別紙 1

サイバーセキュリティ懇談会
開催回別事例集
（16 事例／匿名）

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

目次

サイバーセキュリティ懇談会　事例概要
千葉県　佐倉商工会議所

【佐倉】 E 社（社会保険労務士事務所）代表　Y.H 氏

～個人事務所を経営しながら、社労士会のセキュリティ活動にも貢献～

1.　個人事務所のセキュリティ、商工会議所お助け隊が徹底サポート

スタッフ 1 名の個人社労保険労務士事務所を経営する Y.H 氏。自身でウイルス対策ソフトを導入し、佐倉商工会議所　三谷氏の助力のもと、VPN　やサイバーセキュリティお助け隊サービスによる UTM を導入する等のセキュリティ対策を実施した。また、スタッフにはテレワークを許可しているため、雇用契約時に、公共　Wi-Fi　の使用禁止、会社のパソコンの貸与、ダウンロード禁止といった対策を説明している。小規模な事務所なので、完璧な対策は難しいが、今後はメールの使用をできるだけ控えてチャットに移行する等、工夫しながらセキュリティ対策を推進していきたいとのこと。また、約一年前、UTM　を導入する前に迷惑メールを開いてしまった経験があり、現在も感染状態が継続しているのでは？と不安を抱えていたが、導入した UTM は、たとえ過去に社内ネットワークに侵入したウイルスが社外に不正送信したとしても、UTM が検知し送信を防御するので安心した。

2.　千葉県下社労士会会員のデジタル力向上に奮闘中

Y 氏は、千葉県社会保険労務士会のデジタル化推進委員に任命されており、社労士会全体のデジタル化の推進と、千葉県内の社労士のデジタルセキュリティに関する知識とスキルの向上に向けた取り組みを進めている。ここ 2～3 年は、IPA から講師を招致してセキュリティ研修を実施してきたが、参加者の年齢層は幅広く、また、デジタル経験レベルも、初心者から上級者まで様々である。一律の研修では、参加者のニーズやスキルに応じた研修の実施が困難であることに悩んでいる。ファシリテーターの米澤氏からは、業務上使用するツールやシステムを特定した後、システムごとに段階的な学習コンテンツを作成するのが良いとの助言があった。

【佐倉】B 社（空調設備製造・施工業）代表取締役　K.T 氏

～不安の増すシステム投資判断：公平な立場の相談相手が欲しい～

1.　出入り業者の言いなり？疑問を抱いたままのシステム投資判断

空調設備の製造、販売や工事を手掛ける B 社代表の K.T 社長。悩みは大手 OA 商社の提案について、相談する相手がいないこと。長年の付き合いもあり、ネットワークや VPN などの社内システム環境の構築と保守を、特定の大手　OA　商社の地域支店に一任してきた。出入りベンダーは当該商社一社のみということもあり、提案をほぼそのまま受け入れ、IT　投資を続けてきたが、投資額が膨らむ

につれ、不安が増している。K 社長は、自身がシステムの現状やリスクを正確に把握できていないため、公平な立場で評価してもらえる相談相手が欲しいと考えており、その方法を模索している。また、K 社長の理想は、複数のベンダーが競合することで、より適切な価格でシステムを導入することであるが、佐倉商工会議所 三谷氏によると、当該地域では対応するベンダーが限られており、B 社が所在する佐倉工業団地は当該 OA 商社の出入りが多いとのことであった。

2. 頼れる専門家はどこに？

ファシリテーターの米澤氏から、外部の専門家や商工会議所などの第三者に、社内のシステムを見てもらうことや、ベンダーとの打ち合わせの際、同席をお願いすることで、新たな解決策が見つかる場合があると助言があった。また、佐倉商工会議所 三谷氏からは、どんな些細なことでも構わないので、まずは商工会議所に相談してほしいとの呼びかけがあった。相談を受けた後、外部の専門家を紹介することも可能とのことである。

その他ヒアリング事項

■ サイバーセキュリティ全般について

・ 過去の顧客ヒアリングに基づくと、企業の年間の IT にかかる総費用（通信費、情報端末費や DX 推進費用含む）のおおよそ１0%以下が適切なセキュリティ対策費用ではないかと思う。（ゲストスピーカー・白岡氏）

・「令和５年上半期におけるサイバー空間をめぐる脅威の情勢等について」（警察庁発表）によると、1 日 8,000 件程度、ロシア・中国・北朝鮮から日本のルーターに対する、脆弱性確認のためのパケット通信が確認されている。日本企業の総数が 367 万社とすると、一年半に一回はどの会社も攻撃をされている計算になる。（ゲストスピーカー・白岡氏）

・ ランサムウェアの侵入から実際の被害までのタイムラグ、システムに何らかの兆候が見られるケースが多い。ファイルの紛失や操作時の違和感（遅延）等に気づいた場合は、専門家に相談すること。（ゲストスピーカー・白岡氏）

■ 社員教育について

・ 小規模、かつ、社員の IT 習熟度が様々な会社において、セキュリティ教育を実施するためには、まず”やるべからず集“を作成し、最低限やってはいけないことについて知ってもらうことから始める。（【佐倉】D 社（造園業）T.T 氏）

・ 標的型攻撃メールの抜き打ち訓練と研修を、定期的に実施している。（【佐倉】A 社（化学品製造業）K.A 氏）

・ セキュリティ対策と DX、２つを並行して社員に教育する必要に迫られている。社外から協力者を得つつ、上手に進めていきたい。（【佐倉】A 社（化学品製造業）K.A 氏）

・ 佐倉商工会議所では職員教育のため、毎月第一営業日の朝礼の後に、IPA 情報セキュリティ普及啓発コンテンツ等、情報セキュリティの意識づけに役立つコンテンツを視聴している。（佐倉

商工会議所・三谷氏）

■　現在の悩み

・　工事現場の事務所からポケット Wi-Fi を使用して社内に繋げているので、ウイルスの侵入が心配である。（【佐倉】C 社（土木建設業）S.H 氏）

・　IT 習熟度が低い社員でも、サイバー被害を起こさないようにするための方法を考察する必要がある。（【佐倉】D 社（造園業）T.T 氏）

■　サイバーインシデント事例（未遂含む）

・　過去官公庁を装ったウイルス付きメールを開封し、感染した。（【佐倉】A 社（化学品製造業）K.A 氏）

・　お客様宛に、過去に社内から送信した文面を使用し、それへの返信であるかのように装った攻撃メールが送信された（【佐倉】A 社（化学品製造業）K.A 氏）

・　社員になりすました（社員のメールアドレスを送信元とした）ウイルス付きメールが、お客様に送信されたことがある。（【佐倉】A 社（化学品製造業）K.A 氏）

・　疑わしいメールを受信した職員が、開封する前に、送信者に確認の電話をした。結果、なりすましであることが判明した。（佐倉商工会議所・三谷氏）

サイバーセキュリティ懇談会　事例概要
大阪府　大阪商工会議所①

【大阪①】B 社（樹脂成型品製造業）専務取締役　H.K 氏

～組織全体のセキュリティ意識を強化し、より安全なものづくりの現場を構築したい～

１．　在宅インターネット環境からのウイルスの侵入を心配

樹脂製試作品の開発・製造をする B 社では、コロナ禍を機に在宅勤務者が増加した。社員に会社のノートパソコンを貸与し、自宅のインターネット回線を使用した VPN 接続をさせているが、現在の VPN は UTM を経由しておらず、社内ネットワークにウイルスが侵入する可能性がある。早急に対策を練りたいと考えている。

２．　社内のセキュリティ体制について、組織全体での改善を希望

社員のセキュリティ教育が不十分なため、組織全体で改善に取り組む必要があると感じている。セキュリティポリシーはあるものの、現在のセキュリティ教育は、新入社員への研修時の教育と会社ホームページの掲載のみであり、既存の社員に対する教育ができていない。サイバーセキュリティお助け隊サービスから配信される月次レポートについても、展開方法を検討中で、全社員に向けた共有が実現できていない。また、日々迷惑メールの受信が増える中、社員がウイルスメールを誤って開封するリスクが常にあることも、不安の 1 つである。ソフトウェア（ウイルスソフトやクラウドサービスに付随する機能等)では防御しきれないウイルスメールについて、管理対策などを第三者に相談したいと思っている。

【大阪①】D 社（ソフトウエア開発業）代表取締役　M.N 氏

～サイバー被害における平均的な被害額を知り、顧客対応に活用する～

１．　自社と顧客、両社でランサムウェア被害を経験

自社開発ソフトウェアおよびパッケージソフトの導入・サポートを担う D 社は、自社と顧客先の両方でサイバーインシデントの被害経験がある。自社の被害は約 10 年前、社員がウイルスに感染していた私物パソコンを、社内ネットワークに接続し、社内システムにウイルスが拡散された。全システムの復旧まで 3 日を要した。特にファイルサーバーにおいて、復旧に必要な調査範囲が明確でなかったため、予想以上に時間がかかったとのこと。インシデント発生の要因として、当時のセキュリティ対策の不十分さをあげている。私物 PC の社内接続を禁止していたものの、社員教育や不許可端末の検知機能が十分ではなかった。

