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

最終報告

令和３年 12 月７日

目次

1　はじめに

1.1 取組を進めてきた経緯・背景

2020 年東京オリンピック・パラリンピック競技大会（以下「大会」という。）は国際的にも最高度の注目を集めて開催される行事となり、大会の機会を狙ったサイバー攻撃等の発生が懸念されていた。

大会の準備、運営を担う大会組織委員会、競技会場を始めとする大会関係施設、大会の運営に不可欠な重要サービス等に対するサイバー攻撃が行われた場合、円滑な大会運営に支障を来す懸念があるほか、大会を支える重要なサービスが停止、制御不能となる深刻な影響が生じることになれば、アスリートや観客等の安全が脅かされる事態に発展するおそれもあることから、そのサイバーセキュリティ対策は重要な課題となる。

現に、2012 年ロンドン大会や 2016 年リオ大会では大会関係のウェブページ等に対して様々なサイバー攻撃がなされたほか、2018 年平昌大会では開会式運営への妨害を企図したサイバー攻撃が行われたと報道されている。このようにオリンピック・パラリンピック競技大会を標的としたサイバー攻撃は現実の脅威となっており、大会を標的としたサイバー攻撃にも十分な警戒が必要となった。

こうした情勢の中、政府においては、サイバーセキュリティに係る諸施策の目標及び実施方針を示す「サイバーセキュリティ戦略」（平成 30 年 7 月 27 日閣議決定。以下「旧サイバーセキュリティ戦略」という。）において、大会運営に影響を与える可能性のある重要サービス事業者等におけるサイバーセキュリティ上のリスク評価及びそれにより明確となる各種リスクへの対策を促進するとともに、大会関係組織間でサイバーセキュリティに係る脅威情報の共有と事案発生時に大会関係組織が皆で力を合わせて対応するために国が調整役となるための組織であるサイバーセキュリティ対処調整センター（以下「対処調整センター」という。）の構築を推進するとの方針を示した。

また、大会に係るサイバーセキュリティ対策の円滑な準備に資するよう、関係府省庁の所管する事務を調整するため、セキュリティ幹事会（平成 27 年 7 月 24 日 2020 年東京オリンピック・パラリンピック競技大会関係府省庁連絡会議議長決定）等を設置し、セキュリティ対策に係る基本的な考え方、対策の方向性等を示す「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に向けたセキュリティ基本戦略」の決定、改訂等を行ってきた。同戦略においても、サイバーセキュリティ対策の強化を重要課題の一つとして挙げ、サイバーセキュリティ上のリスク評価及びそれにより明確となったリスクへの対策を促進するとともに、サイバーセキュリティに係る脅威・イ

ンシデント情報（以下「脅威情報等」という。）の共有等を担う中核的組織としての対処調整センターを構築し、その運用改善を図るなどして、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の構築・強化を図るとの方針を示した。加えて、同幹事会において、対処調整センターを構築等し、同センターの運用は、内閣サイバーセキュリティセンターが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推進本部事務局と緊密に連携して行うこととされた。

こうした政府の方針等に基づき、内閣サイバーセキュリティセンターでは、大会におけるサイバーセキュリティの確保に万全を期すべく、関係組織との緊密な連携の下、大会の円滑な運営に不可欠なサービスを提供する事業者等（以下「重要サービス事業者等」という。）に対してリスク評価等の支援を行う「リスクマネジメントの促進」に係る取組、大会組織委員会や重要サービス事業者等との間で的確な情報共有、インシデント発生時の対処調整等を行う「対処態勢の整備」に係る取組を推進してきたところである。

1.2 大会後の活用方策に向けた検討

オリンピック憲章では、オリンピック競技大会の有益な遺産（レガシー）について、開催都市のみならず、開催国として引き継ぐことが期待され、1964年東京大会においては、新幹線、首都高速道路、ごみのない美しい町並みなど、現在にも残る数々のレガシーが生み出された。1964年東京大会のレガシーとして今日に残っているものは、大会前からの官民を挙げた不断の準備・努力によって成し遂げられた成果が大会において高く評価され、大会後に継続されて現在も残っているものである。この度の大会においても、大会の開催に向けて推進された様々な取組、整備された施設、開催によって得られた文化的な恩恵等が、大会後も長期にわたって継承・享受されていくことが期待されている。

この点、大会におけるサイバーセキュリティの確保に向けて整備された仕組み、その運用経験及びノウハウは、大会を契機に関係組織間で協力して作り上げられた重要な成果であり、有用な取組等は大会後においても継承されていくことが求められる。この方針については、旧サイバーセキュリティ戦略において、「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」と記述されている。なお、本年９月に公表された「サイバーセキュリティ戦略」（令和３年９月28日閣議決定。以下「新サイバーセキュリティ戦略」という。）においては、「新たな攻撃にも国全体として網羅的な対処が可能と

なるよう、国はナショナルサート(CSIRT/CERT)の枠組み整備の一環として、東京大会に向けて整備した対処態勢とその運用経験及びリスクマネジメントの取組から得られた知見、ノウハウを活かすことで、大阪・関西万博をはじめとする大規模国際イベント時だけではなく、平時における我が国のサイバーセキュリティ全体の底上げを進める。」旨が盛り込まれた。

他方、その活用に当たっては、大会に向けた取組等を単純に継続するだけでは適当ではなく、取組の成果等を正確に評価しつつ、デジタル化の進展に伴い変容するサイバーセキュリティを取り巻く現下の課題を踏まえ、その活用方策についてしっかりと検討する必要がある。

また、近年、Emotet のような強力な感染力を持つマルウェアによるばらまき型攻撃、国家等の関与が疑われる特定の組織を標的とする高度な攻撃、テレワークの普及等の環境変化をタイムリーに捉えた攻撃等が猛威を奮っているところであるが、これらの脅威は大会後も途絶えることなく存在することも念頭に置いておく必要がある。こうした背景にある中、大会向けの各取組を、大会終了をもって一度止めてしまうと、これまで醸成してきた関係組織間における協力・連携体制等が損なわれることになり、取組を再開する際に関係組織との信頼関係を一から構築し直さなければならず、結果的にサイバーセキュリティ上の脅威への対応に遅れを来すおそれがある。そのため、大会に向けた取組の今後の活用方策等に関する検討に際しては、大会の完遂を待たずして進めていく必要がある。

こうした点を踏まえ、内閣サイバーセキュリティセンターでは、大会に向けた取組の成果等を整理するとともに、これらの取組を今後の我が国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、課題等について外部有識者の視点も踏まえて検討、整理するため、「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」を令和３年１月に設置した。

本有識者会議においては、大会までに内閣サイバーセキュリティセンターが推進してきた各取組の内容、その成果を踏まえ、大会後の活用方策、課題等について討議を行ってきたところ、この度、その結果を最終報告として取りまとめることとした。

２　大会に向けて推進した取組等

本有識者会議において討議を行うに当たり、大会までに内閣サイバーセキュリティセンターが推進した取組、その成果を確認した。これらを整理した結果を以下のとおり示す。

リスクマネジメントの促進と対処態勢の整備の主たる対象となる「重要サービス事業者等」の範囲については、世界各国のアスリート、大会の準備及び運営を支えるスタッフ、観客、テレビ等を通じて観戦する者等の行動等を想定・整理した上で、大会の安全・円滑な準備及び運営並びに継続性を支えるサービスを提供する事業分野を選定した。その上で、NISC 及び事業所管省庁が協力して、各サービス提供事業者等と個別に関係を構築し、サイバーセキュリティに関する取組の必要性についての理解を得ることができた。

2.1 対処態勢の整備

内閣サイバーセキュリティセンターでは、平成 31 年４月に内閣官房に設置された対処調整センターを運用し、以下の取組を推進した。

① インシデント等に対する対処調整

【取組の概要】

対処調整センターでは、大会の安全・円滑な準備及び運営並びに継続性を確保するため、大会の運営を支えるサービスを提供する関係機関等[1]との間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各組織が自律的に未然対処及び事案対処ができるよう必要となる体制（以下「対処体制」という。）を構築・運用した。大会までに対処体制に参加した組織（以下「対処体制参加組織」という。）は約 350 組織となっていた。

インシデント対処に当たっては、対処調整センターが被害組織における対処への支援を調整する役割を担い、これにより関係組織が連携してインシデントに対応できるようになった。インシデント対処に係る主な流れは以下のとおりである。

（対処調整の流れ）

１　大会の運営に影響を及ぼし得るインシデント等が発生した場合又は発生するおそれがある場合等に、被害組織は対処調整センターが整備した情報共有プラットフォーム（Japan cyber-security Information Sharing Platform の略。 以下「JISP」という。）を通じて、同センターに対して対処に係る支援要請又は相談を行うことができる。

２　要請等を受けた対処調整センターは、被害組織に対して助言を行うとともに、必要に応じて情報セキュリティ関係機関[2]と連携して対

1　関係府省庁、大会組織委員会（スポンサー含む。）、東京都、競技会場のある地方公共団体（都道県警察を含む。）、重要サービス事業者等、競技会場の管理者、スポーツ関連団体等

2　国立研究開発法人情報通信研究機構、独立行政法人情報処理推進機構、一般社団法人 JPCERT コーディネーショ

処に係る支援の調整を行う。

3　情報セキュリティ関係機関は、対処調整センターとの調整結果を踏まえて、被害組織におけるインシデント対処を迅速かつ積極的に支援する。

4　1から3の流れについては、被害組織が、事業所管省庁、大会組織委員会、治安機関等の関係組織を情報共有先として指定することで、ワンストップでの情報共有が可能となり、関係組織が共通の認識でインシデントに対応することができる。

【取組による成果】

○　インシデント発生時等に被害組織が関係組織に個別に連絡・報告等をしなければならないこれまでの状態から、ワンストップでの情報共有が可能となり、被害組織における情報の報告作業及びその問合せ対応等の合理化を図ることができた。

○　被害組織からの支援要請等に応じて対処調整する枠組みを整備したことで、個別の組織の対応能力に依存していたこれまでの状態から、関係組織が協力してインシデントに対応できるようになり、総合的に対処能力が向上し、被害拡大防止等を推進することができた。

○　支援要請や相談を行うことができる窓口を提供することで、対処体制参加組織における安心感を醸成できた。

○　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。

②　予防・検知に関する情報の発信・共有

【取組の概要】

対処調整センターでは、オープンソースや国内セキュリティベンダー等から得られた脅威情報等を対処体制参加組織に提供した。脅威情報等の提供に当たっては、対処体制参加組織の知識・技能が多様であることにかんがみて、「一般用」、「プロ用」と内容を書き分け、情報の受け手である対処体制参加組織の知識・技能にあった情報を提供できるように配慮した。

また、情報セキュリティ関係機関において行っている、サイバー攻撃の発生、又は予兆に係る情報の観測等の活動の中で把握された対処体制参加組織に関する情報及びダークウェブ上のサイバー攻撃の呼びかけ活動、

ンセンター及び一般社団法人日本サイバー犯罪対策センター

漏洩したアカウント情報の売買、公開等の情報（以下「観測情報」という。）を、JISP を通じて対象組織に個別に提供した。

本取組については、運用開始以降、令和３年９月末までの間に約 2,100 件の脅威情報等を提供した。

【取組による成果】

○　様々な組織等から発信される脅威情報等が、JISP においてワンストップで、かつ情報の受け手の知識・技能に応じて書き分けられた内容で提供されることで、対処体制参加組織が効果的、効率的に情報を入手・活用できるようになり、被害の未然防止及び極小化につながった。

○　情報セキュリティ関係機関等の協力により、各組織では独自に収集することが困難な観測情報を得られるようになり、被害の未然防止及び極小化につながった。

③ インシデント等への対処能力の向上

【取組の概要】

対処調整センターでは、対処体制参加組織におけるインシデントの未然防止及びインシデント対処能力の向上を目的とした JISP を用いたサイバーインシデント対応演習（以下「演習」という。）、対処体制参加組織間の相互の信頼関係づくりを目的とした意見交換会を開催した。

演習においては、攻撃者グループによる APT 攻撃、テレワークや休日中に確認されたサイバー攻撃、システムへの被害により物理面での被害が生じるサイバー攻撃等、現下のサイバーセキュリティ情勢をタイムリーに捉えたシナリオ等を用いて、大会までの間に計５回の演習を積み重ねた（第１回：令和元年 10 月から 11 月、第２回：令和２年１月から２月、第３回：令和２年８月、第４回：令和３年１月、第５回令和３年６月に開催。）。

意見交換会においては、対処体制参加組織におけるサイバーセキュリティ上の課題等をグループで討議する意見交換会を、大会までの間に計３回開催した（第１回：令和２年９月、第２回：令和３年２月、第３回：令和３年７月に開催。）。このような場を提供することで、各組織において東京大会に向けての運用上の課題解決に資する気づきが得られるとともに、各組織間の相互の信頼関係づくりが推進された。

【取組による成果】

○　演習の開催により、インシデント発生時等における参加組織の内部、関係組織間の情報連絡等をシミュレーションするとともに、各組

織においてセキュリティ上の課題解決に資する気づきを得ることができるようになり、対処体制参加組織のインシデント対処能力を高めることができた。

○　意見交換会の開催では、業種を問わない他組織と交流し、自組織のサイバーセキュリティ対策を改善する上で参考となる他組織の情報（体制、課題、好事例等）が共有されるとともに、対処体制参加組織間の相互の信頼関係が構築され、サイバーセキュリティ対策に係る活動を活性化することができた。

④ 情報共有プラットフォームの提供

【取組の概要】

対処調整センターでは、対処体制参加組織間において、脅威情報等を共有するとともに、インシデントの被害組織からの報告・支援要請に対する助言や対処調整を実施した。これらの活動をワンストップで効率的に実施するため、JISP を整備し、平成 31 年４月から運用した。

JISP では上記のほか、対処体制参加組織間で、個別にコミュニティを作成し、当該コミュニティ内における情報共有、演習訓練等にも活用できるようになっており、現に特定の業界内、地域内におけるコミュニティが構築され有効に活用された。

また、機械連携（STIX/TAXII）の仕組みを活用して、インディケータ[3]情報の共有も行った。

【取組による成果】

○　JISP は、利便性、信頼性が高いプラットフォームとして、対処調整センター等との連絡に用いられるほか、個別のコミュニティ内における連絡ツールとしても活用され、対処体制参加組織間の連携強化に大きく貢献した。

○　機械連携の仕組みの活用により、当該仕組みを活用する機関において効果的かつ効率的にサイバーセキュリティ対策を強化できることが実証された。

2.2　リスクマネジメントの促進

内閣サイバーセキュリティセンターでは、大会を標的としたサイバー攻撃に係るリスクの低減と最新のリスクへの対応を進めるため、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に、以下の取組を推進

[3] サイバー攻撃の痕跡を示すもので、攻撃者が使用した不正プログラムのファイル名やハッシュ値、通信先の IP アドレス等の情報のことをいう

した。

① リスクアセスメント

【取組の概要】

内閣サイバーセキュリティセンターでは、サイバーセキュリティ上のリスクの低減と最新のリスクへの対応を目的としてリスクアセスメントの手順書を作成し、約 300 者の重要サービス事業者等を対象にリスクアセスメントの取組を促進した。

リスクアセスメントについては、各重要サービス事業者等におけるサービスが安全かつ継続的に提供されるよう、維持・継続することが必要なサービスの特定、サービス提供の維持等に必要な業務や経営資源に係る要件の分析・評価、サービスの維持等に影響することが想定されるインシデントの結果からのリスク源の分析を行う、いわゆる機能保証の観点に立った取組を推進した。

また、各事業者等におけるリスクアセスメントの取組を単に促すだけでなく、内閣サイバーセキュリティセンターが各事業者等から提出された実施結果を分析し、リスク等の洗い出しが不十分と思われる点、サイバーセキュリティ対策の運用状況の懸念点等について個別にフィードバックを行った。

リスクアセスメントの取組は、サイバーセキュリティ対策の改善を目的に、その対策の実施状況を確認するため、平成 28 年 10 月から、東京都内の事業者等を対象とした取組を始め、段階的にその対象範囲を拡大し、大会までの間に計６回の取組を実施した。

本取組に関する取組状況は以下のとおりである。

（取組状況）

第１回：平成 28 年 10 月から 12 月、東京都 23 区内の重要サービス事業者等を対象に約 70 組織でリスクアセスメントを実施

第２回：平成 29 年８月から 10 月、東京都、埼玉県、千葉県及び神奈川県内の重要サービス事業者等を対象に約 120 組織でリスクアセスメントを実施

第３回：平成 30 年６月から８月、全競技会場の管理者及び競技会場が所在する都道県の重要サービス事業者等を対象に約 190 組織でリスクアセスメントを実施し、NISC から個別に実施結果に関するフィードバックを実施

第４回：平成 31 年２月から４月、全競技会場の管理者及び競技会場が所在する都道県の重要サービス事業者等を対象に約 270 組織でリスクアセスメントを実施し、NISC から個別に実施結果に関す

るフィードバックを実施

第５回：令和元年９月から 12 月、全競技会場の管理者及び競技会場が所在する都道県の重要サービス事業者等を対象に約 280 組織でリスクアセスメントを実施し、NISC から個別に実施結果に関するフィードバックを実施

第６回：令和２年 11 月から令和３年１月、全競技会場の管理者及び競技会場が所在する都道県の重要サービス事業者等を対象に約 270 組織でリスクアセスメントを実施し、NISC から個別に実施結果に関するフィードバックを実施

【取組による成果】

○　重要インフラ事業者等のみならず、大会を支える周辺サービスを提供する事業者等を対象に、統一的な手法でのリスクアセスメントを促進したことで、サイバー攻撃等による大会の準備・運営への影響の未然防止や軽減等を推進することができた。

○　各重要サービス事業者等によるリスクアセスメント結果を分析し、懸念事項等について個別にフィードバックを行うことで、取組の実効性を確保することができた。

② 横断的リスク評価

【取組の概要】

重要サービス事業者等におけるリスクアセスメントの促進に加えて、特に大会への影響度が大きい重要サービス事業者等、既存の施設を利用する競技会場等を対象に、サイバーセキュリティ対策の実施状況を内閣サイバーセキュリティセンターが検証した。

重要サービス事業者等に対する検証では、大会に関わるリスクが顕在化するリスクシナリオを策定、活用し、その検証を行った。具体的には、検証対象となる個々の事業者等の業務、システム構成等を把握した上で、攻撃者が当該事業者等のどのような経営資源に対してどのような手法で攻撃を実行するか、又は事故・災害がどのような経営資源に対してどのように影響するかについて時系列で整理し、最終的にリスクが顕在化することを想定したシナリオを複数策定し、シナリオごとに検証項目等をブレークダウンし、当該検証項目等に基づいたヒアリング、実地・書面での確認を実施した。また、競技会場等に対する検証では、チェックリストを策定・活用し、確認を行った。具体的には、各競技会場等の業務、情報システム等を把握した上で、その機能を継続的かつ適切に提供されることを確認するために必要なチェックリストを策定し、当該チェックリストに

基づいて書面による検証、現場視察等を行った。

横断的リスク評価の結果については、改善対策案を含め対象事業者等にフィードバックし、大会までの間にその改善状況等を確認するフォローアップを継続して行った。

更に、競技会場におけるリスクを明確化することを目的として、大会の継続を支える特に重要な競技会場の制御システムに対しては、攻撃者が実際に用いる手法での攻撃に耐えられるかという観点から攻撃シナリオを策定した上で、技術的対策の実施状況を検証し、その対策の改善に向けて必要な助言等を行った。

これらの取組の実施状況は以下のとおりである。

（取組状況）

リスクシナリオに基づく検証

平成 30 年度：電力、通信、水道、鉄道、放送分野から５者を対象に訪問検証、全重要サービス分野から 19 者を対象に書面検証を実施

令和元年度：鉄道、放送、大会運営分野から３者を対象に訪問検証を実施

令和元年度–令和３年度：検証結果を踏まえたフォローアップを実施

チェックリストに基づく検証

令和元年度：仮設や情報資産を持たない競技会場を除く 30 会場を対象に、書面及び訪問による検証を実施

令和２年度–令和３年度：検証結果を踏まえたフォローアップを実施

技術的対策の検証

令和元年度–令和３年度：７つの競技会場を対象に検証

【取組による成果】

○　大会の成功に不可欠な機能が継続して提供されることを第三者の立場で客観的に確認するとともに、不備があった場合には、フィードバックを行うことで、当該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ことができた。

③ スポーツ関連団体に対する勉強会

【取組の概要】

2016 年リオ大会においては、スポーツ関連団体がサイバー攻撃によって重大な被害を受けたことを踏まえ、内閣サイバーセキュリティセンタ

ー及びスポーツ庁が協力して、平成 29 年７月から、大会の競技種目となるスポーツ関連団体等を対象に、セキュリティに係る基本的な知識やインシデント発生時等の対処手法を習得することを目的とした勉強会、演習を開催した（全 17 回）。勉強会で用いたコンテンツについては、各団体等において理解度を確認するとともに、その内容を振り返ることができるよう、クイズ形式の自己学習用コンテンツとして提供するなど、更なる知識の定着を図った。

また、JISP で提供される脅威情報等について、スポーツ関連団体のリテラシーを考慮して編集した内容を隔週の頻度（内容の深刻度、緊急度を踏まえてタイムリーに提供する場合もあった）で提供した（計 30 回、令和３年５月末時点。）。

更に、独立行政法人情報処理推進機構の協力を得て、外部からの攻撃を受けやすいスポーツ関連団体のウェブサイトを対象に、サイバー攻撃の被害を受けやすい脆弱な状態となっていないか調査を行い、問題がある場合には修正対応案を提示するなどの取組を行った。

