防衛装備庁

防衛装備庁が来年度から始める新たな調達基準の考え方

30.　9.14

防衛装備庁長官官房審議官
藤井敏彦

目 次

１．取組の全体像 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・１

２．デジタルガバメント推進に向けた取組 ・・・・・・・・・・・・・・・・・・・・・・・・・・・３

３．サイバーセキュリティ上の脅威の増大 ・・・・・・・・・・・・・・・・・・・・・・・・・・・５

４．米国における産業サイバーセキュリティ ・・・・・・・・・・・・・・・・・・・・・・・・・・７

５．我が国における産業サイバーセキュリティ強化の検討 ・・・・・・・・・・・・・・・・・・・１４

１．取組の全体像

我が国の契約企業に適用される現行の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し、契約企業が当該基準に適合するための方策について鋭意検討を行っている

１．取組の全体像

背景・前提

政府全体におけるデジタルガバメントの推進

- 官民間の情報共有のオンライン化・クラウド化
- 「行政サービスの１００%デジタル化」
- 「クラウド・バイ・デフォルト」

×

サイバーセキュリティ上の脅威の増大

- ランサムウェア
- サプライチェーンリスク（不正プログラムの仕掛け）
- サプライチェーンへのサイバー攻撃

↓

取組

サイバーセキュリティの強化

- 産業サイバーセキュリティ
  → サイバー・フィジカル・セキュリティ対策フレームワーク
- 防衛産業のサイバーセキュリティ
  → 防衛調達の新情報セキュリティ基準（NIST SP 800-171と同程度）
- セキュアなクラウドの認証
  → クラウドサービスの安全性評価

（参照の材料）

米国における強化されたサイバーセキュリティ基準

- NIST SP 800-171
- FedRAMP

- 米国を始めとする諸外国からの保全信頼性向上
- 防衛産業をハイレベルな産業サイバーセキュリティのモデルに

２．デジタルガバメント推進に向けた取組

２．デジタルガバメント推進に向けた取組

○　政府においては、成長戦略の一環として、行政部門のデジタル化によるビジネス環境の改善や行政手続きコストの削減、生産性の向上を強力に推進

○　具体的には、内閣総理大臣を本部長とする高度情報通信ネットワーク社会推進戦略本部（ＩＴ総合戦略本部）の下、**行政サービスの100%デジタル化**や、**クラウドサービスの利用促進**等、**デジタルガバメントの実現に向けた取組**を推進

【参考】

世界最先端デジタル国家創造宣言・官民データ活用推進基本計画（平成30年６月15日閣議決定）

第１部Ⅱ１（１）行政サービスの100%デジタル化

行政のあらゆるサービスをデジタルで完結させる（行政サービスの100%デジタル化）ために不可欠な３原則（デジタルファースト、ワンスオンリー及びコネクテッドワンストップ）に沿って、政府一体となってBPRを徹底し、手続オンライン化の徹底、添付書類の撤廃、ワンストップサービスの推進に取り組み、国民・企業の時間・労力の無駄を削減するとともに、行政運営の効率化を実現し、真に必要な分野・業務に行政資源を振り向けていくよう努める。

デジタルガバメント実行計画（平成30年７月20日デジタルガバメント閣僚会議決定）

４．２．１）ア．クラウド利用に関する考え方の整理（◎内閣官房）

投資対効果やサービスレベルの向上、サイバーセキュリティへの対応強化を図るため、政府情報システムの新規開発又は次期の更改、若しくは大幅な改修時期を見据えつつ、システムの方式として、クラウドの活用を推進する。
具体的には、各府省において、上記の「政府情報システムにおけるクラウドサービスの利用に係る基本方針」に基づき、各種クラウドサービスの利用を検討する。

３．サイバーセキュリティ上の脅威の増大

3．サイバーセキュリティ上の脅威の増大　～豪国防調達における具体的事例～

➢ 防衛関連企業に対するサイバー攻撃の事例

Source: The Wall Street Journal（Oct. 12,2017）

Cyberattack Captures Data on U.S. Weapons in Four-Month Assault

4か月間のサイバー攻撃で米国兵器に関するデータを収集

Attacker nicknamed 'Alf' gained access to Australian defense contractor's computers

