資料４

防衛産業保全について

令和５年４月

防衛装備庁

１．防衛産業保全を取り巻く環境

我が国の防衛産業保全

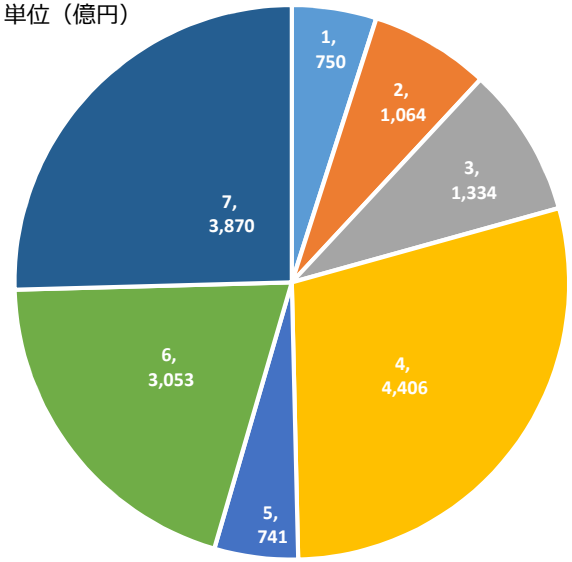
■ **約３．１兆円の防衛生産等を担う防衛産業**は、我が国の防衛力そのもの

■ 防衛装備品の製造等において、**防衛関連企業約１７０社が防衛装備庁との契約により保全措置を実施**

警戒管制レーダ（Ｊ／ＦＰＳ５）
（三菱電機）

宇宙状況監視システム
（富士通）

中距離地対空誘導弾
（三菱重工業）



（グラフ出典）中央調達実績　（令和３年度、総額は約１．５兆円、輸入・ＦＭＳ除く）
※各装備品の額は、当該装備品関連課室（調達事業部）の契約額から作成
（陸上装備＝需品調達官付機械車両室・武器調達官（弾火薬室を除く）、需品＝需品調達官（機械車両室を除く）、艦船＝艦船調達官（誘導武器室を除く）、航空機＝航空機調達官、弾火薬＝武器調達官付弾火薬室、誘導武器＝艦船調達官付誘導武器室、通信電子・指揮統制システム＝電子音響調達官

