導入事例
「QAWを使って未知のPCを検知/遮断！」

2011年1月26日

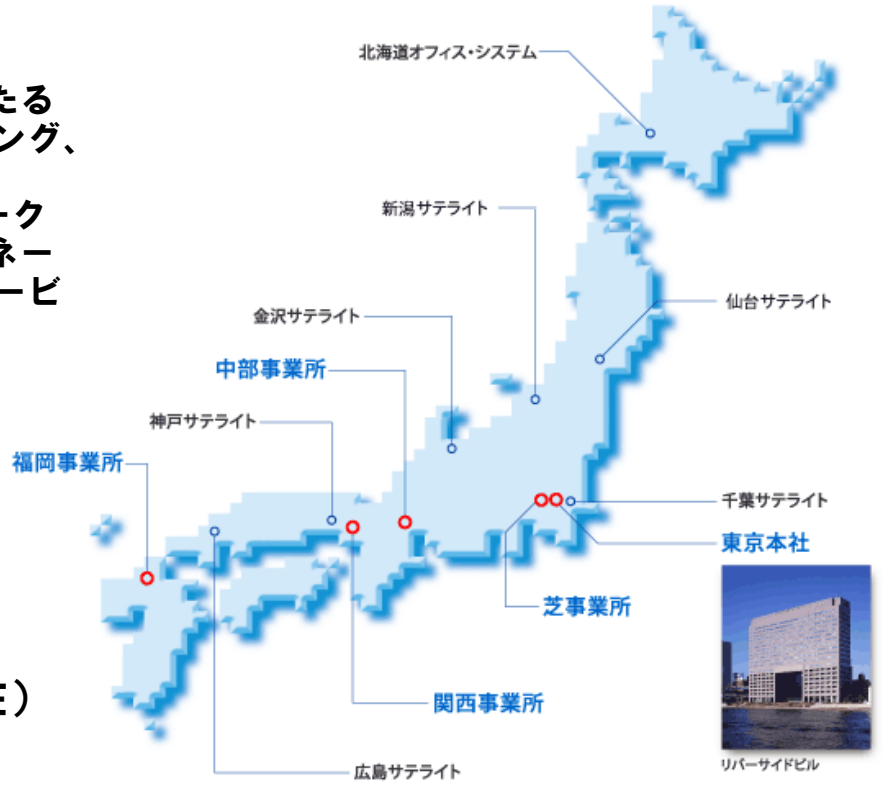
日本オフィス・システム株式会社
情報システム
田中　英樹

会社概要

お客様のITライフサイクル全般に対して、
ワンストップ・サービスを提供しています。

JASDAQ
証券コード 3790

社名	日本オフィス・システム株式会社
所在地（本社）	東京都中央区日本橋箱崎町３６－２　リバーサイドビル
設立	1982年10月1日
代表者	代表取締役会長　尾嶋　直哉
事業内容	お客様のITライフサイクル全般にわたるサービス、すなわち、コンサルティング、エンタープライズ・システムインテグレーション・サービス、ネットワーク基盤構築、保守サービスおよびITマネージメント・サービスといった情報サービス事業と、システム構築に係るソフトウェア、コンピュータおよび関連機器を販売するシステム販売事業を行っています。
拠点	全国１２ヶ所
従業員数	６００名（2010年6月30日現在）



アジェンダ

- 検疫ネットワーク
- ＮＯＳ検疫ネットワーク
- 本稼働までの手順
- 他社製品のデメリット
- Viper（ＱＡＷ機能）
- Viperシステム構成概要
- 現行システムの追加内容
- ホワイトリスト画面
- 遮断設定画面
- Viperによるメリット
- 苦労した点
- 現在の運用
- まとめ

検疫ネットワーク

検疫ネットワークとは

社内ﾈｯﾄﾜｰｸにアクセスしようとするクライアントＰＣがあらかじめ定められたセキィリティ・ポリシーなどのルールに適合するかをチェックする仕組み。

しかし…(他社製品だと)

