

Microsoft のデータ処理の方針に関する最新の情報は、「[Microsoft のプライバシーに関する声明](#)」を参照してください。ここでは、データにアクセスして制御するために提供される最新のツール、またプライバシーに関する質問がある場合の問い合わせ方法についても確認することができます。

Windows 8 および Windows Server 2012 のプライバシーに関する声明

ハイライトペン [声明](#) [機能に関する補足条項](#) [サーバーに関する補足条項](#)

このページの内容 **最終更新: 2012 年 8 月**

お客様の情報 全体的な [Windows 8 および Windows Server 2012 のプライバシーに関する声明](#) ("Windows のプライバシーに関する声明") から一部を抜粋したこのハイライトでは、Windows 8 および Windows Server 2012 ("Windows") で収集されるデータとその用途について、概要を説明します。主な対象はインターネットとの通信を行う機能であり、すべてを説明するものではありません。Microsoft の他のオンラインまたはオフラインのサイト、製品、およびサービスには適用されません。

お客様の選択肢

情報の用途

お問い合わせ方法

このプライバシーに関する声明は、以下の 4 つのセクションで構成されています。

- [ハイライト \(このページ\)](#)
- [声明](#)。Windows 全体のプライバシーに関する声明です。Windows 機能ごとの声明へのリンクも記載されています。

機能に関する補足条項。プライバシー関連の影響がある Windows 8 および Windows Server 2012 の機能について説明しています。

- サーバーに関する補足条項。プライバシー関連の影響がある Windows Server 2012 の追加の機能について説明しています。

オンラインのパーソナル コンピューター、個人情報、および家族の情報を保護する方法については、Microsoft セーフティとセキュリティ センターにアクセスしてください。

お客様の情報

- 一部の Windows 機能では、お客様の PC 内にある情報 (個人情報を含む) の収集や使用を許可するよう求められる場合があります。この情報は、全体的な [Windows のプライバシーに関する声明](#)、[機能に関する補足条項](#)、および [サーバーに関する補足条項](#) に従い、Windows によって使用されます。
- 一部の Windows 機能では、お客様の許可を得たうえで、個人情報がインターネット経由で共有される場合があります。
- ソフトウェアを登録する場合には、個人情報の入力が必要になります。
- Windows では、ソフトウェアの不正コピーを減らし、お客様に期待どおりのソフトウェア品質を享受していただくために、ライセンス認証を行っていただく必要があります。ライセンス認証を行うと、お客様の PC に関する一部の情報が Microsoft に送信されます。
- Windows へのサインインには、[Microsoft アカウント](#)を使用することもできます。この方法でログインすると、Windows の設定が同期され、アプリや Web サイトに自動的にサインインすることができます。Microsoft アカウントを作成する際には、特定の個人情報を入力するよう求められます。
- [追加情報](#)

[ページのトップへ](#)

お客様の選択肢

- Windows では、各種の Windows 機能でインターネット経由の情報転送がどのように行われるかを、さまざまな方法で制御できます。これらの機能を制御する方法については、機能に関する補足条項とサーバーに関する補足条項を参照してください。
- インターネットを使用する機能の中には、エクスペリエンスを向上させるために、既定で有効になっているものもあります。
- [追加情報](#)

[ページのトップへ](#)

情報の用途

- 収集された情報は、お客様が使用する機能を有効にしたり、お客様から要求されたサービスを提供したりするために使用されます。また、製品やサービスを改善させるためにも使用されます。Microsoft では、サービスの提供に役立てる目的で、Microsoft に協力している他の企業に情報を提供することがあります。これらの情報へのアクセス権は、業務で情報を使用する必要がある企業にのみ与えられます。これらの企業は、情報に対する守秘義務があり、他の目的でこの情報を使用することは禁じられています。
- [追加情報](#)

[ページのトップへ](#)

お問い合わせ方法

プライバシーに関する Microsoft の方針の詳細については、全体的な [Windows のプライバシーに関する声明](#) を参照してください。または、Microsoft の [Web フォーム](#) に従い、Windows によって使用されます。

[ページのトップへ](#)

Microsoft のデータ処理の方針に関する最新の情報は、「[Microsoft のプライバシーに関する声明](#)」を参照してください。ここでは、データにアクセスして制御するために提供される最新のツール、またプライバシーに関する質問がある場合の問い合わせ方法についても確認することができます。

Windows 8 および Windows Server 2012 のプライバシーに関する声明

ハイライトペン **声明** 機能に関する補足条項 サーバーに関する補足条項

このページの内容	これは、Windows 8 と Windows Server 2012 ("Windows") についての声明です。Windows の一部のコンポーネントについては、プライバシーに関する声明が別途用意されています。これらは、このページの右側に一覧でまとめられています。またこの一覧に
お客様の情報の収集と使用	は、Windows に関連するソフトウェアやサービスのプライバシーに関する声明と、以前のリリースのプライバシーに関する声明もまとめられています。
お客様のコンピューターに関する情報の収集および使用	特定の機能の詳細については、 機能に関する補足条項 および サーバーに関する補足条項 を参照してください。
お客様の情報のセキュリティ	この声明は、主にインターネットと通信する機能について述べたものであり、すべての機能について網羅的に述べたものではありません。
このプライバシーに関する声明の変更	
お問い合わせ先	お客様の情報の収集と使用
その他のプライバシーに関する声明	お客様から収集した個人情報は、Microsoft とその管理下にある子会社および関連会社が、お客様が使用する機能を有効にしたり、お客

Internet Explorer	様から要求または承認されたサービスを提供したり取引を遂行したりするために使用されます。またこれらの情報は、Microsoft の製品およびサービスを分析または改善するためにも使用されます。
Microsoft エラー報告サービス	この声明に記載がある場合を除き、お客様から提供された個人情報がお客様の同意なしに第三者に転送されることはありません。
Microsoft Online	Microsoft では、弊社サービスの統計的な分析の実行など、一部のサービスを他の企業に委託することがあります。Microsoft は、これらの会社に対して、サービスの提供に必要な個人情報のみを開示し、情報をそれ以外の目的で使用することを禁止しています。
Microsoft Windows 悪意のあるソフトウェアの削除ツール	マイクロソフトは、次の目的で、通信内容を含むお客様の情報にアクセス、あるいは情報を開示することがあります。(a) 法律を遵守するため、あるいは法律上の要請または手続きに応じるため。(b) マイクロソフトまたはそのお客様の権利または資産を保護するため(お客様によるソフトウェアの使用方法を定めたマイクロソフトの契約またはポリシーの履行を含む)。(c) マイクロソフトの従業員、お客様、あるいは公衆の個人的な安全を確保するために、情報へのアクセスや開示が必要と判断された場合に、善意に基づく行動をとるため。
更新サービス	
Windows Media Center	
Windows Media Player	
Windows 7	
	Windows 8 によって収集された情報または Microsoft に送信された情報は、Microsoft またはその関連会社、子会社、あるいはサービスプロバイダーが拠点を構える米国またはその他の国で保存および処理される場合があります。Microsoft は、欧州連合、欧州経済地域、およびスイスからのデータの収集、使用、および保存に関して、米国商務省が規定するセーフハーバー フレームワークを遵守しています。

[ページのトップへ](#)

お客様のコンピューターに関する情報の収集および使用

お客様がインターネット対応機能を搭載したソフトウェアを使用している場合は、ご使用のコンピューターに関する情報("標準的なコンピューター情報")が訪問した Web サイトや使用したオンラインサービスに送信されます。標準的なコンピュータ情報には、通常 IP アドレス、オペレーティング システムのバージョン、ブラウザのバージョン、および地域と言語の設定などが含まれます。また場合によっては、デバイスの製造元、名前とバージョンを示すハードウェア ID が含まれることもあります。特定の機能またはサービスが

Microsoft に情報を送信する場合は、標準的なコンピューター情報も一緒に送信されます。

Windows 8 の各機能のプライバシー関連情報 ([機能に関する補足条項](#)および [サーバーに関する補足条項](#)に掲載) と、このページの脇に一覧で記載されている機能のプライバシー関連情報では、収集される追加情報の種類とその用途について説明しています。

管理者は、グループ ポリシーを使用して、以下で説明している機能の設定の多くを変更できます。詳細については、 [管理者向けのこちらのホワイト ペーパー](#)を参照してください。

[ページのトップへ](#)

お客様の情報のセキュリティ

Microsoft は、お客様の情報のセキュリティを保護することに万全を期しています。マイクロソフトは、未承認のアクセス、使用、または情報開示から個人情報を保護するのに役立つ、さまざまなセキュリティ テクノロジーや手段を使用しています。たとえば、お客様から提供された情報は、管理された施設内のアクセスが制限されたコンピュータ システムに保管されます。Microsoft では、インターネットを通じてクレジットカード番号やパスワードなどの機密情報を転送する場合、SSL (Secure Socket Layer) プロトコルなどの暗号化を使用して機密情報を保護しています。

[ページのトップへ](#)

このプライバシーに関する声明の変更

Microsoft では、製品やサービスの変更およびお客様のフィードバックを反映するために、このプライバシーに関する声明を更新する場合があります。変更を公表した場合は、この声明の上部に記載された「最終更新日」が更新されます。この声明または Microsoft によるお客様の個人情報の使用方法に重大な変更が生じた場合は、その変更を実装する前に、このような変更を告知するか、お客様に直接通知を送信することによってお知らせします。Microsoft がお客様の情報をどのように保護しているかをご理解いただくために、この声明を定期的に確認することをお勧めします。

[ページのトップへ](#)

お問い合わせ先

Microsoft では、このプライバシーに関する声明についてのお客様のご意見、ご感想をお待ちしております。この声明についてご不明な点がある場合や、この声明に準拠していないとお考えの場合は、[Web フォーム](#)を参照してください。

Microsoft Privacy
Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052
USA

[ページのトップへ](#)

Microsoft のデータ処理の方針に関する最新の情報は、「[Microsoft のプライバシーに関する声明](#)」を参照してください。ここでは、データにアクセスして制御するために提供される最新のツール、またプライバシーに関する質問がある場合の問い合わせ方法についても確認することができます。

Windows 8 および Windows Server 2012 のプライバシーに関する声明

ハイライトペン 声明 **機能に関する補足条項** サーバーに関する補足条項

このページ内

最終更新日: 2012 年 10 月

ライセンス認証

このページは、以下の 4 つのセクションで構成されている [Windows 8 および Windows Server 2012 のプライバシーに関する声明](#) ("Windows プライバシーに関する声明") に関する補足条項です。

Active Directory Rights Management Services (AD RMS) クライアント

- [ハイライト](#)

監査

- [声明](#)。これは [完全な Windows のプライバシーに関する声明](#) です。この声明には、独自の声明を持つ Windows 機能のプライバシーに関する声明へのリンクが含まれています。

BitLocker ドライブ暗号化

- [機能の補足条項](#) (このドキュメント)。プライバシー関連の影響がある Windows 8 および Windows Server 2012 の機能について説明しています。

DirectAccess

動的更新

- [サーバーに関する補足条項](#)。プライバシー関連の影響がある Windows Server 2012 の追加の機能について説明しています。

コンピューターの簡単操作センター

個々の Windows 機能またはサービスに対するデータ収集および使用方法の詳細については、[完全なプライバシーに関する声明](#)および

イベントビューアー ファミリーセーフティ	適用される補足条項か、機能ごとの独自の声明を確認してください。
FAX	ライセンス認証
手書き認識個人用設定 - 自動学習機能	この機能について ライセンス認証により、ソフトウェアの偽造が減少します。これにより、Microsoft は、お客様が期待する品質のソフトウェアを提供することができます。ソフトウェアのライセンスが認証されると、ソフトウェアがインストールされた PC (またはハードウェア) に特定の
ホームグループ	プロダクト キーが関連付けられます。このように関連付けることで、プロダクト キーによって複数の PC 上で同一のソフトウェアが
入力方式エディター (IME)	認証されることがなくなります。PC のコンポーネントまたはソフトウェアに変更が生じた場合は、ソフトウェアのライセンス認証を再度行うことが必要になる場合があります。PC のハードウェアまたは
インストール向上プログラム	Windows のライセンス認証を再度行うことが必要になる場合があります。ライセンス認証では、ライセンス認証のエクスプロイト (ソフトウェアのライセンス認証を回避またはバイパスするソフトウェア) を検出して無効にすることが
インターネット印刷 言語の設定	ことができます。ライセンス認証のエクスプロイトが存在する場合、ソフトウェアまたはハードウェアのベンダーが、ソフトウェアの偽造コピーを作成するために、正規の Microsoft ソフトウェアを改ざんした可能性があります。ライセンス認証のエクスプロイトは、システムの正常な動作を妨げる可能性があります。
位置情報サービス 名前とアカウントの画像	収集、処理、または送信される情報
ネットワーク認識 通知、ロック画面に表示するアプリ、タイルの更新	ライセンス認証では、以下の情報が Microsoft に送信されます。
プリントの注文 プログラム互換性アシスタント	<ul style="list-style-type: none"> • Microsoft 製品コード (ライセンス認証を実行している Windows 製品を識別するための 5 桁のコード)。
プロパティ 近接	<ul style="list-style-type: none"> • チャンネル ID またはサイト コード。Windows 製品の当初の取得方法を識別します。たとえば、製品が最初に小売店で購入されたか、評価版として取得されたか、ボリューム ライセンスプログラムを通じて取得されたか、または PC の製造元によってプリインストールされたかを識別します。
リモート アクセス接続	<ul style="list-style-type: none"> • インストールの日付とインストールが成功したかどうか。
RemoteApp とデスクトップ接続	<ul style="list-style-type: none"> • Windows プロダクト キーが改変されていないことを確認する

リモート デスクトップ接続	ための情報。
Microsoft アカウントでのサインイン	<ul style="list-style-type: none"> • PC のメーカーとモデル。 • オペレーティング システムとソフトウェアのバージョン情報。
PC 設定の同期	
Teredo テクノロジ	<ul style="list-style-type: none"> • 地域と言語の設定。
トラステッド プラットフォーム モジュール (TPM) サービス	<ul style="list-style-type: none"> • PC に割り当てられるグローバル一意識別子 (GUID) と呼ばれる一意の番号。
ルート証明書の更新	<ul style="list-style-type: none"> • プロダクト キー (ハッシュ) とプロダクト ID。
更新サービス	<ul style="list-style-type: none"> • BIOS 名、リビジョン番号、およびリビジョンの日付。
Windows カスタマーエクスペリエンス向上プログラム (CEIP)	<ul style="list-style-type: none"> • ハード ドライブ ボリュームのシリアル番号 (ハッシュ)。 • ライセンス認証チェックの結果。これには、エラー コードと、次のような検出または無効化されたライセンス認証の 익스プロイトおよび、関連する悪意のあるソフトウェアや承認されていないソフトウェアに関する情報が含まれます。 <ul style="list-style-type: none"> • ライセンス認証の 익스プロイトの ID。
Windows Defender	
Windows エラー報告 (WER)	<ul style="list-style-type: none"> • ライセンス認証の 익스プロイトの現在の状態 (消去済みや検疫済みなど)。
Windows ファイルの関連付け	<ul style="list-style-type: none"> • PC の製造元の ID。
Windows ヘルプ	
リモート アシスタンス	<ul style="list-style-type: none"> • ライセンス認証の 익스プロイトのファイル名とハッシュ、およびライセンス認証の 익스プロイトの存在を示している可能性がある関連するソフトウェア コンポーネントのハッシュ。
Windows Search	
Windows 共有	
Windows SmartScreen	<ul style="list-style-type: none"> • PC のスタートアップ指示ファイルのコンテンツの名前とハッシュ。 サブスクリプションで Windows のライセンスを取得した場合、サブスクリプションの利用状況に関する情報も送信されます。 標準的なコンピューター情報も送信されますが、PC の IP アドレスが保持されるのは一時的です。
Windows 音声認識	
Windows ストア	
Windows タイム サービス	情報の用途
Windows	

トラブルシューティング

収集された情報は、Microsoft でソフトウェア コピーがライセンス 供与されたものであるかどうかを確認するために使用されま す。Microsoft がこの情報を使用して、お客様に連絡を取ることはあ りません。

選択および管理

ライセンス認証は必須の手続きで、Windows のセットアップ中に自 動的に行われます。ソフトウェアが適切にライセンス供与されてい ないと、Windows をライセンス認証することはできません。

[ページのトップへ](#)

Active Directory Rights Management Services (AD RMS) クライアン ト

この機能について

Active Directory Rights Management Services (AD RMS) クライアン トは、AD RMS 対応アプリと連動して、デジタル情報の不正使用を 防ぐ情報保護テクノロジーです。デジタル情報の所有者が、ファイル 内に含まれた情報を使用する方法（ファイルを開く、修正、印刷ま たは別の操作を行うことができるユーザーの指定など）を定義する ことができます。権限の制限されたファイルを作成または表示する ためには、PC が AD RMS 対応アプリを実行中であり、AD RMS サー バーへのアクセス権を持っている必要があります。

収集、処理、または送信される情報

AD RMS サーバーに対するユーザーの識別には、ユーザーの電子メ ール アドレスが使用されます。結果、ユーザーの電子メール アド レスは、サーバー上、および PC 上の、サーバーによって作成され たライセンスと ID 証明書に保存されます。権利管理によって保護 されたドキュメントに対して特定の操作（開く、印刷する、など）を 実行しようとする、AD RMS サーバーとの間で ID 証明書とライセ ンスが伝送されます。ご使用の PC が企業ネットワークに接続され ている場合、AD RMS サーバーは通常、その企業によって運用され ます。Windows Live AD RMS サービスを使用している場合 は、Microsoft によってサーバーが運用されます。ユーザーのプライ バシーを保護するため、Microsoft AD RMS サーバーに送信される情 報は暗号化されます。

情報の用途

ライセンスは、保護されたファイルへのアクセスを許可します。ID 証明書は、AD RMS サーバーに対してユーザーを特定するために使用されます。また、ファイルの保護および保護されたファイルへのアクセスを可能にします。

選択および管理

AD RMS 機能は、AD RMS 対応アプリを通じて有効化する必要があります。AD RMS 機能は既定では無効化されています。AD RMS 機能を有効化または使用しないことを選択できます。ただし、有効化しない場合、保護されたファイルにアクセスできません。

[ページのトップへ](#)

監査

監査では、管理者は Windows を設定し、イベント ビューアーや他のアプリを使って読むことのできるセキュリティ ログにシステムの動作を記録することができます。このログを使用すると、管理者は PC または PC 上のリソースへの不正なアクセスを検知できるようになります。たとえば、だれかがコンピューターへサインイン、新しいユーザー アカウントを作成、セキュリティ ポリシーを変更、またはドキュメントを開く操作をしていないかどうかを知ることができます。また、このログは問題のトラブルシューティングにも役立ちます。

収集、処理、または送信される情報

管理者は収集される情報の内容、保持される期間、および第三者へ伝送されるかどうかを決定します。情報には、ユーザー名やファイル名などの個人情報が含まれる場合があります。詳細については、管理者にお問い合わせください。Microsoft には情報は送信されません。

情報の用途

管理者は、監査情報の使用方法も決定します。一般に、セキュリティ ログは監査人や管理者が、PC の動作の追跡、または PC や PC 上のリソースへの不正なアクセスを特定するために使われます。

選択および管理

管理者は、この機能を有効にするのかどうか、およびユーザーへの

通知方法を決定します。他のユーザーは、管理者がアクセスを許可しない限り、セキュリティ ログを表示できません。管理ツールで [ローカル セキュリティ ポリシー] を開き、PC の [監査] を設定できます。

[ページのトップへ](#)

BitLocker ドライブ暗号化

この機能について

BitLocker ドライブ暗号化は、データを暗号化して保護することにより、承認されていないユーザーがデータにアクセスすることを防ぎます。サポートされているドライブで BitLocker が有効な場合、そのドライブのデータが Windows によって暗号化されます。

収集、処理、または送信される情報

ソフトウェアの暗号化で BitLocker が有効な場合、メモリ内の暗号化キーは、保護されたドライブからの読み取りや、ドライブへの書き込みを行うときに継続してデータの暗号化と暗号化の解除を行います。ハードウェアの暗号化で BitLocker が有効になっている場合、データの暗号化と暗号化の解除はドライブによって実行されます。

BitLocker の設定時に、回復キーを印刷するか、ネットワーク上の場所に保存できます。BitLocker を非リムーバブル ドライブに設定した場合は、回復キーを USB フラッシュ ドライブにも保存できます。

PC がドメインに参加していない場合は、BitLocker 回復キー、回復キー ID、およびコンピューター名を OneDrive にバックアップできます。お客様のプライバシーを保護するために、送信される情報は SSL によって暗号化されます。

スマート カードに保存されている証明書を使用してデータを暗号化するように BitLocker を設定することができます。スマート カードを使用してデータ ドライブを保護する場合、そのスマート カード用の公開キーと一意の識別子は、暗号化されずにドライブ上に保存されます。この情報は、最初にスマート カードの暗号化証明書を作成するのに使用された証明書の特定に使用することができます。

