Press Release
2022 年 8 月 29 日（月）
Gigamon Inc.

ランサムウェアに関する Gigamon の世界的調査により、全体の 1/3 の企業・組織が、悪意を持つ内部関係者をランサムウェアの侵入経路と考えていることが明らかに

ランサムウェアによるリスクが高まる中で、内部脅威が一般的な脅威ベクトルのひとつと考えていても、現状では悪意を持つリスクか偶発的なものかを判断する可視性が欠如

2022 年 8 月 29 日（月）– Deep Observability（高度な可観測性）のリーディング・カンパニーである Gigamon Inc.（本社：米国カリフォルニア州サンタクララ、日本代表：大久保 淳仁）は、昨今のサイバー脅威の状況がどのように進化し、サイバーセキュリティにおける“非難する文化”が深刻化している状況かについて、価値のある洞察を提供するレポート “State of Ransomware 2022 and Beyond”を発表しました。米国、EMEA（欧州・中東・アフリカ地域）、APAC（アジア・太平洋地域）の IT およびセキュリティリーダーを対象としたグローバルでの調査結果によると、約 1/3 の企業・組織が、悪意を持つ内部関係者によりランサムウェア攻撃を受けたことがあり、偶発的な内部関係者によるものと同様、散見される脅威として回答しています（35 パーセント）。また 59 パーセントの企業・組織がランサムウェアの脅威が過去 3 ヶ月で悪化していると考えており、その他にもフィッシング（58 パーセント）、マルウェア/コンピュータウイルス（56 パーセント）、クラウドアプリケーション（42 パーセント） が一般的な脅威ベクトルとしてあげられています。

昨年、3 分の 2 以上（69 パーセント）の組織がランサムウェアの被害を受け、大半の IT およびセキュリティプロフェッショナルは、この種のサイバー犯罪が自身の職業キャリアにどのような影響を及ぼすかについて懸念を持っています。ランサムウェアの脅威に対抗するため、本調査では、回答者の大半が EDR（エンドポイント検知レスポンス）を不可欠なものと考えている一方で、ネットワーク上にある管理外のデバイスが持つリスクに注意を払っている回答者は僅か 3 パーセントであることを確認しています。この為、IT プロフェッショナルは、今後 12 カ月以内に自社がランサムウェアによる攻撃を受けるであろうことを予測しており、EMEA の回答者の 75 パーセントが、攻撃を受ける可能性が高いまたは非常に高いと予測しており、強く懸念しています。

ランサムウェアの危機が深刻化するなか、Lapsus$グループのようなハッカー集団は、企業・組織に対して不満を持つ従業員を利用して、企業・組織のネットワークへアクセスする手段を行うことで有名になりました。 95 パーセント（CISO/CIO の 99 パーセント）が悪意を持つ内部関係者を重大な脅威リスクとみなしています。幸いなことに、この回答者の 66 パーセントは、現在、両タイプにおける内部関係者の脅威に対処するための戦略を持っています。しかし、大半の企業・組織が、どのタイプの内部関係者による脅威がビジネスを脅かしているのかを区別するために必要な可視性が欠如していることは明らかで、 そのリスクを軽減することは非常に困難です。

ハイブリッドクラウド環境のセキュリティとパフォーマンスの問題をアプリケーションレベルで監視するための可観測性ツールに依拠する企業・組織がふえています。しかし、これらのツールは、ネットワークインフラレベルでの可視性が欠如しているため、企業・組織が危険にさらされる可能性があります。この盲点をなくすため、企業・組織は、高度なネットワークレベルのセキュリティ・フォレンジックとラテラルムーブメント（横方向の脅威拡散）検出の実現、またハイブリッドおよびマルチクラウド環境全体で多層防御を実現する手段として、Deep Observability（高度な可観測性）を備えたソリューションを採用する傾向が強まっています。

Gigamon 社のグローバルフィールド CTO 兼セキュリティアーキテクチャチームディレクターのイアン・ファーカーは、次のように述べています。
「Deep Observability（高度な可観測性）は"多層防御"態勢の実現に不可欠であるとグローバルのセキュリティチームが認めています。クラウド上の設定ミスや悪意を持つ内部関係者による脅威の増加、有事への対処が足りなかった際に責任を追及する文化など、多くの課題と向き合う情報セキュリティのプロフェッショナルを支援するのに、包括的な可視性が不可欠です。」

非難する文化

本調査では、グローバルの回答者の 88 パーセントがサイバーセキュリティ業界では「非難する文化」が存在していると考えており、米国では 38 パーセント、シンガポールでは 37 パーセントの回答者が、侵入被害が発生したときにその責任を追及される傾向が拡大していると見ていることも明らかになりました。懸念点としては、非難する文化を認識している回答者の 94 パーセントは、それがインシデントの報告遅延につながる可能性もあると Gigamon に語っています。この課題を解決するために回答者は、報告内容の透明性の向上（42 パーセント）、業界全体の協業（29 パーセント）、CIO/CISO に「Deep Observability（高度な可観測性）」を提供する必要性（22 パーセント）を指摘しています。

