



SPECTATOR Professional White Paper

目次

はじめに	2
内部セキュリティの脅威	3
ビジネスへの影響	4
IT スタッフの生産性の低下	4
監視と検出	6
内部的脅威の種類	6
修復	7
未然対策	7
SPECTATOR Professional の紹介	7
SPECTATOR Professional の特徴とメリット	8
ユーザ設定モジュール	10
スタートアップモニターとプロセスモニター	11
まとめ	12
PROMISEC について	12
ご連絡	12

はじめに

インターネットの誕生以来「セキュリティ対策」は多くの企業にとって最も重要な課題でした。

事業の収益性を高めるため、インターネットの「利便性」と「セキュリティ」を共存して高めることを目指しています。これまでは「セキュリティ」ソフト／ハードはファイアウォール、アンチウイルス、IDS/IPS、コンテンツ・フィルタリング、その他ゲートウェイ製品の様な境界に機器を使用し境界線を防御する事に注力を注いできました。

セキュリティを真剣に捕らえた企業は、完全な防御を実現するため、様々なベンダーから提供される製品を使って、境界線の防御を何重にも作る事になります。この多重防御法は、一つのセキュリティ機器をすり抜けた場合でも、別の予備的な機器で捕らえられるだろうという考えから導き出されたものです。しかし、管理者がセキュリティシステムを何重に積み重ねても、不満を持った従業員が会社の重要情報を大容量記憶装置（ディスクオンキーなど）にコピーし、それを競合他社に引き渡す様な物理的な行為を防止する事は出来ない。同様に外向けのゲートウェイセキュリティ製品は、内側でトロイの木馬に感染したPCに対して会社のLANに接続制御する事も出来ない。

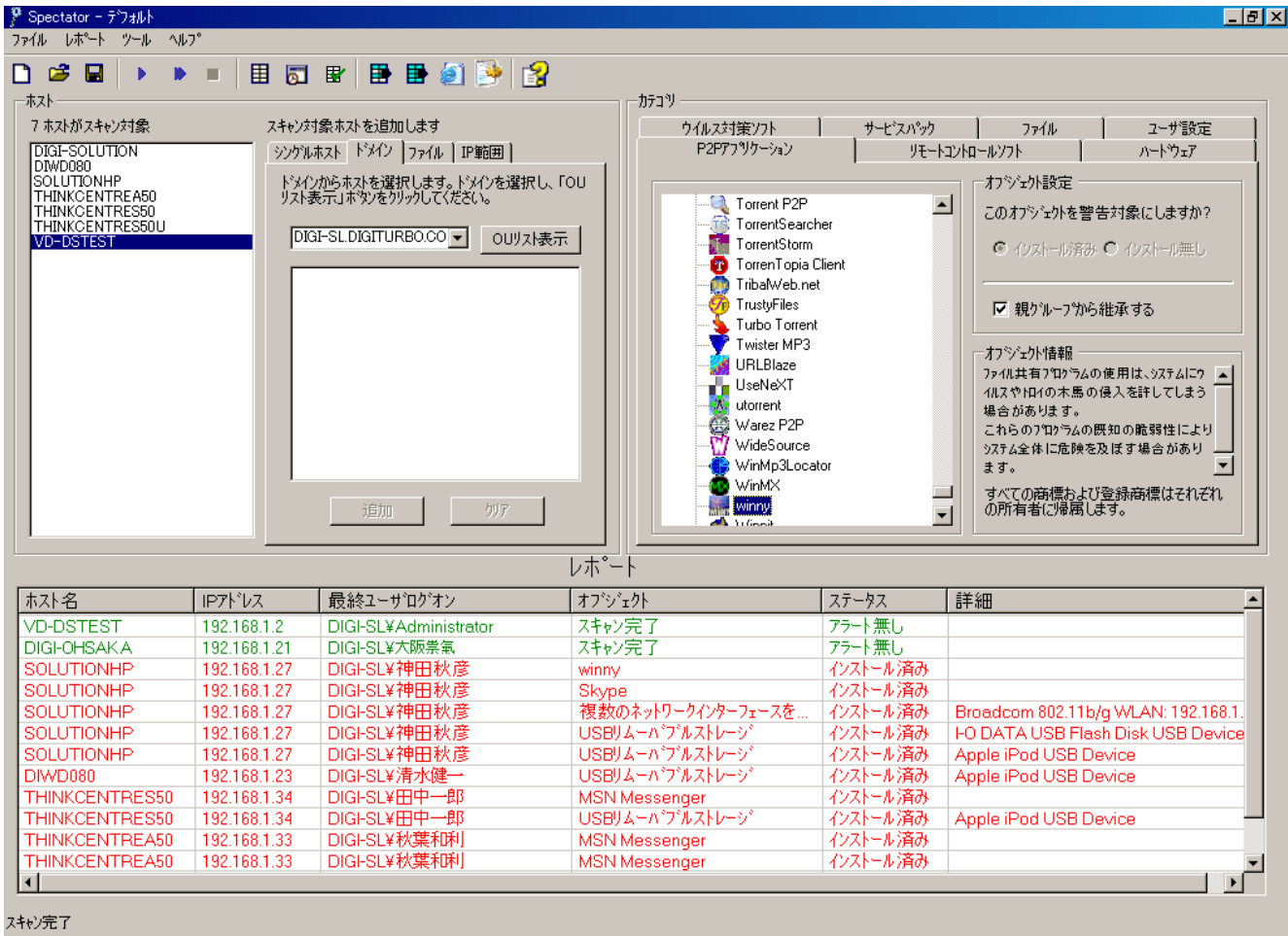
多くの企業が、企業内ネットワークに対してセキュリティ対策の不備に気づき、内部のセキュリティが脅威にさらされている事を改めて気づきます。これらの脅威は、既存のゲートウェイセキュリティ製品の全てをすり抜けて社内ネットワークの外から侵入する攻撃と同様に、企業に大きな脅威となるのです。たとえばガートナー・グループでは最近、会社のセキュリティ情報の違反行為の80%以上が社内から発生していると推定しています。

