NET ASSIST
24/7 Guardian Deity

NEWS LETTER

2022.06
#14

TOPICS

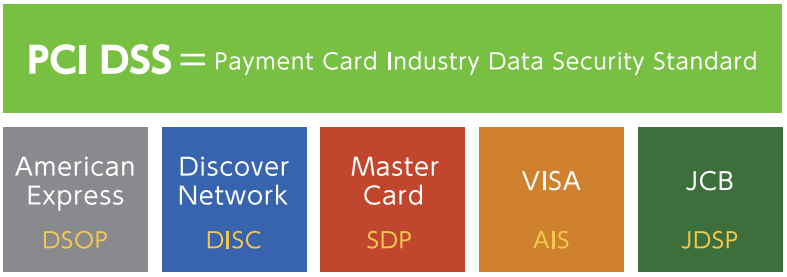
脆弱性診断についてのおはなし②

～なぜ今脆弱性対策が必要なのか～

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。前回（Vol.12）は、脆弱性診断が必要な理由の1つ目として、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状況を、JPCERTのレポートや、IPAの情報セキュリティ10大脅威レポートをもとにご紹介いたしました。今月は、脆弱性診断が必要な理由を、「セキュリティガイドライン」と「個人情報保護法改正」の2つの観点からご紹介したいと思います。

PCI DSSのセキュリティガイドライン

国際的なクレジットカードブランド5社（AMEX、Discover、Master、VISA、JCB）では、クレジットカードの会員データを安全に取り扱うためガイドラインが義務化されており、PCI DSSに準拠しています。PCI DSSの要件では、クレジットカードの会員情報を扱うようなサイトの場合は、4半期に1回の定期的な脆弱性診断を行うことが明記されており、2018年からは、PCI DSSの要件に準拠するか、カード情報を保持しない事が必要となりました。



※PCI DSSとは：クレジットカード業界における、会員データを安全に取り扱うことを目的として策定された国際セキュリティ基準のこと

国際カードブランド各社と実施プログラム（下段の文字）

JPCERTのガイドライン

JPCERTが推奨しているガイドラインでは、Webへのサイバー攻撃に備えてWebサイトの定期的な点検の実施を推奨しています。その中には、Webアプリケーションのセキュリティ診断を1年に1回程度、定期的な診断を実施することが推奨されています。今までは、一部上場企業などに限定されていたセキュリティ要件シートなども、中小企業の多くで導入され始めており、自社で運用するWebサイトに脆弱性診断をかけることが必須要件となってきています。新たな脆弱性が次々と発表されている現状では、開発段階だけではなく、運用フェーズ後の定期的な診断が不可欠です。

Webアプリケーションのセキュリティ診断

目的 自社のWebアプリケーションに脆弱性や設計の不備が存在しないかを確認するため

対象 Webアプリケーション

頻度 1年に1回程度、および機能追加などの変更が行われた時

利用製品のバージョンが最新であることの確認
（プラグインなどの追加の拡張機能も含む）

目的 製品の脆弱性を狙ったサーバー攻撃を回避・低減するため

対象 WebサーバなどのWebシステム、Webサイト運用管理用PC

頻度 数週間～1ヶ月に1回程度

Webサーバ上のファイルの確認

目的 ファイルが改ざんされていないか、不正に作成されていないかなど、確認するため

対象 ファイルのリスト（ファイル名、サイズ、更新日時、ハッシュ値）やバックアップの取得と比較

対象 Webサーバ

頻度 1週間に1回程度

ログインIDとパスワードの確認

目的 複数のサービスで同じパスワードが使用されていないか、安易に推測できるパスワードを使用していないか確認するため

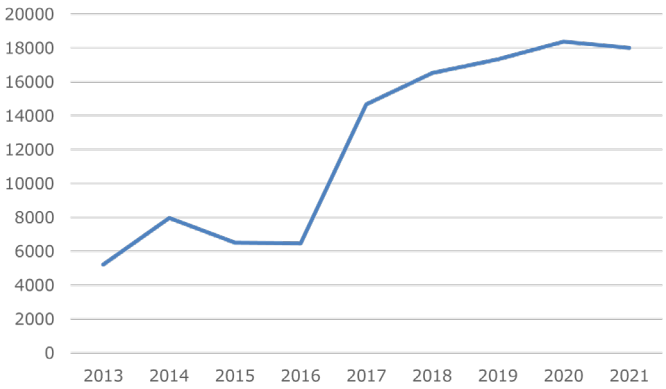
対象 Webサーバ

頻度 1週間に1回程度

こちらのグラフは、2013年からのCVEの登録件数を示したものです。2017年から急激に登録件数が増えています。

2020年度は過去最高の18,361件のCVEが登録されており、1日に換算すると約50件もの脆弱性が発見・報告されていることになるのです。脆弱性が日々発見されている状況では、リリース前に一度診断を実施しただけでは、セキュリティ対策が十分とはいえません。

