



TNC overview

2009/12/08 TCG Workshop

Agenda

Introduce TNC

TNC 概要解説

- NACがなぜ必要なのか？
- Network Access Controlという解決策
- TNCのアーキテクチャ
- TNCに参加しているベンダー
- どちら辺がTNCのいいところ？

まとめ



Trusted Network Connect

ネットワークセキュリティのためのオープンアーキテクチャ

- ベンダーに縛られない中立の規格
- Trusted Computing Groupの成果を用いた強力なセキュリティ
- NACから始まったが、現在はネットワークセキュリティ全般へと広がっている

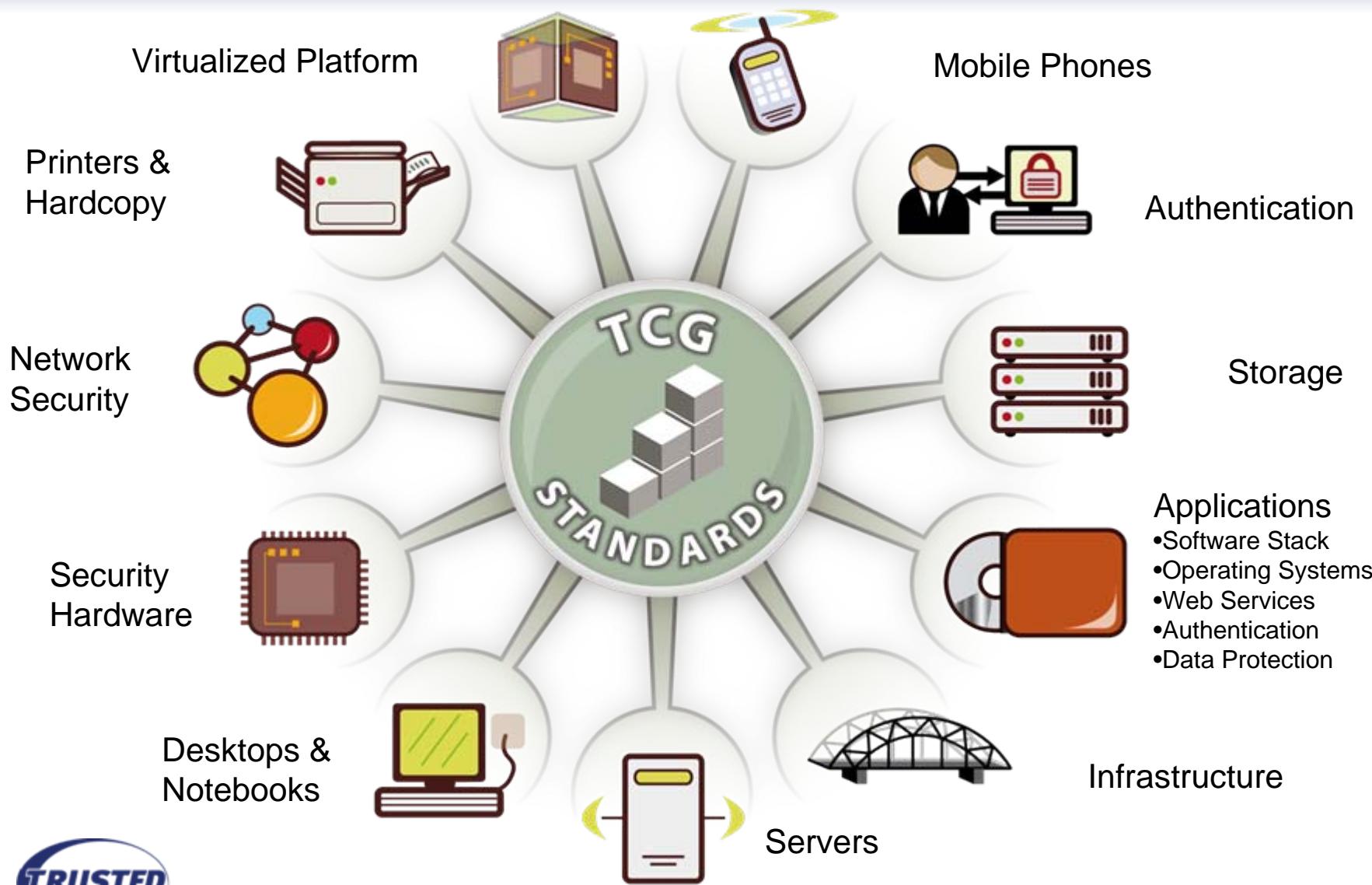
ネットワークセキュリティのためのオープン規格

- ネットワークを全てをカバーできるフルセットが提供されている
- 対応プロダクトは既に4年以上前から出荷されてる

TCGによって開発されている

- 業界標準グループ
- 大小問わず100以上の企業、(開発側、ユーザー側含む)が参加

TCG: Standards for Trusted Systems



NACがなぜ必要なのか？

エンタープライズネットワークへの接続は拡大の一途

- 契約業者、協業パートナー、来客
- モバイルデバイス、組み込み機器
- より強力で柔軟なアクセスコントロールが必要となってきた

拡大、専門化する攻撃

- 組織的な攻撃、国家間での攻撃、(サイバーではない)テロ
- 盗み出したデータを換金できる市場ができあがってしまっている

データの損失に伴う被害

- データを失うこと自体の損失、問題の公開、訴訟リスク、法規制への抵触、ブランドイメージの低下

コンプライアンスへの要求

Network Access Controlという解決策

1. ネットワークアクセスのポリシーを作る
2. ネットワークアクセスする機器に対して、ポリシーの遵守を要求し、記録を取る
3. ポリシーを遵守していない端末を隔離し、修復させる
4. 更にTPMを利用して
5. Optionally, integrate with TPM to
 - 強力なユーザーと機器の認証
 - ルートキットからの防御

