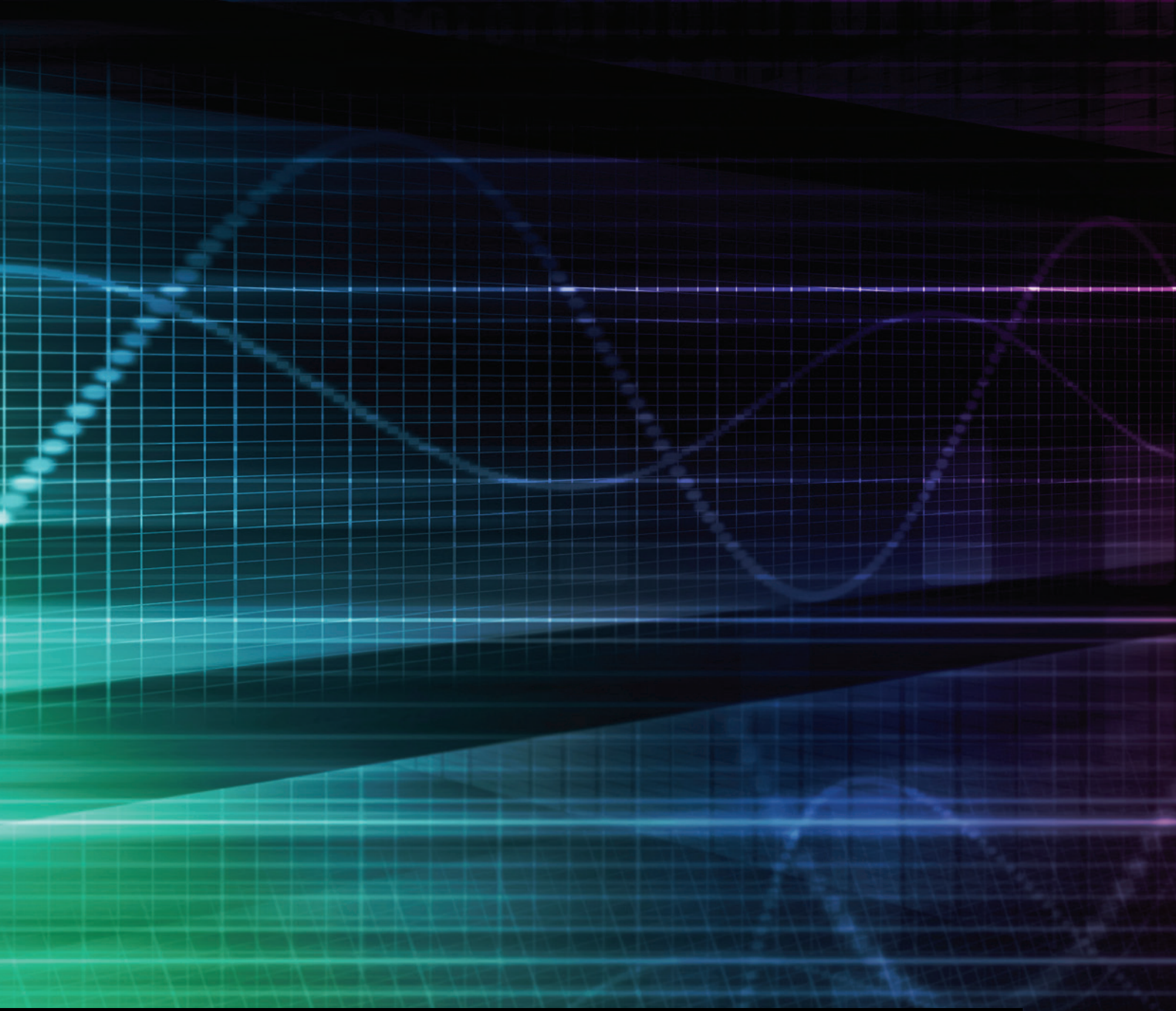


システムリソースへの影響についての比較テスト

CylancePROTECT® と
従来型アンチウイルス製品との比較

CYLANCE™

セキュリティ管理者は、マルウェアに対する適切なセキュリティを確保することと、エンドユーザーの効率を妨げないようにすることの間でバランスを取るのに苦慮しています。セキュリティ対策の副作用の 1 つに、エンドポイントの CPU に管理上のオーバーヘッドが発生するという点が挙げられます。こうした管理上のタスクによって CPU の処理能力が占有されてしまうと、エンドユーザーが自分の作業を行うために保護機能を無効にしてしまうというリスクが生じます。また、データの整合性を維持するという目的では、シンプルでエレガントなソリューションが好まれます。イギリスのサリー大学のアラン・ウッドワード教授は、最近のブログ記事でシグネチャベースのアンチウイルスの課題について述べており、「複雑さはセキュリティの敵である」と指摘しています。保護機能が無効にされることがなくても、従業員の生産性に与える影響は**1 人あたり年間 1,000 ドル**を超える場合があります。

このホワイトペーパーは、エンドポイントの管理を日々行っているセキュリティ管理者と、組織の目標と予算の制約の中でバランスを取る責任を負っているリーダー向けに作成されています。

先進的な考え方を持つセキュリティ管理者は、セキュリティ対策が作業に与える影響を最小限に抑えることを目指しています。それは、CPU 使用率に換算すると、5 ～ 10% が目安となります。CPU 使用率がこの数値を上回ると、生産性に悪影響が生じ、ヘルプデスクの呼び出しが増え、エンドユーザーによる保護機能の無効化が発生し、一般的な不満が高まります。

サイランスでは、コンピューターシステムへの影響、ファイルのコピーや作成などの一般的な作業時のユーザーへの影響、マルウェアの検出・隔離中の影響について、複数のテストを実施しました。

テスト手法：

システム：

