FUJITSU

shaping tomorrow with you

iNetSec Inspection Center ご紹介

2015年8月

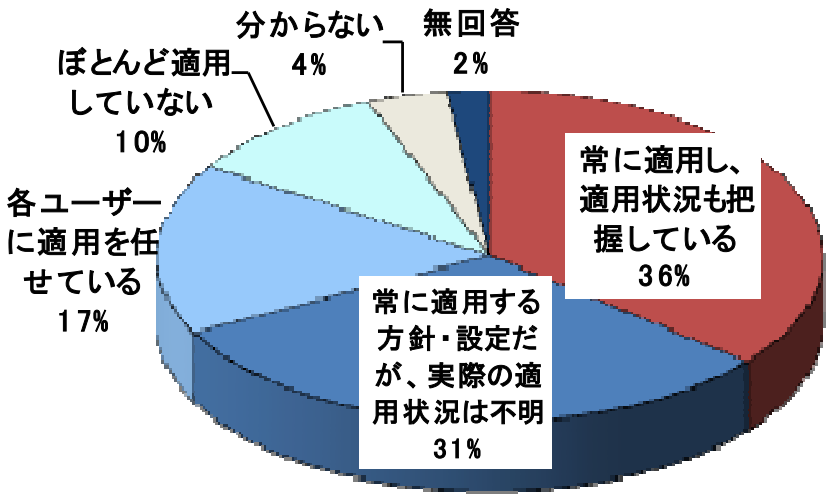
富士通株式会社

パソコンのウィルス対策の現状

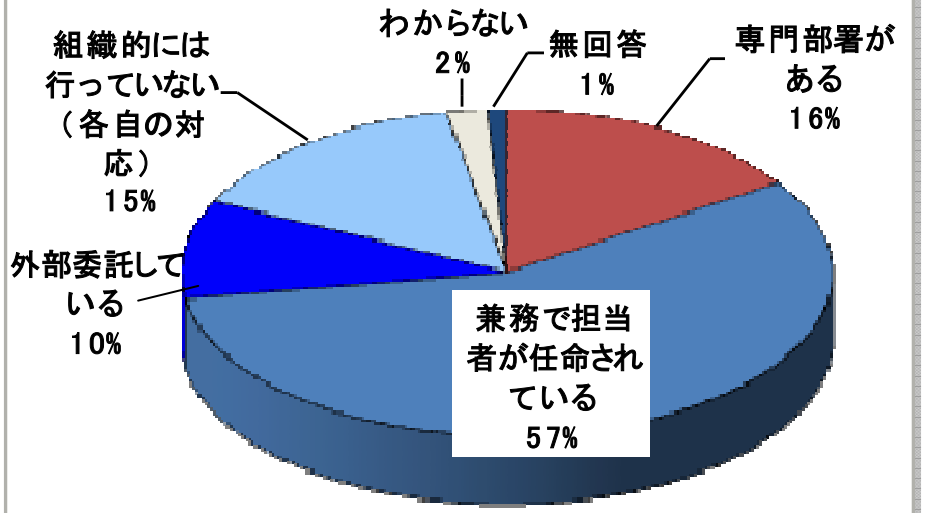
FUJITSU

ウィルス対策ソフトの導入は進んだが、
セキュリティパッチの適用徹底はまだ不充分。

セキュリティパッチの適用状況



ウィルス対策の組織的な対応状況



出典:2013年度 国内における情報セキュリティ事象被害状況調査(IPA)

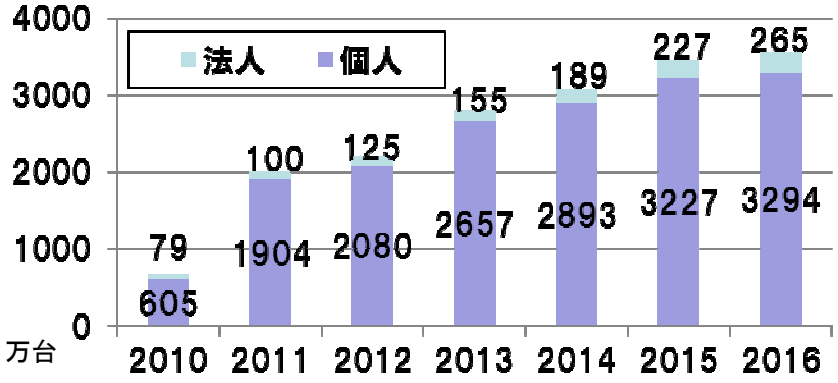
セキュリティパッチの適用徹底には組織的な対応が必要となるが、
企業にとって運用コストUPは課題！

企業ネットワークに接続される機器の多様化

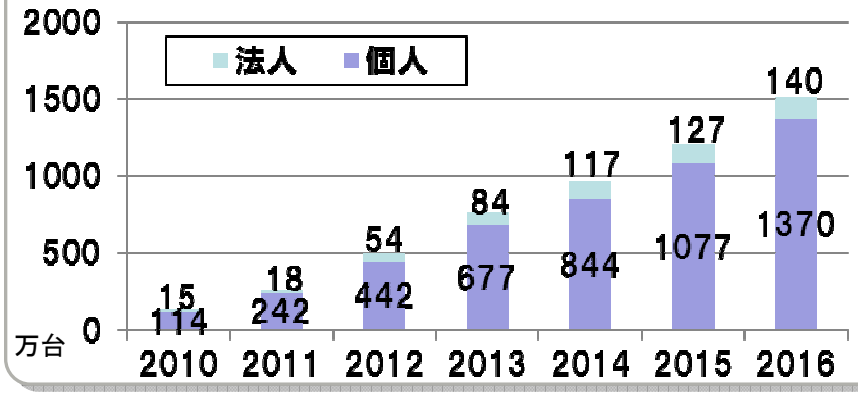
FUJITSU

スマートデバイス（スマートフォン/タブレット）の法人利用も増加傾向。

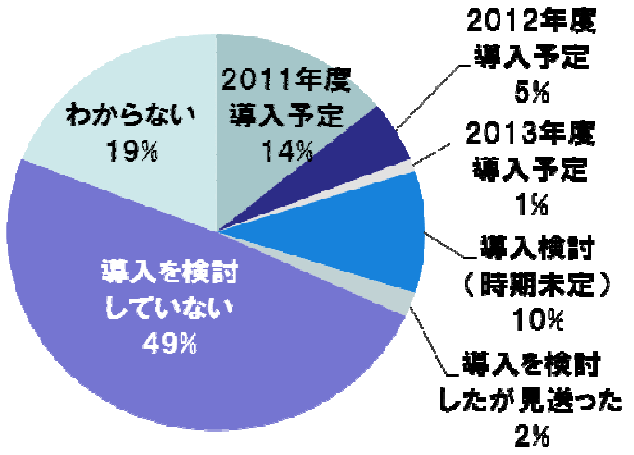
スマートフォン出荷台数



タブレット出荷台数



企業のスマートフォン導入意向

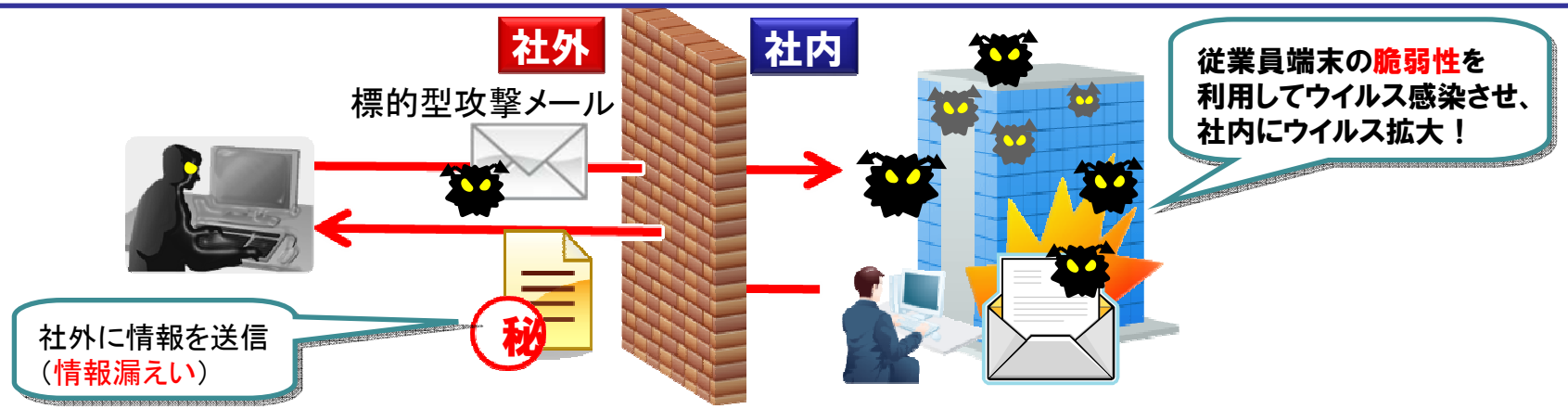


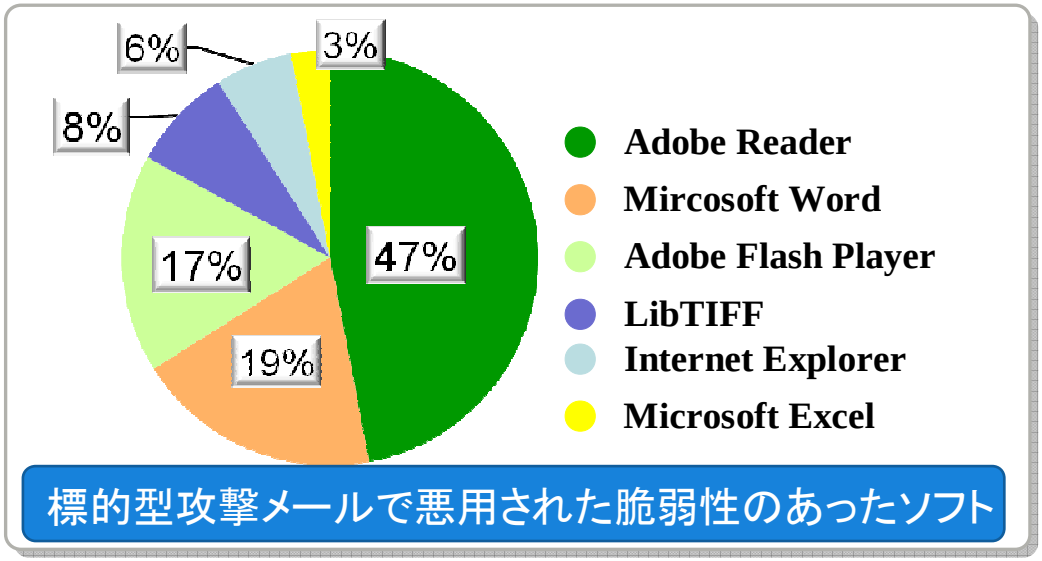
検疫システムを検討する際には、パソコンだけを意識する時代ではありません！！

出展: モバイルコンピューティング推進コンソーシアム

ソフトウェア脆弱性を狙った標的型攻撃メールが増加

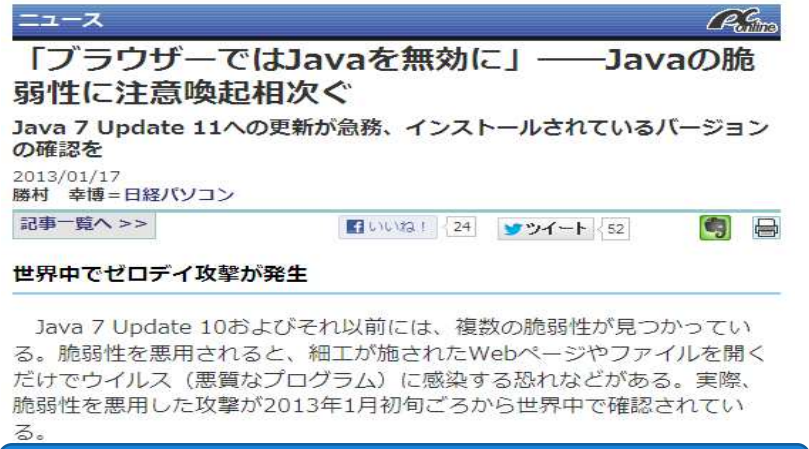
Adobe Reader/Flash Player、Javaの脆弱性を狙った標的型攻撃メールが増加傾向。





標的型攻撃メールで悪用された脆弱性のあったソフト

出展：IPA「標的型サイバー攻撃の事例分析と対策レポート」（2013年1月）


ニュース

「ブラウザーではJavaを無効に」――Javaの脆弱性に注意喚起相次ぐ

Java 7 Update 11への更新が急務、インストールされているバージョンの確認を

2013/01/17
勝村　幸博＝日経パソコン

記事一覧へ >>　いいね！ 24　ツイート 52

世界中でゼロデイ攻撃が発生

Java 7 Update 10およびそれ以前には、複数の脆弱性が見つかっている。脆弱性を悪用されると、細工が施されたWebページやファイルを開くだけでウイルス（悪質なプログラム）に感染する恐れなどがある。実際、脆弱性を悪用した攻撃が2013年1月初旬ごろから世界中で確認されている。

Javaの脆弱性に注意喚起相次ぐ

出展：ITpro News （2013年1月17日）

iNetSec が解決します

FUJITSU

- セキュリティパッチの適用徹底にかかるコストを抑える一つの策として、検疫システムの導入があります。
- これからの検疫システムは、「パソコン」だけではなく「スマートデバイス」も意識したものとすることをお奨めします。
- Windows OS/Microsoft Office/Internet Explorerだけではなく、標的型攻撃メールの対象となっているAdobeやJavaのセキュリティポリシーの徹底も重要です。

iNetSec Inspection Centerであれば、
社内に接続されたパソコンやスマートデバイスの
検疫を実施、セキュリティポリシーを満たさない
機器を隔離します！！

