企業セキュリティをシフトする

コロナ禍によって、企業は大きな変化を強いられている。セキュリティもその一つだ。
大切なのは、セキュリティが、もはや企業活動に不可欠な「環境」の一つであるということだ。
セキュリティの具体的な手法ではなく、経営者自身のセキュリティに対する捉え方が問われている。

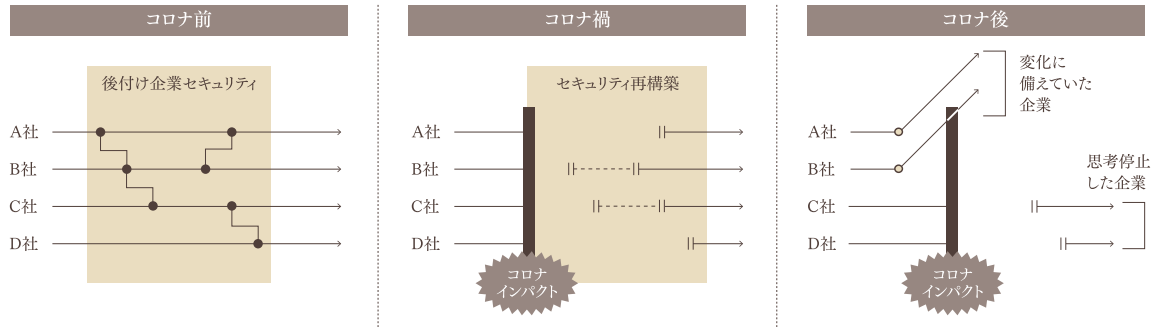
コロナ禍が企業にもたらしたインパクト

新型コロナウイルスの感染拡大をめぐり、政府は2020年4月、緊急事態宣言を発出した。戦後、このような大きな災厄に日本全国が揺さぶられることはなかったのではないか。

企業活動も同様だ。週5日間会社に行き、9時から5時まで勤務する形態から、時差出勤、または在宅勤務やサテライトオフィス勤務をはじめとしたマルチオフィスでのテレワークへ、会議も一室に集まる対面の会議から、電話会議・オンラインミーティングへと様変わりした。

在宅勤務をはじめとしたテレワークへの変化で、今まで以上に重要視されるようになったのがITだ。これまでもITを使わずして業務を遂行することは不可能な状態ではあったが、従来は、人が集まるオフィスに整った環境（設備や機器、ソフトウエア）があればよかった。しかし人が集まることができない今、各人に一定のセキュリティ・レベルをクリアするIT環境が必要になった。社員にスマートフォンやノートPCを配布したり、高速でセキュアなデータ送受信に対応するWiFiルーターを支給したりした企業もあったこ

コロナ禍が企業セキュリティにもたらしたインパクト 図1



とだろう。

新たな課題も生じた。クラウドを利用するために数百人分ものアカウントを新規に購入したことから、大きなコスト増につながった例などはその一つだ。また、VPN（仮想私設網）やVDI（仮想デスクトップ）など、リモート接続環境を整えたものの、多くの社員が同時にアクセスできないといった現象が起き、システムを増強せざるを得なくなったところもあった。

また、セキュリティルールについて、これまではオフィスで業務を遂行する前提で考えていたが、在宅を考慮して大幅な見直しが必要となった。中でも、テレワークやオンラインミーティングの機会が増えたことにより、利用時の注意点やルールを新たに周知・徹底しなければならなくなった。例えば、オンラインミーティング時の背景や、画面・マイクのオン・オフの基準などがそれに当たる。ただ、ルールはつくったものの、社員にそれを徹底する困難さは、今も多くの企業が味わっているのではないだろうか。

それらに加えて、テレワークに取り組んでこなかった企業は、これまで禁止していたことを許可して暫定的な対応に踏み切らざるを得なかった。例えば、私用デバイス（スマートフォン、PC）の利用許可、家庭用インターネット回線や公衆無線LANの利用許可、オンラインサービス（会議システムやSNSなど）における私用アカウントの利用許可などである。

大企業ではコロナ禍においても家庭用インターネット回線や公衆無線LANの利用を禁じているところもある。これはセキュリティ上の観点もあるが、それに掛かる費用を会社が負担するのか、個々の社員が負担するのかという点で、判断に至っていない場合もあるだろう。

