Apani

.....EpiForceのご紹介

株式会社アパニ・ネットワークス・ジャパン

Apaniについて

- 本社：南カリフォルニア
  - US、UK、日本にオフィス
  - 2003年創業
  - オーナーは日本の高原財団
  - ヒューズの技術者が開発
  - シティグループがファーストユーザ

- セキュリティソリューション
  - 企業向けセキュリティ
  - プロフェッショナルサービス
  - 24/7技術サポート

Apani

代表的なお客様

Apani

PCI-DSS事例： カナディアン・タイヤ

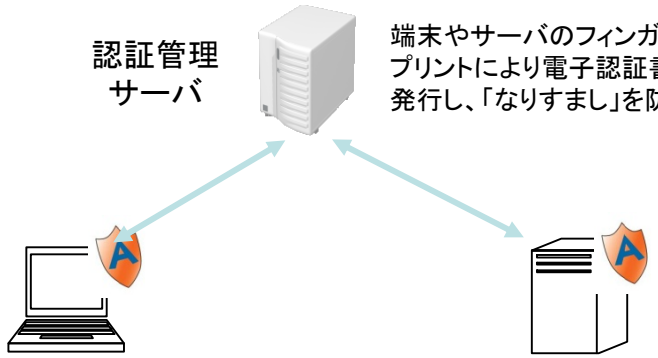
- カナディアン・タイヤ（ホームセンター）の金融部門
  - カナディアン・タイヤはカナダに475の店舗を保有
  - クレジットカード、保険、銀行を世界で展開
- 500万件のクレジットカードを発行
- 通信データの暗号化
- サーバのセグメンテーション
- 異機種IT環境の集中管理

