サイバー攻撃発生時の状況認識における平時のマネジメント手法の適用方法の検討

池田 美穂 [1,*1]　爰川 知宏 [1,*2]

概要：サイバー攻撃が発生したとき，組織は，事業継続のために，インシデント対応と通常業務を両立させなければならない．インシデント対応と通常業務とでは，活動目的が異なるため，利害が対立し，目標に滞りなく到達するのが難しくなることがある．このような事態を避けるには，関係者間で，サイバー攻撃によって組織全体として何が現在起こっているか，今後起こる可能性が高そうかという状況認識を共有し，何をするべきかという活動方針を意識合わせすることが重要である．しかし，組織が業務効率化のために行う分業化によって各人の知識には偏りがあるために，状況認識のために何の情報を収集するべきか，収集した情報をどのように分析・評価するべきかがわからないという課題がある．これに対し，例えば，作業計画やシステムログなどの，平時のマネジメントで用いるモニタリングデータを，事業構造に沿って関連付けて分析・評価すると，この課題が緩和され，サイバー攻撃発生時により適切に状況認識できるようになる．本稿では，平時の各種マネジメントにおける管理対象と管理方法を，サイバー攻撃発生時の状況認識に用いる情報や分析・評価方法として容易に適用するための方法論を提案する．

キーワード：サイバー攻撃，状況認識，インシデント対応，事業継続，マネジメント

Application of Ordinary Operational Management Methods to Situation Awareness in Cyber Incident Response

Miho Ikeda[1,*1]　Tomohiro Kokogawa[1,*2]

Abstract: When an organization comes under cyberattack, it should cope with both incident response and normal operation for the sake of its business continuity. These activities sometimes conflict due to the difference in purpose of the activities, so may not be taken smoothly. To avoid such a situation, it is important to share organizational situation awareness and action plans among the people concerned. However, it is difficult to build organizational situation awareness properly because the information and analytics methods required for organizational situation awareness have been unclear. We propose an application of operational management methods taken at ordinary times in order to facilitate organizational situation awareness in cyber incident response. Business operations consist of many activities, and these activities are monitored and managed in the form such as work plans and system logs. So organizational situation awareness in cyber incident response can be built by relating and analyzing these data along the operational structure.

Keywords: Cyberattack, Situation awareness, Incident response, Business Continuity, Management

1. 研究背景

サイバー攻撃を受けたとき，組織が実行するインシデント対応の良し悪しによって，組織に対する社会的評価が大きく変化し，事業継続そのものが左右されることがある．例えば，2019 年 7 月に発生した 7pay（セブンペイ）における不正利用[1]では，認証関連のセキュリティ設計の不備が根本の原因ではあるものの，ユーザアカウントへの不正アクセスが確認された後の，入金機能停止やパスワードリセットなどの対応は，不正利用の被害拡大防止や連携サービスへの被害波及防止の観点からは，より早期に実施するべきであった．結果的に，7pay のサービスを廃止せざるを得ない状況に追い込まれた．一方，2018 年 12 月に PayPay（ペイペイ）で発生した不正利用[2]では，クレジットカード登録時の本人認証の脆弱性を悪用した手口であったが，対応方法としてクレジットカード登録時におけるセキュリティコードの入力ミスの回数制限の設定，抜本的対策として本人認証サービス（3D セキュア）の導入による認証強化など，問題に迅速に対応していく姿勢を見せたことによって，ユーザ離れを回避し，サービスの存続に成功している．

適切なインシデント対応を行うには，組織全体の状況を把握することが重要である．サイバー攻撃を受けたとき，組織は，事業継続のために，インシデント対応と通常業務を両立しなければならないが，これらの活動は利害が対立することがある．例えば，2015 年 5 月に発生した日本年金機構における個人情報流出[3]では，標的型メール攻撃が段階的に進行する中で，インシデント対応としてインターネット接続を遮断するべき状況が幾度もあったが，ルール（判断者，判断基準，手順）が定まっていなかったために，イ

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

*1 miho.ikeda.da@hco.ntt.co.jp
*2 tomohiro.kokogawa.sc@hco.ntt.co.jp

ンターネット接続を遮断したときの通常業務への影響を恐れて，対応の実施判断ができず適切な対応時期を逃してしまった．このような事態を避けるには，サイバー攻撃によって組織全体として現在何が起こっているか，今後起こる可能性が高そうか，どのような対応を実施すると何に対して効果や二次リスクがあるかを把握した上で，組織全体として最適な対応方法を選択することが重要である．

筆者らはこれまでに，サイバー攻撃が発生したときに，各関係者が円滑に協働して各種作業を行えるよう支援することを目的に，組織全体の状況認識を記述するモデルや関係者間のコミュニケーション方法を検討してきた[4][5].

本稿では，サイバー攻撃を受けた組織が組織全体の状況を把握して適切な対応計画を策定できるよう支援することを目的に，平時の各種マネジメントにおける管理対象と管理方法を適用することでサイバー攻撃発生時の状況認識を実現する方法論を提案する．

本稿の構成は以下のとおりである．2 章にて，インシデント対応における問題の原因を分析する．3 章にて，問題を解決するための既存手法とその課題を挙げ，本研究で解く課題を具体化する．4 章にて提案手法の導出を行う．5 章にて本研究の今後の展望について述べる．

2. 問題

2.1 インシデント対応における問題の原因分析

インシデント対応で失敗する箇所は，人の思考や行動のプロセスに沿って分類すると，大きく 3 つに分けられる．

- 状況認識における失敗
- 意思決定における失敗
- 行動における失敗

上記の分類は，Endsley の状況認識モデル[6]（図 1）を参考にしたものである．この状況認識モデルは，状況認識を誤ると，後続の意思決定も選んだ行動も，実際の状況に対しては不適切なものになることを示している[7].

