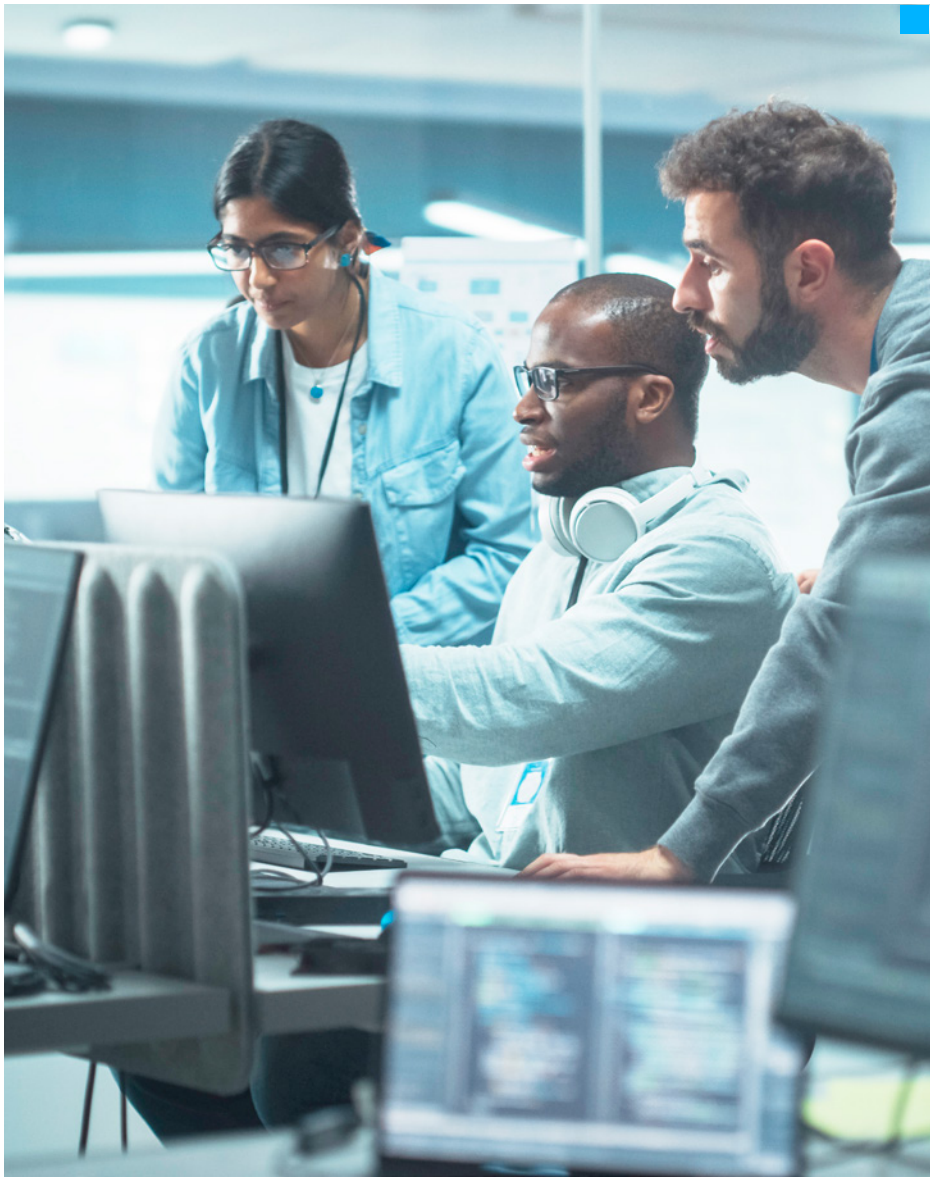
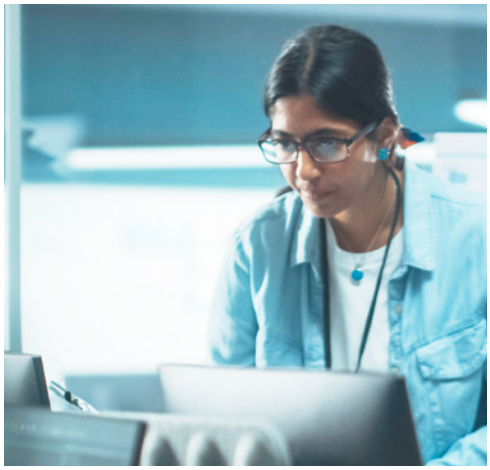


# サイバーセキュリティーを支える AI と自動化

*テクノロジーと人材との融合で成功するリーダーとは*

## IBM をお勧めする理由

IBM セキュリティーでは、機械学習や自然言語処理などの AI 技術を活用して、セキュリティー運用アナリストが脅威を察知しながら、レスポンス時間とコストを削減できるよう支援いたします。詳しくは、こちらをご覧ください：
ibm.com/jp-ja/security/artificial-intelligence



# 重要なポイント

*AI と自動化により、サイバーセキュリティー・チームは、日常的な定型作業から解放され、最も必要とされる場所で、限られた人間の専門知識を活用できるようになります。*

## セキュリティー・インシデントの件数と規模により、新たな運用アプローチが求められるようになりました

AI と自動化により、セキュリティー運用全体の見える化と生産性が向上します。最先端 AI の導入企業では、ネットワーク通信の 95% を監視し、インシデント検知にかかる時間を 3 分の 1 まで短縮しています。

## セキュリティー対策用の AI が注目を集めています

セキュリティー運用で AI を導入する動きが広がっていると報告している経営者のうち、93% がすでに使用しているか、導入を検討しています。

## セキュリティー AI をいち早く導入している企業では、主要なコスト・パフォーマンス指標が向上しています

優れた企業は、セキュリティー投資収益率 (ROSI) を 40% 以上高め、データ漏洩コストを 18% 以上削減したことにより、サイバーセキュリティー人材に再投資するための資金を捻出することができました。

# 急激な変化で高まるサイバーリスク

今のデジタル・オペレーションは、価値を高める一方で、新たな脆弱性も生み出されています。

サイバーセキュリティーの脅威が急増したのは、2021 年です。この時、米国のコロニアル・パイプラインやいくつかの水処理施設のシステムが、攻撃対象とされました。[1] 最近のある調査によれば、2020 年から 2021 年にかけて、ランサムウェア攻撃が 105% 増加し、製造業が最も狙われる業種となったと言われています。[2] また、ここ 1 年では、かつてなく深刻な被害を受けたサプライチェーンへの攻撃も数件見られました。SolarWinds や Microsoft Exchange Server のエクスプロイトから ApacheLog4j の脆弱性に至るまで、認知度の高い攻撃が多く発生するというニュースが多くなり、ビジネス・リーダーやその顧客の間でセキュリティーに対する意識や警戒心が高まっています。[3]

今までの状況と現在の状況の決定的な違いとは何でしょうか？

つまり、パンデミックの状況により、デジタル化が加速し、チャンスとリスクが共に増大したのです。[4] 今では、リモート・ワーカーが大幅に増えています。増えるクラウド・ユーザー。増えるクラウド・サービス。サード・パーティー・パートナーとの間で必須となるシステム・インテグレーション。IoT データをクラウドに転送する圧倒的な数のエッジ・デバイス。すべてが相互につながり、依存し合うことで、高度な接続性が実現し、ほんの数年前ではあり得なかったスピードとスケールで価値が創出されています。

このようなイノベーションにはメリットがありますが、コストもかかります。新しいデバイス、新しいパートナー、そして新しい統合が原因で、企業組織全体の攻撃対象が劇的に増加する恐れがあるのです。サプライヤーの小さなミスから従業員の不満、さらにはデータの流出、サービス妨害、ランサムウェアなど、脅威ベクトルは広がるばかりです。さらに、攻撃者は独自に戦術、技術、および手順を進化させ、人工知能 (AI) や自動化で弱点を探り、より効率的な攻撃をしかけてくるため、問題はより複雑になっています (図 1 参照)。[5]

その結果、経営者の多くは、厳しい現実を目の当たりにすることになります： 現在の「常時接続」のデジタル運用は、価値を高めると同時に、新たな脆弱性が生み出されてしまいます。最先端のテクノロジー・サービスによりあらゆる効率化を実現しても、多くの企業はデジタル・フットプリントが複雑で、まだまだ未知の要素が多いことに徐々に気付き始めています。それらの動的要因がある上に、人手不足であるセキュリティー・チームは、さまざまな情報源からの大量のデータ、膨大なツールの対応に追われ、洞察不足さえ起きています。こうした課題に対して、最も知識の豊富なセキュリティー専門家のスキルや、最大規模で有能なサイバーセキュリティー運用チームの能力を活用しても対応することができません。

## 現状では、運用に対する新たなアプローチが求められているのです。

サイバーセキュリティーのリーダーは、チームを成功に導くために、より予防的かつ先見的な姿勢でコアビジネス運営を保護する必要があります。当社の調査によると、より多くの組織が脅威管理への未来を見据えたアプローチを選択し、AI を活用した自動化を導入して、洞察力の向上、生産性、規模の経済性を推進していることがうかがわれます。

AI テクノロジーを活用した次の 4 つの主な方法でセキュリティーを激変させることができます：

- 機械学習機能により、パターンの特定、新しい資産やサービスの点検、AI モデルの性能を改善することができます。
- 推論機能により、データ分析、シナリオ・モデリングの強化、および新たな攻撃経路を予測することができます。
- 自然言語処理を使用すれば、テキスト・データ・ソースのマイニング、脅威インテリジェンスの向上、知識源の充実を図ることができます。
- 自動化は、時間のかかる作業を調整し、レスポンス時間を改善し、人間のアナリストの負担を軽減するのに役立ちます。

これらの機能を組み合わせることで、セキュリティー運用を一新させることが可能です。

このような AI と自動化の組み合わせによって、スピード、洞察力、柔軟性のいずれにおいても、パフォーマンスを劇的に向上させることができます。本レポートでは、その詳細についてご紹介します。こうしたパフォーマンスの向上により、サイバーセキュリティー・チームは、本当に重要な業務に集中することができます：コストと複雑さを軽減しながら、先を見越した脅威からの保護、検知、応答、および回復を実現させます。

図 1

**セキュリティーの破壊者**

セキュリティー運用チームは新たな課題に直面しています

新たに拡大する攻撃ベクトル

攻撃者は適応的、多変量解析による脅威へと移行しつつあります

攻撃者は、攻撃を自動化へとシフトさせています

サイバー・スキルのギャップと能力の制約

見える化、およびサードパーティー・プロバイダーとの協調性の欠如

メタデータ、状況、行動といったデータ種別にまたがる洞察の欠如

さまざまなデータ・ソースやツールからの情報過多

第 1 章

# 普及が著しいセキュリティー向け AI

セキュリティー運用を支援する際に AI をどう活用しているかを理解し、サイバーセキュリティーのパフォーマンスが受ける影響を定量化するために、IBM Institute for Business Value (IBV) は、APQC (米国生産性品質センター) と共同で、組織の IT および運用技術 (OT) のサイバーセキュリティーに全責任を持つ 1,000人の経営者を対象にアンケートを実施いたしました。16 業種、世界の 5 地域の代表に回答していただきました (P32「調査・研究方法」参照)。

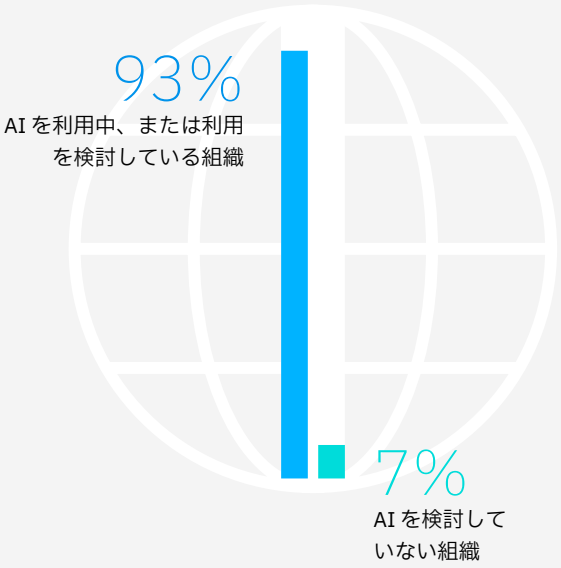
回答者には、組織のセキュリティー機能のパフォーマンスと、サイバー・リスクとコンプライアンスの管理に AI と自動化をどの程度まで活用しているかについての情報を提供していただきました。また、保護や予防だけでなく、検知と応答のプロセスにおいて AI をどのように活用しているか、セキュリティー運用での AI の支援についても、意見を提供していただきました。これらの洞察をもとに、生産性、耐障害性、および関連ビジネス上のメリットに重点を置いて、AI がサイバーセキュリティーのパフォーマンスに与える影響を評価しました。

