NET ASSIST
24/7 Guardian Deity

2025.3 #46

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2025

2025年1月30日にIPA（情報処理推進機構）より「情報セキュリティ10大脅威 2025」が公開されました。
また、2月28日には解説書「組織編」が公開されました。
参考：

IPA「情報セキュリティ10大脅威 2025」
https://www.ipa.go.jp/security/10threats/10threats2025.html

IPA「情報セキュリティ10大脅威 2025」解説書「組織編」
https://www.ipa.go.jp/security/10threats/eid2eo0000005231-att/kaisetsu_2025_soshiki.pdf

10大脅威ランキング2025「個人」向け脅威

「個人」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窃取	ネット上の誹謗・中傷・デマ
インターネット上のサービスへの不正ログイン	フィッシングによる個人情報等の搾取
クレジットカード情報の不正利用	不正アプリによるスマートフォン利用者への被害
スマホ決済の不正利用	メールやSMS等を使った脅迫・詐欺の手口による金銭要求
偽警告によるインターネット詐欺	ワンクリック請求等の不正請求による金銭被害

※個人向け10大脅威では、IPAからの公開では順位の記載をせず、50音順で並べています。これは、順位の低い脅威への対策が疎かになることを懸念してのことです。順位に関わらず自身に関係のある脅威に対して対策を行うことが大切です。

10大脅威ランキング2025「法人」向け脅威

2025年順位	「法人」向け脅威	2024年順位	対前年比
1	ランサム攻撃による被害	1	―
2	サプライチェーンや委託先を狙った攻撃	2	―
3	システムの脆弱性を突いた攻撃	5、7	2、4↑
4	内部不正による情報漏えい等	3	1↓
5	機密情報等を狙った標的型攻撃	4	1↓
6	リモートワーク等の環境や仕組みを狙った攻撃	9	3↑
7	地政学的リスクに起因するサイバー攻撃	圏外	NEW
8	分散型サービス妨害攻撃（DDoS攻撃）	圏外	NEW
9	ビジネスメール詐欺	8	1↓
10	不注意による情報漏えい等	6	4↓

昨年の発表と比較して、法人向け脅威に大きな変動はありませんが、特筆するべき点としては、初選出の「地政学的リスクに起因するサイバー攻撃」と、5年ぶりにランクインした「分散型サービス妨害攻撃（DDoS攻撃）」があげられます。他にも、不動の1位「ランサム攻撃による被害」と、2位の「サプライチェーンや委託先を狙った攻撃」は引き続き注意すべき脅威だと言えます。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 ランサム攻撃による被害

■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（ランサム＝身代金）を要求する手口です。近年は大企業だけでなく、半分以上の事例が人手や予算の不足している中小企業をターゲットとしています。

■事例
大手出版社・動画配信サービスにランサムウェア攻撃が発生。出版部数の減少や動画配信サービスの長期間停止などの被害が起こり、SNSなどでも大きな話題になりました。

■手口
●脆弱性を悪用しネットワークから感染させる
●メール・WEBサイトから感染させる

対策
●修正プログラムを適用して、OSやソフトウェアを常に最新の状態にアップデートしておく
●不審なメールの添付ファイルやURLをクリックしない
●定期的なバックアップを行う

2位 サプライチェーンや委託先を狙った攻撃

■概要
関連企業や取引先の中から、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。「サプライチェーンの弱点を悪用した攻撃」という旧名称から「委託先」という文言が明記されております。自社だけで完結しないため、対策が難しいことが特徴です。

■事例
米国企業が不正アクセスされ、サービスの提供先である国内通信会社の顧客情報（氏名、メールアドレス）が漏洩しました。

■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を攻撃し、標的組織を攻撃するための足掛かりとする

対策
●自社だけでなく、関連企業全体の状況を把握する
●発注企業と委託先がコミュニケーションをとりながら、共にセキュリティレベルを高めていく

3位 システムの脆弱性を突いた攻撃

■概要
「修正プラグラムの公開前を狙う攻撃（ゼロデイ攻撃）」と「脆弱性対策情報の公開に伴う悪用増加」が統合された項目で、OSやソフトウェアに対する脆弱性を悪用して攻撃する手口です。公開された脆弱性の対策をしていないシステムを狙う場合や、対策が公表される前の脆弱性を悪用される場合もあります。

■事例
関西圏で人気のカフェが、旧バージョンのWordPressシステムの脆弱性を悪用され、公式サイトのページを改ざんされました。

■手口
●対策前の脆弱性を悪用
●修正パッチ公開前の脆弱性を悪用（ゼロデイ攻撃）

対策
●修正プログラムを適用して、OSやソフトウェアを常に最新の状態にアップデートしておく
●振る舞い検知のアンチウイルスソフトや、不正アクセスを防ぐIDS/IPSを導入する