このテストでは、次の 3 つのタイプのシステムを使用してパフォーマンスと機能のシミュレーションを行いました。古くて低速なプロセッサーとハードディスクドライブを備えた「ローエンド」のノート PC、

比較的新しい i7 クアッドコア CPU と SSD を備えた「ミッドレンジ」のノート PC、最新の i7 クアッドコア CPU と高速な M.2 NVMe SSD ストレージを備えた「ハイエンド」のデスクトップ PC です。

使用したシステム：

「ローエンド」— ノート PC：

- Toshiba Satellite C55
- Intel Celeron N2820 @ 2.13GHz（2 コア）
- 8GB RAM
- Toshiba MQ01ABF050 500GB 5400RPM
- Windows 10 Enterprise

「ミッドレンジ」— ノート PC：

- Dell Latitude E7450
- Intel Core i7-5600U 2.60GHz（4 コア）
- 16GB RAM
- Samsung PM851 M.2 PCIe 256GB SSD
- Windows 7 SP1

「ハイエンド」— デスクトップ PC：

- Intel “Skull Canyon” NUC6i7KYK
- Intel Core i7-6770HQ 2.60GHz（4 コア、ハイパースレッディングを有効にして論理コア数は 8）
- 32GB RAM
- Samsung 960 PRO M.2 PCIe NVMe 1TB SSD
- Windows 10 Enterprise

どのシステムでも、電力設定は「ハイパフォーマンス」にし、スリープ／アイドルに関するすべての機能は「なし」に設定しました。

テストしたソフトウェア：

3 つのソフトウェアパッケージをテストしました。高い市場シェアを持つ 2 つのアンチウイルス製品（製品 X、製品 Y と呼びます）と、CylancePROTECT です。

テスト対象の 3 つの製品間で保護レベルが同等になるようテスト手法を設定しました。鋭い読者は、設定する機能を増やすにつれて消費するリソースも増えると結論付けるかもしれません。