FUJITSU

製品概要

iNetSecシリーズとは

FUJITSU

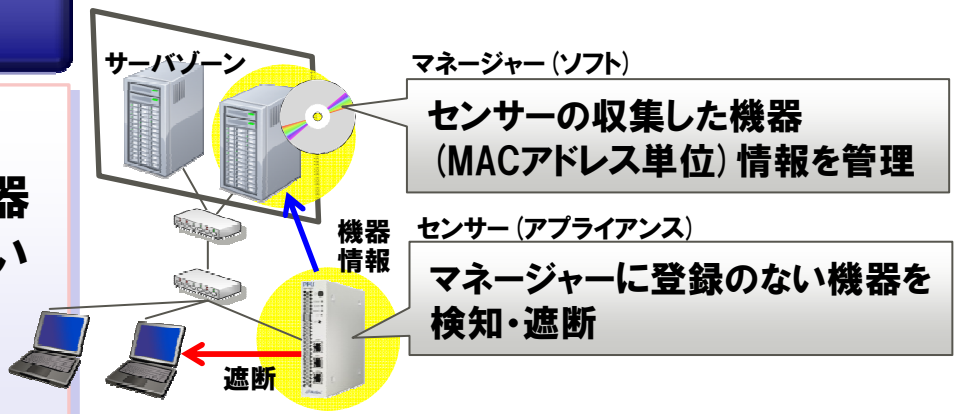
iNetSecは2つの製品群から構成されるセキュリティ製品です。

iNetSec Smart Finder

不正PC接続対策製品

MACアドレスをベースにLANに存在する機器を検知し、持ち込みパソコンなど登録のない機器をネットワークから遮断します。

機器情報収集　　不正PC接続遮断

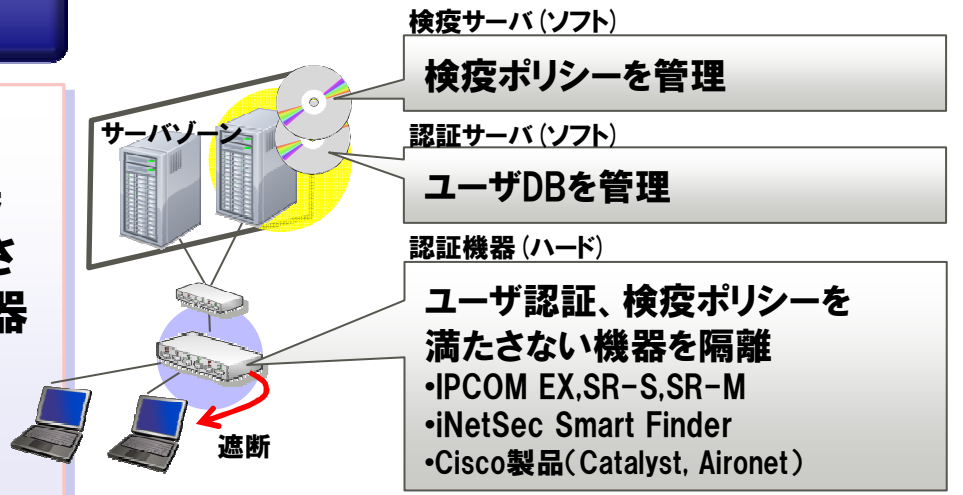


iNetSec Inspection Center

検疫ネットワーク製品

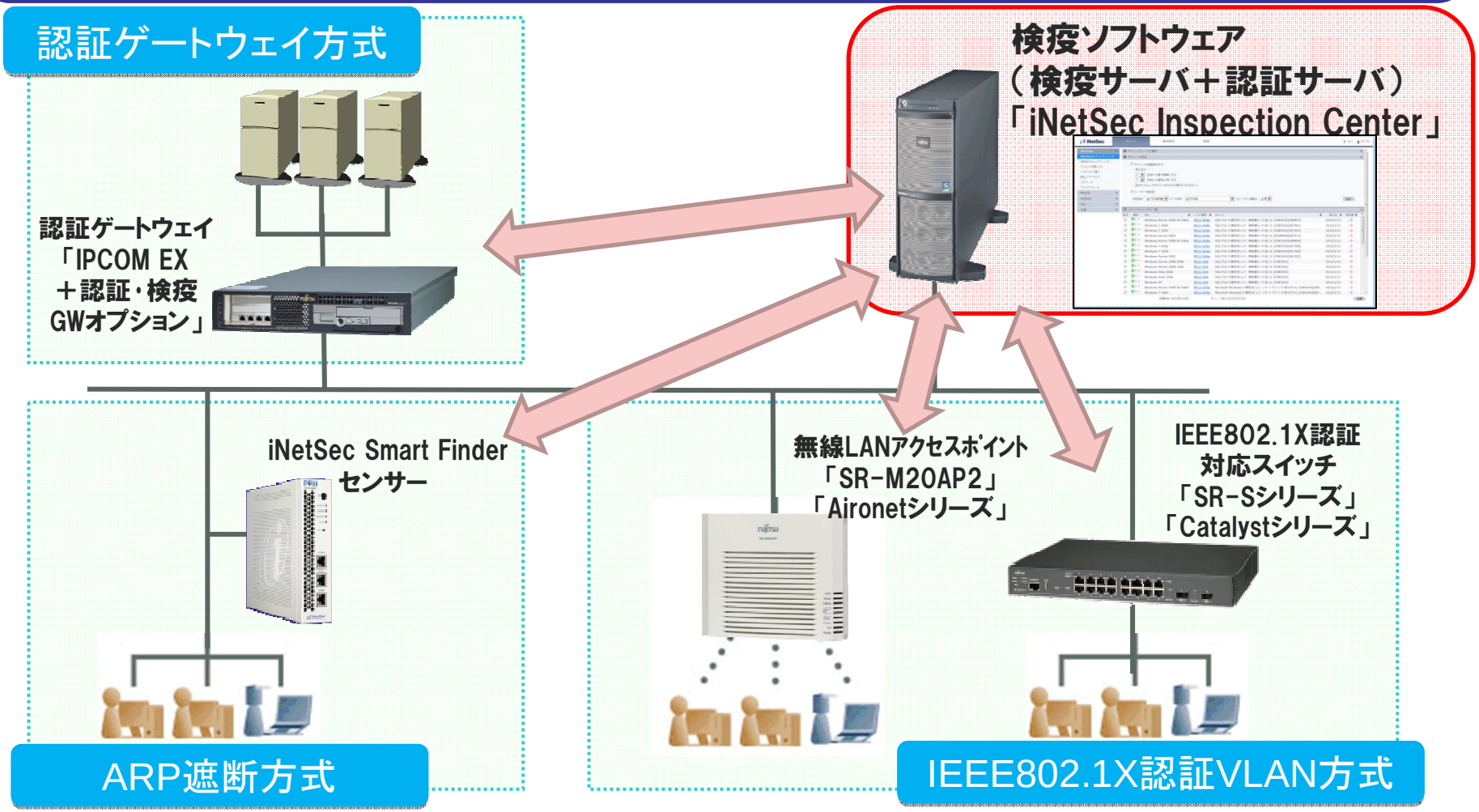
認証機器と連携し、LANに接続される機器の検疫を行い、セキュリティポリシーを満たさない機器を隔離します。さらに隔離した機器には、エラー画面から治療へと誘導します。

ユーザ認証　　セキュリティポリシー検査



iNetSec Inspection Centerとは？

不正利用者や危険なパソコンをネットワークから排除するために
必要なポリシーを定義する検疫ソフトウェアです。



iNetSec Inspection Centerの構成

iNetSec Inspection Centerは、検疫サーバと認証サーバで構成されています。

検疫サーバ

検疫ポリシーを管理

認証サーバ

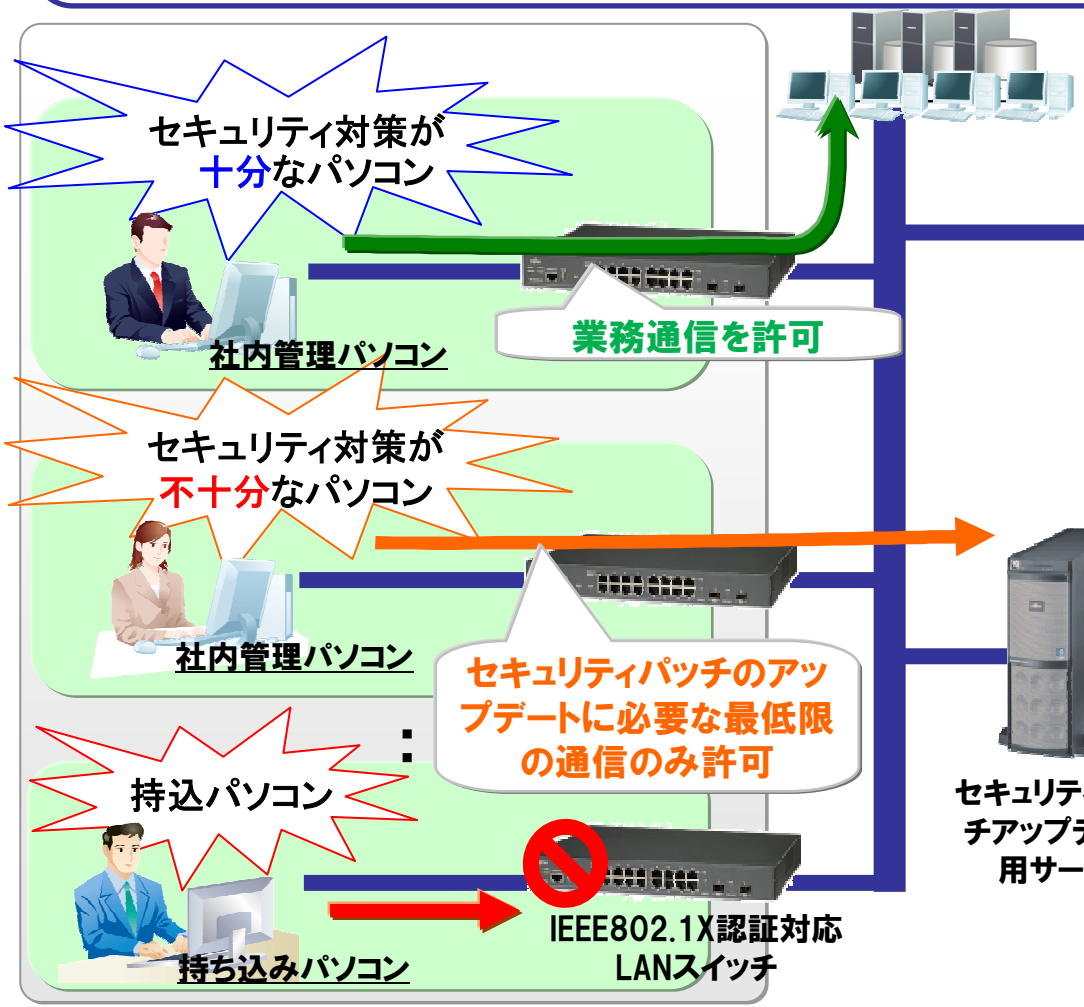
ユーザDBを管理(RADIUSサーバ)

検疫サーバと認証サーバを1台のサーバ上に構築可能です。

(※)サポートする動作環境は検疫サーバ、認証サーバともにLinuxのみ。VMware上でも動作します。
(※)認証サーバ単独での使用不可。認証サーバは検疫サーバのオプション。

検疫ネットワークの役割

ネットワーク機器と組み合わせることで、検疫システムを構築。セキュリティ対策が不十分なパソコンを隔離します。



検疫管理サーバ

iNetSec Inspection Center

■iNetSec Inspection Centerとネットワーク機器を組み合わせることで、
持ち込みパソコン対策だけではなく、
Windowsセキュリティパッチやウイルス対策ソフトのパターンファイルの古いパソコンの隔離が可能

複数の制御方式をサポート

FUJITSU

お客様の要件にあわせてネットワーク機器との組み合わせを選択頂けます。

適用モデル		設置モデル	方式	特徴	富士通提供 ネットワーク機器対応状況
拠点内LANアクセス	センター/フロア	➢ サーバファームやデータセンタの配置場所に認証ゲートウェイを設置 ➢ フロア単位に認証ゲートウェイを設置	認証ゲートウェイ方式	検疫にWebブラウザを利用することで、専用クライアントソフトの導入が必要なくなるため、PC の管理負担が軽い。	IPCOM EXシリーズ
	エッジ（有線，無線）	➢ エッジにネットワーク機器を設置	IEEE802.1X認証VLAN方式	IEEE802.1X認証を利用することで、高いセキュリティレベルの検疫ネットワークシステムを実現可能。	有線LAN SR-Sシリーズ CISCO社製富士通取扱Catalystシリーズ 無線LAN SR-Mシリーズ(SR-M20AP2) CISCO社製富士通取扱Aironetシリーズ
			ARP遮断方式	スイッチの空きポートにセンサーを追加接続するだけで検疫ネットワークシステムを構築可能。	iNetSec Smart Finder
		➢ セキュリティチェックのみ実施、ネットワークでのアクセス制御はなし	ネットワーク制御レス方式	既存のネットワーク構成はそのままに、ソフトウェアのみでシステムを構築可能。	ー
リモートアクセス		➢ VPN装置の後段に認証ゲートウェイを設置	認証ゲートウェイ方式	SSL-VPN接続完了後にリモートアクセス環境における検疫を実現。	IPCOM EXシリーズ

豊富な検疫項目

FUJITSU

認証/検疫	認証/検疫	認証	認証/検疫
			
Windows	MacOS	Linux	スマートデバイス

検査項目	Windows（日本語/英語）	MacOS（日本語/英語）	Linux	スマートデバイス		検査内容
				Android	iOS	
ユーザ認証	○	○	○	○	○	
セキュリティパッチ	○	○	－	○	○	[Windows] Windows / Internet Explorer/Microsoft Office [Mac] [Android] [iOS] OSバージョンのチェック
アプリケーションパッチ	○	－	－	－	－	[Windows] Adobe Reader/Adobe Flash Player/Java
ウイルス対策ソフト	○	○	－	○	－	[Windows] 主要対策ソフト:導入状況/パターンファイル更新状況/リアルタイムスキャン設定状況 任意のウイルス対策ソフト:簡易的な検疫 [Mac] [Android] ソフトウェア導入検査によるウィルス対策ソフト導入状況の確認
ソフトウェア導入	○	○	－	○	－	[Windows] [Mac] [Android] 義務付けソフトウェアの導入状況
禁止ソフトウェア検査	○	－	－	－	－	[Windows] 禁止ソフトウェアの導入状況
パスワード設定	○	－	－	○	－	[Windows] Windowsログオン、スクリーンセーバーのパスワードの設定状況 [Android] スクリーンロックの設定状況
ファイアウォール	○	－	－	－	－	[Windows] パーソナルファイアウォールの設定状況
MACアドレス認証	○	○	－	○	○	管理外機器の不正接続排除
root化/Jailbreak検査	－	－	－	○	○	

（※）スマートデバイス(Android/iOS)に対する検疫機能はiNetSec Inspection Center V7.0L10よりサポート。V6.0以前はユーザ認証のみサポート。
（※）アプリケーションパッチによる検疫機能はiNetSec Inspection Center V7.0L20よりサポート。

スマートデバイス（Android/iOS）検疫

FUJITSU

増え続ける企業ネットワークでのスマートデバイス利用に対しても、iNetSecはネットワーク利用者認証やセキュリティポリシーを徹底することで安心・安全なネットワーク環境を実現します。

iNetSec Inspection Center V7.0L10より Android/iOS端末の検疫をサポート

- Android、iOS端末の個体（MACアドレス）認証により、社給以外のスマートデバイスによるネットワークアクセスを防止
- OSバージョン/ビルド番号のチェック、Root化/Jailbreak検査により、セキュリティレベルの高いスマートデバイスのみネットワークアクセスを許可
- Android端末においては、必須ソフトの導入検査により、ウイルス対策ソフトなどの導入を徹底

