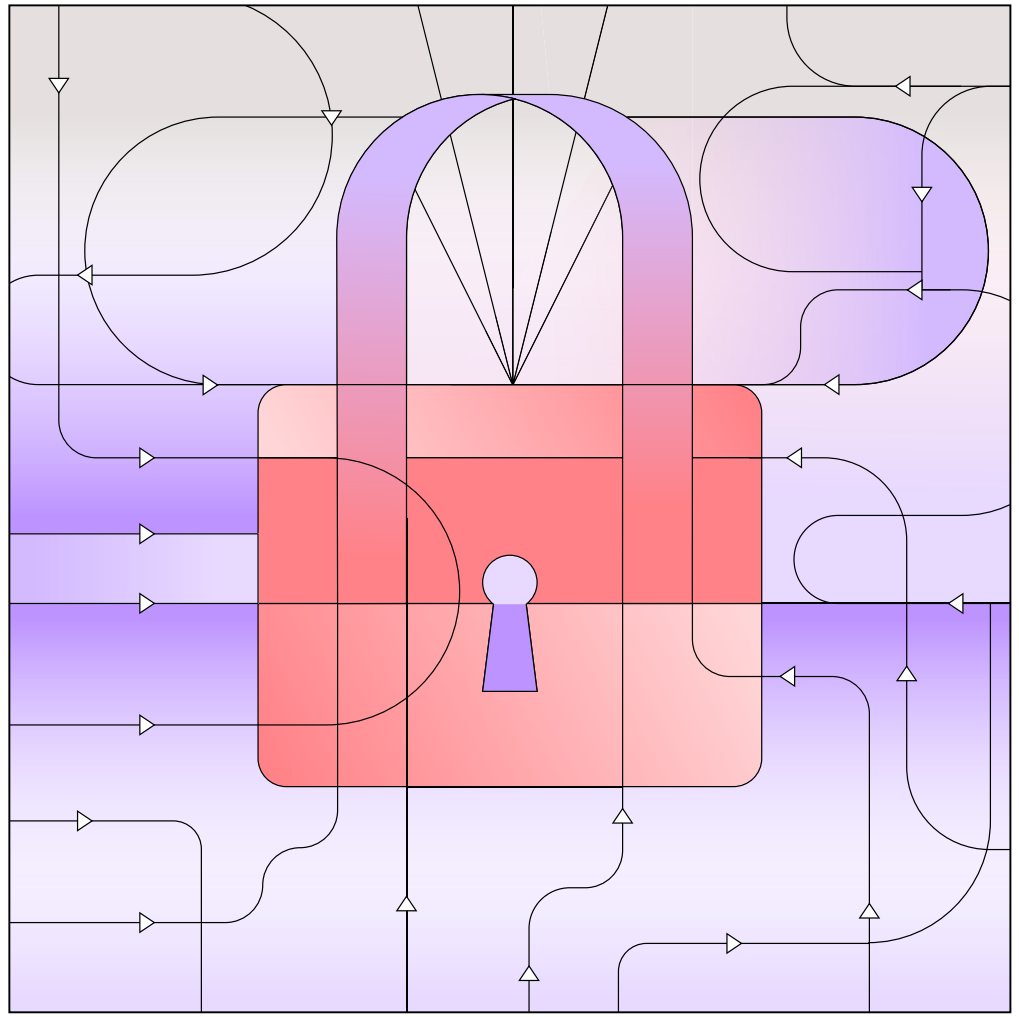
ばらばらなセキュリティー対策を統合する方法

プラットフォーム化が変革を加速する



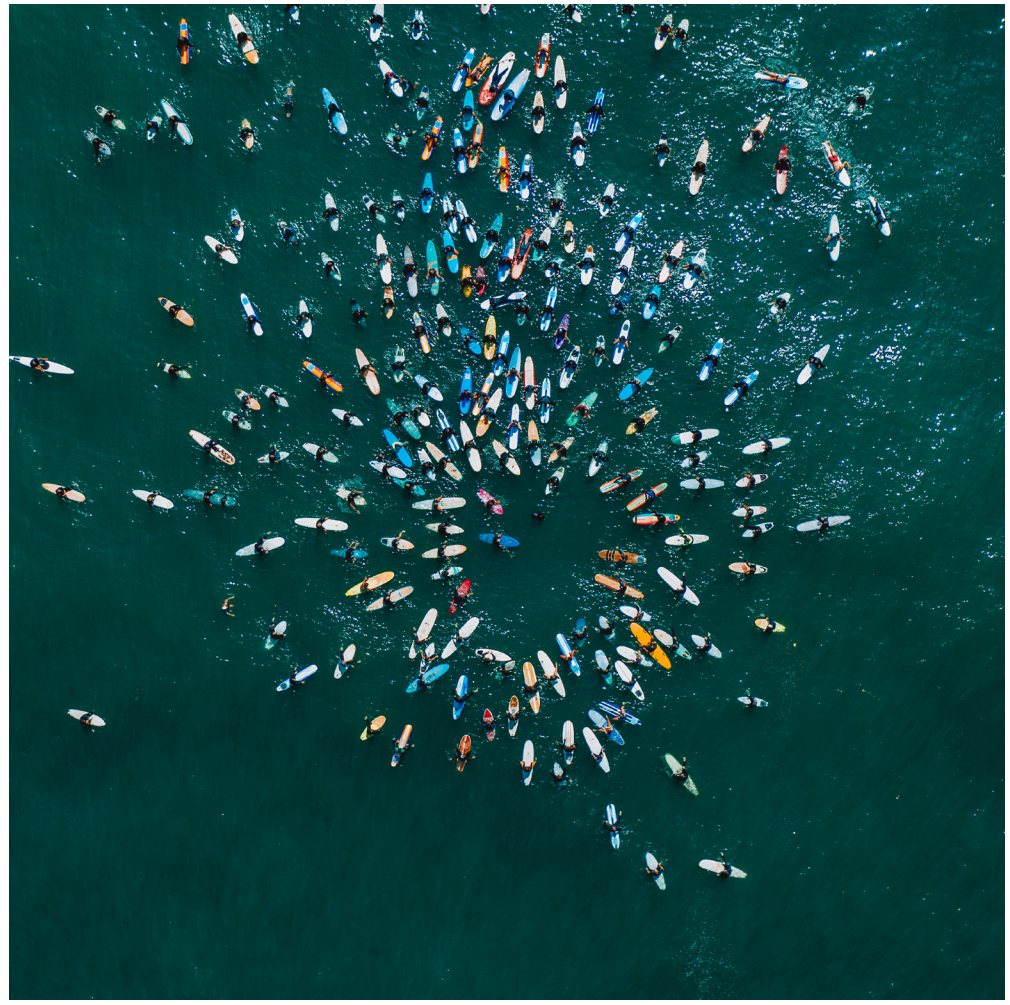
IBM | paloalto NETWORKS

はじめに

サイバーセキュリティーのレジリエンスを高める、新たな基盤の構築へ

経営層から SOC* のオペレーターに至るまで、セキュリティーへの危機感がかつてない高みに達している。背景にあるのはサイバー攻撃の対象と規模の拡大だ。2025 年までに、サイバー犯罪がもたらす経済的損失は年間で 10 兆 5,000 億ドルを超えると見込まれており、企業の最高経営責任者（CEO）はこうした脅威に対処するため、より効果的な方法を模索している[1]。SOC のオペレーターによると、すでに時間不足で日々のアラートの 51% が確認できていない状態に陥っているという。そうした中で、脅威を検出・回避・抑止するためにサイバーセキュリティー担当者が期待を寄せるのは、人工知能（AI）や自動化、一段とシームレス化されたセキュリティー・アーキテクチャーである[2]。