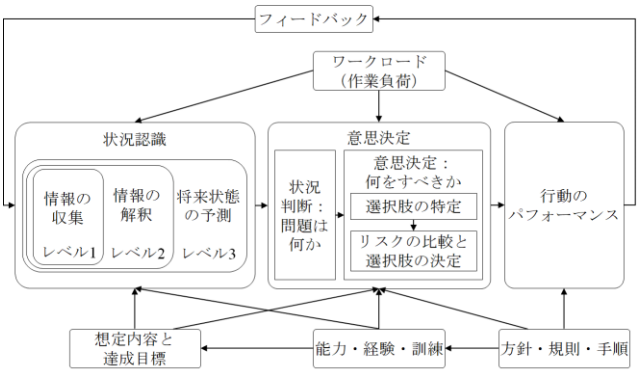

図 1 状況認識モデル（[7]を参考に[6]の Figure1 を加工）
Figure1 Model of situation awareness ([6] [7])

インシデント対応の失敗の原因は，ヒューマンファクターズ分野における事故原因に関するモデルを参照すると[8][9]，一意に定まるものではなく，複数の要因が相互作用することによって生じると解釈できる．

状況認識モデルのうち，思考に関する状況認識～意思決定の箇所に焦点を絞ると，次のような要因が挙げられる．

一つは，インシデント対応の手順の不備，具体的には，いつ・誰がどのようなデータを収集しどのように分析・評価することで，状況を把握したり対応方法を判断したりするかを定めていないことである．インシデント対応の流れは，例えば次のようになる：サイバー攻撃による被害やインシデント対応による影響が小さく，現場層で判断できる範囲に関しては，現場層の裁量で対応を実施する．現場層では対応方法の判断が難しい場合には，管理層，経営層と，状況に応じて段階的により上位の役職に報告して判断や指示を仰ぐ[10]．このような流れを迅速かつ適切に行うためには，状況認識に必要な情報の収集・分析・評価方法，各役職の判断内容と判断基準，エスカレーションの判断基準などの手順を整備することが有効である．日本年金機構での個人情報流出では，このような手順が十分に整備されていなかったため，判断と対応が遅れた[3].

インシデント対応の手順に不備が生じる理由を掘り下げると，知識の不足が要因の一つとして考えられる．状況認識モデルで記述されるように，人は，知識や経験などに基づき，収集した情報を解釈して状況を理解し，何をするべきかを判断して行動する．しかし，システム部門は IT システムの保守運用，営業部門は IT システムを利用したマーケティングというように，組織では業務効率化のために分業化・専門化を行うために，各人の知識には偏りが生じている[4]．このため，知識がある範囲に関しては，情報を適切に解釈して状況を把握できるが，担当外の業務など知識のない範囲に関しては，情報が意味するところを理解できず，状況を見誤ることがある[11][12]．複数人の知識を持ち寄ったとしても，知識が分散していて各領域を適切に関連付けることが難しいため，状況認識および後続の意思決定のために，何の情報を収集するべきか，収集した情報をどのように分析・評価するべきかがわかりづらくなる．このような状況は，サイバー攻撃発生時に限らず，インシデント対応の手順を検討する際にも発生する可能性があり，手順の不備が生じやすくなる一因となる．

以上をまとめると，インシデント対応の手順の不備や，知識の不足，分業という仕組みは，インシデント対応の失敗を引き起こす要因になっていると考えられる．

2.2 インシデント対応における状況認識の重要性

2.1 から，インシデント対応の失敗を防ぐには，起点となる状況認識における失敗を防ぐことが重要であるといえる．状況認識を適切に形成するには，状況認識の方法，具体的には状況認識に必要な情報とその収集・分析・評価方法を形式化することが有効であり，それを簡便に行えるようにする方法が求められている．

3. 既存手法

3.1 インシデント対応関連ガイドライン

サイバー攻撃発生時に組織が収集するべき情報とその分析・評価方法は，例えば NIST サイバーセキュリティフレームワーク[13] にて概略が整理されている．同文書では，サイバーセキュリティ対策の流れを,「識別（Identify）」,「防御（Protect）」,「検知（Detect）」,「対応（Respond）」,「復旧（Recover）」という 5 つのフェーズで分類し，各フェーズでやるべきことの概略を記載している．サイバー攻撃発生時の状況認識の手順は，特に「検知」と「対応」で記述されている．

3.2 既存手法の課題

既存手法に対しては，実用性の観点から課題を 2 つ指摘できる．

1 つ目は，インシデント対応の場面にすぐには導入できず，事前の手間が多くかかることである．例えば，NIST サイバーセキュリティフレームワークでは，サイバー攻撃が発生した際に，サイバー攻撃による影響を算出することの必要性と手順の概略は記載しているが，どのような情報を収集・分析・評価すればよいかの詳細は説明していない．詳細を知るには, リスク分析などの専門知識を有する人が，同文書で参考文献として挙げられている資料を読み込む必要があり, 非常に手間がかかる．なお, このような手間は，他の規格やガイドラインを参照した場合にも発生する．