ソフトウェアのポリシー：

すべてのテストは各システムで 3 回ずつ実行され、それら 3 回の結果を平均することによって対象システムのテスト結果としました。

CylancePROTECT のポリシーは次のように設定しました。

ファイルアクション — 自動隔離、除外なし

メモリ防御 — 有効、すべてを「Terminate」に設定、除外なし

保護設定 —「シャットダウンを防止」を有効、「安全でない実行中のプロセスを強制終了」を有効、「新しいファイルを検査」を有効、除外なし

アプリケーション制御 — オフ

エージェント設定 —「デスクトップ通知」を有効

スクリプト制御 — オフ

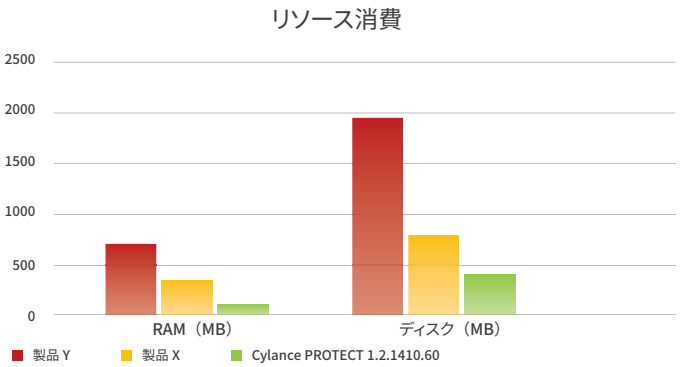
デバイス制御 —「すべてのデバイスのフルアクセス」を有効、除外なし

テストシナリオ：

システムとユーザーに対する影響を測定するため、複数のテストシナリオを用意しました。

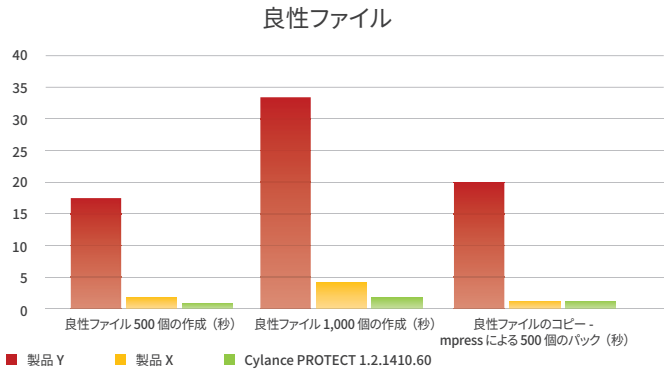
リソース消費テスト：

1. 製品のインストール後に、アイドル状態の製品によって使用されているシステムリソースを調べます。
   - RAM 使用量は、インストールによってシステムに新しいプロセス／サービスが追加され、それによって「使用中」の RAM がどれだけ増えたかによって判断します。
   - ディスク使用量は、ディスクのプロパティを表示し、メインのハードディスクドライブの「使用領域」のバイト数を参照することによって判断します。インストール前と、インストールしてすべてのアップデートを適用した後を比較します。



