2021 年度　中小企業における
情報セキュリティ対策に関する実態調査
―　事例集　―

2022 年 4 月 26 日

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

目次

農業・林業・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・p. 2

建設業・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・p. 4

製造業・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・p. 11

電気・ガス・熱供給・水道業・・・・・・・・・・・・・・・・・・・・・・・・p. 19

鉱業・採石業・砂利採取業・・・・・・・・・・・・・・・・・・・・・・・・・p. 20

情報通信業・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・p. 21

運輸業・郵便業・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・p. 30

卸売業・小売業・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・p. 31

金融業・保険業・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・p. 38

不動産業・物品賃貸業・・・・・・・・・・・・・・・・・・・・・・・・・・・p. 47

サービス業・その他・・・・・・・・・・・・・・・・・・・・・・・・・・・・p. 51

対策･投資多

「中途採用者の知識を活かして、情報セキュリティ対策を強化」

▼会社概要

所在地	北海道
従業員数	21～50 名
業種	農業･林業
実施している対策	● 従業員の PC にデータを残さないための環境構築を実施。 ● 日次でのデータバックアップの実施。

情報セキュリティ対策の取組

当社は北海道で林業を営んでいる。当社では従前からファイアウォールの設定やウイルス対策ソフトウェアの導入等に取り組んでおり、情報セキュリティ対策に関する基本的な基盤があった。一方で、セキュリティパッチの適用等については必ずしも十分ではなく、万全の対策が講じられているとまでは言えない状況でもあった。しかし、基本情報技術者の資格を有する従業員が入社したことをきっかけとして情報セキュリティ対策の強化が図られるようになっている。

会社として最も大きなダメージにつながるのは顧客情報の漏えいと考え、その対策を強化している。たとえば、従業員の PC 内にデータを残さないようにするために、PC を一台準備してファイルストレージとして活用する環境を構築した。当初は NAS サーバの導入も検討したが、コスト面での障壁もあり、それほどコストをかけずに実現できる手段としてこの方法を採用し、環境構築を実現した。この対策を講じることができなければ、たとえばルータに外付けの HDD を接続し、そこでデータを保管するようにするだけでもセキュリティレベルは上がると考えている。

また、近隣の企業にて、ウイルスに感染したことがきっかけでデータが全損したという話を聞いた。しかもバックアップを取っていなかったため大きな被害につながったようである。こうした事態に陥らないようにするために、日次でデータのバックアップを取るようにすることで、有事の際でも早く復旧できる体制をとっている。

情報セキュリティ対策の効果

先述の取り組みを通じて、従業員からは作業効率が上がり、業務環境が便利になったという声が寄せられている。これまでは個々に様々な方法でファイル共有がされていたが、ファイルストレージが整備されたことによって情報共有をしやすくなっている。また、間接的な効果ではあるが、従業員の PC へ直接データを保存せず、ファイルストレージにファイルを保存する運用とすることで、従業員が保有する PC の高寿命化にも多少貢献しているものと考えている。

今後、さらに情報セキュリティ対策を強化するためには、従業員の意識変革が必要であると感じている。たとえば、ファイル送付時に圧縮およびパスワード設定を徹底するような意識啓発に取り組んでいくことも進めていきたい。加えて、同業者のなかにはフリーメールを利用する企業も少なくないが、セキュリティ面でも信頼面でも独自ドメインの方が好ましく、フリーメールに対する対策も進めていきたいと考えている。

対策･投資多

「従業員が安心して働けることが対策実施のメリット」

▼会社概要

所在地	鹿児島県
従業員数	5 名以下
業種	農業･林業
実施している対策	● 操作ログの管理や、デバイスの利用者制限等の基本的な対策実施。 ● 自社の状況を踏まえ、セキュリティ対策の一環としてクラウド利用を開始。

情報セキュリティ対策の取組

当社は鹿児島県で農業を営んでいる。当社には関連会社があり、情報セキュリティ対策は関連会社の担当者が主導している。

農業関連の企業は情報セキュリティ対策について関心が低いと感じることもあったが、同業者の中にも情報セキュリティ対策に関心を持ち、取り組みを開始する企業の話も聞くようになり、当社も情報セキュリティ対策に取り組まなければならないと考えるようになった。

現在実施している情報セキュリティ対策は、従業員が使用するデバイス操作のログの管理、デバイス利用者の制限、定期的なデータのバックアップといった基本的な対策が主である。最近では、情報セキュリティ対策の一環として、一部のデータの管理にあたり、クラウドサービスの導入も行った。クラウドサービス事業者からの情報漏えいリスクはあるものの、当社の状況を客観的にみると、自社で管理するよりもクラウドを利用する方がセキュリティレベルは向上するのではないかと考え、導入に至った。

従業員への情報セキュリティ教育は、関連会社から共有される情報の共有を行うことが主であるが、簡単な勉強会も実施することで、情報セキュリティ意識の向上に努めている。

契約時は、発注元及び発注先のいずれとも秘密保持契約を結ぶ機会は多い。しかし、それ以外に具体的な情報セキュリティ対策の実施を求めたり、求められたりするケースは、現在のところほとんどない。

情報セキュリティ対策の効果

実施している情報セキュリティ対策の内容について、社内外に対して積極的に発信しているわけではなく、当社が実施している対策が社内外からどのようにみられているかはわからない。そのため、情報セキュリティ対策実施の効果を確認することは難しい。しかし、従業員一人ひとりが特別意識することなく自然に情報管理ができているという状況をみると、各種セキュリティ対策の効果が発揮されていると考えられる。また、情報管理がしっかりとできていることで、これまで当社が情報セキュリティ上の被害にあっていないと考えられることも、対策を実施によるメリットの1つであると考えている。

従業員には情報セキュリティ意識を高めてほしいと考えている一方で、本業に注力して業務効率の改善に取り組んでほしいという思いもある。そのため、業務効率を改善しつつ、情報セキュリティ対策を効率よく推進するための方法を模索している。

取引先要請多

「従業員のリテラシー向上に IPA の IT パスポート試験も活用」

▼会社概要

所在地	宮城県
従業員数	5 名以下
業種	建設業
実施している対策	● 業務の IT 化と情報セキュリティ対策を一体的に取り組む。 ● 従業員に IT パスポート試験の合格を推奨し、知識の底上げを図る。

情報セキュリティ対策の取組

当社は宮城県で各種設備の設置･施工等を行う建設業を営んでいる。従業員は 5 名以下の規模で、個人事業主等の小規模な再委託先と協働して施工を行っている。公的機関等との取引もある。

情報セキュリティ対策については、公的機関等との取引時の要請をきっかけに対応しているものが多く、契約上も秘密保持や契約終了時の情報資産の取り扱い等について定めが設けられている。そのため、当社だけでなく再委託先にも同様の要請をしているが、当社からの委託先となるのは、いわゆる「職人」の方々であることが多く、中には PC やスマートフォンを利用していない方もいる。そのため、秘密保持の趣旨や意義を理解してもらう点を大事にしている。

当社では PC 等の IT 端末を利用していることもあり、アカウントの ID･パスワードの管理、セキュリティソフトウェアでのウイルスチェック、VPN の利用、端末認証に生体認証を導入するといった対策を実施している。当社も以前はほぼ紙媒体のみで業務を行っていたが、この 5 年間で取引先からも IT 化対応の依頼があったこともあり、IT 化に取り組んできた。情報セキュリティ対策はこの IT 化の一環として実施してきており、毎年一定の情報セキュリティ投資を行っている。

当社の場合、顧客の建物に係る図面等は機微に扱う必要があるが、大半は紙で管理されている。現状、電子情報として管理が必要なのは受発注の際の見積や顧客に係るデータなどであり、これらはクラウドサーバで管理している。不具合等に備えて、複数のクラウドサーバに分散してデータを保管し、可用性を確保するようにしている。

情報セキュリティ対策の効果

当社の場合は、業務の IT 化と情報セキュリティ対策を一体的に取り組んできたため、一番の効果は IT 化が進んだことである。会社規模が小さいため、業務効率化はもちろんであるが、顧客の要請に対応できたことで、取引機会が消滅することがなかったという点が一番重要な点である。情報セキュリティにかける予算不足にはいつも悩んでいるが、取引先からの信頼獲得は重要であり、情報セキュリティ対策はその基本であると考えている。情報セキュリティ対策を積極的に行っていることで、顧客からの信頼獲得の一助となり、信頼や安心感に基づく、引き合いや発注もあると考えられることから、営業上も重要なことであると認識している。

当社は役員含めて 5 名以下の企業であるため、日頃のコミュニケーションを通じて情報セキュリティの重要性について意識共有している。また、従業員に最低限の IT リテラシーやセキュリティに関する知識を有しておいてもらうため、IPA が実施している IT パスポート試験を受験してもらっている。試験勉強を通じ、従業員のリテラシー向上を期待することができ、結果として情報セキュリティコストの削減につながると考えている。

対策･投資多　被害有

「顧客情報を扱う当社の情報セキュリティ費用は、「原価」！」

▼会社概要

所在地	東京都
従業員数	21～50 名
業種	建設業
実施している対策	● 情報セキュリティの観点やデータ破損等のリスクも加味し、クラウドサービスを利用。 ● 委託先へ情報漏えい対策実施の誓約書提出を依頼。

情報セキュリティ対策の取組

当社は東京都で住宅等の建築請負や建売を行う建設業を営んでいる。近年は収益の複線化･安定化の観点からリフォームやメンテナンス事業も手掛けるようになった。

情報セキュリティ対策は、リフォームやメンテナンス事業を手掛ける際、個人名や住所、連絡先に加えて、住居の間取りやメンテナンス情報等、機微な情報を大量に預かるようになったことを契機として取組を強化した。

情報セキュリティ対策に取り組む中、標的型攻撃による被害を経験した。初動対応できたため、二次被害、三次被害は食い止めることができたようだが、取引先にも同様のメールをバラまくことになってしまった。直後にも注意喚起を行ったが、役職者の定例会議や施工パートナーとの会議等においても定期的に注意喚起は継続している。

専任ではないが 3 名の担当者をシステム、情報セキュリティ対策のために配置している。顧客情報を含め、以前は自社サーバにデータを格納していたが、情報セキュリティの観点やデータ破損等のリスクも加味して、現在ではクラウドサービスを利用している。端末側のセキュリティ対策としては、従業員には会社貸与の PC、タブレット、スマートフォンの利用を求め、必要なセキュリティソフトウェアの導入等を行っている。また、外部メール送信の際のパスワード設定、ファイルダウンロードの禁止といったルールも整備した。

委託先に対して、セキュリティ水準についてまで一律の基準を求めるものではないが、各社には当社が共有する顧客情報等について漏えいが無いよう、徹底したセキュリティ対策を求めており、その旨、誓約書の提出をお願いしている。

情報セキュリティ対策の効果

一般的に建設業界では、IT 化や情報セキュリティ対策が遅れていると言われているが、当社では HP や SNS を通じた発信を通じて引き合いを獲得するというスタイルの営業にも力を入れており、IT 化と情報セキュリティ対策は一体として取り組んでいる。実際、情報セキュリティ対策を進めたことで、社内の IT 化も進み、営業情報の発信もしやすくなったという効果も実感している。

当社でも当初は、シニア層を中心に、情報セキュリティ強化に対する戸惑いもあったが、必要性を理解してもらえれば、「できない」と言う従業員はいない。また、HP や SNS での情報発信についても、情報セキュリティ対策が進んだことで、従業員が安心して、これまでより積極的に行うようになったと感じており、営業上もプラスに働いている。

同業他社の中には、情報セキュリティを「コスト」とみなして、いかに削減するかに注力している企業もある。しかし、当社は情報セキュリティを「コスト」ではなく、「原価」であると捉えており、当社がサービスを提供する上で不可欠の対応であると考えている。

対策･投資多　取引先要請多

「認証維持のための定期的な見直しを好機ととらえる」

▼会社概要

所在地	愛知県
従業員数	51～100 名
業種	建設業
実施している対策	● 認証維持のための定期的な見直しの際に、情報セキュリティ対策が形骸化していないか積極的に見直しを実施。

情報セキュリティ対策の取組

当社は愛知県で工事やメンテナンス業務を行う建設業を営んでいる。取引先は官公庁や民間企業である。

取引先の企業から、情報セキュリティ対策の要請を受ける機会は多くはないが、ISMS 等の認証を取得されている企業から、情報セキュリティ対策の実施状況に関するチェックシートの記載を求められることはあり、都度、対策状況の共有を行っている。また、当社は二次請けのような形で業務を請ける機会もあり、当社へ発注する企業へ発注する親元の企業が ISMS 等の認証を取得している場合に、その後の委託先への確認も厳密に行っているのではないか、と推測している。

情報セキュリティ対策に本腰を入れた理由は、認証の取得が、行政事業の入札案件の要件に含まれるようになってきたためであった。

全社的な情報セキュリティ対策は、情報システムに明るいメンバー数名が連携して対応しているのが実態である。特に、懸念している情報セキュリティ上のリスクとしては、自社のファイルサーバへのアクセスができなくなることである。こうした事態となれば、業務への影響が大きいと考えており、中でも不正アクセスやランサムウェアの被害にあうことが怖いと感じている。

当社も ISMS 取得に向けて取り組み、無事に認証を取得したものの、認証取得に必要な要件は大手企業を想定している、と感じさせる要件が多く設定されており、対応が難しい点も多かった。たとえば、要件への対応にあたり、大きい IT ベンダ社製のソフトウェアの導入が一般的、という話を聞いたりするが、中小企業にとっては、金額が大きいこともあり、そこまでの投資の判断は難しいと感じさせられる。

また、テレワーク導入等の、社会的に求められている IT 環境の構築を行おうとすると、どうしても、より高度な情報セキュリティ対策等が必要となってくる。積極的に情報セキュリティ対策に費用を投じていきたいものの、当社は中小企業であり、潤沢な資金があるわけでもない。そうしたところに投資を行うことは難しいとは感じている。

情報セキュリティ対策の効果

対策を実施し、認証を取得したことで、行政の入札要件を満たすことや、加点要件を得ることができていることは情報セキュリティ対策を進めたことによる大きなメリットの 1 つである。

しかし、それ以上に、認証を維持していくために必要な定期的な見直し機会を利用し、全社的に情報セキュリティ対策の点検を行っていることで、一度実施した対策が、形骸化してしまう事態が防げている。このことは、情報セキュリティ対策実施の大きなメリットであると考えている。認証を維持するための定期的な見直しを前向きにとらえ、今後もセキュリティ対策を高度化させていきたい。

対策･投資多

「適切なシステムやソフトウェアを導入し、リスクを軽減」

▼会社概要

所在地	大阪府
従業員数	21～50 名以下
業種	建設業
実施している対策	● UTM の入替や MDM ソフトウェアの導入により安心してリモートワークが可能に。

情報セキュリティ対策の取組

当社は大阪府でビルの外壁の改修･補修等の業務を行う建設業を営んでいる。

当社では従前から受託業務において、案件に携わる従業員以外が不必要に関係ファイルを閲覧しないよう、アクセス権の適切な設定を求められたことはあった。しかし、当社が顧客から情報セキュリティ対策を強く求められることは少ない。一方で、新型コロナウイルス感染症拡大防止の観点からリモートワークを開始するにあたり、当社独自の判断として必要と考えられる情報セキュリティ対策を実施している。

具体的には、直近決算期に約 150 万円をかけ UTM(Unified Threat Management)の入替や MDM(Mobile Device Management)ソフトウェアの導入を行い、外部からの攻撃防止や会社が許可していない情報端末からの社内へのアクセスの制限等ができるような環境を整備した。

こうした情報セキュリティ対策を通じて、従業員は安心してリモートワークを行うことができるようになった。また、ファイルの暗号化や情報端末の遠隔ロックを通じて、万が一、USB メモリ等のデバイスを紛失してしまった場合も、意図しない情報漏えいを防ぐことができるようになった。しかし、それでもなお、MDM ソフトウェアによりアクセスログを取得することはできるが、「社内からの悪意あるデータの持ち出し」が生じた際、どのファイルが不正に持ち出され、その後、どのように取り扱われているか追跡することはできず、情報セキュリティ対策としては積み残しがあると認識している。

情報セキュリティ対策の効果

当社ではリモートワークを契機として、情報セキュリティ対策を強化した。これにより、クラウドストレージの活用やオンラインのグループ会議等、情報漏えいのリスクがあることから利用を控えていた IT ツールを安心して利用することができるようになった。

また、当社には年配の従業員も多く、IT ツールの利用にあたり事細かなルールを設定しても十分な理解を得ることができない可能性があった。その中で、情報セキュリティの強化を目的とした設備投資を行ったことで、従業員には必要最低限の教育、理解醸成のみを図り、それ以上の点については、システムやソフトウェア側で機械的に対応できるような状況を構築することができた。

IT ツールの利用には、情報セキュリティの観点から一定のリスクがある。しかし、IT ツールの利用に関して社内のルールを厳格化してしまうと、その利便性を大きく損ねることになる。IT ツールを利用することで、本来であれば業務の効率化を図ることができる利点を失わないよう、当社では適当なシステムやソフトウェアを導入し、想定される情報セキュリティ上のリスクを技術的にカバーしていくことが重要であると考えている。

対策･投資多　被害有

「従業員のリテラシー向上が一番の対策」

▼会社概要

所在地	石川県
従業員数	101～300 名
業種	建設業
実施している対策	● IPA が公表する資料を基に、社内規定の整備や周知を実施。 ● 管理者権限を持つアカウントを限定することで、ソフトウェアのインストールを制限。

情報セキュリティ対策の取組

当社は石川県で建設業を営んでいる。受注の際は元請として仕事を請けることも少なくない。

当社では過去に、社内の PC がトロイの木馬等のマルウェアに感染していたことがある。また、ランサムウェアに感染し、サーバ上のファイルが暗号化されて、身代金を要求されたこともある。この際は、復旧作業のために費用や時間を費やすことになってしまった。こうした背景もあり、情報セキュリティ対策には常に関心を持っている。

現在、実施している主な対策としては、IPA が公表する資料を基に情報セキュリティに関する社内規定の整備を行い、従業員のリテラシーを向上させるための周知を継続的に行っている。セキュリティ被害は、メールや改ざんされた Web サイトからのウイルス感染であることが多いと考えており、従業員のリテラシーを向上させる重要性を強く感じている。また、管理者権限がないと PC にソフトウェアをインストールできないようにしている。従業員に自由に仕事をしてもらいたい思いもあるが、情報セキュリティレベルを一定以上に担保しなくてはならないため止むを得ないと考えている。

当社が仕事を受託する際に、情報セキュリティ上の要請を受けることはあるものの、秘密保持の徹底を求められる程度であり、要請を厳しいと感じたことはない。一方で、当社から業務を委託する際は、継続的な取引先や大きな金額の取引を行う場合等には、取引情報確認の一環として、個人情報や機密情報の取り扱いの同意書を取得し、情報セキュリティ対策の徹底を求める注意喚起を行っている。しかし、業界特性上、協業先の中には、一人親方等も含まれており、まずは業法である建設業法の遵守等を優先して求めることとなる。そのため、情報管理について、要請を行い、契約締結時にその旨を盛り込めたとしても、抽象的な同意になってしまい、具体的な取り決めができていない場合があることや、教育･研修を行うことができていない場合があることは、今後の課題であると認識している。

情報セキュリティ対策の効果

当社は社内規定の整備を行っているが、その規定どおりに落ち着いて対応すれば、被害にあうリスクや、被害にあった際にも大きな問題にはならないと考えられるようになっており、安心感を得られている。このことは、対策を実施したことによるメリットと考えている。

現在実施している対策で十分なのかという不安は常にある。また、中小企業においてもテレワークが進んでいるが、どこまでのセキュリティ対策が必要なのかを判断することも難しい。しかし、IT 投資や情報セキュリティ投資を、いつでも十分に行うことができる環境にあるとは限らない。そのため、中小企業では従業員のリテラシーを向上させることが一番の対策になるのではないかと考えている。

対策･投資多

「業務効率化に資する情報セキュリティ対策に経営者も理解を示す」

▼会社概要

所在地	徳島県
従業員数	21～50 名
業種	建設業
実施している対策	● 情報セキュリティ対策の導入にあたっては、業務効率化につなげることも意識して実施。

情報セキュリティ対策の取組

当社は徳島県で施設の工事やメンテナンス等を行う建設業を営んでいる。

当社では業務においてインターネットバンキングを利用する機会が増えている。取り扱う金額も大きくなり、不正送金された際のダメージも大きいと感じたことをきっかけとして、情報セキュリティ対策に積極的に取り組むようになった。対策の検討･実施にあたっては、情報セキュリティ対策が高い水準で求められる業界での勤務経験のある従業員が入社してきたことをうけ、この従業員が主導して対策に取り組んでいる。

具体的には、VPN を含め、情報セキュリティ対策に必要な機能を備えたセキュリティゲートウェイ端末の導入を行った。また、古いサーバの入れ替えも実施した。サーバの入れ替えにあたっては、業務効率化も意識し、従業員に貸与するタブレット端末を使って出先で撮影した画像などの情報管理を行えるようにした。金額としては大きい投資になったものの、経営層の理解もあり、業務効率化にもつなげるための取り組みとしてとらえていたこともあって、スムーズに導入の意思決定を行うことができた。

サプライチェーンにおけるセキュリティの重要性について、最近耳にする機会もあるが、現在のところ、取引先から情報セキュリティ上の要請を求められてはいない。当社から業務委託を行う機会はほとんどなく、当社から情報セキュリティ上の要請を行うことはないが、今後、そうした機会が発生した場合には、積極的に要請を行わざるを得ないのではないかと思う。

情報セキュリティ対策の効果

先述の取組により、情報セキュリティの向上とともにデータ共有の利便性が格段に向上した。それまでは、社内でのデータの共有も、CD や USB メモリにデータを保存した上で、やり取りを行うことも多かった。社外からもデータの共有が行えるようになったことで、従業員が出社する必要のある業務を減らすことができ、新型コロナウイルス感染拡大に対処する対策としても非常に有益であったと考えている。

