Forrester Consulting
Thought Leadership Paper
委託元 : ForeScout

2017 年 11 月

計画し損ねる故の失敗と失敗を招く計画

IoT 環境での安全性の確保における LoB（事業部門）実践者と SOC の役割を理解する

FORRESTER®

目次

プロジェクト ディレクター :
Chris Taylor
(市場影響シニアコンサルタント)

調査協力 :
Forrester セキュリティおよびリスク調査グループ

FORRESTER CONSULTING について

Forrester Consulting は、企業からの委託により第三者機関として客観的な調査と、それに基づくコンサルティングを提供することで事業の成功を支援しています。短期の戦略セッションから個別のご要望に応じた長期のプロジェクトまで、専門知識と経験が豊富な Forrester Consulting のリサーチ アナリストが直接お客様に対応し、それぞれのビジネスに関する課題について専門的な知見を提供いたします。詳細については、forrester.com/consulting をご覧ください。

FORRESTER®

エグゼクティブサマリー

技術的な進歩により、新しいタイプの接続デバイス、すなわち、モノのインターネット（IoT）が氾濫し、これにより企業が対抗することも、認識することさえできない新たなセキュリティ脅威がもたらされます。多くの企業は、これらのセキュリティニーズに対応するための適切な準備が整っておらず、新たな種類の脅威に時代遅れの戦略やポリシーを適用しています。さらに、運用技術（OT）を用いて頻繁に作業する個々の事業部門（LoB) と、セキュリティオペレーションセンター（SOC）などの従来のセキュリティチームは、IoT 接続デバイスをいかに管理するかについて共通の見解を持っていないことがよくあります。

2017 年 8 月、ForeScout は、全社的に使用されているか、特定の分野のビジネスをサポートしているかにかかわらず、ネットワーク上に接続された IoT デバイスの激増により、組織が適切かつ正確に自社のネットワークを保護できるかどうかを判断するよう Forrester Consulting に依頼しました。企業内で運用技術を使用している個々の事業部門は、必要なセキュリティ監視を行わずにこれらの新しいデバイスやアプリケーションを導入し、ネットワーク内のセキュリティ脆弱性を生み出すことがあります。セキュリティチームは、「見えない」ものを守ることはできません。それ故、デバイスに関する知識が安全性の確保のために非常に重要です。弊社の調査では、企業がこの新たな「接続された」時代にネットワークの安全性を確保することについて懸念しており、安全性への懸念の高まりに対応できる適切なツール、リソース、プロセスの発見を急いでいることが判明しました。

Forrester はモノのインターネットを、インターネット型ネットワーク経由で監視 / 解析 / 制御システムとの通信を行うオブジェクトやインフラストラクチャを可能にするテクノロジーであると定義しています。これには、特定のデバイス（すなわち、モノ）だけでなく、このテクノロジーが可能にするプロセスと機能（すなわち、運用技術 OT）の両方が含まれます。当調査では、IoT の広いカテゴリーの下で、接続された「モノ」（すなわちデバイス）と OT をグループ化しました。

調査結果の要点

- IoT により、セキュリティ責任者はネットワークの安全性確保の方法の見直しを迫られている。
- IoT セキュリティのリスク許容度は驚くほど高く、セキュリティチームはセキュリティ戦略の進化を余儀なくされている。
- セキュリティ責任者の 50%以上が、IoT セキュリティについて不安を感じている。
- IoT の管理とセキュリティに関する責任の所在について、個々のビジネス・ラインと IT 部門には共通の認識がほとんどない。
- 可視デバイスに基づく監査はコンプライアンスを満足させることができるが、既知または未知のすべてのデバイスの知識がセキュリティにとって極めて重要。
- デバイスの知識とコンプライアンスの向上は、IoT セキュリティを改善するための重要なステップ。

FORRESTER®

モノのインターネット（IoT）が新たなセキュリティアプローチを要求

世界は接続された製品（モノのインターネット）革命の真っ只中にあり、企業の 90%は向こう数年間に接続されたデバイスの量が増加すると見込んでいます。企業には、ビジネスプロセスや機能を向上させるため、ネットワークに従来接続されていなかったデバイスを接続することによる利点が既に見えています。だが、企業はこれらの新しいデバイスがセキュリティ要件にさらなる負担をかけることを認識しています。企業の 77%は、IoT デバイスの使用の増加が深刻なセキュリティ上の課題を引き起こしていることを認めています。