新たなフロンティア: Deep Observability（高度な可観測性）

Deep Observability（高度な可観測性）は、メトリック、イベント、ログ、トレース情報に基づいた既設可観測性ツールの能力を拡張するため、実用的なネットワークレベルのインテリジェンスを活用する事と定義できます。
CIO/CISO が"非難する文化"に対処するために必要とされるソリューションであり、悪意を持つ内部関係者からの脅威に対するリスクを軽減するために重要な対策として、ゼロトラスト対策（66 パーセント）と同様に、Deep Observability（高度な可観測性）（66 パーセント）が挙げられています。

しかし、Zero Trust 2020 Gigamon レポートが発表されて以来、ゼロトラスト対策の複雑さに対する認識が高まり、多くの回答者がその導入に自信を喪失しているのが現状です。EMEA の 44 パーセントは、ゼロトラストには多大な監視リソースが必要だと考えています（21 パーセント増）。その一方で、ランサムウェア対策だけでなく、ハイブリッドおよびマルチクラウドインフラの保護（グローバル回答者 89 パーセントが同意）、安全なクラウド移行（グローバル回

答者 82 パーセントが同意）のために、Deep Observability（高度な可観測性）がサイバーセキュリティ対策のコアであると認識されるようになってきています。

その他主要な調査結果

- **ランサムウェアは、取締役会レベルの優先事項として捉えられている。** グローバルの取締役会の 89 パーセントが同脅威を優先事項として捉えており、英国（93 パーセント）、オーストラリア（94 パーセント）、シンガポール（94 パーセント）でも、割合が増加しています。同脅威をどのようにみているかという質問に対しては、全地域において「風評問題につながる」（33 パーセント）という認識が最上位でした。
- **サイバー保険が不安を煽っている。** 調査対象者の 57 パーセントが、サイバー保険市場がランサムウェアの危機を悪化させていることに同意しています。サイバー保険が最も多く採用されている APAC では、オーストラリアの回答者の 66 パーセント、シンガポールの回答者の 68 パーセントがこの懸念を感じています。
- **米国がゼロトラスト対策を先導している。** EMEA の回答者からはゼロトラスト対策の導入に対して自信を喪失している傾向がある一方で、米国では 59 パーセントがゼロトラスト対策のフレームワークは実現可能だと考えています。また米国の回答者は、ゼロトラストと Deep Observability（高度な可観測性）の補完的な結びつきについて最も確信を持っており、47 パーセントがこの 2 つは強く関連していると主張しています。

調査結果の詳細については、以下をご覧下さい。（英文資料）
https://www.gigamon.com/resources/resource-library/white-paper/wp-gigamon-report-state-of-ransomware.html
企業・組織のセキュリティ姿勢をどのように向上させるかについては、以下をご覧下さい。（英文資料）
https://www.gigamon.com/resources/deep-observability.html

【Gigamon について】

Gigamon Inc. は、実用的なネットワークレベルのインテリジェンスを活用し、Observability（可観測性）ツールの機能を強化した Deep Observability（高度な可観測性）を提供しています。この高度な連携により、IT 組織はセキュリティとコンプライアンスのガバナンスを保証し、パフォーマンスのボトルネックの根本原因の分析を迅速化し、ハイブリッドおよびマルチクラウド IT インフラの管理に関連する運用負荷を大幅に削減することができます。全世界で販売パートナーおよびサービスプロバイダを通じて、4,200 社以上の企業へ、物理、仮想、クラウドネットワーク向けに可視化基盤ソリューションを提供しています。米国連邦政府機関のトップ 10 すべて、グローバル銀行トップ 10 の 7 行、Fortune100 企業の 83 社、モバイルネットワーク通信事業者トップ 10 の 9 社、テクノロジー企業トップ 10 の 8 社、医療関連プロバイダートップ 10 の 8 社に導入されています。Gigamon のミッションは、中堅・中小企業や分散拠点を持つ大企業や組織で、効率的運用かつ高 ROI のセキュリティ、監視システム環境を実現することです。本社を米国カリフォルニア州サンタクララに置き、世界 20 か国にオフィスを展開しています。
さらなる詳細情報、プロモーション活動、最新動向は https://www.gigamon.com/jp/をご覧下さい。

【本プレスリリースに関するお問合せ】
Gigamon Inc.
〒105-0022
東京都港区海岸 1-2-20 汐留ビルディング 3F
Sales 担当
Tel:03-6721-8349
Email： sales-japan@gigamon.com
URL： https://www.gigamon.com/jp/