「令和 2 年度中小企業サイバーセキュリティ対策促進事業
（関西サイバーセキュリティ促進強化事業）」
関西におけるサイバーセキュリティ対策の実態把握（ヒアリング調査結果）

調査概要

主催：経済産業省近畿経済産業局（事務局　一般財団法人関西情報センター）

調査目的：サイバーセキュリティの取り組み内容やサイバー攻撃の被害実態・対処内容、支援機関への要望等について、またテレワークの実施上の課題や要望等について、アンケートでは得られない個別具体的な取り組み事例を把握・分析するため。

調査期間：2021 年 1 月～3 月中旬

調査方法：Web 会議システム、もしくは電話により実施

調査対象：アンケート回答企業のうち、回答内容を踏まえ、下記条件に該当する企業を抽出

・セキュリティ対策・テレワークにおいて、先進的、特徴的な取り組みを行う企業（アンケート回答を総合的に判断）

・サイバーセキュリティ対策をこれまで実施していない企業

・ランサムウェア等マルウェアによる攻撃、被害が見られた企業　等

調査数：100 社

調査結果のまとめ

１．サイバー攻撃の被害状況及び被害への対応

【サイバー攻撃の被害状況】

・アンケート調査結果と同様に、ウイルス添付メールや標的型メール攻撃、ランサムウェアによる攻撃・被害事例が多く見られた。

・被害内容は、一部ファイルの暗号化や社内 PC へのウイルス蔓延、大きな被害を受けたケースでは、ランサムウェアにより基幹システム・工場の停止に至った事例も聞かれた。

【サイバー攻撃への対応】

・対策事例として、ネットワークの見直しや二段階認証・EDR（Endpoint Detection and Response）の導入、社内ポータルやメールシステムを活用しての注意喚起やテストメール送信による訓練の実施などが挙げられた。

【セキュリティ対策未実施企業の状況】

・セキュリティ対策の未実施企業においては、自社が攻撃を受けているかどうかも分からないとの意見も聞かれ、セキュリティ状況や、対策を実施しない場合のセキュリティリスクの「見える化」を行うための取り組みが必要。また、未実施企業でもセキュリティについて全く意識していないわけではなく、今後の状況に応じて対策を広げていく必要を感じている企業も見られる。

２．サイバーセキュリティ対策の相談先及び具体的な相談内容、公的支援機関の活用状況や期待すること

【セキュリティ対策の相談先、具体的な相談内容】

・セキュリティ対策の相談先として、システムベンダやセキュリティベンダに加え、グループ企業間や業界団体内での相談事例も見られる。

・日頃から付き合いのあるシステムベンダ、セキュリティベンダに対し、セキュリティ対策全般について相談・依頼を行っている。困りごとや問題があれば、その都度、当該問題について相談している。

【公的支援機関の活用状況、公的支援機関に期待する役割】

・公的支援機関には情報提供への期待が高い。中でも、具体的な運用やインシデントに関する事例提供を望む意見が多数。事例提供に当たっては、分かりやすく、一元化された情報発信が求められる。

３．セキュリティコミュニティへの参加状況

・セキュリティコミュニティについて、存在を知らないものの、今後案内があれば是非とも参加してみたいとの意見が多く聞かれた。セキュリティコミュニティに関する情報発信が今後の課題である。

４．テレワーク実施に関する考え方、今後の実施方針

【テレワーク実施の課題】

・テレワーク実施の阻害要因は、紙ベースの業務への対応が難しい点、就業規則、IT 規則が未対応であること。

【テレワークの未実施理由】

・テレワークの未実施理由は、製造部門があり実施業務や部門が限定されること、IT インフラの未導入・導入コスト捻出が難しいこと。

・テレワーク推進に向け、様々な勤務形態に応じたガイドラインの公表、テレワークで必要となる IT インフラに対する補助等が求められる。

５．その他

・取引先や顧客、関係会社等と連携してのサイバーセキュリティ対策（サプライチェーン・セキュリティ）は多くの企業が実施に至っていない。未実施理由は、対象企業が多数に渡るとともに中小企業が多く、対応が難しいため。

調査結果

１．サイバー攻撃の被害状況及び被害への対応

アンケート調査において、これまで受けたサイバー攻撃の手口として、ウイルス添付メールの受信、ビジネスメール詐欺、標的型メール攻撃等が多く見られることを踏まえ、具体的な被害状況や被害への対応を尋ねた。また、セキュリティ対策未実施企業を対象に、未実施理由やサイバー攻撃の被害状況等を尋ねた。

