ネットワークの自己防衛

～コンプライアンス確保のためのITインフラ
検疫ネットワークについて～

2004年10月29日

株式会社ネットマークス　正木 淳雄
Masaki.atsuo@netmarks.co.jp

NSF 2004

We are here

ネットマークス会社概要

設立	：	1997年3月18日
資本金	：	13億7252万円
株式	：	東京証券取引所市場第二部上場
人員	：	811名　(グループ全体、2004年4月1日現在)
事業拠点	：	東京、大阪、名古屋、福岡、札幌、広島、仙台、那覇
海外拠点	：	上海、ジャカルタ、マニラ、バンコク、シンガポール、クアラルンプール、シリコンバレーオフィス
連結子会社	：	株式会社ネットマークスサポートアンドサービス エス・アンド・アイ株式会社 スターネット株式会社

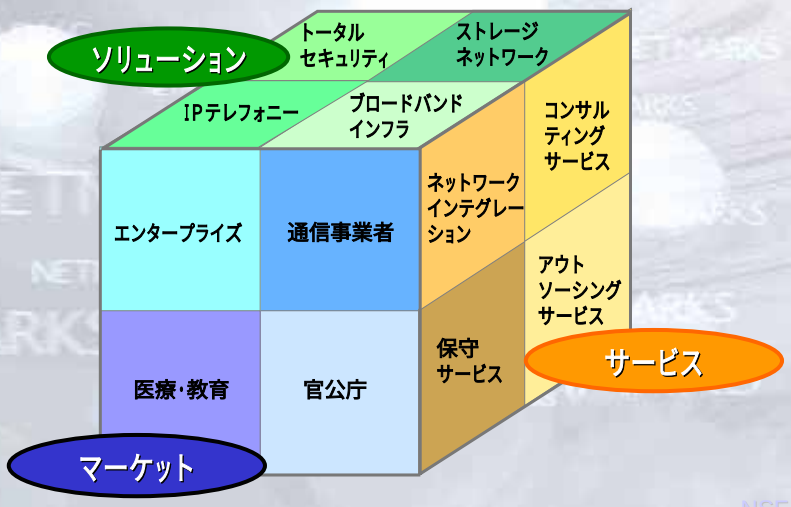
NSF 2004

We are here

 1

事業概要

ネットワークソリューションプロバイダとしてインターネットの基盤技術に特化



NSF 2004

We are here

アジェンダ

1. コンピュータ・ワーム
2. セキュアなITインフラ
3. 検疫ネットワーク

NSF 2004

We are here

コンピュータ・ワーム

ニュースから

- **米調査―企業のウイルス対策費用が大幅に増加**
  2003年には、拡大するウイルス攻撃の被害に苦しんだ企業が増加し、ウイルス駆除に要した**費用が1件につき平均で約10万ドル**に達したことが、新しい調査結果で明らかに。
  (CNET News.com 2004/3/23)
- **MSBlastの感染台数、800万台を超える―マイクロソフト発表**
  Microsoftは、自社が提供したMSBlastワーム除去ツールの利用数調査を基に、MSBlastに感染したWindowsシステムの台数を**800万台**とするデータを発表した。
  (IT media 2004/4/25)
- **大企業、週一で被害に―セキュリティ問題に関する英調査**
  英国政府がITセキュリティに関して行った今年の公式調査によると、ハッキング攻撃やウイルス、ネットワーク侵入の被害にあった英国企業の数が過去最高となり、大手企業ではほぼ**週に1度のペースでこうした攻撃の被害**にあっているという。
  (CNET News.com 2004/4/28)

NSF 2004

We are here

コンピュータ・ワーム

脅威の進化

	1999	2000	2001	2002	2003	2004
	1999年 研究者がDoS攻撃の研究 DoS攻撃ツールの出現	2000年2月 分散DoS攻撃の登場	2001年 研究者がインフラ攻撃を研究	2002年 インフラ攻撃の出現		
攻撃源	コンピュータ			インフラ		
攻撃目標	コンピュータ		ネットワーク	インターネット		

2000年2月 Amazon, CNN,Yahoo, EBay,Etrade の各サイトが分散DoS攻撃でダウン

2001年1月 複数の大規模サイトがルータへの分散DoS攻撃でダウン
2001年3月 Lion Worm
2001年5月 sandmind_iisワーム
2001年7月 Code Red, Code Red II
2001年9月 Nimda

2002年1月 欧州のISPが分散DoS攻撃の影響でサービス停止
2002年2月 SNMPの脆弱性をつくルータへの攻撃開始
2002年10月 ルートDNSサーバへの分散DoS攻撃

2003年1月 SQLワームで世界的にインターネットが混乱
2003年8月 Blasterワームが猛威を揮う
2003年3月 Deloderワーム
Code Red.F
2003年8月 SoBig

2004年1月 MyDoom世界中のコンピュータに感染
2004年3月 W32/NetSky.B ウイルス出現
2004年5月 Sasserワーム世界的に流行

Source: Arbor Networks

NSF 2004

We are here

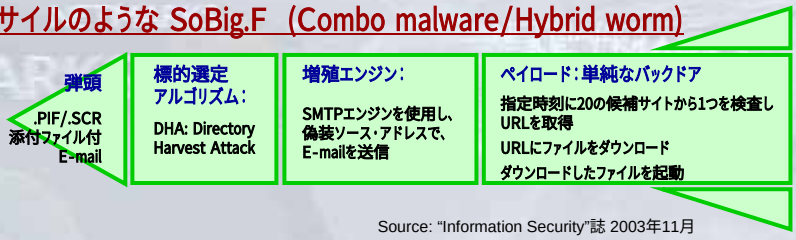
コンピュータ・ワーム

感染

不正コードの増殖方法（ウイルスとワームの感染の仕方）

不正コードの種類	特　徴
直接のインストール	アタッカは手動あるいはインストールスクリプトを用いて、不正プログラムをインストール
ウイルス	自己複製機能によってファイルに感染
ワーム	ネットワーク経由で広がり、システムを攻撃
不正なモバイルコード	QuickTime、Flash、Shockwave ファイルなどのアクティブコンテンツを介してWEBブラウザや電子メールソフトに広がる

