2021年 7 月 13 日
Ivanti Software 株式会社

【コロナ禍におけるサイバー攻撃に関する実態調査】

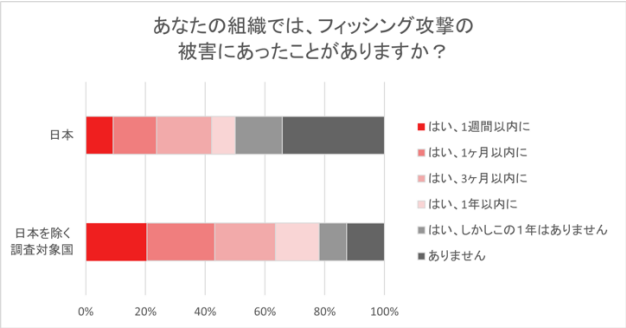
日本、90%超がリモートワーク普及でサイバーセキュリティに不安抱える
巧妙化するフィッシング・ランサムウェア、１年以内で 50%が被害経験
～日本の IT 人材の不足が顕著に～

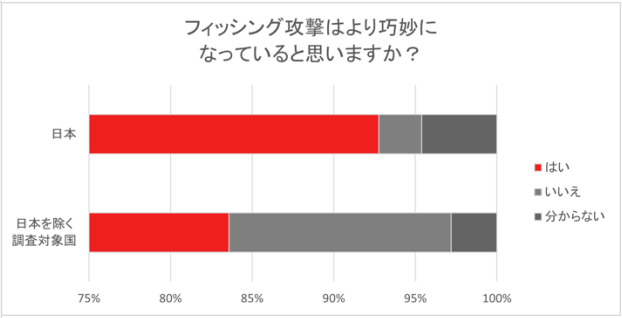
あらゆる IT 接続をよりスマートに、より安全にするオートメーションプラットフォームを提供している Ivanti（本社：ユタ州ソルトレイクシティ、代表者：Jim Schaper）は、コロナ禍で働き方が変化しリモートワークの標準化が加速するなか、米国・英国・フランス・ドイツ・オーストラリア/ニュージーランド・日本の IT 担当者 1,000 名以上を対象にフィッシングやランサムウェアなどサイバー攻撃に関する実態調査を実施しました。

＜調査結果の概要＞
■巧妙化するフィッシング・ランサムウェア攻撃
■リモートワーク普及でサイバーセキュリティへの不安も強く、日本では9割超
■IT人材の不足、日本では8割近く、サイバー攻撃へのリスク要因に

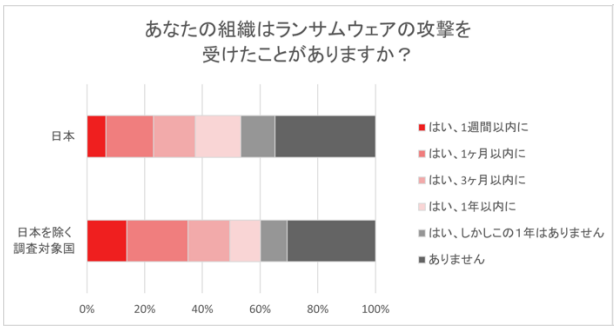
＜調査実施概要＞
・調査時期　：　2021 年 4 月 30 日～5 月 29 日
・調査対象　：　米国・英国・フランス・ドイツ・オーストラリア/ニュージーランド・日本
　　従業員数 500 名以上の企業で働く IT 担当者　1,005 名

