今求められるセキュリティ対策について

～セキュリティインシデントはすぐ近くで起こっている～

Sorridente

株式会社ソリデンテ　〒574-0063　大阪府大東市南郷町2-21　Tel:050-5889-8310 Fax:072-344-5320
http://www.sorridente.biz/

会社概要

【社名】	株式会社ソリデンテ
【創業】	2014（平成26）年7月14日
【設立】	2019（令和元）年7月1日
【取引銀行】	りそな銀行 住道支店／三菱東京UFJ銀行　大東支店
【認定】	経済産業省認定情報処理支援機関（スマートSMEサポーター）
	IT導入支援事業者（IT導入補助金）
【主要取引先】	日本マイクロソフト株式会社／TDシネックス株式会社
	株式会社セールスフォース・ジャパン／サムライシステム株式会社
	Rakumo株式会社／日本事務器株式会社
	サテライトオフィス株式会社／ネクストセット株式会社
	ワークスモバイルジャパン株式会社
【取扱サービス】	Microsoft365シリーズ、Google WorkSpaceシリーズ
	LINE WORKSシリーズ、Salesforce各種ライセンス
	kinotne各種ライセンス、カスタマーコンパス各種ライセンス
	セキュリティあんしんプラスシリーズ
	LANSCOPEシリーズ、各種クラウドサービス、各種セキュリティ

自己紹介

大東正明（だいとうまさあき）

- 1979年3月24日生まれ。大阪府大東市生まれ。
- 大東中央幼稚園→大東市立南郷小学校→四條畷学園中学校→清風高校
- 関西大学商学部卒業後、民間企業、自治体、医療機関向けの業務支援システムを導入する企業に10年在籍。その後、独立開業し地域密着型のITコンサルタントとして、中小企業の課題解決支援を行なっています。
  Microsoft、Google、LINE WORKSの法人向けクラウドライセンスの販売に注力しています。
  SalesforceやkintoneやノーコードシステムやAI開発も実施しています。位置情報活用アプリケーションの販売・導入も行なっています。
- 現在、デジタル庁にてデジタル推進委員を拝命しており、地元の大東商工会議所では、ITアドバイザーをつとめています。日本商工会議所青年部では「講師名鑑」認定講師として全国のYEGから講演依頼をいただいております。
- DXなどの企業向け研修に留まらず、青少年育成事業として中高生を中心にSDGsワークショップを開催しています。
- 趣味は家族旅行とゴルフです。令和3年度から日本YEGに出向する様になり、日本中を旅するようになりましたが、家族が一緒じゃないので寂しい限りです。。。

１．セキュリティインシデントとは？

セキュリティインシデントとは？

一般に言うところのセキュリティインシデントとは、「情報セキュリティインシデント」を指します。「情報セキュリティインシデント」とは、マルウェア感染や不正アクセス・記録媒体の紛失など、企業の安全を脅かし事業などの運営を危ぶむ事象のことです。サイバー攻撃だけでなく、自然災害や設備不良・内部不正による情報漏洩などもセキュリティインシデントに含まれます。

セキュリティインシデントは、主に3つのパターンに分類されます。

分類	概要
サイバー攻撃によるもの	マルウェアや不正アクセス・標的型攻撃など、第三者による悪意ある攻撃のこと。
災害・外部サービスによるもの	自然災害による社内システムの破損、偽Wi-Fiによる情報抜き取りなどのトラブルのこと。
内部での故意・過失によるもの	企業内部の人間による故意な情報漏洩や、デジタル周辺機器の破損などのトラブルのこと。

サイバー攻撃によるもの

サイバー攻撃によるセキュリティインシデントとは、第三者からの悪意ある攻撃により、システム障害や情報漏洩・不正アクセス・サイトの改竄などが引き起こされるものです。以下のようなサイバー攻撃が考えられるでしょう。

- マルウェア感染
- 標的型攻撃
- DoS攻撃
- ランサムウェア
- SQLインジェクション攻撃

これらはそれぞれ、攻撃の手口は異なります。マルウェア感染や標的型攻撃・SQLインジェクション攻撃などは情報漏洩を引き起させることが主な攻撃です。また、DoS攻撃やランサムウェアはシステムの障害が主な症状です。

情報漏洩が起これば、社会的信用の失墜は免れられないでしょう。システム障害で管理サイトなどが停止するなどの状態を引き起こされることになれば、顧客の不安を煽ることとなり、こちらも信用問題に関わります。

