防衛装備庁
技術シンポジウム2019

防衛装備庁における情報セキュリティ基準の改正に係る取組

令和元年11月13日

装備政策部
装備制度管理官
前野　明

目　次

1．背景

１．背景

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

1．背景　～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

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 Report Post Theft," referring to a character from the soap opera "Home and Away."

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 decade-long 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.

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.

・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。

１．背景　～産業界からの提言～

➢ 新たな防衛計画の大綱と中期防衛力整備計画の着実な実現に向けて
（平成３１年４月１６日経団連提言）（抜粋）

3.日米同盟の強化、安全保障協力の推進に向けて

（3）情報保全

技術情報の適切な管理は、日米を含む国際装備・技術協力に不可欠な基盤である。同時に、**規模の大小を問わず、防衛サプライチェーンに参加する全ての企業にとり、重要なテーマ**でもある。既に、わが国においても、**防衛省主導で米国の情報セキュリティ基準に則った対策が進行中**であり、既に一部の日米共同プログラムにおいては、米国のセキュリティ・クリアランスが適用されている。

今後の国際協力の拡大に備え、わが国においても、**米国ならびに友好国との間でも活用し得る情報保全制度**を設けるべきである。同時に、中小企業に対しては、**情報保全体制の確立に向けた各種支援を実施**すべきである。

サイバー攻撃等の脅威の増大に対応することは、

- サイバー攻撃等に起因する情報漏えい等によるレピュテーション・リスクの低減
- 企業の企業価値向上にも寄与

２．米国における産業サイバーセキュリティ

2．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**などを発出

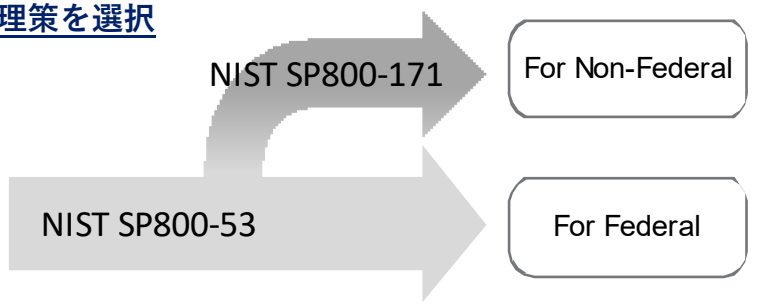
1．ＮＩＳＴ　ＳＰ８００－５３
（連邦政府情報システムにおける推奨セキュリティ管理策）

・ **連邦政府機関向けの情報システム・組織のセキュリティ標準**

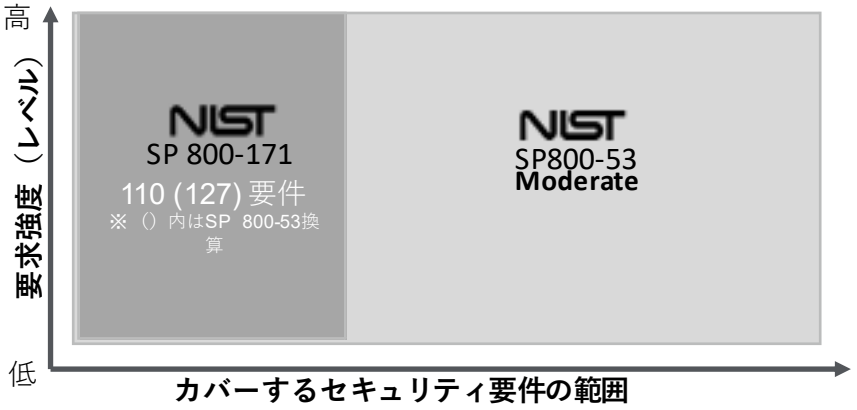
2．ＮＩＳＴ　ＳＰ８００－１７１
（非政府機関情報システムにおけるＣＵＩの保護）

・ **非政府機関で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（産業向け）**

■ **NIST SP800-53を基に、Non-Federal向けに強度はそのままに管理策を選択**



■ **個々の要求強度（レベル）はNIST SP800-53と同等**



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**

※ 米国防省は、同省との契約に基づきCUIを取り扱う防衛関連企業に対し、2017年12月末までにNIST SP 800-171への準拠を要求

２．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、それぞれ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それぞれ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。

３．我が国における産業サイバーセキュリティ強化の検討

３．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～

サイバーセキュリティの強化

➢ 一般的なサイバーセキュリティ

➢ 防衛産業のサイバーセキュリティ

○ 検討会（**「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」**）の設置
- サプライヤーとの検討会（２３社４団体）
- 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**

○ 開催状況
- 令和元年８月までに計９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」として位置付け開催**

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

3．我が国における産業サイバーセキュリティ強化の検討　～防衛調達における情報セキュリティ基準改正の検討～

防衛調達における情報セキュリティ基準改正の検討

➢ 現在、防衛省においては、契約に基づき「保護すべき情報」を取り扱う防衛関連企業に対し、国際標準であるISMS基準ベースの情報セキュリティ基準の遵守を義務付け

➢ サイバー攻撃の脅威増大や米国防調達における情報セキュリティ強化の動向を踏まえ、我が国の防衛調達における情報セキュリティ強化を検討する必要

○ 平成29年2月、**防衛関連企業等との間で官民検討会を設置**し、現在の情報セキュリティ上の課題・問題点や、**今後の情報セキュリティ強化の方向性につき、議論・検討**を実施
（令和元年8月までに計9回の検討会を開催）

