Microsoft Forefront Client Security

TCO の分析

**概要**

組織は常に、セキュリティ対策を強化して生産性、資産、および情報の損失を抑えなければならないという課題に直面しています。Microsoft® Forefront™ Client Security を使用することによって、脆弱性を低下させ、総保有コスト (TCO) を削減できるので、これらの課題を克服できます。このホワイト ペーパーでは、厳選された Forefront Client Security の導入企業から協力を得て実施した、TCO に関する調査結果の概要を紹介します。

2008 年 6 月



**目次**

[このホワイト ペーパーの要点 2](#_Toc204098771)

[インターネットへの接続によってデスクトップにもたらされる セキュリティの脅威 2](#_Toc204098772)

[重要な機能を欠いている既存の製品 2](#_Toc204098773)

[実績のあるソリューションと測定可能な TCO の削減量 2](#_Toc204098774)

[Forefront Client Security による脅威の排除 2](#_Toc204098775)

[一元的な保護 2](#_Toc204098776)

[セキュリティに関する問題の減少 2](#_Toc204098777)

[単純化された管理 2](#_Toc204098778)

[IT 管理コストの削減 2](#_Toc204098779)

[可視性と制御 2](#_Toc204098780)

[可視性と制御によって提供される強力な IT ツール 2](#_Toc204098781)

[Forefront Client Security のコストと展開 2](#_Toc204098782)

[ライセンス、ハードウェア、および展開コスト 2](#_Toc204098783)

[仮想化 2](#_Toc204098784)

[まとめ 2](#_Toc204098785)

[付録 A : 調査の詳細と方法論 2](#_Toc204098786)

[付録 B : 調査に参加した企業 2](#_Toc204098787)

# このホワイト ペーパーの要点

|  |
| --- |
| 「私たちは保護されており、最新の対策を実装していると自信を持って言えます」NRMA (オーストラリア、シドニー)サーバー デスクトップ チーム主任Tom Sammons |

企業は常にセキュリティの脅威にさらされています。企業ネットワークの内外を問わず、ウイルス、スパイウェア、マルウェア、および対象を絞った攻撃が発生しています。企業ネットワークの強固なセキュリティを突破して侵入してくる脅威もあれば、物理的に外部から持ち込まれたラップトップやデバイスを通じて侵入してくる脅威もあります。その結果、組織は常に、セキュリティ対策を強化して生産性、資産、および情報の損失を抑えなければならないという課題に直面します。

|  |
| --- |
| **TCO に関する調査の概要**  |
| **セキュリティに関する問題の発生数が平均 85%減少した** |
| **セキュリティに関する問題への対応時間が平均 75% 短縮された** |
| **デスクトップ 1 台あたり平均 24 ドルの TCO が削減された** |
| **全体的なユーザーのダウンタイムが大幅に短縮された** |

このホワイト ペーパーでは、一元管理機能と拡張可能なレポート機能を提供する、統合型のウイルス対策およびスパイウェア対策ソリューションである Microsoft® Forefront™ Client Security を使用することによって、どのように脆弱性を緩和し、総保有コスト (TCO) を削減して、これらの困難を克服できるかについて説明します。具体的には、Forefront Client Security の早期導入企業 8 社を対象とした、TCO に関する調査結果の概要を紹介します。

 経営コンサルティングおよび財務分析企業の Value Prism Consulting は、Forefront Client Security を導入した企業 8 社で TCO がどれだけ変化するかを調査しました。調査に参加した企業は、IT のセキュリティに関する問題に対応する時間の短縮率に基づき、デスクトップ 1 台あたり平均 24 ドルのコストを削減できると評価しました。また、具体的には数値化されていませんが、いくつかの組織ではエンド ユーザーの生産性が大幅に向上することも確認されました。さらに、これらの参加企業では、Forefront Client Security をインストールした後、セキュリティに関する問題の発生数が全体で 85% 減少しました。いくつかの組織では、IT の管理にかかるコストがさらにデスクトップ 1 台あたり 7.5 ドル削減されるという大きなメリットを得ることができました。これに加えて、調査に参加した組織は、Forefront Client Security によって提供される独自のレポートおよび制御機能からも大きなメリットを得ることができると考えています。これらの組織の初期投資額は、デスクトップ 1 台あたり平均 16.5 ドルです。この Forefront Client Security の展開コストには、展開作業にかかるコスト、および追加で必要になるソフトウェアやハードウェアに関するコストも含まれています。

図 . コストと削減額の概要

# インターネットへの接続によってデスクトップにもたらされるセキュリティの脅威

ここ何年か、企業はスパム、サービス拒否 (DoS) 攻撃、およびウイルス関連のセキュリティ攻撃を回避することに成功してきました。ただし、企業内外でインターネットに接続することによるリスクは大幅に増加しています。

企業ネットワークには、ネットワーク トラフィック セキュリティ (電子メール ウイルス検索プログラム、スパム電子メール ブロック プログラム、Web プロキシ サーバー、その他のネットワーク ソリューション) をはじめとするさまざまな防御策が実装されています。サーバー向けソリューションを使用することによって、電子メール ウイルス、ネットワーク ハッキングなど、多くの脅威を回避できます。ただし、企業ユーザーはさまざまな方法で情報を受け取ります。たとえば、顧客やビジネス パートナーから CD-ROM、DVD-ROM、USB ドライブなどの物理的なデータ移送媒体を受け取ることが考えられます。また、これらのユーザーは、一見無害に見えるファイルやインストーラに潜んでいるウイルスやスパイウェアをダウンロードします。これらの脅威はネットワーク セキュリティ ソリューションを使用しても回避できない場合があります。

