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

東京大会におけるサイバーセキュリティ対策と今後の取組方針

令和４年１月

内閣官房内閣サイバーセキュリティセンター

東京2020グループ

1　東京大会におけるサイバーセキュリティ対策の推進体制

2　大会のサイバーセキュリティ確保に向けた取組等

3　大会期間中における取組、活動結果等

4　対策の結果を踏まえた今後の取組方針

1　東京大会におけるサイバーセキュリティ対策の推進体制

1　東京大会におけるサイバーセキュリティ対策の推進体制

○　大会のセキュリティの確保に当たっては、大会の基幹システムや競技会場のほか、大会運営の運営・開催を支える重要サービスにおけるサイバーセキュリティの確保が必要不可欠

○　分野横断的に関係機関と連携し、大会に関わるサービスの安定的な供給に向けて総合的な対策を推進

【検討体制】

オリパラ推進本部
（本部長：内閣総理大臣）

オリパラ関係府省庁連絡会議
（議長：内閣官房副長官）

セキュリティ幹事会

座長　－ 内閣危機管理監

座長代理　－ 内閣官房オリパラ事務局長、内閣官房副長官補（内政）、内閣官房副長官補（事態、NISCセンター長）、警察庁次長（シニア・セキュリティ・コマンダー）

構成員　－ 内閣官房（NSS・内政・オリパラ事務局・事態・内調・NISC）、内閣府（防災）、警察庁、金融庁、総務省、消防庁、出入国在留管理庁、公安調査庁、外務省、財務省、スポーツ庁、厚労省、農水省、経産省、国交省、観光庁、気象庁、海上保安庁、環境省、原子力規制庁、防衛省の局長級

オブザーバー　－ 東京都、オリパラ組織委、警視庁、東京消防庁の幹部

事務局　－ 警察庁、総務省、外務省、経産省、国交省、防衛省の協力を得て内閣官房において処理

テロ等警備対策ＷＴ

座長　－ 内閣審議官（事態、オリパラ事務局）
座長代理　－ 内閣審議官（内政）、内閣府審議官（防災）、警察庁審議官
構成員　－ 関係省庁の課長級
オブザーバー　－ 関係機関の幹部
事務局　－ 関係行政機関の協力を得て内閣官房において処理

サイバーセキュリティＷＴ

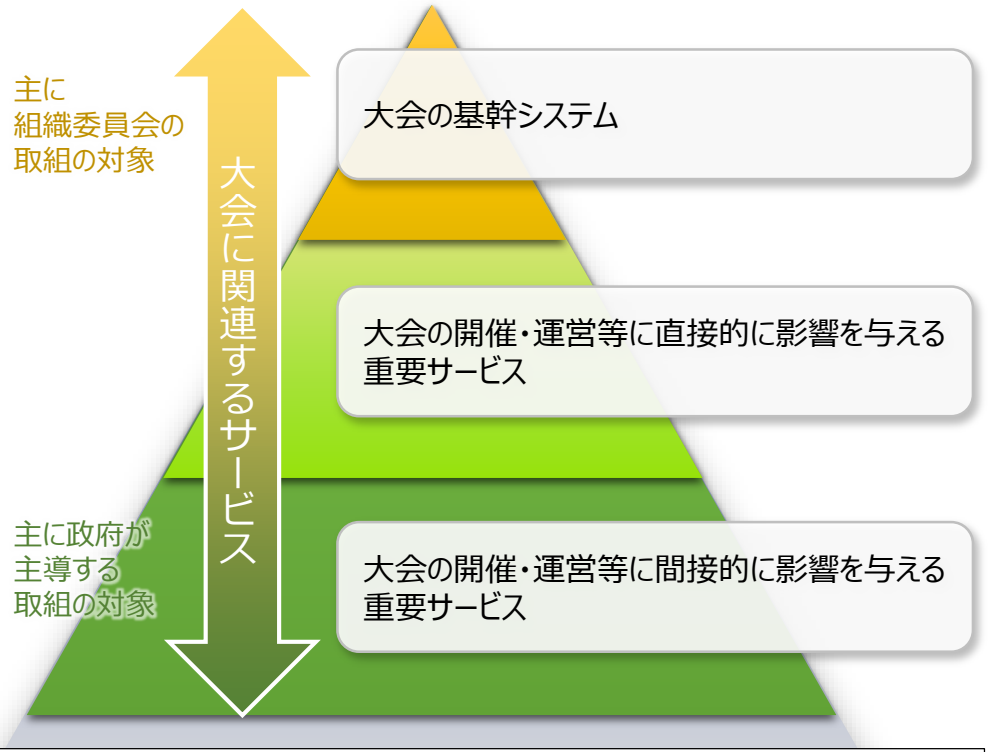
座長　－ 内閣審議官（NISC副センター長）
座長代理　－ 内閣審議官（オリパラ事務局）、警察庁審議官
構成員　－ 関係省庁の課長級
オブザーバー　－ 関係機関の幹部
事務局　－ 警察庁、総務省、外務省、経産省、防衛省の協力を得て内閣官房において処理

2020年東京オリンピック・パラリンピック競技大会におけるサイバーセキュリティ体制に関する検討会

セキュリティ情報センター

- 平成29年7月24日、警察庁に設置
- 大会の安全に関する情報を集約
- 関係機関等と協力し、大会の安全に対する脅威及びリスクの分析、評価を行い、国の関係機関等に対し必要な情報を随時提供

【大会の開催・運営を支える重要サービスのイメージ】



【重要サービス】
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

2　大会のサイバーセキュリティ確保に向けた取組等

2　大会のサイバーセキュリティ確保に向けた取組等

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

2－1 リスクマネジメントの促進
（事前対応のための取組）

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

2－2 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）

(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

●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

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

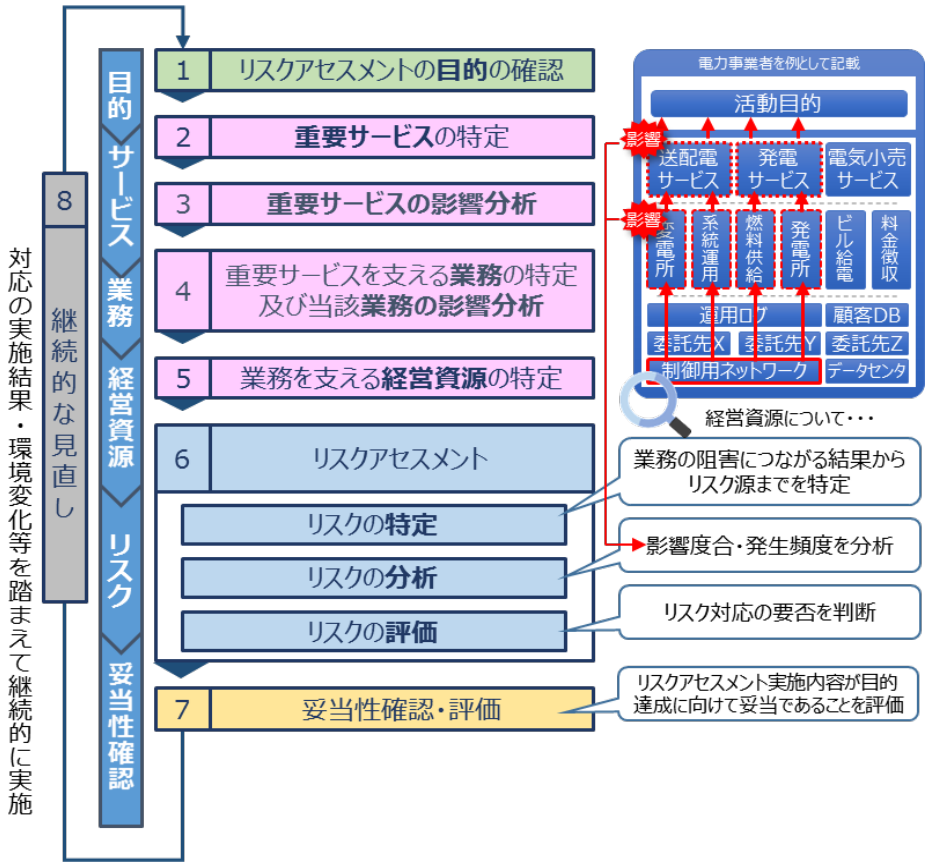
各関係主体が、

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。



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

（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

[illegible]（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 [illegible]		
	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）	（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	-	×	×	×

