AXIOLEによる
ネットワーク認証アカウント管理のご紹介

CAUA第7回合同研究分科会
ソリューションのご紹介

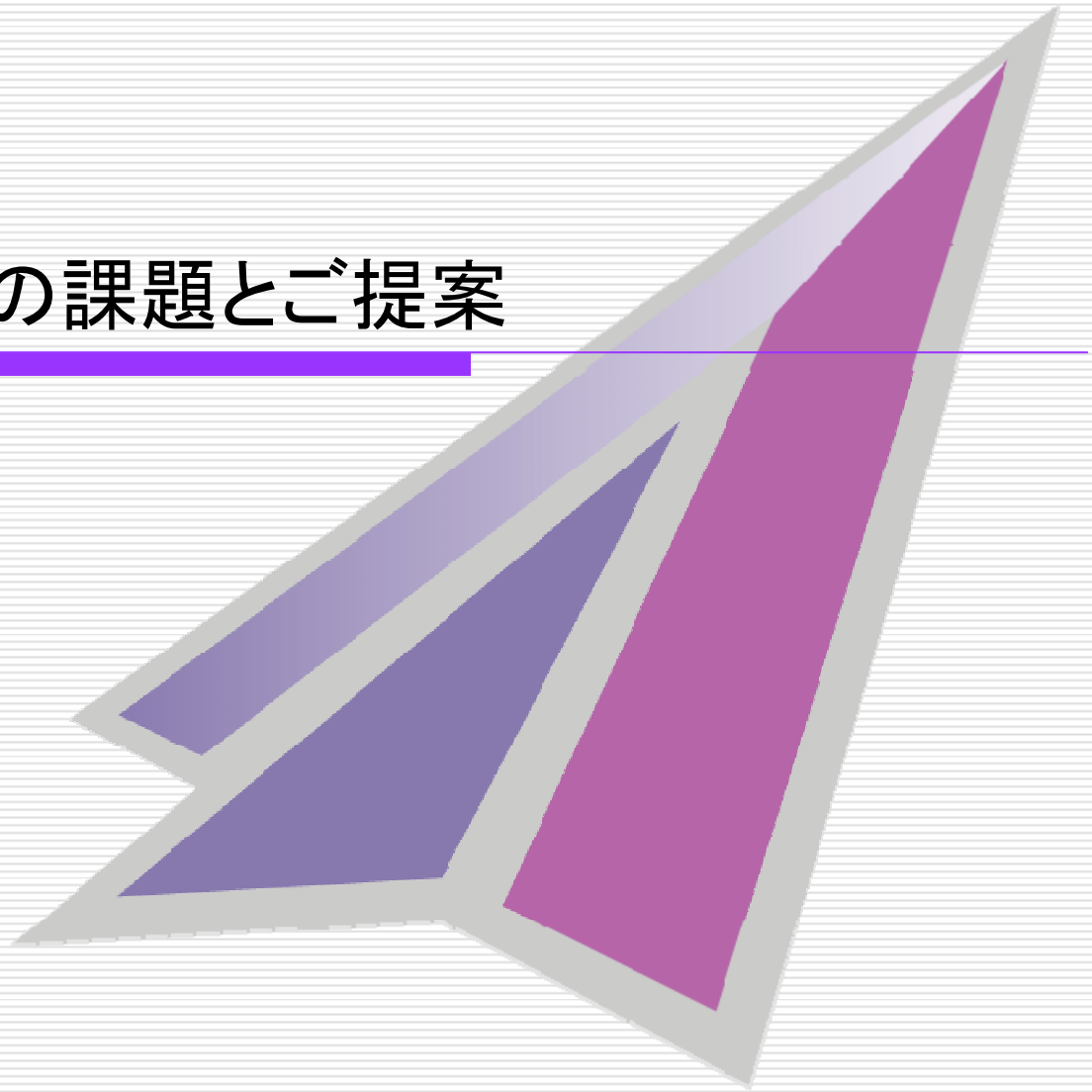
2008/10/24

株式会社ネットスプリング

Agenda

- アカウント管理の課題とご提案
- AXIOLEのご紹介
- 導入事例のご紹介

アカウント管理の課題とご提案



アカウント管理の課題1

- 分散するアカウント
  - ネットワークサービスの増加
  - 管理アカウントの増加

- 管理者の負担増
  - 年度毎など定期的なアカウント作成・削除
  - 不定期のアカウント作成・削除
    - 必要なアカウントが漏れなく作成できているか
    - 不要なアカウントが残っていないか
- 利用者の負担増
  - ユーザ名がサービスによって異なる
  - パスワードが覚えきれない
    - 管理者への問い合わせ・再発行の依頼⇒管理者の負担増
    - 安易なパスワードの設定・メモに残す⇒セキュリティリスク増
    - ネットワーク利用率の低下

