米国発サイバーセキュリティ対策の新しい評価システムCMMC

航空宇宙＆防衛業界から始まる新しい認証制度と我が国への影響

2020.11.12

株式会社エヴァアビエーション
代表取締役　久野保之
コンサルタント　濱田信輔

目次

- Introduction
- CUI と NIST SP800-171
- 防衛省の情報セキュリティ対策
- 米国防総省の取り組み”CMMC”

Introduction

EvaAviation（エヴァアビエーション）

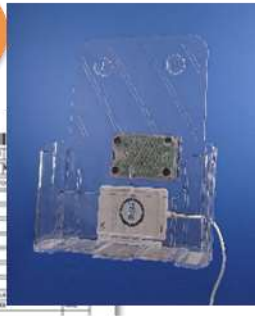
- 創業2015年、10名＋有識者ネットワーク
- 情報サービス（コンサルティング、ソフトウェア開発・サービス）

NIST
SP800-171

情報セキュリティ
コンサルティング
Supply Chain Cybersecurity

A&Dロジスティック
MROシステム
Modeling & Simulation

IoTシステム
RFID/UID
Asset Visibility



今、航空宇宙・防衛産業界で起こっていること

米国では

Press Release

FUJITSU

2019 年 9 月 26 日
富士通株式会社

NIST SP800-171（重要情報保護）基準に対応した Exostar 社クラウドサービスの利用をトータルにサポートする「Fort# Forum」を提供開始

当社は、米国連邦政府機関以外の組織および情報システムにおいて管理すべき重要情報である Controlled Unclassified Information（注 1、以下 CUI）の保護をトータルにサポートする「FUJITSU Defense and National Security Solution Fort# Forum（フォートフォーラム、以下 Fort# Forum）」を、9 月 26 日より国内で提供開始します。

「Fort# Forum」は、米国国立標準技術研究所（以下 NIST）が定めている、CUI を保護するためのサイバーセキュリティ対策基準である NIST SP800-171 に対応しており、民間企業で取り扱う CUI の保護をサプライチェーン企業も含めて支援するものです。欧米の防衛・航空宇宙産業界で豊富な導入実績を有する Exostar LLC（注 2、以下 Exostar 社）が提供する認証・情報共有基盤のクラウドサービスをベースとし、当社がこれまで培ってきた NIST SP800-171 への対応ノウハウ、高度なスキルを組み合わせて提供することで、お客様は、NIST SP800-171 に対応した CUI の保護を、自社で実施することに比べてより安全・早期・経済的に実現する事が可能となります。

当社は今後、国内での CUI のデータ保管を実現するため、NIST SP800 シリーズのサイバーセキュリティ対策基準に準拠させたクラウドサービスを国内に展開予定です。

【 背景 】

近年、米国では、連邦政府機関外の民間企業に対して、CUIを保護するためにサイバーセキュリティ対策基準であるNIST SP800-171への適合を求める動きが加速しており、米国国防総省(以下 DoD)では、DoDに防衛装備品などを納める全世界のサプライヤー（米国企業の下請けとなる日本企業を含む）に対して、NIST SP800-171の定めるセキュリティ要件の遵守を2018年から義務付けています。

また、日本でも、防衛装備庁が、防衛調達において保護が必要な情報について、NIST SP800-171と同程度の新セキュリティ要件への遵守を義務付ける方向で検討しており、今後、日本の防衛関連企業もこの新セキュリティ要件を遵守可能な情報システムの整備が求められるなど、重要情報の管理が世界中で強化されています。

富士通ホームページ（プレスリリース） https://pr.fujitsu.com/jp/news/2019/09/26-2.html

今、航空宇宙・防衛産業界で起こっていること

我が国では

令和２年２月１０日
防　　衛　　省

電機株による機微な情報の漏えいの可能性について

る不正アクセスについては、令和２年（２０２０年）１月２０日、三菱
査の結果、防衛・電力・鉄道などの社会インフラに関する機微な情報、
報や取引先に関わる重要な情報は流出していないことを確認済」と公表
その後、引き続き三菱電機株において、流出した可能性のある情報に

NEWS RELEASE

不正アクセスによる個人情報と企業機密の流出可能性について（第３報）

2020 年 2 月 12 日
三菱電機株式会社

三菱電機株式会社は、1 月 20 日に公表した不正アクセス事案（「不正アクセスによる個人情報と企業機密の流出可能性について」）について、攻撃を受けた可能性のあるすべての端末を精査する中で、流出可能性のあるファイルとして、防衛省の指定した「注意情報」があることを 2 月 7 日に発見し、同日、防衛省に報告の上、2 月 10 日に第 2 報として公表いたしました。当社の調査が完全でなく、国の防衛に関わる情報が流出した可能性があるという事態を引き起こし、深く反省しております。防衛省をはじめ、皆さまにご迷惑とご心配をおかけしていることを、深くお詫び申し上げます。

以下に 2 月 10 日に公表した第 2 報についてあらためてご報告するとともに、サイバーセキュリティーに資する情報の共有を図るべく、攻撃手法や当社での検証プロセスなどを、合わせてお知らせします。

三菱電機ホームページ（ニュースリリース）　https://www.mitsubishielectric.co.jp/news/2020/0212-b.pdf

Orchestrating a brighter world
デジタルトランスフォーメーション（DX）　ソリューション・サービス　業種・業務　製品　企業情報　サイト内検索

ホーム > News Room > 当社の社内サーバへの不正アクセスについて

当社の社内サーバへの不正アクセスについて

（経営 No.2005）

2020年1月31日
日本電気株式会社

当社の防衛事業部門で利用している社内サーバの一部が、第三者による不正アクセスを受けたことを確認し
当社および外部専門機関による調査の結果、これまで情報流出等の被害は確認されておりません。
の皆様には、多大なご迷惑とご心配をお掛けすることとなり、深くお詫び申し上げます。今回の事態を踏まえ
管理体制の強化と再発防止に取り組んでまいります。

アクセスの概要

NECホームページ（NewsRoom）
https://jpn.nec.com/press/202001/20200131_01.html

豪州防衛関連企業に対するサイバー攻撃の事例

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

4か月のサイバー攻撃で米国の武器データは盗まれた　　2017年10月12日

写真： オーストラリア国防軍の配布資料/ロイター

オーストラリア キャンベラ　ー「Alf」というニックネームのサイバー攻撃者がオーストラリアの防衛請負業者のコンピューターにアクセスし、高度な米国の兵器システムに関するデータに４か月にわたって襲撃しました。

「Alf」に、オーストラリアのF-35戦闘機100機の購入計画に関するデータ約30ギガバイトを盗まれたと、オーストラリアの諜報機関高官は述べた。

対象企業は、元請業者から数レベル下の小さな下請業者だったとクラーク氏は語った。同社では1人の従業員が情報技術を管理しており、その人物は9か月間、同じローカル管理者アカウントのパスワードを使用していたため、ハッカーが情報を簡単に盗むことができました。

盗まれた情報は秘密として分類されたものではなかったが商業的には秘匿すべき重要データであると述べました。

オーストラリア政府は今週、サイバー攻撃の数と巧妙さが増加しており、昨年は47,000件の事件が発生したと報告しています。

CANBERRA, Australia—A cyber attacker 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 the third major breach of sensitive U.S. military and intelligence data to come to light in the past week.

