セキュリティインシデント / イベント管理（SIEM）ツールで IT 部門の負担を軽減

トランスフォーメーションと運用の 2 つにコミットする IT

IT 部門は裏方から一転、一躍脚光を浴びる存在となっています。あらゆる業界でデジタルトランスフォーメーションが進む現在、企業の経営者は、新たなビジネスチャンスの獲得や、顧客 / パートナーエンゲージメントの向上を通じた売り上げ促進という課題において、IT が中心的役割を果たすことを認識しています。ビジネスの場にクラウドやモバイルデバイス、機械学習や人工知能（AI）アプリケーションが取り込まれた現在、IT 管理者と IT 部門は極めて重要な存在となり、この変革の土台を担う立場といえます。

ところが、IT 部門は常に業務に追われ、時には過剰な負担を強いられています。CEO や事業部は IT 部門に対して運用効率性を期待し、優れたパフォーマンスで絶え間なく優れたサービスを提供することを求めます。また、進化を続ける脅威の中で、企業ネットワークとデータ資産を保護しながら、多様な業界標準と法規制へのコンプライアンスを維持することも求めています。一方で、管理対象は増加の一途をたどり、ますます複雑で古くなっていきます。

事実、IDG が毎年実施している CIO 調査では、回答者の 72% がビジネス革新や事業運営の卓越性の実現に苦慮していることが明らかになっています。そして 87% は、課題は減るばかりか、増えていく一方だと回答しています [1]。

要員不足と緊縮予算の中、IT が担うあらゆる分野で優秀な人材を獲得することは、ますます困難になっています。中小企業が非常に厳しい状況にあることは、疑う余地もありません。このような課題を解決するために、IT 管理者は、日常業務をこなし新たな戦略的業務を遂行しつつ、IT 部門を悩ます 3 つの根本原因に対処しなければなりません。

CIO の 72% が、ビジネス革新と業務の卓越性の両方に応えるという離れ業に苦慮しています。
（出典 : IDG CIO サーベイ）

小規模な IT 部門の三重苦を軽減

中小企業のビジネスの成長とデジタル化をサポートする方法を考えた場合、IT 管理者は、人材不足と業務の過負荷、テクノロジーの断片化 / サイロ化、セキュリティ脅威と需要の加速という 3 つの課題に直面しています。

ビジネスの成長とデジタルトランスフォーメーションを阻む IT の多様性

IT 管理者とそのチームにとって、多様な範囲に対応できることが非常に重要です。中小企業の IT 部門は、幅広い職務を担う必要があります。組織が小規模であることに加え、成長過程にあり、新たな領域へと拡張し、将来の成果を期待してデジタルトランスフォーメーションを推進しているからでもあります。

ところが、IT 機能の多様性は、専門的な能力獲得の障壁にもなります。人工知能の登場などにより、コンピューティング、ストレージ、ネットワークテクノロジーはますます複雑になっているため、高度な能力を得るには、継続的な教育が必要で、新テクノロジーに対する専門知識が要求されます。このような専門化を行わなければ、IT 担当者はテクノロジーへの投資を有効活用して競争力を最大限に高めることはできません。

また、セキュリティやコンプライアンス管理というスキルにおいて、専門化は極めて重要であり、不足している部分でもあります。専門知識がなければ、システムを最適に活用できないばかりか、多大な被害につながるセキュリティ侵害を阻止することはできません。たとえば、ESG サーベイによると、IT 管理者の 22% が「過去のセキュリティインシデントの原因はセキュリティのスキル不足にある」と指摘しています。企業は、セキュリティ担当者の増員やセキュリティサービスのアウトソーシングを検討するかもしれませんが、適切な人材を見つけることは難しく、また見つかっても高コストで、予算内での雇用は困難であるのが現状です。戦略的意思決定を下す IT 管理者であれば、十分な時間を確保して要員のスキルアップを図るべきです [2]。