我々Promisec社は、企業内の防御をするため、統合的で簡単に使用出来る内部セキュリティソリューションが、企業にとって非常に重要である事を理解しています。このようなソリューションは、情報漏洩やネットワーク内部で発生する不正行為を防止し、ネットワークセキュリティの管理者にリアルタイムのセキュリティ情報を与えるものです。

Promisec社のSPECTATOR Professionalは、スタンドアロンのエージェントレス・ソリューションで、直感的なGUI(図1参照)を備えており、社内ネットワークのどこにでも配置させることができ、不正なハードウェアやソフトウェアの使用が発生しないように個々のエンドポイントとサーバを監視します。また同時にセキュリティ対策ソフトがアクティブに稼働しているかを確認します。SPECTATOR Professionalは、社内ネットワークのユーザから発生する、現在知られている脅威とその可能性のすべてに対処する強力なセキュリティ・ソリューションです。

社内ネットワークの脆弱性によって考えられる脅威、ダメージは重要情報の流出・紛失から、ネットワークのダウンまで様々です。また言うまでもなく、これは生産性の喪失や貴重なネットワークリソースの浪費に繋がるばかりか、企業に対する信用問題に発展し、企業の存続そのものへの脅威となりうるものです。以下の文書では内部セキュリティの問題とSPECTATOR Professionalがそれらを解決する方法について説明します。

図 1: Promisec SPECTATOR Professional の GUI



内部ネットワークの脅威

内部のネットワークに対する脅威として、通常は意図的または不注意などで PC がウイルスやスパイウェアなどの不正コードによる感染が発症となり、社内ネットワークにそのまま接続されたエンドポイントやサーバから不正コードが拡散し、その脅威を組織全体にわたって広げる可能性を持っています。これは、ユーザが悪意のあるコードが埋め込まれた不正 CD と知らずに PC で使用した時に発生する事もあります。悪意のあるコードとは短時間でユーザのパスワードを盗んでしまう単純なキーロガーから、秘密情報を連続的に社外に送信できるバックドア型のトロイの木馬まで様々です。具体的には、会社のラップトップは外回りの営業スタッフ等によって社内ネットワーク以外の様々なインフラで使われており、そこでは個々のユーザを保護するための十分なセキュリティが考慮されていない可能性があります。そのようなラップトップを会社に持ち帰り、再び社内ネットワークに接続すれば、境界のセキュリティ機器では問題があっても確認する事が出来ません。また考えられる危険性としては、有害な実行ファイルを含み、ネットワークにアップロードしてしまう P2P や、リモートアクセスソフトかも知れません。

