# Microsoft Forefront コードネーム "Stirling" Beta 2 のプライバシーに関する声明

最終更新日時 : 2009 年 06 月

Microsoft® では、お客様のプライバシー保護に尽力し、個人のコンピューティングで望まれるパフォーマンス、パワー、および利便性を実現する製品を提供するためにも努力しています。この「プライバシーに関する声明」では、Microsoft Forefront™ Client Security コードネーム "Stirling" Beta 2 (以下「Client Security」といいます) によるデータ収集およびデータの用途の多くの点についてご説明します。この声明は、インターネットとの通信機能を重点的に扱うものであり、すべてを網羅することは意図していません。Client Security 以外のオンラインまたはオフラインの Microsoft のサイト、製品、またはサービスには適用されません。

Forefront Client Security は、ビジネスで使用しているデスクトップ、ラップトップ、サーバー オペレーティング システムをマルウェアから保護する統合マルウェア対策ソフトウェアです。Forefront Client Security は、集中管理による高い管理性と脅威や脆弱性の迅速な検出により、ウイルス、ワーム、トロイの木馬などの従来型の脅威に加えて、スパイウェアやルートキットなどの新たな脅威にも対応します。Forefront Client Security ソリューションには、次の 2 つの部分があります。1 つ目は Client Security エージェントで、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 システムにインストールされ、スパイウェア、ウイルス、およびルートキットなどをリアルタイムで防ぎ、スケジュールされたスキャンを実行します。2 つ目は Client Security 中央管理サーバーで、管理者はこれにより、あらかじめ構成したマルウェア対策エージェントやカスタマイズしたマルウェア対策エージェントを容易に管理および更新することができ、また環境のセキュリティ状態に関するレポートや警告を生成できます。

**ユーザーの個人情報の収集および用途**

お客様個人を特定する情報やお客様への連絡を取るための情報が必要な場合、その点を明確にして情報を依頼いたします。お客様から収集する個人情報は、Microsoft およびその関連会社ならびに提携企業により、お客様から要求または承認されたサービスの提供またはトランザクションの実施に使用されるほか、お客様が使用している製品またはサービスに関してお客様から提供されたフィードバックに関する追加情報をお尋ねするために使用する場合や、ソフトウェアに関する重要な通知を提供する場合、また製品またはサービスを向上する目的 (たとえば、バグやアンケート用紙に関するお問い合わせ) で使用されます。

この声明での説明に該当するものを除き、お客様が提供する個人情報をお客様の同意なく第三者に委譲することはありません。Microsoft は、製品やサービスに関するお客様からの質問への回答や Microsoft のサービスに関する統計分析の実行など限定されたサービスの代行を他社に依頼する場合があります。このような場合、サービスの遂行に必要とされる以上の個人情報を提供することはなく、サービスの遂行以外のいかなる目的でもこの情報を使用することが禁じられています。

法律により要求される場合、または次のような理由で必要であると誠実に認められる場合、Microsoft はお客様に関する個人情報を開示する場合があります。(a) 法令上の要請への準拠または Microsoft またはサイトを対象とする司法手続への順守、(b) Microsoft (契約の履行を含む) の権利の保護および擁護、(c) 緊急な状況で、Microsoft の従業員、Microsoft の製品またはサービスのユーザー、または公衆の個人的安全を保護するための活動。

Microsoft のソフトウェア、サイト、およびサービスにより収集された個人情報は、米国または Microsoft あるいはその提携企業、関連会社、またはサービス プロバイダが拠点を置くその他の国で保存および処理される場合があります。Microsoft のソフトウェア、サイト、またはサービスを使用することにより、お客様はこのような国外へのデータ転送に同意したものとします。Microsoft は、欧州連合 (EU) からのデータの収集、使用、保管に関して、米国商務省が定める Safe Harbor 規制に準拠しています。

**ユーザーのコンピュータに関する個人情報の収集および用途**

このソフトウェアは、お客様のコンピュータ (以下「標準コンピュータ情報」といいます) から特定の標準的な情報を収集し、Microsoft に送信するインターネット対応機能を搭載しています。標準コンピュータ情報には、IP アドレス、オペレーティング システム、および Web ブラウザなどお客様のコンピュータで使用するソフトウェアおよびハードウェアに関する特定の情報が含まれます。この「プライバシーに関する声明」に記載されている Client Security の各機能に関するプライバシーの詳細では、どのような情報が追加して収集され、どのような用途に使用されるかを記述しています。

**ユーザー情報のセキュリティ**

Microsoft は、お客様の情報のセキュリティ保護に真剣に取り組んでいます。多様なセキュリティ技術や手順を使用して、不正アクセス、使用、または開示からお客様の情報を保護しています。たとえば、サーバー認証やセキュア ソケット レイヤ (SSL) プロトコルなどの暗号化を使用することで、SpyNet スパイウェア対策コミュニティに提出されるレポートの内容を保護しています。