ミサイルのような SoBig.F　(Combo malware/Hybrid worm)



Source: “Information Security”誌 2003年11月

NSF 2004

We are here

 6

コンピュータ・ワーム

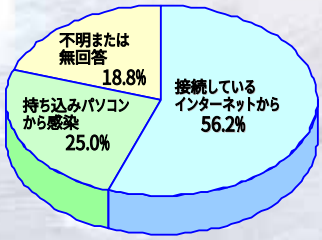
感染

社員が自分のPCを組織内に持ち込み、
ネットワークに接続した

自宅のPCを個人契約しているISPを経由して
社内ネットワークに接続した

利用者のPCにおける、ウイルス対策ソフトの
パターンファイル更新や Windows Update の
実行が利用者任せになっていた

「Windows Update」が必要と思いつつ、
業務APの動作検証が間に合わず、
Windows Update が追いついていなかった



MS/Blasterとウェルチの感染経路
(IPA調査、2003年)

NSF 2004

We are here

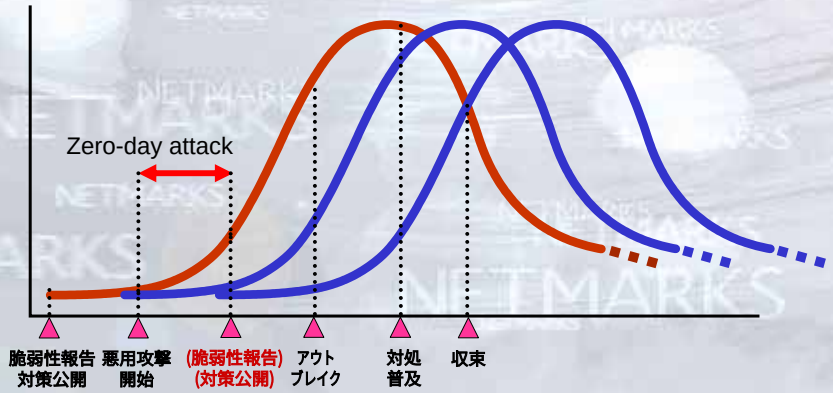
 7

コンピュータ･ワーム

コンピュータ･ワームのライフサイクル

ゼロデイ･アタックの脅威

- 未知の敵との戦い



NSF 2004

We are here

セキュアなITインフラ

ネットワーク運用の課題の変化

- 稼動の確保→利益確保とビジネスの継続維持

対象とするインフラの範囲の変化

- 自社インフラのみ→顧客、パートナーなどとの相互接続

ITインフラの強化／セキュリティ強化

- コンプライアンス→取引関係の条件
- 総合的な対策→目標設定と達成度の指標
  - COBIT成熟度モデル, SSE-CMMなど

COBIT: Control Objectives for Information and related Technology, http://www.isaca.org/

SSE-CMM: Systems Security Engineering - Capability Maturity Model, http://www.issea.org/

NSF 2004

We are here

セキュアなITインフラ

セキュリティ対策の分類

Source: Yankee group

境界フィルタ	ネットワークの完全性	アプリケーションゲートウェイ	ホストの完全性
ネットワーク上の不正トラフィック除去	アプリケーション用ネットワークの可用性確保	専用アプリケーション用セキュリティポリシーの適用	脆弱性の悪用からエンドポイントの保護
ファイアウォール機能 アンチウイルス・フィルタ URLフィルタ 不正侵入フィルタ プロトコルコンプライアンス 拠点間VPN	DoS対策 サーバ検索対策 ワーム被害の緩和 プロトコルのブロック 帯域幅管理	Webアプリケーション Webサービス SSL/VPN 電子メール/スパム IPテレフォニー 無線LAN	コンフィグレーション管理 ホストファイアウォール スパイウェア対策 侵入防止 ウイルス対策
管理 セキュリティをビジネスプロセスに統合する			
セキュリティイベント管理 アイデンティティ管理 パッチ管理 セキュリティエンジニアリング		脆弱性管理 侵入検知監査 セキュアなコンテンツ配信 セキュリティポリシー管理	
サービス 最高のセキュリティ技術・知識の活用			
セキュリティポリシーの展開 マネジド・セキュリティサービスの活用 リスク測定と削減		監査サービス 法規制の順守要請 戦略的コンサルティング	

We are here

 10

セキュアなITインフラ

セキュリティ対策のフェーズ

準備
- 対策手段の確保
- 対策手段のテスト
- 対策手順の策定
- 対策チームの教育
- 演習

攻撃の識別
- 攻撃について得る
- 対策手段を知る

攻撃の分類
- ITプロセスの確認
- 攻撃の深刻度の把握

追跡
- どこから攻撃されたか調べる
- ネットワークへの影響を調べる

対策
- どんな復旧手段があるか
- 現状で最も有効な手段は何か

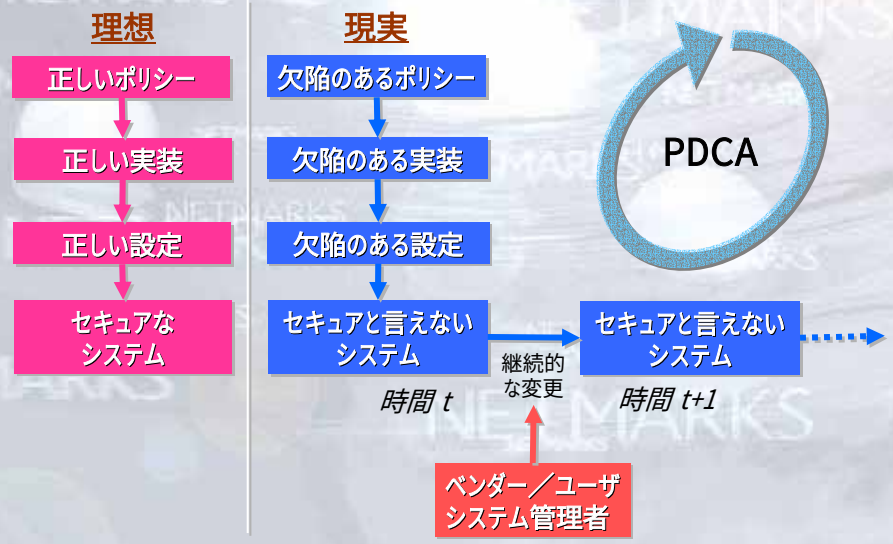
事後処理
- 何が起こったのか全貌把握
- 予防策がなかったか検討
- 将来問題を最小化する方法