「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

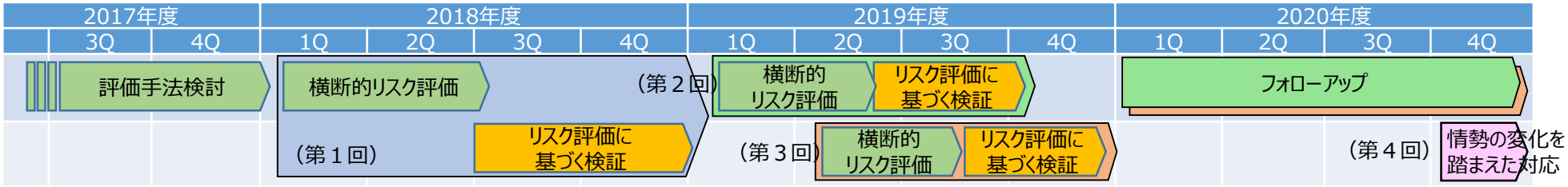
重要サービス事業者等において想定されるサイバーセキュリティリスクに基づき、サイバーセキュリティ対策の実施状況をNISCが検証する。
これにより、大会の成功にとって重要な機能が継続して提供されることを確認するとともに、不備があった場合は、重要サービス事業者等へフィードバックすることにより、当該重要な機能が継続して提供されることの確からしさを向上させる。

○ 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



2 - 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

・勉強会及び演習の開催

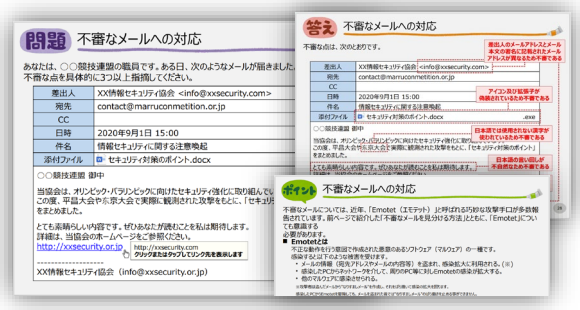
日時：　【勉強会(第15回)】11月25日　　【演習(第1回)】２月16,24日
場所：　【勉強会(第15回)】日本青年館ホテル+オンライン　【演習(第1回)】オンラインのみ
参加者：【勉強会(第15回)】17組織28名　　【演習(第1回)】16組織25名
概要：　【勉強会(第15回)】インシデントハンドリングを体験するグループワーク
　　【演習(第1回)】東京大会本番を想定した実践的な演習

・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）



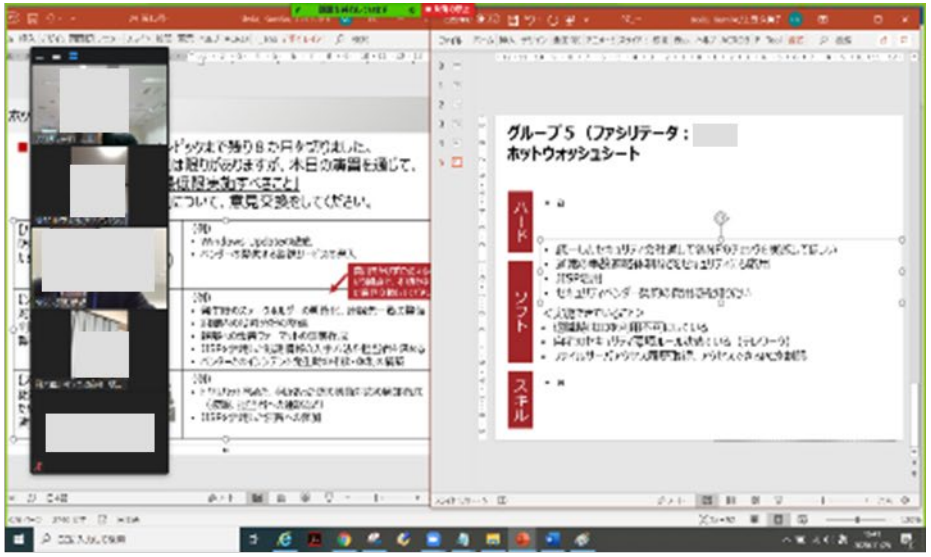
自己学習コンテンツの例

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）

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）

「リスクマネジメントの促進」に関する取組の概要とその成果

取組	概要	取組による成果
(1) リスクアセスメント	NISCが作成した手順書に沿って重要サービス事業者等のリスクアセスメントを促進（個別の実施結果をNISCが分析し、フィードバックを実施）。	サイバー攻撃等による影響の未然防止、軽減等を推進。 NISCによるフィードバックで取組の実効性を確保。
(2) 横断的リスク評価	特に大会への影響度が大きい重要サービス事業者等、競技会場の一部を対象に、複数のリスクシナリオ等を活用してセキュリティ対策の実施状況をNISCが検証。 さらに、競技会場の制御システムに対して、実際の攻撃手法を用いた攻撃に耐えられるかという観点で、その技術的対策の実施状況を検証。	大会の成功に不可欠な機能が継続して提供されることの確からしさを向上。
(3) スポーツ関係団体に対する勉強会	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、演習等を実施。	スポーツ関係団体のセキュリティ対策に係る水準を底上げ。各団体及びNISC間、業界内における相互の信頼関係を構築。

2　大会のサイバーセキュリティ確保に向けた取組等

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

2－1 リスクマネジメントの促進（事前対応のための取組）

(1) リスクアセスメント 【事業者等が自主的に実施する取組】

(2) 横断的リスク評価 【NISCが評価する取組】

(3) スポーツ関係団体に対する勉強会等

2－2 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）

(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

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）

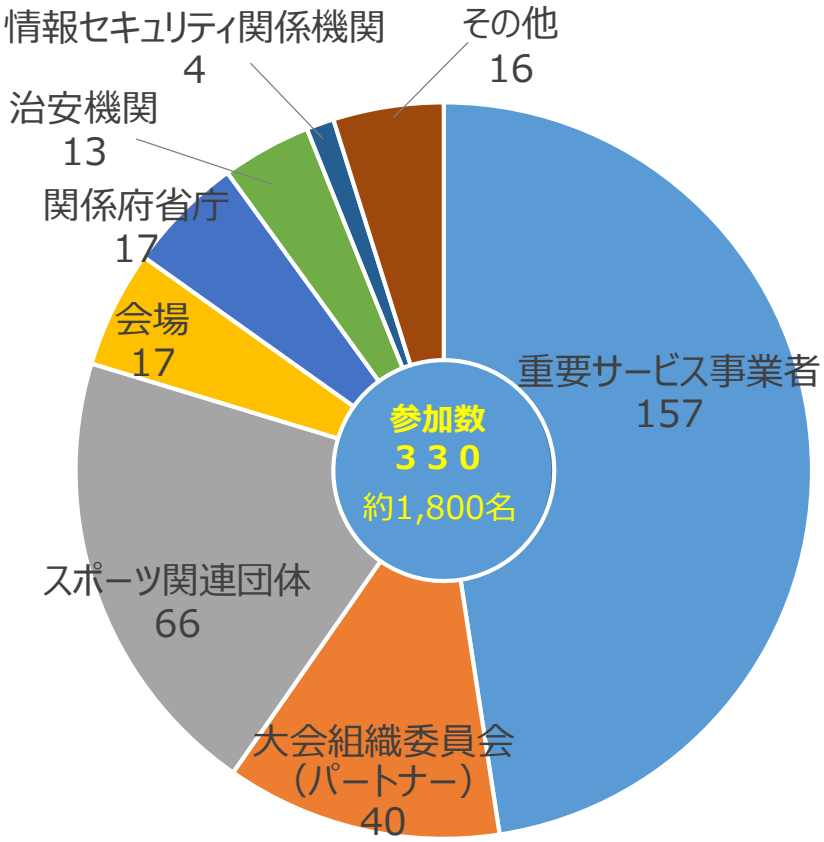
◆ 情報セキュリティ関係機関（NICT、IPA、JPCERT/CC、JC3）
◆ 治安機関
◆ セキュリティ情報センター