'Alf' obtained data on Australia's planned purchase of up to 100 F-35 fighters, a senior Australian intelligence official said.
PHOTO: AUSTRALIAN DEFENCE FORCE HANDOUT/REUTERS

By Rob Taylor
Updated Oct. 12, 2017 7:27 p.m. ET

CANBERRA, Australia—A cyberattacker nicknamed "Alf" gained access to an Australian defense contractor's computers and began a four-month raid that snared data on sophisticated U.S. weapons systems.

Using the simple combinations of login names and passwords "admin; admin" and "guest; guest" and exploiting a vulnerability in the company's help-desk portal, the attacker roved the firm's network for four months. The Australian military referred to the breach as "Alf's Mystery Happy Fun Time," referring to a character from the soap opera "Home and Away."

The incident, detailed by a senior Australian intelligence official in a speech on Wednesday, was

purchase of up to 100 F-35 fighters made by Lockheed Martin , as well as information on new warships and Boeing -built P-8 Poseidon maritime-surveillance aircraft, in the July 2016 breach.

Boeing Co. declined to comment on the theft, which also included details of C-130 Hercules transport aircraft and guided bombs used by the U.S. and Australian militaries. A Lockheed Martin Corp. spokeswoman said the breach did not affect the multinational F-35 program and "all classified F-35 information was protected and remains secure".

"The compromise was extensive and extreme," Mr. Clarke said.

Some of the data stolen from the Adelaide-based engineering firm enabled the hackers to access design information "down to the captain's chair" on new warships for Australia's navy, he said. Adelaide is home to shipyards building destroyers with advanced U.S. Aegis radar systems for Australia's navy, part of a decadelong 200-billion-Australian-dollar (US$156 billion) military modernization.

The Chinese and U.S. embassies in Australia didn't immediately respond to requests for comment.

Mr. Clarke's speech—rare for a senior intelligence official—highlighted Australia's alarm about the vulnerability of cyberdefenses. Foreign Minister Julie Bishop said Thursday that intelligence agencies are aware of where the attack originated but said no classified details of weapons capabilities were lost.

While governments and defense giants such as Lockheed, Boeing and BAE Systems PLC have invested billions of dollars in cybersecurity, the Australian episode exposed the susceptibility of smaller firms as the defense industry becomes more global and projects more complex and costly.

Lockheed's radar-evading F-35 Joint Strike Fighter, for instance, contains components from

The contractor's identity in the Alf breach wasn't disclosed. The intruder went undetected until November, when another company in the defense supply chain alerted the Australian Signals Directorate—the country's equivalent of the U.S. National Security Agency, which oversees cyberdefense and signals intelligence.

Australia's defense industry employs around 27,000 people in 3,000 companies, including units of BAE, Raytheon Co. , Thales SA, Airbus SE and Boeing. The country manufactures command-and-control systems; military vehicles used by allies including Britain, Japan and the Netherlands; and phased-array radar used to defend warships against air and missile threats.

The targeted company was a small subcontractor several levels down from the prime contractor, Mr. Clarke said. The company had one employee to manage information technology, and that person had been in the role nine months, using a common local administrator account password that made it easier for the hacker to steal what Mr. Clarke described as a "good haul."

The hacker used a variety of malware, including an internet Trojan tool known as a "China Chopper," identified in 2012 and favored by Chinese hackers as well as cybercriminal networks and other nations. The China Chopper enables an attacker to use brute-force password guessing against login portals, then upload and download files on victim devices after gaining access.

Australia Defense Industry Minister Christopher Pyne, responsible for large military projects, said Thursday that the stolen information wasn't classified but was commercially sensitive.

The government couldn't directly oversee passwords and security arrangements used by every defense contractor, but the attack highlighted the need for smaller firms as well as defense giants to "get their cybersecurity right," Mr. Pyne said.