一方、クラウドや AI、IoT（モノのインターネット）、エッジコンピューティングが普及したことで、サイバー攻撃が標的とする対象が広がっており、その結果、多大な損失をもたらす攻撃も増えている。「IBM X-Force Threat Intelligence Index 2024（IBM X-Force 脅威インテリジェンス・インデックス 2024）」最新版によると、欧州ではサイバー攻撃が前年比で 31% 増加したほか、有効な認証情報（正当なログイン情報など）を用いた攻撃は世界全体で 71% 増加した[3]。



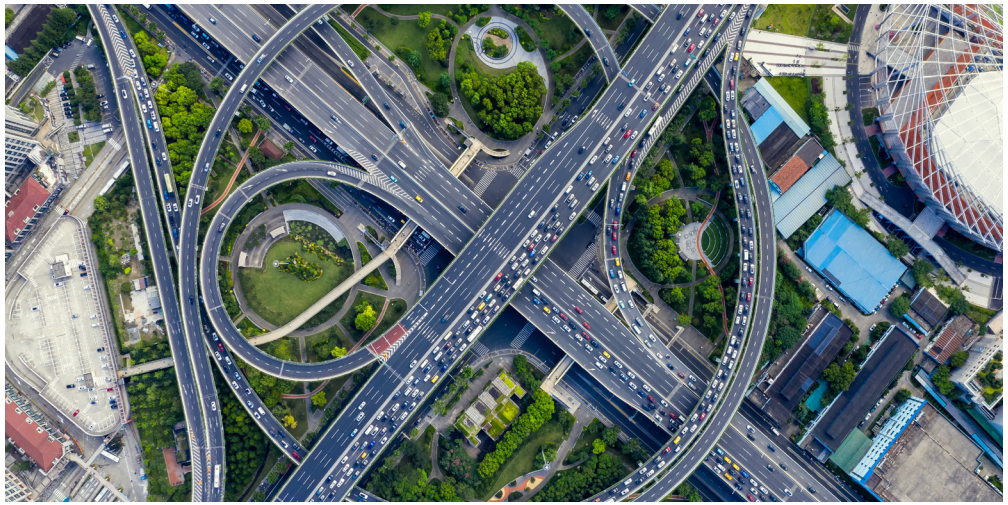
* セキュリティー・オペレーション・センター（SOC）とは、企業の IT インフラストラクチャー全体を 24 時間年中無休で監視し、リアルタイムでサイバーセキュリティー・イベントを検出し、可能な限り迅速に効率よく対処する社内または外部委託チームの IT セキュリティーの専門家のこと

有効な認証情報を用いた攻撃の増加は、セキュリティー脅威に関する懸念すべき変化である。こうした攻撃はハッカーが不正に侵入することなく、単にログインすれば実行できるものであり、攻撃を特定し対処することが著しく難しいからだ。攻撃1件当たりの被害額が増えている一因もここにあるとも考えられる。IBMの調査によると、世界全体のデータ侵害による損害額は平均445万ドルで、1年で15%増加した。米国だけで見ると、損害額の平均は948万ドルに達する[4]。

