# 仮想デスクトップのマルウェア対策機能

## Symantec Endpont Protection と Trend Micro Deep Security の比較テスト

Dennis Technology Labs、2012 年 4 月 5 日
www.DennisTechnologyLabs.com

このレポートは、Symantec Endpoint Protection 12 の有効性を Trend Micro Deep Security 8 仮想アプライアンスと比較することを目的としています。

テストは、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 3 月 16 日から 4 月 5 日の期間で実施されました。

テスト期間中、製品は実際に顧客が遭遇する本物のインターネットの脅威にさらされました。この露出は、できる限り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。

たとえば、テストの際にテストシステムは、多数のインターネットユーザーが遭遇していた脅威に実際に感染している Web サイトにアクセスしました。これらの結果は、テストした製品のいずれかをユーザーが使用した場合どうなるかを反映しています。

## 要約

·どちらが最良の製品か
保護の点からは、Symantec Endpoint Protection が最も性能を発揮した製品でした。
（このテストには、パフォーマンスや仮想デスクトップ密度を含めていません。）

·物理システムを攻撃することが目的のマルウェアは仮想環境でも同様に機能する
このテストに使用されたマルウェアはすべて物理システム上で検証されましたが、仮想デスクトップを攻撃することも確認されています。

·Web サイトのブロックは非常に効果的な保護方法
このテストで最も性能を発揮した製品は、対象システム上でどのマルウェアも実行させませんでした。

·このテストで最も性能を発揮した製品には技術的な強みがあります
Symantec Endpoint Protection が最も良く機能しました。仮想デスクトップシステムごとにインストールする必要がある豊富な機能を持ったセキュリティ製品です。Trend Micro Deep Security は仮想アプライアンスであり、デスクトップごとの管理はあまりできません。これは、仮想環境による制限です。

Simon Edwards、Dennis Technology Labs

**仮想化へのステップ：**
仮想デスクトップのマルウェア対策機能

**目次**

# 1. 全体的な精度の評価

精度の総評価では、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。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取り扱ったかを検討します。

マルウェア対策ソフトウェアは脅威を検出するだけではないと考えています。正当なソフトウェアが邪魔されずに実行できるようにしなければなりません。

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。

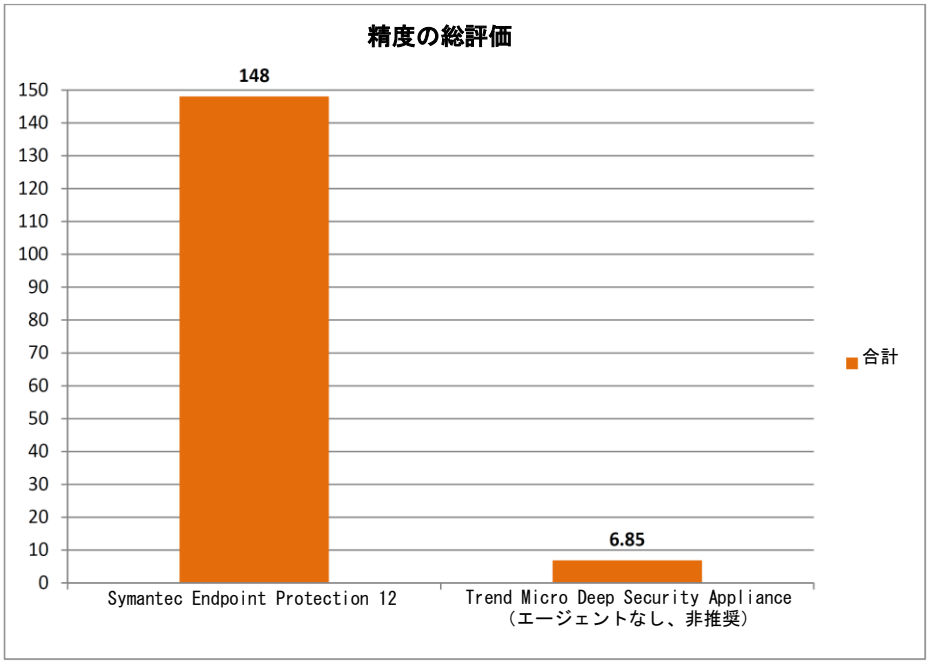
製品がシステムを脅威に対して保護できなかった場合、危殆化されます。正当なソフトウェアに対して警告を発した、またはブロックした場合、「誤検知」結果を生成します。

