

もっと知りたい！JP1活用ノウハウ 「ITコンプライアンス編」

テクニカルトラック【JC-3】

2008/11/17

株式会社 日立製作所 ソフトウェア事業部
JP1販売推進センタ

佐藤 靖広

Contents

1. はじめに
2. PCの省電力設定・セキュリティ対策を徹底したい
3. JP1/NETM/DM Clientを漏れなく導入したい
4. JP1/NETM/DM Clientのアンインストールを防ぎたい

1

はじめに

JP1のITコンプライアンスは、資産情報を一元管理することで、企業情報システムを構成するコンピュータシステムの健全かつ有効な環境を提供します。
さらに、脆弱なクライアントPCの強制排除や情報漏えい対策など、さまざまなセキュリティリスクへの予防対策を講じることができます。

ITコンプライアンスを支える管理製品

- 資産・配布管理
- セキュリティ管理



1-1. ITコンプライアンス – 大切なIT資産を「守る」

ITコンプライアンスを支える管理製品

今回のご紹介の箇所

セキュリティの徹底

JP1/NETM/CSC

資産・配布管理

JP1/NETM/DM

不正接続の排除

JP1/NETM/NM

情報漏えい防止

JP1/秘文

統合資産管理

JP1/NETM/AIM

監査証跡

JP1/NETM/Audit

今回のご紹介の箇所

JP1/NETM/CSC : JP1/NETM/Client Security Control
JP1/NETM/NM : JP1/NETM/Network Monitor
JP1/NETM/AIM : JP1/NETM/Asset Information Manager

2

PCの省電力設定・セキュリティ対策 を徹底したい

2. PCの省電力設定・セキュリティ対策を徹底したい

クライアントPCの省電力設定やセキュリティ対策状況を把握し
対策を徹底させたいが、良い手段はありますか？



省電力設定関連やセキュリティ関連の
インベントリ情報を収集し、チェックしましょう！

【対象製品】 JP1/NETM/DM
JP1/NETM/CSC

2-1. インベントリ情報を取得

その1 省電力設定関連やセキュリティ関連のインベントリ情報を取得

省電力設定関連のインベントリ情報

機器詳細: 7AC222900 - Microsoft Internet Explorer	
機器	ネットワーク
ソフトウェア	バッチ情報
ウィルス対策	インベントリ
変更履歴	
プリンタ用紙サイズ	
プリンタドライバ	
プリンタポート	
プリンタ種別	
モニタの電源を切る (AC)	20分
モニタの電源を切る (DC)	15分
プロセッサ調整 (AC)	NONE
プロセッサ調整 (DC)	NONE
ハードディスクの電源を切る (AC)	なし
ハードディスクの電源を切る (DC)	30分
システムスタンバイ/スリープ (AC)	なし
システムスタンバイ/スリープ (DC)	なし
システム休止状態 (AC)	なし
システム休止状態 (DC)	なし
JP1/NETM/DMノート作成日時	2008/10/07 16:02:21
JP1/NETM/DMノート更新日時	2008/10/10 17:56:01
JP1/NETM/DMシステム情報最終更新日時	2008/10/10 18:32:04
JP1/NETM/DMユーザインベントリ項目 (メールアドレス)	hitachi.tarou@hitachi.com
JP1/NETM/DMユーザインベントリ項目 (確認(1)-アクセス権)	許可なく、他の人に貸与または譲渡しません。
JP1/NETM/DMユーザインベントリ項目 (確認(10)-離席時)	離席時は、パスワードロックをかけます。
閉じる	

セキュリティ関連のインベントリ情報

機器詳細: 7AC222900 - Microsoft Internet Explorer	
機器	ネットワーク
ソフトウェア	バッチ情報
ウィルス対策	インベントリ
変更履歴	
Guestアカウント	
Guestアカウント無効	
脆弱なパスワード	
なし	
アカウント	
Administrator	
アカウント [2]	
ASPNET	
アカウント [3]	
IUSR_JP1DEM011	
アカウント [4]	
IWAM_JP1DEM011	
パスワードを更新してからの経過日数	
4 日	
パスワードを更新してからの経過日数 [2]	
4 日	
パスワードを更新してからの経過日数 [3]	
4 日	
パスワードを更新してからの経過日数 [4]	
4 日	
無期限のパスワード	
Administrator;ASPNET;IUSR_JP1DEM011;IWAM_JP1DEM011	
自動ログオンの設定	
なし	
共有フォルダ	
あり	
匿名接続の制限	
無効(匿名接続が制限されていない)	
スクリーンセーバー	
有効	
スクリーンセーバー パスワードの保護機能	
有効	
パワーオンパスワード	
不明	
Windowsファイアウォールの設定	
Windows自動更新	
有効	
不要なサービス	
不要サービスあり	
物理メモリの空き容量	
999 MB	
閉じる	

2-1. インベントリ情報を取得

その1 省電力設定関連やセキュリティ関連のインベントリ情報を取得

セキュリティパッチのインベントリ情報

機器詳細: 7AC222900 - Microsoft Internet Explorer

ウィルス対策 インベントリ 変更履歴

機器 ネットワーク ソフトウェア パッチ情報

適用 表示

インストール日	パッチ名	バージョン	適用状態
☐ 2008/10/07	832671	0000	適用
☐ 2008/10/07	887619	0000	適用
☐ 2008/10/07	887620	0000	適用
☐ 2008/10/07	887622	0000	適用
☐ 2008/10/07	890830	0000	適用
☐ 2008/10/07	898714	0000	適用
☐ 2008/10/07	923618	0000	適用
☐ 2008/10/07	MS04-027(873379)	0000	適用
☐ 2008/10/07	MS06-006(911564)	0000	適用
☐ 2008/10/07	MS06-012(905649)	0000	適用
☐ 2008/10/07	MS06-012(905758)	0000	適用
☐ 2008/10/07	MS06-017(911701)	0000	適用
☐ 2008/10/07	MS06-061(925673)	0000	適用
☐ 2008/10/07	MS07-013(920816)	0000	適用
☐ 2008/10/07	MS08-013(944429)	0000	適用
☐ 2008/10/07	MS08-015(946985)	0000	適用

追加 削除 閉じる

ウイルス対策製品のインベントリ情報

機器詳細: 7AC222900 - Microsoft Internet Explorer

機器 ネットワーク ソフトウェア パッチ情報

ウィルス対策 インベントリ 変更履歴

AntiVirus Corporate Edition 10.1.10.1.6.6000 表示

ウィルス対策ソフトウェア名	AntiVirus Corporate Edition 10.1
ウィルス対策ソフトウェアバージョン	10.1.6.6000
エンジンバージョン	81.2.0.25
常駐/非常駐	常駐
インストール日付	2008/10/07
ウィルス定義バージョン	20081006.006
インベントリ取り込み制御	インベントリ情報に対応する情報がないとき削除する

追加 削除 閉じる

2-1. インベントリ情報を取得

■ 参照手順

① 保有機器一覧を
選択し検索

資産番号	機器種別	名称	ユーザ名	登録日	機器状態
7AC222900	PC	HP Compaq 2510p Notebook PC		2008/10/07	運用
7H572400	PC	FLORA 210W RF1		2008/10/07	運用
7H572500	PC	FLORA 210W RF1		2008/10/07	運用
7H572600	PC	FLORA 210W RF1		2008/10/07	運用

③ タブを選択

機器詳細: 7AC222900 - Microsoft Internet Explorer

ウィルス対策 | インベントリ | 変更履歴

機器 | ネットワーク | ソフトウェア | バッチ情報

資産番号: 7AC222900

部署: 設計部 [参照]

ユーザ名: [参照]

設置場所: 東京 [参照]

機器種別: PC

稼働管理種別: 稼働管理対象

名称: HP Compaq 2510p Notebook PC

型式:

製造者: Hewlett-Packard

製造番号: CNF82441TM

機器状態: 運用

購入金額: 円

登録日: 2008/10/07 (YYYYMMDD)

使用期間: ~ (YYYYMMDD)

搬卸日付: (YYYYMMDD)

用途:

備考:

[更新] [閉じる]

② 検索結果から参照したい
機器をクリック

表示

2-2. 判定ポリシーを設定

その2 判定ポリシーを設定します

■セキュリティ対策状況の判定ポリシー設定

判定ポリシー編集(営業部)

判定項目

- 更新プログラム
- ウイルス対策製品
- 不正ソフトウェア
- 必須ソフトウェア
- PCセキュリティ設定
- ユーザ定義

更新プログラムの判定

PCの更新プログラムの適用状況について判定条件と危険レベルを指定します。

☒ 判定対象とする(Q)

