企業のエンドポイントセキュリティ

2012 年 7 月～ 9 月

Dennis Technology Labs
www.DennisTechnologyLabs.com

このレポートは、著名なセキュリティ会社から提供されているウイルス対策製品の有効性を比較することを目的としています。

製品はテスト期間中、実際に存在するインターネットの脅威にさらされました。これは、顧客の体験に近づくよう、極めて現実的な方法で行われました。

これらの結果は、ユーザーがいずれかの製品を使用していて、感染した Web サイトにアクセスした場合どうなるかを反映しています。

要約

- **テストした製品**
  - Kaspersky Endpoint Security for Windows
  - McAfee VirusScan、HIPs、SiteAdvisor
  - Microsoft System Center Endpoint Protection
  - Symantec Endpoint Protection
  - Trend Micro OfficeScan（トレンドマイクロ コーポレートエディション）および Intrusion Defense Firewall（脆弱性対策オプション）

- **エンタープライズレベルの組織ではさまざまな保護が可能です。**
  主要な国際的ベンダーが提供する製品は、使用された脅威のうち 80% から 99% を保護しました。最も有効性の高い製品はシマンテックと Kaspersky 社の製品で、最も有効性の低い製品は Microsoft 社の企業向けマルウェア対策製品でした。

- **レピュテーションに基づいた悪質なサイトのブロックは効果的なアプローチです。**
  初めからユーザーが悪質なサイトにアクセスできないようにする製品は、大きな優位性を獲得しました。マルウェアが被害者のコンピュータにダウンロードされなければ、マルウェア対策ソフトウェアは継続して発生する問題に直面することが少なくなります。

- **一部のマルウェア対策プログラムは、正当なソフトウェアの評価が厳しすぎます。**
  Microsoft 社の製品は、すべての正当なソフトウェアを適切に処理する唯一の製品でした。Symantec Endpoint Protection は 2 位で、2 つのアプリケーションのインストールに対して警告します。Trend Micro 社の製品が最も厳しく、1 つのプログラムに対して警告し、14 のプログラムをアクティブにブロックします。

- **どれが最良の製品か。**
  最も精度の高いプログラムは、このテストで最高に近いスコアを獲得した Symantec Endpoint Protection でした。AAA と評価された唯一の製品です。Kaspersky Endpoint Security for Windows は 2 位で、A と評価されました。McAfee 社の VirusScan、HIPs、SiteAdvisor モジュールの組み合わせは C と評価されました。

Simon Edwards、Dennis Technology Labs、2012 年 10 月 12 日

目次

ドキュメントバージョン 1.1。2012 年 10 月 17 日編集: テスト期間の日付と、Kaspersky Endpoint Security for Windows の誤検知の結果を 1 カ所修正。

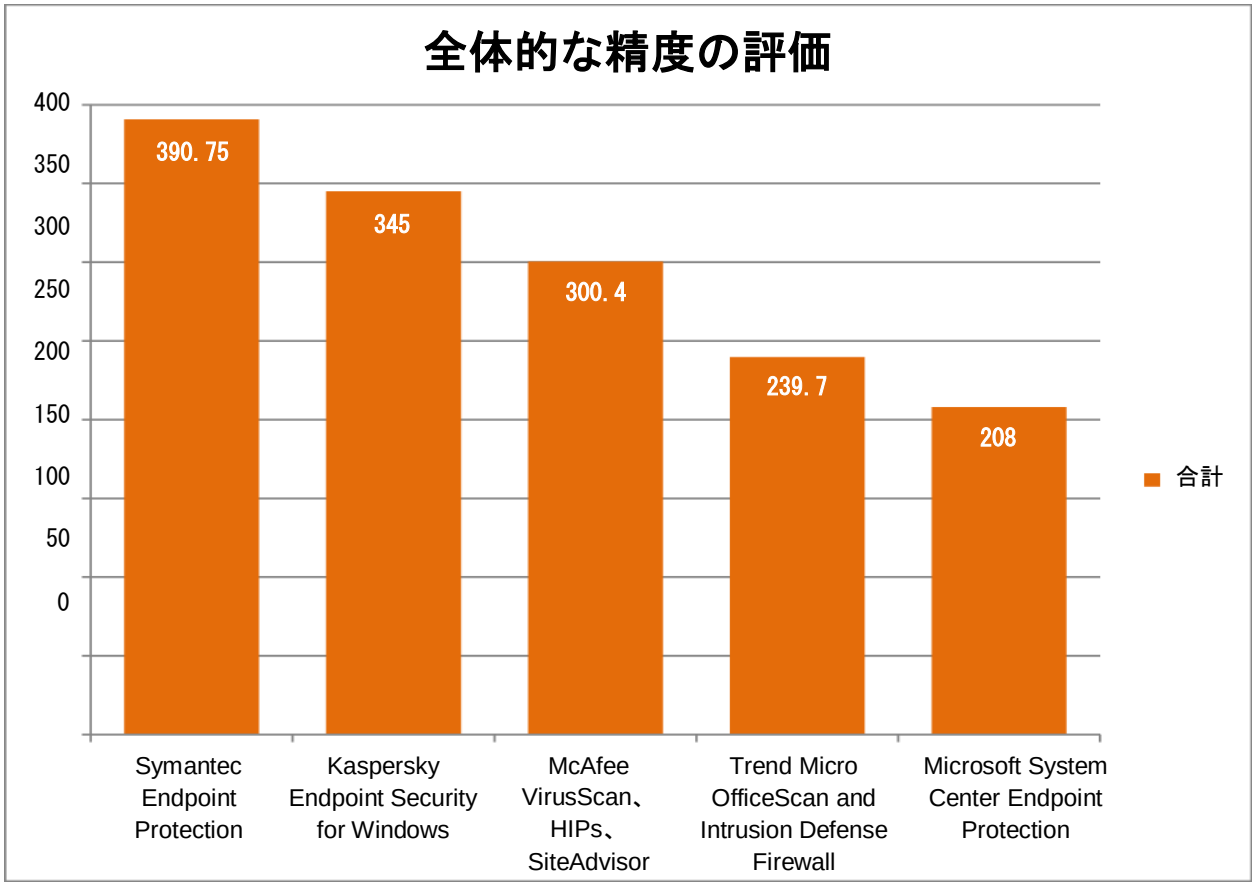
ドキュメントバージョン 1.2。10 月 18 日編集:シマンテックドットクラウドのデータを削除。誤検知の結果から SMB の表を削除。「保護の詳細」の SMB の表を正しい「企業別」の表に差し替え。

1. 全体的な精度の評価

全体的な精度の評価では、1 つのグラフで、セキュリティプログラム機能の有効性を判断できます。

マルウェア対策ソフトウェアは脅威を検出するだけであってはなりません。

正当なソフトウェアが邪魔されずに実行できるようにする必要もあります。以下に示す結果では、プログラムがどれだけ正確に脅威を処理し、正当なソフトウェアを処理したかを考慮に入れています。



全体的な精度の評価では、マルウェアと正当なアプリケーションでの成功と失敗が考慮されます。

2 つの異なったテストを実行しました。1 つはソフトウェアがインターネットの脅威をどのように処理したかを測定し、もう 1 つは正当なプログラムをどのように処理したかを測定しました。