サーバー側のセキュリティ ソリューションは、ファイアウォールで保護されたネットワークに侵入しようとする脅威には適切に対処できます。ただし、モバイル コンピューティングとワイヤレス ホットスポットの発達によって、組織に新たな脆弱性がもたらされました。たとえば、社外にいる従業員は、強固なセキュリティで保護されていないカフェやホテルのアクセス ポイント、アクセスが制限されないホットスポット、自宅のネットワーク内などでラップトップを使用します。社外でのセキュリティ対策は、たいてい場当たり的なものになってしまいます。重要なのは、一見魅力的なフィッシング詐欺のリンクを誤ってクリックすることによってデバイスを破損しないようにすることです。アクセスが制限されないネットワーク上でデバイスを使用することは、無体財産と機密情報を公開しているようなものです。ファイアウォールで保護された企業内に戻ってきたラップトップは、企業

ネットワークに脆弱性をもたらします。

最近公開されたマイクロソフト セキュリティ インテリジェンス レポート (2007 年 7 ～ 12 月)[[1]](#footnote-1) によると、業界全体で明らかになった脆弱性の数は、2006 年以降減少しています (図 2 参照)。ただし、社外で作業するシナリオが増加するにしたがって、モバイル コンピューティングやインターネット接続によってもたらされる脅威の数も増加しています。

脅威は対象を絞った攻撃によってもたらされることもありますが、多くの脅威は、ユーザーが日常的な作業の中で無意識にマルウェアやスパイウェアに遭遇したときに発生します。たとえば、ユーザーが単に Web サイト上または電子メール内のリンクをクリックしただけで、悪意のあるオブジェクトが自動的にダウンロードされて開かれ、コンピュータ内に侵入することがあります。この攻撃は、ポップアップに関する警告を複数使用しても回避できない場合があります。

図 . 業界全体で明らかになった脆弱性の数
 (2003 ～2007 年)

したがって、クライアント側のセキュリティ対策を実装する必要があります。従業員は、インターネットを使用して、コミュニケーション、調査、および生産性向上を実現しています。企業はますますモバイル環境、およびパートナーのシステムや外部のプロバイ

|  |
| --- |
| **一般に定義されているセキュリティの脅威** |
| **マルウェア :** システムを破損または中断させるように設計された悪意のあるプログラムやファイル (ウイルス、ワーム、ルートキット、トロイの木馬など)。**スパイウェア :** インターネットにアクセスしているユーザーの情報を、気付かないうちに収集するソフトウェア。通常この情報は広告目的で使用されますが、電子メール アドレス、パスワード、クレジット カードの情報などが収集される場合もあります。**ウイルス :** 気付かないうちにシステム内に侵入し、そのシステムやデータを破壊するコード。多くの場合、他のプログラムやドキュメント内に潜んでいます。**対象を絞った攻撃/サービス拒否　（Dos） 攻撃:** 情報システムの脆弱性や設計上の制限を利用して、正当なユーザーがリソースにアクセスできないようにすることを目的とした、悪意のあるユーザー (無意識に関与するユーザーを含みます)、プロセス、およびシステムによる試み。 |

ダとの相互接続に依存するようになっています。これらの基本的な事実は既に定着しています。

その結果、企業にはクライアント オペレーティング システム、アプリケーション サーバー、およびネットワークの境界に対するきめ細かな保護と制御を提供するセキュリティが必要になりました。また、その対策を導入することによって、作業やコミュニケーションを妨げることなく強固なセキュリティを提供する必要があります。

## 重要な機能を欠いている既存の製品

既存のクライアント セキュリティ ソフトウェアでは、脅威に対する包括的な保護、統合機能、およびレポート機能が提供されません。また、現在市販されているソフトウェアには、次のような重大な欠点があります。

* **制限されたマルウェアの検出機能 :** 特定のウイルスを検出できず、スパイウェアに対する保護も提供されません。
* **ウイルス エンジンの複雑な更新作業 :** 展開前のテストとメンテナンスが必要になります。
* **インフラストラクチャに関する追加要件 :** ウイルス署名と構成を管理するためにこれらを実装する必要があります。
* **不十分なレポート機能 :** 複数の情報源を参照したり、手動でそれらを更新したりする必要があります。

これらの欠点は、次のようなさまざまな点で組織に影響を与えます。

* **従業員の生産性低下 :** パフォーマンスとリソースの可用性が低下することによって、従業員の生産性が低下します。
* **承認されないアクセス :** 機密情報、アクセスが制限された情報、および個人情報へ、承認を得ていないアクセスが発生します。
* **ネットワークの障害**
* **頻繁な修復、再インストール、交換 :** サーバーやデスクトップのソフトウェアやハードウェアを修復、再インストール、または交換する機会が増加します。

# 実績のあるソリューションと測定可能な TCO の削減量

Microsoft Forefront Client Security は、実績のあるソリューションを企業に提供します。Value Prism Consulting による調査の結果と分析によって、大幅に TCO を削減できること、およびその後もレポート機能と管理機能から得られるメリットを通じてコストの削減を継続できることがわかりました。調査に参加した顧客は、Forefront Client Security の展開に平均 16.5 ドルを費やしましたが、セキュリティに関する問題の発生数を平均 85% 減少させることができ、それによって 1 年間に 24 ドルの節約を実現しました。また、いくつかの組織は、その他の IT 管理作業の生産性が向上することによって、IT にかかるコストをさらに 7.5 ドル削減できる可能性があると評価しました。投資額の回収に 1 年以上かかると評価した企業は 1 社だけであり、その他の企業の大部分は 2 ～ 7 か月で回収が可能であると評価しました。

Value Prism Consulting は、Microsoft Forefront Client Security の早期導入企業 8 社に対してインタビューを実施しました。このうち 4 社は米国、2 社はオーストラリア、1 社はヨーロッパ、そしてもう 1 社はシンガポールを拠点としています。これらの企業は、Symantec、McAfee、Computer Associates などのクライアント セキュリティ ソリューションから Forefront Client Security に切り替えました。

