効率的な危機対応を支援する 総合リスクマネジメント支援システムの検討

倉恒子† 小阪尚子† 岸晃司† 爰川知宏† 前田裕二†

概要：企業や自治体の危機管理室などにおいて，自然災害やサイバー攻撃などの様々な危機に対応するためには，標準化された運用フローを提示し，関係者間におけるコミュニケーションを通じて情報の収集・共有を行い，全員が状況の認識に関する統一見解を持ったうえで，本部が意思決定できる仕組みが必要と考える．本稿では，この仕組みに則って構築した，効率的な危機対応を支援するための総合リスクマネジメント支援システムについて報告する．

キーワード：危機対応，Planning “P”

Study of Comprehensive Emergency Management Support System for Efficient Incident Response

TSUNEKO KURA† NAOKO KOSAKA† KOJI KISHI†
TOMOHIRO KOKOGAWA† YUJI MAEDA†

Abstract: The emergency management center in a company or the local government faces various kinds of crises, such as natural disaster or the cyber-attack. It is necessary to have a COP (Common Operational Picture) by prompt information collecting and sharing, and smooth communication. Especially for the center that crosses organizations and fields, it is important to prepare a standardized emergency management process for quick and decisive responses. In this paper, we introduce a comprehensive emergency management support system to endorse the effective incident response and investigate its applicability for an emergency management center in an infrastructure company by using the system as a communication tool during an important political meeting.

Keywords: Incident Response, Planning “P”

1. はじめに

近年は，地震や台風といった自然災害(リアルな災害)に加え，企業へのサイバー攻撃が激しくなり，一般市民の生活にも影響を及ぼす例が増えつつある．サイバー攻撃では，不正プログラム感染による日本年金機構における個人情報流出，インターネットバンキングに係る不正送金などが発生した．また海外でも，サイバー攻撃により大規模停電が発生する，ランサムウェア感染で病院が身代金を支払うなど，多種多様な攻撃が発生している[1].

一方，内閣サイバーセキュリティセンターは，他に代替することが著しく困難なサービスを提供する事業が形成する国民生活および社会経済活動の基盤を「重要インフラ」と位置づけ，「情報通信」，「金融」，「航空」，「鉄道」，「電力」，「ガス」，「政府・行政サービス（地方公共団体を含む）」，「医療」，「水道」，「物流」，「化学」，「クレジット」および「石油」の 13 分野を特定し，自然災害やサイバー攻撃等に起因する IT 障害が重大な影響を及ぼさないよう，IT 障害の発生を減らすとともに IT 障害発生時の迅速な復旧を図るための行動計画を立てている[2]．今後は，自然災害に便乗したサイバー攻撃も増えてくる可能性がある．その際，各組織がばらばらにリスク管理をしている状況では，情報が共有されず，迅速な危機対応ができない．これは，内閣府が開催した「東日本大震災における災害応急対策に関する検討会」での検証からも明らかになっている．例えば，中間とりまとめでは，以下の内容が課題として記載されている．

- どの情報源からの情報を優先し，どの情報を優先的に処理するかを検討しておく必要がある．
- 災害の種類・規模等に関して最新の知識を元に見直すとともに，対策の実効性を確保することを目的としてシミュレーションも必要である．
- 行政職員間の広域応援をより円滑にするための災害対応業務の標準化が必要である．

また，第 1 回議事概要に「発災三日後位からは，情報が伝わるようになった．それは，自衛隊，警察，消防，海保が被災地に入ることで，分からなかった状況が把握でき，その後，救命・救出活動が展開されることとなった.」とあることからも分かるように，日頃から訓練している組織は迅速な対応ができている．

これらのことから，管理層，経営層のマネジメントフロ

† 日本電信電話株式会社 NTT セキュアプラットフォーム研究所
NIPPON TELEGRAPH AND TELEPHONE CORPORATION
NTT Secure Platform Laboratories

ーである運用フローは作ったら完了ではなく，最新の知識を元に見直し，様々な状況を想定して訓練する．その実施結果を分析して問題箇所を見つけ，運用フローに反映していく作業を繰り返し実施していかなければ，災害が発生したときに業務を遂行できない[3]．すなわち，危機が発生してから体制を構築して対応にあたるのではなく，平時から各機関が協力・連携し，関係者間での情報認識を統一しておく必要がある[4].

