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 8.1 および Windows Server 2012 R2 のプライバシーに関する声明

ハイライト　声明　機能　アプリ　サーバー

このページ内

最終更新日: 2014 年 4 月

この完全な Windows 8.1 および Windows Server 2012 R2 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) のハイライトでは、Windows 8.1 および Windows Server 2012 R2 ("Windows") のデータの収集と使用方法の概要について説明します。このハイライトは、オンライン機能に焦点を当てており、すべての機能について網羅的に説明することを目的としていません。他のオンラインまたはオフラインの Microsoft サイト、製品、またはサービスには適用されません。

このプライバシーに関する声明は以下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。これは完全な Windows 8.1 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。

機能の補足条項。プライバシー関連の影響がある Windows 8.1 および Windows Server 2012 R2 の機能について説明しています。

- アプリの補足条項。プライバシー関連の影響がある Windows 8.1 アプリについて説明しています。
- サーバーの補足条項。プライバシー関連の影響がある Windows Server 2012 R2 の追加の機能について説明しています。

オンラインで PC、個人情報、および家族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 に格納されている情報 (個人情報) を収集または使用するアクセス許可を求められる場合があります。この情報は、完全な Windows 8.1 の プライバシーに関する声明のほか、 機能の補足条項、 アプリの補足条項 、および サーバーの補足条項に従い、Windows によって使用されます。
- 一部の Windows 機能では、必要なアクセス許可があればインターネットを介して個人情報を共有できます。
- ソフトウェアを登録する場合、個人情報を入力するように求められます。
- Windows では、ソフトウェアの不正コピーを減らし、お客様が期待する品質のソフトウェアを提供するために、ライセンス認証が必要です。お客様の PC に関する一部の情報は、ライセンス認証で Microsoft に送信されます。
- Windows に Microsoft アカウントでサインインするように選択した場合、デバイス間で Windows の設定を同期し、一部のアプリや Web サイトに自動的にサインインすることができます。Windows では、サード パーティのメールやソーシャル ネットワーク サービスにアクセスするときに Microsoft アカウントでサインインする必要はありませんが、そのサード パーティが

ストアを通じてアプリを提供している場合は、そのアプリをインストールするために Microsoft アカウントを使ってストアにサインインする必要があります。Microsoft アカウントを作る場合、所在地や生年月日など、特定の個人情報を入力するように求められます。

- 追加情報

ページのトップへ

選択

- Windows では、Windows 機能がインターネットを介して情報をどのように転送す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、 機能の補足条項、 アプリの補足条項 、および サーバーの補足条項に従い、Windows によって使用されます。

- インターネットを使用する機能の一部は、エクスペリエンス向上のために既定で有効になっています。

- 追加情報

ページのトップへ

情報の用途

- Microsoft は、収集した情報を、お客様が使用してい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します。また、製品やサービスを向上させるためにも使用します。Microsoft では、サービスの提供に役立たせるために、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。情報を業務で使用する必要がある企業のみに、この情報へのアクセス権が与えられます。これらの企業は、この情報を機密扱いにする義務があり、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

連絡方法

Microsoft のプライバシーの方針の詳細については、完全な Windows 8.1 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 8.1 および Windows Server 2012 R2 のプライバシーに関する声明

最終更新日: 2014 年 4 月

これは、Windows 8.1 と Windows Server 2012 R2 ("Windows") についての声明です。Windows の一部のコンポーネントには、プライバシーに関する声明が別途設けられており、その一覧がこのページにも掲載されています。Windows 関連のソフトウェアやサービスのほか、先行リリースのプライバシーに関する声明も掲載されています。

特定の機能の詳細については、 機能の補足条項、 アプリの補足条項、および サーバーの補足条項を参照してください。 Windows Embedded Industry Pro と Windows Embedded Industry Enterprise の詳細については、 この声明を参照してください。

これは、インターネットを使用した通信機能に焦点を当てた声明であり、すべての機能について網羅的に説明することを目的とするものではありません。

個人情報の収集と用途

Microsoft が収集した個人情報は、お客様が使用する機能を有効にした

り、サービスを提供したり、お客様が要求または許可した処理を実行したりするために、Microsoft およびその子会社や関連会社によって使用されます。また、Microsoft の製品やサービスの分析と向上にも使用される場合があります。

この声明に明記した場合を除き、お客様から提供された個人情報を、お客様の同意なく、第三者に譲渡することはありません。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。

以下に該当する場合、Microsoft はお客様に関する情報にアクセスし、通信の内容も含めて開示することがあります。(a) 法律の遵守、または法律による正当な要求または法的な手続きに対する責任を果たす場合。(b) ユーザーのソフトウェア使用を規定する契約またはポリシーの実施など、Microsoft、およびそのお客様の権利または所有権を保護する場合。(c) Microsoft の従業員、お客様、または公共の安全を確保するためにアクセスまたは開示が必要であると合理的に判断できる場合。

Windows 8.1 によって Microsoft が収集または受信した情報は、Microsoft および子会社や関連会社、あるいはサービス プロバイダーが設備を管理している米国または他の国で格納および処理される場合があります。Microsoft は、欧州連合、欧州経済領域、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 ハーバー構造に従っています。

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と用途

インターネットを使用する機能があるソフトウェアを使用する場合、お使い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、訪問する Web サイトおよび使用するオンライン サービスに送信されます。標準的なコンピューター情報には、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、ブラウザーのバージョン、地域と言語の設定などの情報が含まれます。場合によっては、デバイスの製造元、デバイス名、およびバージョンを示すハードウェア ID も含まれます。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併せて送信されます。

機能の補足条項、アプリ補足条項、および サーバーの補足条項にある各 Windows 機能とこのページで他に示す機能のプライバシー情報の詳細では、収集される追加情報の種類とその用途について説明します。

管理者は、グループ ポリシーを使用して、ここ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保護に努めています。Microsoft では、さまざまなセキュリティ技術や手段を利用して、無許可のアクセス、使用、または開示からお客様の情報を保護します。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、アクセス制限のあるコンピューター システムに保管されます。Microsoft によって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が転送される場合は、SSL (Secure Socket Layer) プロトコルなどの暗号化を使用して機密情報が保護されます。

ページのトップへ

この声明の変更

Microsoft では、製品やサービスの変更、およびお客様からのフィードバックに応じて、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。その際は、プライバシーに関する声明の上部に記載した "最終更新" 日付も改訂されます。この声明の内容の変更または Microsoft の個人情報取り扱い方法に対する変更があった場合、変更の実施前にかかる変更の通知を掲載するか、お客様に直接通知してお知らせいたします。このプライバシーに関する声明を定期的に確認して、収集した情報がどのように保護されるかを常に把握することをお勧めします。

ページのトップへ

質問の連絡先

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。本声明に関してご質問がある場合、または Microsoft が本声明を遵守していないとお考えの場合は、弊社の 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 8.1 および Windows Server 2012 R2 のプライバシーに関する声明

このページ内

最終更新日: 2014 年 4 月

このページは、以下のセクションで構成されている Windows 8.1 および Windows Server 2012 R2 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。

- ハイライト
- 声明。これは完全な Windows 8.1 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。
- 機能の補足条項 (このページ)。プライバシー関連の影響がある Windows 8.1 および Windows Server 2012 R2 の機能について説明しています。
- アプリの補足条項。プライバシー関連の影響がある Windows 8.1 アプリについて説明しています。
- サーバーの補足条項。プライバシー関連の影響がある Windows Server 2012 R2 の追加の機能について説明していま

す。

個々の Windows 機能またはサービスに関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と適用される補足条項、または機能ごとの独自の声明を確認してください。

ライセンス認証

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認証されることがなくなります。PC のハードウェアまたはソフトウェアに変更が生じた場合は、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 (Microsoft 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。

収集、処理、または送信される情報

ライセンス認証では、次の情報が Microsoft に送信されます。

- 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)。
- チャネル 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。
- 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。

プロパティ

近接通信

リモート アクセス接続

RemoteApp とデスクトップ接続

リモート デスクトップ接続

Microsoft アカウントでのサインイン

OneDrive クラウド ストレージ

同期の設定

Teredo テクノロジ

トラステッド プラットフォーム モジュール (TPM) サービス

ルート証明書の更新

更新サービス

仮想プライベート ネットワーク

Windows カスタマー エクスペリエンス向上プログラム (CEIP)

Windows Defender

Windows エラー報告 (WER)