一般的な例としては、セールスマンがオフィスに戻ってから PC と同期させるために自分の PDA を接続する場合があります。これは多くの危険なアプリケーションを自分の PC に取り込む恐れがあります。あるいは、その PDA に無線 LAN やモデム機能がある場合、データを組織の外に送信するために使われるかも知れま

せん。

この脅威のもうひとつの側面は意図的または無意識に関わらず、情報の盗難や漏洩です。企業の従業員は信頼されており、会社の最も重要な情報にアクセス可能ですが、同時に記憶媒体に簡単に複製でき、社外に持ち出す事が可能です。この種の違反は、会社に罰金や科料として多額の費用負担を強いる(この例は後述します)ほど重大で、事業継続に影響する事さえあります。リムーバブルストレージは、今や様々な形と大きさで出回っており、簡単に取り付けて非常に短時間で多くの情報を記録出来ます。二次ネットワークインターフェースを持つコンピュータは、外部のネットワークに接続可能で、見ず知らずのネットワークから会社のネットワークへのアクセス経路を作り出し、不正なユーザによるアクセスを可能にしています。

ステイクホルダへの影響

企業内部で脅威とされるポイントは、知的財産、顧客個人のデータ、価格表、その他占有情報等の秘密情報へ不正アクセスを試みる等、様々考えられます。個人情報保護法の遵守で、データを暗号化し、解析されなくなったとしても、不正行為は企業の競争力を失わせる事に繋がります。

一般顧客と取引している企業にとっては、顧客の信頼と市場の評判を失うことは顧客との関係を大きく傷つけ、会社に対する信頼を失わせる事は、後に会社の株価にも影響するでしょう。

生産性の低下

社内にマルウェアがあると、従業員のシステム管理に責任を負う IT スタッフに負担を与え、結果的に生産性も低下します。たとえばデル・コンピュータは、顧客から技術サポートへの問い合わせ電話のうち、12%以上がスパイウェア関連であるといえます (Information Week, 2004)。更に法施行により企業は、情報セキュリティ対策の問題から個人情報漏れた場合、金銭的な責任を負う事になります。

次に情報セキュリティ対策の違反によって、企業が実際に金銭的な責任を負った事例を示します。

- 2004年4月に Barnesandnoble.com はニューヨーク検事局と、オンライン書店の顧客の個人情報漏洩した結果、インターネットセキュリティの違反に対する罰金として US\$60,000 を支払い、その違反を修復すると誓約しました (Computer World, 2004)。

スペイン情報保護局が関連会社と顧客情報を不適切に共有していた企業に対して 840,000 ユーロ(約 US\$900,000)の罰金を課したことと、保護されている個人情報を公開したことに対して 108 万ユーロ(約 US\$117 万)を課したことは企業に対する国際的なペナルティの例です (Morrison & Forester LLP, 2004)。

- 台湾財務省は 2003 年 11 月に Citibank のオンラインクレジットカード機構のセキュリティがハッカーによって破られたことに対して、新規のクレジットカードの発行を 1 ヶ月停止するよう命じました。またオンラインバンキングサービスも 3 ヶ月間停止を命じられ、サービスを再開する前に財務省のセキュリティ検査を

受けることを義務付けられました(Taipei Times, 2004)。

- 日本の三井住友銀行のロンドン支店は銀行のシステムに不正にインストールしたキーロガーソフトウェアを使った巧妙なハッカーグループによって、世界中の個人口座に何百万ドルもの資金を送金するための認証証明書を危うく引き出されるところでした(IT Observer, 22 March 2005)。
- モンタナ州では顧客データが漏洩した場合にそれを公表しなかった違反に対して、1 件当たり US\$10,000 以下の罰金を課す事に(Cutter Consortium, 2004)。

上記の例で示されている様に、セキュリティの違反から信用を回復する事は、企業にとって莫大な費用が掛かります。特にプライバシーとセキュリティの規制を受ける企業は、これらの脅威にどう対策するかを考えなければなりません。これは企業には社内ネットワーク全体を監視する能力が必要なだけでなく、検出した問題に対処できる修復ツールと、各エンドポイントの適合性を維持する未然対策ツールの両方を組み入れる必要があるという事です。図2は、上記脅威に対策するための SPECTATOR Professional のモジュール構成と、検出から対策まで、最適な対策をする能力が示されています。

図 2: Promisec SPECTATOR Professional のコンポーネント

管理プラットフォーム	SPECTATOR Reporter				
出力	データ収集とフィルタリング				
監査基準	不正 アプリケーション	アプリケーション 監視	不正接続	不正 ハードウェア	ユーザ設定 (カスタマイズ)
SPECTATOR モジュール	検出エンジン		未然対策エンジン	修復エンジン	
SPECTATOR コア	監査エンジン				