顧客におけるランサムウェア被害経験は 2 件あり、ともに D 社が対応を担当した。1 件はサーバー1 台の被害で済んだが、2 例目は複数台のサーバーが感染し、復旧に 1 週間以上を要した。

2.　顧客対応時におけるランサムウェア被害を防止し、実際の被害額についても把握したい

現在、D 社では、基幹システムを含む多数の顧客先システムをリモートメンテナンスしている。顧客先システムへは SSL で接続するなど、セキュリティには充分留意しているが、インシデントが発生するリスクが常にあることを懸念している。また、現在ネットワークセキュリティの運営を自社で行っているため、社内の負担も多く、サイバーセキュリティお助け隊サービス等、外部サービスを利用することを考えている。また、D 社が顧客先に行ったランサムウェアの被害対応について、対応に要した請求額をいくらにしたら良いか不明で、実際の被害額に関する情報があれば参考にしたいと考えている。

3.　サーバーのパスワード管理について

大企業の場合は企業側のセキュリティポリシーに基づき、納品済みのサーバーのパスワード変更が求められることがあるが、中小企業では一度設定したらそのままになっているケースが多い。また、サーバーのパスワードを強制的に変更してしまうと、お客様がアクセスできなくなる可能性があるため、避けているのが現状とのこと。

その他ヒアリング事項

■　サイバーセキュリティ全般について

・　観光業界における中小のバス会社・旅館・ドライブエリア等は、大手旅行会社に比べてデジタル化が遅れている。特にバス会社においては、情報の授受は主に FAX を通じて行われているが、徐々に電子化（メールなど）が進行している。今後はデジタル化の進行に応じて、取引先全体でのセキュリティ対策が必要になると思われる。（【大阪①】C 社（旅行業）M.M 氏）

・　現在はネットで注文を受けた商品を、FAX を使用してメーカーに発注している。メーカーから FAX の電子化に関する要望は受けておらず、また、電子化子化した場合に必要になるセキュリティ対策がわからないため、こちらから要望することもない。（【大阪①】A 社（EC サイト運営）H.T 氏）

・　大手自動車会社のサプライチェーンにおけるランサムウェア被害事例は、自社だけでなく取引先も含めたセキュリティ対策の重要性を示している。（ファシリテーター・田中氏）

・　外部のサービスを使用し、定期的に標的型攻撃メール訓練を実施することは、大いに有効なセキュリティ対策である。（大阪商工会議所・古川氏）

■　社員教育について

・　情報セキュリティポリシーは社員に公開している。これにはパスワード変更の規定も含まれているが、システムの数が多いため、全てに対応することは現状では難しく、大規模なシステムから対応を進めている状況である。（【大阪①】F 社（デジタルコンテンツ開発業）T.S 氏）

・　月一回の接続レポートや、自身が行ったセキュリティ活動の発表、セキュリティアクションの状況などの情報をグループウェア上で社員に共有している。（ゲストスピーカー・小口氏）

・ サイバー事後対応支援事業の一環として、外部の企業に標的型攻撃メール訓練サービスを提供するのと並行して、自所内でも年 2 回、同様の訓練を実施している。訓練を重ねるにつれて所員の意識が高まり、疑わしいメールを受信した際に、問い合わせるケースが増えてきた。当該訓練の真の目的は、「メールを開かないこと」ではなく、「怪しいメールと思った場合は声をあげる（互いに注意喚起をする）」文化を、組織に根付かせることである。（大阪商工会議所・古川氏）
・ メール訓練の具体的な実施方法は、1 か月前に「送信する」と所内に宣言し、当時流行している標的型メールを模擬したものを送信する。開かなかった場合はもちろん、実際にメールを開いてしまっても、報告をすれば合格とする。ただし、開いても報告をしなかった場合は、注意対象となる。（大阪商工会議所・古川氏）
・ 当該メール訓練は、実際に仕組みを持っていた松本商工会議所と協力して、事業展開したものである。（大阪商工会議所・古川氏）

■ 現在の悩み

・ いわば「いたちごっこ」状態になりつつあるサイバー攻撃対策について、他社の事例を学びたい。（【大阪①】F 社（デジタルコンテンツ開発業）T.S 氏）
・ サーバーのパスワード管理について、頻繁な変更や複雑さが運用を難しくする一方で、他社の対応を知りたい。（【大阪①】E 社（医薬品卸売業）M.H 氏）

■ サイバーインシデント事例（未遂含む）

・ 2020 年 12 月にサイバー被害に遭った。自社ホームページの管理用 ID とパスワードが漏洩し、HP が書き換えられ、ホームページをクリックすると別のサイトにリダイレクトされる事象が発生した。漏洩の原因を調査するための見積もりは約 500 万円であった。そのため、原因追究はせず、書き換えられたコードを元に戻し、UTM とエンドポイントセキュリティを導入するなどの対策を講じて問題を解決した。管理 ID の漏洩ついて、担当者が一人であったことと、管理者が十分に社員教育をしていなかったことが原因であり、現在は担当者に定期的なパスワード変更を通知することによって対策を実行している。（【大阪①】F 社（デジタルコンテンツ開発業）T.S 氏）
・ 2022 年 10 月、グループ内事業部がランサムウェア被害に遭い、取引先の医療機関のシステムにまで被害が及び、復旧まで 3 か月を要した。事故発生後、社に“大丈夫か”など状況を心配した問い合わせを多く受けた。（【大阪①】E 社（医薬品卸売業）M.H 氏）

サイバーセキュリティ懇談会　事例概要
大阪府　大阪商工会議所②

【大阪②】A 社（システム構築・販売業）取締役　I.H 氏
～サイバー攻撃対策は、技術と教育の両輪で～

1.　エモテット等、マルウェア被害を 2 件経験

A 社では、2 件のランサムウェア被害経験がある。1 件目の感染は、取締役の I 氏がなりすましメールを開いたことによるエモテット感染。2 件目は当該被害後、社員がメールに記載されたマルウェアへのリンクをクリックし、ウイルスが社内に拡散された。発生源のメールはウイルスソフトの検知をすり抜けていた。2 件目の被害発生後、セキュリティ対策組織を設け、IPA からの情報を社員に配信するなどの対策を実施した。

2.　被害経験と対策から見えてきた、社員教育の高いハードル

ウイルス対策ソフト等の対策をしていたにもかかわらず、1 件目の感染を経験したことが、セキュリティ対策強化の契機となった。IPA のセキュリティ宣言を 2 つ星に引き上げ、抜き打ちの攻撃メール訓練など具体的な対策を実施した。技術的な側面においても、社員のウェブサイト閲覧履歴の監視などの対策を実施したが、2 件目のサイバー被害が発生した。2 件の被害経験から、技術的な対策をいくら強化しても、人的要因による事故が発生してしまうと実感。今後は、社員一人ひとりの意識をどのように高めるか、他社の例を参考に具体的な施策を検討していきたいとのこと。

【大阪②】C 社（電気器具製造業）常務取締役総務部長 N.Y 氏
～セキュリティ対策を一任され、奮闘する総務部長～

1.　UTM 導入のそのあとは？専門家不在のなか、セキュリティ対策をどう推進

設立 63 年を迎える、従業員数 40 名の老舗電気器具製造業 C 社。社長から社の情報セキュリティ対策を任された総務部長の N 氏は、大阪商工会議所で開催されたセミナーをきっかけにサイバーセキュリティお助け隊サービスを採用。本社と全営業所に UTM を導入した。IPA からの注意喚起メールを社内報に掲載し、社員にセキュリティ対策を呼びかけるなどの対策も実施している。次に何の対策をするかについて、社員へのセキュリティ教育の推進方法と併せて、他社の事例を参考に検討したいとのことである。

2.　経営者によるセキュリティ対策のかじ取りについて　理想と現実

現在Ｃ社では総務部長のＮ氏がセキュリティ方針の策定から実行までを一貫して任されているが、

社長は外出が多いため、インシデントが発生した際に迅速に対応できないことも N 氏が任命された理由の 1 つとのこと。N 氏本人は、自身が IT の専門家ではないので、セキュリティに関する知識が不十分のまま責任者を続けることに、不安を感じている。

その他ヒアリング事項

■ サイバーセキュリティ全般について

・ 従業員数や資本金が少ない中小事業者ほど、セキュリティに対する意識が十分ではなく、保険やシステム投資に消極的である。その一方、実際にはセキュリティ対策が十分ではない小規模事業者を狙った攻撃も多くみられる。（【大阪②】B 社（保険代理店業）N.K 氏）