Windows ファイルの関連付け

Windows ヘルプ

- Windows プロダクト キーが改変されていないことを確認するための情報。
- 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。
- 地域と言語の設定。
- 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。
- プロダクト キー (ハッシュ) とプロダクト ID。
- BIOS 名、リビジョン番号、およびリビジョンの日付。
- 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エクスプロイトおよび、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。
  - ライセンス認証のエクスプロイトの ID。
  - ライセンス認証のエクスプロイトの現在の状態 (消去済みや検疫済みなど)。
  - PC の製造元の ID。
  - ライセンス認証のエクス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エクス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。
- 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。
- ライセンス認証サーバーを利用する Windows のボリューム ライセンス コピーを使用しているとき、そのサーバーの IP アドレスが Microsoft に送信される場合があります。

リモート アシスタンス
Windows Search
Windows セットアップ
Windows 共有
Windows SmartScreen
Windows 音声認識
Windows ストア
Windows タイム サービス
Windows トラブルシューティング
作業フォルダー
社内

情報の用途

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。ライセンス サーバーの情報は、ライセンス サーバーが使用許諾契約に確実に準拠するために使用されます。

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と、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

広告 ID

この機能について

より関連性の高い広告が表示されるように、Windows では、デバイスの各ユーザーの一意の ID にアプリがアクセスすることを許可できます。広告 ID へのアクセスの許可と禁止はいつでも切り替えることができます。

収集、処理、または送信される情報

アプリによる広告 ID へのアクセスを許可した場合、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。

情報の用途

広告 ID は、アプリ開発者や広告ネットワークによって利用されて、各ユーザーが使用しているアプリとそれらの使用状況が認識されます。その結果、アプリからより関連性の高い広告が提供されるようになります。また、広告の表示頻度や有効性を判断し、不正やセキュリティ上の問題を検出することで、サービスの品質を向上させるためにも利用されます。

アプリによる広告 ID へのアクセスを許可した場合、各アプリによる ID の用途について該当アプリのプライバシーの方針が適用されます。

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、自分の広告 ID がアプリで使用できるようになります。設定をカスタマイズする場合は、 **[Microsoft** やその他のサービスと情報を共有する**]** の **[**アプリ間のエクスペリエンスのために、アプリで自分の広告識別子を使うことを許可する**]**をクリックして、自分の広告 ID 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。この設定をオフにすると、広告 ID はそれを要求するアプリに送信されません。設定を再びオンにすると、新しい ID が生成されます。

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 の監査を構成できます。

ページのトップへ

生体認証

この機能について

PC に指紋リーダーが取り付けられている場合、指紋を使用して Windows にサインインし、指紋の認証をサポートしているアプリでユーザー自身を識別することができます。

収集、処理、または送信される情報

新しい指紋をセットアップするとき、指紋を読み取った情報が PC にローカルに保存されます。Microsoft には情報は送信されません。指紋を使用してアプリでユーザー自身を識別するとき、Windows では入力した指紋と PC に保存されている指紋が比較され、スキャンされた指紋がアカウントに関連付けられている指紋と一致するかどうかがアプリに通知されます。Windows は、スキャンされた指紋のデータをアプリには送りません。

情報の用途

指紋を使用して Windows にサインインするとき、Windows は、PC に保存するようにユーザーが選択した指紋の情報を使用します。

選択および管理

[PC 設定] の **[アカウント]** にある **[サインイン オプション]** で、指紋の追加と削除を実行できます。

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、コンピューター名を Microsoft 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。

OneDrive アカウント に格納された回復キーを、表示および管理することができます。

ページのトップへ

連絡先

この機能について

People アプリまたはサポートされているサード パーティ製アプリを使用して連絡先を管理すると、特定の連絡先を PC 上の他のアプリと共有するように選択したり、連絡先カードに連絡先情報を表示したりできるほか、特定の連絡先情報を PC 上の他のアプリと共有して、電話をかけたり住所を地図で表示するなどの操作を実行できます。

収集、処理、保存、および送信される情報

アプリから連絡先情報が要求されると、Windows は、そのアプリと共有する特定の連絡先を選択するようにユーザーに求めます。連絡先は、People アプリまたはサポートされているサード パーティの連絡先アプリから取得できます。連絡先リスト全体が Windows によって要求元のアプリに共有されることはありません。

いずれかの連絡先の一部の情報 (電話番号や電子メール アドレスなど) にアプリがアクセスできる場合、Windows では、その連絡先について、連絡先アプリから取得される追加情報と共に連絡先カードを表示することができます。ただし、連絡先カードを表示しているアプリに対して、Windows が追加の連絡先情報を共有することはありません。

連絡先カードで **[電話]**、**[メール]**、**[マップ]** などのコマンドをタッ

プまたはクリックすると、　　は、その操作を実行する適切なアプリを開き、操作を完了するために必要となる連絡先の詳細をアプリに提供します。たとえば、電話をかける場合は電話番号が渡されます。

情報の用途

Windows では、連絡先アプリからの連絡先情報を、ユーザーが選択した特定の連絡先の共有、連絡先カードの表示、連絡先カードに表示された操作を実行するアプリの起動と連絡先情報の共有、および Windows Search での連絡先の表示のために使用します。People アプリによる連絡先情報の用途は、 Communication Apps のプライバシーに関する声明に格納された回復キーを、表示および管理することができます。

連絡先情報をサード パーティのアプリと共有する場合、アプリによ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。連絡先情報を 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に記載されています。

選択および管理

Windows は、ユーザーが特定の連絡先をアプリと共有するように選択した場合、連絡先カードを表示した場合、または連絡先カードから操作を選択した場合にのみ連絡先を表示および共有します。

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 デバイ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することができます (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、ドライバーを検索しているときに、適切なドライバーがまだ PC で利用可能になっていない場合は、Windows Update サービスにオンラインでアクセスし、デバイス ドライバーを見つけてダウンロードすることがあります。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に格納された回復キーを、表示および管理することができます。

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、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。デバイス アプリが利用可能な場合、そのデバイス アプリが自動的に 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 アカウントの所有する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 が送信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]をクリックして、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]**に格納された回復キーを、表示および管理することができます。

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 を使用できます。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

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]** をクリックします。

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**]** をクリックすると、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 を検出および識別することができます。

[Bluetooth 設定] で **[**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 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

デバイスの暗号化

この機能について

デバイスの暗号化では、BitLocker ドライブ暗号化テクノロジを使用してデータを暗号化して保護することができます。これにより、オフラインのソフトウェア攻撃を防ぐことができます。デバイスの暗号化を有効にすると、Windows がインストールされているドライブのデータが暗号化されます。

収集、処理、または送信される情報

ソフトウェアの暗号化を使用している場合、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を使用している場合、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。

Windows は、PC のトラステッド プラットフォーム モジュール (TPM)

を使用して、ドライブの暗号化に使用される暗号化キーを格納して管理します。デバイスの暗号化が有効な場合は、Windows がインストールされているドライブが自動的に暗号化され、回復キーが生成されます。回復キーは、特定のハードウェアの障害やその他の問題が発生した場合に、保護されているデータにアクセスするために使用されます。

PC の BitLocker 回復キーは、Microsoft アカウントに接続されている各管理者アカウントの Microsoft OneDrive アカウントに、オンラインで自動的にバックアップされます。コンピューター名と回復キーの ID も、同じ OneDrive アカウントにバックアップされます。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。

情報の用途

暗号化キーとグローバル一意識別子 (GUID) は PC のメモリに保存され、BitLocker 操作をサポートします。回復情報は、特定のハードウェアの障害やその他の問題が発生した場合に、保護されているデータにアクセスできるようにします。また、BitLocker が、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識別できるようにします。

回復情報は、オンラインでアクセスできるように、OneDrive アカウントにバックアップされます。Microsoft が回復キー情報を使用したり、OneDrive アカウント以外の場所に格納したりすることはありません。傾向を分析したり、製品やサービスを向上させるために、回復キーに関する要約データを使用することはあります。たとえば、この情報を使って、デバイスの暗号化が有効にされている PC の割合を判断したりします。

選択および管理

PC のセットアップ中に Microsoft アカウントの使用を選択すると、デバイスの暗号化が有効になり (PC によってサポートされている場合)、回復キーが OneDrive アカウントにバックアップされます。PC のセットアップ中にローカル アカウントの使用を選択すると、デバイスの暗号化は無効になります。

後で Microsoft アカウントを PC の管理者アカウントに接続すると、次のようになります。

- デバイスの暗号化がまだ有効になっていない場合は、自動的に有効になり、回復情報がユーザーの OneDrive アカウントにバッ

クアップされます。

- デバイスの暗号化が既に有効になっている場合は、PC の回復情報がユーザーの OneDrive アカウントにバックアップされます。

OneDrive アカウントに格納された回復キーは、 ここに格納された回復キーを、表示および管理することができます。

ページのトップへ

DirectAccess

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の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