全体的に見ると、世界全体および業種を問わず、大多数の企業がセキュリティー機能に AI と自動化を導入している、または導入を検討していることがわかりました。セキュリティー・ライフサイクル・プロセスの少なくとも 1 つにセキュリティー機能向けの AI を導入しているという回答者は、64% に上り、29% が導入を検討中とのことです。つまり、セキュリティー向け AI は、近い将来、ほぼ一般的な機能となる可能性があるのです (図 2 を参照)。残りの 7% は、セキュリティーへの AI と自動化の活用を考えていないと回答しています。しかし、その場合、セキュリティー事象のスピードと量の増加に対応するのに苦慮する可能性が高くなり、危うい立場に置かれることは否めません。

図 2

**広範な導入**

セキュリティー運用で AI の活用を検討していない企業は、ごく少数です



現在、AI セキュリティー・ソリューションを試用、導入、運用、または最適化している 64% を「AI 導入企業」と呼んでいます。セキュリティーにおける AI の活用はまだ始まったばかりで、企業で活用されるようになったのは、ここ 2 年のことです。しかし、今後 AI 導入は急速に進むと予想されます。AI の具体的な利用について考えてみると、AI 導入企業が保護と予防のサポートに AI を活用する割合は、今後 3 年間で平均で約 40% 増加し、検知と応答でも同様に AI を導入する可能性が高くなると予測されます。

他の調査結果でも、同じように、セキュリティー向け AI の導入が加速すると予想されています。最近のある調査では、サイバーセキュリティー関連 AI にかける経費は 2027 年までに、年平均成長率 24% で増加し、市場価値は 460 億ドルに達すると予測されています。[6]

## テクノロジーと人材との融合で成果を上げる

AI 導入企業は、AI 主導の洞察と AI を活用した自動化により、セキュリティー分野の専門家レベルの検知、およびレスポンス機能をどう補完していくべきか検討しています。こうした企業では、セキュリティー AI システムが、熟練したセキュリティー・アナリストのように、異常な行動を見つけ出し、脆弱性を動的に評価し、更に、新たな脅威を知らせる異常な行動に警告を発することが可能であると考えています。こうした AI の活用により、自社のセキュリティー業務に大きなメリットがあったと報告している AI 導入企業は、65% に上ります (7 ページの図 3 を参照)。セキュリティー AI は、人間のアナリストとは異なり、機械学習と自動化を用いて、ハイブリッド型マルチクラウド運用の過酷なスピードと規模に対応し、最も有能で、最も認められたセキュリティー専門家の能力よりはるかに高いレベルで、一貫性と緻密性を実現しています。(視点「セキュリティー AI が有効な理由とは？」を参照)

例えば、AI を活用することで、正常な行動を追跡し、モデル構築を自動化することができます。これにより、AI セキュリティー・ソリューションは、想定される行動からの逸脱に照準を合わせ、例外パスの脅威の影響を分析します。AI 導入企業の 57% は、脅威レスポンスを強化して、脅威封じ込めを自動化し、事業継続性を最適化するなど、大きな影響があると述べています。AI セキュリティー・ソリューションでは、異常な活動を状況から理解することで、危険にさらされているセキュリティー・ポリシーおよび制御を判断し、関連する洞察でアラートを出し、所定の改善措置を講じることが可能になります。

このように、セキュリティー AI が人間の専門家の「サイバー・アシスタント」として働くことで、さらにメリットが大きくなり、スキルや人材の不足に直面するセキュリティー・チームの負担を軽減することができます。60% の AI 導入企業が、アナリストの業務効率を高める自動データ・エンリッチメントやセカンドスクリーン機能は、極めて有益なセキュリティー機能であると回答しています。AI 脅威モデルは、より長い期間、さまざまな動作条件にわたり、はるかに多くの事象を参照するため、人間のアナリストでは理解できないような脅威に対して、専門的な能力を発揮することができるのです。

AI が生成した洞察で強化された AI 主導の自動化機能は、ユーザー、デバイス、場所ごとに脅威を切り分け、適切な通知とエスカレーション措置を講じ、人間の専門家が最善の調査と修復方法を決定することができます。こうした能力を高めた組織では、サイバーセキュリティー・アナリストは、人間の判断が欠かせない、もっと複雑な問題に対処するためのスキルと専門知識を磨くなど、本当に必要な業務に集中することができます。

**視点**

# セキュリティー AI が有効な理由とは?

拡大する攻撃対象領域の防御や、激増するセキュリティー事象への対応には、セキュリティー AI と自動化の導入が急務となっています。AI が有効な理由とは？ 簡単に言うと、反復的な機械学習と分析的なモデルのチューニングを組み合わせているからだ、と言えます。

チューニングとは、状況に応じて変化する変数に頼りすぎることなく、分析モデルの性能を最適化するプロセスのことです。その裏側では、無数の事例をもとに、機械学習アルゴリズムがパターンを見つけ出し、さまざまな変数への最適な対処方法を学習します。この訓練プロセスが、AI モデルのパフォーマンスを向上させる上でのカギとなります。

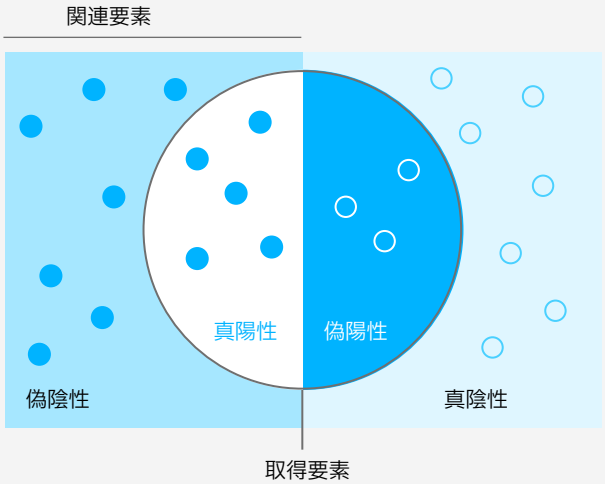
AI セキュリティー・ソリューションは、機械学習でモデルの精度と再現性を高め、実際のセキュリティー脅威、つまり、真陽性と、正常な事象、つまり、偽陽性および真陰性とを区別することで、アナリストのアラート業務の負担を軽減させます (図参照) 。これらのソリューションは、セキュリティー事象の大部分を選別し、さまざまな事象を状況に沿ったデータ洞察で強化し、アナリストによる検査や調査活動を支援します。AI により信号対雑音比を向上させることで、アナリストは、リスクが最大となる実際の脅威への対応業務を集中して行うことができます。

検索された項目のうち、関連するものはいくつありますか?

精度 = 

関連項目はいくつ検索されましたか?

再現性 = 




*出典: 引用元 https://en.wikipedia.org/wiki/F-score*

AI と自動化により、アナリストは最後に人間の判断を必要とする複雑な問題に再び集中できるようになり、より充実した職場環境になります。

AI は非構造化データソースと構造化データソースの両方を分析できるため、脅威情報サービスやオープン・ソース・インテリジェンス (OSINT) を使って内部データおよび外部データを融合し、状況の変化や脅威の状況を包括的に描写することができます。サイバーセキュリティー・アナリストは、AI により、インシデントの検知、応答、回復にかかる時間を短縮することができます。

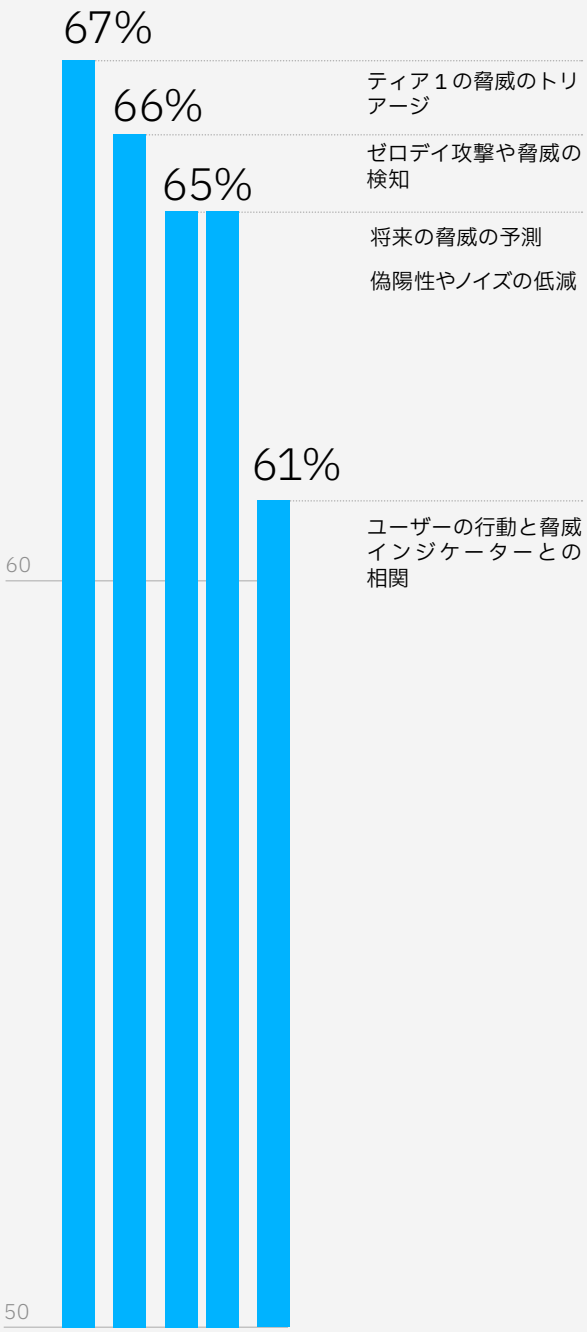
AI が、より効率的なエスカレーション、レビュー、および修復の手順を支援することで、セキュリティー・ガバナンスとコンプライアンスが高まります。AI により、何度も繰り返す、時間のかかる作業が自動化されることで、アナリストの疲労が軽減され、より速く、しかも、ミスを抑えて、情報に基づいた、より的確な意思決定を行う能力をアップさせることができるのです。また、膨大な量のイベントをセキュリティー AI と自動化ソリューションでルーティン化すれば、人間のアナリストの熟練した貴重なスキルが最大限に活かされます。その結果、より充実した、より満足度の高い職場環境となり、優秀なサイバーセキュリティー人材が集まり、定着させることができるようになるのです。

AI の洞察力と自動化を自社の従業員の専門知識と組み合わせることに成功した AI 導入企業は、AI アプリケーションは自社のセキュリティー運用に大きなメリットがある、と述べています (図 3 を参照)。67% の企業が、ティア 1 の脅威をより効果的に選別できるようになったことで、基本的な検知に要するコストが削減され、その時間が短縮されたと報告しています。さらに、誤検知やノイズを減らすことで、アナリストによる検査の必要性が減ったと回答した企業は、65% に上ります。そして、行動分析学を活用することで、将来の脅威を予測できるという回答が 65% もあり、先を見越す上での重要な一歩となっています。

図 3

**AI のメリット**

AI 導入企業は、重要な機能について AI ソリューションを活用し、パフォーマンスを向上させています。




*Q：次の AI アプリケーションのうち、セキュリティー運用に最も影響を与えたものはどれですか (上位 5 つを選択)？*

## AI 投資が実を結ぶ

ある情報筋によれば、2025 年までに、サイバー犯罪による世界経済への被害は毎年平均 10.5 兆ドルにもなると試算されています。[7] 2021 年、Ponemon Institute社と IBM の年次レポート「情報漏えい時に発生するコスト (Cost of a Data Breach) 」によると、データ侵害の平均コストは過去最高に達し、更に、データ侵害の件数は驚愕の 68% に跳ね上がり、関連するコストも大幅に増加しています。[8]

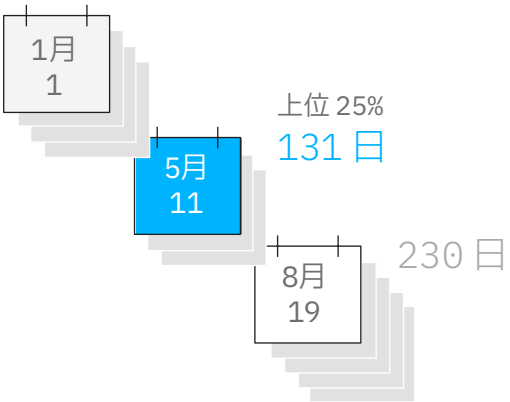
この調査結果の中の、セキュリティー・コスト・パフォーマンス指標から分かるように、セキュリティー・ライフサイクルにおいて AI に初期投資することが、組織のサイバー犯罪対策で効果的に役立っていることが明らかになりました。実際、導入企業の上位 25%、つまり、各指標の 75% または 25% に該当する企業は、AI と自動化で 3 つの主要業績評価指標が大幅に改善し、セキュリティー機能のパフォーマンスと有効性が根本的に改善されたと認めています。(上位企業の測定法については、32 ページの「調査・研究方法」を参照)。効果は以下の通りです。

