Vol.2019-SPT-32 No.23
2019/3/8

# 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

池田美穂† 高橋慧† 上川先之† 倉恒子† 爰川知宏† 岸晃司†

**概要**：本稿では，サイバー攻撃を受けた組織において，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認知的側面から分析する．サイバー攻撃のインシデント管理プロセスは，起点となる状況認識における CSIRT 関連部署のリスク認知－サイバー攻撃が引き起こす可能性のある事象やその結果をどのように認識して判断するかという認知プロセスーに依存していることを示す．また，部署間でコミュニケーションのミスが生じるのは，CSIRT 関連部署から伝達される情報が，彼らのリスク認知に依存した内容であり，彼らとは異なるリスク認知を有する CSIRT 以外の部署にとって理解しやすいとは限らないためであると考察する．この考察に基づき，サイバー攻撃が引き起こす IT システム障害と事業影響を各人が理解しやすい表現方法で提示することで，サイバー攻撃が発生したときの状況認識における組織のリスク認知とコミュニケーションを支援するシステムを提案する．

**キーワード**：サイバー攻撃，リスク認知，コミュニケーション，インシデント対応，事業継続

# Study of Supporting Risk Perception and Communication in Cybersecurity Incident Response

MIHO IKEDA† SATOSHI TAKAHASHI† HIROYUKI UEKAWA†
TSUNEKO KURA† TOMOHIRO KOKOGAWA† KOUJI KISHI†

***Abstract***: We analyze the cognitive problems in multiple departments of an organization collaborating in incident response and normal business operations when cyberattacks happen. We show that the incident management process of cyberattacks depends on CSIRT's risk perception in situation awareness that is the start point of the process. We discuss that communication mistakes and mismatched situation awareness between departments would occur due to the difference in the risk perception about cyberattack: information based on CSIRT's risk perception may not be easy for other departments to understand. On the basis of the discussion, we propose a risk perception and communication assistance system for organizations in cyberattack response, which provides information about a cyberattack and its impact in various ways of expression easy for each person to understand.

***Keywords***: Cyber Attack, Risk Perception, Communication, Incident Response, 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増している．例えば組織では，作業効率化のためやサービスそのものを実現するためなどに IT システムを利用している．サイバー攻撃により IT システム障害が発生すると，組織では，IT システムの復旧だけでなく，組織の本来の目的である事業継続のために，IT システムを利用している作業やサービスへの影響にも並行して対応しなければならない．このように，サイバー攻撃のインシデント対応と事業継続の各作業を両立することは，組織全体での経営課題であり，サイバー攻撃の脅威の高まりから，効果的な対応を実現するための体系的な考え方や仕組みの研究開発が進められている．

サイバー攻撃発生時に各作業を迅速に効果的に行うために，組織では分業を行うが，分業することで新たな問題が発生する．複数人や複数部署で作業を分担すると，知識・経験の違いなどにより，各人での状況の認識や各作業の重要度・優先度の認識にズレが生じることがある．組織全体で作業を効果的に実施するには，適切なコミュニケーションを行ってこれらのズレを解消する必要があるが，ここでも知識・経験の違いなどにより，伝達した情報が期待したようには理解されないことがある．インシデント対応のフレームワークを効果的に用いるためには，このような問題の解決が必要であり，そのためにはヒューマンファクタの観点から人間の思考の特性を踏まえた支援が必要である．

本稿では，サイバー攻撃が発生したときの組織の対応の効率化に向けて，サイバー攻撃を受けた組織において，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認知的側面から分析し，問題の解決を支援する方法の基礎検討を行う．

本稿の構成は以下のとおりである．まず 2 章にて，サイバー攻撃のインシデント対応に関連する規格やフレームワークを整理する．次に，3 章にて，インシデント対応と事業継続を両立するために複数の部署が協働するときの問題を抽出するとともに，問題を詳細分析して解決すべき課題を考察する．4 章にて，課題の解決方法を検討する．最後の 5 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. 関連研究

### 2.1 マネジメントシステム

#### (1) 事業継続マネジメントシステム

事業継続マネジメントおよびその成果物である事業継続計画（Business Continuity Planning: BCP）は，インシデント対応と事業継続の両立を促進する方法の一つである[1]. BCP を適切に策定することで，組織としての事業の重要度と対応方針が整理され，インシデント発生時の指示命令系統，目標復旧時間，目標復旧レベル，実施項目と優先順位などの対応手順が明確になる．特に NIST SP 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems では，IT システムに特化した緊急時対応ポリシーと計画プロセスを策定するための，IT システム障害による事業影響の分析方法の詳細が記述されており[2]，分析には事業と IT システムの両方の知識が要求されることが読み取れる．

#### (2) クライシスマネジメントシステム

インシデント発生時の対応のマネジメントに特化したツールとして，ISO 22320 が策定されている[3]．ISO22320 は 2011 年に策定後，2018 年に改訂されており，改訂版はアメリカを中心に採用されている危機管理の仕組み「Incident Command System (ICS)」を全面的に参照した内容となっている[4]．序章でインシデント対応にあたる関係者全員に共通の指針を示す必要性に言及するほか，5 章でインシデント対応における組織構造やプロセス（図 1），機能，6 章で状況認識の統一，統合意思決定の確立について記述するなど，インシデント対応においては複数の組織や部署の協働が必要であり，各関係者の状況認識とコミュニケーションが重要であることを繰り返し述べている．