On Tuesday, a South Korean lawmaker said North Korean hackers had accessed a military database and stolen top-secret files, including a plan for a decapitation strike against top leaders in Pyongyang. That followed reports that hackers working for the Russian government stole details of how the U.S. penetrates foreign computer networks and defends its own. …more

from The Wall Street Journal Oct. 12,2017

米国連邦政府の情報セキュリティ基準

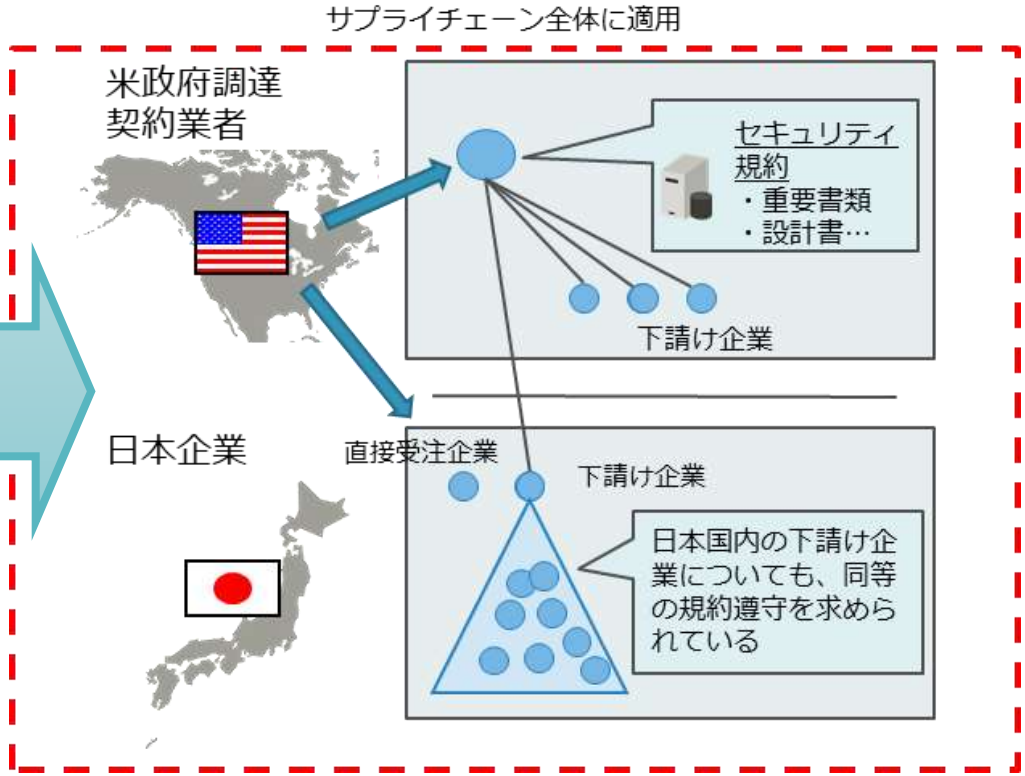
CUI と NIST SP 800-171

米国政府の要求 ～ 国防総省（DoD）

DFARS 252.204-7012

FAR／DFARS

- 情報システムに対して NIST SP 800-171を実装
- 契約時に対応状況を提出
- 下請け会社にフローダウン
- 事案発生時の報告義務



✓セキュリティ事故の大半は、サプライチェーンで発生
✓連邦政府調達の先駆けとして国防総省が2018年から施行（DFARS）
✓NIST SP 800-171では扱う人の個人認証、データ暗号化が前提

CUIとは何か

CUI（Controlled Unclassified Information）

従来Unclassified Informationに分類されていた情報でありながら、管理されるべき内容を含むもの

■ **CTI**技術情報の例

⇒研究・エンジニアリングデータ、エンジニアリング図面及び関連するリスト・仕様・規格・工程表・マニュアル・技術報告書・技術指令書・カタログ品目識別・データセット・分析研究及び関連する情報、 並びにコンピュータソフトウェアの実行コードとソースコード等

対象とする情報　～CUI

大統領令 13556
Controlled Unclassified Information
November 4, 2010.

- **CUI (*Controlled Unclassified Information*)**は、大統領令 Executive Order 13556 (2010)によって定義された
- NARAはその指示を受けて連邦政府全体に対してCUI保護の態勢を作る役割を負った
- NISTはNARAの指示のもと、CUIを保護するための基準をSP800-171として策定した

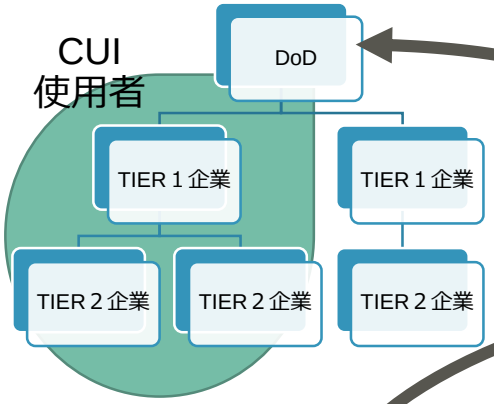
NARA → NIST → **NIST SP 800-171**
Protecting CUI in Nonfederal Systems and Organizations

171の対象は14ファミリー（カテゴリー）、コントロール（要件）は110項目

① アクセス管理
② 意識向上およびトレーニング
③ 監査および責任追跡性
④ 構成管理
⑤ 識別および認証
⑥ インシデント対応
⑦ 保守
⑧ 記録媒体の保護
⑨ 人的セキュリティ
⑩ 物理的保護
⑪ リスクアセスメント
⑫ セキュリティ評価
⑬ システム・通信の保護
⑭ システム・情報の完全性

