DX 時代に求められる「サイバー・トランスフォーメーション」とは

IoT や AI、クラウドを駆使したデジタル･トランスフォーメーションはビジネスを推進する大きな力だが、それらは同時に、サイバー攻撃者側の能力を高めることにもなる。

この事実を踏まえると、DX を構成するさまざまな要素を適切に活用した新しいセキュリティ対策、サイバー・トランスフォーメーションが求められている。

ASAHI INTERACTIVE

いま、あらゆる企業がデジタル・トランスフォーメーション（DX）の波に直面し、さまざまなテクノロジーを活用して新しい価値を生み出そうともがいている。

DX とは単なる情報化ではなく、ビジネスのあり方そのものを変えるアプローチだ。例えば Internet of Things（IoT）を活用して、これまで収集していなかったさまざまな現場のデータを収集し、適材適所で組み合わせたマルチクラウドやハイブリッドクラウド上に構築した AI/ 機械学習基盤で分析して新しい知見を引き出し、その結果をビジネスにフィードバックしていく……という具合だ。さもなければ、市場競争の中で取り残されてしまうだろうという危機感は、多くの企業が感じているだろう。

さて、メディアでは、こうした DX の明るい面ばかりにスポットが当てられがちだ。しかしそこにはリスクも潜む。なぜなら、DX を実現するさまざまなテクノロジーを、サイバー犯罪者・攻撃者の側も享受できるからだ。便利な道具や技術が生まれれば、それを悪用する人が出てくる例は古今東西限りないが、DX も例外ではない。

DX はサイバー攻撃者にとっても チャンスに

日本 IBM セキュリティー事業本部 コンサルティング & SI 理事 / パートナーの小川真毅氏は、DX 時代の課題を次のように説明する。

「この先、膨大な数の IoT や Operation Technology（OT）、制御システムがネットワークにつながるが、攻撃者にとってそれは、約 208 億の『入口』『侵入口』ができることを意味する。また、クラウド環境は便利なものだが、攻撃者にとっても同じだ。攻撃ツールや情報の公開が容易になるほか、ASP/SaaS 的に攻撃を行い、レベニューシェアを行うモデルも登場している。マルウェアや攻撃ツールの作成はアジャイル開発で行われ、ナレッジを共有しやすくなっている。AI も攻撃者にとっては『使える』技術だ。人がわざわざ探さなくても、脆弱性のありそうなところを勝手に見付け、攻撃するようになり、侵入がより容易になってしまう」（小川氏）

日本 IBM
セキュリティー事業本部
コンサルティング & SI 理事 /
パートナー
小川真毅氏

恐ろしいのは、これがただの仮説ではなく、世界で実際に起こり、被害を及ぼしつつあることだ。

例えば OT への攻撃はこの数年活発化しており、ウクライナではサイバー攻撃に起因する停電が 2 度に渡って発生したほか、水道設備や原子力施設といった重要インフラに対するサイバー攻撃も報じられている。こうした事態を放置していては、金銭的被害はもちろん、人命や身体の安全が脅かされかねない。

IoT の領域でも、インターネットにつながった多数の機器に不正アクセスを仕掛けて攻撃者の「ロボット」と化し、他社サービスに大規模攻撃を仕掛ける「Mirai」のようなマルウェアが登場し、民間のみならず日本政府も対策に本腰を入れる事態となっている。

またクラウドでは、国内外を問わず相次いで情報漏洩事件が発生しており、止むことがない。その中には、米陸軍のように高いセキュリティレベルが求められる組織での漏洩も含まれているが、想像のつかないような高度な攻撃テクニックが使われたケースはほとんどない。大半が、ちょっとした「設定ミス」の隙をつかれた格好だ。

DX を前提にした、 新しいサイバーセキュリティのポイント

サイバー脅威のリスクは増大している。ある調査によれば、今後 2 年間でサイバー犯罪によって見込まれる経済的損失は、600 兆円に上るという。また、1 件のサイバーインシデントによって発生する企業の損失額も、復旧作業や顧客へのお詫び・賠償、法令違反による罰則金等を含めると平均 4.5 億円に上るとされており、「ひとたびインシデントが起きると、企業に重大な影響を与えることは明らかだ」（小川氏）