※CVEとは：情報セキュリティにおける脆弱性について、それぞれ固有の名前や番号を付与したリストの事。1999年に米国のマイターコーポレーションが実装。ベンダーをまたいだ脆弱性情報の比較が、容易に行えるようになった。



個人情報保護法の改正

過去のニュースレターでも何度か取り上げておりますが、2022年4月に個人情報保護法の改正が施行されました。改正内容は複数ありますが、改正の大きいポイントはこの2つです。サイバー攻撃や個人情報の漏えいなど、セキュリティに対しての関心が高くなっていく中で、万が一、情報漏えいにより企業名が発表されてしまった場合に、自社やクライアントがこうむる被害や影響は相当大きいと考えられます。こういったペナルティの対象にならないためには、適切なセキュリティ対策を実施する必要があるのではないでしょうか。

改正ポイント①
事業者責務の追加

現在

個人情報取扱事業者による、個人情報の漏えい等の発生時の個人情報保護委員会への報告、本人への通知は法律上の義務ではなかった。

改正後

個人情報取扱事業者による、個人情報の漏えい等の発生時は、個人情報保護委員会に報告し、本人に通知する義務を負う。

改正ポイント②
法令違反に対するペナルティの強化

現在

措置命令（42条2項、3項）の違反の罰則 ：30万円以下の罰金
個人情報データベース等の不正流用 ：50万円以下の罰金
報告義務（40条）違反の罰則 ：30万円以下の罰金

改正後

措置命令（42条2項、3項）の違反の罰則 ：1億円以下の罰金
個人情報データベース等の不正流用 ：1億円以下の罰金
報告義務（40条）違反の罰則 ：50万円の罰金

まとめ

今回は、「セキュリティガイドライン」と「個人情報保護法の改正」の観点から、脆弱性診断の必要性をご紹介しましたが、弊社がお客様に脆弱性診断をお勧めする理由は大きくこの3つです。ネットアシストでは、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しております。
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。

POINT 1
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と

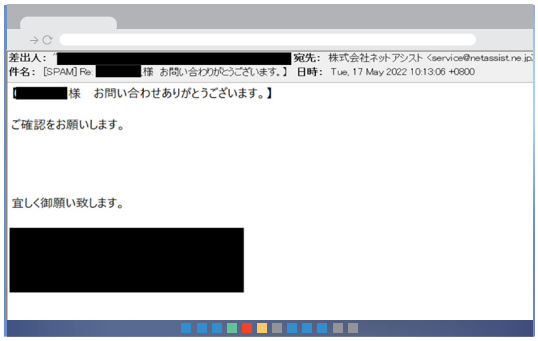
POINT 2
セキュリティ関連機関のガイドラインによって定期的な実施が推奨・義務化されていること

POINT 3
個人情報保護法の改正により、基本的なセキュリティ対策が重要になってきていること

ご興味ございましたら、弊社担当営業へご連絡頂くか、
弊社ホームページの資料ダウンロードページよりお問合せください。

なりすましメールにご注意ください！

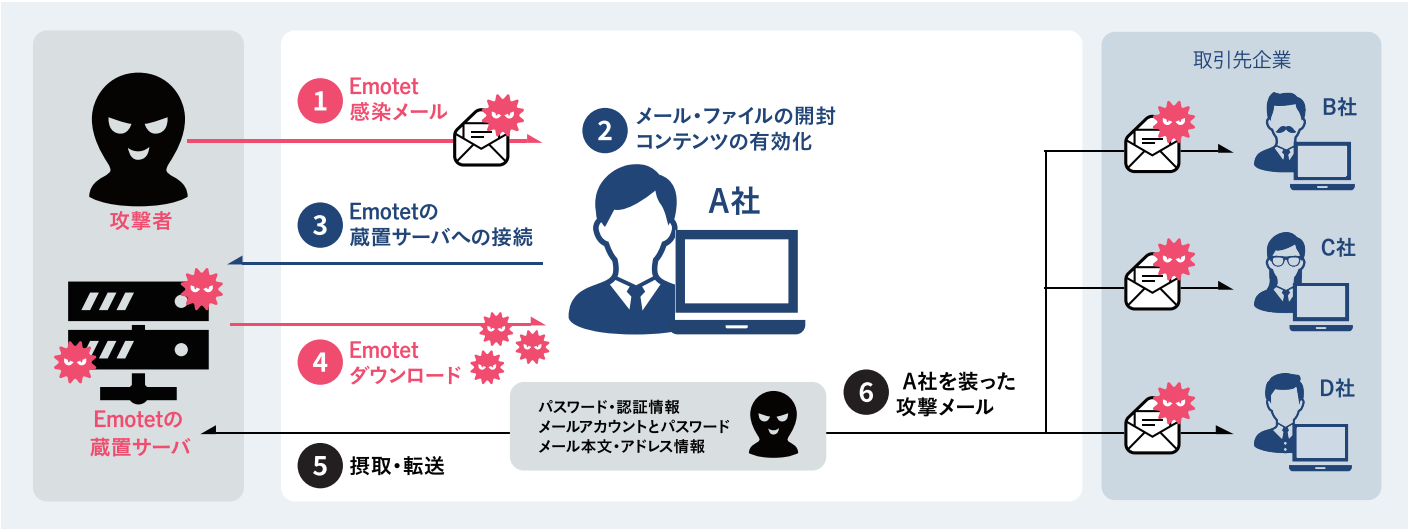
近年、様々なサイバー攻撃が蔓延り、その攻撃手法も巧妙化しています。
そんな中、最近ネットアシストでも「**なりすましメール**」の被害を受けるという出来事がありました。
ある日、いつも通りメールチェックをしていたところ、差出人と本文の関連性がなく、ファイルが添付されている不審なメールを受信していることに気がつきました。すぐに社内相談になり、添付ファイルは開かずに各自でメールを削除して対応しました。幸い、弊社の全PCに導入しているアンチウイルスソフトが起動し、すぐに不審メールの検知と添付ファイルの削除が行われていたので被害の拡散を防ぐことが出来ました。差出人は弊社社員を装ったものもあり、不特定多数に発信された可能性があるため、ネットアシスト公式ホームページやSNSで注意喚起を行いました。



