

エンドポイントのセキュリティ統制による 情報漏えい対策とコンプライアンス対応強化

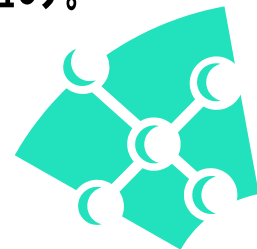
ソリューション営業統括部
セールスマーケティング2部4課
正躰 弥一郎

Contents

- 企業ネットワークにおける新たな脅威とNACソリューションの役割の変遷
- いま、NACソリューションに求められるセキュリティ課題
- 従来のNACソリューションが持つ様々な問題
- 最先端の技術が実現するNACソリューション
- 製品紹介

NAC (Network Access Control) とは

- NACとは…
 - 企業ネットワークにおけるセキュリティ脅威を減少させるために、企業のセキュリティポリシーに適合している端末であるかどうかをチェックし、必要に応じて、その**個体を隔離**し、適切な処置を能動的に行う仕組み。
 - 「個体を隔離」する必要性…
 - 健全な個体への感染防止
 - 状態ごとの処置の必要性

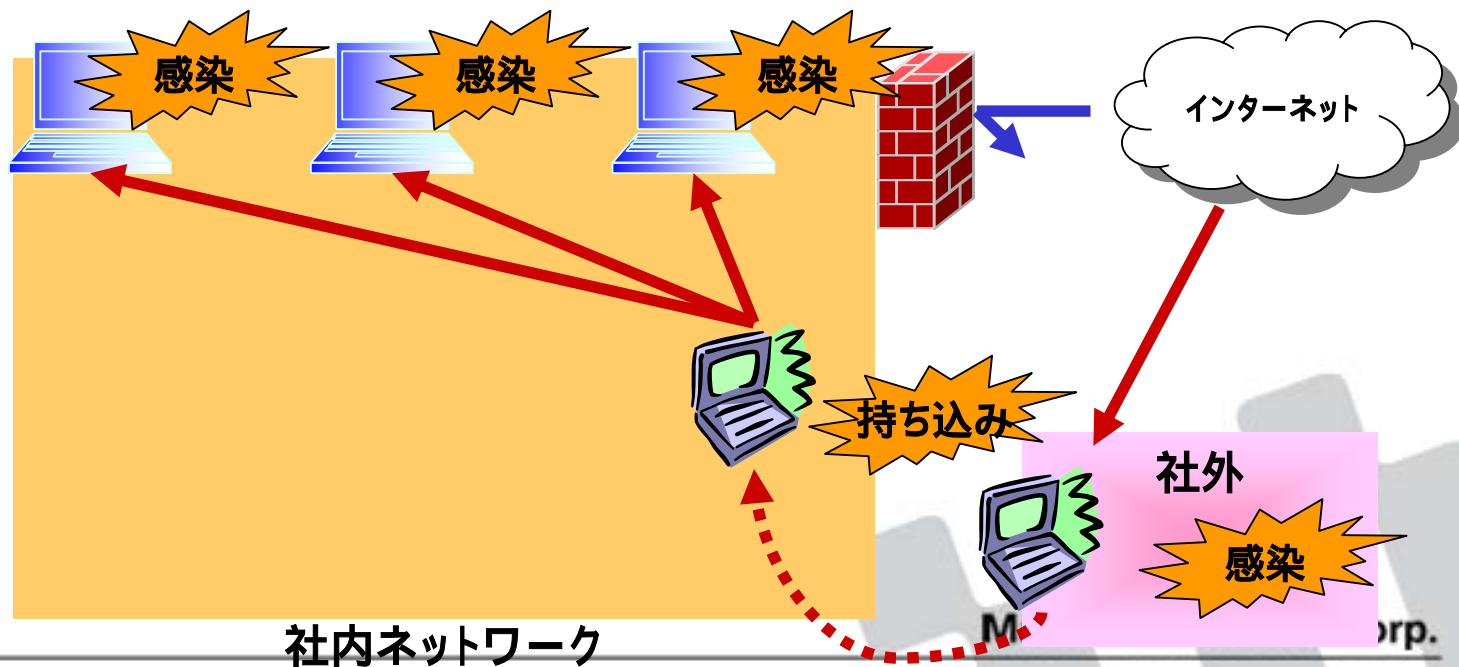


