

防衛省・自衛隊における サイバー攻撃対処について

平成22年5月
防 衛 省

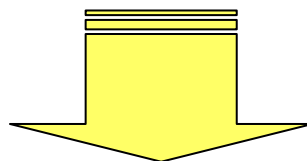
サイバー空間を巡る問題

近年、地理的空間における事象だけでなく、サイバー攻撃などサイバー空間における様々な事象が国の安全や国民の生活に大きな影響を及ぼすようになってきている。

例えば、エストニアでは2007年4月、政府・報道機関や主要な金融機関が大規模なサイバー攻撃を受け、国民生活に大きな影響が生じた。

このような状況を踏まえ、現在、米国をはじめ、各国がサイバー空間における脅威を真剣に受けとめ、サイバー空間の安全を確保するための取組みに力を入れている。

例えば、米国では、2009年5月、サイバー政策を見直し、大統領府に政府や民間機関を含めたサイバー施策の総合調整を行うサイバーセキュリティ調整官を設置することを決定した(同年12月任命)。

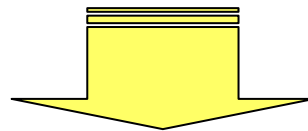


我が国においても、国民生活における情報通信の重要性は高まりつつあり、サイバー空間の安全を確保するため、国全体として取り組む必要性が高まっている。

各国の軍においても、サイバー攻撃等の脅威について認識が深まっている。例えば、米軍においては、2009年6月、ゲーツ国防長官がサイバーコマンドの設置を命令し、米軍のネットワーク防護等を行うほか、国土安全保障省への技術協力も実施する予定。

更に、2010年2月に、米国防省により公表された「4年毎の国防計画の見直し(2010QDR)」において、近年のサイバー攻撃が、サイバー空間も含まれる国際公共財(グローバル・コモンス)の安定に対する脅威となって拡大しているとの認識を示し、以下の方針を示した。

- ・ “サイバー空間における効果的な作戦”のため、サイバー空間における脅威に対抗するサイバー対処能力の強化が必要。
- ・ サイバーに関する専門知識・技術や意識の向上、サイバー作戦の指揮命令機能の集約化、他機関や外国政府とのパートナーシップの強化を促進する必要。



防衛省・自衛隊も、自らの活動が情報システム・通信ネットワークに大きく依存しており、各国と同様にサイバー空間に関する脅威にさらされているため、必要な対処を講じることが重要。

また、政府の一員として、自らの情報システムを防護することに加え、内閣官房情報セキュリティセンター(NISC)の取組みに協力するなど、国民の安全を確保するために必要な努力を続けていく必要がある。

1. 通信ネットワーク・情報システムについて

通信ネットワークの概況

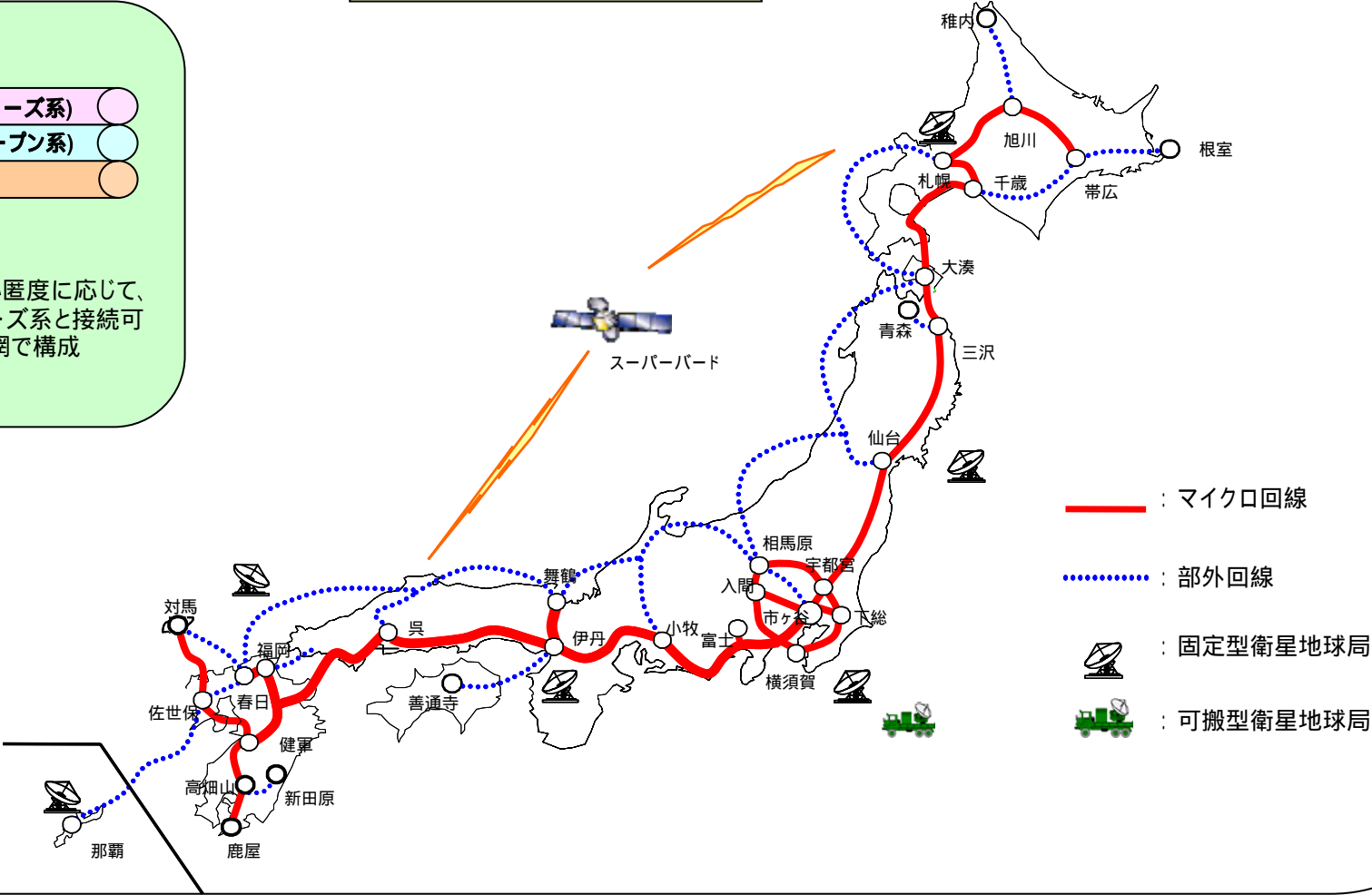
陸海空自衛隊の主要な駐屯地、基地間の通信は、全自衛隊の共通ネットワークとして整備している防衛情報通信基盤(DII: Defense Information Infrastructure)により実施。DIIは、マイクロ回線、通信事業者から借り上げている部外回線と衛星回線を利用し、データ通信網と音声通信網から構成されている。

防衛情報通信基盤(DII)

