infoblox

基礎からわかる DNS、DHCP、IPAMな4日間

INFOBLOX DDI WEEK ONLINE

DDI Week Online

Day2
DHCP/IPAM入門/
infobloxが選ばれる理由

Infoblox株式会社
シニアソリューションアーキテクト
古田　秀哉

© 2025 Infoblox. All rights reserved.

アジェンダ

1. DHCPとは
2. IP Address Management (IPAM)とは
3. Infoblox IPAMのご紹介

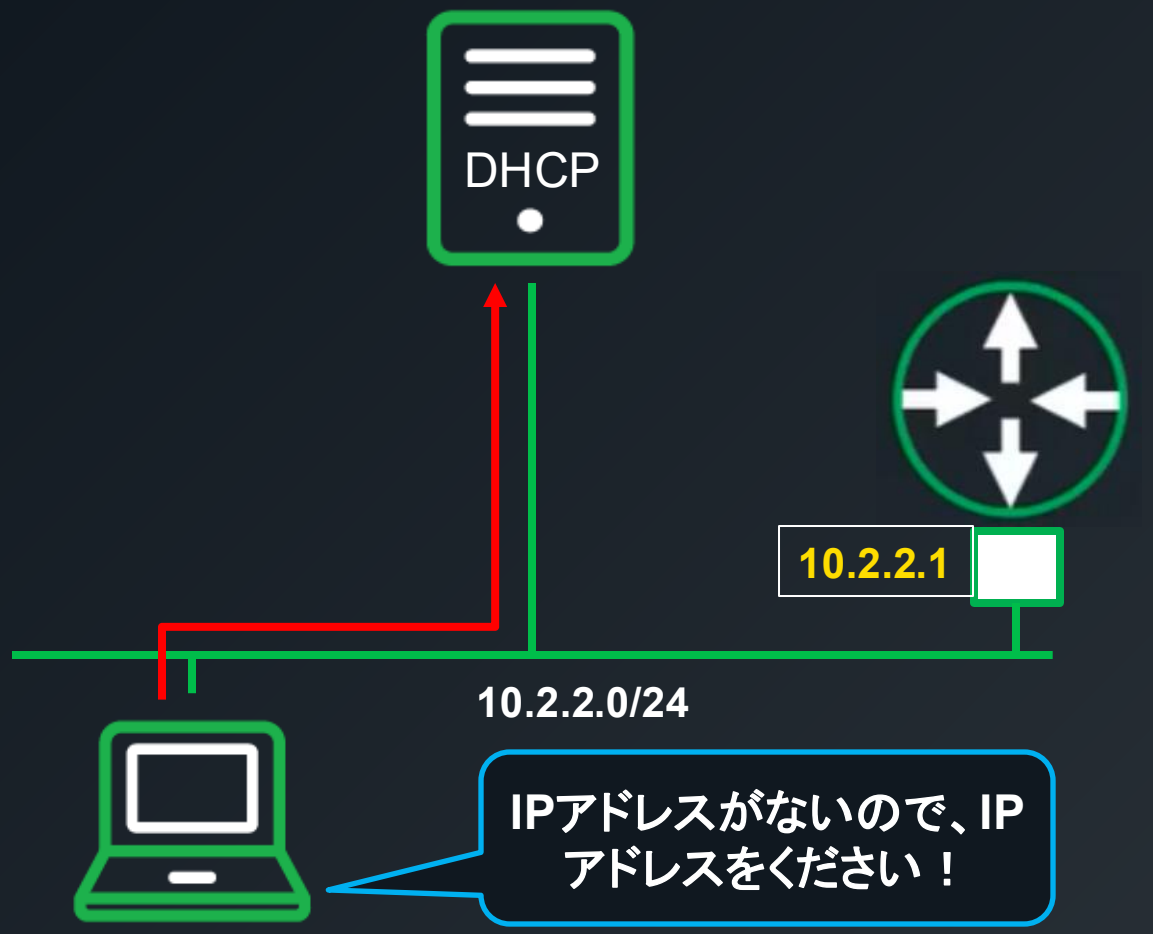
DHCPとは

DHCPとは

Dynamic Host Configuration Protocol (DHCP)

- Client – Serverモデル
  - ClientがIP アドレスを要求
  - ServerがIP アドレスを払い出す
- 動的なIPアドレスを払い出すだけでなく、Subnet, Default gateway, DNSやNTP情報など その他の構成パラメータ (DHCP Option)も割り当てる