脅威はすべてブロックし、正当なアプリケーションの実行はすべて許可するのが理想的な製品です。

製品がシステムを脅威に対して保護できなかった場合、危殆化されます。

正当なソフトウェアに対して警告を発した、またはブロックした場合、「誤検知」結果を生成します。製品が正常に脅威を停止した場合やユーザーが正当なソフトウェアをインストールおよび実行できた場合にポイントが加算されます。製品が脅威を停止できなかった場合や正当なファイルを誤って処理した場合にポイントが減らされます。

その後、各製品は、「脅威」と「正当なソフトウェア」の各テストにおけるパフォーマンスに基づいて、最終的な評価を受けます。

次の結果は、脅威のあるソフトウェアと悪質でないソフトウェアの両方での各製品のパフォーマンスを考慮に入れて、まとめた精度の評価を示しています。

最高が 400 点、最低が -1,000 点です。

詳細な結果と誤検知評価の計算方法については 9 ページの「5. 誤検知」を参照してください。

全体的な精度の評価

製品	全体的な精度の評価
Symantec Endpoint Protection	390.75
Kaspersky Endpoint Security for Windows	345
McAfee VirusScan、HIPs、SiteAdvisor	300.4
Trend Micro OfficeScan and Intrusion Defense Firewall	239.7
Microsoft System Center Endpoint Protection	208

■ **受賞歴**

以下の製品は Dennis Technology Labs 社による賞を受賞しています。

Symantec Endpoint Protection

Kaspersky Endpoint Security for Windows

McAfee VirusScan、HIPs、SiteAdvisor

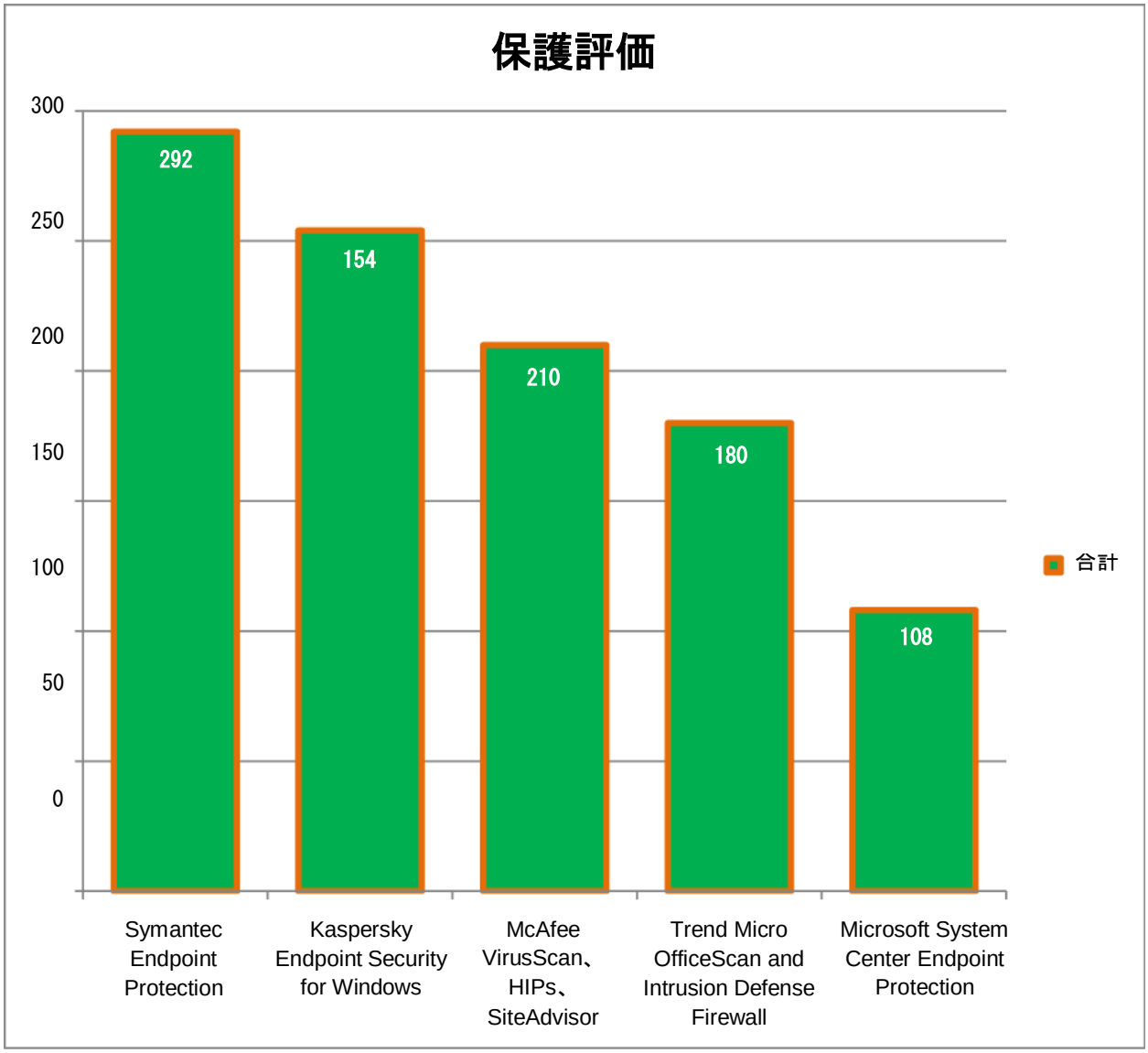
2. 保護評価

次の結果は、各製品がマルウェアの検出と処理の正確性のみにおいて獲得したスコアを示しています。誤検知は考慮されていません。

脅威を防御する場合は 3 点、無効化する場合は 1 点を加算し、製品が危殆化されることを許してしまった場合は 5 点減らしました。最高が 300 点、最低が -500 点です。

このスコアの重み付けの理由は、マルウェアにシステムを改ざんするどのような機会も与えない製品を評価し、感染を防ぐことができない製品に重いペナルティを課すためです。

危殆化のペナルティを重くしたり軽くしたりする必要があると思われる場合は、独自の重み付けを適用することができます。その場合は、8 ページの「4. 保護の詳細」にある結果を使用してください。



保護評価では、脅威を完全にブロックした場合に追加ポイントを加算し、脅威により危殆化された場合にポイントを減らします。

危殆化されたシステムは不安定になるか、専門家の知識なしでは使用できなくなる恐れがかなりあります。アクティブなマルウェアが削除された場合でも、損害を受けたシステムは危殆化されたものと見なしてカウントしました。

評価の計算方法

Symantec Endpoint Protection は 100 の脅威のうち 99 を防御しました。1 回の防御につき 3 点ずつ獲得(3x99)し、合計 297 点になりました。1 回危殆化されたため(1x-5)、5 点失い、小計は 292 点になりました。