当社では現在のところ、取引先から情報セキュリティ上の要請を受けておらず、当社の情報セキュリティ対策の実施が、取引先からの評価につながっているわけではない。そのため、情報セキュリティ対策実施のメリットを大きく感じることは難しいが、同業者が被害にあったといった話を聞くと、当社では被害にあっていないのは対策が有効に機能しているおかげと考えることもできる。

サーバが停止してしまうと、業務が停止してしまう場合や、非効率になる場合も当然考えられる。こうした事態を引き起こすリスクを低下させることは重要と考えることができれば、情報セキュリティ対策の重要性や、実施によるメリットを再確認できるのではないかと考えている。

対策･投資多　被害有

「取引先から要請される前に、自主的に対策を進めることが重要」

▼会社概要

所在地	熊本県
従業員数	101～300 名
業種	建設業
実施している対策	● 発注元企業からの注意喚起情報の従業員への周知･徹底。

情報セキュリティ対策の取組

当社は熊本県で建設業を営んでいる。取引先は、インフラ関連企業や地方自治体を中心とする官公庁、同業他社の企業等である。

10 年以上前から、情報セキュリティ対策には関心を持って取り組んできた。社内の基幹業務の IT 化を進めるにあたり、情報セキュリティ対策は切り離せないものであるためである。近年は、情報セキュリティ対策に関する取り組みについて、取引先から要請を受ける機会も多くなってきている。特に、インフラ関連企業から情報セキュリティ対策を求める機運が高まっている。また、サイバー攻撃も多様化しており、求められる対策も増えてきたと認識している。

数年前、ファイアウォールの入れ替えを実施したが、その際に委託していた IT 関連業者の作業ミスにより、適切にファイアウォールが機能せず、メールを送信したものの不通になってしまうというような被害が生じ、取引先からの信頼を失いかけてしまった。当社のような中小企業が単独で情報セキュリティ対策を強化していくことは難しいと考え、外部の IT 関連業者に委託したものの、このような事態となってしまった。防ぎようのない事態であったと考えているが、高度化するサイバー攻撃にどのように立ち向かうべきか考えさせられた。

情報セキュリティ被害にあっている同業他社の話は、発注元企業の耳にも入っているようであり、最近では、発注元企業から、最新の被害事例について情報共有される機会も増えてきている。具体的な対策として、Windows Update の案内等も発注元から展開されてくるため、その内容を社内にも展開して、従業員への周知･徹底を図るように努めている。しかし、それ以上の対策を取ることの難しさも感じている。

発注元企業の一部には、発注時に PC やタブレット端末等を貸し出し、委託業務に係る作業については、貸与した端末を使用して作業するように要請する企業も出てきているようである。

情報セキュリティ対策の効果

情報セキュリティ対策を積極的に実施することで、高度な対策が求められる業務についても、以前と変わりなく受託できていることは、情報セキュリティ対策実施によるメリットの1つであると考えている。社内の基幹業務の IT 化、情報セキュリティ強化を積極的に進めていなければ、仕事を請けるための情報セキュリティ対策を後追いで実施せざるを得ない状況に追い込まれていただろう。取引先から情報セキュリティ対策を求められることは、対策を強化する動機にはなるが、同時に負担にもなり得る。そのため、進められる取り組みは、少しずつ進めておくことが望ましいと考えている。これまでも、当社では、「情報セキュリティ 5 カ条」を活用した社内への普及啓発を実施し、その上で、「SECURITY ACTION」についても宣言済である。普段から対策を進めておくことで、負担感を少なく情報セキュリティ対策を強化でき、取引先からの安心を獲得することにもつながると考えている。

対策・投資多

「業務フローを整理し、リスクを排除することで対策コストを削減」

▼会社概要

所在地	北海道
従業員数	6～20 名
業種	製造業
実施している対策	● 業務フローを整理し、インターネット接続端末を限定。 ● インターネット接続端末と非接続端末で異なるリスクを意識し対策。

情報セキュリティ対策の取組

当社は北海道で容器や各種部品を製造している製造業を営んでいる。現状、相対取引が多いが、近年は卸売の比率も高まってきている。

当社を取り巻く業界環境としては、IT 化が遅れており、受発注はメールや FAX によるものが多い。物流企業が運用している集荷・配送システム等を活用することはあるが、取引先から受発注システムの利用を求められたケースや、それに付随して情報セキュリティの水準等について求められた経験は現在のところない。

当社において PC 等の IT 端末を利用する用途としては、電子メール、Web 閲覧、デザイン作業、表計算ツールを使った在庫管理、経費管理、出荷管理等がある。当社では、用途によって異なる PC を利用している。メールや Web 閲覧を行う端末はインターネット接続しているが、その他の端末はインターネットに接続せず、単独で動作する環境で利用している。こうすることで、情報セキュリティ対策が特に必要な端末を絞り込み、全社的に必要となる対策のコストを下げている。

当社のように、IT 化が進んでいない業界においても、情報セキュリティ対策自体は必要であると考えている。しかし、当社の規模・業界において、本当にネットワーク接続が必要な端末は限られていると考えており、すべての端末を等しくネットワーク接続し、同等の情報セキュリティ対策ソフトウェアを導入したり、メンテナンスを行ったりする必要まではないと考えている。

インターネットや外部メディアと接続させていない端末は外部から攻撃を受けるリスクは基本的に考えなくてよく、データのバックアップ等に力点を置いた対策を行えばよいと考えている。一方で、インターネット接続されている端末を業務利用しなければならないのは、経営者等の外部とのコミュニケーションが発生するメンバーに対してであり、利用方法も含めて相当の注意を払って運用している。

情報セキュリティ対策の効果

従業員のセキュリティ意識が高まるように周知を行ってきたことで、本当に必要となる情報セキュリティ対策を、従業員と相談の上、取捨選択できるようになったことは、良い効果であったと考えている。

情報セキュリティについて意識の低い企業、経営者も少なくないが、端末がインターネットに接続されている以上、相当程度セキュリティ対策を行わなければ、非常にハイリスクであることを認識すべきと考えている。その上で、業務フローを整理の上、本当にインターネットに接続しておく必要がある端末と、そうでない端末をしっかり検討し、インターネット接続が必要な端末に重点を置いた情報セキュリティ対策を行うことで、小規模企業であっても、一定の対策を実施することにつながるのではないか。

取引先要請多

「SECURITY ACTION をきっかけに危機意識を持ち、認証取得へ」

▼会社概要

所在地	愛知県
従業員数	5 名以下
業種	製造業
実施している対策	● 公的支援を活用して情報セキュリティ対策に取り組む ● 委託先に対して監査協力やインシデント対応を規定したガイドラインを用意し、対策実施を要請

情報セキュリティ対策の取組

当社は愛知県で印刷・印刷関連業を営んでいる。取引先は、個人から企業まで多岐にわたっている。

数年前、「SECURITY ACTION」を宣言するにあたって情報セキュリティ対策について学んだ際に、当時の対策では不足しているのではないかという危機感を覚え、より強固な対策を実施したいと考えるに至った。しかし、高度な専門知識を有する従業員がいないため、実際の取り組みには至っていなかった。その後、関連会社にて IPA が実施する「中小企業の情報セキュリティマネジメント指導業務」を活用してＰマークの取得を取り組むことになり、当社も一緒に Ｐ マークを取得することとした。この時は、情報セキュリティ対策を専門とする大学の先生を紹介いただき、助言・監督していただけたため、無事 Ｐ マークの取得に至った。取得までには約半年の期間を要したと記憶している。

Ｐ マークを取得したことで、会社全体での情報セキュリティ対策に関する意識が高まった。個々人や各部署がこれまでの状況を見直すことで、対策状況がさらに高まり、結果として今の状況がある。最近の取り組みとしては、PC の OS をすべて最新のバージョンに更新したことや、セキュリティレベルを高める観点から、クラウドソフトウェアの導入を実施している。

現時点では、ISMS の取得までは考えていない。当社の業務内容や会社規模を考えると、総合的な情報管理に関する認証や、情報セキュリティ対策は不要であると判断したためである。会社規模に応じた適切な情報セキュリティ対策を今後も実施していくことが重要と考えている。

当社から業務委託を行う際は、秘密保持だけでなく、監査協力の依頼や、インシデントが発生した際の対応等を規定したガイドラインを用意し、対策実施の要請を行っている。

情報セキュリティ対策については、「他社の 1 歩先を行く」ことができるように心がけている。顧客から多くの個人情報等を預かるため、情報セキュリティ対策を積極的に実施し、対策に自信を持てている状況を作ることで、他社に対する優位性を確保できると考えているためである。

情報セキュリティ対策の効果

特に、ここ2～3年で情報セキュリティ対策の実施状況について、顧客から問い合わせを受けることが増えている。問い合わせを受ける際、やはり緊張することも多いが、Ｐマーク取得に端を発した情報セキュリティ対策を徹底していることにより、顧客からの問い合わせには問題なく対応できている。情報セキュリティ対策の実施が、顧客の信頼を勝ち取ることにつながっており、実際の契約獲得にも一役買っている。こうした点は、対策を推進してきたことによるメリットであると考えている。

取引先要請多

「情報セキュリティ対策の実施状況を確認して業務委託先を選定」

▼会社概要

所在地	神奈川県
従業員数	51～100 名
業種	製造業
実施している対策	● 従業員の意識向上に特に力を入れた対策の実施。 ● 委託先への現地確認を行い、情報管理体制を確認。

情報セキュリティ対策の取組

当社は神奈川県で印刷･印刷関連業を営んでいる。取引先は、民間企業だけでなく、行政系の事業もあり多岐にわたっている。

情報セキュリティ対策を強化する必要性を感じたきっかけとしては、顧客の機微な情報を扱う機会が多いことがあげられる。公開されていない事前情報を受け取り、公開日までに印刷する業務もあることから、情報管理の重要性は非常に高いと認識している。そのため、総合的に情報管理の対策を行う必要があるとの考えのもと、ISMS を取得した。認証取得や維持にあたっては、従業員への情報セキュリティ教育に力を入れている。積極的に従業員へメッセージを発信していかないと、セキュリティ意識が薄れていってしまうことを危惧するためである。実務において、顧客によって求められる対策のレベルが異なるため、従業員間でもセキュリティ意識に差が生じている。たとえば、個人情報を取り扱う機会の多い営業担当と、そうではない営業担当との間に、セキュリティ意識の違いがあるようなイメージである。当社としては、全社的なセキュリティ意識の引き上げが必要と感じている。

最近では、大手企業から情報セキュリティ対策の実施状況について、チェックシートが送付され、確認を受ける機会が多い。チェックシートは各社独自に項目を設けて送られてくるため、細かく質問してくる会社もあれば、大まかに把握できればよいというスタンスでチェックしてくる会社もある。

当社から業務委託を行う協力会社への情報セキュリティ対策の重要性の周知や要請も重視している。業務委託の際は、付き合いの長さや品質の良さといった観点に加え、実際に協力会社に出向いて、部外者が入れない環境となっているかどうか、守秘義務を守れるような環境となっているかどうか、認証の取得状況、情報資産の取り扱い方法、といった点について確認した上で、業務委託するかどうかを判断している。

また、直近では、コロナ禍の影響で、リモートで仕事をしなければならなかったこともあり、テレワーク用の端末の購入や VPN を導入し、職場の外から社内のデータにアクセスができるような環境の構築も行っている。

情報セキュリティ対策の効果

取引先からの情報セキュリティ上の要請は増加傾向にあり、取引前に対策実施状況の確認依頼について、年間数 10 件程度対応するようになっている。情報セキュリティ対策を徹底していることで、取引先からのチェックに自信をもって回答でき、顧客に安心して付き合ってもらえていることは対策実施のメリットと考えている。

情報セキュリティは人が守るものであるため、今後も従業員一人一人のセキュリティ教育を継続していきたいと考えている。

被害有

「工場の操業を止めないためにも、全員がセキュリティ意識を！」

▼会社概要

所在地	滋賀県
従業員数	101～300 名
業種	製造業
実施している対策	● 情報セキュリティルールや体制、ライセンス契約を関連会社で共有 ● IPA の説明資料や動画等も活用して従業員への注意喚起を実施。

情報セキュリティ対策の取組

当社は滋賀県で製造業を営んでいる。数年前、関連会社においてコンピュータウイルスにより工場全体が操業を停止するという事故があったことや、技術流出事案があったこと等を契機として、取り組み強化に対する機運が高まった。

当社の情報セキュリティに関する各種ルールや体制は、関連会社で共有しているものに準ずるものとなっている。セキュリティソフトウェアやツールは、関連会社で一括してライセンス契約を結び、各社はユーザ数に応じたコストを負担している。セキュリティポリシーについて、近年の取り組みの中で「性善説」に基づいていたポリシーから、徐々に事故や情報流出は身近に起こり得るということを前提とした内容に変化してきている。

最近の取り組みとしては、まず各製造ラインにセキュリティ担当者（兼務者）を配置し、製造ラインごとのリーダーを経由して、ルールの理解と遵守、意識啓発等を行っている。当社は製造部門が相対的に大きいため、安全管理や品質管理の観点から、他の業種にくらべると現場の指揮命令系統がしっかりしており、製造ラインのリーダーの権限と責任が大きい。そのため、こうしたリーダーにセキュリティ対策の重要性を理解してもらえれば、従業員全員に注意喚起が行き渡る傾向がある。各製造ラインで任命されたセキュリティ担当者向けには、半年に 1 回程度は集合してもらい、注意喚起を行っている。たとえば、標的型攻撃対策について、事前に注意喚起に係る資料を配布した上で、事例等も交えて丁寧に説明するようにしている。その際、IPA から分かりやすい説明資料や動画等も提供されているので、こうしたツールも活用している。また全社に対して、関連会社から提供されるセキュリティ情報等の発信を定期的に行っている。

情報セキュリティ対策の効果

標的型攻撃の脅威には当社もさらされている。先日も取引先を発信者と偽装したメールを受信したが、日頃の注意喚起の甲斐もあって、従業員が不用意に添付ファイルを開くこともなく、被害を未然に防げている。当社は製造工場を持っており、情報システムが被害を受け、操業が停止するといったことが最大のリスクであり、それを防げていることが最大の効果である。また、継続的な注意喚起の成果として、従業員は異常があれば、LAN ケーブルを抜く等、ネットワークから PC を遮断する初動対応はできるようになっている。システム担当者は全体で 6 名いるものの、工場はシフトを組んで 24 時間、土日も稼働するため、初動対応を従業員ができるようになることはとても重要なことであると考えている。

情報システムや情報セキュリティ担当者といった IT 人材の強化も大事ではあるが、同時に現場従業員全体のセキュリティ意識向上も重要であり、両者をバランスよく進めていく必要がある。情報セキュリティはどうしても技術的な用語や対応があるため、従業員の誰もが理解できるよう、上手に伝えていくことが重要であると考えている。

取引先要請多

「情報セキュリティに関する説明責任を果たせる体制を構築」

▼会社概要

所在地	岡山県
従業員数	101～300 名以下
業種	製造業
実施している対策	● 個人情報を取り扱う業務を行う施設を限定し、厳しい対策を実施。 ● アップデート等の手順書を配布し、確実に実施するよう工夫。

情報セキュリティ対策の取組

当社は岡山県で印刷・印刷関連業を営んでいる。印刷業務の受託では、個人情報を含む印刷物を取り扱う場合もあるため、P マークを取得している。情報セキュリティ以外では ISO9001 や業界独自の認証についても取得している。

情報セキュリティ対策の取組としては、個人情報を扱う印刷拠点を限定し、業務プロセスを分けて営業を行っている。個人情報の取り扱いや印刷を行う工場では、特に厳しい対策を実施している。具体的には、個人情報がその拠点内に閉じるように、社内のネットワークとは別のネットワークに切り分けるほか、防犯カメラの設置、データの暗号化、静脈認証、アクセスログの取得、監視カメラの設置等を実施している。

社内と社外とのネットワークの通信はファイアウォールでチェックするほか、個人情報を扱う施設は、ルータでアクセス制限、セキュリティソフトウェアも導入し、社内で運用している。また、Windows Update やセキュリティソフトウェアのサポート期間のアップデートは、従業員に手順書を渡して、従業員の協力のもと進めている。社内で手順書を作成することで、現場の従業員が理解しやすいように工夫している。

このほか、同業他社に会社に関わる業務における情報漏えい等の事件が起こるたび、社内で検証を行い、同じような事案が発生しないか検証し、適切に対応できることを確認している。検証した結果は、営業先で説明できるようにしておき、顧客から信頼を得るようにしている。

印刷業務の受託に際しては、顧客からの要望に基づき、当社の環境が整っていること（他の顧客の個人情報の扱いがない状態であること）を条件に、監査を受け入れることになっている。監査が無くても、チェックシートによる実施状況の確認依頼を受けることがある。各社からのチェック内容をみると、たとえば、作業現場にスマートウォッチを持ち込んでいないか等、現代的な条件を踏まえた監査内容が含まれている。また、同業者による監査は印刷業界をよく知っていることから、社内の個人情報・機密情報の取り扱いに関するチェックは厳しい。加えて、再委託を受ける場合には、エンドユーザや発注者に被害出た場合には、被害額を補償する旨、契約書でも記載がある場合もある。機微な情報を扱っていることから、契約における要求が多い。

こうした要求は、年々厳しくなっている印象であるが、顧客・エンドユーザの利益になることであるため、経営者もセキュリティ対策について関心を持っており、スピーディに対応している。

情報セキュリティ対策の効果

セキュリティ対策は直接的に売上につながらず、費用対効果が見えない中で経営判断がしにくい活動かもしれない。しかし、当社は個人情報を扱うことが多いことから、P マークを取得し、これに基づき個人情報を取り扱うことは、顧客からの信頼の獲得につながっていると感じる。

「業界ガイドラインに準拠しつつ、社内人材の育成を実施」

▼会社概要

所在地	広島県
従業員数	101～300 名以下
業種	製造業
実施している対策	● 各部署からメンバーが参加する情報セキュリティ委員会を設置し、対策の検討･実施を行う。

情報セキュリティ対策の取組

当社は広島県で自動車関連製品を製造する製造業を営んでいる。

自動車業界では、業界全体としてサプライチェーンの中で情報セキュリティ対策を進めていくという考えから、日本自動車工業会が「自動車産業サイバーセキュリティガイドライン」（以下「業界ガイドライン」）を策定している。2020 年 3 月の公表後、発注元の各社から業界ガイドラインに基づいたサイバーセキュリティ対策を進めるようにと指示があった。業界ガイドラインの要求項目は水準が高く、かつ広範である。当面は幅広く対応して、徐々に水準を高めていきたいと考えている。業界ガイドライン自体は ISO27001 に準じていると考えており、ISO9001、ISO14001 の監査に取り込んでいき、一緒にチェックしていくことを想定している。

当社では、業界ガイドラインが策定される前から情報セキュリティ対策を進めてきた。情報セキュリティ専門の担当を複数名配置して、各拠点にて情報セキュリティ対策を進めているほか、各部署からメンバーが参加する情報セキュリティ委員会を設置し、同委員会が全社の取り組みを統括している。こうした場から、社内の次世代の情報セキュリティ人材が育つことを期待している。また、情報セキュリティ投資の用途としては、セキュリティ関連ソフトウェアに加えて、研修費用等に用いている。IPA をはじめ情報セキュリティに関する啓発活動を行う公的団体の発信情報（情報セキュリティの理解度チェックや規定のひな形）等も活用している。また、発注元からの指導によっても情報セキュリティ対策が強化されている。具体的には、発注元から情報セキュリティに関するアンケートがあり、フィードバックを受けることになっている。

情報セキュリティ対策の効果

「技術」はなかなか紙に落とせないこともあり、必ずしも情報セキュリティについて意識が高いかというとそうでもなかったと思われる。しかし、従業員から見ると特筆すべき情報でなかったとしても、社外からみると貴重な情報であることもある。情報セキュリティ対策を進めることによって、自社の情報に対する意識が高まったと考えている。

社外との取引上の効果は、取引上の交渉や新たな顧客の獲得にあると考えている。取引上の交渉については、定期的に値下げ要請に直面するが、値下げを許容できない時には、相当の理由が必要となる。取引先やガイドラインに基づいた情報セキュリティ対策の要請や水準を満たすためのコスト増加であることは、ひとつの説得材料になる。また、顧客の獲得については、自動車業界は 100 年に 1 度の転換期ともいわれている。今後は、電気自動車が増加していくことで、電機メーカーや情報関連産業も自動車業界に参入してくるかもしれない。これらの企業では情報セキュリティ基準は高いと目される。そういった意味では、情報セキュリティ対策を進めることは新しい市場に展開する上でも必要だと認識している。

被害有

「小規模な製造業でも社内の技術情報・機密情報管理は大切」

▼会社概要

所在地	徳島県
従業員数	5 名以下
業種	製造業
実施している対策	● 当社のサーバから情報が漏えいする被害を受けたことを踏まえ、開発に関わる技術情報等の重要情報をスタンドアローン環境で管理。

情報セキュリティ対策の取組

当社は徳島県で製造業を営んでいる。以前は別の地域で事業を展開していたが、現事業への転換を図るため、従業員数を縮小して現在に至っている。現在は従業員が少ないことから、情報セキュリティ対策は経営者が自ら対応している。

当社では過去に内部不正による情報漏えいが疑われる事案があった。当時は日本人従業員だけではなく、外国人従業員も複数名雇用し、海外市場をにらんだ製品の開発に取り組んでいた。しかし、当該製品は安全対策等がなかなか進まず、結果的に開発を途中で断念し、当社の事業自体を縮小することになった。また、事業縮小にともない、研究開発や当時の情報セキュリティ担当であった従業員にも退職してもらった。なお、当社は情報セキュリティについては、当時から社内規定を整備し、それに基づいて運営していた。

その後、従業員の退職後に、経営者がサーバの移管をしたところ、事業の縮小時期から退職後にわたって、当社のサーバに大量のアクセスログが発覚した。サーバには、経理情報等の経営に関わる情報、技術に関する情報等、会社にとって重要な情報を格納しており、それらのデータがダウンロードされていた。調べてみると、退職した従業員によるアクセスであることが明らかになった。当社の情報はダウンロードされてしまったものの、顧客や外部委託先への影響はみられなかったことは不幸中の幸いであった。

