Systemwalker

Systemwalker Desktop Patrol

BIOS パスワード設定状況確認ツール

利用ガイド

第 1.1 版　2011 年 4 月 5 日

１．はじめに

Systemwalker Desktop Patrol V13.0.0 以降でセキュリティ監査として「BIOS パスワード設定の監査」を提供しています。

しかし、「Systemwalker Desktop Patrol メインメニュー」のセキュリティ情報に表示される起動パスワード・設定パスワードの設定内容に対する該当端末/台数が実際の設定状況と異なる場合があります。これは、BIOS パスワード設定状況を参照するシステム的な機構が、メーカ/機種依存により提供されていなかったり、収集された結果が正しく監査できていないケースがあるためです。

このようなセキュリティ監査の表示結果と実際の設定状況に差異が起こりえるため、お客様環境下の各社の PC において、BIOS パスワードが監査できる機種なのか否かをチェックできるように、ツール単独実行が可能な"BIOS パスワード設定状況確認ツール" を提供します。

２．ツール動作条件

当ツールの動作条件は以下の通りです。

◆OS/動作条件

Systemwalker Desktop Patrol V13.0.0 以降の CT の動作環境/OS に従う。

Windows Management Instrumentation (WMI) ランタイムが導入済みであること。*1

当ツールの実行において、administrator 権限は必要なし。

◆製品

Systemwalker Desktop Patrol V13.0.0 以降のインストール有無は問わない。

また、Systemwalker Desktop Patrol V13.0.0 以降の CT が稼動中/停止中は問わない。

*1) Windows 98/Windows NT の場合、初期状態では WMI が導入されていない場合があります。
Microsoft 社のダウンロードセンターホームページより「Windows Management Instrumentation (WMI) SDK 1.5 (Windows 95/98/NT 4.0)」をダウンロードしてインストールしてください。

３．ツール使用方法

◆ツール利用方法

<<準備>>

・ 当ツールにはインストーラはありません。
当ツールは、以下の２つのファイルから構成されます。

ファイル	説明
DtpBiosChk.exe	監査プログラム
DtpBiosChk.dat	監査情報データ

USB メモリ,もしくはネットワーク共有されたフォルダ,等に上記２つのファイルを格納し、そのプログラムを起動してください。

・ このツールは、レジストリを更新しません。アンインストール時は上記２つのファイルを削除してください。

・ 当ツールが格納されたフォルダに 監査結果ファイル "DtpBiosChk_*pcname*.log" を出力します。別のフォルダに出力したい場合は、起動オプション(-o *folder*)を指定してください。
※ *pcname* は、プログラム起動した PC のコンピュータ名
※ *folder* は、出力したいフォルダ名

<<手順>>

下記手順で、**BIOS パスワード設定を変更する前/後の２回、当ツールを実行**してください。
詳細については「５.留意事項」を参照ください。

1) 当ツールを起動します。
エクスプローラから 当ツール(DtpBiosChk.exe)をダブルクリックして起動してください。
または、コマンドプロンプトからプログラム名を指定して起動してください。

➢ 起動引数

DtpBiosChk.exe [-s] [-o *folder*]

option	説明
-s	サイレントモード 監査結果を記録したファイルを起動(表示)しない
-o *folder*	監査結果の出力フォルダ名を指定 当引数の指定がなかった場合は、当 exe が格納されたフォルダ内に出力される ※カレントに存在する '-(ハイフン)' で始まるフォルダ名は指定できません

正しく起動できた場合は、プログラムの復帰値は以下となります。

➢ ツール復帰値

復帰値	説明
0	正常終了
1	起動引数のエラー
2	監査結果ファイルオープンエラー
3	メモリ不足エラー
4	その他のエラー (WMI が導入されていない、WMI 実行環境に問題がある、当ツールの環境情報ファイルが無い/ファイルが異常、など)
5	監査結果ファイルの表示エラー (.log 関連付けプログラムの起動エラー)

2) プログラムが格納されたフォルダ(または指定したフォルダ)に、監査結果が "DtpBiosChk_*pcname*.log" ファイルに記録されます。
※ *pcname* は、プログラム起動した PC のコンピュータ名

3) 当プログラムの終了時に、監査結果ファイルが表示されます。
拡張子 .log に関連付けされたビューア(メモ帳など)が起動され、ファイル内容が表示されます。

4) 監査結果を確認します。
監査結果の内容については 詳しくは、「4.監査結果ファイルの内容」を参照ください。
特に、BIOS 起動パスワード、BIOS 管理パスワード、に注目ください。

※ 処理過程でエラーが発生した場合は、DtpBiosChk_*pcname*.log ファイルに出力されたエラー概要を参照の上、対処してください。

4.監査結果ファイルの内容

監査結果 DtpBiosChk_*pcname*.log の出力内容を例に沿って説明します。
(この PC の場合、PC 名:"FMV6100MG2" なので 監査結果ファイルのファイル名は DtpBiosChk_FMV6100MG2.log になります)

```
2006/07/31 09:12:34
PC 情報
  PC 名      : [FMV6100MG2]
  OS         : [Windows XP SP2]
  メーカ名 : [FUJITSU]
  モデル名 : [FMV2MG6L3]
  S/N        : [R9999999]
BIOS 情報
  Version : [FUJ    - 1030000]
  製造者  : [Phoenix/FUJITSU]
  BIOS 名  : [PhoenixBIOS 4.0 Release 6.0     ]
  SMBIOS Version : [2.3]
  起動パスワード : [設定あり]
  管理パスワード : [設定なし]
```

