サイバーセキュリティ分析における状況認識の研究

小松　文子[†1]　加藤　雅彦[†1]

概要：サイバーセキュリティ状況認識（CSA:Cyber Situational Awareness）とは，サイバー空間において「状況認識」することで的確な意思決定を可能とする，セキュリティアナリストの認知のプロセスである．本稿では海外で進められている研究における，CSA の機能や，セキュリティアナリストの認知推論のプロセスを紹介し，CSA 研究の目的と意義を述べる．本論文は，国内における CSA についての研究の必要性と今後の課題についてのポジションペーパーである．

キーワード：セキュリティ，認知，状況認識

Introduction of Cyber Security Awareness Research

Ayako Komatsu[†1]　Masahiko Kato[†1]

Abstract: Cyber security situation Awareness (CSA) is a process of recognition of the security analyst who makes an accurate decision　making possible to do "SA:　situation awareness" in cyber space. This paper reviews literature which researches on function of CSA and a process of recognition reasoning of a security analyst. This paper is position paper about necessity of a study on CSA and describes future's issues on CSA in Japan.

Keywords: Security, Cognition, Cyber Situational Awareness

1. はじめに

企業や組織の社会経済活動は，情報技術に大きく依存しており,その安全性を確保することが必要である.しかし，サイバー空間はさまざまな脅威によってリスクにさらされているため，サイバーセキュリティ対策は欠くことができない．このような状況で，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などの専門組織は，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．ここで，セキュリティオペレーションセンターの機能は，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，回復および再発を防止する対策を立案することである．我々は，SOC におけるセキュリティアナリストが,その目的を達するために必要な,「状況認識（SA:Situational Awareness)」に関心をもつ．SA は，これまで，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．要員が，正確に状況を認知し，発生するであろう事象を予見するための助けとなる認知のプロセスや，必要な情報と，技術的な対処ツールなどへの要件を明らかにする研究である．本論文では，サイバーセキュリティにおいて取り組まれている SA 研究について紹介し，今後の研究について述べる．まず，第 2 章で SA の基本モデルを述べる．次に SOC の状況について，最近公表された国内の資料を参考に述べ，4 章では主に海外で実施されているサイバー状況認識（Cyber SA，以降 CSA）研究を紹介する．5 章では，我々が取り組む CSA 研究について述べる．

2. 状況認識とは

2.1 状況認識の認知モデル

サイバー空間における状況認識について触れる前に，従来の「状況認識」の概念について，述べる．

状況認識の認知メカニズムとして，M.Endsley による以下の定義が最もよく参照される[1].

“The perception of　the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future”

そして，この”perception”, “ comprehension” , “Projection”は３つのレベルとして以下のようにモデル化された．

レベル１．一定の時間・空間環境における関連要素の認知
レベル２　認知した要素の意味を理解・了解
レベル３　将来の行動へ投影(Projection)

図１は，以上の概念を表したものである．

†1 長崎県立大学　情報システム学部　情報セキュリティ学科
Department of Information Security, University of Nagasaki

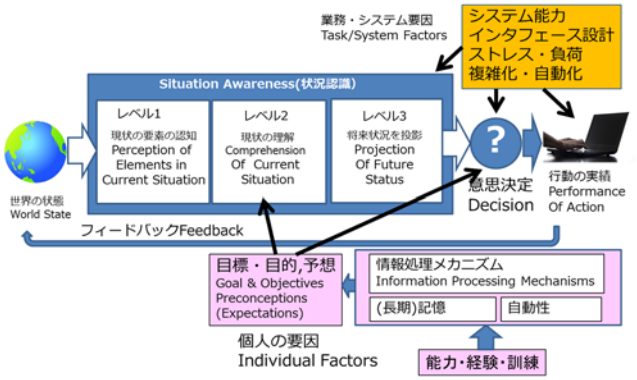


図 1　状況認識（Situational Awareness）　M.Endsley による（1998）[1]