インフラをアップデートする必要があるため、

コストがかかりすぎる。

また、あまりに複雑すぎて理解しにくい。

NOS検疫ネットワーク

- 目的

１．許可されていなＰＣの排除

　　許可されていないＰＣとは、情報システム管理外ＰＣ

２．社内ルールに適合したＰＣのみの接続

　　共通ソフトの導入と不正ソフトの未導入の確認

- 要件　：　検知　・　遮断

　　ＮＯＳ社内ﾈｯﾄﾜｰｸに接続されているＰＣ全て検知

　　不正ＰＣの強制的な排除・遮断

本稼働までの手順　(2010年5月～10月)

- 5月　検疫システムのシステム選定
- 6月　システム構築
- 7月　機器購入(サーバー・ＰＣ・ラック等)
  ＱＡＷサーバーの準備
  Ｖｉｐｅｒノードサーバー（ＰＣ）の準備
- 8月　検証作業（テスト環境の構築）
- 9月　ＱＡＷサーバー＆Ｖｉｐｅｒノードサーバーの
  設置・稼働（検疫のみ）
  クライアントのＱＡＷの導入
  （ホワイトリスト作成）
- 10月中旬　設定の実施

他社製品のデメリット

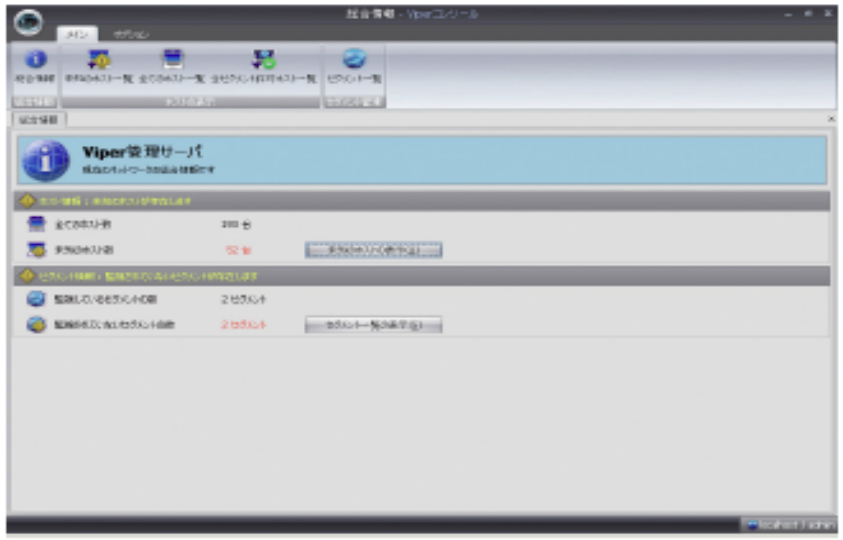
他社の検疫システムと比較すると

- サーバー（ＤＨＣＰ・認証サーバー）が複数必要。
- 大幅なインフラの切り替え
- クライアントのスペックの見直し
- システムの大幅な切り替え
- 導入前のメーカーの調査の必要性

Viper（QAW機能）

Viperとは

- 不審なPC(QAWの管理モジュールがインストールされていないPC)を安易に社内ネットワークに繋がせないための機能
- 不審PCには、ネットワークからの遮断や、新規管理PCとして管理モジュールをインストールする等の処理が可能



