サイバーインシデント発生時初動対応支援・オンサイト対応業務仕様書

1　業務基本要件

(1) 組織委員会は 2021 年 5 月に予定されているワールドマスターズゲームズ 2021 関西大会（以下「本大会」という）の円滑な運営のため、（資料 1）に記載の 13 府県政令市実行委員会、33 開催市町実行委員会とともに各種事業をすすめているところであり、事業遂行にあたり複数のシステムを利用している。受注者は、（資料 2）に示すシステム環境においてサイバーインシデント（おそれ含む　以下「インシデント」という）が発生した際に、事故原因究明、被害範囲確定などを目的とした初動対応支援およびオンサイト対応をおこなうこと。

基本契約は、①準備期間における業務（以下２に記載）、②電話による初動対応支援業務、③オンサイト対応業務・フォレンジック調査業務とし、③については作業時間として 40 時間相当の料金にて提示すること。オンサイト対応業務にかかる旅費・交通費は双方協議の上、別途組織委員会より支払う。

(2) 受注者は、JNSA（特定非営利活動法人　日本ネットワークセキュリティ協会）の会員企業であり、かつ JNSA ホームページにて「サイバーインシデント緊急対応企業」として掲載されており、初動対応支援およびオンサイト対応拠点を国内に設置・運用していること。

(3) 初動対応支援窓口の所在地・主たるオンサイト対応拠点の所在地等を示した業務体制図を提出すること。業務体制図に変更が生じた場合は、変更内容を記載した書面をもって報告すること。

(4) 業務対応は日本語で実施すること。

(5) 受け付けた問合せをインシデントとして管理し、受注者にてインシデント対応完了まで一元的な管理をおこなうこと。

(6) 業務対応中は原則日次で状況報告（特に以下(7)オ・カ等が判明した場合は速報）をおこなうこと。

(7) 業務完了後は業務完了報告をおこなうこと。業務完了報告には以下事項の記載をすること。

ア　インシデントの詳細情報（発生順）
イ　インシデントのタイムライン
ウ　インシデントを構成する事象やイベントなどの関連性
エ　使用された具体的な攻撃手法やインシデントの各段階で悪用された脆弱性
オ　インシデントの根本原因
カ　影響の評価
キ　改善すべき推奨事項

(8) 契約締結後から令和 2 年 11 月 8 日までを準備期間とし、令和 2 年 11 月 9 日から初動対応支援・オンサイト対応・フォレンジック業務を開始すること。

２　準備期間（契約締結後～11 月 8 日）における業務

受注者は、インシデント発生時における円滑な初動対応・各種業務をおこなうことを目的とした以下の各種調査・確認、資料に基づく発注者との協議をおこなうこと。

(1) 組織委員会が利用するシステムの状況・仕様等の確認

(2) 組織委員会におけるインシデント対策（UTM・ログ統合監視システムなどの運用状況）・事後対応（フロー・連絡窓口等）の確認

(3) インシデント発生時、発注者から受注者への状況報告・データ保全方法等（発生した事象を正確に伝えるための確認事項、データ保全・攻撃の痕跡データ保全の方法、データ搬送方法等）の協議

(4) 業務体制図、初動対応支援・オンサイト対応業務フローの作成、資料に基づく協議

(5) 初動対応相談窓口の連絡先等の共有等の事務協議

３　初動対応支援・オンサイト対応・フォレンジック業務（11 月 9 日以降）

(1) 受注者は組織委員会よりインシデント発生の連絡を受けた際、24 時間 365 日、電話にて必要な初動対応支援をおこなうこと。

また、ヒアリングを受けて、インシデントが深刻である場合、エスカレーション対応が必要である場合には、インシデント発生連絡を受けた後、4 時間以内に「インシデント対応に関して高度な専門知識を有する対応者」を定め、速やかに二次的対応をおこなうこと。

(2) 組織委員会より現場陣頭指揮依頼等を含めオンサイト対応依頼があった場合、または受注者がインシデントの深刻度合いを鑑み、オンサイト対応必要であると判断した場合、オンサイト対応決定から 36 時間以内に発注者指示の現場（日本国内）に到着し、オンサイト対応業務を開始すること。

(3) データ保全や攻撃の痕跡データの保全等にあたり、電話等で助言をおこなうこと。

(4) インシデントの影響を受けた可能性のあるコンピュータシステムのメモリ分析、モバイルデバイス等の分析をおこなうこと。

(5) 原因究明等にあたり、組織委員会が設置した UTM 等のセキュリティ機器や統合ログ監視システム等で保全されたネットワークトラフィックや各種ログの分析をおこなうこと。