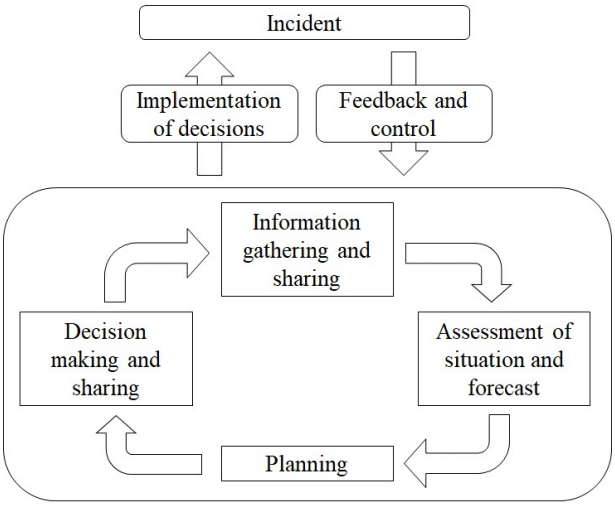


図 1　インシデント管理プロセス[3]
Figure 1　Incident management process[3].

#### (3) その他のリスクマネジメントシステム

その他のリスクマネジメント関連の規格としては，インシデントの予防から対応までを含むリスクマネジメント全般に関する ISO31000[5]，情報セキュリティに特化した ISO/IEC27000 シリーズが挙げられる．

### 2.2 CSIRT[a]関連ガイドライン

#### (1) NIST サイバーセキュリティフレームワーク

NIST サイバーセキュリティフレームワークは，情報セキュリティに特化したリスクマネジメントとして，サイバーセキュリティの改善方法の手順，検討項目とその観点を整理している[6]．サイバー攻撃発生時に関連する事柄は特に，「検知（Detect）」，「対応（Respond）」，「復旧（Recover）」に記述されている．インシデント管理プロセスを踏まえると，「異常とイベント（Anomalies and Event）」と「分析（Analysis）」による情報の収集と分析の重要性が分かる．

表 1　NIST サイバーセキュリティフレームワーク 抜粋[6]
Table 1　Overview of NIST cyber security framework[6].

| Function | Category |
|---|---|
| Identify | Asset Management |
| | Business Environment |
| | Governance |
| | Risk Assessment |
| | Risk Management Strategy |
| | Supply Chain Risk Management |
| Protect | Identity Management and Access Control |
| | Awareness and Training |
| | Data Security |
| | Information Protection Processes and Procedures |
| | Maintenance |
| | Protective Technology |
| Detect | Anomalies and Events |
| | Security Continuous Monitoring |
| | Detection Processes |
| Respond | Response Planning |
| | Communication |
| | Analysis |
| | Mitigation |
| | Improvements |
| Recover | Recover Planning |
| | Improvements |
| | Communication |

#### (2) NICE フレームワーク

NICE フレームワークでは，CSIRT 人材と役割，求められるスキルが定義されている[7]．インシデント対応における組織内外の情報共有は，CSIRT が備えるべき重要な機能の一つであり，外部機関および自組織内との連絡窓口となり情報連携を行う PoC（Point of Contact）と，自組織内を

a) Computer Security Incident Response Team. 組織内で情報セキュリティのインシデント対応を専門に行うチーム．「情報システム管理部門系」や「セキュリティ対策部門系」の部署に配置されることが多い[18][19]．本稿では CSIRT と CSIRT が設置される部署を総称して「CSIRT 関連部署」と表す．

調整し各関連部署への情報発信を行うノーティフィケーション担当が，コミュニケーションの中核人物となる[8].

### 2.3 ヒューマンファクターズ

#### (1) ノンテクニカルスキル

インシデントに対応する人という側面からは，認知心理学や行動経済学などのヒューマンファクタ関連の研究は，インシデントが発生したときの人間の行動に関する多くの示唆を与えてくれる．特に，人間の情報処理モデル，意思決定と限定合理性，集団思考，リスク・コミュニケーションに関する研究は，インシデント対応における人・組織の活動に関する理論的基盤を提供してくれる．

インシデント対応における実践的な知識体系として，ノンテクニカルスキルが研究されており，民間航空業界や医療現場，電力・化学プラントでの適用が進んでいる．ノンテクニカルスキルは，テクニカルスキルー業務に直結した専門知識や技術ーに対する言葉であり，状況認識，コミュニケーション，リーダーシップなど，ヒューマンエラーを避け安全を確保するための認知的，社会的スキルである[9].