Network Access Control ポリシーの例

安全に業務ネットワークにアクセスするために…

1. ユーザーは認証されてなければならぬ

- 認証システムを使用する

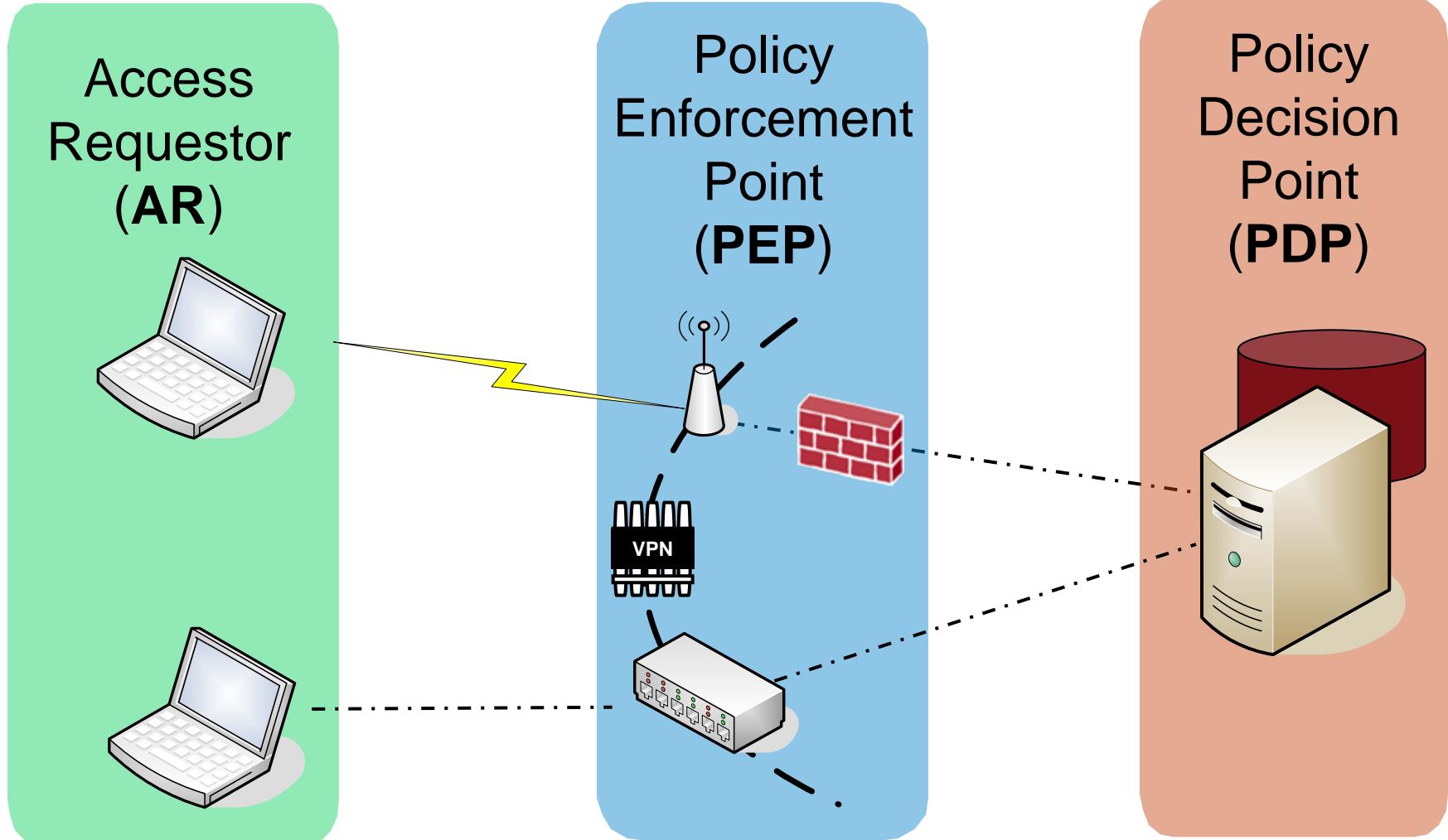
2. エンドポイントは「健康」でなければならぬ

- アンチウィルスソフトウェアが正しく設定され、稼働していなくてはならぬ
- 直近のスキャンで脅威が存在しないことが確認されなくてはならぬ
- パーソナルファイアウォールが適切に設定されていなくてはならぬ
- パッチが最新の状態でなくてはならぬ