現在は、少人数で経営していることや、特許出願にあたっての技術開発等機微な情報も有していることから、Web サイトを除くと、サーバ等にファイルを保存せず、技術情報等をローカルや外付けハードディスクに保持し、経理情報もローカルなソフトウェアで管理する等、スタンドアローン環境での情報管理を中心に経営している。

現在は、国や自治体の補助金も得て、新しい事業の可能性もみえてきており、今後は従業員を増強するとともに、工場等も設置する必要がある。従業員が増えると、IT 環境への投資も必要となってくると考えており、たとえば、サーバを改めて準備する必要がある。その際には、改めて情報セキュリティ対策のレベルを引き上げていく必要がある。

情報セキュリティ対策の効果

事業がうまくいっている間は、従業員も前向きに事業に協力してくれるため、トラブルになりにくい。一方で、事業が縮小していく時には、従業員も不満を持ってしまい、その結果、トラブルを引き起こすことになると考えられる。

事業は必ずしも常に上り調子になるとは限らない。下り調子の時には、トラブルがより大きくなる可能性があるため、その観点からも情報セキュリティは、積極的に取り組む意義があると感じている。

対策･投資多

「継続的に取り組むことが、一番効率的！」

▼会社概要

所在地	沖縄県
従業員数	51～100 名以下
業種	製造業
実施している対策	● 情報セキュリティ対策のルール等は関連会社全体で作成して共有。 ● PCにできるだけデータを残さないよう、シンクライアントの導入を実施。

情報セキュリティ対策の取組

当社は沖縄県で製造業を営んでいる。当社の関連会社で情報漏えい事故があったことや、個人情報保護法の改正等をきっかけとして情報セキュリティ対策の強化に取り組んでいる。

情報セキュリティ対策のルール等は、関連会社全体で作成し、共有している。当社は当該ルールに従いつつ、必要な情報セキュリティ対策投資を定期的に行っている。セキュリティソフトウェア等は、関連会社で一括購入し、各社がユーザ数分のコストを負担する形で対応している。当社の規模だと、情報セキュリティ対策システムを独自に導入するか迷う所であるが、現状では自社単独では対策の難しい部分もあると考えており、関連会社間で補完しながら対応している。

情報セキュリティ担当者は実質的に兼務者が 1 名となっている。会社の規模を考えるともう 1 名位は配置できた方が良いと思うが、直接の部下にも手伝ってもらいつつ、関連会社のセキュリティ部門にも相談したり、サポートを受けたりすることができる体制で実施しており、今のところ対応できている状態である。

その他、具体的な対応の例としては、従業員が使用する PC には、データを残さないようにするシンクライアントシステムの導入、といった取り組みも行っている。また、情報管理という観点から秘密情報の区分を行い、区分に応じたアクセス制限を設定するといった基本的な対応は実施している。

情報セキュリティ教育は、e-ラーニング、OJT、外部セミナー活用等を活用している他、関連会社から動画教材等を提供してもらっている。

中小企業においては、人材が限られていることもあり、どうしても IT や情報セキュリティに土地勘のある従業員がいると担当を任されてしまうという傾向があるが、当人のキャリアという観点からも、会社のリスク分散という観点からも、他の従業員にも経験を積んでもらって、対応できる人材を育成することも大事だと考えている。

情報セキュリティ対策の効果

対策の最大のメリットは、取引先に迷惑をかけないという点であり、当社が取引上信頼してもらえることが大事である。

対策には費用が掛かるが、継続的な取り組みを行っているからこそ、情報セキュリティ担当を兼務者 1 名体制としても対応できており、そうでなければ事故対応や復旧等も考えると大幅に増員しなければならなくなるだろう。シンクライアント導入の際も、導入コストは高額となったが、会社全体の情報セキュリティレベルが向上したことで、結果としてコストダウンにつながったと考えている。また、コロナ禍でテレワークが進んだが、これも情報セキュリティ対策を行ってきた基盤があったからこそ、スムーズに移行できたものと理解している。今後の可能性として、得意先からの IT 化、情報セキュリティ対策強化の要請は増えると考えており、継続的に取り組んでいくことが大事だと考えている。

被害有

「専門職がいないからこそ、しっかりと情報セキュリティ投資を」

▼会社概要

所在地	滋賀県
従業員数	21～50 名
業種	電気･ガス･熱供給･水道業
実施している対策	● ネットワークのセキュリティ対策を強化する目的で、UTM を導入。

情報セキュリティ対策の取組

当社は滋賀県でインフラ関係の事業を営んでいる。主な仕入先は、大手の事業者であるが、当該事業者との取引に際しては、基本的に事業者から指定されたシステムを使っており、システム更新も事業者からの提供で実施されている状況である。そのため、仕入先側からは、情報セキュリティに関する強い要請が来ることはそれほどない。

一方で、当社の事業は個人を含めて様々な顧客を抱えている関係上、自社が保有する顧客情報の管理には非常に気を使っており、顧客情報が漏えいするリスクを大きく捉えている。経営者も情報セキュリティへの投資に対しては前向きであり、担当者から導入を提案すれば対策を講じることのできる環境である。たとえば、ネットワークの情報セキュリティ対策を強化する目的で、UTM（Unified Threat Management）を導入している。UTMについては、導入したままということではなく、最新の機器に入れ替える等、情報セキュリティ強化に向けて常に留意している。UTM の入れ替えは、当社が情報セキュリティインシデントに遭遇したことにも起因している。メールを感染経路とするエモテットが猛威を振るった時期に、従業員の端末が感染したことがあった。その時は、すぐに端末を隔離し、日頃やり取りをすることのある外部者へ電話で注意喚起すると同時に、内部でも拡散状況を調査した。幸い、外部･内部ともに拡散は確認されず、最小限の被害で抑えることができた。後で確認すると、UTM で検知していたようではあるが、通過してしまったようである。こうしたこともあり、最新の UTM 導入や、情報セキュリティ投資への意識が一層高まった。

当社には IT 専門職が配置されているわけではなく、基本的に他業務を担当するものが情報セキュリティ業務を兼務している状態である。情報セキュリティに精通しているわけではないという意識があるので、だからこそ情報セキュリティにはしっかり投資しておこうという発想になっている。また、社内で怪しいメールを確認した際には、担当者が従業員に対して注意喚起の周知を行っている。

情報セキュリティ対策の効果

UTM を導入してからは、たとえば怪しい Web サイトにはアクセスできないようになったり、また迷惑メールが届きにくくなったりしてきている。実際のところの効果はわからないが、少なくとも従業員がそうしたリスクを抱えるものに接する機会が減っているということであるので、会社全体としては情報セキュリティに関するリスクの低減につながっていると感じている。

また、少しずつではあるが、従業員の意識向上にもつながってきていると考えている。怪しいメールを見つけた際に従業員へ周知する等の活動を通じて、少なからず情報リテラシーは高まってきている。ただ、従業員に対する研修等の取り組みにはまだ十分に着手できていないので、今後は実施することによって、一層の意識向上を図っていきたいと考えている。

「いくら投資を行ったとしても最後は従業員教育が重要」

▼会社概要

所在地	宮城県
従業員数	6～20 名
業種	鉱業･採石業･砂利採取業
実施している対策	● 関連会社と連携して各種対策や有事の対応を実施。 ● セキュリティ意識向上を最大の課題としてとらえ従業員教育を実施。

情報セキュリティ対策の取組

当社は宮城県で鉱業･採石業･砂利採取業を営んでいる。

情報セキュリティ対策に取り組むようになったきっかけとしては、関連会社からの要請があったことが大きい。当社は関連会社の担当者と連携し、各種対策に取り組んでおり、有事の際の対応･報告についても、関連会社へ速やかに報告の上、連携して対処する方針をとっている。

実施している具体的な対策としては、Web サイトへのアクセス制限や、情報端末の持ち出し管理、データのバックアップといった基本的な対策を実施している。また、関連会社からの支援も受けていることもあり、セキュリティ監視サービスの活用や、外部の IT 関連企業が提供するぜい弱性診断ツールも活用等の高度な対策も実施している。加えて、関連会社が定期的に実施する監査を受ける必要があり、ここで大きな問題となるような事象がないよう、気を引き締めて取り組んでいる。監査の実施は、当社の情報セキュリティ対策への意識を高めるきっかけになっている。

関連会社からのサポートもあり充実した対策をとれていると思うものの、従業員へのセキュリティ教育については、今後課題になってくると感じている。関連会社から求められる対策の実施にあたり、一定の支援は得られる環境にあるため、技術的な対策については、大きな心配はしていないものの、従業員への意識向上は、関連会社からの支援があったからといって実現する話ではない。そのため当社の IT やセキュリティを担当する従業員が主導して、積極的に情報共有や周知･徹底を行っていくことが必要、との意識を持って取り組んでいる。従業員への教育に当たって用いる教材の中には、IPA が提供するコンテンツも含まれている。

取引先との間での情報セキュリティ対策の要請について、関連会社からの要請は、ここ数年で強化されている傾向にあり、今後もその傾向は続いていく、と考えている。

一方、当社から委託先への情報セキュリティ対策の要請については、現時点は十分にできてはおらず、今後の課題であると考えている。

情報セキュリティ対策の効果

これまで実施してきた対策は、自社が主導した対策は少なかったこともあり、対策の実施により感じられたメリットは、あまりない状況である。しかし、しっかりと対策をしていることで、当社や関連会社が一定の安心感を得ることができているのではないかと考えている。

今後も、関連会社からの要請に対処し、連携しながら対応すれば問題ない環境であると考えているものの、セキュリティ対策は高度化していることから、日々の情報収集がより重要となってくるのではないかと考えている。

対策･投資多　取引先要請多

「認証を取得することで取引先とスムーズに基本契約を締結」

▼会社概要

所在地	宮城県
従業員数	21～50 名以下
業種	情報通信業
実施している対策	● 取引先との契約締結をスムーズにするための認証取得を実施。 ● 委託先へもとめるセキュリティ対策のガイドライン作成。

情報セキュリティ対策の取組

当社は宮城県でソフトウェアやハードウェアの導入、その他サービスを提供する情報通信業を営んでいる。取引先は、IT ベンダや公的機関等も含まれている。

サーバへの攻撃や不具合によって事業運営がストップするリスクや、取引先に提供したシステム等がセキュリティホールとなって取引先に被害が生じるといった事態が発生しないように情報セキュリティ対策に取り組んでいる。現在のところ、当社が直接被害を受けた事例や、当社が提供したシステム等が原因となって取引先が被害を被ったという事例はない。

当社は自社サーバにデータを置いて VPN で接続する方式を採っていたが、テレワークを進める中でサーバのメンテナンス要員を常駐させにくくなったこともあり、クラウドサーバを全面的に活用にすることとした。また、当社は P マークを取得していたが、このタイミングで ISMS 取得へと移行を行った。こうした対応も含め、毎年一定額の情報セキュリティ投資を行っている。こうした取り組みにより、テレワーク実施に伴い求められる対応も概ね完了させることができた。情報セキュリティ体制については、横断組織、ワーキンググループ方式で対応しており、ISMS 取得に関連した対応も横断組織で対応している。従業員の育成やリテラシー向上は継続的に必要であると考えており、次世代の人材育成が目下の課題である。

取引先からは再委託先に対しても同水準の情報セキュリティ対策を求められるため、再委託先に対してもガイドラインを作成している。何をもって同水準と呼ぶかについては個々に判断しているが、たとえばパスワードの設定やメール等の誤送信に対する注意喚起を行う等、再委託先にも一定の啓発･要請は行っている。

情報セキュリティ対策の効果

P マークから ISMS への移行に際しては、規程の見直し、社内教育の実施等が必要とはなったが、マネジメントシステムという意味では P マークを取得していたこともあり、その仕組みを承継することで比較的スムーズに移行することができた。P マークと ISMS の双方を取得することも検討されたが、双方を維持することはコスト的に負担であると同時に、ISMS を取得すれば P マークを維持しなくても事業上は不利益が生じないと判断し、ISMS のみ維持している。

継続的な情報セキュリティ対策の実施、P マークの取得、また近年の ISMS の取得によって、機会損失は大幅に少なくなったと実感している。新規の取引先との商談においても、スムーズに基本契約の締結ができている。

特に、IT ベンダ等と取引をする場合には、最初の基本契約締結に際して満たすべき要件のハードルが高い。1 つでも要件不備があると、「不適合あり」ということで是正を求められ、対応や報告に膨大な労力を要する傾向があるため、最初から高い水準の認証を取っておくことの意義は大きいと感じている。

対策･投資多

「個人情報を取り扱う企業として対策を実施することは当然」

▼会社概要

所在地	埼玉県
従業員数	6～20 名
業種	情報通信業
実施している対策	● 東日本大震災をうけてクラウド活用と情報セキュリティ対策の強化を実施。 ● IT 導入補助金支援事業者として、説得力のある説明ができるようにするため、SECURITY ACTIONを宣言。

情報セキュリティ対策の取組

当社は埼玉県でソフトウェア開発等をおこなう情報通信業を営んでいる。

当社の情報セキュリティ対策については、2 つのターニングポイントが存在する。

1 点目は、ソフトウェアのクラウド化である。当社は自社にサーバを設置してデータを管理していたが、東日本大震災以降、クラウド化の方が安心だということになり、顧客からの要請もあって、クラウド化を行った。顧客からは個人情報を預かっており、クラウドからのデータ流出は確実に避けなければならないと考え、情報セキュリティ対策を強化した。

2 点目は、IT 導入補助金の支援事業者に認定されたことである。IT 導入補助金には SECURITY ACTION の宣言が申請要件となっている。支援事業者が宣言をする必要はないものの、説明や宣言の相談を受けるためには、自社でもやってみるのが最も良いだろうという話になり、の宣言を行った。自己宣言であり、第三者認証と異なり、手間や費用がかからないこともあり、社内でも宣言に対しては前向きであった。

具体的な取り組みとしては、各端末へのセキュリティソフトウェアの導入、ファイル転送サービスの利用等である。また、クラウド環境へのアクセスについては、ID とパスワードでの管理に加え、アクセスできる端末を制限し、万が一 ID とパスワードが流出した場合も、顧客の情報にはアクセスできないような対策を取っている。

現在、P マークや ISMS 取得を検討しているものの、当社のような小さい企業にとってはやや負荷が大きいとも感じており、まずは着実に情報セキュリティ対策を高めることを目標として取り組んでいきたいと考えている。

情報セキュリティ対策の効果

業界全体として、IT 化が遅れている。そのため、クラウドを活用した当社のソフトウェアは、同業他社にはあまり例がなく、当社が先行している状況であり、差異化が実現できている。もちろん、クラウドのセキュリティ対策について、クライアントから問われることもあるが、しっかり説明をすることで理解が得られており、結果として信頼関係の構築･顧客の獲得に繋がっている。

個人情報を扱う企業であれば、対策は必要不可欠な時代である。当社のような小さい企業では、情報漏えいが廃業に直結する恐れもあり、確実に対策を行う必要がある。事業を着実に継続していくためにも、情報セキュリティ対策は不可欠だと考えている。

対策･投資多

「情報セキュリティ対策コストは、適切かつ必要なコスト」

▼会社概要

所在地	東京都
従業員数	51～100 名以下
業種	情報通信業
実施している対策	● 情報セキュリティに係るリスクを特定の上、従業員教育と PC のセキュリティを重視して対策を実施。

情報セキュリティ対策の取組

当社は東京都でデジタルツールを提供する情報通信業を営んでいる。本社は海外にあり、諸外国に拠点を有している。日本支社では、国内企業を主たる顧客として事業を展開している。原則として日本支社単独の対策ではなく、グローバル全体で一体的な情報セキュリティ対策を実施しており、日本事務所に在籍するセキュリティ担当者も、グローバルのセキュリティチームに属し業務を行っている。近年、社会一般や顧客企業における情報セキュリティに対する意識は高まりつつあるが、国ごとに重視する観点の差こそあれ、情報セキュリティ対策の重要性に対する社内のセキュリティ担当者の認識には大きな差異はない。

情報セキュリティに係るリスクは「人が拾ってくるものであること」、また、「トラブルの原因となるエンドポイントは PC であること」から、当社では従業員教育や PC のセキュリティ対策に力を入れて取り組んでいる。加えて、情報セキュリティに関するリスクは常に変容していくものである。そのため、社内のセキュリティ担当者には日々学ぶことが必要とされるとともに、従業員の知識をアップデートさせていくことが求められる。情報セキュリティ対策は、その時点で知識や高い意識を持ちあわせていれば良いというものではなく、継続して学び続ける必要があると考えている。

また、「契約書は会社を守るためのもの」という考えに基づき、取引先との間における情報管理については、契約書等の中で適切な取り扱いを規定するようにしている。なお、当社の契約書ひな型で対応することが難しい案件では、情報セキュリティ上のトラブル等が生じた場合の賠償責任等を明確化するとともに、リスクを当社が受容できる範囲に特定するようにしている。一方、当社は必要と考える情報セキュリティ対策を実施しているものの、顧客企業が当社既存サービスや当社が必要と認識する以上に高い情報セキュリティ対策を求めてくる場合には、顧客側に費用全額あるいは一部を負担してもらうよう交渉している。

情報セキュリティ対策の効果

一部の業界や海外でビジネスを展開する企業は、マーケティングにおけるエンドユーザ等のプライバシー保護に対し、高い要求水準を求めてくる傾向がある。このように、近年、ビジネスを行う上での要件として、情報セキュリティ対策を取引先に求める企業は増えつつあることから、当社でも顧客企業からの要請を満たすため、様々な取り組みを実施している。

一般論として、一昔前は「情報セキュリティ対策はコスト」という認識もあったが、いまでは情報セキュリティ対策に対するコストは、「適切なコスト、必要なコスト」という認識が広がりつつある。当社でも情報セキュリティ対策の強化の観点から、業務上の運用プロセスの変更等の取り組みを行うことは、会社の利益につながること、また、顧客企業による当社サービスの継続利用に資するものであると考えている。

対策・投資多

「あえて関心の低い従業員を担当者に任命し全社でサポート」

▼会社概要

所在地	東京都
従業員数	21～50 名
業種	情報通信業
実施している対策	● IPA が公開するツールを活用し、委託先へのセキュリティ意識の強化を促す。

情報セキュリティ対策の取組

当社は東京都で情報通信業を営んでいる。事業開始当時の主事業はシステム構築であったが、金融システムのデザインや運用、Web 関連業務へと拡大するにつれて、セキュリティ分野についても関心を持つようになった。

当社ではＰマークがないと仕事が受けられないという事態が出てくるようになり、2000 年代後半にＰマークを取得した。周囲の企業の話を聞いても、P マークの取得に伴い、情報セキュリティ対策を始めるという例が多いようだ。P マーク取得時に苦労した点として、申請書が山のようにあり、通常業務に支障がでてしまうくらいまで紙が増えてしまったことがあげられる。そこで、P マーク取得のタイミングで、社内の申請関係のワークフローを電子申請による方式に変更した。なお、SECURITY ACTION についても数年前に宣言している。

新型コロナウイルス感染拡大以降は、在宅勤務を基本としており、セキュリティレベルの高いクラウド上での情報管理を行っている。前述の通り、できるだけ電子申請等を活用していることや、セキュリティレベルが高いクラウドを使用することで、業務で紙が発生していない。このことは、情報管理上望ましいことと考えている。

取引先との契約時に求められる要請としては、守秘義務と個人情報の適切な取り扱いが大半であり、これまで情報セキュリティ対策の具体的な要請が、契約書にまで盛り込まれたことはない。また、実施している情報セキュリティ対策について説明が求められることは多くはないが、説明が求められた場合には、活用しているクラウドのセキュリティについて説明するようにしている。社内向けの情報セキュリティ対策と連動する形で、自社から委託するパートナー企業に対しても、IPA が提供する「5 分でできる！情報セキュリティ自社診断」を参考として、少しだけ難易度を上げたチェック項目を提示し、意識や対応状況等を確認してもらうよう促すこともある。

情報セキュリティ対策の効果

情報セキュリティ対策を数多く実施していることで、従業員の情報セキュリティへの意識は確実に向上している。「5 分でできる！情報セキュリティ自社診断」の点数も、活用し始めたころとくらべて、従業員による回答の点数は上がっている。従業員の意識向上のための工夫として、P マーク申請時の社内担当者は、当時、情報セキュリティや個人情報について、関心・知識のない従業員にお願いした。関心・知識のない従業員へ頼むことで、その従業員の意識を変革することが狙いである。周囲の従業員も、その従業員が担当することに若干不安を覚え、積極的にサポートを行ってくれたことで、全社的なセキュリティ意識・レベルの向上に大きく寄与したと考えている。

対策･投資多

「不正アクセス被害をきっかけにぜい弱性診断や対策強化を実施」

▼会社概要

所在地	東京都
従業員数	6～20 名
業種	情報通信業
実施している対策	● 性善説では情報セキュリティは成り立たない意識を持った対策実施。 ● 外部事業者を活用した自社サービスのぜい弱性診断の実施。

情報セキュリティ対策の取組

当社は東京都で情報通信業を営んでいる。当社は通信事業者からスピンアウトした会社であり、情報セキュリティについては高い意識は持ってきたつもりだが、当社が開発するサービスに対する不正アクセス被害を経験した。具体的には、クラウド経由でハッキングを受け、データの不正取得をされたもので、実際に金銭的な被害も生じたため被害の届出も行った。

被害を受けた後、外部事業者を活用してぜい弱性診断を行い、しっかりと「穴」を塞ぐ対応を行った。対応には 1 か月程度を要したが、今では、新規の開発を行う際には事前にぜい弱性診断のサービスを活用しており、対策も強化している。