筆者らはサイバー，リアル複合的な危機に対して状況の認識に関する統一見解を持ったうえで本部が意思決定できるための総合リスクマネジメント支援システムを提案する．本稿では，2 章で危機対応マネジメントに必要となる要素について述べ，3 章で筆者らが提案する総合リスクマネジメント支援システム，4 章でイベントへの適用を述べ，5 章でまとめと今後の予定を示す．

2. 危機対応マネジメントに必要となる要素

日本での危機対応にあたっている現場の状況をニュースなどで見ると，自然災害においても自治体によって運用フローが異なっていることが分かる．また，指揮命令や活動状況といった情報はホワイトボードに書かれる，組織間の情報は FAX で送信されるなど，手作業での対応やその場にいる人のみで共有されているため，遠隔地には共有されないという欠点がある．ICT の導入は進んできてはいるが，全体に行きわたっているとは言いがたい．FAX や電話などは，情報が埋もれる，あるいは伝えるべき人に伝わったかどうかが把握できないため，的確な対応判断ができない可能性もある．そこで，筆者らは，ISO 標準に準拠した共通マネジメント手法を適用することで意思統一を図り，情報収集・共有の場を ICT で実現することが必要と考えた．

2.1 標準化された運用フローの提示

様々な危機に対して，想定されるリスクを評価し，危機が起きる前に事前にすべきこと，発生した後にすべきことを運用フローとして策定し，関係者間で共有することが重要である．

最初に，組織が対応すべきリスクを識別し，発生確率と影響度によってリスクを評価する．重大なリスクに対しては，被害を予防するために，リスクの回避・緩和策を取る．一方，優先順位が低いリスクに対しては，被害を軽減するためにリスクの転嫁・受容策を取る．このようなリスクマネジメントは，状況が変われば評価も変わるため，繰り返し行う必要がある．

リスクに対する対応方針を決定した後，危機への対応について，マネジメント計画を立てる段階に進む．

米国では，インシデントに対応するための標準化マネジメントシステムとして，インシデントコマンドシステム(ICS)が開発されている．計画プロセスでは，インシデントを効果的かつ効率的に管理するための戦術的な計画を策定し，実行するための方法を確立する．これを可視化したものが「Operational Planning “P”」であり，意思決定のためのマップとしての役目を果たす[5].

一方，危機対応に関係する組織が，全体として最適な効率を維持しつつ，危機対応業務を遂行することを可能とするための最小限の要求事項をまとめたものとして，国際規格 ISO22320 が発行され，以下の 3 点を必要最小限の要求事項としてまとめている[6].

- 各々の組織において，危機対応に関する意思決定や計画の策定などを行うための「指揮・統制に関する要求事項」
- 危機対応活動を効果的に管理・実施し，かつ組織間の連携を可能とするための「活動情報に関する要求事項」
- 危機対応に対して関係組織が共同で行動するために必要となる「協力及び連携に関する要求事項」

先ほど上げた ICS の計画プロセスは，ISO22320 における「指揮・統一に関する要求事項」のうちの指揮・統制プロセスを構築することに該当する（図 1）.