国際共同開発

SM-3 Block ⅡA
（三菱重工業）

GCAP
（次期戦闘機のイメージ図）

機動戦闘車（ＭＣＶ）
（三菱重工業）

潜水艦
（川崎重工業、三菱重工業）

Ｐ－１哨戒機
（川崎重工業）

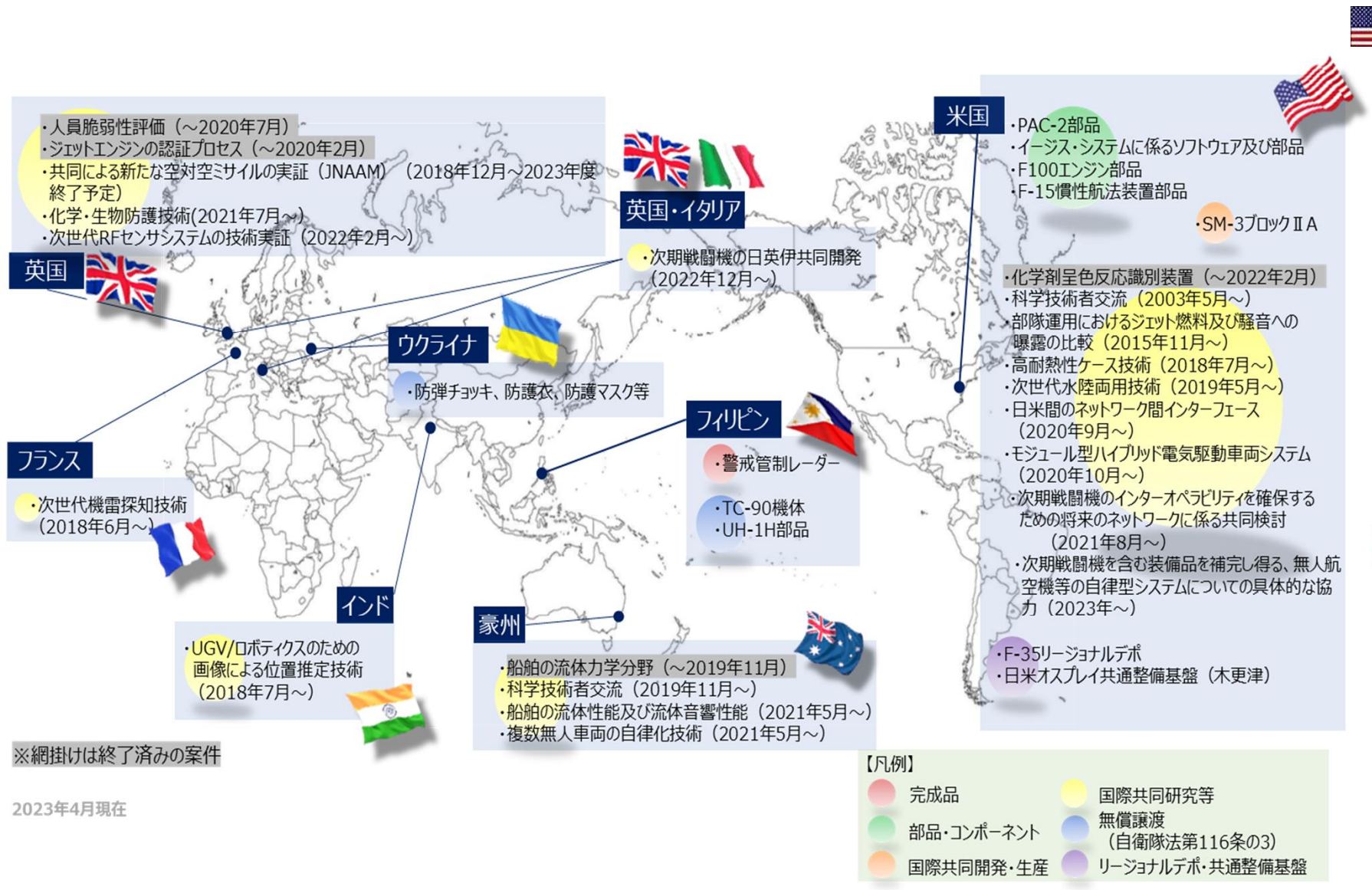
FMS調達・維持整備

F-35A 戦闘機
（三菱重工業等）

V-22 オスプレイ
（SUBARU）

諸外国との防衛装備協力の進展

➢ **諸外国との防衛装備・技術協力が拡大・深化する中、防衛産業保全における諸外国との実質的同等が前提**



※網掛けは終了済みの案件

2023年4月現在

SM－３ブロックⅡA

防護範囲を拡大し、より高性能化・多様化する将来の弾道ミサイル脅威に対処するため、ＳＭ－３ブロックＩＡの後継となる能力向上型迎撃ミサイルの日米共同開発を実施(平成18年度から約12年間を経て、日本側の開発作業が完了)（共同生産・配備段階への移行が決定済み(平成28年)）

グローバル戦闘航空プログラム(GCAP)

2035年の初号機配備に向け、日本、英国、伊国の技術を結集し、開発コストやリスクを分担しつつ、将来の航空優勢を担保する優れた戦闘機を日英伊で共同開発

日米安全保障協議委員会（２＋２）共同発表（抜粋）

Joint Statement of the Security Consultative Committee (“2+2”)

Secretary of State Blinken, Secretary of Defense Austin, Minister for Foreign Affairs Hayashi, and Minister of Defense Hamada (referred to collectively as “the Ministers”) convened the U.S.-Japan Security Consultative Committee (SCC) in Washington, D.C., on January 11, 2023.

(Omit)

The Ministers emphasized the foundational importance of cybersecurity and information security for the Alliance. They welcomed the establishment of JSDF Cyber Defense Command in March 2022, and concurred to intensify collaboration to counter increasingly sophisticated and persistent cyber threats. The United States welcomed Japan’s initiatives to bolster its national cybersecurity posture such as the creation of a new organization to coordinate whole-of-government cybersecurity policies, and the introduction of a risk management framework, which would provide a foundation for a wider range of U.S.-Japan cooperation. The Ministers welcomed progress in strengthening industrial cybersecurity, including Japan’s efforts to establish the Standards on Cybersecurity Measures for Defense Industry. Lastly, the Ministers highlighted important progress made so far under the bilateral information security consultations.

