調査レポート
アクシスコミュニケーションズ

2018年のサイバーセキュリティの現状:

エンドユーザー

サマリーレポート

AXIS COMMUNICATIONS

目次

背景

世界経済フォーラムは、2018年において世界的に最も深刻なビジネスの脅威として、サイバー攻撃を3番目に挙げています。一方、データ侵害の成功例の90%以上は、人的ミス、不適切な設定、および不適切なメンテナンス作業を引き起こすポリシーやプロセスの欠陥に起因しています。

ほとんどの組織はサイバー脅威を認識していますが、こういった脅威に対処する準備が十分に整っていないと回答しています。しかし、それはどの程度なのでしょうか。また、どのエリアでのサポートが求められているのでしょうか。

2018年、アクシスコミュニケーションズとジェネテック社は、企業がサイバー脅威についてどの程度認識していたか、サイバーセキュリティがビジネスにどのような影響を与えたか、そしてどの程度準備していたかについて理解を深めるため、エンドユーザーを対象とした調査を行いました。このレポートは、エンドユーザー企業175社のセキュリティ管理担当者の見解と意見に焦点を当てています。

概要

- 過去5年間に、インターネットに接続しているインフラストラクチャー (IoT) の割合は大幅に増加しています。

- サイバー脅威に対する認識度は高いものの、多くの組織はまだこの問題に積極的に取り組んでいません。

- ほとんどの組織は、自社のインフラストラクチャー、および外部のインテグレーターや設置担当者のセキュリティの成熟度を、中～高と考えています。

- サイバー攻撃は頻繁に発生しており、回答した組織が被害を受けた割合も高くなっています。一般的に攻撃は膨大なコストをもたらし、セキュリティ対策の大幅な再構築と従業員の再訓練が必要になります。サイバー攻撃による信頼の喪失もまた大きな問題です。

- データ侵害はそれほど一般的ではありませんが、これも被害額が大きくなる場合があります。風評被害やデータの喪失も懸念事項です。また、データ侵害も多くの場合、新たなセキュリティ対策や従業員教育の必要性をもたらします。

- 潜在的な攻撃に対する懸念はさほど高くなく、5ポイント評価で平均は3ポイントです。

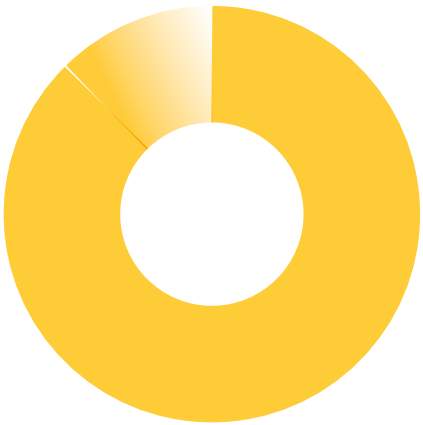
調査結果:

コネクテッドインフラストラクチャーの拡大

質問:5年前、インターネットに接続されていた (IPアドレスを持っていた) インフラストラクチャーの推定割合はどれくらいですか?

エンドユーザーの大多数が、2013年には
インフラストラクチャーの **50〜70%** が…

質問:現在、インターネットに接続されている (IPアドレスを持っている) インフラストラクチャーの推定割合はどれくらいですか?

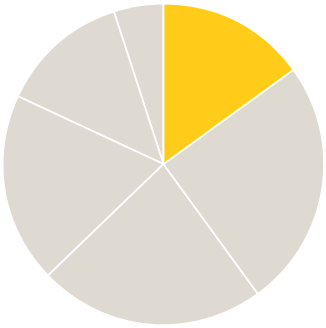


…2018年には **80〜100%** がインターネットに接続されていたと回答しました。

調査結果:

優先事項および準備

質問:貴社ではどの程度サイバーセキュリティの脅威に備えていますか?

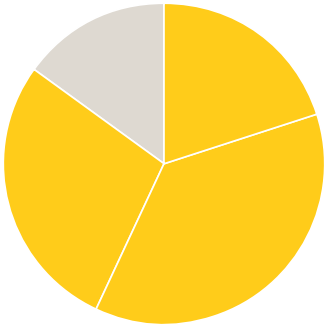


約

15%

のエンドユーザーが十分な準備を
整えていると回答しました

質問:IoTセキュリティにおける組織の優先事項は何ですか?



