

WIDE Technical-Report in 2021

NBCA WG Technical Report 2020  
wide-tr-nebuca-nebuca202012.pdf



WIDE Project : <https://www.wide.ad.jp/>

Title: NBCA WG Technical Report 2020  
Author(s): 太田悟史, 砂川真範, 古寺雄馬, 知念賢一  
Date: 2021-02-24

# NBCA WG Technical Report 2020

太田 悟史, 砂川 真範, 古寺 雄馬, 知念 賢一

2021年2月24日

## 1 概要

本稿は、それまで参加者が同じ場所に集合して開催(集合形式)されていたサイバーレンジを利用したイベント(サイバーレンジイベント)を、参加者が個々に分散した地点から参加(分散形式)する形式に切り替える場合に、必要となる課題の整理と解決についてNBCA-WGで検討した内容を報告する。(本稿では、サイバーレンジはサイバー攻撃や防御の演習のために構築された仮想的な空間を指し、実機や仮想マシンを用いる。)

## 2 背景

COVID-19により、それまで参加者が集合して開催されていた集合形式イベントは困難となり、それに代わってインターネットを経由した、参加者が集まらない分散形式が用いられている。サイバーレンジイベントも、それまで集合形式であったイベントが、参加者が遠隔からアクセスする分散形式で開催されている。分散形式でありながらも集合形式時のような内容とするために、リモートミーティングツールが多く用いられている。リモートミーティングツールは、音声やテキスト(チャット)、本人の映像などの画像を通信し、PCの各種画面(デスクトップや、アプリケーションの窓枠)を共有する等の機能を持つもので、仮想的に集合するイベント(ミーティング)に用いられている。しかしリモートミーティングツールを利用し、集合形式イベントを分散形式イベントとして開催しているものの、進行中に問題のあったイベントも確認されている。NBCA-WGでは課題が内包されているとし、問題の整理をその解決を試みることにした。

## 3 サイバーレンジを用いたイベントについて

COVID-19以前から実施されているサイバーレンジイベントには、参加者が集まらずに開催される分散形式と、参加者が集まり集合的に開催される集合形式がある。ここではそれぞれの形式の特徴を把握しつつ、分散形式と集合形式イベントの差異について考える。

分散形式でのイベントは、参加者自身は集合せずに個々に参加するもので、分散形式でのイベントは主に、次のようなものが挙げられる。

- AppGoat(個人学習モード)
- CTF 予選 (SECCON CTF, DEF CON CTF)
- microhardening

AppGoatはIPA(情報処理推進機構)が提供する脆弱性体験学習ツールである。手元のPC上に体験学習環境としてWEB

サーバー、クライアントを構築し、それを用いて脆弱性のあるサーバーへの攻撃について体験するものである。環境を手元の PC で構築、操作し、その内容を共有する機能がないため、個々に独立したイベントといえる。CTF の予選の多くは、一定期間の間に課題を解く内容となっている (Jeopardy)。回答となるフラグ情報をサーバーに登録する事で、その内容と早さを競うものである。何人でもグループとして参加できる。

分散形式でのイベントは、参加者側のタイミングで開始と終了を行えるため時間と場所の制約を受けずにすむ。そのため、独習や個人による参加が多い。参加者はクラウドや仮想マシンファイルとして用意されたサイバーレンジ環境に対して、アクセスやダウンロードを行い、各自で実施する。

サイバーレンジを用いるイベントは、サイバーレンジ環境の他に、イベントの進行管理や参加者の進捗を管理が必要となる。分散形式のイベントの進行は参加者毎に別々に進められるため、参加者自身で管理する。基本的に分散形式のイベントでは、イベント全体の進行管理については CTF のフラグ登録用のサーバー等、簡略的な内容とできる。

集合形式でのイベントは、開催日時と場所を決めて参加者が集まる。参加者は場所と開催時間の束縛を受けるが、開催側主導での進行がし易い。集中形式でのイベントは次のようなものが挙げられる。

- CTF 決勝イベント (DEF CON CTF Finals, CODE BLUE)
- AppGoat(集合学習モード)
- Hardening
- CYDER

