資料４

【機密性2情報】

東京オリンピック・パラリンピック競技大会等の大規模国際イベントにおけるサイバーセキュリティの確保に向けた取組の今後の活用方策に関する有識者会議
第１回会合

事務局説明資料
（大規模国際イベントにおけるサイバーセキュリティの確保に向けた取組）

2021年２月

内閣官房　内閣サイバーセキュリティセンター

大規模国際イベントにおけるサイバーセキュリティの確保に向けた取組

1　リスクマネジメントの促進

(1) リスクアセスメント

(2) 横断的リスク評価

(3) スポーツ関係団体に対する勉強会

2　対処態勢の整備

(1) 対処体制

(2) 対処支援調整

(3) サイバー攻撃への対処能力の向上

(4) 予防・検知に関する情報の発信・共有

(5) 情報共有プラットフォーム（JISP）の提供

3　有識者会議における検討事項例

1　リスクマネジメントの促進

大規模国際イベントにおけるサイバーセキュリティの確保に向けた取組（リスクマネジメントの促進）

サイバーセキュリティ基本法（平成26年法律第104号）に基づくサイバーセキュリティ戦略（平成30年７月27日閣議決定）に則り、大会の運営に大きな影響を及ぼし得る重要サービス事業者等を対象としたリスクマネジメントの促進や、関係府省庁、大会組織委員会、東京都等を含めた関係組織と、サイバーセキュリティに係る脅威・事案情報の共有等を担う中核的組織としてのサイバーセキュリティ対処調整センターの構築等、対処態勢の整備を推進。

サイバーセキュリティの確保に向けた取組

リスクマネジメントの促進
（事前対応のための取組）

- ○ リスクアセスメント 【事業者等が自主的に実施する取組】
- ○ 横断的リスク評価 【NISCが評価する取組】
- ○ スポーツ関係団体に対する勉強会等

対処態勢の整備
（事案発生時の迅速かつ的確な対処のための取組）

- ○ 対処体制
- ○ 対処支援調整
- ○ サイバー攻撃への対処能力の向上
- ○ 予防・検知に関する情報の発信・共有
- ○ 情報共有プラットフォーム（JISP）の提供

1(1) リスクアセスメント（取組の概要）

●リスクアセスメントの取組

サイバー攻撃等による東京2020大会の準備・運営への影響の未然防止や軽減等のため、大会を支える周辺サービスを提供する事業者等によるリスクマネジメントの強化を通じ、想定されるサイバーセキュリティ上のリスクへの対策を促進。
2016年度から、東京大会において開催・運営に影響を与える重要サービス事業者等を選定した上で、 NISCにおいてリスクの低減と最新のリスクへの対応を目的とした手順書を作成し、当該手順書に沿って各組織がリスクアセスメントを実施。NISCが実施結果を横断的に分析し、各事業者等にフィードバック。

○ リスクアセスメントの促進のため、サイバーセキュリティリスクを特定・分析・評価する手順をNISCで作成

○ 大会の準備・運営に影響に与えうる重要サービス分野から、重要サービス事業者等を関連する所管省庁と調整の上で選定

重要サービス分野 ＋ 会場（競技会場及び非競技会場）

通信、放送、金融、航空、鉄道、電力、ガス、上水道、物流、クレジット、行政サービス（地方公共団体）、下水道、空港、道路・海上・航空交通管制、緊急通報、気象・災害情報、出入国管理、高速道路、熱供給、バス、警備、旅行、病院（病院分野の業務に支障を来さない範囲で対応）、会場

○ NISCが想定する『「事業・重要サービス・経営資源（情報資産）」のモデルケース（重要サービス分野ごと）』、『業務の阻害につながる事象の結果、結果を生じ得る事象（脅威）及びリスク源』を作成、各事業者等へ経営資源、リスク源等の洗い出しの漏れの可能性をフィードバックすることによって、より網羅的なリスクアセスメントの実施を促進

○ サイバーセキュリティ対策の運用状況について、NISCからフィードバックを実施し、必要に応じて助言を実施

1(1) リスクアセスメント（全体像）

対象とするリスク

情報、情報システム、制御システム等の情報資産に係る事象の結果（自然災害やサイバー攻撃等に起因するIT障害）から認識されるリスク

基本的な考え方

全世界からの注目を集める2020年東京オリンピック・パラリンピック競技大会を直接的・間接的に支える重要なサービスを提供する事業者等には、そのサービスを安全かつ継続的に提供することが期待される。

そのために必要な措置を事業者等が自身で講じられるようにするためには、リスクを特定・分析・評価することが必要。

<イメージ>

2020年東京オリンピック・パラリンピック競技大会の成功

成功のためには…

（要件）大会開催に必要なサービスが安全かつ継続的に提供されること
⇒ 大会開催に向けた各関係主体の活動目的

機能を保証するためには…

活動目的に対する不確実さ（＝リスク）を特定・分析・評価し、必要な対処につなげることが重要

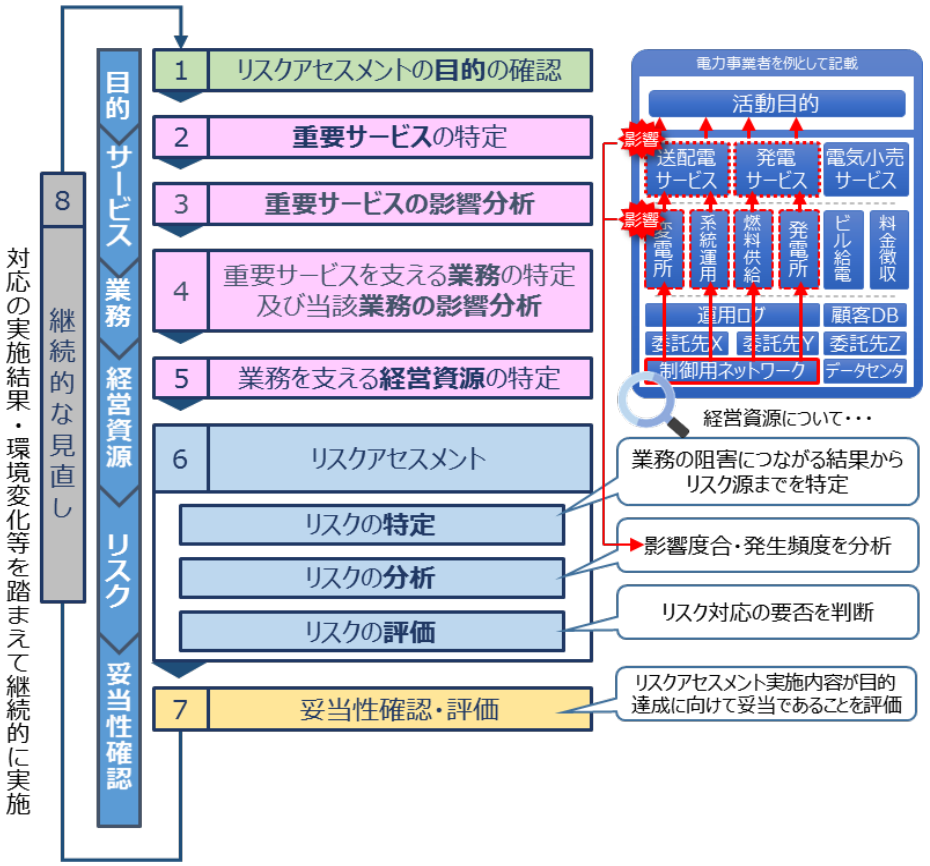
各関係主体が、

① 大会開催を支える重要なサービス及び必要なサービスレベルを特定し、

② そのサービス提供を全うすることに対するリスクを特定・分析・評価することが重要（機能保証のためのリスクアセスメント）

機能保証のためのリスクアセスメントの枠組み

「機能保証の観点から、事業者等が社会経済システムの中で果たすべき役割・機能を発揮するために維持・継続することが必要なサービスを特定」し、その「サービス提供の維持・継続に必要な業務や経営資源に係る要件を分析・評価」した上、これらに影響する「事象の結果からリスク源までを分析」していく。

