NET ASSIST
24/7 Guardian Deity

NEWS LETTER

2022.04
#12

TOPICS

脆弱性診断についてのおはなし①

～なぜ今脆弱性対策が必要なのか～

脆弱性対策、できていますか？

緊張が続いているウクライナ情勢を受け、経済産業省も国内の各企業などにサイバーセキュリティの対策強化を呼び掛けており、実際、日本企業がサイバー攻撃の標的となり、深刻な被害を受けているケースも相次いでいます。
2月～3月にかけて弊社のお客様でも、海外からの不正アクセスやハッキング事例が増えてきている状況で、高額なセキュリティ製品の導入をご検討頂くお客様も決して珍しくありません。
自社で運用しているWebサービスのセキュリティ対策として、最初にご検討頂きたいのが、「脆弱性診断」です。セキュリティ対策ソリューションは、WAFやIDS／IPS、改ざん検知など多数のソリューションがあり自社の環境には何を導入すればいいのだろう？と迷われるケースが多いのですが、まずは、自社の環境を知ること＝健康診断として脆弱性診断の実施をお勧めします。

どのようなシステムにも脆弱性が潜んでいる可能性があり、Webアプリケーションやネットワーク／サーバの脆弱性状況をチェックすることで、セキュリティリスクを未然に防ぐことができます。今月より数回にわたり、「脆弱性診断」についてのお話をしていきたいと思います。

脆弱性とは？

インターネット上の攻撃などに対して、情報漏洩や改ざんなどの可能性のある【安全上の弱点や欠陥】のこと。
悪意のある攻撃者は、様々な手口で脆弱性を狙い攻撃を仕掛けてきます。

