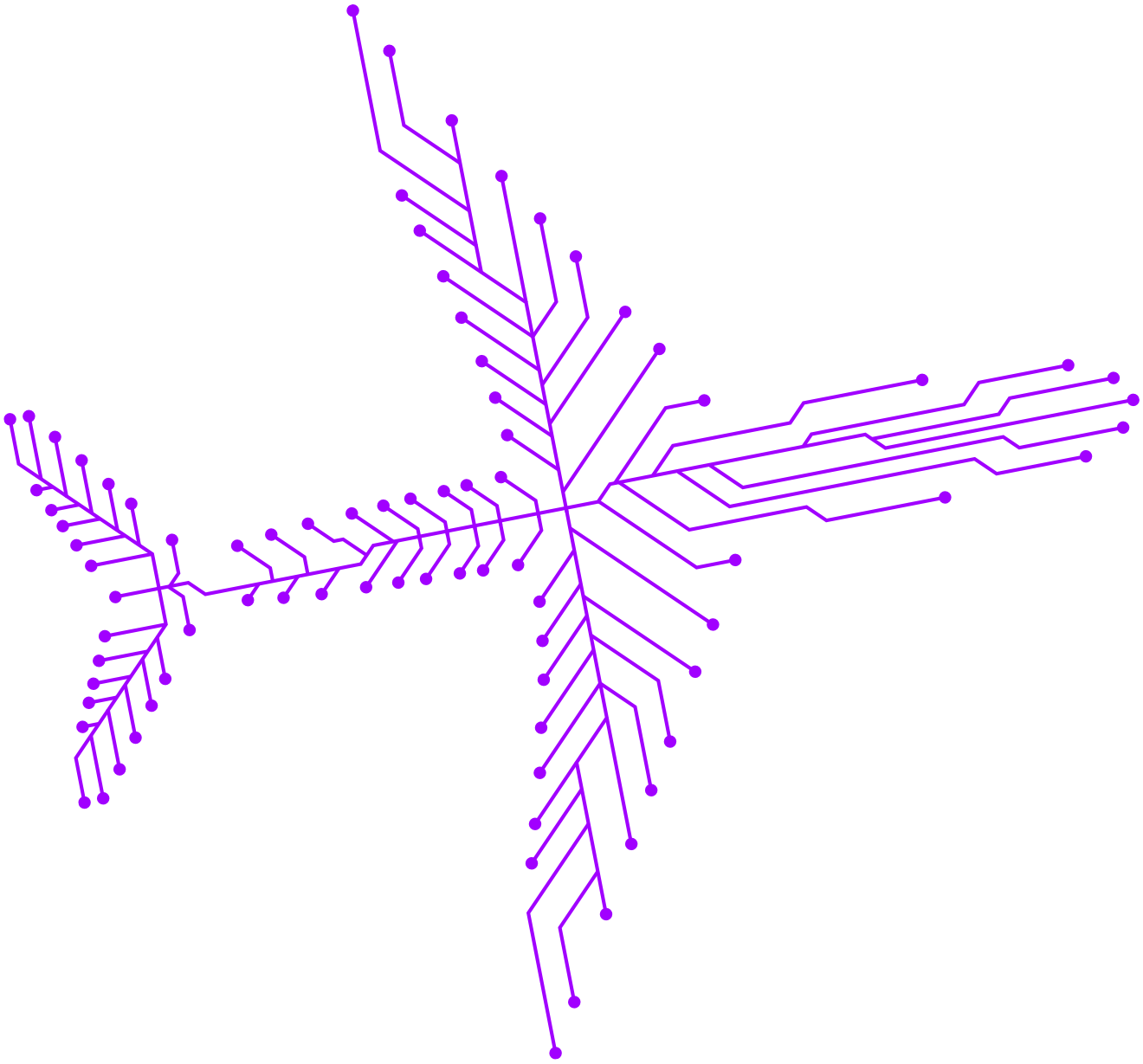
accentureconsulting



デジタル時代の空の安全を守る

航空宇宙・防衛分野のサイバーレジリエンス

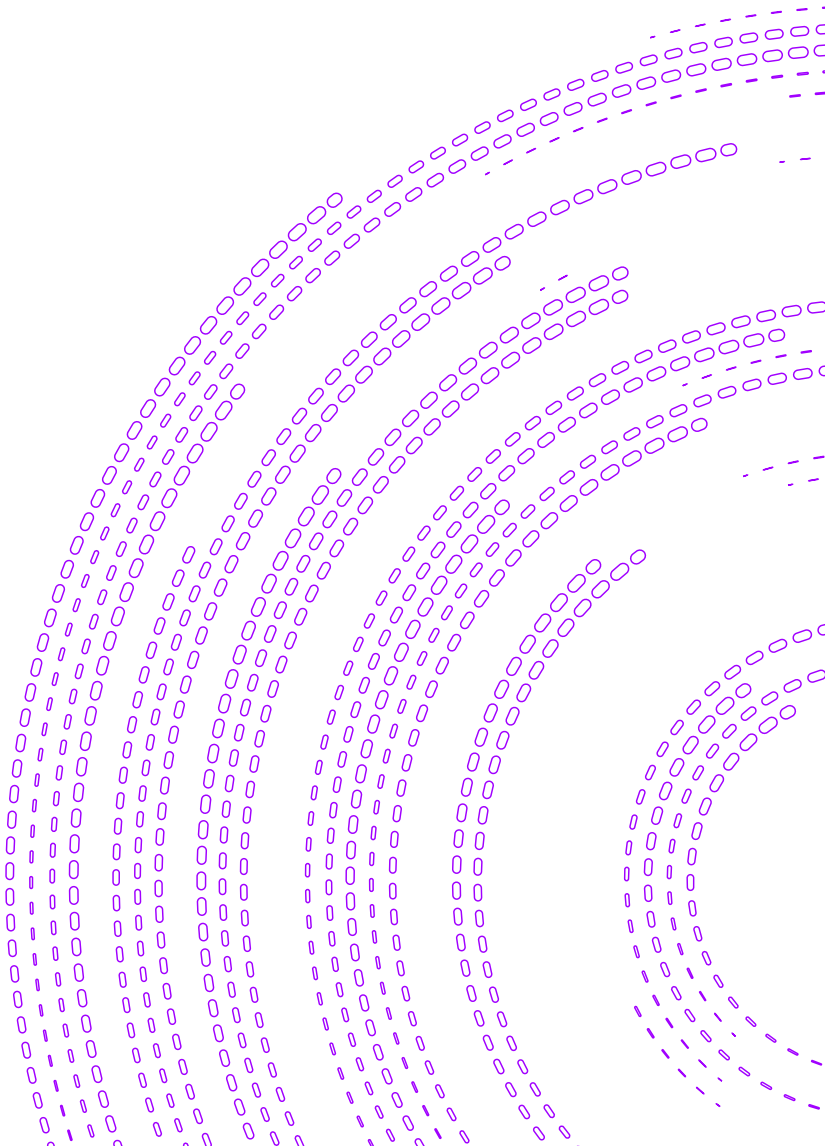
なぜ航空宇宙・防衛企業はサイバーレジリエンスをデジタル変革の中心に据えなければならないのか

