＜新かわら版発刊について＞

今回より、通常のかわら版とは別に情報セキュリティに特化したかわら版を発行させて頂く運びとなりました。
世界が一つで繋がっているインターネットでは世界情勢によってサイバー攻撃は何らかの形で我々の身近にまで迫ってきています。
（ウクライナ情勢でもサイバーテロが実際に発生しており、いつ飛び火してくるか分かりません）
企業をサイバー攻撃から守るためにも常に最新の情報を知っておくことが非常に重要です。
少しでもお役に立てる情報発信するツールとして、皆様のお役に立てれば幸いです。

＜今回のトピックス＞

2022年4月1日より、改正個人情報保護法が全面施行されます。

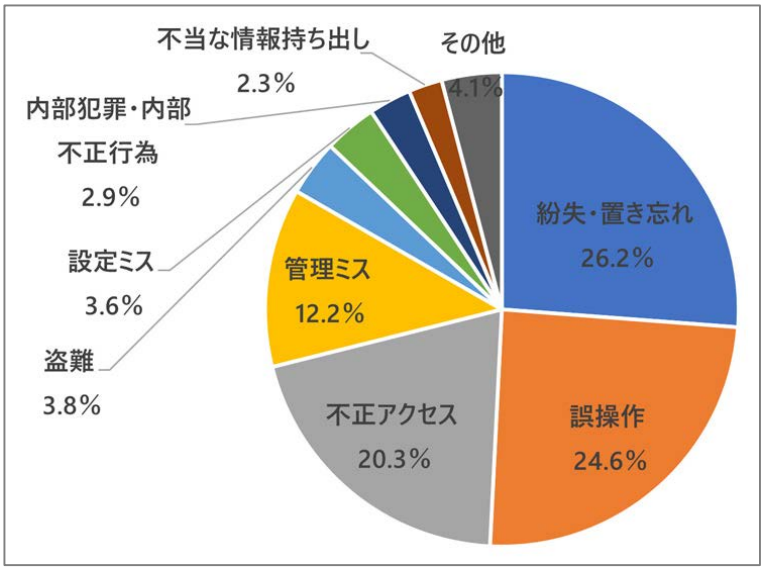
＜主なポイント＞

①ペナルティの厳罰化
②安全管理措置の開示が義務化
③個人情報漏えいの報告義務と本人への通知の義務化

＜企業として求められること＞

①社内データをサイバー攻撃の脅威から守るための、総合的なセキュリティ対策。
②情報セキュリティ全般における管理手法の強化。
③情報漏えい時の報告に必要なサイバー攻撃ログ管理

＜情報漏えいの主な要因＞



今回の法改正で、情報資産管理の厳格化がさらに求められます。
この機会に、今一度社内の情報セキュリティを見直してみましょう！

GODO情報セキュリティかわら版
第1号
令和4年3月発行
ゴードービジネスマシン株式会社

＜情報セキュリティ関連ニュース　2022年2月＞

PCウイルス

エモテット再び猛威
世界で被害270万件超

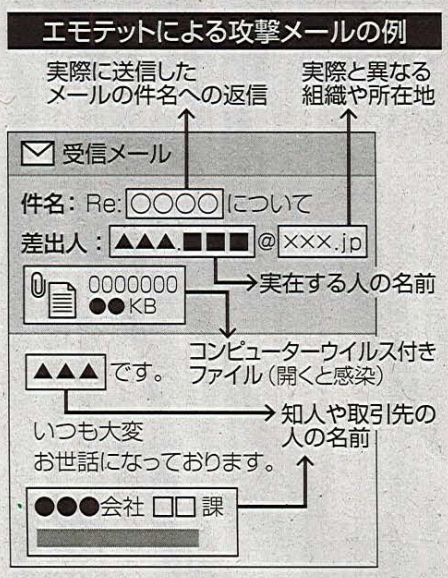
メールの添付ファイルを開くと感染するコンピューターウイルス「Emotet（エモテット）」が全世界で再び猛威を振るい、2021年末から270万件超が確認されたことが15日、米情報セキュリティー会社の調査で分かった。知人や取引先からの返信を装って警戒を緩めさせるのが特徴。国内ではライオンや積水ハウスなど20以上の企業や団体が感染したとみられる。個人情報が盗まれるため専門家は注意を呼び掛けている。

