

# Systemwalker Certified Professional Desktop V13

---

---

---

---

2008 年 12 月 3 版



**FUJITSU**

THE POSSIBILITIES ARE INFINITE



# **Systemwalker Certified Professional Desktop V13**

2008年 12月 3版

富士通株式会社



## はじめに

本書は、富士通ミドルウェアマスター Systemwalker Certified Professional Desktop V13 試験対策のために作成されたテキストです。

### ■略語表記について

- ・以下の製品すべてを示す場合は、“Windows® 2000”と表記します。
  - Microsoft® Windows® 2000 Professional operating system
  - Microsoft® Windows® 2000 Server operating system
  - Microsoft® Windows® 2000 Advanced Server operating system
  
- ・以下の製品すべてを示す場合は、“Windows®”と表記します。
  - Microsoft® Windows Server® 2003, Standard Edition
  - Microsoft® Windows Server® 2003, Enterprise Edition
  - Microsoft® Windows Server® 2003, Standard x64 Edition
  - Microsoft® Windows Server® 2003, Enterprise x64 Edition
  - Microsoft® Windows Server® 2003 R2, Standard Edition
  - Microsoft® Windows Server® 2003 R2, Enterprise Edition
  - Microsoft® Windows Server® 2003 R2, Standard x64 Edition
  - Microsoft® Windows Server® 2003 R2, Enterprise x64 Edition
  - Microsoft® Windows® 2000 Professional operating system
  - Microsoft® Windows® 2000 Server operating system
  - Microsoft® Windows® 2000 Advanced Server operating system
  - Microsoft® Windows NT® Server network operating system Version 4.0
  - Microsoft® Windows NT® Workstation operating system Version 4.0
  - Microsoft® Windows Vista® Ultimate
  - Microsoft® Windows Vista® Enterprise
  - Microsoft® Windows Vista® Business
  - Microsoft® Windows Vista® Home Premium
  - Microsoft® Windows Vista® Home Basic
  - Microsoft® Windows Vista® Ultimate 64 ビット版
  - Microsoft® Windows Vista® Enterprise 64 ビット版
  - Microsoft® Windows Vista® Business 64 ビット版
  - Microsoft® Windows Vista® Home Premium 64 ビット版
  - Microsoft® Windows Vista® Home Basic 64 ビット版
  - Microsoft® Windows® XP Professional
  - Microsoft® Windows® XP Home Edition
  - Microsoft® Windows® Millennium Edition
  - Microsoft® Windows® 98 operating system
  - Microsoft® Windows® 98 Second Edition

- ・以下の製品すべてを示す場合は、“Internet Explorer”と表記します。
  - －Microsoft® Internet Explorer V5.5(Service Pack 2)
  - －Microsoft® Internet Explorer V6.0
  - －Microsoft® Internet Explorer V7.0

■商標について

- Systemwalker は富士通株式会社の登録商標です。
- Microsoft、MS、MS-DOS、Outlook、Windows、Windows Vista、Windows Server、Active Directory およびその他のマイクロソフト製品の名称および製品名は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。
- ActiveX は、米国 Microsoft Corporation の登録商標です。
- FeliCa は、ソニー株式会社の登録商標です。
- Symantec、Symantec ロゴ、Norton AntiVirus は、Symantec Corporation の米国における登録商標です。
- ウイルスバスターは、トレンドマイクロ株式会社の登録商標です。
- VirusScan および NetShield は、米国 Network Associates 社および関連会社の商標または登録商標です。
- Microsoft Corporation のガイドラインに従って画面写真を使用しています。
- Citrix Presentation Server は、Citrix Systems, Inc. の米国およびその他の国における登録商標です。
- UNIX は、The Open Group の米国ならびにその他の国における登録商標です。
- 本資料に記載されているシステム名、製品名などには必ずしも商標表示(TM、®)を付記していません。
- その他の製品名は、各社の商標または登録商標です。