Apani

EpiForceとは

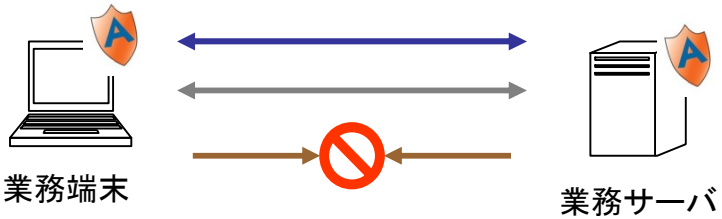
①

機器やユーザーの認証



②

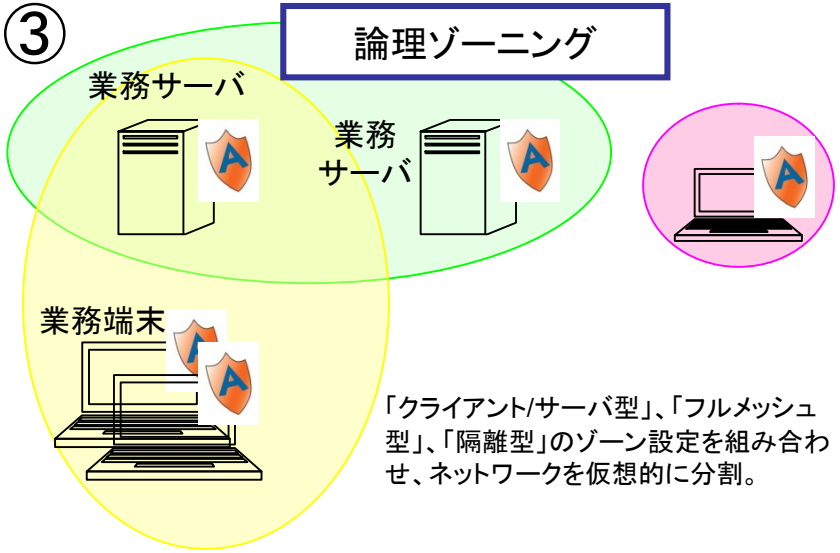
エンドtoエンド通信



端末やサーバは、通信ポート単位で「暗号」、「平文」、「遮断」といったポリシーに従って通信を行う。

③

論理ゾーニング

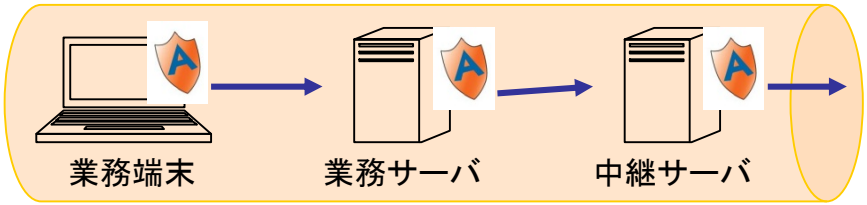


「クライアント/サーバ型」、「フルメッシュ型」、「隔離型」のゾーン設定を組み合わせ、ネットワークを仮想的に分割。

④

オーバーレイ

既存の物理ネットワークの上層にセキュリティネットワークを付加。
論理ゾーニングによる多層のセキュリティを実現。

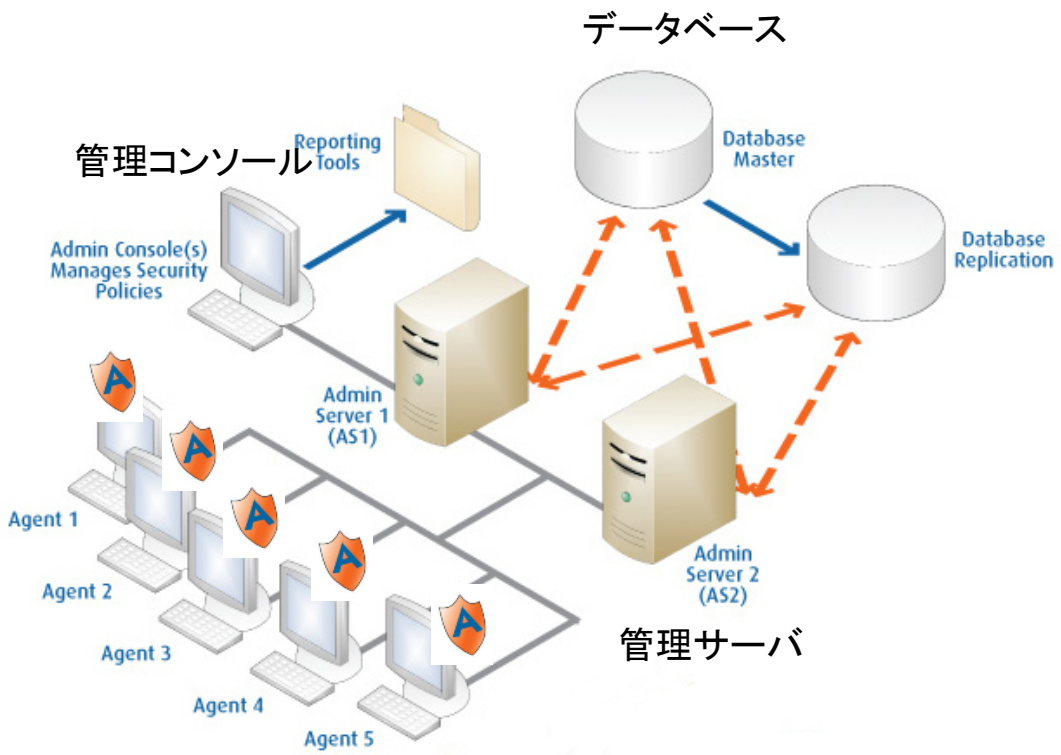


Apani

EpiForceアーキテクチャ

- 分散、フェイルオーバー
  - シングルポイント・フェイリアなし
  - ボトルネックなし
- 高いスケーラビリティ
  - オンデマンド・ポリシー配布
  - 100,000エージェントまで拡張可
- 標準準拠のセキュリティ
  - IPSec、X.509v3
  - 3DES、AES128/256
  - FIPS 140-2 level 1
- エージェントプラットフォーム

  Windows (2003, 2008, XP, 7)
  Linux (RedHat,SuSE, CentOS)
  UNIX (AIX, Solaris, HP-UX), Mac X
  HWエージェント (汎用機, プリンタ等)