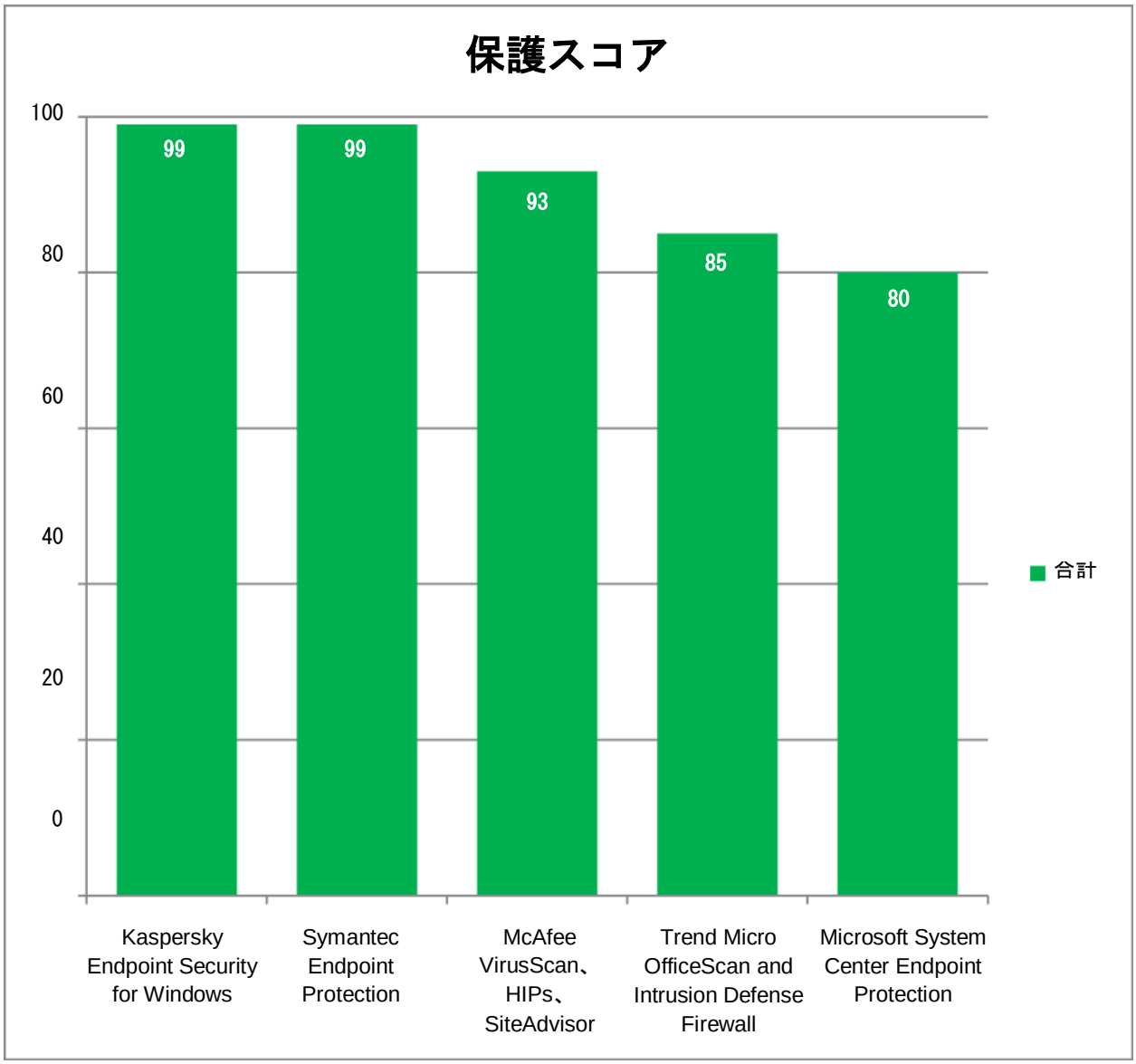
Kaspersky Endpoint Security for Windows は、80 回防御(3x80)した一方で、無効化した脅威は 19 で危殆化は 1 回のため、低いスコアでした。このスコアは次のように計算されます。(3x80) + (1x19) + (-5x1) = 254

保護評価

製品	全体的な精度の評価
Symantec Endpoint Protection	390.75
Kaspersky Endpoint Security for Windows	345
McAfee VirusScan、HIPs、SiteAdvisor	300.4
Trend Micro OfficeScan and Intrusion Defense Firewall	239.7
Microsoft System Center Endpoint Protection	208

3. 保護スコア

次のグラフは、防御された結果と無効化された結果をまとめて、保護の一般的なレベルを示したものです。



保護スコアは、各製品が脅威からシステムの危殆化を保護した回数を単純に示しています。

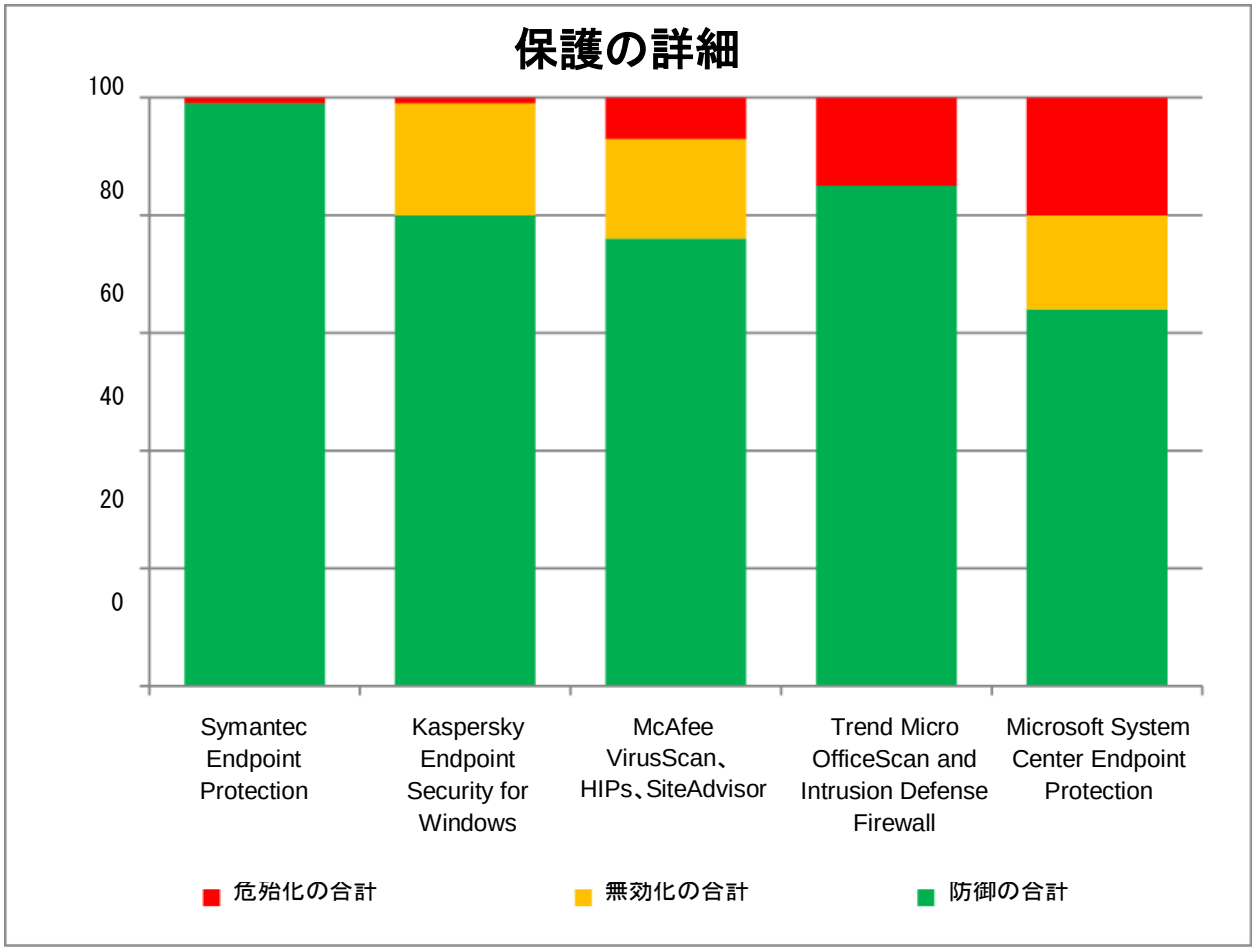
保護スコア

製品	保護スコア
Kaspersky Endpoint Security for Windows	99
Symantec Endpoint Protection	99
McAfee VirusScan、HIPs、SiteAdvisor	93
Trend Micro OfficeScan and Intrusion Defense Firewall	85
Microsoft System Center Endpoint Protection	80