ノンテクニカルスキルの研究と適用は，現場作業者の行動を「状況認識→意思決定→行動のパフォーマンス」という状況認識モデルで記述し（図 2）[9] [10]，各段階に影響を与える認知的, 社会的, 個人的な要素を特定し, 訓練し, 評価するという手順を取る．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[9]．なお，チーム作業の場合は，流れ自体はこの個人の状況認識モデルに沿うが，複数の人間の状況認識や意思決定がまとめられてチームとしての意思決定に至るという点で，個人の意思決定とは異なる部分がある．

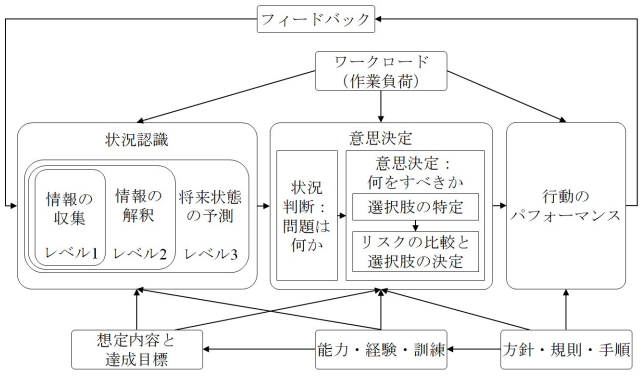


図 2　状況認識モデル（[9]を参考に[10]の Figure.1 を加工）
Figure 2　Model of situation awareness（[9][10]）.

#### (2) その他の人・組織に関する研究

情報セキュリティ分野では，情報セキュリティのリスク認知と IT リテラシーとの相関や[11][12][13], 企業や大学などにおける情報セキュリティの教育・訓練方法が報告されている[14][15]．また，サイバーセキュリティの現場におけるノンテクニカルスキルの研究が始まりつつある[16][17].

## 3. 問題

### 3.1 リスク認知およびコミュニケーションの重要性とこれらが引き起こす問題

関連研究から，リスク認知とコミュニケーションは，組織がサイバー攻撃のインシデント対応と事業継続の作業を両立するための重要な要素であると次のように導き出せる．

#### A. リスク認知

#### A-1. サイバー攻撃のリスク認知の重要性

グローバル化などのビジネス環境の急速な変化，組織が利用する IT システムの複雑化, サイバー攻撃の高度化, IoT の進展によるサイバー攻撃の物理的な空間への波及など，組織を取り巻く環境は目まぐるしく複雑に変化しており，一つのインシデントが多方面で多大な影響を及ぼす可能性が高くなっている．このため，被害や影響の範囲が，予め準備していた BCP 等の手順書で想定していた規模を超え，手順書の内容が実際の状況に適さないことがある．

したがって，組織には，経験したことのないインシデントにも適切に対応するために，現状を理解し将来の状況を推測し，適切な計画を策定し実行する能力が求められる．サイバー攻撃のインシデント対応においてはその能力とは，具体的には，IT システム，情報セキュリティ，事業構造などの多面的な知識・経験に基づく，状況認識と意思決定の能力といえる．すなわち，リスク認知ーサイバー攻撃が引き起こす可能性のある事象やその結果をどのように認識して判断するかという認知プロセスーが，サイバー攻撃のインシデントの予防と対応の巧拙を左右することになる．

以上から，サイバー攻撃の予防と対処は，平時およびインシデント発生時に，サイバー攻撃に関するリスク認知が適切に機能するかどうかに依存するといえる．

#### A-2. サイバー攻撃のリスク認知の問題

サイバー攻撃のリスク認知を向上させることは容易ではない．

一つ目の理由として，事業環境の複雑化や技術の進展により，サイバー攻撃への対応に必要なスキルが広範かつ高度なものとなり，人・組織が十分に有することが難しくなっていることが挙げられる．情報セキュリティ業務担当者として，セキュリティ対策のトレンド・他社動向の把握，セキュリティ脅威・事故に関する情報収集と関係者共有，セキュリティインシデント発生時の緊急対応に課題を感じる傾向は，日本を含む複数の国で見られる[18][19][20].

二つ目の理由として，情報セキュリティへの意識が一般に低いことが挙げられる．サイバー攻撃に適切に対処するためは，情報セキュリティの知識・技術が必要不可欠である．情報セキュリティの重要性は専門家だけでなく一般企業の経営層にも認知が広がっている．しかし，その重要性を真に理解してセキュリティ対策の実施に至るのは，自社で情報セキュリティのインシデントを経験してから，とい

う企業は少なくない[20][21]．また，情報セキュリティの知識・経験が情報セキュリティのリスク認知とリスク回避行動につながるが[11][12][13]，従業員の情報セキュリティへの関心は薄く，サイバー攻撃の脅威や防御手段を理解していない従業員が半数以上を占めるという報告もある[22].

**B. コミュニケーション**

**B-1. インシデント対応時のコミュニケーションの特徴**

インシデント対応を組織的に行う，すなわち複数人で分業して行うには，コミュニケーションは欠かせない．

インシデント対応の指揮命令系統は，ISO22320 と ICS を参照すると，階層型組織構造となる．ICS によると，この指揮命令系統は，平時の組織構造に依存するものではなく，各々の役割に求められるスキルを有する人がその役割を果たすとされている．ただし，インシデント対応と事業継続の両立という観点を踏まえると，平時が階層型組織構造を取っている場合には，インシデント管理プロセスを回す主体は経営層から権限移譲された管理層と現場層であり，現場層が各種作業を実施し，管理層が対応計画の策定および現場層の指揮監督を実施するという，状況認識と意思決定を迅速に行える体制が取られると考えられる．経営層は，管理層から適宜報告を受け，経営判断が必要なときに意思決定に関与すると考えられる．このような運用は，サイバー攻撃のインシデント対応の判断・意思決定において，CSIRT が全面的または一部の権限を持つとする組織が多いという実態に即している[18][19].