各通信回線

- データ通信網(クローズ系)
- データ通信網(オープン系)
- 音声通信網

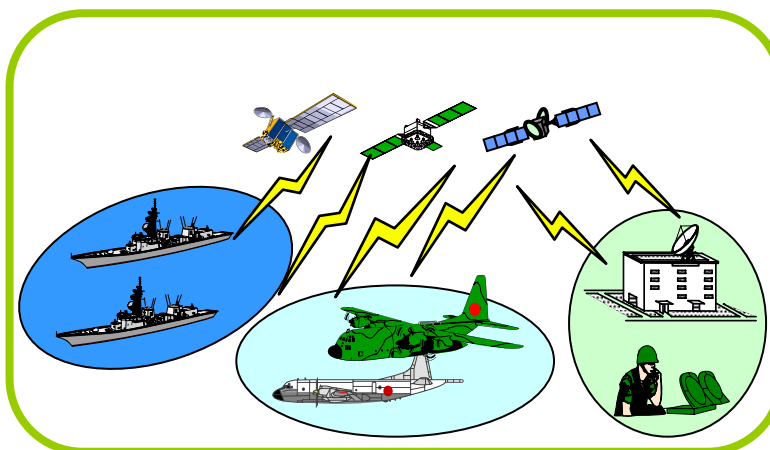
データ通信網は、データの秘匿度に応じて、外部との接続を有しないクローズ系と接続可能なオープン系の2つの通信網で構成



通信ネットワークの概況

各自衛隊において、駐屯地・基地内の通信ネットワーク(駐屯地電話網や駐屯地LAN等)を整備するとともに、展開する陸上部隊、艦艇、航空機のための通信ネットワークを無線や衛星回線を利用して構成している。

自衛隊における衛星通信の利用のイメージ



- ・ 陸海空を問わず、地上のインフラが整備されていない場所で活動する自衛隊にとっては、衛星通信の活用が重要。
- ・ 衛星通信については、高速・大容量化への対応が重要となってきている。

中央指揮システム (CCS: Central Command System)

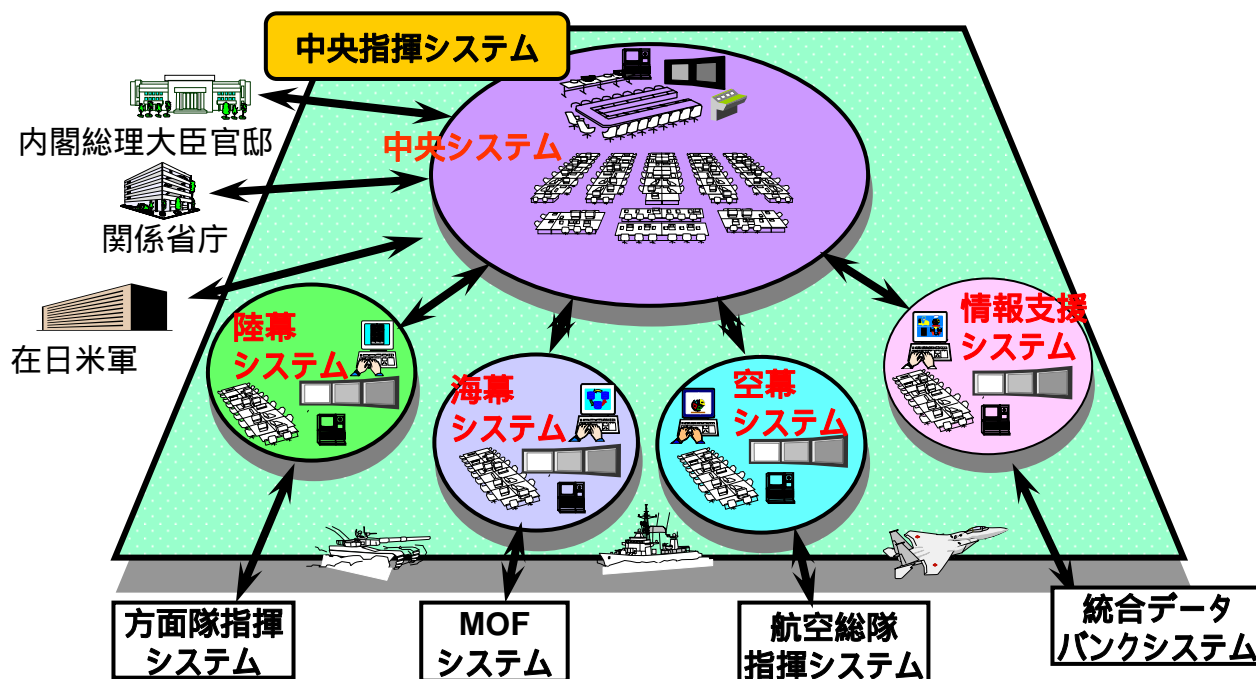
防衛大臣が指揮・統制を行うためのシステム。中央システム、陸・海・空幕システム、情報支援システムの5つのシステムからなる統合システムであり、官邸、関係省庁等と連携している。本システムの主要な機能は以下のとおり。

- ・ 部隊の展開状況等を把握する機能
- ・ テレビ会議またはチャットを利用したリアルタイムな相互調整機能
- ・ 各種計画、命令及び報告資料の作成機能

陸海空自衛隊の主要な指揮システム

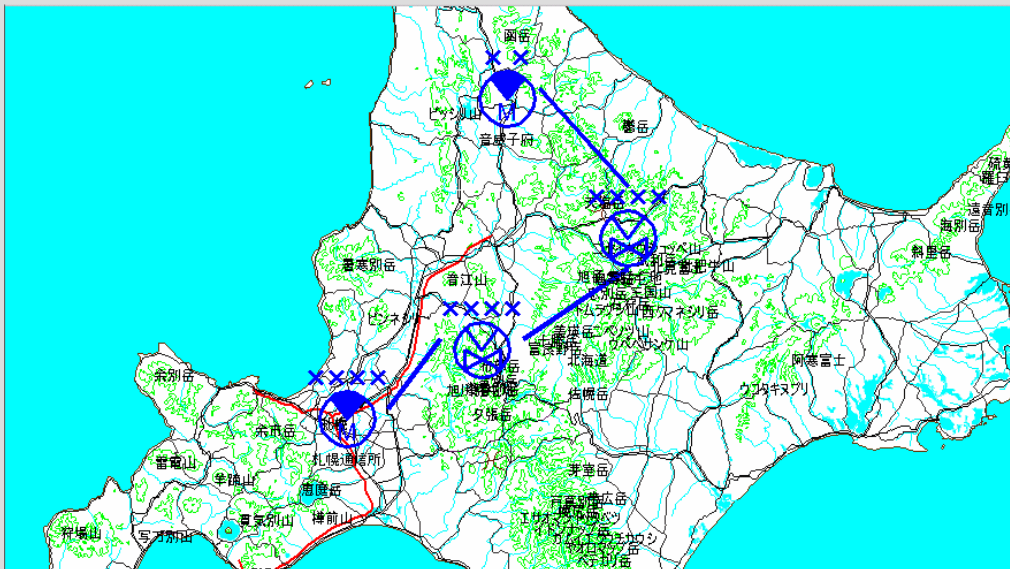
陸海空自衛隊の指揮官が作戦指揮を行うため、陸上自衛隊においては方面隊指揮システム、海上自衛隊においてはMOFシステム(海上作戦部隊指揮統制支援システム)、航空自衛隊においては航空総隊指揮システムを整備。

