防衛装備庁

研究開発ビジョン

多次元統合防衛力の実現とその先へ

解説資料

サイバー防衛の取組

令和２年３月31日

防衛装備庁

「研究開発ビジョン」とは

「研究開発ビジョン」とは、先進的な研究を中長期的な視点に基づいて体系的に行うため、今後の我が国の防衛に必要な能力の獲得に必要な技術について、基本的な考え方を示した上で、技術的課題やロードマップを提示した文書です。

これまで、防衛省は、平成22年に「将来戦闘機に関する研究開発ビジョン」、平成28年に防衛生産・技術基盤戦略及び防衛技術戦略に基づき「将来無人装備に関する研究開発ビジョン」を策定したところですが、今般、「平成31年度以降に係る防衛計画の大綱」に示された方向性を踏まえ、多次元統合防衛力の実現に資するとともに、今後の更なる防衛力の強化に必要となる技術革新を実現すべく、新たに「電磁波領域」、「宇宙を含む広域常続型警戒監視」及び「サイバー防衛」といった新たな領域における能力の獲得・強化や「水中防衛」及び「スタンド・オフ防衛能力」といった従来の領域における能力の強化につながる研究開発ビジョンを策定することとしました。

防衛省は今後、本研究開発ビジョンを踏まえつつ、将来必要となる技術を戦略的に育成し、効果的・効率的に研究開発を行ってまいります。

注　装備化を見据えた開発に着手するか否かは、本研究開発ビジョンに基づき実施される研究の成果や、その時の安全保障環境、諸外国の類似装備品の取得可能性等、防衛力整備や、財政状況を踏まえ、総合的に判断されます。

目　次

研究開発ビジョン本冊との対応表

研究開発ビジョン

P11-12

サイバー防衛技術の分類 (p.8)

サイバー防衛機能コンセプト図 (p.12)

はじめに

我が国を取り巻く安全保障環境

情報通信等の分野における急速な技術革新に伴い、軍事技術の進展は目覚ましいものとなっており、この技術進展を背景に、現在の戦闘様相は、陸・海・空のみならず、宇宙・サイバー・電磁波といった新たな領域を組み合わせたものとなっている。各国は、全般的な軍事能力の向上のため、新たな領域における能力を裏付ける技術の優位を追求している。宇宙領域やサイバー領域は、民生分野でも広範に活用されており、この安定的な利用が妨げられれば、国家・国民の安全に重大な影響が及ぶおそれがある。

周辺諸国におけるサイバー領域に関する情勢

軍隊は任務遂行上、電力をはじめとする様々な重要インフラに依存しており、これらの重要インフラに対するサイバー攻撃が、任務の大きな阻害要因になり得る。このような中、中国は、今世紀半ばまでに「世界一流の軍隊」を建設することを目標に、透明性を欠いたまま、高い水準で国防費を増加させ、軍事力の質・量を広範かつ急速に強化しており、その際、指揮系統の混乱等を可能とするサイバー領域における能力を急速に発展させている。また、北朝鮮は非対称的な軍事能力として、サイバー領域について、大規模な部隊を保持するとともに、軍事機密情報の窃取や他国の重要インフラへの攻撃能力の開発を行っているとみられる。

サイバー領域における能力獲得の方向性

30大綱には、「サイバー領域を活用した情報通信ネットワークは、様々な領域における自衛隊の活動の基盤であり、これに対する攻撃は、自衛隊の組織的な活動に重大な障害を生じさせるため、こうした攻撃を未然に防止するための自衛隊の指揮通信システムやネットワークに係る常時継続的な監視能力や被害の局限、被害復旧等の必要な措置を迅速に行う能力を引き続き強化。また、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。その際、専門的な知識・技術を持つ人材を大幅に増強する。」とされている。

① サイバー領域の安定的な利用が妨げられた場合、国家・国民の安全に重大な影響
② 防衛省・自衛隊は様々な重要インフラに依存しており、重要インフラへのサイバー攻撃は任務への大きな阻害要因
③ 周辺諸国は、サイバー領域に係る能力を向上させており、現実的な脅威
④ サイバー領域に係る能力を引き続き強化するためには、最新の技術動向を踏まえながら、研究開発を進める必要

といった理由から防衛省・自衛隊のサイバー空間における活動に必要な技術について、防衛省として解決に取り組むべき技術的課題を整理し、我が国が技術的優越を着実に確保するための実行可能なロードマップを導出することにより、各種施策を推進する。