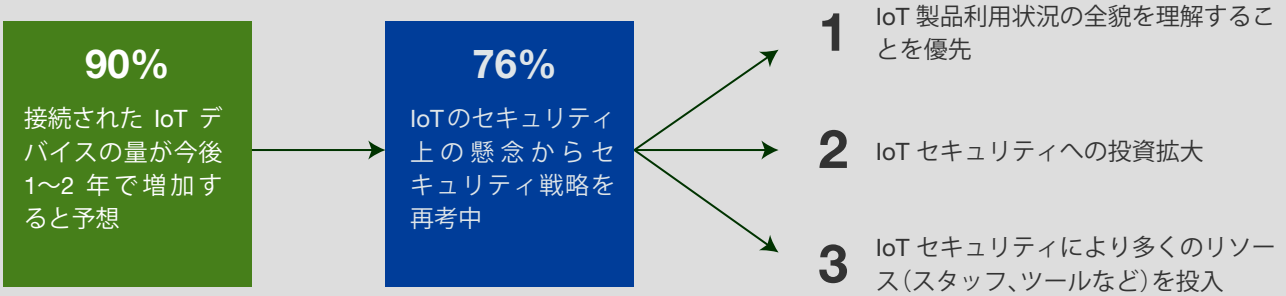
問題は、大半の組織にこれらのセキュリティ上の課題を適切に管理する体制が整っていないのです。セキュリティチームは深く根付いた従来の方法を踏襲してセキュリティ対応を行っているが、そうした技術やプロセスでは必要なセキュリティが提供されないことを認識しています。その結果、企業の 76%は IoT のセキュリティ上の懸念により、IT や事業部門のセキュリティ戦略の再考を余儀なくされていると回答しています（図 1 参照）。この戦略の改革には以下が含まれます。

- IoT 製品利用状況の全貌を理解することを優先。
- IoT セキュリティへの投資を拡大。
- IoT セキュリティにより多くのリソース（スタッフ、ツールなど）を投入。

企業の 77%は、IoT デバイスの使用の増加が深刻なセキュリティ上の課題を引き起こしていることに同意しています。

図 1

IoT の成長により企業はセキュリティ戦略の調整を迫られている



調査対象 : 組織のネットワークとデータセキュリティプロセスに携わる IT およびビジネスの意思決定者 603 人。
出所 :ForeScout からの委託により Forrester Consulting が実施した調査 (2017 年 8 月)

FORRESTER®

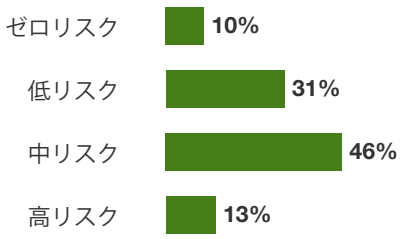
高すぎるリスク許容度

企業の 59%は、IoT セキュリティ遵守に際し、中〜高リスクをとることを厭わないと回答しました。これは、IoT セキュリティの脅威について企業がいかに無知であるかの驚くべき証しです（図 2 参照）。企業が IoT についてこのレベルのリスクを受け入れることを厭わないという事実は、当問題について驚くほど理解不足であることを示しており、将来的な様々のサイバー攻撃の基になります。IoT について高リスクを許容することは、保有車両の大半に機械的問題があることを認めながら、対応せずに最善の結果を望む輸送会社のようなものです。

許容リスクの水準についての回答は特筆すべきであり、実態が見かけ以上に深刻である可能性を示唆しています。このリスク許容度を、IoT が重大なセキュリティ上の課題を引き起こしていると企業の 77%が回答していることに照らし合わせると、企業の「許容度」が、安心してというより、制御できない故であることが伺えます。問題の一つは、企業の 44%が IoT セキュリティ向上にとり、予算の制約を挙げていることです。企業が IoT デバイスの急増と、それに関するコンプライアンス要件への対応に苦労するなか、セキュリティ予算はそれに見合うペースで増加しなければなりません。そうならないと、企業は別の対応をする体制にないが故、より高いリスクを許容することを余儀なくされるでしょう。

図 2

「IoT セキュリティのコンプライアンス要件に関し、貴社はどの程度のリスクを許容できますか？」



調査対象：組織のネットワークとデータセキュリティプロセスに携わる IT およびビジネスの意思決定者 603 人。
出所 :ForeScout からの委託により Forrester Consulting が実施した調査 (2017 年 8 月)

