

昨日のネットワークで、 明日のビジネスは支え られない

エンタープライズグレードの DDI は
近代化、自動化、セキュリティの鍵

目次

はじめに	3
重要なネットワークサービスはデジタルライフライン	5
レガシーネットワークサービスでは、今日のニーズに対応できない	6
現状維持はビジネスの苦境を招く	7
エンタープライズグレードの DDI が IT モダナイゼーションへの第一歩となる理由	8
エンタープライズグレードの DDI は、現代 IT の基盤	9
INFOBLOX UNIVERSAL DDI™ PRODUCT SUITE は、比類のないエンタープライズグレード の重要なネットワークサービスを提供	11
INFOBLOX UNIVERSAL DDI が可能にする、近代化の基礎	14
INFOBLOX UNIVERSAL DDI—前進するための構築	15

異なる重要なネットワークサービスの 隠れたコスト

今日のハイパーコネクテッドな企業において、DNS、DHCP、IP アドレス管理（DDI）は単なるバックグラウンドサービスではなく、安全でスケーラブルなデジタルオペレーションの基盤となっています。それにもかかわらず、多くの組織は、老朽化し、断片化したインフラに「十分だ」と推測して頼り続けています。

見過ごされがちなのは、時代遅れのソリューションを続けることがどれほどのコストを生むかです。これは、単に金銭的なものだけでなく、ダウンタイム、リスクの増大、生産性の低下にもつながります。最近の調査*によると、非エンタープライズグレードの DDI を使用している組織は、業務中断に対して非常に脆弱であり、停止後の回復に時間がかかり、監査の失敗率が高く、コストも高くなります。



**ID、クラウド、
エッジサービス全体で需要が高まるにつれ、エンタープライズグレードの DDI は単なるアップグレードではなく、近代化の必須要件です。**

* エンタープライズグレードの DDI を使用しないことによる 9 つの落とし穴、Enterprise Strategy Group、2025年2月

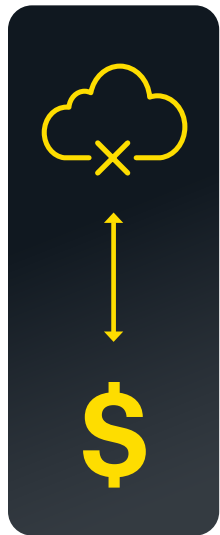
**エンタープライズ
DNSがダウンする
と、現代の世界は
停止します：取引
も、フライトも、
電力もすべてが止
まります。すべて
が凍結します。**

従来のサイロ化された DNS、DHCP、IPAM の主要な課題

- ❗ 予期しないダウンタイム
- ❗ 可視性と制御の不足
- ❗ 生産性の損失
- ❗ コストの増加
- ❗ スケーリングの課題
- ❗ 単一障害点
- ❗ より深刻なセキュリティ脆弱性

重要なネットワークサービスは デジタルライフライン

あなたの組織はアプリケーションとクラウドレイヤーでは近代化しているかもしれませんが、エンタープライズグレードの DNS や DHCP がなければ、基盤全体が危険にさらされることになります。エンタープライズリソースプランニング（ERP）システムから ID プラットフォームまで、ほぼすべての最新アプリケーションは、デジタルエントリーポイントとして DNS に依存しています。1 つの DHCP スコープが誤って構成されると、部門全体がネットワークにアクセスできなくなる場合があります。



障害の真のコスト

DNS と DHCP の障害はもはや単なる IT の問題ではなく、ビジネスリスクです。大規模組織では、ネットワーク障害の平均コストは 1 分あたり 9,000 ドル* に近づいてきており、顧客対応システムや ミッション・クリティカルなプロセスに障害が及ぶと、その額はさらに膨れ上がります。

具体例

古い Microsoft DNS インフラストラクチャに依存しているグローバル小売業者で、同期の問題により、100 店舗以上の POS（販売時点管理）システムが 3 時間にわたって停止しました。

➤➤➤ 推定収益損失は750万ドル。顧客の信頼回復はさらに困難です。

**DNS と DHCP
の障害はネット
ワーク障害を引き
起こし、注目を集
め、役員会議の議
題にまで上がる可
能性があります。**

* The True Cost of Downtime, Forbes, David Flower, Forbes Technology Council, April 10, 2024