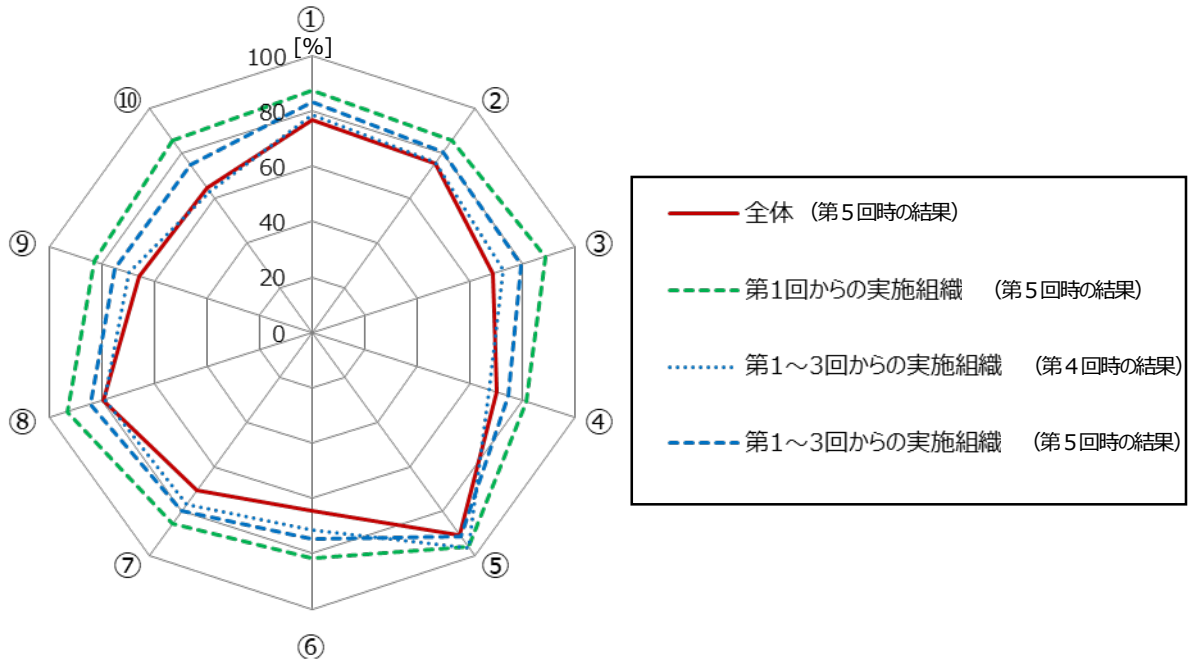


1(1) リスクアセスメント（サイバーセキュリティ対策の全般的な運用状況）

第５回（2019年９月～12月に実施）終了時点での、各事業者等のサイバーセキュリティ対策の全般的な運用状況は以下のとおり。

- 「Check」(⑨)、「Act」(⑩)及び「Do」の⑥の実施率は、他と比べてやや低い。
- 第１～３回から実施の組織について、前回回答と比較して、多くの項目でも５ポイント前後上がっており、本取組を通じてサイバーセキュリティ対策の運用改善に取り組んでいることがうかがえる。
- 特に、第1回から実施の組織については、各回の取組を経て、演習・訓練に取り組むことで、大会本番に備えているとともに、是正すべき対策の検討を進めていることがうかがえる。

Plan	①	基本方針の策定
	②	内規等の策定
	③	対策の計画策定
	④	研修実施
	⑤	内部統制の強化
Do	⑥	コンティンジェンシープランの策定
	⑦	事業継続計画の策定
	⑧	演習・訓練の実施
Check	⑨	監査の実施
Act	⑩	是正すべき対策の検討



1(1) リスクアセスメント（結果に関するフィードバック）

各事業者等から提出されたリスクアセスメント結果に対して、NISCにて以下の観点で分析し、
各事業者等に対して個別にフィードバックを実施。

リスクアセスメント結果

No.	経営資源（情報資産）システム番号（記入例：①）	経営資源（情報資産）	業務の阻害につながる事象の結果	結果を生じ得る事象	リスク源	フィードバックレポート反映箇所
1	①	Aシステム	システムの停止	不正な処理・機能の実行	不正検知システムの未導入・不備	【外部不正：不正な処理・機能の実行】 【偵察、配送、遠隔操作、目的の実行】（ｻｲﾊﾞｰｷﾙﾁｪｰﾝﾌﾟﾛｾｽ） 【可用性】
2					ネットワーク[illegible]	【外部不正：不正な処理・機能の実行】 【偵察】（ｻｲﾊﾞｰｷﾙﾁｪｰﾝﾌﾟﾛｾｽ） 【可用性】
3					[illegible]ポリシーの未策定	【外部不正：不正な処理・機能の実行】 【偵察】（ｻｲﾊﾞｰｷﾙﾁｪｰﾝﾌﾟﾛｾｽ）

提出された「リスクアセスメント結果」において、Aシステムのリスク源がNISCが例示した「結果を生じ得る事象（脅威）とリスク源」のどれに対応するかを分析

フィードバックレポート

C. 結果を生じ得る事象（脅威）とリスク源

○外部不正

モデルケース	貴組織からご提出いただいた実施結果（第３回）	貴組織からご提出いただいた実施結果（第４回）	サイバーキルチェーンのプロセス（攻撃者視点）	貴組織からご提出いただいた実施結果（第3回）	貴組織からご提出いただいた実施結果（第４回） 業務の阻害につながる事象の観点におけるリスク源の洗い出し状況 （可用性）	（完全性）	（機密性）
不正な処理・機能の実行	不正な処理・機能の実行	不正な処理・機能の実行	偵察	-	○	×	×
			配送		○	×	×
			侵入、インストール	-	×	×	×
			遠隔操作 目的の実行		○	×	×
サービス妨害攻撃	-	-	偵察	-	×	×	
			配送、侵入・感染、インストール、遠隔操作、目的の実行	-	×	×	
脆弱性を標的にした攻撃	-	-	偵察	-	×	×	×
			配送、侵入・感染、インストール、遠隔操作、目的の実行	-	×	×	×

（例）「リスクアセスメント結果」の「フィードバックレポート反映箇所」の記載が以下の場合

【外部不正：不正な処理・機能の実行】
【配送、遠隔操作、目的の実行】(ｻｲﾊﾞｰｷﾙﾁｪｰﾝﾌﾟﾛｾｽ)
【可用性】

「フィードバックレポート」の記載場所
- 「外部不正」⇒「不正な処理・機能の実行」⇒「配送」⇒「可用性」に“○”
- 「外部不正」⇒「不正な処理・機能の実行」⇒「遠隔操作、目的の実行」⇒「可用性」に“○”

- 「リスクアセスメント結果」に記載されたリスク源が当てはまる箇所に「○」を記載
- 当てはまるリスク源が「リスクアセスメント結果」に記載されていない場合は「×」を記載

1(2) 横断的リスク評価（取組の概要）

●横断的リスク評価の取組

重要サービス事業者等において想定されるサイバーセキュリティリスクに基づき、サイバーセキュリティ対策の実施状況をNISCが検証する。
これにより、大会の成功にとって重要な機能が継続して提供されることを確認するとともに、不備があった場合は、重要サービス事業者等へフィードバックすることにより、当該重要な機能が継続して提供されることの確からしさを向上させる。