航空宇宙・防衛企業は、デジタルの未来への移行を加速する必要性を認識しています。クラウドやロボティックプロセスオートメーション（RPA）などの技術を導入し、ビジネスモデルやオペレーションモデルを改善することで、経費削減と増収を促進していかなければなりません。しかし、一部の企業においては、データ主導型でコネクテッドな未来の企業への転換に伴うサイバーリスクに対処する準備がいまだ整っていないのが現状です。サイバーレジリエントな企業になるには、準備段階にあるものも含め、自社の活動の全てにセキュリティを組み込むことはもちろん、パートナーやサプライヤーのセキュリティについても適切な標準を満たす必要があります。

デジタル化ですべてがリスクに直面

航空宇宙・防衛企業は、新しい規制を順守しながら、投資による経費削減と増収を見込んで、テクノロジーベースのビジネスモデルの刷新とオペレーションモデルの刷新に取り組んでいます。ビジネスおよびオペレーション全般でインテリジェントな技術を利用し、サプライヤーやパートナー、顧客との持続的で親密なデジタルでのつながりを強化し、有意義性と競争力を維持できる企業に生まれ変わるべく、舵を切っています。

しかし、このようなコネクテッドでインテリジェントかつ自律的な企業になるには、新たなサイバーリスクが伴います。最高情報セキュリティ責任者（CISO）[1]を含む航空宇宙・防衛企業の経営層を対象にしたアクセンチュアの調査では、ビジネステクノロジーの新規導入や機能強化に伴い、今後数年間でサイバーセキュリティのリスクが大幅に増すとの回答が75%を占めました。ビジネスへのリスクとしては、セキュリティ侵害による業務の中断、機密データ（例：知的財産、管理対象情報、個人識別情報）の喪失などが挙げられます。



未来の到来により、サイバーリスクが増大

未来のビジネスを効率化・高速化し、競争力を向上させるデジタル・テクノロジーを活用するには、システムやネットワークへの接続が伴います。接続によって、腐敗分子が紛れ込み、セキュリティインシデントが発生するリスクが高くなってきています。たとえば、情報を提供するデータとプログラムは、いずれもハッキングの対象になる可能性があります。高度に規制された業界で事業を展開している航空宇宙・防衛企業の経営層にとって、機密データの盗難は重要な懸念事項のひとつです。さらに、製造・生産分野におけるオペレーショナルテクノロジー（OT）の統合により、企業はこれまで以上にサイバー脅威の影響を受けやすくなっています。

多くの企業が身をもって学んでいることですが、新しいデジタルビジネスの世界において、顧客の機密情報や個人識別情報が漏えいすれば、事業の中断が生じるだけなく、顧客と消費者、両方のつなぎ止めに欠かせない信頼を失墜させることにもなりかねません。

コネクテッド
常時接続＝常時危険にさらされる

未来の航空宇宙・防衛ビジネスは、24時間365日の接続に依存しながら、社内プロセスを実行し、パートナーと連携し、顧客へとリーチします。企業は、バリューチェーンとサプライチェーンの全てを電子的に接続――無線ネットワークの利用が増加――しており、その範囲は長距離に及びます。加えて、IoTの活用が進み、物理的な世界でのデータの検索や機器の管理にもデジタル接続が利用されるようになっています。今回の調査では、どのテクノロジーを導入すると、自組織のサイバーリスクが高まると考えているか、回答者に挙げてもらいました（図1参照）。

第1位は人工知能（AI）で、84%の回答者がサイバーリスクは高まる、もしくは大幅に高まると述べています。航空宇宙製造業界では、AIを利用して工場の生産データを解析し、製造プロセスの変動を予測しており、これによって企業は生産における諸問題に対応しています。AIはまた、就航中の設備の故障を予測し、航空機の運用効率を上げる目的でも使用されています。

サイバーリスクを高める技術として、AIに次いで上位に挙がっているのが、モバイルコンピューティング（82%）とIoT（80%）です。航空会社や保守・修理・点検プロバイダー（MRO）は、クラウドベースのソリューションの導入とあわせて、オンプレミスのテクノロジーや、ハードウェアの管理が不要なモバイルデバイス、タブレットなどを利用することで、デジタル変革を取り入れようとしています。

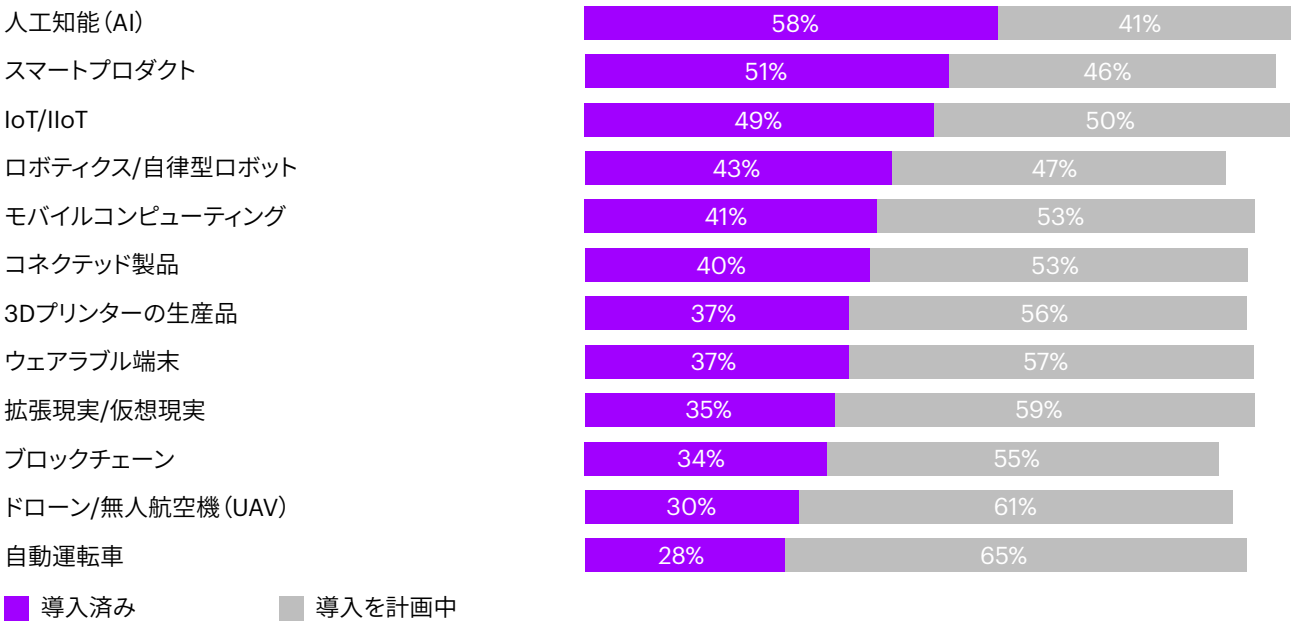
ITオペレーションの柔軟性を高め、AI分析などの専用サービスにアクセスするために、クラウドを利用する企業が増えています。多くのスマートフォンアプリのバックグランドでもクラウドコンピューティングが動作しており、電話では行えないデータクランチングを実行しています。その結果、BYOD (Bring your own device) の仮想作業環境における、もう1つの潜在的脆弱性が生み出されています。