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に送信されます。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になります。

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 サイトで、お子様の活動記録レポートの閲覧やその設定の変更を実行できます。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、お子様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タッチ キーボードによる入力内容。
- 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用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して、手書き認識機能を向上させるために使用されます。また、タッチ キーボードを使用して入力するときの自動修正と入力ヒントを有効にする場合にも使用されます。

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手書き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。自動学習機能の有効と無効は、コントロール パネルの [言語] にある [詳細設定] でいつでも切り替えることができます。自動学習機能を無効にすると、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 上のすべての Microsoft アカウントの情報 (電子メール アドレス、表示名、画像など) 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有効になります。

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を確認し、その内容の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 の **[ホームグループ]** で、指紋の追加と削除を実行できます。

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。

クラウド IME 候補

この機能について

Microsoft Pinyin IME を使って簡体字中国語を入力する場合、IME は

PC のローカル辞書に存在しないキー入力の表意文字候補をオンラインから検索します。

収集、処理、または送信される情報

Microsoft Pinyin IME を使って簡体字中国語を入力すると、使用可能な表意文字が表示されます。ローカル辞書に適切な候補が見つからない場合、キーボード入力が Microsoft に送信され、その入力に対応するより良い候補があるかどうかを確認します。候補がある場合は候補のリストに表示され、選択した候補はローカル辞書に追加されます。ランダムに生成された一意識別子も送信され、この機能の使用方法の分析に活用します。識別子はお使いの Microsoft アカウントと関連付けられることはなく、連絡先や広告の送信に使われることもありません。

情報の用途

Microsoft は収集された情報を、クラウドの表意文字の検索と、製品とサービスの向上に使用します。お客様を識別したり、連絡したり、広告の対象とするために、情報が使用されることはありません。

選択および管理

クラウド IME 候補は、簡体字中国語用の Microsoft Pinyin IME で既定で無効になります。この設定を表示または変更するには、PC 設定を開き、 **[時刻と言語]**をクリックし、 **[地域と言語]**をクリックして言語を選び、 **[オプション]**に格納された回復キーを、表示および管理することができます。

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

自動学習機能および入力ヒント機能は、それらの機能をサポートする IME では既定で有効になっています。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に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

インターネット接続の共有

この機能について

インターネット接続の共有を使用すると、Wi-Fi 経由で他のデバイスとモバイル ブロードバンド インターネット接続を共有できます。PC からの操作により、モバイル ブロードバンド デバイス上でインターネット接続の共有をリモートで開始することもできます (PC とモバイル ブロードバンド デバイスの両方に、同じ Microsoft アカウントで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

インターネット接続を初めて共有する場合、Windows によってネットワーク名とパスワードが自動的に生成され保存されます。これらのネ

ットワーク名とパスワードはいつでも変更できます。

PC でインターネット接続の共有がサポートされており、その PC を信頼できるデバイスとして Microsoft アカウントに追加した場合、Windows によってネットワーク名とパスワードが Microsoft アカウントと同期されます。また、Windows では他の情報も同期され、これにより、信頼できる他のデバイスからインターネット接続の共有をリモートで開始することができます。この情報には、Bluetooth 無線のハードウェア アドレスおよび接続のセキュリティを確保するためのランダムな番号が含まれます。

情報の用途

この情報は、インターネット接続の共有をセットアップするために使用されます。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

インターネット接続の共有をサポートするデバイスに Microsoft アカウントを使用してサインインし、そのデバイスを信頼できるデバイスとして追加する場合、インターネット接続の共有をリモートで開始するための情報が OneDrive と同期されます。パスワードを同期しないように選択することで、情報の同期を停止できます。詳しくは、このページの「同期の設定」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]に格納された回復キーを、表示および管理することができます。

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 8.1 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 位置情報サービスを使用すると、PC の位置を特定することを許可するアプリ、Web サイト、および Windows 機能を決めることができます。Windows 位置情報サービスは 2 つのコンポーネントから構成されます。Windows 位置情報取得機能は Microsoft オンライン サービスに接続して位置情報を特定します。Windows 位置情報プラットフォームは、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。

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および一部の Windows 機能が、PC の位置を特定する許可を要求できるようになります。アプリによる位置情報の使用を許可すると、Windows 位置情報プラットフォームは、アプリの使用中に位置情報を提供するだけでなく、アプリで定義された地理的な境界の内外を PC が移動するタイミングをアプリに通知できます。たとえば、アプリを使用して、職場を出たときに食料品を買うことを知らせるアラームを設定できます。Windows 位置情報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。

Windows 位置情報プラットフォームでは、アプリが他の方法で PC の位置を特定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、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 (Windows 位置情報プラットフォームがこれらの機能に問い合わせて PC の位置を特定する場合)。位置情報プラットフォームを使用して PC の位置を特定することを承認されたアプリ、Web サイト、機能も、情報を送信または保存することがあります。アプリが地理的な境界をセットアップして監視する場合、これらの境界は PC では暗号化されて保存されます。これらの境界について保存された情報には、名前、位置、前回位置を特定したときに PC が境界の内側や外側にいたかどうかなどの情報が含まれます。地理的な境界をセットアップするアプリは、この情報を送信または保存する場合があります。

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、Web サイト、および Windows 機能は PC の位置情報にアクセスし、パーソナル設定され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、[Microsoft やその他のサービスと情報を共有する] の [Windows とアプリで Windows 位置情報プラットフォームから自分の位置情報を要求することを許可する] をクリックして、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、アプリが位置情報を使用すること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。この設定は、アプリの設定の [アクセス許可] でストア アプリごとに表示および変更できま

す。

Windows 位置情報プラットフォームを利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 **[位置情報の設定]** で、すべてのユーザーに対して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。アプリで定義された地理的な境界を越えたタイミングを通知しないようにするには、管理ユーザーはコントロール パネルで Windows Location Framework Service 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 ネットワークと 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

位置情報の受信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、PC の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近くの 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には、BSSID (Wi-Fi アクセス ポイントの MAC アドレス) とシグナルの強さの情報が含まれます。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、PC を一意に識別する情報は送信されません (ただし、すべてのインターネット接続で必要となる標準的なコンピューター情報は送信されます)。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、SSID (Wi-Fi アクセス ポイント名) や隠し Wi-Fi ネットワークに関する情報は送信されません。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。

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は、アプリが PC の位置情報を要求した後で、近くの Wi-Fi アクセス ポイントに関する情報が Microsoft に再送信されることがあります。従量制課金接続を使用している場合は、インターネット接続の利用を制限するために、この情報の 1 日あたりの送信回数が制限されます。

情報の用途

Windows 位置情報取得機能が利用する情報は、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通知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、Microsoft に送信される 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、お客様の識別やお客様への連絡ができる場合、お客様を広告の対象とすることができる場合、または PC の位置情報履歴の追跡や作成を実行できる場合は、それらの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」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、 **[Microsoft** 製品やサービスの品質向上に協力する**]** の **[**位置情報認識アプリを使う場合に一部の位置データを **Microsoft** に送る**]**をクリックして、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

資格情報の管理

この機能について

Windows では、Windows ストア アプリを Web サイトで使用するアカウントに関連付けることができます。Internet Explorer で Web サイト用のパスワードを以前に保存した場合、アプリが Web サイトに接続するときに、Windows では保存したパスワードを使用できます。

収集、処理、または送信される情報

Web サイトへサインインするための資格情報をアプリが要求するとき、それらの情報を保存するように選択できます。Internet Explorer で Web サイトに既にサインインしたことがあり、資格情報を保存するように選択してある場合は、保存された資格情報が自動的に入力されます。資格情報は、暗号化されて PC に保存されます。資格情報が OneDrive と同期される方法の詳細については、このページの「同期の設定」を参照してください。

情報の用途

Windows では、選択した Web サイトへのサインインをサポートするためにのみ、保存された資格情報を使用します。アプリが Web サイトに接続するときに資格情報を保存した場合、保存された資格情報は Internet Explorer や他のアプリでは使用されません。

選択および管理

保存した資格情報は、コントロール パネルの [資格情報マネージャー] で管理できます。資格情報が OneDrive と同期される方法の詳細については、このページの「同期の設定」を参照してください。

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 **[アカウント]** にある **[サインイン オプション]** 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

Windows Windows PC

用して　　にサインインした場合、　　は　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、 **[Microsoft** やその他のサービスと情報を共有する**]** の **[**アプリ間のエクスペリエンスのために、アプリで自分の広告識別子を使うことを許可する**]**をクリック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 **[**サインイン オプション**]** 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 の **[通知]** で、すべてのアプリまたは特定のアプリに対して無効にすることができます。特定のアプリに対して通知を無効にしたり、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 Windows ストア 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、PC がロックされているときでもタスクを実行できます (バックグラウンドでの電子メールの同期や電話の着信への応答など)。ロック画面から PC のカメラを直接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

