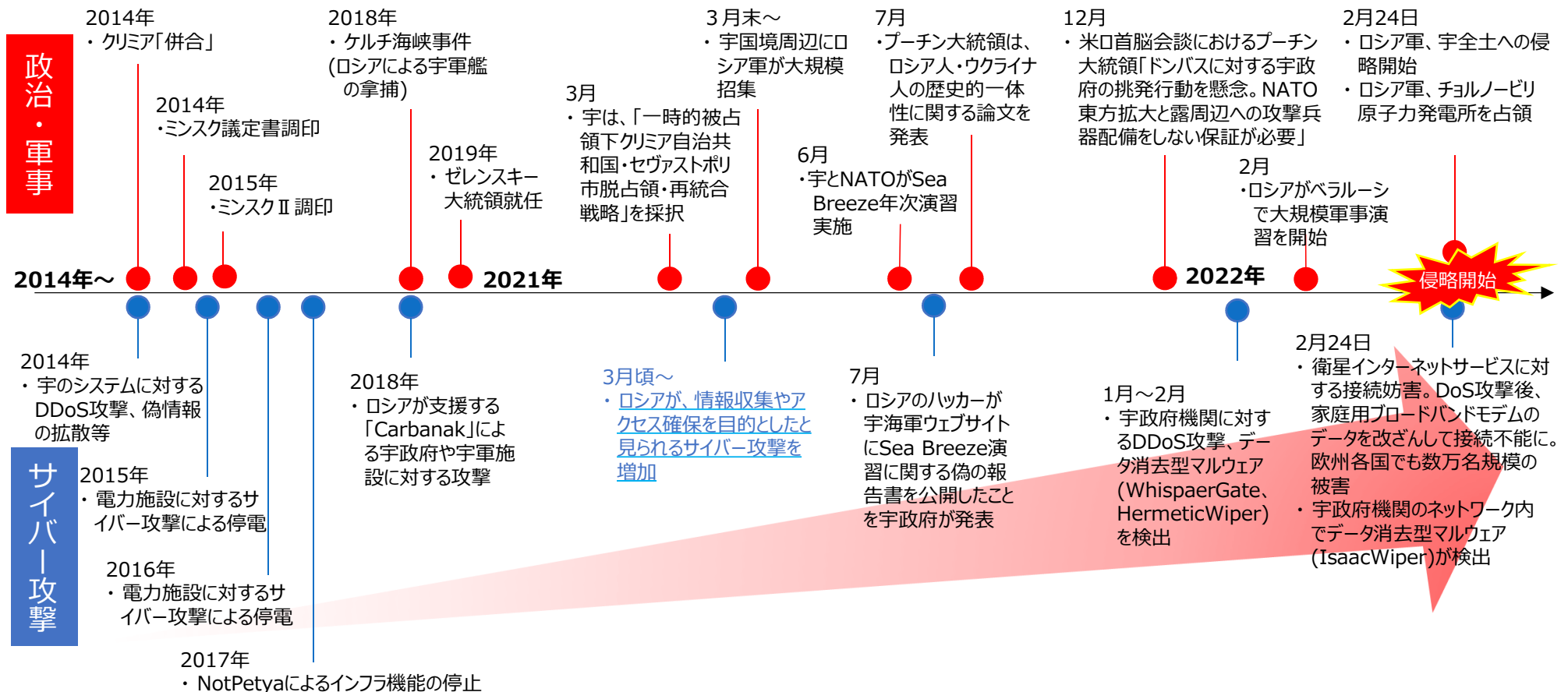


防衛省・自衛隊におけるこれまでの取組等

令和 6 年 7 月 1 日
防衛省

- サイバー攻撃は攻撃主体の特定や被害の把握が容易でないことから、敵の軍事活動を低コストで妨害可能な非対称的な攻撃手段として認識されており、**多くの外国軍隊がサイバー攻撃能力を開発**
- ロシアはウクライナ侵略において、**侵略開始時から、物理的な攻撃にサイバー攻撃を組み合わせることで効果の最大化を企図**
また、ロシアは**事前の段階から長期間にわたり、侵略開始を見据えて重要インフラ等への高度なサイバー攻撃を実施**



- **中国が、将来の紛争を見据えて、米国の重要インフラに対して悪意あるサイバー活動**を行っているとの指摘
- **中国が、2027年までに台湾侵攻**を可能とする能力構築を行っているとの指摘

(参考) 米国政府高官等の発言

- ・ 米中央情報局のバーンズ長官は、中国の習近平国家主席が「**2027年までに台湾侵攻**を成功させるための準備を**人民解放軍に指示**したことをインテリジェンス（情報）として把握している」と述べた。（2023年2月3日）
- ・ アクイリノ・インド太平洋軍司令官（当時）は、**中国軍は2027年までに台湾に侵攻**できる能力を完成させる計画だとの認識を示した。（2024年4月23日）