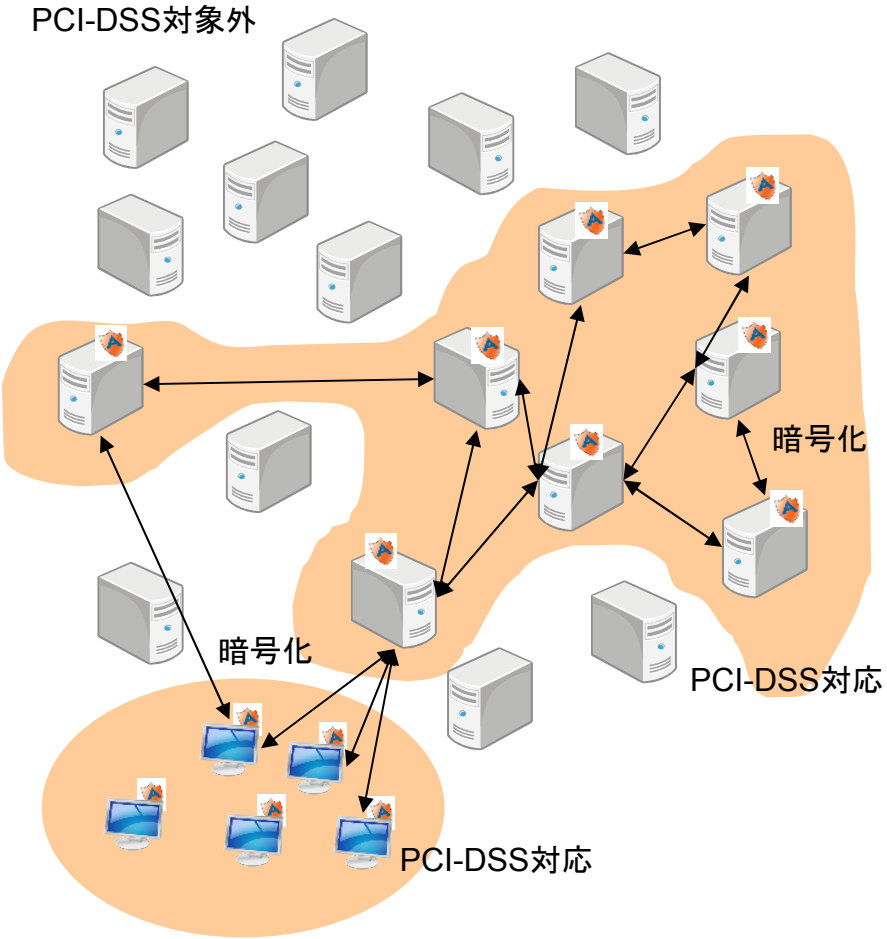


Apani

PCI DSSへの適用

- 論理ゾーニングによるセグメンテーション（評価対象の限定）
- デフォルトで拒否のアクセス制御
- 管理アクセス、会員データ伝送の暗号化
- ユーザ識別ネットワーク
- 監査証跡とレポートツール

論理ゾーニングによる評価対象の限定



ネットワークセグメンテーションは以下を引き下げる方法として強く推奨されます。
・PCI DSS評価の対象範囲
・PCI DSS評価のコスト
・PCI DSS コントロールの実装と維持に関するコストおよび難易度
・組織のリスク

ネットワークセグメンテーションが適切に設定されていない場合（「フラットネットワーク」とも呼ばれます）、ネットワーク全体が PCI DSS 評価の対象範囲になります。