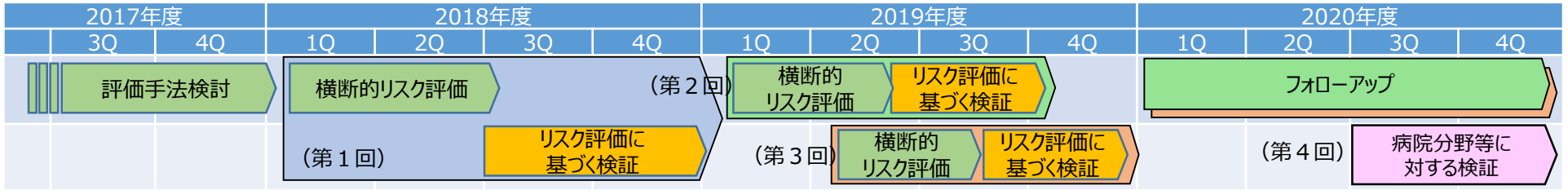
○ 大会に関わるリスクが顕在化するシナリオをリスクシナリオとして策定・活用し、重要サービス事業者等が設定したルールの妥当性や実効性について検証（リスクリシナリオ検証）

○ 第１回の取組においては、電力、通信、水道、鉄道、放送等５者程度を対象に実地検証。全重要サービス分野から20者程度を対象に書面検証

○ 第２回及び第３回の取組においては、重要サービス事業者等（会場（レガシー部分）を含む。）を対象に検証（実地又は書面）
なお、会場のオーバーレイ部分の対策の整備状況及び監督状況については、組織委を対象に実地検証

○ 第４回の取組においては、コロナウイルス感染症の感染拡大等の情勢変化を踏まえ、病院分野等を対象に実地又は書面検証
（病院分野の業務に支障を来さない範囲で対応）

○ 会場・病院分野については、業務、情報システム、制御システム等を把握した上で、会場・病院の機能が継続的かつ適切に提供されることを確認することを目的としたチェックリストを策定・活用して、会場・病院が設定したルールの妥当性や実効性について検証（チェックリスト検証）



1(3) スポーツ関係団体に向けた勉強会（取組の概要（2020年度））

リオ2016大会でスポーツ関連団体がサイバー攻撃の被害にあったことを受け、2017年よりNISCとスポーツ庁が事務局となり隔月ペースで東京オリンピック・パラリンピック競技団体等を対象とした勉強会を開催。

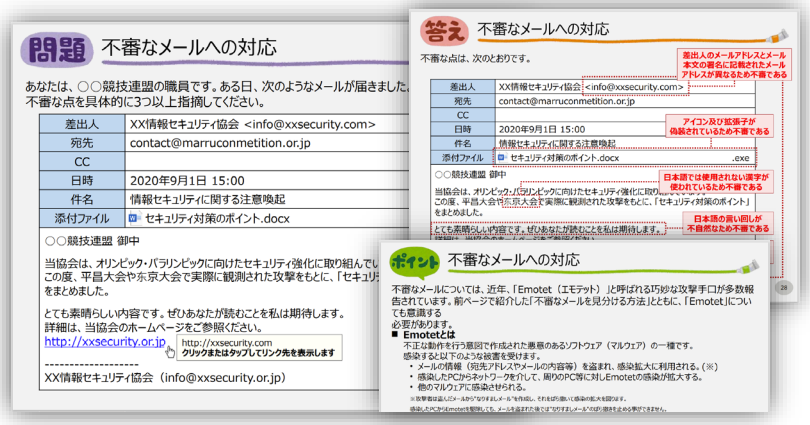
○ 取組概要

・第15回勉強会「インシデントハンドリング模擬演習」
日時：2020年11月25日
場所：日本青年館ホテル＋オンライン
概要：模擬演習を通じてインシデント対応を体験するグループワーク。
感染症拡大防止の観点から、会場参加とオンライン参加のいずれかを選択可能とし、会場のみならずオンライン上でもグループ分けしてグループワークを実施。

・自己学習用コンテンツ提供
期間：2020年９月～12月
概要：過去勉強会（右表）の理解度を確認するとともに、振り返りを通じてさらなる勉強会内容の定着を図るため、クイズ形式の自己学習用コンテンツを８回に分けて提供

・CTI情報の発信
期間：2020年４月～（大会まで継続）
概要：JISPで発信される情報について、スポーツ関連団体のリテラシを考慮して取捨選択した上で隔週ペースで提供（深刻度、緊急度に応じては、随時発信）

・Webサイトに対する簡易チェック（フォローアップ）
時期：2020年４月～12月
概要：Webサイトの改善状況を確認するため再度簡易チェックを実施（IPAによる協力）



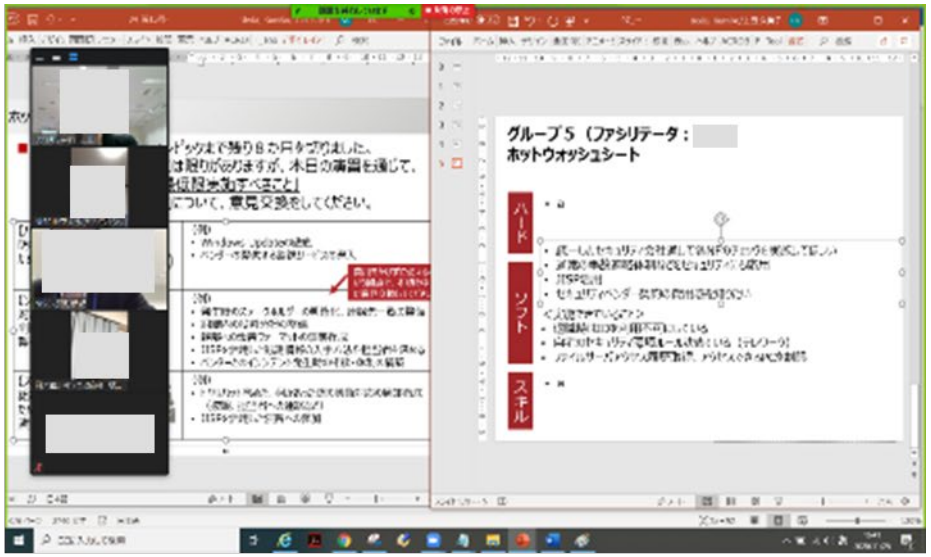
自己学習コンテンツの例

表：過去勉強会一覧

取組回	開催時期		勉強会開催テーマ
第１回	2017年度	７月	個人情報保護
第２回		９月	標的型メール攻撃対策
第３回		12月	スポーツ関連団体における取組の共有
第４回	2018年度	５月	利用者が意識すべきサイバーセキュリティ対策
第５回		７月	管理者が意識すべきサイバーセキュリティ対策
第６回		９月	サイバー攻撃への技術的対策
第７回		11月	組織的なサイバーセキュリティ対策
第８回		１月	インシデントハンドリング演習体験
第９回		３月	平成３０年度勉強会のまとめ
第10回	2019年度	５月	リスクアセスメント（概要）
第11回		７月	リスクアセスメント（詳細）
第12回		９月	インシデントハンドリング（前編）
第13回		11月	インシデントハンドリング（後編）
第14回		１月	CSIRTの構築及び運用
第15回	2020	11月	インシデントハンドリング模擬演習

勉強会の内容（第15回）

2020年11月25日（水）の第15回勉強会では「インシデント対応に係る模擬演習」をテーマに、模擬演習を通じてインシデント対応を体験するグループワークを実施。感染症拡大防止の観点から、会場参加とオンライン参加のハイブリッド方式とし、会場のみならずオンライン上でもグループ分けして演習を実施。



（ファシリテーターがオンラインを含む各グループの議論進行を補助）

1(3) スポーツ関係団体に対する勉強会等（スポーツ関連団体及び地方公共団体向け簡易Webチェック）

背景と目的

リオ2016大会では、サイバー攻撃の対象がスポーツ関連団体やリオ州等政府機関のWebサイトに及び、個人情報が流出するなどの被害が生じた。2020東京大会に向けて、スポーツ関連団体や地方公共団体のWebサイトの状況をチェックしフィードバックを行うことで対策の実施を促進。

実施状況

- ・2019年10月　スポーツ関連団体のWebサイトに対してチェック実施及びレポート送付（新規チェック）
- ・2020年２月　スポーツ関連団体等のWebサイトに対してチェック実施及びレポート送付（再チェック及び新規チェック）
- ・2020年９月　スポーツ関連団体等のWebサイトに対してチェック実施（再々チェック及び新規チェック）し、2020年12月にレポート送付

