情報提供資料｜2021年7月
（データ基準日：2021年7月21日）

オリンピック・パラリンピック開催期間中

ここを押さえよう！サイバーセキュリティ対策のツボ

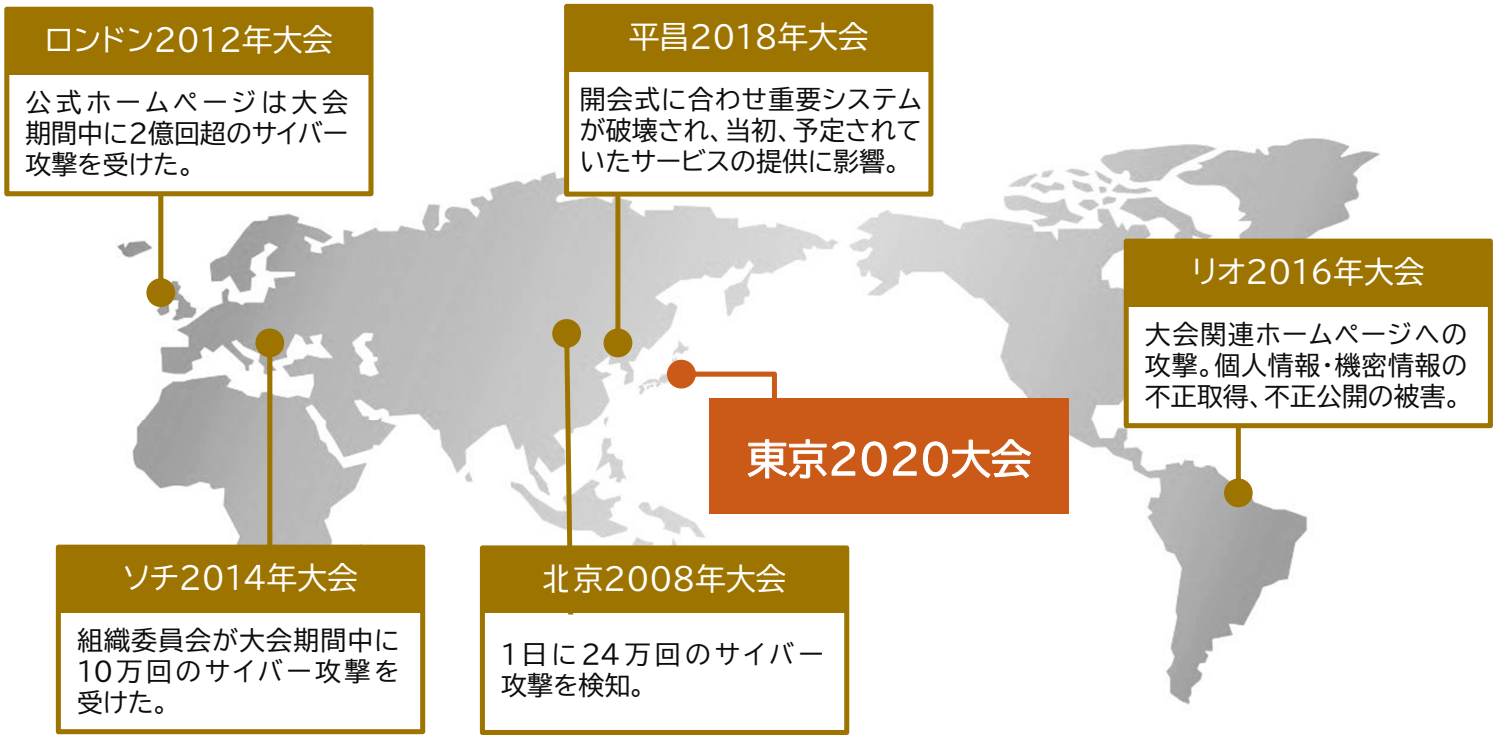
世界的なイベントはサイバー攻撃の標的に

世界からの注目度が高いイベントは、主義主張を目的としたサイバー攻撃の対象となりやすい傾向があります。

今回は開催目前の『オリンピック』が、過去に開催された際、主催国・組織委員会が攻撃の対象となったサイバー攻撃についてご紹介します。

今後、スタジアムや公共交通機関などの関連インフラも攻撃の対象となる可能性があり、そうした場合にはサイバーセキュリティに対する関心がさらに高まることが予想されます。

