Supported by 日本財団 THE NIPPON FOUNDATION

企業経営基盤強化等セミナー
プ ロ グ ラ ム

◎ 日　　時　　令和５年４月26日（水）13：30 ～ 15:00

◎ 会　　場　　オリエンタルホテル福岡　博多ステーション　２階
福岡市博多区博多駅中央街４－23　TEL 092－461－2091

◎ 主　　催　　（公財）九州運輸振興センター

◎ 後　　援　　九州運輸局　　ＪＲ九州

◎ スケジュール

13:30　　開　　会

13:35　　講　　演

テーマ　　サイバーセキュリティの実情と今やるべきこと

講　師　　(株)ＢＣＣ ﾃﾞｼﾞﾀﾙﾌﾟﾗｯﾄﾌｫｰﾑｻｰﾋﾞｽ事業本部
ﾃﾞｼﾞﾀﾙｻｰﾋﾞｽ営業部　部長　奥　新 一 郎　氏

14:35　　意見交換

15:00　　閉　　会

会　場　風　景

奥新一郎講師

会場風景

サイバーセキュリティの実情と今やるべきこと

(株)ＢＣＣ デジタルプラットフォームサービス事業本部
デジタルサービス営業部　部長
奥　新一郎

日　時　令和５年４月26日（水）
場　所　オリエンタルホテル福岡 博多ステーション
主　催　公益財団法人 九州運輸振興センター
後　援　九州運輸局　ＪＲ九州
助　成　日本財団

ＢＣＣの奥と申します。本日はよろしくお願い致します。

いろいろなところでセキュリティの講師をしていますが、誰もが、セキュリティには興味がある、何かやらなければいけないと思われています。ただ具体的にどうしたらいいのかを悩んでいて、その中でセキュリティに関する事故等が多発しています。これは対岸の火事ではなく明日は我身で、現に私の周辺でも事故が起きています。

本日は様々な情報をお話しますが、対岸の火事ではなく自分ごとということでお聞き頂ければと思います。

まず弊社ＢＣＣを紹介致します。

本社は福岡市中央区六本松にございます。昭和41年、１９６６年に設立、今年の10月で丸57年になります。従業員数は約３８０名でＲＫＢ毎日ホールディングスのグループ企業です。

いわゆるＩＴ企業で民間、官公庁、医療関係等のお客様のシステムの導入・構築・運用保守など様々なサービスを提供しています。

また、データセンターを保有しており、そこから全国のお客様にセキュリティサービスを提供しています。

このデータセンターにはセキュリティ専門部隊が常駐しており、24時間体制でサービスを提供しています。元々データセンターではお客様のシステムを預かり、24時間安定稼働させるということを行っています。そのサービスの一環でセキュリティサービスにおいても、24時間体制でオペレーターが監視しています。

大型モニターでセキュリティ情報を集約し、預かっているサーバーで何か異常が起きてないか、システムが止まってないかなどが一目でわかるようになっています。何か異常があると、パトライトが鳴ってオペレーターが駆けつけて確認します。

弊社ではお客様に安定したサービスを提供するために、セキュリティ専門の技術者は当然ながら、24時間体制でシステムの安定稼働を確認するオペレーター、何か起きた時にすぐ顧客に対応できる営業職、これらが同じフロアで仕事をしており、スピーディーな対応を実現しています。

それでは本題に入りたいと思います。

1．サイバーセキュリティに関する世の中の状況

新聞、テレビで何度も報道されておりますが、四国の病院で、ある日突然システムのデータが暗号化され電子カルテが使えなくなりました。（**資料１**）予定していた手術ができなくなるなど非常に大きな影響が出ました。大阪でもやはり同じような事件があり、ランサムウェア感染が相次いでいます。他にも自動車メーカーが全国の工場を丸一日止めなければならなくなったといったようなこともありました。これは自動車メーカー自身ではなく、その取引先でウイルス感染が起き、その影響を受けての対応ということです。

また、ウクライナ侵攻が始まる少し前からサイバー攻撃が増えてきて、現在まで続いているという状況です。

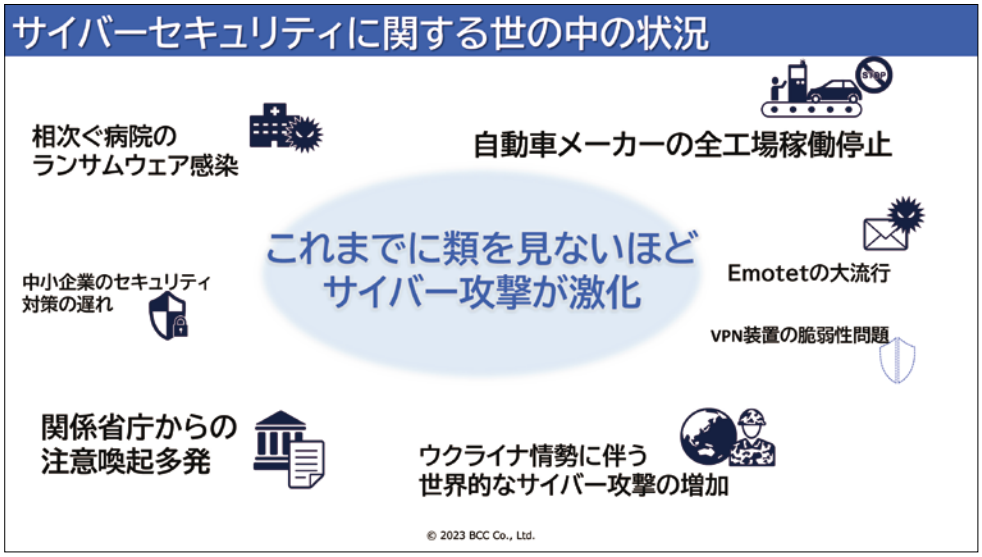
皆様も聞いたことがあるかと思いますが、Ｅｍｏｔｅｔ（エモテット）というのはメールを使った攻撃で、非常に蔓延、大流行しました。