New Lease

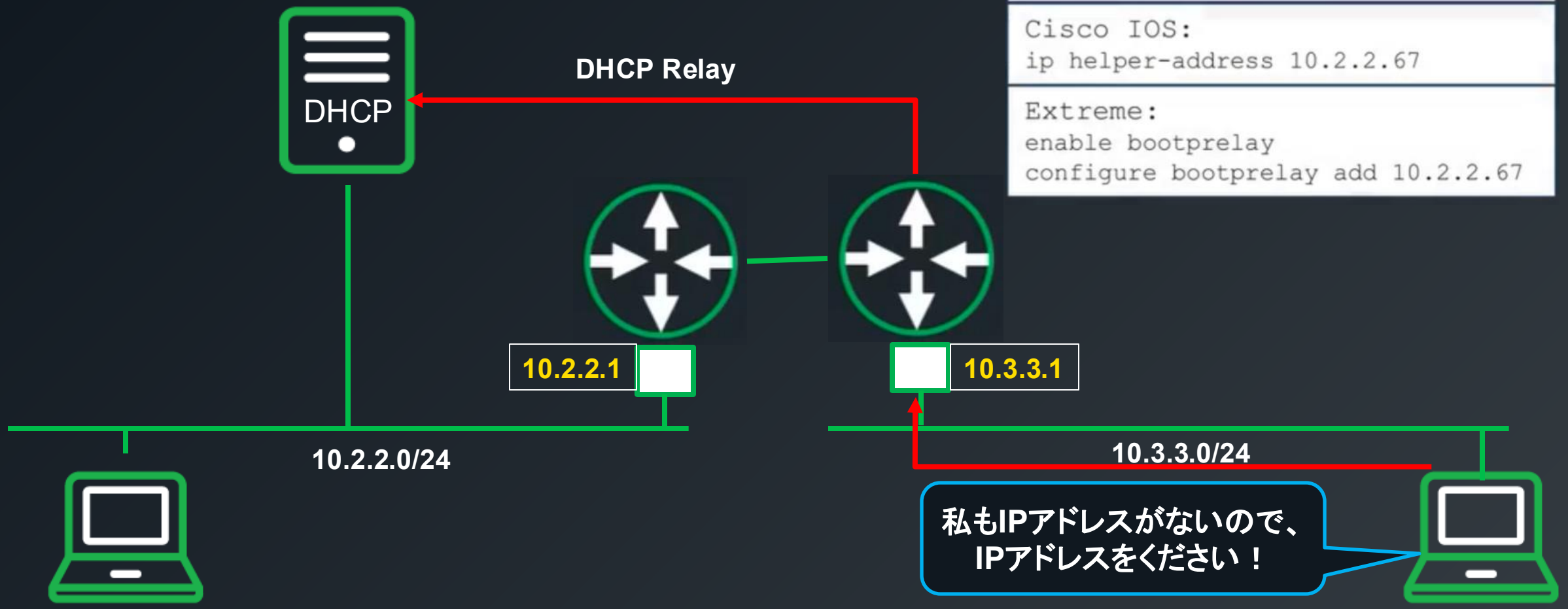


New Lease with Relay

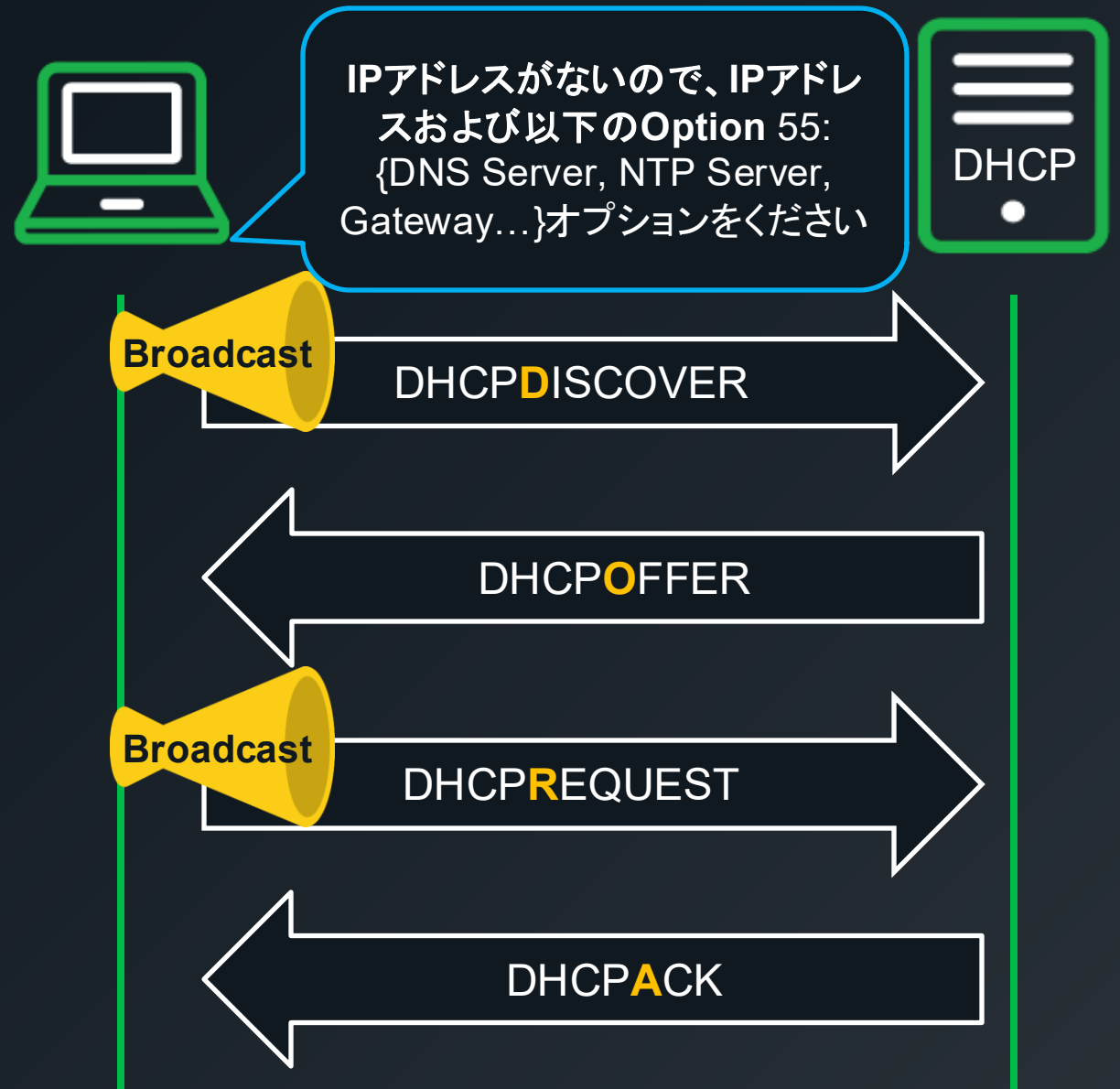
```
Cisco PIX:
dhcprelay server 10.2.2.67 outside
dhcprelay enable inside
dhcprelay timeout 60
```

```
Cisco IOS:
ip helper-address 10.2.2.67
```

```
Extreme:
enable bootprelay
configure bootprelay add 10.2.2.67
```