筆者らは，本プロセスを表した「Operational Planning “P”」を，各々の段階で実施すべきチェックリストと併せて整備することで，関係者が取るべき行動を示すことが必要であると考える．

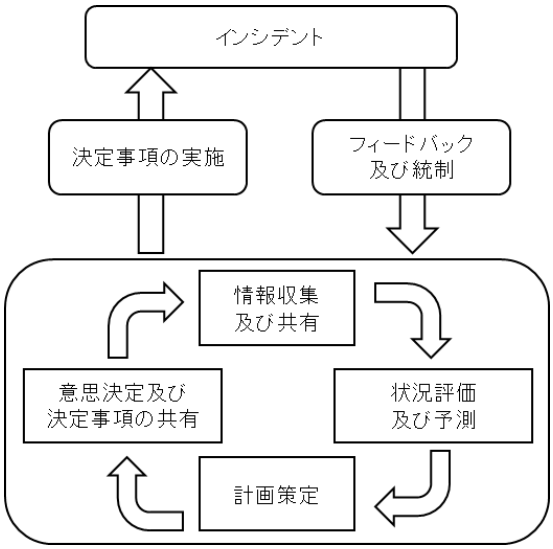

図 1 指揮・統制プロセス（JIS Q22320:2013 内の図 1）
Figure 1 Command and control process

2.2 関係者間におけるコミュニケーションの場，および情報の収集・共有の場の提供

計画の各々のフェーズで危機対応業務が発生する．過去の危機対応でも共通して発生する業務は，定型化し，関係

者間で共有することで，現場ですべきこと・情報集約した結果が容易に把握でき，かつ現場に権限を委譲することで，意思決定を素早く行えるようにする必要がある．そのために，被害の状況確認や災害概況などの集計結果や，インシデントが発生している場所などが，全体を俯瞰できるようにするのが望ましい．

一方，今まで経験したことのない新たな課題も発生する．これらは決定権限を持つ関係者間で状況認識を共有して，重点的に対応する必要がある．そのため，電話や FAX，ホワイトボードなどの非定型情報を一元管理できること，課題の優先度，課題に対する指示とそれに対する関係組織からの回答状況，課題の完了・未完了を迅速に把握できる場を提供することが不可欠となる（図 2）．

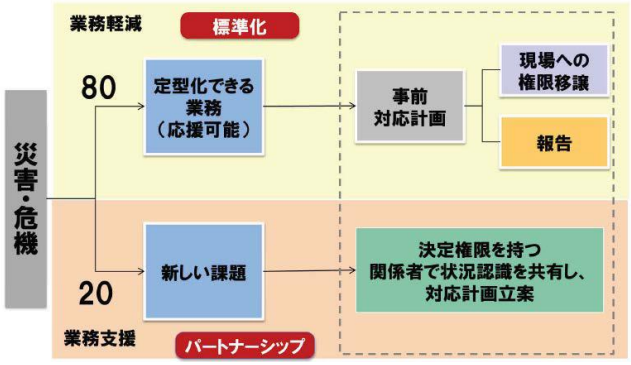

図 2　災害時に行う対応業務の効率化
Figure 2　Efficiency of the corresponding duties to do at the time of a disaster

新しい課題は，これまでに経験がなく，その場で対応し計画を立案して取り組む必要があることから，「非定型業務」と考えられる．非定型業務は，ホワイトボードや電話などでやり取りされることが多く，意識して記録しない限り，後には残らない．これを避けるために，自由記述形式のタスクを設定し，事案の優先度や重要度，進捗状況を付与することができるものを提案している．災害対応訓練に参加していただいた市町村にアンケートを実施し，事案管理に役立てることが有効であることを検証している[7].