(注) MOFシステム: Maritime Operation Force Systemの略

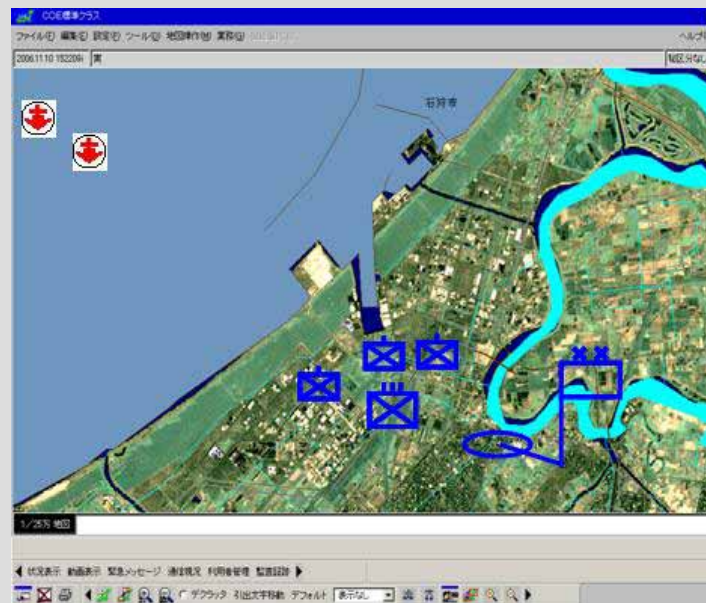


中央指揮システムの機能

中央指揮システム



1/100万 地図 現況:骨幹通信組織図 エリア指定検索



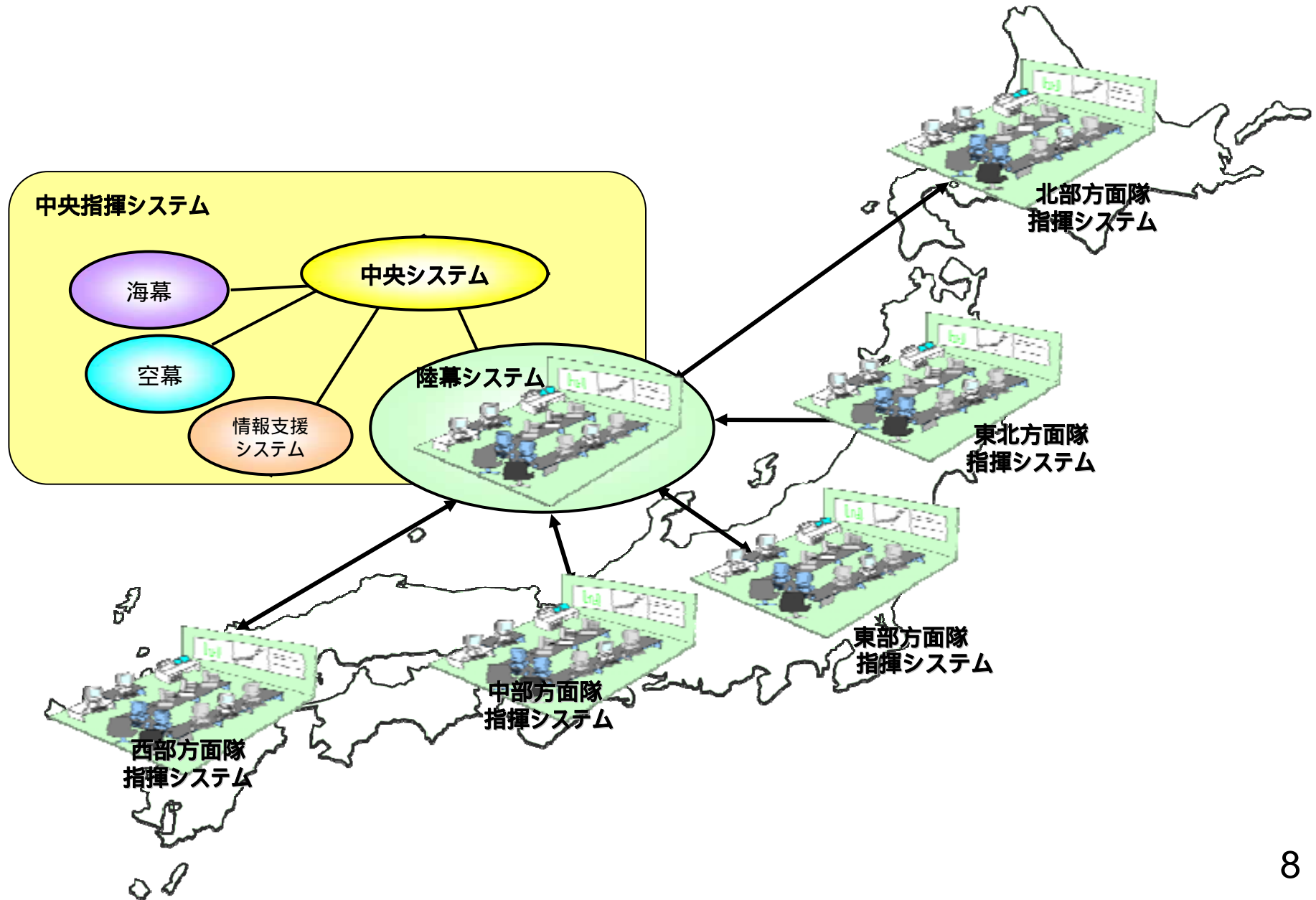
コンピュータ・システム共通運用基盤(COE)

中央指揮システム等の指揮システムでは、上記のような各種の地図ソフトウェア等を使用する。このように多用されるソフトウェアをシステム毎に開発すると無駄なコストが生じるため、どのシステムも単一の地図ソフト等を使用することで効率化を実現している。これらの共通に利用されるソフトウェアをCOEという。

