サイバーセキュリティがエンタープライズ・リインベンション（企業全体の再創造）を促進し、ビジネスレジリエンスを強化

State of Cybersecurity Resilience 2023

目次

トランスフォーメーション
を成功させるために

変わりゆく世界情勢

変わりゆく世界情勢に合わせて、サイバーセキュリティも変化を続けています。一方でその変化のスピードは、時に不十分です。

トランスフォーメーションを成功させるために

テクノロジーの進化や複雑化する規制、地政学的緊張、経済の不確実性――。これらに起因する市場のディスラプション（創造的破壊）は、ある意味グローバル企業のリスクとレジリエンスに対するアプローチを試すものです。

アクセンチュアのトータル・エンタープライズ・リインベンション（企業全体の再創造）調査によると、大企業経営者企業の多くは、かつてないスピードと頻度で自社を変革しています。

アクセンチュアの最新のサイバーセキュリティ調査の結果、サイバーセキュリティを変革の差別化要因として捉えている企業はその他の企業に比べ、優れたビジネス成果を創出できることが分かりました。また、サイバーセキュリティプログラムとビジネス目標との相関性が高い企業は、収益、市場シェア、顧客満足度、信頼性、そして従業員の生産性を向上させる可能性が、そうでない企業と比較して18%高くなります。

さらに、デジタルトランスフォーメーション（DX）の取り組みに主要なサイバーセキュリティ施策を組み込み、企業全体で強力なサイバーセキュリティを運用する企業は、その両方に対応していない企業に比べて、効果的なDXを実現する可能性が約6倍も高くなります。

一方で、企業サイバーセキュリティの取り組みへの遅れから、変革を推進しても将来の課題や機会創出に対応することができない企業もあります。

セキュリティ管理策の導入に関しては、調査回答者の18%が変革完了後も、脆弱性が検知された場合には導入を続けていることが判明しました。

手遅れになる場合もあります。最新の調査では、初期の計画フェーズではなく、アプリのコーディングフェーズにおいて、不十分なアプリケーションセキュリティに起因するエラーが検出された場合、修正には5倍のコストがかかり、リリース後に至ってはコストは30倍にも膨れ上がることが明らかとなっています。[1]

従来、ビジネストランスフォーメーションといえば、独立したデジタルケイパビリティの確立がメインでした。一方、今後多くの企業いわゆる共有現実（シェアード・リアリティ）基盤の構築を進めるでしょう。私たちが生活する現実世界と、急速に拡大しているデジタル世界が融合していくのです。そうした環境下では、企業はサイバーセキュリティを様々な段階で組み込んだ上で、より大きなリスクに対して高いレベルのリスクマネジメントを実施する必要があります。

トランスフォーメーションを成功させるために

インシデント発生ベースのサイバーセキュリティの対応ではなく、企業変革そのものの一部として組み込むことで、企業はサイバーセキュリティのレジリエンスを高めるだけでなく、企業全体を再変革し、安全な方法で新たな領域でパフォーマンスを発揮することができます。

サイバーセキュリティが
チェンジメーカーに

サイバーセキュリティがチェンジメーカーに

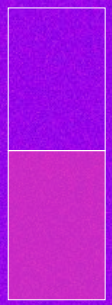
アクセンチュアが毎年実施しているサイバーセキュリティレジリエンスに関する調査は、
世界**14**カ国、**15**業種の企業から**3,000**人の経営幹部を回答対象としています。

調査から、半数以上の企業が、
変革の初期段階から、安全性を
確保する重要性を認識している
ことが明らかになりました。

53%

**サイバーセキュリティが
変革の中核に据えられている
と回答**

&



53%

**あらゆるソリューションを
新規導入する前に、
サイバーセキュリティの
管理が必要だと回答**

出典: Accenture State of Cybersecurity Resilience 2023
（N = 3,000人のセキュリティエグゼクティブおよびビジネスリーダー）

サイバーセキュリティがチェンジメーカーに

DX実行企業の多くは、以下3つの対策を講じることで、DX内容に組み込むサイバーセキュリティのレベルに十分満足できる可能性が**10%**高まることが明らかになりました。

