サイバーセキュリティを自分ゴト化する

2025年8月

JCIC客員研究員　澤田雅広

1．はじめに

攻撃者側は常に組織やサービスの隙を狙っており、守る側は新たな技術やデバイスの普及によって防御すべき領域が拡大し続けている。企業としてセキュリティのためのルールや仕組みを整備し、技術的対策を講じていても、時間の経過とともにどこかに隙が生まれ、完全な防御は困難である。一人ひとりの社員がサイバーセキュリティを自分ゴトとして捉えることが、今後の重要な課題である。

どのような大きな事故であっても、実際は些細なことがきっかけで発生することが多い。それぞれを分析すると、わずかな気の緩みや意識の低下が真因として挙げられる。サイバーセキュリティも例外ではない。どれほど堅牢な仕組みを構築しても、組織を構成する誰か一人の油断が外部からの侵入を許す原因となり得る。サイバーセキュリティを強化するためには、社員一人ひとりがその基礎となる意識を持つことが不可欠である。リスクマネージャ[1]にとっては、社員の意識にいかに働きかけるかが課題である。

本レポートでは、サイバーセキュリティを少しでも社員の自分ゴトとするための企業における取り組み事例を紹介する。まず、情報セキュリティ事故を招く心理的要因と、それによって引き起こされる事態の重大性を再確認する。そのうえで、これらのリスクを少しでも減らすための取り組みについて述べる。

2．情報セキュリティ事故にありがちなきっかけ

次に挙げるのは、事故を起こした本人や関係者による事故報告書やヒアリング時によく出てくるキーワードである。

- うっかり
- 自分は大丈夫
- 急ぎだったので
- 誰かがやってくれているはず
- よかれと思って
- 知りませんでした

まず「うっかり」である。例えばメール誤送信などは、慣れや不注意、あるいは疲労による集中力の低下が原因となる単純なヒューマンエラーであり、誰にでも起こり得るものである。人に依存する仕組み自体に課題がある場合もあれば、標的型メール攻撃のように、通常の注意力だけでは識別困難な巧妙な手口によるものもある。

[1] 本レポートでは、サイバーリスクに対応するために、情報セキュリティ担当役員（CISO）やリスク管理担当役員（CRMO）を補佐し、現場部門と連携しながら、セキュリティ統括機能または全社的なリスク管理機能を担う責任者を「サイバーセキュリティ・リスクマネジメントにおけるリスクマネージャ」と定義。以降、文中では「リスクマネージャ」と表記する。組織内のポジションとしては、セキュリティ統括室長やリスク管理室長などが該当。

次に「自分は大丈夫」である。これは根拠のない過信を指し、自分は間違えない、騙されることはないと考えたり、自分が標的になるはずがないとリスクを過小評価したりすることによる油断である。

「急ぎだったので」は、納期が迫っているなどの理由から、通常踏むべき手順を省略した結果、事故につながるケースである。たとえば、「どうしても今すぐ接続テストが必要なので、一時的に設定をパブリックにした」結果、その後に設定を戻し忘れて不正な侵入を許す例などがある。これは、守るべきルールよりも他の要素を優先したことによるものであり、自己判断で通常のルールや手順を一時的に軽視してしまう心理的傾向である。

また、「誰かがやってくれているはず」というケースもある。必要性は理解していても、当事者意識の欠如や無自覚な他者依存、あるいは自分がその役割を担っている認識の不足などが原因となる。さらに、組織全体で役割やプロセスが明確になっていない場合にも、事故につながる可能性がある。

「よかれと思って」は、その逆のパターンである。本来業務上必要のないことを、適切なプロセスや十分な知識を持たずに、善意から独断で行った結果、事故が発生するケースがある。たとえ会社や顧客のために「よかれと思って」行動したとしても、それは業務範囲を逸脱した行為であり、事故を引き起こす要因となりかねない。

最後に「知りませんでした」である。これは、特定のルールが存在すること自体を知らなかったという主張である。本人の責任回避や自己防衛の意図も見受けられるが、リスクマネージャとしては、守るべきルールが現場に浸透していないことへの対策を検討する必要がある。

このようなバイアスや直感的・迅速な思考[2]は、サイバーセキュリティの分野において特に注意が必要である。個人の判断だけでなく、組織全体のリスク認識に影響を及ぼすため、教育や啓発活動による意識の向上が重要となる。