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、および Skype 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。[PC 設定] の **[PC とデバイス]** の **[ロック画面]** で、このようなロック画面のアプリや他のアプリを追加または削除したり、カメラの使用を無効にしたりすることができます。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 の **[通知]** で、指紋の追加と削除を実行できます。

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、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エクスプローラーを使用してファイルに関連付けることができる個人情報 (キャプションなど) が含まれる場合があります。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

プリフェッチと事前起動

この機能について

Windows では、アプリおよび機能がいつどの程度の頻度で使用されるか、どのシステム ファイルが読み込まれるかを追跡して、アプリおよび Windows 機能をより迅速に起動するために役立てることができます。

収集、処理、または送信される情報

Windows では、アプリまたは Windows の機能を使用する場合、アプリまたは機能がいつどの程度の頻度で使用されるかに加えて、使用システム ファイルに関する一部の情報を PC に保存します。

情報の用途

Windows は、アプリおよび機能をより迅速に起動するために、アプリおよび機能の使用法に関する情報を使用します。場合によっては、中断状態のアプリが自動的に起動されることがあります。

選択および管理

自動的に起動および中断されるアプリは、タスク マネージャーに表示され、終了できます。中断時のアプリでは、以前に該当機能を有効にしていても、起動するまで Web カメラまたはマイクにアクセスできません。

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デスクトップ 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、Windows エラー報告または Windows 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　　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

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、ファイル名などの一部の固有プロパティ、およびアプリ独自の一部のプロパティは、この方法では削除できません。アプリ独自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

近接通信

近距離近接サービス

この機能について

PC が近距離通信 (NFC) ハードウェアを備えている場合、NFC ハードウェアを備えた別のデバイスまたはアクセサリを PC 側のハードウェアに向けて接近させることで、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ティブになります。

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。デバイスの構成によっては、このデータに Bluetooth のペアリング情報、Wi-Fi のネットワーク アドレス、および PC の名前が含まれる場合があります。

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、近接通信接続を使用して、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] に用意されているオプションを使用して、このサービス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 PC 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ティング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。

Microsoft が接続先の PC またはアプリをホストしている場合、接続に関する追加の情報が、サポートのために Microsoft に送信される場合があります。

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。リモート接続が Microsoft によってホストされていない限り、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** とデスクトップにアクセスする**]**をクリックし、ダイアログ ボックスの [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。レジストリにはリストは保存されません。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。リモート接続が Microsoft によってホストされていない限り、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を使用すると、必要な設定に基づいてリモート デスクトップ サービスを実行しているホスト PC に接続することができます。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 アカウントを使って Windows にサインインするか、Microsoft アカウントをサポートする製品で、ローカル アカウントまたはドメイン アカウントを Microsoft アカウントに関連付けることができます。これを行った場合、Windows では Windows アプリと Microsoft アプリの設定および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。Microsoft アカウントを使用してサインインする Web サイトにアクセスすると、Windows によって、その Web サイトに自動的にサインインされます。

収集、処理、または送信される情報

PC の設定中または [PC 設定] の **[サインイン オプション]** に、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き、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が確認されます。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、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。

Microsoft アカウントでサインインすると、デバイスの製造元、モデル名、バージョンを含む、標準的なコンピューター情報が Windows から Microsoft に送信されます。

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。同期される設定と同期を制御する方法の詳細については、このページの「同期の設定」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、People、Microsoft Office など) 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、Outlook.com または Hotmail.com アドレス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 (アドレスを所有している場合)。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、Bing.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ァイ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。同期される設定と同期を制御する方法の詳細については、このページの「同期の設定」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、 Microsoft アカウントのプライバシーに関する声明のページをお読みください。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、各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] または [バージョン情報] ダイアログ ボックスで確認できます。

標準のコンピューター情報は、お使いのデバイスの概要を記載した電子メールといった、お客様に合わせた情報をお送りする際に使用する場合があります。

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、このページの「同期の設定」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。

Microsoft アカウントをサポートする製品では、[PC 設定] の **[サインイン オプション]** で、いつでもローカル アカウントまたは Microsoft アカウントを作ることができます。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 [アカウント] でいつでも **[サインイン オプション]** で、指紋の追加と削除を実行できます。

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

OneDrive クラウド ストレージ

この機能について

Microsoft アカウントを使用してデバイスにサインインすると、一部のコンテンツや設定を Microsoft サーバーに自動的に保存するかどうかを選択できます。自動的に保存することにより、デバイスで問題が発生した場合でもバックアップを保持できます。

収集、処理、または送信される情報

セットアップ中に、クラウド ストレージ用に OneDrive を選択すると、Windows によって次のコンテンツが Microsoft のサーバーに送信されます。

- ご使用のデバイスで **[カメラ ロール]** フォルダーに保存されている写真やビデオ。
- 複数のデバイス間で共有されない、各デバイス専用の設定。
- デバイスの名前や種類など、デバイスに関する説明情報。

ユーザーは Microsoft サーバー上のコンテンツをインストールするように選択できます。またアプリでは、Microsoft サーバーをユーザーのファイルを保存するための既定の場所として選択できます。

情報の用途

Windows は、このコンテンツを使用してクラウド ストレージ サービスを提供します。Microsoft では、このコンテンツや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

PC のセットアップ中に OneDrive を使用する設定を選択した場合、Windows によって、このセクションで説明したコンテンツが OneDrive に保存されます。この設定は、[PC 設定] の OneDrive セクションでいつでも変更できます。

ページのトップへ

同期の設定

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 1 台または複数の 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 にサインインする設定を選択した場合、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。

- スタート画面のレイアウト
- Windows ストアからインストールしたアプリ
- 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
- IME

スペル チェック辞書、　　辞書、ユーザー辞書

- Web ブラウザーの履歴、お気に入り、現在開いている Web サイト
- 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
- 接続している共有ネットワーク プリンターのアドレス

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にもアクセスできます。

情報の用途

Windows 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、既定で設定が同期されます。[PC 設定] の [OneDrive] セクションにある同期の設定 では、設定を同期するように選択したり、同期の内容を制御したり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 接続を常に有効化する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。 詳細な手順については、 この技術的なホワイト ペーパーに格納された回復キーを、表示および管理することができます。

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、デバイスの暗号化、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。通常の管理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 TPM 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 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、デバイスの暗号化は、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。 また、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。

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 ポリシーを構成して、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

更新サービスでは、Microsoft によるサービスの運用および向上のために、ユーザーの PC から以下の情報を収集します。

PC にインストールされている、更新サービスで提供される更新プログラムの適用対象となる Microsoft ソフトウェア、およびその他のサポート ソフトウェア (デバイス製造元が提供するドライバーやファームウェアなど)。この情報は、該当する更新プログラムの判定に使用されます。

- Windows Update や Microsoft Update の構成設定 (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)。
- 更新サービスへのアクセス時および使用時の、成功、失敗、エラーなどの結果。
- ハードウェア デバイスのプラグ アンド プレイ ID 番号。デバイスの製造元によって割り当てられた、デバイス (キーボードの種類など) を識別するコードです。
- 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、個人情報は含まれていません)。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、ベンダー、およびリビジョンの日付。ハードウェアのテスト、PC のオペレーティング システムの起動、および PC 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。
- 製造元、モデル、プラットフォームの役割、および SKU 番号。ドライバーのインストール時に診断調査を有効にするために使用される、PC に関する情報です。

これらの更新サービスを利用するには、コントロール パネルの [Windows Update] に移動して更新プログラムをチェックするか、または更新プログラムが利用可能になったときに Windows によって自動的にインストールされるように設定を変更します (推奨)。Windows Update 機能では、Microsoft Update を使用するかどうかを選択できます。

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 の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 に格納された回復キーを、表示および管理することができます。

情報の用途

Microsoft に送信されたデータは、更新サービスの運用および管理に使用されます。また、集計情報の生成にも使用され、傾向分析や、更新サービスをはじめとした製品とサービスの向上に役立てられます。

更新サービスでは統計情報を生成するために、更新サービスで収集した GUID を使用して、更新サービスを使用する個別のコンピューターの数、特定の更新プログラムのダウンロードおよびインストールの成功と失敗を追跡し、記録します。ダウンロードおよびインストールを試行したコンピューターの GUID、要求された項目の ID、更新が利用可能であったかどうか、および標準的なコンピューター情報を記録します。