監視と検出

監視作業は、総合的内部セキュリティシステムの主要機能です。これは社内のすべてのエンドポイントとサーバ上の脅威を検出し、セキュリティの違反が発生したらセキュリティ管理者に警告を発する能力をもっていなければなりません。以下のリストは社内ネットワークの内部に存在していても境界セキュリティソリューションでは必ずしも違反を検出できない脅威を示しています。

内部脅威の種類

- **ネットワークへの接続機器** — 不正な無線 LAN(AP)機器やモバイルモデムは、ネットワークへ簡単に接続でき、境界の防御を完全に無力化します。これには不正なラップトップを社内ネットワークに接続することも含まれます。
- **P2Pアプリケーション** — Winny、Kazaa、ICQ、Skype や、その他のファイル共有プログラムやチャットプログラム(ゲートウェイ製品ではその使用を防止できない)は、ウイルスやスパイウェアの恰好の侵入経路となり、社内ネットワークをデータ漏洩とウイルス攻撃の危険にさらします。ゲートウェイ製品の中には(Firewall や IDS 機器等)、いくつか既存 P2P アプリケーションをブロック出来るものもありますが、全てをブロックする事は出来ず、特に新しいベンダーのアプリケーションや暗号化を使用したアプリケーション、あるいは通常の P2P の様な動きをしないものは対策不可能です。
- **リモートアクセスプログラムの不正使用** — Dameware、GoToMyPC、PCAnywhere などのリモートアクセスプログラムは、社内ネットワークと外のコンピュータのセッションを開く事があり、重要情報の漏えいを許してしまいます。多くの企業では特定のユーザにこれらのアプリケーションの使用を許可していますが、その様なスタッフの行動を追跡し、社内ネットワークを開放したままにしておかないためには、誰がその様なアプリケーションの使用を許可されているかを明確に定義する事が重要です。
- **大容量記憶装置の不正使用** — ディスクオンキー、PDA、USB メモリ、ポータブル音楽プレイヤーの様な外付の記憶装置は、社内に有害なデータを容易に持ち込むことになり、会社をウイルス攻撃の危険にさらします。さらにこのタイプのハードウェアの不正使用は、大量のデータを短時間でメディアに転送し、社外へ簡単に持ち出してしまう恐れもあり、権限を持たない人物による、秘密データの持ち出しを可能にします。
- **業務に不必要なファイルの持込** — 動画、静止画、音楽ファイル等をインターネットやP2Pソフトウェア等を使って入手する行為が発生する場合、興味をひくファイル名に騙され、予め埋め込まれているマルウェアを実行させてしまう可能性があります。このタイプのマルウェアは瞬く間に、社内ネットワーク全

般に蔓延し被害をもたらす恐れがあります。

これらは、社内ネットワークに脆弱性を生んでしまう脅威の一例に過ぎません。前述のような脅威が発見された場合には、会社のシステムは何をしなければならないかをしっかりと把握し、確認してダメージから防御しなければなりません。また同時に未然対策も必須となります。この様に総括的なソリューションは、様々な脅威に対し、どの様に未然対策するかを考慮したものでなければなりません。

修復

これまで解説した問題に対するソリューションは、まずは自身の安全を確保し、あるいはネットワーク上で他のセキュリティ機器が確認した異常を修復し、不正処理を終了させる能力がなければなりません。これにはレジストリ値の変更を修復し、さらに正しいレジストリ値を定義してその値を維持する能力を持っていないとできません(ただしこれに限定されない)。これに加えて、ウイルス対策ソフトがインストールし、正常作動している事、必要な全てのパッチやサービスパックが最新の状態で適用されている事、また特定のアプリケーションが正しいバージョンで作動している事を監視するため、各エンドポイントにセキュリティポリシーを執行出来るものでなければなりません。

未然対策

企業は、各 PC 全てがセキュリティポリシーに対応して未然対策する必要があります。エージェント型のソリューションは、個別で見つかった問題を物理的に修復する必要があるため、情報システム部門、セキュリティスタッフの貴重な時間と労力を費やします。セキュリティ問題が発生する前に対処出来る、未然対策ツールを持ったソリューションは、セキュリティ対策に掛かる経費は大幅に低減されます。