**詳細情報**

このプライバシーに関する声明についてのご質問は、電子メールで spypriv@microsoft.com までお問い合わせください。

SpyNet
Microsoft Corporation
One Microsoft Way

Redmond, Washington 98052 USA

## 固有の機能

この文書の以降の部分では、次のような固有の機能について説明します。

**Microsoft SpyNet**

**機能の内容 :** オンラインの Microsoft SpyNet コミュニティは、ユーザーが任意で参加する世界的なコミュニティです。Microsoft SpyNet を通じて、管理された Client Security のユーザーは、管理者の判断により、スパイウェアやその他の不要である可能性のあるソフトウェアを Microsoft に報告できます。Client Security グループ ポリシーを使用することで、管理者は不審な活動を行うプログラムまたはプログラム コンポーネントで、現在定義ライブラリに収録されていないものが Client Security に検出された場合、管理クライアントがいつでも Microsoft にレポートを送信するように構成できます。

**収集、処理、または送信される情報 :** Microsoft SpyNet レポートには、ファイル名、暗号化ハッシュ、ベンダ、サイズ、および日付スタンプなど問題となっているファイルまたはプログラムに関する情報が含まれています。また、ファイルの元の場所を示すために完全な URL を収集した場合、検索語やフォームに入力したデータなどの個人情報が含まれることもあります。レポートには、ソフトウェアが検出されたことを Client Security から通知されたときに取ったアクションが含まれる場合もあります。Microsoft SpyNet レポートは、この情報を含めることにより、悪意のあるソフトウェアや不要である可能性のあるソフトウェアの検出と除去に対する Client Security の効果を Microsoft が評価できるようにしています。レポートには標準コンピュータ情報も含まれており、次の場合に Microsoft に自動的に送信されます。

* Client Security が検出したソフトウェアにアクションを適用した場合。
* Client Security は、スケジュールされたスキャンを完了し、ユーザーの設定に従って検出したソフトウェアにアクションを適用します。

管理者は、管理クライアントが Microsoft SpyNet に参加するときに、基本メンバシップで参加するか、上級メンバシップで参加するかを選択できます。基本メンバ レポートには、上記の情報が含まれます。上級メンバ レポートはさらに包括的であり、ファイルのパスや部分的なメモリ ダンプなどの個人情報が含まれる場合があります。これらのレポートは、Microsoft SpyNet に参加している他のユーザーのレポートと共に、Microsoft の調査員がより迅速に新しい脅威を検出する上で役立ちます。次に、分析の条件に適合するプログラムに合わせてスパイウェア対策ソフトウェアまたはウイルス対策ソフトウェアの定義を作成し、更新された定義は Microsoft Update によってすべてのユーザーが使用できるようになります。

管理クライアントを Microsoft SpyNet に参加させることを管理者が決定した場合、Microsoft からサンプルの送信レポートを要求される場合があります。このレポートには、お客様のコンピュータに存在するファイルが含まれ、その中には Microsoft が不要である可能性のあるソフトウェアであると疑っているファイルが含まれることがあります。このレポートは以後の分析に使用されます。Microsoft にサンプル送信レポートを送信するかどうか毎回確認されます。プライバシーを保護するため、Microsoft に送信される情報は SSL を使用して暗号化されます。

レポートに個人情報が含まれている場合でも、Microsoft は、その情報を使用してお客様を特定したり連絡を取ったりすることはありません。

**情報の用途 :** Microsoft SpyNet レポートは、Microsoft ソフトウェアおよびサービスの向上に使用されます。統計、その他のテストまたは分析、トレンド分析、および定義の生成などにも使用される場合があります。レポートへのアクセスは、業務上レポートを使用する必要がある Microsoft の従業員、契約業者、およびベンダに限定されています。

**選択/制御 :**

Client Security サーバーの最初のインストールでは、管理された Client Security エージェントのユーザーについて、基本メンバシップで Microsoft SpyNet に参加するように規定で選択されます。管理者は、次の手順に従って、この既定の設定を変更できます。

1. Microsoft Forefront コードネーム "Stirling" 管理コンソールを開きます。
2. [ポリシー管理] タブをクリックします。
3. 左側のペインで [ポリシー] を展開します。
4. [コンピュータ ポリシー] をクリックします。
5. 右側のペインで、ロールベースの既定の設定グループを選択し、展開します (右クリックして [編集] をクリック)。オプションは次のとおりです。
	1. Default Client security Policy
	2. Client Security for Exchange server Policy
	3. Client Security for NPS server Policy
	4. Client Security for SharePoint server Policy
6. 新しい画面が表示されたら、[マルウェア対策ソフトウェア] マージ単位を選択します (これが表示されない場合は、SpyNet が設定されていないので何も変更する必要はありません)。
7. [詳細] を選択し、[SpyNet レポート] に移動します。
8. 参加モデルを選択します。
9. 保存して閉じます。