①サイバー攻撃の被害状況

・アンケート同様、ヒアリングにおいても、ウイルス添付メールや標的型メール攻撃、ランサムウェアによる攻撃・被害事例が多く聞かれた。被害内容は、一部ファイルの暗号化や社内 PC へのウイルス蔓延、大きな被害を受けたケースでは、ランサムウェアにより基幹システム・工場の停止に至った事例も聞かれた。
・ヒアリング企業では、社内における被害に留まり、社外への被害事例は聞かれなかった。

②サイバー攻撃への対応

・上記の被害を受けて、ネットワークの見直しや二段階認証・EDR（Endpoint Detection and Response）の導入が行われている。
・ウイルス添付メールや標的型メール攻撃の被害を防止するため、社内ポータルやメールシステムを活用しての注意喚起やテストメール送信による訓練を実施する事例が聞かれた。
・セキュリティ投資に当たり、イニシャルコストよりランニングコストが継続的に必要となることが阻害要因となっている。

【ヒアリング企業の意見】（セキュリティ対策実施企業）

・3～4 年前に社外接続用のネットワークにランサムウェアが侵入し、関係ファイルを暗号化される被害があった。被害を受け、ネットワークの見直しを実施。以前は拠点ごとに管理していたものを本社で一元管理し、帯域も共通化した。
・サイバー攻撃の中でも大きな被害を受けたのは、ランサムウェアに感染したことで、基幹システムが停止し、工場が停止するまでに至った。ランサムウェアの現象が発症後すぐに気づき、主なものについては１週間で復旧、優先順位が低いものについては復旧に１ヶ月を要した。具体的な対策については、EDR の導入等である。
・ウイルス添付メールを従業員が開いてしまい、それが社内に蔓延ということがあった。業務上大きな被害は出なかったが、それをきっかけにメールソフトに関しては二要素認証を取り入れ、ID・パスワードだけではアクセスできないようにした。
・社内の PC がランサムウェアに感染し、デスクトップ上の Word ファイルだけが開けない状態となった。また、取引先からのメールのやり取りを装った、マルウェア（Emotet）を含むウイルス添付メールを受信した。メール本文にリンクがあり、クリックすると

Word ファイルをダウンロードする仕組みであった。社内的に全てのマクロを無効にしていたことから実質的な被害はなかった。

・メールサーバでのアンチウイルス・アンチスパムのチェック、ファイルサーバ・PC でのウイルス対策ソフト導入を行っており、ウイルス添付メールのマルウェア検出程度はされているが、感染することなく対処できている。

・全社的にウイルス添付メールが届くことがある。メールシステムで全社員に啓発を実施。攻撃メールが届くと、Web 上の最新情報を添付して社内への発信を行っている。

・詐欺メールの送付があまりにも多い時は注意喚起を社内で実施。また、社内サイトで事象を具体的に公開して注意喚起を行っている。さらに、3 年前より、年 2 回ほど標的型メール訓練を実施している。

・今のところ具体的な被害は無いが、ほぼ毎日のようにウイルス添付メールが届く。社内の人間を装ったメール攻撃もあり、「怪しいメールは開かず削除する」ことを徹底している。

・アンチウイルスソフト導入、ファイアウォールや検知システム導入等の対策は講じているが、従業員に向けた教育実施が十分でない点があると考える。今後は、従業員へのテストメール送信によるメール訓練等を検討している。

・従業員がマルウェアに気づいたり、検知したりした際に問い合わせを行う「セキュリティ窓口」を設置している。

・セキュリティシステムへの投資にイニシャルコストが掛かることについてはリスクを考えると問題視しておらず、むしろ投資すべきであると考えている。しかしながら、問題となるのはこの手のシステムはランニングコストがかなり必要になるところだ。永久にランニングコストが掛かるとなると、どうしても二の足を踏む。

③セキュリティ対策未実施企業における現状

・セキュリティ対策の未実施企業においては、サイバー攻撃の被害事例は聞かれなかった。また、一部企業においては、攻撃を受けているかどうかも分からないとの意見も挙げられた。アンケートにおいて、セキュリティ対策を推進する上での課題として、セキュリティリスクの可視化が困難であることが多くの企業より挙げられているが、セキュリティ対策を推進するためには、セキュリティ状況や対策を実施しない場合のセキュリティリスクの見える化を行うための取り組みが求められる。