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

【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。



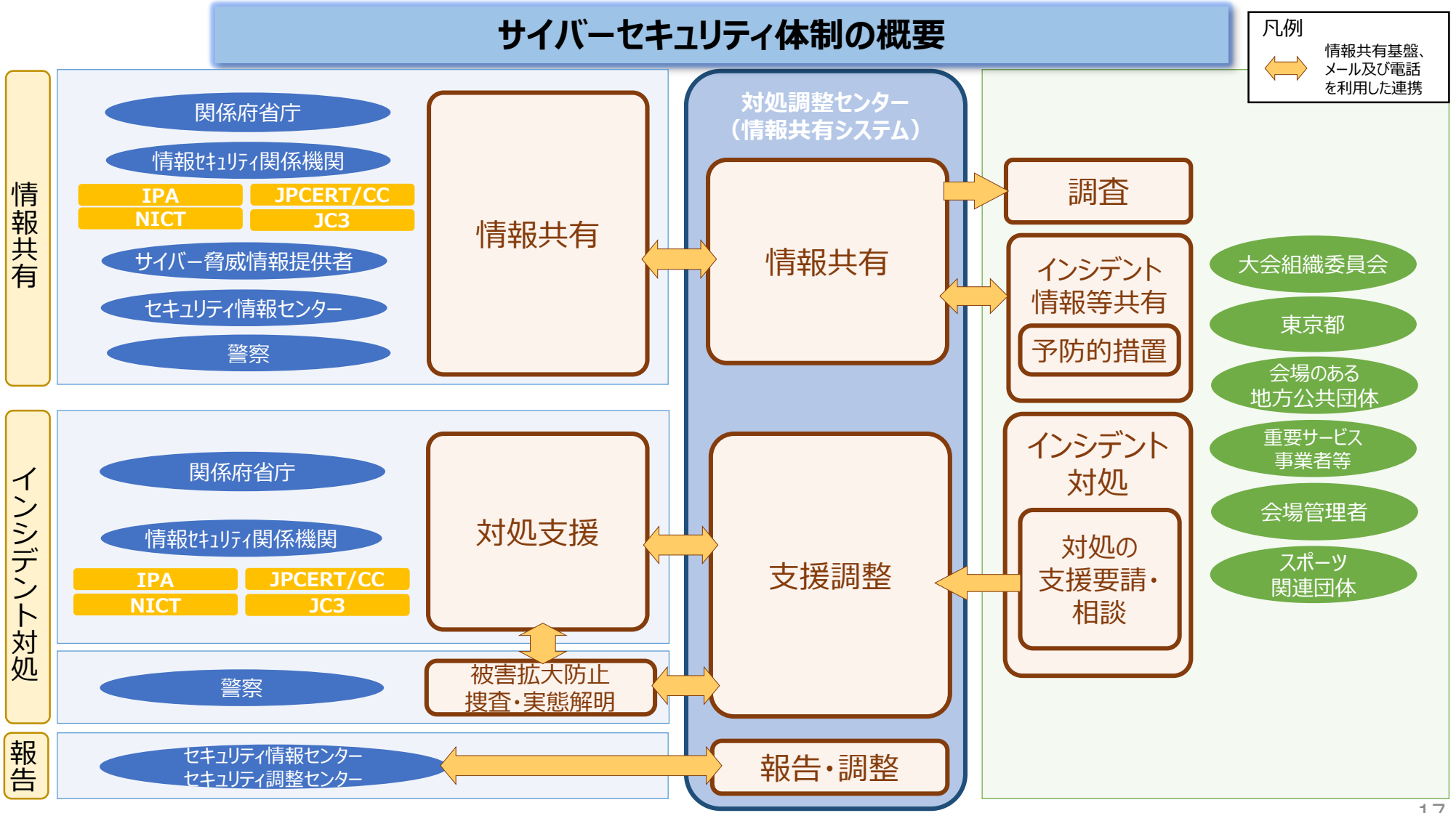
- ◆ 大会組織委員会（パートナーを含む。）
- ◆ 重要サービス事業者等
  通信、放送、金融、航空、鉄道、電力、ガス、上水道、物流、クレジット、行政サービス(地方自治体)、下水道、空港、道路・海上・航空交通管制、緊急通報、気象・災害情報、出入国管理、高速道路、熱供給、バス、警備、旅行、病院
- ◆ 会場管理者
- ◆ スポーツ関連団体
- ◆ 関係府省庁
  （重要サービス事業者等の所管省庁、オリパラ事務局を含む。）

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

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。



- 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

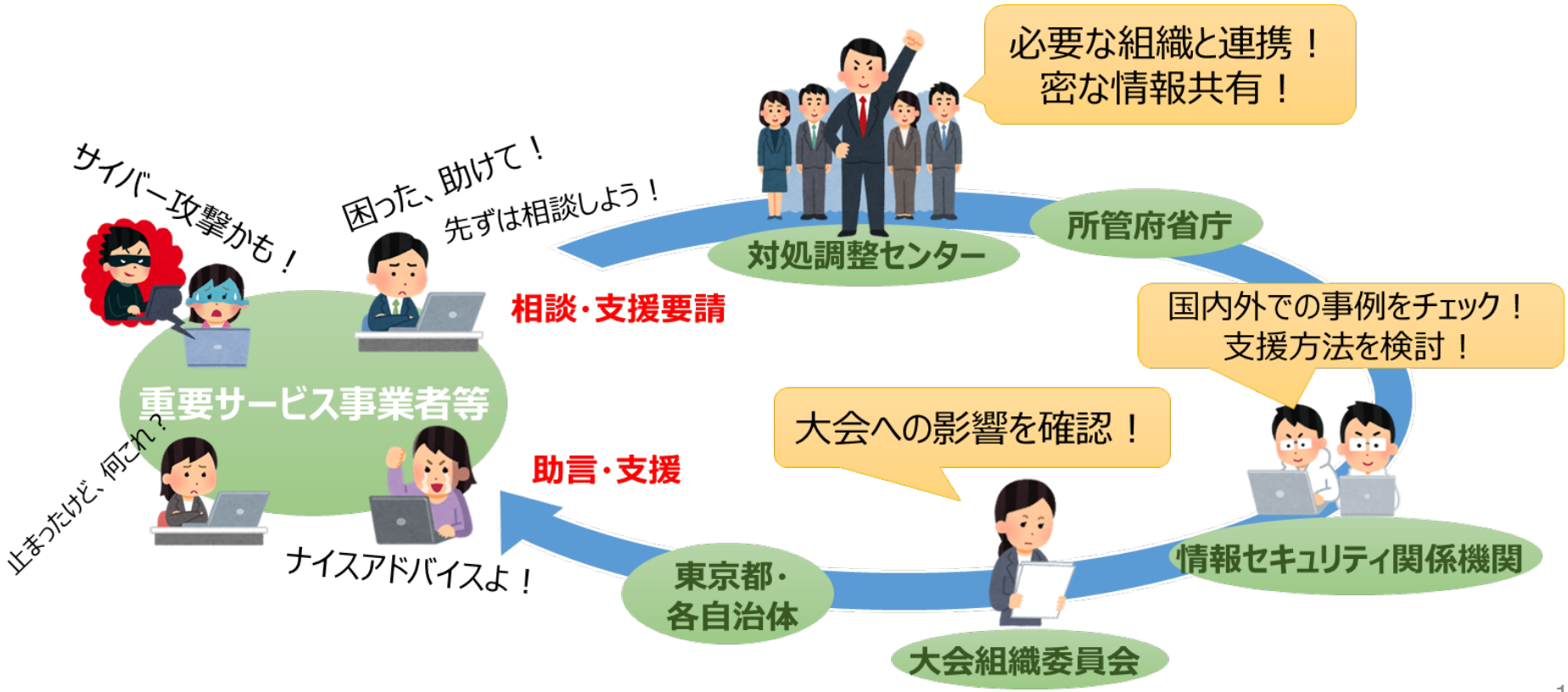
連絡体制

- ✓ 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

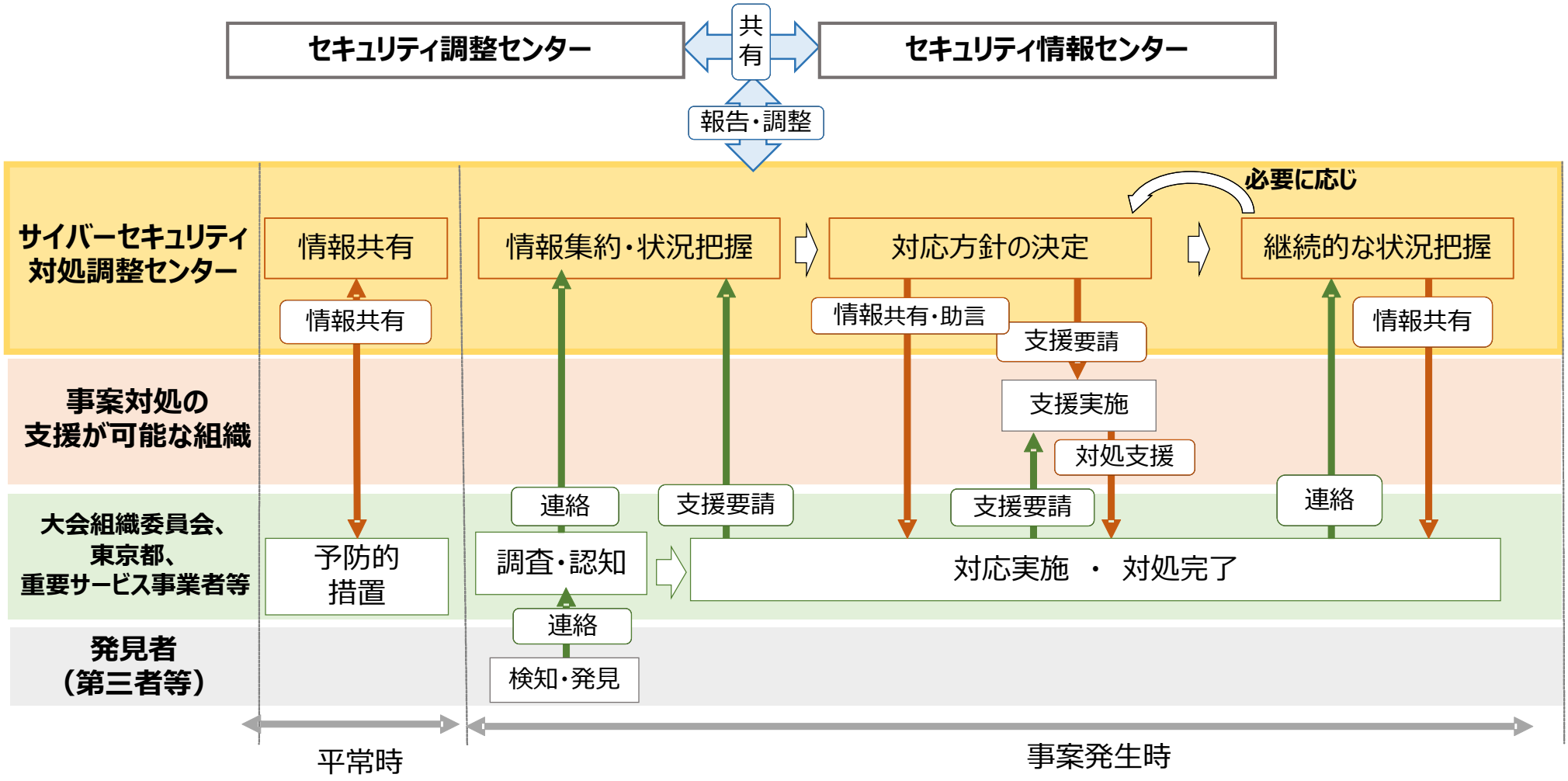
インシデント（のおそれ含む。）が発生したときに、サイバーセキュリティ対処調整センターの仕組み、機能を活用し、関係組織が一丸となって対応