Australia's government reported this week that cyberattacks were increasing in number and sophistication, with 47,000 incidents last year.

・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に、豪州が調達予定であったロッキードマーチン社製のF-35に関する30GB分のデータに加え、ボーイング社製の対潜哨戒機に関する情報も窃取された。

・今回情報を漏洩した契約事業者は、プライムから２～3階層下に位置する中小企業であり、情報システム管理者も一人しかいないという状況であった。

・盗まれた情報は機密情報ではなかったものの商業的に重要なデータであった。

４．米国における産業サイバーセキュリティ

４．米国における産業サイバーセキュリティ　～NIST SP 800等～

➢　NISTシリーズの概要

○　NIST（National Institute of Standards and Technology：国立標準技術研究所）は、コンピュータ・セキュリティ関連の標準である**SP 800シリーズ**（※）や、**サイバーセキュリティ向上フレームワーク**などを発出

（※）SP 800シリーズのうち、例えば

- **SP 800-53は連邦政府の情報システム・組織のセキュリティ標準**
- **SP 800-171は連邦政府以外でCUI**（Controlled Unclassified Information：保護対象となる非秘密情報）**を扱う情報システム・組織のセキュリティ標準**

これらのセキュリティ標準は、**国際標準であるＩＳＯ/ＩＥＣ 27001（ＩＳＭＳ）よりも内容が強化**されており、インシデント防止（特定、防御）だけでなく、**インシデント発生以降**（検知、対応、復旧）**も十分にカバー**している点に特徴

