

通信および設定履歴にもとづく ネットワーク運用の自動化

情報通信マネジメント研究会 2017年1月

大阪市立大学 大学院工学研究科

阿多 信吾

ata@eng.osaka-cu.ac.jp

(共著者)

吉田直樹 (大阪市立大学)

中山裕貴、林經正 (ボスコ・テクノロジーズ)

発表の趣旨

□ 将来的な ICT インフラの管理運用とは？

- 現状と課題
- 目的

□ 提案する自動化フレームワーク

- 概要
- 個別機能

□ 検証

- 環境

□ 今後の課題

ICT インフラストラクチャの管理運用

□ インフラ全体の管理の必要性

□ ネットワーク、計算機資源が密接に関連

- 仮想化、プライベートクラウド構築
- ネットワーク機器のソフトウェア化
- NFV (Network Function Virtualization)

□ インフラ規模の大規模化、複雑化

- 端末数の増加 (PC 以外の組み込み機器、M2M)
- アプリケーションの多様化

□ 対策すべき脅威の高度化

- 攻撃の巧妙化
- 潜在的リスクの増加

社会インフラとしての情報通信基盤

□ 管理運用技術が重要な鍵

□ インフラの安定動作

- 障害の早期検出
- 状況の可視化
- 将来に向けたプロビジョニング

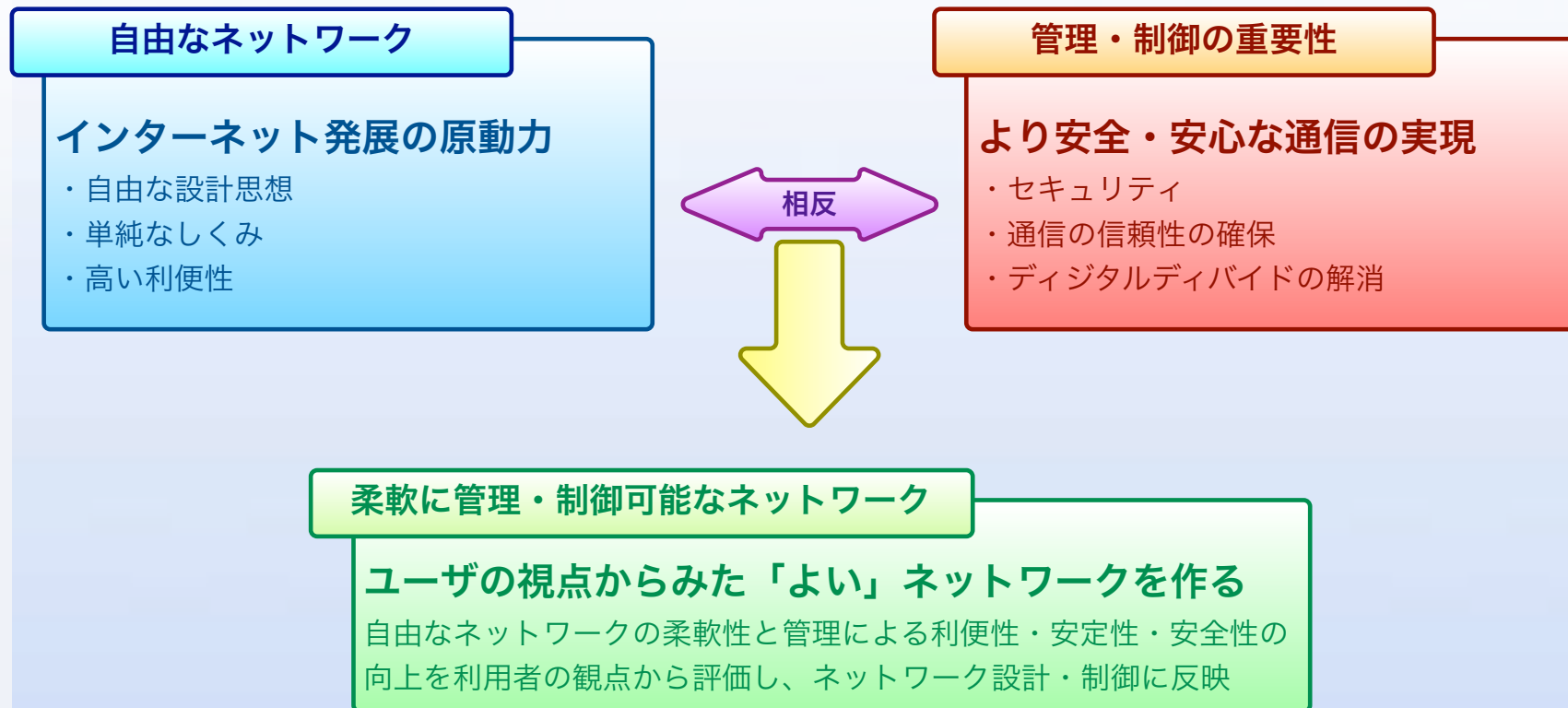
□ インフラの安全性向上

- セキュリティ対策（攻撃検知、防御）

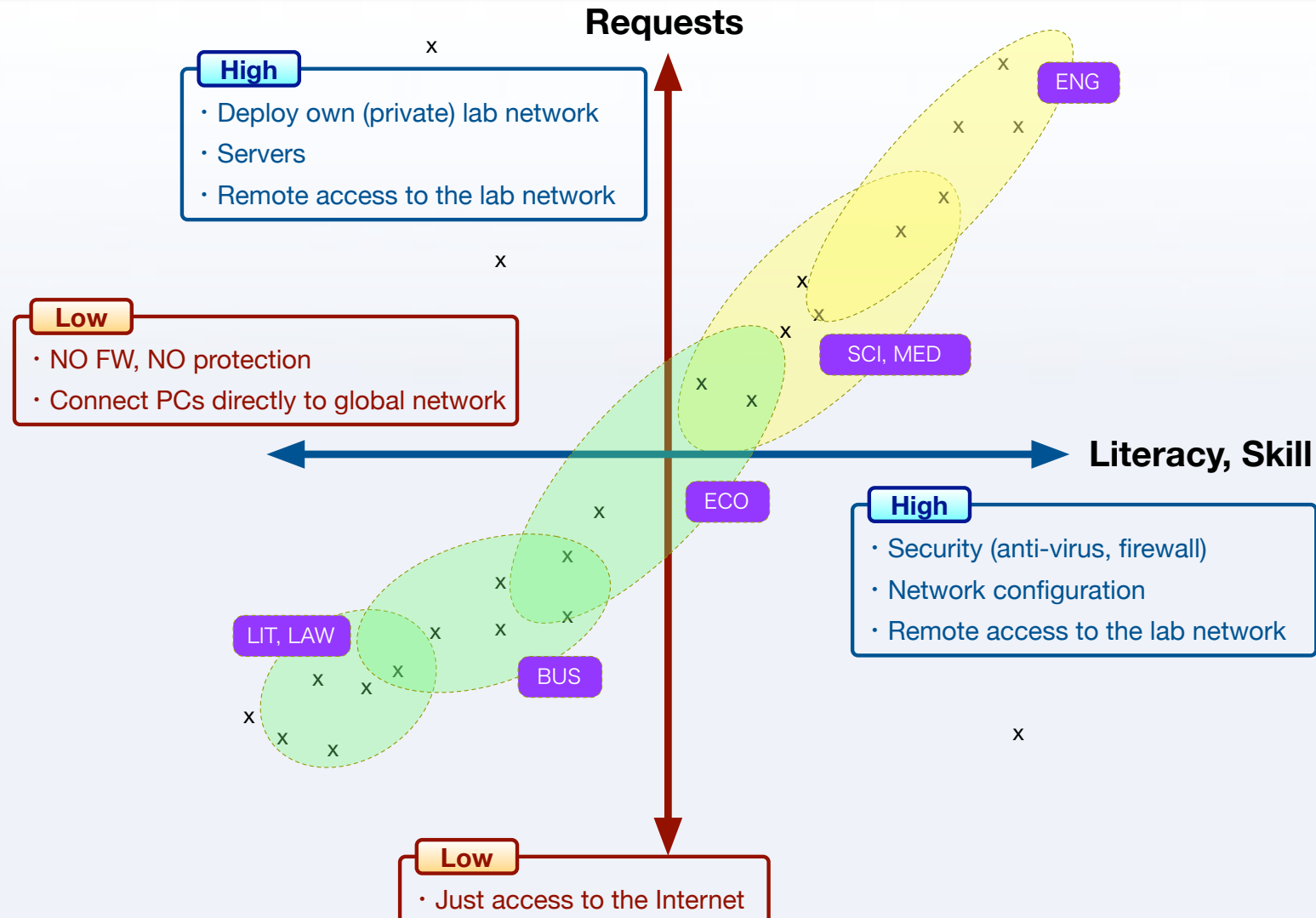
□ 利用状況に応じた適切な制御

- パーソナライズされた制御ができるか？
- 個人の能力に応じた制御

パーソナライズ制御



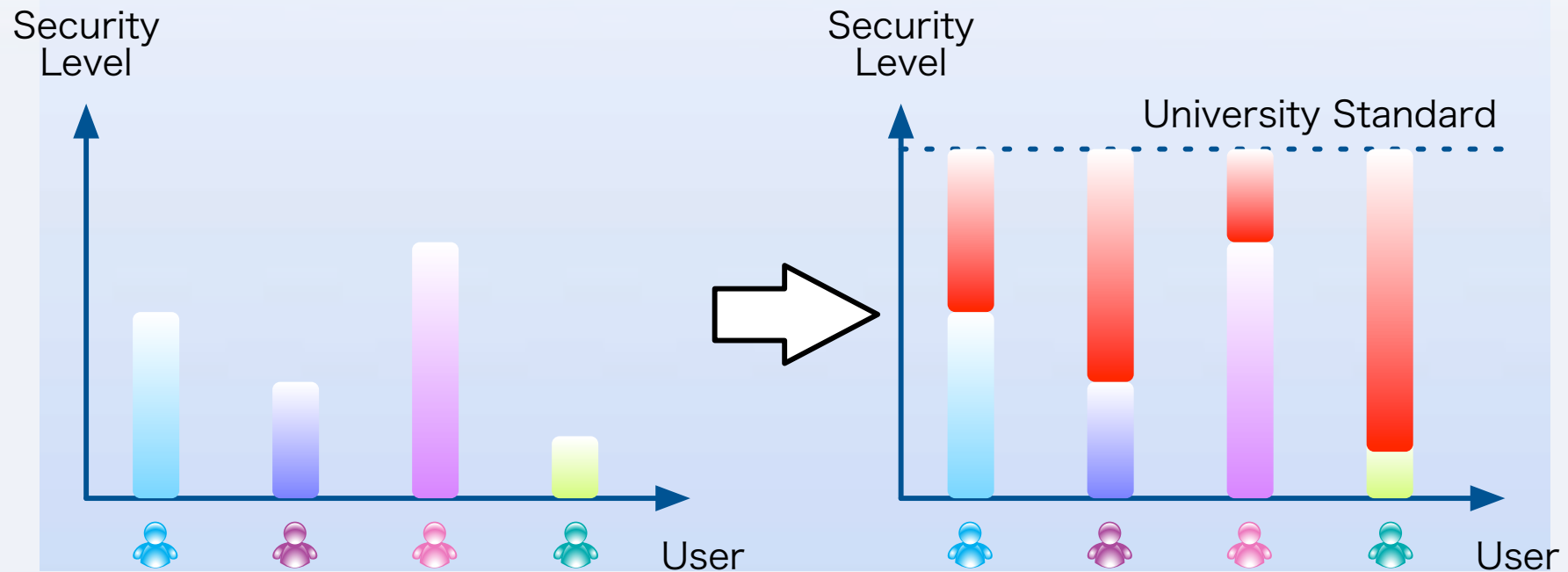
スキルと要望分布（例）