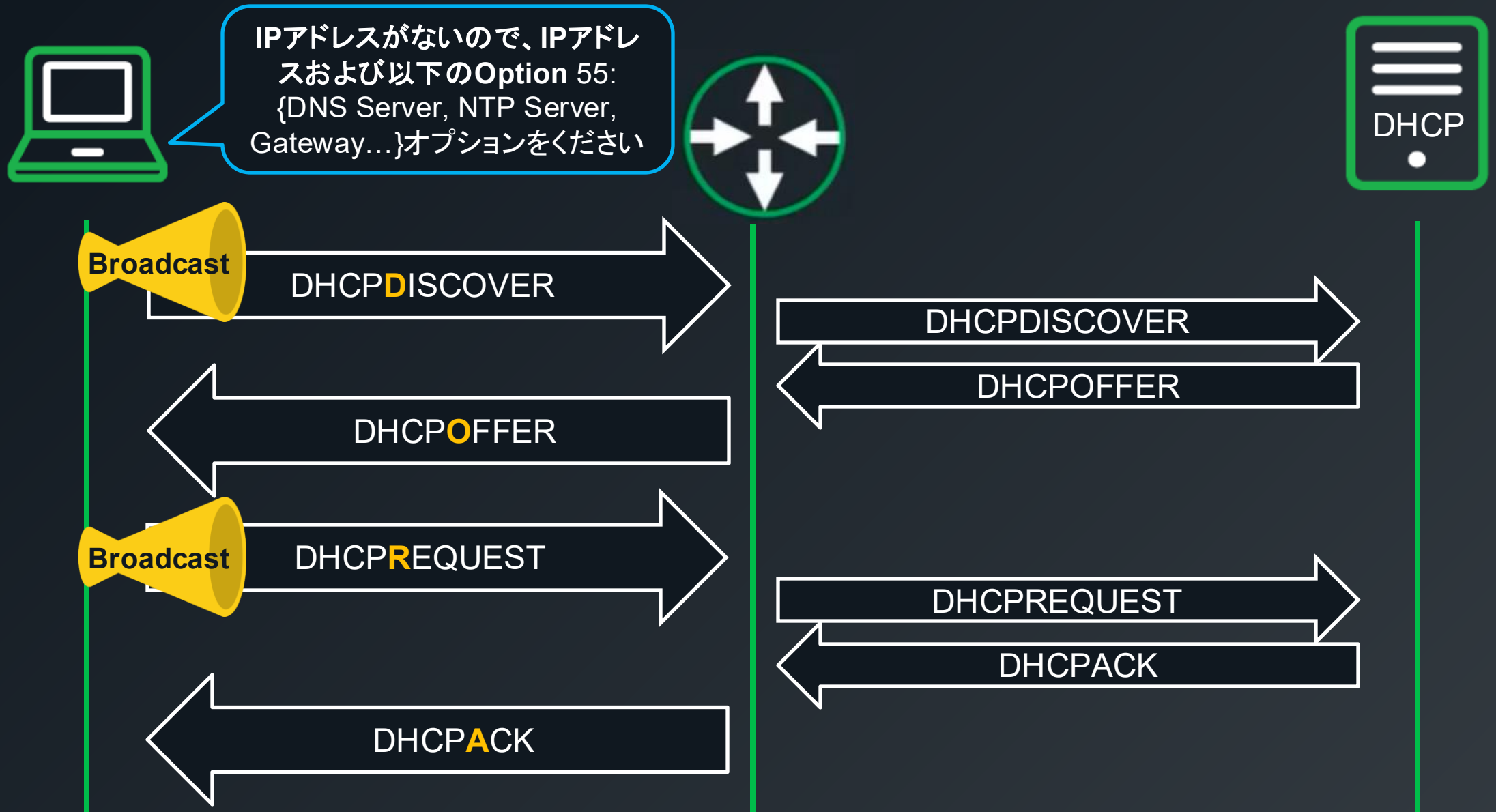
New Lease - DORA



1. DHCP クライアントは DHCP サーバーを検索します。 DHCP クライアントは DHCPDISCOVER メッセージをブロードキャストし、DHCP サーバーのみがメッセージに応答します。
2. DHCP サーバーが、未割り当ての IP アドレス (事前定義されたプールから選択) を、他の設定パラメーターとともに、一定期間 (リース時間) の間、DHCP クライアントに提供します
3. DHCP クライアントは、たとえば複数の DHCP サーバーがその発見メッセージに応答する場合に IP アドレスを選択し、選択された IP アドレスを含む DHCPREQUEST メッセージを各 DHCP サーバーにブロードキャストします。
4. Ack フェーズでは、DHCP サーバーがクライアントによって選択された IP アドレスに確認応答します。

infoblox

New Lease with Relay - DORA



infoblox

Renewal

infoblox

企業は通常DHCPに対してどうしているか？

多くのネットワークが”無料”の **DHCP オプションを使用**

- ほとんどのネットワークではユーザーログインに **Microsoft Server**が必要 (**Active Directory**)
- Microsoft Serverには**DHCPが含まれている**
- 通常、ネットワークの最初の設計時に利用されている

DHCPは一般的なネットワーク機器にも含まれている

- Wifi access points
- Routers
- Firewalls

ほとんどの企業は１つの共通システムに標準化しようとしている

Microsoft
DHCP Server

Access Point
DHCP Server

Firewall
DHCP Server

infoblox

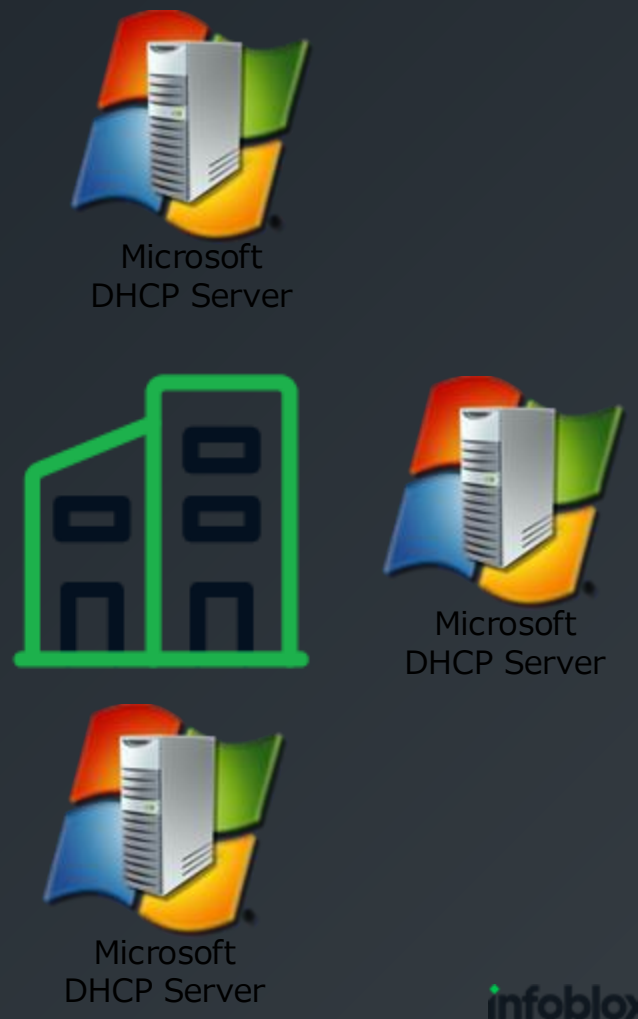
なぜMicrosoftの DHCP Serverを使用しているのか？

多くの企業ではユーザーログインにMicrosoft (**Active Directory**)を使用

- 共通の低コストシステムを提供
- 他のオプションと比較してサーバーを経済的に導入できる

IPネットワークとアドレスの管理には追加の監視が必要

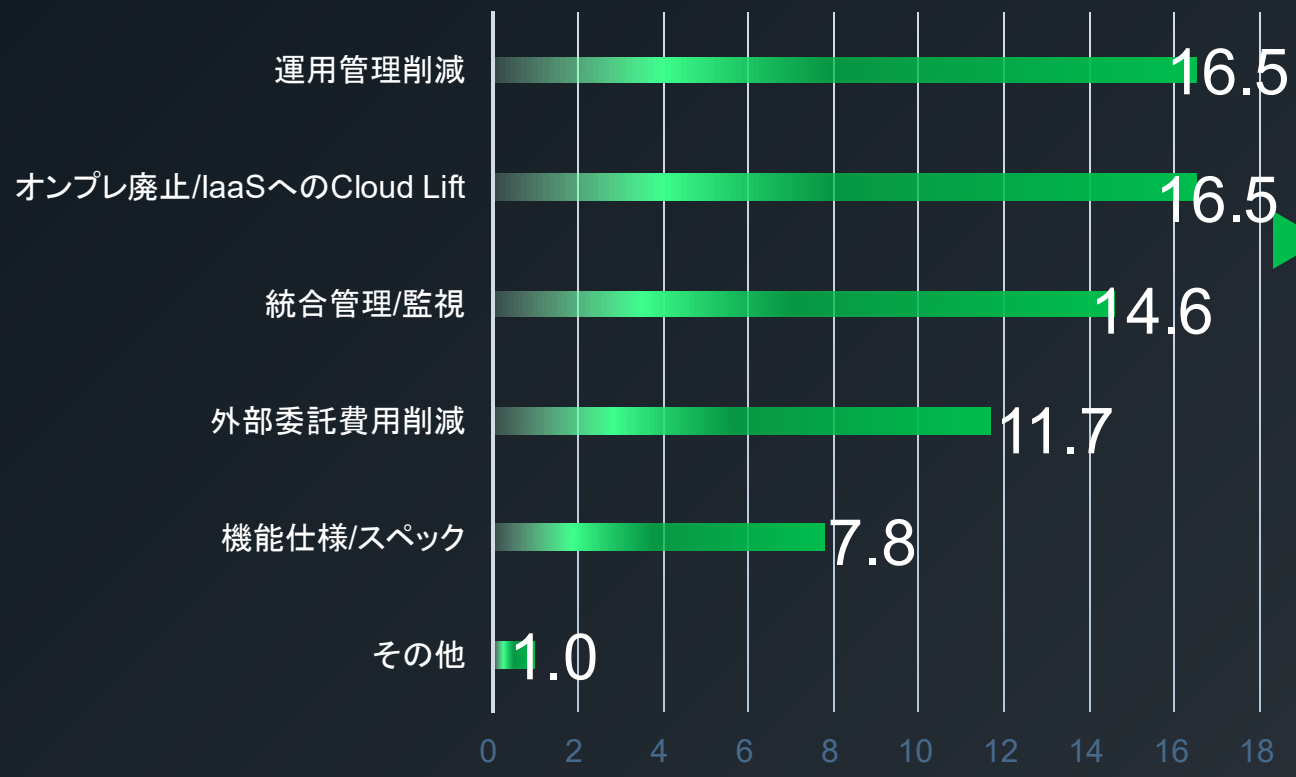
- **IPネットワークとアドレスの一元的な文書化が不可欠**
- 通常はスプレッドシートを使用して行われている
- システム停止を引き起こす人為的なミスが発生しやすい
  - **注意** – 重複、または誤ったIPネットワークやアドレスを発生させてはいけない



