Benchmark Insights

—

旅行業界向けの IIoT サイバーセキュリティー

セキュリティーの脅威から
旅行業界を守る

IBM **Institute for Business Value**

IBM

IBM にできること

十分なセキュリティーを担保せずに、インターネット接続を行う物理サーバーを監視･制御することは、リスクが高く、結果としてコストが高くなります。IoT を利用した旅行業務がサイバー攻撃を受ければ、壊滅的な被害を招く恐れがあります。しかし、こうしたリスクの多くは対処が可能で軽減することができます。サイバー攻撃の対象領域は広がる一方ですが、IBM は旅行業界の経営層が、この問題に対処できるよう支援します。私たちはセキュリティー分野にコグニティブなアプローチを取り入れることで、重要なインフラ資産を保護しながら、各種のプラットフォームやエコシステムをサポートする新しいサービスを提供します。IBM が有するセキュリティー専門家の世界的なネットワークは、資産やプロセスを保護し、業界の品質面の課題に貢献することができます。コグニティブ･アプローチにより、セキュリティー･リスクの低減を支援します。詳細については、ibm.com/industries/travel-transportation をご覧ください。

著者
Lisa-Giane Fisher
Greg Land
Eric Maass
Julian Meyrick
Gerald Parham
Steve Peterson

主なポイント

IIoT のメリットを実現するためには、コストが高くなることを覚悟しなくてはならない

旅行関連企業の多くは、複雑な業務を管理するために、IIoT（産業用の IoT）ソリューションを活用している。旅行業界におけるサイバーセキュリティー・インシデントのうち、3 分の 1 は IIoT 関連のものになる。旅行関連企業の業務は、適切な保護がなければ、サイバー攻撃により、壊滅的なダメージを受ける恐れがある。

レガシー・システムにおける脆弱性は、重大なリスクを伴う

多くの旅行関連企業は、いまだ旧来の産業用制御システムに依存しており、その中には致命的な脆弱性を抱えるシステムも含まれている。これらのシステムはアップデートが難しく、本質的に安全ではない。ところが業務の遂行上、これらのシステムに、IIoT デバイスを接続して運用する企業が少なくない（旅行者が利用する場合もある）。

サイバー・レジリエンスを向上させる、10 の対策とプラクティス

今回の調査で我々は、企業が予防、検知、および対応の能力を向上させるのに役立つ、具体的なセキュリティー対策と AI を活用したプラクティスを明らかにした。これらを活用すれば、企業は IIoT 関連のサイバー攻撃に迅速に対処し、被害を軽減し、復旧することができるようになる。

新型コロナウイルス感染症の危機の結果、世界中で旅行者が激減し、旅行業界の就労者の数が減少したが、航空業界に対する脅威はとどまることを知らない。その一例が、2020 年 3 月にサンフランシスコ国際空港で発生したデータ流出事件である。報道によると、この攻撃は、ロシア政府から支援を受けたハッカー集団「Dragonfly」によるものとされる。[1] この集団は、重要なインフラ組織をターゲットに、偵察、ラテラル・ムーブメント、サイバー・スパイ活動を行っている。[2]

旅行・運輸関連の企業が、重要インフラを維持し、その安全性を確保することは、常に大きな課題となっていた。ここに、新型コロナウイルス感染症の問題が加わったことで、企業のセキュリティーやレジリエンス、そして事業継続の計画は今や限界に達しつつある。業界はやがてコロナ禍から回復するだろうが、サイバー攻撃から完全に免れられる日は、永遠にやって来ないだろう。このグローバルな課題を克服するためには、優れた適応力、革新的なセキュリティー、およびリスク管理の実践が必要だ。

旅行業界は、悪意ある攻撃者にとって魅力的なターゲットだ。業務を円滑に進めるための情報技術（IT）への依存、サードパーティー・ベンダーとの提携、そしてグローバルに広がる旅行サプライチェーンへの参加は、結果として大規模かつ多様な攻撃の対象領域を広げているからだ。

自動化を可能にする IIoT プラットフォームやデータ・サービスへの依存度が高まるにつれ、新たな脆弱性が誕生する。外部のプラットフォームやサービスを利用することで、自社が管理するデータやシステムへの不正アクセスが起きる可能性は高まり、物的資産を破壊される危険性が生まれる。攻撃者が金銭的な動機を持ったサイバー犯罪者であれ、政治的な意図を持った国家であれ、旅行業界の一部が攻撃されただけで、旅行業界全体、ひいては世界経済全体に、深刻な影響を及ぼす恐れさえあるのだ。

攻撃者の数は増えており、短期間で集中的に脆弱性を突かれると、リスクは指数関数的に増大する。その被害は前例のない水準にまで達してしまう可能性さえあるのだ。2001 年 9 月 11 日に米国で発生した同時多発テロが壊滅的な被害をもたらした要因の 1 つは、テロリストが複数の安全・セキュリティー・プロトコルを巧みに回避し、さらに複数の攻撃を同時かつ複合的に実行したからだ。このテロ行為における被害額は、物的損害だけでも 1,000 億米ドル近くに上り、経済的損失の総額は 2 兆米ドルに達すると試算されている。[3]

68%

の旅行関連企業の経営層が、DDoS 攻撃は IIoT 関連の最大の脅威であると回答している

59%

のセキュリティー対策のリーダー的企業が、IIoT コンポーネントが危険にさらされた場合の対応策をインシデント対応計画に盛り込んでいるが、その他の企業では、34% にとどまっている

2 倍

IIoT 関連のインシデントやセキュリティー侵害の検知、対応、および復旧作業を積極的に行っている企業はその他の企業と比べて 2 倍以上の速さで実施できる

エコシステムが拡大するほど、個別の企業は脆弱化する。にもかかわらず、旅行業界全体でイノベーションが続いているため、業界のエコシステムは拡大する一方であり、進化はこれからも続くだろう。ゆえに将来に備えるため、旅行関連企業はサイバー・レジリエンスの向上に、今すぐ注力しなくてはならない。

今回、IBM が実施した調査を分析した結果、IIoT のサイバーセキュリティー・パフォーマンスにプラスの影響を与える 10 の対策、および AI を活用したプラクティスが明らかになった。これらは、Center for Internet Security（CIS）の重要セキュリティー項目と、IBM の IoT セキュリティー研究から得た AI 主導型プラクティスを組み合わせたものである。[6] 本レポートでは、旅行関連企業がどうすればこれらのセキュリティー対策を導入できるかについて提案を行う。次の 2 段階のアプローチを踏めば、IIoT のサイバーセキュリティー体制とレジリエンスの向上が実現できるはずだ。

フェーズ 1：IIoT のサイバーセキュリティーの戦略とプログラムを定義し、さらに実施する。その後、効果的な保護や予防の対策やプラクティスを実践することで、強固な防御基盤を確立する。