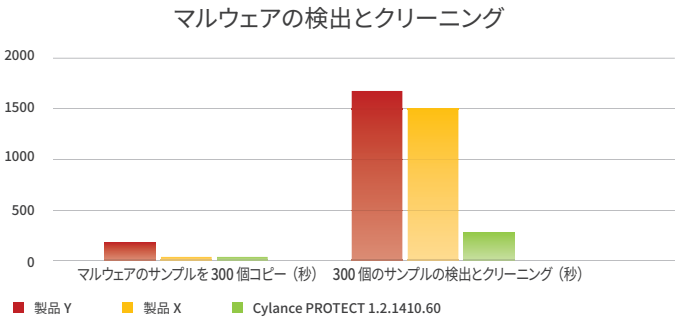
良性ファイル：

1. 良性ファイルの作成 – 500
   - このテストは、ディスクに新しいファイルを作成する場合に、セキュリティソフトウェアがシステムに与える影響を判断するためのものです。Windows Media Player のセットアップファイル（setup_wm.exe）をコピーし、コピーしたファイルの名前を setup_wm###.exe に変更する操作を、シンプルな FOR ループによって 500 回実行します。シンプルな時間測定バッチスクリプトを使用してファイル作成に要する時間を測定します。
2. 良性ファイルの作成 – 1,000
   - このテストは、ディスクに新しいファイルを作成する場合に、セキュリティソフトウェアがシステムに与える影響を判断するためのものです。Windows Media Player のセットアップファイル（setup_wm.exe）をコピーし、コピーしたファイルの名前を setup_wm###.exe に変更する操作を、シンプルな FOR ループによって 1,000 回実行します。シンプルな時間測定バッチスクリプトを使用してファイル作成に要する時間を測定します。
3. 良性ファイルのコピー – MPRESS による 500 ファイルのパック
   - このテストは、外部の USB 3 ハードディスクドライブからファイルを 500 個コピーする際に、セキュリティソフトウェアがシステムに与える影響を判断するためのものです。このテストでは、Windows Media Player のセットアップファイル（setup_wm.exe）のコピーファイルを 500 個用意し、一般的なパッカーである MPRESS を使用してすべてのファイルをパックします。



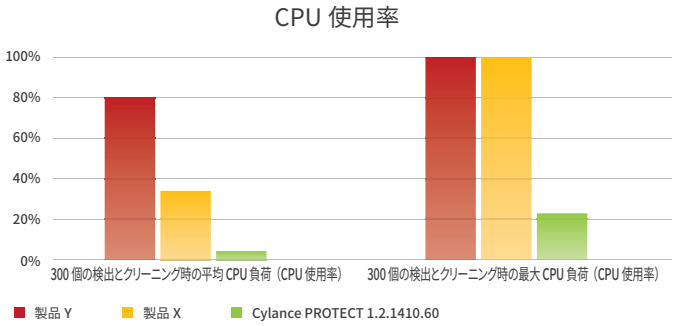
マルウェアの検出とクリーニング：

1. マルウェアのサンプルを 300 個コピー
   - このテストは、ネットワーク共有からマルウェアのサンプルを 300 個コピーする際に、セキュリティソフトウェアがシステムに与える影響を判断するためのものです。このテストでは、100 種類のランダムなランサムウェアのサンプルからなる 300 個のサンプルを使用します。100 種類のランダムなマルウェアのサンプルのサイズは 3MB 以上であり、100 種類のランサムウェアのサンプルはパックされています。
2. 300 個のサンプルの検出とクリーニング
   - このテストは、前のテストでシステムにコピーされた 300 個のサンプルを検出してクリーニングする際にシステムに与える影響を判断するためのものです。検出とクリーニングの時間は次のように測定されます。ファイルコピー処理の開始時に PERFMON データモニターを開始し、セキュリティソフトウェアがファイルのスキャンを停止して CPU の負荷がほぼ 0% に戻ったときに、データモニターを停止します。



3.CPU に対する影響

- CPU の平均と最大の負荷は、PERFMON のデータセットを作成し、インストールされたセキュリティソフトウェアがマルウェアの 300 個のサンプルを検出してクリーニングする際の CPU 負荷（パーセント）を収集することによって測定します。



結果：

1. マルウェアのスキャンと検出において、製品 Y と製品 X はまったく異なるアプローチを採用している

製品 Y は、ドライバを使用して読み取り／書き込み機能に自らの機能を注入しています。これは、ローカルディスク、リムーバブルストレージ、ネットワークドライブのすべてにおいて同じです。製品 Y では、この機能は「オンアクセススキャナ」という名前で呼ばれており、デフォルトで有効になっています。多くのアンチウイルスベンダーはこの手法を一般的に使用していますが、これはアンチウイルス製品によって PC が非常に遅くなったとユーザーが不平を言う場合の大きな原因となっています。大きな ZIP アーカイブファイルを展開したり、多くのファイルをコピーしたりするなどの一般的なタスクを実行する際に、この種のシステムはパフォーマンスに大きな影響を与えます。結果からわかるように、ほとんどの場合、ファイル作成時やコピーにおいて製品 Y のスキャン機能は、平均で CylancePROTECT システムの 16 倍の時間がかかっています。