- サイバーセキュリティーにかかる総コストが 15% 以上削減され、保護と予防、検知と応答のセキュリティー・ライフサイクル・プロセスの効率と生産性が向上します。
- 情報漏えいのコストが少なくとも 18% 削減されています。これは、検知と応答プロセスの効率性が改善されたことを示しています。これには、損失しうるビジネス (顧客とサプライヤー)、投資、将来のビジネス・チャンスといった、関連する運用コストと風評コストの削減、または回避が反映されています。
- セキュリティー投資収益率 (ROSI) が 40% 以上向上し、サイバーリスクとそれに伴う運用コストや風評被害が減少、回避されたことを示しています。

AI が同様の効果をもたらすとした当社の調査は、他の調査と同様の結果となっています。Ponemon Institute社と IBM の報告によると、AI と自動化との組み合わせは、データ侵害の総コストを削減することができる唯一かつ最大の方法であることが判明しています。[9] 同様に、ゼロトラスト・セキュリティーに関する IBV の調査から、主要企業の 61% がセキュリティーの自動化と編成を導入することで、セキュリティーの資本コストと運用コストが削減されたことが明らかになっています。[10]

これらの結果から、セキュリティー・リーダーがセキュリティー・ライフサイクルにおいて AI と自動化を採用している理由が分かると言えるでしょう。次に、2 つの重要な分野において、リーダーがどう業績を向上させているかを探ってみましょう：保護と予防、および検知と応答

AI を使用していない組織が、サイバー・インシデントの検知、応答、回復に 230 暦日かかるとすると、AI を使用することで、その時間を最大 99 日まで短縮することができます。



第 2 章

# AI でセキュリティー・ライフサイクル全体のパフォーマンスが向上

クラウド・セキュリティー固有の責任共有モデル、およびゼロトラスト・アプローチに固有の IT 統合に加えて、AI と自動化は、今後のセキュリティー運用の基本的な機能となるでしょう。

セキュリティーの AI と自動化により、状況と過去のデータで強化された有意義な洞察を作り出し、組織内外のパートナーとの連携と協力関係が一層推進されます。これにより、スキルの高い人材は、脅威が深刻化する前に調査することができます。AI と自動化により、保護と予防、および検知と応答の両プロセスのパフォーマンスを向上させることで、組織全体のサイバー・レジリエンスに大きな影響を与えられます。

この影響についてさらに理解を深めるために、AI 導入企業が、セキュリティー運用のライフサイクルにおいて、保護と予防、および検知と応答のプロセスの双方で、AI と自動化をどのように活用しているかについて調査しました。これらの洞察から、こうしたテクノロジーを組み合わせることで、業務の効率と効果がどう向上するかを評価しています。また、こうした洞察は、パフォーマンスの向上が、生産性の向上や従業員満足度の向上など、ビジネスのダウンストリームにどのようなメリットをもたらすかを説明するのにも役立ちました。

AI と自動化によって運用パフォーマンスを向上させれば、全社的なサイバー・レジリエンスを強化することができます。

## 保護と防止：AI によるリスク軽減、コスト・コントロール、および信頼関係の構築

**課題**

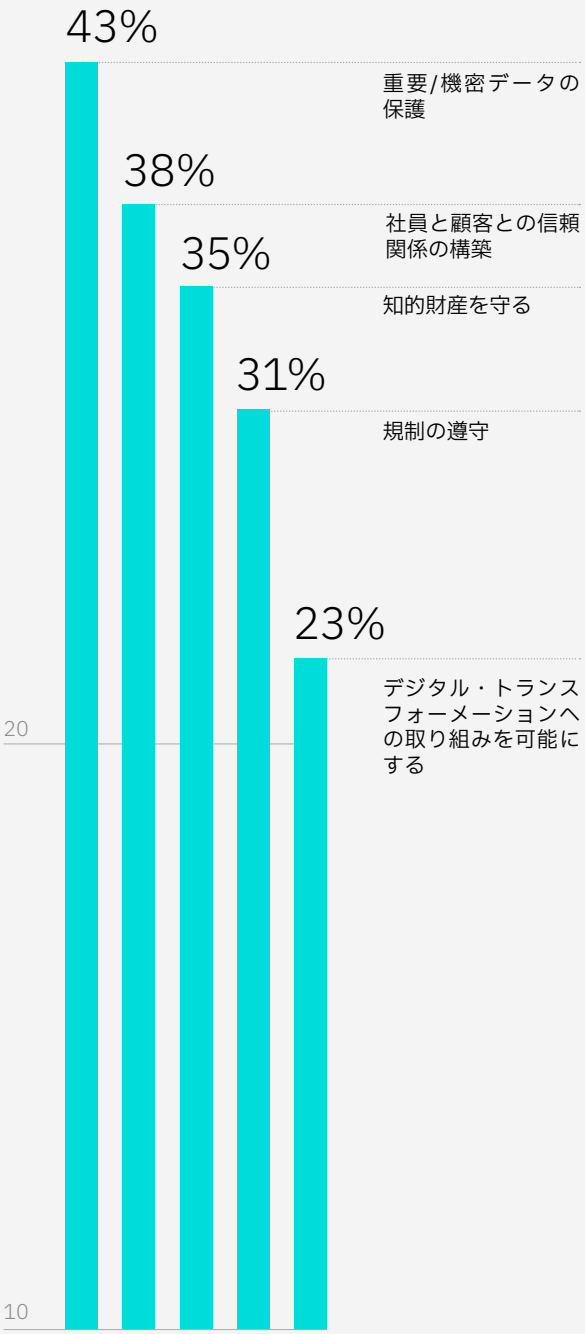
近年、リモート・ワーカー、およびクラウドベース・アプリケーションやサーバーの増加に伴い、監視しなければならないエンド・ポイントやアプリケーションの数も増大しています。サイバー犯罪者は、接続されたサービスを悪用して新たな脅威ベクトルを作り出し、場当たり的なフィッシング詐欺などの攻撃から、支払うまで企業を実質的に人質に取るランサムウェア・キャンペーンへと巧妙化が進んでいます。IBM X-Force® により 2021 年に検出された攻撃種類のうち、ランサムウェアがトップに入った一方で、フィッシング詐欺は侵害経路からの攻撃でトップとなり、攻撃全体の 41% となっていました。[11]

このように巧妙化するサイバーセキュリティーの脅威は、企業とその顧客にも影響を及ぼします。AI 導入企業は、顧客、パートナー、従業員から信頼を勝ち取り、築き上げるために、リスク低減、機密データの保護、および知的財産権の保護に重点的に取り組んでいます (図 4 を参照) 。

図 4

**見張る AI**

AI 導入企業は、企業や顧客のデータを保護し、信頼性を維持していくことを目指しています




*Q：貴社が AI を推進する際の主な要因は何でしょうか？ (保護と予防に焦点を当てた目標。)*

### AI の価値提案

おそらく、AI と自動化をゼロトラスト・モデルと組み合わせることで、ビジネスで最も大きなメリットを得られるのではないでしょうか。保護と予防については、これらの機能が運用上のサイロを取り払い、組織のデジタル資産 (データ、デバイス、ユーザー、ネットワーク、ワークロード、アプリケーション、エコシステムを通じたパートナーとのやり取り) 全体の可視性を向上させます。

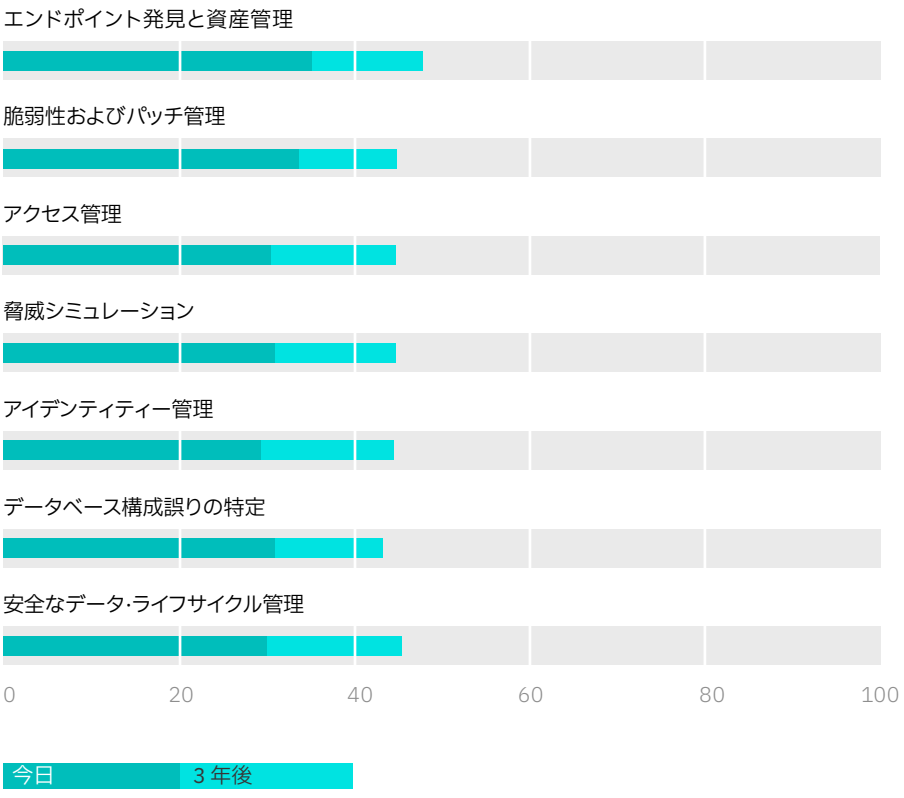
AI と自動化により、オンプレミス、エンドポイント、輸送中、クラウド上における機密データが定期的に発見、分類されることで、こうした見解が推進されます。このテクノロジーによって、企業はソース・データとメタデータを使用して、ある所定のやりとりの完全な状況を再現し、最も機密性の高いデータがある場所、誰が (どのように) このデータにアクセスし、誰が (いつ) それにアクセスし、このデータで何を行っているかを理解することができます。これにより、データ・プライバシーや規制遵守のための基準を満たし、機密性の高いデータ・リポジトリーへのアクセスを監視し、制御することができます。

AI 導入企業は、自社のデジタル環境の全体的な視野を求めるために、エンドポイントの発見と資産管理に AI を活用することを最優先としています。現在、導入企業の 35% が、これらの業務に AI と自動化を導入し、3 年後には導入率が 50% 近くになる予定です (図 5 参照) 。さらに、34% という僅差で、脆弱性管理への AI 導入が続いています。AI 導入企業は、今後 3 年間で、保護と予防向けの AI 活用を平均 40% 程度増やすと見込んでいます。(視点「AI は、保護や予防に、どのように役立つのか」参照) 。

図 5

**AI を保護と予防に活用**

AI 導入企業は、拡大し続けるデジタル資産全体の保護にも AI を活用することを検討しています




*Q. 現状、AI による自動化はどのような用途で実施されていますか？更に、3 年後は？(保護と予防に重点を置いた使用事例。)*

**視点**

# AI による保護と予防の仕組み

これらのトップ 5 の活用事例を見ると、AI 導入企業は、リスク低減、攻撃防止、ひいては信頼関係の構築にこだわり、ビジネスの根本的な価値を守るために投資していると言えます。

**エンドポイント発見と資産管理を実現する AI 。**不正デバイスは、組織の従来のセキュリティー・ポリシーをかいくぐって動作するため、発見が難しくなっています。AI に、特定の資産タイプ、ネットワーク・サービス、エンドポイントに関連する状況、環境、動作を学習させることで、企業は許可されたデバイスのみにアクセスを制限し、未許可のデバイスや未管理のデバイスからのアクセスを防止できるようになります。

**脆弱性管理用の AI。**AI を活用した脆弱性評価により、不適切な構成のデバイスを特定し、管理者はデバイスの削除や再構成を行うことができます。運用技術 (OT) 環境において脆弱性スキャンが有効になるとシステムが不安定になることがありますが、組織は AI と自動化によりパッシブ監視を行うことができます。また、AI から不正な攻撃に関する情報が提供されることで、脆弱性パッチを当てる際の優先順位付けが簡単になり、顧客はリスクベースのアプローチで脆弱性管理を行えるようになります。

**アクセス管理用の AI。**企業は、ユーザーやアプリケーションによるデータやサービスへのアクセスを、AI で監査することができます。機密性の高いリソースの権限が確立されると、AI により、コントロール・プレーン全体の活動の調整、行動の監視､異常の警告、状況に基づく洞察の生成、アラートの送信、是正措置の実施などが行われます。

**脅威シミュレーション用の AI**。脅威シミュレーターは、企業ネットワーク上のソフトウェア・エンドポイントに接続され、サイバーセキュリティー・インシデントのライフサイクルをエミュレートすることができます。これは、実稼働環境のサーバーやエンドポイントに関わることなく、実際のセキュリティー防御がテストされるため、企業は、事業運営が影響を受けずに、防御の穴を見つけ、対処することができます。