We are here

 11

セキュアなITインフラ

システムの不完全性



We are here

セキュアなITインフラ

完全はない

ゼロデイ・アタックの恐怖

- 誰も事前に対策を知らない
- 事前情報によらない対策→状況に応じて自律的に対応する
- Anomaly detection (異常検知) という方法
- 何が異常？→異物を識別する人体の免疫の仕組みは？
- 「からだ」はネットワーク？　それともホストコンピュータ？
- そのうち、携帯電話や家電にも電子リンパ球が活躍する？

生体の免疫システムの特徴

- 「自己」と「非自己」を識別し、「非自己」を排除する点にある
- ランダムに抗体を（1億パターン）産生し、あたりまえの対象には学習して「寛容」になる
- 一度知った異物には、次回から直ちに攻撃して中和する

We are here

セキュアなITインフラ

ITインフラと免疫システム

コンピュータがおかれている環境

- 不完全で
- 管理しきれず
- オープン

永久に問題は解決しない？

コンピュータ免疫システム

- 「自己」と「非自己」をITセキュリティで置き換えてみる．．．
- 「正しいXX」と「正しくないXX」

生体免疫システムの特徴

- 分散処理能力
- 多様性
- 廃棄性
- 順応性
- 自律性
- 対象範囲の動的決定
- 異常検出
- 多階層性
- ふるまいに基づく自己同一性
- 必ずしも信頼できない構成要素
- 不完全な検出

NSF 2004

We are here

 14

セキュアなITインフラ

「自己」と「非自己」

病原体

- コンピュータウイルス・ワーム、攻撃的アクセス、情報の窃盗、etc.

自己と非自己

- ビジネス上必要なアプリケーションと不必要なアプリケーション
- ビジネス上必要な通信と不必要な通信
- シグネチャの登録されていないプログラムと登録されているもの
- 統計的に正常なプロトコルの動作と異常な動作
- プロトコル仕様に準拠したプロトコル動作と逸脱した動作
- 正しく認可されたユーザとそうでないユーザ
- 正しく認証されたユーザとそうでないユーザ
- 正しく認証された機器とそうでない機器
- コンプライアンスに合致する機器と合致しない機器
- 統計的に正常なユーザ行動と異常な行動
- 統計的に正常なアプリ行動と異常な行動

アンチウイルス

IDS/IPS

認証・認可

コンプライアンス

フォレンジック
コンピューティング

NSF 2004

We are here

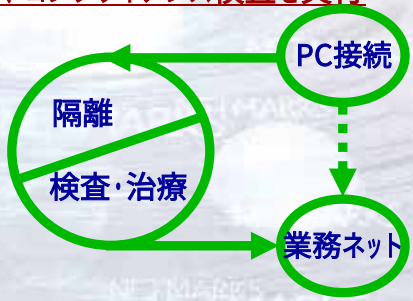
 15

検疫ネットワーク

PCを「検疫ネットワーク」に隔離し、コンプライアンス検査を実行

検疫ネットワークの要素

- 隔離 (通信制限)
- 検査 (コンプライアンス検査)
- 治療 (アップデート)

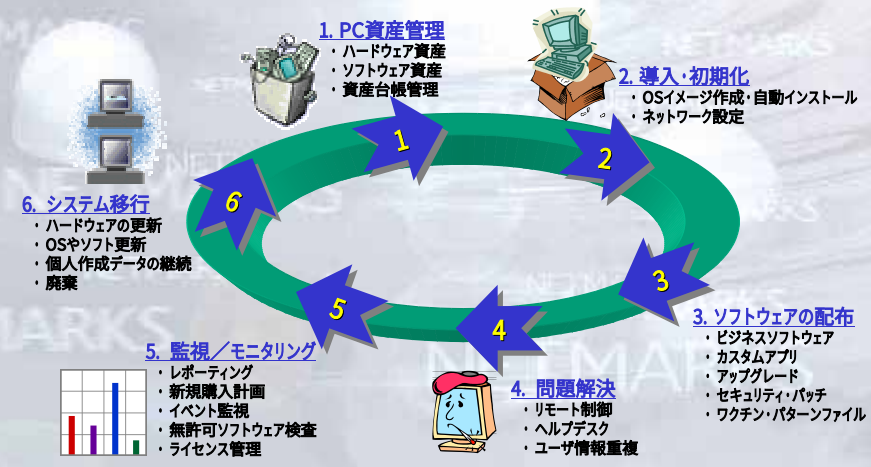


要件

- 既存のネットワークへの影響を最小限にする (導入コスト、設計変更等)
- 既存の資産管理ソフトなどを有効活用できる
- 運用を支援するサービスが用意されている

PCライフサイクル管理

ワーム対策やパッチ管理を、PCライフサイクル管理の中でとらえる



検疫ネットワーク

ネットワークレベルの対策の重要性

ルールの限界

- 利用者の知識不足
- 「大丈夫」だろうという軽率な判断

管理・運用の限界

- 新規導入PCや持込みノートPC、休眠PCなどの未対策PCが感染源に
- パッチ適用などの能率とワームの感染速度

接続することじたいが問題

- 危険なものはつながない、という発想
- なんらかの検査を行い、PCがクリーンであることを確認してから、業務ネットワークにつながせる仕組みが重要
- それでも侵入するワームはIPSなどで拡散を防ぐ

【ルール化】全社ルールの明文化とオーソライズ
【管理】管理対象PCの正確な把握
【運用】管理されていないPCやパッチ未適用のPCの早期発見
【危機管理】有事の際の対応
【教育・訓練】セキュリティ意識の啓発、理解