米国防総省のDFARS 252.204-7012規則

「CDI（管理対象防衛情報）の保護とサイバーインシデント報告」という調達規則補遺により、契約相手方に対し規準遵守を求めた



関係するサプライチェーン全体へ

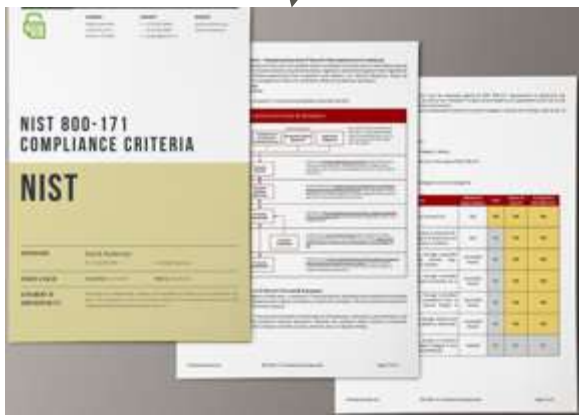
システムに対して NIST SP800-171を遵守

下請け会社にフローダウン

契約時に対応状況を提出

サイバーインシデント発生時の報告義務

SSP
(System Security Plan)



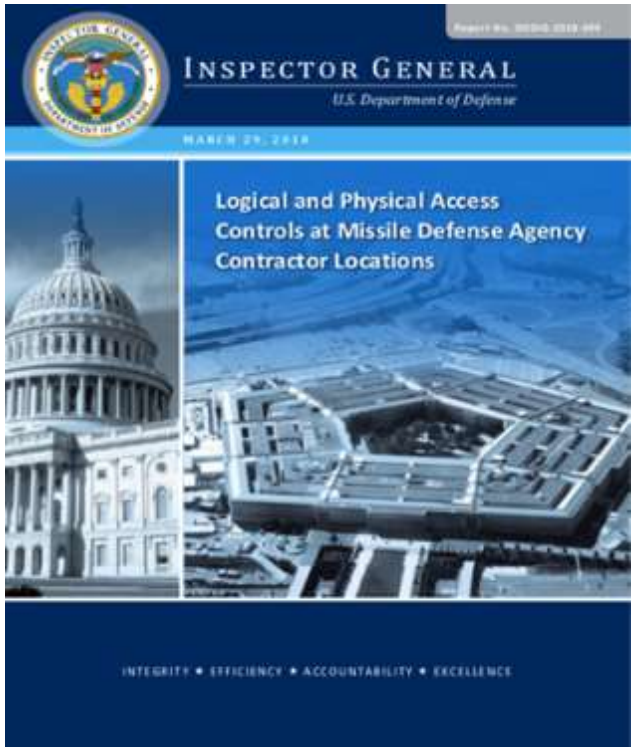
DIB CS
サイト

ECA電子証明書が必要

米国防総省監査官によるMDA事前調査レポート

MDAと契約している7社ほどを抽出して、DFARS 252.204-7012の適合を含む技術情報の保護状況を調べた結果が公表
（2018年3月29日付）

管理策定義	契約事業者						
	A	B	C	D	E	F	G
多要素認証が一貫して適用されていない		X	X	X	X	X	
システムパスワードの強度が不十分		X	X	X	X		
契約事業者は定期的なリスクアセスメントを行なっていなかった			X	X	X	X	X
ネットワークとシステムの脆弱性が一貫して軽減される方策を講じていない	X	X	X	X	X	X	X
サードパーティ事業者のネットワーク防護活動を監視していない				X			
契約事業者は、個人の携帯端末によるアクセスを許している				X			
可搬媒体が適切に保護されていない	X	X		X		X	X
操作終了またはログイン失敗時にシステムが自動的にロックされない	X	X	X		X	X	
システムアクセスとユーザーの特権が適時確認されていない	X		X	X	X	X	
システムログレポートが適切に保管、レビューされていない	X	X		X		X	



評価結果は、左表の通りで、7社中全てに合格した事業者はいない。
米国防総省はNIST SP 800-171の適用を含むCUI保護対策をさらに厳格化する方向に動いている。

NIST SP 800-171の特徴

① NIST SP 800-171は管理策ではなく「要件」

「政府の指定したCUIを如何にしたら漏らさないようにできるか、守るべきミニマムルールを要件書として示したもの」

② 情報セキュリティ3要素の内「秘匿性」にフォーカス

情報セキュリティの３要素である**C・I・A**（秘匿性（Confidentiality）・完全性（Integrity）・可用性（Availability））の内、Cの秘匿性のみにフォーカス

③ 遵守状況は「自己申告」、インシデント発覚時には「申告通りか」が問われる

NIST SP 800-171には特定の機関が認定や合否を出すきまりはない

防衛省の情報セキュリティ対策

「保護すべき情報」

防衛省「情報セキュリティ基準」

■防衛関連企業における情報セキュリティ確保について

防衛省が指定する**「保護すべき情報」**を扱う調達契約受注企業は、以下の対策を取ることを指示した。（平成１８年４月より）　（2006年）

- 情報セキュリティ管理の体系を策定
- 受注企業に同様な情報セキュリティ管理体系作成を要求
- 情報セキュリティ確保策が適切に実施されているか監査

防衛省ホームページにおける説明

＊具体的には、以下のURL（防衛省ホームページ）を参照
https://www.mod.go.jp/j/approach/defense/cyber/kigyo/index.html