・ 2、3 年前の社内のセキュリティ対策は、個人でウイルス対策ソフトを導入する程度であったが、大企業や大学などの大規模な組織が会員として参加しているため、より本格的なセキュリティ対策が必要となり、2 年前から段階的に対策を進めてきた。その一環として、現在 ISMS の導入を進めている。（【大阪②】D 社（産学連携支援サービス業）N.M 氏）

・ インシデントが発生した際に、相談できそうな相手はいない。（【大阪②】E 社（特殊塗装業）M.M 氏）

・ 企業と大学をつなぐインターンシップ情報システムを運用しているが、登録情報のセキュリティが不安で、大学や企業から登録してもらえないという問題がある。したがって、まずはシステムのセキュリティを向上させることで、信頼を獲得し、より多くの情報を登録してもらうことを目指している。（【大阪②】D 社（産学連携支援サービス業）N.M 氏）

・ サイバーセキュリティ対策について、予防だけでなく、事後対策も重要である。インシデントは必ず発生するという前提で、検知、対応、そして復旧の手順を確立すること、また経営層もサポートしていくことが重要である。（ファシリテーター・田中氏）

■ 社員教育について

・ 学生のアルバイトを多数雇用しており、彼らについても、職員と同じレベルのセキュリティ知識を持ち、業務を遂行できるような教育方法を確立することが必要。（【大阪②】D 社（産学連携支援サービス業）N.M 氏）

・ 派遣社員を受け入れる際は、業務開始前にセキュリティに関する資料（IPA の「情報セキュリティ自己診断」）の閲覧と受講を義務付けている。（【大阪②】A 社（システム構築・販売業）U.R 氏）

■ 現在の悩み

・ 社員の増員を予定しており、サイバーセキュリティ対策について一層学ぶ必要がある。（【大阪②】E 社（特殊塗装業）M.M 氏）

・ 経営陣に情報セキュリティ対策の重要性を理解してもらうためのアプローチ方法を知りたい。（【大阪②】E 社（特殊塗装業）M.M 氏）

・ クラウドのパスワード管理について、他社事例を参考に運用計画作成に取り組みたい。（【大阪②】D 社（産学連携支援サービス業）N.M 氏）

■ サイバーインシデント事例（未遂含む）

・ 過去に個人の SNS アカウントを盗まれた経験がある。焦ると集中力が落ちると自覚があり、なりすましメールを受信した場合、開封してしまう可能性が高いと思う。（【大阪②】B 社（保険代理店業）H.S 氏）

・ 過去に取引先から不審なメールを受信した際、送信元に電話で確認をしたところ、被害を免れることができた。（【大阪②】B 社（保険代理店業）N.K 氏）

■ サイバー保険について

・ 調査費用、復旧費用、場合によっては賠償費用など、多くの金額が必要となる場合がある。またこれらの費用は、企業規模にかかわらず、全て自己負担となる。たとえ一人あたりの見舞金が「500 円」のクオカードであっても、件数によっては億単位の費用になる可能性がある。（【大阪②】B 社（保険代理店業）N.K 氏）

・ 保険料はそれほど高くなく、また、セキュリティ対策の実施状況に応じて保険料が変動するという仕組みがあるため、取り組みやすいのではと思う。割引の具体的な仕組みは、契約時に、パスワードの管理方法や、使用しているソフトウェアなど様々な項目について告知が求められ、適切な対策を施しているほど割引率が高まる。また、商工会議所等の加盟団体であれば、団体割引が適用されることもある。（【大阪②】B 社（保険代理店業）N.K 氏）

・ サイバー保険の事業者にはセキュリティの専門家が多く、保険に加入することによって、金銭的な補償に加えて専門家とのつながりができること大きな利点である。特にセキュリティベンダーとの関係がない中小企業にとっては、システムに問題が発生した際、すぐに対応してもらえる相手がいることは極めて安心なことである。（関西情報センター・石橋）

サイバーセキュリティ懇談会　事例概要
熊本県　熊本商工会議所

【熊本】G 社（広告代理店業）社長　H.H 氏
～海外からのサイバー攻撃の被害を受けて～

１．　海外からのサイバー攻撃を特許庁、警察に相談

広告代理店業務、販売促進計画の立案およびテレビ CM やプロモーションビデオなどの動画コンテンツの制作を行う G 社の H.H 社長。一日に 100 通もの迷惑メールが送られてくるなど、日々の通常業務においてもサイバー攻撃にさらされているが、過去には、自社の偽サイトが立ち上げられ、詐欺の踏み台サイトとされた経験を持つ。海外（韓国）からの仕掛けにより、偽サイトから商品購入すると、海外へと送金される仕組みとなっており、結果的には熊本県警の捜査により解決した事案であるが、著作権の侵害が大きな問題であったため、被害発覚時にまず相談したのは、特許庁であった。特許庁から、熊本県警サイバー班を紹介してもらい、証拠提出、捜査を経て解決へと至っている。なお、本件に関連し、民事裁判にまで発展したが、相手は賠償金未払いのまま廃業しており、H 氏は、こういったケースは、きりがないと感じている。

２．　サイバーセキュリティの甘さを危惧

G 社が行っている事業は、許認可事業であり、各業者がきちんと判断して守っているのが業界の基本である。しかし、オンラインによって、利便性が高くなった反面、デジタル関係の情報が取りやすくなり、リスクははるかに大きくなったと感じている。特にチャット GPT が出てきてからはさらに加速するのではないかと、制作業界では、危機感を持っている。最近、韓国の技術協会からマーケティング関連の商談がきたが、先方はセキュリティを非常に甘く考えている。契約書に関しても、印鑑はデジタルでとの申し出があったが、セキュリティがかかってないと、簡単に抜かれて、悪用される恐れがあるので、デジタル印鑑には同意していない。海外との取引の際には、国際契約を取り交わすこともあるが、常にセキュリティの甘さを危惧しながら、取り組んでいるのが実情であるとのことである。

【熊本】B 社（レジャー施設業）DX 担当　K.S 氏
～IT 投資のスタンダードとは？～

１．　どこまでやれば良いのか？IT 対策の悩み

九州などを拠点に様々なレジャー事業を展開する B 社で DX（デジタルトランスフォーメーション）を担当する K.S 氏。会社全体の IT 関連を管理する立場にあるが、近年、IT 監査が厳しくなったことで、逆に IT 予算が取りやすくなったと話す。監査法人から指摘されたことで、「セキュリティが経営にも

必要である」という上層部の意識改革へと繋がったと実感している。具体的な予算化というのは今後の問題であるが、かなりやり易くなったとは感じている。ただ、実際に IT 投資、サイバーセキュリティ対策を進めるにあたって、「どこまでやれば良いのか分からない」という大きな悩みを抱えている。様々なベンダーが来ては、いろんな製品を薦めていくが、全部を取り入れていたら、莫大な予算がかかる、1つの切り口でもいろんな製品が出てくる。正直なところ、どこまでやれば良いのかが全く分からないとのことである。今回の懇談会のような機会に顔を出しては、今のスタンダードがどのようなものか情報収集を行っているが、未だ方向性は定まっていない。

２．　サイバー攻撃の被害を受けて

過去にエモテットにやられたことがある。自社の施設の管理職の名前で関連会社にメールを一斉に送るという手口で、発覚してすぐに、全ての関連先約 60 件に電話でメールを開かないように注意喚起したが、開けてしまったところがあり、結果、顛末書の提出を求められたということがあった。なお、警察やベンダーへの相談については、客商売のため、世間にあまり広がり過ぎるのもためらわれ、報告レベルにとどまっている。また、業者に相談すると、全 PC クリーンアップするべきとの指摘があり、数千万単位の莫大な費用となるので、本インシデントが発生した事業部の PC30 台をクリーンアップし、様子見とした。結局この時一番問題になったのは、どこまで広がっているのか、追いかけられる形にしておかないとだめということである。その後は、ある程度はログがとれるようにしているが、被害が発生するのはある意味もう防げない。いろいろ注意喚起しても、完全にゼロにすることができないため、どこまで広がったかを把握するというのが大事だとつくづく感じている。

*ファシリテーター森本氏からのアドバイス

ウイルス対策ソフトはそれぞれパソコンに入っているが、最近では、ウイルス感染後のパソコンの異常な振る舞いを検知するものが出ていたり、パソコンだけではなくてネットワークも含めた広範囲な振る舞いを検知するような製品が出てきているので、活用を検討されると良い。

その他ヒアリング事項

■　サイバーセキュリティ全般について

・ 全てのシステムを自社で用意しようと頑張るのではなく、クラウドサービスを使用する等工夫をしている。（【熊本】D 社（農業コンサルティング業）N.K 氏）

・ 日本情報システムサービス協会によると、上場企業とそれに準ずる企業では、売上の 1%を IT 系の予算に取っており、そのうち、セキュリティにかけられているのが大体 5%～15% という結果である。（ファシリテーター・森本氏）