これらの組織は中規模から大規模の企業であり、平均 6,600 人の従業員を抱えています (その中で中間に位置する企業の従業員数は約 3,600 人です)。どの企業も、Microsoft Active Directory® とポリシーに基づいて Forefront Client Security を展開または構成しました。

### 調査に参加した顧客

|  |  |  |
| --- | --- | --- |
| **顧客名** | **業種** | **所在地** |
| **Allina** | 医療 | 米国 |
| **Analog Devices** | 製造 | 米国 |
| **Advantage Sales & Marketing** | サービス | 米国 |
| **CSR Limited** | 製造 | オーストラリア |
| **Des Moines School District** | 教育 | 米国 |
| **Konnex Dienstleistungen** | IT サービス | オーストリア |
| **National Roads and Motorists' Association** | サービス | オーストラリア |
| **PhillipCapital** | 金融サービス | シンガポール |

### TCO の概要データ

|  |  |  |
| --- | --- | --- |
| **カテゴリ** | **導入にかかるデスクトップ 1 台あたりのコスト** | **1 年間で削減できるデスクトップ 1 台あたりの TCO** |
| **展開および投資コスト** | 16.50 ドル |  |
| **一元的な保護** (セキュリティに関する問題のコストが減少します) |  | 24.00 ドル |
| **単純化された管理** (IT 管理作業が減少します) |  | 7.50 ドル |

### Forefront Client Security による脅威の排除

Forefront Client Security の特徴は、統合型のウイルス対策およびスパイウェア対策エンジン、他の IT 管理ソフトウェアと統合できる一元管理システム、およびリアルタイムのセキュリティ評価レポートです。

このソリューションでは、次のようなセキュリティが提供されます。

* **クライアントおよびサーバー オペレーティング システムのセキュリティ :** ウイルスとスパイウェアの両方からビジネス デスクトップ、ラップトップ、およびサーバー オペレーティング システムを保護できるので、容易に管理作業を行うことができます。

Forefront Client Security はマイクロソフトから提供されている他の Forefront Security ソリューションと統合されているので、次のようなセキュリティも提供されます。

* **サーバー アプリケーションのセキュリティ :** マイクロソフトから提供されているメッセージングおよびコラボレーション サーバー アプリケーションをウイルス、ワーム、スパム、および不適切なコンテンツから保護できます。
* **ネットワーク "境界" のセキュリティ :** 組織はファイアウォール、VPN、および SSL VPN 機能を使用して、サーバーやアプリケーションへのセキュリティで保護されたリモート アクセス、ブランチ オフィス間の接続とそれらのセキュリティ保護、および Web アクセスの保護を実現できます。

Forefront Client Security によって大幅にクライアントのセキュリティが強化され、セキュリティ関連コストが削減されます。

* **一元的な保護 :** ウイルス、スパイウェア、およびその他の既存の脅威や新しい脅威に対する保護が一元的に提供されます。インタビューに回答した企業の多くは、Forefront Client Security を使用することによってスキャンの質が大幅に向上したと報告しています。具体的には、より多くの問題がすばやく検出されたこと、およびマルウェアとスパイウェアの両方が確認されたことが挙げられました。
* **単純化された管理 :** 一元管理システムによって、管理作業が単純化されます。どの参加企業でも、セキュリティに関する問題の解決に必要なリソースと、ヘルプ デスクへのセキュリティに関する問い合わせ件数が減少しました。その結果、ネットワーク管理などのより重要な作業にリソースを割り当て直すことができました。
* **可視性と制御 :** 優先順位付けされた詳細なセキュリティ レポートによって、優れた可視性ときめ細かな制御が提供されます。インタビューに回答した企業の大部分は、以前に使用していたクライアント セキュリティ ソリューションでレポート システムを実装していませんでした。Forefront Client Security では、レポートを容易に構成し、デスクトップ環境の現在の状態を把握するための重要な資産としてそのレポートを活用できます。

# 一元的な保護

Forefront Client Security によって提供される高品質のセキュリティ ソリューションを使用して、ウイルスとスパイウェアの両方からコンピュータを保護できます。これによって、次のようなメリットとベスト プラクティスを得ることができます。

|  |
| --- |
| **ベスト プラクティス – Des Moines Public Schools**[[2]](#footnote-2) |
| Des Moines Public Schools では、Forefront Client Security を使用して、より効率的にシステムの脅威に対処できるようになりました。この学校のある学区では、学区内のコンピュータとネットワークへの広範なアクセスが許可されていますが、IT 管理者は 1 つのソリューションを使用して、マルウェアやウイルスの攻撃を受ける可能性を最小限に抑えることができます。 また、Des Moines Public Schools の IT 管理者は、マルウェアの定義が頻繁に更新されること、およびその他の更新が Microsoft Update によって配布されることからもメリットを得ることができます。 |

* IT 管理者は、1 つのアプリケーションを使用してスパイウェアとマルウェアの両方に対する保護を提供できます。
* Forefront Client Security によって、セキュリティに関する問題の発生数が減少し、それらの問題への対処にかかる時間も短縮されます。
* いくつかの参加企業では、これまでスパイウェアの取り締まりが義務付けられていなかったので、Forefront Client Security でスパイウェアとマルウェアの両方に対する保護が提供されることによって、これらの企業はさらに多くのメリットを得ることができます。
* いくつかの参加企業からは、Forefront Client Security によって、以前使用していたソフトウェアでは検出されなかった多くのウイルスが検出および駆除されたという報告を受けました。
* エンド ユーザーが作業を妨害される回数は、多くてもセキュリティ スキャンが実行されるときの 1 回のみです。

