Windows Analytics

評価ガイド

日本マイクロソフト株式会社

発行日 ：2018 年 12 月

このドキュメントに記載されている情報は、このドキュメントの発行時点におけるマイクロソフトの見解を反映したものです。変化する市場状況に対応する必要があるため、このドキュメントは、記載された内容の実現に関するマイクロソフトの確約とはみなされないものとします。 また、発行以降に発表される情報の正確性に関して、マイクロソフトはいかなる保証もいたしません。
このホワイトペーパーは情報提供のみを目的としており、明示、黙示、または法律上の保証に関わらず、これらの情報についてマイクロソフトはいかなる責任も負わないものとします。
お客様ご自身の責任において、適用されるすべての著作権関連法規に従ったご使用を願います。このドキュメントのいかなる部分も、米国 Microsoft Corporation の書面による許諾を受けることなく、その目的を問わず、どのような形態であっても、複製または譲渡することは禁じられています。 ここでいう形態とは、複写や記録など、電子的な、または物理的なすべての手段を含みます。
ただしこれは、著作権法上のお客様の権利を制限するものではありません。 マイクロソフトは、このドキュメントに記載されている内容に関し、特許、特許申請、商標、著作権、またはその他の無体財産権を有する場合があります。別途マイクロソフトのライセンス契約上に明示の規定のない限り、このドキュメントはこれらの特許、商標、著作権、またはその他の知的財産に関する権利をお客様に許諾するものではありません。
© 2018 Microsoft Corporation. All rights reserved.
Microsoft、Windows、Windows ロゴ、及びWindows Server は米国 Microsoft Corporation の米国またはその他の国における登録商標または商標です。
このドキュメントに記載されている会社名、製品名には、各社の商標のものもあります。