攻撃者はより大きな成果を追い求める傾向にある。ランサムウェア攻撃やデータ侵害に加え、攻撃者はAIの中核資産であるGPUサーバーのインフラをも標的としている。実際、10億ドル相当のマシンとコンピューティング・パワーを乗っ取ろうとする計画が、研究者によって最近発見されている[5]。

サイバー攻撃の脅威は日増しに大きくなりつつあり、企業リーダーやサイバーセキュリティー管理者は、従来のセキュリティー戦略を見直し、態勢強化を図る必要に迫られている。そのためには自動化を全面導入し、サイバーセキュリティーの担当者が本来業務に専念できるよう時間的余裕を与える。個別の機能では解決できない極めて厄介なセキュリティー課題に全力を挙げて取り組む。個別のセキュリティー・ソリューションを後から継ぎ合わせるのではなく、最初から統合する。そうすれば、段階的に実現できない体系的な統合が可能になり、セキュリティー効果は格段に向上する。

次世代に向けてセキュリティーを飛躍させる上では、設計段階からハイブリッドを意識したハイブリッド・バイ・デザイン*のアーキテクチャーが基盤となるだろう。AIを活用し、「プラットフォーム化」という基本的かつ遠大な戦略を通じてセキュリティーを強化することが重要である。



企業リーダーやサイバーセキュリティー管理者は、従来のセキュリティー戦略を見直し、態勢強化を図る必要に迫られている。

*ビジネス優先事項を達成するための戦略的な設計に基づくアプローチによる、ハイブリッドクラウド・アーキテクチャー・フレームワーク（詳細はこちら https://www.ibm.com/downloads/cas/6PRQ40JO）。

セキュリティーの分断は強靭性を削ぐ

サイバー攻撃は、スピードを増し、大規模化しつつある。しかし、いまだごく一般的な対策をもって、自社のネットワークを守る企業は多い。特定の問題に都度、個別のソリューションを追加する方法だ。このアプローチを続けていると、やがてはパッチワークのようなセキュリティー態勢が構築され、広範な戦略性に乏しい、継ぎはぎだらけのソリューションになる。

新たな防御層が加わるたび、場当たり的なシステムは複雑になり、より多くのリソースが運用と更新に必要となる。その結果、現在、組織が契約するセキュリティー・ベンダーの数は平均 13 社以上、セキュリティー・ソリューションの種類は平均 31 にも及ぶ[6]。

こうした複雑性はパフォーマンスに悪影響を及ぼし、コストを押し上げる。このため、契約先のセキュリティー・ベンダーを整理・統合しようと模索する企業は 4 社に 3 社に及ぶ。この割合は、2020 年には 29% にとどまっていた[7]。IBM Institute for Business Value（IBM IBV）がこのほど行った調査も複雑性の問題を取り上げており、その中で経営層は、セキュリティー対策にとって最大級の障壁は社内共通のツールがないことだと答えている[8]。

4 社に 3 社

の企業が、契約先のセキュリティー・ベンダーを整理・統合しようと模索している。

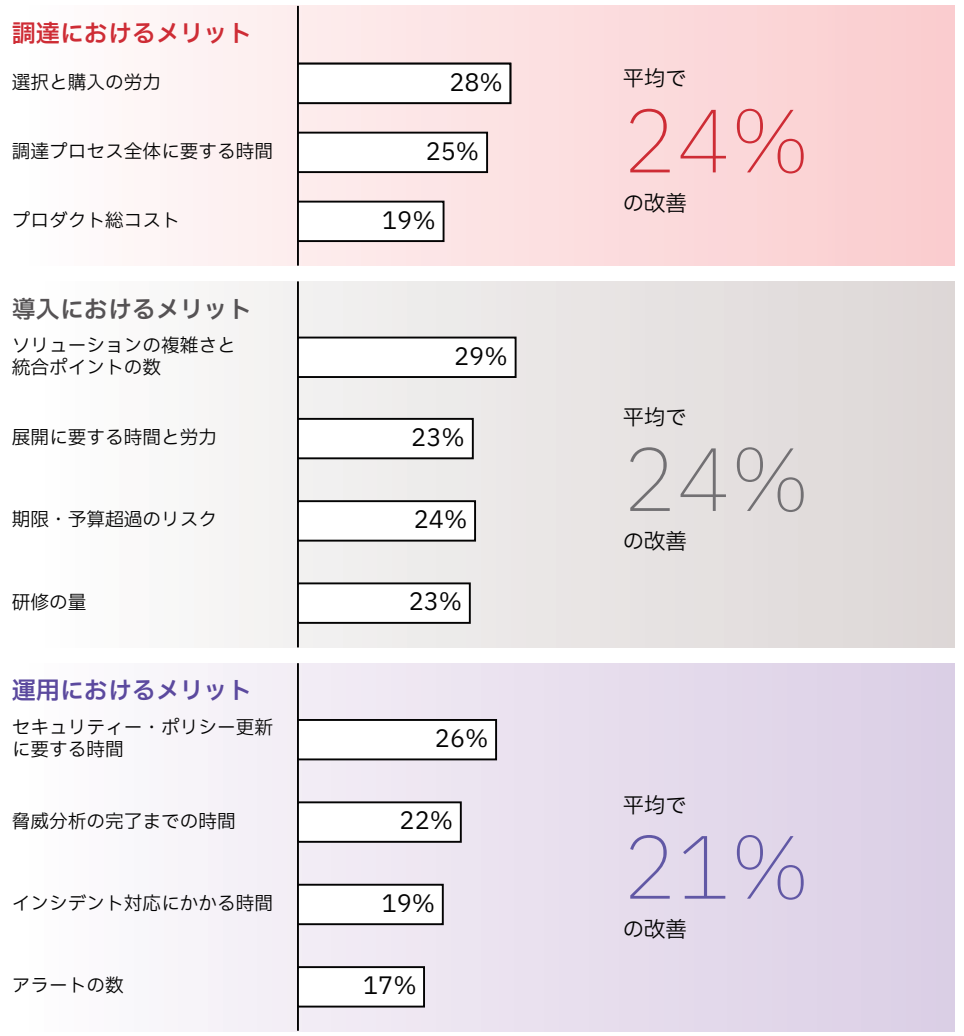
ソリューションが分断された状況は、セキュリティー対策が戦略的に行われていないという、より根本的な問題を内包している。IBM IBV の調査によると、セキュリティー戦略を策定している組織は全体の 86% に及ぶが、実際に実行している組織は 35% に過ぎなかった[9]。

