資料３

第18回重要インフラ専門委員会説明資料

防衛省におけるサイバー攻撃対処の取り組みと事案対処省庁としての役割の検討について

平成20年7月18日

防衛省運用企画局
情報通信・研究課情報保証室

省全体のサイバー攻撃対処態勢

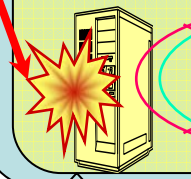
攻撃者
（多様なレベル：犯罪～国家レベル）

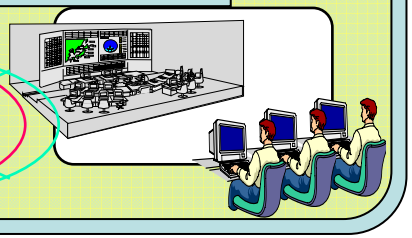
防衛省
事案対処統括者　ＩＴ担当防衛参事官
運用企画局 情報通信・研究課 情報保証室

省全体で連携した
迅速な対処

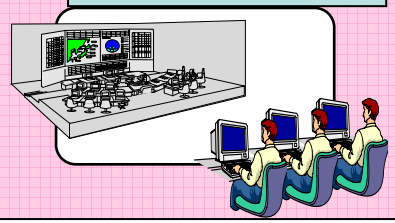
アラート情報等の
集約・共有

統合幕僚監部
２４時間態勢でネットワークを監視
対処部隊
自衛隊指揮通信システム隊
オープン系／クローズ系



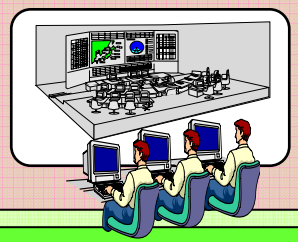


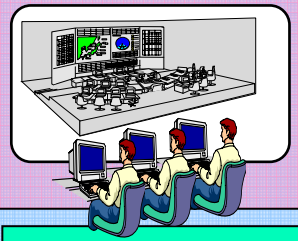
企画部署