基盤にエンタープライズグレードのDDIがないデジタルトランスフォーメーションは流砂の上を超えるようなもの

レガシーネットワークサービスでは、今日のニーズに対応できない

デジタル変革が加速する中、企業にはレガシー DNS および DHCP ツールに依存するリスクを冒す余裕はありません。10 年前には機能したとしても、今日のニーズには対応しきれません。

運用リスク

レガシーシステムは、多くの場合、DNS、DHCP、そして Microsoft Active Directory が同じ Windows Server 上に導入されているため、脆弱な相互依存関係にあります。そして、先に述べたように、単一障害点が連鎖的な停止を引き起こす可能性があります。

コストの非効率性

レガシーインフラストラクチャをサポートするには、多くの場合、メンテナンス、パッチ適用、トラブルシューティングに専任の人員が必要です。これに高価なハードウェアの更新サイクルが加わると、DDIのコスト曲線は持続不可能になります。

断片化された可視性

ほとんどのレガシー DDI デプロイメントには、ハイブリッドおよびマルチクラウド環境における IP アドレスの使用状況や資産のステータスに対して、リアルタイムで信頼できる統合ビューがありません。こうした低い可視性により、侵害された エンドポイント の特定と隔離が遅れ、スプレッドシートでの IP アドレスの手動追跡と調整が必要になり、コンプライアンスと監査証跡の適用が困難になり、IP アドレスの競合と重複が発生します。

イノベーションのボトルネック

従来のDDIシステムは自動化を遅らせ、統合を制限し、DevOpsチームが手動のチケットや古いスクリプトに頼らざるを得なくなります。

レガシーツールでは総合的な対応はできない

DNS 同期の遅延、ごみ箱の欠如、制限付きロールベースアクセス制御（RBAC）などの特徴により、レガシーシステムに、大規模に依存することはできません。さらに悪いことに、多くの場合、サーバーごとに 1 つの管理コンソールが必要であるため、運用のサイロ化が発生し、構成ドリフトの可能性が高まります。

現状維持はビジネスの苦境を招く

サイロ化された重要なネットワークサービスは、ネットワーク、クラウド、セキュリティの管理者に多くの課題をもたらし、悪意のある者にはより多くの機会を提供します。どのようなビジネスに携わっていても、時代遅れのネットワークサービスでデジタルの未来を築こうとしているのであれば、問題が起こるのは当然です。

ランサムウェアが患者ケアを麻痺させた方法

- ・ ランサムウェア集団が主要な病院システムを標的に
- ・ DNS/DHCP とディレクトリサービスが同じサーバーを共有していたため、トラブルシューティングが最も緊急に必要なときにアクセスが遮断された
- ・ 一名の従業員によるダウンロードが重要なサーバーの侵害につながった
- ・ 医療業務が崩壊：記録、電話、患者ポータルが停止
- ・ 560 万件の患者記録が数週間にわたり混乱の影響を受けた

**総コスト：
13 億ドル**

サーバーへのパッチ適用に伴う隠れたコスト

- ・ エネルギープロバイダーは、管理する 400 台のサーバーに、年間 4,800 件のパッチを適用
- ・ 停止率が 1% の場合、年間 48 件のクラッシュが発生
- ・ 毎回約 50 人の従業員が 4 時間稼働不可になる推定
- ・ 従業員一人当たりの平均時給コストは 100 ドル

ダウンタイムが年間に及ぼす影響：960,000 ドル

2024 年 7 月に世界中で発生したクラッシュ

- ・ 史上最大の IT 障害
- ・ 数百万台のサーバーがダウン
- ・ 世界中で重要な DNS/DHCP サービスが停止
- ・ 10,000 便のフライトが運行停止
- ・ 数え切れないほどの病院が混乱

数千の企業に侵害

最近Forrester社が行った調査によると、エンタープライズグレードのDDIは時間とお金を大幅に節約します。

710万ドル節約

レガシーインフラから最新のDDI*に移行することで

2日から1時間に短縮

1000のサイトに渡る仮想マシン（VM）の導入時間

14,000時間節約

ネットワーク全体で、最新のDDIを使用することで

* The Total Economic Impact™ Of Infoblox DDI, Forrester Consulting, October, 2023