2 つ目は，インシデント対応と通常業務との両立の観点が抜けていて，サイバー攻撃発生時に実際に組織が必要とする情報を網羅していないことである．サイバー攻撃は，進行状況によっては，IT システムへの被害だけでなく，IT システムを利用している業務・事業への影響が出ることがある．これらへ迅速に対応するには，複数の人・部署の協力が不可欠である．一方，組織は事業継続のために，通常業務も実施しなければならない．インシデント対応のリソースを常備していない組織では，突発的なインシデント対応と計画済みの通常業務との間でリソースを配分する必要がある．しかし，どの規格やガイドラインも，特定の領域に特化していて，組織全体での優先順位付けやリソース配分を最適化するために，領域を横断してどのような情報を収集･分析･評価すればよいかについては記述していない．

3.3 本研究が扱う課題

本研究では，事業の実現という組織の本来の目的を踏まえて，サイバー攻撃を受けたときもインシデント対応と通常業務を両立することが重要であると考え，インシデント対応と通常業務を両立する対応計画を策定するために必要な状況認識を容易に実現する方法を検討する．

4. 提案手法

4.1 着目する観点

サイバー攻撃発生時に必要な状況認識の実現方法の検討に入る前に，そもそもインシデント対応の目的は何であるかを，事業継続の観点から整理する．

組織は，製品・サービスを生産または提供する事業を営んでおり，事業の中断・阻害などを引き起こすインシデントが発生した後も，製品・サービスを提供し続けることを社会から期待されている．これを実現する組織の能力を事業継続[14]と呼び，イメージを時系列で表現すると図 2 のようになる．また，インシデント発生後に，組織の機能すなわち製品・サービスを生産または提供する事業活動のレベルを早期復旧させるために必要な一連の行動を，危機対応もしくはインシデント対応と呼ぶ[15][16].

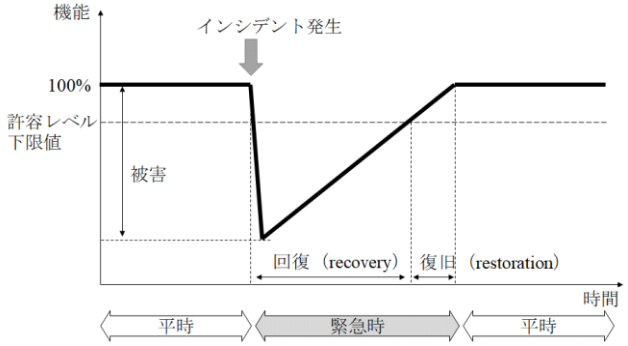

図 2 事業継続のイメージ（[16][17]を参考に筆者作成）
Figure2 Overview of business continuity ([16][17]).

図 2 を見ると，インシデントの発生を検知したり被害の大きさを把握したりするには，機能の状態を平時から継続してモニタリングしている必要があることがわかる．機能の状態をモニタリングしていなければ，平時すなわち状態が正常であるかも，緊急時すなわち状態が異常であるかの判別ができず，また被害の大きさを測ることもできない．

インシデント対応の目的は機能の状態を早期に回復させることであることと，そのためには機能の状態の継続的なモニタリングが必要なことを踏まえると，サイバー攻撃発生時の状況認識に関して, 次の 2 つの仮説が立てられる:

仮説 1: サイバー攻撃発生時における状況認識とは，組織が平時に管理している対象の状態とそれに関連する情報を把握することである．

仮説 2: サイバー攻撃発生時における状況認識は，組織が平時において管理対象を管理するために用いる方法を通じて実現できる．

簡単に言うと，サイバー攻撃発生時に必要な状況認識を実現するために，情報の収集・分析・評価方法を新たに導入する必要はなく，組織が平時に既に実施しているマネジメント手法を活用することで，サイバー攻撃発生時に必要な状況認識が実現できると考える．というのも，組織は平時に，機能の状態および機能の状態を変化させる可能性のある物事などを把握することで管理を行い，事業継続を実現している．これは，サイバー攻撃発生時に，インシデント対応と通常業務を両立する対応計画を検討するために必

要な状況認識の内容そのものであると考えられる．

上記の仮説を検証するために，下記の順で検討を進める．

(1) 状況認識における情報の収集・分析・評価の結果は，対応計画を策定する際の材料になる．したがって，インシデント管理プロセス[15]などを参照して，対応計画の策定に必要な情報を提供するという観点から，サイバー攻撃が発生したときに必要とされる状況認識の要件を整理する．

(2) 組織は，事業活動を管理しやすい観点や単位に分割して管理することで事業を実現している．このような組織が平時に行っている各種マネジメントの管理対象と管理方法を，ビジネス業績管理[18]やビジネスプロセス管理[19][20]などの考え方を参照して整理する．

(3) (1)と(2)を比較して，平時の各種マネジメントにおける管理対象と管理方法を，サイバー攻撃発生時の状況認識に用いる情報や分析・評価方法として適用する方法を導出する．

(4) (3)で導出した提案手法の検証方法を検討する．

4.2 提案手法の導出

4.2.1 サイバー攻撃発生時の状況認識の要件の整理

時系列に沿った状況認識の内容の分類

サイバー攻撃は，時間が経過すると，被害を受ける IT システムの範囲や影響を受ける業務・事業の範囲が拡大する可能性があるため，適切に対応するには，時系列で状況を把握・予測することが重要である．