3.　総合リスクマネジメント支援システム

大都市大震災軽減化特別プロジェクトの重点課題 2「効果的な災害対応を可能にする災害対応シミュレーターの開発」において，標準的な危機対応の流れにおける重要な要素として，①被害状況の把握，②対応・資源状況の把握，③対応内容の記録，④意思決定機能，⑤危機管理計画の参画，⑥当面の対応計画の策定を集約して総覧できることが必要であることが示されている[8, 9]．2.1 は⑤，⑥の機能を，2.2 は①～④の機能を表す．

本システムでは，これらを 3 つの画面に集約し，⑤⑥を Plan 画面，①②を See 画面，③④を Do 画面として提供している．3.1 に総合リスクマネジメント支援システムの構成を，3.2 から 3.4 で各画面の詳細を示す．

3.1　システム構成

総合リスクマネジメント支援システムは，Web3 層構成を取る．災害が起きたときの影響を受けにくいクラウドサービス上で動くことを想定して設計している．また，外部システムとの連携は，Representational State Transfer(REST) を用いて一旦バッファに蓄積し，その後でシステムに取り込むようにしている．

3.2　Plan 画面

「Operational Planning “P”」を中心に，自組織でやるべきことを提示して，関係者間で統一された状況把握できるよ

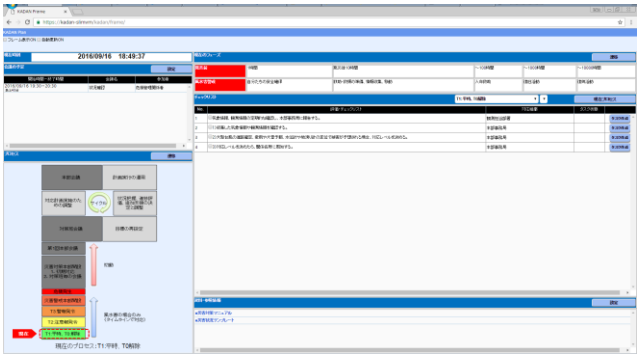

図 3　Plan 画面
Figure 3　Screen of the “Plan”

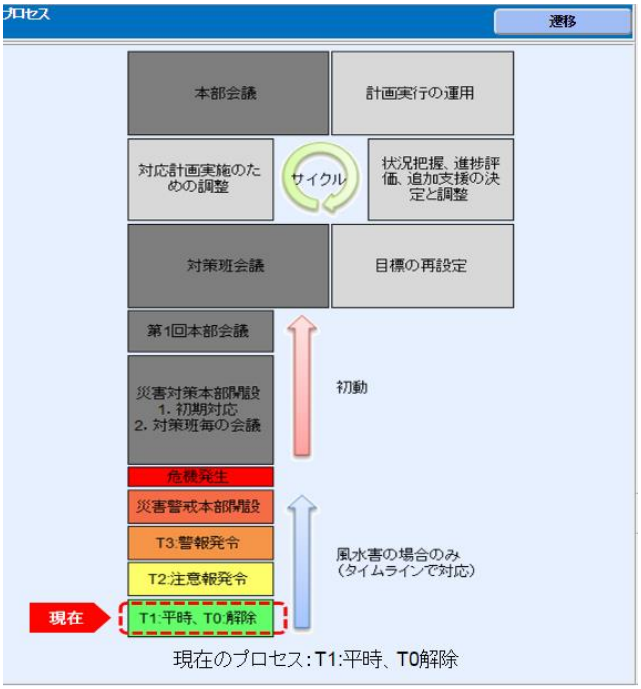

図 4　台風災害における Operational Planning “P”
Figure 4　Operational Planning “P” for the typhoon disaster

うにする画面である．具体的には，運用フロー（対応計画），各々のフェーズで準備すべき具体的な行動，資源，人員など実施すべき内容をチェックリスト，意思決定の場となる会議のスケジュールなどである．運用フローでは，現在どのフェーズにいるかを明示し，今何をすべきか，これから何をするかを一目で把握できるようにする（図 3，図 4）．

また，フェーズごとに表示したチェックリストに対して，関連組織に指示を出すなどの作業依頼は Do 画面で実行できるように連携している．図 5 は，図 4 の「T1:平時，T0:解除」時に実施するチェックリストである．このリストの右にある「タスク作成」ボタンをクリックすると，Do 画面にやるべきタスクを登録できるようになっている．