サイバーセキュリティー戦略を実施している場合でも、事業とテクノロジーの広範なニーズに十分には合致していない。自社のセキュリティー戦略が事業戦略に合致していると回答した経営層は 52% であり、自社のセキュリティー戦略が IT 戦略に合致していると答えた経営層も 48% にとどまっている[10]。

セキュリティーの分断化を解消できないのは、多くの組織でセキュリティー態勢の構築が「積極的・戦略的」でなく、「受動的・戦術的」な色彩を強めていることを意味している。組織の中でセキュリティー対策がばらばらだと、組織全体にわたるセキュリティー・リスクの状況を誰も把握することができない。明確で包括的なインサイト（洞察）がないまま、未知のセキュリティー脅威ランドスケープに対処していては、組織はいつかサイバー・リスク管理上の問題に突き当たるだろう。

図 1

「ポイントベース」ではなく「プラットフォームベース」を用いることのメリット



プラットフォーム化による セキュリティーのパラダイム・シフト

サイバー攻撃の頻度と巧妙性が増し、セキュリティー侵害に関わるコストが増える中、ばらばらの「ポイントベース」のセキュリティーから、シームレスな「プラットフォームベース」のセキュリティーへの移行が急務となっている。

セキュリティー対策をプラットフォーム化することで、対策の簡素化や強化、統合を実現することが可能だ。これにより、個別に設計されたソリューションを急いで統合する際に起こりがちな、非効率で高コストの対応を企業は避けることができる。

今後、個々のソリューションの統合や、組織全体の可視性の向上、新たな脅威に応じた容易な拡張性を企業が実現するためには、共通のプラットフォーム上で機能するソリューションを戦略的に設計することが不可欠である。さらに、自動化、機械学習、AI を活用して、サイバーセキュリティーのプラットフォームを統合することで、人員不足を補い、現場のセキュリティー・チームの効率性を高めることができる。

加えて、複数のベンダーから互換性のない製品を調達していると、覚えるべきことが増えすぎるという問題が生じるが、プラットフォームベースのアプローチを取れば、それを防ぐことができる。そうしてセキュリティー・チームはリスクの評価や軽減といった、より価値の高いタスクに集中できるようになる。さらに、ネットワークの監視や認証情報の検証といった定型的なタスクは、マシンやデジタル・アシスタント、ボットに代替させることも可能になる。

セキュリティー対策をプラットフォーム化することで、対策の簡素化や強化、統合を実現することが可能だ。

組織構造に関して言えば、プラットフォーム化により、セキュリティーのサイロ化は解消され、セキュリティー効率は向上する。米調査会社 IDC の最近の調査によると、プラットフォームベースのアプローチによってセキュリティーを統合した組織は、以下のような成果を上げている。

- サイバー攻撃への対応が 55% 速くなり、セキュリティー事象の修復が 58% 速くなった [11]。
- セキュリティー・チームの効率性が 34% 高まった [12]。
- セキュリティー関連プラットフォームの年間コストが 10% 低下した [13]。

統合プラットフォームを運用することで、上記のような成果が現れ、ビジネス・オペレーションはより積極的かつ効率的なものになる。最近の IBM IBV の調査によると、成熟したセキュリティー機能を有する組織は、5 年間で収益成長率が 43% 向上し、セキュリティーの強化により収益が 69% 改善された [14]。純粋にビジネスの観点から見ても、セキュリティーをプラットフォーム化することで、デジタル・トランスフォーメーション（DX）を促進し、成長を加速させることができる。

セキュリティーをプラットフォーム化することで、DX を促進し、成長を加速させることができる。

ケース・スタディー

デジタル・ファーストの住宅ローン会社がプラットフォーム化戦略を導入して、セキュリティーのオペレーションを統合・自動化

2016 年に設立された Better 社は、これまで 1,000 億ドル以上の住宅ローンを扱ってきた企業である。住宅の購入をより簡便かつ迅速にできるよう、住宅ローン業界に変革をもたらすことをミッションとしている。会社は次々と新サービスを立ち上げ急成長したが、並行してサイバー攻撃に見舞われる頻度が上昇し、セキュリティー担当者の作業量が増加した。リモートでログインする社員が毎日数千人に及ぶため、拡大したアタック・サーフェス（攻撃対象領域）も守る必要があった。