【取組による成果】

○　サイバーセキュリティ対策に係る知見を有する人材、組織的なノウハウの蓄積が十分とは言えないスポーツ関連団体等を対象に、様々な方法で対策を講じる上で必要な知識等を提示し、対策に関する水準の底上げを図ることができた。

○　業界内の横の関係が強固に構築されていない団体等の間で、有事の対応に必要不可欠な相互の信頼関係を構築することができた。

３　大会期間中における活動結果等

内閣サイバーセキュリティセンターでは、大会期間中、サイバーセキュリティを確保するため、対処調整センターを運用した。大会期間中における活動内容、その結果等を以下のとおり示す。

3.1　対処態勢の概要

対処調整センターでは、大会のイベントや競技スケジュールを踏まえ、サイバー攻撃のリスクが高まる期間において、関係組織との情報共有、相談や報告の受付、インシデント対処等に 24 時間対応可能な態勢を構築・運用した。

対処調整センターでは、各日で個別のインシデントへの対応を担当するチームを複数構成するとともに、大会組織委員会との円滑な連絡調整を行うための職員（以下「リエゾン」という。）を大会組織委会へ派遣し、情報セキュリティ関係機関及び治安機関から対処調整センターに対するリエゾン

の受け入れを行うことで、広範囲にわたる被害等が生じた場合でも柔軟かつ円滑に対処調整等ができるようにした。

3.2　インシデント等に対する対処調整

大会期間中は、関係組織 Web サイトの閲覧障害、不審なサイトに誘導する Web サイト、システム障害等のインシデントが複数確認又は報告されたものの、大会運営に影響を与えるインシデント等を発生させずに大会を無事に終えることができた。

対処調整センターでは、インシデント等を認知した場合、被害組織等との間で、その影響範囲、復旧に向けた対応方針等に関する情報共有を行い、必要に応じて助言を行った。また、これらの情報はセキュリティ調整センター[4]との間で適切に情報共有を行うとともに、他の体制参加組織に対しても定期的にインシデント発生状況等を取りまとめて情報発信を実施した。

3.3　予防・検知に関する情報の発信・共有

対処調整センターでは、情報セキュリティ関係機関等の協力を得るなどして把握したサイバー攻撃に関する脅威情報や観測情報を関係組織に迅速に共有した。脅威情報としては、関係組織の気を引くような名称の不審なプログラムの存在が確認された情報、大会関係組織を標的としたサイバー攻撃を予告する情報等を確認し、対処体制参加組織に対して、講ずるべき対策等を含めて注意喚起を実施した。また、観測情報としては、開閉会式や競技の偽ライブ配信サイト、大会関係組織に対する DDoS 攻撃、競技会場等の貸し出し用ネットワークに接続した端末からの不正通信等の情報を確認し、個別に対象組織に連絡した上で、対処・対策を促した。

4　英国、米国におけるサイバーセキュリティ対策（調査結果）

内閣サイバーセキュリティセンターでは、大会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等を検討するに当たって、その課題を明確化する目的で、国内外のサイバーセキュリティ対策の推進体制等に係る調査を行った。その中から、サイバーセキュリティ対策における官民連携等を検討する上での参考事例となる、「ロンドン 2012 大会後の英国の施策とその成果」及び「米国のサイバーセキュリティに関する情報共有体制」の概要を以下のとおり示す。

---

[4] 大会期間中において関係機関の連携を確保しつつ、大会組織委員会、東京都及び競技会場のある地方公共団体等との緊密な連携・調整を図るために内閣官房に設置された態勢

4.1　ロンドン 2012 大会後の英国の施策とその成果

ロンドン 2012 大会後の英国は、当時抱えていた多くの課題を解決するために、大会での経験も踏まえ、政府のサイバーセキュリティ対策に関する機能を国家サイバーセキュリティセンター（以下「NCSC」という。）へ統合し、「国家サイバーセキュリティ戦略 2016-2021」を推進している。この中で、政府が主導する英国内の民間事業者等のサイバーセキュリティを確保する取組として、重要インフラ事業者や公共・民間組織に対しての情報提供、実運用の有償・無償サポートを含む包括的な支援を積極的に実施している。主な取組を以下のとおり示す。

なお、内閣サイバーセキュリティセンターでは、ロンドン 2012 大会で英国が得た教訓、その教訓等を踏まえて推進された NCSC の取組を参考に、「対処態勢の整備」に係る取組を推進した。

① 重要な国家インフラ事業者等のサイバーセキュリティ運用への積極的な支援

NCSC では、サイバーセキュリティ対策に係るサービスの信頼性を確保する取組を推進している。具体的には、アドバイス、サポート、ガイド、脅威インテリジェンスの提供、重要なサービスを提供する組織に対してのセキュリティ運用支援等に係る多様な各種製品・サービス等について、NCSC が独自の基準に基づいた検証・認定を行った上で、公式にこれらのサービス等の有償提供を仲介するなどして、サイバーセキュリティ対策に係る運用面での積極的な支援を実施している。NCSC において検証・認定を受けて提供される製品・サービス数は、現在では 200 件を超えて、ペネトレーションテスト、業務向け製品セキュリティ、セキュリティコンサル、インシデントレスポンス、トレーニング等のサービスが英国内の多くの組織で活用されている。

② 非重要インフラ事業者等におけるサイバーセキュリティの確保に向けた積極的な支援

サイバー攻撃による被害があらゆる領域に拡大し、その影響が深刻化していることを踏まえ、NCSC では、重要インフラ分野のみに止まらず、国全体のサイバーセキュリティ対処能力を高めるため、ログイン管理、フィルタリング、脆弱性チェック、インシデント対処訓練等のサイバー攻撃の被害を防ぐ上で重要な対策サービスを認定ベンダー又は NCSC が自ら広く一般に提供している。

③ Cyber Security Information Sharing Partnership（CiSP）

NCSC では、登録組織向けに、政府や関係組織と安全な環境で連携することができ、また脅威情報の随時取得や組織間での情報交換、相談が可能と

なるプラットフォームとコミュニティを提供している。このプラットフォームとコミュニティの利用に当たっては、通信手段等で一定の基準を満たした組織等が利用できるようになっており、その利用者数は毎年右肩上がりで拡大し、英国全体のサイバーセキュリティを支えるコミュニティに成長している。

4.2　米国のサイバーセキュリティに関する情報共有体制

米国では、サイバーセキュリティの脅威に関する情報共有、分析等の取組を、各主体の相互協力により推進する活動が活発に行われている。

① Information Sharing and Analysis Center（ISAC）

ISAC は、重要インフラ分野を始めとして同一の業界内の事業者同士で、サイバーセキュリティに関する情報を共有するなどして、サイバー攻撃に対する防御力を高めることを目指して活動する民間組織である。

米国では、現在までに 24 の ISAC が組織されていて、各分野における情報共有等が推進されている。また、各 ISAC は、全米 ISAC 協議会(NCI) を通じて政府と相互に連携・調整を行っている。現在 24 の組織から構成されており、各部門において情報共有と運営を担っている。

我が国でも、ISAC が組織されているが、その組織数は米国よりも少ない。

② Information Sharing and Analysis Organizations（ISAO）

ISAO は 2013 年 2 月の大統領令に基づき国土安全保障省（DHS）に設置促進が指示されたもので、ISAC と同様にサイバーセキュリティに係る脅威の情報共有と分析を行う組織であるが、ISAC が組織されていない分野や ISAC のメンバーでない民間企業など幅広い分野において情報共有等を行うことを目的としている。ISAC とは異なり、産業分野ごとに関連付けられるものではなく、広く産官学の分野や地域等においてコミュニティが組織されたものとなっている。

政府は、国土安全保障省サイバーセキュリティ・インフラセキュリティ庁（CISA）の官民連携による情報共有分析組織である国家サイバーセキュリティ通信統合センター（NCCI）を通じて、ISAO と継続的に連携するとともに、包括的な調整を行っている。

５　大会に向けて推進した取組の大会後における活用方策

本有識者会議では、大会に向けて内閣サイバーセキュリティセンターが推進してきた取組の内容、その成果を踏まえ、今後の活用方策についての課題や期待される取組について討議を行った。その結果を以下のとおり示す。

5.1　大会に向けた取組を今後活用するに当たっての基本的な考え方

大会に向けた取組の全体を捉えた基本的な考え方について、構成員から示された意見・指摘は以下のとおりである。

【各構成員からの意見・指摘】

○　持続的なサイバーセキュリティ対策としての活用

大会に向けて整備した仕組み、推進した取組は、関係組織間で相当の期間、コストを費やして準備してきたものであり、我が国のサイバーセキュリティ対策として有効なものは、大会後の大規模国際イベントのみに限定することなく、平時の持続的な取組としてしっかりと継承していくべきである。他方、大規模国際イベント向けの取組として、限られた期間内で集中的に推進する分には効果が期待できるものの、対策に要する負担等を考慮すると、持続的な取組として継続するには現実的でないものもあることから、持続的な取組と大規模国際イベント向けの取組とでは同水準の対策を求めるのではなく、メリハリをつけて推進していくべきである。また、大会に向けた取組と比較すると、平時の持続的な取組の重要性は理解されづらいものであることから、そのブランディング・プロモーションについても重視していく必要がある。

○　様々な機関等が推進する取組、整備する連絡系統等を考慮した上での合理的な運用

取組等の継承に当たっては、内閣サイバーセキュリティセンターがサイバーセキュリティ対策に係る総合調整の事務等を担う観点から、社会全体を俯瞰し、十分に対応が進められていない領域を整理するなどした上で、必要な取組を推進していくべきである。

大会に向けた取組において、インシデント発生時等の相談・報告の窓口のワンストップ化を目指した工夫が講じられたところであるが、大会終了後においても窓口等が多岐にわたるものは同様にワンストップ化を図るなど、合理的・効果的に取組を推進することが重要である。

各府省庁、情報セキュリティ関係機関が、それぞれの役割に応じて推進している様々なサイバーセキュリティ対策としっかり連携するとともに、内閣サイバーセキュリティセンターが、これまでの取組に固執することなく、それぞれの取組の機能等を調整すること、既存の取組でカバーされていない領域のサポート等も含め、サイバー空間を必要最低限の健全な状態に保つために我が国のサイバーセキュリティを底上げできる仕組み作り、取組を推進するべきである。

○　公益性の観点に立った取組の推進

事業者等によって様々なサイバーセキュリティ対策に係るサービスが既に提供されていることにかんがみ、大会に向けた取組を今後活用する際には、

公益性の観点から真に政府が取り組む必要がある内容となっているか十分に留意しなくてはならない。

ただし、サイバー空間を必要最低限の健全な状態に保つための取組（サイバー衛生の確保）については、必要以上に公益性に固執するべきではない。

○　対処調整センター等における能力の維持

大会のために整備した規程、ガイドライン等の成果物は、大会後の取組にも活用できる重要な財産となるが、業務を通じて職員が得たノウハウや、インシデント対処等に係る経験も重要なものである。行政機関では、人事異動が定期的に行われているところであるが、職員の人事異動周期への配慮のほか、これまでに蓄積された職員の経験やノウハウが組織的にしっかりと継承できるようにすることが重要である。

○　大会後の大規模国際イベントにおける取組の活用

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は、今後も重要な課題となり、大会と同様に政府を中心とした対策が求められる。大会における経験を、2025 年日本国際博覧会（以下「大阪・関西万博」という。）を始めとした大規模国際イベントにおけるサイバーセキュリティ対策にしっかりと引き継ぎ、活かしていく必要がある。

【意見・指摘を踏まえた大会後の活用方策】

デジタル経済が急速に浸透しサイバー空間自体が公共空間化する中で、高度なサイバー攻撃が急増している状況を踏まえ、サイバー空間を必要最低限の健全な状態に保つため（サイバー衛生の確保）に、大会に向けて推進した取組から得た経験やノウハウを十分に活用しながら、我が国のサイバーセキュリティを底上げできる仕組み作り及び取組を推進し、社会経済を支えるサービスを安全安心に利用できるようにする必要がある。そのため、上記の各構成員からの意見・指摘に沿って、国として取り組むべき施策を力強く推進することが重要であり、特に人事異動により担当者が代わることを前提として、大会に向けて推進した取組から得た経験やノウハウを組織として受け継ぐ必要がある。

5.2　各取組に関する大会後の活用方策等

大会に向けて推進された個別の取組について、大会後にどのような役割が期待されるか、どのような点に留意するべきかなど、今後の活用方策等について討議を行った。各取組に対する構成員からの意見・指摘、これらの意見・指摘を踏まえた大会後の活用方策とその具体例を以下のとおり示す。

5.2.1 対処態勢の整備

①　インシデント等に対する対処調整

【各構成員からの意見・指摘】

○　インシデントの被害を受けた場合、被害組織においては自組織で調査等を行うことになるが、その被害が深刻な場合等には外部の機関等に対して助言や支援を求めたりする場合があるほか、被害状況の公表が不可欠な場合や、治安機関、地方自治体、事業所管省庁等の関係組織への報告が必要な場合がある。個別の場面によって対応が異なるものの、サイバーセキュリティ対策に十分な態勢を設けられていない事業者等からすると、このように相談先・報告先として複数の関係組織が存在する中で、どの組織に、どのような連絡を行えばよいかわからないというケースも少なくない。この点、助言や対処調整をワンストップで受け付ける窓口を設けたことは、各組織においてインシデント被害を受けた際の報告及びその問合せ対応等に係る負担を大きく低減したと評価できる。

○　インシデントの被害は特定組織のみでなく、広範囲に渡っていることも考えられることから、早期に政府としてインシデントを認知し、迅速かつ的確に対処することが望まれる。他方、事業者等によっては、どのようなレベルのインシデントで相談、支援の要請を行えばよいかイメージできず、躊躇することがある。大会後も対処調整センターにおける対処調整に係る機能等を継続するのであれば、被害組織から積極的なインシデント被害に係る報告、相談がなされるよう、想定するインシデント等の事例を積極的に示すとともに、報告・連絡・相談等が実施できる相互の信頼関係を醸成していくことが重要である。

○　被害組織に対する支援内容については、セキュリティ関係事業者において既にインシデントの原因調査、対策の提案等に係るサービスが多数提供されているが、被害組織のニーズに十分に応えられない場合もある。重大なインシデントの早期把握、被害拡大防止等の観点からの初動対応のように公益性の観点から真に政府が取り組む必要がある内容については、政府がスピード感をもって積極的に支援を実施していくべきである。

○　報告を受けたインシデント等への助言、対処調整等、インシデント発生時の対応に重点を置いた取組が推進されてきたが、サイバー攻撃の抑止の観点から、攻撃者の視点からインシデントを分析し、その分析結果を踏まえた対応を積極的に講じることも重要である。被害情報等に関する総合的な分析を行うことによって、特定が難しい攻撃者の情報や攻撃ターゲットの解明も可能になる。そのため、対処調整に際しては、個別のインシデントへの対処のみに止まらず、被害情報等を総合的に分析し、分析結果から明らかになった攻撃者等に関する情報の

発信、指令サーバのテイクダウンを始めとする広義の対処に関する取組の企画・支援等、積極的なサイバーセキュリティ対策の推進についても期待したい。

【意見・指摘を踏まえた大会後の活用方策】

大会後における「インシデント等に対する対処調整」に係る取組は、各組織における自律的なインシデント対処を原則としつつ、被害組織単独で対応が困難なインシデント対処を迅速、的確に支援することを主たる目的に、内閣サイバーセキュリティセンターにおいて被害組織等からの支援要請、相談、報告等をワンストップで受け付ける窓口を設け、インシデント対処への初動支援等を行うことが望まれる。また、支援要請等によって享受可能なメリットの周知等を通じて事業者等への働きかけを行うとともに、大会に向けた取組と同様に、内閣サイバーセキュリティセンターが、インシデント対処に係る助言や支援を行うことができる情報セキュリティ関係機関、被害組織の事業所管省庁、治安機関等の関係組織と緊密に連携して対応に当たることが望まれる。さらに、個別のインシデント対処のみならず、被害情報等を総合的に分析し、分析結果から明らかになった攻撃者等に関する情報の発信、指令サーバのテイクダウンを始めとする対処に係る企画、支援を行うなどの積極的なサイバーセキュリティ対策の推進が望まれる。想定される具体的な取組事例を以下のとおり示す。

○　被害組織等からの支援要請、相談、報告等に係る関係組織間のワンストップでの窓口
○　各組織が自組織内で対処が困難なインシデント対処に係る支援、情報セキュリティ関係機関との対処調整
○　サイバーセキュリティに関する相談等の促進及び相談等への助言
○　被害情報等の分析及び分析結果から明らかになった攻撃者等に関する情報の発信
○　不正サイトのテイクダウン等の対処手法に係る企画、調整
○　報告・連絡・相談等が実施できる相互の信頼関係醸成のための取組

②　予防・検知に関する情報の発信・共有

【各構成員からの意見・指摘】

○　脅威情報等の提供に当たっては、推奨される具体的な対策等も含めて提供することが重要であるが、その点、対処調整センターの情報発信等は、対処体制参加組織のリテラシーに合わせて対策等の内容が示されているため有効である。

○　情報セキュリティ関係機関、民間のセキュリティ事業者等においてもサイバーセキュリティ上の脅威情報は様々なものが発信されているが、注意喚起する組織が多いほど脅威の深刻性が高いと判断する材料になる。特に内閣サイバーセキュリティセンターから発信される脅威情報であれば注目度も高まることから、脅威になり得る情報は躊躇することなく積極的に提供するべきである。
○　政府として把握、分析した結果、通信遮断等を行うことが好ましいと判断された有害なインディケータ情報等は、各事業者等で活用しやすい形式に加工して積極的に提供していくべきである。
○　国内におけるサイバー攻撃被害について報道されることがあるが、どのような弱点を突かれて被害が生じたのか、その技術的な原因を把握できるようなケースは多くない。実被害が生じたものこそ、他の事業者等で二次的な被害を受けないようしっかりと対策を講じていく必要がある。そのため、インシデント被害の相談等を扱う中で把握された被害情報等については、可能な範囲で、被害組織及びそのシステム等の機微な情報をサニタイズした上で共有していくべきである。
○　自律的に情報収集できている組織にとっては、一次情報源からの情報提供は有用であるが、二次情報源以降の情報提供については中間組織が付加価値を付けないと有用度が下がることになる。

【意見・指摘を踏まえた大会後の活用方策】

大会後における「予防・検知に関する情報の発信・共有」に係る取組は、インシデント被害の未然防止や各組織におけるインシデント対処を支援することを目的に、高度な情報発信機能が求められる内閣サイバーセキュリティセンターにおいて、付加価値を付けるため、様々な機関、事業者等から発信される脅威情報等をワンストップで活用しやすい内容で共有するとともに、情報セキュリティ関係機関等と連携した上で各組織に関する観測情報を個別に提供することが望まれる。また、国内事業者等におけるインシデント被害の原因とその技術的な対策に係る情報、そのサイバー攻撃で実際に用いられたインディケータ情報等を必要に応じてサニタイズした上で提供するなど、更なる被害の拡大防止に向けた積極的な情報共有も望まれる。想定される具体的な取組事例を以下のとおり示す。

○　内閣サイバーセキュリティセンターにおいて収集した脆弱性情報、攻撃予見情報、国家レベルの攻撃グループの攻撃動向に係る情報等の脅威情報、インディケータ情報、インシデント情報（被害組織が特定できる情報をサニタイズしたもの）等を、各組織のリテラシーが異なる

ことを考慮しつつ、対処方法等を含めた上で、JISP を用いてワンストップで積極的に提供

○　各組織における個別具体の脅威について、情報セキュリティ関係機関等の協力を受けた上で観測された情報を対象組織に個別に提供

○　内閣サイバーセキュリティセンターにおいて把握・分析した有害なインディケータ情報を機械連携の仕組み等を活用して提供

③ インシデント等への対処能力の向上

【各構成員からの意見・指摘】

○　取組の継続に際しては、対処体制参加組織間の情報連携に止まらず、基本的な対処能力の底上げに向けた実践的な演習・訓練にも取り組んでいくべきである。他方、サイバーセキュリティ対策に係る演習等は民間のセキュリティ企業のサービスを始め多方面で開催されていることから、内閣サイバーセキュリティセンターにおける演習・訓練にあっては、定型化したインシデント対応の手法等を題材にするのではなく、被害が急増している又はそのおそれがある事例等最新の情勢を捉えるなどして、民間のセキュリティ企業等が既に提供するサービスとの役割を整理した上で取り組むべきである。

【意見・指摘を踏まえた大会後の活用方策】

大会後における「サイバー攻撃への対処能力の向上」に係る取組は、インシデント発生時における関係組織間の連携強化だけでなく、被害組織による自律的なインシデント対処及び未然防止が可能となるような知識・技能の習得を目的に、内閣サイバーセキュリティセンターにおいて、既存の訓練や演習との役割分担に留意しながら、JISP を利用した実践的な演習を開催することが望まれる。また、演習だけでなく、サイバーセキュリティ対策の強化が急務となるテーマや、高度化・進化するサイバー攻撃への対処をテーマに各組織で意見交換会を開催するなどの取組が望まれる。想定される具体的な取組事例を以下のとおり示す。

○　インシデント発生時に政府を始めとする関係組織と的確に情報共有する手順に加えて、各組織が自律的に最低限の対処を行うために必要な能力等を習得するための訓練・演習の開催