災害・外部サービスによるもの

自然災害や外部サービスによるセキュリティインシデントは、設備の破損や外部サービスに接続などした結果として起こります。システム障害などが考えられるでしょう。主に以下のような要因が考えられます。

- 停電や台風によるシステム停止
- 地震や水害・火災によるデジタル機器や設備の故障
- クラウドサービスなど外部サービスのエラーや停止
- ネットワーク環境の脆弱性発覚による自主的なサービスの停止

災害や外部サービスによるセキュリティインシデントでは、システムの停止が起こる可能性だけでなく、企業の社内ネットワークそのものが破損することも考えられます。

業務がストップしてしまうことに加えて、事業の再開に時間がかかる・再開が不能になることも考えられるセキュリティインシデントです。

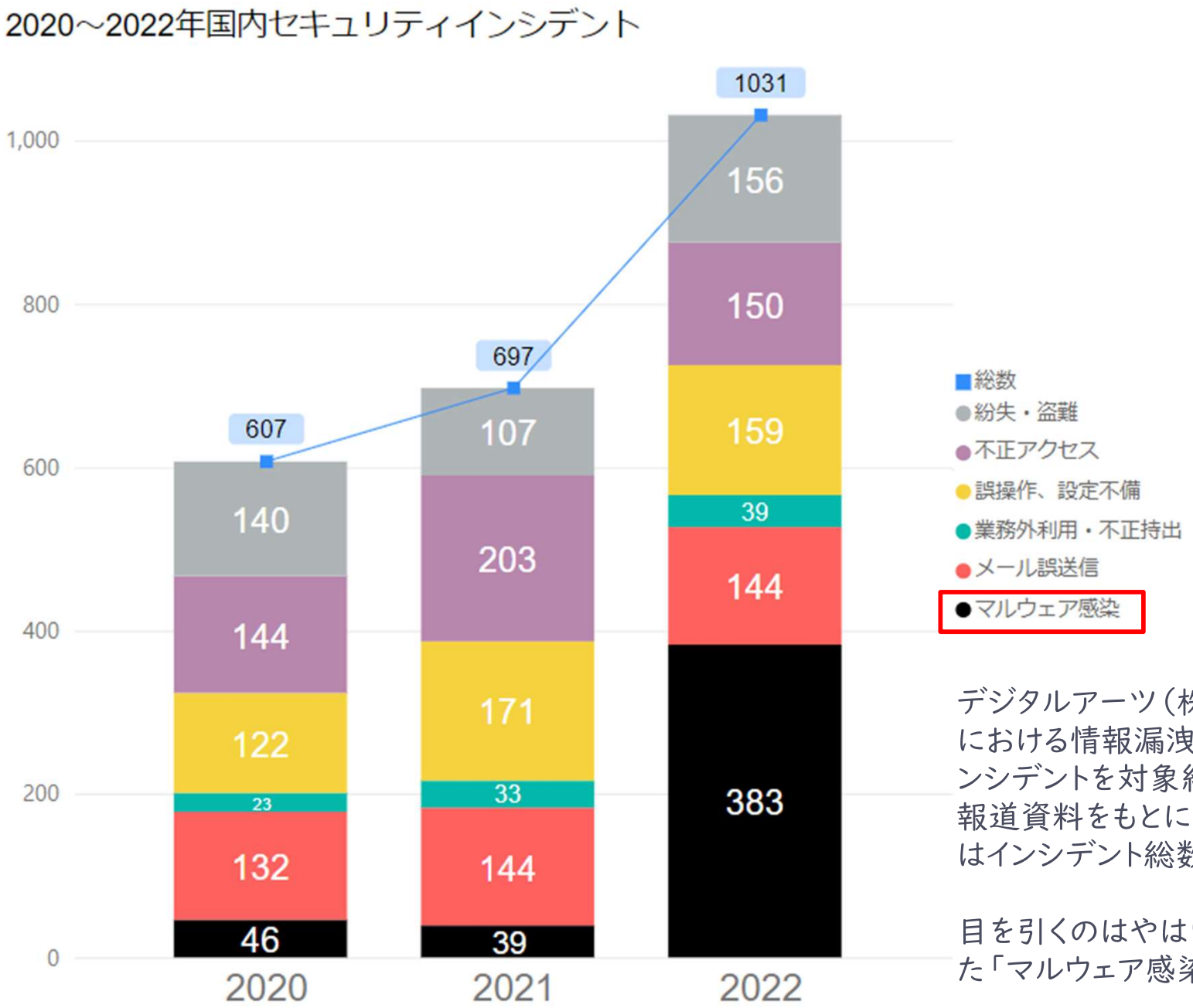
内部での故意・過失によるもの

企業や組織内部の人間による故意・過失で、セキュリティインシデントが起こる場合があります。具体的には、以下のような状態が考えられます。

- 記録媒体など社外持ち出し時の紛失
- 情報共有時の誤送信
- 不注意のよるデジタル機器の破損

記録媒体の紛失や誤送信などは、情報資産が第三者の手に渡る状態となります。情報漏洩につながり、企業や組織の信用を落とす結果になりかねません。また、ヒューマンエラーによって使用しているデジタル機器を破損させた場合、復旧するまでに業務が滞るなど支障をきたし、顧客対応などが遅れるなど発生する可能性が高まるでしょう。