防衛省（装備庁）では、現在基準の見直しを実施中

➢ 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**

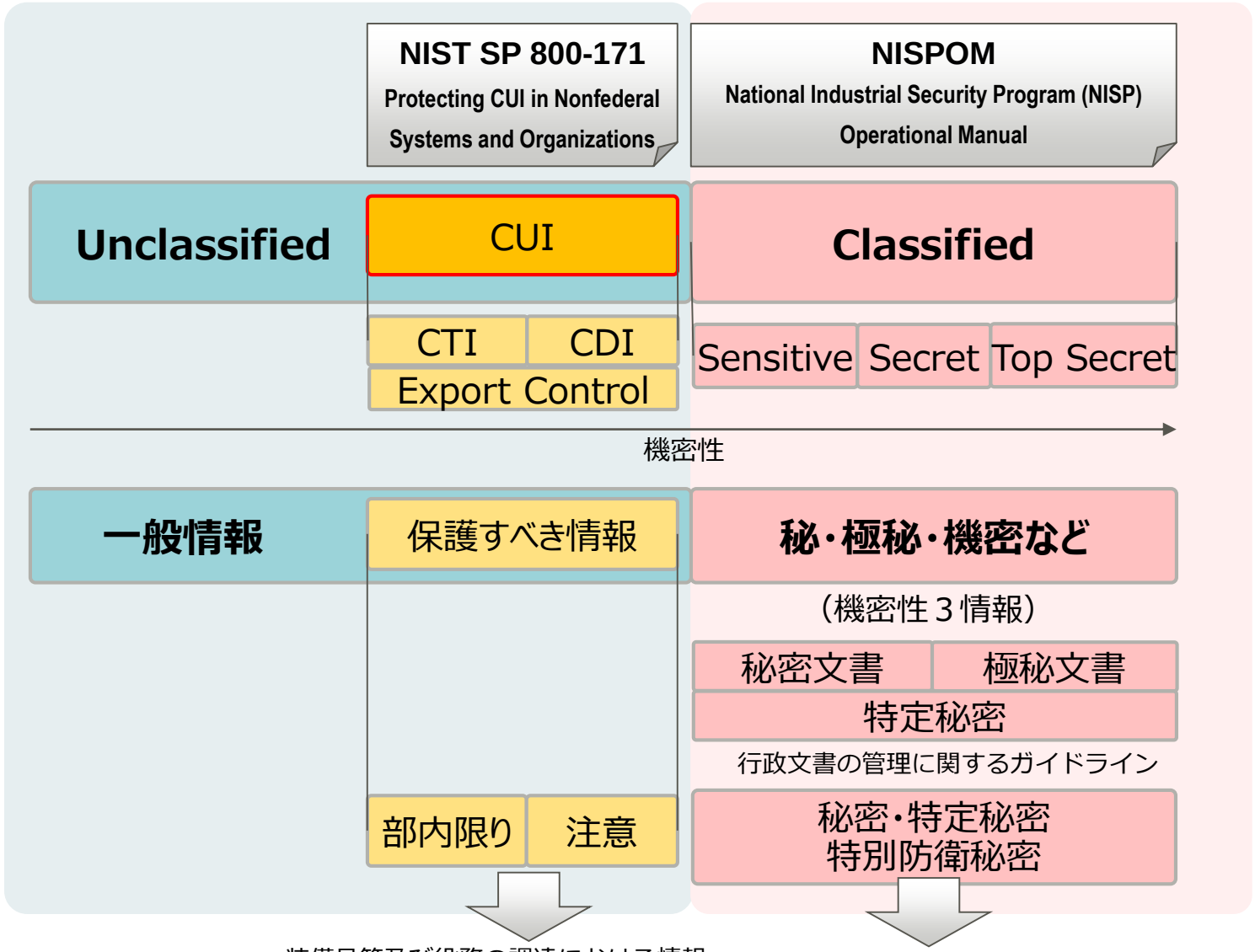
- 防衛関連企業との意見交換による問題点の把握
- 米国の国防調達における新標準（NIST SP 800-171）の分析
- **我が国の防衛調達における新情報セキュリティ基準の策定の検討**

➢ 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

https://jp.ext.hp.com/business-solution/security/report/

情報の定義（分類）


NIST SP 800-171
Protecting CUI in Nonfederal Systems and Organizations
NISPOM
National Industrial Security Program (NISP) Operational Manual
米国
Unclassified
CUI
Classified
CTI
CDI
Export Control
Sensitive
Secret
Top Secret
機密性
日本
一般情報
保護すべき情報
秘・極秘・機密など
（機密性３情報）
秘密文書
極秘文書
特定秘密
行政文書の管理に関するガイドライン
部内限り
注意
秘密・特定秘密
特別防衛秘密
情報セキュリティ管理基準
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
自衛隊法
秘密保全に関する訓令など

産業分野ごとの検討の促進：分野別のSWGの設置

- WG1で検討する『サイバー・フィジカル・セキュリティ対策フレームワーク』を、産業分野別に順次展開し、具体的適用のためのセキュリティポリシーを検討。

WG１　制度・技術・標準化

2/7 第1回会合, 3/29 第2回会合,
8/3 第3回会合, 12/25 第4回会合開催

標準モデル

Industry by Industryで検討 (分野ごとに検討するためのSWGを設置)

- ビル（エレベーター、エネルギー管理等）
  2/28 第1回会合, 4/16 第2回会合, 6/11 第3回会合,
  7/12 第4回会合,8/10 第5回会合,
  10/31 第6回会合, 1/9 第7回会合, 2/25 第8回会合開催
- 電力
  6/12 第1回会合, 9/4 第2回会合,
  11/21 第3回会合, 2/22 第4回会合開催
- 防衛産業
  3/29 第1回会合, 9/5 第2回会合開催
  (防衛装備庁 情報セキュリティ官民検討会)
- 自動車産業
  設置に向けた検討中
- スマートホーム
  3/13 第1回会合, 4/5 第2回会合, 6/13 第3回会合,
  7/18 第4回会合, 9/19 第5回会合, 10/24 第6回会合,
  12/19 第7回会合開催
  (JEITA スマートホーム部会 スマートホームサイバーセキュリティWG)
- その他コネイン関係分野

コラボレーション・プラットフォーム

（参考）防衛産業SWG（防衛装備庁 情報セキュリティ官民検討会）

● 我が国の防衛調達におけるセキュリティ強化の方策について検討

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ついて、防衛装備庁と主要な防衛関連企業（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」**を開催

＜検討の背景＞

1. **我が国におけるサイバー攻撃の増大**：高度化するサイバー攻撃により、我が国のサプライチェーンが標的となる可能性。
2. **米国の情報セキュリティ強化の動き**：米国の新標準（NIST SP800-171）を満たすことが、今後の米国をはじめとする国際共同研究・開発への参加を継続する最低条件となる可能性。

＜対応方針＞

契約企業が保護すべき情報を取り扱う際に適用される情報セキュリティ基準を、**米国の新標準と同程度まで強化した新情報セキュリティ基準を策定**する。

＜開催の状況＞

	開催日	検討テーマ
第１回	平成２９年　２月２８日	米国の防衛調達における情報セキュリティ強化の動向
		我が国の防衛調達における情報セキュリティ強化の方向
第２回	平成２９年　４月　５日	情報セキュリティ強化のためのルールのあり方
第３回	平成２９年　５月１９日	
第４回	平成２９年　６月１５日	中間的論点整理
第５回	平成２９年１１月２８日	これまでの振り返り及び現在の検討状況
第６回	平成３０年　３月２９日	新基準適合に向けた取り組み
第７回	平成３０年　９月　５日	防衛調達におけるサイバーセキュリティの強化に向けて