フォローアップ状況

2020年12月に各団体に対し、不備があったチェック項目について積極的な修正対応を推奨するとともに、万一のインシデント発生時には、JISP（情報共有システム）を利用してサイバーセキュリティ対処調整センターに相談するよう依頼。

2　対処態勢の整備

大規模国際イベントにおけるサイバーセキュリティの確保に向けた取組（対処態勢の整備）

サイバーセキュリティ基本法（平成26年法律第104号）に基づくサイバーセキュリティ戦略（平成30年７月27日閣議決定）に則り、大会の運営に大きな影響を及ぼし得る重要サービス事業者等を対象としたリスクマネジメントの促進や、関係府省庁、大会組織委員会、東京都等を含めた関係組織と、サイバーセキュリティに係る脅威・事案情報の共有等を担う中核的組織としてのサイバーセキュリティ対処調整センターの構築等、対処態勢の整備を推進。

サイバーセキュリティの確保に向けた取組

リスクマネジメントの促進
（事前対応のための取組）

- ○ リスクアセスメント 【事業者等が自主的に実施する取組】
- ○ 横断的リスク評価 【NISCが評価する取組】
- ○ スポーツ関係団体に対する勉強会

対処態勢の整備
（事案発生時の迅速かつ的確な対処のための取組）

- ○ 対処体制
- ○ 対処支援調整
- ○ サイバーインシデント対応演習等
- ○ 予防・検知に関する情報の発信・共有
- ○ 情報共有プラットフォーム（JISP）の提供

2(1) 対処体制（体制構築の目的等）

大会の成功に向け、事案発生の未然防止及び発生時における迅速かつ的確な検知・対処のために必要となる体制を構築

大会の安全な開催及び継続性の確保のため

○ 相互信頼、情報共有
⇒ 相互の信頼関係の構築

○ 迅速な連携、的確な報告
⇒ 支援調整

○ 情報の集約と提供、対処状況把握
⇒ 関係機関等による自律的な未然対処及び事案対処

2(1) 対処体制（参加組織）

対象とする組織

◆ 大会組織委員会（パートナー含む。）
◆ 東京都
◆ 会場のある地方公共団体
◆ 重要サービス事業者等
　　通信、放送、金融、航空、鉄道、電力、ガス、上水道、物流、クレジット、
　　行政サービス（地方自治体）、下水道、空港、道路・海上・航空交通管制、緊急通報、
　　気象・災害情報、出入国管理、高速道路、熱供給、バス、警備、旅行、病院
◆ 会場管理者
◆ スポーツ関連団体
◆ 関係府省庁（重要サービス事業者等の所管省庁等）

対処支援調整の対象（関係機関等）

◆ 情報セキュリティ関係機関（NICT、IPA、JPCERT/CC、JC3）
◆ 治安機関
◆ セキュリティ情報センター

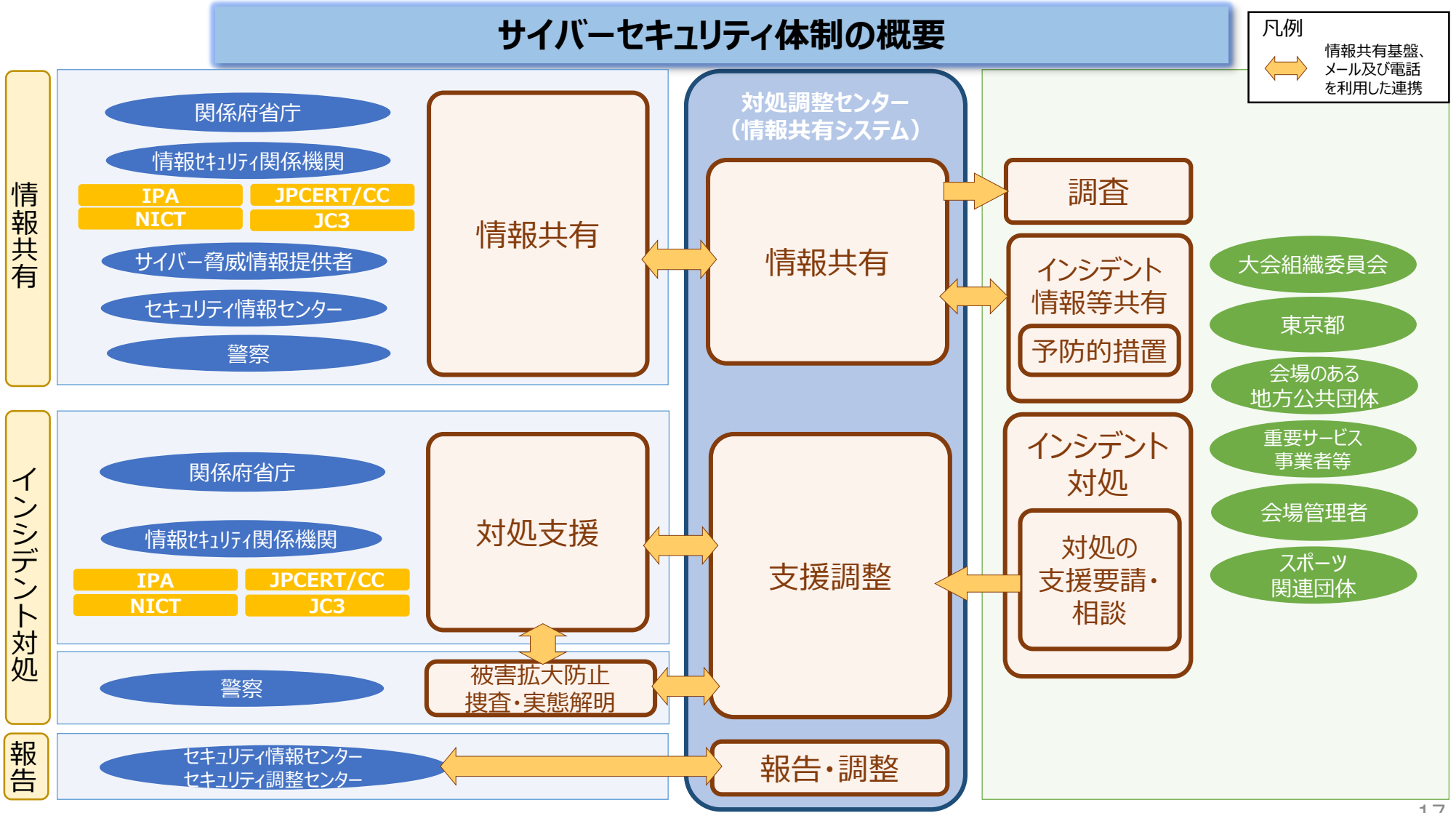
情報提供・共有の対象

◆サイバー脅威情報提供者（本取組にご協力頂いている民間事業者）

情報提供の対象

2(1) 対処体制（体制の概要）

大会の安全・円滑な準備及び運用並びに継続性を確保するために、各組織が相互に協力して取り組みます。本体制の概要を下図のとおり示します。



2(1) 対処体制（サイバーセキュリティ対処調整センターの構築）

- 大会のサイバーセキュリティに係る脅威・インシデント情報を収集し、これら情報を大会組織委員会を始めとした関係機関等に提供、必要があるときには関係機関等のインシデント対処に対する**対処調整**を実施
- 2019年４月１日に設置
- センターの構築及び運用は、オリパラ推進本部の下で、オリパラ事務局と緊密に連携し、内閣サイバーセキュリティセンターが中心となって実施

対処調整センターが提供するサービス

インシデント発生時の対処支援
- ✓ インシデント発生時には、対処支援を要請することが可能
- ✓ 困ったときなど、インシデント以外でも気軽に相談をすることが可能