未然対策とは、セキュリティ管理者がネットワークのエンドポイントに接続する全ての周辺機器を制限し、コントロール出来るという事です。例として次の様なものがあります。

- 記憶装置 — USB フラッシュメモリ、外付 HDD
- 通信機器 — PCI モデム、外付 NIC/PHS モデム、Wi-Fi 機器
- 記憶媒体 — FDD、CD/DVD、マルチメディアカード

SPECTATOR Professional の紹介 ~ エージェントレスのエンドポイントセキュリティ ~

SPECTATOR Professional は、セキュリティ管理者が革命的な特許出願技術を使って、社内ネットワーク上にある各 PC とサーバに対し、強力なセキュリティ対策を簡単に運用管理出来るエージェントレスのソリューションを企業に提供します。このソフトウェアは 1 日 24 時間またはあらかじめ決められたスケジュールに従って、あるいは必要時にスポットでクライアント側のソフトウェア(エージェントやアプレット)を必要とせず、内部監査する様、設計されています。

この「エージェントレスタイプ」のエンドポイント・セキュリティ ソリューションは、セキュリティ管理者が企業

内のクライアントとサーバ全てに対して、セキュリティポリシーのコンプライアンスを運用管理するため、つまり容易な業務処理統制の実現を提供します。エージェントレスであることは、クライアントを使用する類似のソリューション商材に比べ、マシン上でのソフトウェア同士の衝突問題がない事は、SPECTATOR Professional にとって非常に大きなアドバンテージとなります。このため企業は、これらのエージェントを管理し、サポートするためのスタッフを確保、維持しておく必要がなく、またエージェントが非アクティブになり、停止状態に陥っていないか？や、正常稼動している事をチェックする必要も全くありません。加えて、エージェント導入型のソリューションは、通常ハードウェアをコントロールする内部（エンドポイント）セキュリティの側面しか取り扱いませんが、SPECTATOR Professional は内部的な脅威のすべての範囲に対する網羅性のあるソリューションを実現し、またエンドポイント上で展開しているエージェントが実際に正しく作動していて、不正が行われていない事も確認できます。

従ってクライアント導入型のソリューションが持つ問題と欠点、エージェントレスソリューションでは大きなものも些細なものも、財務的なものも含め、全て開放されるソリューションと言えます。セキュリティソリューションの導入と（特に販売の後で）、日常のメンテナンスに伴う費用はソリューションのコスト計算には考慮しない企業もあります。さらに SPECTATOR Professional は、導入する上で追加のハードウェアなど設備を必要とせず、またネットワークのどの地点からでも、ネットワークやモニタリングするマシンに大きな負担を掛けずに作動する様、設定できます。これら2つの特徴だけでも、SPECTATOR Professional は TCO と高い ROI を持った費用対効果の高いソリューションとなります。

SPECTATOR Professional のエージェントレス・エンドポイントセキュリティは、従業員、下請業者、コンサルタント等が社内ネットワークリソースを使用する環境下で、誰に対しても高いレベルの信頼を維持する能力を企業に提供しており、たとえ意図的にセキュリティの違反や会社のネットワークに対して脆弱性を許しません。境界線上のセキュリティソリューションが、社外のパートナーや関連企業と安全に信頼のある取引が出来るように、SPECTATOR Professional は会社のネットワーク内で作業する内部ユーザに対して、シームレスにポリシーコンプライアンスを遵守させる仕組みを容易に提供します。

SPECTATOR Professional の特徴とメリット

- すべてのエンドポイントとサーバを対象としたセキュリティ管理を提供
- ゲートウェイのセキュリティソリューション等、組み合わせが用意
- 導入が簡単ですばやく、ネットワークの構成を変更する必要がない
- ホスト 1 台あたり 1~3 秒というすばやいチェック機能
- サーバ、DB など専用ハードウェアが不要
- シンプルで直感的に使いやすい GUI とレポート機能
- I/O 機器の挿入と使用を完全にコントロール
- 不正なソフトのインストールと使用を完全にコントロール
- 脅威の可能性を網羅した総合的なデータベース

- 柔軟性 – 検査する特定の脅威をユニークにユーザ設定可能
- 使用許可済の機器とアプリケーションのホワイトリスト搭載
- 24 時間連続運用作動、内部監査でスポット作動、定時作動をカスタマイズ可能
- セキュリティポリシーの遵守とイベントログの追跡
- リモート修復機能を持ったコンソール
- エージェントレス技術、– ユーザに対する高い透明性: 追加経費が不要

