防衛的観点からのサイバー攻撃対処能力の強化

Enhancement of Counter Cyber-attack Capabilities from Viewpoint of National Defense

笠井 大騎 Kasai Daiki
田島 萌絵 Tajima Moe
齋藤 嘉幸 Saito Yoshiyuki
谷川 嘉伸 Tanigawa Yoshinobu

昨今，サイバー攻撃の軍事利用，防衛産業や重要インフラに対するサイバー攻撃が増加し，防衛的観点からのサイバー攻撃対処能力の強化が急務となっている。
日立グループは，日立製作所ディフェンスシステム社が保有する，防衛分野における指揮統制システムの構築などに関わるノウハウを活用し，防衛的観点からのサイバー攻撃対処能力のあり方について検討している。
今後は検討結果に基づき，サイバー攻撃対処能力の向上に資するソリューションのさらなる強化を図り，サイバー空間を含む安全・安心な社会の実現に貢献していく。

1. はじめに

2011年7月，米国国防総省はサイバー戦に関する初めての戦略となる「Department of Defense Strategy for Operating in Cyberspace（サイバー空間作戦戦略）[1)]」を発表した。この戦略が発表された背景には，政府や重要インフラなどに対するサイバー攻撃が相次いで発生し，政治的あるいは軍事的な目的を達成させるための手段としてサイバー攻撃が利用されるケースが増加している状況がある。

この戦略では，サイバー空間を陸，海，空，宇宙に続く「第5の作戦領域」として扱うという考え方をはじめ，組織，装備および関連省庁ならびに企業などとの関係を強化するなどの五つの方針が示され，米国のサイバー戦に対する強固な姿勢が確認できる。

サイバー攻撃が軍事目的で利用された具体的な事例として，イスラエルからシリアに対する空爆作戦（2007年）が有名である[2)]。これは，イスラエルがシリアに対しサイバー攻撃を実施し，シリアの防空システムの探知能力を無力化させたうえで爆撃を行ったもので，サイバー攻撃が軍事目的で利用され，かつ，物理的な作戦と高度な連携を実施した例である。

また，最近では企業を標的としたサイバー攻撃が増加傾向にあり，2011年には，日本，イスラエル，インドおよび米国の防衛産業などを標的としたサイバー攻撃が発生した[3)]。

これらの事例は，従来のセキュリティリスクであるコンピュータウイルスの無差別拡散や，感染による情報流出事故などとは明らかに性質が異なる。明確な目的に基づき，高度な戦略と蓄積された技術により，サイバー攻撃が実行されている。

一方で，現代社会はIT（Information Technology）に大きく依存している。例えば，電力，ガス，水道，交通および通信などのいわゆる重要インフラは，ITによって支えられている。政府機関のインフラや防衛装備品も同様であり，近代化に伴ってITへの依存度が高まっている。したがって，サイバー攻撃が及ぼす影響は，サイバー空間だけに留まらず，現実社会に及ぶ。

このように，国家安全保障を脅かすリスクとしてサイバー攻撃が利用されている状況，すなわちサイバー戦が顕在化している状況を踏まえ，防衛的観点からのサイバー攻撃対処能力の強化が必要である。

ここでは，サイバー攻撃対処能力の強化のあり方，米国における政策や企業の対応，および日立グループの取り組みについて述べる。

2. サイバー攻撃対処能力の強化に関する検討

軍事分野において古くから用いられる理論として，米国空軍のジョン・ボイド大佐が提唱したOODAループがある。朝鮮戦争における空中戦で勝利を収めた経験を洞察した結果から提唱されたもので，指揮官のあるべき意思決定のプロセスとして理論化され，しばしばビジネスなどにおいても活用されている。

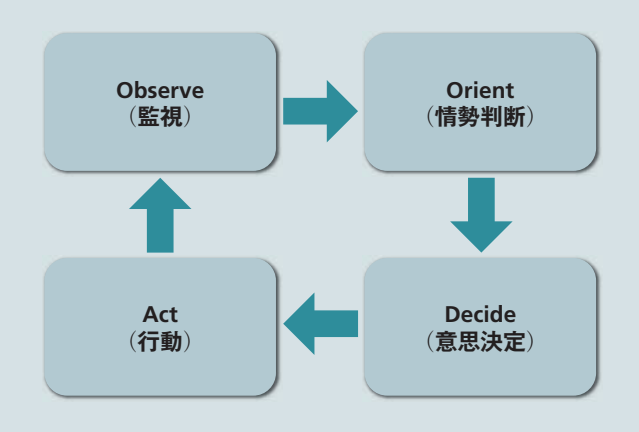


図1｜OODAループ
米国空軍のジョン・ボイド大佐によって提唱された意思決定理論であり，Observe（監視），Orient（情勢判断），Decide（意思決定），Act（行動）を繰り返すことにより，迅速かつ的確な意思決定を行うという考え方である。