判定条件と危険レベルの設定

判定条件(Q)
最新の更新プログラム

危険レベル(Q)
警告

PCに最新の更新プログラムが適用されているかをチェックします。
特定の更新プログラムを除外する場合、定義ボタンを押して更新プログラムを指定してください。

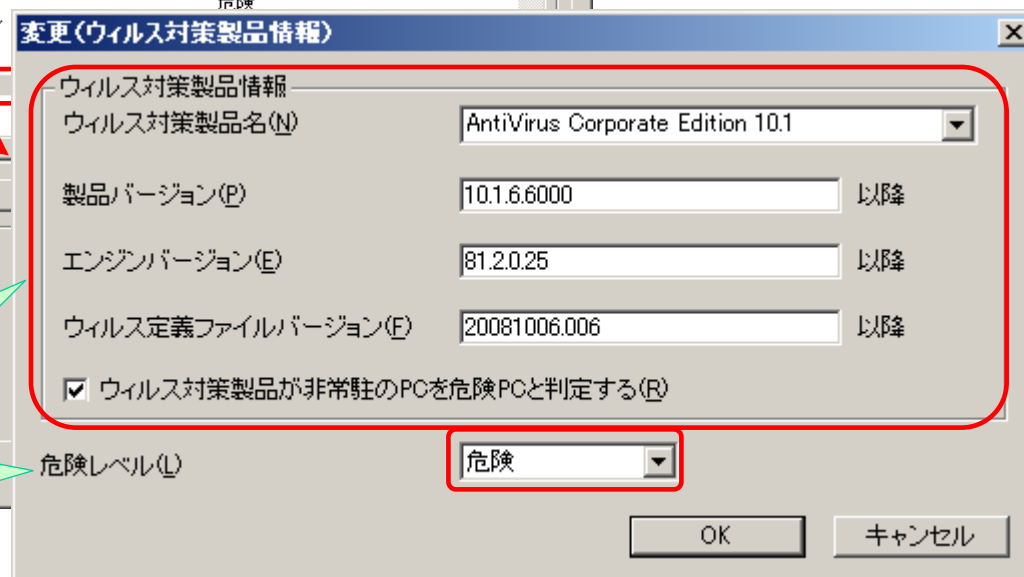
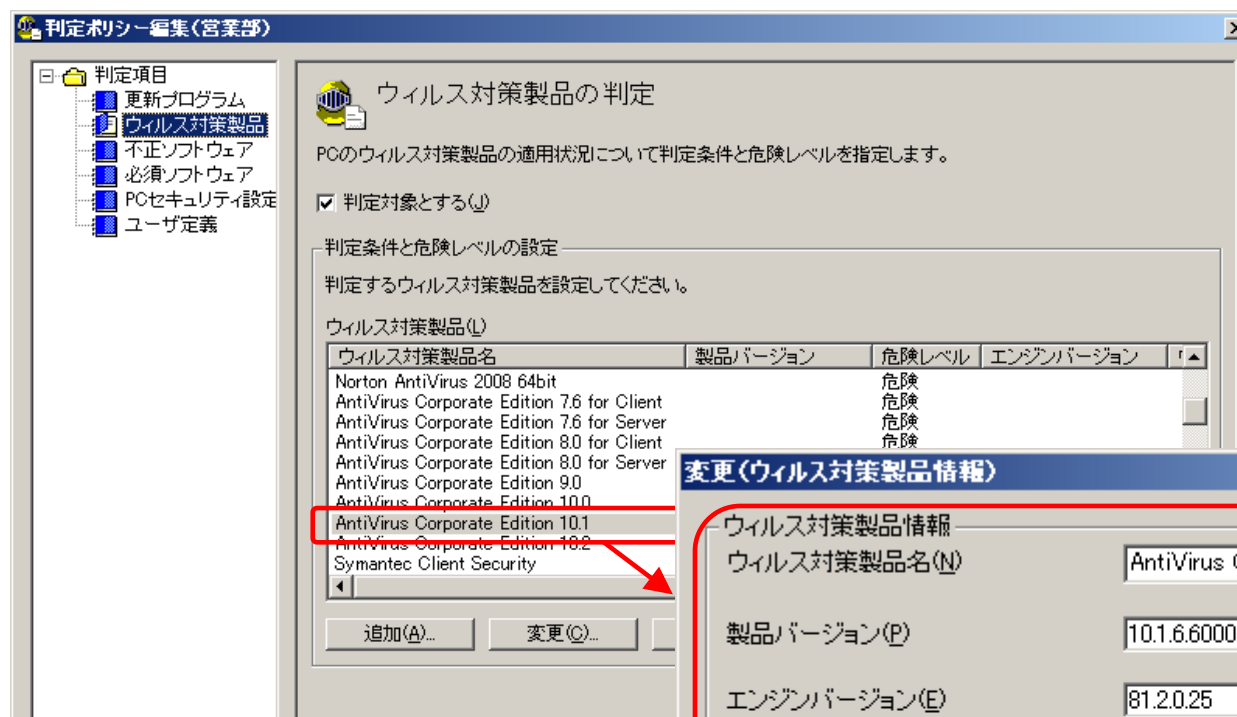
☐ 特定の更新プログラムを除外する(Q) 定義(D)...

保存 閉じる

Windowsセキュリティパッチが最新の状況でなければ、危険レベルを「警告」と判定する。

2-2. 判定ポリシーを設定

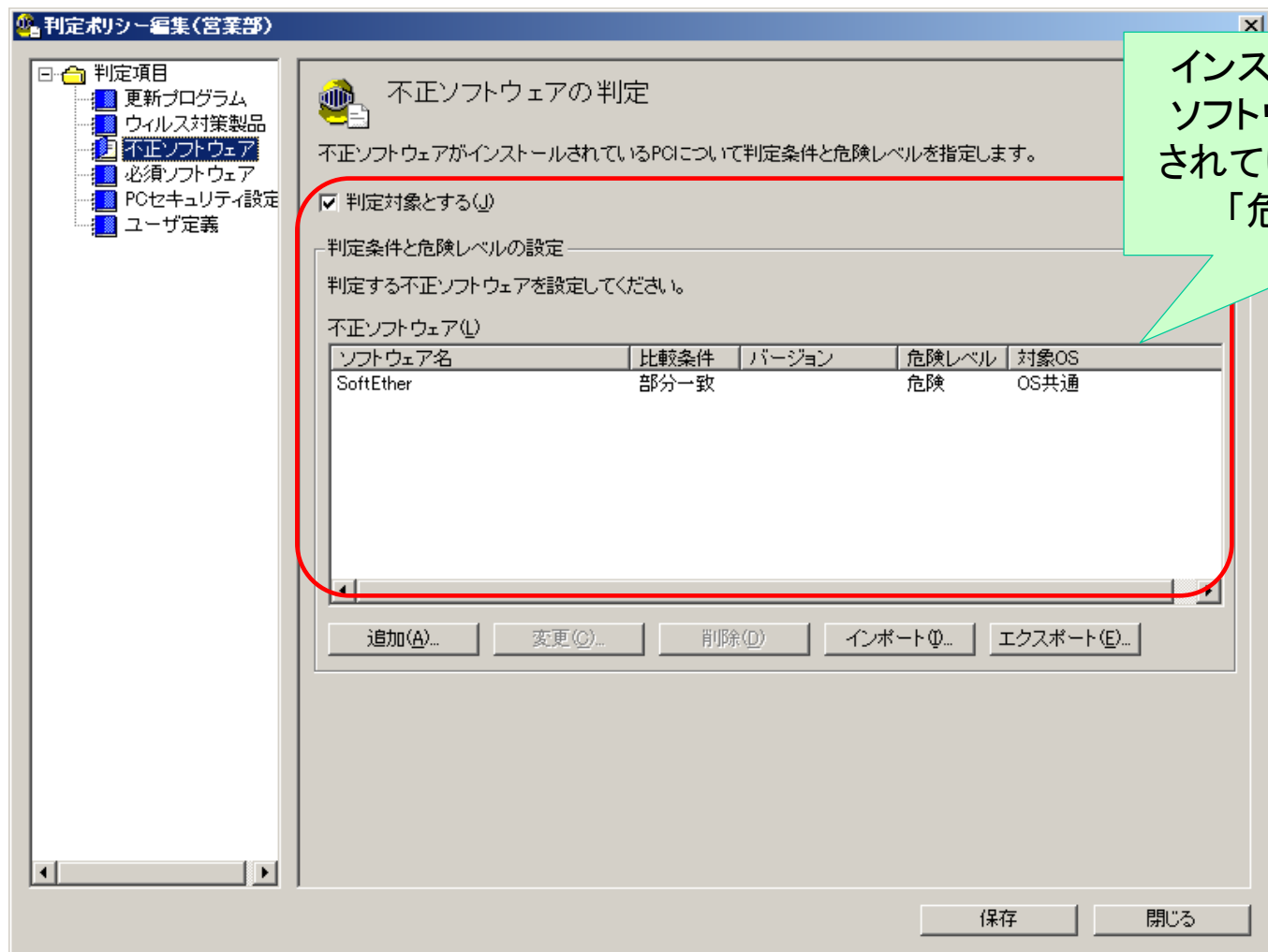
■セキュリティ対策状況の判定ポリシー設定



ウィルス対策製品が
最新バージョンでない、
または非常駐であったら、
危険レベルを「危険」と判定する。

2-2. 判定ポリシーを設定

■セキュリティ対策状況の判定ポリシー設定



2-2. 判定ポリシーを設定

■セキュリティ対策状況の判定ポリシー設定

判定ポリシー編集(営業部)

判定項目

- 更新プログラム
- ウイルス対策製品
- 不正ソフトウェア
- 必須ソフトウェア
- PCセキュリティ設定
- ユーザ定義

必須ソフトウェアの判定

必須ソフトウェアがインストールされていないPCについて判定条件と危険レベルを指定します。

☒ 判定対象とする(U)

判定条件と危険レベルの設定

判定する必須ソフトウェアを設定してください。

必須ソフトウェア(L)

グループ名	ソフトウェア名	バージョン	危険レベル	注
JP1/秘文	"HIBUN-AE"	" "	注意	O

追加(A)... 変更(C)... 削除(D) インポート(I)... エクスポート(E)...

JP1/NETM/DM の判定

☒ Clientの判定を実施する(U) バージョン(V) [] 以降 危険レベル(R) [注意]

☐ 中継マネージャの判定を実施する(U) バージョン(Q) [] 以降 危険レベル(N) [注意]

☐ SubManagerの判定を実施する(G) バージョン(S) [] 以降 危険レベル(Q) [注意]

保存 閉じる

必須インストールして欲しい
ソフトウェアがインストール
されていなかったら、
危険レベルを「注意」と判定する。

2-2. 判定ポリシーを設定

■セキュリティ対策状況の判定ポリシー設定

判定ポリシー編集(営業部)

判定項目

- 更新プログラム
- ウイルス対策製品
- 不正ソフトウェア
- 必須ソフトウェア
- PCセキュリティ設定
- ユーザ定義

PCセキュリティ設定の判定

PCセキュリティ設定について判定条件と危険レベルを指定します。

☒ 判定対象とする(J)

判定条件と危険レベルの設定

判定する項目を設定してください。

PCセキュリティ情報(I)

グループ名	判定
アカウント	判定する
パスワード	判定する
ログオン	判定する
共有設定	判定する
匿名接続	判定
サービス	判定
ファイアウォール	判定
自動更新	判定
スクリーンセーバー	判定

定義(D)...

スクリーンセーバー定義

☒ 判定対象とする(J)

スクリーンセーバーの設定

危険PCと判定する条件

危険レベル(L)

判定項目が存在しないときの扱い(N)

☒ パスワードによる保護(P)

危険PCと判定する条件

危険レベル(R)

判定項目が存在しないときの扱い(Q)

OK

キャンセル

スクリーンセーバー設定のパスワードによる保護が設定されていない場合は、危険レベルを「注意」と判定する。

2-2. 判定ポリシーを設定

■省電力設定状況の判定ポリシー設定

判定ポリシー編集 (営業部)

判定項目

- 更新プログラム
- ウイルス対策製品
- 不正ソフトウェア
- 必須ソフトウェア
- PCセキュリティ設定
- ユーザ定義

ユーザ定義の判定

任意の条件で判定することができます。

☒ 判定対象とする (U)

判定条件と危険レベルの設定

判定する項目を設定してください。
複数の判定項目で安全でない」と判定された場合、安全でなかった判定項目のうち、最も高い危険レベルが判定結果となります。

判定項目 (U)

判定項目名	クラス	プロパティ
モニタ電源OFF設定率 (AC)...	ハードウェア資産情報	モニタの電源を切る (AC)
モニタ電源OFF設定率 (DC)...	ハードウェア資産情報	モニタの電源を切る (DC)
モニタ電源OFF設定率 (DC)...	ハードウェア資産情報	モニタの電源を切る (DC)
CPU省電力モード設定率 (A)...	ハードウェア資産情報	CPU省電力モード設定率 (A)
CPU省電力モード設定率 (D)...	ハードウェア資産情報	CPU省電力モード設定率 (D)
新型マシン (省電力対応) OP...	ハードウェア資産情報	ハードウェア資産情報
ハードディスク電源OFF設...	ハードウェア資産情報	ハードディスク電源OFF設...
ハードディスク電源OFF設...	ハードウェア資産情報	ハードディスク電源OFF設...