また、時間をかけて、企業システムの戦略的な改善を計画する必要もあります。大企業の CIO は、非常に苦心して必要な時間を捻出しています。ところが、中小企業ではこれさえも難しいでしょう。たとえば、アプリケーションの展開において、クラウドプラットフォームにどの程度の時短効果があるかを検証したくても、担当者全員が既存のアプリケーションとシステムのサポートに手一杯であれば、その作業は困難になります。サイバーセキュリティの専門家の実に 67% が、「日常業務が忙しすぎて、スキル開発やトレーニングの時間がない」と主張しています [3]。

スキル開発の時間的余裕がない？

サイバーセキュリティの専門家の 67% が「忙しすぎる」と回答しています。

このように時間に追われる状況は、プロアクティブではなくリアクティブな対応を招いています。IT セキュリティ担当者が手一杯で、予期しない IT/ セキュリティの問題の対応に追われている場合、攻撃のリスクや影響を軽減する方法をじっくり考えることは困難です。

フランケンシュタインのような IT はシステム管理を阻むモンスターと化す

期待通りのテクノロジー ROI を実現できない理由は、多くの場合、高い保守コストと複雑さにあります。

ハードウェア、ソフトウェア、ネットワーキング、セキュリティ機器、サービスは、IT 部門や事業部が購入したものや社員の私物の寄せ集めになっており、ほとんどの場合、IT セキュリティ担当者に過剰な負担がかかる原因になっています。個々の機器、プロセス、コントロールを寄せ集めた「フランケンシュタイン」のような IT インフラストラクチャを運用する IT 担当者は、非常に煩雑な管理インタフェースやコマンドセットを使い、複雑なワークフローの対応を余儀なくされます。エンドポイント、E メール、ネットワークなどの製品をテクノロジーベンダーから購入した場合でも、監視と保守に非常に手間がかかります。中小企業を対象にした新たな調査によると、期待以上のテクノロジー ROI を実現できない最大の理由に、継続的保守のコスト、運用と保守にかかる時間、複雑性があげられています [4]。

テクノロジーとスキルの多様化が限界に達すると、ほとんどの IT 管理者は、スキルセットとテクノロジープラットフォームの統合に着手します。このプロセスでは、IT とセキュリティアーキテクチャを見直し、個々の要素を全体にどのように組み込むかを再検討しなければなりません。そのためには、大規模な再トレーニングを必要とせずに、使い慣れたインタフェースを使った製品を統合する必要があります。

また、認定プログラムが確立された成熟度の高い製品を選択すれば、必要なタイミングで必要なスキルを持つ IT 担当者を容易に見つけることが可能になります。それでも、IT、セキュリティ、コンプライアンスといった機能の運用には、監視や保守、アップグレード、トラブルシューティングのための様々なテクノロジースタックが立ちはだかります。その結果、中核的なインフラストラクチャの運営に貴重な時間を費やすことになり、ビジネスイニシアティブのための新たなテクノロジーの調査、計画、導入といった時間がとれない状況に陥るのです。

ますます複雑で困難になるセキュリティ

IT 部門が担うさまざまな責務の中でも、多くの場合、デジタルセキュリティは最も重要だとみなされます[5]。IT 部門は、セキュリティに長年取り組んできました。サーバーのパッチ適用、電子証明書の管理、ファイアウォールの保守、感染エンドポイントの除染、パスワード保護やサイバー攻撃対策に関するユーザー教育など、さまざまなセキュリティタスクを担当してきました。

セキュリティ侵害や障害が次々に発覚したことから、ここ数年で企業やステークホルダーのサイバーセキュリティに対する意識は変化し、関心が高まりつつあります。同時に、企業では、デジタルトランスフォーメーションの成果も求めています。つまり、顧客に関する情報、サプライチェーンの合理化、ビジネスプロセスの高速化、顧客エンゲージメントの改善などを、すべて安全な方法で実現したいと考えています。

そのために大企業では、CISO（最高情報セキュリティ責任者）やCSO（最高セキュリティ責任者）の指揮下、専任のセキュリティチームを編成し、エンドユーザーのセキュリティ意識向上プログラムを推進しています。一方で中小企業の IT 管理者は、大企業のようなツールやエンドユーザートレーニングを使用できない状況にもかかわらず、自社のデジタルトランスフォーメーションやセキュリティの責務を担っています。