## セキュリティに関する問題の減少

組織は、1 つのアプリケーションでマルウェアとスパイウェアの両方に対処できることによって、ソフトウェアと管理にかかるコストを削減できます。インタビューに回答したどの企業もマルウェア対策ソフトウェアを使用していましたが、スパイウェア対策ソフトウェアの使用を義務付けていた企業は 2 社のみで、その他の企業はスパイウェア対策をエンド ユーザーの判断に任せていました。Konnex の代表取締役である Markus Kleinen は次のように述べています。「これまで、スパイウェアとマルウェアの両方に対しては適切な保護を提供できませんでした。」また、パフォーマンスに関する問題もありました。「以前使用していたソリューションでは、コンピュータのスキャンに時間がかかっていたので、従業員の生産性が低下していました。」[[3]](#footnote-3)

Forefront Client Security を導入することによって、一元的なソリューションが提供されます。シンガポールの金融サービス企業である PhillipCapital でシステム エンジニアを務める Ken Ong Kok Keng は次のように述べています。「金融機関としてコンピュータを厳重に保護することは、ビジネスのためだけでなく、政府規制に準拠するうえでも重要です。Forefront Client Security は、デスクトップ コンピュータをウイルスやスパイウェアから保護するのに役立ちます」

インタビューに回答した企業は、セキュリティに関する問題への対応にかかるコストを大幅に削減できました。これは、問題の発生数とそれぞれの問題の解決にかかるコストの両方を削減することによって実現されました。顧客はセキュリティが強化されたことをすぐに実感しました。いくつかの参加企業は、以前のセキュリティ ソフトウェアでは検出されなかったが Forefront Client Security の初回スキャンで検出された問題の数に言及しました。

|  |
| --- |
| **問題の減少によって節約できる金額を見積もる方法** |
| 1. デスクトップのセキュリティに関して 1 年間に発生する問題の数を特定します。この数を 15% (問題が 85% 減少することを反映します) で乗算します。
2. セキュリティに関する 1 つの問題 (またはヘルプ デスクへの問い合わせ 1 件) にかかるコスト (つまり標準的なコストである 75 ドル) でこの数を乗算します。
 |

レポート機能と可視性が強化されたことによって、セキュリティに関する問題をすばやく特定し、IT 部門にそのことを通知できるようになります (エンド ユーザーからヘルプ デスクに問い合わせがあって初めて問題を認識することはなくなります)。このため、すばやく問題に対応し、該当するコンピュータをネットワークから隔離できるようになり、その結果、企業全体に伝染する可能性がある問題の数が減少します。オーストラリアのシドニーを拠点とする National Road and Motor Association でサーバー デスクトップ チームの主任を務める Tom Sammons は次のように述べています。「私たちは保護されており、最新の対策を実装していると自信を持って言えます」

さらに、スキャンの実行時間やシステム リソースを効率的に使用できるので、エンド ユーザーへの影響も抑えられます。Forefront Client Security の製品テスト レポートを独自に作成した West Coast Labs からは次のような報告が寄せられています。「Forefront Client Security の最も印象的な特徴は、クライアント システム リソースに影響を与えないことです。」[[4]](#footnote-4)

調査に参加した企業は、セキュリティに関する問題の発生数が平均 85% 減少すると評価しました。TCO の分析によると、Forefront の前に使用していたソリューションでは、1 つの問題の解決に通常 75 ドルかかっていましたが、Forefront の使用によってこのコストが 25 ドルに減少し、1 年間で平均 24 ドルの TCO を削減できることが予想されます。

# 単純化された管理

|  |
| --- |
| **ベスト プラクティス – Analog Devices**[[5]](#footnote-5) |
| ボストンを拠点とする製造企業である Analog Devices は、セキュリティ関連の IT インフラストラクチャと、それに関連する管理プロセスの単純化に成功しました。この単純化は Forefront Client Security によって提供される次の機能によって実現されました。* Microsoft Windows Server™ Update Services を使用して新しいウイルス署名を配布します。Analog Devices では以前 12 箇所の配布ポイントを使用していましたが、この機能によってその必要がなくなりました。
* Active Directory と統合されているので、企業のデスクトップ向けウイルス対策ソリューションを管理するために独自の専用ツールを使用する必要がなくなります。
* デスクトップのセキュリティ状態を 1 つのレポートで毎日監視できます。これによって、システム管理者はすべてのコンピュータの状態をすばやく確認し、容易に特定のコンピュータの詳細情報を調べることができます。
 |

Forefront Client Security の管理ツールおよび機能によって、次に示す大幅な機能強化とメリットが IT 部門にもたらされます。

* Forefront Client Security を管理する IT 管理者は、ユーザーのデスクトップに 1 つのアプリケーションを手動で展開するか、標準的なイメージの一部として展開します。
* IT 管理者は、Active Directory のグループ ポリシーを使用して Forefront Client Security を管理します。たとえば、法規制に準拠していないコンピュータによるネットワークへのアクセスをブロックするポリシーを使用します。
* Forefront Client Security の署名の更新は、Windows Server Update Services (WSUS) を通じて自動的にすべてのコンピュータに展開されます。この展開時刻は、エンド ユーザーに影響を与えないように勤務時間外に設定することもできます。
* 調査に参加したいくつかの企業は、強化された管理ツール、対処する必要があるセキュリティに関する問題の減少、およびソフトウェアにかかるコストの削減によって、IT に関する大きなメリットを得ることができました。

## IT 管理コストの削減

|  |
| --- |
| **各組織にとってのメリット** |
| どの組織でも Forefront Client Security のメリットを実感できるとは限りません。このメリットを評価するには、まず現在のスタッフの配置と、現在 IT セキュリティの管理を担当しているリソースを他の職務で有効に利用できるかどうかを評価します。次に、Forefront Client Security を展開した後、現在セキュリティの解決を担当しているリソースを実際にどれぐらい再配置できるかを確認します。その後、IT に関するコストを平均でどれぐらい削減できるか、および (以前は人員が不足していた) 新しい役割を担う IT 部門のスタッフにメリットがもたらされるかどうかを評価します。 |