追加 (A)... 変更 (C)... 削除 (D) インポート

変更 (判定項目情報)

判定項目情報

判定項目名 (O) モニタ電源OFF設定率 (AC)-1

この判定項目の判定条件を設定してください。
すべての判定条件を満たした場合、危険レベルが設定されます。

判定条件 (O)

クラス	プロパティ	比較条件	比較値
ハードウェア資産情報	モニタの電源を切る (AC)	完全一致	0000000000

追加 (A)... 変更 (C)... 削除 (D)

危険レベル (L) 注意

OK キャンセル

モニタの電源を切る (AC) の設定が、「なし (0秒)」に設定されていたら、危険レベルを「注意」と判定する。

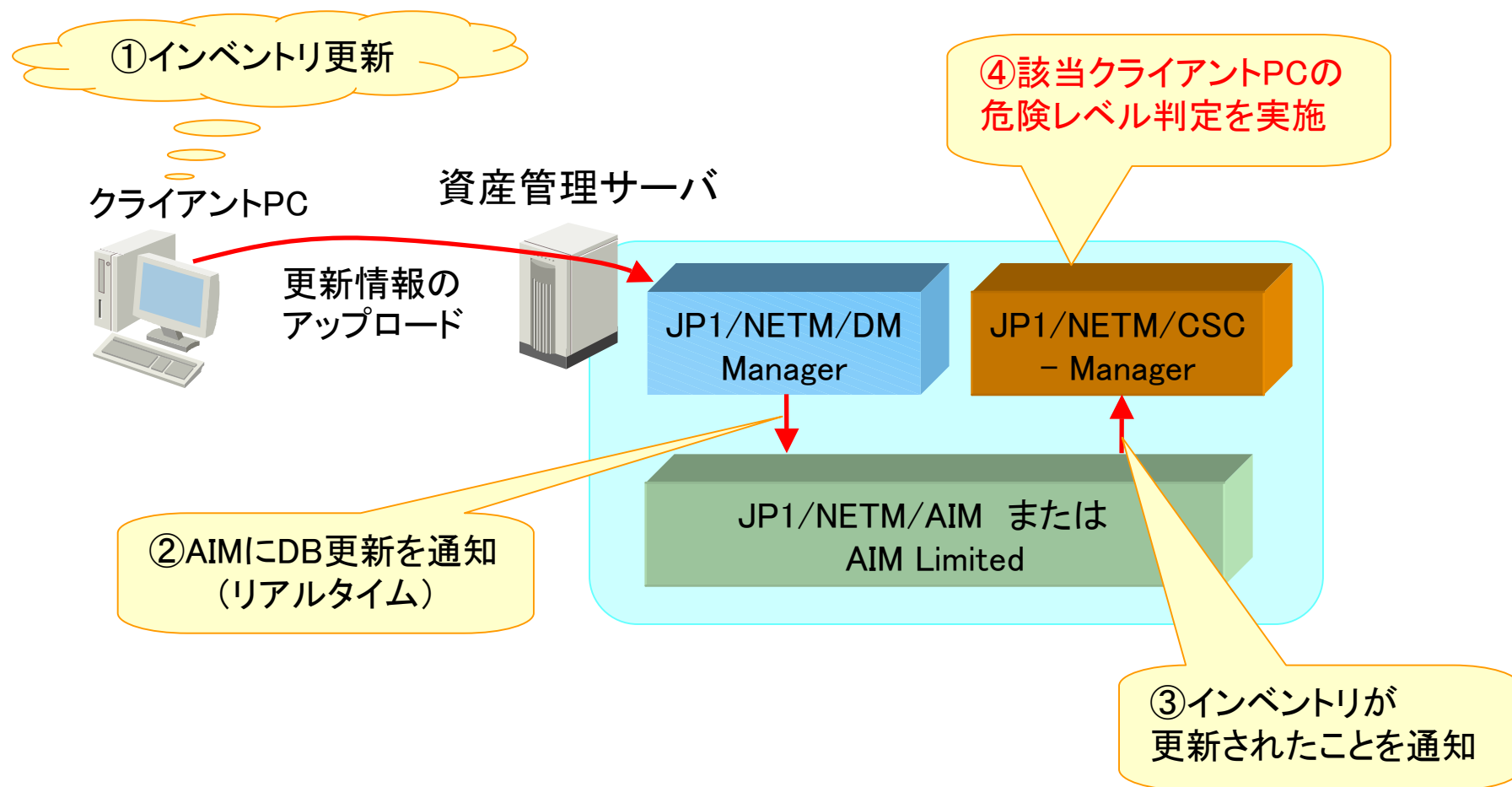
その3 判定処理を実行します。

判定の契機は、次の3パターンになります。

- クライアントPCのインベントリ情報が更新されたことを契機に『判定』を実施
- コマンドの実行(スケジュール)を契機に『判定』を実施
- 管理者指示を契機に『判定』を実施

2-3. 判定処理を実行

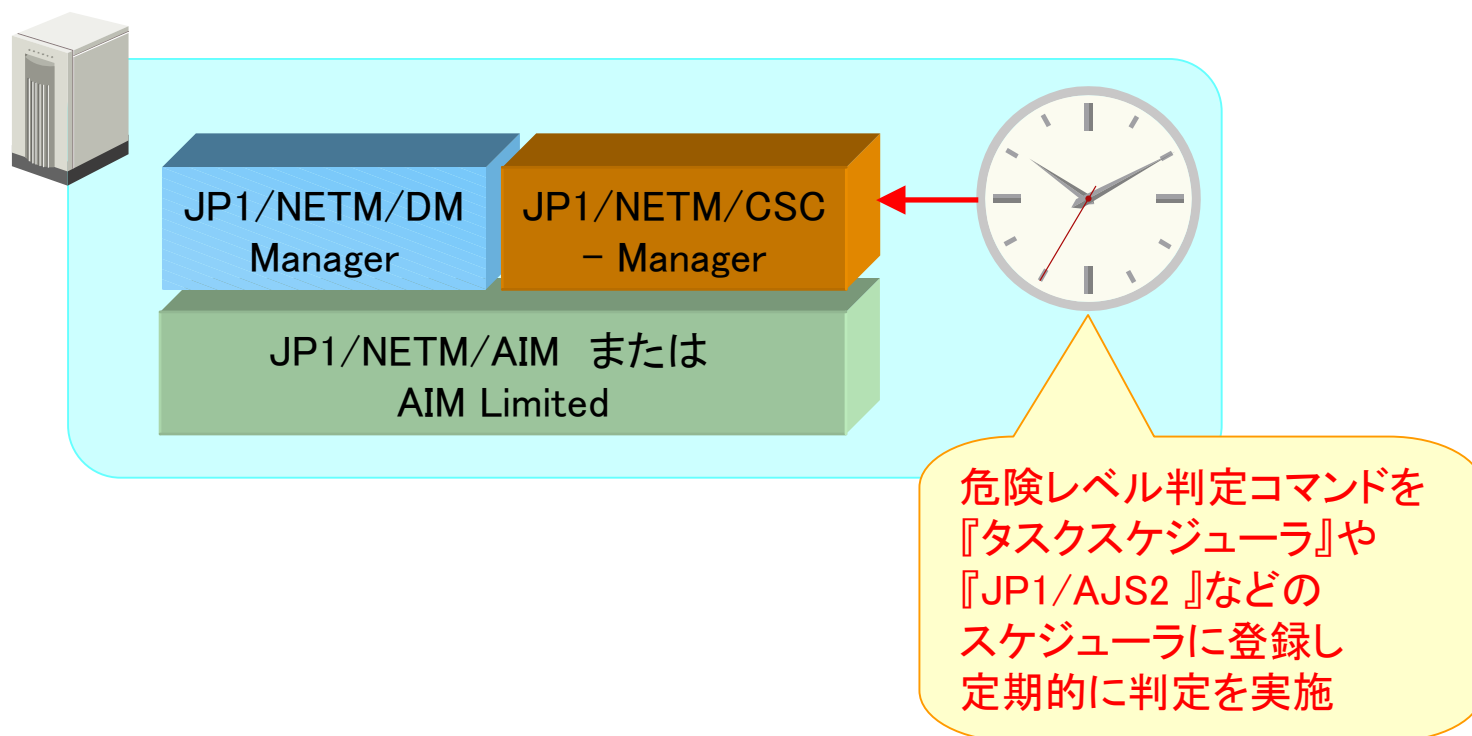
■ クライアントPCのインベントリ情報が更新されたことを契機に『判定』を実施



2-3. 判定処理を実行

■ コマンドの実行(スケジュール)を契機に『判定』を実施

資産管理サーバ



2-3. 判定処理を実行

■ 管理者指示を契機に『判定』を実施

Asset Information Manager - Microsoft Internet Explorer

ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)

アドレス(D) http://jp1demo11/jp1asset/jamwscript.dll

Asset Information Manager dm_admin ログアウト

部署
営業部
設計部
総務部

設置場所

管理業務
機器管理
ライセンス管理
ソフトウェア適用管理
ソフトウェア利用管理
セキュリティ管理
システム管理
システム定義
クライアントセキュリティ
PC危険レベル管理
許可PC登録
セキュリティ対策評価
統計データ

評価点 [] 点 以下

判定ポリシー名 [] 部分一致

判定ポリシー更新日時 [] ~ [] (YYYYMMDD)

判定ポリシー割当日時 [] ~ [] (YYYYMMDD)

アクションポリシー名 [] 部分一致

アクションポリシー更新日時 [] ~ [] (YYYYMMDD)

アクションポリシー割当日時 [] ~ [] (YYYYMMDD)

4件中 1~4件目

資産番号	ホスト名	IPアドレス	ユーザ名	部署	PC危険レベル	PC危険レベル判定日
☒ 7H5722900	jp1demo11	10.210.160.200		設計部	警告	2008/10/21 09:40:05
☐ 7H572400	kanri-sv.soft.hitachi.co.jp	10.210.160.150		営業部	警告	2008/10/10 18:35:15
☐ 7H572500	chiryou-sv	10.210.160.151		総務部	警告	2008/10/10 18:39:28
☐ 7H572600	office-cl	10.210.160.152		営業部	警告	2008/10/10 18:35:15

