

DMM.com インフラ部における

SSoT への道

～過去・未来・そして現状～

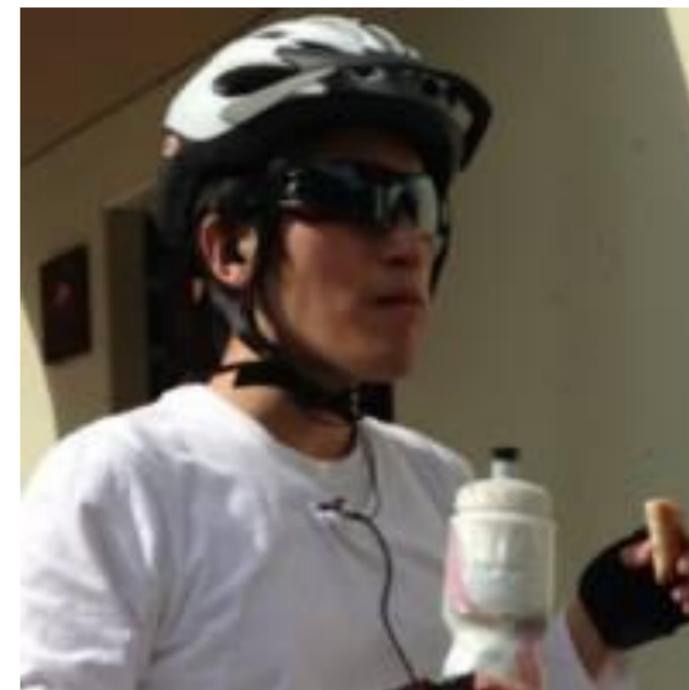


DMM.com ITインフラ本部 - インフラ部 / 大山 裕泰

登壇者プロフィール

大山 裕泰 (DMM.com / IT インフラ本部)

インフラの運用効率化に従事。2017年1月から社内
の情報管理システムの改善に取り組み、2018年11月に
旧システム (RackTables) を内製システムにリプレース。
システムの機能改修を重ね、現在は情報管理システムと
IFTTT 運用基盤 (StackStorm) を連携させた、機動的なインフラの運用に取り組む。



Introduction

✓ 概要と目的

これまでにどのような課題を持ち、
何を目指し、何を行なってきたかをご紹介します

同じ課題（目的）を持つ人たちと、
異なる手法について議論を交わしたい。

過去の情報管理の課題

- その昔、誰も管理情報を信頼していなかった頃の話

過去の情報管理の課題 1

✓ 実情報と管理情報の差異

- 実情報 (e.g. 機器の設定, システムの状態) と管理情報が違っている
作業毎の確認作業コストと、情報の棚卸しの作業コスト増



過去の情報管理の課題 2

✓ 追えない履歴

- 登録情報が誰が、いつ、設定したものかわからない
変更履歴も追えず、誰に問い合わせればよいかわからない

いつ実施するのか？ 誰に問い合わせるか？



運用者

...	
備考	近日削除予定
...	

情報管理システム

過去の情報管理の課題 3

✓ 復旧不能なデータの消失

- オペミス等によって登録データを空値で更新

更新前のデータがわからない（復旧に伴う作業コスト & データの消失リスク増）

元々設定されていた情報は何だった？



運用者

運用担当チーム

...

