統合リスクマネジメント支援システムのサイバー分野での活用

岸晃司[1] 吉田芳浩[1] 倉恒子[1] 小阪尚子[1]

概要：複数組織に渡る大規模な危機対応業務においては，危機対応の国際標準 ISO22320 に書かれているように，それぞれの組織における指揮・統制，危機対応に必要な情報の活用，及び複数組織間の連携・協力が重要である．このことは，台風や地震等の自然災害だけではなくサイバー分野の危機対応においても同様である．そのような考え方に基づき，我々はこれまでに自然災害やサイバー攻撃等への対応を支援するシステム「KADAN®」の研究開発を進めてきた．
本稿では，2016 年 11 月に実施された大規模，複数組織におけるサイバー分野での危機対応業務訓練における，KADAN®の実効性を検証した結果について報告する．

Utilization of Integrated Risk Management Support System in Cyber Field

KOUJI KISHI[1] YOSHIHIRO YOSHIDA[1]
TSUNEKO KURA[1] NAOKO KOSAKA[1]

1. 背景と目的

近年，サイバー攻撃による被害の拡大が深刻な問題となっている．2015 年には日本年金機構の加入者情報の流出があり，国内で大きな問題となった．2017 年 7 月には米国の信用情報会社 Equifax から 1 億 4300 万件にも上る米国一般消費者の個人情報が流出した. また, 情報漏洩だけでなく，社会生活に直接影響を与える事件として，原子力発電所の遠心分離機が一時的に使用不可となったり，大規模停電が発生したり，金融機関のコンピュータネットワークが麻痺したり，不正送金が発生したりと，重要な設備やインフラが狙われた事例も海外では発生している[1]. 内閣サイバーセキュリティセンター（NISC）では，2020 年東京オリンピック・パラリンピック競技大会（「東京 2020 大会」，以降は“開催地名＋開催年＋大会”で表記）の開催を控え「重要インフラの情報セキュリティ対策に係る第 4 次行動計画」を 2017 年に策定しており，その中では，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」，をはじめ「金融」や「電力」，等の 13 分野を特定している．そして，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共に 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]. ロンドン 2012 大会，リオ 2016 大会ではいずれも多くのサイバー攻撃が報告されており，東京 2020 大会では更に増加することが予想される．国際規格 ISO20121「イベントの持続可能性に関するマネジメントシステム」[3]では，自然災害や感染症，情報システム, ライフライン等, 様々なリスクが定義されている．

このように今後はサイバー攻撃により社会基盤を支える重要インフラが被害を受けたり，イベント妨害として様々なリスクが複合的に発生したりする可能性が考えられる．その際，各組織が個別にばらばらに対応してしまっては危機対応が非効率なものとなる．従って，危機対応を標準化し複数の組織が協力・連携して効果的・効率的な危機対応を実現する必要がある[4].

筆者らは，これまでに自治体での自然災害に対する危機対応を対象として，マネジメントフローの標準化や統合リスクマネジメント支援システム「KADAN®」の研究開発を行ってきた[5]. 数年に渡る図上訓練での検証において，その有用性について確認した[6,7]. また，小規模なサイバー攻撃訓練での検証において，その有用性について確認した[8].

本稿では，2016 年 11 月に実施された，23 組織，約 200 名による，民間企業でのサイバー攻撃対応演習を対象として，我々が研究開発している統合リスクマネジメント支援システムのサイバー分野の危機対応業務での有効性を検証した結果について報告する．

2. 効率的な危機対応マネジメント

2.1 危機対応の標準化

リスクマネジメントのサイクルは大きく 4 段階，準備(Plan)，危機対応(Do)，振返り(Check)，見直し(Action)に分けられる（図 1）[9]. 平常時から関係者間で想定したリスクへの対策を打ち，それでも被害が発生した場合には，速