OODAとは，Observe（監視），Orient（情勢判断），Decide（意思決定），Act（行動）の頭文字を取ったもので，これらを繰り返すことにより，迅速かつ的確な意思決定を行うという考え方である（**図1**参照）。

次に，防衛的観点からのサイバー攻撃対処能力の強化のために必要な要件を，OODAループに基づいて検討する（**図2**参照）。

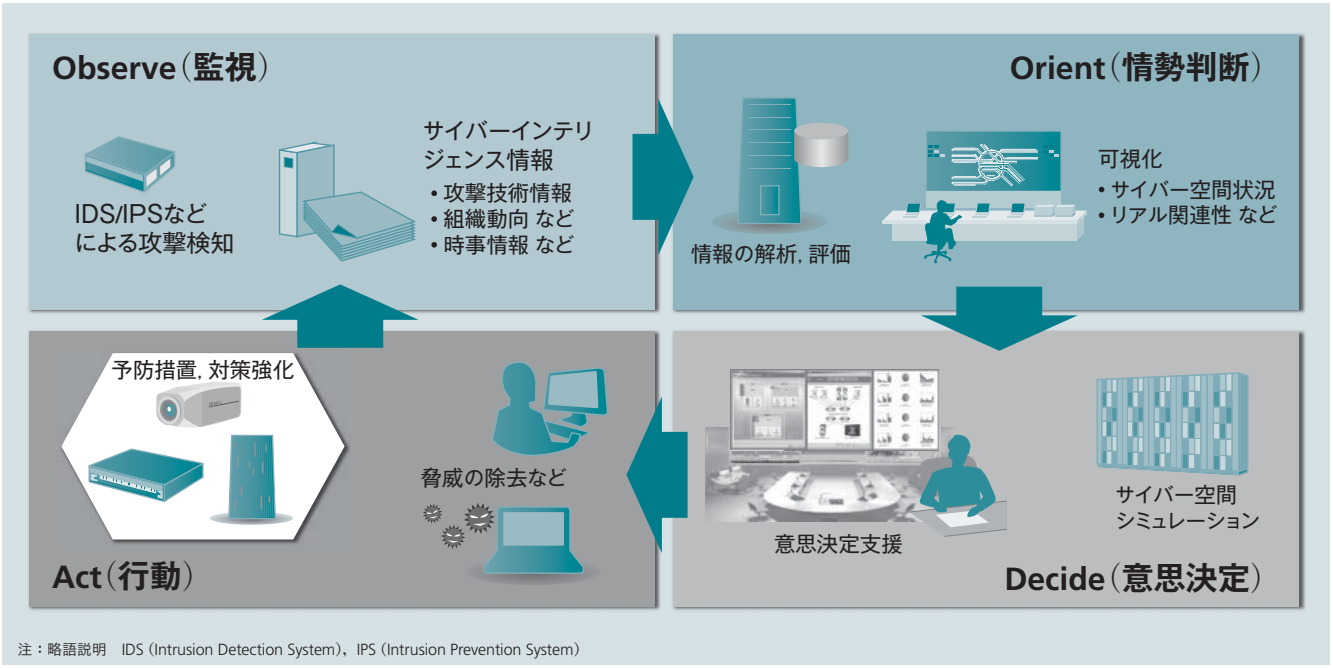
2.1　Observe（監視）

監視の主目的は，敵の発見や追跡などのための情報の入手である。収集した情報の解析を行うことで敵の能力や目的などを推測し，また，味方の情報を敵から守ることで，作戦展開を優位に進めることが可能となる。

サイバー空間における監視の例としては，アンチウイルスソフトウェア，侵入検知装置，およびログ収集ツールなどにより，外部から自組織などに対する攻撃や脅威の侵入を検知する機能が考えられる。しかし，これらの機能だけでは，検知されたサイバー攻撃が，どのような目的・意図に基づくものかを識別することは極めて困難である。

目的・意図を識別するための追加機能として，さまざまな情報の収集・共有などを行うサイバーインテリジェンス機能が考えられる。収集すべき情報の具体例としては，システムやソフトウェアなどの脆（ぜい）弱性（セキュリティ上の問題），新たなウイルスなどの発生状況，および悪意を持つハッカーグループなどの活動状況などが挙げられる。また，昨今のサイバー攻撃の動向を踏まえると，関係組織との情報共有が極めて重要である。特に，政府機関や重要インフラに対する攻撃の準備のため，サプライチェーンとして位置づけられる民間企業が攻撃される事例が増加傾向にあるなど，複数の事案の関連性を考慮しなければいけない状況にある。このため，自組織内の監視にあたっては，事案の関連性を考慮した情報収集，情報共有を行う必要がある。