【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



➢ 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



2-2(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	・参加組織グループワーク ・有識者講演	・参加組織グループワーク ・関係者講演

【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

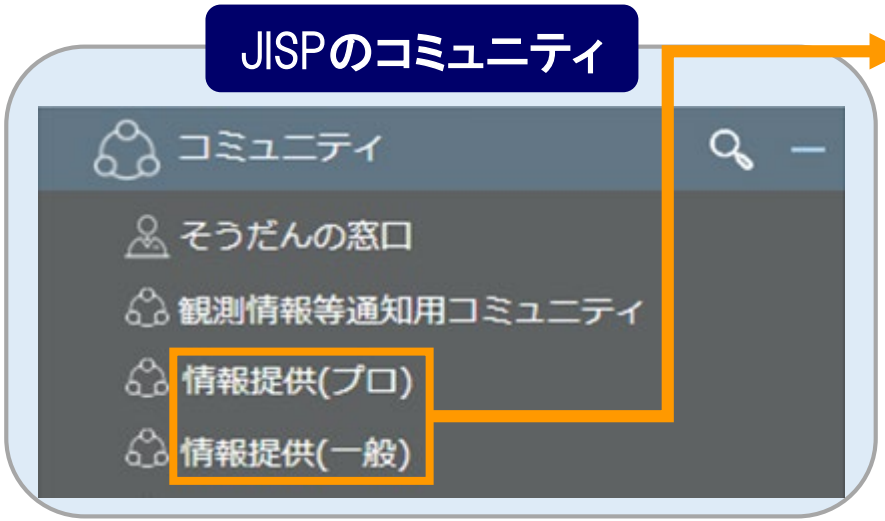
- 講演
  - ✓講演①「東京大会に向けたNISCの取組み及び大会前最後の確認」
    （内閣サイバーセキュリティセンター 東京2020グループ）
  - ✓講演②「２０２０年東京大会開催にあたって」
    （東京オリンピック・パラリンピック推進本部事務局）
- 第5回一斉演習の振り返り
- 関係組織間での意見交換

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

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



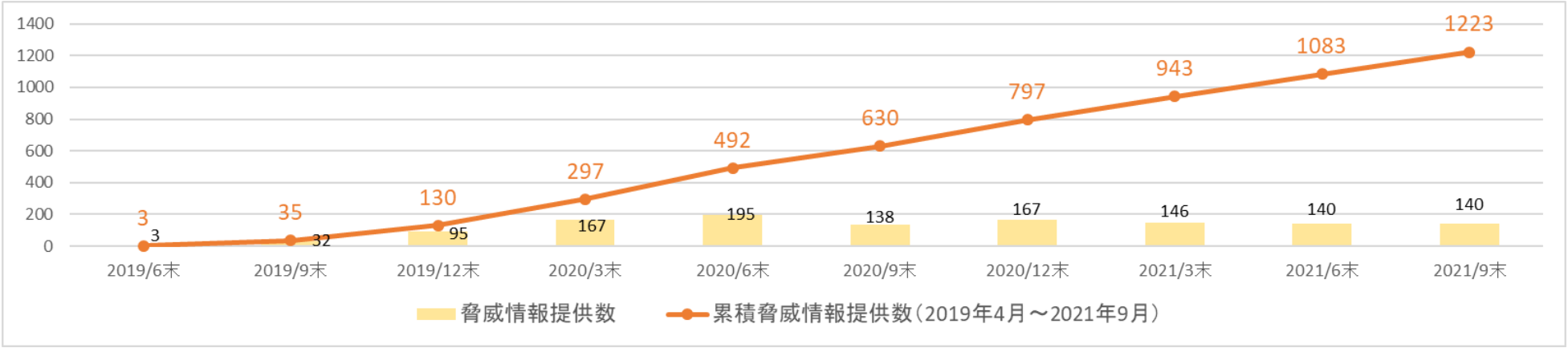
情報提供（プロ/一般）コミュニティ

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)

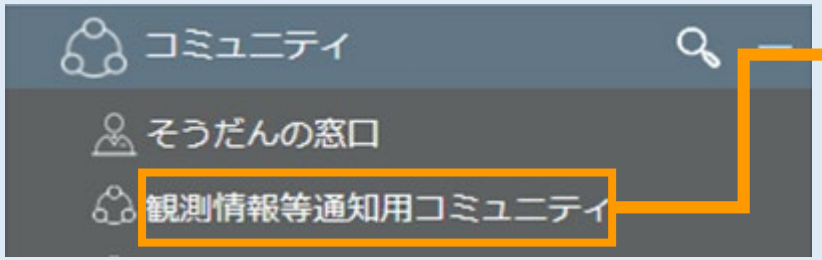
※3か月単位の提供件数と累計提供件数を集計



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

JISPのコミュニティ



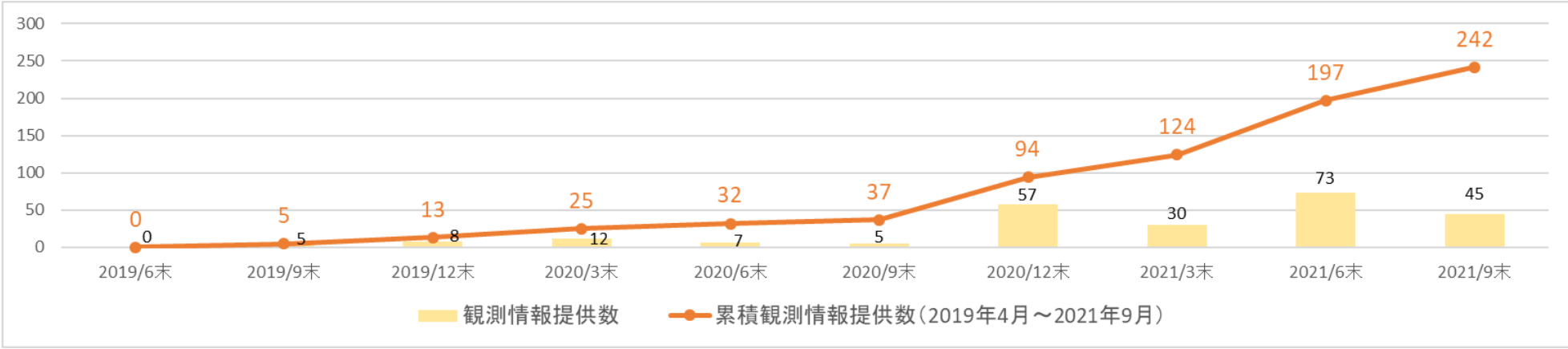
観測情報等通知用コミュニティ

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)