サイバーインシデント対応演習機会の提供
- ✓ インシデント発生時の対応力向上、連絡体制確立を目的とした演習に参加可能

有用な情報、情報共有システム（JISP※）の提供
- ✓ 大会のサイバーセキュリティに係る脅威・インシデント情報を受け取ることが可能
- ✓ 各事業者の利用者間や対処調整センターとのコミュニケーションが可能

※Japan cyber-security Information Sharing Platform

連絡体制

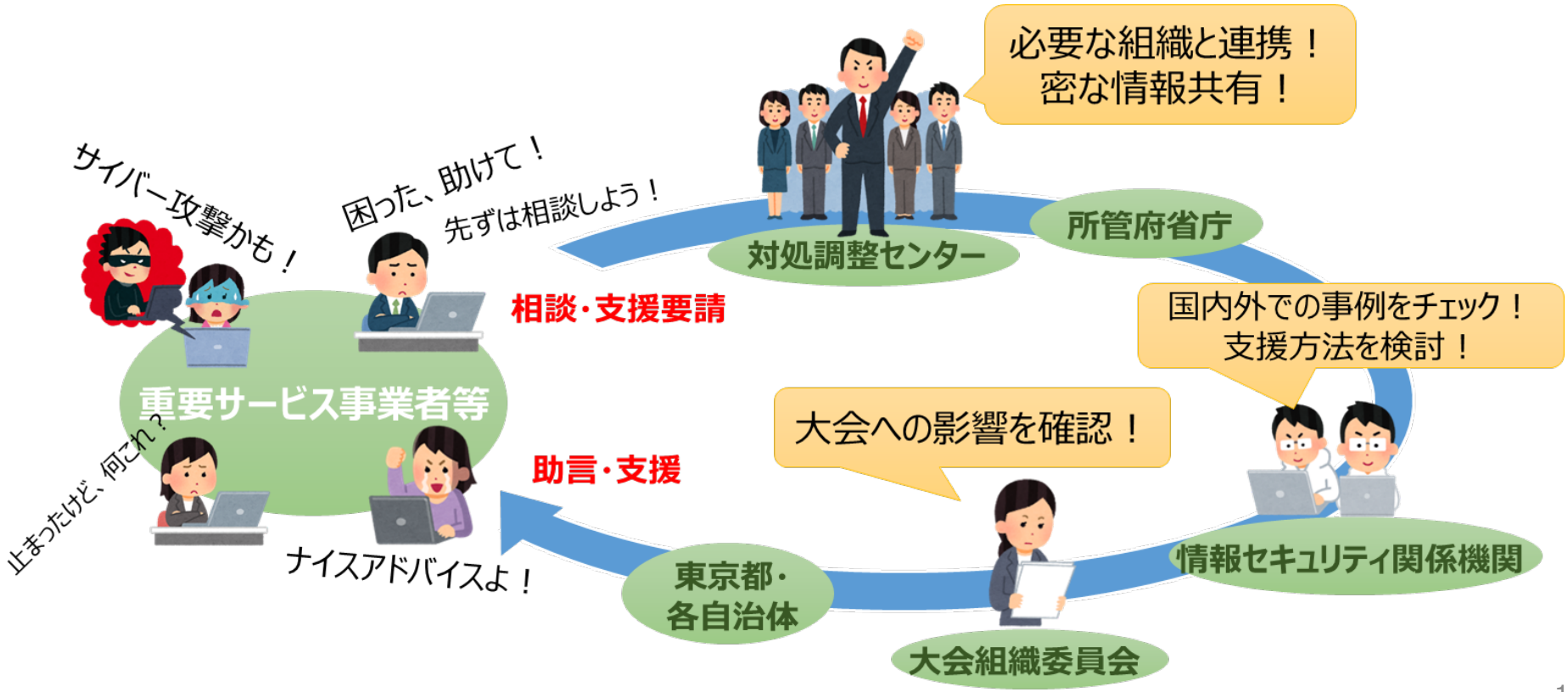
- ✓ 情報共有システム（JISP）、電話及びメールによる連絡体制を確立
- ✓ 原則、情報共有システム（JISP）を用いて連絡（必要に応じて電話又はメールを併用）
- ✓ 大会期間中は、24時間連絡が可能となる窓口を設置

2(2) 対処支援調整（インシデント（のおそれ含む。）発生時の対処支援）

インシデント（のおそれ含む。）が発生したときに、サイバーセキュリティ対処調整センターの仕組み、機能を活用し、関係組織が一丸となって対応

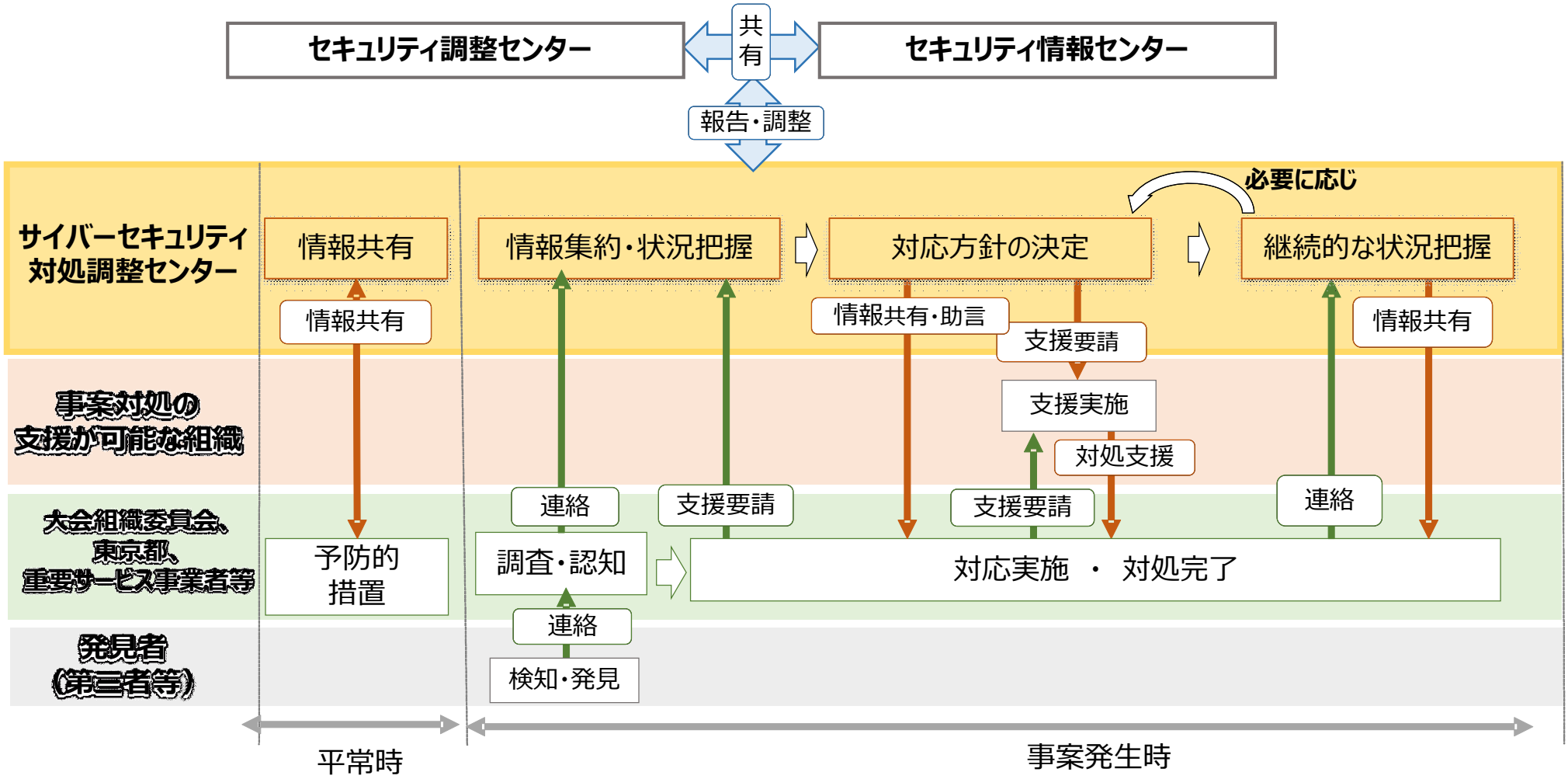
【サイバーセキュリティ対処調整センターの仕組み等の活用による特徴】

- 必要な関係組織と速やかに連携が可能（組織別にバラバラと連絡を取らなくてもよい。）
- 大会への影響を確認可能
- インシデント対処に役立つ助言や支援を受けることが可能