過去3年分の国内セキュリティインシデント集計



デジタルアーツ（株）が、2022年国内組織における情報漏洩等にかかるセキュリティインシデントを対象組織による公開報告書や報道資料をもとに集計したグラフ。2022年はインシデント総数が1031件となりました。

目を引くのはやはり昨年比で約10倍となった「マルウェア感染」インシデントです。

2. セキュリティインシデントの被害事例

大阪急性期・総合医療センター（外的要因による）

2022年10月、公立病院である大阪急性期・総合医療センターにおいて、ランサムウェアによるサイバー攻撃が発生。電子カルテの利用や閲覧ができなくなり、地域の医療提供体制に影響が出ました。

食事搬入などを担当していた事業者のシステムから侵入した可能性が高いとされ、古いバージョンのままセキュリティ機器を使用していたことによる脆弱性が、侵入の要因だと考えられています。

厚生労働省は2021年6月に発表していた「医療機関を標的としたランサムウェアによるサイバー攻撃（注意喚起）」に加え、2022年11月には「医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起）」を発表。

内閣サイバーセキュリティセンターにて、ランサムウェア対策に関する特設サイトを作成し、注意喚起をおこなっています。

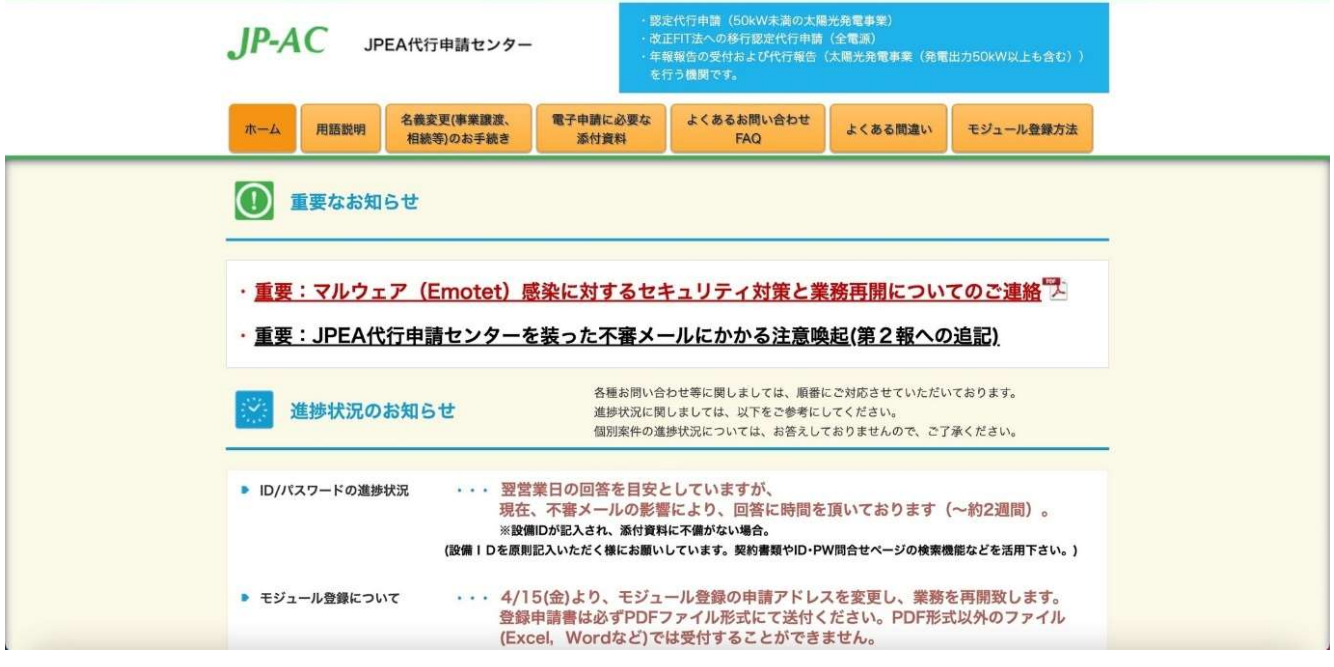
https://www.youtube.com/watch?v=BgaQhFqtwDU

