情報セキュリティ事故対応１日コース 机上演習事例

株式会社電通コーポレートワン 様

全社員を「プラス・セキュリティ人材」に。dentsu Japanが挑む、実践的な事故対応訓練の狙い

サイバー攻撃の脅威が高まる中、今やセキュリティ対応はセキュリティ部門だけでなく、全社的に取り組む重要課題となっている。こうした状況を受け、dentsu Japan では事業部門の管理職を対象に、グループ全体を巻き込んだ大規模な事故対応訓練を実施した。本記事では、この取り組みを企画した背景や実施内容に関して、プロジェクトをリードした４名に話を聞いた。

株式会社電通コーポレートワン
テクノロジーオフィス
サイバーセキュリティ部
部長　金島 利明氏

株式会社電通コーポレートワン
テクノロジーオフィス
インフラ開発部
小宮山 佳氏

株式会社電通コーポレートワン
テクノロジーオフィス
サイバーセキュリティ部
喜多村 恒一氏

株式会社電通コーポレートワン
テクノロジーオフィス
サイバーセキュリティ部
塙 美幸氏

サプライチェーン全体の信頼を支える「現場起点」のセキュリティ戦略

dentsu Japan は、広告・マーケティング領域における国内外の多様な企業と連携しながら、顧客企業のビジネス変革を支援する総合的なビジネスモデルへと進化を遂げている。

2022 年に設立された電通コーポレートワンは、グループ全体の業務基盤を支えるコーポレート機能を担い、業務基盤の整備とともに情報セキュリティ強化にも注力している。現在は ISO27001 のグループ認証を国内グループ会社全体で取得するなど、着実に体制を築き上げている。

背景には、広告業界におけるビジネス環境の変化がある。従来の広告代理業から、顧客企業の DX 支援やデータ活用といった領域へ事業が広がる中で、情報の信頼性と安全性がブランド価値そのものに直結する時代となった。技術的なセキュリティ対策にとどまらず、セキュリティを経営課題として捉えている。広告主やメディア、制作会社、テクノロジーパートナーなど多様な企業と連携する中で、１件のインシデントがグループ全体の信頼を揺るがすリスクとなり得るからだ。そのため、セキュリティ対応はグループ内の１部門だけで完結するものではなく、全社的かつ横断的な取り組みが不可欠となっている。

対象は約300名。信頼され続ける企業であるために、現場の判断力を鍛える

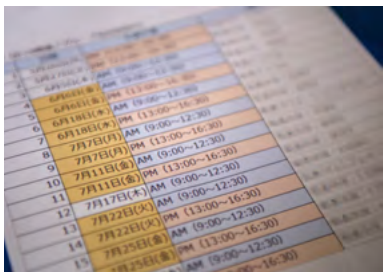
今回のセキュリティ研修を企画・実施するに至った背景には、過去のインシデントで痛感した危機感がある。情報漏えいやサイバー攻撃のリスクが高まる中で、被害の最小化と再発防止は、企業の信頼を守るための最重要課題となっている。

「従来、セキュリティ研修は専門部署を中心に行われることが一般的ですが、実際にインシデントが発生した際、最前線で説明責任を果たすのは現場の管理職です。だからこそ、管理職が適切な判断をするためには、セキュリティの基本的な理解を持っておくことが重要だと考えています。」と金島氏は語る。

こうした認識のもと、事業部門の管理職層を対象としたセキュリティ研修を企画した。対象者はグループを横断する形で選定され、研修は約 300 名規模、18 回にわたって実施されるという大規模な計画だ。営業やマーケティングなど、普段はインシデント対応の専門チームである CSIRT との接点が少ない部門にも対象を広げたことで、セキュリティ対応を「自分ごと化」させる重要な一歩となった。この取り組みは、IPA が提唱する「プラス・セキュリティ人材※」の育成にも通じる、先進的な取り組みといえる。

※「サイバーセキュリティ体制構築・人材確保の手引き」（第 2.0 版）（METI/経済産業省）
https://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf

なお、今回の研修は、2024 年度に実施したパイロット版研修をベースに設計されている。パイロット版では、グループ全体への展開を見据え、情報セキュリティ事故対応をテーマとした机上演習形式の研修をラックが提供する標準シナリオで実施した。研修内容の妥当性を確認するとともに、現場社員の意見を収集することを目的としていた。



パイロット版研修には、セキュリティ部門や現場管理職、人事部門がそれぞれ異なる視点から参加した。セキュリティ部門は内容の妥当性を検証し、現場管理職は実務に即した理解度を確認、人事部門は人材育成の観点から意見を集めるなど、複数部門が連携して研修の有効性を検証した。その結果を踏まえ、2024 年度は電通の管理職向けに 8 回の研修を実施し、2025 年度は対象を拡大して 18 回にわたる本格展開へと発展した。

