オフライン端末のセキュリティ検査方法

砂田　英之‡　山田　耕一‡　鷲尾　元太郎‡　中野　初美‡　近藤　誠一‡
三菱電機株式会社　情報技術総合研究所†

1．はじめに

近年、多くの企業では情報漏洩の対策として、セキュリティ施策の設定・運営を実施し、企業内で用いる端末が正しくパスワード設定されているか、ウイルス対策ソフトウェアがインストールされているかなどのセキュリティ検査を実施している。

これらのセキュリティ検査の作業は手順が複雑であり、作業時間も掛かることから検査および検査結果の収集を自動化することによって実施されることが多い[1]。しかし、社外に持ち出す端末など、通常オフラインにて利用する端末に対応できないといった課題があった。

この課題に対しては、既存技術として USB メモリを用いた収集方式[2]が提起されているが、セキュリティ施策として USB など外部記憶媒体を利用禁止としている場合に、検査結果の自動収集が行えないという課題が残っていた。

本論文では、これらの課題を解決するために、セキュリティ検査の結果を可読情報に変換することで、簡単かつ正確に集計する検査方式について提案する。

2．従来技術

(1)USB メモリを用いた収集方式

文献 2)では、オフライン端末に対するセキュリティ検査結果の収集方式として、図 1 の構成で、USB メモリを用いる方法が示されている。

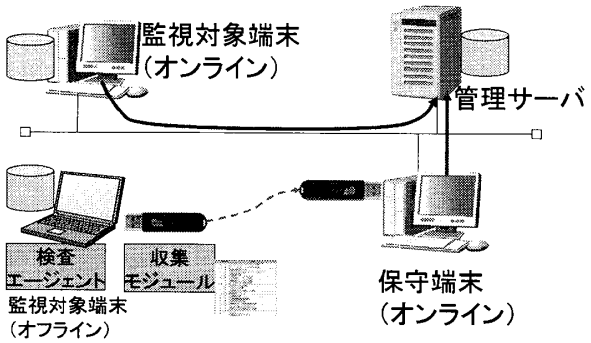

図1　システム構成（従来技術）

Method of Security Inspection for Off-line PC
† Information Technology R&D Center, Mitsubishi Electric Corporation

監視対象端末（オフライン）に検査エージェントを、USB メモリ内に収集モジュールを配置する。監視対象端末（オフライン）に USB メモリを挿入し、収集モジュールの自動起動・自動収集を行うことで、効率的にセキュリティ検査の結果が収集できる。

(2)課題

近年、企業内で利用する端末は、セキュリティ施策として、USB やフロッピーなど外部媒体への書き込みを禁止することで情報漏洩を図ることが多くなっており、USB メモリを用いた収集方法が適用できないことが課題となっている。

また、上記端末を手動で検査および結果の収集を行う場合には、作業負荷の問題や、誤操作・誤認識により不正確な検査結果が収集される場合があるなどの従来の課題が残っている。

3．解決策

(1)可読情報を介した収集方式

監視端末（オフライン）のセキュリティ検査結果を集計する方法として、図 2 の構成で、監視対象端末（オフライン）にインストールした検査エージェントの検査結果を可読情報に変換し、その結果を別端末に入力し、集計する方法が考えられる。

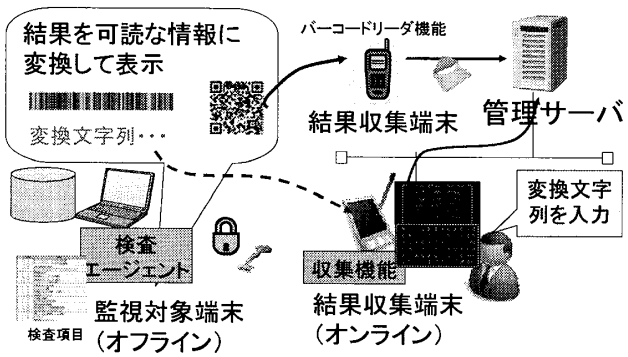

図2　システム構成（解決策）

可読情報には、文字列やバーコードといった方式が考えられ、収集機能の画面に検査エージェントが表示する変換文字列を入力する方式や、バーコードを読み取り、その結果を通知する方式などがある。

