愛知県警察
サイバー犯罪対策課

# サイバー犯罪対策通信

第R８-２１号
組織向け

# 大規模な大会を狙うサイバー犯罪

狙われるのは、会場だけではありません

## ①企業ネットワークの脆弱性を狙った脅威

大規模な国際スポーツ大会では、大会関係組織だけでなく、スポンサーや委託先のほか、宿泊・運輸・警備・IT事業者など開催地域の企業もサイバー犯罪の対象となる可能性があります。

### 金銭を奪う（恐喝）

ランサムウェアによる身代金要求が行われ、業務停止による影響が大きくなります。

### 業務を妨害する

ウェブサイトの予約、物流、決済、通信などを停止させ、大会運営や地域経済に混乱を与えることが目的となる場合があります。

### 情報を盗む（情報窃取）

従業員、顧客、宿泊者、取引先の情報やメールアカウント、パスワードが盗まれるおそれがあります。

### 取引先への侵入の足掛かりにする（踏み台）

セキュリティ対策が比較的弱い委託先等を侵害し、大会関係組織・大企業のシステム侵入への足掛かりとする場合があります。

### 今すぐ確認！6項目チェックリスト

- ☑ VPN・UTM・ルータ等を最新の状態にしているか
- ☑ メール、VPN、クラウドサービスに多要素認証を設定しているか
- ☑ 貴重なデータをネットワークから切り離してバックアップしているか
- ☑ インターネット上に不要な管理画面やポートが公開されていないか
- ☑ 管理者用パスワードを使い回ししていないか
- ☑ 不審なログインや大量の通信を確認できるか

## ②大規模大会に便乗する詐欺等の脅威

注目度の高いイベントの開催時期は、インターネット上において、人々の関心に乗じたり、関連の取引を装った犯罪の発生が懸念されます。

### フィッシング

大会や協賛企業、取引先などを装い、メールやSMSで偽サイトへ誘導し、ID・パスワードやクレジットカード情報などを盗み取る手口です。

### BEC（ビジネスメール詐欺）

取引先を装い「支払いの振り込み先が変更された」、上司を装い「協賛金を指定する口座に振り込むように」などと偽のメールを送り、犯人の口座にお金を振り込ませる手口です。

### チケット詐欺

大会のチケット販売を装い、偽造チケットを販売したり、偽の公式サイトやSNS、フリマアプリなどでチケットの販売・譲渡を持ちかけ、代金をだまし取る手口です。

### 被害を防ぐためのポイント

- ☑ 送信元を確認！
  メールアドレスやドメインをよく確認しよう
- ☑ メールのリンクを押さない！
  リンク先は安易に押さず、必ずURLや送信元を確認しよう
- ☑ 別ルートで確認！
  取引先や銀行の依頼は、必ず公式ホームページ等で確認しよう
- ☑ 社内で共有・教育！
  全従業員のセキュリティ意識を高めよう

「大会とは関係ない会社だから大丈夫」ではありません！！

愛知県警察
サイバー犯罪対策課

# サイバー犯罪対策通信

第R８-２２号
組織向け

# お盆休み前後に確認！

## セキュリティ担当者向け　休暇前の重点確認

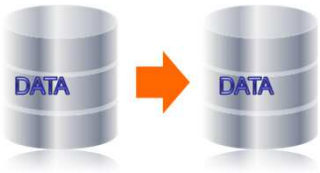
### 緊急対応体制

- ☑ 緊急連絡体制の確認
- ☑ 委託先・保守会社の連絡先確認

### 更新状況の確認

- ☑ VPN機器
- ☑ ファイアウォール
- ☑ NAS・ストレージ
- ☑ 公開サーバ

### バックアップ




- ☑ 最新バックアップの取得
- ☑ バックアップの保管方法（オフライン保管等）に注意

### 公開資産の確認

- ☑ 不要サービスの停止
- ☑ 公開ポートの確認
- ☑ 脆弱性情報の確認と対応

## 全従業員向け　従業員も要確認

### パソコンを最新の状態にする

- ☑ Windowsの更新
- ☑ ソフトウェアの更新

### 不審なメールに注意

- ☑ 配送通知・請求書等を装うメールに注意
- ☑ 休暇中、社員・関係企業等をかたるメールに注意

### 使用しない機器の電源をOFFにする

- ☑ 使用しないパソコンの電源OFF
- ☑ ネットワーク接続機器の電源OFFの要否確認

## 会社が休みでも、犯罪者は休みません

## ～生活安全総務課からのお知らせ～

**店舗・事業所の侵入盗対策**

店舗の現金はゼロ！
機械警備の導入！
施設内にある高額な商品や資機材等は確実な管理を！