状況認識モデル[6]やインシデント管理プロセス[15]，リスクマネジメントプロセス[21]を参照すると，対応計画（対応方法やリソース配分，実施時期などを記載したもの）を決定するまでに必要な状況認識の内容は，下記のように分類できる．

- 現在～将来の分析・評価
  - 現在何が起こっているか
  - 今後何が起こりそうか
- 対応計画の分析・評価
  - どのような対応方法があるか
  - いつ・どの対応方法を実施すると，どのような効果や二次リスクが起こりうるか

なお，時系列の各タイミングにおける物事の状況は，それぞれ複数の可能性が考えられる．未来が不確かで一意に定まらないのはもちろんのこと,「現在何が起こっているか」に関しても，情報を十分に収集・分析・評価していない段階では，状況を断定できないためである．

状況認識は，時間経過に伴い繰り返し実行してアップデートし，例えばサイバーキルチェーン[22]を参考にして，対応方法が変わるタイミングとそのときの状況を把握・予測すると，今後の見通しがついて，プロアクティブな対応を効果的に実施できるようになる．また，サイバー攻撃が進行した場合も慌てずに対応できるようになる（図 3）．

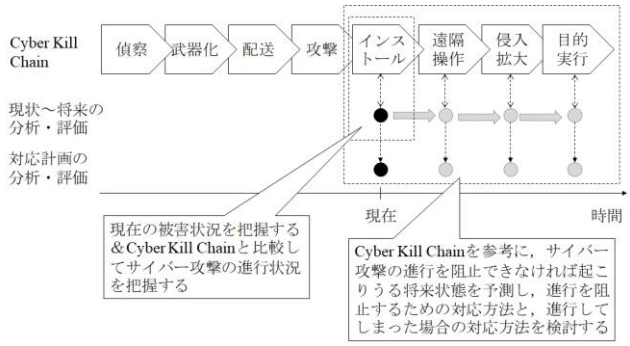

図 3 時系列に沿った状況認識の内容のイメージ

Figure3 Time-line of situation awareness.

対応計画策定の観点からの状況認識の内容の分類

リスクアセスメントの考え方[21]や，プロジェクトマネジメントの方法[23]を参考にすると，対応計画を策定するための材料として，下記を把握している必要がある．

- 対応対象の候補
- 対応の重要度
- 対応目標
- 対応方法とその効果または二次リスク
- 対応する際の制約条件

「対応対象の候補」とは，何らかの対応が必要かもしれないという対象を単純にリストアップしたものであり，IT システムや通常業務などの組織が管理する物事とその状態が該当する．なお，重要度や優先度などの評価はここには含まないものとする．

「対応の重要度」とは，事業継続の観点から対応する必要性がどの程度であるかを示す指標であり，例えば高・中・低の 3 段階や数値などの尺度で表現する．対応の重要度は，事業継続計画を策定する過程で事業影響度分析を行っていると想定されるため[14]，その分析結果を参照すればよい．なお，対応の実現性を加味した重要度は，後述の「対応する際の制約条件」を把握した上で検討するものであるため，この項目には含まないものとする．

「対応目標」とは，対応方法を具体的に検討するために必要な要素で，対応対象の候補の状態を，いつまでに・どの程度の状態にするかという目標を指す．事業継続計画などで定められている目標復旧レベルや目標復旧時間を参照してもよいし，新たに設定してもよい．

「対応方法とその効果または二次リスク」とは，対応目標を実現するための方法と，その方法を実施した場合のリスクを示したものであり，前述の「時系列に沿った状況認識の内容の分類」における「対応計画の分析・評価」の要素と同一である．

「対応する際の制約条件」とは，対応方法の実行可否や実行順番を決定づける要素であり，インシデント対応や通常業務を行うために必要な人員・スキル・機器・費用・所要時間などのリソースが該当する．また，参考情報として，

現在のリソースの状況を記載してもよい．

事業構造に基づくサイバー攻撃の被害・影響の伝搬構造

システムアーキテクチャの考え方を参照すると[24]，事業構造とその因果関係は，図 4 のように整理できる[5]．

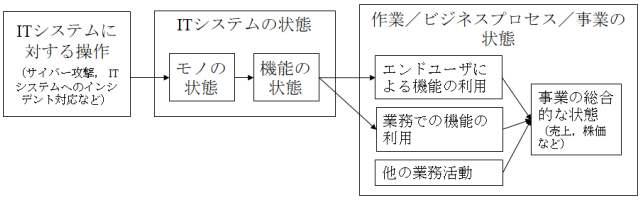

図 4 事業の構成要素の因果関係（[5]を一部加工）

Figure4 Causal relationship of organization’s activities [5].

