NET ASSIST
24/7 Guardian Deity

NEWS LETTER

2022.02
#10

TOPICS

ご利用頂いていますか？
意外と便利なネットアシストお客様ポータル！

第1回 サービスデスク直通フォーム

ネットアシストでは、ご契約者様専用の「お客様ポータル」というシステムをご提供しております。弊社内の監視運用システムとも連携している独自開発のポータルサイトです。ご請求書はこちらのポータルサイトよりダウンロード頂く形式ですので、ご契約社様はほとんどご利用頂いていると思いますが、「請求書の発行時にしか利用したことがない」「活用方法がわからない」というお客様向けに、本連載でお客様ポータルの活用方法をご紹介していきます！

「サービスデスク直通フォーム」を活用する

サーバ監視保守運用サービス（MSPアシスト）のご契約社様は、障害発生時のお問合せや作業依頼など、弊社エンジニアに日々様々なご連絡を頂いております。そこでぜひ、お客様ポータルの機能の1つである「サービスデスク直通フォーム」をご利用ください。

1 ポータルログイン後、TOPページの左の一番上にありますので、こちらをクリック！

2 ご依頼者様の情報を入力する画面にとびますので、ご担当者様のお名前・電話番号・メールアドレスをご入力ください。

POINT

・ご入力いただいたメールアドレスには、問合せの受付メールが送られます。

・依頼完了後には入力情報が保存されますので、同じご担当者様のご依頼であれば再度の入力は必要ありません。

対象サーバを選択する画面の次は、ご依頼内容の入力画面にうつります。こちらに詳細を入力頂き、依頼内容の確認をクリックしてください。

4 ここに依頼内容の詳細をご入力ください

POINT

・対象サーバが不明の場合は「対象サーバ不明」を選択してください。

・エンジニア直通のフォームとはなりますが、契約関連のお問合せも可能です。その場合は、「請求・契約に関する問合せ」にチェックを入れましょう。営業直通の問合せとなります。

メール関連の調査依頼時には

作業依頼に続いて多いのが、調査依頼です。障害発生時のログをみてほしい、アプリケーションをバージョンアップしたらエラーが発生した、など数多くの調査依頼を日々頂きますが中でも多くみられるのがメール関連の調査依頼です。
「今まで送れていたのに、急にメールが使えなくなって困っている」という場合は、早急に解決を望まれるお客様が多いのですが、このような場合、まずは下記情報を依頼内容にご入力いただけると調査から対応までがスムーズに進み、解決までの時間が短縮できます。

- 障害の発生時刻(分かる範囲で)
- 対象となる送信元メールアドレス、送信先メールアドレス
- ご利用のメールソフト
- エラー画面やメールソフトの設定画面のキャプチャ

犯人捜査でも様々な情報や証拠を積み上げて目星をつけるように、サーバの調査にも証拠となる様々な情報が必要となります。サーバエンジニアは、サーバ内の各種ログファイルから、色々なキーワードを基に必要な情報を収集しているので、時刻やアドレス、具体的なキーワードがわかると調査が捗ります。情報が豊富にある場合は、あっという間に原因が特定できる事もありますので、まずはお客様のお手元にある情報をご共有ください！

5 確認画面の内容で問題なければ、依頼内容を送信してください。

※メール関連の調査の場合、内容にもよりますが、2～5営業日程度調査に日数を頂きます。

実際の記入例。エラー画面など、ファイルの添付も可能です。

「サービスデスク直通フォーム」はその名の通り、エンジニアがいるサービスデスクへ直接依頼が届きますので、

ご契約中のサーバでお困りのことがございましたら、
是非こちらの直通フォームをご利用ください！

サイバー攻撃からオリンピックを守ったセキュリティ対策とは？

2月4日より北京オリンピックがスタートしました。選手の活躍だけでなく、五輪マスコットのビンドゥンドゥンの可愛さや公式アプリ「MY2020」の脆弱性などが話題となっていますね。このニュースレターが配信される頃にはもうそろそろ閉会式を迎えるか、またはもうすでに終了している時期かもしれません。オリンピック開催期間中や開催前の時期にサイバー犯罪やサイバー攻撃が頻発することをご存じの方は多いと思います。実際、2021年夏に開催された東京オリンピック・パラリンピックでは、大会組織委員会に対し約4億5000万回のサイバー攻撃があったそうです。（ちなみに、この4億5000万回は2012年に開催されたロンドンオリンピックの約2倍以上の攻撃回数です。）大量のサイバー攻撃を受けながらも、大会運営に支障が出なかったと大会組織委員会は発表しました。大会組織委員会や関連企業はどのような対策をしていたのでしょうか？今回は東京オリンピックで発生したサイバー攻撃とその対策に用いられた標的型メール訓練について紹介しようと思います。

サイバー攻撃の手口とは？

東京オリンピック開催期間中には、IDやパスワードを組み合わせて連続的に攻撃するブルートフォース攻撃の一種である『パスワードスプレー攻撃』が大量に発生しました。そのほか、大会1年半前から、IOC会長や組織委員会・事務総長などに成りすました不審メールが大量に観測されていたとのことです。6000件以上確認されている成りすましメールには、IDとパスワードを入力させて情報を盗む『フィッシングサイト』に誘導する記載がありましたが組織委関係者で誤ってIDなどを入力した事例はありませんでした。