デジタル変革の加速に向け、企業が取るべきサイバーセキュリティ対策の3つのアクション：

1. あらゆるソリューションを新規導入する前に、サイバーセキュリティ管理を義務付ける

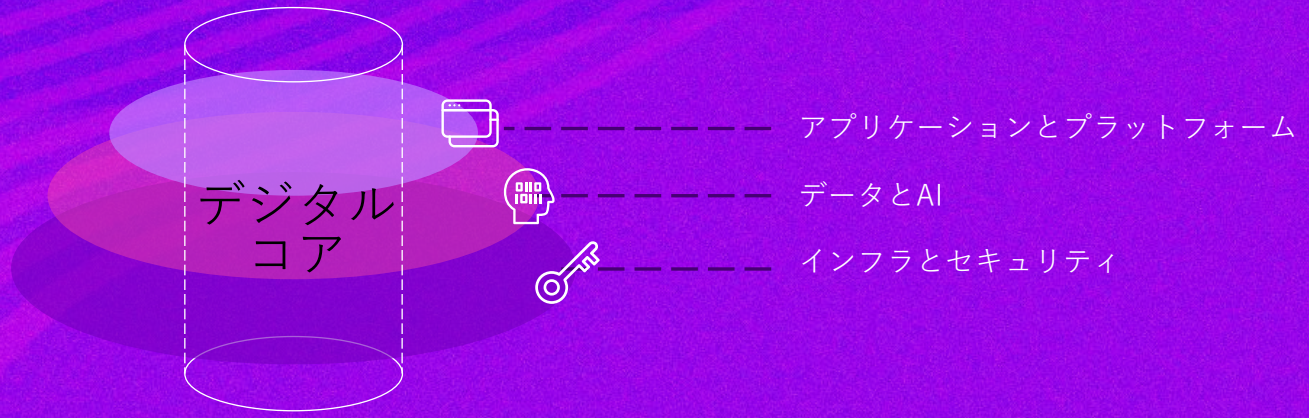
2. DXの達成状況に応じて、サイバーセキュリティを段階的に適用する

3. DXの中核メンバーにサイバーセキュリティ責任者を配置し、DXの取り組み全体をサイバーセキュリティの視点で指揮する

サイバーセキュリティがチェンジメーカーに

アクセンチュアが最近発表したResilience for Reinvention調査[2]によると、長期的に収益を拡大している企業は、インフラとセキュリティ、データと人工知能（AI）、アプリケーションとプラットフォームという3つの層から成る、デジタルコアの開発に力を入れていることが明らかになりました。

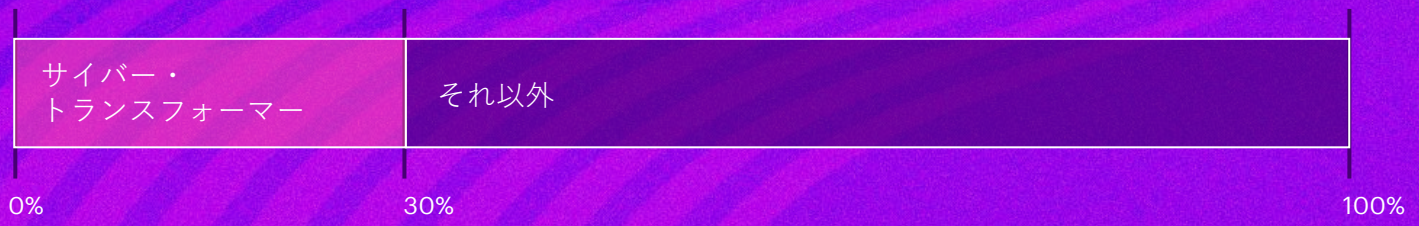
これらの企業はまた、最新のテクノロジー、イノベーション、サイバーセキュリティへの投資を継続的に拡大しています。



サイバーセキュリティがチェンジメーカーに

最新のサイバーセキュリティレジリエンスに関する調査では、回答企業の**30%**が、サイバーセキュリティを重視することで大きな成果がもたらされることを実証しています。私たちが「サイバー・トランスフォーマー」と呼ぶこれらの企業は、優れたサイバーセキュリティ対策が企業の発展につながることから、DXの取り組みを推進しており、今後も継続する計画です（図1）。

図1. DXを推進するサイバー・トランスフォーマーの割合



サイバーセキュリティがチェンジメーカーに

アクセンチュアが2021年のレポートで発表したサイバーチャンピオンと同じく、今年のサイバー・トランスフォーマーも、優れたサイバーレジリエンスとビジネス戦略とのバランスを取り、より良いビジネス成果の実現につなげています。

サイバーセキュリティがチェンジメーカーに

サイバー・トランスフォーマーは、サイバーセキュリティプログラムをビジネス目的と密接に連携させています。これにより、以下の成果を上げる可能性が**18%**高まっています。

- 目標とする収益成長と市場シェアの達成
- 顧客満足度と信頼性の向上
- 従業員の生産性拡大

さらに、サイバー・トランスフォーマーが、ビジネス計画の初期段階からサイバーセキュリティチームを関与させるケースが2倍近いこともわかっています。結果、サイバー・トランスフォーマーは、企業内のサイバーセキュリティ計画を非常に円滑に実行できています。

73%

ビジネス計画の初期段階からサイバーセキュリティチームを関与させるサイバー・トランスフォーマー

VS.

37%

ビジネス計画の初期段階からサイバーセキュリティチームを関与させる、サイバー・トランスフォーマー以外の企業

サイバー・トランスフォーマーは2つの方法でトランスフォーメーション基盤を構築

サイバー・トランスフォーマーは、トランスフォーメーションの取り組みに、3つの主要なサイバーセキュリティ対策を組み込むだけでなく、強力なサイバーセキュリティ運用を初期段階から適用することで、より優れた基盤を構築します。その結果、その他と比較して、より効果的なDXを実現する可能性が**5.8倍**高くなります（図2）。

図2. サイバー・トランスフォーマーがトランスフォーメーション基盤を構築する2つの方法

出典：アクセンチュア リサーチによるState of Cybersecurity Resilience 2023のデータの ロジスティック回帰分析（DXを実施する際、サイバーセキュリティのベストプラクティスを適用することで予測されるメリット、N = 2,500人のセキュリティエグゼクティブ

サイバーセキュリティがチェンジメーカーに

サイバー・トランスフォーマーは、強力なサイバーセキュリティ運用を通じて、他社を上回る成果を実現しています。

サイバーセキュリティとリスク管理を高度に**統合**

サービスとしてのサイバーセキュリティを頻繁に**活用**し、セキュリティの運用を強化

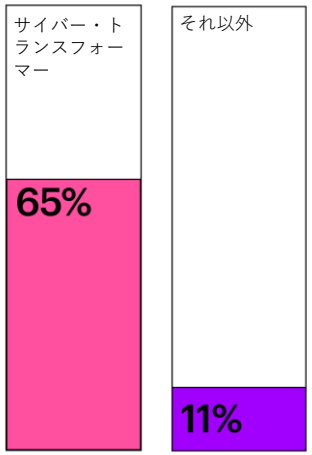
外部の攻撃からエコシステムを保護することに**注力**

オートメーションを最大限に**活用**

サイバー・トランスフォーマーに必要な要素

サイバー・トランスフォーマーに必要な要素

サイバー・トランスフォーマーとそれ以外には明確な相違点があります。



出典：Accenture State of Cybersecurity Resilience 2023（N = 2,500人のセキュリティ部門の経営幹部）

サイバー・トランスフォーマーの**65%**が、3つのベストプラクティスを適用し、高度なリスクマネジメントを実現しています。対照的に、それ以外の企業で「クラス最高水準」のアプローチを採り入れている割合は、わずか**11%**に留まります。

