Vol.2019-GN-108 No.4
Vol.2019-SPT-33 No.4
2019/5/9

サイバー攻撃対応における組織全体としての状況認識を記述するモデルの提案

池田美穂† 高橋慧† 上川先之† 爰川知宏† 小阪尚子† 岸晃司†

概要：本稿では，サイバー攻撃のインシデント対応において，組織が適切な状況認識をできるように支援するための，組織全体としての状況認識に必要な要素を記述するモデルを提案する．組織活動を複数人で分業しているため，各人は組織活動全体のうちの一部をモニタリングして状況認識している．この各人の分散的な状況認識と状況認識に用いたデータを，組織活動の因果関係に基づき適切につなぎ合わせることで，組織全体としての状況認識とその要素を記述するモデルを導出する．また，本モデルを適用して，架空の EC サイトにおいてサイバー攻撃が発生したときの組織全体としての状況認識を表現することで，本モデルの妥当性を確認する．

キーワード：サイバー攻撃，インシデント対応，状況認識，情報共有，事業継続

Model of Organizational Situation Awareness in Cybersecurity Incident Response

MIHO IKEDA† SATOSHI TAKAHASHI† HIROYUKI UEKAWA†
TOMOHIRO KOKOGAWA† NAOKO KOSAKA† KOUJI KISHI†

Abstract: We propose a model of organizational situation awareness in cybersecurity incident response; it contributes to effective information sharing and situation awareness. People in organizations play some rolls that are the components of organization's business process, so they perform and monitor some parts of organization's activities and build their own partial situation awareness based on their experience and knowledge. We develop the proposed model by joining such distributed situation awareness together in accordance with the causal relationship of business process. We verify the model through assessing test cases of cyberattack to a hypothetical EC system with using the model.

Keywords: Cyber Attack, Incident Response, Situation Awareness, Information sharing, Business Continuity

1. はじめに

IT システムの普及により，サイバー攻撃の脅威が高まっている．企業などの組織は，業務効率化やサービス実現のために IT システムを利用している．また，技術の進展により，事業の広範にわたって IT システムによる作業の自動化が進んでおり，IT システムの事業への寄与度は大きくなっている．そのため，サイバー攻撃によって IT システムの障害が発生すると，その影響は事業全体に及ぶ恐れがある．

サイバー攻撃が発生したときに迅速かつ適切に対応できるよう，CSIRT (Computer Security Incident Response Team) の構築が進められている．CSIRT は，組織内で発生した情報セキュリティのインシデントに対処するための専門チームである．ただし，インシデントの被害規模や対応内容によっては，他の部署も協働する必要がある場合もある．

サイバー攻撃のインシデント対応を効果的に実施するには，関係者間で状況認識を統一することが重要である．サイバー攻撃による各種影響への対応は，時間的制約を考慮すると，複数人で分業して実施すると効率的である．しかし，複数人で分業すると，認識のズレが発生して，作業が計画どおりに実施されないなどの問題が生じることがある．そのため，事業継続計画などに沿って，作業の優先度と作業内容の認識を関係者間で統一すると，インシデント対応として必要な作業の抜け漏れを防ぐことができる．

状況認識の統一を円滑に実現するには，関係者間ではどのような種類・粒度での状況認識の統一が必要か，適切な状況認識のためにはどのような情報と知識が必要か，複数の情報や知識をどのように統合して状況認識するかなどを，事前に把握して手順を整理しておくとよいと考えられる．

本稿では，組織がサイバー攻撃のインシデント対応を効果的に実施できるよう，適切な状況認識を支援するための，サイバー攻撃対応における組織全体としての状況認識とその要素を記述するモデルを構築する．

本稿の構成は以下のとおりである．2 章にて，サイバー攻撃のインシデント対応に関する状況認識の先行研究と問題を整理する．3 章にて，サイバー攻撃発生時の組織全体としての状況認識とその要素を記述するモデルを導出し，4 章にてその妥当性を評価する．5 章にて，提案モデルに基づく状況認識の支援方法を検討する．最後の 6 章では，本検討の今後の展望について述べる．

† 日本電信電話株式会社
NIPPON TELEGRAPH AND TELEPHONE CORPORATION

2. 先行研究

2.1 CSIRT ガイドラインにおける状況認識に関する記述

状況認識は，インシデント対応の起点となる重要な要素である．インシデント発生時のマネジメントに特化した規格である ISO 22320 では，状況認識を対応計画の策定や決定・実行に先立つプロセスとして位置付けており，情報の収集・分析・共有の活動により構成されることを示している[1]. CSIRT ガイドラインの 1 つである NIST Cybersecurity Framework では，サイバーインシデント発生時の一連の活動の構成要素を示しており, 特に“Detect”全般と, “Respond”と“Recover”の“Communication”を情報の収集・分析・共有に関する活動として記述している[2]. 同じく CSIRT ガイドラインである FIRST CSIRT Framework では, “Service Area 4 -Situational Awareness”が，状況認識に関する項目であり，“Service Area 1 – Incident Management”のインシデント対応を支援する重要な要素であることが読み取れる[3].