取引先が ISMS を取得しているケースが多く、当社に対しても情報セキュリティに関しての要請がある。そのため、ISMS または P マークの取得を検討している。

また、業界的にはどうしても内部者からの情報漏えいが多いと言われているので、内部マネジメントはしっかり体制を整える必要があると考えている。現在、兼務者 3 名の担当者を置いて対策している。性善説に立った仕組みを作る訳にもいかないため、たとえば、端末の持ち出しを制限するためにセキュリティワイヤーを設置したり、社内の体制整備、取引先の要請への対応を行ったりしている。加えて、当社の体制･仕組みが機能していることを、内部監査や外部監査等を通じてチェックし、改善するといった対応も行っている。

情報セキュリティ対策の効果

外部事業者を活用したぜい弱性診断を行うにはそれなりにコストがかかる。しかし、外部事業者にお墨付きをもらっていることを示せるようになったことで、当社サービスの信頼性は各段に高まったと感じている。

また、外部専門家に診断をしてもらうことを通じて、情報セキュリティレベルが高まるというだけでなく、自社のエンジニアのスキル向上につながっている。エンジニアは自分で設計、プログラミングしたものに自信を持っているが、第三者の指摘によって、よりよい方法があったと気づかされることも多い。当然、外部事業者によるぜい弱性診断の対象となる新規サービス自体の改善にも資するが、当該サービス以外の開発場面にも応用できる視点が多く、エンジニアからもぜい弱性診断を実施して良かったという声や、ぜい弱性診断によってプログラミングやコーディングの質が上がったという声も聞かれる。

ぜい弱性診断とは別に、基幹業務でもクラウド化を進めており、クラウド化を進めるにあたっての情報セキュリティ対策を強化してきた。こうした経緯もあり、コロナ禍にテレワークを増やした際も比較的スムーズに対応することができたことも、日々、情報セキュリティ対策に取り組んだことにより感じられたメリットの1つであると考えている。

対策･投資多

「経営層と現場の目線あわせを行い、必要な対策を実施」

▼会社概要

所在地	岐阜県
従業員数	6～20 名
業種	情報通信業
実施している対策	● 自社の状況･情報セキュリティ対策が甘い部分について、経営層が関心を持つように、会議で問題提起を実施。 ● PDCA を回す際、従業員には責任を追及しないよう留意。

情報セキュリティ対策の取組

当社は岐阜県で情報通信業を営んでいる。情報セキュリティには日頃から関心を持っており、ISMS とＰマークを取得している。ISMS は、関連会社が取得する際にあわせて取得した。Ｐ マークは、もともと取得しようとしていたのではなく、ISMS を取得する際に、同時に取得した。

情報セキュリティ対策を行うにあたって、現場と経営層の情報セキュリティに対する認識の違いを感じることが多々ある。一般論だが、現場で起きたインシデントをそのまま報告すると、経営層は文字通り「報告」として処理し、新たな対策方法の検討につながらない場合があると言われている。また、経営層は自社内の報告より、センセーショナルな報道等をきっかけとして、危機感を持つことがあり、現場での問題意識とズレが生じる場合があるという指摘も聞かれる。当社の経営層の場合、そうした懸念も少ないが、担当としては自社の状況･情報セキュリティ対策が甘い部分について、経営層が少しでも関心を持つような形で議題に取り上げ、改善策や追加の情報セキュリティ対策に繋げられるよう心がけている。

情報セキュリティ対策をしっかり実施するためには、PDCA をしっかり回すことが必要と考えている。その際、従業員の責任を追及しないような形にすることが重要だと考えている。このように、現場と経営層の目線あわせを行い、折り合いを付けながら情報セキュリティ対策を実施して行くことが重要であると考えている。

従業員に対しても、最新のセキュリティ情報の啓発を行っている。最近で言えば、エモテットの情報をすぐに全社に連絡した。

猶予期間が設けられたものの、2022 年1月から電子帳簿保存法が改正され、電子取引については、証跡を電子データで保存することが今後求められるようになる等、一層のデジタル化が今後進んでいくため、引き続き PDCA を回しながら十分な対策を心がけていきたい。

情報セキュリティ対策の効果

ISMS を取得しているため、機密情報保持に関する内容を契約書上で明文化することができ、実際の契約につなげることができた。

他にも、個人情報保護方針があるかとの問い合わせを受けたこともあるが、HP に掲載しており、顧客の信頼を得られた経験もある。

さらに、従業員に対しての情報セキュリティ訓練を数年に 1 回実施しているが、ほとんどの従業員は引っかからない。こちらとしても毎回、手を替え品を替え実施しているが、従業員には見透かされている。特に、担当者が情報セキュリティ対策に厳しいことが従業員の間で周知の事実になっており、新入社員にも気をつけるように情報共有がされているようである。口酸っぱく注意してきたことで、従業員の意識が高い状態で保たれていると考えている。

取引先要請多

「情報セキュリティ対策実施、認証取得、信頼獲得の好循環の実現」

▼会社概要

所在地	広島県
従業員数	6～20 名
業種	情報通信業
実施している対策	● 取引先から提供されるチェックシートに基づいた対策実施。 ● 関連会社とタイミングを合わせた認証取得。

情報セキュリティ対策の取組

当社は広島県で情報通信業を営んでいる。取引先は、地方自治体を中心とする官公庁や、その他大手の民間企業である。

当社には関連会社があるものの、社内システムについては、ほとんど関連会社から独立しており、メールサーバ等は別に設けられている。そのため、自社単独での情報セキュリティ対策を実施することが求められる環境にある。また、情報通信サービスの提供にあたっては、顧客のネットワーク環境についてもくわしく把握する必要がある。顧客のネットワーク環境という機微な情報を取り扱うことになるため、情報管理は、当社にとって重要な課題であると認識している。

取引先から求められる情報セキュリティ対策については、5 年ほど前までは、ウイルス対策ソフトウェアの導入有無の確認程度であった。しかし、ここ数年で求められる項目が急増し、要求水準も高まっている。情報セキュリティ対策への意識の高い顧客も増えてきており、顧客側が用意するチェックシートの提供を受け、情報セキュリティ対策の実施状況について確認を受けることがある。「業務で使用する端末に、特定のアプリのインストールがないか」、「USB メモリ等の記憶媒体の持ち出しが発生しない環境であるかどうか」、といった、情報漏えいしない体制が取られているかどうかのチェックである。分量にすると、A4 用紙 5～6 枚程度の内容があり、対応しなければ、取引することはできないかもしれない。

取引先からの要請に対応することで、当社の情報セキュリティ対策が加速した部分もあるが、対応に苦慮したことも当然ある。たとえば、これまで使用してきた自社サービスの動作確認に用いる検証用端末は、取引先からの要請にあわせてセキュリティレベルを高めてしまうと、使うことができなくなってしまう場面もあった。取引先からの要請を受ける形で、各種情報セキュリティ対策に取り組んできた部分も大きかったが、関連会社が ISMS を取得する動きが出てきたこともあり、同時に当社も ISMS を取得する流れとなった。

情報セキュリティ対策の効果

積極的に情報セキュリティ対策に取り組んでいたことで、顧客の信頼を得るために役立つ認証取得に係る労力をそこまで感じなかったことが、メリットとしてあげられる。ISMS の取得に手間取る企業も多いと聞いていたが、それまでも情報管理には積極的に取り組んできたこともあり、認証取得にあたって、大きな苦労があったとは感じなかった。大きな苦労を感じず、顧客の信頼獲得に役立つ認証を取得できたことは、過去に取り組んできた対策が役立った結果であると考えている。また、認証を取得していなければ、取引が実現しなかったかもしれない。認証取得の重要性や、情報管理の重要性について、従業員に理解してもらえたことは、大きなメリットであったと考えている。

対策･投資多

「外部サービスを活用することで従業員の負担を軽減」

▼会社概要

所在地	佐賀県
従業員数	6～20 名
業種	情報通信業
実施している対策	● 物理的な管理や、アクセス制御等を中心とした対策の実施。 ● USB メモリ等による持ち出し管理や、通信インフラの制御機器等がある区域への立ち入り制限も実施。

情報セキュリティ対策の取組

当社は佐賀県で情報通信業を営んでいる。取引先は、個人と法人の双方にいる。

当社では川上の取引先及び川下の企業からデータを預かったり、独自にデータを取得したりすることはほとんどない。管理が必要な情報という意味では、顧客情報がメインとなる。情報セキュリティという意味では、情報漏えいだけでなく、通信環境自体の安全･安定を確保する必要はあり、必要な対応は行っている。

顧客情報管理やインフラのセキュリティについては、専門事業者に委託をしている。当社が独自に実施している情報セキュリティ対策としては、物理的な管理や、アクセス制御等が中心である。情報漏えい対策として、USB メモリ等による持ち出し管理や、制御機器等がある区域への立ち入り制限を行っている。アクセス制御については一般的な話ではあるが、情報区分に応じてパスワードの設定、ファイルへのアクセス制限等を行っている。また、当社従業員が端末で閲覧･編集を行う際には VPN 回線を用いている。

現在、システムや情報セキュリティを担っている従業員は 3 名であり、2 名がハード面の担当、1 名が情報セキュリティやその他ソフト面を担当する体制である。当社の事業内容に照らして、3 名で対応できているのは、外部委託を活用しているためであり、すべて自前で対応しようと思えば、大きな負担となる上、人材を確保出来ない。

従業員に対して注意喚起等は行っているが、従業員全員の情報セキュリティや IT リテラシーレベルを高めていくのは容易なことではない。メールのやり取りをする際に本文に宛名を記載しないといったルールは設けているが、そもそも全員が機微情報に接している訳でも、機微情報の外部とのやり取りが必要な訳でもない。そのため、基本的な考え方としては、IT リテラシーレベルを高めるだけではなく、システム上、情報漏えいが起きないよう仕組み化することを意識している。

情報セキュリティ対策の効果

情報セキュリティ被害にあったことはなく、大きな脅威や危険を感じる場面も過去には無かったと認識している。情報通信業を営む事業者である以上、一定レベルの情報セキュリティ対策を行っていることは、顧客から見ても当然視されることであると考えられる。顧客からの信頼の前提として、情報セキュリティに取り組むことは重要であると考えている。取引先から、具体的な情報セキュリティ水準についての要請がある訳ではないが、だからと言って情報セキュリティ対策がおろそかになって良いということはなく、しっかりと取り組んでいく必要があると認識している。

「認証取得により従業員のセキュリティ意識が向上」

▼会社概要

所在地	長崎県
従業員数	6～20 名
業種	情報通信業
実施している対策	● 情報漏えいに備えるため、人的、物理的な対策を重視して実施。 ● 情報セキュリティに関する情報収集のために、社外の情報処理安全確保支援士へ相談。

情報セキュリティ対策の取組

当社は長崎県で医療･福祉向けシステム開発を行う情報通信業を営んでいる。

当社は秘匿性の高い情報を扱うシステムの開発を手掛けていることもあり、従前から情報セキュリティに対する関心は高く持ってきた。特に、個人情報保護法が施行された頃からは、情報漏えいを防ぐことが事業継続にあたり必須という認識を持って対策にあたっている。

情報管理を徹底する観点から、各種対策を実施している。特に、人的対策及び物理的対策には力を入れている。人的対策としては、出入口の常時施錠、入退出時の顔認証システムの導入、PC の社外持ち出し時に従業員からの書類提出の義務化といった対策を実施している。物理的な対策としては、セキュリティワイヤーによる情報端末の固定といった対策を行っている。

また、情報管理に万全を期すため、P マークの取得にも取り組み、認証を取得済みである。

従業員の意識向上も重要と考えており、情報セキュリティ教育にも力を入れている。従業員向け教育は、担当者が主導して社内で実施しているが、可能な限り外部研修を受講する機会も設ける努力をしており、その際には従業員全員で受講するように努めている。

情報セキュリティに関する情報収集にあたっては、社内だけで十分に知見を得ることは難しいと考えており、社外の情報処理安全確保支援士（登録セキスペ）への相談を行ったこともある。

取引時に、情報セキュリティ対策の実施を要請されることとして、発注者から秘密保持契約を結ぶよう求められることはあるが、具体的なセキュリティ対策の実施を要請されたことはない。

当社から他社に対して、業務委託を行う機会は少なく、委託の場合にも情報セキュリティ対策の義務化まで求めている状況ではない。とはいえ、セキュリティ対策ソフトの導入を勧める程度の会話は行っている。

情報セキュリティ対策の効果

情報セキュリティ上の被害にあったことがないことから、情報セキュリティ対策実施による一定の効果はあったものと考えている。

また、P マークを取得したことにより、社内の情報セキュリティへの意識は格段に高まった。P マーク等の認証取得は、社外からの信頼を得る効果を期待できると考えていたが、それよりも社内のセキュリティ対策への意識が向上したことの方が感じられたメリットとしては大きい。

P マークを取得する前後の時期は、情報管理に関する取り組みを一気に加速させたこともあり、対応が大変であると感じる従業員も多かったと思うが、従業員全員が気を引き締めて対応したことで、現在は安心感を持って業務を継続することができている。

「対策実施には、従業員の理解を得ることが重要」

▼会社概要

所在地	岡山県
従業員数	21～50 名以下
業種	運輸業･郵便業
実施している対策	● 関連会社の水準を目標に情報セキュリティ対策を実施･強化。 ● 勉強会を数カ月に1度の頻度で開催し、情報セキュリティ対策の必要性を「納得」してもらえるよう意識の醸成を図る。

情報セキュリティ対策の取組

当社は岡山県で運輸業を営んでいる。顧客である物流事業者とのやり取りはメールや電話、FAX を通じて行われているが、顧客との契約締結にあたり、情報セキュリティ対策の強化を求められたことはない。一方、行政機関への各種届出が必要なものについては、書類のリモート申請に関するガイドラインが定められており、当該ガイドラインに基づき一定の情報セキュリティ対策が必要とされている。

当社では業務上、海外とのメールのやり取りも多く、ウイルス感染が懸念されるメールを受信することも少なくない。そのため、当社ではコンピュータウイルス対策として、UTM（Unified Threat Management）を導入するとともに、従業員が利用する各 PC にはウイルスチェックソフトウェアをインストールしている。

当社では、Web サイトの閲覧に伴う情報セキュリティ上のリスクには、システムに対する設備投資を通じて一定の対応を実施している。しかし、外部からのメール受信を起点とした情報セキュリティの被害が生じるリスクは依然としてゼロではない。ただし、当社の従業員も外部からのメールによるコンピュータウイルスの感染リスクを理解しているため、現在のところ追加的な情報セキュリティ対策は不要であり、社内に大きなリスクが残されているとも考えていない。

情報セキュリティ対策の効果

当社は関連会社と一部業務システムを連携させているため、仮に社内でコンピュータウイルスの被害が広がってしまった場合、共倒れになる恐れがある。こうしたことから、関連会社の情報セキュリティ水準を目標に対策を進めている。当社の経営者は関連会社からの出向者であるため、関連会社の水準に倣い、情報セキュリティ対策を強化することには理解を得やすい状況がある。関連会社から「最近、〇〇のコンピュータウイルスが流行っているため注意するように」というメールが送られてくることもあるが、当社と付き合いのある IT ベンダからの提案を受け、先回りし対策を進めている場合、上司の理解を得やすくなる。

また、情報機器は何かの拍子に物理的に壊れてしまうこともある。そのため、業務継続の観点からも、情報機器で取り扱う各種ファイルのバックアップは定期的に取得しておくことが重要である。一方、情報セキュリティ対策を強化することは、既存の業務効率の低下をもたらす恐れがある。たとえば、過去に「情報機器のパスワードの都度入力」や「180 日毎のパスワードの変更」をルール化した際には、現場の従業員から業務上の非効率との反発があった。そのため、当社では社内で情報セキュリティ関連の勉強会を数カ月に1度の頻度で開催し、情報セキュリティ対策は、業務上、必要な取り組みとして「納得」してもらえるよう意識の醸成を図っている。

対策・投資多　被害有

「元従業員による機密情報の持ち出しの疑いから、対策を拡充」

▼会社概要

所在地	東京都
従業員数	6～20 名以下
業種	卸売業・小売業
実施している対策	● 社内の機密情報に関する社内規定を策定。 ● 情報資産管理やログ管理、デバイス管理を行うシステムを導入。

情報セキュリティ対策の取組

当社は東京都で海外から素材を輸入して国内メーカーに販売する卸売業を営んでいる。

社内の情報セキュリティ体制を整備した背景は、社内から情報漏えいが発生した疑いがあったことが大きな理由である。元従業員が退職前に大量にファイルをダウンロードし、かつ同従業員が用いていた PC が専門家でも復旧できないほど履歴が消去されていた。機密情報の持ち出しをした確定的な証拠が得られなかったため、結果的には被害届を提出するに至らなかった。社外からの脅威への対策としてウイルス対策ソフトウェアや電子メールへの対応、アクセス制限等を進めていたが、社内からの脅威への対策については、かつては十分ではなかった。

前述のトラブルが発生してから、社内の機密情報に関する社内規定を策定した。続いて、情報資産管理やログ管理、デバイス管理を行うシステムを導入した。このほか、機密情報を取り扱い場合には、専用の鍵付きのケースを用いる等、様々な取り組みを進めた。情報セキュリティ対策には自社の規模に対してそれなりの費用が必要となったが、中小企業庁「IT 導入補助金」を用いることで比較的負担が小さく導入することが可能となった。また、従業員向けの研修を行った。情報資産は会社の財産であること、従業員は情報資産を用いてビジネスを行うことで得られる交渉スキル等が、自らのキャリア上の資産になること、こうした共通認識をお互い持つことができた。

情報セキュリティ対策の効果

情報セキュリティ対策を行うことの効果は、経営者も従業員も安心できることである。小規模な会社で社内規定を作り、システムを導入することで、当初、従業員は自分が疑われているのではないかと感じたかもしれない。しかし、環境を整備し、従業員がそのルールに従って情報資産を管理することで、従業員自身も疑われずに安心して働くことができるようになる。

また、実際に被害にあった時のデメリットが大きいため、情報セキュリティ対策はこれらを予防できることである。前述のトラブルが起こった時には、「被害届を提出しない」と判断するまでに2年間の時間を要した。その間、弁護士に情報提供するために、様々な作業が必要になった。たとえば、情報漏えいしたと疑われるログをみて、どれが機密情報でどれが機密情報ではないのかを経営者と総務担当で膨大なデータをチェックする等の作業を強いることになった。トラブルの時には人件費以上に心的負担が大きい。対応している期間の心的負担は非常に大きかった。こうした問題から逃れることができるのはメリットがある。

また、情報セキュリティ対策を進めることは、クライアントから信頼を得ることができる。私用の鞄から機密情報が出てくると、クライアントも不安に感じるのではないだろうか。一方で、専用の鍵付きのケースで管理することで、万が一の対策が取れることに加え、クライアントから好感されることも多いと考えている。

対策･投資多　被害有

「身の丈にあった対策を、自社で考え実施していくことが必要」

▼会社概要

所在地	東京都
従業員数	101～300 名
業種	卸売業･小売業
実施している対策	● 取引先からの認証取得要請を機にアクセス制御等の対策を実施。 ● セキュリティ被害を教訓に、破られにくいパスワードの設定やスパムメール等への注意喚起を実施。

情報セキュリティ対策の取組

当社は東京都で施設の運営業務や施設運営に必要な設備の提供を行う卸売業を営んでいる。顧客としては、行政機関や大手企業が多くなっている。施設の運営業務や必要な設備の提供にあたっては、他社や行政との連携した業務が多くなっており、情報セキュリティ上、求められる対策についても増加傾向にある。また、社内の IT 化を進める観点から、最近は、社内サーバをクラウド化し、情報共有をクラウド型に変更する等の対策を実施している。

現在実施している情報セキュリティ対策として、5 年ほど前から、ゲートウェイセキュリティ装置を導入しており、社内ネットワークを保護している。こうした対策は、取引先から ISMS の取得要請を受け、何らかのアクセスに対する制御がなければ、認証基準を満たせないのではないか、との判断から導入にいたっている。

ゲートウェイセキュリティ装置では、外部から社内ネットワーク内に入ろうとしている者がいた場合には、グローバル IP の解析を行うこともできるようにしている。その他にも、ホワイトリスト･ブラックリストを用意し、アクセスの許可･禁止をできるようにしている。もう少し積極的な対策ができればと思うものの、コストや専門人材の不足が課題となり、現時点ではあまり手がかからずにできる対策がメインとなっている。一般的なサイトにアクセスする際に、一般的なブラックリストで拒否されてしまい、アクセスができないようになってしまったことはあり、そのサイトをホワイトリストに移行する、という作業等、セキュリティ対策導入に際して必要な対応もあるが、必要な取り組みと思い、実施してきた。また、外部からのアクセスを試みたグローバルIPアドレスやその他情報について、レポートを見ることはできるが、レポートを踏まえた対策を実施するまでには至っていないのが実態である。

当社ではメールアドレスとパスワードの漏えい被害があり、そのメールアドレスから、取引先に向けて大量のメールが送りつけられ、メールが不通になるという被害があった。この被害を受けて、特別な対策を追加したということはないが、破られにくいパスワードの設定や、スパムメール等への注意を強く呼び掛けるようになっている。

情報セキュリティ対策の効果

取引先からは、守秘義務や情報漏えい対策の実施、認証取得していることが求められており、取り組みを行っていなければ取引が実現しない可能性は高かった。また、ISMS 取得前までは、情報セキュリティに関するルールは社内にほとんどない状態であったが、認証取得のための社内のルール化に伴い、従業員の意識が向上し、積極的に情報収集してくれるようにもなっている。

被害を受けないために、身の丈に合ったセキュリティを考え、自社で判断していくことも必要と考えている。

対策･投資多

「IT の高度化は便利と脅威の「諸刃の剣」、対策の重要性を実感」

▼会社概要

所在地	東京都
従業員数	51～100 名以下
業種	卸売業･小売業
実施している対策	● 顧客･仕入先両者からの要請に応じた対策の実施。 ● マネージャー会議を通じて対策を現場で徹底するよう依頼。