このようにいろいろな方法でサイバー攻撃が行われていますが、運輸・海運業界に関する情報を紹介します。

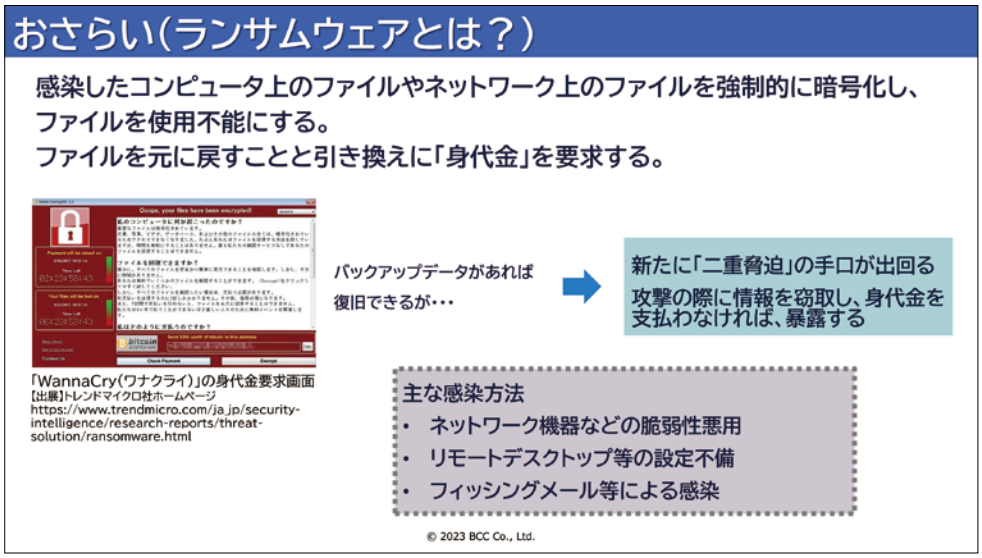
これは国内ではなくグローバルの話になりますが、ランサムウェア感染の影響を受けた業界として、第2位が運輸・海運業界となっています。

サイバー攻撃において標的を定めてそこに執拗に継続した攻撃を行う標的型攻撃があります。

現在標的型攻撃の標的において運輸・海運業界がトップになりました（「Trellix 2022年第3四半期 脅威レポート」より）。世界的に経済活動が復興しつつある中で、運輸業界の重要性が当然ながら増しています。攻撃者はそこに対して攻撃を仕掛け、そこからお金を取るということを考えるわけです。



資料１



資料２

国内においても大手貨物輸送会社がランサムウェアの攻撃を受けてシステム障害が発生し、業務停止に陥りました。パソコンやサーバー上のデータが強制的に暗号化されてシステムが止まるという被害を受けています。大手食品製造会社でもサイバー攻撃を受け、データが流出し、盗まれた情報がダークウェブ上に公開されました。ダークウェブというのは犯罪者がデータの共有や売買などを行うサイトで、普段皆さんが使う通常のブラウザではアクセスできないようなサイトです。

先ほどから出ています「ランサムウェア」という言葉ですが、少し詳しく説明します。（**資料２**）

ランサムウェアはウイルスの一種で、これに感染した場合、パソコン上のデータが暗号化されてしまいます。そのため、ファイルを開くことができません。そこでとどまればまだ良いのですが、社内でデータのやり取り、社員の方とのデータの共有ということでファイルサーバー等を利用されていると思いますが、その共有フォルダのデータまでが、暗号化されてしまいます。たった一人の社員がランサムウェアに感染した

メールを誤って開くと、パソコンのデータが暗号化され、ネットワークでつながる全員のデータまで暗号化されてしまう。そういう恐ろしいことが起きます。暗号化するだけで終わるとただの業務妨害ということになりますが、攻撃者の目的は金銭窃取です。暗号化したデータを元に戻したければ金銭を支払えということになります。要するにデータの身代金です。ランサムウェアという言葉は造語で「ランサム（身代金）」と「ソフトウェア」をつなげたものです。