SPECTATOR Professional の豊富な機能(検出、修復、未然対策および適合性の監視)は、複数のポイント製品を使わなければ実現できなかった内部セキュリティのさまざまな側面をカバー出来る事を意味しています。これはエンドポイントやサーバから発生して、社内ネットワークの内部で問題を引き起こす脅威全体に対応する多様性のあるエージェントレスのセキュリティアプリケーションです。

例えば PC のスイッチを入れたときに悪意のあるプログラムを起動してしまうと、境界線上の防御システムでは検出できません。SPECTATOR Professional は、異常な現象が発生しないかどうかを確認するために PC のスタートアップを監視する事で、このタイプの脅威を検出し、もし異常があればそれがネットワーク内のほかのシステムへの脅威となる前に処理を終了させる事が出来ます。同様に、ダウンロードやその他の方法で持ち込まれた未知の実行ファイルが PC で稼動していた場合、それが有害なものかどうかに関わらず、SPECTATOR Professional は認識して、必要な場合は強制終了します。

マシン上で起動している悪意のあるコードやネットワークに作られた不正なアクセスポイント(AP)などが関係する脅威を除去する事に加えて、SPECTATOR Professional は、ネットワーク内の PC とサーバ上にある必要なプログラムやポリシー定義が最新のものであるかを確認します。攻撃を防ぐためにセキュリティ管理者は、組織内の全ての PC とサーバに最新のサービスパックやパッチプログラムやアンチウイルスプログラムがインストールされている事を確認する様に、モニター機能を設定する事が出来ます。こうしておく、何か問題が発生した場合、セキュリティ管理者にアラートします。下の図 3 は SPECTATOR Professional のレポートモジュールの例で、詳細な情報を表示可能です。これは勤勉さを実証し、また従業員の行動を確認する必要のある、多くの企業にとって不可欠のものです。

図 3: リポートモジュール

ホスト名	IPアドレス	アプリケーション	ログオン中のユーザ	ステータス	補足情報
192.168.2.47	192.168.2.47	Cannot Connect to Host		ホストをスキャンすることに失敗	Unknown Reason
DIWIN006	192.168.2.35	Modem	DIWIN006#iwama	未修正のアートがあります	Honda Electron AH-H403C
DIWIN006	192.168.2.35	MSN	DIWIN006#iwama	修正されました	The process "MSNMGR" found and was eliminated
DIWIN006	192.168.2.35	Microsoft Office	DIWIN006#iwama	未修正のアートがあります	Microsoft Office Standard Edition 2003
DIWIN006	192.168.2.35	SKYPE	DIWIN006#iwama	修正されました	The process "SKYPE" found and was eliminated
DIWIN006	192.168.2.35	More Than One Netw...	DIWIN006#iwama	修正されました	Realtek RTL8139/810x Family Fast Ethernet NIC: 172.16.2.247
DIWIN006	192.168.2.35	MSN Messenger	DIWIN006#iwama	未修正のアートがあります	
DIWIN006	192.168.2.35	USB Removable Storage	DIWIN006#iwama	未修正のアートがあります	I28MB USB2.0FlashDrive USB Device
DIWIN006	192.168.2.35	More Than One Netw...	DIWIN006#iwama	未修正のアートがあります	Intel(R) PRO/Wireless 2915ABG Network Connection: 192.168.0.7
DIWIN006	192.168.2.35	Skype	DIWIN006#iwama	未修正のアートがあります	
DIWIN006	192.168.2.35	Messenger	DIWIN006#iwama	未修正のアートがあります	停止中
DIWIN006	192.168.2.35	Remote Desktop Help...	DIWIN006#iwama	未修正のアートがあります	停止中
DIWIN006	192.168.2.35	USB Removable Storage	DIWIN006#iwama	未修正のアートがあります	DMNA RIO Audio Player USB Device
DIWIN006	192.168.2.35	Adobe	DIWIN006#iwama	未修正のアートがあります	Adobe Reader 7.0.5 - Japanese
DIWIN006	192.168.2.35	Microsoft Office	DIWIN006#iwama	修正されました	Microsoft Office 2000 3x1 Personal
DIWIN006	192.168.2.35	notepad	DIWIN006#iwama	修正されました	The process "NOTEPAD" found and was eliminated
DIWIN006	192.168.2.35	Anti Virus	DIWIN006#iwama	修正されました	Anti Virus is not installed on the host
DIWIN006	192.168.2.35	Windows XP Service P...	DIWIN006#iwama	修正されました	Service Pack 2 Installed
DIWIN006	192.168.2.35	More Than One Netw...	DIWIN006#iwama	修正されました	Realtek RTL8139/810x Family Fast Ethernet NIC: 192.168.2.35
DIWIN006	192.168.2.35	Windows XP with any ...	DIWIN006#iwama	修正されました	Service Pack 2 Installed
DIWIN006	192.168.2.35	Modem	DIWIN006#iwama	未修正のアートがあります	Honda Electron AH-H407P
DIWIN006	192.168.2.35	Modem	DIWIN006#iwama	未修正のアートがあります	Panasonic V.92 MDC Modem
DIWIN006	192.168.2.35	More Than One Netw...	DIWIN006#iwama	未修正のアートがあります	Realtek RTL8139/810x Family Fast Ethernet NIC: 172.16.2.171
DIWIN006	192.168.2.35	USB Removable Storage	DIWIN006#iwama	未修正のアートがあります	HAGIWARA UD-RAM USB Device
192.168.2.1	192.168.2.1	Cannot Connect to Host		ホストをスキャンすることに失敗	Unknown Reason
192.168.2.45	192.168.2.45	Cannot Connect to Host		ホストをスキャンすることに失敗	Access Denied
192.168.2.44	192.168.2.44	Cannot Connect to Host		ホストをスキャンすることに失敗	Unknown Reason
192.168.2.36	192.168.2.36	Cannot Connect to Host		ホストをスキャンすることに失敗	Access Denied

