン、アンチウイルス、仮想化、リモートアクセス管理などにおいて、日本の企業の製品がブラックリストに表記されているという。また推奨製品の範囲は、PC、スマートフォン、タブレットのほか、複合機、プロジェクターなどが含まれ、ハードウェアからソフトウェアまで幅広い。

　「どんなITシステムを調達するかが、企業経営にも影響する可能性を持つ」と、多摩大学の國分所長は語り、「サイバーセキュリティは、技術や情報漏えいの話でなく、経営戦略として考えていく必要がある。これからの時代は、技術の話ではなく、何を利用しているかが経営を左右することになる。ブラックリストに乗った製品を利用しているだけで、政府や政府と取引のある企業の調達計画の乗らないことになる。ブラックリストの製品を使ってITシステムを構築していては、問題が内在する形での経営をすることになる。裏を返せば、NIST SP800-171で推奨された製品や技術、サービスを利用していることが営業ツールになりうる」とする。

　こうしたなかで気になる動きが、米国が、安全保障政策のひとつとして、中国製のIT機器の利用禁止を発表。米政府および米政府と取引する企業、政府のデータを保有する企業に対して、これを順次実施しているという動きだ。

　米国では2016年に、米セキュリティ会社が、携帯電話のフラッシュメモリのファームウェアに仕込まれている不正プログラムを発見。これが、中国企業が開発・製造したものであり、ユーザーの同意なしに、72時間おきに携帯電話内の情報が中国のサーバーに送信されていることがわかった。

　こうした事件もあって、米国政府は、中国企業5社の電子通信製品の取引を禁止。これを部分的にでもITシステム内に利用する組織との取引も禁止した。

　また、豪州においては、5Gプロジェクトにおいて、重要情報漏えいへの懸念から中国企業の締め出しを決定するといった動きも出ている。

　現時点では、日本においてはこうした動きはないが、米国政府と密接な関係があり、米国政府の調達基準に準拠する流れがあるなかで、同様の判断が出る可能性もある。

　多摩大学の國分所長は、「日本の企業は、社内システムをどうするか、サプライチェーンをどう組むかといったことを考える必要がある。システムインテグレータをはじめとするIT関連企業も、プッシュする製品を変える必要がある」とする。

　NIST SP800-171が及ぼす影響は、現時点で、多くの人が思っている以上に大きいといわざるを得ないことを知っておくべきだ。