図 4 から，サイバー攻撃による被害や影響は，「モノの状態→機能の状態→エンドユーザによる機能の利用／業務での機能の利用→事業の総合的な状態」の順序で伝搬することが分かる．したがって，サーバやルータなどの，サイバー攻撃を受けたモノが特定できれば，モノが実現する機能の被害や，業務・事業への影響の範囲も特定できる．なお，「IT システムの状態→作業／ビジネスプロセス／事業の状態」の因果関係に関しては，厳密にはシステム構成を考慮する必要がある．例えば，サーバが冗長構成や分散構成を取っている場合は，サイバー攻撃によってあるサーバが停止しても，代替のサーバが動作していれば，機能は正常に動作するため，機能を利用する作業やビジネスプロセス，事業への影響は発生しないことがある．

状況認識の要件の整理

以上を踏まえると，サイバー攻撃発生時に求められる状況認識は，表 1 のように整理できる．縦の行の項目は，図 4 の事業の構成要素に対応しており，任意の IT システム，例えば現在サイバー攻撃を受けているシステムを起点に，作業やビジネスプロセスをこの項目に従って分類すると，事業の各要素を網羅的にリスト化できる．横の列の項目は，「時系列に沿った状況認識の内容の分類」と「対応計画

表 1 サイバー攻撃発生時に求められる状況認識の要件と記入例

Table1 Detail of organizational situation awareness under cyberattack.

状況認識の対象 ＼ 状況認識の内容		現状の分析・評価				対応計画の分析・評価			
		対応対象の候補		対応の重要度	リソースの現状	対応目標	対応方法		対応する際の制約条件
		現在何が起こっているか	今後何が起こりそうか				どのような対応方法があるか	対応方法の効果と二次リスク	
ITシステムに対する操作	サイバー攻撃	サイバー攻撃の手法など	サイバー攻撃の手法など	事業影響度分析を参照する	（ITシステム対応する人員の稼働状況など）	目標復旧レベル・目標復旧時間など	何もしない*1/ ITシステム対応の内容*2	状態継続（サイバー攻撃の継続）/ 対応による状態変化（サイバー攻撃の遮断など）	必要リソースなど
ITシステムの状態	モノの状態	被害あり・被害内容	被害あり・被害内容	事業影響度分析を参照する	（ITシステム対応する人員の稼働状況など）	目標復旧レベル・目標復旧時間など	何もしない*1/ ITシステム対応の内容*2	状態継続（被害あり・被害内容）/ 対応による状態変化の様子（暫定復旧，完全復旧など）	（ITシステム対応の制約条件を引き継ぐ）
		被害なし	被害あり・被害内容					被害なし/ 対応による二次リスクの有無とその様子	
			被害なし						
	機能の状態	被害あり・被害内容	被害あり・被害内容	事業影響度分析を参照する	（ITシステム対応する人員の稼働状況など）	目標復旧レベル・目標復旧時間など	何もしない*1/ ITシステム対応の内容*2	状態継続（被害あり・被害内容）/ 対応による状態変化の様子（暫定復旧，完全復旧など）	（ITシステム対応の制約条件を引き継ぐ）
		被害なし	被害あり・被害内容					被害なし/ 対応による二次リスクの有無とその様子	
			被害なし						
作業／ビジネスプロセス／事業の状態	エンドユーザによる機能の利用	影響あり・影響内容	影響あり・影響内容	事業影響度分析を参照する	（需要の推定など）	目標復旧レベル・目標復旧時間など	何もしない/ ITシステム対応の内容*2/ 代替手段の内容	状態継続（影響あり・影響内容）/ 対応による状態変化の様子（暫定復旧，完全復旧など）	必要リソースなど
		影響なし	影響あり・影響内容					影響なし/ 対応による二次リスクの有無とその様子	
			影響なし						
	業務での機能の利用	影響あり・影響内容	影響あり・影響内容	事業影響度分析を参照する	当該業務を行う人員の稼働状況など	目標復旧レベル・目標復旧時間など	何もしない/ ITシステム対応の内容*2/ 代替手段の内容	状態継続（影響あり・影響内容）/ 対応による状態変化の様子（暫定復旧，完全復旧など）	必要リソースなど
		影響なし	影響あり・影響内容					影響なし/ 対応による二次リスクの有無とその様子	
			影響なし						
	他の業務活動	影響なし	影響なし	事業影響度分析を参照する	当該業務を行う人員の稼働状況など	維持すべき業務レベル	業務継続する/ インシデント対応の支援に回る	影響なし/ インシデント対応支援による二次リスクの有無とその様子	必要リソースなど
	事業の総合的な状態	影響あり・影響内容	影響あり・影響内容	事業影響度分析を参照する	（現状のリソースのサマリ）	目標復旧レベル・目標復旧時間など	（全体の対応方針＝各種対応方法のサマリ）	状態継続（影響あり・影響内容）/ 対応による状態変化の様子	（制約条件のサマリ）
		影響なし	影響あり・影響内容					影響なし/ 対応による二次リスクの有無とその様子	
			影響なし						

*1, 2 サイバー攻撃に対する対応方法の内容を引き継ぐ．

策定の観点からの状況認識の内容の分類」をマージしたもので，対応計画策定に必要な状況認識の内容を網羅している．この表を埋めるように情報を収集・分析・評価すると，事業の各要素および組織全体がどのような状況であるかを容易に把握でき，対応計画を策定しやすくなると考える．

4.2.2 平時の各種マネジメントにおける管理対象・管理方法の整理

事業活動の階層構造に基づく管理対象・管理方法の分類

事業活動は，ビジネスフレームワークの一つである戦略ピラミッドを用いると例えば，戦略－戦術－実行計画という 3 階層で表現できる．戦略では組織が進むべき方向性を示し，戦術，計画と階層を下るごとに詳細化・細分化する．

ビジネス業績管理の観点からは，順に経営戦略，事業計画，作業計画などが管理対象として該当し，それぞれ適した指標を設定して管理を行う（図 5）[18].