1. **サイバーリスクの統合：**サイバーリスクベースのフレームワークをエンタープライズリスク管理プログラムに完全統合
2. **優先事項への同意：**サイバーセキュリティ運用と経営幹部のリーダー層は、保護すべき資産と運用の優先事項について一貫して同意
3. **包括的なリスクの注視：**企業全体のリスクを評価する際に、サイバーセキュリティのリスクを最大限に検討

ケーススタディ

例えば、あるグローバルな旅行会社は、サイバーセキュリティリスクをより広範なエンタープライズリスク管理フレームワークに統合することで、より優れたリスク管理、規制要件へのコンプライアンス向上、企業と顧客保護の強化を得ることができました。

業界トップクラスの包括的企業リスク管理アプローチによって、同社はサードパーティベンダーやITシステムにかかわるセキュリティリスクの、詳細かつ総合的な知識を得られたほか、侵害が発生した場合の備えと復旧計画を整備できました。

サイバー・トランスフォーマーに必要な要素

サイバー・トランスフォーマーは、サービスとしてのサイバーセキュリティを頻繁に活用し、運用を強化しています。

サイバー・トランスフォーマーの**40%**が、サードパーティまたはマネージドサービスプロバイダーを用いて、サイバーセキュリティの管理業務や人材不足に対処しています。一方、それ以外の企業ではわずか**24%**に留まっています。

ケーススタディ

北米を拠点とする小売りチェーンは、公開会社として独立する際、IT運用を見直す必要がありました。アクセンチュアは、サービス型のサイバーセキュリティモデルを適用することで同社のセキュリティ専門チームを支援するよう要請を受けました。そして、脅威インテリジェンスやセキュリティオペレーションセンター（SOC）の設立など、セキュリティ運用を実施しました。

現在、アクセンチュアは、データ保護、アイデンティティ管理、ネットワークセキュリティ、脆弱性管理、セキュリティアウェアネス、リスク管理など、幅広いサービスを提供しています

サイバーセキュリティ運用の改善により、同社は継続的なイノベーション、円滑な店舗運用、消費者からの信頼維持を実現しています。また初期段階から安全性確保に努めることで、サイバーレジリエンスとビジネス成果を向上させることができました。

サイバー・トランスフォーマーに必要な要素

サイバー・トランスフォーマーはエコシステムの保護に力を注いでいます。

アクセンチュアの分析によると、エコシステム保護対策の面でも、サイバー・トランスフォーマーはそれ以外の企業より優れた成果を上げています。

例えば、サイバー・トランスフォーマーは、自社のインシデント対応計画にエコシステムやサプライヤーを組み込み（**45% vs. 37%**）、自社のエコシステムやサプライヤーに対して厳格なサイバーセキュリティ基準を満たすよう義務付けています（**41% vs. 29%**）。このような自社のエコシステム保護において、サイバー・トランスフォーマーは、それ以外の企業に比べ10%優位に立っていますが、未だ改善の余地があります。

ケーススタディ

ある大手製薬会社は、Amazon Web Services（AWS）と連携し、医薬品開発の推進、運用アジリティの向上、技術コストの削減、未来の人材開発を行いました。

より拡張可能で信頼性が高く安全なアーキテクチャを構築するために、同社はアプリケーションの80%をクラウドに移行することで、差別化されていないテクノロジーを排除し、社内データセンターのフットプリントを引き下げ、資本支出を削減してレジリエンスを高めました。

顧客、従業員、そしてパートナー企業が、同社の迅速な対応能力、アジリティ、バリューチェーン全体のインサイトから利益を得ることができ、これがひいては患者のエクスペリエンス向上にもつながります。

データサービスとケイパビリティの提供を促進することで、同社の安全なコネクティビティ、およびライフサイエンスのエコシステムと外部パートナーとのコラボレーションを向上させることができます。

サイバー・トランスフォーマーに必要な要素

サイバー・トランスフォーマーはオートメーションを最大限に活用しています。

サイバー・トランスフォーマーの**89%**が積極的に自動化を推進している一方、そうでない企業ではわずか**57%**にとどまっています。

さらに、サイバーセキュリティプログラムを大規模に自動化する企業の**96%**が、サイバーレジリエンス上の重要課題であるサイバー人材不足をオートメーションにより軽減できると認識しています。人間＋マシンのアプローチが主流となっていることを示す証拠として、アクセンチュアの分析でも、サイバーセキュリティ関連のAI特許の割合が、2017年1月から2022年10月の間で**2.7倍**に増加していることが分かりました。

ケーススタディ

738,000の従業員を擁するアクセンチュアでは、Intelligent Application Security Platformを活用して、AIとオートメーションを取り入れてきました。プラットフォームは最新のコマーシャルスキャニングツールを用いて、大規模なアプリケーションのセキュリティテストを行い、脆弱性とコードの問題を検出します。また、アプリケーションテストやパイプラインゲーティングに加え、オンボーディングアプリケーションも自動化、調整、拡張されます。