情報セキュリティ対策の取組

当社は東京都で海外企業から仕入れを行う卸売業を営んでいる。仕入先の海外企業は、大手企業からベンチャー企業まで多岐にわたる。

仕入先からの情報セキュリティ上の要請としては、特に海外の大手企業から代理店としてのコンプライアンス対応が正しく行われているかチェックされる。このコンプライアンス対応の一部として情報セキュリティに関する要請がある。具体的には、情報セキュリティ担当の設置状況、情報セキュリティポリシーの設定、対策の方針等を仕入先企業に対して回答する必要がある。また、定期的に当該企業から監査が入り、正しく適用されているかチェックが行われる。一方、顧客からもファイルの取り扱い等について具体的な指示がある等、情報セキュリティ対策の要請もある。

情報セキュリティ対策のきっかけとしては、研究機関を顧客としていることが大きい。研究機関が行っている研究内容の多くは、機微な内容のものが多い。したがって、情報漏えいしてしまうことは、取引の信用上大きな問題となりうる。また、顧客の保有する情報を扱うこともあり、もし、漏えいしてしまえば取引が無くなってしまう恐れもある。一方で、情報セキュリティ上のリスクも高まっている。たとえば、標的型攻撃のメールが非常に増加している。アンチウイルス対策に加えて、ユーザへの教育にも力をいれている。疑わしいメールがあればファイルを開かず、削除するように教育を行っている。従業員をみると、自らが用いている PC の情報セキュリティにはあまり関心がない人もいる。従業員全体をある程度のレベルまで引き上げていくことも必要と考えている。マネージャー層の会議で、情報セキュリティ対策を現場で徹底するように依頼している。

顧客にも企業の研究員や大学の研究者が多いが、必ずしも情報セキュリティリテラシーが高いとは限らない。当社では、顧客からファイルを預かった場合には、社内ネットワークから隔離された端末でウイルススキャンを行う等の対策も行っている。

外部ネットワークと自社内ネットワークの境界を重点的に対策する境界型防御や VPN では完全な対策ができないという問題意識から、すべてを疑ってかかる勢いで対策を進めていくことが必要と認識している。当社の情報セキュリティ担当は、ウェビナー等を活用しながら情報収集を進めている。

情報セキュリティ対策の効果

情報セキュリティは「何も(トラブルが起こら)ないこと」、「あたりまえ」がゴールとなる。過去にトラブルがなかったことは情報セキュリティ対策からみると成功であるが、わかりやすい「ありがたみ」はない。しかし、ネットワークが高度化し、情報端末の高度化にともない脅威もさらに高まってきた。「平穏に仕事ができること」を維持することの負担が高まってきている。便利と脅威が「もろ刃の剣」になっている中で、情報セキュリティ対策の重要性を感じている。

対策･投資多

「身近な専門家に相談しながら適切な対策を」

▼会社概要

所在地	静岡県
従業員数	51～100 名
業種	卸売業･小売業
実施している対策	● 入退出管理や施錠保管、アクセス制御からセキュリティ監視サービスの活用まで幅広く実施。 ● 身近な専門家である IT サービスベンダからの積極的な情報収集。

情報セキュリティ対策の取組

当社は静岡県で資材等を扱う卸売業を営んでいる。

情報セキュリティ対策に取り組むにあたっての基本的な考え方としては、情報セキュリティありきではなく、業務の効率化･省力化のために様々な IT 化を検討していく中で、情報セキュリティ対策についても検討し、必要な対策に取り組むという考え方を採用している。また、取引先から、情報セキュリティ対策実施の要請を受ける機会も出てきており、対外的に情報セキュリティ対策の実施状況をアピールすることが、顧客からの信頼獲得にもつながるのではないかとの考えもあり、対策を進めるようになっている。

具体的な情報セキュリティ対策の取り組みについては、フロアや施設への入退出管理や書類等の施錠管理といった一般的なものから、アカウント毎のアクセス制御やセキュリティ監視サービスの活用といった取り組みまで、幅広く実施している。

また、通常業務で使用している販売管理システムや会計ソフトウェア等のソフトウェアについては、アップデートにあわせて常に最新のものを適用するように注意している。業務で使用する OS についても同様にセキュリティパッチは最新のものを適用するように心掛けている。こうした対策は、特段高い水準で実施しようという意識は持っていないが、必要なことを必要なだけ取り組むことは必須との意識を持って取り組んでいる。

当社は IT や情報セキュリティの専門部署を持っておらず、情報セキュリティ対策については総務部門の業務の一環として実施している。担当者も兼務で情報セキュリティ対策を実施している状態であるため、社内には IT や情報セキュリティ対策の専門家がいる訳ではない。

そこで重要になるのが、普段から使用している IT サービスのベンダとの関係性であると考えている。最も身近な専門家であり、困ったことがあればいつでも相談できる関係性を維持することで、安心感も得られ、担当者から新たな脅威や最新のサービスについて情報提供を得ることができる。

実際に現在行っている取り組みについても、ベンダの担当者から情報提供があった内容について、社内で考慮した上で実施しているものが大半である。

情報セキュリティ対策のポイント

情報セキュリティ対策によってプラスの効果が生まれているかは分からないのが本音である。しかし、他社の事故事例について耳にする機会も増えているなか、これまでのところ、ウイルス感染等の被害が出ていないのは、当社の取り組みが功を奏していることの証左ではないだろうかと感じている。

現在のところ、各種セキュリティ対策の実施により、顧客からの信頼獲得につながった実感はないものの、従業員のセキュリティや IT 全般に対する意識は向上していると感じている。

対策･投資多　被害有

「扱う情報のレベルに応じて、情報セキュリティ対策を依頼」

▼会社概要

所在地	沖縄県
従業員数	101～300 名以下
業種	卸売業･小売業
実施している対策	● 通信事業者の閉域網により、安全かつ高速なネットワーク環境を構築。

情報セキュリティ対策の取組

当社は沖縄県で卸売業を営んでいる。また、小売店や EC サイトの運営も展開している。

卸売業としては、納入先に大手小売店があり、大手企業から個人情報を預託する場合もあるため、これらの企業から会社の情報セキュリティや個人情報保護に関する要請がある。具体的には、情報セキュリティに関するアンケートが定期的に行われ、その結果を踏まえてフィードバックが行われる。このフィードバックを踏まえて、従業員教育の充実等も進めてきた。従業員教育には YouTube にある「IPA Channel」を活用しており、同チャンネルの情報セキュリティに関する動画を視聴してもらっている。

また、EC サイトの構築や会員情報の管理においては業務委託先があり、商品を仕入れることから仕入先も多数ある。扱う情報のレベルに応じて、情報セキュリティ対策を依頼しているところである。たとえば、業務委託先の中でも EC サイトの構築に関わる事業者については、高いセキュリティの要件を求めている。こうした企業では、情報セキュリティ対策の理解が高いため、高い要件を求めてもスムーズに取引できる。他方で、仕入先には家族経営の事業者も多く、情報セキュリティの理解が必ずしも高くない場合もある。ただし、これらの事業者ではセキュリティで保護すべき情報はあまり多くないため、EC サイトの事業者にくらべると緩い依頼としている。加えて、店舗間のネットワークにおいて、通信大手のもつ閉域網を活用している。閉域網はコストこそかかるものの、これを活用することで、早い通信速度を維持しつつも、安全なネットワーク環境を構築できている。このほか、自社の対策としては、入退室管理や個人情報を含んだ媒体の廃棄処分等もある。新型コロナウイルス以降、PC を持ち帰って在宅作業をする必要が増えている。Windows の BitLocker 等を使った PC の暗号化によるセキュリティ対策も行っている。

情報セキュリティ対策の効果

DoS 攻撃を受けて業務が止まってしまうことや、顧客等に影響が出ない範囲でウイルス被害にあった経験がある。しかし、EC サイトの運営の開始にあたり、情報セキュリティ対策を推進し、一定水準の対策が執られている。

経営層には、トラブル事例として、EC サイトからの個人情報漏えいで謝罪会見を開いたり、会員に金券を配ったりすることで理解を得ている事例等を伝えることで、情報セキュリティ対策に関する予算について理解を得ている。他方、情報セキュリティに必要な対策も増加している。ある程度改善しつつも、経営層と相談して情報セキュリティに関する損害保険にも加入している。

将来的には、Pマークの取得や「SECURITY ACTION セキュリティ対策自己宣言」等も検討している。これらは中小企業として補助金･助成金の受給要件に含まれていることもある。こうした観点からも当社としては、さらなる情報セキュリティ対策を進めたいと検討している。

取引先要請多

「法令順守に限らない積極的な対策が今後必要となる」

▼会社概要

所在地	京都府
従業員数	51～100 名
業種	卸売業･小売業
実施している対策	● 他業界の事例も活用した従業員教育の実施。 ● 業務委託先に対して研修実施や業務終了時の情報破棄を要請。

情報セキュリティ対策の取組

当社は京都府で携帯電話販売の代理店を営んでいる。

携帯電話の契約業務にあたっては、携帯キャリアの端末やシステムを用いている。そのため、当社が個人情報を電子的に保有する機会や保有する情報量は多くない。また、できるだけ当社が必要以上の情報を保有することがないよう、携帯キャリア主導で仕組化もされている。具体的に受ける要請としては、提供される業務端末へのウイルススキャンを定期的に実施すること、OS を最新にしておくこと、等がある。

一方で、すべての業務の仕方が携帯キャリアに定められているわけではない。たとえば、携帯キャリアから提供される研修の中には、本人確認書類を預かり、必要がなくなったらすぐに返すように、ということは書かれているものの、そのためのオペレーションについては、現場の裁量に任されている。そのため、独自に対策を考えていく必要があり、従業員の情報セキュリティ意識を高めていくために、新入社員向けの研修に情報セキュリティ研修も含めている。研修内容としては同業他社の事例だけではなく他業界の事例も示しつつ、意識を高めるように努めている。従業員が、情報セキュリティ対策に関する知識を正しく理解できているかは不安であるが、定期的に従業員向けの周知も実施し、正しく理解してもらうように取り組んでいる。

帳票電子化の傾向は進んでいるが、ペーパーを希望される顧客もいる。その際、印刷が必要になるが、しっかりと指差し確認をしないと、違う顧客に情報を提示してしまう可能性もある。こうしたこともあり、引き続き情報管理への取り組みが必要という意識は強い。

当社から業務委託を行う際にも、業務終了時の情報の破棄や、情報セキュリティ研修の実施を要請する場合もある。内容的に少し厳しいかもしれないという感覚もあるが、緩めるわけにはいかないと考えており、取引先に対して申し訳ない部分もあるが、お願いするようにしている。

情報セキュリティ対策の効果

情報セキュリティ対策を実施して得られた効果として、社内でのセキュリティ意識の向上があげられる。研修を実施していくと、従業員からもっと重視すべき情報セキュリティ対策に関する意見が上がってくるようになっている。また、情報管理の観点から、情報の確認に指差し確認や従業員間のダブルチェックを行うようにしており、そうした光景が顧客や取引先の目に入ると、感心してもらえることも多く、安心感を与えられている。

取引先からの要請は、情報セキュリティ対策を加速させる大きなきっかけになると思うが、そもそも個人情報保護法はすべての企業にかかわってくるため、法令違反しないためにもしっかりと対策する必要がある。また、社会全体で情報管理に対する目も厳しくなっているため、法令順守に限らない積極的な対策に取り組んでいくことが、今後必要になると考えている。

被害有

「手軽にECサイトを持てるからこそ対策が不可欠」

▼会社概要

所在地	大阪府
従業員数	5名以下
業種	卸売業･小売業
実施している対策	● 海外のIPアドレスから自社のECサイトにアクセスがあった場合、クレジットカード決済に必要な番号等の入力に失敗した場合のアクセス制限･アクセス遮断を厳格化。

情報セキュリティ対策の取組

当社は大阪府で店舗販売や通信販売を行う小売業を営んでいる。通信販売はECサイト経由の注文よりもFAXによる注文が多い。

現在、物流システムを刷新して新たなシステムに移行している最中であり、システム稼働後に追加の情報セキュリティ対策を実施することとしている。ただし、通信販売を行う上で、顧客の情報を適切に管理することは必要不可欠である。そのため、情報セキュリティ対策の根本をなす、守秘義務、情報の外部持ち出しの規定、情報の取り扱いに関する誓約書の締結は社内で規定している。また、個人情報保護方針についても取りまとめており、HPに掲載している。

先日、自社のECサイトに不正アクセスの痕跡があった。決済方法としてクレジットカード決済も認めているのだが、決済のページに多数のアクセスがあった。具体的にはクレジットカード番号をランダムに入力し、決済を試みていたようである。幸い、決済はすべて失敗していたためクレジットカードの不正利用はなかった。しかし、手当のために1週間程度の期間が必要となってしまい、その間、一部の機能が制限されたこともあり、金銭的にもわずかであるがマイナスが生じてしまった。この出来事は、情報セキュリティ対策強化の重要性を認識するきっかけとしては十分な経験であった。

不正アクセスの被害に気付いた後、サーバの履歴を確認したところ、海外のIPアドレスから大量にアクセスされていることが判明した。もちろん、クレジットカード会社を含む決済サービスを提供する会社側でも一定の情報セキュリティ対策を行っている所ではあるが、やはり、自社でも対策をする必要があると改めて感じた。これを受けて実施した対策として、海外のIPアドレスからアクセスがあった場合、クレジットカード決済に必要な番号等の入力に失敗した場合のアクセス制限･アクセス遮断を厳格にする取り組みを実施した。

情報セキュリティ対策の効果

不正アクセス対策を実施した後、ECサイトに再度同じ海外のIPアドレスから攻撃があったものの、無事に不正な決裁を未然に防ぐことができ、その後は同様のアクセスもなくなり、安全にECサイト運用ができている。そのため、しっかりと対策することで、被害をある程度防ぐことができることがわかったのは、大きな収穫であったと考えている。

ECサイトの構築･運用は、ひとりの担当者だけで行える時代であり、会社の規模に関わらず気軽に構築･運用できる。今回経験した海外からの不正アクセスについて、大きな被害は出なかったものの、不正に決済が行われていれば大きな被害が出ていた可能性もあり、情報セキュリティ対策は必要であると改めて気づかされた。

取引先要請多

「徹底した記録管理による情報管理を実施」

▼会社概要

所在地	福島県
従業員数	21～50 名以上
業種	金融業･保険業
実施している対策	● 関連会社が策定する規定や、所管官庁の通達に対応。 ● 紙や記憶媒体の溶融･破壊は、従業員が目視や写真で確認。

情報セキュリティ対策の取組

当社は福島県で金融業を営んでいる。金融業界は、業界として求められるセキュリティレベルが高く、業界独自の対策も積極的に行うことも求められる環境下にある。そのため、関連会社の支援を受けながらセキュリティ対策を進めてきた。また、当社の関連会社に相談したところ、金融業界のセキュリティに強みを持つコンサルティング会社の紹介を得た。同社の指導の下、情報セキュリティ対策を進めるほか、同社からの外部監査を受けている。

基本的には、関連会社が策定する規定に従うとともに、業界団体等の所属団体を通じて、所管官庁からも通達も来る。業界団体の方で、所管官庁とある程度調整･取りまとめがなされた状態で通達が来るため、対応している。このほか、情報セキュリティに関する保険にも入っている。情報セキュリティへの対応コストは、年々価格が上がっている。サーバを入れ替え等も求められる等、ある程度の費用を必要とする様々な対策が求められる。それに伴う指導のため、コンサルティング会社への費用も高まっている。

また、個人からの申込書類や届け出等の書類に記載している情報を扱うこともあれば、ハードディスクに各種情報の記録が残る可能性もある。情報セキュリティ対策、情報管理は「記録である」といわれており、当社では記録を徹底している。こうした申込書類は従業員が運送会社に同行し、廃棄する場所で溶解処理が行われていることを確認している。また、廃棄する PC 等はハードディスクを破砕して、これらを写真で破砕していることを記録している。

加えて、当社はプロパー従業員だけではなく、関連会社から人事異動により入社する場合もある。したがって、情報セキュリティについては、コンサルティング会社の作成した社内用の情報セキュリティマニュアルを勉強するように指導している。このマニュアルには、情報セキュリティに関する入門的な内容や、スマートフォンの不正利用等の事例も含まれており、これまで情報セキュリティに親しみが無くても理解できるようにかみ砕いた内容となっている。

こうした情報セキュリティ対策によって、当社ではこれまで情報セキュリティ被害はなく、外部からの攻撃等はいずれも防いできたところである。

情報セキュリティ対策の効果

近年、キャッシュレスの動きの中で、デジタル化された金融サービスの提供機会が増えてきている。また、当社でも一般消費者だけではなく、地方自治体との取引機会も増加してきた。

地方自治体からは、関連会社への信頼に加えて、情報セキュリティ対策等からも評価を得ることができており、当社の取引に結び付いている。

また、情報セキュリティ対策が万全であることは、営業担当も安心してセールスすることにもつながっていると考えており、引き続き、万全の対策をとっていくつもりである。

対策･投資多　被害有

「自社の対策に加え、顧客への注意喚起等の取り組みも重要」

▼会社概要

所在地	神奈川県
従業員数	301 名以上
業種	金融業･保険業
実施している対策	● 高い業界水準を意識し、委託先も含めて対策を推進。 ● 業界内での情報共有、人材育成については精力的に取り組む。

情報セキュリティ対策の取組

当社は神奈川県で金融業を営んでいる。金融業界では、様々な場で情報セキュリティについて議論する機会が多い。特に最近では、エモテットやランサムウェアへの対策等が話題になっているほか、サイバー攻撃に対する情報共有を行っている。また最近では、情報セキュリティ分野の人材育成が重要なトピックとして議論されているところである。

過去に行政が金融関連業界を対象に視察を行った時に、情報セキュリティ対策が十分ではなかったことから、金融業界全体としてセキュリティ水準が高く求められるようになったようにも感じている。当社もこれをきっかけに、人材面･システム面も含めて強化してきたところである。

情報セキュリティ対策については業界基準が定められているため、それに従った対策を進めている。金融業界は前述の通り、全体的に要求水準が高い業界であるため、堅牢な情報システムを構築しているところである。金融業界という特性からか、一定程度攻撃を受けることも多いが、これらの攻撃により当社から情報漏えいをしたことはない。また当社が要因になって、他社から情報が漏えいするケースもみられない。外部委託先に業務を依頼する場合には、情報セキュリティに関するチェックリストを使って委託先企業の情報セキュリティの状況を把握している。

しかし、金融業界では、企業の名前を悪用されてしまうことで、一般消費者である顧客がフィッシング詐欺にあってしまうことが実際に発生している。具体的には金融関連企業の名前等をかたり、第三者が顧客にアプローチし顧客がカード情報や個人情報を入力してしまうことがある。顧客への十分な情報セキュリティに関する情報の周知も引き続き重要だと認識している。

加えて、情報セキュリティに関する人材は獲得が難しく、金融業界の専門性を有する人材となるとさらに希少となる。このため、社内での人材育成が肝要だという認識を持っている。育成にあたっては、社内研修はもちろんのこと、社外の様々な研修や動画教材、e-ラーニング教材も活用しながら人材育成に取り組んでいる。

情報セキュリティ対策の効果

情報セキュリティ対策は費用対効果の説明が難しいところである。しかし金融業界では、仮に顧客の個人情報等が漏えいしてしまった場合には、甚大な影響を受けてしまう。具体的には、問題解決に向けた調査費用や賠償金も莫大な金額になると見込まれる。

また、風評被害による影響も甚大であり、多くの顧客を失ってしまう恐れもある。このため、十分なセキュリティ投資をシステム面、人材面において行う必要があると認識している。

対策･投資多

「従業員のリテラシー向上と、経営者の学ぶ姿勢が大切！」

▼会社概要

所在地	山梨県
従業員数	6～20 名以下
業種	金融業･保険業
実施している対策	● 外部ベンダを活用することで情報セキュリティ水準を確保。 ● 従業員に対する定期的な勉強会の開催。

情報セキュリティ対策の取組

当社は山梨県で保険代理店を営んでいる。取引上は保険会社とのやり取りはあるが、業務の再委託先はシステム･情報セキュリティに係るものを除くとほとんどない。主な情報のやり取りは顧客とのやり取りが中心であり、電子メール等でのやり取りについては留意が必要であると感じている。これまでに具体的な情報セキュリティ被害の経験は無いが、やはり脅威としては強く認識している。標的型攻撃を含むサイバー攻撃についても、自分たちが被害者になる懸念と同時に、加害者ともなり得る点で、怖いリスクであると認識している。

当社のシステムは端末等のハードウェアやソフトウェアも含めて外部のベンダに委託をして構築･メンテナンスを行っており、事業を行う上で必要とされる情報セキュリティ水準は確保している。電子メール等のやり取りを含め、従業員等の不注意による流出懸念はもちろんある。この点、保険代理店として高いコンプライアンスが求められていると理解しており、毎週定例で従業員との勉強会を開催しており、モバイル端末の取り扱い等についても勉強会で取り上げている。勉強会では、他者が作成･提供している動画コンテンツ等も活用している他、外部の研修･セミナー等も利用している。また従業員のリテラシー向上を狙って、標的型攻撃の訓練等も実施し、啓発を行っている。

最近は、コロナ禍の影響で、リモートワークが増えたことや、顧客ともオンラインで面談する機会が増えている。そのため、リモートワークやオンライ面談に対応した社内規程も整備を行い、端末や設備についての対応も行った所である。

取引先との関係では、やはり保険会社からの要請はある。保険業界自体、情報セキュリティに対する意識が高いため、具体的な要請やチェック、監査等も行われている。

情報セキュリティ対策の効果

情報セキュリティ対策に取り組んでいることで、顧客からの信頼に応えることができており、取引を継続してもらえていると認識している。また、情報セキュリティ対策を通じて、業務の効率化が図られている側面もあり、この点もメリットであると感じている。最近は電子メールの管理やログの管理等がしっかりできていなければ取引をしてくれない企業もあり、情報セキュリティに取り組むこと自体が事業活動の前提となっている。