中でもSNSの個人アカウントの利用は、いまだに大きな焦点だ。使い慣れたツールで業務がはかどる、格別のコストが不要などのメリットがある一方、発言の内容がプライベートなのか企業の見解なのか不透明、アカウントが乗っ取られたり、そのメンバーが退社したりした時にどうなるのかなどの問題もある。今はただ、暫定的な対応として黙認している企業も多いのではないか。

変化に備えていた企業と思考停止した企業

このように、コロナ禍によってITやセキュリティに求める要件が大きく変化する現在だが、明確になったのは、特に影響なく企業活動を継続している企業と、大きく影響を受けて企業活動がままならない企業との差だ。

影響なく企業活動を継続できた企業に共通するのは、2020年以前に在宅勤務やテレワーク環境に対応済み、もしくは何らかのトライアルを行ったことのある企業

だ。一方で、大きく影響を受けた企業は、オフィスへの出勤・対面会議が前提だった企業で、こうした企業の多くでは、緊急事態宣言の発出で社員が在宅勤務という名の自宅待機となり、事実上企業活動が止まってしまった。

いずれにしても大方の見立ては、近い将来に訪れるべきシフトが、大幅に前倒しになったというものだ。

今回の事態は、経営者のセキュリティに対する意識自体にも変化を迫っている。これまでは、隣の街の火事を見てわが家を案ずるという経営者がほとんどだった。新聞で「株式会社〇〇、機密情報が漏洩」という記事を見た経営者が、「うちの会社は大丈夫か？」と部下に尋ねるというパターンだ。

だが、そもそも「うちの会社は大丈夫か？」と言っている時点で、その企業は極めて憂慮すべき状態だと考える。この場合問題視すべきは、同業他社しか見ていないということだ。想像力の欠如した「隣が大丈夫ならうちも大丈夫」という意識が下地にあり、未来を見つめ変化に対応する力が弱くなってしまっているのではなかろうか。

企業にとってセキュリティは事業環境の一部

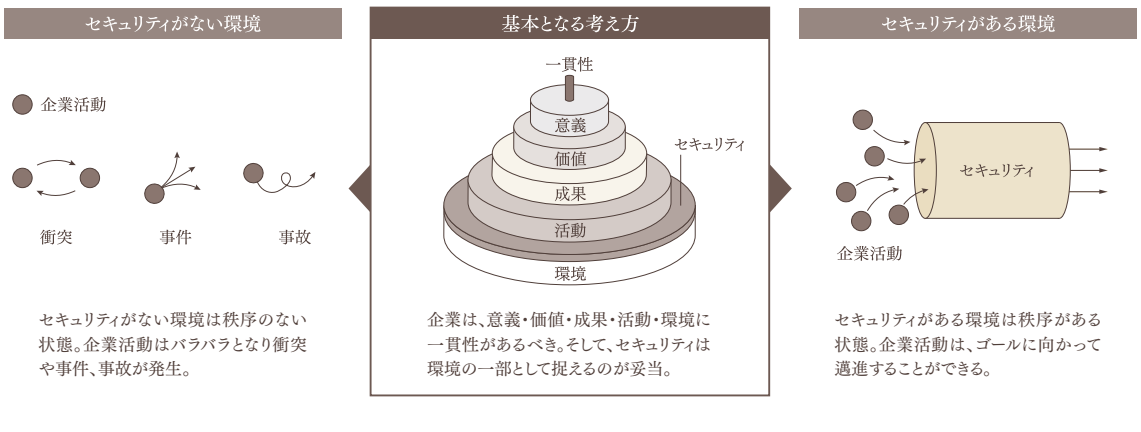
これからも企業は、ある日突然、想定外の事象への対応を迫られることになるだろう。コロナ禍はその学びをわれわれにもたらした。これまで何かあれば、ガイドライン、フレームワークをよりどころに対策を施してきた。例外の少ない平常時ならそれでよかった。しかし、ガイドラインやフレームワークの多くは、過去の事例をもとにつくられている。先が読めない事態では役に立たない。先行きが読めない山道で、バックミラーを見ながらクルマを運転するようなものだ。それでは安全・安心は担保できない。

セキュリティは、企業活動にとってどのようなものなのか。われわれは、「セキュリティとは、恐れや不安から解放された状態をつくる大前提であり、組織やチーム、個人が生存するために整えるべき環境の一部」と定義している。

ブレーキがないクルマに乗る人はいない。しかし、セキュリティに関しては、ブレーキのないクルマで走り出してから後付けでブレーキを取り付ける企業は多い。クラウドサービスをリリースしたので、セキュリティチェックをしてほしいといった相談が当社に寄せられるのはこれに当たる。