・未実施企業においても、「オンラインバンキングを使っているため、銀行が推奨するブラウザのセキュリティ設定等を行っている」企業も見られるなど、セキュリティについて全く意識を行っていない企業に限定されるわけではない。

・アンケート回答時点では未実施であったものの、報道等においてサイバー攻撃の話題が増加していることを背景にセキュリティ対策を始めた企業、また、今後のデジタル化に応じて対策を広げていく必要を感じている企業も見られた。

【ヒアリング企業の意見】（セキュリティ対策未実施企業）
・攻撃を受けたことがないと思われるが、攻撃を受けたかどうかも分からない。
・アンケート回答時点では、セキュリティ対策は未実施であったが、その後メール用のフィルタリングソフトを導入した。ウイルス対策ソフトのみでは不十分だと感じた。これまで特に被害はないが、報道等で最近サイバー攻撃の話題が増えてきていることから、用心しておこうと考えたためである。
・セキュリティ対策は特に実施していないが、オンラインバンキングを使っているので、銀行が推奨するブラウザのセキュリティ設定等は行っている。今後、オンラインバンキングや受発注の範囲がさらにデジタル化されるようなことになれば、対策は広げていかなければならないと感じている。

２．サイバーセキュリティ対策の相談先及び具体的な相談内容、公的支援機関の活用状況や期待すること

セキュリティ対策の相談先として、アンケートではシステムベンダ・セキュリティベンダを挙げる割合が高くなっている。ヒアリングでは、具体的な相談内容や、公的支援機関の活用状況、公的支援機関に期待する役割について尋ねた。

①セキュリティ対策の相談先及び具体的な相談内容
・セキュリティ対策の相談先として、システムベンダやセキュリティベンダに加え、グループ企業間や業界団体内が見られる。
・中小企業を中心に、日頃から付き合いのあるシステムベンダ、セキュリティベンダに対し、セキュリティ対策全般について相談・依頼を行っている。困りごとや問題があれば、その都度、当該問題について相談している。
・ベンダについては、業務システムの導入等で日頃から付き合いのある企業やセキュリティ対策ソフト・機器の提供企業が選ばれる傾向にある。
・大企業を中心に、セキュリティ最新の最新動向の収集にコンサルティング会社の活用が見られる。
・公的支援機関の活用先として挙げられたのは、IPA（独立行政法人情報処理推進機構）、JPCERT であった。具体的には、セキュリティインシデントの報告や、セキュリティの最新動向や事例などの情報収集、また、社内研修用の教材活用など人材育成用途での活用が見られる。

②公的支援機関の活用状況、公的支援機関に期待する役割
・公的支援機関には情報提供（事例紹介、セミナー開催等）への期待に加え、金融支援（補助金、助成金の導入等）、人材育成支援（教育プログラムの提供等）に期待している。

・情報提供については、製品やソリューションに関する情報発信は多く見られるものの、企業におけるセキュリティの具体的な運用やインシデント事例に関する情報は少ない現状にある。また、自社のセキュリティ対策の現状や立ち位置を理解し、適切なセキュリティ対策を取るためにも具体的な事例を参考にしたい。公的支援機関には、中立機関として、企業の現場における実態や具体的な取り組みが分かる事例を収集・公表することが望まれている。
・加えて、サイバー攻撃がますます巧妙になる中、セキュリティ担当者、さらにセキュリティ担当者以外（経営層・マネジメント層など）でも理解できる、最新動向やインシデント事例をわかりやすく解説した、一元化されたポータルサイトを望む意見が聞かれた。公的支援機関によるセキュリティに関する情報発信のさらなる強化が求められている。
・その他、公的支援機関が中小企業にセキュリティ対策の取り組みを広げていくためには、中小企業との間に、日頃から中小企業と近い距離にあり、ノウハウを有するベンダやソフトウェアハウスが入ることで支援を一層広げていくことができるのではないか、との意見が聞かれた。