数年前に流行ったＷａｎｎａＣｒｙ（ワナクライ）というランサムウェアでは、感染後データが一斉に暗号化されて使えない状態になり「あと○日と○時間○分以内に身代金を払いなさい」「払ったらデータを元に戻します」という画面がでてきました。この例ではビットコインで支払いなさいとなっていました。支払期限が近付くほど身代金の値段が上がるという表示です。早いうちに支払わないと値段が上がるということです。ただし支払ったら１００％元に戻るかというとそれは犯罪者がやることですから保証はありません。ただ高額な身代金を支払ってしまったという事例は多くあるようです。

基本的に身代金は支払うべきではありませんが、事業への影響度合いを考えて、支払うという判断をしたようです。

弊社の取引先からも多くの相談を受けました。実際に暗号化され、助けてほしいという相談もありましたが、暗号化されたものを復元するには鍵が必要となります。これは攻撃者しか持っていないものなので、復元することは非常に難しいです。

そこでこのような被害にあわないようにするにはどうするのかということです。

まずはウイルスが入ってくるのを防ぐことです。メールで侵入してくる、あるいは誤って危険なＷｅｂサイトを開いた時等々、いろいろな場面で感染することを防ぐため、出入口対策をすることです。当然そのようなセキュリティ製品は多数ありますが、１００％防げるかというと、それは難しいです。日々新しいサイバー攻撃の手法が生まれておりセキュリティ製品の対応が追いつかないこともあります。完璧を望むのではなく、侵入されることを前提に対策を練ることも重要です。

暗号化されて困るならバックアップを取っておけばいいという理屈になります。しかし攻撃者も当然バックアップがあると分かっているので、確実に身代金を取るために二重脅迫を行います。暗号化する前にデータを盗んでおき、身代金を払えば暗号化されたものを元に戻す、払わなければ盗んだデータをばらまくという二重脅迫をしてきます。

現在のランサムウェア被害では、こういう二重脅迫型が非常に多くなっています。

感染ルートですが、ネットワーク機器の脆弱性を悪用する手法が多くなっています。四国の病院でのサイバー攻撃の例を紹介しましたが、まさにこれなのです。

コロナ禍が始まってからリモートワークのための設備を整える企業が急増しました。社外からリモートで接続するために入り口を作らなければいけない、そういう機器をＶＰＮ装置と言います。その装置に接続してＩＤ・パスワードを入力し、社内ネットワークに接続できるようになります。その装置に脆弱性、つまりセキュリティホールがあると、先ほどの例のように攻撃を受けるという事になります。攻撃者はデータを盗み、ランサムウェアを送り込んでデータを暗号化します。

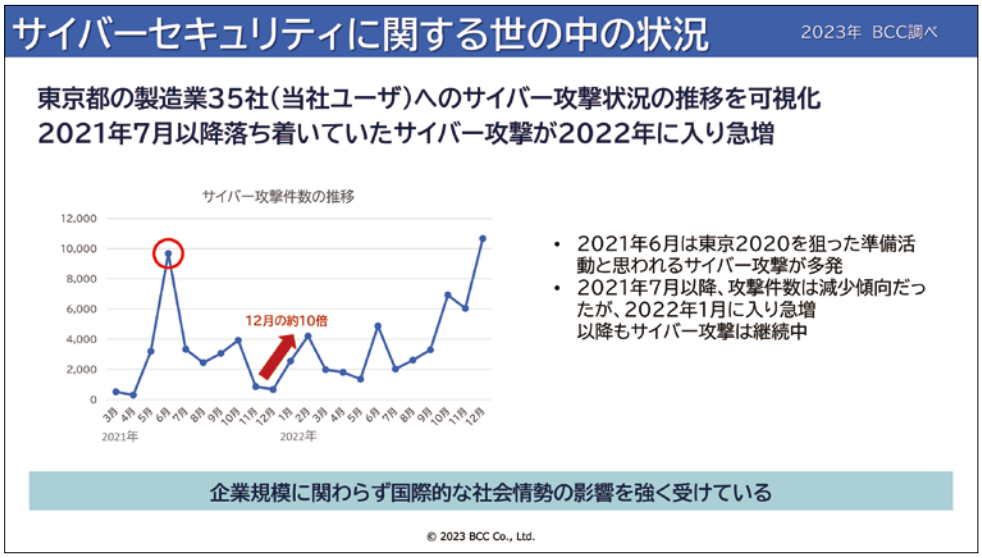
他にはリモートデスクトップの設定不備やフィッシングメールによる感染等があります。

弊社顧客の製造業35社の情報ですが、２０２１年から直近２０２２年12月までのサイバー攻撃件数を紹介します。何れの企業も保有するパソコンの台数は10～20台程です。

攻撃の件数ですが、２０２１年６月に跳ね上がっています。（**資料３**）これは東京オリンピックが1年遅れで開催される直前で、オリンピックを狙った準備活動によるものだと推測されます。その後12月からまた少し増加傾向となっていますが、２０２２年２月にまた急増していて、これはウクライナへの侵攻が始まった時期と重なります。このように、国際的な社会情勢の影響を小規模な事業者でも受けているということです。