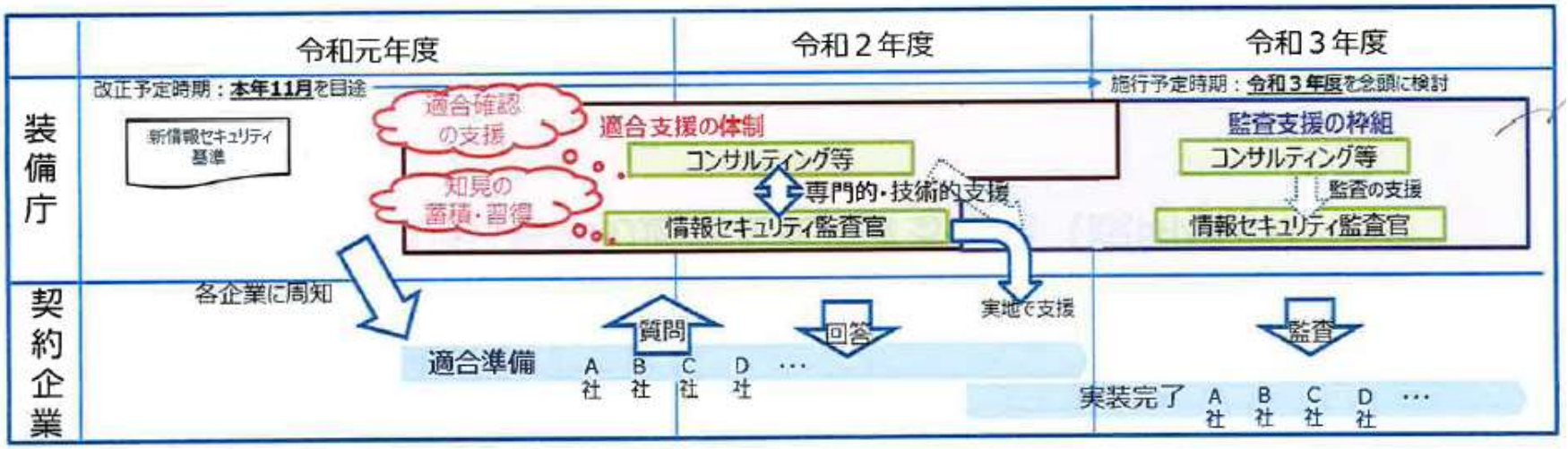
第６回検討会より、経済産業省産業サイバーセキュリティ研究会と連携を図るため**「産業サイバーセキュリティ研究会WG1防衛産業SWG」**として実施。

＜作業部会の設置＞

第７回検討会以降10/15より、情報セキュリティ官民検討会における検討を促進していくための枠組みとして、作業部会を設置
→11/22までに計４回の作業部会を実施し、情報セキュリティ基準改正の考え方に関する、**技術的・専門的観点からの認識を共有**

防衛省の検討

○ 適合支援のスケジュール



新情報セキュリティ管理基準

第３　対象

１　対象とする情報

(1)　対象とする情報は、防衛関連企業において取り扱われる保護すべき情報とする。

(2)　防衛関連企業は、契約の目的物が保護すべき情報である場合には、当該契約の履行の一環として収集、整理、作成等した一切の情報について、防衛省が当該情報を保護すべき情報には当たらないと確認するまでは、保護すべき情報として取り扱わなければならない。ただし、保護すべき情報の指定を解除する必要がある場合には、その理由を添えて防衛省に協議を求めることができる。

２　対象者

対象者は、防衛関連企業において保護すべき情報に接する全ての者（保護すべき情報に接する役員（持分会社にあっては社員を含む。以下同じ。）、管理職員、派遣社員、契約社員、パート、アルバイト等を含む。この場合において、当該者が、自らが保護すべき情報に接しているとの認識の有無は問わない。以下「取扱者」という。）とする。

第４　情報セキュリティ基本方針等

１　情報セキュリティ基本方針等の作成及び変更

(1)　防衛関連企業は、本基準の内容に沿った情報セキュリティ基本方針等を、経営者等の承認を得て作成しなければならない。

(2)　防衛関連企業は、情報セキュリティ基本方針等を適切、有効及び妥当なものとす

米国防総省の取り組み

CMMC

背景

知的財産と機密情報の盗難は、
私たちの国の防衛態勢と経済を蝕みます。

それらによる昨年の損失費用は推定で6,000億ドルで、
アメリカ人1人あたりの平均費用は4,000ドルです。

(CMMC ABサイトより引用)

NIST800-171がなぜ機能しなかったのか

過大な要求事項と自己申告制が各企業に都合の良い解釈・判断を許していた

米国防総省監査官によるMDA事前調査レポート
MDA*と契約している7社ほどを抽出して、DFARS 252.204-7012の適合を含む技術情報の保護状況を調べた結果、**全てに合格した事業者はいなかった。**（2018年3月29日付）

*MDA:Missile Defense Agencyアメリカミサイル防衛局

下請け会社にフローダウン → **Tier1と同等の管理は下請け会社には無理**

契約時に対応状況を提出 → **自己申告のため、管理レベルは各自の判断に委ねれていた**

AIAの取り組みを参考にした新たな仕組みの創出

受審側にとって受け入れやすい仕組み

米国航空宇宙産業協会(AIA)/Exostar社によるNAS9933の取り組み

NAS9933は、業界の認証・サイバーセキュリティ対策をリードするExostar社のサービス（PIM：Partner Information Manager）基準を出版したもの。

・管理策評価基準は、22ファミリーにまたがる194の管理策に対して**Yes/Noのアンケート**回答する形式で、**具体的で回答しやすく工夫**されている
・**管理策は５段階のレベル分け**がされていて、自社の対応レベルが判定できる仕組み

米国防総省
NIST SP800-171要件を展開して
５レベル評価を加えた新しい認証制度の仕組みとして
CMMC（Cybersecurity Maturity Model Certification）
適用することを宣言

CMMCの概要

CMMCとは
FCIとCUIを保護する防衛産業基盤企業の
セキュリティ対応能力を測定するための
米国防総省の認証プロセス

防衛産業基盤企業のサプライチェーンにおける、
FCI（Federal Contract Information：連邦契約情報）と
CUI（Controlled Unclassified Information：管理対象非機密情報）の
保護を目的に*OUSD（A&S）がCMMCを開発

*OUSD（A&S）【調達と持続性のための国防長官室】
(Office of the Under Secretary of Defense for Acquisition and Sustainment)