☐ 全選択

危険レベル 警告通知 判定 メッセージ

PC危険レベル管理画面より、判定対象クライアントPCを選択後、判定ボタンをクリックし判定を実施

2-4. 判定結果を確認

JP1/NETM/DM

JP1/NETM/CSC

その4 判定結果を確認します

①「注意」と判定された機器を検索

Asset Manager

評価点: [] 点 以下

判定ポリシー名: [] 部分一致

判定ポリシー更新日時: [] (YYYYMMDD)

判定ポリシー割当日時: [] (YYYYMMDD)

アクションポリシー名: [] 部分一致

アクションポリシー更新日時: [] (YYYYMMDD)

アクションポリシー割当日時: [] (YYYYMMDD)

4件中 1~4件目

資産番号	ホスト名	IPアドレス	ユーザ名	告
☒ 7AC222900	jp1demo11	10.210.160.200		設計部
☐ 7H572400	kanri-sv.soft.hitachi.co.jp	10.210.160.150		営業部
☐ 7H572500	chiryu-sv	10.210.160.151		総務部
☐ 7H572600	office-cl	10.210.160.152		営業部

危険: [] 警告通知: [] ネットワーク接続: [] セキュリティ管理: [] 判定・アクション履歴: []

メッセージ: [] 許可: [] 拒否: [] 有効: [] 無効: [] 履歴CSV: []

③各判定項目の判定結果が確認できます。

PC危険レベル詳細: 7AC222900 - Microsoft Internet Explorer

ホスト名	jp1demo11	
ネットワーク情報	IPアドレス	MACアドレス
	10.210.160.200	00:1e:68:44:05:da
PC危険レベル	警告	
PC危険レベル判定日時	2008/10/21 09:40:05	

各判定項目に関する判定結果

判定項目	危険レベル
更新プログラム	警告
ウイルス対策製品	安全
不正ソフトウェア	安全
必須ソフトウェア	注意
PCセキュリティ設定	警告
ユーザ定義	注意

判定・アクション履歴: [] 機器詳細: [] 閉じる: []

②検索結果から判定結果を参照したい機器をクリック

表示

④判定項目をクリックで詳細判定結果を表示

2-4. 判定結果を確認

■セキュリティ対策状況の確認

JP1/NETM/DM

JP1/NETM/CSC

「更新プログラム」の詳細判定結果

管理者側でどこの設定が不十分であるかを把握できます。

更新プログラム詳細: 7AC222900 - Microsoft Internet Explorer

更新プログラムに関する危険レベル	警告
PC危険レベル判定日時	2008/10/21 19:51:17
OS情報	Windows Server 2003, Standard Edition
サービスパック	Service Pack 1
判定条件	最新更新プログラム

更新プログラム情報	危険レベル
MS07-040(928365)	警告

危険レベル「警告」

閉じる

2-4. 判定結果を確認

JP1/NETM/DM

JP1/NETM/CSC

■セキュリティ対策状況の確認

「ウイルス対策製品」の詳細判定結果

管理者側でどこの設定が不十分であるかを把握できます。

危険レベル「安全」

ウィルス対策製品詳細: 7AC222900 - Microsoft Internet Explorer

ウィルス対策製品に関する危険レベル	安全
PC危険レベル判定日時	2008/10/21 19:51:17
製品名	AntiVirus Corporate Edition 10.1
製品バージョン	10.1.6.6000
エンジンバージョン	81.2.0.25
ウィルス定義ファイル	20081006.006
常駐状態	常駐

ウィルス対策製品のポリシーおよび判定結果

製品名	製品バージョン	エンジンバージョン	ウィルス定義ファイル	非常駐判定	危険レベル
AntiVirus Corporate Edition 10.1				判定する	安全

閉じる

2-4. 判定結果を確認

■セキュリティ対策状況の確認

「不正ソフトウェア」の詳細判定結果

管理者側でどこの設定が不十分であるかを把握できます。

危険レベル「安全」

不正ソフトウェアに関する危険レベル 安全

PC危険レベル判定日時 2008/10/21 19:51:17

不正ソフトウェアに関する判定結果

不正ソフトウェア名	インストール状態	インストールバージョン	不正バージョン	危険レベル
SoftEther	未インストール			安全

閉じる

2-4. 判定結果を確認

JP1/NETM/DM

JP1/NETM/CSC

■セキュリティ対策状況の確認

「必須ソフトウェア」の詳細判定結果

管理者側でどこの設定が不十分であるかを把握できます。

必須ソフトウェア詳細: 7AC222900 - Microsoft Internet Explorer

必須ソフトウェアに関する危険レベル	注意
PC危険レベル判定日時	2008/10/21 19:51:17

必須ソフトウェアに関する判定結果

グループ名	必須ソフトウェア名	インストール状態	インストールバージョン	必須バージョン	ソフトウェアの危険レベル	グループの危険レベル
JP1/NETM/DM Client		インストール済み	0852		安全	安全
JP1/秘文	HIBUN-AE	未インストール			注意	注意

閉じる

危険レベル「注意」

2-4. 判定結果を確認

■セキュリティ対策状況の確認

JP1/NETM/DM

JP1/NETM/CSC

「PCセキュリティ設定」の詳細判定結果

管理者側でどこの設定が不十分であることを把握できます。

危険レベル「警告」

PCセキュリティ設定詳細: 7AC222900 - Microsoft Internet Explorer

PCセキュリティ設定に関する危険レベル 警告

PC危険レベル判定日時 2008/10/21 19:51:17

グループ	判定項目	PC設定	判定条件	危険レベル
アカウント	Guestアカウント設定	Guestアカウント無効	Guestアカウント有効	安全
パスワード	脆弱なパスワード	なし	-	安全
	無期限パスワード	Administrator;ASPNET;IUSR_JP1DEMO1;IWAM_JP1DEMO11	-	警告
	パスワード更新経過日数	なし	180日以上	安全
ログオン	自動ログオンの設定	設定なし	-	安全
共有設定	共有フォルダの設定	設定あり	-	警告
匿名接続	匿名接続による制限	無効(制限されていない)	-	警告
サービス	不要サービスの稼働	不要サービスあり	-	警告
自動更新	Windows自動更新の設定	有効	-	安全
スクリーンセーバー	スクリーンセーバーの設定	有効	-	安全
	スクリーンセーバーのパスワードによる保護	有効	-	安全

判定結果の詳細

閉じる

2-4. 判定結果を確認

■省電力設定状況の確認

JP1/NETM/DM

JP1/NETM/CSC

「ユーザ定義」の詳細判定結果

管理者側でどこの設定が不十分であることを把握できます。

危険レベル「注意」

ユーザ定義詳細: 7AC222900 - Microsoft Internet Explorer

ユーザ定義に関する危険レベル	注意
PC危険レベル判定日時	2008/10/21 09:40:05

判定項目	クラス	プロパティ	値	比較条件	比較値	結果	危険レベル
モニタ電源OFF設定率(AC)-1	ハードウェア資産情報	モニタの電源を切る(AC)	0000001200	完全一致	0000000000	○	安全
モニタ電源OFF設定率(AC)-2	ハードウェア資産情報	モニタの電源を切る(AC)	0000001200	以上	0000000600	×	注意
モニタ電源OFF設定率(DC)-1	ハードウェア資産情報	モニタの電源を切る(DC)	0000000900	完全一致	0000000000	○	安全
モニタ電源OFF設定率(DC)-2	ハードウェア資産情報	モニタの電源を切る(DC)	0000000900	以上	0000000600	×	注意
CPU省電力モード設定率(AC)	ハードウェア資産情報	プロセッサ調整(AC)	NONE	不一致	ADAPTIVE	×	注意
CPU省電力モード設定率(DC)	ハードウェア資産情報	プロセッサ調整(DC)	NONE	不一致	ADAPTIVE	×	注意
新型マシン(省電力対応CPU)	ハードウェア資産情報	CPU	28694	不一致	28694	○	安全
	ハードウェア資産情報	CPU	28694	不一致	28695	-	
ハードディスク電源OFF設定率(AC)-1	ハードウェア資産情報	ハードディスクの電源を切る(AC)	0000000000	完全一致	0000000000	×	注意
ハードディスク電源OFF設定率(AC)-2	ハードウェア資産情報	ハードディスクの電源を切る(AC)	0000000000	以上	0000001800	○	安全
ハードディスク電源OFF設定率(DC)-1	ハードウェア資産情報	ハードディスクの電源を切る(DC)	0000001800	完全一致	0000000000	○	安全
ハードディスク電源OFF設定率(DC)-2	ハードウェア資産情報	ハードディスクの電源を切る(DC)	0000001800	以上	0000001800	×	注意

開じる

判定結果の詳細

2-5. 対策傾向をグラフで確認

その5 グラフで対策傾向を把握します

③「検索」ボタンをクリック

②「セキュリティ対策率」「省電力設定率」などグラフの集計観点を選択

⑤対象を選択し「グラフ」ボタンをクリックで対策率をグラフで表示

④部署毎の月単位の対策率を表示

①判定結果の統計データを検索

The screenshot shows the 'Asset Information Manager' web application. The left sidebar contains a tree view with categories like '機器管理' (Device Management), 'ライセンス管理' (License Management), 'ソフトウェア適用管理' (Software Application Management), 'セキュリティ管理' (Security Management), 'システム管理' (System Management), and 'クライアントセキュリティ' (Client Security). Under 'セキュリティ管理', '統計データ' (Statistics Data) is selected. The main area has a search form with fields for '部署' (Department), '部署階層' (Department Hierarchy), '集計観点' (Aggregation Point), '集計期間' (Aggregation Period), '集計間隔' (Aggregation Interval), and '週の開始日' (Start of Week). The '集計観点' dropdown is set to '対策率' (Countermeasure Rate). Below the form are buttons for '検索' (Search), 'CSV', 'グラフ' (Graph), '全選択' (Select All), and '全解除' (Deselect All). The 'グラフ' button is highlighted. Below the buttons is a table showing the countermeasure rates for various departments from January to July 2008. The table is titled '7件中 1～7件目' (7 items, 1-7 items). The departments listed are 営業部 (Sales), 開発部 (Development), 経理部 (Accounting), 情報システム部 (Information Systems), and 総務部 (General Affairs). The table columns are labeled with months from 2008/01 to 2008/07. The data shows the percentage of countermeasures implemented for each department over time.