組織は Forefront Client Security によって提供される次の機能を使用してデスクトップ セキュリティの管理を強化できます。

* グループ ポリシーによって管理された容易な展開
* 一元化されたツールを使用した容易な毎日の管理作業
* WSUS を使用して自動化された署名の更新の展開

調査に参加した企業は、使いやすく有益な情報を提供する Forefront Client Security の管理システムに基づき、WSUS を使用して署名の更新を展開することによって、デスクトップ セキュリティの管理に必要な時間を短縮できました。また、法規制に準拠していないコンピュータの検出と更新に必要な時間も短縮できました。

Des Moines Public Schools でネットワーク スペシャリストを務める William Fulton は次のように述べています。「WSUS を使用してウイルス定義の更新を展開してみましたが、非常に容易にプロセスを完了できたので、今ではどのマイクロソフト製ソフトウェアの更新を展開するときでも WSUS を使用しています。」

調査に参加したすべての組織が IT の管理に関するメリットを得ることができたわけではありません。その理由は、既に IT インフラストラクチャを強化するための投資を行っていたからです。ただし、このカテゴリでのメリットを認めた組織は、1 年間でデスクトップ 1 台あたり平均 7.5 ドルのコストを削減できると評価しました。これは、新しい人員を雇用することなく、既存の人員をより重要な IT 関連の役割に再配置することによって実現されます。Fulton は次のように述べています。「マルウェアの攻撃が原因で破損したコンピュータのイメージを再作成する必要がなくなるので、今まで技術的なサービスに費やしていた時間を非常に有効に利用できるようになります。」[[6]](#footnote-6)

# 可視性と制御

|  |
| --- |
| 「今までよりもシステムの状態を把握しやすくなったので、セキュリティに関する問題をすばやく特定し、多くの問題を完全に回避できるようになりました。新しいセキュリティ ソリューションを探している企業は、Forefront Client Security を試してみることをお勧めします。統合によるメリット、また優れたレポート機能だけでもこのソリューションを導入する価値はあります。」[[7]](#footnote-7)Thomas Thiew (IT マネージャ、PhillipCapital) |

IT 管理者は、自動化された機能豊富な Forefront Client Security のレポートにアクセスし、次のような重要なメリットを得ることができます。

* スパイウェアやマルウェアの攻撃に基づく脅威、最新のセキュリティ更新プログラムが適用されていないコンピュータ、および最近ネットワークに接続していないコンピュータに関する情報をまとめた詳細なレポートを利用できます。
* インタビューに回答した企業の中で、以前にセキュリティ レポートを作成していた (定期的でないものも含みます) 企業はごくわずかです。これらの企業は、1 時間から 1 週間かけてレポートを作成していました。
* インタビューに回答したすべての企業は、Forefront Client Security のレポート機能、問題をすばやく警告する機能、およびすべてのコンピュータの状態を要約した "スナップショット" レポートを頻繁に作成する機能によって、大きなメリットを得ることができました。

## 可視性と制御によって提供される強力な IT ツール

West Coast Labs が 2008 年 4 月に作成した Forefront Client Security の製品テスト レポートでは、Forefront のレポート作成機能が "競合他社との大きな差別化要素" として評価されています。さらにこのような記述もありました。「このソリューションのレポート機能では、リアルタイム レポート、重要な問題と評価スキャンに基づく概要レポートなど、非常に役立つ情報が提供されます。これは、Forefront Client Security が Microsoft® SQL

|  |
| --- |
| **ベスト プラクティス – PhillipCapital**[[8]](#footnote-8) |
| PhillipCapital は、Forefront Client Security のレポートを使用して、自社の IT 環境のセキュリティと状態に関する情報をリアルタイムで収集できます。また、常時実行されるスキャンを使用して、セキュリティ更新プログラムが適用されていないコンピュータや未構成のコンピュータを IT ポリシーに基づいて確認できます。さらに、IT 管理者は環境内で脅威が検出された場合、そのことを通知するセキュリティ警告を受け取ることができます。Thiew は次のように述べています。「Forefront Client Security によって提供される優れたレポート作成機能は、特に展開時や更新時に非常に役立ちます。今までよりもシステムの状態を把握しやすくなったので、セキュリティに関する問題をすばやく特定し、多くの問題を完全に回避できるようになりました。」 |

Server® や Microsoft® Operations Manager などの既存のマイクロソフト製テクノロジと連

携し、効率化されたソリューションを提供することによって実現されます。」[[9]](#footnote-9)

調査に参加した企業は、Forefront Client Security のレポート作成機能とデータ アクセス機能を高く評価しています。PhillipCapital で IT マネージャを務める Thomas Thiew は次のように述べています。「Forefront Client Security によって提供される優れたレポート作成機能は、特に展開時や更新時に非常に役立ちます。今までよりもシステムの状態を把握しやすくなったので、セキュリティに関する問題をすばやく特定し、多くの問題を完全に回避できるようになりました。新しいセキュリティ ソリューションを探している企業は、Forefront Client Security を試してみることをお勧めします。統合によるメリット、また優れたレポート機能だけでもこのソリューションを導入する価値はあります。」[[10]](#footnote-10)

Analog Devices でデスクトップ コンピューティング サービス部門のマネージャを務める Susan Blandy は次のように述べています。「Forefront Client Security のレポート機能は非常に使いやすく、この機能を使用して有用なデータをシステムから入手できます。毎日受信する電子メール メッセージには、クライアントのセキュリティに関する簡潔な 1 ページのレポートが含まれています。必要であれば、マルウェアによってもたらされる脅威、攻撃を受けたコンピュータや脆弱になっているコンピュータなどに関する詳細な情報をそこから得ることができます。Forefront Client Security のレポートを使用すると、社内で使用されているデスクトップ システムのセキュリティ状態を非常にすばやく確認できます。」[[11]](#footnote-11)