PC にバージョン 1.2 以上のトラステッド プラットフォーム モジュー

ール (TPM) が搭載されている場合、BitLocker は TPM を使用して Windows がインストールされているドライブのハードウェアを強化したデータ保護を提供します。詳細については、「トラステッドプラットフォーム モジュール (TPM) サービス」セクションを参照してください。TPM が搭載されている PC では、暗証番号 (PIN) を設定し、暗号化されたデータをさらに保護することもできます。BitLocker では、この TPM ベースの PIN を、ドライブ上にハッシュおよび暗号化された形式で保存します。

BitLocker で収集された情報は、回復キーを OneDrive にバックアップしない限り、Microsoft に送信されません。

情報の用途

暗号化キーとグローバル一意識別子 (GUID) は PC メモリに保存され、BitLocker 操作をサポートします。ハードウェアの障害またはその他の問題が発生した場合は、BitLocker 回復情報を使用して保護されているデータにアクセスできます。この回復情報により、BitLocker は承認されているユーザーと承認されていないユーザーを見分けます。

Microsoft は、個人の回復キーをどのような目的にも使用しません。回復キーが OneDrive に送信された場合、Microsoft は、傾向を分析したり、製品やサービスを向上させるためにそれらの回復キーに関する要約データを使用することがあります。

選択および管理

BitLocker は既定でオフになっています。コントロール パネルの [BitLocker ドライブ暗号化] を開き、リムーバブル ドライブで、いつでも BitLocker をオンまたはオフにすることができます。管理者は、すべてのドライブの BitLocker のオンとオフを切り替えることができます。

回復キーを OneDrive にバックアップする場合は、[ここで](#)回復キーにアクセスしたり、回復キーを削除したりできます。

[ページのトップへ](#)

デバイスの検出と設定

Windows には、デバイスのインストール、モバイル ブロードバンド デバイスのインストール、ネットワークの探索、ワイヤレス デ

バスのペアリングなど、PC でのデバイスの検出と設定に役立ついくつかの機能が用意されています。

デバイスのインストール

この機能について

Windows では、PC に新しいデバイスがインストールされたときに、ドライバー ソフトウェアを自動的に検索し、ダウンロードしてインストールできます。説明、画像、製造元のロゴなどのデバイスに関する情報も自動的にダウンロードできます。Windows と同期する特定のプリンター、Web カメラ、モバイル ブロードバンド デバイス、ポータブル デバイスなど、一部のデバイスには、機能やユーザー エクスペリエンスを最大限に活用できるようにするアプリがあります。デバイスの製造元がそのデバイス用のアプリを提供している場合は、そのアプリを Windows ストアから自動的にダウンロードしてインストールできます (ストアにサインインしている場合)。

収集、処理、または送信される情報

Windows は、ドライバーを検索するときにまず、該当するドライバーが PC 上に存在するかどうかを確認します。PC 上に存在しない場合は、Windows Update サービスにオンラインでアクセスし、デバイス ドライバーを検索してダウンロードします。Windows Update によって収集される情報とその用途の詳細については、[Update サービスのプライバシーに関する声明](#)で回復キーにアクセスしたり、回復キーを削除したりできます。

デバイス情報を取得し、そのデバイス用のアプリが利用可能かどうかを判断するため、デバイス ID (ご使用のデバイスのハードウェア ID またはモデル ID など)、地域と言語、およびデバイス情報の最終更新日などのデバイスに関するデータが Microsoft に送信されます。情報またはデバイス アプリが利用可能な場合、そのデバイス アプリが Windows ストアからダウンロードされ、インストールされます。このアプリは、Windows ストア アカウントのダウンロードしたアプリの一覧から利用できます。

情報の用途

Microsoft に送信された情報は、目的のデバイスに適したデバイス ドライバー、デバイス情報、およびデバイス アプリを決めてダウンロードするために使用されます。Microsoft がこの情報を使用してお客様を識別したり、連絡したり、広告の対象としたりすることはあ

りません。

選択および管理

Windows のセットアップ時に簡単設定を選択した場合は、デバイスドライバー、デバイス情報、およびデバイス アプリの自動的なダウンロードとインストールを有効にします。設定をカスタマイズする場合は、[PC を保護し、最新の状態に保つ] の [新しいデバイス用のデバイス ドライバー、デバイス アプリ、および情報を自動的に入手する] を選択して、デバイス ドライバー、アプリ、および情報の自動的なダウンロードとインストールを管理できます。Windows のセットアップ後に、コントロール パネルでこれらの設定を変更できます。これを行うには、[デバイスのインストール設定の変更] を選択し、[いいえ、実行方法を選択します] で回復キーにアクセスしたり、回復キーを削除したりできます。

デバイス アプリは、デバイスをアンインストールしなくても、いつでもアンインストールできます。ただし、デバイスの特定の機能を使用するにはアプリが必要である場合があります。デバイス アプリをアンインストールした後で、再度インストールするには、Windows ストアで、所有するアプリの一覧を使います。

モバイル ブロードバンド デバイスのインストール

この機能について

特定の通信事業者から提供されているモバイル ブロードバンド ハードウェアが PC に搭載されている場合は、Windows で PC のモバイル ブロードバンド ハードウェアを提供した通信事業者と共に自分のアカウントとデータ プランを管理できるアプリケーションが自動的にダウンロードおよびインストールされます。追加のデバイス情報もダウンロードされ、ネットワーク一覧にモバイル ブロードバンド接続を表示することができます。

収集、処理、または送信される情報

Windows は、ダウンロードするデバイス情報とアプリを特定するために、通信事業者を識別するハードウェア ID の一部をモバイル ブロードバンド ハードウェアから取得して送信します。ユーザーのプライバシーを保護するため、モバイル ブロードバンド ハードウェア ID 全体を Microsoft に送信することはしません。

通信事業者が Microsoft にアプリを提供している場合は、Windows

でそのアプリが Windows ストアからダウンロードされて、インストールされます。インストール後にアプリを開くと、そのアプリが、モバイル ブロードバンド ハードウェアにアクセスします。たとえば、その際に取得した固有のハードウェア ID を使用して、通信事業者は、ユーザーのアカウントを識別することができます。

情報の用途

Microsoft では、Windows から送信されたモバイル ブロードバンド ハードウェアの ID の一部を使用して、コンピューターにインストールするキャリアのアプリを判断します。インストールされたアプリでは、モバイル ブロードバンド ハードウェアの ID を使用できません。たとえば、通信事業者のアプリでそれらの ID を使用してアカウントおよびプランの情報をオンラインで検索できます。この情報のアプリの使用については、通信事業者のプライバシーの方針に従います。

選択および管理

初めて Windows をセットアップするときに簡単設定を選択した場合、通信事業者アプリを Windows が自動的にチェックしてダウンロードします。この機能はコントロール パネルでオンとオフを切り替えることができます。詳細については、前の「デバイスのインストール」セクションを参照してください。

通信事業者のアプリは、モバイル ブロードバンド ハードウェアをアンインストールしなくてもいつでもアンインストールできます。

ネットワーク検索

この機能について

PC を、家庭にあるような小規模なプライベート ネットワークに接続すると、Windows でネットワーク上の他の PC および共有デバイスが自動的に検出され、ネットワーク上の他のユーザーはその PC を表示できるようになります。共有デバイスが使用できるようになると、Windows ではそれらのデバイスに自動的に接続し、インストールすることができます。共有デバイスには、プリンターやメディア エクステンダーなどがありますが、カメラや携帯電話などの個人用デバイスは含まれません。

収集、処理、または送信される情報

デバイスの共有およびデバイスへの接続を有効にすると、名前やネ

ットワーク アドレスなどの PC に関する情報がローカル ネットワーク上でブロードキャストされ、他の PC から検出および接続できるようになります。

ネットワークに接続されているデバイスを自動的にインストールするかどうかを判断するために、ネットワークに関するいくつかの情報が収集されて、Microsoft に送信されます。この情報には、ネットワーク上のデバイスの数、ネットワークの種類（プライベート ネットワークなど）、ネットワーク上のデバイスの種類とモデル名などが含まれます。ネットワーク名やパスワードなどの個人情報は収集されません。

デバイスのインストール設定によっては、Windows で共有デバイスがインストールされると、Windows からいくつかの情報が Microsoft に送信されて、PC にデバイス ソフトウェアがインストールされる場合があります。詳細については、「デバイスのインストール」セクションを参照してください。

情報の用途

Microsoft に送信されたネットワークに関する情報を使用して、自動的にインストールするネットワーク上のデバイスが判断されません。Microsoft がこの情報を使用してお客様を識別したり、連絡したり、広告の対象としたりすることはありません。

選択および管理

ネットワークに参加するときにデバイスの共有やデバイスへの接続を有効にした場合、そのネットワークに対してネットワーク探索が有効になります。現在使用しているネットワークに合わせてこの設定を変更するには、[ネットワークと共有センター] でネットワークの名前の下に示されているネットワークの種類をクリックします。

ネットワーク探索を完全に有効にするかどうか、およびネットワークに接続されているデバイスの自動設定を有効にするかどうかを選択するには、[ネットワークと共有センター] で [共有の詳細設定の変更] を選択します。

ワイヤレス デバイスのペアリング

この機能について

Windows では、Bluetooth または Wi-Fi Direct を使用するワイヤレス デバイスと PC を関連付けることができます。Wi-Fi Direct

は、Wi-Fi ネットワークに接続しなくてもデバイスどうしが直接通信することができるワイヤレス技術です。

収集、処理、または送信される情報

[Bluetooth 設定] で **[Bluetooth デバイスによる、この PC の検出を許可する]** を選択すると、Windows では Bluetooth 経由で PC の名前がブロードキャストされ、Bluetooth 対応デバイスで PC を検出および識別できます。

[デバイスの追加] を選択すると、Windows では Wi-Fi で PC の名前がブロードキャストされて、Wi-Fi Direct 対応デバイスで PC が検出および識別されるようになります。**[デバイスの追加]** を閉じると、Windows は Wi-Fi 経由での PC の名前のブロードキャストを停止します。

デバイスのインストール設定によっては、Windows がワイヤレスデバイスと関連付けられると、Windows からいくつかの情報が Microsoft に送信されて、PC にデバイス ソフトウェアがインストールされる場合があります。詳細については、前の「デバイスのインストール」セクションを参照してください。

情報の用途

Windows で PC の名前がブロードキャストされて、他のデバイスで PC を識別したり、PC に接続できるようになります。PC の名前は Microsoft に送信されません。

選択および管理

Windows で PC の名前が Bluetooth を使ってブロードキャストされるように変更するには、コントロール パネルの **[デバイスとプリンター]** で PC を長押しするか右クリックして、**[Bluetooth の設定]** をクリックし、**[Bluetooth デバイスによるこの PC の検出を許可する]** をクリックします。デバイスを追加するときに Windows で PC の名前を Wi-Fi でブロードキャストしない場合は、デバイスを追加する前に **[PC 設定]** の **[ワイヤレス]** で Wi-Fi を一時的に無効にします。

[ページのトップへ](#)

この機能について

DirectAccess を使用すると、ユーザーがどこにいるかに関係なく、PC がインターネットに接続するたびに職場ネットワークにシームレスにリモート接続されます。

収集、処理、または送信される情報

PC を起動するたびに、ユーザーが職場にいるかどうかに関係なく、DirectAccess で職場ネットワークへの接続が行われます。接続すると、PC に職場のポリシーがダウンロードされ、職場ネットワーク内の設定済みリソースにアクセスできるようになります。職場の管理者が DirectAccess 接続を使用して PC をリモートで管理および監視する場合があります。この場合、職場にいないときでも、アクセスした Web サイトなどが監視されます。

DirectAccess から Microsoft に情報は送信されません。

情報の用途

会社のポリシーによって、職場の管理者が収集した情報の使い方が決まります。

選択および管理

DirectAccess は、グループ ポリシーを使用して職場の管理者が設定する必要があります。管理者は DirectAccess のいくつかの要素を一時的に非アクティブにすることができますが、管理目的で Windows から職場への接続を停止できるのは、職場の管理者だけです。ユーザーまたは職場の管理者が職場のドメインから PC を削除すると、DirectAccess は接続できなくなります。

[ページのトップへ](#)

動的更新

この機能について

動的更新により、Windows は Windows Update を一度にチェックし、Windows のインストール中にユーザーの PC 用の最新の更新プログラムを取得できます。更新プログラムが見つかった場合は、動的更新により自動的にダウンロードおよびインストールされるので、初めてサインインまたは使用するときに PC は最新の状態になっています。

収集、処理、または送信される情報

互換性のあるドライバーをインストールするため、動的更新は PC のハードウェアに関する情報を Microsoft に送信します。動的更新で PC にダウンロードできる更新プログラムには、次のような種類があります。

- インストール更新プログラムで回復キーにアクセスしたり、回復キーを削除したりできます。インストールの成功を確実にするために役立つ、インストール ファイルの重要なソフトウェア更新プログラムです。
- インボックス ドライバー更新プログラムで回復キーにアクセスしたり、回復キーを削除したりできます。インストールする Windows バージョン用の重要なドライバー更新プログラムです。

情報の用途

動的更新は、ユーザーのシステムに適したドライバーを識別するために、PC のハードウェアに関する情報を Microsoft に報告します。動的更新が収集する情報の使用法については、「[Update サービスのプライバシーに関する声明](#)」で回復キーにアクセスしたり、回復キーを削除したりできます。

選択および管理

Windows のインストールを開始すると、オンラインにして更新プログラムをインストールするかどうかをたずねられます。

[ページのトップへ](#)

コンピューターの簡単操作センター

この機能について

コンピューターの簡単操作センターでは、ユーザー補助オプションと設定を有効にし、PC をより容易に操作できます。

収集、処理、または送信される情報

この機能を使用するには、シリーズから該当する声明を選択するよう求められます。

これらの声明には、次のものがあります。

- テレビの画像やテキストが見えにくい。
- 照明の状況のため、モニターの画像が見えにくくなる。
- キーボードを使用しません。
- 目が見えません。
- 耳が聞こえません。
- 話すときに困難があります。

この情報は、人間が読み取ることのできない形式で、ユーザーの PC にローカルに保存されます。

情報の用途

選択した声明に基づいて、推奨設定のセットが提供されます。この情報は Microsoft には送信されません。ユーザーと PC の管理者以外の他のユーザーは利用できません。

選択および管理

コントロール パネルの [コンピューターの簡単操作] で該当する声明を指定できます。選択内容はいつでも変更できます。また、推奨設定のうち、PC に設定したいものを選択することもできます。

[ページのトップへ](#)

イベント ビューアー

この機能について

PC のユーザー、主に管理者は、イベント ビューアーを使用して、イベント ログを閲覧および管理できます。イベント ログには PC のハードウェア、ソフトウェア、およびセキュリティ イベントに関する情報が含まれます。また、[イベント ログ オンライン ヘルプ] リンクをクリックすることで、イベント ログのイベントについての情報を Microsoft から取得できます。

収集、処理、または送信される情報

イベント ログには、PC 上のすべてのユーザーとアプリによって生成されたイベント情報が含まれます。既定では、すべてのユーザー

はログ エントリを表示できるようになっていますが、管理者はイベント ログへのアクセスを制限することができます。イベント ビューアーを開いて PC のイベント ログへアクセスできます。イベント ビューアーの開き方の詳細については、Windows ヘルプとサポートを参照してください。

[イベント ログ オンライン ヘルプ] を使用して特定のイベントに関する追加情報を検索すると、そのイベントについての情報が Microsoft に送信されます。

情報の用途

[イベント ログ オンライン ヘルプ] を使用してイベントに関する情報を検索すると、PC から送信されたイベント データを基に、イベントに関する追加情報が特定されて提供されます。Microsoft のイベントの場合、イベントの詳細が Microsoft へ送信されます。Microsoft がこの情報を使用してお客様を識別したり、連絡したり、広告の対象としたりすることはありません。サードパーティのアプリに関連するイベントの場合、情報はサードパーティの発行元または製造元が指定した場所へ送信されます。イベントに関する情報をサードパーティの発行元または製造元に送信する場合、情報の用途は各サードパーティのプライバシー基準に従うこととなります。

選択および管理

管理者は、イベント ビューアー ログへのアクセスを制限するよう選択できます。イベント ビューアーへのフル アクセスを持つユーザーは、ログをクリアすることができます。イベント情報の自動送信を行うよう同意しない限り、[イベント ログ オンライン ヘルプ] をクリックすると、表示された情報をインターネットで送信することに対する同意が求められます。送信に同意しない限り、イベント ログ情報がインターネットで送信されることはありません。管理者はグループ ポリシーを使用して、イベント情報を送信するサイトを指定または変更することができます。

[ページのトップへ](#)

ファミリー セーフティ

[この機能について](#)

ファミリー セーフティは、PC を使う子供を守る保護者のための機能です。保護者の方は、お子様が利用できるアプリ、ゲーム、Web サイトを管理することができます。また、制限時間を設定したり、活動記録レポートを定期的に電子メールで受け取ることもできます。制限の管理や活動記録レポートの閲覧は、保護者がご自身の PC からローカルで行うことができるほか、Microsoft ファミリー セーフティ Web サイトを使用してオンラインで行うこともできます。

収集、処理、または送信される情報

ファミリー セーフティの設定と子供の活動記録は PC に保存されます。活動記録レポートには、コンピューターの使用時間、個々のアプリやゲームに費やされた時間、訪問した Web サイト（ブロックされているサイトを閲覧しようとしたなど）に関する情報を含めることができます。設定の変更や活動記録レポートの閲覧は、PC の管理者が実行できます。

お子様のアカウントに対してオンライン管理を有効にする
と、Microsoft ファミリー セーフティ Web サイトから、お子様の活動記録レポートを閲覧したりその設定を変更したりすることができます。Microsoft ファミリー セーフティ Web サイトに他のユーザーを保護者として追加することで、活動記録レポートの閲覧と設定の変更をそのユーザーに許可することができます。ファミリー セーフティの構成を行う保護者が Microsoft アカウントで Windows にサインインすると、オンライン管理が自動的に有効となります。

オンライン管理が有効な状態でお子様のアカウントにファミリー セーフティを構成すると、保護者のもとに、子供の活動記録が毎週自動的に電子メールで配信されます。

情報の用途

Windows と Microsoft ファミリー セーフティ Web サイトでは、収集した情報を使用してファミリー セーフティの機能を実現しています。Microsoft は、データの質の観点から、アクティビティ ログの情報を総合的に分析する場合がありますが、この情報を使用して個人を特定したり、連絡したり、広告の対象とすることはありません。

選択および管理

既定では、ファミリー セーフティがオフになっています。コントロール パネルの [ファミリー セーフティ] からアクセスできます。フ

ファミリー セーフティを有効にできるのは管理者だけです。加えて、監視または制限の対象は、管理者特権を持たないユーザーに限られます。お子様は、その設定を表示することはできますが、変更することはできません。ファミリー セーフティが有効になっている場合、お子様が Windows にサインインする際、その都度、自分のアカウントがファミリー セーフティによって監視されていることが、お子様に通知されます。アカウントの作成時に、それがお子様のアカウントであることを指定した場合、そのアカウントに対してファミリー セーフティを有効にするかどうかを選択できます。

子供のアカウントをセットアップしている管理者が Microsoft アカウントで Windows にサインインすると、オンライン管理が自動的に有効となり、子供のアクティビティについてのレポートが週単位で送信されます。保護者のアカウントは、Microsoft ファミリー セーフティ Web サイトで追加または削除できます。この Web サイトで保護者として追加されたユーザーはだれでも、子供の活動記録レポートを閲覧したり、子供のファミリー セーフティ設定を変更したりすることができます。その保護者が、子供の使用している PC の管理者である必要はありません。

ファミリー セーフティを適切に使用するには、保護者のみが PC の管理者となり、子供には管理者権限が与えられないようにする必要があります。この機能を使用して他のユーザー（成人など）を監視すると、適用される法令への違反となる場合があるので注意してください。

[ページのトップへ](#)

FAX

この機能について

FAX 機能では、FAX 送付状を作成および保存し、PC や外部または内蔵 FAX モデム、または FAX サーバーを使用して FAX の送受信を行うことができます。

収集、処理、または送信される情報

収集される情報には、FAX 送付状に入力された個人情報や、送信端末識別 (TSID) や被呼端末識別 (CSID) などの業界標準プロトコルに含まれる識別子が含まれます。既定では、Windows は各識別子の値として "FAX" を使用します。

情報の用途

送信者のダイアログ ボックスに入力された情報は、FAX 送付状に表示されます。TSID や CSID などの識別子には、受信側の FAX 機器または PC が送信者の特定のために一般的に使用する、任意のテキストが含まれます。Microsoft には情報は送信されません。