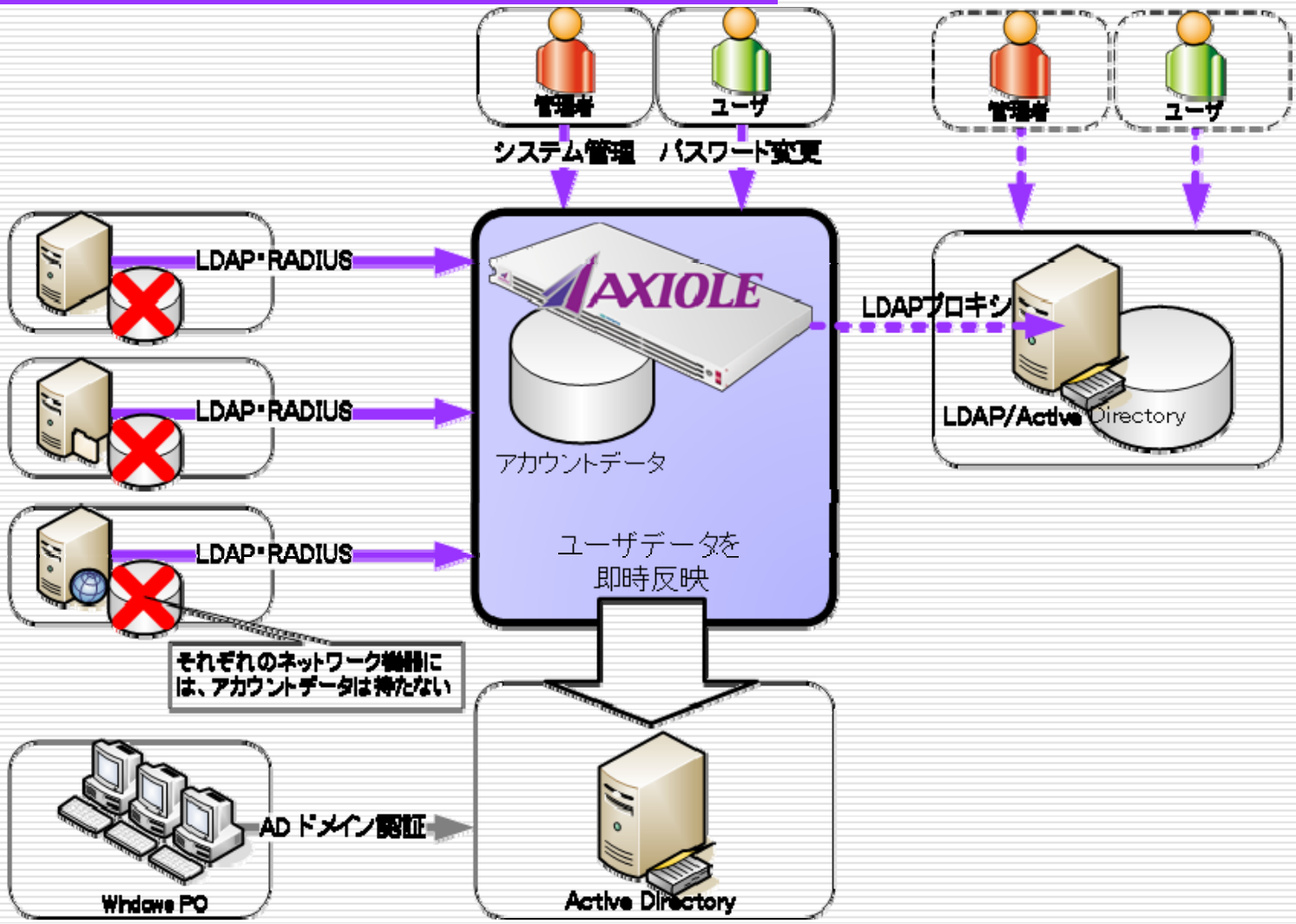
アカウント管理の課題2

- アカウントの一元化を検討

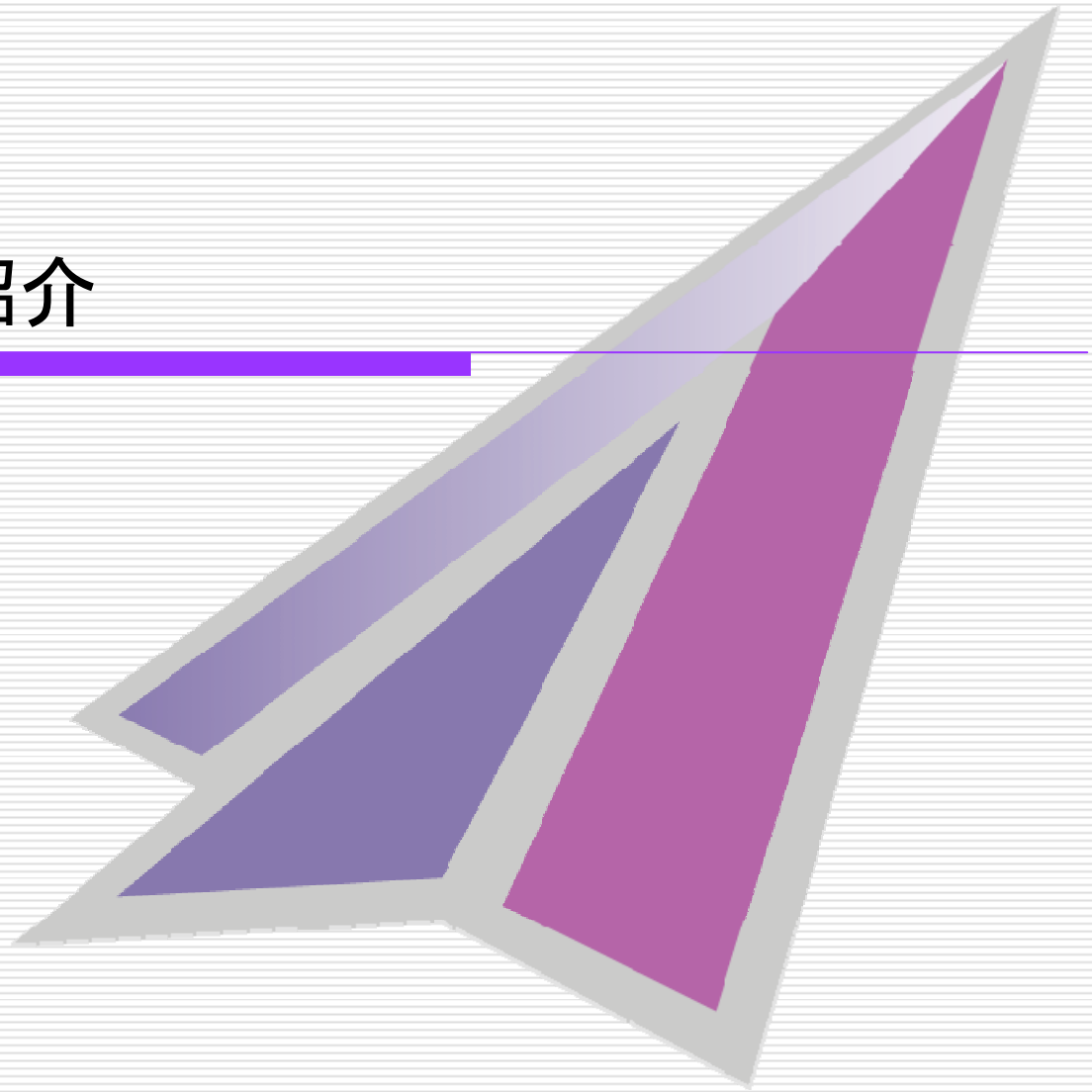
- LDAPの導入…しかし
  - 管理者がいない
  - 導入時の設計・環境構築＋作り込みが必要
  - アカウント情報のみを管理
    - ➔ 運用規模とコストが釣り合わない
  - 様々な情報を統合管理
    - ➔ 巨大なDB化⇒ネットワーク管理者から利用しづらい