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検討して、まとめた精度の評価を示しています。最高が 150 点、最低が -350 点です。

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




精度の総評価では、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。

| 製品 | 精度の総評価 |
|---|---|
| Symantec Endpoint Protection 12 | 148 |
| Trend Micro Deep Security Appliance（エージェントなし、非推奨） | 6.85 |

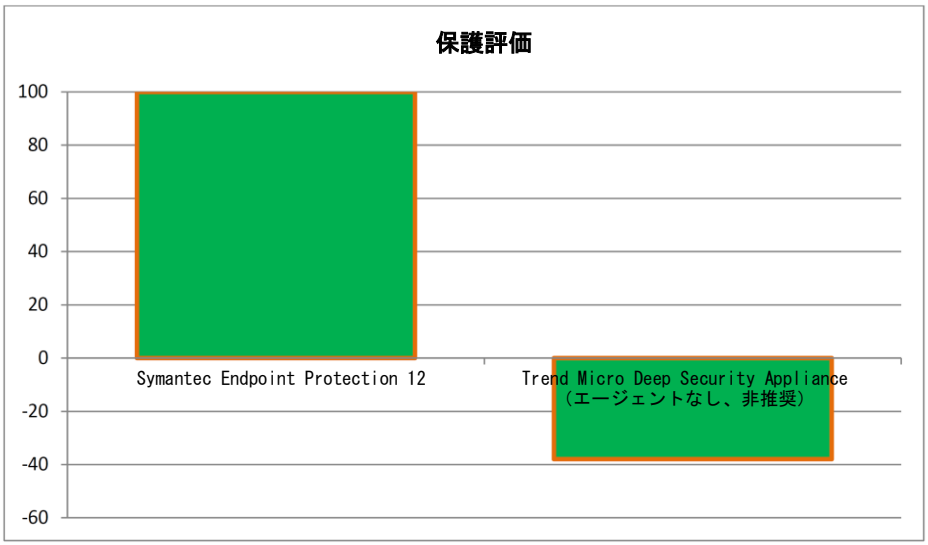
## 2. 保護評価

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 2 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 2 点減らしました。最高が 100 点、最低が -100 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機会を与えない製品を評価し、マルウェアがシステムに損害を与えることを許してしまった製品にペナルティを課すためです。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みなしてカウントしました。

シマンテックの製品は、50 の脅威をすべて防御し、100 点を獲得しました。各防御に対して 2 点ずつ獲得（2x50）し、合計 100 点になりました。Trend Micro 社の製品は、50 の脅威のうち 8 回防御し 10 回無効化（1x10）しましたが、32 回危殆化されました。このスコアは次のように計算されます。(2x8) + (1x10) - (2x32) = -38




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。

### 保護評価

| 製品 | 保護評価 |
|---|---|
| Symantec Endpoint Protection 1200 | |
| Trend Micro Deep Security Appliance（エージェントなし、非推奨） | -38 |