金融サービス業界では、機密性の高いデータや顧客および従業員のアカウント情報を安全に管理し続けることが求められる。データ・セキュリティーこそが、顧客からの信頼を獲得し、連邦・州政府の規制を順守するための鍵である。

Better 社は脅威の検出と対応を高度化し、プロセスを自動化するため、パロアルトネットワークス（Palo Alto Networks）社が手掛けるセキュリティー・ソリューションの統合プラットフォームを導入した。ネットワークやクラウド、エンドポイント、セキュリティー・オペレーションに対応しており、これにより SOC チームはより効果的、効率的に動けるようになった。各ソリューションは、ビジネス・チームとエンジニアリング・チーム間の摩擦を減らし、連携が強まるよう、構成されている。

現在、同社は複数ベンダーによるセキュリティー・ソリューションをばらばらに管理するのをやめて、パロアルトネットワークス社のセキュリティー・プラットフォームで統合的に管理している。このスケーラブルなプラットフォームには、実質上どこからでも安全にアクセスでき、クラウド・セキュリティーに対する可視性とコントロール性は著しく向上した。さらに、複数ベンダーを使っていた頃に比べ、大幅にコストを削減することができた。

インシデント対応が迅速化し、その 90% は自動化された。また調査時間も数時間から数分へ短縮化された。これによって、Better 社の IT チームはセキュリティー戦略に専念し、将来を見据えたより複雑な課題に取り組む時間を大幅に確保できるようになった。

プラットフォームを活用し、生成 AI をセキュリティー・リスクからセキュリティー資産に変える

生成 AI をセキュリティー上の潜在的脅威と見なす経営層の割合は 96% にも上る[15]。これほど経営層の意見が一致することはめったにない。ほとんどの経営層は生成 AI を導入すれば、今後 3 年以内に組織内でセキュリティー侵害の発生する可能性が高まると考えている。このため、AI ソリューションの導入前にセキュリティーを確保すべきだと指摘する経営層の割合は 94% にもなる。ところが、今後 3 カ月以内に自社の生成 AI プロジェクトにサイバーセキュリティー対応を組み込む予定だと回答した経営層は 24% にとどまる。それどころか、経営層の 69% は生成 AI の導入において、セキュリティーよりもイノベーションを優先している[16]。

AI に対する認識が「セキュリティー・リスク」から、「セキュリティー資産」に変わると、何が起こるのだろうか。AI がセキュリティーを改善し、セキュリティーが AI 駆動のイノベーションを進めるといった流れが実現するのだろうか。

プラットフォーム化は、新しい AI アプリケーションの展開を、より安全かつ効率的にする。

実際に AI は、これまでになかった能力をセキュリティー担当者に与えてくれる。AI とプラットフォームを組み合わせることで、エンドポイントやネットワーク、サーバー、クラウド・ワークロード、セキュリティー情報・イベント管理（SIEM）システムから、インサイトや推奨事項を引き出し、セキュリティー態勢全体を動的に把握することが可能になる。履歴分析や、脅威イベントの可視化、自動化された根本原因分析を通じて、AI は脅威対策の立案を自動化し、より合理的なワークフローに統合する。

IBM IBV が最近実施した調査によると、AI と自動化をセキュリティーに活用することで、セキュリティー・オペレーション全体の可視性と生産性は向上する。AI を導入する先進的な組織は、ネットワーク通信の 95% を監視し、インシデント検出にかかる時間を 33% 短縮した。こうした組織は自動化を通じて、セキュリティー投資対効果（ROSI）を 40% 以上高め、データ侵害による損失を少なくとも 18% 削減することに成功している[17]。こうしたコスト削減で生まれた資金を、サイバーセキュリティー関連の人材の確保や研修に使うことも可能になる。

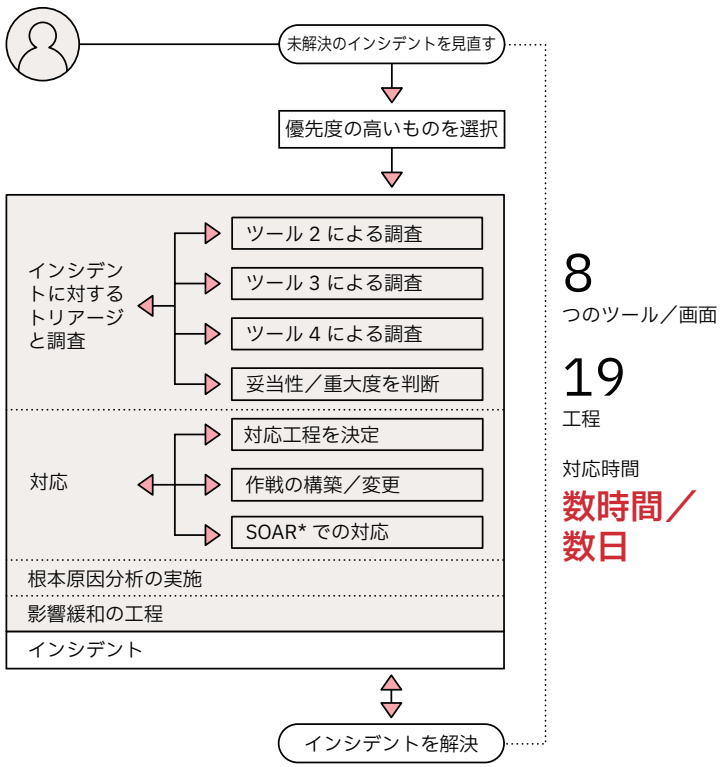
プラットフォーム化は、敵対的 AI のような新たな脅威に対処する新しい AI アプリケーションの展開を、より安全かつ効率的にする。AI を使ってプラットフォーム全体を活用できるようになれば、脅威に対する検出機能の改善と緩和の迅速化が図られ、それによってサイバー防御を強化し、組織のセキュリティー態勢やレジリエンスを高めることができるようになる。

