CyberNews

令和2年2月
宮城県警察本部
サイバー犯罪対策課

東京オリンピック・パラリンピック競技大会に向けたサイバーセキュリティ対策

過去のオリンピック・パラリンピック競技大会では、開催国を標的とした様々な手段のサイバー攻撃が行われています。

円滑にオリンピック・パラリンピック競技大会を運営するためには、事前のサイバーセキュリティ対策が重要となります。

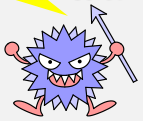
2016年リオデジャネイロ大会

- ✓ 大会開始前から、大会公式サイトへのDDoS攻撃が確認された
- ✓ ウイルス感染による情報漏えいが発生
(大会に関わる公共事業を請け負った建設会社のウェブサイトから個人情報漏えい)
- ✓ なりすましWi－Fi、ATMスキミングが設置される

- 認知した攻撃の多くはSNS等にて攻撃の予告や実施の書き込みが確認されたため、事前、早期の対応を行った

2018年平昌大会

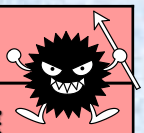
- ✓ 大会公式サイトへのサイバー攻撃により、一時的に入場チケットが印刷できない状況
- ✓ 会場内のWi－Fiが使用できない事態
- ✓ 大会に関連するフィッシングメールの増加



- 観光客に対してサイバーセキュリティに関する注意喚起を実施
- 情報共有・分析を行うことにより、運営に重大な影響を与えるサイバー攻撃は発生せず

オリンピック・パラリンピック競技大会に関する想定されるサイバー犯罪

金銭目的の犯罪	偽チケット販売サイト、ランサムウェアによる脅迫
ハクティビスト（※）による攻撃	大会サイトへの攻撃、スポンサー・競技対戦国関連サイトへの攻撃
サイバーテロ	大会システムへの侵入によるシステム破壊、重要インフラへのサイバー攻撃



※社会的・政治的な主張を目的としたハッキング活動を行う者

各企業が実行すべき取組

① セキュリティに関する組織全体の対応方針を定める
② セキュリティ対策のための予算や人材などを確保する
③ 必要と考えられる対策を検討し、実行する
④ セキュリティ対策に関する見直しを行う
⑤ 緊急時の対応や復旧のための体制を整備する
⑥ 委託や外部サービスを利用する際は、セキュリティに対する責任を明確にする
⑦ セキュリティに関する最新の動向を収集する