・ システムの属人化を排除し、できるだけ外部ツール利用へと移行している。（ゲストスピーカー小口氏）

・ 経営者には、サイバーセキュリティを自然災害や労災と同じ部類で捉えてもらい、保険という切り口からサイバーセキュリティを予算化してもらうような促しをするのも一つである。（ゲストスピーカー小口氏）

・ セキュリティ対策に最終的にお金がかかったとしても、会社を守るという体制、仕組みづくりにおいては重要であると考えている。（【熊本】C 社（害虫駆除サービス業）S.I 氏）
・ BCP 対策の一環として、 セキュリティシステムを入れるのも一案である。（ファシリテーター・森本氏）
・ 自社には、EDR を導入している。なお、外部とメールをやり取りする人や経理担当者のパソコンは当該 EDR でがっちり固めているが、畑仕事従事者の共有パソコンは OS の標準機能を使用するなど、役割によってメリハリを付けている。（【熊本】D 社（農業コンサルティング業）N.K 氏）
・ なるべく直近のウイルスの種類や被害事例にアンテナ立てておき、それに対してどういう対策がとれるかとかを調べるようにしている。（【熊本】C 社（害虫駆除サービス業）S.I 氏）
・ 仕事柄、センシティブな情報を山ほど持っているので、情報漏洩が一番怖いが、セキュリティは取引業者にお任せしている。（【熊本】F 社（法律事務所）H.M 氏）
・ 自社で導入しているクラウド型のセキュリティは、保険も付いており、万が一のときには、初動対応してくれるという仕組みになっている。（ゲストスピーカー小口氏）
・

■ 社員教育について
・ 誰がどの PC でどこにアクセスしたか、会社は全部履歴を取って見ている、ということを社員に公表することで、一つの抑止力としている。（ゲストスピーカー小口氏）
・ 従業員に対する抑止力という点においては、経営からなんらかの発信をすることは 非常に重要と考える。（ファシリテーター・森本氏）
・ 経営者側は、社員を監視しているというイメージを持たせるのが怖いというパターンもある。ただ、逆に情報漏洩があった時に「社員から出たわけじゃないよ」と証明するための手段という考え方もある。社員を疑わなくて済むための保険という考え方である。（一般社団法人熊本県サイバーセキュリティ推進協議会・橘氏）

■ 現在の悩み
・ セキュリティの予算は「コスト」という認識が社内にはある。認識を変えるには、上層部への説得材料が必要である。（【熊本】D 社（農業コンサルティング業）N.K 氏）
・ デジタル人材不足は大きな問題である。自社の場合、各世代に一人ずつしか IT が分かる人いないので、将来的にどうやって回していくか、懸念している。（【熊本】A 社（食品加工業）I.Y 氏）
・ まだ必要なしとの経営者の判断により、サイバー保険にも入ってない。サイバーセキュリティお助け隊サービスとは、どのようなものか興味はある。（【熊本】E 社（観光振興業）N.K 氏）
・ サイバー攻撃で懸念しているのは、内部からの持ち出しである。周りをがちがちにセキュリティで固めてしまうと、逆に業務の効率化を悪くする可能性があるが、社員を全部信じるというのもリスクがあるので、どこまでやるのか懸念材料である。（【熊本】C 社（害虫駆除サービス業）S.I 氏）

■ サイバーインシデント事例（未遂含む）

・ カード会社を偽ったフィッシング詐欺メールがくる。（【熊本】A 社（食品加工業） I.Y 氏）

・ 一日に 100 件以上の迷惑メールやショッピングサイトの購入通知などの怪しいメールがくる。（一般社団法人熊本県サイバーセキュリティ推進協議会・橘氏）

・ セキュリティベンダーは営業の人柄や対応によって決定している。実際に事前にエモテットに関する情報提供をもらっていたため、被害を防げたことで、上層部の導入判断となった例もある。（【熊本】C 社（害虫駆除サービス業） S.I 氏）

・ 実は知らないところで既にパソコンがウイルス感染していることが多い。月一回のレポートを見ると、ブロックはしているが、DOS 攻撃などについては受けている。一般社団法人熊本県サイバーセキュリティ推進協議会・橘氏）

サイバーセキュリティ懇談会　事例概要
神奈川県　横須賀商工会議所

【横須賀】A 社（自動車部品製造業）代表取締役　O.H 氏
～サプライチェーンインシデントを発生させないために　できること～

1.　大手自動車会社の関連会社のサイバーインシデント事件を教訓に

プラスチック製品を中心とした輸送用機械器具を製造する A 社。昨年、大手自動車会社の取引企業がマルウェアに感染したことをきっかけとして、サプライチェーン全体が巻き込まれるサイバーインシデントが発生した。事件の影響で、大手自動車会社は 1 日間操業を停止し、また、A 社自体も、納品を停止する事態となった。この経験から、O 社長は、自社が同様のインシデントを発生させてしまわないよう、セキュリティ対策を不備無く実施したいと感じている。

2.　UTM や攻撃メール等、社内のセキュリティ対策の現状と課題

2 年ほど前、情報ベンダーの紹介により UTM を導入した。だが、実際の運用については、未着手な部分が多く、今後は月次レポートやサポート等の利用を進めていきたいとのこと。迷惑メールについては、日々50 件ほど受信しているが、実際に被害にあったことはない。また、昨年の冬、生産本部長あてに不審なメールが届いたことがあった。当該メールについては開封せず、また、エモテットが流行っていた時期と重なっていたため、社員全員に注意喚起メールを発信した。社内に情報システムを専門に担当する社員がいないため、現在は事務員 1 名と生産本部長の 2 名で情報システムの業務を兼務している。

3.　上流取引先からのセキュリティ調査の現状と展望

上流の取引先企業からセキュリティ調査を受けるケースが増えてきている。環境や生産設備など、様々なテーマの調査を受けているが、セキュリティについては、自動車業界の取引先 5 社のうち 3 社からチェックリストの提出が求められた。現在は、チェックリストにある項目に対し、現状を「〇×△」で回答し、また、「×」、「△」と回答したものについては対応を質問されるといった状況である。今後は、「×」と回答した項目については監査が行われる可能性が高いと感じており、より一層の対応が求められるのではと考えている。

【横須賀】B 社（建築物修繕業）代表取締役　S.M 氏
～最新エンドポイントセキュリティの導入でエモテット被害を最小限に抑える　～

1.　エモテット被害に遭遇も、実害なく

ビルの保守・修繕・警備・設備管理等の事業を展開する B 社。昨年 6 月頃、エモテットによる攻撃メール被害に遭遇した。協力会社からの情報漏洩が原因と見られる。発覚のきっかけは、不審なメールが一定の時期に集中して社内に送られたこと。最初の問い合わせが情報システムに寄せられた後、似た内容の問い合わせが相次いで寄せられ、事態が判明した。IPA の攻撃関連サイトを参照したところ、当該事象がエモテット被害と確認できたため、全社に対して注意喚起を発信した。また、同サイトから提供されていた感染チェックツールを使用し、メールを受信したパソコンの感染の有無の確認をした。また、メールを開いてしまった社員もいたが、最新のエンドポイントセキュリティが導入されていたため、実害は出なかった。当該被害を受け、エンドポイントセキュリティソフトの最新化の重要性を再認識した。更新漏れ防止のため、更新通知受信後はすぐに更新する運用に改め、また、インシデント発生時対応の見直しも実施した。

2. 社内休眠パソコン、200 台が"ウイルスの温床"に？

社内には定期的なセキュリティ更新を実施していない、約 200 台の使われていないパソコンが存在する。これらについて、使い始める際にセキュリティソフトを更新することが重要であるが、台数が多いため、十分な管理がされていないとのこと。また、厳密な管理を実施するにもコストが多くかかるので、対策の検討が必要と考えている。

その他ヒアリング事項

■ サイバーセキュリティ全般について

・ メールを使用した受発注や、クラウドサービスを利用した営業日報管理等、業務のデジタル化を推進中。取引先に、請求書をエクセルや PDF ファイルで作成してもらえるように依頼した。（【横須賀】C 社（衣料洋品販売業）T.K 氏）

・ お客様から預かった図面や、自社の金型図面などの重要な情報を守るため、セキュリティ対策を強化している。会社にある 8 台のパソコンのうち 1 台が古い OS のままであったため、その危険性を指摘され、OS の入れ替えを実施した。UTM も導入済みである。（【横須賀】E 社（金属プレス業）M.A 氏）

・ UTM の運用については、メーカーに一任している。月に 1 回レポートを受け取っているが、内容についての理解が難しく、受け取るだけになっている。（【横須賀】E 社（金属プレス業）M.A 氏）