サイバー事案の一例

【中国】Volt Typhoonによる重要インフラに対するサイバー事案（2023年5月）

- ・ 米国、英国、豪州、カナダ及びNZやマイクロソフト社は**中国政府が支援するとされる「Volt Typhoon」**によって米国の重要インフラに対して悪意あるサイバー活動が行われていることを発表
 - 2021年半ばから、グアム島の**米軍施設を含む米国の重要インフラを標的**とした高度な Living Off The Land 戦術（システム内寄生戦術）※等を通じ、広範な不正アクセスを実施
 - 本活動を中国が**太平洋地域での将来の紛争**において**通信等の基幹インフラを破壊しうる能力を獲得**するためのものである可能性有と評価



戦略3文書に基づくサイバーセキュリティ強化の取組

国家安全保障戦略・国家防衛戦略

- サイバー空間の安全かつ安定した利用、特に国や重要インフラ等の安全等を確保するために、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上
- サイバー領域は、我が国の防衛にとっても領域横断作戦を遂行する上で死活的に重要

防衛省・自衛隊は、

- ・ **サイバー要員の大幅増強などにより高度なサイバーセキュリティを実現**
- ・ サイバーの領域において、**相手方の利用を妨げるために必要な能力を拡充**
- ・ **高いサイバーセキュリティ能力により、あらゆるサイバー脅威から自ら防護するとともに、その能力を生かして我が国全体のサイバーセキュリティの強化に取り組んでいく**
- ・ 自らのサイバーセキュリティのレベルを高めつつ、**関係省庁、重要インフラ事業者及び防衛産業との連携強化**に資する取組を推進
- ・ 能動的サイバー防御を含むサイバー安全保障分野における政府全体での取組と連携

防衛力整備計画



- **体制の大幅な拡充 サイバー専門部隊を約4,000人（サイバー関連業務を含む総サイバー要員約20,000人）**
- **高度人材の確保・育成 システム通信・サイバー学校への改編 など**
- **専門能力の高度化 同盟国・パートナー国との連携、共同訓練の実施（米、英、豪、NATO等）**
スレット・ハンティング機能の強化 など
- **自衛隊の能力を生かした国全体のセキュリティ強化への貢献 重要インフラ事業者・防衛関連企業との連携強化**

サイバー体制の大幅な拡充

- 防衛力整備計画期間中に**サイバー専門部隊を約4,000人に拡充（R5年度末時点で約2,230人）**
- そのうち、防衛大臣の直轄部隊である**自衛隊サイバー防衛隊**は、自衛隊のサイバーの中核を担う高度専門部隊として、陸・海・空自衛隊の各サイバー部隊等から**特に選抜されたハイレベル人材を登用**

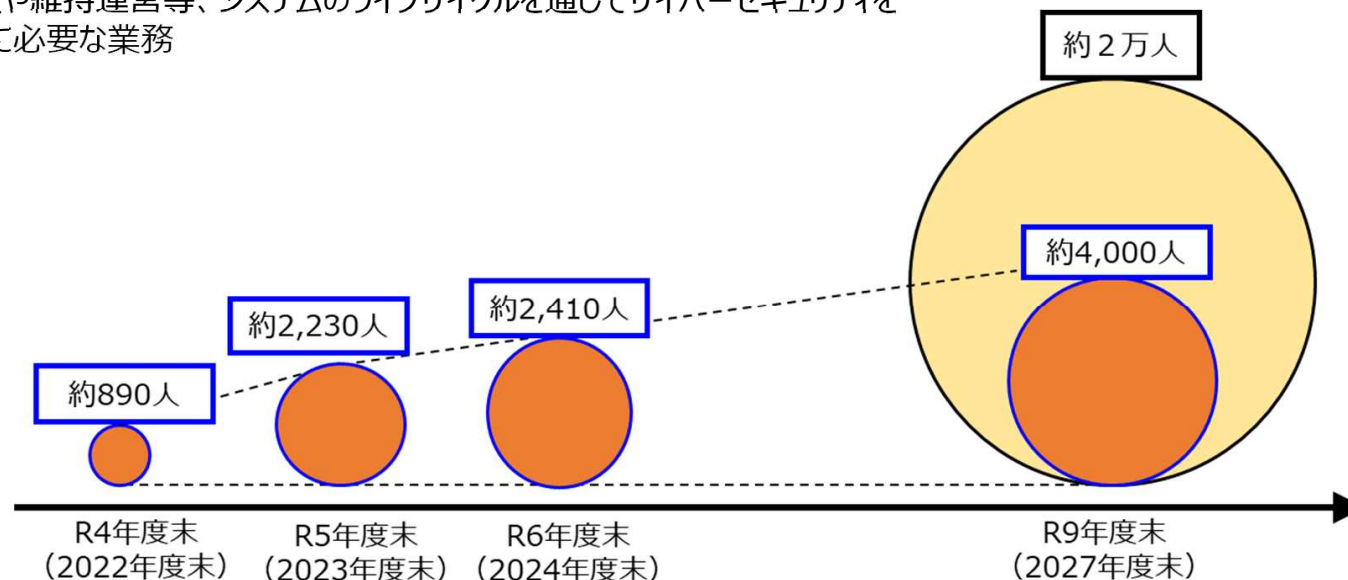
● サイバー関連業務(※)に従事する要員を含む総サイバー要員

● コア要員：サイバー専門部隊隊員
(総サイバー要員の内数)