しかし，サイバー攻撃のインシデント対応時に，状況認識のためにどのような情報を収集・分析・共有すべきかを具体的に記述したガイドラインは見当たらない．FIRST CSIRT Framework によると，必要な情報の収集・分析・共有とは，組織やステークホルダが必要とする状況認識の要求分析を行い，要求を満たすデータや分析手法を特定することで求まる（4.1 Service – Metric Operations）．この手順の詳細は, NIST Cybersecurity Framework の“Identify”, “Protect”, “Detect”で言及されているリスク分析・防御・監視対象に関する情報の収集･分析･共有に該当すると解釈できるが，状況認識に用いる情報は具体的には記述されていない.

以上をまとめると，必要な状況認識と情報共有はシステムごとに異なるという事情は理解できるものの，具体的にいつ・誰に・どのような種類や粒度の情報を共有すると状況認識が適切になるという指針は明らかにされていない.

2.2 ヒューマンファクターズにおける状況認識のモデル

状況認識（Situation Awareness）を記述するモデルとして，Endsley による状況認識モデルは, 各分野で広く引用されている[4]．このモデルは，人は状況認識するとき，収集した情報だけではなく知識･経験なども用いることを説明する．なおこのモデルは，基本的には個人の状況認識を記述するものであり，複数人すなわちチームで協働する場合のチーム全体の状況認識に対してはそのまま適用することはできない．チームとしての状況認識の流れは，個人の状況認識と類似すると考えられるが，複数人の状況認識の統合などを加味する必要があるため，より複雑なものとなる．

チームの状況認識に関する理論の一つとして，分散状況認識（Distributed Situation Awareness）が挙げられる[5]．分散状況認識は，Stanton らが提唱した理論であり，同じ状況下に居合わせた複数のエージェント―人およびモノを含む―はそれぞれ異なる状況認識を有しているという．分散状況認識の分析手法を用いると，例えば，関係者の全体集合としては状況認識に必要な情報が揃っていても，ある担当者が必要とする情報が伝わっていなかったために，その人の判断や行動が不適切なものになったことを説明できる．

分散状況認識に関する研究報告から，インシデント発生時に必要な状況認識と情報共有に関する指針が得られる．Kitchin と Baber は，3 人一組のチームを組み，画面に表示される道路通行中の車両の中から違法な車両を検知するという実験を通じて，熟練者同士の場合は，異なる情報に基づき各人が異なる状況認識をしてコミュニケーションする方が，同じ情報を共有して同じ状況認識をするよりもパフォーマンスが良いと考察した[6]．このことは，COP（Common Operation Picture. 状況認識の統一図）は役割に特有である必要があるという重要な示唆を与える[7].

これらの状況認識に関するモデルは，人や組織が状況を認識する仕組みを理解する手助けにはなるものの，しかしながら，サイバー攻撃発生時の状況認識に用いる情報や知識を特定するものではないことには留意する必要がある．

2.3 インシデント対応における状況認識の問題

2.1 および 2.2 を整理すると，サイバー攻撃のインシデント対応の活動の流れに関してのコンセンサスは存在するが，具体的にいつ・誰／何が・何の作業によって・何の情報を入手していて，いつ・誰／何に・何の作業のために・何の情報を伝達すればよいかの指針は定まっていない.

筆者らはこれまでに，サイバー攻撃発生時に複数の部署が協働してインシデント対応と事業継続の各作業を行うときの問題を分析し，状況認識の支援方法を検討してきた[8].

本稿では，状況認識の支援方法を具体化するため，サイバー攻撃対応の状況認識に必要な要素を簡単に特定できるモデルの構築を試みる.

3. 提案モデル

サイバー攻撃が発生したとき，組織は各種影響に対応することを考慮すると，サイバー攻撃のインシデント対応における組織全体としての状況認識には，サイバー攻撃を受けた IT システムの被害に加えて，IT システムを利用する各活動への影響も含むことが要件として挙げられる.

この要件を踏まえて本稿では，組織全体を俯瞰する状況認識のモデルを構築したうえで，サイバー攻撃対応における組織全体としての状況認識に必要な要素を検討する.

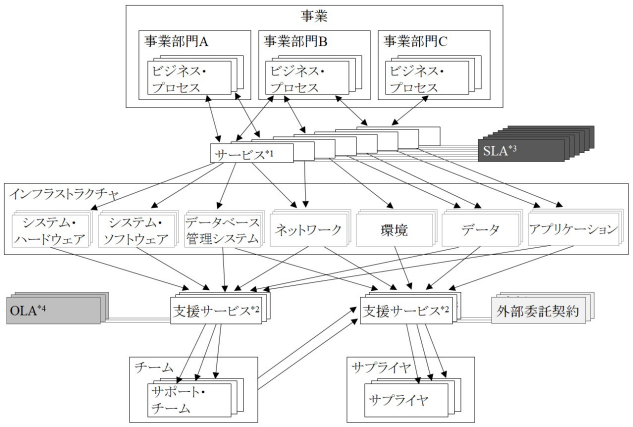
モデルは以下の手順で導出する：はじめに組織活動の因果関係を整理し，次に組織活動のモニタリング方法を整理し，最後にこれらを統合することでモデルを構築する.

ステップ 1. 組織活動の因果関係の整理

組織全体を俯瞰する方法の一つとして，事業構造から解釈する方法が挙げられる.