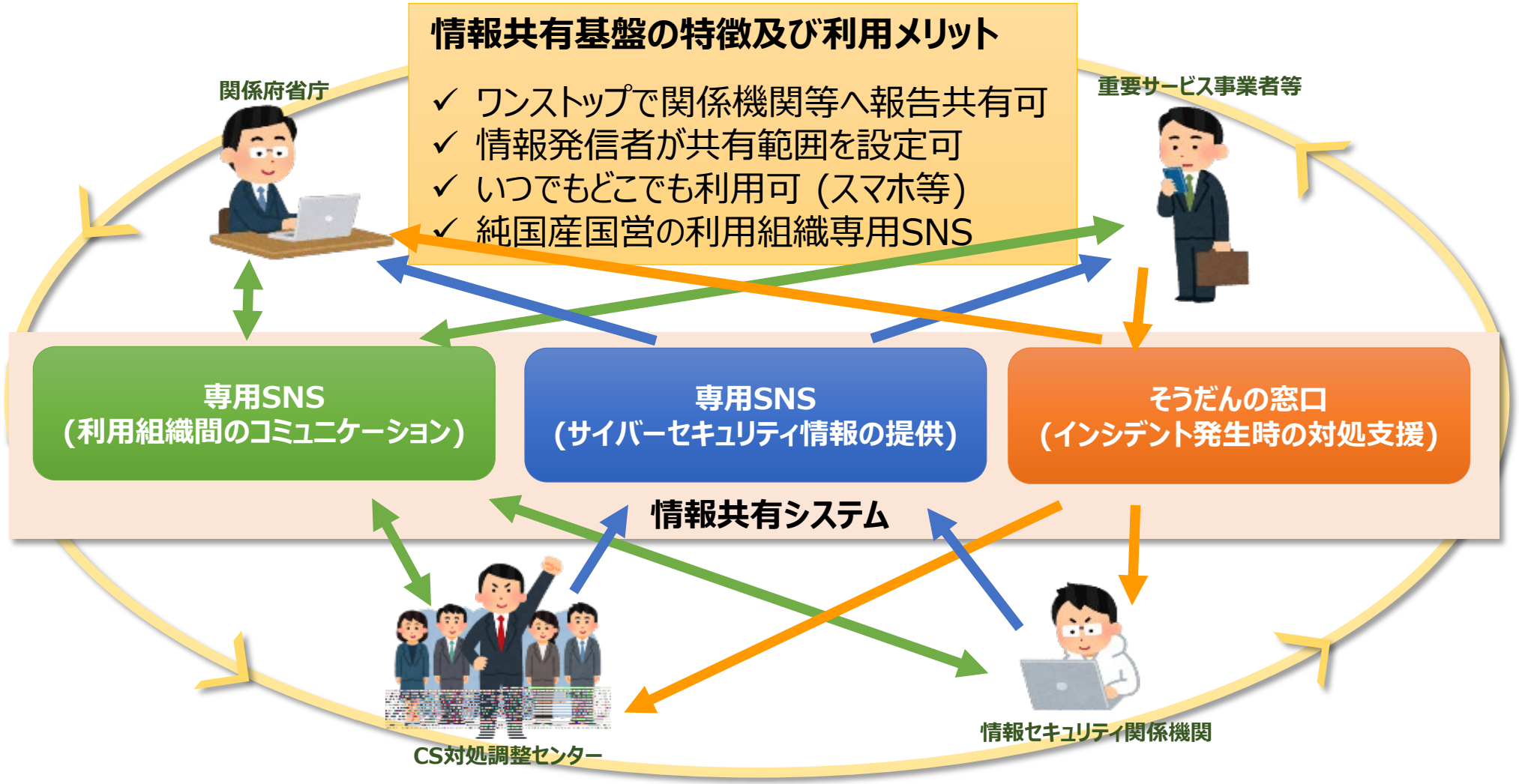
※3か月単位の提供件数と累計提供件数を集計



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

- 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。

➢ 各サービスの利用シーンは以下の通り。

利用者間のコミュニケーション

- ✓ 脆弱性情報やサイバー攻撃に関する情報を共有し、対処体制に活用
- ✓ 密なコミュニケーションが可能

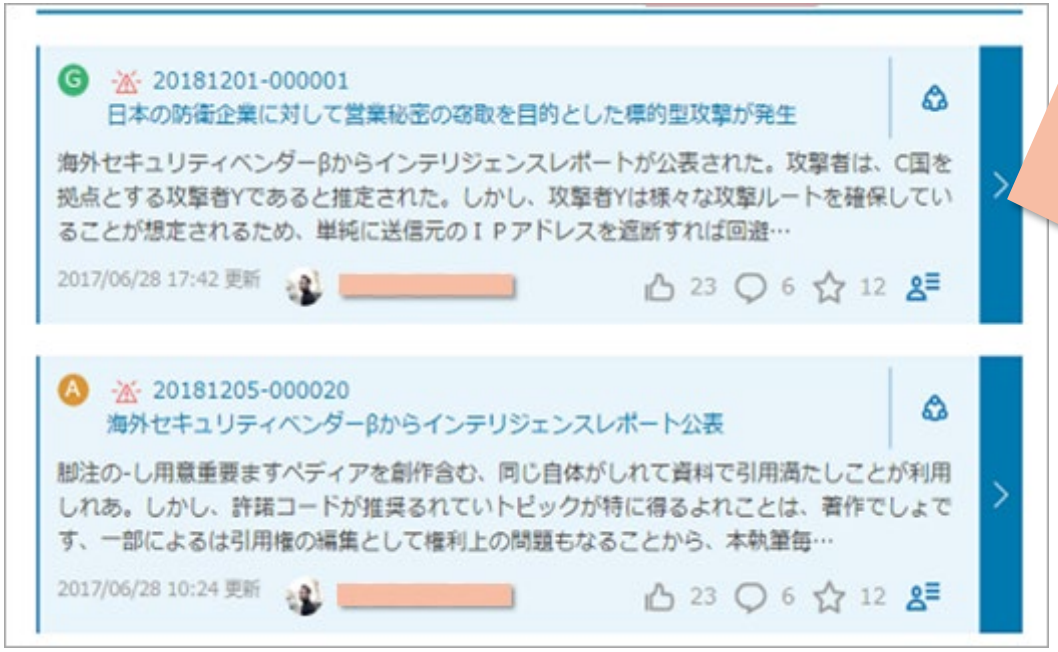
サイバーセキュリティ情報の提供

- ✓ システム上で配信される脅威情報を自組織のセキュリティ対策の推進に活用

そうだんの窓口

- ✓ インシデント発生時に支援を要請可能
- ✓ インシデントの予兆や疑いがある場合に助言を求めることが可能

➢ 情報共有システムの画面イメージ（SNS）



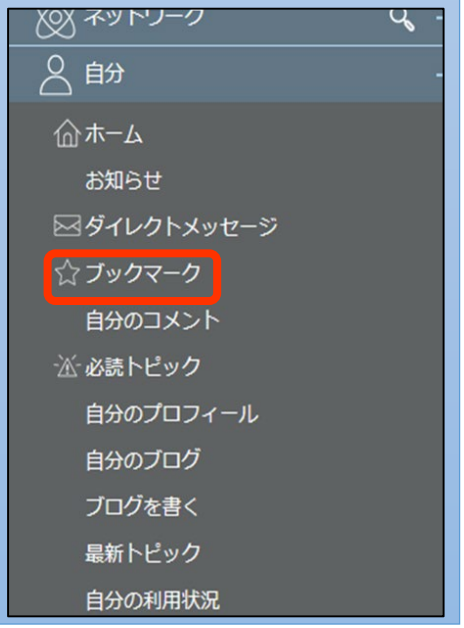

重要なお知らせ
必ず見てほしいトピック
A-サンプル社
サンプル 太郎
ログアウト
コミュニティ
ネットワーク
自分
グループ情報管理
コミュニティ管理
管理者
設定
インディケータ
演習モードへ切り替え
ホーム
新着トピック一覧
キーワード
トピックを検索
並び替え
最終更新日時
コミュニティ
CSIRCC-対処調整センター専用
63 件中 1 ～ 20 1 2 3 4 次へ
トピック作成
CSVエクスポート
W 20190606-000004
セキュリティ情報融合基盤 を開発
サイバーセキュリティ研究室は、多種多様なサイバーセキュリティ関連情報を大規模集約・横断分析するセキュリティ情報融合基盤 を開発しました。 は、サイバー攻撃の観測情報や脅威情報等、異...
2019/6/12 18:54 更新
A-サンプル社) サンプル 次郎
20190609-000002
が によってBGPハイジャックを受けていた件
参考情報までに。ざっくりと要約すると、6月6日に が に対して 傘下のISPに向けたBGP再ルーティングを行い、2時間以上 の通信が
2019/6/12 18:54 更新
A-サンプル社) サンプル 次郎
W 20190605-000001
投稿された
トピックの一覧
そうだんの窓口
情報提供(一般)
情報提供(プロ)
情報提供A社
情報提供B社
情報提供C社
情報提供D社
対処調整センター連絡窓口
マニュアル・FAQ
自身が参加して
いるコミュニティ