さらに注目すべきは、この研修がボトムアップの提案によって実現したという点だ。パイロット版の準備段階から今年度の本格展開に向けた企画まで、現場の声が十分に反映されている。経営層もその重要性を理解し、積極的に支援した。これは、dentsu Japan 全体がセキュリティを「経営課題」として捉えている証といえる。

グループの業務実態に即した設計と、現場に届く研修運営の工夫

今回実施した「情報セキュリティ事故対応 1 日コース 机上演習編」は、非技術部門の管理職層を対象に、実際の業務に即した対応力を養うことを目的に設計された。IT 部門向けの既存研修を流用するのではなく、営業やマーケティングなど、日常的にセキュリティ対応に関わる機会が少ない部門に向けて、一からシナリオを構築。オンライン形式で実施され、実際の勤務状況に近い環境で進行した。

「意思決定のタイミングや社内外への報告、顧客対応など、現場で求められる判断力を体感的に学べるように設計した。」と小宮山氏は語った。研修は単なる座学ではなく、参加者が能動的に考え、判断する演習形式を採用した。実務に直結する場面を想定し、対応力を自分ごととして身につけられる構成となった。

設計段階では、電通ならではの文化や現場発想を反映するため、表現や伝え方にも細心の注意が払われた。リハーサルでは、言葉のニュアンスやシナリオのリアリティなど受講者への伝わり方を確認し、受講者が違和感なく受け入れられるよう細部にわたる調整が重ねられた。

また、運営面でも多くの工夫が凝らされた。2025 年度の対象者は約 300 名にのぼり、大規模開催ならではの課題となった受講者への連絡やスケジュール調整、当日の対応、アンケートの回収などは、ラックが全面的に支援した。塙氏は「運営面でしっかりとサポートしてもらえたことで企画に集中でき、欠席者がほとんど出ず、満足度の高い研修ができた。」と振り返る。こうした設計と運営の工夫が功を奏し、研修後のアンケートでは参加者の 9 割以上が「参加して良かった」と回答した。さらに、「ゲーム感覚で集中して参加できた」「実際の業務に役立つ気づきが得られた」「自分たちが対応の主役であることを実感した」など、ポジティブな声が多く寄せられた。

喜多村氏は、「現場にはもともと『対応は自分たちの責任』という意識はあったが、実際にどう動けばよいのかが分からず、不安を感じていた人も多かった。」と語る。今回の研修を通じて、そうした層が正しい対処の流れや判断のポイントを具体的に理解できるようになり、対応への自信と行動力が育まれてきたという。また、研修を通じて CSIRT の認知度も向上した。研修前には、約 4 割の参加者が CSIRT の役割を十分に理解していなかったが、研修後にはその重要性や連携の必要性についての理解が深まり、社内での情報共有や連携の動きも活発化している。このように、研修の設計・運営において、現場に届く工夫を重ねながら、セキュリティ対応力の底上げを図っている。

継続的な意識づくりと、さらなる拡張に向けた挑戦

セキュリティ研修は、管理職層にセキュリティ対応を自分ごととして捉える意識変革を促し、グループ全体の対応力を押し上げる成果を生んだ。ただし、セキュリティ対応力の強化は 1 度の研修で完結するものではない。金島氏は「継続的な取り組みを通して、社内に定着をさせていくことが大事であり、それがクライアントに対して責任を果たすということになると考えている。」と語る。

今回の成果を踏まえ、今後は対象層をさらに広げていく方針だ。すでにグループ会社からは「新卒社員にも研修を受けさせたい」「他部門にも展開してほしい」といった声も上がっており、次年度に向けては更なる水平展開の検討がはじまっている。経営層に対してはレポーティングを通じてセキュリティに対する理解を深め、より主体的に関与してもらうための取り組みが進められている。トップと現場の認識が一致すれば、意思決定のスピードと質が両立し、グループ全体のセキュリティレベルはさらに高まるだろう。

また、dentsu Japan のビジネスは多くの関係会社やパートナー企業との協業によって支えられている。サプライチェーン全体でのセキュリティ意識の統一は、今後の重要なテーマだ。こうした取り組みを継続的に支えるには、運営体制の充実も欠かせない。研修設計や運営支援には外部パートナーの協力も得ながら、企業文化や課題に合わせた柔軟な対応が行われており、引き続きその連携が期待されている。グループとしてセキュリティを高める体制づくりに挑戦することは、企業の信頼を守るだけでなく、社会全体のセキュリティ意識の底上げにもつながっていくだろう。

左から、株式会社電通コーポレートワンの喜多村氏、金島氏、塙氏、小宮山氏

［お問い合わせ］
株式会社ラック
サービス紹介ページ https://www.lac.co.jp/education/course/incident_response_intensive.html