各階層の役割は異なるため，各々に共有すべき情報の種類・内容も異なるものになる．経営層に対しては，経営判断という意思決定に役立つよう，経営における共通言語である金額という指標を用いて情報を提示する方法が考えられる[23]．管理層と現場層に対しては，平時の役割で用いる共通言語や考え方という観点から，マネジメントや作業に関連付けてそれぞれ情報提供すると，適切な状況認識と意思決定を促進できると考えられる．

**B-2. インシデント対応時のコミュニケーションの問題**

B-1 から，組織が協働して作業するためには，相手が必要とする情報を，相手が理解可能な表現方法で伝達することが必要不可欠であるといえるが，具体的にいつ・誰に・何の情報を・どのような表現方法で伝達すれば，各役割に期待される行動が適切になされるのかという問題が生じる．

ある人に対して伝達すべき情報の種類・内容とは，その人の認知プロセスを起動させるもの，とも言い表せる．

認知プロセスは知識・経験などにより各人で異なる．例えば，組織の規模が大きくなり分業化・専門化が進むと，インプットとして同じ情報を受け取っても，担当する役割によってアウトプットとしての行動が異なるのであれば，途中の情報処理としての認知プロセスも異なるものになると考えられる．インプットの情報が不完全な場合には，知識や経験などを参考にして各人の頭の中で情報を補完して処理することもある．このような認知プロセスの働きは，意識的な側面と無意識的な側面を併せ持つため，人の認知プロセスを客観的に記述して比較するのは容易ではない．

情報を伝達するとき，その表現方法は発信者の認知プロセスに少なからず引きずられるが，それが受信者の認知プロセスを起動させやすいものであるとは限らない. 例えば，CSIRT 関連部署は，情報セキュリティに関する認知プロセスが強化されているため，サイバー攻撃関連情報を受け取ったときに，状況を理解し自分が何をすればよいかすぐに判断できる．しかし，CSIRT 関連以外の部署は，普段用いている認知プロセスとサイバー攻撃関連情報との結びつきが弱いため，その情報が何を意味するのか，自分は何をしなければならないかを理解しづらい，と考えられる．

リスク認知とコミュニケーションの能力が欠如した組織では，インシデント発生時に次のような現象が観測されると考えられる．

- CSIRT 関連部署の視点：
  －他の部署に作業を依頼しても，通常業務を優先して，期待したように動いてくれない
- CSIRT 関連以外の部署の視点：
  －組織全体としての／依頼された作業の目的や必要性，重要度を理解できない
  －自分達の業務で必要とする情報が CSIRT 関連部署から共有されない
  －CSIRT 関連部署が事業影響を考慮せずに IT システムを停止したために，自分達は顧客からの問い合わせの急増などのイレギュラーな対応に追われる

リスク認知の欠如は特に，プロアクティブな対応の実行を妨げるおそれがある．例えば，すでに発生しているサイバー攻撃と IT システム障害，事業影響に対応するために，各部署からリソースを拠出することに関しては，サイバー攻撃の被害の実態を根拠とすることで，被害に対する共通認識が形成され，各部署の協力が得られやすいと推測される．しかし，サイバー攻撃の被害やその拡大を防ぐための作業に関しては，被害の発生確率や被害規模などをどのように感じるかというリスク認知の違いによって，作業の必要性が理解されず協力を得られなかったり，作業の必要性は理解されても優先度の解釈が異なるために，作業が適切なタイミングで実施されなかったりすることが発生しうる．

**3.2 問題の原因分析**

サイバー攻撃が発生したとき，組織では，インシデント対応のどの箇所で，リスク認知とコミュニケーションのミスが生じる可能性があるかを分析する．

ISO22320 のインシデント管理プロセス，ノンテクニカルスキルの状況認識モデル, NIST サイバーセキュリティフレームワークと，インシデント対応における階層型組織構造をマッピングすると（図 3），サイバー攻撃のインシデント