・ 本社は UTM を導入済みである。調剤薬局の各支店については、メーカーが受注したものが設置されている。（【横須賀】F 社（調剤薬局チェーン業）M.Y 氏）

・ クラウドサービスへのアクセスは、シングルサインオンを採用している。社内からのアクセスには証明書が必須となっており、また、社外からのアクセスは VPN を経由する設定となっている。VPN の管理は外部の委託会社によって行われている。（【横須賀】B 社（建築物修繕業）S.H 氏）

・ 少し前、会社の HP を更新するタイミングで HP の SSL 化を実施した。（【横須賀】C 社（衣料洋品販売業）F.M 氏）

・ 現在、バイヤーはテザリングを活用して発注を行っている。（【横須賀】C 社（衣料洋品販売業）T.K 氏）
・ 社外にシステムに詳しい相談相手がおり、UTM以外の社内システムの相談を委託している。現在、社内にあるパソコン 40 台の入れ替えを依頼している。（【横須賀】C 社（衣料洋品販売業）T.K 氏）
・ セキュリティの専門家ではないが、社内でパソコンが一番得意なのは社長本人であるため、実質的な担当者と化している（【横須賀】E 社（金属プレス業）M.A 氏）
・ 先日、会員企業を対象にセキュリティアンケートを実施した。3,600 件の発信に対し 209 社から回答を得、うち 36 社がサイバー被害の経験があることがわかった。回答が得られなかった 9 割の会員企業については、セキュリティに対する関心が薄いものと推測しており、意識向上にむけた対策を検討する必要がある。（横須賀商工会議所・菊池氏）
・ 今回の懇談会の参加企業のように、セキュリティ対策が実施できている企業は少ないのではと感じている。やはり費用面のハードルが高く、社長に意識はあるものの、セキュリティ対策以外の支出が優先される状況があるのではと思っている。（かながわ信用金庫・片岡氏）
・ クラウド型オンライン会議サービスを使用する際は、データの保存先を注意している。（【横須賀】D 社（NPO 法人）T.Y 氏）

■ 社員教育について
・ 社員のセキュリティ意識の向上が課題。現在、売り場ではタブレット端末を使用して採寸を行っているが、採寸した情報を個人情報として注意深く取り扱うという意識が、現場の担当者に持てていない。（【横須賀】C 社（衣料洋品販売業）T.K 氏）
・ 信用金庫内においても、金融機関として多くの顧客情報を預かる立場とはいえ、職員のセキュリティ意識は必ずしも高くない。意識の向上が必要であると感じている。（かながわ信用金庫・片岡氏）

■ 現在の悩み
・ 取引先である小規模な町工場においては、多くの場合、設備投資が遅れており、10 年、20 年前の古い機械を使い続けている。また、その場合、機械につなぐシステムも古いままの場合が多い。（古い OS や磁気憶記録媒体など）取引先が保有するリスクについて、我々ができることをアドバイスいただきたい。（【横須賀】E 社（金属プレス業）M.A 氏）
・ BCP 時やインシデント等の発生時の運用について（連絡体制等）教えてもらいたい。（小口社長へ）（【横須賀】E 社（金属プレス業）M.A 氏）

■ サイバーインシデント事例（未遂含む）
・ 行政機関になりすましたメールを過去に受信した。普段受信するメールにはない、行政機関のホームページへのリンクが貼られていたので不審に思い、従業員に開かないように注意を促した。その後、市内の介護事業所で大規模なコンピュータウイルス感染が判明したとのことである。たまたま、

システムに詳しい従業員が最初にメールを見たおかげで、不審な点に気づき、社内の感染を防げた。（【横須賀】F 社（調剤薬局チェーン業）M.Y 氏）

・ あるアジア圏の国の企業とのやり取りの間だけ、社内のセキュリティシステムがブロックする不正サイト数が増加する。画面に勝手にチャットボットのようなものが沢山出現する。（ゲストスピーカー・小口氏）

・ 地域の団体にて聴取した事例だが、あるアジア圏の国から、振込先の変更を知らせるメールが届き、それを信じて振り込むと詐欺だった、というケースが多いとのこと。お金が関係する事項については必ず先方と電話で確認する必要がある。（ゲストスピーカー・小口氏）

■ その他（提言等）

・ 大企業の事例だけニュースに取り上げられるが、サプライチェーンの下流や小規模事業者もサイバー攻撃を受けている。中小企業がその事実を知ることが重要なので、商工会議所等から会員企業に向けた発信を希望する。（ファシリテーター・田中氏）

・ サプライチェーン内は、チェーン全体のセキュリティ向上が必要。一社だけがセキュリティ対策をしていても弱いところが攻撃され、共倒れしてしまう。サプライチェーン内における委託先の会社に対し、共にセキュリティ対策を強化していきましょう、と働きかけることが重要である。（ファシリテーター・田中氏）

・ 社内のセキュリティ対策について、複数人に相談できる体制を整えると良い。セキュリティ動向は変化が激しく、また、分野も多岐に渡るので、すでにお付き合いがある業者のほかにセカンドオピニオン的な第三者を加えることにより、より確かなアドバイスを得られるので安心である。可能であれば商工会議所や金融機関に、専門家の紹介の仲介役を担ってもらいたい。（ファシリテーター・田中氏）

・ 不審なメールを見分けるには、送信元のメールのアドレスをきちんと確認することである。メールソフトの設定によっては実際のメールアドレスが見えない仕様になっている場合もあるので、注意が必要とのこと（ファシリテーター・田中氏）

・ 社員のセキュリティ意識が、教育によって向上させることが困難な場合、システム内の操作について権限を限定的に付与する等、技術的な取り組みが有効な場合もある。ただその場合、運用のしやすさと事業継続リスクの天秤にかけることにもなる。（ファシリテーター・田中氏）

・ クラウドサービス利用時、データの保存先（国）に留意すること。（ファシリテーター・田中氏））

・ 何かあったときの連絡網を作成し、社内にて共有しておくことが重要である。また、バックアップしたデータのリカバリー方法についても事前に手順を作成し、机上演習と同様、訓練をしておくこと。（ファシリテーター・田中氏）

サイバーセキュリティ懇談会　事例概要
群馬県　高崎商工会議所

【高崎】C 社（建材卸売・建築業）　代表取締役社長　K.M 氏

～リスクに備え、事業継続のためにできることを最優先に取り組む～

1. 大切な企業情報を守るために

鋼材、建材の卸売業及び建築・土木専門工事等を営む C 社は、創業 200 年の老舗企業である。当社を率いる K 社長は、独自の方法でデータのバックアップ運用を実施し、大切な企業情報を守り続けている。クラウド利用の考え方として、インターネットにアクセスできなくなった場合のリスクを考え、最も信用でき、最も安心できる対策として、自らバックアップを行う運用方法を選択したとのことである。一般的に、データセンター等にバックアップすることが推奨されるが、中小企業においては、その予算化も難しく、クラウド側でデータ損失等の事故により業務が止まることが最大のリスクと考える。例えば、電気通信事業者は、「接続」を保証しているが、逆に「インターネット」は保証しておらず、「接続」を保証していた電話回線ですら、東日本大震災の時にはつながらなかった。インターネット回線あるいは電源が消失した際に、データが外（クラウド）にあった場合、自分のデータが見られないことになるので、最善の方法として、自分が生きている限りはこれからも当該運用を継続するだろうとのことだった。

2. その他のリスクへの備えと対策

サイバー攻撃に関して、個人メールに身代金要求メールが届いたら、まずメールを開く前にゴミ箱捨てるよう指示しているとのこと。最近は、PC のカメラを塞ぐ対策もしており、幸い、これまでのところ、事故は発生していない。また、K 社長はよく海外旅行をするので「死んだときマニュアル」というものを用意していると言う。銀行口座のパスワード、葬式の方法等、何から何まで全部書いており、毎年更新しているとのことであった。リスクへの備えについて日頃から考えられ、事業の継続を図るべき対策を取られていることがうかがえた。電子帳簿保存法の施行にあたり、現時点では紙も残すつもりだが、将来、紙を残さない時代になった時に、過去に遡ってどこまで対策すれば良いかという不安を持っているとのことである。

【高崎】D 社（情報処理サービス業）専務取締役　S.J 氏

～組織の信頼を失う内部不正を未然に防ぐため、管理体制と社内教育の徹底を～

1. 内部不正を防ぐための取組

D 社は、創業 45 年、群馬県某所を本社に、国内の別都市に拠点を設けて、情報処理及びソフトウェアの開発を行っている。データ入力、コールセンター事業等を行い、多くの個人情報を扱うた