○　高度化・複雑化するサイバー攻撃への対処に必要な能力を習得するための訓練・演習の開催

○　サイバーセキュリティ対策に係る取組事例、サイバー攻撃への対処方法、ノウハウ等の情報を業界に捕らわれずに多様な組織間で情報交換できる場の提供

④ 情報共有プラットフォームの提供

【各構成員からの意見・指摘】

○　標的とする情報の窃取等、明確な目的を持って行われる組織的・国家的なサイバー攻撃による被害が顕著になる中、同一の活動目的又は業界内の組織間における情報共有や連携強化が、二次被害等を防ぐ上で重要となる。このような特定のコミュニティ内での情報共有では機微な情報を扱うことになるため、情報共有プラットフォームのサイバーセキュリティ対策が非常に重要となるが、事業者間で調整してこのような基盤を準備することは容易ではない。政府が整備・運用する JISP を信頼性の高い基盤の一つとして提供可能になれば、コミュニティの立ち上げ、活動の活性化が図られるほか、コミュニティ内、コミュニティ間の情報連絡、連携も円滑になることが期待される。

○　インディケータ情報の共有は、体制参加組織において実効的なサイバーセキュリティ対策を講じる上で、有効な取組である。円滑に対策が講じられるよう機械連携等の仕組みを用いつつ、積極的な情報共有を行うべきである。

○　コミュニティ内のメンバーのみで有用な情報が共有される場合があるため、自らが所属するコミュニティにおける情報収集も重要である。

【意見・指摘を踏まえた大会後の活用方策】

大会後における「情報共有プラットフォームの提供」に係る取組は、情報共有に参加する組織が信頼関係を構築する際の礎となるものであることから、各組織間での情報共有を安全かつ効率的に行うことを目的に、内閣サイバーセキュリティセンターが、持続可能性等に留意しながら JISP を整備・運用し、各組織に提供していくことが望まれる。また、JISP の提供は、サイバーセキュリティの確保を目的とした ISAC、ISAO 等のコミュニティの立ち上げ、活動の活性化等に貢献することも期待され、複数のコミュニティが JISP を利用するようになることで、コミュニティ間の横串での情報共有が望まれる。加えて、情報共有プラットフォームにおける機能の一つとして、機械連携等の仕組みを用いたインディケータ情報の提供についても期待される。想定される具体的な取組事例を以下のとおり示す。

○　インシデント発生時における被害組織からの対処支援要請、相談、報告、内閣サイバーセキュリティセンターからの脅威情報等の提供等、各機能を提供する統一窓口としての運用

○　インシデント発生時における情報共有等が必要となる関係組織

（ISAC、セプター、システム整備事業等の委託先となるベンダー事業者、大規模国際イベント関連組織等）の参加促進に係る調整

○　ISAC、ISAO 等の設立、運営に用いるプラットフォームとしての提供による各コミュニティ活動の活性化とコミュニティ間の情報共有 HUB としての活動

○　内閣サイバーセキュリティセンターにおいて把握・分析した有害なインディケータ情報を機械連携の仕組み等を活用して事業者等に提供（再掲）

5.2.2　リスクマネジメントの促進

①　リスクアセスメント

【各構成員からの意見・指摘】

○　複数の事業者等が共通の手法でリスクアセスメントに取り組むことで、自組織の幹部とサイバーセキュリティ対策についての考え方、その手法等についての議論を行ったり、同一業種内の他事業者等との間で効果的な対策について意見交換を行ったりする機会が作られた。自組織における対策を見直すような機会が設けられることは貴重であり、対策を促進していく上で効果的である。

○　リスクアセスメントは、自組織の状況を把握することが重要であるため、その対象事業者等が外部からの求めでやらされているという認識では効果が期待できず、自ら問題意識を持って取り組む組織を対象に取組を推進するべきである。

○　より多くの事業者等で取り組まれるよう、ガイドライン等機微な情報が含まれない資料は積極的に公開するとともに、効果的な活用事例等を整理して周知するなどして、取組についての考え方や必要性をしっかりと社会に広げていくことが重要である。今回のリスクアセスメントの取組が事業者間で情報交換を実施するきっかけにもなったことから、ISAC や事業所管省庁と連携して、コミュニティ内において一斉に取組を実施するなどキャンペーンとして推進することも有効である。

○　リスクアセスメントの結果等について個別にフィードバックを得ることができるという点が事業者等にとってのメリットであるが、各組織が自組織に適した方法・内容でリスクアセスメントを自ら効果的・効率的に実施できるような仕組み・ツールを設けるなど、内閣サイバーセキュリティセンター及び事業者等の両者に負担が生じない取組を講じていくことも重要である。

○　この度の取組では、事業継続に重点を置いた取組を推進したとのこと

であるが、リスクとして捉えるものは、個々の事業者等のサービス、情報資産等によって異なることから、複数のアプローチによる評価手法を検討するほか、事業者等の規模や対策のレベルに応じた手法・内容を検討するべきである。

○　リスクアセスメントの評価結果は、自組織の対策状況を評価する上でわかりやすい指標となるものの、総合的な評価として他の事業者等と比較して「よくできている」「足りていない」等の単純な結果を示してしまうと、その子細についての確認がなされずに満足されてしまうおそれがある。個々の事業者等のサイバーセキュリティ対策は、一概に並べて比較することができるものではないという点に留意し、その評価結果が短絡的に捉えられないよう配慮するべきである。

【意見・指摘を踏まえた大会後の活用方策】

大会後における「リスクアセスメント」に係る取組は、特に経済・社会活動を支える事業者等を対象としてサイバーセキュリティ上のリスクを軽減させることを目的に、内閣サイバーセキュリティセンターが、リスクアセスメントの手法等を提供していくことが望まれる。その際、個々の組織のサービス、情報資産等に応じた複数のアプローチによる評価手法、各組織の規模や対策のレベルに応じた評価手法を準備・公表することが望まれるほか、各組織がリスクアセスメントの機会をどのように位置づけ、活用するべきであるかなどの観点についてガイダンスを示すことが有用である。また、リスクアセスメント結果に対するフィードバックによって取組の実効性を確保することも重要であり、対象事業者等にとって取り組みやすく、かつその負担が軽減されるように、評価結果の充足性等を効果的・効率的に確認できる仕組み・ツールの開発等の取組を推進することが望まれる。想定される具体的な取組事例を以下のとおり示す。

○　リスクアセスメントに関する位置づけ、活用方策、手順等の提供・公表を含めた各組織による自主的なリスクアセスメントの支援

○　事業者の分野、規模、対策レベル等に応じて活用できるリスクアセスメント手法の開発・普及

○　サイバーセキュリティに係るリソースが十分でない組織等に対するリスクアセスメント結果をフィードバックする点検ツール等の提供

②　横断的リスク評価

【各構成員からの意見・指摘】

○　サプライチェーン対策等の重要性が認識され始めたが、各組織にお

ける自主的なサイバーセキュリティ対策のみでは限界がある。政府自らが直接的にセキュリティ対策の実施状況に係る検証を実施したことは、セキュリティの確保に不可欠であり、今後の大規模国際イベント等でも積極的に取り組むべきである。

○　攻撃シナリオを使って、事業者等にその対処方法をシミュレーションさせたり、又は、多層防御のどこでそのような攻撃を防御可能になっているのかを考えさせたりする取組について、このような攻撃シナリオは自社の内情を知っているからこそ各事業者内で作成することが難しく、外部からの目線でシナリオを作成することが効果的である。今後の大規模国際イベント等において、国を挙げてサイバーセキュリティ対策を講ずる際にも、セキュリティ動向や攻撃パターンを知る内閣サイバーセキュリティセンターが主導して大会に向けた取組と同様の取組を推進するべきである。

○　サイバーセキュリティ対策の検証において事業者内で対応しなければならないシステム上の脆さ等が確認された際に、当該課題に対処できる期間を考慮したスケジュールで取組を実施するべきである。

【意見・指摘を踏まえた大会後の活用方策】

大会後における「横断的リスク評価」に係る取組は、大規模国際イベントにおいて特に重要な役割を担う事業者等を対象として、各組織における自主的なサイバーセキュリティ対策では不十分と考えられる場合や、十分な公益性が認められる場合に、内閣サイバーセキュリティセンターが、最新の攻撃手法等を踏まえた攻撃シナリオ等を用いて、特に重要な役割を担う事業者等におけるサイバーセキュリティ対策状況について検証を行い、その対策を改善していくことが望まれる。想定される具体的な取組事例を以下のとおり示す。

○　大規模国際イベントにおいて特に重要なサービスを提供する事業者等のサイバーセキュリティ対策に関する攻撃シナリオ等を用いた早期の政府による検証

○　大規模国際イベントにおける会場施設等に対するペネトレーションテスト

③　スポーツ関連団体に対する勉強会

【各構成員からの意見・指摘】

○　標的とする情報の窃取等について明確な目的を持って行われる組織的・国家的なサイバー攻撃による被害が顕著になる中、同一の活動目的又は業界内の組織における情報共有や、連携強化が、二次被害等

を防ぐ上で重要となる。(再掲)

○　情報共有、連携強化のためのコミュニティの立ち上げ、運営に際しては、仮にサイバーセキュリティ対策についての問題意識を事業者等の間全体で共有していた場合でも、事業者等の間でセキュリティに係る人的リソースやコミュニティ運営に係るノウハウが一定程度保有されていなければ、その実現は容易ではない。その点、大会に向けてスポーツ関連団体に対して行った取組は、コミュニティ内のサイバーセキュリティ対策のレベルの底上げ等を図る上で有効であり、ISAC、ISAO 等のコミュニティの立ち上げ、活動の活性化を図るための支援策として有効に機能することが期待される。

○　ISAC、ISAO 等の特定のコミュニティ内での情報共有は機微な情報を扱うことが想定され、情報共有プラットフォームのサイバーセキュリティ対策が非常に重要になるものの、各事業者等の間で調整してこのような基盤を準備することは決して容易なことではない。政府が整備・運用する JISP のような信頼性の高い基盤が一つの選択肢として提供されるのであれば、コミュニティの立ち上げ、活動の活性化が図られるほか、コミュニティ内、コミュニティ間の情報連絡、連携も円滑化すると期待する。

【意見・指摘を踏まえた大会後の活用方策】

「スポーツ関連団体に対する勉強会」に係る取組は、大会後における新たなコミュニティの立ち上げ・運営を支援する取組において有用である。そのため、サイバーセキュリティ対策に係る能力の底上げが急務となる組織における基本的な知識・技能の習得等を目的に、内閣サイバーセキュリティセンターが、事業所管省庁等と連携して取組を加速することが望まれる。特に、事業分野全体でデジタル化の推進が期待されるものの、IT やセキュリティに関する専門知識や業務経験が乏しい分野等に対して必要な支援を重点的に実施していくことが重要である。また、コミュニティ内では安全で効率的な情報共有が求められるため、信頼性の高い情報共有基盤が必要となる。想定される具体的な取組事例を以下のとおり示す。

○　支援対象のコミュニティに係る事業所管省庁等との調整

○　支援対象のコミュニティに対する勉強会・机上演習の開催、セキュリティ情報ニュースの発信・共有、簡易ウェブサイトチェック等の実施、JISP の提供等

5.2.3　大規模国際イベントにおけるサイバーセキュリティ対策

【各構成員からの意見・指摘】

○　イベントが開催される際は、平時には業務上の関係がない組織と連携する機会が生じるため、平時の取組をベースに、この度の大会で構築した対処態勢と同様の体制を構築することにより、各関係組織におけるサイバーセキュリティ対策やインシデント対応を他の体制参加組織の取組と有機的に結びつけていくべきである。

○　リスクマネジメントを促進するため、大規模国際イベントに際しては、関係事業者等における自主的なリスクアセスメントのほか、内閣サイバーセキュリティセンターが関係事業者等の対策状況を検証する横断的リスク評価、ペネトレーションテスト等の取組を推進することによって、実効的な対策を関係組織が講じていくようにすることが重要である。一方で、あらゆる関係事業者等を対象に同一の水準で対策を講じることは現実的でなく、非効率な面もあることから、当該イベントにおけるサービスの重要性等に照らし、メリハリをつけた対策が講じられるようにするべきである。

【意見・指摘を踏まえた大会後の活用方策】

大会後における「大規模国際イベントにおけるサイバーセキュリティ対策」に係る取組は、特に国が主体的な役割を担うイベントにおけるサイバーセキュリティの確保を目的に、大会におけるサイバーセキュリティの確保に向けた取組に倣って、内閣サイバーセキュリティセンターにおいて、関係組織との間で「対処態勢の整備」、「リスクマネジメントの促進」に係る取組を推進していくことが望まれる。想定される具体的な取組事例を以下のとおり示す。

○　平時の取組をベースにした大規模国際イベント等の関係組織間での対処態勢の整備（インシデント等に係る対処調整、予防・検知に関する情報の発信・共有、サイバー攻撃への対処能力の向上、情報共有プラットフォームの提供等）、リスクマネジメントの促進（リスクアセスメント、横断的リスク評価、勉強会の開催等）

○　大規模イベント時等には、平時に加えて、根拠のない情報による混乱を抑えるための情報発信を実施

5.2.4　取組を推進するに当たって対象とする領域

サイバー空間の秩序の維持に当たっては、様々な社会システムがそれぞれの任務・機能を自律的に実現し、あらゆる組織がその役割や責任を果たすことが必要となる。他方、サービスの進化・多様化が進む一方で、サイバー空間の脅威の増大、脆弱性の顕在化等、不確実性が増す

情勢にあり、各組織で講ずるべきサイバーセキュリティ対策に求められる水準は高度化、複雑化していると言える。デジタル化の更なる進展に向けて、各組織に求められる対策は今後より一層重要になると考えられるものの、個々の自律的な取組のみで対応していくには限界がある。我が国のサイバーセキュリティ対策をより高い水準に引き上げるには、英国において取り組まれる政府から事業者等への積極的なサイバーセキュリティ対策を参考に、政府から事業者等に対する支援を推進するとともに、米国における ISAC、ISAO 等の特定の目的を共有するコミュニティ内又はコミュニティ間での強固な連携等を参考に、各組織における相互の支援・連携の強化に向けた支援を推進することが重要であると考える。

内閣サイバーセキュリティセンターが大会を契機に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整備・運用した対処調整センター、準備・運営への影響の未然防止や想定されるサイバーセキュリティ上のリスクへの対策の促進のために推進してきたリスクマネジメントは、サイバーセキュリティの確保に向けて、業種分野等の隔たりなく、関係組織が緊密に連携・協力して取り組んできたものであるが、こうした取組は前述の課題認識や社会的要請に応えられるものであると期待できる。

これまでの取組は、大会の関係組織を対象に実施してきたものであるが、大会後にあっては取組の対象領域を、社会経済を支えるサービスを提供する事業者等に拡大し、各組織が提供するサービスにおいて適切にサイバーセキュリティが確保されるようにするべきである。取組の対象領域の拡大に当たっては、サイバー脅威情勢等を考慮することとし、公益性等の観点から優先度の高い分野について、事業所管省庁等と連携した上で、コミュニティの構築・運営支援や対処体制の追加等を通じて、徐々にその対象を拡大していくことが望まれる。一方、持続的な対策としての各取組の推進に当たっては、様々な既存の取組における現状と課題を踏まえた上で各取組との整合性を確保すること、対象拡大の方法や基準の考え方を整理すること、取組の必要性や有益性について各組織の理解を得ること等の運用上の課題が存在するところ、大会後においても各取組が確実に機能するよう、内閣サイバーセキュリティセンターが全体を俯瞰しながら、これらの課題を関係組織との間でしっかり調整するなど丁寧な対応が求められる。

また、令和５年に我が国での開催が予定されるＧ７サミット、７年の

大阪・関西万博といった大規模国際イベント開催時には、大会と同様に、関係組織間で緊密に連携した上で対処体制を構築し、イベントの安全、円滑な準備及び運営における継続性の確保に向けてサイバーセキュリティ対策を進めていくべきである。特に、大阪・関西万博は、「未来社会の実験場」をテーマに ICT を含む様々な最先端技術を発信する場に位置づけられ国内外から大きな注目を集めるほか、大会と同様に、関係する機関、事業者等が多岐にわたるなどの特徴を有していることから、サイバーセキュリティ対策上の課題も多岐にわたると考えられる。そのため、同イベントへの対策については、速やかに準備を進めていくべきである。

加えて、サイバーセキュリティリスクが多様化・高度化する中で、国内外の関係者と協調しながら、こうした取組を継続的に進めるため、内閣サイバーセキュリティセンターにおいては、これまで以上にしっかりとした体制を整備することが求められる。

６　まとめ

大会のセキュリティ確保に当たっては、内閣サイバーセキュリティセンターを中心に、リスクマネジメントによって関係組織全体のセキュリティ対策を漏れなく強化するとともに、インシデント発生時等における分野横断的な情報共有と関係組織間で連携した対処支援が可能となる仕組みを構築するなど総合的な対策を推進した。結果的に、大会の運営に影響を及ぼすサイバー攻撃を許すことなく大会を終えることができたが、この成果は、各組織が相互に連携し、自身の役割に応じたセキュリティ対策をしっかりと講じたことによるものであり、関係組織全体で勝ち取ったものであるといえる。

サイバー空間において提供されるサービスは、クラウドサービスの普及、サプライチェーンの複雑化等に伴い、サイバー空間内やサイバーとフィジカルの垣根を越えた主体間の「相互連関・連鎖」が一層深化する傾向にあり、サイバーセキュリティの確保に当たっては、各組織の役割や防御すべき対象を不断に検証するとともに、サイバー攻撃等の抑止につながるような取組も含めて、多層的に取組を強化していかなければならない。このような情勢において、自律的な取組、多様な組織の緊密連携の重要性は不変であるが、それらの基盤となる「公助」の機能も必要不可欠であり、自助共助では対応が困難な事象や課題に対して、国が総合的な調整を行う機能を担って、社会全体のセキュリティを確保するための取組を不断に推進するべきである。「４　英国、米国におけるサイバーセキュリティ対策（調査結果）」で紹介したように、諸外国においては各組織の相互連携、相互支援に係る取組が活発に推進されて

おり、我が国でも、対策の強化に向けてあらゆる組織が効果的に連携する取組を推進していく必要がある。この点、内閣サイバーセキュリティセンターが中心となって推進した大会に向けた取組は、新たな「公助」の取組のモデルになると考える。

本有識者会議では、大会に向けた取組の成果を踏まえつつ、今後の我が国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、課題等について討議を行い、その方向性を示すことができたと考える。今後は、新サイバーセキュリティ戦略で謳われている「サイバー攻撃対処から再発防止等の政策措置までの総合的調整を担うナショナルサート機能の強化」についての検討とも連動しながら、本報告書で示された方向性に即した具体的施策を検討し着実に実行に移していくことが求められる。取組の推進に当たっては、関係組織の取組が最大限効果を発揮できるよう、各取組の関係性や役割を丁寧に調整するなど解消すべき課題も存在するが、大会を通じて得られた経験や信頼関係を活かし、実りのある対策に発展させるべく各組織が一丸となって取り組んでもらいたい。大会に向けた取組が、今後の我が国のサイバーセキュリティ対策の新たなステージへの一歩となることを期待している。

最後に、本報告書は、大規模イベントにおけるサイバーセキュリティの確保の観点のみならず、社会への安全な環境の提供に向けて産学官で前向きに連携して重大な成果を得ることができたという点においても、非常に有益なノウハウが取りまとめられたと認識している。これらのノウハウは、今後の我が国のサイバーセキュリティ対策の在り方を検討する上での道標となるものであり、サイバーセキュリティ対策に携わる者に広く本報告書が読まれることを期待したい。

参考資料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の開催について

１．趣旨

東京オリンピック・パラリンピック競技大会、G20 大阪サミット、ラグビーワールドカップ 2019 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て整備した仕組み、その運用経験及びノウハウを、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を行うため、「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」（以下「有識者会議」という。）を開催する。

２．構成

（１）有識者会議の構成は、別紙のとおりとする。

（２）有識者会議に座長を置く。座長は、その構成員の互選により決する。

（３）座長は、必要があると認めるときは、構成員以外の者に対し、有識者会議に出席して意見を述べることを求めることができる。

３．庶務

有識者会議の庶務は、内閣官房において処理する。

４．その他

前各号に掲げるもののほか、有識者会議の運営に関する事項やその他必要な事項は、座長が定める。

別紙

「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」 構成員

猪俣 敦夫	大阪大学 サイバーメディアセンター 情報セキュリティ本部 教授
金子 啓子	大阪経済大学 経営学部 ビジネス法学科 准教授
斎藤 衛	株式会社インターネットイニシアティブ セキュリティ本部長
清水 詳士 （令和3年1月から10月まで）	東京都 デジタルサービス局総務部 情報セキュリティ担当課長
谷口 浩	東京電力ホールディングス株式会社 セキュリティ統括室長
藤本 正代	情報セキュリティ大学院大学 教授
満永 拓邦	東洋大学 情報連携学部 准教授

（五十音順、敬称略）

参考資料２

開催実績

第１回　令和３年２月１日
　１　有識者会議の進め方について
　２　大規模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について
　３　その他

第２回　令和３年３月 11 日
　１　国内外の政府機関等におけるサイバーセキュリティ施策について
　２　各取組を推進する中で得られた成果と今後の課題等について
　３　その他

第３回　令和３年４月 19 日
　１　中間整理に向けた確認・討議事項等について
　２　その他

第４回　令和３年６月 21 日
　１　中間整理（案）について
　２　その他

第５回　令和３年 10 月 11 日
　１　東京大会における活動報告について
　２　サイバーセキュリティ戦略について
　３　東京大会における活動結果等を踏まえた今後の活動方針について
　４　その他