オリンピック・パラリンピックに関連するサイバー攻撃例



東京2020大会もすでにサイバー攻撃を！

東京オリンピック・パラリンピックの1年延期が決まった直後の2020年4月、JOC（日本オリンピック委員会）はサイバー攻撃を受け、業務が停止する被害を受けました。
専門業者の調査では、ランサムウェア（身代金ウイルス）に感染させるサイバー攻撃によるものと判明したと報道されていますが、犯行声明や金銭の要求などは「一切なかった」としており、妨害目的とも考えられます。
なお、約60台あるパソコンやサーバーすべてを1カ月かけて入れ替え、JOC幹部の説明では、約3千万円の費用がかかったとされています。

（出所）JCIC（一般社団法人 日本サイバーセキュリティ・イノベーション委員会）の資料、各種報道を基に三菱UFJ国際投信作成

・上記はオリンピック・パラリンピックに関連するサイバー攻撃例であり、すべてを網羅するものではありません。

あなたの情報を守るために！

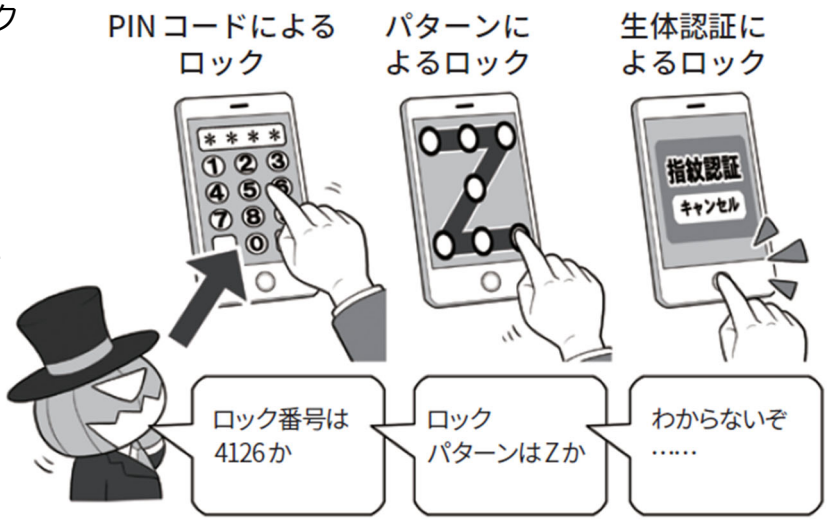
個人でできる「サイバーセキュリティ対策」

対策例 1

スマートフォンは情報の金庫！こまめにロックを！！

2021年、日本人のスマートフォン保有者は1億人を超えることが予想されています。これは、日本の総人口の約83%にあたります。

- スマートフォンの情報を守る第一歩は、待ち受け時にロックすることです。
  ロックには、「PINコード」、「パターン」、「生体認証」とさまざまなパターンがあります。
- 一方、ロック機能を設定してもロック解除したまま、その場を離れたり、他人に貸してしまったり。
  また推察しやすいコードなども危険！
  一瞬で情報を盗んだり、乗っ取ったりすることが可能です。必ず自分のそばに置き、こまめにロックをかけた状態にしましょう。



対策例 2

アプリごとにPINコードをかけられる場合はかける！

- SNS用のアプリなどには、本体のロックとは別にアプリ用のPINコードなどを設定できるものもあります。
  盗難などの際、SNSの内容などを見られたくなければ、PINコードも設定しましょう！

※一部の機種では、顔認証や指紋認証など、いわゆる「生体認証」でロック解除に利用できるものもあります。

（出所）内閣サイバーセキュリティセンター（NISC）「インターネットの安全・安心ハンドブック」、statista、総務省統計局のデータを基に三菱UFJ国際投信作成

・上記は個人でできると考えられるサイバーセキュリティ対策であり、すべてを網羅するものではありません。画像はイメージです。

対策例 3　屋外ではむやみに公衆無線LANを使用しない。

情報漏れには、攻撃者による無線LANを使った盗聴やデータの盗用などがあります。

- そもそも、自分と「契約関係がない」ものは基本的には使わない！
  また、その中でも運営主体がわからない無線LANは絶対に使用しないようにしましょう。

対策例 4　偽宅配「メールで不在通知？それ偽物かも！？」

- オリンピック・パラリンピック期間中、特に開催地域では、宅配便の遅れなどが生じるケースもあるとされています。
- ショートメッセージ（SMS）で宅配便の不在通知が来た場合、これは業者を装って偽サイトに誘導し、個人情報やパスワード等の重要な情報を入力させて騙し取ったり、ウイルスに感染させる手口です。
- 宅配業者はショートメッセージで不在通知を送らないので、メッセージは無視しましょう。また、ショートメッセージに記載されているアドレスはクリックしてはいけません。