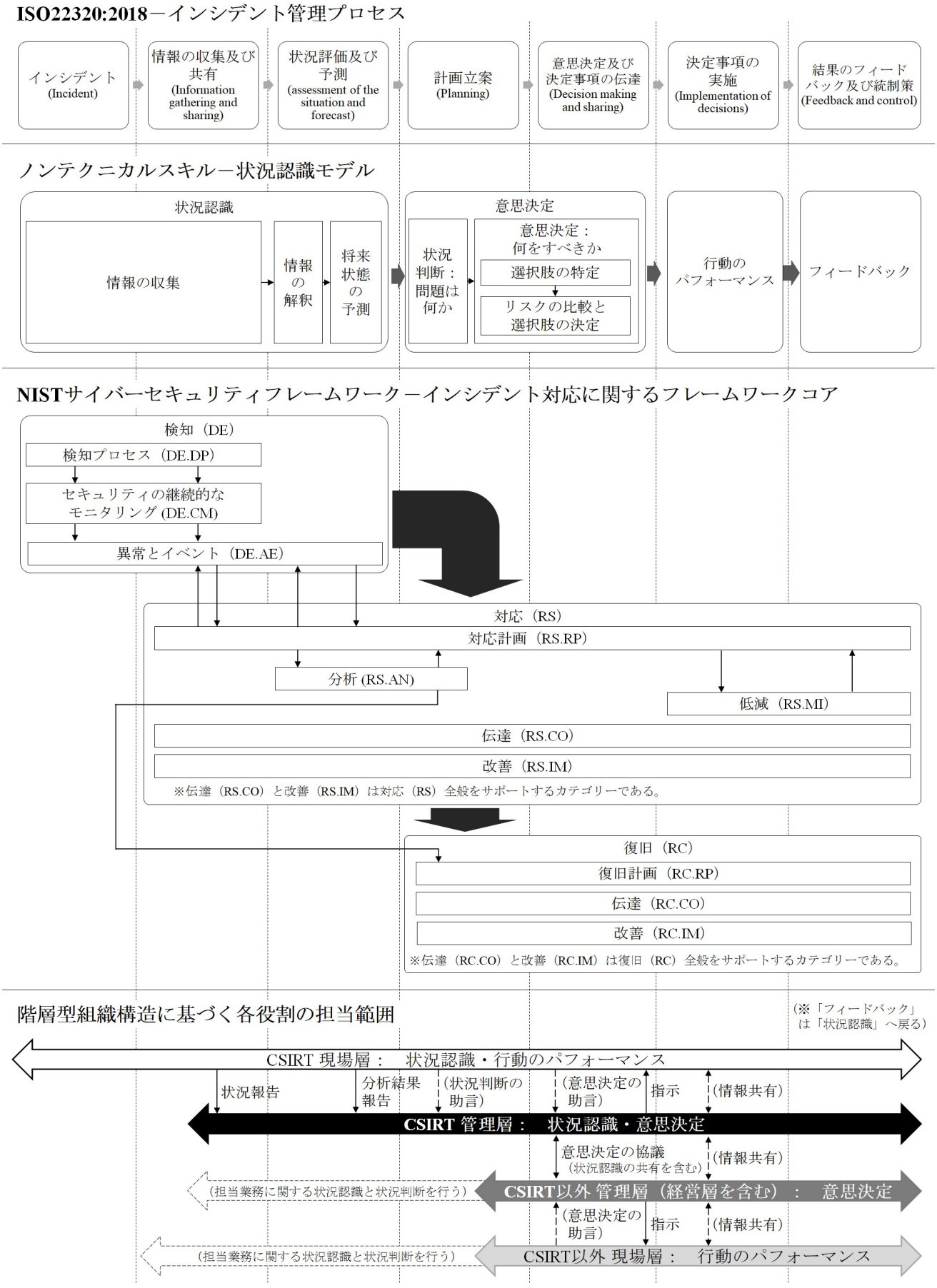


図 3 サイバー攻撃のインシデント対応における人と機能のマッピング

Figure 3 Mapping of people and situation awareness in cyber incident response.

対応時には，各階層では下記の機能を担うと整理できる．複数階層が機能を担っている場合には，主体となる階層を太字下線で示している．なお，フィードバックは，状況認識へ連続的にすぐに移行することから記述を省略した．

- 現場層：**状況認識**，意思決定（指示内容の理解），**行動のパフォーマンス**
- 管理層：状況認識，**意思決定**
- 経営層：意思決定　※インシデントの規模による

この整理に基づくと，リスク認知とコミュニケーションのミスは，それぞれ下記の箇所で発生すると考えられる．

**パターン 1：単一人物のリスク認知のミス**

- 現場層：状況認識，意思決定（指示内容の理解）
- 管理層：状況認識，意思決定
- 経営層：意思決定

**パターン 2：リスク認知の差異によるコミュニケーションのミス**

- CSIRT 現場層⇔CSIRT 管理層：状況認識（状況報告，分析結果報告），意思決定（指示内容の理解）
- CSIRT 管理層⇔CSIRT 以外の管理層および経営層：意思決定（意思決定の協議）　※状況認識の共有を含む
- CSIRT 以外の管理層⇔CSIRT 以外の現場層：意思決定（指示内容の理解）

以上から，サイバー攻撃のインシデント対応は，CSIRT 関連部署のリスク認知に依存していることが分かる．インシデント対応の起点である状況認識は，CSIRT 関連部署の現場層と管理層が担当しており，サイバー攻撃を検知し，収集した情報と知識・経験に基づきサイバー攻撃が現状および将来にどのような被害をもたらすかを推測する．この状況認識に基づき，CSIRT 関連部署の管理層と CSIRT 以外の管理層が，インシデント対応と事業継続の観点から，対応方針と具体的な作業計画を協議して決定し，この意思決定が各部署の現場層に伝達される．これらの手順と状況認識モデルを踏まえると，インシデント対応の成否は，起点となる CSIRT 関連部署のリスク認知に依存すると言える．