※ システムの調達や維持運営等、システムのライフサイクルを通じてサイバーセキュリティを確保するために必要な業務



令和4年3月、自衛隊サイバー防衛隊を新編



高度人材の確保・育成

○ 自衛隊による計画的な人材育成とともに、民間の最先端の知見・技能を積極的に取り入れるための取組を推進

- ・ 自衛隊サイバー防衛隊、陸・海・空サイバー部隊の要員育成を行うため、**陸上自衛隊システム通信・サイバー学校を立ち上げ**
- ・ **防衛大学校サイバー・情報工学科**の新設、**高等工科大学校システムサイバー専修コース**の拡充など、部内のサイバー教育の充実
- ・ 民間人材の活用、部外の教育機関への派遣、専門企業での研修等により人材の高度化を推進



令和6年3月、陸自システム通信・サイバー学校改編行事（除幕式）

自衛隊による計画的な人材育成

サイバー教育基盤の拡充

- 陸自通信学校のサイバー教育体制を拡充し、システム通信・サイバー学校に改編し、サイバー教育のための施設、機材等を整備

意欲ある若年層への教育の実施

- 陸自高等工科大学校の「システム・サイバー専修コース」（令和3年度開講）の拡充
- 防衛大学校に「サイバー・情報工学科」を設置（令和6年度改編）

安全保障のフロントラインでの勤務経験

- サイバー部隊等での勤務により、安全保障の最前線での対処を経験



「システム・サイバー専修コース」の様子

民間分野における高度な知見を防衛分野で発揮

官民におけるサイバー人材の相互交流

自衛隊のサイバー人材も民間分野で活躍可能

民間の最先端の知見・技能の活用

高度な知見を有する民間人材の活用

- 「サイバーセキュリティ統括アドバイザー」や「AI・データ分析官」の採用

最新の脅威・技術に係る教育の実施

- 国内外の大学への派遣をはじめとする、部外教育機関を活用した教育

官民連携の強化

- 専門企業研修や官民人事交流の推進、NATOサイバー防衛協力センター主催の実践的な国際的サイバー防衛演習「ロックド・シールズ」に官民共同参加



「ロックド・シールズ」演習の様子

サイバー専門能力の高度化①（同盟国・パートナー国との共同訓練）

- サイバー空間における安全保障上の脅威の増大を受け、各国の軍隊もサイバー能力を強化
- 防衛省・自衛隊は、**高いサイバー能力を有する同盟国・パートナー国との共同訓練等を通じて、サイバー専門部隊の能力のさらなる高度化を推進**

＜直近の主な実績＞

【日本主催】

- ・ 令和6年 2月、多国間サイバー競技会「Cyber KONGO」
（参加国：米国、オーストラリア、ドイツ、フランス、リトアニア、ベトナム、フィリピンなど計16か国）

【米国】

- ・ 令和4年10月、米サイバー軍主催多国間演習「サイバーフラッグ」
- ・ 令和4年11月、日米共同統合演習（実働演習）
- ・ 令和4年11月、日米共同訓練（サイバー共同対処訓練）
- ・ 令和6年 2月、日米共同統合演習（指揮所演習）