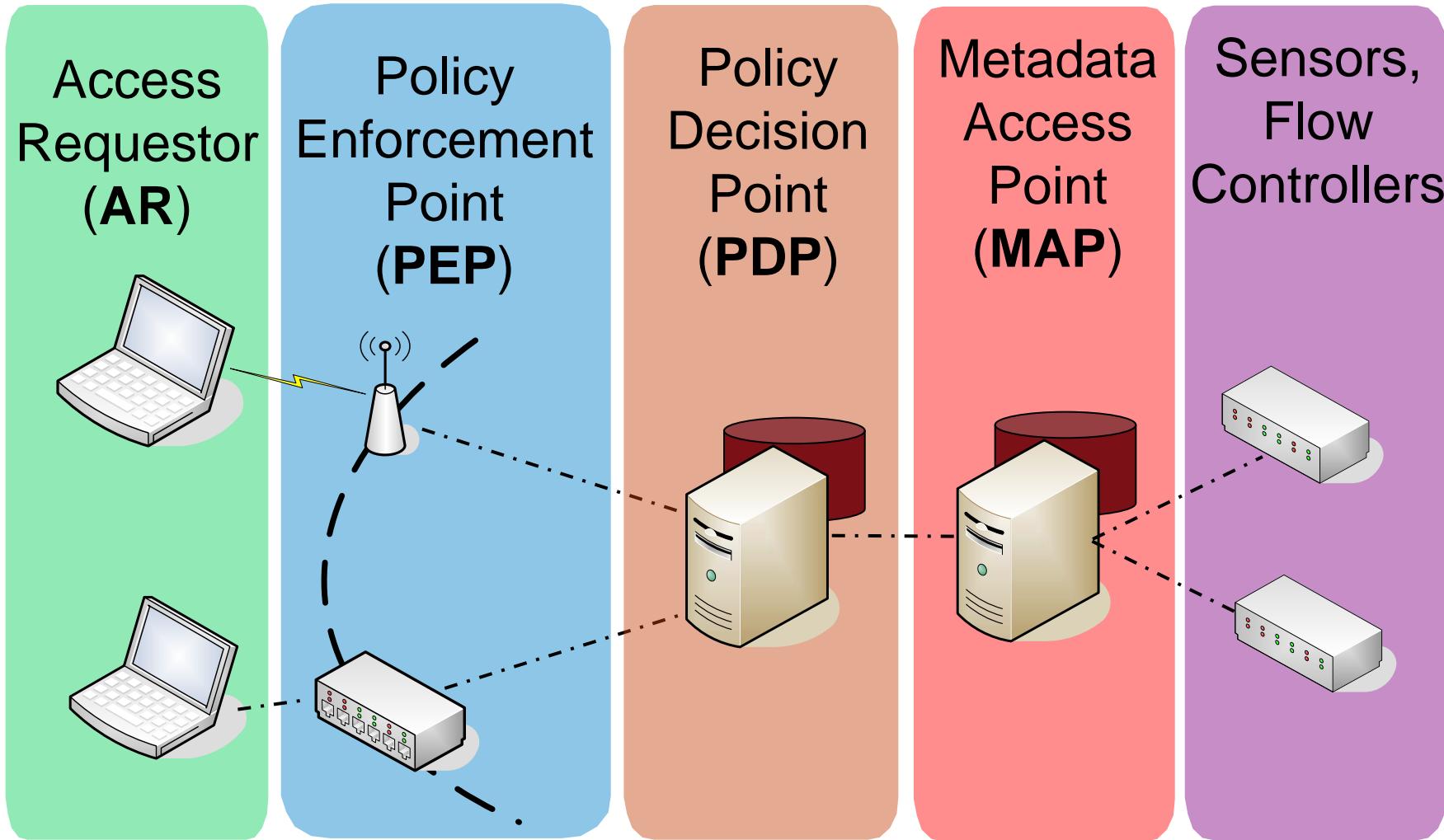
3. 接続後も、ポリシーに沿わない振る舞いをしてはならぬ

- ポートスキャンの禁止、スパム送信の禁止、等々

基本的なNACアーキテクチャ



MAPによる他のセキュリティデバイスとの連携



典型的なTNCの活用方

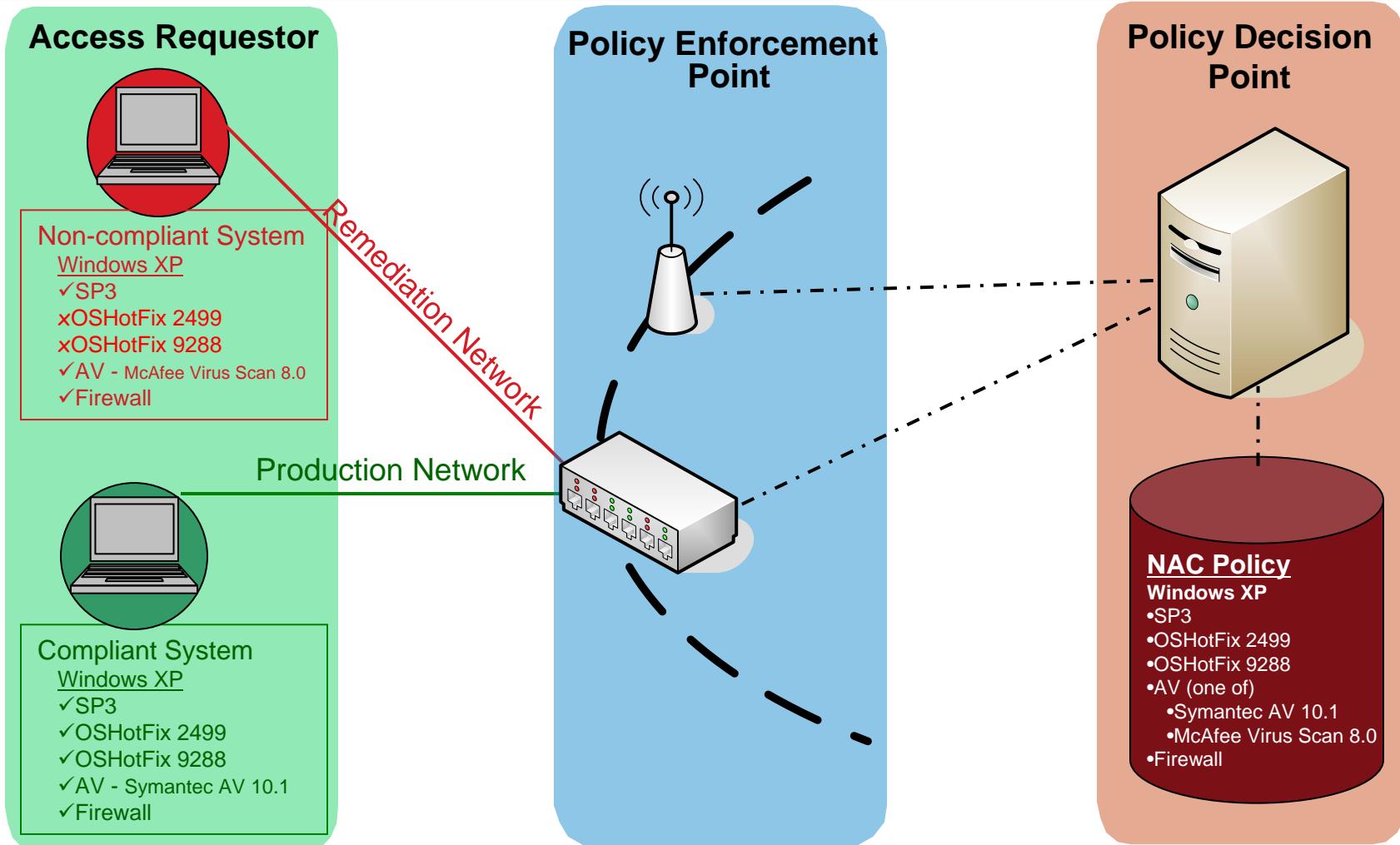