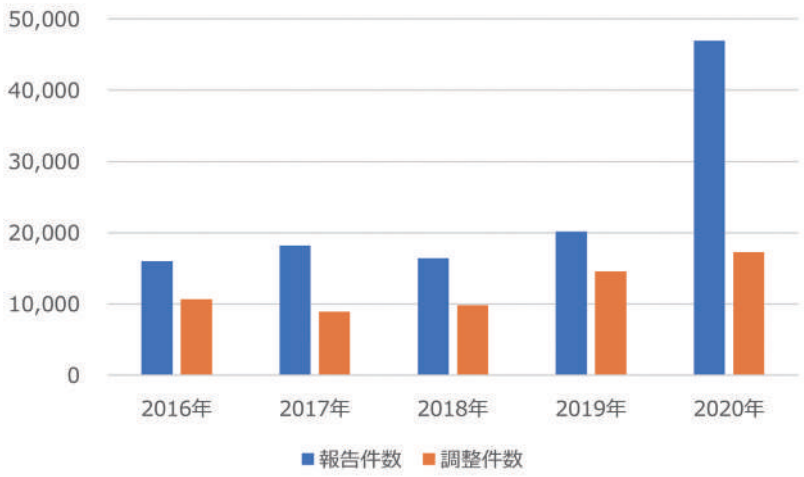
脆弱性診断が今必要な理由

～Webアプリケーションの脆弱性をついたサイバー攻撃が増加している～

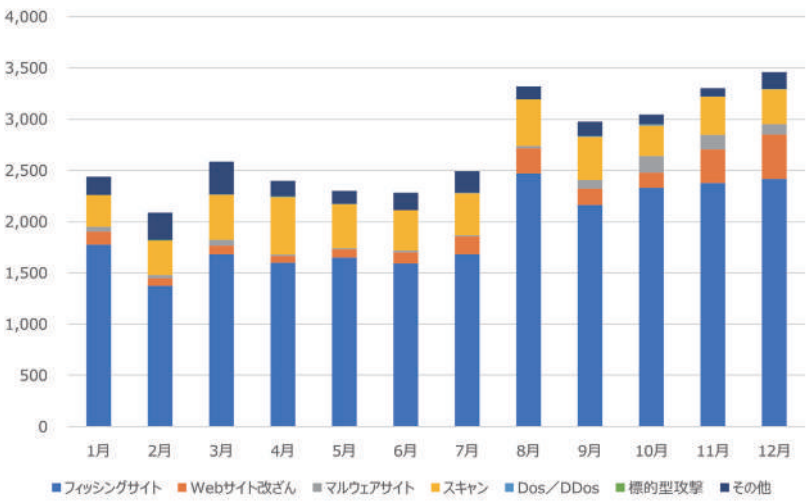
こちらのグラフは、JPCERTが発表している2020年度を含む過去5年間のセキュリティインシデントの報告・調整件数の推移グラフです。
2020年度の報告件数は前年度と比較して、約133%増加しており、調整件数も前年度と比較して約18%増加しています。近年、インターネット上で発生するセキュリティ関連のインシデントが急激に増えてきているというのが一目でわかるグラフです。

※JPCERT/CCとは・・・

インターネット上で発生するセキュリティインシデントについて、日本国内の報告受付・対応支援状況の把握・手口の分析・再発防止の検討や助言を行う組織



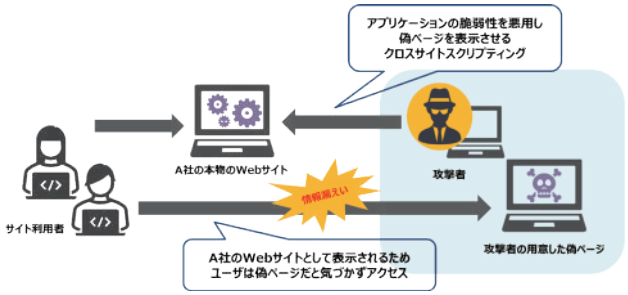
次のグラフも、先ほどのJPCERTが2021年に発表している、セキュリティインシデントの事象別・カテゴリ別の内訳をあらわしているグラフです。
年間を通して多かったインシデントはフィッシングサイトによる被害で、続いて、スキャンによる被害と、Webサイトの改ざん、マルウェアの被害です。この中でも、「脆弱性」に関連したセキュリティインシデントは、フィッシングサイト・Webサイトの改ざん・マルウェアサイト・標的型攻撃・その他、が当てはまります。
こうしてみると、2021年に発生したセキュリティインシデントの実に約8割以上が脆弱性と関連があり、脆弱性を狙ったサイバー攻撃が非常に多く発生している状況です。



カテゴリ別の被害で多かった、フィッシングサイトとWebサイト改ざん

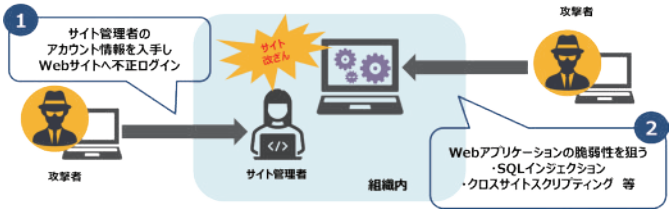
フィッシングサイト

一般的にフィッシング詐欺として知られているのは、サイト利用者向けにサイト運営者を装ってメールを送信し偽サイトに誘導させ、個人情報などを入手する、という手法が良く知られているかと思いますが、実はWebアプリケーションの脆弱性を狙った攻撃による被害も、多く報告されています。ユーザからの入力内容をWebページに表示するようなサイト（アンケート、掲示板）などに、脆弱性がある場合、攻撃者はそこを狙ってきます。悪意を持ったスクリプトが埋め込まれると、攻撃者が用意した偽ページの表示が可能になるので、利用者はA社のサイトから偽ページへ誘導されることになります。A社のサイトを閲覧していたため、利用者も偽ページということに気づかず、フィッシング詐欺に悪用されてしまうのです。フィッシング被害は、直接的な被害は利用者・一般ユーザーが受けるもので、企業やサービス事業者は関係のないものだと誤解している方が多いかもしれませんが、上記のような事例の場合は、運営企業のブランドイメージや信用が失われ、場合によっては利用者に対する損害賠償なども発生する可能性があります。利用者側の意識の向上だけではなく、Webサイト運用側でもWebサイトの安全性を確保するための脆弱性対策が重要です。