検査(チェック)、隔離(個体隔離)、治療がキーワード

企業ネットワークにおける新たな脅威 と NACソリューションの役割の変遷

従来のNACソリューションが対応する脅威

- 外部から持ち帰った端末(エンドポイント)により、社内にウィルスが持ち込まれること



従来のNACソリューションの役割

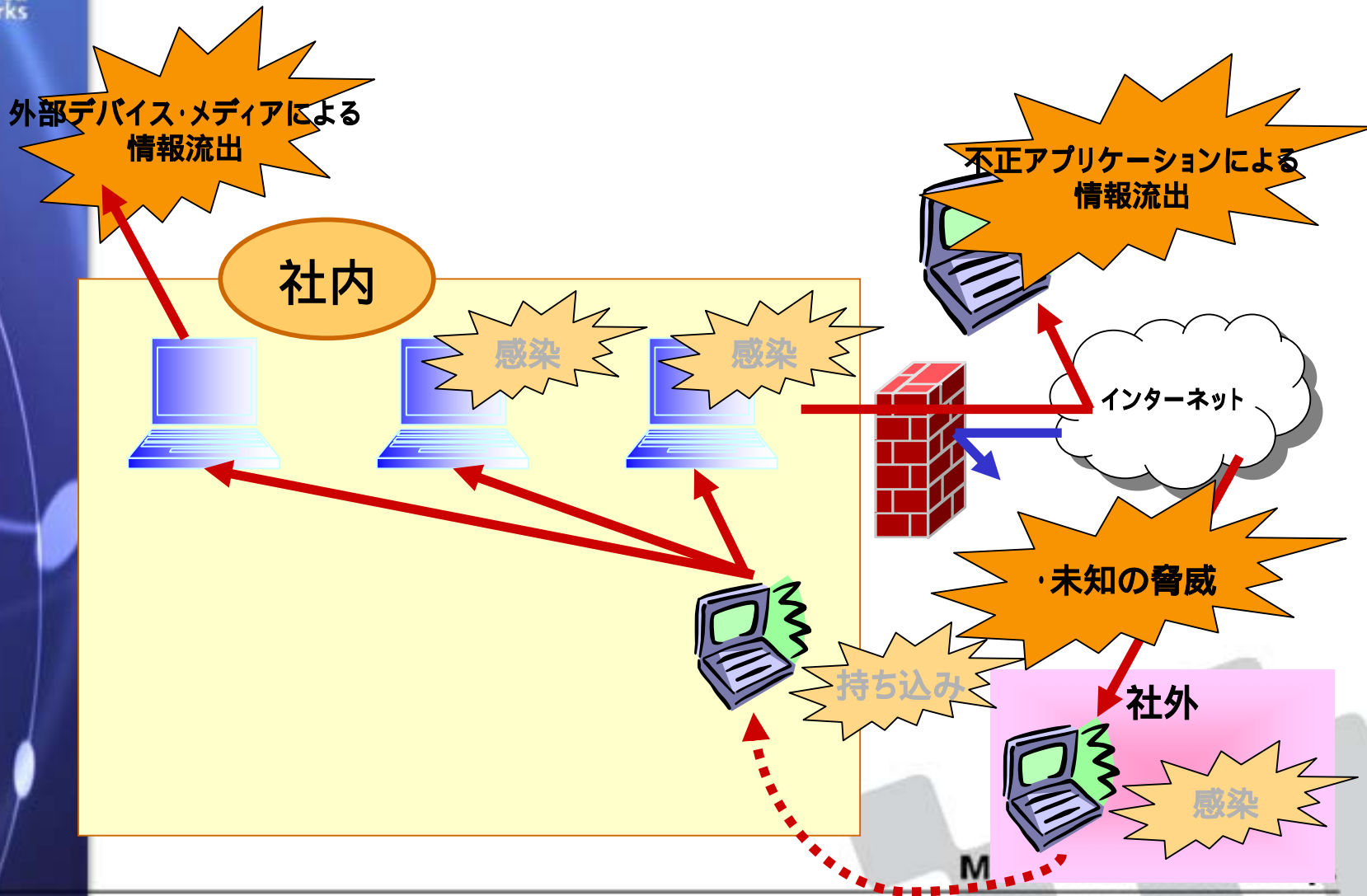


- 接続端末の健全性チェック
 - ウィルス定義ファイルの更新
 - OSアップデート
- ポリシー不適合端末への処置
 - 健全性チェック結果に基づいた端末隔離
 - 治療(パッチ配信、定義ファイル更新)の強制

従来のNACソリューションでは防ぎきれない 脅威

- ゼロデイアタックに対する端末保護
- モバイル環境における端末ポリシーの徹底
- 外部記憶メディアやモバイル機器の無断使用/データ移行による情報漏えい
- 不正ツール利用による情報の漏えい
- スパイウェア/クライムウェアによる情報の漏えい
- 関連会社、パートナー企業などの端末への対策