infoblox

顕在化している課題とベストプラクティス

現状でDHCPに課題や問題はありますか？（複数回答）



Source: Infoblox Japan 独自調査結果（調査日2024年5月/N=103/マクロミル）

DHCPサーバーのベストプラクティス

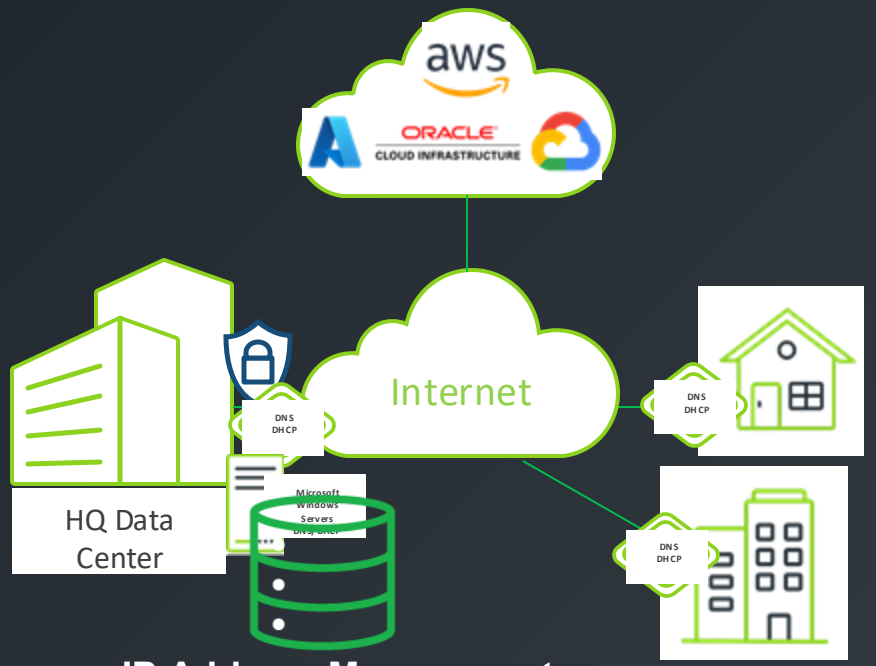
1. **運用管理削減**
   OS付属のDHCPでのUpdate適用の煩雑さやサービス停止が発生したり、複数拠点にわたるIPアドレス管理など運用効率が悪くなるため、堅牢かつ統合IP管理プラットフォームが必須
2. **クラウド化/SaaS化**
   オンプレからクラウド化に伴い、仮想化環境やパブリッククラウドなど様々なプラットフォームで運用できることが求められる
3. **統合管理**
   DCや支社などのオンプレからクラウドまでDHCPの管理がバラバラな場合、DHCP管理の運用効率が悪くなるため、統合管理が必須
4. **監視/可視化**
   誰がいつどのIPアドレスを配置したのか、DHCPレンジの利用状況はどの程度なのか、インシデント発生時のDHCPリースヒストリなど監視/可視化が必要

infoblox

DHCP利用時の課題で求められる機能

企業全体のIPネットワーク/アドレス一元的な管理・可視化

- 複数のデータセンター、事業所、クラウドなど、企業全体のネットワーク, アドレスのIP管理
- IPアドレスの構成ミスや競合などによる不具合の防止
- DHCPレンジの利用状況の可視化
- IPを払い出されたデバイスの詳細情報
- 監査のためのリース履歴やログ機能の提供
- わかりやすいレポート機能



IP Address Management
(IPAM)

IP Address Management (IPAM)が解決します

infoblox

IP Address Management (IPAM) とは

典型的なIPAMとは

Without Infoblox

IT部門はどのIP ネットワーク/アドレスが利用可能か知る必要がある

デバイスに割り当てられたIPアドレスの記録

- IT部門がデバイスにどのIPアドレスが割り当てられているか識別する必要がある
- 割り当てられた全てのネットワークと手動で割り当てられたIPアドレスの追跡
- IT部門の**キャパシティプラニング**を支援
- 通常は **spreadsheets** で管理 (ただしユーザーはIPAMを考慮しない場合があります)

DHCPで割り当てられたIPアドレスに対するユーザー情報を手動で管理

手動で割り当てられたServer IP アドレス

手動で割り当てられた IP Network

手動でのIP Address Managementの課題

NetworkとIPアドレス計画の不一致

- このIPアドレスは本当に利用可能か？
- 彼らは誰でどこにいるか？
- 時間のかかる、手動でprovisioning

非効率で手順が多すぎる

- 利用可能なIPのリクエストおよび検索
- spreadsheetの更新
- DNSの変更
- DHCPの変更
- タスクの委任なし

自動化されていない

	A	B	C	D	E	F	G	H
1	Machine Type	Brand/Model	Data Point	Lab	OS	Ethernet Address	IP Address	Host Name
2	C-3000 x86	Del VEP 1425	3A-18	D321	CentOS	00-C0-4F-4A-18-F4	192.168.128.001	D321-1
3	C-3000 x86	Del VEP 1425	3A-18	D321	CentOS	00-C0-4F-4A-18-F7	192.168.128.002	D321-2
4	C-3000 x86	Del VEP 1425	3A-18	D321	CentOS	00-C0-4F-4A-18-F8	192.168.128.003	D321-3
5	C-3000 x86	Del VEP 1425	3A-18	D321	CentOS	00-C0-4F-4A-18-F9	192.168.128.004	D321-4
6	C-3000 x86	Del VEP 1425	3A-18	D321	CentOS	00-C0-4F-4A-18-EC	192.168.128.005	D321-5
7	C-3000 x86	Del VEP 1425	3A-18	D321	CentOS	00-C0-4F-4A-18-DA	192.168.128.006	D321-6
8	C-3000 x86	Del VEP 1425	3A-18	D321	CentOS	00-C0-4F-4A-18-FB	192.168.128.007	D321-7
9	C-3000 x86	Del VEP 1425	3A-18	D321	CentOS	00-C0-4F-4A-18-DC	192.168.128.008	D321-8
10	C-3000 x86	Del VEP 1425	3A-18	D321	CentOS	00-90-27-10-A1-D8	192.168.128.009	D321-9
11	C-3000 x86	Del VEP 1425	3A-18	D321	CentOS	00-90-27-13-EE-BC	192.168.128.010	D321-10
12	C-3000 x86	Del VEP 1425	3A-18	D321	CentOS	00-90-27-13-EE-C0	192.168.128.011	D321-11
13	C-3000 x86	Del VEP 1425	3A-18	D321	CentOS	00-90-27-13-8A-50	192.168.128.012	D321-12
14	C-3000 x86	Del VEP 1425	3A-18	D321	CentOS	00-90-27-13-E6-2D	192.168.128.013	D321-13
15	C-3000 x86	Del VEP 1425	3A-18	D321	CentOS	00-90-27-13-88-BE	192.168.128.014	D321-14
16	C-3000 x86	Del VEP 1425	3A-18	D321	CentOS	00-90-27-13-EB-FD	192.168.128.015	D321-15
17	C-3000 x86	Del VEP 1425	3A-18	D321	CentOS	00-90-27-10-A1-D8	192.168.128.016	D321-16
18	C-3000 x86	Del VEP 1425	3A-18	D321	CentOS	00-A0-C9-93-81-34	192.168.128.017	D321-17
19	C-3000 x86	Del VEP 1425	3A-18	D321	CentOS	00-90-27-13-7C-FF	192.168.128.018	D321-18
20	C-3000 x86	Del VEP 1425	3A-18	D321		RESERVED	192.168.128.019	D321-19
21	C-3000 x86	Del VEP 1425	3A-18	D321		RESERVED	192.168.128.020	D321-20
22	Print Server Box			C440	v08.41afirmware	00-A0-C9-A2-D0-DC	192.168.128.021	v1 axis1 printsrv
23								
24								
25								

ethernetadd Sheet2 Sheet3 +

InfobloxのDHCP IPAMソリューション概要

統合IP管理データベース

- DNS, DHCP, IP管理の全機能を統合ソリューションとして提供
- Network全体のIP利用状況の可視化
- DHCPレンジの使用率の確認/アラート