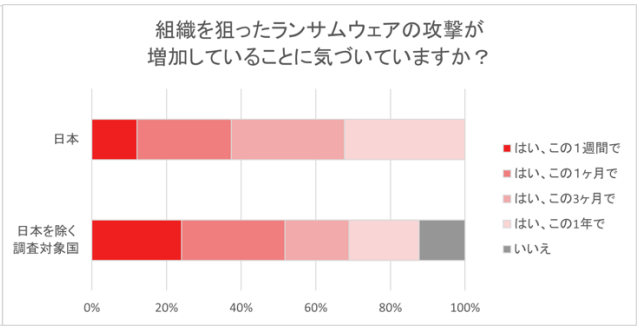
■巧妙化するフィッシング・ランサムウェア攻撃



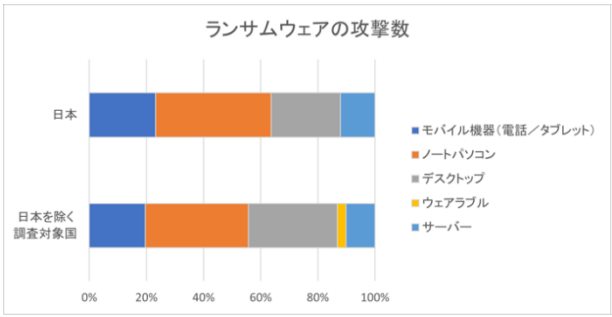


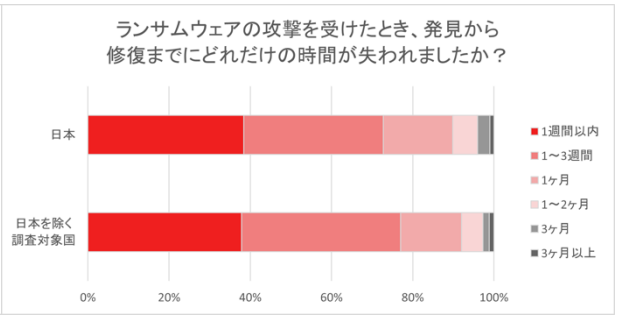
１年以内に自社がフィッシング攻撃の被害にあったと回答した人の割合は、オーストラリア/ニュージーランドが 96%と最も多く、次いでフランスが 83%、日本は 50%という結果となりました。また、以前に比べてフィッシング攻撃はより巧妙になっていると思いますか？との問いには、日本を除く調査対象国（米国、英国、フランス、ドイツ、オーストラリア/ニュージーランド）で 85%、日本では 93%の人が「巧妙になっている」と回答しました。





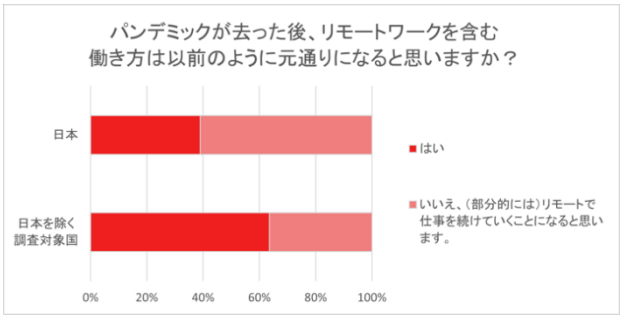
１年以内に自社がランサムウェアの被害にあったと回答した人の割合は、オーストラリア/ニュージーランドが 93%と特出して多く、日本は 53%という結果となりました。組織を狙ったランサムウェアの攻撃が増加していると思いますか？との問いには、日本を除く調査対象国で 88%、日本では 100%の人が「増加している」と回答しました。

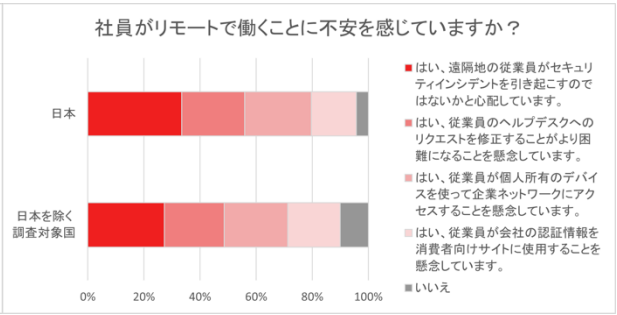




ランサムウェアの攻撃をデバイス別に見ると、日本はノートパソコンが 40%と最も多く、デスクトップ（24%）、モバイル機器（23%）、サーバー（12%）と続きました。また、ランサムウェアの攻撃を受けた際の、発見から修復までにかかった時間について、1 週間以内と回答した人が 38%いる一方で、1 ヶ月以上時間を要している人が 27%いることが判明しました。日本を除く調査対象国でも同様の傾向が見られました。