【英国】

- ・ 令和6年 2月、英陸軍サイバー協会主催多国間演習「ディフェンス・サイバー・マーベル3」

【豪州】

- ・ 令和4年11月、豪国防省主催多国間演習「サイバースキルズチャレンジ」

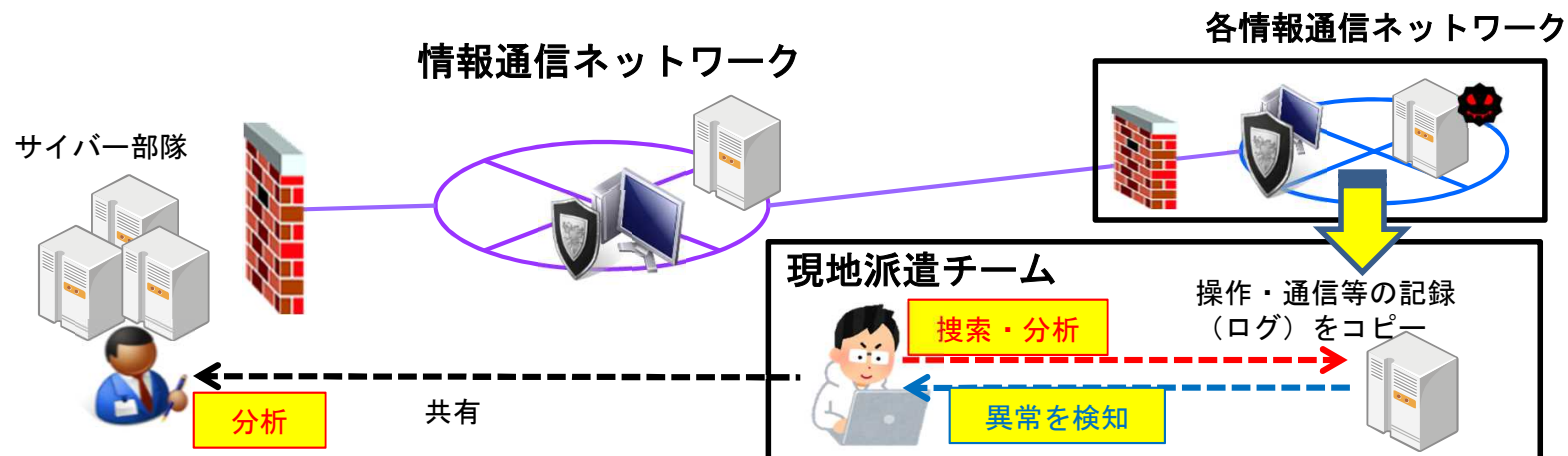
【NATO】

- ・ 令和5年12月、NATO主催多国間演習「サイバー・コアリション」
- ・ 令和6年 4月、NATO CCDCOE主催多国間演習「ロックド・シールズ」
（英軍との合同チーム。過去には米国、豪州と合同チームを編成して参加）



サイバー専門能力の高度化②（スレットハンティング機能の強化）

- 防衛省・自衛隊としてサイバーセキュリティを一層強化していくため、**攻撃者の視点に立ってシステム・ネットワークの潜在的脅威を洗い出す能力**を強化
 - ・ 「Volt Typhoon」の事案のように、従来の対策では検知できない高度なサイバー攻撃が発生
 - ・ システム・ネットワーク内部の安全性を当然視せず、**脅威が既に侵入していることを想定**して最新脅威を踏まえた仮説を立て、潜在的な脅威を積極的に探索・検出（スレットハンティング）



凡例： 通信の流れ

セキュリティ対策装置
(ファイアウォールなど)

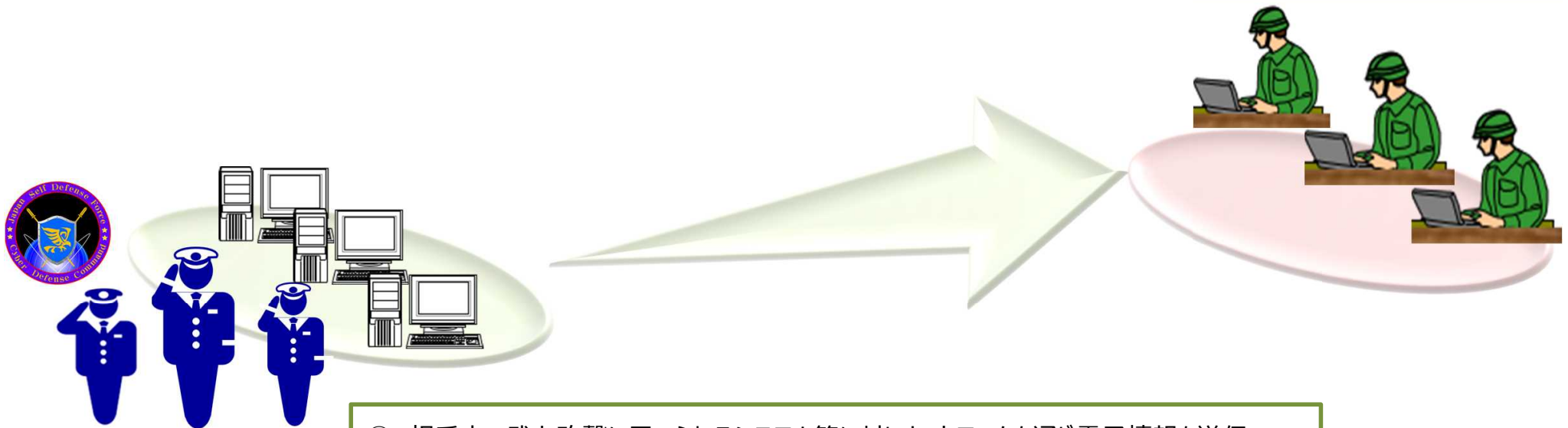
ウイルス対策装置
(ウイルス対策ソフトなど)