＜弊社に届いた「なりすましメール」＞
※こういうメールに添付されているファイルは絶対開かないでください！

今回の「なりすましメール」は、弊社の取引先（A社）が「 **Emotet** 」に感染したことによるものと想定されます。Emotetとは、感染端末内からアドレスなどの情報を窃取して「なりすましメール」の送信に悪用するマルウェアで(端末内のメーラーのアドレス帳などから情報を窃取しているものと思われます)、メールの添付ファイルが主要な感染経路です。情報窃盗に加えて他のウイルスの媒介も行います。攻撃手口の特徴として、「正規メールの返信」を偽装するなどがあります。過去に（A社）様とメールの送受信をしたことから、今回の「なりすましメール」の送信に悪用されたことが考えられます。また、そのメールには弊社社員の携帯電話番号が記載されたシグネチャ（署名）が添付されているものもあったので、電話番号を変更して対応しました。弊社内ではEmotetに感染したPC端末は無く、お客様の情報が漏洩することはございませんのでご安心ください。

Emotet(エモテット)の特徴



このようなメールを使った攻撃は、添付ファイルの開封やURLをクリックしない限り被害を防ぐことが出来ますが、差出人の名前を信用しすぎると誤って開封やクリックをしてしまう可能性も考えられます。対策として、日頃からメールをチェックする際は意識して気をつけることを基本に、アンチウイルスソフトの最新バージョンを導入する事も大切です。サイバー攻撃は、被害者が加害者になることもあります。それが企業となると、会社のブランド価値低下・信用喪失・利益減少にも繋がります。弊社はインフラ専門の会社のため、今回のような出来事も冷静に対処することが可能でしたが、普段馴染みのない企業だと、突然サイバー攻撃を受けた際には慌ててしまうこともあると思います。

そのような時は、お力になれることもございますので、是非一度ネットアシストにご相談ください。

今回は、なりすましメールの実体験をご紹介しました。弊社のようにある日突然被害を受けることもありますので、この記事が少しでも参考になりますと幸いです。

NET ASSIST
24/7 Guardian Deity

2022年6月1日をもちまして、株式会社ネットアシストは創業22周年を迎えることが出来ました。これもひとえに、お取引先の皆様からのご支援の賜物と深く感謝いたします。そして今年も沢山のお祝いのお花や品物をお贈り頂き、オフィスが華やかになりました。社員一同大変喜んでおります。皆様、誠にありがとうございます。

今年の4月、弊社は2名の新入社員を迎えましたが、なんと今年の新入社員とネットアシストは同じ22歳であることが分かりました。ネットアシストは2000年の創業、新入社員も同じ2000年の生まれです。会社が出来た年に生まれてきた人が、今こうして新入社員としてネットアシストで働いていると考えると何だか感慨深いですね。22年という会社の歴史の重みを感じます。これからも次の20年、50年、100年とネットアシストが永続的に発展していくことが出来るよう、社員一同努めて参ります。

今後ともご指導ご鞭撻を賜りますよう、宜しくお願い申し上げます。

※抜粋「スタッフブログ：創立22周年。」代表取締役　伊藤誠史
ネットアシスト公式サイト（https://www.netassist.ne.jp）からご覧頂けます。

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