掲載日時： 2021-01-04 06:30

クラウド、職場、セキュリティ--激動経て、2021年に注目したいテクノロジー動向

2020年は企業がデジタルトランスフォーメーション（DX）を加速させるために動かざるを得ない年だった。2021年はどのような1年が待ち受けているのだろうか。海外各国のZDNetの記者が展望した。

著者 : Larry Dignan Chris Duckett Steve Ranger （ZDNet.com） Bill Detwiler （TechRepublic）

URL : https://japan.zdnet.com/article/35164372/

2020年の企業は、つぶれたくなければデジタル化するしかなかった。デジタルトランスフォーメーション（DX）が技術的なプロジェクトを後押しし、コロナ禍によってリモートワークやリモート教育が当たり前のものになり、クラウドコンピューティングや、人工知能（AI）や、機械学習などの要素技術の発展が加速した。

Salesforceのプレジデント兼最高執行責任者（COO）であるBret Taylor氏は、ビジネスの現状について「デジタル化されていないビジネスはビジネスではない」と一言で説明している。

2021年のビジネステクノロジーに関する展望に期待できることは確かだが、不確定要素も多い。例えば、次のような問題がある。

今後、仕事のニューノーマル（新しい日常）はどのようなものになり、コラボレーションはどのように発展していくのか。

企業は、職場文化を維持するためにどのようにテクノロジーを利用していくのか。

今後、技術的なプロジェクトのマネジメントのあり方は変わるのか。

エッジコンピューティング、5G、クラウド、自動化は各産業にどのような影響を与えるのか。

疑問への答えがすべて分かっているわけではないが、この記事では、海外各国のZDNetの編集リーダーが、2021年の展望についての見通しをいくつか示すことにしたい。

2021年は2020年のDXラッシュの延長線上にある

Larry Dignan

2020年には、企業の急速なデジタル化や、リモートワークへの移行や、DXの大幅な加速などさまざまな変化が起こったが、2021年の最大の不確定要素は「その中の何が定着するのか」ということかもしれない。

明らかなのは、仕事とコラボレーションのニューノーマル（新しい日常）が生まれるということだ。また、コラボレーション技術が進歩することと、ハイブリッドな業務体制や、業務継続に必要なクラウドコンピューティングなどの基本技術に対する関心の高さが今後も続くことも確実だろう。仕事のリモート化がこれ以上進展するとは考えない人もいるが、それは誤りだ。リモートワークにはあまりにも経済的なメリットが多い。企業はオフィス用不動産の経費を削減でき、従業員を雇用できる地域を広げられ、生産性も維持できる。

筆者の予想では、PCベンダーや、新しい企業のアライアンスが、仕事の新しい日常に参画するためにイノベーションを推進するだろう。解決すべきことはすでに分かっている。これまで、同じ部屋に集まって行っていたことをどうするかだ。例えば研究室もそうだし、プロトタイピングの作業や、業務フローの改善などもそれにあたる。あるいは2021年には、企業における拡張現実（AR）や仮想現実（VR）の使い方が発達するかもしれない。

以下では、2021年に注目を浴びる可能性があるその他のテクノロジーをいくつか挙げておく。

量子コンピューティング。2020年の量子コンピューティング業界は順調に発展したが、2021年にはこの技術の導入がこれまで以上に一般的になるだろう。今この業界に欠けているのは、クラウド経由で利用される量子コンピューティングのアプリケーションスタックだ。また、この技術が定着するにつれて、ベンダーの間に新たな序列が生まれるだろう。

3Dプリンティングおよび付加製造。コロナ禍によって、サプライチェーンには大きなギャップがあり、製造業には素早く対応する能力が必要であることが明らかになった。2020年中には、金属や新しい材料を使った3Dプリンティングや、さまざまな業界に特有の利用事例が発達したが、サプライチェーンの問題を完全に解決するまでには至らなかった。また3Dプリンティングの企業は、コロナ禍で顧客の状況が悪化したことで打撃を受けた。2021年には、付加製造分野への投資が増えるだろう。また、製品のパーソナライズが大幅に進む可能性がある。

マルチクラウドへの移行が加速する。新型コロナウイルスが蔓延すると、クラウドファーストの方針を取っていた企業が優れた業績を上げた。また現在、多くの企業が、マルチクラウドの導入を計画している。問題は、顧客がハイパースケーラーを信頼して複数クラウドの管理を任せるようになるかどうかだ。筆者の直感では、既存のデータセンター事業者が、他のクラウドのリソースも一元的に管理するようになる可能性が高い。

自動化、人工知能（AI）、機械学習。ワークフローは急激な勢いで自動化されつつある。2020年が自動化の必要性を明らかにした年だったとすれば、2021年は自動化が本格的に展開される年になるだろう。簡単に言えば、AIと、機械学習と、ロボティックプロセスオートメーション（RPA）に任される仕事が増えることになる。最大の問題は、これらの技術をうまく管理することができるかどうかだ。

