# 4.1 ネットワークアクセス保護（NAP）とは

## 4.1.1 ネットワークアクセス保護（NAP）の概要

ネットワークアクセス保護（NAP；Network Access Protection）は，検疫あるいは検疫ネットワークと呼ばれるセキュリティ技術の一種です．検疫は，Windows Server 2003のRRAS（Routing and Remote Access Service）に初めて実装されました．Windows Server 2008に実装されたNAPは，Windows Server 2003 の検疫を大幅に機能強化したものです（Windows Server 2003の検疫とNAPの違いについては，「参考 Windows Server 2003検疫制御とNAPの違い」を参照してください）．

検疫は，MS Blasterワームの流行以降に考え出された，ネットワークを保護するための，比較的新しいセキュリティ技術です．例えば，セキュリティ設定に問題があり，すでにウィルスやワームに感染しているユーザーの個人所有のノートPCがあるとします．このコンピュータをユーザーが会社に持ち込んで，社内ネットワーク接続した途端，ウィルスやワームの被害が社内ネットワークに及びます．あるいは，社内ネットワークに直接接続するのではなく，こうしたコンピュータがVPN経由で，社内ネットワークにリモートアクセスした場合も同様の被害が発生する恐れがあります（**図4.1**）．

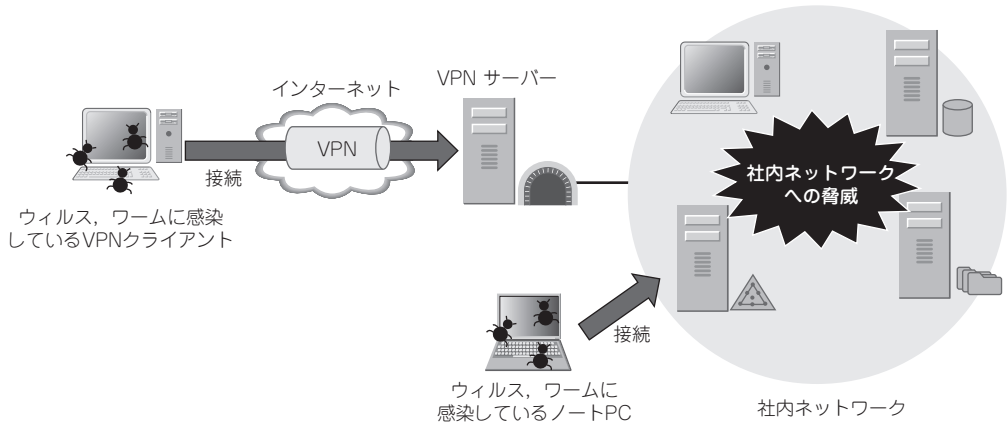


**図4.1　社内ネットワークへの脅威**

しかし，企業の管理者がこうした個人所有のノートPCや，自宅に設置されたコンピュータのセキュリティ設定まで，集中管理することは困難です．さらに，こうしたセキュリティ侵害は，ファイアウォールやDMZ（非武装地帯）などのエッジセキュリティ

では，通常防ぐことができません．

そこで考え出されたセキュリティ技術が検疫，あるいはNAPです．

NAPを使用すると，コンピュータが社内ネットワークに接続する際，そのコンピュータが企業のセキュリティ要件を満たしているか検査し，セキュリティ要件を満たしていない場合，リソースへのアクセスを制限することで社内ネットワークを保護します．さらにNAPにはセキュリティ要件を満たしていないコンピュータに対し，セキュリティ要件を満たすように自動構成する自動修復機能が実装されています．



## 4.1.2　ネットワークアクセス保護（NAP）のアーキテクチャ

NAPでは，**図4.2**のようにネットワークを論理的な三つのネットワークに分割します（ネットワークではなく，「ゾーン」と呼ぶ場合もあります）．

セキュリティで保護されたネットワークは，社内サーバーなど保護対象となるリソースを配置するネットワークです．

境界ネットワークは，決められたセキュリティ要件を満たしていない非準拠クライアントでも接続できる緩衝地帯のネットワークです．境界ネットワークには，修復サーバーを配置します．修復サーバーとは，非準拠クライアントがセキュリティ要件を満たすために必要なコンポーネントを持つサーバーや，トラブルシューティング用の情報をユーザーに提示するWebサーバーなどです．