ブリンケン国務長官、オースティン国防長官、林外務大臣及び浜田防衛大臣（以下、併せて「閣僚」という。）は、２０２３年１月１１日、ワシントンDC において日米安全保障協議委員会（ＳＣＣ）を開催した。

（中略）

閣僚は、**同盟にとっての、サイバーセキュリティ及び情報保全の基盤的な重要性を強調**した。閣僚は、２０２２年３月の自衛隊サイバー防衛隊の新編を歓迎し、更に高度化・常続化するサイバー脅威に対抗するため、協力を強化することで一致した。米国は、より広範な日米協力の基盤を提供することとなる、政府全体のサイバーセキュリティ政策を調整する新たな組織の設置及びリスク管理の枠組みの導入など、国家のサイバーセキュリティ態勢を強化する日本のイニシアティブを歓迎した。閣僚は、**日本の防衛産業サイバーセキュリティ基準の策定に係る取組を含む、産業サイバーセキュリティ強化の進展を歓迎**した。そして、閣僚は、**情報保全に関する日米協議の下でのこれまでの重要な進展を強調**した。

サイバーを含む情報保全の強化は、緊密な日米同盟協力の基盤

２．防衛省における制度

秘密情報の保護に関する法的枠組み

【秘密等区分】

区分	(一般的な英語)
特定秘密（機密）／特別防衛秘密（機密）	TOP SECRET
特定秘密／特別防衛秘密（極秘）	SECRET
秘／特別防衛秘密（秘）	CONFIDENTIAL
注意	RESTRICTED※/ Controlled Unclassified Information

秘密情報（Classified Information）
取り扱うためには資格
「セキュリティ・クリアランス」
が必要

秘密情報ではないが機微な情報

※GSOIA等においては、対応する秘密区分はなく原則として「秘」として扱うが、相手国から特段の通知がある場合「注意」として扱う。

【法的根拠】

- 特定秘密の保護に関する法律
  - 特定秘密の指定及びその解除並びに適性評価の実施に関し統一的な運用を図るための基準 -
- 日米相互防衛援助協定等に伴う秘密保護法（MDA秘密保護法）
- 自衛隊法

【情報保護協定の既締結国等】 → **相互の国等の秘密保全制度が実質的同等として秘密を共有する協定**

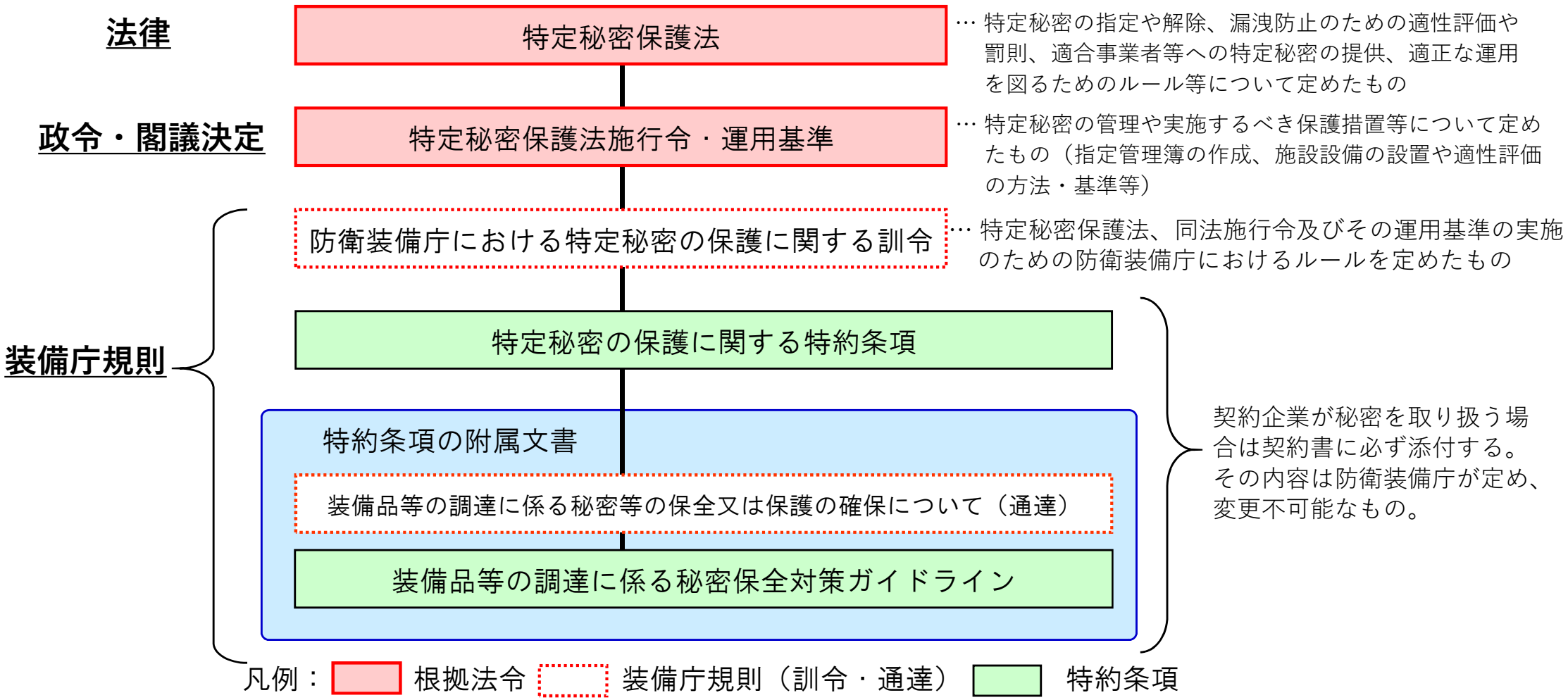
国名	米	NATO	仏	豪	英	印	伊	韓	独
保護対象	秘密軍事情報に限定	秘密情報全般	秘密情報全般	秘密情報全般	秘密情報全般	秘密軍事情報に限定	秘密情報全般	秘密軍事情報に限定	秘密情報全般
署名・締結日	H19.8.10	H22.6.25	H23.10.24	H24.5.17	H25.7.4	H27.12.12	H28.3.19	H28.11.23	R3.3.22