■ 企画/執筆/監修

執筆 ：株式会社ソフィアネットワーク
企画/監修/改訂 ：日本マイクロソフト株式会社

■ 改訂履歴

バージョン	年月日	改訂者	内容
1.5	2018 年 12 月	日本マイクロソフト	改訂
1.0	2018 年 10 月	ソフィアネットワーク	初版を作成

内容

1 はじめに 5

2 Windows Analytics の構成要素 6

2.1 モダン管理 6

2.2 Windows Analytics の構成要素とアーキテクチャ 7

2.3 Upgrade Readiness とは 9

2.4 Update Compliance とは 10

2.5 デバイスの正常性とは 11

2.6 Log Analytics による状態監視 12

2.7 Power BI との連携 13

3 評価環境と前提条件 14

3.1 Microsoft Azure 無料試用版の取得 15

4 Windows Analytics の初期設定 21

4.1 Log Analytics ワークスペースの作成 22

4.2 ソリューションの追加 24

4.3 Upgrade Readiness Deployment スクリプトの実行 30

5 Upgrade Readiness による現状分析 39

5.1 アップグレードの概要 41

5.2 Spectre と Meltdown 43

5.3 ステップ 1： 重要なアプリを識別する 45

5.4 ステップ 2： 問題を解決する 47

5.5 ステップ 3： 展開 49

5.5.1 コンピューター グループの作成 50

5.6 ステップ 4： モニター 57

5.7 Office アドイン 58

5.8 サイト検出 58

6 Update Compliance による現状分析 59

6.1 対処が必要 60

6.2 セキュリティ更新プログラムの状態 62

6.3 機能の更新状態 64

6.4 Windows Defender AV 状態 66

6.5 配信の最適化の状態 67

7　デバイスの正常性 による現状分析 69

7.1　デバイスの信頼性 71

7.2　アプリの信頼性 75

7.3　WIP アプリの学習 80

7.4　ログインの正常性 82

8　クエリの書き方 85

8.1　クエリ作成・実行ユーザーインターフェイスへのアクセス 85

8.2　クエリの書式 88

8.2.1　参照するレコード 88
8.2.2　フィルター処理 89
8.2.3　カウント処理 89

9　まとめ 91

1　はじめに

オンプレミスにすべてのサーバーとクライアントが設定されている環境では、様々なシステム管理製品を利用してクライアント デバイスの管理を行っていました。しかし、近年のワークスタイルの変化や、それを支えるクラウド テクノロジーの台頭により、クライアント デバイスは社外で利用されるケースが多くなっています。こうした環境の中で、Windows 10 を適切に管理するためには、管理そのものもクラウドをベースにしたものに変化させていく必要があります。そこで、本評価ガイドでは、クラウド ベースで Windows 10 の様々な状態管理が行える Windows Analytics の利用方法と Windows 10 の管理方法について解説します。

本書の構成

章段		説明
1	はじめに	このドキュメントの概要について説明します。
2	Windows Analytics の構成要素	この章では、Windows Analytics の特徴について紹介します。
3	評価環境と前提条件	この章では、本書で構築する評価環境および前提条件について説明します。
4	Windows Analytics の初期設定 (Step by Step)	この章では、Windows Analytics を使って、これから Windows 10 を管理する際に必要な初期設定について説明します。
5	Upgrade Readiness による現状分析	この章では、Upgrade Readiness で提供される情報の見かたと運用管理への活かし方について説明します。
6	Update Compliance による現状分析	この章では、Update Compliance で提供される情報の見かたと運用管理への活かし方について説明します。
7	デバイスの正常性 による現状分析	この章では、デバイスの正常性 で提供される情報の見かたと運用管理への活かし方について説明します。
8	クエリの書き方	この章では、Log Analytics におけるクエリ文の書き方について説明します。
9	まとめ	

2 Windows Analytics の構成要素

Windows Analytics とは、Microsoft Azure のサービスとして提供される、Log Analytics に含まれる、クラウド ベースのクライアント デバイス監視サービスです。「監視」といっても、実際の組織の中では、クライアントデバイスに対して行う管理の種類によって、監視すべき項目・要素は異なります。そこで、本章では Windows Analytics の構成要素とそれぞれの特徴について解説します。

2.1 モダン管理

従来のシステム管理製品を利用した IT インフラの管理は、サーバー/クライアント共にオンプレミスにあることを前提としたものでした。しかし、冒頭でも紹介したように、近年ではワークスタイルの変化により、クライアント デバイスは社外で利用されたり、個人用のデバイスを使って仕事をしたりするようになっています。このようにクライアント デバイスの使われ方が変化する中で、従来のシステム管理製品を使って物理的な場所に基づくデバイスの管理方法では、適切なデバイスの管理ができない可能性が高まり、結果として生産性の低下やセキュリティの問題などを引き起こす可能性があります。

そこで、従来のシステム管理製品に代わり、クラウド ベースでデバイスを管理することで、場所やデバイスの種類を問わずデバイスを利用できるようなソリューションが求められています。このようなデバイスの管理方法を「モダン管理」(Modern management) と呼びます。
デバイス管理に関わる、様々な要素をクラウド ベースで行えるようにし、シンプルな管理を実現することがモダン管理を実現する上で重要な要素となります。
図 2.1-1 では、Windows 10 デバイスを管理する際の、これまでの管理とモダン管理、それぞれの管理ステップを表したものです。

図 2.1-1 これまでの管理とモダン管理による Windows 10 の管理ステップ

	展開とプロビジョニング	ID と認証	構成	更新とサービス
これまでの管理	・キッティング プロセスによるイメージ展開 ・イメージ展開サーバーを利用した展開	・Active Directory による認証とデバイスの管理	・グループ ポリシーまたは SCCM によるポリシー管理	・WSUS または SCCMを利用した更新プログラムの管理と展開
モダン管理	・クラウド ベースで既存の状態を確認し、アップグレード ・新規デバイスの自動登録 (Windows AutoPilot) ・BYOD	・Azure AD による クラウド ベースの認証とデバイスの管理	・MDM サービスによる ポリシー管理	・クラウド経由で更新プログラムの適用状況の管理と更新に関わるポリシーの管理