め、セキュリティについても細心の注意を払っている。情報システム部門を担当するK氏によると、今、最も怖いのは、内部不正、人に拠るところだという。いくら誓約書を書いても、何か事件を起こされると一発でアウトという点が今、最重要課題ではないかと考えているという。昨今、報道に出ているのは、PCにスマホやUSBメモリ等を差して、何回かに分けて持ち帰るというものだが、当社のPCは、USBや外部記憶媒体にデータを書けない設定にしており、自分の PC にスマホの充電をさせようとして差しても、管理者に通知が届く設定にしている。ただ、業務上、USBを使わなければならないPCは必要であり、一部設置していて、全て禁止というわけにはいかず、その辺りが難しい。

2. 社内教育の重要性を実感

当社にはコールセンターがあり、過去、あるオペレーターが、自分に与えられた PC ではない他の PC で何かしようとした形跡が残っていたことがあった。公表はしないが、後で管理側から当該オペレーターに、内々に注意している。オペレーターが30～40人いるが、暇な時間にインターネット検索等した際、急に「あなたの PC をロックしました」と画面に出て、オペレーターから管理者に慌てて連絡があり、確認すると、ブラウザーにただ表示されているだけで問題ないことが大半である。こうしたものまでは、システムでなかなか検知できない。今後、このような内容の社内教育も非常に重要と考えているとのことだった。ツール更新や教育面等、今後も終わることはないと考えている。事故が起きた時に、どのように行動するかをしっかりと考え、目標を明確にして、社内全体で進めていきたいとのことであった。監視装置の実績レポートについては、月に一度届き、目は通している。

その他ヒアリング事項

■ サイバーセキュリティ全般について

ビジネスメール詐欺に関して、私のお客さんも被害に遭われ、数千万円を振り込んでしまったという事件が実際に起こっている。ビジネスメール詐欺とは、例えば経理担当者のメールアカウントがどこかで乗っ取られる等、情報が漏れ、犯人から直接取引先への連絡が始まり、犯罪へとつながっていく。（ファシリテーター・山本氏）

・ 工場系では、ネットワークを分けている会社もあるが、そこでランサムウェア等のウイルス感染する事例をいくつも見た。工場を止めて全部 PC をチェックするという事例もあった。（ファシリテーター・山本氏）

・ 一応、メインの基幹システム、販売管理システムは関東に所在する会社に VPN でつなぎ、当社に 15 分に 1 回バックアップを取るようにしている。基幹システムが一番重要なので、万が一、本社、バックアップ拠点のどちらか 15 分のデータが確保できなかった場合は諦める判断をしている。(ゲストスピーカー・小口氏)

・ 20 年ほど前に福岡西方沖地震があったが、会社の所在地が海に近く、また、3 階のサーバールームに設置していた 10 台ほどのサーバーが全て落下した。復旧はできたものの、以後危機管理意識が高くなった。この経験から、会社にサーバーを置いておきたくないため、ほとんどをクラウドに変更し、基幹システムのみ、相模原に設置したバックアップサーバーに接続している。(ゲストスピーカー・小口氏)

・ 第 3 の拠点で重要なデータを持つということは共通認識と思う。（ファシリテーター・山本氏）
・ クラウド業者がバックアップを取り、要するに復元できるということ契約内容を信用しており、幸いなことに今のところ事故はないが、これに対するシミュレーションをしたことはない。（【高崎】A 社（ソフトウエア開発業） A.A 氏）
・ 製薬会社等では、データ、メールの保存期間について、3 年間だけは保存し、3 年後には自動で全て消えるということを会社のルールとして設定しているところも結構ある。（ファシリテーター・山本氏）
・ 経済産業省が、「地域 SECUNITY（セキュニティ）」というコミュニティづくりについて取組を進めており、セキュリティ・コミュニティという言葉はとても重要だと感じている。そのコミュニティの中心には商工会議所等がある。商工会議所等をハブにしながら、地域の企業が繋がり、各企業が事業継続していければと願う。（ファシリテーター・山本氏）

■ 社員教育について
・ グループウェアで毎月のセキュリティレポートを共有し、不正サイトにアクセスしかけてロックされた社員には私から大丈夫か？というコメントを投げかけたり、日頃から管理者が見ているという情報を出すことによって、社員の自発的な意識の向上を狙っている。年に 1 回の経営計画の発表会時にも、セキュリティ対策にまつわる話題に触れるようにしている。(ゲストスピーカー・小口氏)
・ お客様へも啓発する姿勢が必要だが、人とお金と時間をそこまでかけられないという課題もある。懇談会、セミナー等で新しい情報を取り入れて、それを当社だけではなく、関わる業者や、お客様にもきちんと伝えられたら、と思っているので、今回は良い機会をいただいた。（【高崎】E 社（情報処理サービス業） M.K 氏）
・ サイバーセキュリティお助け隊サービスは、非常に安価で良いが、これに全て頼ってしまう、丸投げというのも違うと考えている。サイバーセキュリティは進化していくので、アップデートもきちんとした上で、これらと合わせたサービスが必要であると考えている。（【高崎】E 社（情報処理サービス業） M.K 氏）

■ 現在の悩み
・ 当社では、P マーク研修等について、定期的に社員教育、社内の見直し等は行っているが、今、世代交代の時期で、多くの人間がこうしたセキュリティというものを意識しなければならないということで、できるだけ若手社員に順番に取り組ませているが、若手社員は、意識が IT 寄りになる傾向がある。本来であれば、本業に注力して、それに対してのセキュリティと捉えてもらえたらと思うが、その辺が逆転している。やはり、IT 世代、デジタルで育ってきた人達であり、いかに IT を便利に使うかに長けているが、会社での役割とセキュリティについて、同等に捉えられてしまうと、なかなか動き出せず萎縮する。いろいろチャレンジンさせたいが、結局チャレンジの裏側にそういったリスクがあることを感づいている。社会的にも大きな影響を与えることでもあり、その辺りのバランスが必要と感じている。（【高崎】E 社（情報処理サービス業） M.K 氏）

■　サイバーインシデント事例（未遂含む）

・　事故はないが、最近、郵便サービス会社をかたるメールなど、見分けがつかないなりすましが多い。察知した場合、社内に共有をしているが、特に現場は、受信したメールをいち早く処理しなければならないため、クリックをしてしまう可能性がたかく、危険と隣合わせの状況がある。（【高崎】E社（情報処理サービス業）M.K 氏）

・　相談窓口として、ホームページにアドレスを載せているが、そのアドレスに毎日かなりの数のないすましメールが届く。対策を講じても、イタチごっこで、すぐに別のメールが送られてくる。（【高崎】D社（情報処理サービス業）S.J 氏）

サイバーセキュリティ懇談会　事例概要
長野県　松本商工会議所

【松本】C 社（ウェブサイト制作業）代表取締役　N.Y 氏

～社員のセキュリティ意識の均一化を図り、社内外共にリスク対策を万全に～

1．ウェブサイト制作会社の脆弱性対策

ウェブサイトの制作と保守管理、プログラム開発などを行っているC社。主な取引先は民間企業だが、行政のウェブサイトも多数手がけている。ウェブサイトは主に CMS で構築しており、アップデートやセキュリティホールへの対応が頻繁に発生する。発生の度に更新を行うと、ウェブサイトが停止するなど顧客の負荷が高くなるため、社内で優先順位をつけながら対応を進めている。

2．　セキュリティ対策は、顧客側の意識も重要

長年システム開発に携わり、システムの使いやすさとセキュリティの強度を、バランスよく実現することが難しいと感じている。しかし、セキュリティ設定は不可欠であるため、顧客のセキュリティ意識を高めながら、対策を推進していきたいと考えている。セキュリティ対策費用については、近年のサイバーインシデント事例やセキュリティに関する知識の普及により、費用を支出することへの抵抗が薄れつつあると感じている。ただし、その場合もセキュリティ対策単体ではなく、保守管理サービスの一環として契約するケースが多い。

3．　セキュリティ知識、社内外で均一化へ

社内においては、現在、社員のセキュリティ知識レベルにばらつきがあり、同じレベルのセキュリティ対策が社内・外ともに均一にできていない。セキュリティリスクに対し、社員が共通の理解を持つことにより、効果的な顧客対応や、的確な社内インシデント対応につながると考えている。また、最新のセキュリティ情報の収集と、その社内共有についても、改善を進めていきたいとのこと。

4．　被害事例（顧客のウェブサイトが盗用クレジットカード 1 万枚の使用確認に利用される）

5，6 年ほど前、ある顧客のショッピングサイトで、約 1 万件のカード情報が使用され、そのカードが使えるかどうかを何度も試みられた。予審手数料が短時間で数十万円に上ったことをカード会社が検知し、不正使用が発覚した。調査の結果、当該事件はあるアジア圏の国からのアクセスだったといい、また、当時は類似する事件が横行していたとのことである。

