

【経営層600人に聞く最新セキュリティ対策調査】

大企業経営層の85%以上がサイバーセキュリティを経営リスクとして認識
一方、対策企業の91.9%は「社内セキュリティ」と「Webセキュリティ」を“誤認識”！？

株式会社サイバーセキュリティクラウド(本社:東京都渋谷区、代表取締役社長:大野 暉、以下「サイバーセキュリティクラウド」)はこの度、従業員規模が1~99名、100~299名、300名以上の企業の経営層それぞれ200名ずつ、計600名に対して、「サイバーセキュリティ対策に関する意識調査」を実施し、その調査結果を発表します。

近年増加傾向にある個人情報漏えいをはじめとするサイバー攻撃のリスクについて、企業が実施している対策の実態や課題が見えてきました。

調査結果 サマリー

- ① 経営層全体の7割以上(75.0%)がサイバーセキュリティを経営リスクとして考えていると回答
2018年の個人情報漏えい事件のうち、「Webサイト」が原因の上位8件だけでも
年間の漏えい人数全体の40%以上を占める
- ② 大企業の10%以上(13.5%)が、1年以内にサイバー攻撃の被害に遭ったと回答
被害に遭ったことがある企業の3分の1以上は「情報漏えい」を経験
- ③ サイバーセキュリティ対策をしている企業の約8割(78.3%)は、
「社内セキュリティ」と「Webセキュリティ」どちらも実施していると回答
一方で、90%以上(91.9%)もの経営層は「Webセキュリティ」を誤認識している可能性が
- ④ 従業員規模が100名未満のベンチャー企業の経営層では、
6割以上(61.1%)が自社のセキュリティ対策について把握していないことが判明
- ⑤ 現時点でAIによるセキュリティ対策の強化を行っていない経営層の
およそ4割(38.3%)は、今後AIの導入が必要だと考えていると回答
- ⑥ 2020年、従業員規模300名以上の大企業経営層の半数近く(46.0%)が
サイバーセキュリティへの投資を前年よりも積極的に行っていくと回答

～危険性の高い「Webセキュリティ」対策への意識と実態に大きなギャップ～

近年、AI技術の発達、IoT機器の普及、5Gサービスの開始といった情報革命によって、インターネット(Web)は生活に欠かせないものとなっています。社会・経済のITへの依存度が高まるなかで、サイバーセキュリティリスクも増加し、その対策は企業にとつて必須かつ急務となってきています。

そのなかで、この度の意識調査の結果から、企業のサイバーセキュリティ対策への意識と実態のギャップが浮かび上がってきました。昨今、外部からのサイバー攻撃による企業の個人情報漏えい事件が数多く起きていますが、経営層600名のうち7割以上(75.0%)はサイバーセキュリティを経営リスクとして考えていると回答。さらに従業員規模が300名以上の大企業では、86.0%とより高い危機感を示しました。また、全体の6割以上(66.0%)の企業は実際になにかしらの対策を講じています。

一方で、マルウェアに対してPCや社内ネットワークを守る「社内セキュリティ」は十分な対策がとられているのに対し、ソフトウェアの脆弱性やWebアプリケーション層への攻撃から外部公開サーバを守る、WAF(Web Application Firewall)などの「Webセキュリティ」は、個人情報漏えいのリスクが高いにもかかわらず、認識や対策が不十分な傾向にあることがわかりました。

サイバーセキュリティ対策を実施している経営層の約8割(78.3%)は社内セキュリティとWebセキュリティをどちらも実施していると回答しましたが、そのうちの91.9%は「WAFの導入を実施していない、もしくは実施しているか把握していない」と回答するなど、Webセキュリティそのものを“誤認識”してしまっているケースが見られました。過去に発生したセキュリティインシデントではセキュリティ被害の多くはWeb経由であり、こうした「Webセキュリティ対策は万全である」といった経営層の誤認識が原因のひとつとなっている可能性も考えられます。