** ある一企業の結果

エンタープライズグレードのDDIがITモダナイゼーションへの第一歩となる理由

ハイブリッドクラウド、ゼロトラスト、エッジコンピューティングへの道のりは、新しいアプリケーションやピカピカのUIから始まるわけではありません。それは、信頼性が高く、拡張性があり、安全な重要なネットワークサービスから始まります。

統合されたDNS、DHCP、IPAM = DDI

ネットワークを変革するには、まずその導入方法と管理方法を変革する必要があります。エンタープライズグレードのDDIは、DNS、DHCP、IPアドレス管理（IPAM）の導入と管理を単一の管理ワークフローに統合します。この組み合わせにより、従来のネットワークサービスの複雑さが簡素化され、事業運営が効率化されます。また、ハイブリッドクラウドとクロスクラウドの可視性が向上するため、プロセスの自動化が容易になり、ネットワークサービスをオンプレミスまたはクラウドで実行できるようになります。今日の企業が求める弾力性、可視性、自動化を提供するために特別に設計されています。

実際、エンタープライズグレードのDDIを使用している組織は、手動の手順が減り、構成エラーが少なくなり、DDIタスクの生産性が60%以上向上したと報告しています。ある企業は、老朽化したMicrosoft以外のDDIツールを100%廃止し、必要なMicrosoftインフラストラクチャを50%以上削減することができました。

エンタープライズグレードの DDI は、現代 IT の基盤



一元化された統合管理

エンタープライズグレードの DDI ソリューションは、オンプレミス、ハイブリッド、マルチクラウドなどの多様な環境における DNS、DHCP、IPAM 機能の自動化とオーケストレーションを一元化します。これらのコアネットワークサービスを単一の管理パネルに統合することで、IT チームは次の利点を得られます。

- 簡素化された操作
- ポリシー適用の強化
- 運用効率



ルールベースの管理

エンタープライズ DDI プラットフォームは、NetOps、SecOps、CloudOps チーム間の協力を支援し、責任を維持するために、より厳格なアクセス制御を組み込んでいます。この協働的な管理により、次のことが可能になります。

- 許可に基づくアクセス
- 監査性と変更追跡
- 委譲管理



可視性の向上

エンタープライズ DDI プラットフォームは、ネットワーク上のすべての IP 対応デバイスとサービスにリアルタイムの可視性を提供します。これは、運用管理とセキュリティの両方にとって重要です。主な機能には以下が含まれます。

- 動的資産の検出
- リースの追跡と IP の使用状況
- 統合型分析



より強固なセキュリティ体制

エンタープライズグレードの DDI ソリューションは、DNS をサイバーセキュリティの基盤要素として活用することで、セキュリティを強化します。この強化には、悪意のあるドメインへのトラフィックを積極的にブロックし、DNS ベースの攻撃を防ぐことが含まれます。最新の DDI は、内蔵されたセキュリティ機能により、以下を可能にします。

- 先制的セキュリティ
- DNS トラフィックおよび異常のリアルタイムでの可視化
- ハイブリッドおよびマルチクラウド環境全体で一貫したセキュリティポリシー



柔軟な導入オプション

エンタープライズグレードの DDI は、固定的な製品設計に縛られることなく、ビジネス目標と IT 戦略に沿った方法でサービスを導入できます。この柔軟性により、以下のことが可能になります。

- クラウドネイティブおよびハイブリッドのサポート
- インフラストラクチャ不要の DNS/DHCP をサービスとして提供
- 仮想および物理アプライアンスオプション
- スケーラブルなアーキテクチャ

近代化は、変化のための変化ではありません。それは、レジリエンス、可視性、そして運用の健全性に関するものです。





INFOBLOX UNIVERSAL DDI™ PRODUCT SUITE

は、比類のないエンタープライズグレードの重要なネットワークサービスを提供

Infoblox Universal DDI™ Product Suite は、ハイブリッド、マルチクラウド、オンプレミス環境全体にわたる中央管理と制御、自動化、スケーラビリティ、セキュリティを組み合わせた、業界で最も強力なエンタープライズグレードの DDI ソリューションです。DNS、DHCP、IPAM を単一の統合プラットフォームに結合させ、オンプレミスまたは AWS、Google Cloud、Azure などのクラウドネイティブ DNS システムで実行されるミッションクリティカルなネットワークサービスに、リアルタイムの可視性、インテリジェントな自動化、高可用性を提供します。また、組織は Universal DDI を管理に使用しながら、クラウドネイティブな DNS を引き続き使用できます。