選択および管理

FAX へのアクセスは、PC 上のユーザー アカウント権限によって決定されます。FAX 管理者がアクセス設定を変更しない限り、すべてのユーザーは FAX の送受信を行うことができます。既定では、すべてのユーザーが、送信するドキュメントや PC 上で受信したすべての FAX を表示できるようになっています。管理者は FAX で送信または受信されたすべてのドキュメントを閲覧できます。また、FAX を表示または管理する権限を持つユーザー、TSID および CSID 値などの FAX 設定を行うこともできます。

[ページのトップへ](#)

手書き認識個人用設定 - 自動学習機能

この機能について

自動学習機能は、タッチまたはタブレット ペンを使って PC で使用できる手書き認識個人用設定ツールです。この機能は、使用される単語や単語の書き方に関するデータを収集します。この機能により、手書き認識ソフトウェアは手書き入力の書き方やボキャブラリを認識し、その変換精度を向上できます。また、入力方式エディター (IME) を使用しなくても、言語の自動修正やテキストのヒントを向上させることもできます。

収集、処理、または送信される情報

自動学習機能で収集された情報は、PC 上の各ユーザーのユーザー プロファイル内に保存されます。データは専用フォーマットで保存され、テキスト表示アプリ (ノートパッドやワードパッドなど) で読み取ることはできません。本人以外で読み取ることができるのは、PC の管理者のみです。

収集される情報には、次の項目が含まれます。

- 電子メール アプリ (Office Outlook や Windows Live メールな

ど)を使用して作成したメッセージのテキストや、作成したカレンダー エントリの内容。これには送信済みのメッセージがすべて含まれます。

- 入力パネルに記載したインク。
- 入力パネルに記載したインクから認識されたテキストまたはスクリーン キーボード上の入力内容。
- 認識されたテキストを修正するよう選択した置き換え後の文字。

情報の用途

収集された情報は、ユーザー独自の書き方やボキャブラリに個人設定された認識ソフトウェアのバージョンを作成することにより、手書き認識精度を向上させ、ソフト キーボード上の入力内容に応じて自動修正とテキストのヒントを可能にするために使用されます。

テキスト サンプルは、拡張辞書の作成に使用されます。インク サンプルは、PC の各ユーザーに対する文字認識機能を向上させるために使用されます。Microsoft には情報は送信されません。

選択および管理

自動学習機能は既定で有効になっています。自動学習機能のオンとオフは、コントロール パネルの [言語] の [詳細設定] でいつでも切り替えることができます。自動学習機能をオフにすると、自動学習機能によって収集および保存されたデータはすべて削除されます。

[ページのトップへ](#)

ホームグループ

この機能について

Windows では、ホーム ネットワーク上の PC を簡単にリンクして画像、音楽、ビデオ、ドキュメントおよびデバイスを共有することができます。また、メディア エクステンダーなど、ホーム ネットワーク上のデバイスに対し、PC からメディアをストリーム配信できるようになります。これらの PC とデバイスがホームグループです。パスワードを使用してホームグループの保護を行ったり、共有する内容を選択することができます。

収集、処理、または送信される情報

ホームグループのどの PC からでも、画像、ビデオ、音楽、ドキュメントなど独自のファイルにアクセスできます。ホームグループに参加すると、PC 上のこれらすべてのアカウントの Microsoft アカウント情報（電子メール アドレス、表示名、画像を含む）がホームグループ内の他のアカウントと共有され、それらのユーザーとの共有が可能になります。

情報の用途

収集した情報によって、ホームグループ内の PC は内容を共有するユーザーと、表示方法を理解することができます。Microsoft には情報は送信されません。

選択および管理

ホームグループに PC を追加またはホームグループから PC を削除できます。また、他のホームグループ メンバーと共有する内容を指定することもできます。[PC 設定] の [ホームグループ] でホームグループを作成し、その設定を管理できます。

[ページのトップへ](#)

入力方式エディター (IME)

Microsoft 入力方式エディター (IME) は、東アジアの言語に使用され、キーボード入力を表意文字へ変換するのに使用されます。このセクションでは、IME の自動調整と予測、IME 変換エラー報告、IME 単語の登録などの機能について取り上げます。

IME の自動調整と予測

この機能について

使用する IME および設定によっては、IME の自動調整および入力ヒント機能を使って、単語や文字列を記録し、表示される表意文字の選択精度を向上させることができます。

収集、処理、または送信される情報

IME 自動調整（自己学習）と入力ヒント機能により、単語や文字列、およびそれらを使用する頻度を記録できます。自動調整の情報（数字/記号文字の配列を除く）は、PC 上の各ユーザーのファイル内に保存されます

情報の用途

自動学習および入力ヒントのデータは PC で IME によって使用され、IME の使用時に表示される表意文字の選択精度を向上させることができます。このデータを Microsoft に送信するように選択した場合、送信されたデータは、IME およびそれに関連した製品やサービスの向上に使用されます。

選択および管理

簡体字中国語版の IME (予測機能が既定でオフになっている) を除き、既定では自動認識および入力ヒント機能はそれらをサポートする IME でオンになっています。収集されたデータは Microsoft に自動的に送信されません。このデータを収集または送信するかどうかは、コントロールパネルの [言語] で選択できます。

IME 変換エラー報告

この機能について

表意文字を表示したり、キーボード入力を表意文字へ変換するときエラーが発生すると、この機能によりエラーに関する情報が収集されます。この情報は、Microsoft で製品やサービスを向上させるために使用されます。

収集、処理、または送信される情報

IME 変換エラー報告では、IME 変換エラーに関する情報 (入力した内容など)、最初の変換または予測結果、代わりに選択した文字列、使用している IME に関する情報、および IME の使用方法に関する情報が収集されます。また、日本語の IME を使用する場合は、変換エラー報告に自動学習の情報を含めるかどうかを選択できます。

情報の用途

Microsoft は、この情報を製品やサービスを向上させるために使用します。Microsoft がこの情報を使用してお客様を識別したり、連絡したり、広告の対象としたりすることはありません。

選択および管理

特定の数の変換エラーが保存された後に、誤変換報告ツールで、変換エラー報告を送信するかどうか確認が行われます。IME 誤変換報告ツールから変換エラー報告を送信することをいつでも指定できます。送信するかどうかを選択する前に、各報告に含まれる情報を表

示できます。また、[日本語入力システムの設定] で変換エラー報告の自動送信を有効にすることもできます。

IME 単語の登録

この機能について

使用する IME によっては、単語の登録を使用して、サポートされていない単語 (キーボード入力から表意文字へ正確に変換されない場合がある単語) を報告することができます。

収集、処理、または送信される情報

登録には、報告される単語について [単語の追加] ダイアログ ボックスに記入した情報と、IME のソフトウェア バージョン番号を含めることがあります。単語登録を使用する個人の名前を追加する場合など、これらの報告に個人情報が含まれる場合があります。送信前に各報告で送信するデータを見直す機会があります。

情報の用途

Microsoft は、この情報を製品やサービスを向上させるために使用します。Microsoft がこの情報を使用してお客様を識別したり、連絡したり、広告の対象としたりすることはありません。

選択および管理

単語登録報告を作成するたびに、この報告を Microsoft へ送信するかどうかをたずねられます。送信するかどうかを選択する前に、報告に含まれる情報を表示することもできます。

[ページのトップへ](#)

インストール向上プログラム

この機能について

インストール向上プログラムでは、PC の基本情報と Windows 8 のインストール状況に関する情報を含む 1 つの報告が Microsoft に送信されます。Microsoft はこの情報を使用して、インストール エクスペリエンスを向上させ、一般的なインストールの問題に対する解決策を作成します。

収集、処理、または送信される情報

報告には、インストールの日付、インストールの各フェーズが完了

するまでにかかった時間、インストールが製品のアップグレードなのか新しいインストールなのか、バージョンの詳細、オペレーティングシステムの言語、メディアの種類、PCの構成、エラーコードを含む成功またはエラーの状態など、インストールに関する情報が含まれます。

インストール向上プログラムへの参加を選択すると、インターネットへの接続時に、報告が Microsoft に送信されます。インストール向上プログラムでは、この報告と共に Microsoft に送信されるグローバル意識別子 (GUID) と呼ばれる番号がランダムに生成されます。GUID を使用して、長期間特定のコンピューターから送信されるデータを確認できます。GUID には個人情報が含まれておらず、GUID を使用してお客様を特定することはありません。

情報の用途

Microsoft とそのパートナーは、この報告を製品とサービスの向上に役立てます。Microsoft では、GUID を使用して、このデータを Windows カスタマー エクスペリエンス向上プログラム (CEIP) によって収集されたデータに関連付けます。CEIP は Windows 8 を使用する際に参加を選択できるプログラムです。

選択および管理

Windows 8 をインストールする際に、このプログラムへの参加を選択できます。参加する場合は **[Windows インストールの品質向上に協力する]** で回復キーにアクセスしたり、回復キーを削除したりできます。

詳細については、「Windows CEIP」セクションを参照してください。

[ページのトップへ](#)

インターネット印刷

この機能について

インターネット印刷では、インターネットを介して印刷することができます。

収集、処理、または送信される情報

この機能を使用して印刷を行う場合、最初にインターネット プリン

ト サーバーに接続し、自分自身を認証する必要があります。プリンター サーバーへ送信する必要がある情報は、プリンター サーバーがサポートするセキュリティのレベルによって異なります (たとえば、ユーザー名とパスワードの入力が求められる場合があります)。接続が完了すると、互換性のあるプリンターの一覧が表示されます。PC に選択したプリンター用のプリンター ドライバーがない場合は、プリント サーバーからドライバーをダウンロードするよう選択できます。印刷ジョブは暗号化されていないため、他人が送信される内容を見ることができるよう可能性があります。

情報の用途

収集された情報によって、リモート プリンターを使用して印刷できます。Microsoft によってホストされているプリント サーバーを使用するようにお客様が選択した場合、Microsoft が、お客様個人を特定したり、連絡したり、広告の対象としたりするために、提供された情報を使用することはありません。情報をサードパーティのプリント サーバーに送信する場合、情報の用途はサードパーティのプライバシー基準に従うことになります。

選択および管理

コントロール パネルの [プログラムと機能] を開いて **[Windows の機能の有効化または無効化]** で回復キーにアクセスしたり、回復キーを削除したりできます。

[ページのトップへ](#)

言語の設定

この機能について

使用する言語を Windows 8 の言語の一覧に追加できます。アプリや Web サイトは、その一覧で利用可能な最初の言語で表示されます。

収集、処理、または送信される情報

Web サイトにアクセスして PC にアプリをインストールすると、アクセスした Web サイトに優先する言語の一覧が送信されます。使用するアプリは、この一覧を利用して、優先する言語でコンテンツを提供できるようになります。

情報の用途

優先する言語の一覧は、ユーザーに合った言語でコンテンツを提供するために、Microsoft の Web サイトやアプリで使用されます。Microsoft は、お客様を特定したりお客様に連絡したりするために言語の情報を使用することはありません。サードパーティの Web サイトおよびアプリによって送信されたり使用されたりする言語の情報は、サードパーティの Web サイトまたはアプリの発行元のプライバシーの方針に従って使用されます。

選択および管理

優先する言語の一覧は、インストールするアプリおよびアクセスする Web サイトに提供されます。この一覧の言語の追加または削除は、コントロールパネルの言語の設定で実行できます。この一覧に言語を設定しない場合、アクセスする Web サイトには、コントロールパネルの地域にある [形式] タブで選択した言語が送信されます。

[ページのトップへ](#)

位置情報サービス

Windows を実行している PC では、"位置情報サービス" は、お使いの PC のおおよその物理的な位置を特定するために使用される Windows ソフトウェアおよび Microsoft オンライン サービスのことを指します。この位置情報は、アクセスが許可されているアプリまたは Web サイトに提供されます。Windows 位置情報プラットフォームは、PC の GPS センサーなどの専用ハードウェア、または Windows 位置情報取得機能などのソフトウェアから位置情報を取得します。

Windows 位置情報プラットフォーム

この機能について

Windows 位置情報プラットフォームを有効にすると、Windows ストアからインストールしたアプリが PC の位置情報へのアクセス許可を要求できるようになります。プラットフォームは、システムの構成に応じて、GPS センサーなどのハードウェア、または Windows 位置情報取得機能などのソフトウェアを使用して PC の位置を特定します。

プラットフォームでは、アプリが他の方法で PC の位置情報にアクセスすることは防止されません。たとえば、位置情報をアプリに直

接送信し、位置情報がプラットフォームを完全にバイパスするデバイス (GPS 受信機など) をインストールできます。Windows 位置情報プラットフォームの設定に関係なく、オンライン サービスは PC の IP アドレスを使用してそのおおよその位置 (通常は PC がある都市) を特定できます。

収集、処理、または送信される情報

Windows 位置情報プラットフォーム自体は、PC の情報を一切送信しません。ただし、位置認識に対応したアプリを使用する場合、Windows 位置情報取得機能などの個々の位置情報取得機能が情報を送信することがあります。位置情報プラットフォームを使用して位置を特定することが承認されたアプリも、情報を送信または保存することがあります。

情報の用途

Windows 位置情報プラットフォームを有効にした場合、承認されたアプリは PC の位置情報にアクセスし、ユーザーに合わせたコンテンツを提供することができます。サードパーティのアプリまたは位置情報取得機能を使用している場合、PC の位置情報の用途にはサードパーティのプライバシーの方針が適用されます。Windows ストア アプリをダウンロードする前に、そのアプリが位置認識に対応しているかどうかを [アプリの説明] で確認できます。

選択および管理

Windows のセットアップ時に簡単設定を選択して、Windows 位置情報プラットフォームを有効にします。設定をカスタマイズする場合は、[アプリと情報を共有する] の [Windows 位置情報プラットフォームをオンにして、アプリがユーザーの位置を確認できるようにする] を選択して、Windows 位置情報プラットフォームを管理できます。各ストア アプリが PC の位置情報を初めて要求したときに、位置情報へのアクセスを許可するかどうかをたずねるメッセージが表示されます。位置情報の要求をアプリに許可するかどうかは、PC 設定の [プライバシー] で制御できます。また、個々のストア アプリに位置情報の使用を許可するかどうかは、アプリの設定チャームの [アクセス許可] で制御できます。

Windows 位置情報プラットフォームを使用するデスクトップ アプリを使用している場合、そのデスクトップ アプリは PC の位置情報を使用するためのユーザーのアクセス許可を要求します。そのデス

クトップアプリが PC の位置情報にアクセスすると、PC の位置情報がアクセスされたことを警告するアイコンが通知領域に表示されます。各ユーザーは、PC 設定の [プライバシー] で、すべてのアプリの位置情報の設定を管理できます。また、管理者は、コントロールパネルの [位置情報] で、すべてのユーザーに対して Windows 位置情報プラットフォームを無効にすることができます。

Windows 位置情報取得機能

この機能について

Windows 位置情報取得機能は、オンラインの Microsoft 位置情報サービスに接続します。Microsoft 位置情報サービスは、PC の近くにある Wi-Fi ネットワークまたは PC の IP アドレスに基づいて PC のおおよその位置を特定します

収集、処理、または送信される情報

位置情報を受信することを承認されたアプリが位置情報を要求すると、Windows 位置情報プラットフォームは、インストールされているすべての位置情報取得機能 (Windows 位置情報取得機能を含む) に対し、現在の位置を特定するように要求します。Windows 位置情報取得機能は最初に、位置認識に対応したアプリから以前に要求されたときに保存した Wi-Fi アクセス ポイントの一覧があるかどうかを確認します。近くの Wi-Fi アクセス ポイントの一覧がまだない場合、または一覧が古い場合は、近くの Wi-Fi アクセス ポイントに関する情報と GPS 情報 (存在する場合) を Microsoft 位置情報サービスに送信します。Microsoft 位置情報サービスは PC のおおよその位置を Windows 位置情報取得機能に返します。この位置情報は、Windows 位置情報取得機能から Windows 位置情報プラットフォームに渡され、続いて Windows 位置情報プラットフォームから PC の位置情報を要求したアプリに提供されます。また、Windows 位置情報取得機能は、保存済みの Wi-Fi アクセス ポイントの一覧を更新する場合があります。Windows 位置情報取得機能は、毎回インターネットに接続せずに PC のおおよその位置を特定できるように、この一覧を保持します。このアクセス ポイントの一覧は、アプリが直接アクセスできないように、ディスクへの保存時に暗号化されます。

送信される近くの Wi-Fi アクセス ポイントに関する情報は、BSSID (Wi-Fi アクセス ポイントの MAC アドレス) とシグナルの強さです。GPS 情報には、観測された緯度、経度、方向、速度、および高

度が含まれます。Windows 位置情報取得機能では、お客様のプライバシーを保護するため、すべてのインターネット接続で送信される標準的なコンピューター情報を除き、PC を一意に識別するために情報が送信されることはありません。Wi-Fi ネットワークの所有者のプライバシーを保護するため、Windows では SSID (Wi-Fi アクセス ポイント名) や隠し Wi-Fi ネットワークは送信されません。プライバシーおよびセキュリティ上の理由により、送信される Wi-Fi ネットワークに関する情報は SSL によって暗号化されます。

情報の用途

この情報は、承認されたアプリが PC のおおよその位置を要求したときに、Windows 位置情報プラットフォームにその位置を提供するために使用されます。

Microsoft 位置情報サービスの向上に協力することを選択した場合、送信される Wi-Fi および GPS に関する情報は、Microsoft の位置情報サービスの向上に使用されます。これにより、アプリに提供される位置情報サービスが向上します。Microsoft では、このサービスによって収集されたデータを使用して、お客様を識別したり、連絡したり、広告の対象としたりできる場合や、PC の位置情報履歴を追跡または作成できる場合は、データを保存しません。

選択および管理

Windows 位置情報取得機能は、承認されたアプリが PC の位置を要求した場合にのみ使用されます。アプリが位置情報を要求できるかどうかを制御する方法の詳細については、「Windows 位置情報プラットフォーム」セクションを参照してください。アプリによる位置情報の要求を承認した場合、Windows 位置情報取得機能によって暗号化および保存される、近くの Wi-Fi アクセス ポイントの位置のキャッシュされた一覧は定期的に削除および置換されます。

Windows のセットアップ時に簡単設定を選択した場合は、Microsoft 位置情報サービスの向上に協力することを選択します。設定をカスタマイズする場合は、**[Windows とアプリの機能向上のために、情報を Microsoft に送る]** の **[Microsoft のサービスの機能向上のために、位置情報認識アプリを使う場合に一部の位置データを送る]**を選択して、Microsoft 位置情報サービスの向上に協力するかどうかを管理できます。Windows のセットアップ後に、コントロールパネルの **[位置情報の設定]** でこの設定を変更できます。サービスの向上に協力しない場合でも、Windows 位置情報取得機能を使用し

て、PC のおおよその位置を特定することができます。

Windows 位置情報取得機能は、コントロール パネルの **[Windows の機能の有効化または無効化]** を開いて、有効または無効にすることができます。Windows 位置情報取得機能を無効にした場合でも、Windows 位置情報プラットフォームで他の位置情報取得機能 (GPS など) を使用できます。

[ページのトップへ](#)

名前とアカウントの画像

この機能について

各ユーザーに合わせたコンテンツを提供するために、アプリはユーザーの名前とアカウントの画像を Windows に要求することができます。ユーザーの名前とアカウントの画像は、PC 設定の [ユーザー] の [お使いのアカウント] の下に表示されます。Microsoft アカウントを使用して Windows にサインインした場合、Windows はそのアカウントに関連付けられた名前とアカウントの画像を使用します。アカウントの画像を選択していない場合、アカウントの画像は Windows によって提供される既定の画像です。

収集、処理、または送信される情報

アプリが名前とアカウントの画像にアクセスすることを許可した場合、Windows は要求したすべてのアプリにその情報を提供します。アプリはこの情報を保存または送信することがあります。

ドメイン アカウントを使用して Windows にサインインし、アプリが名前とアカウントの画像にアクセスすることを許可した場合、Windows 資格情報を使用できるアプリは、他の形式の特定のドメイン アカウント情報にアクセスできるようになります。この情報には、ユーザー プリンシパル名 (jack@contoso.com など) や DNS ドメイン名 (corp.contoso.com\jack など) などが含まれます。

Microsoft アカウントを使用して Windows にサインインした場合、または Microsoft アカウントに関連付けられたドメイン アカウントを使用して Windows にサインインした場合、Windows は PC 上のアカウントの画像と Microsoft アカウントの画像を自動的に同期できます。

情報の用途

サードパーティのアプリを使用している場合、アプリによる名前とアカウントの画像の用途にはサードパーティのプライバシーの方針が適用されます。Microsoft のアプリを使用している場合、アプリのプライバシーの方針はプライバシーに関する声明で説明されています。