フェーズ 2：効果的に検知、対応、復旧を管理する。自動化された対応機能を構築し、さらにテストすることで、大規模な旅行セキュリティーの自動化が実現できる。

旅行業界は、
悪意ある攻撃者にとって
魅力的な標的である。

旅行業界における IIoT 技術：状況は混沌

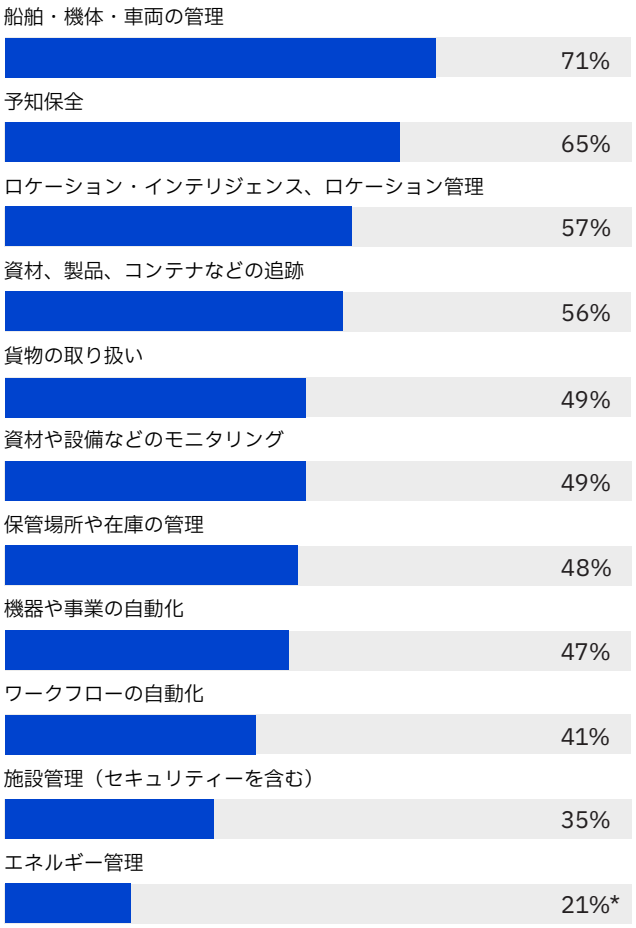
旅行関連の企業は、IIoT 技術を業界全体で幅広く適用している。例えば航空会社や地上交通機関におけるオペレーション業務はもちろんのこと、旅行代理店、ツアー業者、旅行仲介業者の販売、マーケティング、顧客サービス業務など、さまざまな分野で活用している。しかし旅行関連企業が、サイバーセキュリティー・リスクについてどの程度理解しているのか、またリスクを軽減する機能にどれほど成熟しているか、その有効性はどれほどなのかについては明らかにされていない。

IBM Institute for Business Value（IBV）は、旅行関連の企業各社のセキュリティーやサイバー・レジリエンスを比較して理解を深めるために、Oxford Economics 社の協力を得て、世界 11 地域にある旅行・運輸会社の IT およびオペレーショナル技術（OT）のリーダー 300 人を対象として調査を実施した（そのうち 75 人は旅行業界）。インタビューを受けたリーダーらは、各組織の IIoT の導入と環境セキュリティー部門の責任者である（「調査方法」のセクションを参照）。

今回の調査結果において、幅広い機能分野で IIoT 技術の導入が、急速に進んでいることが確認された。多くの企業は、これらのテクノロジーを自社のサプライチェーンやロジスティクスのプロセス（車両管理、予知保全、ロケーション管理など）に適用できるよう、日々模索している（図 1 参照）。

図 1

旅行業務における IIoT 技術の利用方法



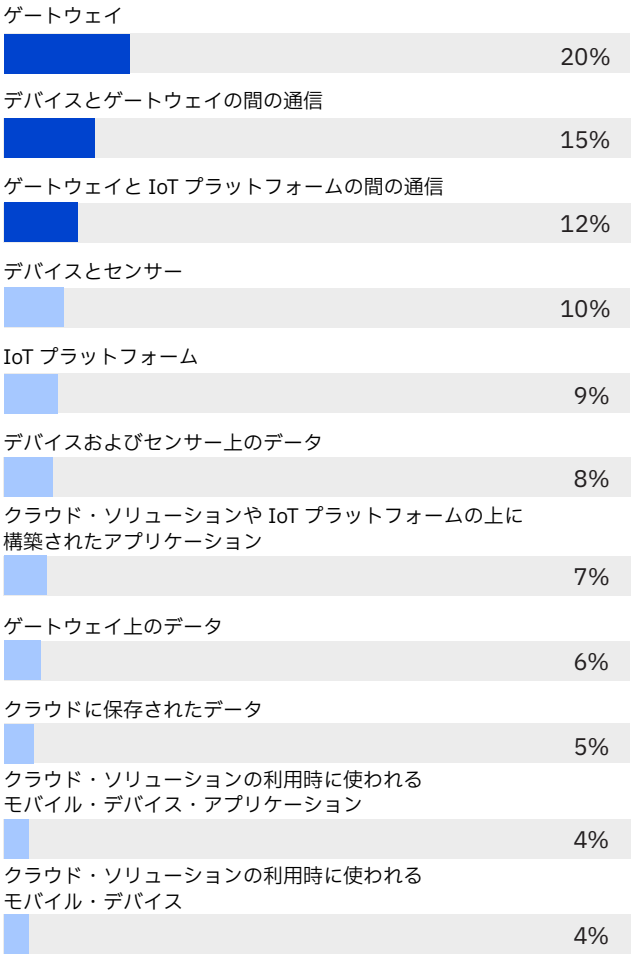
出典：IBM Institute for Business Value のベンチマーク調査、2019 年
* すべての図において、アスタリスクは、n 数が少ない（n<20）ことを示す。これらのデータは、統計的な信頼性は高くないものの、他の回答との比較において、一定の方向性は示されている。
Q：貴社の業務において、IoT 技術はどのように利用されていますか。当てはまるものをすべて選択してください。

多くの旅行関連企業は、IIoT 技術を導入しているがセキュリティーの担保が追い付いていない。

ところで経営層は、自社の業務ネットワークと外部企業のネットワーク、および IIoT ネットワークの間を行き交う情報のセキュリティーに不安を感じている。旅行関連企業の回答によると、最も脆弱な IIoT コンポーネントは、ゲートウェイとゲートウェイに関わる接続性であり、回答の半分近くを占めていた（図 2 参照）。

図 2

IIoT の展開における、最も脆弱な部分



出典：IBM Institute for Business Value のベンチマーク調査、2019 年
Q：貴社が導入している IoT ソリューションで、最も脆弱な部分はどこですか。1 つ選択してください。

インターネットなどの公共ネットワークに接続する物理サーバーを監視･制御するためのシステムにはリスクが生まれる。特にシステムが、広範なセキュリティー･ガバナンス･ポリシーに基づくセキュリティーで保護されていない場合、リスクはさらに高まる。潜在的なリスクとして、データの漏洩による個人への影響や、消費者からの信頼低下などが挙げられる。

すでにリスクを認識している旅行関連企業も存在するが、多くはセキュリティーを担保しないまま、IIoT 技術を導入している。その結果、設定や制御に隙が生じ、悪用される可能性が生じている。今回の調査では、経営層の 3 分の 2 近くが、IIoT 対応の新しい商品やサービスを提供する最低限の能力は持っていると回答している。しかし、それらを安全な方法で提供できると答えた経営層は、半数にとどまった。以上の結果は、運用インフラのセキュリティーの隙からリスクが生じる可能性があることを如実に示している。

本調査では、さまざまな場面におけるサイバーセキュリティーのリスクを、発生する可能性と潜在的な影響の両方に基づいて、回答者に評価してもらった（図 3 参照）。旅行関連企業の経営層が最も懸念しているリスクは、以下の通りだ。

顧客データの漏洩

旅行関連企業の経営層が、IIoT サイバーセキュリティーの 2 大リスクの 1 つとして挙げるのは、旅行者の顧客データの漏洩だ。一旦データが漏洩すると、社会関係的な責任が発生するだけでなく、多額の金銭上の負担も生じることになる。

一例として、2019 年、某大手航空会社の 50 万人分の顧客情報が漏洩した事件が挙げられる。同社には EU 一般データ保護規則（GDPR）に違反したとされ、2 億 3,000 万米ドルの罰金を科された。同社のセキュリティー体制は不十分であり、そのためログイン情報、決済カード、旅行予約情報のほか、氏名や住所などのさまざまな個人情報が流出した。この罰金の金額は、同社の年間総売上高の 1.5% に相当し、英国情報コミッショナーズ･オフィス（IOC）がデータ漏洩企業に科した罰金の最高額でもある。[7]