事業構造の例を図 1 に示す[9]. 事業は複数のビジネス・プロセスから構成され，ビジネス・プロセスは複数のサー

ビス―IT システムの利用を含む―により実現され，さらに IT システムはハードウェアなどのインフラストラクチャの各要素と，メンテナンスなどのインフラストラクチャを支えるサービスなどにより実現される．



*1 ここでの「サービス」には「ITシステム」または「ITシステムが実現する機能」が含まれる．
*2 サービスデスクやシステムメンテナンスなどの，ITシステムおよびその利用者を支援する作業が該当する．
*3 Service Level Agreement．サービスの提供者とその利用者の間で結ばれる，サービスのレベルに関する合意書．
*4 Operational Level Agreement．運用レベル契約や組織内SLAを指す．

図 1　事業の構成要素の関係（[9]を基に一部編集）
Figure 1　Relationship of business elements.

事業の構成要素は，各エージェントによる各活動の役割分担という観点から見ると，表 1 のように分類できる．

表 1　事業の構成要素の分類
Table 1　Classification of business elements.

エージェント	担当する役割	EC サイトでの例
人	1-1. IT システムに対する操作を実施する	・システム監視 ・システムメンテナンス ・EC サイトの障害対応
	1-2. IT システムを利用する作業を実施する	・注文内容の確認 ・商品の梱包 ・配送業者への引き渡し
	1-3. 上記以外の作業を実施する	―
IT システム	2-1. ビジネス・プロセスを実現する	・商品説明の表示 ・注文受付
	2-2. ビジネス・プロセスを実現する作業を支援する	1-2.の作業の進捗管理

図 1 と表 1 を踏まえると，IT システムに関する組織活動，すなわち事業を構成する各活動と各作業の因果関係は，図 2 のように簡略的に表せる．図 1 は，事業構造をトップからブレークダウンした記述であり，これは事業を実現するための条件を樹形構造で示すと解釈できる．したがって，これらの条件の因果関係に沿って，事業構造をボトムアップで見ると，図 2 のように整理できる．なお，図 2 は，「IT システムに対する操作」を起点としているため，各活動・各作業の因果関係によっては，表 1 の 1-3 に該当する要素の一部が表現されない可能性があることに留意する．

図 2　IT システムに関する組織活動の因果関係
Figure 2　Causal relationship of organization's activities.

ステップ 2. 組織活動のモニタリング方法の整理

表 1 のように，多くの組織では，組織活動を複数のエージェントが分担して実施していると考えられる．

したがって，組織活動は，各活動・各作業を担当する各エージェントによって分散してモニタリングされる(図 3)．例えば，システム担当者が，サーバの追加などの IT システムに対する作業を実施すると，IT システムの配置や状態が変化する．IT システムの状態が変化すると，IT システムが実現する機能の状態―図 1 でいうサービス―が変化する．このように，システム担当者は，作業のフィードバックとして，IT システムのモノの状態の変化をモニタリングし，機能の状態の変化もモニタリングする（表 1 の 1-1）．EC 営業担当は，商品の梱包作業のために IT システムの機能を利用すると，機能の利用可否と，機能による処理結果をモニタリングする（表 1 の 1-2 および 2-2）．顧客により機能

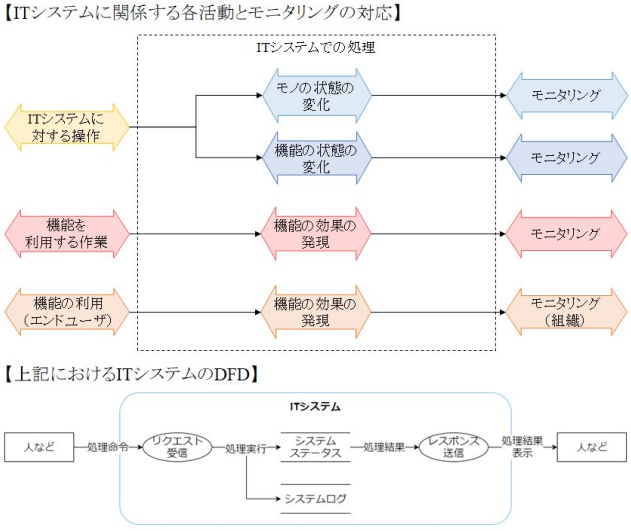


図 3　各活動のモニタリング
Figure 3　Monitoring of organization's activities.

が利用された場合には，その結果を組織はモニタリングし，例えば EC サイトの閲覧数や注文数などを EC 営業担当が確認する（表 1 の 2-1）．

ステップ 3. 組織全体としての状況認識のモデルの導出

ステップ 1 で導出した組織活動の因果関係に沿って，ステップ 2 で述べた組織活動のモニタリング方法により取得したデータを整理すると，組織全体を俯瞰する状況認識とその要素を記述するモデルを導出できる（図 4）．

状況認識の対象は，「IT システムに対する操作」，「IT システムの状態」，「作業／ビジネス・プロセス／事業の状態」に大きく分類できる．各対象は因果関係から次のように関連付けられる：IT システムに対する操作を行うと，その効果は即時に IT システムの状態に伝搬して，モノの状態すなわち配置や設定などが変化し，機能の状態が変化する．機能の効果は，任意のタイミングで機能を利用すると，機能が実現するビジネス・プロセスや機能を利用する作業に伝搬する．事業を構成する複数のビジネス・プロセスの状態の総和により，事業の総合的な状態が最終的に変化する．

