信頼される安心を、社会へ。
SECOM
セコムトラストシステムズ株式会社

SECURITY NEWS LETTER 01

2023
January issue

セコムサイバーコントロールセンターでは、24時間365日サイバーセキュリティの脅威を監視・分析しています。
日々の監視で得られた知見をもとに、お客様のセキュリティ対策に役立つ情報をお届けします。

特集

#01 被害にあったその時どうする
もしも、会社のシステムがセキュリティ被害にあったら?

#02 経営層から見た事前の備え
重大インシデントに備える!大切にしたい2つのこと

定期観測レポート / 2022年9月以降の観測値

SECOM Cyber Control Center

特集　#01 被害にあったその時どうする

もしも、会社のシステムがセキュリティ被害にあったら？

- セコムサイバーコントロールセンターでこれまでに支援してきたセキュリティ被害は**560件**
- 被害に遭いお問合せいただいた企業は、いずれも**事前の備え**ができていなかった
- 万が一の事態に実施すべきは『**①保全・調査　②復旧　③公表・報告**』の3項目

◆ 拡がるランサムウェア被害、緊急対応件数は5倍に！

セコムサイバーコントロールセンターでは緊急対応窓口を設置しており、お客様がセキュリティ被害に遭われた時の駆け込み寺として機能しています。これまでの支援は560件にのぼり、年々増加する傾向にあります。中でも特にランサムウェア被害が拡がっており、直近の2年間では対応件数が5倍に膨らんでいます。

これまで緊急対応でご支援したお客様には、ある共通点があります。それは、セキュリティ被害にあうことを想定しておらず、「事前の備えがされていない」ことでした。
多くのお客様では、セキュリティ製品の導入やセキュリティポリシー策定をしているものの、万が一被害を受けた場合の具体的な対応手順や役割分担などが想定されていないケースがほとんどでした。

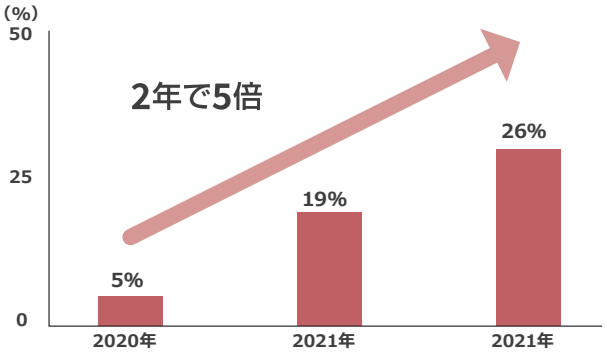

図. 緊急対応窓口で支援した事案のうちランサムウェア被害の割合

いざという時に慌てないようにするため、事前の備えがとても大切です。被害にあうことを前提として、検知の仕組みや連絡網の構築、情報分析と問題解決に役立つ仕組みの導入、知見の蓄積、マニュアルやチェックリストによる対応手順の整備など、社内の状況を見直すことをおすすめします。

◆ セキュリティ被害発生！そのとき現場では何が起こっていたか

セキュリティ被害発生時、現場でいったい何が起こっていたのか、お客様の実例をいくつかご紹介します。
事例から被害状況をイメージし、あらかじめ対応計画を整えておくことで、被害の軽減につながります。

<現場で起きたこんなこと>

- 受発注用のサーバーがマルウェアに暗号化され、取引先との調整に苦労した
- システムを構築した人がすでに退職しており、資料化されておらず影響範囲の確認ができなかった
- システム復旧作業中に役員に頻繁に呼び出され、いつ直るのか？ と何度も聞かれて困った
- 消失データをバックアップから戻すのか？ 構築しなおすのか？ 短時間で判断するのが難しかった
- 被害の公表をどうするのか、取引先への連絡はどうするのか？ 広報担当との相談に苦労した

