IDC ANALYZE THE FUTURE

IDC ANALYST BRIEF

Sponsored by: Splunk

デジタルトランスフォーメーション（DX）への取り組み方は企業によってさまざまである。願わくは、今 DX の前に立ちはだかる壁は一時的なものであってほしいと考えている。しかし、人、プロセス、テクノロジーの間には常に調和が必要であることを、我々は何度も繰り返し学んできている。

デジタルトランスフォーメーションによってビジネス成果を上げる新たな挑戦

January 2021

Written by: Chris Kissel, Research Director, Security and Trust Products

序論

2 年ほど前、先駆者や業界アナリスト、先駆的な企業などがデジタルトランスフォーメーション（DX）の未来を熱く語っていた。DX には、データを知見に変えるという魅力があった。DX によって、企業は顧客行動を理解し、その情報を利用して優れた顧客エクスペリエンスを生み出せる。メンテナンスサイクルは、流れ込むデータをリアルタイムに分析することで予測可能となる。多様な分析を繰り返すことで、人間の能力だけでは発見が難しい傾向を明らかにできる。

当時、DX には主に以下の 3 つの促進要因が存在した。

» **自己防衛**：Uber の急速な普及とそれがタクシー業界に与えた混乱や、Airbnb を始めとするさまざまな「ギグエコノミー」が引き起こした同様の混乱によって、企業はこの種の急激な規模拡大に対する脆弱性を直視せざるを得なくなった、というのが率直な見方である。

» **すぐに利用可能な進んだツール**：同じく、2 年前のパラダイムによって、企業はネットワークがいかに変化しているかを理解した。顧客は直接ネットワークにアクセスでき、請負業者はネットワークによる制約の範囲内に留まって業務を遂行できた。パブリッククラウドは、クラウドコンピューティングとアナリティクスを組み込み、アプリケーションの利用を広め、クラウドをホストとして活用するように企業を誘導した。

» **近未来の光景**：企業は当時、IoT（Internet of Things）について、工場の在庫管理や自動化、さらに個人のウェアラブルデバイスに活用することを思い描くと共に、その応用にも可能性を見出していた。さらに、5G ネットワークが利用可能になることは、有線イーサネットの速度を無線で実現できることを意味していた。

当然のことながら、DX を概念として理解することと、デジタルを使わない状態から、実際に DX に移行して業務を加速することとは、まったく別である。しかし、DX ジャーニーで企業が経験するプ

AT A GLANCE

要点

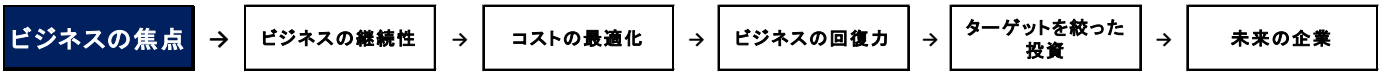
良くも悪くも、新型コロナウイルス感染症（COVID-19）の世界的な感染拡大は、デジタルトランスフォーメーション（DX）の導入を加速させた。DX をさらに推進するために次に何が必要なのかやっと気づいたにすぎない。

押さえるべきポイント

企業が、陳腐化の罠を避けるため先を見据えて考えるためには、（データ、IT、セキュリティ、運用に関わらず）協力できるベンダーが必要である。

ロセスから、やがて 1 つのパターンが出現し始めた。Figure 1 は、DX を実現するために企業が辿る一連の過程を IDC が描き出したものである。

FIGURE 1：***DX を実現するまでに企業が辿る一連の事象***



Source: IDC, 2020

このマッピングは、厳密ではないにしても説明には妥当なところであろう。たとえば、レストランなどではビジネスの継続性の確保は難しくないかもしれないが、製造業の場合は、プロセスの刷新や再構築は相当に手間のかかる作業となる。DX の取り組みに合わせて予算を配分することは難しく、プロセスを最適化するのも容易ではない。しかし、要点は、企業が予定通りに DX ジャーニーを開始し、時間と共にコントロールできることである。

ところが突然事態は急変した。中国の武漢で新型ウイルスが発生した。数か月のうちに新型コロナウイルス感染症（COVID-19）が世界中に広まり、パンデミック（世界的大流行）によって感染者が広がり、多くは死に至った。最善策（かつ、現時点で最善の予防策）は、ソーシャルディスタンスを保つことである。