集合形式でのサイバーレンジの構築は、現地やクラウドなど自由に提供できる。進行管理は主催側が行う。イベント期間での閉鎖的なサイバーレンジ環境は、セキュリティ面からも隔離が容易であるため、より実践的で高度なコンテンツを扱える。

## 4 集合形式イベントの分散開催

COVID-19 対策により、人が長時間密接する事が制限されている現状では、会食やコンサートを始め、集合形式のイベント全般の開催が困難となっている。イベント開催の中止や参加人数を制限するなどの対応がとられている他に、集合形式のイベントを分散形式で開催している。

分散形式で開催するためにリモートミーティング用ツールを用いて意思の疎通を図っているが、進行が滞る場合がみられる。当 WG ではリモートミーティング用ツールだけでは解決できない問題があると考え、課題の洗い出しを行った。

洗い出しの検討に先だって、検討の対象内容を明らかにしておく必要がある。イベントによってスタッフの役割や構成は様々であるが、本稿ではイベントの参加者の他にイベントの進行役と進行の補助役として、次の構成としている。

- 司会: イベントのメインとして進行を務める。参加者からの質問にも答え、参加者のサポートのため TA に指示を与える場合もある。
- Teaching Assistant(TA): イベントが速やかに進行するために、司会と参加者のサポートを行う。司会からの指示に従うと共に、参加者からの質問にも答える。また、活動が停滞していそうな参加者に対して能動的に働きかける。TA が複数の場合には TA 同士で連携し、参加者への十分なバックアップを提供する。
- 参加者: イベントの参加者として、司会から提供される情報を元に学習や操作を行う。不明な事がある場合には、司会や TA に質問を行う。参加者が個々でイベントを進める場合と、グループを組んで協力して進める場合がある。

なお、サイバーレンジが開催される前後 (準備や撤収) については、司会や TA は関係なく、課題の検討については、時系列的に準備期間、開催期間中のそれぞれについて考察した。

## 4.1 開催準備期間中に考えられる問題

サイバーレンジイベントを分散形式で開催する場合、参加者に向けてサイバーレンジ環境を構築する必要がある。準備期間中に考えられる問題として、次の内容が挙げられる。

- 外部からのアクセス（参加者）  
分散形式イベントでの参加者は匿名性が高く、参加登録時に参加者情報の入力を促して取得したとしても、その内容が参加者個人を特定できる情報かどうかは判断がつかない。そのため、イベント中での評価結果を個人に紐付けるのは難しい。イベント内での評価結果が、参加者の社会的評価に直結する場合には個人の識別が重要となるが、評価結果をイベント内だけにとどめる場合には、参加者情報の正確性について追求する必要はない。
- 複数の構築者によるコンテンツ管理  
参加者だけではなく、開催側での準備作業も集まる事なく、リモートで進める必要がある。この開催側スタッフ間のリモート対応は、それまでのリモートによる打合せやリモートでの協調作業と同じである。サイバーレンジイベントでは、複数の演習課題（コンテンツ）をサイバーレンジ上に設ける場合があり、コンテンツの構築に複数の人数でとりかかる場合には、サイバーレンジのバージョン管理が可能であれば、構築作業の手戻りも少なく済む。

## 4.2 開催中に考えられる問題

サイバーレンジイベントを分散形式で開催する場合を考える。

このイベントは、司会が進行を管理しつつ、TA が遅れないように参加者をバックアップする内容となっている。時間に制限のある進行のため、参加者には大幅な遅れを出さないよう、ある程度の前提条件が必要となる。

- コミュニケーション  
司会、TA、参加者の間で指示や質問、共有を目的とした情報のやりとりに使われるコミュニケーションを分散形式で行う場合、1つの通信チャンネル上でやりとりが行われると、役割によって必要のない情報や届いて欲しくない情報までを共有してしまう。逆に人単位に通信チャンネルを設けると、チャンネル数が著しく増加するために、扱えなくなる。
- 進捗の管理・把握  
答え合わせ用の情報を入力させて整合確認を行うコンテンツ（ジョパティ、CTF）であれば、各参加者の進捗管理はし易い。また、Hardening のように評価指標を売上げに絞る事により、可視化を可能にして優劣がわかりやすくなっている。その一方で、参加者が問題に直面しているか否かを把握する事は難しく、特に TA が分散形式で参加者の様子を把握するのは難しい。