【松本】B 社（ソフトウェア開発業）取締役執行役　T.H 氏）

～システムインテグレーター、ホームページ改ざんから学ぶセキュリティ対策　～

1．CMS の脆弱性を狙った自社ホームページの改ざん被害を経験

B 社は長野県に本社を置くシステムインテグレーター。長野県の中小企業を中心に、システム開発、運用、保守、および IT コンサルティングなどのサービスを提供する。また、首都圏の企業向けにもニアショア開発サービスも提供している。1 年ほど前に CMS の脆弱性が原因で、ホームページの一部が攻撃され、フィッシングサイトに誘導するような改ざんを受けた。外部から「おかしい」という情報が入って発覚し、発覚後すぐに HP を止めたが、その後サーバーがダウンした。被害直後は、ホームページ上での公表、IPA への報告やお客様への説明などの対応に多く時間を要した。また、攻撃された CMS について、毎月脆弱性が発表されているとが、被害後の調査にて判明し、使い続けるリスクが高いと判断。CMS を排除した、新たなホームページを作成することを決定した。業務への直接の影響はなかったものの、結果復旧まで 2～3 ヶ月を要した。ただ、新しいホームページになった今も、外部からの不審なアクセスは続いている。

2．全てのセキュリティ対策を実施すると負荷が高く リスクを許容しながらバランスの良い対策を

改ざん被害を経て、セキュリティ対策の重要性を再認識し、専門会社にリスクアセスメントを依頼した。ネットワーク構成図、組織の体制、ドキュメント類の整備状況、教育など各種対策の実施状況のヒアリングが 3～4 か月かけて行われた。結果、エンドポイントのウイルス対策や EDR、クラウドセキュリティなどの技術的な対策、また、インシデントが起きた時の業務フローや体制の整備が必要と判明し、現在対策を進めている。アセスメントの結果については、社員へ共有し、また、セキュリティ対策に言及する機会も増えたので、全体のセキュリティ意識が高まったと感じている。ただ、ベンダーから提案された対策について、全てを実施すると費用と対応の負荷が大きく、どこまで対策をすれば良いのかわからない悩みもある。リスクを許容しつつ、コストパフォーマンスの良い対策を選択していきたいと感じている。

3．開発標準プロセスと契約書で、セキュリティの責任範囲を明確化

開発標準プロセスや契約方法について、セキュリティを意識したものへ改善していくような取り組みが進行している。今までの契約書には、セキュリティの責任範囲が記載されておらず、万が一インシデントが発生した場合、システムを開発者の責任なのか、或いは運用するユーザーの責任なのかがはっきりしない。そのため、IPA のモデル契約書を参考に、法務部と協力して契約書の改善を進めている。また、開発標準プロセスにおいても、セキュリティ要件をユーザーと合意し、記録した上で進める、ように改善している。最近のシステムは多くの他のシステムと情報を連携しており、別のシステムからの侵入やアカウントの乗っ取りが発生した場合、責任が誰にあるかについて、決める等の対応に時間多くかかるようになってきていることが、背景の 1 つであるとのこと。

その他ヒアリング事項

■　サイバーセキュリティ全般について

・ 今年の初めに ISMS を取得したものの、自社のセキュリティ対策が適切かの確認がしたい（【松本】A 社（ICT 導入サポート業）K.K 氏）

・ システムの利便性とセキュリティリスクのバランスについては、企業ごとに正解がある。通常、最低限守らねばならない範囲を決め、複数のシステムを組み合わせて、希望の環境を構築する。（【松本】B 社（ソフトウェア開発業）T.H 氏）

・

■　社員教育について

・ 社内で責任者を決め、一月に一回、セキュリティの講義動画を社員に閲覧させている。ただ、ISMS 取得の条件として取り組んでいるので、「やらされ感」 がある。社員の意識が実際に高まっているかについてはわからない。（【松本】A 社（ICT 導入サポート業）K.K 氏）

・ 毎月のレポート等、サイバーセキュリティ関連の情報についてはグループウェアに情報を載せて社員に公開している。チャットを利用する場合もある。（ゲストスピーカー・小口氏）

・ セキュリティ対策の最大の課題は社員の意識。どれだけ教育をしても、悪意があったり、警戒心が低いと事故が発生してしまう。（【松本】A 社（ICT 導入サポート業）K.K 氏）

・ 松本商工会議所では、希望のメールアドレスと日時を提供するだけで、「標的型」攻撃メール訓練の申し込みができる、簡易メール訓練サービスを展開している。（松本商工会議所・梶原氏）

・ 社員の「教育」に頼らなければいけないセキュリティ対策からそろそろ脱却したい。工場なども、外国人労働者が多く所属するようになり、「教育ありき」から「仕組化」へと流れが変化している。本当は「教育」ではない方法で、セキュリティ対策が実行できる環境が望ましい。（ゲストスピーカー・小口氏）

■　現在の悩み

・ １つのウェブサイトに、多数の人間が携わる場合、１つのアカウントを使いまわす場合と、複数アカウントを運用する場合と、どちらがセキュリティリスクが高いかわからない。（【松本】C 社（ウェブサイト制作業）N.Y 氏）

・ 社員が５名と少なく、インシデント発生時の体制が確立されていない。ログをきちんと調べることができるのか、また、アカウント情報が漏洩した場合の対策が十分なのかといった課題がある。（【松本】A 社（ICT 導入サポート業）K.K 氏）

■　サイバーインシデント事例（未遂含む）

・ フィッシングサイトにアクセスした経験がある。普段使用しているクレジットカードの請求日を狙ってメールが送られた。ID とパスワードを要求され、入力すると次にクレジットカードの番号も求められた。不審に思い、メールを見直すと、URL があきらかにクレジットカードのものではなかった。その翌日には本物のクレジットカードの請求書が届き、フィッシング URL も UTM でブロックされた。偽 URL に ID とパスワードを入れたため、カード会社等に連絡をするなどし、全ての対応が完了するまで合

計 2 時間ほどかかった。（【松本】A 社（ICT 導入サポート業）K.K 氏）

・ プライベートで SNS アカウントの乗っ取り被害に遭遇したことによって、同様の事態が会社で発生することへの危機感が高まり、セキュリティ意識が高まった。（ゲストスピーカー・小口氏）

■ その他（提言等）

・ 生成 AI の登場により、文面のなりすまし技術が高度化している。一番確実ななりすましの見分け方は、やはりメールヘッダーを見ること。（松本商工会議所・梶原氏）

サイバーセキュリティ懇談会　事例概要
新潟県　新潟市商工会議所

【新潟】C 社（住宅用空調機販売業）取締役　相談役　Y.S 氏

～経営者も担当者と一緒にセキュリティ意識を高め、一丸となって会社を守っていく～

１．　経営者が情報セキュリティの重要性を正しく認識することが重要

主に工務店や販売店に住宅関連の設備や資材を販売する C 社。6 か所ある営業所等拠点との連携に、パソコンやオンライン会議を利用する機会が多く、社内のセキュリティ対策や規程等の整備が必要な状況である。中小企業におけるセキュリティ対策で重要なことは、経営者が情報セキュリティの重要性を正しく認識することと感じている。経営者も社員と一緒に情報収集をし、話し合って会社を守っていく姿勢が大切である。

２．　セキュリティ対策は、まずは「何を守るべきか」について考えることから

セキュリティ対策の第一歩は、まず「何を守るべきか」と「どの程度守るべきか」を社内で話し合うことであると考えている。数年前にエモテットが流行していた頃、取引先から、「攻撃メールをしたのではないか」と懸念する電話を受けたことがある。実際の被害はなかったものの、サイバー被害に遭遇すると、データだけでなく、取引先の信頼も失墜することを実感した。被害に遭遇した場合のリスクとその対策費用を明らかにし、対策を行う範囲について、社内で話し合い、ルールを策定する必要があると痛感した。また、セキュリティに関する最新情報をグループ会社全体に発信することも重要であると考えている。

３．　住宅関連業界におけるデジタル化の現状について

住宅関連業界は特にデジタル化が遅れている分野である。また、中小企業においては、社員の IT リテラシーの差が大きく、また、IT 担当者の有無や、経営者が IT にどれだけ詳しいかなどによって、会社のデジタル化が大きく左右される。デジタル化については、新しい法令への対応など、企業として IT 化を進めざるを得ない状況になって初めて動くのが現実。従って、セキュリティ人材育成や社員教育、予算の確保については、なかなか進んでいない状況である。また、紙に印刷された個人情報等の機密情報の管理については、社内に規程はあるが、運用については現場の判断にゆだねられている。

４．　中小企業では、通常、セキュリティ対策予算は後回しに

中小企業の経営者は、セキュリティ対策への関心はあるものの、実際に被害に遭っていない場合は、利益を生む投資を優先してしまうのが現状。中小企業では、売上、利益、賃上げなど、先にお金がかかることから予算を決定する。実際に被害が発生していないセキュリティ対策に予算を充てることは難しい。しかし、今回の懇談会に出席したことで、売上利益に対して、一定の割合でセキュリティ対策の予算を組む必要との意識に変化した。