マルチクラウド・SaaS対応

- オンプレミス、仮想基盤、クラウドなど企業全体のネットワークにわたるIPアドレス管理を一元的に実現
- SaaSでのDDIソリューションの提供

強力なレポート機能

- 登録外のデバイス検知および可視化
- 未使用IPアドレス/重複トしたIPアドレスの迅速な検出・確認
- インシデント発生時の端末およびユーザーの特定による迅速な対応
- IPAM業務の大幅な工数削減

IPAM画面イメージ

infoblox

統合IP管理 - 企業ネットワークの可視化/管理

IPアドレス／ネットワーク／デバイスの状況を最新の情報にアップデート。**無線端末の追加などの際にもネットワーク接続後、自動的に認識。**

フィルターや検索、
ソートで必要な情報に
瞬時アクセス

接続スイッチ/ポート情報 (Option)
- 接続場所特定が可能

VMware連携
- VMの仮想スイッチ情報を取得
- Infoblox DDI標準機能

IPAM Home > 192.168.0.0/16

192.168.100.0/24 IPv4

IP Map | List

Quick Filter [G] - Used | On | Filter Off | Show Filter

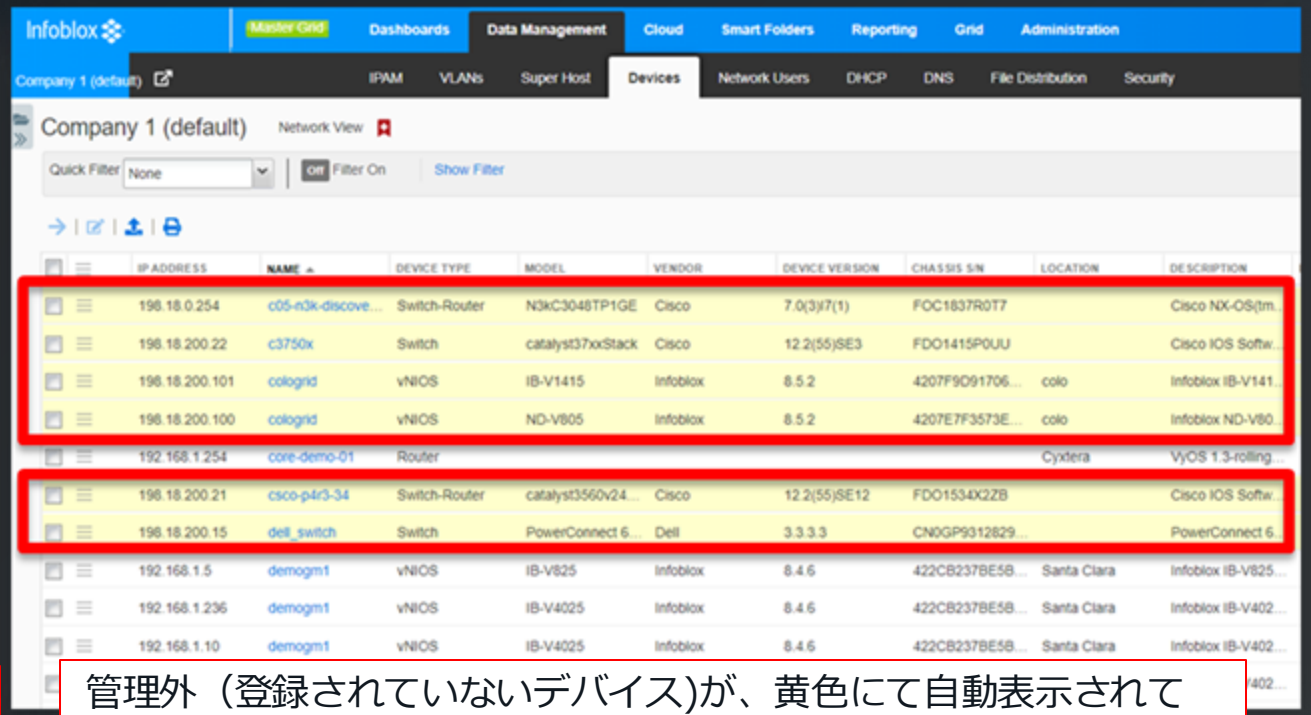
Go to | Go

Clear
Convert
Discover Now
To Host
To A Record
To PTR Record
To Fixed Address

IP Address	MAC Address	OS	Fingerprint	Attache...	Attac...	VLAN ID	Virtual Sw...	Virtual...	Virtual Entity Name	管理者部署	Type
192.168.100.73	00:17:a4:e2:b2:98		Microsoft Windows XP	cat2900	Fa0/6	100				技術部	Lease, IPv4 DH
192.168.100.74	28:d2:44:62:29:71	Microsoft	No Match							技術部	Lease, IPv4 DH
192.168.100.75	00:0c:29:c1:47:c1	Linux 3.0	Ubuntu 11.04	cat2900	Fa0/1	100	vSwitch2	vmnic2	GNS3WB86	技術部	A Record, Leas
192.168.100.76	00:0c:29:c1:47:cb	Linux 3.0	Ubuntu 11.04	cat2900	Fa0/1	100	vSwitch2	vmnic2	GNS3WB86	技術部	Lease, IPv4 DH
192.168.100.77	00:0c:29:c1:8f:23	Ubuntu...	Ubuntu/Debian 5/Knoppix 6	cat2900	Fa0/2	100	vSwitch3	vmnic3	matsu-host-172	技術部	A Record, Leas
192.168.100.78	2c:27:d7:e7:75:2e		No Match	cat2900	Fa0/4	100				技術部	Lease, IPv4 DH
192.168.100.79	d4:3d:7e:e7:[illegible]		No Match	cat2900	Fa0/5	100				技術部	Lease, IPv4 DH
192.168.100.80	00:0c:29:c4:eb:98	Ubuntu...	No Match				vSwitch2	vmnic2	matsu-GNS3 Wo...	技術部	Lease, IPv4 DH
192.168.100.81	00:0c:29:c4:eb:6e	Ubuntu...	Ubuntu/Debian 5/Knoppix 6				vSwitch2	vmnic2	matsu-GNS3 Wo...	技術部	Lease, IPv4 DH
192.168.100.82	00:0c:29:3b:1b:9d	Ubuntu...	Ubuntu (lubuntu, matsu)	cat2900	Fa0/1	100	vSwitch2	vmnic2	matsu-lubuntu01	技術部	A Record, Leas
192.168.100.83	00:0c:29:24:b9:f7	Ubuntu...	Ubuntu (lubuntu, matsu)	cat2900	Fa0/2	100	vSwitch3	vmnic3	matsu-lubuntu04	技術部	A Record, Leas
		Ubuntu...	Ubuntu (lubuntu, matsu)	cat2900	Fa0/1	100	vSwitch2	vmnic2	matsu-lubuntu02	技術部	A Record, Leas
		Ubuntu...		cat2900	Fa0/2	100	vSwitch1	vmnic1	matsu-host2-IBHP	技術部	IPv4 Fixed Addr
			Microsoft Windows 8	cat2900	Fa0/1	100				技術部	Lease, IPv4 DH
		Microsoft	Microsoft Windows Vista/7				vSwitch3	vmnic3	win7	技術部	Lease, IPv4 DH
			No Match								

