Press Release

2025 年 8 月 5 日（火）

Infoblox 株式会社

Infoblox が「Threat Defense」を大幅強化
AI 時代の巧妙な攻撃に先回りする先制型セキュリティ対策を実現

- ユーザー、デバイス、IoT/OT、クラウドワークロードを守り、脅威を未然に防ぐ強力な先制的セキュリティ対策を推進
- 新たに強化されたプロテクティブ DNS により、AI を活用した高度な脅威を事前に察知し、攻撃を未然に防ぐことを実現
- 柔軟なトークンベースのライセンスを導入し、効率的な保護の拡張と進化するセキュリティニーズに応じた価格設定を実現
- プロテクティブ DNS 分野でのリーダーシップをさらに高め、今後も最新の NIST ガイドラインに対応、進化するサイバー攻撃に対抗する組織の支援を推進
- Google Cloud の DNS Armor を支え、クラウドワークロードにネイティブなセキュリティを提供。今年後半にパブリックプレビュー開始

2025 年 8 月 5 日(火) ― クラウドネットワークとセキュリティサービスのリーダーである Infoblox は本日、プロテクティブ DNS ソリューション「Infoblox Threat Defense™」の大幅な強化を発表しました。これにより、高度な AI 駆動のサイバー脅威に対してより先制的なセキュリティ対策で先手を打つことが可能になります。

世界のサイバー犯罪コストが 2027 年までに 23 兆ドルに達すると予測される中[※1]、従来の「Detection and Response（検知して対応するアプローチ）」型のセキュリティツールは追いつけなくなっています。現代の攻撃者は AI を駆使し、再利用されない一度きりのマルウェアや巧妙なフィッシングキャンペーンを作成し、従来の防御を回避するため、どの組織も「患者ゼロ（patient zero）」になるリスクがかつてないほど高まっています。

Infoblox のプロテクティブ DNS ソリューション「Infoblox Threat Defense」は、予測的な脅威インテリジェンスとアルゴリズムおよび機械学習に基づく検知を組み合わせることで、インフラに影響が及ぶ前に脅威を阻止します。従来ツールより平均 68 日も早く高リスクかつ悪意のあるドメインをブロックし、業界最高水準の誤検知率 0.0002%を誇ります。

「ほとんどの DNS セキュリティツールと当社のアプローチの違いは、法執行機関が路上の麻薬密売人を追いかけるのと、カルテルを壊滅させる違いのようなものです」と Infoblox 最高製品責任者の Mukesh Gupta（ムケシュ・グプ

タ）は述べています。「我々はサイバー攻撃者の背後にいる供給者、つまりカルテルを標的にしているため、脅威がネットワークに到達する前にブロックできます。この先制的戦略により、セキュリティチームはリスクを減らし、ノイズを排除し、脅威を DNS レイヤーで止めることが可能になります。」

新たな AI 駆動脅威の波に先んじるため、Infoblox は画期的な脅威インテリジェンスを継続的に提供し、Threat Defense の役割を積極的かつ高速な脅威ブロッカーとして確固たるものにしています。より良い可視化と実用的な洞察、柔軟なライセンス、先制的保護の明確な指標など、これらの新機能は攻撃者が隙を突く前にセキュリティチームがギャップを埋めるのを支援するために設計されています。

- **先制的保護（ROI の可視化）**：被害をもたらす前に、無効化された脅威に関する明確で定量的な指標をセキュリティリーダーに提供し、報告を効率化しセキュリティ投資対効果（ROI）を示します。
- **セキュリティワークスペース**：直感的で集中管理されたインターフェースにより、セキュリティチームは環境を深く可視化し、リスク軽減のための実用的な洞察を得て、平均対応時間（MTTR）を短縮します。
- **検知モード（Detection Mode）**：既存の DNS 設定を変更せずに、現在見逃している脅威を可視化し、運用リスクを最小限に抑えます。
- **資産データ統合**：先制戦略の一環として保護された対象に関する深いコンテキストを提供し、セキュリティチームがさらなる調査と分析を行えるようにします。
- **トークンベースライセンス**：保護対象資産に連動した柔軟なトークンベースの価格設定により、調達を簡素化し ROI を明確化します。
- **Google Cloud の DNS Armor を支援**：Infoblox のプロテクティブ DNS 機能は Google Cloud の DNS Armor にも採用されており、クラウドワークロードにネイティブなセキュリティを提供します。今年後半にパブリックプレビューを開始します。

