NET ASSIST
24/7 Guardian Deity

2024.12 #43

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」TOP3

2024年が間もなく終わりますね。そこで今年の締めくくりとして、2024年に多かったセキュリティインシデントTOP3をご紹介いたします！年々増加するセキュリティ被害ですが今年も増加しており、どなたの身にも起こりえる身近な脅威になっています。今年1年間のトレンドをチェックして、2025年のセキュリティ強化の参考にしていただければ幸いです。

順位

1位 ランサムウェアによる被害

2位 サプライチェーンの弱点を悪用した攻撃

3位 内部不正による情報漏えい等の被害

※下記を参考に独自集計し、事例数や事例内容等からランキングにしています。

・独立行政法人情報処理推進機構「情報セキュリティ10大脅威2024」
https://www.ipa.go.jp/security/10threats/10threats2024.html
・CSC社「2024年第3四半期 Webアプリケーションを狙ったサイバー攻撃検知レポート」
https://www.cscloud.co.jp/news/press/202410227554/
・トレンドマイクロ社「2024年上半期における法人・個人に対するサイバー攻撃を解説」
https://www.trendmicro.com/ja_jp/jp-security/24/j/securitytrend-20241001-01.html
・ScanNetSecurity
https://s.netsecurity.ne.jp/

1位 ／ ランサムウェアによる被害

ランサムウェアとは、感染させたサーバーやコンピューターのファイルを暗号化して、元に戻す事と引き換えに身代金を要求するタイプのマルウェアです。さらに現在は、身代金を支払わないとデータを流出させる、という脅迫もしてくるため企業にとってはとてつもない脅威になっています。

そのランサムウェアが昨年に引き続き今年も、最も被害の多いセキュリティインシデントになりました。今年はランサムウェアをしかける国際的なサイバー犯罪集団ロックビットが摘発され、2月にメンバーの2人が逮捕されました。さらに後日、他のメンバーも数人逮捕されています。日本でも2021年10月に、徳島県の半田病院で電子カルテや会計システムに被害が出た事が話題になりました。

ロックビットの摘発で少しは被害が減少するかと思われましたが、期待を裏切って被害は増加の一途を辿っています。理由としては別グループの活動が活発になっているためです。今年で特に有名になったのは、KADOKAWAへのランサムウェア攻撃で記憶に残っている方も多いでしょう。

ランサムウェアはサイバー犯罪の収益として確立しているため、2025年も被害が続くと予想されています。

2位 ／ サプライチェーンの弱点を悪用した攻撃

サプライチェーン攻撃とは、セキュリティレベルの低い取引先や子会社を経由する事で、侵入が難しいセキュリティレベルの高い親会社などに侵入する方法です。信用している取引先や子会社を経由して侵入してくるため、気付かない間に被害が増大していきます。

サプライチェーン攻撃も、昨年に引き続き2番目に多いセキュリティインシデントになりました。サプライチェーン攻撃には右記3つの分類があります。

今年で特に有名になったのは2月14日のLINEからの公表で、委託先2社を通じた不正アクセスがあったとの事でした。委託先従業員のコンピューターがマルウェアに感染し、そのコンピューターを通じてLINEのシステムに不正アクセスが行われていました。その後、委託先管理の強化を再発防止策として挙げています。

ビジネス サプライチェーン攻撃
関連組織や子会社、取引先などを侵害し、標的組織への侵害を図る攻撃

サービス サプライチェーン攻撃
サービス事業者を侵害し、サービスを通じてその顧客に被害を及ぼす攻撃

ソフトウェア サプライチェーン攻撃
ソフトウェアそのものやアップデートプログラムなどに不正コードを混入し、標的組織に侵入する攻撃

次ページへ

前ページより

3位 ／ 内部不正による情報漏えい等の被害

内部不正による情報漏えいは言葉の通り、組織内部者の不正行為によるセキュリティインシデントです。一般的に外部からの攻撃より、被害額が高額になっています。また取引先や顧客から見ると、その会社の不正になるため社会的信用を大きく失う事になります。