また，このようなサイバー攻撃のインシデント対応における情報処理と情報伝達の構造は，リスク認知の違いのために，部署間でのコミュニケーションのミスを生じさせると考察できる．CSIRT 関連部署から発信される情報は，CSIRT 関連部署のリスク認知の影響を受けるため，他の部署にとって理解しやすい表現方法であるとは限らない．また，CSIRT 関連部署が各部署の作業内容とそのために必要な情報をすべて把握することは非常に困難であるため，各部署が必要とする情報や観点が抜け漏れやすくなる．このため，CSIRT 以外の部署では，インシデント対応や事業継続の各作業において担当する作業を実施するために必要な情報が入手できず，またその情報が入手できないため状況認識が不十分となり，必要な作業を想起したりその必要性を理解したりすることも難しくなると考えられる．

## 4. 解決方法の検討

### 4.1 アプローチの整理

3 章を踏まえて，サイバー攻撃発生時のインシデント管理プロセスの起点である状況認識における，リスク認知とコミュニケーションを支援する方法を検討する．

状況認識モデルを参照すると，サイバー攻撃のインシデント対応における状況認識の概略は，用いるデータの種類を踏まえて図 4 のように記述できると考えられる．IT システムのモニタリングと事業関連のモニタリングとでは，用いるデータの種類・内容は異なると考えられる．IT システムのモニタリングは CSIRT 関連部署が実施し，事業関連のモニタリングは当該事業を管轄する部署が実施することが多いと考えられる．また，IT システム障害はサイバー攻撃以外が原因で発生する場合もあるし，事業関連の変化はサイバー攻撃や IT システム障害とは無関係に起こる場合もあるし，サイバー攻撃による IT システム障害の発生と事業影響の発生がそれぞれ異なるタイミングで発生する場合もある．そのため，サイバー攻撃と IT システム障害，事業影響とをそれぞれ適切に関連付ける必要がある．なお，サイバー攻撃の事業影響を簡易に見積もるのであれば，BCP などで事前に実施した事業影響の分析を参照する方法があるが，そのときの実際の被害とは多少の誤差が生じる．

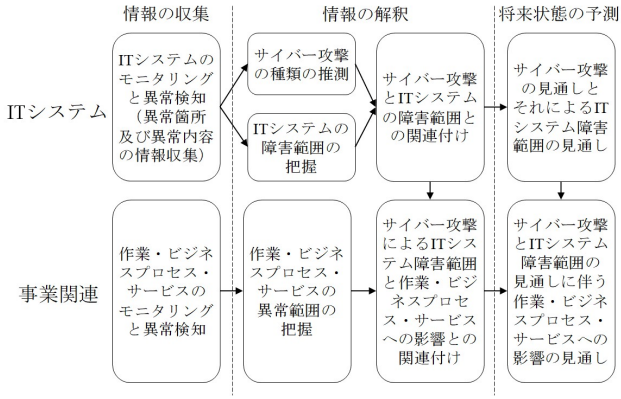


図 4　サイバー攻撃のインシデント対応における状況認識
Figure 4　Situation awareness in cyber incident response.

図 4 から，サイバー攻撃が発生したときに組織の状況認識を支援する方法は，2 つのアプローチに分類できる．

1 つ目のアプローチは，サイバー攻撃による，IT システムへの被害に関する状況認識の支援である．例として，詳細調査が必要なセキュリティアラートの自動抽出，情報セキュリティに関する各種ログの相関分析によるサイバー攻撃の目的と影響範囲の推定などの，CSIRT 関連部署の分析作業を支援する方法が挙げられる．

2 つ目は，サイバー攻撃が引き起こす IT システム障害による，事業関連への影響に関する状況認識の支援である．このアプローチは，組織活動全体に関する状況認識を支援する方法と言い換えることができる．またサイバー攻撃や

それに伴う IT システム障害を事業関連に関連付けて表現することは，CSIRT 以外の部署や経営層の状況認識を促進するための重要な要素の一つと考えられる．

本稿では，複数部署の協働を支援するという点でより直接的な方法と考えられる，後者のアプローチを検討する．

### 4.2 アプローチの詳細

平時およびインシデント発生時に担う役割やそれに伴う認知プロセスを考慮すると，各部署・各階層に対してそれぞれ次のような形で情報を表現して伝達すると，各人の状況認識を促進できると考えられる．

- CSIRT 現場層・管理層：
  －サイバー攻撃の種類を推測するための情報とその推測方法
  －IT システム障害範囲を把握するための情報
  －サイバー攻撃と IT システム障害範囲とを関連付けるための情報およびその関連付け方
  －IT システム障害範囲と事業影響とを関連付けるための情報およびその関連付け方
- CSIRT 以外の管理層:サイバー攻撃が引き起こした IT システム障害による，自部署が管轄しているビジネスプロセスやサービスへの影響
- CSIRT 以外の現場層:サイバー攻撃が引き起こした IT システム障害による，担当している作業への影響
- 経営層：サイバー攻撃により引き起こされた IT システム障害による，サービスや事業活動への影響

これらの情報の起源は，図 4 を参照するといずれも同一であり，IT システム関連情報と事業関連情報を処理して生成されている．すなわち，情報を伝達する相手に応じて，提示する情報の処理段階を変えているということになる．