相手方のサイバー空間の利用を妨げる能力の強化

- 「平成31年度以降に係る防衛計画の大綱（平成30年12月）」において、**自衛隊が有事に際し、相手方がサイバー攻撃を行うこと自体を阻止する**能力等を強化することを閣議決定。戦略3文書（令和4年12月）においても、引き続き能力を拡充していくことを決定
- 2019年度から現在までの**約5年間、高度専門部隊である自衛隊サイバー防衛隊において、能力拡充等を推進**

（参考）平成31年度以降に係る防衛計画の大綱（平成30（2018）年12月閣議決定）抜粋

有事において、我が国への攻撃に際して当該攻撃に用いられる相手方によるサイバー空間の利用を妨げる能力等、サイバー防衛能力の抜本的強化を図る。



- ① 相手方の武力攻撃に用いられるシステム等に対しネットワークを通じ電子情報を送信
- ② 当該システム等の機能発揮に支障
- ③ 相手方がサイバー攻撃を行うこと自体を阻止 / 相手方の戦力の円滑な機能発揮を妨害

（令和3（2021）年3月15日 衆議院 安全保障委員会 岸国務大臣答弁）

重要インフラ事業者との連携強化（ロックド・シールドズ）

- **重要インフラに対するサイバー攻撃は、安全保障上の重大な脅威**であることから、防衛省・自衛隊として、自らの能力を生かしつつ連携強化に資する取り組みを推進
- 防衛省・自衛隊は、**多国間サイバー防衛演習（ロックド・シールドズ）**に**重要インフラ事業者等との合同チームを編成して参加**
（令和３年から正式参加し、これまで計４回参加）

ロックド・シールドズ（Locked Shields）2024の実績

- ・ 主催： NATOサイバー防衛協力センター（※）
- ・ 概要： **重要インフラ等のサイバー攻撃への対処能力向上のための対抗形式の演習（参加国数：40か国以上）**
- ・ チームの構成：日本は英国と合同チームを組み参加

（日本側）チームリーダー：自衛隊（**自衛隊サイバー防衛隊等**）

重要インフラ事業者、サイバーセキュリティ企業、防衛産業等 <計31法人>

内閣官房、外務省、経済産業省、警察庁

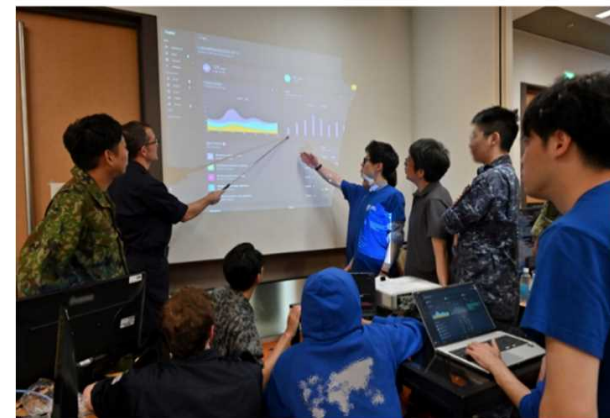
（英側）英国防省、英軍

（合計約180人）

（※） Cooperative Cyber Defence Centre of Excellence（CCDCOE）



ロックド・シールドズの光景（CCDCOE公式サイトより）



日本の演習会場の様子

防衛産業におけるサイバーセキュリティの強化

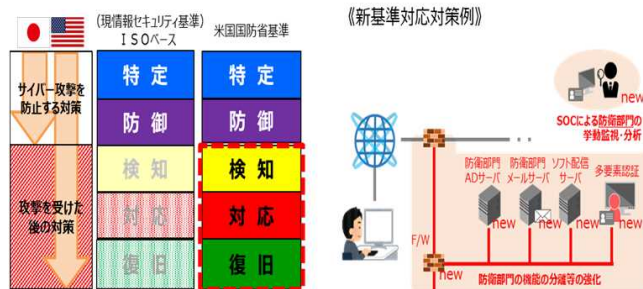
- 安全保障上、我が国の防衛力の一部である防衛産業のサイバーセキュリティの確保は、防衛生産及び国際装備・技術協力の前提として極めて重要
- 防衛省は、防衛産業のサイバーセキュリティを確保するため、米国基準である**NIST SP800-171※**と同水準の管理策を盛り込んだ**「防衛産業サイバーセキュリティ基準」**を令和4年3月に整備（令和5年度から施行）
- あわせて、**実効性確保のための財政的措置**や**防衛省と企業の間での安全なデータ共有を可能とするシステムの整備**等を実施
- また、防衛省と防衛産業との協力枠組み（**サイバーディフェンス連携協議会（CDC）**）を通じて、**防衛産業との情報共有や自衛隊との共同訓練を年1回実施し、対処能力の向上に貢献**