一方で、対策は後手に回りがちだ。サイバー犯罪・攻撃は防御するだけでなく、侵入にいち早く気付く体制作りが重要とされているが、それがまた難しい。別の調査では、企業や組織がサイバー犯罪に気付いて対

処完了するまでの平均時間は 266 日と、解決までに半年以上要する状況にあるという。

こうした状況を踏まえると「DX 時代には、サイバー・トランスフォーメーションも必要だ。サイバーセキュリティも DX の観点に沿っての対策が必要だ」と小川氏は強調する。

つまり、

- あらゆるデバイスがネットワークにつながり、狙われることを前提に、一貫した対策が不可欠なこと
- マルチクラウドやハイブリッドクラウドでは、自ずと異なるセキュリティレベルの環境が混在・連携することになるため一律のセキュリティ対策を講じて終わりではなく、共通的な対策と、各環境特有の対策の両面が必要なこと
- 攻撃側も AI をはじめとする最新テクノロジーを活用している以上、防御側ももっと、AI やデータアナリティクス、オーケストレーションといった最新技術を活用すべきこと

という 3 つのポイントに留意しながら対策に取り組むことが重要だ。

その際には、オンプレミスに閉じ、PC やサーバだけで完結してきた従来の IT 環境以外にも目を向けなければならない。

例えば「IT の世界では情報の機密性が重視されるが、OT では止めないこと、稼動し続けることが求められる。IT 機器ならば、脆弱性を修正するためにパッチを当てて再起動するのは簡単だが、OT では機器を停止できるのは 1 年に 1 回程度で非常に難しい。パッチを適用するとベンダーのサポート外になる恐れもあるし、ライフサイクルも平均で 10 ～ 15 年と IT よりもずっと長い」（小川氏）

その上、IT に関しては、セキュリティ部門や担当者を整えている企業がほとんどだろうが「OT の場合、今もセキュリティ管理部門や専属の担当者がいない企業がまだまだ多い。従って、IT 部門が OT 側のセキュリティをサポートしていかなければならないだろう。統合とまではいかなくても、互いに近付け、横並びで対策していく必要がある」と小川氏は述べる。

同様に、クラウドのセキュリティ対策にもポイントがある。それは「クラウドを利用するメリットを失わないようにすることだ。セキュリティはとかくブレーキになりがちだが、クラウドならではのスピードや使いやすさ、拡張性といったメリットをいかに弱めないようにして、許容範囲に収めるかがポイントだ」（小川氏）

またクラウド環境では、自社でコントロールできる部分とクラウドサービス事業者がコントロールする部分、責任の境界が分けられている。その事実を踏まえ、「データ保護や認証、インシデントが起きたときの対応や脆弱性管理といった事柄のうち自社としてコントロールすべきことは何かを押さえ、どのレベルで実現するかを、ビジネスとのバランスを取りつつ決めていく必要がある」（小川氏）

加えて、マルチクラウド環境においては、クラウドベンダーごとに実現できるセキュリティレベルの違いを理解し、一律の対策がとれるかどうかの確認も必要だとした。

こうした困難な状況を踏まえ、政府も対策を後押ししつつある。例えば IoT セキュリティの領域については、経済産業省や総務省、米 NIST といった組織がガイドラインを提示しているほか、一歩進んで政府主導で IoT 機器の脆弱性をチェックする「NOTICE」と呼ばれる取り組みも始まっている。こうした全体的な動向も視野に入れておく必要があるだろう。

AI やオーケストレーションを活用し、サイバー・トランスフォーメーションの実現を支援

では、DX 時代のセキュリティ対策は、具体的にどのように進めていくべきだろうか。小川氏はまず、「ばらばらに対策を進めても収拾がつかないし、どこまでやればいいかも分からない。体系的に関連付けながら、点と点を結んだ対策を進めていくべきだ」とアドバイスする。

その上で、DX を前提としたサイバー・トランスフォーメーションを目指すならば、AI をはじめとするテクノロジーを活用し、プロセスを自動化していくことも必須の要件だ。そこで「IBM では近年、オーケストレーションを活用し、人間の免疫システムのようなセキュリティを作っていこうと提唱している。例えば、一度目は攻撃がすり抜けて侵入してきても速やかに見つけて解析し、ファイアウォールのルールを動的に変更して同じ攻撃元からの通信を遮断するといった具合