プラットフォームは、人口知能を搭載したフィルターを用い、脆弱性を数千から数個にまで除去・削減し、これによりキュレーションされた管理が容易なプロセスを実現します。

その結果、このスキャニングサービスは、スキャニングツールによって生成される擬陽性結果を自動削除することで、アプリケーションチームが、何千時間も時間短縮することを可能にしました。

サイバー・トランスフォーマーに必要な要素

ジェネレーティブAIをはじめとするAI開発の急拡大を受けて、サイバーセキュリティの発展も新たに進むと予想されます。

今後、ジェネレーティブAIは、エンタープライズ・ガバナンスと情報セキュリティをサポートし、不正行為からの保護、規制コンプライアンスの向上、企業内外のクロスドメインの関係と推論を引き出すことで事前のリスク特定が可能となるでしょう。[3]

実際、ChatGPTの出現はディスラプション（創造的破壊）と新たな機会を創出しました。脅威の検知、分析、対応などサイバーセキュリティのケイパビリティを急速に発展させているほか、オートメーションの利用促進による作業負荷の軽減や人員増強を実現しています。

あるCISOの視点：

「Security Operations Center（SOC）レベルの自動化には様々な意見があり、YARAルールやより複雑なクエリの作成を支援する声もあります。ジェネレーティブAIには既にこのケイパビリティが備わっています。しかし、私は、依然として人間の監視も必要だと考えます。」

サイバー・トランスフォーマーに必要な要素

アクセンチュアの調査でも述べているとおり、トータル・エンタープライズ・リインベンション（企業全体の再創造）とは、企業が事業展開する業界において、新たな領域でパフォーマンスを発揮することを目的とした意図的戦略です。

サイバー・トランスフォーマーは、差別化されたサイバーセキュリティの実践と行動から直接的な便益を得ることで、企業の再変革戦略を成功させています。

サイバーセキュリティのインシデントが日々発生する中、サイバー・トランスフォーマーは、過去12カ月のサイバー攻撃およびインシデント対応コストを、他の企業より平均で**26%**削減していると報告しています。これはオペレーションの最適化、成長の促進、レジリエンスの改善に向けて、全社的に割り当てられる総コストの4分の1以上に相当します。

ケーススタディ

ある大手リテールおよび銀行は、プライベートクラウドへの移行とパブリッククラウドを用いた新商品の作成という2つのDXに取り組みながら、サイバーセキュリティに関するアジャイルな意思決定を導入しました。

同行の分散化された運用モデルを、DXの早期段階でサイバーセキュリティと一体化させたことで、リスクと脆弱性を軽減し、データ保護を向上させ、セキュリティ体制全般の強化に成功しました。

さらに同銀行は、コンプライアンスを向上させ、安全で信頼できる企業としての評価を高めながら、コストとダウンタイムを削減しました。

その他の課題

安全なDXの管理が重要な検討事項である一方、アクセンチュアの調査から、あらゆる企業にプレッシャーを与え、サイバーセキュリティのレジリエンス状況にも影響を及ぼす課題の存在も明らかになりました。世界中からの回答を見渡すと、以下の課題が浮き彫りとなりました。

不安定な地政学的状況が脅威と攻撃を助長

地政学的な緊張状態が続く中、企業のサイバーレジリエンスは、特にサプライチェーン、物理的インフラ、外部ネットワークを通じたプレッシャーにさらされています。

サイバーリスク対策のアプローチを社内外で精査中

企業はサイバーリスクが及ぼす範囲とその規模に対応できていません。

サイバーセキュリティとビジネスの連携には未だ改善の余地が存在

企業は、ビジネスリーダーシップのもと、サイバーセキュリティとビジネスを巧く連携させていますが、それに反してその効果は十分に創出されていません。

その他の課題

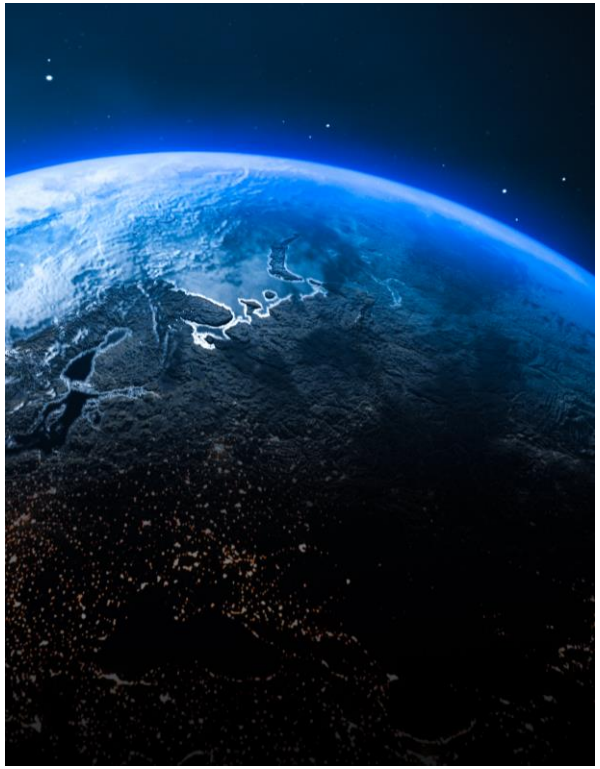
不安定な地政学的状況が脅威と攻撃を助長

地政学的な緊張が続く中、企業のサイバーレジリエンスは、特にサプライチェーン、物理的インフラ、投資パートナーなどの外部要因によるリスクにさらされています。

大半の人がロシアによるウクライナ侵攻の影響を感じています。ほぼ全ての企業（**97%**）が、戦争の勃発以降、サイバー脅威の増加を実感しており、調査回答者のほとんど全員が何らかの措置を講じています。