これまでの管理では、Active Directory や System Center Configuration Manager (SCCM) などのサーバー製品を利用してオンプレミス ベースでのシステム管理を行っていました。これに対し、モダン管理では展開、認証、構成、更新と Windows 10 のそれぞれの管理ステップごとに用意されるクラウド サービスを活用し、デバイスの種類や場所を問わない管理を実現しています。

2.2 Windows Analytics の構成要素とアーキテクチャ

図 2.1-1 の Windows 10 の管理ステップのうち、[展開とプロビジョニング] ステップでは Windows 7 や Windows 8.1 を利用した既存のデバイスからのアップグレード、[更新とサービス] ステップでは既存の Windows 10 デバイスからに対する品質更新プログラムや機能更新プログラムの適用が主な作業として挙げられます。このとき、アップグレードや更新プログラムの適用を行うに当たり、現状の構成に問題がないか？や、必要な要件を満たしているか？などを事前に把握しておくことが必要です。また、これらの情報の把握は、モダン管理の環境においてはクラウド ベースで実現できる必要があります。そこで、Windows Analytics ではアップグレードや更新プログラムの適用を行うに当たっての現状の把握ができるようにするために、OS テレメトリ (匿名化され、送信されるデバイスの診断データ) を利用してクラウド ベースで情報収集を行います。
Windows Analytics は、次の 3 つのサービスから構成されています。

- ✓ **Upgrade Readiness**
  OS 展開を行うに当たり、デバイスが要件を満たしているかなどの情報の可視化を担当
- ✓ **Update Compliance**
  更新プログラムの適用を行うに当たり、デバイスが要件を満たしているかなどの情報の可視化を担当

✓ **デバイスの正常性**

デバイスの現状のトラブルがないかについての情報の可視化を担当

それぞれのサービスは次のような処理の流れでポータル画面に情報収集の結果を表示します。

① Windows Analytics から提供されるスクリプトを実行したコンピューターからクライアント デバイスの状態に関わる情報（テレメトリ）をスクリプトの実行時に指定した商用 ID と共にクラウドに送信します。商用 ID は送信したデータがどの Windows Analytics のワークスペースで扱うかを表わす情報になります。

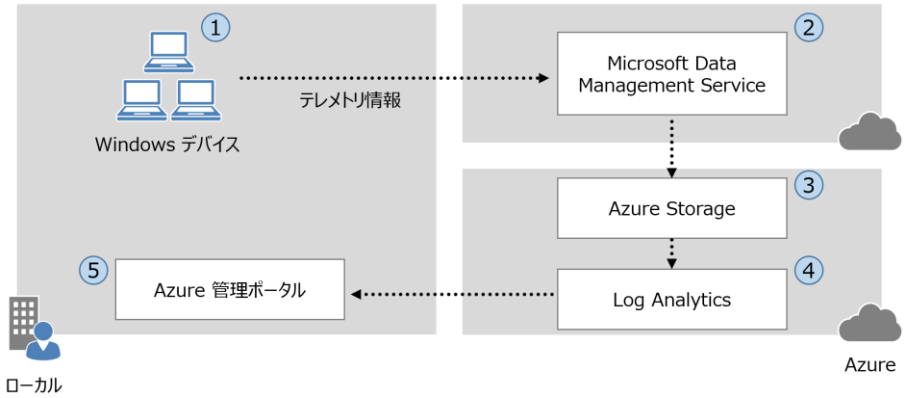
② クライアントから送信された情報は、米国リージョンにある Microsoft Data Management Service へ送信され、毎日スナップショットを作成します。

③ 作成したスナップショットは、米国リージョンにある Windows Analytics 用の Azure Storage にコピーされます。このとき、個々のスナップショットは商用 ID の情報に基づいて、別々に保管されます。