- アカウント管理に特化した
- 専門的なスキルを必要とせず
- コストパフォーマンスのよい
- 認証アプライアンス「**AXIOLE**」のご提案

AXIOLEのシステム構成の概要



AXIOLEのご紹介



AXIOLEの特徴1

- ネットワーク認証に特化したアプライアンスサーバ
  - ➔ 必要最小限のアカウント情報のみ管理
- LDAP、RADIUS認証プロトコルに対応
  - LDAP over SSL対応
  - RADIUS認証（PAP、CHAP）対応
    ※IEEE802.1Xは2008年末対応予定
  - RADIUSアカウンティング対応
  - RADIUSによるMACアドレス認証をサポート
- 日本語WebUIによる管理
  - 設定・運用は全てWebUIから可能
  - LDAPの専門的なスキルは不要
  - 面倒なディレクトリの設計は不要
  - スキーマは定義済み
  - 充実したアカウント管理機能

AXIOLEの特徴2

- アカウント管理機能
  - ～10,000のアカウントをサポート
  - ユーザアカウントの管理のみを行う管理者ユーザ権限
    - アカウント管理を別の管理者にアウトソース
  - POSIX対応
  - 検索機能
  - マルチグループ機能
  - ライフタイム管理（アカウント有効期間の設定）
  - テキストファイルからのインポート／エクスポート機能
  - パスワード強度チェック
  - ➔ 大量のアカウントを効率よく管理

AXIOLEの特徴3

- 利用者向け機能もWebUIで提供
  - パスワード変更
  - パスワード再発行機能
  - → エンドユーザのユーザビリティを向上
  - → 管理者の負担軽減
- パスワード再発行機能
  - ユーザ名とパスワード再発行用のメールアドレス（事前に設定）によって本人確認を行い、そのメールアドレス宛てに再発行したパスワードを送信
  - 送信するメールは、管理者が編集可能

AXIOLEの特徴4

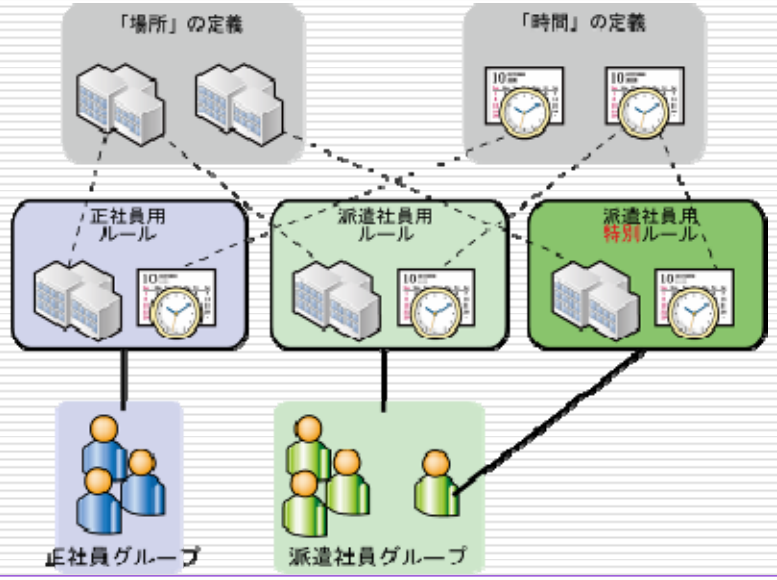
- 基本的な認証機能
  - LDAP
    - LDAP v2/v3
    - LDAP over SSL
    - Anonymous（匿名）Bind
  - RADIUS
    - PAP・CHAP（※IEEE802.1Xは2008年末対応予定）
    - ベンダ固有属性（VSA）
    - MACアドレス認証
      - ブラックリスト方式／ホワイトリス方式
      - ユーザ紐付け（持込PCなど）／共有（PC教室の端末など）
      - ユーザとは独立して管理

AXIOLEの特徴5

- 認証機能の拡張1
  - 無効ユーザ
    - ユーザ名とパスワードが正しくても認証を拒否することによって無効化する機能
    - ユーザは保存されたまま
  - ライフタイム
    - 有効期間以外はユーザ名とパスワードが正しくても認証を拒否することによって無効化する機能
    - ユーザは保存されたまま
    - 有効開始日時と終了日時をそれぞれ設定可能
    - 有効期間になると自動的にアカウントが有効になる
    - 有効期間外になると自動的にアカウントが無効になる
    - 例:2009/4/1 10:00から有効になるアカウントデータを2009/3中に予め作成しておく
    - 例:期間の決まっている契約社員のアカウントデータを契約期間に合わせて設定しておく

AXIOLEの特徴6

- 認証機能の拡張2
  - 認証ポリシー
    - 「時間」と「場所（IPアドレス）」定義の組み合わせに認証の許可・拒否を設定した「ルール」を作成して任意のユーザやグループに適用
    - ➔ 「人」の認証に加えて、「時間」＋「場所」による複合的な認証が可能
    - 例：正社員と契約・派遣社員／教職員と学生がそれぞれ利用可能なネットワーク機器の制御がAXIOLEの設定のみで可能



AXIOLEの特徴7

- 外部LDAPサーバ連携
  - 認証プロキシ機能
    - 外部のLDAP/Active Directoryの設定は変更不要
    - 外部のLDAP/Active Directory上のユーザ名・パスワードで認証
    - 「人」の認証は外部LDAPで行い、さらにAXIOLEの認証ポリシーを加えた認証が可能
  - Active Directoryへのデータ反映
    - AXIOLE上のアカウントデータをActive Directoryへ即時反映
      - 管理者によるアカウントデータの追加・変更・削除
        - ユーザ名、パスワード、無効状態、姓名、メールアドレス、AD上のプロファイル情報、AD上の所属グループ
      - ユーザによるパスワード変更
        - パスワード
    - ➔ **アカウントの管理操作をAXIOLEで一元化**