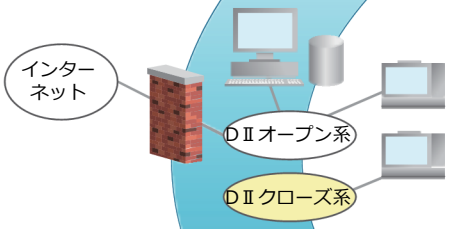
防衛省・自衛隊のサイバー空間における活動

防衛省・自衛隊におけるサイバー攻撃対処のための総合的施策

サイバー攻撃により自衛隊の重要なシステムの機能が停止した場合、わが国の防衛の根幹に関わる問題が発生する可能性がある。そのため、防衛省・自衛隊としては、①情報システムの安全性確保、②専門部隊によるサイバー攻撃対処、③サイバー攻撃対処態勢の整備、④最新技術の研究、⑤人材育成、⑥他機関等との連携を「サイバー攻撃対処6本柱」と位置づけ、施策の総合的かつ効果的な推進を図っている。

1. 情報システムの安全性確保

- ファイアーウォール、ウィルス検知ソフトの導入
- ネットワークをDⅡオープン系・クローズ系とに分離
- システム監査の実施等



2. 専門部隊によるサイバー攻撃対処

- サイバー防衛隊（統）、システム防護隊（陸）、保全監査隊（海）、システム監査隊（空）によるネットワーク・情報システムの24時間監視、高度なサイバー攻撃対処（ウィルス解析）

3. サイバー攻撃対処態勢の整備

- 情報システムのセキュリティ対策基準の制定
- 職員が遵守すべきセキュリティ対策の制定
- サイバー攻撃発生時の対処態勢の整備
- サイバー政策検討委員会の設置

サイバー攻撃対処6本柱

4. 最新技術の研究

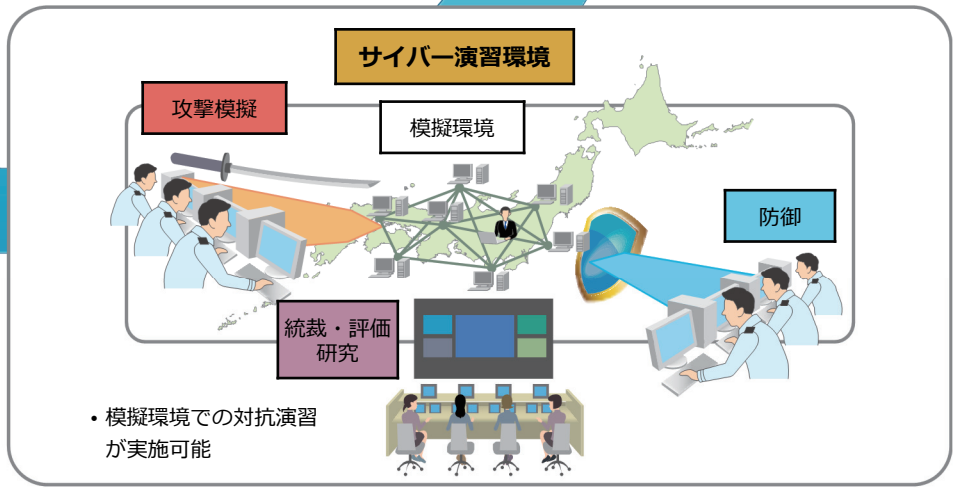
- サイバー演習環境構築技術の研究

6. 他機関等との連携

- 内閣サイバーセキュリティセンター、米軍、関係各国等との情報共有

5. 人材育成

- 人材育成のため、米国カーネギーメロン大学付属機関、国内大学院への留学や各自衛隊の専門課程における教育の実施
- セキュリティ意識の醸成のため、職場における教育、防衛大学校における専門教育の実施



- 模擬環境での対抗演習が実施可能

サイバー防衛の強化を図る上での課題

防衛省・自衛隊のサイバー防衛の強化を図る上での課題

全般

- サイバー攻撃には、情報通信ネットワークや情報システム等の悪用により、サイバー空間を経由して行われる不正侵入、情報の窃取、改ざんや破壊、情報システムの作動停止や誤作動、不正プログラムの実行やDDoS攻撃（Distributed Denial of Service Attack）等が存在。防衛省・自衛隊のネットワーク及びシステムにサイバー攻撃が行われた場合には、自衛隊の運用継続に大きな影響を与える可能性があり、対応策の内容は重要な課題となっている。
- また、30大綱に示されたとおり、有事においては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の獲得も喫緊の課題である。

技術

- 防衛省・自衛隊においてはシステムをインターネットに接続するオープン系と接続しないクローズ系に分け、サイバー防衛隊及び各自衛隊のシステム防護部隊によって、常時システム及びネットワークを監視・防護している。その一方で、近年、標的型攻撃やゼロデイ攻撃のように、ファイアウォールやマルウェア対策等の従来の未然防止対策をすり抜ける攻撃手法が増加。また、インターネットに接続しないシステムへの攻撃成功の事例も報告されている。
- それに伴い、防衛省・自衛隊においても、使用システムを長期間停止させないために、「未然防止対策」と仮に攻撃を受けた場合においても、いち早く発見・対処する「運用継続対策」を両立させ、システムの抗たん性を向上させることが重要となっている。