ヘルスチェック

振る舞いチェック

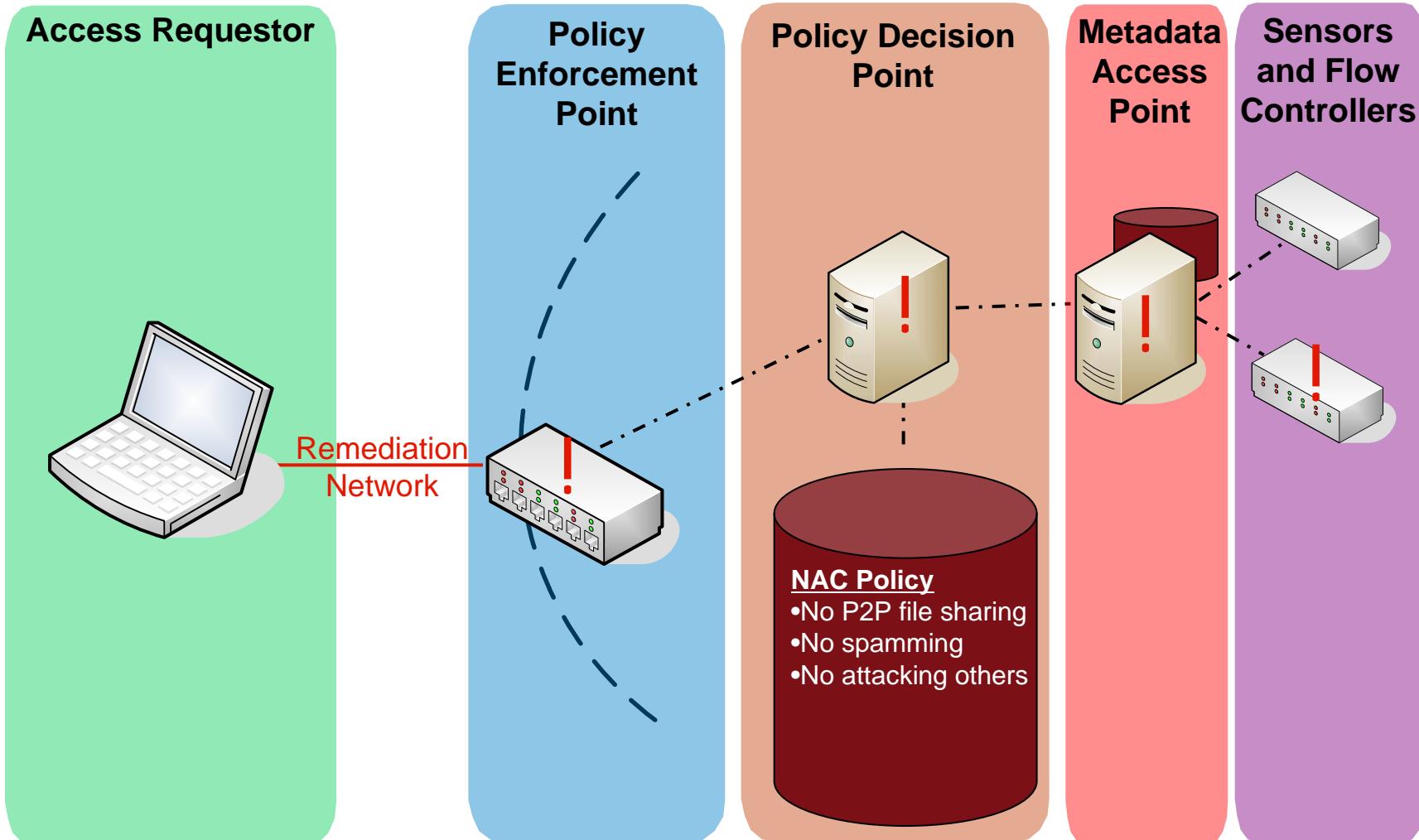
ユーザー毎のポリシー遵守

TPMによるプラットフォームの整合性確認

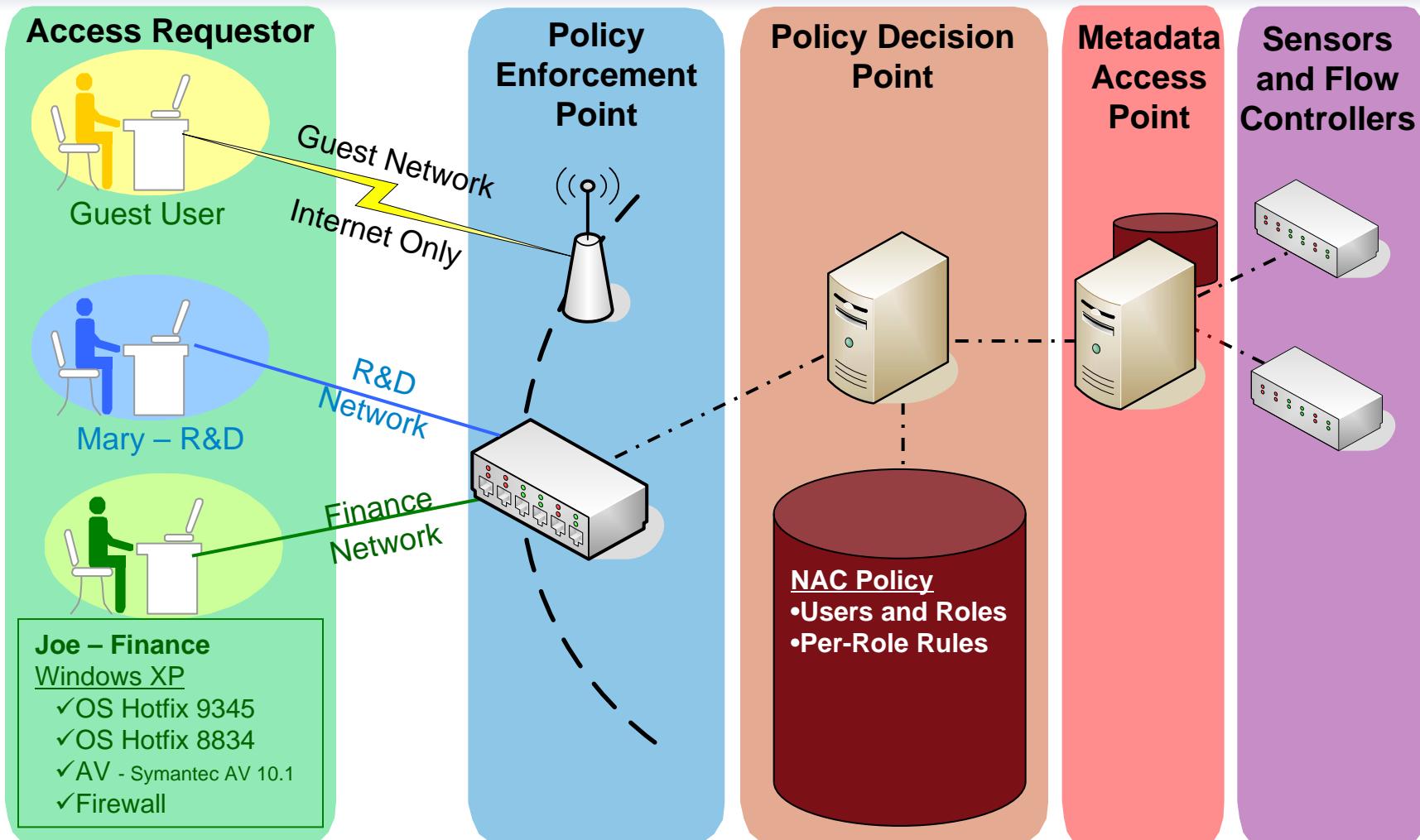
ヘルスチェック



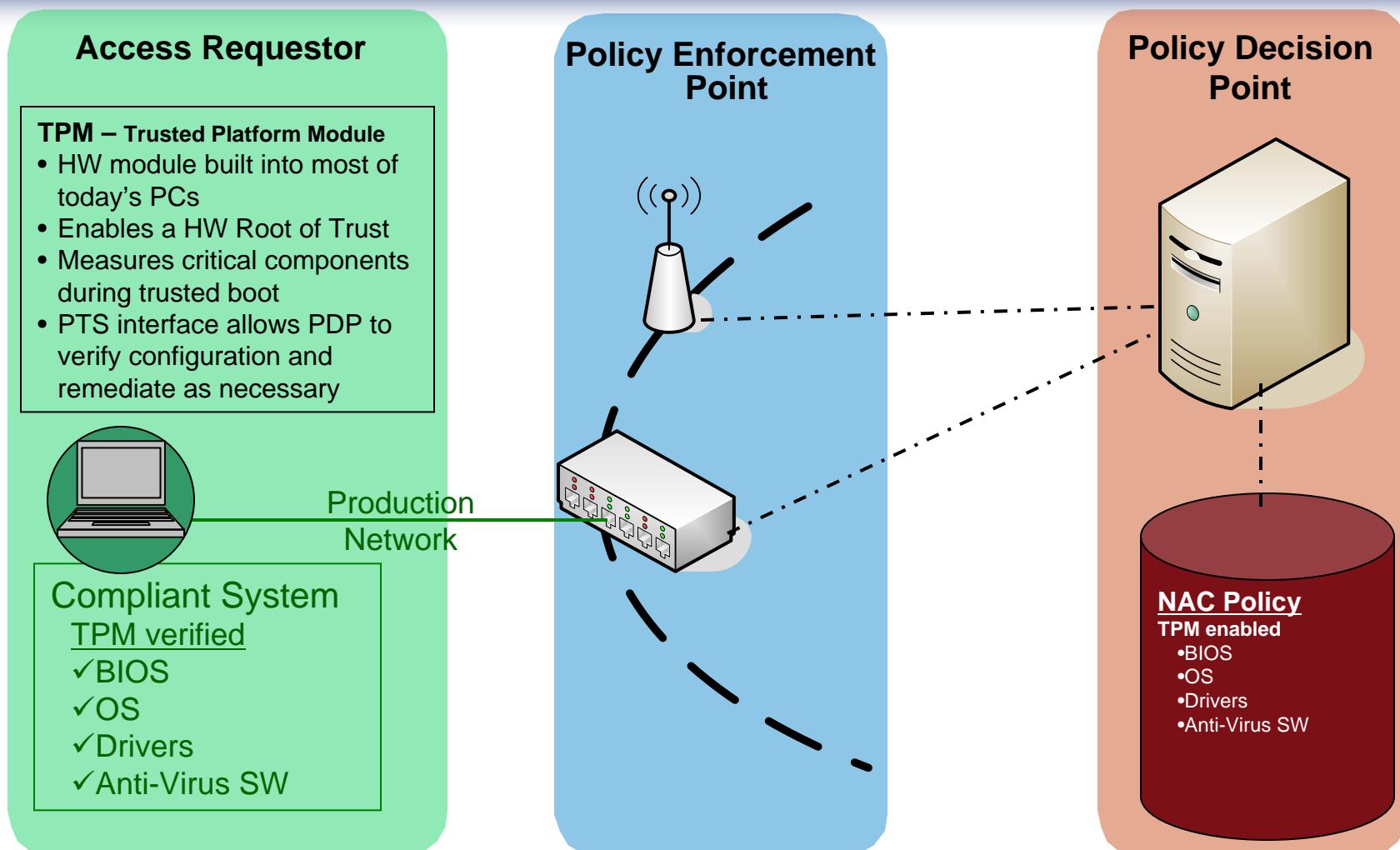
振る舞いチェック