「口にパンチを受けるまでは、誰であろうとゲームプランを持っている」

—Mike Tyson 氏

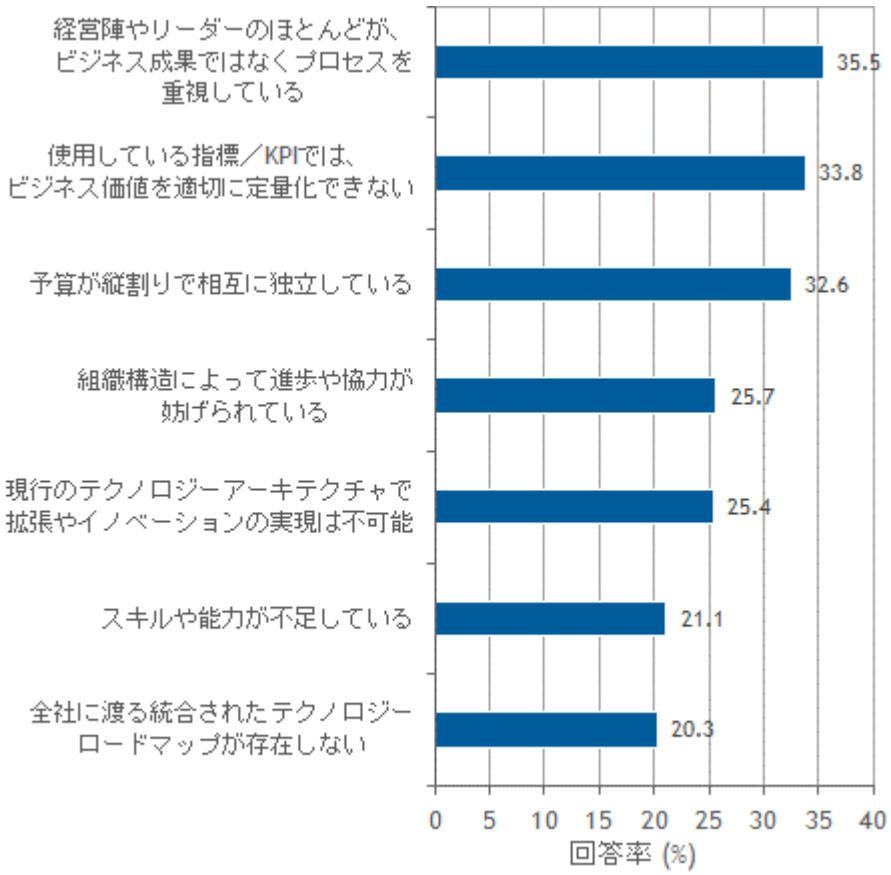
適応した企業もあったが、完全に廃業した企業も多い。リモートワークフォースの維持や必要性について考えもしなかった企業が、在宅勤務（WFH：Work-From-Home）モデルを導入しなければならなかった。VPN（Virtual Private Network）やビデオ会議などの一時しのぎのテクノロジーソリューションが、急遽用意された。最終的には、計画的に進めていた DX 変革が、突然、無計画に適用されてしまった。「口にパンチを受けるまでは、誰でもゲームプランを持っている（Everybody has a plan until they get punched in the mouth.：訳注 準備があっても対処可能とは限らない）」と語った元ヘビー級チャンピオンの Mike Tyson 氏は、明らかに DX の予言者でもある。

グローバル企業にとって、COVID-19 は、口にパンチを受けた状況と言っても過言ではない。

IDC は 2020 年 2 月中旬から、COVID-19 が組織の業務運営（人材、プロセス、テクノロジーなどあらゆる側面）に与えた影響について、一連の調査を開始した。Figure 2 は、これらの調査のうち 2020 年 11 月に実施された 15 回目の結果から引用している。興味深いのは、COVID-19 が DX プロジェクトのビジネス成果に現時点で与えた影響についてたずねた質問である。

FIGURE 2：***DX からビジネス価値を導き出す上での課題（上位 7 項目）***

Q *貴社の DX プロジェクトから価値が引き出され、具体的なビジネス成果を示す上で、最も大きな課題は何ですか？*



n = 619

Source: IDC's COVID-19 Impact on IT Spending Survey, November 9–23, 2020

本調査では、幅広い問題が指摘されたが、以下のような大きな傾向が、あらゆる種類の組織において根強く存在しているようである。

» **成果ではなくプロセスが重視されている**：この見解は、DX のアンチテーゼのように見えるが、非常に人間的とも言える。企業は WFH 用のビデオ、オーディオ、電話設備に即座に投資しなければならない。多くの場合、従業員の再教育も実施しなければならない。事業継続は、ターゲットを絞った投資よりも優先すべきである。