約

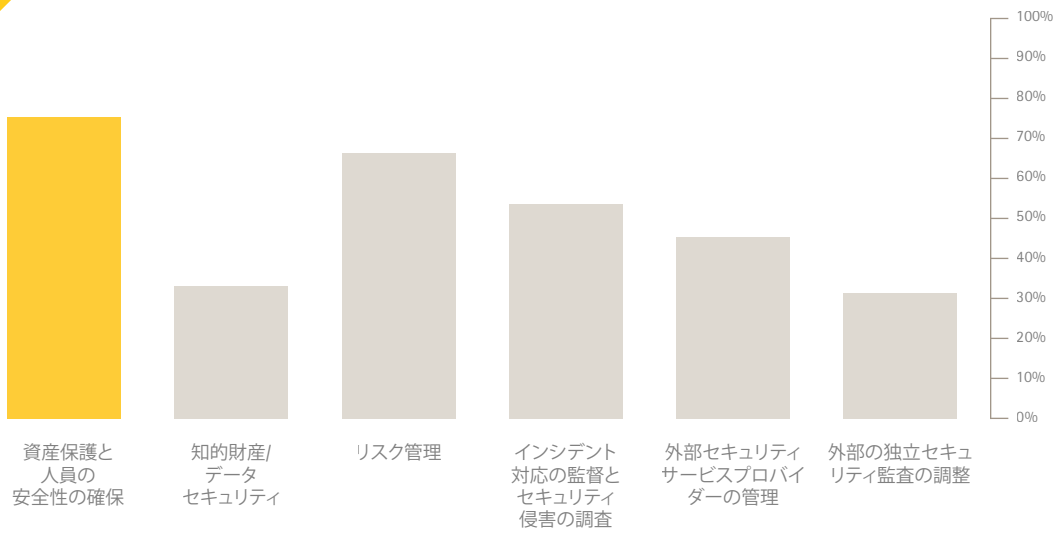
87%

がサイバーをリスクとして優先しています

調査結果:

セキュリティテクノロジーにおける懸念事項

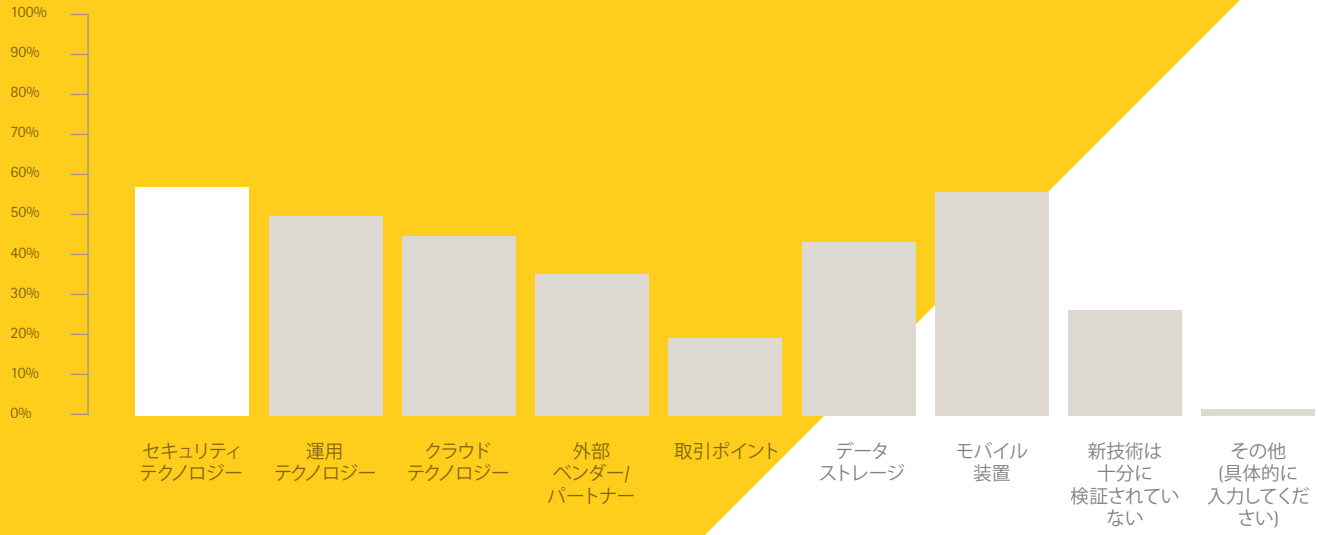
質問:あなたの責務は何ですか?