2008 年 12 月      3 版

## 目次

|         |                                      |    |
|---------|--------------------------------------|----|
| 第 1 章   | クライアント管理の概要                          | 1  |
| 1.1     | クライアント管理の問題と対策                       | 2  |
| 1.2     | クライアント管理製品の位置付け                      | 3  |
| 1.3     | 情報漏えい対策ソリューション                       | 5  |
| 第 2 章   | Systemwalker Desktop Patrol          | 7  |
| 2.1     | 概要                                   | 8  |
| 2.2     | 特長                                   | 9  |
| 2.3     | システム構成                               | 11 |
| 2.4     | ポリシー                                 | 13 |
| 2.5     | 機能                                   | 15 |
| 2.5.1   | 資産管理                                 | 16 |
| 2.5.1.1 | 資産管理の概要                              | 16 |
| 2.5.1.2 | インベントリ情報                             | 17 |
| 2.5.1.3 | インベントリ情報の収集方法(エージェントモード)             | 19 |
| 2.5.1.4 | インベントリ情報の収集方法(コマンドモード)               | 20 |
| 2.5.1.5 | クライアントポリシーの種類                        | 21 |
| 2.5.1.6 | PC稼働管理                               | 23 |
| 2.5.2   | セキュリティ管理                             | 24 |
| 2.5.2.1 | セキュリティパッチの自動適用                       | 24 |
| 2.5.2.2 | セキュリティパッチ自動適用のポリシー設計                 | 25 |
| 2.5.2.3 | セキュリティ監査                             | 27 |
| 2.5.2.4 | ソフトウェア辞書                             | 29 |
| 2.5.3   | ライセンス管理                              | 32 |
| 2.5.4   | コンテンツ管理                              | 33 |
| 2.5.5   | 廃棄管理                                 | 35 |
| 2.5.6   | リモート操作                               | 37 |
| 2.6     | 導入/運用                                | 38 |
| 2.6.1   | マスタ管理情報の設定                           | 39 |
| 2.6.2   | Active Directory 連携                  | 41 |
| 2.6.3   | モバイル PC 運用                           | 42 |
| 第 3 章   | Systemwalker Desktop Patrol Assessor | 45 |
| 3.1     | 概要                                   | 46 |
| 3.2     | 特長                                   | 47 |
| 3.3     | システム構成                               | 48 |
| 3.4     | 機能                                   | 49 |
| 3.4.1   | 機器管理                                 | 50 |
| 3.4.2   | 契約管理                                 | 52 |
| 3.4.3   | 棚卸支援                                 | 54 |
| 3.4.4   | レポート出力                               | 56 |
| 3.5     | 導入/運用                                | 59 |
| 3.5.1   | インベントリ情報の登録機能                        | 60 |
| 3.5.2   | 未登録機器の自動検知                           | 62 |
| 第 4 章   | Systemwalker Desktop Keeper          | 65 |
| 4.1     | 概要                                   | 66 |

|          |                                   |     |
|----------|-----------------------------------|-----|
| 4.2      | 特長                                | 67  |
| 4.3      | システム構成                            | 68  |
| 4.4      | ポリシー                              | 71  |
| 4.4.1    | ポリシーの概要                           | 72  |
| 4.4.2    | CTグループ/CT単位のポリシー設定                | 73  |
| 4.4.3    | ユーザーグループ/ユーザー単位のポリシーの設定           | 74  |
| 4.5      | 機能                                | 76  |
| 4.5.1    | 記録機能                              | 77  |
| 4.5.1.1  | ファイル持出しログ                         | 78  |
| 4.5.1.2  | 印刷操作ログ/PrintScreenキーログ            | 80  |
| 4.5.1.3  | アプリケーション動作ログ                      | 82  |
| 4.5.1.4  | 画面キャプチャ                           | 84  |
| 4.5.1.5  | メールログ                             | 85  |
| 4.5.1.6  | デバイス構成変更ログ                        | 87  |
| 4.5.1.7  | コマンドプロンプト操作ログ                     | 88  |
| 4.5.1.8  | 設定変更ログ                            | 89  |
| 4.5.1.9  | ファイル操作ログ                          | 90  |
| 4.5.1.10 | ログオン/ログオフログ                       | 91  |
| 4.5.2    | 抑止機能                              | 92  |
| 4.5.2.1  | ファイル持出し抑止                         | 93  |
| 4.5.2.2  | 印刷抑止/PrintScreenキー抑止              | 94  |
| 4.5.2.3  | ログオン抑止                            | 95  |
| 4.5.2.4  | アプリケーション起動抑止                      | 96  |
| 4.5.2.5  | メール添付抑止                           | 97  |
| 4.5.3    | 管理機能                              | 98  |
| 4.5.3.1  | サービス/プロセス一覧参照/更新                  | 98  |
| 4.5.3.2  | 操作ログの参照（ログビューアの使用方法）              | 99  |
| 4.5.3.3  | 操作ログの参照（ファイル追跡）                   | 101 |
| 4.5.3.4  | 部門管理機能                            | 102 |
| 4.6      | 導入/運用                             | 104 |
| 4.6.1    | 持出しユーティリティの使用方法                   | 105 |
| 4.6.2    | データベースの運用設計                       | 106 |
| 4.6.2.1  | データベースの容量見積もり                     | 106 |
| 4.6.2.2  | データベースのバックアップ                     | 107 |
| 4.6.3    | シンクライアント環境での運用                    | 108 |
| 第5章      | Systemwalker Desktop Log Analyzer | 109 |
| 5.1      | 概要                                | 110 |
| 5.2      | 特長                                | 111 |
| 5.3      | システム構成                            | 112 |
| 5.4      | 機能                                | 113 |
| 5.4.1    | 情報漏洩予防診断機能                        | 114 |
| 5.4.2    | 目的別集計機能                           | 115 |
| 5.4.3    | レポート出力機能                          | 117 |
| 5.5      | 導入/運用                             | 119 |
| 5.5.1    | ログ連携                              | 120 |
| 5.5.2    | レポート出力ツールの運用方法                    | 121 |