NSF 2004

We are here

検疫ネットワーク

検疫ネットワークの機能要素

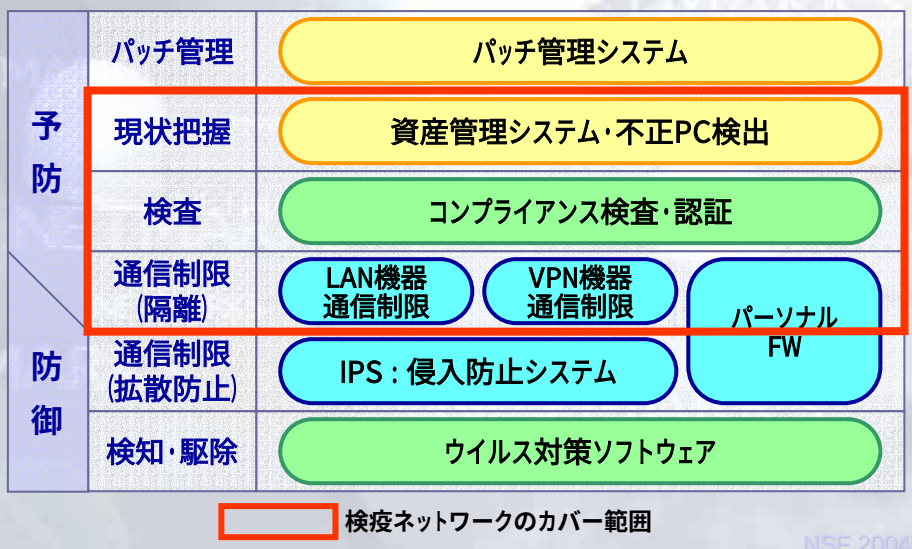
隔離 通信制限	業務ネットワークに接続する際に、強制的に検疫ネットワークに隔離 ・ネットワーク認証技術を応用して、条件によってアクセスできるネットワークを変える ・ウイルス感染やポリシー違反の有無を検査するため、または検査結果によって、PCの通信を強制的に検疫用ネットワークに隔離
検査 コンプライアンス検査	セキュリティポリシー／運用ポリシーが遵守されているかどうかを検査 ・機器は正規に登録され、承認されているか ・OS、ビジネスソフト、ウイルスソフトが、規定されたバージョン・パッチレベルにあるか ・PC利用規定上、必須とされているソフトが正しく導入され、稼動しているか ・端末やサーバ機が、ウイルスに感染していないか
治療 アップデート	コンプライアンスに合致するようにアップデート ・OSパッチのアップデート、アンチウイルスソフトのパタンファイル適用 ・利用者による実施、またはセンタ側から強制（自動）適用 ・アップデート終了後、ポリシーに合致しているかどうか再検査（検疫を再実行し、問題がなければ業務ネットへの接続を許可）

NSF 2004

We are here

検疫ネットワーク

ワーム対策と検疫ネットワーク



We are here

検疫ネットワーク

さまざまな検疫システムの登場

ソリューションを発表しているベンダー

- IBM、エクストリームネットワークス、NEC、NTTデータ／日立電線、エンテラシス・ネットワークス、京セラコミュニケーションシステム、クオリティ、シスコシステムズ、トレンドマイクロ、日本アルカテル、日本HP、日本テレコム、ネットマークス、PFU、富士通、マイクロソフト

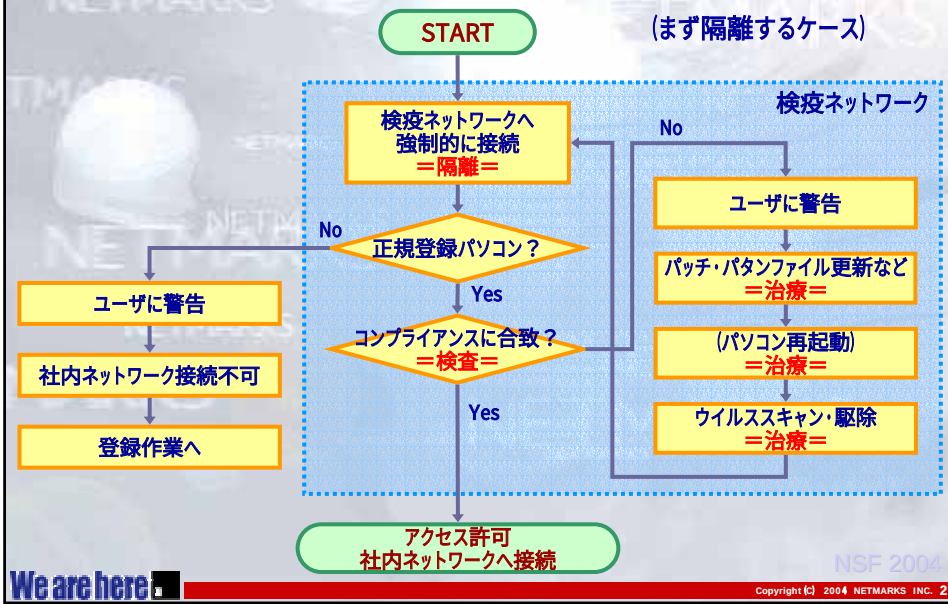
ソリューション選定上のポイント

	導入コスト	運用負荷	現状への親和性	技術の将来性
ユーザ認証方式				
導入時のネットワーク機器の変更				
クライアント用エージェントの有無				
治療機能の有無				
IDS/IPSとの連携				
対応クライアントOSの豊富さ				