３つのレベルは，1. 重要なデータの基礎認知　2. データを解釈し結合して知識とし，3. 事象を予見できる　，と進展していく．外部要因の業務・システム要因として，システム能力，インタフェース設計，ストレス・負荷，複雑化・自動化が影響し，個人の要因として，能力・経験訓練が個人の情報処理メカニズムに入力され，目標・目的や予想が状況認識やその後の意思決定に影響をすることを表している．

状況認識は複数の散在する情報を認知し意思を決定する複雑な認知のプロセスである．

2.2　サイバー空間における状況認識研究の必要性

国際的には，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「状況認識」の研究をサイバー空間へ適用しようという研究が始まった．サイバー状況認識は，状況認識のサイバー空間版であり，攻撃者が誰か，どんなサイバー攻撃であるか，攻撃の対象は何かを「認知」し，現在の状況が引き起こされていた手段，理由やいかなる影響があるかを「理解」し，将来の攻撃の場所や影響を予見することを決定する（投影）ことである．SOC におけるセキュリティアナリスト達が，的確な判断を下すために，どのような情報が必要であるか，また，それらをもとにした状況を認識するプロセスやメカニズムを明らかにすることは，サイバーセキュリティを維持・運用する SOC に必要であることは自明である．

3.　SOC の状況

サイバー空間における状況認識が必要とされる場所は企業や組織の情報システムやネットワークを監視する SOC である．そこでは，いくつかの役割を担うセキュリティアナリストが，監視対象であるネットワークを含むシステムにおいて日々発生する事象を監視している．本章では，日本シーサート協議会におけるセキュリティ人材タスクフォースでの，シーサートにおける人材とそのタスクの整理，および日本セキュリティオペレーション事業者協議会（ISOG-J）が公表した，「SOC の役割と人材のスキル」[2] を参照して機能と役割について述べる．前者は，組織内に CSIRT を構築する際の構成する要因と役割を定義したもので，後者は人材育成の観点からの SOC の役割を定義し，要求される人材のスキルを規定している．

3.1　シーサートにおける役割と業務内容

図 2 は，有事におけるシーサートの役割と業務内容の関連を表している [3]．インシデントハンドラやトリアージ，フォレンジクスなどがコマンダーを中心に連携して活動することを示している．各役割は「状況説明」によって連携されていることがわかる．これは CSA が的確に実施される必要性も表すと考える．

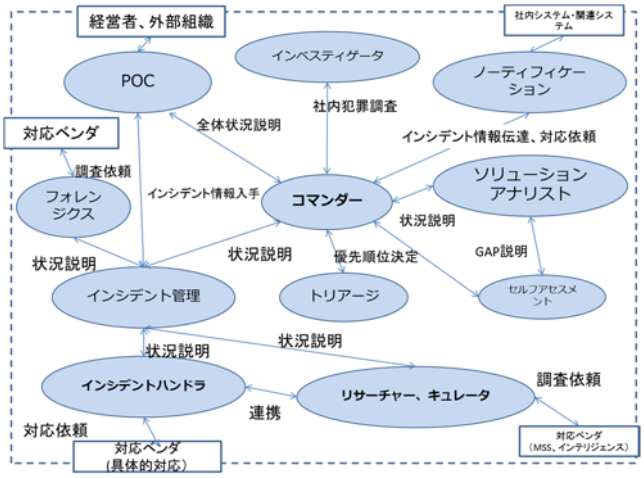


図 2　シーサートの役割と業務内容の関連図[3]

3.2　セキュリティオペレーションセンターにおける機能と役割

次に，ISOG-J の資料を参照すると，セキュリティ対応を行う組織の持つ機能として，以下の８つを規定している．

① リアルタイム分析
② 脅威情報と傾向分析
③ インシデント対応と分析
④ インシデント：証拠の分析
⑤ ツールのライフサイクルのサポート
⑥ 監査と内部犯行対応
⑦ 診断と評価
⑧ 外部との連携