クライアントOS自動判別
- 払い出し制御も可能
- Trinzic DDI標準機能
  DHCPフィンガープリンティング

統合IP管理 – 不正デバイスの検知 / 重複IPの検出

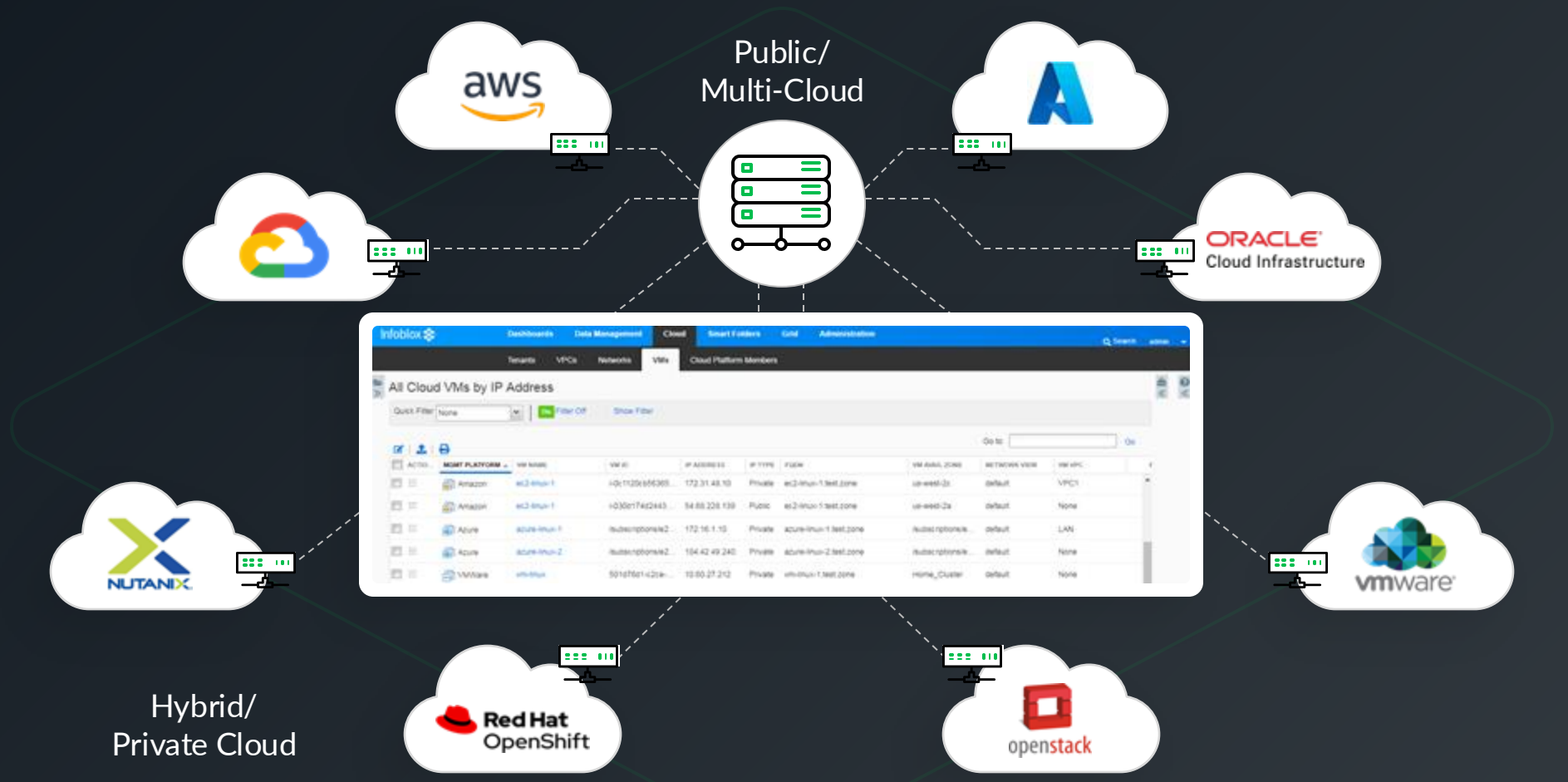


- 管理外（登録されていないIPアドレス)が、黄色にて自動表示されて、管理者へ通知可能。
- 重複したIPを可視化(赤色表示)。Option製品と組み合わせることで特定のノードがどのスイッチポートに接続されているかも即座に判明

管理外（登録されていないデバイス)が、黄色にて自動表示されて、管理者へ通知可能。
＊管理者の意図しないデバイスの接続を把握し、情報表示。インシデント時の疑わしい接続の切り分けに役立ちます

Cloud化/SaaS化 - Public/Hybrid/Multi-Cloud への対応

クラウド ネットワーク オートメーションと vNIOS を使用した、
プラットフォームに依存しない統合と制御によるマルチクラウドの実現



Infoblox Universal DDI™
(フルSaaS型 DDIソリューション)