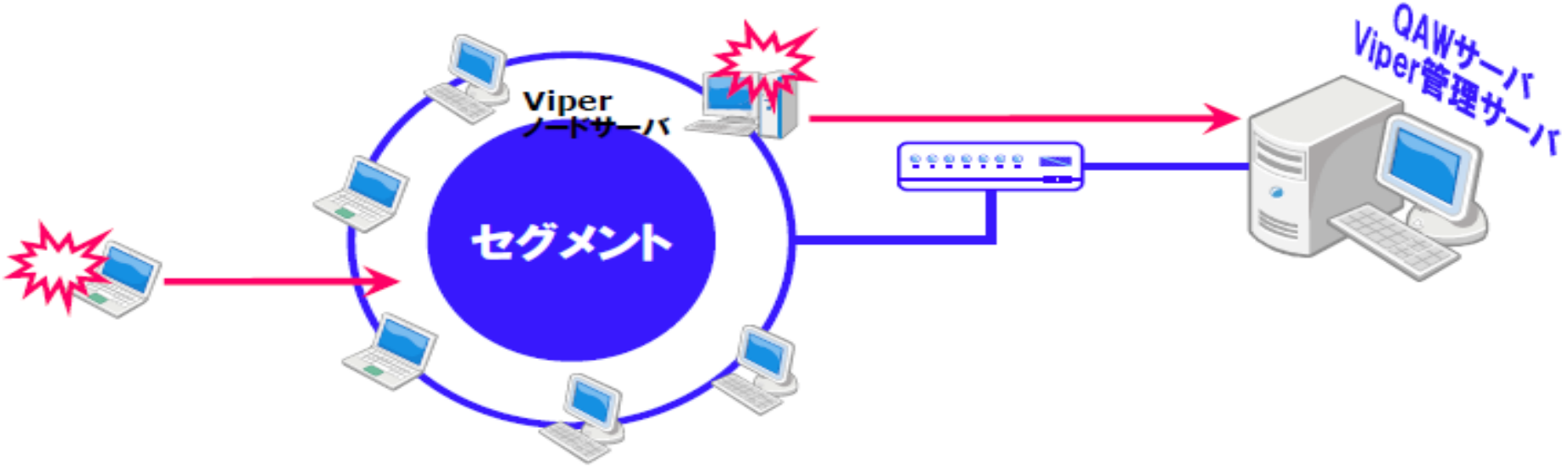
Viper（QAW機能）

危険PC発見のしくみ

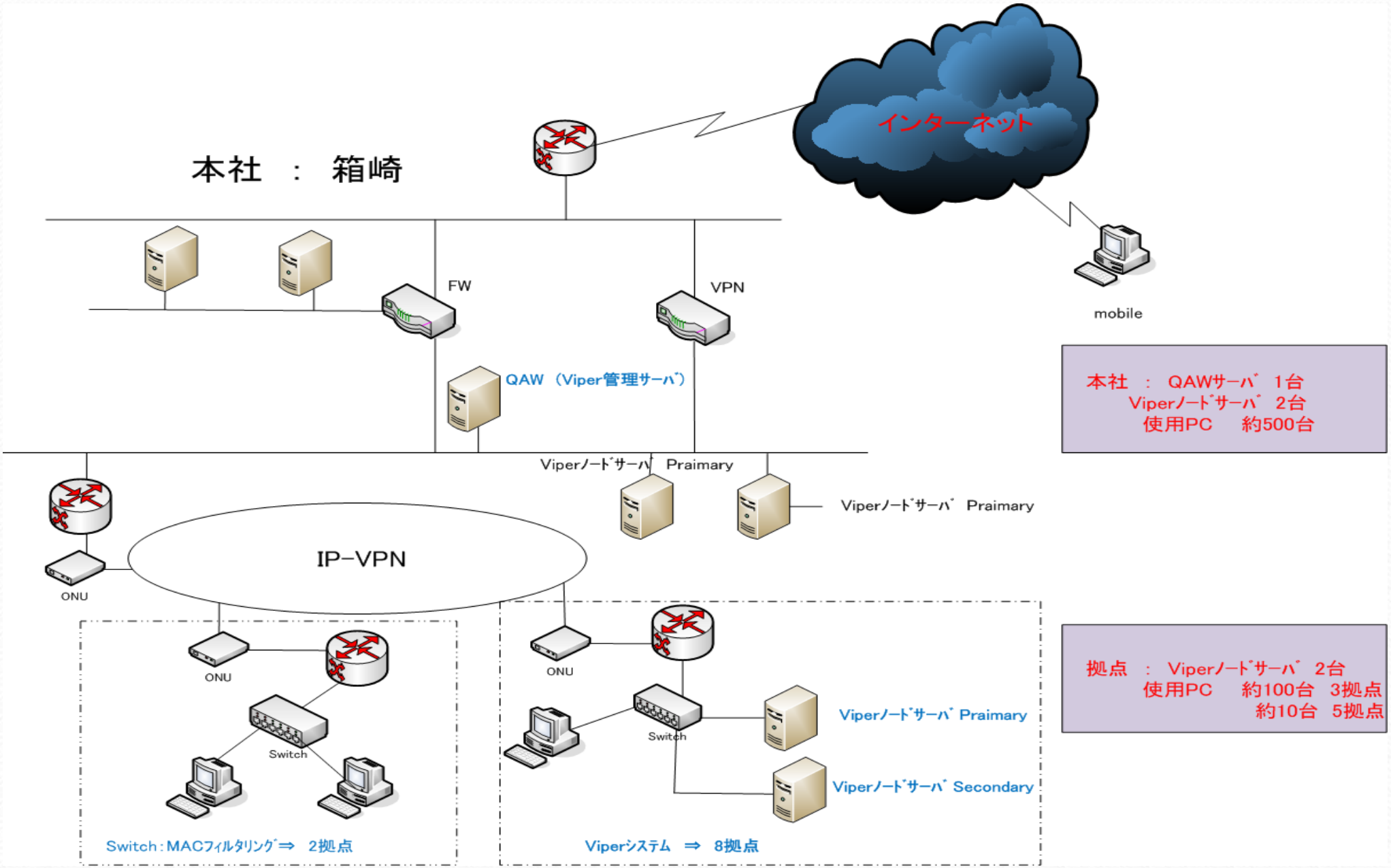
QAW管理下にない
未知のPCが
社内ネットワークに接続

そのセグメントにある
監視サーバ(ノードサーバ)が
不審PC検知を報告

管理サーバで
遮断or管理開始の
判断を行う



Viperシステム　構成概要



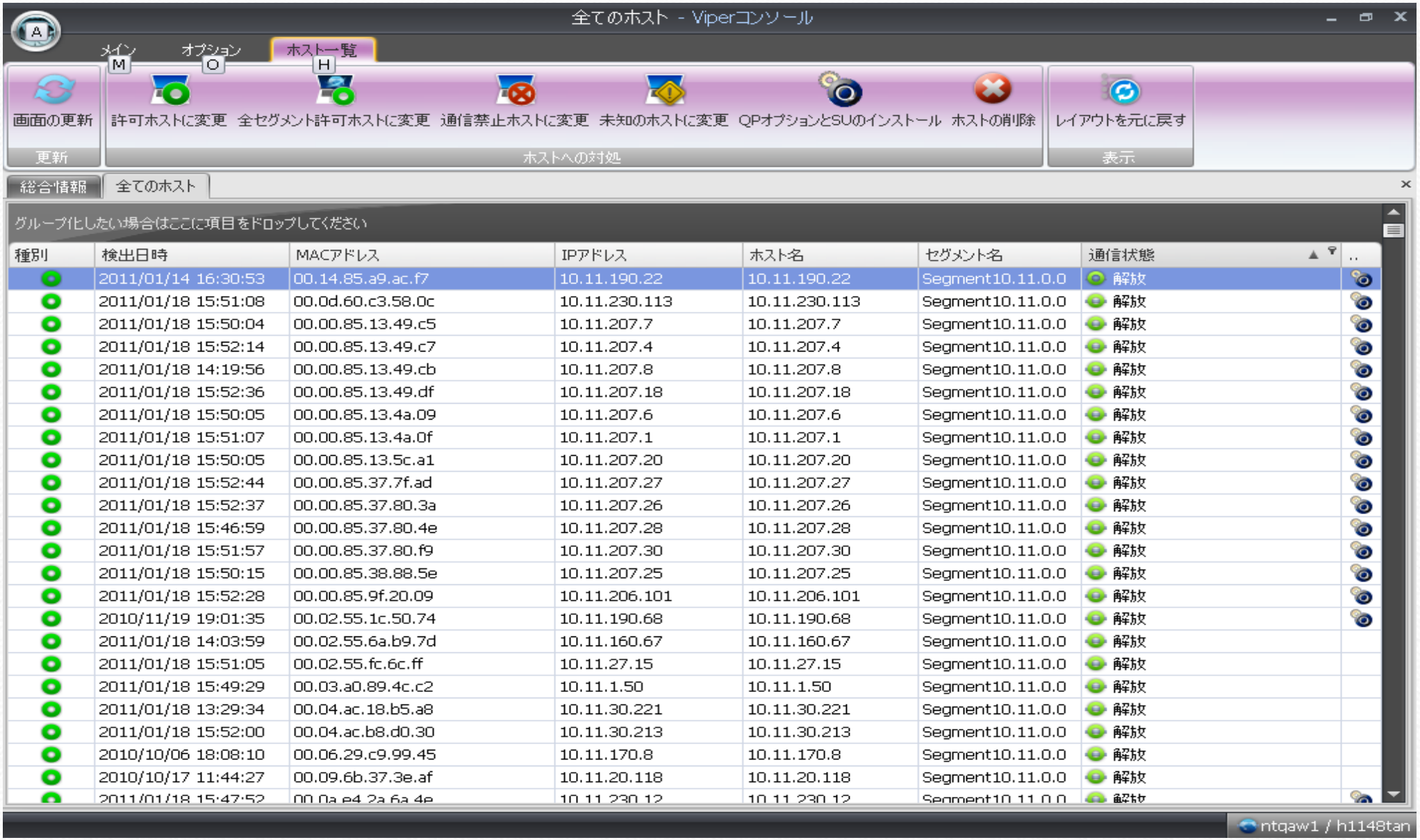
現行システムの追加内容

- ＱＮＤ　ＰｌｕｓからＱＡＷにｱｯﾌﾟﾃﾞｰﾄ

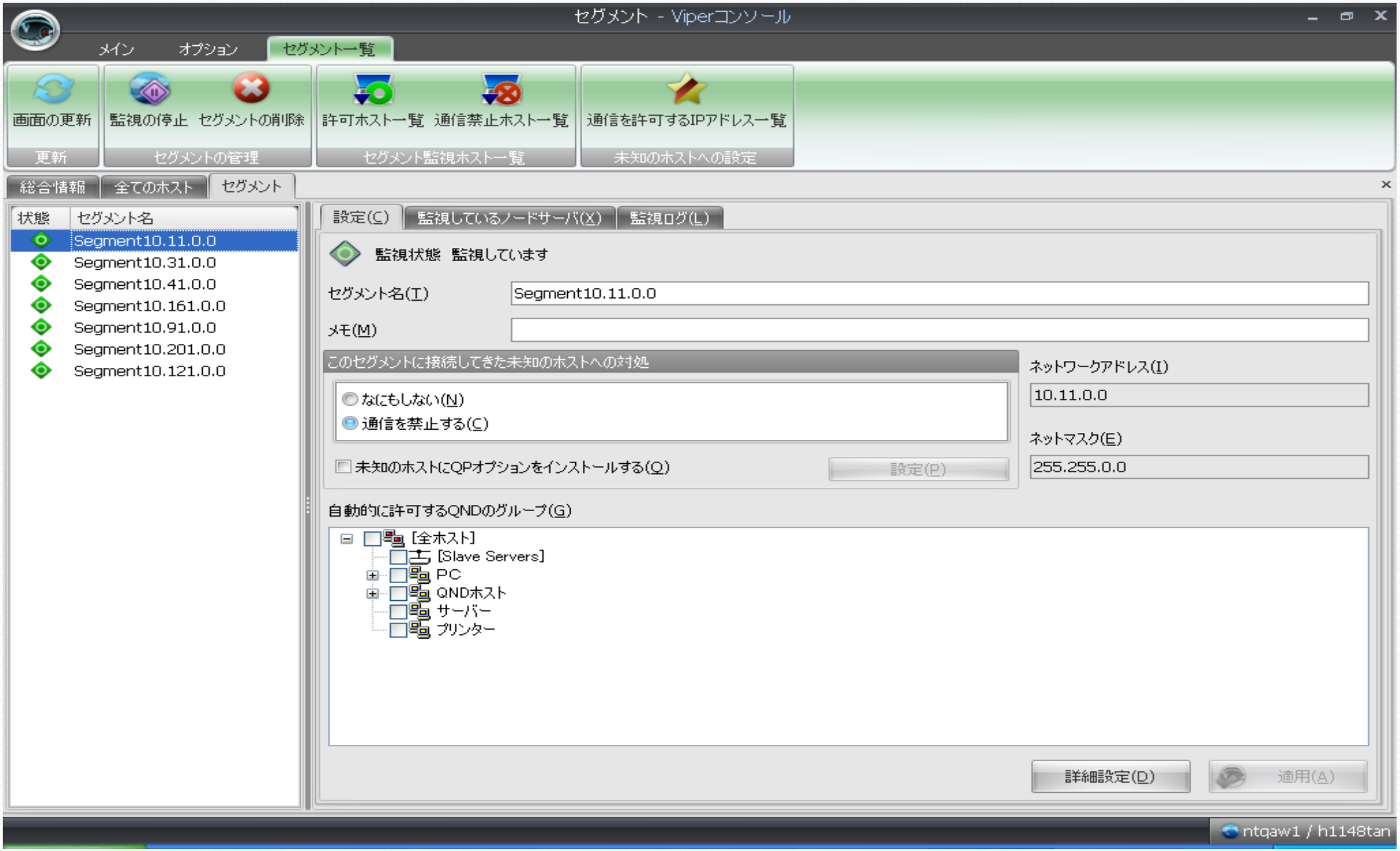
- Viperノードサーバ設置　8拠点
  ＊冗長化　2台/拠点

- Switch　MACフィルタリング　4拠点

ホワイトリスト画面


全てのホスト - Viperコンソール
メイン
M
オプション
O
ホスト一覧
H
画面の更新
更新
許可ホストに変更
全セグメント許可ホストに変更
通信禁止ホストに変更
未知のホストに変更
QPオプションとSUのインストール
ホストの削除
ホストへの対処
レイアウトを元に戻す
表示
総合情報
全てのホスト
グループ化したい場合はここに項目をドロップしてください
種別
検出日時
MACアドレス
IPアドレス
ホスト名
セグメント名
通信状態