（PCI DSS前文）

論理ゾーニング

IPネットワークの仮想的な分割（セグメンテーション）

EpiForceのメリット

＃1　セグメントの重複が可能

＃2　IPアドレスや物理的な接続に依存しない

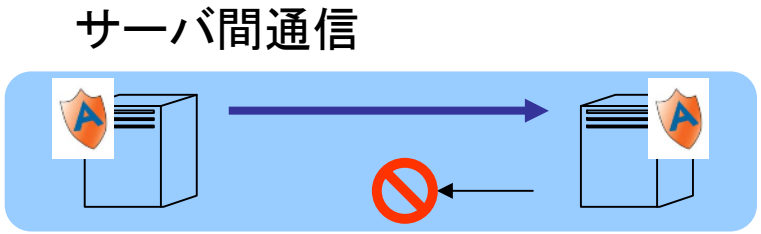
＃3　ネットワーク、アプリケーションは変更不要

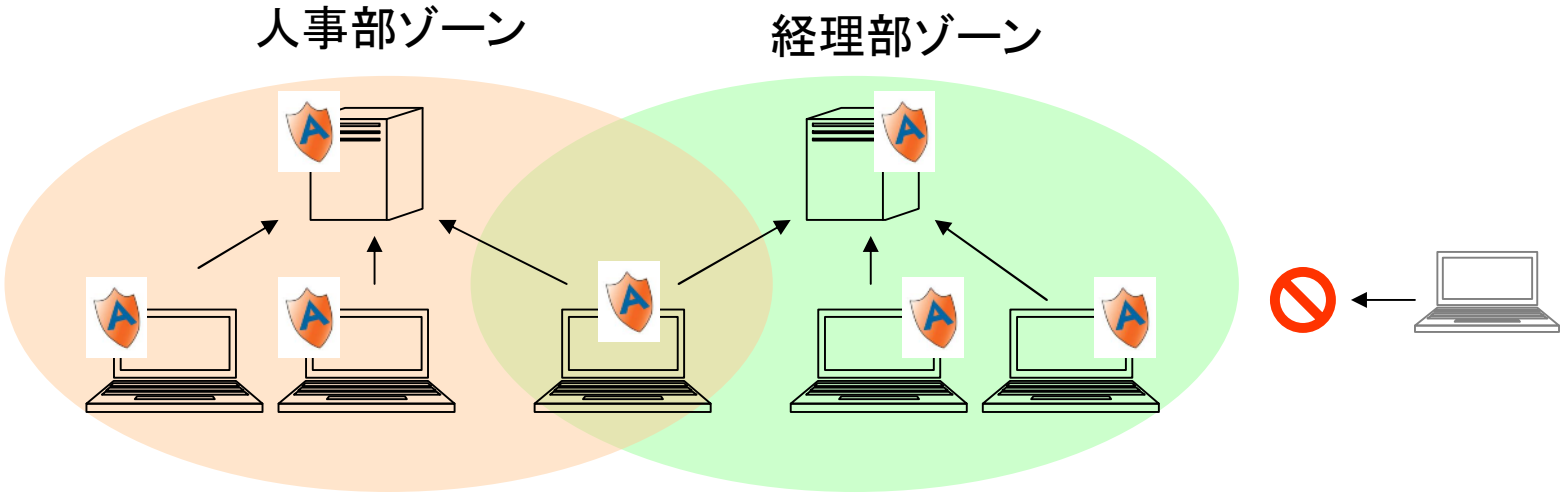
＃4　エンド−エンド接続で直観的な設定

Apani

論理ゾーニング例（CSZ）

- 「ゾーン」の重複設定が可能
- ポート単位のアクセス、通信の方向を制御
- VLAN+FWと等価





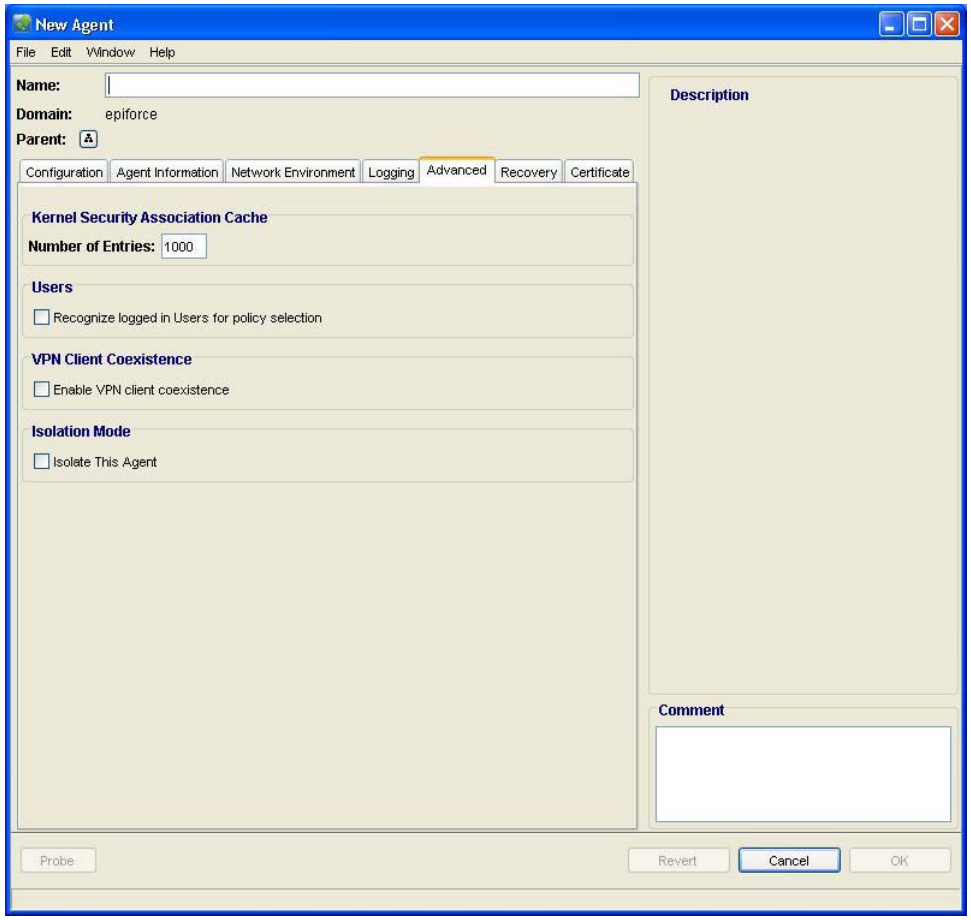
適合要件

要件	内容	EpiForce機能
2.3	強力な暗号化を使用して、すべてのコンソール以外の管理アクセスを暗号化する。	通信データ暗号化
4.1	オープンな公共ネットワーク経由で機密性の高いカード会員データを伝送する場合、強力な暗号化とセキュリティプロトコル（SSL/TLS、IPSEC、SSH など）を使用して保護する。	通信データ暗号化
7.1	システムコンポーネントとカード会員データへのアクセスを、業務上必要な人に限定する。	ユーザ識別ネットワーク
7.2	複数のユーザが使用するシステムコンポーネントで、ユーザの必要性に基づいてアクセスが制限され、特に許可のない場合は「すべてを拒否」に設定された、アクセス制御システムを確立する。	アクセスのデフォルト拒否
8.4	強力な暗号化を使用して、すべてのシステムコンポーネントにおいて伝送および保存中にすべてのパスワードを読み取り不能にする。	通信データ暗号化
10.1	システムコンポーネントへのすべてのアクセス（特に、ルートなどの管理権限を使用して行われたアクセス）を各ユーザにリンクするプロセスを確立する。	管理サーバ
10.2	以下のイベントを再現するためにすべてのシステムコンポーネントの自動監査証跡を実装する。	管理サーバ
10.3	イベントごとに、すべてのシステムコンポーネントについて少なくとも以下の監査証跡エントリを記録する。	管理サーバ
10.4	時刻同期技術を使用してすべての重要なシステムクロックおよび時間を同期し、時間を取得、配布、保存するために以下の要件が実施されていることを確認する。	NTPによる同期