選択および管理

Windows のセットアップ時に簡単設定を選択すると、アプリから自分の名前とアカウントの画像にアクセスできるようになります。設定をカスタマイズする場合は、**【アプリと情報を共有する】**の**【Windows 位置情報プラットフォームをオンにして、アプリがユーザーの位置を確認できるようにする】**を選択して自分の名前とアカウントの画像へのアクセスを管理できます。この設定は、Windows のセットアップ後に PC 設定の**【プライバシー】**で変更できます。PC 設定の**【パーソナル設定】**でアカウントの画像を変更できます。特定のアプリにアカウントの画像の変更を許可することもできます。

[ページのトップへ](#)

ネットワーク認識

この機能について

ネットワーク アクセスを介した (モバイル ブロードバンド接続経由など) サブスクリプション プランがある場合、この機能で、サブスクリプション プランに関する情報を PC 上のアプリと Windows 機能に提供します。Windows 機能とアプリは、この情報を使用して動作を最適化できます。たとえば、従量制課金接続プランを利用している場合、Windows Update では、ユーザーが別の種類のネットワークに再接続するまで PC に優先度の低い更新プログラムを配信するのを待機します。この機能では、シグナルの強さや PC がインターネットに接続されているかどうかなど、ネットワーク接続に関する情報も提供します。

収集、処理、または送信される情報

この機能は、PC のドメイン名サービス (DNS) サフィックス、ネットワーク名、PC が接続しているネットワークのゲートウェイアドレスなどのインターネットおよびイントラネット ネットワーク接続情報を収集します。この機能では、プランに残っているデータ量など、サブスクリプション プラン情報も受信します。

ネットワーク接続性プロファイルには、アクセスしたすべてのネットワークの履歴や、最後に接続した日時を含めることができます。この機能では、Microsoft サーバーに接続して、ユーザーがインターネットに接続しているかどうかを判断できます。ネットワーク接続チェック中に Microsoft へ送信されるデータは、標準の PC 情報だけです。

情報の用途

データが Microsoft に送信された場合、そのデータはネットワーク接続の状態を提供するためにのみ使用されます。ネットワーク接続の状態は、ネットワーク接続情報を要求している PC 上のアプリや機能で使用できます。サードパーティのアプリを使用している場合、収集される情報の用途にはサードパーティのプライバシーの方針が適用されます。

選択および管理

ネットワーク認識は既定で有効になっています。管理者は、コントロールパネルの [管理ツール] で [サービス] のオプションを使用して、これらを無効にすることができます。一部の Windows 機能が正常に動作しなくなるため、この機能の無効化はお勧めしません。

[ページのトップへ](#)

通知、ロック画面に表示するアプリ、タイルの更新

Windows ストア アプリは、自動的にコンテンツを受信し、さまざまな方法で通知を表示することができます。たとえば、受信した通知を画面の隅やアプリ タイル (タイルがスタート画面にピン留めされている場合) に表示することができます。必要であれば、これらの通知をロック画面で受信することもできます。また、ロック画面には、特定のアプリのステータスを詳細に、または簡潔に表示することができます。Windows ストア アプリには、アプリの発行者が、Microsoft サーバー上で動作する Windows プッシュ通知サービスを通じてコンテンツを送信できるほか、アプリがサードパーティのサーバーから直接情報をダウンロードすることもできます。

通知

この機能について

Windows ストア アプリは、画面の隅に通知として一時的に表示さ

れる定期的な情報またはリアルタイムの情報を配信できます。

収集、処理、または送信される情報

アプリによる通知には、テキスト、画像、またはその両方を使用できます。通知のコンテンツは、アプリからローカルに提供することができます (時計アプリのアラームなど)。アプリのオンライン サービスから Windows プッシュ通知サービスを介して通知を送ることもできます (ソーシャル ネットワークの更新など)。通知に表示される画像は、アプリの発行者によって指定されたサーバーから直接ダウンロードできます。このとき、そのサーバーには、標準的なコンピュータ情報が送信されます。

情報の用途

Microsoft はアプリからユーザーへ通知を配信するためにのみ通知情報を使用します。通知は、PC に配信される前に、Windows プッシュ通知サービスによって一時的に保存されることがあります。通知がすぐに配信できない場合は、削除されるまで数分間のみ保存されます。

選択および管理

通知は、PC 設定の **通知** で、すべてのアプリまたは特定のアプリに対してオフにすることができます。特定のアプリに対して通知をオフにしたり、アプリをアンインストールした場合でも、アプリの発行者は Windows プッシュ通知サービスに更新情報を送信できますが、それらの通知が PC に表示されることはありません。

ロック画面のアプリ

この機能について

一部のアプリは、PC がロックされているときに、ステータスや通知を画面に表示できます。ロック画面に表示されるアプリは、使用されていないときでも、バックグラウンドでタスクを実行できます (電子メールの同期など)。

収集、処理、または送信される情報

ロック画面に表示されるアプリは、アプリの発行者から Windows プッシュ通知サービスを通じて、あるいは、アプリの発行者 (または別のサードパーティ) のサーバーから直接、ステータスの更新を受け取ることができます。通知や最新情報とは関係のない情報が、ロック画面のアプリによって送信、処理される場合もあります。

情報の用途

Windows は、ロック画面のアプリから提供されるステータス情報や通知情報を使用してロック画面を更新します。

選択および管理

Windows をセットアップすると、メール、カレンダー、メッセージングの各アプリは、自動的にロック画面に表示するアプリとして設定されます。こうしたロック画面のアプリは、[PC 設定] の [パーソナル設定] で追加または削除できます。また、特定のアプリを 1 つ選んで、詳細なステータスをロック画面に常時表示することもできます (カレンダー上で次に迫っている約束の詳細情報など)。

ロック画面のアプリがロック画面に通知を表示できるかどうかは、[PC 設定] の [通知] で制御できます。

タイルの更新

この機能について

Windows ストア アプリは、スタート画面でアプリのタイルへの更新として表示される定期的な情報またはリアルタイムの情報を配信できます。

収集、処理、または送信される情報

スタート画面にピン留めされているストア アプリでは、テキスト、画像、またはその両方を使用してタイルを更新できます。アプリのタイルに表示されるコンテンツは、アプリからローカルに設定できるほか、アプリの発行者によって指定されたサーバーから定期的にダウンロードしたり、アプリのオンライン サービスから Windows プッシュ通知サービスを介して送信したりすることもできます。アプリの発行者によって指定されたサーバーからタイルのコンテンツを直接ダウンロードした場合、そのサーバーには、標準的なコンピューター情報が送信されます。

情報の用途

Microsoft はアプリからユーザーへタイルの更新を配信するためにのみタイルの情報を使用します。この情報は、PC に配信される前に、Windows プッシュ通知サービスによって一時的に保存されることがあります。タイルの更新をすぐに配信できない場合、削除されるまで数日間のみ保存されます。

選択および管理

アプリがタイルの更新を受信し始めてからタイルの更新を無効にするには、スタート画面でアプリのタイルを選択し、アプリで使用可能なコマンドの中から【ライブ タイルをオフにする】を選択します。スタート画面からアプリのタイルのピン留めを外すと、それ以後、タイルの更新は表示されません。アプリをアンインストールした場合でも、アプリの発行者が Windows プッシュ通知サービスに更新情報を送信できますが、それらが PC に表示されることはありません。

スタート画面のタイルに表示されている現在の更新を消去するには、スタート画面の右側からスワイプするか右上隅をポイントし、【設定】をタップまたはクリックし、【タイル】をタップまたはクリックします。【タイルから更新情報を消去】で、【消去】をタップまたはクリックします。最新の更新をクリアした後に配信されるタイルの更新は、引き続き表示されます。

[ページのトップへ](#)

プリントの注文

この機能について

プリントの注文を使用すると、PC またはネットワーク ドライブ上に保存されているデジタル写真を、選択したオンラインの写真印刷サービスへ送信することができます。このサービスによって、写真をプリントして郵送してもらうか、地元の店でプリントを受け取ることができます。

収集、処理、または送信される情報

オンラインの写真印刷サービスで注文を行った場合、デジタル写真はインターネットで選択したサービスに送信されます。サービスが画像を表示およびアップロードできるように、選択したデジタル写真へのファイルパス（ユーザー名を含む場合があります）がサービスに送信される場合があります。デジタル写真ファイルには、カメラによってファイルに保存された画像についてのデータ（撮影日時など）、またはカメラに GPS 機能が搭載されている場合は撮影場所が含まれる可能性があります。ファイルには、デジタル写真管理アプリと Windows エクスプローラーの使用を通じてファイルと関連付けられる可能性のある個人情報（キャプションなど）が含まれる可能

性があります。詳細については、以降の「プロパティ」セクションを参照してください。

プリントの注文でオンラインの写真印刷サービスを選択すると、[プリントの注文] ウィンドウ内に表示されたサービスの Web サイトへ移動します。オンラインの写真印刷サービスの Web サイトに入力した情報は、サービスへ伝送されます。

情報の用途

カメラによってデジタル写真ファイルに保存された情報は、印刷プロセス中、画像の色や鮮明さの調節などのために、オンラインの写真印刷サービスによって使用される場合があります。デジタル写真管理アプリに保存された情報は、プリント コピーの表または裏面にキャプションとしてプリントするために、オンラインの写真印刷サービスで使用される場合があります。オンラインの写真印刷サービスによって、この情報、およびユーザーがサービスに対して提供したその他の情報 (Web サイト上に入力した情報など) の使用は、それらサービスのプライバシー基準に従うことになります。

選択および管理

プリントの注文を使用して、送信する写真と、写真の印刷に使用するサービスを選択することができます。一部の写真管理アプリでは、プリントする写真の送信前に、保存されたユーザーの個人情報を削除できるようにしている場合があります。また、ファイルのプロパティを編集して、保存した個人情報を削除することもできます。

[ページのトップへ](#)

プログラム互換性アシスタント

この機能について

実行しようとしているアプリで互換性に関する問題が見つかった場合は、プログラム互換性アシスタントでその問題を解決できます。

収集、処理、または送信される情報

実行しようとしているアプリで互換性の問題が見つかった場合、アプリ名、アプリのバージョン、必要な互換性の設定、これまでのアプリの操作などの情報を含むレポートが生成されます。互換性のな

いアプリについての問題は、 エラー報告または
カスタマー エクスペリエンス向上プログラム (CEIP) を通じて
Microsoft に報告されます。

情報の用途

エラー報告は、アプリを報告する問題に対する応答を提供するのに
使用されます。応答には、アプリの発行者の Web サイトへのリン
ク (利用可能な場合) が含まれます。これにより、ユーザーが考えら
れる解決策についての詳細を確認することができます。アプリの失
敗によって作成されたエラー報告は、このバージョンの Windows
で実行するアプリに対する、互換性の問題が生じた場合に、どの設
定を調整してみるのかを決定するために使用されます。CEIP を通じ
て報告された情報は、アプリの互換性の問題を特定するために使用
されます。

Microsoft が、この機能で収集した情報を使用してお客様を識別した
り、お客様に連絡を差し上げたり、広告をお送りすることはありま
せん。

選択および管理

Windows エラー報告を通じて報告される問題に関しては、オンライ
ンで解決策を確認するためのオプションを選択した場合にのみエラ
ー レポートが作成されます。解決策を確認するために自動的に問題
を報告するようユーザーが事前に同意した場合を除き、エラー レポ
ートを送信するかどうかをたずねるメッセージが表示されます。詳
細については、「Windows エラー報告」のセクションを参照してく
ださい。

Windows CEIP に参加するように選択した場合、一部の問題は自動
的に CEIP を通じて報告されます。詳細については、「Windows カ
スタマー エクスペリエンス向上プログラム」のセクションを参照し
てください。

[ページのトップへ](#)

プロパティ

この機能について

プロパティは、ファイルをすばやく検索したり整理したりするこ
とができるファイル情報です。プロパティには、ファイル固有のもの

(ファイルのサイズなど)と、アプリまたはデバイス特有のもの(写真を撮る際のカメラの設定や、写真についてカメラによって記録される位置データなど)があります。

収集、処理、または送信される情報

保存される情報の種類は、ファイルやそれを使用するアプリの種類によって異なります。プロパティの例には、ファイル名、更新日、ファイルサイズ、作成者、キーワードやコメントが含まれます。プロパティはファイル内に保存され、ファイルが共有されたり、電子メールの添付ファイルとして送信されたりするなど、別の場所に移動またはコピーされる場合はファイルと一緒に移動します。

情報の用途

プロパティを使用すると、ファイルをよりすばやく検索したり整理したりできます。アプリで使用し、アプリ特有のタスクを実行することもできます。Microsoft には情報は送信されません。

選択および管理

Windows エクスプローラーでファイルを選択して[プロパティ]をクリックすると、ファイルのプロパティの一部を編集または削除することができます。更新日、ファイルサイズ、ファイル名などの固有プロパティ、およびアプリ特有プロパティはこの方法で削除できません。アプリ特有のプロパティについては、ファイルの作成に使用されるアプリがこれらの機能をサポートする場合にのみ編集または削除できます。

[ページのトップへ](#)

近接

近距離近接サービス

この機能について

PC に近距離通信 (NFC) ハードウェアが備えられている場合、NFC ハードウェア付きの別のデバイスを PC に物理的にタップして、リンク、ファイル、およびその他の情報を共有することができます。近接接続には、Tap and Do と Tap and Hold の 2 種類があります。Tap and Do では、Wi-Fi、Wi-Fi Direct、または Bluetooth を使用して、デバイス間の短時間または長時間の接続を作成できます。Tap and Hold では、デバイスが隣接している間だけ接続がアク

タイプになります。

収集、処理、または送信される情報

近接対応デバイスをタップして合わせると、相互の接続を確立するための情報が交換されます。このデータには、デバイスの構成によって、Bluetooth および Wi-Fi のネットワーク アドレスと PC の名前が含まれることがあります。

接続が確立されると、特定の近接機能または使用中のアプリに応じて、その他の情報がデバイス間で交換されることがあります。Windows では、近接接続を使用して、ファイル、リンク、およびその他の情報をデバイス間で送信できます。近接を使用するアプリは、アクセス権が与えられている情報を送受信できます。この情報は、ネットワーク、インターネット接続、またはデバイス間ワイヤレス接続を通じて送信される可能性があります。

情報の用途

近接接続を通じて交換されるネットワークおよび PC の情報は、ネットワーク接続を確立したり、相互に接続するデバイスを特定したりするために使用されます。アプリ内で開始された近接接続を通じて転送されるデータは、そのアプリによって使用される可能性があります。Microsoft には情報は送信されません。

選択および管理

近距離近接サービスは既定で有効になっています。管理者は、コントロール パネルの [デバイスとプリンター] に提供されているオプションを使用して、これを無効にすることができます。

タップして送信

この機能について

Windows の "タップして送信" を使用すると、隣に立っている友人、または携帯電話などの別のデバイスと選択した情報を簡単に共有することができます。たとえば、ブラウザーを使用しているときは、[デバイス] ウィンドウからタップして送信を開始することができます。タップした隣のデバイスは、現在表示されている Web ページへのリンクを受け取ります。これは、画像、テキスト、ファイルなどの情報の共有をサポートするアプリでも機能します。

収集、処理、または送信される情報

タップして送信では、共有している情報と、近距離近接サービスのセクションで説明した情報を使用します。

情報の用途

この情報は、2つのデバイス間の接続を作成するためにのみ使用されます。共有される情報は、タップして送信には保存されません。Microsoft には情報は送信されません。

選択および管理

近距離近接サービスが有効になっている場合、タップして送信も有効になります。詳細については、「近距離近接サービス」セクションを参照してください。

[ページのトップへ](#)

リモート アクセス接続

この機能について

リモート アクセス接続では、仮想プライベート ネットワーク (VPN) 接続およびリモート アクセス サービス (RAS) を使用してプライベート ネットワークに接続することができます。RAS は、クライアント PC (通常はユーザーの PC) をホスト PC (リモート アクセス サーバーとも呼ばれます) に業界標準プロトコルを使用して接続するコンポーネントです。VPN テクノロジーを利用すると、インターネットを通じて会社のネットワークなどのプライベート ネットワークに接続できます。

リモート アクセス接続のコンポーネントであるダイヤルアップ ネットワークにより、ダイヤルアップ モデム、またはケーブル モデムやデジタル加入者線 (DSL) などのブロードバンド技術を使用してインターネットにアクセスできます。ダイヤルアップ ネットワークには、RAS クライアント、接続マネージャー、RAS 電話などのダイヤラー コンポーネント、および rasdial などのコマンドライン ダイヤラーが含まれます。

収集、処理、または送信される情報

ダイヤラー コンポーネントは、ユーザーの PC から、ユーザー名、パスワード、ドメイン名などの情報を収集します。この情報は、接続しようとしているシステムに送信されます。ユーザーのプライバ

シーおよび のセキュリティを保護するために、ユーザー名やパスワードなどのセキュリティに関する情報は暗号化されてユーザーの PC に保存されます。

情報の用途

ダイヤラー情報は、ユーザーの PC をインターネットに接続するために使用されます。リモート アクセス サーバーはアカウントिंगと準拠の目的でユーザー名と IP アドレスの情報を保持することがありますが、Microsoft へ情報が送信されることはありません。

選択および管理

コマンド ライン以外のダイヤラーの場合、[このユーザー名とパスワードを 保存する]をオンにすることでパスワードの保存を選択できます。また、いつでもそのオプションをオフにすることで、以前保存したパスワードをダイヤラーから削除できます。このオプションは既定ではオフになっているので、インターネットまたはネットワークに接続するためのパスワードの入力を求められる場合があります。Rasdial などのコマンド ライン ダイヤラーの場合、パスワードを保存するオプションはありません。

[ページのトップへ](#)

RemoteApp とデスクトップ接続

この機能について

RemoteApp とデスクトップ接続を使用すると、リモート アクセス用に公開されたリモート PC のアプリやデスクトップにアクセスすることができます。

収集、処理、または送信される情報

接続を有効にすると、指定したリモート URL から構成ファイルがユーザーの PC にダウンロードされます。これらの構成ファイルは、リモート PC のアプリとデスクトップにリンクします。これにより、ユーザーが自分の PC からこれらを実行できます。PC は、定期的にこれらの構成ファイルに対する更新を自動的にチェックしてダウンロードします。これらのアプリはリモート PC で実行し、アプリに入力した情報は、接続を選択したリモート PC にネットワークを介して送信されます。

情報の用途

構成ファイルへの更新プログラムには、新しいアプリへのアクセスの提供など設定の変更が含まれる場合がありますが、新しいアプリは、実行を選択した場合にのみ実行されます。この機能は、リモートアプリを実行しているリモート PC にも情報を送信します。リモートアプリによるこのデータの使用は、アプリの提供者およびリモート PC の管理者のプライバシー ポリシーに従います。Microsoft には情報は送信されません。

選択および管理

RemoteApp とデスクトップ接続を使用するかどうかを選択することができます。コントロールパネルの [RemoteApp とデスクトップ接続] で RemoteApp とデスクトップ接続を追加または削除できます。**[RemoteApp とデスクトップ接続の新しい接続設定]**をクリックし、ダイアログ ボックスで [接続 URL] を入力すると、新しい接続を追加できます。[接続 URL] は、電子メール アドレスを使用して取得することもできます。接続の詳細ダイアログ ボックスで **[削除]** をクリックすると、接続およびその接続ファイルを削除できます。開いているすべてのアプリを閉じないで接続を切断すると、これらのアプリはリモート PC で開いたままになります。RemoteApp とデスクトップ接続は、コントロールパネルの [プログラムの追加と削除] のリスト内には表示されません。

[ページのトップへ](#)

リモート デスクトップ接続

この機能について

リモート デスクトップ接続により、リモート デスクトップ サービスを実行中のホスト PC でリモート接続を確立できます。

収集、処理、または送信される情報

リモート デスクトップ接続設定は、アプリのローカル記憶域内、または PC のリモート デスクトップ プロトコル (RDP) ファイル内に保存されます。これらの設定には、ドメイン名と、(リモート PC の名前、ユーザー名、表示情報、ローカル デバイス情報、オーディオ情報、クリップボード、接続設定、リモート アプリ名、セッションアイコンまたは縮小表示などの) 接続構成設定が含まれます。

これらの接続の資格情報、リモート デスクトップ ゲートウェイの資格情報、信頼できるリモート デスクトップ ゲートウェイ サーバー名のリストはローカル PC に保存されます。このリストは、管理者によって削除されない限り保存されます。Microsoft には情報は送信されません。

情報の用途

リモート デスクトップ 接続によって収集された情報によって、ご希望の設定を使用してリモート デスクトップ サービスを実行しているホスト PC に接続できるようになります。ユーザー名、パスワード、およびドメイン情報が収集されるため、接続設定を保存し、RDP ファイルをダブルクリックする（またはお気に入りをクリックする）ことによって接続を起動することができ、この情報を再入力する必要がありません。