Webサイトの改ざん

Webサイトを改ざんする際の攻撃手口は、大きくわけると2つあります。管理者アカウントを乗っ取られサイトに不正ログインされ改ざんされてしまうケースと、脆弱性を狙った攻撃です。こちらの場合、攻撃者はOSやミドルウェア、アプリケーションなどの脆弱性を狙い攻撃を仕掛けてきます。フィッシングサイトの事例でも紹介しましたが、クロスサイトスクリプティングやSQLインジェクション等の脆弱性に対する攻撃により、攻撃者はWebサイトの改ざんが可能になるのです。こういったケースは、開発段階で積み残した脆弱性によって引き起こされる場合も少なくないようなので、やはり開発の段階から診断を実施し、脆弱性を摘み取った状態で、Webサービスの運営を始めることがおすすめです。



IPAが発表した「情報セキュリティ10大脅威2022」

こちらは、2021年に発生した、社会的に影響が大きかったと考えられる情報セキュリティにおける事案からIPAが選定を行い決定した10大脅威です。
ランサムウェアによる被害が1位、標的型攻撃による情報漏洩が2位となっており、この2つは昨年も同じ順位でした。オレンジで囲っている脅威がWebを攻撃対象とした脆弱性を狙った攻撃であり、脅威ランキングの中の、1位、2位含む5つが該当しています。

順位（昨年順位）	情報セキュリティの脅威	攻撃対象
1位（1位）	ランサムウェアによる被害	Web／メール
2位（2位）	標的型攻撃による機密情報の搾取	Web／メール
3位（4位）	サプライチェーンの弱点を悪用した攻撃	Web／メール／NW
4位（3位）	テレワーク等のニューノーマルな働き方を狙った攻撃	Web／メール
5位（6位）	内部不正による情報漏えい	－
6位（10位）	脆弱性対策情報の公開に伴う悪用増加	Web
7位（NEW）	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	Web
8位（5位）	ビジネスメール詐欺による金銭被害	メール
9位（7位）	予期せぬIT基盤の障害に伴う業務停止	－
10位（9位）	不注意による情報漏えい等の被害	－

まとめ

3つのデータをご紹介しました。セキュリティインシデントは、年々飛躍的に増加しています。ご紹介したデータによれば、国内で発生したセキュリティインシデントの8割以上が脆弱性に関連し、情報セキュリティの脅威として挙げられているものの、5割以上がWebやネットワークの脆弱性を狙う攻撃です。このような状況では、Webサービスを運営する企業にとって、セキュリティ対策としての脆弱性診断は、重要なリスクマネジメントの一つといっても過言ではありません。

ネットアシストでは、2022年4月より、制作会社様や開発会社様等向けにWebアプリケーションの自動診断ツールを特別価格でご提供致します。制作したWebサイトに対してセキュリティ診断を付加価値として提供して頂くことや、診断をプラスすることで単価をUPして頂くことも可能です。ご興味ございましたら、弊社担当営業へご連絡頂くか、こちらの資料ダウンロードページよりお問合せください。

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2回　ファイルアップローダ

皆様は、お客様ポータル画面よりファイルアップローダ機能が使えることをご存じでしょうか？実は2020年3月にセキュリティレベルや利便性を向上させるために機能リリースをしています。最近ではEmotet対策として、パスワード付きZipファイルの送付を取りやめている企業様も多いかと思います。
よりセキュアなデータ共有をするために、ネットアシストとのやり取りにはぜひファイルアップローダ機能をご活用ください！明日からでも皆さまが活用できるように、今回は基本的な使い方を紹介したいと思います。

