NET ASSIST
24/7 Guardian Deity

2024.3 #35

NEWS LETTER

TOPICS

＊ TOPICSの各タイトルをクリックすると該当の記事へ飛びます

#1 情報セキュリティ10大脅威2024

IPA（独立行政法人 情報処理推進機構）より「情報セキュリティ10大脅威 2024」が公開されました。
https://www.ipa.go.jp/security/10threats/nq6ept000000g22h-att/kaisetsu_2024.pdf

10大脅威ランキング2024

「個人」向け脅威	対前年比	2023年順位	2024年順位	2023年順位	対前年比	「法人」向け脅威
インターネット上のサービスからの個人情報の搾取	7↑	8	1	1	ー	ランサムウェアによる被害
インターネット上のサービスへの不正ログイン	7↑	9	2	2	ー	サプライチェーンの弱点を悪用した攻撃
クレジットカード情報の不正利用	1↑	4	3	4	1↑	内部不正による情報漏えい等の被害
スマホ決済の不正利用	1↑	5	4	3	1↓	標的型攻撃による機密情報の搾取
偽警告によるインターネット詐欺	2↑	7	5	6	1↑	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
ネット上の誹謗・中傷・デマ	4↓	2	6	9	3↑	不注意による情報漏えい等の被害
フィッシングによる個人情報等の搾取	6↓	1	7	8	1↑	脆弱性対策情報の公開に伴う悪用増加
不正アプリによるスマートフォン利用者への被害	2↓	6	8	7	1↓	ビジネスメール詐欺による金銭被害
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	6↓	3	9	5	4↓	テレワーク等のニューノーマルな働き方を狙った攻撃
ワンクリック請求等の不正請求による金銭被害	ー	10	10	10	ー	犯罪のビジネス化（アンダーグラウンドサービス）

IPA（独立行政法人情報処理推進機構）より公開された資料より引用しています。
https://www.ipa.go.jp/security/10threats/10threats2024.html

昨年の発表と比較して、個人向け脅威の変動は大きかったですが、法人向け脅威はあまり変動が無く固定化しているようです。特に1位の「ランサムウェアによる被害」と、2位の「サプライチェーンの弱点を悪用した攻撃」は引き続き最も注意すべき脅威と言えますね。それ以外も多少の順位変動はありましたが、1位から10位まで同じ顔触れとなっているので、今年もこの10項目に注意し続ける必要がありそうです。

それでは「組織」向け脅威のランキングから、サーバーに関係のある項目を抜粋してご紹介いたします。

次ページへ

前ページより

1位：ランサムウェアによる被害

■概要

「ランサムウェア」と呼ばれるウイルスに感染させ、PCやサーバーのデータを暗号化し、業務の継続を困難にした上で、データを復旧することと引き換えに、金銭を要求する手口です。なお、金銭を支払ったとしても、データの復旧や漏えいした情報の削除が行われないケースが増加しています。

■手口

●弱性を悪用しネットワークから感染させる
●公開サーバーに不正アクセスして感染させる
●メールから感染させる
●Web サイトから感染させる

■事例

港運協会のターミナルシステムにランサムウェア感染による障害が発生。このシステム障害によりトレーラーによるコンテナ搬出入作業ができなくなりました。

2位：サプライチェーンの弱点を悪用した攻撃

■概要

商品の企画・開発～調達～製造～在庫管理～物流～販売までの一連のプロセスに関わる組織群の中から、セキュリティ対策が脆弱な組織を最初の標的とし、そこを踏み台として顧客や本命の標的を攻撃する手口です。

■手口

●取引先や委託先が保有する機密情報を狙う
●ソフトウェア開発元やMSP等を攻撃し、標的組織を攻撃するための足掛かりとする

■事例

病院が契約している給食配給事業者の脆弱性対策が不十分だった事から侵入され、病院の電子カルテシステムが攻撃を受けました。

5位：修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

■概要

OSやソフトウェアに脆弱性が存在することが判明し、脆弱性の修正プログラム（パッチ）や回避策がベンダーから提供される前に、その脆弱性を悪用してサイバー攻撃を行う手口です。これをゼロデイ攻撃といいます。