職場の安全確保のためのソフトウェアには見直しが必要になる。ServiceNowやSalesforceのような企業は、職場の安全確保を、わずか数カ月のうちにソフトウェアの1つのカテゴリーとして確立した。今日では、職場の安全確保ツールが、労働者や、労働者の健康状態や、新型コロナウイルス検査や、パンデミックへの対応の管理に使われている。しかし、ワクチンの登場によって状況は変わるはずだ。Salesforceは、すでにワクチンの配布管理に「Work.com」を使用している。2021年の今頃に、このカテゴリーのソフトウェアがどうなっているかは未知数だ。

提供：Service NSW

2021年もワクチンが行き渡るまではQRコードのスキャンに頼る年に

Chris Duckett

欧米では、この10年間のほとんどの期間、ニッチな領域に定着できなかったテクノロジーの冗談を言いたければQRコードの話をすればよかった。

QRコードを使ったWalmartの決済システムも笑われたし、MicrosoftがブルースクリーンにQRコードを表示したときにもジョークになった。

米ZDNetの過去の記事でも、「QRコードは、一時的な流行で終わってしまうのを回避する必要がある」とか「QRコードを利用しようと思うのはやめるべきだ」などとたびたび書いてきた。これらの表現が使われたのはどちらも2012年の記事で、QRコードの普及には最初から抵抗があったことを示している。

欧米から見れば、2019年までのQRコードは、広告に表示されている単なる邪魔な模様でしかなかった（欧米では、アジアではQRコードが一般的に使われていたことが都合良く忘れられてしまっているのだが）。

「Android」カメラでQRコードをスキャンしたことがあるユーザーは滅多におらず、「QRコードなんてどうでもいい。誰もあんなものは使わない」というのが2019年までの普通の反応だった。

しかしコロナ禍に襲われたことで、QRコードは再び息を吹き返した。

新型コロナウイルスをある程度管理できた地域（例えばオーストラリア、シンガポール、ニュージーランド）では、あらゆる場所にQRコードが貼られ、誰もがそれをスキャンした。これは、政府が市民に、人が集まる場所や飲食店に入るときにはQRコードを使ってチェックインすることを求めたからだ。

呪われた2020年の経験から言えば、デジタルシステムはある1点で人間にとって有利なシステムだといえる。ウイルスはペンや紙などの物体に付着した飛沫で感染する可能性があるが、非接触型のシステムであればそのリスクを回避できるのだ。保健当局にとっても、デジタルシステムは、ある施設で陽性の患者が発生した際に接触状況を調べるための信頼できる唯一の情報源を生み出してくれるし、データベースがクラウド上にあれば、紙が破れたり、なくなったり、こぼしたビールで水浸しになる可能性も低い。

2020年がQRコードが復活した年だとすれば、2021年は多くの国がパンデミックを乗り越え、経済活動を再開するためにQRコードを大規模に使用する年になるだろう。すでに普段の状態に戻りつつある国では、ワクチンが届くまでの間、QRコードが日常生活の一部になると考えられる。

QRコードの奇妙な四角の模様は、あっという間に「邪魔なもの」から命を救うかもしれない存在へと変わったが、2021年にも私たちの生活の中にとどまる可能性が高い。

新型コロナウイルスについてもう少し書いておきたい。以前は、Googleが提供しているAndroidの標準カメラアプリは、デフォルトの状態ではQRコードを読み取れなかった。コードを読み取るには「Googleレンズ」を使う必要があった。この状況は変わってきたが、そうでなければ多くの人が混乱していたかもしれない。

これは特に意外ではないが、サムスンのカメラアプリは以前からQRコードの読み取りに対応している。

提供：Getty Images/iStockphoto

上司が在宅勤務による生産性向上の障害になる可能性がある

Steve Ranger

2021年は、ようやく上司が在宅勤務を生かせる（あるいは完全に台無しにする）年になるだろう。

2021年のビジネスライフで確実に変わるとみられる点が1つある。ワクチンで生活が普段の状況に戻っても、リモートでの在宅勤務があたりまえになるということだ。

この1年間で、リモートワークでもオフィスと同じかそれ以上に働けることが証明されたため、今後上司がスタッフはオフィスでしか働けないと言い張ることは難しくなる。

優れた組織や経営者は、どうすればオフィスを最大限に活用できるかを考えるようになるはずだ。ただし、在宅勤務でも生産性は維持できるが、創造性は低下する可能性があると指摘されている。これは、オフィスは各席に従業員を詰め込むための場所ではなく、相互作用と創造性を促進するための場所にすべきであることを意味している。

オフィスはチームで新しいプロジェクトや新しいアイデアに取り組むために使用し、それを発展させていく作業は、どこでも適切な場所で行えばよいということだ。

この考え方に従えば、オフィスを今よりも小さくし、デスクの数を減らし、ミーティングスペースを増やす方向に向かうはずだ。そのバランスを取り戻せば、チームの満足度は上がり、創造性も

高まり、その一方であらゆる気が散る要因を排除して自宅で生産的に作業するチャンスも作ることができる。

しかし上司の中には、その教訓を理解できない者もいるかもしれない。リモートワークは構わないが、スタッフが業務時間に行っているすべての作業を常に監視した方がよいと考えるようになるマネージャーもいるだろう。

