

報道関係者各位

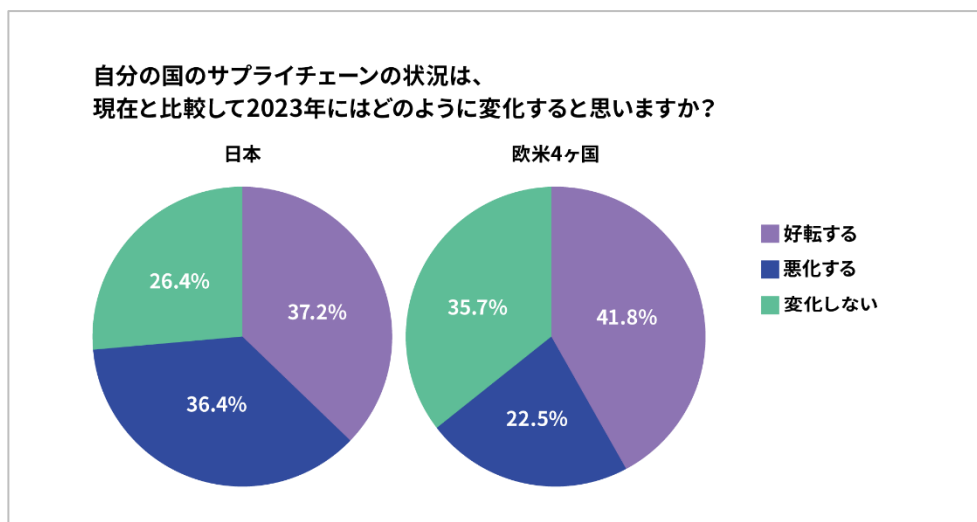
グローバルサプライチェーンの混乱とサイバーセキュリティに関する 5ヶ国でのリサーチの結果をウイズセキュアが発表

～ 日本は欧米と比較し、自国のサイバーセキュリティ対策が不十分だという認識 ～

2022年10月5日
ウイズセキュア株式会社

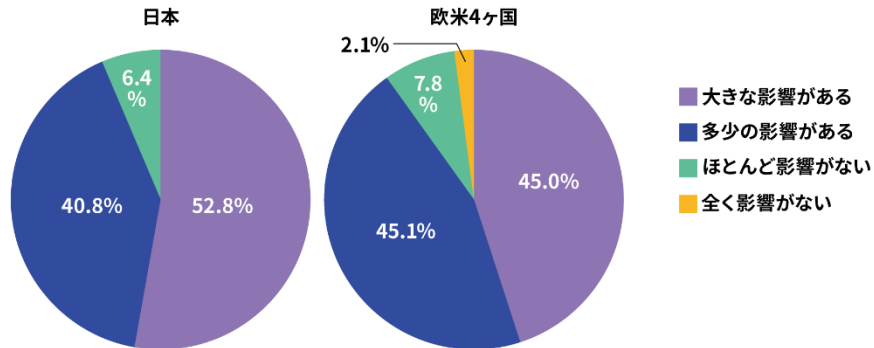
2020年に発生した新型コロナウイルスのパンデミックに端を発したグローバルサプライチェーンの混乱は、本年においてもその深刻さが増しています。先進的サイバーセキュリティテクノロジーのプロバイダーである WithSecure (旧社名: F-Secure、本社: フィンランド・ヘルシンキ、CEO: Juhani Hintikka、日本法人: 東京都港区、以下、ウイズセキュア) は、本年8月に日本/アメリカ/フランス/ドイツの各国250名とイギリス256名の合計1,256名のIT意思決定者に対して実施したグローバルサプライチェーンとサイバーセキュリティとの関連についての調査の結果を発表しました。

「自分の国のサプライチェーンの状況は、現在と比較して2023年にはどのように変化すると思いますか？」との質問に対し、日本以外の4ヶ国の対象者の22.5%が「悪化する」という見通しを持っているのに対し、日本の対象者のうち36.4%がそう回答していることです。これは、日本が外国からの資源/物資の輸入に依存する割合が高いこと、そして島国であるがために船舶や飛行機での輸送に依存していることを表していると考えられます。



また、グローバルのサプライチェーンの多くがオンラインで運営されているなか、様々なサイバーセキュリティの問題がサプライチェーンに与える影響に関する問題については、日本のIT意思決定者の52.8%、そしてその他4ヶ国の45%が「かなり影響がある」と回答しています。さらに、「多少の影響がある」と回答した日本40.8%と欧米の45.1%を追加すると、それぞれ90%以上がサプライチェーンへのセキュリティ問題を深刻に受け止めています。

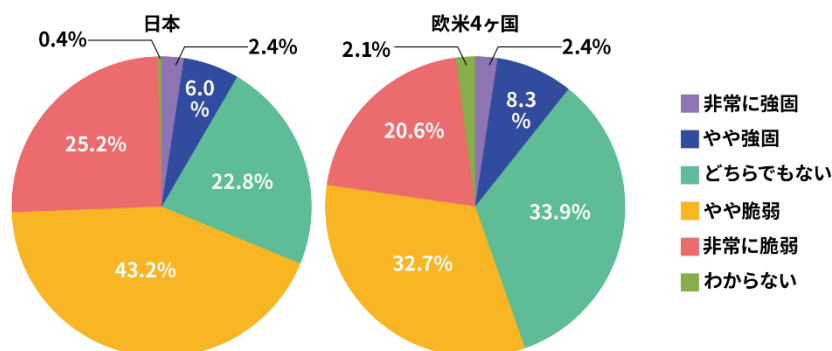
サイバーセキュリティがサプライチェーンに与える影響はどの程度あると考えますか？



特筆すべきは、「自分の国が他国と比較してサイバー攻撃に対して強固／脆弱である」という点において、日本以外の国では 53.3%が「やや脆弱」または「かなり脆弱」と考えているのに対し、日本ではこの割合が 68.4%とかなり高くなっています。この違いについて、ウィズセキュアでアジアパシフィック地域担当バイスプレジデントを務める John Duley (ジョン・デューリー) は次のように語っています。