中小企業では従業員数は少ない分、セキュリティへの意識が低い従業員が重大な損害を引き起こす可能性も低くなります。しかしながら、トレーニングを受けておらず、フィッシングの罠にはまる従業員やセキュリティ保護されていないパブリックネットワークを介して業務を行う従業員が 1 人でもいれば、大惨事を招きかねません。そして、中小企業は、大企業に比べて準備が整っていないと言えます。調査では、65% の企業が「パスワードポリシーはあるが実践されていない」と回答しています[6]。

デジタルトランスフォーメーション時代のセキュリティの大きな課題とは、攻撃対象範囲の拡大です。データは常に企業やクラウドを移動し、遠く離れたモバイルデバイスや IoT（モノのインターネット）デバイスまで伝送されています。攻撃対象範囲が拡大することで、サイバー犯罪者が悪用できる脆弱性が増し、攻撃ベクトルが格段に大きく動的になります。

脅威が多様になり、増加し、速度が速まるほど、IT セキュリティ担当者の猶予時間は短くなります。つまり、新たな脅威の検知、侵入検知、未然の修復に使える時間が少なくなるのです。また、脅威の防御、検知、対応のみならず、業界団体や政府機関の法規制遵守を目的にしたセキュリティイベントの監視やレポートにかけられる時間も短縮されます。

IT 管理者の 22% が、過去のセキュリティインシデントの原因はセキュリティスキルの不足であるとしています。

IT 部門の貢献がもたらす価値を高める

デジタルトランスフォーメーションは、ますます複雑になると考えられます。テクノロジーは、複雑さを増す要因であると同時に、目標実現を支援する要因でもあると考えられます。IT 管理者は、自身の役割やチームの役割に変革をもたらすツールとして、テクノロジーを認識するのが現実的でしょう。これには、さまざまなアプローチがあります。

- 運用タスクを自動化し、戦略にフォーカスしたスペシャリストとして担当者が活躍できる時間を確保します。これによって IT 管理者は、現在のビジネスの稼働時間要件を満たすと同時に、将来に向けて IT アーキテクチャを再設計できます。
- 差し迫った障害や新たなセキュリティ侵害の兆候をプロアクティブに特定および監視し、迅速に対応するテクノロジーを導入することで、ダウンタイムを想定した訓練を省略できます。
- 中小企業は、ベストプラクティスが標準構成され、すぐに使えるレポートが実装されているインテリジェントなシステムを選択することで、セキュリティとコンプライアンスの課題に自信を持って対応できるようになります。

システムやセキュリティ障害の検知、監視、アラート、対処の支援を自動で行う最新テクノロジーは、担当者の負担を軽減します。そこから生まれた時間を、新たな売上の創出やビジネス変革をもたらすサービスの調査、計画、提供に投入することができます。これこそが、中小企業の経営陣の 1 人である IT 管理者が提供できる価値の本質です。

専門化と戦略的思考に向けて担当者を解放：

1. 運用タスクを自動化
2. 異なるシステムをプロアクティブに監視
3. サイバー攻撃対象領域と脅威の変化を逃さず対応

[1]「State of the CIO 2017」、IDG、2017 年 1 月 17 日（英語）https://www.idg.com/tools-for-marketers/tech-state-of-the-cio-2017/

[2]「Cybersecurity skills shortage creating recruitment chaos」、Jon Oltsik 著、CSOOnline.com、2017 年 11 月 28 日（英語）：https://www.csoonline.com/article/3238745/cybersecurity-skills-shortage-creating-recruitment-chaos.html

[3]同上

[4]「Industry Outlook 2018」、CompTIA、2018 年 1 月（英語）：https://www.comptia.org/content/research/it-industry-outlook-2018

[5]「Top 10 Strategic CIO Priorities Of 2018」、Rob Preston 著、Forbes、2018 年 1 月 29 日（英語）

[6]「Small- and Mid-Sized Businesses: Cyber Threats by the Numbers」、cyberreadinessinstitute.org、2018 年 3 月 5 日時点（英語）

FORTINET
フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7
Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

WP-Using-Siem-to-Unburden-IT-202001-R1