2021年は、業務時間中に自宅で実際に働いていることを確認するためのリモートワーク監視ツールに投資する経営者もいるだろう。これらのツールは、従業員のベッドルームをパノプティコン（一望監視施設）の一部のようにしてしまう。しかしこのやり方では、従業員の信頼が損なわれ、従業員は自分たちがスパイされていると感じるようになる。

2021年には、自分の会社をどんな企業にしたいか（あるいは自分がどんな上司になりたいか）を考える必要がある。

セキュリティ：2021年の新たな常識

Bill Detwiler

これまで議論してきたように、2021年は2020年に起こった出来事の影響を色濃く受ける年になる。セキュリティに関しては、特にコロナ禍とSolarWindsを悪用した攻撃という2つの問題は、長く社会に爪痕を残すはずだ。

企業がDXの取り組みを加速させ、クラウドや自動化、モバイル決済、XaaS、AI、5Gなどの新しい技術を取り込もうとすると、攻撃者もシステムの弱点を悪用しようとする取り組みを増やし、セキュリティリスクが上昇する。

同様に、コロナ禍はリモートワークのトレンドの転換点となった。世界中の企業がオフィスを閉鎖し、非常に多くの従業員が初めて在宅勤務を経験した。2021年に入ると、新型コロナウイルスワクチンの接種が増えるに従い、一部の労働者はオフィスに戻っていくだろう。しかし、オフィスの再始動には時間がかかり、多くの労働者にとっては、ハイブリッドモデル（主にリモートで働き、オフィスで働く時間が減る）が新たな日常になるはずだ。サイバー攻撃者は、この事態になるとすぐにリモートワーカーに狙いを付けた。2020年前半にはランサムウェア攻撃の件数が急増し、フィッシングメールの発生率も上昇したほか、リモートワークに使われることが多いモバイルデバイスにおけるフィッシング攻撃も増えた。2021年にはリモートワーカーへの攻撃がさらに激しくなる可能性が高い。IT部門とリモートワーカーは、どちらも常に警戒を怠らず、安全に在宅勤務を行うためのベストプラクティスに従う必要があるだろう。

当然ながら、ITリーダーはすでにリモートワークとセキュリティの問題に対応するために予算を修正しようとしている。米TechRepublicが実施した2021年のIT予算に関する調査によれば、回答者の26％は従業員の在宅勤務を可能にするためにリモート技術に対する支出を増やすと答えており、22％はセキュリティへの支出を増やすと回答していた。

SolarWindsの製品に対するサプライチェーン攻撃は、過去10年間で最大規模の被害をもたらしたサイバー攻撃だと言っていいほどのもので、世界中で1万8000社が影響を受けたとみられる。被害を受けた組織には、米連邦政府の国土安全保障省（DHS）、国務省、財務省、商務省、国立衛生研究所（NIH）なども含まれていた。サプライチェーン攻撃は特に新しいものではないが、SolarWindsに対する攻撃のスコープと規模、そして攻撃で狙われた標的が、この攻撃をとくに厄介なものにしている。また、攻撃者も問題だ。

Mike Pompeo国務長官は米国時間12月18日のインタビューで、今回の攻撃とロシアを結びつけ、「これは非常に重大な攻撃だ。私の考えでは、ロシア人がこの活動に関与したことは極めて明確だといえる」と述べている。ロシア政府は関与を否定している。

米国政府は過去にもサイバー攻撃や情報漏えいを経験しているが、今回の攻撃は異なっているように感じられる。

今回のインシデントに関しては、Dick Durbin上院議員（民主党、イリノイ州選出）などの議員や、匿名の政府関係者や、現政権の元高官が警鐘を鳴らしており、その多くが報復措置を求めている。すでに措置が計画されている可能性もある。NPRや米CNNなどを含むメディアは、米政権はロシアのウラジオストクにある領事館を閉鎖し、エカテリンブルクの領事館の業務を停止する予定だと伝えている。

2021年には、米国政府や重要インフラで使用されるソフトウェアやサービスを提供する企業のサイバーセキュリティ対策が一層吟味されるだろう。また、製品に求められるセキュリティ要件に関する新しい法律や規制や、ITの分野で進んでいるコンシューマライゼーションの再考を求める声も出てくる可能性が高い。

いずれにせよ、何かを変える必要があることは明らかだ。政権が変わってもその事実は変わらない。

Joe Biden次期大統領は12月17日、今回の攻撃とサイバーセキュリティに対する次期政権の対応について、「私の政権では、政府のあらゆるレベルにおいてサイバーセキュリティを最優先事項とし、政権が移行した瞬間から、今回の侵害に最優先で対処することを明確にしておく」との声明を出している。Biden氏はまた、「わが国の敵は、私は大統領として、わが国に対するサイバー攻撃を手をこまねいて傍観することはないと知るべきだ」とも述べている。

この記事は海外Red Ventures発の記事を朝日インタラクティブが日本向けに編集したものです。