（※）スマートデバイスには専用クライアントソフトの導入が必要です。Androidは「Google Play」、iOSは「App Store」より入手頂けます。

スマートデバイス（Android/iOS）検疫

FUJITSU

検査項目	Android	iOS
携帯端末接続許可	OS種別（Android系/iOS系）毎に、接続可否を指定することができます。	
機器認証 （MACアドレス）	MACアドレスであらかじめ管理されているスマートデバイス以外の接続を排除できます。機器認証を行うか否かが、Windwos/MacOS系とは別に選択できます。	
ユーザ認証	ユーザ名/パスワードであらかじめ管理されているユーザ以外の接続を排除できます。クライアント起動時にログイン画面を表示せるか否か（ユーザ認証を行うか否か）を、接続方法（Wi-Fi/VPN）毎に選択できます。	
OSセキュリティ レベル	OSのセキュリティレベルの検査を、OSのバージョンおよびビルド番号により行えます。 OSの系統（2.x系、3.x系、4.x系など）および、端末の機種毎に検査条件を設定することができます。	OSのセキュリティレベルの検査を、OSのバージョンにより行えます。 端末の機種毎に検査条件を設定することができます。
ウイルス対策 ソフト	導入を義務づけたウィルス対策ソフトの導入検査を、後述のソフトウェア導入検査機能により行えます。なお、パターンファイルのアップデートについては検査できません。	行えません。
ソフトウェア導入	導入を義務づけた任意のソフトウェア（代替ソフトウェアを含む）の導入検査を、パッケージ名と版数により行えます。 OSの系統（2.x系、3.x系、4.x系など）および、端末の機種毎に検査条件を設定することができます。	行えません。
禁止ソフトウェア	行えません。	
パスワード	スクリーン（画面）の自動ロックおよび、ロック解除時の認証設定について検査できます。	行えません。
ファイアウォール	行えません。	
root化/Jailbreak 検査	ユーザーモードがroot権限に変更されていないかを検査できます（root化検査）。	保護機能（不正なアプリケーションの起動防止など）が解除されていないかを検査できます（Jailbreak検査）。

アプリケーション（Adobe/Java）検疫

FUJITSU

アプリケーション検疫機能によって、脆弱性が確認された版数のAdobe Reader/Adobe Flash Player/Javaがインストールされたパソコンを隔離。iNetSecは、標的型攻撃メールによる情報漏えい対策を実現します。

iNetSec Inspection Center V7.0L20より Adobe Reader/Adobe Flash Player/Java の検疫をサポート

- Adobe社, Oracle社の公開情報に基づき、版数一覧と脆弱性有無を収録したiNetSec専用検疫辞書ファイルを提供
- セキュリティポリシーに反した版数がインストールされたパソコンや、脆弱性の確認された版数がインストールされたパソコンを隔離

（参考）制御方式毎の認証/検疫対象OS

制御方式毎に検疫可能なOSが異なりますので、ご注意願います。

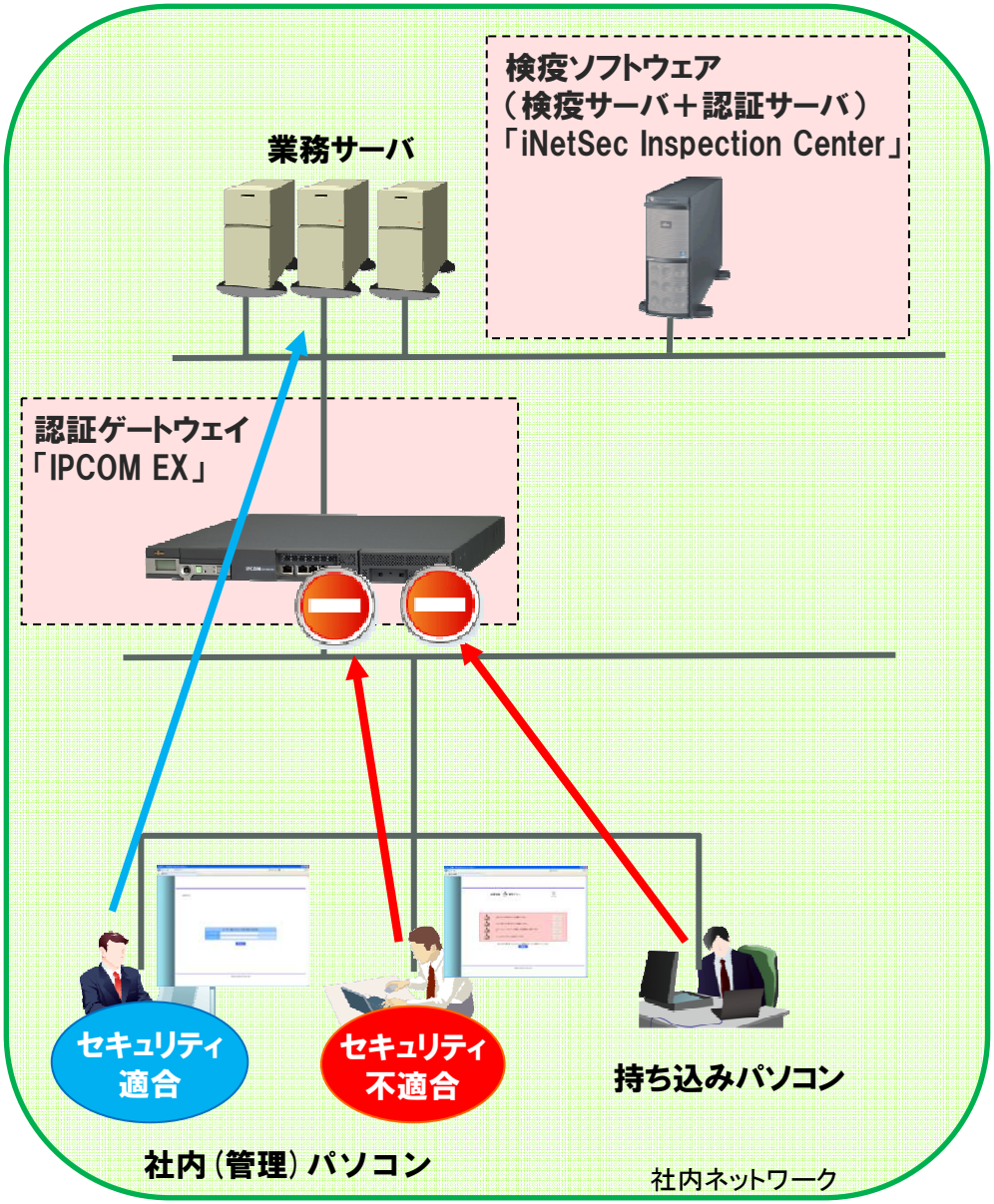
方　式	サポートOS			
	Windows （日本語/英語）	Mac OS （日本語/英語）	Linux （日本語）	Android/iOS （日本語/英語）
認証ｹﾞｰﾄｳｪｲ方式	○	○	○ (*1)	○
IEEE802.1X認証VLAN方式	○	－	－	－
ARP遮断方式	○	○	○ (*1)	○
ネットワーク制御レス方式	○	○	○ (*1)	○

(*1) Linux は検疫（セキュリティ監査）を実施せず、ユーザ認証による運用となります。

FUJITSU

各制御方式の概要

認証ゲートウェイ方式



■ 特長

- 既存ネットワークの設計変更や、機器の入れ替えをほとんど伴わずに導入が可能。
- WEB型クライアントにより、クライアントソフトのインストールが不要（専用クライアントソフトによる検疫も可能）。
- IPCOM EXとクライアントPCの間にルータやL3スイッチが存在しても、認証が可能。

■ 検疫システムの動作（概要）

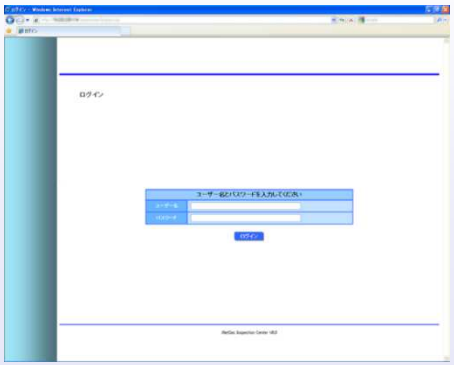
①検疫対象パソコンからWEBブラウザで任意のURLにアクセスすると自動的に検疫画面にリダイレクト。

②検疫OKのパソコンは認証ゲートウェイ上に設定されたアクセスコントロール条件に従った通信が可能。検疫NGのパソコンは認証ゲートウェイ上に設定されたアクセスコントロール条件に従ってWSUS等の治癒サーバへの通信のみ可能。

認証ゲートウェイ方式 利用者イメージ

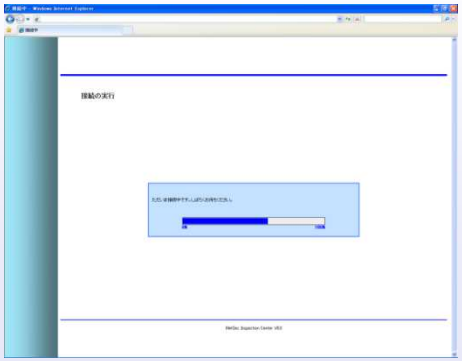
① 利用者認証

- Windowsにログオンし、最初にInternet Explorerを起動して認証画面を表示します。
- ユーザ名とパスワードを入力し、接続を実行します。ユーザ認証を省略することもできます。



② 検疫の実行

- 認証と検疫が実施されます。
- ユーザ認証はiNetSec Inspection Center 認証サーバのユーザDBで行います。



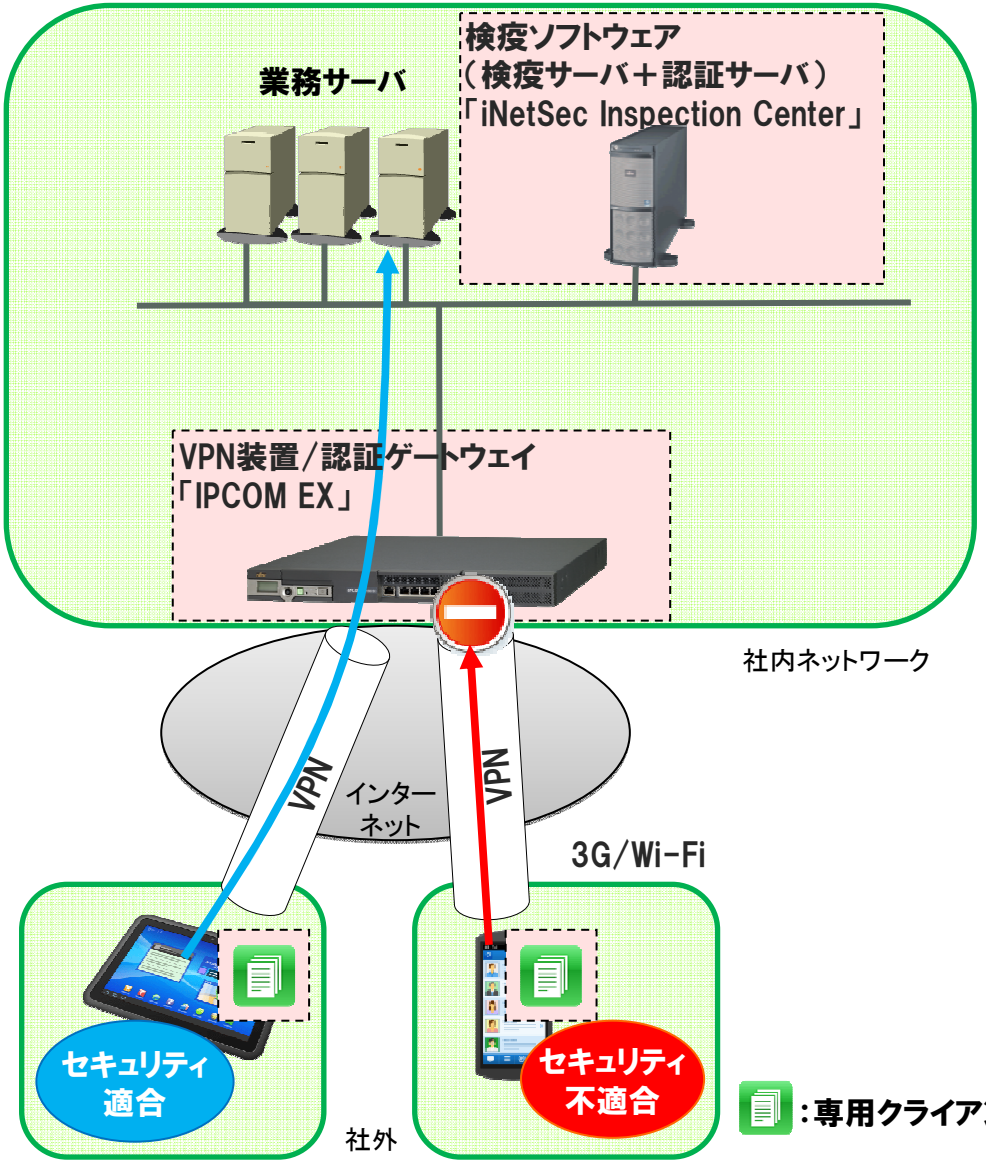
③-1 検疫結果NG

- 検疫の結果、セキュリティに問題があるクライアントは、警告画面が表示されます。
- 警告画面をクリックし、セキュリティのアップデートを実施します

③-2 ネットワークにログオン

- 検疫結果OKを確認し、本来のアクセスすべきサイトを表示します。

認証ゲートウェイ方式によるスマートデバイス検疫



■ 特長

- 検疫対象スマートデバイスには、VPNクライアントソフトとともに、セキュリティ検査を実施するための専用クライアントソフトのインストールが必須。

■ 検疫システムの動作（概要）

①VPN接続完了後、専用クライアントソフトを起動しセキュリティ検査を実施。

②検疫OKのスマートデバイスは認証ゲートウェイ上に設定されたアクセスコントロール条件に従った通信が可能。検疫NGのスマートデバイスは認証ゲートウェイ上に設定されたアクセスコントロール条件に従ってセキュリティ不適合時に実施する項目が記載されたWebサーバへの通信のみ確保する等を実施。

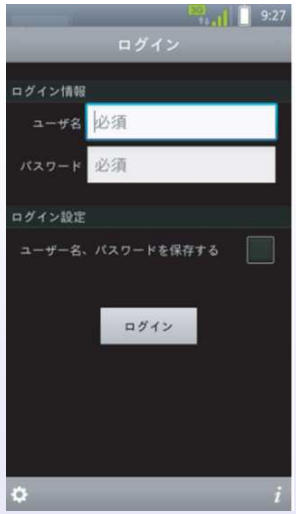
：専用クライアントソフトの導入必須

認証ゲートウェイ方式によるスマホ検疫 利用者イメージ

① 利用者認証

- Android 端末(※)、iOS 端末ともにVPN接続完了後に専用クライアントを手動起動が必要です。
- ログイン画面でのユーザー認証は設定により省略可能で、省略時は②の接続中画面が初めに表示されます。

