

本サービスにおける著作権および一切の権利はアイティメディア株式会社またはその情報提供者に帰属します。また、本サービスの出力結果を無断で複製・複製・転載・転用・頒布等を行うことは、法律で認められた場合を除き禁じます。

10人に7人が「DDoS攻撃が何か知らない」と回答：

## 「日本の従業員はセキュリティへの関心が薄い」——A10が企業のサイバー攻撃への意識調査公開

<http://www.atmarkit.co.jp/ait/articles/1803/13/news027.html>

A10ネットワークスは、日本を含む10カ国のIT管理者と従業員約2000人を対象にした「企業のサイバー攻撃の実態やセキュリティ意識に関する調査結果」を公開した。同社によれば、日本企業の多くが、サイバー攻撃を受けたにもかかわらず、気付いていない可能性があるという。

2018年03月13日 11時00分 更新




[@IT]

A10ネットワークスは2018年3月9日、日本を含む10カ国のIT管理者と従業員約2000人を対象にした「企業のサイバー攻撃の実態やセキュリティ意識に関する調査結果」を公開した。

IT管理者を対象にした質問のうち、情報漏えいやDDoS攻撃、ランサムウェアといったサイバー攻撃の経験が「ある」と回答した割合が最も高かったのは米国で、最も低かったのは日本だった。ただし、日本は「被害に遭ったかどうか把握していない」と回答した割合が高かったことから、A10ネットワークスでは「日本企業は他国に比べて被害が少ないのではなく、サイバー攻撃に気付いていない可能性がある」としている。

また、調査の対象になったIT管理者の47%が「情報漏えいの被害に遭ったことがある」と回答。同様の回答を寄せた割合を国別にみると「米国(71%)」が最高で、「日本(18%)」が最低だった。一方、「過去1年間にDDoS攻撃を受けたことがある」と回答した割合は全体で38%。米国は61%、日本は21%だった。

IT管理者に聞くサイバー攻撃の被害状況の実態

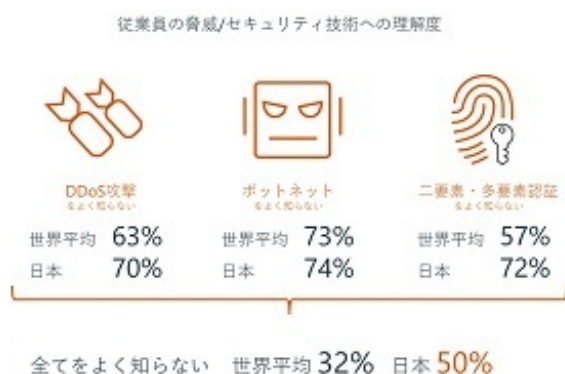
	 情報漏えい		 DDoS攻撃 <small>過去1年以内</small>		 ランサムウェア	
	経験	把握せず	経験	把握せず	経験	把握せず
世界平均	47%	10%	38%	9%	22%	8%
米国	71%	4%	61%	2%	47%	3%
ブラジル	61%	5%	34%	5%	17%	9%
イギリス	54%	9%	41%	11%	30%	7%
インド	54%	11%	29%	12%	18%	8%
韓国	47%	12%	32%	13%	26%	8%
フランス	46%	9%	40%	8%	25%	6%
ドイツ	45%	18%	45%	9%	15%	8%
シンガポール	45%	12%	40%	8%	20%	7%
中国	36%	7%	34%	2%	14%	2%
日本	18%	15%	21%	22%	7%	10%

出典：A10 Networks Inc. 「アプリケーションインテリジェンスレポート」

各国のIT管理者を対象にした調査の結果（提供：A10ネットワークス）

「少なくとも1度はランサムウェアの被害にあった」と回答した割合は、全体で22%、「ランサムウェアによる攻撃があったかもしれないが、最終的には不明」と回答した割合は、26%だった。「ランサムウェアの被害を経験している」と回答した割合は、最も多い米国で47%、最も低い日本で7%だった。

次に、従業員に対する調査では、「DDoS攻撃が何であるか知らない(全体:63%、日本:70%)」「botネットについて知らない(全体:73%、日本:74%)」「2要素または多要素認証を知らない(全体:57%、日本:72%)」などの回答が集まった。また、「(DDoS攻撃、botネット、2要素または多要素認証について)全て知らない(全体:32%、日本:50%)」と回答した割合は、日本の割合が全体よりも高かった。



出典：A10 Networks Inc. 「アプリケーションインテリジェンスレポート」

従業員に対するセキュリティ脅威の理解度調査の結果(提供:A10ネットワークス)

A10ネットワークスでは、これらの結果から「日本の従業員のセキュリティへの関心のなさがうかがえる」としている。また、日本の従業員の43%が、「ビジネスアプリや個人情報の管理責任はIT部門にある」と回答した点について、「さらに不安を煽る。セキュリティについての理解や意識が足りない従業員を脅威から守ることは困難だからだ」としている。

## 関連記事



### [インターネットで大規模障害、DDoS攻撃か？](#)

8月のセキュリティクラスタは毎年恒例となっている「セキュリティ・キャンプ」の話題が大盛り上がりでした。この他、大きな動きが2つ。1つ目はいろいろなWebサイトでSQLのダンプファイルが公開されており、企業サイトで情報漏えいが発生したこと。2つ目は大規模な接続障害が発生したことです。一時はDDoS攻撃かもしれないと疑われました。



### [利便性よりもセキュリティ、パスワードよりも生体認証——IBM、IDや認証に関する意識調査を発表](#)

IBMの「IDの未来に関する調査」によると、デバイスやアプリケーションなどにログインする際には、利便性よりもセキュリティが優先される傾向が強く、指紋読み取り、顔認識、音声認識といった生体認証テクノロジーのメリットを認識している回答が多かった。この傾向が強い若年層が今後の市場をけん引する可能性も指摘する。



### [2018年のサイバーセキュリティ脅威はどうなる？](#)

2018年は前年に引き続き、ランサムウェアやIoTを用いた攻撃の脅威がそのまま残るとというのが各社に共通する予測です。2018年はサプライチェーン攻撃や仮想通貨に関連した攻撃、ビジネスメール詐欺(BEC)が拡大する可能性があります。AIを利用した新種の攻撃を示唆するセキュリティ企業もありました。

## 関連リンク