Apani

アスセスのデフォルト拒否

『Isolation Mode』では、明示的にゾーンに含めない限りインバウンド、アウトバウンドのトラフィックを全て拒否します。



Apani

通信データの暗号化

IPsec（トランスポートモード）による暗号化通信

EpiForceのメリット

＃1　グループ-グループ、グループ内の定義が可能

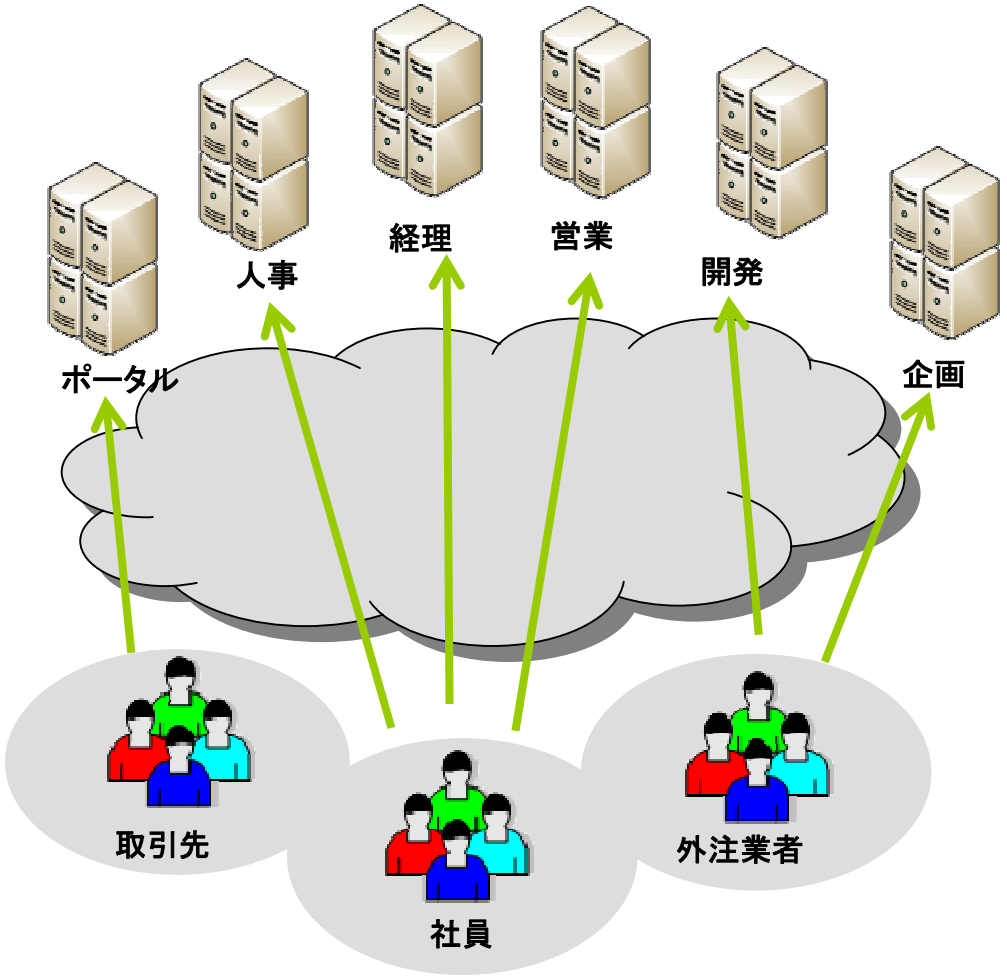
＃2　強力な暗号化（3DES、AES128/256）サポート

＃3　HWエージェント利用

＃4　証明書管理、鍵管理の自動化

Apani

ユーザ識別ネットワーク



- ADによるユーザ識別
- ユーザ＋機器でゾーニング
- ユーザ操作の証跡、レポート
- 大規模な導入・運用が可能