調査概要

名称:経営層600人に聞く最新セキュリティ対策調査
調査対象者:20~59歳の役員・経営者(男女)
サンプル数:600名(従業員規模100名未満、100~299名、300名以上の企業各200名ずつ)
調査地域:全国
調査方法:インターネット調査
調査期間:2020年1月24日(金)~2020年1月26日(日)

【報道関係者へのご留意事項】

本リリースの転載にあたりましては、出典として「サイバーセキュリティクラウド調べ」とご記載いただきますようお願い申し上げます。当リリース記載のグラフ等データの提供につきましては、サイバーセキュリティクラウドPR事務局(下記参照)までお問い合わせください。

調査結果

経営リスクとして危機感が高まる“サイバーセキュリティ”対策

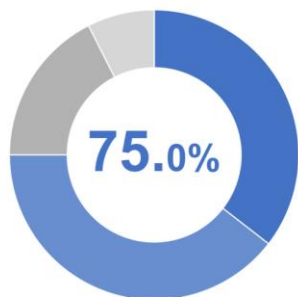
① 経営層全体の7割以上(75.0%)がサイバーセキュリティを経営リスクとして考えていると回答 2018年の個人情報漏えい事件のうち、「Webサイト」が原因の上位8件だけでも 年間の漏えい人数全体の40%以上を占める

全国の企業経営層600名に対して、企業経営においてサイバーセキュリティを経営リスクと考えているか聞くと、全体の7割以上(75.0%)が経営リスクとして考えていると回答しました。さらに、従業員規模300名以上の大企業においては、8割を超える86.0%と、経営層がより高い危機感を示す結果となりました。

2018年の個人情報漏えいに関するインシデント(※1)を見てみると、個人情報漏えいした被害人数の総数は、1年間で実に561万3,797人にまでのぼります。また、漏えい人数の多い上位10件のうち、8件は「Webサイト」への不正アクセスが原因の被害であることがわかっており、その8件の漏えい人数だけでも、計230万859人と個人情報漏えい人数総数の約41%を占めています。

近年増加している企業の個人情報漏えいなどを受け、企業経営におけるサイバーセキュリティのリスクに対して危機感が強まっていることが伺えますが、特に“Webサイト”を起因とする個人情報漏えいは被害人数としてもリスクが高く、企業としても対策が急務であることが見受けられます。

Q.企業経営において、サイバーセキュリティを経営リスクと考えていますか。

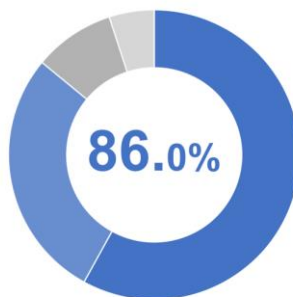


【単一回答、全員、n=600】

経営層全体の7割以上がサイバーセキュリティを経営リスクと考えている

■ そう考えている
■ どちらかといえばそう考えている
■ あまりそう考えていない
■ そう考えていない

Q.企業経営において、サイバーセキュリティを経営リスクと考えていますか。



【単一回答、従業員300名以上の企業、n=200】

従業員規模300名以上の大企業では86.0%とより高い危機感を示す結果に

■ そう考えている
■ どちらかといえばそう考えている
■ あまりそう考えていない
■ そう考えていない

2018年の個人情報漏えいに関するインシデントTop10

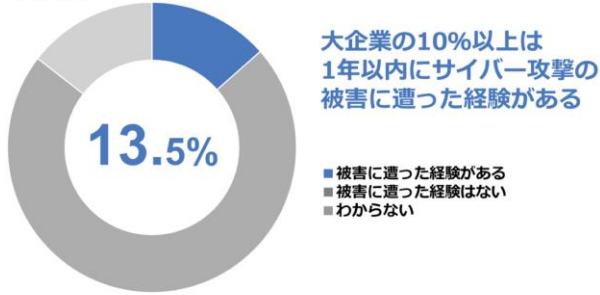
順位	漏えい人数	業種	原因
1	171万2,580人	情報通信業	管理ミス
2	57万0000人	学術研究、専門・技術サービス業	不正アクセス
3	56万1,625人	情報通信業	不正アクセス
4	40万4,254人	情報通信業	不正アクセス
5	37万9,000人	情報通信業	不正な情報持ち出し
6	27万0000人	卸売業、小売業	不正アクセス
7	18万4,181人	情報通信業	不正アクセス
8	12万4,963人	宿泊業、飲食サービス業	不正アクセス
9	9万3,014人	情報通信業	不正アクセス
10	9万2822人	製造業	不正アクセス