防衛省・自衛隊として獲得すべき技術

※ 主要な構成技術として考えられるものを例示

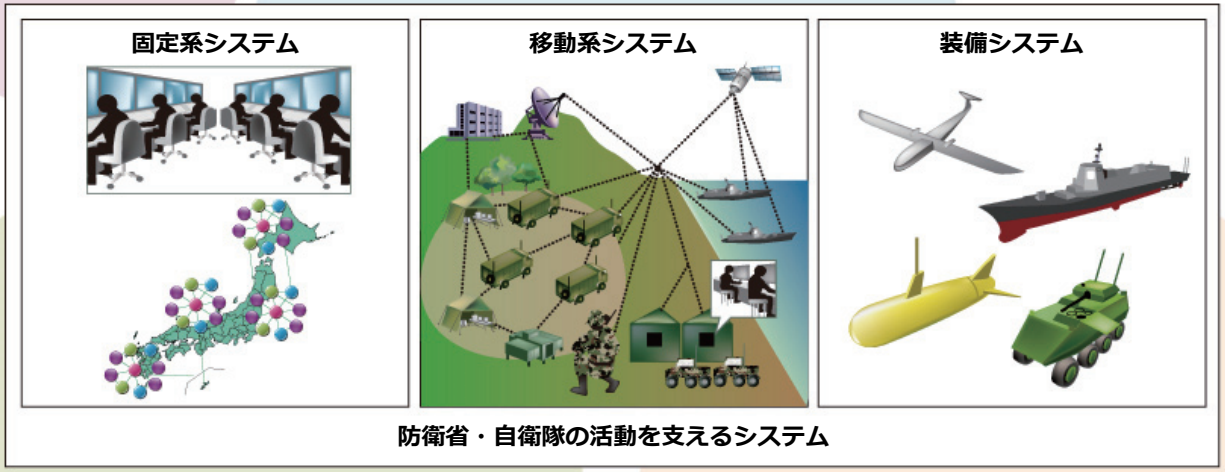
未然防止対策

サプライチェーン・インテグリティ技術　　脆弱性調査技術

耐タンパー技術　　装備システムサイバー攻撃対処技術

ファイアウォール技術　　マルウェア対策技術

“妨げる能力”に資する技術



防衛省・自衛隊の活動を支えるシステム

人的対処で行う運用継続対策

サイバー演習環境構築技術

サイバー攻撃再現・制御技術

サイバー演習統制情報収集技術

サイバー演習環境回復技術

自動対処を行う運用継続対策

サイバーレジリエンス技術

統制機能抗たん性技術

システム基盤・ネットワーク基盤の情報管理技術

システム基盤・ネットワーク基盤の基盤統制技術

未然防止対策のうち、民生分野との共通技術については、先進的な民生技術の積極的な活用により必要な技術を獲得。一方、未然防止対策のうち、市場からの調達が困難な装備システムサイバー攻撃対処技術、脆弱性調査技術及び妨げる能力に資する技術や、運用継続対策については、防衛省・自衛隊に固有の要求があるため、研究開発を通じ技術を戦略的に獲得する。

求められる先進技術

サイバー防衛の技術的進展

- 未然防止対策においては、マルウェア対策技術などは民間で活発に研究がすすめられている。他方、耐タンパー技術などは民間でも研究はしているが公開情報としては少ない
- 人的対処で行う運用継続対策においては、サイバー対策要員の訓練のため、一般的な器材を用いた実環境とは異なるサイバー演習環境は実用化しつつあるが、実環境を用いたサイバー演習環境を構築する技術は少ない
- 自動対処を行う運用継続対策においては、セキュリティのログ情報のリアルタイム解析や人工知能技術の活用など動的なサイバー攻撃の検知は実用化しつつあるが、運用継続と未然防止の両立を行う技術は少ない