IOT セキュリティはセキュリティ担当者に不安を与える

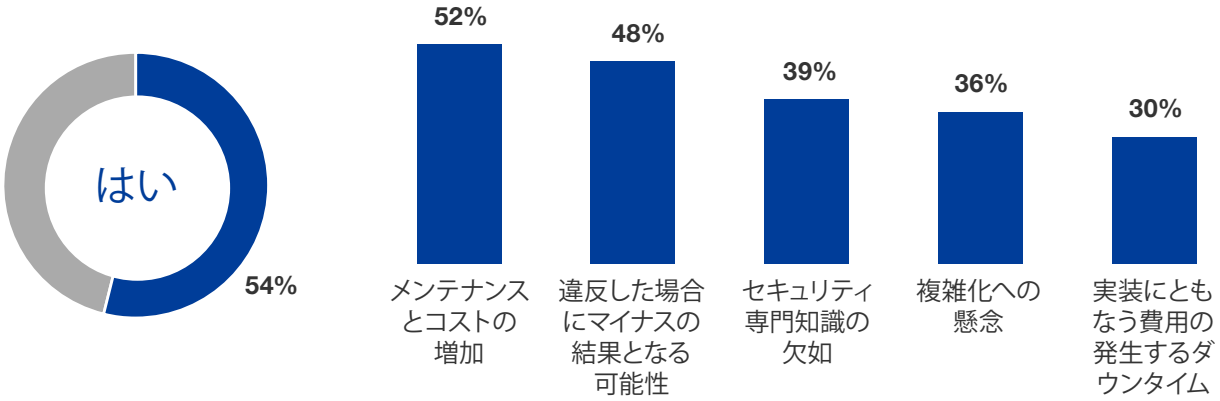
多くのセキュリティ責任者が許容せざるを得なくなっているリスクを勘案すると、彼らの 54%が IoT セキュリティに不安を感じていると回答していることは驚くに値しません。しかし、企業が様々な課題に直面するなか、弊社はこの数字がさらに上昇すると見込んでいました。そうならなかった理由は恐らく、セキュリティの責任者たちが自ら制御できないものに対して不安になる必要性を感じていないためです。一方、事業部門のセキュリティの意思決定者のうち、IoT セキュリティに不安を感じているのは 58%と、IT 責任者（51%）よりも高い割合であることが弊社の調査で判明しました。これは、IoT セキュリティへのアプローチ方法に関する両者の見解の食い違い、または障害点を示唆しています。技術的に問題を是正しなければならない IT チームが IoT に関して同様の懸念を表明しない限り、LoB（事業部門）責任者が必要とする、自分たちのデバイスが安全であるという保証をえることは困難であると考えられます。IoT をめぐる不安は、以下の 3 つの要因により引き起こされています（図 3 参照）。

- **管理に必要なコストと時間**。IoT はネットワークの攻撃対象領域を飛躍的に増加させるため、セキュリティ責任者が適切な管理を行うには従前よりもかなり多くの時間を必要とします。また、比較的新しい概念でもあります。適切な管理方法を知ることが、その他のセキュリティプロセスほど単純明快ではありません。
- **セキュリティ侵害の潜在的な悪影響**。ネットワーク上のあるデバイスのセキュリティ障害が、ネットワーク全体を危険にさらす可能性があります。
- **セキュリティスキル不足**。IoT の管理が難しい場合は、セキュリティを確保することも難しくなります。新たな技術は、セキュリティチームの多くが是正のための適切な訓練を受けていない新たなセキュリティ要件をもたらします。

IoT について高リスクを許容することは、保有車両の大半に機械的問題があることを認めながら、対応せずに最善の結果を望む輸送会社のようなものです。

図 3

「IoT セキュリティに不安を感じますか？その理由は？ *」



調査対象 : 組織のネットワークとデータセキュリティプロセスに携わる IT およびビジネスの意思決定者 603 人。
* 調査対象：IoT セキュリティに不安を感じると指摘した IT およびビジネス意思決定者 327 人。
出所 :ForeScout からの委託により Forrester Consulting が実施した調査 (2017 年 8 月)

IT とビジネスリーダーが IoT セキュリティ管理で連携していない

IT と事業部門が IoT デバイスとセキュリティの設定および管理方法について異なる認識を持っています。事業部門ごとにセキュリティを個々に所有すべきだと考える者もいれば、別の誰かがセキュリティを担当すべきであると考える者もいます。全社の IT ネットワークにある IoT デバイスの安全性確保について誰が最終的に責任をとるべきかとの質問に対し、IT 責任者の 44%がセキュリティ運用センター（SOC）と回答した一方、LoB（事業部門）では自分たちが第一責任者であると特定した回答が多くありました。逆に、デバイスのデフォルト設定については、IT 責任者の 45%は LoB（事業部門）が責任を負うべきであると考える一方、LoB（事業部門）の回答者の 46%は IT が担当すべきであると回答しました。これにより、2 つの可能性が想定されます。1) IoT セキュリティがサイロ状（IT は IT、LoB は LoB）に管理され、全社的な共通の利用状況が限定的、あるいは、2) 誰もが他人が責任を負うことを期待している環境（図 4 参照）。貴社が直面している状況がどちらであれ、デバイスが未対応のまま放置されていたり、設定が不適切であった場合、セキュリティが無効化する可能性があります。