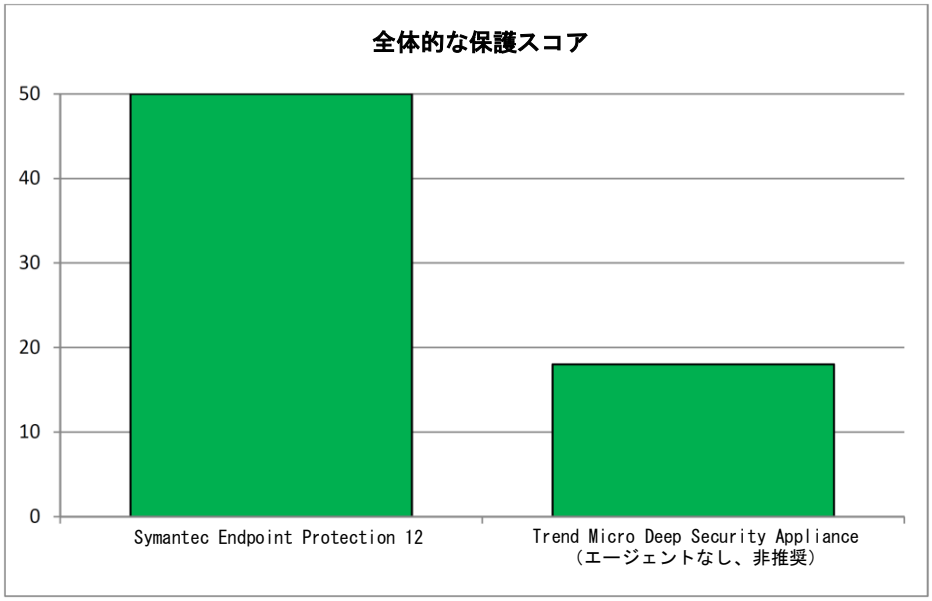
## 3. 保護スコア

次のグラフは、セキュリティ製品ごとに提供される保護の一般的なレベルを、防御されたインシデントと無効化されたインシデントは合計数にまとめて示したものです。

この数字は、防御または無効化により、システムが保護された回数を示します。

この数字は、「1. 精度の総評価」や「2. 保護評価」で行ったような任意の評価システムによる重み付けはされていません。

このテストで使用された脅威にさらされた場合、テストされた製品により得られる平均の保護レベルは 68 パーセントでした。




保護スコアは、各製品が脅威によるシステムの危殆化を防止した回数を単純に示しています。

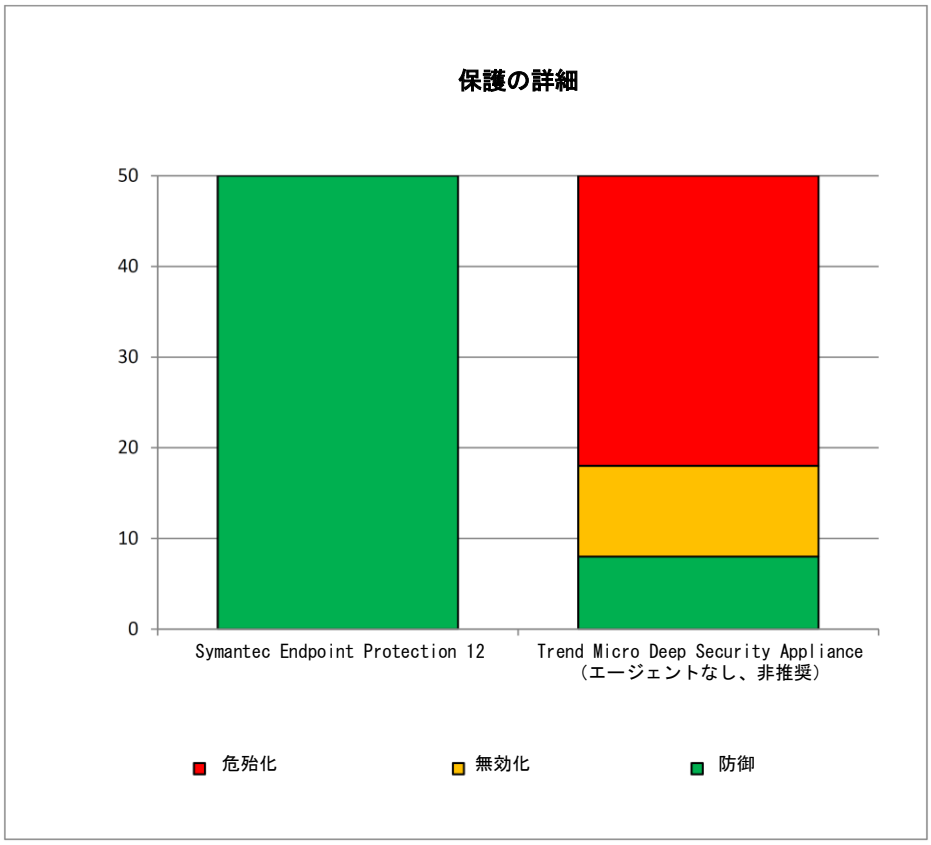
保護スコア

| 製品 | 保護スコア | |
|---|---|---|
| Symantec Endpoint Protection 12 | 50 | 100% |
| Trend Micro Deep Security Appliance（エージェントなし、非推奨） | 18 | 36% |

（平均スコア：68%）

## 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できる、またはシステムに感染できる場合があり、場合によっては、悪用が行われた後またはそれ以降に、製品がその脅威を無効化しました。無効化できない場合、システムは危殆化されました。