パーソナライズ制御の目的（例）

□セキュリティの向上

- 個人の能力向上（教育、研修等）
- ソフトウェアで補間（クライアント、**インフラ**）



ICT インフラ管理運用の現状課題

□ 大規模インフラの一元的な管理

- ネットワーク機器、サーバ等

□ 柔軟かつ迅速なポリシ設計と適用

- 既知の通信だけでなく将来における未知の通信、サービスへの応用
- 速く激動する技術進化への追従
- 「守りの IT」化

□ 属人的な管理運用

- 適切な判断と処理には豊富な経験を有する技術者が必要不可欠
- セキュリティは高度な専門的知識を要する

管理運用の自動化

□ 定常的に繁忙となる業務負担の軽減

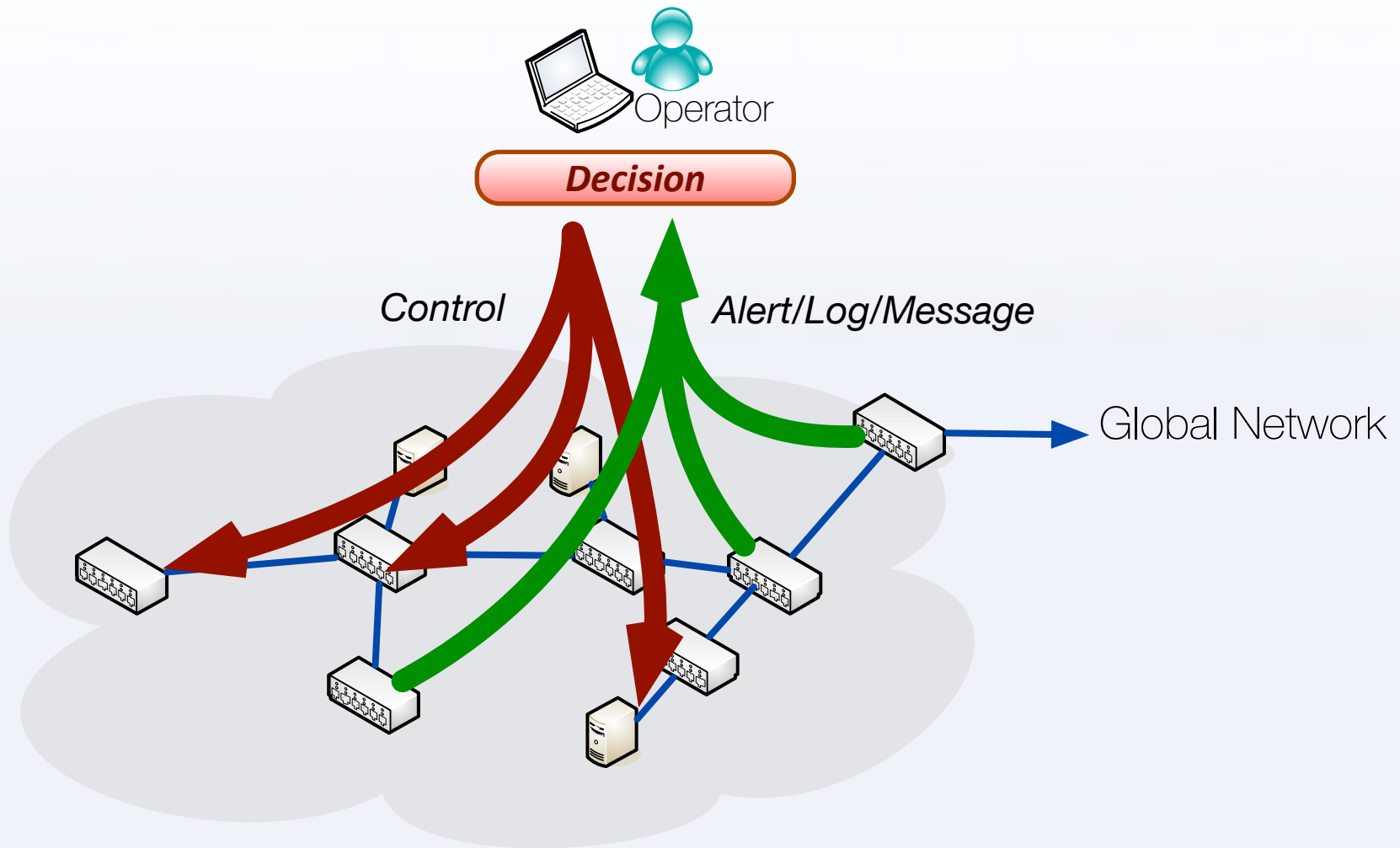
- ルーチン化された処理
- 対応が定型化されているインシデント
- より高度な業務に人的リソースを注力