状況認識に用いるデータと知識などは，組織活動の役割分担に基づき特定できる．例えば，システム担当者は，システムログをモニタリングし，システム構成の知識などを用いて「IT システムに対する操作→IT システムの状態」の状況認識を行う．EC 営業担当は，作業手順に基づき IT システムが実現する機能を利用し，「機能の状態→B)機能を利用する作業およびビジネス・プロセスの状態」の状況認識を行う．このように，各エージェントの役割と業務内容から，各対象の状況認識に用いるデータと知識を整理できる．

また，各活動のモニタリング指標はそれぞれ，事業状態の良し悪しの判断指標の一部であることを踏まえると，サイバー攻撃対応における状況認識と用いるデータや知識などは，多少の粒度の差異はあるものの，基本的には平時と同じであると考えられる．例えば，サイバー攻撃の手口とサイバー攻撃による IT システムの被害は，システムログと，システム構成やセキュリティに関する知識などに基づき解釈される．サイバー攻撃による各作業や事業への影響は，作業計画や事業構造などに基づき推測される．このように，本モデルを適用すると，サイバー攻撃対応における状況認識と用いるデータや知識なども整理できる．

4. 評価・考察

4.1 提案モデルの評価

3 章の提案モデルの妥当性を確認するため，架空の EC サイトを想定し，本モデルを用いてサイバー攻撃が発生したときの状況認識を表現できるかを評価する．

評価ステップ 1. 架空の EC サイトの設定

架空の EC サイトのシステム構成とワークフローの概要を図 5，図 6 に示す．エンドユーザは，EC サイトにアクセスして，商品情報 API を用いて商品を閲覧し，注文 API を用いて商品を注文する．EC 営業担当は，注文管理 API を用いて注文内容を確認し，商品を梱包し，商品を配送業者へ引き渡す．システム担当は，FW などのセキュリティ製品や死活監視ツールなどを用いて EC サイトとネットワークの状態をモニタリングし，異常を検知するとシステムログの調査などの対応を行う．なお，注文情報 DB には，

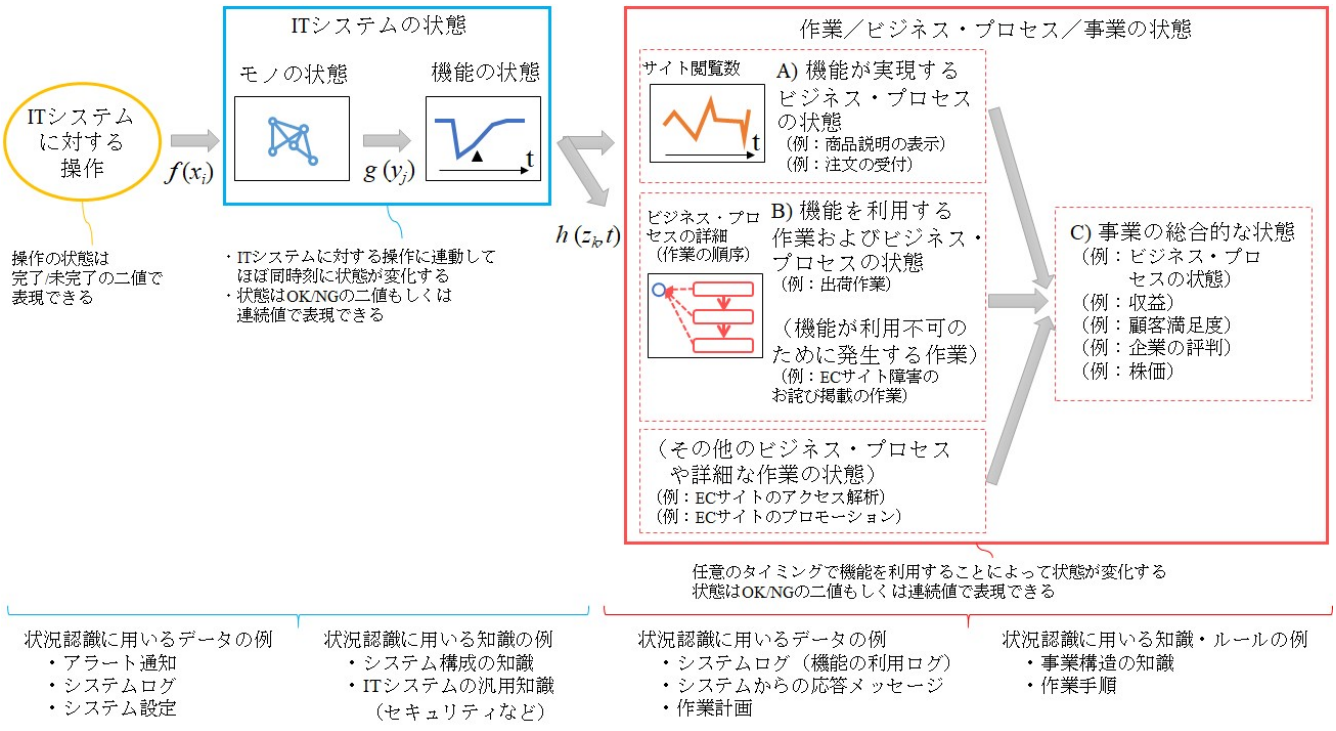


図 4　組織全体を俯瞰する状況認識とその要素を記述する提案モデル

Figure 4　Proposed model of for descripting organization’s activities and situation awareness.