1 NTT セキュアプラットフォーム研究所

ⓒ2018 Information Processing Society of Japan

やかな復旧に向けて対応する．対応後には振返りにより問題点，課題を分析・評価し改善策を講じて次の対応に備えるという営みとなる．その中で，危機対応については米軍ジョン･ボイド氏により提唱された OODA ループ（Observe, Orient, Decide, Act）[10]という指揮官のあるべき意思決定プロセスが適用できる．危機対応に関する国際規格 ISO22320 では，指揮・統制プロセスとして図 2 のように規定されており，対象とするインシデントに係る被害や対応状況に関する情報を収集・共有し，収集した情報を分析・評価して今後の予測をし，その結果に基づいて計画を策定し，最後に意思決定を行い関係者に共有する．決定事項に応じて対応を実行する．規格の中では以下の 3 点を必要最小限の要求事項としてまとめており，あらゆる危機に対して共通的に適用できるとされている．

A) 指揮・統制に関する要求事項
B) 活動情報に関する要求事項
C) 協力及び連携に関する要求事項

指揮・統制プロセスについては上記 A)で，協力・連携体制においては上記 C)で規定されており，図 2 のそれぞれのステップにおいて協力・連携して実施することが求められる．ここで，規格の中では協力と連携を明確に区別しており，『“協力”とは複数の部局・組織が達成すべき共通の“目的”を持つことであり，“連携”とは複数の部局・組織で合意した共通の目的を達成すべく行動を同期させることである』となっている．多種多様な組織が集まって危機対応にあたる場合には，このように“目的”を明確化して，お互いの対応を同期させることが重要であり，危機対応全体をマネジメントする機能が大きな役割を果たす．ISO のベースとなったのが，米国で策定されている ICS(Incident Command System)というフレームワークである[11]．ISO の指揮統制プロセスを更に具体化したものとして「Operational Planning “P”」が規定されている（図 3）．“P”の下半分の足の部分はインシデント発生前の事前準備やインシデント発生後の初動を示しており，P の上半分のループの部分は会議を基軸にサイクルを回す部分となっている．このようにプロセスを明確にすることにより関係機関全体で効率的に意思決定や組織間の連携ができるようになる．組織体制に合わせて具体的な会議体を設定し承認プロセスを明確にすることができる．

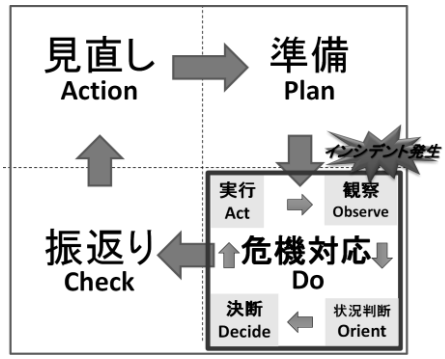

図 1 リスクマネジメントのサイクル

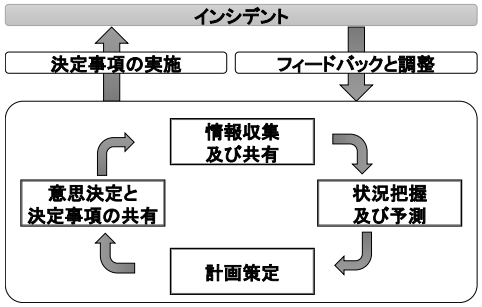

図 2 **指揮・統制プロセス**

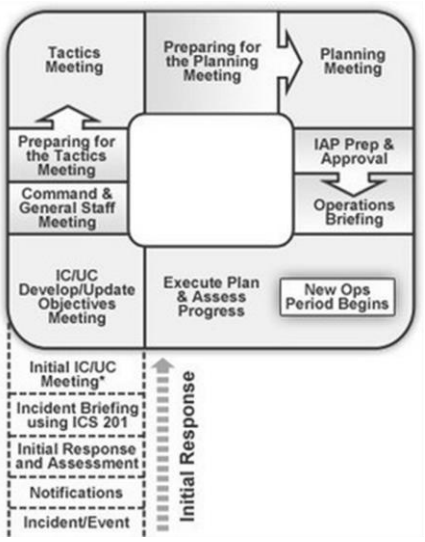

図 3 **Operational Planning “P”**

2.2 統合リスクマネジメント支援システム

本研究で提案する統合リスクマネジメント支援システム KADAN®は，危機対応を主に対象とすると共に，訓練や実対応後に振返りを行うことができる．システムでは，収集した情報を情報集約画面 Plan/Do/See で総覧できるようにし，効率的・効果的な意思決定や組織間連携を支援する．Plan 画面では「今，何をすべきか？」，Do 画面では「今，何をしているか？」, See 画面では「今，どうなっているか？」を確認できるような情報を提供する．