AXIOLEの特徴8

- パスワードポリシー
  - パスワード強度の設定パスワード設定時に即時チェック
    - 脆弱なパスワードが保存されることを防ぐ
    - パスワード長や必要な文字種別などの設定が可能
    - パスワード辞書ファイルによるチェックが可能
    - ➔ **脆弱なパスワードの保存を排除**
  - 長期間パスワードが変更されていないユーザの管理
    - 一定期間パスワードを変更していないユーザを抽出
    - さらに、抽出したユーザに一斉メール送信
  - ➔ **パスワード管理の負担を軽減**

AXIOLEの特徴9

- システム関連
  - ログ
    - 認証ログ
      - 「いつ」「だれが」「どこから」「認証に成功（失敗）」したか
      - 失敗した原因（パスワード間違い、ポリシー不適合など）
    - 操作ログ
      - 「いつ」「だれが」「どこから」「どのユーザ情報」の「どの操作（作成・更新・パスワード変更・削除）に成功（失敗）」したか
    - RADIUS アカウンティングログ
    - 各々最大90世代（≒日）保存
    - PCへのダウンロードが可能
    - 外部syslogサーバへの転送が可能（RADIUSアカウンティングログは除く）
  - SNMP
  - RAID-1によるミラーリングによってデータを保護
  - AXIOLE 2台による冗長化が可能

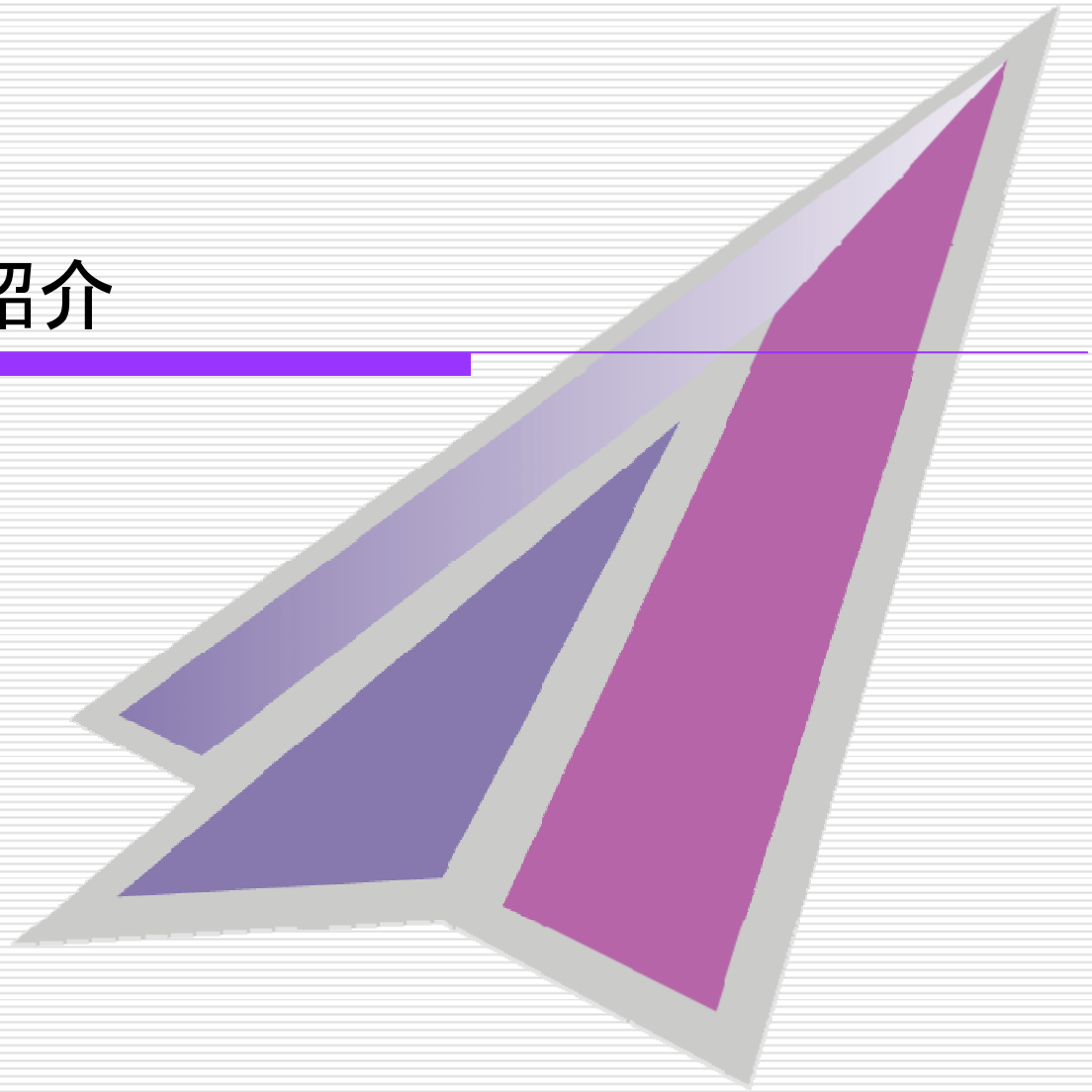
AXIOLEの特徴10

- LDAPスキーマオプション（オプション機能）
  - LDAPサーバの機能強化する2つの機能を提供
    - アカウント情報に任意のオブジェクトクラスおよび属性型を追加可能
    - LDAPプロトコルを介して、アカウント情報の追加・更新が可能
    - ➔ **AXIOLE標準のアカウント情報だけでは利用できないLDAP機器からも利用可能に！**
    - ➔ **LDAPを活用した、より高度な利用が可能に！**
    - LDAPプロキシとの併用によって、外部LDAPのスキーマ定義を変更することなく、AXIOLEにスキーマを追加して、外部LDAPにはない属性を用いた認証が可能

最新情報

- Mirapoint社メールアプライアンス製品への正式対応をプレスリリース（2008/08/27）
- ファームウェアVer.1.3.1リリース（2008/10/15）
- ファームウェアVer.1.4.0（仮）2008年末リリース予定
  - IEEE802.1X対応

