Press Release

2023 年 6 月 8 日（木）

Infoblox 株式会社

Infoblox、ネットワークチームとセキュリティチームを統合したサイバー攻撃保護の強化で業界をリード

- Infoblox は、複雑なハイブリッド環境やマルチクラウド環境を含むあらゆる環境において、ネットワークおよびセキュリティをシンプルに統合します
- フィッシング攻撃が世界中で話題となる中、Infoblox は、Infoblox BloxOne® Threat Defense に重要なセキュリティ機能強化を提供することで、類似ドメイン監視や新たな脅威に対する保護を可能にし、サイバー犯罪の防止を支援します
- Infoblox は、「2023 Global State of Cybersecurity Study（2023 年サイバーセキュリティグローバル状況調査）」を発表し、悪意のある脅威が世界中で増加する中、業界が直面し続けるセキュリティおよびネットワークのトレンドを明らかにしました
- Infoblox は、世界的な大企業のネットワークを保護する重要な役割を担っており、ネットワークとセキュリティの両専門家への訴求を図るため、信頼性とビジネスの焦点を反映したブランドの再構築に取り組んでいます

2023 年 6 月 8 日、東京 –パフォーマンスおよび防御の改善を実現するシンプルなクラウド対応ネットワークおよびセキュリティプラットフォームを提供する Infoblox Inc.は、本日、サイバー犯罪との戦いにおいてネットワークチームとセキュリティチームの協力が必要である理由について、強い主張を持ちいくつかの発表を行いました。重要なセキュリティ機能の新規追加、およびブランドアイデンティティの刷新は、Infoblox の戦略、信頼性、ビジネスの焦点を反映したもので、顧客の重大な脅威を検出し対応することが可能になることで、ビジネスの成功をサポートします。

Infoblox の CEO 兼社長であるスコット・ハレルは次のように述べています。「Infoblox は、複数のネットワークやマルチクラウド環境において、接続するユーザーやデバイスをリアルタイムに可視化・制御することが可能な唯一の企業であり、顧客は、より安全で回復力の高い環境を構築できます。また、ネットワーク運用チームとセキュリティ運用チームを統合し、可視化やデータコンテキスト、自動化、制御を共有することで、マルウェアによる通信を防止したり、脅威の発生源を特定することが可能になり、パフォーマンスと保護を新たなレベルに引き上げます」。

日本の組織はサイバーセキュリティ機能を強化しているが、懸念は残っている

今日の企業では、競争力を維持するためにハイブリッド環境やマルチクラウド環境の採用が増加しており、複雑さが増し、攻撃対象領域が拡大しています。日本を拠点とする企業のデータ漏えいの発生率は、調査対象のどの国より低く、驚くべきことにわずか 26%です。一方で、「2023 Global State of Cybersecurity Japan（2023 年サイバーセキュリティグローバル状況（日本））」レポートによると、これらのセキュリティ侵害による累積コストは平均で 4 億 6,000 万円で、世界の平均より 60%高くなっています。

多くのシステムやユーザーは、今日の困難な環境とそれに伴うデジタル習慣の変化にさらされています。日本の組織の半分以上（57%）は、データ漏えいを最も懸念しており、その後に、リモートワーカー接続を利用したランサムウェアおよび攻撃と続きます。攻撃から保護する上で予想される上位の課題は、IT セキュリティスキル不足

（38%）、および予算不足（32%）に関するものです。ただし、本レポートによると、既知および最新の脅威に対抗するために、2023 年にセキュリティ予算の増加を見込んでいる日本の組織は、わずか 42%でした。

類似ドメイン監視（Lookalike Domain Monitoring）などを新たに追加して、BloxOne® Threat Defense を強化

Infoblox の新しい類似ドメイン監視（**Lookalike Domain Monitoring**※）機能を利用すると、フィッシングやマルバタイジング（不正広告）などの攻撃によってパートナーや顧客を騙す目的で利用が増加している、会社ブランドのなりすましサイトを特定できます。これは、Infoblox の新機能である、不正な意図の兆候を取得して攻撃発生前に攻撃を防止できる脅威インテリジェンスフィードの導入によるものです。これらの機能強化を通して、カスタマーエクスペリエンスが向上し、安全性が高まります。
※https://blogs.infoblox.com/security/getting-in-front-of-threats/

Infoblox は、1 日に 700 億件以上の DNS クエリを分析しています※。Infoblox の最新の類似ドメインレポートによると、不正行為者による類似ドメインの悪用は引続き継続していますが、2022 年に手口が大幅に進化し、あらゆるセクターを標的に、多要素認証（MFA）対策を迂回する目的で使用されるなど、複雑なサイバー攻撃において重要な役割を果たしていることが明らかになりました。
※https://www.infoblox.com/products/bloxone-threat-defense/

ハレルは次のように話しています。「Infoblox は、ベストオブブリードの DNS レイヤーセキュリティソリューションプロバイダとして、独自の脅威インテリジェンスのソースおよび強化ポイントとして、DNS 利用の発展を開拓し続けます」。「当社は、攻撃者が悪用する類似ドメインの使用を防ぐことができる最初かつ唯一の DNS セキュリティベンダーです。これらの攻撃は巧妙化し蔓延しており、専門的なソリューションは、企業やそのユーザーの安全を守る上で、あると便利であるだけでなく必須となっています」。

決して休むことのない世界において、Infoblox は、デジタルトランスフォーメーションのスピードに対応するために応答性の高いネットワークを構築したり、隠れた脅威を検出して攻撃を早期に防止できるよう、顧客のサポートに取り組んでおり、豊富なコンテキストのネットワークインテリジェンスで、セキュリティサービスを提供します。

Infoblox の日本法人、Infoblox 株式会社 代表執行役社長である司馬聡は次のように述べています。「デジタル革命の勢いが引き続き増す中、機密データが悪意のある人物の手に渡るのを防止するには、応答性と信頼性の高いネットワークが非常に重要です。ネットワークとセキュリティを統合することで、企業各社は、24 時間 365 日ネットワークの可視性を高め、重要な脅威を事前に検知したり、絶えず変化するサイバー環境に適切に対応することができるようになります」。

Infoblox は、クラウドファーストのコンサルティングアプローチを採用しており、顧客の固有のビジネスニーズに基づいて、耐障害性の高いネットワークを構築し、重要な脅威を迅速に阻止できるよう、具体的なソリューションとアクションを提供します。詳細は、infoblox.com をご覧ください。

Infoblox について
Infoblox は、ネットワーキングとセキュリティを一体化して、比類のないパフォーマンスと保護機能を提供します。当社は、フォーチュン 100 企業や新興のイノベータから信頼されており、ネットワークに接続するユーザーやデバイスをリ

アルタイムに可視化し制御することが可能で、組織のオペレーションが迅速化し、脅威を早期に防止することができます。詳細は、infoblox.com にアクセスするか、LinkedIn または Twitter を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
Tel：03-5772-7211
Email：SalesJapan@infoblox.com
https://www.infoblox.com