3．社員の意識に働きかける取り組み例

現代の急速な環境変化の中で、企業内のあらゆる業務や事象に対し、リアルタイムでルールや仕組みを整備することは困難である。また、慣れやルール軽視、他者依存といった人間特有の弱点に対して、いかに継続的に対応していくかも大きな課題である。そのため、社員の意識に働きかけ、サイバーセキュリティを「自分ゴト」として捉えるための取り組みが必要となる。ここでは、社員の意識に働きかける具体的な取り組み例を三つ紹介する。

（1）社員一人ひとりの想像力とリスク感度に働きかける

（2）組織長に働きかける

（3）教育・研修担当者に働きかける

---

[2] バイアスなどに関する詳細は、ダニエル・カーネマン『ファスト&スロー　あなたの意思はどのように決まるか？（上・下）』（村井章子訳、早川書房、2012年）を参照されたい。本レポートで取り上げた事例も、カーネマンの理論と整合している。たとえば、「自分は大丈夫」と考える心理は、以下のような認知バイアスと関連している。

- 自信過剰バイアス：人は自分の知識や判断力を過大評価する傾向がある。
- 楽観バイアス：人は自分に悪いことは起こらないと考える傾向がある。

これらのバイアスは、意思決定やリスク認識に影響を与える重要な要素であり、カーネマンの理論に照らして理解することができる。

（1）社員の想像力とリスクに対する感度に働きかける

一つ目は、社員の「想像力とリスクに対する感度」を高める取り組みである。想像力とリスク感度は、すべての社員に必要不可欠な資質である。しかしながら、これらを涵養する汎用的かつ再現性の高い手法は、まだ十分に確立されているとは言い難い。意識の有無やその高さを数値化することが困難であり、効果を定量的に測定しにくいことが一因と考えられる。また、人はさまざまな業務や環境に慣れることで心理的負担を軽減し、効率的に仕事を進められるようになる。その環境が危険であっても同様である。物理的な環境で事故に遭えば痛みを伴うが、サイバー空間においては直接的な痛みを感じることがない。そのため、情報セキュリティ事故に対する当事者意識やリスク感度が低下しやすい傾向がある。

このような状態から少しでも脱却するためには、社員が次のような問いを考える時間を設けることが有効である。

- 自分が扱っている「この情報」が外部に漏えいした場合、何が起きるのか。
- それが個人情報や顧客情報であれば、対象となる個人や顧客はどう感じるのか。
- 漏えいによって自社や自分はどのような状況に置かれるのか。
- 現在の自分たちの情報の取り扱いは本当に安全であるのか、そのままで良いのか。

自分たちが日々取り扱っている情報が、もし外部に漏えいしたら何が起きるのか――。

「そんなことは起きるはずがない」と片付けるのではなく、「もし起きたら」と具体的に想像することが重要である。自分にとっては単なる処理対象であっても、その情報の持ち主である個人や顧客にとっては極めて重要な情報であり、漏えいした場合の影響を真摯に考える必要がある。

さらに、それによって自社や自分がどういう立場に置かれるのかを、できる限り具体的に想像することが求められる。その影響範囲は、対象の個人や顧客だけでなく、事故を起こしてしまった本人、管理・監督・指導すべき立場にあった組織長、ステークホルダーに説明責任は果たすべき社内関係者、さらには報道を通じて知る顧客やパートナー、社員の家族、内定者やその家族にまで及ぶ可能性がある。情報漏洩は、多くの人々の生活や人生に、多大な影響を与えてしまうかもしれない。だからこそ、自社や自分が「必要なことはすべてやっていた」と説明責任を果たせるのかどうかを、あらかじめ考えておくことが肝要である。

このような背景を踏まえ、社員の「想像力」と「リスクに対する感度」を涵養する施策として、各組織において車座会議形式で議論を行うことは有効である。自らの考えや不安を言語化し、共有することで、個々の意識向上が図られる。加えて、発見された課題に対しては、組織内で具体的な改善を実施し、組織を越えたより大きな課題については、組織長から上位層へエスカレーションするルールを設けることで、企業全体の改善につながる。

なお、車座会議形式でのリスクの洗い出しは、際限なく多くの項目を挙げることが可能であり、その分、関係者の負担も大きくなる。そのため、一定の段階で洗い出しを区切る判断も重要である。

（２）組織長に働きかける

二つ目は組織長を対象とした取り組みである。CISOがどれほどメッセージを発信しても、社員全員に確実に届けることは極めて難しい。社員にとっては、自身が担当する業務を着実に遂行することが最優先事項であるため、多忙な日々の中で重要なメッセージが見過ごされてしまうこともやむを得ないと言える。