導入事例のご紹介



S大学様の事例－概要

規模	ユーザ数：13,000（カスタム） AXIOLE 2台で冗長化
用途	全学生・教職員の認証サーバ
主なLDAP・RADIUS機器	□Postfix（SPAM対策。受信メールの宛先ユーザの有無をチェック） □SquirrelMail（Webメール） □Moodle（eラーニングCMS） □RHLE4 and 5、CentOS5、Solaris10（POSIX認証） □ETERNUS NR1000F（富士通社製ファイルサーバ） □FEREC（弊社 認証GWアプライアンス）、その他
その他	□NIS、LDAP、AD、RADIUSが混在していた環境からのリプレイス ■アカウントの同期が困難で、反映に時間がかかっていた ➔AXIOLEとADに集約 ➔ADとリアルタイムに同期 ■パスワードの強度チェックに手間がかかっていた ➔パスワード保存時にチェック→管理負担減 □リプレイス時には約12,000のアカウントを数時間で移行 ■/etc/passwd、/etc/shadowから移行 ■既存のアカウントは、元のパスワードのまま移行

S大学様の事例ー移行前のアカウント同期について

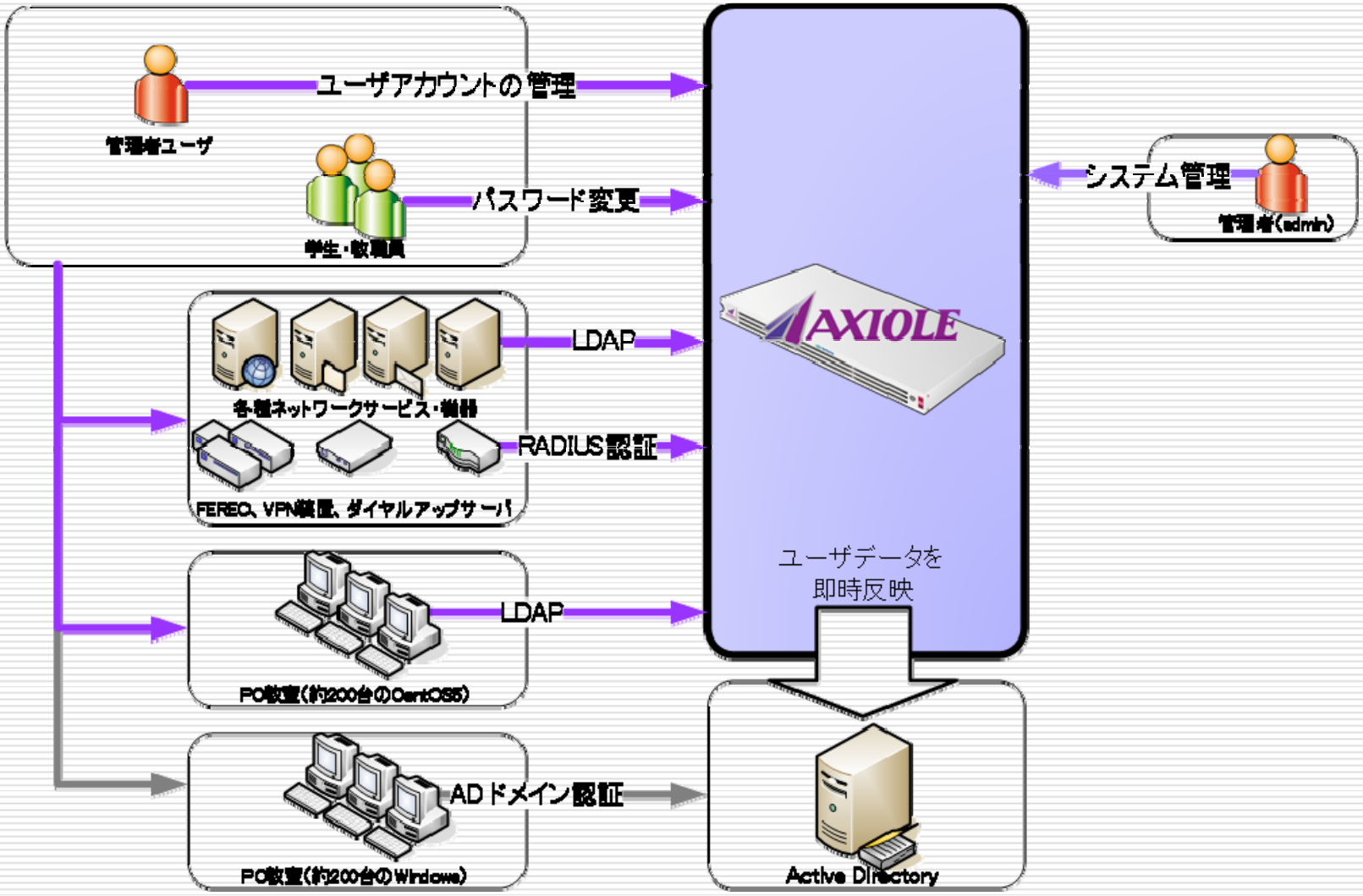
- NIS、LDAP、ADでアカウントの同期、RADIUSはNISを参照
  - スルーPASS(富士通北陸システムズ製)を使用してNISーADを同期
    - スルーPASSはLDAPとの同期ができないため、スクリプトを自作
      - 定期的にNIS→LDAPの反映を実行
- パスワード強度チェック自作スクリプトを定期的に実行
  - 週に1回程度実行
  - 脆弱と判断したパスワードのユーザにはその都度メールを送信

- もっと簡単に同期できないか
  - LDAPとADで簡単にアカウントの同期ができないか
  - NISはそろそろ必要ない
- より柔軟かつ手軽にパスワード強度のチェックが行えないか

S大学様の事例ーアカウントの移行

- 移行の条件
  - 移行後にも移行前のパスワードが使用できること
  - 移行時に「姓」「名」「メールアドレス」などのデータ（移行前のActive Directory上のデータ）も追加すること
- 以下の方法で移行
  1. 移行前のSolarisから/etc/passwd、/etc/shadowを入手し、AXIOLEにそのままアップロード
  2. AXIOLEからアカウントデータをLDIF形式でダウンロード
  3. ADからもアカウントデータをLDIF形式でエクスポート
  4. 2つのLDIFファイルをマージ（予めスクリプトを用意）
  5. マージしたLDIFファイルを再度AXIOLEにアップロード