注文した商品と数量の情報に加えて，注文者や配送先の住所・氏名などの個人情報が含まれるものとする．

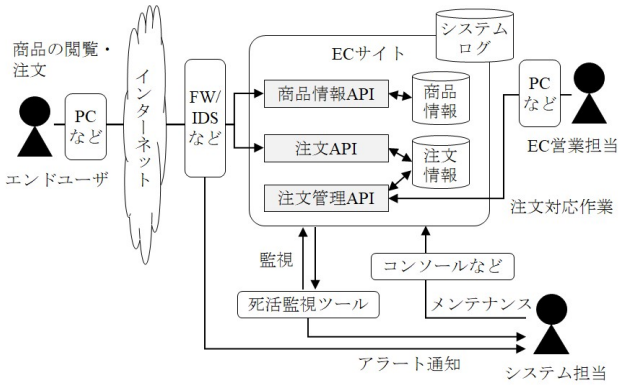


図 5　架空の EC サイトのシステム構成の概要
Figure 5　Overview of an EC system infrastructure.

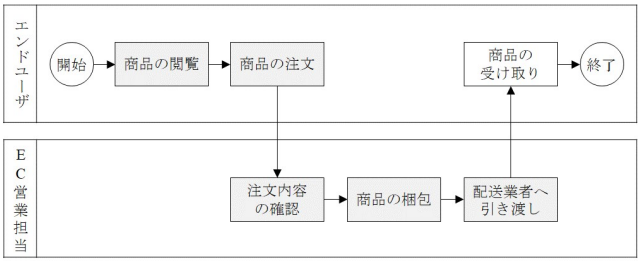


図 6　架空の EC サイトのワークフローの概要
Figure 6　Workflow of an EC business activities.

評価ステップ 2. EC サイトに対するサイバー攻撃の抽出

次に，架空の EC サイトに対するサイバー攻撃の脅威を，Fault Tree Analysis (FTA)を用いて簡易的に抽出する．サイバー攻撃の脅威を網羅的に抽出する方法としては，架空の EC サイトのシステム構成を詳細化した上での脅威モデリングが挙げられるが[10][11]，提案モデルはそこまでの詳細な分析を行わなくても適用できるため，本稿では厳密な脅威モデリングは省略する．

EC サイトに関する組織活動の FTA は図 7 のようになり，

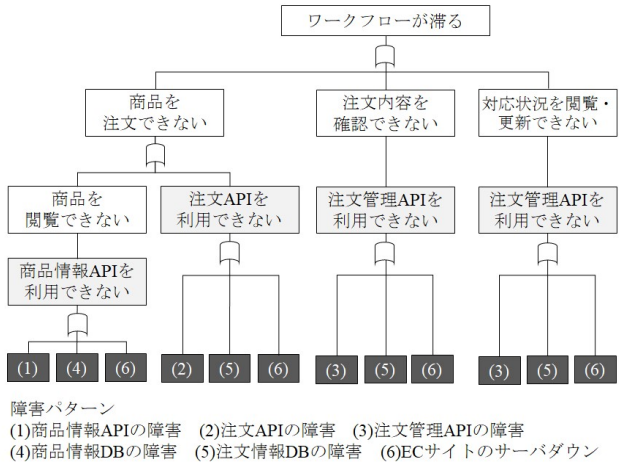


図 7　EC サイトに関する組織活動の FTA の例
Figure 7　FTA of an EC business activities

トップ事象に至る EC サイトの障害パターンを 6 つ抽出できる．FTA のトップ事象は，分析目的に応じて任意に設定できる．今回は，サイバー攻撃が発生したときの組織活動全体に対する影響とその状況認識を，提案モデルを用いて説明できるかを評価することが目的であるため，図 6 のワークフローが滞ることをトップ事象として選択した．

FTA で抽出した障害パターンを引き起こすサイバー攻撃の詳細を，IPA の情報セキュリティ 10 大脅威 2019 を参照して分類すると[12]，表 2 のようになる．今回は詳細な脅威分析を行っていないため，抽出したサイバー攻撃の手法には過不足の可能性が考えられるが，後続の評価ステップには大きな影響は与えないため，この粒度のままとする．

表 2　EC サイトの障害を引き起こすサイバー攻撃の例
Table 2　Examples of cyberattacks to an EC system.

