#	ご質問	回答
私たちにできること		
1	職場のPCから業務とは無関係のサイトを閲覧して、画面に掲載された広告などからウイルス感染するケースがあるとのことでした。現代社会では、職場でwebサイトを閲覧しないという規制は難しいと感じます（業務で必要な場合もあるため）。広告を誤ってクリックしないよう注意する、という対応がベターなのでしょうか？職場のWi-Fiを利用して、スタッフ個人がスマホを利用しています。NTT東日本提携会社のセキュリティ診断を受けたところ、そのようなルート（個人スマホを介して）でも、ウイルス感染などが発生するリスクがあると指摘されました。こちらも規制が難しいと感じます、どのように対応するのがよいのでしょうか？	お伝えしたのは勤務時間中に業務とは関係ないサイトを閲覧することはリスクにつながる、ということですので、業務上必要な場合はそれは業務ですので規制する必要はないかと思います。また、広告を誤ってクリックしないように、というよりもそういうリスクがあることの注意喚起、さらにこういうメッセージ（偽メッセージ）が表示された場合は自分ひとりで対応せず、担当部署に相談することを周知することが大切です。 個人スマホについてはスマホが感染していた場合、PCにケーブルなどでつなげることでUSBメモリをPCにつなぐのと同じように、そこからPCに感染させる可能性があります。また、スマホも外部記憶装置となりますので、PCからスマホにデータを移すことが可能ですので、情報漏えいのリスクもあります。 ただ個人のスマホのセキュリティ対策をすべて確認するわけにもいきませんので、リスクが大きいと判断した場合は、業務用のWi-Fiとゲスト用のWi-Fiを別々に設置してプライベートの利用はゲスト用Wi-Fiを利用してもらうなどの対策をするとよいでしょう。またPCのUSBから充電をするためにスマホを接続することもあるかもしれませんが、情報漏えいのリスクを考えると充電する場合は直接電源からしてもらったり、別途充電ステーションを用意したりするなども工夫としてできるかと思います。
サイバー攻撃の実情		
1	①日本におけるサイバー攻撃の事例を確認する方法はあるのでしょうか？ ②医療機関に対するサイバー攻撃の詳細（病床数，患者数，スタッフ数，攻撃の種類など）をまとめたものはあるのでしょうか？	①サイバー攻撃に関しては公開されなければわからない情報ですのですべてを確認することはできません。公開情報についてはセキュリティ関連のニュースサイト等をこまめにチェックするとよいでしょう。 ②医療機関に対するサイバー攻撃の詳細も同様で、一般的に、公開された情報のみとなります。