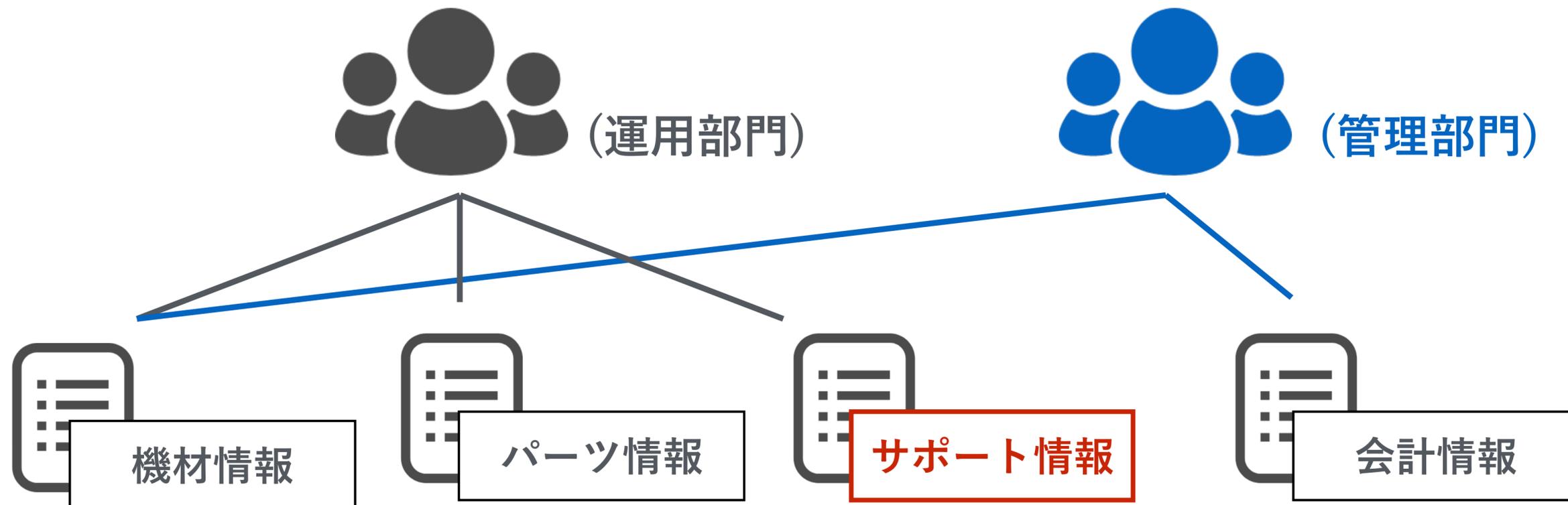
情報管理システム

過去の情報管理の課題 4

✓情報の分散・多重管理

- 部署毎に関連する情報を独自に管理

情報の冗長管理・整合性検査に伴う管理コスト増

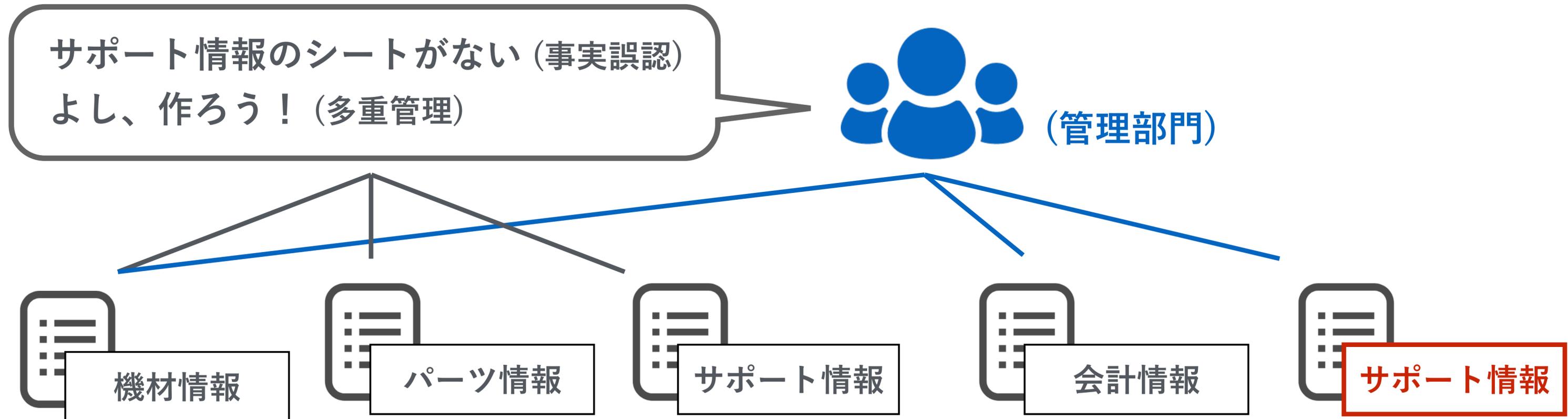


過去の情報管理の課題 4

情報分散・多重管理

- 部署毎に関連する情報を独自に管理

情報の冗長管理・整合性検査に伴う管理コスト増

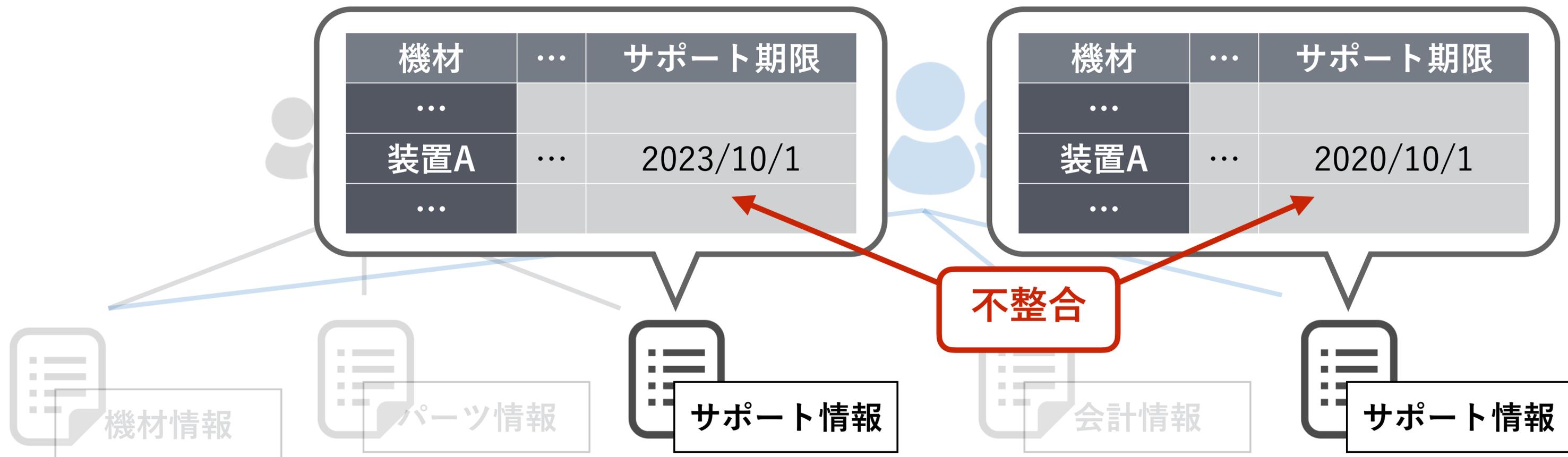


過去の情報管理の課題 4

情報分散・多重管理

- 部署毎に関連する情報を独自に管理

情報の冗長管理・整合性検査に伴う管理コスト増



過去の情報管理の課題 - まとめ

✓ 運用上の課題・機能的な制約に伴う課題

- 実・管理情報の不整合
- 変更履歴の追跡、データの部分復旧ができない

✓ 各部署が独自に関連情報を管理し始める

- 分散・多重管理による、オペミス危険性や管理コストの増大

我々が目指す情報管理システム

- SSoT を実現させるためにあるべき情報管理のあり方

対象とする情報と「管理」のあり方

✓情報が正しく「管理」されているとは？

- 情報が保存・取得できる状態が保たれている
- 保存された情報の整合性が保たれている
- 保存された情報に対する適切な権限が保たれている

✓情報

- 物理情報：機器のラック配置、物理配線、電源容量 等
- 論理情報：VLAN, IP アドレス 等
- 管理情報：減価償却費、リース期限 等
- 運用情報：機器の利用者・利用状況 (e.g. サービスxxx / STG 用) 等

我々が目指す情報管理システム

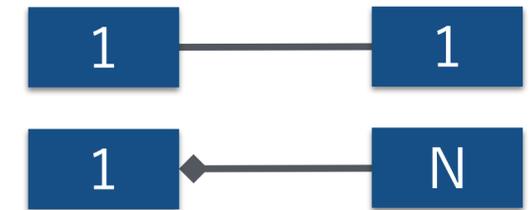
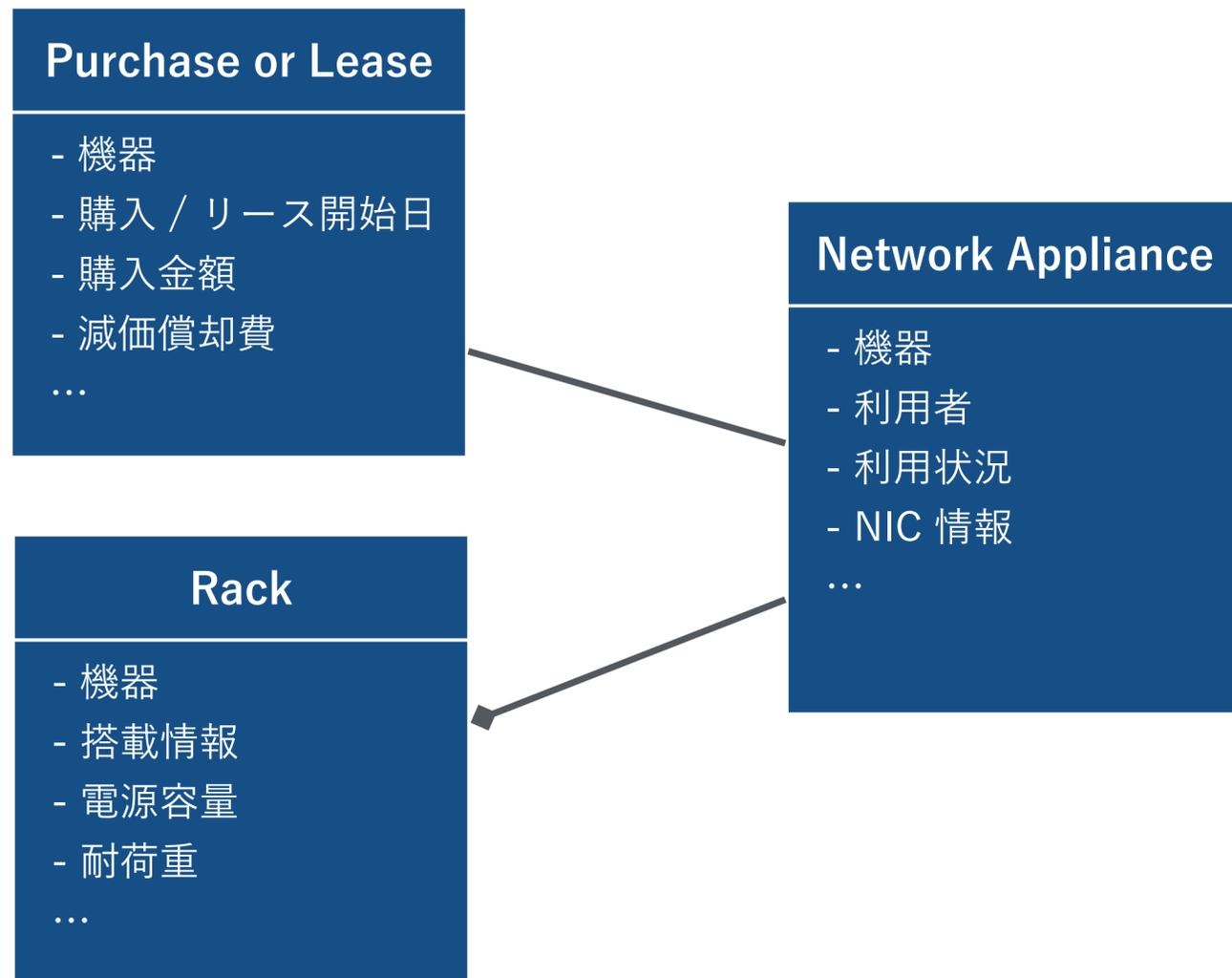
✓情報管理システムに求める基本要件