【ヒアリング企業の意見】
・従来から付き合いがあるベンダに相談し、それぞれの提供するセキュリティツールを必要に応じて導入している。
・電話からネットシステムまで、ベンダに全般を委託している。ソフトのバージョンアップ等もベンダ側がリスク管理し、安全が担保されたものしか使用できないようになっている。何かあれば、すぐに対応してもらえる関係を構築できている。
・UTM を導入しており、何かあった場合はそちらのベンダに相談している。
・セキュリティ対策を含むネットワーク関係をベンダに委託しており、24 時間体制で監視を依頼し、何か問題があれば、情報が来るようになっている。
・システムインテグレータ、システムベンダへの相談は高額のため、相談できていない。
・業界団体を通して共有されるため、個別には実施していない。
・IPA から紹介いただいた情報処理安全士にセキュリティ対策に関する講義を依頼し、受講している。
・基本的には自社で対応しているが、ベンダの提供するセキュリティ診断等を受け、相談を行うことがある。
・社内教育用に IPA の資料を活用する程度である。公的支援機関に求めることは情報提供であり、セキュリティ予算を獲得する際に材料となる数字を提供してほしい。
・セキュリティソリューションは高額であり、導入にあたってどこまで対策を行うべきかを経営層に説得する必要がある。経営層でも理解できる、わかりやすいガイドラインの公表やセキュリティ対策実施事例の紹介等を期待している。
・セキュリティ製品に関する情報提供は多いが、運用面のベストプラクティスに関する

情報提供を、中立機関として行ってほしい。また、様々なガイドラインが公表されているものの、「べき論」ではなく、実際に現場でどう対応しているか、運用・インシデント事例が知りたい。
・セキュリティソフト等は導入しているが、どんどん精巧になっているサイバー攻撃の現状や最新動向がよく分からず、情報を得たい。
・セキュリティに関するニュース等では目にするが、具体的な攻撃例等については情報が不足しており、実態がよく分からない。それらを気軽に確認できる仕組みがあれば望ましい。
・公的支援機関は現状活用していないが、セキュリティ導入にかかるコストの補助金などの支援をいただきたい。
・セキュリティ対策について、大企業のため支援を受けられない。しかしながら、新型コロナウイルス感染拡大以降、売り上げが減少しており、投資できる金額が限られている。大企業も対象とした支援があると望ましい。
・ソフトウェアハウスを巻き込んだ形で、関西地区の中小企業向けにセキュリティ勉強会を実施すべきである。＜中略＞社内にセキュリティ・情報システム担当がいない企業に向けて、いきなりセキュリティに関する支援を行ったとしても、企業側に知識が無いため、実施が難しい。その間にパッケージハウスが入り、巻き込んでいくことで、支援を広げていくことができるのではないか。

３．セキュリティコミュニティへの参加状況

セキュリティコミュニティの認知・参加状況について、アンケート結果では９割以上が認知・参加を行っていない結果であった。ヒアリングでは、認知していない企業の今後の参加意欲や、認知しているものの参加に至っていない企業に未参加の理由を伺い、セキュリティコミュニティの認知度向上、普及啓発のために必要な要素の把握を目指した。

・認知しているセキュリティコミュニティとして、CSIRT 協議会、大阪商工会議所「サイバーセキュリティお助け隊」、「サイバー犯罪に関する白浜シンポジウム」、ベンダのユーザーコミュニティ等が挙げられた。また、存在を知らないものの、今後案内があれば是非とも参加してみたいとの意見が多く聞かれ、セキュリティコミュニティに関する情報発信が重要となる。
・セキュリティコミュニティを認知しているものの参画しない理由として、「セキュリティ担当者は他業務との兼業であるため時間を割くことが難しい」、「参加に当たって業務上の工数が発生するため会社として積極的な推薦が難しい」「業界内で情報交換を行っており参加の必要性を感じていない」ことが挙げられる。

【ヒアリング企業の意見】
・セキュリティコミュニティを認知しているものの、従業員の参加に当たっては工数が発生してしまうこともあり推薦が難しい状況である。加えて、他業務との兼業のため、参加は難しい状態である
・ベンダの開催するイベント、コミュニティに参加することがある。
・かつて「サイバー犯罪に関する白浜シンポジウム」に参画していた。
・セキュリティについて、横連携や異業種間で情報を得られる場があるということを知らなかった。それは無料で参加でき、インタラクティブに交流できるのか。＜中略＞自分が参加できないにしても、自社の誰かを参加させることもできるし、WEB であれば場所も関係ない。ぜひ案内してほしい。
・セキュリティコミュニティの存在については、まったく認識がなかった。セミナー等があればメール等で案内いただきたい。
・セキュリティコミュニティがあるというのを知らなかった。自社の立ち位置等を知りたいので、そういう情報が得られるのであれば参加してみてもよいと考える。
・セキュリティ担当者同士の情報交換としては、業界団体での定期的な会合の中でセキュリティの話題が出ることもある。
・セキュリティについては、業界団体において最新情報の提供、勉強会があり、そちらに参画している。
・小さな業界なので、県内で業界組合に加盟しているのは 1 社だけである。全国レベルでの協会があるが、そういったところへの情報提供は有効かもしれない。