④ Azure Storage にコピーされたデータは、特定の Azure テナントで作成された Log Analytics のワークスペース（ワークスペースを作成したリージョン）にコピーされます。

⑤ Log Analytics に格納されたデータは Azure 管理ポータルから Upgrade Readiness、Update Compliance、Device Health のいずれかの情報として参照できるようになります。

図 2.2-1 Windows Analytics のアーキテクチャ



以上のステップから、Windows Analytics で参照可能な各コンポーネント（Upgrade Readiness、Update Compliance、デバイスの正常性）の情報は Log Analytics のアーキテクチャを利用して収集した情報に対して特定のクエリを実行し、可視化したものであることがわかります。

なお、Microsoft Azure の管理ポータル画面（https://portal.azure.com/）では、Windows Analytics の各コンポーネントは Log Analytics のワークスペース内のソリューションとして登録され、参照することができます。

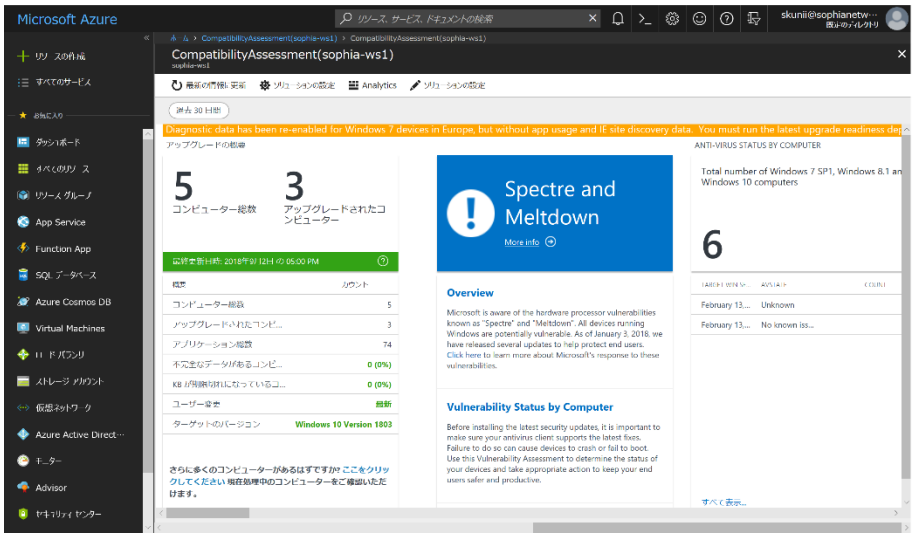
2.3 Upgrade Readiness とは

Windows 8.1/7 から Windows 10 へのアップグレードや、Windows 10 の機能更新プログラムの適用によって定期的なアップグレードを行いますが、アップグレードを行うにあたり、必要な情報の収集は欠かせません。Upgrade Readiness では組織に展開している Windows 10/8.1/7 のコンピューターから収集した情報のうち、以下の情報を可視化することで、正常な状態であることを確認し、コンピューターのアップグレードが可能な状態であることを確認できるようにしています。

- ✓ ウイルス対策の状態
- ✓ 更新プログラムの適用状況
- ✓ アプリの互換性
- ✓ ドライバーの互換性
- ✓ Office のアドイン
- ✓ Web サイトのドキュメント モード

収集した情報は Azure 管理ポータル画面から Upgrade Readiness の情報として参照することができます (画面 2.3-1)。

画面 2.3-1 Azure 管理コンソール画面内の Upgrade Readiness



これらの情報を収集し、分析を行うことにより、Windows 7 や Windows 8.1 からの OS アップグレードはもちろんのこと、新しい機能更新プログラムの適用を検討している Windows 10 コンピューターのアップグレードの妥当性について検討することができるようになります。

2.4 Update Compliance とは

Windows 10 では機能更新プログラム、品質更新プログラム、Windows Defender ウイルス対策の 3 点の定期的なアップデートにより、最新の状態を保ちますが、アップデートを行うにあたり、アップデートの適用状況や、アップデートを行うための準備ができているか、などの必要な情報の収集は欠かせません。Update Compliance では組織に展開している Windows 10 コンピューターから収集した情報のうち、以下の情報を可視化し、コンピューターの状態を確認できるようにしています。