以上の 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。

必須の更新プログラム

更新サービスを有効にしている場合、正しく機能できるようにするために、更新サービスを構成しているか、または更新サービスに直接関係している、システム上のソフトウェア コンポーネントを随時更新する必要があります。これらの更新は、他の更新プログラムのチェック、ダウンロード、またはインストールの前に実行しておく必要があります。これらの必須の更新プログラムでは、エラーの修復、継続的な向上の実現、およびサービスをサポートする Microsoft サーバーとの互換性の維持が行われます。

更新サービスを無効にすると、これらの必須の更新プログラムは受信されなくなります。

Windows ストア アプリのインストールと更新に必要なソフトウェア

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。アプリが正しく機能するためには、これらの更新プログラムを実行する必要があります。

Cookie とトークン

トークンは Cookie に似ています。トークンは、更新サービス サーバーによってユーザーのハード ディスクに格納される小さいファイルであり、その中に情報が保存されます。コンピューターが更新サービス サーバーに接続する際に、有効な接続を維持するために使用されます。トークンはユーザーのコンピューターにのみ格納され、サーバーには格納されません。この Cookie やトークンには、最新の利用可能な更新プログラムを検索するために、最終スキャン時刻などの情報が格納されます。またこの情報には、ユーザーのコンピューターを特定するための GUID に加えて、ユーザーのコンピューターにダウンロードするコンテンツを管理するための情報も含まれています。

Cookie やトークンに格納された情報は、サーバーによって暗号化されます (ただし、Cookie やトークンの有効期限は暗号化されません)。この Cookie やトークンは、ブラウザーの Cookie とは異なるため、ブラウザーの設定では管理できません。この Cookie/トークンは削除できませんが、更新サービスを使用しない場合は、この Cookie やトークンが使用され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すると、Windows Update サービスが有効になり、自動的に更新プログラムをインストールするように設定されます。

更新サービスを有効にした場合、選択している設定にかかわらず、サービスの一部のコンポーネントに必須の更新プログラムが通知なしで自動的にダウンロードされ、インストールされます。必須の更新プログラムが自動的にダウンロードされないようにする場合は、更新サービスを無効にしてください。

重要な更新プログラムと推奨される更新プログラムの両方をチェックするか、重要な更新プログラムのみをチェックするかも選択できます。また、それらをコンピューターに自動的にインストールするかどうかを選択することもできます。オプションの更新プログラムは自動的にはインストールされません。Windows Update の設定は、Windows のセットアップ後にコントロール パネルまたは [PC 設

定] で変更できます。

コンピューター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と共に MSRT を受信する場合は、 MSRT の報告機能を無効にできますに格納された回復キーを、表示および管理することができます。

ページのトップへ

仮想プライベート ネットワーク

この機能について

仮想プライベート ネットワーク (VPN) を使用すると、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。VPN 接続は、Windows VPN クライアントまたはサードパーティの VPN アプリで利用できます。

収集、処理、または送信される情報

VPN に接続すると、VPN クライアントで入力した資格情報がリモート ネットワークに送信されます。これらの資格情報は PC に保存できます。接続後、VPN の構成方法によっては、ネットワーク活動の一部またはすべてがリモート ネットワークを経由してルーティングされます。管理者は特定のアプリを構成して、トラフィックが常に VPN を経由してルーティングされ、これらのアプリの起動時に VPN に自動的に接続するようにできます。Microsoft には情報は送信されません。

サード パーティの VPN ソフトウェアでは、追加の情報も収集される場合があります。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。

情報の用途

VPN クライアントでは、ユーザーが指定した資格情報を使用して、リモート ネットワークに対する認証を行い、リモート ネットワークとの間のネットワーク トラフィックをルーティングします。サード パーティの VPN クライアントが追加の情報を収集する場合、収集される情報のサード パーティでの用途にはサード 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

[PC 設定] の **[ホームグループ]** で、VPN 接続の追加や削除、および既

存の接続の状態の確認を実行できます。VPN 接続がセットアップされたら、[設定] にある一覧からネットワークを選択することで、VPN の接続や切断を手動で実行できます。

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、PC の 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を含みます。
- 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、デスクトップに通常作成するフォルダー数などの情報です。

CEIP 報告には、CEIP への参加を開始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) が含まれることもあります。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。受信された個人識別子に関して、Microsoft が個人識別子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。

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。一部の CEIP レポートには、Microsoft アカウントから派生した GUID が含ま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することがあります。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 のパートナーが製品とサービスを改善できるように、収集した CEIP 情報をパートナーと共有することもありますが、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 ストアからインストールした 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、 **[Microsoft** 製品やサービスの品質向上に協力する] の [位置情報認識アプリを使う場合に一部の位置データを **Microsoft** に送る]をクリックして、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、 CEIP のよく寄せられる質問に格納された回復キーを、表示および管理することができます。

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

Windows Defender を使用すると、Microsoft Active Protection Service (MAPS) によって、新たに検出されたマルウェアの新しいシグニチャが自動的にダウンロードされ、PC のセキュリティの状態が監視されるので、PC の保護がさらに強化されます。MAPS によって、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。また、マルウェアが含まれている可能性のあるファイルも送信できます。ある種類のマルウェアに PC が感染していることが MAPS によって検出されると、問題を解決するために、Microsoft アカウントを使用してユーザーに自動的に連絡されます。

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。また、MAPS はファイルの配布元を示す完全な URL およびマルウェアの可能性のあるファイルが接続する IP アドレスを収集することがあります。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。
- Windows Defender が、Internet Explorer の ActiveX コントロールをスキャンした場合。

Windows のセットアップ中に MAPS 参加を選択すると、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、および MAPS に参加している他の Windows Defender ユーザーからの報告によって、Microsoft の調査担当者は新しい脅威をより迅速に発見することができます。新しい脅威が発見されるとマルウェア定義が作成され、すべてのユーザーは Windows Update を介してこれらの更新された定義を利用できるようになります。

MAPS に参加すると、Windows Defender 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または Web コンテンツを送信します。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。ファイルに個人情報が含まれる可能性がある場合、送信前に確認のメッセージが表示されます。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のダウンロードを試行します。

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。

ある特定の種類のマルウェアの感染を検出し取り除くことができるように、Windows Defender は PC のセキュリティ状態を MAPS に定期的に送信します。これには PC のセキュリティ設定に関する情報とログ ファイルも含まれます。ログ ファイルには、PC の起動時に読み込まれたドライバーなどのソフトウェアについての情報が記述されています。PC を一意に識別する番号も送信されます。

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。

MAPS が収集した PC のセキュリティ状態に関する情報は、ある特定の種類のマルウェアが PC に感染しているかどうかを判断するために使用されます。この場合、Microsoft ではお客様の Microsoft アカウントに関する連絡先情報を使用して、問題とその修正方法の詳細についてお客様に連絡します。

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、MAPS を有効にします。設定をカスタマイズする場合は、 **[Microsoft** やその他のサービスと情報を共有する] の **[**アプリ間のエクスペリエンスのために、アプリで自分の広告識別子を使うことを許可する**]**をクリックして、MAPS を管理できます。Windows のセットアップ後に、Windows Defender の **[**設定**]** メニューで、MAPS のメンバーシップや設定を変更することができます (MAPS の無効化を含む)。

Windows Update で悪意のあるソフトウェアの削除ツールを受け取る場合、Windows Defender が無効になっていても、MAPS に同様の情報が送信される場合があります。詳細については、 Windows の悪意のあるソフトウェアの削除ツール に格納された回復キーを、表示および管理することができます。

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てます。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。状況に応じて、問題の診断に役立つ、PC メモリの部分的なスナップショットなどの追加情報が送信されます。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。

特定の種類の問題を診断できるようにするために、ログ ファイルなどの付加情報を含む報告が Windows エラー報告により作成される場合があります。自動報告を有効にしている場合でも、この付加情報を含む報告を送信する前に、その報告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。

報告の送信後、発生した問題に関する詳細情報の提供を報告サービスから求められる場合があります。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 には個人情報は含まれません。

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、[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]をクリックして、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、 Microsoft エラー報告サービスのプライバシーに関する声明に格納された回復キーを、表示および管理することができます。

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 コンテンツを探す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 (HEIP) 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 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。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、Microsoft がその情報を

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、 **[Microsoft** 製品やサービスの品質向上に協力する] の **[**位置情報認識アプリを使う場合に一部の位置データを **Microsoft** に送る]をクリックして、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、デバイスとインターネットを 1 か所で検索することができます。検索結果を向上させるために、Windows Search では Bing と Windows 位置情報プラットフォームを使用します。デバイス上で利用できるその他の検索機能も Microsoft によって提供されていることに注意してください。たとえば、Windows ストア、Internet Explorer、その他の Microsoft 製品での検索などです。