MROにおいてIoTは、予測的メンテナンスを実行するための効果的なデータ収集を助けるセンサーとしての重要な役目を担っており、エンジン、機体、着陸装置などの航空機システムに導入されています。サプライチェーンにおいても、運用効率の向上、資産の管理や追跡、重要プロセスのモニタリングなどにIoTが広く利用されています。経営トップは、サードパーティ（提携/委託先）とデータを共有することの潜在的な危険性に対しても大きな懸念を抱いています。今回の調査では、戦略的パートナーをはじめとするサードパーティとのデータのやりとりによってサイバーリスクが高まるとの回答が69%を占めています。また89%が、自社のエコシステム内のサードパーティと戦略的パートナーの数が今後3年間で増加するであろうと予想しています。要するに、「侵害を受けない」製品やサービスを提供することは航空宇宙・防衛企業が今日抱えている大きな課題であり、それは今後も変わることはないでしょう。

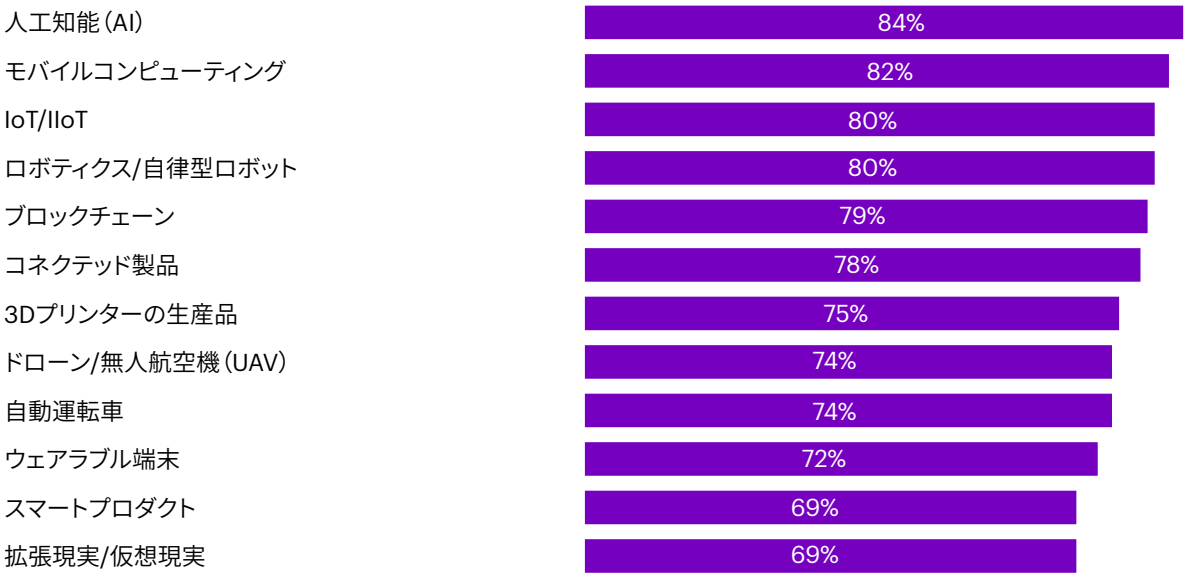
また企業は、ウェアラブル端末から次世代アビオニクスソリューション、機内接続ソリューションまで、従来以上の航空機用のコネクテッド製品およびソリューションを製造、販売していく予定です。ここで考慮するべき潜在的リスクとしては、死亡事故や物理的破壊、さらには金銭的損失やレピュテーションの低下にまで及びうる、壊滅的なサイバーリスクが挙げられます。

図1：技術の導入状況と予想されるサイバーセキュリティリスク

航空宇宙・防衛企業がすでに導入している、もしくは導入を計画している新興技術



その技術が航空宇宙・防衛企業のサイバーセキュリティリスクに影響する、もしくは大いに影響すると考える回答者の割合（%）



インテリジェント
データとともにリスクは増大する

インテリジェントシステムは、AIなどの最新技術と大量のデータセットを組み合わせて使うことで、それまで人の手によって行われていたタスクを引き受けるほか、人間が容易には行えないことを実行します。かつて、高度な分析はデータサイエンティストを大量に雇用できる一部の大企業の領域とされていましたが、今ではインテリジェントシステムによって、あらゆる企業で実行できるようになりました。たとえば、機械学習を利用することで、視覚処理プログラムが組み立てラインで部品を選別する方法を自己学習したり、電話をかけてきた人の話を「聞いて」、カスタマーサービスの質問に応じたりといったことが可能です。経営においては、インテリジェントシステムはデータ主導型の意思決定を下すのに役立っています。今回調査対象となった企業は、インテリジェント技術の利用の広がりによって自社が負うことになると考えられるリスクについて認識しています。上級役職者の70%が、顧客データの利用によって自社のリスクが増す、もしくは大幅に増すと回答しています。

企業内でAIや機械学習、ビッグデータが横断的に利用されていることを考えると、リスクの高まりとともに、セキュリティとデータプライバシー保護の両方の重要性が増大すると見込まれます。量も種類も増しつつある機密データを保護することは、経営層にとって重要な懸念事項の1つとなっています。86%の回答者が、機微性・機密性の高いデータを、エコシステムパートナーとやりとりする量は、今後3年間で増加する、もしくは大幅に増加すると考えています。

企業は、売上の拡大およびロイヤリティの構築を可能にする商品・サービスのカスタマイズを行い、優れた顧客体験を生み出すために、人口動態、金融、購買履歴、ライフスタイルなど、これまで以上に多くのカテゴリーにおいて、顧客に関する多くの情報を収集しています。たとえば、航空券に付随する事業の売上を押し上げるために、航空会社では予測分析と機械学習を利用して、パーソナライズされた提案を顧客に対して行っています。これらのデータが盗まれたり悪用されたりすれば、財務上の損失や罰金、評判の失墜など、ビジネスに深刻な打撃が及ぶ可能性があることを企業は認識しています。

自律型
セルフディレクティング（自ら方向付けを行う）システムの保護

たとえば、Boeingの777X型旅客機とLockheed MartinのF-35型戦闘機には自律型マシンが採用されています。86%の回答者が、ロボティクスを発生源とするサイバーリスクが今後増えるだろうと考えています。これらの自律型マシンは、悪意あるハッカーの標的になる可能性があります。ハッカー達は、システムのコントローラソフトウェアに侵入し、動作に変更を加え、安全ではない製品へと変えようとします。たとえば、昨年、Boeingの製造工場はランサムウェア攻撃を受け、数台のコンピュータシステムが侵入の被害に遭い、777型機の組み立てラインに影響が及ぶ事態となりました。[2]