※ Android 2.2/2.3/3.0/3.1/3.2では、VPN接続完了後に専用クライアントの自動機能が可能でしたが、Andoroid4.0以降は手動起動が必須となりました。



② 検疫の実行

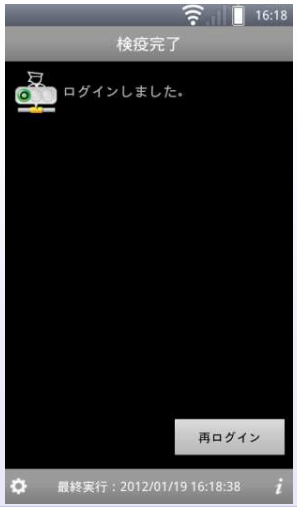
- 認証と検疫が実施されます。

③-1 検疫結果NG

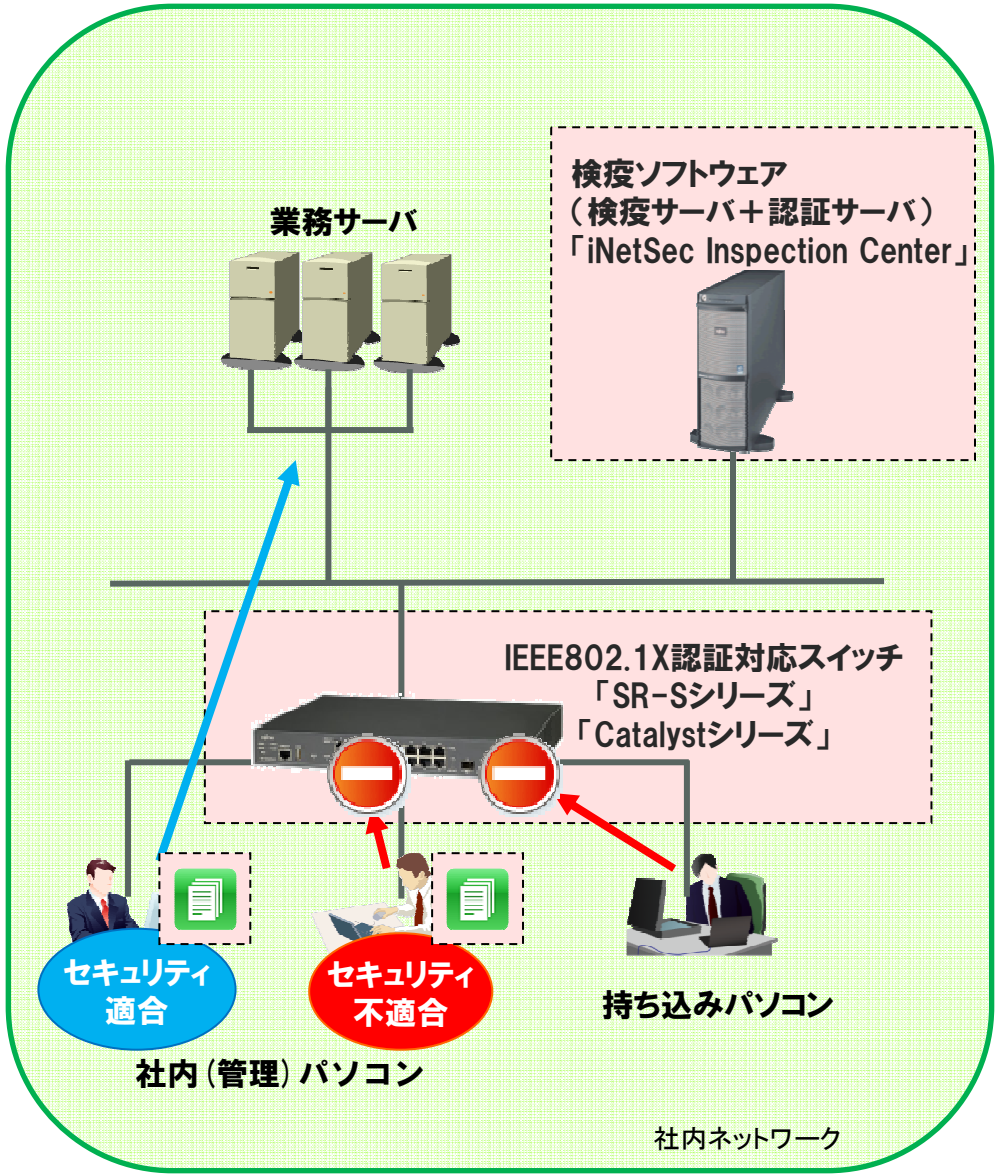
- 検疫処理の結果、検疫ポリシー違反があると、検疫ポリシー違反画面にメッセージが表示されます。メッセージに従って対処し、再度ログインしてください。

③-2 ネットワークにログイン

- 検疫処理の結果、OKとなった場合は、ネットワークに接続できるようになります。



IEEE802.1X認証VLAN方式



：専用クライアントソフトの導入必須

■ 特長

- 既存ネットワークの設計変更を伴うものの、IEEE802.1X認証を利用することで、高いセキュリティレベルの検疫ネットワークシステムを実現可能。
- LANスイッチに加えて、無線LANアクセスポイント(SR-M、Aironet)との連携も可能。
- 検疫対象パソコンには、Windows標準サプリカントとともに、専用クライアントソフトの導入が必須。

■ 検疫システムの動作（概要）

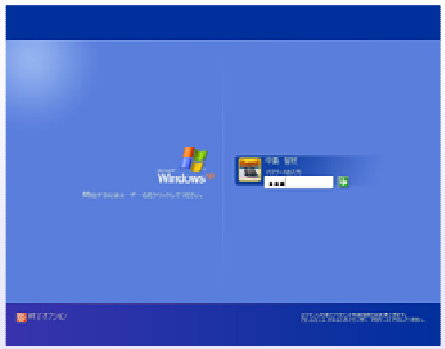
①IEEE802.1X認証にあわせて、専用クライアントソフトによってセキュリティ検査を実施（詳細は次ページを参照のこと）。

②検疫OKのパソコンに対してIEEE802.1X認証対応スイッチ（もしくは無線LANアクセスポイント）は検疫OK用VLAN（業務サーバとの通信が可能なVLAN）を割り当て。検疫NGのパソコンに対しては検疫NG用VLAN（WSUS等の治癒サーバへの通信のみ可能なVLAN）を割り当て。

IEEE802.1X認証VLAN方式 利用者イメージ

① Windowsにログオン

- Windowsにログオンします



② 自動的に認証＆検疫

- Windows標準サプリカントによる認証作業完了後、専用クライアントソフトが自動的に検疫を実行します

③-1 検疫NG

- 検疫の結果、セキュリティに問題があるパソコン上には検疫エラー画面が表示されます。[詳細]ボタンをクリックし、エラーの内容に従って対処を行います

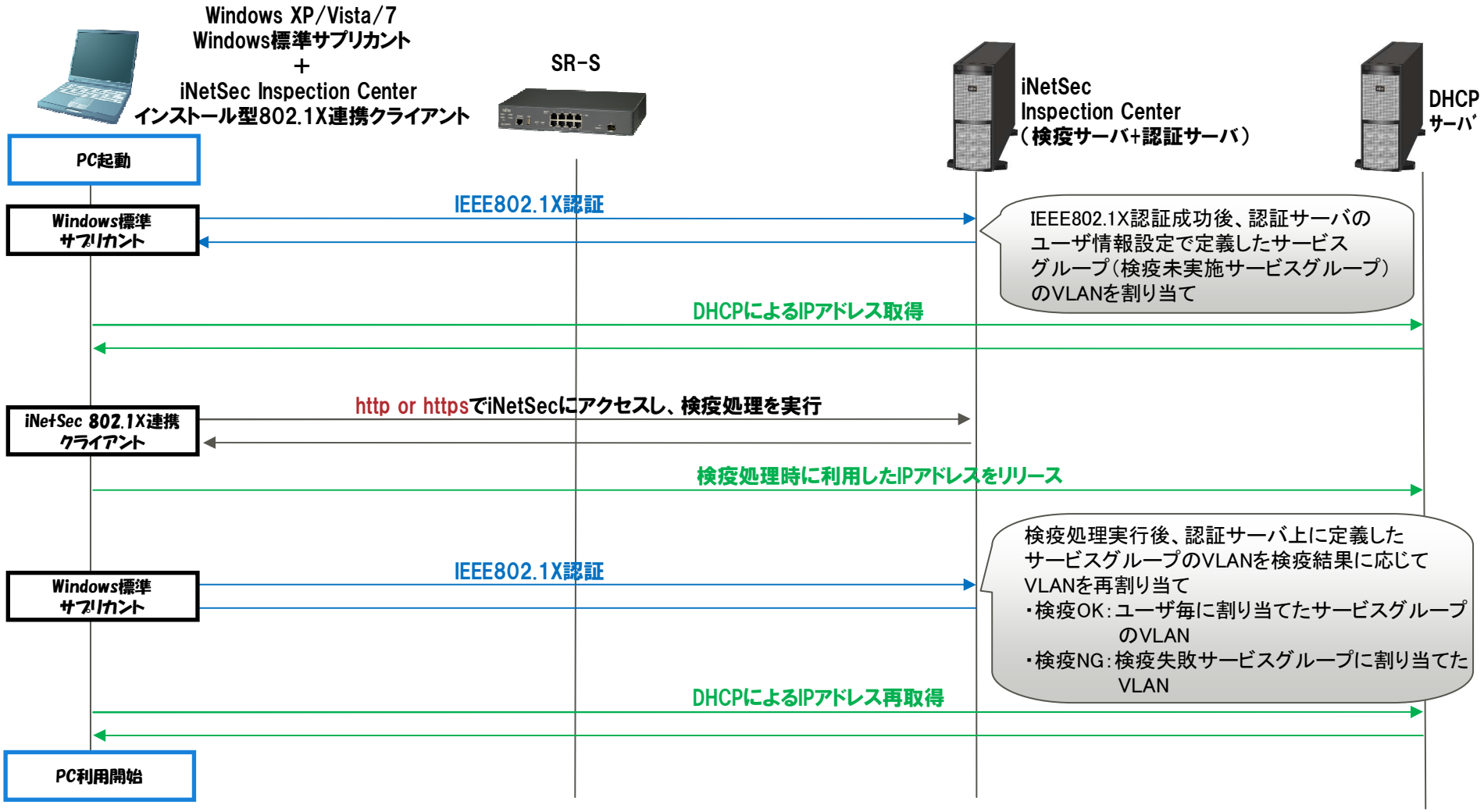
③-2 検疫OK

- セキュリティに問題がないパソコン上には検疫成功を示す画面が表示されます。

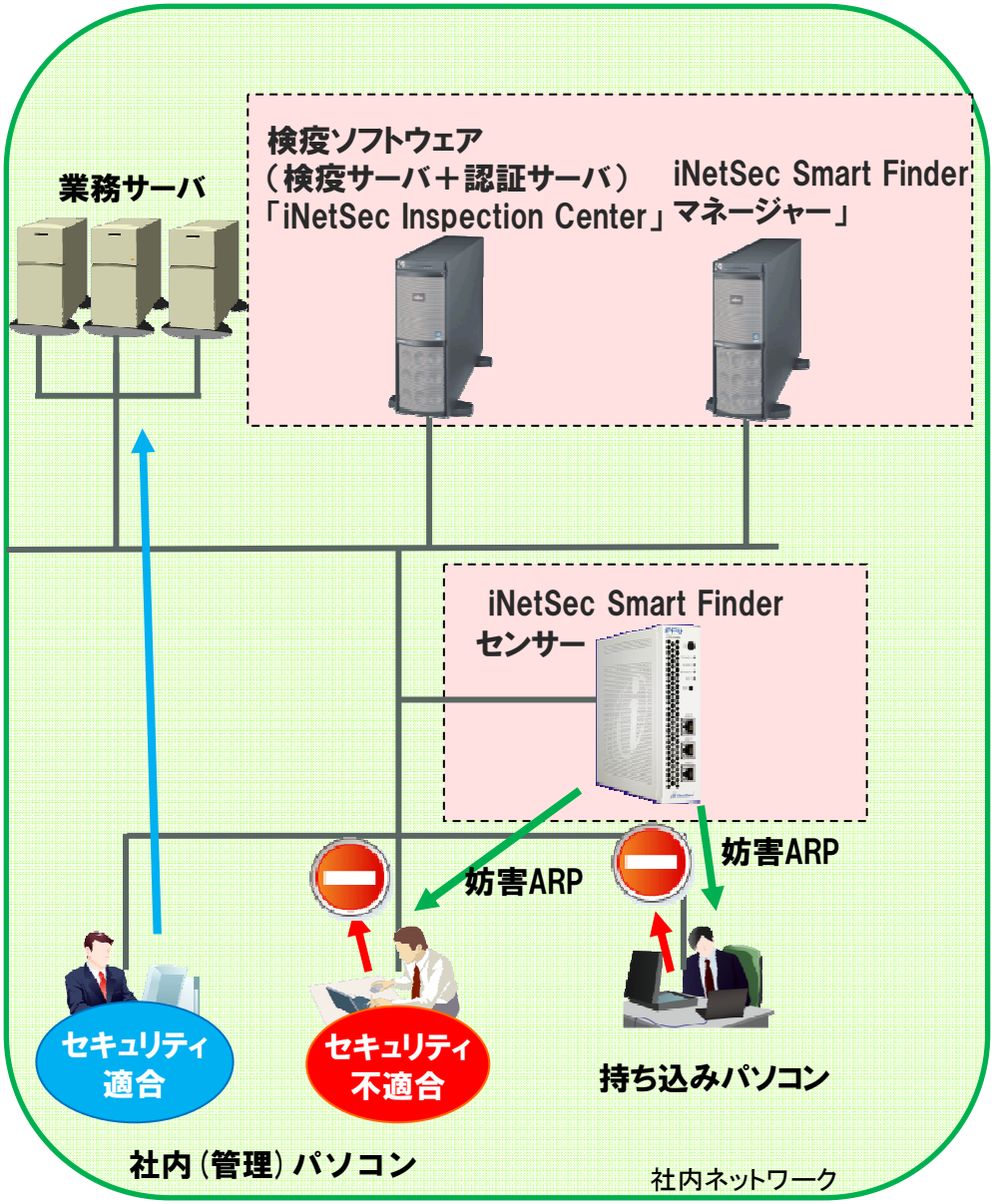
（参考）IEEE802.1X認証VLAN方式 実行時の流れ

■ PC起動後の認証・検疫処理の流れ（概要）

■ IEEE802.1X認証（ユーザ認証のみ）＋検疫（セキュリティ検査）



ARP遮断方式



■ 特長

- 既存ネットワークの設計変更を伴わず、センサーを既存ネットワークにアドオン追加可能。
- WEB型クライアントにより、クライアントソフトのインストールが不要（専用クライアントソフトによる検疫も可能）。