収集、処理、または送信される情報

Web 検索の結果を取得することを選択した場合、Windows Search に入力した内容が Microsoft に送信されます。検索結果を向上させるために、ユーザーによる Windows Search の使用状況に関する情報も Windows Search から Microsoft に送信されます。さらに、Bing やその他の Microsoft の製品やサービスの使用状況に基づいて、パーソナル設定された検索結果を提供するために、そのユーザーの識別情報も送信されます。Microsoft アカウントを使用して Windows にサインインした場合、識別情報は Microsoft アカウントに関連付けられます。ユーザーは、Windows Search でパーソナル設定された検索結果を取得しないように選択できます。その場合、この識別情報は送信されません。

Windows Search に位置情報の利用を許可すると、デバイスについて Windows Location プラットフォームから提供される物理的位置情報が、検索リクエストと共に Microsoft に送信されます。または、IP ア

ドレスに基づいてユーザーのおおよその物理的位置の特定が試みられる場合があります。

Windows Search を使用してアプリ内で検索すると、入力した検索語句がアプリに提供されます。

情報の用途

Web 検索の結果を取得することを選択した場合、ユーザーが入力した検索語句、ロケールとオンライン検索の履歴、Microsoft アカウントに関連付けられた情報、ご使用のデバイスの物理的位置情報が、その他の Microsoft の製品やサービスで使用されて、関連性の高い検索候補や、パーソナル設定された検索結果とエクスペリエンスを提供するために役立てられます。ユーザーのデータの利用方法については、 Bing のプライバシーに関する声明に格納された回復キーを、表示および管理することができます。

Windows Search を使用してサード 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 のアプリ内で検索を実行する場合、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 のセットアップ時に簡単設定を選択した場合、Windows Search からユーザーは検索候補と Web 検索結果を取得できます。Microsoft は位置情報などのデータを取得して、Windows Search やその他の Microsoft サービスでパーソナル設定されたエクスペリエンスを提供できます。設定のカスタマイズを選択した場合、Windows Search のこれらの設定を変更するかどうかをユーザーが決定できます。この設定は、Windows のセットアップ後に [PC 設定] の **[検索]** で、指紋の追加と削除を実行できます。

[PC 設定] の **[検索]** にある **[通知]** で、ローカル検索履歴、および Windows Search エクスペリエンスのパーソナル設定に使用される Bing 検索履歴を削除できます。検索履歴を削除することにより、検索候補のパーソナル設定または検索結果の順序付けのために以前に収集された検索履歴が使用されなくなります。(検索履歴から派生した情報を含めて) 広告またはその他のパーソナル設定に関する情報は削除されません。また、検索結果およびその他の Microsoft エクスペリエンスの向上のために Microsoft によって使用される集計情報も削除され

ません。そのような情報は、 Bing のプライバシーに関する声明に記載されているように、保持および匿名化されています。Microsoft の広告およびその他のパーソナル設定情報はオンラインで管理できます。

ページのトップへ

Windows セットアップ

ここでは、Windows のインストール プロセスの一部として利用できる機能について説明します。

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に格納された回復キーを、表示および管理することができます。 インストールの成功を確実なもの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に格納された回復キーを、表示および管理することができます。 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。

さらに、Windows ストアから Windows をインストールする場合、動的更新によってお使いの PC に必要なハードウェア ドライバーに加えて、最新の Windows 更新プログラムがダウンロードされ、インストールされます。

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。

選択および管理

Windows ストアから Windows をインストールする場合、更新プログラムは自動的にダウンロードされてインストールされます。物理メディアから Windows をインストールすると、オンラインで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。

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 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。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。

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. 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 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**]** に格納された回復キーを、表示および管理することができます。

詳細については、「Windows CEIP」セクションを参照してください。

インストール互換性アドバイザー

この機能について

Windows をインストールする際、現在の PC が Windows 8.1 へのアップグレードに対応しているかどうかを判断することができ、お使いのプログラムやデバイスに関する互換性情報が表示されます。

収集、処理、または送信される情報

互換性を確認すると、コンピューター ハードウェアの性能、コンピューターに接続されているデバイス、コンピューターにインストールされているプログラムなど、アップグレードに影響する可能性のある情報が収集されます。場合によっては、プログラムの発行元情報に、発行者名や発行者の電子メール アドレスなどの情報が含まれることがあります。

情報の用途

Microsoft では、収集した情報を、お使いの PC に適したドライバーを決定し、お使いの PC、プログラム、およびデバイスと Windows 8.1 との互換性を判別するために使用します。また、製品やサービスを向上させるために使用する場合もあります。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 ストア、または既存の Windows インストール内の物理メディアから Windows をインストールする場合、ここで説明している情報が Microsoft に送信されます。Windows をインストールするために、物理インストール メディアから起動する場合、オンラインで互換性情報は確認されません。

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] の **[検索とアプリ]** の **[通知]** で、指紋の追加と削除を実行できます。

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、ダウンロードされたファイルとアプリ内の Web コンテンツをチェックして、悪意のあるソフトウェアと安全でない可能性がある Web コンテンツから PC を保護することができます。ダウンロードしたファイルが不明なファイルである場合

や、安全でない可能性がある場合は、それらを開く前に警告が表示されます。SmartScreen がアプリ内で安全でない可能性がある Web コンテンツを検出すると、Windows によってコンテンツの代わりに警告が表示されます。

収集、処理、または送信される情報

ダウンロードされたファイルをチェックするために Windows SmartScreen を使用することを選択した場合、Windows によって SmartScreen オンライン サービスに情報が送信されます。この情報には、ファイル名、ファイル ID ("hash")、およびデジタル証明書情報、さらに標準的な PC 情報および Windows SmartScreen フィルター バージョン番号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。

アプリ内の安全でない可能性があるコンテンツをブロックするために Windows SmartScreen の使用を選択した場合は、Windows ストア アプリの使用時にアクセスされるコンテンツのアドレスと種類などの情報が SmartScreen オンライン サービスに送信されます。この送信に応じて、オンライン サービスは、コンテンツが安全でないまたは疑わしいとして Microsoft に報告されているかどうかを PC に通知します。Microsoft に送信された報告には、アプリの名前や識別子、アプリがアクセスする Web コンテンツの完全なアドレスなどの情報が含まれています。

ユーザーのプライバシーを保護するため、Microsoft に送信される情報は暗号化されます。Microsoft に送信されるアドレスには、アプリ内でアクセスされる Web ページに関連付けることができる情報 (アプリに入力した検索用語など) 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。

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。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ダウンロード ファイルやアプリ内のコンテンツに関する警告をユーザーに示すために、上記で説明した情報を使用します。たとえば SmartScreen が、SmartScreen をサポートするアプリ内で潜在的な脅威を検出すると、Windows によってコンテンツの代わりに警告が表示されます。また Microsoft では、SmartScreen および他の製品やサービスを向上させる場合にも、これらの情報を使用します。この情報を使用してお客様を広告の対象と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、**[PC やプライバシーを保護する]** の **SmartScreen** オンライン サービスを使って、**Windows** ストア アプリと **Internet Explorer** で読み込まれたサイト内の悪意のあるコンテンツや、悪意のあるダウンロードから保護する] をクリックして、Windows SmartScreen 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。Internet Explorer SmartScreen の詳細については、「 Internet Explorer のプライバシーに関する声明に格納された回復キーを、表示および管理することができます。

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 音声認識のドキュメント レビュー機能が有効になると、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

Microsoft Office Word (

いるファイル共有にある、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。ストアから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。

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。

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。

アプリの自動更新

この機能について

この機能は、Windows ストア アプリの更新プログラムをチェックし、更新があればダウンロードとインストールを実行して、アプリが最新バージョンになるようにします。アプリの更新プログラムには、セキュリティ更新プログラム、パフォーマンス更新プログラム、および新しい機能やコンテンツが含まれます。 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。機能の変更については、Windows ストアでアプリの製

品説明ページを参照してください。

収集、処理、または送信される情報

アプリを自動更新するために、ストアは次の情報を 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
- 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、個人情報は含まれていません)
- BIOS 名、リビジョン番号、およびリビジョン日付
- PC の製造元、モデル、Windows のエディションなどの PC に関する基本情報

情報の用途

この情報は、更新サービスを提供するために使用されます。また、集計情報の生成にも使用され、傾向の分析や、製品とサービスの向上に役立てられます。お客様を識別したり、連絡したり、広告の対象とするために、情報が使用され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 ストアからサインアウトしているときでもアプリの更新プログラムを自動的にチェックして、ダウンロードとインストールを実行します。アプリの自動更新をオフにした場合、Windows ストアへのサインイン時にアプリの更新プログラムをインストールするかどうかを選択できます。