一方で、アクセルとブレーキを同時に踏んでいる企業もある。例えばSNS、クラウドサービスを業務で利用することを禁止している企業では、セキュリティを管理している部門が、「リスクがありそうだから全面禁止」と宣言している場合が多い。ビジネスが新しい未来（ビジョン）に向けて動き出そうとアクセルを

事業環境の一部としてのセキュリティの考え方 図2



踏む瞬間、従来の観念にとらわれたセキュリティ意識が足かせとなれば、可能性のあるビジネスを止めてしまうことにもなりかねない。セキュリティも、時代に応じた不断のシフトが必要だ。

ZoomとPPAP。問題はツールにあるのではない

コロナ禍において企業の利用が急速に進んだサービスの一つに、Zoom をはじめとしたオンライン会議ツールがある。ただ、中には Zoom をビジネスで使うリスクを考え、導入をためらう声もある。「Zoom 爆弾」がインターネットニュースで話題になったことなどから、そうした判断に至った経緯がある。Zoom 爆弾とは、オンラインミーティングに呼ばれていない人が、突然勝手に入ってきて、ミーティングを妨げることだ。

ここでもっとも簡単なのは、「NO」ということだろう。使わなければリスクも生じない。ただし、これでは「オンライン営業」、「オンラインセミナー」などによる新規顧客開拓など、新しい成長の芽を摘むことになりかねない。コロナにより企業活動の前提が、対面から非対面にドラスティックにシフトする中、どのように事業の継続・発展に資するセキュリティをデザインし、実装するかが問われている。

この文脈で、PPAP についても考えてみたい。PPAP とは、文書ファイルなどをパスワードが必要な ZIP ファイルにしてメールで送り、パスワードを別のメールで送るものだ。これまで大手企業などで一般的な手順だった PPAP が改めて注目されたのは、2020 年 12 月に、政府におけるデジタル改革 Idea Box で、内閣府・内閣官房が PPAP を廃止したと公表したことにある。「同一経路で暗号化ファイルとパスワードを送る方法は情報セキュリティ対策として有効ではない上、メールを受け取る側にも不要な手間を強いるなどのデメリットがある」というのがその理由だ。その後、一部の公的機関や企業において、PPAP を廃止することが報道され、PPAP は「悪しき習慣」として認知されつつある。

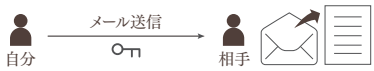
PPAPの問題点 図3

メール添付ファイルの誤送信防止としてのPPAP（正しい手順）

手順❶ 電子ファイルをパスワードが必要なZIP形式で圧縮し、メールにて送信

手順❷ メール添付ファイルを開封し、内容が正しいことを確認

手順❸ パスワードをメールにて送信



PPAPの問題点（PPAPが悪いわけではない）

- 手順❷「添付ファイルの中身を確認していない」が形骸化してしまったことが問題
  もし添付ファイルの中身が間違っていたことに気づけず、パスワードを相手に送ってしまった場合誤送信防止策とはなり得ない

参考 PPAPが嫌がられるケース

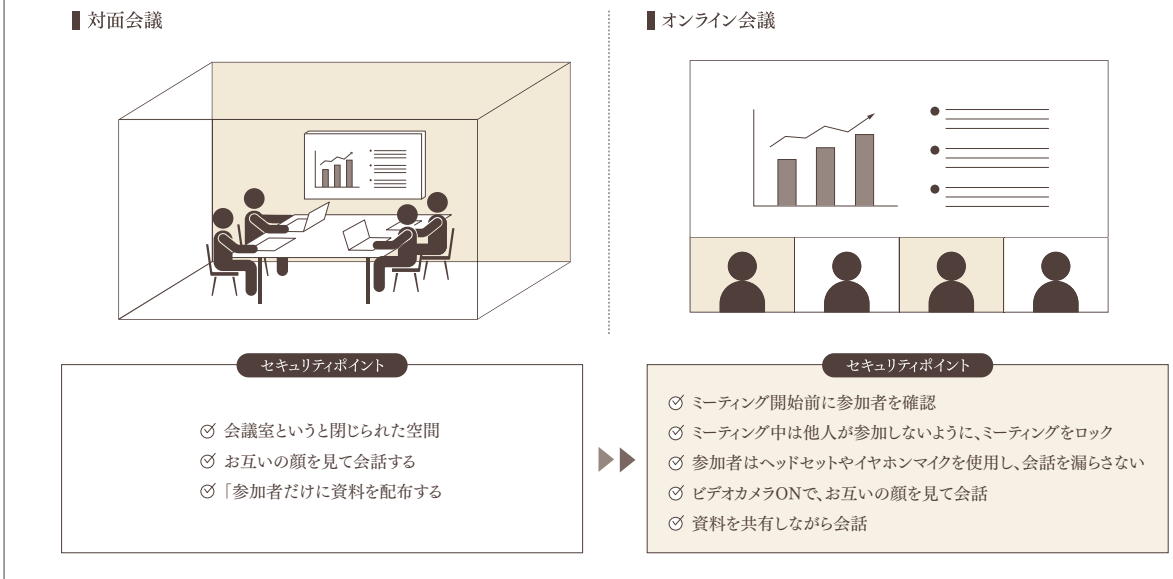
- 相手の企業セキュリティ対策としてPPAPされると、メール添付ファイルのウィルス検査ができない
- PPAPの慣習を逆手に取り、マルウェアをPPAPで送り付けるサイバー攻撃が発生している
- パスワードの送信忘れや、受け取る側のパスワード入力ミスによる問い合わせが発生し煩わしい