ブランドへのダメージと社会的信用の失墜

旅行業界へのサイバー攻撃が成功すると、データが漏洩し、業務が中断するだけでなく、人身事故につながる可能性が生じる。このことによる企業の評判への悪影響は、計り知れない。

一旦事故が起きると、ブランドの信頼や信用が損なわれるだけでなく、将来のビジネスや顧客との関係も修復不能なほどのダメージを受ける。当然のことだが、ブランドや社会的信用への影響を、回答者は IIoT 関連の 2 大リスクの 1 つとして挙げている。

知的財産（IP）の侵害

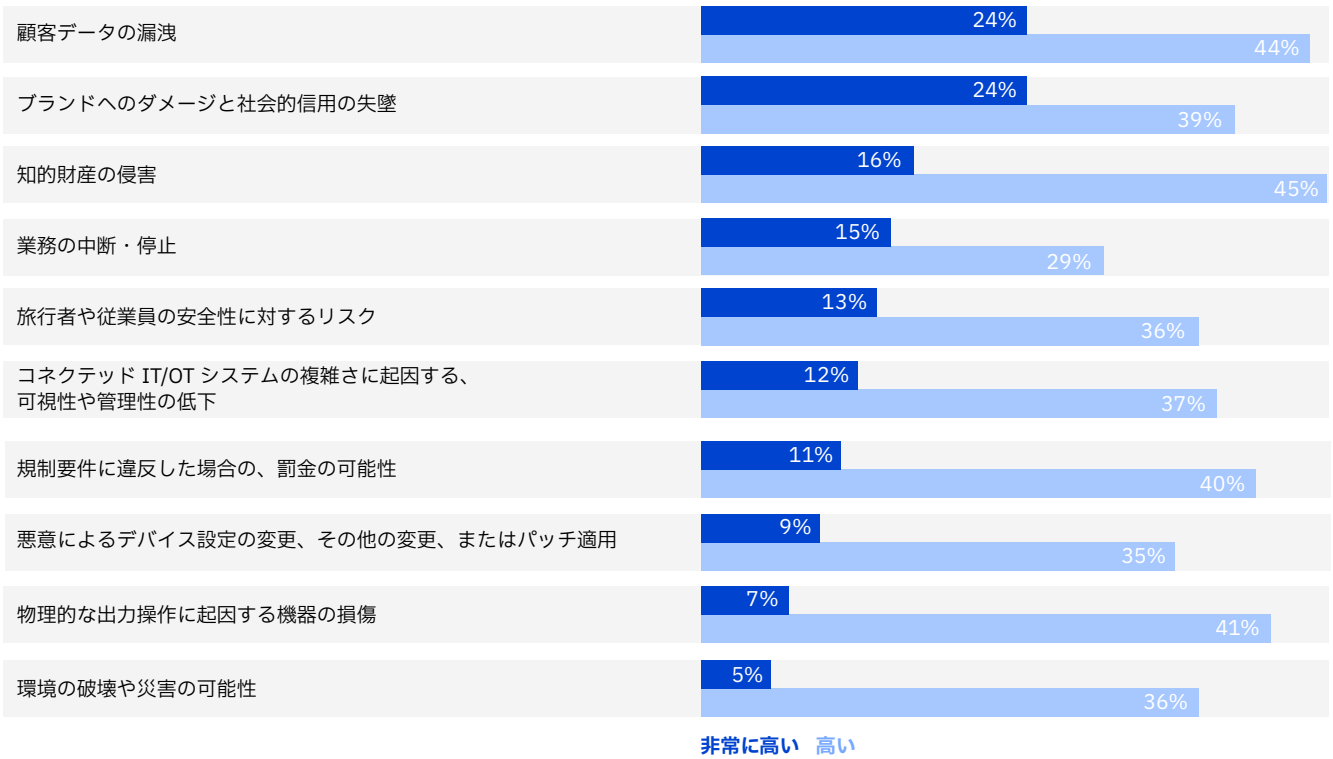
多くの旅行関連企業は、差別化を図る目的で、ブランド資産や独自の知的財産を構築するために、多額の投資を行っている。商標、地理的表示（認証マーク、団体商標、または独自システム）、工業意匠、そして特許、著作権、企業秘密などのさまざまな形の知的財産（IP）は、競争力の源泉である。旅行関連企業の経営層は、IP の盗難が将来の自社の成長に与える影響を認識しており、IIoT セキュリティー・リスクの第 3 位に挙げている。

業務の中断・停止

旅行関連企業の経営層の 15% は、業務の中断を非常に高いリスクと考えている。2016 年には、サンフランシスコの路面電車システムがマルウェア攻撃を受けた。組織内の電子メールやバックオフィスのコンピューター・システムがハッカーに乗っ取られ、盗まれたデータの引き換えとして、ビットコインが要求された。[8]

図 3

IIoT サイバーセキュリティー・リスクの評価（リスクが非常に高い順）



出典：IBM Institute for Business Value のベンチマーク調査、2019 年
Q：貴社において、以下の各 IoT サイバーセキュリティー・リスクが発生する確率と、発生した場合に貴社が受ける影響は、どの程度ですか。各リスクの発生確率と影響度を 1 ～ 5（1 ＝非常に低い、2 ＝低い、3 ＝中程度、4 ＝高い、5 ＝非常に高い）で評価してください。

アトランタ市の交通局も、ランサムウェア攻撃を受けた結果、数カ月にわたってサービスが停止し、復旧のために要した費用は260 万米ドルにもなった。[9] また物流業者の場合も同様の被害が想定され、経路システムがウイルス攻撃を受ければ、全トラックの運用が麻痺してしまう可能性がある。

旅行者や従業員の安全性に対するリスク

旅行関連企業の経営層の 13% が、旅行者や従業員が危険にさらされるリスクは非常に高いと回答している。信号機のタイミングが数秒でも狂ってしまえば、けがや死亡につながる事故が発生するかもしれない。また、鉄道の信号などを制御する機械的･電気的な装置の改ざんがあった場合でも、同様の結果を招く可能性がある。

例えば、ポーランドのウッチ市に住む 14 歳の少年は、テレビのリモコンを改造したデバイスを使って、鉄道のポイントを切り替える装置に不正な指示を行った。その結果、4 台の車両が脱線し、12 人が負傷するようなことも起こっている。[10]

IIoT セキュリティーを改善するための 2 段階のアプローチ

我々は今回の調査データに基づき、各社の IIoT サイバーセキュリティー予算、セキュリティー対策による既知の脆弱性への対応、その復旧にかかる時間から、「セキュリティー･リーダー」と呼ぶ企業グループを特定した（関連コラム「洞察：数字で見るセキュリティー･リーダー」を参照）。調査の結果、セキュリティー･リーダーは、IIoT サイバーセキュリティー･リスクを詳細に評価しており、リスクを軽減するために必要なサイバーセキュリティー能力の必要性についても深く理解していることが明らかになった。

このような企業は、セキュリティー KPI のパフォーマンス指標が高く、自社の脆弱性管理機能は最新の脅威から自社を守っているという自信を持っている。また、セキュリティー管理を、非常に効果的な「イネーブラー」や「プロテクター」と見なす傾向が強い。[11] しかし「セキュリティー･リーダー」の最大の特徴は、サイバー･レジリエンスであり、IIoT 関連インシデントの検知、対応、復旧を他社の 2 倍以上の速さで実施できる点である。

洞察：数字で見るセキュリティー･リーダー

「セキュリティー･リーダー」には、旅行業界だけでなく、運輸業界の企業も含まれる。調査対象の 300 社のうち、59 社がこのグループに属し、そのうち 23 社が旅行業界の企業だった。これらの企業は、以下の 3 つの指標において、平均して上位 20% のパフォーマンスを発揮できるものと定義される。