» **ビジネスとセキュリティとの言葉の溝を埋める**：セキュリティは高度に専門的な分野である。セキュリティオペレーションセンター（SOC：Security Operations Center）以外のチームにとって、セキュリティ担当者の仕事は複雑で理解しがたいものに思える。残念なことに、こうした状況が、チーム間の連携を妨げる意思疎通の欠如につながり、取り組みの定量化を難しくしている。リスクに応じた属性が分かれば、潜在的な脅威についてさまざまな情報が明らかになるため、組織内のチームは、一見ばらばらに見えるアラートをどのようにつなぎ合わせれば、分

かりやすく一貫性のあるセキュリティの筋書きにつながるのかを理解できる。各種の属性に基づいた（attribution-based）新たなアプローチをとることで、SOC と企業との間にさらに緊密な協力関係が構築され、全体のセキュリティ保護体制を向上させることができる。

» **サイロ化した思考はテクノロジーに留まらない**：IT においては、IT 運用とセキュリティ運用との間に以前から線引きがなされている。残念なことに、本調査では、予算や業務にもサイロ化が見られ、それがイノベーションやスケーラビリティを阻んでいることが分かった。ソフトウェアやコミュニケーションを統合して、業務の一本化を実現することはかなり難しいが、喫緊のニーズに注力するために予算を振り替えることさえ、組織的な課題なのである。

» **テクノロジーロードマップとスキル不足については、課題としての順位が意外にも低い結果となった**：この結果には少し疑問が残る。現在、企業は目の前の問題で手一杯という状況にあるだけかもしれないため、ロードマップについては、この順位が当てはまらない可能性がある。

しかし、DX の構造（Figure 1 を参照）や、調査で IT 関係者が挙げたあらゆる不満（Figure 2 を参照）については、新たな解釈やベストプラクティスが、ソフトウェアプロバイダーにとって役立つであろう。

企業の DX ジャーニーを成功させるために IT およびセキュリティベンダーができること

おそらく、DX に生じている最も重大な変化は、ビジネスの運用方法に関して COVID-19 が強引に引き起こした一時的な変化とそれに続く DX プロセスの加速的な展開スピードであろう。もし DX 変革を、必ずしも時間をかけてじっくり進める必要がないのであれば、企業はストラクチャの問題を（引力からの）脱出速度並みのスピードで解決しなければならない。そうした課題は、過去においても現在においても、非常に困難なものであるが、IT、業務運営、セキュリティ、そして DX に対するソフトウェアベンダーの考え方も変わらなければならない。以下の手法は、ソフトウェアベンダーが DX を支援する際に、最も効果を発揮してきたものであり、今後最も重要となるものであろう。

» **「ニューノーマル」が現在のノーマルであることに気づく**：企業にとっては、自社の環境で使うことのできる、可能な限り既製（レディーメード）のソフトウェアが必要であった。企業が新たな VPN を導入する際には、IT サービスマネジメント（ITSM：IT service management）や LDAP（Lightweight Directory Access Protocol）を組み込んだ製品を提供するベンダーを選ぶしかなかった。ツールも組み込まれていなければならない。企業には長期に渡って概念実証を行う余裕がないため、ソフトウェアベンダーは、拡張性の高いツールを導入し、すぐに使用でき、すぐに効果が出る機能を提供することで、対応しなければならない。

» **できるだけ多くのサイロを排除する**：企業にはサイロについての問題があるようであるが、ソフトウェアベンダーにはそうした問題はあってはならない。この見解は単純化しすぎているように思えるかもしれないが、それは一見したところでは分かりにくい。ネットワークに関して言えば、事業部門の最大の関心は、商品やサービスが可能な限り容易に利用できるかということである。つまり、問題の原因がサイバーセキュリティ侵害であろうと、ネットワークのボトルネックであろうと、ユーザーの過失であろうと、誰も頓着しない。ネットワークの最適化が最優先事項である。それが、最も安全な手法を目指した、IT と SOC の再編成や、エンドユーザ

ーのトレーニングを意味するのであれば、こうした統合はソフトウェアにおいて行うべきである。

» **経営幹部に分かりやすい言葉で説明する**：回答者の約 34%が、指標／KPI がビジネス価値を的確に定量化していないと答えた。サーバーの可用性（アップタイム／ダウンタイム）、平均検出時間（MTTD：Mean Time To Detect)／平均修復時間（MTTR：Mean Time to Respond）、および警告数と処理された警告数の比較などは、技術者にとっては大きな意味を持つが、これらの指標は商品開発の担当者にとっては無意味であり、またビジネスの損失や利益を定量化できなければ、CEO にも、事実上取るに足らない問題として処理される恐れがある。事前の切り分け作業（トリアージ）によって失われた工数、失われた e コマースの売上、あるいは規制当局による罰金がどれほどの額になるかなどが、皆の関心を呼ぶ。スマートツールのプロバイダーは、ダッシュボードでこうした類の変換を実現したいと考えているかもしれない。