ⓒ2018 Information Processing Society of Japan

2.2.1 Plan 画面

Plan 画面例を図 4 に示す． 図 3 で示した「Operational Planning “P”」を中心に，それを構成する各ステップで誰が何をやるかを整理したチェックリストと共に提示する．（なお，Plan 画面は主に現場層ではなく管理層向けの画面であるため，このチェックリストは管理層向けのチェックリストである.）これにより経験の浅い担当者でも「今，何をすべきか」，更に「今後何をするべきか」を見通すことができる．その他に，組織の長が掲げる目標，会議等のスケジュール，対応フェーズ，会議資料やマニュアル等の参照情報を提供する．

図 4　Plan 画面イメージ

2.2.2 Do 画面

Do 画面を図 5 に示す．図 5 は，非定型情報である連絡処理票の一覧表示画面であり，各組織間の情報連絡が時系列で一覧表示されている．ID，重要，緊急，対応状況，起票日時，更新日時，送信元，送信先，件名，内容，回答，操作ボタンから構成されている．重要度や緊急度の表記や対応状況のレベルに応じた色分け表示により，確認が必要な連絡をすぐに抽出できるようになっている．また，発出した連絡に対する回答は「回答」欄に追記されていくため，1 つの連絡に関するやり取りを 1 スレッドで管理している．

図 5　Do 画面イメージ（連絡処理票）

2.2.3 See 画面

See 画面例を図 6 に示す．See 画面は，被害や対応の状況を俯瞰的に提示するものである．直感的に状況を把握できるように，ISO22324 のカラーコードを参考に，危険な場合に「赤」，安全な場合に「緑」，その間として「黄」とし，システム内で色を統一するようにしている．定型情報に関しては，集計や集約するのが容易であるため，表形式での一覧化や地図上で可視化して表示することで，関係者間の状況認識の統一を効率化する．

図 6　See 画面イメージ

3. サイバー攻撃対応演習での検証

3.1 演習の概略シナリオ

サイバー攻撃対応演習は，2016 年 11 月に開催された．参加組織数は 23，参加者は約 200 名であった．当演習は 8 回目の実施であり，6 組織（Z，A～E）は初回からの参加，5 組織（F～J）は 2 回目の参加，12 組織（K～V）は初参加である．また，Z 組織は A～V の上位組織である．すなわち，基本的には Z は A～V に指示を出し，A～V は Z に報告や回答を行う．

サイバー攻撃対応演習の目的は，対応マニュアルの検証，及び各組織が対応マニュアルに沿った動きをできているかどうかの検証である．その中で，従来使用していたメールやメーリングリストの代替として連絡メッセージ送受信に KADAN®を利用し，組織内及び組織間のコミュニケーションが円滑に行えるかどうかを評価した．

演習のシナリオの概要は以下の通りである．

■シナリオ 1

脅威情報（ソフトウェアの脆弱性情報）を上位組織から下位組織に配信し，該当モジュール使用の有無，攻撃の有無について下位組織から上位組織に調査報告．

■シナリオ 2

サービス妨害攻撃が複数組織で発生したため，連携して対処した結果を上位組織に報告．

3.2 演習での Plan 画面

あらかじめ準備し演習で使用した Plan 画面を図 7 に示す．画面左下の「Operational Planning “P”」が「P」の形ではなく一直線となっているが，それは繰り返し行う可能性のあるプロセスの部分を 1 回だけ記述したためであり，本質的には「P」の形となるものである．