バックオフィスでは、時間短縮とコスト削減のためにロボティックプロセスオートメーション（RPA）が導入され、自律型システムの利用が急速に拡大しています。同時に、さまざまなビジネスプロセスの標準化と合理化により、品質の向上にもつながっています。これには機械間のコミュニケーションが関わっており、たとえば、調達システムから在庫切れが発生しそうとの通知があった時点で、サプライヤーのコンピュータで商品の発注が自動で行われるといったことが可能になっています。

現在のセキュリティ戦略の勝利は、過去の戦績にすぎない

企業はサイバー犯罪との戦いに勝利しています。アクセンチュアの『2018年サイバーレジリエンスの現状』レポートによると、2018年には標的型攻撃の発生件数が2倍以上に増加したにもかかわらず、調査対象となった全業種合算でサイバー攻撃の成功率が30%から13%へと低下しています。[3]目覚ましい成果のように思えますが、阻止された攻撃のほとんどが既存のシステムに対する既知の脅威であった点にも注目しなければなりません。航空宇宙・防衛企業は、国家によるシステムへの侵入や、マルウェアやエクスプロイトコードの埋め込みなど、未知の脅威に対し、より大きな懸念を抱いています。実際、未来はすぐそこまで来ており、新たな脅威が今まさにもたらされようとしています。企業は、これらの新たなサイバーリスクについてまだ大局的な視点でとらえておらず、新しい環境で業務を行うために必要な対策や修復の計画も立てていないのが現状です。要するに、私達は過去の戦いに勝利しているのにすぎないのです。未来のビジネスのコネクテッドでインテリジェントな自律型システムによって生み出されるリスクに対しては、適切な防御がいまだ構築されていないのです。

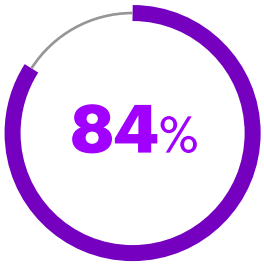
明日の戦いに勝利するには、今日のセキュリティアプローチでは不十分です。ほとんどの企業において、セキュリティは独立した機能部門として、主要なITシステムと機密データを外部の組織や脅威から保護する業務にあたっています。

現在、サイバーセキュリティ予算の5割弱がOTセキュリティの保護にあてられています。また、標準的なセキュリティ戦略では脅威の検出と被害の最小化に重点が置かれており、開発段階でデジタル製品およびプロセスの安全性を高めることは行われていません。強力なDevSecOpsプログラムがあれば、セキュリティを最適化しつつ、コンプライアンス目標を容易に達成、維持できるようになります。そのためには、ソフトウェア開発のライフサイクルおよびその後の工程にセキュリティ対策を組み入れる権限を、開発者とアプリケーション管理者に委譲することが必要です。[4]

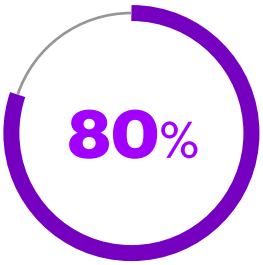
コネクテッドでインテリジェントな自律型企業には、広範囲のサイバーレジリエンスが求められます。それを実行するには、サイバー攻撃によりビジネス活動が妨げられないようにするための実証済みの方法を用いて、組織のあらゆる活動にセキュリティを統合することが必要です。セキュリティの専門知識をフロントラインに行きわたらせ、ITだけでなく、製品設計、ビジネスプロセス、従業員の日常業務にもセキュリティを組み込むようにします。経営層の84%が、セキュリティ/IT部門以外にサイバーセキュリティを組み込むには、新たなセキュリティ職務を追加する必要があると考えています（図2参照）。

図2：組織のセキュリティ職務についての航空宇宙・防衛企業経営幹部の見解

新たなセキュリティ職務を追加

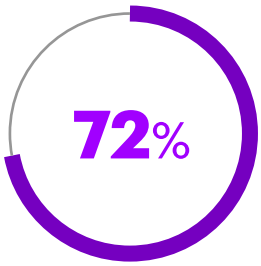


CXOの84%が、セキュリティ/IT部門以外（オペレーショナルテクノロジー、物理的セキュリティ）にサイバーセキュリティを組み込むために新たなセキュリティ職務を追加する必要があると考えています。

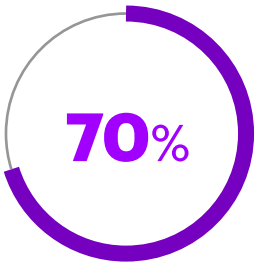


CXOの80%が、シームレスなコミュニケーションとビジネス整合性の確保のために、CISOとビジネスの橋渡し役をする幹部レベルの職務が必要であると考えています。

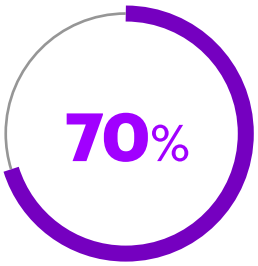
次世代のCISO職務の進化



CXOの72%が、CISOの職務は「権威ある執行者」から、他の経営幹部にとっての「インフルエンサー/コーチ」へと進化していくであろうと考えています。



CXOの70%が、ビジネスリーダーによる戦略、新規事業、新技術の導入に関する話し合いの場に、CISOも参加する必要があると考えています。



CXOの70%が、ビジネスリーダーをセキュリティに関与させ、セキュリティとビジネスとの関連性を高めるために、CISOがビジネスに十分精通する必要があると考えています。

リスクと防御のギャップを埋める

企業が考えるリスクと実際のサイバーセキュリティ態勢とのギャップは広がる一方です。多くの航空宇宙・防衛企業が、潜在的リスクへの恐れとそれらの持つ不確実性から、新興技術の導入を躊躇しています。また、これらの企業は変化の受け入れを拒む文化を持つ傾向にあります。経営層が新たな懸念分野であると述べている事柄と、防御のために企業が採用しているサイバーセキュリティ戦略との間には、ずれがあります。たとえば、企業はサードパーティとやりとりするデータの量が増加していることはリスクであると述べる一方で、自社の業務活動を超えた範囲でデータの整合性を確保できている企業はごくわずかです。航空宇宙・防衛企業の52%が、サードパーティのプロトコルに依存しているか、もしくは共有する情報を相手が保護してくれるはずだと信頼しています。

図3にあるように、今回の調査によって、リスクが拡大しているという認識と、現在のサイバーセキュリティ戦略によって得られる防御との間のギャップに一貫したパターンがあることが分かってきました。たとえば、75%の企業がクラウドサービスによってサイバーリスクが高まると考えているものの、サイバーセキュリティ戦略によってクラウド技術を保護しているとの回答は49%に留まっています。リスクと防御のギャップが特に大きな分野は、API、従業員の業績データの保護、スマート製品です。