制限付きネットワークは，セキュリティ要件に非準拠，あるいは，NAPの機能に対

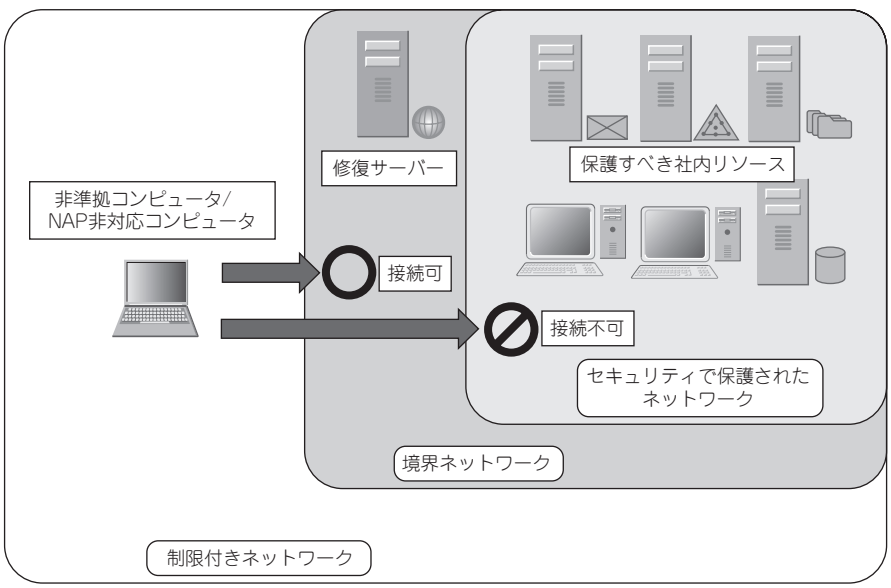


**図4.2　NAPの論理ネットネットワーク**

応していないコンピュータが配置されるネットワークです．

制限付きネットワークから境界ネットワークへの接続は可能ですが，制限付きネットワークからセキュリティで保護されたネットワークへの接続はできません．これによりセキュリティ要件を満たしていない非準拠クライアントはセキュリティで保護されたネットワークに接続できないため，もし，制限付きネットワークに所属するクライアントがワームやウィルスに感染していたとしても，危険にさらされるのは，境界ネットワークだけで，社内のリソースを安全に保護することができます．

NAPの検査にパスしたセキュリティ要件を満たしている準拠クライアントは，セキュリティで保護されたネットワークに所属することになり，セキュリティで保護されたネットワークのコンピュータにアクセスすることができます．

NAPのコンポーネントには，NAPクライアント，NAP強制サーバー（アクセスデバイス），ネットワークポリシーサーバー（NPS）があります（**図4.3**）．Windows Server 2008，Windows Vista，Windows XP SP3をNAPクライアントとして構成することができます．

NAP強制サーバーは，アクセスデバイスとも呼ばれ，実際にNAPクライアントに制限を設けるサーバーです．NAP強制サーバーは，NAPの実施オプションにより異なり，DHCPサーバーであったり，802.1x対応のスイッチであったり，VPNサーバーであったりします．

ネットワークポリシーサーバーは，Windows Server 2008上に構築されます．ネットワークポリシーサーバーには，クライアントの正常性をどのように検証するか条件と制約のポリシーが定義されています．また必要に応じてこれらのコンポーネントに加え，