これらの機能は組織として以下の 4 か所に配置される．名称は，ISOG-J のものである．

- ティア 1（監視）：①，②のための情報収集
- ティア 2（高度な分析）：①，④，⑥，⑦
- 情報収集・分析（専門知識の活用）：②，④，⑧

・　システム管理：⑤，⑥
・　技術開発：⑤

セキュリティ対応の際は，ティア１，ティア２，情報収集分析が相互に連携し，システム管理や技術管理は，運用・技術面で支援する．

以上は，CSA を直接扱ったものではないが，SOC や CSIRT における要員の役割が述べられているため，どの要員のタスクとして CSA が必要とされているか，CSA に対する大まかな入力情報の種類を読みとることができる．

監視運用やインシデント対応において，状況認識しつつ判断している組織は，ティア１，ティア２，情報収集・分析である．本論文では，これらの活動を遂行する要員をセキュリティアナリストと総称する．ISOG-J の資料では，それぞれの機能を詳細化しており，セキュリティアナリストが実施する役割が明らかになっている．ただし，要員がいかに認知し，その情報を活用して意思決定するかなどについては述べられていない．

サイバー攻撃やインシデントの状況を認知し，的確な判断を下すためには，これらに携わるセキュリティアナリスト達の認知と推論のプロセスの研究が重要である[4].

4.　サイバー空間における状況認識の関連研究

サイバー空間における SA の関連研究は，主にサイバー攻撃や情報セキュリティ事故の認知とその対処の領域に多い．すでに述べた Endsley の SA のモデルを起点として，多数の研究がある．2014 年には，文献レビューの論文が公表された[5].このレビューによると，サイバー空間における状況認識の研究は，大きく分けて以下に分類されている．

・　サイバーセキュリティ状況認識の一般論
・　制御システムに対する状況認識
・　緊急時対応における状況認識
・　ツール，アーキテクチャ，アルゴリズム
・　情報融合（Information Fusion）
・　状況認識の可視化（Visualization）
・　ヒューマン･コンピュータインタフェース，設計仕様，状況認識ワークフロー
・　広域ネットワークにおける状況認識
・　サイバー状況認識の訓練
・　サイバー状況認識の情報共有
・　軍におけるサイバー状況認識

サイバー状況認識の研究は主に以下を目的としている．

・　サイバー監視の運用効率化．例えば多量の情報から必要な情報だけを抽出すること
・　セキュリティアナリストがどのような情報を元に攻撃を認識するかを明らかにする[6]
・　セキュリティアナリストの訓練に資する
・　サイバー監視運用にかかる指標を明らかにし，SOC の評価に利用すること

本章では，CSA 研究の領域を示し，3 つの関連研究を紹介する．

4.1　サイバー状況認識研究の領域

CSA 研究の領域を図 3 に表す．まず，コンピュータ・ネットワーク環境からの情報を収集するセンサーが存在し，そのセンサー情報を処理するセキュリティツールがある．セキュリティツールは，ネットワーク構成図のマッピングやイベント相関傾向分析などの機能を提供する．これらの情報がユーザインタフェースによって人間に提供され，これを状況認識することで，インシデント原因究明やインシデント予測などを意思決定する．

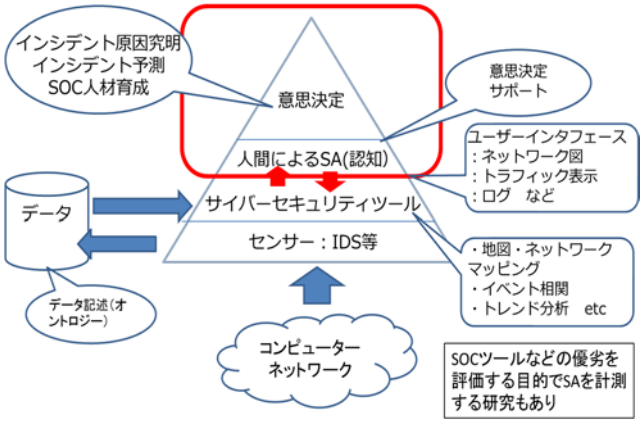


図 3　サイバー状況認識研究の領域

なお，センサーからのデータを保存のためのオントロジーによるデータ記述や，セキュリティツールの優劣を評価する目的で，SA を計測する研究もある．さらに，SOC の人材育成や訓練を目的とした研究も存在する．