その内部不正情報漏えい被害が今年は初のTOP3入になりました。独立行政法人情報処理推進機構から結果が発表されていますので、下記に引用いたします。

1. 内部不正の理由の約6割は故意が認められない“うっかり”

内部不正経験者に行為の理由を聞いたところ、“うっかり違反した”が40.5%、“ルールを知らずに違反した”が17.5%（合計58.0%）と、全体の約6割は“うっかり”によるもので、故意が認められませんでした。うっかりミス等を防ぐため、管理者は扱う情報に格付けする等のルールや規則を明確にし、周知徹底することが対策として有効です。
その一方、42.0%は故意によるもので、その理由は“業務が忙しく、終わらせるために持ち出す必要があった”が16.0%、“処遇や待遇に不満があった”が11.0%などでした。

2. 主たる情報の持ち出し手段は“USBメモリ”

情報の持ち出しには“USBメモリ”の利用が最多でした。組織での対策はUSBメモリ等の外部記録媒体に関する利用ルールの徹底、および利用制限が有効と考えられます。しかしその対策状況をみると、従業員規模が300名未満の企業の過半数で“方針やルールはない”と回答しています。

3. 経営者等が重要視していない対策が内部不正行為の抑止に有効

内部不正経験者と経営者・システム管理者とで、有効と考える内部不正対策の違いが顕著だったのは“罰則規定を強化する”、“監視体制を強化する”ことでした。なお、監視強化についての意識の差は前回調査でも同様の傾向が示されています。不正行為抑止のためには、監視だけでなく、監視している旨を通知することが有効です。
経営者・システム管理者は、不正行為を思い留まらせるのに有効な
対策を的確に把握し、実施する必要があります。

4. 内部不正経験者の約5割がシステム管理者（兼務を含む）

内部不正経験者の職務を尋ねたところ、51.0%がシステム管理者（兼務を含む）でした。システム管理者は社内システムに精通し、高いアクセス権限（特権）を有することが多いため、権限の最小化・分散、および作業監視等の対策が有効です。