先ほど標的型攻撃について述べましたが、ある特定の大企業を執拗に狙う攻撃もありますが、攻撃者に

とってコストパフォーマンスが悪いため、それよりもセキュリティ対策の甘い小規模な企業を数多く狙うこともあります。バラマキ型で攻撃メールを大量に送ることも機械的に行えるので簡単なことなのです。数万件送ってその中で1件でも引っかかればそこから先ほどのランサムウェアで身代金要求ができてしまいます。



資料３

このように業種や規模を問わず、多くの企業が攻撃にさらされているうえに、攻撃の頻度が増しています。当然ながら国としてもこれは大きな課題として認識されています。

次に経済産業省を主体とした活動についてです。

経済産業省では中小企業を狙ったサイバー攻撃の増加を踏まえて対策を講じています。

中小企業が狙われるとどうなるでしょうか。多くの企業は何かしらのサプライチェーンに属しています。多くの取引先がつながっていて、それらがさらに多数に枝分かれし膨大なサプライチェーンができ上がっていると思います。もし、その中の1社に何かあればその取引先全てに影響が出てしまうこともあります。これをサプライチェーンリスクと言いますが、そのリスクが非常に増大しています。

その中小企業のセキュリティ対策が進まない理由の1つは、もしかするとニーズにあったサービスが無いのではないかと考えましたが、世の中には多種多様なサービスがあり、弊社も含めて多くのセキュリティベンダがサービスを展開しています。必要な機能がないということだけではなく、費用が高すぎる、あるいは導入しようと思っても手が掛かる、運用負荷が高くなる等々、各社様々な事情があるようです。

そこで中小企業向けのサービスに必要な機能や体制、価格等について検討を行うため、経済産業省は２０１９年度と２０２０年度の2年間にわたり、全国の中小企業の実態調査を行う実証事業を実施しました。

この実証事業は「サイバーセキュリティお助け隊事業」と呼ばれます。２０２０年度に弊社も参加し、九州エリアの調査を担当しました。中小企業54社にご協力いただきながら、実態調査などの実証事業を行いました。

ご協力いただいた企業はパソコンの台数にすると一社あたり平均20台程です。業種は様々で物流業、小売業、製造業、教育関連や医療機関などがあります。

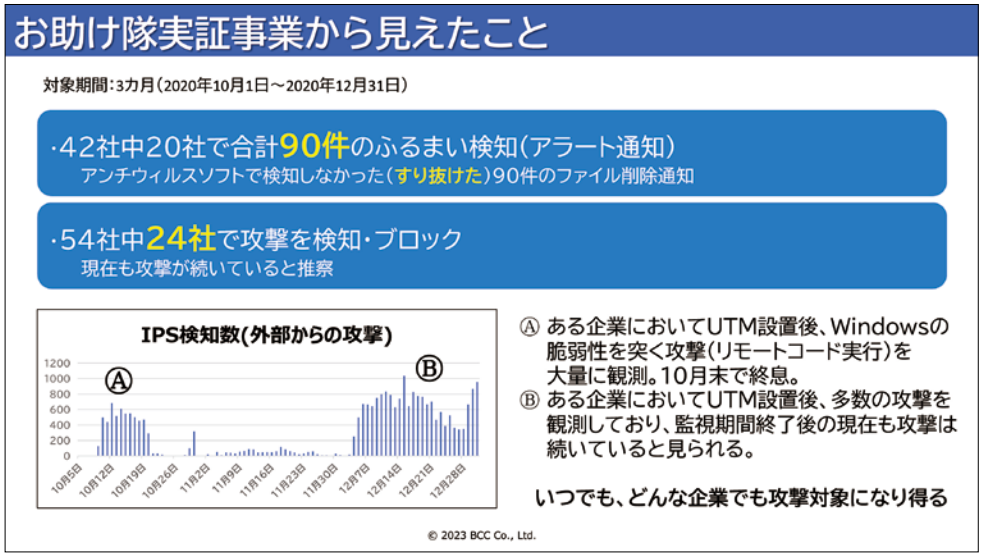
２０２０年10月から12月という3ヶ月間の短い期間でしたが、まず実態調査として、どのようなセキュリティ対策を講じているかヒアリングするとともに、どのような攻撃を受けているか調査し、さらにセキュリティ対策にどのくらいの費用をかけているか確認しました。

また、次世代型マルウェア対策サービス（弊社が新たに構築したセキュリティサービス）を無償で利用していただき、効果の有無も調査し、セキュリティサービスの普及が進まない理由の1つと考えられる「運用負荷」や「導入難易度」についても確認しました。