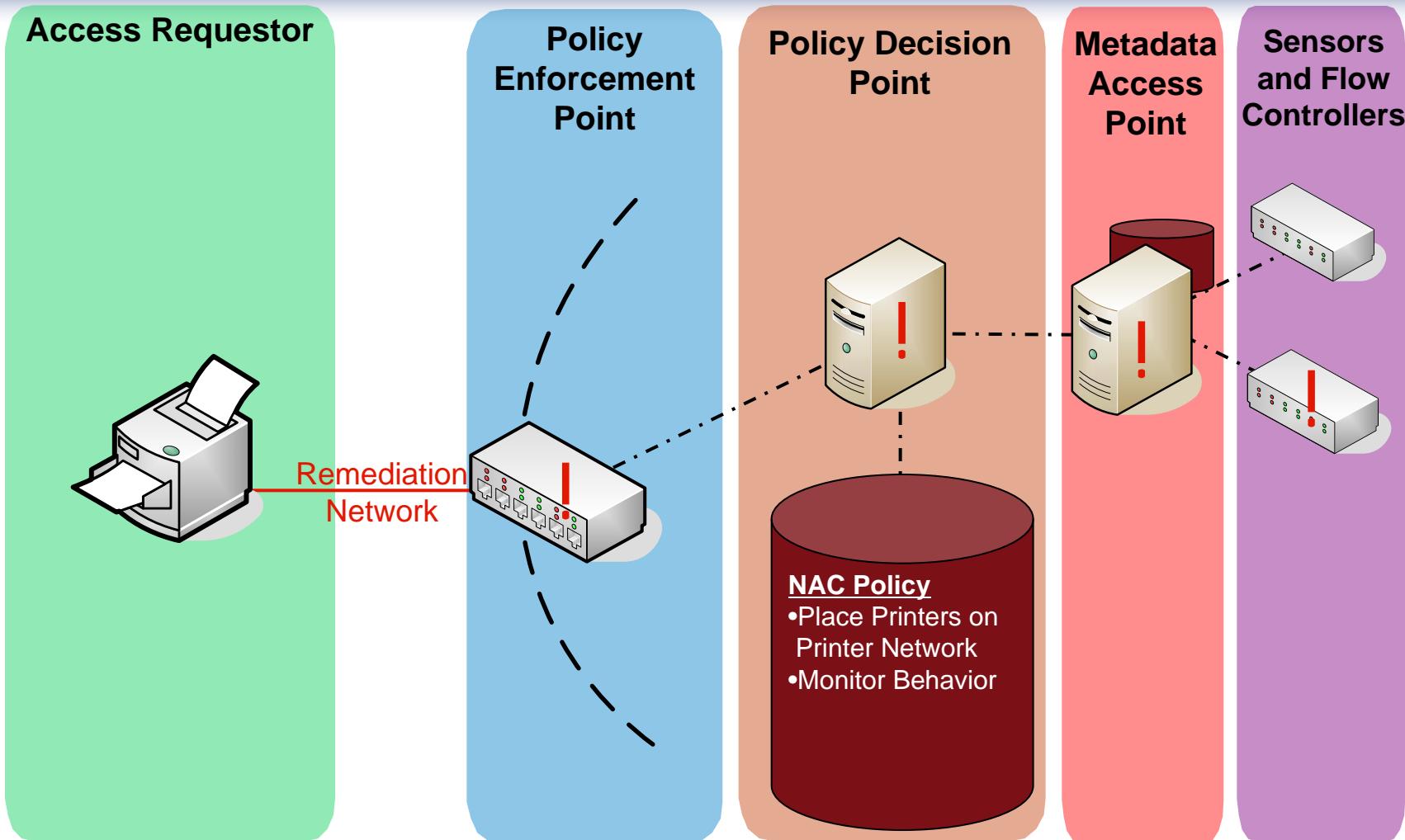
ユーザー毎のポリシー遵守



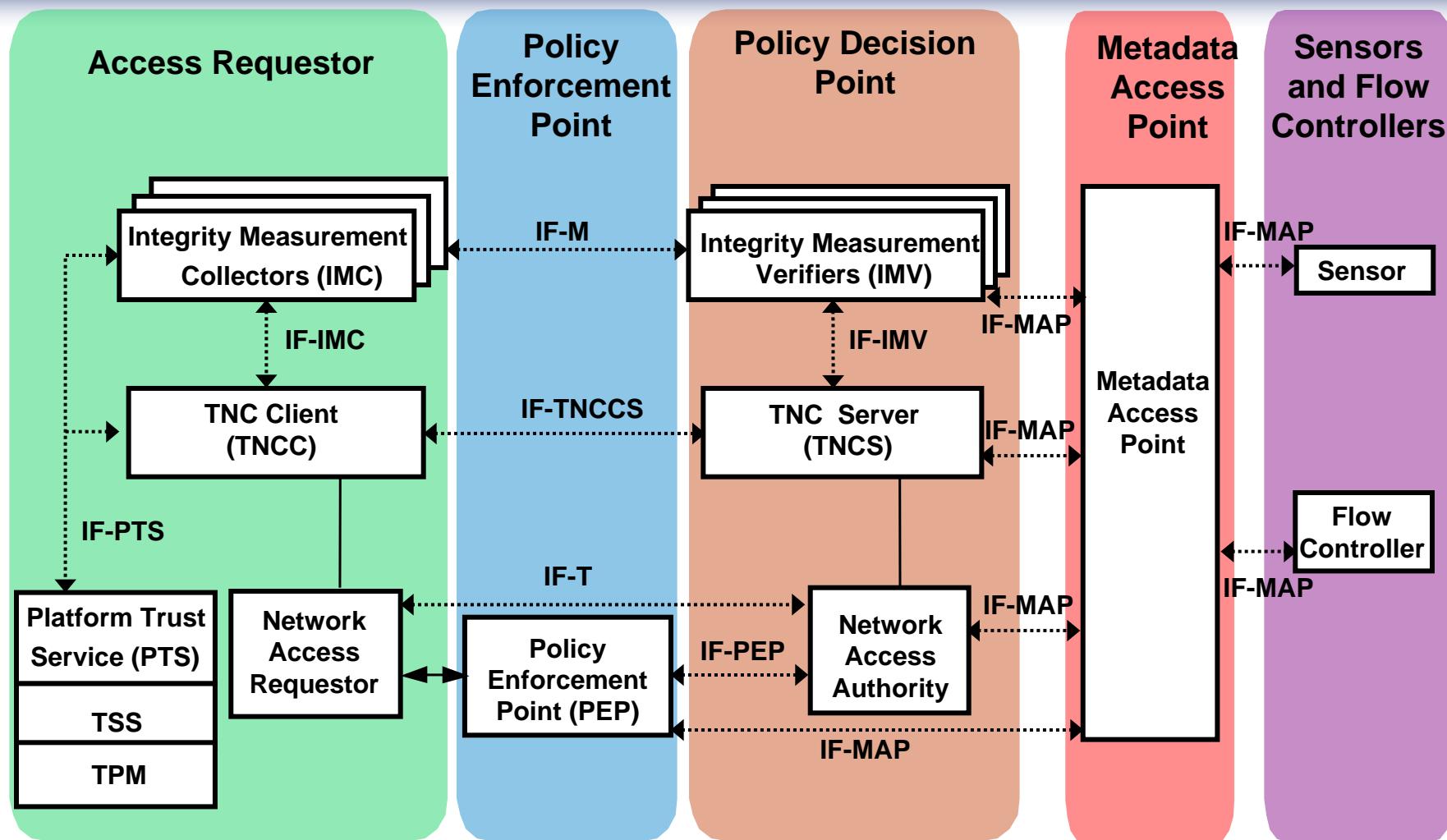
TPMによるプラットフォームの整合性確認



NACクライアントを利用できない機器の管理



TNCの各モジュール概念図



TPMとTNCでルートキットを排除する

これにより、致命的なリスクとなる「嘘をついている端末」を排除できる

- セキュリティステータスをレポートさせてもそれが安全なのかというリスクがある

TPMではプラットフォームのブートシーケンスの検証を行うことが出来る

- ソフトウェアを使用する前にPCRにそのソフトウェアのハッシュを格納
- PCRの値はハードウェアごと再起動しなくてはリセットできないため、ソフトウェアの整合性の検証が可能となる