項番	障害パターン	サイバー攻撃の例
(1)	商品情報 API の障害	①標的型攻撃による被害 ③ランサムウェアによる被害 ⑨脆弱性対応情報の公開に伴う悪用増加
(2)	注文 API の障害	①標的型攻撃による被害 ③ランサムウェアによる被害 ⑨脆弱性対応情報の公開に伴う悪用増加
(3)	注文管理 API の障害	①標的型攻撃による被害 ③ランサムウェアによる被害 ⑨脆弱性対応情報の公開に伴う悪用増加
(4)	商品情報 DB の障害	①標的型攻撃による被害 ③ランサムウェアによる被害 ⑨脆弱性対応情報の公開に伴う悪用増加
(5)	注文情報 DB の障害	①標的型攻撃による被害 ③ランサムウェアによる被害 ⑤内部不正による情報漏えい ⑦インターネットサービスからの個人情報の窃取 ⑨脆弱性対応情報の公開に伴う悪用増加 ⑩不注意による情報漏えい
(6)	EC サイトのサーバダウン	①標的型攻撃による被害 ③ランサムウェアによる被害 ⑥サービス妨害攻撃によるサービスの停止 ⑨脆弱性対応情報の公開に伴う悪用増加

補足：〇の中の数字は，情報セキュリティ 10 大脅威（組織）の順位を示す[12].

Vol.2019-GN-108 No.4
Vol.2019-SPT-33 No.4
2019/5/9

評価ステップ 3. 提案モデルの適用による，サイバー攻撃が発生したときの組織活動全体としての状況認識の表現

表 2 を要約して評価シナリオを 3 つ設定し（表 3），各々に対して提案モデルを適用したときに，組織全体としての状況認識がどのように記述されるかを評価する．

各シナリオにおける組織全体としての状況認識は，図 4 に示す提案モデルの各要素で記述すると，表 4 のように表現できる．なお，「IT システムに対する操作」は「サイバー攻撃」と読み替えた．また，シナリオ C の「注文情報 DB からの情報漏洩」は，情報漏洩した時点では API などの利用には影響はないが，将来的にシステム停止や報道発表などの事後対応の影響を受けると表現できる．

表 3　評価シナリオ

Table 3　Test cases for the model assessment.

シナリオ	サイバー攻撃	EC サイトの被害
A	①or③or⑨	いずれかの API の停止もしくはいずれかの DB の停止
B	①or③or⑥or⑨	EC サイトのサーバダウン
C	⑤or⑦or⑩	注文情報 DB からの情報漏洩

表 4　提案モデルの適用による，サイバー攻撃が発生したときの組織全体としての状況認識

Table 4　Organizational situation awareness in cyber incident by using the proposed model.

	サイバー攻撃（IT システムに対する操作）	IT システムの状態		作業／ビジネス・プロセス／事業の状態			
		モノの状態	機能の状態	A)機能が実現するビジネス・プロセス	B)機能を利用する作業	（その他の作業やビジネス・プロセス）	C)事業の総合的な状態
A-1-1	商品情報 API へのサイバー攻撃	商品情報 API の停止	商品情報 API の利用不可	エンドユーザの EC サイトの閲覧不可	変化なし ※事後対応の影響を受ける	変化なし ※事後対応の影響を受ける	・（顧客満足度の低下）
A-1-2	商品情報 DB へのサイバー攻撃	商品情報 DB の停止	商品情報 API の利用不可	エンドユーザの EC サイトの閲覧不可	変化なし ※事後対応の影響を受ける	変化なし ※事後対応の影響を受ける	・（顧客満足度の低下）
A-2-1	注文 API へのサイバー攻撃	注文 API の停止	注文情報 API の利用不可	エンドユーザの EC サイトからの注文不可	変化なし ※事後対応の影響を受ける	変化なし ※事後対応の影響を受ける	・売上の減少 ・（顧客満足度の低下）
A-2-2	注文情報 DB へのサイバー攻撃	注文情報 DB の停止	注文情報 API の利用不可， 注文管理 API の利用不可	エンドユーザの EC サイトからの注文不可	・EC 営業担当の注文確認作業の実施不可 ・EC 営業担当の商品梱包作業の実施不可	変化なし ※事後対応の影響を受ける	・売上の減少 ・出荷の遅延 ・（顧客満足度の低下）
A-3-1	注文管理 API へのサイバー攻撃	注文管理 API の利用不可	注文管理 API の利用不可	変化なし ※事後対応で影響を受ける	・EC 営業担当の注文確認作業の実施不可 ・EC 営業担当の商品梱包作業の実施不可	変化なし ※事後対応の影響を受ける	・出荷の遅延 ・（顧客満足度の低下）
B	EC サイトへのサイバー攻撃	全 API，全 DB の停止	全 API，全 DB の利用不可	・エンドユーザの EC サイトの閲覧不可 ・エンドユーザの EC サイトからの注文不可	・EC 営業担当の注文対応作業の実施不可 ・EC 営業担当の商品梱包作業の実施不可	変化なし ※事後対応の影響を受ける	・売上の減少 ・出荷の遅延 ・（顧客満足度の低下）
C	注文情報 DB へのサイバー攻撃	注文情報 DB のアクセス権限の変更	変化なし ※事後対応の影響を受ける	変化なし ※事後対応の影響を受ける	変化なし ※事後対応の影響を受ける	変化なし ※事後対応の影響を受ける	変化なし ※事後対応の影響を受ける

また，各人のサイバー攻撃の状況認識と状況認識に用いるデータは，図 5 に記載の役割と図 6 のワークフローに従うと，表 5 のようにマッピングできる．

表 5　サイバー攻撃が発生したときの各人の状況認識
Table 5　Each person's situation awareness in cyber incident.