We are here

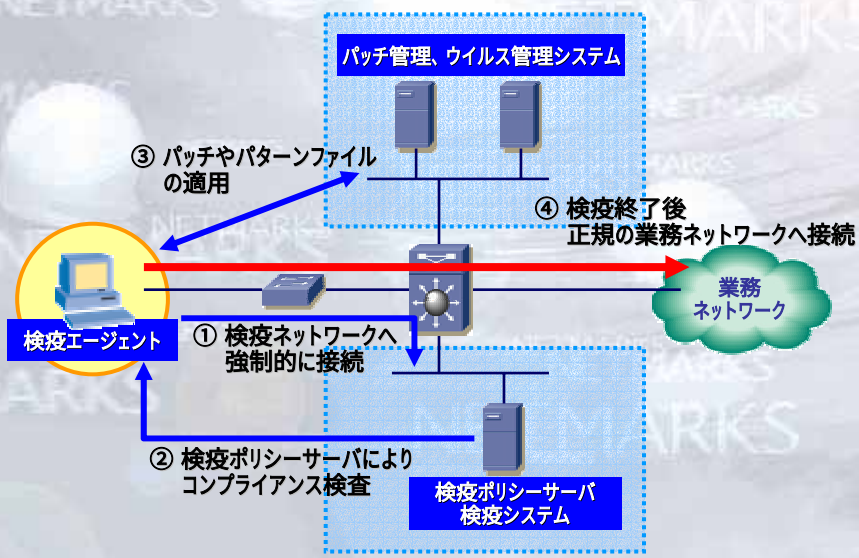
検疫ネットワーク

検疫ネットワークの処理の流れの例



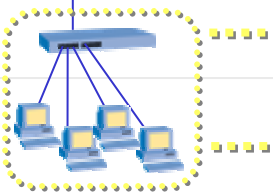
検疫ネットワーク

検疫ネットワークの構成



検疫ネットワーク

検疫（隔離）を実行する位置

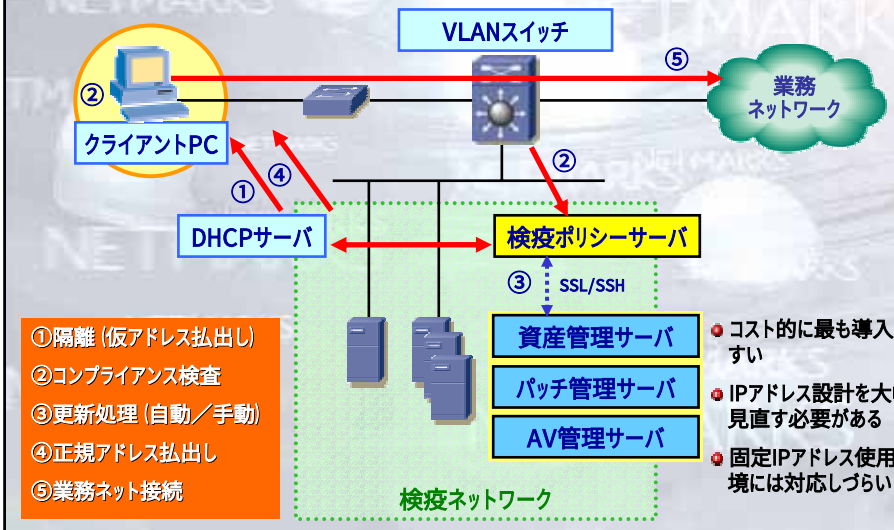
検疫の位置	構　成	説　明
DHCPサーバ		✓ ネットワーク機器変更なし ✓ DHCPサーバでのMACアドレス認証 ✓ エンドポイント単位でIPアドレスによる隔離
上位スイッチ		✓ WEB認証対応スイッチが必要 ✓ 配下のセグメントでワームの拡散の可能性あり
エッジスイッチ		✓ 802.1X対応スイッチなど。エッジスイッチの総入れ替え必要。認証をリレーできる上位スイッチも ✓ ポート単位でPCなどエンドポイントを隔離可
エンドポイント		✓ パーソナルFW ✓ ウイルス対策ソフトに包含されるもの ✓ 資産管理ソフトに包含されるもの ✓ 適宜ダウンロードするもの（ActiveX, JavaApplet）