- 拡張性：管理・運用に必要なデータが全て集まっている
- 機密性：必要なユーザだけが必要な情報にアクセスできる
- 追跡性：誰が、いつ、何を設定したのかが追跡・復旧できる
- 整合性：登録データが正である（実情報と差異がない）と信頼できる

我々が目指す情報管理システム

✓ 1. 拡張性の保証

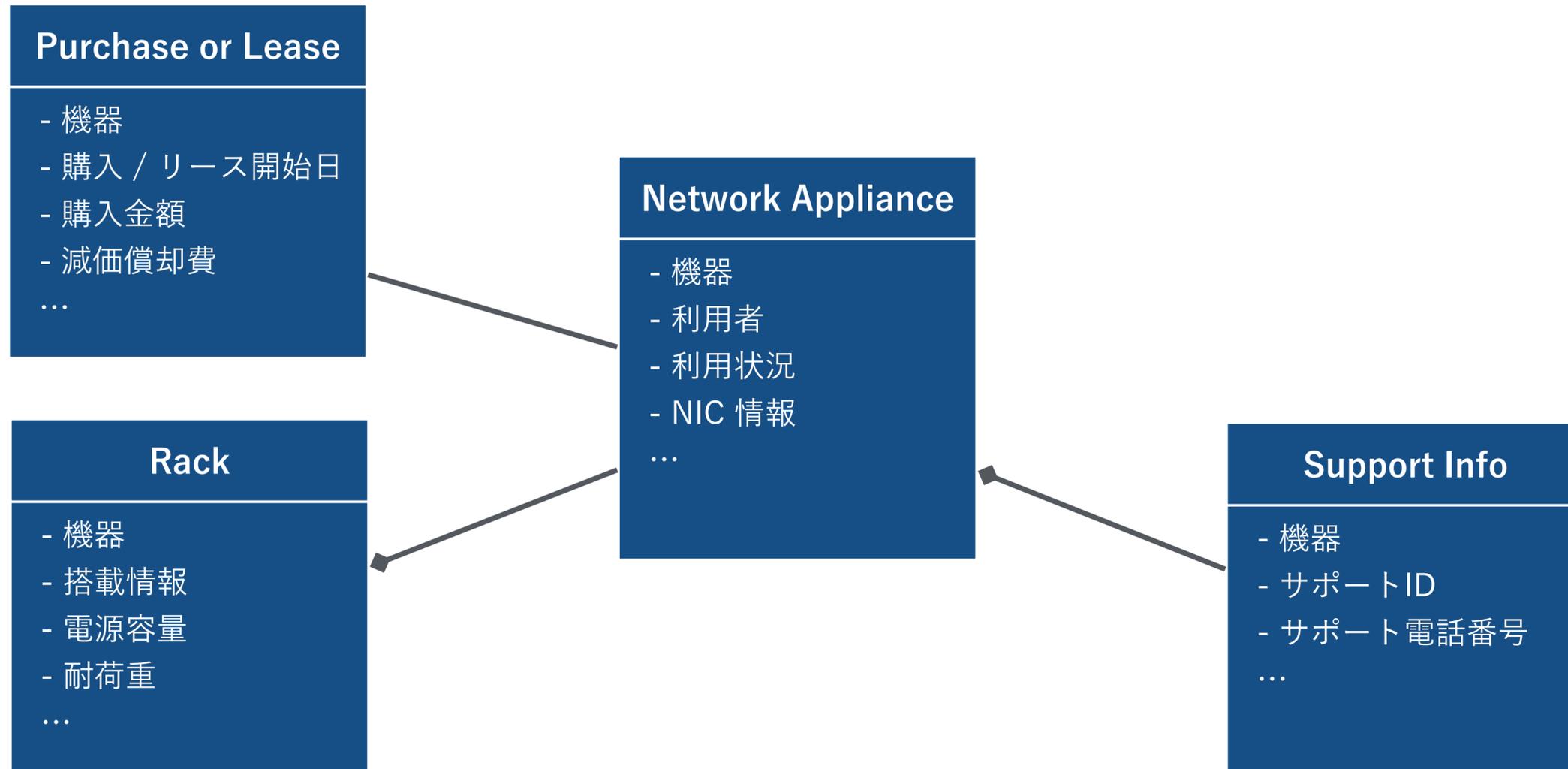
- どんなに複雑なデータ構造でも定義・拡張できる仕組み



我々が目指す情報管理システム

✓ 1. 拡張性の保証

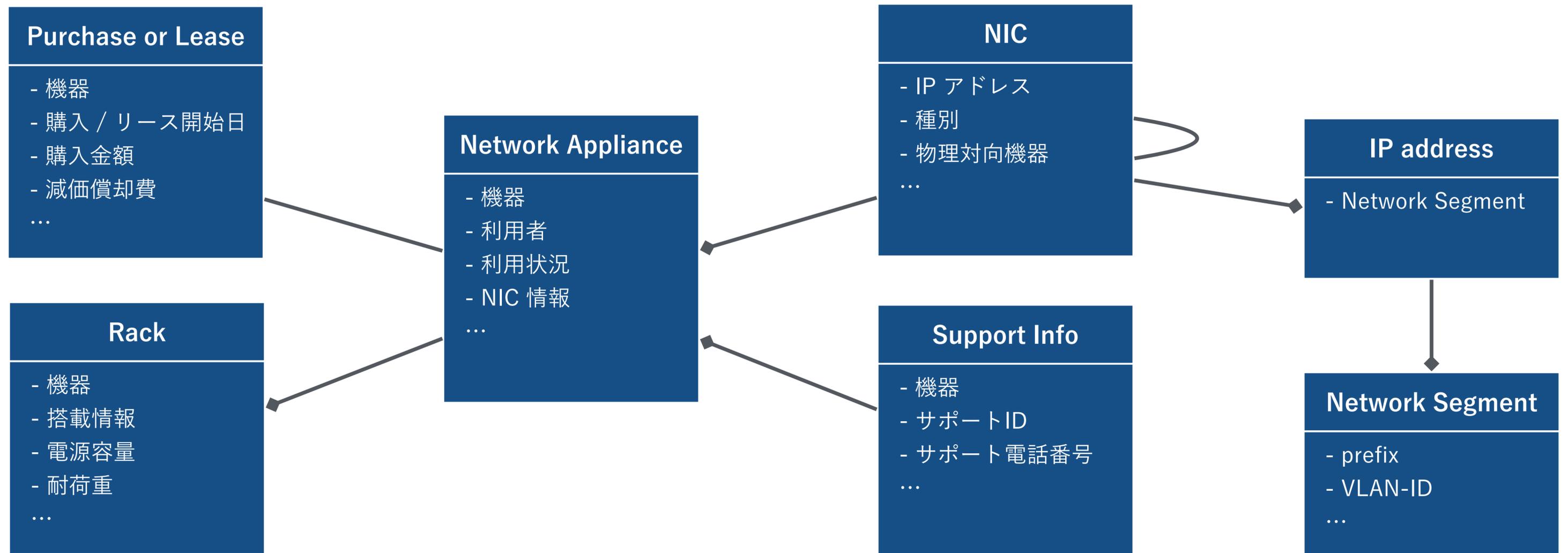
- どんなに複雑なデータ構造でも定義・拡張できる仕組み



我々が目指す情報管理システム

✓ 1. 拡張性の保証

- どんなに複雑なデータ構造でも定義・拡張できる仕組み