Infoblox のクラウドネイティブアーキテクチャは、現代企業の IT 戦略に合わせた柔軟な導入オプションも可能にする一方、threat intelligence の統合や API 主導の拡張性などの高度な機能により、組織は業務を効率化し、セキュリティ体制を強化し、大規模なデジタル変革をサポートできるようになります。実証済みの信頼性とグローバル企業での採用により、Universal DDI は、今日の複雑で動的なネットワークを管理・保護するためのゴールドスタンダードです。



クラウドとオンプレミスを横断する統合された中央管理

Universal DDI は、その中核的機能として、DNS、DHCP、および IPAM を統一されたコントロールプレーンに統合し、オンプレミスのインフラストラクチャと 3 つの主要なクラウドプロバイダー（AWS、Azure、および Google Cloud）すべてにわたって、これらの重要なネットワークサービスの合理化された管理を可能にします。制御を一元化することで、Universal DDI は以下のことを可能にします。

- サイロを解消
- セキュリティの強化
- ネットワークサービスのプロビジョニングにおいて迅速化を実現
- オペレーションを簡素化
- 設定ミスリスクを軽減



詳細な可視性により、セキュリティとコンプライアンスが向上

設定された IP 範囲、使用状況、リース状況などをリアルタイムで可視化することで、IT チームは異常を事前対応的に検出し、ポリシーを施行し、予期せぬ高額なコストを回避できます。いくつかの企業は、次のことを達成しています。



»» 60%

セキュリティインシデント時に侵害されたデバイスをより迅速に特定する

»» 70%+

コンプライアンスレポートの作成に費やす時間を削減



お客様のアーキテクチャに適した柔軟な導入オプション

As-a-Service、物理または仮想のオンプレミス、またはハイブリッド DDI モデルが必要な場合でも、Infoblox はお客様の要件に適応します。エッジ、クラウド、またはその両方でサービスをロールアウトし、一貫性と自動化による分散サービスのポリシー管理を実現します。



実証ポイント：あるグローバル物流企業は、Infoblox の自動化されたデプロイメントテンプレートを使用して、エッジサイトのプロビジョニングを 7 日間から 2 時間に短縮しました。



ロールベースの管理によりガバナンスが簡素化

機能、地域、またはコンプライアンスの範囲に基づいてロールを簡単に割り当てることができます。オールオアナッシングのアクセスやリスクの高いマニュアルオーバーライドは不要になります。



実証ポイント：ある米国の連邦機関は、Infoblox RBAC を使用して、機密ネットワークと非機密ネットワークを厳密に分離しつつ、1,200 人以上のユーザーをサポートしました。



DNS セキュリティで脅威を早期に阻止

Infoblox Universal DDI は、Infoblox Threat Defense™ を通じて、エンタープライズグレードのセキュリティを組み込みで提供します。Protective DNS 機能を DNS、DHCP、IPAM と統合した統一プラットフォームにより、セキュリティチームは脅威を事前に阻止できます。平均して、他のソリューションよりも 63 日以上早く脅威を阻止できます。Universal DDI では、以下のことができます。

- 悪意のあるドメインやフィッシングドメインへのトラフィックを先制的にブロック
- コマンド・アンド・コントロール（C2）、データの持ち出し、ドメイン生成アルゴリズム（DGA）などの DNS ベースの脅威をリアルタイムでブロック
- 類似ドメインを特定し、ブランドの評判を保護
- エンドポイントのエッジからクラウドまで、一貫したセキュリティポリシーを適用
- DNS イベントの優先順位付けとエンドポイントの属性付けによりインシデント対応を迅速化



ミッションクリティカルなサービスを切り離すことによる、より高い回復力

エンタープライズグレードの DDI は、ネットワークサービスを ID から分離し、ハイブリッド環境全体での稼働時間、可視性、セキュリティを確保します。Infoblox は、エンタープライズ規模、ロールベースのアクセス制御、セキュリティ、自動化に特化した回復力のある DDI を提供することで、重要なネットワークサービスを近代化します。