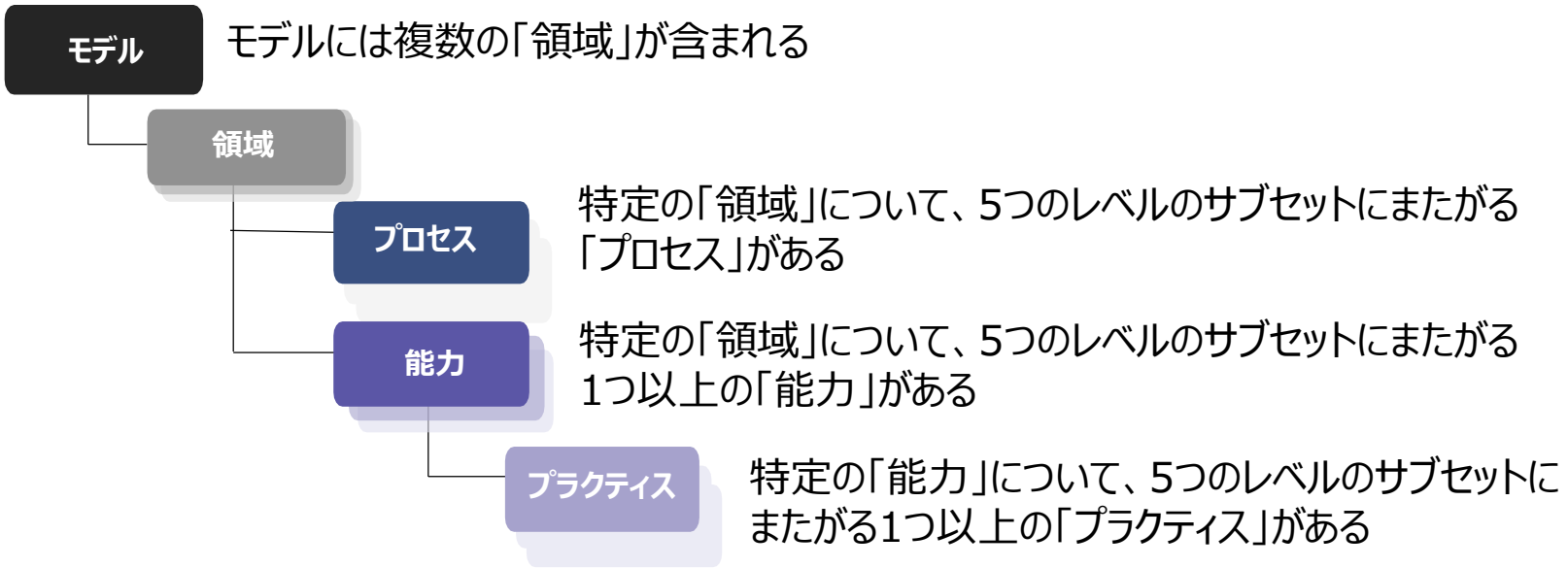
CMMCの開発に当たり、米国防総省のステークホルダーと産業界及び以下の協力を得た。
UARC（University Affiliated Research Centers：大学関連研究センター）
FFRDC(Federally Funded Research and Development Centers:連邦資金研究開発センター)
ジョンズ・ホプキンズ大学 応用物理学研究所（APL）
カーネギーメロン大学 ソフトウェア工学研究所（SEI）

CMMCの特徴　成熟度モデルの採用

CMMCは

- **成熟度モデル**の構成をとっている
- 定義された領域に対し、**実施すべきプロセス、プラクティス**が**成熟度レベル（レベル1～5）にマップ**されている

以下の複数のソースからプラクティスを組み込んでいる。
NIST SP 800-171 rev.1 / NIST SP 800-172 (旧171B)
英国のCyber Essentials / オーストラリアのEssential Eight等、



CMMCの成熟度モデルの構成

防衛に関わる全企業への必須要件

米国防総省の案件を受託する
全サプライチェーン各社は、
レベル１のCMMC認証を取得する
（CUIの取扱いの有無に関わらず）

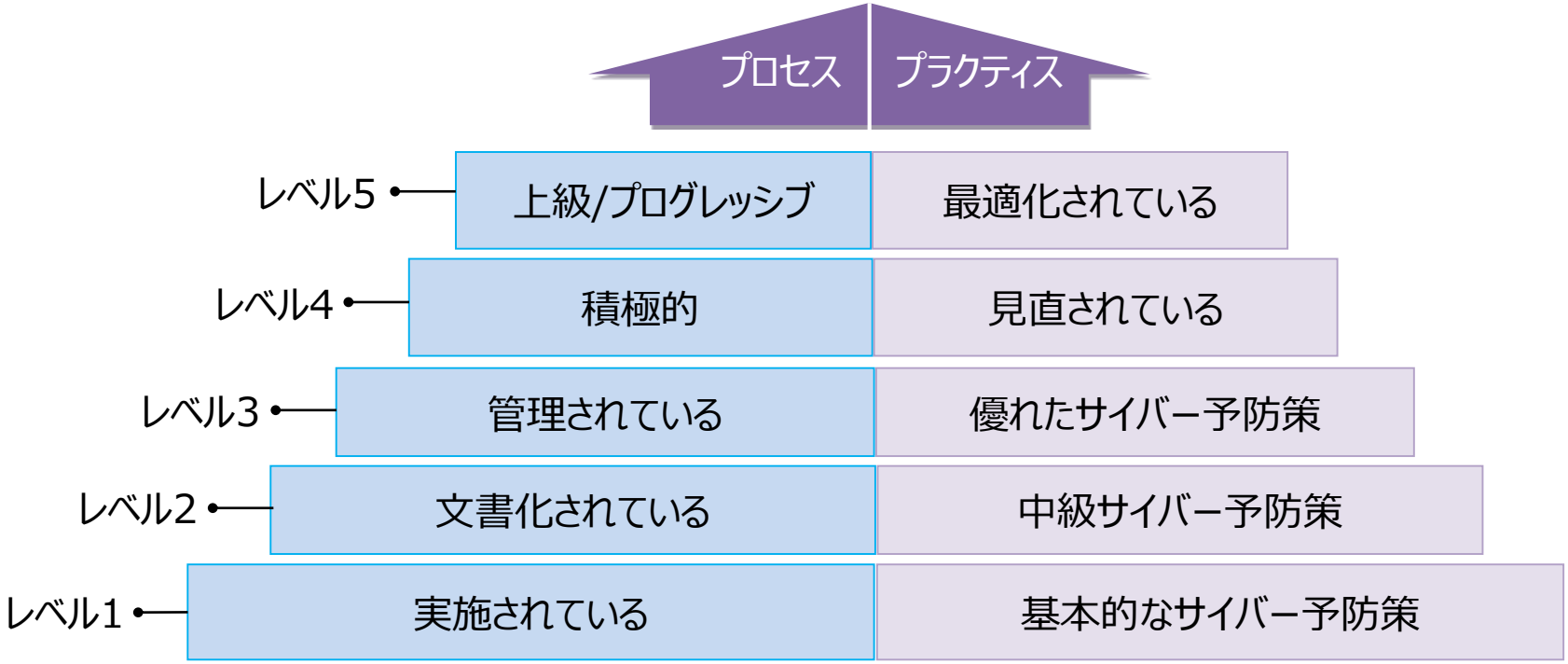
CMMCは、サイバーセキュリティ要件の
実装状況を検証するための認証の枠組みも含んでいる。