4.2　サイバー状況認識形成についての研究

ここではグラフ理論を利用した研究 [7]を紹介する．[7]では，サイバー状況認識フレームワークとして，必要となる機能とアナリストの置かれた立場を具体化し，脆弱性や依存性をグラフで表す。これらのツールを開発し、取るべきシナリオをアナリストに提示する．

4.2.1 サイバー防御プロセスの機能

サイバー防御プロセスは，サイバー攻撃を発見し，攻撃によって影響を受けるシステムの危殆化を防ぐだけでなく，過去の攻撃の影響や将来の攻撃を予想し防御する．そのために必要な機能が以下の５つである．

(1)　攻撃から学習
危殆化を引き起こす実際の攻撃の知識であり，基本となるものである

(2) 優先度付け
危険な脅威より保護しリスクを低減するための優先付け

(3) メトリックス（尺度）
経営陣と，IT 技術者，監査人，セキュリティオフィサーとの情報共有するための指標である．必要な調整と速やかな実行のために，セキュリティ対策（コントロール）の効果を計るものである，

(4) 継続した診断と被害軽減
現状のセキュリティ対策の効果をテスト・評価することを計測し，次のステップへの優先順位を導出することに役立たせる

(5) 自動化
高信頼で計測可能なモニタリングを継続して可能とするための自動化である．人間のアナリストの労働依存やエラー傾向のある労働を補う．

4.2.2 セキュリティアナリストの問い

サイバー監視において，セキュリティアナリストたちは，以下のような疑問に答えつつ業務を進める．言い換えればサイバー状況認識のフレームワークは，これらの疑問へ答える必要がある．

(1) 現在の状況
今，攻撃が実施されているか．そうであるならその侵入の段階と攻撃者の場所はどこか？
この質問への回答となるのは，IDS，ファイアウォールや他のセキュリティ監視ツールからのログであり，状況認識の結果は，侵入された活動の詳細情報である．

(2) 影響
攻撃は，どの程度組織やミッションに影響を与えるか？被害を見積もることはできるか？
状況認識では，組織の資源の価値などの知識を必要とする．その情報を基に，侵入行為によって引き起こされる被害状況を見積る．

(3) 進展
状況は進展するか？攻撃の次の段階を追跡できるか？
この状況で，状況認識に必要な情報は最初のステップ（現在の状況）の成果であり，状況認識の結果は，攻撃がどのように進んでいるかがわかることである．

(4) 振る舞い
攻撃者はどのようにふるまうかが想定されるか？
この答は，攻撃者の目的や戦略を理解するために攻撃者の振る舞いをモデル化することである．理想的にはこの振る舞いを形式的にモデル化することであるが．
この振る舞いは，時間とともに変化しモデルも変わっていく．

(5) フォレンジクス
攻撃者はどうやってこの状況を作り出したのだろうか．
この疑問へ答えることは，攻撃者がどこからやってきて進んできたかを理解するために，事実と観察との関連を明らかにすることである．また，４つめの疑問のふるまいの答えによってこの答えを得られる．このケースでは，SA プロセスは攻撃を許す弱点や脆弱性の詳細な理解が成果となる．この情報は，セキュリティ技術者や管理者が，同様の攻撃を防ぐシステム構成を構築することを可能とする．

(6) 予測
この状況の可能な未来を予測できるか？
これに答えることは攻撃者が次の攻撃に移ることを予測可能な時である．これまでの問いである現状と今後の進展，攻撃者の振る舞いの知識によって予測する．