2011/01/14 16:30:53 00.14.85.a9.ac.f7 10.11.190.22 10.11.190.22 Segment10.11.0.0 解放
2011/01/18 15:51:08 00.0d.60.c3.58.0c 10.11.230.113 10.11.230.113 Segment10.11.0.0 解放
2011/01/18 15:50:04 00.00.85.13.49.c5 10.11.207.7 10.11.207.7 Segment10.11.0.0 解放
2011/01/18 15:52:14 00.00.85.13.49.c7 10.11.207.4 10.11.207.4 Segment10.11.0.0 解放
2011/01/18 14:19:56 00.00.85.13.49.cb 10.11.207.8 10.11.207.8 Segment10.11.0.0 解放
2011/01/18 15:52:36 00.00.85.13.49.df 10.11.207.18 10.11.207.18 Segment10.11.0.0 解放
2011/01/18 15:50:05 00.00.85.13.4a.09 10.11.207.6 10.11.207.6 Segment10.11.0.0 解放
2011/01/18 15:51:07 00.00.85.13.4a.0f 10.11.207.1 10.11.207.1 Segment10.11.0.0 解放
2011/01/18 15:50:05 00.00.85.13.5c.a1 10.11.207.20 10.11.207.20 Segment10.11.0.0 解放
2011/01/18 15:52:44 00.00.85.37.7f.ad 10.11.207.27 10.11.207.27 Segment10.11.0.0 解放
2011/01/18 15:52:37 00.00.85.37.80.3a 10.11.207.26 10.11.207.26 Segment10.11.0.0 解放
2011/01/18 15:46:59 00.00.85.37.80.4e 10.11.207.28 10.11.207.28 Segment10.11.0.0 解放
2011/01/18 15:51:57 00.00.85.37.80.f9 10.11.207.30 10.11.207.30 Segment10.11.0.0 解放
2011/01/18 15:50:15 00.00.85.38.88.5e 10.11.207.25 10.11.207.25 Segment10.11.0.0 解放
2011/01/18 15:52:28 00.00.85.9f.20.09 10.11.206.101 10.11.206.101 Segment10.11.0.0 解放
2010/11/19 19:01:35 00.02.55.1c.50.74 10.11.190.68 10.11.190.68 Segment10.11.0.0 解放
2011/01/18 14:03:59 00.02.55.6a.b9.7d 10.11.160.67 10.11.160.67 Segment10.11.0.0 解放
2011/01/18 15:51:05 00.02.55.fc.6c.ff 10.11.27.15 10.11.27.15 Segment10.11.0.0 解放
2011/01/18 15:49:29 00.03.a0.89.4c.c2 10.11.1.50 10.11.1.50 Segment10.11.0.0 解放
2011/01/18 13:29:34 00.04.ac.18.b5.a8 10.11.30.221 10.11.30.221 Segment10.11.0.0 解放
2011/01/18 15:52:00 00.04.ac.b8.d0.30 10.11.30.213 10.11.30.213 Segment10.11.0.0 解放
2010/10/06 18:08:10 00.06.29.c9.99.45 10.11.170.8 10.11.170.8 Segment10.11.0.0 解放
2010/10/17 11:44:27 00.09.6b.37.3e.af 10.11.20.118 10.11.20.118 Segment10.11.0.0 解放
2011/01/18 15:47:52 00.0a.e4.2a.6a.4e 10.11.230.12 10.11.230.12 Segment10.11.0.0 解放
ntqaw1 / h1148tan