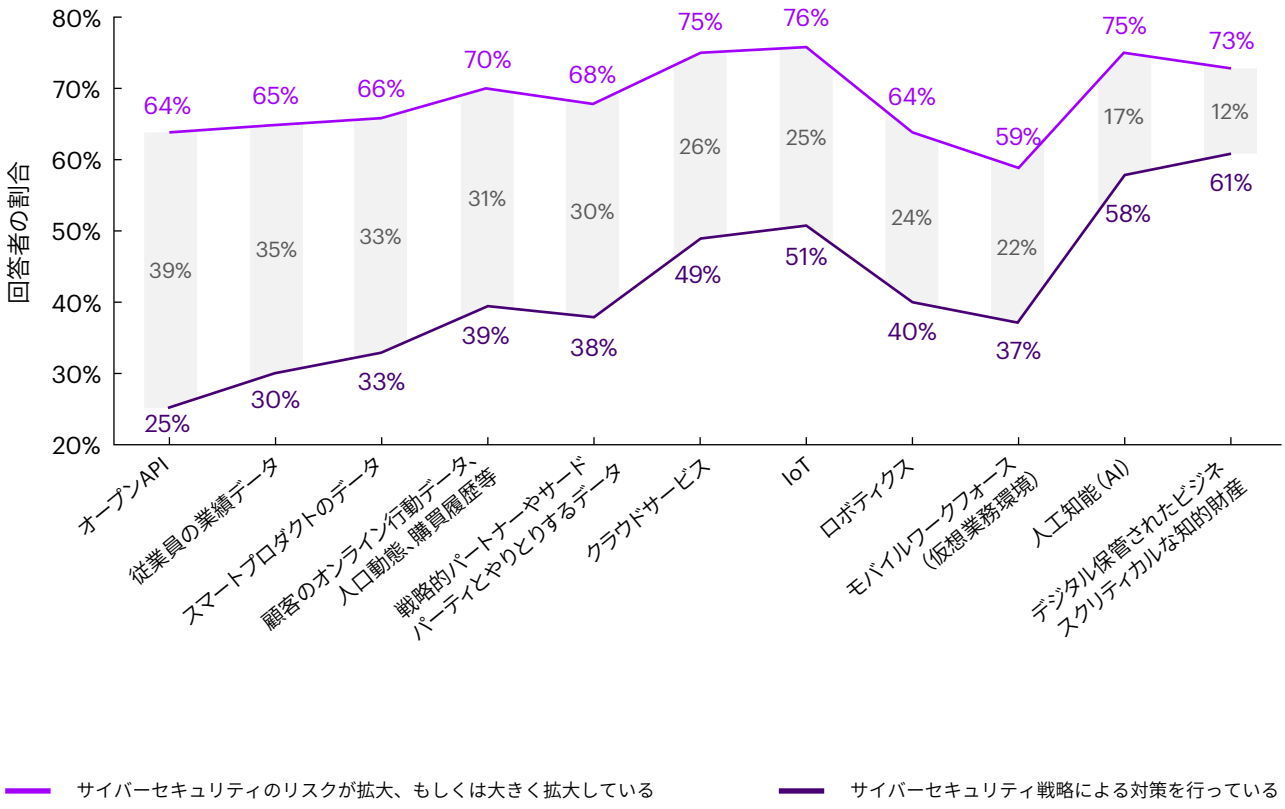
リスクが拡大しているという認識と、現在のサイバーセキュリティ戦略との間のギャップを埋めるには、サイバーセキュリティを計画、実行する方法を改訂する必要があります。

たとえば、航空宇宙・防衛企業の90%が、現在と過去の既知のリスクとセキュリティコンプライアンス要件のみに基づきサイバーセキュリティ投資を行っており、将来のビジネスニーズを考慮することなくサイバーセキュリティの投資計画を立てています。将来のビジネスによって生じる広範なリスクに対応するための効果的なガバナンスが構築されていないケースがほとんどです。多くの場合、その責任はCISOとサイバーセキュリティチームに委ねられています。

事業部門リーダーに依頼して、製品などの設計にセキュリティを組み込んでいるケースは稀です。事業部門リーダーがサイバーセキュリティの責任を担っているという組織はわずか31%しかありません。ほとんどの企業がCISOを雇用するか、サイバーセキュリティの職務をCIOなど幹部レベルのリーダーに割り当てているものの、多くの場合、これらのリーダーはセキュリティ組織を超えて十分な影響力を発揮できてはいません。たとえば、回答者の半数近くが、CISOが話し合いに加わるのは、新たなビジネスチャンスについて経営トップの合意が得られた「事後」であると述べています。

航空宇宙・防衛企業は、従業員の間にセキュリティ知識を広める取り組みを強化することで、広範囲のサイバーレジリエンスをサポートする「セキュリティファースト」の文化を生み出すことが可能です。入社時に全ての従業員にサイバーセキュリティの研修を受けてもらい、退職するまで定期的に最新の研修を受けられるようにしているとの回答は半数に留まっています。インサイダー脅威プログラムの制定や拡大が優先度の高い職責であることを認識しているCISOは52%です。