1. サイバーセキュリティー予算に占める IIoT 関連の割合。
2. 既知の IIoT 脆弱性に対し、セキュリティー対策を実施している割合。
3. IIoT サイバーセキュリティー･インシデントへの対応と復旧にかかるサイクル･タイム。

本調査における「セキュリティー･リーダー」は、旅行関連企業 23 社を含む 59 社だった。「その他の企業」は、残りの 241 社の旅行関連企業と運輸会社だ。

2 段階のアプローチにより、IIoT のサイバーセキュリティー体制とレジリエンスを改善。

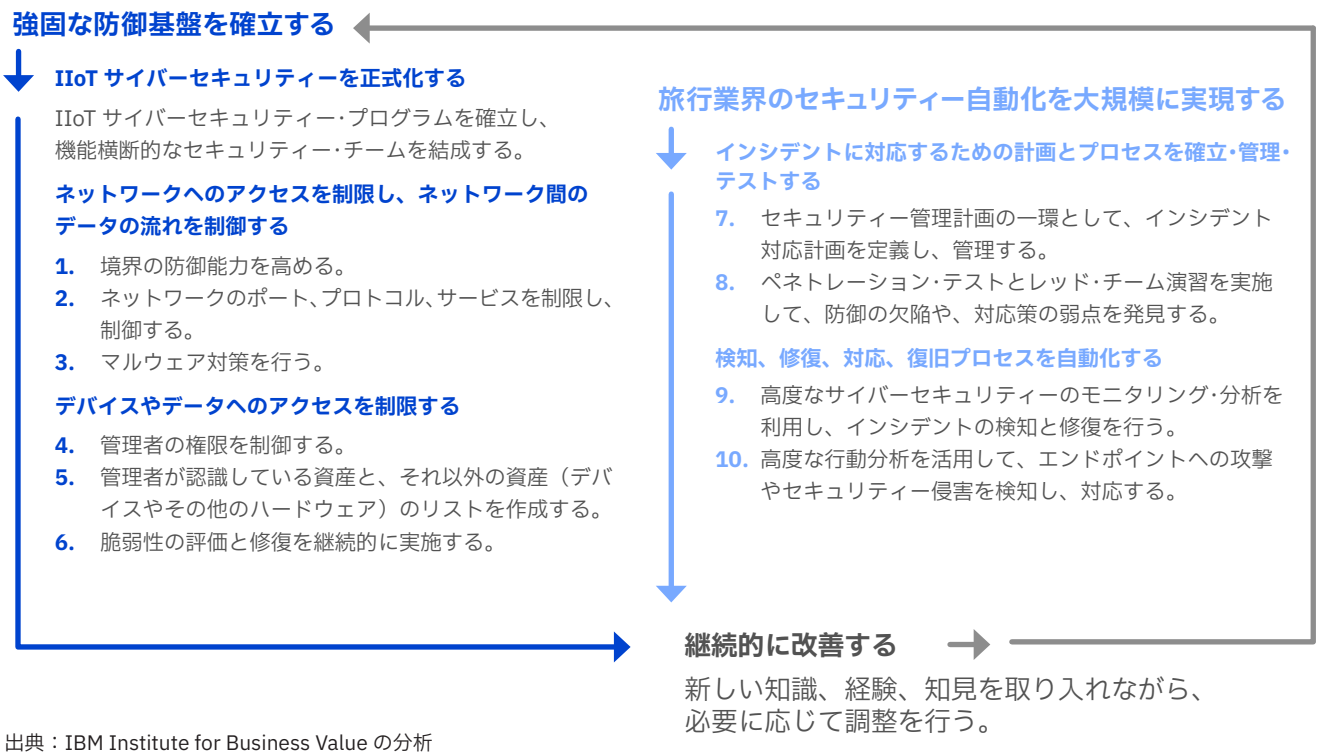
このパフォーマンスは、Center for Internet Security（CIS）の重要セキュリティー対策（Critical Security Controls）と、多くの旅行関連企業が採用しているより高度な AI を活用したプラクティスとの組み合わせを適切に実行できているかどうかによって、大きく左右される。[12] Critical Security Controls には、合計 10 の項目があり、それぞれが保護と予防や検知、対応、復旧などのセキュリティー機能に関連している。IBM は、これらの極めて効果的な対策とプラクティスを実施し、IIoT のサイバーセキュリティー体制とレジリエンスを向上させるための、2 段階のアプローチを推奨している（図 4 参照）。

IIoT の強固な防御基盤を確立する

第 1 フェーズは、3 つの指令で構成されている。第 1 の指令は、IIoT のサイバーセキュリティー戦略と計画の策定を促進することだ。このためには組織の広範な IT および OT のリスクと、セキュリティーのフレームワークを整合させる必要がある。第 2 と第 3 の指令は、効果的な保護や予防の対策を講じ、プラクティス（およびそれらに関連するテクノロジー）を利用して、防御能力を強化することである。

図 4

IIoT のサイバーセキュリティー体制とレジリエンスを向上させるための 2 段階のアプローチ



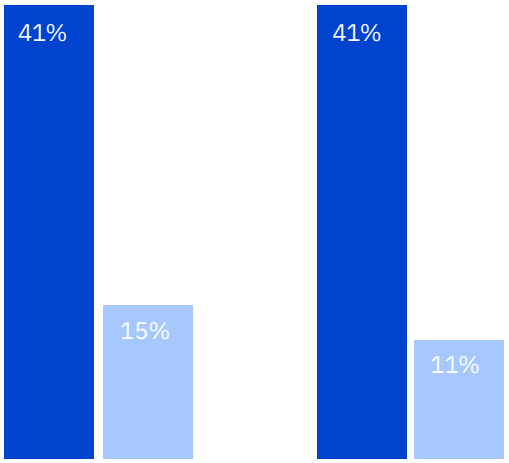
出典：IBM Institute for Business Value の分析

IIoT サイバーセキュリティーを正式化する

旅行関連企業は、効果的な IIoT サイバーセキュリティー・プログラムを導入すれば、必要な IIoT サイバーセキュリティーのツール、プロセス、スキルを定義・管理・更新することが可能になる。セキュリティー・リーダーの 41% がこうしたプログラムを構築していたが、その他の企業では、その割合は 15% にとどまった（図 5 参照）。IIoT 関連のリスクは、旅行関連企業の広範なセキュリティー・リスクの管理フレームワークの一部として対処するべきだ（関連コラム「洞察：IIoT リスクを管理するためのフレームワーク」を参照）。そのためには、まずリスクを評価し、優先順位を付けることから着手する。次にリスクを可視化し、IT および OT 分野にまたがる共通のリスク・アプローチを用いて、企業レベルで管理すること。そしてコネクテッド ICS を含む IIoT 環境における脆弱性を特定し、定期的なリスク評価を実施する。最後に脆弱性を軽減する計画を文書化し、実行する。

図 5

IIoT サイバーセキュリティーを正式化する



出典：IBM Institute for Business Value のベンチマーク調査、2019 年
Q：貴社の IoT サイバーセキュリティーに対する理解を表す記述として、最も当てはまるものは以下のうちどれですか。
Q：貴社は、IoT サイバーセキュリティー・リスクを軽減するために、以下の運用アプローチをどの程度実施していますか。
注：図 5 ～ 9 は、回答時に「4 ＝現在展開中」または「5 ＝完全に実施済み」を選択した企業を示す。

洞察：IIoT リスクを管理するためのフレームワーク

米国標準技術研究所（NIST）の「重要インフラ・サイバーセキュリティーのためのフレームワーク」と、「ISO/IEC 27000-1」など、セキュリティーとガバナンスのフレームワークを組み合わせて、以下を実行する。

- 重要なデータ、資産、およびセキュリティーの境界線を特定する。
- IIoT システム、コネクテッド本番環境、および人材資産における脆弱性を特定する。
- リスク管理のフレームワークを構築し、カスタマイズする。
- リスクを評価し、それらのリスクを軽減するための計画を文書化して実行する。
- 投資を確保し、最も緊急性の高いセキュリティー施策の、進捗状況を伝達する。
- 許容できるリスク・レベルと、ビジネス目標やコンプライアンス要件との間でバランスを取る。[13]

