2021 年 09 月 24 日

サービス＆セキュリティ株式会社 e-Gate センター

東京オリンピック・パラリンピックのセキュリティインシデントの振返りと フィッシング件数増加の注意喚起

1. 概要

東京オリンピック・パラリンピック(以下東京オリパラ)は様々なサイバー攻撃が行われることが予想されていました。

そこで 2021 年 7 月のセキュリティニュースでは、過去のオリンピックでのサイバー攻撃の事例からサプライチェーン攻撃に焦点を当て、その手法と対策を紹介いたしました。幸い予想された大規模な攻撃の発生は東京オリパラ期間中に発生したという報道はありませんでした。しかし、東京オリパラとの関連性は不明ですが、個人を狙ったフィッシング攻撃が活発に行われており、フィッシング報告件数の増加が見られました。

今回は東京オリパラでのセキュリティインシデントに関する振り返りとフィッシング攻撃に関する最新動向と対策について紹介いたします。

2. 東京オリパラで確認されたサイバー攻撃

2021 年 7 月のセキュリティニュースでご紹介した通り、過去のオリンピックにおけるサイバー攻撃は主に、大会本部や競技会場を狙った標的型攻撃と個人を狙った攻撃に二分されます。

攻撃事例の詳細は 2021 年 7 月のセキュリティニュースをご参照ください。
『注意喚起：オリンピックにおけるサイバー攻撃事例とセキュリティ対策』
https://www.ssk-kan.co.jp/topics/?p=11853

東京オリパラでは大会本部や競技会場を狙った目立つ攻撃の発生は報じられませんでした。しかしサイバー攻撃が何も起こらなかったわけではなく、東京オリパラに乗じた不特定多数の個人を狙うフィッシングサイト（後述）が観測されました。

無観客開催により大会のライブ配信が盛んに行われました。直接競技会場を狙った攻撃ではなく、このライブ配信サイトを騙ったフィッシング攻撃発生について報じられています。また、関連する自治体や団体等になりすました偽サイトなどもあると報じられています。

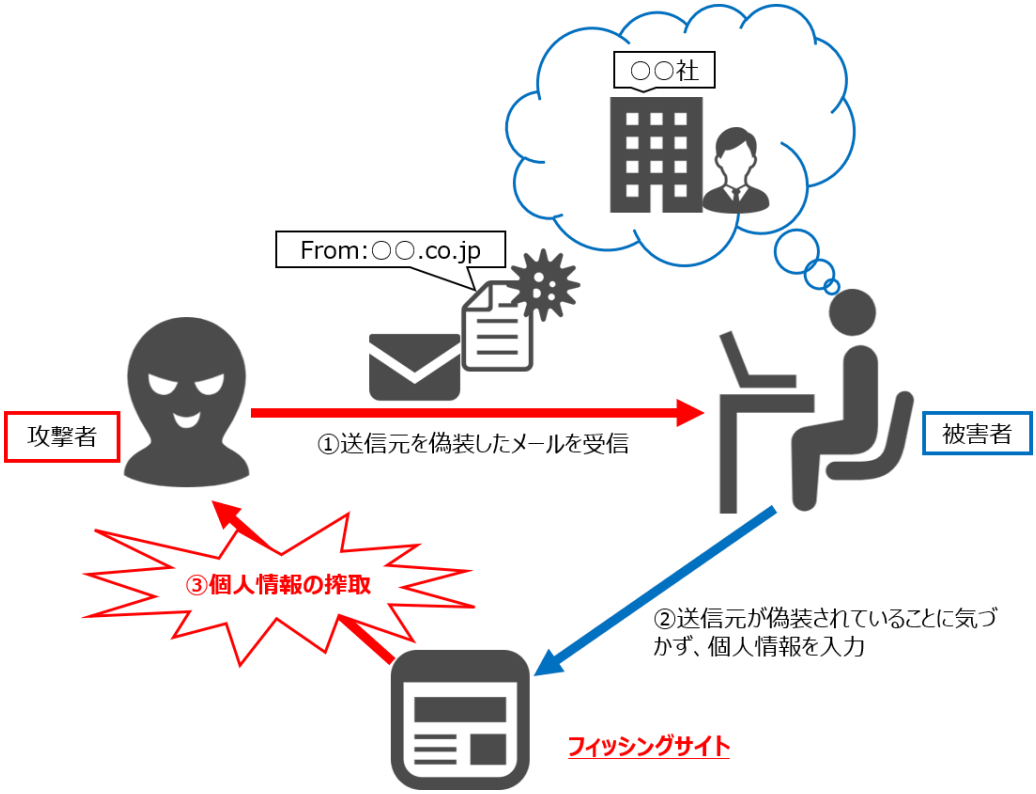
東京オリパラのセキュリティインシデントについては今後、組織委員会、関係機関などから発表があると思われますが、近年の大会としては大きなセキュリティインシデントがなかった大会と言えるのではないでしょうか。