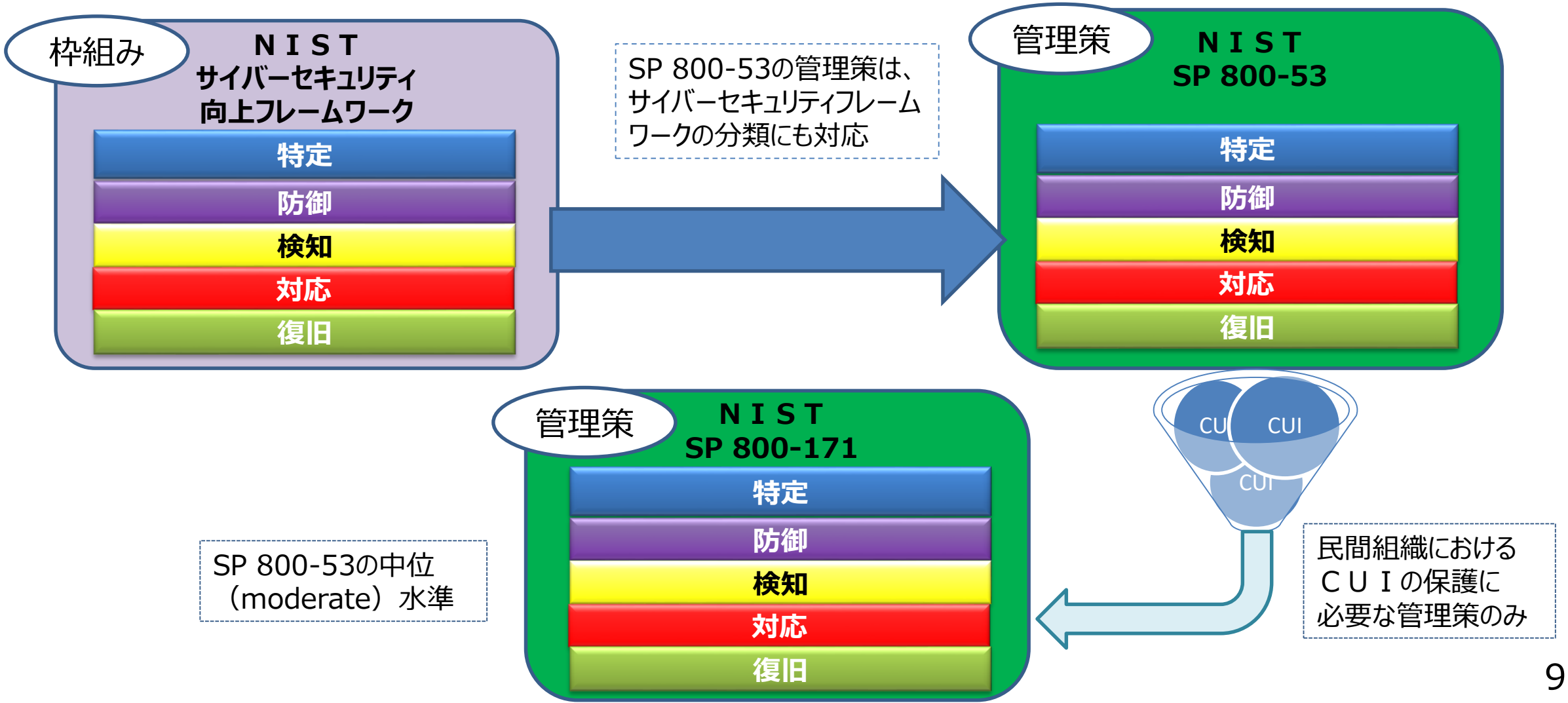
➢　CUIを取り扱う防衛関連企業へのNIST SP 800-171の適用

○　CUIについては、2010年11月の大統領令（E.O. 13556）発出以降、米政府全体として、セキュリティ強化の取組を実施

○　特に国防省との契約を通じて**CUIを取り扱う防衛関連企業**については、国防省は、2016年10月、DFARS（国防調達規則）252.204-7012を発出し、**2017年12月末までにNIST SP 800-171相当の情報セキュリティ対応を要求**

４．米国における産業サイバーセキュリティ　～NIST SP 800等～

- **NIST SP 800-53の管理策が基本**となっており、SP 800-171を含む各標準の管理策に対応
- **NIST SP 800-171**は、CUIの保護のために必要な管理策として、原則として、**SP 800-53における中位（moderate）水準を満たすことを要求**



４．米国における産業サイバーセキュリティ　～NIST SP 800等～

➢ NIST SP800-171とNIST SP800-53の対応の例：NIST SP800-171の3.6.3

SP800-171	NIST SP800-53		
	Control Number	Control Description	Supplemental Guidance
3.6.3 組織のインシデント対応（Incident Response）能力をテストする。	IR-3	組織は、［指定：組織が定めたテスト］を用いて、情報システムのインシデント対応能力を［指定：組織が定めた頻度で］テストし、インシデント対応の有効性を判断した後に、結果を文書化する。	・組織は、インシデント対応能力をテストして、そうした能力の全般的な有効性を判断し、弱点または欠陥を特定する。 ・インシデント対応テストには、たとえば、チェックリストの使用、実地訓練または机上訓練、シミュレーション（平行した、完全な割り込み型の）、包括的な訓練がある。 ・インシデント対応のテストには、また、インシデント対応が組織の業務にもたらす影響（例：ミッション遂行能力の低下）と、組織の資産や個人にもたらす影響の判断も含まれる。
	IR-3 （１）	組織は、インシデント対応テストを、関連する計画に責任のある部署との間で調整する。	・インシデント対応テストに関連する計画には、たとえば、事業継続計画、緊急時対応計画、災害復旧計画、政府存続計画、緊急時コミュニケーション計画、重要インフラ計画、居住者非常時計画がある。