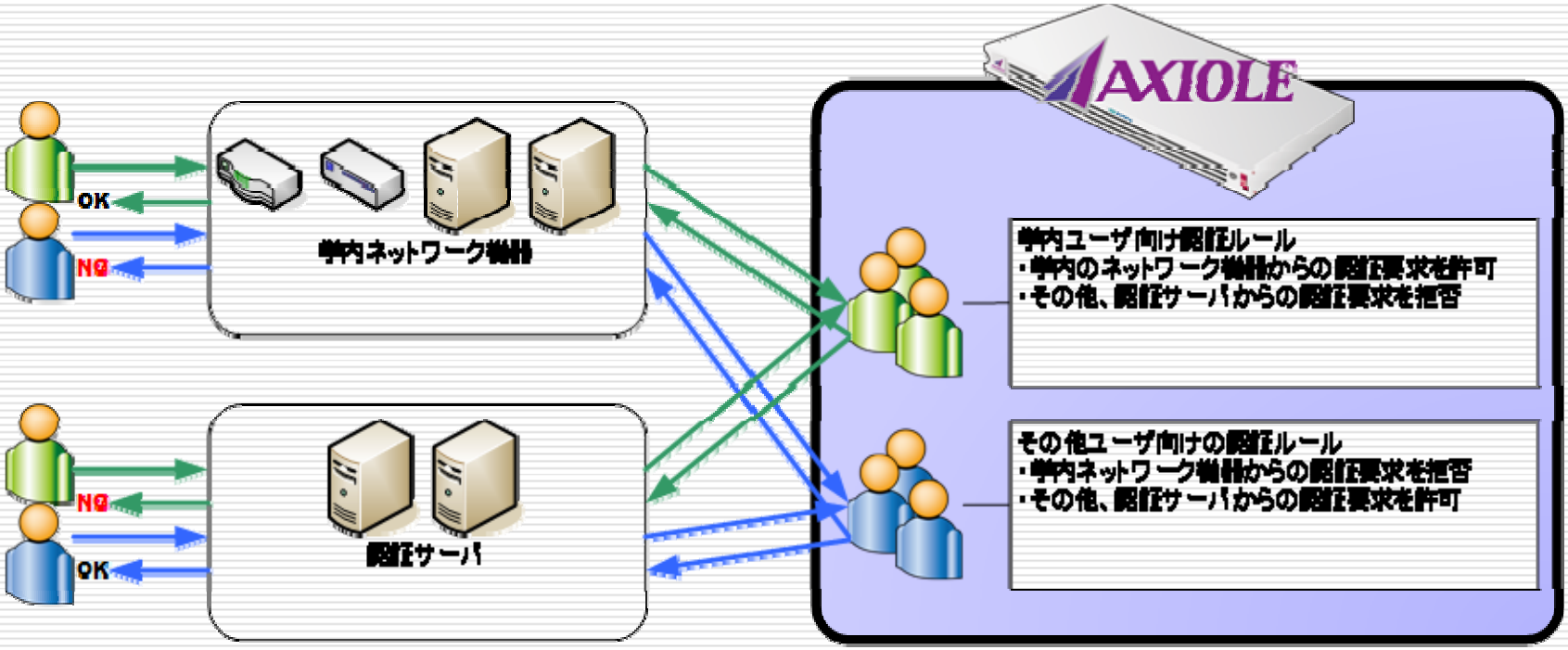
S大学様の事例ー構成



O大学様の事例ー概要

規模	ユーザ数：7,000 AXIOLE 2台で冗長化
用途	全学生・教職員の認証サーバ
主なLDAP・RADIUS機器	□FEREC □e-ラーニングCMS □VPNサーバ □その他
その他	□認証ポリシーを使用し、教職員と学生が利用可能なネットワーク機器を制御 □「ADデータ反映」を使用し、管理はAXIOLEで一元化