一般社団法人太陽光発電協会（外的要因による）

2022年3月には、政府や自治体へ太陽光発電システムなどに関する提言活動も行う企業である一般社団法人太陽光発電協会（JPEA）にて、マルウェアであるEmotetの感染が発覚しました。

JPEA代行申請センター職員の端末がEmotetに感染した影響から、端末内のメール情報約85万件とメールアドレス約9万5千件が漏洩したことが明らかになっています。

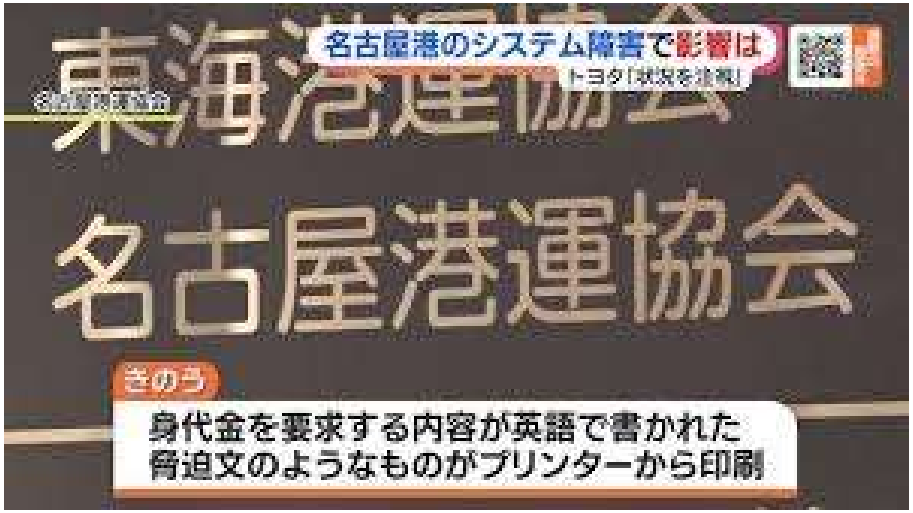
感染が確認された端末は即時ネットワークから隔離、全端末の感染チェック及び感染端末のメールドメイン停止の措置を行っています。再発防止策として、外部のセキュリティ専門機関の指導の元でシステム環境を新規構築されました。



名古屋港運協会（外的要因による）

2023年7月、名古屋港統一ターミナルシステム（NUTS）に障害が発生し、名古屋港運協会と愛知県警察本部により、システム障害の原因がランサムウェア感染であることが判明した。結果的に7月4日から6日にかけて、コンテナの搬出入作業が一時中止された。システムは6日7時半に復旧し、搬出入作業は同日午後から順次再開されたとしている。

名古屋港のコンテナターミナルがサイバー攻撃の被害を受けたことを受け、インテリジェンスアナリストのJohn Hultquistは「攻撃者は港湾や輸送・ロジスティクス拠点を攻撃することで、複数の関連組織全体にまで連鎖的な影響を引き起こすことができる（＝ゆえに身代金を支払いやすい）」と指摘している。



https://www.youtube.com/watch?v=yWiSk6G4G4s

３．中小企業の経営者が陥りがちな誤った認識

①「ウイルスソフトをいれているから大丈夫」

サイバー攻撃を防ぐためのウイルスソフトの導入は主要な対策の一つですが、完璧に防げるものではありません。なぜなら、新たなサイバーウイルスは日々無数に生み出されているからです。

例えば、新たに脅威となるサイバーウイルスが発生しそのウイルスソフトを開発するとしても、少なくとも半年から1年はかかります。また無数に存在するサイバーウイルスに対応できるソフトを作るのは、現実的に不可能です。

専門家の意見では、最新のウイルスソフトを入れたとしても、世の中の40%～45%程度のサイバーウイルスしか検知できないだろう、といわれています。よって、ウイルスソフトだけではセキュリティ対策は不十分なのです。

②「うちみたいな小さな企業が狙われるわけない」

規模の小さい中小企業だからといって、インシデントが起きない、サイバー攻撃を受けないということは全くありません。なぜなら、「サプライチェーン攻撃」という事故が主流になりつつあるからです。