（※地域セキュリティコミュニティ :サイバーセキュリティ関連の教育・普及・啓発や各種勉強会・研修会、地域での人的・組織的ネットワーク拡大に資する活動、市場開拓や受注促進活動などを目的に、地域の企業が参画して自主的に取り組んでいるコミュニティ活動）

４．テレワーク実施に関する考え方、今後の実施方針

テレワークの実施状況について、アンケートでは実施企業の大半が新型コロナウイルス感染拡大以降に急遽実施していることが明らかとなっている。ヒアリングでは、テレワーク実施上の課題や公的支援機関の支援として期待することに加え、テレワーク未実施企業を対象に、未実施理由や阻害要因について尋ねた。

①テレワークの実施状況及び課題
・テレワーク実施の阻害要因は、紙ベースの業務への対応が難しい点、就業規則、IT 規則が未対応であることであり、ペーパーレス化・DX の一層の推進が重要となる。
・新型コロナウイルス感染拡大以前よりテレワークを実施、もしくは試行的に実施暦がある

企業においては、制度化やBYOD（Bring Your Own Device）の推進により、新型コロナウイルス感染拡大のテレワーク実施においても、比較的円滑に移行できていることが明らかとなった。

・テレワーク実施のメリットとして、移動費等の経費削減が挙げられている。一方で、課題として「リモートアクセスへの対応によるセキュリティレベルの低下」「意思疎通や人事評価の難しさ」「ITインフラや実施環境の未整備」が多く聞かれた。特に、「ITインフラや実施環境の未整備」については、個人デバイスを使用する場合に、セキュリティ監視が難しくなること、また従業員のリテラシーが問われるようになることが挙げられている。

・テレワーク推進に向け、様々な勤務形態に応じたガイドラインの公表、テレワークで必要となるITインフラに対する補助等が期待される。

【ヒアリング企業の意見】（テレワーク実施企業）

・新型コロナウイルス感染拡大の影響で導入に踏み切った。そもそも外資系という背景もあり、実施しやすい環境にあったと思う。出張費など営業経費を大幅に削減できており助かっている。他社とも、テレワークにより営業人員を半分にできるのではないかと話していたところである。

・紙に依存している業務が多いのでテレワークでパフォーマンスを出しづらい。また、社内アクセス増加のため、セキュリティの運用基準を下げている。VPN経由での社外アクセスをもともと用意しており、＜中略＞今回のテレワークでは機能を全体的に使えないといけないため、機能制限を外す必要があるとともに、ファイアウォールへもアクセス権限の穴を開けた状態である。

・急遽テレワークを導入せざるを得ない状況であったため、就業規則やIT規則が対応しておらず、パソコンの設定等、在宅勤務者からの問い合わせに対する時間を要した。

・現在はテレワークを実施しているものの、ITインフラやアプリケーションについて不十分であると認識しており、導入のための費用が捻出できないため、継続して実施するかどうか検討している。

・今後の課題として、個人端末からのプリントアウト等、システムでカバーできていない部分での利用者のリテラシー向上の必要性を感じており、教育の実施を計画している。

・課題としては、成果物評価をどうするかが難しいことが挙げられる。営業職は営業成績があるので評価しやすいが、事務系だと成果の評価ができない。

・在宅勤務の対象は事務系（データ分析など）、営業系と言いつつ、家に拘束するだけで仕事ができない状態。請求書、書類などが紙ベースのため、紙がないと仕事ができないことが課題である。

・新型コロナウイルス感染拡大前からテレワークを制度化し、トライアルで実施してきた。緊急事態宣言からは原則テレワークとして対応。＜中略＞もともと制度化していたことが幸いにして、比較的スムーズに移行できた。