出典: NPO日本ネットワークセキュリティ協会「2018年情報セキュリティインシデントに関する調査結果～個人情報漏えい編～」

② 大企業の10%以上(13.5%)が、1年以内にサイバー攻撃の被害に遭ったと回答 被害に遭ったことがある企業の3分の1以上は「情報漏えい」を経験

従業員300名以上の大企業経営層に対して、過去1年間でサイバー攻撃による何らかのセキュリティ被害に遭った経験があるか聞くと、全体の10%以上にも及ぶ13.5%がサイバー攻撃による被害に遭ったことがあると回答しました。また、被害に遭ったことがある企業のうち、3分の1以上(38.5%)が「情報漏えい」を経験していると判明。被害に遭った経験があるサイバー攻撃の種類は、1位から「システムの障害(42.3%)」、「情報漏えい(38.5%)」、「業務データの破壊・損失(30.8%)」がトップ3となりました。サイバー攻撃による個人情報漏えいの被害が、多くの会社にとって身近に起きている事件であることが見受けられます。

Q.過去1年間で、サイバー攻撃による何らかのセキュリティ被害に遭った経験がありますか。



【単一回答、従業員300名以上の企業、n=200】

Q.サイバー攻撃の被害の種類として当てはまるものをお答えください。



【複数回答、直近1年でサイバー攻撃の被害を経験した企業、n=52】

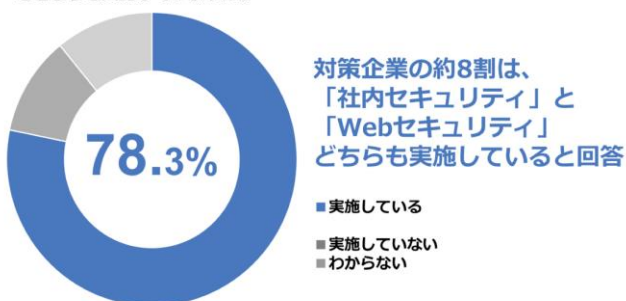
企業のサイバーセキュリティに対する意識と実態のギャップ

③ サイバーセキュリティ対策をしている企業の約8割(78.3%)は、「社内セキュリティ」と「Webセキュリティ」どちらも実施していると回答 一方で、90%以上(91.9%)もの経営層は「Webセキュリティ」を誤認識している可能性が

経営層600名に対して、現在、自社でサイバーセキュリティ対策を行っているか聞くと、全体の6割以上(66.0%)が現在サイバーセキュリティ対策を行っていると回答。さらに、そのうちの約8割(78.3%)は、マルウェアに対してPCや社内ネットワークを守るための「社内セキュリティ」と、ソフトウェアの脆弱性やWebアプリケーション層への攻撃から外部公開サーバを守るためのWAF(Web Application Firewall)をはじめとする「Webセキュリティ」をどちらも実施していると回答しました。

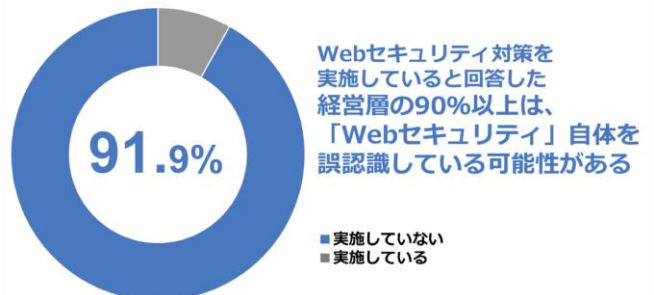
一方で、さらにそのうちの9割以上(91.9%)は、「Webセキュリティ」を実施していると回答したにもかかわらず、「WAFの導入を実施していない、もしくは実施しているか把握していない」と回答するなど、不正アクセスの侵入口となるWebアプリケーション層への対策である「Webセキュリティ」そのものを「誤認識」している可能性があることがわかりました。