3. フィッシング攻撃の最新動向

フィッシング攻撃とは、攻撃者が金融機関や有名企業を騙って送信した「フィッシングメール」から、受信者を本物そっくりの WEB サイトである「フィッシングサイト」へと誘導します。そこでクレジット番号やパスワードを入力させ、個人情報を奪うことを目的とした攻撃です。9 月 2 日にフィッシング対策協議会から公開されたフィッシング報告状況によると、2021 年 8 月のフィッシング攻撃の報告件数は 2021 年 7 月より 18,390 件増加し、53,177 件となり、高い増加傾向にあります。

3.1 「メールスプーフィング」による巧妙化

フィッシング対策協議会の行った調査によると、有名ブランドを騙って大量に配信されるフィッシングメールの約 90.7%が「メールスプーフィング」を施したものでした。「メールスプーフィング」とは、送信元メールアドレスを偽装し、正規のメールアドレスになりすますことです。差出人メールアドレスが正規のドメインであるため、受信者が正規メールか否か判別することが難しく、本文中の URL をクリックしフィッシングサイトに誘導されるケースが増えております。

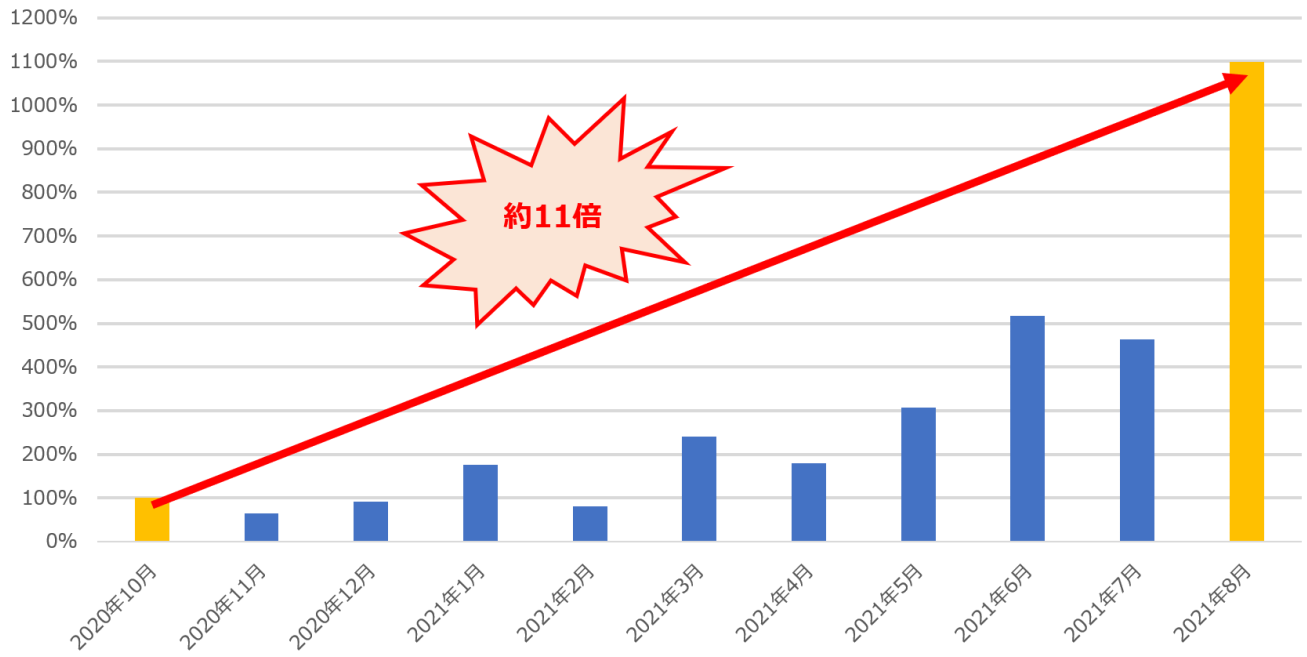


【図 1】「メールスプーフィング」によるフィッシング攻撃

3.2 e-Gate センターでの観測状況

e-Gate センターでも多くのフィッシングメールを検知しております。過去 2020 年 10 月、2021 年 5 月にフィッシング件数の増加について取り上げましたが、その後も継続して検知件数は増加しており、2021 年 8 月には 2020 年 10 月と比べて約 11 倍のフィッシングメールを検知しております。