» **新たなネットワークサーフェス（接面）を描く**：DX が実施される前でさえ、ネットワークは絶えず変化し、IoT、モバイル、ダイレクト to ユーザー（ユーザーとの直接コンタクト）アプリケーション、パブリッククラウド IaaS、そして恐らくソーシャルメディアさえも取り込む仕組みを推進してきた。サイバーセキュリティ戦略は、こうしたサーフェスすべてを考慮して策定されなければならない。さらに、サイバーセキュリティは、予防、検知、対応といった従来の機能だけを指すのではない。サイバーセキュリティの保護体制（posture）には、企業の回復力、苦情対応業務、リスク評価、正常起動時の構成（known good configurations）、災害復旧、および個人の責任なども組み込まれていなければならない。

» **プロセスを自動化する**：IDC は、IT とセキュリティのプロセスを可能な限り調和させ、その結果である指標／KPI はビジネス上の成果に連動する形で示すべきであるという、かなり思い切った提案をしているが、ワークフロー自体を標準化することは当然である。SOC のインシデントで発生する、誰が／何を／どこで、といった類の情報の大半は、ボタン一つでアナリストに提供されるべきである。また、次に何をすべきかについては、プレイブックに概要が記載されていなければならない。自動化によって、事業の継続性の確保や、ヒューマンエラーの軽減といったメリットが生まれる。

» **より多くのデータを使うべきだが、それは一度に限る**：データにはそれぞれの重要性がある。しかし、そのデータを繰り返し使うと、その完全性が失われ、データ処理の不手際によってプライバシーに対する損害賠償が発生する可能性が高くなる。

» **リスクを考慮する**：現実には、最高の安全性を誇るネットワークであろうと侵入される可能性がある。データ保護において、ソフトウェアベンダーは、個人を特定できる情報（PII：Personally Identifiable Information）と知的財産を特に重視しなければならない。また、ベンダーは、ネットワークに関して、インターネットに接続する機器や Web／メールサーバーなどのビジネス資産が脅威にさらされることを SOC が防ぎ、またこれらの機器への不正アクセスのために敵対者に利用される恐れのある漏洩経路を明確化する必要がある。ソフトウェアベンダーがリスクを明確に説明すれば、それに応じて提供できる価値は高まる。

結論

パンデミックによって、多くの企業が突如として DX を強いられることにはなったが、変革（トランスフォーメーション）自体は、包括的、継続的かつ発展的なプロセスとして理解すべきである。「包括的」である理由は、DX にはアナリティクスやワークフローだけでなく、ネットワーク、IT、通信、サイバーセキュリティも含まれており、さらに、ネットワークがインタラクティブになった（ほぼ無制限の相互通信性を備えた）ためである。DX が「継続的」である理由は、DX にはメンテナンスが必要であり、それは、多くの企業が、緊急保護（immediate protection）のためにシステムを設置する際に発生することになる技術的負債（technical debt）であるとして説明することになるであろう。世界全体が、何とか無事に COVID-19 を乗り越えられれば、次世代の DX は、拡張現実や、5G ネットワークを利用した、これまで想像もしなかったような新しいアプリケーションを始めとする、文字通り没入型に「発展」していくであろう。

アナリストについて

Chris Kissel、リサーチディレクター、Security and Trust Products

Chris Kissel は、IDC の Security and Trust Products グループのリサーチディレクターであり、サイバーセキュリティテクノロジー分析、新たなトレンド、市場シェアの報告などを担当している。同氏の主な研究分野は、サイバーセキュリティアナリティクス、インテリジェンス、レスポンス、オーケストレーション（AIRO：Analytics, Intelligence, Response, and Orchestration）である。この業務における主な技術グループには、SIEM、デバイスとアプリケーションの脆弱性管理、脅威アナリティクス、自動化およびオーケストレーションのプラットフォームなどがある。同氏は、セキュリティオペレーションセンター（SOC）のアナリストが、セキュリティおよび脆弱性の管理、ならびにセキュリティアナリティクスパラダイム内で、ネットワークを攻撃しようとする脅威アクターを監視、検出、修復、緩和するために採用するプロセスについて効果的に取り上げている。

スポンサーからのメッセージ

Splunk（スプランク）について

Splunk は、貴社のテクノロジーインフラストラクチャ、セキュリティシステム、およびビジネスアプリケーションから生成されるビッグデータの未開発の価値を簡単に収集、分析、処理することで、運用パフォーマンスとビジネス成果を促進する知見を貴社に提供します。***こちらのサイト***からご希望の無料トライアルの提供方法を選択し、Splunk のパワーを体験してください。

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
5 Speen Street
Framingham, MA 01701, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com