◆ いまこそ『CSIRT』を設置し、セキュリティ被害を軽減する

CSIRT（シーサート：Computer Security Incident Response Team の略）をご存じですか？セキュリティ被害が発生した際に対応する組織のことで、一般的に専任チームに加え、社内の関係部門の代表者から構成されます。CSIRTでは、セキュリティ被害の発生を前提に、具体的な役割や行動、必要な機能やリソース、関係各所との連絡体制などを検討し、対応計画をあらかじめまとめておきます。

昨今、セキュリティ被害による事業への影響を軽減するため、CSIRTを設置する企業が増えてきました。国内のCSIRTコミュニティ「日本シーサート協議会」には、約470の組織が所属しています。この1年間では新たに40チームが加わり、CSIRTの運営ノウハウや、実際の対処事例などの相互共有が行われ、セキュリティ被害に対する協力の輪が拡がっています。こうしたコミュニティから積極的に情報を収集し、どのような被害が発生しているか傾向を知ることで、脅威への対処のコツをつかむことが期待できます。

万が一の事態が発生！CSIRTが実施する3つのこと

①保全・調査

攻撃や被害の実態を把握するためのログを保全します。サーバーやクライアントPC上のログ、VPNのログ、ファイアウォールのログ、場合によってはウイルス対策ソフトの検出ログなどが保全対象となります。

②復旧

“業務停止状態からの復旧”は、最優先課題です。複数のシステムが停止した場合に備え、あらかじめ復旧の優先順位を決めておくことが必要です。また、リカバリー作業の手順を、定期的な訓練で試しておくことも大切です。

③公表・報告

個人情報が流出した場合は、個人情報保護委員会への報告、業態・業種によっては監督官庁への報告を行います。その他、取引先との契約内容によっては、関係先への報告・情報共有が求められている場合もあるため、被害の公表や報告については経営判断を迫られる重要な局面となります。

特集 #02 経営層から見た事前の備え

重大インシデントに備える！大切にしたい2つのこと

【事例】大手自動車メーカーの迅速な対応から学ぶ

2022年3月、大手自動車メーカーの取引先である部品製造業の企業がサイバー攻撃を受け、14工場28ラインが1日生産停止となりました。このニュースは各種メディアで大きく取り上げられ、サプライチェーン全体の管理・対策の重要性が問われるきっかけとなりました。ニュースの内容では、大手自動車メーカーの「生産が停止した」つまり「攻撃の被害が出た」という結果に注目が集まりがちでした。しかし見方を変えると、**「停止は1日のみ」「次の日から生産は問題無く再開された」**と捉えることができ、そこから新たに見えることがあります

＜現場で起きたこんなこと＞

- 取引先のセキュリティ被害が即座に**情報共有**されている
- 被害の把握から工場の生産停止の**決断と外部への公表**が迅速に行われた
- **必要な安全確認**を行ったうえで、被害拡大は無いと判断し翌日に生産再開している

これらのことから、大手自動車メーカーでは、いざという時に決断が遅れ生産における被害が拡大しないよう、予めの準備を徹底的に実施してきたことがうかがえます。
「直ちに復旧」という課題に対し、いつ復旧できるのか見積ができないまま数日が経過する事態と比べると、事前の備えの有無で、被害に大きな差が出てくるのではないでしょうか。

◆ 拡がるランサムウェア被害、緊急対応件数は5倍に！

大手自動車メーカーの事例から、経営層の視点で大切にしたいポイントを、大きく2つにまとめました。

1．業務継続性の確保

被害の範囲について情報収集し、業務継続への影響を把握できるようにします。業態やサービス内容によっては業務停止を検討する必要があるため、判断条件を明確化します。被害の最小化を目指し、システムの復旧作業等を進め、迅速に業務を通常の状態に戻せるよう準備します。

2．報告・公表

被害発生時、監督官庁等への報告が義務付けられている場合や、契約条件に応じて取引先などに報告する必要があります。個人情報の漏えい時には本人への通知義務があり、外部への公表が求められています。第三者からのレピュテーションリスクを鑑み、予防としての公表という観点も必要です。