このような状況下では、社員に最も近い立場でマネジメントを担う組織長の役割が極めて重要となる。組織長は、メンバー一人ひとりに対して直接的な働きかけが可能であり、その影響力は大きい。CISOが全社員に向けてメッセージを発信することも重要だが、それとは別に、組織の要となる階層である組織長に対して重点的に意識付けを行うことが、より効果的である。可能であれば、CISO自らが講師となり、組織長向けの研修を定期的に実施することが望ましい。

その際、CISOが組織長に伝えるべき事項の例を以下に示す。

- 自組織の業務に会社のルールを結び付けて考えること。
- なぜそのルールが必要なのかを理解し、メンバーにも具体的に指導すること。
- 自組織で取り扱う情報を常に把握し、そのリスクを認識すること。
- その情報が漏洩した場合にどのような事態が発生するか、最悪のケースを具体的に想像すること。
- 最悪の事態を引き起こす要因を排除するために、実行可能な対策を検討し、着実に組織内へ定着させること。
- これまでのやり方を安易に是とせず、業務の目的を明確にした上で、本当にあるべき姿に見直すこと。

実際、サイバーセキュリティに限らず、事故の原因を分析すると、組織長が適切なマネジメントを怠り、メンバーを放置していたケースが散見される。また、不祥事を起こした企業に関する第三者による調査報告書では、多くの場合、中間管理職の機能不全が根本的な原因の一つとして指摘されている。こうした状況を未然に防ぐためにも、組織長への意識付けは不可欠である。特に多忙な組織長が受け入れやすいタイミングとしては、昇格直後が挙げられる。新任組織長向けの必須研修や、要となる階層の組織長を対象とした必須研修として実施することが有効である。

（３）教育・研修担当者に働きかける

三つ目は教育・研修担当者を対象とした取り組みである。これまで述べてきたのは、教育の対象となる社員や組織長に焦点を当てた内容だったが、ここでは教育や研修を企画・設計する担当者に着目する。一般的に企業では、社員の知識や能力向上を目的として、さまざまな教育・研修が実施されている。これらの企画は、各業務を主管する部門が担っている場合が多い。しかし、部門ごとの独自の考え方や優先事項に基づいて研修が企画されることで、リスク管理に必要な視点や要素が十分に盛り込まれない可能性がある点は、重要な課題である。その中でも、リスク管理、情報セキュリティ、コンプライアンス系の教育に共通する重要な視点は、単なる知識の習得ではなく、社員の「意識」に働きかけ、行動へ定着を図る必要があるという点である。そのため、eラーニングのような一方通行の学習形式ではなく、双方向の学習が有効となる。

リスクマネージャとしては、このような考え方に基づき、会社として教育・研修の企画方針をガイドラインとして定めることで、各分野の教育研修が一貫した姿勢で企画・運営されることが望ましい。

以下に、そのガイドラインのサンプルを示す。

●リスク関連研修の実効性確保のためのガイドライン

1. 考えさせ、想像力を涵養する内容を含めること
2. 参加者個々の気付きを増やす／個々人が発言する形式とすること
3. 多様な視点を活用する／多様な視点を持った参加者で構成すること
4. 理解度を測る／理解するまで終了できない形式とすること
5. 外部専門家を活用すること
6. 定期的に改良すること

社員が備えるべきものとして「知識」と「意識」がある。知識を与える教育はeラーニングでも実施可能であるが、意識に働きかける教育には上記のガイドラインを適用することが望ましい。自ら考えること、言葉にして表現すること、他者へ伝えてフィードバックを受けること、そして異なる業務を担当する参加者の話を聞き多様な意見に触れることで、理解がより深まる。このようなプロセスの積み重ねが、理解の先にある「行動」へとつながるのである。教育・研修の種類や目的に応じて全ての項目を満たす必要はないが、行動変容を促す教育・研修においては、必要な項目を充足させるべきである。

「理解度を測る／理解するまで終了できない形式とする」については、特にeラーニング形式の場合に必ず配慮すべき項目である。単純な理解度テストにとどまらず、基準点に達しない場合は設問を変えて再テストを行う、あるいは回答を記述形式とするなど、可能な範囲で工夫することが重要である。