NACソリューションにおける新しい脅威



クライアント(エンドポイント)への攻撃



- **ゼロデイアタック**

- **ゼロデイアタックとは**

- ソフトウェアにセキュリティ上の脆弱性(セキュリティホール)が発見されたときに、問題の存在自体が広く公表される前にその脆弱性を悪用して行なわれる攻撃

- **ポイント**

- 脆弱性の発見からウィルスによる攻撃までの時間が短い
 - セキュリティパッチ、アンチウィルスのパターンファイル等による事後対策では防げない

クライアント(エンドポイント)を起点とする脅威

- 情報漏えい

- 不正アプリケーション起因型

- スパイウェア/クライムウェア

- ユーザーの認識や承認なく、情報収集とそれらの外部送信を行う。
 - フリーソフトやファイル交換ソフト等に潜んでいる可能性がある。

- P2P

- 不特定多数間での情報交換を直接行う。



クライアント(エンドポイント)を起点とする脅威

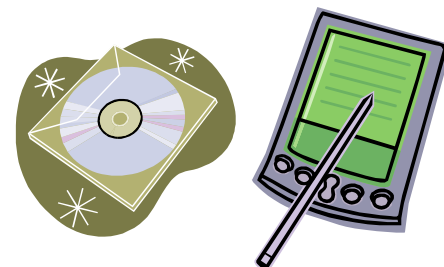
- 情報漏えい

- 外部デバイス、メディア起因型

- 情報の持ち出し

- 端末起因型

- 本来社内LANへの接続を許可しない端末が、ネットワークに接続し情報を持ち出す。
- 接続許可端末のユーザーが故意にデータを持ち出す



つまり・・・

- エンドポイントに対する新しい脅威の出現と従来のセキュリティ対策の限界
- ということは・・・

NACに対する要求、役割も変わってきている。

NACソリューションの新たな役割

従来の役割

・健全性チェックと接続端末の**隔離・治療**

加えて...

更なる役割

エンドポイントへの様々な脅威に対し対応できる
機能を有していること

NACソリューションに対する その他の課題

柔軟なポリシー設定

- 従来の課題点
 - 限定的な健全性チェックポリシー
 - ウィルス対策ソフト
 - セキュリティパッチ
- 企業セキュリティポリシーへの準拠
 - 求められるセキュリティポリシーの徹底
 - 情報漏えい対策ソフトの利用
 - 禁止アプリケーションの有無
 - 他

特定のネットワーク機器への非依存性

- 従来の課題点
 - 特定のベンダ機器に統一する必要性
 - ソリューション対応機器の限定
- 導入によるインパクト
 - 初期コスト
 - 運用/オペレーションの複雑化
 - 機器メンテナンスの煩雑化

多彩な検疫方式への対応

- 従来
 - NAC対応方式が限定
- 既存環境への対応
 - ネットワークの大幅な構成変更が発生
 - 大規模環境への対応難
 - ワンシステムで対応できず、運用が煩雑

従来のNACソリューションが持つセキュリティ的な盲点を解決する

- 「隔離」に対する安全性？
 - 隔離セグメント内でウィルスに二次感染

cf) 病院に行って、逆に風邪をうつされる。

最先端の技術が実現する NACソリューション

ソリューション

- **セキュリティプロテクション機能を提供するソリューション**
 - NACソリューションは、プロアクティブなセキュリティ対策
 - 情報漏えいの可能性となる正規以外のユーザを未然に排除するソリューション
 - ウィルス感染のリスクとなる可能性の高い端末を未然に排除するソリューション



プロアクティブ(事前予防的)対処であるために



ゼロデイアタックに対するプロテクション機能が必要！

ソリューション

- セキュリティプロテクション機能を提供するソリューション
 - セキュリティリスクへの対策
 - 脅威・脆弱性レベル / 情報資産価値レベル
 - NACシステムが守るもの
 - ポリシー違反端末の、社内ネットワークへの接続だけ？

企業ネットワークにおいて脅威脆弱性レベルの
高いポイント

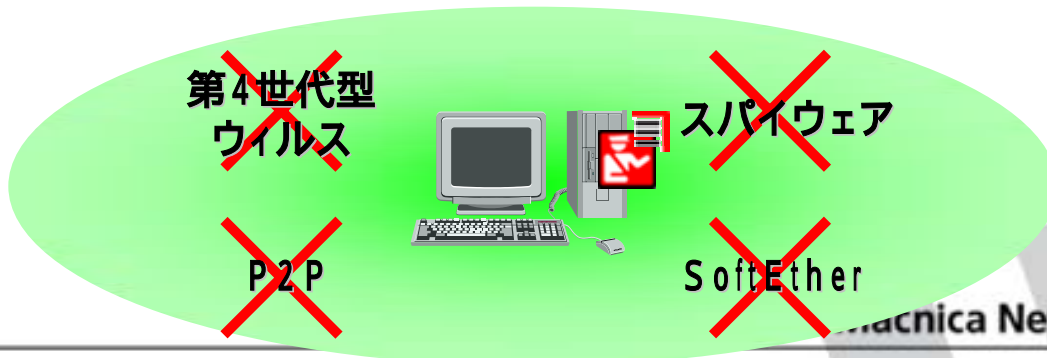
エンドポイント



エンドポイントへのセキュリティプロテクションが必要！

ソリューション

- アプリケーションベースでのアクセスコントロール機能を提供するソリューション
 - 決められたアプリケーション通信のみを許可するホワイトリスト方式
 - アプリケーションセンタリックな仕組みによって、決められたアプリケーションによる通信のみを許可する、セキュリティの高い運用を行うことが可能
 - 不正ネットワークアプリケーションによる通信の禁止
 - PFWルールの設定により、P2Pソフト、仮想VPNソフト、あるいはスパイウェアによる不正な通信を禁止することが可能
 - P2P経由でのウィルス感染、スパイウェアによる情報漏えいの防止