検索情報:
 検出範囲:
 14/02/2006 12:24:31
 14/02/2006 12:24:37-03/03/2006 23:11:57
 表示時間:
 表示日付:
 最終ユーザログオン:
 詳細:

カスケード 自動ホストモード

スキャン開始日: 03/03/2006 11:09 午後
 スキャン終了日: 03/03/2006 11:09 午後
 実行

リフレッシュ 保存 セットアップ 最小化 About 終了

ユーザ設定モジュール

ユーザ設定モジュールは、各 PC やサーバがポリシーコンプライアンスを遵守していて、企業のポリシーにも従っており、そのポリシーが社内ネットワーク全体で実施されている事を確認するためにカスタマイズ出来ます。ユーザ設定モジュールによって、ネットワークセキュリティ管理者は起動させなければならない、あるいは起動させてはならない特定のアプリケーションを見つけるための検査をカスタマイズ出来ます。これはインストールされているサービスをチェックして、その作動を許可するか禁止にするか、更に終了させるかを設定可能です。これはまたどの PC が特定のプログラムを作動しているかをチェックし、有害なプロセスを見つけ出す事や、不正なプロセスが実際に PC 上で作動しているかどうかを確認するように設定出来ます。またこれはユーザがリセット出来るレジストリ値にも適用可能です。SPECTATOR Professional は、レジストリ値が変更された場合、それを会社のポリシー（グループポリシーなど）に従って、元の設定値に確実に戻します。

ユーザ設定モジュールは、ポリシー適合性維持機能として、あるいは外部の監査法人に対する報告書作成用の監査ツールとして使用出来る便利なツールです。その上、ループスキャン（連続検査）の一環として使った場合には、レポートモジュールは各エンドポイントの行動履歴と、修復後にセキュリティ違反の再発生をしたかどうか、またその理由を提示する事が出来ます。これらのツールによって企業は完全な内部監

査を行い、また情報セキュリティ対策の活動が正しく行われている事を示す事が出来ます。

スタートアップモニターとプロセスモニター

ユーザ設定モジュールには、有害な処理やアプリケーションに対する更なる防御を付け加える 2 つの標準機能が含まれています。それはスタートアップモニターとプロセスモニターです。

スタートアップモニターは、以前には PC やサーバには存在しなかったトロイの木馬やその他のマルウェアを確認して、悪意のあるあらゆる処理を中止させます。これはプロセスモニターも同様です。それまで見られなかった新しいプロセスが PC やサーバに突然現れると、ネットワークセキュリティ管理者に警告が発せられて、そのプロセスを許可するかどうかを問い合わせます。セキュリティ管理者はそれによってとるべき適切な行動を判断出来ます。