- ✓ デバイスの状態
- ✓ 更新プログラムの適用に関わるトラブル
- ✓ 品質更新プログラムの適用状況
- ✓ 機能更新プログラムの適用状況
- ✓ Windows Defender ウイルス対策による保護状況
- ✓ 配信の最適化の状態

収集した情報は Azure 管理ポータル画面から Update Compliance の情報として参照することができます (画面 2.4-1)。

画面 2.4-1 Azure 管理コンソール画面内の Update Compliance

2.5 デバイスの正常性とは

デバイスの正常性は、Windows 10 デバイスに関わる正常性の情報を可視化するサービスで、具体的には以下の情報を提供します。

- ✓ 頻繁にクラッシュが発生するデバイスの識別
- ✓ 特定のデバイスドライバーが原因でクラッシュが発生するデバイスの識別
- ✓ Windows Information Protection に追加するべきアプリの確認
- ✓ 他のデバイスとの正常性の比較

なお、Windows Analytics のデバイスの正常性を利用する場合、次のいずれかのライセンスが必要となります。

- ✓ ソフトウェア アシュアランスが有効なデバイスごとに Windows 10 Enterprise または Windows 10 Education のライセンス
- ✓ デバイスごと、またはユーザーごとの Windows 10 Enterprise E3 または E5 のサブスクリプション (Microsoft 365 F1, E3, E5 を含む)
- ✓ Windows 10 Education A3 または A5 (Microsoft 365 Education A3 または A5) のライセンス
- ✓ デバイスごと、またはユーザーごとの Windows VDA E3 または E5 のサブスクリプション

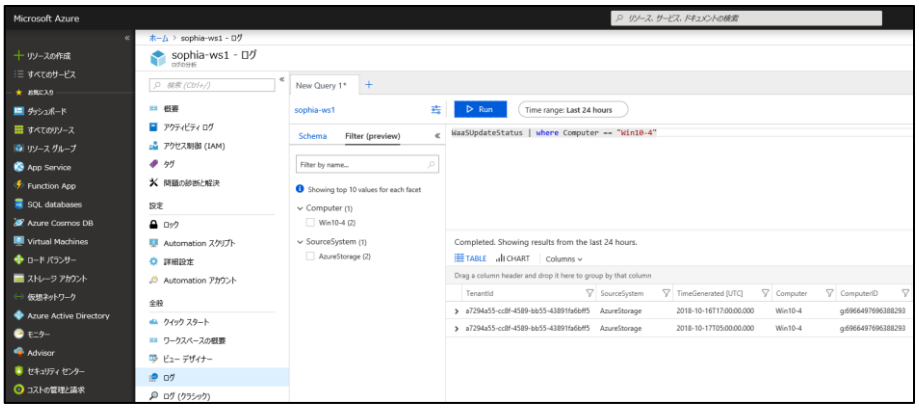
これらのライセンスは保有するだけでよく、デバイスにインストールしてある必要はありません。

2.6 Log Analytics による状態監視

Windows Analytics は Log Analytics サービスから提供されるため、スクリプトが実行されたデバイスの情報は Log Analytics のデータとして収集されます。そのため、収集した情報は Upgrade Readiness や Update Compliance からだけでなく、Log Analytics から直接参照することができます。

Upgrade Readiness や Update Compliance は、あらかじめ用意された形式の結果だけを参照できるような仕組みですが、Log Analytics では、収集した情報に対してクエリを実行することによって、管理者が望む、様々な形式の情報を参照できるメリットがあります。