４．米国における産業サイバーセキュリティ　～クラウドサービスのセキュリティ～

➢ 米国では、政府及び企業のシステムについて、クラウド化をミニマムスタンダードにしていくことを前提に、サイバーセキュリティの技術レベルの国際標準作りをリード

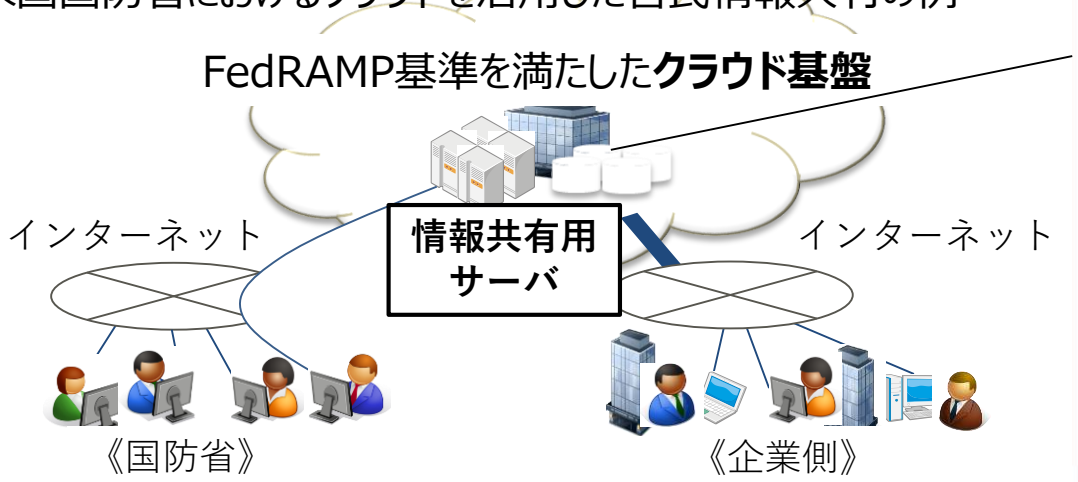
➢ 具体的には米国政府のクラウド調達の基準である「FedRAMP」（※）が国際標準となっていく可能性

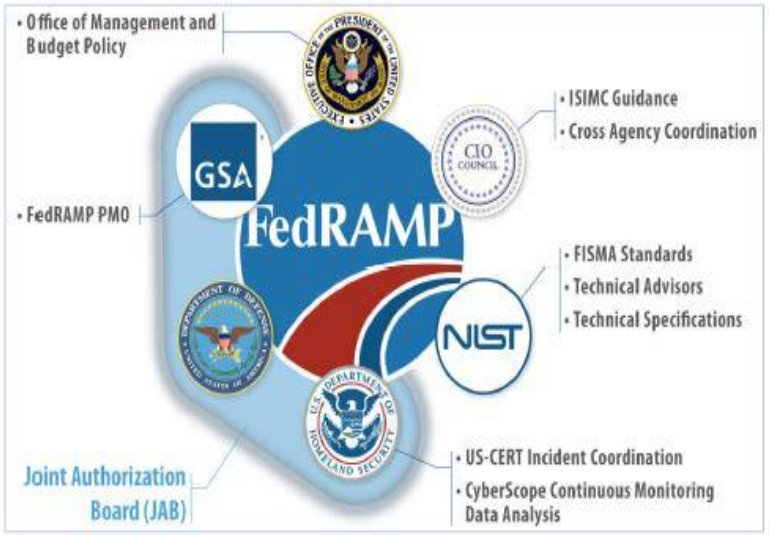
（※）Federal Risk and Authorization Management Program

・DFARS （国防調達規則）252.204-7012による要求事項

契約業者が、契約の履行に際して、外部のクラウドサービスプロバイダを使用して、保護対象防衛情報を保存・処理・送信しようとする場合には、クラウドサービスプロバイダが、連邦リスク・認証管理プログラム（FedRAMP）中級ベースラインが設定したセキュリティ要求事項と同等の要求事項を満たしており、かつ、当該プロバイダが、サイバー事案報告、悪意のあるソフトウェア、記録媒体の保存・保護、フォレンジック分析に必要な追加情報と機器へのアクセス及びサイバー事案損害評価に対する本条項（c）から（g）までの要求事項を満たしていることを要請・確保