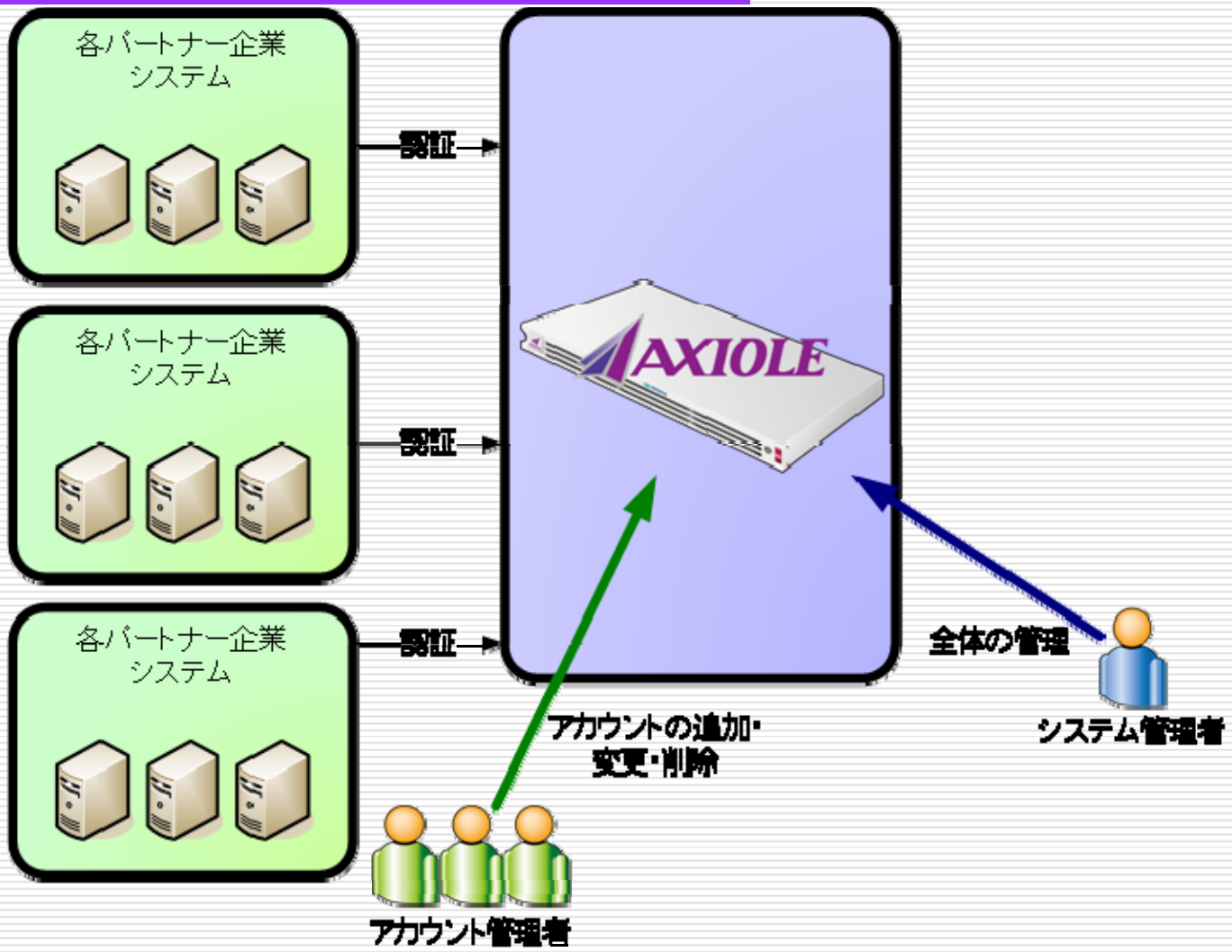
O大学様の事例－構成



某銀行様の事例ー概要

規模	ユーザ数：4,000 LDAPスキーマオプションを適用 AXIOLE 2台で冗長化
用途	パートナー企業用システム向け認証サーバ
主なLDAP・RADIUS機器	□Linux端末、Webサーバなどパートナー企業が使用するネットワーク機器
その他	□出入りするパートナー企業が企業毎に認証サーバを立てて運用し、登録アカウントの把握が困難だった □パートナー企業同士が連携するプロジェクトもあり、アカウント管理に手間がかかっていた □アカウント管理の一元化を目的に、当初OpenLDAPでの構築を予定していたが、導入や運用の手間を考えると実行できなかった

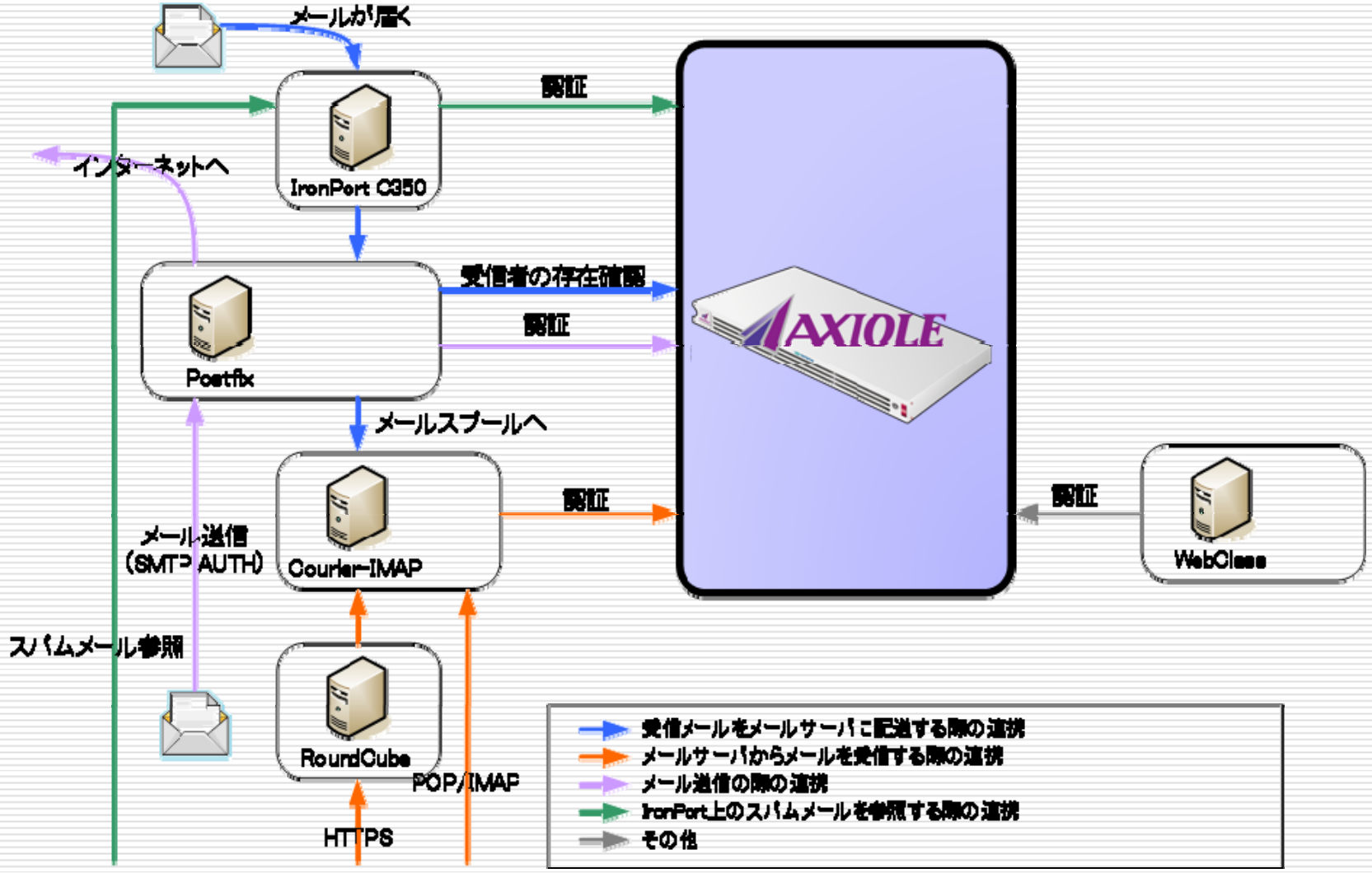
某銀行様の事例ー構成



K高専様の事例ー概要

規模	ユーザ数：2,000 AXIOLE 2台で冗長化
用途	全学生・教職員のメール環境のアカウント管理
主なLDAP・RADIUS機器	□IronPort C350（電子メールセキュアアプライアンス） □Postfix □Courier-IMAP □RoundCube（Webメール） □WebClass（e-Learningサーバ） □その他
その他	□e-Learningサーバ（当初は、サーバ内で認証）の導入などによって、アカウントの管理コストが増大していた □複数アカウントによって利用者が混乱→ネットワーク管理者の負担も増大 □メールのスパム対策と合わせてユーザ管理の一元化を検討 □WebUIによる容易な管理に高い評価頂く □パスワード再発行機能によって、センターへの問い合わせ数の削減を実現