	サイバー攻撃（IT システムに対する操作）	IT システムの状態	作業／ビジネス・プロセス／事業の状態
システム担当	○	○(1)(2)	△(4) ※部分的
EC 営業担当	—	△(3) ※部分的	△(5)(6) ※部分的
（エンドユーザ）	—	△(3) ※部分的	△(6) ※部分的
状況認識に用いるデータ（モニタリングするデータ）	・アラート通知 ・システムログ	(1)アラート通知 (2)システムログ (3)EC サイトや API のエラー表示	(4)システムログ（API の利用傾向など） (5) EC サイトや API のエラー表示 (6)作業の進捗状況

4.2　提案モデルの考察

提案モデルは，4.1 の評価範囲に関しては，サイバー攻撃発生時の組織全体としての状況認識や状況認識に用いるデータの実態に即すると考えられ，妥当であると判断する．

4.1 の評価ステップを踏まえると，提案モデルの適用条件と課題として下記が挙げられる．

適用条件 1：システム構造を把握していること

提案モデルは，脅威分析により求められる各要素と要素間の因果関係を取り込むことができる．今回の評価ステップでは省略したが，脅威モデリングを用いて脅威分析を詳細に行うと，「IT システムに対する操作→IT システムの状態→作業／ビジネス・プロセス／事業の状態」の因果関係を網羅的に抽出できる．この分析結果を，提案モデルの「IT システムに対する操作」，「IT システムの状態」，「作業／ビジネス・プロセス／事業の状態」の各要素に当てはめると，分析結果を端的に要約できる．

このことは反面，提案モデルを有効に使うには，システム構造を把握している必要があるともいえる．特に「モノの状態→機能の状態」は，事業影響を導く上で肝となる箇所であり，その因果関係は冗長構成や分散構成などのシステム構成に依存する．したがって，本モデルを用いて組織全体の状況認識を適切に表現するには，脅威分析などを通じて，機能の動作条件を理解することが不可欠となる．

適用条件 2：事業構造を把握していること

提案モデルは，事業構造に基づき構築しているという性質上，提案モデルを適用するには，事業構造を把握していることが条件となる．もしくは，今回の評価ステップで実践したように，主要なワークフローを把握しておく必要がある．もし事業構造を把握していなければ，提案モデルを用いても，サイバー攻撃による事業影響の説明は部分的もしくは不適切なものとなる可能性がある．

適用条件 3：事業構造に各役割を対応付けていること

提案モデルは，事業構造を構成する各活動に，エージェントの各役割が対応付けられると想定している．

そのため，事業構造に対応する部署・人などを把握していることが，提案モデルの適用条件として挙げられる．

事業構造と各役割の対応を把握していれば，各人が組織活動全体のうちのどの箇所に関するデータをモニタリングして状況認識しているかを容易に特定できる．例えば表 5 のように，平時およびサイバー攻撃のインシデント発生時に，各人が何をモニタリングして状況認識しているかを簡単に整理できる．また，各人の状況認識を適切に統合して，組織全体としての状況認識を表現することもできる．

課題 1：状況認識に用いるデータや知識などの検証

提案モデルでは，各役割は担当する各活動を行ってモニタリングし，モニタリングしたデータを組織活動の因果関係に基づき整理することで，組織活動全体を俯瞰する状況認識を記述できると想定している．

しかし実際に，提案モデルが想定するような，データのモニタリングや統合方法により状況認識がなされているかどうかは，現時点では検証できていない．

提案モデルの妥当性と利便性を高めるためには今後，いつ・誰が・何のデータをモニタリングして・どのような知識などを用いてデータを解釈し分析して状況認識しているかの実態を調査し，モデルを精査する必要があると考える．

課題 2：各種影響の分析精度

提案モデルは，IT システムに対する操作を起点に，組織活動の因果関係に基づき組織活動の全体像を表現している．

そのため，IT システムに関する情報を充分に収集していないときに，提案モデルを適用しても，サイバー攻撃による各種影響を適切に表現できない可能性がある．特に，サイバー攻撃を検知した直後や標的型攻撃の初期活動など，状況認識に必要な情報が揃ってなく，IT システムの被害範囲や攻撃者の目的を把握していない状況においては，各種影響を実際より過小評価してしまう恐れがある．

また，サイバー攻撃による事業影響を精度よく見積もるには，「機能の状態→作業／ビジネス・プロセス／事業の状態」に関して，システムログや組織活動のログなどの統計分析を行う必要がある．因果関係が示すのは定性的な影響度であるため，定量的な影響度を求めるには，統計分析により機能の利用傾向などを算出・予測する必要がある．