「欧米と比較して、日本ではまだセキュリティが『コスト』として考えられており、何か起こってから対応／投資するケースが多く見受けられます。そういった中で、セキュリティに十分に投資していると考える経営層と、まだ十分ではないと感じる、今回回答者となっている現場の IT 意思決定者との認識の温度差があり、こうした回答につながっているのではないのでしょうか。また、日本人は気質的にも控えめに見積もる傾向にあるため、そうした点からも自分たちの環境が脆弱であると感じていることもあると考えます。」

自分の国は他国と比較してサイバー攻撃に対して強固／脆弱だと思いますか？



クラウドの導入における最大のメリットとしては(複数回答)、日本が「複数デバイス間でのクラウド」(53.2%)、「バックアップとリカバリー」(50.0%)、「アクセスの容易さ」(45.6%)が上位に挙げられ、欧米では「バックアップとリカバリー」(57.5%)が1位となり、「アクセスの容易さ」(53.3%)、「セキュリティ」(48.6%)が続いています。デメリットを感じるものとしては、日本では「ハッキング」(48%)、「継続的なコスト」(41.6%)、「データ損失」および「不安定な回線などの技術的な問題」(ともに 40.4%)が上位に挙げられ、欧米ではそれが「ハッキング」(56.0%)、「不安定な回線などの技術的な問題」(49.3%)、「データ損失」(41.4%)という順位となっています。

その他、今回の調査での回答の一部は以下のとおりです：

- グローバルサプライチェーンの混乱は、今後何年続くと考えていますか？
 - 日本： 1年以下 (8.0%) 2年から3年 (61.2%) 4年以上 (30.8%)
 - 欧米： 1年以下 (15.0%) 2年から3年 (54.5%) 4年以上 (30.5%)
- クラウドに機密性の高いコンテンツ(プライベートメッセージ、写真、文書など)を保存していますか？
 - 日本： はい (66.0%) いいえ (32.0%) 回答保留 (2.0%)
 - 欧米： はい (63.5%) いいえ (32.4%) 回答保留 (4.1%)
- 生活必需品のうちオンラインで購入する割合は？
 - 日本： 0-20% (24.0%) 21-40% (41.6%) 41-60% (23.6%) 61-80% (9.6%) 81-100% (1.2%)
 - 欧米： 0-20% (21.8%) 21-40% (28.1%) 41-60% (29.1%) 61-80% (16.0%) 81-100% (5.0%)

サプライチェーンに属する企業が一旦サイバー攻撃を受けてしまうと、既に発生している混乱がさらに悪化することが想定されます。ウィズセキュアのサイバーセキュリティアドバイザーである Paul Brucciani (ポール・ブルッチアーニ) は、グローバルサプライチェーンとサイバーセキュリティの関係について、以下のコメントで締めくくっています。「大企業のサプライチェーンには何万ものサプライヤーが存在し、攻撃は増加の一途をたどり、どの業界も無防備ではられません。サプライチェーンの全てのステージで働く一人ひとりが標的となる可能性があるのです。企業は、従業員やサプライヤーがどのように危険にさらされる可能性があり、どのように自らを守ることができるかを理解することで、供給リスクを減らすことができます。侵入の4分の3は、強力なパスワードと多要素認証を使用し、不審なメールに注意することで防ぐことができます。効果的なサイバーセキュリティ対策を行い、常にデータのバックアップを取ることで、リスクの多くを軽減することができるのです。」

WithSecure Web サイト:

<https://www.withsecure.com/jp-ja/>

WithSecure プレスページ:

<https://www.withsecure.com/jp-ja/whats-new/pressroom>

WithSecure について

WithSecure™は、IT サービスプロバイダー、MSSP、ユーザー企業、大手金融機関、メーカー、通信テクノロジープロバイダー数千社から、業務を保護し成果を出すサイバーセキュリティパートナーとして大きな信頼を勝ち取っています。私たちは AI を活用した保護機能によりエンドポイントやクラウドコラボレーションを保護し、インテリジェントな検知と対応によりプロアクティブに脅威を探し出し、当社のセキュリティエキスパートが現実世界のサイバー攻撃に立ち向かっています。当社のコンサルタントは、テクノロジーに挑戦する企業とパートナーシップを結び、経験と実績に基づくセキュリティアドバイスを通じてレジリエンスを構築します。当社は 30 年以上に渡ってビジネス目標を達成するためのテクノロジーを構築してきた経験を活かし、柔軟な商業モデルを通じてパートナーとともに成長するポートフォリオを構築しています。

1988 年に設立された WithSecure は本社をフィンランド・ヘルシンキに、日本法人であるウィズセキュア株式会社を東京都港区に置いています。また、NASDAQ ヘルシンキに上場しています。詳細は www.withsecure.com をご覧ください。また、Twitter @WithSecure_JP でも情報の配信をおこなっています。