企業が IoT セキュリティの管理方法を検討する際、大半の企業が既知の事柄に固執し、セキュリティをセキュリティ運用センターなどの IT の権限下に保ちます。通常、このアプローチは概して機能しますが、それはネットワーク上に存在するデバイスについて、組織が把握している場合に限られます。どのような SOC もデバイスの管理またはサポートが可能であるが、それには彼らがデバイスを接続している資産管理者、LoB（事業部門）チームおよびネットワークチームと連携し協働することが欠かせません。これは、以下の 2 つの理由により重要です。

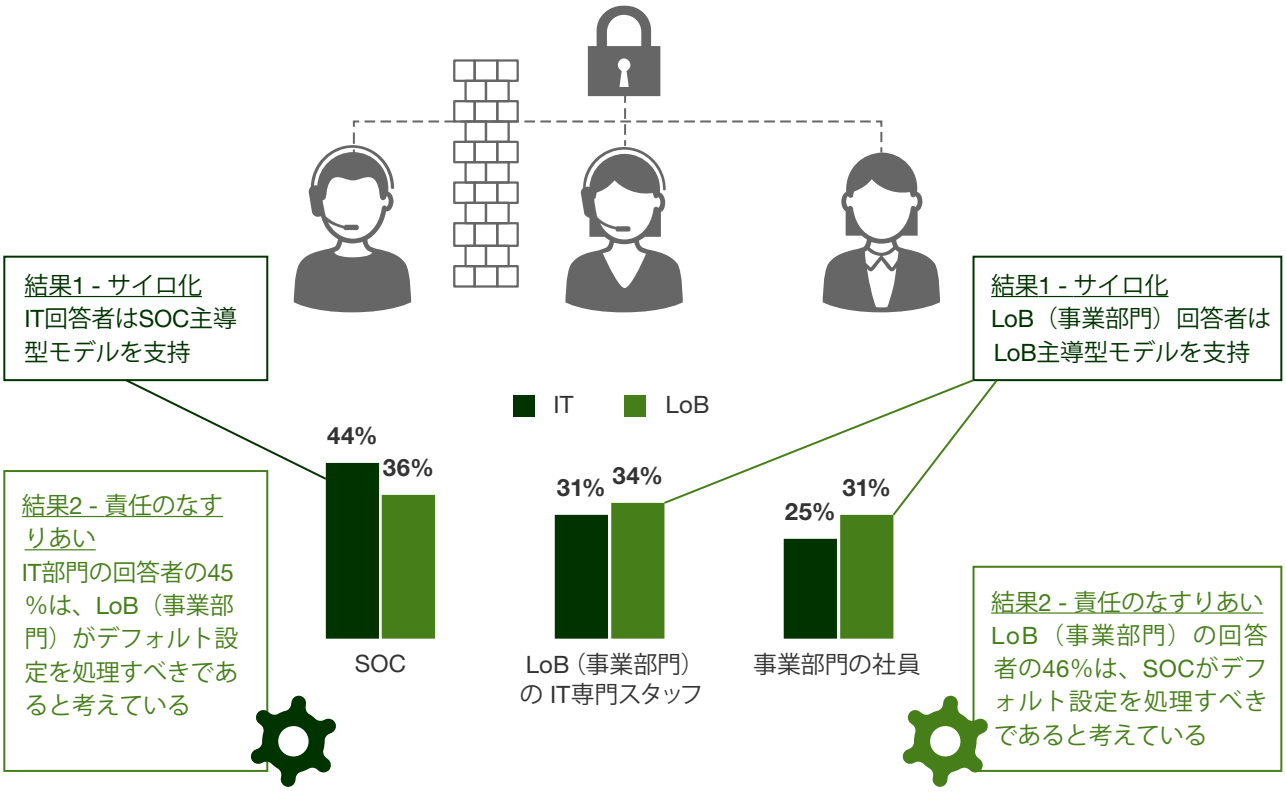
- **セキュリティのデフォルト設定の管理**。企業の 50%は、IoT デバイスのデフォルト設定は SOC が処理するべきであると回答しています。しかし、役職別に見ると、LoB（事業部門）回答者の 54%が、デフォルト設定は LoB スタッフまたはデバイスメーカーが管理すべきであると考えています。この調査結果は、LoB（事業部門）ユーザーが、自分たちの IoT セキュリティニーズのために SOC をコマンドおよび制御ポイントとして活用する必要すらなく、すべての適切なコントロールが配備されているという想定のもと、デバイスを導入していることを示唆しています。さらに、IT 回答者の 45%は事業部門がこれを所有していると考えており、それ故、協働する動機が少なくなっています。
- **ネットワーク上のデバイスについて適切な可視性を得る**。デバイスの設定期間に資産管理者や事業部門のチームに積極的に関与していない限り、SOC が接続されているデバイスの正確な数を完全に把握することは困難です。ネットワーク上の一つのデバイスのセキュリティ障害がネットワーク全体を危険にさらす可能性があるため、SOC は 100%の可視性を必要とします。