※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）を取り扱う契約企業に対して義務付けている情報セキュリティ基準）

実効性を高めるための事業

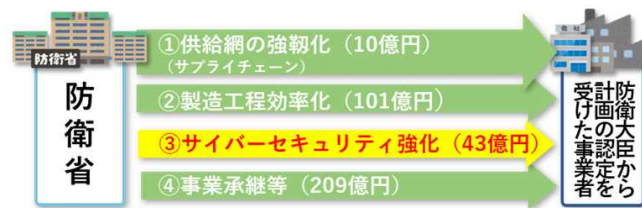
「防衛産業サイバーセキュリティ基準」の適用に係る措置（526億円）

基準に基づき、防衛産業が講じるサイバーセキュリティ対策に係る経費負担を防衛調達において措置（原価計算方式を採用する企業への措置）



防衛装備品等の生産基盤強化のための体制整備事業（363億円）

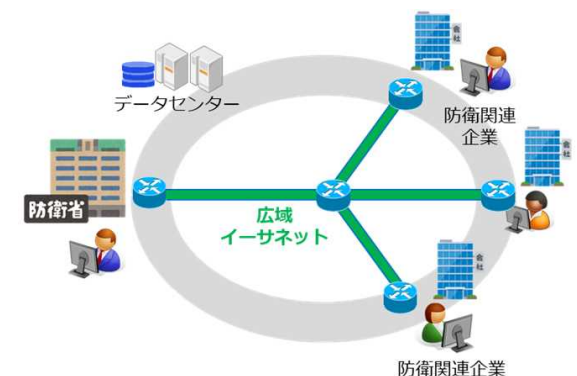
国内の防衛生産・技術基盤を維持・強化するため、サイバーセキュリティ強化体制などを整備等するための事業を実施



・防衛省と契約関係にある企業の防衛部門のみならず、下請企業に対しても総合的・一体的なサイバーセキュリティ対策を実施等

防衛セキュリティゲートウェイの整備（441億円）

防衛省と防衛関連企業の間で安全なデータ共有を可能とするネットワーク機能及び関連サービスを提供



注：予算額は、令和5年度予算

令和6年度サイバー関連予算

【サイバー領域における能力強化】 約2,115億円

- 高度化・巧妙化するサイバー攻撃に対し、将来にわたって適切に対処する能力を獲得し、自衛隊の任務遂行を保證できる態勢を確立するとともに、防衛産業のサイバー防衛を下支えできる態勢を構築。

リスク管理枠組み（RMF）の実施（365億円）

一過性の「リスク排除」から継続的な「リスク管理」へ考え方を転換し、情報システムの運用開始後も常時継続的にリスクを分析・評価し、必要なセキュリティ対策を実施

情報システムの防護

装備品や施設インフラを含む情報システムの防護態勢を強化

- システム・ネットワーク管理機能（SNMS）の整備（138億円）
- サイバー防護分析措置の整備（11億円）
- サイバー演習環境の整備（14億円）
- スレットハンティング器材の整備（22億円）

サイバー分野における教育・研究機能の強化

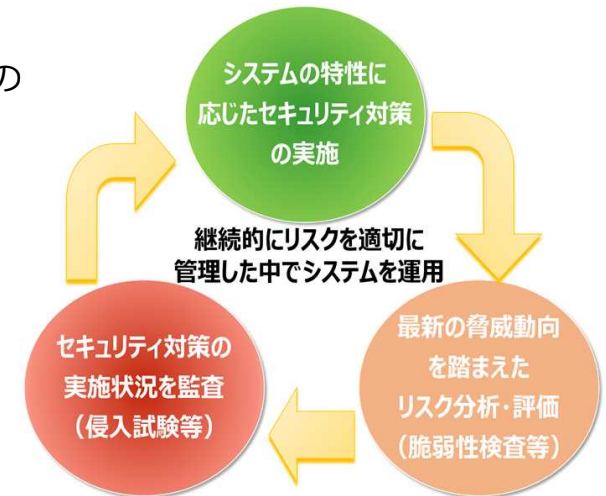
- 各学校におけるサイバー教育基盤の拡充（20億円）
- 部外力を活用したサイバー教育（16億円）
- 諸外国とのサイバー分野における連携強化（4億円）
- サイバー等安全保障研究体制の強化（2億円）

