

リスクマネジメントの促進に係る取組の推進状況

カテゴリ	具体的な取組内容（2020年12月末時点）	
(1) リスクマネジメント	1 説明会	<p>【概要】</p> <ul style="list-style-type: none"> ○ 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、リスクの低減と最新のリスクへの対応のため、リスクアセスメントの実施を依頼。 <p>【取組状況等】</p> <ul style="list-style-type: none"> ○ 対象事業者等 約300 ○ 10都道県で53回開催し、約のべ2000名が参加
	2 情報交換会	<p>【概要】</p> <ul style="list-style-type: none"> ○ NISCが作成したリスクアセスメントの手順に対する理解促進のためのワークショップ開催等。 <p>【取組状況等】</p> <ul style="list-style-type: none"> ○ 5都道県で13回開催し、約のべ450名が参加
	3 フィードバックレポート	<p>【概要】</p> <ul style="list-style-type: none"> ○ サイバーセキュリティ対策のPDCAサイクルにおける改善点や、リスクアセスメントにおいて実施が不十分な可能性がある事項等を事象者等に個別にフィードバックを実施。 <p>【取組状況等】</p> <ul style="list-style-type: none"> ○ 第3回の取組から実施し、約のべ750組織にフィードバック
(2) 横断的リスク評価	4 リスクシナリオに基づく検証	<p>【概要】</p> <ul style="list-style-type: none"> ○ サイバーセキュリティ対策の実施状況をNISC作成したリスクシナリオに沿って検証。 <p>【取組状況等】</p> <ul style="list-style-type: none"> ○ 2018年度：選定した重要サービス事業者等を対象に検証 ○ 2019年度：組織委員会等を対象に検証
	5 チェックリストに基づく検証	<p>【概要】</p> <ul style="list-style-type: none"> ○ サイバーセキュリティ対策の実施状況をNISC作成したチェックリストに沿って検証。 <p>【取組状況等】</p> <ul style="list-style-type: none"> ○ 2019年度：会場等（仮設や情報資産を持たない会場等を除く）を対象に、書面及び訪問による検証 ○ 2020年度：病院分野を対象に書面による検証を実施予定（病院業務に支障を来さない範囲で対応）
	6 技術的検証（ペネトレーションテスト）	<p>【概要】</p> <ul style="list-style-type: none"> ○ 大会の継続を支える会場の制御システムに対して、攻撃者が実際に用いる手法で実際に侵入できるかどうかの観点から対策の実施状況を検証。 <p>【取組状況等】</p> <ul style="list-style-type: none"> ○ 選定した会場を対象に検証
(3) スポーツ関係団体に対する勉強会	7 勉強会（演習含む）	<p>【概要】</p> <ul style="list-style-type: none"> ○ 2016年リオ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開催。 <p>【取組状況等】</p> <ul style="list-style-type: none"> ○ 平成29年から、隔月ペースで15回の勉強会を開催
	8 自己学習用コンテンツの提供	<p>【概要】</p> <ul style="list-style-type: none"> ○ 勉強会の理解度を確保するとともに、振り返りを通じてさらなる定着を図ることを目的に提供。 <p>【取組状況等】</p> <ul style="list-style-type: none"> ○ 2020年9～12月に、隔週で配信
	9 スポーツ関連団体向けCTI提供	<p>【概要】</p> <ul style="list-style-type: none"> ○ スポーツ関連団体に特化したサイバーインシデントに係る情報を提供。 <p>【取組状況等】</p> <ul style="list-style-type: none"> ○ 2018年2月から、隔週で配信
	10 簡易Webチェック	<p>【概要】</p> <ul style="list-style-type: none"> ○ インターネット経由でWebサイトをチェック <p>【取組状況等】</p> <ul style="list-style-type: none"> ○ 2019年度から、勉強会参加者のうち希望する団体に対して実施