**定義の更新**

**機能の内容 :** Client Security は、Windows Server Update Services (WSUS) と Microsoft Update またはどちらか一方を使用して、管理クライアントにソフトウェアの更新や更新プログラムを展開します。更新プログラムのチェックが有効になっている場合、Client Security は自動的に新しいスパイウェア定義とウイルス定義、およびソフトウェア更新プログラムを毎時間チェックして、存在する場合は、ダウンロードします。この機能を有効にしておくと、Client Security を最新の状態に保つことができます。

**収集、処理、または送信される情報 :** ユーザーまたは管理者が自動更新を有効にすると、コンピュータは定期的に Microsoft サーバーと通信し、使用しているバージョンの Client Security でソフトウェア更新プログラムおよびスパイウェアとウイルス定義が最新かどうかを判断します。Client Security のバージョン情報と共に、標準コンピュータ情報が Microsoft に送信されます。収集される情報の詳細については、WSUS のプライバシーに関する声明 (<http://go.microsoft.com/fwlink/?LinkId=78929>) (英語) および Microsoft Update のプライバシーに関する声明 (<http://update.microsoft.com/microsoftupdate/v6/privacy.aspx?ln=ja-jp>) を参照してください。

お客様または管理者が自動更新を有効にしている場合、更新プログラムは自動的にダウンロードされインストールされます。

**情報の用途 :** Microsoft に送信される情報は、更新サービスの提供と向上に使用されます。情報の用途の詳細については、WSUS のプライバシーに関する声明 (<http://go.microsoft.com/fwlink/?LinkId=78929>) (英語) および Microsoft Update のプライバシーに関する声明 (<http://update.microsoft.com/microsoftupdate/v6/privacy.aspx?ln=ja-jp>) を参照してください。

**選択/制御 :** Update Services の使用は任意です。管理者は、Client Security による WSUS と Microsoft Update の使用方法を構成できます。お客様または管理者は、Client Security を手動で更新することもできます。詳細については、『Microsoft Forefront Client Security 展開ガイド』(<http://go.microsoft.com/fwlink/?LinkID=59684>) (英語) を参照してください。

**Microsoft 承認されたソフトウェア管理**

**機能の内容 :** Client Security には、Microsoft 承認されたソフトウェア管理ツール (ASM ツール) が含まれていることがあります。これは、アクセスしてデバイス上で実行したファイルに関する情報を収集し、この情報を Microsoft に送信するものです。

**収集、処理、または送信される情報 :** 実行するファイルに関する情報 (名前、バージョン、説明、その他のメタデータ) です。その他に、管理クライアント数、特定のファイルを持つ管理クライアント数、展開内で特定のファイルが許可されているかどうかなど、Client Security 環境に関する統計情報が含まれる場合があります。

**情報の用途 :** Microsoft に送信された情報は、問題を引き起こす可能性のあるソフトウェアを特定し、そのようなソフトウェアが管理クライアント上で実行されないようにするために使用されます。また、この製品および他の Microsoft の製品およびサービスの向上に使用される場合があります。

**選択/制御 :** ASM ツールの使用はオプションであり、既定では無効になっています。管理クライアントのカスタム ポリシーを構成して、この機能を有効にすることができます。詳細については、Client Security のドキュメントを参照してください。

**カスタマ エクスペリエンス向上プログラム**

**機能の内容 :** カスタマ エクスペリエンス向上プログラム ("CEIP") は、傾向や用途のパターンを調査するために、お使いのハードウェア構成に関する基本的な情報と、Microsoft のソフトウェアおよびサービスの使い方に関する情報を収集します。また、CEIP では、発生したエラーの種類と数、ソフトウェアおよびハードウェアのパフォーマンス、サービス速度の情報を収集します。ユーザーの名前、住所、その他の連絡先情報を収集することはありません。

**収集、処理、または送信される情報** **:** CEIP によって収集、処理、または送信される情報については、CEIP のプライバシーに関する声明 (<http://www.microsoft.com/products/ceip/JA-JP/privacypolicy.mspx>) を参照してください。

**情報の用途 :** この情報は、Microsoft のソフトウェアおよびサービスの品質、信頼性、パフォーマンスの向上に使用されます。この情報は、ユーザーの特定や連絡に使用されることはありません。

**選択/制御 :** セットアップ中に CEIP に参加する機会が提供されます。参加を後で取り消す場合は、Client Security をアンインストールするか、またはレジストリを次のように変更することで、CEIP をいつでもオフにできます。

**レジストリ キー** "HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Microsoft Forefront\Forefront System\Config" **は、値の名前 "SQMEnabled" および値の種類 "REG\_DWORD" で作成でき、値を "0x00000000" にすることができます。これにより、Microsoft Forefront コードネーム "Stirling" の CEIP レポート機能が無効になります。**

**警告 :** レジストリを誤って編集すると、システムに深刻な損害が発生する場合があります。レジストリを変更する前に、コンピュータの重要なデータをバックアップすることをお勧めします。手動で変更を適用した後に問題が発生した場合は、前回正常起動時の構成オプションを使用することもできます。