このようにして企画・設計したリスク管理や情報セキュリティ研修は、効果測定を行いながら、内容や実施タイミング、形式等について不断に改良を重ねることが重要である。

４．サイバーセキュリティ研修の実装例

サイバーセキュリティを自分ゴト化するための教育・研修の中で、リスク関連研修ガイドラインへの適応度の高い実装例をいくつか紹介する。

（１）全グループ社員向け情報セキュリティ週間

（２）新任組織長向けセキュリティ＆リスクマネジメント研修

（３）本部長・事業部長向け模擬記者会見訓練（クライシスマネジメント研修）

（１）全グループ社員向け情報セキュリティ週間

「ｘｘｘ強化週間」や「ｘｘｘ月間」といった特定のテーマを社内に浸透・啓発する施策を集中的に実施する取り組みは、コンプライアンス強化週間や安全週間など、多くの企業で導入されている。サイバーセキュリティについては、政府が2月1日から3月18日までを「サイバーセキュリティ月間」と定め、期間中、政府機関や各種啓発主体と連携して普及啓発活動を集中的に実施している。これは重点的かつ効果的にサイバーセキュリティへの取り組みを推進するための施策である。

ここで紹介するのは、重大な情報セキュリティ事故の教訓を風化させないために、情報セキュリティ週間を活用した取り組みの事例である。社会的に大きな影響を及ぼした情報セキュリティ事故が再び発生しないよう、グループ全社員が毎年、その事故の発生日を含む1週間を「情報セキュリティ週間」と定め、関連する施策を集中的に実施している。

情報セキュリティ週間の概要は以下の通りである。

- **目的**

  重大な情報セキュリティ事故の風化や意識の希薄化、再発防止策の形骸化を防ぎ、二度と同様の事象を起こさないようグループ全社員に意識と自覚を促すことである。また、自社グループの情報セキュリティ目標についても理解・共感を得ることを目指している。

- **実施期間・対象・形式**

  実施期間は、当該重大事故の発生日を含む1週間とし、対象はグループ全社員である。実施形態はWebセミナー形式のリアルタイム配信とし、各セッションは録画して後日オンデマンドでも受講できる体制を整えている。

- **主なコンテンツ**

  毎年度、その年に即したテーマを設定し、リスク関連研修の実効性を確保するためのガイドラインに準拠し、次の内容で構成する。

  - オープニングセッション

    CISOによるオープニングメッセージ、外部専門家による基調講演、外部専門家とCISOおよび現場を担当する役員クラスや組織長複数名によるパネルディスカッションを実施する。これにより、受講者が親近感を持ち、自分事として捉えやすくなることを意図している。

  - CISO特別セッション

    自社グループのサイバーセキュリティ戦略の進捗報告や、組織長向けの階層別研修など、対象者を指定したセッションを実施する。これは、経営の考えを直接伝えることが重要であるとの認識に基づいている。

  - ミニセッション

    CRMOオフィス、CISOオフィス、CSIRTメンバー等によるリスク管理、情報セキュリティ、サイバーセキュリティ、事故模擬体験などの多数のセッションで構成される。

これにより、自社の事業や顧客対応においてサイバーセキュリティがいかに重要かを社員に再認識させるとともに、重大な情報セキュリティ事故の風化や意識の希薄化、再発防止策の形骸化を防止する活動である。

（２） 新任組織長向けセキュリティ＆リスクマネジメント研修

新任組織長が新たな役割を担うにあたり、意識すべき事項について理解を深めるための必須研修である。本研修では、ケーススタディを通じて、CRMOおよびCISOとの対話を交えながら、実践的な気づきを得ることを目的としている。特に、新任のタイミングで実施することで、組織長自身が自分ゴトとして受け入れやすくなり、理解の定着と行動変容につながる点が重要である。

【内容】

1. CRMOから新任組織長へのメッセージ
2. 組織長が知っておくべきリスクマネジメント
3. ケーススタディ
4. CISOからまとめのメッセージ

ケーススタディでは、自身がその立場にあった場合にどのように行動するかを具体的に考え、自らの言葉でCRMOおよびCISOと意見を交換することで、当事者意識を持って捉えることを目指している。こうした事態を未然に防ぐために、組織長としてどのような行動を取るべきだったのか、また、自身がその組織に着任した場合にどのような対応をすべきかを考察する。さらに、「こうすべきだ」と考えた対応を実行しようとした際に、どのような課題が生じるかを明確にし、それに対してどのような対応策が考えられるかを議論することで、実践的な理解を深める構成となっている。

【新任組織長向けセキュリティ＆リスクマネジメント研修での問いの例】

- このような事態が起きないようにするには、組織長はどうすべきだったか
- あなたが組織長としてこの組織に着任したとしたらどうしたか
- 「こうすべき」と考えたことを、本当に実行しようとすると何か課題がないか
- その課題があることに対して、どのような対応が考えられるか

これらの問いには唯一の正解は存在しないが、今後組織長として直面し得るさまざまな状況について、CRMOおよびCISOと対話を通じて考えを深めることで、意識の定着を図ることを目的としている。