セキュリティに関する問題を把握しやすくなったこと、およびソフトウェアの更新やセキュリティ更新プログラムなどのその他のセキュリティ情報が通知されることによって、組織は今までとは異なる種類のセキュリティ情報にアクセスできるようになりました。調査に参加した企業の大部分は、エンド ユーザーからヘルプ デスクに問い合わせがあるまで、セキュリティに関する問題を把握できませんでした。Konnex Dienstleistungen でプロジェクト マネージャを務める Harald Gumpenberger は次のように述べています。「驚くべきことに、このソリューションでは、今までまったく入手できなかったセキュリティ情報が提供されます。Forefront Client Security はシステムの情報を収集し、その情報からリスクを識別します。たとえば、ドメイン アカウントにいくつかのコンピュータのローカル管理者特権が与えられている場合、これはリスクとして識別されます。また、このソリューションではスパイウェアのインスタンスも検出されます。このような機能は、以前使用していたソリューションに比べると大幅に優れています。」[[12]](#footnote-12)

1 つ例を挙げますが、参加企業へのインタビューで「Forefront Client Security を展開する前、特定の時点でセキュリティ要件を満たしていないデスクトップは何台ありましたか。」と質問したとき、ほぼすべての組織から「わかりません。」という答えが返ってきました。「現在セキュリティ要件を満たしていないデスクトップは何台ありますか。」と質問したときは、「少々お待ちください。」という答えが返ってきた後、担当者が Forefront Client Security のレポートを開き、その時点で検出されているセキュリティとソフトウェアの更新に関する問題の正確な数を報告してくれました。

このカテゴリにおける TCO の削減量は計測されませんでした。その理由は、参加企業の大部分が比較対象となるレポート作成システムを以前使用していなかったからです。ただし、企業に非常に大きなメリットがもたらされることが予想されます。たとえば、可視性の向上によってレポートの管理作業が容易になること、セキュリティ管理の範囲がデスクトップ ソフトウェアの更新状態にまで拡張されること、セキュリティに関する致命的な問題の発生を回避できることなどが挙げられます。

# Forefront Client Security のコストと展開

## ライセンス、ハードウェア、および展開コスト

調査に参加した企業は、Forefront Client Security の導入にかかる全体的なコストをデスクトップ 1 台あたり平均 16.5 ドルと見積もりました。このコストの内訳は次のとおりです。

* インストールやトレーニングなど、展開に必要な作業と費用。
* Forefront Client Security などのソフトウェアと必要なサーバー コンポーネント。
	+ Forefront Client Security Management Console
	+ Windows Server Update Service (無料のサービスですが、専用の Windows Server コンピュータが必要です。)
	+ SQL Server (Forefront Client Security Management Console に同梱されているバージョンを購入することによって安価に入手できます。)
	+ Microsoft Operations Manager (いずれかのバージョンが Forefront Client Security Management Console に同梱されています。)
* Forefront を展開するために購入した新しいサーバーに必要なハードウェア

この調査に参加した企業が Forefront の導入に費やしたコストは、当初の予想を下回りました。その理由は、1 社を除くすべての参加企業が、次に示す 1 つ以上の方法で TCO を削減できたからです。

* Forefront Client Security を含む既存の Enterprise クライアント アクセス ライセンス (ECAL) の契約内容 (11 種類の製品を含むマイクロソフトのライセンス プログラム)[[13]](#footnote-13) を活用する。
* サーバーまたはソフトウェアを再利用する。
* SQL Server の実行時ライセンス (Forefront Client Security と共に使用することのみが許可されるライセンス) が付属した Forefront Client Security Management Console を購入する。
* ハードウェアに関する追加コストが発生しないように、既存の仮想ネットワーク環境に Forefront Client Security を展開する。 (詳細については次のセクションを参照してください。)

すべての参加企業がハードウェアおよびソフトウェア一式を購入し直した場合、総コストはデスクトップ 1 台あたり約 27 ドルになります。サーバー、仮想化、およびボリューム ライセンスを再利用することによって、これらの企業はデスクトップ 1 台あたり平均 10 ドルの節約を実現しました。

詳細については、Microsoft Forefront Security の購入方法に関するページ ([http://www.microsoft.com/forefront/clientsecurity/howtobuy/default.mspx](http://www.microsoft.com/japan/forefront/howtobuy/default.mspx))（英語） を参照してください。

## 仮想化

調査に参加した企業の半数が、新規または既存の仮想ネットワーク環境内で Forefront Client Security 管理サーバーを実装することによって、展開コストを大幅に削減できました。NMRA で IT マネージャを務める Tom Sammons は次のように述べています。「基本的に私たちはネットワーク環境のあらゆる要素を仮想化しており、マイクロソフトのすばらしいサポートによって、Forefront Client Security 管理サーバーも仮想化することができました。」

 図 3 は、仮想サーバー環境で個々のサーバーがどのように最適化されるかを大まかに示しています。仮想ネットワーク環境は管理しやすく、ソフトウェアも効率的に実行できるので、必要なサーバーの数が減少し、管理コストを削減できます。Microsoft Virtual Server の詳細については、<http://www.microsoft.com/japan/windowsserversystem/virtualserver/default.mspx> を参照してください。

インタビューに回答し、新規または既存の仮想ネットワークに Forefront Client Security を展開したすべての顧客が、仮想ネットワークを使用しない組織よりも低いコストで展開を実現できました。ある企業は、既存の仮想環境が Forefront 管理およびレポート サーバーを追加できるだけの容量を備えていたので、新しいハードウェアへの投資を行う必要がありませんでした。Advantage Sales and Marketing でシステム エンジニアとシニア テクノロジ スペシャリストを務める Hessam Toudiee は次のように述べています。「私たちは既存のシステムとテクノロジを使用して、仮想ネットワークに Forefront Client Security 管理サーバーを実装しました。」