第６回　令和３年 12 月２日
　１　最終報告（案）について

参考資料３

最終報告
資料集

1　東京大会に向けて対処調整センターが推進した取組

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

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

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

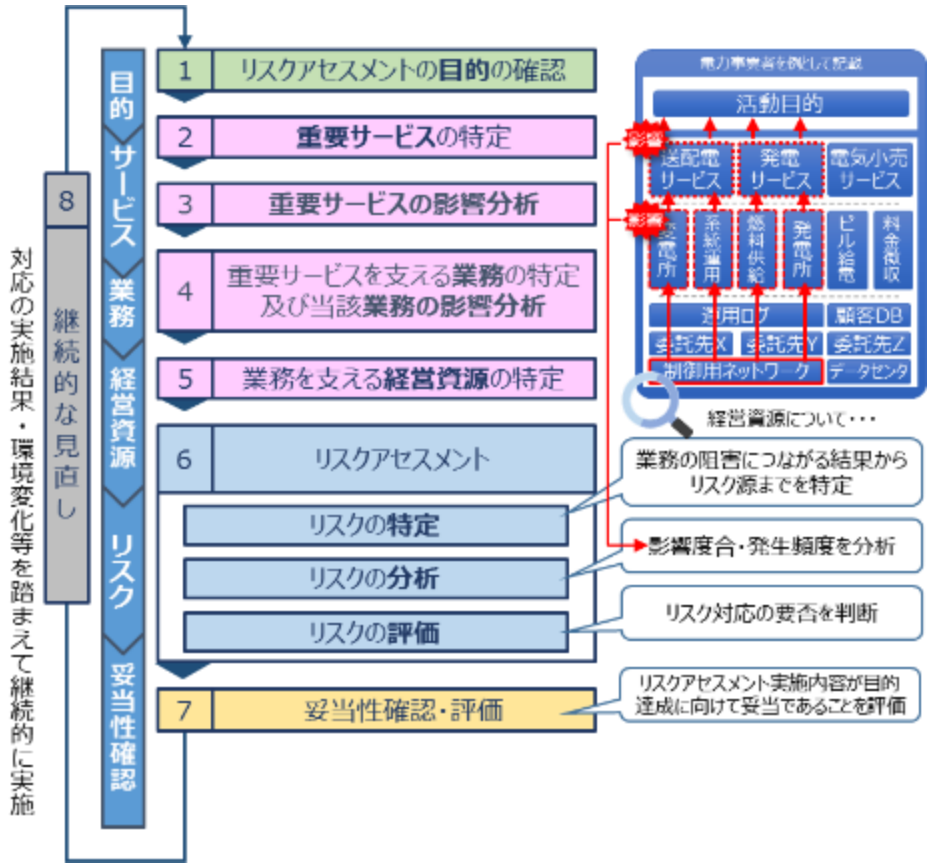
各関係主体が、

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。

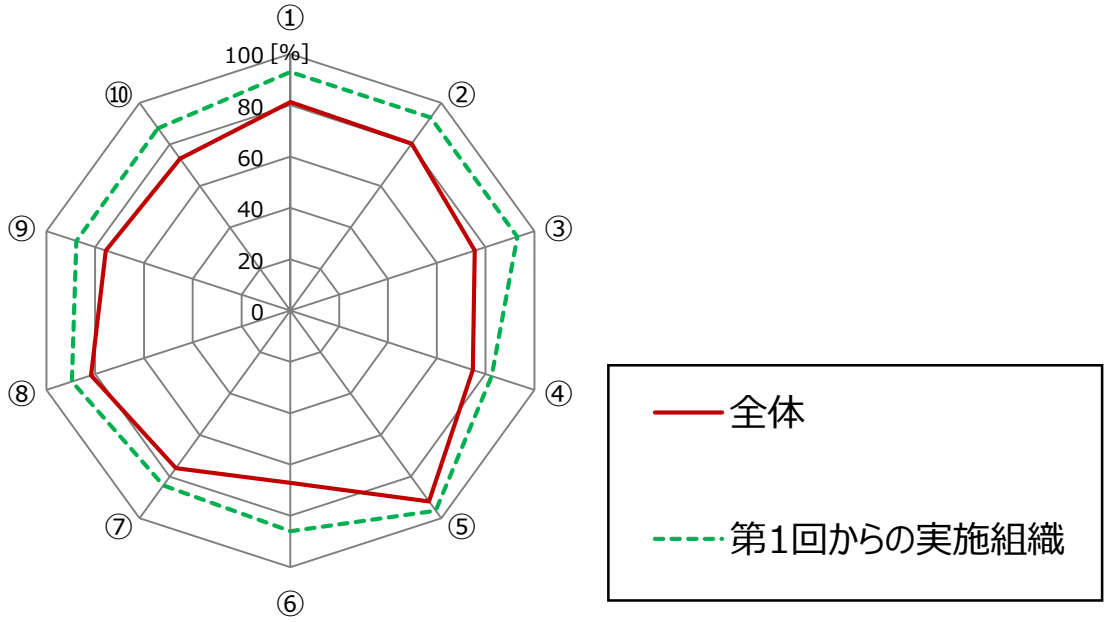


リスクアセスメント（サイバーセキュリティ対策の全般的な運用状況）

第６回（2020年11月～2021年１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。

- リスクアセスメントの回数を重ねるにつれて対策の実施状況が改善されている様子を確認(下図)。
- 特に、第1回からの実施組織は、各回の取組を経て、自組織等における演習・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。

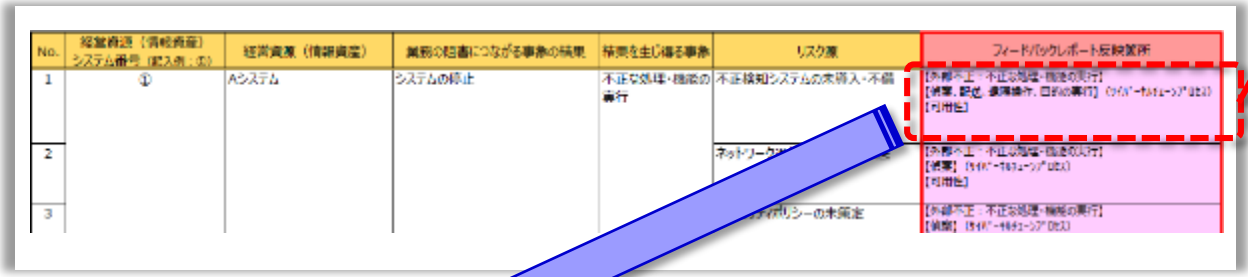
Plan	①	基本方針の策定
	②	内規等の策定
	③	対策の計画策定
	④	研修実施
	⑤	内部統制の強化
Do	⑥	コンティンジェンシープランの策定
	⑦	事業継続計画の策定
	⑧	演習・訓練の実施
Check	⑨	監査の実施
Act	⑩	是正すべき対策の検討



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



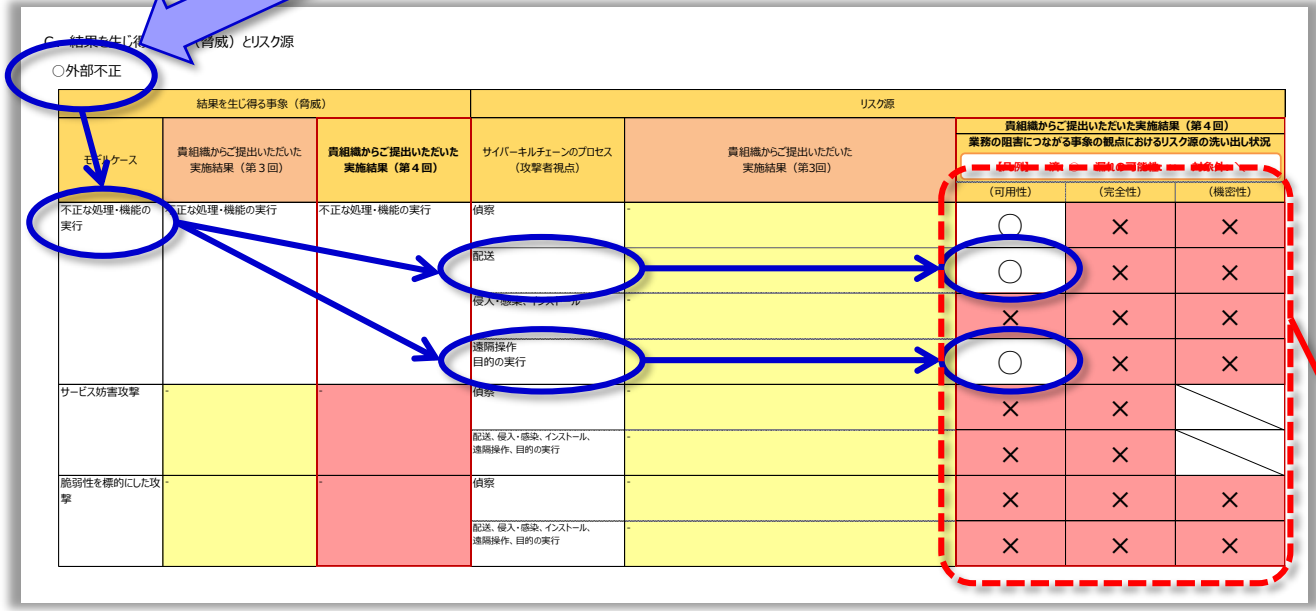
No.	経営資源（情報資産） システム番号（記入例：①）	経営資源（情報資産）	業務の阻害につながる事象の結果	脅威を生じ得る事象	リスク源	フィードバックレポート反映箇所
1	①	Aシステム	システムの停止	不正な処理・機能の実行	不正検知システムの未導入・不備	【外部不正：不正な処理・機能の実行】 【配置、配信、遠隔操作、目的の実行】（ｻｲﾊﾞｰｷﾙﾁｪｰﾝﾌﾟﾛｾｽ） 【可用性】
2					ネットワーク	【外部不正：不正な処理・機能の実行】 【侵害】（ｻｲﾊﾞｰｷﾙﾁｪｰﾝﾌﾟﾛｾｽ） 【可用性】
3					ポリシーの未策定	【外部不正：不正な処理・機能の実行】 【侵害】（ｻｲﾊﾞｰ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

（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



C．結果を生じ得る事象（脅威）とリスク源

○外部不正

結果を生じ得る事象（脅威）			リスク源		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		
シナリオケース	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）	（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・感染、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	-	×	×	×

「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

横断的リスク評価（取組の概要）

●横断的リスク評価の取組

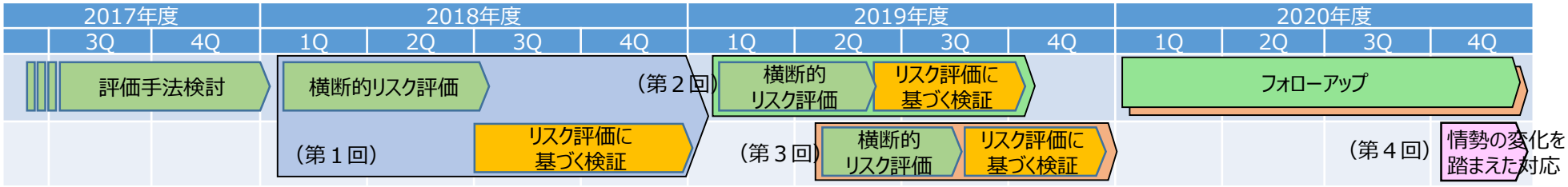
重要サービス事業者等において想定されるサイバーセキュリティリスクに基づき、サイバーセキュリティ対策の実施状況をNISCが検証する。
これにより、大会の成功にとって重要な機能が継続して提供されることを確認するとともに、不備があった場合は、重要サービス事業者等へフィードバックすることにより、当該重要な機能が継続して提供されることの確からしさを向上させる。

○ 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

○ 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

○ 2020年度においては、第４回の取組として、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た対応を実施



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勉強会及び演習を開催。参加団体は、東京オリンピック・パラリンピック競技団体を中心に、JOC、JPC、日本スポーツ協会の加盟団体やその他希望する団体としており、これまでに、延べ371団体、503名が参加した。

○ 取組概要

・勉強会及び演習の開催

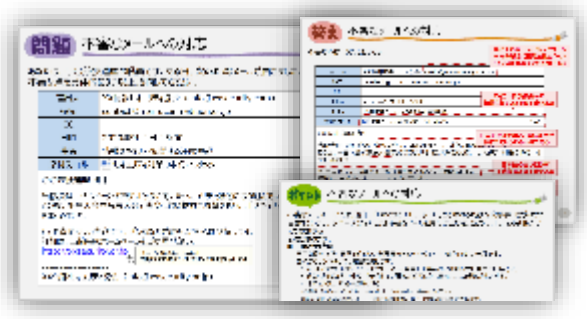
日時：　【勉強会(第15回)】11月25日　　【演習(第1回)】２月16,24日
場所：　【勉強会(第15回)】日本青年館ホテル+オンライン　【演習(第1回)】オンラインのみ
参加者：【勉強会(第15回)】17組織28名　　【演習(第1回)】16組織25名
概要：　【勉強会(第15回)】インシデントハンドリングを体験するグループワーク
　　【演習(第1回)】東京大会本番を想定した実践的な演習

・自己学習用コンテンツ提供

期間：2020年９月～12月
対象：100組織250名程度
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）
対象：100組織250名程度
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）



自己学習コンテンツの例

表：過去勉強会及び演習一覧

取組回		開催時期		勉強会開催テーマ
勉強会	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年度	11月	インシデントハンドリング模擬演習（体験）
演習	第１回		２月	インシデントハンドリング模擬演習（実践）

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

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

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

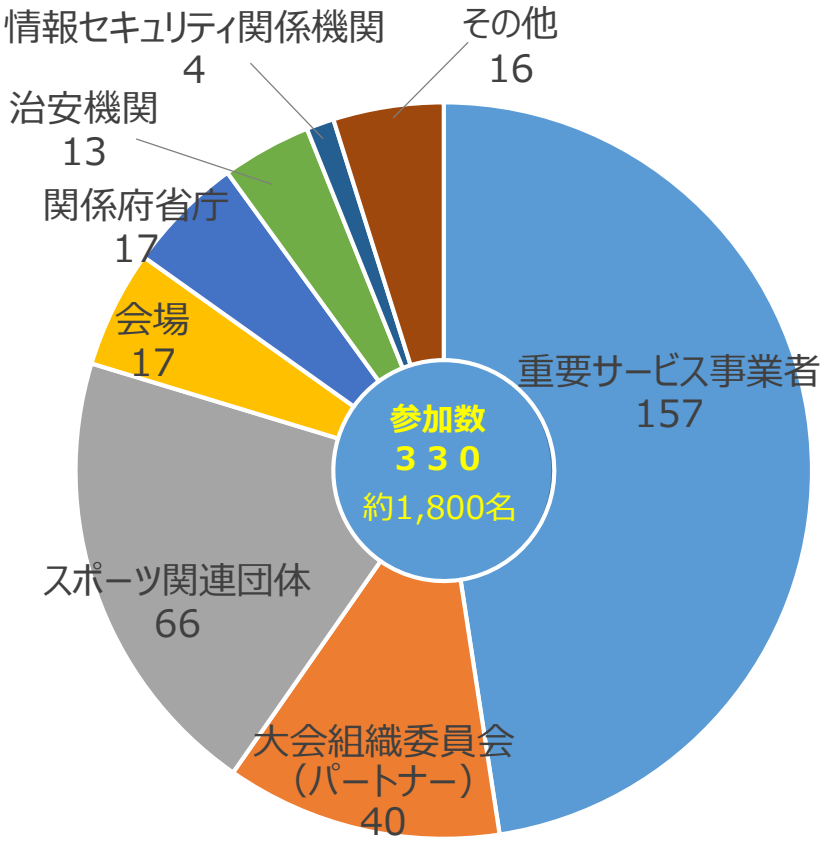
情報提供・共有の対象

◆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

対処体制（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、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、オリパラ事務局を含む。）

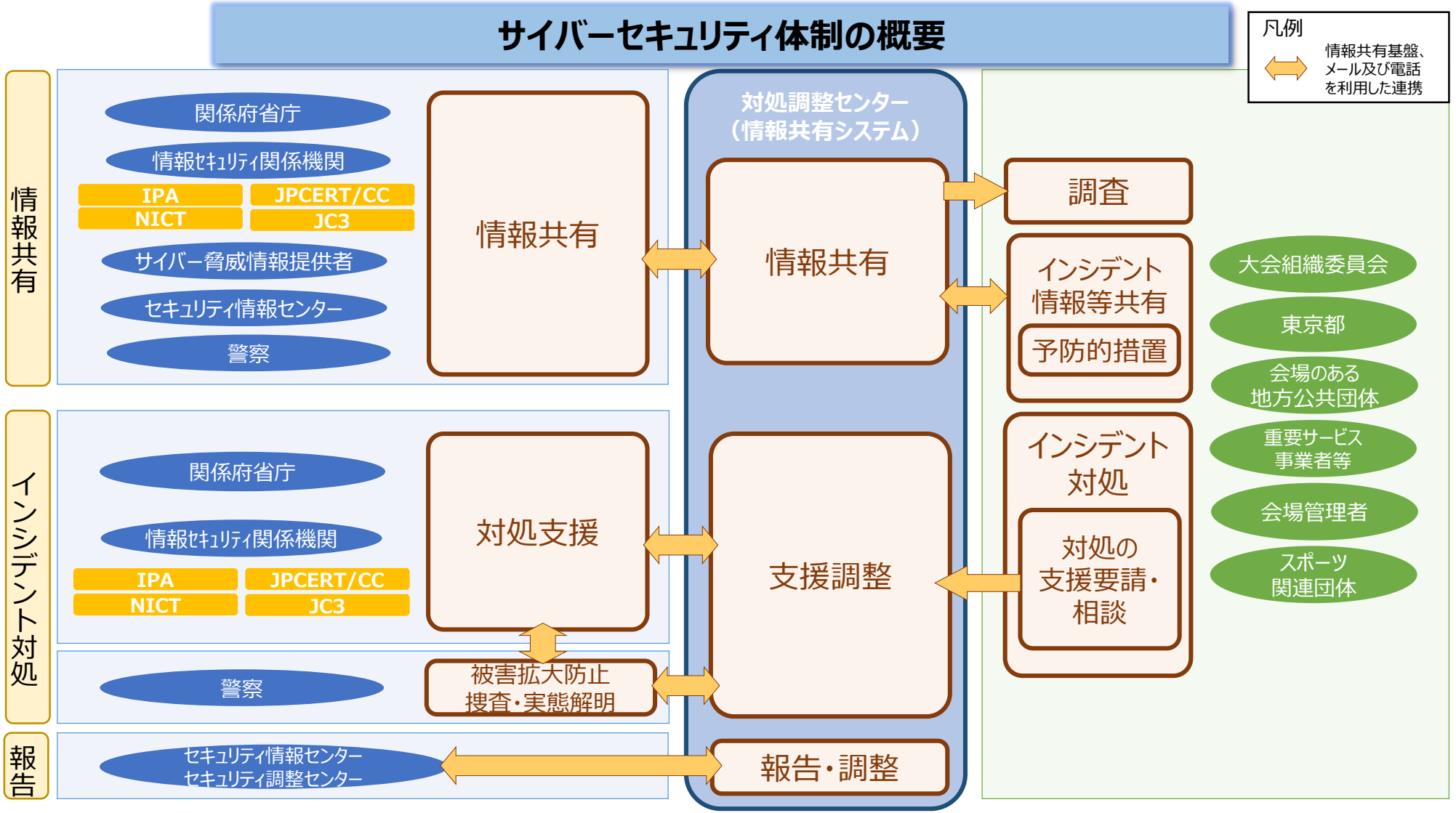
対処支援調整の対象（関係機関等）

- ◆ 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

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組を実施。本体制の概要は下図のとおり。



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、これらの情報を大会組織委員会をはじ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

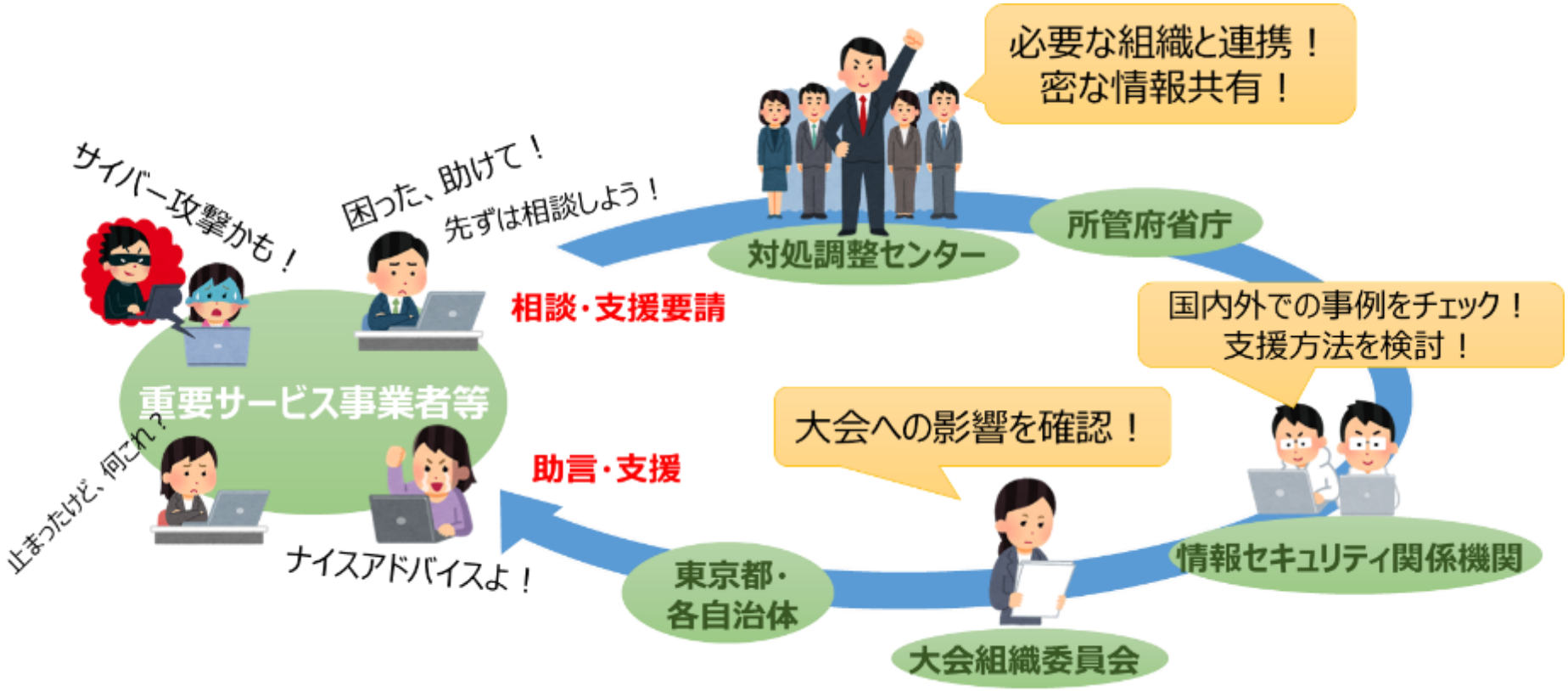
- ✓ 情報共有システム（JISP）、電話及びメールによる連絡体制を確立
- ✓ 原則、情報共有システム（JISP）を用いて連絡（必要に応じて電話又はメールを併用）
- ✓ 大会期間中は、24時間連絡が可能となる窓口を設置