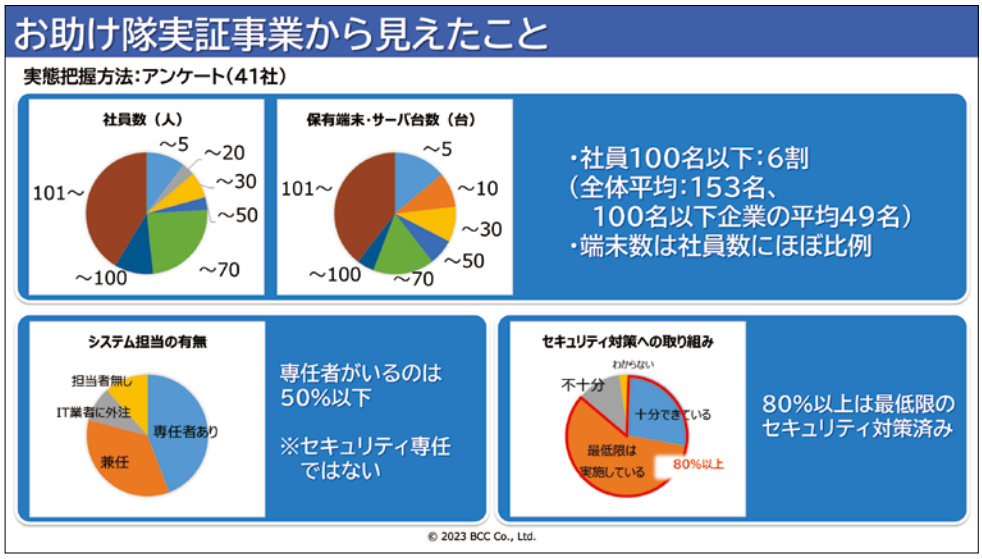
この実証事業から見えた結果についてです。

九州エリアの中小企業の皆様の実態ですので、今日ご参加いただいている皆様の参考になるのではと思います。

まず3ヶ月間で90件のふるまい検知がありました。（**資料４**）ふるまい検知についてですが、ほとんどの企業はウイルス対策ソフトを導入し



資料４



資料５

ていますが、そこに弊社の次世代型マルウェア対策のソフトを追加導入しました。元々のウイルス対策ソフトで検知できなかった、つまりすり抜けたものをふるまい検知（アラート通知）したということです。42社のうち20社、約半数で検知がありました。

さらに54社中24社でネットワーク経由での攻撃を検知・ブロックしました。これはネットワークを監視して、社外から社内、社内から社外双方向の攻撃の通信を検知するものです。社内から社外の検知はパソコンから危険なサイトにアクセスしようとするようなものになります。先ほど話に出ました、フィッシングメール等により危険サイトに誘導されるものです。そのようなものを監視した結果、半数近くの企業で検知・ブロックしました。

ある企業において10月中旬から突然検知件数が急増し、10月末には終息。弊社が何か手を打ったというわけではないのですが、監視期間でこのようなことが起きました。しかし12月からまた急増、12月末で実証事業は終わっていますのでデータとしてはここまでですが、おそらくその後も攻撃が続いていたものと思われます。

この攻撃の内容を見ると、Ｗｉｎｄｏｗｓの脆弱性を悪用するような攻撃でした。仮に攻撃が成功した場合には攻撃対象のパソコンが乗っ取られ、攻撃者が遠隔で自由に操作できるようになります。企業規模や業種は関係ない上に、時を選ばず攻撃対象になり得るということをあらためて実感しました。

次にアンケートを行った結果についてです。（**資料５**）

41社から回答いただき、半数以上は従業員１００名以下の企業となっています。各企業が保有しているパソコンやサーバーの台数はほとんど社員数に比例しています。

システム担当者がいるかという問いについては、専任者がいるという企業は50％以下、兼任者を含めると

80％くらいでしょうか。しかしセキュリティの専任者いる企業はほぼありませんでした。

セキュリティ対策への取組みはできているかという問いでは、十分できている、最低限の対策はできているという企業を合わせて80％以上となっています。

その80％以上の企業についてどのような対策をしているのかという問いではアンチウイルスソフトの導入が一番多く、93％となっています。

セキュリティの対策にかける年間の費用では、半数近くの企業が年間50万円以下となっています。従業員数と比較すると、従業員1人当たり1万円程度です。

取引先からのセキュリティ対策の指示があるのか、についてです。取引先からセキュリティ対策をしていますかというヒアリングシート、チェックリストが来ることが最近多くなっているのではないでしょうか。これをきちんと行っていないと取引ができない、あるいは取引要件に入っている、要件までにはなっていないが依頼されているという企業は合わせて半数近くとなりました。

サイバー攻撃の被害を受けたことがあるかという問いでは、37％がメール経由でのウイルス感染の経験があるということです。

先ほど80％以上の企業でセキュリティ対策は行っているという回答でしたが、それをすり抜けて、1／3以上の企業で実際に被害が発生していることになります。

では攻撃を受けた時にどうしたかというと、26％がクリアインストールを行っています。これは感染したパソコンをそのまま使うのは危ないので、全データを消去し、ＷｉｎｄｏｗｓＯＳを再度インストールし直すということです。当然、データは全てクリアになります。そして専門家依頼が30％となっています。それら合わせて半数を占めています。

何れにしても業務に対するインパクトが大きな対応です。対象がサーバーの場合にはシステムが止まるわけで、復旧するまでどのくらい時間を要するのか、復旧にかかる費用もどれほどになるのか、パソコンに比べるとより大きな影響になると考えられます。一言でクリアインストールといっても、様々なソフトを再度インストールし、データをリストアするといった、いろいろな作業が発生し、それぞれに対価が発生します。