(7) 情報
信じられる情報の元はどれか？これらの品質を評価できるか？これにこたえることは，他のすべての作業の情報の能力を意味する．

4.2.3 サイバー状況認識フレームワーク

[7]では，CSA の機能とセキュリティアナリストの問いから，図４のフレームワークを提唱している．このフレームワークは，ネットワークトポロジーから開始し，既知の脆弱性やゼロデイ攻撃の仮説より攻撃グラフを作成する．また，サービスや機器の依存性を分析し依存グラフを作成する．攻撃グラフと依存グラフを対応させることにより，可能性のある攻撃シナリオをアナリストへ提示する．

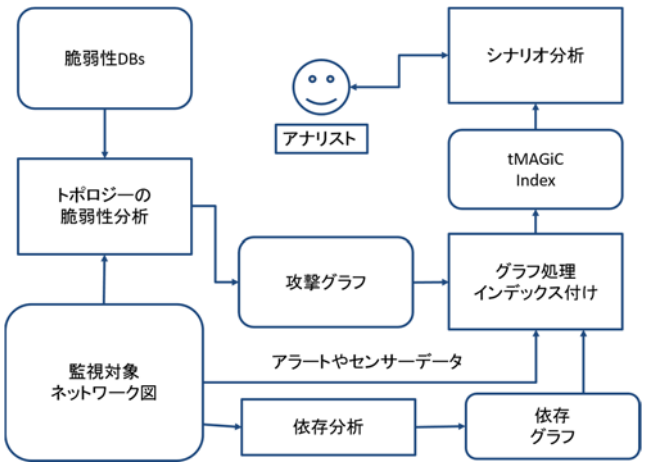
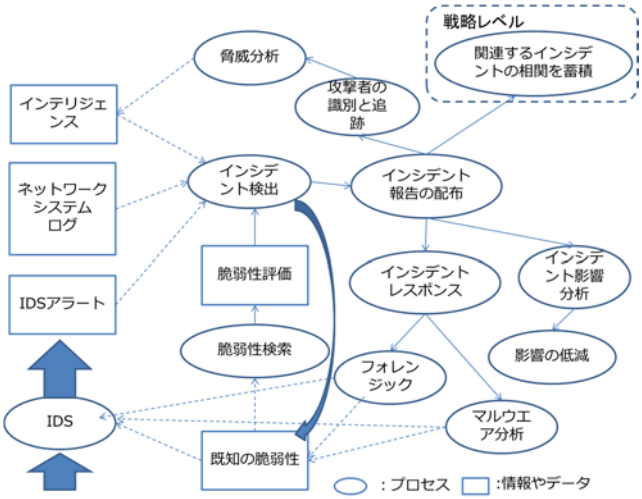


図４　サイバー状況認識のフレームワーク[7]

4.3 サイバー状況認識の詳細な認知プロセス

２ つ目の関連研究は，詳細な認知プロセスについて検討したものである[4]．サイバーセキュリティ分析を①トリアージ，②エスカレーション③相関④脅威⑤インシデントレスポンス⑥フォレンジック６つに分類した研究[8]があるが，まず，これをもとに，図５の示す企業組織内の戦術レ