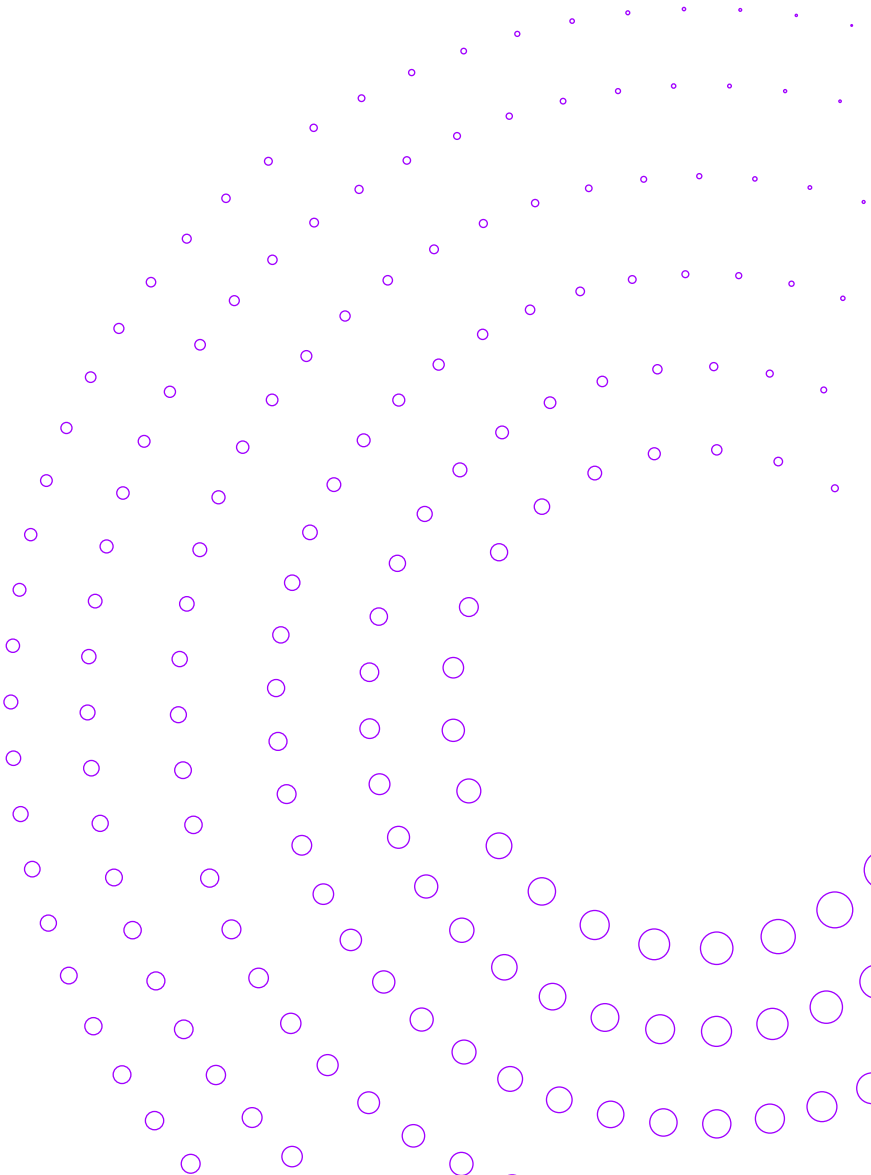
図3：リスクの拡大と実際のサイバーセキュリティ対策とのギャップ



未来を守るには

未来のビジネスをサイバーレジリエントなものにするには、新しいビジネスモデルやインテリジェント技術の導入に伴い発生するリスクに備えることが不可欠です。企業はセキュリティとビジネスを関連付けるだけでなく、ビジネスで――さらにはハッカー達により――利用されているのと同じインテリジェント技術を採用する必要があります。回答者の80%が、サイバーセキュリティのリスクは今後数年で大幅に低下すると考えています。ハードウェア認証、ユーザー行動分析、ディープラーニングなどの新しいサイバーセキュリティ技術によって、リスクの低減が可能になると見込まれます。

インテリジェントな企業が安全に成長するのに必要な広範囲のサイバーレジリエンスを構築するには、CISOの行う全てのことにセキュリティを組み込む必要があります。まずは、首尾一貫したサイバー戦略と、データガバナンスとデータ保護の重要課題にフォーカスした投資計画を立てることから始めると良いでしょう。セキュリティを社内全体に広め、組織、サプライヤー、パートナーの全てに広く説明責任を持たせるための構造的な変革を起こす必要があります。従業員と顧客に教育を施し、エンドツーエンドのセキュリティの強化に向けて、戦略的パートナー、サードパーティ、業界アライアンスと連携して取り組むことが求められます。



1 ビジネスリーダーを「レジリエンスリーダー」にするには

企業戦略、製品設計、予算、日常的なビジネス活動の全てにサイバーセキュリティが組み込まれている必要があります。

米国のある大手造船会社では、セキュリティの専門知識を組織全体に行きわたらせるために事業部門レベルでCISOを配置しています。

ビジネス戦略にセキュリティを考慮

セキュリティを事業戦略に取り入れる戦略の決定や選択肢の比較検討の際に、セキュリティを考慮するようにする必要があります。今回の調査では、航空宇宙・防衛企業で新規事業を検討する際、CISOが事前に関与するとの回答はわずか34%でした。セキュリティを後付けのように考えていたのでは、真にサイバーレジリエントな事業にすることはできません。サイバーセキュリティ侵害による影響は、他の財務リスク、ビジネスリスクによって企業が被る損害と同レベルのものであり、CEOや取締役による同等の戦略的配慮が必要です。

セキュリティの責任をフロントラインにまで広げる

今回の調査では、82%がサイバーセキュリティの担当者および活動を広く組織全体に行きわたらせる必要があると回答しています。しかし、79%の企業で、サイバーセキュリティが1カ所に集中したままの状態になっています。CISO以外の経営層の36%が、現在、事業部門リーダーがサイバーセキュリティの責任を担っていると述べており、将来的に事業部門リーダーが責任を担うべきであるとの回答もほぼ同数存在しました。一方で、このことを余分な負担ととらえている企業も一部存在します。その原因として、事業部門やIT部門でセキュリティを自分達の日常的な責任として受け入れるだけのリソース、スキル、関心が不足していることが挙げられます。

未来のレジリエンス予算へ賢明な決断を下す

未来のビジネスのための正しい防御を手にするには、まず予算とプランニングから始めなければなりません。現在、サイバーセキュリティ予算を割り当てる際に将来のニーズを評価しているという航空宇宙・防衛企業は10社に1社しかありません――残りの企業は、既知のリスクにのみ焦点を絞っています。IT、セキュリティ、事業部門のリーダーと連携して戦略的なサイバーセキュリティ計画を立てているという企業は1/4にも満たないのが現状です。

2 信頼できるビジネスイネーブラーとしてセキュリティリーダーをサポート

CISOが、多くの人に必要とされるコラボレーター、そして信頼できるパートナーになるには、事業部門と緊密に連携して、経営層の思い描く変革と成長の取り組みを実現させる必要があります。

セキュリティ人材をアップグレードし、事業部門と関連付ける

未来のビジネスの広範なニーズを反映させるためのアプローチの1つに、可能な限り幅広い文脈の中でセキュリティを監視し、セキュリティ部門と事業部門、およびCEOや取締役会との橋渡し役を務める「最高デジタルトラスト・セキュリティレジリエンス責任者（Chief Digital Trust, Security and Resilience Officer）」を設置するというものがあります。今回の調査では、80%を超える回答者が、CISOとビジネスのギャップを埋め、シームレスなコミュニケーションとビジネス整合性を確保するために、幹部レベルの職務が必要であると述べています。航空宇宙・防衛企業のCISOの半数近くが、組織の安全保護のためのCISOの責任が急速に拡大しており、セキュリティ問題に対処する能力が追い付いていないと認識しています。企業は、新しい製品やサービス、業務、プロセスにセキュリティを組み込むために、事業部門と連携して取り組むセキュリティの専門家の採用を今こそ検討すべきでしょう。

サイバーセキュリティの優先事項に関する明確なガイダンスを示す

CISOの責任とビジネスとの関連を理解するために経営幹部や取締役からどのようなことを教えてもらう必要があるかをたずねたところ、攻撃によって最も大きな損失を受ける事業分野を知ること、企業の持つ最も脆弱なデジタル資産を知ること、そしてサイバーセキュリティに対する経営幹部の関心を高めることの3つが、最優先事項として浮かび上がってきました。その一方で、サイバーセキュリティポリシーでビジネスに関連するリスクと高価値資産を特定するための正式なプロセスが定義されていると回答した経営層は46%に留まっています。