過去に取り上げているフィッシング件数の増加については、以下の記事をご参照ください。
『フィッシング件数の急増について』（2020 年 10 月）
https://www.ssk-kan.co.jp/topics/topics_cat05/?p=11188
『ニューノーマル時代によるセキュリティインシデントの移り変わり』（2021 年 5 月）
https://www.ssk-kan.co.jp/topics/topics_cat05/?p=11682



【図 2】e-Gate センターにおけるフィッシングメール検知件数
（2020 年 10 月を 100%として算出）

3.3　注目すべきフィッシング攻撃　――新型コロナウイルスに乗じた偽サイト

また、新型コロナウイルスのワクチン接種に乗じたフィッシングメールも検知しております。e-Gate センターで検知したフィッシングメールの本文中にあった URL にアクセスしてみたところ、【図 3】のようなワクチン接種予約の偽サイトに誘導されました。本物のサイトのコピーで一目見た限りでは偽物判別することが難しくなっています。フィッシング攻撃は常に注目が集まる話題に乗じて行われるため、今後も注意が必要です。

【図 3】ワクチン接種予約サイトに似せたフィッシングサイト

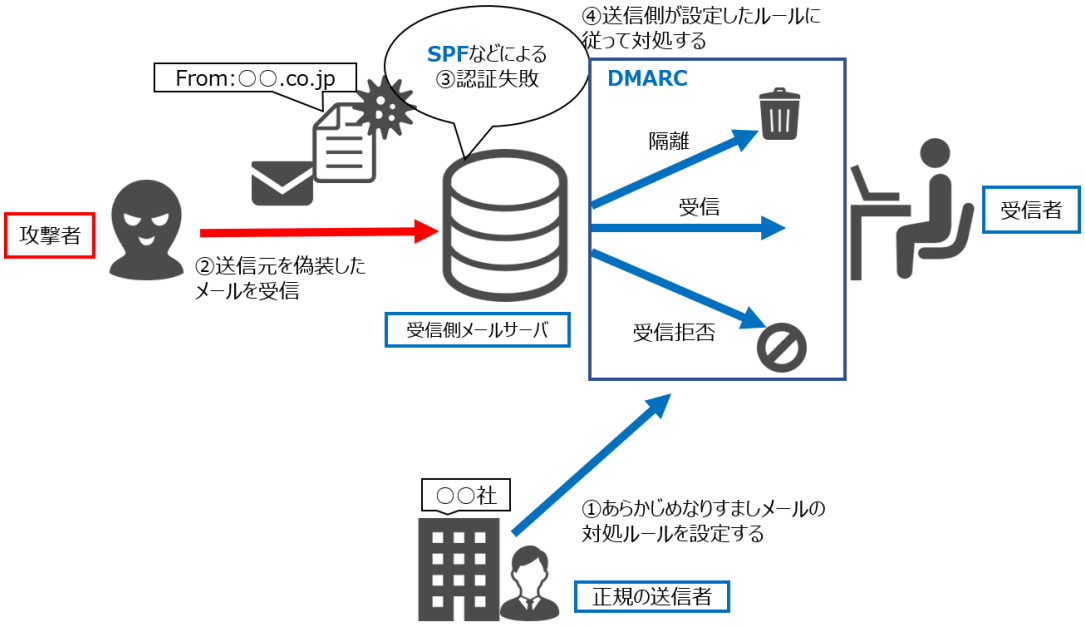
4. フィッシング攻撃対策

オリンピック・パラリンピックや新型コロナウイルスの蔓延など社会状況が移り変わる中で、特定の企業や組織を狙った標的型攻撃だけではなく、引き続き不特定多数の個人を狙った攻撃にも注意を払う必要があります。フィッシング攻撃の被害件数は今後も増加すると考えられるため、対策を講じる必要があります。