ベルの認知プロセスを表した．図中で，戦略レベルとは，地域や他国などと関係するプロセスである．



出典：[8]，著者邦訳

図 5 企業組織内でのサイバー分析の認知プロセス

図 5 では，ツールなどによるプロセスと人間のプロセスが混在している．IDS アラート，ネットワークやシステムログによりインシデントが検出されると，インシデント報告が以降の分析(インシデントレスポンス分析, 影響分析, 脅威分析を通した攻撃者の識別と追跡，およびフォレンジック）のために配布される．前述した 6 つの分析のうち，①，②はインシデント検出に含まれる．[4]では，図 5 の認知プロセスをハイレベル認知プロセスとし，さらに詳細な認知の推論プロセス(fine-grained cognitive reasoning process)の必要性を説く．つまり現状のサイバー分析の推論プロセスは, 言語による分析(会話や考察, 過去を振り返ること), ケーススタディ, 振る舞い追跡などにより実施しているが, これらをよりシステム的に詳細な認知のプロセスに分解していくことである．そこで,「動作（Action）」と,「観察情報」と「仮説」の相互関連を示し，AOH(Action-Observation-Hypothesis)モデルを提案している．例えば，IDS のアラートをチェックする動作と IDS アラートの内容である観察情報と，それらから導出される複数の仮説(例として DNS サーバがキャッシュポイズニングによって攻撃されているや, 誤検出など)，さらに仮説からの動作，観察情報というように情報が連関していく認知を追跡し表記できるようにした．この研究で特記すべきは，これらの情報を自動的にとらえるツールを作成したことである．このようなセキュリティアナリストの推論を捉えるには，インタビューや推論途中にアナリストに記録を取ってもらうなどの介入が必要であるが，思考が中断するという弊害がある. このため, 認知を追跡するためのツールを開発し，公開されている VAST チャレンジという IDS とファイアウォールのアラートデータを含んだデータを利用して，米国陸軍研究所のアナリストの協力を得て，認知の推論を追跡している（図 6）．

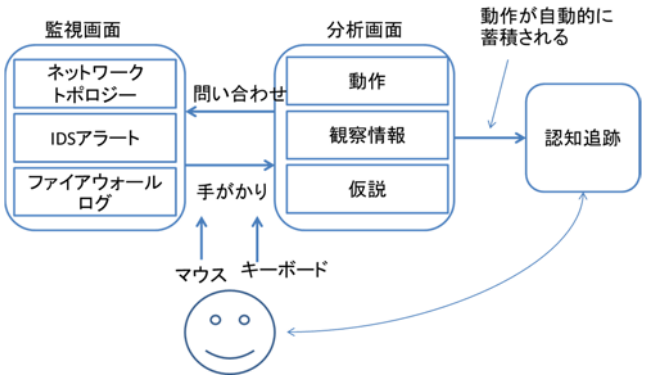


図 6　認知追跡の捕捉モデル

4.4　インスタンスベース（IBL）による研究

最後に紹介するのは，人間の動的環境下での意思決定理論であるインスタンスベースラーニング（IBL）による研究である[9].

意思決定者のメンタルプロセスを認知科学のモデルを基に，認知，判断，選択，実行，フィードバックとし，また，エンズレイの状況認識モデルにも一部対応している．ここで，インスタンスとは，過去の経験をさし，事象を表す属性である状況(Situation) と期待された決定の結果の程度である効用(Utility)からなる．IBL では，頻度や近時性という属性のある記憶に依存して，選択し，学習する．[9]では, 防御の成果を攻撃者の振る舞いにいかに依存するかを実証している．

5.　国内における CSA 研究の課題

これまで，SA と CSA について，主に海外の研究を紹介した．国内における CSA の研究では，セキュリティインタフェースの研究[10]，イベント分析ツール[11]など，CSA を構成する部分的なものに留まってきた．また，セキュリティアナリスト自身の認知に関した研究は筆者らの知る限りされていない．一方で CSA は，企業・組織における SOC だけでなく，国家の安全保障の観点，セキュリティ人材育成という観点からも重要である．すでに進められている海外での CSA 研究を踏まえたうえで, 以下の研究が必要と考える．

5.1　CSA 研究のレビュー

本論文で紹介した研究の他にも，多くの研究があり，これらのレビューが必要である．

5.2　SOC の状況確認

3 章で述べたように，国内の SOC におけるセキュリティアナリストの役割はすでに報告されているが，実際の状況を確認する必要がある．特にセキュリティ人材が不足してい

るとされているため，アナリストが複数の役割を担っていると想定される．国内の SOC の組織構成や，アナリストの役割の状況を確認する．海外での研究を参照するために，CSA に要求される機能や，プロセスについて，特に海外との差異などがあるか否かの確認が必要である．