【参考】米国国防省におけるクラウドを活用した官民情報共有の例





FedRAMPは、NIST等の基準を適用しつつ、国防省等の承認を経て採用された政府統一的な認証プログラム

４．米国における産業サイバーセキュリティ　～防衛関連企業によるセキュアなクラウド利用～

➢ 米国の防衛関連企業においては、DFARS（国防調達規則）の要求に従い、FedRAMP認証のクラウドを採用

米国における主な防衛関連企業のクラウド利用状況（一例）

認証プログラム	クラウドサービス	利用防衛関連企業	備考
FedRAMP	AWS	Lockheed Martin	
		Raytheon	
		Textron	
		Booz Allen Hamilton	
	Azure	Boeing	
		L3 Technologies	
		Thales Group	Azureをベースに共同開発
	Google Cloud	Airbus	
		United Technologies	
	GC	Northrop Grumman	
	複数のクラウド	GE	

その他、General DynamicsやBAE Systemsでは自社製クラウドを利用。

４．米国における産業サイバーセキュリティ　～日本の防衛産業に対する懸念・誤解～

➢ 日本の防衛産業の情報保全態勢に関する懸念・誤解

Japan's Industrial Security Problem

日本の産業保全問題

For the good of its defense industry, Tokyo needs to get serious about protecting secrets.

By Arthur Herman
April 18, 2018 5:53 p.m. ET

PHOTO: ISTOCK/GETTY IMAGES

When President Trump and Japanese Prime Minister Shinzo Abe met this week, let us hope their agenda included Japan's weak industrial security. The inability of Japan's government and contractors to protect sensitive information undercuts both countries by making it harder to design and produce the advanced weapons systems of the future.

After decades of servicing only the Japanese military, Japan's defense industry is poised to enter the global marketplace. Many American companies would love to partner with Japanese companies like Mitsubishi Heavy Industries , Fujitsu, NEC and IHI Aerospace on joint defense projects. But Japan's lack of secure systems for handling sensitive data means those hopes are more or less on hold.

Japan also lacks a coherent system for regulating employment in its defense industry. Its current laws have failed to ensure that workers with access to sensitive information have appropriate training and security clearance.

Industrial security is the cornerstone of a modern defense industry. No government—and certainly not the U.S.—is going to share sensitive data and technology with a foreign counterpart or contractor unless it is sure the information will be safe from prying eyes. Private companies will also continue to reject Japanese partnerships, greatly limiting the capacity of Japan's defense industry in an era when few firms are capable of producing advanced systems on their own.

Cybersecurity is the key ingredient in protecting defense secrets. The U.S. discovered its importance in the mid-2000s, when Chinese hackers stole classified data from the Pentagon and private companies involved in the production of the highly advanced F-35 Joint Strike Fighter.

But while the U.S. and other nations have stepped up their security in recent years, Japan has lagged. Only 27% of Japanese companies have a designated information-security chief, compared with 70% to 80% of American and European firms. Japan's defense industry still has no "information sharing and analysis center," a type of network American and European companies use to share info about cyberattacks and hacks.

Though Japan has signed an agreement with the U.S. to mutually secure military information and has passed a law to protect state secrets from public access, it still lacks an enforceable system for regulating security clearances among government and private personnel. Instead, Japan has relied on U.S. government experts to do spot fixes while waiting for a robust system of its own to develop.

Past collaborations between the two nations show how the U.S. might help bring Japan's industrial security up to speed. After World War II, Japanese engineer Genichi Taguchi adapted a new American process of statistics-based manufacturing to fit the detail and quality craftsmanship of Japan's industrial culture. Those manufacturing practices helped Japan develop a powerful industrial sector, able to dominate the sale of cars and electronics in the competitive global marketplace.

"We imported the system," economist Naohiro Yashiro once observed, "but modified it to the Japanese style." That is what Japan must now do with industrial security. Its government should adapt best practices from the U.S. and other countries to vet personnel and protect intellectual property and classified information. Naturally, the resulting security regime will correspond to the unique character of Japanese industry.

Securing Japanese industry would not only expand bilateral defense trade between the U.S. and Japan, but would also help both countries build a more secure world by better preparing their armed forces. It's a goal both the Trump and Abe administrations ought to embrace as soon as possible.