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。

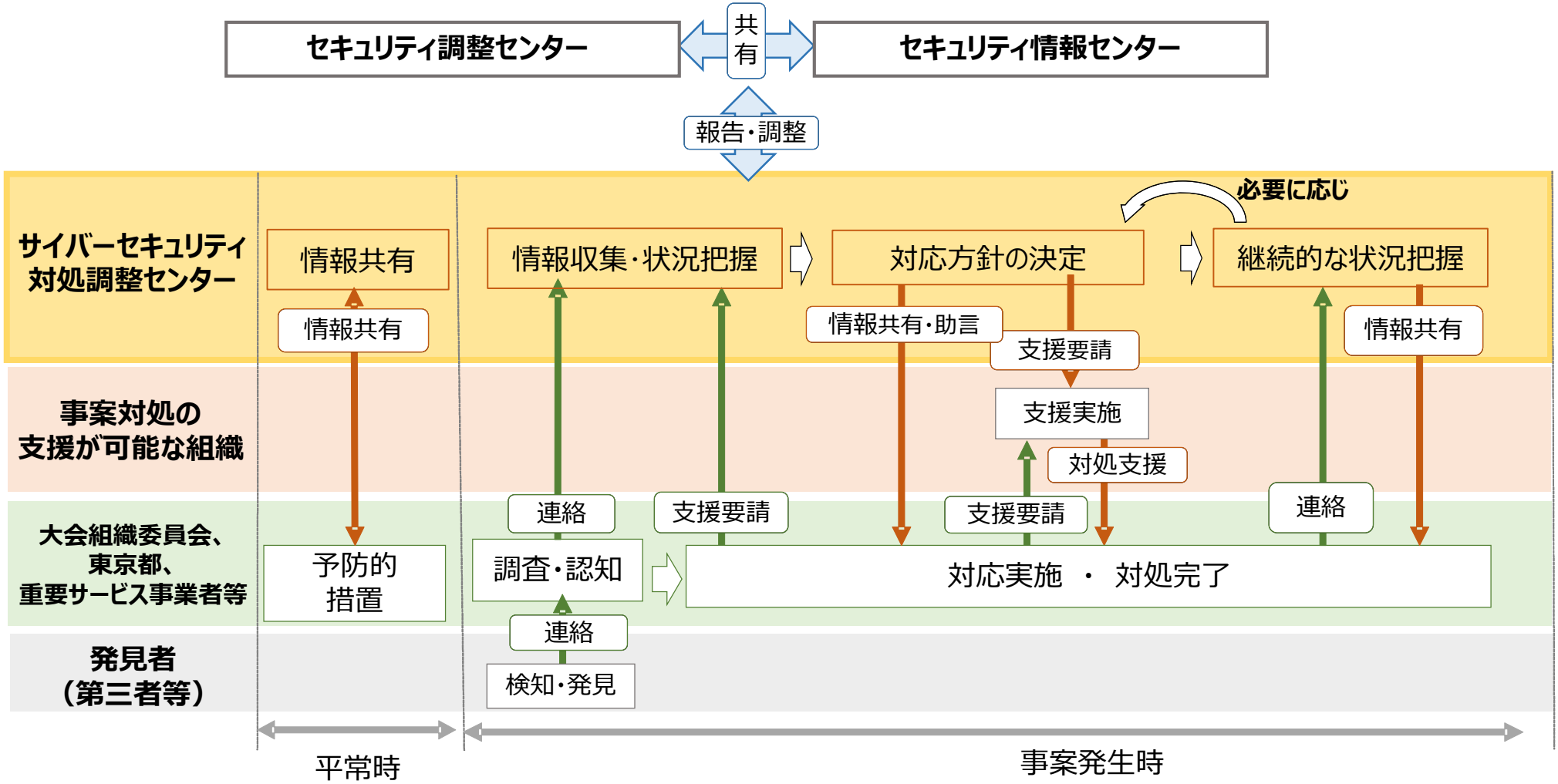
【サイバーセキュリティ対処調整センターの仕組み等の活用による特徴】

- 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



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。



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では、重要サービス事業者等が対処調整センターの提供する「そうだんの窓口」等の機能を十分に理解して非常時に活用できるようにし、また、対処調整センターの体制や運用の適切性の不断の検証するために、事案発生時を想定して、運用手順書に沿って関係機関間で情報連携等のシュミレーションをする「一斉演習」の取組を実施。

カテゴリ		令和元年度		令和二年度		令和三年度
		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
一斉演習	開催日	1)令和元年10月18日 2)令和元年10月31日 3)令和元年11月28日	1)令和2年1月31日 2)令和2年2月6日	1)令和2年8月5日 2)令和2年8月6日	1)令和3年1月20日 2)令和3年1月26日	1)令和3年6月8日 2)令和3年6月10日
	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	連携手順の練度向上 ・情報連絡タイミング、速度 ・対処支援調整の連携	・情報連絡の最終確認（FAとの連携含む。） ・大会成功に向けた意識醸成
	訓練内容	・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)によるサイバー攻撃への未然対処・事案対処	・運用手順の最終確認 ・基本的な情報連携の運用手順を体系化→体制の確立
意見交換会	開催日	－	－	令和2年9月2日	令和3年2月18日	令和3年7月2日
	内容	－	－	・参加組織グループワーク ・有識者講演 JPCERT/CC,シスコシステムズ	・参加組織グループワーク ・有識者講演 IPA,トレンドマイクロ	・参加組織グループワーク ・関係者講演 NISC、オリパラ事務局

サイバーインシデント対応演習等（演習の内容）

【一斉演習のシナリオ（第5回一斉演習の例）】

	想定日時	状況付与（演習シナリオ）
第一部	2021 7/27 (火) 13:30 ～	• 重要サービス事業者において、重要サービス提供システムで不具合の発生が発覚。職員が状況を調査したところ、当該システムで使用するファイルが暗号化されていることが判明。
		• 対処調整センターから、多数の組織でランサムウェアと想定される不正プログラムが起因のシステム不具合が発生している旨を情報共有。
		• 重要サービス事業者職員数人の端末で、重要サービス提供システムで感染したものと同じ不正プログラムが保存されていることが確認。
		• 対処調整センターから、複数の重要サービス事業者のオフィスネットワーク環境下において不正プログラムが確認された旨について注意喚起。
第二部	2021 7/28 (水) 14:40 ～	• 自職場職員が、自組織の情報が漏えいしている可能性を示唆するSNSの投稿を発見。
		• 重要サービス事業者において、情報漏えいのSNS投稿を確認した顧客やメディアからの問い合わせが発生。
		• 対処調整センターから、不正プログラムには情報を窃取する機能も組み込まれていたことが判明した旨を情報共有。
		• 不正プログラムが保存されていた端末において、外部と通信を取っていたことが発覚。外部公表を含めた対応について検討。

【一斉演習後の意見交換会（第5回一斉演習後の意見交換会の例）】

１．目的

- 関係組織間で大会に向けた課題や演習を通じた気づき等を話し合う意見交換会を開催し、情報共有体制の運用の改善につなげる。

２．開催日程

- 2021年7月2日(金)　13:00~16:20

３．実施内容

- 講演
  - ✓講演①「東京大会に向けたNISCの取組み及び大会前最後の確認」
    （内閣サイバーセキュリティセンター 東京2020グループ）
  - ✓講演②「２０２０年東京大会開催にあたって」
    （東京オリンピック・パラリンピック推進本部事務局）
- 第5回一斉演習の振り返り
- 関係組織間での意見交換

４．意見交換のテーマ

- 大会まで残り3週間、最後に改めて確認したいこと

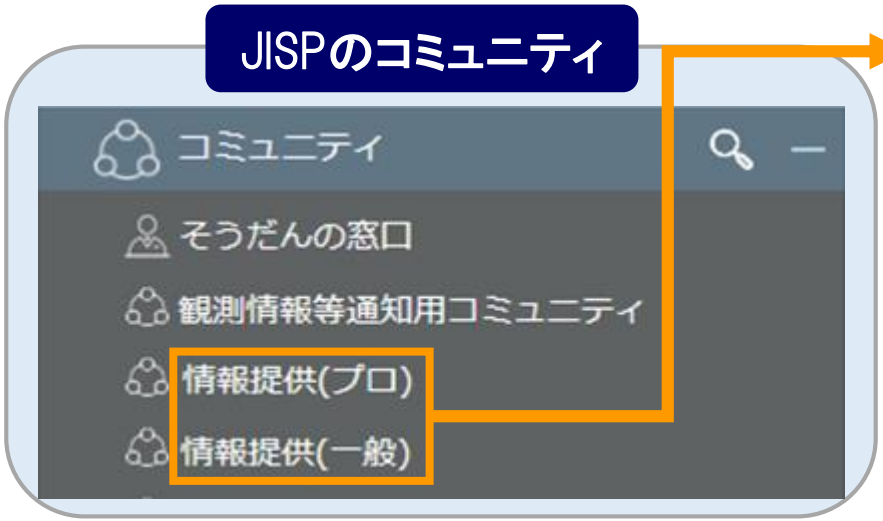
  （具体的な議論例）
  - ✓自組織で実施して短期間で効果があった対応
  - ✓特別な体制を組んでいる等の共有

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

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）

※ 2021年9月末時点



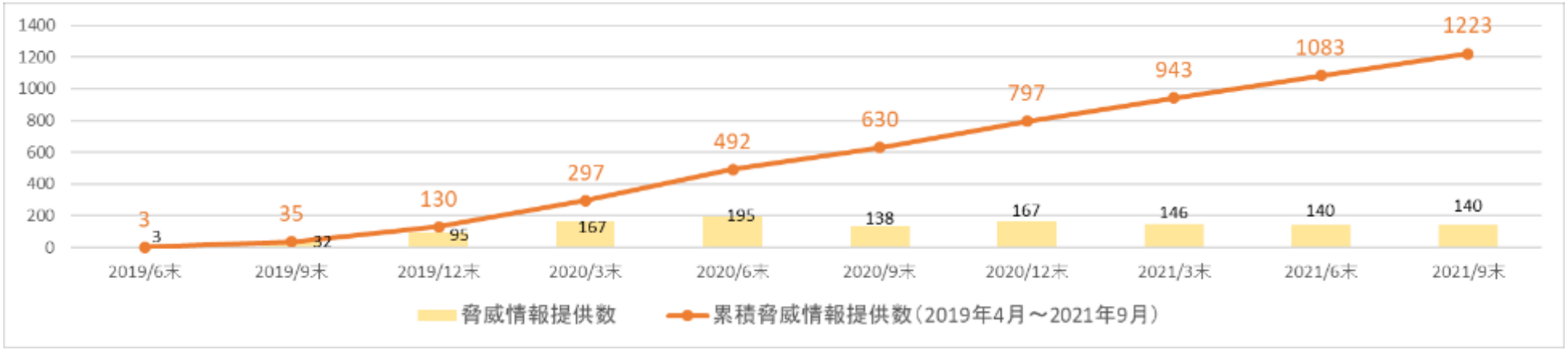
情報提供（プロ/一般）コミュニティ

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

対処対処調整センターからの脅威情報発信件数(2019年4月～2021年9月)

※3か月単位の提供件数と累計提供件数を集計



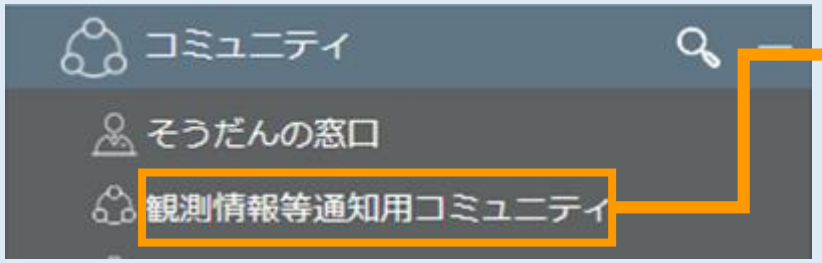
トピックタイトルに【重要】【注意】のタグ付け

【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

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）

※ 2021年9月末時点

JISPのコミュニティ



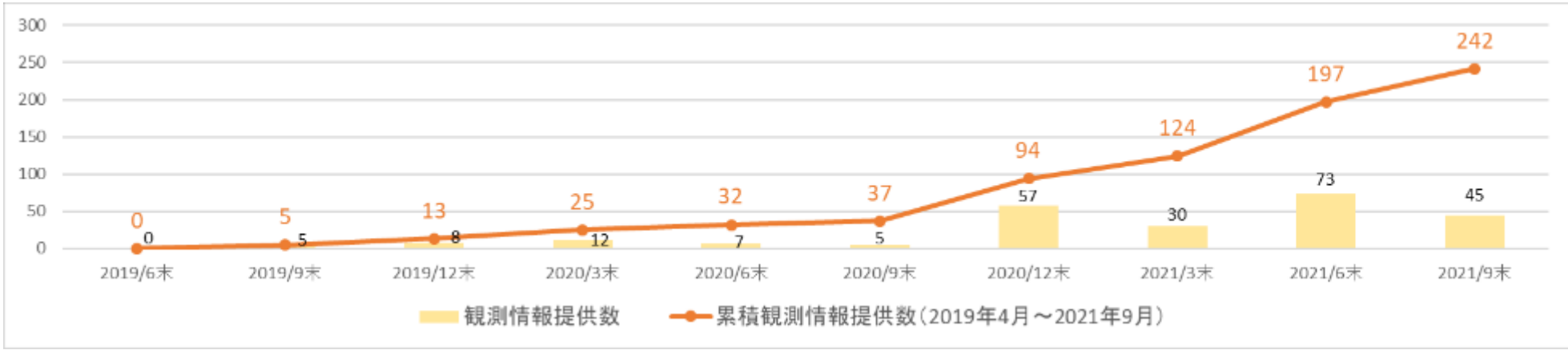
観測情報等通知用コミュニティ

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。

対処対処調整センターからの観測情報通知件数(2019年4月～2021年9月)