回答してください。

貴社の SOC または事業部門のチームは、IoT 設定とセキュリティ管理の責任者は誰であると考えますか？

図4

ネットワーク上のIoTデバイスのセキュリティを確保する責任の所在が曖昧な場合、2つの結果を招く



調査対象: 組織のネットワークとデータセキュリティプロセスに携わるITおよびビジネスの意思決定者603人。
出所: ForeScout からの委託により Forrester Consulting が実施した調査 (2017 年 8 月)

セキュリティに関する自己満足が問題につながる可能性

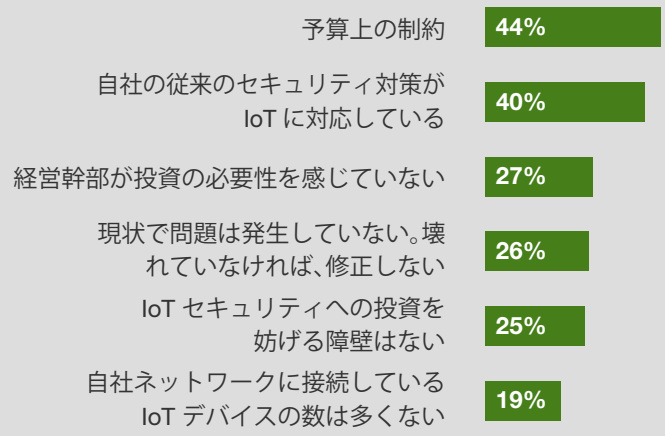
IoT セキュリティが大きな課題であり懸念であるとの認識に基づき、弊社は回答者に IoT セキュリティの改善を阻む重要な障壁を特定するように尋ねました。IT および事業部門の回答者は同様の課題を報告し、IoT セキュリティについてのアプローチが並行（非効率な場合）であることを示唆しています。要するに、双方のグループが同時期に同じ方法で格闘しているように見えます。上位の回答は以下の通りです（図 5 参照）。

- **従来のセキュリティアプローチで IoT が賄えるとの考え**。セキュリティチームは長年にわたりレガシーシステムの安全性を確保してきました。彼らが同様の慣行を IoT にも適用するのは簡単であるという通念があります。しかし、比較的検証されていない、または未確認の新技術を扱う場合、「壊れていない場合は修正しない」という考え方は適用されません。
- **シニア責任者からのサポートの欠如**。現行の方法が十分であるとの考えに基づき、シニア責任者の多くは新たなツールや人員への投資を正当化するのが困難であると考えているようです。残念ながら、セキュリティ侵害でもおきなければ注意が喚起されない可能性が高く、その時点で手遅れです。
- **予算上の制約**。44%の企業が予算を重要な障壁として挙げています。予算の欠如は、適切な技術スキルを持つ人材を雇用したり、IoT セキュリティを適切に管理するのに見合ったツールを購入する企業の能力に影響を及ぼします（企業のそれぞれ 31%と 25%が課題として報告しました）。これは、IoT セキュリティに関する不安の最も普遍的な原因にメンテナンスとコストが挙げられる理由を説明するのにも役立ちます。予算が増加している場合でさえ、企業は IoT デバイスの成長に比例した IoT セキュリティ予算の拡大を確保する必要があります。現行のセキュリティが適切であるという誤った考えと管理職の支持を思うように得られずにいるなか、必要な予算を見つけるのは困難な戦いになり得ます。