## 5 コミュニケーション

司会、TA、参加者の間で交わされる情報について検討し、必要となるコミュニケーションの形態について考える。

図 1 は、イベント開催中の司会、TA、参加者の間で考えられるコミュニケーションの繋がりを示す。矢印は発信と受信の向きを表しており、ループバックは複数人いる場合に同じ役割の者同士のやりとりを意味する。

コミュニケーションの発信元を考慮すると、9つの辺を持つ有向グラフが考えられる。表 1 は、各辺を 1つの通信チャンネルと捉え、その内容と方式について考えたものである。表の“方向”は、左側が送信元で矢印の右側が送信先となる。また、“内容”は、そのチャンネルを使ってやりとりされるもので、それに適した“伝達方法”を設定している。

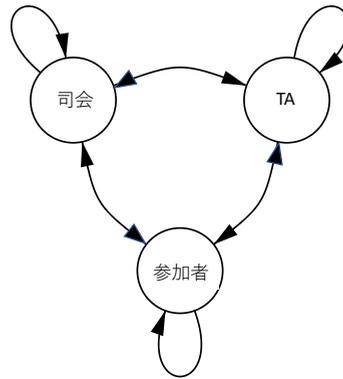


図1 コミュニケーションのグラフ

表1 全グラフとチャンネルの対応

方向	内容	伝達方法	備考
司会→司会	進行の確認や調整	音声やテキスト等	
司会→TA	進行の連絡, 行動指示	音声やテキスト等	
司会→参加者	説明, 指示, 質問等への返答	画像や音声, テキスト等	イベントの詳細な説明
TA→司会	報告, 連絡	音声やテキスト等	
TA→TA	ヘルプ等	音声やテキスト等	
TA→参加者	指摘や指導, アドバイス等	画像や音声, テキスト等	詳細な情報伝達
参加者→TA	質問, 支援の依頼	画像や音声, テキスト等	操作中の端末画面による説明
参加者→司会	質問	画像や音声, テキスト等	
参加者→参加者	報告や指示, 支援等	音声や画像による伝達	グループ内の連携対応

司会とTAは主催側であるため、事前にイベントの内容について理解し、打ち合わせを行う事により、イベント開催中の通信の頻度は抑えられると共に内容も合図のような簡単なものとなる。司会同士,TA 同士も同様に簡単なものになる。参加者との通信の内容は、座学や質疑応答、トラブル対応があり、これには画像を含めた詳細な情報の伝達が必要となる。参加者同士の場合には、相互に協力するためにプログラム等のデータもやり取りする事が考えられる。

## 5.1 チャンネルの整理

前項では司会,TA, 参加者間の2者間について、それぞれのチャンネルで考えられるコミュニケーション内容について述べた。例えば司会が参加者へ向けてイベント中のルールについて説明する場合、個々の参加者に向けたチャンネルではなく、参加者全体に向けた一斉送信が効率が良い。このように内容によって、個々の送信/一斉送信と配送単位の使い分けが必要となる。表2は、内容によって伝達範囲を考察したものである。

司会とTAの開催側については、伝達範囲は対象グループ全体向けのチャンネルがあれば良いと言える。

参加者からTAにむけての伝達は、個々となっている。これは内容について個人差があり,1対1で解決できる場合が含ま

表 2 伝送内容と伝達範囲

方向	内容	伝達範囲	備考
司会→司会	進行の確認	全体	一方的な伝達
	進行の調整	全体	複数者間での意見交換
司会→TA	進行の連絡	全体	
	行動指示	全体	
司会→参加者	説明, 指示	会場全体	TA を含む
	質問等への返答	個々/会場全体	TA を含む
TA →司会	報告, 連絡	全体	
TA →TA	ヘルプ等	全体	TA 内で問題を共有
TA →参加者	指摘や指導, アドバイス等	個々	
参加者→TA	質問, 支援の依頼	個々	
参加者→司会	質問	会場全体	TA を含む
参加者→参加者	報告や指示, 支援等	全体	参加者グループの場合