■ 検疫システムの動作（概要）

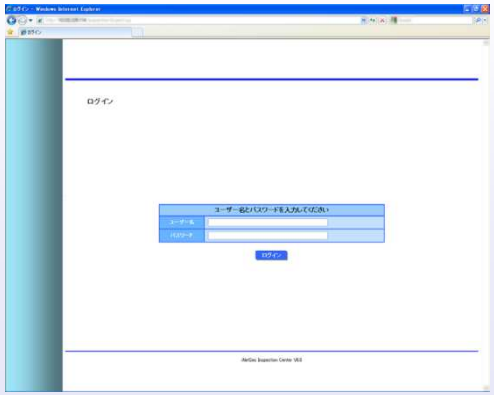
①検疫対象パソコンからWEBブラウザで任意のURLにアクセスすると自動的に検疫画面にリダイレクト（全ての検疫対象パソコンに対して妨害ARPを送信し、通信を遮断）。

②検疫OKのパソコンは業務サーバとの通信が可能（センサーより通信可能となるようなARPを送信し、妨害ARPによって誤学習状態のARPテーブルを正しい状況に自動更新）。

ARP遮断方式 利用者イメージ

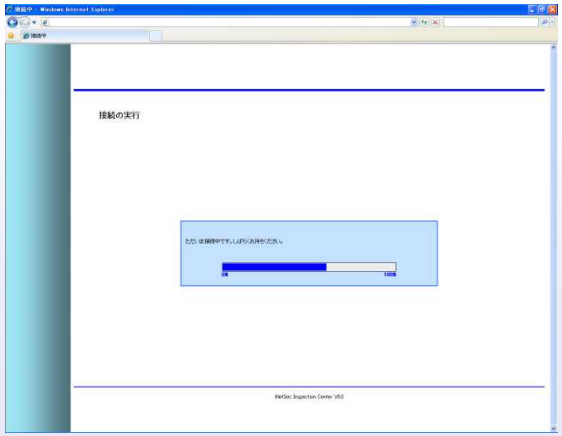
① 利用者認証

- Windowsにログオンし、最初にInternet Explorerを起動して認証画面を表示します。
- ユーザ名とパスワードを入力し、接続を実行します。ユーザ認証を省略することもできます。



② 検疫の実行

- 認証と検疫が実施されます
- 認証はRADIUSのユーザDBで行います



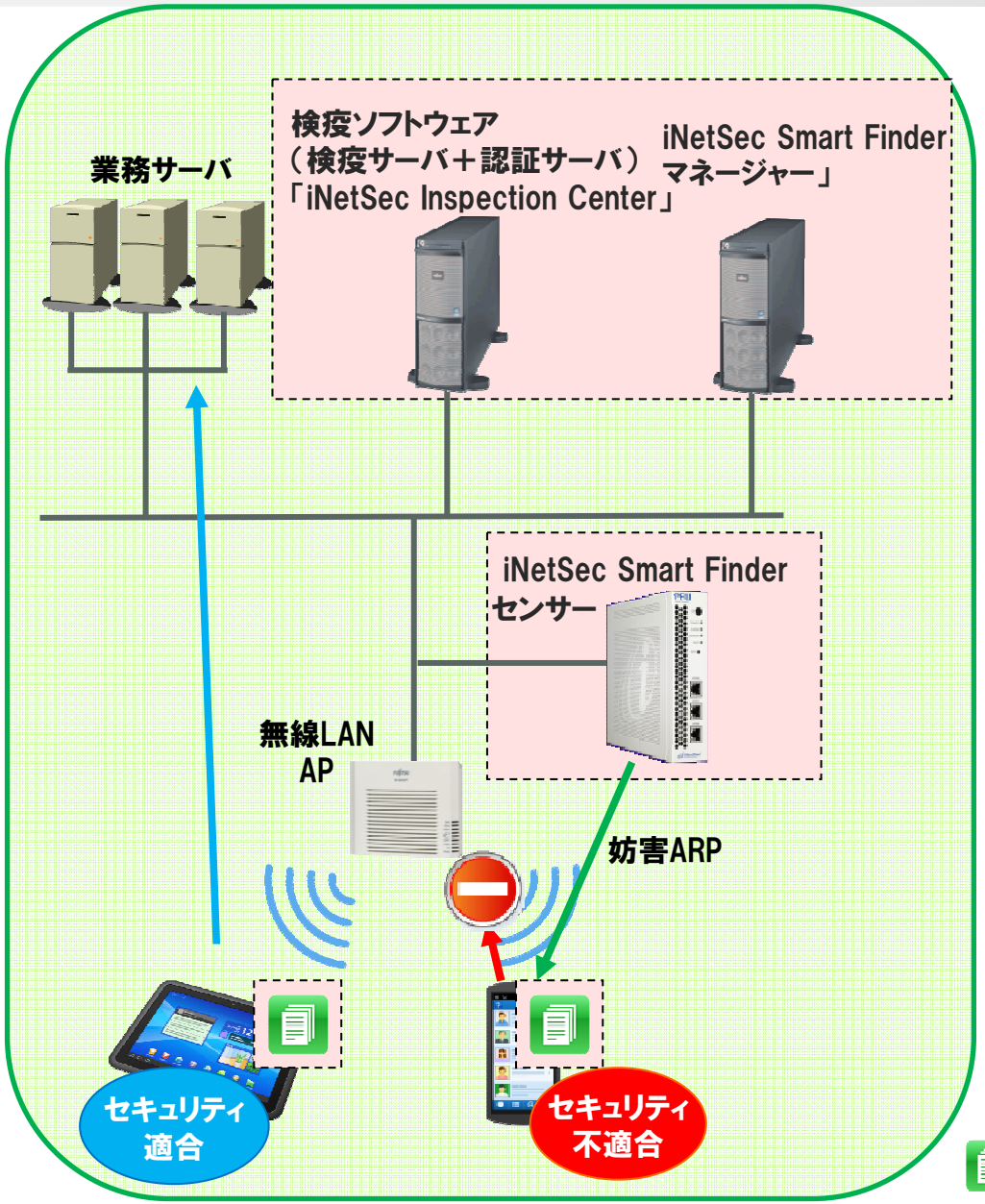
③-1 検疫結果NG

- 検疫の結果、セキュリティに問題があるクライアントは、警告画面が表示されます。
- 警告画面をクリックし、セキュリティのアップデートを実施します

③-2 ネットワークにログオン

- 検疫結果OKを確認し、本来のアクセスすべきサイトを表示します。

ARP遮断方式によるスマートデバイス検疫



■ 特長

- 既存ネットワークの設計変更や、機器の入れ替えをほとんど伴わずに導入が可能。
- 検疫対象スマートデバイスには、VPNクライアントソフトとともに、セキュリティ検査を実施するための専用クライアントソフトのインストールが必須。

■ 検疫システムの動作（概要）

①Wi-Fi接続完了後、検疫対象スマートデバイスにて専用クライアントソフトを手動起動し、セキュリティ検査を実施。

②検疫OKのスマートデバイスは、業務サーバとの通信が可能（センサーより通信可能となるようなARPを送信し、妨害ARPによって誤学習状態のARPテーブルを正しい状況に自動更新）。検疫NGのスマートデバイスは、iNetSec Smart Finderマネージャー上に規定したセキュリティ不適合時に実施する項目が記載されたWebサーバへの通信のみ確保する等を実施。

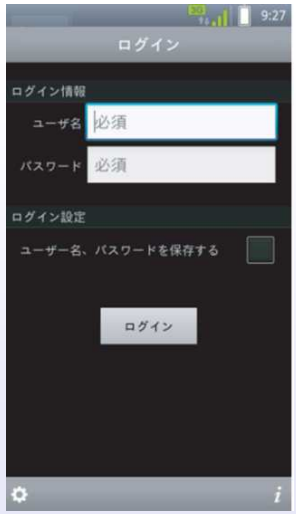
（※）無線LAN APのProxy ARP動作によっては、正しく動作できない可能性もあります（無線LAN APがSR-M20AP2の場合には、検知動作およびネットワーク利用申請動作は問題なく利用できます）。

：専用クライアントソフトの導入必須

ARP遮断方式によるスマホ検疫 利用者イメージ

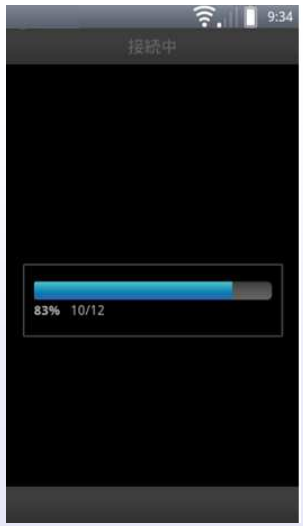
① 利用者認証

- Android、iOS端末ともにWi-Fi接続完了後、専用クライアントを手動起動します。
- ログイン画面でのユーザー認証は設定により省略可能で、省略時は②の接続中画面が初めに表示されます。



② 検疫の実行

- 認証と検疫が実施されます。

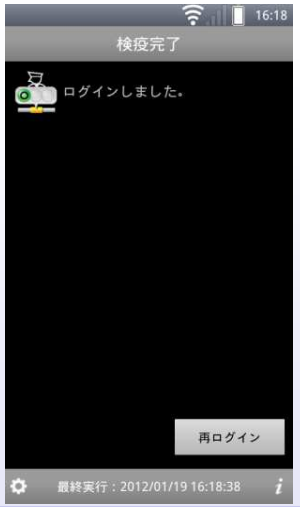


③-1 検疫結果NG

- 検疫処理の結果、検疫ポリシー違反があると、検疫ポリシー違反画面にメッセージが表示されます。メッセージに従って対処し、再度ログインしてください。

③-2 ネットワークにログイン

- 検疫処理の結果、OKとなった場合は、ネットワークに接続できるようになります。



FUJITSU

動作環境

制御方式毎の認証/検疫対象OS(Windows)

FUJITSU

Windows

方　式		日本語	英語
認証ｹﾞｰﾄｳｪｲ方式 ARP遮断方式 ﾈｯﾄﾜｰｸ制御ﾚｽ方式 (*1) (*2)	ユーザ認証のみ可能	Windows NT4.0, Windows98 SE, Windows Me, Windows 2000	Windows 2000
	ユーザ認証・検疫が可能	Windows Server 2003 (R2含む), Windows Server 2008 (R2含む), Windows Server 2012 (R2含む), Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1	Windows Server 2003 (R2含む), Windows Server 2008 (R2含む), Windows Server 2012 (R2含む), Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1
IEEE802.1X認証VLAN方式 (*3)		Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1	Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1

(*1) 認証ゲートウェイ方式/ARP遮断方式/ネットワーク制御レス方式では、Webブラウザを使った検疫方式とインストール型専用クライアントを使った検疫方式の2パターンを提供。Webブラウザ型の場合、Internet Explorer 6, 7, 8, 9, 10, 11(ActiveXコントロール)に対応。
(*2) Windows 8/Windows 8.1/Windows Server 2012 の場合、Webブラウザを使った検疫方式ではデスクトップアプリケーション(従来のWindowsアプリケーション)のInternet Explorer 10, 11 (ActiveXコントロール)のみをサポート。インストール型専用クライアントについてもデスクトップアプリケーションとして動作。
(*3) Windows 8/Windows 8.1の場合、IEEE802.1X認証VLAN方式で必須となるインストール型802.1X連携クライアントはデスクトップアプリケーションとして動作。

制御方式毎の認証/検疫対象OS(Mac/Linux)

FUJITSU

Mac

方　式		日本語	英語
認証ｹﾞｰﾄｳｪｲ方式 ARP遮断方式 ﾈｯﾄﾜｰｸ制御ﾚｽ方式 (*1)	ユーザ認証・検疫が可能	Mac OS X 10.5, 10.6, 10.7, 10.8, 10.9, 10.10	Mac OS X 10.5, 10.6, 10.7, 10.8, 10.9, 10.10

(*1) 認証ゲートウェイ方式/ARP遮断方式/ネットワーク制御レス方式では、Webブラウザを使った検疫方式のみサポート。
Webブラウザはは Safari 4.1, 5.0, 5.1, 6.0, 6.1, 7, 8に対応。Java Runtime Environment 5.0, 6, 7, 8も必要。

Linux

方　式		日本語 (*1)	英語
認証ｹﾞｰﾄｳｪｲ方式 ARP遮断方式 ﾈｯﾄﾜｰｸ制御レス方式 (*2)	ユーザ認証のみ	Red Hat Enterprise Linux 5.2/5.3/5.4/5.5/5.6/5.7/5.8/5.9/5.10/6.0/6.1/6.2/6.3/6.4/6.5/7.0 Server (x86) Red Hat Enterprise Linux ES 4.6/4.7/4.8/4.9 (x86) Red Hat Enterprise Linux 5.2/5.3/5.4/5.5/5.6/5.7/5.8/5.9/5.10/6.0/6.1/6.2/6.3/6.4/6.5/7.0 Client (x86) Red Hat Enterprise Linux 3 Update 8/9 ES, 8/9 WS (x86) Red Hat Desktop 4.6/4.7/4.8/4.9 (x86)	ー

(*1) インストール時の言語として、日本語を選択したもののみ対象。
(*2) 認証ゲートウェイ方式/ARP遮断方式/ネットワーク制御レス方式では、Webブラウザを使ったユーザ認証のみサポート。
Webブラウザは Firefox3.6, 10, 17,24,31またはOpera10.63, 11.x(11.60以降), 12に対応。Java Runtime Environment 5.0, 6.0, 7.0も必須。

制御方式毎の認証/検疫対象OS(スマートデバイス)

Android/iOS/Windows RT

方　式		日本語	英語
認証ｹﾞｰﾄｳｪｲ方式 ARP遮断方式 ﾈｯﾄﾜｰｸ制御ﾚｽ方式	ユーザ認証のみ可能 (*1)	Android 1.6, 2.0, 2.1, 2.2, 2.3, 3.0, 3.1, 3.2, 4.0, 4.1, 4.2, 4.3, 4.4, 5.0 iOS 3, 4, 5, 6, 7, 8 Windows RT	Android 1.6, 2.0, 2.1, 2.2, 2.3, 3.0, 3.1, 3.2, 4.0, 4.1, 4.2, 4.3, 4.4, 5.0 iOS 3, 4, 5, 6, 7, 8 Windows RT
	ユーザ認証・検疫が可能 (*2)	Android 2.2, 2.3, 3.0, 3.1, 3.2, 4.0, 4.1, 4.2, 4.3, 4.4, 5.0 iOS 4, 5, 6, 7, 8	Android 2.2, 2.3, 3.0, 3.1, 3.2, 4.0, 4.1, 4.2, 4.3, 4.4, 5.0 iOS 4, 5, 6, 7, 8

(*1) Webブラウザを使ったユーザ認証のみサポート。
Webブラウザは標準搭載のWebブラウザに対応。

(*2) 専用クライアントのインストールが必須。

動作環境

検疫サーバ、認証サーバ

CPU	Intel Xeon 1.60GHz または同等以上のプロセッサを推奨
メモリ	実メモリ：1GB 以上を推奨、スワップ容量：1GB以上を推奨
HDD	1GB以上の空きディスク
OS	Red Hat Enterprise Linux 5.7, 5.8, 5.9, 5.10, 5.11 Server (x86) (*1) Red Hat Enterprise Linux 6.1, 6.2, 6.3, 6.4, 6.5, 6.6 Server (x86) (*1)