対策例 5　ライブ配信を騙るフィッシング詐欺に注意！

- 東京2020オリンピック聖火リレーで、聖火リレーの無料ライブ配信を装い、動画を閲覧するために個人情報やクレジットカード情報などの入力を求めるフィッシングサイトが確認されています。
- オリンピック・パラリンピック競技大会の開催中も競技をライブ配信すると騙るフィッシングサイトの出現が予想されます。

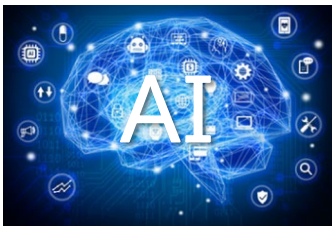
①ウイルス対策ソフトを導入し、OSやアプリは常に最新バージョンに更新した状態にする。
②動画配信サービスやSNSに貼り付けられたリンクやURLを安易にクリックしない。
③あらかじめ正規の動画配信サイトを、お気に入りに登録しておく。
④安易に個人情報等の入力はしない。

等の対策方法を確実に行い、フィッシング詐欺に注意しましょう。

※フィッシングとは、攻撃者がターゲットから、お金につながる情報や個人情報を盗み取るための詐欺。
フィッシング（phishing）は洗練された（sophisticated）＋釣る（fishing）から来ている。

（出所）内閣サイバーセキュリティセンター（NISC）「インターネットの安全・安心ハンドブック」、警視庁HPを基に三菱UFJ国際投信作成

・上記は個人でできると考えられるサイバーセキュリティ対策であり、すべてを網羅するものではありません。画像はイメージです。



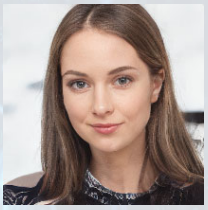
Column
サイバー攻撃とサイバーセキュリティでより重要となる人工知能（AI）

増加・高度化するサイバー攻撃に手動で対処することはもはや不可能といえ、AIによる自動検出・対応が今後のセキュリティで重要な役割を果たすと考えられています。
一方、AIの発展は皮肉にもサイバー攻撃の多様化にもつながっており、2020年の米大統領選においても「フェイクニュース」などが話題となりました。また、AIが創り出した実在しない人物画像を使用した「ディープフェイク」は動画や音声でも使用されており社会問題化しつつあります。ディープフェイクは選挙時の情報操作による有権者の誘導や顔認証回避といった悪用が考えられ、コンピューターシステム自体の弱点ではなく、人間のすきを突く手法になります。

こうしたデマ情報の拡散が攻撃手段となり、心理的な社会の分断などを意図的に行うなど、将来的にはAIが状況に応じて瞬時にフェイク動画を生成し、人々を貶めるような誤情報を拡散させることも可能となるとみられます。
クラウドストライク社によると、同社は世界初のクラウド上で動作するサイバーセキュリティプラットフォームを提供し、毎週2．5兆ものデータを学習させるなど、AIを活用しています。こうしたAIを中心とした攻防は今後も目が離せません。

AIが生成した人物画像例

「ディープフェイク」とは「深層学習」（deep learning）と、偽物を意味する「フェイク」（fake）を組み合わせた造語。
写真はAIが創り出した実在しない人物の画像。



（出所）写真AC

（出所）各種情報、CROWDSTRIKE（WE STOP BREACHES, December 2019）を基に三菱UFJ国際投信作成

・上記は、将来の運用成果等を保証するものではありません。個別銘柄の推奨を目的とするものではありません。画像はイメージです。

本資料に関するご注意事項等

- 本資料は、サイバーセキュリティに関する情報提供のために三菱UFJ国際投信が作成した資料であり、金融商品取引法に基づく開示資料ではありません。販売会社が投資勧誘に使用することを想定して作成したものではありません。
- 本資料の内容は作成時点のものであり、将来予告なく変更されることがあります。
- 本資料は信頼できると判断した情報等に基づき作成しておりますが、その正確性・完全性等を保証するものではありません。

本資料の作成は

三菱UFJ国際投信

三菱UFJ国際投信株式会社
金融商品取引業者　関東財務局長（金商）第404号
加入協会：一般社団法人投資信託協会
一般社団法人日本投資顧問業協会

FP21-07191

※本資料の【本資料に関するご注意事項等】の内容を必ずご覧ください。