マルウェア対策技術

耐タンパー技術

ファイアウォール技術

⇒ 未然防止対策等を中心に進展

今後の進展の方向性

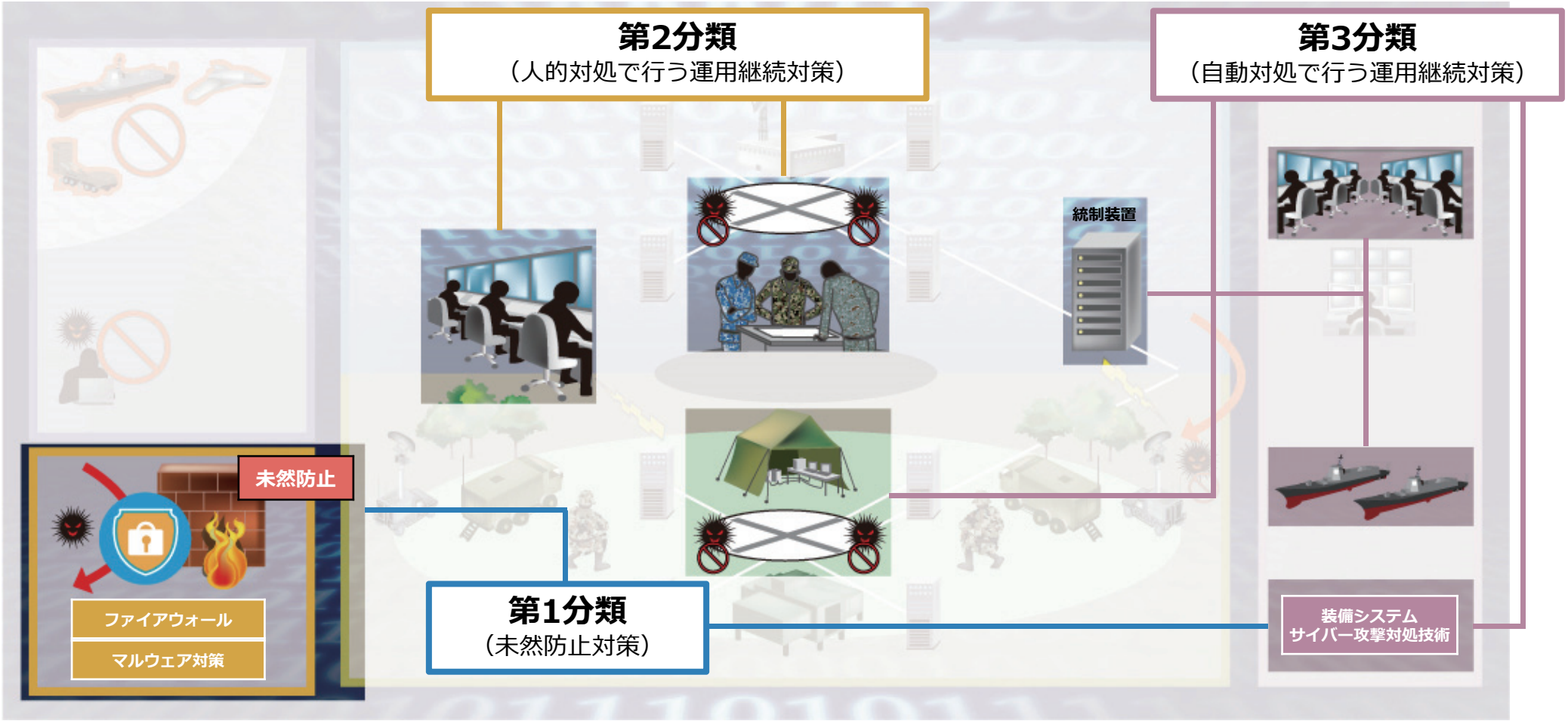
- システム及びネットワークへのサイバー攻撃を未然に防止するため、優れた民間技術を取り入れ、防衛省・自衛隊のシステム等に適合させていく必要（将来的にサイバー防衛の能力向上に資する可能性のある、量子通信・量子暗号技術等を注視）
- 人的に行う運用継続対策においては、クラウド化技術の進展により、セキュリティの境界が曖昧となることでサイバー攻撃が高度化し、モバイル端末の増加や移動系システムのCOTS適用等によるマルウェア感染元の爆発的な増加等が予想されるため、サイバー対策要員の能力の向上の対策を行う必要
- 自動的に対処を行う運用継続対策において、移動系システムのような低品質、低速度の回線に対して、サイバー攻撃の被害拡大防止と運用継続の確保を迅速に行う必要。加えて、自動対処を行う運用継続対策については、ＡＩ及び量子関連技術の活用について、システムへの適合性を確認しつつ、活用していく必要
- リアルタイム処理が要求される装備システムにおいては、これまで列挙した未然防止や自動的に対処を行う運用継続対策を、装備システムに適合させることが必要

サイバー防衛機能の実現で鍵となる先進技術

- 民間技術を効果的に適合させた、相手からのサイバー攻撃を事前に防止するための技術（例えば、内部情報漏えい・改ざんを防止する技術、我のシステムの脆弱性を調査可能な技術、不正な改造が行われたハードウェア・プログラムを検出する技術）