防衛省の保護対象情報

秘密区分	概　　要	指定根拠	漏えい時の罰則
特定秘密	防衛省の所掌事務に係る自衛隊の運用、電波情報、画像情報、武器等の仕様、暗号等に関する情報であって、公になっていないもののうち、その漏えいが我が国の安全保障に著しい支障を与えるおそれがあるため、特に秘匿することが必要であると行政機関の長が指定したもの。	特定秘密の保護に関する法律（平成25年法律第108号）	隊員・事業者は、10年以下の拘禁刑・罰金
特別防衛秘密	日米相互援助協定等に伴う秘密保護法に掲げる事項（日米相互防衛援助協定等に基づき米国政府から供与された装備品等の構造又は性能等）及びこれらの事項に係る文書、図画、又は物件で、公になっていないもの。	日米相互防衛援助協定等に伴う秘密保護法（昭和29年法律第166号）	隊員・事業者は、10年以下の拘禁刑・罰金
秘　密	防衛省の所掌する事務に関する知識及びそれらの知識に係る文書、図画又は物件のうち、国の安全又は利益に関わる事項であって、関係職員以外に知らせてはならないもの。	秘密保全に関する訓令（平成19年防衛省訓令第36号）	隊員は、自衛隊法（昭和29年法律第165号）により1年以下の拘禁刑・罰金
保護すべき情報 （部内限り又は注意）	装備品等及び役務の調達に関する情報のうち、部内限り・注意の情報等。 ●部内限り 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もの。 ●注意 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もの。	取扱い上の注意を要する文書等及び注意電子計算機情報の取扱いについて（防防調第4608号。19.4.27）	隊員は、自衛隊法の罰則の適用を受ける場合もある

秘密保全法令・組織 - 防衛装備庁の産業保全に関する法令 -

➢ 防衛産業に対して、法律、政令、装備庁規則、契約企業との秘密保全に係る特約条項の体系を整備し、必要な保全措置を実施



防衛産業保全制度（契約企業における秘密保全）

■ 防衛省では、**特定秘密保護法、MDA秘密保護法及び関連の省内規則**により**産業保全制度を確立**。

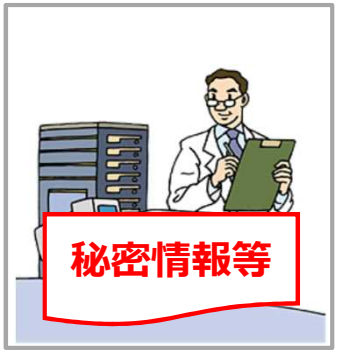
■ 装備品等の調達に当たり、**秘密情報等に指定された物件の製造・修理等を企業に委託する場合、防衛省との契約に基づき、秘密情報等を交付**している。

【契約に基づき企業に「秘密等」を提供するときのイメージ】

企　業

特約条項に基づき、
○**保全規則**の作成
○**保全教育**の実施
○**保全施設**の設定
○官の定期的な**保全検査**の受入れ
○システム上での取扱措置

等を講じることにより、官から提供される秘密情報等を保護する。



契　約

・秘密の保全に関する特約条項
・特定秘密の保護に関する特約条項
・特別防衛秘密の保護に関する特約条項
・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