図 2

AI はユーザー体験を簡素化し、セキュリティー・インシデント対応を迅速化する

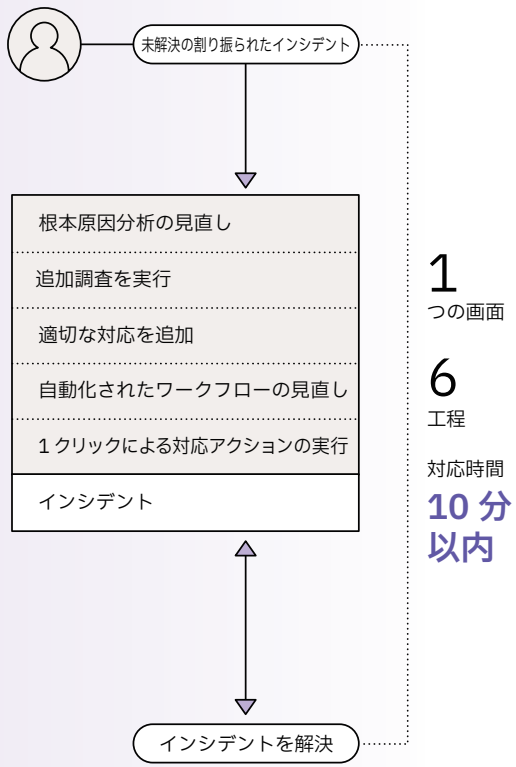
AI を使用しない場合

セキュリティー・アナリストの複雑なワークフローの典型



AI を使用した場合

AI ベースの XDR により簡素化されたワークフロー**



*SOAR（セキュリティー・オーケストレーション、自動化、レスポンス）は、セキュリティー・チームが個別のセキュリティー・ツールを統合および調整し、反復的なタスクを自動化して、インシデントと脅威への対応ワークフローを合理化できるようにするソフトウェア・ソリューションのこと

**XDR（Extended Detection and Response）とは、セキュリティー・ツールを統合し、セキュリティー・チームがより迅速かつ効果的に脅威を検知して阻止できるよう支援するセキュリティー・ソリューションのこと

企画・設計段階からハイブリッドでセキュアな基盤を構築することで、DX を促進する

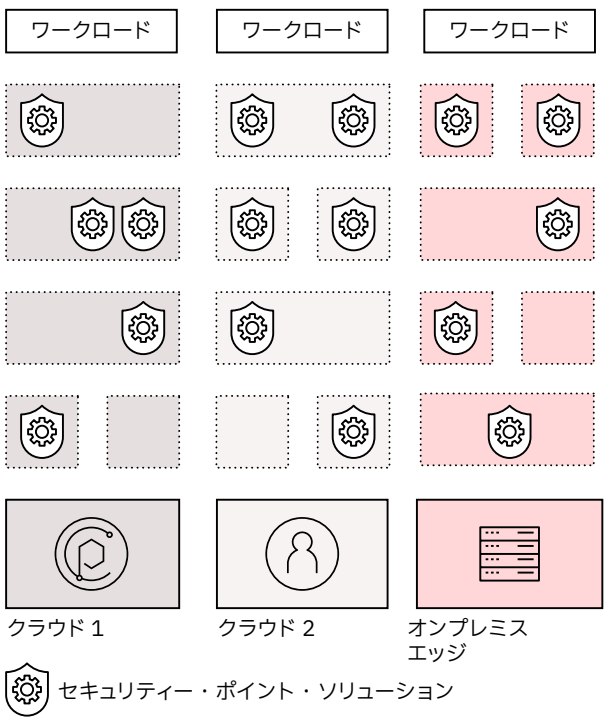
ハイブリッドクラウド・インフラを基盤とし、生成 AI を活用してプラットフォーム化を図る場合、セキュリティーがビジネス変革にとって重要な基礎となる。オープンなハイブリッドクラウド・アプローチを追求するとき、組織はユーザー体験を損なうことなく、異なる環境間でデータを保護しなくてはならない。セキュリティーはオンプレミスやエッジコンピューティングだけでなく、クラウド全体で統一された管理が必要であり、業務を阻害するような複雑なレイヤーを積み重ねてはいけない。