※3か月単位の提供件数と累計提供件数を集計

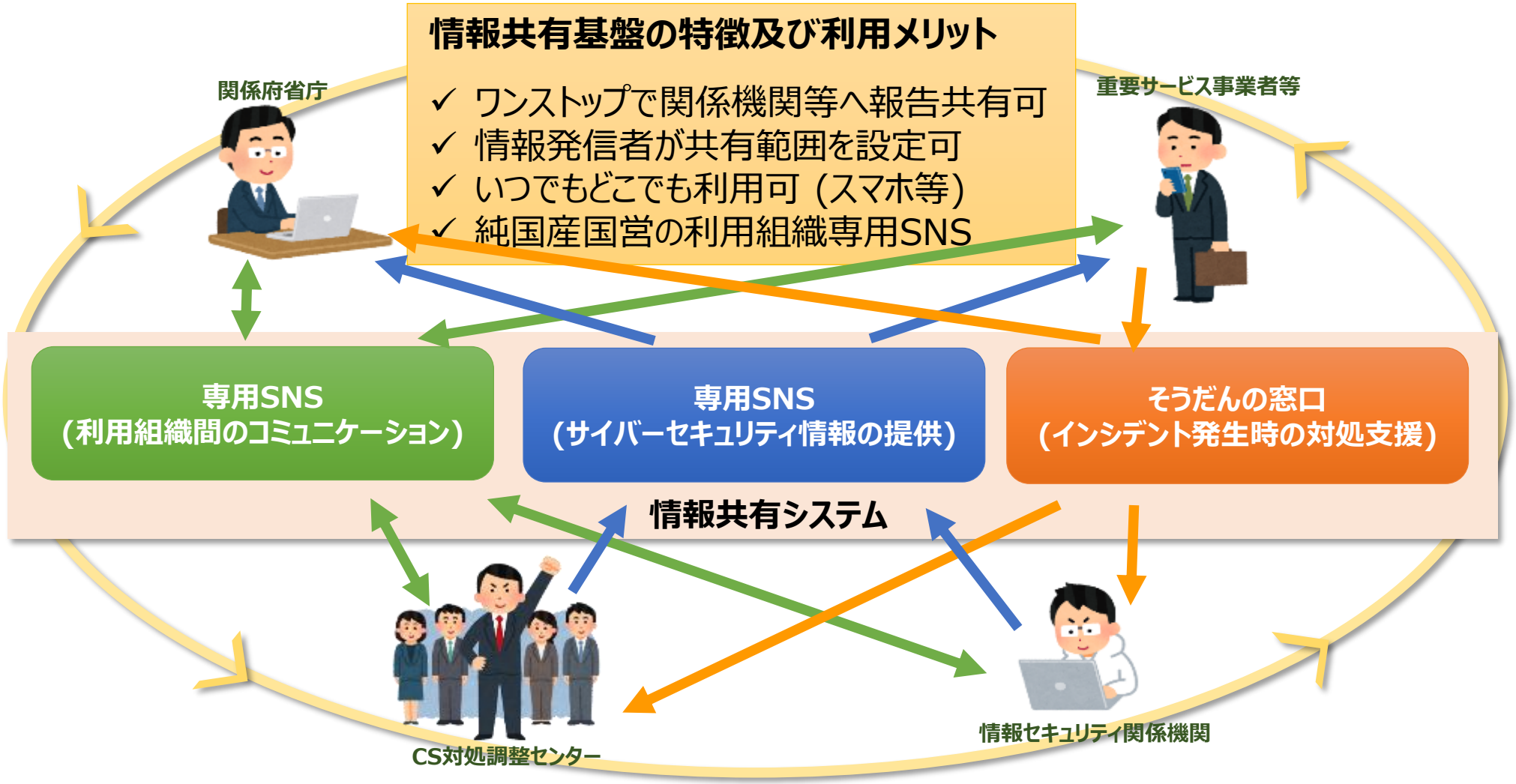


通知した観測情報の例

・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

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。



※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。

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）

➢ 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

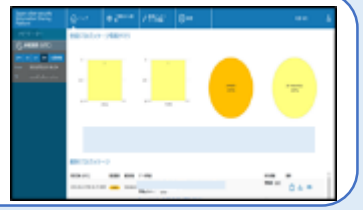
演習システム

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

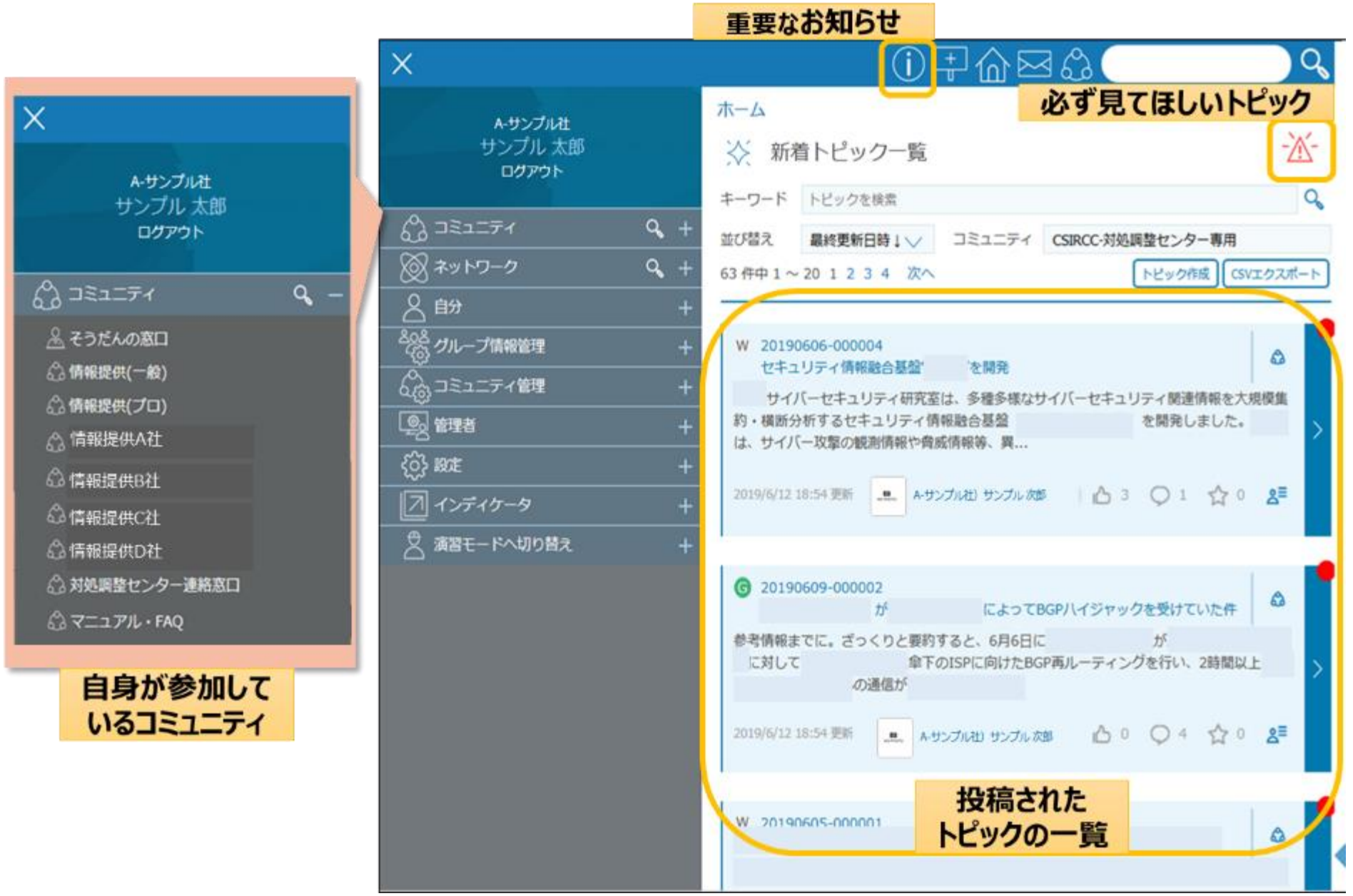
インディケータ情報システム

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



※予兆・ヒヤリハット・疑い含む。

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）の画面）



情報共有プラットフォーム（JISP）の提供（投稿された情報の閲覧方法等）

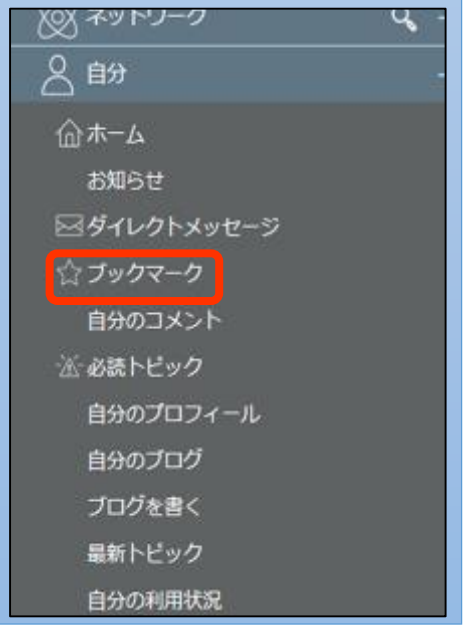
- 記事一覧より見たい情報をクリックすると詳細を閲覧可能

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

東京大会に向けて推進した取組等

		取組の実施手順・ノウハウ	システム、ツール	人材	対象組織との関係構築
リスクマネジメントの促進	リスクアセスメント	○ 関係組織において実施するリスクアセスメントのガイドライン等 ○ NISCによるフィードバックレポートの作成	—	【NISC】 ○ 国家公務員（他省庁等からの出向者）、民間事業者からの派遣職員が能力向上 【重要サービス事業者等】 ○ リスクアセスメント等に従事する職員が能力向上	○ 重要サービス事業者等 約300組織
	横断的リスク評価	○ NISCが実施するリスクアセスメントの手順等（リスクシナリオ検証、チェックリスト検証） ○ NISCによるフィードバックレポートの作成	—	【NISC】 ○ 国家公務員（他省庁等からの出向者）、民間事業者からの派遣職員が能力向上	【リスクシナリオ検証】 ○ 選定した重要サービス事業者等 ○ 大会組織委員会 【チェックリスト検証】 ○ 競技会場等
	スポーツ関係団体に対する勉強会	○ 勉強会、演習、自己学習のコンテンツ ○ セキュリティ関係情報の発信・共有 ○ webサイトに対する簡易チェック	—	【NISC】 ○ 国家公務員（他省庁等からの出向者）、民間事業者からの派遣職員が能力向上 【スポーツ関係団体】 ○ セキュリティ対策等に従事する職員が能力向上	○ 東京大会に関係するスポーツ関係団体等
対処態勢の整備	対処支援調整	○ 関係組織からの支援要請、相談への対応手順等(運用要領、運用手順書等) 〇 関係組織向け説明会のコンテンツ	（○ JISP（そうだんの窓口）） （〇 JIRA（センター内インシデント管理））	【NISC】 ○ 国家公務員（他省庁等からの出向者）、民間事業者からの派遣職員が能力向上	○ 重要サービス事業者等、大会関係組織、情報セキュリティ関係機関、セプター、スポーツ関係団体、関係省庁等 約360組織
	サイバー攻撃への対処能力の向上	○ 演習説明会、演習のコンテンツ、結果レポート ○ 意見交換会のコンテンツ、結果レポート	（○ JISP（演習環境）） （〇 オンライン会議ツール）	【NISC】 ○ 国家公務員（他省庁等からの出向者）、民間事業者からの派遣職員が能力向上 【重要サービス事業者等】 ○ 事案対処等に従事する職員が能力向上	
	予防・検知に関する情報の発信・共有	○ 脅威情報の収集・発信・共有に係る対応手順等（運用手順書等） ○ 観測情報の管理・発信・共有に係る対応手順等（運用手順書等）	（○ JISP（情報提供(一般・プロ)、観測情報提供、インディケータ情報(STIX/TAXII)等））	【NISC】 ○ 国家公務員（他省庁等からの出向者）、民間事業者からの派遣職員が能力向上	
	情報共有プラットフォーム（JISP）の提供	○ システムの利用・運用に係る手順等（利用手順・運用手順書等） ○ 体制参加・システムの利用に係る文書(申込書・規約等)	○ JISP（情報共有のプラットフォーム） 〇 JIRA（センター内インシデント管理） 〇 その他（Web会議ツール、通信機器等） ※ 以上全て、NISCにおいて整備・運用（2023年度以降は更新等の必要あり）	【NISC】 ○ 国家公務員（他省庁等からの出向者）、民間事業者からの派遣職員が能力向上	

２　大会期間中における活動結果等

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）

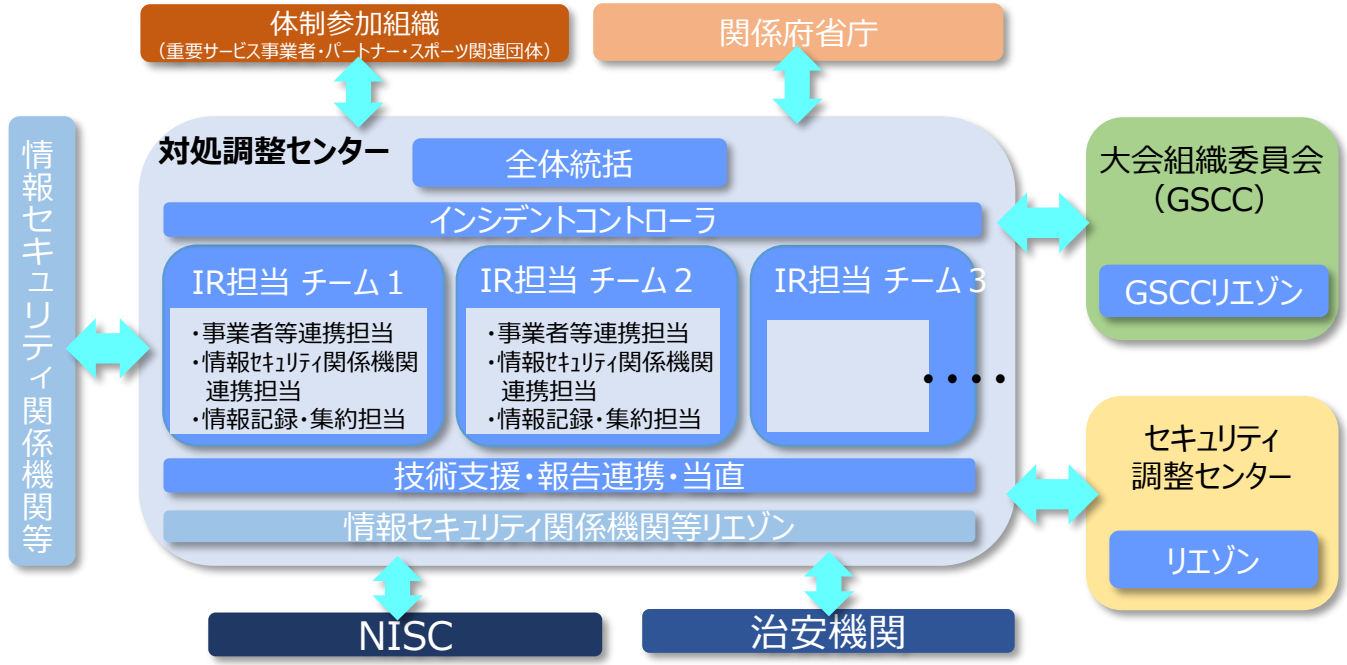
第1回	大会に向けた様々な課題 他	2020/09
第2回	大会を狙った攻撃への対策 他	2021/02
第3回	大会直前に改めて確認すべきこと	2021/07

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



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。

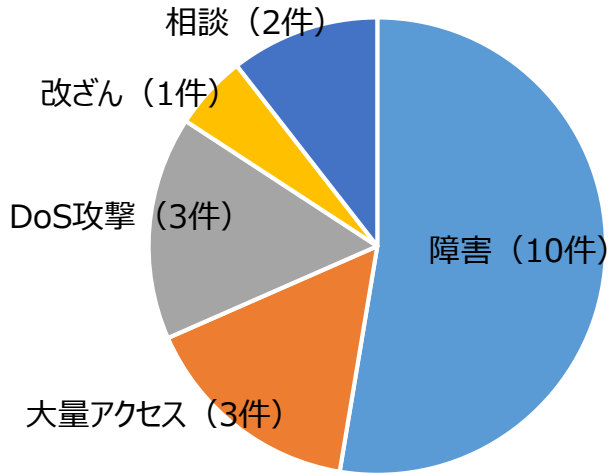
【対応件数】
体制参加組織から提供された情報は、全19件。うち、7件をセキュリティ調整センターへ報告。

【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）

観測情報・脅威情報の提供

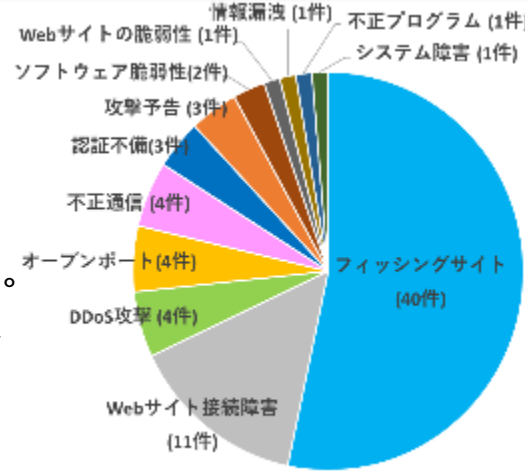
【活動概況】
- ◆ 情報セキュリティ関係機関等の協力のもと、東京大会関連システム等の観測を行い、通常時と異なる観測結果や攻撃予見情報を検出した場合は、対処調整センターより該当する組織へ個別に情報提供。
- ◆ フィッシングサイトや、攻撃者グループによる攻撃キャンペーン情報等の検知のためダークウェブ調査を実施。
- ◆ 対処調整センターが収集した大会のサイバーセキュリティに係る脅威情報を体制参加組織に対して提供。
- ◆ 大会へ悪影響を及ぼす可能性を念頭に主な攻撃者グループを選定調査し、攻撃手法の分析と注意喚起を実施。

【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。

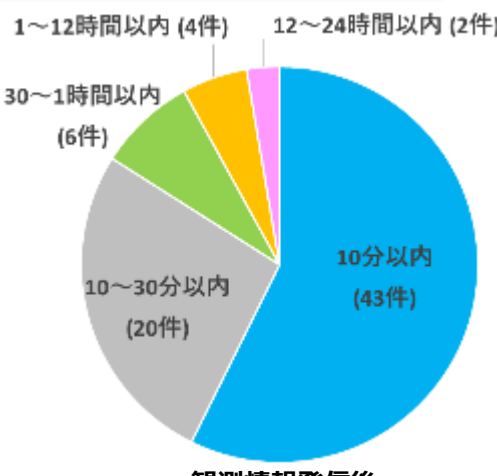
【主な活動】

◆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

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)

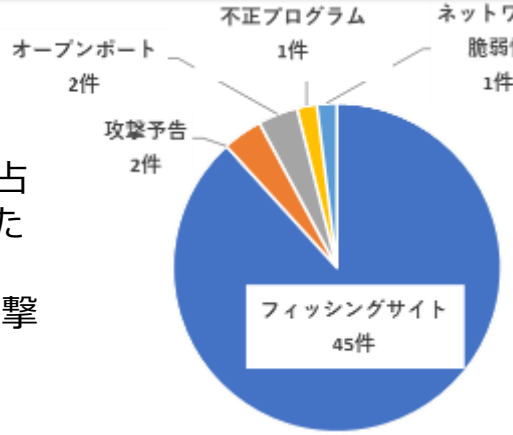
【活動概況】
- ◆ 大会関係組織に関連するドメイン・キーワードを対象に、大会関係組織を狙ったサイバー攻撃、ネットワーク脆弱性、漏洩情報、不正サイト情報等について調査を行い、大会を安全かつ継続的に開催しきるために必要となる対応を実施。
- ◆ 「大会開催に反対する活動」や「大会関連の攻撃による被害報告を装った不正プログラム」、「大会観戦者を狙ったフィッシングサイト」等の緊急性の高い脅威情報が確認されたため、関係組織へ通知。

【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。

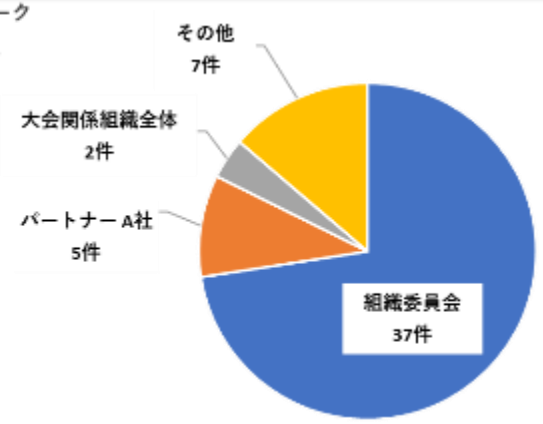
【主な活動】

◆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。

◆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。



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）

サイト接続後に案内される不正なアカウント登録画面

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。

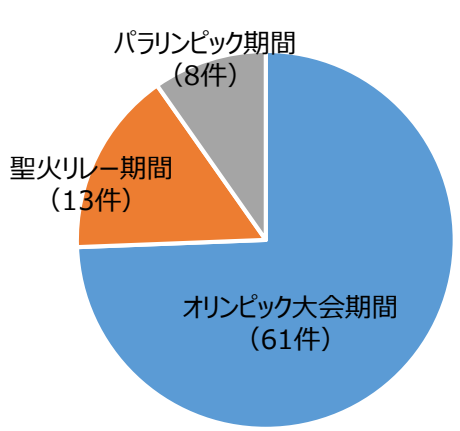
【件数】
- ◆ オリンピック大会期間に61件、パラリンピック聖火リレー期間に13件、パラリンピック大会期間に8件の情報を検知した。
- ◆ 不正通信、DDoS、Webサイト閲覧障害、フィッシングで全体検知数の約80%を占めた。

【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。

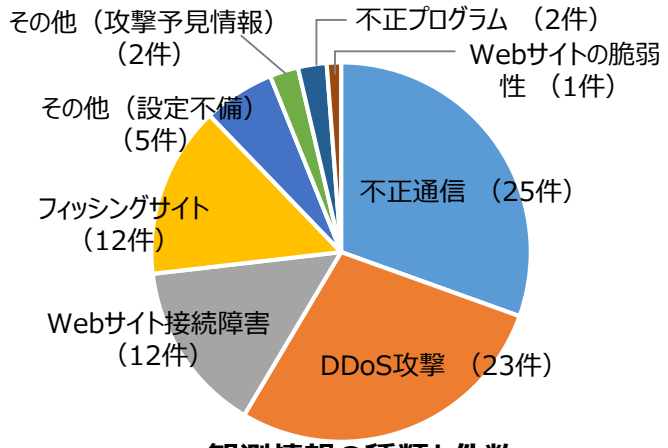
◆システムの観測
- ・Webサイトの脆弱性関連情報の提供
- ・Webサイトの生死監視
- ・DDoS攻撃の監視
- ・不正通信の監視
- ・ダークウェブ上での攻撃予告等の監視
- ・フィッシングサイト等の監視
- ・大会関連で気づいた情報の提供　等

◆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

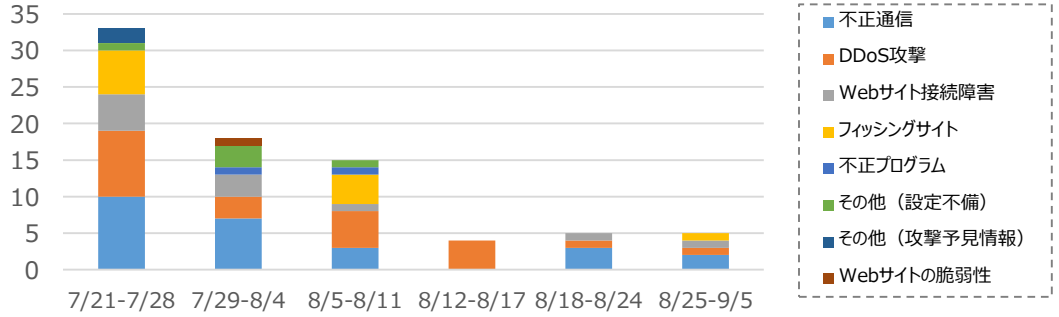
◆大会期間中の観測による検知数（7月21日～9月5日）



検知件数の総数



観測情報の種類と件数



大会期間中の週間検知数（攻撃分類単位）

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】

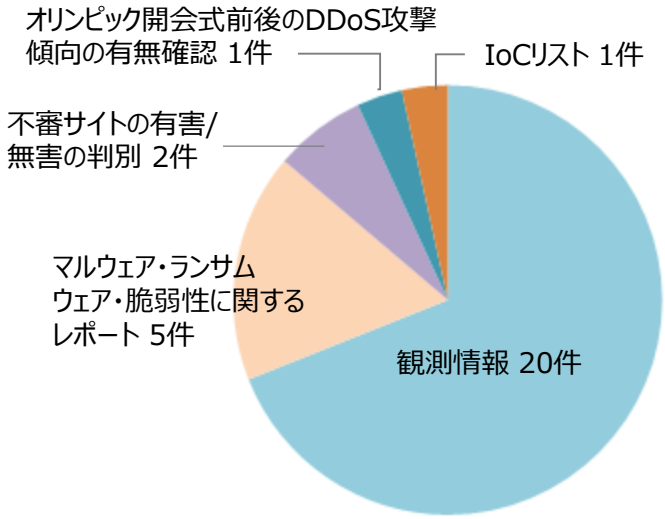
◆大会期間中のCTI事業者からの情報提供は29件
（対処調整センターからの相談に対する応答を含む）

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

◆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。

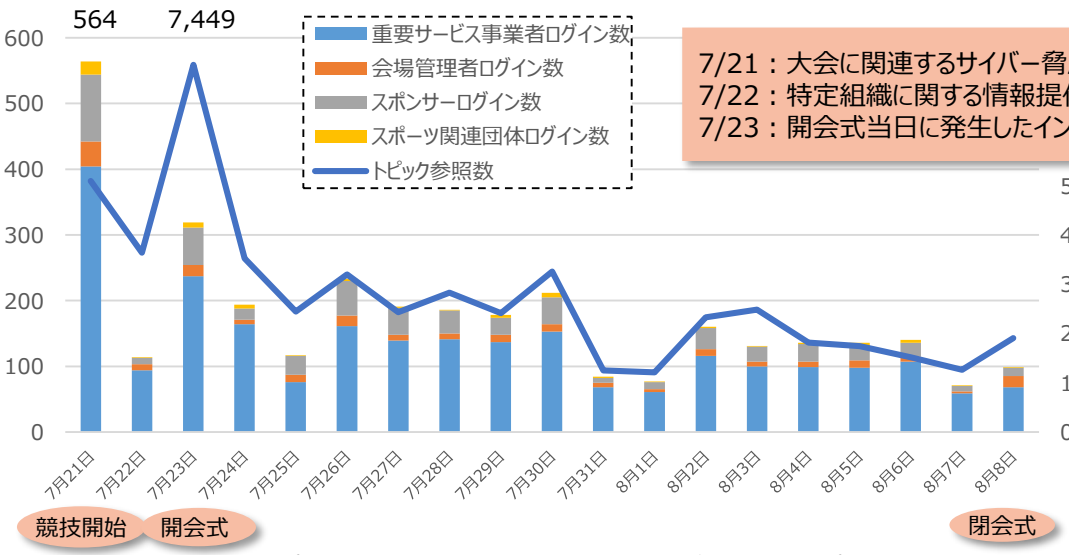


大会期間における情報提供(種別)
（7月21日～9月5日）

情報共有状況(JISP利用状況)