2(2) 対処支援調整（対処支援調整等の流れ）

➢ 2020年東京オリンピック競技大会・東京パラリンピック競技大会のサイバーセキュリティに係る脅威・インシデント情報を収集し、これら情報を大会組織委員会を始めとした関係機関等に提供、必要があるときには関係機関等のインシデント対処に対する**対処支援調整**を実施



2(3) サイバーインシデント対応演習等（取組の概要）

■ サイバーセキュリティ対処調整センターは、東京2020大会に向けて、「一斉演習」を通して体制確立の確認及び運用手順の確立を令和元年度に行ってきたところ、大会延期を受け、更なる信頼関係づくり及び手順習熟を目的に「一斉演習」を継続して実施し、大会の対処態勢を万全なものとしていく。

カテゴリ	2019年度		2020年度		2021年度
	第1回演習	第2回演習	第3回演習	第4回演習	第5回演習（最終）
開催日	1)2019年10月18日 2)2019年10月31日 3)2019年11月28日	1)2020年1月31日 2)2020年2月6日	1)2020年8月5日 2)2020年8月6日 3)2020年9月2日	1)2021年１月20日 2)2021年１月26日 3)2021年２月18日	2021年5～6月頃を想定
目的	基本手順の理解 ・JISP基本操作の習得 ・情報連絡手順の理解	基本手順の理解 ・JISP基本操作の習得 ・情報連絡手順の理解	基本手順の習得 ・JISP改修効果確認 ・情報連絡手順の習得	連携手順の練度アップ ・情報連絡タイミング、速度 ・対処支援調整の連携	大会前最終確認 ・組織委員会窓口との連携
訓練内容 (シナリオ)	・受信した情報の取り扱い方 ・事案の情報連絡手順	・受信した情報の取り扱い方 ・事案の情報連絡手順	・テレワーク中(≒大会中休日)の組織内連携	・攻撃者グループ(APT)による重要サービスに影響のあるサイバー攻撃への対処	・物理被害の発生するサイバー攻撃への対処
意見交換会	–	–	・参加組織グループワーク ・発表(テレワーク(コロナ)) セキュリティベンダー、公的機関	・参加組織グループワーク ・発表(攻撃者グループ(APT)) セキュリティベンダー、公的機関	・参加組織グループワーク ・発表

2(3) サイバーインシデント対応演習等（演習の内容（第４回（2021年１月20,26日開催））

2021年
6月5日
（土）
13:30
～

- あるAPTグループにより東京2020大会が妨害される動きがあることを察知
(JISPにて注意喚起)
- ある重要サービス事業者が、
大会の中断を求める内容の脅迫をメールで受けていることが発覚
- ある重要サービス事業者の大会関係システムで不具合発生
- 不審なメールが複数届いていたことがわかり、大会関係組織へ注意喚起

第1部

2021年
8月1日
（日）
14:40
～

- 自組織において、従業員の端末で不具合を確認、
端末の特定のフォルダに不審なファイルが複数存在していることを確認
- 時間の経過とともに複数の端末が動作しなくなる
- 調査の結果、2018年に確認されたマルウェア「Olympic destroyer」の亜種であることが判明
- 自組織の重要サービスシステムで不具合が発生、
システムの不具合により、大会運営に影響が発生
- 対処調整センターから暫定対処方法を展開
各組織は暫定対処を実施

第2部

●参加組織に期待する行動の概要

【第一部】

・提供された情報に対して、自組織の規定等に基づき迅速・的確に自組織内（保守業者を含む）の情報連携、注意喚起、大会関係システムへの警戒など未然対処を行うこと。その際に、適宜、JISPのそうだんの窓口に報告・相談を行うこと。

【第二部】

・自組織で発生したインシデントの状況を迅速・的確に把握するとともに、自組織内（保守業者を含む）で連携して事案対処を行うこと。第一部で提供された情報との比較、自組織での被害状況の把握に努め、必要に応じて自組織内での情報共有・エスカレーション及び対外説明等を行うこと。その中で、支援要請の要否検討等を速やかに行い、JISPのそうだんの窓口に報告・相談を行うなど最初の報告を行うこと。

・大会関係システムへの被害拡大については、その影響を把握し、JISPのそうだんの窓口に報告・相談するなど経過報告を行うこと。その際に、自組織で独自に把握したマルウェアに関する情報を共有すること。

2(3) サイバーインシデント対応演習等（関係組織間の意見交換による運用の改善(第４回演習後の意見交換会の概要)）

１．目的

- 組織間で大会に向けた課題や演習の状況等を話し合う意見交換会を通じて、運用上の課題解決につなげる。

２．実施日時

- 2021年2月18日(木) 13:00～16:50

３．実施概要

- 有識者による講演
- 第４回一斉演習の振り返り
- 意見交換

  【第1テーマ】大会を狙った組織的かつ高度な攻撃に対して事前に備えておくべき対策

  【第2テーマ】大会期間中のインシデント対応に向けた体制や役割

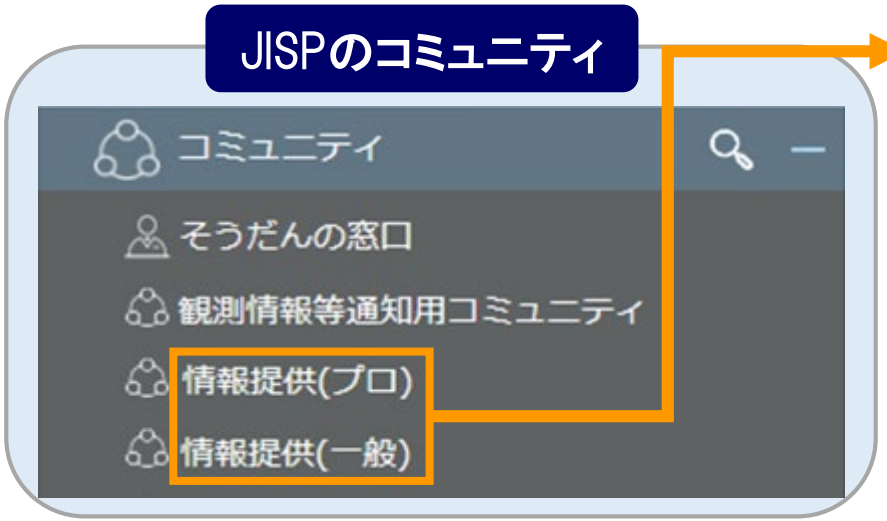
４．開催概要

- 意見交換会は５人程度のグループに分かれて参加者同士で意見交換を行います。
- グループ分けは、希望する意見交換テーマ及び業種等を考慮します。

2(4) 予防・検知に関する情報の発信・共有（取組の概要）

No	情報の種類	概要	
①	脆弱性情報 (攻撃手法・対策含む。)	ソフトウェアや製品に関する脆弱性の概要と、その対策情報	脅威情報の提供
②	攻撃予見情報	・特定組織に対するサイバー攻撃を呼び掛けている情報	
		・サイバー攻撃対象に組織名やURLなどが指定されている等の攻撃予兆に関する情報	
③	不正プログラム情報	・コンピュータウイルスや通信を盗聴するアプリ等の、不正プログラムの種類や挙動に関する情報	
		・不正プログラムを検知・検疫するための情報等	
④	注意喚起情報	・サイバー攻撃への対処に関して適切な措置を講ずることが強く推奨される情報	
⑤	観測／分析関連情報	・サーバの稼働状況に関する観測情報	観測情報の提供
		・通信量に関する観測情報	
		・不正通信の送信状況に関する観測情報	
		・不正通信を行っているブラックリスト情報　等	
⑥	インシデント情報	・インシデントに関して共有すべき情報（組織や個人を特定し得る情報は秘匿）	
⑦	大会関連スケジュール情報	・大会に関連する行事やイベント等の情報	
⑧	緊急事態情報	・自然災害、大規模な事件・事故等の緊急事態に関する情報	

