内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

資料１

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５回会合

東京大会における活動報告

2021年10月

内閣官房　内閣サイバーセキュリティセンター

はじめに

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、大会の運営を支える機能を提供する関係機関等 における相互の信頼関係を築き、サイバーセキュリティに係る脅威・インシデントに対し関係機関等が自律的に未然対処及び事案対処ができるように必要となる体制の構築・運用を行う中核的組織として、2019年4月に、サイバーセキュリティ対処調整センターを構築するとともに、その運営を支える情報共有プラットフォームであるJISP(Japan cybersecurity Information Sharing Platform)の運用を開始しました。

計画の変更を余儀なくされ、新型コロナウイルスの影響による働き方の変化等新たな課題・困難に直面しましたが、「前を見てできることはすべてやる」ポリシーのもとで、関係組織と連携協力しながら準備を進め、東京オリンピック・パラリンピック競技大会を無事に終了することができました。

当資料は、東京大会で得られた経験と学びを、レガシーとして継承し、デジタル社会における安全・安心の確保に役立ていくために整理したものです。

＜主な活動＞
・大会関係組織間の信頼関係の構築深耕（情報共有体制の構築と運営）
・各組織の自律的なサイバーセキュリティ対策を支援するための公助（参加組織にとって価値のあるサービスの提供）
・安心して情報共有できるプラットフォームの提供（双方向の情報共有）

＜主な経験と学び＞
・組織間の信頼関係構築と価値のある公助の提供による体制参加組織のサイバーセキュリティに対する行動の変化
・情報セキュリティ関係機関がひとつの目的のために連携した経験
・各参加組織の行動を促すための活用しやすい情報提供のための工夫