部署	2008/01月	2008/02月	2008/03月	2008/04月	2008/05月	2008/06月	2008/07月
営業部	86.0%	81.0%	79.8%	78.0%	74.7%	72.3%	70.6%
開発部	54.7%	66.5%	68.0%	71.8%	75.6%	80.5%	81.4%
経理部	66.0%	66.9%	68.0%	65.8%	66.2%	67.6%	68.5%
情報システム部	60.7%	72.5%	74.0%	77.8%	81.6%	86.5%	90.3%
総務部	43.4%	49.8%	57.3%	64.8%	70.0%	78.7%	86.5%

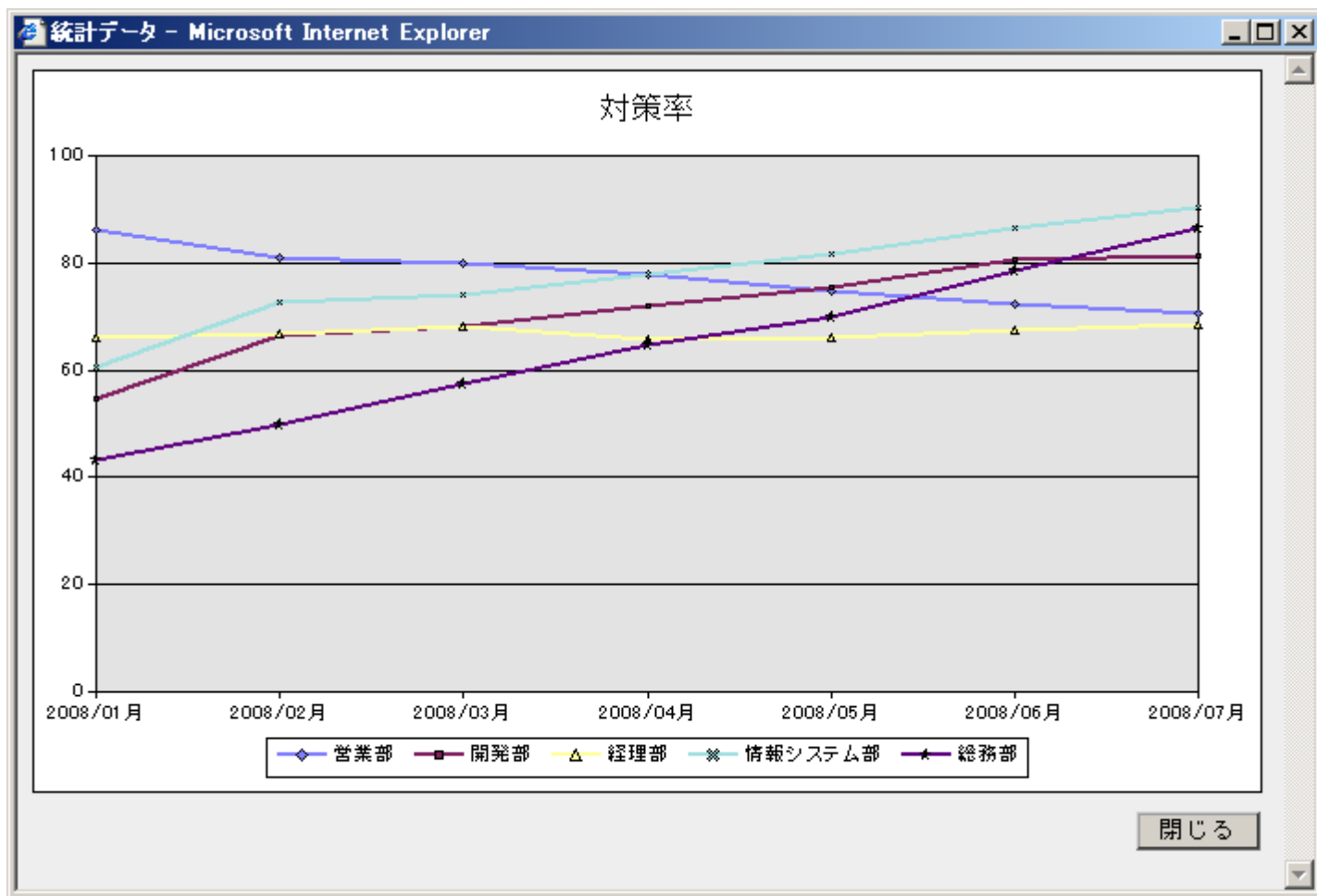
2-5. 対策傾向をグラフで確認

JP1/NETM/DM

JP1/NETM/CSC

部署毎のPCのセキュリティ対策率をグラフで表示

管理者側で部署毎のセキュリティ対策率の傾向をビジュアル的に把握できます。



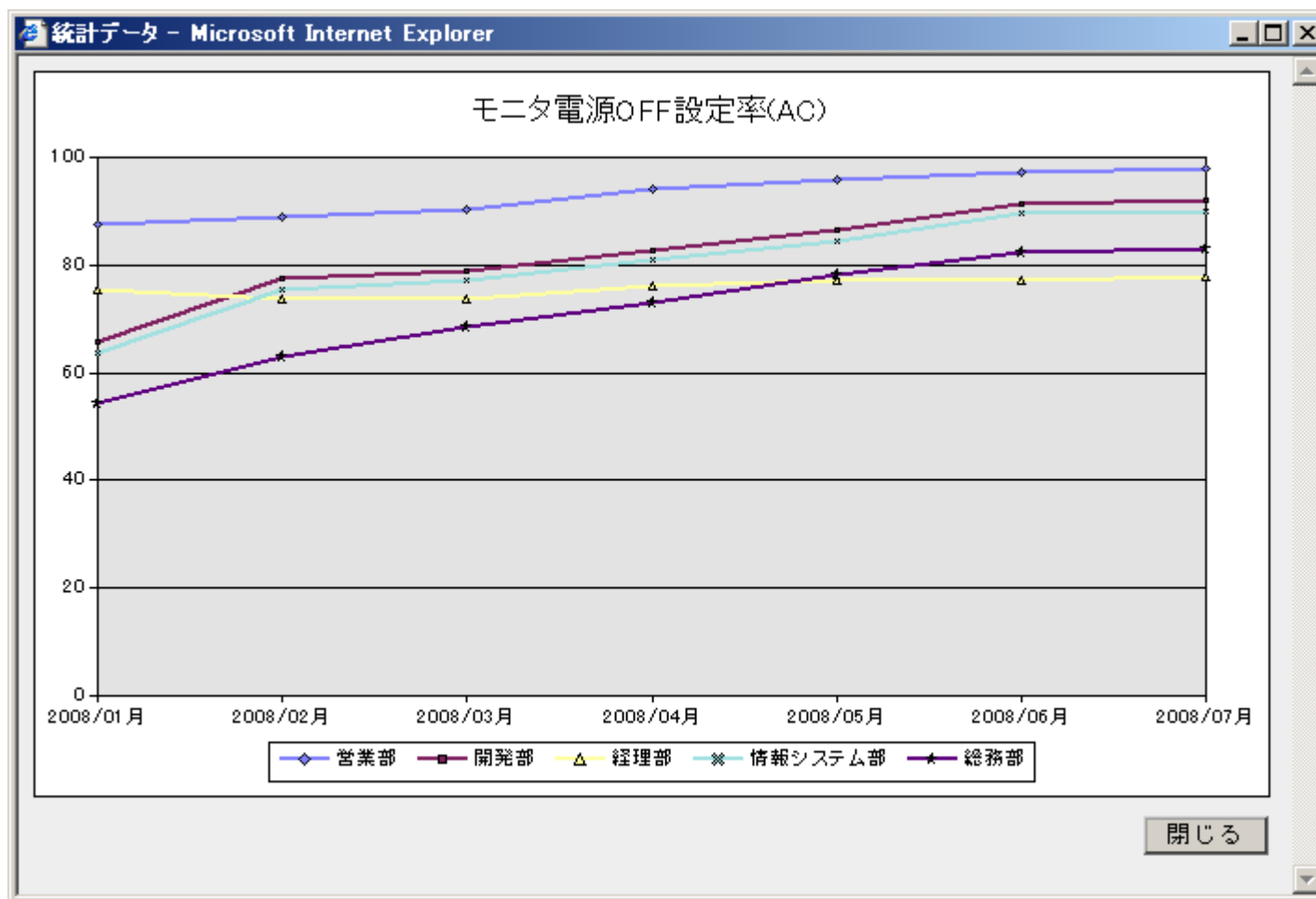
2-5. 対策傾向をグラフで確認

JP1/NETM/DM

JP1/NETM/CSC

部署毎のPCの省電力設定率をグラフで表示

PCの省電力設定率を観点に対策傾向をグラフ表示することもできます。



2-6. 部署毎のセキュリティ対策状況を点数評価

その6 部署毎にセキュリティ対策状況を点数評価できます

①集計観点を選択

②「検索」ボタンをクリック

評価点 = 100(点)

- × (更新プログラムの係数)
- × (ウィルス対策製品の係数)
- × (不正ソフトウェアの係数)
- × (必須ソフトウェアの係数)
- × (PCセキュリティ設定の係数)
- × (ユーザ定義の係数)

【危険レベル係数】

安全	: 1
注意	: 0.75
警告	: 0.5
危険	: 0.25

③部署毎の
点数評価結果

部署	最低点	平均点	集計台数	管理台数
営業部	37	37	2	2
設計部	13	13	1	1
総務部	37	37	1	1

3

JP1 / NETM / DM Clientを漏れなく
導入したい

3. JP1/NETM/DM Clientを漏れなく導入したい

クライアントPCへのJP1/NETM/DM Clientの導入を徹底したいが、
良い方法がありますか？



**JP1/NETM/DM未導入ホスト検出機能を
使用しましょう！**

【対象製品】 JP1/NETM/DM

3-1. 探索範囲を指定

IPアドレスで検索
範囲を指定します。

SNMPを使用して
ホストの情報を
取得します。

ホスト探索設定の追加

探索設定

名称(N) demo

IPアドレス - 開始(L) 10 210 160 1

IPアドレス - 終了(U) 10 210 160 254

コミュニティ名

コミュニティ名一覧(O)

コミュニティ名
public

追加(A) 変更(C) 削除(D)

スケジュール設定

☒ 即時実行(Q)

☐ スケジュール実行(H)

☐ 毎日(E) ☐ 毎週(W) ☐ 毎月(M)

日(Y) 時間(P) 時 分

オプション

☒ ホスト名を取得する(G)

情報取得範囲

☒ ルータから情報取得(R)

☐ 全端末から情報取得(B)

☐ 起動確認する(F)