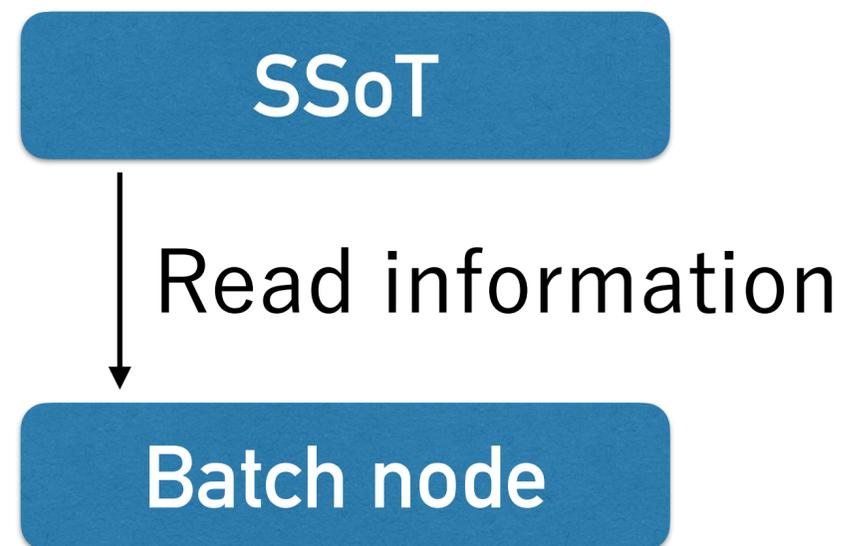


我々が目指す情報管理システム

✓ 2. 機密性の保証

- 集約されたデータに対する柔軟なアクセス制御の必要性

Case1: 勝手にデータが改変されると困る場合



Cloud Service

Appliance

Other Service

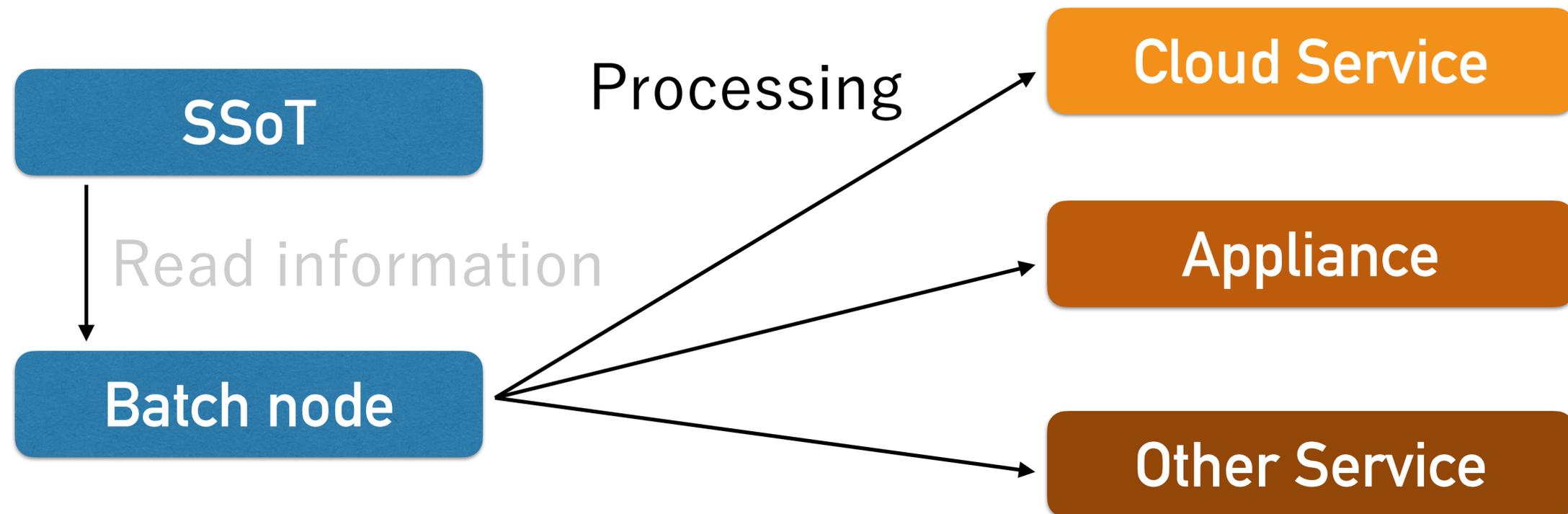


我々が目指す情報管理システム

✓2. 機密性の保証

- 集約されたデータに対する柔軟なアクセス制御の必要性

Case1: 勝手にデータが改変されると困る場合

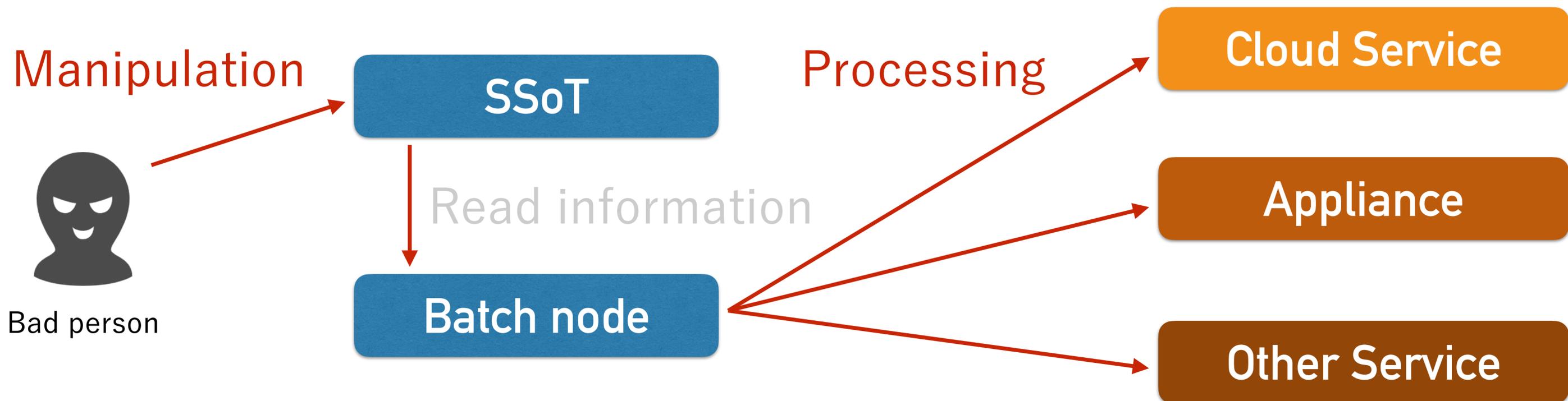


我々が目指す情報管理システム

✓2. 機密性の保証

- 集約されたデータに対する柔軟なアクセス制御の必要性