ⓒ2018 Information Processing Society of Japan

図 7 演習での Plan 画面

3.3 演習での See 画面

あらかじめ準備し演習で使用した See 画面を図 8 に示す．今回の演習では各組織からの情報を一覧表として提示した．

図 8 演習での See 画面

これはシナリオ 1 で使用したものであり，各下位組織が対処結果を報告し，上位組織が一覧の形で見るものである．調査のステータスについて左から 4 列目に色分け（対応中が赤（図 8 では黒），完了が青（図 8 ではグレー））で表示され，対応中の組織が分かる．また，各下位組織が入力した内容は上位組織だけが確認できるような開示制御の設定を行った．

3.4 演習における各組織の共通的なふるまい

演習における組織構成，情報連絡の経路と順序を図 9 に示す．

上位組織である Z 以外の組織については，現場チームと統括チームに分かれ，前者は集合会場で，後者は各事業所で演習を行う（ 図 10）．なお，集合会場では組織ごとにホワイトボードを設置した．

また，組織間および組織内での連絡共有/連絡ツールとして，組織内での電話会議装置に加え，一斉同報ができ，また記録が残る KADAN®を利用する．なお，サイバー攻撃対応演習での指示報告内容，および相談内容については他組織等関係者外に見えてはいけないので，図 10 の各矢印に閉じたコミュニケーションが行えるように KADAN®の情報開示設定を行った．

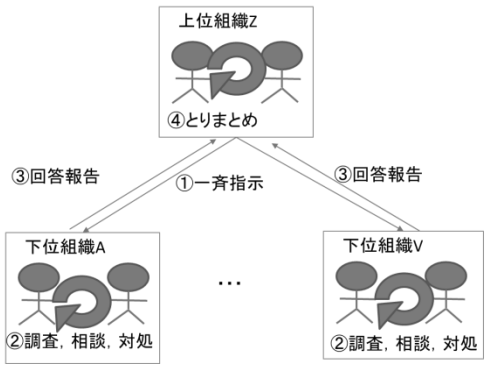

図 9 組織構成，情報連絡経路と順序

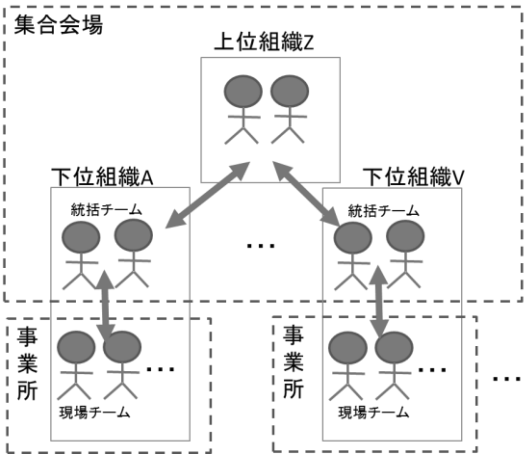

図 10 演習参加者の物理的配置

KADAN®でコミュニケーションがスムーズに行われたかどうかの検証は，KADAN®に記録されたログの分析と，参加者へのアンケートによるものの 2 種類で行った．アンケートでは，以下の項目について意見を収集した．

【Q1】メッセージ送受信に利用した KADAN®について 4 段階評価
（役に立つ，まあまあ役に立つ，あまり役に立たない，役に立たない）
【Q2】メッセージ送受信に利用した KADAN®について，ご意見等あればお願いします．

ⓒ2018 Information Processing Society of Japan

4. 結果と考察

4.1 KADAN®のログによる評価

4.1.1 各組織の投稿数

メッセージ投稿数を表 1 に示す（下位組織の一部は別の下位組織と同一組織として演習に参加したため, KADAN®のログとしては組織数は 21 である）.

Z は上位組織であり, 他の組織に対して情報共有や報告指示のためのメッセージを投稿する.

下位組織である A～T については，組織によって，投稿数が大きく異なる．投稿内容を見ることにより，その理由を以下の 3 種類に分類した.

①組織により異なるシナリオ

②KADAN®以外のツールの利用

③KADAN®に記入する内容

まず「①組織により異なるシナリオ」について述べる．今回の演習では，過去の演習への参加回数に応じて，演習シナリオの複雑度を変えている．また，演習シナリオにおける各組織内での対応内容については，ある程度，各組織に委ねられている．よって，必要なコミュニケーションの量も組織ごとに異なることとなる.