これに加え，マニュアルや過去の対応で参考になった情報を格納しておくことで，手順の確認やノウハウ活用が容易にできるようにしている．

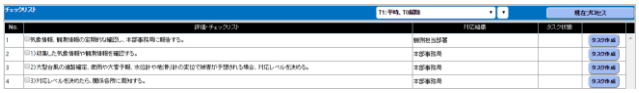

図 5　台風災害での「T1:平時，T0:解除」におけるチェックリスト

Figure 5　checklist for “T1:peacetime, T0:release” on the typhoon disaster

3.3 Do 画面

非定型情報を一元管理するために，タスクという概念を導入する．課題は当面の対応計画に基づき，複数のタスクに分割される．

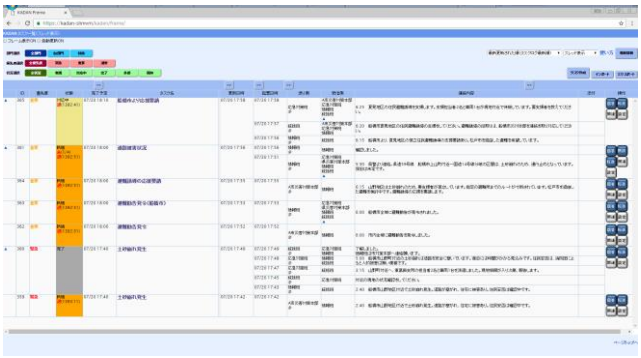

図 6　Do 画面

Figure 6　Screen of the “Do”

各々のタスクに対して，優先度，現在の状態とともに，各組織とのやり取りをスレッド表示することで，効率的に進捗確認ができるようにする．優先度は，緊急/重要/通常の文字の色を赤/橙/黒で表し，状態は，新規/対応中/完了/周知の背景色を橙/黄土/灰/白にしている．また，完了予定から遅れているものは，状態に赤字で「遅」と表示している．周知は，各組織からの確認結果を表示するようにしている（図 6）．

また，脆弱性対策情報や気象情報など，外部システムからの情報を取り入れ，重要なものは情報共有するためにタスクとして登録することもできるようにしている（図 7）．

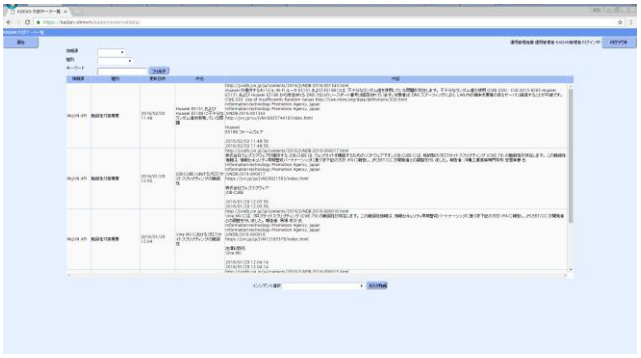

図 7　脆弱性対策情報データベースの情報を取り込んだ画面

Figure 7　Screen which took in information of JVN(Vulnerability Countermeasure Information Database)

3.4 See 画面

定型化業務についてはテンプレートを提供し，状況報告を一元管理できるようにする．表や地図を用いて，視覚的に分かるようにする（図 8，図 9）．例えば，避難所状況報告において，充足している場合は緑，不足していて何らかの手を打たなければいけない場合は赤，未確認は灰色としている．これは，ISO22324 で定められている，カラーコードを用いた危険の深刻度に従っている．

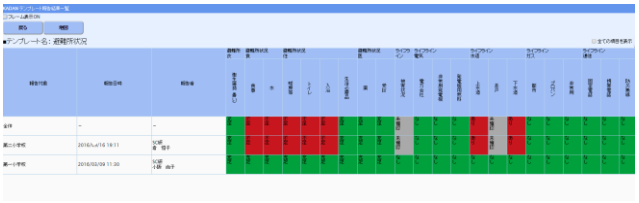

図 8　避難所状況報告結果一覧

Figure 8　List of results reported the status of evacuation sites

4. イベントへの適用

4.1 実施概要

あるイベントに対するサイバー危機対応訓練（1 日）と，イベントへの適用（事前準備，本番，フォローを含む 8 日間）を実施した．ここでは，対応内容の記録を取ってもらうことを目的として，Do 画面を使い，操作面，性能面，運用面で評価した．