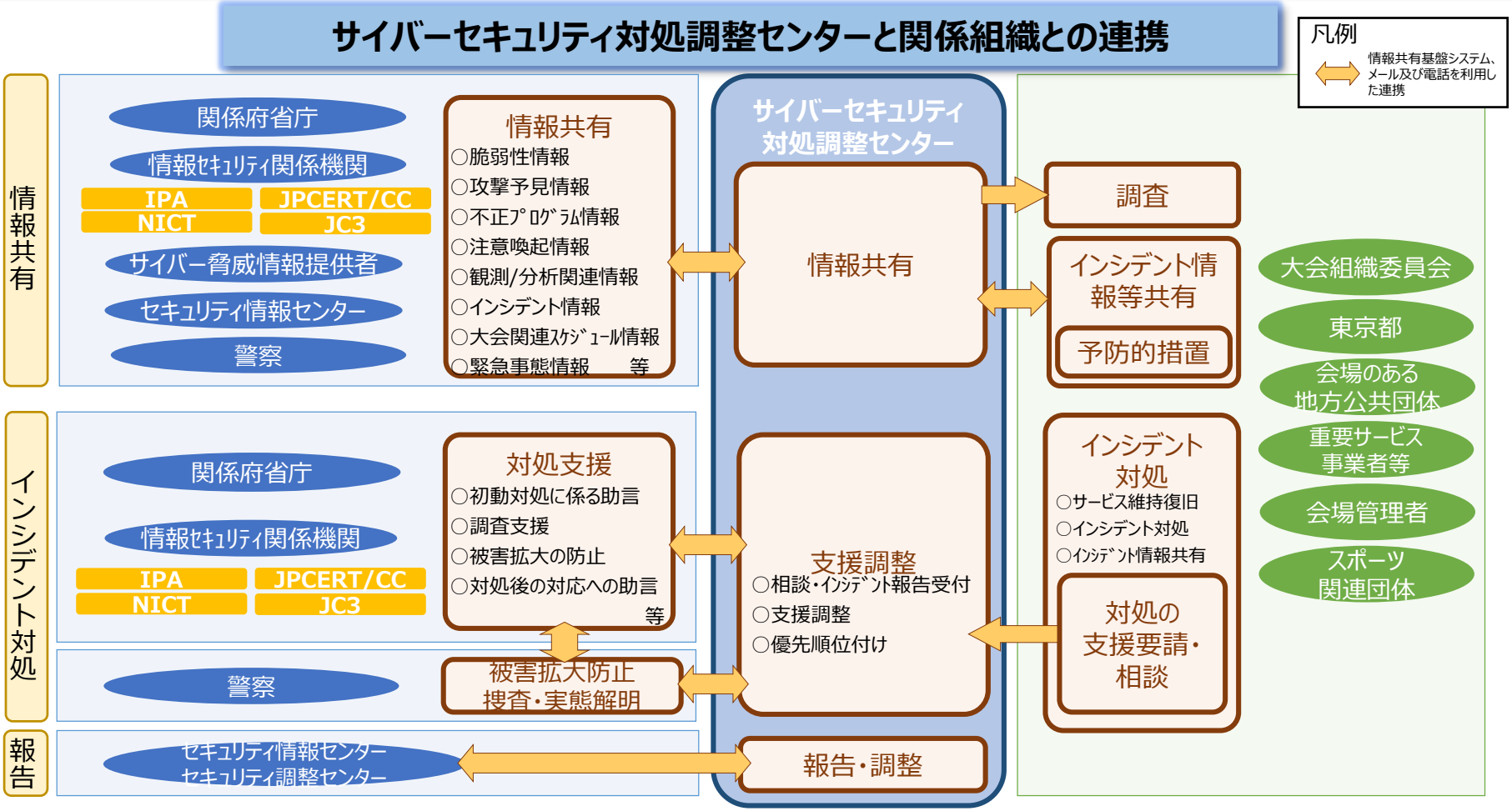
具体的な内容については、資料内をご覧ください。

目次

1.情報共有態勢

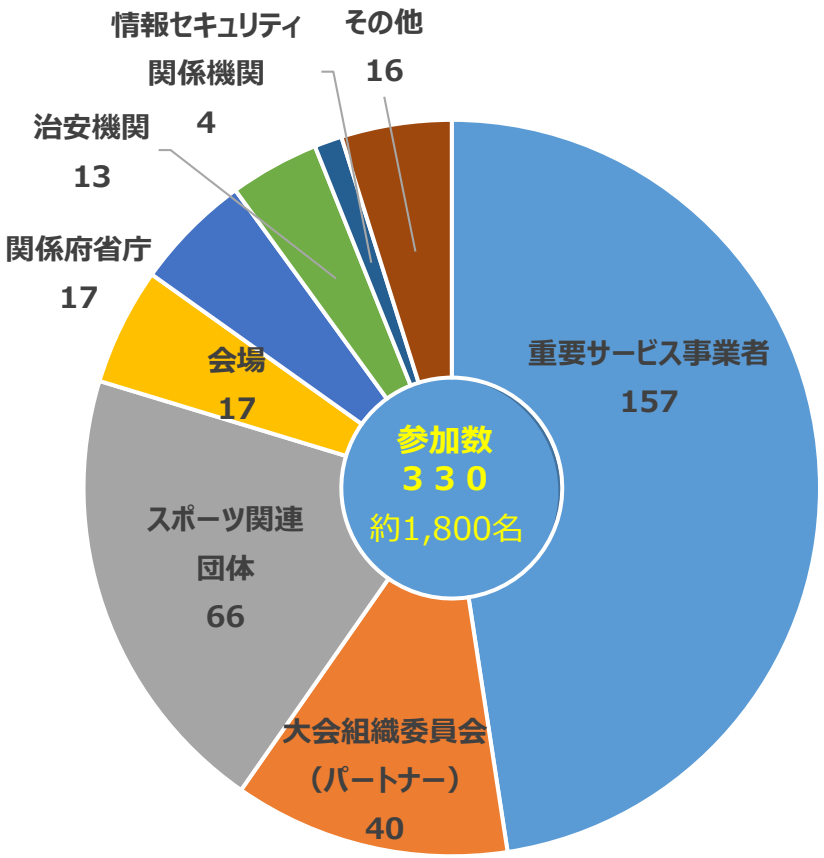
【対処調整センターと関係組織との連携】
2019年４月１日、内閣官房にサイバーセキュリティ対処調整センターを設置した。
対処調整センターは、政府機関との緊密な連携のもと、大会のサイバーセキュリティに係る**脅威・インシデント情報を収集**し、これら情報をサイバーセキュリティ対処体制に**参加した組織に提供**するとともに、関係機関等のインシデント対処に対する**支援調整**を実施した。

サイバーセキュリティ対処調整センターと関係組織との連携



1.情報共有態勢

【情報共有プラットフォーム（JISP)の登録状況】
体制への参加の呼び掛けを継続的に行った結果、大会開催直前までに、330組織、約1,800名の登録があった。



- ◆ 大会組織委員会（パートナーを含む。）
- ◆ 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
- ◆ 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、オリパラ事務局を含む。）

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
- ◆ その他

情報提供・共有の対象

2.インシデントレスポンス（事前準備・実施体制）

【事前準備】
- （演習/意見交換会）情報連携運用手順の理解・習熟を実施
- （机上シミュレーション）インシデント発生時の対処態勢を確認し、対処に関わる関係組織の抽出及び役割分担を整理。

【インシデントレスポンス実施体制】
- センターにおいては、全体統括、インシデントコントローラー、インシデントレスポンス（IR）担当、大会組織委員会リエゾン、当直等の役割に職員を割り当て、大会期間中は24h体制でインシデント態勢を構築。