残念ながら、セキュリティ侵害がなければ、一部の経営幹部の注意を引くことは出来ない可能性が高い。その時点では時すでに遅しです。

図 5

「貴社で IoT セキュリティへの投資拡大を阻む最大の障壁は何ですか？」



調査対象 : 組織のネットワークとデータセキュリティプロセスに携わる IT およびビジネスの意思決定者 603 人。
出所 :ForeScout からの委託により Forrester Consulting が実施した調査 (2017 年 8 月)

予算が増加している場合でさえ、企業は IoT デバイスの成長に比例した IoT セキュリティ予算の拡大を確保する必要があります。

FORRESTER®

企業は IOT のセキュリティを十分に信頼していない

多くの企業が、現行のセキュリティポリシーが IoT を賄うのに十分であるとの信念を抱くなか、弊社は、企業に自社の現行の IoT セキュリティへの信頼度を評価するように尋ねました。1 から 10 の段階評価（10 は完全に信頼）で、大半の回答はポジティブであり、70%が 8 から 10 の範囲内でした。しかし、残る 30%の企業は、自社の IoT ネットワークのセキュリティについての信頼度が中程度、または低いものでした。特に、10（完全に信頼）と評価した企業はわずか 13%でした。セキュリティ上の問題とセキュリティ侵害の潜在的な影響を考慮すると、企業の 87%が IoT セキュリティに完全な自信を持っていないことが判ります。

この点をさらに掘り下げようと、弊社は次の仮説的な質問をしました。

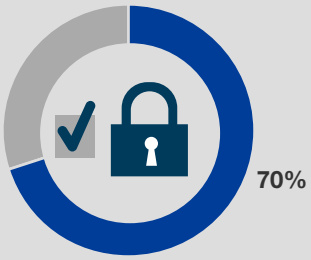
「貴社が 監査され 使用中の IoT 接続デバイスとソリューションのすべてを特定する必要が生じたら、それらの IoT 接続デバイスとソリューションの 100%を正確に識別する能力にどの程度自信がありますか？」

セキュリティの信頼度に関する回答結果と同様、大半の回答は 8 から 9 の範囲内となりましたが、完全に信頼しているとの評価はわずか 18%でした。82%の企業が自社ネットワークに接続されたすべてのデバイスを完全に把握していないのであれば、これは大きな問題です（図 6 参照）。我々のビジネスが今あるネットワークとセキュリティの世界は、コンプライアンス主導型であり、監査に重点を置いています。弊社の調査では、大半の組織は IoT コントロールに焦点を当てたコンプライアンス監査を適切にパスすることができると感じている一方、実際には 100%確実ではないことを意識的に認めています。これは、多くの企業にとってネットワーク侵害の重大な手段となりうる、潜在的な障害点を際立たせています。

企業の 87％は、自社の現行の IoT セキュリティを完全に信頼していません。

図 6

「貴社の IoT ネットワークの安全性についてどれくらい自信がありますか？」



70% 非常に自信がある

「監査された場合、使用されている接続された IoT デバイスやソリューションの 100%を特定することに、どれくらい自信がありますか？」

18% 完全に自信がある

調査対象 : 組織のネットワークとデータセキュリティプロセスに携わる IT およびビジネスの意思決定者 603 人。
出所 : ForeScout からの委託により Forrester Consulting が実施した調査 (2017 年 8 月)

現状の IoT セキュリティへの満足度は高いが、本格的に検証された場合満足度は持続しない。

FORRESTER®

IoT セキュリティは IoT の可視性から始まる

弊社は、企業が IoT の成長に適応するためのネットワークセキュリティ戦略の再定義を始めるなか、増大する課題に対応するために取っている 4 つの重要なステップを特定しました（図 7 参照）：

- **IoT デバイスの認識と可視性の向上。**どのデバイスがネットワーク上にあるのかを理解することは、そのデバイスを保護するための重要な第一歩です。見えないものを保護することは出来ません。それ故、これが、次のステップとして最も普遍的に特定されました（48%）。
- **コンプライアンスをより重視する。**多くの企業が現在IoTセキュリティの遵守にあたり中〜高リスクを容認していますが、それは必ずしも選択の結果ではありません。コンプライアンスに再び焦点を当て、ネットワーク可視性を向上させる努力をすることにより、セキュリティ責任者は監査の際により自信をもって、容認せざるを得なかったリスクを引き下げることができるでしょう。
- **IoT デバイスの管理と実行の一元化。**大半の企業は SOC または IT のコントロールのもと、デバイスを一元管理していますが、初期設定と導入についての責任の所在については依然として隔たりがあります。IoT デバイスの導入と管理の両方を一元化することで、企業はより一貫性のある設定を得、新しいデバイスの認識を向上させ、セキュリティのオーナーシップについて IT と LoB（事業部門）チームの間の混乱を少なくすることが可能になるでしょう。
- **ツールと専門知識を提供する IoT セキュリティパートナーを見つける。**企業が IoT セキュリティへの投資を増やす際、スキルのギャップを埋め、適切なツールを使用する手助けとなるパートナーが必要となるでしょう。次世代の IoT セキュリティソリューションの検討を求められた際に最も重要な基準を尋ねられた際、上位の回答は以下のようでした。1) ソリューションは既存のセキュリティシステムと統合されなければならず、2) 導入が容易であること。企業は、自社のセキュリティソリューションのすべてを完全に改革することなく、シームレスに協働することでセキュリティを増強できるパートナーを求めています。