対処態勢の整備に係る取組の推進状況

カテゴリ	具体的な取組内容（2020年12月末時点）	
(1) 対処支援調整	1 ワンストップでの情報連絡	<p>【概要】</p> <ul style="list-style-type: none"> ○ インシデント発生時等にワンストップで必要な組織に情報連絡できるように、JISPにおけるコミュニティ「そだんの窓口」を開設。当窓口では最新の状況から過去の経緯まで共有可能。 <p>【取組状況等】</p> <ul style="list-style-type: none"> ○ メールでの情報交換等と異なり、「意図せず関係組織外に漏洩しづらい(アクセス制御)」、「関係者が同一の情報を同時に把握可能」、「関係組織への連絡漏れを極小化できる」などの利点がある。
	2 インシデント対処支援調整	<p>【概要】</p> <ul style="list-style-type: none"> ○ 体制参加組織からの要請・相談を受け付け、必要に応じて、助言及び支援調整を実施。 <p>【取組状況等】</p> <ul style="list-style-type: none"> ○ 36件（「そだんの窓口」トピック数）
	3 対処調整センターの構築	<p>【概要】</p> <ul style="list-style-type: none"> ○ 官民問わず、CSIRTを取りまとめる組織と体制を構築。ギブアンドテイクが成立している状況でより強い信頼関係を築くことができる。 <p>【取組状況等】</p> <ul style="list-style-type: none"> ○ 参加組織数 357組織 （重要サービス事業者 152/スポンサー 39/スポーツ関連団体 67/関係省庁等 30/他 69） ○ 参加者数 2,100名
(2) サイバー攻撃への対処能力の向上	4 演習訓練	<p>【概要】</p> <ul style="list-style-type: none"> ○ 大会に向けて様々なレベルの組織における演習訓練を開催（会場に集合しないリモート形態での演習のノウハウも蓄積されている）。 <p>【取組状況等】</p> <ul style="list-style-type: none"> ○ 延べ参加組織数 397組織（内訳 第1回140/第2回 149/第3回 108） ○ 現在までに計 3 回開催（大会までに追加で 2 回の開催を予定）。
	5 説明会、意見交換会などイベント	<p>【概要】</p> <ul style="list-style-type: none"> ○ 第一回、二回の演習訓練前に説明会を開催。第三回～五回の演習訓練後は信頼関係の構築及び深耕を目的とした官民間及び異業種間の交流を行う意見交換会を開催。 <p>【取組状況等】</p> <ul style="list-style-type: none"> ○ 延べ参加組織数 406組織（内訳 第1回 242/第2回 125/第3回 39）
(3) 予防・検知に関する情報の発信・共有	6 脅威情報提供(SNS)	<p>【概要】</p> <ul style="list-style-type: none"> ○ JISPのSNS機能を用いて、体制参加組織への最新の脅威情報を提供。オープンソースを元にニュース情報を作成し、同一情報を2つのスキルレベルに書き分けて提供している。加えて、協力ベンダー等からの情報も提供。 <p>【取組状況等】</p> <ul style="list-style-type: none"> ○ 情報提供数 2,217件（対処調整センタ 797/ニュース 759件/協力ベンダー等 661件）
	7 脅威情報提供（機械連携）	<p>【概要】</p> <ul style="list-style-type: none"> ○ CTI事業者から最新の脅威情報の提供を受けるとともに、TAXIIサーバ（STIXフォーマット）により組織委員会のSIEM（セキュリティ情報管理システム）に当該情報を自動登録させ、同組織のセキュリティ対策に活用。 <p>【取組状況等】</p> <ul style="list-style-type: none"> ○ 提供インディケータ数 23,733件(国内)
	8 公開サイト等の観測	<p>【概要】</p> <ul style="list-style-type: none"> ○ セキュリティ関係機関の協力を得て、グローバルIPからのダークネットへの通信、公開サイトへの攻撃、脆弱性、攻撃予見情報等の観測を行い、対象組織に情報を提供。 <p>【取組状況等】</p> <ul style="list-style-type: none"> ○ 観測対象 URL 2,203/G-IP 1,471(申請組織数 193)、観測情報提供数 94件
	9 ダークWeb、OSINTからの情報収集	<p>【概要】</p> <ul style="list-style-type: none"> ○ 大会及び大会関係組織に関する脅威情報の収集、提供。 <p>【取組状況等】</p> <ul style="list-style-type: none"> ○ 検知した情報数 121件(有効件数)/通知数 49件 上記とは別に検知した大会関連の類似ドメイン数 274件（大会組織委員会と共有）

対処態勢の整備に係る取組の推進状況

	10 インシデント情報の共有	<p>【概要】</p> <ul style="list-style-type: none"> ○ 体制参加組織において発生したインシデント情報(IoC情報等を含む)を共有。 <p>【取組状況等】</p> <ul style="list-style-type: none"> ○ 該当情報を匿名化した上で共有
(4)情報共有プラットフォーム(JISP)の提供	11 情報共有プラットフォーム Japan cyber security Information Sharing Platformの略 (JISP、ジスプ)	<p>【概要】</p> <ul style="list-style-type: none"> ○ サイバーセキュリティ対処調整センターが提供し運用する情報共有プラットフォーム。脅威情報、インシデント情報等をワンストップで共有でき、参加組織からのインシデント報告に対して、要請に応じて助言及び対処支援調整を実施。 <p>【取組状況等】</p> <ul style="list-style-type: none"> ○ 累積のログイン数 約14.5万、参照数 約34.1万、投稿数 約0.6万、コメント数 約2.0万 (月平均 ログイン数 6,885、参照数 16,241、投稿数 270、コメント数 943)
	12 インシデント管理(JIRA)	<p>【概要】</p> <ul style="list-style-type: none"> ○ インシデントレスポンスに係るNISC内の情報共有、官邸への報告のため、インシデントレスポンス記録を蓄積 (チケット管理、ナレッジ管理を実施)。 <p>【取組状況等】</p> <ul style="list-style-type: none"> ○ 36件 (「そうだんの窓口」トピック数と同じ)