（3）本部長・事業部長向け模擬記者会見訓練（クライシスマネジメント研修）

本研修は、ビジネスの現場で最上位責任者となる本部長・事業部長クラスを対象に、新任のタイミングで実施されるものであり、サイバー攻撃による影響の重大さを体感することを目的としている。研修では、模擬記者会見のロールプレイを通じて、実際よりも一段、二段高い役割・責務・視点で状況を考察し、翻って自組織のセキュリティの重要性を「自分ゴト」として捉えることができる構成となっている。本研修も新任のタイミングで実施することで、危機対応に対する意識を早期に醸成し、責任者としての自覚と行動変容につなげる点が重要である。

レピュテーションリスク・コンサルタントによる講義の後、具体的なインシデントシナリオをもとに、5名ずつのグループで企業としての対応方針を議論する。その後、決定した方針に基づき模擬記者会見を実施する。受講者は社長、営業部門担当役員、システム部門担当役員、広報部長などの役割を分担し、記者役は経験豊富なコンサルタントが務め、厳しい質問に応答する形式で進行される。

これにより、発生したインシデントやその対応が社会からどのように受け止められるかを肌で感じ、事故を未然に防ぐことの重要性を、経営および社会的な視点から再認識することができる。

本研修の概要は以下のとおりである。

- 通常は経営者向けに実施される模擬記者会見訓練を、簡易版として本部長・事業部長クラス向けに実施する。

- 新任の本部長・事業部長は受講必須である。
- 自社のサービスから顧客情報が窃取され流出した可能性があるというシナリオおよび状況設定を提示する。
- 5名程度のグループで社長役、マーケティング担当役員役、システム部門担当役員役、リスク管理担当役員役、広報部長役を割り当て、対応策や記者会見での説明内容・質疑応答の準備を行う。
- 外部専門家の指導のもと、模擬記者会見において記者役からの厳しい質疑応答を体験する。

参加者からは、「実際よりも高い役割・責務・視点で考えさせられることで、現職における為すべきことをより明確に認識できた」という意見が多く寄せられている。

危機管理においては、初動対応が最も重要である。初動を確実に行うためには、現場を担う各部門の組織長のリスク感度およびリスクマネジメント能力が不可欠である。インシデント発生時には、事故発生部署のリスク管理責任者として、迅速かつ的確に行動することが求められる。本研修は、危機管理に対する認識や考え方についても理解を深められる内容となっている。

ここまで説明した実装例のリスク管理研修ガイドラインへの適応度を表1に示す。

表１：リスク関連研修ガイドラインへの適応度の例[3]

対象	研修名称	ベースとなる知識を与える	1．考えさせ、想像力を涵養する	2．気付き増やす／個々人が発言する	3．多様な視点を活用する	4．理解度を測る	5．外部専門家を活用する
全グループ社員	**情報セキュリティ週間**	○	○	○	○	―	○
全グループ社員	**車座会議**	○	○	○	○	―	
本部長・事業部長	**クライシスマネジメント研修**	―	○	○	○	○	○
組織長	**CISOによる組織長研修**	○	○	○	○	―	
新任組織長	**新任組織長研修向けセキュリティ＆リスクマネジメント研修**	○	○	○	○	―	
全グループ社員	**全社員向けeラーニング**	○				△	

凡例：○：適応、△：一部適応、空欄：未適応、―：対象外

[3] 所属企業の事例をもとに筆者作成。

5．おわりに

サイバーセキュリティ対策は、単なる技術やルールの整備にとどまらず、企業を構成する一人ひとりの意識と行動がその根幹を成すものあり、特にリスクマネージャにはその要となる役割が求められる。目まぐるしく変化するビジネス環境や巧妙化するサイバー攻撃に対応し続けるためには、現場の声や日々の業務に根ざした気付き、そして「自分ゴト」として捉える姿勢が不可欠である。リスクマネージャは、そうした現場の意識を醸成し、組織全体へと波及させる推進役として重要な存在である。

どれほど堅牢なシステムや制度を構築したとしても、最後の砦となるのはそこに集う人の意識であり、日々のリスクへの感度と行動の積み重ねである。本レポートで紹介したさまざまな取り組みや研修は、その第一歩に過ぎない。今後も一人ひとりが主体的にリスクと向き合い、組織全体で学び合う文化を育むことが、真に効果的なリスクマネジメント、そしてサイバーセキュリティの強化につながるのである。その普段の努力にリスクマネージャが積極的に関与し、組織の信頼と持続的な発展を支える基盤となることが重要である。

以上

[本調査に関する照会先]

客員研究員 澤田雅広 sawada@j-cic.com

JCIC 事務局 info@j-cic.com