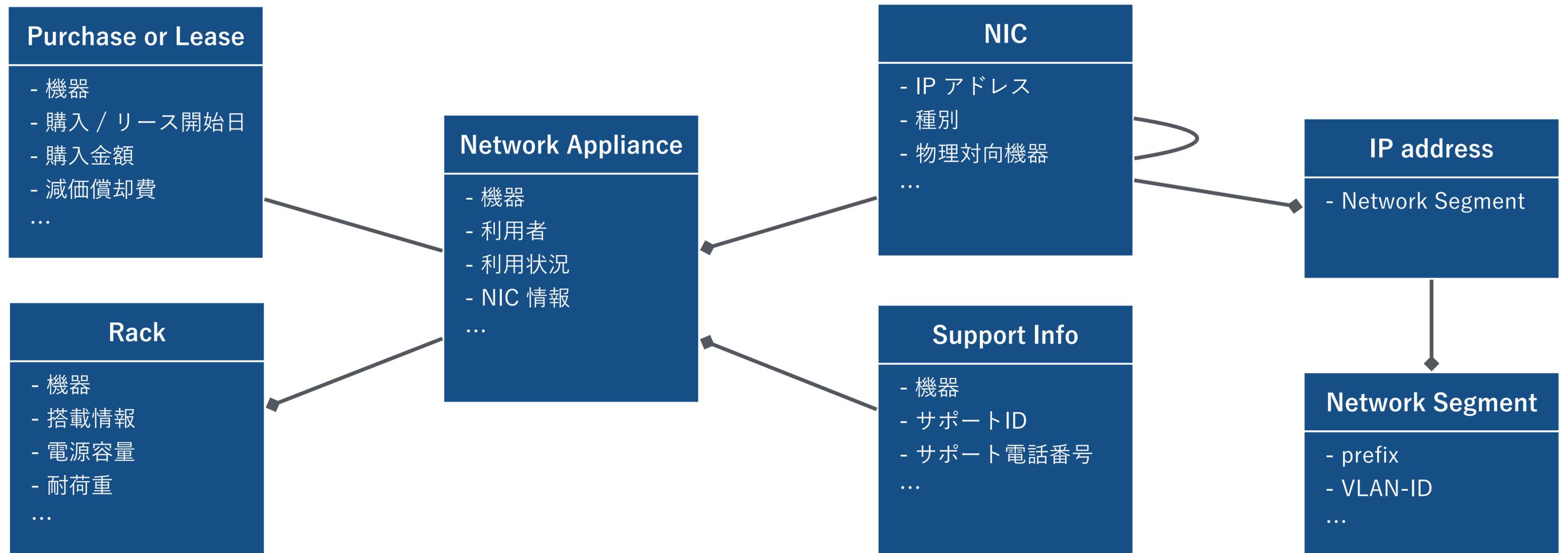
Case1: 勝手にデータが改変されると困る場合



我々が目指す情報管理システム

2. 機密性の保証

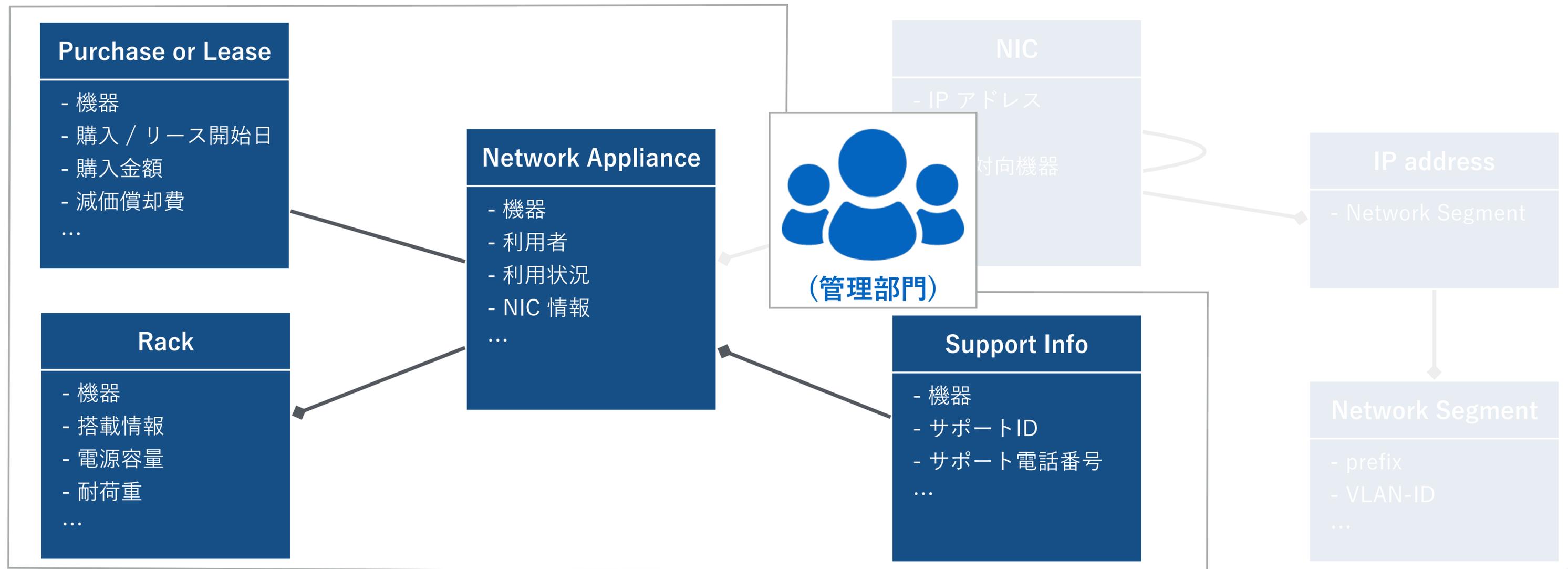
- 集約されたデータに対する柔軟なアクセス制御の仕組み



我々が目指す情報管理システム

2. 機密性の保証

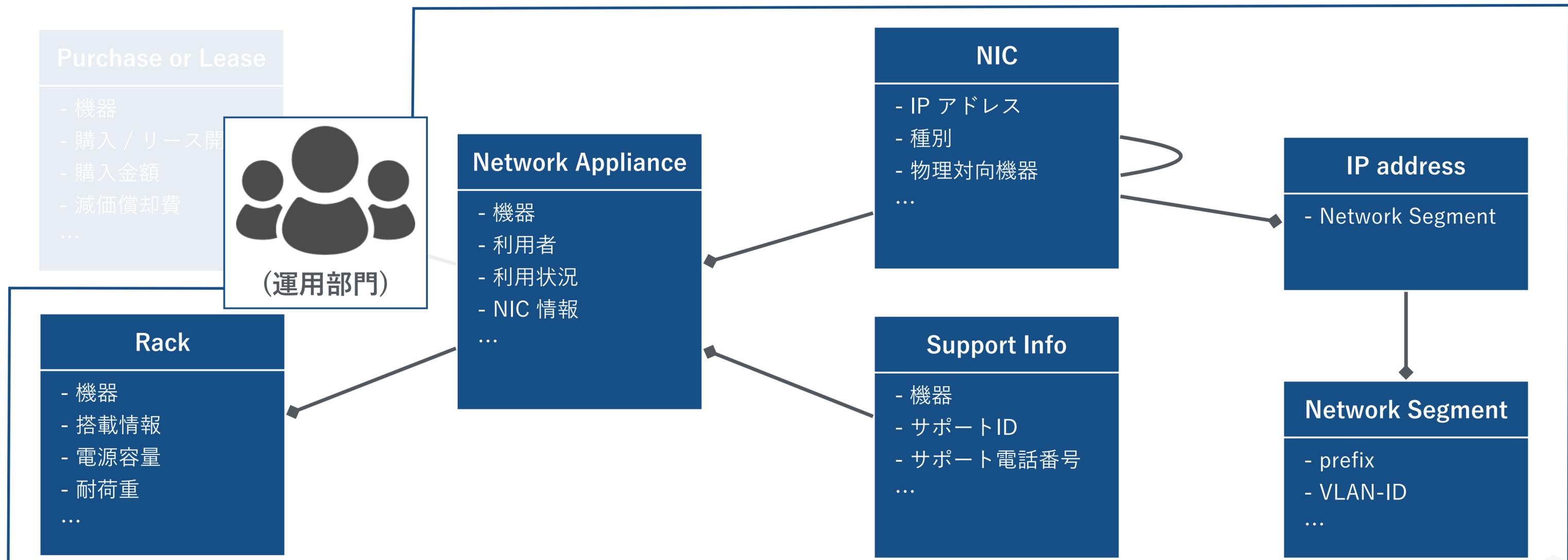
- 集約されたデータに対する柔軟なアクセス制御設定



我々が目指す情報管理システム

2. 機密性の保証

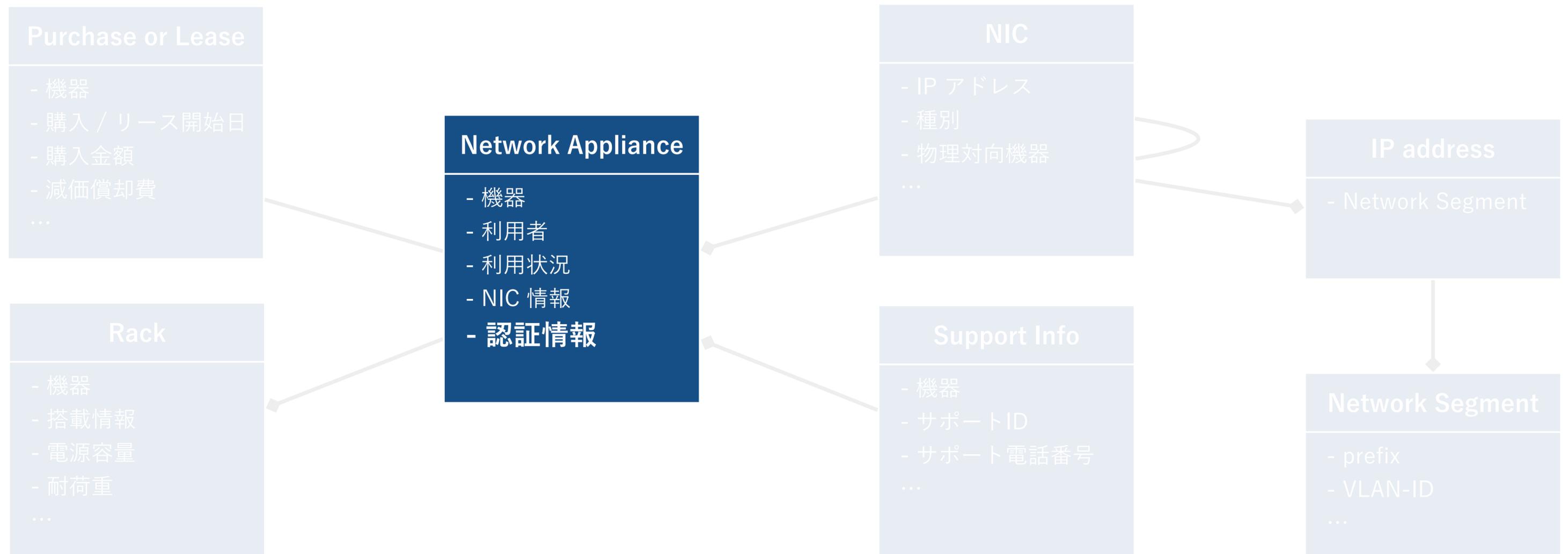
- 集約されたデータに対する柔軟なアクセス制御設定



我々が目指す情報管理システム