だが、この潮流に私は疑問を感じている。というのも、そもそも PPAP とは、電子ファイルをメール送付する際、次の手順を踏むことにより、メールの誤送信を防止するものだったからだ。

① 電子ファイルをパスワードが必要な ZIP 形式で圧縮し、メール添付にて送信
② 送信メールの添付ファイルを開封し、内容が正しいことを確認（間違っていたら手順③は行わない）
③ パスワードをメールにて送信

正しい手順を踏んだ PPAP は誤送信防止策として

Zoomミーティングで実現するセキュリティ　図4



一定の効果があるが、実態として手順②を行わないことが多々あった。さらに、これを逆手に取り、マルウェアをPPAPで送り付けるサイバー攻撃が多発した。

PPAP を始めたころは、何を目的に PPAP するのか明らかになっていたはずだが、月日が流れ、担当者が変わり、「メール添付ファイルは PPAP」というフローが形骸化してしまった。目的を見失い、手段が目的化してしまったセキュリティ対策の代表が PPAP と言える。PPAP が悪いわけではない。

Zoom も同様だ。導入の可否を議論するなら、オンラインミーティングを始めるに当たり、安全・安心な会議を実現するためには、何が必要であるかという問い掛けから始めるべきであろう。PPAP も、ビジネスとして電子ファイルを相手方に確実に送り届けるためには、どのような方法が適切であるかを検討すべきだ。Zoom や PPAP が問題ではない。

自社ビジネスの前提となる環境としてのセキュリティ

こうしたことを踏まえて私が伝えたいのは、「セキュリティを不安産業にしたくない」という思いだ。セキュリティサービスやツールを販売する企業には、リスクをあおるところも少なくない。ツールありきではなく、企業のサービスがどこをゴールとしているのかを見定め、そのために欠かせないセキュリティを検討するのが本筋だ。

セキュリティ単体で考えればどこまでやっても限度がない。だが、自社が目標としているゴールを踏まえると、セキュリティの落としどころも見えてくる。私たちは、セキュリティの必要性をあおって企業を過剰な投資へと向かわせるのではなく、逆に「ここまでできていれば今は大丈夫」と妥当性を説き、コスト削減を提案することもある。例えば、600 万人のユーザーへサービスを提供する事業ならば、その 600 万人のユーザーが安全・安心に使えるセキュリティを環境として整えなければならない。足りなければユーザーをリスクにさらしてしまうが、行き過ぎればユーザーの良好なエクスペリエンスを妨げることになりかねないし、そもそも事業規模が軽自動車の段階で、F1 用のブレーキはいらない。

Zoom、PPAP を例に挙げたが、自社のビジネスが多様な変化に対して柔軟に対応するためには、その前提となる「環境レベル」でセキュリティを実装しておくことが重要だ。ブレーキがないままクルマを発進させたり、後付けのブレーキをばらばらに使用しながらアクセルを全開にしたり、そんなちぐはぐな状態に陥っていないか。今こそ、事業の土台にある「環境」の視点でセキュリティを備える時が来ている。