そこで本稿では，同一の情報のインプットを用いて，伝達する相手によって提示する情報のアウトプットを選択できるシステムを提案する．

提案システムの概略を図 5 に示す．業務分析の手法に従うと，IT システム関連情報と事業関連情報とを次のように関連付けることができる．組織が提供するサービスは複数のビジネスプロセスから構成され，各ビジネスプロセスは複数の作業から構成される．ある作業では IT システムが提供する機能を利用し，その機能はハードウェアおよびソフトウェアにより実現される．このようにして，「サービス⇔ビジネスプロセス⇔作業⇔機能⇔マシン（ソフトウェア，ハードウェア）」の関連付けができる．例えば，システムログを分析すれば，どの機能がどの程度の頻度で利用されているかが分かる．サービスの売り上げなどがどのビジネスプロセスや作業により実現されているかを分析し，先の分析結果と関連付ければ，IT システムの事業への寄与度が求められる．したがって，IT システム障害が発生したときには，システムログが示すエラー箇所・エラー内容に基づき障害が発生している機能を特定すれば，影響を受ける事業とその影響の程度も算出することができる．

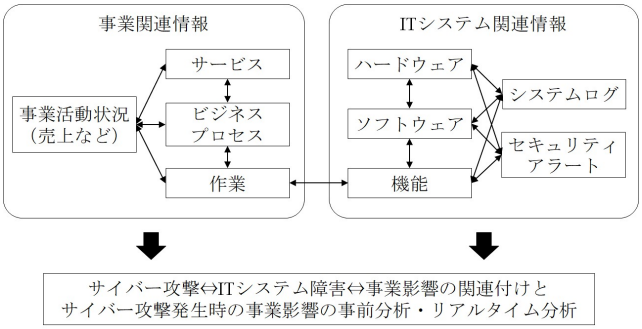


図 5　IT システム関連情報と事業関連情報との関連付け方法の概要

Figure 5　Mapping of IT system information and business information.

このようにして，IT システム関連情報の詳細と事業関連情報の詳細とを関連付けておくことで，サイバー攻撃が発生したそのときの事業影響を，IT システム関連の各種ログに基づき，任意の粒度で算出できるようになる．経営層に対しては，サイバー攻撃の影響を受けているサービスと事業活動状況をリアルタイムで提示できる．管理層に対しては，サイバー攻撃による事業影響のマネジメントのために事業関連情報全般を関連付けて提示でき，現場層に対してはサイバー攻撃による担当作業への影響を提示できる．

以上のように，システムが，IT システム障害範囲と事業影響とを関連付けて，相手によって提示する情報の粒度を出し分けすることで，組織全体で各人の適切な状況認識の促進と，CSIRT 現場層・管理層の作業の負担軽減，組織全体でのコミュニケーションの効率化も実現できると考える．

## 5. 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いて，サイバー攻撃のリスク認知とコミュニケーションの欠如が複数部署での協働を妨げると考察し，インシデント対応の起点となる状況認識において，組織のリスク認知とコミュニケーションを支援する方法を検討した．

今後の課題として，まずは本稿の検討システムの評価が挙げられる．状況認識の支援は，後続の意思決定に寄与するものでなければならない．そのためには，いつ・誰が・何の情報を状況認識や意思決定に用いるかを詳細に分析して定型化してシステム化し，訓練や実際の現場で有効性を検証する必要があると考える．実用化に向けては，必要な情報の簡便な収集方法と提示方法を検討する必要がある．

状況認識モデルに沿うと，次のような課題の解決も必要である．状況認識の支援として，検討システムの他に，各種ログ分析に基づくサイバー攻撃の目的と影響範囲の推測，IT システムと関連する事業状態のモニタリングと分析による事業影響評価の精度向上などが考えられる．意思決定～行動のパフォーマンスの支援として，各選択肢の効果や

2 次リスクをシミュレーションして提示する方法や，各選択肢の詳細計画を自動作成・提示する方法，対応状況に応じて計画を自動修正・提示する方法の検討などが考えられる．これらの理論的根拠となる，サイバー攻撃のインシデント対応における認知プロセスの解明も必要である．

また，実世界とサイバーにおけるインシデント管理の統合という観点で, ISO22320 が定義するインシデント管理プロセスが，サイバー攻撃のインシデント対応にどの程度適用可能か精査する必要があると考える．

ISO22320 では, 想定するインシデントの種類を限定していないが，自然災害などの実世界でのインシデント対応に適した内容となっている．実世界でのインシデントの被害は，物理的な空間の広がりをもっていて，対応にあたっては物量的な資源が必要となり, 人海戦術となる側面がある．サイバー攻撃は，例えばサーバが停止した場合，サーバ停止によるサービス影響は全世界に広がる可能性があるが，サーバそのものへの対応に関しては，知識・習熟度や操作権限の観点から，対応人数は少人数となる．

このように，物理的な被害を対象とするインシデント対応と，サイバーインシデント対応とでは，人の認知プロセスや体制などの組織行動の詳細な箇所で差異が現れ，そのため人・組織の状況認識や意思決定，行動のパフォーマンスを支援する方法も変化すると推測される．その差異を明らかにすることで, ISO22320 を適用した他分野のインシデント対応の手法を参考に，サイバー攻撃のインシデント対応のパフォーマンスを効果的に引き上げられると考える．