Q.セキュリティ対策において「社内セキュリティ」と「Webセキュリティ」をどちらも実施していますか。



【単一回答、サイバーセキュリティ対策企業、n=396】

Q.セキュリティ対策において「WAF」の導入を実施していますか。



【単一回答、社内・Web両セキュリティ対策企業、n=310】

④ 従業員規模が100名未満のベンチャー企業の経営層では、6割以上(61.1%)が自社のセキュリティ対策について把握していないことが判明

経営層に対して、会社で実施している具体的なセキュリティ対策について聞くと、全体の2人にひとり以上となる52.0%は、具体的なセキュリティ対策は「わからない／情報システム部門等社内の担当部署に任せている」と回答しました。さらに、従業員が100名未満のベンチャー企業の経営層では、60%を超える(61.1%)など、より顕著な結果となりました。企業の経営層は、サイバーセキュリティが経営リスクになると感じている一方で、自社で実施しているセキュリティ対策への理解が不十分であることが伺えます。

Q.あなたの会社で実施しているセキュリティ対策について当てはまるものをお選びください。



【複数回答、サイバーセキュリティ対策企業、n=396】

Q.あなたの会社で実施しているセキュリティ対策について当てはまるものをお選びください。



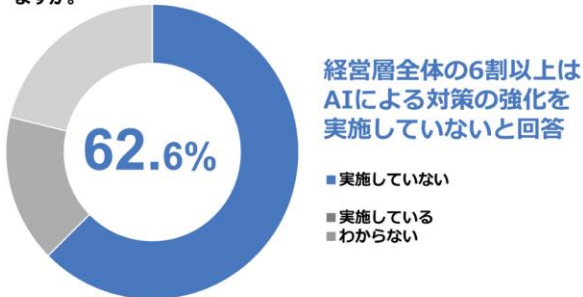
【複数回答、従業員100名未満のサイバーセキュリティ対策企業、n=95】

AIの活用や、2020年のセキュリティ対策への投資

⑤ 現時点でAIによるセキュリティ対策の強化を行っていない経営層のおよそ4割(38.3%)は、今後AIの導入が必要だと考えていると回答

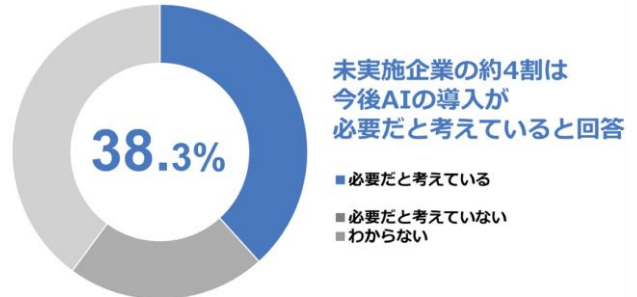
調査対象企業のうち、AIを搭載したセキュリティ対策の強化を実施している企業は全体の16.2%にとどまり、6割以上(62.6%)はAIによる対策の強化を実施していないと回答しました。しかし、AIを搭載したセキュリティ対策の強化を行っていないと回答した企業のうち、およそ4割(38.3%)の企業では、今後AIの導入が必要だと考えていることがわかりました。近年の情報革命によって社会・経済のITへの依存度が高まるなかで、AIが搭載されたサイバー攻撃も増加するなどその危険性は高まっており、今後、防御側のシステムにもAI搭載のニーズが増加していくことが予想されます。