アプリの自動更新を無効にするには

1. Windows ストアを開きます。
2. 画面の右端からスワイプし、 **[設定]**に格納された回復キーを、表示および管理することができます。

マウスを使用する場合は画面の右下をポイントし、 **[設定]**に格納された回復キーを、表示および管理することができます。

3. **[アプリの更新]**に格納された回復キーを、表示および管理することができます。

4. **[アプリを自動的に更新する]** をタップまたはクリックして、アプリの自動更新を無効にします。

最新バージョンのアプリの機能やアプリの更新情報については、Windows ストアで各アプリの製品説明ページを参照してください。

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、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。

上で説明したアクセス許可に加えて、ユーザーまたはユーザーの行動に関する情報が保存されているデバイスからの情報をアプリが要求した場合に、Windows では、その情報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。たとえば、ユーザーの場所を追跡する体調維持のためのデバイスを接続した場合、Windows では、そのデバイスへのアクセス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。

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]**をクリックし、 **[アクセス許可]**に格納された回復キーを、表示および管理することができます。

ユーザーに合わせたストアでの検索とおすすめアプリ

この機能について

Windows ストアでアプリを参照または検索するとき、Microsoft では、ユーザーに合ったアプリの検索に役立つおすすめのアプリと検索結果を提示します。

収集、処理、または送信される情報

検索結果を向上させるため、検索機能の使用状況に関する情報 (検索したアプリや選択した検索結果など) が Windows ストアから Microsoft に送信されます。また、Bing およびその他の Microsoft 製品やサービスの使用状況に基づいて、各ユーザーに合わせた検索結果を提示するために、Microsoft アカウントに関連付けられた識別情報も送信されます。各ユーザーに合わせた検索結果を取得しないように選択することもできます。その場合は、識別情報は送信されません。

情報の用途

ストアでは、ストアおよびその他の Microsoft 製品やサービス (Bing や Windows Phone ストアなど) の使用状況に基づいて、パーソナル設定された検索結果とおすすめアプリを提示するために、Microsoft アカウントに関連付けられた識別情報を使用します。この情報には、購入したアプリ、Microsoft アカウントに指定したプロファイル情報、およびアプリの評価とレビューなどの情報が含まれます。この情報は、他の Microsoft 製品やサービスをユーザーに合わせるために使用される場合もあります。

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、Windows ストアのユーザーに合わせた検索結果とおすすめアプリの機能が既定で有効になります。ユーザーに合わせた検索結果とおすすめアプリをストアから取得しないように選択することもできます。その場合は、ストアの設定の **[基本設定]** セクションを使用します。

アプリで使用している Web コンテンツの URL を送信して、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、**[Microsoft** 製品やサービスの品質向上に協力する**]** の **[**位置情報認識アプリを使う場合に一部の位置データを **Microsoft** に送る**]**をクリックして、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、指紋の追加と削除を実行できます。

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、PC の時刻を自動的に同期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。この機能は、[PC 設定] の **[**日付と時刻**]** でオフにできます。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、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てます。

選択および管理

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]**に格納された回復キーを、表示および管理することができます。

ページのトップへ

作業フォルダー

この機能について

作業フォルダーは、職場のファイル サーバーに対して自動的に同期が維持される PC 上のフォルダーです。

収集、処理、保存、または送信される情報

作業フォルダーにファイルを保存すると、そのファイルは職場で管理されたファイル サーバーに対して自動的に同期されます。他の PC から自身の作業フォルダーに保存されたファイルは、自身で使用中の PC に同期されます。

情報の用途

Windows は、フォルダーの同期を維持するために作業フォルダー内のファイルを送受信します。職場のサーバーに格納された情報の用途には、職場のプライバシー ポリシーが適用されます。

選択および管理

[PC 設定] の 社内 で、指紋の追加と削除を実行できます。

ページのトップへ

社内

"社内" 機能を使用すると、デバイスを Windows Intune に接続できます (別途 Microsoft のサブスクリプションが必要)。または、他のサード パーティのデバイス管理サーバーに接続できます。"社内" 機能を使用した PC の管理を社内の管理者に許可すると、その管理者は、PC へのセキュリティ ポリシーの適用、アプリのインストール、PC 上にある特定の構成や各種情報の確認など、さまざまな管理タスクを実行できます。この機能を会社で利用する際の詳細については、社内のプライバシー ポリシーを参照するか、システム管理者にお問い合わせください。

収集、処理、または送信される情報

"社内" 機能をセットアップして使用する場合、PC は、会社で利用しているデバイス管理サービス (Microsoft でホストされている場合もあります) と通信します。"社内" 機能に接続する際に入力した資格情報は、そのサービスに送信されます。

情報の用途

デバイス管理サービスに送信される情報は、そのサービスと PC 間の接続を確立するために使用されます。また、Windows ストアからセルフサービス アプリをインストールする場合も、この情報が使用されます。セルフサービス アプリの詳細については、社内のプライバシー ポリシーを参照するか、システム管理者にお問い合わせください。

選択および管理

会社で "社内" 機能を使用する場合、[PC 設定] の **[ホームグループ]**にある [社内] で接続や切断を実行できます。自分の PC がサービスに接続された後はいつでも、その接続に関する情報を確認したり、接続を切断したりすることができます。

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 8.1 および Windows Server 2012 R2 のプライバシーに関する声明

このページは、以下のセクションで構成されている Windows 8.1 および Windows Server 2012 R2 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。

- ハイライト
- 声明これは 完全な Windows 8.1 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。
- 機能の補足条項。プライバシー関連の影響がある Windows 8.1 および Windows Server 2012 R2 の機能について説明しています。
- アプリの補足条項 (このページ)。Windows 8.1 でプライバシー関連の影響があるアプリについて説明しており、各アプリに適用されるプライバシーに関する声明へのリンクを含みます。
- サーバーの補足条項。プライバシー関連の影響がある Windows Server 2012 R2 の追加の機能について説明していま

す。

個々の Windows 機能またはサービスに関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と適用される補足条項、または機能ごとの独自の声明を確認してください。

PC のセットアップ時にカスタマー エクスペリエンス向上プログラム (CEIP) に参加することを選択した場合、これらのアプリではアプリのパフォーマンスおよび信頼性に加えて各アプリの使用方法に関するレポートのために情報が収集されます。 Microsoft は、CEIP 情報を製品やサービスを向上させるために使用します。 お客様を識別したり、連絡したり、広告の対象とするために、情報が使用されることはありません。 [PC 設定] で CEIP はオフにできます。 詳細については、「CEIP プライバシーに関する声明」を参照してください。

次のリンクにより、一覧の各アプリに適用されるプライバシーに関する声明に移動します。

アラーム

電卓

カレンダー

カメラ

ファイナンス

フード

ゲーム

健康

ヘルプ+使い方

メール

地図

ミュージック

ニュース

People

リーダー

リーディング リスト

スキャン

Skype

サウンド レコーダー

スポーツ

トラベル

ビデオ

天気

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 8.1 および Windows Server 2012 R2 のプライバシーに関する声明

このページは、Windows 8.1 および Windows Server 2012 R2 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セクションで構成されています。

- ハイライト
- 声明。これは完全な Windows 8.1 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。
- 機能の補足条項。プライバシー関連の影響がある Windows 8.1 および Windows Server 2012 R2 の機能について説明しています。
- アプリの補足条項。プライバシー関連の影響がある Windows 8.1 アプリについて説明しています。
- サーバーの補足条項 (このドキュメント)。プライバシー関連の影響がある Windows Server 2012 R2 の追加の機能について説明

プログラム (CEIP) と Windows エラー報告 (WER)

ソフトウェア インベントリ ログ

しています。

個々の Windows 機能またはサービスに関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 Windows のプライバシーに関する声明および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。

Windows Server 2012 R2 Essentials に含まれる機能の プライバシーに関する影響については、Windows Server 2012 R2 Essentials および Windows Server Essentials Experience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、サーバーの役割とローカル サーバーにインストールされている製品 (UAL に登録されている場合) について、クライアント要求 (ユーザーとデバイスの両方の要求) のレコードを収集して集約する機能です。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、オフラインの顧客のクライアント アクセス ライセンス (CAL) 登録の管理で、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、DNS の役割がインストールされている場合はホスト名、Hyper-V の役割がインストールされている場合は仮想マシン ID がサーバー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