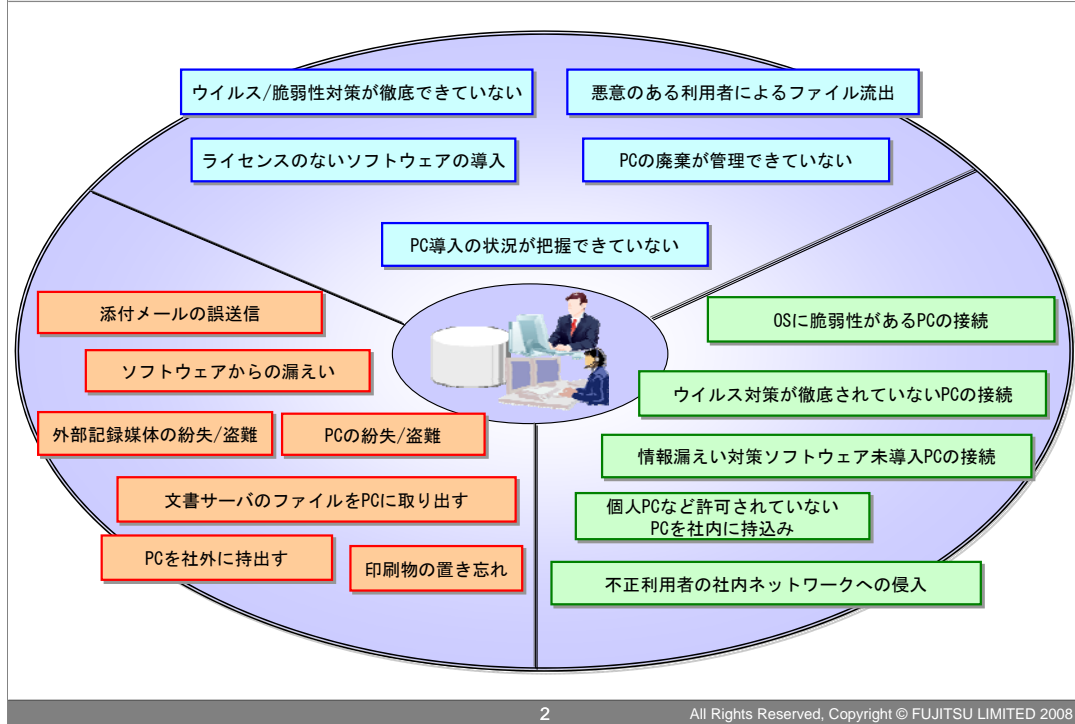
|   |     |
|---|-----|
| 第 6 章 Systemwalker Desktop Inspection         | 123 |
| 6.1 概要  | 124 |
| 6.2 特長  | 125 |
| 6.3 システム構成                                    | 126 |
| 6.4 検疫の流れ                                     | 128 |
| 6.5 機能  | 129 |
| 6.5.1 検疫機能                                    | 130 |
| 6.5.2 ポリシーグループ機能                              | 132 |
| 6.5.3 不正 PC 遮断機能                              | 134 |
| 6.6 運用モデル                                     | 135 |
| 6.6.1 持込み PC の遮断のみモデル                         | 136 |
| 6.6.2 業務サーバの直前で遮断を行うモデル                       | 137 |
| 6.6.3 PC 単位で遮断を行うモデル                          | 138 |
| 6.6.4 その他の運用モデル                               | 139 |
| 第 7 章 Systemwalker Desktop Rights Master      | 143 |
| 7.1 概要  | 144 |
| 7.2 特長  | 145 |
| 7.3 システム構成                                    | 147 |
| 7.4 機能  | 149 |
| 7.4.1 ライセンス管理                                 | 150 |
| 7.4.2 ファイル操作制御                                | 151 |
| 7.4.3 オフライン制御                                 | 152 |
| 7.4.4 Active Directory 連携                     | 153 |
| 7.4.5 操作履歴の記録                                 | 155 |
| 7.4.6 重置印刷                                    | 156 |
| 第 8 章 Systemwalker Desktop シリーズ製品構成           | 157 |
| 8.1 製品エディション                                  | 158 |
| 8.1.1 Systemwalker Desktop Patrol のエディション     | 159 |
| 8.1.2 Systemwalker Desktop Keeper のエディション     | 160 |
| 8.1.3 Systemwalker Desktop Inspection のエディション | 161 |
| 8.2 Desktop シリーズの製品間連携                        | 162 |
| 付録  | 163 |
| 付録 1 用語集                                      | 164 |
| 付録 2 模擬問題                                     | 171 |
| 付録 2-1 模擬問題の解答用紙                              | 190 |
| 付録 2-2 カテゴリ別出題範囲                              | 191 |
| 付録 2-3 正解表                                    | 191 |
| 付録 2-4 模擬問題解説                                 | 192 |