図 5 戦略ピラミッドと管理対象・管理方法の例
（[18]を参考に筆者作成）

Figure5 Strategy pyramid and management methods [18].

ビジネスプロセス管理の観点からは[19][20], 事業活動は，ビジネスモデルービジネスプロセスータスクという順で詳細化・細分化できる（図 6）．なお，前述の戦略ピラミッドの各階層は順に，ビジネスモデル，ビジネスプロセス，タスクを定義し目標設定し実行するものであると解釈すると，内容を理解しやすくなる．

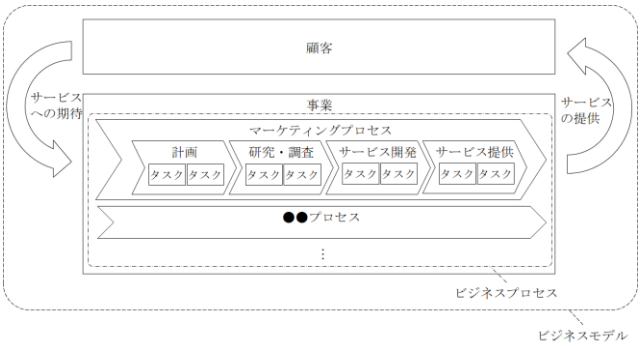

図 6 ビジネスモデル，ビジネスプロセス，タスクの関係
（[20]を参考に筆者作成）

Figure6 Relationship among business model, business processes and tasks [20].

上記の 2 つの観点は，作業ないしタスクという粒度まで分解すると，管理対象と管理方法は実質的に同じになる．

タスクの実行主体に着目した管理対象・管理方法の分類

事業活動を細分化した単位であるタスクに着目すると，タスクは人や IT システムが活動することで実現される．

- IT システムの活動

IT システムの活動は，厳密には，人が利用する機能を実現するためにオペレーションシステムなどが動作する場合と，人が機能を利用したり IT システムの設定変更などの操作をしたりする場合とに分けられるが，いずれもログとしてリアルタイムで記録されるように設計・実装される．ログの時間単位および内容の粒度は，システム監査の要件やログ分析の目的などを満たすものが選択される．

なお，ログの生成がリアルタイムでも，分析・評価がリアルタイムであるとは限らない．ログがどのような契機や頻度で分析されるかは，組織がどのような頻度で分析を必要とするかに依存する．例えば，EC サイトにおいて，「注文機能」がエンドユーザによってどの程度の回数・頻度で利用されたかを，1 か月単位のデータの粒度で 1 か月毎の頻度で分析をする場合もあれば，週単位・日単位・時間単位で 1 週毎・1 日毎・1 時間毎に分析する場合もある．

- 人の活動.

人の活動は，定常業務に関しては月・週・日・時間単位などの作業計画，非定常業務すなわちプロジェクトに関しては WBS (Work Breakdown Structure)などを用いてタスク単位で管理されることが多い．これらの管理は，組織におけるマネジメントとして扱いやすい粒度・頻度で実施される．例えば，製品やサービスの営業活動は，メールや電話でのアポ取り，提案資料の作成，打ち合わせ，見積書の作成，契約条件の交渉，契約書の作成などの複数のタスクから構成され，各タスクの進捗状況を日単位で管理する．

人の活動は，必ずしもリアルタイムに記録されるとは限らない．人の活動は，IT システムの利用有無の観点から，IT システムを利用する活動と IT システムを利用しない活動とに分類できる. 前者は IT システムのログとしてリアルタイムに記録されるが，後者は人手で記録が必要なため，活動から記録までの間に時間差が発生する，もしくは記録されないことがある．また，記録に引きずられて分析のリアルタイム性も失われることになる．

情報の更新頻度に着目した管理対象・管理方法の分類

組織が管理する対象に関する情報は，情報の更新頻度に着目すると，静的情報と動的情報とに大別できる．静的情報とは，事業を実現するための仕組みに関する情報で，一旦内容が決まると頻繁には更新されないものを指す．例えば，ビジネスプロセス，作業手順書，システム仕様書，システム構成図，ネットワーク図などが該当する．動的情報とは，事業活動の状態を示すものであり，経営戦略の KGI の状態，事業計画や作業計画の進捗状況，システムログなどが該当する．

平時の各種マネジメントの管理対象と管理方法の整理

以上を踏まえて，事業構造の各要素（図 4）が，平時の各種マネジメントでどのように管理されているかをマッピングすると，図 7 のようになる．各要素の因果関係は，ビジネスプロセスや作業手順書，システム仕様書，システム構成図，ネットワーク図などの静的情報から導出できる．各要素の状態は，システムログや作業計画などの動的情報から把握できる．また，動的情報を関連付けて分析することで，各要素の因果関係を定量的に把握できる．

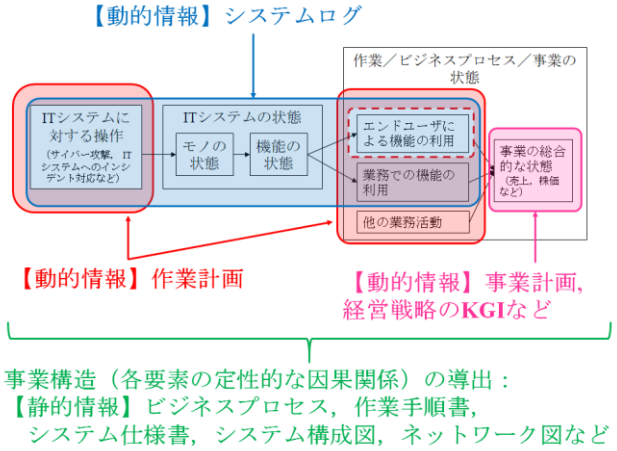

図 7 平時の各種マネジメントの管理対象と管理方法のマッピング

Figure7 Mapping of management methods.