ソリューション

- デバイスのアクセスコントロール機能を提供するソリューション
 - ポリシーで定められた以外の外部記憶デバイス使用を制限
 - モバイルコンピューティング端末使用の制限
 - ポリシー・運用で定められたネットワークアダプタ以外の通信を制限



従来の
NACソリューション

- 健全性チェック
- 健全性不適合端末の隔離、治療



新たな脅威へ対応が出来ない！！

- ゼロデイアタック
- 情報漏えい

エンドポイントへの対応力
を持ったNACソリューション



実現

- ・情報漏えいの防止
- ・コンプライアンス対応強化

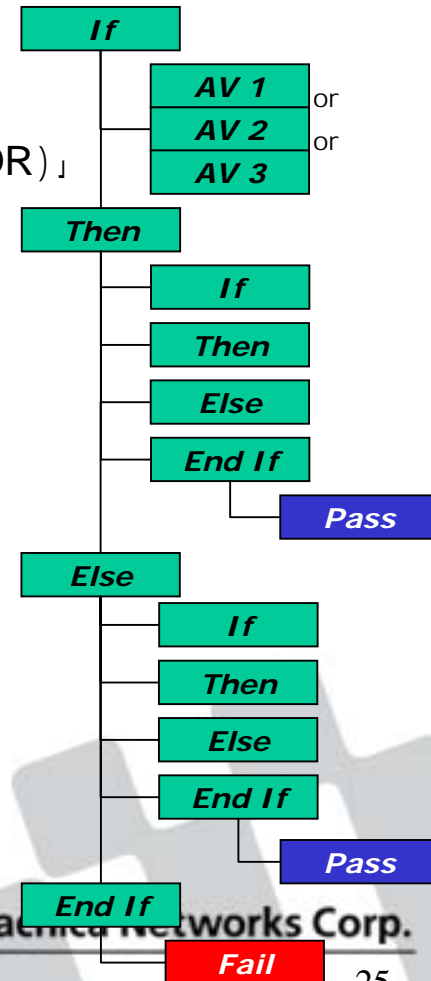
- アプリケーションベースのアクセスコントロールを実現する
- デバイスのアクセスコントロールを実現する
- etc

ソリューション

● 柔軟なポリシー設定を実現するソリューション

- 複数条件への対応 (AND/OR条件)
 - 複数のアンチウイルスソフトを使用する企業
 - 「すべてを満たす (AND) / どれかを満たす (OR)」

- 複雑な条件設定 (条件分岐) へ対応する柔軟性
 - 脆弱性に応じた最適な対処 (治療) の実施
 - あらゆる条件設定、治療設定への対応
 - 「IF/THEN/ELSE」による階層設定



ソリューション

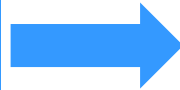
- マルチベンダ対応のソリューション
 - なぜマルチベンダ対応が必要か？
 - 企業ネットワークにおける機器は、必ずしも統一されていない
 - マルチベンダ対応のための検討項目
 - VPN機器
 - エッジスイッチ
 - 無線LANスイッチ
 - ウィルス対策ソフト
 - その他の各種セキュリティ製品・ソフトウェア

ソリューション

- Universal NAC対応ソリューション

パーソナルファイアウォール
セキュリティゲートウェイ
IEEE802.1x認証
DHCP
Cisco NAC

(Universal NAC)