多層サプライチェーンの**下請け事業者へのフローダウンを考慮**し、
防衛産業基盤企業が**リスクに見合ったレベル**で
FCIおよびCUIを適切に保護できることについて、
適切に認証されるように設計されている。

CMMCレベル

・CMMCモデルでは**5つの成熟度レベル**が定義されている。

・特定のCMMCレベルを満たすには、**該当レベル以下の全てのレベルの「プラクティス」と「プロセス」を満たす**必要がある。



CMMCモデルの5つの成熟度レベル

CMMCのプラクティス

・レベル１,2, 3　NIST SP800-171の要件(110項目)のほとんどを含む

・レベル４, 5　　NIST SP800-172　（SP800-171B(Draft)から改称）
さらに高度な対応を求められる主にTEIR-1企業に要求される

CMMC レベル	CMMCレベルで導入されたプラクティスの数	出典			
		48 CFR 52.204-21	NIST SP800-171r1	NIST SP800-172	その他
1	17	15*	17*	–	–
2	55	–	48	–	7
3	58	–	45	–	13
4	26	–	–	11	15
5	15	–	–	4	11
Total	**171**	**15**	**110**	**15**	**46**

*注: 48 CFR 52.204-21 からの 15 の保護要件は、NIST SP 800-171 の 17 のセキュリティ要件に準じている。

CMMCレベル毎のプラクティスの出典

CMMCの認定組織 CMMC AB

Cybersecurity Maturity Model Certification Accreditation Body

メリーランド州で非営利法人として法人化された団体(2020/1)

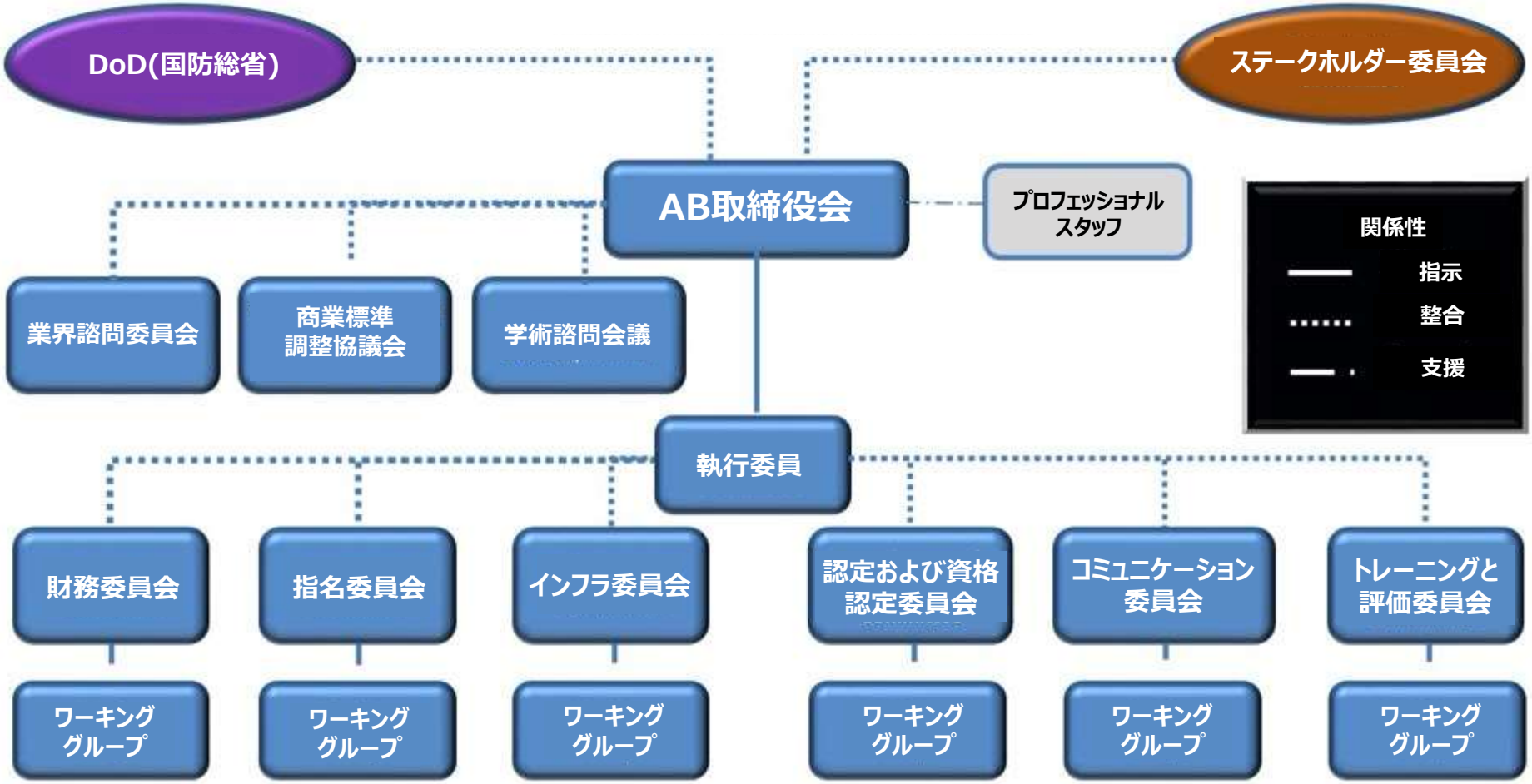
CMMC-ABは以下の活動を行うための組織(制度等)を整備している

1. 国防総省サプライチェーンにおける35万社以上の企業の評価
2. 評価者およびC3PAO（認定された第三者評価機関）向けのトレーニング
3. 当目的を達成するための基盤
4. CMMCプロセスに参加する組織および審査員の公認
5. 個々の請負業者または監査で発生する抗議または問題の裁定
6. サプライチェーンのサイバーセキュリティ防御態勢の定義および改善を未来思考で改革