  ※ 将来的には、高度な秘匿化に資する可能性のある量子暗号・量子通信技術等
- サイバー対策要員の育成及び対処要領の演練に寄与する、サイバー演習環境構築技術（我のシステム等を模擬する技術、演練者の練度に合わせた自律的な攻撃を行う技術、演練者の対処を評価する技術等）
- 自動でシステムの運用の継続性を確保するための、サイバー攻撃の被害拡大防止と運用継続の確保を踏まえた、サイバーレジリエンス技術（システム基盤等を基盤統制機能を維持する技術、被害拡大防止と重要システムの運用を継続させるための技術、重要システムの運用状況等の管理を行う技術）が必要。また、その自動化・高速化を促進するための、ＡＩ等技術
- 装備システムへのサイバー攻撃を事前に防止するための技術及び内部で発生したサイバー攻撃を検知し、システムの運用状況等を判断し、運用継続を行う技術

サイバー防衛技術の分類



分　類	内　容
第1分類（未然防止対策）	情報セキュリティ製品としてマルウェア対策ソフトやファイアウォールなどがあり、サイバー攻撃を未然に防止するもの
第2分類（人的対処で行う運用継続対策）	サイバー攻撃後に人的対処で行う運用継続対策を行うため、サイバー対策要員の訓練のためのもの。移動系サイバー演習環境構築技術等が該当
第3分類（自動対処を行う運用継続対策）	サイバー攻撃後にシステム等で自動対処を行う運用継続対策を行うためのもの。サイバーレジリエンス技術等が該当

取り組むべき主な技術課題（サイバー防衛）①

赤： 主として防衛省が行うサイバー関連研究により確立する技術
青： 防衛省が行うサイバー以外の研究により確立する技術（他の研究開発成果を活用できる）
灰色： 他機関との共同研究等により獲得する技術
水色： 民生分野における進展を待つ技術

項目	主要構成技術		技術の概要	技術的課題	期待できる効果
第1分類	耐タンパー技術	ハードウェア耐タンパー技術	ハードウェアによる内部情報漏洩・改ざん防止技術	防衛省・自衛隊のシステムへの最適化	システムの一部がろ獲等された場合における、ろ獲されたハードウェア等からのプログラムの逆解析等を困難化
		ソフトウェア耐タンパー技術	ソフトウェアによる内部情報漏洩・改ざん防止技術	防衛省・自衛隊のシステムへの最適化	
	脆弱性調査技術		システムの脆弱性を調査可能な技術	防衛省・自衛隊のシステムへの最適化	システム内の未知の脆弱性を発見可能 ハードウェアの真贋を判定可能 不正改造されたプログラムを発見可能
	サプライチェーン・インテグリティ技術		不正改造されたハードウェアや、不正なプログラムを発見する技術	防衛省・自衛隊のシステムへの最適化	
	マルウェア対策技術、ファイアウォール技術等		不正なプログラムの実行防止、 不正な通信の防止等	防衛省・自衛隊のシステムへの最適化	防衛省、自衛隊のシステムへのサイバー攻撃の防止
	装備システムサイバー攻撃対処技術		装備システムと接続する外部のシステム等からのサイバー攻撃への防護を行う	戦闘指揮システムの性能への影響を局限化しつつ防護を実現すること	戦闘指揮システム等へのサイバー攻撃の防止

取り組むべき主な技術課題（サイバー防衛）②

赤： 主として防衛省が行うサイバー関連研究により確立する技術
青： 防衛省が行うサイバー以外の研究により確立する技術（他の研究開発成果を活用できる）
灰色： 他機関との共同研究等により獲得する技術
水色： 民生分野における進展を待つ技術

項目	主要構成技術		技術の概要	技術的課題	期待できる効果
第2分類	移動系サイバー演習環境構築技術	サイバー攻撃再現・制御技術	演習者の練度に合わせた自律的な模擬マルウェアによる攻撃を行う技術	中央からの制御通信が発生しない、自律的なサイバー攻撃を再現・制御	実環境を模擬した訓練が可能となり、効果的な人材育成・対処要領の演練が可能
		サイバー演習統制情報収集技術	サイバー攻撃の状況、対処の状況等演習統制に必要な情報を通信のタイミングや情報量の削減を行い情報収集を行う技術。	情報収集にかかる通信を削減し、演習統制に必要な情報を収集する技術	
		サイバー演習環境回復技術	サイバー攻撃や対処により変更された部分のみを速やかに回復を行う技術	サイバー攻撃や対処により変更された部分のみを迅速に復元する技術	
第3分類	サイバーレジリエンス技術	システム基盤・ネットワーク基盤の情報管理技術	サイバー攻撃の状況、システムの運用情報及び各種事態の状況等を一元的に管理する技術。	各種事態に応じたシステムの重要度の動的な変化に対応する技術。 サイバー攻撃や物理的攻撃等により複数拠点やネットワークが被害を受けた場合においても対応可能な技術。	蓄積されたログの自動解析等により、サイバー攻撃の兆候を早期検出 ・攻撃と被害発生を早期に検出 ・被害拡大防止・対処の自動化 ・被害発生時における、重要システムの運用継続可能
		システム基盤・ネットワーク基盤の基盤統制技術	サイバー攻撃の状況、システムの運用情報及び各種事態の状況等に応じて動的に環境を構成するシステム基盤及びネットワーク基盤の制御等を行う統制技術。	各種事態に応じたシステムの重要度の動的な変化に対応する技術。 サイバー攻撃や物理的攻撃等により複数拠点やネットワークが被害を受けた場合においても対応可能な技術。	
		統制機能抗たん性技術	サイバー攻撃発生時において、システム基盤及びネットワーク基盤の統制機能を維持する技術。	サイバー攻撃や物理的攻撃等により複数拠点やネットワークが被害を受けた場合においても対応可能な技術。	