□ 完全自動化がよい？

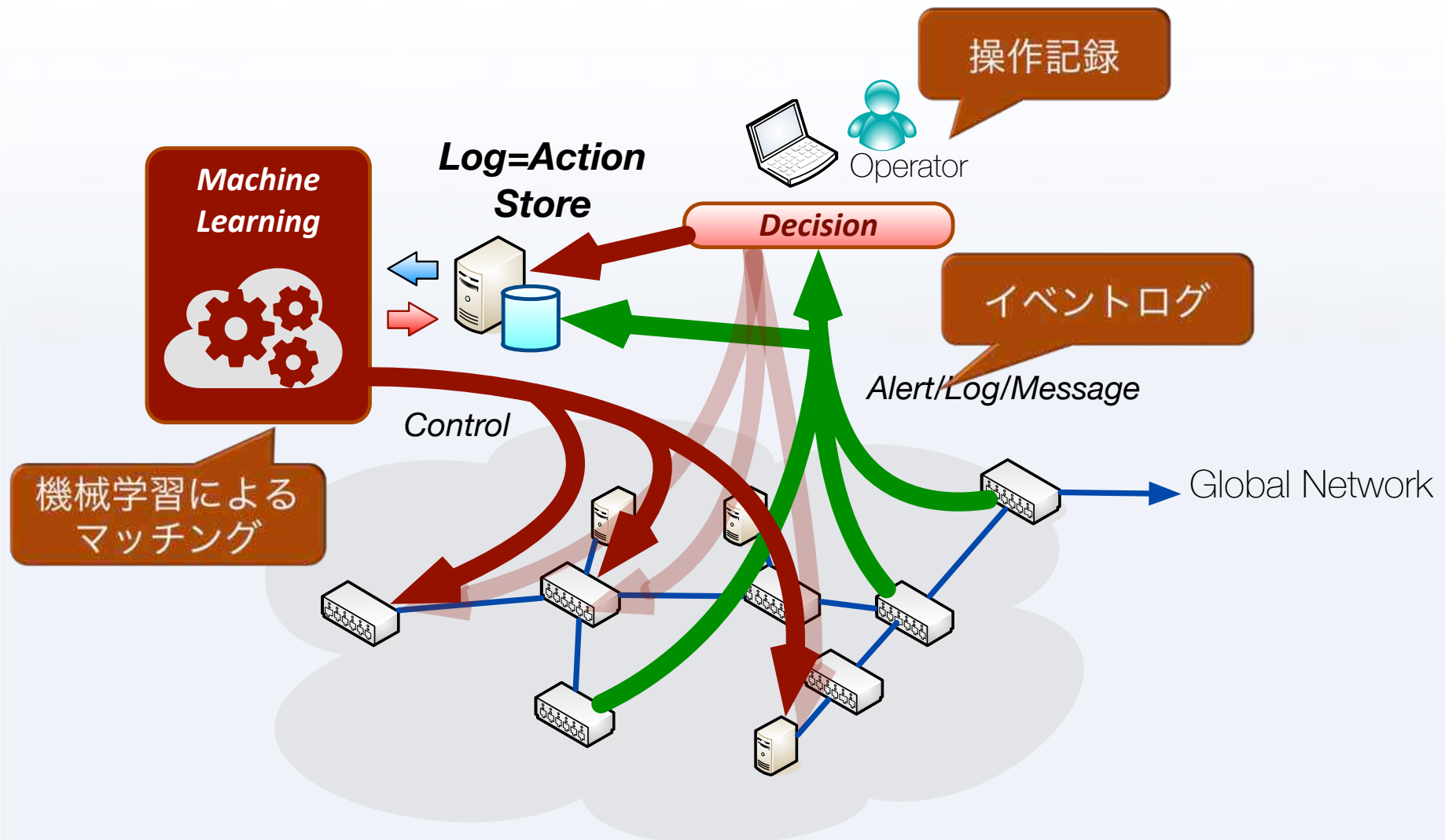
- インフラのブラックボックス化、ベンダロック
- （将来的な）技術者の不足

管理運用者の人材育成も可能な自動化フレームワーク

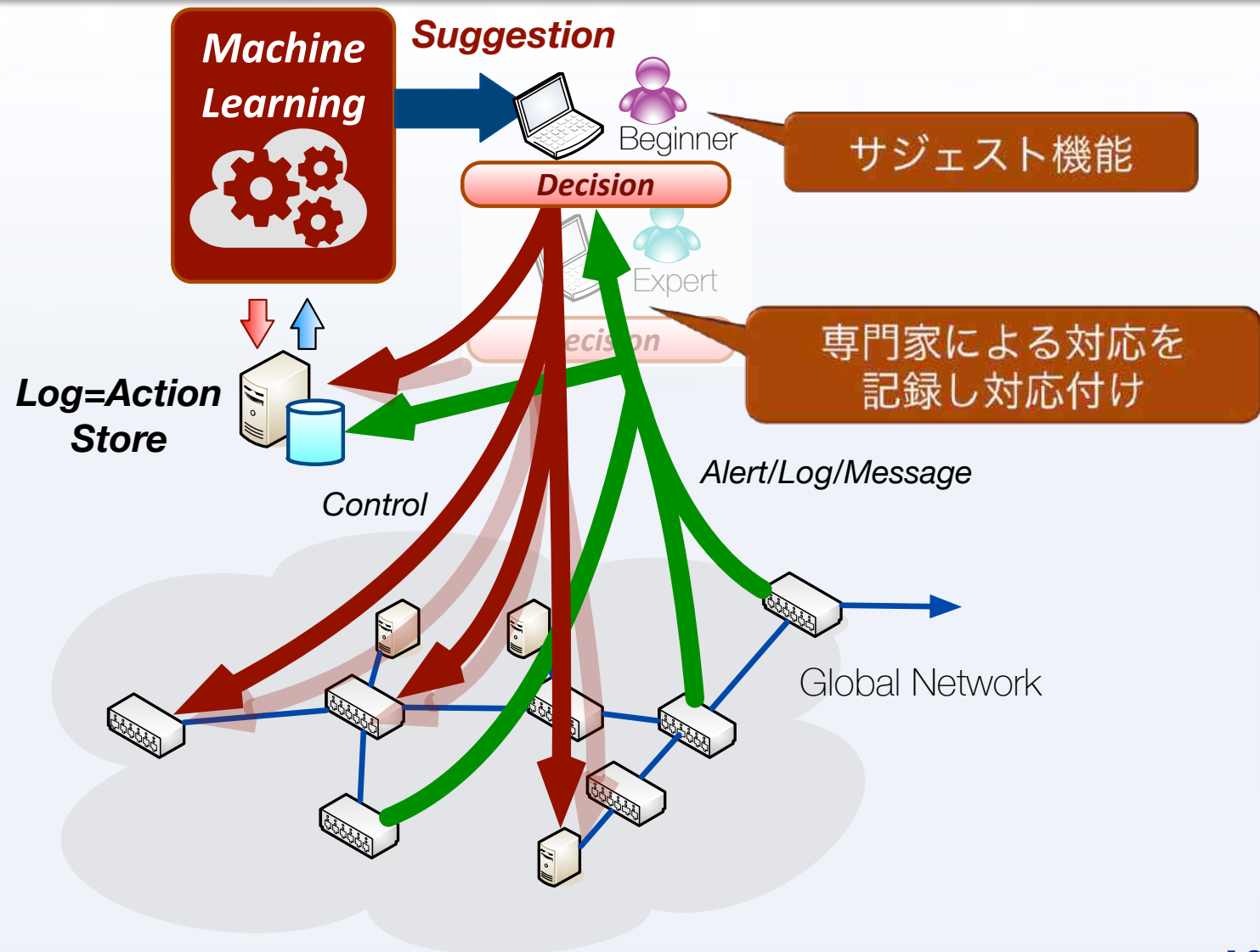
一般的な管理運用モデル



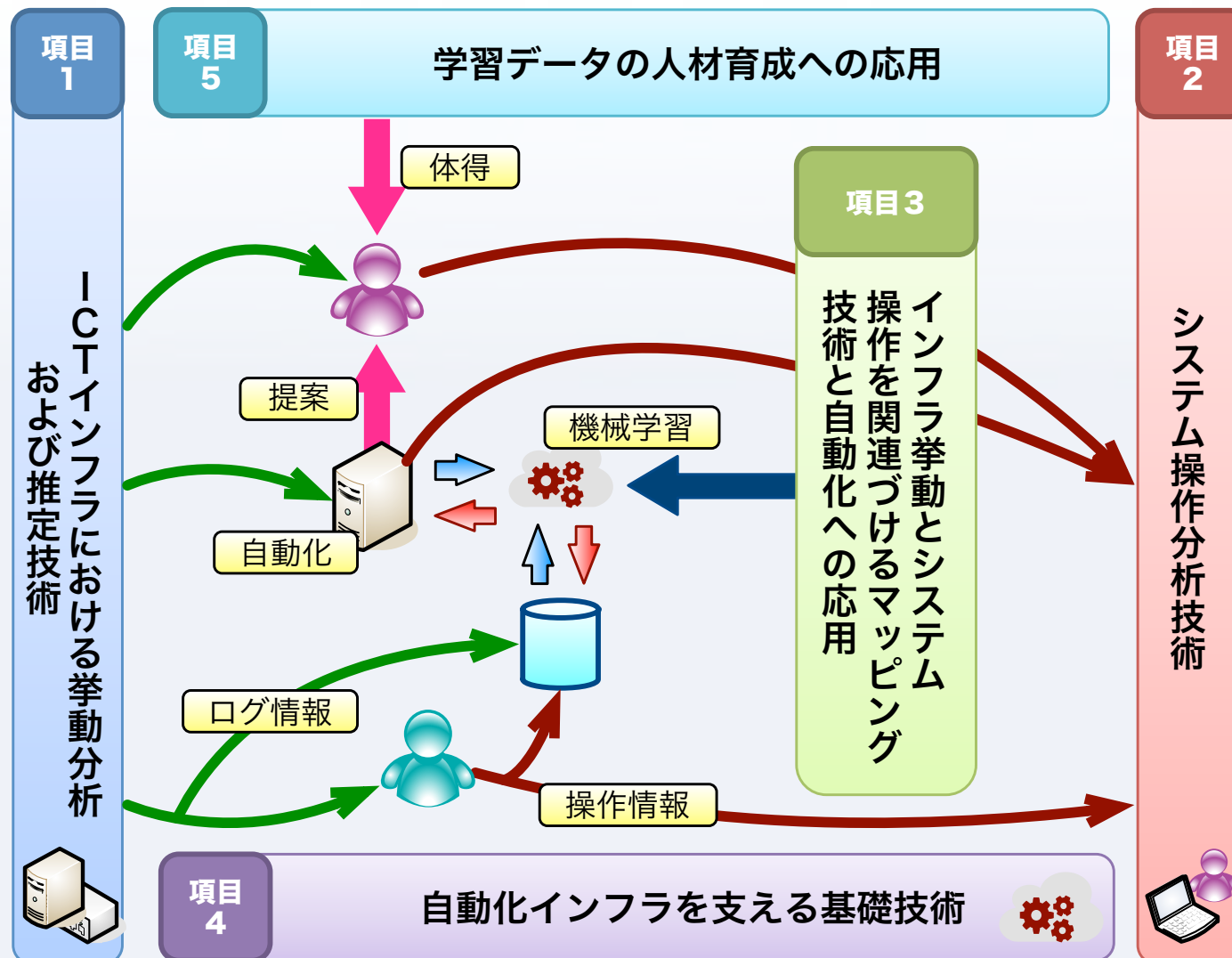
提案モデル（概要）



人材育成モデル（概要）

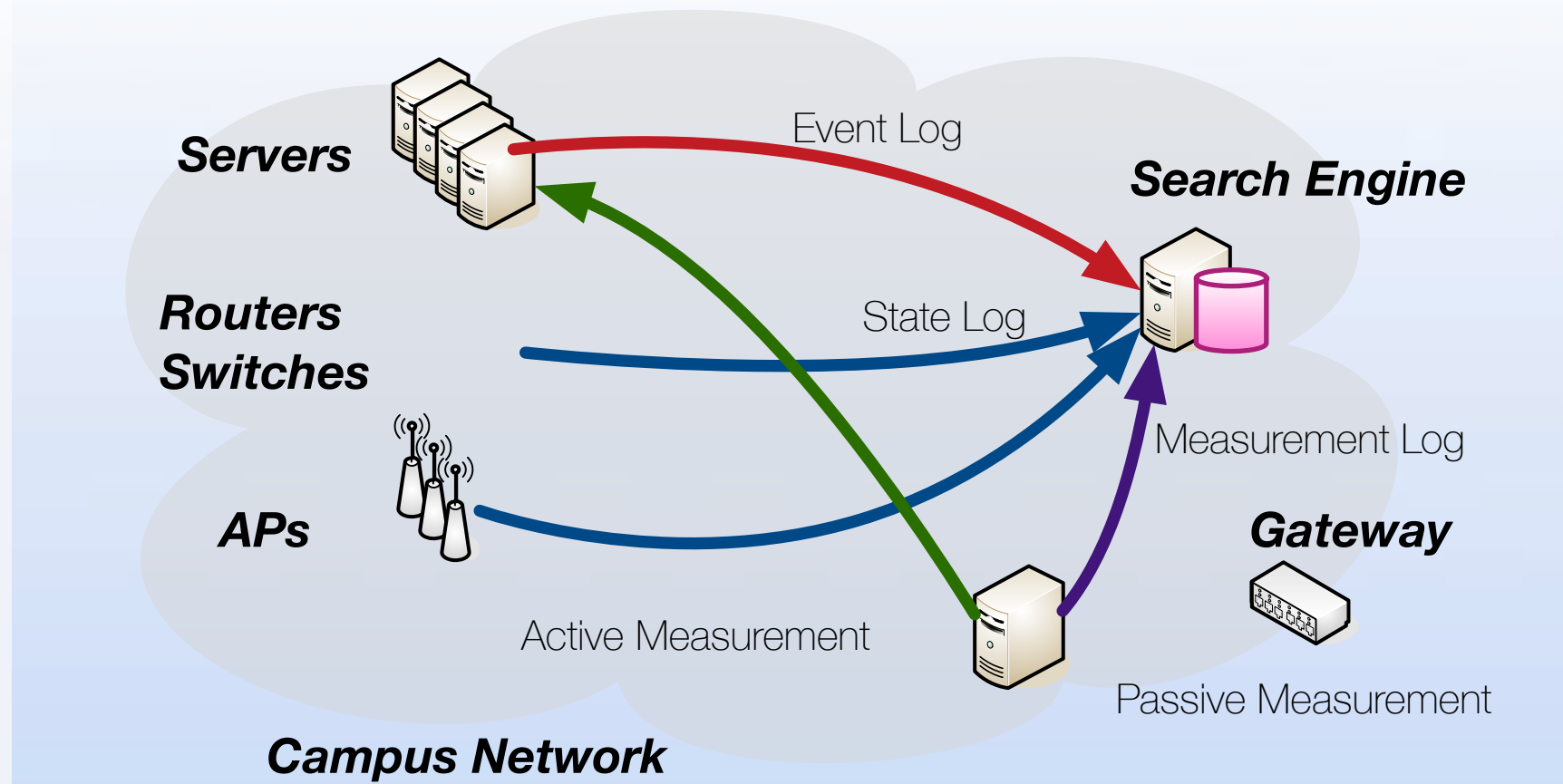


提案モデルにおける課題



ICT インフラの状況把握

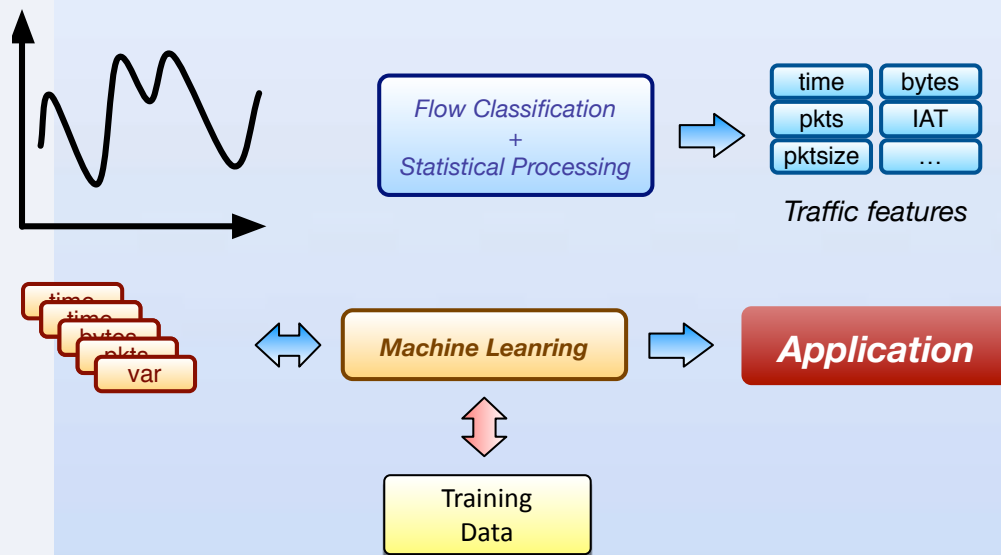
□ 一元的に情報収集、分析可能なフレームワーク



機械学習による複数ログの関連性分析

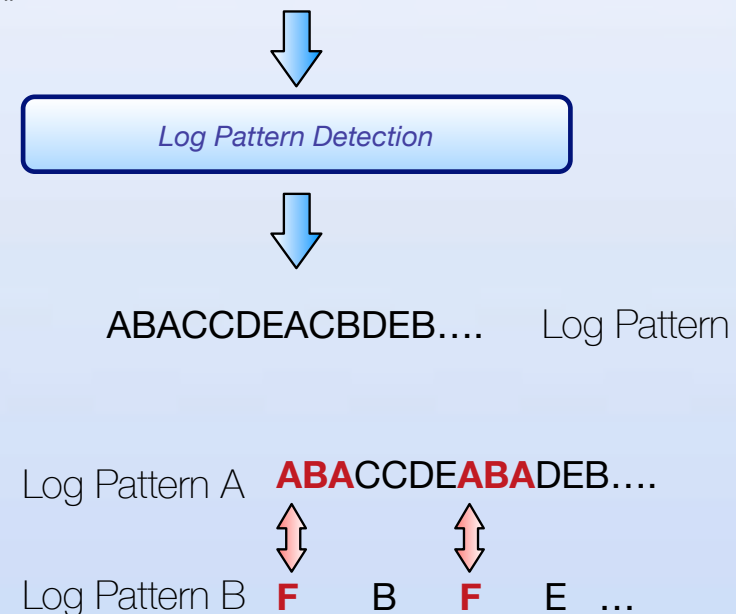
パターンマッチングの応用により複数のログにおける相関性を検出

- 単一の機構に依存せず複数の機構の相関性により総合的に判断

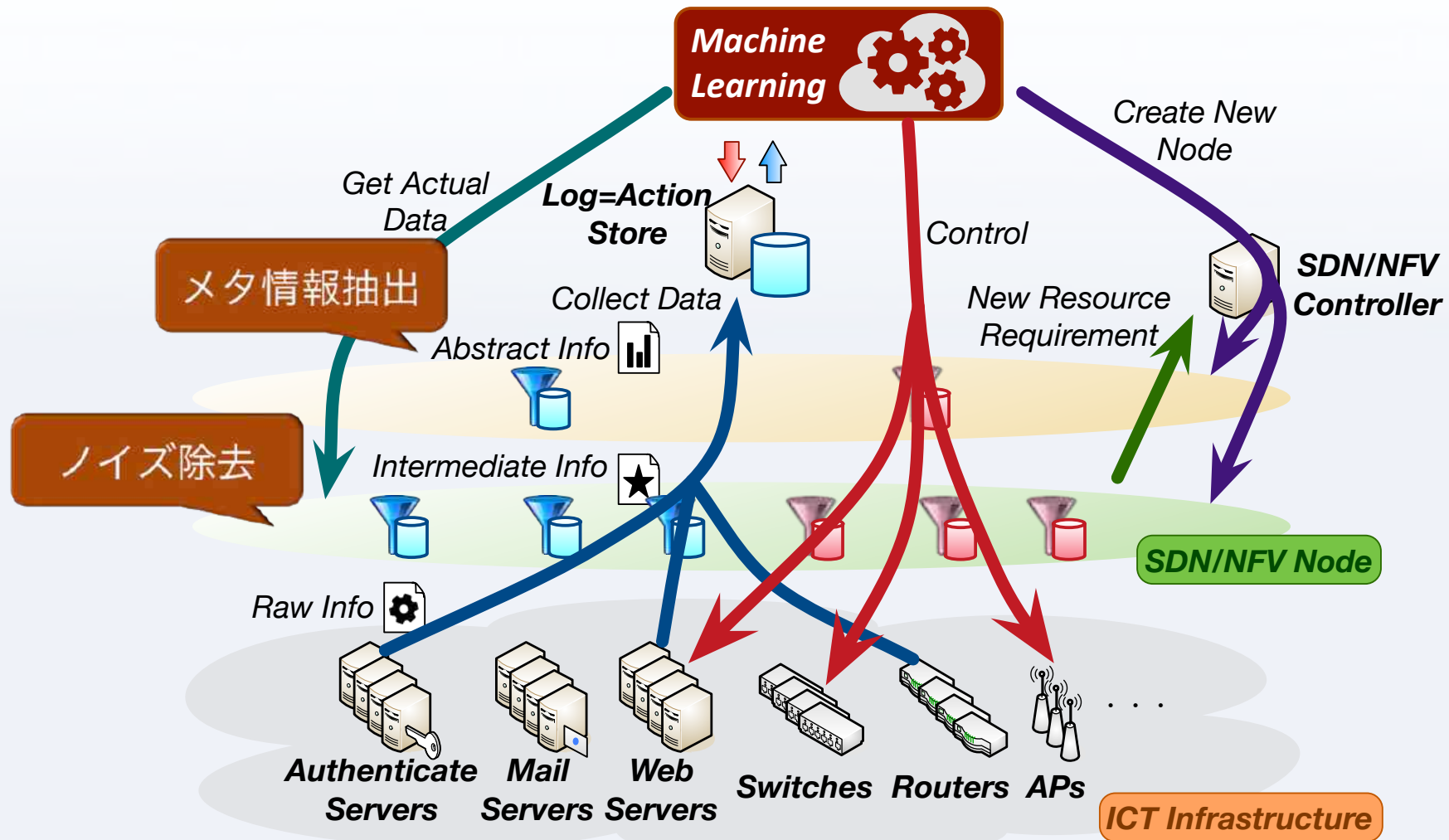


```
Oct 29 20:04:54 atimcrt AOUDownloadCount[4959]: ERROR(AOUDownloadCount.m)368L(