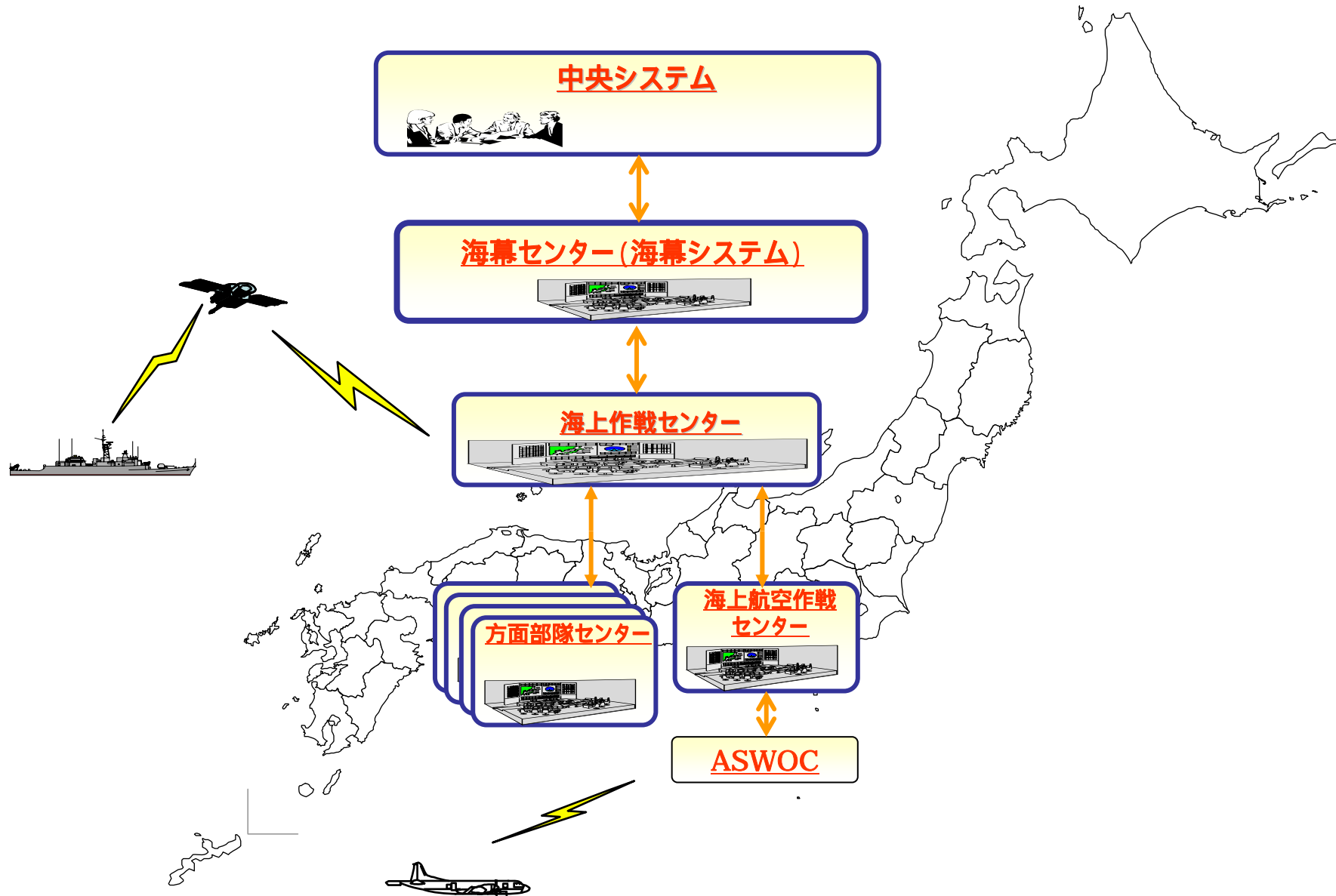
(COE :Common Operating Environment)