セキュリティ被害に伴い、発生するコスト、復旧時間の算出、取引先などへの情報公開手順について、事前に検討し、計画しておくことが重要です。

定期観測レポート
2022年9月～

ダークウェブの観測について

前号のSECURITY NEWS LETTERで、ランサムウェアの攻撃ターゲットとなる侵入先リストや攻撃ツールが売買されている「ダークウェブ」についてご紹介しました。今回から、セコムサイバーコントロールセンターが、ダークウェブで観測した情報についてお伝えしていきます。

(1) 売買されているリーク情報

4つの攻撃者グループ（ランサムウェアグループ）が企業や団体から盗み取ったデータをダークウェブ上に公開（リーク）し、高額で売買しています。9月～10月で検出した結果を、以下の通りです。

ランサムウェアグループ	件数		合計数	先月の件数
	日本	日本以外		
Black Cat(ALPHV)	0	23	23	14
Ragnar Locker	0	7	7	8
LockBit	6	115	121	108
Cheers!	–	–	–	–

表1：リーク検出数（2022年9月15日～10月15日）

「LockBit」という攻撃グループにより、日本企業では6件のリーク被害がありました。海外企業のリーク件数が圧倒的に多い中、「LockBit」についてはいままでにない特徴が見られました。それは、データを盗み出したとする日本企業の説明に、日本語が記載されていたことで、明確に日本企業をターゲットにしていることがわかります。

セコムサイバーコントロールセンターでは、他の攻撃者グループの動向も含め、引き続きダークウェブ観測を続けて参ります。

(2)「LockBit」が攻撃する対象の分析

2022年6月末に「LockBit」が盗んだデータを公開するサイトを刷新しました（名称：LockBit3.0）。
7月～9月の3か月間、LockBit3.0の調査を行い、リークされた企業や団体、その日時について分析しました

①リーク発生タイミング
普段は1日に0～数件で推移し、曜日や月ごとの特長は特段見受けられませんでしたが、9月11日頃は一時的にリーク件数が増加し、1日で50件を超えていました。

②国の分析
どこの国の企業・団体か判断できたものをカウントし、国の割合を示したものが下図の円グラフです。
最も被害件数の多いのが米国（US）で35%、2番目がフランス（FR）で11%、3番目が英国（GB）4%という結果でした。日本は3件のリークが確認できましたが、ワースト10には含まれませんでした。

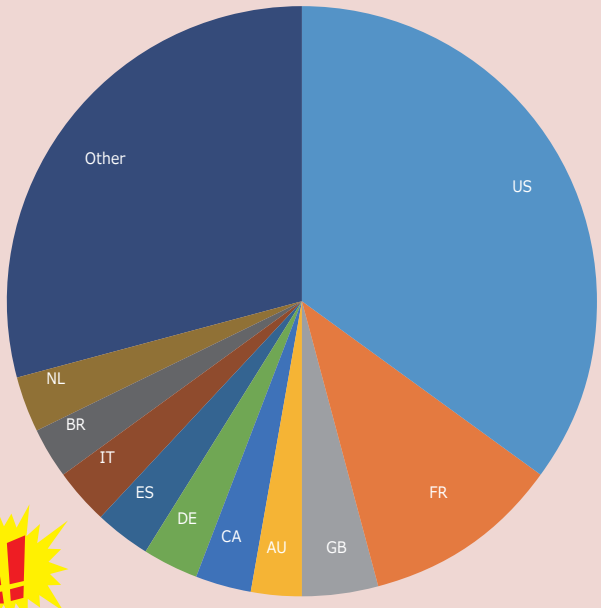

表2：リーク件数に関する国別の割合

定期観測レポート
2022年9月～

セキュリティログ観測①

セコムサイバーコントロールセンターのWAFで検知している攻撃の分析結果についてご説明します。

ある3か月間について、1時間ごとの検知数を表したものが図3です。月によって検知数の変動があり、集中して攻撃が増える箇所が複数みられます。

図3の①（9月25日）は、特定のお客様のシステムを狙う攻撃を検知したものです。攻撃方法は、Webサイト上の様々なページに対してSQLインジェクションの脆弱性を狙う攻撃や、2021年に話題となった「Apache log4jの脆弱性(CVE-2021-44228)」を狙う攻撃が多く見られました。