NIST

米国国立標準技術研究所 SP 800-81

2.3.1. 専用 DNS サービス：サイバー犯罪者やその他の攻撃者は、ミッションクリティカルなシステムを攻撃することで、サイバーインシデントの混乱を増幅し、最大化しようとします。特に、複数の重要なコンポーネントをホストしているターゲットが狙われます。

サイバーレジリエンスを確保するために、複数のミッションクリティカルなサービスの1つのシステムに共存させることは制限する必要があります（職務の分離）。

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81r3.ipd.pdf>

INFOBLOX UNIVERSAL DDI が可能にする、近代化の基礎



ID の近代化



課題：

ある企業はハイブリッドID管理プラットフォーム（OktaとAzure AD）に移行していましたが、DNSとDHCPは依然としてオンプレミスのMicrosoft Active Directoryに結びついていました。

解決策：

Infoblox Universal DDI は重要なネットワークサービスをレガシーインフラストラクチャから切り離し、統合された可視性と管理を備えた、クラウドネイティブでスケーラブルなDNSとDHCPを提供しました。

結果：

- ✓ シームレスなハイブリッド ID 管理プラットフォームの移行
- ✓ 稼働時間の向上と管理性の改善
- ✓ レガシー Microsoft Active Directory への依存度の低減

Universal DDI は、混乱を起こすことなく、スムーズで安全かつスケーラブルなID変換を実現しました。

クラウドトランスフォーメーション



課題：

大手医療機関はワークロードをAWSとAzureに移行しましたが、断片化されたオンプレミス環境とクラウド環境全体でDNSを管理することに苦労していました。

解決策：

Infoblox Universal DDI は、複数のクラウドプロバイダーとプライベートインフラストラクチャ全体でDNSを管理するための集中型プラットフォームを提供しました。

結果：

- ✓ ハイブリッド環境全体で包括的な可視性を確保
- ✓ 稼働時間の向上と管理性の改善
- ✓ DevOpsの自動化を簡素化
- ✓ 安全で回復力のあるサービス提供を実現

100%
30%+

レガシーDNSセキュリティツールの廃止

SOC
生産性向上

エッジサービスの近代化



課題：

リモートワーク、IoT、エッジ処理の増加に伴い、ある物流会社はIT部門の介入を必要としない、数十のエッジノードにわたって信頼性の高いDNS/DHCPを必要としていました。

解決策：

Infoblox Universal DDI は、回復力のあるリモート管理サービスを使用して、エッジでのDNS/DHCPプロビジョニングを自動化します。

結果：

- ✓ ゼロタッチプロビジョニングを用いた即時サイトセットアップ
- ✓ リモートサイトでの停止が70%減少
- ✓ 集中管理によるセキュリティ体制の強化

Infoblox は、IT 担当者を現場に派遣することなく、エンタープライズグレードのネットワークサービスをエッジに提供しました。



DNS が故障すると、ビジネスが停止します。シンプルな仕組みです。

infoblox

INFOBLOX UNIVERSAL DDI 前進するための構築

デジタル変革を進める企業にとって、信頼性が高く、安全で、スケーラブルな重要なネットワークサービスが必要です。Universal DDI は、管理を統合し、運用を自動化し、エッジを保護するクラウドネイティブの DDI プラットフォームです。従来のサイロ化された DNS および DHCP ツールとは異なり、Infoblox は、ビジネスの俊敏性、回復力、セキュリティ、コスト削減を実現する最新のネットワークインフラストラクチャを提供します。

Infoblox Universal DDI は単なるアップグレードではなく、現代の企業にとっての基盤的な要件です。それは、レジリエントで、応答性が高く、あらゆる状況に対応できるネットワークを構築する方法です。



現状を打破する準備はよろしいですか？

詳しくは次の URL からご覧ください：

infoblox.com/jp/networkmodernization



Infoblox は、ネットワーキング、セキュリティ、クラウドを統合し、俊敏性と回復力を兼ね備えた運用基盤を形成します。当社は重要なネットワークサービスをシームレスに統合し、保護し、自動化することで、企業が妥協することなく迅速に行動できるようにします。

Infoblox株式会社
〒107-0062 東京都港区南青山
2-26-37VORT外苑前I 3F

03-5772-7211
www.infoblox.com/jp