【対処調整センターにおけるインシデントレスポンスの取組】
- 体制参加組織からのインシデント報告（支援要請）を受け、対処支援を実施。
- インシデント事象、支援要請の内容に応じて、情報セキュリティ関係機関に支援を依頼。
- インシデントによる大会影響の有無や範囲を大会組織委員会と連携して確認。
- 大会の運営等に影響のあるインシデントの発生及び対処状況をセキュリティ調整センターへ報告。

事前準備

演習・意見交換会

・のべ609組織が演習に参加（以下、目的）

第1回	JISP利用基本手順の理解	2019/10
第2回		2020/01
第3回	情報連携の基本手順の習得	2020/08
第4回	情報連携の練度向上	2021/01
第5回	大会前最終確認（FA連携）	2021/06

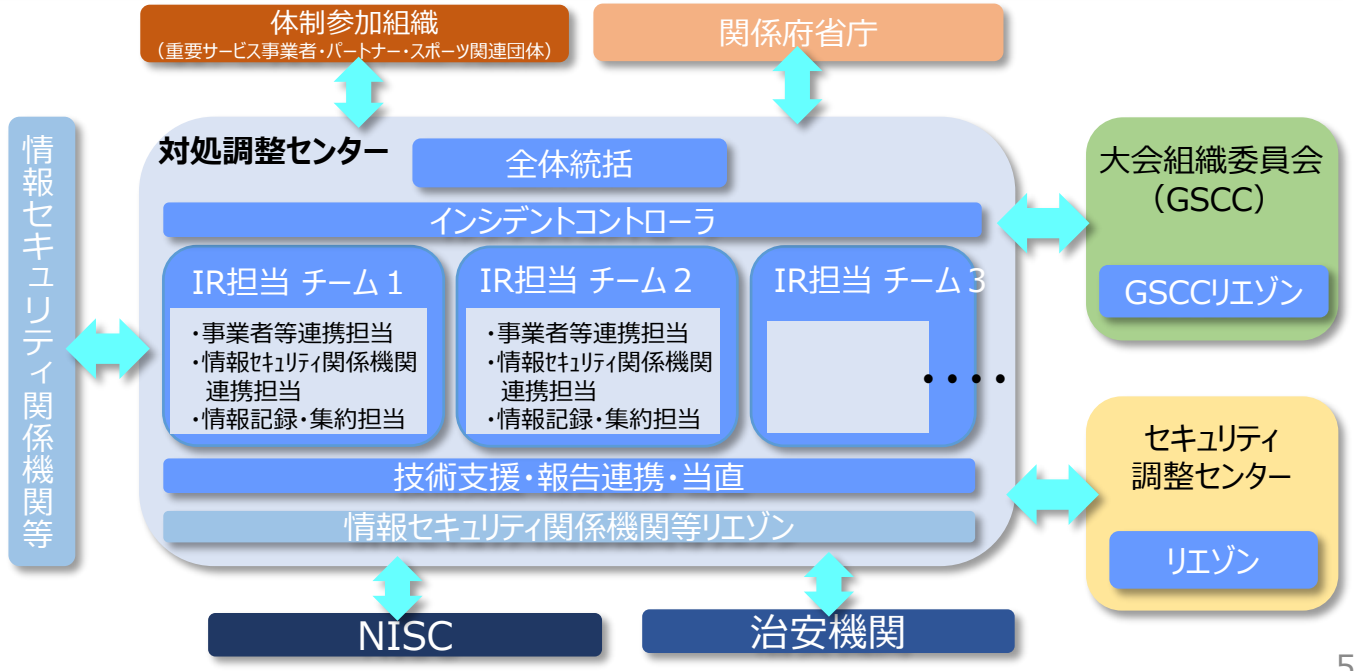
・のべ108組織が意見交換会に参加
（以下、意見交換テーマ）

第1回	大会に向けた様々な課題 他	2020/09
第2回	大会を狙った攻撃への対策 他	2021/02
第3回	大会直前に改めて確認すべきこと	2021/07

机上シミュレーション

・以下を対象に机上シミュレーションを実施
- 大会組織委員会システム（全165システム）
- 重要サービス事業者システム（全24分野）
- 物理-サイバー連携事案

インシデントレスポンス実施体制



2.インシデントレスポンス（活動概況）

大会期間中において、大会の運営に影響を及ぼすインシデントの発生はなかった。
【活動概況】
- ◆ 体制参加組織における大会の運営に影響する、または、その可能性のある事象について前広に情報を収集。その中から大会影響あり又は対外対応ありと判断された事象をセキュリティ調整センターへ報告。
- ◆ 関係機関（体制検討会参加組織、体制参加各事業者等）に大会に関する情報や対処調整センターにおける活動状況の情報発信を実施。