（平均スコア: 91%）

4. 保護の詳細

セキュリティ製品はさまざまなレベルの保護を提供しました。製品は脅威を防御するとき、マルウェアが対象システム上に足場を得られないようにしました。脅威はシステムを悪用するか、システムに感染できる場合があり、場合によっては、悪用の実行後またはそれ以降に、製品がその脅威を無効化しました。無効化できなかった場合、システムは危殆化されました。



製品は、「防御」と「危殆化」の結果に基づいて、アルファベット順に並べられています。全体的な保護スコアについては、7 ページの「3. 保護スコア」を参照してください。

保護の詳細

製品	防御の合計	無効化の合計	危殆化の合計
Symantec Endpoint Protection	99	0	1
Kaspersky Endpoint Security for Windows	80	19	1
McAfee VirusScan、HIPs、SiteAdvisor	76	17	7
Trend Micro OfficeScan and Intrusion Defense Firewall	85	0	15
Microsoft System Center Endpoint Protection	64	16	20

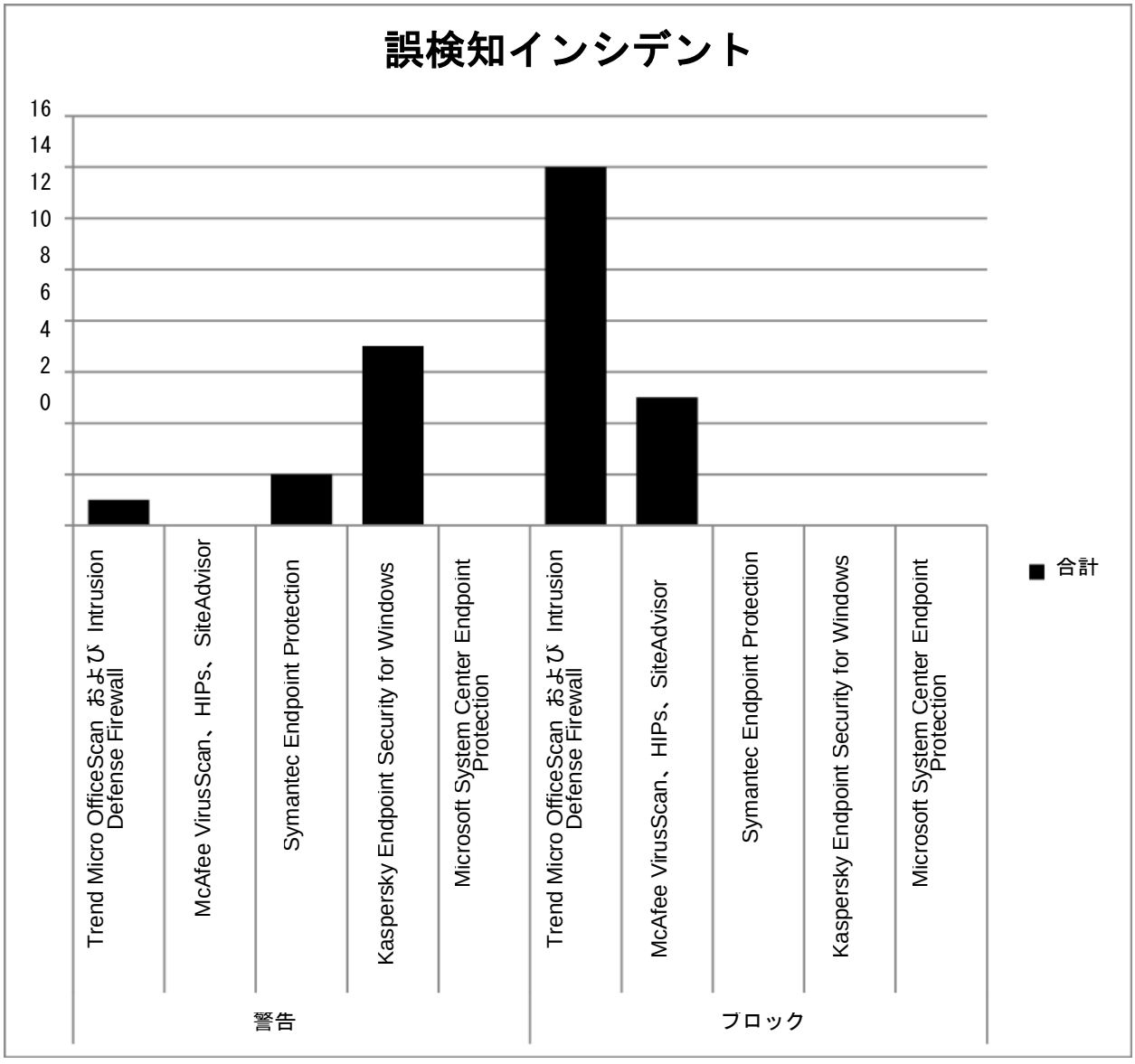
5. 誤検知

■ 5.1 誤検知インシデント

セキュリティ製品は脅威からシステムを防御できる必要がある一方で、正当なソフトウェアが適切に動作できるようにする必要もあります。正当なソフトウェアが誤って分類されると、誤検知が生じます。

テストする製品のほとんどが、正当なプログラムからシステムを保護しようとするとき 2 つの基本的な方法のうち 1 つを採用するため、テスト結果を 2 つの主要なグループに分けました。ソフトウェアが疑わしいことを警告するグループと、より明確な方法でそれをブロックするグループです。

正当なアプリケーションをブロックすることは、ユーザーを直接邪魔することになるため、警告を発行するよりも深刻です。



誤検知の発生時、製品は完全にブロックするよりも、プログラムのインストールや実行に対して警告する傾向がありました。

誤検知インシデント

誤検知のタイプ	製品	合計
警告	Trend Micro OfficeScan および Intrusion Defense Firewall McAfee VirusScan、HIPs、SiteAdvisor Symantec Endpoint Protection Kaspersky Endpoint Security for Windows Microsoft System Center Endpoint Protection	1 0 2 7 0
ブロック	Trend Micro OfficeScan および Intrusion Defense Firewall McAfee VirusScan、HIPs、SiteAdvisor Symantec Endpoint Protection Kaspersky Endpoint Security for Windows Microsoft System Center Endpoint Protection	14 5 0 0 0

■ 5.2 ファイルの普及度を考慮する

各ファイルの普及度は重要です。製品が一般的なファイルを誤って分類した場合、あまり一般的でないファイルの検出に失敗する場合よりも深刻な状況になります。つまり、通常、マルウェア対策プログラムはすべての正当なソフトウェアを誤って分類しないことが期待されています。