に、人間の免疫システムのように、二度は同じ攻撃を受けない仕組みを目指している」（小川氏）

もちろん、完全な自動化はまだ先の話になるだろう。だが IBM ではそれを支援し、部分的に自動化していく技術とサービスを提供している。その際に強みとなるのが、全世界で約 8,000 人、日本国内にも約 300 人いるセキュリティ専門家による知見・情報の収集と解析だ。世界 8 カ所の SOC を通じて 24 時間 365 日体制で監視を行い、新しい脆弱性や攻撃キャンペーンなど、最新の脅威情報を蓄積し、防御に反映する仕組みだ。

サイバー・トランスフォーメーションを具現化した取り組みの 1 つが、コグニティブ技術「Watson」を生かした脅威情報の解析だ。ビッグデータ解析やビジネスアナリティクスだけでなく、IBM セキュリティとしても Watson の技術を取り入れ、脅威情報をいち早く解析し、初動対応の支援に生かしている。「ゆくゆくは、アラートを受け付け、必要に応じてエスカレーションするアナリストの初期対応部分の作業を全部自動化できればいいと考えている」（小川氏）

また、インシデントレスポンスの支援では、世界最大規模のセキュリティー研究開発機関である IBM X-Force をベースに、さまざまなマネージド・セキュリティ・サービスや駆け付け対応サービスを提供してきた。この先、オーケストレーションを組み合わせることで、インシデント発生時に自動的に対応までできるようにしていく方針という。同時に、攻撃者の視点で今の環境にどのようなリスクがあるかを IBM のホワイト・ハッカー集団“IBM X-Force Red”が分析するサービスも実施しているが、ネットワークやアプリケーションといった IT システムだけでなく、ハードウェアも含め、POS や ATM、車載端末などの組み込み機器、IoT 機器を検査できることがほかにない特徴だ。

クラウド領域については、あらためていうまでもないだろう。オンプレミスからマルチクラウド環境までをカバーし、認証・アクセス管理やデータ保護といったクラウド特有のセキュリティ対策に加え、エンドポイントやアプリケーションのセキュリティ、さらにはモニタリング、分析・オーケストレーションといったセキュリティサービスを一通り、クラウドに対応した形でそろえている。

そして、この先ぜひ注目したい要素が「オーケストレーション」だ。オーケストレーションと言うと、クラウド基盤の構築を半自動化するものというイメージが強いかもしれないが、セキュリティ対策の現場で求められるさまざまな作業にも適用できる。

インシデントレスポンスの現場はただでさえ慌ただしい。限られた時間の中で、調査から対処に至るすべての作業を人手で進めようにも、抜け・漏れが生じる恐れがあるほか、誰が何をしたのか、作業記録を取るのもままならないことが多い。そこで IBM の「Resilient」では、インシデント対応に必要な一連の作業を、あらかじめ定義した「プレイブック」に沿ってオーケストレーションする。チケットのように「インシデント」を作成すれば、必要な人物にアサインし、次に必要なタスクを示し、関連する情報を紐付けながら優先順位を付け、適切に対処できるよう支援していく。

とかく属人的になりがちだったインシデントレスポンス。ここにオーケストレーションという要素を取り入れることで、一定の水準を満たしつつ、作業や運用プロセスを半自動化していくことができるだろう。

このように DX は多くの企業にさまざまなメリットをもたらしつつあるが、サイバー攻撃者・犯罪者もまた、その能力を高めている。この事実を踏まえ、国を挙げての対策が求められている。それも、従来からの IT の領域だけでなく、IoT やクラウドといった新しい領域も含んだ、DX 全体にまたがる視野で取り組む必要があるだろう。

「これを実現するには、オーケストレーションを活用して対策を半自動化し、自浄作用を働かせていかなければならない。それこそがサイバー・トランスフォーメーションの本質だ」（小川氏）

日本アイ・ビー・エム株式会社

お問い合わせ

日本アイ・ビー・エム株式会社

IBM アクセスセンター　0120-550-210

受付時間 9:00 ～ 17:00 (土、日、祝日を除く)

IBM Security

https://ibm.biz/security_jp