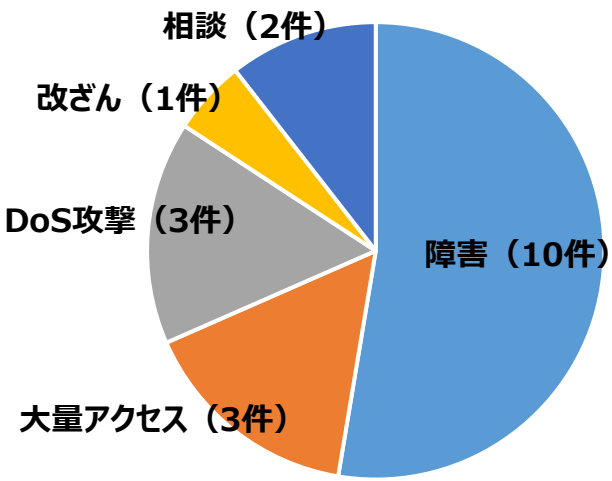
【対応件数】
体制参加組織から提供された情報は、全19件。うち、7件をセキュリティ調整センターへ報告。

【主な活動】

◆体制参加組織から提供された情報
- ➢ 情報提供は全19件であり、うち17件はJISPにて、2件はNISC内連携にて受領した。
- ➢ **全19件中、17件はインシデントの報告、2件はセキュリティ対策に関する相談。**
- ➢ インシデント報告17件のうち最も多かったのはシステム等の障害で、**クラウドサービスの障害7件**及び**システムの障害3件**の**計10件**。
- ➢ **公式オンラインショップのアクセス過多による閲覧障害**が**開会式後数日間と閉会式**に発生。
- ➢ サイバー攻撃報告は、**DoS攻撃3件**、**Webサイト改ざん1件**の**4件**。

◆セキュリティ調整センター報告（AM/PM）
- ➢ 体制参加組織から報告を受けた事象のうち、**大会影響のある事象（大会に関係するサイトにおける事象を含む）、または公に認知されうる事象（報道されてる事象を含む事象を含む）を報告。**大会影響のある事象の報告はなかった。
- ➢ 報告対象となった事象は、**サイト閲覧障害4件**、**システム等の障害３件**の**計7件**。

◆関係機関への情報共有
- ➢ 体制検討会窓口宛てにセキュリティ調整センター報告の概要を情報共有（AM/PM）
- ➢ 体制参加各事業者向けに大会に関する情報や対処調整センターの活動状況を情報発信（デイリー）



提供された報告・相談のインシデント分類
（7月21日～9月5日）

3.観測情報・脅威情報の提供

【概況活動】
- ◆ 情報セキュリティ関係機関等の協力のもと、東京2020大会関連システム等の観測を行い、通常時と異なる観測結果や攻撃予見情報を検出した場合は、対処調整センターより該当する組織へ個別に情報提供。
- ◆ フィッシングサイトや、攻撃者グループによる攻撃キャンペーン情報等の検知のためダークウェブ調査を実施。
- ◆ 対処調整センターが収集した大会のサイバーセキュリティに係る脅威情報を体制参加組織に対して提供。
- ◆ 大会へ悪影響を及ぼす可能性を念頭に主な攻撃者グループを選定調査し、攻撃手法の分析と注意喚起を実施。