保存(S) 保存して開始(T) キャンセル

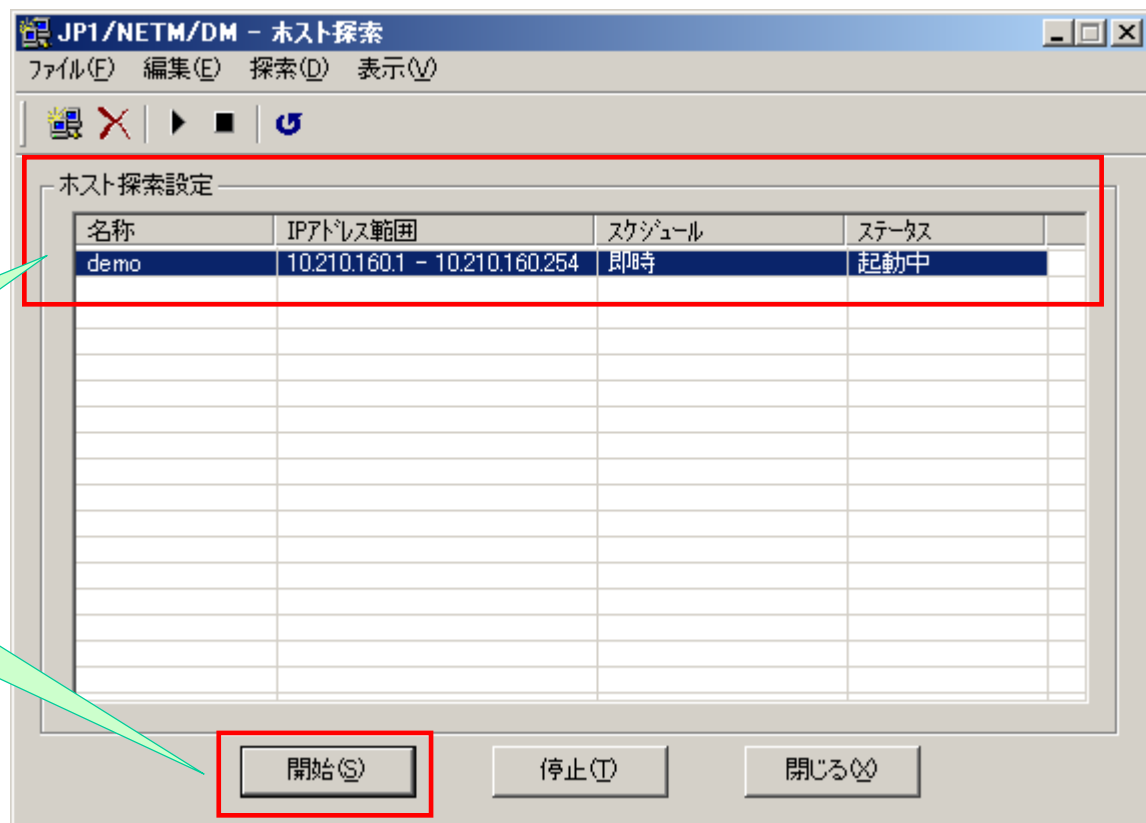
情報取得先を
指定します。

探索経路にSNMP
に回答しない
ルータが含まれる
場合、ルータから
の取得だけで
不十分な場合に
選択します。

3-2. 探索を実行

その2 探索を実行します

設定したIPアドレスの探索範囲に対し、探索を開始します。

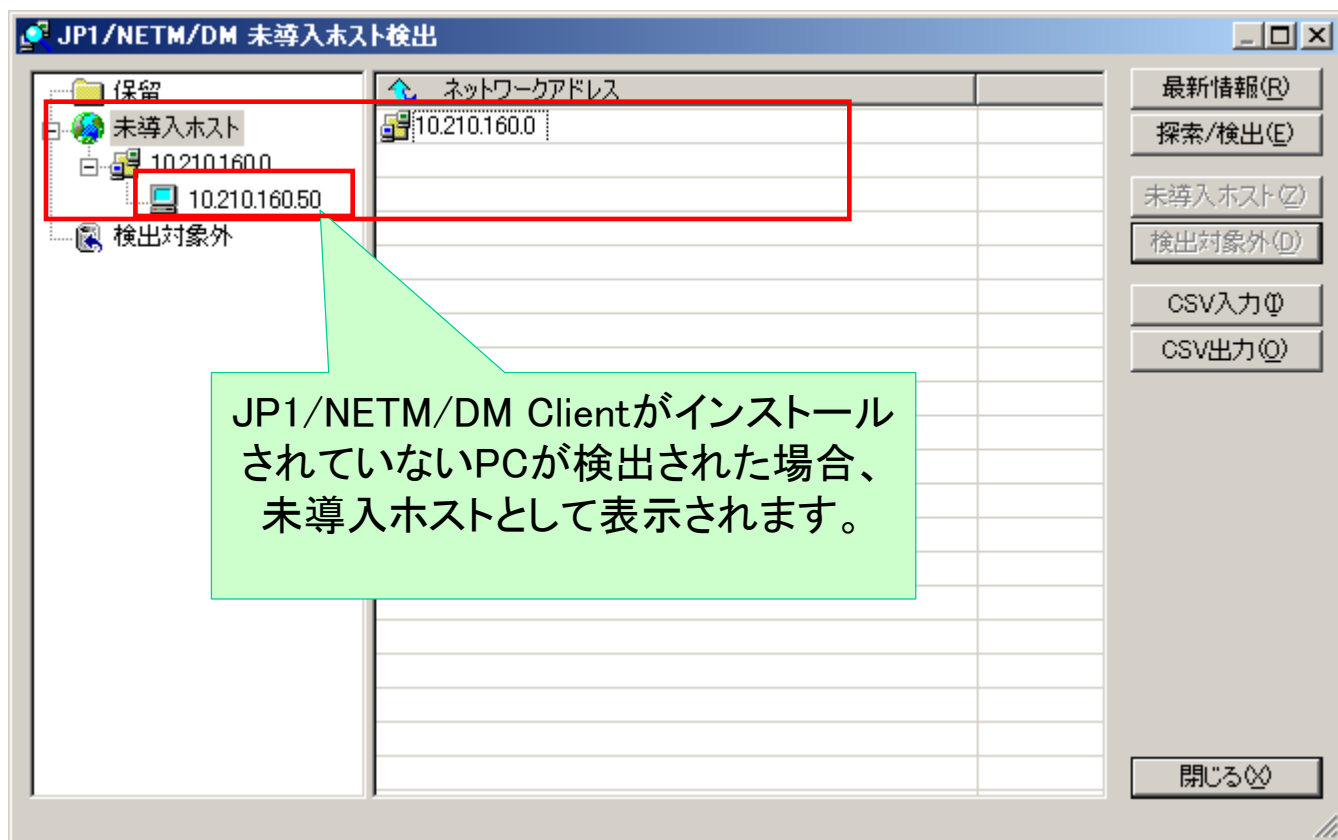


設定したIPアドレス
範囲を選択し、
探索を開始します。

3-3. 探索結果を確認

その3 JP1/NETM/DM Client未導入PCの探索結果を確認します

「JP1/NETM/DM未導入ホスト検出」画面に未導入のホストが表示されます。



4

JP1 / NETM / DM Clientの アンインストールを防ぎたい

4. JP1/NETM/DM Clientのアンインストールを防ぎたい

JP1/NETM/DM Clientをアンインストールされないようにする方法はありませんか？



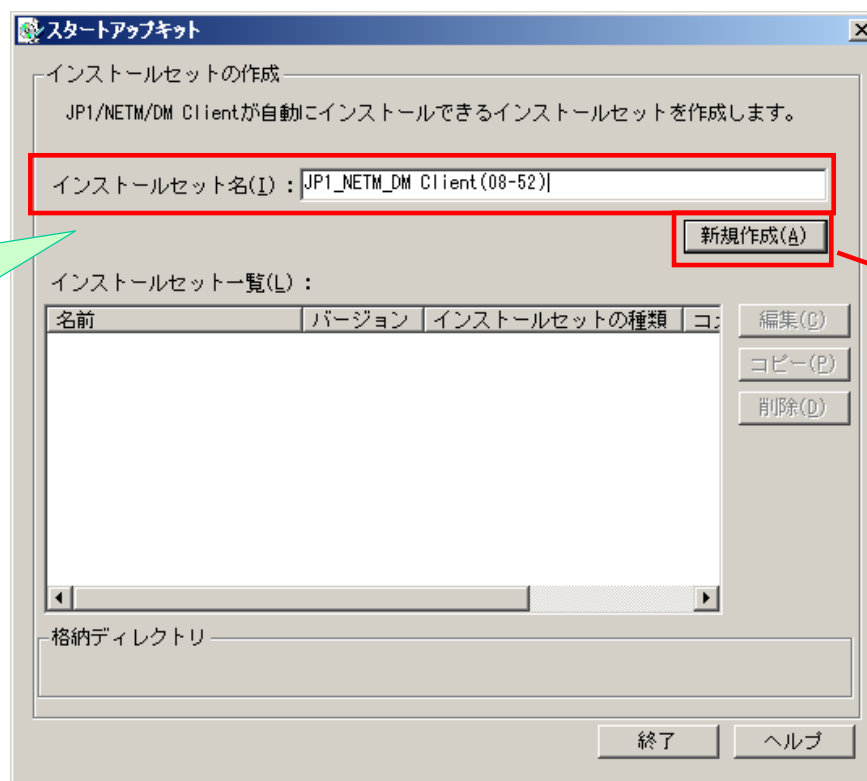
JP1/NETM/DM Administrator Kitを利用しましょう！

【対象製品】 JP1/NETM/DM Administrator Kit

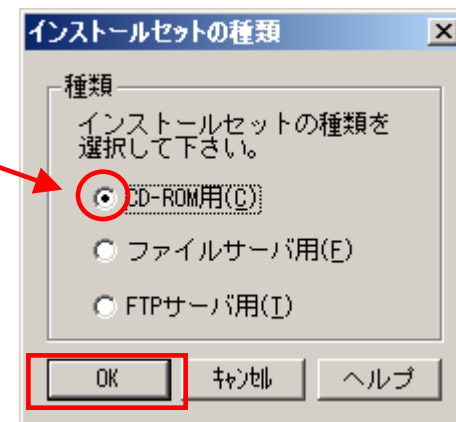
4-1. アンインストール防止インストール媒体を作成

JP1/NETM/DM ADKでワンタッチインストールのJP1/NETM/DM Client
インストール媒体を作成できますが、ユーザーによるアンインストールを防止できる
インストール媒体を作成することができます。