企業の**51%**は、事業継続性とリスク計画を見直したことで、インシデント対応能力を向上させています。同時に、戦時に適したポリシーや対応について政府機関との密なコラボレーションを優先する企業はわずか**39%**に留まっており、半数以上（**54%**）は、サードパーティと外部ネットワークを最も攻撃を受けやすい領域であると考えています。

実際に、昨年度の調査結果と同様、企業の外部からの侵害の割合は高く、むしろわずかに上昇しています（昨年度の60%に対して**61%**）。一方、ユーティリティなどの業界では、サプライチェーンパートナーの脅威が**62%**と再び高まっています。



その他の課題

サイバーリスク対策のアプローチを社内外で精査中

企業はサイバーリスクが及ぼす範囲とその規模に対応できていません。

サイバーリスク管理は企業社内における課題のひとつになっています。企業におけるリスク管理の一側面である、サイバーリスクベースのフレームワークがプログラムに完全統合されているという調査回答は、わずか半数以下でした。

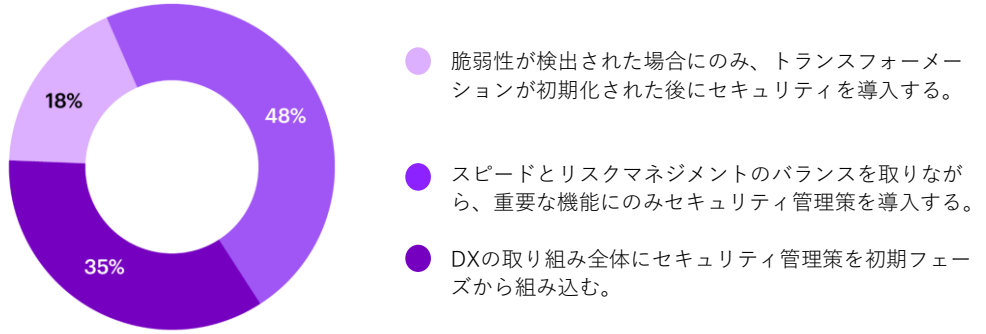
これには規制環境が影響しています。リスク統合は、規制の厳しい金融業界では**81%**と高く、一方ソフトウェアやプラットフォーム業界では**65%**となっています。

また、セキュリティ対策に並行で取り組むことなくDXを進めると、リスクがより高まる恐れがあります。

回答者の**35%**は、すべてのDXの初期段階からセキュリティ管理を組み込むと回答しましたが、事後にセキュリティを導入するとの回答も依然として**18%**あります。スピード感を持って変革を実現するには、セキュリティを変革の中心に組み込む必要があります。そうでなければ、企業はこの先、インシデントが発生するたびにより多くのコストや作業が発生することが予想されます（図 3）。

また、サイバーリスクは企業の外でも増大しています。環境変化によるサイバー脅威が増加しているほか、サイバーセキュリティの不備によって企業はリスクにさらされます。

図3. DXセキュリティの取り組み



出典：Accenture State of Cybersecurity Resilience 2023（N = 2,500人のセキュリティエグゼクティブおよび500人のビジネスリーダー）

例えば、ロシアによるウクライナ侵攻は、企業の経営幹部に対し、事業継続性の見直し、インシデント対応、従業員のサイバーアウェアネス向上など、サイバーセキュリティ対策を促すきっかけとなりました。

実際に、全社的なリスク評価時に、サイバーセキュリティリスクを「大いに」検討すると回答したのは全体のわずか3分の1（**35%**）に留まります。このことは、サイバーセキュリティをビジネス上の積極的かつ戦略的な必須事項と位置付けるには、未だ道半ばであることを浮き彫りにしています。

その他の課題

サイバーセキュリティとビジネスの連携には未だ改善の余地が存在

サイバーセキュリティとビジネスの連携は取れていても、その効果は十分に創出されていません。

ビジネスリーダー（今回の調査回答者におけるCEOやCFOなど）は、CISOが従来の役割を超えて、企業の代表的存在として活躍することを期待しています。また、サイバーセキュリティの技術的側面をCEOと取締役会に説明（**44%**）し、セキュリティ侵害時の対応をリード（**42%**）し、お客様の信頼を構築（**41%**）するなど、CISOが従来の役割を超えて活躍することが重要であると回答しました。

あるCISOの見解：

「セキュリティリーダーが抱える最大の障害は、エグゼクティブとしての存在感です。ビジネスケイパビリティと価値を実証し、セキュリティに関する会話以外にも参加する必要があります。」

この結果は、セキュリティ以外の関係者に対する教育者およびコラボレーターとしての役割を担うビジネス主導型のCISOを擁することがいかに重要であるかを示しています。

特に、CISOとビジネスリーダーとの間には、セキュリティ侵害後のコミュニケーション戦略に関して認識の齟齬があります。しかし、サイバー攻撃を経験した企業であれば分かるとおり、危機の渦中では、迅速かつ透明性の高いコミュニケーションを通じて、ステークホルダーに情報と安心を提供することが重要です。