UAL のデータは、管理者が WMI プロバイダーおよび Windows PowerShell コマンドレットを使用して、ローカルの ESE データベースから使用できます。UAL 機能以外で Windows がこのデータを使用す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 を完全に無効にするには、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 および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、およびスタートアップの種類。

- 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。
- パフォーマンスに関する情報。 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、ローカル サーバーを除く任意のサーバーについて、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、データを収集する対象のサーバーを選択することができます。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。サーバー マネージャーでは、資格情報のローカルへの保存に関して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

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 ベースのアプリ向けの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、アプリのセキュリティを維持しながら組織間での共同作業が可能になり、ローカルまたは他のネットワークのアプリに簡単にアクセスできるようになります。AD FS で使用されるセキュリティ トークン サービスでは、Active Directory ドメイン サービス (AD DS) を使用してユーザーを認証し、各種のプロトコルを使用してセキュリティ トークンを発行します。このデジタル署名されたトークンには、ユーザーについての要求が含まれます。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

AD FS でユーザーの認証を行う際、ユーザーの資格情報が収集されます。この資格情報は、認証用の Active Directory ドメイン サービスにそのまま送信され、AD FS でローカルに格納されることはありません。Active Directory ドメイン サービスに格納されているユーザーの属性は、AD FS 管理者が構成した要求規則に応じて、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されたパートナーに送信されます。Microsoft には情報は送信されません。

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、ユーザーのみが使うこと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、信頼されたパートナーに送信したりす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、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) をユーザー ログオン情報で追跡できます。

収集、処理、または送信される情報

IPAM サーバーでは、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、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て、収集されたログを 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検索できます。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、ユーザーのみが使うこと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ず、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 をインストールしたサーバーで 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 の 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。統合リモート アクセスでは DirectAccess を使用して、Windows 8 を実行しているリモート クライアント コンピューターに、会社のネットワークへの中断のない透過的な接続を提供します。また、サイト間のローカル接続、その他のネットワーク接続など、リモート アクセス サービス (RAS) 機能 (従来の VPN サービス) も提供します。

収集、処理、または送信される情報

統合リモート アクセスによるユーザーの監視では、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 (クライアントがネットワーク アドレス変換 (NAT) の背後にある場合はパブリック IP アドレス) などが含まれます。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表示できるのは、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

査や準拠の目的で管理者が使用します。Microsoft には情報は送信されません。

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、アカウンティングでそれらのいずれかを使用するように管理者が構成した場合だけです。管理者がアカウン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 サーバーのアカウンティングでユーザー名と 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、デスクトップの集中管理戦略の実施、デスクトップやアプリの管理、柔軟性および準拠とデータ セキュリティの向上の両立に役立つプラットフォームです。

収集、処理、または送信される情報

RDS によるユーザーの監視では、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 (クライアントがネットワーク アドレス変換 (NAT) の背後にある場合はパブリック IP アドレス) などが含まれます。このデータは、ユーザーが同意した場合、Windows Internal Database (WID)/SQL サーバーに自動的に格納されます。Microsoft には情報は送信されません。この情報にアクセスして表示できるのは、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、内部監査や準拠の目的で管理者が使用します。Microsoft には情報は送信されません。

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、 機能の補足条項 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、 機能の補足条項 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、 機能の補足条項 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 マネージャーおよびコントロール パネルとコマンド ラインのどちらでも実行できます。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、**[関連項目]**をクリックし、**[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 の有効化
  サーバー マネージャーを開き、 ローカル サーバーをクリックします。[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] をクリックして、 **[OK]**もお読みください。

- CEIP の無効化
  サーバー マネージャーを開き、 ローカル サーバーをクリックします。[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**]** をクリックして、 **[OK]**もお読みください。

- WER の有効化
  サーバー マネージャーを開き、 ローカル サーバーをクリックします。[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**]**をクリックして、 **[OK]**もお読みください。

- WER の無効化
  サーバー マネージャーを開き、 ローカル サーバーをクリックします。[Windows エラー報告] リンクをクリックし、 **[**参加しません**]**をクリックして、 **[OK]**もお読みください。

複数のコンピューター

- CEIP の有効化
  サーバー マネージャーを開き、 **[**すべてのサーバー**]**をクリックします。[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**]** をクリックします。[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**)]**をクリックします。[サーバーの選択] コントロールの [サーバー名] の横のチェック 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 の無効化
  サーバー マネージャーを開き、[すべてのサーバー] をクリックします。[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**]** をクリックします。[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**]**をクリックします。[サーバーの選択] コントロールの [サーバー名] の横のチェック 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 の有効化
サーバー マネージャーを開き、 **[すべてのサーバー]**をクリックします。[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**]** をクリックします。[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**)]**をクリックします。[サーバーの選択] コントロールの [サーバー名] の横のチェック 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 の無効化
  サーバー マネージャーを開き、 **[すべてのサーバー]**をクリックします。[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**]** をクリックします。[Windows エラー報告] タブで、 **[**いいえ、参加しません**]**をクリックします。[サーバーの選択] コントロールの [サーバー名] の横のチェック 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

ソフトウェア インベントリ ログ

この機能について

ソフトウェア インベントリ ログ (SIL) は、Windows Server のオペレーティング システム エディション、Windows Server にインストールされているソフトウェア、そのソフトウェアが実行されているサーバーの特性の基本インベントリを簡素化する新しい WMI クラスと Powershell コマンドレットのセットを提供します。 また、SIL には、管理者が有効にした場合に、WMI プロバイダーから 1 時間ごとにデータを収集する機能があります。さらに、Set-SilLogging -TargerUri を使って集計サーバーを指定すると、収集したデータをネットワーク経由で集計サーバーに送信できます。

収集、処理、または送信される情報

管理者によって構成されている場合は、データがネットワーク経由で集計サーバーに送信されます。 既定では、何も収集、処理、送信されません。 このデータには次のようなものが含まれます。

- Windows Server の名前とインストールされているオペレーティ

ング システムのエディション。

- サーバーにインストールされているすべてのソフトウェアの名前、バージョン、発行元の一覧と、各ソフトウェアがインストールされた日付。
- サーバー システムの完全修飾ドメイン名。
- サーバー システムにインストールまたは割り当てられているプロセッサ、論理プロセッサ、コアの数、種類、製造元。

次のデータについては収集と処理が行われますが、管理者によって時間単位のタスクが有効にされ、対象の集計サーバーが指定されていても、既定では送信されません。

- MsftSil_UalAccess クラスと Get-SilUalAccess コマンドレットでは、ユーザー アクセス ログ (UAL) 機能に登録された役割または製品ごとに、照会時点の 2 日前からの一意のユーザーとデバイスの合計数が処理されます。 これらはカウントだけで、ユーザー情報やデバイス情報が出力または送信されることはありません。 SIL 自体がカウントを計算するときは、UAL クラスからユーザー情報とデバイス情報を処理する必要があります。 このデータにアクセスできるのはローカル コンピューターの管理者だけです。 UAL API に必要なアクセス権を SIL が変更することはありません。

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

SIL WMI プロバイダーは、システムに既に存在する他の API から提供されたデータを集計します。 管理者によって構成されている場合は、より高度な集計操作のためにデータがネットワーク経由でサーバーに送信されます。 既定では、何も収集、処理、送信されません。 MsftSil_UalAccess クラスと Get-SilUalAccess コマンドレットの場合、処理されたデータには、ユーザー アクセス ログ (UAL) 機能に登録された役割または製品ごとの、収集時点の 2 日前からの一意のユーザーとデバイスの合計数が含まれます。ただし、ユーザーやデバイスを識別するデータは一切出力されません。 また、この WMI クラスとコマンドレットはシステムに存在しますが、システム管理者によって SIL が構成されている場合、収集されて 1 時間ごとに集計サーバーに送信される SIL データ ペイロードにはこれらは含められません。

選択および管理

SIL の時間単位のタスクは、既定で無効になっています。すべての SIL API は、ローカル システムの管理者が既定で照会できます。 SIL の時間単位のタスクは、サーバーの実行中に Start-SilLogging コマンドレットと Stop-SilLogging コマンドレットを使うことで開始したり停止したりできます。 サーバーの管理者は、Set-SilLogging コマンドレットを使って、時間単位のタスクを開始する日付と時刻 (既定値はローカル システム時刻の午前 3 時)、送信先の集計サーバーの Uniform Resource Identifier (URI)、データを安全に送信するために必要な証明書の拇印を設定できます。

すべての SIL 構成設定は、時間単位のタスクの開始と停止も含めてレジストリで変更できます。ただしこの方法は、システムが仮想マシンである場合にのみ、かつシステムの初回起動前にのみ使うことができます。

ページのトップへ