■リモートワーク普及～日本は9割超がサイバーセキュリティーに不安、他国より 10 ポイント以上高く

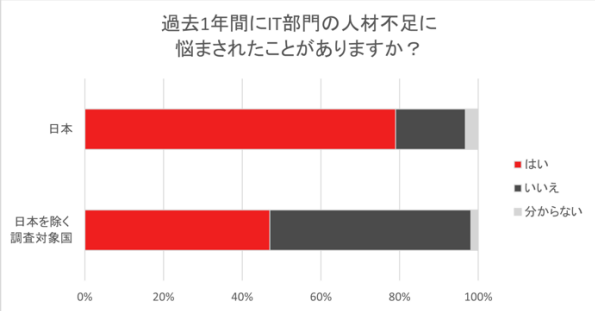


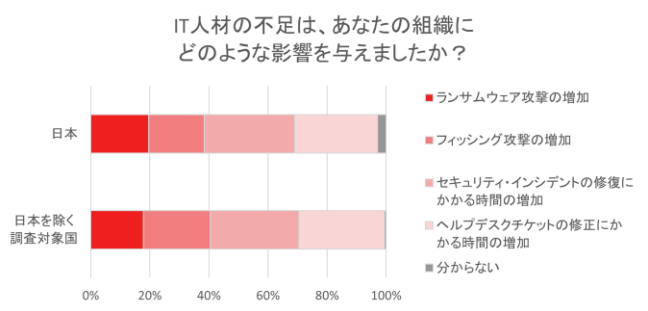


新型コロナウイルスのパンデミックが去った後、リモートワークを含む働き方は以前のように元通りになると思いますか？との問いに、日本は「いいえ」と回答した人の割合が 61%と調査対象国の中で最も多くなりました。リモートワークがそれほど進んでいなかった日本において、コロナ禍により急速にリモートワークが普及拡大したことが背景にあると考えられます。

また、日本を含む調査対象国全体で 9 割以上がサイバーセキュリティのトレーニングを実施している一方で、社員がリモートワークで働くことに不安を感じていますか？との問いには、日本では 92%と、日本を除く調査対象国より 10 ポイント以上高くサイバーセキュリティに不安を感じていることがわかりました。

■IT人材の不足、日本では8割近く、サイバー攻撃へのリスク要因に





過去 1 年間で IT 部門の人材不足に悩まされたことがあると答えた人の割合は、日本を除く調査対象国が 47%に対し、日本は 79%という結果となりました。さらに、その人材不足は新型コロナウイルスの影響によるものか調査したところ、日本は 28%の人がコロナによるものではないと回答しており、常態的に IT 人材が不足している状況がうかがえました。

さらに、IT 人材の不足は組織にどのような影響を与えましたか？との問いには、セキュリティインシデントの修復やヘルプデスクチケットの修正にかかる時間の増加と回答した人が約 6 割、ランサムウェア攻撃やフィッシング攻撃の増加が約 4 割という結果となりました。日本では IT 人材の不足によってサイバー攻撃に対する様々なリスクが生じていることが明らかになりました。

◆Ivanti について

Ivanti は「Everywhere Workplace」を実現します。「Everywhere Workplace」では、働く場所にかかわらず、従業員は多種多様なデバイスでさまざまなネットワークから IT アプリケーションやデータにアクセスし、高い生産性を保つことができます。Ivanti Neurons 自動化プラットフォームは、業界をリードする統合エンドポイント管理、ゼロトラストセキュリティと、エンタープライズサービス管理のソリューションをつなぎ、デバイスの自己修復および自己保護、またエンドユーザーのセルフサービスを可能にする統合 IT プラットフォームを提供します。 Fortune 100 の 78 社を含む 40,000 社以上のお客さまが、クラウドからエッジまで IT 資産を検出、管理、保護、保守し、働く場所にかかわらず従業員に優れたエンドユーザー体験を提供するために Ivanti を選択しています。 詳細については、www.ivanti.co.jp をご参照ください。