れているからである。司会と参加者間のチャンネルの場合,TA を含めた会場全員向けに送信する、としている。これは、司会者から発信される情報は、開催側の間でも共有されている必要があるため、同様に参加者から司会者への質問についても、開催側全体で共有されている方が、その後の対応が速やかに行える。以上から、司会と参加者の間のチャンネルについては、会場全体に向けて発信する事が必要となる。

参加者同士でのチャンネルは、グループ単位でのイベント参加となる場合が考えられる。参加者同士での情報共有となるため、グループ内全体への伝達が考えられる。

以上から、チャンネルは次のように1つのメインチャンネルとイベント側に2つのチャンネル、そして参加者サポート用チャンネルと参加グループ用チャンネルの5つにまとめる事が出来る。

- 司会間, 司会～TA 間: イベント主催用チャンネル. 一斉送信で利用
- TA 間: TA 用チャンネル. ヘルプ等, 協力用として一斉送信で利用.
- 司会～参加者間: イベント用チャンネル.TA も参加するメインチャンネルとして一斉送信で利用.
- TA →参加者: サポート用チャンネル
- 参加者→TA: サポート用チャンネル
- 参加者間: 参加グループ用チャンネル

## 5.2 コミュニケーションツールの考察

司会とTA, 参加者で構成されるイベントでは,5つのチャンネルでの対応が可能である事を述べた。イベント用チャンネルはイベントのメインとして, 司会のプレゼンテーションを視聴する。

リモートミーティング用アプリにより, パソコンでやスマートフォン, タブレットでの参加が可能となる。

イベント主催用チャンネルでは, 司会とTA がイベントの進行に関する情報をリアルタイムでやりとりする。タイムキーパーのようなサポート情報を司会に伝えなければならない事から, トランシーバーアプリ等によりイベント用チャンネルとは別に

音声でのやりとりが可能である必要がある.TA 間も同様にトランシーバーアプリを利用する.

参加者サポート用チャンネルでは同様な質問が繰り返される事が想定されるため, 同様な疑問をもつ参加者が後から検索して利用できるよう, 掲示板システムのような機能が求められる.

## 6 議論

### 6.1 進捗の把握

参加型のイベントにおいて, 進行の管理やヘルプの有無の決定, 競争相手との比較など, 進捗の把握は大事である. イベントの進行が段階的である場合には, その区切りにチェックポイントを設けて把握を図る. その段階における問題への答えや, 正解手順により得られるフラグ等による答え合わせなどにより判断が可能となる. あるイベントでは複数の問題を抱えたシステムについて, システムの稼働時間を評価に用いることにより, 個々の問題の把握の代わりにトータルとした持続状態として把握を試みている. これらは, イベント進行中のあるポイントでの結果を知る事ができる. その一方で, 結果が悪かった場合には, その原因や悪い度合いを知る事が難しい. 集合形式イベントでは TA が積極的に参加者に関わる事により, 参加者が抱えている問題点の把握と解決を試みている.

### 6.2 分散イベントと開催規模

分散形式のイベントは, 参加者はインターネットを経由して世界中からアクセスが可能となる. イベントを人的に進行させようとする場合, 時差を考えるとアクセスするタイミングはバラバラであり, また, 開催されるタイムエリアによっては一部の地域の人々の参加は難しくなる. タイムエリアをいくつか分けて開催すれば対応が可能である反面, 開催側のコストが増えてしまう. 開催側の進行や, 参加者へのサービスの省人化が必要となる. 開催側の人的リソースに関わらない, より大規模な分散形式イベントの開催を可能にする仕組みが求められる.

## 7 まとめ

今回我々は, 集合形式イベントを分散形式で開催するために必要となる要素を挙げ, その中からコミュニケーションを中心に考察した. COVID-19 をきっかけとした分散形式イベント方式での開催は, 一極集中していた生活様式の見直しと共に今後も継続的に行われ, より効率のよい技術が考えられて行くと思われる.

集合形式イベントは開催側の人的コストによる制限があったが, 分散形式化すると共にその制限への見直しが行われると思われる. 世界中から超大規模な分散イベントへの参加が可能となるようなサイバーレンジ環境について, 今後も我々は検討を続けたい.