We are here

 24

検疫ネットワーク

DHCP方式

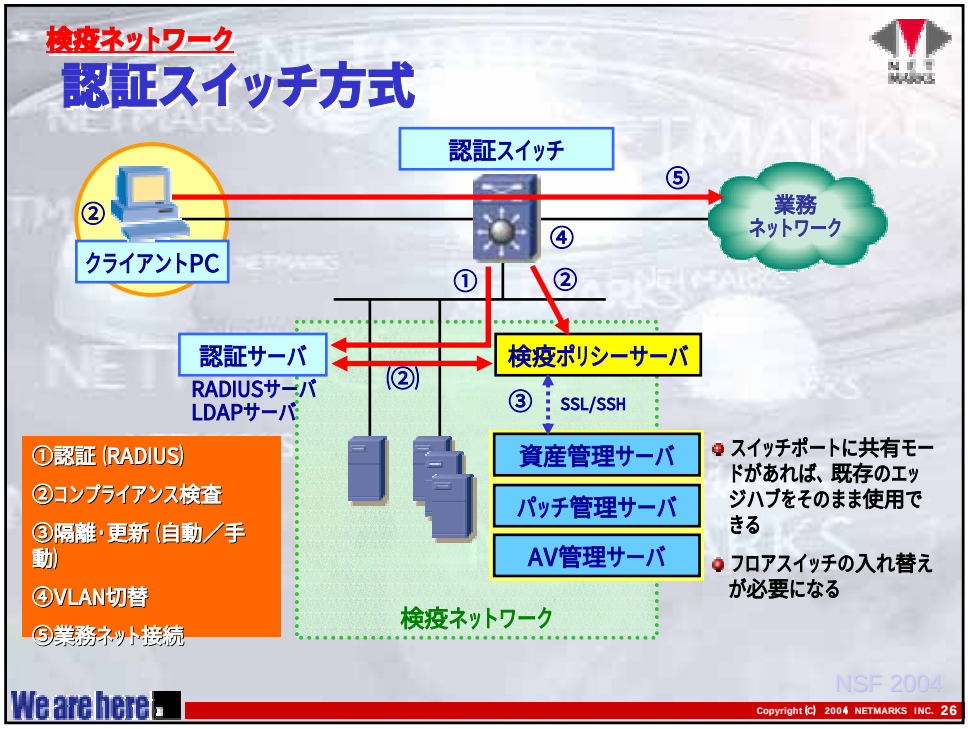


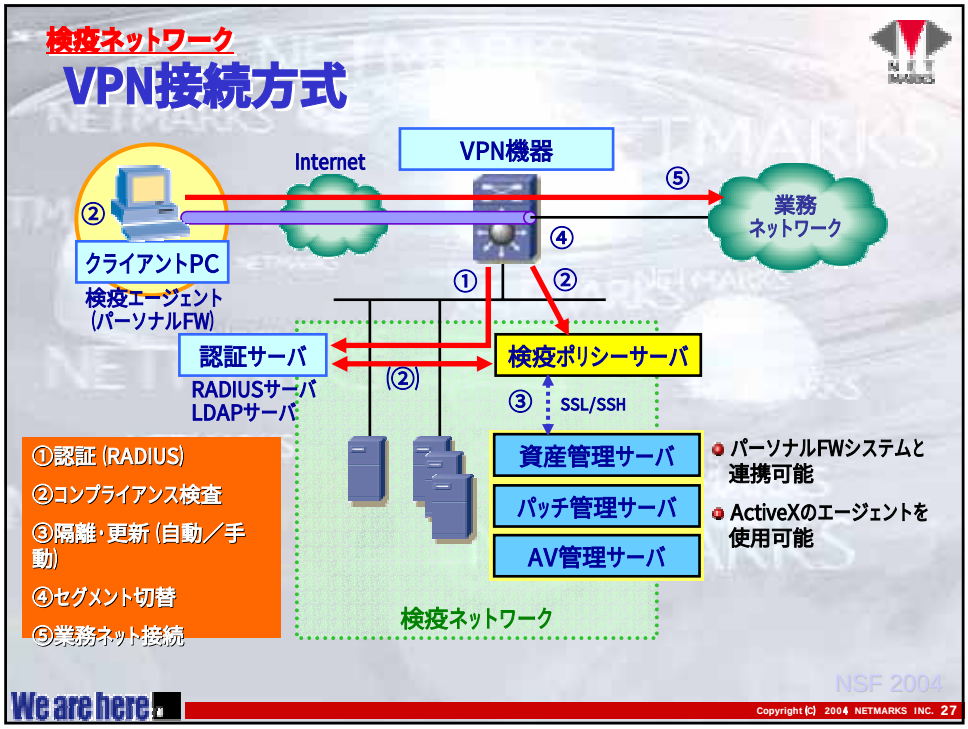
①隔離（仮アドレス払出し）
②コンプライアンス検査
③更新処理（自動／手動）
④正規アドレス払出し
⑤業務ネット接続

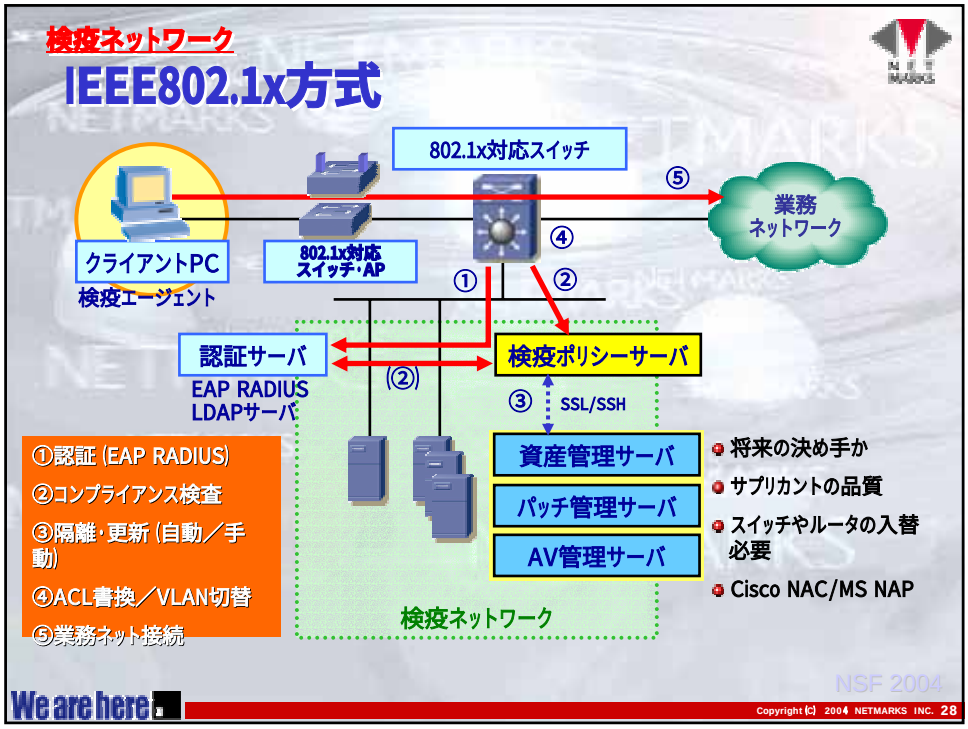
- コスト的に最も導入しやすい
- IPアドレス設計を大幅に見直す必要がある
- 固定IPアドレス使用環境には対応しづらい