今日では、IIoT デバイスや
プラットフォームに特化した
マルウェアが出回っている。

セキュリティー・リーダーの 41% は、旅行関連企業が機能横断的に俯瞰すれば、IIoT システム、企業の IT システム、および業務用機器の違いをより明確に理解できるようになると認識している（図 5 参照）。旅行関連企業が、IT セキュリティー、エンジニアリング、オペレーション、制御システムやセキュリティーのベンダーからなる横断的なセキュリティー・チームを結成すれば、IT と OT の専門知識を活用して、最適なリスク軽減のための適正なセキュリティー対策の優先順位付けを行うことが可能になる。[14]

ネットワークへのアクセスを制限し、ネットワーク間のデータの流れを制御する

IIoT デバイスが生成する膨大な量のデータは、企業間のネットワークや、保護の不十分な IIoT ネットワークの間を自由に行き来する。一貫したセキュリティー体制を維持するためには、役割と権限を定義し、ネットワークへのアクセスを制限し、ネットワーク間のデータの流れを制御することが不可欠だ。その際に効果的な対策は、以下の 3 つである。

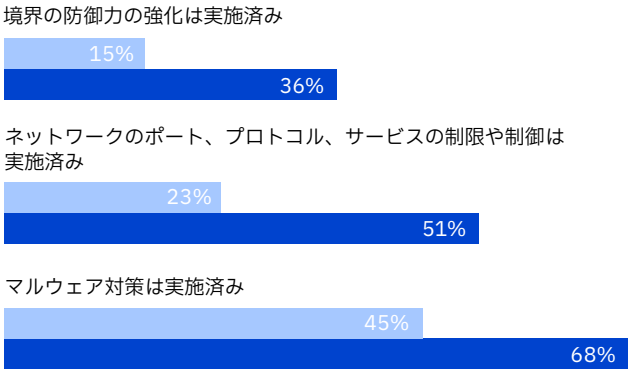
1. 境界の防御能力を高める：今回の調査によると、IIoT のサイバーセキュリティー・パフォーマンスに最も大きな影響を与えるのが、この防御策だ。特にセキュリティー上有害なデータに焦点を当てながら、信頼度が異なるネットワーク間の情報の流れを検知し、予防や修正を行う。分離戦略を活用し、IIoT コンポーネントを独自のゾーン内、または独自の別ネットワーク上で動作させている企業の数は、セキュリティー・リーダーではその他の企業の 2 倍だった（図 6 参照）。[15] この防御策を採用すれば、信頼性の低い IIoT ネットワークが安全性の高い企業の IT ネットワークに対して与え得る悪影響を軽減することができる。

2. ネットワークのポート、プロトコル、サービスを制限し、制御する：今回の調査では、その他の企業と比べて 2 倍以上の数のセキュリティー・リーダーが、自社の業務環境の IIoT デバイスで使われる可能性があるポート、プロトコル、およびサービスを積極的に定義し、適用していることが判明した（図 6 参照）。デバイスによっては、企業のネットワークに乗らない Bluetooth などの通信プロトコルが実装されている場合もあり、各デバイスで使われているプロトコル（つまり、どのプロトコルが自社のセキュリティー・ポリシーに沿っているか）を完全に把握すれば、脆弱性の風穴を大幅に縮小することができる。そのためには IIoT デバイスをテストし、セキュリティー・ポリシーに当てはまらないデータ移行が、どれほど影響を与えるかについて評価を行うべきだ。[16]

3. マルウェア対策を行う：今日では、IIoT デバイスやプラットフォームに特化したタイプのマルウェアやエクスプロイトが出回るようになっている。そのため、悪意あるコードのインストール、拡散、実行を制御する戦略を、組織全体の複数ポイントで構築する必要がある。IIoT デバイスの情報（アップデートやデータ）が流れるゲートウェイを継続的に監視し、マルウェアを検知する。さらに観測されたアクティビティーを適正なアクティビティーと相互に関連付けることで、悪意の攻撃から組織を防御しなくてはならない。

図 6

ネットワークへのアクセスを制限し、ネットワーク間のデータの流れを制御する



出典：IBM Institute for Business Value のベンチマーク調査、2019 年
Q：IoT サイバーセキュリティー・リスクを軽減するため、以下の重要なセキュリティー対策をどの程度実施していますか。

重要なシステムへのアクセス権がある従業員は、ハッカーの標的になりやすい。

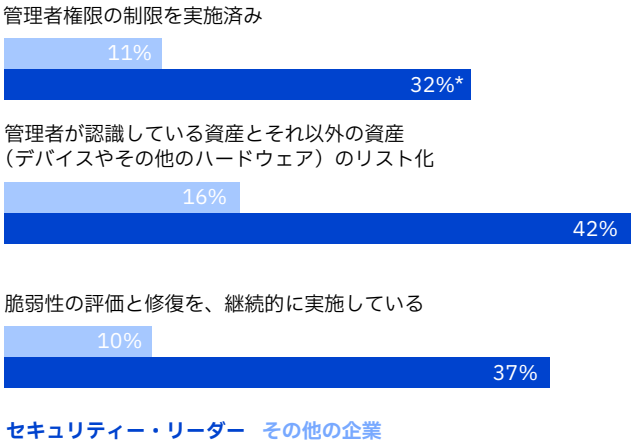
デバイスやデータへのアクセスを制限する

ネットワークへのアクセスとデータの流れを管理するだけでは、防御の方程式の半分を満たしたにすぎない。使用中のデータ、移動中のデータ、保存データ、およびデバイスへのアクセスを管理することで、ようやく残りの半分が満たされる。これらを実現するためには、以下の 3 つのセキュリティー対策が極めて効果的だ。

4. 管理者の権限を制御する：重要なシステムへのアクセス権がある従業員は、悪意であれ、不注意であれ、サイバーセキュリティーにとって最大の弱点となりやすい。外部の悪意あるハッカーよりも、彼らは情報や重要なインフラにアクセスできる範囲がはるかに広いため、しばしば標的になる。セキュリティー・リーダーは、このような攻撃に対処するために機密データへのアクセス権を管理するフレームワークを用意しており、その点において他の企業に比べ優位である（図 7 参照）。

図 7

デバイスやデータへのアクセスを制限する



出典：IBM Institute for Business Value のベンチマーク調査、2019 年
Q：IoT サイバーセキュリティー・リスクを軽減するため、以下の重要なセキュリティー対策をどの程度実施していますか。

効果的なセキュリティー・プログラムを作成し、アクセス権限を厳重に管理する。また機密性の高い機能やデータにアクセスする資格を持つ人物リストをドキュメント化し、関連する各種ネットワーク上の全ユーザーの活動を監視する。特に旅行業界でリスクとなっているのは、IIoT デバイスを管理する技術者の、アカウント ID の共有利用だ。また IIoT 資産を、安全が確保されていない場所に保管することもリスクとなり得る。運用のライフサイクル全体を通して安全性を強化するためには、物理的なアクセスを制限し、管理者権限を厳格化するべきだ。さらに詳細なロールベースの権限を設けるなど、柔軟な方法も検討する価値はあるだろう。[17]

5. 管理者が認識している資産とそれ以外の資産（デバイスやその他のハードウェア）のリストを作成する：旅行関連企業の経営層の 28% が、管理する資産やデバイスの可視化が、IIoT 導入時のセキュリティー確保における最大の課題の 1 つであると回答している。管理者が存在を認識していない IIoT デバイスやネットワークは、「シャドー IIoT」と呼ばれ、従来のセキュリティー・ポリシーでは捕捉されず、存在を把握することは困難だ。