CMMC-ABはサイバーセキュリティは国防だけにとどまらず、**他の産業への浸透**や**大学への教育**としての浸透を通して、アメリカ合衆国の**サイバー基盤の磐石化**することを考えている。(CMMC-ABのWebinarより)

CMMC認定機関の組織構造

会長　：タイ･シーバー氏(制度設計工程の責任者) ⇨ カールトン･D･ジョンソン氏(実行工程責任者)
財務　：ヤンゴン･チャン氏
その他　8名の執行役員が組織の遂行に取り組んでいる。



CMMC ABの動向

CMMC AB或いはサイバーセキュリティ関連企業から得られた情報は以下のとおり

1. **CMMCレベルの要件は、契約ごとにRFIおよびRFPに含まれる。**
   すべての契約は現行のDoDガイダンスに従い、最初からCMMC要件の対象となるわけではない。

2. **CMMC認証は契約に結びついているのではなく、契約(入札)する組織に結びついている。**

3. **DoDは2020年夏までにRFIにCMMCの要件を含める予定で、年末までにはRFPに含めると言っている。**
   2020年は数社を予定しているが、本件についてはまだ公式に開始したとの情報は無い

4. **2026年までには米国内の国防総省と取引がある企業35万の全社が、最低でもレベル1を取得することをめざす**
   例えば元請負業者にレベル4が要求される場合でも、末端企業においてはCUIの露出度などの状況に基づいて、異なる認証レベルが求められる。

5. **米国外におけるC3PAOについても、CMMC ABに認定の責任がある。**

CMMCの契約プロセス

RFPがリリースされる – 元請け業者に対するCMMC要件を含む

契約は、RFPで要求されるCMMCレベルを有する入札者が対象

下請け企業のCMMC要件について、発注側と元請け業者間で確認

元請業者は要求されるCMMCレベルを有する事業者に下請けを依頼

二次請け業者以降、要求されるCMMCレベルを保有する請負い企業と契約

契約が履行される

CMMC ABの活動状況 2020/10現在

1. CMMCの開発状況

2020/1/30 1.0版として発表。**2020/3/18 1.02版が最新**

2. CMMC AB

1) 少数の有識者によって基礎を作成し、次のフェーズへ

従来上記のワークンググループで活動していたが、初期の役割(制度設計)を終え、**実施におけるワーキンググループを再編中**である。

2) 暫定審査員育成

CMMC-ABから12名、実績のある審査機関から30名、その他一定以上の実績を持った審査員(抽選)30名の**72名の暫定審査員**により、審査に関する内容についてレビューを実施中。

3) 認定機関/認定者の公開

CMMC-ABは順次、公式に認定された審査機関、審査員、インストラクター、パートナー出版社、トレーニング機関等をABのサイトに公表していくことを表明。
現在、**公認パートナー出版社(CMMCカリキュラムの開発)として11社が登録済。**

3. DFARS CMMC ルール公開

2020年**11月リリース予定**(Case No. 2019-DO41)

サプライチェーン全体を考える

2020/6/12 経済産業省は大企業から中小企業までが含まれた**サプライチェーン上の弱点を狙って、攻撃対象への侵入を図るサイバー攻撃が顕在化・高度化している**ことを踏まえ、「昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取組の方向性」を公表

企業が取るべきアクションとして、

①サプライチェーンを共有する企業間における高密度な情報共有

②機微技術情報の流出懸念がある場合の報告

③多数の関係者に影響するおそれがある場合の公表

2020/11/1

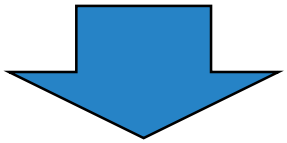
サプライチェーン・サイバーセキュリティ・コンソーシアム(SC3)設立

目的：**サプライチェーン全体でのサイバーセキュリティ対策の推進**を行う

元請け企業の責任（ サプライチェーン全体マネジメント ）

・プロジェクト単位に**サプライチェーン全体の情報セキュリティ管理体制を一元化したポリシーを策定する必要**がある

・プロジェクトの契約上位にある企業(元請け企業等)は、**自らポリシーマネジメントを行い、サプライチェーンにやり方・具体的対策などを示す必要**がある



- **審査対象が当該企業だけでは済まなくなる?**
  - ⇨ 元請け企業はサプライチェーン全体まで責任を負う
    - 従来 ：本来なら全体を管理できれば良いと思っている
    - 今後 ：何かあった場合は元請け企業にも責任を負う
- **中小企業の末端までサイバーセキュリティに関するモラル、知識の浸透は必須**
  - ⇨ e-learningによる情報モラル教育が、セキュリティレベルの底上げに繋がる

日本における課題とEva社の対応

1) CMMC-ABの海外に対するアナウンス

海外C3PAO(公認第三者審査機関)については以下のように記載されているのみ。

① C3PAOが拠点を置く国の国民である

② その国に拠点を置く請負業者の評価のみを許可される

Eva社としてCMMC-ABに対して、日本の状況について情報を提供済

2) 日本国内の状況

防衛に関わる中小企業にもCMMCというキーワードは流れているが、**正しい情報をつかみ取る体制もなく、余計な業務が増えるのでは**ないかと心配している。(名古屋商工会議所より)

⇒ Eva社としてはCMMCに関する正しい知識を習得できるよう**講演会、及び簡易チェックツールを提供**している。IPA**サイバーセキュリティお助け隊事業**にも参画中(航空・防衛分野)

防衛省の新情報セキュリティ基準は、NIST SP800-171を参考にするとのことだが、今後それを**末端企業まで一律に強いる**ことになると、**米国と同じ状況に陥る可能性**がある。

3) CMMIについて

CMMIは成熟度モデルとして知られており、CMMCはその仕組みを採用したが、本来の目的は**米国防総省のDFARS 252.204-7012に則ったセキュリティ対策が行われて**いるかが重要。成熟度アセスメントが目的とならない審査がポイントになると考える。

JASAの会員の皆様へ

コロナによって、私たちの生活は一変しました。

従来この分野を軽視していた企業においても、サイバーセキュリティの重要性を再認識しています。

元請け業者がサプライチェーン全体の責任を持たなければならないとすると、中小企業におけるサイバーセキュリティに対する意識の底上げ及び全体を簡易に管理できる仕組みが必要になってきます。

皆様におかれましては、これを新たなビジネスチャンスであると捉え、新たな環境下においても、日本のサイバー環境の安心安全のために動き始めてはどうかと考えております。

Eva社は、今後も航空・防衛分野を中心に、また中小企業に対する活動を推進していきます。
皆様と一緒に活動できることを祈っております。
ご静聴ありがとうございました。