陸上自衛隊の指揮システムの概要

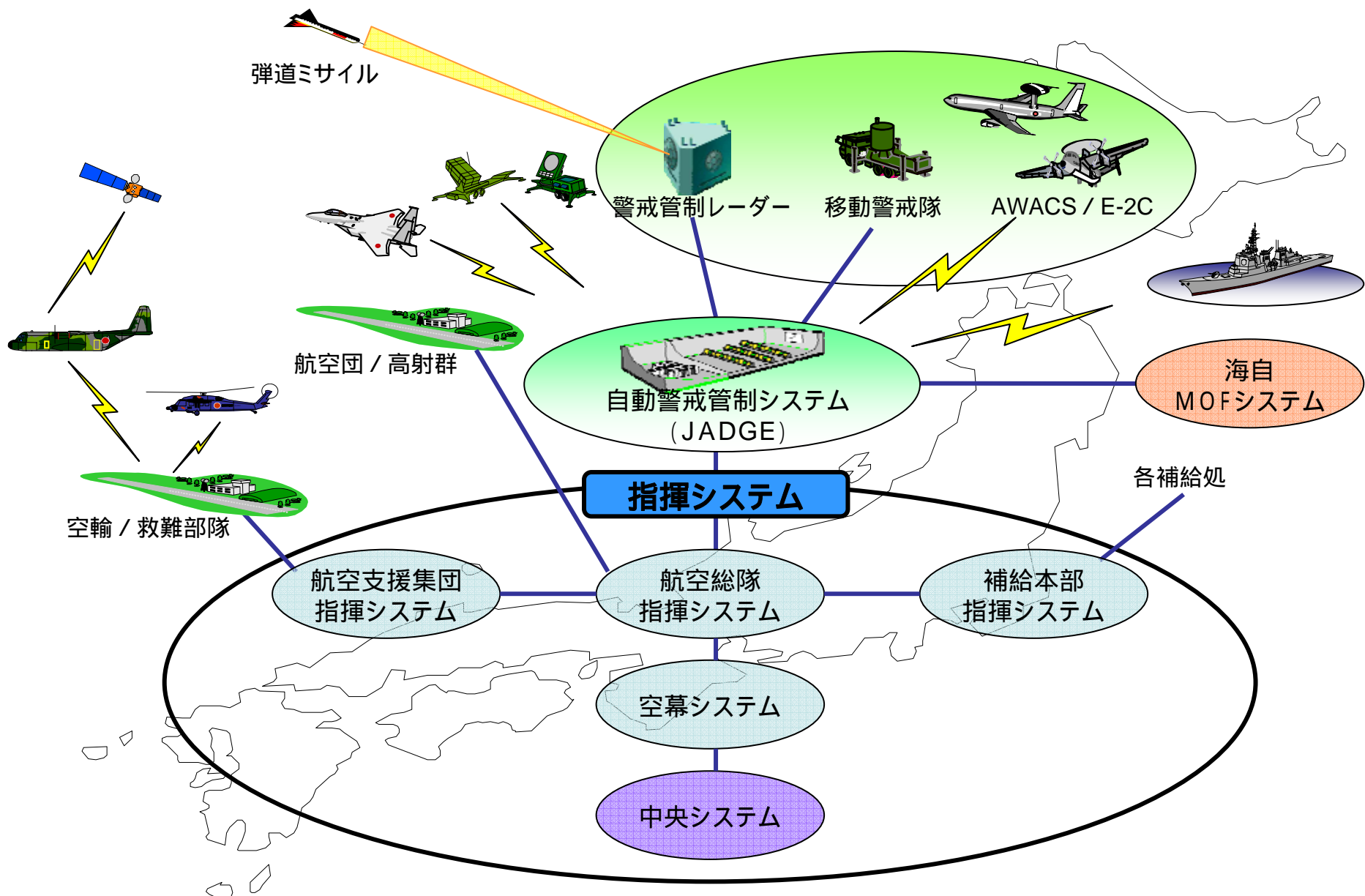


海上自衛隊の指揮システムの概要



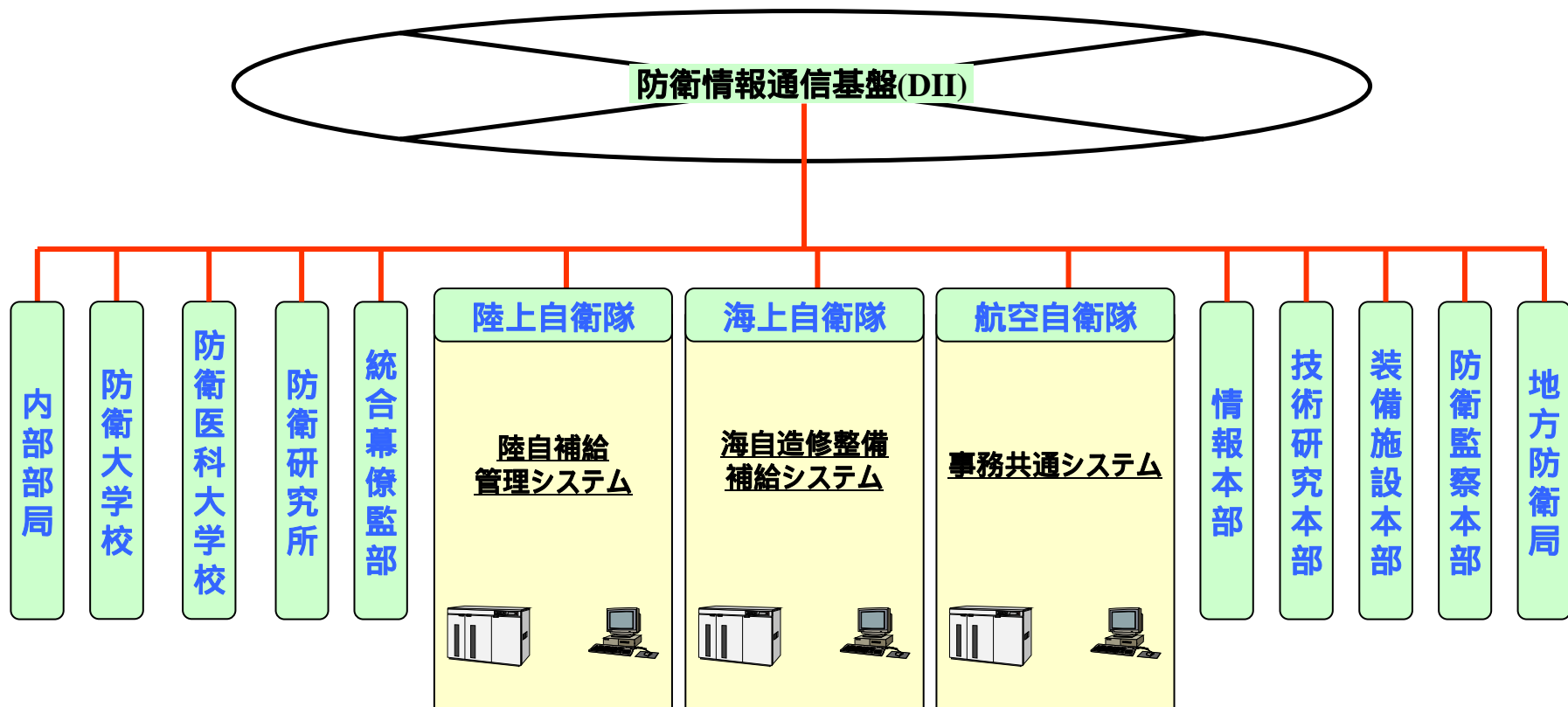
ASWOC (Anti-submarine Warfare Operation Center : 対潜戦作戦センター)
P-3Cの対潜戦作戦用の支援センター

航空自衛隊の指揮システムの概要



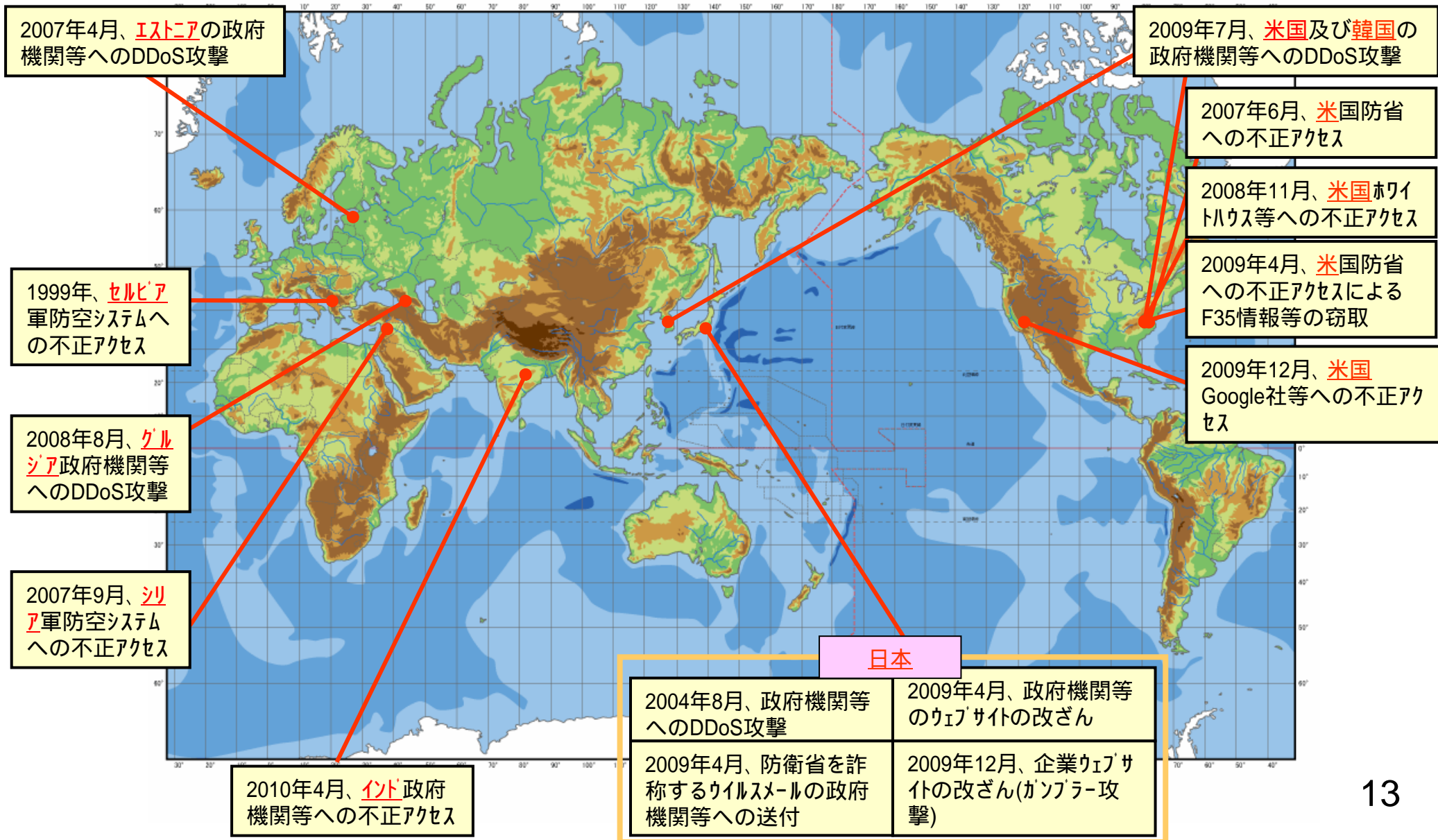
業務系システム

- ・ 各自衛隊や機関等に整備されている補給、整備、人事、一般事務などのための各種システム。
- ・ このうち、人事や給与など各府省が共通のシステムを使用することとされたものについては、順次導入を進めている。
- ・ 年間運用経費が1億円以上のシステムについては、最適化計画を作成して効率的に整備。
(注)最適化計画:業務の見直しやバラバラに使用されている情報システムの一元化などを進める計画



