

第 69 回 變会

NPO 法人日本交渉協会 常務理事 窪田恭史



第 69 回 變(やわらぎ)会を、6 月 21 日(土)に弊社会議室にて開催いたしました。



今回は 2 部構成。第 1 部は、1 級会員の吉山洋一さんによる事例発表。「サイバーセキュリティにおける交渉」と題してお話いただきました。

少し前まで、「交渉」といえば、会議室での契約交渉や外交の場が連想されてきました。しかし現代では、サイバー空間が新たな交渉の主戦場となりつつあります。私たちのところにも頻繁に届く詐欺メール、サイバー攻撃による脅迫、そこで展開される情報戦。サイバーセキュリティの本質は、そうしたことから人々の安全と信頼を守ることにあります。そしてそのためには、冷静かつ戦略的な交渉力が不可欠となっているのです。

今や、サイバー攻撃は攻撃を受けた組織に留まらず、取引先や国家、社会を巻き込み、重大な悪影響をもたらします。そのため、攻撃を受けた企業や国家には、単なる技術的対応を超えて、攻撃してきた犯罪者のみならず、さまざまな利害関係者と交渉が必要になります。際、2024 年に日本で起きた大手出版社に対するサイバー攻撃にあたっては、犯罪者だけでなく、国家、産業界、ユーザー、世論との複層的な交渉が必要となり、結果として 36 億円もの損失が発生したと言われています。

サイバー攻撃に対しては、脅迫に対する心構えと戦略、緊急時の判断体制と情報発信、外部関係者（警察、PR、法務等）との協力体制などを整備する必要がありますが、多くの組織は、サイバー攻撃への備えにおいて今もって脆弱な状況にあります。

サイバー攻撃は、私たちの身の回りでも日常的に起こっています。代表的なものが毎日のように送られてくるフィッシングメールですが、昨年、私たちが受け取るメールの内、悪性メールと呼ばれるものがついに普通の良性メールを数の上で上回ったそうです。また、生成 AI の進化により、フィッシングメールの巧妙さは急速に高まっています。例えば、SNS などから個人の行動傾向を分析し、「その人がハマりやすい話題」で攻めてくる、偽ショッピングサイトはもちろん、音声・映像を利用したディープフェイクも目覚ましく進歩し、ますます判別が難しくなっています。お話の中で挙げられた例では、オンライン会議に参加した相手が、みな「知っている声」かつ「知っている顔」であったにもかかわらず、全員偽者だった（つまり、その会議そのものが詐欺であった）という事件があったそうです。本物と偽物の識別が難しくなっているどころか、ある実験では、むしろ偽物の方をより本物と認識する傾向があったとさえ言われています。今や、サイバー空間の脅威のほとんどは「だまし」であり、人間の心理を利用した高度な技術なのです。

さて、ランサムウェア攻撃を受けた場合、攻撃してきた犯罪者と身代金（ランサム）の交渉を行うことは、日本では非行行為とみなされ、違法だそうです。しかし、海外ではすでに「ランサムウェア交渉人」が存在し、犯罪者との身代金交渉を行っています。お話の中でいくつかの失敗事例や成功事例が紹介されましたが、やりとりのログはオンライン上で公開されているそうです。それを見て感じたのは、攻撃側は事の良し悪しは置いておくとして、非常に洗練された交渉者であるということです。今のところこの分野においては被害者側の立場は非常に弱く、成功事例と呼ばれるものも如何に身代金を減額できたか？というレベルに留まるのですが、それであっても攻撃者側の被害者側に関する情報収集、想定される被害金額と比較して算出した身代金金額、理性的なコミュニケーションを行うなど、高度な交渉力を駆使していることが分かります。このことから、サイバー攻撃は単なる技術的問題ではなく、究極的には人の問題であることが分かります。

たとえば、2021 年、米国の東海岸に燃料を供給する大規模パイプライン、「コロニアル・パイプライン」が「ダークサイド」と呼ばれるグループからランサムウェア攻撃を受け、パイプラインの操業が停止。東海岸全体にガソリン不足と価格高騰の影響が及ぶという事件が発生しました。この事例を、「交渉の 7 要素」に基づいて分析すると、以下の表のようにまとめられます。交渉結果から攻撃側は彼我双方について、これらの要素をよく理解して交渉していたことが窺えます。

交渉の7要素	説明	加害者（ダークサイド）	被害者（コロニアル・パイプライン）
1. 選択肢	交渉で考えうる選択肢のリストアップ	即時支払い or 公開、交渉の即決誘導	支払うか、業務停止を継続するか
2. 代替案	交渉が決裂した場合の最善策	他企業を攻撃対象とする準備	連邦支援／FBI支援の活用、運用再開計画
3. 利害関係	表面的な立場ではなく、本質的な関心・ニーズ	金銭、影響力、ブランド価値の破壊	社会的責任、顧客への信頼回復
4. 関係性	相手との信頼関係や過去の関係性	地下組織としての信頼確保（履行実績）	規制当局・顧客との関係性維持
5. コミュニケーション	情報伝達の方法、タイミング、姿勢	暗号チャットを用いた対話	時間との戦いで主導権が取れず
6. 正当性	合意内容の正当性・客観性の根拠	「市場価格」「過去の相場」を主張	業界慣行との整合性提案
7. コミットメント	誰がいつどこまで約束を履行するか	暗号通貨で即日支払いを要求	即日支払いを選択（のちに回収成功）

そのように考えると、サイバーセキュリティにおいて重要なのは、「備え」と「冷静な交渉力」であるということが出来ます。たとえば攻撃を受ける被害者側としては、以下のような対応がサイバー交渉を成功させるうえで必要になるでしょう。