製品は、「防御」結果を生じた回数に基づいて並べられています。全体的な保護スコアについては、5 ページの「3. 保護スコア」を参照してください。

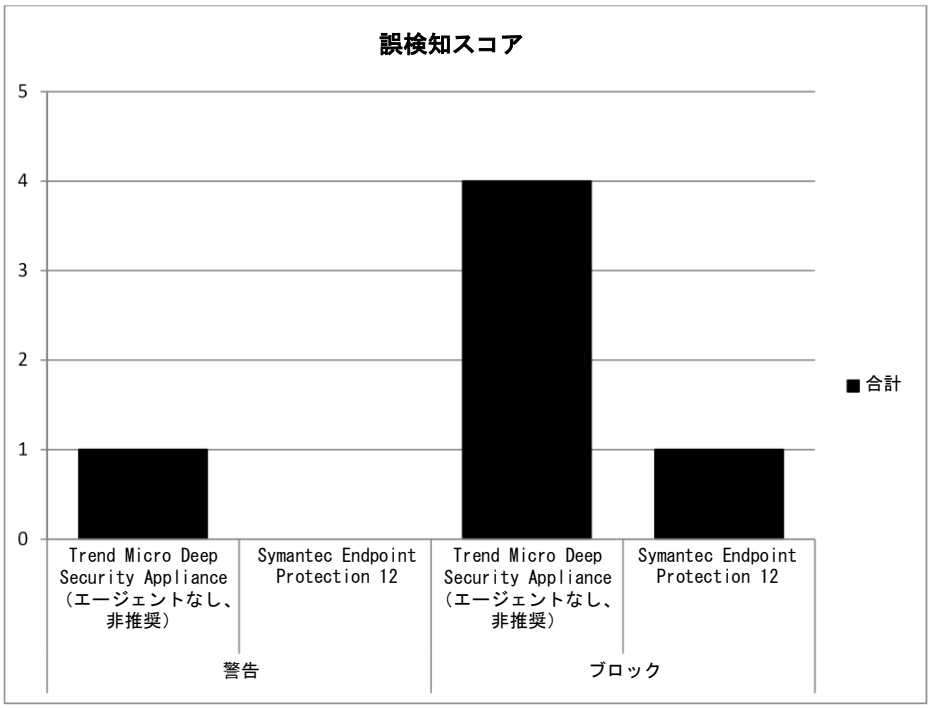
### 保護の詳細

| 製品 | 防御 | 無効化 | 危殆化 |
|---|---|---|---|
| Symantec Endpoint Protection 12 | 50 | 0 | 0 |
| Trend Micro Deep Security Appliance （エージェントなし、非推奨） | 8 | 10 | 32 |

# 5. 誤検知

## 5.1 誤検知スコア

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。




誤検知を生成する場合、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。

### 誤検知スコア

| 誤検知の種類 | 製品 | 合計 |
|---|---|---|
| 警告 | Trend Micro Deep Security Appliance（エージェントなし、非推奨） | 1 |
| | Symantec Endpoint Protection 12 | 0 |
| ブロック | Trend Micro Deep Security Appliance（エージェントなし、非推奨） | 4 |
| | Symantec Endpoint Protection 12 | |

## 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識別した場合、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、普通、マルウェア対策プログラムはどの正当なソフトウェアも間違って識別してはならないと思われています。

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

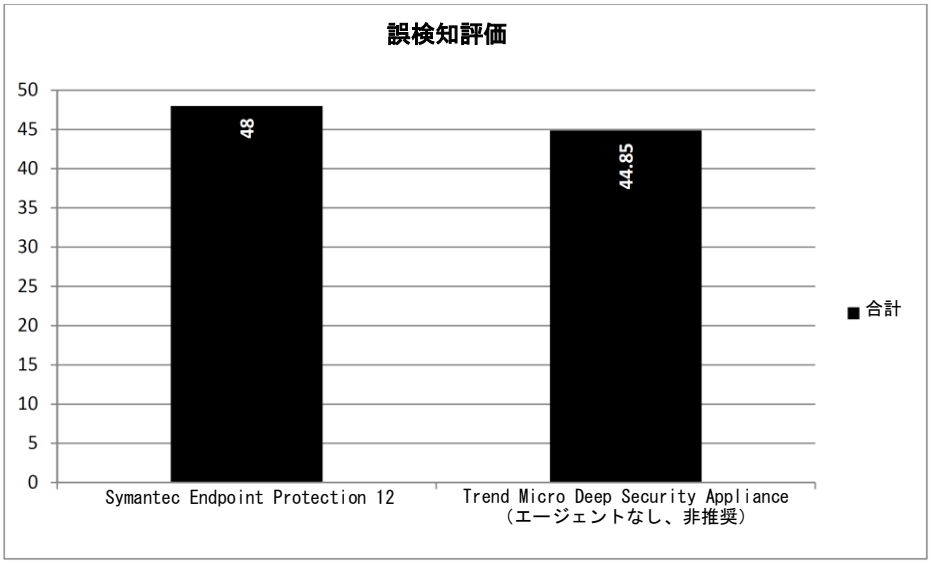
最も高いスコアを獲得した製品は、テストに使用した正当なアプリケーションを最も正確に処理しました。最高スコアは 50 点、最低スコアは -250 点です（すべてのアプリケーションが非常に大きい影響に分類され、ブロックされたと仮定）。実際、影響カテゴリにおけるアプリケーションの分布は、非常に大きい影響だけに限定されません。下の表に、実際の分布を示します。