【件数】
該当期間において体制参加組織に対して提供された観測情報は75件、脅威情報は32件。

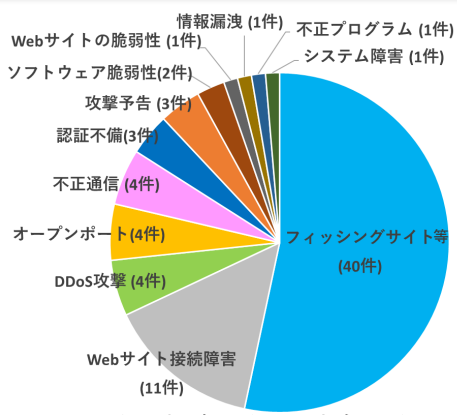
【主な活動】

◆対処調整センターから提供した観測情報

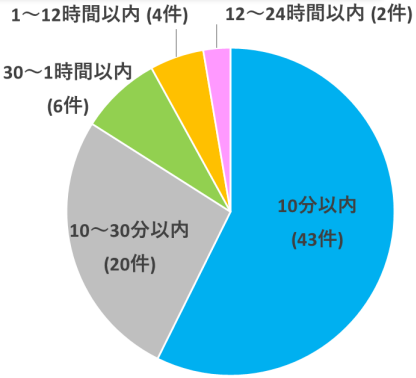
- ➢ 重要サービス事業者等に影響を及ぼす又はその恐れのある事象75件について、対象組織に個別に情報提供。
  - - **開会式、閉会式及び競技の偽ライブ配信サイト**（フィッシングサイト等）をダークウェブ調査で多数観測し組織委員会に通知。
  - - 競技初日(7/21)及び翌日に**3組織をターゲットにした攻撃予告とDDoS攻撃**を観測。その後、**開会式、閉会式当日等にもDDoS攻撃**を観測。いずれも大会運営に影響はなかった。
  - - 上記の他、**認証不備やRDPポート公開**、**Microsoft Exchangeサーバの脆弱性が残る機器の情報公開**等が観測されたため、関係組織へ通知し対処を依頼した。

◆対処調整センターから提供した脅威情報

- ➢ 脅威情報の提供は全32件。
- ➢ **大会関連の被害報告を装う不正プログラム**、**東京2020大会を騙るプログラムの存在を確認**及び**DDoS 攻撃キャンペーン**等に関し、体制参加組織全体へ注意喚起。



観測通知を行った事象の分類
（7月21日～9月5日）



観測情報発信後
参照されるまでの所要時間
（7月21日～9月5日）

参照数の多かった脅威情報（7月21日～9月5日）

	提供した脅威情報 ※上位3件は発信内容の概要を記載	提供日
1	大会関連の被害報告を装う不正プログラムを確認	7/21
2	DDoS 攻撃キャンペーン（#OpBoycottOlympics）	7/23
3	東京2020大会を騙るプログラムの存在を確認	7/30
4	iOS、iPadOS(Apple社)におけるゼロデイ脆弱性	7/24
5	Windows OSに特権昇格が可能となるゼロデイ脆弱性	7/21

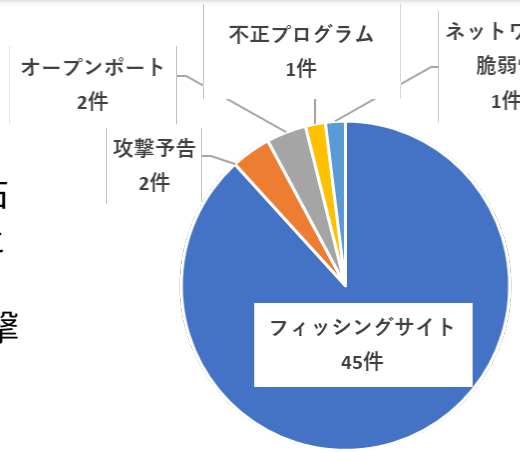
3.観測情報・脅威情報の提供(大会中のダークウェブ情報等の調査活動)

【概況活動】
- ◆ 大会関係組織に関連するドメイン・キーワードを対象に、大会関係組織を狙ったサイバー攻撃、ネットワーク脆弱性、漏洩情報、不正サイト情報等について調査を行い、大会を安全かつ継続的に開催しきるために必要となる対応を実施。
- ◆ 「大会開催に反対する活動」や「大会関連の攻撃による被害報告を装った不正プログラム」、「大会観戦者を狙ったフィッシングサイト」等の緊急性の高い脅威情報が確認されたため、関係組織へ通知。

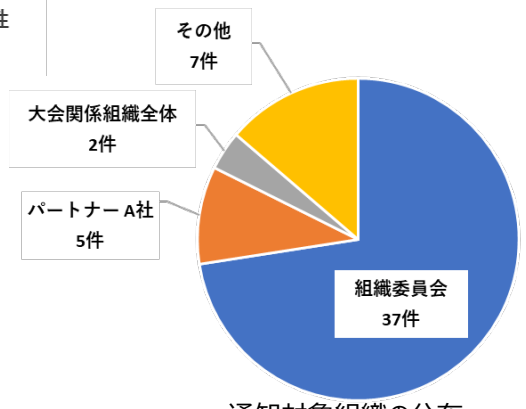
【件数】
該当期間において提供された脅威情報は90件。不審ドメインは “5,542件”あり、その内フィッシングサイトは “45件”確認された。

【主な活動】

◆対処調整センターから提供した情報
- ➢ 当該期間における情報提供は “全90件”
  - 「大会の偽ライブ配信サイト」が “36件” と多くを占めており、オンライン観戦を行う大会観戦者を狙った攻撃が多く確認された。
  - 競技初日および翌日に大会関係組織を狙った攻撃予告（※右下図参照）が確認されると共に、DDoS攻撃実行を示唆する情報が公開された。