(*1) 製品のサポートOSを正式にサポートしているVMware Hypervisorでご利用いただけます。
ただし、VMware固有機能(Fault ToleranceやHigh Availability)のサポート状況については、お問合せください。

運用管理端末

＊ 検疫サーバ、認証サーバに対してWebブラウザで接続し、
各種設定/管理を行うための端末

CPU	サポートOSの推奨するCPU以上
メモリ	サポートOSの推奨するメモリ以上
HDD	2MB以上
OS (*2)	Windows XP, Windows Vista, Windows 7, Windows 8 (*3), Windows 8.1 (*3), Windows Server 2003 (R2含む) (*4), Windows Server 2008 (R2含む) (*4), Windows Server 2012 R2 (*3)
必須ソフトウェア (*5)	Internet Explorer 7, Internet Explorer 8, Internet Explorer 9, Internet Explorer 10 (*6), Internet Explorer 11 (*7)

(*2) 日本語版のみサポート。(*3) デスクトップ版のブラウザにのみ対応しています。
(*4) Server Core およびHyper-V には対応していません。(*5) 互換表示はサポートしていません。
(*6) Windows 7および、Windows 8のInternet Explorer 10のみサポートしています。
(*7) Windows 7、Windows 8.1および、Windows Server 2012 R2のInternet Explorer 11のみサポートしています。

標準価格・保守サービス

標準価格

製品名	富士通型名	標準価格	補足
iNetSec Inspection Center V7.0 サーバパッケージ	FSPG23112	¥300,000	検疫サーバ
iNetSec Inspection Center V7.0 認証サーバパッケージ	FSPG23212	¥800,000	認証サーバ
iNetSec Inspection Center V7.0 クライアントライセンス10	FSPG25112	¥80,000	全ての方式で検疫対象となるパソコンの台数だけ本ライセンスが必須
iNetSec Inspection Center V7.0 クライアントライセンス100	FSPG25122	¥500,000	
iNetSec Inspection Center V7.0 クライアントライセンス1,000	FSPG25132	¥4,000,000	
iNetSec Inspection Center V7.0 クライアントライセンス5,000	FSPG25142	¥17,500,000	
iNetSec Inspection Center V7.0 クライアントライセンス10,000	FSPG25152	¥30,000,000	

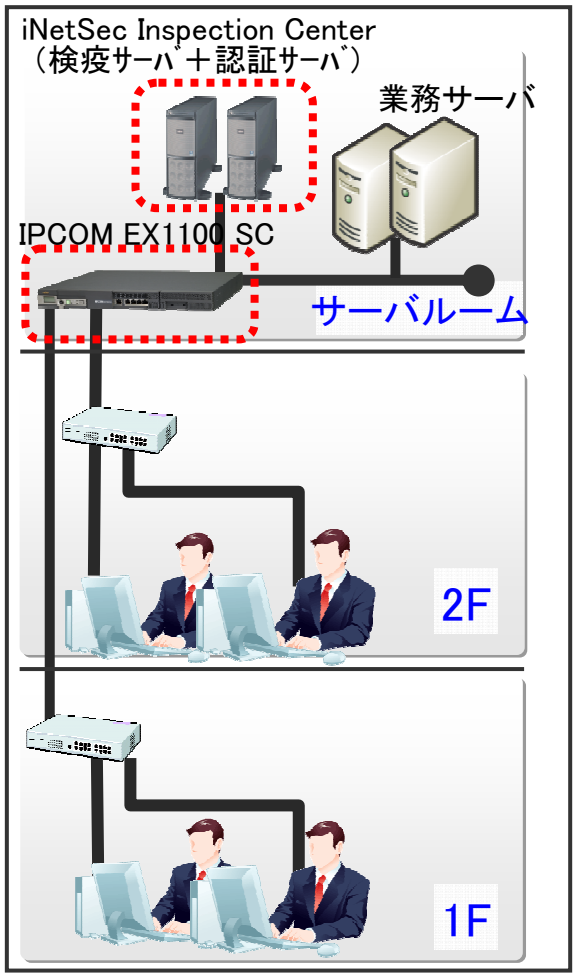
（*）iNetSec Inspection Center V7.0L10とV7.0L20の富士通型名は同じ。2013年2月1日出荷品よりV7.0L20。

構成・価格例(認証ゲートウェイ方式)

FUJITSU

パソコン500台を認証ゲートウェイ方式で認証・検疫を行う場合

参考価格:6,675,400円(税抜)



管理パソコン台数 合計500台

- 検疫(セキュリティ検査)に加えて、ユーザ認証(ユーザID/パスワード)を実施
- iNetSec Inspection Centerは冗長構成

機能名	機器名	標準単価	数量	標準合計
認証ゲートウェイ	IPCOM EX1100 SC (認証・検疫GWオプション)	¥1,298,000	1台	¥1,298,000
検疫サーバ＋認証サーバ	PRIMERGY RX1330 M1	¥338,700	2台	¥677,400
	iNetSec Inspection Center V7.0 サーバパッケージ	¥300,000	2	¥600,000
	iNetSec Inspection Center V7.0 クライアントライセンス 100	¥500,000	5	¥2,500,000
	iNetSec Inspection Center V7.0 認証サーバパッケージ	¥800,000	2	¥1,600,000
合計				¥6,675,400

※1秒あたりの検疫対象端末処理台数を19台とします。
※本構成例ではIPCOM EX1100 SCを選択していますが、機種によりポート数、同時接続数、処理性能に制限があります。参考情報としてください。
※本価格例には、Windows Server用ウイルス対策ソフト、バックアップ装置/ソフト、ディスプレイ、無停電電源装置、導入費/現調費、サポート費は含まれません。参考情報としてください。
※サーバ・ハードウェアの価格は2015年8月現在の情報です。

（参考）見積もりの考え方

FUJITSU

- 認証ゲートウェイ方式で連携可能なネットワーク機器はIPCOM EXシリーズです。1台のIPCOM EXで最大10,000台（機種により最大数は異なります。ユーザ追加オプションが必要）の端末を収容できます。

- iNetSec Inspection Centerを冗長構成とする場合、サーバパッケージおよび認証サーバパッケージを複数個ご購入頂くことが必須です。

- 検疫対象端末数にあわせて、クライアントライセンスをご購入頂きます。

- 検疫（セキュリティ検査）とあわせてユーザ認証実施時は、認証サーバが必要です。iNetSec Inspection Centerでは、認証サーバパッケージをご購入頂くことで認証サーバ（RADIUSサーバ）を検疫サーバと同じサーバ上で構築できます。ユーザ認証未実施（セキュリティ検査のみ実施）の場合は、認証サーバは必要ありません。

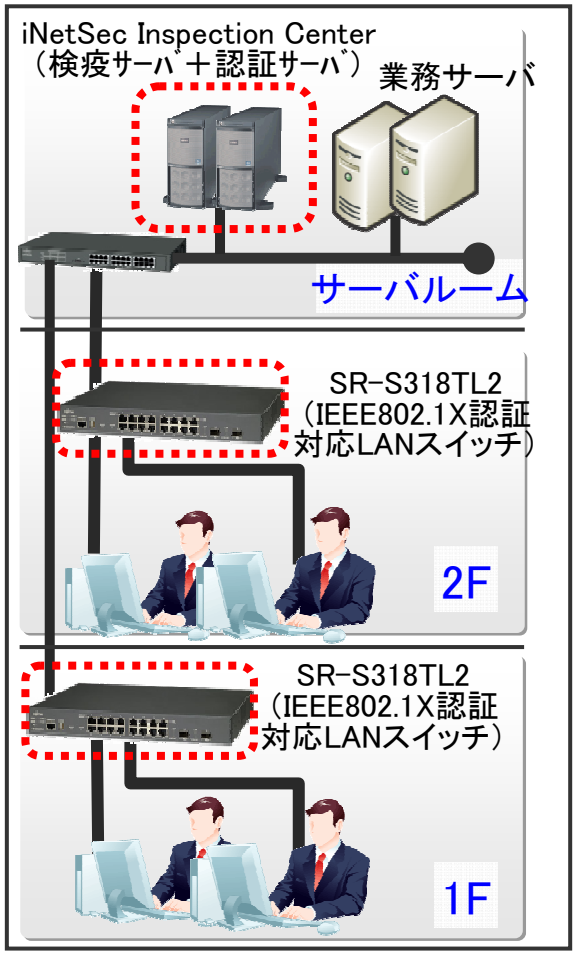
- お客様既存の任意の認証サーバ（RADIUSサーバ、もしくはLDAPサーバ）を利用することも可能です（本システムとの連携可否を事前に確認させて頂くことが必須です）。なお、LDAPサーバ連携時には、認証サーバパッケージが必須です。

構成・価格例（IEEE802.1X認証方式）

FUJITSU

パソコン500台をIEEE802.1X認証方式で認証・検疫を行う場合

参考価格:8,875,400円（税抜）



管理パソコン台数 合計500台

- 検疫対象PCはIEEE802.1X認証対応LANスイッチに対して1ポート1PC接続
- iNetSec Inspection Centerは冗長構成

機能名	機器名	標準単価	数量	標準合計
IEEE802.1X認証対応LANスイッチ	SR-S318TL2（10/100/1000BASE-T×18、うち1000BASE-T/SFP×2）	¥116,600	30台（1ポート1PC接続）	¥3,498,000
検疫サーバ＋認証サーバ	PRIMERGY RX1330 M1	¥338,700	2台	¥677,400
	iNetSec Inspection Center V7.0 サーバパッケージ	¥300,000	2	¥600,000
	iNetSec Inspection Center V7.0 クライアントライセンス 100	¥500,000	5	¥2,500,000
	iNetSec Inspection Center V7.0 認証サーバパッケージ	¥800,000	2	¥1,600,000
合計				¥8,875,400

※検疫対象PC OSは全てWindows7とします。1秒あたりの検疫対象端末処理台数を20台とします。
※本価格例には、Windows Server用ウイルス対策ソフト、バックアップ装置/ソフト、ディスプレイ、無停電電源装置、導入費/現調費、サポート費は含まれません。参考情報としてください。
※サーバ・ハードウェアの価格は2015年8月現在の情報です。

(参考)見積もりの考え方

FUJITSU

- IEEE802.1X認証VLAN方式で連携可能なネットワーク機器は以下のとおりです。
  - LANスイッチ:SR-Sシリーズ、Catalystシリーズ
  - 無線LAN アクセスポイント:SR-M20AP2、Aironetシリーズ

  ※ 端末収容数は製品毎に異なります。別途事前にご確認願います。

- iNetSec Inspection Centerを冗長構成とする場合、サーバパッケージおよび認証サーバパッケージを複数個ご購入頂くことが必須です。

- 検疫対象パソコンの台数にあわせて、クライアントライセンスをご購入頂きます。検疫対象OSは、Windows XP/Vista/7/8/8.1です。

- サーバパッケージとあわせて認証サーバパッケージが必須です。IEEE802.1X認証VLAN方式では、ユーザ認証の実施が必須です。

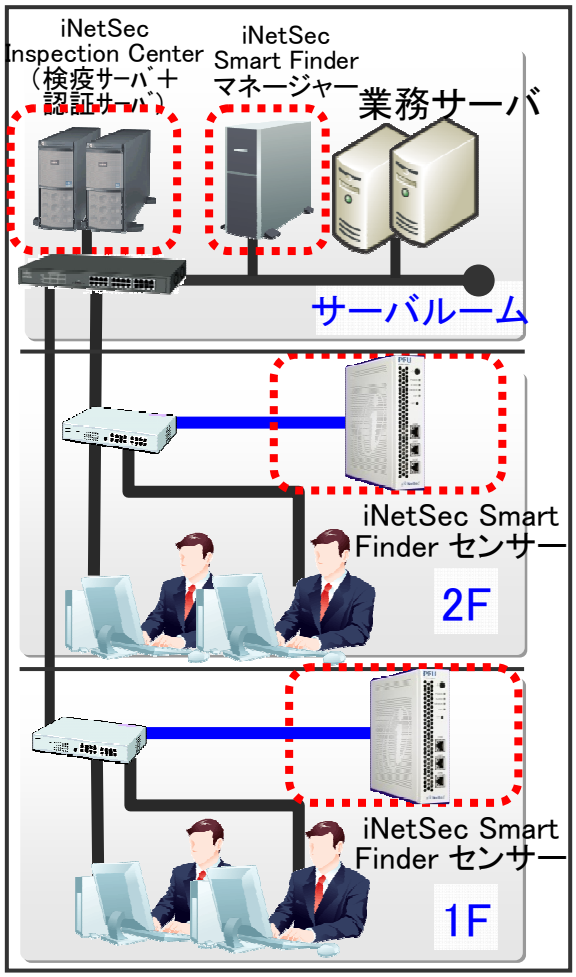
- お客様既存の任意の認証サーバ(RADIUSサーバ、もしくはLDAPサーバ)を利用することも可能です(本システムとの連携可否を事前に確認させて頂くことが必須です)。なお、RADIUSサーバ、もしくはLDAPサーバ連携時には、認証サーバパッケージが必須です。

構成・価格例(ARP遮断方式)

FUJITSU

パソコン500台をARP遮断方式で認証・検疫を行う場合

参考価格:6,343,100円(税抜)



管理パソコン台数 合計500台

- 検知センサーは1フロア(サブネット)に一台設置
- マネージャーは各フロアの検知センサーを一括管理
- iNetSec Inspection Centerは冗長構成

機能名	機器名	標準単価	数量	標準合計
検知センサー	iNetSec Smart Finder センサー	¥180,000	2台(1フロアに1台)	¥360,000
iNetSec Smart Finder 管理サーバ	PRIMERGY RX1330 M1	¥325,700	1台	¥325,700
	iNetSec Smart Finderマネージャー	¥280,000	1	¥280,000
検疫サーバ＋認証サーバ	PRIMERGY RX1330 M1	¥338,700	2台	¥677,400
	iNetSec Inspection Center V7.0 サーバパッケージ	¥300,000	2	¥600,000
	iNetSec Inspection Center V7.0 クライアントライセンス 100	¥500,000	5	¥2,500,000
	iNetSec Inspection Center V7.0 認証サーバパッケージ	¥800,000	2	¥1,600,000
合計				¥6,343,100