指揮通信システム部

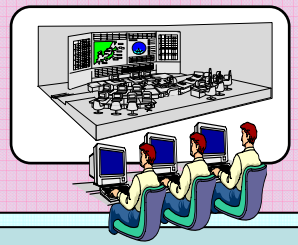


陸上自衛隊
海上自衛隊
航空自衛隊

陸上幕僚監部
海上幕僚監部
航空幕僚監部







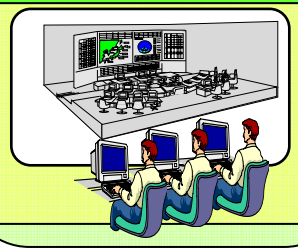
企画部署

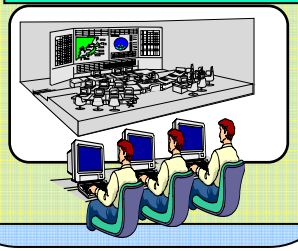
技術研究本部

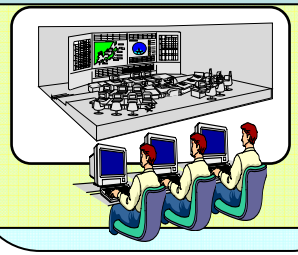
研究開発

陸自システム防護隊
海自保全監査隊
空自システム監査隊

対処部隊





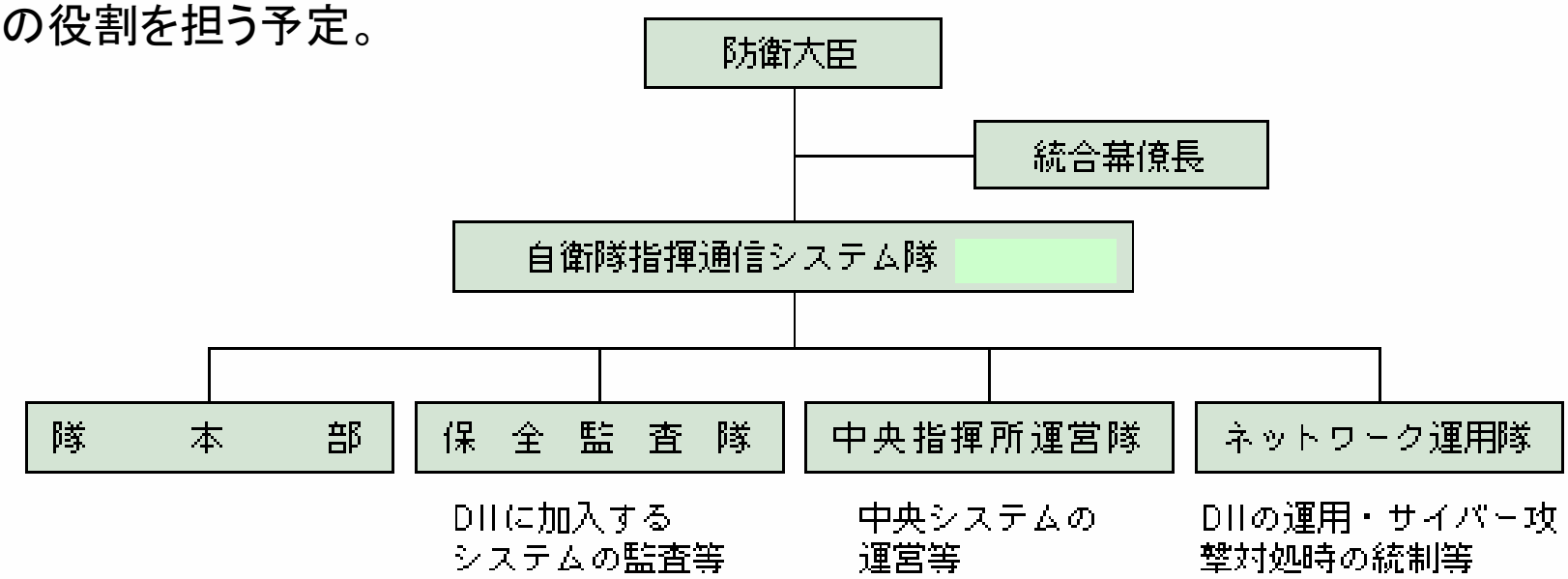


自衛隊指揮通信システム隊」の新編

○自衛隊の情報通信機能について、情報システムやネットワークの整備・維持管理などの静的な機能に加え、中央と現地部隊との迅速な連絡調整、広範な地域での部隊間の連絡調整など部隊運用に直結する動的な機能を担うため、平成20年3月26日に初の常設の統合部隊である「自衛隊指揮通信システム隊」を新編。