製品 X では、「遅延スキャン」と呼ばれる手法を使用しています。この機能は CylancePROTECT の File Watcher 機能と似ています。ディスクに書き込まれるファイルを追跡してそれをキューに入れ、後でスキャンを実行します。結果からわかるように、この手法ではユーザーに対する直接的な影響は少なく、ファイルの作成／コピーのテストにおいて、製品 X と CylancePROTECT は非常によく似た結果を示しています。

2. 製品 X と製品 Y はいずれも、CylancePROTECT と比較すると非常に多くのシステムリソースを使用している（アイドル時）

CylancePROTECT と比較すると、製品 X と製品 Y はいずれも、はるかに多くのホスト上のリソースを使用します。CylancePROTECT は、アイドル時に約 107MB の RAM と約 380MB のハードディスク領域を消費し、2 つのプロセスが実行されています。

製品 Y は、インストールされているアプリケーションとアップデートによってアイドル時に約 13 倍の RAM が使用され、5 倍のディスク領域が消費されます（約 2GB）。また、製品 Y では、13 個のプロセスが実行されています。

製品 X の最新バージョンでは、前のバージョンよりも RAM の使用量とプロセスが大きく削減されています。しかし、CylancePROTECT と比較すると、製品 X はアイドル時でも 5 倍のメモリと 2 倍のディスク領域を使用します。

3. パフォーマンスの最大の違いは検出とクリーニング時

エンドユーザーのシステムに対する影響が最も大きく異なったのは、ホストに 300 個のマルウェアサンプルをコピーしたときでした。

製品 Y は、コピープロセスに自分自身の機能を注入するため、ファイルコピーが開始されるとすぐにマルウェアの検出が開始されました。製品 Y は、300 個のサンプル（の一部分）の検出とクリーニングを最も高速に実行し、203 秒しかかかりませんでした。しかし、その処理時に CPU はほぼ完全に消費されてしまいました。300 ファイルのコピー時の平均 CPU 負荷は 79% であり、最大では 100% に到達しました。さらに、製品 Y では、全体の 2/3 のファイルしかクリーニングできませんでした。300 個のサンプルのうち 99 個の検出に失敗したのです。CylancePROTECT と比較すると、製品 Y は、67% のサンプルの検出とクリーニングを 20% 高速に実行しました。しかし、この処理時の製品 Y の平均 CPU 使用率は、CylancePROTECT が同じ処理を行うときと比べて約 20 倍でした。

製品 X の結果は、製品 Y と大きく異なります。製品 X は、ファイルコピーに自分自身の機能を注入するのではないため、ファイルコピー自体は非常に高速に行われます。しかし、「遅延スキャン」が開始されると、CPU 使用率は劇的に上昇し、平均 CPU 使用率は 33.6%（最大時は 100%）に達しました。また、300 サンプルのうち 94.3% の検出とクリーニングが行われ、それには約 1,500 秒かかりました。CylancePROTECT と比較すると、製品 X は、CPU を 8.4 倍も消費し、サンプルの検出とクリーニングに約 6 倍の時間がかかりました。

CylancePROTECT の CPU 使用率は平均で 4%（最大時 23.4%）であり、サンプルの 99.7% を検出して隔離するのに 277 秒かかりました。300 個のサンプルの中で検出できなかったのは 1 つだけでした。これは破損したファイルであり、有効な WIN32 アプリケーションではありませんでした。

テスト時に判明したその他の事項：

以下は、テスト時に判明したその他の事項をまとめたものです。

製品 Y：

- 最初にインストールした後、アップデートプロセスに 1 時間以上かかりました。ローカルに接続された管理コンソールソフトウェアリポジトリからアップデートをダウンロードした場合でもこれだけの時間がかかったのです。
- 再起動してデータをロードする際に、「オンアクセススキャナ」のプロセスが CPU リソースを激しく消費します。ローエンドのノート PC では、ログイン後に大量のハードディスクのアクセスが何分も続きます。

製品 X：

- アップデート処理では 15 個のアップデートをダウンロードし、完了するまで約 10 分かかりました。
- インストール時に再起動が必要です。
- マルウェアサンプルのテスト時に、製品 X のエージェントは、再起動が必要なアップデートを何回もダウンロードしました。