76%

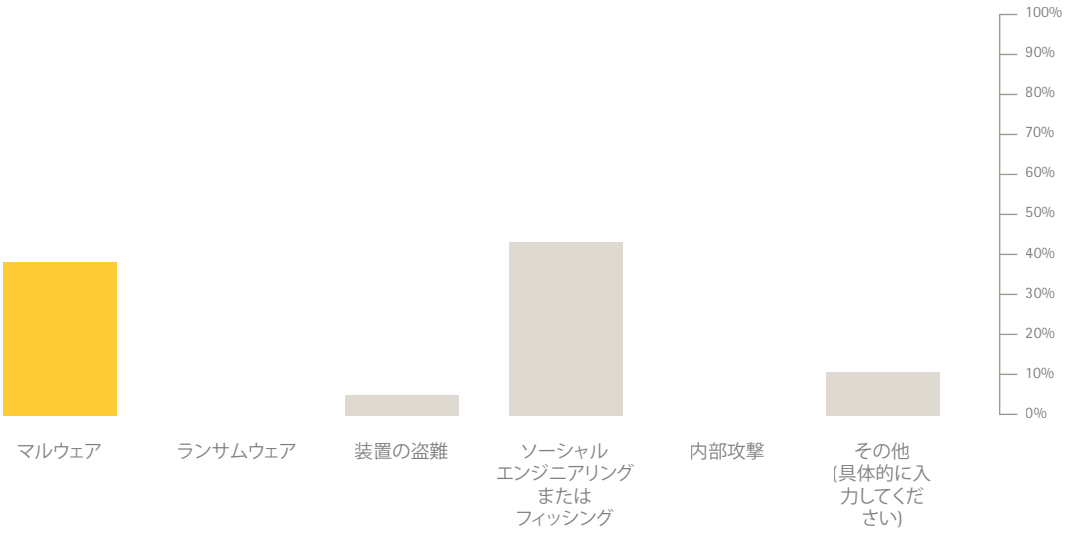
のエンドユーザーが、
安全性と資産の保護が
主な責務であると回答しました。

質問:サイバーセキュリティに対する主な懸念事項となる具体的なベクトルやテクノロジーは何ですか?



一番の
懸念事項は、
セキュリティ
テクノロジーでした

質問:データ侵害の突破口として使用された要因は何ですか?



0%

データ侵害の要因として
内部攻撃を挙げたユーザーはいませんでした

調査結果:

インフラストラクチャーおよびアドバイザーの成熟度

質問:IoTデバイスとテクノロジー、および組織のインフラストラクチャーへの接続が考慮されているIoTアプライアンスのインテグレーターと設置担当者のセキュリティ成熟度について総合的に評価してください

セキュリティテクノロジーとインテグレーター/
設置担当者は共に、サイバー成熟度に関して
「良い」
と評価されました。

調査結果:

サイバー攻撃および
データ侵害の被害

質問:貴社は過去12か月間にサイバー攻撃を受けたことがありますか?

28%

のエンドユーザーが、
過去12か月間にサイバー攻撃を
受けたことを把握しています。

質問:貴社は過去12か月間にデータ侵害を受けたことがありますか?

11%

のエンドユーザーが、
過去12か月間にデータ侵害を
受けたことを把握しています。

調査結果:

サイバーセキュリティ向上に対する主な障害

質問:貴社にとって、IoTの脅威への対処に対する主な障害は何ですか?

59%

のエンドユーザーが、
旧式システムを障害として考えています。

57%

のエンドユーザーが、
社内優先順位の低さと
関連する能力の欠如を挙げています。

調査結果:

サイバーセキュリティ テクノロジーに関する精通度

質問:X.509証明書に精通していますか?

63%

のエンドユーザーが、
X.509証明書について十分な知識がありません。

質問:VMS向けのFIPS 140-2認証は、あなたにとって重要ですか?

71%

のエンドユーザーが、
FIPS 140-2認証について重要ではない、
またはよくわからないと回答しています。

調査結果:

一意のパスワード およびカメラの使用

質問:管理者アカウントのデフォルトのパスワードは変更しますか、それとも使用しますか?

78%

のエンドユーザーが、
デフォルトの管理者アカウント用ログイン
パスワードを変更しています

質問:サーバー管理者アカウントへのログインに使用するデフォルトのパスワードは変更しますか、それとも使用しますか?

76%

のエンドユーザーが、
デフォルトのサーバー管理者アカウント用ログイン
パスワードを変更しています

質問:Security Centerと互換性のあるカメラでHTTPSを使用していますか?

79%

のエンドユーザーが、HTTPSカメラを試用しています

調査方法

調査方法および回答者のプロフィール

記載された結果は、175社の企業による回答に基づいています。回答者はすべて、セキュリティ管理者のための世界最大の組織、ASIS インターナショナルのメンバーです。

以下は調査回答者のプロフィールです。

60%

民間の営利企業に勤務

49%

商業関連企業に勤務

80%

学士号または大学院の学位取得者

76%

安全性と資産の保護を主な責務とする

Axis Communicationsについて

アクシスは、セキュリティの向上とビジネスの新しい推進方法に関する洞察を提供するネットワークソリューションを生み出すことで、よりスマートでより安全な世界の実現を目指しています。ネットワークビデオ業界をけん引するリーダーとして、アクシスは映像監視、インテリジェントアプリケーション、アクセスコントロール、音声システムなどに関連する製品とサービスを提供しています。アクシスは50ヶ国以上に3,000人を超える熱意にあふれた従業員を擁し、世界中のパートナーと連携することで、カスタマーソリューションをお届けしています。アクシスは1984年に創業し、スウェーデン・ルンドに本社を構えています。
より詳しい情報はwww.axis.comをご覧ください。