秘密情報等

防衛省

企業の従業者が、秘密情報を取り扱う際には、セキュリティ・クリアランスの取得が必要

契約企業における秘密保全

【物的保全】 契約企業の保全施設等の基準

○ 外周には有刺鉄線等付のフェンスを設置
○ 施設の外壁は、鉄筋コンクリート等で建造
○ 出入口は原則１箇所のみ
○ 扉は鋼鉄製で三段式文字盤かぎ及び差込式かぎ等による二重施錠方式
○ 窓は無窓
○ 警報装置の設置
○ 開口部には金網又は鉄格子等を設置
○ 三段式文字盤鍵とさし込み式鍵による二重施錠方式の金庫等に保管

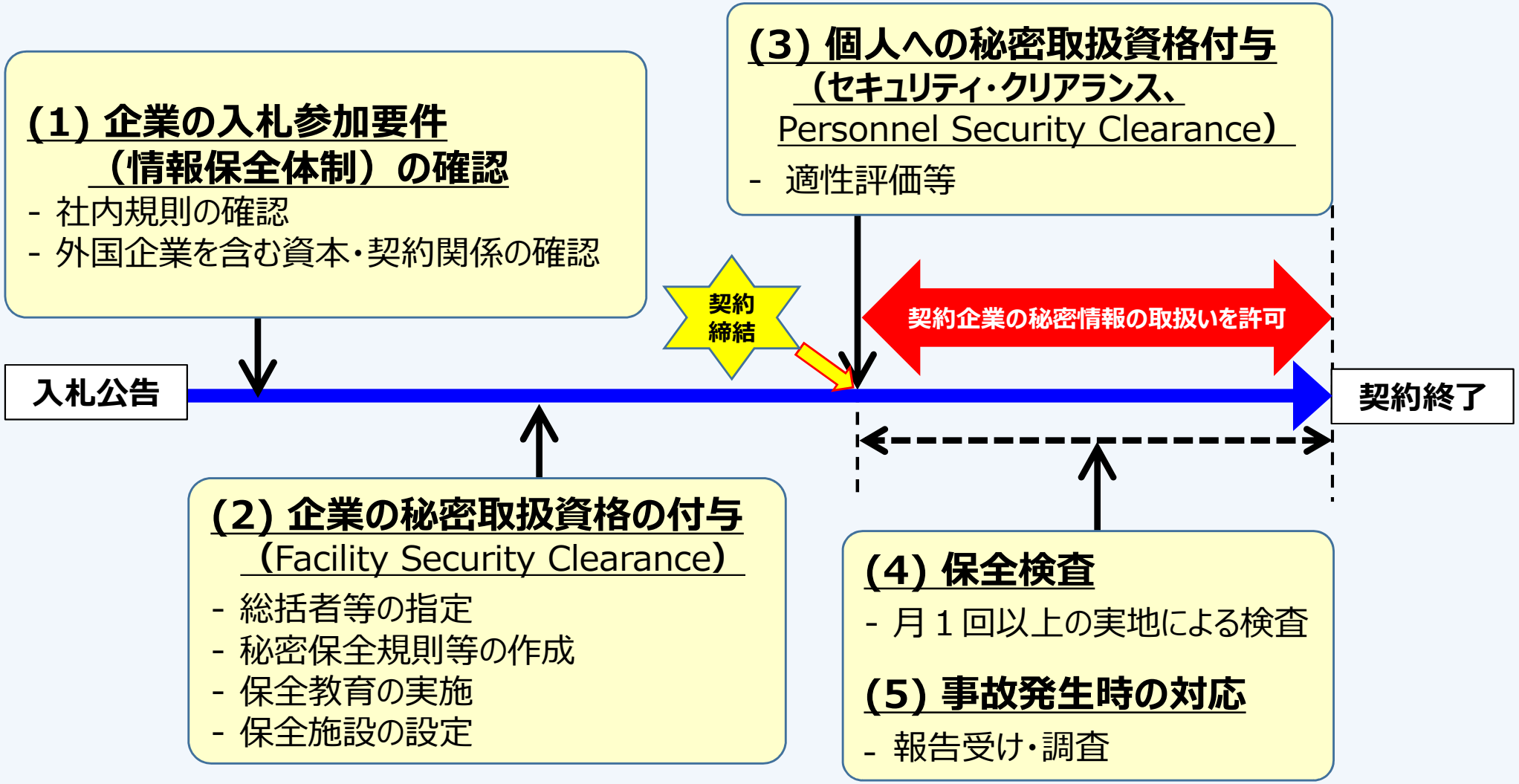
○ スタンドアローンのパソコン又は秘密保全施設内のみで有線接続されたシステム
○ パソコンはセキュリティワイヤー等により固定、又はロッカー等に保管
○ 週に１回以上のウィルスチェック等の実施
○ 業務用不要なソフトウェアのインストール禁止
○ パソコン利用者のアクセス権を厳格に設定・管理
○ パソコン利用者にＩＤを付与及びパスワードを設定し、パスワードは定期的に変更
○ パソコン利用者の使用履歴を記録