2. サイバー攻撃の脅威

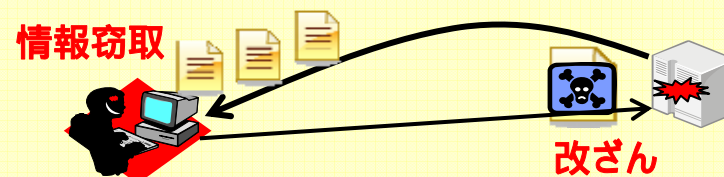
最近のサイバー攻撃事例(報道ベース)



主なサイバー攻撃の手法

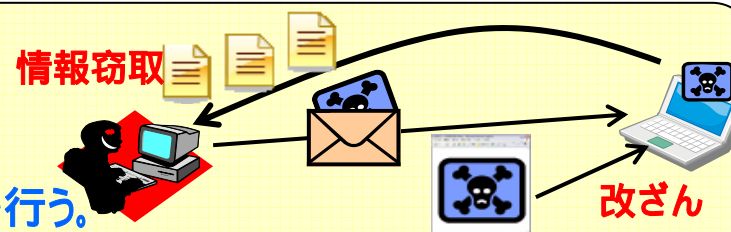
・不正アクセス

情報システムに不正にアクセスし、機能不全化、情報改ざんや窃取を行う。



・ウイルス

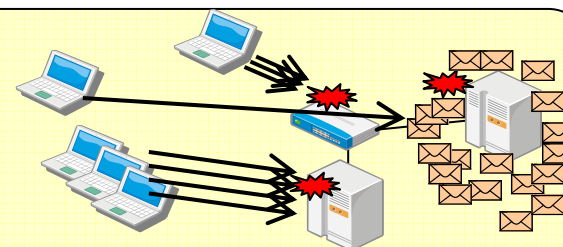
メールにウイルスを添付したり、ウェブサイトにウイルスを仕込み、閲覧時に取り込まれるように細工して、情報システムにウイルスを送り込み、機能不全化、情報改ざんや窃取を行う。



・DDoS

大量のデータを情報システムに送信することにより、情報システムの機能を停止させる。

(DDoS (Distributed Denial of Service) : 分散サービス妨害)