4.1 フィッシングメール対策の強化方法

3.1 のとおり、受信したメールがフィッシングメールかどうかを判断することがますます困難になっております。その中で一般的なメールソフトでは、送信元ドメインを認証する技術を導入しており、その一つが SPF(Sender Policy Framework)です。SPF とは、送信元サーバの IP アドレスと DNS を利用してあらかじめ想定された送信元以外からのなりすましメールを検出できるようにする仕組みのことです。

さらに、SPF などで「なりすましメール」と判定されたメールがメールソフトのユーザーに届かないようにする技術として、DMARC(Domain-based Message Authentication, Reporting and Conformance)も順次導入されています。DMARC とは、あらかじめ送信ドメイン管理者が、受信側のメールサーバで SPF などによって送信元ドメインの認証が失敗した際に、そのメールをどう処理するかを送信ドメイン管理者が宣言する仕組みです。この技術により、受信したメールが正規のものであるかどうかを受信側が判定する負担が軽減され、より高い確率でフィッシング攻撃の被害を防ぐことが出来ます。



【図 4】DMARC によるなりすましメールの判定

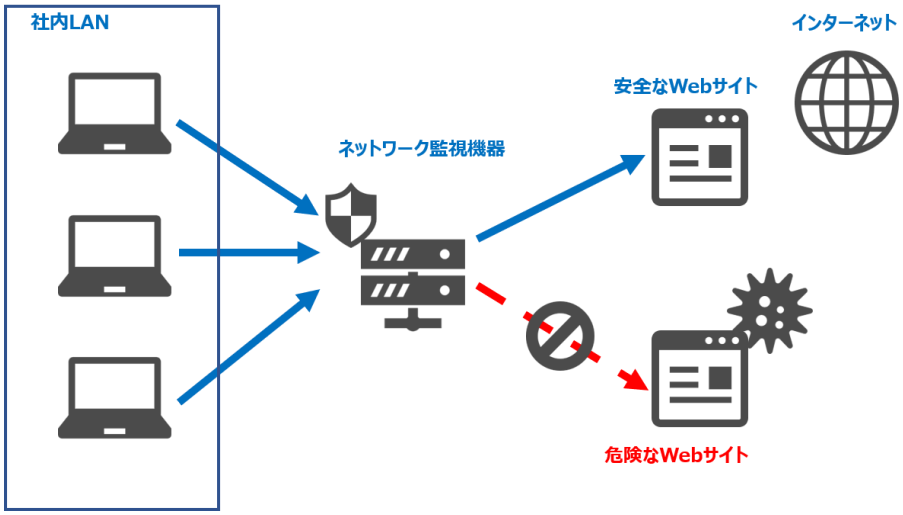
また、Office 365 のメールフィルタリングサービスである「Microsoft Defender for Office 365」のように、フィッシングメール対策ポリシーの設定を行うのもフィッシングメールの受信を防ぐ上では有効です。

フィッシングの被害にあうのを防ぐためには、SPF、DMARC などの認証技術を導入するメールソフトを使用し、フィッシングメール対策ポリシー設定を行うだけではなく、以下の対策も実施する必要があります。

- メールから直接 WEB サイトにアクセスしないようにする
- 「重要」「緊急」などの急かす文言に焦らない
- 電子署名の確認

4.2 ネットワーク監視機器の導入

しかし、これらの対策を念入りに実施するには多大な労力がかかってしまい、通常の業務に支障をきたすおそれがあります。その場合、ネットワーク監視機器を導入し、フィッシングサイトを検知、防御することも有効です。さらに、ネットワーク監視機器が出力するログを分析し、危険性を判断することで、セキュリティインシデントの未然防止や早期発見による即時対応が可能となります。



【図 5】ネットワーク監視機器によるフィッシングサイトの検知・防御

しかし、社内だけでこれらの運用を行うには多くのコストがかかってしまいます。そこで、外部の SOC（セキュリティオペレーションセンター）にネットワーク機器の運用をアウトソーシングするという手段があります。

5. 参考情報

・Kaspersky
オリンピックに乗じたオンライン詐欺：5 つのパターン
https://blog.kaspersky.co.jp/olympic-scams-top-5-schemes/31272/