今後については、経営者自らがより情報セキュリティに係るリスクを深く理解していくべきであると考えている。現時点でも情報セキュリティに対する意識は高く持っているつもりで、システム･情報セキュリティについてはしっかりと外部のベンダに対応してもらってはいるが、技術的な部分はベンダに任せてしまっている部分もあり、より主体的にリスクの把握･認識、チェック、判断が行えるようになっていくべきであると考えている。

対策･投資多　取引先要請多

「取引先からの要請への積極的な対応が事業継続につながる」

▼会社概要

所在地	愛知県
従業員数	6～20 名以下
業種	金融業･保険業
実施している対策	● 取引先から提供されたチェックシートを活用してセキュリティ自己点検を実施。 ● 従業員のリテラシー向上に IPA の資料を活用。

情報セキュリティ対策の取組

当社は愛知県で保険代理店を営んでいる。

情報セキュリティ対策は、過去にメールの誤送信による情報漏えいが起きた経験もあり、情報管理の一環として、積極的に取り組んでいる。

特に、保険代理店業を担当する部門に対しては、保険会社から情報セキュリティ上の対策実施の要請を受けるようになっており、社内でも最も高いレベルで対策を実施している。保険会社から要請を強く受けるようになったのは、保険業法の改正に伴い、保険代理店の業務体制整備の一環として、求められるようになってきたと記憶している。具体的な内容としては、個人情報に触れる従業員を限定することといった人的な対策だけでなく、ソフトウェアのバージョンアップ、サーバのバージョンアップ等、システム面での対策についても要請を受けている。最近では、SNS やフリーメールの使用は控えるように、という要請も出てきている。事業においては、保険代理店向けのシステムを用いているが、こうしたシステムにアクセスするための端末のセキュリティ対策は、当社独自に取り組む必要がある。対策の実施状況は、代理店側が自己点検するよう求められており、自己点検に用いるチェックシートの提供も受けている。また、新型コロナウイルス感染拡大を受け、できるだけ対面ではなく、デジタルを活用した事業活動を要請されるようになっている。それに伴い、たとえば、電子契約システムの導入等も検討しているが、追加的な情報セキュリティ対策が必要かどうかといった点について、現在検討を進めているところである。

現在は、それぞれの事業部ごとに取引先から求められている対策を事業部ごとに進めているのが実態であり、今後は、全社的にセキュリティ対策の実施レベルを高い水準で一律にそろえていきたいと考えている。自社独自の対策としては、個人情報保護対応の一環として、社内メール便についても、後からトレースできるようにログを取る等の対策を取っている。また、従業員への情報セキュリティ教育を定期的に実施する等、従業員のリテラシーを向上させる取り組みも実施している。教育にあたっては、IPA の資料を活用していることが多く、特に、最近はどういったウイルスや手口が広まってきており、それに対する対策についてまとめられている資料を活用していることが多い。

情報セキュリティ対策の効果

取引先からの要請に対応することで、当社の情報セキュリティ対策のレベルを向上させることにつながっている。特に、保険会社からの要請に対応することは事業継続のために必須であるため、情報セキュリティ対策を実施し、事業継続ができていることは対策実施のメリットであると考えている。今後も、あらゆる取引に共通して、こうしたセキュリティ対策を実施していないと事業継続が難しいととらえて対策を進めていかないといけないと考えている。

対策･投資多　被害有

「取引先に対する信頼性向上のためのセキュリティ対策」

▼会社概要

所在地	兵庫県
従業員数	21～50 名
業種	金融業･保険業
実施している対策	● 携帯電話･タブレット端末へ個人情報を残さない運用を整備。 ● コンサルティングサービスを活用し、取引先の安心材料を獲得。

情報セキュリティ対策の取組

当社は兵庫県で保険代理店を営んでいる。主な取引先は保険会社である。個人情報を扱う業態であることから、自社としても情報セキュリティ対策には一定の取り組みを講じてきているところであるが、取引先である保険会社からの要請でさらなる強化を行うことも少なくない。昨今、保険会社が金融庁から「品質」面での取り組み強化を求められている背景もあり、その一環で保険会社から代理店へと要請が来ることも多く、特にここ数年はそうした傾向が強くなってきている。たとえば、保険会社から「クラウド」の導入を求められたこともある。当社の場合は、既に類似したシステムを導入していたため、保険会社と交渉し、既存システムに対して、クラウドと同等のセキュリティレベルを担保できる機能を追加する対応を取ることとした。具体的には、二段階認証の活用や、パスワード付き zip ファイルとそのパスワードを別送する、いわゆる「PPAP」廃止等である。ほとんどがパスワードに関するものであった。こうした仕組みは、それほど負担なく設定できる一方で、従業員の運用として定着させていくのは苦労したところである。従業員によって、情報セキュリティに対する意識や知識に差があるため、なかなかパスワード等の運用に慣れない者がいたのも事実である。

以前、当社が利用している外部レンタルサーバが攻撃を受けたことがあったが、特に大きな損失にはつながっていない。外部サーバが攻撃を受けたものの、中に入られた形跡はなかった。ただし、直接的な被害はなかったものの、念のためサーバへ入る際のパスワードを変更した。

営業担当者には、携帯電話やタブレット端末を支給されているが、その扱いについても厳しく規定している。そもそも、タブレット端末には個人情報を保存しないようにしているのと、携帯電話に情報を登録する際には個人を特的できないような登録をするようにしている。また、こうした端末で写真を撮影した際にはオンラインストレージへ即座にアップロードし、端末には写真を残さないようにもしている。こうした情報セキュリティ対策は自社負担で実施しているが、以前、保険会社からの提案でコンサルティングサービスを自社負担なしで受け入れた際には、保険会社を安心させることにもつながった。

情報セキュリティ対策の効果

業界として情報セキュリティ対策に対する要請が強くなってきている中で、保険代理店が継続的に各保険会社との関係を築き、取引を継続していくには、情報セキュリティ対策の実施が必須となっている。当社の場合は、そうした要請に対して適切に対応してきていることもあり、現状として保険会社と良い関係性を継続できている。従業員全体の情報リテラシー向上は今後の課題だと感じている。情報セキュリティ関連のルールを導入･変更すると、一定数の反発があるのも事実であり、そうした状況を改善していくためにも、従業員全体として情報セキュリティに関する知識･意識を高めていく必要がある。

「高い業界水準を意識した情報セキュリティ対策の実施」

▼会社概要

所在地	岡山県
従業員数	51～100 名程度
業種	金融業･保険業
実施している対策	● 関連会社からの要請を受けて網羅的に対策を実施。 ● 委託先に対して契約時の秘密保持、契約終了時の情報資産取り扱いを要請。

情報セキュリティ対策の取組

当社は岡山県で保険代理店を営んでいる。主な顧客は個人であり、企業間取引は多くはない。当社には関連会社があり、関連会社から情報セキュリティ対策の要請を受けることもある。要請に対応するため、社内に情報セキュリティ担当を複数名配置し、対策を実施している。

関連会社から要請される内容としては、特定の情報セキュリティ対策に特化しているわけではなく、広く浅く要請を受けているという理解である。様々な項目において、一定水準以上の情報セキュリティ対策を取るように依頼されるが、対策の実施にあたり、関連会社から特定の製品の活用を求められることはなく、関連会社一括で対策のためのツールが導入されているわけでもない。そのため、本社内の設備や事業所内の設備に対しては、基本的に自社単独で対策を実施することが求められており、社内の情報セキュリティ担当が主導して取り組みを実施している。こうした経緯もあり、情報セキュリティ対策実施にあたっての費用負担については、自社単独で実施しているといえるだろう。

実施している対策の中で、特に重視している対策があるわけではなく、基本的に求められる対策を実施しているという考えだが、十分に対策ができているかと問われると、わからない部分もある。

サプライチェーンセキュリティ対策という観点では、自社から業務を委託することはあまり多くはないものの、委託先に対して、契約時に秘密保持や、契約終了後の情報資産の扱いについて要請を行っている。

情報セキュリティ対策の効果

これまで、特段大きな情報セキュリティ関係の被害にあったことはないと認識している。これまでの情報セキュリティ対策を実施したことによるメリットを明確に感じられているわけではないが、被害にあっていないこと自体がメリットの1つであると考えている。

今後、対策をさらに進めていくことで、情報セキュリティ対策のメリットを感じていけるようにしたいと考えているが、情報セキュリティ対策を推進するうえで苦労する点として、情報セキュリティ教育があげられる。今後、自社のセキュリティレベルを上げていくためには、従業員の情報セキュリティに関する知識･意識レベルを向上させていくことが必須と認識している。どうしても情報セキュリティ担当の従業員と一般の従業員との間では、情報セキュリティ対策への関心･危機感の持ち方に差が生じてしまう。

金融業界に属する企業であることから、中小企業の中でもより高いレベルの情報セキュリティ対策が求められると認識している。今後は、従業員により情報セキュリティ対策に関する意識を高めてもらえるような社内教育を実施し、全社的なセキュリティレベルを向上させていきたい。

対策･投資多

「従業員の安心感が対策実施の原動力に」

▼会社概要

所在地	高知県
従業員数	6～20 名以下
業種	金融業･保険業
実施している対策	● IT ベンダや商工会議所を通じた情報収集を実施。 ● 自社が提供するサービスへのぜい弱性診断を実施。

情報セキュリティ対策の取組

当社は高知県で保険代理店を営んでいる。主な顧客は保険を付保される方であり、個人から法人まで様々な方がいる。

取引先から情報セキュリティ対策実施の要請を受けることもあるが、現時点でそうした要請への対応に苦慮しているということはなく、要請には対応できている。また、当社から業務を委託する機会はほとんどなく、当社から取引先に対して情報セキュリティ対策の要請は行っていない。

情報セキュリティ対策の必要性を感じたきっかけとしては、保険の見積書を作成する際に、顧客情報を預かる必要性があり、情報漏えいがあっては大変なことになると考えたことがあげられる。また、IT ベンダや商工会議所からも情報セキュリティ被害の事例についても話を聞く機会が増えている。周囲でも被害が起きていることを聞き、情報セキュリティ対策の実施が必須であると感じさせられるようになっていた。

対策の実施にあたっては、IT ベンダに委託し、対策の一部を担ってもらうほか、自社主導で実施する対策のアドバイスをもらっている。特に、ぜい弱性診断ツールを導入し、自社が提供するサービスのぜい弱性を診断してもらうようになり、大きな安心感が得られている。当社が主導して実施する対策としては、ウイルス対策ソフトウェアの導入や、閲覧できる Web サイトを制限するフィルタリングサービスの導入、ファイアウォールの導入等がある。

当社では、常に情報セキュリティ対策を継続した上で業務運営を行っていくことが必要という意識を持っているが、そのためには、従業員のセキュリティ意識の向上が必須ととらえている。現時点での従業員に向けた教育はまだ十分とは言えないものの、意識向上のための教育について、今後も積極的に取り組むことが求められていると考えている。また、社内規則の整備も行ってきているが、まだ改善の余地はあるのではないかと感じており、今後、規則の再整備等にも積極的に取り組んでいきたいと考えている。

情報セキュリティ対策の効果

これまで情報セキュリティ被害にあっていることはなく、対策が一定の効果を発揮しているのではないかと考えている。

また、IT ベンダに対策を委託して情報セキュリティ対策に費用をかけていることで、社内外から一定の評価や安心感を得られているのではないかと考えている。

従業員からも一定の安心感を持って業務にあたることができている、との声を聞いている。従業員の安心感を得られていることは、対策を実施している側からすると非常に嬉しいことであり、対策を実施してよかったと感じさせてくれる。

取引先要請多

「取引先や業界団体からの要請を重視した対策実施」

▼会社概要

所在地	宮崎県
従業員数	6～20 名以下
業種	金融業･保険業
実施している対策	● 取引先からの要請を受けて、秘密保持、監査協力、インシデント対応、契約終了後の情報破棄等に対応。

情報セキュリティ対策の取組

当社は宮崎県で保険代理店を営んでいる。

情報セキュリティ対策を実施しなければならないと感じたきっかけとしては、業務上、個人情報を取り扱うため、情報漏えいすることを避けたかったこと、ここ数年で取引先や業界団体から情報セキュリティ対策実施の要請が多く来るようになっていることがあげられる。

当社は複数の会社の保険商品を取り扱っており、それぞれの会社ごとに、情報セキュリティ対策の要請がある。多くの場合、秘密保持の要請や、監査への協力、インシデントが発生した場合の報告、契約終了後の情報の破棄、といった項目が主である。業界として要請にあたってのガイドラインが整備されている印象はなく、各社ごとに独自のフォーマットで要請は送られてくるものの、その内容は概ね似通っており、取引先ごとに個別対応が必要という印象はあまりない。

しかし、当社で保有する端末やシステムのセキュリティは自社で守る必要があるため、一定程度の対策、投資は必要であり、気を引き締めて対策を実施している。

当社の顧客は個人が主であるため、当社からの業務の委託等は発生する機会はない。そのため、当社から、情報セキュリティ対策実施の要請を行う機会は発生していない。

保険代理店業を少しでも手掛けている企業は、個人情報を取り扱う前提で、情報管理体制を構築する必要がある。そのため、保険会社からの要請を受けたとしても、その対応にあたり特段苦慮することはないケースが多いのではないかと感じている。

情報セキュリティ対策の効果

業界全体として、情報セキュリティ対策の強化に関心が高い傾向にあると考えており、情報セキュリティ対策を徹底しておかなければ、取引が実現しない可能性も高い。以前から情報管理への意識は高くもっていたつもりであるが、現在、保険会社と継続して取引ができているのは、日々の対策のおかげであると考えており、このことが対策実施の一番のメリットであると考えている。

また、当社もコストをかけて情報セキュリティ対策を実施しなくてはならない。取引先や業界団体から実施すべき対策についてレクチャーがあることは、専任の担当者がおらず、情報セキュリティの知見が蓄積されていない当社にとっては、大きな安心材料になっている。実際に、取引先からの要請に応じて対策を強化したことで、従業員の情報セキュリティへの意識は向上し、以前よりも、従業員の端末を経由した情報セキュリティ被害にあうリスクは軽減されているのではないか、と感じている。

業界団体からも情報セキュリティ対策の重要性について触れられることも出てきており、ますます対策が求められる環境になったとの認識を持って、今後も業務にあたりたいと考えている。

対策･投資多　取引先要請多

「ツールを導入することで従業員に負荷をかけず対策を推進」

▼会社概要

所在地	福岡県
従業員数	101～300 名以下
業種	金融業･保険業
実施している対策	● 通信に係るハートウェア･ソフトウェアについて、対策すべき事項を定め、定めた項目について情報セキュリティ対策を最新状態とする。 ● 事業継続やリスク管理の観点から、決裁者への働きかけを実施。

情報セキュリティ対策の取組

当社は福岡県で個人向けの金融サービスを提供する企業を営んでいる。

金融業界では、顧客番号の不正使用や悪用、海外からのサイバー攻撃等の問題が多く、顧客番号情報の漏えいや不正アクセス等に関する情報セキュリティ対策が進められてきた。しかし、近年、顧客番号漏えいだけでなく、顧客番号に紐づく個人情報をしっかりと守ることを重視し、それに向けた対策が強化されている。

当社では業界として高い水準の情報セキュリティ対策が求められることを認識し、日々の業務を行っている。具体的には、通信に係るハードウェアやソフトウェアについて、充足すべき事項を定め、情報セキュリティ対策を高い水準に保つため、毎年多額の設備投資を行っている。

サイバー攻撃の頻度や攻撃のレベルが上がることにより、当社でも社内の情報セキュリティ対策を強化している。また、高い水準の情報セキュリティ対策が実施できていなければ、当社も事業を継続に支障をきたす恐れもあることから、情報セキュリティ対策に本腰を入れ取り組んでいるところである。一方、情報セキュリティ対策は利益を生む取り組みではなく、組織のトップの考え方に左右されてしまう面もある。そのため、情報セキュリティ対策の担当者は、事業継続やリスク管理の観点から、決裁権者に対し、情報セキュリティ対策の重要性を訴えていくことが重要である。

情報セキュリティ対策の効果

顧客情報の漏えいは防がなければならない事項である。しかし、当社の収益に対するリスクという観点では、マルウェア等のサイバー攻撃を受け、業務システムが機能しなくなることも大きな脅威である。なお、業界としてもサイバー攻撃は多いものの、当社では情報セキュリティに対して積極的な対応をしてきたことから、これまでのところ情報セキュリティ上の問題は起きていない。

情報セキュリティ対策を推進する際、既存の業務フローを変えるような方針には、現場の従業員から反発が出ることもある。また、短期的な視点から、情報セキュリティ対策への投資を避け、現場の業務フローを見直すことで対応する場合、セキュリティ基準が強化される度に業務フローの見直しが必要になる。当社ではこれまでの取り組みを通じて、業務に支障がでないよう費用をかけてでも、機械化できる点は機械化することで、組織の業務効率の低下や現場の反発を防ぎつつ、情報セキュリティに関する対策を「表に出ない、深いところ」で推進することの重要性を感じている。

さらに、日々のルーティン業務の中で、従業員に対し、「やって良い情報の取り扱い」と「してはいけない対応」を自然に伝えていくことが情報セキュリティ対策を組織的に進めていく上でのポイントであると考えている。

対策･投資多

「企業活動のデジタル化に対応するためにも対策を進めておく」

▼会社概要

所在地	北海道
従業員数	5 名以下
業種	不動産業･物品賃貸業
実施している対策	● 情報セキュリティを理解している従業員が、周囲の従業員に積極的にサポートする形で、情報セキュリティ対策を推進。

情報セキュリティ対策の取組

当社は北海道で共同住宅の管理や賃貸等の不動産業を営んでいる。

不動産業界は、紙文化が強く残っている業界であり、急ぎの情報共有や書面の共有の場合には、速達郵便を使うことも多い。この傾向は、新型コロナウイルス感染拡大後も続いており、デジタル化が進みにくい文化は依然として残っている。そのため、情報セキュリティ対策の必要性を感じにくい環境にある。そうした中で、当社が情報セキュリティ対策の必要性を感じたきっかけとしては、賃貸業を開始した際に、業務で個人情報を取り扱う場面が出てきたため、情報漏えいが起きては大変なことになる、という危機感が生まれたことがあげられる。紙媒体の情報を管理するためにできることといえば、施錠管理くらいになってしまうが、PC で管理する部分も出てくるため、取り組まなくてはいけないという考えに至った。

取り組みの際、特に苦労した点として、これまであまり PC に触れていなかった従業員へのセキュリティ教育があげられる。小規模な企業であり、従業員の年齢層も高いため、普段の生活やこれまでの業務で PC を使用する機会がほとんどなかった従業員に対し、いきなり情報セキュリティ対策に関する内容を伝えていくことは難しい。そのため、情報セキュリティに関する知識をまとめたマニュアルを作るというよりは、ニュースになった被害の事例や、ソフトウェアのアップデート、ウイルス対策ソフトの起動等、情報セキュリティを理解している従業員が都度教えたり、場合によっては、代わりに実施したりすることで被害にあわないように努めている。

情報セキュリティ対策の効果

デジタルデータを管理する際に安心することができるということが、情報セキュリティ対策を実施したことによるメリットと考えている。今後、企業活動は業界を問わずにデジタル化が進んでいくことが予想される。特に経理周りは、デジタル化が急速に進み、領収書等をデジタルデータで管理する必要性が高まってくる。そのため、情報セキュリティ対策を進めておくことで、これまで紙で管理していた記録のデジタル化が求められた際にも、情報管理に不安を感じずに済むのではないか、と考えている。行政においてもデジタル化の機運が高まっており、事業者から行政へ行う申請の一部もデジタル化されているものも出てきている。日々、セキュリティ対策を実施しておくことで、企業活動に関する情報を安心してデジタルで管理することができるようになり、行政への申請の際の効率化につながる効果も期待できるようになるのではないかと考えている。

対策・投資多

「セキュリティ対策としてデータの棚卸を行い、業務効率化が実現」

▼会社概要

所在地	東京都
従業員数	301 名以上
業種	不動産業・物品賃貸業
実施している対策	● 外部事業者を活用したサイバー攻撃への対処訓練の実施。 ● 情報漏えい事故発生に備え、損害賠償保険にも加入。

情報セキュリティ対策の取組

当社は東京都で不動産業・物品賃貸業を営んでいる。

近年、コロナ禍の影響もあり、テレワークや外勤先でのモバイル利用が増えている。当社の場合、元々の情報セキュリティ対策が PC を持ち出さない前提で仕組みが構築されていたため、テレワークやモバイル利用の観点から、情報セキュリティ対策について取り組むべきことは多くなっている。

テレワークの機会が増加したことにより、社外における端末利用に伴うリスクが増えていると認識しており、アンチウイルスの強化等を検討している。当社には多数の PC があり、それらすべてにセキュリティ対策ソフトウェアを入れると年間にかかる費用は高額となるため、躊躇はするものの、導入する方向で検討している。

体制面においても、情報セキュリティ部門を近年設置し、現在 5 名の体制で対応している。また、当社の全社的な枠組みとして情報セキュリティ委員会を設置し、各部署に担当者を置いている。また、情報セキュリティ管理規程等は、関連会社が大枠を示しており、その大枠を受けて、当社での具体的な対策に落とし込んで整備をしている。

最近は、標的型攻撃の脅威が高まっていることを受けて、外部事業者を活用し標的型攻撃訓練を実施したり、従業員研修を実施したりする等の対応も行っている。訓練の結果については、ファイルや URL を開いてしまった人の人数をイントラネットで開示し、注意喚起をするとともに、各部門のセキュリティ担当者には個人を特定してフィードバックし、個別の注意喚起を行っている。当社では、IPA が作成している啓発動画等も活用しており、経営層にも視聴を促している。

加えて、情報漏えい事故発生に備え、損害賠償保険にも加入している。自社のリスク分析を踏まえ、当社にとって情報漏えい事故の発生は極めて大きなリスクとなることが明らかであることから、万が一の発生に備えたものである。

情報セキュリティ対策の効果

情報セキュリティ対策を実施している結果、従業員のセキュリティ意識は各段に高くなっている。当社は業種としても顧客からの信頼が特に重要であると認識しており、従業員の意識が高めることは会社として重要であると考えている。