サイバー防衛体制の抜本的強化

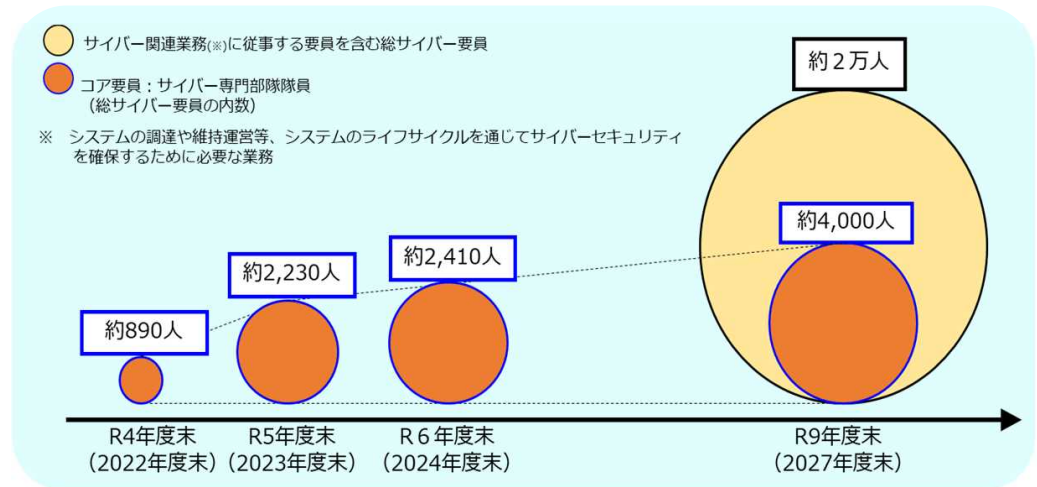
防衛省・自衛隊として備えるべきサイバー防衛機能の見直し、必要なサイバー要員を拡充

防衛産業におけるサイバーセキュリティ対策

- 防衛装備品の生産基盤強化のための体制整備事業（86億円）
防衛省と契約関係にある企業の防衛部門のみならず、下請企業に対しても総合的・一体的なサイバーセキュリティ対策を実施



リスク管理枠組み（イメージ）



体制強化（イメージ）

參考資料

「国家防衛戦略」（令和4年12月16日 国家安全保障会議 閣議決定）

Ⅲ 我が国の防衛の基本方針

1 我が国自身の防衛体制の強化

(2) 国全体の防衛体制の強化

Ⅰ 宇宙・サイバー・電磁波の領域は、国民生活にとっての基幹インフラであるとともに、我が国の防衛にとっても領域横断作戦を遂行する上で死活的に重要であることから、政府全体でその能力を強化していく。

（中略）

サイバー領域においては、諸外国や関係省庁及び民間事業者との連携により、平素から有事までのあらゆる段階において、情報収集及び共有を図るとともに、我が国全体としてのサイバー安全保障分野での対応能力の政策が一元的に総合調整されていくことを踏まえ、防衛省・自衛隊においては、自らのサイバーセキュリティのレベルを高めつつ、関係省庁、重要インフラ事業者及び防衛産業との連携強化に資する取組を推進することとする。

2 日米同盟による共同抑止・対処

(1) 日米共同の抑止力・対処力の強化

（中略）

具体的には、日米共同による宇宙・サイバー・電磁波を含む領域横断作戦を円滑に実施するための協力及び相互運用性を高めるための取組を一層深化させる。

(3) 共同対処基盤の強化

（中略）

あらゆる段階における日米共同での実効的な対処を支える基盤を強化する。まず、日米がその能力を十分に発揮できるよう、あらゆるレベルにおける情報共有を更に強化するために、情報保全及びサイバーセキュリティに係る取組を抜本的に強化する。

Ⅳ 防衛力の抜本的強化に当たって重視する能力

4 領域横断作戦能力

(2) サイバー領域では、防衛省・自衛隊において、能動的サイバー防御を含むサイバー安全保障分野における政府全体での取組と連携していくこととする。その際、重要なシステム等を中心に常時継続的にリスク管理を実施する態勢に移行し、これに対応するサイバー要員を大幅増強するとともに、特に高度なスキルを有する外部人材を活用することにより、高度なサイバーセキュリティを実現する。このような高いサイバーセキュリティの能力により、あらゆるサイバー脅威から自ら防護するとともに、その能力を生かして我が国全体のサイバーセキュリティの強化に取り組んでいくこととする。

このため、2027年度までに、サイバー攻撃状況下においても、指揮統制能力及び優先度の高い装備品システムを保全できる態勢を確立し、また防衛産業のサイバー防衛を下支えできる態勢を確立する。

今後、おおむね10年後までに、サイバー攻撃状況下においても、指揮統制能力、戦力発揮能力、作戦基盤を保全し任務が遂行できる態勢を確立しつつ、自衛隊以外へのサイバーセキュリティを支援できる態勢を強化する。

(4) 宇宙・サイバー・電磁波の領域において、相手方の利用を妨げ、又は無力化するために必要な能力を拡充していく。

「防衛力整備計画」（令和4年12月16日 国家安全保障会議 閣議決定）

Ⅱ 自衛隊の能力等に関する主要事業

4 領域横断作戦能力

(2) サイバー領域における能力

政府全体において、サイバー安全保障分野の政策が一元的に総合調整されることを踏まえ、防衛省・自衛隊においては、自らのサイバーセキュリティのレベルを高めつつ、関係省庁、重要インフラ事業者及び防衛産業との連携強化に資する取組を推進することとする。