有線LAN

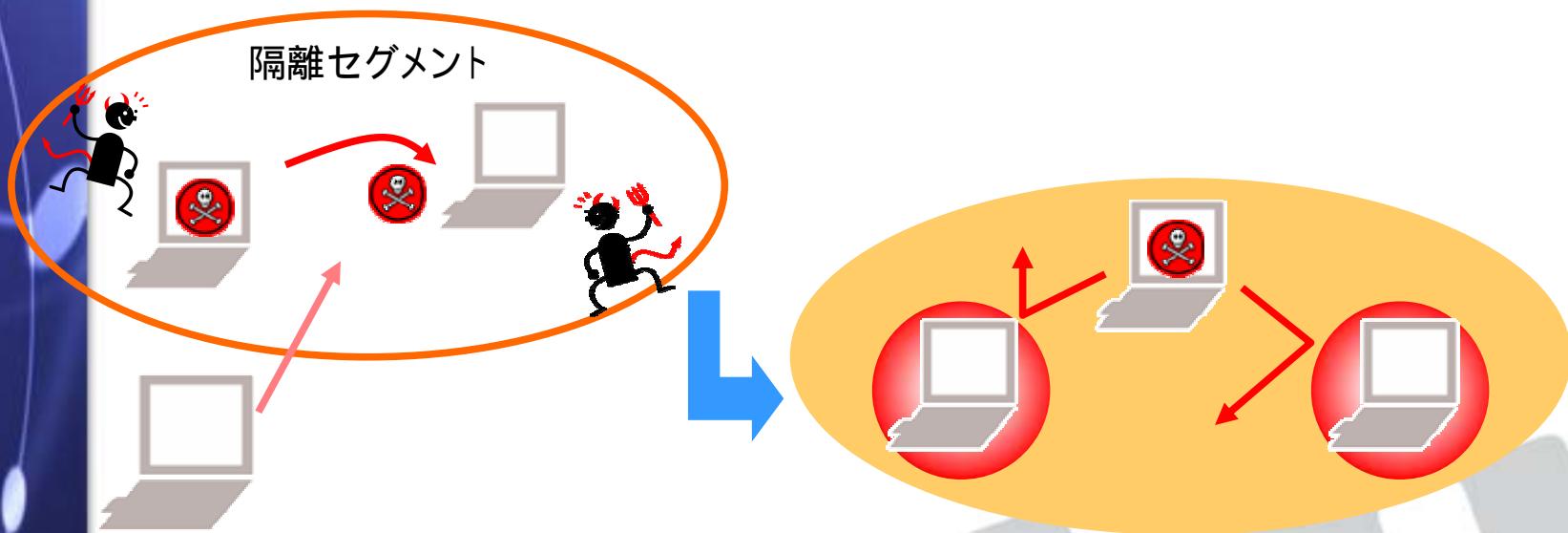
無線LAN

リモートアクセス

- 複雑かつ大規模なコーポレートネットワーク環境に対応するためには、様々なNAC方式を同時に組合せてサポートする必要がある。

ソリューション

- 二次感染を防止するソリューション
 - 隔離セグメント(エリア)が危険地帯
 - 隔離されたセグメント内で、2次感染を引き起こす可能性が大きい

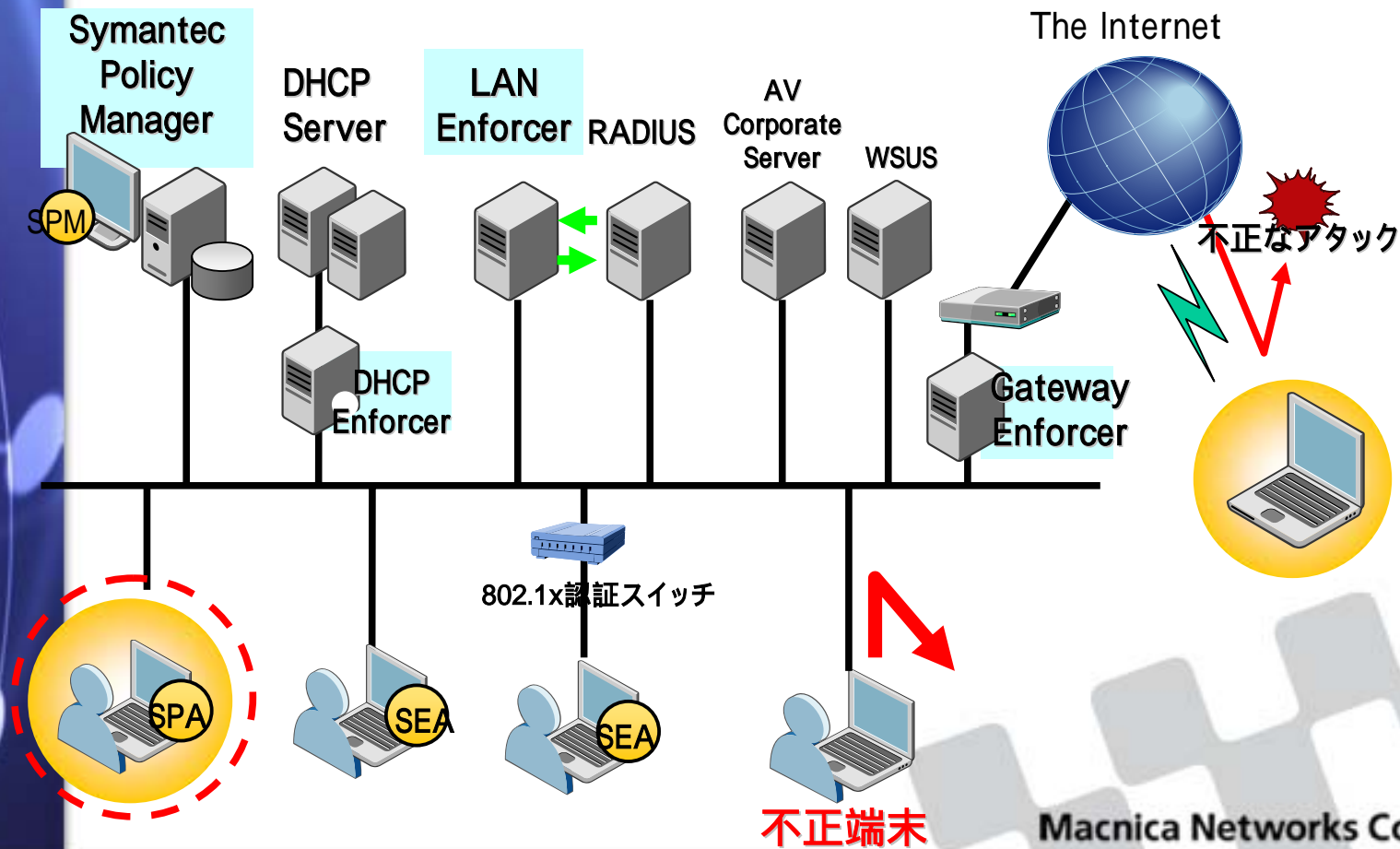


個体を隔離することが必要！

製品紹介

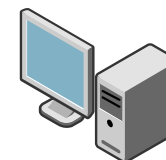
- Symantec Sygate Enterprise Protection
- Symantec Network Access Control