ファイルアップローダ機能の特徴

お客様・ネットアシストの双方でファイルのアップが可能です。また、アップできるファイル容量は1.5GBと大容量ファイルにも対応しています。ファイルアップローダ機能をご利用の際に発生する通信は、すべてHTTPS通信(暗号化)されているため、安心してご利用いただける点もポイントです。

『ファイルアップローダ』を活用する

A：ネットアシストへのファイル共有（お客様→ネットアシスト）

1 お客様ポータルのTOP画面から『ファイルアップローダ』をクリック

2 『アップロード済みファイル一覧』へ移動します。

3 ページ右下の『アップロード』をクリックするとファイルアップロードページへ移動します。

4 『ファイル選択』をクリックしてアップロードしたいファイルを選択してください。

※「Internet Explorer」でご利用の場合、ファイルのダウンロードのみ可能です。

5 ファイルを選択後、『アップロード』をクリックするとアップロードが開始します。

※アップロードするファイルについて、ファイルサイズは1.5GBまで、ファイル名は40文字まで

6 アップロードが完了のアナウンスが表示されたら『完了』をクリックしてください。

7 アップロード済ファイル一覧ページでアップロードしたファイルが表示されているのを確認し、『詳細』をクリックしてください。

※詳細ページへ移動しなくても、ファイル一覧から「DL用URLのコピー」「ファイルDL」が可能です。

8 『ファイル詳細』ページへ移動します。

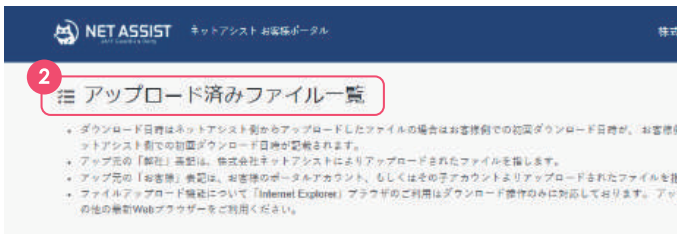
※このページではアップロードしたファイルの「ダウンロード」「削除」「詳細情報の確認」が可能です。

ファイルのアップロード完了後は、メールにダウンロード用URLを記載の上、ネットアシストまでご共有ください。

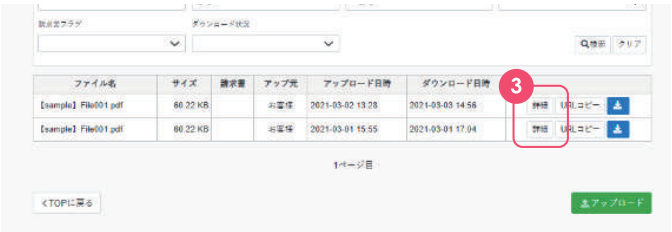
B：ネットアシストからのファイル共有（ネットアシスト→お客様）

1 お客様ポータルのTOP画面から『ファイルアップローダ』をクリック

2 『アップロード済みファイル一覧』へ移動します。



3 ダウンロードしたいファイルの詳細をクリックしてください。

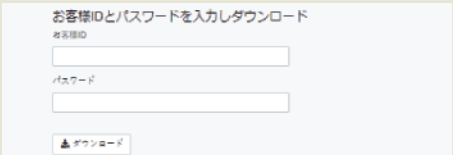


※ネットアシストがアップロードしたファイルは「アップ元」が"弊社"で表示されます

4 「ファイル詳細」ページへ移動します。

※このページではアップロードしたファイルの「ダウンロード」「詳細情報の確認」が可能です。

その他、ネットアシストからダウンロード用のURLを共有することでお客様がファイルのダウンロードをすることも可能です。
ダウンロードの際にはお客様ポータルのID/パスワードの入力をお願します。



