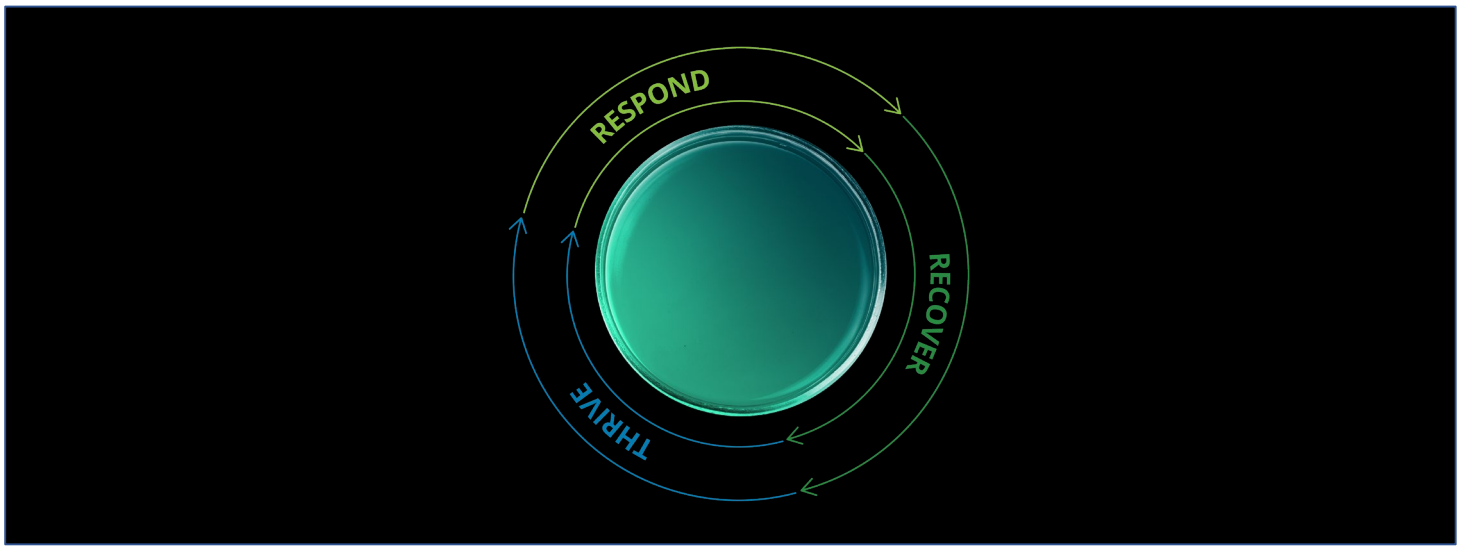
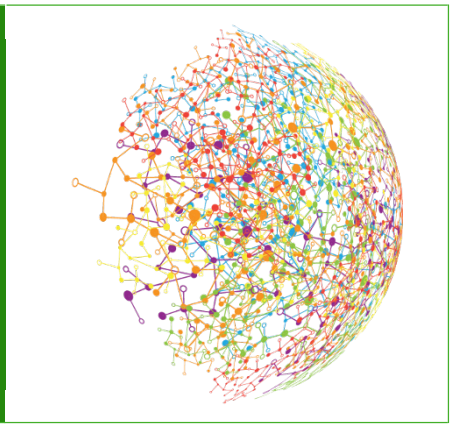
Deloitte.



COVID-19 がサイバーセキュリティをNext Normalに向けて再編

リモートワークは、業務効率、脆弱性、および複雑さを生み出している。

COVID-19の混乱をこれほど深刻なものにしたのは、ほとんどの組織が世界的なパンデミックを事業継続計画に織り込んでいなかったからである。COVID-19は、サイバー攻撃や自然災害、サプライチェーンの混乱といった事業継続計画でベースとなる一般的な緊急事態とは異なり、全てが元の状態に戻る、というきれいな結末にはならないだろう。
COVID-19はすでに、人、プロセス、テクノロジーに関する戦略に根本的かつ永続的な変化を与えており、強靭な組織であることの意味を問われている。簡単に言えば、誰もがどこからでも仕事ができるようになる日が迫っているということである。



Next Normal (新しい日常)