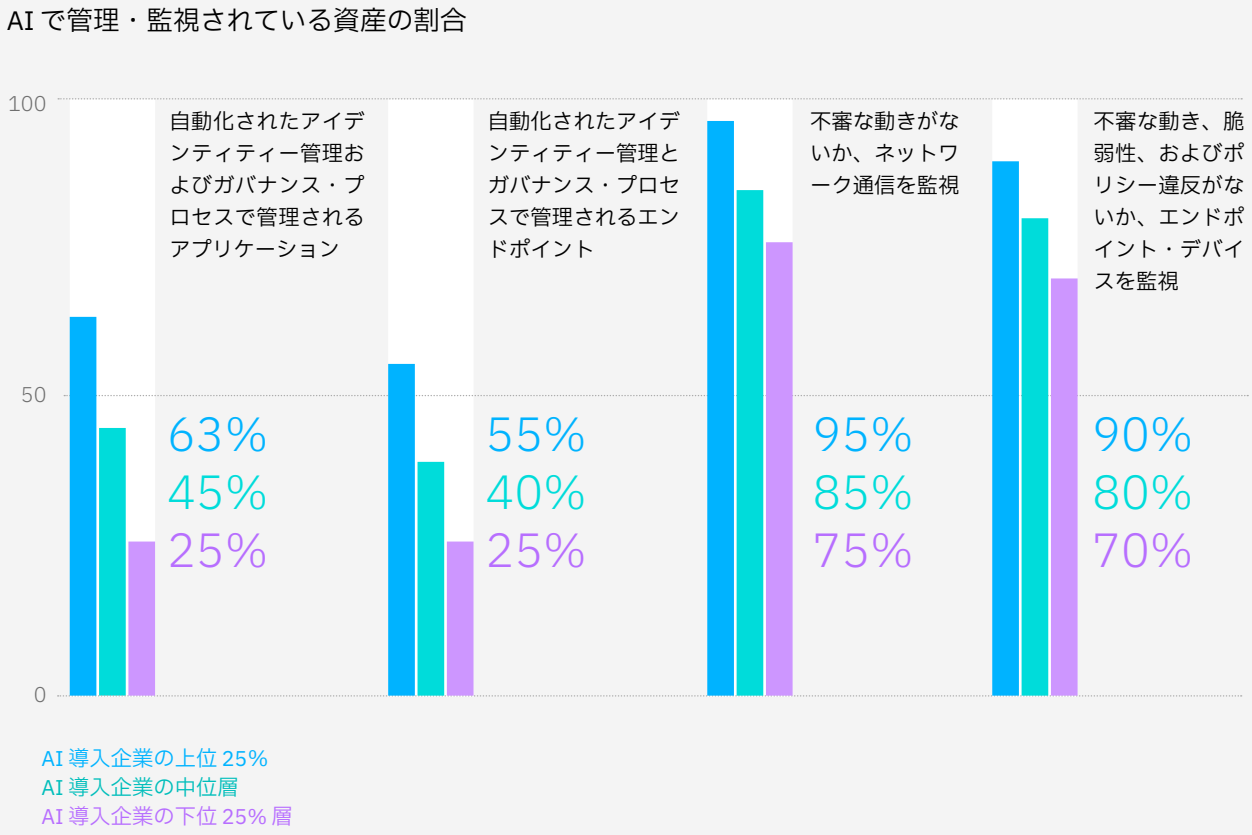
**アイデンティティー管理用の AI**。ゼロトラスト・セキュリティー運用により、IT インフラストラクチャーとセキュリティー認証機能で求められる要求が高まります。特に ID に関しては、ほぼリアルタイムでの調整が必要になります。ゼロトラストでは、運用能力が大幅に向上する一方で、運用能力や調整 (例えば、複数の場所から複数のデバイスを使用するリモート・ワーカーへの対応) において、新たな問題が発生することもあります。AI により、過去の行動、状況データ、およびロールベースのポリシーの組み合わせに基づいて、唯一のユーザー・プロファイルが作成されることにより、認証サービスを強化することができます。

AI と自動化の導入により、より多くのエンドポイントやアプリケーションの保護が可能になると同時に、ネットワーク通信の監視能力も向上させることができます (図 6 参照)。AI を導入したトップ企業は、自動アイデンティティー管理およびガバナンスを適用しているのは、アプリケーションで 63%、エンドポイントで 55% であると報告しています。これらのAI 導入率は、アプリケーションで 67% 増加、エンドポイントで 50% 増加したことになります。これにより、複数のクラウドにおけるサービスに依存し、拡大し続ける運用をより広く見える化することができます。

図 6

**広がる可視性**

AI 導入企業は、自動化により、
より多くの資産を管理し、監視
できるようになります



これらの分野で報告されたパーセンテージの中央値でさえも、自動化で管理されているアプリケーションとエンドポイントの数は増加傾向にあり、パフォーマンスが向上すれば、もっと大きな効果も期待できます。AI 導入企業は、ネットワーク通信やエンドポイント・デバイスに不審な動きがないかを監視するために、AI と自動化の併用を一層進めていると報告しています。優れた AI 導入企業は、ネットワーク通信の 95%、エンドポイント・デバイスの 90% の割合で監視に AI を利用しているといいます。

保護と予防の本当の価値は、本質的に回避を測定することが困難なものに根付いていると いえるでしょう。すべてのデジタル資産から、適時、関連性の高いパフォーマンスに関する洞察を得ることで、セキュリティー・チームはより効果的に脅威を回避し、リスクを軽減し、組織の収益とブランドの評判を保護、維持することができるのです。

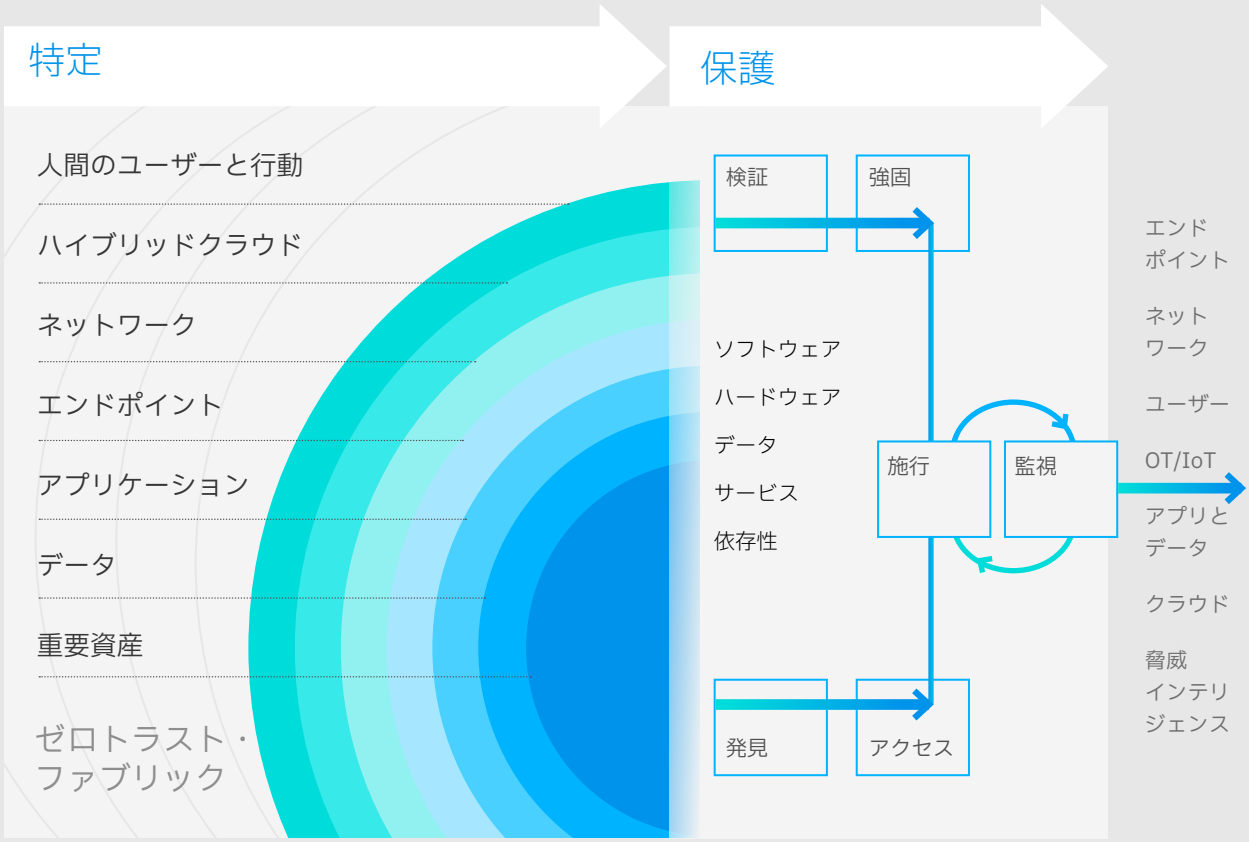
先進的な AI 導入企業は、アプリケーションの 63%、そして、エンドポイントの 55% を自動化により管理しています。

**視点**

# AI と自動化との組み合わせで、より優れたセキュリティー制御を実現

## 保護と予防

AI によるマルチクラウド環境
全体での多層監視をサポート

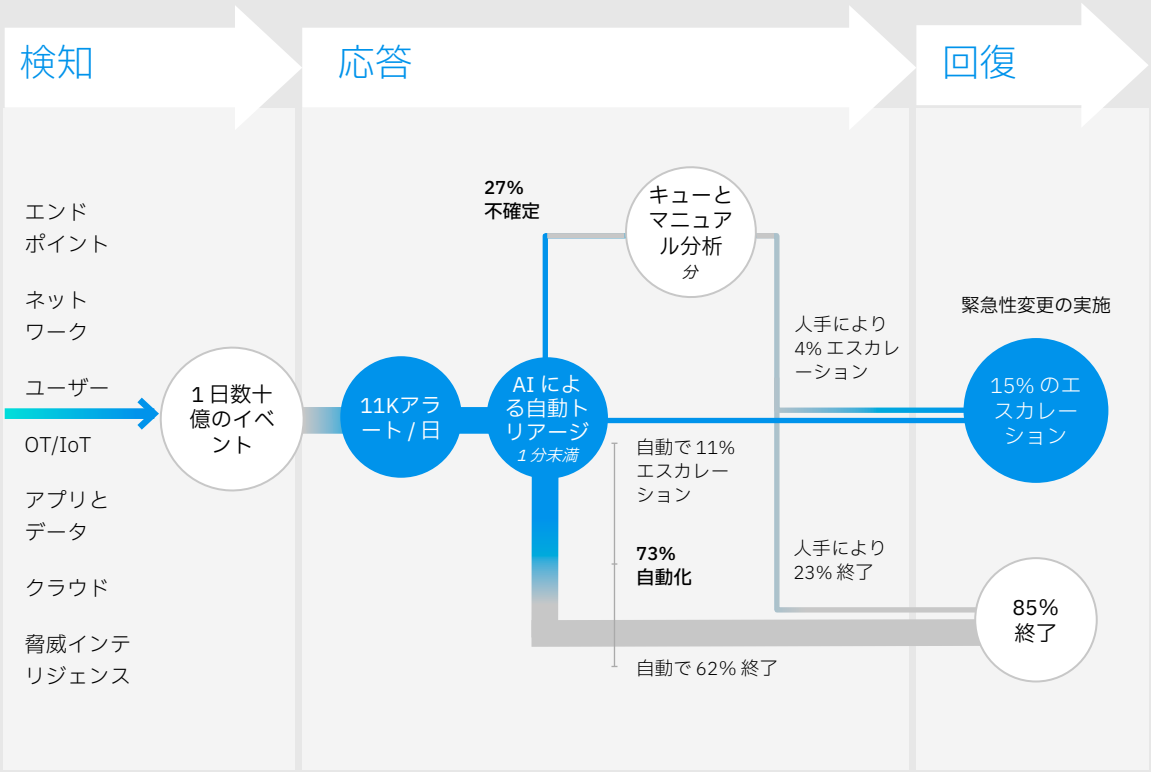


**視点**

# AIと自動化との組み合わせでセキュリティー運用のパフォーマンスが向上

## 検知と応答

AI と自動化との併用でパフォーマンス指標を圧縮可能




## 未来のアナリストの体験

**AI を使用しない場合**

8 ツール / スクリーン
19 ステップ
時間 / 日単位のレスポンス時間

**AI と自動化の場合**

1 スクリーン
6 ステップ
分単位のレスポンス時間

*出典: 集約された 2021 年の業績データの分析に基づく IBM Security Service。*
*注: 図示の業績閾値は、継続的に改善されると見込まれています。*

## 検知と応答： AI による生産性向上と迅速な回復

**課題**

ビジネスの健全性は、インシデントを防御、防止するだけでなく、いかに早くインシデントを検知し、応答し、回復できるかにかかっています。セキュリティー専門家は、ゼロトラスト・デザインの原理では、自社の組織はすでに侵入され、これからも侵入される可能性を想定するべきである、と提言しています。