システム構成イメージ



SSEP/SNAC コンポーネント構成

Enforcement	<ul style="list-style-type: none"> ▪ CNAC, Self Enforcement ▪ DHCP/LAN/Gateway/API
Host Integrity	<ul style="list-style-type: none"> ▪ HI and Remediation
HIPS	<ul style="list-style-type: none"> ▪ OS Protection (File, Registry, Process Control) ▪ System Lockdown (Application Control) ▪ Buffer Overflow Protection ▪ Peripheral Device Control
Adaptive Policies	<ul style="list-style-type: none"> ▪ Auto-Location Switching
IPS	<ul style="list-style-type: none"> ▪ Signature-based IPS
PFW	<ul style="list-style-type: none"> ▪ Desktop Firewall



Symantec Policy Manager (SPM)



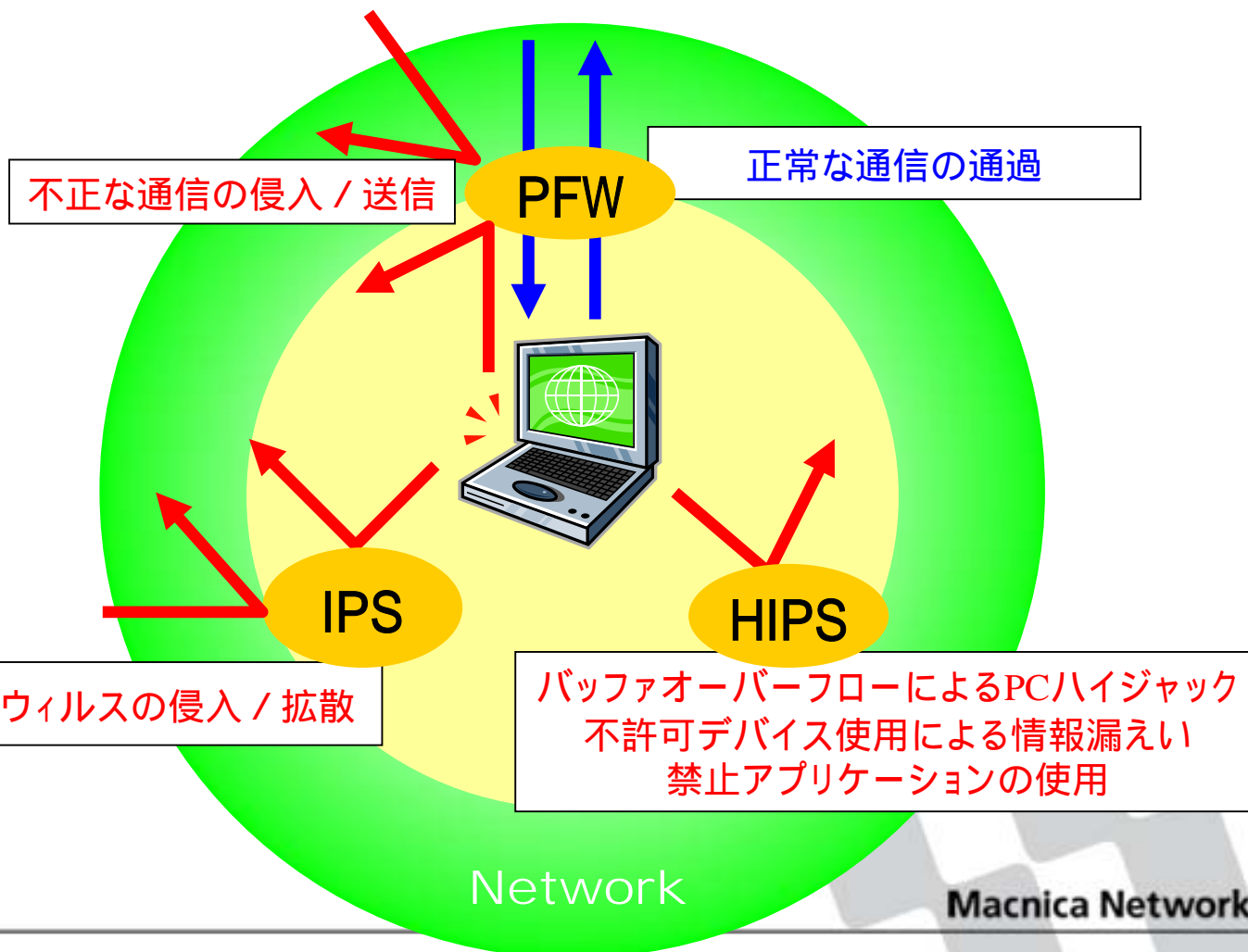
Symantec Protection Agent (SPA)



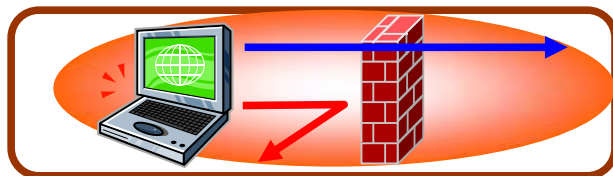
Symantec Enforcement Agent (SEA)

Macnica Networks Corp.