【人的保全】 秘密等を取り扱う企業従業員の確認

○ 経営者等は、防衛省の秘密等に係る情報を取り扱わせる者の指定の範囲を必要最小限とするとともに、ふさわしいと認める者を充てなければならない。

○ 特定秘密における適性評価の対象となる者（評価対象者）については、提出された質問票や上司との面接等により、犯罪及び懲戒の経歴や薬物の濫用及び影響等について調査等を実施

防衛省による契約企業に係る保全措置のプロセス（秘密以上）



防衛産業保全制度（セキュリティ・クリアランス）

特定秘密

特定秘密の取扱いの制限

特定秘密保護法に基づき、特定秘密の取扱いができる者は、**適性評価**により**特定秘密の取扱いの業務を行った場合にこれを漏らすおそれがないと認められた**行政機関の職員若しくは**事業者の従業者に限る**。

実施者

行政機関の長
（防衛大臣、防衛装備庁長官）

評価対象者

特定秘密の取扱いの業務を行うことが見込まれる行政機関の職員若しくは**事業者の従業者**

調査事項

テロ諜報活動	犯罪検挙	懲戒処分	情報非違行為	薬物濫用	精神疾患	飲酒節度	信用状態
							

秘密保全法令・組織 - 防衛産業保全に関する組織 -

■ 産業保全政策・クリアランス審査等を行う組織

防衛装備庁（装備保全管理官）は、契約企業の保全措置を確保するため、産業保全に関する政策、規則の制定及び、関連する行政事務を行っている。

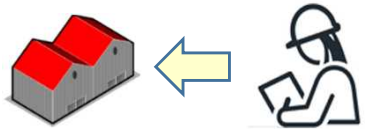
加えて、防衛装備庁は、個別の契約企業の保全に関しても、クリアランス付与に係る審査や地方防衛局を通じた指導等を行っている。