次に「②KADAN®以外のツールの利用」について述べる．各組織における統括チームと現場チームとのコミュニケーションでは，KADAN®だけではなく電話（電話会議システム及び携帯電話）も利用されている．KADAN®と電話との使用割合により, KADAN®に書き込まれるメッセージの件数が異なることとなる．また，サーバ等の ICT 資産を管理するツールを利用している組織については，ソフトウェアの脆弱性が判明した際に，その影響を受ける可能性のあるサーバの一覧を簡単に把握可能であるため，その一覧を把握するために必要なチーム間，チーム内でのコミュニケーションが少なくて済む．このように，KADAN®以外のツールの利用が KADAN®への書き込みの数に影響を与えることとなる.

最後に「③KADAN®に記入する内容」について述べる．統括チームが現場チームに何かの作業を依頼した場合，現場チームから統括チームに結論だけを伝える組織もあれば, 途中経過を随時伝える組織もある．また，統括チーム内，あるいは現場チーム内のコミュニケーションを, KADAN®に書き込む組織と書き込まない組織がある．そのように, KADAN®に書き込むタイミングや内容によって, その件数に違いが生じる.

このように，大きく 3 つの理由により，KADAN®へのメッセージ投稿数に違いが生じることが分かった．メッセージの中身を見ると，いずれの組織でも周知，指示，報告等の組織内外の情報連携が概ね KADAN®上でスムーズに行われていることが分かった．なお②③については，KADAN®の担うコミュニケーションの範囲や内容といった KADAN®の運用ルールが組織によって異なるということである．複数組織間で連携する上では，組織間の連携部分の運用ルールについて各組織の意識が合っていれば，各組織内の運用については各社事情により多少異なっていても問題ないと考えられる.

表 1　連絡メッセージの送受信数結果

組織	統括	現場	総計
Z	20		20
A	15	32	47
B	9	19	28
C	4	0	4
D	16	0	16
E	40	0	40
F	20	2	22
G	37	0	37
H	56	0	56
I	8	9	17
J	14	0	14
K	31	0	31
L	20	0	20
M	8	2	10
N	5	0	5
O	17	2	19
P	6	0	6
Q	7	0	7
R	4	14	18
S	5	1	6
T	5	34	39

4.1.2 投稿数の時間的変遷

メッセージ投稿件数の時間遷移を図 11 に示す．脅威情報配信をトリガーとして各組織・チームへの連絡が即時になされており, 時間経過と共に収束する傾向となっており, 迅速な対処がなされていることが分かる.

メッセージの中身をみると, メッセージ登録が比較的遅かった組織においても，脆弱性対応やインシデント対応のためのコミュニケーションがきちんと行われており，コミュニケーション上の問題が発生しているというわけではなかった.

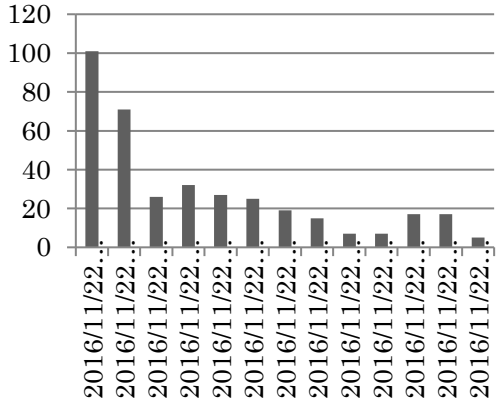

図 11　連絡メッセージ数変遷

ⓒ2018 Information Processing Society of Japan

4.2 アンケートによる評価

アンケートの回答者数は 86 名であった.

4.2.1 【Q1】KADAN®によるコミュニケーションの有効性（4 段階評価）

結果を図 12 に示す. 4 段階評価によるコミュニケーション有効性に関しては, 半分強で「役に立つ」もしくは「まあまあ役に立つ」との評価を得た. 本結果, 及び KADAN®への投稿内容の確認より, KADAN®でのコミュニケーションにおいて特に大きな問題はなかったと考えられる.