およそ半数のCISOが、セキュリティ侵害時の外部に向けたコミュニケーションを担うエグゼクティブが不在であると回答しています。

その他の課題

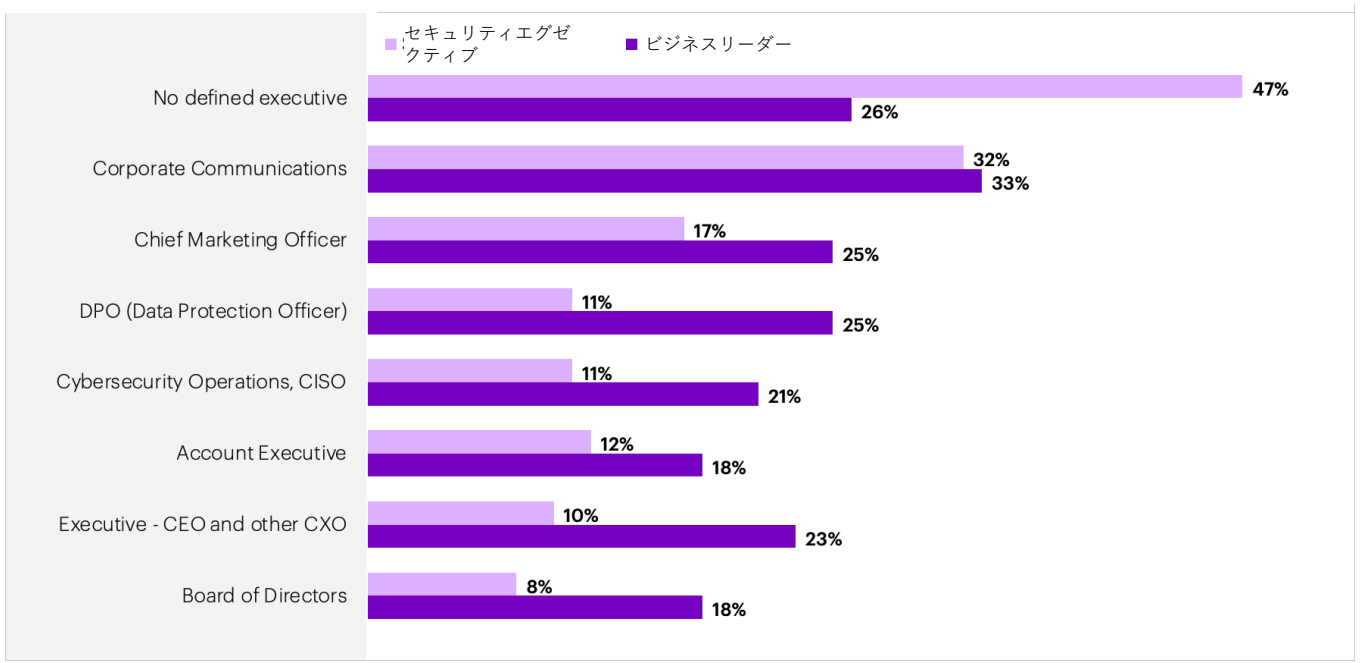
サイバーセキュリティとビジネスの連携には未だ改善の余地が存在

また、責任の所在に関するCISOとビジネスリーダーの意見の相違は、セキュリティ侵害後の明確なコミュニケーションが欠如することを示唆しています（図4）。

これは、セキュリティ侵害によるブランドや顧客満足度スコアのダメージを最小限に抑えることを目指す企業にとって危険信号であり、調査回答者の**50%**がセキュリティ侵害後の最も重要な懸案事項として挙げています。

企業は、アジャイルにサイバーイベントの複雑性を考慮に入れ、ステークホルダーとのコミュニケーションの役割と責任が明確に定義されたクライシス・コミュニケーション戦略を定義する責任があります。

図4. セキュリティ侵害時のコミュニケーション責任



出典：Accenture State of Cybersecurity Resilience 2023（N = 2,500人のセキュリティエグゼクティブおよび500人のビジネスリーダー）

次のステップ

次のステップ

現実的には、サイバーセキュリティを包括的に捉えなければ、サイバー攻撃からビジネスを完全に守ることはできません

次のステップ

優れた成果をもたらすサイバーセキュリティの採り入れ方

デジタルコアを保護するサイバーセキュリティの導入

ビジネスの俊敏性と拡張性を実現するだけでなく、継続的なイノベーションを促進し、企業のデジタルコアを確立するためにセキュリティは不可欠です。セキュリティによって従業員や各部門は、リスクを軽減しながらビジネスにおける新たな試みやビジネスの拡大に挑戦し続けることができるのです。

実行すべき点

3つのサイバーセキュリティ対策を実施して、サイバーセキュリティ運用の強力な基盤を確立することで、ビジネス成果と全体的なパフォーマンスを向上させる。

サイバーセキュリティを応用してデジタルと物理世界を融合

クラウド・コンティニウム（クラウドの継続活用）とレガシー環境におけるアクセス、デバイス、ソフトウェア、接続性が向上したことで、脅威の対象となる領域がこれまでになく拡大しています。またジェネレーティブAIにより、俊敏性とサイバー保護の新時代が到来した一方で、ジェネレーティブAIはサイバー犯罪者（ハッカー）にとっても新しい攻撃手段となる恐れがあります。

実行すべき点

データとその価値、アクセス可能ユーザーの理解に投資する。企業と顧客のアイデンティティを再検討し、物理世界とデジタル世界のなめらかに融合を促進する。エンドポイントの検出と対応（EDR）やセキュリティのオーケストレーション、自動化、対応（SOAR）テクノロジーを用いて、レガシー環境とクラウド環境の両方におけるモニタリングおよび可視性を強化する。

サイバーセキュリティをDXの取り組みの一部とする

サイバーセキュリティに対する従来のアプローチは持続可能ではありません。継続的なサイバー脅威に対処できるサイバーセキュリティ人材が世界的に不足していることに加え、サイバー攻撃が企業の事業継続性、経済性、評判に及ぼす影響に対処できる人材も不足しています。DXの開始時期と終了時期の境界線が曖昧になりつつあります。