まとめ

PC の処理能力がセキュリティスキャンと修復に使用されることによって、生産性の損失が発生します。その損失がたとえ 1 日あたり 1 分だとしても、中規模の企業にとってそのようなコストは、1 年で膨大に膨れ上がります。1 万人の従業員がいる場合、直接的な生産性の損失だけで 1,000 万ドルに達します。PC ハードウェアの更新は多額の費用がかかりますが、ヘルプデスクへの問い合わせが多くなれば、それは更新の必要があることを示しています。しかし多くの企業では、PC に大きな負荷をかけないセキュリティソリューションを導入することによって、ハードウェアの更新サイクルを 12 ～ 24 カ月延長できると考えています。また、製品やブランドの評判、機会損失などに関連する間接的なコストは、毎年数千ドルにもなります。さらに、環境保護に取り組んでいる組織の中には、セキュリティ対策関連の電力消費に注目し、エネルギー消費の少ないソリューションを推奨しているところもあります。したがって、先進的な考え方を持つ企業は、セキュリティソフトウェアの選択肢を評価する際に、ソフトウェアライセンス料金以外のことも考慮に入れています。

肥大化したアンチウイルスプログラムを使用していると、従業員 1 人あたり **年間1,000ドルを超える損失が発生する。**

平均的な従業員の労働時間は週 **5 日**、年間 **50 週**。

5 日
× 50 週
250 日

平均的なナレッジワーカーが 1 日 **10 分**の時間を無駄にすると仮定。

10 分
× 250 日
2,500 分 /42.67 時間

平均的なアメリカの労働者は 1 時間あたり **26 ドル**の賃金を得る。

$26.00
× 42.67 時間
$1,109.42

出典：https://www.bls.gov/news.release/empsit.t19.htm

具体的なテスト結果を次の表に示します。

製品Y Threat Prevention 10.5	データ	CylancePROTECT、 1.2.1480 — データ	Cylanceと比べた場合の倍率
RAM 消費	689MB	**107MB**	**6.4**
ディスク消費	1,932MB	**381MB**	**5**
良性ファイルの作成（500 個）	17.49 秒	**1.02 秒**	**17.1**
良性ファイルの作成（1,000 個）	33.82 秒	**1.98 秒**	**17.1**
良性ファイルのコピー – mpress による 500 個のパック	20.13 秒	**1.28 秒**	**15.7**
マルウェアのサンプルを 300 個コピー	203 秒	**28.3 秒**	**7.2**
300 個のサンプルの検出とクリーニング	203.0 秒	**277.0 秒**	**0.8**
300 個の検出とクリーニング時の平均 CPU 負荷	79%	**4.0%**	**19.9**
300 個の検出とクリーニング時の最大 CPU 負荷	100%	**23.4%**	**4.3**
製品X Endpoint Protection 14	データ	CylancePROTECT、 1.2.1480 — データ	Cylanceと比べた場合の倍率
RAM 消費	269MB	**107MB**	**6.4**
ディスク消費	785MB	**381MB**	**2.0**
良性ファイルの作成（500 個）	2.02 秒	**1.02 秒**	**2.0**
良性ファイルの作成（1,000 個）	3.98 秒	**1.98 秒**	**2.0**
良性ファイルのコピー – mpress による 500 個のパック	1.76 秒	**1.28 秒**	**1.4**
マルウェアのサンプルを 300 個コピー	29.2 秒	**28.3 秒**	**1.0**
300 個のサンプルの検出とクリーニング	1,496 秒	**277.0 秒**	**5.7**
300 個の検出とクリーニング時の平均 CPU 負荷	33.6%	**4.0%**	**8.4**
300 個の検出とクリーニング時の最大 CPU 負荷	100.0%	**23.4%**	**4.3**

Cylance Japan 株式会社
〒100-6510
東京都千代田区丸の内 1-5-1　新丸の内ビルディング 10F
www.cylance.co.jp
03-6386-0061 (代表)

CYLANCE™