8位 分散型サービス妨害攻撃（DDoS攻撃）

■概要
特定のサーバーやサイトに過剰なアクセスを行うことで、サービスの継続を困難にする攻撃をDoS攻撃と言います。その中で、複数のサーバーを踏み台にして、攻撃元を分散し、より過剰な負荷をかける攻撃をD（Distributed＝分散型）DoS攻撃と言います。DDoS攻撃の被害を受けるだけでなく、踏み台のサーバーとして攻撃を行う加害者になるリスクがあります。

■事例
2024年の年末から2025年の年初にかけて、金融機関や公共インフラ、通信事業者が相次いで攻撃を受けて、多くのサービスが遅延・停止に陥りました。

■手口
●複数のデバイスを不正に乗っ取り、そこから一斉にDoS攻撃を行う

対策
●アクセス許可を日本に限定する
●CDNを利用する
●WAFによる不正アクセスの検知・遮断

次ページへ

前ページより

Topics

初選出

7位　地政学的リスクに起因するサイバー攻撃

■概要

地政学的リスクとは、特定地域が抱える政治的・軍事的・社会的な緊張の高まりが、地理的な位置関係によって与える悪影響のことを指します。具体例で言えば、国家の関与が疑われる高度で組織的なサイバー攻撃のことです。

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。

- ●認証を適切に対応する
- ●情報リテラシー、モラルを向上させる
- ●添付ファイルの開封やリンク・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PC、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

上記の中から弊社へのご相談も多い、「サーバーやPC、ネットワークに適切なセキュリティ対策を行う」について、方法をご紹介いたします。

- ●ネットワーク管理を適切に行う
  Fire Wall、プロキシサーバーの設置、不要ポートの遮断　等……
- ●脆弱性対策を適切に行う
  OSのサポート期限、更新プログラムの適用　等……
- ●セキュリティ製品を導入する
  WAF、IDS/IPS　等……
- ●アクセス権限管理を適切に行う
  不要なアカウントを作成しない、アクセスログの監視　等……
- ●その他
  定期的に脆弱性診断を行う、ペネトレーションテストを行う　等……

上記は一例ですが、セキュリティ対策は多岐に渡るため、環境によって適切な対策をする必要があります。記載した対策のほとんどは、弊社でもご提案可能です。気になることがございましたら、是非1度ご相談くださいませ。

#2　リリース予定　安心安全なAI活用の未来へ　「あんしんオフィスGPT」

当社はこの度、グループ企業である「株式会社エボルブ社」と提携し、**安心安全な生成AIサービス「あんしんオフィスGPT」をリリースいたします**（正式リリースは2025年4月以降です）

アメリカのオープンAI社が2022年11月30日に発表した「ChatGPT」は、世界中に瞬く間に広がり、我々のような一般ユーザが気軽に「AI（人工知能）」を利用できるようになりました。ChatGPTの登場をきっかけに、非常に多くの生成AIサービスが市場に登場したことから、2023年はAI元年とも呼ばれています。
すでに個人や企業レベルで、メールや資料作成などに活用されているケースもあるかと思いますが、ChatGPTに、社内の機密情報や個人情報などを記入したり、ファイルを添付したりするのは、セキュリティ的にもまだまだ抵抗がある企業様も多いのではないでしょうか。
そのようなお悩みを抱える企業様向けに、高セキュリティな専用の生成AI環境をご提供するのが「あんしんオフィスGPT」です。
ChatGPTを始めとした「SaaS型」の生成AIサービスは、オペレーションミスやプログラムの不具合で情報漏えいが発生するリスクも抱えていますが、お客様専用の環境を提供する「あんしんオフィスGPT」であれば、そのような心配は不要です。

あんしんオフィスGPT

次ページへ

前ページより

あんしんオフィスGPTの特徴

✓ お客様専用の環境を提供するため安心
✓ 生成前後の情報の権利侵害もチェックでき安心
✓ Azureで作られた環境を24365で監視しているので安心

プラン例	Aプラン	初期費用	月額費用
	～30名	60万円（税抜き）	6万円（税抜き）

正式なリリースは2025年4月以降を予定しておりますが、サービス資料やデモ環境をご案内することもできますので、ご興味がありましたら以下のサイトもしくは、ネットアシスト営業部までお気軽にお問い合わせください。
あんしんオフィスGPT特設ページ
（https://aogpt.netassist.ne.jp/）

#3 AI博覧会　Spring2025　出展のお知らせ

国内最大級のAIポータルサイトを運営する、アイスマイリー社が主催する「AI博覧会Spring2025」に**ネットアシストも出展いたします。**
当社のブースでは、メイン事業であるサーバーの保守サービスを中心に、先の記事でご紹介した「あんしんオフィスGPT」もご紹介いたします。
皆様、是非ご来場くださいませ！

会　期　2025年
3月27日（木）～3月28日（金）

会　場　東京都立産業貿易センター浜松町館
（4F・5F展示室）

住　所　東京都港区海岸1丁目7-1
東京ポートシティ竹芝オフィスタワー

参考：https://aismiley.co.jp/ai_hakurankai/2025_spring/

ブースイメージ

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