実行すべき点

サイバーセキュリティをDXの取り組みの要とし、CISOの報告を強化・向上することで、CISOの機能がビジネス変革の中心となるようにする。

次のステップ

リスク評価と管理からセキュリティ管理策の導入、およびセキュリティ意識向上とトレーニングからインシデント対応と復旧に至るまで、サイバーセキュリティはあらゆる変革プログラムにおいてダイナミックな保護を維持するために必要不可欠です。また、サイバー・トランスフォーマーが示すとおり、ビジネスリーダーは、サイバーセキュリティの影響を、企業・ビジネスの保護にとどまらず、継続的かつダイナミックに再変革を実現するためポジティブな影響を及ぼす機会を有しています。

リサーチについて

統計データ

アクセンチュアの「サイバーセキュリティレジリエンス最新レポート2023」調査は、世界14カ国、15業種の企業から経営幹部3,000人を対象に実施しました。この調査は、企業のトランスフォーメーションへのアプローチにおけるサイバーセキュリティの役割、および安全なDXを円滑に進めるための幅広いサイバーセキュリティ対策の把握を目的としています。回答者は北米、南米、ヨーロッパ、アジア太平洋地域の年間売上高10億米ドル以上の企業に属しています。

3,000

回答者数合計

最高情報セキュリティ責任者 2,500人
ビジネスリーダー（CEO、CFO） 500人

10億米ドル以上

売上高

14

カ国

オーストラリア (234)
ブラジル (100)
カナダ (115)
フランス (201)
ドイツ (223)
アイルランド (102)
イタリア (200)
日本 (221)
オランダ (101)
ノルウェー (100)
サウジアラビア(55)
スペイン (100)
英国(360)
米国(888)

15

業種

バンキング（265)
キャピタルマーケット(177)
化学 (186)
消費財＆サービス (288)
エネルギー – 石油・ガス (277)
保険支払者 (102)
医療機関 (130)
ハイテク (209)
保険 (209)
ライフサイエンス (199)
米国連邦サービス (100)
小売 (259)
ソフトウェア＆プラットフォーム (135)
通信 (202)
ユーティリティ (262)

メソッド

調査データの分析

標準的な調査データ分析を用いて、全体的な状況とサンプルに含まれる様々なグループの特性を把握しました。特にサンプルに含まれるセキュリティ担当幹部の30%を占めるサイバー・トランスフォーマー（回答者741名）と、それ以外のセキュリティ担当幹部（回答者1,759名）を比較しました。その結果、サイバー・トランスフォーマーを、DXの取り組みを加速させており、それを今後2年間も継続して加速する予定の企業と定義しました。

複合指標

より複雑な分野で企業がいかに成果を上げているのかを把握するための2つの独立した指標を策定しました。

1. **エコシステム保護指標：**アクセンチュアの調査データを組み込み、企業が実施しているエコシステム保護対策に関する質問への肯定的な回答数に基づいています。均等加重が適用され、指標は0～100の基準に区分されています。

2. **アラインメントとガバナンス指標：**昨年度のアラインメント定義に基づき、本年度の調査データを適用して指標を策定しました。この指標は、企業がセキュリティをどのようにビジネス目標に整合させ、どのようなガバナンスを適用しているかに関する質問への回答に基づいています。均等加重が用いられ、指標は0～100の基準に区分されているほか、ロジスティック回帰分析で使用した指標の一部でもあります。

ロジスティック回帰計量経済アルゴリズム

成功確率と企業による取り組みの関係性を予測するにあたり、ロジスティック回帰アプローチを適用しました。いずれのモデルも企業の規模、地理的な位置、ビジネスを展開する業界に応じて管理しました。

1. **ビジネス成果分析 -** アラインメントとガバナンス指標で測定したビジネスアラインメントとガバナンスのレベルと、企業がサイバーセキュリティにより以下の成果すべてにプラスの影響を与える確率の関係性を分析しました。
   - 目標とする収益成長の達成能力の向上
   - 市場シェアの拡大
   - 顧客満足度と信頼性の向上
   - 従業員の生産性の向上

2. **安全な変革の取り組みの分析 -** 安全な変革への取り組みに高い満足度を示す確率に着目しました。調査サンプルの特定のコホートについて、セキュアな変革のベストプラクティスとの関連性を検証しました。

公開データの自然言語処理と傾向分析

自然言語処理（NLP）アプローチでLexisNexisの特許データを使用し、AIを含むサイバーセキュリティ関連の特許を選択しました。2017年1月から2022年10月までの公開データを用いて、サイバーセキュリティに焦点を当てた特許全体の件数に占める、AI関連特許の割合の推移を特定するために傾向分析を行いました。

用語集

「**Compressed Transformation**（短期間で戦略、デジタル、オペレーションを含むすべてを変える全社変革）」とは、戦略、デジタル、オペレーションを含む複数の事業領域を、同時かつ非常に短期間で実行する全社的な変革を指します。

デジタルコアは、企業のあらゆる戦略的ニーズの礎となるものです。変革によってテクノロジーの役割を拡大することは、すなわち従来の静的で独立した部分からなるテクノロジー環境から、意図的に統合されクラウドを用いた相互運用可能な状況へと移行することを意味します。デジタルコアは、インフラとセキュリティ、データとAI、アプリケーションとプラットフォームの3つのレイヤーで構成されています。単発のプロジェクトでは強力なデジタルコアを構築することはありません。新たなテクノロジーとビジネスケイパビリティを、継続的に組み込むことが必要です。