また、情報セキュリティ対策に取り組んだ結果、データの棚卸が進み、業務の効率化が実現した。外部からの攻撃対策だけでなく、BCP の観点から、各事業所におけるファイルサーバの入れ替えを行った。データを移行する際に、各事業所に不要なデータを削減するように依頼し、結果として保有するデータの活用も視野入れたデータの体裁を揃える等のきっかけにもなった。今後、パート契約や派遣契約も含めた全従業員の更なる意識向上に取り組んでいきたいと考えており、今期中にケースメソッド方式の研修を実施し、自分で考えてもらう時間を取りたいと考えている。

対策･投資多

「外部の IT ベンダを活用して、効率的かつ効果的な対策を実施」

▼会社概要

所在地	愛知県
従業員数	6～20 名以下
業種	不動産業･物品賃貸業
実施している対策	● 外部のITベンダに全面的に委託してツールを活用した対策を実施。 ● さらされている脅威については、定期的に報告を受け、危機意識や取り組みへの意識を高めている。

情報セキュリティ対策の取組

当社は愛知県で不動産仲介や分譲販売等を行う不動産業を営んでいる。取引先として、物件の仕入れ先は法人が多く、顧客は個人が多い。そのため、取り扱う情報としては、物件情報はもちろんだが、顧客情報が多くなっている。

当社は設立当初より情報セキュリティについては意識を持っていた。情報セキュリティ被害は、しばしば報道されており、サイバー攻撃や事務処理ミスによる顧客情報の漏えいは経営上重大なリスクであると認識し、同様の意識を従業員に対しても発信し続けている。

情報セキュリティ対策の取り組みとしては、設立当初より、システム全般を外部のITベンダに委託しており、システムの構築及び情報セキュリティ対策も任せている。情報通信機器(PC やタブレットだけでなく、スマートフォンや複合機等も含め)も、個々に対策を講じるのではなく、IT ベンダからウイルス対策やメール誤送信防止ツールの導入等、情報セキュリティ対策を施したものを提供してもらい、監視、セキュリティソフトウェア等の更新を含むメンテナンスの対応もしてもらっている。

業界の特徴として、どうしても電子化されていない書類が多く、書類については施錠キャビネを利用して管理している。また、業務上 FAX の利用も残っており、従業員の事務ミスを防ぐのは大変だが、継続的な注意喚起、やり取りの前に再チェック等を徹底するようにしている。

情報セキュリティ対策の効果

IT ベンダに一括してシステム構築･運用、情報セキュリティ対策を委託することで、一定の費用が掛かっているが、個々に対応、対策を行うコストを考えればむしろ効率的であると考えている。IT ベンダに管理を委託しているため、社内には情報セキュリティ担当者を配置する必要が無く、経営者が定期的にITベンダと会議を行うことで、課題の把握や対応等を判断すれば足りる状況となっている。その際、毎月検知された脅威等の情報の報告を確認する機会を設け、完全に任せきりにならないように気をつけている。結果として従業員には、不動産仲介や売買業務に安心して注力してもらえており、活力の一端にもなっていると感じている。

近年、個人の顧客は企業をしっかり見ており、顧客情報を預かる企業は、情報セキュリティ対策をしっかり実施していて当然だと思っている。感覚的には、「有料駐車場を利用するコストを惜しんで、路上駐車という法令違反を犯すべきではなく、有料駐車場を利用するのが当然。仮に路上駐車をして、運よく反則切符を切られなくても、お客様はちゃんとその会社のコンプライアンス意識は見ているもの」と考えている。情報セキュリティ投資は、「もったいない」と考えるべきものではなく、当然支払うべき経費だと考える必要がある。

被害有

「従業員のフィッシング詐欺被害を機に、対策の必要性を実感」

▼会社概要

所在地	兵庫県
従業員数	1～5 名
業種	不動産業･物品賃貸業
実施している対策	● ウイルス対策ソフトウェアの導入に加え、ルータに追加する形で外付けの情報セキュリティ対策端末を導入。

情報セキュリティ対策の取組

当社は兵庫県で不動産業を営んでいる。個人向けには賃貸物件の仲介を行い、業者向けには物件の修繕等に係る内容の取引が多くなっている。また、規模は小さいものの、飲食業も営んでいる。

自社が情報セキュリティ上の被害にあったことはないと考えているが、自社の従業員が個人的にフィッシング詐欺の被害にあったことで、情報セキュリティ上の被害に自社があう可能性についても考えるようになった。

それまでは、ウイルス対策ソフトウェアを業務に使用している端末に入れている程度であったが、ルータに追加する形で外付けの情報セキュリティ対策端末を導入した。これまで付き合いのあった IT 関連業者とセキュリティ対策について相談し、ソフトウェアだけでウイルス対策をすることは難しいとの助言を受けたことも、導入に至ったきっかけである。小規模に運営している企業であり、利用している端末も少ないことから、情報セキュリティ対策実施の必要性を強く感じてこなかったが、社会的に情報セキュリティ対策を高度化させることが企業に求められていると感じたことも、導入を決めた理由である。

また、当社は従業員数が少ないこともあり、これまで情報セキュリティ教育を実施してこなかった。今後、全社的に対策を強化していくにあたり、従業員へ啓発も実施する必要性があると考えている。

情報セキュリティ対策の効果

情報セキュリティ対策を実施しても、目に見える効果が実感できないため、その必要性を感じられず、具体的な取り組みに結びつかなかった。しかし、従業員がフィッシング詐欺の被害にあった事例を振り返ると、被害にあう時は突然であり、会社で使用している端末を経由して情報セキュリティ被害にあってしまうと、業務にも大きな支障が出てしまう恐れもある。また、取引先とのやり取りにおいて、電子契約やオンラインでのファイルのやり取りを行う機会は少ないものの、クラウド上の情報管理を行う機会は増えてきているほか、オンライン会議ツールを活用する機会も増加している。そのため、情報セキュリティ対策実施により、被害にあう可能性を低減させることができている、という安心感は得られている。

小規模な企業においては、どういった対策を進めるべきか判断することが難しく、対策を充実させていくことは容易ではない。実際のところ、自社で行っている対策として、被害にあった際の報告方法等、組織的な対策は実施できているものの、従業員それぞれの意識向上といった人的な対策や、当社が抱える情報セキュリティ上のリスクを回避するための技術的な対策については、まだ取り組みを始めたばかりの段階である。そのため、外部の IT 関連業者にも相談しながら、対策を進めていくことが必要と考えている。

対策･投資多

「情報セキュリティ対策を取引条件として要請」

▼会社概要

所在地	北海道
従業員数	21～50 名
業種	サービス業・**その他**
実施している対策	● 情報セキュリティ対策レベルが一定以上の企業との取引のみ実施。 ● 従業員教育として、基本的な情報セキュリティ対策を日々周知。

情報セキュリティ対策の取組

当社は北海道で生活関連サービス業を営んでいる。個人向け事業も行っており、個人情報を取り扱う必要がある。そのため、情報セキュリティ対策への意識･関心は高く持っている。対策にあたっては、関連会社から要請を受け、その要請内容に沿った情報セキュリティ対策を実施している。自社で使用する端末やシステムは、関連会社から提供されるものを使用しており、自社でそれらシステムのセキュリティレベルを判断し、使用有無を決定するといった意思決定は行っていない。ただし、自社の通信に係る費用は負担する必要がある。また、Windows ライセンス料については、関連会社から使用する端末の台数に応じて、一定の負担が求められている。

個人向け事業であっても、事業の推進に当たり必要な備品･資材を購入するため、企業との取引も一定程度発生している。その際、当社から情報セキュリティ対策上の要請を行うことはないが、関連会社から許可された事業者としか、取引を行うことが認められていない。関連会社から許可された事業者については、情報セキュリティ対策についても一定以上の水準であることを確認できた企業であると聞いている。そのため、自社主導の取り組みとはいえないものの、取引先への情報セキュリティ対策上の要請を間接的に行うことはできていると考えている。

従業員への情報セキュリティに関する教育も、関連会社から要請された内容に沿って実施している。内容は、「外部からの問い合わせメールの中にある迷惑メールをむやみに開かないようにする」といった基本的なものであるが、社内の担当者が内容の周知を日々行っている。

情報セキュリティ対策の効果

従業員の情報セキュリティに対する意識が向上していることが最大の効果でありメリットである。当社は、個人の顧客と直接対面する場面もある業態であるため、情報管理への意識が低くければ、顧客にも態度で伝わってしまい、不安な思いをさせてしまう恐れもある。組織が情報漏えいや、サイバー攻撃の被害にあわないことも重要だが、情報セキュリティ上の課題に対して、組織的な対策を行っている様子を従業員に対して見せることで、従業員への意識づけを行っていく効果は期待できると考えている。

今後、情報セキュリティ対策を進めていくにあたっては、引き続き従業員への普及啓発が取り組みの中心になることを想定しているが、どうしても必要性を説明するだけでは、心の底から理解してもらうことは難しいと感じている。そのため、IPA からの情報発信等も参考にしつつ、実際に起きた情報漏えい、サイバー攻撃の事例や、そうした事例が生じた際に、過去の事例では、どういった対処を行ってきたのか、というケーススタディを充実させたうえで、従業員に周知していきたいと考えている。

「情報セキュリティ対策は家の鍵をかけるのと同じ」

▼会社概要

所在地	北海道
従業員数	5 名以下
業種	サービス業・**その他**
実施している対策	● 用途に応じて PC の使い分けを実施。 ● 協業先企業の情報セキュリティ対策状況を把握。

情報セキュリティ対策の取組

当社は北海道で測量を中心にサービスを提供している企業である。建設工事を行う前や設計の前段階に行う事前調査を中心に手掛けている。

情報セキュリティ対策を始めるきっかけとしては、国や自治体関係の仕事を請ける際に情報セキュリティ対策を要請される場面が少なくないことがあげられる。具体的には、国や自治体の業務を請ける際には、国土交通省の地方整備局が設定している基準があり、応札時に評価項目の対象になることもあることから、情報セキュリティ対策に積極的に取り組むようになった。

社内で実施している対策としては、フリーソフトウェア等のインストールを制限している。ルータについても、市販のものではなく、外部の IT 関連業者に相談の上、ファイアウォール等セキュリティ対策が施されたルータを導入している。また、PC は用途別に使い分けるようにしており、すべての PC が外部とつながっている状況にしないように努めている。

各種セキュリティ対策の導入で苦労した点や工夫をした点として、従業員へのセキュリティ対策への理解を得ることがあげられる。情報セキュリティ対策を推進していくと、やはり面倒という印象を持たれてしまう。従業員も、全員がデバイスの操作等になれているわけではない。もともと手書きの図面を作成していた方々も従業員にはいるため、こうした方々にも情報セキュリティ対策の重要性を周知していくことが難しいと感じている。また、情報セキュリティ対策を実施するにしても、新たなソフトウェアやツールの導入や、社内規定の整備を行うと、不便になる印象を持たれてしまうこともある。不便になる点があったとしても、取り組みは必須であると認識しているが、できるだけ、情報セキュリティ対策実施が、これまでの業務の妨げにならないよう、バランス感を持っているように従業員へ見せていくことを意識している。

当社が仕事を請ける際の契約書は、基本的には相手方にあわせることが多く、秘密保持や業務終了後の情報の返却･破棄が求められることは多い。委託先や協業先に対しては、契約終了後の情報破棄や情報セキュリティに関する脅威の可能性の共有といった取り決めや、簡易的な情報セキュリティ対策の実施状況把握のためのチェックシートを送付することがある。

情報セキュリティ対策の効果

ジョイントベンチャーのような形態で仕事を請け負うこともあり、比較的取引先とのやり取りは活発に行っているが、当社の情報セキュリティ対策が好意的にみられているかどうかはわからない。とはいえ、行政機関からの仕事を、情報セキュリティ対策に関する水準により受託できないということはこれまでなく、対策を実施しておいてよかったと感じることもある。情報セキュリティ対策は、家の鍵をかける要領で実施する必要があると考えており、必ずしもメリットを感じられなくても多くの企業が自然と実施していると考えている。

対策･投資多

「認証取得による網羅的な対策を実施」

▼会社概要

所在地	福島県
従業員数	21～50 名以上
業種	サービス業・**その他**
実施している対策	● IPA や報道を通じ、情報セキュリティ被害に関する情報を収集。 ● 認証取得を機に担当者設置やバックアップ方法等を規定。

情報セキュリティ対策の取組

当社は福島県でサービス業を営んでいる。全社的に B2C のビジネスを進めており、主な顧客は個人となっている。

会社全体の情報セキュリティ対策や基準については関連会社のシステム部門が統括して管理を行っている。たとえば、ハードディスク暗号化ソフトウェアの導入をはじめ、セキュリティソフトウェアの導入、Windows Update の対応、情報資産の施錠管理、ハードディスクの破棄時の破砕等がある。このほか、IPA や PC 販売店、商工会議所等から OS のぜい弱性に関する情報やランサムウェア等のウイルス蔓延に関する情報を収集し、従業員に伝えている。万が一被害が出た場合のことを想定し、損害保険にも加入している。想定される情報セキュリティ対策をまんべんなく取り組んでいるところである。

当社の事業のなかには、個人情報を扱う必要があるものも含まれていることから、独自に P マークを取得した。主に B2C のビジネスであるが、顧客から P マーク取得の要請があったわけではない。しかし、行政から業界団体を経由して、P マークの取得依頼があったことや、情報セキュリティの重要性が高まっている社会情勢を踏まえ、取得の必要性を感じて P マーク取得に至った。基本的に会社としての情報システム及び情報セキュリティ対策は関連会社で管理しているため、当社にはシステム担当や情報セキュリティ担当は設置していなかったが、取得に当たっては P マークの担当者を設置した。また、取得に必要な情報収集は、現場の P マークの担当者が中心に行ったものの、申請に必要な情報（通信方法･バックアップの方法等）は関連会社から適宜情報を入手した。P マークの運用は、当社の担当が中心となり、維持･更新に努めているところである。

今後は、PC の対策に加えて、スマートフォンや GPS を用いて社用車の管理等も行う等の取り組みを進めていくほか、従業員への情報セキュリティ教育にも力を入れていきたい。

情報セキュリティ対策の効果

B2C のビジネスの場合、企業顧客と異なり、取引条件に P マーク等が記載されているわけでは無い。このため、P マークを取得しないことで、直接的に事業機会が喪失する等の影響はないかもしれない。しかしながら、管理をしっかりやることで顧客に対して安心を与えることができる。

また、万が一の時に備えるために、事業継続計画（BCP）の策定･運用にはかなり力を入れている。その一環として、損害保険にも加入している。損害保険を実際に利用する機会はこれまでにはなかったものの、仮にトラブルが起こった場合に、その対応のための弁護士費用等のサポートを受けるような内容となっている。こうした情報セキュリティの対応は対外的にアピールできている。

対策･投資多

「デジタル化のメリットを守るための情報セキュリティ対策」

▼会社概要

所在地	茨城県
従業員数	5 名以下
業種	サービス業・**その他**
実施している対策	● ソフトウェアの最新化や不審メールを開かないといった基本的対策。 ● 生体認証機能付き端末の使用。

情報セキュリティ対策の取組

当社は茨城県で企業向けにシステム開発を手掛けている。当社の顧客の中には、許認可を受けて事業を行う規制産業も含まれているため、行政との結びつきもある。行政への対応に当たっては、紙での申請･確認や、現地確認を基本とする文化が残っており、意外とデジタル化されていない印象もある。規制業種の顧客へ提供するシステムへのセキュリティ上の要求は厳しいため、情報セキュリティ対策への関心は以前から高かった。複数の顧客と取引を行っており、自社の情報管理体制や情報セキュリティ体制について、取り組みが十分であるか、ヒアリングを受けることも多い。求められる項目はチェックシート形式で記載されており、確認の上、問題なければ取引に至るという流れである。ただし、極めて厳しい基準が設けられているわけではなく、厳格にチェック項目が確認されているわけでもない。そのため、このチェックにより、サプライチェーンセキュリティが高度化しているかというと疑問符が付く。

ルータが攻撃を受けることには危機感を持っていたため、ルータのパスワード変更を定期的に行う対策を実施している。また、Windows Update や各種ソフトウェアのアップデートも欠かさず取り組むようにしている。その他の対策として、迷惑メールが疑われるものについては絶対に開かないようにすることや、生体認証機能が備え付けられている端末を利用すること、端末のパスワードも定期的に難しい文字列で変更していくといった対策は実施している。

情報セキュリティ対策の効果

これまで情報セキュリティ上の被害にあった認識はなく、初歩的な対策を実施してきたことで、重要情報を保護し、取引先に迷惑をかけずに済んでいると考えている。

情報セキュリティ対策単体に視野を向けてしまうと、対策実施によるメリットを感じることは難しい。そのため、デジタル化を積極的に推進し、デジタル化によって享受できるメリットを情報セキュリティ対策により守る、という認識で取り組んでいる。自社においても、以前は紙による契約を結んでいたが、大手企業に対しても当社主導で電子契約による契約を依頼し、実際に電子契約に切り替えることができた。情報漏えいの懸念等から、契約書等を紙でやり取りしたい事業者の気持ちもわかるが、事業所が火事にあってしまうと紙は燃えてなくなってしまうし、施錠管理していても盗難にあった場合にどこに流出したのかを追うことが難しい。デジタル化し、ファイルにアクセスした時間や PC のログをとっていくことの方が、情報管理上の安全性も高いと考えている。情報セキュリティ対策実施によるメリットを追求するのではなく、デジタル化のメリットをしっかりと守っていくための取り組みの一環として、今後も情報セキュリティ対策を進めていきたい。

対策･投資多　取引先要請多

情報セキュリティ対策は会社の「保険」

▼会社概要

所在地	東京都
従業員数	51～100 名
業種	サービス業・**その他**
実施している対策	● 取引先の監査や助言を活かして、対策を実施。 ● 情報セキュリティ対策や個人情報保護に関する IPA の資料を用いて従業員教育を実施。

情報セキュリティ対策の取組

当社は東京都で OA 機器等の販売やメンテナンス保守を実施するサービス業を営んでいる。

情報セキュリティ対策を実施するきっかけは、2010 年頃から 2017 年頃までに行われた、取引先からセキュリティ監査である。これは他社で起きた情報セキュリティ被害や P2P ソフトウェアによる流出事件の多発、個人情報保護法等を背景として実施されたものであり、情報セキュリティ対策に関して、取引先から様々なご助言をいただいた。

具体的な取り組みとしては、施設への入退出管理や書類の施錠管理、セキュリティワイヤー等による機器の固定、事業継続計画(BCP)の策定等、多岐にわたる。取り組み内容に関しても、定期的な見直しを図っている。また、ISMS や P マークについても取得をしている。

高いレベルの情報セキュリティ対策を実施しているのは、取引先からの要請やガイドラインによる側面も大きい。たとえば、P マークの取得に関しても、要請があったため対応している。取引先から、取り組みを行う上で必要なソフトウェアについて無償で提供される場合もある。ガイドラインについては定期的に更新をしており、新たな脅威や法整備により必要な対策を追加することもある。なお、当社から別の企業に再委託する際にも同様の内容を確認することを社内規程で定めている。

高い水準の情報セキュリティ対策を実施していると自負しているが、人的なミスや従業員の油断といった点には気を付けたいと考えている。たとえば、何か作業をする際にファイルをローカルドライブに保存した方が作業はしやすいものの、情報漏えいのリスクが高くなる行為と言える。他にも紙資料や端末の暗号化は実施しているものの、万が一紛失やパスワードの流出はリスクとして意識している。

そこで、従業員教育も積極的に実施している。実施している教育は大きく 3 点あり、取引先の IT 企業からの研修、情報セキュリティ対策全般の研修、個人情報保護に関する研修である。後者 2 点については、IPA の資料を活用している。IPA の資料は、従業員教育には最も適していると考えている。

情報セキュリティ対策の効果

情報セキュリティ対策は業務を行う上で必要不可欠な取り組みである。現在も高い水準の対策を実施しているつもりではあるが、当たり前であるという意識の下で実施している。

言うなれば、情報セキュリティ対策は保険のようなものである。仮にセキュリティソフトウェアをインストールすることで、端末の動作が多少遅くなることがあったとしても、業務の実施の上で非効率だといったことは考えるべきではないと考えている。

取引先要請多

「情報セキュリティ対策による信頼獲得は契約獲得につながる」

▼会社概要

所在地	東京都
従業員数	21～50 名
業種	サービス業・**その他**
実施している対策	● 端末の情報セキュリティ対策の徹底。 ● 認証取得と、定期的な内部監査、PDCA 管理の実施。

情報セキュリティ対策の取組

当社は東京都で国内･海外旅行の企画をおこなう旅行会社を営んでいる。

旅行会社であるため、顧客の個人情報を取得する必要がある。特に、海外旅行については、本籍地、病歴、保険の加入状況といった、扱いに細心の注意を要する情報も管理する必要が出てくる。そのため、情報セキュリティ対策は高い水準で行っている。対策の実施にあたっては、関連会社の基準に基づいた対策を行うことを基本としている。

関連会社の基準に準じているため、当社独自の取り組みは少ないものの、十分な対策を実施できていると考えている。経営層も情報セキュリティ対策に対する感度を高く持っており、情報セキュリティ対策の経費は必要経費であるとの認識を持っているため、手厚い情報セキュリティ対策を長年実施してきたという自負がある。

具体的な取り組みとしては、プログラムインストールの制限や PC 等の情報端末の固定等を行っている。また、定期的に情報セキュリティに関する内部監査を実施しており、PDCA を回すことで、対策が十分かを確認している。また、P マークも取得しており、取得したことを当社 Web サイトにも表示している他、個人情報保護方針についても掲載を行っている。

情報セキュリティ対策の効果

近年、顧客から契約に際して、情報セキュリティ対策の取り組みについて確認を受けることが増えた。高い意識を持って情報セキュリティ対策を実施していることから、確認を受ける内容は問題なく実施できていることが大半であり、対策の実施状況を確認されるチェックリスト等を提示された場合でも、すべてのチェック項目について対応できていることが大半である。そのため、顧客からも信頼獲得につながり、契約獲得にも繋がっている。