(6) インシデントに関係する可能性のあるマルウェアまたはその他のバイナリファイルを分析すること。

(7) インシデントに関係するネットワークイベントまたはシステムログイベントを分析すること。

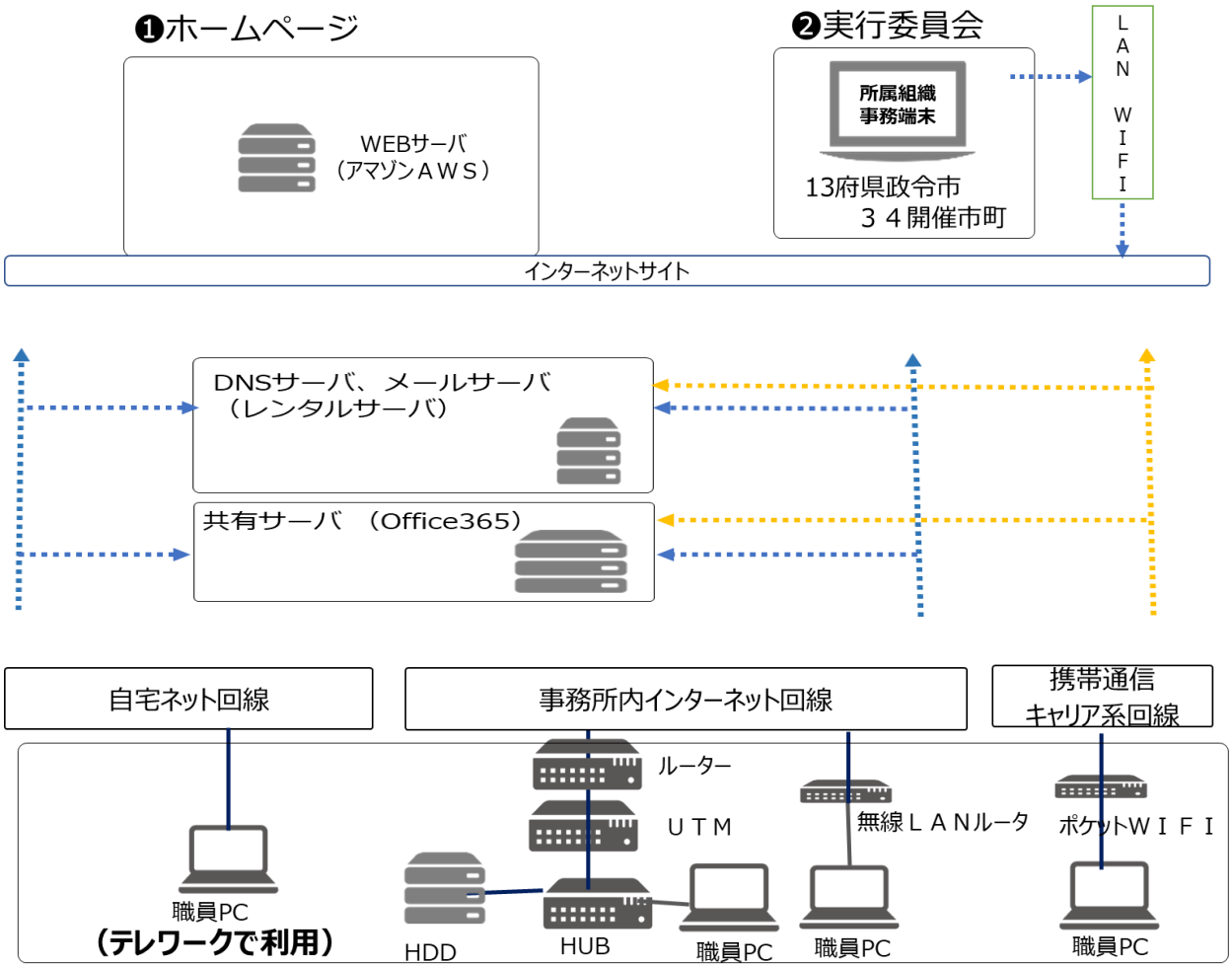
(8) 上記以外にも原因究明・影響範囲調査などにあたり技術的な調査手法を検討すること。