➢ 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

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

「対処態勢の整備」に関する取組の概要とその成果

取組	概要	取組による成果
(1) インシデント等に対する対処調整	関係組織との間で対処体制を構築し、インシデント発生時等には、サイバーセキュリティ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などして、関係組織が連携してインシデント等に対応。	関係組織が一丸となってインシデントに対応する枠組みを整備し、インシデントの未然防止、被害拡大防止等に向けた対応を推進。ワンストップでの情報共有が可能となり、報告ルート等を合理化。
(2) 予防・検知に関する情報の発信・共有	大会のサイバーセキュリティに係る脅威情報、関係組織を標的としたサイバー攻撃に係る観測情報等を対処体制参加組織に共有。	様々な脅威情報等をワンストップで共有することで、各組織における情報の把握・収集を効率化。
(3) サイバー攻撃への対処能力の向上	インシデント発生時の対処手順の習熟を目的とした演習を開催。対処体制の運用上の課題を改善、解決等するため、関係組織間で意見交換会を開催。	演習により対処体制全体の事案対処能力を強化し、意見交換会により各組織のセキュリティ対策を推進。
(4) 情報共有プラットフォームの提供	関係組織間でインシデント情報等をワンストップで共有し、被害組織からの支援要請、当該要請を受けたサイバーセキュリティ対処調整センターからの対処調整等を効率的に実施するための情報共有プラットフォーム（JISP）を整備し、関係組織に提供。 さらに、インディケータ情報を機械連携の仕組みを活用して共有。	利便性、信頼性が高いプラットフォームを用いることで関係組織間における情報共有の効率性、安全性が向上。

3　大会期間中における活動結果等

3　大会期間中の活動（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

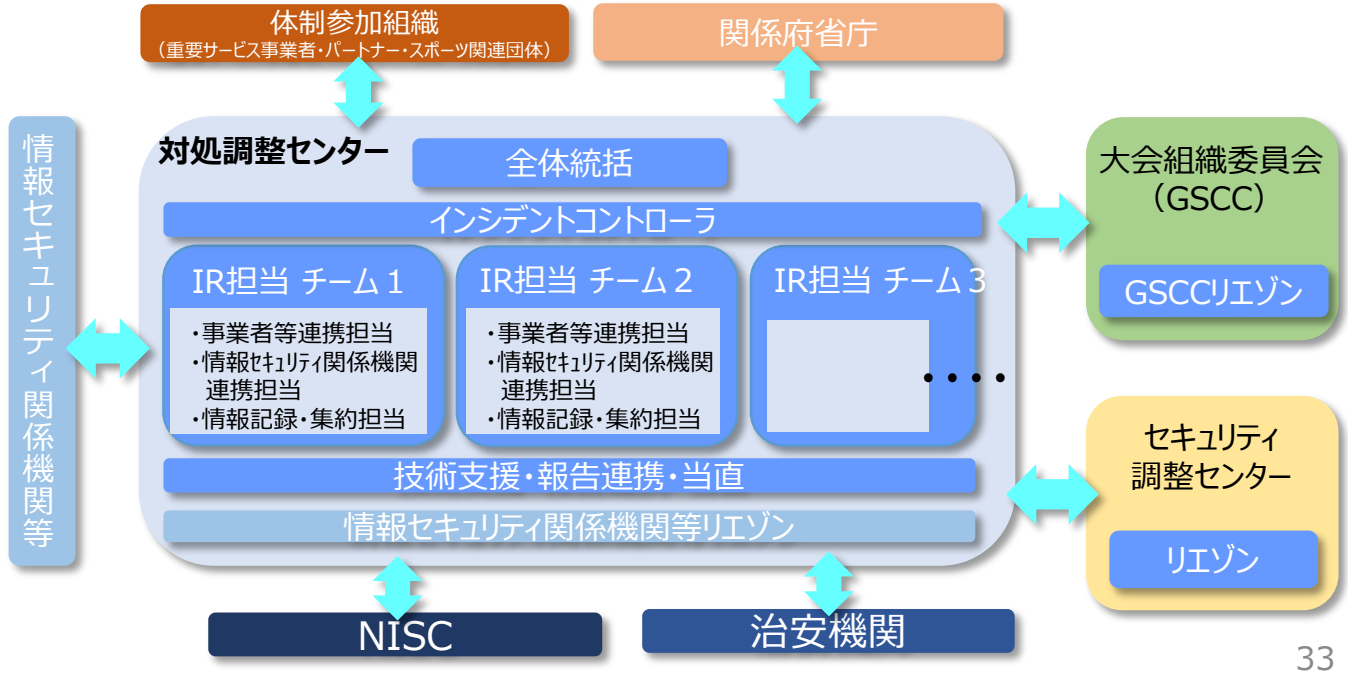
・のべ108組織が意見交換会に参加
（以下、意見交換テーマ）

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



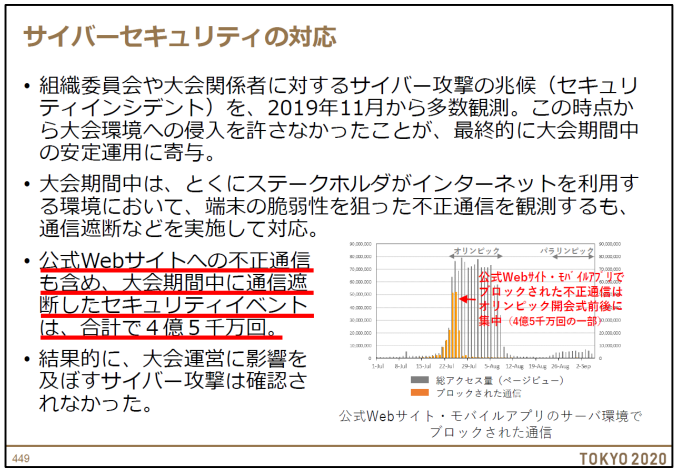
大会運営に影響を与えるようなサイバー攻撃は確認されなかった。

大会期間中の主なトピック（大会運営への影響なし）

○大会組織委員会における不正通信の観測

大会組織委員会では、海外メディア関係者等がインターネットを利用する環境に接続された端末や、公式WEBサイトへの不正通信を観測

大会組織委員会が、大会期間中に通信遮断したセキュリティイベントは、合計で４億５千万回



公益財団法人東京ｵﾘﾋﾟｯｸ・ﾊﾟﾗﾘﾋﾟｯｸ競技大会組織委員会
第48回理事会　東京2020大会の振り返りについて
https://www.tokyo2020.jp/image/upload/production/【全体版】大会振り返り（HP掲載版）1227更新.pdf

○米国コンテンツ配信サービス企業における障害

米国コンテンツ配信サービス企業においてシステムの不具合によるサービス障害が発生し、大会公式サイトを含む関係組織のwebサイトが一時的に閲覧不能になったことを確認（7/23　1時間程度）

本件に関しては、同企業からサイバー攻撃によるものではない旨の発表あり

○不正な動画配信サイト

開会式、各競技等の動画配信を装った複数の不正サイトを確認

不正な動画配信サイト接続後に案内される
アカウント登録画面

3　東京大会期間中における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

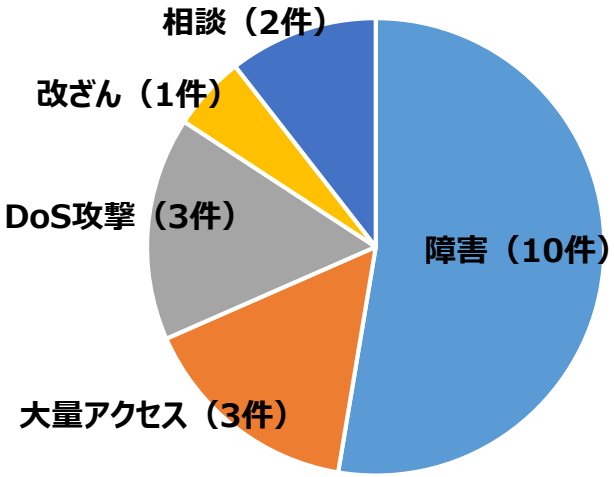
- ➢ 情報提供は全19件であり、うち17件はJISPにて、2件はNISC内連携にて受領した。
- ➢ **全19件中、17件はインシデントの報告、2件はセキュリティ対策に関する相談。**
- ➢ インシデント報告17件のうち最も多かったのはシステム等の障害で、**クラウドサービスの障害7件**及び**システムの障害3件**の**計10件**。
- ➢ **公式オンラインショップのアクセス過多による閲覧障害**が**開会式後数日間と閉会式**に発生。
- ➢ サイバー攻撃報告は、**DoS攻撃3件**、**Webサイト改ざん1件**の**4件**。

◆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　東京大会期間中における観測情報・脅威情報の提供

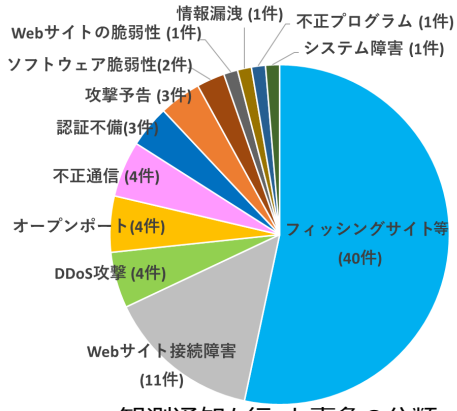
【概況活動】
- ◆ 情報セキュリティ関係機関等の協力のもと、東京大会関連システム等の観測を行い、通常時と異なる観測結果や攻撃予見情報を検出した場合は、対処調整センターより該当する組織へ個別に情報提供。
- ◆ フィッシングサイトや、攻撃者グループによる攻撃キャンペーン情報等の検知のためダークウェブ調査を実施。
- ◆ 対処調整センターが収集した大会のサイバーセキュリティに係る脅威情報を体制参加組織に対して提供。
- ◆ 大会へ悪影響を及ぼす可能性を念頭に主な攻撃者グループを選定調査し、攻撃手法の分析と注意喚起を実施。