図 . 標準的な環境と仮想環境の比較。左側は典型的な Forefront Client Security ネットワーク環境、右側は仮想ネットワークを示しています。

全体的に見て、仮想ネットワークを使用した組織では、物理ネットワークを使用した他の 4 社の平均と比べて 43% 低いコストで展開を完了できました。また、仮想化を活用する組織は管理コストも削減できるので、1 年間でさらに多くのメリットを見込むことができます。

# まとめ

Microsoft Forefront Client Security は、包括的なセキュリティ アーキテクチャ (ポリシーの管理、ネットワーク セキュリティ、インターネットのセキュリティ保護などを目的としたその他の Forefront ソリューションを含みます) の重要な構成要素です。Forefront Client Security ではマルウェアとスパイウェアに対するトップレベルの保護が提供されるので、セキュリティが侵害される確率を大幅に低下させることができます。また、包括的なレポート作成機能、問題をすばやく通知する機能、およびセキュリティに関するその他の機能強化がシステムに組み込まれることによって、他の追随を許さない高度なセキュリティ機能およびツールが提供されます。

Forefront Client Security を導入するには追加のサーバー ハードウェアおよびソフトウェアが必要になる場合もありますが、調査に参加した企業からの報告で示された大幅なコストの削減によって、その投資を上回る利益を得ることができます。もう一度述べますが、これらの参加企業は、問題の発生数が減少することによって 1 年間で 24 ドルの節約を実現し、それに加えて 7.5 ドルの IT コストの削減を見込むことができました。これに対し、展開コストはデスクトップ 1 台あたり平均 16.5 ドルしかかかりません。投資額の回収に 1 年以上かかると評価した企業は 1 社だけであり、その他の企業の大部分は 2 ～ 7 か月で回収が可能であると評価しました。

このソリューションを導入することによって、セキュリティに関する問題を回避し、脆弱性を低下させ、総保有コストを削減できるので、全体的に見て、優先度の高いセキュリティの課題に対処するのに役立つ方法であると言えます。

# 付録 A : 調査の詳細と方法論

経営コンサルティングおよび財務分析企業の Value Prism Consulting は、2008 年 3 月と 4 月に、Microsoft Forefront Client Security の早期導入企業 8 社 (マイクロソフトの Technology Adoption Program に参加している企業) に対してインタビューを実施しました。このうち 4 社は米国、2 社はオーストラリア、1 社はヨーロッパ、そしてもう 1 社はシンガポールを拠点としています。これらの企業は、Symantec、McAfee、Computer Associates などのクライアント セキュリティ ソリューションから Forefront Client Security に切り替えました。

これらは中規模から大規模の組織であり、平均 6,600 人の従業員を抱えています (その中で中間に位置する企業の従業員数は約 3,600 人です)。どの企業も Active Directory と Microsoft Internet Explorer® 6 または 7 を使用し、ポリシーに基づいて Forefront Client Security を展開および構成しました。半数の企業は Windows ファイアウォールを使用し、もう半数の企業は Microsoft Operations Manager を使用しています。

大部分の企業は、Forefront Client Security とサーバー管理ソフトウェアを展開するために少なくともいくつかのソフトウェアとハードウェアを追加で購入しましたが、1 社だけはすべてのサーバー ソフトウェアを既存のサーバーに展開しました。

インタビューに回答した企業のうち 3 社は、Forefront Client Security 管理サーバー、SQL Server データベース、Microsoft Operations Manager および WSUS サーバー ソフトウェアを仮想ネットワーク環境に展開しました。1 社は仮想環境に WSUS のみを展開しました。

いくつかの企業では、Forefront Client Security のライセンスにかかるコストが以前に使用していたソリューションよりも安価だったので、1 年間でクライアント セキュリティ ソフトウェアにかかるコストを削減できました。これらの顧客の購入費用は 0 ドルになります (収益に貢献しないコストは発生しません)。その他の顧客には、Forefront Client Security のライセンス価格が使用されます。

サーバーとソフトウェアについては、ハードウェアおよびサーバー ソフトウェアのコストを統一するために、基準コストが使用されました。このコストは、サーバー コンピュータは 5,000 ドル、Windows Server は 5,000 ドル、SQL Server は (1 プロセッサあたり) 15,000 ドルまたは 2,500 ドル (Forefront に付属しているバージョン)、Microsoft Operations Managerは 2,500 ドル (個別に購入した場合) または無料 (Forefront Client Security Management Console に付属しているバージョン)、Forefront Client Security Management Console は 2,500 ドル (SQL Serverと Microsoft Operations Managerを所有していない場合) です。

IT に関する生産性の計算には、1 時間あたり 35 ドルという標準的な賃金が使用されました。例外として、2 社ではより安価な 25 ドルが 1 時間あたりの賃金として使用されるという報告を受けたので、その金額が使用されました。