選択および管理

リモート デスクトップ 接続を使用するかどうかを選択することができます。使用する場合、RDP ファイルおよびリモート デスクトップ 接続のお気に入りには、接続の自動保存時に構成されたオプションや設定などの、リモート PC に接続するために必要な情報が含まれます。RDP ファイルおよびお気に入りをカスタマイズすると、別の設定で同一の PC に接続するためのファイルを含めることができます。保存した資格情報を修正するには、コントロール パネルの [ユーザー アカウント] で [資格情報マネージャー] を開きます。

[ページのトップへ](#)

Microsoft アカウントでのサインイン

この機能について

Microsoft アカウント (以前の Windows Live ID) は、Microsoft のアプリ、サイト、およびサービスにサインインして、Microsoft パートナーを選択する際にサインイン情報として使用できる単一の電子メールアドレスとパスワードです。Microsoft アカウントは Windows で取得できます。また、Microsoft アカウントでのサインインを要求する Microsoft の Web サイトで取得することもできます。

Microsoft アカウントを使用して Windows にサインインするか、ローカル アカウントまたはドメイン アカウントを Microsoft アカ
Windows

トに関連付けることができます。これを行った場合、[こちら](#)は Windows アプリと Microsoft アプリの設定と情報を自動的に同期することにより、PC の外観を同じにすることができます。これらの Web サイトのサインイン ページにアクセスすると、Microsoft アカウントを使用してサインインする Web サイトにも自動的にサインインします。

収集、処理、または送信される情報

PC の設定中に、または PC 設定の [ユーザー] で Microsoft アカウントとして使用する電子メール アドレスを入力すると、その電子メール アドレスが Microsoft に送信され、その電子メール アドレスに関連付けられた Microsoft アカウントが既に存在するかどうかを確認されます。お客様が既にその電子メール アドレスを Microsoft アカウントとして使用している場合は、その電子メール アドレスとパスワードを Microsoft アカウントとして使用して Windows にサインインできます。お客様の Microsoft アカウントのセキュリティ情報がまだ不足している場合、Microsoft では、お客様がアカウントにサインインできない場合にアカウントがお客様のものであることを確認するために使用できるその他のセキュリティ情報（携帯電話番号など）を最初に要求することがあります。Microsoft アカウントをお持ちでない場合は、任意の電子メール アドレスを使用して Microsoft アカウントを作成できます。

PC をインターネットに接続している場合、Microsoft アカウントを使用して Windows にサインインするたびに、電子メール アドレスとパスワードが Microsoft のサーバーで確認されます。Microsoft アカウントまたは Microsoft アカウントに関連付けられたドメイン アカウントを使用して Windows にサインインすると、次の処理が実行されます。

- Microsoft アカウントでサインインする PC 間で特定の Windows 設定が同期されます。同期される設定とそれを制御する方法の詳細については、「[PC 設定の同期](#)」を参照してください。
- 認証に Microsoft アカウントを使用する Microsoft アプリ（メール、カレンダー、フォト、People、メッセージング、OneDrive、Microsoft Office、およびその他のアプリ）は、自動的にユーザー情報のダウンロードを開始できます。たとえばメール アプリは、ユーザーの Outlook.com または

Hotmail.com アドレス (所有している場合) に送信されたメッセージを自動的にダウンロードします。

- Web ブラウザーでは、Microsoft アカウントでサインインする Web サイトに自動的にサインインできます (たとえば、OneDrive.com にアクセスすると、Microsoft アカウントのパスワードを再入力せずに自動的にサインインできます)。

Windows は、ユーザーの Microsoft アカウントに関連付けられたプロフィール情報またはその他の個人情報の使用をサードパーティのアプリに許可する前に、ユーザーのアクセス許可を要求します。Microsoft アカウントに関連付けられたドメイン アカウントを使用して Windows にサインインした場合は、選択した設定と情報がドメイン アカウントと同期され、上で説明したように自動的にアプリと Web サイトにサインインします。ドメイン管理者は PC 上のすべての情報にアクセスできるため、ユーザーが Microsoft アカウントを使用して他の PC と同期することを選択した設定および情報にもアクセスできます。これには、名前やアカウントの画像などの設定およびブラウザーの履歴が含まれます。同期される設定とそれを制御する方法の詳細については、「PC 設定の同期」を参照してください。

情報の用途

Windows で新しい Microsoft アカウントを作成する場合、お客様が入力した情報はアカウントの作成とセキュリティ保護に使用されます。たとえば、入力したセキュリティ情報 (電話番号や連絡用メールアドレスなど) は、お客様がアカウントにサインインできない場合にのみ使用されます。Microsoft アカウントを使用して Windows にサインインすると、Windows は Microsoft アカウントの情報を使用してアプリと Web サイトに自動的にサインインします。Microsoft アカウントを所有することによるプライバシーへの影響については、[メールアドレスを新規登録する] を選択したときに表示される [プライバシーに関する声明](#) をお読みください。個々の Microsoft アプリで Microsoft アカウントに関連付けられた情報を使用する方法については、そのアプリのプライバシーに関する声明を参照してください。Microsoft アプリのプライバシーに関する声明は、アプリの設定チャームまたは [バージョン情報] ダイアログ ボックスで確認することができます。

選択および管理

Microsoft アカウントを使用して Windows にサインインすると、一部の設定が自動的に同期されます。同期される Windows 設定を変更する方法または同期を停止する方法の詳細については、「PC 設定の同期」セクションを参照してください。認証のために Microsoft アカウントを使用する Microsoft アプリで収集されるデータの詳細については、そのアプリのプライバシーに関する声明をお読みください。Windows Live アプリ (メール、カレンダー、フォト、People、メッセージング、OneDrive) のプライバシーに関する声明は、go.microsoft.com/fwlink/?LinkId=257483にアクセスして確認できます。Microsoft Office のプライバシーに関する声明は、go.microsoft.com/fwlink/?LinkId=257484で確認できます。また、アプリのプライバシーに関する声明は、アプリの設定チャームまたは [バージョン情報] ダイアログ ボックスでも確認できます。

Microsoft アカウントを使用して Windows にサインインする必要はありません。PC の設定中に、または PC 設定の [ユーザー] で PC にユーザーを追加すると、ローカル アカウントまたは Microsoft アカウントを使用するように選択できます。PC 設定の [ユーザー] でいつでもローカル アカウントまたは Microsoft アカウントに切り替えることができます。ドメイン アカウントを使用して Windows にサインインした場合は、PC 設定の [ユーザー] でいつでも Microsoft アカウントとの関連付けを設定または解除できます。

Internet Explorer で InPrivate ブラウズを使用すると、Microsoft アカウントを使用する Web サイトに自動的にサインインしません。

[ページのトップへ](#)

PC 設定の同期

この機能について

Microsoft アカウントを使用して Windows にサインインすると、一部の設定と情報が Microsoft サーバーと同期され、複数の PC 間で簡単にエクスペリエンスを各ユーザーに合わせることができるようになります。Microsoft アカウントを使用して PC にサインインした後、同じ Microsoft アカウントを使用して別の PC に初めてサインインしたときに、他の PC と同期することを選択した設定と情報が Windows によってダウンロードされ、適用されます。同期することを選択した設定は、その設定を使用するときに、Microsoft サーバーと他の PC で自動的に更新されます。

収集、処理、または送信される情報

Microsoft アカウントを使用して Windows にサインインすることを選択した場合、Windows は特定の設定を Microsoft サーバーと同期します。これらの設定には次のものが含まれます。

- 言語の設定
- コンピューターの簡単操作の設定
- 個人設定 (アカウントの画像、ロック画面イメージ、デスクトップ テーマの背景、マウスの設定など)
- Windows ストア アプリの設定
- スペル チェックおよび IME 辞書
- Web ブラウザーの履歴およびお気に入り
- 保存されたアプリ、Web サイト、およびネットワークのパスワード

ユーザーのプライバシーを保護するために、同期される設定はすべて SSL で暗号化されてから送信されます。これらの設定の一部は、ユーザーが PC を信頼済み PC として Microsoft アカウントに追加するまで PC で同期されません。

Microsoft アカウントに関連付けられたドメイン アカウントを使用して Windows にサインインすると、選択した設定と情報がドメイン アカウントに同期されます。Microsoft アカウントに関連付けられたドメイン アカウントを使用して Windows にサインインしているときに保存したパスワードは同期されません。ドメイン管理者は PC 上のすべての情報にアクセスできるため、ユーザーが Microsoft アカウントを使用して他の PC と同期することを選択した設定および情報 (閲覧履歴も含む) にもアクセスできます。

情報の用途

Windows 8 は、これらの設定と情報を使用して同期サービスを提供します。ユーザーが同期した設定および情報を使用して個人を特定したり、連絡したり、広告の対象にすることはありません。

選択および管理

Microsoft アカウントを使用して Windows にサインインする場合、PC 設定の同期が有効になります。PC 設定の **PC 設定の同期** では、同期する設定を選択することや、同期の内容を制御することができます。ドメイン アカウントを使用して Windows にサインインし、そのアカウントを Microsoft アカウントに関連付けることを選択した場合、Microsoft アカウントとの関連付けが設定される前に、同期する設定をたずねるメッセージが表示されます。

[ページのトップへ](#)

Teredo テクノロジ

この機能について

Teredo テクノロジ (Teredo) により、PC およびネットワークは、複数のネットワーク プロトコルで通信できるようになります。

収集、処理、または送信される情報

ユーザーが PC を起動するたびに、Teredo はインターネット上のパブリック インターネット プロトコル バージョン 6 (IPv6) サービスを検出しようとします。これは、PC がパブリックまたはプライベート ネットワークに接続されている場合は自動的に行われますが、エンタープライズ ドメインなどの管理されたネットワークでは行われません。IPv6 接続の使用に Teredo が必要なアプリを使用している場合、または IPv6 接続を常に有効化しようファイアウォールを設定している場合、Teredo はインターネットを介して Microsoft Teredo サービスに定期的に連絡します。Microsoft に送信される情報は、標準の PC 情報と、要求されたサービスの名前 (teredo.ipv6.microsoft.com など) のみになります。

情報の用途

Teredo によって PC から送信された情報は、PC がインターネットに接続しているかどうか、またパブリック IPv6 サービスを検出できるかどうかを決定するために使用されます。サービスが検出されると、IPv6 サービスとの接続を維持するために情報が送信されます。

選択および管理

netsh コマンド ライン ツールを使用して、サービスがインターネットを経由して送信するクエリを変更し、Microsoft 以外のサーバーを

代わりに使用したり、この機能を無効にしたりすることができます。詳細な指示については、この技術的なホワイトペーパーのインターネットプロトコルバージョン6、Teredo、および関連テクノロジーに関するセクションを参照してください。

[ページのトップへ](#)

トラステッドプラットフォームモジュール (TPM) サービス

この機能について

トラステッドプラットフォームモジュール (TPM) は、一部の PC に内蔵されているセキュリティハードウェアです。これがある場合、プロビジョニングすることで高度なセキュリティ機能をフル活用できるようになります。TPM を使用する Windows の機能には、BitLocker ドライブ暗号化、仮想スマートカード、セキュアブート、Windows Defender、および TPM ベースの証明書記憶域が含まれます。

収集、処理、または送信される情報

既定では、Windows は TPM の所有権を取得して完全な TPM 所有者認証情報を保存し、Windows 管理者のみが使用できるようにします。通常の実行操作と標準のユーザー操作の実行には限定的な認証値が作成され、Windows によって管理されます。

TPM 管理コンソールを使用すると、ユーザーは TPM を対話的にプロビジョニングすることができます。また、TPM をプロビジョニングした後には、USB フラッシュドライブなどの外部メディアに TPM 所有者の認証値を保存することができます。保存されたファイルには、TPM についての TPM 所有者の認証情報が含まれています。ファイルにはまた、ファイルの認識に役立つ PC 名、オペレーティングシステムのバージョン、作成者、および作成日の情報も含まれています。

ドメイン環境では、ドメイン管理者は TPM のプロビジョニング時に完全な TPM 所有者パスワードを構成し、TPM オブジェクトの Active Directory に格納することができます。

各 TPM は、その信頼性を示す一意の暗号化保証キーを持っています。保証キーは PC の製造元によって作成されて TPM に保存される場合がありますが、古い PC で作成されていない場合は、Windows

によって 内の保証キーの作成をトリガーする必要があることがあります。保証キーのプライベート部分が TPM の外部に公開されることは決してなく、いったん作成されると通常リセットできません。保証キーの証明書は、ほとんどの Windows 8 コンピューターの TPM に保存されます。保証キーの証明書は、ハードウェア TPM に保証キーが存在することを示します。証明書は、リモートの検証者が TPM が TPM の仕様に準拠していることを確認するために役立ちます。保証キーの証明書は、通常、TPM 製造元またはプラットフォーム製造元によって署名されています。

情報の用途

TPM が初期化されると、アプリは TPM を使用して、一意の暗号化キーを追加作成し、セキュリティ保護に役立てることができます。たとえば、BitLocker ドライブ暗号化は、TPM を使用してドライブを暗号化するキーを保護します。

TPM 所有者パスワードをファイルに保存することを選択した場合、このファイル内に保存された PC およびユーザーの追加情報は、該当する PC と TPM の認識に役立ちます。TPM 保証キーは、TPM に送信される前に、TPM の初期化時、Windows が TPM 所有者の認証値を暗号化するために使用されます。Windows は暗号化キーを PC 外部に送信しません。Windows は、マルウェア対策ソフトウェアのようなサードパーティのアプリに対し、認証を使用したメジャーブートなどの特定の TPM シナリオに保証キーを使用するためのインターフェイスを提供します。マルウェア対策ソフトウェアでは、ブートの測定が特定の製造元の TPM によって提供されていることを確認するために、保証キーと保証キーの証明書が役立ちます。既定では、管理者または管理者権限を持つアプリのみが TPM 保証キーを使用できます。

選択および管理

ユーザーまたは管理者は、TPM を使用する Windows の機能を有効にするか、TPM を使用するアプリを実行することによって、TPM の使用を選択します。

ユーザーは、TPM をクリアして工場出荷時の状態にリセットすることができます。TPM をクリアすると、所有者情報や、保証キー以外の、TPM の使用中にアプリが作成したすべての TPM ベースのキーまたは暗号化情報が削除されます。

ページのトップへ

ルート証明書の更新

この機能について

証明書の主な使用目的は、個人またはデバイスの身元の保証、サービスの認証、またはファイルの暗号化です。信頼されたルート証明機関とは、証明書を発行する組織です。ルート証明書の更新は、オンラインの Windows Update サービスと接続して、Microsoft が信頼できる機関の一覧に認証機関を追加しているかどうかを確認します。ただし、これが実行されるのは、直接信頼されていない証明機関によって発行された証明書 (PC の信頼された証明書の一覧に保存されていない証明書) をアプリが提示した場合だけです。Microsoft の信頼された機関の一覧に認証機関が追加されている場合、その証明書は自動的に PC 上の信頼された証明書の一覧に追加されます。

収集、処理、または送信される情報

ルート証明書の更新は、オンラインの Windows Update サービスに対して、Microsoft ルート証明書プログラムにある最新のルート証明機関一覧を求める要求を送信します。一覧に信頼されていない証明書がある場合、ルート証明書の更新は Windows Update からその証明書を取得し、PC の信頼された証明書ストアに保存します。転送される情報には、ルート証明書の名前および暗号化ハッシュが含まれます。

Windows Update とプライバシーの詳細については、「[Update サービスのプライバシーに関する声明](#)」で回復キーにアクセスしたり、回復キーを削除したりできます。

情報の用途

情報は、PC の信頼された証明書一覧を更新するために Microsoft によって使用されます。Microsoft がこの情報を使用してお客様を識別したり、連絡したり、広告の対象としたりすることはありません。

選択および管理

ルート証明書の更新は、既定では有効になっています。管理者は、グループ ポリシーを設定して、PC 上での [ルート証明書の更新] を無効にすることができます。

[ページのトップへ](#)

更新サービス

この機能について

Windows の更新サービスには Windows Update と Microsoft Update があります。

- **Windows Update** は、Windows ソフトウェア、デバイス製造元が提供するドライバーなど他のサポート ソフトウェアに対するソフトウェア更新プログラムを提供するサービスです。
- **Microsoft Update** は、Windows ソフトウェア、Microsoft Office などその他の Microsoft ソフトウェアに対するソフトウェア更新プログラムを提供するサービスです。

収集、処理、または送信される情報

PC の重要なソフトウェア更新プログラムを取得する場合、これらの更新プログラムに Windows 悪意のあるソフトウェアの削除ツール (MSRT) が含まれる場合があります。MSRT は、特定の一般的な悪意のあるソフトウェア ("マルウェア") による感染がないか PC をチェックし、検出された感染を削除する手助けとなります。このソフトウェアを実行すると、Microsoft サポート Web サイトに一覧表示されている [マルウェア](#) が削除されます。マルウェアのチェック中に、検出されたマルウェアに関する具体的な情報、エラー、および PC に関するその他の情報を含む報告が Microsoft に送信されます。詳細については、[Windows 悪意のあるソフトウェアの削除ツールのプライバシーに関する声明のページ](#) で回復キーにアクセスしたり、回復キーを削除したりできます。

更新サービスが収集するその他の情報については、「[Update サービスのプライバシーに関する声明](#)」で回復キーにアクセスしたり、回復キーを削除したりできます。

情報の用途

この MSRT 情報は、マルウェア対策ソフトウェアおよびその他のセキュリティ製品とサービスの向上に役立てるために使用されます。MSRT 報告の情報は、お客様個人を特定するためや、お客様と連絡をとるために使用されることはありません。

更新サービスでのその他の情報の使用方法については、「[Update サービスのプライバシーに関する声明](#)」で回復キーにアクセスしたり、回復キーを削除したりできます。

選択および管理

Windows のセットアップ時に簡単設定を選択した場合は、更新サービスを有効にし、自動的に更新プログラムがインストールされるように Windows Update を設定します。設定をカスタマイズする場合は、**Windows Update** の [**Windows Update**] で更新サービスを管理できます。Windows のインストール後は、コントロールパネルで更新サービスの設定を変更できます。詳細については、「[Update サービスの個人情報保護方針](#)」を参照してください。

PC で重要な更新プログラムをチェックしてインストールし、これらの更新プログラムの一部として MSRT を受信する場合は、Microsoft サポートに [記載されている手順](#) に従って、ソフトウェアの報告機能を無効にできます。

[ページのトップへ](#)

Windows カスタマー エクスペリエンス向上プログラム (CEIP)

この機能について

Windows カスタマー エクスペリエンス向上プログラム (CEIP) は、アプリ、PC、接続されているデバイス、および Windows の使用方法に関する情報を収集します。また、パフォーマンスと信頼性に関する問題がある場合は、その問題に関する情報も収集します。Windows CEIP に参加することを選択した場合、Windows から Microsoft にこのデータが送信されます。また、Windows およびアプリの使用方法について関連性の高い情報を収集するために、ファイルが定期的にダウンロードされます。CEIP 報告は、お客様が最もよく使用する機能の改善や、一般的な問題の解決に役立てることを目的に、Microsoft に送信されます。

収集、処理、または送信される情報

CEIP 報告には、次のような情報が含まれます。

- 構成情報。PC のプロセッサ数、使用しているネットワークの接続数、ディスプレイ デバイスの画面解像度、実行している Windows のバージョンなどの情報です。

- パフォーマンスと信頼性に関する情報。ボタンをクリックしたときのアプリの応答速度、アプリやデバイスで発生した問題の数、ネットワーク接続で情報が送受信される速度などの情報です。
- アプリの利用状況。アプリの起動頻度、Windows ヘルプとサポートの使用頻度、アプリへのサインインに使用するサービス、一般的にデスクトップに作成されるフォルダー数などの、最も頻繁に使用される機能に関する情報です。

CEIP 報告には、CEIP への参加を決定した時点から最大で 7 日前からの PC のイベントに関する情報 (イベント ログ データ) も含まれます。ほとんどのユーザーは、Windows をセットアップしてから数日以内に CEIP への参加を決定するため、Microsoft は Windows のセットアップ エクスペリエンスの分析と向上のためにこの情報を使用します。

この情報は、インターネットへの接続時に Microsoft に送信されます。CEIP 報告には、名前、住所、電話番号などの連絡先情報は含まれません。ただし、一部の報告には、PC に接続されたデバイスのシリアル番号など、個人識別子が意図せずに含まれる可能性があります。Microsoft は、CEIP 報告に含まれる情報をフィルタリングして、含まれている可能性がある個人識別子を削除することに努めます。

CEIP では、各 CEIP 報告と共に Microsoft に送信されるグローバル一意識別子 (GUID) と呼ばれる番号がランダムに生成されます。GUID を使用して、長期間特定のコンピューターから送信されるデータを確認できます。Windows と同時にライセンスされる、プリインストール済みの Microsoft アプリは、独自の一意識別子を生成して CEIP に使用する場合があります。この識別子はユーザーの Microsoft アカウントの情報に基づいて作成される場合があります。