これらの次のステップをサポートするため、企業の 82%は向こう 1 〜 2 年間に IoT セキュリティへの支出が増えると見込んでいます。理論的には、IoT に向かう相対的な支出は、IoT デバイスに見られる成長と従来のセキュリティの改善を反映すべきです。しかし、回答者の 40%が、IoT には従来のセキュリティ対策で十分であると感じていることから、これを売るのは厳しいでしょう。従って、IoT 環境の安全性を確保することの重要性と、そうしなかった場合のリスクについて、セキュリティチームが経営陣チームに実証することが、これまで以上に重要になります。経営陣に IoT セキュリティの重要性と価値を示すことで、セキュリティチームは自社の IoT 環境の適切な保護に必要な資金とリソースの配分を得ることができます。資金の増加、可視性とコンプライアンスに焦点を置いた新たなセキュリティ戦略により、企業は IoT についての不安を軽減し自社ネットワークの安全性への確信を取り戻すために前進し始めることができます。

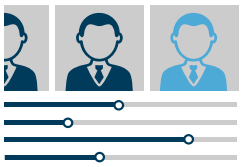
図 7

「貴社は IoT セキュリティを改善するためにどのような手続きを実施していますか？

意識と可視性の向上

コンプライアンスをより重視

IoT セキュリティの集中管理



適切なツールと専門知識を持つパートナーを探す

調査対象：組織のネットワークとデータセキュリティプロセスに携わる IT およびビジネスの意思決定者 603 人。
出所 :ForeScout からの委託により Forrester Consulting が実施した調査 (2017 年 8 月)

48% の企業は、IoT デバイスの認識と可視性の向上を、IoT セキュリティの改善のための重要な次のステップであると見なしています。

FORRESTER®

主な提案

今日の企業は、絶え間なく拡大し続ける接続の世界に直面しています。日々、企業が成長し繁栄するにあたり、決定的な利点を提供できる新たなデバイスと機能が出現します。しかし、これらのデバイスやテクノロジーが無計画に放置されれば、ネットワーク侵害の原点となり、最終的には組織の終焉を招く可能性があります。IoT 対応システムをより効果的に防御するため、弊社は企業に以下を行うことを推奨します。

汝自身を知れ。明確なセキュリティ戦略がなければ、貴社は引き続きセキュリティの不安と課題に直面するでしょう。以下の質問を自身に問い、正直に答えてください。

- **自社のネットワークについて完全な可視性を得ているだろうか？どの程度のリスクを容認できるだろうか？**ネットワークに接触するすべてのデバイスについて包括的な知識とコントロールがなければ、認識しているデバイスに基づいて監査をパスしたとしても、そのネットワークは安全ではありません。
- **新しいデバイスの設定と導入の設定を所有しているのは誰か？**貴社のセキュリティチームとネットワークチームが連携し、IoT 導入とセキュリティプロトコルを調整して、デバイス全体の監視を可能にすることが不可欠です。
- **あなたにそれは可能か？あなたがすべきか？**あなたのチームにソリューション、または「ニーズ」として新たなデバイスか技術が提供された時、これらの質問をしてください。ワイヤレス接続のトースターを使用できるか？確かに。社員の便宜のため、自社ネットワークに不要な脅威の媒介となるものを導入すべきか？恐らく、導入すべきではないでしょう。

標準よりも上を目指す。コンプライアンス基準または監査権限を満たすことは、能力の最低ランクを達成するにすぎません。これは、文字通り、失敗の可能性を回避するだけです。貴社のチームは、これらの基準を上回り、革新と最適化を推進しつつビジネスに有益な新技術を安全に採用する計画と戦略をもって前進するよう努めなければなりません。