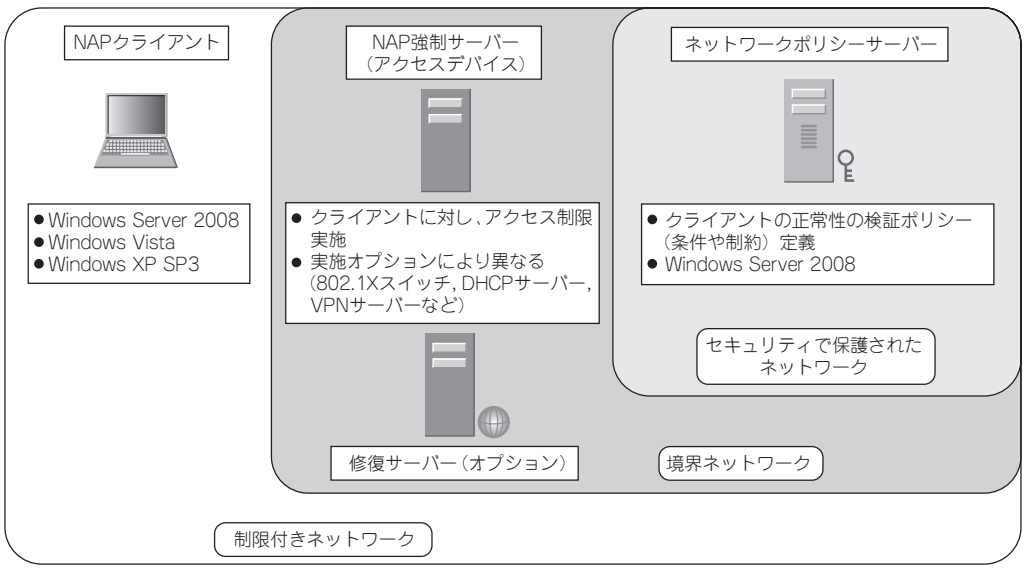


**図4.3　NAPのコンポーネント**

修復サーバーを構築することもできますが，修復サーバーはオプションの構成であり，NAPに必須なコンポーネントではありません．

次にこれらのコンポーネントがどのように動作するかを解説します．

企業ネットワークに接続したNAPクライアントは，NAP強制サーバーに対し，自分の状態を表す正常性ステートメント（SoH；Statement of Health）を送信します．NAP強制サーバーは，RADIUSプロトコルを使用して，正常性ステートメントをネットワークポリシーサーバーに転送します．

ネットワークポリシーサーバーは，転送された正常性ステートメントと定義されたポリシーを比較し，そのクライアントのアクセスを許可するのか拒否するのか決定をします．もし正常性ステートメントの検証の結果，セキュリティ要件を満たしていない非準拠クライアントであると判断されると，NAP強制サーバーによりNAPクライアントはアクセス制限され，セキュリティで保護されたネットワークには接続できません．

クライアントの通知エリアには「ネットワーク要件を満たしていません」というメッセージが表示され（**図4.4**），メッセージをクリックすると，「ネットワークアクセス保護」ウィンドウが表示され，現在のNAPの状態を確認することができます（**図4.5**）．

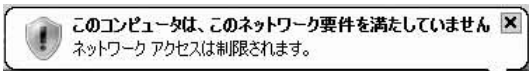


**図4.4　非準拠クライアントに対する「ネットワーク要件を満たしていません」メッセージ**

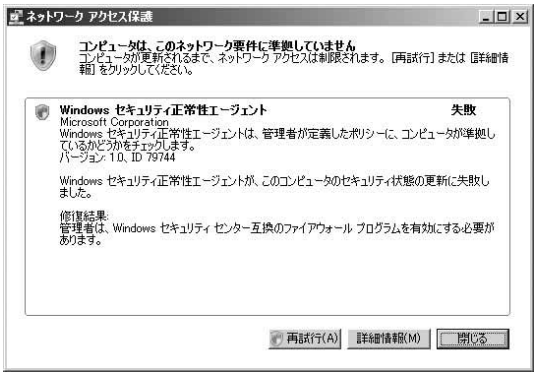


**図4.5　非準拠クライアントに対する「ネットワークアクセス保護」ウィンドウ**

トラブルシューティング用の情報を利用者に提供するためのWebサーバーを修復サーバーとして構築し，ネットワークポリシーサーバーで，この修復サーバーをトラブルシューティング用URLとして設定すると，利用者は，[詳細情報]ボタンをクリックすることで，このWebページを表示し，セキュリティ要件を満たすのに必要な手順を確認することができます．さらに更新プログラムやウィルス対策ソフトウェア，パターンファイルなど修復に必要なコンポーネントを配置するサーバーをネットワークポリシーサーバー上で修復サーバーとして設定することで，非準拠クライアントはこれらの修復サーバーに接続することが可能になります．