ネットアシストとファイルのやり取りをする時には、是非こちらのファイルアップローダをご利用ください！

詳細情報

ファイル名
アップロードしたファイル名が表示されます。
※ 同名のファイルをアップロードした場合、上書きはされず、別ファイルとして保存されます。

ダウンロードURL
子アカウントまたはネットアシストへメールでファイルの共有をされる際は、こちらのURLをコピーしご共有ください。

Fileタイプ
アップロードしたファイルのデータ形式が表示されます。
※PDF・MSOffice（Excel・Word・PowerPoint）画像ファイル・テキストファイル・Zip形式のファイルに対応しています。

ファイルサイズ
アップロードしたファイルのデータサイズが表示されます。
※1ファイル1.5GBまでのデータがアップロード可能です。

アップ元
ファイルをアップロードしたアップ元が表示されます。
弊社・・・ネットアシストがアップロードしたファイル
お客様・・・お客様がアップロードしたファイル

アップロード日時
ファイルをアップロードした日時が表示されます。

請求書
ネットアシストから請求書がアップロードされた際は、こちらに表示されます。
※ 特殊フォーマットの請求書のみこちらにUPされます。通常の請求書はTOP頁の「請求履歴」からダウンロードしてください。

ダウンロード日時
ファイルをはじめてダウンロードされた日時が表示されます。
※ ダウンロード期限はありません。
※ ダウンロードされていない場合は未表示です。ただし、ネットアシストが複数のアカウントに同一のファイル共有をした場合には、そのファイルを最初にダウンロードされたアカウントの日時が表示されます。

ネットアシストに
新しいメンバーが加わりました！

ネットアシストでは、今年度から新しく4名が入社いたしました。
今回は日頃お世話になっているお客様へ向けて、簡単ですが自己紹介をさせていただきます！

中途採用

R.H（営業部/3月入社）

出身大学、前職

東京経済大学出身で、前職は生命保険の個人営業をしていました。

休日の過ごし方

猫がいるお気に入りの喫茶店に行ったり最近パソコンを新調したのでゲームをしたりなどと、まったり過ごしています。

抱 負

業界・業種ともに未経験のため努力を惜しまず、頼りになる営業員になれるよう日々精進していきます。

M.K（技術部/3月入社）

出身大学、前職

立正大学で自然環境（特に地質・岩石分野）を研究しました。化石を見ると気分が上がります。前職は年金機構で事務職をしていました。

休日の過ごし方

読書や自然のある場所に出かけたりします。特に江國香織さんの小説が好きです。また、メンタリストDaiGoさんが紹介する本を読んで心身の改善に役立てています。お気に入りの場所は、新橋駅近くの浜離宮恩賜庭園です。

抱 負

ITは全くの未経験分野のため、勉強や仕事を通して成長していく自分を楽しみにする姿勢で様々なことに挑戦していきたいです。そしてたくさんの仕事をこなしていく先輩方にめげずに喰らいついていき、早く追いつけるよう頑張ります。

新卒採用

K.K（技術部）

出身大学、前職

出身大学は佛教大学で、社会福祉を専攻していました。

休日の過ごし方

読書をして過ごしています。ミステリー小説や漫画を中心に読んでいます。

抱 負

知識や経験はありませんが、精一杯努力を重ね、頼りになるエンジニアになれるよう邁進していきます。

I.T（技術部）

出身大学、前職

駿河台大学のメディア情報学科で、図書館情報学を学んでいました。

休日の過ごし方

サッカーをしたり、観戦したりして過ごしています。プレミアリーグのシティを応援しています！
また、アニメやゲームの聖地に行ってリフレッシュすることもあります。

抱 負

初挑戦で右も左も分からないですが、1日でも早く戦力として活躍できるよう、頑張っていきます。

新しい風を取り入れ、今年度も更なる発展に向けて歩み続けてまいります。お客様により良いサービスをご提供できるよう社員一同尽力いたしますので、今後ともどうぞ宜しくお願いいたします。

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