「社会を揺るがす重大サイバー事案：社長はどう語り、政治家は何を問うのか」

日本サイバーセキュリティ・イノベーション委員会　藤原未来子

【重大サイバー事案の事後コミュニケーションにおける経営トップと政治家のあり方：米国公聴会の事例】

●経営トップは、経営の「プロ」として、コミュニケーションのトレーニングを平時より受け、かつセキュリティが専門ではなくても「プラス・セキュリティ人材」として、「自分の言葉」で明瞭に語る

●政治家は、真に糾弾すべき相手を見誤らず、サイバー攻撃を受けた企業が「被害者」であることを明言し、過度に責めることをしない

●双方とも、大切なのが対立ではなく連携であり、「将来の被害を軽減する」ために「経験から学ぶ」という未来志向を示す

～～～

【はじめに】

ここ数年、重要インフラ企業を狙ったサイバー攻撃が世界各地で頻発している。特にランサムウェア攻撃は顕著に増えている。

市民生活に影響を及ぼす事案が発生した場合、それは被害を受けた企業だけの問題ではなく、社会問題となる。多くの場合、被害企業のトップが表に立ち、説明を求められることになる。事案発生直後であれば記者会見であろうし、しばらく経過した後には総括的な説明も求められる。そのような総括の場の一つとして、市民・国民の代表者である政治家が事情を聞くこともある。日本であれば国会である。そのような場で、企業のトップはどう発信すべきか、政治家はどのような姿勢を見せるべきか。目指すべきところは何か。つまり、どのようなコミュニケーションが望ましいのか。

本コラムでは、今後も発生するであろう民間企業を狙った重大なサイバー攻撃に関し、上記のような「総括の場でのコミュニケーション」にフォーカスしてみたい。題材とするのは、2021 年 5 月に発生した北米最大のパイプライン運営会社であるコロニアル・パイプライン社を襲ったサイバー攻撃に関する、米国上院議会国土安全保障・政府活動委員会の公聴会の事例である。同社 CEO は一人で公聴会に臨み、質問に答えた。「コミュニケーション」に焦点をあてるため、本コラムでは被害の詳しい内容など技術的な部分には踏み込まない。

米国東海岸の燃料パイプライン 45%を保有する同社は、ロシアに本拠地を置く犯罪集団ダークサイドによるランサムウェア攻撃を受け、約 1 週間の操業停止を余儀なくされた。ガソリンが不足するというパニック心理から東海岸のガソリンスタンドでは長蛇の列、各地で売り切れ、ガソリン価格は急騰。また航空機のジェット燃料も不足して長距離飛行ができなくなるなど、大きな社会不安を引き起こした。同社はダークサイドに約 440 万ドル相当のビットコインを支払うこととなった（後に約 85%を取り返したとされている）。事案発生から約 1 ヵ月後の 2021 年 6 月に開催された公聴会では、コロニアル・パイプライン社のブラウント CEO が出席し、議員からの質問に答えた。

公聴会では、下記の４つの点について質問が複数回出た。

1. 事案発生直後に同社から米国政府機関におけるサイバーセキュリティの総本山である国土安全保障省サイバーセキュリティ庁（Cybersecurity and Infrastructure Security Agency：CISA）に直接連絡が行かなかった理由
2. 同社のシステムの認証方式などサイバーセキュリティに関する防御態勢の状況
3. 攻撃者である犯罪集団ダークサイドに金銭を支払った経緯
4. 今回の事案から得た教訓について

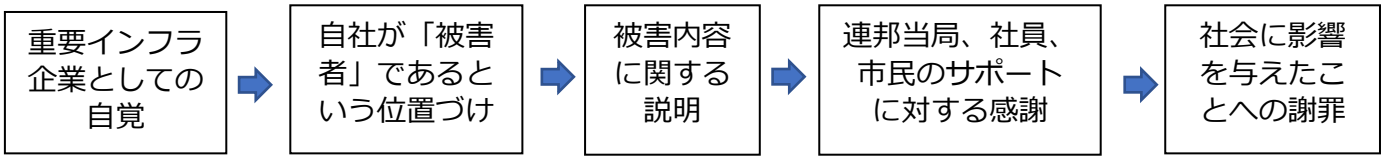
【ブラウント CEO は何をどう話したか：自分の言葉で主張すべきところは主張、不備は認める】

コロニアル・パイプライン社のジョセフ・ブラウント CEO はエネルギー業界で 40 年近い経験を持ち、エネルギー各社の CEO を務めた後、2017 年にコロニアル・パイプライン社の CEO に就任した。言葉づかい、アクセント共に、典型的な米国東部のビジネス・エグゼクティブであり、公聴会での口調はよどみなく、発音も明瞭で聞きやすい。視線を一定に保ち、表情もコントロールしており、時に笑みも見せる。スピーチに関する経営トップ向けのトレーニングを受けていることがうかがえる。