(9) 組織委員会との十分な協議および合意に基づき、各種業務を開始すること。

（資料 1）実行委員会一覧

府県	府県市町	各実行委員会の正式名称	
福井県	福井県	ワールドマスターズゲームズ2021関西 福井県実行委員会	1
滋賀県	滋賀県	ワールドマスターズゲームズ2021関西・滋賀実行委員会	2
	大津市	ワールドマスターズゲームズ2021関西・大津市実行委員会	3
	彦根市	ワールドマスターズゲームズ2021関西・彦根市実行委員会	4
	草津市	ワールドマスターズゲームズ2021関西・草津市実行委員会	5
	守山市	ワールドマスターズゲームズ2021関西・守山市実行委員会	6
	東近江市	ワールドマスターズゲームズ2021関西・東近江市実行委員会	7
	米原市	ワールドマスターズゲームズ2021関西米原市実行委員会	8
京都府	京都府	ワールドマスターズゲームズ2021関西京都府実行委員会	9
	福知山市	ワールドマスターズゲームズ2021関西福知山市実行委員会	10
	宇治市	ワールドマスターズゲームズ2021関西宇治市実行委員会	11
	京田辺市	ワールドマスターズゲームズ2021関西京田辺市実行委員会	12
	京丹後市	ワールドマスターズゲームズ2021関西京丹後市実行委員会	13
	南丹市	ワールドマスターズゲームズ2021関西南丹市実行委員会	14
	和束町	ワールドマスターズゲームズ2021関西和束町実行委員会	15
	京丹波町	ワールドマスターズゲームズ2021関西京丹波町実行委員会	16
大阪府	大阪府	「ワールドマスターズゲームズ2021関西」大阪府実行委員会	17
	岸和田市	「ワールドマスターズゲームズ2021関西」岸和田市実行委員会	18
	東大阪市	ワールドマスターズゲームズ2021関西東大阪市実行委員会	19
	泉南市	ワールドマスターズゲームズ2021関西泉南市実行委員会	20
兵庫県	兵庫県	ワールドマスターズゲームズ2021関西 兵庫県実行委員会	21
	姫路市	ワールドマスターズゲームズ2021関西 姫路市実行委員会	22
	尼崎市	ワールドマスターズゲームズ2021関西 尼崎市実行委員会	23
	三木市	ワールドマスターズゲームズ2021関西 三木市テニス競技準備委員会	24
	加西市	ワールドマスターズゲームズ2021関西 加西市実行委員会	25
	養父市	ワールドマスターズゲームズ2021関西 養父市実行委員会	26
	南あわじ市	ワールドマスターズゲームズ2021関西 南あわじ市大会実行委員会	27
	宍粟市	ワールドマスターズゲームズ2021関西 宍粟市実行委員会	28
	神河町	ワールドマスターズゲームズ2021関西 神河町実行委員会	29
	香美町	ワールドマスターズゲームズ2021関西 香美町オリエンテーリング大会運営委員会	30
奈良県	奈良県	「ワールドマスターズゲームズ2021関西」奈良県実行委員会	31
	葛城市	「ワールドマスターズゲームズ2021関西」綱引実行委員会	32
	吉野町	「ワールドマスターズゲームズ2021関西」吉野町実行委員会	33
和歌山県	和歌山県	ワールドマスターズゲームズ2021関西 和歌山県実行委員会	34
鳥取県	鳥取県	ワールドマスターズゲームズ2021関西鳥取県実行委員会	35
	鳥取市	ワールドマスターズゲームズ2021関西鳥取市実行委員会	36
	米子市	ワールドマスターズゲームズ2021関西米子市実行委員会	37
	倉吉市	WMG2021関西自転車競技倉吉市・北栄町実行委員会	38
	湯梨浜町	ワールドマスターズゲームズ2021関西湯梨浜町実行委員会	39
徳島県	徳島県	ワールドマスターズゲームズ2021関西徳島県実行委員会	40
	那賀町	(仮)ワールドマスターズゲームズ2021関西那賀町競技実行委員会	41
	美波町	ワールドマスターズゲームズ2021関西美波町競技実行委員会	42
京都市	京都市	「ワールドマスターズゲームズ2021関西」京都市実行委員会	43
大阪市	大阪市	ワールドマスターズゲームズ2021関西大阪市実行委員会	44
堺市	堺市	ワールドマスターズゲームズ2021関西堺市実行委員会	45
神戸市	神戸市	ワールドマスターズゲームズ2021関西神戸市実行委員会	46

（資料 2）



❸組織委員会

❶ホームページ

インシデント発生時は、ホームページ運用委託事業者（主にホームページの表示更新作業等を委託）が持つログ情報等を基にして AWS サーバ（WEB サーバ・DB サーバ）に係るインシデント対応をおこなうこと。

❷実行委員会

13 府県政令市実行委員会・33 開催市町実行委員会が利用する端末（自治体所有端末、競技団体所有端末）に係るインシデント対応をおこなうこと。

❸組織委員会

LAN 接続時、WIFI 接続時、テレワーク環境時における職員 PC・HDD・共有サーバ（Offoce365 サーバ）に生じたインシデント対応をおこなうこと。レンタルサーバに関連したインシデントについては、組織委員会がレンタルサーバ運営事業者の協力を得ながら証跡等を入手することとし、入手できた証跡等に基づきインシデント対応をおこなうこと。