※既にこのファイルが存在していた場合、その後ろに連結して出力(APPEND)されます。

・記録される各項目は以下の通りです。

No	項目	説明
1	監査日時	コマンド実行日時
PC 情報		
2	PC 名	OS 上のコンピュータ名, OS バージョン
3	OS	
4	メーカ名	WMI から参照される機種情報 (機種を特定するための情報)
5	モデル名	
6	S/N	

BIOS 情報		
7	Version	WMI から参照される BIOS 情報 (BIOS バージョンを特定するための情報)
8	製造者	
9	BIOS 名	
10	SMBIOS Version	
11	**起動パスワード**	PC 電源投入時にパスワード確認される設定になっているか "設定あり","設定なし","不明" で報告される　*1
12	**管理パスワード**	BIOS 管理画面を表示する際にパスワード確認される設定になっているか "設定あり","設定なし","不明" で報告される　*1

*1 ： **BIOS パスワード設定を変更する前/後の２回 当ツールを実行し**、この 2 項目が正しく監査できているか確認してください。詳細については「５.留意事項」を参照ください。
なお、１回目に "不明"と記録された場合は、２回目を起動する必要はありません。

もし、監査結果ファイルに以下のような "##ERROR.x ～" の記載があった場合、「3. ツール使用方法」の復帰値に示した環境異常が発生しています。エラーを対処の上、再度実行してください。

例１）

```
2006/07/30 20:08:51
PC 情報
  PC 名      : [FMV6100MG2]
  OS         : [Windows XP Professional Service Pack 2]
##ERROR.3 GetBiosInfo Insufficient memory.(-1)
```

例２）

```
2006/07/30 18:51:43
PC 情報
  PC 名      : [TRINITY]
  OS         : [WindowsNT Server 4.0 Service Pack 6]
##ERROR.4 GetBiosInfo Other errors.(-2)
```

また、監査結果ファイルの一部に 例３のような "<ERROR.??(???)>" と記録される場合があります。これはメーカ/機種依存な影響から その情報が参照できなかったケースです。 それ以外の情報については監査可能ですので、監査可能な情報の範囲で確認してください。

例３）

```
2006/07/31 09:12:34
PC 情報
  PC 名      : [FMV6100MG2]
  OS         : [Windows XP Professional Service Pack 2]
  メーカ名   : [FUJITSU]
  モデル名   : [FMV2MG6L3]
  S/N        : [R2609999]
```

```
BIOS 情報
  Version : [FUJ    - 1030000]
  製造者  : [<ERROR.1 (161)>]
  BIOS 名  : [PhoenixBIOS 4.0 Release 6.0     ]
  SMBIOS Version : [3.2]
  起動パスワード : [設定あり]
  管理パスワード : [設定なし]
```

５．留意事項

当ツールの性質上、メーカ/機種に依存して動作結果が違うことが予想されます。
特に、以下の点にご留意頂き、正しく情報取得できているのかをご確認ください。

a) SMBIOS から情報採取されているように見えるが、正しく採取されない機種があります。
具体的には、PC 起動時の BIOS 設定画面には 「起動パスワード：使用しない」と設定したのに、当ツールの結果には ″設定あり″ と記録される機種があります。
この事象が見られるのは、「BIOS 起動パスワード」と「BIOS 管理パスワード」の２項目です。
→ これを確認するには､PC の BIOS 設定画面の｢起動パスワード｣｢管理パスワード｣を ″使用する(Enable)″, ″使用しない(Disable)″ を切り替える前/後で当ツールを起動し、その２回の出力結果を比較して、BIOS 設定したように記録されているか否かを確認してください。

b) 「BIOS 起動パスワード」要求は、PC 電源断からの投入時だけ要求され、Windows 再起動では要求されない場合があります。
→ 「BIOS 起動パスワード」の設定確認をする際は、PC 電源断～PC 電源再投入 の操作を行ってください。
電源投入後に当ツールを起動する、この操作を BIOS パスワード設定変更前/後の２回実行することで正しく監査できます。

付録. 用語

用語	説明
WMI	″Windows Management Instrumentation″ の略。 Windows の管理基盤のインターフェイス。システム情報を監視/制御することが可能。 当ツールでは、この WMI インタフェースを使用して PC 情報,BIOS 情報を参照している。
SMBIOS	″System Management BIOS″ の略。 各 PC の BIOS 内のデータを外部から参照できるようにするための仕様。 1999 年頃から DistributedManagementTaskForce,Inc.(DMTF)という団体から仕様が公開された。Windows からも SMBIOS 情報を参照する機能が提供された。 最近の各社の PC には、この仕様に基づいた BIOS が搭載されるようになってきた。ただし全仕様が搭載されている訳ではなく、SMBIOS 情報のうちの ″BIOS パスワード設定状況″ の参照に対応している機種がまだ限られているのが実情である。 当ツールでは、この SMBIOS インタフェースを使用して″BIOS パスワード設定状況″ を参照している。