検知と応答活動で AI を活用する主要な原動力となっているのは、いくつかの課題があるからだといえるでしょう。前述のように、ほとんどの組織では、デジタル・フットプリントが急速に拡大し、ビジネス・モデルがますます公開され、リモートワークの従業員が急激に増加しているため、新たなセキュリティー事象が多数発生しています。セキュリティー組織の多くは、これらすべてを人手により監視、管理し、迅速かつ効果的に対処する能力を持ち合わせていません。

サイバー人材不足により、事態は一層悪化しています。高いスキルの従業員が不足しているため、組織のセキュリティー運用体制に大きく影響しています。人材を効果的に活用して応答時間を短縮し、専門知識でセキュリティー効果の質を高める必要があります。

国立労働分析会社 (EMSI) によると、サイバーセキュリティー業務に必要な従業員は 100 人であるのに、有能な志願者は 68人しかおらず、その多くは、すでに有給雇用されているとのことです。[12] IBV の最新調査によると、企業はサイバーセキュリティーの欠員を高スキルの志願者で埋め合わせるのに、150 日要することがわかりました。[13] 第一線で活躍する新人アナリストが、効果的に仕事をこなすには、適時業務サポートが必要となるため、必ずしも人材不足が解消されているというわけではありません。彼らは業界での経験がまだ浅く、脅威の評価と調査の能力を発揮し、実際に自信と成熟度が高まるまでには時間がかかります。

AI と自動化では、ナレッジ・マネジメント、ケース・マネジメント、および運用サポート機能 (例えば、最先端のチャットボットや自然言語ナレッジ・リポジトリー) でこれらのアナリストを支援することができます。まさに画期的です： 人間の判断、および AI と自動化との組み合わせで可能になった拡張インテリジェンス機能。(視点「AI と自動化 - 人材革命」を参照)

**視点**

# AI と自動化 - 人材革命

サイバー文化に対する認識、およびサイバーセキュリティーの人材は、セキュリティーとビジネスの成果を達成する上で重要な役割を担っています。人材を無駄にしないのが、成功する AI プログラムなのです。AI により、セキュリティー・アナリストの効率性と効果性が向上し、セキュリティー・ナレッジ・ワーカーの活躍の場が広がります。AI により、より柔軟なエンゲージメント・モデルの扉が開かれることで、セキュリティー効果の良し悪しを決定付ける要因となる人材やスキルの制約を緩和することができます。[14]

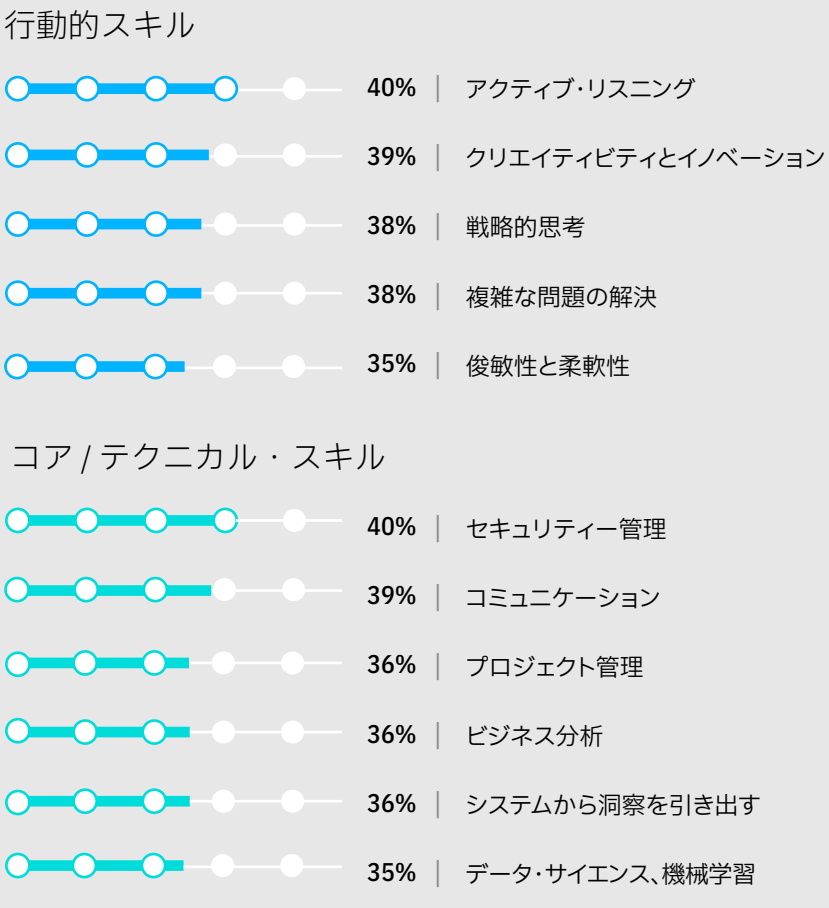
AI 導入企業では、新たな人材への需要が急増しています。ここ 12ヶ月の間、サイバーセキュリティーの従業員が 15% 増加しています。このうちの 40% は、セキュリティー AI の導入によるものだとされています。回答者の話によると、セキュリティー関連職種の 34% でスキル要件が変わってきており、そのうちの 35% は、AI の導入が直接的または間接的な要因となっているとのことです。

AI 導入企業は、サイバーセキュリティー人材に再投資し、人的要因とテクノロジーとを組み合わせることで、人材の足りない部分を直接的に補うことができます。コストの最適化ではなく、専門性の向上、職場環境の改善、従業員のスキルアップに自動化を活用することで、人材を積極的に成長させることができます。

AI 導入企業は、従業員の行動スキルと技術スキルとの組み合わせを優先しています。行動面では、AI 導入により、40% の従業員が、最も必要とされるスキルは、アクティブ・リスニングであるとしています。39% の従業員が、イノベーションと独創性であると挙げています。技術面では、40% の従業員がセキュリティー管理能力を最も重要視している一方、39% の従業員がコミュニケーション能力を重視しています(図参照)。このようにソフト・スキルとハード・スキルを柔軟に融合させることが、AI の新たな価値提案であり、最も有力な分野の一つとなります。

**AI により求められるスキル・ミックス**

サイバーセキュリティーの従業員が AI で成功するには、ハード面とソフト面の両方のスキルが必要です




*Q. AI の導入によって、貴社のサイバーセキュリティー業務の担当者が身につけたり、高めるべきスキルには、どういったものがありますか？*

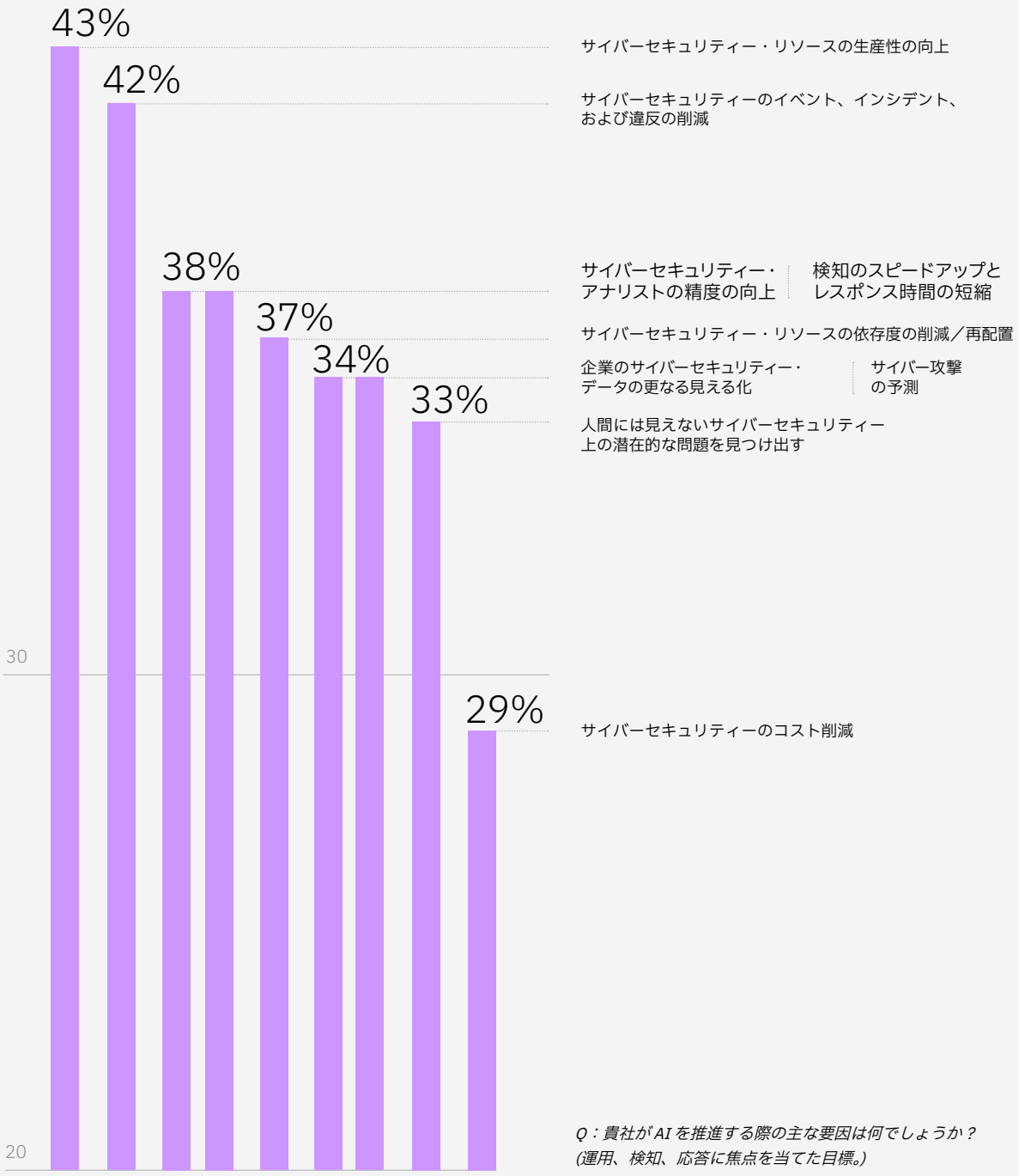
人材不足に対処するため、企業は AI と自動化とを導入し、今まで先延ばしになっていた人材の生産性と業務経験の向上に取り組んでいます。実際、43% の企業が、AI を利用する一番の理由として、サイバー人材の生産性を高めることを挙げています。セキュリティー・イベント、インシデント、侵害の削減を掲げる企業が 42%、がサイバーセキュリティー・アナリストの精度向上のために AI を活用している企業が 38% という結果が出ています (図 7 参照) 。

全体として考えれば、AI と自動化の導入は、膨大な量とペースのセキュリティー・イベントに対応しなければならない、セキュリティー・アナリストの職場環境を劇的に改善させ、プラスの影響を与える重要な要素となります。注意を要する脅威についてもっと理解すれば、アナリストは日常的なトリアージではなく、より価値の高い脅威の調査業務に集中することができます。最終的な成果： サイバーセキュリティーの人材全体の能力と専門性の双方を向上させることができます。

図 7

## 生産性をアップ

AI 導入企業は、アナリストの検知と応答の効率を向上させることを目指しています




*Q：貴社が AI を推進する際の主な要因は何でしょうか？(運用、検知、応答に焦点を当てた目標。)*

## AI の価値提案

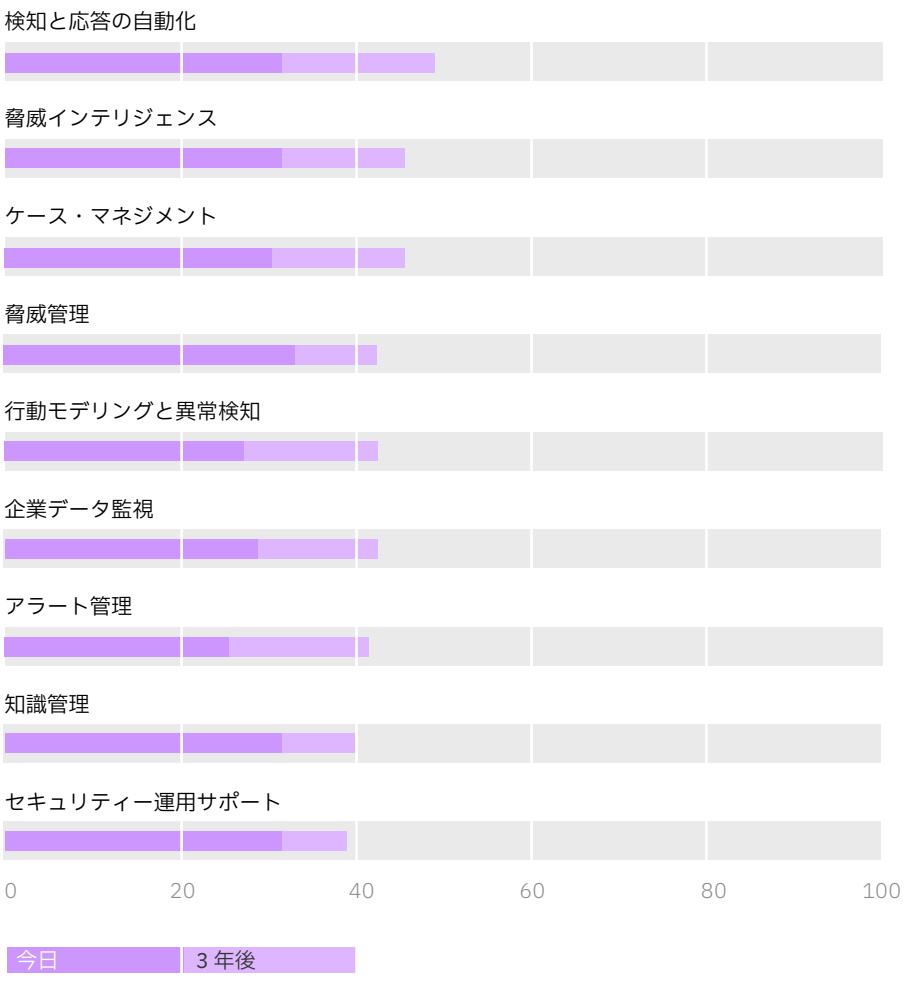
生産性を向上させる秘訣は、テクノロジーをうまく活用し、労働力をサポートすることです。例えば、理想的なのは、AI と自動化により脅威を検知することです。これにより、人手を減らし、効率性を高めることができます。自動化された AI 主導の調査プロセスにより、高価値のデータや資産、ネットワーク・セグメント、およびクラウド・サービスを選択的に保護することができます。ネットワーク通信、トラフィック、およびエンドポイント・デバイスの可視性を高めることで、AI と自動化により潜在的脅威の検知能力が高まり、サイバーセキュリティー担当者は、情報に基づいて、より正確に、一貫した判断を下すことが可能になります。