テクノロジーをもってテクノロジーと闘う。 現在普及しているネットワーク接続デバイスの成長と多様性に人間が追いつくことは不可能です。IoT セキュリティと会計に関する問題の是正に取り組む機会を得るには、貴社のチームは IoT セキュリティコントロールの特質に焦点を絞った、専用の技術的ソリューションを活用する必要があります。技術的な失敗にはテクノロジーを用いて対処し、貴社のセキュリティと LoB（事業部門）チームに IoT スプロール現象を是正する権限を与えます。

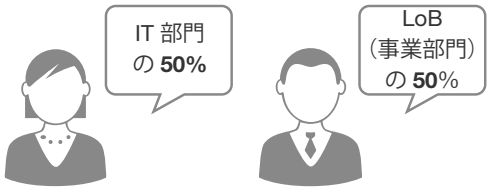
FORRESTER®

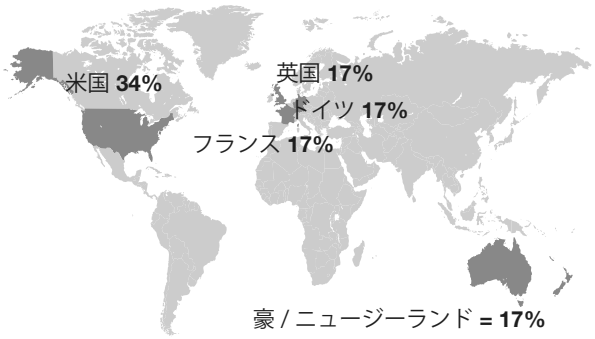
付録 A：調査方法

当調査で、Forrester は組織のネットワークとデータセキュリティ / エンドポイントのセキュリティプロセスに携わる IT およびビジネスの意思決定者 603 人にインタビューを行いました。参加者には、IoT セキュリティに関する課題と自社のネットワーク上のデバイス全般についての認識についての質問が提供されました。調査対象は、米国、英国、ドイツ、フランス、オーストラリア / ニュージーランドにある、従業員数 2,500 人以上の企業です。今回、貴重な時間を割いて調査にご協力いただいた方々には薄謝を送らせていただきました。本調査は 2017 年 8 月に終了しました。

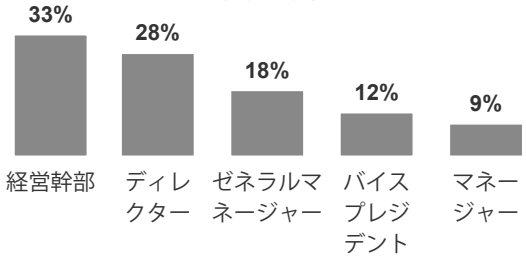
付録 B：調査対象者について / データ

回答者の地理的分布：

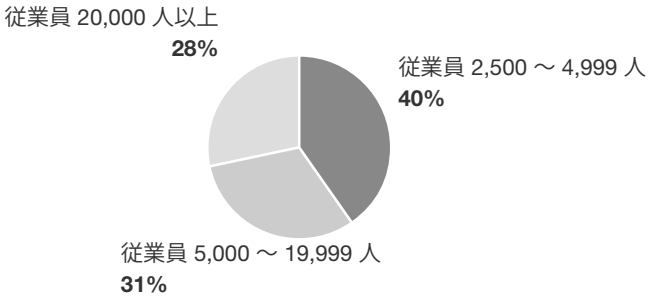




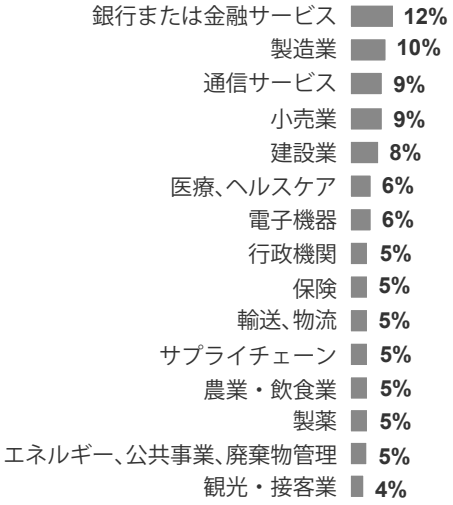
回答者の職位



会社規模 (従業員数)



業種



調査対象：組織のネットワークとデータセキュリティ / エンドポイントのセキュリティプロセスに携わる IT およびビジネスの意思決定者 603 人。
出所 :ForeScout からの委託により Forrester Consulting が実施した調査 (2017 年 8 月)

FORRESTER®