



サイバーセキュリティの置き薬

2021年
第8号

オリンピック・パラリンピックに乗じたサイバー犯罪にご注意ください。

2020年東京オリンピック・パラリンピック競技大会の開催に乗じた金銭目的の詐欺やなりすましメール、偽サイト等によるサイバー犯罪の被害にご注意ください。



チケット詐欺サイト等に注意！

偽チケットや模造品の販売サイトなど、偽サイト・詐欺サイトに注意！

都職員、組織委員会の関係者から、次の情報等を問い合わせることはありません。

- ・TOKYO2020 関連の ID、パスワード
- ・クレジットカード情報、金融機関の口座情報
- ・クレジットカード、キャッシュカードの提出や控えを送るよう依頼する



参考：「東京 2020 大会公式ウェブサイト」より



URL 等で公式サイトか確認！ブックマーク等も活用する！



不審なメール、SNS メッセージ、SMS 等によるフィッシングに注意！

巧妙な文言や類似した URL が用いられたフィッシングメールに注意！

不審なメール等に記載されているリンクや添付ファイルを安易にクリックすると、フィッシングサイトに誘導されたり、コンピュータウイルスに感染するなど危険です。



身に覚えのないものや不審な内容のものは、本文中のリンクや添付ファイルを安易にクリックしない！

対策の基本

- ID、パスワードの管理を徹底する
アカウントの管理をしっかり行うことが大切です。
また、同じパスワードを使い回さず、複雑で長いパスワードに設定しましょう。
- スマートフォンやパソコンの情報セキュリティ対策を行う
OS やアプリは常に最新の状態にし、ウイルス対策ソフト等を利用しましょう。
- 不審なメールに記載されているリンクや添付ファイルはクリックしない
クリックすると、フィッシングサイトに誘導されたり、コンピュータウイルスに感染するなどし、情報を窃取されるおそれがあります。
- 脅威や攻撃の手口を知っておく
巧妙な手口が増えてきているため、脅威や攻撃の手口を知って、対策をとりましょう。



万が一被害に遭った場合は、警察など関係機関にご相談ください。



参考：(公財)東京オリンピック・パラリンピック競技大会組織委員会ウェブサイト
東京 2020 大会公式ウェブサイト内「お知らせ」-「チケット・模造品・寄付金等の不正サイト・メールや詐欺にご注意ください」<https://olympics.com/tokyo-2020/ja/news/notice-0006>
NISC「小さな中小企業と NPO 向け情報セキュリティハンドブック」