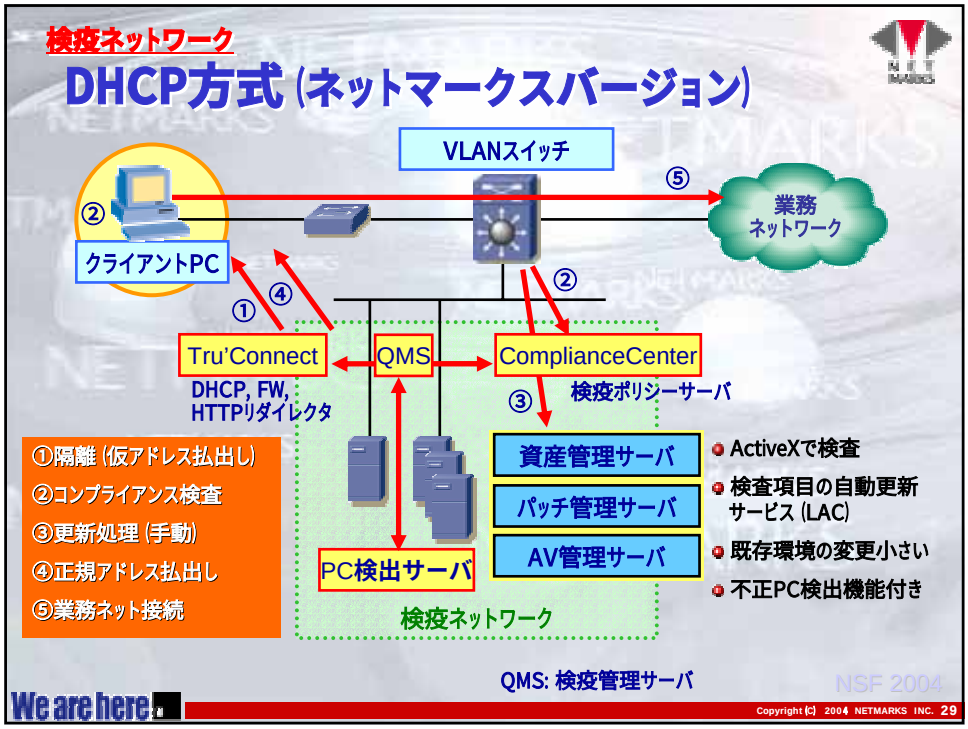
We are here

 25


検疫ネットワーク
認証スイッチ方式
認証スイッチ
⑤
業務
ネットワーク
②
クライアントPC
④
①
②
認証サーバ
RADIUSサーバ
LDAPサーバ
(②)
検疫ポリシーサーバ
③
SSL/SSH
資産管理サーバ
パッチ管理サーバ
AV管理サーバ
①認証 (RADIUS)
②コンプライアンス検査
③隔離・更新 (自動／手動)
④VLAN切替
⑤業務ネット接続
検疫ネットワーク
スイッチポートに共有モードがあれば、既存のエッジハブをそのまま使用できる
フロアスイッチの入れ替えが必要になる
NSF 2004
We are here
Copyright (C) 2004 NETMARKS INC. 26


検疫ネットワーク
VPN接続方式
Internet
VPN機器
⑤
業務
ネットワーク
②
クライアントPC
検疫エージェント
(パーソナルFW)
④
①
②
認証サーバ
RADIUSサーバ
LDAPサーバ
(②)
検疫ポリシーサーバ
③
SSL/SSH
資産管理サーバ
パッチ管理サーバ
AV管理サーバ
①認証 (RADIUS)
②コンプライアンス検査
③隔離・更新 (自動／手動)
④セグメント切替
⑤業務ネット接続
検疫ネットワーク
パーソナルFWシステムと連携可能
ActiveXのエージェントを使用可能
NSF 2004
We are here
Copyright (C) 2004 NETMARKS INC. 27


検疫ネットワーク
IEEE802.1x方式
802.1x対応スイッチ
⑤
業務
ネットワーク
クライアントPC
検疫エージェント
802.1x対応
スイッチ・AP
④
①
②
認証サーバ
EAP RADIUS
LDAPサーバ
(②)
検疫ポリシーサーバ
③ SSL/SSH
資産管理サーバ
パッチ管理サーバ
AV管理サーバ
①認証 (EAP RADIUS)
②コンプライアンス検査
③隔離・更新 (自動／手動)
④ACL書換／VLAN切替
⑤業務ネット接続
検疫ネットワーク
将来の決め手か
サプリカントの品質
スイッチやルータの入替必要
Cisco NAC/MS NAP
We are here
NSF 2004
Copyright (c) 2004 NETMARKS INC. 28


検疫ネットワーク
DHCP方式 (ネットマークスバージョン)
VLANスイッチ
⑤
業務
ネットワーク
②
クライアントPC
①
④
②
Tru'Connect
QMS
ComplianceCenter
DHCP, FW,
HTTPリダイレクタ
③
検疫ポリシーサーバ
資産管理サーバ
パッチ管理サーバ
AV管理サーバ
PC検出サーバ
①隔離 (仮アドレス払出し)
②コンプライアンス検査
③更新処理 (手動)
④正規アドレス払出し
⑤業務ネット接続
検疫ネットワーク
ActiveXで検査
検査項目の自動更新サービス (LAC)
既存環境の変更小さい
不正PC検出機能付き
QMS: 検疫管理サーバ
We are here
NSF 2004
Copyright (c) 2004 NETMARKS INC. 29

検疫ネットワーク

コンプライアンス検査

コンプライアンス検査のタイミング

- 起動時検査
- リアルタイム（定期）検査

ポリシーの強化（Policy Enforcement）

- セキュリティポリシーや運用ポリシーを一定の水準に維持する

ワーム対策にとどまらない

- 特定のツールのインストールや稼動をポリシーとして定める
  - 必須：アンチウイルスソフト、パーソナルFW、アンチ・スパイウェア、資産管理ソフト、情報漏洩対策ソフト、特定の業務ソフトなど
  - 不許可：P2PツールやSoftEther、特定の周辺機器など
- 例外を排除することで、情報漏洩対策など、対策徹底の支えになる
- 全体的な運用コストの削減につながる

We are here

検疫ネットワーク

主なコンプライアンス検査項目

OSのサービスパック、セキュリティパッチ適用状況	[検査] Windows系OSのサービスパックおよびセキュリティパッチの適用状況を検査 →未適用 のクライアントPCには、対策内容を表示するなど、ガイダンスを示す [対策] サービスパック、パッチを入手しクライアントPCに適用
アプリケーションのサービスパック、セキュリティパッチ適用状況	[検査] Microsoft Internet Explorerのサービスパックなどのパッチ適用状況を検査 →未適用 のクライアントPCには、対策内容を表示するなど、ガイダンスを示す [対策] サービスパック、パッチを入手し、クライアントPCに適用
アンチウイルス・ソフトのパターンファイル更新状況	[検査] アンチウィルス・ソフトのパターンファイル更新状況を検査 [対策] ウィルス検知ソフトのアップデート機能を用いてパターンファイルを更新
稼動ソフトの状況	[検査] PC上のソフト稼動状況 [対策] 不要なソフトの稼動、必要なソフトの稼動状況を検査→ポリシーに適合しない場合は、ガイダンスを示し、改善を求める