4.1.1 危機対応訓練

参加人数は 100 名程度で，平常時と非常時の 2 つのシナリオを用いて訓練を 2 回ずつ行った．

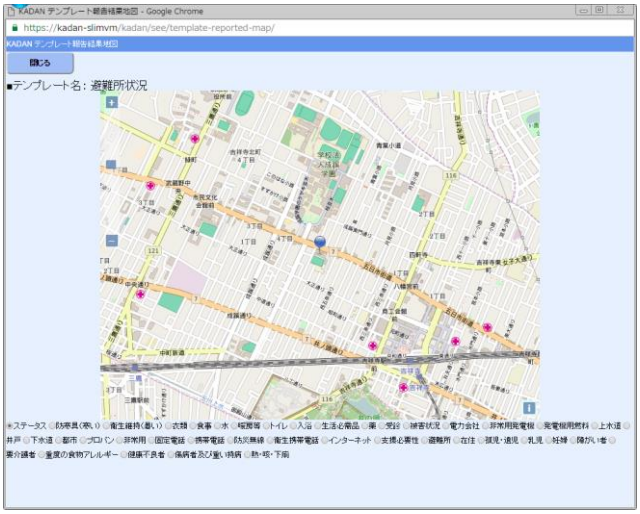

図 9　避難所の位置を表した地図

Figure 9　the map that shows the location of the evacuation sites

サーバは，外部のクラウドサービスを利用した．確実に運用するため，事前にアクセスする端末の IP アドレスをサーバ側に登録し，登録されていない IP アドレスからのアクセスは拒絶する運用とした．

以下に，平時，非常時の訓練での活用内容を示す．

(1) 平時訓練における活用

- 情報統括班から定期報告指示を本システムのタスク作成で登録し，各班が回答を報告する．
- 情報統括班から勤務者の交代・引き継ぎを指示し，各班が交代に関して報告する．

(2) 非常時訓練における活用

- 障害を発見した組織が，本システムで新規タスクを作成し，障害に関する各班の確認状況と対応内容を報告する．
- 障害対応中に別の障害が発生したときには，別タスクを作成し，1 タスク 1 障害で状況を把握する．

4.1.2 イベントへの適用

参加人数は 100 名程度で，4 日間は 24 時間利用とした．サーバ環境は，訓練時と同じものを使用し，期間中は定期バックアップを実施した．

活用内容は次のとおりであり，合計 40 テーマの Do 画面が作成された．

- 定期報告（記録を含む）（4〜7 回/日）
- 障害対応（申告・発見に伴う対応）状況報告
- 幹部への報告内容の共有
- 各種依頼事項や情報共有

4.2 アンケート結果と考察

イベント終了後に参加者にアンケートを採り，操作面，性能面の 2 つの観点で評価した．また，実際に使用している現場の確認や，書き込まれたタスク等から運用面で評価した．

4.2.1 操作面

Web ベースのシステムであるため，訓練時にはほとんどの人が初めて操作する状況であったが，操作に関する質問はなく，おおむね良い評価をいただけた．

実際のイベントでは，口頭で報告すると音声が聞き取れないなどの問題があったこと，勤務者の交代後も情報を共有する必要があることから，本システムに情報を残すことは有意義とのコメントが得られた．様々な使い易さは評価されたが，画面の表示に関する要望は多数出ており，見え方には工夫の余地があることが分かった．