(2)実現方式

可読情報を介したセキュリティ結果の収集方式の機能構成を図3に示す。

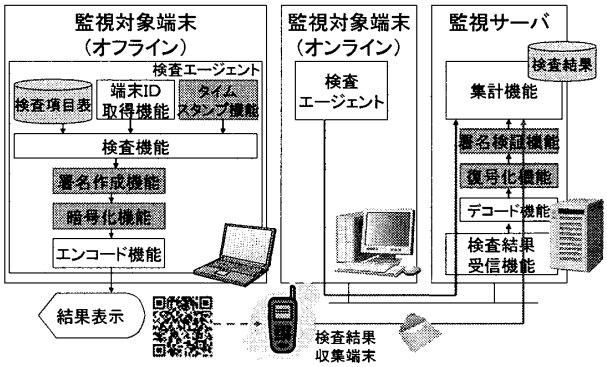

図3　機能構成

監視対象端末（オフライン）、監視対象端末（オンライン）、監視サーバから構成される。監視対象端末（オンライン）は、従来方式によりセキュリティ検査を実施する。

監視対象端末（オフライン）には、端末ID取得機能、タイムスタンプ機能、検査機能、署名作成機能、暗号化機能、エンコード機能を有する検査エージェントをセキュリティ検査の実施前にインストールしておく。

検査機能では、表1の内容に従って、端末のプロセス監視やファイル検索、設定情報の確認などを実施し、検査結果を収集する。

表1　検査項目表

グループID	グループ名	検査項目一覧	実施間隔
001	常時監視項目	使用禁止S／W Winny、・・・・	毎日12時
002	定期監視項目1	ウイルス対策ソフト、パスワード設定・・・	PC起動時
003	定期監視項目2	OSパッチ適用状況	毎月10日 10時
004	定期監視項目3	MS－Officeパッチ適用状況	毎月15日 17時

また、ホスト名、IPアドレス、MACアドレス、HDDシリアル番号などを端末IDとして取得する。検査実施時間からタイムスタンプを生成し、検査結果、端末IDと結合してエンコード機能に渡す。この際、改竄や結果の盗聴ができないように署名添付、暗号化を実施しても良い。

セキュリティ検査実施者からの検査結果の表示要求を受けて、エンコード機能では受け取った検査結果をBASE64、uuencodeなどの方式で可読な文字列に、またはQRコードなどのバーコードに変換する。セキュリティ検査実施者はエンコードされた文字列またはバーコードを結果収集用の端末に入力し、監視サーバと通信可能なLAN接続、または携帯などのメール送信により監視サーバに検査結果を送付する。

監視サーバは、集計機能、署名検証機能、復号化機能、デコード機能、検査結果受信機能から構成され、検査結果収集端末を経由して受信した検査結果を、デコード、復号、署名検証、タイムスタンプ検証を実施し、端末IDをキーとして検査結果の集計を実施する。

以上により、監視対象端末（オフライン）で検査エージェントが実施したセキュリティ検査の結果を監視サーバに収集することが可能となる。また、署名添付、タイムスタンプ添付により、検査結果の改竄や不正な検査結果を入力するのを防止することが可能となる。

4．評価

セキュリティ検査において、オフラインの監視対象端末の検査結果を簡単かつ正確に収集する方法が課題となっていた。従来技術ではUSBメモリを用いた収集方法が提示されていたが、USB禁止の端末に対応できないという問題があった。また、手動で収集する場合には、膨大な検査項目に対する結果を読み取り、入力し直す必要があり、作業負荷が高いことや、誤入力や改竄の危険性が問題となっていた。

弊社でも、約100項目の検査結果を手動で集計しており、入力処理に20分程度必要であった。また、入力ミスが発生することもあり、集計結果が必ずしも正しいとは言えなかった。

本方式を用いると、上記処理がQRコードを読み取り監視サーバに対してメール送信するといった1分程度の操作で完了し、入力ミスも発生しなく、利用者の作業負荷を低減するとともに、正確な結果を収集することが可能となった。

5．今後の課題

本論文にて、監視対象端末（オフライン）のセキュリティ検査を簡単かつ正確に実施する方法を示した。今後は、企業内のセキュリティ施策の見直しとともに必要な検査項目表の更新方法やタイムスタンプ／署名／暗号化に用いる鍵の管理方法について検討を進めるとともに、本方式の有効性の検証、および実用化に向けた開発を実施する予定である。

参考文献

[1] 坂田匡通、Webシステムにおけるセキュリティ検査手法の検討、情報処理学会2005年

[2]斉藤幸士、保守対象装置のログ情報収集システムと方法、情報サーバ、及びプログラム、特開2008-158862