この問題に対処するには、すべての IIoT エンドポイントを特定してプロファイリングし、資産リストに追加して監視するべきである。管理者が公式に承認したデバイスにのみアクセスすることを認め、未承認のデバイスや管理下にないデバイスにアクセスすることを禁止する。

6. 脆弱性の評価と修復を継続的に実施する：監視制御やデータ収集（SCADA）システムなどの産業用制御システムや IIoT デバイスには、欠陥やセキュリティー・ホールがどうしても生じる。よってこれらを使用する以上、旅行関連企業は、分散型サービス拒否（DDoS）攻撃や、マルウェアを拡散するボットネット（Mirai、Aidra、Wifatch、Gafgyt など）に対し脆弱になる。[18] 旅行関連企業の経営層によると、サイバーセキュリティー・インシデント全体における DDoS 攻撃の割合は、33% を占める。回答者の 68% もが、IIoT 関連の最大の脅威として DDoS 攻撃を挙げている。

管理者は脆弱性評価を定期的に実施し、不適切に設定された IIoT デバイスを特定して、これらのデバイスを処分または再設定するべきだ。ただし運用したままの状態で、大掛かりな脆弱性スキャンを行うと、システムが不安定になる場合がある。自動スキャンが適切でない場合は、パッシブ・モニタリングを行う方がよいだろう。

旅行業界のセキュリティー自動化を大規模に実現する

IIoT サイバーセキュリティーの防御基盤ができた後に行うべきなのが、残りの 2 つのフェーズ（7 と 8）だ。このフェーズにより、効果的な検知、対応、復旧の対策、そして自動対応能力の導入が可能になる。

インシデントに対応するための計画とプロセスを確立･管理･テストする

インシデントやセキュリティー侵害があった場合、迅速でダイナミックかつ統制の取れた対応が求められ、そのために必要なテクノロジーとプロセスが存在する。組織的に行うべき、効果の高い対策としては、プロセス面では以下が挙げられる。

7. セキュリティー管理計画の一環として、インシデント対応計画を定義し、管理する：IIoT コンポーネントが危険にさらされたときのための、インシデント対応計画（IR）を準備している企業の割合は、セキュリティー･リーダーでは 59% だったが、その他の企業では 34% だった（図 8 参照）。IR チームが日常的にテストを実施することで、対応能力はさらに強化される。

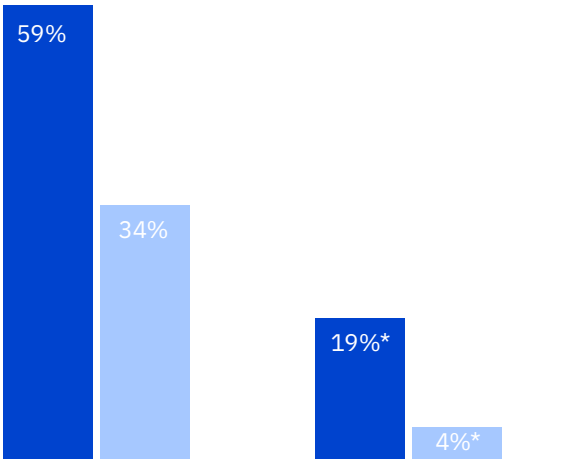
日常的にセキュリティー侵害のシミュレーションを実行していれば、問題が発生した場合にどのプロセス、人材、ツールが利用できるのかが特定できる。専門的なスキルが不足しているのなら、ICS/SCADA のセキュリティー専門家など、エコシステム内の共有リソースを活用すればよい。またミッションクリティカルな IIoT プラットフォームが停止した場合や、事業の中断を迫る恐喝があった場合、それらをカバーするサイバー保険があるため、事前に加入することで、リスクは軽減できる。しかし今回の調査においては、サイバー保険に加入している旅行関連企業はほとんど存在しなかった。

8. ペネトレーション･テストとレッド･チーム演習を実施する：これらを実施すれば、IR 計画の有効性をより詳しく検証することができる。レッド･チームとは、故意にサイバー攻撃を行う善意のハッカー集団のことだ。彼らの力を借りて IR 計画のストレステストを実施すれば、セキュリティーに穴があった場合はそれを特定し、修復を行うことができる。ペネトレーション･テストは、アドホックな脆弱性を発見し、セキュリティー･ポリシーやデータ･プライバシー規制が守られているかを判断するのに役立つ。

このような積極的防御戦略を実施している企業は、セキュリティー･リーダーでは 19% だった。その他の企業では、わずか 4% にすぎなかった（図 8 参照）。IIoT を展開する環境では、スキャンでエラーが発生しただけで、事業運営に重大な影響を及ぼす場合がある。ゆえに慎重な対応は絶対に求められる前提である。

図 8

インシデントに対応するための計画とプロセスを確立･管理･テストする



出典：IBM Institute for Business Value のベンチマーク調査、2019 年
Q：IoT サイバーセキュリティー･リスクを軽減するため、以下の重要なセキュリティー対策をどの程度実施していますか。

検知、修復、対応、復旧プロセスを自動化する

ハイエンドの保護や予防のプラクティスを採用しても、必ずしも確実な安全が訪れるわけではない。悪意ある攻撃者は、システムに侵入するための新たな方法を絶えず開発している。残念ながらサイバーセキュリティーのスキルは不完全であるため、セキュリティー侵害があった場合は、それを検知して修復する仕組みが自動化されていることが望ましい。これを実現するための、極めて効果的な AI 対応プラクティスを以下に 2 つ紹介する。

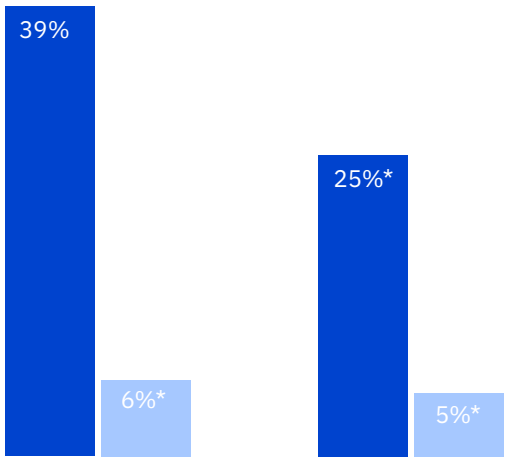
9. 高度なサイバーセキュリティーのモニタリング･分析を利用し、インシデントの検知と修復を行う：業務環境全体で IIoT 情報をリアルタイムで把握するために、自動的にあらゆるモニタリング･ポイントからのデータを収集し、統合･分析を行う包括的なセキュリティー･テレメトリー機能を確立している企業の割合は、セキュリティー･リーダーでは 39%（その他の企業は 7%）だった。この機能により取得されたデータには、システム･ログ、ネットワーク･フロー、エンドポイント･データ、クラウドの利用状況、ユーザーの行動などが含まれており、セキュリティー運用（SOC）チームは、アラートが起動した場合は、その状況を迅速に把握し、誤検知があればそれを区別することができる。SOC チームは、内部の IIoT データから抽出した情報を外部から入手した脅威インテリジェンス･データと組み合わせて分析し、機械学習を適用することにより、攻撃者の次の動きを予測することができる。

10. 高度な行動分析を活用して、エンドポイントへの攻撃やセキュリティー侵害を検知し、対応する：AI 対応の脅威検知機能を企業レベルで活用すれば、ユーザーの異常な行動を発見し、リスクに優先順位を付けることができる。セキュリティー･リーダーの 25% が、機械学習によるユーザー行動の分析機能をすでに活用していた（図 9 参照）。これらの企業は、機械学習を利用して、「正常」なユーザー行動を自動的に追跡し、異常な兆候が見られた場合は、その行動にフラグを付けることもできるようにしている。