脅威情報の分類
（7月21日～9月5日）



通知対象組織の分布
（7月21日～9月5日）

◆通知先の組織の傾向
- ➢ 組織委員会が 37件 と最も多かった。偽ライブ配信サイト36件に加え大会公式サイトに類似したドメインが悪用されたフィッシングサイトを含め、全て大会関連の脅威情報であった。
- ➢ 大会関係組織全体に関連する脅威情報として、「サイバー攻撃による被害報告を装ったワイパー型の不正プログラム」が確認された他、「コロナワクチンナビを装った不正サイト」 が確認されたため、2件について関係組織への通知および対応依頼を実施。

サイト接続後に案内される不正なアカウント登録画面

4.情報セキュリティ関係機関等の活動

【活動概況】
- ◆ 支援が必要となるインシデントは生じなかったが、インシデント発生時に被害組織を支援できる体制がとられた。
- ◆ 情報セキュリティ関係機関等の得意分野を活かし、感度を高めた情報収集や観測を実施された。

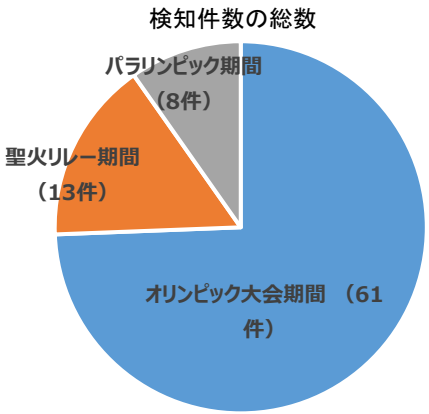
【件数】
- ◆ オリンピック大会期間に61件、パラリンピック聖火リレー期間に13件、パラリンピック大会期間に8件の情報を検知した。
- ◆ 不正通信、DDoS、Webサイト閲覧障害、フィッシングで全体検知数の約80%を占めた。

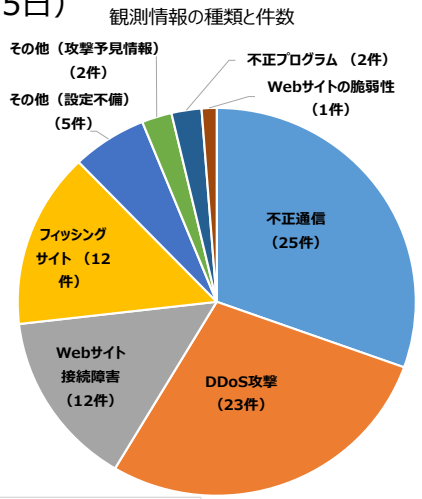
【主な活動】
情報セキュリティ関係機関から協力を得た活動は以下のとおり。

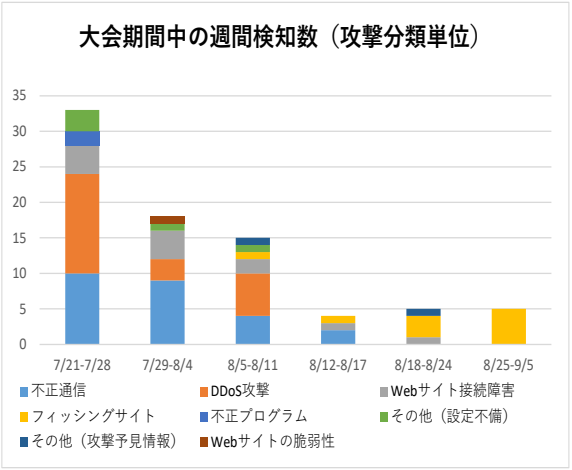
◆システムの観測
- ・Webサイトの脆弱性関連情報の提供
- ・Webサイトの生死監視
- ・DDoS攻撃の監視
- ・不正通信の監視
- ・ダークウェブ上での攻撃予告等の監視
- ・フィッシングサイト等の監視
- ・大会関連で気づいた情報の提供　等

◆インシデントの対応
- ・リモートでの助言
- ・現地対応(状況により)
- ・標的型マルウェアの調査
- ・停止したサイトの原因調査　等

◆大会期間中の観測による検知数（7月21日～9月5日）







5. CTI事業者（サイバー脅威情報提供者）の協力活動

【活動概況】
- ◆ MOU に基づきCTI事業者の事業分野の強みや特性を活かした協力体制がとられた。
- ◆ 大会関連組織へのサイバー攻撃が疑われる通信元について有害/無害を判別し、対処調整センターから大会関連組織へ報告。
- ◆ 対処調整センターから提供したIoC情報を各事業者の製品・サービスに登録し不正通信を遮断。