①JP1/NETM/DM ADKを使用しDM Clientインストール媒体作成を開始。

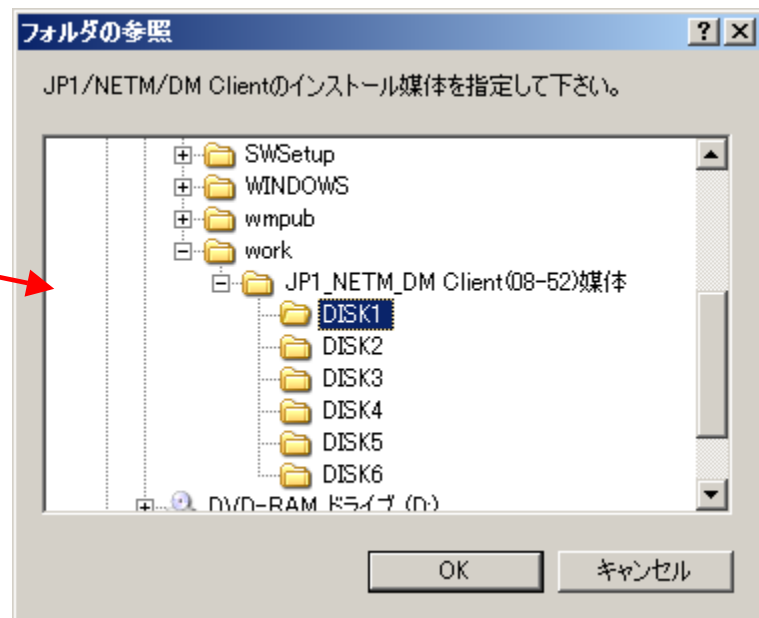
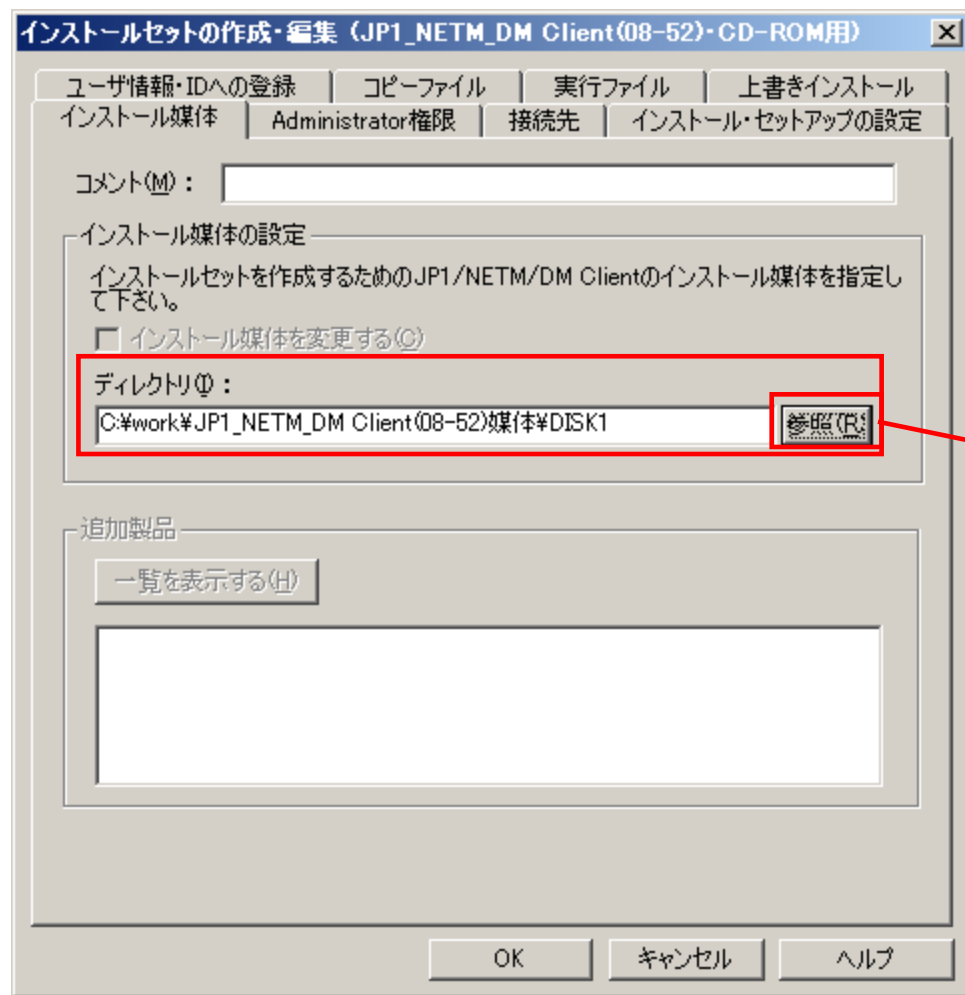


インストールセット名
を指定し、「新規作成」
ボタンをクリック



4-1. アンインストール防止インストール媒体を作成

②JP1/NETM/DM Clientインストール媒体のあるフォルダを指定します。



4-1. アンインストール防止インストール媒体を作成

③上位接続先を指定します。

インストールセットの作成・編集 (JP1_NETM_DM Client(08-52)-CD-ROM用)

ユーザ情報・IDへの登録 | コピーファイル | 実行ファイル | 上書きインストール
インストール媒体 | Administrator権限 | 接続先 | インストール・セットアップの設定

接続先の指定方法を選択し、必要な項目を指定して下さい。

☒ 接続先を指定する(P) ————
クライアントの接続先の製品種別、ホスト名又はIPアドレスを指定して下さい。

☒ JP1/NETM/DM Manager(M)
☐ JP1/NETM/DM Client(中継システム)
☐ またはJP1/NETM/DM SubManager(S)

ホスト名又はIPアドレス(H)

☐ 自動に指定する(T) ————
JP1/NETM/DM ClientをインストールするマシンのIPアドレスの範囲によって接続先を決定します。IPアドレスの範囲と接続先を指定して下さい。
ファイルから読み込む場合は、ファイルを指定してから「入力・編集」ボタンを押して下さい。

ファイル(F) : 参照(R)

☐ インストール後も自動に指定する(Q)

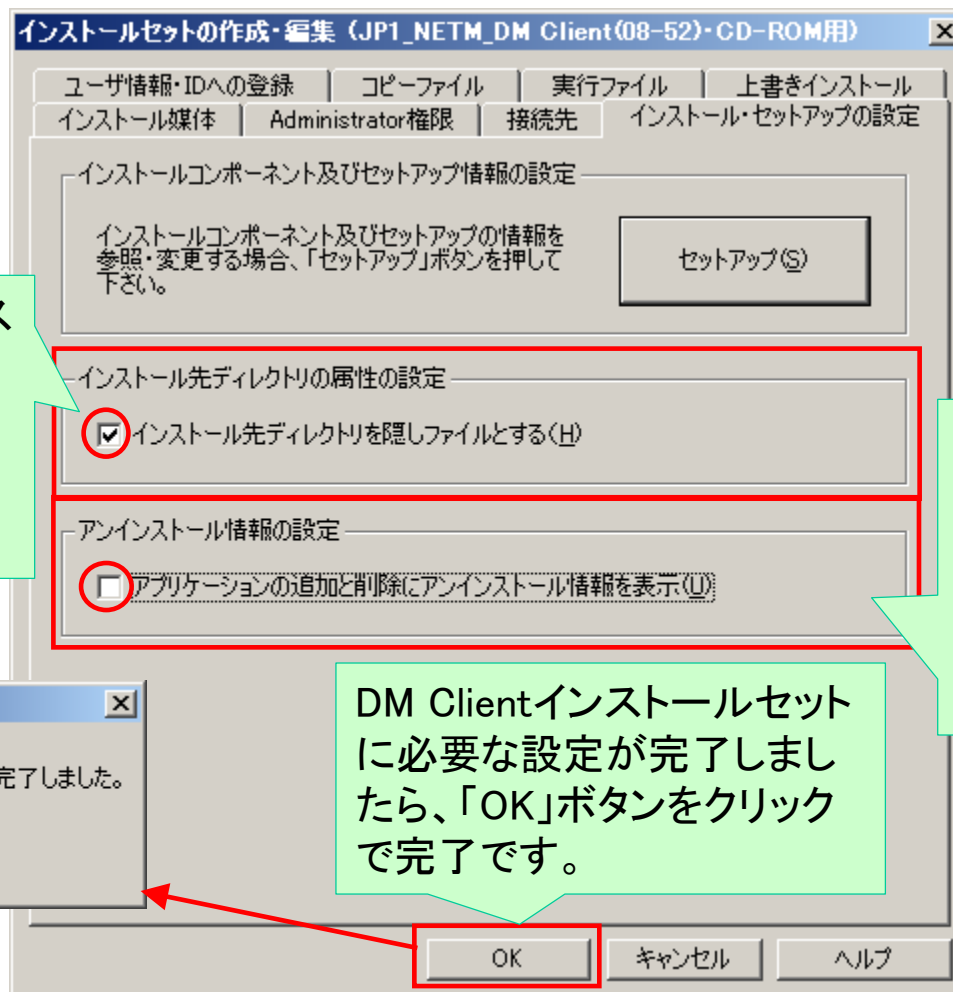
☐ JP1/NETM/DM Clientインストール時に入力(F)