4.2.3 サイバー攻撃発生時の状況認識への平時のマネジメント手法の適用方法

4.2.1 で整理したサイバー攻撃発生時の状況認識の内容（表 1）に，4.2.2 で整理した平時の各種マネジメントの管理対象と管理方法（図 7）をマッピングすると，サイバー攻撃発生時の状況認識は，平時のマネジメント手法を次のように適用することで実現できる:「現在何が起こっているか」と「リソースの現状」には，作業計画やシステムログなどの動的情報がそのまま該当する.「対応の重要度」と「対応目標」，「どのような対応方法があるか」，「対応する際の制約条件」には，事業継続計画やインシデント対応手順などの中から，「現在何が起こっているか」に当てはまる箇所の内容を記入する．なお，「今後何が起こりそうか」に関しては，未来の状態でまだ観測されていないため，動的情報と事業構造に基づき，現状から今後遷移する可能性のある状態を予測して記入する．「対応方法の効果と二次リスク」は，事業継続計画やインシデント対応手順の中に記載がある場合はその内容が該当し，記載がない場合には動的情報と事業構造，対応方法に基づき予測して記入する（図 8）．

4.3 提案手法の検証方法の検討

仮説の検証すなわち提案手法の妥当性と有効性の検証は，次の手順で実施できると考える：まず，予備調査として，サイバー攻撃発生時に対応計画を検討・判断する人にインタビューを行い，思考する内容とその順番，用いる情報の収集・分析・評価方法を，フローチャートや表などにまとめる．それらと提案手法とを比較することで，関係者が実際に必要とする状況認識の内容を提案手法が満たしているか検証する．次に，本調査として，実際のインシデント対応の場面で提案手法を利用し，提案手法を用いて情報を整理することで，従来よりも組織全体の状況の把握や対応方法の判断が適切になったり早くなったりしたかなどの，ユーザビリティの観点[25][26]で評価を行う．

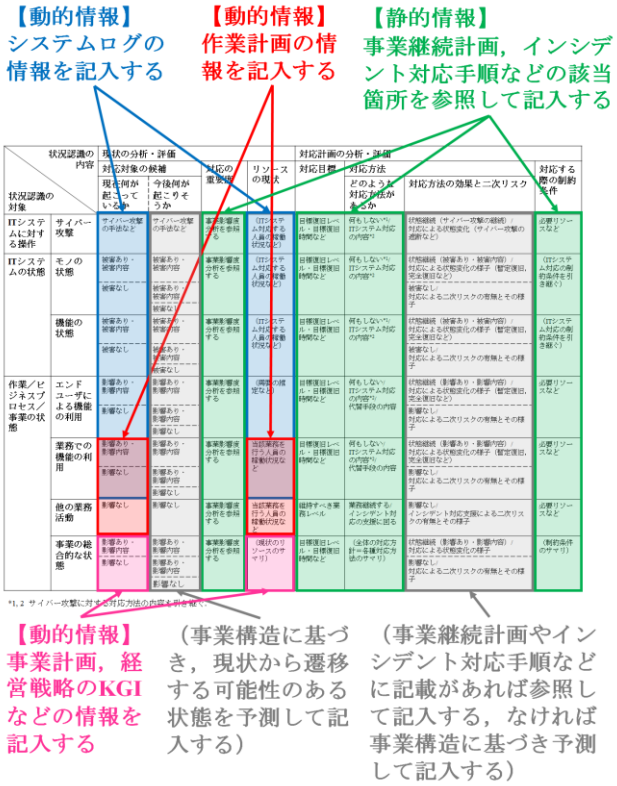

図 8 平時のマネジメント手法の適用によるサイバー攻撃発生時の状況認識の方法

Figure8 Application of ordinary management methods to situation awareness under cyberattack.

4.4 考察

しかし，仮説が正しい場合には，次のような疑問が生じる：表 1 における状況認識の対象は，組織の平時の管理対象と一致する．状況認識の内容は，リスクマネジメントやプロジェクトマネジメントでは一般的な観点である．つまり，本稿で提案するまでもなく，各組織は平時に実施している各種マネジメントそのもので，サイバー攻撃発生時に必要な状況認識を実現しているはずである．では，インシデント対応の現状として，なぜ適切に状況認識できていないのだろうか．

ここで，図 7 を導出した手順を踏まえると，現在の各種マネジメントでは，次に挙げる問題のうち 1 つ以上の問題が発生しているために，適切な状況認識の形成が阻害され