５． 今後は業界団体もセキュリティ対策のまとめ役を

当社が所属する業界団体（協同組合）においては、情報セキュリティや事故の話は出ていない。組合会員はライバル会社もいるので、情報セキュリティに対して「じゃぁどうしようか」という話しにはならない。協同組合がまとめ役となり、意見交換会等を主催する方向性については正しいと思うが、協同組合の事務局は限られた人数でやっているので、そういった話まではいかない。

【新潟】A 社（パソコン設定・サポート業）代表取締役 S.H 氏

～33 あるグループ会社のサイバーセキュリティ対策の展開に注力～

１． 33 社あるグループ会社全体のセキュリティ対策を開始

建築事業者のグループ企業にパソコンやネットワーク機器等をレンタルする A 社。今まではパソコン等電子機器の納品が主だったが、近年はネットワーク関連の仕事が非常に多い。複数のグループ会社がサイバーセキュリティ被害に遭遇したことを受け、昨年度、33 社のグループ会社に対しセキュリティに関するアンケート調査が実施された。調査の結果が良くなく、親会社から啓発活動を一任されたことを受け、来年度からグループ全体のセキュリティ対策について展開していきたいと考えている。対策を開始するにあたり、セキュリティに対する意識や社内にある最も重要なデータは、グループ会社によって異なるため、まずは 各社に「今、守らなければいけない情報はなにか」について整理してもらうことから始めている。

２． 機材の導入よりも、まずはセキュリティアクションの実行

セキュリティアンケート調査の結果、グループ会社ごとに「どこが弱いか」という話しをしている。セキュリティ対策として機材を入れるのは簡単だが、実際にどう使うかが重要であり、人の問題が一番ひっかかっている。例えば、外部に漏れてはいけないデータをネットワーク上に置かない、データを扱うことのできる人を分ける等を行っている最中である。また、グループ会社各社にとっても、どれだけの費用がかけられるか、ということもあるので、まずはセキュリティアクション一つ星の 5 か条を各社が徹底するのが良いのでは、と考えている（A 社自体はセキュリティアクション二つ星を宣言済）。

３． 過去 2 回、ウイルスメール被害に遭遇

S 氏個人の経験だが、過去に 2 回ウイルスメール被害遭遇している。1 件目は、1 台の端末から突然異常な数のメールが発信される現象が起こった。汚染された端末をクリーンアップした後も、別の端末から同様のメールが発信される現象が連鎖的に発生した。最終的には全社のネットワークを遮断し一斉クリーンアップを実施し、解決した。2 件目はアドミニストレーター（admini@xxx）宛にウイルス付きのメールが送信され、誤ってメールを開いた端末のデータが一気に消去された。攻撃されたメールアドレスのドメインが大手製薬会社の社名と酷似していたため、誤って攻撃されたものとみている。当時はまだウイルス対策ソフトが普及し始めの頃であったため、その一年後に全端末へウイルス対策ソ

フトを導入した。

その他ヒアリング事項

■　サイバーセキュリティ全般について

・　最新のデジタルツールを利用するなど、社内のデジタル化は進んでいるが、セキュリティ対策については未対策の部分が多い。自社内において、サイバーセキュリティ対策が進まない原因は、①実際に被害に遭った場合の具体的な社内への影響や損害について想定ができていない　②攻撃を受けている自覚がない（攻撃を受けたかわからない）の 2 点であると感じている。（【新潟】B 社（食品販売業）N.S 氏）

・　数々のセミナーを開催し、サイバーセキュリティに関し「そのものに興味がない」「うちの会社には関係ない」と思っている事業者が多いと実感している。（ファシリテーター・武内氏）

・　経営者は、セキュリティ対策への関心を維持させることが難しく、費用も可能な限り抑えたいとの方針を持っている。そのような経営者に対し、必要なセキュリティ対策について、いかに説得するかが悩みどころである。（【新潟】B 社（食品販売業）N.S 氏）

■　　社員教育について

・　EC での WEB サイト販売を運営するなど、多くの個人情報を取り扱っているなか、社員も個人情報を漏洩させてはいけないという意識は強く持っている。しかし、具体的な取り組みについては、まだこれからである。太田油脂様の一回 15 分のセキュリティ対策動画を年に 15 回視聴する、という教育の仕組みに興味を持った。（【新潟】B 社（食品販売業）N.S 氏）

■ サイバーインシデント事例（未遂含む）

・　従業員数一桁の会員事業者が身代金要求型攻撃を受けた。その事業所に出入りしていた業者が、たまたまサイバーセキュリティお助け隊の駆けつけを担当しており、紹介を経てお助け隊の UTM を導入した。事件を経て、このような小さな事業所でも攻撃を受けることがあるということと、小規模の事業所には IT 担当者がおらず、攻撃をうけた場合、現場がパニックになると学んだ。（新潟商工会議所・相馬氏）

・　リンクや添付ファイル等何もついていない、脅迫文のみのメールを受信した。（【新潟】B 社（食品販売業）N.S 氏）（*メールアドレスが実際使用されているかの確認後、次の攻撃がされるケースがある。もしくはメールの半分がウイルス対策ソフトによって消去されている可能性もある。(ファシリテーター・武内氏)）

・　セキュリティソフトの設定を忘れたパソコンを、社員に渡したことがある。設定の担当者が 1 名しかおらず、が同時に複数の社員が入社したり、パソコンの入れ替えの時などに、設定が忘れられがちであるとのこと。（【新潟】B 社（食品販売業）N.S 氏）（*再発防止のために、運用手順書の作成とルール化が必要（ファシリテーター・武内氏））

・　協力業者の利益率が記載された見積書を、顧客にそのまま転送する誤送信が発生した。事

件後、防止対策として、メールの遅延機能を導入した。（【新潟】A 社（パソコン設定・サポート業）S.H 氏）

・ 禁止されているにもかかわらず、ブラウザーへパスワードを実際に保存する社員がおり、その結果、3 件の情報漏洩が発生した。（ゲストスピーカー・太田氏）

■ その他（提言等）

・ どの会社もセキュリティ対策単体で予算を取ることへのハードルが高い。ただ、「デジタル対応」には必ず「セキュリティ」はセットで考える必要がある。（ファシリテーター・武内氏）

・ デジタルツールの導入とセキュリティ対策は両輪である必要がある。デジタル化が進めば、コストダウンが可能と意識し、その浮いたコストをセキュリティ対策に当てる、という考え方で進める。（ファシリテーター・武内氏）

・ 社内にあるオーバースペックのシステムを見直し、浮いた費用をセキュリティ対策に充てるのも方法の１つ。ただ、システムの見直し１つについても担当者の負荷が高いので、経営者の理解が必要である。（ゲストスピーカー・太田氏）

・ 会社に導入したシステムについて、安全性を確保することは会社（経営者）の責任である。（ファシリテーター・武内氏）

・ 一見面倒なセキュリティの運用ルールについても、繰り返し社内に発信することによって、社員の意識向上を図ることが大切である。（ゲストスピーカー・太田氏）

・ セキュリティ対策において、一番重要なことは、社員が「何のためにルールを守るのか」をきちんと理解をしたうえでルールを実行すること。また、インシデントが発生した場合に、社内の業務が完全に止まってしまうリスクについても正しく理解しておくことである。（ファシリテーター・武内氏）

＊新潟商工会議所における、お助け隊の普及状況に関する情報共有
（新潟商工会議所・山口氏/相馬氏）

・ サイバーセキュリティお助け隊の再販事業者になっているが、普及が苦戦する理由として、「ファイヤーウォールで対策が十分だと考えている」、「実際に攻撃を受けておらず対策の必要性を感じにくい」といった声が聞かれる。セキュリティ対策に関する告知などを工夫し、会員企業に UTM の必要性について実感してもらう必要がある。

・ 実際に UTM を導入した事業者は、社内に IT 担当者を置いている場合が多い。事業者の規模感は二極化しており、大きな事業者では、UTM の知識があり、複数のサービスを検討した結果、安価なお助け隊を選択するケースが多い。一方で小さな事業者では、UTM の知識がなく、言われるがまま利用していた高額な UTM の保守契約が切れたタイミングで、より安価なお助け隊を選択するケースが多い。このため、お助け隊の普及に向けて、IT 担当者を置いていない事業者へのアプローチを検討する必要がある。

・ お助け隊への問い合わせは、経営者からと、IT 担当者からが半々。IT 担当者は、経営者に

対して説得するための情報を取集するケースが多い。

・　病院でのサイバー被害事件をニュースで知ったことをきっかけに、自社のセキュリティ対策の見直しを検討し、UTM の導入につながった事業者（介護事業者）があった。