IIoT は、IT と OT のソリューション･セットの融合を意味するが、その多くはサイバーセキュリティーを考慮するより前の時代に設計されたものだ。そのため複雑さが増し、固有のリスクが発生している。セキュリティー対策の一部として、IIoT セキュリティー戦略を取り込めば、旅行関連企業は、組織や従業員、顧客の利便性を損なわずに、これらの新技術を利用することができる。

図 9

検知、修復、対応、復旧プロセスを自動化する



出典：IBM Institute for Business Value のベンチマーク調査、2019 年
Q：IoT サイバーセキュリティー･リスクを軽減するため、以下の人工知能（AI）および分析を活用したアプローチをどの程度実施していますか。

重要なインフラを守ることができるのか

- 自社の IIoT のセキュリティー･プラクティスと、リスク管理のフレームワークを、どう整合させているのか。
- セキュリティー･ツールと管理プロセスを、組織のセキュリティー･フレームワークと運用プロセスに、どう統合させているのか。その場合、運用のライフサイクルを通じて、可視性、透明性、および説明責任を担保する方法でなされているのか。
- 安全性の低い IIoT ネットワークは、どうすれば適正に隔離できるのか。
- 困難な状況下において、インシデント対応計画を強化するためには、何が必要か。
- 脅威からの影響を防ぎ、混乱を最小化し、攻撃から迅速に回復するためには、どんな能力が必要だろうか。

アクション･ガイド

サイバー・レジリエンスを高める 2 段階のアプローチ

IIoT の強固な防御基盤を確立する。

IIoT に関するサイバーセキュリティー対策およびプラクティス（そして関連テクノロジー）を取り込んだ、総合的な IIoT セキュリティー戦略を構築する。さらに保護と予防の能力を強化する。

IIoT サイバーセキュリティーを正式化する。

- IIoT サイバーセキュリティーのプログラムを確立する。
- 機能横断的なセキュリティー･チームを結成する。

ネットワークへのアクセスを制限し、ネットワーク間のデータの流れを制御する。

- 境界の防御能力を高める。
- ネットワークのポート、プロトコル、サービスを制限し、制御する。
- マルウェア対策を行う。

デバイスやデータへのアクセスを制限する。

- 管理者の権限を制御する。
- 管理者が認識している資産とそれ以外の資産（デバイスやその他のハードウェア）のリストを作成する。
- 脆弱性の評価と修復を継続的に実施する。

防御基盤ができた後に、旅行業界のセキュリティー自動化を大規模に実現する。

IIoT サイバーセキュリティーを組織のセキュリティー業務に統合して、IIoT 関連のインシデントやセキュリティー侵害に、迅速かつ効果的に対応できるようにする。

インシデントに対応するための計画とプロセスを確立･管理･テストする。

- セキュリティー管理計画の一環として、インシデント対応計画を定義し、管理する。
- ペネトレーション･テストとレッド･チーム演習を実施して、防御の欠陥や、対応策の弱点を発見する。

悪意ある攻撃者は、システムに侵入するため、絶えず新たな方法を模索している。一方で、サイバーセキュリティー･スキルは十分でない。こうした事態に対処するためには、自動化された適応性の高い対応機能を大規模に導入すべきである。

検知、修復、対応、復旧プロセスを自動化する。

- 高度なサイバーセキュリティーのモニタリング･分析を利用し、インシデントの検知と修復を行う。
- 高度な行動分析を活用して、エンドポイントへの攻撃やセキュリティー侵害を検知し、対応する。

著者紹介

Lisa-Giane Fisher
linkedin.com/in/lisa-giane-fisher
lfisher@za.ibm.com

IBM Institute for Business Value の中東･アフリカ地域担当のベンチマーキング･リーダー。M&A やセキュリティーのベンチマーキングを担当。社内の専門家と協力し、業界のプロセス･フレームワークを開発･管理。活動の拠点は南アフリカ。

Julian Meyrick
linkedin.com/in/julianmeyrick
julian_meyrick@uk.ibm.com

IBM Security のグローバル･セキュリティー戦略、リスク＆コンプライアンス、およびクラウド･セキュリティー業務を統括。クライアントが直面するサイバー･リスクを分析し、セキュリティー戦略を支援する。サイバーセキュリティーがビジネスに与える潜在的な影響について、各社の経営層に適切な助言を行っている。活動拠点はロンドン。

Greg Land
linkedin.com/in/gregland
greg.land@us.ibm.com

IBM のホスピタリティー･旅行関連サービス担当のグローバル･セグメント･リーダー。25 年間、旅行業界で戦略コンサルタント、アドバイザー、経営者として活躍。世界規模の航空会社、旅行技術プロバイダー、ホスピタリティー企業のデジタル･トランスフォーメーション導入を支援した実績を持つ。ニューヨークを拠点に活動。

Gerald Parham
linkedin.com/in/gerryparham/
gparham@us.ibm.com

IBM Institute for Business Value のグローバル･セキュリティーおよび CIO 責任者。セキュリティー戦略、セキュリティー運用、リスク、アイデンティティー、プライバシー、および信頼性について調査し、サイバー･ポートフォリオのトータルな研究を行う。企業経営、研究、イノベーション、知的財産開発などの分野で 20 年以上の経験を有す。南カリフォルニアを拠点に活動。

Eric Maass
linkedin.com/in/ezmaass/
emaass@us.ibm.com

IBM Security Services の戦略および先端技術担当ディレクター。組織のポートフォリオ全体（先進的なセキュリティー技術を含む）に関する、事業戦略と投資戦略を統括。セキュリティー業界で長年の実績を積む。企業、国防機関、情報機関、スタートアップなど、さまざまな分野で約 20 年の実務経験を持つ。2014 年、IBM が買収したクラウド･セキュリティー企業では、創業者兼 CTO を務めていた。ニューヨークを拠点に活動。

Steve Peterson
linkedin.com/in/stevenjohnpeterson
steve.peterson@us.ibm.com

IBM Institute for Business Value の旅行･運輸業務の責任者。多くの業界研究レポートを著し、1998 年以来は旅行業界の戦略コンサルタントとして活躍。世界中の IBM の顧客から高い評価を得ており､業界紙だけでなく一般紙からも称賛される。デンバーを拠点に活動。

日本語翻訳監修

Takuji Fujimoto
日本アイ･ビー･エム株式会社
IBM コンサルティング
製造 / 流通事業本部
シニアマネージングコンサルタント
fujimo@jp.ibm.com
www.linkedin.com/in/takuji-fujimoto-833725169

旅行･運輸業界のコンサルタントとして、主に航空会社の業務変革の支援を担当。システム開発プロジェクトの経験を元に、システムの構想からデリバリーまでフルスコープのサポートを行う。航空会社の旅客業務や顧客サービスを専門領域としており、AI を活用したパーソナライズオファリングのソリューションを得意としている。

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、業界知識と洞察力、高度な研究成果とテクノロジーの専門知識を組み合わせることにより、急速な変化を遂げ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。

IBM Institute for Business Value

IBM グローバル･ビジネス･サービスの IBM Institute for Business Value は企業経営者の方々に、各業界の重要課題および業界を超えた課題に関して、事実に基づく戦略的な洞察をご提供しています。

詳細について

IBM Institute for Business Value（IBV）の調査結果の詳細については iibv@us.ibm.com までご連絡ください。IBV の Twitter は @IBMIBV からフォローいただけます。発行レポートの一覧または月刊ニュースレターの購読をご希望の場合は、ibm.com/ibv よりお申し込みください。