取り組むべき主な技術課題（サイバー防衛）③

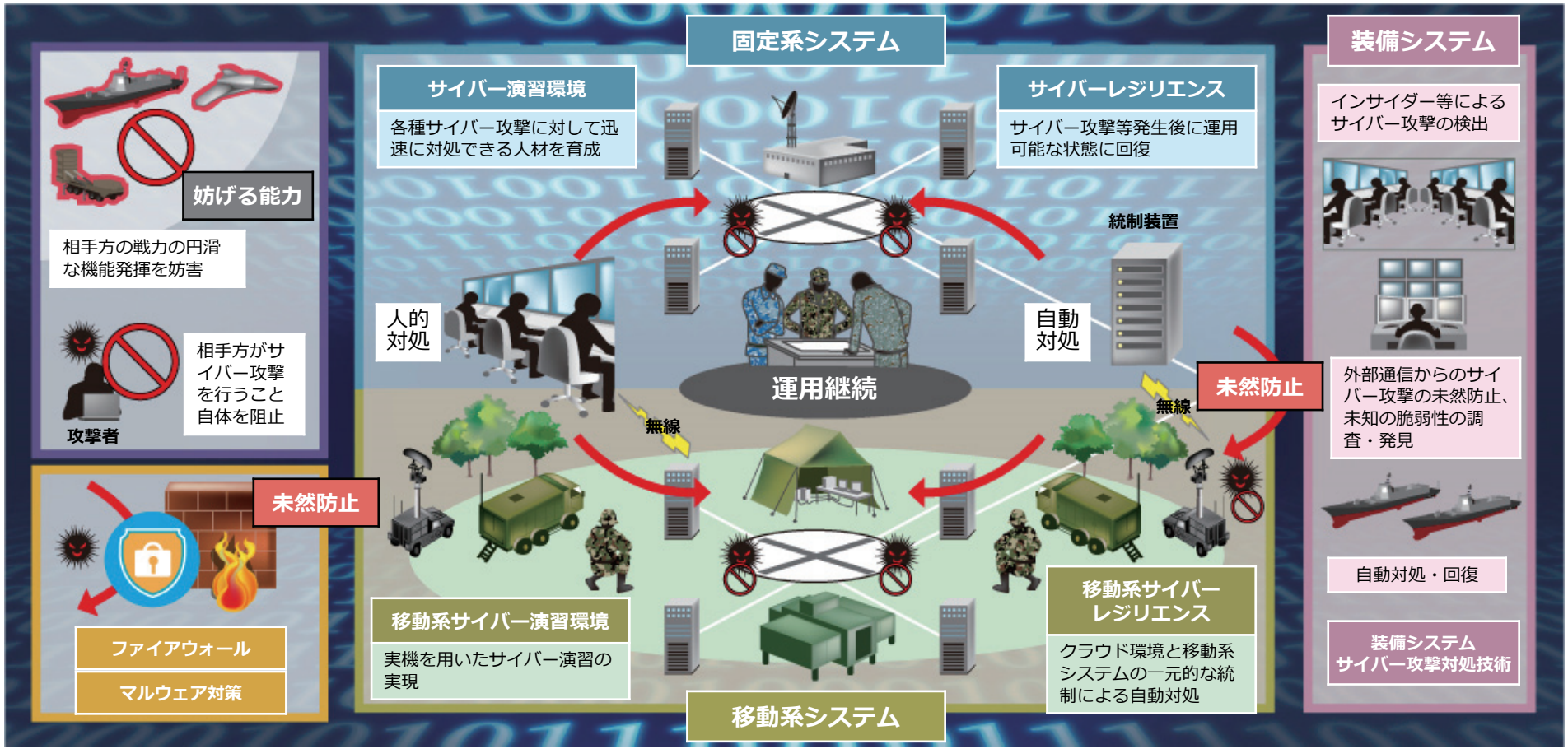
赤： 主として防衛省が行うサイバー関連研究により確立する技術
青： 防衛省が行うサイバー以外の研究により確立する技術（他の研究開発成果を活用できる）
灰色： 他機関との共同研究等により獲得する技術
水色： 民生分野における進展を待つ技術