誤検知テスト用に選択したファイルを次の 5 つのグループに整理分類しました。非常に大きい影響、大きい影響、中程度の影響、小さい影響、ほとんど影響なしです。

これらのカテゴリは、テスト時点で Download.com などのサイトにより報告されたダウンロード数に基づいています。これらのカテゴリの範囲を次の表にまとめます。

誤検知と普及度のカテゴリ

影響カテゴリ	普及度（先週のダウンロード数）
非常に大きい影響	>20,000
大きい影響	1,000 - 20,000
中程度の影響	100 - 999
小さい影響	25 - 99
ほとんど影響なし	< 25

■ 5.3 スコアの修正

次のスコア修正因子を使って、影響の重み付けの精度スコアを作成しました。製品が正当な新しいプログラムのインストールと実行を許可するたびに、1 ポイント加算しました。誤検知を生じると、数ポイント（または数分の 1 ポイント）減らされます。次のスコア修正因子を使用しました。

誤検知と普及度 スコア修正因子

誤検知アクション	影響カテゴリ	スコア修正因子
ブロック	非常に大きい影響	-5
	大きい影響	-2
	中程度の影響	-1
	小さい影響	-0.5
	ほとんど影響なし	-0.1
警告	非常に大きい影響	-2.5
	大きい影響	-1
	中程度の影響	-0.5
	小さい影響	-0.25
	ほとんど影響なし	-0.05

■ 5.4 影響カテゴリの分布

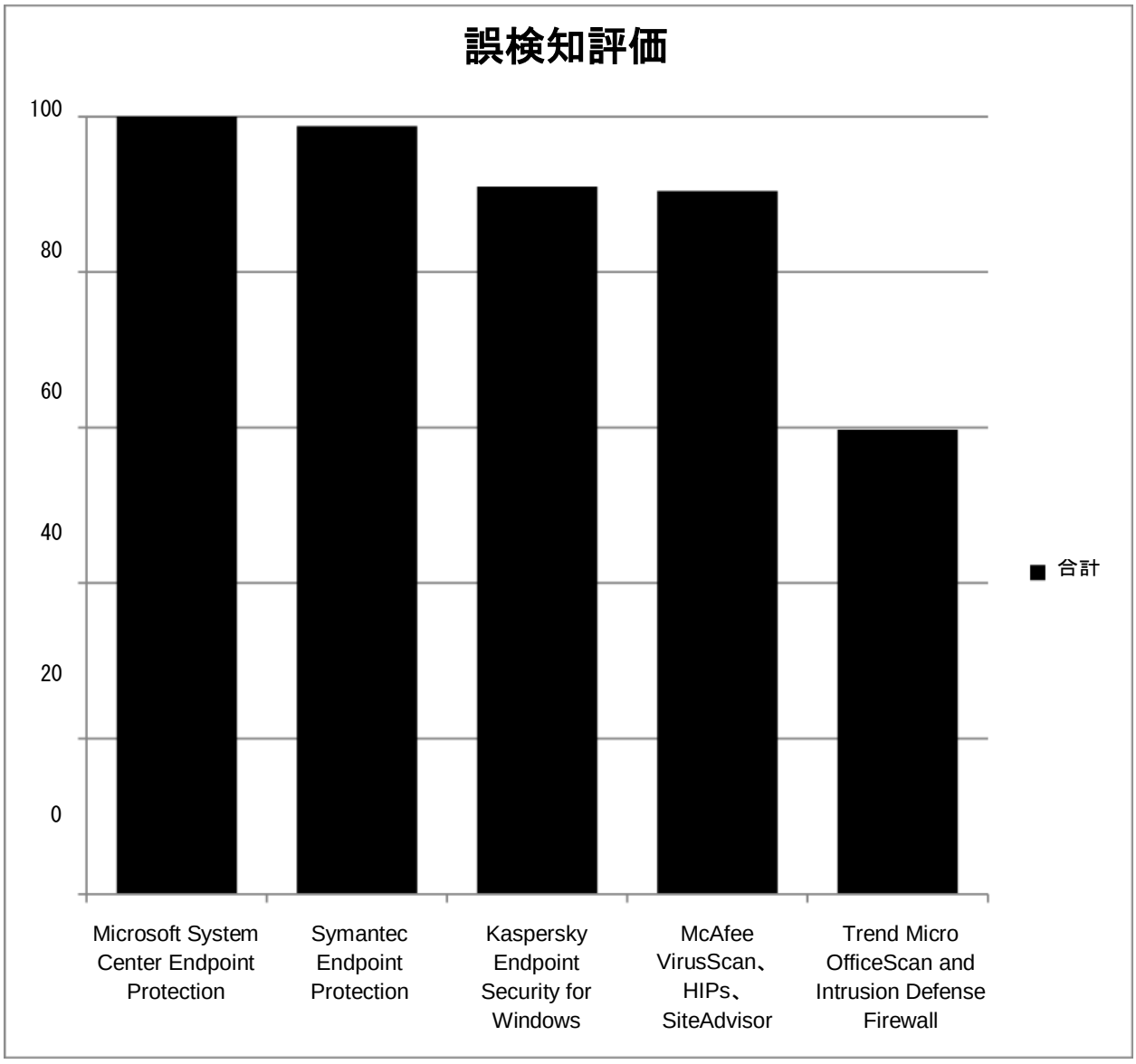
最も高いスコアを獲得した製品は、テストに使用した正当なアプリケーションを最も正確に処理しました。最高スコアは 100 点、最低スコアは -500 点です（すべてのアプリケーションが非常に大きい影響に分類され、ブロックされたと仮定した場合）。実際、影響カテゴリにおけるアプリケーションの分布は、非常に大きい影響だけに限定されません。下の表に、実際の分布を示します。

誤検知カテゴリと頻度

普及度評価	頻度
非常に大きい影響	17
大きい影響	17
中程度の影響	6
小さい影響	5
ほとんど影響なし	5

■ 5.5 誤検知評価

影響カテゴリと重み付けされたスコアを組み合わせることにより、次の誤検知の精度評価が作成されます。



普及しているプログラムを誤って分類した場合、普及度が低いファイルを検出した場合よりも厳しいペナルティが課せられました。

誤検知評価

製品	精度の評価
Microsoft System Center Endpoint Protection	100
Symantec Endpoint Protection	98.75
Kaspersky Endpoint Security for Windows	91
McAfee VirusScan、HIPs、SiteAdvisor	90.4
Trend Micro OfficeScan and Intrusion Defense Firewall	59.7

6. テスト

■ 6.1 脅威

ユーザーがインターネット上の脅威に遭遇したときに実際に起きることを把握するためには、現実的なユーザー体験を提供することが重要でした。

たとえば、これらのテストでは、Web ブラウザを使って、オリジナルの感染した Web サイトにアクセスすることにより、Web ベースのマルウェアにアクセスしました。CD や内部のテスト用 Web サイトからダウンロードしたのではありません。

対象となるすべてのシステムは完全に脅威にさらされました。これは、エクスプロイトコードの実行が許可されたことを意味します。他の悪質なファイルのように、インストールされたセキュリティソフトウェアによるチェックを前提に、実行され、その目的に沿うように実行が許可されました。

マルウェアが動作する機会として、最低 5 分間の時間が与えられました。

■6.2 テストラウンド

テストは数ラウンド実施されました。各ラウンドでは、特定の脅威に対する製品ごとの流出度を記録しました。たとえば、「ラウンド 1」では、各製品は、同一の悪質な Web サイトにさらされました。