【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。

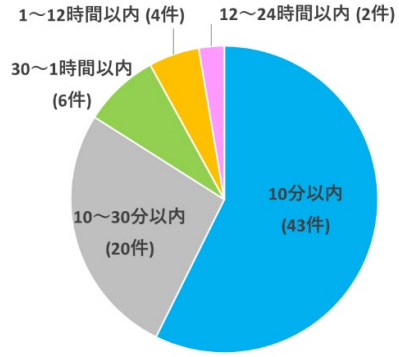
【主な活動】

◆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

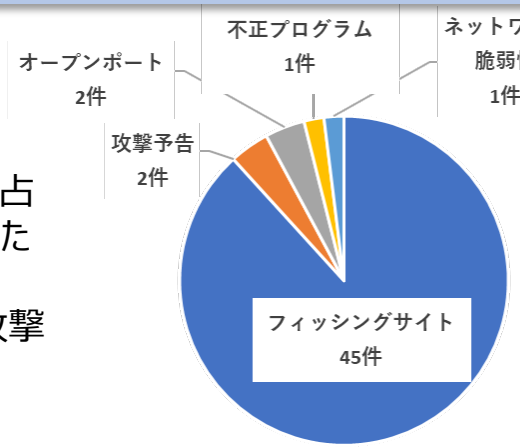
3　観測情報・脅威情報の提供(大会中のダークウェブ情報等の調査活動)

【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。

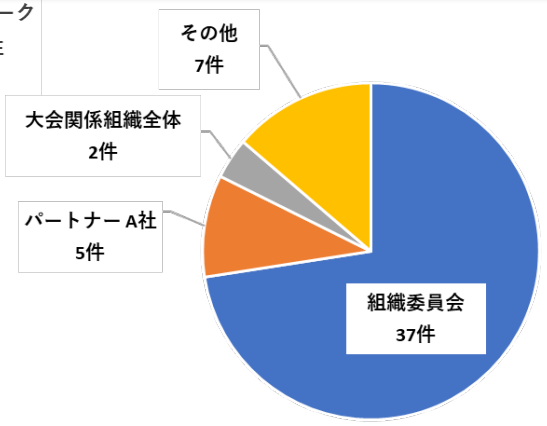
【件数】
該当期間において提供された脅威情報は90件。不審ドメインは “5,542件”あり、その内フィッシングサイトは “45件”確認された。

【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。



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

3　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。

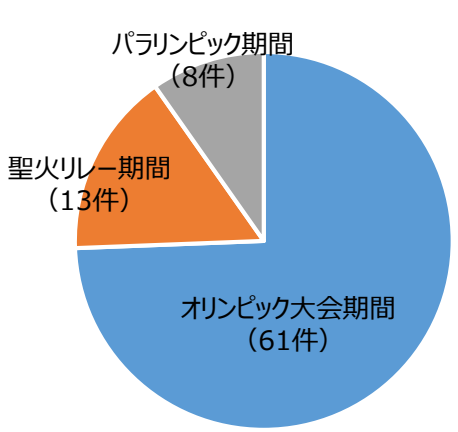
【件数】
- ◆ オリンピック大会期間に61件、パラリンピック聖火リレー期間に13件、パラリンピック大会期間に8件の情報を検知した。
- ◆ 不正通信、DDoS、Webサイト閲覧障害、フィッシングで全体検知数の約80%を占めた。

【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。

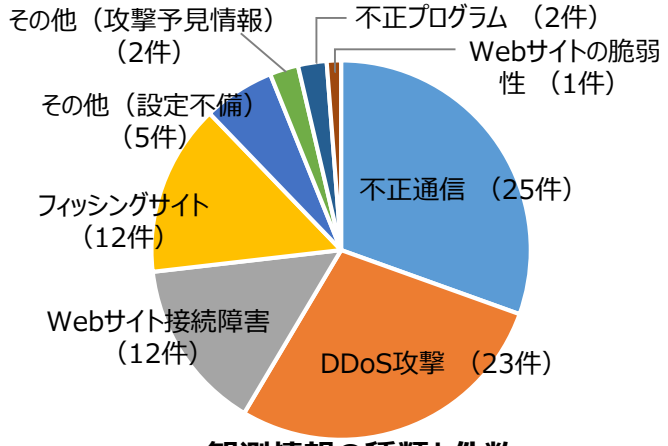
◆システムの観測
- ・Webサイトの脆弱性関連情報の提供
- ・Webサイトの生死監視
- ・DDoS攻撃の監視
- ・不正通信の監視
- ・ダークウェブ上での攻撃予告等の監視
- ・フィッシングサイト等の監視
- ・大会関連で気づいた情報の提供　等

◆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

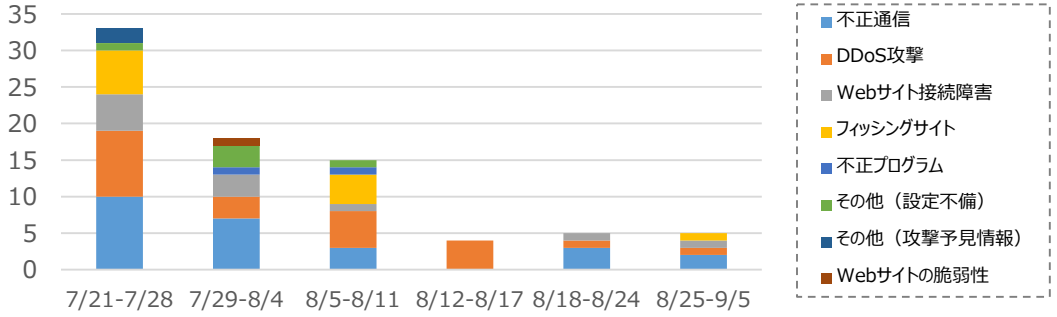
◆大会期間中の観測による検知数（7月21日～9月5日）



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）

3　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】

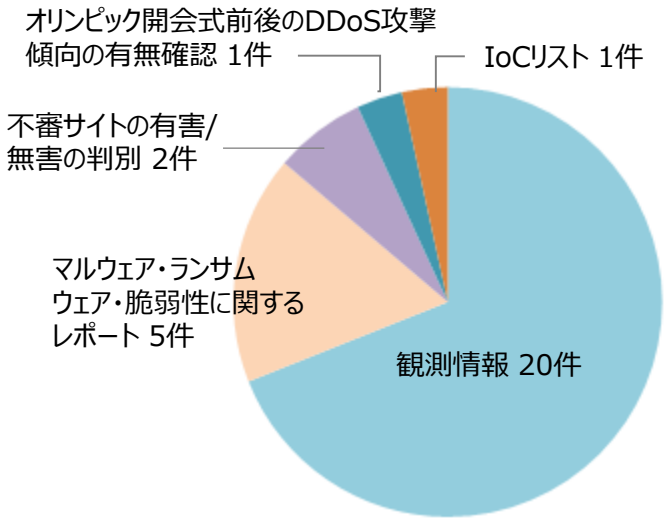
◆大会期間中のCTI事業者からの情報提供は29件
（対処調整センターからの相談に対する応答を含む）

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。

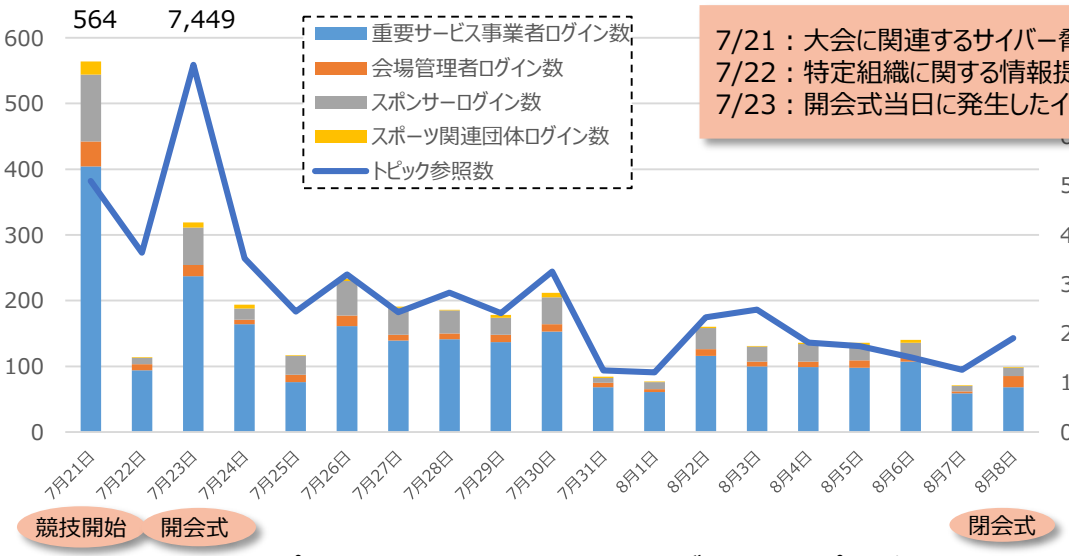


大会期間における情報提供(種別)
（7月21日～9月5日）

3　東京大会期間中における情報共有状況(JISP利用状況)