項目	主要構成技術		技術の概要	技術的課題	期待できる効果
第3分類	移動系サイバーレジリエンス技術	移動系システム 情報管理技術	制約のあるネットワークでサイバー攻撃、情報、重要システム運用状況、通信経路情報等の管理を一元的に行う技術	各種事態に応じたシステムの重要度の動的な変化に対応する技術 サイバー攻撃や物理的攻撃等により複数拠点やネットワークが被害を受けた場合においても対応可能な技術	蓄積されたログの自動解析等により、サイバー攻撃の兆候を早期検出 ・攻撃と被害発生を早期に検出 ・被害拡大防止・対処の自動化 ・被害発生時における、重要システムの運用継続可能
		移動系システム 基盤統制技術	制約のあるネットワークでサイバー攻撃の拡散防止と重要システムの運用継続ため、移動系システム環境を構成するシステム基盤及びネットワーク基盤等の統制を一元的に行う技術	各種事態に応じたシステムの重要度の動的な変化に対応する技術 サイバー攻撃や物理的攻撃等により複数拠点やネットワークが被害を受けた場合においても対応可能な技術	
		移動系システム 統制機能抗たん性技術	制約のあるネットワークでサイバー攻撃発生時等における移動系システム環境を構成するシステム基盤 及びネットワーク基盤等の基盤統制機能を維持する技術	サイバー攻撃や物理的攻撃等により複数拠点やネットワークが被害を受けた場合においても対応可能な技術	
	装備システムサイバーレジリエンス技術		戦闘指揮システム内部で発生したサイバー攻撃を検知し、システムの運用状況、リソース使用可能状況等からシステム機能の運用継続を行う技術	装備システムの性能への影響を局限化しつつ運用継続を可能にする技術	

サイバー防衛機能コンセプト図

サイバー防衛を行うため、未然防止対策を行うとともに、サイバー攻撃を受けた後の運用継続対策を人と自動対処の両面で対応し、システムの抗たん性を向上させる。

- 未然防止対策として、マルウェア対策、ファイアウォール、耐タンパー等の民生技術を最大限活用する。また、有事において、相手方の戦力の円滑な機能発揮の妨害、サイバー攻撃の阻止のため、妨げる能力を獲得する。
- 人的対処で行う運用継続対策として、サイバー演習環境構築技術により、サイバー防衛の人材の能力向上に対応する環境を構築する。
- 自動対処を行う運用継続対策として、サイバーレジリエンス技術により、防衛省・自衛隊が運用する通信ネットワーク・システムにサイバー攻撃を受けた後に自衛隊の運用に即した形で自動対処を行う。



研究開発ロードマップ

	2019～2023	2024～2028	2029～2038
人的対処で行う運用継続対策	移動系サイバー演習環境構築技術	 移動系サイバー演習環境構築技術	実戦的なサイバー訓練環境の整備
自動対処を行う運用継続対策	サイバーレジリエンス技術 移動系サイバーレジリエンス技術	 サイバーレジリエンス統制装置	 移動系サイバーレジリエンス統制装置 運用可能な状態に自動回復する技術の獲得
未然防止対策	装備システムサイバー攻撃対処技術 耐タンパー技術 サプライチェーン・インテグリティ技術 マルウェア対策・ファイアウォール技術 脆弱性調査技術		共同研究の成果及び最新民生技術の取込による未然防止対策の充実・強化
“妨げる能力”に資する技術	“妨げる能力”に資する技術		

主として研究開発により獲得
最新民生技術の取込により獲得

注1　具体的な研究開発事業の実施に当たっては、運用面、技術面、コスト面から検討を十分に行う。
注2　実現が考えられる将来装備品のイメージを示すものであり、開発予定を示すものではない。
注3　線の終端は一例に過ぎず、迅速な研究開発の考え方に鑑み、技術の早期獲得に努める。

おわりに

主な研究開発の進め方と効果

- 防衛省・自衛隊にとっても、サイバー空間の安定的な利用が必要不可欠となっており、システムの特性上、長期間停止させられないため、未然防止対策と運用継続対策を両立させる必要がある。
- 未然防止対策のうち、民生分野との共通技術については、先進的な民生技術の積極的な活用により必要な技術を獲得する。一方、未然防止対策のうち、市場からの調達が困難な装備システムサイバー攻撃対処技術、脆弱性調査技術及び妨げる能力に資する技術や、運用継続対策については、防衛省・自衛隊に固有の要求があるため、研究開発を通じ技術を戦略的に獲得する。
- 人工知能、量子コンピュータ・センシング・通信といった量子技術等の将来のゲーム・チェンジャーとなりうる技術は、ボーダレス化・デュアルユース化が進展し、特に民生分野において進展が速いことから、国内外の技術の進展に合わせて、継続的な技術向上及び最先端技術の反映に努める。