成功要因	具体的な内容	意義
事前準備	・脅迫シナリオの訓練 ・バックアップ体制 ・IRP（インシデントレスポンス計画）策定 ・法的対応ルート ・支払い方針の明確化	初動対応を明確にし、交渉の迷いを排除。優位な交渉へつなげる。
専門チーム編成	・CSIRT（Computer Security Incident Response Team）の常設 ・交渉人材の確保 ・外部ベンダーとの連携 ・24時間対応体制	技術・法務・広報の専門家が連携し、損害を抑制。
冷静な交渉	・冷静な情報収集 ・相手の目的分析 ・構造的交渉 ・情報管理 ・段階的対応	脅迫に動じず、冷静に対応。相手の交渉の隙を突く。
強靱性向上	・段階的復旧 ・復旧戦略の確保 ・PRと信頼維持策 ・通知と再発防止 ・説明責任体制	交渉結果に左右されず、信頼回復と業務継続を実現。

サイバー攻撃による被害額は年間 2.4 兆円、これは日本の防衛装備費に匹敵する額だそうです。しかも、その額は年々増え続けています。ここまでのお話のように、サイバーセキュリティとは、技術の話にとどまらず、人間の話でもあります。巧妙な詐欺を見抜く洞察力、脅迫に冷静に対処する判断力、組織を導く説得力、これらはすべて、交渉の技術から学ぶことができます。攻撃を防ぐことは難しくとも、被害を最小限にとどめる交渉力は、誰もが備えるべき防衛スキルだといえるでしょう。



『コグニティブセキュリティ実践入門 デジタル時代の戦略的意思決定』
吉山 洋一 著

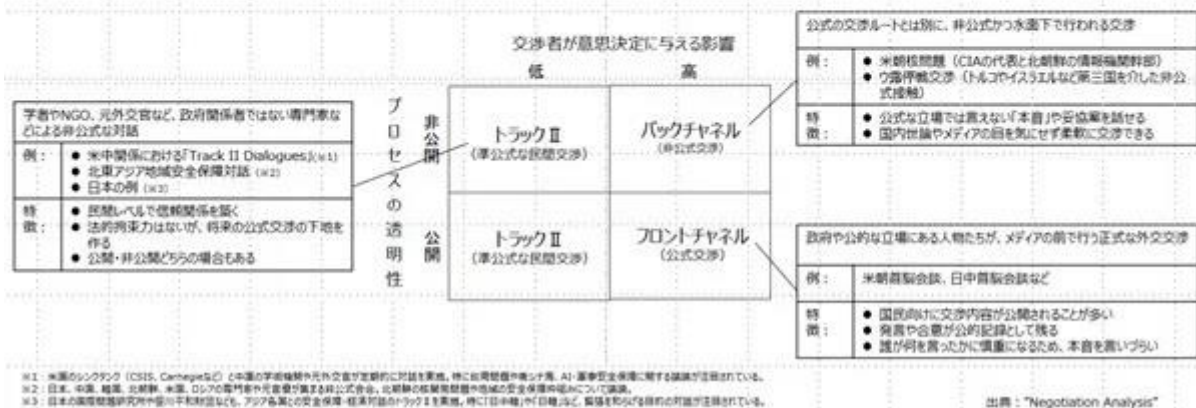


第2部は、恒例の「交渉理論研究」。第27回のテーマは「並行交渉」です。

1. 並行交渉とは？

- 今回は、前回までで述べた第三者の介入による支援の一形態である「並行交渉」に焦点を当てる。
- 並行交渉とは、表の交渉（公式の交渉）と、裏の交渉（非公式交渉）が同時に進む形態のことをいう。現代の複雑な国際交渉や紛争解決の場面で、よく使われている。

1-1. 並行交渉の種類



並行交渉とは、たとえば外交交渉などで首脳同士が行う「フロントチャネル交渉」と並行して行われる、実務者による非公式または水面下の交渉（バックチャネル交渉）、や政府関係者ではない専門家などによる非公式な対話（トラックII交渉）を言います。

バックチャネル交渉やトラックII交渉が行われる理由は、フロントチャネル交渉には、たとえば国としての面子や有権者に向けたアピールの必要など、交渉の進展を妨げるさまざまな障壁があるため、それらを緩和し、交渉を前に進めるためです。”Negotiation Analysis”の著者であるハワード・ライファは、そうした障壁を11個特定し、挙げています。

実際、ライファは太平洋戦争（1879～1884、硝石戦争）以来、対立関係が続いていたボリビア、チリ、ペルーの代表者をハーバード大学に集め、交渉のロールプレイ・シミュレーションを通じて彼らを協働させることで、和平にむけた創造的な交渉の土台づくりをしました。これは、トラックII交渉の一例です。同様に、MIT（マサチューセッツ工科大学）のローレンス・サスカインドもアメリカ合衆国環境保護庁（EPA）と利害関係者の

代表にロールプレイ・シミュレーションを行わせ、実際の交渉の示唆となる共創機会への気づきや交渉を円滑に行うための共通言語の共有に貢献しました。



今回は、これに因んで「バッチフォゲン」というロールプレイ・シミュレーションを行いました。今回のテーマ「並行交渉」は、前回までの「第三者の介入」による交渉の一つであるため、このシミュレーションには、交渉当事者（プレイヤー）だけでなく、交渉の進行を導くファシリテーターも加わりました。限られた時間の中ではありましたが、みなさん結構良い交渉ができていたように思います。

最後に補足として、近年発達の著しい生成 AI を利用した交渉シミュレーションの可能性についてお話ししました。



懇親会は、昨年に続いて、近所の『仙や』さんで行いました。