# 第1章 クライアント管理の概要

- 1.1 クライアント管理の問題と対策
- 1.2 クライアント管理製品の位置付け
- 1.3 情報漏えい対策ソリューション

本章では、クライアント管理の概要について説明します。



今日、以下のようなパソコンに関連する問題があります。

#### ■環境の不備により発生する問題

- ・パソコンの導入状況や廃棄するパソコンの状況が管理できていない
- ・共有利用しているサーバのファイルが悪意のある利用者やファイル交換ソフトウェアにより社外に流出する危険がある

#### ■ネットワーク接続時のチェック漏れにより発生する問題

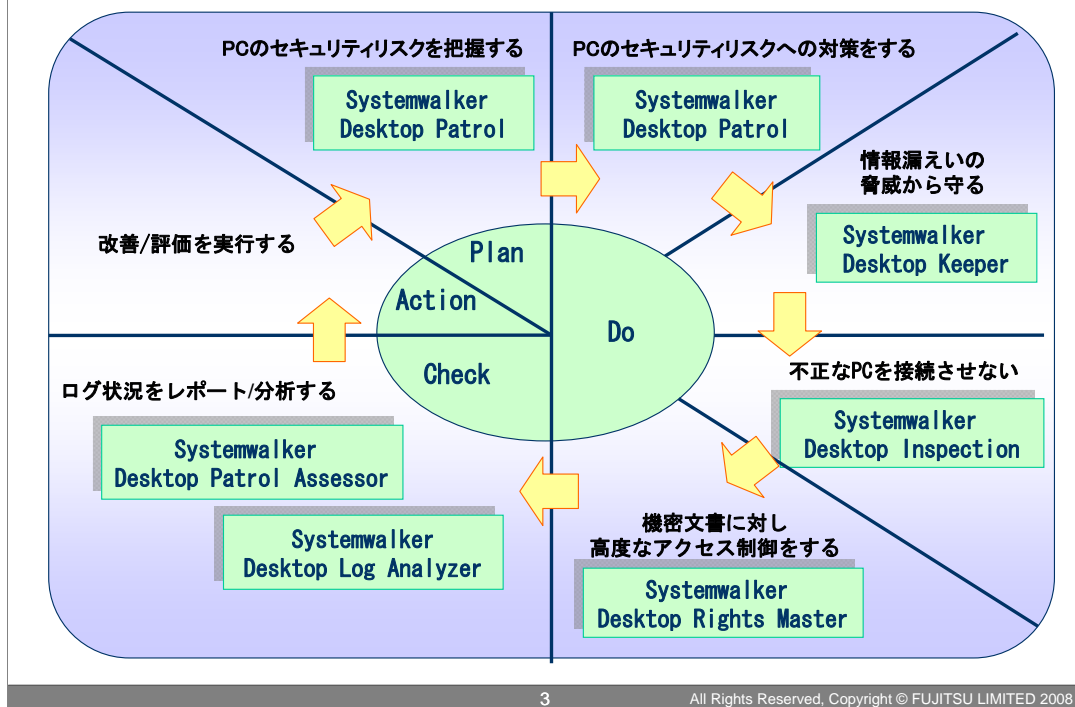
- ・セキュリティレベルの低いパソコンが社内ネットワークに接続してウィルスを蔓延させる危険(リスク)がある
- ・個人パソコンなど許可されていないパソコンを社内に持込むことにより、セキュリティリスクが高くなる
- ・許可されていない利用者が悪意をもって社内ネットワークに侵入することにより被害が発生する