SSEP エンドポイントプロテクション

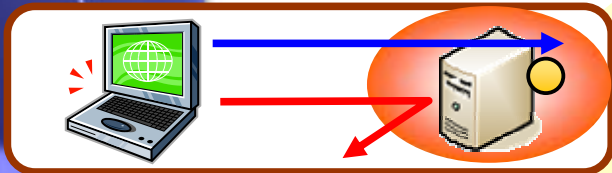


SNAC Universal NAC コンセプト

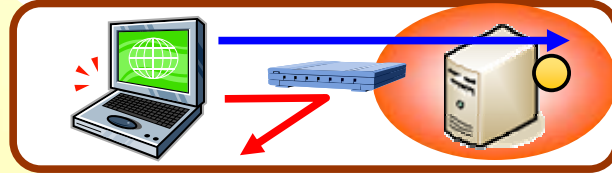


パーソナルファイアウォール方式

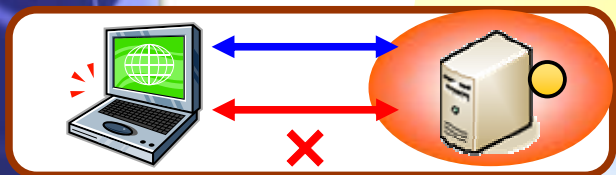
セキュリティゲートウェイ方式



802.1xスイッチ連携方式

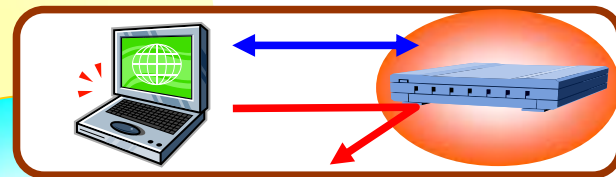


隔離



DHCP方式

検査



CNAC連携方式

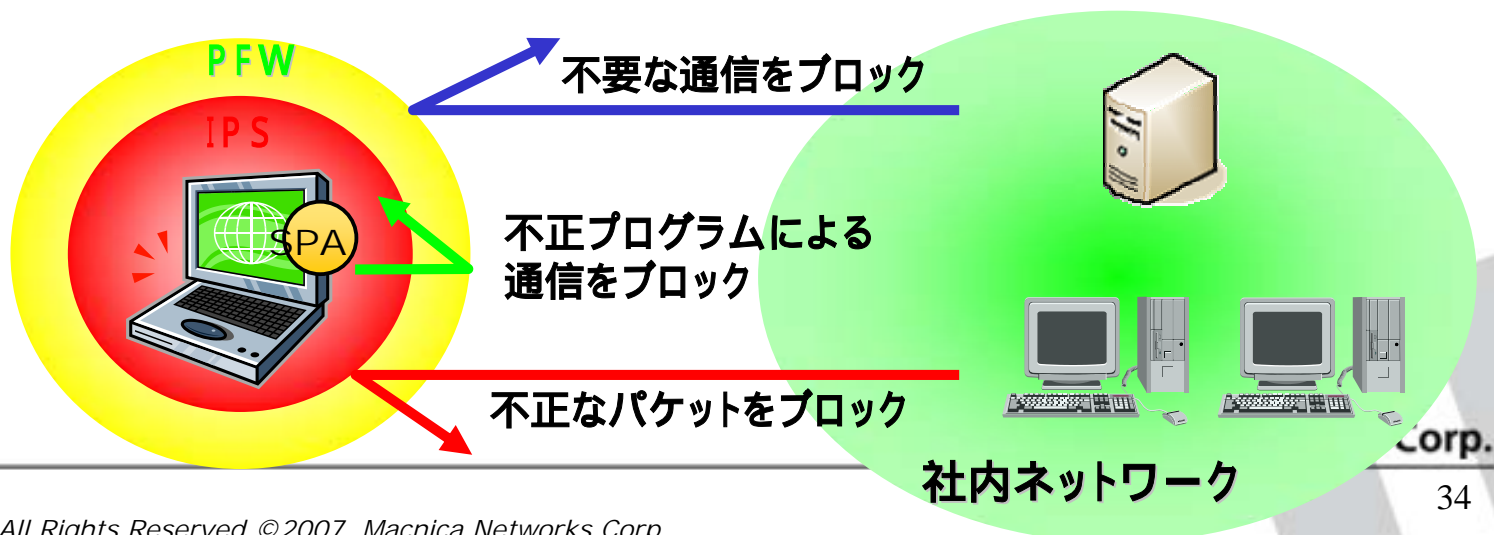
治療

健全性チェック・治療(ホストインテグリティ)