図3の②（9月30日）は、攻撃に「Nikto」という脆弱性診断ツールが利用されており、SQLインジェクション脆弱性を狙ったものでした。

表2は検知数が上位のものを月単位でまとめたものです。Microsoft社の提供するサーバーソフトのIISや、Oracle社の提供するアプリケーションの管理画面へのアクセスを狙う攻撃が多く観測されています。「アカウント情報窃取の試み」は、誤って公開されているアカウントなどのデータを探索する攻撃です。攻撃者は、システムの脆弱性だけではなく、管理画面やアカウントの管理不備を狙っていることがわかります。

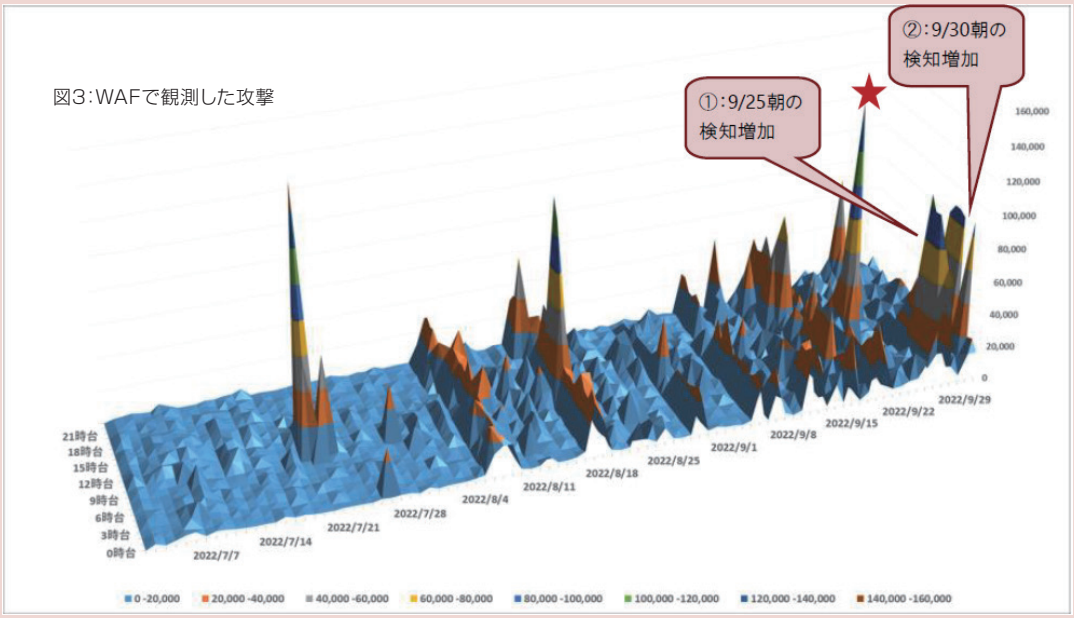

図3：WAFで観測した攻撃

	2022年7月	2022年8月	2022年9月
1位	IIS管理者ページへのアクセス	IIS管理者ページへのアクセス	IIS管理者ページへのアクセス
2位	Oracle管理画面へのアクセス	ORACLEリソース監視サービスへのアクセス	アカウント情報窃取の試み
3位	アカウント情報窃取の試み	アカウント情報窃取の試み	Oracle管理画面へのアクセス

表2：月ごとの攻撃検知数トップ3

定期観測レポート
2022年9月～

セキュリティログ観測②

続いて、通信の分析結果についてご説明します。
図4はインターネット側から内部への通信を宛先ポート別にグラフ化したものです。
グラフの中で、灰色のSSH（ポート番号22）とオレンジ色のTelnet（ポート番号23）が大きく表れています。これらのポート番号は、ルーターやIoT製品で使われることが多く、これを狙った通信であると推察されます。図4の赤枠部分は、Telnet（ポート番号23）を狙う通信が徐々に増加していることを示しています。他には、ポート番号3702/UDPの通信量が増加傾向でした。これは、ネットワーク上のデバイス検索をおこなう「WS-Discovery」というプロトコルで利用されるポートで、デジタルカメラやプリンターなど様々な機器で使用します。LAN内にあることを想定したものですが、設定誤り等によりインターネットに公開されていると、DoS攻撃等に悪用される恐れがあります。