したがって，提案モデルは，組織活動の各種データの因果関係を整理するための枠組みとして利用できるが，各種

影響の分析精度に関しては現時点では保証できない．各種影響の分析方法として確立するには，モデルの論理構造に起因する分析結果のブレの問題を解決する必要がある．

5. 状況認識の支援方法の検討

事業構造と組織構造を考慮すると，サイバー攻撃のインシデント対応における役割分担と担当範囲は，平時の役割と担当範囲を踏襲することが多いと考えられる（図 8）．

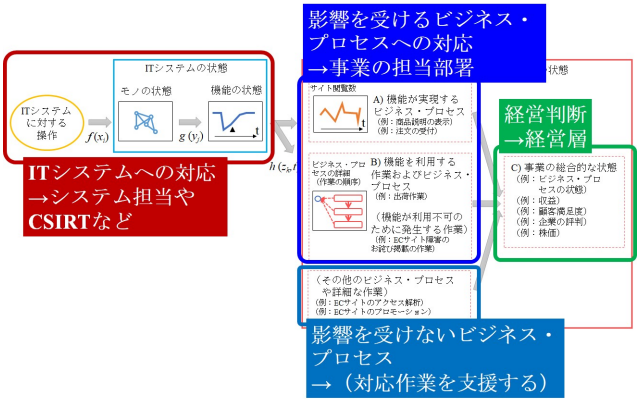


図 8　インシデント対応における役割分担

Figure 8　Division of incident response activities.

また，担当する役割に応じて，各人が必要とする情報の種類や粒度には偏りがあると考えられる．分業による専門化を考慮すると，自分の役割を遂行するために必要な情報は詳細に把握していることが求められるが，担当でない役割に関しては，概要の理解は必要であるが詳細の理解までは求められないことがある．また，各人が自分の役割の情報のすべてを他者と共有しようとすると，組織全体で見ると情報量が膨大なものとなり，重要な情報を識別しづらくなる．したがって，情報には，状況認識の統一のために必要な情報と，担当する役割のために必要な情報という 2 つの分類が存在し，後者は役割によって異なると考えられる．

これらを踏まえると，提案モデルの分類方法に基づき，組織全体としての概況情報とともに各人の役割に対応する箇所の詳細情報を提示することで，状況認識を支援できると考える（表 6）．概況情報とは，提案モデルの各分類の正常／異常程度の情報量で充分であり，組織全体から見たインシデント対応の各作業の必要性の理解を促進する．詳細情報とは，各役割が各々の担当作業の実施に必要とする粒度の定量的および定性的な情報を指す．

このように，役割ごとに必要な情報とその粒度が異なることを前提とした情報提示により，インシデント対応における効果的な情報共有と状況認識を支援できると考える．

表 6　各人の状況認識を支援する情報

Table 6　Information for each person's situation awareness.

	サイバー攻撃（IT システムに対する操作）	IT システムの状態	作業／ビジネス・プロセス／事業の状態
CSIRT	◎	◎	○
事業の担当部署	○	○	◎ ※担当範囲
経営層	○	○	◎ ※事業の状態

凡例　◎：詳細情報を提示する　○：概況情報を提示する

6. 今後の展望

本稿では，サイバー攻撃のインシデント対応における組織の状況認識を支援することを目的に，組織全体としての状況認識に必要な要素を記述するモデルを構築した．

モデルの妥当性検証と実用化に向けて今後，実際のシステムに対するリスクアセスメントや過去のサイバーインシデントの事例分析，インシデント対応訓練などにモデルを適用し，モデルの課題の抽出と解決を試みる予定である．

参考文献

[1] “ISO 22320:2018 Security and resilience -- Emergency management -- Guidelines for incident management”. https://www.iso.org/standard/67851.html, Nov. 2018, (参照 2019-3-12).

[2] National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf, Apr. 2018, (参照 2019-3-11).

[3] Forum of Incident Response and Security Teams. FIRST CSIRT Framework Version 1.1. https://www.first.org/education/csirt_service-framework_v1.1, May, 2017, (参照 2019-3-11).

[4] Endsley, M.R.. Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors Journal 37(1), p.32-64, Mar. 1995.

[5] Stanton, N.A., R. Stewart, D. Harris, R.J. Houghton, C. Baber, R. McMaster, P. Salmon, et al. Distributed Situation Awareness in Dynamic Systems: Theoretical Development and Application of an Ergonomics Methodology. Ergonomics 49, 1288-1311, 2006.

[6] Kitchin, J., Baber, C.A.. A comparison of shared and distributed situation awareness in teams through the use of agent-based modelling. Theoretical Issues in Ergonomics Science, 17:1, 8-41, 2016.

[7] Stanton, N.A.. Distributed situation awareness. Theoretical Issues in Ergonomics Science, 17:1, 1-7, 2016.

[8] 池田美穂，高橋慧，上川先之，倉恒子，爰川知宏，岸晃司. サイバー攻撃のインシデント対応におけるリスク認知とコミュニケーションの支援方法の検討．情報処理学会研究報告. Vol.2019-SPT-32 No.23, May, 2019.

[9] itSMF Japan 翻訳. ITIL 2011 edition：サービスデザイン. TSO, http://www.itsmf-japan.org/books/index.html, 2011.

[10] Shostack, A.. Threat Modeling: Designing for Security. Wiley, Feb. 2014.

[11] Threat Model Analysis. https://docs.microsoft.com/ja-jp/biztalk/core/threat-model-analysis, Jun. 2017, (参照 2019-3-14).

[12] 情報処理推進機構．情報セキュリティ 10 大脅威. 2019https://www.ipa.go.jp/security/vuln/10threats2019.html, Mar. 2019, (参照 2019-3-14).