成功の評価基準を見直す

CISOがビジネスリーダーの強力なパートナーになった際には、サイバーセキュリティの成功を評価するための基準を拡大する必要があります。70%の企業が、コンプライアンス監査で用いる合格か不合格かの単純な基準を使ってサイバーレジリエンスを評価していると回答しています。CISOおよびセキュリティチームのための従来の評価基準は、脅威を検出し、それらに対応することを奨励するものになっています。しかし、サイバーセキュリティ機能が将来のビジネスに関連するリスクに対処できるか、サイバーレジリエンスの知識をフロントラインにまで広げることができているかといった、新たな基準を加えることが必要です。現在、2/3を超える回答者が、サイバーセキュリティの評価基準は専門的すぎてビジネスリーダーに理解してもらいにくいと考えています。

3 従業員をソリューションの一部にする

従業員が偶然もしくは意図的に攻撃をしかけるというのはよくあることです。侵害の発生を減らし、サイバーセキュリティを組織の中にしっかりと組み込むには、まず第１に、従業員がセキュリティの責任を担っていることをはっきりと示す必要があります。

Raytheon社では、従業員のサイバーセキュリティに対する意識を高める目的で、毎年「RTN Secure Week」を開催しています。あわせて、フルタイムの正式な高度教育プログラム「Cyber ELITE」を通して、従業員がサイバーセキュリティスキルを強化するための機会を設けています。[5]

現在、従業員がサイバーセキュリティの責任を担っていると回答したCISOはわずか12%でした。セキュリティの専門家はトレーニングとスキル強化（フィッシングメールテストなど）を継続的に行うだけでなく、リスクを定義し、それらに対処するのを支援するツールとインセンティブを従業員に提供する必要があります。効果的なインサイダー脅威プログラムを制定するには、組織のCEOとCIOが人事、人材開発、法務、ITのチームをとりまとめ、保安部門や事業部門と緊密に協力して必要な評価基準の策定と導入に取り組ませるようにしなければなりません。

安全な行動の強化とトレーニング

セキュリティファーストの考え方なくして、従業員が最弱リンクである状態を変えることはできません。新しい業務形態の広がり（請負業者やリモートワークの多用等）に伴い、従業員のトレーニングが喫緊のニーズとなっています。しかし、セキュリティを念頭に置いて考え、行動するためのトレーニングは、サイバーセキュリティ活動全体の中でも最も予算の割当額が少なくなっています。[6]企業は、有資格者向けのスキル強化策を含む、全従業員を対象とした基本的なトレーニングプログラムに注力する必要があります。

加えて、テクノロジーを活用することでユーザーの責任の重圧を減らすことも必要です。たとえば、パスワードの管理をユーザー任せにするのではなく、属性に基づくアクセス制御を利用するといったことが考えられます。

サイバーセキュリティチャンピオンを育てる

サイバーセキュリティチャンピオンは組織全体のセキュリティを主導するだけでなく、セキュリティプログラムの有効性について中央のチームにフィードバックを提供するという役目を担います。組織のあらゆるレベルでサイバーセキュリティチャンピオンを育て、セキュリティ組織以外の人材もサイバーセキュリティに関与させるようにする必要があります。

「セキュリティファースト」の行動に褒賞を与える

悪意ある行為や同僚の犯罪行為を報告した従業員に褒賞を与え、セキュリティを主導することに対するインセンティブを提供するようにします。サイバーセキュリティにコミットしているビジネスリーダーにインセンティブを提供している企業は34%に留まっています。褒賞は、サイバーセキュリティ・ハイジーン（サイバーセキュリティの衛生管理）に対する意識の向上を促すのに役立ちます。組織内のIT部門や事業部門では、ビジネス機能の停滞や中断（意図せぬサービスの妨害や中断など）を恐れ、セキュリティ対策が導入されなかったり、導入が遅れたりするケースがしばしば見られます。

強固な防御を確保する

トレーニングとスキル強化によって、従業員がうっかりサイバー犯罪に手を貸してしまうリスクを減らすことができます。たとえば、ユーザーおよびエンティティの行動分析（UEBA）システムは、犯罪の意思をうかがわせる異常なファイル伝送など、従業員の疑わしい行動に警告を与えられるようになっています。しかし、UEBAソリューションは複雑なため、多くの航空宇宙・防衛企業ではなかなか導入できずにいます。航空宇宙・防衛分野では、データの識別、分類、タギング、保護に関しても大きなギャップが生じています。企業が保護しようとしているデータの機密性に合った適切なレベルのセキュリティを提供するために、このようなギャップを解消するソリューションに注目が集まり始めています。

4 顧客の保護を主導する

企業にとって、顧客の要求に応じることは、リスク低減に次いで、2番目に緊急性の高い優先事項です。回答者の70%が、顧客の機密情報を会社で利用することが今後増えるであろうと考えていますが、現在のサイバーセキュリティプログラムにより顧客やパートナーの環境が適切に保護されているとの回答は51%に留まっています。しかし、データ保護に関しては、企業はコンプライアンスの枠を超えて、顧客を先導できるはずだと私達は考えます。

Thales社は、デジタルトラストプラットフォームT-SUREのもと、サイバーセキュリティコンサルティング、セキュアな通信製品および技術、運用制御サービスといった自社の能力を1つに統合しています。これにより、顧客がセキュリティを犠牲にすることなく、将来にわたって継続可能なレジリエントな方法でデジタル変革プロジェクトに着手できるよう支援しています。[7]

新たなセキュリティ規制に備える

顧客データの窃盗や乱用に対応するため、EU一般データ保護規則（GDPR）や米国国防省調達規則（DFARS）など、顧客保護のための新たな規則が規制機関により制定されています。これらの規制に違反した場合、現在および将来の契約の機会を失うだけでなく、違約金の支払いを命じられる可能性があります。[8]セキュリティ規制を順守するうえで重要な課題となるのが、サプライチェーン全体のセキュリティのギャップ、修復の状況、現在の強制措置について正確に把握することです。

顧客の自衛を支援する

顧客に自社のデータで何が起きているのかを知ってもらい、自衛の手段を伝えることで、顧客からの信頼を得ることができます。

5 自社だけでなく、エコシステム全体を考える

未来の企業は、世界中の数百から数千のサプライヤーやパートナーと電子取引を行うことになると考えられます。それらのいずれか1社を経由して、サイバー攻撃にさらされるという事態も起こりえます。戦略的パートナーやサードパーティとやりとりするデータがサイバーセキュリティ戦略により適切に保護されていると回答している航空宇宙・防衛企業はわずか38%です。したがって企業は、エコシステムパートナーと協力して、自社組織を共同で防御する必要があります。

Boeing社は、航空情報共有分析センター（ISAC）経由で、脅威に関する情報を業界の他の企業だけでなく、国家安全保障諸機関とも共有しています。[9]

BAE Systems社は、脅威インテリジェンスを共有するうえで企業が直面する課題に対応するために、サイバーセキュリティインテリジェンス・ネットワークの運用を開始しました。[10]