また CEIP では、Windows とアプリの使用方法について関連性の高い情報を収集するために、定期的にファイルをダウンロードします。このファイルは、一般的な問題の解決策を作成し、Windows とアプリの使用パターンを詳細に分析するための情報を収集するために役立ちます。

情報の用途

Microsoft では、Microsoft の製品やサービス、さらにはこれらの製

品やサービスを使用するサードパーティのソフトウェアおよびハードウェアを改善するために、CEIP 情報を使用します。また、Microsoft は、そのパートナーが製品とサービスを改善できるように、CEIP 情報をパートナーと共有することもあります。共有される情報は集約された形式となっており、この情報を使用して個人を特定したり、連絡したり、広告の対象とすることはできません。

Microsoft は GUID を使用して、お客様から頂くフィードバックの範囲やその重要度を識別します。たとえば、Microsoft は GUID を使用して、ある問題が 1 人のお客様に 100 回発生した場合と、ある問題が 100 人のお客様に 1 回ずつ発生した場合を区別できます。Microsoft が、CEIP によって収集された情報を使用して個人を特定したり、連絡したりすることはありません。

選択および管理

Windows のセットアップ時に簡単設定を選択した場合、Windows CEIP を有効にすると、Windows および Windows と同時にライセンスされる Microsoft アプリでは PC のすべてのユーザーに関する CEIP 報告を送信できるようになります。設定をカスタマイズする場合は、**[Windows とアプリの機能向上のために、情報を Microsoft に送る]** の **[Microsoft のサービスの機能向上のために、位置情報認識アプリを使う場合に一部の位置データを送る]** を選択して、CEIP を管理できます。Windows のセットアップ後に、管理者はコントロールパネルの [アクション センター] でこの設定を変更できます。

詳細については、オンラインの [CEIP に関するよくある質問](#) を参照してください。

[ページのトップへ](#)

Windows Defender

Windows Defender は、PC 上のマルウェアやその他の望ましくない可能性のあるソフトウェアを検索します。Microsoft Active Protection Service や履歴機能が備わっています。

Microsoft Active Protection Service

この機能について

Microsoft Active Protection Service (MAPS) コミュニティ

は、Windows Defender ユーザーを含む自主的な世界的規模のマルウェア対策コミュニティです。MAPS を通じて、マルウェアや望ましくない可能性のあるその他のソフトウェアに関する情報を Microsoft に報告できます。MAPS は、新たに検出されたマルウェアの新しいシグニチャを自動的にダウンロードすることによって PC を保護します。

収集、処理、または送信される情報

MAPS の報告には、マルウェアの可能性のあるファイルに関する情報 (ファイル名、暗号化ハッシュ、ソフトウェアの発行元、サイズ、日付スタンプなど) が含まれます。さらに、MAPS はファイルの配布元を示す完全な URL を収集する場合があります。これらの URL には、検索用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場合があります。さらに報告には、望ましくない可能性のあるソフトウェアの検出が通知された際に、ユーザーが Windows Defender で行った操作も含まれます。MAPS の報告にはこの情報が含まれ、Windows Defender がマルウェアおよび望ましくない可能性のあるソフトウェアを検出し削除する機能の有効性を Microsoft が評価したり、新しいマルウェアを識別したりするのに役立ちます。

報告は、次の場合に自動的に Microsoft に送信されます。

- Windows Defender が、まだリスク分析されていないソフトウェアを検出した場合。
- Windows Defender が、まだリスク分析されていないソフトウェアによる PC の変更を検出した場合。
- Windows Defender が、マルウェアの検出時にそのマルウェアに (自動修復の一部として) アクションを実行した場合。
- Windows Defender がスケジュールされたスキャンを完了し、ユーザーの設定に基づいて検出されたソフトウェアに対して自動的にアクションを実行した場合。

ユーザーは、MAPS に基本メンバーシップまたは上級メンバーシップで参加できます。Windows のセットアップ中に MAPS を有効にすると、基本メンバーシップでの参加が設定されます。基本メンバーシップの報告には、このセクションで説明した情報が含まれます。上級メンバーシップの報告には、さらに包括的な情報が含まれま

す。この情報には、ファイルパスや部分的なメモリ ダンプなどから収集される個人情報が含まれる場合があります。これらの報告は、MAPS に参加している他の Windows Defender ユーザーからの報告と共に、Microsoft の調査担当者が新しい脅威をより迅速に発見することを可能にします。その後、マルウェア定義が作成され、これらの更新された定義が Windows Update によってすべてのユーザーに提供されます。

基本メンバーシップまたは上級メンバーシップで MAPS に参加されている場合は、次のようになります。

- Microsoft からサンプル報告の提出をお願いする場合があります。この報告には、Microsoft が望ましくないソフトウェアである可能性を疑う、PC 内の特定のファイルが含まれます。このサンプルは、さらに詳しい分析のために使用されます。このサンプル報告を Microsoft に送信しようとするたびに、報告を送信するかどうかの確認が表示されます。
- Windows Update が Windows Defender の更新された署名を一定期間取得できないと、Windows Defender は MAPS を使用して、別のダウンロード場所から署名をダウンロードします。

ユーザーのプライバシーを保護するため、MAPS に送信される情報はすべて SSL によって暗号化されます。

情報の用途

MAPS に送信される報告は、Microsoft のソフトウェアおよびサービスを向上するために使用されます。報告は、統計およびテストや分析、定義の作成に使用される場合もあります。MAPS では、意図的に個人情報を収集することはありません。MAPS が意図せずに収集した個人情報に関して、Microsoft がその情報を使用してお客様を識別したり、連絡したり、広告の対象としたりすることはありません。

選択および管理

Windows のセットアップ時に簡単設定を選択した場合は、MAPS を有効にします。設定をカスタマイズする場合は、**[Windows とアプリの機能向上のために、情報を Microsoft に送る]** の **[Microsoft のサービスの機能向上のために、位置情報認識アプリを使う場合に一部の位置データを送る]**を選択して MAPS を管理できま

Windows

MAPS

す。 のセットアップ後に のメンバーシップや設定を変更するには (MAPS の無効化を含む)、Windows Defender の [ツール] メニューを開きます。

履歴機能

この機能について

この履歴機能は、Windows Defender が検出する PC 上のすべてのアプリと、それらのアプリが検出された際に行われた動作の一覧を提供します。

さらに、Windows Defender が PC で実行されているときに監視対象とならないアプリ (これらは許可されている項目と呼ばれます) の一覧を表示できます。また、ユーザーが削除するか、再実行を許可する選択をするまで Windows Defender が実行を抑止するアプリ (これらは検疫されている項目と呼ばれます) を表示することもできます。

収集、処理、または送信される情報

Windows Defender が検出するソフトウェアの一覧、ユーザーおよびその他のユーザーの対処内容、および Windows Defender が自動的に行った対処内容は、ユーザーの PC に自動的に保存されます。すべてのユーザーは Windows Defender の履歴を表示して、PC にインストールまたは PC で実行されそうになった、または別のユーザーが実行を許可したマルウェアやその他の望ましくない可能性のあるソフトウェアを確認できます。たとえば、新しいマルウェアの脅威について聞いた場合に、履歴をチェックして、Windows Defender がユーザーの PC を感染から防いだかどうかを確認できます。Microsoft には情報は送信されません。

選択および管理

履歴の一覧は管理者が削除できます。

[ページのトップへ](#)

Windows エラー報告 (WER)

この機能について

Windows エラー報告は、ユーザーが使用しているソフトウェアの問題を、Microsoft および Microsoft のパートナーが診断して解決策を

提供するのに役立てられます。すべての問題に解決策があるとは限りませんが、解決策が存在する場合、その解決策が、報告された問題を解決する手順、またはインストールする更新プログラムとして提示されます。問題の再発を防止しソフトウェアの信頼性をより高めるため、一部の解決策は、ソフトウェアのサービスパックおよび将来のバージョンにも含まれます。

収集、処理、または送信される情報

多くのソフトウェア製品が、Windows エラー報告サービスと連携するように設計されています。これらの製品のいずれかで問題が発生すると、報告を送信して解決策を調べるかどうかの確認が表示されます。

Windows エラー報告では、発生した問題の診断と解決に役立つ情報が収集されます。収集される情報には、問題が発生したソフトウェアまたはハードウェアの場所、問題の種類または重大度、問題の説明に役立つファイル、ソフトウェアおよびハードウェアの基本情報、ソフトウェアのパフォーマンスと互換性について考えられる問題などがあります。Windows を使用して仮想マシンをホストしている場合、Microsoft に送信されるエラー報告には、仮想マシンに関する情報が含まれることがあります。

また、Windows エラー報告では、アプリ、ドライバー、およびデバイスに関する情報を収集して、アプリとデバイスの互換性の把握と改善に役立っています。アプリに関する情報には、アプリの実行可能ファイルの名前などが含まれます。デバイスとドライバーに関する情報には、PC にインストールされたデバイスの名前、それらのデバイスのドライバーに関連付けられている実行可能ファイルなどが含まれます。アプリまたはドライバーを発行した会社に関する情報も収集されます。

Windows のセットアップ時に自動報告を有効にした場合は、報告サービスにより問題が発生した場所に関する基本情報が自動的に送信されます。一部のエラー報告には、意図せず個人情報が含まれることがあります。たとえば、PC メモリのスナップショットを含む報告には、ユーザーの名前、作業中だったドキュメントの一部、または Web サイトに最近送信したデータが含まれる場合があります。この種の情報が報告に含まれる可能性がある場合、Windows では、自動報告を有効にしている場合でも、その情報を送信するかどうかをたずねるメッセージが表示されます。ファイルやデータを含む報告

は、送信または削除するまでユーザーの PC に格納することができます。

報告の送信後に、報告サービスが、発生した問題に関する詳細情報の提供を依頼する場合があります。この回答で電話番号または電子メールアドレスを提供することを選択をした場合、エラー報告による個人特定が可能になります。お客様から報告された問題を解決するため、Microsoft がお客様に連絡してさらに情報の提供をお願いする場合があります。

Windows エラー報告サービスでは、各報告と共に Microsoft に送信されるグローバル一意識別子 (GUID) と呼ばれる番号がランダムに生成されます。GUID を使用して、長期間特定のコンピューターから送信されるデータを確認できます。この GUID には個人情報を含みません。

お客様のプライバシーを保護するために、送信される情報は SSL によって暗号化されます。

情報の用途

Microsoft は、Windows ユーザーが報告したエラーおよび問題に関する情報を Microsoft の製品やサービスの向上に使用します。また、それらの製品やサービス向けに設計されたサードパーティ製のソフトウェアおよびハードウェアの向上にも使用します。Microsoft は GUID を使用して、そのフィードバックがどの程度一般的な事象であるかを判断し、またその重大度を区別します。たとえば、Microsoft は GUID を使用して、ある問題が 1 人のお客様に 100 回発生した場合と、ある問題が 100 人のお客様に 1 回ずつ発生した場合を区別できます。

Microsoft の従業員、外注業者、ベンダー、およびパートナーには、収集された情報のうち、関連性の高い部分へのアクセスが認められる場合もありますが、この情報の用途は、Microsoft の製品やサービスの修復と向上、またはそれらの製品やサービス向けに設計されたサードパーティ製のソフトウェアおよびハードウェアの修復と向上に限定されます。エラー報告に個人情報が含まれる場合、Microsoft がこの情報を使用してお客様を特定したり、連絡したり、広告の対象にしたりすることはありません。ただし、前に説明した連絡先情報をお客様が提供することを選択した場合は、この情報を使用してお客様に連絡を取ることがあります。

選択および管理

Windows のセットアップ時に簡単設定を選択した場合は、Windows エラー報告により基本的なレポートが送信され、問題の解決策がオンラインで自動的にチェックされます。設定をカスタマイズする場合は、[【問題の解決策をオンラインで調べる】](#)の[【問題の解決策を Windows エラー報告を使って調べる】](#)を選択して、Windows エラー報告を管理できます。Windows のセットアップ後に、コントロールパネルの[【アクション センター】](#)でこの設定を変更できます。

詳細については、オンラインの [Microsoft エラー報告サービスのプライバシーに関する声明](#) で回復キーにアクセスしたり、回復キーを削除したりできます。

[ページのトップへ](#)

Windows ファイルの関連付け

この機能について

Windows ファイルの関連付けでは、ファイルの種類と特定のアプリを関連付けることができます。アプリが関連付けられていないファイルを開こうとすると、Windows では、Windows ファイルの関連付けを使用してファイルに関連付けるアプリを検索するかどうかを確認するメッセージが表示されます。これには、Windows ストア内の互換性のあるアプリの検索も含まれます。ファイル名拡張子に一般的に関連付けられているアプリが表示されます。

収集、処理、または送信される情報

Windows ファイルの関連付けの使用を選択すると、ファイル名拡張子 (docx や pdf など) と、PC の表示言語が Microsoft へ送信されます。ファイル名の残りの部分は Microsoft へは送信されません。特定のアプリとファイルの関連付けが行われると、そのアプリの一意の識別子が送信されて、ファイルの種類ごとに既定のアプリが識別されます。

情報の用途

ファイル名拡張子を送信すると、Microsoft がその拡張子のファイルを開くことができると認識しているアプリの一覧が、サービスから返されます。アプリのダウンロードおよびインストールを選択しない限り、ファイルの種類との関連付けは変わりません。

選択および管理

アプリが関連付けられていない種類のファイルを開くときに、Windows ファイルの関連付けを使用するかどうかを選択できます。サービスの使用を決定しない限り、ファイルの関連付け情報が Microsoft に送信されることはありません。

[ページのトップへ](#)

Windows ヘルプ

Windows オンライン ヘルプとサポート

この機能について

Windows オンライン ヘルプとサポートをオンにすると、インターネットに接続している場合、利用可能な最新のヘルプおよびサポート コンテンツを取得できます。

収集、処理、または送信される情報

Windows オンライン ヘルプとサポートを使用している場合は、ヘルプの検索クエリおよびリンクをクリックしたときのヘルプのコンテンツの要求が Microsoft に送信されます。的確なヘルプ コンテンツを探ることができるように、ご使用の PC の構成に関する情報が Windows によって送信されます。Windows オンライン ヘルプとサポートには、Cookie に代表される標準の Web テクノロジも使用されています。

情報の用途

Microsoft では、収集した情報を使用して、ユーザーの検索クエリに対して最も関連性の高いヘルプ トピックを返すようにしたり、新しいコンテンツを作成して既存のコンテンツの向上を図ったりします。PC の構成に関する情報は、個々のユーザーの PC の構成に応じて適切なヘルプ コンテンツを表示するために使用されます。Cookie などの Web テクノロジは、ヘルプ コンテンツの閲覧を容易にすると共に、Windows オンライン ヘルプがユーザーによってどのように使用されているかを把握するために使用されます。

選択および管理

オンライン ヘルプとサポートは既定で有効になっています。この設定を変更するには、[ヘルプとサポート] ウィンドウの上部にある

[設定] アイコンをタップまたはクリックし、[オンライン ヘルプの表示]をオンまたはオフにします。Windows ヘルプで使用されている Cookie をクリアするには、コントロールパネルの [インターネット オプション] を開いて [閲覧の履歴] で、[削除] ボタンをクリックまたはタップし、[クッキーと **Web** サイト データ] を選択して [閲覧の履歴] をクリックまたはタップします。すべての Cookie をブロックするように ([インターネット オプション] の [プライバシー] セクションで) 選択した場合、Windows ヘルプは一切 Cookie を設定しません。

ヘルプ エクスペリエンス向上プログラム

この機能について

ヘルプ エクスペリエンス向上プログラムは、Windows オンラインヘルプとサポートの利用状況の傾向を識別し、検索で返される結果やコンテンツの関連性を向上させるのに役立てられます。

収集、処理、または送信される情報

HEIP は、ユーザーの PC で稼動している Windows のバージョン、および Windows ヘルプとサポートで検索するときにユーザーが入力するクエリおよび表示されたヘルプ トピックに関する評価やフィードバックを含む、Windows ヘルプとサポートの使用状況に関する情報を Microsoft に送信します。ヘルプ トピックに関する評価またはフィードバックを検索、参照、または入力すると、この情報が Microsoft に送信されます。

HEIP では、各 HEIP 報告と共に Microsoft に送信されるグローバル一意識別子 (GUID) と呼ばれる番号がランダムに生成されます。GUID を使用して、長期間特定のコンピューターから送信されるデータを確認できます。この GUID には個人情報を含れません。この GUID は、Windows エラー報告および Windows CEIP で使用される GUID とは異なります。

情報の用途

収集されたデータは、傾向や利用パターンの特定に使用され、Microsoft が提供するコンテンツの品質や検索結果の妥当性を向上するために役立てられます。Microsoft は GUID を使用して、その問題がどの程度一般的な事象であるかを区別し、またその重大度を区別します。たとえば、Microsoft は GUID を使用して、ある問題が 1 人のお客様に 100 回発生した場合と、ある問題が 100 人のお客様

に 1 回ずつ発生した場合を区別できます。

個人を特定できるような情報をヘルプ エクスペリエンス向上プログラムが意図的に収集することはありません。ユーザーが検索ボックスやフィードバック ボックスに個人の特定につながるような情報を入力した場合、その情報はそのまま送信されますが、このように収集された情報を Microsoft が使用して個人を特定したり、連絡したり、広告の対象としたりすることはありません。

選択および管理

Windows のセットアップ中に簡単設定を選択すると、ヘルプ エクスペリエンス向上プログラムに登録されます。設定をカスタマイズする場合は、**[Windows とアプリの機能向上のために、情報を Microsoft に送る]** の **[Microsoft のサービスの機能向上のために、位置情報認識アプリを使う場合に一部の位置データを送る]** を選択して、ヘルプ エクスペリエンス向上プログラムの設定を管理できます。Windows のセットアップ後、Windows ヘルプとサポートでこの設定を変更できます。

[ページのトップへ](#)

リモート アシスタンス

この機能について

リモート アシスタンスを使用すると、近くにいない人でも、自分の PC に招待して接続し、PC の問題について支援してもらうことができます。接続すると、相手は接続先の PC 画面を表示できます。PC のユーザーが許可すると、相手は自分のマウスおよびキーボードを使用してその PC を操作し、問題解決の方法を示すことができます。

収集、処理、または送信される情報

リモート アシスタンスは、インターネットまたはローカル ネットワークを介して、2 台の PC 間に暗号化された接続を作成します。リモート アシスタンスを使用して他のユーザーの PC に接続した人は、その接続先ユーザーのデスクトップおよび開いているドキュメント (プライベートな可視情報を含める) を見ることができます。さらに、支援を受けるユーザーが他の人に、その人のマウスまたはキーボードを使用して、支援を受けるユーザーの PC を制御すること

を許可した場合、その人はファイルの削除、設定の変更などの操作を実行できます。接続が確立されると、リモート アシスタンスはユーザー名、PC 名、およびアカウントの画像を含めた連絡先情報を交換します。セッション ログ ファイルには、すべてのリモート アシスタンス接続の記録が保持されます。

情報の用途

この情報は、暗号化された接続を確立し、他のユーザーに対してお客様のデスクトップへのアクセスを許可するために使用されます。Microsoft には情報は送信されません。

選択および管理

自分の PC への接続をだれかに許可する前に、別の人に見られたくない、開いているアプリまたはドキュメントを閉じてください。その人が自分の PC 上で見ているものや実行していることについて不快に感じた場合は、Esc キーを押してセッションを終了します。セッション ログと連絡先情報の交換を無効にするには、リモート アシスタンスの設定でこれらのオプションをオフにします。

[ページのトップへ](#)

Windows Search

この機能について

Windows Search を使用すると、アプリ、設定、ファイル、アプリ内のコンテンツをすばやく一貫した方法で検索できます。

収集、処理、または送信される情報

Windows Search を使用する場合、検索フィールドに入力した文字（入力時）と最後に送信した検索クエリは Windows および検索対象のアプリにのみ渡されます。これにより、Windows またはアプリは、検索候補を提示したり検索結果を表示したりすることができます。Windows は、検索クエリとアプリ内での検索の頻度に関するデータを保存します。

情報の用途

Windows は、保存済みの以前の検索を使用して、[検索] ウィンドウに検索候補を表示します。アプリ内での検索の頻度に関する保存済みの情報は、[検索] ウィンドウで検索可能なアプリの一覧を頻度順

に並べ替えるために使用されます。サードパーティのアプリ内を検索する場合、収集される情報の用途にはサードパーティのプライバシーの方針が適用されます。Microsoft のアプリ内を検索する場合、アプリのプライバシーの方針はプライバシーに関する声明で説明されています。

選択および管理

Windows は、既定でこの情報を保存します。PC 設定で、この情報の保存を無効にしたり、過去に Search で行った保存済みの検索をすべて削除したりできます。

[ページのトップへ](#)