冒頭、議員による公聴会の趣旨説明の後、ブラウント CEO に 7 分間のスピーチの時間が与えられた。同社の業務の詳細な説明と、同社が safety と security について真剣に取り組んできたことに言及した後、「常に自分の頭の中には顧客、シッパー（輸送を委託する業者）、そして『国』がある」と述べ、米国を支える重要インフラ企業としての責任感を CEO として備えていることを示した。そして、「1 ヵ月前、我が社はランサムウェア攻撃の被害者となり、システムが暗号化され」、その結果操業停止に追い込まれたと述べた。同社が「被害者」であることを明確に打ち出したのである。また、事案発生から数時間後には連邦当局に連絡し、その後彼らはずっと我が社の真の協力者となってくれた、その尽力に感謝する。我が社の社員、米国の人々のサポートにも感謝する。と感謝の意を示した後、表情を引き締めて「今回の攻撃による影響については深くお詫びする」と発言した。その後、パイプラインの重要性を鑑み、ブラウント CEO が犯罪集団への金銭の支払いという苦渋の決断をしたこと、現在同社がサイバー防衛の堅牢化に注力していることを述べてスピーチを締めくくった。

スピーチの流れを見てみると、下の図のようになる。一連の流れ、特に、「被害者としての位置づけ」、「各者への感謝」を「謝罪」より前に示しているところがきわめて米国的と言えよう。

［冒頭スピーチの流れ］



先述の通り、質疑応答パートでは４つの点で質問が複数回出た。回答ぶりを以下の表に簡単にまとめた。

［複数回出た質問に対するブラウント CEO の打ち返し］

質問内容	回答内容	CEO の姿勢
事案発生直後に国土安全保障省サイバーセキュリティ庁（CISA）に直接連絡をしなかった理由	・事案認識後、同社は数時間のうちに FBI に連絡 ・FBI 側で CISA に連絡すると言われ、実際その日のうちに行われた会議には CISA も出席した ・当日報告を上げねばならない政府機関が多数 ・CISA とは CISO を通じて緊密な関係性あり	判断に不備を認めず
質問内容	回答内容	CEO の姿勢
同社のシステムの認証方式などサイバー防御態勢の状況	・使われていなかったレガシーVPN システムから攻撃された ・単純ではないもののパスワードでログインできた ・同社の緊急事態対応プランの中にランサムウェア攻撃が入っていなかった ・過去 5 年間で IT システム総投資額は 2 億ドル強	防衛の不備を認める
攻撃者側に金銭を支払った経緯	・39 年の職業人生の中で一番厳しい決断 ・被害の全貌は決断時には見えていなかった ・企業として、米国にとってのパイプラインの重要性を認識し、米国の利益を一番に考えて決断 ・支払いについてはセキュリティの観点から機密扱い ・支払った甲斐はあったと考えている ・この判断は間違っていなかったと信じる	判断に誤りはなかったと明言
今回の事案で得た教訓	・迅速な対応とコミュニケーションの重要性 ・出来る限りの透明性 ・「not being afraid to come forward」（前に進むことを恐れない） ・関係各機関をまとめた窓口を通じての連邦政府とのコミュニケーションの重要性	臆することなく未来志向

ブラウント CEO はサイバーセキュリティのプロではない。しかし、約 1 時間半に及んだ公聴会にあたり、はじめのスピーチの時こそ手にした紙に目をやりながら話したが、質疑応答のパートでは、同氏は紙に目を落とすことはほぼなく、誰かからのメモが入ることもなく、誰にでもわかる言葉で明瞭に語った。サイバー防衛に関する不備も認めた。同じ質問が複数回出ても、いらだつそぶりもほぼ見せなかった。わずかに苛ついた表情を見せたのは、筆者が見た限り、年毎のサイバーセキュリティへの投資額を聞かれた 1 回のみであった。「教訓」についても明確に回答し、また随所で、今回エネルギー省が政府側の窓口となり関係各機関への連絡業務を調整してくれたことの重要性とそれへの感謝の意を表明した。

受け答えをほぼコントロールし、さらには「感謝」というポジティブな発信を随所に加えた結果、ブラ

ウント CEO は、彼が事案の内容を把握し、コミュニケーションも円滑に行っているという印象を与えることに成功した。この印象は、「同社及び同 CEO が事案をコントロールできている」という安心につながる。