2(4) 予防・検知に関する情報の発信・共有（脅威情報提供活動の状況）　※ 2020年12月末現在



情報提供（プロ/一般）コミュニティ　JISP参加者全員が参照可

- **情報提供（プロ）**
  ⇒ **システム運用担当者や委託先事業者等のセキュリティ対策に携わる方**向け
- **情報提供（一般）**
  ⇒ **システム運用やセキュリティ対策を直接担当していない方**向け

◆ 2020年情報提供数
合計667件、月平均55件の情報を発信

対処対処調整センターからの脅威情報発信件数

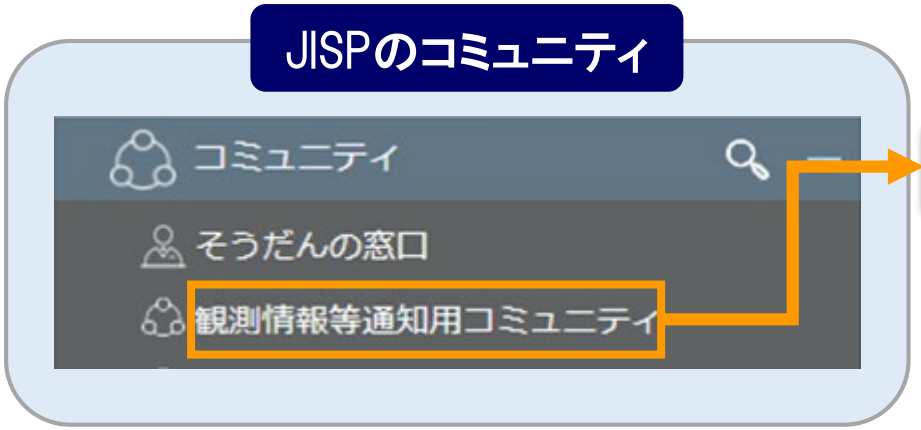
（単位：件）

	2020年											
	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
発信件数	58	63	46	89	52	54	62	36	40	55	60	52
累計（2019年4月～）	188	251	297	386	438	492	554	590	630	685	745	797

トピックタイトルに【重要】【注意】のタグ付け

【重要】：早めに該当する製品等の確認と対策検討を進めて頂きたい項目
【注意】：監視強化や対策の検討準備を進めて頂くことが望ましい項目

2(4) 予防・検知に関する情報の発信・共有（観測情報提供活動の状況）　※ 2020年12月末現在



観測情報等通知用コミュニティ　対象組織のみが参照可

申請いただいたURL、IPアドレスに係るシステム観測情報を各組織に対して個別にお知らせ。

◆ ダークウェブ観測でアカウント情報の漏洩等の検知が増加

対処対処調整センターからの観測情報通知件数　（単位：件）

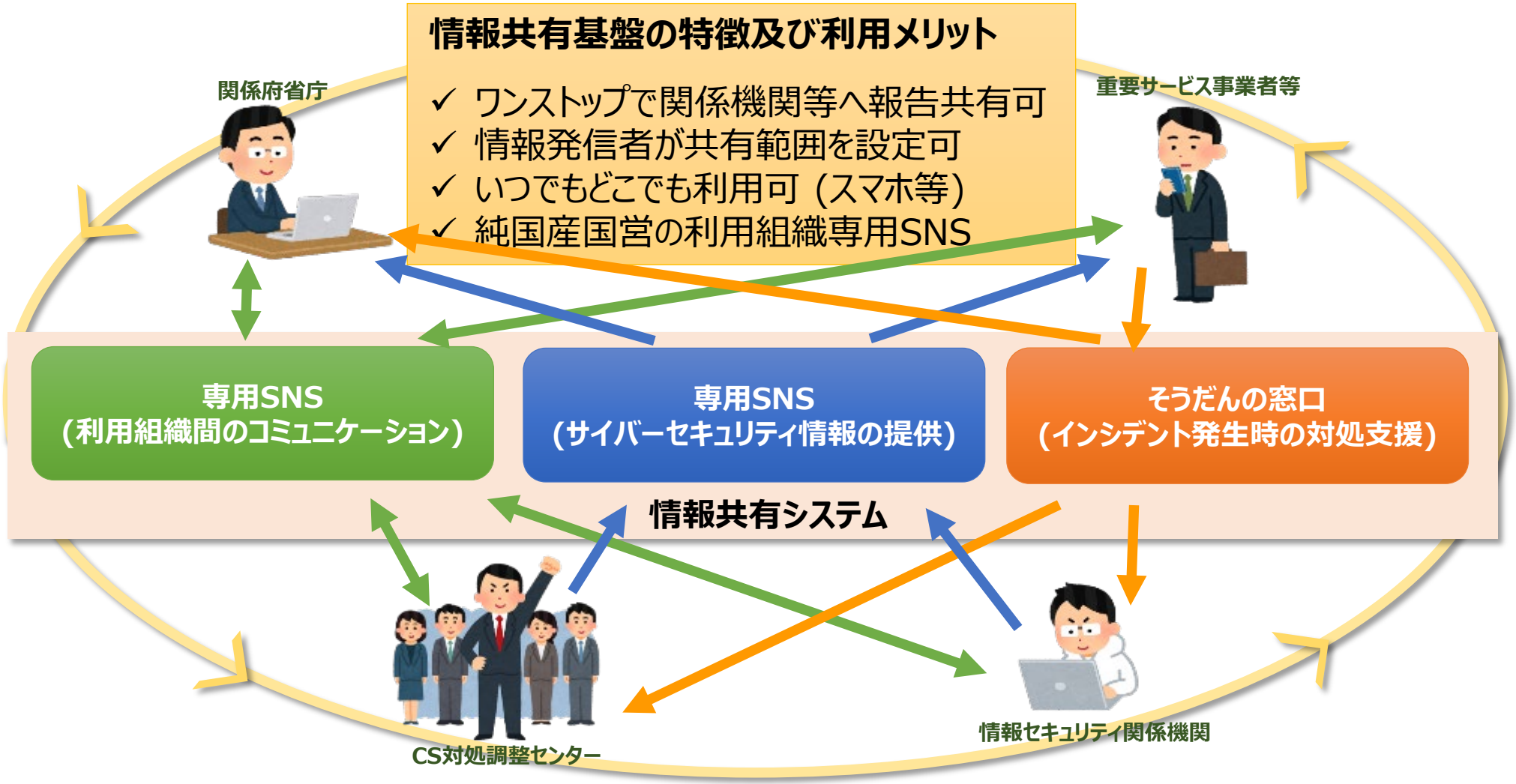
	2020年											
	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
通知件数	0	6	6	2	1	4	0	0	5	5	46	6
累計 (2019年4月～)	13	19	25	27	28	32	32	32	37	42	88	94

通知した観測情報の例

・不正と思われる通信の送信情報
・一般公開されている観測対象Webサイトの脆弱性情報
・DDoS攻撃通信の送信情報
・ダークウェブ観測情報

2(5) 情報共有プラットフォーム（JISP）の提供（情報共有システム（JISP）の概要）

- 2019年4月より、CS対処調整センターは利用組織(※)に情報共有システムを介してサービスを提供する。
- 情報共有システムを活用して、連絡体制確立のための演習・訓練を開催予定。