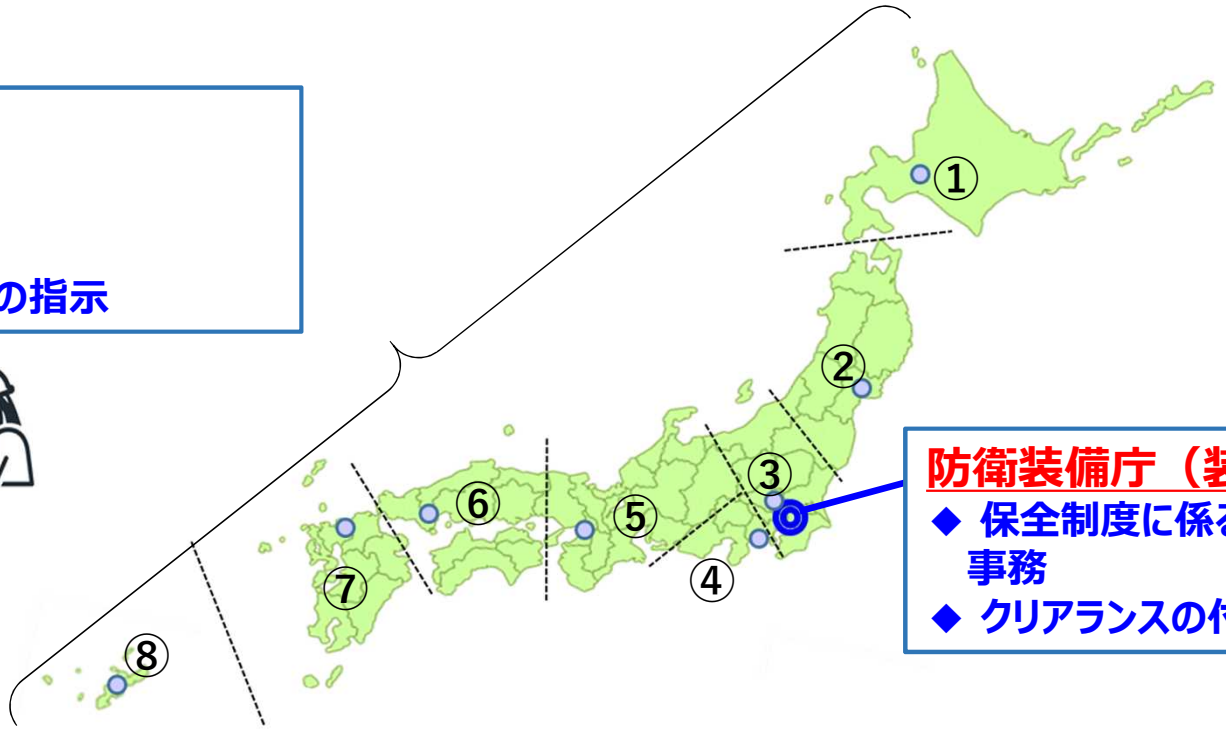
■ 保全検査等を実施する組織

地方防衛局は、契約企業の立入検査を実施し、結果を防衛装備庁に報告する。検査結果に基づき、地方防衛局は、保全管理のため契約企業に対し、指示を実施する。

地方防衛局
(全国８防衛局)

- ◆ 立入検査の実施
- ◆ 保全管理に係る企業への指示





防衛装備庁（装備保全管理官）

- ◆ 保全制度に係る政策・規則制定・行政事務
- ◆ クリアランスの付与に係る審査

国家防衛戦略、防衛力整備計画を踏まえた情報保全等に関する施策

国家防衛戦略（令和４年１２月１６日閣議決定）

Ⅶ　いわば防衛力そのものとしての防衛生産・技術基盤

１　防衛生産基盤の強化

我が国の防衛産業は、自衛隊の任務遂行に当たっての装備品の確保の面から、防衛省・自衛隊と共に国防を担うパートナーというべき重要な存在であり、高度な装備品を生産し、高い可動率を確保できる能力を維持・強化していく必要がある。（中略）さらに、防衛産業のサプライチェーンリスクに対応するとともに、**国際水準を踏まえたサイバーセキュリティを含む産業保全を強化**し、併せて機微技術管理の強化に取り組む。こうした観点から、同盟国・同志国等の防衛当局と、防衛産業に関するサプライチェーン保護、機微技術管理等を実施していく。

防衛力整備計画（令和４年１２月１６日閣議決定）

Ⅸ　いわば防衛力そのものとしての防衛生産・技術基盤

１　防衛生産基盤の強化

我が国の防衛産業は装備品のライフサイクルの各段階を担っており、装備品と防衛産業は一体不可分であり、防衛生産・技術基盤はいわば防衛力そのものと位置付けられるものである。（中略）**サイバー攻撃を含む諸外国の情報活動等からの情報保護は、防衛生産及び国際装備・技術協力の前提であり、防衛産業サイバーセキュリティ基準の防衛産業における着実な実施、防衛産業保全マニュアルを策定・適用するための施策を講じるとともに、産業保全制度の強化を行う。**また、特許出願非公開制度等の経済安全保障施策と連携した機微技術管理を実施する。