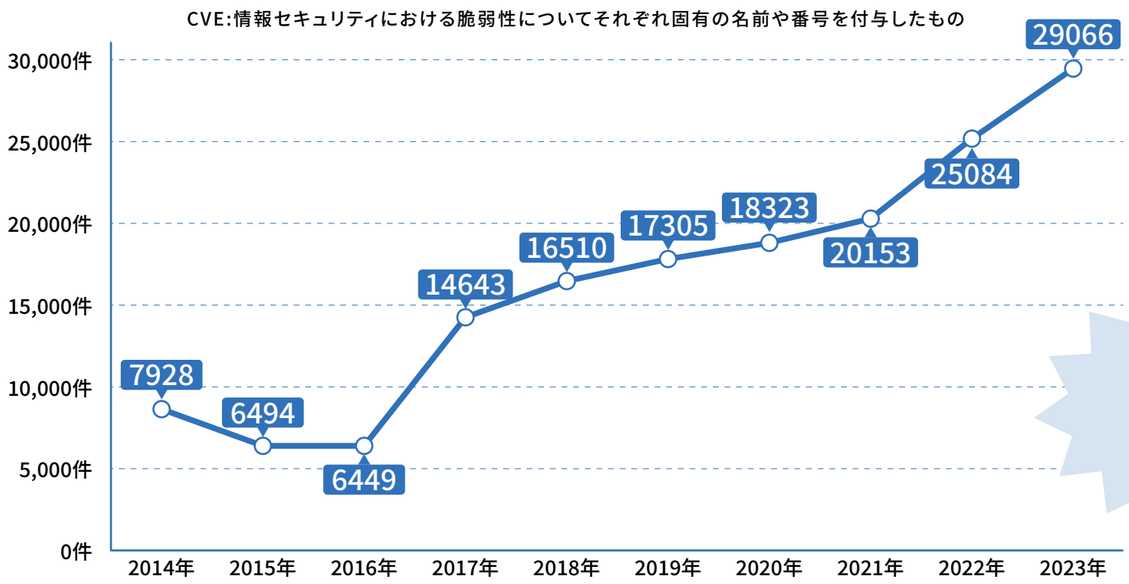
対策が難しいと言われる内部不正対策ですが、できる事はたくさんありそうです。

セキュリティインシデントを防ぐためには、IDS/IPSやWAF、アンチウィルスなどの仕組みと、業務に携わる人への教育が大切ですね。

#2 継続的な脆弱性対策

12月11日にサイバーセキュリティクラウド社と合同で、脆弱性管理のセミナーを開催いたしました。参加いただいたお客様ならびにイベント運営にご助力いただいた皆様、誠にありがとうございました。
久しぶりの開催でしたが、大変充実した内容で無事に終えることができました。
今回は、日程が合わず参加ができなかった方向けに、セミナーの内容を要約してお届けいたします。

継続的な脆弱性対策



脆弱性の発見数は年々増えており、2023年には1日に換算して約80件もの脆弱性が報告されていることになります。それに合わせて脆弱性を突いた攻撃も急増しており、年に数回の脆弱性診断では対策が追いつかないのが現状です。そこで、継続的な脆弱性対策として「脆弱性管理」というアプローチが重要になります。

1日約80件の脆弱性が発見！

次ページへ

前ページより

「脆弱性管理」と「脆弱性診断」の違い

■脆弱性管理

WEBアプリケーションや、OS／ミドルウェア、ソフトウェアの脆弱性情報を収集・評価し、対応するまでの管理体制を含めた「脆弱性を修正するまでのサイクル管理」のことです。
継続的に脆弱性対策を行うことで、重大な脆弱性が放置されるリスクを回避します。
脆弱性を人間の病気に例えた場合、手洗いうがいや栄養バランスの良い食事など、病気にならないための毎日の健康管理と考えられます。

目的
脆弱性を修正するまでのサイクル管理

効果
重大な脆弱性が放置されるリスクの回避

■脆弱性診断

WEBアプリケーションや、OS／ミドルウェア、ネットワークに潜在する「その時点での脆弱性の有無を調査」するものです。プロの手や専用のツールを用いることで、項目ごとに詳細な診断が可能です。ただし、確認できるのは診断時の脆弱性に限ります。
同じく脆弱性を人間の病気に例えた場合、こちらは病院での診断と考えられます。

目的
脆弱性の有無を調査

効果
診断時点での脆弱性を解消

「脆弱性診断」は、「脆弱性管理」のプロセスの一部とも考えることができます。

脆弱性管理のサイクル

脆弱性管理は下記のサイクルを繰り返すことで、継続的な対策をします。

1 収集

WEBアプリケーションや、OS／ミドルウェア、ソフトウェアの脆弱性と、対応する「セキュリティパッチ」の情報収集を行います。
収集には下記のようなサイトを活用するのが一般的です。

- JVN iPedia　日本の脆弱性データベース
  https://jvndb.jvn.jp/
- NVD　世界の脆弱性データベース
  https://nvd.nist.gov/
- WEBアプリケーションや、OS／ミドルウェア、ソフトウェアの各種製品ベンダーサイト

2 評価

情報収集ができれば、リスクの評価を行います。評価には「CVSS」という指標が活用され、共通の基準で定量的に比較することができます。ただし、CVSSは技術的な深刻度を数値化した指標のため、サーバー環境ごとのセキュリティリスク度合いと必ずしも一致しないことに注意が必要です。

3 対応

評価の次は、実際に脆弱性への対応を行います。収集したセキュリティパッチの適用やプログラムの更新により対応します。
アップデートの対象によってはサーバーの再起動が必要になる場合もあります。

4 管理

これら一連のプロセスを記録して管理します。脆弱性は日々膨大な量が更新されていくため、リスクに合わせて実際に対策したものを常に管理しておくことが大切です。
そして、①～④のサイクルを繰り返し継続する必要があり、非常に手間やコストがかかるのが脆弱性管理の課題です。