※大会組織委員会、会場管理者、東京都、会場のある地方公共団体、重要サービス事業者等、スポーツ関連団体、情報セキュリティ関係機関、政府機関、警察等。

2(5) 情報共有プラットフォーム（JISP）の提供（提供するサービス）

➢ 情報共有システム（JISP）では、下記のサービスを利用可能

情報共有システム（JISP）

PC or スマホ

SNSシステム

サイバーセキュリティ情報の提供

情報セキュリティの専門家から、サイバーセキュリティ情報を受け取り対策に活用

そうだんの窓口

自組織においてインシデント※が発生した際に報告・相談・支援要請を行う窓口

訓練

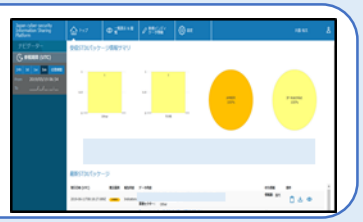
演習システム

SNSシステムを模したシステムを使用し、連絡・連携能力の向上のため、有事の際に円滑な連絡が行えるよう訓練するシステム

PC のみ

インディケータ情報システム

技術者向けサイバー脅威情報が提供されます。（サイバーセキュリティに関する専門知識が必要です。）



※予兆・ヒヤリハット・疑い含む。

2(5) 情報共有プラットフォーム（JISP）の提供（情報共有システム（JISP）の実際の画面）

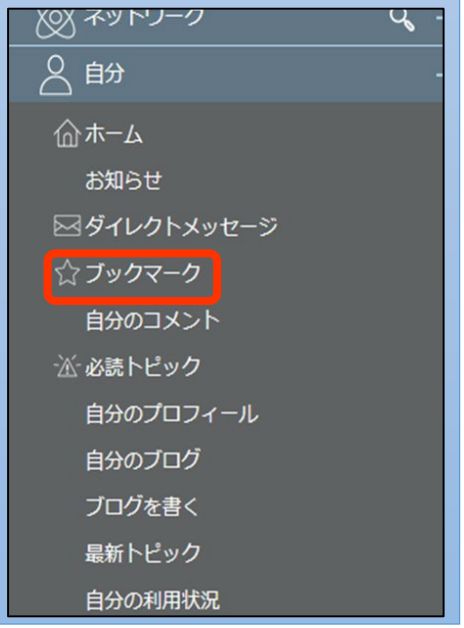
➢ 記事一覧より見たい情報をクリックすると詳細を閲覧可能

クリック

いいね！ボタン
（閲覧したら押してください。）

記事にファイルを添付・閲覧可能

ブックマークボタン
（後から参照したい記事に対して押してください。）



コメント
（追加情報の提供や質問等に利用してください。）

- 組織、個人の単位で閲覧できる人(共有範囲)を設定
  - コミュニティメンバー：コミュニティ参加者全員が閲覧可
  - 手動選択：組織、個人単位で指定した範囲でのみ閲覧可
- 投稿した情報を受け取った人が、展開できる範囲を設定(TLP)
  - RED　：他者へ展開不可
  - AMBER：業務の遂行にあたって知る必要がある者まで可
  - GREEN：関係する組織の範囲まで可
  - WHITE：自由に展開可

3　有識者会議における検討事項例

3　有識者会議における検討事項例（背景（サイバーセキュリティ戦略における記載内容））

サイバーセキュリティ戦略（平成30年７月27日閣議決定）（抄）

4.2　国民が安全で安心して暮らせる社会の実現

4.2.5　2020年東京大会とその後を見据えた取組

オリンピック・パラリンピック競技大会は、世界中から多数のアスリート、要人、観客等が集まり、国際的にも最高度の注目を集めて開催される行事であることから、サイバー攻撃のターゲットとなるおそれがある。

過去の大会を振り返ると、ロンドン大会では、大会の運営には影響はなかったものの、膨大な数のサイバー攻撃があったとされるほか、リオデジャネイロ大会においても平昌大会においても、相当数のサイバー攻撃が行われ被害を受けたとの報道がある。2020年東京大会においても、過去の大会以上のサイバー攻撃が予想され、その特性上各種サービス分野にまたがるような攻撃も想定される。このため、以下のとおり、2020年東京大会のサイバーセキュリティの確保及びその後を見据えた施策を推進する。

また、**2020年東京大会後も各種施策は適用範囲を拡大して引き続き推進し、整備した仕組み、その運用経験及びノウハウは、レガシーとして、以降の我が国の持続的なサイバーセキュリティの強化のために活用していく。**

（中略）

(2)　未来につながる成果の継承

2020年東京大会の態勢整備のための各種施策を引き続き推進し、整備した仕組み、その運用経験及びノウハウは、レガシーとして、2020年東京大会以降の我が国の持続的なサイバーセキュリティの強化のために活用していく。また、構築した「サイバーセキュリティ対処調整センター」を、**サイバー攻撃等に対してオールジャパンで力を合わせて対処するための調整役・調整窓口（ナショナルCSIRT）として活用**し、サイバーセキュリティの基本的な在り方でも掲げた**「リスクマネジメント」の手法については、広く全国の事業者等に適用できるよう整備・普及を促進していく。**

3　有識者会議における検討事項例（サイバーセキュリティをめぐる情勢と課題認識）

国家レベルの攻撃者によるサイバー攻撃の高度化・活発化、サイバー攻撃のビジネス化等により、サイバーセキュリティに係る脅威が急激に高まる中、東京大会に向けて推進した取組の成果等を踏まえつつ、関係組織がより一層連携を強固にし、実効的なサイバー攻撃対策を講じてまいりたい。

昨今の情勢を踏まえた主な課題等

○　サイバー攻撃等によって生じる影響の深刻度が増大する領域・分野が顕在化

ICT、IOT活用範囲の拡大と国民生活への影響

○　ICT利活用が急速に拡大する一方、各事業者等（ICTに不慣れな組織）におけるサイバーセキュリティ対策不足

サイバー攻撃の広範囲化
DX、働き方改革、テレワーク等

○　世界から注目を集める国際イベント等を標的としたサイバー攻撃のリスクの増大

大阪万博等

○　ITサプライチェーン上で発生する不正アクセス、内部不正、人的ミス等のインシデントの顕在化

委託先・請負先において生じる問題等

3　有識者会議における検討事項例（検討事項例の観点等）

大規模国際イベントにおけるサイバーセキュリティの確保に向けた取組を推進する中で整備された仕組み、その運用経験から得られた知見、ノウハウを今後のサイバーセキュリティ対策の強化に活用するための方策、課題等について整理する必要がある

検討事項例

○　サイバーセキュリティのリスクの低減と最新のリスクへの対応強化

これまでに推進してきた「リスクマネジメント」の取組について今後の活用方策等を検討する

【観点】

- 特定のイベント等への対策にとどまらない形で、取組から得られた知見等を広範囲の事業者等におけるリスクアセスメントに活用する場合、**どのような対象に、どのような観点から取り組んでいくべきか**
- スポーツ関連団体を対象にサイバーセキュリティ対策に係る支援、連携強化に取り組んできたが、**特定分野におけるコミュニティづくり、支援等に活かすことができるのではないか**　等

○ セキュリティインシデントに対する迅速・的確な対応、二次被害防止に向けた対処態勢の構築

これまでに推進してきた「対処体制の構築」の取組について今後の活用方策等を検討する

【観点】

- 特定のイベント等への対策にとどまらない形で、取組から得られた知見等をサイバーセキュリティインシデントへの対応に活用する場合、**どのような対象に、どのような観点から取り組んでいくべきか**
- セキュリティインシデント発生時に備えた演習・訓練に取り組んできたが、昨今のサイバー攻撃の被害状況等を踏まえ、**どのような能力の強化が求められているか**　等

○ 2025年日本国際博覧会を始めとした今後の大規模国際イベントに向けたサイバーセキュリティ対策の推進

今後の大規模国際イベントに向けたサイバーセキュリティ対策について検討する

【観点】

- **今後の大規模国際イベントにおいても**、安全な開催・運営に向けて、その**サイバーセキュリティの確保に国として取り組むべきでないか**

○ その他

これまでに推進してきた取組や昨今のサイバー空間をめぐる情勢を踏まえ、国として取り組むべき課題について検討する