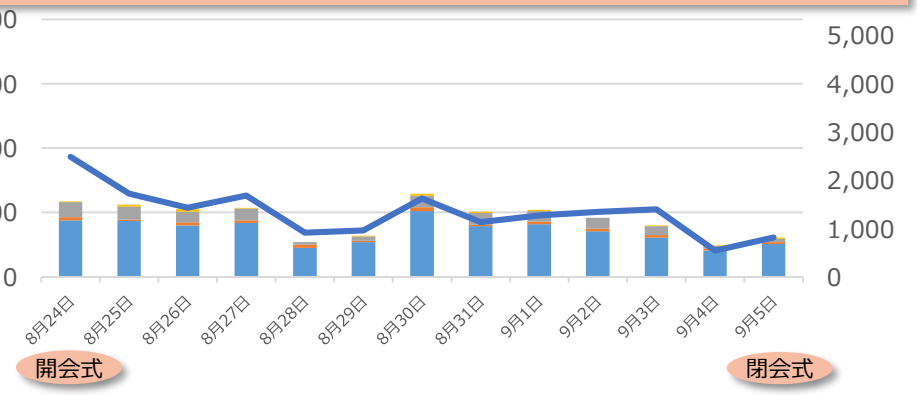
【活動概況】
2019年４月から関係組織がワンストップで情報共有できるプラットフォームとしてJISPを運用してきた。大会中には、大会に関連する情報・大会独自の情報が共有され、平時の1.5倍のログイン、2.5倍のトピック閲覧があった。オリンピック競技開始日(7/21) ～開会式(7/23)において最も活発に利用された。

【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



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

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：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

3　諸外国の取組

（※*NISC*の委託を受けたエヌ・ティ・ティ・コミュニケーションズ株式会社が調査しとりまとめたものです。）

London2012大会後の英国の施策 –NCSC設立–(1/2)

英国のセキュリティ機能集約が必要な背景としては、大会以前から次のような問題が発生。大会の4年後、このCERT-UKやその他の重複する機能を持つ組織が乱立していた状況「Alphabet Soup問題」はNational Cyber Security Centre (NCSC) への機能統合により解消。

解決した課題：

- 「国家サイバーセキュリティ戦略 2016-2021」が出される前の2016年4月、中央政府内に少なくとも12のサイバーセキュリティに関連する組織・チームが存在
- 各々の組織が相互の調整なしに指針を出すため重複や矛盾も生じ、産業界からも政府のどの部署に助言を求めればよいのかわからないと不満が募っていた。

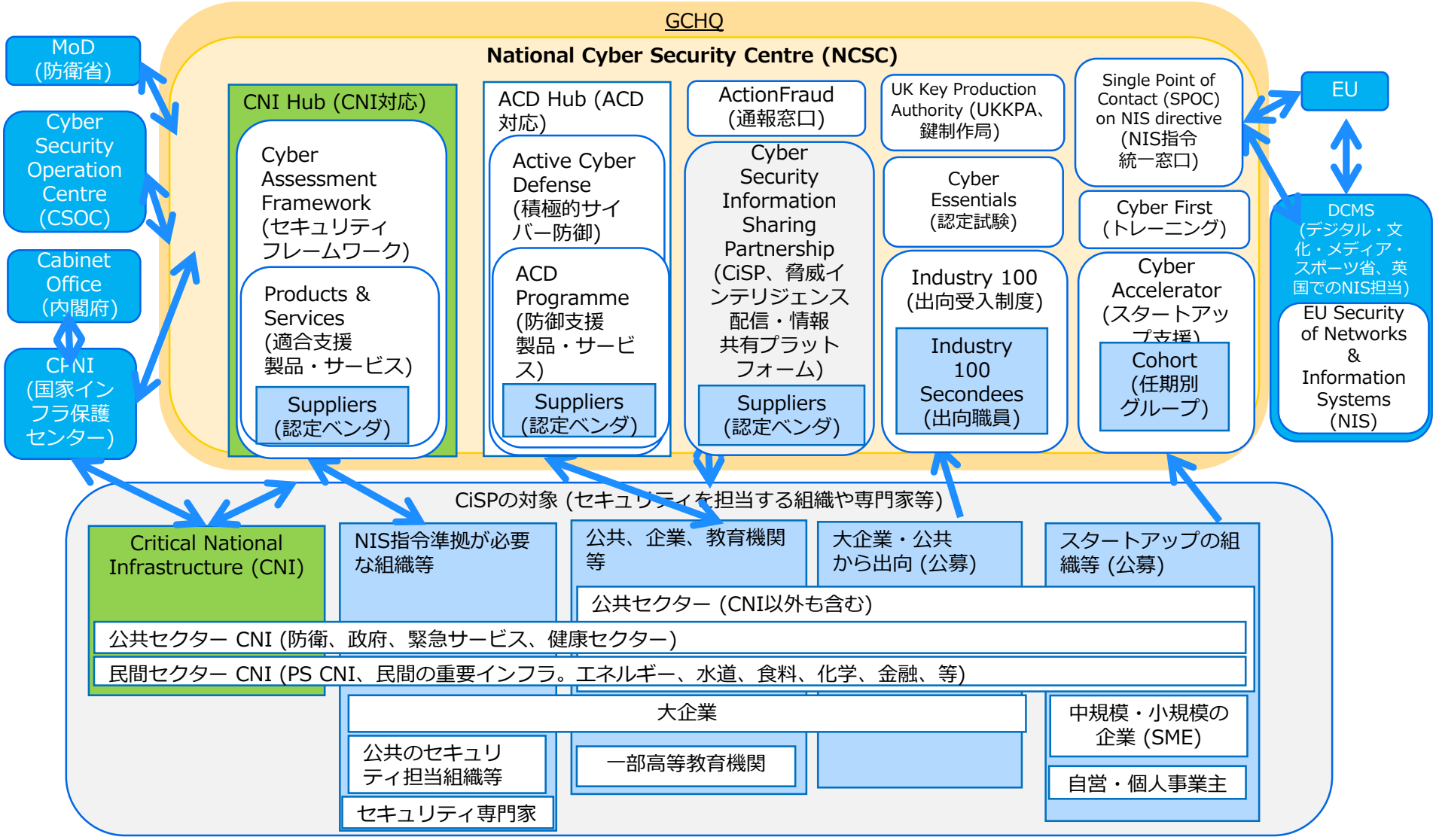
解決策：

- 民間や諸外国と対外的な活動を行う部署の機能を1つに集めて窓口一本化
  (CESG-GCHQ の情報セキュリティ部門、CCA、CERT-UK、CPNIのサイバー関連部門の 4 組織 -> NCSC)
- NCSC (国家サイバーセキュリティ・センター) は GCHQ (政府通信本部) 傘下
  -GCHQ の情報やスキル・経験を活用できる。
  ※ 敵対国による大規模なサイバー攻撃かサイバー犯罪から防御することも NCSCの役目であるが、相手国をサイバー攻撃するような「戦争行為」は国防省（MoD:Minitry of Defence）及び軍のサイバー部隊の仕事と位置づけられている。

https://www.jetro.go.jp/ext_images/_Reports/01/427a23803575001d/20170120.pdf

London2012大会後の英国の施策 –NCSC設立–(2/2)

NCSCは各管轄省庁等と連携しての国家中枢防衛、重要インフラや公共・民間組織に対しての情報提供、実運用の有償・無償サポートを含む包括的な支援を提供



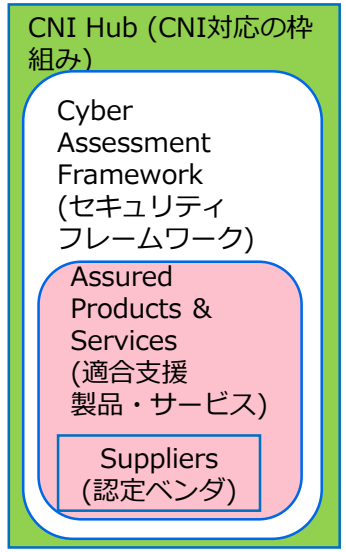
CiSP ： 英国全体で官民連携でのリアルタイムでの脅威情報共有を推進する取組（ Cyber Security Information Sharing Partnership の略）

London2012大会後の英国の主な施策 –ｾｷｭﾘﾃｨ運用面の支援– (1/2)

NCSCはCNI (重要な国家インフラ、政府および民間組織) を次の方法でサポート。
ロンドン大会後の動向、例えばペネトレーションテスト等、セキュリティ対策の実運用に対しても認定製品やサービス等で積極的な支援を開始（CNI以外の組織も購入可）。

1. アドバイス、サポート、ガイドの提供
2. 信頼できるグループ内でフォーラムやイベント開催
3. 支援サービス提供 (CAF準拠支援、インシデントレスポンス)
4. 産業内コラボレーション推進 (Industry 100での出向制度)
5. 政府でのCNI向けセキュリティ政策検討時のアドバイスや支援
6. 脅威インテリジェンスの提供 (CiSP経由、または対象組織への直接提供)
7. 政府での新しいICT環境向けセキュリティ政策検討時のアドバイスや支援
8. MSPなどのCNIに重要なサービスを提供する組織に対しての支援

（実運用に対しての積極的な支援）
セキュリティ運用支援の各種製品・サービスやベンダーにつき、基準に基づいた検証・認定の上で、公式に有償提供を仲介。CAF適合支援の枠組みで提供される製品・サービス数は200以上に上り、ペネトレーションテスト (47件)、業務向け製品セキュリティ (43件)、セキュリティコンサル (28件)、インシデントレスポンス (9件)、トレーニング (2件) 等が含まれる。



https://www.ncsc.gov.uk/section/private-sector-cni/cni#section_5
https://www.ncsc.gov.uk/section/products-services/all-products-services-categories

London2012大会後の英国の主な施策 –ｾｷｭﾘﾃｨ運用面の支援– (2/2)

CNI以外の非重要インフラに対しても、大会後の「国家サイバーセキュリティ戦略 2016-2021」からの英国全体でセキュリティを飛躍的に向上させるための取組として、Active Cyber Defense (積極的サイバー防御) の枠組みが存在。フィッシング、メールフィルタリング等の多くの攻撃により発生する大部分の弊害から保護することを目的に、基本的な対策を実施するもの。次のサービスが認定ベンダまたはNCSCにより提供されている。

1.Protective Domain Name Service (DNSフィルタリング、公共セクター向け)
2.Web Check　(Webチェック、公共セクター・大学以上の高等教育機関向け)
3.Mail Check　(メールチェック、公共セクター・大学以上の高等教育機関向け)
4.Host Based Capability (エージェントセキュリティ、中央政府向け)
5.Logging Made Easy (ログイン管理製品、Windows向け、対象不問)
6.Vulnerability Disclosure
　-Vulnerability Reporting Service (脆弱性通報システム、対象不問)
　-Vulnerability Disclosure Pilot (脆弱性検出・トリアージ、中央政府向け)
　-Vulnerability Disclosure Toolkit (脆弱性検出・報告用ツール、対象不問)
7.Exercise in a Box (インシデント対応シナリオによる訓練、対象不問)
8.Suspicious Email Reporting Service (不審メール報告、対象不問)
9.The NCSC Takedown Service (NCSCによるテイクダウン、公共向け)

https://www.ncsc.gov.uk/section/products-services/active-cyber-defence
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

London2012大会以後の英国の主な施策 –官民連携の情報共有 CiSP–

Cyber Security Information Sharing Partnership (CiSP) は、大会後の2013年から運用を開始。英国全体で官民連携でのリアルタイムでの脅威情報共有を推進。

2015年以降NCSCの管轄に移行され、通信手段等で一定の基準を満たした組織及び所属する個人がCiSPに登録可能で、次の機能を提供。

- 政府や産業界のカウンターパートと、安全な環境で繋がることができる。
- 脅威情報を随時取得可能
- CiSPのフォーラム上で組織間での情報交換や質問などが可能
- 登録組織向けにカスタマイズされたネットワーク監視レポート無償購読

CiSPのサイバー脅威インテリジェンス (Cyber Threat Intelligence) には Open Source Intelligence (OSINT) によるレポートや、政府や産業界による レポートが含まれ、CiSPに所属する組織がインテリジェンスを利用した脅威分析の 初歩として、攻撃者、その攻撃手法等を自ら分析し監視や対策に役立てることが可能

CiSPについては、過去に次の数字の発表あり。
・22のセクターから10,569名登録、20,270点のコンテンツ (2018年時点)
・22のセクターから約5,500組織が加入、15,571名登録 (2019年時点)

Cyber Security Information Sharing Partnership (CiSP、脅威インテリジェンス配信・情報共有プラットフォーム)

Suppliers (認定ベンダ)

https://www.ncsc.gov.uk/section/keep-up-to-date/cisp#section_4
https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Cyber-Threat-Intelligence-A-Guide-For-Decision-Makers-and-Analysts-v2.0.pdf

London2012大会以後の英国の主な施策 –NCSCの活動成果、年推移–

NCSCの直近3年のCiSP、ACD、CNI等各枠組みを総合した対応の規模や推移は次のとおり。資格認定数、CiSP加入者数、インシデント対応数が増加しており、指針発行から事故対応までを把握しつつ統括する機関として実績を重ねている。

種別	2018年	2019年	2020年	成長率 (Growth)
対応したインシデント数	557	658	723	130%
対応した被害組織数	N/A	約900	約1200	133%
対応した脅威の件数	214	154	414	193%
閉鎖したフィッシングサイトの数	138,398	177,335 (62.4%は24h以内に閉鎖)	166,710 (65.3%は24h以内に閉鎖)	120%
CiSP新規加入者数	2,361	5,000	2,953	125%
暗号鍵の提供数 (NCSC内 UK Key Production Authority (UKKPA)経由)	145,000 (クライアント数 200)	108,411 (クライアント数 170)	101,747 (クライアント数 140)	70%
ホームページ訪問数	190万	280万	270万	142%
ガイダンスとブログの発行数	ガイダンス134、ブログ95	ガイダンス34、ブログ69	ガイダンス30、ブログ60	39%
Cyber Essentialsの認定数	8900以上	14,234	17,100	192%
CyberFirst courseの受講者数 (学生)	1,968	2,614	1,770	90%
Cyber Security Awareness等の無償セッションの提供数	1,000以上	2,700以上 (トレーニングイベントを含む)	100以上 (ワークショップ、ポッドキャスト、ウェビナー等)	10%
海外訪問 (受け入れ) 数	54	56	20以上	37%
イベント開催数 (参加者数)	80	197 (参加者数9,000名以上)	101 (参加者数4,602名以上)	126%

https://www.ncsc.gov.uk/annual-review/2018/ncsc/docs/ncsc_2018-annual-review.pdf
https://www.ncsc.gov.uk/annual-review/2019/ncsc/docs/ncsc_2019-annual-review.pdf
https://www.ncsc.gov.uk/files/Annual-Review-2020.pdf
https://www.cbronline.com/feature/punched-tape-ukkpa

London2012大会以後の英国の主な施策 –NCSCの活動成果、2020年–

最新の2020年度では次のような取り組みと成果 (数量) が示されている。
リスクの高いベンダーへの対応や、Covid-19関連等といった新しい対象に対しても迅速で柔軟な対応を行い、一年以内に可視化できる成果に繋げている。

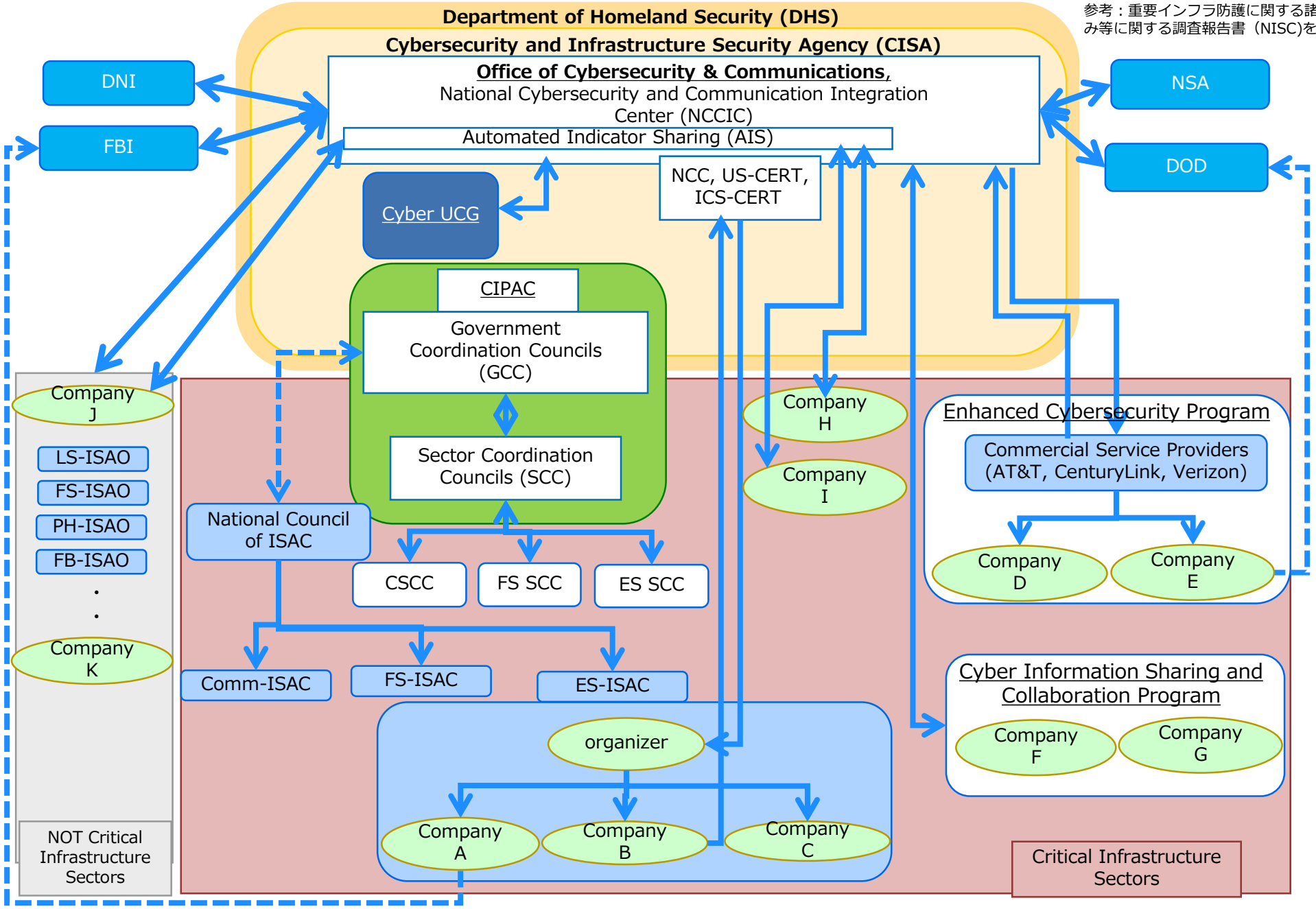
新しい脅威への対応：
- リスクの高いベンダー対応として米国のHuaweiに対する制裁を迅速にレビューし、英国で必要を政府および実務者視点の両面で検討し、速やかに政府に提案
- Covid-19およびリモートワーク関連
  - 125か国で利用されているトレーニングツール「Exercise in a Box」においてリモートワークに関連したコンテンツを追加、新しいリスクを学びとして提供
  - リモートワーク、Covid-19関連攻撃者に関してガイドラインをタイムリーに展開