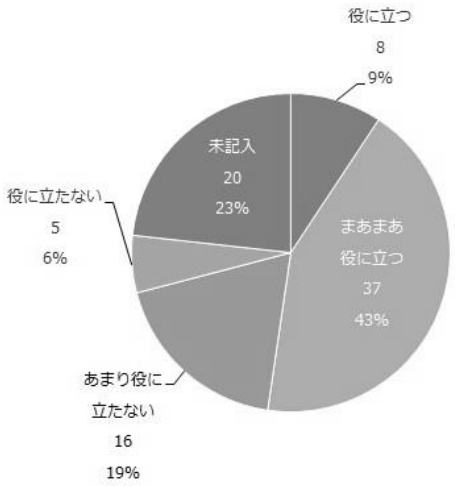

図 12　Q1 の回答結果

4.2.2 【Q2】KADAN®についての意見（自由記述）

図 13 に KADAN®についての意見の, 区分による集計を示す. 視認性の向上, 機能性の向上に関する意見が約半数を占めた. なお,【Q1】にて「役に立たない」もしくは「あまり役に立たない」を選択したユーザの大部分は,【Q2】において視認性の向上, 機能性の向上を挙げている. 危機対応業務においては即時対応が求められるので, 更に分かりやすく容易に利用できるよう機能改善を行い, また KADAN®利用に慣れてもらうための事前の操作訓練が必要と考えられる.

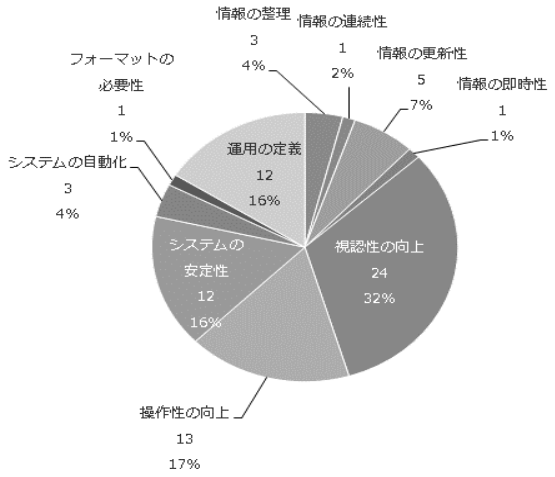

図 13　Q2 の回答結果（区分集計）

4.2.3 個別意見

Plan 画面について, 上位組織 Z のメンバーから「対応プロセスの可視化や, ToDo リストの提示はありがたい」というコメントがあった. Plan 画面により, 今そして次にすべきことについて関係者間で認識を共有することは, 効率的な危機対応のために重要であると考えられる.

Do 画面について,「重要度/緊急度のフラグ, 及びステータス（新規, 対応中, 完了）のフラグについて, 各タスクの状況が分かり便利」とのコメントがあった. 危機対応のような時間が限られている状況において, タスクのそのような属性がひと目で分かることは重要である.

See 画面について,「テンプレートにより入力すべき内容が明確化されているため入力しやすかった」という意見があった. 非定型情報は Do 画面, 定型情報は See 画面で入力, という棲み分けが訓練でも実践できていた.

また,「SNS のような気軽に使えるコミュニケーションツールと連携できるとよい」という意見があった. KADAN®へは「正式な情報や指示」を登録し, SNS ツールでは「正式」ではない気軽なコミュニケーションをとる, という棲み分けがよいのではないか, という意見である. 確かに本システムの Do 画面は, SNS ツールの画面と比較すると情報量も多く, 気軽なコミュニケーションをとるという気持ちにはなりにくいかもしれない. 本システムと SNS ツールを連携させる方法もあるが, 本システムにおいて「簡易版 Do 画面」を用意することで, 気軽なコミュニケーションの場を提供する方法もあると考えられる.