「サプライチェーン攻撃」とは、まだセキュリティ対策が脆弱な中小企業を狙い、そこを踏み台として大企業を襲うという攻撃です。仮に大企業がサプライチェーン攻撃によって被害を受けた場合、事故の発端となる元請企業や関連会社に対し、多額の賠償請求や調査請求を行います。

よって、たとえ中小企業であってもサイバー攻撃の対象に十分なり得るのです。

③「個人情報を扱わないから大丈夫」

個人情報を持たないのであれば、情報漏えいリスクは低いといえるかもしれません。

しかし取引先に大企業や大口客先がある場合、前段で説明した「サプライチェーン攻撃」を受けて、知らぬ間に取引先に被害を与える可能性があります。身に覚えがなくとも、自社が加害者となって取引先にサイバー攻撃をしかける可能性があるのです。

たとえ個人情報を扱っていない企業でも、セキュリティ対策を行う必要があるのです。

④「怪しいサイトにいかないから大丈夫」

「怪しいサイトや不要なサイトに訪問しないこと」を、社内に徹底することは大切なことです。

しかしながら、メイン銀行のネットバンキングやAmazon・楽天等のECサイトを装った悪質サイトによる被害や、フィッシング詐欺も頻発しています。

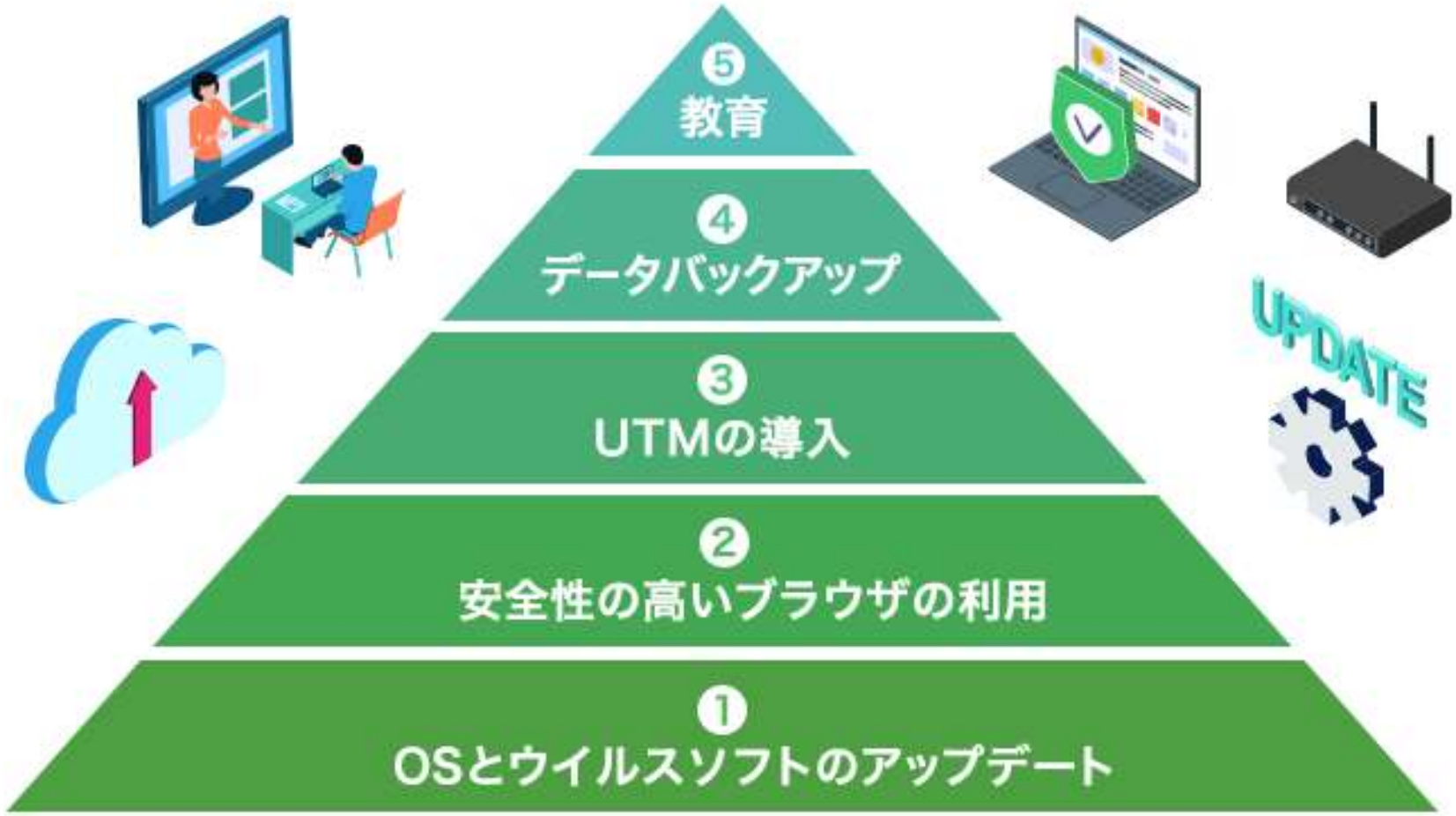
日常と同じルーチンでメインのネットバンキングから入金しようとしたところ、実は全く同様のネットバンキングを装った悪質サイトだったことに気づかず、会社のIDやパスワードが抜き取られ、多額の資金をだまし取られるという事例も発生しています。