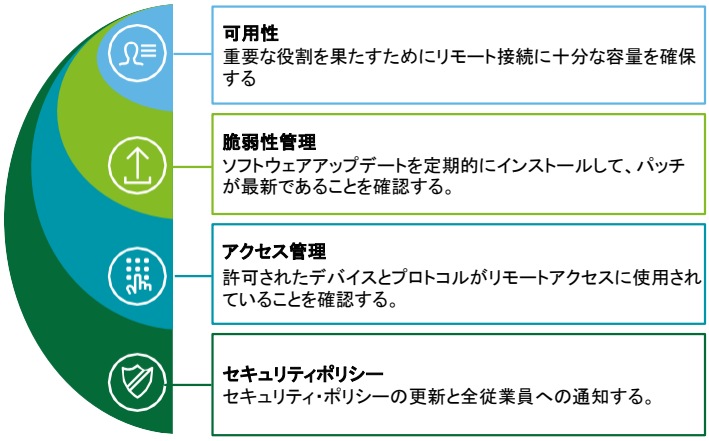
一夜にしてロックダウンになり、世界中の企業が、従業員が在宅勤務を余儀なくされる状態に陥った。これにより、以下のような多面的なサイバーセキュリティストレッサーが生まれた。

- **” BYOD (Bring Your Own Device)”の爆発的増加–** 多くの従業員は、自宅用のノートパソコンを会社から支給されていない。これは、脆弱性のあるデバイスや既に危険にさらされているデバイスを使って企業ネットワークやシステムにアクセスしていることを意味する。同様に、従業員はウェブ会議やコラボレーションツールに大きく依存しており、脅威の主体(”Zoom-Billing” をめぐる最近のニュースはその最も顕著な例だが、唯一の例ではない)によって危険にさらされる可能性がある。一夜にして企業の攻撃対象領域（アタック・サーフェイス）が拡大したため、セキュリティの複雑さが大幅に増大している。

アメリカ、イギリス、ドイツの企業の30%において、ITに詳しくない従業員1,000名以上が毎日セキュリティ保護されていない自分のデバイス企業のネットワークにアクセスしている。

- **ホームコンピューティング環境**– 企業は、従業員のホームコンピューティング環境を制御できない。COVID-19 危機の環境から発生した問題は、ルームメイトと同居しており業務を行うのが難しいというものや、通信速度が遅くテレビ会議がスムーズに行えないというものまでに及んだ。また、テレビからトースターに至るまで、あらゆるものがインターネットに接続されている可能性があるため、一般的な家庭環境では、IoT（モノのインターネット化）の脆弱性が特に問題となっている。真の”work from anywhere (自由に働く場所を選ぶ働き方)”未来のために、セキュリティチームやIT全般は組織に過度のリスクや生産性の低下をもたらすことなく、リモートワーカーが仕事を遂行できるようなプログラムやプロトコルを開発する必要がある。
- **安全なリモート・アクセス**–ほとんどの企業は、すべての従業員がネットワークやシステムに安全にリモートアクセスできる環境を整えられていなかった。レガシーシステムに依存している組織では、パフォーマンス、スケーラビリティ、や可用性の問題が発生しやすいため、特に問題となる。米国では多くの州の失業事務所で膨大な請求処理に古いCOBOLベースのシステム（その一部は数十年前のものもある）を使用していたという問題も明らかになった。リモートアクセスもまた、内部脅威の問題をもたらす。従業員が自宅から好きなデバイスでのアクセスを可能にするのであれば、適切なセキュリティ衛生と企業のセキュリティポリシーも理解する必要がある。また、セキュリティ・チームは、強固なID管理とアクセス管理を実装し、異常な動作を簡単に検出して対応できる、ゼロ・トラスト・モデルを採用する必要がある。
- **インサイダーの脅威** – 労働や経済情勢により今後もインサイダーの脅威は拡大するだろう。リーダーは、リスクベースのインサイダー脅威監視プログラムを追求するためどのように備えているかを検討する必要がある。故意かどうかに関わらずサイバーインシデントの大半は、インシデントを受けた組織の従業員によって引き起こされているのである。
- **安全でない“アドホック”プロセス**– セキュリティ保護されたオフィス環境のために設計されたビジネス・プロセスは、現在、セキュリティ保護されていない分散した、自宅環境で行なわれている。例えば、COVID-19 が登場するまでは、自宅からの住宅ローンを承認する銀行はなかった。しかし、“Next Normal（新しい日常）"の下では、銀行はこの新たなアドホック・プロセスに適応せざるを得ない。（一斉に融資を停止しない限り）。短期的には、セキュリティチームはこの新しいプロセスにセキュリティとコンプライアンスを組み込む必要があるが、これは簡単なことではない。アイデンティティの認証、サポートドキュメントへの安全なアクセスの確保、政府システムへのリンクバックのすべてを、企業が貸与していない個人用ノートパソコンから行う必要があるが、この手順書はない。これまでにリモートで実行されたことがないためである。今後、あらゆるタイプの企業が社内プロセスを評価し、リモート作業環境へ安全に移行できるように必要な手順を実行する必要がある。