繰り返しますが、80％以上の企業で最低限のアンチウイルスは導入済みとなっている中、1／3以上の企業で被害が起きています。このようなことからも、従来のセキュリティ対策だけでは不十分だということが言えます。

また、実証事業の結果から組織の規模や業種を問わず、例外なく攻撃にさらされているということが明らかになりました。（**資料6・7**）

さらに、コスト面も大きなポイントとなります。セキュリティ対策サービスの費用や運用の負荷が大きくなると中小企業では導入が難しくなります。

全国15カ所同時にこの実証事業は行われ、他のエリアの報告内容を見ても同じような結果が出ています。

この結果報告を経済産業省で取りまとめ、サイバーセキュリティお助け隊サービス基準が制定されることになりました。

「サイバーセキュリティお助け隊」制度というのは、中小企業向けのセキュリティサービスはこうあるべきだという要件を定めたものになります。そしてその要件を満たしているかどうか審査を行い、合格したものがサイバーセキュリティお助け隊サービスリストに登録されます。

要件の一部に、「見守り」、「駆付け」、「保険」があります。

「見守り」はセキュリティ製品の提供で終わらず、それが正常動作しているか、危険なものを検知してないか等を常時監視するものです。

「駆付け」は緊急事態が発生した場合にはいち早く技術者を現地に駆けつけさせ、一次対処の支援を

させます。

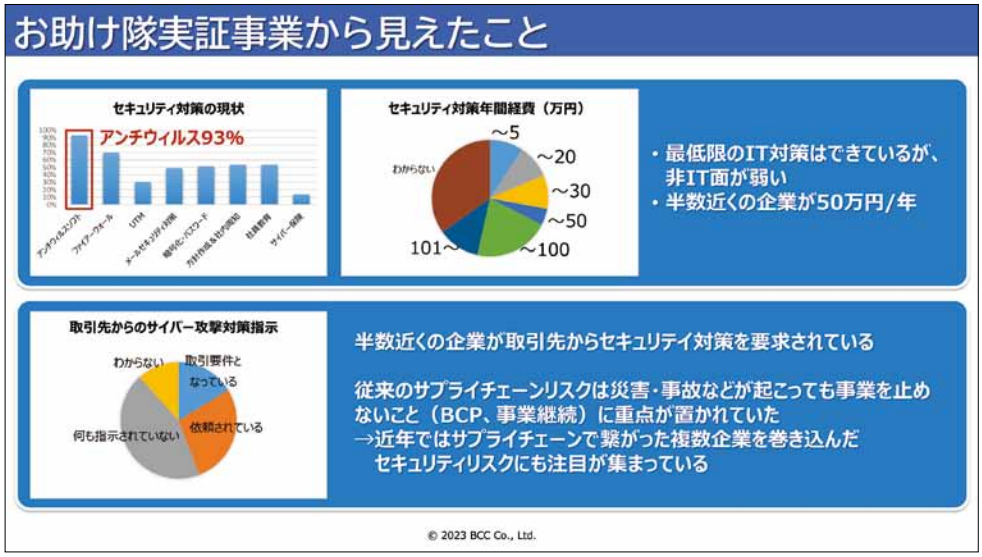
「保険」は「駆付け」等により発生した突発的な費用を補償します。

このように「見守り」「駆付け」「保険」で中小企業のセキュリティ対策に不可欠なサービスをワンパッケージで提供しているかということが要件の一部となります。

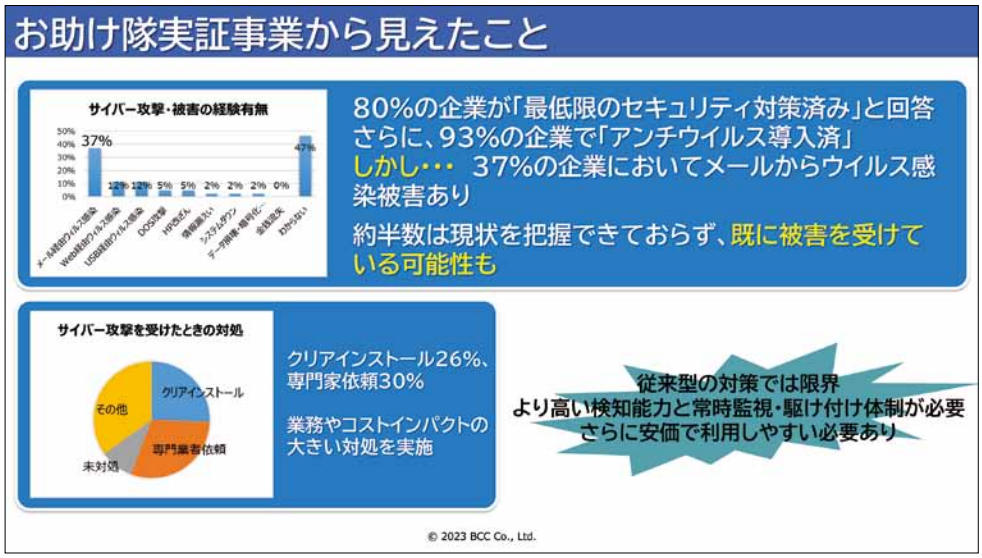
さらに困った時の相談窓口を提供することも要件に含まれています。

お助け隊サービスはまだ耳なじみがないかと思いますが、経済産業省などがPRに努めています。政府も自動車メーカーの事件を受けて、サイバーセキュリティお助け隊サービスの普及に努めるという主旨の発言を行っています。