Error:AOUDownloadCount::readDownloadCountInfo:get DownloadCountInfo failed.
Oct 29 20:04:54 atimcrt appleeventd[58]: SecTaskLoadEntitlements failed error=22
Oct 29 20:09:04 Safari[848]: tcp_connection_tls_session_callback_write_block_invoke_v34 error 22
tcp_connection_tls_session_callback_write_block_invoke_v34 error 22
Oct 29 20:09:16 atimcrt syslogd[47]: ADL Sender Statistics
Oct 29 20:10:46 atimcrt com.apple.backupd[4957]: Finished scan
Oct 29 20:10:47 atimcrt com.apple.backupd[4957]: Saved event cache at /Volumes/1394HD/Backups.backupdb/
atimcrt/2015-10-29-200446.inprogress/DEDA810-68F4-44B0-83A9-36C8610C28E2/.ODP56843-C907-38A5-B223-
CFFA92DAA6AF.eventdb
Oct 29 20:10:47 atimcrt com.apple.backupd[4957]: Not using file event preflight for Macintosh HD
Oct 29 20:11:56 atimcrt lsd[216]: launchservices: Could not store lsd-identifiers file at /private/var/
db/lsd/com.apple.lsd.schemes.plist
Oct 29 20:12:10 --- Last message repeated 1 time ---
Oct 29 20:14:12 atimcrt Mail[2629]: Skipping STATUS for INBOX because CHECK failed with error: Error
Domain=MIMEMailErrorDomain Code=1029 "C:\IMAPConnection: 0x7fba4695a4f0" (Disconnected) account:
<MFIMAPAccount: 0x7fba41c7fb70> skington01@yahoo.co.jp imap.mail.yahoo.co.jp (85944373-639D-4D82-
8D24-8C7888D3BDB) [Disconnected mailbox=受信 - Yahoo! Japan] lost connection to socket"
UserInfo=(NSLocalizedDescription=C:\IMAPConnection: 0x7fba4695a4f0" (Disconnected) account: <MFIMAPAccount:
0x7fba41c7fb70> skington01@yahoo.co.jp imap.mail.yahoo.co.jp (85944373-639D-4D82-8D24-8C7888D3BDB)
[Disconnected mailbox=受信 - Yahoo! Japan] lost connection to socket)
Oct 29 20:15:03 atimcrt AtokSyncHelper[4979]: objc[4979]: Class ATOKPathResolver is implemented in both /
Library/Application Support/JustSystems/ATOK 2014/Frameworks/ATOKDE.framework/Versions/A/ATOKDE and /
Applications/JustS
```