事業の将来性と社会的意義がセキュリティの在り方を決める

場当たり的で全体感を欠いたセキュリティ対策から脱するためには、「環境」レベルで考えるべきだと述べた。この点に、もう少しフォーカスしてみたい。経営者はまず、自社の社会における「存在意義」を改めて明確にしていただきたい。その上で、以下の 5 階層で企業活動が構成されていることを意識する。

①意義：社会における企業の存在意義
②価値：企業成果がもたらす価値
③成果：企業活動の結果、生み出される成果
④活動：社員や取引先関係者を含む一人一人の活動
⑤環境：企業活動を支える環境
（ここにセキュリティが含まれる）

企業はセキュリティを考えるなら、上記のように存在意義に立ち返ることから始めて、価値、成果、活動へと落とし込み、最後にそれらを受けたセキュリティを含めた環境を整える。このアプローチがないままセキュリティを整えようとすると、企業として一貫性のないものになってしまう。

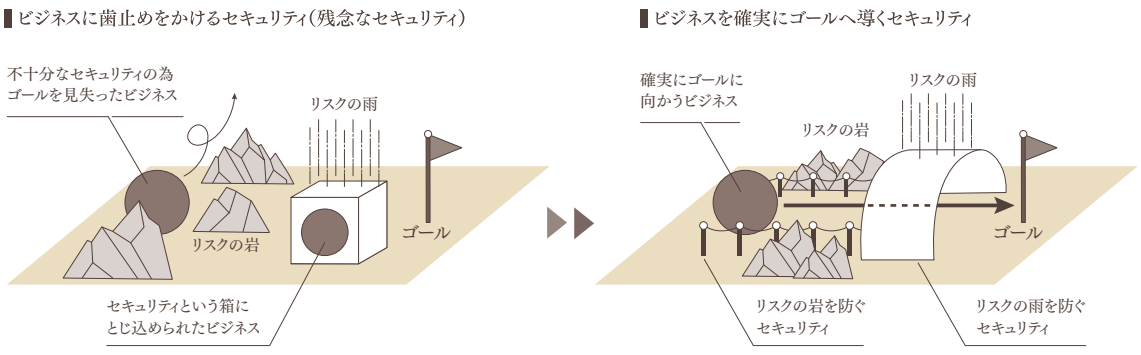
企業全体ではなく、事業単位であってもアプローチは同じだ。「私たちが提供するオンラインサービスの社会における存在意義は何か？」を問うところからスタートし、価値、成果、活動を定め、その上で環境として整えるべき妥当性のあるセキュリティを考えていく流れだ。

企業セキュリティをシフトする

これからの未来、企業はどうあり続けるのか。今、業界規模でも事業単位でも、あらゆる場面や立場において、未来（ビジョン）を描いて、日々活動していることだろう。しかしその時、ビジョンが見えない、そもそも存在意義が見いだせないなど、思考停止に陥っている企業はないだろうか。その一因として、セキュリティが足かせとなっていたら残念でならない。それを感じるのは、次のような相談を受ける時だ。

・顧客向けサービスを完全にオンライン化したいが、セキュリティが怖い

企業セキュリティシフトの概念（残念なセキュリティよ、さようなら） 図5



・自社内外のデータを活用し、新しいビジネスモデルを創出したいがセキュリティが邪魔
・長期間使えるプロダクトを目指してどのようなセキュリティをデザインするか、どのようにアップデートしていくか。そのようなセキュリティ体質がない

このような状況に陥っている企業のセキュリティは、本当に「残念なセキュリティ」である。根本原因は、残念なセキュリティに陥ってしまった環境を放置していたことにある。または、問題が表面化していないため見てみぬふりしてきたことにある。

今コロナ禍により、このような残念なセキュリティがあらわになった企業が多く見受けられる。今こそ、残念なセキュリティとは別れを告げ、企業が次なる未来（ビジョン）を描くため、自由に発想できる環境をセキュリティとして整えるべきである。

安全が確保されておらず、誰もが不安を覚える状況では未来を描くことは出来ない。これからの企業セキュリティは、安全・安心を企業に提供するものであることはもとより、企業が存続するための環境として欠かせない前提条件であることを、経営者、そして企業セキュリティに携わる方は、マインドセットとして心に刻んでおいていただきたい。

繰り返しになるが、未来はビジョンにより決まるものであり、そのビジョンを描くには、安全で安心な環境が欠かせない。その環境の主要な要素の一つがセキュリティである。これを肝に銘じて、新しい未来へ向けてビジネスを力強くシフトさせていただきたい。

西村 啓宏　チーフエキスパート