2. 機密性の保証

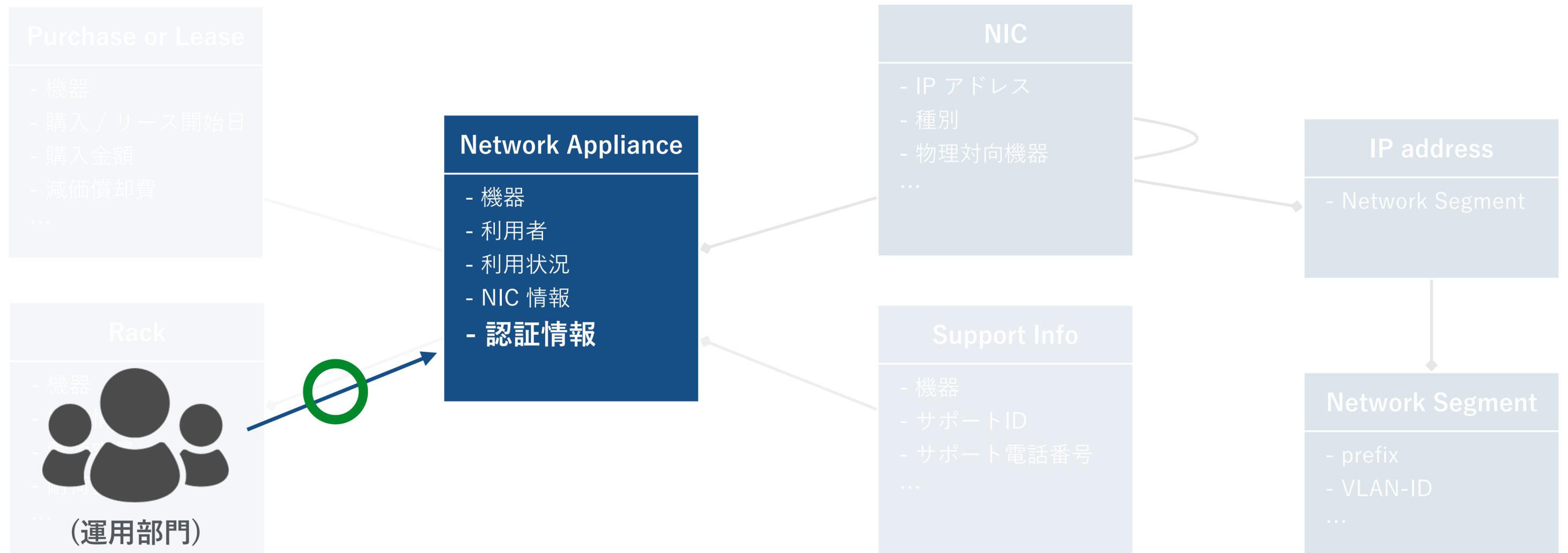
- 集約されたデータに対する柔軟なアクセス制御設定



我々が目指す情報管理システム

✓2. 機密性の保証

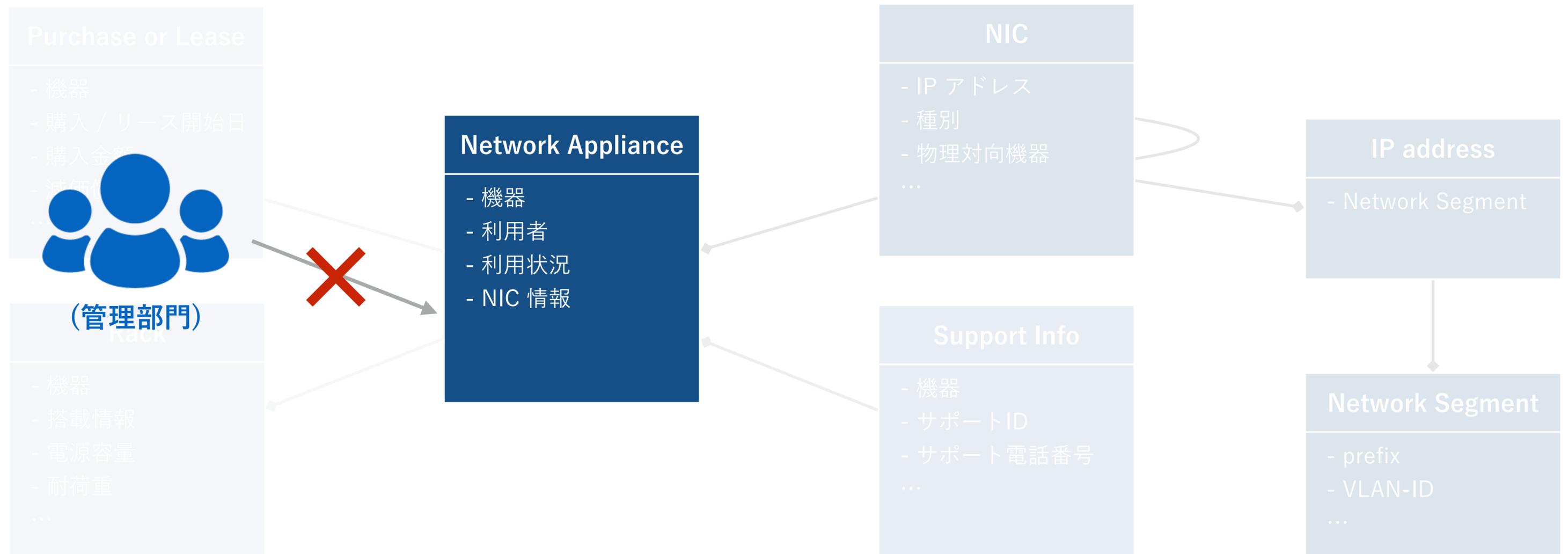
- 集約されたデータに対する柔軟なアクセス制御設定



我々が目指す情報管理システム

2. 機密性の保証

- 集約されたデータに対する柔軟なアクセス制御設定



我々が目指す情報管理システム

✓ 3. 追跡性の保証

- データの発生から現在に至るまでの全ての変更データを保持
 - 「誰が、いつ、何の情報を、何から、何に変更したか」の情報を保持
 - ある時点における、ある Network Appliance の「利用状況」のデータ