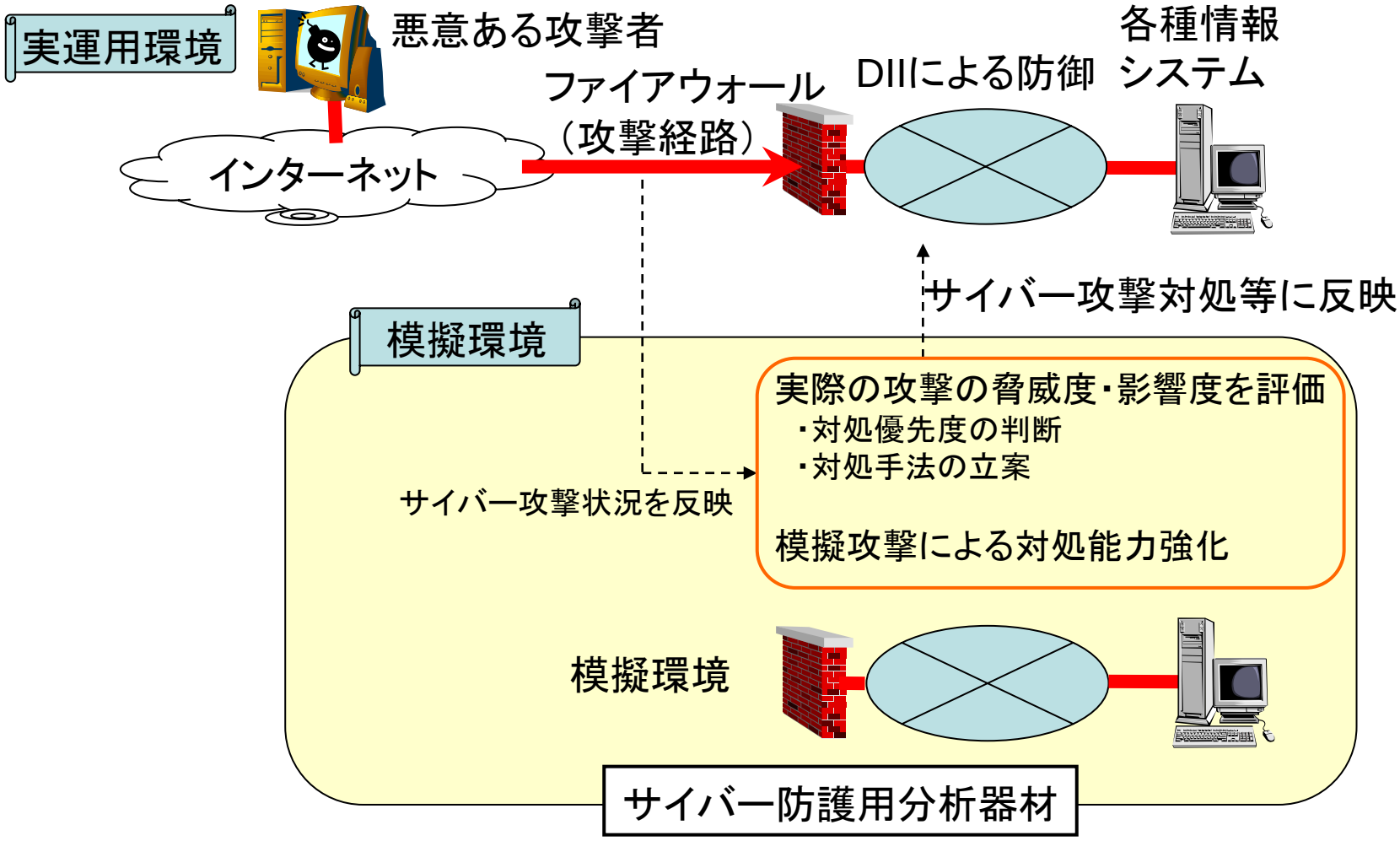
○　同隊では、自衛隊の指揮命令中枢である中央指揮所（CCP）および自衛隊の骨幹ネットワークである防衛情報通信基盤（DII）の維持管理機能・サイバー攻撃対処機能などを24時間態勢で実施。

○　今後、同隊において、陸海空毎に個別に存在する通信インフラの有機的組み合せによる通信系の臨機応変な構築や、サイバー攻撃発生時の適時適切な通信機能回復などの役割を担う予定。



防衛省における最新技術の研究

平成19年度から統幕において、部外からのなりすましメール等の未知のサイバー攻撃の脅威・影響度を分析し、迅速な対処優先度の判断や対処手法の立案等に資するため、サイバー防護用分析器材を整備。



防衛省の役割の検討

防衛省が有する能力

○ 未知のサイバー攻撃に対する静的・動的な解析・分析能力

○ サイバー攻撃によるIT障害発生時の障害復旧手順等の情報提供

防衛省の役割の検討

防衛省として、重要インフラの障害回避・復旧等にどのように貢献可能か　→　**分野的横断演習等の機会を通じた検討が必要**

例）防衛省への未知のサイバー攻撃の解析・分析結果及び障害復旧対処手順等をNISCを通じて情報提供等