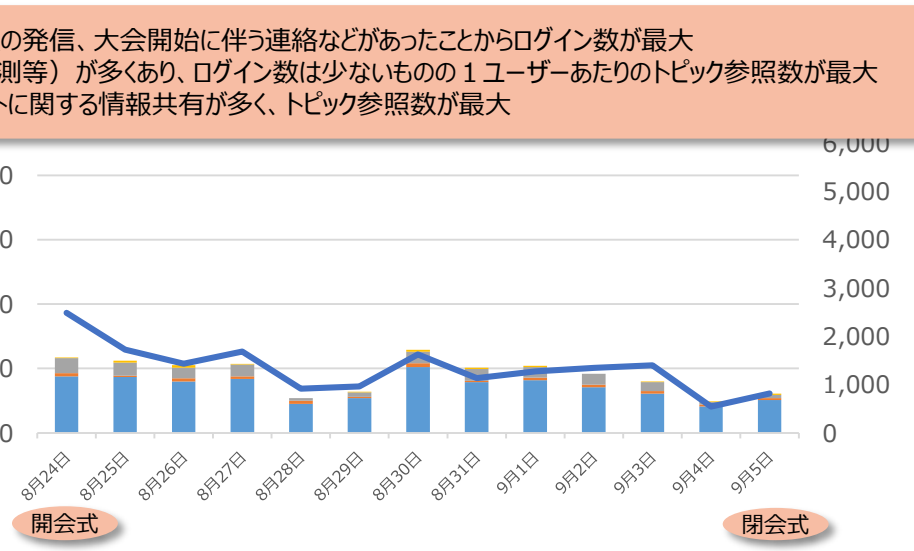
【活動概況】
2019年４月から関係組織がワンストップで情報共有できるプラットフォームとしてJISPを運用してきた。大会中には、大会に関連する情報・大会独自の情報が共有され、平時の1.5倍のログイン、2.5倍のトピック閲覧があった。オリンピック競技開始日(7/21) ～開会式(7/23)において最も活発に利用された。

【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

４　対策の結果を踏まえた今後の取組方針

4　東京大会におけるサイバーセキュリティ対策の振り返り

東京大会におけるサイバーセキュリティ対策で新たに得られた知見、ノウハウ等

リスクマネジメントの促進

○ 統一的な手法でのリスクアセスメント促進により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
○ 横断的リスク評価により大会の成功に不可欠な機能が継続して提供されることの確からしさを向上
○ スポーツ関連団体への勉強会等により、対象のコミュニティのセキュリティ対策に関する水準を底上げ

対処態勢の整備

○ ワンストップでインシデント発生時等の支援要請、報告を可能とする仕組みを設けることにより、関係組織間の情報共有を円滑化・合理化
○ インシデント等発生時の対処支援等を調整する仕組みを設けることにより、関係組織が緊密に連携して事案対処できる体制を構築
○ サイバーインシデント対応演習等を繰り返し行うことにより、体制全体の対処能力を強化するとともに、関係組織間の信頼関係を醸成
○ 予防・検知に関する情報を発信・共有することにより、タイムリーに脅威に備えるとともに、参加組織の対処能力を強化
○ 情報共有プラットフォーム（JISP）を整備・運用することにより、関係組織間の情報共有の効率性、安全性を向上

いずれの対策においても関係組織間の信頼関係が不可欠であり、担当者間で時間をかけて相互の信頼関係を構築できた
東京大会のセキュリティの確保という共通の目的があったことで、多くの組織が主体的に取り組むとともに、相互に協力しあうことができた

今後の取組方針

東京大会における対策から得た知見、ノウハウ（情報共有プラットフォーム（JISP）の運用、リスクマネジメントの手法等）を活かし、**我が国のサイバーセキュリティ全体の底上げを推進**

【取組の進め方等】

○ **大規模国際イベント時のみならず、持続的に取組を推進**
○ 取組の推進に当たり、**サプライチェーン管理、IoTや５G等の新たな技術やサービスの実装における安全・安心の確保、クラウドサービス等の新たなサイバーセキュリティの担い手との協調等の課題の重要性を踏まえて対象領域を拡大**
○ 取組の推進に当たり、**サイバーセキュリティ協議会をはじめとした情報共有体制間の連携を推進**
○ 我が国のサイバーセキュリティ政策に関する国際的な情報発信の中で、**東京大会における我が国の経験等を他国に共有**

我が国のサイバーセキュリティ全体の強化に向けた「リスクマネジメントの促進」及び「対処態勢の強化・拡大」

東京大会の関係組織との間で推進した対策を、持続的な取組として、我が国全体の社会経済を支える事業者等と協力関係を構築し、各組織における自律的な取組が可能となるような支援、各組織間の連携が機能するような支援を推進

リスクマネジメントの促進

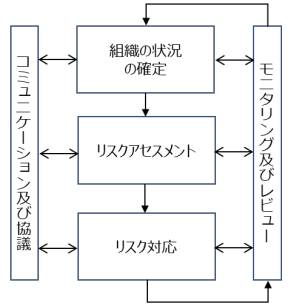
【当面の取組方針】

○　各組織による自主的なリスクアセスメントの支援　　等

○　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への政府による検証　　等

○　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　　等

リスクマネジメントのプロセス



対処態勢の強化・拡大

【当面の取組方針】

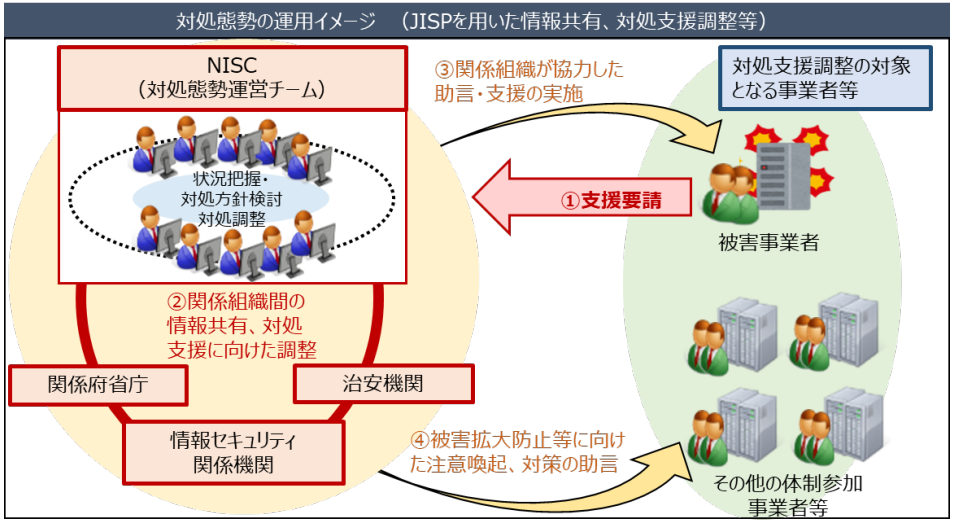
○　新たに体制に参加する組織のための説明会の開催 等

○　体制全体の対処能力の向上等を目的とした演習等のイベントの開催 等

○　対象組織に対する対処支援調整、情報提供等の支援 等

○　効率的かつ安全に情報共有を実現するためのシステムの提供　等

○　大規模国際イベントを支える組織との情報共有体制の構築準備 等



大阪・関西万博におけるサイバーセキュリティの確保に向けた取組の推進

2025年に開催が予定される大阪・関西万博に向けて、関係省庁、日本国際博覧会協会、イベントの開催・運営に必要不可欠なサービスを提供する事業者、情報セキュリティ関係機関等との間で分野横断的に連携し、イベントに関わるサービスの安定的な供給に向けた総合的な対策を推進

大阪・関西万博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
（事前対応のための取組）

(1) リスクアセスメント 【事業者等が自主的に実施する取組】

(2) 横断的リスク評価 【NISCが評価する取組】

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）

(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

参考：サイバーセキュリティ戦略（東京大会等に向けた取組の今後の活用方策関係）

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。

参考：サイバーセキュリティ戦略（東京大会等に向けた取組の今後の活用方策関係）

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。