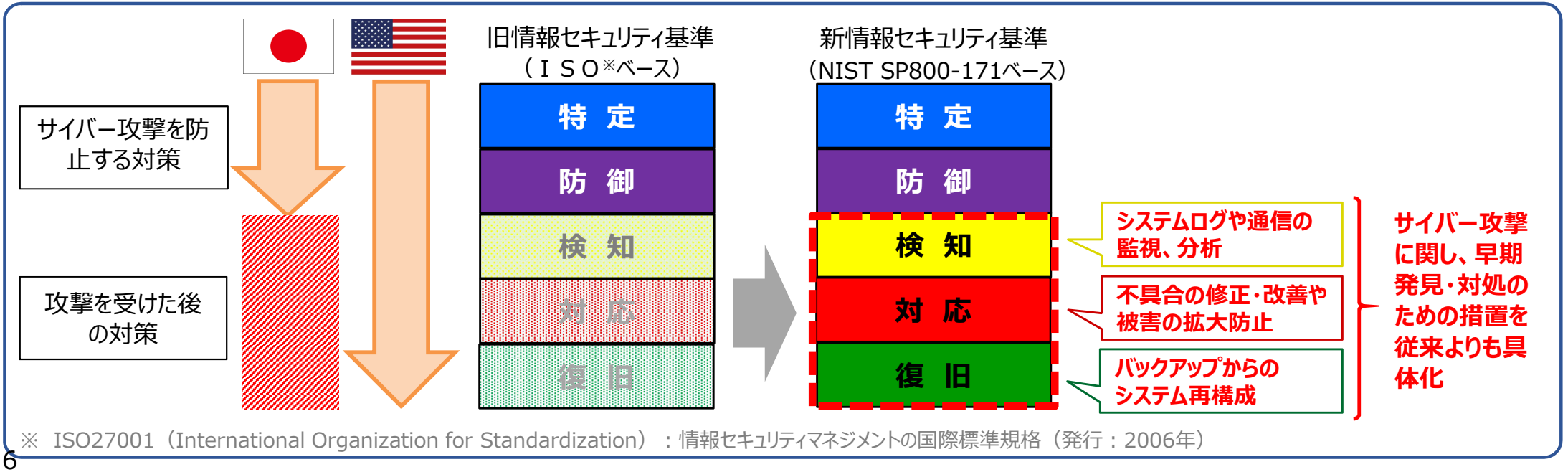
サイバーセキュリティ対策の強化（防衛産業サイバーセキュリティ基準）

米国の産業保全制度（注意情報）

- **NIST SP800-171： 非政府機関情報システムにおけるセキュリティ管理策**
  - ・米国防省が注意情報（CUI）を取り扱う契約相手方に対して義務付けている米国立標準技術研究所（NIST）が策定した情報セキュリティ基準

日本の産業保全制度（注意情報）

- 防衛省は、**NIST SP800－171と同水準の管理策を盛り込んだ**新たな情報セキュリティ基準である**「防衛産業サイバーセキュリティ基準」を令和４年３月に整備**（令和５年度から施行）



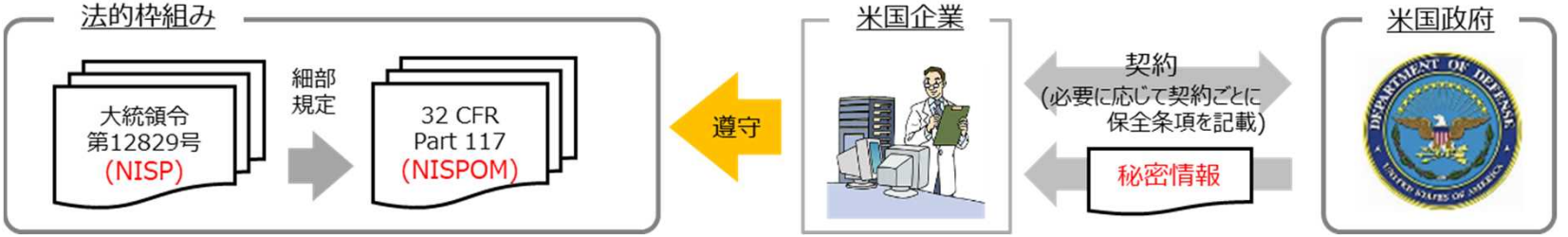
※ ISO27001（International Organization for Standardization）：情報セキュリティマネジメントの国際標準規格（発行：2006年）

防衛産業の国際化（防衛産業保全マニュアル整備）

米国の産業保全制度（秘密情報）

- **NISP：国家産業保全プログラム**
  (National Industrial Security Program)
  ・大統領令により設立された、米国政府の契約相手方に対して秘密情報の保護を義務付ける制度

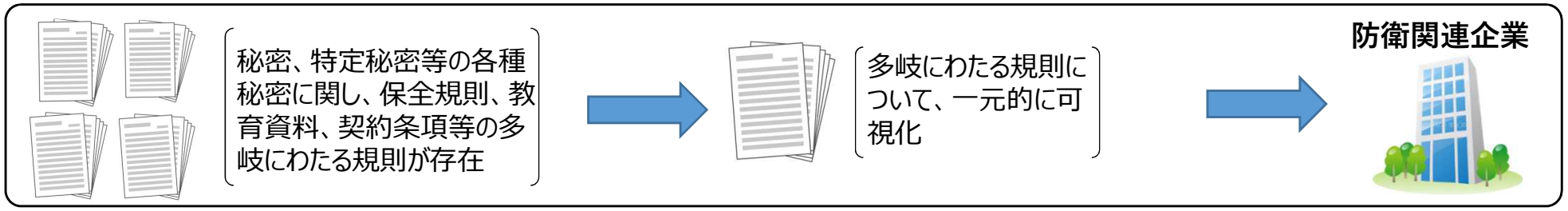
- **NISPOM：国家産業保全プログラム運用マニュアル**
  (National Industrial Security Program Operating Manual)
  ・大統領令に基づき、米国政府の契約相手方に対して秘密情報の保護を義務付けるための細部事項を定めた文書



日本の産業保全制度（秘密情報）

- 防衛省は、**国内法及び省内規則により産業保全の基本的なルールは整備済**
- 国際的な信頼性を高めるため、海外企業等にも分かりやすく理解できるよう、**NISPOMを参考にして「防衛産業保全マニュアル」を現在策定中**

防衛産業保全マニュアル整備（イメージ）



ATLA

Acquisition,Technology &
Logistics Agency