

## Economist Intelligence Unit (EIU) と Arbor Networks の調査により、 83% の企業でオンライン・セキュリティ・インシデント対策が万全ではないことが判明

英国ロンドン、2014年3月19日ーエンタープライズやサービス・プロバイダーのネットワーク向けに分散型サービス拒否 (DDoS) 攻撃や高度な脅威の対策ソリューションを提供するリーディング・プロバイダ [Arbor Networks, Inc.](#) (以下「Arbor Networks」) は、本日、Economist Intelligence Unit (EIU) に依頼したインシデント対応への取り組みに関する調査の結果を発表しました。EIU の調査は 360 名のビジネス・リーダーを対象とし、その大部分 (73%) は C レベルの管理者または取締役会メンバーです。世界各国の企業が参加しており、内訳は、31% が北米、36% が欧州、29% がアジア太平洋となっています。

『[Cyber incident response: Are business leaders ready?](#) (サイバー・インシデントへの対応: ビジネス・リーダーの準備は万全か?)』と題されたレポートでは、77% の企業が過去 2 年間にセキュリティ・インシデントに見舞われているにもかかわらず、インシデント対応計画を整備していない企業の割合が 3 分の 1 を超えている (38%) ことが明らかとなりました。オンライン・セキュリティ・インシデントへの対策が万全である企業は、世界全体で 17% に過ぎません。

インシデント対応計画を推進し、対策が比較的万全である企業では、ほとんどの場合、IT 部門が対策を担当していますが、大部分の企業は、IT フォレンジック調査員、専門弁護士、法執行機関などの外部業者にも協力を依頼しています。

Economist Intelligence Unit のシニア・エディターであるジェイムズ・チェンバースは、「企業においては、本格的なインシデント対策の導入に向けた動きが活発化しています。しかし、脅威の発生源や影響を予測することの困難さが増す中、企業幹部としては、インシデント対応を単なる既製の計画ではなく組織の実状に即したものにすることが必要です」と述べています。

Arbor Networks プレジデントのマシュー・モイナハン (Matt Moynahan) は、「このレポートが指摘しているように、サイバー攻撃に関しては、私たちは『もし発生したら』ではなく『発生したときには』の世界に生きています。最近では小売業界で衝撃的な標的型攻撃が発生していることから、企業がインシデントを速やかに検出して特性を把握し、対応計画を実行できることは、企業の資産や顧客データを保護するためだけでなく、企業のブランド、評判、利益を守るうえでも非常に重要となっています」と述べています。

### 調査結果の概要:

#### 脅威に対する理解の不足が対策のレベル向上を妨げている

- インシデントへの対策が万全であると考えているビジネス・リーダーは、全体の 17% に過ぎません。
- ビジネス・リーダーの 41% は、潜在的な脅威に対する理解が深まれば、対策をより万全にできると考えています。
- 本格的な計画やチームが存在することは、対策が万全であることに対する企業幹部の意識に大きな影響を与えます。

- 企業の半数は、セキュリティ侵害が発生した場合に生じるビジネスへの影響を予測できないと感じています。

#### 企業としての評判を重視することが本格的な計画やプロセスの確立につながる

- 調査の対象となった企業幹部の 3 分の 2 が、インシデントに対して効果的な対応をすることは企業としての評判を高めることにつながると回答しています。
- インシデント対応のチームおよび計画を既に導入している組織の割合は、今後数年のうちに 80% を超えるレベルまで増加すると考えられます。
- 外部の専門家に依頼する割合は、過去 24 か月間にインシデントを経験した企業において、経験していない企業の 2 倍に達しています。

#### 詳細情報

##### 企業はインシデントの公表や脅威に関する情報の共有に前向きではない

- 組織の 57% は、法的に強制されない限りインシデントについて自発的に報告しないと回答しています。
- ベスト・プラクティスの普及や他社との比較による自社のインシデント対応の評価を目的としてインシデントの情報を他社と共有している企業は、全体の 3 分の 1 に過ぎません。

#### 追加リソース:

- レポートの全文をダウンロードするには、[www.arbornetworks.com/ciso/eiureport](http://www.arbornetworks.com/ciso/eiureport) (英文) をクリックしてください。
- 主な調査結果については、Arbor Networks のブログ ([www.arbornetworks.com/corporate/blog](http://www.arbornetworks.com/corporate/blog)) をご覧ください。
- Twitter で @arbornetworks をフォローすると、詳細な調査結果をご覧ください。

#### Economist Intelligence Unit について

Economist Intelligence Unit は、グローバル・ビジネス・インテリジェンスにおける世界的なリーダーであり、『The Economist』誌の発行元である The Economist Group の B2B 部門です。Economist Intelligence Unit は、カンントリー・インテリジェンスの世界的なリーディング・プロバイダとして、世界全体の市場動向やビジネス戦略に関するタイムリーで信頼性の高い公正な分析結果を提供することにより、企業幹部のよりの確かな意思決定に貢献しています。Economist Intelligence Unit の詳細については、[www.eiu.com](http://www.eiu.com) をご覧いただくか、[www.twitter.com/theeiu](https://www.twitter.com/theeiu) で当社をフォローしてください。

#### Arbor Networks について

Arbor Networks は DDoS 攻撃や高度化する脅威から世界の大手企業および大手サービス・プロバイダーのネットワークを安全に守ることを支援しています。Arbor Networks は全世界のエンタープライズ、キャリア、モバイルの市場において DDoS 保護ソリューションを提供する世界をリードする主要ソリューションプロバイダーです (Infonetics Research 社調べ)。高度化する脅威に対する Arbor Networks のソリューションは、パケットキャプチャと NetFlow 技術を組み合わせることで、ネットワーク全体を可視性し、マルウェアや悪意のあるインサイダーの脅威を迅速に検出し、削除することを可能にします。Arbor Networks はまた、動的なインシデント対応、履歴分析、視認性、フォレンジクスについても市場をリードする分析機能を提供しています。Arbor Networks は、企業のネットワークやセキュリティの担当者がセキュリティのエキスパートになり、企業のセキュリティ強化を実現することを目指しています。Arbor Networks の目標は、お客様がセキュリティ問題を迅速に解決し、事業リスクを低減できるよう、ネットワーク上の脅威の視認性とセキュリティ・インテリジェンスの提供を可能することです。



Arbor Networks の製品およびサービスについて詳しく知りたい方は、Arbor Networks の日本語サイト [www.arbornetworks.com/jp/](http://www.arbornetworks.com/jp/) を参照してください。また、業界唯一の革新的なインターネット監視システム ATLAS<sup>®</sup>のデータに基づく調査、分析および知見については、[ATLAS セキュリティポータル](#) (英文) をご覧ください。

*著作権情報: Arbor Networks, Peakflow, ArbOS, ATLAS, Pravail, Arbor Optima, Arbor Cloud, Cloud Signaling, Arbor Networks のロゴおよび Arbor Networks: Smart. Available. Secure. は Arbor Networks, Inc. の商標です。その他のブランド名はすべて各所有者の商標です。*