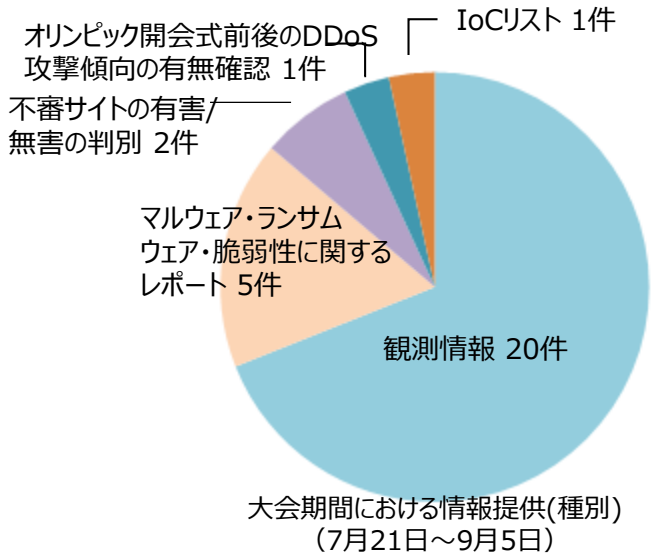
【件数】
大会期間において体制参加組織及び対処調整センターに対して提供された情報提供は29件

【主な活動】

◆大会期間中のCTI事業者からの情報提供は29件
（対処調整センターからの相談に対する応答を含む）

内訳
- 観測情報 20件(※)
- マルウェア・ランサムウェア・脆弱性に関するレポート 5件
- 不審サイトの有害/無害の判別 2件
- オリンピック開会式前後のDDoS攻撃傾向の有無確認1件
- IoCリスト 1件

※Emotet、Trickbot、Mirai、XSS、SQLインジェクション等



大会期間における情報提供(種別)
（7月21日～9月5日）

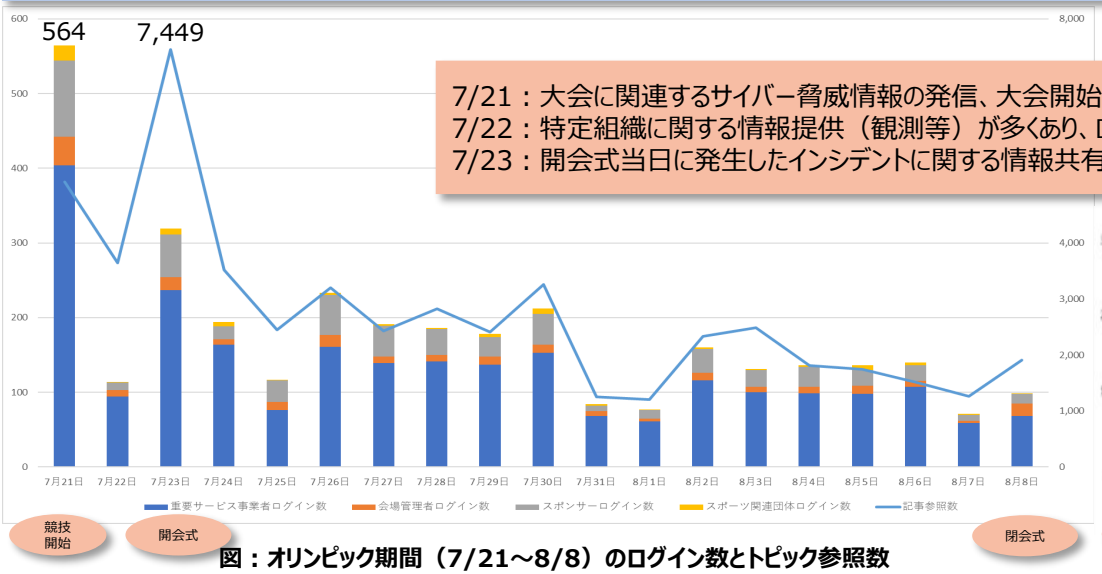
◆CTI事業者の１社からは、観測情報及びマルウェア・ランサムウェアに関するレポートの提供を受け、NISC/事案分析チームへ共有した。

◆対処調整センターからCTI事業者へ提供したIoCをブラックリストとして、CTI事業者の製品・サービスへ登録し、不正な通信を遮断した。

6.情報共有状況(JISP利用状況)