各ラウンドの終わりに、テストシステムは完全にリセットされ、次のテストが始まる前にマルウェアの痕跡をすべて取り除きました。

■6.3 監視

対象システムの詳細なログ記録は、マルウェアとマルウェア対策ソフトウェアの相対的な成功を測定するために必要でした。これには、ネットワークトラフィック、ファイルの作成、重要なファイルに対する処理や変更などのアクティビティの記録が含まれました。

■6.4 保護のレベル

製品はさまざまなレベルの保護を示しました。製品は、脅威による実行を防止するか、少なくとも対象システムに重大な変更が行われることを防止する場合がありました。

また、セキュリティ製品がマルウェアの一部またはすべてに介入し削除した後、対象システム上でタスクを実行できる場合もありました（セキュリティの脆弱性を悪用する、悪質なプログラムを実行するなど）。

最後に、脅威は、セキュリティ製品を迂回して、邪魔されることなく悪質なタスクを実行できる可能性があります。セキュリティソフトウェアを無効にできる可能性すらあります。

時には、Windows 独自の保護システムが脅威を処理し、ウイルス対策プログラムがその脅威を無視する場合がありました。さまざまな理由によりマルウェアがクラッシュする結果になることもあります。

各製品により提供されるさまざまなレベルの保護は、ログファイルの分析に従って記録されました。

製品がとった特定の防護措置ではなく、セキュリティ製品が存在するという理由で、あるインシデントにおいてマルウェアが適切に動作できなかった場合、その製品に有利な解釈がなされ、「防御」結果が記録されました。

テストシステムが損害を受け、攻撃実施以降の使用が困難になった場合は、マルウェアのアクティブな部分が製品により最終的に除去されたとしても、危殆化としてカウントされました。

■ 6.5 保護の種類

テストされた製品はすべて、リアルタイムとオンデマンドという主要な 2 種類の保護を提供しました。リアルタイムの保護は、脅威からのアクセスを防ぐために、絶えずシステムを監視します。

オンデマンドの保護は、基本的に、随時ユーザーにより実行される「ウイルススキャン」です。

テスト結果は、脅威の導入時と導入後の各製品の動作に注目します。リアルタイムの保護メカニズムはテスト全体を通して監視されました。一方、オンデマンドのスキャンは、製品によってシステムがどの程度安全であると判断されたかを測定するため、各テストの終わり近くに実行されました。

手動によるスキャンは、マルウェアが対象システムとのやり取りを行ったとテスターが判断した場合にのみ実行されました。言い換えると、セキュリティ製品が初期段階で攻撃をブロックしたことを示し、監視ログに記録されている場合、ケースは解決したと見なされ、「防御」結果が記録されました。

7. テストの詳細

■ 7.1 対象

公正なテスト環境を構築するために、各製品は、クリーンな Windows XP Professional の対象システムにインストールされました。オペレーティングシステムは、Windows XP Service Pack 3（SP3）に更新されましたが、最新のパッチまたは更新は適用されませんでした。

Windows XP SP3 と Internet Explorer 7 でテストを実施しましたが、これはこの組み合わせに依存するインターネットの脅威が非常に普及しているためです。これらの脅威の普及は、現在インターネットに接続されたシステムの多くがこのレベルのパッチを適用していることを示しています。

また、目的はセキュリティ製品をテストすることであり、システムを完全に最新の状態に保つことによる保護をテストすることではありません。

正規であっても古い一連のソフトウェアが対象システムにプレインストールされていました。これらは、既知の脆弱性を含んでいるため、セキュリティリスクを引き起こしました。サポート対象外のバージョンの Adobe Flash Player や Adobe Reader などがありました。

各システムには別のセキュリティ製品がインストールされました。各製品の更新メカニズムを使って、最新の定義、その他の要素を備えた最新バージョンがダウンロードされました。

実際の悪質な Web サイトでリアルタイムに実行するというテストの動的な性質のため、製品の更新システムの自動実行が許可され、各テストの実施前にも手動で実行されました。

製品がリアルタイムでデータベースに問い合わせるようにプログラムされている場合は、「コールホーム」も許可されました。一部の製品は、テスト中に自動的にアップグレードされることもありました。テストのどの時点でも、最新バーションの各プログラムが使用されました。

対象システムは、Intel Core 2 Duo プロセッサ、1 GB の RAM、160GB のハードディスク、DVD-ROM ドライブが搭載された、まったく同じハードウェアを使用しました。マルウェアの交差感染を回避するために、それぞれがその独自の仮想ネットワーク（VLAN）を介してインターネットに接続されました。

■ 7.2 脅威の選択

テストに使用する悪質な Web のリンク（URL）は、マルウェア対策ベンダーからは提供されませんでした。

これらのリンクは、Dennis Technology Labs 社の独自の悪質サイト検出システムにより生成されたリストから選択されました。このシステムは、Google に送信される一般的な検索エンジンキーワードを使用します。多くの検索エンジンから得られた検索結果にあるサイトを分析して、悪質な Web サイトをデータベースに追加します。

いずれの場合も、制御システム（Verification Target System - VTS）を使って、URL がアクティブな悪質サイトにリンクしていることを確認しました。

テストプロセス中、悪質な URL およびファイルは、どのベンダーとも共有されません。

■ 7.3 テスト段階

個々のテストには次の 3 つの主要な段階がありました。

1. 導入
2. 観察
3. 修復

「導入」段階の間、対象システムは脅威にさらされました。脅威が導入される前に、システムのスナップショットが作成されました。これにより、ハードディスク上にレジストリのエントリとファイルのリストが作成されました。その後、脅威を導入しました。

システムが脅威にさらされるとすぐに、「観察」段階に移ります。この段階は通常少なくとも 10 分間は続き、その期間中、テスターは視覚的に、および他社製のツールを使ってシステムを監視しました。

テスターは、後述（15 ページの「7.5 観察と介入」を参照）の指示に従ってポップアップやその他の指示に対応しました。

スパムが対象システムによって送信されているなど、他のインターネットユーザーに対する悪意のある活動が観察された場合、この段階は途中で切り上げられました。

観察段階は、システムのスナップショットをもう 1 つ作成して終了します。脅威に「さらされた」このスナップショットは、元の「クリーン」なスナップショットと比較され、レポートが生成されました。その後、システムは再起動されました。

「修復」段階は、感染したシステムをクリーニングする製品の能力をテストすることを目的としています。「観察」段階で脅威を防御した場合は、この段階をスキップしました。「スキャン済み」のスナップショットが作成された後、対象システム上で、オンデマンドのスキャンを実行しました。これは、元の「クリーン」なスナップショットと比較され、レポートが生成されました。

スナップショットのレポートや製品独自のログファイルなど、すべてのログファイルが対象システムから回復されました。

場合によっては、ログ回復が現実的でないと思われるほど、対象システムが損害を受けています。その後、対象システムはクリーンな状態にリセットされ、次のテストの準備が整えられました。

■ 7.4 脅威の導入

Web ブラウザを使ってリアルタイムで悪質な Web サイトにアクセスしました。このリスクのある動作は、実際のインターネット接続を使用して行われました。URL はブラウザに直接入力されました。

Web でホストされるマルウェアは時間の経過に伴って変化することが多くあります。短時間で同じサイトにアクセスすることで、(検出されないようにほんの少しだけ変更された同じ脅威の場合がありますが)さまざまな脅威にシステムをさらすことができます。