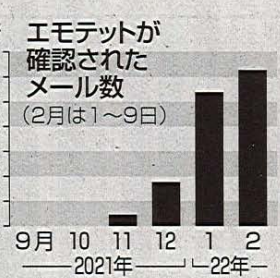
エモテットは大量のパソコンが感染した「最強のウイルス」とも呼ばれ、国際的な捜査でいったんは制圧された。しかし摘発されなかった仲間のハッカーが同様の手法を使って21年末に復活させたとみられる。

米情報セキュリティー会社プルーフポイントの調査によると、21年10月まではほとんど確認されなかったが、21年11月に9万件、22年1月は107万件と大幅に増加し、2月は上旬だけで125万件だった。前回流行時の18年には1カ月で1900万件以上が確認された。

ライオンは2月3日、グループの従業員のパソコンが感染したと発表した。サーバーからメールアドレスと件名などが盗まれ、従業員を装ったメールが送信された。アドレスの「@」以下に記載される、組織や所在地を示す部分が本物と異なっていたという。

積水ハウスは1月末、感染によって、従業員に成り済ましたメールが送られていると公表した。クラシエ





引用文献：大分合同新聞朝刊　2022年2月16日記事

Security NEXT　Security NEXTでは、最新の情報セキュリティに関するニュースを日刊でお届けしています。

マルウェア減るもランサムウェアは前年から倍増

2021年はマルウェアの検知件数が減少するも、ランサムウェアは前年の2倍強に増加したとする調査結果をSonicWallが取りまとめた。

同社がUTMなどグローバルで稼働する約110万台の同社製品をセンサーとして用い、攻撃や脅威情報を収集、分析し、2021年の動向について取りまとめたもの。

マルウェアの検知数は54億件で前年比4%減。3年連続で減少が続いており、2021年は7年ぶりの低水準となった。ただし、上半期に22%減となる25億件となるものの、下半期は29億件に増加しており、年間を通じてはひと桁台前半の減少幅にとどまった。

マルウェア全体では減少するも、2021年に検知したランサムウェアの件数は6億2325万件となり、2020年の3億463万件から倍増。2019年の1億8790万件と比較すると、2年で約3.3倍に拡大している。

米国では全体の105%増をわずかに下回る104%増となったが、アジアでは122%増、ヨーロッパでは175%増と特に増加が目立つ。ランサムウェアのファミリーを見ると、「Ryuk」がもっとも多く、「SamSam」「Cerber」「GandCrab」「CryptoJoker」が続いている。

緊張高まる国際情勢を受けてセキュリティ対策強化呼びかけ - 経産省

経済産業省は、ウクライナ問題など世界情勢で緊張が高まっていることを受け、サイバー攻撃の潜在的なリスクも増加しているとしてあらためてセキュリティ対策の強化を呼びかけた。

経営者のリーダーシップのもと、脅威に対する認識を深め。具体的な対策の強化を進めるよう求めたもの。国内のシステムに限らず、攻撃の足がかりに利用されるとして
国外拠点についても国内と同様の対策を実施するよう求めている。

具体的には、十分な強度のパスワードを用いることや多要素認証の活用、アクセス権限の確認、不要なアカウントの削除など、本人認証の強化やアクセスコントロールの再点検など挙げている。

IoT機器を含めて情報資産の保有状況を把握し、なかでも標的となることが多いインターネットよりアクセスできるVPN機器やゲートウェイなどの脆弱性対策を求めた。

2022年2月24日掲載

引用文献：https://www.security-next.com/

【お問い合わせ】　ゴードービジネスマシン株式会社（大分市下郡北1-2-12）
TEL：097-568-4600　FAX：097-569-0121