サイバーセキュリティお助け隊の審査合格したサービスが2022年3月28日時点で33社となっています。



資料６



資料７

弊社のサービスも審査合格しており、全国のお客様にご利用いただいています。

2. 情報セキュリティ対策の必要性

マイナンバーを含む従業員情報、取引先の情報、お客様情報等、様々な機密情報が外部に漏洩したらどうなるでしょうか。（資料８）

当然ながら損害賠償等の金銭的な対応が出てきますが、それだけではなく社会的な信頼を失墜してしまいます。ランサムウェアに感染した場合にはシステム停止に伴い業務停止などいろいろな事象が起こります。

では、セキュリティ対策をどこから始めたら良いでしょうか。

3. どこから始めたら良いか？

忘れられがちですがセキュリティ対策をするというのは、セキュリティ製品をただ導入するのではなく、それと並行してルールを決め、ガイドラインを示して社員に教育をすることも必要です。年に1回、基本的なことからでも良いので認識を新たにさせる。（資料９）

例えばお客様先での打ち合わせに資料の入っているパソコンを持って行き、帰りに飲食店に立ち寄って飲酒し、紛失した。このようなことがないよう、お酒を飲みに行く時はパソコンを持って行かないなど基本的なことですが、きちんとルールを定め社員教育を行うべきです。

この教育は重要で、内部不正という面でも抑制につながります。社員のモラル低下を防ぐためにも教育という対応を忘れてはいけません。

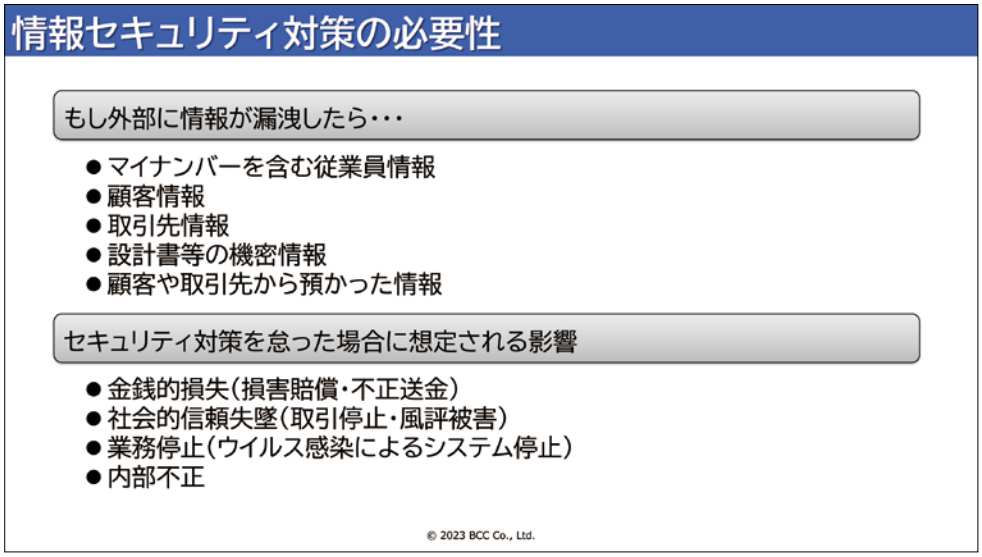
万が一そういう事故が起きた場合、様々な法律で罰則が規定されています。不正を行った当人だけではなく、会社や経営者に対しての罰則規定等もあるので注意が必要です。

前置きが長くなりましたが、では、どこから始めたら良いか。

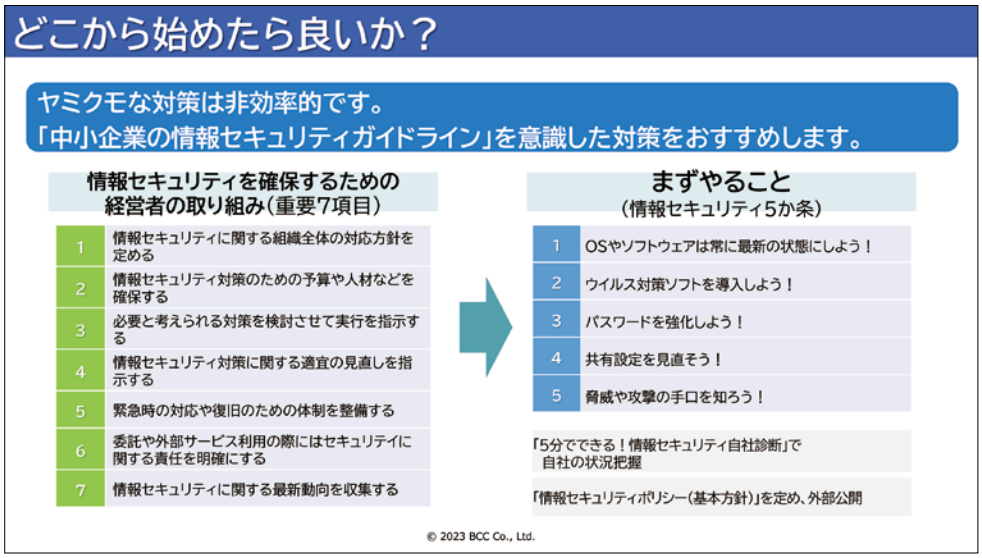
いろいろなセキュリティサービスがありますが、それを導入する前にまずやるべきこと、「情報セキュリティ5か条（IPA SECURITY ACTIONより）」があります。

