Ksisnetだより

発行:Ksisnet事務局
令和 2年 2月 4日
Vol.73

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６ヶ月を切りました。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、巨額の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、日本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、開催地である日本にあるというだけで攻撃の対象になりえることから、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。

実は基本的な情報セキュリティ対策が万全であれば、サイバー攻撃のおよそ80%は防げるのです！

「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）

基本的な情報セキュリティ対策を行ったら...

社員教育を徹底しましょう

情報セキュリティ対策を完璧に行っても、担当者以外の社員に知識がないと、人がセキュリティ・ホールとなり、情報漏えいや攻撃などが起こる可能性があります。

担当者だけでなく、全ての社員が情報セキュリティに対する基本の知識を持ち、自分自身が情報セキュリティ対策の当事者であることを認識する必要があります。

また、情報セキュリティに関する社内でのルールを整備し、新しい情報などを迅速に社内共有できるような連絡体制を確立することも重要です。

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。

会社全体で再度情報セキュリティ対策を徹底し、オリンピック開催に伴い増加するであろうサイバー攻撃に遭うリスクを減らしましょう！