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 | 10 |
| 大きい影響 | 20 |
| 中程度の影響 | 10 |
| 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識別した場合、普及度が低いファイルを検知した場合よりも厳しいペナルティが課せられました。

# 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何が起きるのか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露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。

| | | | Introduction | | |
|---|---|---|---|---|---|
| Incident | Product | Product code | Alert (intro | Effect (intro) | Threat Report (intro) |
| 1 | Symantec Endpoint Protection 12 | SEP | Toaster | Blocked | food.bgreunion.com/content/a |
| 1 | Trend Micro Deep Security Appliance (no | DS2-ar | None | None | None |
| 2 | Symantec Endpoint Protection 12 | SEP | Toaster | Blocked | Blackhole Toolkit Website |
| 2 | Trend Micro Deep Security Appliance (no | DS2-ar | None | None | None |
| 3 | Symantec Endpoint Protection 12 | SEP | Toaster | Blocked | Blackhole Toolkit Website |
| 3 | Trend Micro Deep Security Appliance (no | DS2-ar | None | None | None |
| 4 | Symantec Endpoint Protection 12 | SEP | Pop-up | Quarantined | vale%20presente%20boticario |
| 4 | Trend Micro Deep Security Appliance (no | DS2-ar | Toaster | Quarantined | TSPY_BANKER.DMS |
| 5 | Symantec Endpoint Protection 12 | SEP | Toaster | Blocked | Blackhole Toolkit Website |
| 5 | Trend Micro Deep Security Appliance (no | DS2-ar | None | None | None |
| 6 | Symantec Endpoint Protection 12 | SEP | Toaster | Blocked | Blackhole Toolkit Website |
| 6 | Trend Micro Deep Security Appliance (no | DS2-ar | None | None | None |
| 7 | Symantec Endpoint Protection 12 | SEP | Pop-up | Quarantined | Trojan.ADH.2 |
| 7 | Trend Micro Deep Security Appliance (no | DS2-ar | Toaster | Quarantined | PAK_Gwnwric.001 |

各「ラウンド」で、すべての製品が特定の 1 つの脅威にさらされました。ラウンド 4 の記録（上記の強調箇所）は、特定の脅威に対して製品がどのように対応したかを示しています。Alert 列には、製品が生成したアラートの種類が示されます（もしあれば）。Effect 列には、製品が脅威に対して行ったとする処置が説明され、Threat Report には詳細が示されます。フォレンジック技術を使用して、その処置が行われたどうかを検証しました。

## 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相互作用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みなされ、「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。

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。

各ベンダーの推奨に基づいて、別のセキュリティ製品が各システムにインストールされました。Symantec Endpoint Protection は、要求されたデフォルト設定を使ってインストールされました。

Trend Micro Deep Security はソフトウェアエージェントなしおよび推奨のセキュリティパッチを適用せずに導入されました（そのため、グラフには「非推奨」と記載してあります）。管理システムと保護機能は、Trend Micro 社の推奨に従って設定されています。

各製品の更新メカニズムを使って、最新バージョン、最新の定義、その他の要素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。

各対象システムは、VMware ESXi 4.1 が稼働する HP ProLiant DL360 G5 サーバー上で実行する仮想デスクトップでした。各仮想デスクトップには、2GB の RAM、1 プロセッサ、最大 27GB のディスクスペースが割り当てられました。