Source: The Wall Street Journal（Apr. 18,2018）

・日本の防衛産業には、欧米企業がサイバー攻撃やハックに関する情報を共有するために利用するネットワークである「情報共有分析センター」（ISAC）も未だに設置されていない。

・*日本は機微な情報を取り扱うセキュアなシステムを欠いている。*

・*日本の現在の法律は、防衛関連企業の従業員が機微な情報にアクセスするための適切なトレーニングや確認を受けることを確保できていない。*

➡ 一部の懸念が大きな誤解につながり、拡散されかねない状況

５．我が国における産業サイバーセキュリティの取組

５．我が国における産業サイバーセキュリティ強化の検討　～全般～

○　経産省の**産業サイバーセキュリティ研究会**（平成２９年１２月設置）において、産業全体をカバーしたサイバーセキュリティ上の課題への対応を議論（政府全体の取組として関係省庁とも連携）

（経済産業大臣）

産業サイバーセキュリティ研究会

■大所高所から政策や産業界の取組の方向を議論

ＷＧ１　制度・技術・標準化

■標準モデルである「サイバー・フィジカル・セキュリティ対策フレームワーク」の策定を検討

ＷＧ２　経営・人材・国際

■サイバーセキュリティ政策全体の共通基盤となる経営・人材・国際戦略を検討

ＷＧ３　サイバーセキュリティビジネス化

■セキュリティサービス品質向上と国際プレーヤー創出に係る政策を検討

●税制、政府調達、インフラ国際展開政策などと連動して議論

中小企業政策審議会基本問題小委員会等

■中小企業の生産性向上に資するIT利活用支援策とともに検討

連携

■産業分野ごとのSWGと分野横断的なＳＷＧを設置して議論

分野横断ＳＷＧ（設置予定）

- **ビル**（エレベーター、エネルギー管理等）
- **電力**
- **防衛産業**（防衛装備庁主催）
- **自動車産業**（設置に向け検討中）
- **スマートホーム**
- **その他コネイン関係分野**

５．我が国における産業サイバーセキュリティ強化の検討　～防衛装備庁における取組～

➢　防衛装備庁における検討の枠組み・目的

○　防衛装備庁においては、平成２９年２月、我が国の防衛調達における情報セキュリティ強化の方策に関し、主に以下の事項を議論するため、主要な防衛関連企業等（２３社４団体）との間で**「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」を設置**

- 防衛関連企業との意見交換による問題点の把握
- 米国の国防調達における新標準（NIST SP 800-171）の分析
- **我が国の防衛調達における新情報セキュリティ基準の策定の検討**

➢　検討会の開催状況

○　平成３０年９月までに計７回の検討会を開催

○　経産省の産業サイバーセキュリティ研究会との連携を図るため、第６回検討会より、**「産業サイバーセキュリティ研究会WG1防衛産業SWG 」として位置付けて開催**