国内外のルールの動向を注視

- サイバー攻撃事案への国際法の適用に関して、明確なルールは存在しない。サイバー空間に関する定義も各国で異なる。サイバー攻撃と自衛権の関係については、これまで国際的な場において様々な議論が行われてきた。
- これまでのところ、サイバー攻撃のみをもって「武力攻撃」に該当するか否かについては、国際的にも様々な議論が行われている段階。政府としては、どのようなサイバー攻撃であれば、それのみでも「武力攻撃」と評価できるかについて、今後とも、サイバー攻撃をめぐる情勢や国際的な議論を踏まえつつ、検討を進めていく考え。
- 組織としての対応方針、法的認識を整備する上で、国内外のルールの動向を継続的に注視する必要がある。
- 上記を踏まえたうえで、研究開発を進めていく。

未然防止対策と運用継続対策の両立

- 未然防止対策においては、最新の民間技術を効率よく取り込むことが必要
- 人的対処で行う運用継続対策においては、サイバー対策要員の能力向上を行う必要
- 自動対処を行う運用継続対策においても、サイバー攻撃の被害拡大防止と運用継続の確保を迅速に行う必要

▶ 未然防止対策と運用継続対策を両立させ、システムの抗たん性を向上

参 考

サイバー空間における
これまでの取組及び国内外の動向

防衛省におけるこれまでの取組

第1分類（未然防止対策）

- 平成19年度以降、暗号モジュール実装技術及び耐タンパー暗号技術に関する研究を行っている。

第2分類（人的対処で行う運用継続対策）

- 平成25年度～29年度にサイバー演習環境構築技術の研究を実施。防衛省・自衛隊のシステムを模擬した環境上で、隊員のレベルに合わせた効果的なサイバー防衛の演習が実施可能な技術を実現し、その成果を統幕の実戦的サイバー演習実施体制の整備に反映。

サイバー演習構築技術の研究試作

- 平成30年度から、狭帯域な回線環境下での状況付与やモニタリング、民生品ではない GOTS （ Government Off The Shelf）等で構成された移動系システムにおけるサイバー演習環境構築技術について研究中。

第3分類（自動対処で行う運用継続対策）

- 平成26年度～28年度でネットワークサイバー攻撃対処実験装置の研究を実施。サイバー攻撃発生時等において、防衛省・自衛隊のネットワークの安定的・効果的利用を維持し、任務を遂行するために、重要通信の経路確保と被害拡大防止について研究を行った。
- 平成29年度から、システム基盤・ネットワーク基盤が被害を受けたとしても、残された基盤を最大限活用し、その時々において重要となるシステムの運用を継続するためのサイバーレジリエンス技術について研究中

- ✓ 第1分類については、一部の要素技術に関する研究の実績あり。
- ✓ 第2分類については、固定系システムにおける演習環境構築技術の研究実績あり。移動系システムについて研究中。
- ✓ 第3分類については、固定システムにおけるサイバーレジリエンス技術に関する研究の実績あり。

国内外の技術動向

第1分類（未然防止対策）

- 国内では、Webのシングル・サインオンなど従来のアクセス制御管理に加えて、さらに一歩進んだ統合認証管理、統合アクセス制御、管理、監査レポート機能、高信頼性構成といったものが登場している。
- 自由裁量アクセス制御機能を持ったOS製品や、ファイアウォール製品が民間企業から発売され、普及している。
- 国内では、民間セキュリティベンダーが、サイバー攻撃による被害を最小化し、可能な場合には、攻撃者を特定できるよう貢献するという役割を担っている。

第2分類（人的対処で行う運用継続対策）

- 米国においては、2009年から、サイバー戦の作戦試験を行うため国家仮想領域 (NCR: National Cyber Range)が進められていたが、テスト期間を終えて、国防省はサイバー戦のテストや演習を本格的に実施可能になった。
- 欧州では、2016年、ENISA（European Network and Information Security Agency; 欧州ネットワーク情報セキュリティ庁）が、欧州サイバー演習のためにCyber Europe 2016を立ち上げた。
- ロシアの国営通信社の報道によれば、ロシア軍はサイバー戦部隊を創設する検討を進めている模様である。

第3分類（自動対処で行う運用継続対策）

- 米軍では，2010年から ”Department of Defense (DoD) Information Technology (IT) Enterprise Strategy and Roadmap” により、それまで進めていた最適化を発展させ、”Department of Defense Chief Information Officer, Cloud Computing Strategy” 等のイニシアチブに従いクラウド技術をベースとした大規模なシステム整理統合が進められている。

- ✓ 第1分類については、国内外において、民間企業及び民間セキュリティーベンダーが、製品及び技術を保有。
- ✓ 第2分類については、各国ともサイバー演習環境構築及び組織の編成に取り組んでいる。
- ✓ 第3分類については、各国とも研究に取り組んでいると思われるが、一部を除き詳細は不明である。