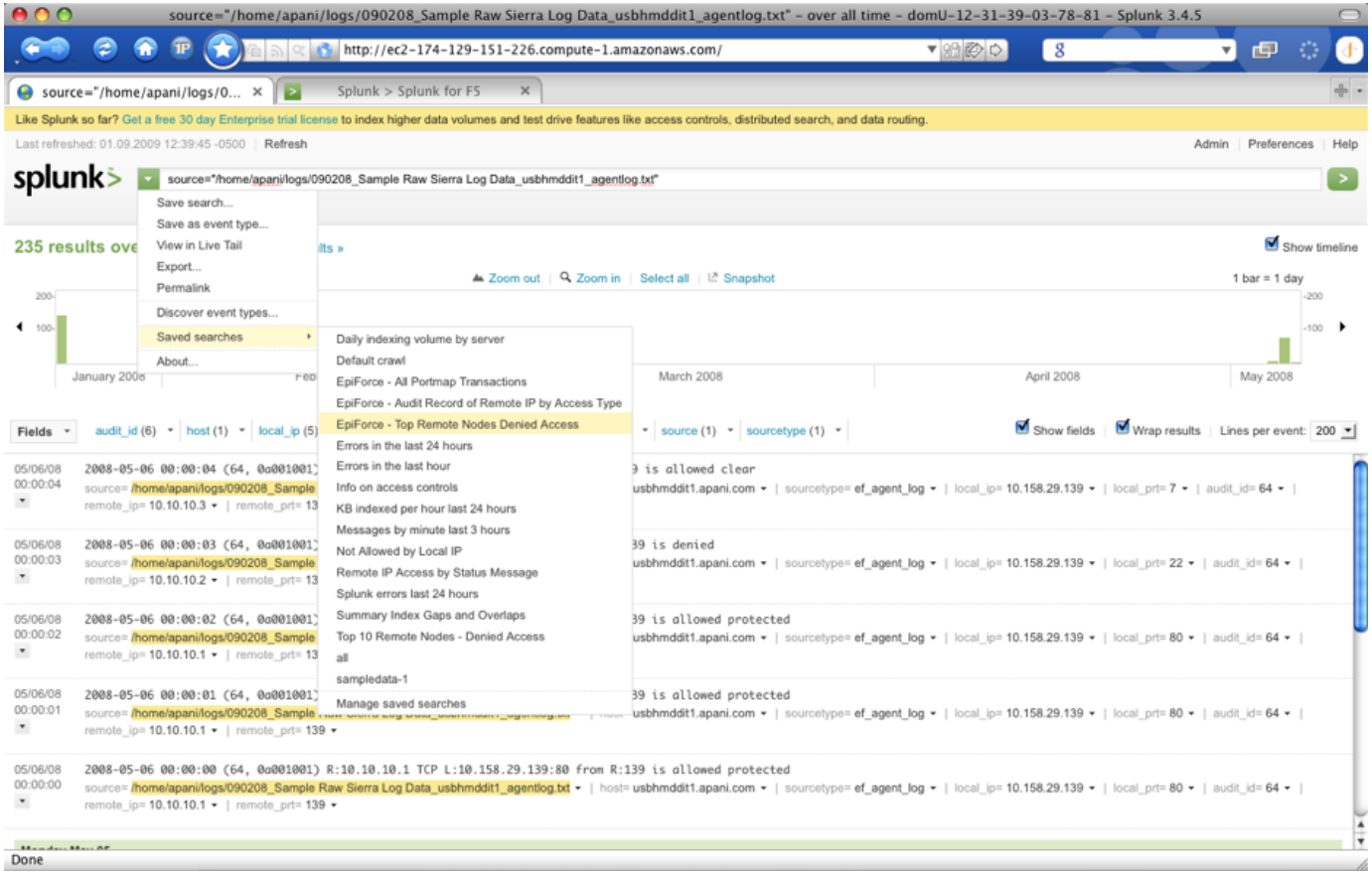
Apani

（参考）ADとEpiForceの比較

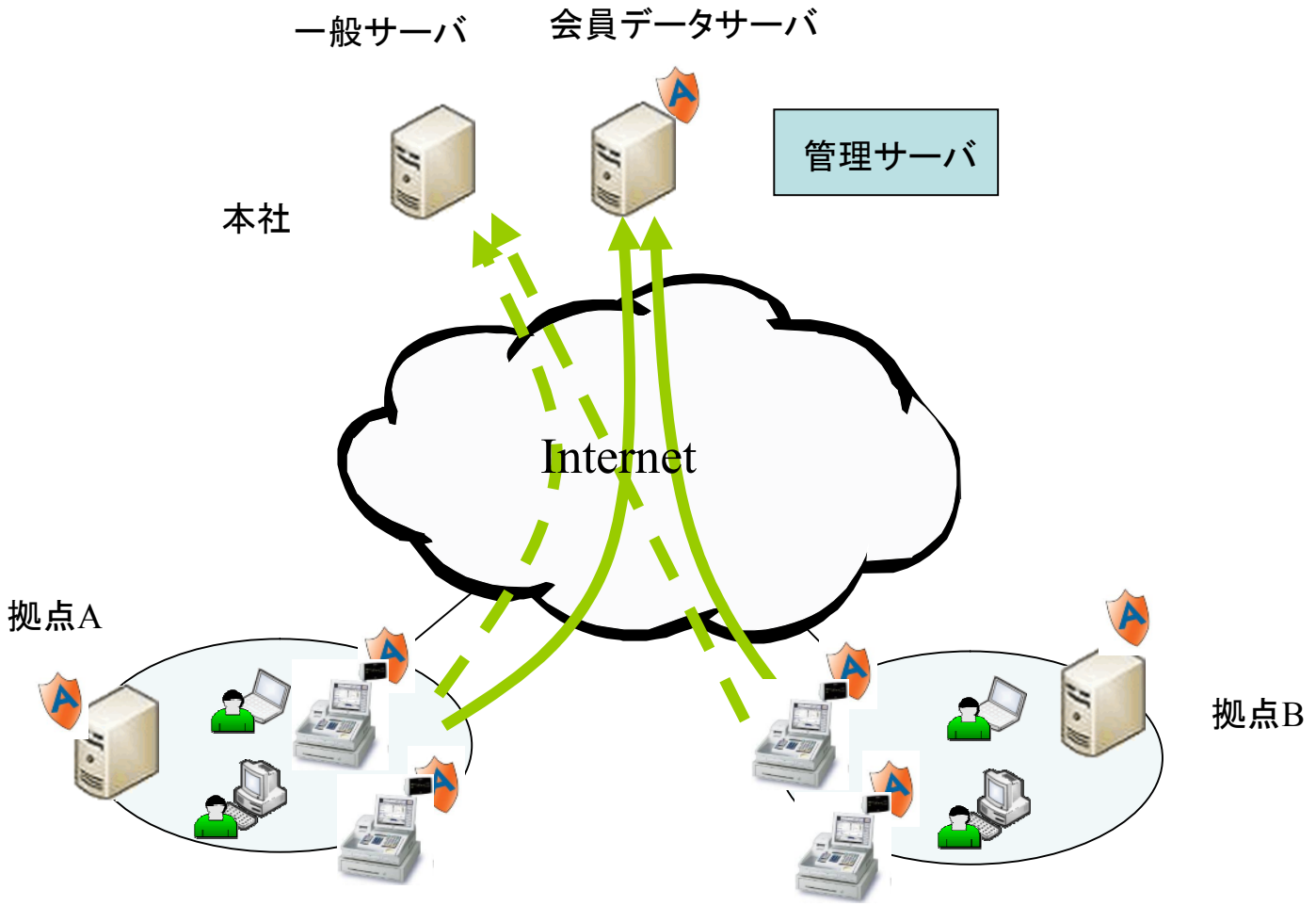
	AD	AD + EpiForce
複数AD制御	×	○
論理ゾーニング	×	◎（多重可）
サーバとの接続	アプリケーション（L7） サーバにアクセスできる	ネットワーク（L3） サーバ自体にアクセスできない
サーバ機器認証	×	○
通信ポート指定	×	○
通信方向制御	×	○
サーバ間接続制御	×	○
通信データ暗号化	×	○
ライブマイグレーション対応	×	○
アクセス制御対象サーバ		
Windowsサーバ	○	○
Linuxサーバ	×	○
Unixサーバ	×	○
汎用機	×	○（by HWエージェント）