ただし，サイバーインテリジェンスの実施要領・範囲に関しては，細心の注意を払って運用を設計する必要がある。「何を収集したいのか」，「何を検知することができたのか」などの情報，すなわち自身の目的・意図および能力に関する情報は，最も保護すべき，攻撃者に知られてはならない情報である。



注：略語説明　IDS（Intrusion Detection System），IPS（Intrusion Prevention System）

図2｜サイバー空間におけるOODAのイメージ
OODAループに基づき，防衛的観点からのサイバー攻撃対処能力の強化のために必要な要件を検討する。

2.2 Orient(情勢判断)

情勢判断は，攻撃の目的・意図を識別したうえで，自組織に対する影響を把握するために実施する。

つまり，監視結果の解析により，その攻撃が無差別攻撃や不注意などによるものか，または軍事的な目的・意図に基づくサイバー攻撃であるのかを識別する。さらに，自組織のシステムや作戦運用に与える影響の範囲と深刻度合いを分析する。これにより，リアル空間への影響を含めてリスクの高さを判断する。

サイバー空間における情勢判断にあたっては，ログ分析ツール，ネットワークモニタリングツール，およびインシデント管理ツールなどを活用した，監視情報の分析が必要になる。

軍事分野では，情勢判断を支援するツールとしてCOP(Common Operational Picture：共通作戦状況図)がある。敵および味方の能力，状態，目的および状況(地形・気象・海象)などの情報を，各指揮官などの役割や階級などに応じて表示することで，状況認識の統一化を図りながら情勢判断を支援する。

サイバー空間の情勢判断を行うために，同様のツールを利用する必要がある。さらに，リアル空間のCOPとの連携を図ることで，リアル空間とサイバー空間の相関を含めた情勢判断が可能となる。

2.3 Decide(意思決定)

軍事分野では，意思決定能力は指揮官に最も求められる能力の一つであり，意思決定は，基本的に人がするべきものである。しかし，意思決定の迅速性や的確性を向上させるための機能により，指揮官の意思決定を支援することが可能である。

例えば，シミュレーション機能が挙げられる。サイバー空間におけるシミュレーション機能とは，自組織で利用するシステムやネットワークの模擬環境を構築し，サイバー攻撃などの脅威に対する影響の評価や，対応要領の訓練演習を行うための機能である。

意思決定に関して，国家安全保障の観点からの極めて特殊な考え方がある。例えば端末がマルウェア(悪意のあるソフトウェアの総称)に感染するなど，組織内において脅威を発見した場合，一般的には，他の端末への二次感染などを防ぐために，ネットワークからの切り離しや端末の初期化などのセキュリティ措置を行うことが多い。

しかし，それにより作戦運用に影響が発生する可能性がある場合，適切なリスク評価を行ったうえで，任務の達成を最優先に，セキュリティ措置の対応を遅らせる判断を採ることがある。また，あえて即時対処をせずに様子見する，いわば「泳がせる」という対応を取ることが考えられる。これにより，例えば，攻撃者によるサイバー攻撃の状況を監視することで，攻撃手法などに関する情報を入手し，情勢判断を支援することが可能となる。

2.4 Act(行動)

行動のフェーズにおいては，問題解決やリスク要因の排除などの処置を行う。OODAループにおける重要な考え方として，Act(行動)までの結果をObserve(監視)に積極的に反映する点がある。つまり，Actのフェーズで一連の対応を完了せず，Observe(監視)へのフィードバックを重要視する。

この考えの下，例えばマルウェアの駆除や不正通信の切断によって対処完了とするのではなく，攻撃の傾向分析や予測した結果に基づき，情報収集の範囲拡大などや事前対処に関わる設定を行うといったフィードバックを図る。

3. 米国の政策および企業の対応

米国国防総省は，サプライチェーンである企業に対するサイバー攻撃が増加している状況と，情報共有の重要性を鑑みた施策を推進している。これは，米国国防総省におけるOODAループ上の監視能力強化の一環であるとともに，防衛産業においてもOODAループに基づく能力整備を図ることを求めていると捉えることができる。

具体的な施策としては，米国国土安全保障省と連携し，防衛関連企業のネットワークやシステム上に存在する防衛機密情報を保全するための取り組みを行っている。その一つに，「DIB CS/IA (Defense Industrial Base Cyber Security/Information Assurance：防衛産業基盤サイバーセキュリティ／情報保証)」プログラム[4]がある。

2011年6月から約1年間実施されたパイロットプログラムでは，米国国防総省と企業(開始時20企業)が，機密扱いの情報を含むサイバー脅威情報を共有してきた。さらに2012年5月，パイロットプログラムは，防衛関連企業すべてに門戸を開くプログラムとして発展した。