5.3　セキュリティアナリスト達を対象とした調査

SOC のセキュリティアナリスト達へのインタビューなどを通して，アナリスト達がどのようなセンサー情報をどのように利用し，CSA を実施しているかの調査を実施する．また，セキュリティアナリストについて，属性情報として以下の点を調査し，アナリストの活動に影響するかを分析する．

- 経験年数や過去の対応有無などの情報
- 保持する知識の種類（ネットワーク，マルウエア，Web サーバ，プログラミング，コンピュータアーキテクチャ，暗号・認証技術など）
- リスク選好の程度
- 忍耐力の有無

リスク選好の程度は，意思決定に影響すると考えらえる．

5.4 CSA における推論プロセスの調査と実証

セキュリティアナリスト達を対象とした調査の結果とこれまでの研究レビューを踏まえて，仮説モデルを設定していく．なお，これまで筆者らがいくつかの SOC の状況を確認しているが，インシデント監視においては誤検出を含む多量のインシデントが発生する．したがって，認知の推論プロセスを調査する際には，2 段階のフェーズに分け，まずは確からしいイベントを抽出し，次に CSA 推論プロセスを明らかにしていく．

CSA 推論プロセスは，4.3 で述べた研究を参考に，実際のデータを利用して，実証することを計画している．

おわりに

サイバー空間において，サイバー攻撃を監視し，防御を行う SOC は近年ますます重要な位置を占めている．しかし，SOC で活躍するセキュリティアナリストは，その業務量が多大で，高負荷と言われる．また，人材も不足している．CSA 研究を通して，セキュリティアナリストの的確で効果的な意思決定の助けになることは，有意義であると考える．今後，CSA 研究を推進し実証評価していきたい．

参考文献

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

[2]日本セキュリティオペレーション事業者協議会　セキュリティオペレーション連携 WG，SOC の役割と人材のスキル，1.0 版，2016.7.11，http://isog-j.org/output/2016/SOC_skill_v1.0.pdf

[3]日本コンピュータセキュリティインシデント対応チーム協議会, CSIRT　人材の定義と確保(Ver.1.0), 2015.11.16　,http://www.nca.gr.jp/activity/imgs/recruit-hr2015116.pdf

[4]J. Yen, Robert F. Erbacher, C.Zhong, P.Liu, Cognitive Process,A.Knott et al.(Ed.), Cognitive Process, Cyber Defense and Situational Awareness, Advances in Information Security 62,Springer Int. Publishing ,2014

[5]Ulrik Franke, Joel Brynielsson,Cyber situational awareness - A systematic review of the literature, Computers & Security 46(2014) 18-31,ELSEVIER,2014

[6]Noam Ben-Asher , Cleotilde Gonzalez, Effects of cyber security knowledge on attack detection, Computers in Human Behavior 48 (2015) 51–61

[7]M Albanese, S.Jojodia, Formation of Awareness,A.Knott et al.(Ed.), Cognitive Process, Cyber Defense and Situational Awareness, Advances in Information Security 62,Springer Int. Publishing ,2014

[8]D'Amico,A. and Whitley,K,The Real Work of Computer Network Defense Analysis, VizSEC 2007; Proceedings of the Workshop on Visualization for Computer Security, Springer-Verlag Berlin Heidelberg,pp.19-37,2008

[9]Varun Dutt　Indian Institute of Technology, Mandi,Young-Suk AhnCyber Situation Awareness: Modeling Detection of Cyber Attacks With Instance-Based Learning，Human Factors: The Journal of the Human Factors and Ergonomics Society, 55, 3, 605-618.2013

[10]松本他,ネットワークインシデント分析システム構築運用におけるユーザインタフェースの検討,SCIS2006 論文集，2006

[11]中尾他, インターネットにおける実時間イベント分析の研究開発，SCIS2006 論文集