Ksisnetだより

発行:Ksisnet事務局
令和 3年 5月14日
Vol.93

東京五輪に向けた情報セキュリティ対策について

東京オリンピック開幕まであと２ヶ月と迫りました。オリンピックのような大規模イベントは世界中の注目が集まり、巨額な資金が動くことから、様々な組織などがこの機会を狙って利益を得ようとしたり、単に開催国にダメージを与えるためにサイバー攻撃をしかける可能性があり、我が国は今まで以上にサイバー攻撃のリスクに晒されると考えられます。

こうした状況下においては、オリンピックに直接関わりのない企業や組織であっても、開催国にあるというだけで攻撃の対象になり得ることから、全ての企業があらゆる攻撃に備えておく必要があります。

サイバー攻撃による被害を軽減するため、情報セキュリティ対策を万全にしましょう！

「情報セキュリティ対策の基本」

攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消し攻撃によるリスクを低減
ウイルス感染	セキュリティソフトの利用	攻撃をブロック
パスワード窃取	パスワードの管理・認証の強化	パスワード窃取によるリスクを低減
設定不備	設定の見直し	誤った設定を攻撃に利用されない
誘導（罠にはめる）	脅威・手口を知る	手口から重要視するべき対策を理解

多数の脅威があるが「攻撃の糸口」は似通っており、基本的な対策の重要性は長年変わらない。

参考　ＩＰＡ（情報処理推進機構）

IoT機器の情報セキュリティ対策

リオデジャネイロオリンピックでは、IoTを利用したDDos攻撃が問題となりました。

IoT機器はCPU性能やメモリー容量が少なく、セキュリティソフトを導入できないことから、攻撃対象として狙われやすいと考えられます。IoT機器の更なる普及により、今大会では更に多くの攻撃が予想されます。

IoT機器をインターネットに直接接続せずに、**セキュリティ対策を行っているネットワークに接続する**ことが有効な対策となります。今一度IoT機器を見直し、インターネットに**接続する必要がなければ接続しない**ということが最も有効なセキュリティ対策であるといえます。

ランサムウエアによるサイバー攻撃に注意

昨年11月に大手ゲーム会社が不正アクセスにより顧客情報が盗まれた上、システムデータが暗号化される被害に遭い、情報の暴露の取りやめとデータ暗号化の解除を引き換えに身代金を要求される**「二重脅迫型」ランサムウエア被害**に遭ったことは記憶に新しいところです。

オリンピック開幕が近づき、再びランサムウエアによるサイバー攻撃が活発になり、本年４月30日付でNISC（内閣サイバーセキュリティセンター）から注意喚起が発出されています。ランサムウエアの感染を防止するための具体的対応策等について掲載されていますので、参考にして下さい。

昨年12月８日付発行しました「Ksisnetだより第88号」でも、**「二重脅迫型」ランサムウエア被害**について解説していますので、こちらも是非ご確認下さい。

「ランサムウエアによるサイバー攻撃に関する注意喚起について」（NISC）
https://www.nisc.go.jp/active/infra/pdf/ransomware20210430.pdf