次ページへ

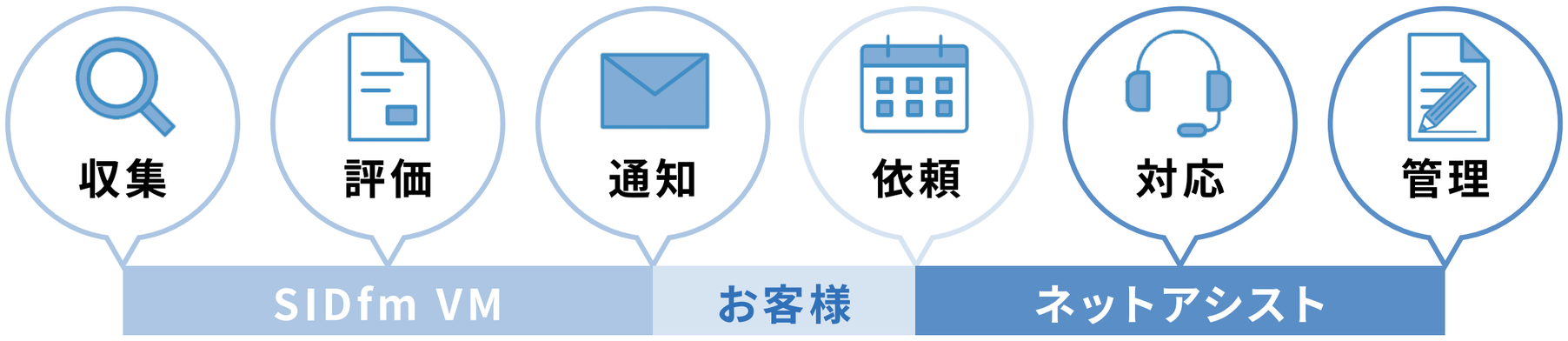
前ページより

ネットアシストの脆弱性管理サービス

弊社ではセキュリティ事業者であるサイバーセキュリティクラウド社の「SIDfm VM」を利用した「セキュリティアップデートサービス」を提供しております。こちらは弊社の保守運用代行サービス「MSPアシスト/AWSアシスト」の追加オプションとしてご案内しております。

■サービスのご紹介

SIDfm VM により自動で脆弱性とサーバーの情報を収集し、「SRI」という環境に合わせた指標で評価します。脆弱性がSRI値「重大」と評価されたものはお客様に自動でメール通知いたします。そしてお客様にご依頼いただき、弊社にてアップデート対応いたします。また、脆弱性への対応状況はSIDfm VMの管理画面にて、作業履歴は弊社のポータルサイトにてそれぞれ確認が可能です。



■セキュリティアップデートサービス料金プラン

初期費用/1台あたり（税抜き）
30,000円～

月額費用/1台あたり（税抜き）		
シルバープランご利用	ゴールドプランご利用	ゴールドプラスご利用
対象外	+20,000円～	+10,000円～

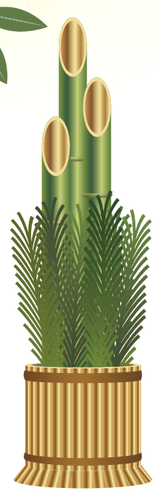
※本サービスはMSPアシスト/AWSアシストのオプションサービスとしてご提供しております。セキュリティアップデートサービスのみのご契約は対応できかねますので、何卒ご了承ください。

#3 年末年始休業のお知らせ

日頃より弊社サービスをご利用いただき誠にありがとうございます。
本年度の年末年始休業についてお知らせします。

年末年始休業

2024年12月28日（土）～2025年1月5日（日）



サービスデスクは24時間365日稼働しております。
ご契約中のお客様におかれましては、技術的なお問合せがございましたらサービスデスク宛てにご連絡ください。

サービスデスク 03-3985-6781/sd@netassist.ne.jp

営業部、管理部(経理・ドメイン/SSL)へのお問い合わせに関しては、年末年始休業明けの2025年1月6日（月）以降に順次回答させていただきます。
ご不便をおかけいたしますが、ご了承いただきますようお願い申し上げます。

本年も大変お世話になり誠にありがとうございました。来年も変わらぬご愛顧の程よろしくお願いいたします。

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