ていると推測される：(1)事業構造を整理していない＝管理対象の事業構造における位置づけがわからない．(2)リスクマネジメントが不十分である＝管理対象の状態を把握するために必要な情報の収集・分析・評価方法を適切に定めていない．(3)情報の収集・分析・評価の頻度が低い，粒度が粗い（例：定量評価していない）＝管理対象がどのような状態や傾向にあるかを詳細に把握していない．(4)各管理対象を関連付けて分析・評価していない＝ある管理対象の状態が他の管理対象の状態にどの程度影響を及ぼすかを把握していない．

これらの問題を解決するよう，平時の各種マネジメントを改善すれば，平時の各種マネジメント手法を用いてサイバー攻撃発生時の状況認識を容易に実現できるようになる．

すなわち，提案手法は，組織の平時の各種マネジメントの改善を提案するものであり，その改善を通じてサイバー攻撃発生時の状況認識を実現するものであると考えられる．

5. 今後の展望

本稿では，サイバー攻撃を受けた組織が，インシデント対応と通常業務を両立する対応計画を策定できるよう，平時の各種マネジメントの管理対象と管理方法を，サイバー攻撃発生時の状況認識に用いるデータや分析・評価方法として適用する方法論を提案した．提案手法を実践することで，組織は，サイバー攻撃発生時の状況認識だけでなく，平時の各種マネジメントを改善する効果も期待できる．

今後は，提案手法の実用化に向けて，インシデント対応の訓練や実際の現場で提案手法を利用して，妥当性や有効性の検証を行う予定である．

参考文献

[1] “7pay（セブンペイ）」 サービス廃止のお知らせとこれまでの経緯，今後の対応に関する説明について”. https://www.7andi.com/library/dbps_data/_template_/_res/news/2019/20190801_01.pdf, (参照 2019-08-05).

[2] “3D セキュア（本人認証サービス）の対応と，クレジットカード不正利用への補償について”. https://paypay.ne.jp/notice/20181227/01/, (参照 2019-08-05).

[3] “不正アクセスによる情報流出事案に関する調査結果報告”. https://www.nenkin.go.jp/info/index.files/kuUK4cuR6MEN2.pdf, (参照 2019-08-14).

[4] 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.

[5] 池田美穂, 高橋慧, 上川先之, 爰川知宏,小阪尚子, 岸晃司．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．情報処理学会研究報告．Vol.2019-SPT-33 No.4, Mar, 2019.

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

[7] ローナ・フィリン/ポール・オコンナー/マーガレット・クリチトゥン 著, 小松原明哲/十亀洋/中西美和 訳．現場安全の技術―ノンテクニカルスキル・ガイドブック．海文堂, 2013.

[8] J. Reason. Human Error. New York: Cambridge University Press, 1990.

[9] J. Rasmussen. Risk Management in a Dynamic Society: A Modelling Problem. Safety Science, 27(2/3), 183-213, 1997.

[10] 平井達哉，本川祐治，佐々木慎一，丹京真一．企業における CSIRT の活動とそれを支援する情報共有システム．情報処理学会デジタルプラクティス，Vol.9 No.3, Jul. 2018.

[11] M. Tyworth, N.A. Giacobe, V. Mancuso, C. Dancy. The Distributed Nature of Cyber Situation Awareness. 2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support, 2012.

[12] N.A. Stanton, , 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.

[13] 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 2019-08-14).

[14] “ISO 22301:2012 Societal security -- Business continuity management systems – Requirements”. https://www.iso.org/standard/50038.html, Jun. 2012, (参照 2019-08-14).

[15] “ISO 22320:2018 Security and resilience -- Emergency management -- Guidelines for incident management”. https://www.iso.org/standard/67851.html, Nov. 2018, (参照 2019-08-14).

[16] 林春男，危機対応標準化研究会編著．世界に通じる危機対応―ISO22320:2011(JIS Q22320:2013)社会セキュリティ‐緊急事態管理‐危機対応に関する要求事項解説．日本規格協会, 2014.

[17] C.S. Renschler, A.E. Frazier, L.A. Arendt, G.P. Cimellaro, A.M. Reinhorn, M. Bruneau. Developing The ‘PEOPLES’ Resilience Framework for Defining and Measuring Disaster Resilience at The Community Scale. 9th US and 10th Canadian Conference on Earthquake Engineering, Paper No 1827, 2010.

[18] R. S. Kaplan, D. P. Norton. The Balanced Scorecard – Measures That Drive Performance. Harvard Business Review (January–February), 71–79, 1992.

[19] “第 2 回 BPM の活用：ビジネスの視点から”. https://www.ibm.com/developerworks/jp/websphere/library/bpm/bpm_intro/2.html, (参照 2019-08-20).

[20] 山本政樹．ビジネスプロセスの教科書．東洋経済新報社, 2015.

[21] “ISO 31000:2018 Risk management ‐ Guidelines”. https://www.iso.org/standard/65694.html, Feb. 2018, (参照 2019-08-14).

[22] E. M. Hutchins, M. J. Clopperty, R. M. Amin. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf, (参照 2019-08-19).

[23] “ISO 21500:2012 Guidance on project management”. https://www.iso.org/standard/50003.html, Sep. 2012, (参照 2019-08-14).

[24] 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.

[25] “ISO 9241-11:2018 Ergonomics of human-system interaction -- Part 11: Usability: Definitions and concepts”. https://www.iso.org/standard/63500.html, Mar. 2018, (参照 2019-08-14).

[26] J. Nielsen. Usability Engineering. Morgan Kaufmann, 1994.