誰が、いつ設定した値だっけ？



運用者

利用状況

廃棄/返却済



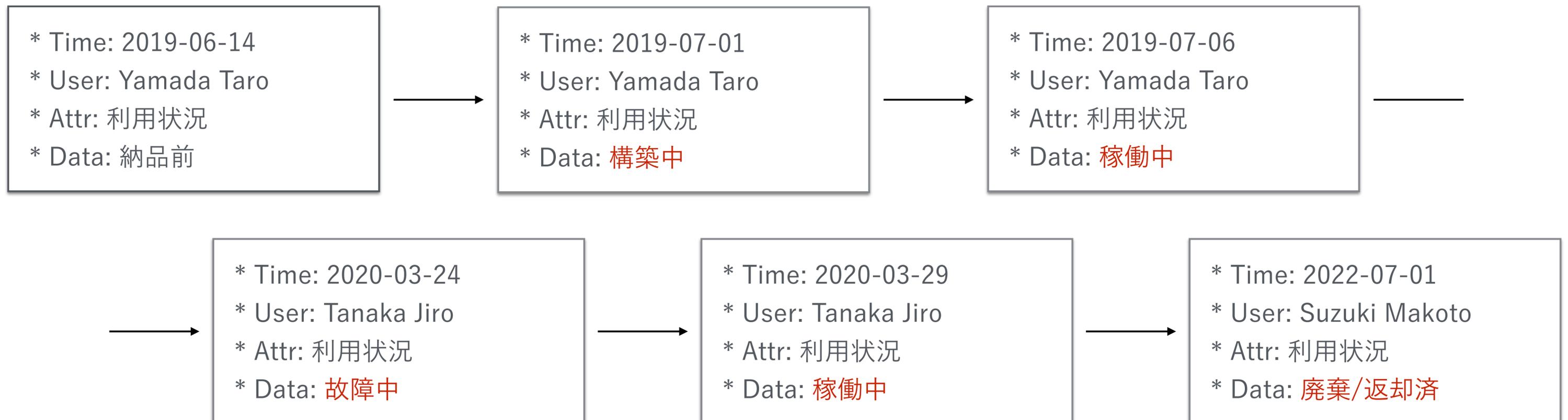
我々が目指す情報管理システム

3. 追跡性の保証

- データの発生から現在に至るまでの全ての変更データを保持

「誰が、いつ、何の情報を、何から、何に変更したか」の情報を保持

- 当該 Network Appliance の「利用状況」のデータの更新履歴



我々が目指す情報管理システム

✓ 4. 整合性の保証 (1/2)

- 管理システム ⇔ 実システムの整合性を保証する仕組み

情報の作成・更新が行われた際、予め webhook に登録されたリクエストハンドラを実行

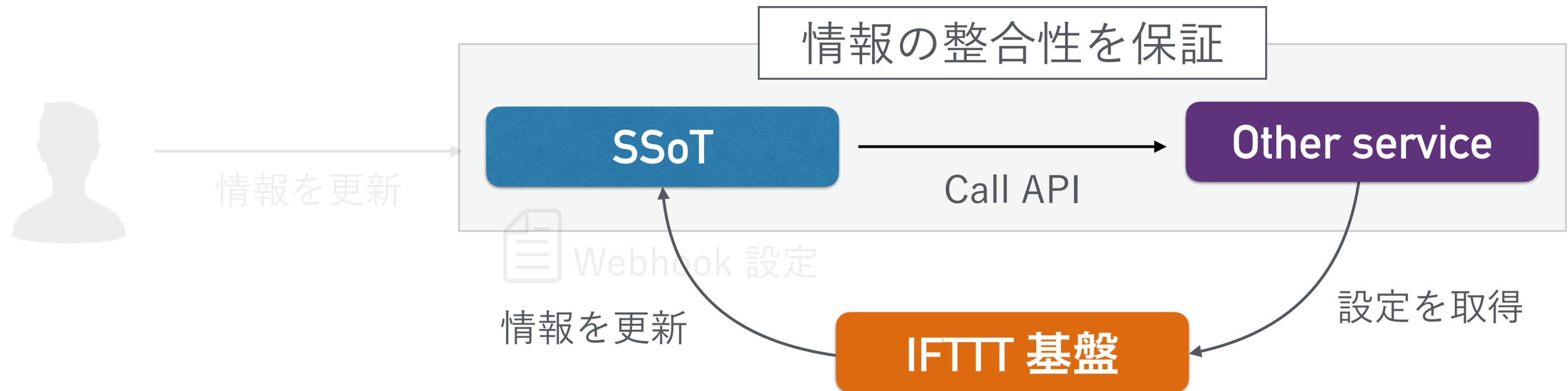


SSoTと運用効率化の現状

✓ 4. 整合性の保証 (2/2)

- 管理システム ⇄ 実システムの整合性を保証する仕組み

仮想基盤の各 VM の構成情報が AirOne (SSoT) に反映させる仕組みを構築



我々が目指す情報管理システムの実現方法

- SSoT をどのように実現させたか？

我々が目指す情報管理システムの実現

✓SSoTの実現方法

- 以下の要件を満たす情報管理システム AirOne を内製
 - 拡張性：管理・運用に必要なデータが全て集まっている
 - 機密性：必要なユーザだけが必要な情報にアクセスできる
 - 追跡性：誰が、いつ、何を設定したのかが追跡・復旧できる
 - 整合性：登録データが正である（実情報と差異がない）と信頼できる

2020/01 に OSS として公開。絶賛開発継続中

- <https://github.com/dmm-com/airone>



我々が目指す情報管理システムの実現

✔SSoTの実現状況 - 情報の集約

- 導入開始（旧システムからのデータ移行後）から現在までの情報規模の変化

2018-11-01 時点

2022-07-13 時点

スキーマ数

(e.g. Server, L2 Switch, ...)

39

x2.92

114

属性数

(e.g. サポートID, 購入費用, ...)

151

x5.87

886

インスタンス数

(e.g. srv0001, sw0001, ...)