DIB CS/IAプログラムでは，米国国防総省は，サイバー攻撃に使用されるマルウェアの特徴情報，この脅威に関連する背景情報，および対策に関する情報を参加企業に提供する。参加企業は，受け取ったマルウェアの特徴情報を企業内におけるマルウェア検出に活用するほか，背景情報によって脅威に対する理解を深め，対応能力を向上させることができる。これに対して参加企業は，自社が受けたサイバー攻撃情報を，米国国防総省やプログラム参加企業に対して任意で提供する。

以上のように，米国では，高度化・深刻化するサイバー

攻撃への対策のため，サプライチェーンを含めた情報共有と対応能力の強化を推進している。

4. 日立グループの取り組み

日立製作所は，2009年よりカンパニー制を導入しており，その一つであるディフェンスシステム社は，防衛分野をはじめとする社会インフラ安全保障事業の推進カンパニーである。ディフェンスシステム社は，国家安全保障を支えるサイバーセキュリティソリューションを提供している。

このソリューションでは，OODAループに基づく，サイバー攻撃対処能力の向上を実現するための機能を提供する。今後，前述のサイバー攻撃対処能力の強化に関する検討を踏まえ，特に以下の2点に関するソリューション強化を図る。

4.1 サイバーインテリジェンスに関わるソリューション

サイバー攻撃への対処のために収集すべき情報は多岐にわたる。自組織内に設置したネットワーク機器のログ，資産管理情報，メールなどの技術情報だけでなく，現実社会の動向などの背景情報，組織外の攻撃事例などの情報を含め，多種多様かつ広範囲な情報が必要になる可能性がある。

これらの情報を効率的に収集・利用するために情報の体系化を行うとともに，収集した情報に対して分類，評価，相関分析および予測処理などの解析を加えることで，情報の利用しやすさ，意味，および判断材料としての価値を与えることを可能とする。

4.2 サイバー空間の状況認識に関わるソリューション

サイバー攻撃に対して迅速かつ的確な対応を図るためには，状況を正しく認識することが重要である。

サイバー攻撃の自組織に対する影響範囲やリスク評価を行うとともに，役割や階級，例えば指揮官，現場のシステム管理要員などに応じ，必要な情報を可視化して利用可能とする。すなわち，サイバー空間におけるCOPを実現する。これにより，サイバー攻撃に対し，組織全体での状況認識の統一化と総合的な対応が可能となる。

5. おわりに

ここでは，サイバー攻撃対処能力の強化のあり方，米国における政策や企業の対応，および日立グループの取り組みについて述べた。

これまで述べたとおり，昨今のサイバー攻撃は目的や手法に変化が生じ，サイバー戦が顕在化している状況にある。

日立グループは，これまで蓄積してきた防衛分野における指揮統制システムの構築などに関わるノウハウを活用し，防衛的観点からのサイバー攻撃対処能力の強化について検討中である。 今後は検討結果に基づくソリューション強化などにより，サイバー空間を含めた安全・安心な社会の実現に，よりいっそう貢献していく。

参考文献など

1) U.S. Department of Defense, News Release, DOD Announces First Strategy for Operating in Cyberspace (2011.7)
http://www.defense.gov/releases/release.aspx?releaseid＝14651
2) リチャード・クラーク，外：核を超える脅威 世界サイバー戦争　見えない軍拡が始まった，徳間書店 (2011.3)
3) Trend Micro Inc., Malware Blog, “Japan, US Defense Industries Among Targeted Entities in Latest Attack” (2011.9)
http://blog.trendmicro.com/japan-us-defense-industries-among-targeted-entities-in-latest-attack/
4) U.S. Department of Defense, News Release, DOD Announces the Expansion of Defense Industrial Base (DIB) Voluntary Cybersecurity Information Sharing Activities (2012.5)
http://www.defense.gov/releases/release.aspx?releaseid＝15266

執筆者紹介

笠井 大騎
2004年株式会社日立アドバンストシステムズ入社，事業推進本部 防衛情報システム部 所属
現在，防衛省向けサイバーセキュリティ関連システムの提案業務に従事

田島 萌絵
2008年日立製作所入社，ディフェンスシステム社 情報システム本部 エンジニアリング部 所属
現在，防衛省向けサイバーセキュリティ関連システムの提案業務に従事

齋藤 嘉幸
1993年日立製作所入社，ディフェンスシステム社 情報システム本部 応用システム設計部 所属
現在，防衛省向けサイバーセキュリティ関連システムの設計業務に従事

谷川 嘉伸
1993年日立製作所入社，横浜研究所 情報サービス研究センタ エンタープライズシステム研究部 所属
現在，サイバー攻撃対策に関わるセキュリティ応用技術の研究開発業務に従事
情報処理学会会員