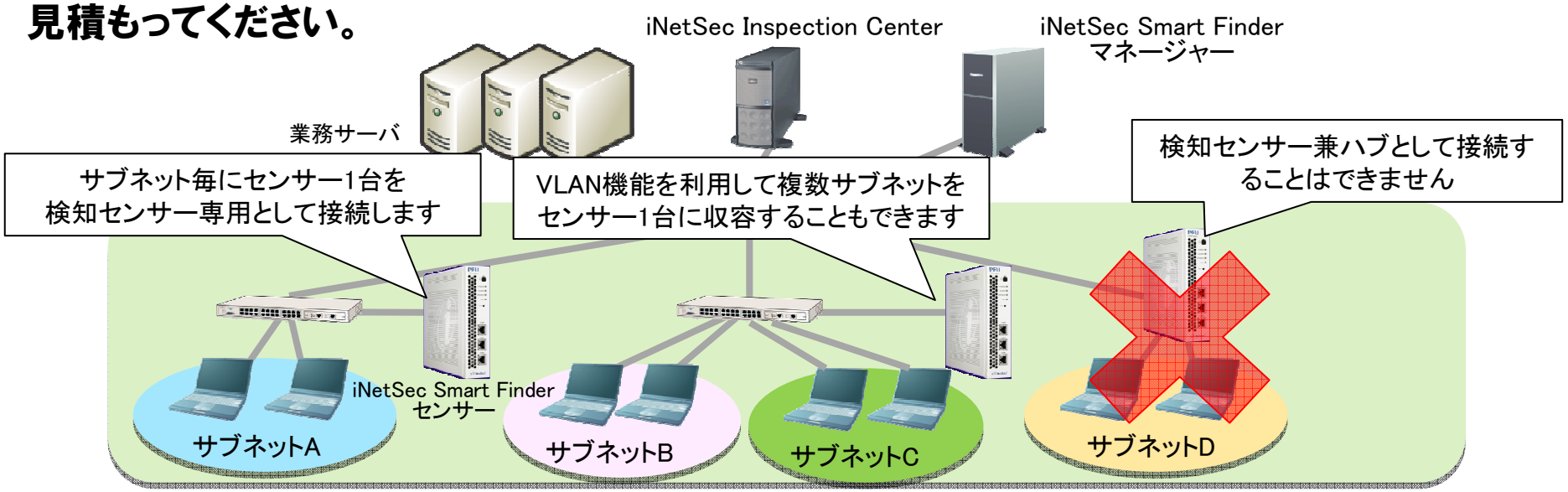
※フロア内で複数サブネットで構成されている場合や、構成によってはiNetSec Smart Finderセグメントライセンスの追加が必要な場合があります。
※iNetSec Smart Finderセンサー1台で監視できる端末数は、3,000台となります。
※本価格例には、Windows Server用ウイルス対策ソフト、バックアップ装置/ソフト、ディスプレイ、無停電電源装置、導入費/現調費、サポート費は含まれません。参考情報としてください。
※サーバ・ハードウェアの価格は2015年8月現在の情報です。

（参考）見積もりの考え方①

- ARP遮断方式で連携可能なネットワーク機器は、iNetSec Smart Finderです。
- iNetSec Inspection Centerを冗長構成とする場合、サーバパッケージおよび認証サーバパッケージを複数個ご購入頂くことが必須です。
- 検疫対象パソコンの台数にあわせて、クライアントライセンスをご購入頂きます。
- 検疫（セキュリティ検査）とあわせてユーザ認証実施時は、認証サーバが必要です。iNetSec Inspection Centerでは、認証サーバパッケージをご購入頂くことで認証サーバ（RADIUSサーバ）を検疫サーバと同じサーバ上で構築できます。ユーザ認証未実施（セキュリティ検査のみ実施）の場合は、認証サーバは必要ありません。
- お客様既存の任意の認証サーバ（RADIUSサーバ、もしくはLDAPサーバ）を利用することも可能です（本システムとの連携可否を事前に確認させて頂くことが必須です）。なお、LDAPサーバ連携時には、認証サーバパッケージが必須です。

（参考）見積もりの考え方②

- **基本的に、iNetSec Smart Finderセンサーはサブネット毎に1台接続します。検知センサーを兼スイッチングハブとして既存スイッチングハブと置き換えることはできません。**
- **VLAN機能を利用することで、1台のiNetSec Smart Finderセンサーに複数サブネット（最大16個まで）を収容することもできます。この場合、システムで管理するセグメント数分のセグメントライセンスが必要です。**
- **iNetSec Smart Finderセンサーで監視できる端末数は、3,000台です。**
  この数値は、不正端末/登録端末を合わせた総数です。L3スイッチやプリンタ等のあらかじめ許可する必要があるMACアドレスに加え、不正接続数を考慮し、余裕をみて端末台数を見積もってください。



サブネットとは、複数のLANを接続した場合の1つのセグメント(意味的な区切り単位)を指します。
通常は、ルータまたはL3スイッチで区切られた範囲となりサブネットから外にはブロードキャスト・データは伝送されない範囲をいいます。

（参考）見積もりの考え方③

FUJITSU

- iNetSec Smart Finderセンサー管理のためにiNetSec Smart Finderマネージャーも必要です。1台のiNetSec Smart Finderマネージャーでは、最大1,000セグメント/最大50,000台のMACアドレス情報を管理できます。
- iNetSec Smart Finderマネージャーを冗長構成とすることはできません。但し、センサーとマネジャー間でMACアドレス情報を共有するため（センサーとマネージャー間でMACアドレス情報の同期処理を行う間隔は1/5/10分のいずれかを選択）、マネージャーの故障やセンサーとマネージャー間の経路障害発生時にも、センサー単独で持ち込み機器の検知・遮断動作を継続することができます。
- マネージャーはサーバOS（Windows Server2003/2008/2012）上に構築することを推奨します。マネージャーをWindows XP/7などのクライアントOS上で動作させることも可能ですが、マネージャーはセンサーや機器情報の一元管理など重要な役割を担うため安定稼働が要求されます。

保守サービス(Support Desk)

■iNetSec Inspection Center ソフトウェアサポート

製品名	サービス型名	標準価格(税別)(月額)	備考
検疫サーバサポートサービス	SV719101A	¥4,400	
検疫辞書(日本語)エントリパック	SV719102A	¥70,000	
検疫辞書(日本語)スタンダードパック	SV719103A	¥100,000	
検疫辞書(英語)エントリパック	SV719104A	¥70,000	
検疫辞書(英語)スタンダードパック	SV719105A	¥100,000	
認証サーバサポートサービス	SV719106A	¥12,000	

■iNetSec Inspection Center ライセンスサポート

製品名	サービス型名	標準価格(税別)(月額)	備考
サポートサービス 10	SV719107A	¥1,200	
サポートサービス 100	SV719108A	¥7,440	
サポートサービス 1000	SV719109A	¥60,000	
サポートサービス 5000	SV719110A	¥262,440	
サポートサービス 10000	SV719111A	¥450,000	

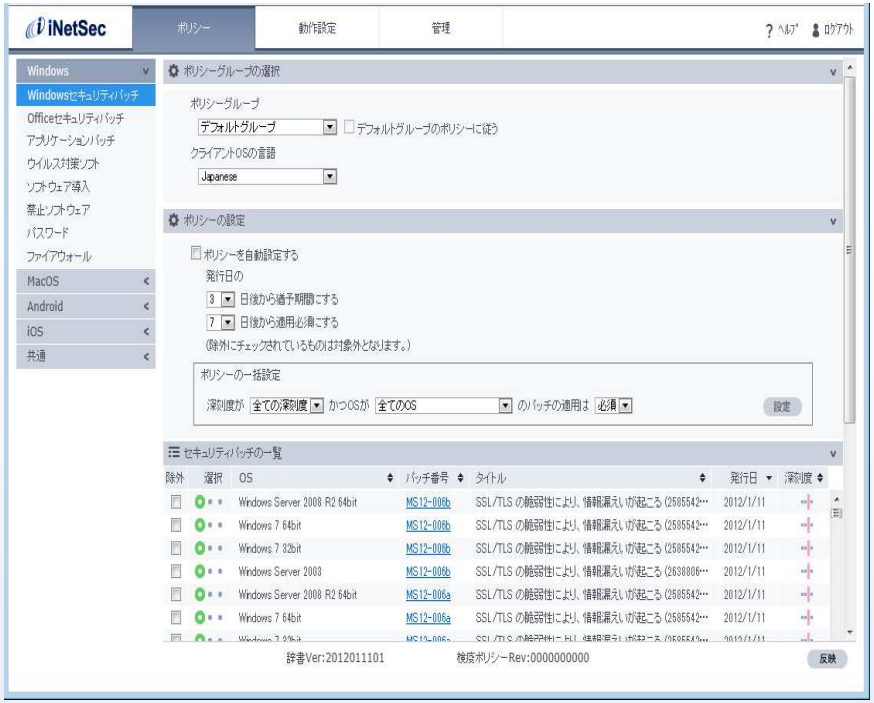
- iNetSecシリーズ製品は、セキュリティ機能の継続実現のためにサービス契約が必須の製品です。
- 製品には各々1対1の対応サポートサービスが必要です(例えば、サーバ冗長構成時には、購入したサーバパッケージ本数だけサポートサービスの契約も必要)。
- 検疫を行なう場合、検疫対象端末種類に応じた辞書サービスが必要です(システム単位)。
  - 検疫対象端末が日本語/英語双方有る場合は2種類のサービス契約が必要です。
  - 検疫辞書配布サービスのエントリパックとスタンダードパックの差異は以下の通りです。
    - エントリパック:Windows/IE のパッチとウイルス対策ソフトに関する辞書配布
    - スタンダードパック:エントリパックの内容に加えて、Microsoft Office パッチ/アプリケーションパッチの辞書配布

※Adobe Reader, Adobe Flash Player, Javaに関する検疫を実施する際には、アプリケーションパッチ辞書配布の可能なスタンダードパックが必須です。

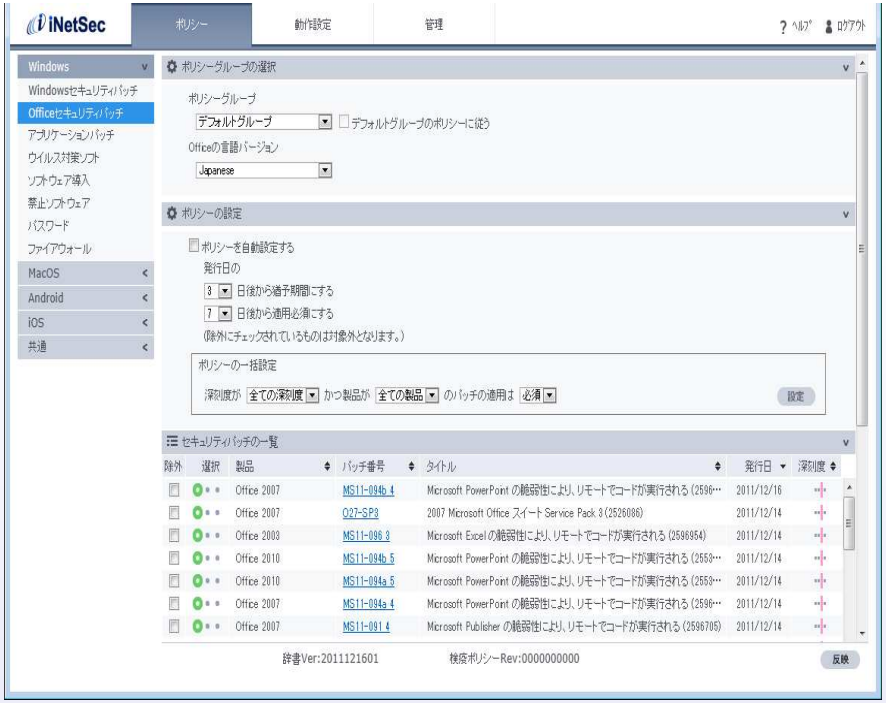
参考）管理画面

検査項目①

セキュリティパッチ



<Windowsパッチ>



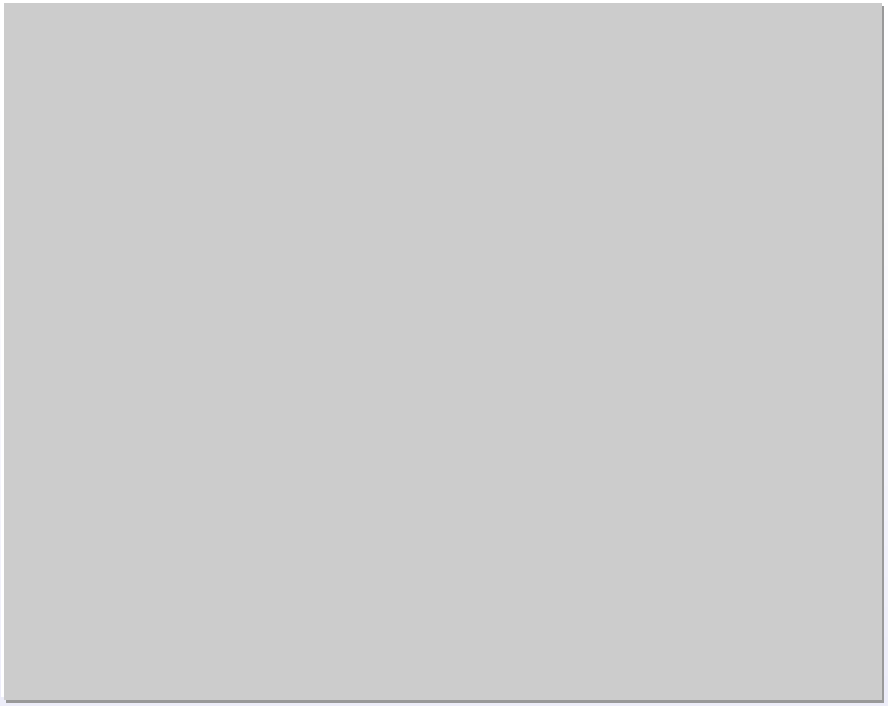
<Officeパッチ>

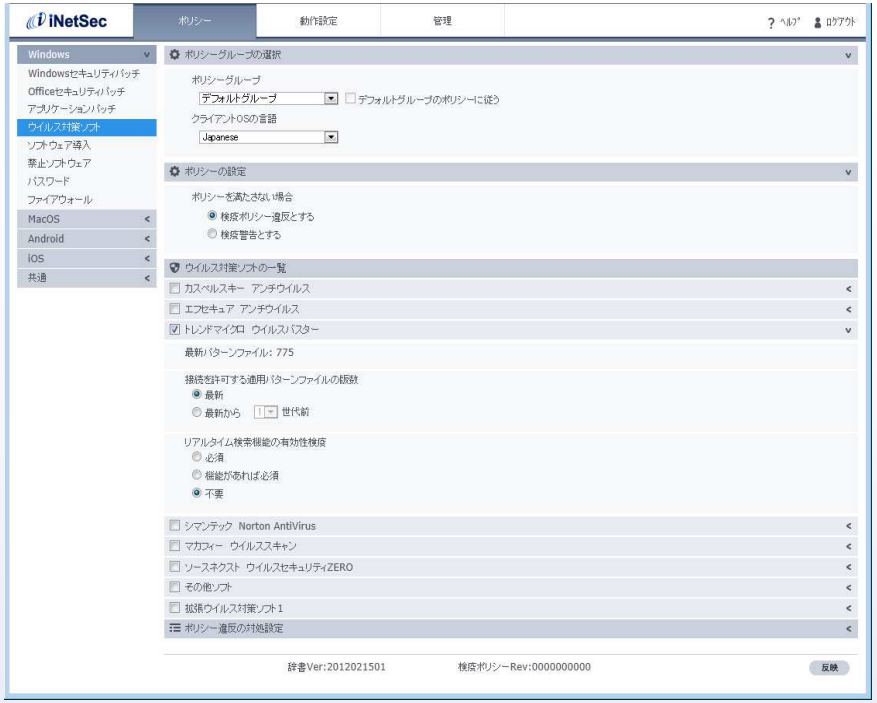
セキュリティパッチ検疫ポリシーの設定

セキュリティパッチの深刻度／対象OSに応じた運用ポリシーをあらかじめ設定しておけば、検疫対象のセキュリティパッチが自動的に選択されます。
警告モードにも対応。

検査項目②

アプリケーションパッチ、ウィルス対策ソフト検疫





アプリケーションパッチ検疫ポリシーの設定

アプリケーションパッチに基づいて、Adobe Reader/Adobe Flash Player/JAVAの検査を行います。

ウイルス対策ソフト検疫ポリシーの設定

TRENDMICRO、Symantec、McAfee、F-Secure、SOURCENEXT、Kasperskyの他に任意のウイルス対策ソフトに対応。リアルタイムスキャンの設定も検査できます。