# 付録 B : 調査に参加した企業

|  |  |
| --- | --- |
| **顧客** | **詳細** |
| **Allina Hospitals & Clinics**医療米国 | ミネソタ州ミネアポリスを拠点とする Allina Hospitals & Clinics は、ミネソタ州とウィスコンシン州で病院、診療所、およびその他の医療サービス施設を運営しています。23,000 人を超える従業員が、11 箇所の病院、75 箇所の診療所、その他のさまざまな医療施設に勤務しています。  |
| **Analog Devices**製造米国 | Analog Devices は、10,000 種類を超えるさまざまなアナログ混合信号処理およびデジタル信号処理用の高性能集積回路を設計、製造、および販売しています。これらの回路は、携帯電話、液晶テレビ、デジタル カメラなどの製品で使用されます。 |
| **Advantage Sales & Marketing, LLC**サービス米国 | カリフォルニア州アーバインを拠点とする Advantage Sales and Marketing, LLC は、委託販売、商品化計画、部門管理、およびマーケティングを専門に扱う有数の販売およびマーケティング代理店です。 |
| **CSR Limited**製造オーストラリア | CSR Limited はオーストラリアを拠点とし、アルミニウム、砂糖製品 (純粋エタノールなど)、および建造物を生産する大手の事業会社です。従業員数は約 4,500 人です。 |
| **Des Moines SchoolDistrict**教育米国 | アイオワ州の中心部を拠点とする Des Moines Public Schools は、小学校から高校までの 32,000 人の生徒を抱えており、5,000 人を超える従業員が勤務しています。この学区では、自宅のコンピュータや 60 箇所を超える施設でコンピューティング資源とインターネットへのアクセスを提供することによって、カリキュラムを強化しています。 |
| **Konnex Dienstleistungen**IT サービスオーストリア | Konnex Dienstleistungen は、オーストリアを拠点とし、40 箇所のオフィスに勤務する 1,800 人の従業員を抱える親会社の BBRZ Gruppe に IT サービスを提供する、グループの内部企業です。BBRZ Gruppe は、事故や重病に苦しんだ人々の職場復帰を支援するために、職業訓練や社会人教育、およびさまざまな形態での雇用機会を提供しています。 |
| **National Roads and Motorists' Association**サービスオーストラリア | 会員制の共済組織である NMRA は、ニューサウスウェールズ州とオーストラリア首都特別地域で、けん引車サービス、旅行情報サービス、車検などのサービスを提供しています。また、NMRA は他の旅行およびレクリエーション企業の持株会社でもあります。 |
| **PhillipCapital**金融サービスシンガポール | 1975 年に Phillip Securities として設立された PhillipCapital は、シンガポール内外に共通の株主を持つ独立系企業のグループです。これらの企業は、個人、小売店、企業、および公共機関にさまざまな金融サービスを提供しています。PhillipCapital はアジアとヨーロッパに 2,500 人の従業員を抱えており、10 箇所の金融中心地にオフィスを構えています。 |

このドキュメントに記載されている情報は、このドキュメントの発行時点におけるマイクロソフトの見解を反映したものです。マイクロソフトは市場の変化に対応する必要があるため、このドキュメントの内容に関する責任をマイクロソフトは問われないものとします。また、発行日以降に発表される情報の正確性を保証できません。

このホワイト ペーパーに記載された内容は情報の提供のみを目的としており、明示、黙示または法律の規定にかかわらず、これらの情報についてマイクロソフトはいかなる責任も負わないものとします。

お客様ご自身の責任において、適用されるすべての著作権関連法規に従ったご使用を願います。このドキュメントのいかなる部分も、米国 Microsoft Corporation の書面による許諾を受けることなく、その目的を問わず、どのような形態であっても、複製または譲渡することは禁じられています。ここでいう形態とは、複写や記録など、電子的な、または物理的なすべての手段を含みます。ただしこれは、著作権法上のお客様の権利を制限するものではありません。

マイクロソフトは、このドキュメントに記載されている内容に関し、特許、特許申請、商標、著作権、またはその他の無体財産権を有する場合があります。別途マイクロソフトのライセンス契約上に明示の規定のない限り、このドキュメントはこれらの特許、商標、著作権、またはその他の無体財産権に関する権利をお客様に許諾するものではありません。

 2008 Microsoft Corporation. All rights reserved.

Microsoft、Forefront、SQL Server、Active Directory、および Windows は米国 Microsoft Corporation の米国またはその他の国における登録商標または商標です。

記載されている会社名、製品名には、各社の商標のものもあります。

1. マイクロソフト セキュリティ インテリジェンス レポート (2007 年 7 ～ 12 月、Microsoft Corporation) [↑](#footnote-ref-1)
2. <http://www.microsoft.com/casestudies/casestudy.aspx?casestudyid=201421> (英語) [↑](#footnote-ref-2)
3. <http://www.microsoft.com/casestudies/casestudy.aspx?casestudyid=4000000072> (英語) [↑](#footnote-ref-3)
4. <http://westcoastlabs.com/downloads/productTestReport_0051/Forefront_Client_Security.pdf> (英語) [↑](#footnote-ref-4)
5. <http://www.microsoft.com/casestudies/casestudy.aspx?casestudyid=201421> (英語) [↑](#footnote-ref-5)
6. <http://www.microsoft.com/casestudies/casestudy.aspx?casestudyid=201288> (英語) [↑](#footnote-ref-6)
7. <http://www.microsoft.com/casestudies/casestudy.aspx?casestudyid=201398> (英語) [↑](#footnote-ref-7)
8. <http://www.microsoft.com/casestudies/casestudy.aspx?casestudyid=201398> (英語) [↑](#footnote-ref-8)
9. http://westcoastlabs.com/downloads/productTestReport\_0051/Forefront\_Client\_Security.pdf [↑](#footnote-ref-9)
10. <http://www.microsoft.com/casestudies/casestudy.aspx?casestudyid=201398> (英語) [↑](#footnote-ref-10)
11. <http://www.microsoft.com/casestudies/casestudy.aspx?casestudyid=201421> (英語) [↑](#footnote-ref-11)
12. <http://www.microsoft.com/casestudies/casestudy.aspx?casestudyid=4000000072> (英語) [↑](#footnote-ref-12)
13. Enterprise クライアント アクセス ライセンスの詳細については、http://www.microsoft.com/japan/calsuites/enterprise.mspx を参照してください。 [↑](#footnote-ref-13)