個々の製品が必要とする管理ツールが導入されました。これには、管理ツールを持たないスタンドアロン製品として Symantec Endpoint Protection を実行する管理コンソールが含まれます。

## 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す。

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 Registry エントリとファイルのリストが作成されました。Regshot（**付録 B: ツールを参照**）を使用して、システムのスナップショットを作成して比較しました。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（**「7.6 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敵対的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した。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

Internet Explorer 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 Internet Explorer のアドレスバー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、全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 セカンダリダウンロード

感染したマルウェアはファイルをさらにダウンロードしようとする場合があります（セカンダリダウンロード）。このファイルはネットワーク上のプロキシによりキャッシュに保存され、状況次第でその他の対象システムに再提供されます。たとえば、次のような状況があります。

1. ダウンロード要求が HTTP を使って行われる（例、http://badsite.example.com/...）
2. 毎回同じファイル名を要求される（例、badfile1.exe）

対象システムがさまざまなセカンダリダウンロードを受け取るシナリオがあります。たとえば、次のような場合があります。

1. ダウンロード要求が HTTPS または FTP などの Web 以外のプロトコルを使用して行われる
2. 毎回異なるファイル名を要求される（例、badfile2.exe、random357.exe）

## 7.6 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。

## 7.7 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。「**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みなされる脅威は「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たが、オンデマンドスキャンを実行する必要がない場合は、無効化されたとみなされます。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行われたことが示される必要があります。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みなしますが、それ以上のスキャン要求は無視されました。マルウェアが観測されなかった場合でも、ハードディスク上に悪質と思われる新しいファイルが存在し、システムの起動時にそれらのファイルのうち少なくとも 1 つを実行することを目的としたレジストリのエントリがあることをスナップショットレポートが示している場合は、「危殆化」結果がレポートされました。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。

## 7.8 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、ある程度の自分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、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、テストに使用した製品と同時期に、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 T 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。

一部の脅威は、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、偽のウイルス対策プログラムやその他のユーティリティプログラムをインストールしない限り、普通の観察者には通常気づかれず、マルウェアが正体を現すことはめったにありませんでした。ある種の脅威は、銀行の詳細情報を盗む試みの一部として、システムのホストファイルを変更します。

**どこから保護を始めれば良いか**
脅威の防御に最も優れた製品は、Symantec Endpoint Protection でした。すべての場合において、脅威が実行される前に、その脅威をブロックしました。Trend Micro Deep Security は、いくつかの悪質なサイトをブロックしましたが、いくつかの脅威はシステムに到達した後に無効化しました。

対象システムが干渉される前にサイトや悪用をブロックする方が優れています。これは、Trend Micro Deep Security により保護されたシステムが受けた危殆化の数を見ると明らかです。

**製品間でこれほど結果が異なる理由**
このテストは、仮想化されたデスクトップを対象とするマルウェア対策のテストです。通常、セキュリティベンダーが仮想デスクトップの保護に採用する手法には、主に 2 つの手法があります。1 つはデスクトップごとに完全なセキュリティ製品をインストールする手法、もう 1 つは仮想プラットフォーム内に保護を統合する手法です。これは頻繁に、「仮想アプライアンス」の形式をとっています。

どちらの手法にも利点があります。完全なセキュリティスイートを仮想デスクトップにインストールすると、広範な保護対策が得られます。たとえば、その製品は、システムのメモリ内の状況を監視したり、悪質な可能性のある動作をブロックすることができます。

仮想アプライアンスを使用することの重要な利点は、セキュリティ製品を 1 つインストールするだけで、多くのシステムを保護することができ、個々の仮想デスクトップをパフォーマンスの問題を引き起こす可能性があるソフトウェアがない状態にすることができます。

仮想デスクトップ環境がさまざまな方法で広範な目的のために設定されることは注目に値します。ユーザーが自由にインターネットにアクセスし、ソフトウェアをインストールできる場合もあります。その他のシナリオでは、ユーザーがより広い範囲にロックダウンされます。

別のセキュリティ製品が、このような環境で使用される場合もあります。たとえば、Web をブロックするゲートウェイアプライアンスがネットワークに追加されることがよくあります。

このテストにおいて、「ユーザー」は、制限なくあらゆる Web サイトに問題なくアクセスできます。

Trend Micro Deep Security の場合、各デスクトップにインストールされた追加のソフトウェアエージェントを使用しないと、製品は各対象デスクトップインストールのメモリとは直接やり取りできません。これは、現行の VMware ベースの仮想アプライアンスすべてに共通した状況です。このように、このテストにおいては、メモリに直接アクセスできる Symantec Endpoint Protection に比べて重大なデメリットがあります。