・インサイダー

情報システムにアクセスする権限を有する者等が、その権限を不正に利用し機能不全化、情報改ざんや窃取を行う。



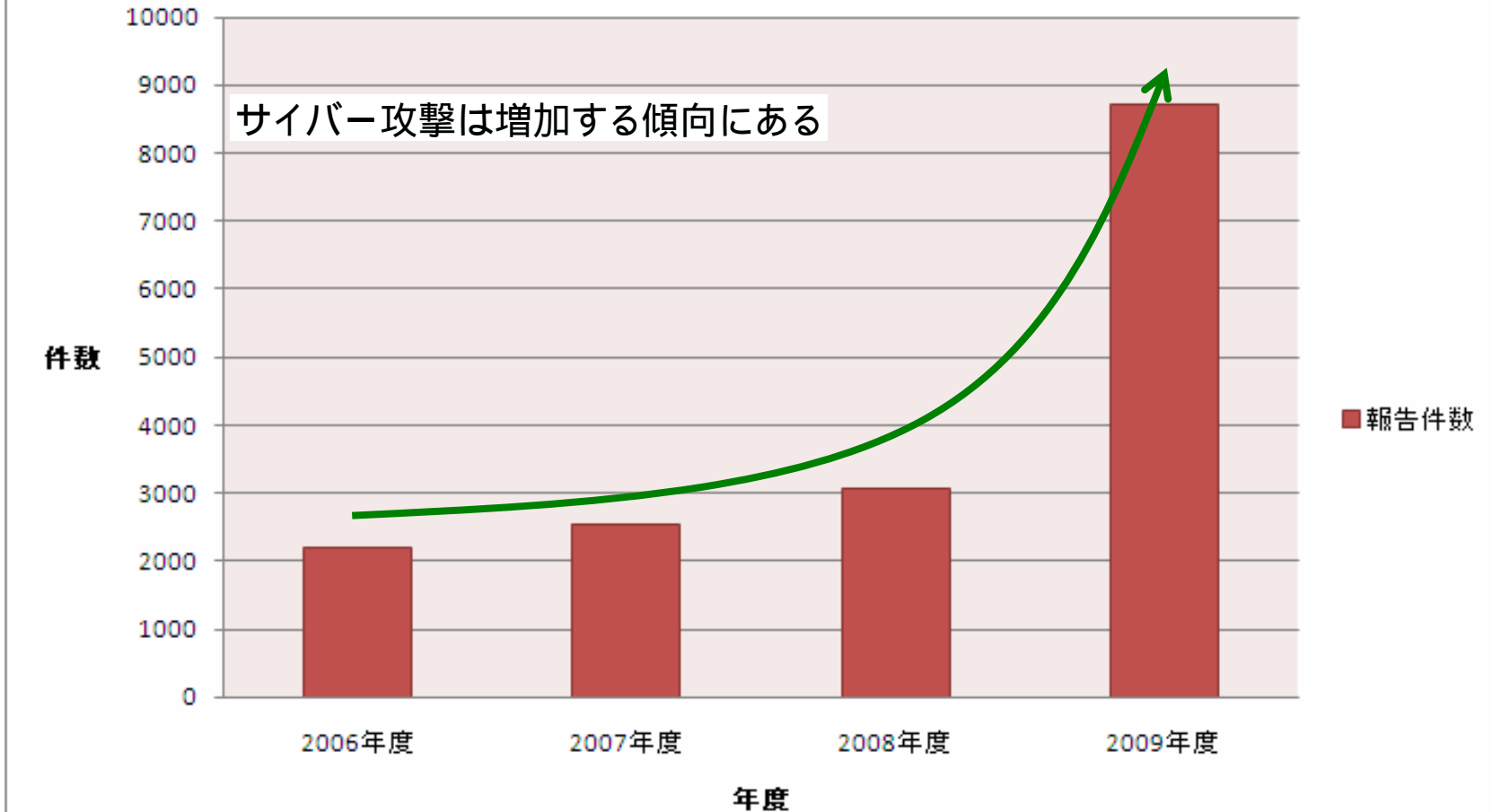
・可搬記憶媒体

ウイルス入り可搬記憶媒体 (USBメモリ等) を職員に使用させる等の手段により、ウイルスを送り込む。



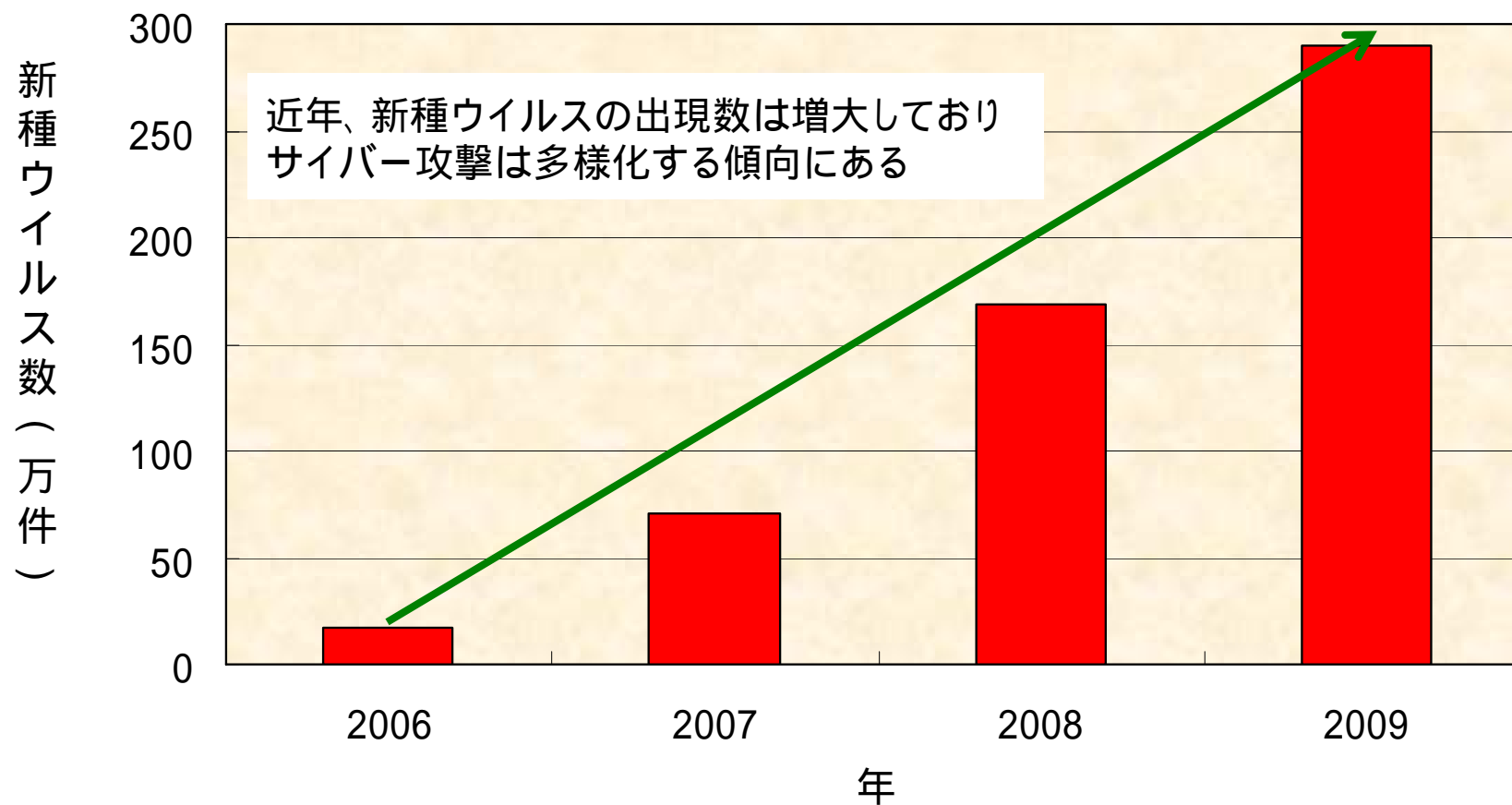
増加するサイバー攻撃の件数

JPCERT/CC インシデント報告数の推移



引用：一般社団法人 JPCERTコーディネーションセンター
インシデントハンドリング業務報告
JPCERT/CCへのインシデント報告件数推移
(経済産業省からの委託により実施)
<http://www.jpccert.or.jp/ir/report.html>

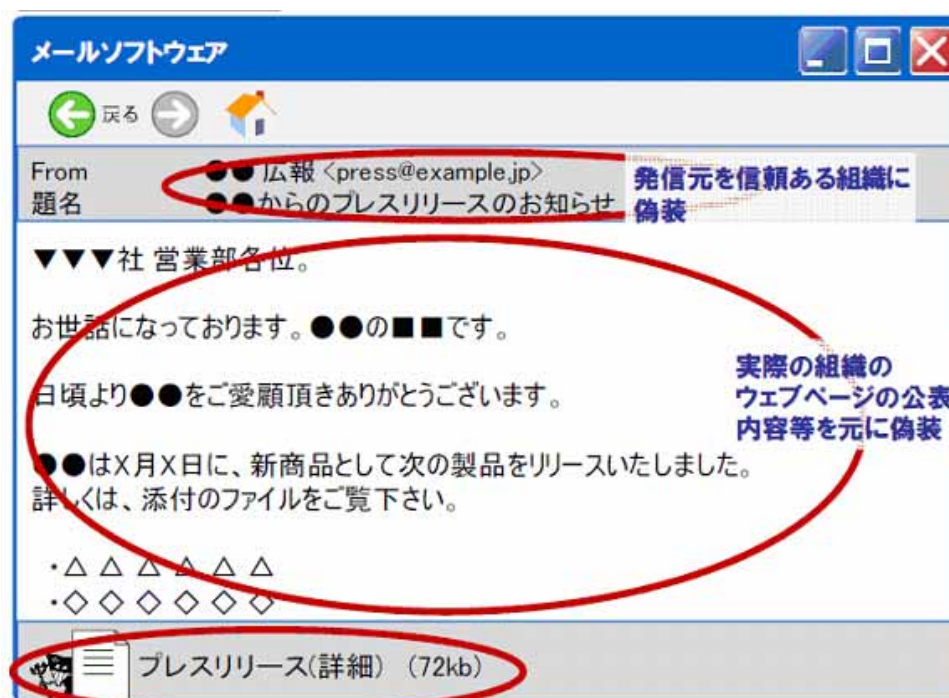
新種ウイルス出現数の推移



引用 : Symantec Corporation
Symantec Global Internet Security Threat Report Trends for 2009

サイバー攻撃の巧妙化

- ・ 人間の心理・行動の隙を突くことで情報を不正に取得する「ソーシャル・エンジニアリング」の手口を利用し、ソフトウェアの脆弱性を利用したウイルスを配布するなど、攻撃手法が巧妙化。
- ・ 具体的には、信頼ある取引先や人物からのメールとして差出人を偽装し、メールの内容も信憑性の高い情報を記載するなどした、「なりすましメール」による被害が発生。