もちろんサイバーセキュリティのプロからすれば、粗は見えるだろう。認証方式など防御態勢のくだりは、筆者が見ていても弱さが感じられた。ただし、こういった社会的影響が大きい事案の場合、聞き手（本公聴会の場合は上院議員）及び関心を示す者の多くが、サイバーセキュリティのエキスパートという訳ではない。テクニカルな内容に突っ込んでいく必要はない。かえって弱みが露呈するリスクがある。セキュリティの専門家ではないが、事案の内容は理解できているという、「プラス・セキュリティ人材」としての振る舞いができれば乗り切れる。ブラウント CEO はそこを理解していた。CEO として、自社の PR が流暢に出来ることは当たり前である。それに加えて、「弱みがある立場であっても、自社が必要以上の責めを負わないよう公の場において自分の言葉で明瞭に語ること。ポジティブな印象を与える要素も入れて、『CEO が状況を理解し、対応をコントロールできている』という印象をつくること。そのための準備を CEO 自身が怠らないこと」。現代の経営者が身につけておくべき資質として、きわめて重要なポイントである。ブラウント CEO はまさに、プロの経営者であり、「プラス・セキュリティ人材」である。

【政治家たちのスタンス：企業が「被害者」であることを明示】

ブラウント CEO の落ち着いた物腰、ポジティブさを入れ込んだスピーチや回答は、しかし場の雰囲気が寄与したところも多分にあると思われる。日本の国会での参考人招致を見慣れた身としては、「国会はつるし上げの場である」という意識が強いが、本公聴会で議員達が見せた姿勢は、それとは大いに異なっていた。

公聴会の冒頭、チェアを務めた委員長のピーターズ上院議員は概略こう述べた。「米国全土でランサムウェア攻撃が相次いでおり、米国市民の生活を混乱させている。関係各機関に、サイバー攻撃を受けた被害者であるコロニアル・パイプライン社をどうサポートするかを真剣に考えてもらいたい。サイバー攻撃への備えをステップアップさせないと、シビアな結末になる。同社への攻撃は、数百万の米国市民に影響を及ぼした。次にこういう事案が発生したら、（被害は）もっとひどいことになるかもしれない。重要インフラのネットワークをもっと守るべきだ。過去の失敗からしっかり学んで、（政府と民間セクターとで）一体となって取り組み、（サイバー攻撃という）この大きなチャレンジに立ち向かわねばならない」。

明確に、「サイバー攻撃を受けた企業」が「被害者」だと述べているのである。ピーターズ議員だけにとどまらない。複数の議員が、質問の冒頭で「You are/were the victim」（御社は被害者だ）と明言している。企業サイドも、政治家サイドも、「被害者であること」においてコンセンサスが取れている。加えて、ピーターズ上院議員をはじめ複数の議員が、この公聴会は将来の被害を防ぐために企業と政府の連携を促す目的で開催していると述べている。複数の議員から出た 4 つの質問のうちの 1 つは、「今回の事案から学んだ教訓は何か」であった。未来のためにこの会合がある。ブラウント CEO も明快に回答した。

共に将来を見ている。

議員達の発言は、公聴会がコロニアル・パイプライン社の不手際を糾弾する目的で開催されているのではないことを示している。ランサムウェア攻撃が国内で相次いでいることが明らかになり、攻撃者への怒りが高まっていた時期であったことも、ある意味コロニアル・パイプライン社には有利に働いた。もちろん、加害者側への金銭の支払いの正当性やサイバー防衛体制の不備を問う厳しい質問は多くあった。しかし、コロニアル・パイプライン社の位置づけ、公聴会の目的を明確化することにより、ブラウント CEO のストレスは相当程度軽減されたであろう。

甚大な影響が出た事案の場合、日本ではともすれば、「なぜこんなことになったのか」、「どんな不備があったのか」という、責任追及という名の糾弾大会になりがちだ。サイバー被害に遭った企業も、「被害者」であることを表明しづらい空気がある。しかし果たしてそこから何が生まれるのであろうか。そろそろそういう風潮に歯止めをかけるべきではないか。「被害者」であることを社会が認知すること、いたずらに責め立てるのではなく、今後の被害を軽減させるために事案を精査し、教訓を共有して将来の攻撃に備えることこそが重要ではないのか。追及する側に立つことの多い政治家やメディアにも、考え方の転換が求められている。

米国を立て続けに襲うサイバー攻撃。対岸の火事ではない。日本でも既に、コロニアル・パイプライン社ほどの規模ではなくても、重要インフラが狙われる事案は相次いでいる。より大規模な攻撃が起きる可能性は高い。その時、企業は、政治家はどう対応するのか。この公聴会には、コミュニケーションに関する様々なヒントが示されているように思う。

（了）

参考資料（映像）：
米国上院国土安全保障・政府問題委員会ヒアリング：“Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack”（2021 年 6 月 8 日）
https://www.hsgac.senate.gov/hearings/threats-to-critical-infrastructure-examining-the-colonial-pipeline-cyber-attack