**悪質なサイトとアプリケーションから正当なサイトとアプリケーションを区別する**
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。テストされた両製品は、この領域ではよく機能しました。

誤検知対象プログラムは、主に消費者にのみ適しており、企業のネットワークではほとんど見つかることはありません。この理由により、両製品が影響の大きいファイルをいくつかブロックした場合でも、深刻な問題とは考えません。

**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 50 という比較的小さなサンプルであっても、製品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。

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、ウイルス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少できることがわかります。

## 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、悪質であるとして間違って分類される。 |
| 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 | マルウェアまたは悪用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。<br>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: ツール

**Ebtables**
http://ebtables.sourceforge.net
ebtables プログラムは、ファイアウォールを補強するフィルタリングツールです。ネットワークトラフィックが透過的に Squid proxy を通過するよう強制するために使用されます。

**Fiddler2**
www.fiddlertool.com
Web トラフィック (HTTP/S) デバッガ。感染したサイトに検証対象システム (VTS) を使ってアクセスするときにセッションをキャプチャするために使用されます。

**HTTPREPLAY**
www.microsoft.com
HTTP トラフィックの分析とリプレイを可能にする SOCKTRC プラグイン。

**Process Explorer**
http://technet.microsoft.com/enus/sysinternals/bb896653.aspx
Process Explorer は、開いているまたはロードしているハンドルと DLL プロセスの情報を示します。また、新しいプロセスの開始と古いプロセスの停止を明確かつリアルタイムに表示します。

**Process Monitor**
http://technet.microsoft.com/enus/sysinternals/bb896645.aspx
Process Monitor は、リアルタイムでファイルシステム、レジストリ、プロセス/スレッドの活動を示す監視ツールです。

**Regshot**
http://sourceforge.net/projects/regshot
Regshot はオープンソースのレジストリ比較ユーティリティです。レジストリのスナップショットを作成して、もう 1 つのスナップショットと比較します。

**Squid**
www.squid-cache.org
Squid は、HTTP、HTTPS、FTP、その他のプロトコルをサポートするキャッシュ Web プロキシです。

**Tcpdump**
www.tcpdump.org
Tcpdump は、バイナリを含むネットワークトラフィックのコピーを作成できるパケットキャプチャユーティリティです。

**TcpView**
http://technet.microsoft.com/enus/sysinternals/bb897437.aspx
TcpView は、リアルタイムでシステム間のネットワーク接続を表示します。

**Windows コマンドラインツール**
付属の「systeminfo」と「sc query」を使用しました。systeminfo コマンドにより、「管理者は基本的なシステム設定情報を問い合わせることができます。」sc コマンドは「NT Service Controller やサービスとの通信に使用されます。」

**Wireshark**
www.wireshark.org
Wireshark はネットワークプロトコルアナライザです。今後の分析のために、バイナリを含むネットワークトラフィックを保存できます。

# 付録 C: テスト条件

## このテストはシマンテックの依頼によるものです。

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 3 月 16 日から 4 月 5 日の間に実施されました。

すべての製品は、インターネット上で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、シマンテックが選択しました。

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シマンテックに提供されました。

サンプルセットは、50 のアクティブな悪質 URL と 50 の正当なアプリケーションで構成されました。

よくある質問とその回答は、次のとおりです。

**テスト前またはテストの間、スポンサ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。開示した場合、スポンサーが有利になる可能性があり、それは現実を反映しません。

**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、スポンサーはすべてのサンプルをダウンロードできます。テストに関係する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管理手数料が少しかかります。

**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、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。

**スポンサーは全く自由に製品を選択できますか。**
いいえ。スポンサーは比較を希望する製品を指定することができますが、この決定に対して私たちは常にアドバイスを行い、他製品との比較が不公平であると思われる場合は、その製品を含めることを拒否します。

**脅威を検出し除去したことを結果が明確に示している時、製品はどのように「危殆化」とされますか。**
私たちの Threat Report グラフには、製品が行ったとする処置と私たちが判断した最終結果の両方が示されます。
製品がシステムを保護したと主張する場合でも、フォレンジックの結果が異なる場合があります。製品が攻撃の要素の一部を検出しても、残りを防げないのはよくあることです。