Windows 共有

この機能について

Windows 共有を使用すると、共有をサポートする Windows ストアアプリ間でコンテンツを共有できます。また、友人とコンテンツを共有することもできます。

収集、処理、または送信される情報

共有する場合、[共有] ウィンドウで共有先を選択した後にのみ、共有元のアプリから共有先のアプリにコンテンツが渡されます。共有元アプリが共有を実装していない場合は、画面に表示される内容のイメージを共有できます。頻繁にコンテンツを共有する共有先アプリや共有相手に簡単にアクセスできるように、[共有] ウィンドウの一覧にこれらの共有先が表示されます。Microsoft には情報は送信されません。

情報の用途

頻繁にコンテンツを共有する共有先アプリや共有相手との共有の頻度に関する保存済みの情報は、[共有] ウィンドウの一覧を頻度順に並べ替えるために使用されます。サードパーティのアプリと情報を共有する場合、収集される情報の用途にはサードパーティのプライバシーポリシーが適用されます。Microsoft のアプリと共有する場合、アプリのプライバシーの方針はプライバシーに関する声明で説明されています。

選択および管理

Windows 共有の使用状況についての情報は、Windows によって既定で保存されます。PC 設定で、この情報の保存を無効にしたり、保存済みの共有先をすべて削除したりできます。

[ページのトップへ](#)

Windows SmartScreen

この機能について

Windows SmartScreen を使用すると、開こうとしているファイルや実行しようとしているアプリを Microsoft で事前にチェックして、安全でない可能性があるファイルとアプリから PC を保護することができます。ファイルまたはアプリが不明な場合や、安全でない可能性がある場合は、それらを開く前に、どうするかをたずねるメッセージが表示されます。

収集、処理、または送信される情報

この機能を使用する場合は、使用するアプリの一部とインターネットからダウンロードするファイルの一部に関する情報が Microsoft に送信されます。この情報には、標準の PC 情報や Windows SmartScreen フィルターのバージョン番号と共にファイル名、ファイル ID ("ハッシュ")、およびデジタル証明書情報が含まれる場合があります。ユーザーのプライバシーを保護するため、Microsoft に送信される報告は SSL で暗号化されます。

Windows SmartScreen では、SmartScreen 利用状況データと共に Microsoft に送信されるグローバル一意識別子 (GUID) と呼ばれる番号がランダムに生成されます。GUID を使用して、長期間特定の PC から送信されるデータを確認できます。この GUID には個人情報は含まれません。

情報の用途

Microsoft では、安全でない可能性のあるファイルやアプリに関する警告をユーザーに提供するために上記で説明した情報を使用します。また、機能のパフォーマンスを分析し、製品やサービスの品質を向上させるためにもこの情報が使用されます。Microsoft は GUID を使用して、そのフィードバックがどの程度一般的な事象であるかを判断し、またその重大度を区別します。たとえば、Microsoft は GUID を使用して、ある問題が 1 人のお客様に 100 回発生した場合

と、ある問題が 人のお客様に 回ずつ発生した場合を区別できません。この情報を使用してお客様を識別したり、連絡したり、広告の対象としたりすることはありません。

選択および管理

Windows のセットアップ時に簡単設定を選択した場合は、Windows SmartScreen を有効にします。設定をカスタマイズする場合は、**[プライバシーや PC を保護する]** の **[Windows SmartScreen フィルターを使ってファイルとアプリを Microsoft に確認する]** を選択して、Windows エラー報告を管理できます。Windows のセットアップ後に、コントロール パネルの **[アクション センター]** でこの設定を変更できます。

[ページのトップへ](#)

Windows 音声認識

この機能について

Windows 音声認識は、Windows 内で、この機能を使用するよう選択したすべてのアプリに対して音声認識を提供します。Windows 音声認識は、音声やよく使う単語などを含め、言語の使用方法を学習することで精度を高めます。

収集、処理、または送信される情報

Windows 音声認識では、PC 上に単語の一覧と発音が保存されます。音声辞書を使用してこの一覧に単語や発音が追加され、Windows 音声認識を使用することによって単語の読み上げや修正が行われます。

Windows 音声認識ドキュメント見直し機能が有効にされると、PC 上および、(Windows 検索インデックスの場所に含まれる) 接続されているファイル共有にある、Microsoft Office Word ドキュメント (ファイル名拡張子が .doc または .docx のもの) や電子メール (削除済みアイテムや迷惑メール以外の電子メール フォルダーにあるもの) から、テキストが収集され、1 ~ 3 語のフラグメントで保存されます。1 語のフラグメントは、カスタム辞書に追加した単語のみとなります。2 語または 3 語のフラグメントには、標準辞書にある語句のみが含まれます。

収集された情報はすべて、PC 上の個人音声プロファイル内に保存さ

れます。音声プロファイルはユーザーごとに保存され、ユーザーは、PC 上の他のユーザーのプロファイルにアクセスすることはできません。ただし、管理者は PC 上のすべてのプロファイルへアクセスできます。Windows 音声認識によるメッセージが表示され、送信するよう選択した場合を除いて、プロファイル情報は Microsoft には送信されません。送信前にデータを見直すことができます。この情報の送信を選択すると、音声の特徴に適用させるための音響適応データも送信されます。

音声トレーニング セッションを完了すると、Windows 音声認識では、音声プロファイル情報を Microsoft へ送信するかどうかをたずねるメッセージが表示されます。送信前に情報を見直すことができます。この情報には、トレーニング セッションでのユーザーの声の録音と、個人音声プロファイルからのその他の情報などが含まれる場合があります。

情報の用途

Windows 音声認識は、音声プロファイルの単語を使用して、音声をテキストに変換します。Microsoft は、製品やサービスを向上させるために個人の音声プロファイルを使用します。Microsoft がこの情報を使用してお客様を識別したり、連絡したり、広告の対象としたりすることはありません。

選択および管理

Windows 音声認識を実行するかどうかを選択できます。Windows 音声認識を実行している場合は、既定ではドキュメント レビュー機能が有効になっています。Windows 音声認識をはじめて実行するときに、ドキュメント レビュー設定の変更を選択できます。コントロール パネルの [音声認識] に移動し、【高度な音声オプション】をクリックして、ドキュメント レビュー設定や個人音声プロファイル（およびほとんどのドキュメント レビュー情報）の削除を行うことができます。また、音声辞書の [既存の単語を変更する] オプションを使用して、音声プロファイルに追加した単語を削除することもできます。しかし、個人音声プロファイルを削除しても、音声辞書から追加した単語は削除されません。

Windows 検索インデックスに含まれる場所を修正することで、ドキュメント レビューによって語句が収集される場所を制御できます。Windows 検索インデックス内に含まれる場所を表示または修正するには、コントロール パネルの [インデックスのオプション] に

移動します。

すべてのトレーニング セッションの最後には、トレーニング データとその他のプロファイル情報を Microsoft へ送信するかどうかを選択できます。Windows 音声認識の起動時に [マイク] ボタンを右クリックし、[音声認識の改善に協力] をクリックして情報を送信することもできます。どちらの場合でも、送信前にすべてのデータ ファイルを表示し、送信しないことを選択することができます。

[ページのトップへ](#)

Windows ストア

Windows ストアを使用すると、PC のアプリを検索、管理、およびインストールできます。以下では、ストアの機能とストアを使用して取得したアプリがプライバシーに及ぼす影響と、それに対処する方法について説明します。

ストア アプリとサービス

この機能について

ストアを使用すると、PC のアプリを検索およびインストールできます。また、インストールしたストア アプリが追跡されるため、それらのアプリの更新プログラムを取得して複数の PC にインストールできます。

収集、処理、または送信される情報

アプリを検索してインストールするには、Microsoft アカウントを使用してストアにサインインする必要があります。これにより、ストアは、ユーザーの名前、電子メール アドレス、アカウントの画像などの Microsoft アカウント プロファイル内の情報にアクセスできるようになります。ストアは、次の追加情報を収集し、ユーザーのストア アカウントに関連付けます。

- ストアへの支払い。ユーザーが購入したもの、支払った金額、アプリを購入したときまたはストア アカウントを使用してアプリ内購入を行ったときの支払い方法に関する情報。
- インストールしたアプリ。ユーザーがインストールしたアプリの一覧、各アプリのライセンス ポリシー (恒久ライセンスまたは期限付きのトライアル)、ストア アカウントを使用して各アプリ内で行った購入の一覧。ストアは、この情報をユーザーの

アカウントにオンラインで保存することに加えて、ユーザーがインストールした各アプリのライセンス情報を PC に保存します。この情報により、ユーザーがライセンスの所有者として識別されます。

- ユーザーがアプリをインストールした PC。ユーザーがアプリをインストールした各 PC のメーカー、モデル、およびコンピューター名と PC を一意に識別する番号。この番号は、PC のハードウェア構成に基づいて生成され、ユーザーに関する情報は一切含んでいません。
- 評価、レビュー、および問題レポート。アプリをインストールすると、アプリのレビューを書いたり、アプリの評価をストアに残したりできるようになります。これらの評価には、ユーザーの Microsoft アカウントが関連付けられます。ユーザーがレビューを書くと、ユーザーの Microsoft アカウントに関連付けられた名前と画像がレビューと共に公開されます。
- ストアの基本設定。ストアでアプリを表示するために設定した基本設定。たとえば、母国語で利用できるアプリのみを表示するかどうかなどです。

クレジットカード番号などの支払い情報をストア アカウントに保存できます。セキュリティ上の理由により、この情報は SSL 経由で送信され、クレジットカード番号の最後の 4 桁以外は暗号化されて保存されます。

ストアは、ユーザーの Windows のコピーに関する情報を収集し、それが小売店で販売されたか、評価版であるか、ボリューム ライセンス プログラムの一部か、または PC の製造元によってプレインストールされたかを識別します。ユーザーが初めてストアに接続すると、PC にプレインストールされているすべてのアプリの一覧がストアに送信され、それらのアプリのライセンスが、そのユーザーのストア アカウントに関連付けられます。

ストアは、ユーザーのアプリの更新プログラムを自動的に確認するため、新しい更新プログラムが利用可能になったときにユーザーに通知できます。ストアは、更新プログラムを提供するために、次の情報を Microsoft に送信します。

- PC 上のすべてのユーザーによってストアからインストールされたすべてのアプリの一覧

- 各アプリのライセンス情報 (各ライセンスの所有者を含む)
- 更新プログラムを自動的にダウンロードするか、自動的にインストールするかなどの、Windows Update や Microsoft Update の構成設定。
- ストアからアプリを更新するときの、成功、失敗、エラーなどの結果。
- グローバル一意識別子 (GUID)。ランダムに生成された番号であり、個人情報はありません。GUID により、ユーザーを特定せずに個別の PC を識別します。
- BIOS 名、リビジョン番号、およびリビジョンの日付。ハードウェアのテスト、コンピューターのオペレーティングシステムの起動、およびコンピューターに接続されたハードウェアデバイス間でのデータ転送を行う重要なソフトウェアルーチンのセットに関する情報です。

Microsoft は、ユーザーがストアを閲覧するときやストアから取得したアプリを使用するときに、一部の情報を収集し、利用パターンや傾向を把握するために使用します。これは多くの Web サイトが訪問者の閲覧データを分析するのと同様です。このアクティビティデータは、個人の特定やお問い合わせの目的で使用されることはありません。

情報の用途

Microsoft は、ユーザーの連絡先情報を使用して、ユーザーが購入したアプリの領収書などのストア サービスの提供に必要な電子メールを送信します。Microsoft は、ユーザーの支払い情報を使用して、ユーザーが購入の支払いをできるようにします。この情報を保存するように選択した場合は、支払い情報を毎回入力する必要がなくなります。Microsoft は、ユーザーの購入に関する情報を使用して、ストアの運営とカスタマー サポートの提供を行います。

ストアは、ユーザーがインストールしたすべてのアプリを追跡します。ストアを使用して、アプリをインストールしたデバイスの一覧を管理できます。また、この情報を管理する際には、カスタマー サポートの支援を受けることもできます。インストールしたアプリは、アンインストールする場合でも、ストアの購入履歴でいつでも

確認できます。この一覧は、Windows ストアの使用条件で説明されているように、ユーザーがアプリをインストールできる PC の数の制限を強制するためにストアでも使用されます。ユーザーがアプリのレビューを書くと、ユーザーの Windows アカウントに関連付けられた名前とアカウントの画像がストアでレビューの横に公開されます。アプリの問題を報告すると、ストア担当者が問題レポートを評価し、それに基づいて対策を講じることができるようになります。ストア 担当者は、レポートをレビューしたときに、必要な場合には、ストア アカウントに関連付けられたユーザー名と電子メールアドレスを使用してユーザーに連絡することがあります。

インストールしたアプリの更新プログラムが利用可能になると、ストアに通知が表示され、利用可能な更新プログラムの数がストアのアプリのタイルで示されます。その後、利用可能な更新プログラムの一覧を確認し、インストールする更新プログラムを選択できます。更新されたアプリでは、以前のバージョンとは異なる Windows 機能が使用される場合があります。これにより、アプリが PC 上の異なるリソースにアクセスすることがあります。更新された機能一覧は、利用可能な更新プログラムの一覧が表示されているページからリンクされている [アプリの説明] ページで確認できます。

ストアは、ユーザーの Windows のコピーに関する情報を収集し、その情報を使用して、Windows がユーザーの PC にどのようにインストールされたか (PC の製造元によってプレインストールされたかどうかなど) を識別します。この情報により、ストアは、該当する製造元がその顧客のみを対象に提供したアプリへのアクセスをユーザーに提供できます。この情報は、Windows の利用パターンに関する情報を Microsoft に (場合によっては、集計情報として製造元に) 提供するためにも使用されます。

Microsoft は、アプリの購入と利用に関する集計データを使用して、ユーザーによるストアの利用方法 (たとえば、インストールするアプリをどのように見つけるかなど) を学習します。Microsoft は、これらの集計情報の一部をアプリの開発者と共有する場合があります。Microsoft は、ユーザーの個人情報をアプリの開発者と共有することはありません。Microsoft は、ストアによって収集された閲覧データと利用状況データを使用して、ユーザーによるストアの利用方法についての理解を深め、ストアの機能とサービスを改善します。

選択および管理

ストアを使用するように選択した場合は、上で説明したように、このセクションで示した情報が Microsoft に送信されます。

アプリについて自分が公開したレビューを削除する場合は、ストアでアプリの説明にアクセスし、レビューを編集してテキストをすべて削除します。

ストア アプリのアクセス許可

この機能について

ユーザーが Windows ストアからインストールするアプリの多くは、ユーザーの PC の特定のハードウェアおよびソフトウェア機能を活用するように設計されています。たとえば、フォト アプリでは、Web カメラを使用することが必要になる場合があります、レストランガイドでは、近くのお勧めのレストランを紹介するために、ユーザーの所在地を把握することが必要になる場合があります。

収集、処理、または送信される情報

次に、アプリが使用することを公開する必要がある機能の一覧を示します。

- ユーザーのインターネット接続。アプリがインターネットに接続できるようにします。
- ファイアウォール経由の着信接続。アプリがファイアウォールを介してユーザーの PC との間で情報を送受信できるようにします。
- ホーム ネットワークまたは社内ネットワーク。アプリがユーザーの PC と同じネットワーク上の他の PC との間で情報を送信できるようにします。
- ユーザーの画像、ビデオ、音楽、またはドキュメントのライブラリ。アプリがユーザーのライブラリのファイルにアクセスしたり、それらのファイルを変更または削除したりできるようにします。これには、これらのファイルに埋め込まれた追加のデータ（写真の場所情報など）へのアクセスが含まれます。
- リームバブル記憶域。アプリが外部ハード ドライブ、USB フラッシュ ドライブ、またはポータブル デバイス上のファイルにアクセスしたり、それらのファイルを追加、変更、または削除したりできるようにします。

- ユーザーの Windows 資格情報。アプリがユーザーの資格情報を使用して認証し、社内イントラネットへのアクセスを提供できるようにします。
- ユーザーの PC とスマート カードに保存された資格情報。アプリが資格情報を使用して、銀行、政府機関、ユーザーの勤務先などの組織に安全に接続できるようにします。
- ユーザーの PC のテキスト メッセージング機能。アプリがテキスト メッセージを送受信できるようにします。
- ユーザーの Web カメラとマイク。アプリが写真を撮ったり、オーディオとビデオを記録したりできるようにします。
- ユーザーの所在地。アプリが GPS センサーまたはネットワーク情報に基づいてユーザーのおおよその位置を特定できるようにします。
- ユーザーの PC の近距離通信機能。アプリが、同じアプリが動作している近くの別のデバイスに接続できるようにします。
- ユーザーのポータブル デバイス。アプリがユーザーの携帯電話、デジタル カメラ、ポータブル ミュージック プレーヤーなどのデバイスと通信できるようにします。
- ポータブル デバイスのユーザー情報。アプリがポータブル デバイスの連絡先、予定表、タスク、メモ、状態、または着信音にアクセスしたり、それらの情報を追加、変更、または削除したりできるようにします。
- ユーザーのモバイル ブロードバンド アカウント。アプリがユーザーのモバイル ブロードバンド アカウントを管理できるようにします。

アプリが使用する機能の一覧は、[アプリの説明] ページに表示されます。アプリをインストールすると、Windows は、これらの機能（位置情報、テキスト メッセージング、Web カメラ、マイクなど、特に機密性の高い情報は除く）の使用をそのアプリに許可します。Windows では、機密性の高いこれらの機能のいずれかへのアクセスをアプリが初めて要求したときに、その機能の使用をアプリに許可するかどうかをたずねるメッセージが表示されます。アプリがその機能を使用できるようにするかどうかは、いつでも変更できま

す。

情報の用途

各アプリによるこれらの機能の使用は、開発者のプライバシーの方針に従います。上に挙げた機密性の高いいずれかの機能をアプリが使用する場合は、アプリの発行者のプライバシーに関する声明へのリンクがストアの [アプリの説明] ページに表示されます。

選択および管理

アプリをインストールする前に、アプリが必要とする機能をストアで確認できます。Windows では、各アプリが最も機密性の高い機能 (所在地、テキスト メッセージング、Web カメラ、およびマイク) を初めて使用する前に、その機能へのアクセスを許可するかどうかをたずねるメッセージが表示されます。

Windows ストアでアプリの [アプリの説明] ページを参照すると、アプリが使用する機能の簡易表記の一覧が左の列の下部にあります。完全な一覧は、[アプリの説明] の [詳細] ページにあります。アプリをインストールしたら、アプリが使用する機能の完全な一覧をいつでも確認し、特に機密性の高い機能へのアクセスを制御することができます。これを行うには、アプリを開いて設定チャームをクリックまたはタップし、[アクセス許可] で回復キーにアクセスしたり、回復キーを削除したりできます。

自分のアプリで使っている Web コンテンツの URL を送って、Windows ストアの改善に協力する

この機能について

ストアで入手できる一部のアプリは Web サイトと同様、マルウェアなど安全でない可能性のあるソフトウェアによってコンピューターが被害を受ける可能性があります。この機能を有効にすると、これらのアプリで使用されている Web コンテンツに関する情報が収集され、Microsoft はこの情報を利用して安全でない可能性のある動作を診断します。たとえば、この情報を使用してストアからアプリを削除する場合があります。

収集、処理、または送信される情報

アプリで使用される Web コンテンツについての情報を送信するようにユーザーが選択した場合、Microsoft は、ユーザーがそれらのア

プリを使用したときに、そのアプリによってアクセスされるコンテンツの種類と URL に関する情報を収集します。これにより、有害な Web サイトや安全でない Web サイトからコンテンツを受信しているアプリを特定できます。Microsoft に送信される報告には、アプリの名前や識別子、アプリがアクセスするアドレスの完全な URL、アプリがアクセスする JavaScript の場所を示す完全な URL などの情報が含まれます。Windows では、各報告と共に Microsoft に送信されるグローバル一意識別子 (GUID) と呼ばれる番号が生成されます。GUID を使用して、長期間特定のコンピューターから送信されるデータを確認できます。GUID には個人情報は含まれておらず、GUID を使用してお客様を特定することはありません。

ユーザーのプライバシーを保護するため、Microsoft に送信される報告は暗号化されます。これらのアプリがアクセスする Web ページに関連付けられている可能性のある情報 (アプリに入力した検索用語やデータなど) が含まれる可能性があります。たとえば、辞書のアプリで単語を検索している場合は、検索した単語が、そのアプリからアクセスされた完全なアドレスの一部として Microsoft に送信される情報に含まれることがあります。Microsoft はこれらのアドレスをフィルタリングして、可能な限り個人情報を削除します。

情報の用途

Microsoft は送信された情報を定期的にレビューし、有害な Web アドレスやスクリプトなど安全ではない Web コンテンツとやり取りしているアプリを検出する際の参考にします。この情報を使用して、有害である可能性のあるアプリに対して措置を講じることができます。Web コンテンツのアドレスには、意図せず個人情報が含まれる場合がありますが、Microsoft がそのような情報を使用して個人を特定したり、お問い合わせや広告目的でそれらの情報を使用することはありません。Microsoft は GUID を使用して、そのフィードバックがどの程度一般的な事象であるかを判断し、またその重大度を区別します。たとえば、GUID を使用して安全でない可能性のある動作が 1 台の PC で 100 回発生した場合と、安全でない可能性のある動作が 100 台の各 PC で 1 回ずつ発生した場合を区別できます。