TNC Handshakeの中でできることは...

- PDPはTPMとの間に安全な通信経路を用意する
- TPMはPCRの値にサインしてPDPへ安全に送信する
- PDPはPCRの値を持ちの「安全な状態」と比較する
- もしアプリケーションが改竄されていた場合、送られたPCRが違うため検知できる
- 「安全な状態」が確認出来ない端末は隔離され、修復される

Federated TNC連携

セキュリティドメイン間で、TNCの評価結果を共有する

- コンソーシアム、協業、パートナーシップ、アウトソーシング、アライアンスパートナー
- セキュリティの管理が分割されているような大きな組織などで有効

何が出来るか？

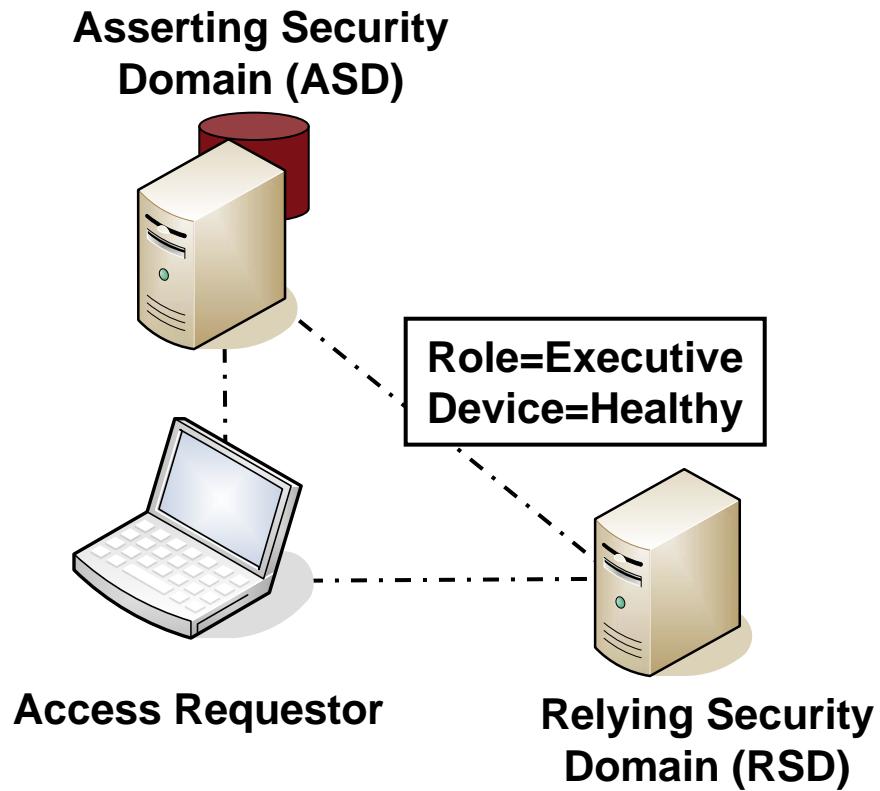
- Web SSOステータスと状態の情報
- ヘルスチェック情報を含めたローミング

どうやってやるのか？

- SAMLプロファイル for TNC

なにに対応しているのか？

- ネットワークローミング
- セキュリティドメイン間での連絡



NACの概念全てを包括するTNC

チェックできる項目

- 認証情報、エンドポイントの状態、振る舞い
- TPMによるハードウェアベースの監査
- 接続前、接続後に渡ってのチェックが可能

ポリシーエンフォースメントの選択肢

- 802.1X、ファイアウォール、VPNゲートウェイ、DHCP、集中管理ソフトウェア

クライアントレス(NACクライアントを利用できない)エンドポイントの管理

- NACに適用できない組み込み機器など
- 例えば、ネットワークプリンタ、IP電話、制御機械、FA、ゲストPC等

NACでの情報の共有

- IF-MAP機能はユーザ情報やチェック項目、振る舞いと言った情報を共有できる
- Federated TNCによるネットワーク環境の連携が可能

どちら辺がTNCのいいところ？

オープン規格

- 誰にも独占されていない = 誰でも取り扱う事が出来る
- オープンのため、広い互換性をもつ
- ユーザーは多くの選択肢を持つことになる
- 常に他者の目にさらされ、洗練される

ネットワークインフラの投資効果を大きく向上させる

- Return-on-Investment (ROI)の向上

将来できな方向性として

- 標準規格としてフルセットを用意する
- Trusted Platform Module (TPM)をサポート

TNCスタンダードに準拠した製品は既に出荷されている！

TNC準拠の製品を持つ参加企業

Access Requestor

McAfee®

Microsoft®

 symantec™

 Juniper®
NETWORKS

 Lumension
SECURITY.

 StillSecure®

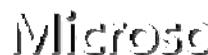
 extreme
networks
 wave®

Policy Enforcement Point

 ARUBA
networks

 extreme
networks

 ProCurve Networking
HP Innovation

 Microsoft®

 enterasys®
Secure Networks

 Juniper®
NETWORKS

 NORTEL

 TRAPEZE
smart mobile.

Policy Decision Point

 symantec™

 Microsoft®
 

 Juniper®
NETWORKS

 ①Labs

 wave

 Lumension
SECURITY.