AI 導入企業は、脅威管理に AI と自動化を活用することの有望性を認識しています。企業の 34% は、AI 導入が検知と応答活動の一番の活用事例であると回答しています (図 8 参照)。自動検知と自動応答がこれに続き、49% が 3 年以内に最も広く導入されるという結果が出ています。また、保護と予防の使用事例と同様に、AI 導入企業は今後 3 年以内に、検知と応答に AI を活用する事例が平均約 40% 増加すると見込んでいます。(視点「AI による検知と応答の迅速化」参照)。

図 8

**検知と応答に AI を適用**

AI 導入企業は、AI で脅威を迅速に特定し、サイバー攻撃に対して先を見越した対応をしています




*Q. 現状、AI による自動化はどのような用途で実施されていますか？ 更に、3 年後は？ (検知と応答に重点を置いたユースケース)。*

# AI で検知と応答をスピード･アップ

AI 導入企業が、複数の主要業績評価指標により測定すると、AI と自動化を併用したことで、サイバーセキュリティー人材の生産性が大幅に向上したという結果が出ています。5 つの使用事例で、その方法をご紹介します。

**検知と応答の自動化。**セキュリティーの AI と自動化は、数百、更には、数千の制御点からのデータの収集、統合、分析を自動化し、システム・ログ、ネットワーク・フロー、エンドポイント・データ、クラウド API コール、ユーザー行動を総合的に判断します。脅威管理およびアラート優先順位付けと合わせて、組織は既存のテレメトリー・ソリューションをエンドポイント検出と応答(EDR)、およびクロスレイヤー検知と応答 (XDR) 機能を強化することができます。これにより、セキュリティー運用チームは、セキュリティー例外の状況をすぐに理解し、優先順位を決め、影響力の大きい脅威の調査に十分な人材を割り当てることができます。

**脅威インテリジェンス。**企業は、AI によるセキュリティー・インテリジェンスにより、ライブ・データ・ストリームを分析して、異常な行動をリアルタイムで検知することができます。内部テレメトリー信号と外部情報源とを統合し、セキュリティー情報をドメインに組み込むことで、実用的な情報を現実的な時間で提供します。さらには、脅威発生に関連するセキュリティー・ポリシーの有効性を改善させることもできます。また、クラウド環境全体に同じ手順を適用することでログ取得機能を拡充し、ゼロ・デイや高度標的型攻撃 (advanced persistent threats：APT) といった、より見つけにくい攻撃の兆候を示す不規則な構成をスキャンすることも可能です。

**ケース・マネジメント。**セキュリティー・ケース・マネジメント機能により、セキュリティー・チームは不審な行動に関する情報を収集し、ケースに関連する詳細な情報やログで調査を進めることができます。AI を使用して、データ処理の量とスピードを上げ、データ・サイエンス技術を統合し、文書内のデータの自動識別と分類を可能にします。状況を理解する AI により、事前に分類することなく、トピックごとにデータをグループ化することができるので、セキュリティー・チームは、関連があると認められたデータで推論を行い、見た目にはわからない類似性を見出すことができます。

**脅威管理。**AI の導入により、アナリストは最も重要なアラートに最初に焦点を当て、効果的に選別し、偽陰性と偽陽性とを見分けることができます。また、重要なインシデントを見落とす可能性を大幅に削減することもできます。また、AI では、攻撃シグネチャー、セキュリティー侵害インジケーター (IOC)、および振る舞いの痕跡 (IOB) に基づき、脅威を分類し、優先順位をつけて、アラートを出すこともできます。

**行動モデリングと異常検知。**自動化された AI セキュリティー・モデルでは、異常な動作を認識し、脆弱性を動的に評価し、異常な動作をフラグ付けすることができます。これらはすべて、セキュリティー侵害インジケーターとなりうるものです。次に、機械学習により、状況変数、過去の事例、または脅威の情報源といった、幅広い要因に基づいて改善策を提案し、次に、特定の制御点でポリシー管理を更新します。

AI 導入企業は、インシデントの検知と応答にかかる時間の短縮に成功したと報告しています (図 9 参照) 。AI 導入企業は、AI 導入前のパフォーマンス推定値と比較すると、インシデント検知にかかる日数の中央値が 12% 減少し、インシデントに対する応答と回復にかかる日数の中央値が 11% 減少したと、報告しています。優れた企業の例を見れば、AI と自動化が大幅な改善を実現する本当のきっかけとなったことがわかるでしょう。AI 導入企業の上位 25% は、AI でインシデントの調査時間を約 3 分の 1 に、応答と回復にかかる時間を約 4 分の 1 まで短縮したと報告しています。また、滞留時間も 45% 短縮されました。

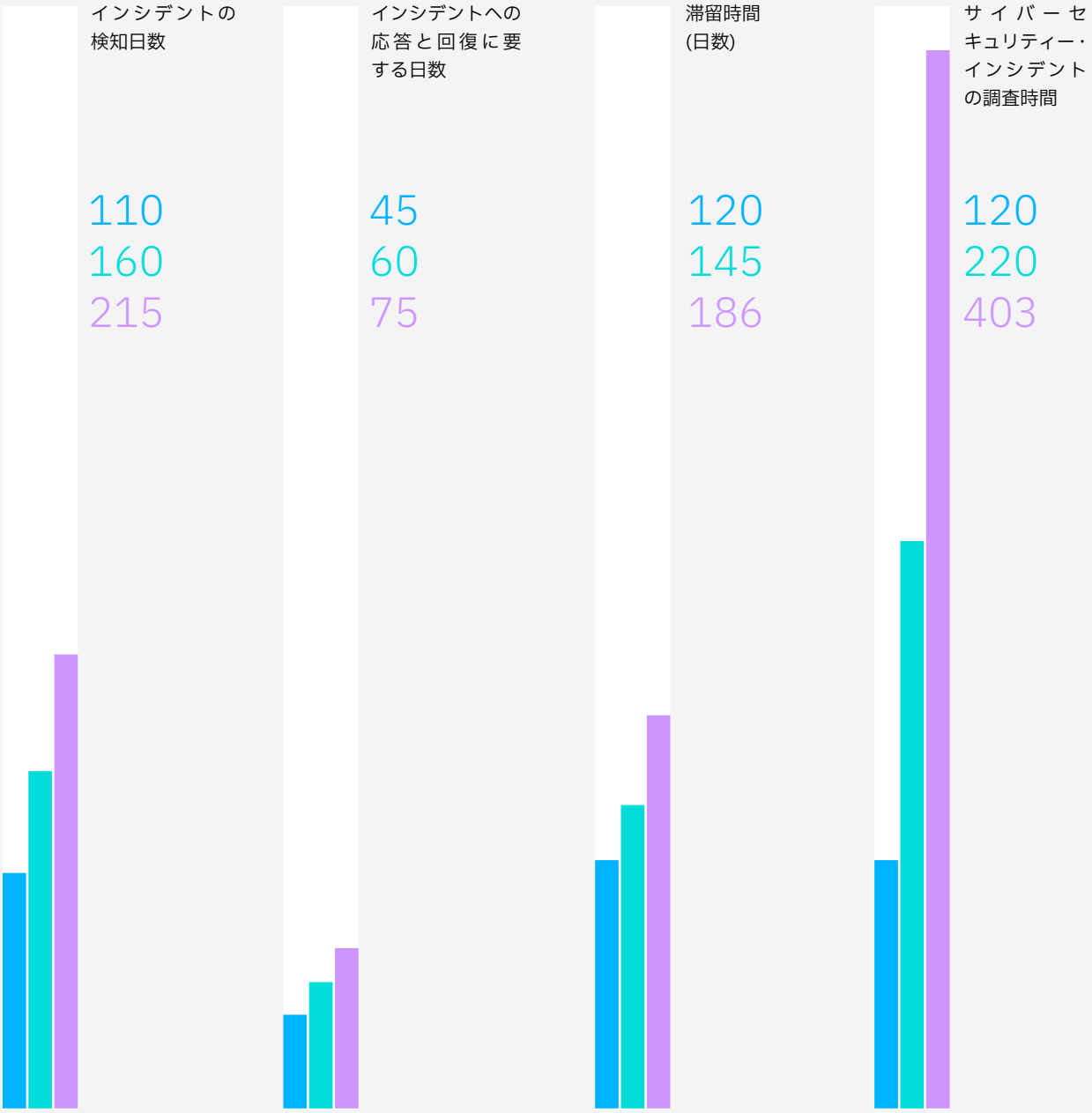
AI 導入企業は、セキュリティー運用のライフサイクルに AI と自動化を導入することで、検知と応答のパフォーマンスが向上し、保護と予防の能力も向上していることが明らかになっています。これら企業の成功を見ると、AI を利用することで、サイバー攻撃に遭った時に時に、総合的なサイバー耐性を大幅に強化できる可能性があることが分かります。(導入事例「AI と自動化 - より良い労働環境、より良いパフォーマンスに向けて」を参照)。

AI 導入で優れた成果を上げた企業は、サイバーセキュリティー・インシデントの調査時間を約 30% 短縮しました。

図 9

## 回復のスピードアップ

優れた企業は、セキュリティー・インシデントの検知と応答に要する時間が大幅に短縮されています。




AI 導入企業の上位 25%

AI 導入企業の中位層

AI 導入企業の下位 25% 層

*グラフの長さが短いほど、パフォーマンスが高いことを示しています*

**お客様事例**

# グローバル・マネージド・セキュリティー・サービス・プロバイダー

**AI と自動化 - より良い労働環境、より良いパフォーマンスに向けて**

あらゆる業界の何百ものグローバルな顧客にサービスを提供しているマネージド・セキュリティー・サービス・プロバイダーは、ハイブリッド型クラウドとゼロトラスト機能でセキュリティー運用を刷新したにもかかわらず、容量の問題に何度も直面していました。「攻撃対象は大きくなる一方だ」と、同社の主任セキュリティー・アナリストの一人は述べていました。「我々は両極端の問題に直面しています。つまり、さまざまな情報源からの情報が多すぎるか、最も重要な時に適切な情報がまったくないか、のどちらかなのです。」

さらに厄介なことに、技術や専門性も不足していたのです。「貴重な人材を獲得するために、少しでも優位に立ちたいと考えています」と、リード・クライアントの幹部は語っていました。クライアントのリーダーは、デザイン思考と IBM Garage™ との連携による手法を用い、ビジネス実績を見据えてチャンスを作り上げることから始めました。「アナリストがより働きやすい環境を作りたかったのです。また、自動化を進めることで、チームのパフォーマンスがどう改善されるのかにも興味がありました」と、クライアント企業の幹部は語っています。

開発と運用の統合チームは、以下の 4 つの主要な目標を立てました。

– アナリストのノイズを削減して、価値の高いアラートに集中できるようにする
– コンテキスト・データ、メタデータ、およびサービス・ログを集計し、脅威環境を正確に再現することでトリアージ時間を短縮する
– コンテキストを増やし、データ / メタデータを充実させることにより調査スピードをアップする
– 説明と理由付けにより、ピンポイントの提案事項を強化する