■手口

●ソフトウェアの脆弱性の悪用

■事例

電機メーカーでゼロデイ攻撃の被害が発生し、約8,000件以上の個人情報が流出しました。システムにはセキュリティ対策を講じていましたが防げませんでした。

7位：脆弱性対策情報の公開に伴う悪用増加

■概要

公表されたばかりの脆弱性情報を悪用し、対象製品への脆弱性対策を講じていないシステム（Nデイ脆弱性）を狙って攻撃を行います。近年では脆弱性関連情報の公開後に攻撃コードやツールがダークウェブ上に流通し、攻撃が本格化するまでの時間もますます短くなっています。

■手口

●対策前の脆弱性（Nデイ脆弱性）を悪用
●ダークウェブ上に公開されている攻撃ツールを使用

■事例

建築業者で既知の脆弱性を衝いた不正アクセス被害が発生。攻撃者がランサムウェアによる暗号化を展開し、情報資産が利用できなくなりました。

共通対策

本書では10大脅威への共通対策についても記載されていましたので、ご紹介させていただきます。対策に迷ったら共通対策から始める事をお勧めいたします。

●パスワードを適切に運用する
●情報リテラシー、モラルを向上させる
●メールの添付ファイル開封や、メールやSMS のリンク、URL のクリックを安易にしない
●適切な報告／連絡／相談を行う
●インシデント対応体制を整備し対応する
●サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う
●適切なバックアップ運用を行う

次ページへ

前ページより

上記の中から最も基本と言える「パスワードを適切に運用する」について、対策をご紹介します。サーバーの利用においてもパスワードは様々な場面で利用されています。

- ●クラウドのコントロールパネル
- ●メールアカウント
- ●コンテンツのログイン
- ●サーバーへのログイン
- ●FTPアカウント
- ●Gitアカウント
- ●データベースへのログイン

上記は一例ですが、パッと思いつくだけでもたくさんありますね。どれだけセキュリティ強化していても、簡単なパスワードを使っていると侵入されてしまいます。IPAから、下記のような運用例が発表されていますので参考にしてください。

1. IDとパスワードを同じ文字列にしない
2. 数字、アルファベット、記号等の複数の文字種を組み合わせる
3. 生年月日や名前を使わない
4. 連続した数字やアルファベットにしない
5. 単純な単語一語だけにしない

なお弊社でご提供させていただいている「IDS/IPS」や「WAF」などのセキュリティ製品導入についても、共通対策として言及されていました。
未導入の場合は、お気軽にご相談ください。

#2 SSL証明書 の取得方法が変わります!!

昨年から随時アップデートしているお客様ポータルですが、来月4月よりSSL証明書の新規取得もお客様ポータルを通じて、より簡略化されます!そこで今回はリリースに先立ち、SSL証明書の新規取得フローをご紹介いたします。

【変更点】証明書の登録情報の提出方法が変わります!

(従来)
証明書の登録情報を
Excelシートにてご提出

》

(今後)
お客様ポータル上にて
証明書の登録情報をご入力

【新規取得フロー】

1. 貴社担当営業にSSL証明書新規取得依頼のご連絡いただく
2. 担当営業より見積送付
3. お客様よりご発注いただく
4. お客様ポータルにて証明書の登録情報をご入力
5. 入力いただいた内容をもとに弊社にて新規取得手続き開始

次ページへ

前ページより

【お客様ポータルの操作フロー】

1 お客様ポータルにログインいただき「SSL/TLS証明書一覧と新規取得」をクリック

2 右上の「SSL証明書取得申請」をクリック

次ページへ

前ページより

3 SSL証明書を設定するサービス(サーバー)を選択し、「次へ」をクリック

ネットアシスト管理SSL/TLS証明書取得申請

対象サービス・サーバー選択 > SSL/TLS証明書必要情報入力

新規取得の場合、証明書自体の費用（年間契約）が発生いたします。
費用のご案内が必要な場合は、営業担当までご連絡ください。

SSL/TLS証明書を紐づける予定のサービス・サーバーを選択してください。
対象サーバーが不明な場合は未選択のままで次へお進み下さい。

サービス: サービス テストA

対象	管理番号	管理サービス名	ホスト名	IPアドレス	保守プラン
☑	03-0015	サービス テストA	portal-test.netassist.com	255.255.255.255	

