サイバーセキュリティアナリストの状況認識構造の研究

研究期間　平成 29 年度～平成　　年度
研究代表者名　小松文子
共同研究者名　加藤雅彦

１．はじめに

サイバー空間は，様々な脅威に晒されている．これらの脅威によるリスクを早期発見するために，セキュリティオペレーションセンター（以降 SOC）のセキュリティアナリスト（以降アナリスト）は，日々「状況認識」を行っている．「状況認識」は，従来，交通管制や制御システムなどで研究された分野であるが，本研究は，これを多くの複雑なデータが行き交うサイバー空間の活動としてとらえる．そして，アナリストが参加可能な実験環境を整備し，アナリストのふるまいを収集，分析し，的確な状況認識するために必要な要素を追究する．具体的には，状況認識の際に利用するデータ，そのプロセス，そして，いかなる知識セットが必要とされているかを明らかにする．本研究によって，国内における SOC の質的向上と，アナリスト人材の育成に貢献することができる．

２．関連研究

情報が流通するサイバー空間は，年金機構の情報流出事件など社会的に大きな関心をもたれた標的型攻撃をはじめ様々な脅威にさらされている．サイバーセキュリティ対策は，このような脅威に対抗し，安全な情報社会を支えることを使命とする．これまで，セキュリティ対策は，技術対策や組織対策に加え，経営，経済，制度などの社会科学領域からも研究されてきた．そして，近年重要視されているのが，「人」を対象とした研究である．サイバーセキュリティ対策の主体となる「人」への対策実施推進や，被害に遭う「人」の分析研究など，サイバーセキュリティ対策において，「人」を対象とした研究が欠くことができない要素となっている．

多くのセキュリティベンダや企業内のセキュリティ監視，セキュリティ運用サービス部門は，セキュリティオペレーションセンター（以降 SOC）を運用している．SOC の機能は，日々の情報ネットワークやシステム運用を監視し，セキュリティ事故の兆候

または異変を発見し，その原因を追究し，自システムへの影響を分析し，回復および再発を防止する対策を立案することである．しかしながら，SOC に従事するアナリストは，その目的を達するために，個人の経験や勘を頼りに、複数のツールを利用しつつ、この業務、すなわちサイバー空間における「状況認識」を進めている状況である．本研究は，SOC に従事するアナリストを研究対象とする．

「状況認識（Situational Awareness，以降 SA）」は，航空機，航空交通管制，海上と港の交通管制，発電所，生産システム，オートメーションなどの領域で研究されてきた．そして，M.Endley により「異常を知覚し（Perception），その原因等を把握し（comprehend），自身の思考を対象空間に射影し（projection），意思決定すること 」と定義されている．また，そのメカニズムは，以下のようなレベルでモデル化されている(図 1 を参照).

① レベル１　一定の時間・空間環境における関連要素の認知（重要なデータを認知し）
② レベル 2 認知した要素の意味を理解・了解　（データを解釈し結合して知識とし）
③ レベル 3 将来の行動へ投影(Projection)（事象を予見できる）

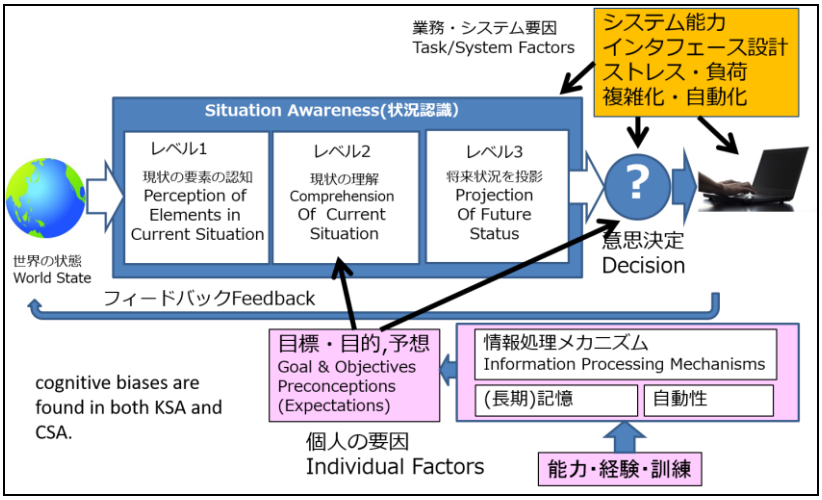


図１　Model of situational awareness in dynamic decision making(Endsley,1995)[1]