遮断設定画面


セグメント - Viperコンソール
メイン
オプション
セグメント一覧
画面の更新
監視の停止
セグメントの削除
許可ホスト一覧
通信禁止ホスト一覧
通信を許可するIPアドレス一覧
更新
セグメントの管理
セグメント監視ホスト一覧
未知のホストへの設定
総合情報
全てのホスト
セグメント
状態
セグメント名
Segment10.11.0.0
Segment10.31.0.0
Segment10.41.0.0
Segment10.161.0.0
Segment10.91.0.0
Segment10.201.0.0
Segment10.121.0.0
設定(C)
監視しているノードサーバ(X)
監視ログ(L)
監視状態 監視しています
セグメント名(T)
Segment10.11.0.0
メモ(M)
このセグメントに接続してきた未知のホストへの対処
なにもしない(N)
通信を禁止する(C)
未知のホストにQPオプションをインストールする(Q)
設定(P)
ネットワークアドレス(I)
10.11.0.0
ネットマスク(E)
255.255.0.0
自動的に許可するQNDのグループ(G)
[全ホスト]
[Slave Servers]
PC
QNDホスト
サーバー
プリンター
詳細設定(D)
適用(A)
ntqaw1 / h1148tan

Viperによるメリット

- 不正ＰＣの接続の抑止
  以前は検知されず、トラブル後発覚していた。
- ＩＰアドレスに関する、モラルの向上
  ＩＰアドレス申請を行わず、勝手に割振り使用していた。
- 社内機器の管理の向上
  ＩＰアドレス申請がなかったため、情報システムの把握外の機器が存在した。
- 経費の削減
  他社システムでの構築を検討していたが、現行システムにしたことにより大幅な経費の削減が行えた。
- 運用の簡略化
  データ管理が不完全だったため、現状確認が困難だった。

苦労した点

- テスト環境の作成

  ルータ越えでの接続や、ノードサーバーの停止時の自動切り替えなどのテストを行う為、複数のスイッチとＰＣを準備して試しました。

- ホワイトリストの作成

  ＩＰ申請ＤＢ（Notes)で接続の管理を行っていたが登録にない機器等があった為、調査するのに時間がかかった。

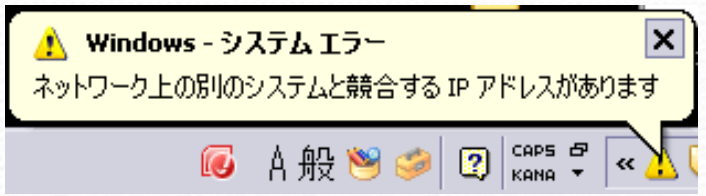
- ホワイトリストからの削除

  1度許可ホストに変更した場合、ホワイトリストからの削除を行い、次に接続しても、遮断された状態にするには、「通信禁止ホストに変更」し、「ホストの削除」を行わなければいけない。

現在の運用

ＰＣを新たに社内ＬＡＮに接続する場合

- NotesＤＢにてＩＰアドレス申請をする。
- 情報システムにてＩＰアドレスを割り振る。
- ＰＣにＩＰアドレスを設定し、社内ＬＡＮに接続。
- システムエラー表示されたら、情報システムに連絡。



- Ｖｉｐｅｒコンソールにて、ＩＰアドレス・ＭＡＣアドレスを確認し、許可ホストに変更する。
- 社内ＬＡＮ接続後、ＱＡＷの導入を行う。

まとめ

- 導入後の評価

  不正に接続してきたＰＣを検知し、遮断している実績があらわれ、ＩＰ申請を行ってから社内ＬＡＮに接続するルールが守られるようになり不正ＰＣの社内ＬＡＮへの接続がなくなりました。

- 今後の予定

  社内ルールに適合したＰＣ（共通ソフトの導入と不正ソフトの未導入）を検知し、不適合のＰＣに関しては、社内ＬＡＮへの接続を遮断する対応を検討します。

  →ＱＡＷの機能の活用