大規模で情勢にも対応した積極的なサイバー防御 (ACD)：
- 不審メール報告サービスにおいて、2.3億件の不審メールの報告に対応
- 22000件以上の不正URLをCovid-19に関連した詐欺行為で閉鎖 (テイクダウン)
- 200件以上のCovid-19に関連したサイバーインシデントに対応
  - NHSトラストを含む健康セクターに対して支援を提供
  - NHSトラストのIPアドレス1億以上に対して脆弱性スキャンを実施

https://www.ncsc.gov.uk/files/Annual-Review-2020.pdf

米国のサイバーセキュリティに関する情報共有体制

参考：重要インフラ防護に関する諸国の枠組み等に関する調査報告書（NISC)を元に作成

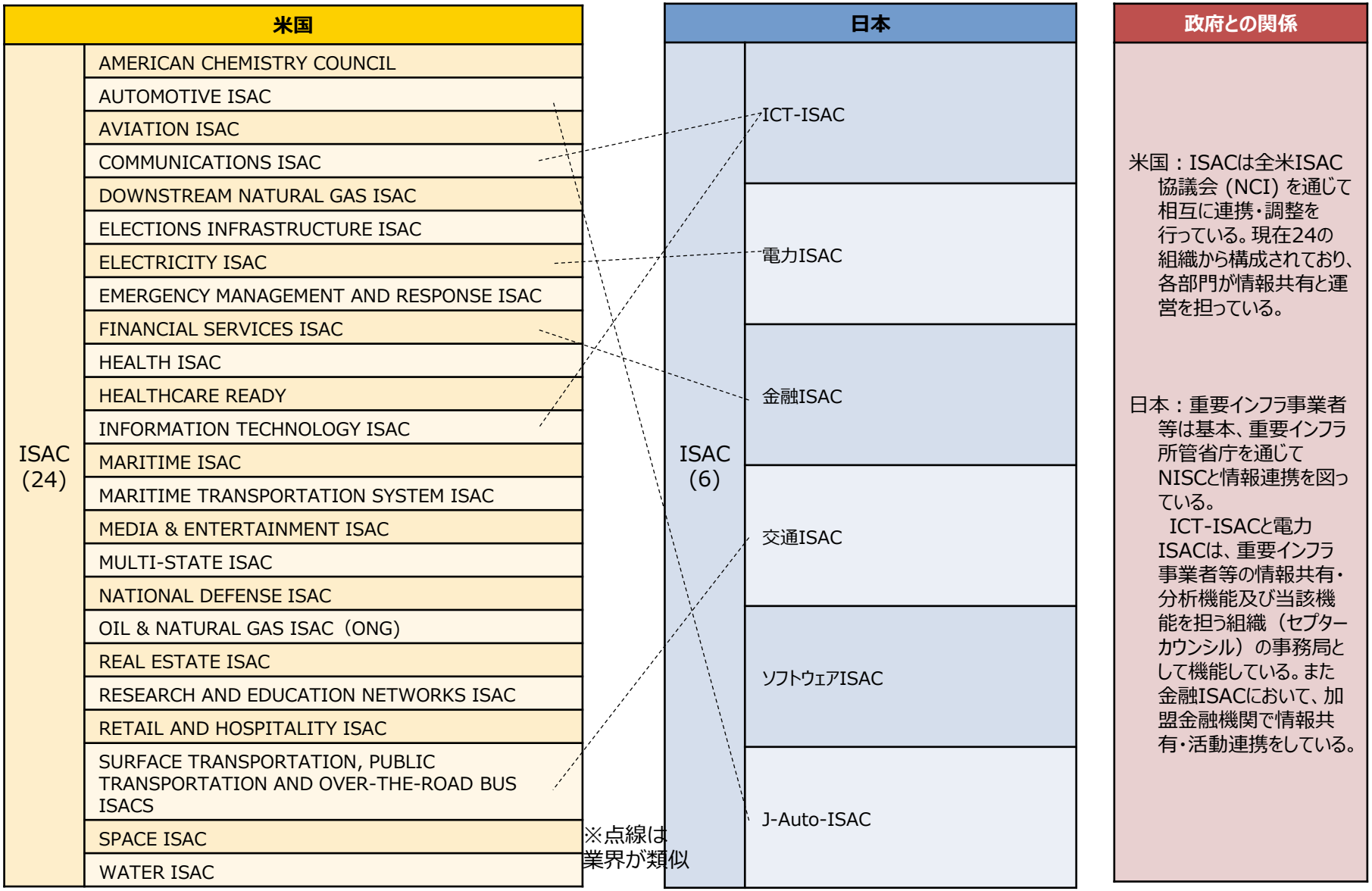


米国の施策等概要

米国		
関係主体	**施策（実施主体）**	**概要**
CISA	政府調整委員会:GCC	国家インフラ防護計画(NIPP)等の政府計画に関する導入、運用、アップデート等についてセクタ毎に検討。
	NCCIC	情報共有の窓口、調整役として位置 24時間365日監視
	Cyber UCG	重大なサイバー攻撃の脅威が発生した場合、関係省庁を統括 平常時はNCCICをサポート
	重要インフラパートナーシップ助言協議会:CIPAC	GCC/SCCの親会 重要インフラ施策等のレビュー
	サイバー情報共有・連携プログラム:CISCP	政府・重要インフラ事業者での脆弱性情報共有枠組み。脅威情報に関する①指標速報、②分析速報、③警報速報、④施策提案を作成し、 関係主体に共有。
	拡大サイバーセキュリティサービス(ECS)プログラム	DHSから認可された商用サービス事業者が、契約先企業に対して脅威情報等を販売 リアルタイムの機械間情報共有を実施。
	インディケータ自動共有(AIS)	連邦政府および民間組織のシステム間で脅威指標共有や随時配信を行う。共有・配信にはSTIXおよびTAXIIの仕様を利用
重要インフラ分野	セクタ調整委員会:SCC	各セクタの行動計画の導入、運用、改訂
	全米ISAC協議会 (NCI)	セクタ間の関係強化や共通の問題等の意見交換
	ISAC	重要インフラを構成する民間の同じ業界の事業者同士で、サイバーセキュリティに関する情報を共有し、サイバー攻撃への防御力を高めることを目指して活動する民間組織 (24 ISAC)
重要インフラ分野以外	ISAO	ISAOはISACと同様にサイバー脅威に関する情報共有と分析を行う組織であるが、ISACが組織されていない分野やISACのメンバーでない民間企業など幅広い分野を対象として情報共有を可能とすることを目的としている

米国と日本のISACの比較

Information Sharing and Analysis Center（ISAC) は、重要インフラを構成する民間の同じ業界の事業者同士で、サイバーセキュリティに関する情報を共有し、サイバー攻撃への防御力を高めることを目指して活動する民間組織である。



米国ISAOの活動状況

Information Sharing and Analysis Organizations（ISAO）は、2013年2月12の大統領令に基づきDHSに設置促進が指示されたものである。

ISAOはISAC と同様にサイバー脅威に関する情報共有と分析を行う組織であるが、ISACが組織されていない分野やISACのメンバーでない民間企業など幅広い分野を対象として情報共有を可能とすることを目的としている。従って、ISACとは異なり、産業分野毎で関連付けられているものではなく、広く産官学の分野や地域等において団体が組織されている。

米国		政府との関係
カテゴリー	代表的なISAO	
地域ISAO (17) 産業・セクターISAO (46) 特定テーマISAO (7) その他ISAO (9)	・Cyber USA 各州に作られた官民パートナーシップ体制の集合体 2016 年10 月に7 組織で結成され、オバマ政権下でサイバーセキュリティ顧問を務めた Howard A.Schmidt 氏らが設立した財団により運営している ・Advanced Cyber Security Center 米国New England の大学・企業・政府機関等21 団体が参加する非営利ISAO（Facebook, RSA, Harvard University, MIT など） 情報共有により、最先端のセキュリティ研究や教育プログラムの作成、セキュリティ政策の作成を遂行する ・The National Cybersecurity Society 社員数499人以下の中小企業を対象とした非営利ISAO これまでISAC の枠組みに入れなかった中小企業に対し、セキュリティ情報の提供や教育を実施している ・Accountability Group 広告代理店の他、広告主や出版社、セキュリティベンダー、政府機関などが業種を超えてデジタル広告の不正排除、マルウェア防止などに取組む ・Global Resilience Federation FS-ISAC（金融）、Energy Analytic Security Exchange（エネルギー）、Legal services ISAO（法務）の3 組織を運営する ISAC・ISAO を束ねるISAO であるという点で特徴的 ・Information Association of Certified ISAOs 情報共有組織の立ち上げ・活動支援を行っている団体 国土安全保障省でISAO の枠組み作成に携わった者が設立したISAO ・The Trustworthy デジタル広告のセキュリティ向上を目的としたISAO	CISAの官民連携による情報共有分析組織であるNCCIC（国家サイバーセキュリティ通信統合センター）を通じて、ISAOとの継続的なコラボレーションを推進し、包括的な調整を行う

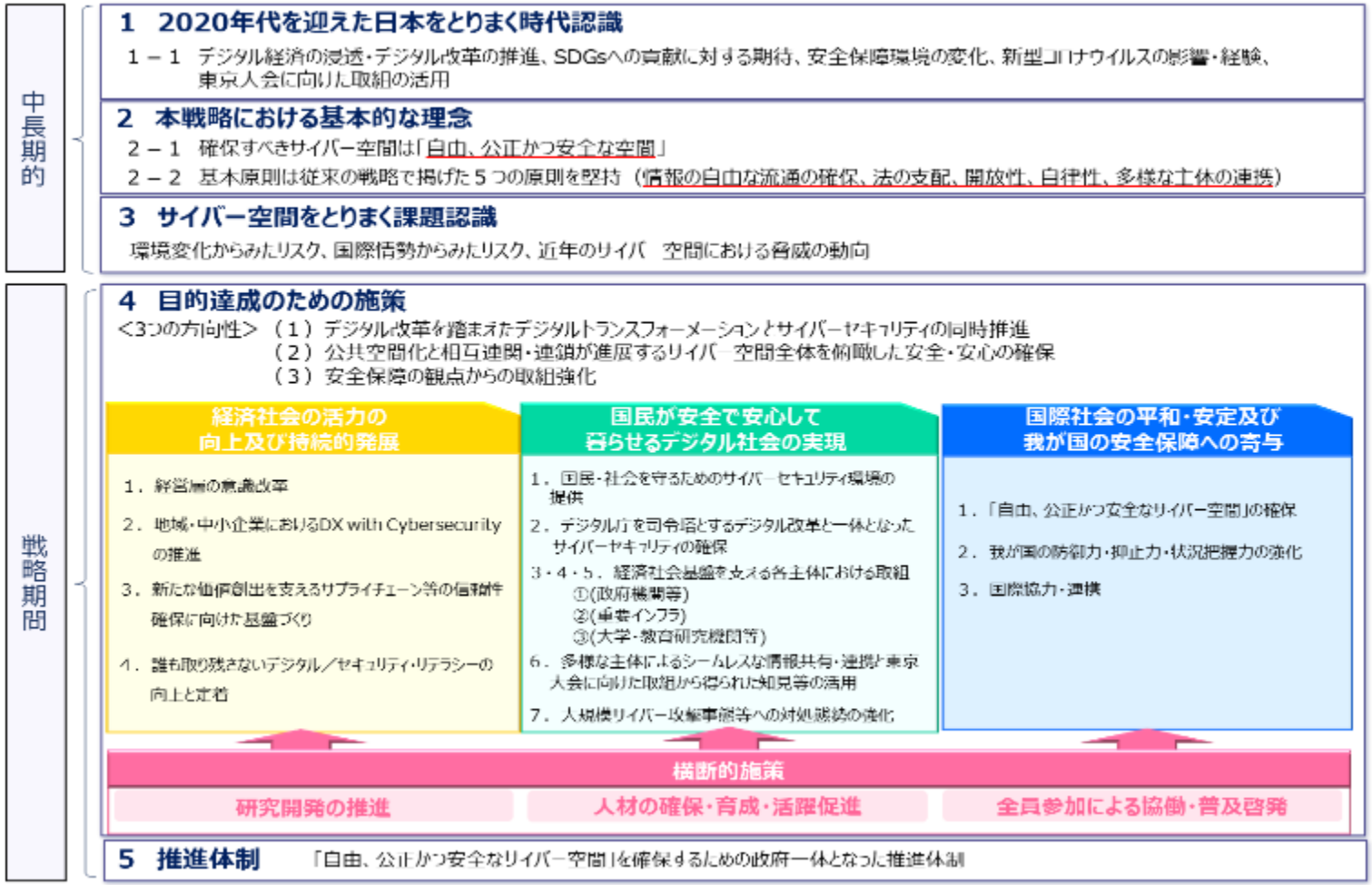
出典:サイバー攻撃に対するセキュリティ情報共有組織(ISAC)の構築に関する調査研究
https://www.jttri.or.jp/pdf/H29cyber_ISAC-houkoku.pdf

４　サイバーセキュリティ戦略（東京大会関係）

新たなサイバーセキュリティ戦略

○　９月28日の閣議において、2020年代初めの今後３年間にとるべき諸施策の目標や実施方針を示すものとして、新たなサイバーセキュリティ戦略を決定。

○　当該戦略では、有識者会議での討議等を踏まえ、東京大会等におけるサイバーセキュリティの確保に向けた取組の活用に当たっての方針・方向性を明記。



新たなサイバーセキュリティ戦略の構成

新たなサイバーセキュリティ戦略の課題と方向性

2020年代を迎えた日本を取り巻く時代認識　：　「ニューノーマル」とデジタル社会の到来

- デジタル経済の浸透、**デジタル改革**の推進
- **新型コロナウイルス**の影響・経験
テレワーク、オンライン教育等の進展
- 厳しさを増す**安全保障**環境
- **SDGｓ**への
デジタル技術の貢献期待
- **東京オリンピック・パラリンピック**に向けた取組

サイバー空間をとりまく課題認識　：　国民全体のサイバー空間への参画

- サイバー空間は、国民全体等**あらゆる主体が参画し公共空間化**
サイバー・フィジカルの垣根を超えた各主体の相互連関・連鎖の深化
攻撃者に狙われ得る弱点にも
- 地政学的緊張を反映
国家間競争の場に
安全保障上の課題にも
- 不適切な利用は
国家分断、人権の阻害へ
- 官民の取組の
活用

あらゆる主体にとってサイバーセキュリティの確保は自らの問題に
５つの基本原則※は堅持

「Cybersecurity for All」
～誰も取り残さないサイバーセキュリティ～

デジタルトランスフォーメーション（DX）とサイバーセキュリティの同時推進

安全保障の観点からの取組強化

公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保

「自由、公正かつ安全なサイバー空間」の確保

※情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携

国民が安全で安心して暮らせるデジタル社会の実現

課題認識と方向性 － 公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心確保 －

- サイバー空間の**公共空間化**、**相互連関・連鎖の深化**、**サイバー攻撃の組織化・洗練化**。

  国は、様々な主体と連携しつつ、①自助・公助による**自律的なリスクマネジメントが講じられる環境づくり**と、②持ち得る手段の全てを活用した**包括的なサイバー防御の展開**等を通じて、**サイバー空間全体を俯瞰した自助・共助・公助による多層的なサイバー防御体制を構築**し、国全体のリスク低減、レジリエンス向上を図る。

主な具体的施策（１）国民・社会を守るためのサイバーセキュリティ環境の提供

① 安全・安心なサイバー空間の利用環境の構築

- サプライチェーン管理のためのガイドライン策定や産業界主導の取組、IoT、5G等の新技術実装に伴う安全確保
- 利用者保護の観点から安全かつ信頼性の高い通信ネットワークを確保するための方策の検討

② 新たなサイバーセキュリティの担い手との協調（クラウドサービスへの対応）

- 政府機関・重要インフラ事業者等向けにクラウド利用の際に考慮すべきセキュリティルール策定
- ISMAPの取組等の民間展開による一定のセキュリティが確保されたクラウド利用の促進
- 信頼性が高く、オープンかつ使いやすい高品質クラウドの整備の推進

③ サイバー犯罪への対策

- サイバー空間を悪用する犯罪者やトレーサビリティを阻害する犯罪インフラを提供する悪質な事業者等の摘発を推進し、実空間と変わらぬ安全・安心を確保
- 警察におけるサイバー事案対処体制の強化

④ 包括的なサイバー防御の展開

- サイバー攻撃対処から再発防止等の政策措置までの総合的調整を担うナショナルサート機能の強化（対処官庁のリソース結集と連携強化、サイバーセキュリティ協議会等の関係機関との連携による官民連携・国際連携強化）
- 包括的サイバー防御のための環境整備（脆弱性対策、技術検証、制御システムのインシデント原因究明機能の整備等）

⑤ サイバー空間の信頼性確保に向けた取組

- 個人情報や知的財産を保有する主体への支援
- 経済安保の視点を踏まえたITシステム・サービスの信頼性確保（政府調達、重要なインフラ、国際海底ケーブル等）

主な具体的施策（２）デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保

- デジタル庁が策定する国等の情報システム整備方針にサイバーセキュリティの基本的な方針も示し実装を推進。
- 情報と発信者の真正性等を保障する制度を企画立案し、普及を促進。ISMAP制度を運用し、民間利用の推奨。

主な具体的施策（３）経済社会基盤を支える各主体における取組

① 政府機関等

- 政府統一基準群に基づく対策の推進や監査・CSIRT訓練・GSOCによる監視等を通じた政府機関全体としてのセキュリティ水準の向上。
- クラウドサービスの利用拡大を見据えた政府統一基準群の改定・運用やクラウド監視に対応したGSOC機能の強化。

② 重要インフラ

- 「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」を改定し、環境変化に対応した防護の強化や経営層のリーダーシップを推進。
- 地方公共団体情報システムの標準化や行政手続きのオンライン化等に対応したガイドラインの見直し等の諸制度整備。

③ 大学・教育研究機関等

- リスクマネジメント・事案対応に関する研修・訓練や、サプライチェーンリスク対策を含む、先端情報を保有する大学等への対策強化支援等。

主な具体的施策（４）多様な主体による情報共有・連携と大規模サイバー攻撃事態等への対処体制強化

- 東京大会での対処態勢や運用により得た知見やノウハウを広く全国の事業者等に対する支援として積極活用。
- 平素から大規模サイバー攻撃事態等へのエスカレーションを念頭に、国が一丸となったシームレスな対処態勢を強化。

サイバーセキュリティ戦略における記載内容（東京大会等に向けた取組の今後の活用方策関係）

【「サイバーセキュリティ戦略（令和3年9月28日 閣議決定）」から関連部分を抜粋】

4　目的達成のための施策

4.2.1　国民・社会を守るためのサイバーセキュリティ環境の提供

（中略）サイバー空間の変容を背景に、インシデントの影響が複雑かつ広範囲に伝播するリスクが顕在化している状況を踏まえ、各サービスの提供主体が、直接の利用者のみならずその先の利用者の存在も見据えつつ、相互連関・連鎖全体を俯瞰してリスクマネジメントの確保に務めることがスタンダードとなるよう、国は、関係主体と連携して環境づくりに取り組んでいく。

国民の安全・安心の根幹に関わる経済社会基盤の防護については、これを担う各主体が役割に応じた機密性、可用性、完全性を確実に保証することが基本であるが、前述のサイバー空間の変容に加え、近年の攻撃手法の組織化・洗練化などの脅威に晒されるなど厳しい環境下では、自助、共助の取組だけで対応することは益々困難となっていることから、国が主体的に関係機関とも連携を図りつつ、攻撃者の視点も踏まえ、持ち得る全ての手段を活用して包括的なサイバー防御を講ずることによって、国全体のリスクの低減とレジリエンスの向上に精力的に取り組む。

(4)　包括的なサイバー防御の総合的な調整を担うナショナルサート機能等の強化

国は、深刻なサイバー攻撃に対し、情報収集・分析から、調査・評価、注意喚起の実施及び対処と、その後の再発防止等の政策立案・措置に至るまでの一連の取組を一体的に推進するための総合的な調整を担う機能としてのナショナルサート（*CSIRT/CERT*）の枠組みを強化する。具体的には、対処官庁のリソース結集と連携強化を通じて対処能力の向上と対処に係る一体性・連動性を図るとともに、サイバー関連事業者との連携強化によって組織・分野横断的に影響が波及し得る事案の情報収集や初動を含めた対処調整の迅速化を図る。また、サイバーセキュリティ協議会やサイバーセキュリティ対処調整センター、国内外の関係者との連絡調整について十分な技術的能力及び専門的な知識経験を有する専門機関をはじめとした情報共有体制間や海外関係機関との連携を一層推進することで、官民間・国際間での情報共有と対処調整の円滑化を図る。さらに、発生した事案等から得られた課題や気づきを踏まえ、国は、官民を含む関係者と総合的な調整を行い、適時に制度化など必要な政策の立案・措置を講じていく。

これらの取組により、官民を含む関係者からの適宜迅速な情報収集と被害の全体像の迅速な把握力を強化するとともに、国の防御に関する情報発信の訴求力と網羅性の向上、攻撃の特性や深刻度、個々の分野の事情に応じた系統的できめ細かい対応、防御の実効性向上に資する経営から現場レベルまでの様々なニーズに応じた適時な注意喚起や情報提供、サイバー攻撃の無害化等を模索するグローバルなオペレーションへの協力、さらに、円滑な総合調整による迅速な政策立案等の更なる推進を図り、国全体の包括的な防御力を向上する。

サイバーセキュリティ戦略における記載内容（東京大会等に向けた取組の今後の活用方策関係）

【「サイバーセキュリティ戦略（令和3年9月28日 閣議決定）」から関連部分を抜粋】

4　目的達成のための施策

4.2.6　多様な主体によるシームレスな情報共有・連携と東京大会に向けた取組から得られた知見等の活用

サイバー空間におけるリスクの高まりを踏まえ、国は、リスクへの感度とレジリエンスを高め、実効性かつ即応性のあるサイバー攻撃対処に資する、時間的・地理的・分野的にシームレスな情報共有・連携を推進し、平時から大規模サイバー攻撃事態等に対する即応力を確保する。

また、新たな攻撃にも国全体として網羅的な対処が可能となるよう、国はナショナルサート（CSIRT/CERT）の枠組み整備の一環として、東京大会に向けて整備した対処態勢とその運用経験及びリスクマネジメントの取組から得られた知見、ノウハウを活かすことで、大阪・関西万博をはじめとする大規模国際イベント時だけではなく、平時における我が国のサイバーセキュリティ全体の底上げを進める。また、国は東京大会での運用で得られた知見、ノウハウを適切な形で国際的にも共有していく。

(2) 包括的なサイバー防御に資する情報共有・連携体制の整備

サイバー攻撃等に対して国全体として網羅的な対処が可能となるよう、ナショナルサート（CSIRT/CERT）の枠組み整備の一環として、国はサイバーセキュリティ協議会やサイバーセキュリティ対処調整センター、国内外の関係者との連絡調整について十分な技術的能力及び専門的な知識経験を有する専門機関をはじめとした情報共有体制間の連携を進め、外部との連携や調整の在り方について具体的に検討する。

また、国は東京大会に向けて整備した対処態勢とその運用経験及びリスクマネジメントの取組から得られた知見やノウハウを、東京大会の運営を支える事業者等にとどまらず、広く全国の事業者等におけるサイバーセキュリティ対策への支援等として積極的に活用することで、大阪・関西万博をはじめとする大規模国際イベント時から、平時に至る我が国のサイバーセキュリティ全体の底上げを進める。

4.3.3　国際協力・連携

(1) 知見の共有・政策調整

（略）我が国のサイバーセキュリティ政策等に関する国際的な情報発信も強化し、東京大会における我が国の経験等も他国に共有し国際貢献を果たす。