We are here

検疫ネットワーク

現実解はどれか？

再び、「検疫ネットワーク」の要件

- 既存のネットワークへの影響を最小限にする（導入コスト、設計変更等）
- 既存の資産管理ソフトなどを有効活用できる
- 運用を支援するサービスが用意されている

再び、検疫ネットワーク選定のポイント

	導入コスト	運用負荷	現状への親和性	技術の将来性
ユーザ認証方式				
導入時のネットワーク機器の変更				
クライアント用エージェントの有無				
治療機能の有無				
IDS/IPSとの連携				
対応クライアントOSの豊富さ				

検疫ネットワーク

治療（アップデート）

強制的なパッチ適用（資産管理システム）

- AssetView、QND、PALLET CONTROL、Altiris、Ecoraなど多様な資産管理システム、パッチ管理システムがある

Microsoft Software Update Service (SUS)

- マイクロソフトのWindows Update Serviceを、中継サーバ(SUS)を用いて、パッチ動作の確認後に公開するなど、企業内で管理できる

アンチウイルス・ベンダー各社のアップデートシステム

- 各社ともに、コンシューマ向けにはインターネット接続でのアップデート、企業向けには統合管理製品で自動アップデート機構を提供

検疫ネットワークでは、上記のような各システムを有効に活用できる必要がある

検疫ネットワーク

ネットマークスの「検疫ネットワーク」

アウトソーシングサービス、ASPサービスとして3カテゴリ

1. 検疫ネットワークサービス ▪ 検疫ネットワークサービス LAN ▪ 検疫ネットワークサービス REMOTE (予定)	接続されたPCを「隔離」し、強制的にコンプライアンス検査を実行するサービスです。設備はすべて、ユーザ様宅内に設置。運用アウトソーシングサービスです。
2. コンプライアンス検査サービス ▪ コンプライアンス検査　エクスプレス ▪ コンプライアンス検査　スタンダード ▪ コンプライアンス検査　プラス	PCの「隔離」を行わず、コンプライアンス検査のみを実行するASP型のサービスです。ユーザはサービスWEBサイトにアクセスし、検査を受けます。
3. 不正PC検出サービス ▪ 不正PC検出サービス ▪ ネット接続PC検出サービス	定期的にネットワークを高速スキャンし、PCを含めネットワークに接続されているIPデバイスを検出します。正規台帳と比較することによって「不正PC」を洗い出します。

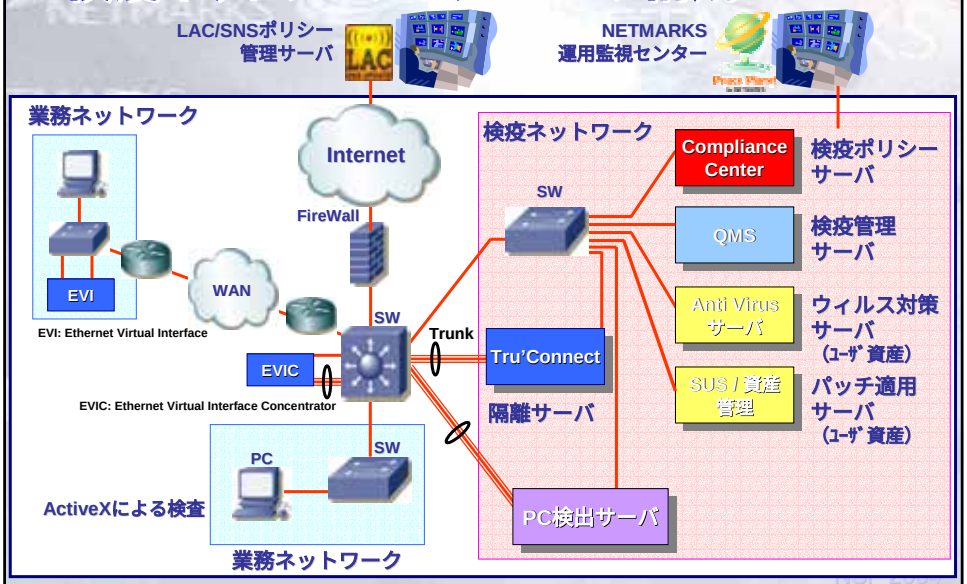
NSF 2004

We are here

 34

検疫ネットワーク

検疫ネットワークネットワーク構成



We are here

 35

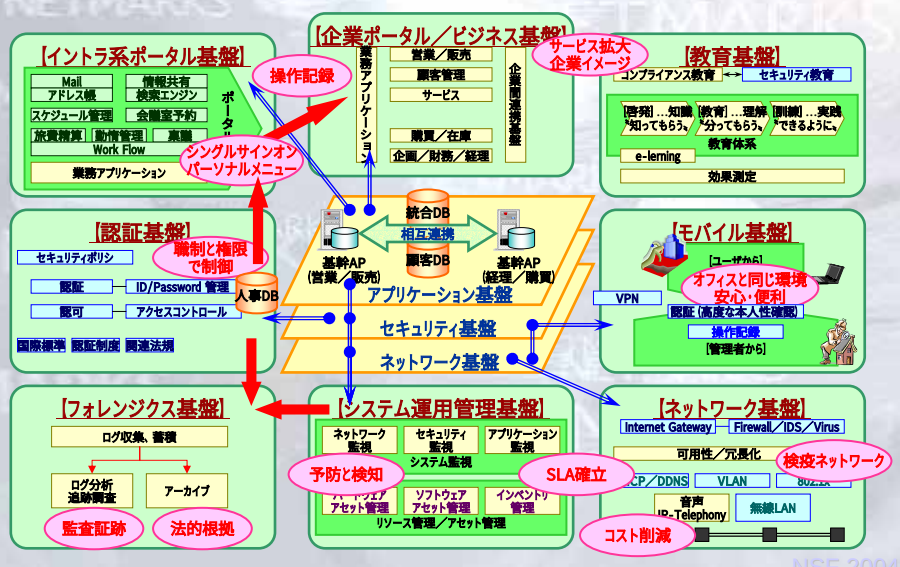
検疫ネットワーク

コンプライアンス検査結果画面

We are here

検疫ネットワーク

「性悪説」と「安全な」ネットワーク



We are here


We are here.
On Customers' Side.
www.netmarks.co.jp
info@netmarks.co.jp
NSF 2004
We are here.
Copyright (c) 2004 NETMARKS INC. 38