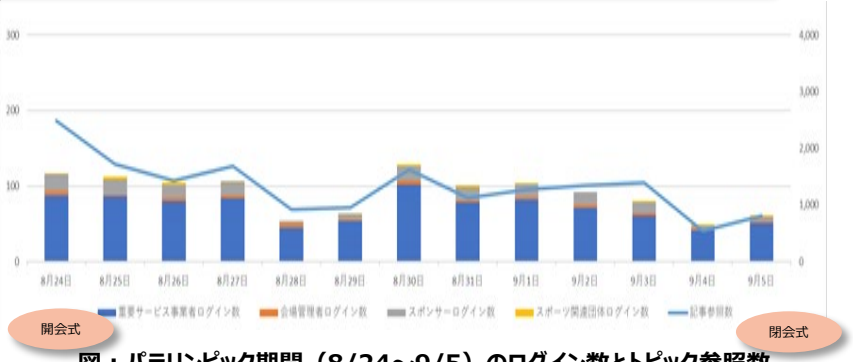
【活動概況】
2019年４月から関係組織がワンストップで情報共有できるプラットフォームとしてJISPを運用してきた。大会中には、大会に関連する情報・大会独自の情報が共有され、平時の1.5倍のログイン、2.5倍のトピック閲覧があった。オリンピック競技開始日(7/21) ～開会式(7/23)において最も活発に利用された。

【件数】（パラリンピック閉会式(9/5)時点）
・330組織、約1,800名がシステムを利用
・累計利用状況 ログイン数 約19.8万、トピック参照数 約55.9万、トピック投稿数 0.8万



7/21：大会に関連するサイバー脅威情報の発信、大会開始に伴う連絡などがあったことからログイン数が最大
7/22：特定組織に関する情報提供（観測等）が多くあり、ログイン数は少ないものの１ユーザーあたりのトピック参照数が最大
7/23：開会式当日に発生したインシデントに関する情報共有が多く、トピック参照数が最大

図：オリンピック期間（7/21～8/8）のログイン数とトピック参照数



図：パラリンピック期間（8/24～9/5）のログイン数とトピック参照数

大会中（7月21日～9月5日）に参照数の多かったトピック（情報提供（プロ））

	提供情報	発信元
1	(プロ)【重要】大会関連の被害報告を装う不正プログラムを確認。開かないように注意を。	対処調整センター
2	7/30更新(プロ)【情報】東京2020大会を騙るプログラムの存在を確認	対処調整センター
3	(プロ)【重要】DDoS 攻撃キャンペーンに関する注意喚起	対処調整センター

7.大会後に向けて

【東京2020大会おける主な活動】

◆インシデントレスポンス体制とそうだんの窓口

- 必要な関係組織がワンストップで情報共有できる体制と安心して情報共有できるシステム(JISP)を構築し、各組織の対処能力の向上を目指すとともに、関係組織と積極的にコミュニケーションをとり信頼関係を構築深耕した。
  - JISPによる情報共有、演習や意見交換等
- インシデント対処やサイバーセキュリティ対策全般について、相談できる仕組みを構築運用した。
  - そうだんの窓口
- 大会の運営に影響するようなインシデントは発生しなかったが、インシデント発生時に情報セキュリティ関係機関と協力連携できる態勢を確立した。

◆観測情報・脅威情報の提供

- 脅威情報の発信において、関係組織に有用な情報を理解し活用しやすい形で関係組織全体に情報提供した。
- 関係組織から申請された観測対象(URL、IPアドレス)の観測を実施し観測結果を個別に情報提供した。
  - 情報セキュリティ関係機関等の協力による観測、ダークウェブ調査、不審ドメイン調査
- CTI事業者から、脅威情報の提供、有害/無害判別、不正通信の遮断等、積極的な協力を得た。

【東京2020大会における主な経験と学び】

- インシデント発生時等に、所管省庁、治安機関及び所属する各種団体に**一元的に報告(情報共有) できる**ことは、**関係組織への情報の的確な流通、各事業者等の負荷軽減の観点でメリットが大きい**。
- 情報共有体制において、**組織間の信頼関係は必須条件**である。そのためには、参加組織のメリットを真剣に考えて活動するとともに、こちらから積極的にコミュニケーションをとっていく必要がある。（成功の最低条件）
- 体制参加組織においても、**自律的に未然対処及び事案対処ができているとは言い切れない組織が少なくなかった**。必要な時に相談できる窓口や扱いやすい脅威情報の提供等は、これらの組織にとって非常に有効に機能する。
- **情報セキュリティ関係機関が一同に会してひとつの目的のために活動連携**できた経験は、特に、将来の**国家的イベントや大規模なインシデント発生時に活かせる貴重な経験**となった。
- 結果、多くの体制参加組織においての**サイバーセキュリティに対する意識と行動の変化を感じることができた**。
- 今回の情報共有体制成功の大きな要因は、**「同じメンバが時間をかけて信頼関係を構築したこと」**、**「オリパラの安全を守るというシンプルな目的があったことで多くの組織が協力を惜しまなかったこと」**の２点と考える。大会後は、我々を含めた参加組織のモチベーションの維持が一番の課題。