こうしたサイバー上の課題は、企業にデジタル変革への取り組みを再考させている。ポストCOVID-19の世界に向けて準備を進めている企業は、当初、収益を上げるためのアプローチとして考えられていたカスタマーエンゲージメントを、リモートでの従業員の有効化 と生産性のプランに入れようとしている。これは、誰もがどこからでも仕事ができるようにすることで、従業員のレジリエンスの究極の状態を達成するための要件である。しかし、あらゆるデジタル変革の取り組みと同様に、”Next Normal”がサイバーリスクの次の発生源にならないよう、設計段階でセキュリティを組み込む必要がある。



Next Normal（新しい日常）

COVID-19 危機からの回復は、スイッチの切り替えのようにスムーズにいくものではなく、通常業務や新しい生活を取り戻していくためには、特定集団、地域（同じ国内であっても）、年齢層、ビジネスセグメント等、段階的なプロセスを採用することになるだろう。各国では国民が仕事に復帰し、経済活動に戻るために様々なアプローチを取ると考えられるが、経験したことがないが故に、間違った選択や、感染が再拡大し在宅に関する条例が再発例される可能性もある。（アジアの一部の国ではすでにこの現象が起きており、今後数か月間の間に他国でも同様のことが起きるだろう。）

このような環境では、単一の「Next Normal」ではなく、一連の「Next Normals」が必要であろう。医療関係者の予測によると、ワクチンが世界的に入手可能になるまで、社会の状況は常に変化し続ける。このような変化する環境に適応するためには、新たなレベルのアジリティを採用することが、サイバーセキュリティ組織の責務である。」

例えば、Next Normalsの概念は、ベースライン化および異常検出に対する従来のアプローチがもはや関連しないことを意味する。オフィスで業務する従業員、在宅で業務する従業員、国や地域によってソーシャル ディスタンス（社会的距離）の政策をとるため、アクセスと利用パターンは常に変動する。このため、従業員のアクセスパターンや行動が予測可能であると想定されるため、従来のベースライン手法は、時代遅れになっている。また、ベースラインがなければ、何が正常で何が異常かを確立できず、サイバーセキュリティ戦略の基本原則の1つを乱すことになる。

企業は、New Normalsの世界に対応するために、新しい戦略とアプローチを開発する必要がある。たとえCOVID-19 が危機的状況を脱したとしても、ビジネスの強靭性を構築するため新しく、アジャイルなオペレーションモデルが必要となる。それは、オペレーションを大規模にスケールアップする能力であろうと、短期間でサプライチェーンを再構築する能力であろうと、あるいは大量の従業員を在宅で働かせる能力であろうと。サイバーセキュリティ組織は、これらの新しい運用モデルにセキュリティを組み込むことができるように、同様の機敏性をアーキテクチャや運用に組み込む必要がある。

未来への繁栄

COVID-19 のパンデミック以前は、企業はテクノロジーとセキュリティ関連の支出の大部分を、収益創出と業務の効率化に充てていた。これらは一般的にどの組織でも最優先事項であるため、これは理にかなっている。しかし、COVID-19後の世界では、企業の回復力に向けたリソースのリバランスが見られるようになる。皮肉なことに、サーバのクラッシュや自然災害を恐れて、組織がデータのバックアップとリカバリに重点を置いていた今世紀初頭の状況に戻ることになる。しかし、今後は、オフィス環境にアクセスできなくなったときにも生産性を維持できるようにする必要があり、一般の従業員にもビジネスの柔軟性がもたらされるようになる。

これにより、安全なリモートアクセスと生産性を実現する次のようなテクノロジーへの関心が再び高る。

- **仮想デスクトップインフラストラクチャ（ VDI ）**とDaas（Desktop as a Service）。これにより、セキュリティチームとITチームがユーザーのデスクトップを一元管理できるようになり、従来のデスクトップよりもはるかに強力な制御が可能になるため、承認されていないデバイスを使用してエンタープライズコンピューティング資産にアクセスするユーザーの問題が軽減される。VDIは2000年代初頭から存在していたが、複雑さとパフォーマンスの問題のため、定着には時間がかかった。しかし今日では、クラウドベースのVDIとDaaSによって、これらの問題は大幅に軽減され、今後、VDIはどこからでも仕事をするための強力なソリューションとなっている。