SPECTATOR Professional とは異なり、他の内部セキュリティ製品はこの文書で説明した脅威のすべてに対応する能力はありません。ポリシーコンプライアンスに対応するという製品は PC 上で秘かに作動して秘密データを社外の何者かに送信するトロイの木馬のようなマルウェアを検出する事は出来ないでしょう。脆弱性を評価するツールは USB 記憶装置の不正使用を検出したりブロックしたりする事は出来ないかも知れません。さらに検疫ソリューション製品の多くは、マシン 1 台 1 台でエージェントやクライアントソフトを都度使う必要があり、セキュリティ管理者のための費用が増加し、また個々の PC やサーバでソフトウェアの衝突が発生する恐れがあります。

ゲートウェイソリューションを配置し、その投資を最大限に生かし、境界のすり抜けを防止できる総合的な内部ソリューションを実現するのは、Promisec 社の SPECTATOR Professional だけです。企業への脆弱性を生む可能性のある、防御されていないエンドポイントがひとつあるだけで、ゲートウェイのセキュリティに費やした多額の投資が無駄になってしまうのです。従ってゲートウェイで展開するファイアウォールやアンチウイルス、IDS/IPS ソリューションと一緒に SPECTATOR Professional を社内に展開することによってのみ、総合的なセキュリティ対策が実現出来るのです。

SPECTATOR Professional は次のような脅威に対処します。

- あらゆる種類の周辺機器の不正使用
- オンボードやその他の大容量記憶装置の不正使用
- 不正なアプリケーションや有害なプロセスの検出と修復
- エンドポイントとサーバの脆弱性を診断、内部監査
- スタートアップの異常検知
- セキュリティレベルの詳細な分析
- ポリシーコンプライアンス

まとめ

Promisec 社は、ファイアウォールや IPS システム等の境界セキュリティ機器を完全に補完し、重要データ

の社外流出を防止するために、特定の接続をブロックする緊急時の対応策を作るために、それらの機器と統合する(チェックポイント製品との統合については www.opsec.com を参照ください)事も可能なツールとして SPECTATOR Professional を提供しています。これは、エンドポイントやサーバから発生する内部セキュリティの脅威すべてに対処でき、それらの脅威に迅速に対応するために、必要なツールを兼ね備えた、業界唯一のエージェントレスソリューションです。

SPECTATOR Professional は、特殊なハードウェアに依存しない純粋なソフトウェア製品として、社内ネットワーク内で発生する可能性のある複数のセキュリティ問題に対応した、非常に費用対効果の高い、セキュリティソリューション製品です。SPECTATOR Professional は、専門知識を必要とせず、セキュリティの専門家はもちろん、IT に詳しくない人でも簡単に運用させる事が出来るため、IT セキュリティの専属人員を増員して、運用コストに負担を掛けません。

PROMISEC 社について

Promisec 社は、組織にとって最も重要な財産、つまり従業員に対する確かな信頼をもたらすセキュリティソフトウェアソリューションの開発と販売を行っています。常に稼働されている社内ネットワークのセキュリティソリューションは、脅威を検出して排除し、セキュリティポリシー推進効果を高め、重要情報の流出を防止します。

Promisec 社は、“エージェントレス”タイプでのエンドポイントセキュリティを運用管理出来るソフト開発のパイオニアとして、今後も企業にとって最も負担の少ない、エンドポイントソリューション分野のリーダーを目指しています。

Promisec 社は、フロリダ州ボカレイトンに事務所を持ち、またイスラエルに R&D センターを有しており、豊かな経験を持つ著名な個人投資家に支えられています。Promisec 社の経験豊富な経営チームはネットワークセキュリティ産業から幅広い実績をもたらします。同社の経営陣は全て、イスラエル軍のエリート IT 技術部隊出身であり、同時に CheckPoint 社、Aladdin 社、およびその他の先進企業で技術管理職を経験しています。これらの経営陣を中心に、経験豊富な専門技術チームを編成、そして一体となって創造的でスキルの高い、業界をリードする力を構成しています。

ご連絡先

SPECTATOR Professional 開発元: Promisec Ltd. <http://www.promisec.com>

※ご質問や詳しい情報は sales@spectator.jp までお問い合わせください。

日本代理店: 株式会社デジターボ ソリューション事業部 <http://www.digiturbo.co.jp/>

〒101-0021 東京都千代田区外神田 3-1-16 ダイドーリミテッドビル 5F

TEL: 03-5297-8585 FAX: 03-5297-8081