約 1 年後、顧客は業務効率を格段に向上させることができました。

– 信頼度 90% 以上のレベルで、アラート選別の自動化が 40% から 73% まで向上
– ワークロードに特化したゼロトラスト制御により、攻撃対象および関連リスクを推定 50% まで削減
– 攻撃者の滞留時間や脆弱性の幅を 50% 削減
– セキュリティー・インシデントを 75% まで削減し、平均侵入時間性能が倍増

AI により自動化が促進されることで、ソリューションを活用する人間の問題にも大きく、強力な力で影響すると言えるでしょう。AI と自動化とを組み合わせることで、アナリストはゼロデイ、APT 検知、脅威ハンティング、犯罪科学など、より影響力の大きい脅威の検出に集中できるようになります。セキュリティー・アナリストから絶えずフィードバックが提供されるため、ソリューションはより賢く、そして、より人に優しく機能するようになります。クライアントの幹部は、ビジネスへの影響を統括しています：「私たちチームにとって、より良い作業環境にするために自動化を組み合わせることで、状況が一変しました。」

第 3 章

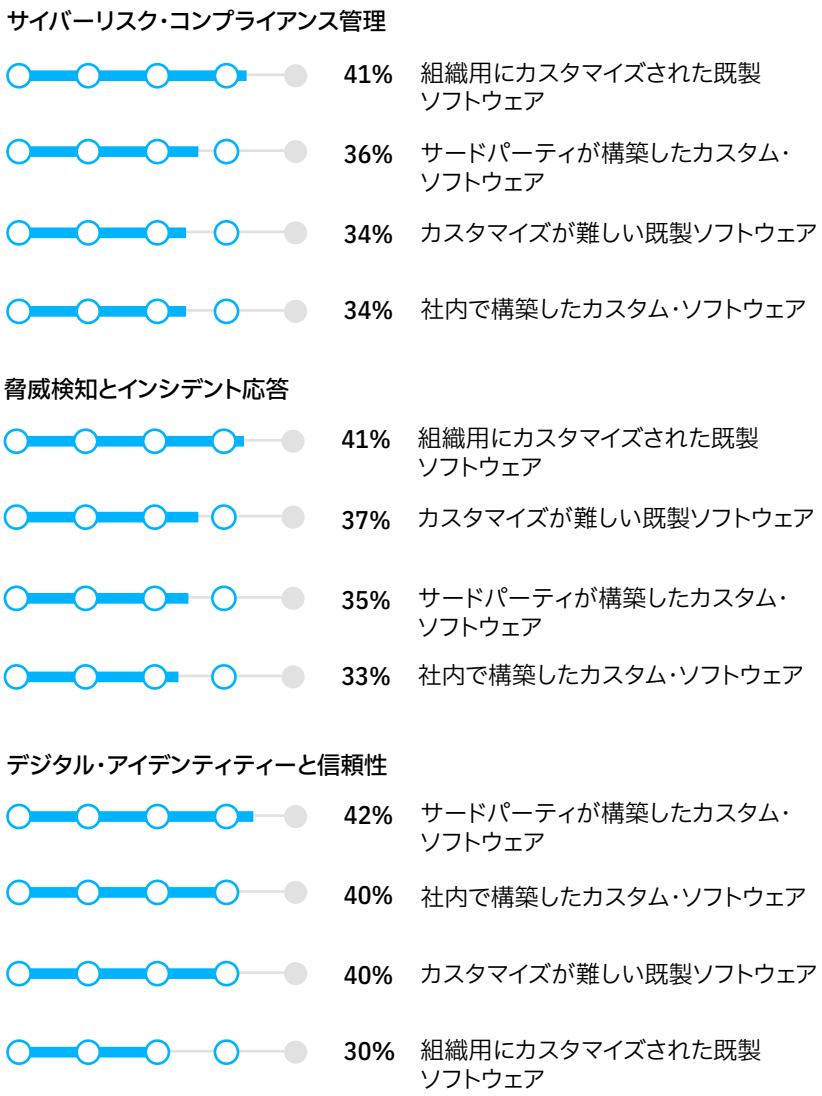
# セキュリティー AI 導入のロードマップを計画

AI による洞察と自動化をセキュリティー運用に組み込むことを検討する際、どのようにすれば展開に成功するのかを考えてみましょう。AI 導入企業は、既製のソリューションと自社開発のツールを併用しています。サイバー・リスクとコンプライアンス、並びに、脅威検知とインシデント応答については、構成可能な市販のソフトウェアの導入が最も成功した形態である、と多くの AI 導入企業が報告しています (図 10 を参照)。しかし、デジタル・アイデンティティーと信頼性管理については、自社またはサードパーティー企業が構築したカスタム・ソフトウェアがより成功につながったと述べています。

図 10

**セキュリティー AI の実現**

最も成功したデプロイメントでは、ほとんどの場合、何らかの形でカスタマイズが実施されています。




*Q. AI テクノロジーをサイバーリスクとコンプライアンス管理に導入することについて、貴社ではどのようにお考えでしょうか。(上位 3 つを選択)*

*Q. AI テクノロジーを脅威検知とインシデント応答管理に導入することについて、貴社ではどのようにお考えでしょうか? (上位 3 つを選択)*

*Q. AI テクノロジーをデジタル・アイデンティティーと信頼性の管理に導入することについて、貴社ではどのようにお考えでしょうか? (上位 3 つを選択)*

高度な構成を行い、独自開発したセキュリティー・ソリューションは、性能が高く、得られるメリットも大きくなりますが、開発とサポートに関わる継続的なコストを、セキュリティー運用の予算に組み込まれなければなりません。

特殊な AI セキュリティー・アプリケーションの恩恵を受けている業界 (銀行や金融市場など) もあるでしょうが、特に、保守や脆弱性管理については、継続的なサポート費用、スタッフの要件、パッチ・スケジュールなどを慎重に検討する必要があります。ソリューションをカスタマイズする際には、説得力のあるビジネス上の根拠を反映させ、組織の展開するリスク態勢と潜在的なセキュリティー脆弱性に基づいて判断しなければなりません。

カスタム AI ソリューションでは、継続的にかかるサポート・コストについて考慮する必要があります。

# アクション・ガイド

**セキュリティーに AI と自動化を活用して、ビジネスの価値を生み出す**

最も成功したセキュリティー組織であっても、まだ未熟な部分があります。常に変化する業務の性質や絶え間なく生じる新たな脅威ベクトルに対応するには、準備とレジリエンスを優先させる必要があります。貴社の組織が侵害されるかどうかではなく、いつ、どの程度まで侵害されるのかが問題なのです。

それと同時に、AI モデルには常に学習させる必要があり、貴社のセキュリティ・チームは、新たなパフォーマンスに関する洞察を継続的に伝えなければならないことを理解しておく必要があります。このように絶えず学び続ける姿勢こそが、実現と成功を左右するのです。

AI 導入企業では、セキュリティー・パフォーマンスが、経営効率とビジネス価値の双方に大きく影響を与えます。一方で、セキュリティー・パフォーマンスが強化されると、適応力のあるセキュリティー分析環境を作り出すことができます。つまり、これらの要因は、組織全体のサイバー・レジリエンスに大きな影響を与える可能性があるということです。

このような機能を初めて試験的に導入する場合や、既存アプリケーションの機能を拡張する場合などは、以下の 3 つの推奨事項を参考にしてください。

## 01

### 主要なセキュリティー指標に基づく貴社の業績のベンチマーク

セキュリティー改善の推進要因を特定

- AI と自動化機能をセキュリティー運用で導入するために急務となる戦略的根拠を理解した上で、サイバー・リスクとサイバーセキュリティ戦略を更新して、この優先順位の変更を反映させます。サイバーセキュリティー・インシデントやデータ侵害を減らすためなのか、それとも業務効率化に向けたコスト削減のためなのか。もしかしたら、顧客、従業員、パートナーとの信頼関係を向上させるためなのでしょうか。

ベンチマーク比較による改善箇所の絞り込み

- 保護と予防、並びに、検知と応答に関する主要なリスクとセキュリティー・メトリクスを検証し、貴社の業績を同業他社と比較することができます。ギャップとは、AI と自動化が最も役立つ分野を目標に、改善の取り組みに注力できる分野を表しています。
- 比較を行うために、公式なベンチマーク・サービスを提供している組織もあります。あるいは、Ponemon Institute社、Gartner社、Forrester社、IDC、SANS Institute社、Cloud Security Alliance (CSA) などのオンライン・ソースにも、セキュリティー・メトリクスを活用することもできます。

## 02

### 価値を最大限に高め、最上位のセキュリティー目標に沿ったセキュリティーの改善を優先する

影響に基づく優先順位を設定し、主要業績評価測度における改善を目標とする

- 貴社の各主要業績評価指標のパフォーマンスを向上させることで実現できる潜在的メリットを評価する。これにより、コスト、効率、品質、および時間といった業務上の要因の観点から、どの分野で最大の価値を提供できるかが見えるようになります。候補とされる分野が貴社のセキュリティー戦略と合致しているとすれば、その対策は戦略目標の達成に最も貢献するはずです。

パフォーマンスを向上させる可能性が高い AI アプリケーションを特定する

- 保護と予防、並びに、検知と応答に最も密に関連するパフォーマンス指標について理解します。例えば、保護と予防の場合、自動化されたアイデンティティーまたはエンドポイント管理で管理されるアプリケーションとエンドポイントの数が重要な尺度となります。検知と応答では、滞留時間が重要なメトリックとなります。
- 両分野のうちパフォーマンス向上をもたらす可能性が最も高い AI アプリケーション、および最も重要であると判断されたビジネス上のメリットについて検討します。これらの優先順位を活用して、貴社組織のセキュリティー AI 、および自動化ロードマップを定義します。自らの強みを把握し、パートナーを活用して、自身の専門性を高められる分野を特定します。最後に、既存のソリューションを構成する場合でも、専用ソリューションを開発する場合でも、最も成功しやすい AI 導入モデルを選択し、更に、開発とサポートをどの程度までサードパーティに任せるかを選択します。

## 03

### セキュリティー向上施策用の主要な実現要素の構築

セキュリティー AI 戦略とそれに対応する運用計画の策定

- 組織の広範なサイバーリスクおよびセキュリティー戦略に沿った、AI アプリケーションの実装、管理、統制。これらが運用方針、統制、およびプロセスに反映されていることを確認する。

組織が成功する上で必要な行動力と技術力を見極め、展開する

- 自動化がサイバーセキュリティー人材に与える影響について検討する。自動化を脅威と捉えるか、それともチャンスと捉えるか。このやりとりでは、どのような関わり方が正しいのでしょうか。
- セキュリティー AI と自動化が成功する要因について考える場合、職場環境、専門性や専門知識の必要性、および、関連するスキルアップや再教育といった、成長と持続の要素を考慮する必要があります。AI プラスアルファの自動化環境では、どのようなスキルが必要とされるでしょうか。
- AI と自動化により、サイバーセキュリティー人材に最大のメリットをもたらすことができる分野を特定します。必要とされる行動スキルと技能スキルを構築、強化するために、ギャップを特定し、職務に応じたトレーニングを提供します。現実的、実践的な経験を提供し、社内外の人材パートナー・サービスを活用し、経験学習やサイバーセキュリティー・シミュレーションなどで人材のスキルアップを図る必要があります。
- 最後に、ご自身の進捗状況を確認します。新しい AI アプリケーションや機能を導入する際には、実際のパフォーマンスを目標ベンチマークと突き合わせて検証し、さまざまな投資に関する相対的な効率性を判断します。

# 概要

## 著者


*スリザール・マッピディ*

最高技術責任者
IBM Security
linkedin.com/in/smuppidi
muppidi@us.ibm.com/jp-ja

スリザールは、IBM フェローであり、IBM Security の CTO です。彼は、製品、およびサービスの IBM セキュリティー・ポートフォリオの技術戦略、アーキテクチャー、および研究の主導を担当し、脅威への防御の管理、デジタル資産の保護について、顧客の対応にあたっています。セキュリティー製品の構築、顧客へのソリューション・アーキテクチャーの提供、公開標準の推進、および技術チームのリーダーとして 25 年の経験を持つ、結果主義の技術ソート・リーダーです。

*リサ・フィッシャー*

グローバル・ベンチマーク・リサーチ リーダー, IT、セキュリティ、クラウド
IBM Institute for Business Value の中東・アフリカ地域担当リーダー
linkedin.com/in/lisa-giane-fisher
lfisher@za.ibm.com/jp-ja

リサは、業界と地域を問わず、サイバーリスクとサイバーセキュリティーの観点からテクノロジーがビジネスに与える影響を予測し、それを明確にするベンチマーク調査の作成を担当しています。リサは南アフリカを拠点に活動しています。

*ジェラルド・パラム*

グローバル・リサーチ・リーダー-セキュリティー & CIO
IBM Institute for Business Value
linkedin.com/in/gerryparham/
gparham@us.ibm.com/jp-ja

ジェラルドは、IBM Institute for Business Value のセキュリティーと CIO の研究分野を統括しています。サイバー戦略、諮問委員会、およびエコシステム・レベルのセキュリティー、とりわけ、戦略、リスク、オープン・セキュリティー、信頼性、およびビジネス価値の関係に力を入れています。彼は、経営幹部のリーダー、イノベーション、および知的財産開発において、20 年以上の経験があります。

## Benchmark Insights について

Benchmark Insights は、経営者向けの重要なビジネス、および関連するテクノロジーの話題に関する洞察を特集したものです。これらは、業績データの分析、およびその他のベンチマーク指標に基づいています。詳細については、以下の IBM Institute for Business Value までお問い合わせください global.benchmarking@us.ibm.com/jp-ja.