#### ■人為的なミスにより発生する問題

- ・添付ファイル付きメールを誤った相手に送り、情報漏えいする危険がある
- ・ノートパソコンや外部記憶媒体によって社内から持出された機密情報が、紛失/盗難などにより漏えいする危険がある
- ・印刷した機密文書の置き忘れにより情報が漏えいする可能性がある

クライアント管理では、上記の問題に対して「PDCAライフサイクル」のアプローチで対策を提案します。

※以降、「パソコン」を「PC」と呼称します。



Systemwalker Desktopシリーズは、あらゆる情報漏えいリスクを回避するための機能を搭載すると同時に、情報セキュリティマネジメントシステムの「PDCAサイクル」を確実に回していくことで、セキュリティレベルを継続的に改善します。

Systemwalker Desktopシリーズの各製品は、図のように「PDCAサイクル」の各フェーズに対応しています。

#### ■Plan(セキュリティポリシーの策定)

##### ・ Systemwalker Desktop Patrol

セキュリティパッチの自動取得/自動適用により、セキュリティを維持/向上できます。廃棄やリース切れで返却するPCのハードディスクのデータを完全消去して、情報漏えいを防止できます。

#### ■Do(セキュリティシステムの導入/運用)

##### ・ Systemwalker Desktop Patrol

PCのハードウェア/ソフトウェア情報の収集、セキュリティ監査(BIOSパスワードの設定状況やOSのセキュリティ設定、スクリーンセーバーのパスワード設定、IEのセキュリティレベルなどの監査)により、現状のセキュリティリスクを把握できます。

##### ・ Systemwalker Desktop Keeper

情報漏えいリスクとなるクライアントの操作を記録したり、組織内にある電子情報の流出(ファイル持出し、印刷)を防止できます。

・ Systemwalker Desktop Inspection

ネットワーク機器と連携して、外部からの持ち込みPCによる不正接続の排除や、セキュリティレベルの低いPCを検疫し、ウイルス感染を防ぎます。

・ Systemwalker Desktop Rights Master

共有フォルダに登録された電子文書(Microsoft® Office文書、PDF文書など)をファイル単位でアクセス制御することで、情報漏えいを防止します。常時アクセス制御が働くため、不正持出し、不正コピー、廃棄機器/媒体、盗難などの不正アクセスがあっても情報漏えいの脅威から情報を保護できます。

■ Check (セキュリティシステムの分析/評価)

・ Systemwalker Desktop Patrol Assessor

PCからプリンタやFAXなども含めたIT資産全体を、セキュリティ管理と、資産管理の両面からの一元管理を実現します。PCのセキュリティ監査や持出し状況、IT資産の設置場所、リース契約、棚卸など、一括した管理を実現し、監査や内部統制に必要な各種のレポートを作成できます。

・ Systemwalker Desktop Log Analyzer

内部情報漏えい対策としてSystemwalker Desktop Keeperにより記録/収集された企業内部でのPC操作ログ、ファイル操作ログから、クライアント操作の傾向を分析し、システムのセキュリティポリシーの遵守状況、情報漏えい対策における脆弱性などのセキュリティ分析の運用ができます。



2-2. 操作記録：不正行為や問題行為の抑制、漏えい経路の追跡/特定。

PCの操作を記録することで、心理的な抑止効果が期待できます。また、情報が流出した場合に操作ログを検索することで、不正な操作の追跡ができます。

このステップに対しては、Systemwalker Desktop Keeperによりユーザー操作の記録、重要データの操作記録を採取できます。また、Systemwalker Desktop Log Analyzerにより操作ログの集計や分析ができます。

3. 不正接続の排除：不正アクセス、セキュリティレベルの低いPCのアクセスを排除する。

事前に登録されていないPCやセキュリティレベルが社内の規定に達していないPCが社内ネットワークに接続しようとしたとき、検疫により排除できます。

このステップに対しては、Systemwalker Desktop Inspectionにより不正接続の排除を実施し、さらにSystemwalker Desktop Patrolと連携することによりセキュリティパッチ未適用のPCに対して、セキュリティパッチの適用を誘導できます。

4. ファイルへのアクセス制御：オフィスの機密文書に閲覧権限を設定して情報は漏えいさせない。

企業や組織の内部で保有する電子文書(Microsoft® OfficeやPDFなど)のファイル単位/利用者単位でアクセス制御を実施し、知的財産、機密情報などを保護します。また、アクセス履歴を記録し、ファイルが流出した場合でも、認証がなければアクセスできないため、外部に情報が漏れることはありません。

このステップに対しては、Systemwalker Desktop Rights Masterによりオフィスの機密文書のアクセス制御を実現します。