アクセスの追跡/監視

システム管理者を含む全てのアクセスは監査証跡として管理サーバに蓄積され、Splunk等のレポートツールにて出力可能です。

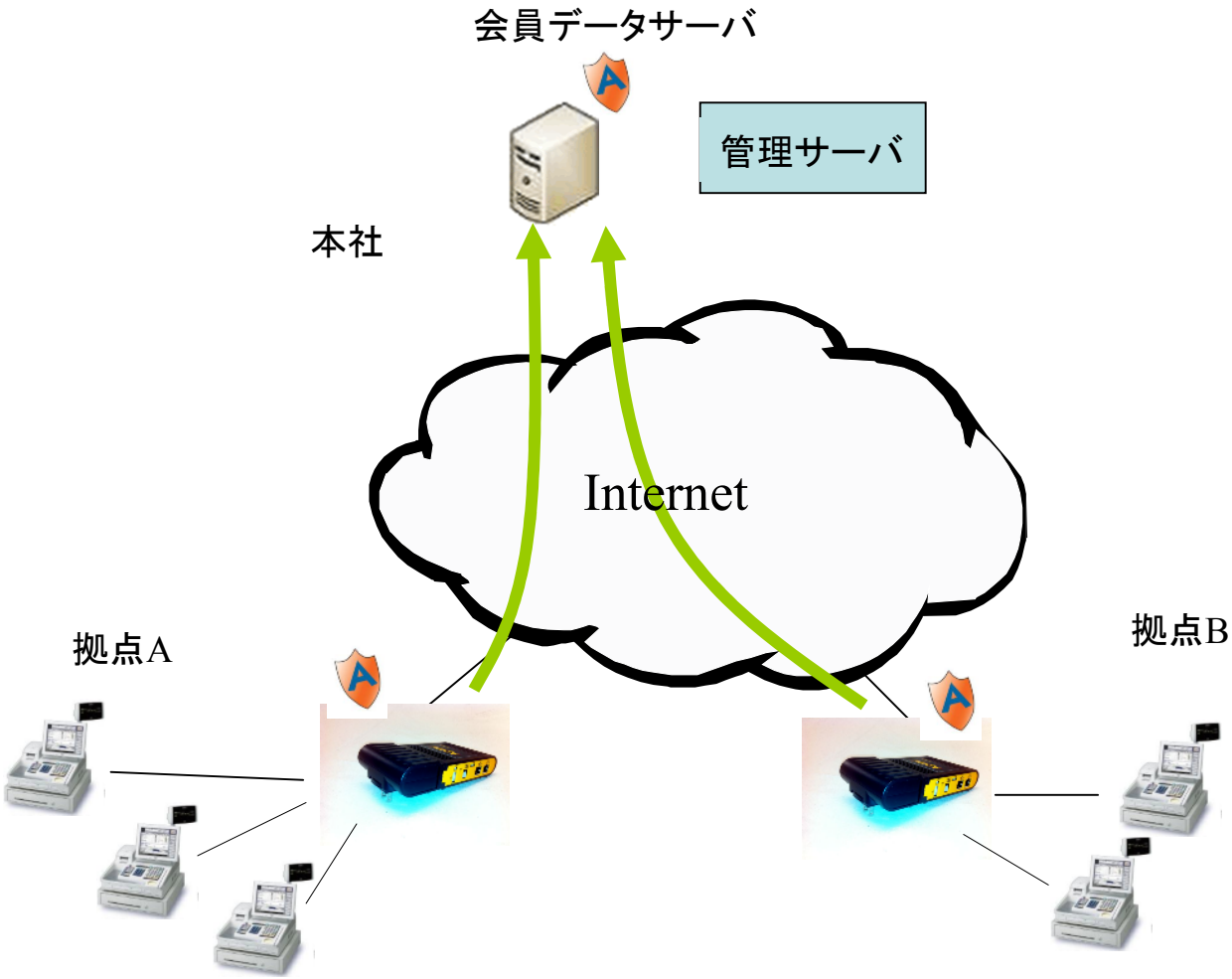


構成例 - 1



拠点サーバ、POSからのみ会員データサーバにアクセス可能
その他からは一般サーバのみにアクセス可能

構成例 - 2



拠点からのアクセスは会員データサーバのみに可能（リアルタイムに設定変更が可能）