また、感染したサイトの多くは、特定の IP アドレスを 1 度攻撃するだけなので、同じ脅威に対して複数の製品をテストするのが困難になります。

各対象システムが悪質な Web サーバーから同じ体験を受ける機会を向上するために、Web リプレイシステムを使用しました。

検証対象システムが悪質なサイトにアクセスすると、悪質なコードなど、ページのコンテンツがリプレイシステムにダウンロード、保存、ロードされました。その後、各対象システムがサイトにアクセスすると、まったく同じコンテンツを受け取ります。

ネットワーク構成は、Web リプレイシステムに関係なく、テスト全体を通して、すべての製品がインターネットに自由にアクセスできるように設定されました。

■ 7.5 観察と介入

各テストの間、対象システムを手動およびリアルタイムで観察しました。これにより、テスターはシステムの動作で気づいた点について包括的なメモをとることができました。また、表示によるアラートを製品のログエントリと比較することもできました。

ある段階では、テスターが通常のユーザーとして行動する必要がありました。一貫性を達成するために、テスターは特定の状況に対処するためのポリシーに従いました。この状況には、製品やオペレーティングシステムが表示するポップアップ、システムのクラッシュ、タスクを実行するマルウェアによる勧誘などへの対処が含まれます。

このユーザー動作ポリシーには、次の指示が含まれます。

1. 単純に行動してください。たとえば、悪質なプロンプトに対して OK をクリックして、脅威を対象に導入できるようにします。
2. ブロックされたダウンロードを執拗に繰り返さないでください。製品がサイトへのアクセスに対して警告を発した場合は、そのサイトにアクセスするための措置はそれ以上とらないでください。
3. マルウェアが Zip ファイル形式などでダウンロードされた場合、デスクトップに解凍して実行を試みてください。アーカイブがパスワードで保護されていて、そのパスワードを知っている場合(元の悪質なメール本文に記載されているなど)は、それを使用します。
4. 常にデフォルトのオプションをクリックします。これは、セキュリティ製品のポップアップ、オペレーティングシステムのプロンプト(Windows ファイアウォールを含む)、マルウェアの動作勧誘に適用されます。
5. デフォルトオプションがない場合は、待機します。自動的に動作が選択されるよう、プロンプトで 20 秒待機します。
6. 自動的に動作が選択されない場合、最初のオプションを選択します。オプションが縦方向に一覧表示されている場合は、一番上のオプションを選択します。オプションが横方向に一覧表示されている場合は、一番左のオプションを選択します。

■ 7.6 修復

対象システムがマルウェアにさらされると、脅威がシステムに感染する可能性が高くなります。セキュリティ製品もまた、対象システムを保護する可能性が高くなります。14 ページの「7.3 テスト段階」で説明したスナップショットが提供する情報を使って、テスト終了時のシステムの最終的な状態を分析しました。

マルウェアにさらされている間に行われた変更についての情報を提供するために、各テストの前、途中、テスト後に対象システムの「スナップショット」が作成されました。たとえば、悪質な Web サイトにアクセスする前に作成されたスナップショットとアクセス後に作成されたスナップショットを比較して、レジストリ内の新しいエントリとハードディスク上の新しいファイルに注目します。

スナップショットは、対象システムに感染した脅威を取り除く際に製品がどれだけ効果的であったかを判断するためにも使用されました。この分析により、製品が提供する保護レベルがわかります。

これらの保護レベルは、防御、無効化、危殆化の 3 つの表現を使って記録されます。対象システムに足場を得られなかった脅威は「防御」、活動の継続を防がれた脅威は「無効化」、対象システムの危殆化に成功したと見なされる脅威は「危殆化」として記録されます。

最初の脅威導入後に、目視または他社製の監視ツールで悪質な活動が観察されなかった場合、防御インシデントが発生します。スナップショットレポートファイルを使って、この良好な状態が検証されます。

システム上でアクティブに実行している脅威が観察されても、オンデマンドスキャンを実行する必要がない場合は、無効化されたと見なされます。

スナップショットレポートの比較では、導入後に悪質なファイルが作成されたことと、レジストリのエントリが作成されたことを示す必要があります。ただし、「スキャン済み」のスナップショットレポートが、そのファイルが削除されたか、レジストリのエントリが削除されたかのいずれかを示している場合、脅威は無効化されています。

オンデマンドスキャン後も実行しているマルウェアが観察された場合、対象システムは危殆化されています。完全に削除するために、製品は追加のスキャンを必要とする場合がありました。セカンダリスキャンは許容できると見なしましたが、進展が確認されない場合、継続的なスキャン要求は無視される可能性があります。

編集された「ホスト」ファイルまたは変更されたシステムファイルも危殆化としてカウントされました。

■ 7.7 自動監視

他社製アプリケーションおよびセキュリティ製品を使用して、ログが生成されました。

対象システムがマルウェア（および正当なアプリケーション）にさらされている間、対象システムを手動で観測することにより、セキュリティ製品の動作に関する詳細な情報が得られました。

監視は対象システムとネットワーク上で直接行われます。

クライアントサイドのログ記録

Process Explorer、Process Monitor、TcpView、Wireshark を組み合わせて、対象システムを監視しました。システムのスナップショットを記録するために、各テスト段階の間で Regshot を使用しました。

追加のシステム情報を提供するために、多くの Dennis Technology Labs 社製スクリプトを使用しました。各製品は、ある程度のログ記録を生成できました。

Process Explorer と TcpView がテスト全体を通して実行され、システム上の悪質と思われる活動について視覚的なキューをテスターに提供しました。さらに、Wireshark のリアルタイム出力と Web プロキシの表示（後述の「ネットワークログ記録」を参照）により、セカンダリダウンロードなどの特定のネットワーク活動が示されました。

Process Monitor は、悪質なインシデントの再現に役立つ有益な情報も提供しました。Process Monitor と Wireshark は、自動的にログをファイルに保存するように設定されました。これによって、マルウェアにより対象システムがクラッシュまたは再起動する際のデータ損失が減少されました。

稼働しているシステムの状態の追加スナップショットを作成するカスタムスクリプト内で、「systeminfo」や「sc query」などの Windows の内部コマンドを使用しました。

ネットワークログ記録

対象のシステムはすべて、透過的な Web プロキシとネットワーク監視システムを組み込んだ実際のインターネットに接続されました。インターネット間のすべてのトラフィックは、このシステムを通過しなければなりません。

さらに、すべての Web トラフィックはプロキシも通過しなければなりません。これによって、テスターは完全なネットワークトラフィックを含んだファイルを取得することが可能になりました。Web ベースのトラフィックを迅速かつ容易に表示できるようになりました。これは、リアルタイムでテスターに表示されます。

ネットワークモニターは、透過的なルーターとして稼働する二重ホームの Linux システムで、Squid プロキシを通してすべての Web トラフィックを送ります。

HTTP リプレイシステムは、すべての対象システムが互いに同じマルウェアを確実に受信できるようにしました。インターネットへのアクセスを許可して、製品が更新プログラムをダウンロードし、「クラウド内」で使用可能なサーバーと通信できるように設定されました。

8. 結論

■ 脅威はどこにあるか

このテストでは、製品をテストしたのと同時期に、全世界で感染被害を出している本物の実在する脅威を使用しました。ほぼすべての場合において、脅威は、攻撃者により危殆化された正当な Web サイトから発信されます。