サイバー攻撃を防ぐ事前準備

サイバーセキュリティ対策として多くの企業や人が関わるからこそ、セキュリティに関する知識やスキルだけでなく、どのようなマインドセットで業務に臨むかという点を重要視し、関係者はセキュリティに関するトレーニングを事前に行いました。
トレーニングでは外部攻撃者の目線に立って疑似攻撃を仕掛ける“レッドチーム”が編成され、標的型メール訓練などを10回以上、延べ1万人に実施しています。

標的型メール訓練とは？

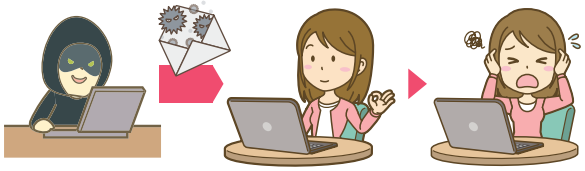
“レッドチーム”が実施した標的型メール訓練とは、特定の組織やユーザー層に対して、知り合いや取引先の振りをして悪意のあるメールを送るサイバー攻撃『標的型メール攻撃』への対処方法を学ぶものです。

標的型メール訓練には
一般的に下記のような内容が含まれています。

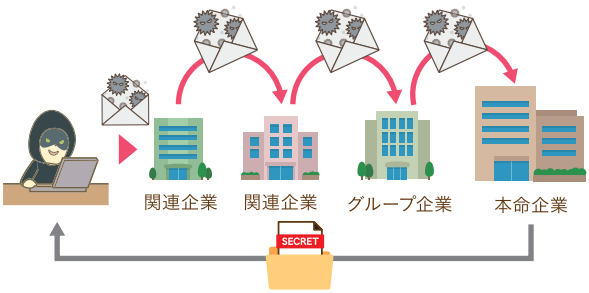
- 標的型攻撃の基本情報学習
- 危険なメールを模した模擬メールの送付
- 模擬メールを開封してしまった件数の集計・分析

事前に疑似メールを受信し、傾向や特徴を知っておくことや標的型攻撃についての情報を学習することで、日頃から不審メールに対しての警戒意識を高めることに繋がります。今回は、東京オリンピックのサイバー攻撃と、その対策として取り入れられた、標的型メール訓練についてご紹介しました。標的型メール攻撃は中小企業には関係ないと思われる方もいるかもしれませんが、流通の中で関わりのある企業へ成りすましメールを送り、本命である大企業や親会社へとサイバー攻撃を行う『サプライチェーン攻撃』も登場していることから、他人事ではないということを意識していく必要がありそうです。

標的型メール攻撃



サプライチェーン攻撃



セキュリティ連盟 発足！

今月、2月2日に弊社のパートナーでもあるサイバーセキュリティクラウド社が発起人となりセキュリティ連盟が発足しました。「日本のDXをもっと安全に」を合言葉に「サイバーセキュリティの重要性を啓発する」為34社の企業が集結した連盟です。もちろんネットアシストも加盟しました。コロナ禍によるリモートワークの実施で急激にDXが進みセキュリティの必要性は高くなりましたが、実際に現場で対応される担当者の方からは下記のようなお悩みを良く伺います。

- 担当者が自分しかいないので、相談相手がいない。
- サイバー攻撃の統計データを見ても実感がわかない。
- セキュリティの情報交換をしたいがコミュニティがない。
- 経営層にセキュリティの必要性をうまく伝えられない。

これまでもサイバー攻撃やセキュリティ対策について

公式SNSやニュースレターを通じて情報発信をしてきましたが今後はセキュリティ連盟としても、「サイバー攻撃被害の裏側」などのリアルな情報発信や企業の垣根を越えたコミュニティの形成を行い、お客様のお悩みやサイバー攻撃のリスクが払拭できるように更なるご提案をしていきます。サイバー攻撃やセキュリティについて、お悩みや疑問などありましたら担当営業までお気軽にご相談ください。

日本の DX をもっと安全に

セキュリティ連盟
現状の参加企業 34社

「セキュリティ連盟」特設ページ
https://www.cscloud.co.jp/dx-security/

SoftTek / Aeye Security Lab / COLLO / Cloud Ace / CloudSafe / classmethod
DXHR / Cgen / GMO / Maromaro / PJ-T&C合同会社 / Serverworks
Rworks / IBC / iret / AsiaQuest / WILL@NET / CLARA / TOKAIコミュニケーションズ
Timeshare / NET ASSIST / HYPER BOX / 5G innovations / Unitea
beyond / FUTURE SPIRITS / Rangeforce / SiteCloud / YONA / SUNLOFT
RIDE / CSC / cybereason

お問い合わせはこちらまで！

NET ASSIST 24/7 Guardian Deity 株式会社ネットアシスト
TEL 03-3985-6780 Mail sales@netassist.ne.jp
URL https://www.netassist.ne.jp