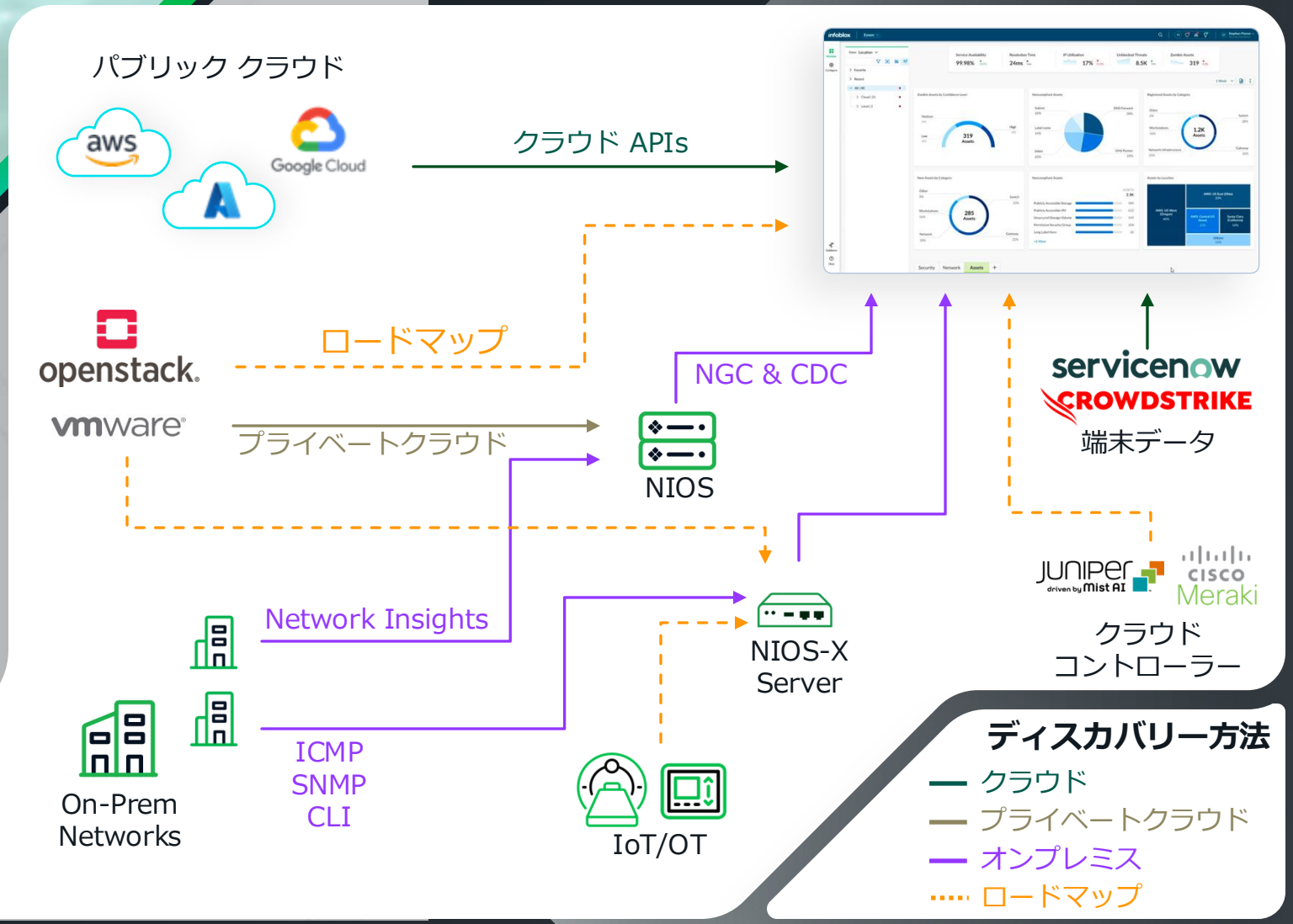
Infoblox Universal DDI Management ™

- Universal DNS Management™
- Universal DHCP Management™
- Universal IP Address Management™
- Universal Asset Insights™

- NIOS-X Physical Server
- NIOS-X Virtual Server
- NIOS-X as a Service

3rd Party

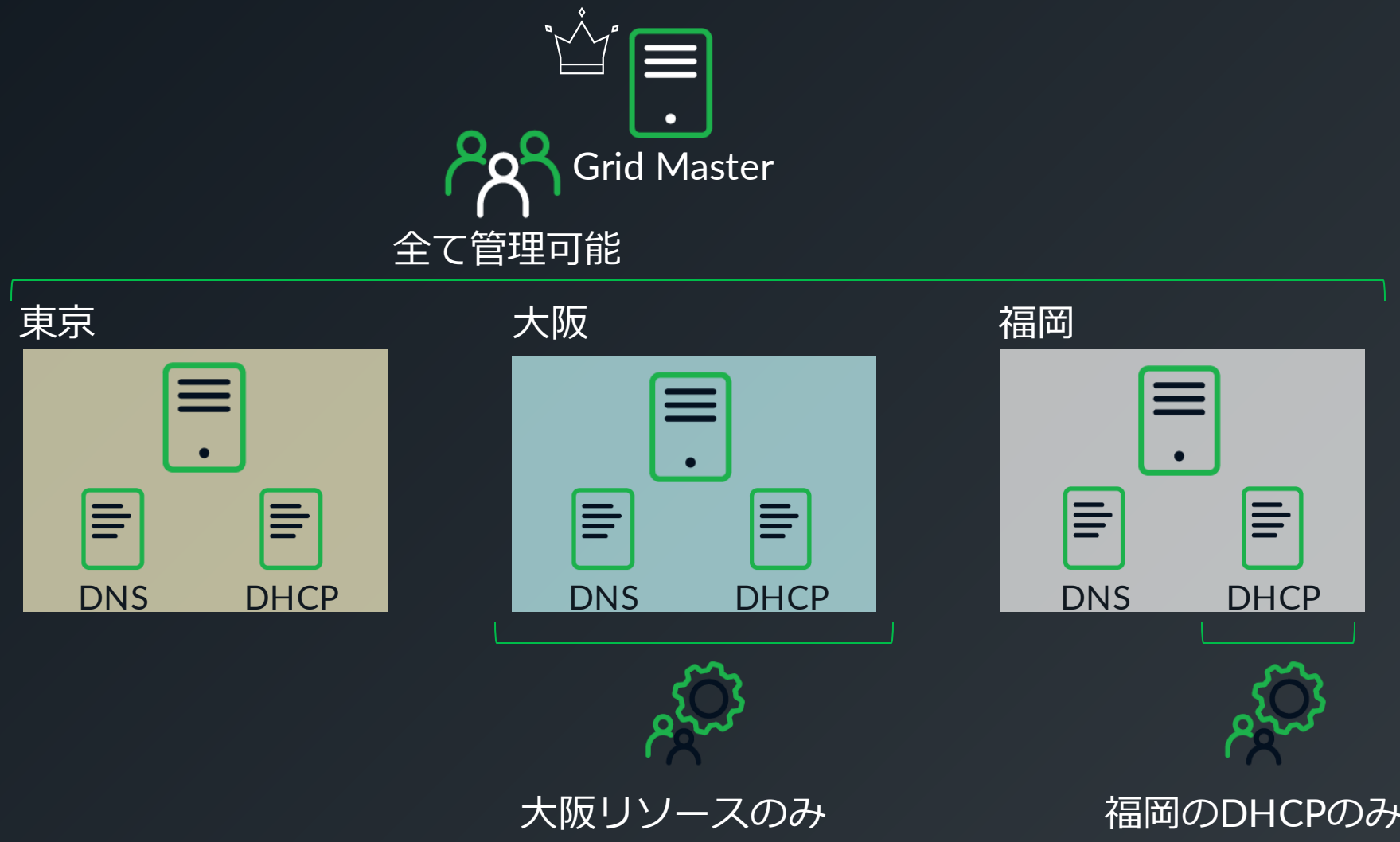
UNIVERSAL ASSET INSIGHTS (Cloud環境も含めた統合アセット管理)