サイバー攻撃を受けている状況下において、指揮統制能力及び優先度の高い装備品システムを保全し、自衛隊の任務遂行を保証できる態勢を確立するとともに、防衛産業のサイバー防衛を下支えできる態勢を構築する。

このため、最新のサイバー脅威を踏まえ、境界型セキュリティのみでネットワーク内部を安全に保ち得るという従来の発想から脱却し、もはや安全なネットワークは存在しないとの前提に立ち、サイバー領域の能力強化の取組を進める。この際、ゼロトラストの概念に基づくセキュリティ機能の導入を検討するとともに、常時継続的にリスクを管理する考え方を基礎に、情報システムの運用開始後も継続的にリスクを分析・評価し、適切に管理する「リスク管理枠組み（RMF）」を導入する。さらに、装備品システムや施設インフラシステムの防護態勢を強化するとともに、ネットワーク内部に脅威が既に侵入していることも想定し、当該脅威を早期に検知するためのサイバー・スレット・ハンティング機能を強化する。また、防衛関連企業に対するサイバーセキュリティ対策の強化を下支えするための取組を実施する。

防衛省・自衛隊のサイバーセキュリティ態勢の強化のため、陸上自衛隊通信学校を陸上自衛隊システム通信・サイバー学校に改編し、サイバー要員を育成する教育基盤を拡充する。さらに、我が国へのサイバー攻撃に際して当該攻撃に用いられる相手方のサイバー空間の利用を妨げる能力の構築に係る取組を強化する。

これらの取組を行う組織全体としての能力を強化するため、2027年度を目途に、自衛隊サイバー防衛隊等のサイバー関連部隊を約4,000人に拡充し、さらに、システム調達や維持運営等のサイバー関連業務に従事する隊員に対する教育を実施する。これにより、2027年度を目途に、サイバー関連部隊の要員と合わせて防衛省・自衛隊のサイバー要員を約2万人体制とし、将来的には、更なる体制拡充を目指す。

Ⅲ 自衛隊の体制等

1 統合運用体制

(2) サイバー領域における更なる能力向上のため、防衛省・自衛隊のシステム・ネットワークを常時継続的に監視するとともに、我が国へのサイバー攻撃に際して当該攻撃に用いられる相手方によるサイバー空間の利用を妨げる能力等、サイバー防衛能力を抜本的に強化し得るよう、共同の部隊としてサイバー防衛部隊を保持する。

Ⅳ 日米同盟の強化

1 日米防衛協力の強化

あらゆる段階における日米共同での実効的な対処を支える基盤を強化するため、日米間の情報共有を促進するための情報保全及びサイバーセキュリティに係る取組を強化する（以下略）

相手方のサイバー空間の利用を妨げる能力

国家防衛戦略（令和4年12月16日 国家安全保障会議 閣議決定）

Ⅳ 防衛力の抜本的強化に当たって重視する能力

4 領域横断作戦能力

（4）宇宙・サイバー・電磁波の領域において、相手方の利用を妨げ、又は無力化するために必要な能力を拡充していく。

防衛力整備計画（令和4年12月16日 国家安全保障会議 閣議決定）

Ⅱ 自衛隊の能力等に関する主要事業

4 領域横断作戦能力

（2）サイバー領域における能力

さらに、我が国へのサイバー攻撃に際して当該攻撃に用いられる相手方のサイバー空間の利用を妨げる能力の構築に係る取組を強化する。

Ⅲ 自衛隊の体制等

1 統合運用体制

（2）サイバー領域における更なる能力向上のため、防衛省・自衛隊のシステム・ネットワークを常時継続的に監視するとともに、我が国へのサイバー攻撃に際して当該攻撃に用いられる相手方によるサイバー空間の利用を妨げる能力等、サイバー防衛能力を抜本的に強化し得るよう、共同の部隊としてサイバー防衛部隊を保持する。

衆議院 安全保障委員会（令和3年3月15日）

○ 美延委員

（略）サイバー上の反撃能力について大臣はどのようにお考えなのか、御所見を伺えますでしょうか。

○ 岸国務大臣

防衛大綱では、有事において、相手方によるサイバー空間の利用を妨げる能力等の抜本的強化を図ることとしています。

この能力は、有事に際して、相手方の武力攻撃に用いられるシステム等に対し、ネットワークを通じ電子情報を送信することによって、当該システム等の機能発揮に支障を生じさせることで、相手方がサイバー攻撃を行うこと自体を阻止する、又は相手方の戦力の円滑な機能発揮を妨害する能力であります。
この能力を含め、引き続きサイバー防衛能力の抜本的な強化を図ってまいります。