・新型コロナウイルス感染拡大前はテレワークの制度がなく、感染拡大後に制度化を行い、推進している。モバイルワーク、BYOD の推進をコロナ禍以前から推進しており、それゆえに円滑に導入できた。
・テレワークに関係するガイドラインは見られるものの、テレワークには様々な勤務形態があり、それぞれのリスクをわかりやすく整理して基準を設けてもらえれば、上層部への説得材料となる。
・テレワークのインフラは準備できていたが、実際にどのように運用しているか、ペーパーレス化など、他社事例やベストプラクティスを知りたい。
・全社員が使用するアプリケーションの予算化が課題。一時的なものであれば良いが、恒常的な導入だと検討が必要となる。予算的にも大きくなるため、経営資源的にすぐに進められない。
・テレワークの実施コスト軽減のため、パソコン、セキュリティソフト、通信環境等、テレワークで必要となる設備を一括で安価に貸し出す仕組みを提供してほしい。

②テレワークの未実施理由

・テレワークを実施しない理由としては、「製造部門（及びその間接部門）がありテレワークを実施できる業務や部門が限定される」、「経営資源の不足（IT インフラの導入コスト捻出が難しい等)」ことが挙げられた。
・通信環境やクラウドの未整備、また、社内規則（個人データの持ち出しを不許可）により実施できない企業も見られる。また、中小企業の場合、従業員数が限られるため、製造部門との兼ね合いで間接部門であっても実施が難しいとの意見が聞かれた。

【ヒアリング企業の意見】（テレワーク未実施企業/実施をやめた企業）
・テレワーク制度を設けたが、現在は実施していない。クラウド等が整備されておらず、顧客との連絡は直接電話で行う必要があるため、出社が必要である。また、中小企業で人員が少なく、テレワークを実施すると他の部署の業務にも支障が出るためである。
・テレワークが出来る環境は整えたが、今も実施はしていない。メーカーであり、工場は機械を動かすためにオペレータ業務が必要なため、テレワークは不可能である。
・緊急事態宣言発令後、急遽テレワークを導入したが、当社の場合、工場勤務者及びその管理部門のため、導入段階でも、管理部門の 10 名弱程度しか実施しておらず、現在はテレワークを実施していない。また、工場の立地的な問題の関係上、高速通信が導入できないこともあり、今後の導入は難しいと考える。
・個人データを持ち出しできないため実施が難しく、今後の実施予定もない。
・テレワークは実施しておらず、今後も導入予定は無い。事務部門はテレワークを実施出来る環境は作っているが、送り状の出力等で問題が有ったので実施はしていない。また、会社は郊外にあり、公共交通機関を使う人は少ない。コロナ禍がもっと著しくなっ

た場合に実施できるように準備は行っている。

５．その他

①サプライチェーン・セキュリティの取り組み状況

・取引先や顧客、関係会社等と連携してのサイバーセキュリティ対策（サプライチェーン・セキュリティ）については、実施していない、また、指示を受けたことがない企業が大半であった。実施しない理由として、「対象企業が多数に渡り、さらに中小企業が多いため対応が難しい」との意見が聞かれた。

・サプライチェーン・セキュリティの実施企業において、具体的な実施内容として、「契約の際に情報保護規約の盛り込み」、「取引先へのアンケート・研修会の実施」、「ISMS 認証・プライバシーマーク（P マーク）上の規程に基づいての実施」が挙げられた。しかしながら、実施企業においても現状では十分な対策を実施できているとは言えないとの回答が聞かれた。

【ヒアリング企業の意見】

・現時点で、発注元からサイバーセキュリティ関連の施策や対策について指示を受けたことはない。

・仕入先には、事業の関係上、ニッチかつ小規模の企業も含み、対象企業も非常に多いこともあって、資材部門がアンケートレベルで確認することもあるが、世の中で求められているレベルまでは行えていない。

・取引先（下請業者）には、セキュリティに関する研修会を開催し、参加を求めている。

・発注先に対して細かいセキュリティ要件を課すということは、契約上の一般的な情報保護の規約・条文以外には特にない。＜中略＞最近、大手企業や病院等の取引先から、会社や製品のセキュリティについて問われることがかなり増えた。そういった際には、グループ全体のセキュリティ対策について説明したり、ISMS 認証を取得していること、情報処理安全確保支援士（登録セキスペ）資格を有する職員が在籍すること等によってセキュリティレベルを確保していることを説明したりしている。

以上