Infoblox Threat Defense は、マルウェアが展開される前、そして最初の感染者が出るずっと前に、脅威アクターのインフラが構築されている段階で攻撃を阻止するための予測的な洞察をセキュリティチームに提供します。最初の被害者の検出と対応を待たなければならない従来のセキュリティツールとは異なり、Infoblox のアプローチは攻撃を完全に未然に防ぐことが可能です。

攻撃を早期に阻止することで、Infoblox は XDR や SIEM などの検知・対応ツールの負荷を軽減し、2028 年までに従来のソリューションの 40%が先制的サイバーセキュリティに置き換わるとするガートナーの見解と一致します。最新の NIST SP 800-81 ガイドラインもこの変化を支持し、DNS が他のシステムよりも早期にセキュリティインシデントを防ぐことが多いと指摘しています。

「従来の『検知と対応』型セキュリティは、今日の AI 駆動の攻撃者やマルウェアに追いつけません。サイバー犯罪はかつてない速さで進化し、世界に数兆ドルの損失をもたらし、旧来の防御の隙を突いています」と Infoblox の社長兼 CEO、Scott Harrell（スコット・ハレル）は述べ、ています。「旧来のキルチェーンアプローチは、誰かが『患者ゼロ』になるのを待って学習・対応する仕組みですが、今日の攻撃者は個別の企業や業界を狙ったマルウェアをカスタマイズするため、旧来の受動的な手法は AI 対応の現代攻撃者には無力です。患者ゼロになれば、失うのはビジネスそのものです。サイバーセキュリティの未来は先制的でなければなりません。脅威が組織に到達する前に阻止するのです。」

「Infoblox 導入前は、DNS がセキュリティ体制の盲点でした」とサンフランシスコ市・郡の最高情報セキュリティ責任者、Nathan Sinclair（ネイサン・シンクレア）は語ります。「DNS リクエストとそこに潜む脅威を完全に可視化できる価値をすぐに実感しました。Infoblox Threat Defense は脆弱性の悪用や侵入を阻止する強力なソリューションであり、防御力を大幅に強化し、我々が提供する重要なサービスの保護に自信をもたらしました。」

先制的 DNS セキュリティの重要性について詳しくは、当社の Security Momentum ローンチブログ（英語）をご覧ください。進化する脅威に関する最新調査や、DNS セキュリティが 82%の攻撃を影響前にブロックする仕組みについては、2025 年 DNS 脅威ランドスケープレポート（英語）をお読みください。

※1 「2025 年の主要サイバーセキュリティ統計」、SentinelOne、2025 年 5 月 15 日。 https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/

Infoblox について

Infoblox は、ネットワーク、セキュリティ、クラウドを統合し、回復力と俊敏性を兼ね備えた運用プラットフォームを構築します。フォーチュン 100 社の 92 社を含む 13,000 社以上のお客様に信頼されており、重要なネットワークサービスをシームレスに統合、保護、自動化することで、企業は妥協することなく迅速に行動できます。
infoblox.com にアクセスするか、LinkedIn でフォローしてください。

【本プレスリリースに関するお問合せ】
Infoblox 株式会社
〒107-0062 東京都港区南青山 2-26-37 VORT 外苑前Ⅰ 3 階
Email：SalesJapan@infoblox.com
https://www.infoblox.com/jp