社会問題である“オレオレ詐欺”が日々巧妙化していることと同様、サイバー攻撃やフィッシング詐欺も巧妙化しています。「自社は大丈夫だろう」と慢心せずにインシデントや事故に備えることが重要です。

４．中小企業が行うべき最低限のセキュリティ対策とは？

最低限のセキュリティ対策

以下の図は、下層から上層にかけて、行うべきセキュリティ対策の重要度を示したものです。
ぜひ参考にして、重要度の高いものから対策を始めてください。



①ＯＳやウイルスソフトの最新アップデート

OSのアップデートには、セキュリティ強化に関するバージョンアップも多く含まれてますので、WindowsやMacOSなど、定期的なバージョンアップは必ず実施してください。

注意点としては、バージョンアップのためには必ず再起動する必要があるということです。PCをシャットダウンする習慣がない人は、必ず作業終了時にシャットダウンすることを意識してください。

②安全性高いブラウザの利用

ネット上で検索作業するときは、必ず安全性の高いブラウザを利用する様にしてください。

安全性の高いおすすめブラウザは、「Google Chrome」もしくは「Edge」です。もし社内で利用ブラウザを統一していない場合は、これらに統一する事をご検討ください。

③ＵＴＭの利用

UTMとは「統合脅威管理（Unified Threat Management）」の略で、コンピューターネットワークを包括的に保護する管理手法の一つです。インターネットと社内ネットワークの間に設置するセキュリティ機器で、以下の様な機能を持っています。

- 迷惑メールやフィッシング詐欺メールの拡散を未然に防ぐ
- ウイルスが付着している添付メール等を未然に防ぐ
- 知らずにウイルス感染サイトに立ち寄ろうとした場合でも入口でブロックする
- 業務に不要なサイト情報を集めて未然にブロックする
- ファイアウォール機能

④データのバックアップ

データのバックアップは必ず定期的に取るようにしてください。
データさえしっかり残っていれば、万が一の際にも自社の業務はすぐ復旧させることが可能です。

手動や自動化ツールでまとまったデータをこまめにバックアップする方法もありますが、日常使用するメールや共有データについてはMicrosoft365やGoogle WoekSpace等のクラウドサービスを利用することによって、意識する事なくデータの冗長化を図ることが可能になります。

⑤社内勉強会や標的型メールの実施

定期的に社内向け勉強会や標的型メールを実践し、従業員教育を行うことをお勧めします。
情報セキュリティインシデントや事故は、ほとんどのケースが人間を起点として発生するものだからです。

- 同業他社でインシデントが発生したニュースをしたら社内に伝達する
- 定期的に社内データを棚卸しし管理・確認する
- 従業員向けに標的型メール等を実践し、不用意にメールやファイルを開かないよう意識付けし続ける

5．まとめ

まとめ

セキュリティインシデントとは、事業の運用を危ぶませるような情報セキュリティ事象のことです。サイバー攻撃・自然災害などの外的要因、内部の人間による故意・過失という内的要因により発生する場合もあります。

近年、サイバー攻撃による企業組織の被害事例がたびたび発生しています。事前のセキュリティ対策はもちろん、セキュリティインシデント発生後に迅速な対応が行えるよう、経営者は勿論、従業員の方にも適切な教育を行うことが重要です。

その上で、組織に応じたセキュリティツールをご検討くださる事をお勧めします。

～スムーズなIT活用で笑顔を創造する～

Sorridente