Log



階層的な収集・制御フレームワーク



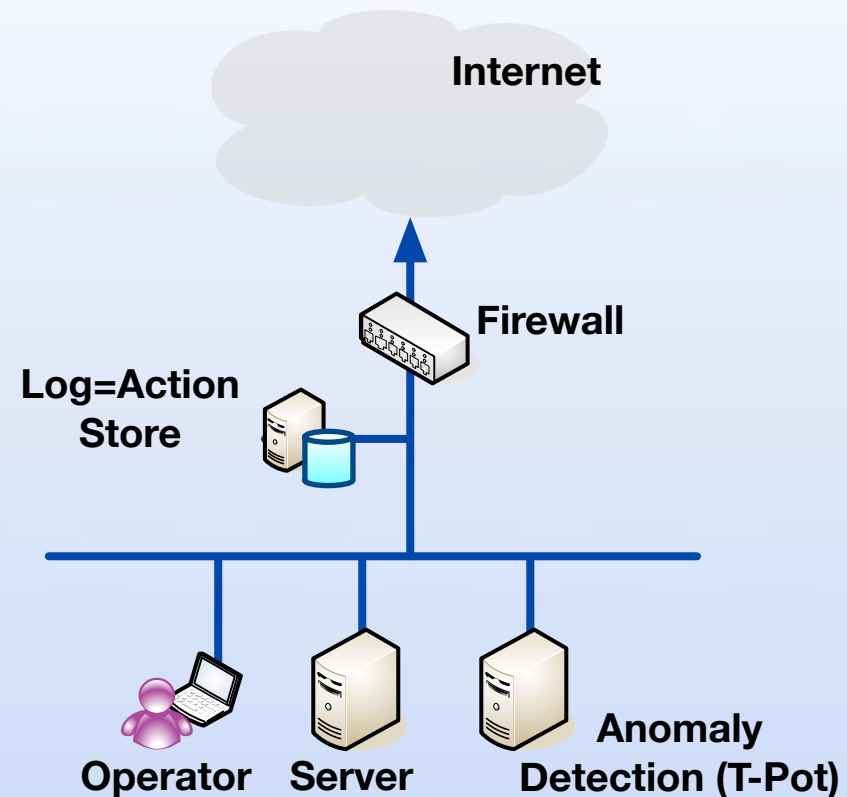
検証

□ 実験環境

- 異常検知装置
- 制御対象サーバ
- ファイアウォール
- 情報収集データベース

□ 使用ツール

- 異常検知：T-Pot
- データベース：ElasticSearch
- 操作記録収集：SMART-GW



動作状況



まとめと今後の課題

□ ICT インフラ管理運用の自動化に向けて

- 複数ログと操作記録情報の連結によるインシデント対応自動化
- サジェストによる管理者育成

□ 今後の課題

- 学習データの効率的かつ正確な収集
- 複数ログの相関性分析手法の精査
- ログのテンプレート化