OK キャンセル ヘルプ

上位接続先は、
①固定で指定
②IPアドレスの範囲によって指定
③DM Clientインストール時に指定
の3点の方法で指定が可能です。

4-1. アンインストール防止インストール媒体を作成

④DM Clientのアンインストール防止設定を設定します。



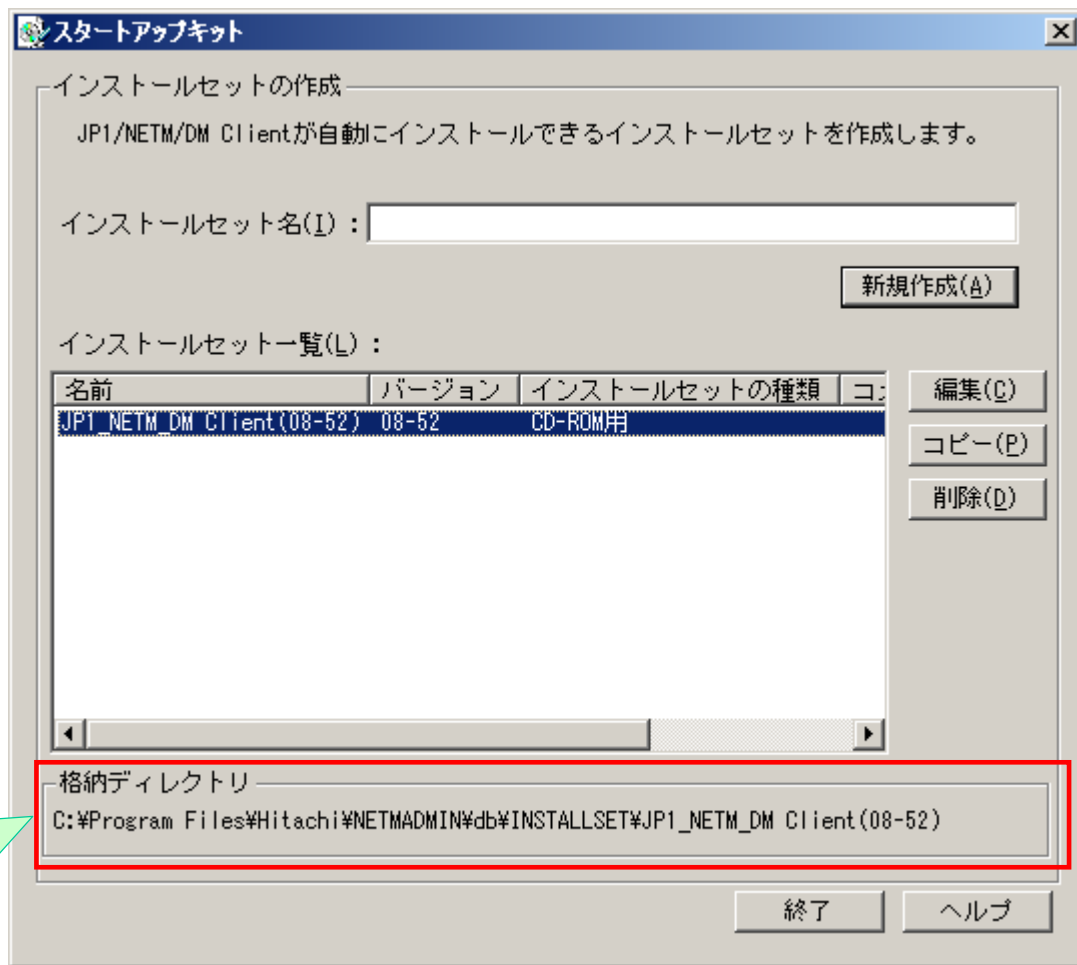
こちらのチェックボックスをオンにすると、JP1/NETM/DM Clientのインストールフォルダを非表示にします。

こちらのチェックボックスをオンにすると、「アプリケーションの追加と削除」にJP1/NETM/DM Clientが表示されません。

DM Clientインストールセットに必要な設定が完了しましたら、「OK」ボタンをクリックで完了です。

4-1. アンインストール防止インストール媒体を作成

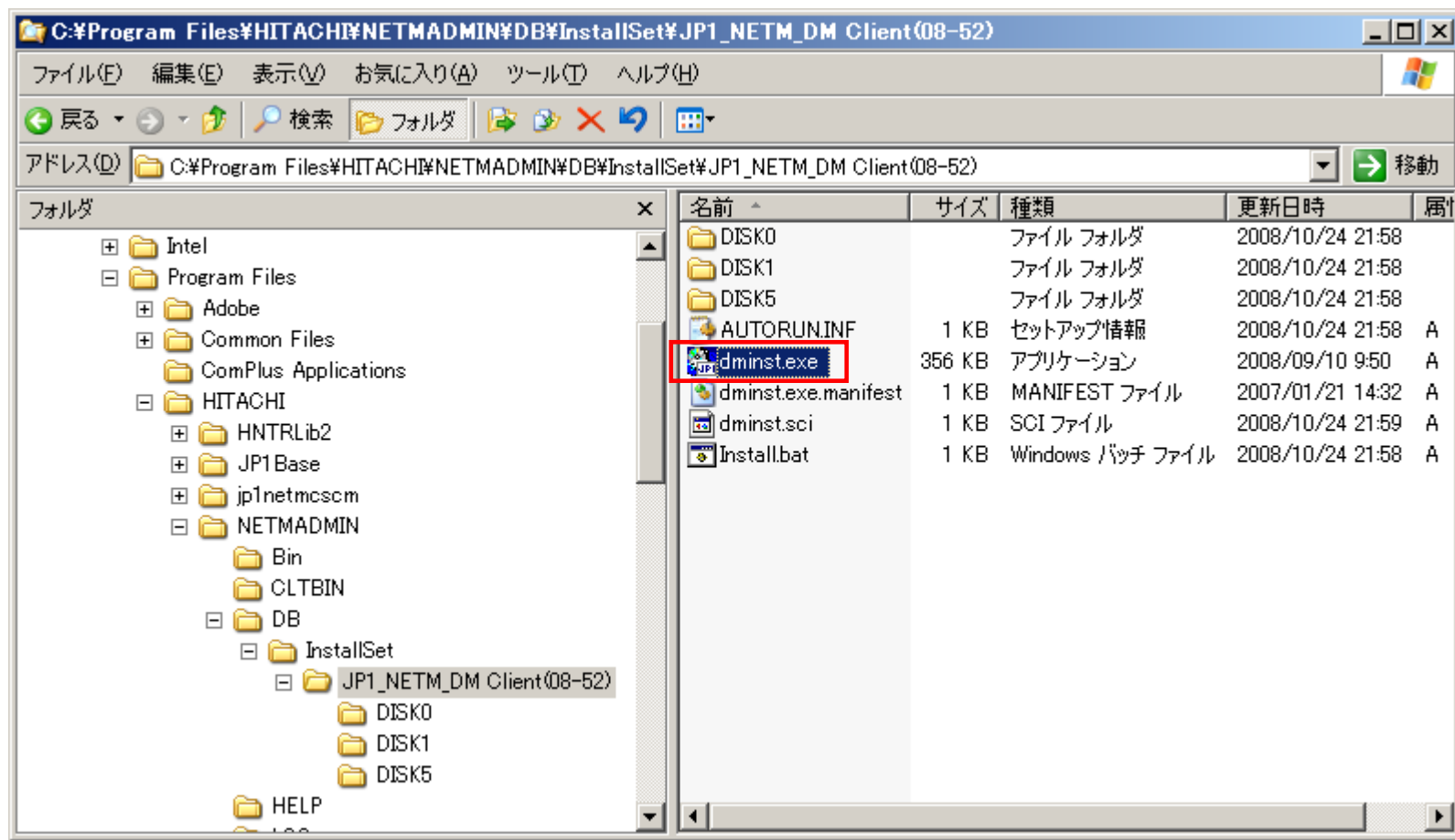
- ⑤DM Clientアンインストール防止設定がされたインストール媒体が作成されます。



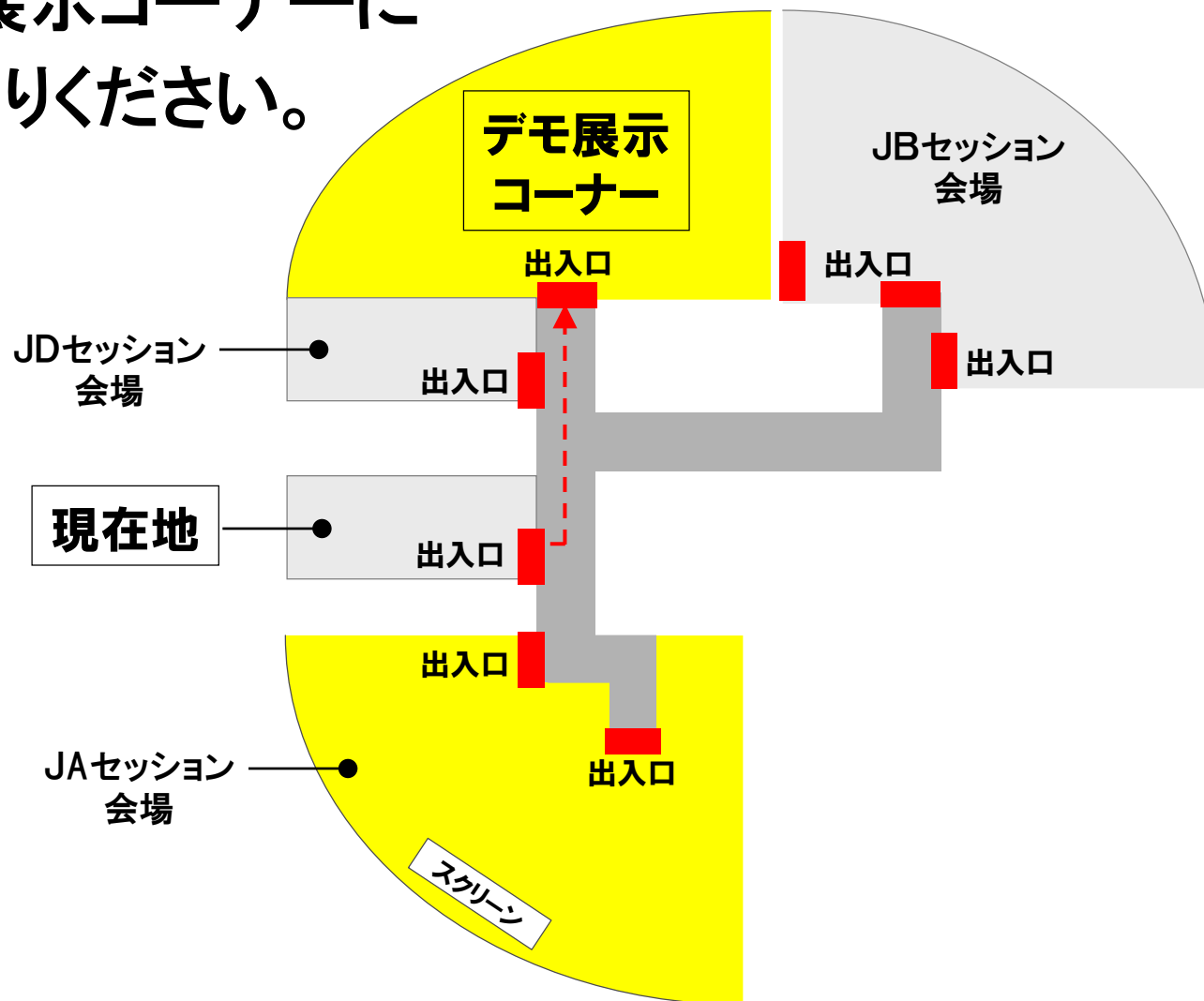
格納ディレクトリ直下にインストール媒体が作成されています。

4-1. アンインストール防止インストール媒体を作成

- ⑥作成されたDM Clientアンインストール防止設定がされたインストール媒体を使用してDM Clientを上書きインストールまたは新規インストールすることで、アンインストール防止がされたDM Clientを展開することができます。



ぜひ、デモ展示コーナーに
お立ち寄りください。



- Windowsは、米国およびその他の国における米国Microsoft Corp.の登録商標です。
- 秘文は、日立ソフトウェアエンジニアリング(株)の登録商標です。

その他記載されている会社名、製品名は各社の商標または登録商標です。

本資料に記載しております画面表示をはじめ、製品仕様は、改良のため変更することがあります。

本製品を利用したシステム構築をする場合は、ご利用の製品のマニュアルを必ず参照いただけるようお願いします。