4.2.2 性能面

システム停止といったトラブルは発生しなかった．また，100 人での運用でレスポンス低下になる状態は発生しなかった．

4.2.3 運用面

現場では，障害対応情報とそれ以外のもので本システムを含めた情報共有のやり方，幹部への通知や意思決定方法が決められており，運用フローとして参加者に提示されていた．マネジメントプロセスが運用されていたことから，今回は使用しなかった Plan 画面が，実際の現場で活用できたと考えられる．

また，リアルな災害への対応とサイバーにおける危機対応での違いも明らかになった．リアルな災害への対応では，1 つのインシデントに関連するタスクが発生し，進捗を管理していくやり方である．一方，サイバーにおける危機対応の場合は，種類や分野の異なる小さなインシデントがいくつも発生していくため，現場ではテーマ名と障害状況をインシデント名とするルールを採用し，担当者がどのインシデントに対応しなければいけないか分かるように工夫していた．インシデント数が多くなると工夫だけでは賄いきれない可能性もあり，分野ごとにグルーピングする，あるいはインシデント名に加えて属性を付与することで検索しやすくするなどの対応が必要であることが判明した．

5. まとめと今後の予定

危機対応を効率的に支援するための要件を抽出し，意思決定できるための総合リスクマネジメント支援システムを構築した．社内のイベントで利用するなどして，システムに対する意見を収集したところである．使い勝手等を含めて，改善すべき点が見いだせたので，今後対応していく予定である．

危機が発生してからシステムを使おうとしても，使い慣

れないと入力等に手間がかかり，肝心の危機対応業務に支障が出る恐れがある．そのため，日常業務やイベントなど平時にも活用することで，システムに慣れてもらうことに加え，普段の業務でも危機対応と同じ考え方を適用して進めることができるようになるため，特別なことをやらなければいけない，といった心理的圧迫も減らすことができると考える．

これに加え，様々な活動の有効利用にも着手する予定である．例えば，平時に実施する訓練のシナリオとして，過去ログを活用する，危機対応時には，過去の対応からノウハウを抽出し，対応を決定するときの参考にするなどの機能を盛り込む予定である．

謝辞 実証実験にご協力いただいた方々に，心より感謝の意を表します．

参考文献

[1] 「レジリエンス社会」をつくる研究会．しなやかな社会の挑戦．日経 BP コンサルティング, 2016.
[2] 21 世紀政策研究所. “サイバー攻撃の実態と防衛”. http://www.21ppi.org/pdf/thesis/130611.pdf, (参照 2016-09-16).
[3] 内閣府. “東日本大震災における災害応急対策に関する検討会”, http://www.bousai.go.jp/oukyu/higashinihon/index.html, (参照 2016-10-06)
[4] 内閣サイバーセキュリティセンター. “重要インフラ防護に対する考え方”. http://www.nisc.go.jp/active/infra/pdf/infra_rt3_r1.pdf, (参照 2016-09-16).
[5] Tim Deal, Michael de Bettencourt, Vickie Deal, Gary Merrick, Chuck Mills. Beyond Initial Response: Using The National Incident Management System’s Incident Command System 2nd Edition. AuthorHouse, 2012.
[6] 林春男，危機対応標準化研究会．世界に通じる危機対応．日本規格協会, 2014.
[7] 小阪尚子，一ノ瀬文明，小山晃，爰川知宏，前田裕二．危機管理情報マネジメント支援システムにおける対応フェーズに応じた定型／非定型情報の活用方法の検討．第 6 回安全・安心な生活のための情報通信システム研究会, 2014.
[8] 大都市大災害軽減化特別プロジェクト. “11.2 巨大連担都市圏での災害対応シミュレーション・プラットフォームの開発”. http://www.ddt33.dpri.kyoto-u.ac.jp/katsudou/ddt33_sokatsu_pdf/sokatsu33_11_2.pdf, (参照 2016-09-20)
[9] 京大・NTT リジリエンス共同研究グループ．しなやかな社会の創造．日経 BP 企画, 2009.