機能概要

パーソナルファイアウォール&IPS

- PFW & クライアントIPS
 - アプリケーションによる通信を個々に制御
 - アウトバウンド、インバウンドの通信を制御
 - IPS (Intrusion Prevention System) により不正なパケットを防御
 - シグネチャのダウンロード、カスタマイズ



機能概要

HIPS

- Host-based Intrusion Prevention System
 - OSプロテクション
 - ファイル、レジストリ、プロセスへのコントロール
 - システムロックダウン
 - アプリケーションのコントロール
 - バッファオーバーフロープロテクション
 - プロセスに対するバッファオーバーフロー攻撃の防御
 - デバイスコントロール
 - USBデバイスの制御

機能概要

ホストインテグリティ

- ウィルス対策ソフトの常駐、定義ファイルの更新
- OSごとのサービスパック
 - パッチ適用の有無
- アプリケーションの常駐
- 任意のファイル・任意のレジストリ値の有無
- 補完(治療)動作
- その他特徴
 - IF_THEN_ELSE設定による階層的な条件設定
 - ポップアップメッセージのカスタマイズ

機能概要

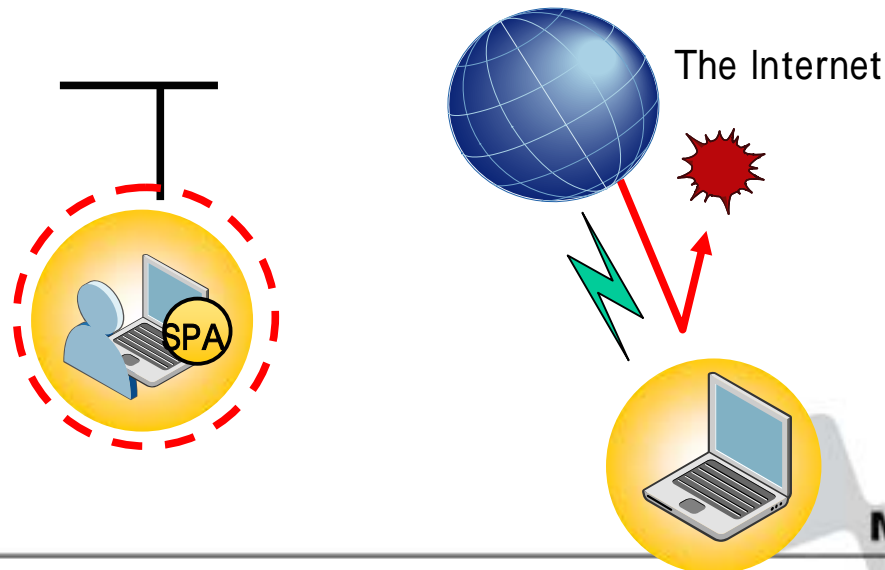
アダプティブポリシー

それぞれの接続環境(ロケーション)に応じたセキュリティリスクに最適なセキュリティポリシーを適用する

ことで、 unnecessaryな通信を制御し、不正なアクセス/アタック等から防御



Agentはロケーションを自動判断し、ダイナミックに切り替えることが可能



機能概要

- 管理サーバ(Symantec Policy Manager)
 - ポリシー設定の一元管理
 - PFWポリシー / IPSシグネチャ / OS Protectionルール / Host Integrityルール
 - ログ監査・レポーティング
 - 各クライアントから収集されたログ管理
 - セキュリティログ/トラフィックログ/パケットログ/Behaviorログ他
 - レポート作成機能
 - 他

機能概要

- Network Access Control
 - パーソナルファイアウォール(PFW)方式
 - セキュリティゲートウェイ方式
 - 802.1x認証スイッチ連携方式
 - DHCP方式

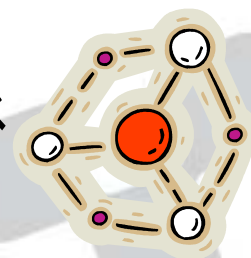
ポイント まとめ

- 新たに出現する様々な脅威に対して
 - ゼロデイアタック(未知の攻撃)への対策ができる
 - 情報漏えい対策が出来る
- これまで導入の課題とされていた項目についても
 - 柔軟なポリシー設定ができる
 - システム機器、ネットワーク環境へ柔軟に対応できる。
 - 盲点(隔離先での二次感染)



ポイント まとめ

- **様々なソリューションをご提供**
 - エンドポイントへのセキュリティプロテクション
 - アプリケーションごとのアクセスコントロール
 - デバイスコントロール
 - 柔軟なポリシー設定
 - マルチベンダー対応のソリューション
 - Universal NACシステムの実現
 - “**個体隔離**”を実現する強固なセキュリティレベル



ご清聴ありがとうございました。