 StillSecure®

 extreme
networks

 McAfee®

Metadata Access Point

 Infoblox

 Juniper®
NETWORKS

Sensors, Flow Controllers

 ArcSight

 Great Bay
Software Inc.

 ARUBA
networks

 TRAPEZE
smart mobile.

 Juniper®
NETWORKS

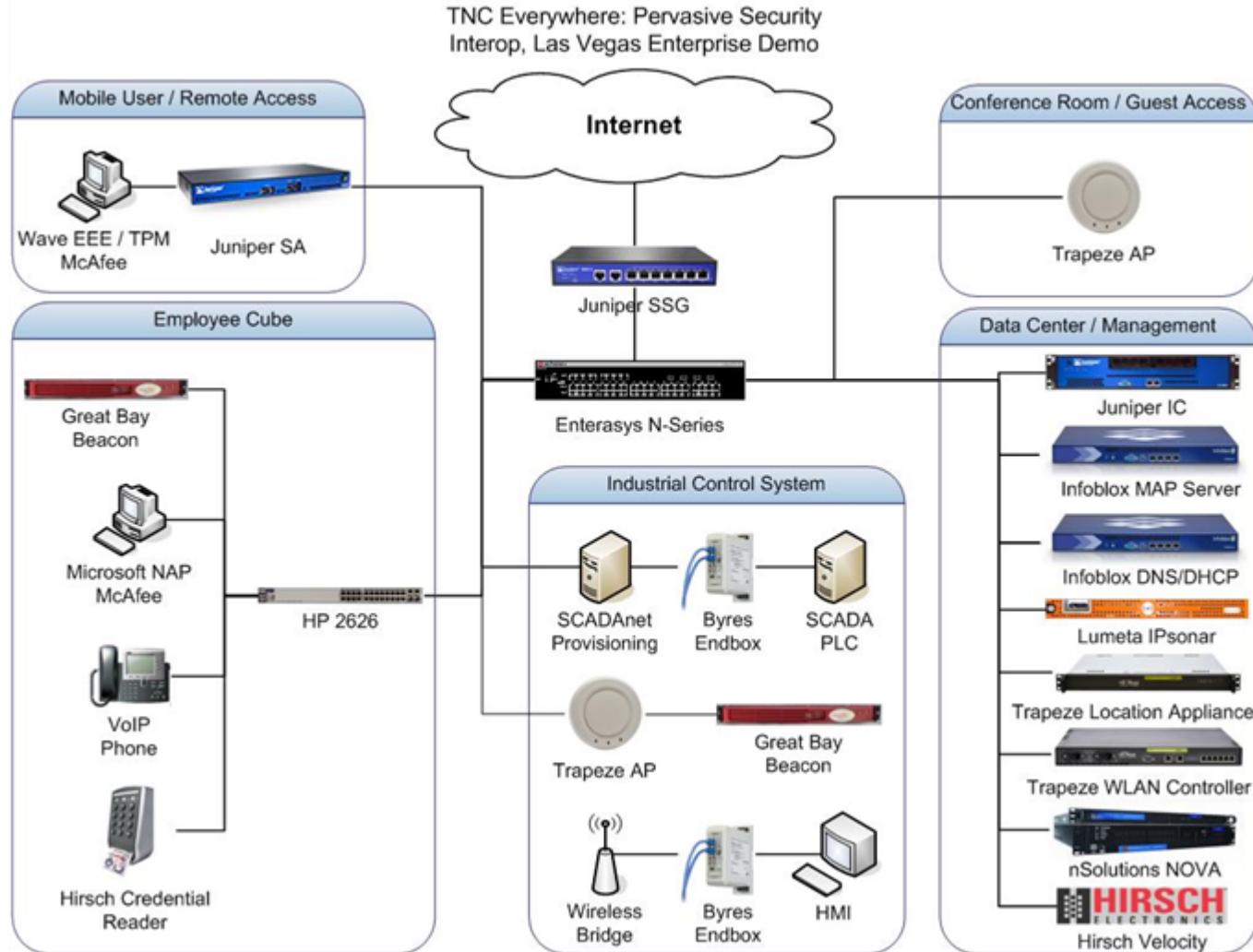
 GLUMETA®

 nSolutions
Effortless Infrastructure

 HIRSCH
ELECTRONICS

 insightIX
TOFINO™

TNC準拠の製品によるデモネットワーク



Microsoft NAP and TNC



IF-TNCCS-SOH Standard

- Developed by Microsoft as Statement of Health (SoH) protocol
- Donated to TCG by Microsoft
- Adopted by TCG and published as a new TNC standard, IF-TNCCS-SOH

Brings Microsoft NAP into TNC Architecture

- NAP servers can health check TNC clients without extra software
- NAP clients can be health checked by TNC servers without extra software
- As long as all parties implement the open IF-TNCCS-SOH standard

Availability

- Built into Windows Vista, Windows 7, Windows Server 2008, and Windows XP SP 3
- Also built into products from other TNC vendors

Implications

- Single agreed-upon open standard client-server NAC protocol
- True client-server interoperability (like web browsers and servers) is here
- Industry (except Cisco) has agreed on TNC standards for NAC

IETF and TNC

IETF NEA(Network Endpoint Assessment) WG

- Goal: Universal Agreement on NAC Client-Server Protocols
 - Co-Chaired by Cisco employee and TNC-WG Chair

Adopted TNC protocols as WG drafts

- IETF calls them PA-TNC and PB-TNC
- TCG calls them IF-M 1.0 and IF-TNCCS 2.0
- Cisco Engineer Is Co-Editor

Expected to reach RFC status in 2009

まとめ

NACは重要な問題を解決できる

- 今日存在する様々なモバイルデバイス、ユーザーまで含めて一貫したポリシーでのアクセスコントロールを行うことが出来る

TNC = オープンスタンダードなNACソリューション

- マルチベンダー環境での互換性があることがNACでは非常に重要
- 最大の投資効果を得るために既存のインフラや製品を活用できる方が良い
- ベンダーによる囲い込みはもっとも避けるべき事である

TNCはもっとも強力なセキュリティ手段の一つである

- ルートキット対策が可能である(ルートキットを防ぐのは非常に難しい)
- 常に他者の目にさらされているため、洗練され続ける

TNCスタンダードは広い支持を受けている

- たくさんのベンダー、オープンソース、IETF