次へ >

4 従来Excelシートにご入力いただいていた、「CSR情報」、「SSL種別(プルダウン式)」「お客様情報」を入力し「SSL/TLS証明書の取得申請を行う」をクリックし完了。

ネットアシスト管理SSL/TLS証明書取得申請

対象サービス・サーバー選択 > **SSL/TLS証明書必要情報入力**

■CSR情報

すべて**半角英数字 64文字以内**で入力して下さい。
※*印が付いている項目は必須です。
※識別名の入力には、以下の文字が使用できます
　コモンネーム：-(ハイフン)　.(ドット)　*(アスタリスク)
　その他項目：半角スペース　,(カンマ)　-(ハイフン)　.(ドット)　/(スラッシュ)　((かっこ)
　　)(閉じかっこ)　'(アポストロフィ)　:(コロン)　=(イコール)
※「&」が含まれる場合、半角英字のandに置き換えてください
※スペースのみの入力項目がある場合、証明書が発行されません
※ワイルドカード証明書の場合「*.example.jp」のように、一番左側のラベルにワイルドカード文字「*.」を
　指定してください。ワイルドカード証明書以外の証明書では、ワイルドカード文字は使用できません
※2048bitの鍵長で作成されます
※GMOグローバルサイン(ワイルドカード以外)で2wayを希望される場合はコモンネームの先頭にwww.を付与して下さい

コモンネーム*	ssl.netassist.jp
組織名*	NETASSIST Inc.
部門名	webmaster
市区町村*	Toshima ku
都道府県*	Tokyo
国*	JP

次ページへ

前ページより

■SSL種別

本人確認用メールアドレスについては以下のいずれかに当てはまるものをご入力下さい。
admin@_____　administrator@_____　hostmaster@_____　webmaster@_____　postmaster@_____
whois記載のメールアドレス(登録者、管理担当者など)
※ @_____ は、コモンネームまたはドメイン名となります。
※GMOグローバルサイン(ワイルドカード以外)で2wayを希望される場合は、本人確認用メールアドレスに○○○@ドメイン名または、Whois記載のアドレスをご入力下さい

SSL証明書種別* 株式会社日本レジストリサービス（JPRS) DV: サーバー証明書（ドメイン認証型）/1年

2way希望* ◉希望する ○希望しない ※ワイルドカードでご申請の場合は2wayは「希望しない」になります。

本人確認用メールアドレス*

■お客様情報

連絡先メールアドレスに対して、弊社よりSSL/TLS証明書の更新/廃止確認メールが届きます。

連絡先 会社名* 200文字まで

連絡先 担当者名* 200文字まで

連絡先 メールアドレス(To)*

連絡先 メールアドレス(Cc) ※カンマ区切りで5件まで登録できます。6件以上必要な場合はメーリングリスト等をご利用下さい。

■請求先(発注団体)情報

会社名* 株式会社ネットアシスト

会社名カナ* ネットアシスト

部署名 システム課

担当者名* 山田　太郎

担当者名(First Name)* taro

担当者名(Last Name)* yamada

郵便番号* 111-1111

住所1* 東京都豊島区南池袋

住所2* 3-13-5 池袋サザンプレイス 7F

担当者メールアドレス* yamada@netassist.ne.jp

電話番号* 03-3985-6780

FAX 03-3985-8884

以上の入力内容でよろしければ「SSL/TLS証明書の取得申請を行う」をクリックして下さい。

〈戻る　SSL/TLS証明書の取得申請を行う✔

上記フローにて証明書の登録が完了いたしますと、弊社にて取得手続きを行います。
尚、この時点でご発注いただけていない場合は、別途担当営業よりご連絡させていただき、お客様よりご発注いただき次第、取得手続きを行います。

新規サイトを立ち上げる場合など、新たにSSL証明書の取得が必要になった際、上記フローに沿ってご依頼いただきますようお願いいたします。
今後もお客様により効率的にご利用いただけるよう、随時アップデートを行ってまいりますのでご期待ください！

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
web https://www.netassist.ne.jp