Q.あなたの会社では、AIを搭載したセキュリティ対策の強化を実施していますか。



【単一回答、サイバーセキュリティ対策企業、n=396】

Q.セキュリティ対策において、AIの導入が必要だと考えていますか。



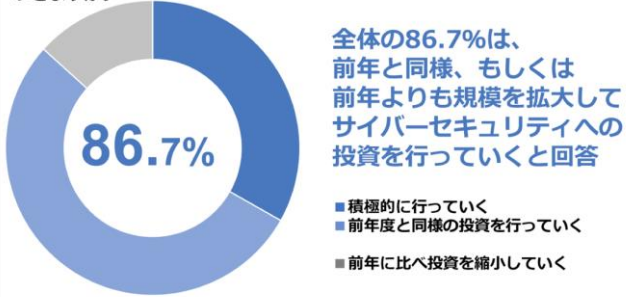
【単一回答、AIによる対策強化未実施企業、n=248】

⑥ 2020年、従業員規模300名以上の大企業経営層の半数近く(46.0%)がサイバーセキュリティへの投資を前年よりも積極的に行っていると回答

経営層600名に対して、2020年、サイバーセキュリティへの投資について聞くと、全体の9割近くとなる86.7%は、前年と同様、もしくは前年よりも規模を拡大してサイバーセキュリティへの投資を行っていると回答。さらに、従業員規模300名以上の大企業では、半数近く(46.0%)もの経営層が前年よりもサイバーセキュリティへ積極的に投資していくと回答しました。

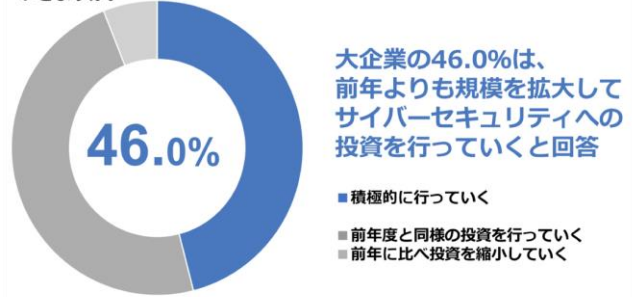
2020年、国際的な大会が日本で開催されることを受け、サイバー攻撃の数も増加することが予想されていますが、企業経営の大きな選択として、サイバーセキュリティへの投資を拡大する企業も増えていくことが伺えます。

Q. 2020年、サイバーセキュリティへの投資を前年に比べ積極的に行っていきますか。



【単一回答、全員、n=600】

Q. 2020年、サイバーセキュリティへの投資を前年に比べ積極的に行っていきますか。



【単一回答、従業員300名以上の企業、n=200】

■株式会社サイバーセキュリティクラウドについて

会社名：株式会社サイバーセキュリティクラウド

所在地：〒150-0011 東京都渋谷区東3-9-19 VORT恵比寿maxim3階

代表者：代表取締役社長 大野 暉

設立：2010年8月

URL：<https://www.cscloud.co.jp/>

「世界中の人々が安心安全に使えるサイバー空間を創造する」という理念を掲げ、サイバーセキュリティクラウドでは、世界有数のサイバー脅威インテリジェンスとAI技術を活用した、Webアプリケーションのセキュリティサービスを全世界に向けてサブスクリプションで提供しています。また、クラウド市場世界シェア47.8%(※2)を持つAWSにおいて、世界で7社目となるAWS WAFマネージドルールセラーにも認定されております。

これからも私たちは、リーディングカンパニーとして、世界中の人々が安心安全に利用できるサイバー空間を創造するためのサービス開発を行い、情報革命の推進に貢献してまいります。

※1 出典：NPO日本ネットワークセキュリティ協会「2018年情報セキュリティインシデントに関する調査結果～個人情報漏えい編～」

※2 出典：Gartner(July 2019)・・・Worldwide IaaS Public Cloud Services Market Share, 2017-2018 (Millions of U.S. Dollars)

* 本リリースに記載された会社名、サービス名等は該当する各社の登録商標です。

* アマゾンウェブサービス、AWSは、Amazon.com, Inc.またはその関連会社の商標です。

* 本リリースの情報は発表日現在のものです。最新の情報とは異なる場合がありますのでご了承ください。

<本件のお問い合わせ>

■サービスに関するお問い合わせ先

株式会社サイバーセキュリティクラウド

Webセキュリティ事業部 PR・マーケティングチーム

電話：03-6416-9996 FAX：03-6416-9997

E-mail：pr@cscloud.co.jp