1つ目、OSやソフトウェアは常に最新の状態にする。2つ目、ウイルス対策ソフトを導入する。3つ目、パスワードを強化する。推測されやすいパスワードにしていると不正ログインされるリスクがありますので、できるだけ複雑なパスワードを設定しましょう。4つ目、共有設定を見直す。クラウドサービスのデータ共有サービス等で意図せず第三者が見える状態になっていると情報漏洩につながりかねません。設定に誤りが無いか確認しましょう。5つ目、脅威や攻撃の手口を知る。今、まさに脅威や攻撃の手口を紹介しましたが、このようなセミナーに参加することや、普段ご利用の金融機関のホームページ等にも、注意喚起情報が掲載されていることもあります。普段から新しい情報を集めるよう心がけましょう。

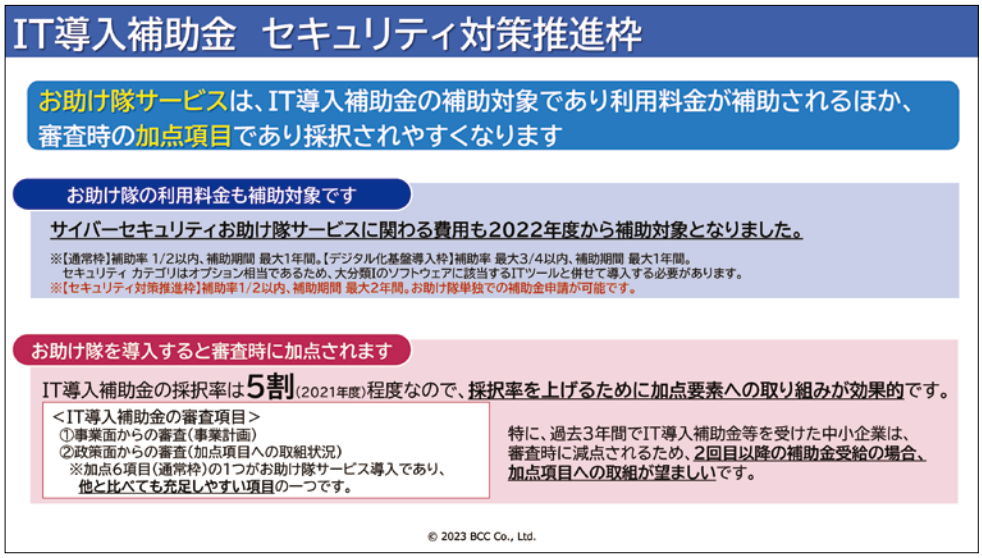
この5か条を行った上でセキュリティ対策をする、ここを疎かにすると良いセキュリティ製品を導入しても、効果半減ということになってし



資料８



資料９



資料 10

う対策をしたらいいかを相談してみてください。

先ほども申し上げましたが、弊社もサイバーセキュリティお助け隊サービスに登録され、安心してご利用いただけるサービスを提供しています。

お助け隊サービスのご導入に際しては、ＩＴ導入補助金をご利用いただけます。

以前から行われている補助金事業で、今年度もＩＴ導入補助金２０２３が展開されています。元々は業務効率化や売上アップをサポートすることを目的とした補助金制度ですが、セキュリティ対策も対象となっています。

システムやサービスを新たに導入する際、同時にセキュリティサービスを導入すると、メインとなるサービスだけではなく、セキュリティサービスの導入費用まで補助対象になります。ただし、そのセキュリティサービスはサイバーセキュリティお助け隊に登録されているサービスだけが対象となります。

また、セキュリティサービス単体での補助金申請も可能です。（**資料10**）

これは２０２２年度から始まりましたが、今年度も同じような内容でスタートしています。各種セキュリティサービスがある中から選択するのは難しいとは思いますが、経済産業省の施策から生まれた「サイバーセキュリティお助け隊サービス」というものがあるということをご認識して頂ければと思います。２年間の実証事業の結果をもとに中小企業に必要な機能やご利用いただきやすい価格を定め、厳密な審査が行われています。

その審査を合格し、サービスリストに登録されたサービスは弊社を含め全国33社ありますのでその中から皆様の組織に合ったものを選ぶことでご安心いただけるのではないでしょうか。

ご清聴ありがとうございました。