○ その結果を踏まえ、**防衛調達における情報セキュリティ基準**について、**令和元年度のできるだけ早い段階**で、**米国のNIST SP 800-171と同程度まで強化する改正を行うことを検討。**

○ **NIST SP 800-171では、政府機関が準拠すべき管理策（NIST SP 800-53）から民間企業が準拠する管理策を、要求レベルは維持しつつ選択。**

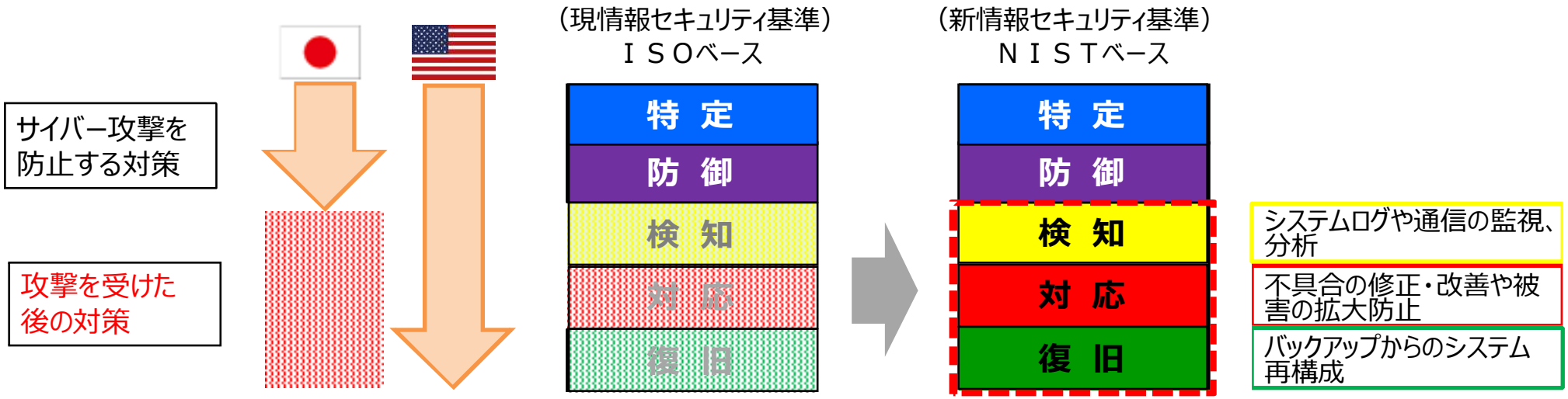
なお、施行までの間に**十分な準備期間を確保することが必要であることから、施行時期は令和3年度**を念頭に検討

中期防衛力整備計画（平成31年度～平成35年度）（平成30年12月閣議決定）（抄）
Ⅲ－２－（5） 産業基盤の強靭化
我が国の防衛産業が国際的な取引を行うために必要となる情報セキュリティに係る措置の強化（中略）を行う。

３．我が国における産業サイバーセキュリティ強化の検討　～セキュリティ基準強化のイメージ～

情報セキュリティ基準強化のイメージ

➢ 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



○ **国際標準であるＩＳＯ/ＩＥＣ 27001（ＩＳＭＳ）よりも内容が強化**

○ インシデント防止（特定、防御）だけでなく、サイバー攻撃をはじめとした情報セキュリティ上の**インシデント発生以降**（検知、対応、復旧）**も十分にカバー**している点が特徴

3．我が国における産業サイバーセキュリティ強化の検討　～新情報セキュリティ基準の概要～

情報セキュリティ基準の概要

➢ 新情報セキュリティ基準は、NIST基準を整理し、28項目から構成（現行基準は13項目）

1. 趣旨	2. 定義	3. 対象
4. 情報セキュリティ基本方針等	5. 組織のセキュリティ	6. 保護すべき情報の管理
7. 人的セキュリティ	8. 教育及び訓練	9. 物理的セキュリティ
10. システムセキュリティ準拠証明書	11. 構成設定	12. 基本防御設定
13. アクセス制御	14. 識別及び認証	15. 通信制御
16. システム監視	17. システムログ	18. 脆弱性スキャン
19. バックアップ	20. システム開発及び調達等	21. システムメンテナンス等
22. セキュリティ事象等への対応	23. セキュリティ事故等への対応	24. リスク査定
25. セキュリティ監査等	26. 是正計画	27. 防衛省による監査
28. 補則		

➢ 検知

○ システムログ、通信を常時監視するとともに、悪意のあるコードを検知するための高性能ウイルス対策ソフトウェアを導入し、週１回以上定期的にスキャンを実施

○ ファイルの開封及び実行等の都度、リアルタイムスキャンを実施

○ 取得したシステムログを週１回以上定期的及び情報セキュリティ事故等時に分析

○ 脆弱性発見のため、月１回以上及び脆弱性情報取得時に脆弱性スキャンを実施

○ 現場に所在して又はシステム上から、システムの外部業者によるメンテナンス作業を監視

➢ 対応・復旧

○ 基準違反等（情報セキュリティ事象）や保護システムの脆弱性を発見した場合、原則30日以内に修正・改善を実施

○ 30日以内の修正・改善が困難な場合、是正計画を策定し、原則１年以内に修正・改善を実施

○ 事前に詳細な対処計画を策定し、対処テストを年１回以上定期的に実施

○ 事故等への対処の教訓反映（教育、訓練、対処計画への反映）

○ 保護システムの復旧に必要なデータについて、24時間に１回以上定期的にバックアップ

（下線部分は新規）