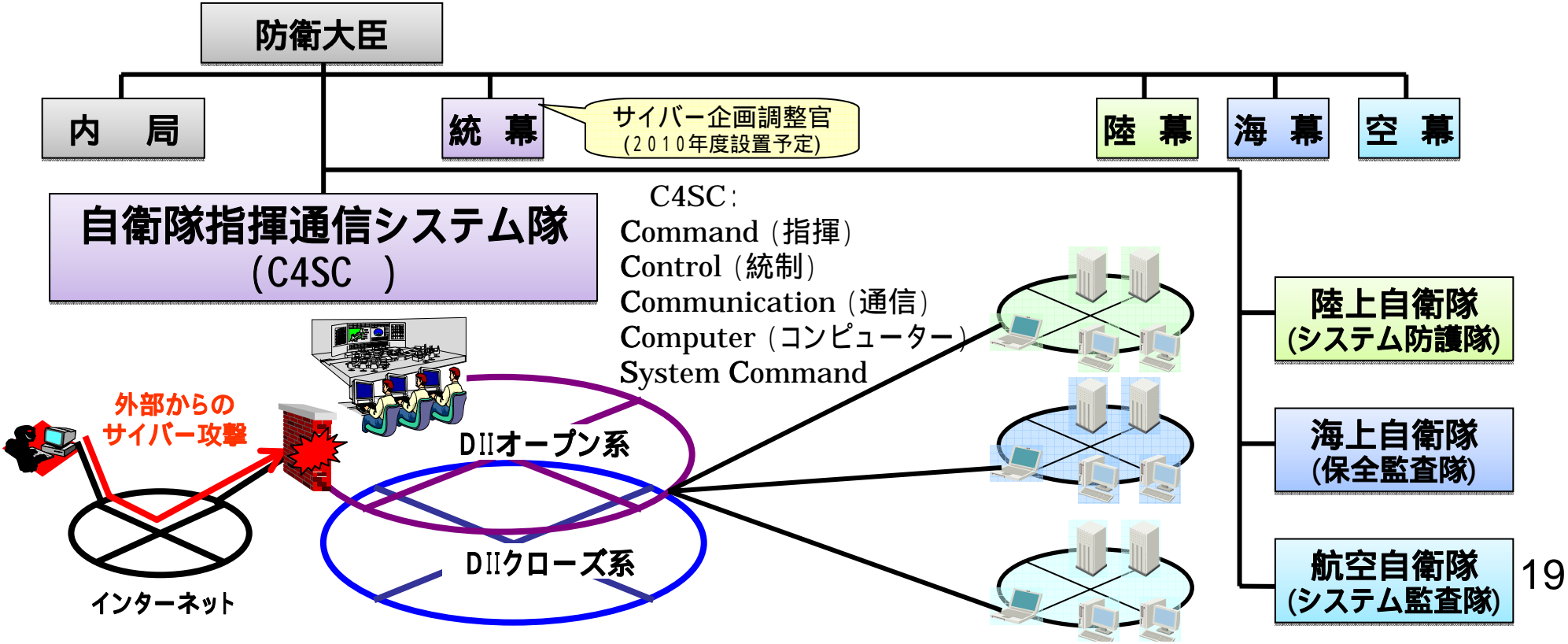


文章を開くと感染するウイルスを添付


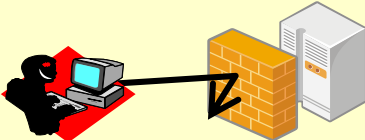




3. サイバー攻撃対処の現状

防衛省・自衛隊のサイバー攻撃対処の現状 ～ 態勢や規則の整備 ～

現 状	課 題 等
<ul style="list-style-type: none"> ・ DIIを24時間態勢で監視統制し、サイバー攻撃への対処等を実施する自衛隊指揮通信システム隊の整備 (2008年3月に陸海空3自衛隊の共同部隊として整備) 	<ul style="list-style-type: none"> ・ サイバー攻撃の多様化・巧妙化を踏まえ、サイバー攻撃対処部隊の機能強化について検討が必要
<ul style="list-style-type: none"> ・ 情報システムに求める機能要件やサイバー攻撃発生時の対処要領等を定めた規則の整備 	<ul style="list-style-type: none"> ・ 技術の進展に合わせて、規則の改正について継続的な検討が必要



防衛省・自衛隊のサイバー攻撃対処の現状
 ~ 安全性の向上を図るための措置 ~

現 状	課 題 等
<ul style="list-style-type: none"> データの秘匿度に応じて、外部との接続を有しないクローズ系と接続可能なオープン系を整備 	<ul style="list-style-type: none"> 技術水準の向上に合わせて、サイバー攻撃への対策について、継続的な充実・強化が必要
<ul style="list-style-type: none"> 情報システム・通信ネットワークへの侵入防止システム等の導入 	
<ul style="list-style-type: none"> DIIや各自衛隊への情報システムに対するウイルス対策ソフトの導入 	
<ul style="list-style-type: none"> 未知のウイルスを解析するサイバー防護分析装置等の防護システムの導入 	
<ul style="list-style-type: none"> サイバー空間の安全に関する情報収集や技術研究の実施 	<ul style="list-style-type: none"> サイバー攻撃の脅威の増大を踏まえ、情報収集の強化が必要
<ul style="list-style-type: none"> 一般職員に対する、サイバー攻撃に関する教育の実施 	<ul style="list-style-type: none"> サイバー攻撃について、一般職員に対して継続した教育を行い、より理解を深めることが必要

防衛省・自衛隊のサイバー攻撃対処の現状
 ~ 高度な知識・技能を有する人材の育成 ~

現 状	課 題 等
<p><u>国内外教育機関への留学等</u> 米国カーネギーメロン大学や国内の大学院に留学し、情報セキュリティに関する課程を受講</p> <ul style="list-style-type: none"> ・ カーネギーメロン大学 毎年度2～3名留学 ・ 国内大学院(情報セキュリティ大学院大学, 北陸先端技術大学院大学等) 毎年度1名留学 	<ul style="list-style-type: none"> ・ 多様化・巧妙化するサイバー攻撃に対応するための技術的対策等について十分に検討し、優秀な人材を確保することが必要。
<p><u>各自衛隊の術科学校等の部内組織における教育</u></p> <ul style="list-style-type: none"> ・ 陸上自衛隊(システム防護課程) ・ 海上自衛隊(情報セキュリティ課程) ・ 航空自衛隊(通信幹部課程) 	

防衛省・自衛隊のサイバー攻撃対処の現状
 ~ 関係各国・関係機関との情報共有の推進 ~

現 状	課 題 等
<p>関係機関との情報共有・協力の推進</p> <ul style="list-style-type: none"> ・ NISC等との情報共有 ・ NISCへのサイバー攻撃対処に知見を有する自衛官の派遣 	<ul style="list-style-type: none"> ・ NISCが進めている情報セキュリティ政策について、引き続き協力 ・ サイバー攻撃に関する対処のあり方や法的問題については、国際的にも議論が発展途上の段階であることから、各国防衛当局と協議を推進
<p>米国等との情報共有・協力の推進</p> <ul style="list-style-type: none"> ・ 2006年、防衛省と米国防省は、「情報保証とコンピューターネットワーク防御における協力に関する了解覚書」を締結し、サイバー攻撃時の対処能力向上を目的とした情報交換を実施 ・ また、IT政策についての情報交換を行うことを目的に、米国やシンガポールと定期協議を実施し、サイバー攻撃対処を含め幅広く議論 ・ 米軍との間でサイバー分野の共同訓練を実施 	