ハイブリッドクラウドと生成 AI にセキュリティーをシームレスに組み込み、プラットフォーム化することで、企業は DX の価値を最大限に引き出せるようになる。プラットフォーム化により、企業はいかなる環境においてもエンドツーエンドのユビキタスなセキュリティーを確保し、セキュリティー・ポリシーを簡素化できる。こうしたことにより、例えば大規模なファイアウォールを導入したり、数千にも及ぶファイアウォールの修正指示を短時間で展開したりすることが可能になる。

つまり、プラットフォーム化により、組織はセキュリティーを強固にし、チャンスを実際の成長へつなげやすくなる。さらに、効率性が高まり、対応も迅速化するほか、スケーラブルに変わる。いずれも、パフォーマンスが高く、レジリエンスに優れた組織に求められる特性である。プラットフォーム化というパラダイムを理解し、実践する組織は、よりハイブリッドでセキュアな組織へと変貌を遂げ、将来のチャンスを最大限に活用する先駆者となるだろう。

図 3

ポイント・セキュリティー・アーキテクチャー：サイロ化、分断化された状態

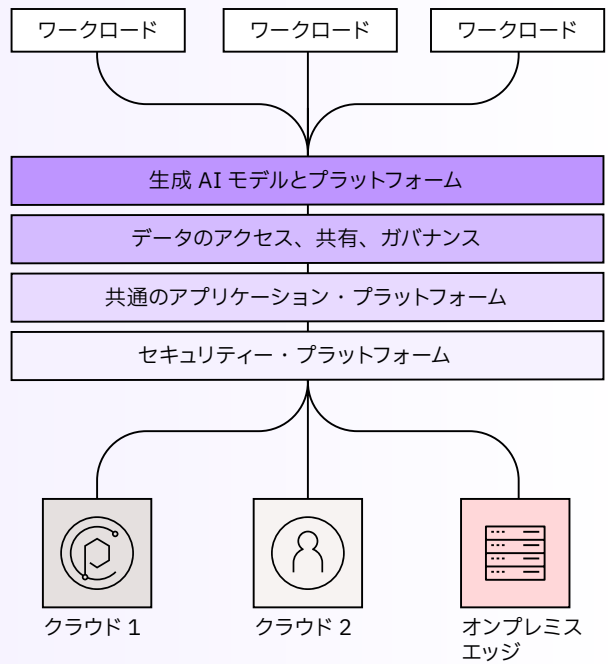


現状

- 組織はサイロ化され、イノベーションは不均質
- リソースの利用が非効率的
- 事業間の連携が困難
- 生成 AI を展開することに制約がある

図 4

ハイブリッド・プラットフォーム・アーキテクチャー：セキュア・バイ・デザイン（企画・設計段階からセキュリティーを確保）



将来像

- 安全で信頼できる生成 AI を大規模に展開
- IT（情報技術）と IS（情報システム）を緊密に統合し、迅速かつ安全なイノベーションを実現
- 自動化と標準化により、オペレーションを効率化する
- 意思決定を迅速に行い、価値実現までの時間を短縮

ケース・スタディー

クラウド・セキュリティー・アーキテクチャーの最新化により、サイバーセキュリティー・リスクを低減させた世界最大級の航空会社

ある世界最大級の航空会社は、アプリケーションのクラウド移行を決断したときに、今後は、それまでと根本的に異なるサイバー脅威環境に置かれることになると認識した。同社はこの DX を成功させるため、サイバー攻撃に対するレジリエンスの強化へ積極的な行動を取った。

同社は、アジリティー（機敏性）とより成熟したセキュリティー態勢を実現するように設計されたクラウド・セキュリティー・アーキテクチャーの構築に取りかかった。まずはマイクロセグメンテーション * に集中して取りかかり、社全体の IT 環境にわたってゼロトラスト・アプローチを適用した。侵入者による機密データへのアクセスやランサムウェアの脅威を防ぐためだった。このソリューションを導入したことで、同社はサイバー・リスクに対する可視性を高め、脅威により迅速に対応し、ハイリスクなシステムをリアルタイムで隔離できるようになった。

さらに、DevSecOps** モデルを用いてアプリケーション開発プロセスを変革し、開発者の意識を高め、セキュリティーへの備えをより強固なものにした。

この全社的なセキュリティー・ソリューションを 1 年間にわたり本番稼働し続けた結果、新たなアプリケーションやクラウド環境の残留リスクは軽減され、DX は加速度的に前進した。セキュリティーを自社の変革の中核に据えたことで、同社は自信を持ってオペレーションをクラウドに移行し、競争力も高まっている。

顧客体験はよりカスタマイズされ、効率的で費用対効果の高いオペレーションも実現した。

* マイクロセグメンテーションとは、ゼロトラスト・アプローチの考え方を踏襲し、アクセスが必要なリソースだけが IT 資産に接続できるよう細かくアクセス制御を行う新しいセキュリティーの概念のこと

** DevSecOps とは、「開発（development）」「セキュリティー（security）」「運用（operation）」の略。ソフトウェア開発の初期設計から統合、テスト、実装、デリバリーまですべてのフェーズでセキュリティーの統合を自動化すること

アクション・ガイド

1

プラットフォーム化を通じて、次世代のサイバーセキュリティーへ迅速に移行する。

取締役会から現場マネージャーまで、あらゆるレベルのリーダーが足並みをそろえて、複雑さやコスト、摩擦ポイントを減らすように努め、組織全体でサイバーセキュリティーを強化する。プラットフォーム化がもっとも効果を発揮するサイバーセキュリティー・インフラおよびプロセスを優先する。