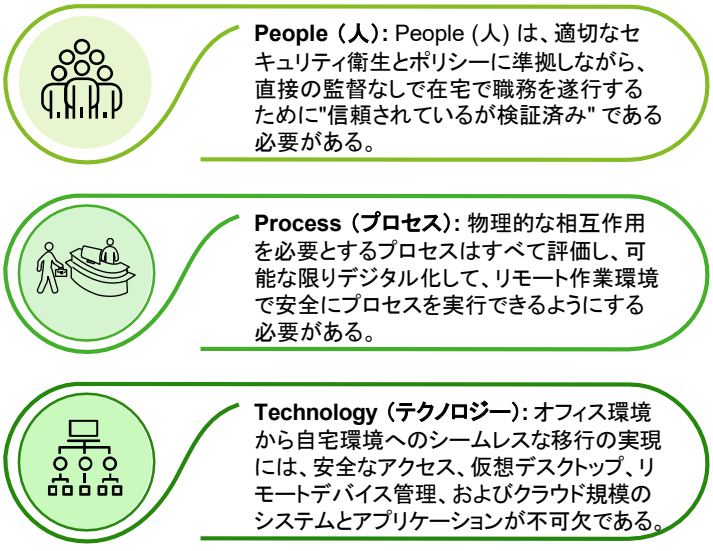
- **IDおよびアクセス管理（ IAM ）**も、コストと複雑さのために導入時の問題を抱えている。多くのIAMプロジェクトは、IAMを完全に実装するために必要なコミットメントを企業が過小評価していたために失敗している。VDIと同様に、クラウドベースのIAMソリューションの出現により、技術的な複雑さが大幅に軽減されたため、セキュリティチームが企業規模の展開を実装することが現実的になった。IAMは、大規模なリモートワーク環境でリスクを適切に管理しようとするほとんどの組織で必要とされる、ゼロトラストアーキテクチャの採用において中心的な役割を果たす。

- **クラウドマイグレーション**は、COVID-19 のパンデミックにより、大きく加速化することになる。レガシーシステムに依存している企業は、オンプレミスのインフラストラクチャで、パフォーマンス、スケーラビリティ、可用性に関する悲惨な問題に直面している。これにより、これらのシステムのクラウドへの移行が加速し、セキュリティチームはクラウドセキュリティに関して新たなレベルの成熟度を達成する必要がある。

クラウドネイティブな組織がCOVID-19 のパンデミックを生き抜いたのは偶然ではない。彼らはすでに現代的なクラウド、アイデンティティ、リモートアクセス技術を完全に受け入れていたので、100%リモートワークフォースモデルへの移行は比較的小さなステップだった。最も苦労しているのは、レガシーマインドを維持し、古いシステムに"間に合わせを"している組織だ。これらの組織がもはや、"Work from anywhere（誰もがどこからでも働くことができる）"を可能にする People（人）, Process（プロセス）, Technology（技術）への投資を避けて通れないことをこの世界的流行は示している。

People（人）, Process（プロセス）, Technology（技術）の未来

いつものように、企業のパフォーマンスはPeople（人）, Process（プロセス）, Technology（技術）によって左右されます。そして、リモートワークが標準である世界にするためには、必要なデジタル変革を効果的に実行する、これら3つすべてに取り組む必要がある。



COVID-19 のパンデミックは、世界各地に永続的な変化をもたらす可能性が高い。どこでどのように働くか、という働き方の変化は、COVID-19のパンデミックの中で起きた最も顕著な変化のひとつであり、多くの企業がリモートワークによる士気やコスト削減、生産性向上のメリットを経験している。これにより雇用者と従業員の間に必要とされる信頼が高まることは、この経験から得られるプラスの結果であり、柔軟性は、雇用者と従業員、両観点から新しい規範となる。世界中からの初期のフィードバックでは、柔軟性とワークライフバランスに高い価値を置く傾向がある若い従業員に、これが非常によく当てはまることを示している。COVID-19 は実際に、ビジネスの主流おける価値システムの存在感を高めている。

サイバーの観点から見れば、パンデミックの結果として、組織のサイバー環境とセキュリティ衛生は自然に改善されるだろう。パッチ適用、脆弱性管理、サイバー意識向上プログラムなどの中核的なセキュリティ機能は、かつてないほど重要になる。Work from anyware-誰もがどこからも働くことができるように、ゼロトラストアーキテクチャの採用は、これをこれからの世界では、重要な役割を果たす。

お問い合わせ

Emily Mossburg
Global Cyber Leader
+1 571 766 7048
emossburg@deloitte.com

Amir Belkhelladi
Canada
+1 514 3937035
abelkhelladi@deloitte.ca

Simon Owen
North South Europe
+44 20 7303 5133
sxowen@deloitte.co.uk

Deborah Golden US
+1 571 882 5106
debgolden@deloitte.com

James Nunn-Price
Asia Pacific
+61 293227971
jamesnunnprice@deloitte.com.au

Peter Wirnsperger
Central Europe
+49 40320804675
pwirnsperger@deloitte.de

Nicola Esposito
Spain
+34 918232431
niesposito@deloitte.es

For more information contact visit Deloitte.com/covid or（日本語）Deloitte.com/jp/cyber

Deloitte Cyberグローバルの翻訳になります。