147,857

+26,426

174,283



SSoT による運用効率化の現状

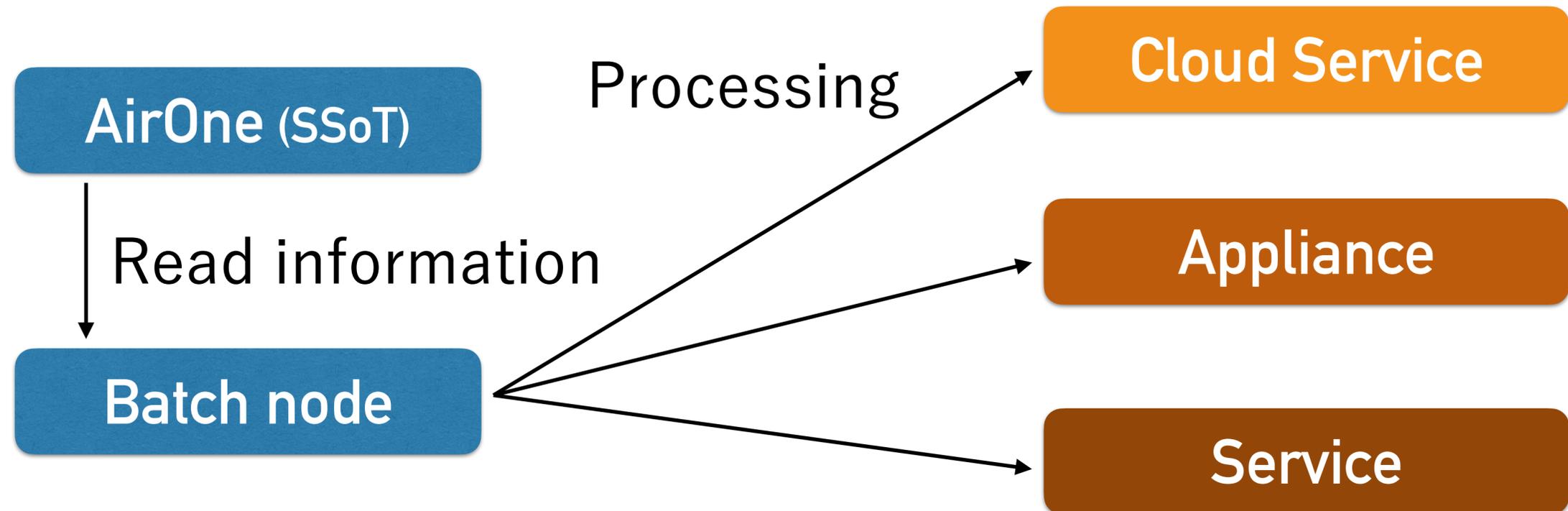
- AirOne を活用したことによる運用の変化

SSoTと運用効率化の現状

✓運用効率化の状況

- サービスのポリシーとメカニズムの分離

サービスが SSoT の設定パラメータを参照することで、柔軟なサービス運用を行う

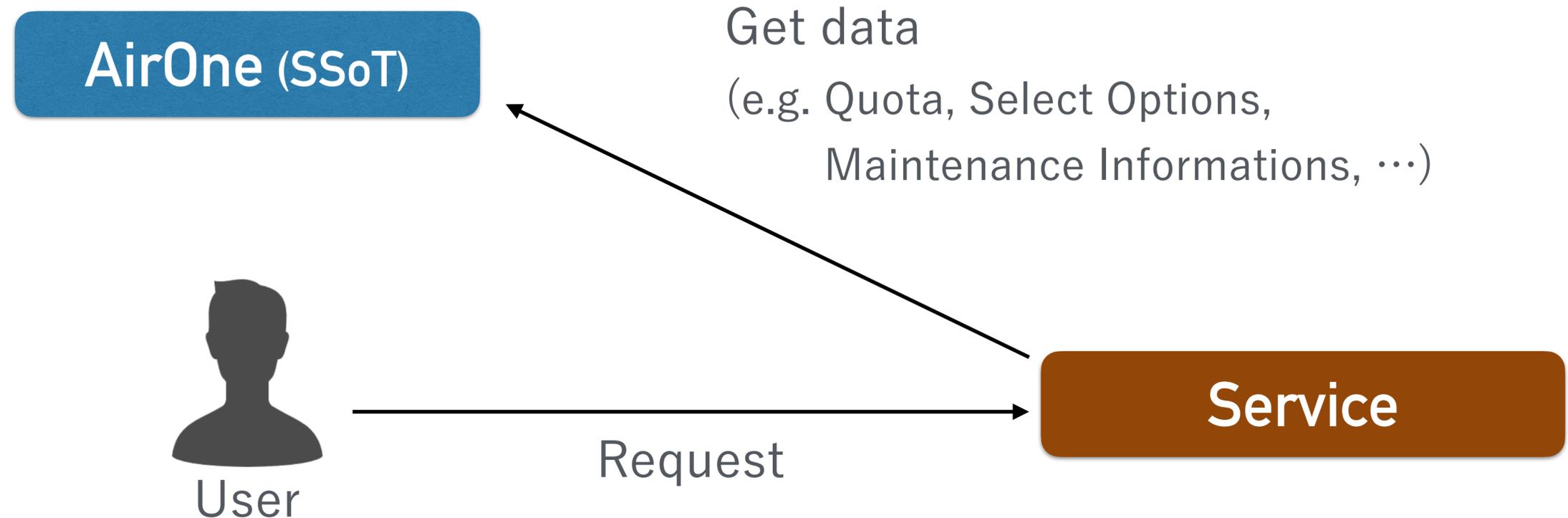


SSoTと運用効率化の現状

✓ 運用効率化の状況

- サービスのポリシーとメカニズムの分離

サービスが SSoT の設定パラメータを参照することで、柔軟なサービス運用を行う



SSoTと運用効率化の現状

✓運用効率化の状況

- 用途・運用毎にビューをカスタマイズ（ポリシー分離の応用）

用途・ケース別にビューをカスタマイズすることで、細かなニーズに対応 (e.g. IPAM, DCIM)



物理アプライアンスの配置情報



SSoTと運用効率化の現状

✓運用効率化の状況

- 用途・運用毎にビューをカスタマイズ（ポリシー分離の応用）

用途・ケース別にビューをカスタマイズすることで、細かなニーズに対応 (e.g. IPAM, DCIM)

Ports and Links

I/F名	I/Fタイプ	ラベル	備考	対向エントリ	対向エントリの I/F
IPMI	1000Base-T				ge-0/0/17
PCI2-1	10GBase-T	1			xe-0/0/1
PCI2-2	10GBase-T	2			
PCI3-1	10GBase-T	1			xe-0/0/40
PCI3-2	10GBase-T	2			10GE 1/0/3
オンボード1	1000Base-T	1			
オンボード2	1000Base-T	2			ge-0/0/3
オンボード3	10GBase-T	3			
オンボード4	10GBase-T	4			

IP addresses

OS interface	IP address	Network	VLAN
IPMI			
PCI2-1.1263			
PCI2-1.1506			
PCI3-1			
PCI3-2			
オンボード2			

a-01 ステータス	
a-02 メーカー・機種	
a-03 CPU	
GPU	
a-04 ディスク構成	
a-05 メモリ	
a-06 サイズ	
b-01 OS	
b-02 ライセンス	
b-03 Hypervisor	
b-04 RAID情報	
b-05 大分類	
b-06 中分類	
b-07 小分類	
b-08 バックアップ	
b-09 部門分類	
b-10 MySQLライセンス	
b-11 請求先	
c-01 Inf担当チーム	
c-02 Sys担当チーム	
d-01 リース会社	
d-02 リース番号	
d-03 リース開始日	
d-04 リース完了日	

物理アプライアンスの物理・論理ネットワーク、管理・運用情報



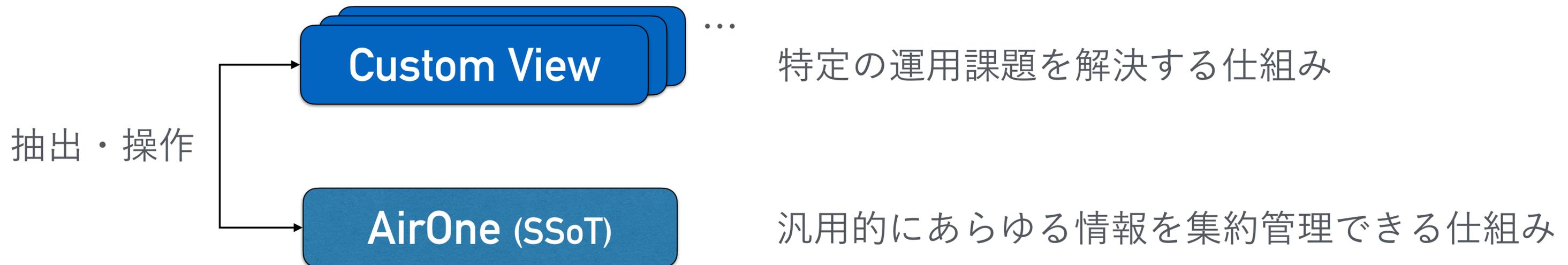
まとめ

まとめ

✓我々が目指す情報管理システム

特定の運用課題に依らない、以下を実現する情報管理システム

- 情報が保存・取得できる状態が保たれている
- 保存された情報の整合性が保たれている
- 保存された情報に対する適切な権限が保たれている



(<https://github.com/dmm-com/airone>)