2

サイバーセキュリティー担当者が、最重要課題に取り組めるようにする。

プラットフォーム化により定型的な業務を自動化することで、サイバーセキュリティー担当者は単純作業から解放され、高度で戦略的な仕事に向き合えるようになる。プラットフォーム・ファーストのアプローチを用いることで、セキュリティーへの考え方が「受動的」から「積極的」に変わる。

3

セキュリティーの全プロセスにゼロトラスト戦略を採用する。

今日のサイバー脅威の下では、セキュリティーのゼロトラスト・アプローチは不可欠だ。例えば、セキュリティー・オペレーション基準の設定や、脅威ベクターの抑制、さらにレジリエンス向上に取り組む上で必要な思考態度や手法を取り入れる。あらゆるユーザーとデバイスが脅威になり得ると想定することで、社内外の脅威から身を守れるようになる。

4

リターンの大きいセキュリティー投資を優先することで、関係者の理解を得る。

プラットフォーム化によって、セキュリティー機能の向上とコスト削減が同時に図れる領域に目を向ける。具体的には、セキュリティー・ソリューションや契約先ベンダーの整理・統合、オペレーションの効率化、複雑性の低減、イノベーションの加速などだ。こうした領域は早期に効果を示せるため、セキュリティー運用モデルをより大きく変革するきっかけとなり得る。

IBM Institute for Business Value

IBM Institute for Business Value（IBV）は、20 年以上にわたって IBM のソート・リーダーシップ・シンクタンクとしての役割を担い、ビジネス・リーダーの意思決定を支援するため、研究と技術に裏付けられた戦略的洞察を提供しています。

IBV は、ビジネスやテクノロジー、社会が交差する特異な立ち位置にあり、毎年、何千もの経営層、消費者、専門家を対象に調査、インタビューおよび意見交換を行い、そこから信頼性が高く、刺激的で実行可能な知見をまとめています。

IBV が発行するニュースレターは、ibm.com/ibv よりお申し込みいただけます。また、LinkedIn（ibm.co/ibv-linkedin）をフォローいただくと、定期的に情報を入手することができます。

変化する世界に対応するためのパートナー

IBM はお客様と協力して、ビジネス・インサイト、高度な研究成果、およびテクノロジーの専門知識を組み合わせることにより、急速に変化し続ける今日の環境における卓越した優位性の確立を可能にします。

注釈および出典

1 Muggah, Robert and Mac Margolis. “Why we need global rules to crack down on cybercrime.” World Economic Forum. 2023 年 1 月 2 日。https://www.weforum.org/agenda/2023/01/global-rules-crack-down-cybercrime/#:~:text=Cybercrime%20is%20big%20business.,%2410.5%20trillion%20annually%20by%202025

2 Global Security Operations Center Study Results. Morning Consult and IBM. 2023 年 3 月。https://www.ibm.com/downloads/cas/5AEDAOJN

3 IBM X-Force Threat Intelligence Index 2024. IBM. 2024 年 2 月。邦訳「IBM X-Force 脅威インテリジェンス・インデックス 2024」https://www.ibm.com/jp-ja/reports/threat-intelligence

4 Cost of a Data Breach 2023. IBM. 2023 年 7 月。邦訳『2023 年「データ侵害のコストに関する調査」』https://www.ibm.com/jp-ja/reports/data-breach

5 Basu, Suswati. “Massive hack hits AI servers, exploits Ray framework vulnerability.” readwrite. 2024 年 3 月 28 日。https://readwrite.com/massive-hack-hits-ai-servers-exploits-ray-framework-vulnerability

6 Unlock the benefits of simplified security. Palo Alto Networks. 2024 年 4 月 25 日にウェブサイトよりアクセス。https://www.paloaltonetworks.com/why-paloaltonetworks/consolidation

7 同上

8 McCurdy, Chris, Shlomi Kramer, Gerald Parham, and Jacob Dencik. Prosper in the cyber economy. IBM Institute for Business Value. 2023 年 1 月 30 日。https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/security-cyber-economy

9 同上

10 同上

11 Dickson, Frank and Matthew Marden. The business value of Palo Alto Networks cybersecurity platforms. IDC. 2024 年 2 月。https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/idc-panw-business-value.pdf

12 同上

13 同上

14 McCurdy, Chris, Shlomi Kramer, Gerald Parham, and Jacob Dencik. Prosper in the cyber economy. IBM Institute for Business Value. 2023 年 1 月 30 日。https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/security-cyber-economy

15 The CEO's guide to generative AI/Cybersecurity. IBM Institute for Business Value. 2023 年 10 月 30 日。https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/ceo-generative-ai/cybersecurity

16 Muppidi, Sridhar, Lisa Fisher, and Gerald Parham. AI and automation for cybersecurity. IBM Institute for Business Value. 2022 年 7 月 20 日。邦訳『「生成 AI を以って生成 AI を制す」ー新たな局面を迎えるサイバーセキュリティー対策とは』https://www.ibm.com/thought-leadership/institute-business-value/jp-ja/report/cybersecurity-jp

17 同上

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America | May 2024

本書は英語版「Unify your fragmented security: Accelerate transformation with platformization」の日本語訳として提供されるものです。