infoblox

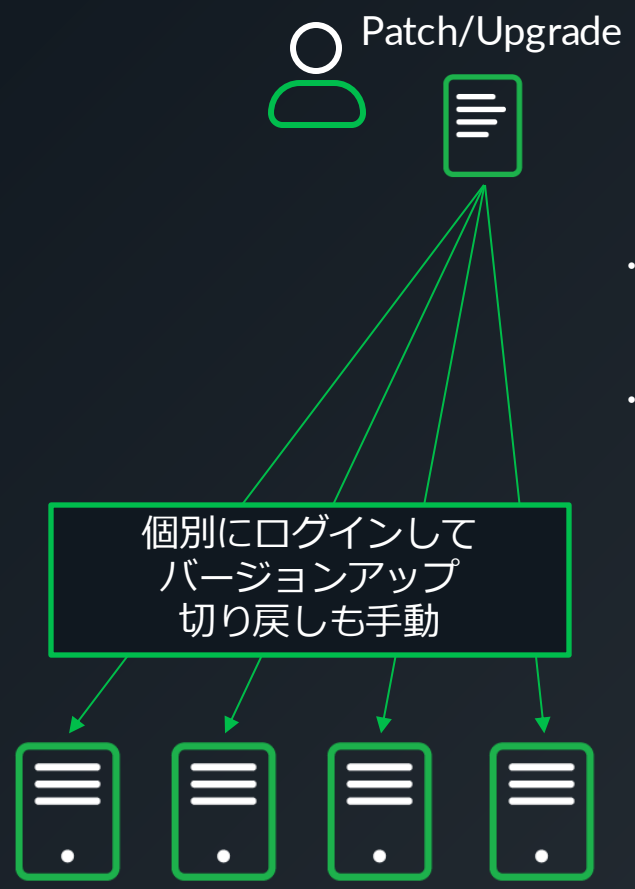
統合管理 – 権限委譲

統合管理を実現しつつ、各拠点や役割に応じて柔軟なアクセス権限を設定可能

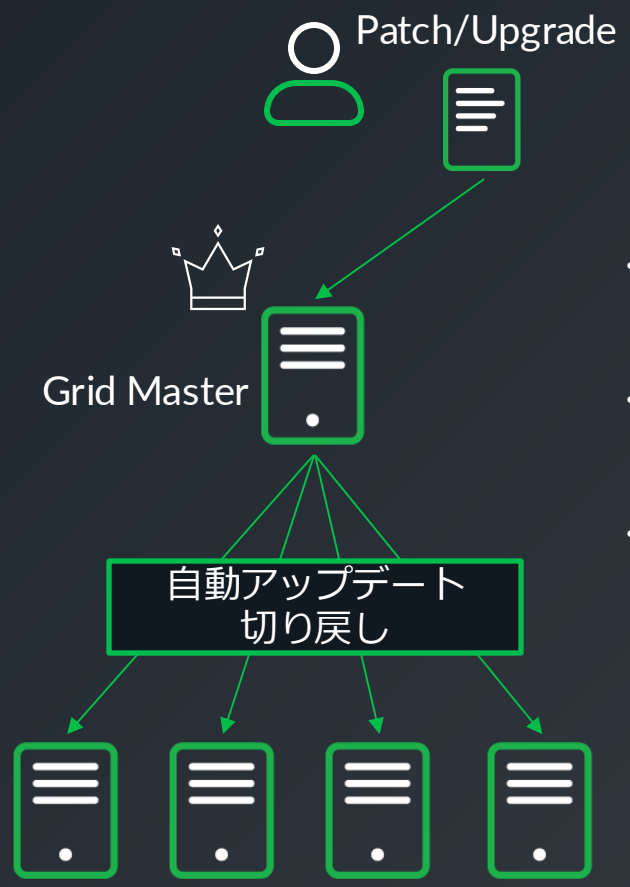


統合管理 – バージョンアップ

パッチ適用 / バージョンアップ管理が容易



- 全てのサーバーを手動でバージョンアップが必要
- 不具合が出た場合、個別に切り戻し作業が必要



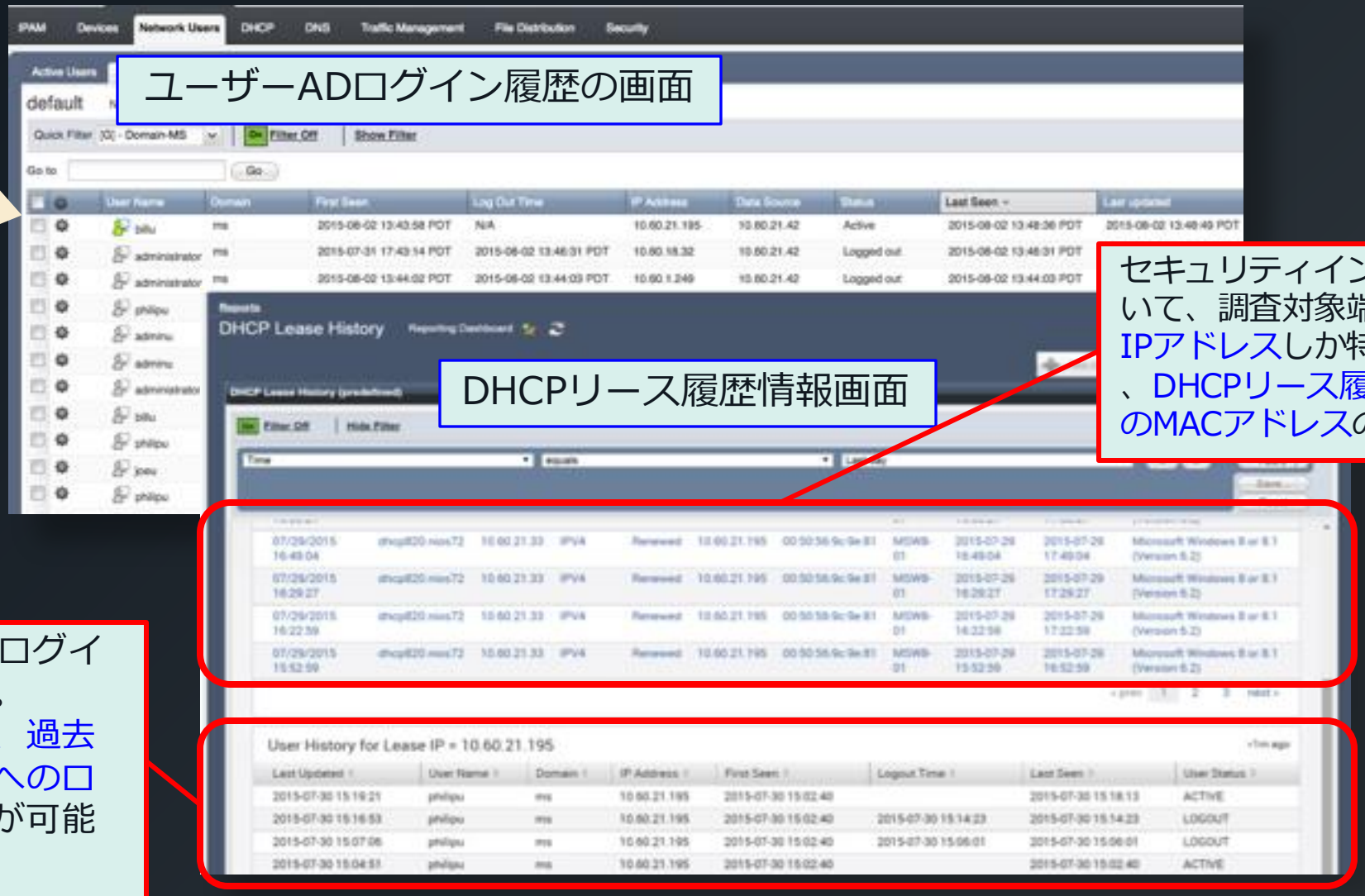
- 自動でバージョンアップ検証を実施
- ワンクリックでバージョンアップ作業を実施
- 不具合が出た場合、ワンクリックで全サーバで切り戻しを実施

infoblox

レポート機能 - インシデント発生時の端末及びログインユーザー特定機能

閲覧可能なADログイン情報

Data
User Name
Domain
First Seen
IP address
Data Source
Last Seen
Last Update



セキュリティインシデント対応において、調査対象端末のIPアドレスしか特定できない場合に、DHCPリース履歴から即座に端末のMACアドレスの特定が可能。

DHCPリース履歴にADログイン情報を紐づけが可能。インシデント対応時に、過去のある時点の特定端末へのログインユーザーの特定が可能。

まとめ

DHCPは業務に必要なコアネットワークサービスであり
優れた堅牢性や管理性が重要

Public/ Hybrid/Multiクラウドへの対応が必須に
セキュリティやコンプライアンスの観点からDHCPのリース
ログや可視化が必要

企業ネットワーク全体でのリアルタイムでのネットワーク健
全性のためにIPAMが必要。DHCP, DNSも含めた一元的
なDDIデータベースを持つIPAMが必要

THANK YOU!!!

© 2024 Infoblox Inc. All rights reserved.