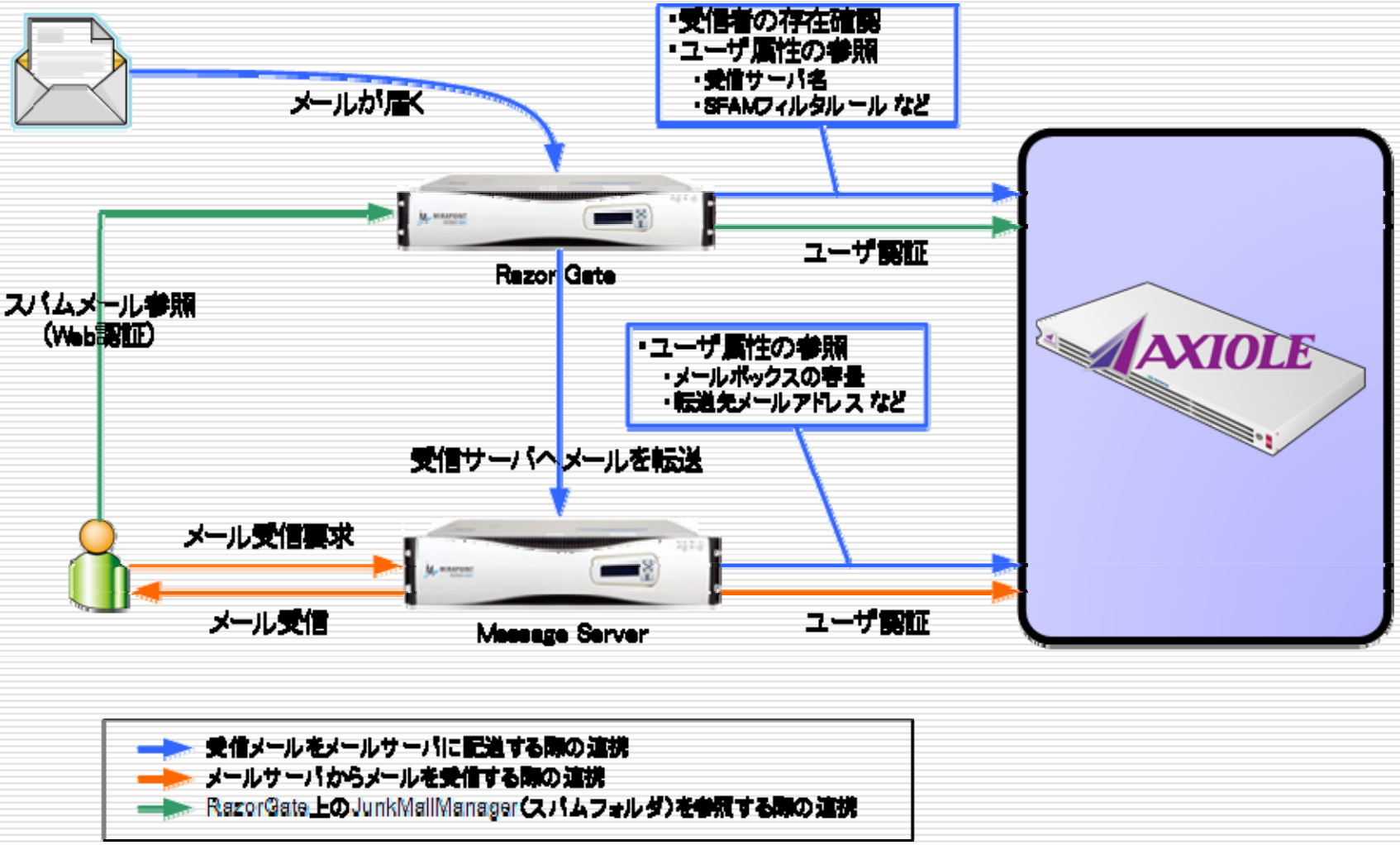
K高専様の事例ー構成



B社様、S社様の事例ー概要

規模	ユーザ数:1,000 LDAPスキーマオプションを適用
用途	ミラポイント社 メールアプライアンスの外部LDAPサーバとして利用
主なLDAP・RADIUS機器	□ミラポイント社 Message Server □ミラポイント社 RazorGate
その他	□ミラポイント製品付属のLDAPスキーマ定義をAXIOLEにインポート □アカウントの移行も含めて導入作業は数時間で完了

B社様、S社様の事例－構成



Ni社様、Ne社様の事例－概要

規模	ユーザ数：1,000および7,000 AXIOLE 2台で冗長化
用途	MACアドレス認証のRADIUSサーバとして利用
主なLDAP・RADIUS機器	□日立電線 Apresia □CISCO Catalyst
その他	□多彩なMACアドレス認証の設定が可能 ■ブラックリスト・ホワイトリスト ■共有・ユーザ関連付け ■例外ユーザ □MACアドレスとユーザを別々に管理できるため分かりやすい □将来LDAPの利用を行う場合に追加コストが不要 ■追加コストが不要 ■ユーザデータの再登録などの手間が不要 ■AXIOLEの設定画面で「LDAP」「LDAPS」をオンにするだけ

事例を通して

- 導入時の手間が少ない
  - 短期間での環境構築～運用開始を実現
  - 既存のアカウントデータの取り込みにより環境移行時の負担を軽減（パスワードの再設定などが不要）
- 専門的なスキルが不要
  - 分かりやすいWebUI
  - 日々の運用はネットワーク管理者以外の方が従事されている

株式会社ネットスプリング
http://www.netspring.co.jp/

AXIOLE
http://www.axiole.jp/
E-mail: info@axiole.jp