## IBM Institute for Business Value

IBM Institute for Business Value は、20 年にわたり、IBM のソート・リーダーシップ・シンクタンクとして、その役割を果たしてきました。私たちを突き動かすのは、リーダーがより的確なビジネス上の意思決定を行えるような、研究に裏付けられ、技術に則した戦略的な洞察を生み出す製品です。

ビジネス、テクノロジー、社会との接点という当社独自の見地から、毎年、何千人もの経営者、消費者、専門家による調査、インタビュー、交流を実施しています。そして、信頼性が高く、刺激的で、かつ実行可能な洞察として、彼らの視点を総合的に取り入れています。

常につながり、情報を得るには、以下にサインアップして、IBVのメール・マガジンをご覧ください。ibm.com/jp-ja/ibv. 以下の Twitter をフォローすることもできます @IBMIBV あるいは、以下の LinkedIn で検索してください https://ibm.co/ibv-linkedin

## 変わりゆく世界にふさわしいパートナー

IBM では、お客様とのコラボレーションを通じて、ビジネスの洞察、最先端のリサーチ、およびテクノロジーを集結させ、めまぐるしく変化する昨今の環境において、お客様に圧倒的な競争力を提供します。

## 関連レポート

**ゼロトラスト・セキュリティーを始める**

クリス・マッカーディ、シュー・ジェーン・トンプソン、リサ・フィッシャー、およびジェラルド・パーハム。「ゼロトラスト・セキュリティーを始める。」IBM Institute for Business Value 2021 年 7 月ibm.co/zero-trust-security

**クラウド・セキュリティーの新時代**

シュージェーン・トンプソン、シャムラ・ナイドゥ、ショーン・ドゥザ、およびジェラルド・パーハム。「クラウド・セキュリティーの新時代： 信頼ネットワークによるサイバー・レジリエンスの強化」 IBM Institute for Business Value 2021 年 4 月ibm.co/cloud-security-cyber-resilience

**AI 倫理の取り組み**

「AI 倫理の取り組み： 信頼に値する AI を進展させるための企業向けガイド。」 IBM Institute for Business Value 2022 年 4 月。ibm.co/ai-ethics-action

## 研究と調査方法

IBM Institute for Business Value は、APQC (米国生産性品質センター) と提携し、自社組織における IT および運用技術 (OT) サイバーセキュリティーと情報セキュリティーの全責任を負う1,000人の経営者を対象にアンケートを実施しました。銀行金融市場、電子機器・ソフトウェア、政府、保険、メディア・エンターテインメント、小売、およびサービスなど、16 業界の代表者に回答していただきました。回答者は、以下の世界 5 地域に点在しています：アフリカ・中東、アジア太平洋、中南米、欧州、米国・カナダ。セキュリティー機能のプロセスに AI を活用していない企業も含まれます。

回答者には、自社のサイバーリスクとサイバーセキュリティーのプロセス、並びに、セキュリティー機能のパフォーマンスにおいて、現状および計画中の AI の活用に関する情報を提供していただくよう、お願いしました。多くの要因がパフォーマンスに影響するので、AI 導入企業、ここでは、少なくとも 1 つのセキュリティー・プロセスで AI を試験的に導入、実装、運用、または最適化している 637 社に対して、AI が一般的なサイバーリスクとセキュリティー機能 KPI のパフォーマンスにどう影響したか、独自の推定値を提示していただきました。それらのデータをもとに、各 KPI のパフォーマンスの範囲と、AI が各 KPI に与えた影響の範囲を算出することができました。

本レポートにおける KPI は、以下のように定義されています：

**滞留時間** とは、侵入 / 侵害が成功してからこれを発見 / 検知されるまでの時間のことです。

**サイバーセキュリティー・インシデントへの応答と回復に要する平均時間 (暦日)** は、インシデントが検知され、その範囲が確定した時点から始まります。脅威を取り除き、被害を受けたシステムをインシデント前の状態に戻すための活動、つまり、被害を受けたシステムのテスト、監視、検証、そして業務回復が含まれます。

**サイバーセキュリティー・インシデントの調査に要する平均時間 (単位：時間)** は、セキュリティー・アラートが調査用にエスカレーションされてから調査が完了するまでの時間です。

**IT コスト** に占めるサイバーセキュリティー・コストには、アプリケーション、クラウドおよびデータセキュリティー、アイデンティティー・アクセス管理、インフラストラクチャー保護、統合リスク管理、ネットワーク・セキュリティー機器、他の情報セキュリティー・ソフトウェア、セキュリティー・サービス、およびコンシューマー向けセキュリティー・ソフトウェアに関連する IT コストが含まれます。企業運営を支えるプロセスにかかるすべての費用を含み、減価償却費 / 償却費 (つまり、キャッシュ・フローに基づく)、および「転売された IT」は除きます。

**セキュリティー投資収益率 (ROSI)** はパーセンテージで表され、{[推定損失総額 (米ドル) ×サイバーセキュリティーの総コスト (サイバーセキュリティー・ソリューション (複数) 、または努力で軽減された割合)]、つまり、サイバーセキュリティーの総コスト (サイバーセキュリティー・ソリューション (複数) または努力の総コスト)} / サイバーセキュリティーの総コスト (サイバーセキュリティー・ソリューション（複数）、または努力の総コスト)、に相当します。

**データ侵害** コストには、検知、エスカレーション、通知、およびデータ侵害後の応答活動で発生した直接および間接的な費用が含まれます。情報漏えいの平均コストは、以下の通りです：(年間の侵害件数にすべてのコスト要因を乗じたもの) / (年間の侵害件数)。

本レポートで使用されるパフォーマンス範囲は、以下のように定義されています：

トップ・パフォーマーとは、各メトリックについて 75 パーセンタイル、または 25 パーセンタイルで業績を上げている AI 導入企業のことです。特定の測定値について、値を高くしたり、低くする場合により、そのデータは異なります。ある特定のメトリクスでは、値が高い方が良いとされる場合、トップ・パフォーマー、つまり、AI 導入企業の上位 25% は、75 パーセンタイルで業績を上げている組織ということになります。75% の回答者がこのレベル未満であり、25% の回答者がこのレベル以上となります。値が低い方が良い場合、トップ・パフォーマーは 25 パーセンタイルで業績を上げている AI 導入企業ということになります。回答者の 25% がこのレベル以下、75% がこのレベルよりも高いパフォーマンスということになります。中央値とは、回答分布の中間値であり、つまり、半数の回答者がこの値未満であり、もう半数がこの値よりも高いということです。

# 謝辞

IBV は、セキュリティー・ライフサイクルにおける新技術と応用イノベーションの影響について研究している、IBM Researchの優秀なセキュリティー研究者チームに感謝したいと思います。このチームは、J.R.Rao、Marc Stoecklin、および Ian Molloy のメンバーで構成されています。また、重要テーマを明らかにする上で、快くその専門知識を教えていただいた、Srini Tummalapenta 氏と Charles Henderson 氏にも感謝いたします。本レポートは、これらの同僚の惜しみない協力なしには、実現することはできませんでした。

IBM Security のグローバル・セキュリティー専門家チームを率いる、Mary O'Brien と Chris McCurdy の両氏に感謝の意を表します。何百社ものグローバル・クライアントと関わってきた IBM Security の同僚たちから、実体験に基づいた貴重なアドバイスをいただきました。彼らの研究は、私たちのさまざまな研究に欠かせない基板となっています。

最後になりますが、この資料作成に協力してくれた IBV の仲間に感謝申し上げたいと思います。そのメンバーは、Dave Zaharchuk、Kirsten Palmer、Heba Nashaat、Sherihan Sherif、Joanna Wilkins、Angela Finley、および Kathy Cloyd です。IBV は毎週、一次調査に基づく新しいソート・リーダーシップ・レポートを出しています。各レポートは、研究、分析、およびクリエイティブの専門家からなる多彩なチームの尽力によるものであり、彼らが協力し合って、これらの資料を形にしています。

# 注記および出典


1 Turton, William, and Kartikay Mehrota. “Hackers Breached Colonial Pipeline Using Compromised Password.” Bloomberg. June 4, 2021. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password; Holmes, Aaron; “Ransomeware gangs targeted 3 different US water treatment plants this year in previously unreported attacks, according to federal agencies.” Insider. October 16, 2021. https://www.businessinsider.com/3-us-water-treatment-plants-attacked-by-ransomware-gangs-report-2021-10

2 Vigliarolo, Brandon. “Report: Pretty much every type of cyberattack increased in 2021.” TechRepublic. February 17, 2022. https://www.techrepublic.com/article/report-pretty-much-every-type-of-cyberattack-increased-in-2021/; 2022 IBM X-Force Threat Intelligence Index.” IBM Security. February 2022. ibm.com/jp-ja/security/data-breach/threat-intelligence/

3 “SolarWinds hack was ‘largest and most sophisticated attack’ ever: Microsoft president.” Reuters. February 14, 2021. https://www.reuters.com/article/us-cyber-solarwinds-microsoft/solarwinds-hack-was-largest-and-most-sophisticated-attack-ever-microsoft-president-idUSKBN2AF03R; Robertson, Paul. “Best of 2021—Worldwide Hack: Microsoft Exchange Server Zero-Day Exploits.” Security Boulevard. December 27, 2021. https://securityboulevard.com/2021/12/worldwide-hack-microsoft-exchange-server-zero-day-exploits/; Torres-Arias, Santiago. “What is Log4j? A cybersecurity expert explains the latest internet vulnerability, how bad it is and what’s at stake.” The Conversation. https://theconversation.com/what-is-log4j-a-cybersecurity-expert-explains-the-latest-internet-vulnerability-how-bad-it-is-and-whats-at-stake-173896

4 “The 2021 CIO Study. The CIO Revolution: Breaking barriers, creating value.” IBM Institute for Business Value. November 2021. ibm.co/c-suite-study-cio

5 Schneier, Bruce. “The Coming AI Hackers.” Harvard Kennedy School, Belfer Center for Science and International Affairs. April 2021. https://www.belfercenter.org/publication/coming-ai-hackers

6 “AI & Cybersecurity: Balancing Innovation, Execution & Risk.” Pillsbury Law and The Economist Intelligence Unit. September 9, 2021. https://www.pillsburylaw.com/en/news-and-insights/ai-and-cybersecurity-balancing-innovation-execution-and-risk.html

7 Morgan, Steve. “Cybercrime to Cost the World $10.5 Trillion Annually by 2025.” Cybercrime Magazine. November 13, 2020. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

8 “Cost of a Data Breach Report 2021.” IBM Security and the Ponemon Institute. July 2021. ibm.co/security/data-breach. “Identity Theft Resource Center’s 2021 Annual Data Breach Report Sets New Record for Number of Compromises.” Identity Theft Resource Center. January 24, 2002. https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/

9 “Cost of a Data Breach Report 2021.” IBM Security and the Ponemon Institute. July 2021. ibm.com/jp-ja/security/data-breach

10 McCurdy, Chris, Shue-Jane Thompson, Lisa Fisher, and Gerald Parham. “Getting started with zero trust security: A guide for building cyber resilience.” IBM Institute for Business Value. July 2021. ibm.co/zero-trust-security

11 “2022 IBM X-Force Threat Intelligence Index.” IBM Security. February 2022. ibm.com/jp-ja/security/data-breach/threat-intelligence/

12 Hatton, Tim. “The Cybersecurity Talent Shortage: An Urgent Threat.” EMSI. March 8, 2022. https://www.economicmodeling.com/2022/03/08/the-cybersecurity-talent-shortage/

13 McCurdy, Chris, Shue-Jane Thompson, Lisa Fisher, and Gerald Parham. “Getting started with zero trust security: A guide for building cyber resilience.” IBM Institute for Business Value. July 2021. ibm.co/zero-trust-security

14 Brandenburg, Rico and Paul Mee. “Cybersecurity for a Remote Workforce.” MIT Sloan Management Review. July 23, 2020. https://sloanreview.mit.edu/article/cybersecurity-for-a-remote-workforce/

日本アイ・ビー・エム株式会社
〒103-8510
東京都中央区日本橋箱崎町19 -21

米国で制作 | 2022 年 6 月



本書は、バイオベース・インクを使用した森林管理協議会(FSC)の CoC 認証を得た認定プリンターによって、塩素を含まない再生紙に印刷されています。この紙と印刷物の製造で使用されるエネルギーは、再生可能グリーン・エネルギーから生み出されたものです。リサイクルにご協力ください。


9NGZA7GK-JPJA-01

IBM