4.3 訓練運営者インタビューによる評価

訓練を実施しその行動内容を評価する立場の人にインタビューを行った.「訓練シナリオに基づき, 時刻や状況に合わせて, 一斉に複数組織へメッセージを送信できると良い」,「KADAN®に書き込まれたメッセージのログをもとに, 依

ⓒ2018 Information Processing Society of Japan

存関係のある複数のメッセージの流れを時刻情報と共に表示できると，“事務局が想定している正しい情報連携”と比較できて良い」という要望が得られた．

これらの要望に対しては，今後対応していきたいと考えている．

5. 結論

本稿では，23 組織，約 200 名による民間企業でのサイバー攻撃に対する危機対応訓練において，組織間・チーム間のコミュニケーションが KADAN®を利用してスムーズに行われたかどうかについて検証した．

訓練はホワイトボード, 電話（電話会議, 及び携帯電話），KADAN®の活用によりスムーズに実施でき，KADAN®に残るログからコミュニケーションの内容や流れを読み取ることができた．

KADAN®での自由記述によるコミュニケーションを演習で活用した結果，半分強で「役に立つ」もしくは「まあまあ役に立つ」との評価を得た．否定的な意見は 4 分の 1 程度という評価結果であり，概ねサイバー分野に適用可能であることが示された．

また，個々の組織でコミュニケーションの運用ルールが異なることが見て取れた．組織体系や組織文化によって最適な運用ルールは異なると考えられる．そうであっても，組織間で連携を取る部分の運用については標準化しておく必要がある．自治体防災や大規模イベントにおいて運用の標準化が重要であることは確認されている[12][13].

今後の課題としては，視認性，機能性の向上を中心としたさらなる利便性向上がある．なお，個々の組織やメンバー，及びその習熟度によって，適切な機能セットや GUI は異なるため，システムは柔軟なカスタマイズ性を持つことが望ましい．また，SNS のように気軽に投稿できる機能も望まれていることが分かった．また，訓練実施者のためには，あらかじめ準備しておいたメッセージを自動的に容易に送る機能や，マニュアルや熟練者の行動ノウハウに基づく理想的行動との差分分析を容易とするための訓練実施結果の分析支援，例えば全体のメッセージ送受信の流れを俯瞰的に表示する等の機能についても整備する必要があると考える．

謝辞 本研究を進めるにあたり，演習を企画運営された事務局の方々，演習に参加して下さった皆様に多大なるご協力を頂いた．謹んで感謝の意を表する．

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] サイバーセキュリティ戦略本部，“重要インフラの情報セキュリティ対策に係る第 4 次行動計画” https://www.nisc.go.jp/active/infra/pdf/infra_rt4.pdf, (参照 2018-5-10).

[3] ISO20121:2012, “Event sustainability management systems – Requirements with guidance for use,” http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54552, (参照 2018-5-10).

[4] 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.

[5] 小阪尚子他, “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.

[6] 東田光裕他, “災害対策本部を対象とする図上訓練における情報処理の分析,” 地域安全学会発表会予稿集, C-5, 2012.

[7] 一ノ瀬文明他，“災害情報システムにおける非定型情報処理の重要性の検証とその効果的な活用方法の提案,” 地域安全学会論文集, No.27, pp. 179-188, 2015.

[8] 小阪尚子他, “総合リスクマネジメント支援システムの検討,” 電子情報通信学会ライフインテリジェンスとオフィス情報システム研究会, 2016.

[9] 中島編，岡部等著，“ISO22301:2012　事業継続マネジメントシステム　―要求事項の解説―,” 日本規格協会, 2013.

[10] 田中靖浩，“米軍式人を動かすマネジメント―「先の見えない戦い」を勝ち抜く D-OODA 経営，”日本経済新聞出版社, 2016.

[11] 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.

[12] Tomohiro Kokogawa et al.,“Efficiency Evaluation of Standard Operating Procedures in a Disaster Information System”, Journal of Disaster Research Vol.12 No.1, 2016

[13] 小阪尚子他，“統合リスクマネジメント支援システム「KADAN」の適用評価 －大規模国際スポーツイベントでの活用－”，FIT2017（第 16 回情報科学技術フォーラム）

ⓒ2018 Information Processing Society of Japan