トータル・エンタープライズ・リインベンション（企業全体の再創造）とは、企業が属する業界において、新たな領域でパフォーマンスを発揮することを目的とした意図的な戦略です。強力なデジタルコアを中心に、企業の成長を加速と業務の最適化を図ります。再創造を実現するには、継続的でダイナミックな戦略が必要です。成功のためには、あらゆる人が関わり、責任を負う必要があります。また、経営幹部や各部門、および事業領域全体を融合することが求められます。企業で起きていることと世界で起きていることを結びつける、アウトサイド・インの視点も重要です。そして、新たなスキルだけでなく、テクノロジーやチェンジマネジメント、コミュニケーション、エコシステム・パートナーを活用してより迅速に結果を出す方法などの知識も必要です（図5）。

図5. トータル・エンタープライズ・リインベンションの差別化要素

1. **戦略としてリインベンションを行っています。**もはや実行手段ではありません。
2. **デジタルコアを競争優位性の主要な源泉としています。**企業全体で円滑にデータをやり取りできる相互運用性の高いシステムを実装し、クラウド、データ、AIの力を活用した新たな機能を迅速に開発することができます。
3. **リインベンションのためにベンチマークを設定するだけでなく、最善の現実解を導き出しています。**テクノロジーと新しい働き方を通じて、新たな領域でパフォーマンスを発揮しています。
4. **人材戦略と人材育成を、リインベンションの補足的な要素としてではなく、中心に据えています。**チェンジマネジメントをコア・コンピテンシーと見なしています。
5. **リインベンションの範囲を限定しません。**企業内のサイロを排除し、企業活動の上流から下流にいたるあらゆる能力を対象に再創造しています。
6. **継続的なリインベンションを行います。**一回限りのものではなく、企業が変革し続けられる能力を獲得しています。

参考資料

1. デジタルとは　リンク
2. Reinventing for Resilience（アクセンチュア、2023年）　リンク
3. A New Era of Generative AI for Everyone（アクセンチュア、2023年）　リンク
4. Ibid　リンク

著者紹介

Paolo Dal Cin
アクセンチュア セキュリティ統括

Jacky Fox
アクセンチュア セキュリティ
ヨーロッパ統括
シニア・マネジング・ディレクター

Harpreet Sidhu
アクセンチュア セキュリティ
北米統括
シニア・マネジング・ディレクター

James Nunn-Price
アクセンチュア セキュリティ
グロースマーケット統括
シニア・マネジング・ディレクター

謝辞
Sarah Bird、Edward Blomquist、Katarzyna Furdzik、Corbin Lazier、Anna Marszalik、Eileen Moynihan、Juan Pablo Romero、Ann Vander Hijde による、本レポートへの貢献に感謝の意を表します。

アクセンチュアについて

アクセンチュアは、世界有数のプロフェッショナル サービス企業です。アクセンチュアは、世界をリードする企業や、行政機関をはじめとするさまざまな組織の中核にデジタル技術を実装することで、組織運営を最適化し、収益を拡大させ、また市民サービスの向上にも貢献するなど、お客様に対して目に見える成果を圧倒的な規模とスピードで創出しています。 アクセンチュアでは、優れた才能でイノベーションを主導する約733,000人もの社員が120カ国以上のお客様に対してサービスを提供しています。 また、テクノロジーが変革の成否を分ける時代において、世界中のエコシステム・パートナーとの緊密な連携を図りつつ、クラウド、データ、AIおよび業界ごとの比類のなき知見、専門知識や、グローバル規模のデリバリー能力を最適に組み合わせながらお客様の変革を支えています。アクセンチュアは、ストラテジー＆コンサルティング、テクノロジー、オペレーションズ、インダストリーX、ソングの領域をまたぐ、幅広いサービス、ソリューションやアセットを活用して成果につなげています。アクセンチュアでは、成功を分かち合う文化や、360度でお客様の価値創造を図ることで、長期にわたる信頼関係を構築しています。またアクセンチュアは、お客様、社員、株主、パートナー企業、社会へ提供している360度での価値創造を、自らの成功の指標としています。

詳細については https://www.accenture.com/jp-ja をご参照ください。

アクセンチュア セキュリティについて

アクセンチュア セキュリティは、ストラテジー、プロテクション、レジリエンス、業界に特化したサイバーサービスを含む、エンド・ツー・エンドなサイバーセキュリティサービスを提供するリーディング・プロバイダーです。Cyber Fusion Centersのネットワークを通じて、グローバル規模で世界中のデリバリーケイパビリティを組み合わせた、セキュリティイノベーションを提供します。また、高度なスキルを備えたプロフェッショナルチームの支援により、クライアントの安全なイノベーション、サイバーレジリエンスの構築、確実な成長を実現します。

詳細については https://www.accenture.com/jp-ja/services/security-index をご参照ください。

アクセンチュア リサーチについて

アクセンチュア リサーチはトレンドを具現化するとともに、世界の企業が直面する最も逼迫した課題に関する、データドリブンなインサイトを策定しています。革新的なリサーチ手法とクライアント業界に関する詳細な知識を融合させ、250人の研究者とアナリストから成るチームは、世界23カ国にまたがり、毎年何百件ものレポート、記事、見解を発表しています。プロプライエタリデータやMITやSingularityなどの一流企業とのパートナーシップに支えられた、示唆に富んだ研究は、私たちのイノベーションを導き、理論と斬新なアイデアをクライアントに向けた現実のソリューションに落とし込みます。

詳細については www.accenture.com/research をご参照ください。