調査方法

IBV が Oxford Economics 社の協力を得て行った今回の調査で対象としたのは、IIoT のセキュリティーを担当する 300 人の IT および OT リーダーである。この 300 人の内訳は、旅行業界から 75 人、運輸業界から 225 人である。いずれの企業も、サプライチェーンやロジスティクスのプロセスを支えるために、IIoT アプリケーションを導入している。回答者の地域属性は中東とアフリカを除くすべての主要地域であり、タイトルは経営層（CEO、CTO、CISO、CSO、COO、CRO）、IT 担当ディレクター、バイス･プレジデント、部門マネージャー、および内部監査マネージャーなどである。また業界の詳細は、深海･沿岸･湖沼の水上運輸、一般貨物トラック輸送、鉄道、不定期航空便、そして定期航空便である。運輸の手段ごと（陸路、空路、水路）に、サンプル全体の 3 分の 1 ずつを占めている。

企業のセキュリティーとサイバー･レジリエンスの差異を明らかにするために、2 部構成のオンライン調査を用いて、IIoT サイバーセキュリティーのパフォーマンスと成熟度を評価した。1）IIoT に関するサイバーセキュリティー･リスクを特定し、それらから組織を守るための能力。インシデントを検知して対応し、復旧するための能力。2）リスクやインシデント管理能力の有効性を測定するために必要なコスト、そのサイクル･タイム、品質、および効率性。

回答結果は、2 つに分けて分析した。1 つ目の分析では、3 つの重要業績評価指標（KPI）について、各社の平均スコアを算出した。その3つとは、サイバーセキュリティー予算に占める IIoT サイバーセキュリティーの割合、セキュリティー対策によって処置された既知の IIoT 脆弱性の割合、そして IIoT サイバーセキュリティー･インシデントへの対応と復旧にかかるサイクル･タイムである。この分析の結果、80 パーセンタイルのパフォーマンスを発揮したセキュリティー･リーダーを特定することができた。2 つ目の分析では、Center for Internet Security（CIS）の 20 個の重要セキュリティー項目と、6 つの AI を活用したプラクティスのうち、どれが KPI に最も大きな影響を与えているかを把握するため、回帰分析を行い、全 26 要素を影響度の観点からランク付けし、そのリストを作成した。上位 10 位までは、平均を超える影響力を持つ。財務情報を含むすべてのデータは、自己申告によるものである。

関連レポート

Hahn, Tim, Marcel Kisch, and James Murphy. “Internet of threats: Securing the Internet of Things for industrial and utility companies.” IBM Institute for Business Value. March 2018. ibm.biz/iotthreats

Fisher, Lisa-Giane, Giuseppe Serio, and Ben Stanley. “Automotive Industrial Internet of Things: Quick to implement, slow to secure.” IBM Institute for Business Value. August, 2018. ibm.biz/autoiiot

Borrett, Martin, Lisa-Giane Fisher, Cristene Gonzalez-Wertz, and Peter Xu. “Electronics Industrial IoT cybersecurity: As strong as its weakest link.” IBM Institute for Business Value. October 2018. ibm.biz/electronicsiiot

Dougherty, Steven, Cristene Gonzalez-Wertz, Lisa-Giane Fisher, and Mark Holt. “Mind the utilities cybersecurity gap: Move from pieced together to peace of mind.” IBM Institute for Business Value. January 2019. ibm.co/utilitiesiiot

注釈および出典

1 Muncaster, Phil. “San Francisco Airport Attack Linked to Russian State Hackers.” Information Security Magazine. April 2020. https://www.infosecurity-magazine.com/news/san-francisco-airport-attack/

2 “DragonFly: Energy sector attacks.” IBM X-Force Exchange. https://exchange.xforce.ibmcloud.com/collection/Dragonfly-Energy-Sector-Attacks-d4cf1567963a2cdbd24fae1fbff27111

3 Riedel, Bruce. “Al Qaeda’s 9/11 Obsession.” Brookings. July 15, 2011. https://www.brookings.edu/opinions/al-qaedas-911-obsession/

4 Bonderud, Douglas. “Loco Motives? Hacker Attacks Could Derail Train Cybersecurity, Researchers Say.” IBM Security Intelligence. January 12, 2016. https://securityintelligence.com/loco-motives-hacker-attacks-could-derail-train-cybersecurity-researchers-say/

5 Alvarez, Michelle. “Industry Overview – Critical Infrastructure (Basic Needs).” IBM Managed Security Services (MSS). March 25, 2015. https://portal.sec.ibm.com/mss/html/en_US/support_resources/pdf/industry_overview_crit_infra_3-25-2015.html?cm_mc_uid=48776590151015659713589&cm_mc_sid_50200000=52979001567332373470&cm_mc_sid_52640000=66539761567332373474

6 “CIS Controls™.” Center for Internet Security. https://www.cisecurity.org/controls/; Hahn, Tim, and JR Rao. “IoT Security: An IBM Position Paper.” Watson IoT. IBM. October 2016. https://www.ibm.com/internet-of-things/spotlight/iot-security. 同書への直接リンクはこちら: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfWWW12379USEN

7 Lunden, Ingrid. “UK’s ICO fines British Airways a record £183M over GDPR breach that leaked data from 500,000 users.” Techcrunch. July 8, 2019. https://techcrunch.com/2019/07/08/uks-ico-fines-british-airways-a-record-183m-over-gdpr-breach-that-leaked-data-from-500000-users/

8 Rodriguez, Joe Fitzgerald. “Alleged Muni ‘hacker’ demands $73,000 ransom, some computers in stations restored.” San Francisco Examiner. November 28, 2016. https://www.sfexaminer.com/news/alleged-muni-hacker-demands-73000-ransom-some-computers-in-stations-restored/

9 Newman, Lily Hay. “Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare.” Wired. April 23, 2018. https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/

10 Baker, Graeme. “Schoolboy hacks into city’s tram system.” The Telegraph. January 11, 2008. https://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html

11 このデータ･ポイントは、IIoT のサイバーセキュリティー能力に対する、セキュリティー･リーダーたちの相対的な信頼度を示している。n 数が少ない（n<20）ため、統計的な信頼性は高くないものの、他の回答者との比較において、一定の方向性は示されると考えられる。

12 “CIS Controls™.” Center for Internet Security. https://www.cisecurity.org/controls/; Hahn, Tim, and JR Rao. “IoT Security: An IBM Position Paper.” Watson IoT. IBM. October 2016. https://www.ibm.com/internet-of-things/spotlight/iot-security. 同書への直接リンクはこちら: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WWW12379USEN

13 “National Institute of Standards and Technology (NIST) Risk Management Framework.” NIST Computer Security Resource CenterのWebサイト。https://csrc.nist. gov/projects/risk-management/risk-management framework-(rmf)-overview; “NIST Special Publication 800-series General Information.” NIST Information Technology Laboratory. https://www.nist.gov/itl/nist special-publication-800-series-general-information; “ISO/IEC 27000 family - Information security management systems.” International Organization for Standardization. https://www.iso.org/isoiec-27001-information-security.html

14 Hahn, Tim, Marcel Kisch, and James Murphy. “Internet of threats: Securing the Internet of Things for industrial and utility companies.” IBM Institute for Business Value. March 2018. https://www-935.ibm.com/services/us/gbs/thoughtleadership/iotthreats/

15 “CIS Controls Internet of Things Companion Guide.” Center for Internet Security. July 27, 2019. https://www.cisecurity.org/white-papers/cis-controls-internet-of-things-companion-guide/

16 同上。

17 同上。

18 “IBM X-Force Threat Intelligence Index 2019.” IBM Security. February 2019. https://www.ibm.com/security/data-breach/threat-intelligence

Benchmark Insights について

Benchmark Insights は経営層の方々に、ビジネスや関連技術の重要トピックについての洞察を提供するものです。この洞察は、パフォーマンスのデータやその他のベンチマーク指標の分析結果に基づいています。詳細については、IBM Institute for Business Value（iibv@us.ibm.com）までお問い合わせください。

IBM Corporation
New Orchard Road
Armonk, NY 10504
Produced in the United States of America
April 2020

本書は英語版「IIoT cybersecurity for travel companies - Protecting travel operations」の日本語訳として提供されるものです。