感染したサイトや悪質なサイトの種類はさまざまです。これは、Windows PC を使用して Web を利用しようとする人々にとって、効果的なウイルス対策ソフトウェアが不可欠であることを示しています。

ほとんどの脅威は、感染した Web サイトにユーザーがアクセスすると自動的にインストールされました。この感染は、多くの場合、普通の観察者には気づかれませんでした。

■ どこから保護を始めれば良いか

このテストでは、かなりの数の危殆化と、比較的多くの無効化がありました。

最も優れた製品は、ペイロードの配信が可能になる前にサイトをブロックしました。最も評価の低い製品は、対象システムとやり取りを始めた後で脅威を処理する傾向がありました。

■ 各製品の選別

マルウェア対策の点では、Kaspersky Endpoint Security と Symantec Endpoint Protection が最も高いスコアを獲得しました。

ブロックする脅威の数が Kaspersky 社のソフトウェアよりも多いため、全体ではシマンテックの製品が 1 位になりました。

同時テストでは、Kaspersky 社のコンシューマソフトウェアが同社のエンタープライズ製品よりも多くの脅威をブロックしました。

Kaspersky Lab は、この不均衡は Dennis Technology Labs 社のテストの結果として見つかったバグによるものであると主張し、この問題は解決済みであると付け加えています。

修復は標準の更新プロセスによって実行されました。システムの再起動などのユーザーによるアクションは必要ありません。

マルウェア対策製品は、悪質なプログラムと悪質でないプログラムを区別できなければなりません。Microsoft 社の製品はこの点に焦点を合わせています。すべての正当なアプリケーションを、警告メッセージを表示せずにインストールしたり使用したりできる唯一の製品でした。

Symantec Endpoint Protection は、脅威をブロックしただけでなく、正当なアプリケーションをほぼすべてインストールして実行できるために、全体的には高いスコアを獲得しました。

McAfee 社と Kaspersky 社の製品は僅差の同点 2 位でしたが、Trend Micro OfficeScan および Intrusion Defense Firewall は正当なアプリケーションの点で厳しい評価となりました。1 つのプログラムに対して警告しただけで、その他の 14 はアクティブにブロックしました。

■ ウイルス対策が重要（ただし、万能薬ではない）

このテストは、脅威の数が 100 という比較的小さなサンプルであっても、ウイルス対策プログラム間のパフォーマンスに大きな違いがあることを示しています。最も重要なことは、テスト時に実際のコンピュータを攻撃している本物の脅威を使用して、この違いを示しているということです。

テストした製品の平均的な保護レベルは 91%（7 ページの「3. 保護スコア」を参照）です。これは次の 2 つの理由で大きな価値があります。1 つは、ここ何年かの間に Dennis Technology Labs 社の依頼により実施したレポートで発表された平均的な数字に非常に近いという点です。もう 1 つは、一般的にマルウェア対策のマーケティング材料で取り上げられる検出結果よりもかなり低いという点です。

アクセスしているサイトだけが悪質な活動があることが証明されている場合でも、マルウェア対策ソフトウェアがあれば、マルウェアに感染する可能性を減らすことができることがわかります。とはいえ、保護率が 100% の製品が 1 つもなかったのに対し、誤検知の結果がゼロの製品は 1 つだけでした。

付録 A: 用語と定義

危殆化	オンデマンドスキャン後も、マルウェアが感染したシステム上で実行を継続する。
防御	マルウェアが対象システム上で実行することを阻止される、または対象システムを変更することを阻止される。
誤検知	正当なアプリケーションが、悪質であるとして誤って分類される。
導入	対象システムが脅威にさらされるテスト段階。
無効化	マルウェアまたはエクスプロイトコードが対象システム上で実行可能だったが、セキュリティ製品により削除された。
観察	マルウェアが対象システムに感染するテスト段階。
オンデマンド（保護）	ユーザーにより随時実行される、手動の「ウイルス」スキャン。
プロンプト	マルウェア、セキュリティ製品、オペレーティングシステムなどのソフトウェアにより尋ねられる質問。セキュリティ製品では、プロンプトは通常ポップアップウィンドウの形式で表示される。一部のプロンプトは質問をせずにアラートを提供する。プロンプトがユーザーとのやり取りなしで表示され消えた場合、このプロンプトは「トースター」と呼ばれる。
リアルタイム（保護）	多くのセキュリティ製品により提供される「常時」の保護。
修復	インストールされた脅威を除去する製品の能力を測定するテスト段階。
ラウンド	各対象システムを同じ脅威にさらす、複数製品の一連のテスト。
スナップショット	対象のファイルシステムとレジストリ内容の記録。
対象	セキュリティ製品の動作を監視するために脅威にさらされるテストシステム。
脅威	システムを破壊することを目的とするプログラムまたはその他の手段。
更新プログラム	ソフトウェアを最新の状態に維持するためにベンダーが提供するコード。これには、ウイルス定義、エンジン更新、オペレーティングシステムのパッチが含まれる。

付録 B: FAQ

- このテストは依頼により実施したものではありません。
- テストラウンドは、その時点で入手可能な最新バージョンのソフトウェアを使用して、2012 年 7 月 27 日から 8 月 24 日の間に実施されました。
- すべての製品は、インターネットを介してそのバックエンドシステムと通信できました。
- このテスト用に選択された製品は、Dennis Technology Labs 社が選択しました。
- サンプルは Dennis Technology Labs 社が特定し、検証しました。
- 製品は、脅威が検証されてから 24 時間以内に同じ脅威にさらされました。実際には、最大 3、4 時間程度の遅れです。
- URL やコードなど、サンプルの詳細はテスト完了後にパートナーベンダーに提供されました。
- サンプルセットは、100 のアクティブな悪質 URL と 100 の正当なアプリケーションで構成されました。

テスト前またはテストの間、参加しているベンダーは使用されるサンプルを知っていますか。

いいえ。使用される脅威は、私たちもテストが開始されるまで知りません。毎日のように、新しい脅威が発見されるため、テストを開始する前にこの情報を提供することは不可能です。いずれにせよ、この情報はテストが終了するまで開示しません。

ベンダーとパートナーベンダーの違いは何ですか。

パートナーベンダーは、結果のプレビュー、発表前に結果に異議を申し立てる機会、マーケティング材料に受賞ロゴを使用する権利と引き換えに、財政貢献します。その他の参加者が結果を確認するのは発表日で、どのような目的でも受賞ロゴを使用できない場合があります。

サンプルはベンダーと共有しますか。

テストが完了した後、パートナーベンダーはすべてのサンプルをダウンロードできます。

その他のベンダーは、自分たちで結果を検証するために、製品を危殆化した脅威のサブセットを要求できます。ネットワークキャプチャファイルなど、クライアントサイドのログも同様です。このサービスの提供には少額の管理手数料が必要です。

サンプルとは何ですか。

私たちのテストにおいて、サンプルとは、単にシステム上で実行する悪質な実行可能ファイルのセットではありません。サンプルとは、感染元の Web サイトが利用できなくなった場合でも、研究者がインシデントを複製できるリプレイアーカイブ全体のことです。つまり、攻撃を再現して、どの保護層が迂回可能であったかを判断することができます。多くの場合、攻撃を再現することにより、関連する実行可能ファイルが作成されます。作成されない場合は、通常はクライアントサイドのネットワークキャプチャ（pcap）ファイルを利用できます。