※任意のウイルス対策ソフトはWindowsセキュリティセンターやWindows Action Centerとの連携により簡易的な検疫を行います。

※ Kasperskyのサポートは iNetSec Inspection Center V7.0以降です。

検査項目③

ソフトウェア導入、禁止ソフトウェア検査

ソフトウェア導入検疫ポリシーの設定

任意のソフトウェアの導入を検査できます。
警告モードにも対応。

禁止ソフト検疫ポリシーの設定

ローカルディスク、USBメモリ等の中から、指定されたファイル名を検査します。

検査項目④

パスワード設定、パーソナルファイアウォール設定検査

パスワード検疫ポリシーの設定

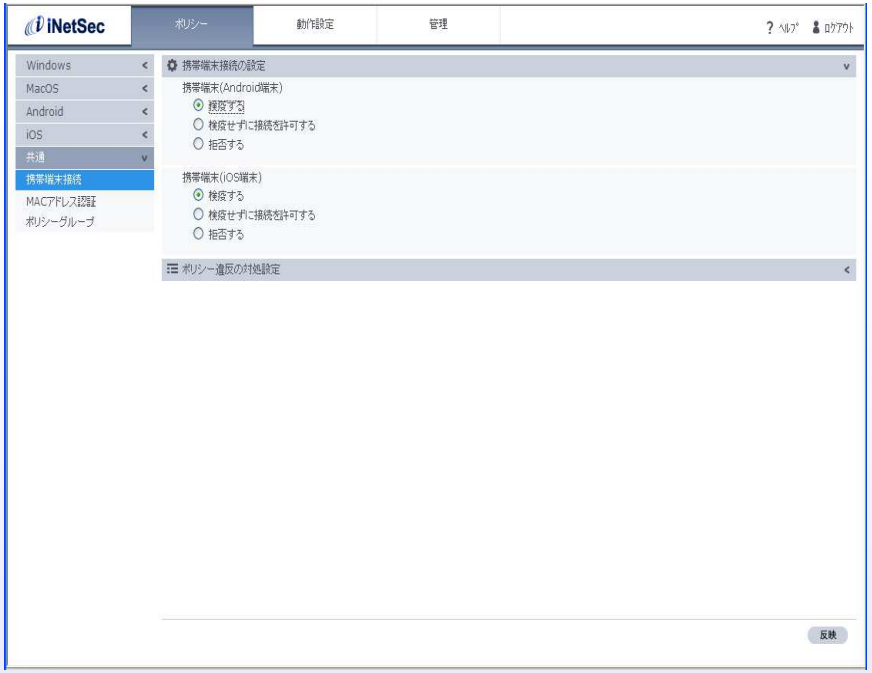
スクリーンセーバのパスワードの設定、Windowsログインパスワードの設定を検査します。

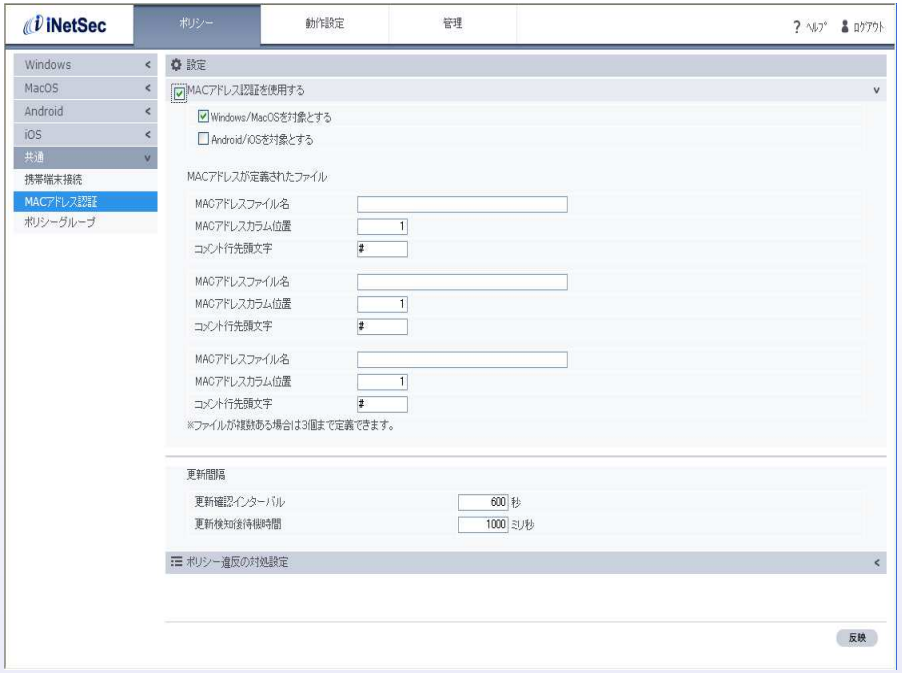
パーソナルファイアウォール導入検疫ポリシーの設定

Windowsファイアウォール、ウイルス対策ソフトのパーソナルファイアウォールが有効になっているかどうかを検査します。

検査項目⑤

携帯端末接続ポリシー、MACアドレス認証





携帯端末接続ポリシーの設定

Android端末とiOS端末に対して以下のいずれかを選択します。
- 検疫する
- (ネットワークへの接続を)検疫せずに接続を許可する
- (ネットワークへの接続を)拒否する

MACアドレス認証ポリシーの設定

MACアドレス認証を有効にし、登録済コンピュータの接続かどうかを検査します。

検査項目⑥

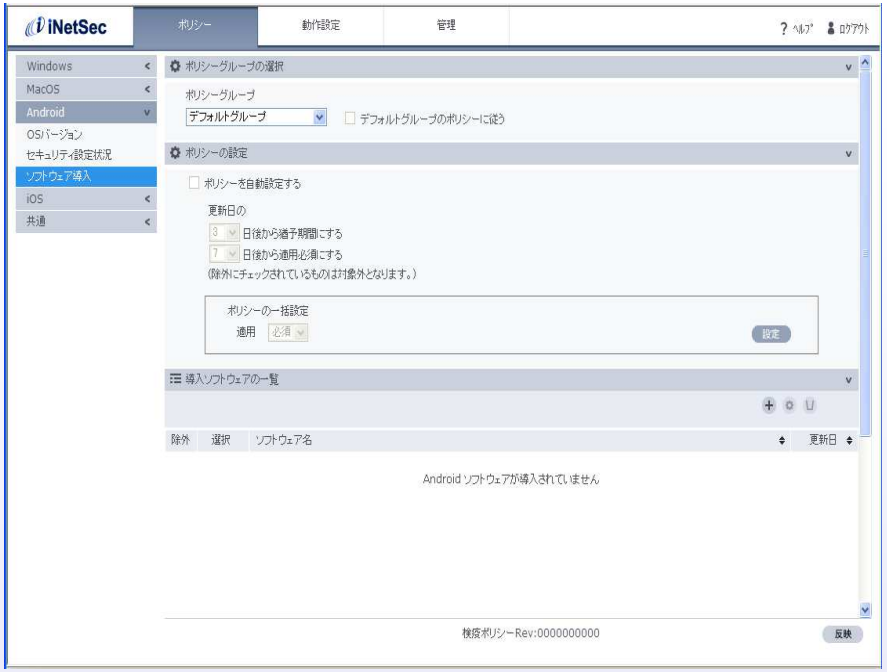
Android OSバージョン検査

Android OSバージョンの設定

Android 端末のOS バージョンやビルド番号を検疫することで、規定の端末のみを検疫成功とし、セキュリティレベルの低い端末(適切なアップデートがされていない端末)をネットワークから隔離できます。

検査項目⑦

Android セキュリティ設定状況検査、ソフトウェア導入検査



Android セキュリティ設定

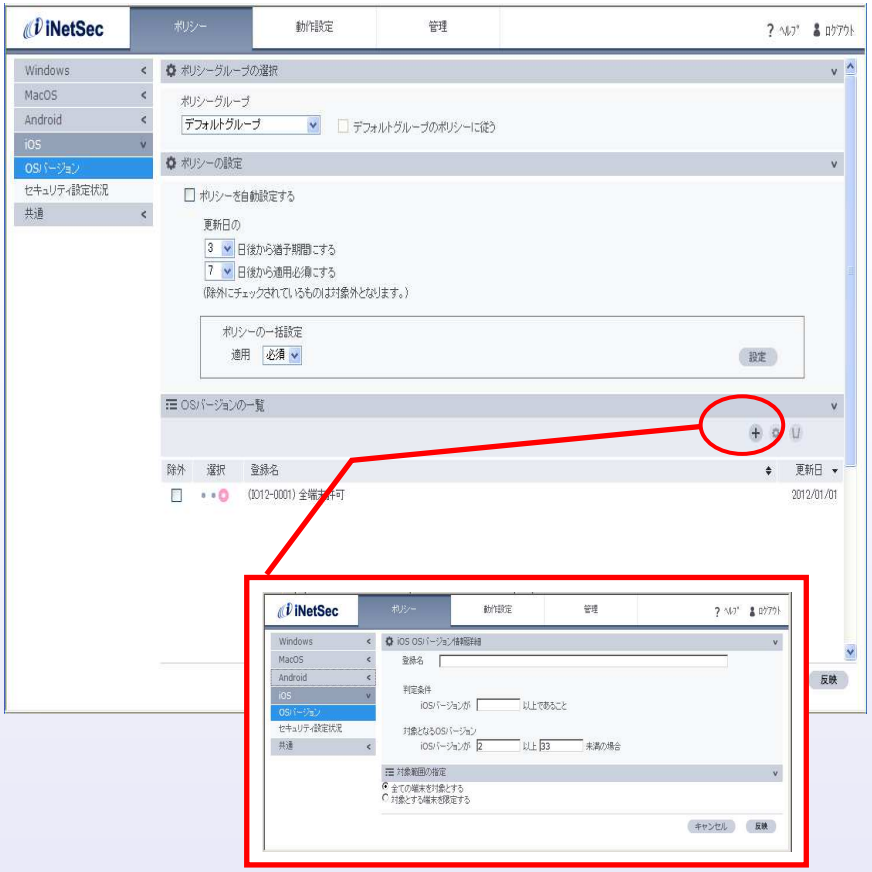
スクリーンロックが設定されているか、root化されていないかを検査できます。

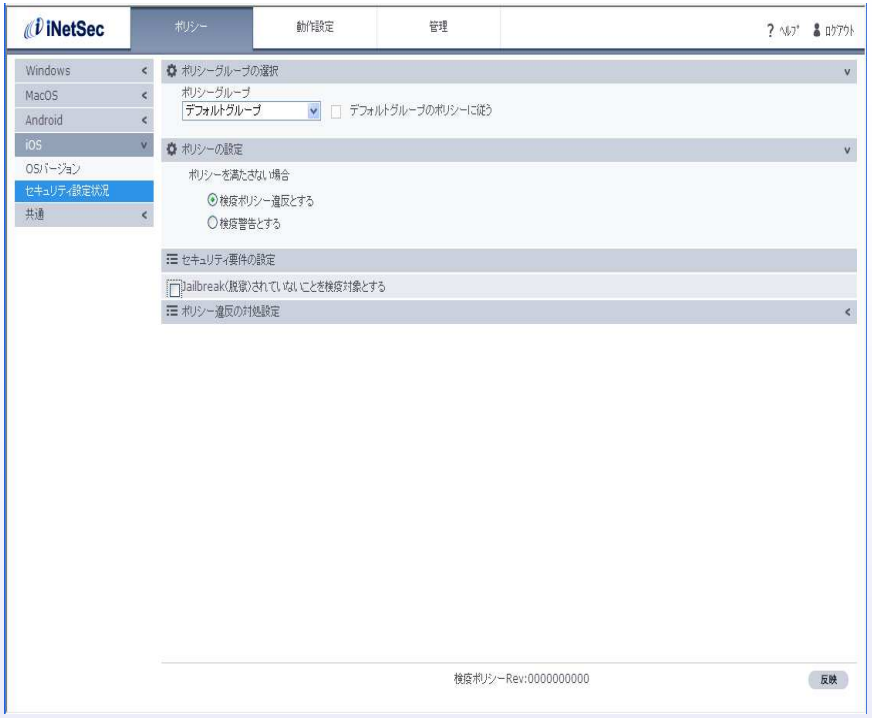
Android ソフトウェア導入検疫ポリシーの設定

任意のソフトウェアの導入を検査できます。
警告モードにも対応。

検査項目⑧

iOS OSバージョン検査、セキュリティ設定状況検査



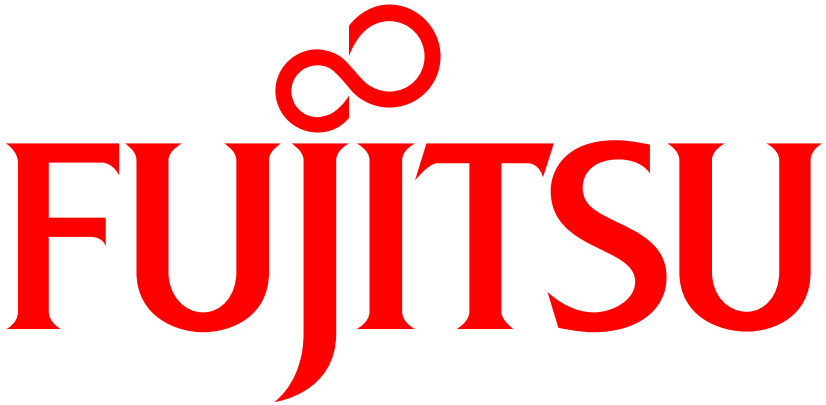


iOS OSバージョンの設定

iOS 端末のOS バージョンやビルド番号を検疫することで、規定の端末のみを検疫成功とし、セキュリティレベルの低い端末(適切なアップデートがされていない端末)をネットワークから隔離できます。

Android セキュリティ設定

Jailbreakされていないかを検査できます。



shaping tomorrow with you