このような視点での研究は，IoT の普及により実世界への物理的な被害をもたらすサイバー攻撃が今後増加すると予想される現在において，実世界とサイバーの両空間でのインシデントに対する組織の対応能力の向上に貢献できる．

## 参考文献

[1] “ISO 22301:2012 Societal security -- Business continuity management systems -- Requirements”. https://www.iso.org/standard/50038.html, Jun. 2012, (参照 2019-1-10).
[2] National Institute of Standards and Technology. “NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems”. https://doi.org/10.6028/NIST.SP.800-34r1, May. 2010, (参照 2018-12-18).
[3] “ISO 22320:2018 Security and resilience -- Emergency management -- Guidelines for incident management”. https://www.iso.org/standard/67851.html, Nov. 2018, (参照 2019-1-10).
[4] Tim Deal, Michael de Bettencourt, Vickie Deal, Gary Merrick, Chuck Mills. Beyond Initial Response--2Nd Edition: Using The National Incident Management System Incident Command System. Author House, 2012.
[5] “ISO 31000:2018 Risk management – Guidelines”. https://www.iso.org/standard/65694.html, Feb. 2018, (参照 2019-1-10).
[6] 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 2018-12-18).
[7] National Institute of Standards and Technology. NIST Special Publication 800-181 National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, https://doi.org/10.6028/NIST.SP.800-181, Aug. 2017, (参照 2018-12-18).
[8] 日本シーサート協議会. CSIRT 人材の定義と確保 Ver.1.5. http://www.nca.gr.jp/activity/imgs/recruit-hr20170313.pdf, Mar. 2017, (参照 2019-1-10).
[9] 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.
[10] Endsley, M.R.. Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors Journal 37(1), p.32-64, Mar. 1995.
[11] 情報処理推進機構. リスク認知と実行に関する調査 調査報告書. https://www.ipa.go.jp/files/000011763.pdf, May. 2012, (参照 2019-1-10).
[12] 浜津翔, 栗野俊一, 吉開範章. 集団的防護動機理論に基づく情報セキュリティ対策実行意思モデルの提案とその活用. 情報処理学会論文誌, Vol.56. No.12, p.2200-2209, Dec. 2015.
[13] 澤谷雪子, 山田明, 半井明大, 浦川順平, 松中隆志, 窪田歩. セキュリティリスク回避行動に影響を与えるユーザ要因間の構造の解析. 情報処理学会論文, Vol.57 No. 12 p.2696-2719, Dec. 2016.
[14] 山崎勇二, 後藤田中, 米谷雄介, 林敏浩, 八重樫理人, 最所圭三. インシデント対応におけるリスクアセスメント過程認識のための可視化・伝達を支援するシステムの開発と評価. 信学技報, vol. 117, no. 469, ET2017-103, p.83-88, Mar. 2018.
[15] 寺田剛陽, 鳥居悟, 安野智子, 瀧澤弘和, 新真知. リスク認知に基づく標的型メール対策の検討. 情報処理学会研究報告 Vol.2013-SPT-5(9), p.1-8, May. 2015.
[16] Jessica D. and Robert T.. The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. Front. Psychol., Jun. 2018.
[17] 小島恵美, 奈良和春, 神薗雅紀. 国内におけるサイバー演習の現状と、技術演習にとどまらないノンテクニカルスキル要素を加えたサイバー演習の提案. 信学技報, vol. 117, no. 316, ICSS2017-41, p. 17-22, Nov. 2017.
[18] 情報処理推進機構. 企業の CISO や CSIRT に関する実態調査 2017. https://www.ipa.go.jp/files/000058850.pdf, Apr. 2017, (参照 2019-1-10).
[19] JPCERT コーディネーションセンター. 2017 年度 CSIRT 構築および運用における実態調査. https://www.jpcert.or.jp/research/20181218_CSIRT-survey2017.pdf, Dec. 2018, (参照 2019-1-10).
[20] NRI セキュアテクノロジーズ. NRI Secure Insight 2018 企業における情報セキュリティ実態調査 2018. https://www.secure-sketch.com/hubfs/e-book/NRISecure_Insight2018_Report.pdf, Jul. 2018, (参照 2019-1-10).
[21] 中島浩光. 情報セキュリティと「しみじみ感」. https://www.grcs.co.jp/column/20180126-0, Mar. 2018, (参照 2019-1-10).
[22] A10 ネットワークス. アプリケーションインテリジェンスレポート(AIR) －従業員のセキュリティ意識の欠如は潜在的脅威を孕んでいるか？－. https://www.a10networks.co.jp/news/blog/airblog20180309part2.html, (参照 2019-1-10).
[23] 日本サイバーセキュリティ・イノベーション委員会. 取締役会で議論するためのサイバーリスクの数値化モデル ～サイバーリスクの金額換算に関する調査～. https://www.j-cic.com/pdf/report/QuantifyingCyberRiskSurvey-20180919(JP).pdf, Sep. 2018, (参照 2019-1-10).