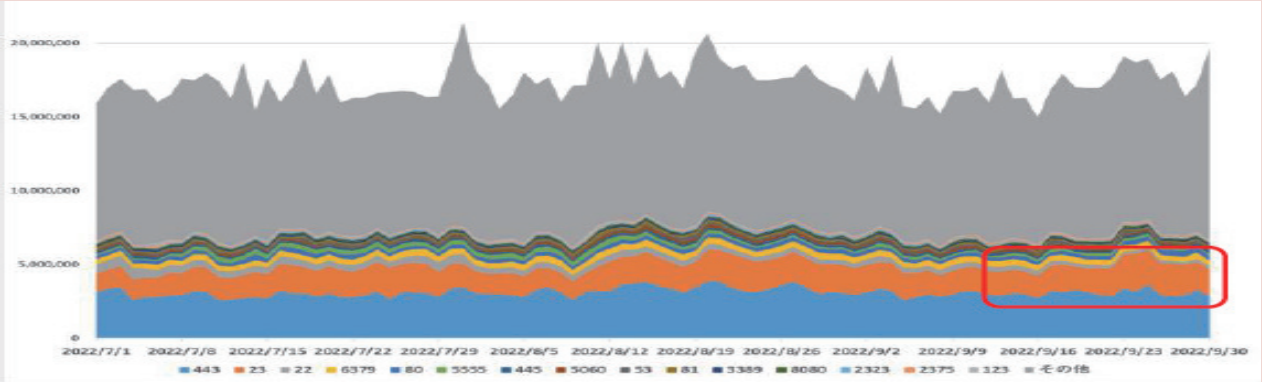

図4：外部からFWへの日ごとの通信量（プロトコル別）

<Tor Exit Nodesからの攻撃について>

ダークウェブに利用されるサーバー群(Tor Nodes)からの攻撃について観測状況をご紹介します。
図5は、Tor Nodesからの攻撃検知数を日ごとにまとめたものです。件数は多くないものの、定期的に攻撃を検知しています。攻撃の内容は、SQLインジェクション等の一般的な攻撃以外にも、FortiOSの脆弱性を狙ってVPNの認証情報を取得しようとする攻撃や、WordPressの設定ファイル、バックアップファイルを取得しようとする攻撃を確認しています。

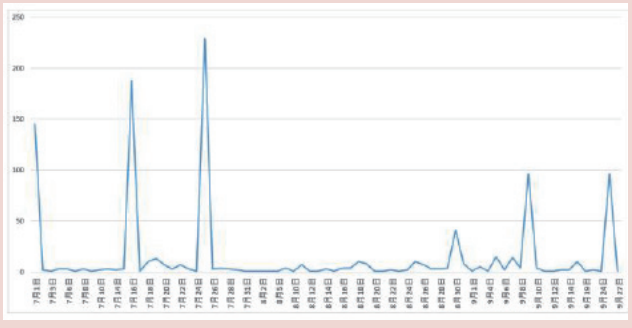

図5：Tor Exit Nodesからの攻撃の検知状況

SECURITY NEWS LETTER
編集後記

本号のセキュリティニュースレターでは、万が一セキュリティ被害が発生した場合の備えについて、情報をお届けしました。
被害を想定し、事前に備えをしておくことが被害軽減につながりますので、社内の体制がどうなっているのか、あらためてチェックをお奨めします。

セコムトラストシステムズ株式会社
www.secomtrust.net

お問い合わせ

ソリューション営業本部
03-5931-5210

受付時間：9～12時・13時～18時
土・日・祝日・年末年始（12/30～1/3）は除きます。