➢　新情報セキュリティ基準の方向性

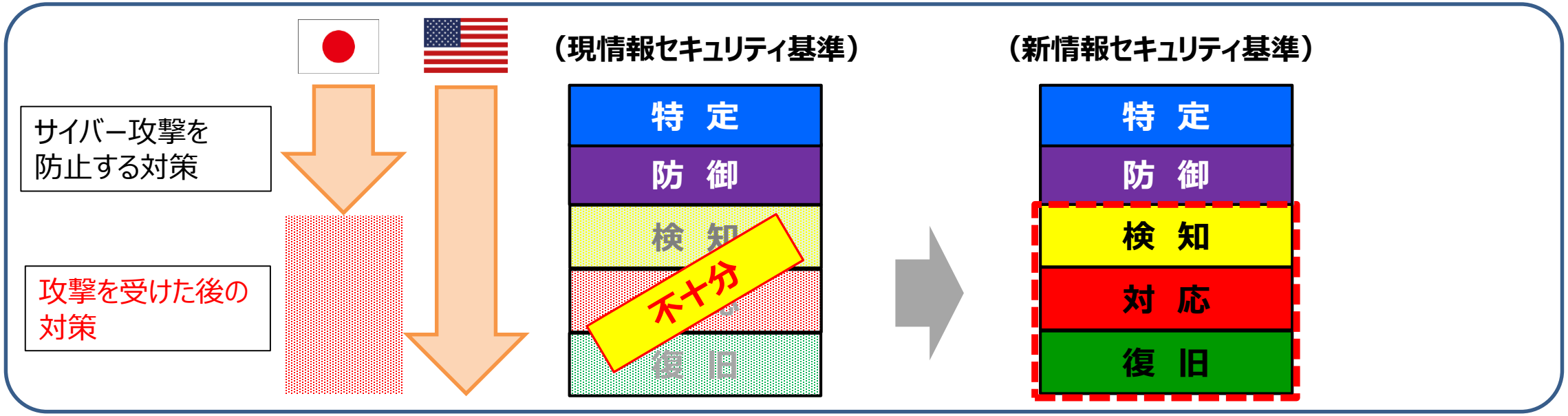
○　検討の状況を踏まえ、防衛省の「保護すべき情報」（注意・部内限り）を取り扱う**防衛関連企業に要求する情報セキュリティ基準について、NIST SP 800-171と同程度まで強化**する方向

防衛産業のサイバーセキュリティについて、

- 米国を始めとする諸外国からの信頼性を向上
- ハイレベルな産業サイバーセキュリティのモデルケース化

5．我が国における産業サイバーセキュリティ強化の検討　～防衛装備庁における取組～

➢ 米国のNIST SP 800-171と同程度への情報セキュリティ基準強化のイメージ



○　<u>コスト面の課題</u>
・我が国の防衛産業が、新基準に対し**より安価に対応するための方策**が必要

○　<u>国内クラウドサービスの利用追求に当たっての課題</u>
・現状では、米国の**NIST SP 800-171を満たすクラウドサービス事業者が我が国に存在せず**
→　今後、防衛関連企業へのクラウドサービスの提供を図る**国内事業者は、新基準を満たす必要**

○　<u>中小企業に対するケア</u>
・新基準への準拠は、プライム企業のみならず**下請けとなる中小企業も対象**となることを踏まえた対策が必要
→　**適合支援体制**構築の検討

５．我が国における産業サイバーセキュリティ強化の検討　～クラウドサービスの安全性評価～

○　本年８月、経産省及び総務省において、クラウドサービスの安全性評価方法を検討するため、情報セキュリティやデータ利活用に深い見識を有する有識者から構成される**「クラウドサービスの安全性評価に関する検討会」を設置**（防衛省・防衛装備庁もオブザーバー参加）

【参考】

未来投資戦略2018（平成３０年6月15日閣議決定）

Ⅱ．経済構造革新への基盤づくり
[１]データ駆動型社会の共通インフラの整備
１．基盤システム・技術への投資促進
（３）新たに講ずべき具体的施策

ⅱ）サイバーセキュリティの確保
　クラウドサービスの多様化・高度化に伴い、官民双方が一層安全・安心にクラウドサービスを採用し、継続的に利用していくため、情報資産の重要性に応じ、信頼性の確保の観点から、クラウドサービスの安全性評価について、諸外国の例も参考にしつつ、本年度から検討を開始する。

サイバーセキュリティ戦略（平成３０年7月27日閣議決定）

4. 目的達成のための施策
4.2. 国民が安全で安心して暮らせる社会の実現
4.2.3 政府機関等におけるセキュリティ強化・充実

(2) クラウド化の推進等による効果的なセキュリティ対策
　各府省庁において情報の特性に応じて適切な情報システムの形態を選択するとともに、政府全体としてセキュリティ施策を効率的・効果的に実施できるよう、システムの構築と運用の集約及びセキュリティ水準向上の利点を活かすことができる、政府プライベートクラウドとしての政府共通プラットフォームへの移行を含むクラウド化を推進する。クラウド化の推進に当たっては、安全性評価など、適切なセキュリティ水準が確保された信頼できるクラウドの利用を促進する方策について検討を進める。