サイバー空間が第 4 の戦場と言われた 2010 年前後より，従来の SA の研究をサイバー空間へ適用する研究が米国で始まった．しかし，国内では，技術的なツールの研究が優先され，アナリストの協力が不可欠なアナリスト本人に焦点を当てた研究成果

[1]MICA R. Endsley,Towards a Theory of Situation Awareness in Dynamic Systems, HUMAN FACTORS,1995,37(1),32-64

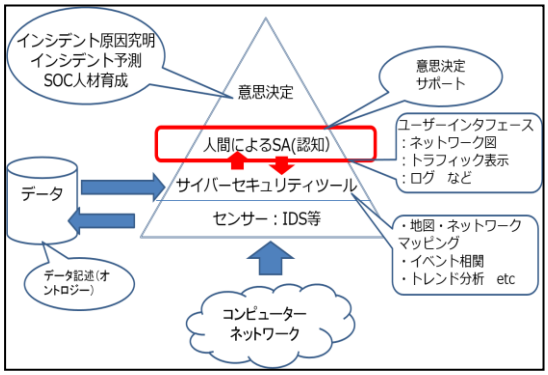
は研究代表者の知る限り公表されていない．これは，企業等の機密保護の観点から研究の対象とする SOC からのデータ収集や，日々SOC に従事するアナリストの協力を得ることが困難であったためである．

以上のような背景のもと，本研究では，SOC に従事するアナリストが，日々の監視・分析業務において，サイバー攻撃による異常を，どのようなデータを用い，どのような手順（プロセス）でその異常を解析し，原因追及を進めていくかを明らかにしていくことを問い（リサーチクエスチョン）とする．

３．研究内容

3.1　概要

サイバーSA は，図１の赤枠で示すように，センサーやツールからのデータを状況認識し，意思決定に有効な情報として提供する領域である．海外の関連研究では，サイバーSA の様々な局面について研究がされているが，本研究は，アナリストが、どのような不正侵入検知システムやシステムログはじめとする事象データを認識し、脆弱性情報を含むシステムの様々な関連情報を探索し、何が起きているかを推測する局面である。



これは、「データトリアージ」のフェーズと呼ばれる．このような研究は，国内ではいまだ成果（論文）は公表されていない．なぜなら，アナリストが従事する SOC では，扱う情報を SOC 外部に持ち出すことが困難であり，また，日々業務に従事するアナリスト自身を対象として研究することが困難であるからである．したがって研究環境の整備が非常に重要である。本研究では，本学の演習設備を活用し，学外からの攻撃情報を収集するデータを対象として実験実証することとする．

3.2　研究環境の整備

的確な SA のため、アナリストに必要とされる要素を明らかにするために，関連研究レビューとともに，研究環境を整備する．すなわち攻撃用模擬システムを構築し，データを収集する．

① 実験設備の構築と実験データの収集

本学セキュリティ演習室の研究用ネットワークを活用し，2017 年 10 月に，UNIX サーバ（OS は CentOS7）を構築し，外部への IP アドレスを公開した．その後 1 か月程度状況を監視した．その結果，当時のよく知られたランサムウエアなどや一般的なウイルスのデータを観測することはできたものの，不正アクセスに類した攻撃を観察することはできなかった．これは，本学のネットワークが外部より観察するとビジネス的な構成になっていないことなどが原因と考えられた．このためには，中小企業などの仮想的なネットワーク構成のシステムを外部に見えるようにする必要があることが想定された．研究協力者の伊藤忠商事　佐藤氏と討議し，伊藤忠商事が収集しているデータを提供していただき，(来年度)これを対象に研究することとした．平行して，外部からの攻撃情報収集については取り組んでいく．

② アナリストの振る舞いを記録するソフトウエアの導入

アナリストがデータ解析をする際の振る舞いを記録するため, PC 上の操作を記録するソフトウエアを導入した．本ソフトウエアの本来の目的は，内部者からの情報漏えいを抑止，監視するためのものである．本ソフトウエアを導入し，その記録状況や，記録データ量などについて実証することができた．今後，本ソフトウエアを活用し，データを解析する振る舞いを記録していく．

4. おわりに

期待していた情報収集ができなかったため，当初予定していた，実証実験まで実施することはできなかった．しかし，時間をかけて情報を収集すること，学外研究協力者からの情報提供を受けて，本年度整備した設備・環境を活用し研究を進めていく．