特に、高い水準の情報セキュリティ対策を実施している成果を感じるのが、行政関係の仕事である。行政関係の仕事においては、数ある顧客の中でも、最も高い水準の情報セキュリティ対策が求められる印象である。このような高い水準の情報セキュリティ対策を求められる場面であっても、現在の取り組みの水準で問題なく対応できており、実際に受注に至っているケースも多数ある。このように、新たな取引機会が増加したことは、情報セキュリティ対策に取り組んで感じられた大きなメリットであると考えている。

また、情報セキュリティ上のトラブルを未然に防げているのではないかと考えられることも、対策を実施していることによる効果の1つであると考えている。

対策･投資多　取引先要請多

「全従業員で規定を策定・推進するセキュリティ体制を構築」

▼会社概要

所在地	岐阜県
従業員数	21～50 名
業種	サービス業・**その他**
実施している対策	● 取引先の要請に基づいた対策の実施。 ● 認証取得を目指して情報管理体制の整備を実施。

情報セキュリティ対策の取組

当社は岐阜県で測量と設計をおこなうサービス業を営んでいる。昨今では、「i コンストラクション（建設現場に ICT を活用して、生産性を高める取り組みを指す）」の流れから、ドローンや測量機器等のデータから図面化して行う業務が増えてきている。業務は、公共事業が多くを占め、国･自治体から直接受注する場合もあれば、民間企業から再委託で受託する場合もある。民間企業や官公庁･自治体との契約においては、情報セキュリティ対策について要請されており、特に大手の建設会社からの要請はある程度厳しい内容のものも多い。当社が扱うデータは、顧客の保有する機密情報に加えて、個人情報も取り扱う場合がある。こうした中、データのやり取りについて、物理的なメディアからメールやその他の手段によるやり取りが増えてきており、これまでとは異なる形での情報漏えいリスクも高まっている。そのため、当社の情報セキュリティ担当としては、具体的な改善策を検討している。

情報セキュリティ対策は、社内の情報セキュリティ担当が担い、関連する規定を策定してきた。現在は、ISMS の取得を目指して、社内の関連規定の整備を進めている。この規定の策定にあたっては、情報セキュリティ担当のみで検討するのではなく、現場の従業員にとって現実的かつ実効性があるものにするため、人的対策･情報資産管理･アクセス制御･IT 機器の利用等の項目ごとに社内の各部署を2つ程度のグループ分けをして、各従業員が各担当に属して一緒に検討し、より精緻な規定の整備を進めている。規定を現場のメンバーでも精査することで、「自分たちで議論して決定したからには積極的に取り組んでもらう」ように各従業員には依頼している。

また、現場の従業員が考えることで様々な発見をすることができる。たとえば、PC のデータは、暗号化して万が一に備えるようにしている。しかしながら、測量機器の中には暗号化に対応しておらず、USB メモリで持ち運びする必要があるものもある。そういった場合には、可能な限り当該機材から離れないようにする等ルールとしている。加えて、業務内容によっては外部委託を行うこともあるため、共通仕様書の整備を進めている。

情報セキュリティ対策の効果

現状では、官公庁も総合評価方式（価格に加えて技術や社内体制等も評価に加えた入札方式）による入札や、元請企業からの情報セキュリティ対策に関するアンケートへの回答などに応じているが、どの程度情報セキュリティ対策が評価にされているかは直接的にはわからず、保険のような位置づけでもある。しかし、情報セキュリティ対策を進めることは、取引の上で顧客に安心感を与えることはできると感じている。情報セキュリティに関する規定も、各従業員が慣れるまでは煩雑と感じるかもしれないが、慣れてしまえば、そのルールを守ることで、会社として情報セキュリティ対策をしていると発信できると思う。将来的に、ISMS が取得できれば、具体的に PR のひとつになると考えている。

取引先要請多

「フランチャイズ本部･加盟店の協働による安全な管理体制の構築」

▼会社概要

所在地	和歌山県
従業員数	21～50 名
業種	サービス業・**その他**
実施している対策	● フランチャイズ本部の方針に基づいた基本的対策の実施。 ● アルバイト従業員に向けた独自のセキュリティ講習を実施。

情報セキュリティ対策の取組

当社は和歌山県で店舗を運営する企業であり、フランチャイズで複数店舗を展開している。

情報セキュリティ対策はフランチャイズ本部企業の方針に基づいて実施している。店舗内の Wi-Fi も含む社内のインターネットは本部企業に管理されており、情報セキュリティに関する問題が発生した際も本部が遠隔対応を行う仕組みとなっているため、フランチャイズ加盟店側が被害にあった場合でも本部や他の加盟店に影響が及ぶリスクを低減している。

また、使用しているソフトウェアについても基本的には全加盟店が使用するオリジナルのソフトウェアを導入している。このソフトウェアは加盟店側から意見を収集することで随時改良･更新されているため、加盟店側にとって非常に使い勝手の良いものになっている。こういった新たなソフトウェア導入の際も、本部による PC のリモート操作で導入され、年数回スパムメールの検知結果が届く等、本部によるモニタリングとフィードバックが行われており、情報セキュリティ対策システムの導入･運用面では本部主導でスムーズに実施されている。

一方で、加盟店側でもクレジットカードの決済情報やポイントカードの個人情報等、顧客の情報を管理するため、加盟店における独自の情報セキュリティ対策は必要である。そのため、当社では年に 1 回、従業員を対象として情報セキュリティ対策に関する講習を行っている。たとえば、「PC をログインした状態で離席しない」といった対策を周知し、従業員の情報セキュリティ対策への意識向上に努めている。またアルバイトに対しても、事例を用いた情報漏えいのリスクの説明等の当社独自の講習を契約時に受講してもらうこととなっている。この講習も一度きりではなく、契約更新の際には再度受講する必要がある。アルバイトであっても店舗で直接個人情報を扱うため、情報セキュリティ対策に関して入念な指導を行っている。

それ以外にも、店舗側はごみ収集業者やメンテナンス業者等に業務を委託する必要がある。たとえば、ごみ収集業者は店舗内に入ることとなるため、鍵の受け渡しに関する条項等、契約書にはセキュリティに関する項目を記載し、対策を行っている。

情報セキュリティ対策の効果

フランチャイズ本部企業による非常に強固な情報セキュリティ対策の導入と、モニタリング･フィードバックの支援があることによって情報漏えい等のリスクが極小化されているため、一般的な中小企業と比較して情報セキュリティの面では安心できる。ただし、当社側で情報セキュリティ被害があった場合は、本部･その他加盟店へ被害が拡大する恐れがあり、そのような事態となった場合は加盟店である当社も責任を負わなければいけない可能性がある。現状は、本部主導で導入されたソフトウェア等の改善に協力しつつ、自社主導の対策をできるだけ実施することで、フランチャイズ全体のより安全な情報セキュリティ対策の体制が構築され、安心して営業することができている。

対策･投資多　取引先要請多

「販路拡大のために取引先から求められたセキュリティ対策を実施」

▼会社概要

所在地	滋賀県
従業員数	5名以下
業種	サービス業・**その他**
実施している対策	● UTM を導入して統合的なセキュリティ対策の実施。 ● 個人向けネット販売実施のために個人情報管理を徹底。

情報セキュリティ対策の取組

当社は滋賀県でサービス業を営んでいる。法人となる前は個人経営で操業しており、その時期を含めると創業からかなり経過している。飲食サービスを提供している他、インターネットを通じた販売や、店舗周辺へのデリバリー業務も行っている。自社内で使用している IT 端末は、PC やタブレット、スマートフォンがそれぞれ複数台程度であり、主に、仕入れ管理やデリバリー関連業務で活用している。店舗での飲食サービスの提供のみを行っていたころは、IT を活用する機会は少なかったものの、最近では、インターネットを通じた販売や、デリバリー業務にも力を入れるようになっており、IT を活用する機会が増加傾向にある。また、売上情報や顧客情報等もシステム上で管理するようにしている。こうした IT 端末の導入やシステム構築にあたっては、IT 導入補助金等の行政支援も活用してきた。

情報セキュリティ対策は、主に社外に委託して実施している。これまで複数回、会社として保有する法人向けクレジットカードの不正利用を受けた経験がある。不正利用については、カードに付帯する保険で対応したため、実際に損害を受けたことはないが、誰であっても被害を受ける可能性があることを痛感し、特に、決済に関わる業務については、セキュリティを強化しておく必要性を感じていた。そこで、情報セキュリティ対策は社外に委託し、UTM(Unified Threat Management)の導入を行った。

その他、迷惑メールが来る機会も多く、変なメールをうっかり開いてしまうことがないよう気をつけている。

インターネットを通じた販売にあたっては、一部の企業から、契約上、一定以上のセキュリティ対策を行うことが求められている。特に、個人情報の管理については厳格に行うよう求められており、対策を実施していなければ、契約を結ぶことができなかったかもしれない。

情報セキュリティ対策の効果

インターネットを通じた販売にあたっては、大手百貨店や大企業の EC サイトと連携することができている。また、しっかりと情報管理を行っていなければ、EC サイトを経由し、顧客や見込み客向けにダイレクトメールを送ることができない企業もある。そのため、販路を拡大･多様化するための企業との連携を、情報セキュリティ対策をしっかり行うことで実現できたことは、情報セキュリティ対策実施のメリットの 1 つであると考えている。

個人情報等の漏えいは、起きてしまうと大問題になりかねないが、アナログな管理を行っていると、どうしても漏えいリスクが高まってしまう。そのため、できる限り仕組化し、漏えいリスクを低下させる必要がある、という考えのもと、今後も情報セキュリティ対策を進める必要性を感じている。しっかりとセキュリティ対策をしないと、万が一の事故や事件が起きてしまう可能性があるため、今後も気を緩めず対策を進めていきたい。

被害有

「会社規模に関わらず、不正アクセスの攻撃対象に！」

▼会社概要

所在地	兵庫県
従業員数	5～20 名
業種	サービス業・**その他**
実施している対策	● セキュリティ監視サービスの利用やアクセス制御の実施等の基本的対策は従前より実施。 ● 不正アクセス事案をきっかけとして、不正アクセス対策を強化。

情報セキュリティ対策の取組

当社は兵庫県で廃棄物の処理や収集運搬を中心としたサービスを提供している。

以前から、セキュリティ監視サービスの利用やアクセス制御の実施等、基本的な情報セキュリティ対策は実施していると自負していた。しかし、今年に入って、さらに一段階高い情報セキュリティ対策を実施することとなった。

対策の高度化を行った理由としては、具体的な被害はなかったものの、当社に対する不正アクセスが認められたためである。

不正アクセスの経緯としては、HP を作成している外部のHP作成･管理サービスにログインしたところ、本来動作するはずのトップページが動かず、画面表示がおかしいことに気付いた。そこでサービスを提供している事業者に問い合わせを行い、急遽アクセス制御を実施した。サーバへの安全なアクセス環境を確立し、当社が設置していないファイルを削除し、HP のコンテンツの復旧作業を行うこととなった。

結果として、当社の顧客や関連会社に影響･被害が出なかったことが不幸中の幸いであった。

情報セキュリティ対策のポイント

当社のように規模の大きくない会社に対して、不正アクセスによる攻撃が行われるとは考えていなかったため、驚いたというのが正直な感想であった。これを機に、更なる対策を実施しなければならないと感じ、ルール等の見直しも行った。

今回経験した不正アクセス事案は、いわゆる「辞書攻撃」によるものであったと分析している。そこで、同様の被害を防ぐために、ID やパスワードは辞書攻撃でも破られないような文字列に変更を行った。さらに、関連会社で同じものを使用していたが、それぞれ別のものに変更を行った。

さらに、IP アドレスの制御を行うように設定を行い、社外からのアクセス自体を受け付けないように設定を変更することで、二重三重の対策を行うこととした。

また、外部サービスのアップデートルールは特に定めていなかったため、最新版へのアップデートを義務付けることとした。同時期に利用しているサービスのマイナーアップデートは自動化されたため、基本的にはそれに従うこととしている。ただし、仕様が大きく変わるメジャーアップデートに関しては、不具合がないか、問題なく動作するか調査や試行を行った上での実施としている。

今回の事案を通して、これまでルール化できていない部分が浮かび上がり、根本から見直す良い機会となった。

対策･投資多

「社内体制の構築の一環としての情報セキュリティ対策を実施」

▼会社概要

所在地	愛媛県
従業員数	21～50 名
業種	サービス業・**その他**
実施している対策	● IT 関連業者に意見を求めながら情報セキュリティ対策を推進。 ● 兼務の担当者の設置や、有事の際の報告体制を内規で定める。

情報セキュリティ対策の取組

当社は愛媛県で生活関連サービス業を営んでいる。主な顧客は個人であり、企業間取引は多くない。

情報セキュリティ対策は、IT 関連業者からの提案を受け、社内で検討し、製品･サービスの導入を決める形で進めることが多い。特に重視している対策があるわけではなく、基本的に求められている対策を実施している。しかし十分な対策ができているかと問われると、必ずしも自信を持てない部分もある。会社として、情報セキュリティ対策を実施することは当たり前である、という認識のもと、IT 関連業者にも意見を求めながら情報セキュリティ対策を進めている。情報セキュリティを専門とする担当者はいないものの、兼務の担当者を任命し、担当者主導による対策を進めている。

情報セキュリティ対策を業者に任せきりにするのではなく、社内体制の構築や報告体制の構築には力を入れている。たとえば、有事の際の報告体制として、経営者、責任者、関係先、業界団体も含め、報告ルートを細かく内規で定めている。情報セキュリティ上の被害にあったことが疑われる場合には、情報セキュリティ以外の有事の際の報告ルートと同様の報告を行うよう、従業員には求めている。

サプライチェーンセキュリティ対策という観点では、自社から業務を委託することはほとんどなく、取引時における情報セキュリティ対策上の要請を受けることもない。

情報セキュリティ対策の効果

これまで特段大きな情報セキュリティ関係の被害にあったことはないと認識しており、被害に合っていないこと自体が、情報セキュリティ対策を実施してきたメリットの 1 つであると考えている。定期的に社外の IT 関連業者から話を聞き、必要と感じた対策を都度導入していることも、被害を受けないことに寄与しているのではないかと考えている。

また、各種情報セキュリティ対策を推進してきたことにより、従業員の情報セキュリティに関する意識レベルも向上したと感じている。業態の特性上、個人情報を扱う場面もあるため、従業員一人ひとりが情報管理に対する意識を強く持っておく必要があると考えている。IT 関連業者にも話を聞きつつ、情報セキュリティ対策を実施している様子を従業員が見ていることも、全社的な情報セキュリティの意識向上に寄与している。

情報セキュリティ対策の必要性を認識したとしても、自社単独で情報セキュリティ対策の企画･実行を進めていくことには限界がある。そのため、社外の IT 関連業者からも話を伺い、最新の情報セキュリティ被害に関する知識も得つつ、自社の状況も分析し、対策に必要なコストと得られるメリット･安心を天秤にかけ、意思決定していきたいと考えている。

対策･投資多

「自社にできる情報セキュリティ対策の把握が重要」

▼会社概要

所在地	愛媛県
従業員数	1～5 名
業種	サービス業・**その他**
実施している対策	● パスワード設定やアクセス制御、バックアップ等の基本的対策を実施 ● まずは費用負担の小さいツールから導入。

情報セキュリティ対策の取組

当社は愛媛県で生活関連サービス業を営んでいる。近年はソフトウェア関連の仕事が増加しており、情報通信業も営んでいる状況である。

ソフトウェア関連の業務を通じ、情報セキュリティ対策に関する情報に触れる機会も増えてきたことで、対策の必要性を痛感し、慌てて取り組み始めたところである。

基本的な対策として、端末へのパスワードの設定やアカウントごとのアクセス制御、重要なシステムのバックアップ、といった対策にまずは取り組んできた。必要性を感じた「セキュリティ監視システム」や、「ぜい弱性診断システム」については、外部の IT 業者からツールを購入し、導入している。小規模に経営しているため、大掛かりな情報セキュリティ対策の実施や、外部の IT 業者に大掛かりに委託することを前提とした対策の実施は難しい。それでも、せめて簡単なツール程度は導入しておかなければならないと思い、まず費用負担が比較的小さいツールから導入してきた。情報セキュリティ分野は、攻撃の高度化や技術進歩のスピードが速いため、自社の対策が十分な水準にあるのかどうか、について自信を持ててはいないが、周囲の小規模企業と比較すると、自社は情報セキュリティ対策に積極的なのだと感じる。

取引先企業から、情報セキュリティ対策の実施状況について、確認を受けることもあるが、現時点では、秘密保持の徹底や、業務終了後のデータ破棄を要請される程度にとどまっている。取引先企業から受ける要請の中で、極端に負担を感じた経験はないが、これからより多くの対策が求められることが一般的になっていくのであれば、日々の情報セキュリティ対策レベルを上げていく必要性があるのではないかと感じている。

情報セキュリティ対策の効果

各種対策を行ってきたことで、従業員の情報セキュリティに対する意識が向上していることが、最大のメリットであると考えている。結局のところ、自社に求められる情報セキュリティ対策のレベルはわからず、現時点でどこまで自社単独で対策をすべきなのか、判断することが難しい。そして、しばらくこの傾向は続いていくと予想している。こうした中でも、情報セキュリティ対策に関心の高い従業員がいてくれることで、最新の情報セキュリティ対策に関する動向を速やかに把握することができ、どこまで自社で対策すべきなのか、他社から本来不要な対策を求められていないか、といった判断を正しく行うことにつながっている。

企業規模が小さいと、取り組むことができる対策にはどうしても限界がある。しかし、対策を実施する必要がない訳ではなく、どこまでなら対策できるのか、ということを常に検討し、実施できる範囲での対策を実施しておく必要性があると考えている。これまで、情報セキュリティ上の被害を確認してはいないが、今後も被害をうけることがないよう、取り組みを進めていきたいと考えている。

参考資料

用語集（事例集掲載分）

No.	用語	内容
1	クラウドストレージ	インターネット上でデータを保存・共有できるサービス。
2	VPN	あたかも自社ネットワーク内部の通信のように、自宅や外出先などの遠隔地の拠点から安全に社内ネットワーク（社内 LAN）にアクセスが行える技術のこと。
3	Windows Update	マイクロソフト社の Windows に関して、製品の発売以降に見つかったセキュリティ上の問題の修正のための更新プログラム。
4	セキュリティパッチ	ソフトウェアにセキュリティのぜい弱性が発覚した時に配布される修正プログラム。最新のセキュリティパッチを適用すると、ぜい弱性から守られる可能性を高められる。
5	サーバ	他のコンピュータから要求や指示を受け、求められた情報や処理を行う役割を持つコンピュータやソフトウェアのこと。
6	ぜい弱性	プログラムの不具合や設計上のミスが原因となって発生した情報セキュリティ上の欠陥。
7	e ラーニング	インターネットを利用した学習形態。対面の講義ではなく、パソコンやコンピュータネットワークなどを利用して教育を行う。
8	インシデント	事故の一歩手前の重大な結果に繋がりかねない出来事や状況や異変のこと。例えば、情報システムの運用や個人情報の管理に支障を来すような事態に陥りかねない状況等を指す。
9	ISMS	企業における情報資産を脅威から守り、適切に管理を可能にする仕組みのこと。国際規格に基づき、日本でも国内規格が発行されている。
10	プライバシーマーク（P マーク）	個人情報の保護体制を構築している事業者に対する認証制度。個人情報の取扱基準をクリアした事業者に対し、プライバシーマークの使用が許諾される。
11	バックアップ	データやプログラムの紛失や損失、破損などに備え、データのコピーを別に保存すること。
12	ファイアウォール	外部からの通信に対して、通信のあて先の情報の確認等を行い、不正が疑われる場合に侵入を防ぐ仕組み。
13	フィルタリングソフトウェア	不正な Web サイトや有害な Web サイトへのアクセスを未然に防ぐためのソフトウェア。
14	クライアント PC	サーバにサービスを要求し、サーバからのサービスを受け取る PC のこと。
15	スパムメール	大量に繰り返し送られる迷惑メールのこと。
16	（コンピュータ）ウイルス	パソコンへの攻撃や情報の窃盗を目的に、悪意を持った人間が意図的に作った不正プログラム。電子メールやホームページ閲覧などによってコンピュータに侵入する。
17	DoS 攻撃、DDoS 攻撃	ウェブサイトやサーバに対して過剰なアクセスやデータを送付するサイバー攻撃のこと。1 台の機器からの攻撃を DoS 攻撃、複数の機器から大量に行うことを DDoS 攻撃と呼ぶ。
18	標的型攻撃	メールの添付ファイルやウェブサイトを利用してパソコンにウイルスを感染させ、そのパソコンを遠隔操作することにより、特定の組織や企業の重要情報を窃取する手法。
19	不正アクセス	アクセス権限を持たない者が企業のサーバや情報システムの内部へ侵入を行う行為のこと。
20	SECURITY ACTION	中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度。取組段階に応じ、「一つ星」「二つ星」のロゴが設定されており、無料で使用することができる。
21	P2P	複数のコンピュータ間が互いに対等な関係で通信する形式。
22	ランサムウェア	コンピュータウイルスの一種。PC を使用不能にした後、元に戻すことと引き換えに「身代金（ランサム）」を要求する不正プログラムのこと。
23	UTM（Unified Threat Management）	コンピュータウイルス・サイバー攻撃等の脅威から、統合的にネットワークを保護する管理方法やそのシステムのこと。
24	MDM（Mobile Device Management）	ビジネスで使用するスマートフォン等のシステム設定やセキュリティ対策を統合的に管理する方法やそのシステムのこと。
25	BitLocker	Windows に搭載されているデータ保護機能の一種。
26	IP アドレス	インターネットに接続されているコンピュータを特定し、通信するために必要となるアドレスのこと。
27	閉域網	主に通信事業者などが提供する不特定多数からアクセスができない形で構築されるネットワークのこと。