・トレンドマイクロ
新型コロナウイルス「Covid-19」のワクチン接種に便乗する脅威
https://blog.trendmicro.co.jp/archives/28421

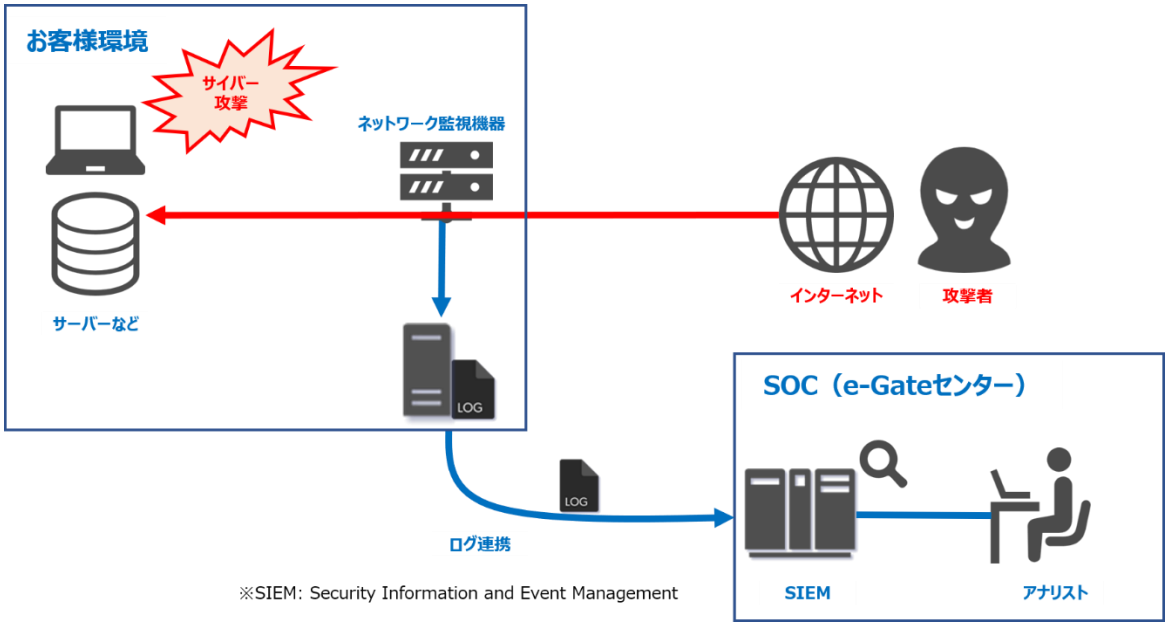
・フィッシング対策協議会
2021/08 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202108.html

6. e-Gate の監視サービスについて

e-Gate のセキュリティ機器運用監視サービスでは、24 時間 365 日、リアルタイムでセキュリティログの有人監視を行っております。サイバー攻撃への対策としてセキュリティ機器を導入する場合、それらの機器の運用監視を行い、通信が攻撃かどうかの分析、判断をして、セキュリティインシデント発生時に適切に対処できるようにすることが重要です。e-Gate のセキュリティ監視サービスをご活用いただきますと、迅速なセキュリティインシデント対応が可能となります。

また、e-Gate の脆弱性診断サービスでは、お客様のシステムにて潜在する脆弱性を診断し、検出されたリスクへの対策をご提案させていただいております。

監視サービスや脆弱性診断サービスをご活用いただきますと、セキュリティインシデントの発生を予防、また発生時にも迅速な対処が可能なため、対策コストや被害を抑えることができます。



【図 6】e-Gate の監視サービス

■総合セキュリティサービス e-Gate

SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた「IT 運用のノウハウ」と最新のメソッドで構築した「次世代 SOC“e-Gate センター”」。この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルにサポートするのが SSK の“e-Gate”サービスです。e-Gate センターを核として人材・運用監視・対策支援という 3 つのサービスを軸に全方位のセキュリティサービスを展開しています。

【参考 URL】

https://www.ssk-kan.co.jp/e-gate/

※本資料には弊社が管理しない第三者サイトへのリンクが含まれています。各サイトの掲げる使用条件に従ってご利用ください。
リンク先のコンテンツは予告なく、変更、削除される場合があります。

«お問合せ先»
サービス＆セキュリティ株式会社
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-3499-2077
FAX 03-5464-9977
sales@ssk-kan.co.jp