選択および管理

Windows のセットアップ時に簡単設定を選択した場合、ストアから入手した、JavaScript を使用して作成されたアプリで使用されている Web コンテンツに関する情報が送信されます。設定をカスタマ

イズする場合は、[Windows とアプリの機能向上のために、情報を Microsoft に送る] の [Microsoft のサービスの機能向上のために、位置情報認識アプリを使う場合に一部の位置データを送る] を選択して、この設定を管理できます。この設定は、インストール後に PC 設定の [プライバシー] で変更できます。

[ページのトップへ](#)

Windows タイム サービス

この機能について

Windows タイム サービスは、PC の時刻を、ネットワーク上のサーバーの時刻と自動的に同期します。

収集、処理、または送信される情報

このサービスは、業界標準のネットワーク タイム プロトコルを使用して、インターネットまたはローカル ネットワークでタイム サーバーと接続します。既定では、このサービスは週に一度 time.windows.com と同期化するようになっています。標準 PC 情報以外の情報はタイム サーバーには送信されません。

情報の用途

情報は、Windows タイム サービスによって、ローカル PC の時刻を自動的に同期化するために使用されます。

選択および管理

Windows タイム サービスは既定ではオンになっています。コントロール パネルの [日付と時刻] で [インターネット時刻] タブを選択し、[設定の変更] をクリックして、この機能をオフにしたり、好きなタイム ソースに変更できます。Windows タイム サービスをオフにしてもアプリや他のサービスに直接的な影響はありませんが、信頼のおけるタイム ソースを設定していないと、ローカルの PC の時刻が、ネットワークやインターネット上の他の PC とずれる場合があります。ネットワーク接続した PC の間に著しい時間のずれがある場合、時間に依存するアプリやサービスが失敗したり、正常に動作しなくなる場合があります。

[ページのトップへ](#)

Windows トラブルシューティング

この機能について

Windows トラブルシューティングを使用すると、PC の一般的な問題を診断および修復できるようになります。

収集、処理、または送信される情報

トラブルシューティング パックの実行後、PC に結果が保存されます。これらの結果には、ユーザー名やデバイス名などの個人情報が含まれる場合があります。Windows トラブルシューティングは、オンラインの Windows ヘルプと Windows コミュニティで問題の解決策を探すのに役立ちます。解決策を探すのに役立つよう、問題に関連したキーワードが Microsoft へ送信されます。たとえば、「プリンターが正常に動作せず、ヘルプを探している場合」、「プリンター」、「印刷」、「印刷する」などの単語が Microsoft に送信されます。

情報の用途

Microsoft は、Windows トラブルシューティングから収集した情報を使用して、ユーザーが遭遇する問題の解決に役立っています。

選択および管理

Windows のセットアップ時に簡単設定を選択した場合、既定では Windows トラブルシューティングはオンラインでトラブルシューティング パックを検索するようになっています。トラブルシューティングの結果は、コントロール パネルの [トラブルシューティング] で削除できます。【履歴の表示】をクリックし、結果を選択してから、【閲覧の履歴】で回復キーにアクセスしたり、回復キーを削除したりできます。

[ページのトップへ](#)

最新情報

[Surface Pro 8](#)

[Surface Laptop Studio](#)

[Microsoft Store](#)

[アカウント プロファイル](#)

[ダウンロード センター](#)

教育

[Microsoft Education](#)

[教育機関向けデバイス](#)

Surface Pro X

Surface Go 3

Surface Duo 2

Microsoft 365

Windows 11 **アプリ**

HoloLens 2

ビジネス

Microsoft Cloud

Microsoft Security

Azure

Dynamics 365

Microsoft 365

Microsoft Advertising

Microsoft Industry

Microsoft Teams

Microsoft Store **サポート**

返品・返金

ご注文履歴

Microsoft Store **をお選びいただく理由**

開発者 & IT

デベロッパー **センター**

ドキュメント

Microsoft Learn

Microsoft Tech Community

Azure Marketplace

AppSource

Microsoft Power Platform

Visual Studio

Microsoft Teams for Education

Microsoft 365 Education

Office Education

教育者向けトレーニングおよび開発

学生および保護者向けキャンペーン

学生向け Azure

会社

採用情報

会社のニュース

マイクロソフトにおけるプライバシー

投資家

アクセシビリティ

持続可能性

Microsoft **に問い合わせ**

プライバシー

使用条件

商標

広告について

© Microsoft 2022

Microsoft のデータ処理の方針に関する最新の情報は、「[Microsoft のプライバシーに関する声明](#)」を参照してください。ここでは、データにアクセスして制御するために提供される最新のツール、またプライバシーに関する質問がある場合の問い合わせ方法についても確認することができます。

Windows 8 および Windows Server 2012 のプライバシーに関する声明

ハイライトペン 声明 機能に関する補足条項 **サーバーに関する補足条項**

このページの内容 最終更新: 2012 年 8 月

ユーザー アクセス ログ このページは、[Windows 8 および Windows Server 2012 のプライバシーに関する声明](#) ("Windows のプライバシーに関する声明") の補足条項です。このプライバシーに関する声明は、以下の 4 つのセクションで構成されています。

サーバー マネージャー

Active Directory フェデレーション サービス (AD FS)

IP アドレス管理

統合リモート アクセス

リモート デスクトップ サービス

Windows カスタマ

- [ハイライト](#)
- [声明](#)。Windows 全体のプライバシーに関する声明です。Windows 機能ごとの声明へのリンクも記載されています。
- [機能に関する補足条項](#)。プライバシー関連の影響がある Windows 8 および Windows Server 2012 の機能について説明しています。
- [サーバーに関する補足条項](#) (このドキュメント)。プライバシー関連の影響がある Windows Server 2012 の追加の機能について説明しています。

ー エクスペリエンス向上プログラム (CEIP) と Windows エラー報告 (WER)

個々の Windows 機能またはサービスに対するデータ収集および使用方法の詳細については、Windows 全体のプライバシーに関する声明か、適用される補足条項を確認してください。また、[管理者向けのこちらのホワイト ペーパー](#)もお読みください。

ユーザー アクセス ログ

この機能について

ユーザー アクセス ログ (UAL) は、サーバーの役割とインストールされている製品 (UAL に登録されている場合) を対象に、クライアント要求 (ユーザーとデバイスの両方の要求) のレコードをローカルサーバーで収集し、集約する機能です。このデータには、IP アドレスとユーザー名のほか、場合によってはホスト名や仮想マシン ID も含まれます。データはローカルの Extensible Storage Engine (ESE) データベースに格納され、管理者だけがアクセスできます。UAL では、WMIv2 プロバイダーおよび関連する Windows PowerShell コマンドレットを使用してユーザー アクセス データを取得できます。このデータは、オフラインのお客様のクライアント アクセス ライセンス (CAL) 登録を管理するためのもので、一意のクライアント要求の実際のレコードが必要な場合に使用できます。

収集、処理、または送信される情報

UAL が有効になっていると、IP アドレスとユーザー名のほか、ホスト名 (DNS の役割がインストールされている場合)、仮想マシン ID (Hyper-V の役割がインストールされている場合) がサーバー上でローカルに収集されます。収集されたデータが Microsoft に送信されることはありません。

情報の用途

管理者は、ローカルの ESE データベース、WMI プロバイダー、および Windows PowerShell コマンドレットを通じて、UAL のデータを使用できます。Windows では、これらのデータが UAL 機能以外で使用されることはありません。

選択および管理

UAL は既定で有効になっています。UAL サービスは、サーバーの実行中に停止したり開始したりできます。UAL を永続的に無効にするには、Windows PowerShell を開いて「Disable-UAL」と入力し、サーバーを再起動します。管理者は、収集されたすべての履歴データ

を削除することができます。これを行うには、まずサービスを停止して UAL を無効にし、続いて %SystemRoot%\System32\LogFiles\SUM\ フォルダー内のすべてのファイルを削除します。

[ページのトップへ](#)

サーバー マネージャー

この機能について

サーバー マネージャーは、1 つまたは複数のサーバーを監視したり、全般的な状態や役割固有の状態を確認したりするための管理ツールです。管理者はこのツールを使用して、管理タスクを実行したり、他のサーバー管理ツールにアクセスしたりできます。

収集、処理、または送信される情報

サーバー マネージャーでは、管理対象のサーバーから次の種類の情報が収集されます。

- **サーバーに関する全般的な情報:** NetBios 名と完全修飾ドメイン名 (FQDN)、"管理者" 機能で入力されたアカウント資格情報、IPv4 アドレス、IPv6 アドレス、管理性の状態、説明、オペレーティング システムのバージョン、種類、前回の更新、プロセッサ、メモリ、クラスター名、クラスター オブジェクトの種類、ライセンス認証の状態、SKU、オペレーティング システムのアーキテクチャ、製造元、カスタマー エクスペリエンス向上プログラム (CEIP) の構成、Windows エラー報告 (WER) の構成。
- **イベント:** Windows のログと管理者が選択したその他のログに含まれる各イベントの ID、重要度、ソース、ログ、日付、および時刻。
- **すべてのサービス:** 名前、状態、および開始の種類。
- **サーバーの役割に関する情報:** サーバーにインストールされている役割についての、ベスト プラクティス アナライザー (BPA) の結果。
- **パフォーマンス情報:** パフォーマンス カウンターのサンプル、および CPU 使用率と使用可能なメモリに関する通知。

情報の用途

これらの情報はサーバー マネージャーに保存され、Microsoft へは送信されません。管理者は、サーバー マネージャーに表示されるこれらの情報を参照して、システムを監視することができます。

選択および管理

管理者は、サーバー マネージャーでサーバーを追加または削除することで、データ収集の対象となるサーバーを選択することができます (ローカル サーバーを除く)。管理者は、資格情報を明示的に指定してリモート サーバーに接続できます。管理者は、資格情報をローカルに保存することについて、サーバー マネージャーから明示的な同意を求められます。管理者は、それらの資格情報をいつでも削除することができます。

[ページのトップへ](#)

Active Directory フェデレーション サービス (AD FS)

この機能について

Active Directory フェデレーション サービス (AD FS) は、ローカルまたはその他のネットワーク ベースのアプリケーションを対象とした、エンタープライズ対応のフェデレーションおよびシングル サインオン ソリューションです。AD FS を使用すると、管理者はアプリケーションのセキュリティを維持しながら、ユーザーが組織間で共同作業できるようにしたり、ローカルやその他のネットワーク上のアプリケーションに簡単にアクセスできるようにすることができます。AD FS では、Active Directory Domain Services (AD DS) を使ったセキュリティ トークン サービスを使用して、ユーザーを認証したり、各種のプロトコルを使用してユーザーにセキュリティ トークンを発行することができます。トークンはデジタル署名され、トークン内にはユーザーについての要求が格納されます。これは、AD DS、ライトウェイト ディレクトリ アクセス プロトコル (LDAP)、SQL Server、カスタム ストア、またはこれらの任意の組み合わせから生成されます。

収集、処理、または送信される情報

ユーザーが AD FS で認証を行う際には、ユーザーの資格情報が収集されます。資格情報は、Active Directory Domain Services に直ちに送信され、認証用に使用されます。AD FS によってローカルに格納されることはありません。AD FS 管理者が構成した要求規則によつ

ては、Active Directory Domain Services に格納されているユーザーの属性が、出力方向の要求の生成に使用されることがあります。出力方向の要求は、AD FS 管理者が信頼関係を確立した信頼済みパートナーに送信されます。情報が Microsoft に送信されることはありません。

情報の用途

Microsoft がこの情報にアクセスすることはありません。この情報は、お客様が使用することだけを目的としています。

選択および管理

AD FS は、AD FS でデータを収集したり、信頼済みパートナーにデータを送信する必要がある場合に使用します。

[ページのトップへ](#)

IP アドレス管理

この機能について

IP アドレス管理 (IPAM) を使用すると、サーバーの管理者はユーザーのログオン情報を使用して、ネットワーク上のコンピューターやデバイスの IP アドレス、ホスト名、およびクライアント識別子 (IPv4 の MAC アドレスや IPv6 の DUID など) を追跡できます。

収集、処理、または送信される情報

IPAM サーバーは、DHCP サーバー、ドメイン コントローラー、およびネットワーク ポリシー サーバーから監査ログとイベントを収集し、その後、IP アドレス、ホスト名、クライアント識別子、およびログオンしているユーザーのユーザー名をローカルに格納します。サーバー管理者は IPAM コンソールを使用し、IP アドレス、クライアント識別子、ホスト名、およびユーザー名に基づいて、収集されたログを検索できます。この情報が Microsoft へ送信されることはありません。

情報の用途

Microsoft がこの情報にアクセスすることはありません。この情報は、お客様が使用することだけを目的としています。

選択および管理

IPAM は、既定ではインストールされていません。サーバー管理者がインストールする必要があります。IPAM をインストールする

と、IP アドレス監査が自動的に有効になります。IPAM がインストールされたサーバーで IP アドレス監査を無効にするには、IPAM サーバーでタスク スケジューラを起動し、Microsoft\Windows\IPAM にある Audit Task を参照して、このタスクを無効にします。

[ページのトップへ](#)

統合リモート アクセス

この機能について

統合リモート アクセスを利用すると、リモート ユーザーがインターネットを通じてプライベート ネットワーク (会社のネットワークなど) に接続できるようになります。統合リモート アクセスでは、DirectAccess を使用することで、Windows 8 を実行しているリモート クライアント コンピューターから会社のネットワークへ、中断なく透過的に接続することができます。また、サイト間のローカル接続やその他のネットワーク接続を含むリモート アクセス サービス (RAS) 機能 (従来の VPN サービス) を使用することもできます。

収集、処理、または送信される情報

統合リモート アクセスのユーザー監視のために、プライベート ネットワークに接続しているリモート ユーザーの詳細が DirectAccess サーバーに格納されます。この情報には、リモート ユーザーのホスト名、Active Directory ユーザー名、リモート クライアントのパブリック IP アドレスなどが含まれます (クライアントがネットワーク アドレス変換 (NAT) の背後にある場合、これはパブリック IP アドレスになります)。このデータは、管理者が同意した場合に限り、Windows Internal Database (WID)/RADIUS サーバーにも格納されます。この情報にアクセスして内容を参照できるのは、サーバーにアクセスしている DirectAccess 管理者 (ローカル管理者アカウントを持つドメイン ユーザー) だけです。

情報の用途

この情報は、クライアント接続のトラブルシューティングのほか、監査やコンプライアンスの目的のために、管理者によって使用されます。情報が Microsoft に送信されることはありません。

選択および管理

リモート クライアントの監視は既定で有効になっており、無効にす

ることはできません。監視データが WID/RADIUS サーバーに格納されるのは、それらのオプションのいずれかをアカウントティングで使用するよう管理者が構成した場合だけです。管理者がアカウントティングを構成していなければ、この情報は格納されません。管理者は、リモート アクセス サーバー上でのアカウントティングについて、ユーザー名と IP アドレスの情報を格納しないように構成することもできます。

[ページのトップへ](#)

リモート デスクトップ サービス

この機能について

リモート デスクトップ サービス (RDS) は、企業がデスクトップの一元管理戦略を実施し、デスクトップやアプリケーションを管理し、柔軟性とコンプライアンスを改善しながらデータ セキュリティを向上させるためのプラットフォームを提供します。

収集、処理、または送信される情報

RDS のユーザー監視のために、RDS リソースに接続しているリモート ユーザーに関する情報がリモート デスクトップ セッション ホスト サーバーに格納されます。この情報には、リモート ユーザーのホスト名、Active Directory ユーザー名、リモート クライアントのパブリック IP アドレスなどが含まれます (クライアントがネットワーク アドレス変換 (NAT) の背後にある場合、これはパブリック IP アドレスになります)。このデータは、ユーザーが接続する際に、Windows Internal Database (WID)/SQL サーバーに自動的に格納されます。情報が Microsoft に送信されることはありません。この情報にアクセスして内容を参照できるのは、ローカル管理者アカウントを持つドメイン ユーザーだけです。

情報の用途

この情報は、クライアント接続のトラブルシューティングのほか、内部監査やコンプライアンスの目的のために、管理者によって使用されます。情報が Microsoft に送信されることはありません。

選択および管理

クライアントの監視は既定で有効になっており、無効にすることはできません。監視情報は WID/SQL サーバーに格納されます。

[ページのトップへ](#)

Windows カスタマー エクスペリエンス向上プログラム (CEIP) と Windows エラー報告 (WER)

この機能について

これらの機能の詳細については、[機能に関する補足条項](#)または [管理者向けのこちらのホワイト ペーパー](#)もお読みください。

収集、処理、または送信される情報

これらの機能によって収集、処理、および送信される具体的な情報については、[機能に関する補足条項](#) の CEIP と WER に関するページを参照してください。

情報の用途

これらの機能によって収集される情報の用途については、[機能に関する補足条項](#) の CEIP と WER に関するページを参照してください。

選択および管理

CEIP は既定では無効になっています。WER は既定では、クラッシュ レポートを Microsoft に送信する前に、メッセージを表示するように設定されています。CEIP の有効と無効の切り替えは、サーバー マネージャーとコントロール パネルから行うこともできますし、コマンド ラインを使用して行うこともできます。WER はコマンド ラインでのみ制御できます。

コントロール パネルを使用して CEIP の有効と無効を切り替えるには、[\[システムとメンテナンス\]](#)、[\[問題のレポートと解決策\]](#) の順にクリックします。次に、左側のウィンドウの [\[関連項目\]](#) で、[\[カスタマー エクスペリエンス向上の設定\]](#) をクリックして CEIP を有効または無効にします。

サーバー マネージャーのコントロール

ローカル サーバー

- CEIP を有効にする

サーバー マネージャーを開き、ローカル サーバーを選択します。[\[カスタマー エクスペリエンス向上プログラム\]](#) リンクをクリックし、ダイアログ ボックスで [\[はい、CEIP に参加します\]](#) を選択して、[\[OK\]](#) をクリックします。

- CEIP を無効にする

サーバー マネージャーを開き、ローカル サーバーを選択します。[カスタマー エクスペリエンス向上プログラム] リンクをクリックし、ダイアログ ボックスで [いいえ、参加しません] を選択して、[OK] をクリックします。

- WER を有効にする
サーバー マネージャーを開き、ローカル サーバーを選択します。[Windows エラー報告] リンクをクリックし、[はい、自動的に要約レポートを送信します] を選択して、[OK] もお読みください。
- WER を無効にする
サーバー マネージャーを開き、ローカル サーバーを選択します。[Windows エラー報告] リンクをクリックし、[レポートを送信せず、この確認画面も今後表示しません] を選択して、[OK] もお読みください。

複数のコンピューター

- CEIP を有効にする
サーバー マネージャーを開き、[すべてのサーバー] を選択します。[サーバー] タイルですべてのサーバーを選択し (Ctrl + A キー)、右クリックして [Windows 自動フィードバックの構成] を選択します。[カスタマー エクスペリエンス向上プログラム] タブで、[はい、参加します (推奨)] を選択します。[サーバーの選択] コントロールの [サーバー名] の横にあるチェック ボックスをオンにして、この設定をすべてのサーバーに適用し、[OK] もお読みください。
- CEIP を無効にする
サーバー マネージャーを開き、[すべてのサーバー] を選択します。[サーバー] タイルですべてのサーバーを選択し (Ctrl + A キー)、右クリックして [Windows 自動フィードバックの構成] を選択します。[カスタマー エクスペリエンス向上プログラム] タブで、[いいえ、参加しません] を選択します。[サーバーの選択] コントロールの [サーバー名] の横にあるチェック ボックスをオンにして、この設定をすべてのサーバーに適用し、[OK] をクリックします。
- WER を有効にする
サーバー マネージャーを開き、[すべてのサーバー] を選択し

ます。[サーバー] タイルですべてのサーバーを選択し (Ctrl + A キー)、右クリックして **[Windows 自動フィードバックの構成]** を選択します。[Windows エラー報告] タブで、**[はい、自動的に要約レポートを送信します (推奨)]** を選択します。[サーバーの選択] コントロールの [サーバー名] の横にあるチェック ボックスをオンにして、この設定をすべてのサーバーに適用し、**[OK]**もお読みください。

- WER を無効にする

サーバー マネージャーを開き、**[すべてのサーバー]** を選択します。[サーバー] タイルですべてのサーバーを選択し (Ctrl + A キー)、右クリックして **[Windows 自動フィードバックの構成]** を選択します。[Windows エラー報告] タブで、**[いいえ、参加しません]** を選択します。[サーバーの選択] コントロールの [サーバー名] の横にあるチェック ボックスをオンにして、この設定をすべてのサーバーに適用し、**[OK]**もお読みください。

[ページのトップへ](#)