エコシステムのリスクを系統的に制御・管理する

書面による契約などの正式な仕組みとあわせて、非公式な手続きを制定することで、サプライヤー、パートナー、その他サードパーティとのしっかりとしたつながりを生み出し、維持することができます。組織に影響を与える実際のサプライチェーン攻撃のシミュレーションを定期的に実施することが必要です。また、サポートを必要としているパートナーやサプライヤーを支援するためのプログラムを導入し、サイバーハイジーンを向上させる必要があります。[11]

業界のセキュリティに関する取り組みに参加する

82%の回答者が、今後3年間で、同業他社と連携して、サイバーレジリエンスを向上させるための知識、サービス、製品を共有するようになるであろうと考えています。

このような情報共有の進展は、業界内のあらゆる組織の参加と標準の開発を具体化する機会にもなります。今回の調査により、一部でこれが実践されていることが判明しました。62%の企業が、コミュニティ内で連携することで、サイバーセキュリティ標準の策定に取り組んでいます。

まとめ：広範囲にわたるサイバーレジリエンスの構築

セキュリティが組織全体のコアコンピテンシーになるようにすることで、コネクテッドでインテリジェントな自律型企業の成功が確実なものになります。そうなれば、敵の侵入を食い止められるだけでなく、顧客やパートナーとの間に信頼関係が築かれます。ビジネスプロセスのサイバー脅威に対する回復力を高めることで、より高い競争力を身につけることができます。広範囲にわたるサイバーレジリエンスを確保することで、たとえサイバー攻撃を受けたとしても、日常業務や評判への影響を最小限に抑えられるという確信のもと、未来のビジネスを成長させることができます。

特に、政府と直接的、もしくは防衛関連企業を介して間接的に取引している組織では、サプライチェーン全体のセキュリティ管理を重点的に行う必要があります。技術アセスメントや対応/復旧計画を含むセキュリティ対策を必ず整備します。そうすることで、機密情報、資産、人材を保護するための措置が実際に講じられていることを政府に対して証明することができます。

参考文献

1.『2018年サイバーレジリエンスの現状』アクセンチュア、2018年4月 https://www.accenture.com/jp-ja/insights/security/2018-state-of-cyber-resilience-index

2. The Seattle Times (2018), Boeing hit by WannaCry virus: https://www.seattletimes.com/business/boeing-aerospace/boeing-hit-by-wannacry-virus-fears-it-could-cripple-some-jet-production/

3.『2018年サイバーレジリエンスの現状』アクセンチュア、2018年4月。https://www.accenture.com/jp-ja/insights/security/2018-state-of-cyber-resilience-index

4. NIST SP 800-171: Compliance through DevSecOpsに関する発表 アクセンチュアセキュリティ、2017年5月、於Aerospace Industries Association

5. Raytheon, Protecting Every Side of Cyber: https://www.raytheon.com/ responsibility/cyber

6. Security Awareness Training Explosion, Cybersecurity Ventures, February 6, 2017

7. Thales Group, Digital Trust: https:// www.thalesgroup.com/en/digital-trust

8. Cybersheath (2018), Understanding DFARS 252.204-7012 and NIST SP 800- 171: https://www.cybersheath.com/ understanding-dfars-252-204-7012-and- nist-sp-800-171/

9. Transportation Research Board, Aviation ISAC: http://trbcybersecurity.erau.edu/resources/01_14_16_Francy_TRB_Panel_ AISAC_FINAL.pdf

10. Bae Systems, The Intelligence Network: https://content.baesystems.com/theintelligencenetwork/uk

11. アクセンチュアセキュリティ・サイバーディフェンス：サプライチェーンディフェンスサービス

著者

Kelly Bissell：アクセンチュア・セキュリティのグローバルリードとして、クライアントのサイバーリスクに対するレジリエンスの構築、デジタルビジネスの成長の促進、安全なイノベーションを支援する取り組みを指揮しています。

Ryan LaSalle：アクセンチュア・セキュリティの北米部門マネジング・ディレクターとして、北米のセキュリティ事業全般を統括。クライアントのサイバーレジリエンスの向上を支援し、確実な成長を可能にすべく取り組んでいます。

Madhu Vazirani：インドのムンバイ事業所を拠点に、金融サービス分野のAPACリサーチリードとして活動しています。世界中の銀行・資本市場業界の戦略解析を定期的に実施しており、近年は新興市場のファイナンシャルインクルージョン（金融包摂）にも注目しています。

Roy Hu：アクセンチュア・セキュリティのプリンシパル・ディレクター。北米の航空宇宙・防衛業界のアクセンチュアセキュリティリードとして、セキュリティ事業を管理し、航空宇宙・防衛分野のクライアントに価値あるサービスを提供しています。

Aerospace and Defense

John Schmidt
Aerospace and Defense
Global Industry Lead

Marc Gelle
Aerospace and Defense
Europe Industry Lead

Jeffrey Wheless
Aerospace and Defense
Global Research Lead

Anshul Sharma
Aerospace and Defense
Research Associate Manager

調査概要

サイバーレジリエントな企業とは

今回の調査では、サイバーレジリエントな企業を、「サイバーセキュリティとビジネス継続性の両方の能力をあわせ持ち、脅威にすばやく対応し、被害を最小限に抑え、攻撃を受けている最中も事業を継続するための戦略を有する組織」と定義しています。このような特徴によって、サイバーレジリエントな企業は、デジタルビジネスモデルにおけるイノベーションを推し進め、顧客の信頼を高め、確実に成長していくことが可能です。

調査について

2018年の初め、アクセンチュア・セキュリティは経営層1,460人（航空宇宙・防衛分野のサンプル数100）を対象に、新たなビジネスイニシアチブでセキュリティにどの程度重点を置いているのか、未来のビジネスニーズに対応したセキュリティ計画になっているのか、どのようなセキュリティ能力を有しているのか、セキュリティに関して社内外でどの程度連携しているのかを調査しました。調査対象者は、南北アメリカ、ヨーロッパ、アジア太平洋地域の16カ国、14業界の、年間売上高10億ドル以上の企業の代表者です。回答者の半数が最高情報セキュリティ責任者もしくは同等の役職に就いており、残りの半数はCEOおよびその他の経営幹部となっています。

アクセンチュアについて

アクセンチュアは「ストラテジー」「コンサルティング」「デジタル」「テクノロジー」「オペレーションズ」の5つの領域で幅広いサービスとソリューションを提供する世界最大級の総合コンサルティング企業です。世界最大の規模を誇るデリバリーネットワークに裏打ちされた、40を超す業界とあらゆる業務に対応可能な豊富な経験と専門スキルなどの強みを生かし、ビジネスとテクノロジーを融合させて、お客様のハイパフォーマンス実現と、持続可能な価値創出を支援しています。世界120カ国以上のお客様にサービスを提供する49万2,000人の社員が、イノベーションの創出と世界中の人々のより豊かな生活の実現に取り組んでいます。

アクセンチュアの詳細はwww.accenture.comを、アクセンチュア株式会社の詳細はwww.accenture.com/jpをご覧ください。