画面 2.6-1 Log Analytics 画面からクエリを実行した様子

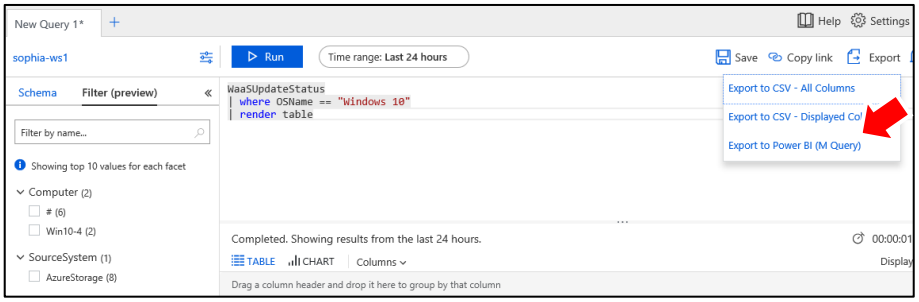


2.7 Power BI との連携

Log Analytics で収集した情報は、Upgrade Readiness や Update Compliance による資格化だけでなく、Power BI でクエリを実行させることによって、Power BI から収集結果を視覚化することができます。

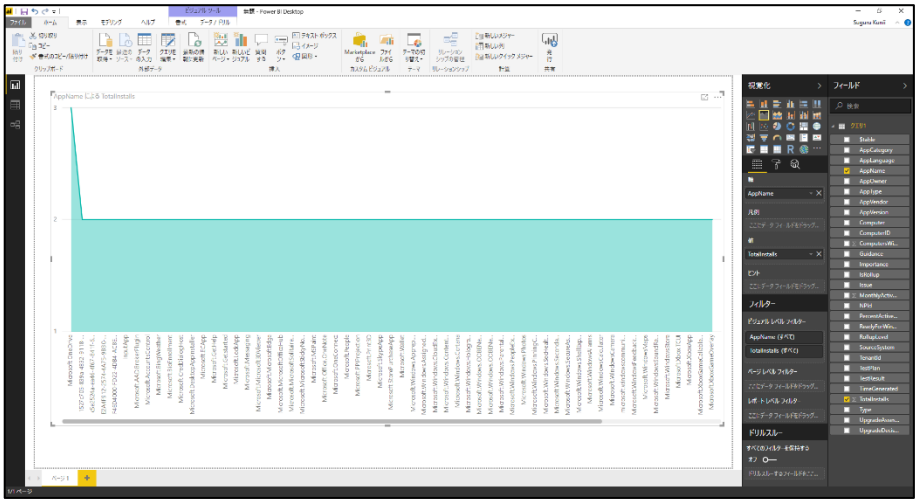
画面 2.7-1 にある [Export to Power BI] ボタンをクリックすることで、Log Analytics で入力・実行したクエリ文を Power BI のクエリ文に変換した文字列をテキストファイルでダウンロードできます。

画面 2.7-1 Log Analytics 画面の [Export to Power BI] ボタン



ダウンロードしたクエリ文は Power BI デスクトップ アプリの Power Query に直接コピーアンドペーストすることで、Power BI からクエリを実行し、結果を Power BI の各種形式に沿った視覚化ができるようになります (画面 2.7-2)。

画面 2.7-2 Power BI のレポート画面



3　評価環境と前提条件

本書では、Windows Analytics のサービスのうち、Upgrade Readiness と Update Compliance の 2 つを利用して、Windows 7、Windows 8.1、 Windows 10 の管理に関わる各種情報を収集し、その結果の評価ができるようにすることを目標に、それぞれの手順を解説します。Windows Analytics はテレメトリのデータを利用しているため、前提条件として、テレメトリが有効になっていることが必要です。既定でテレメトリ情報が収集されるように定義されていますが、グループポリシーなどによって無効化することが可能であるため、無効化していないことを確認してください。
本書の解説に基づく評価を行うに当たり、あらかじめ Windows 7 SP1、Windows 8.1、Windows 10 のいずれかのコンピューターを Hyper-V の仮想マシンまたは物理マシンにてご用意ください。

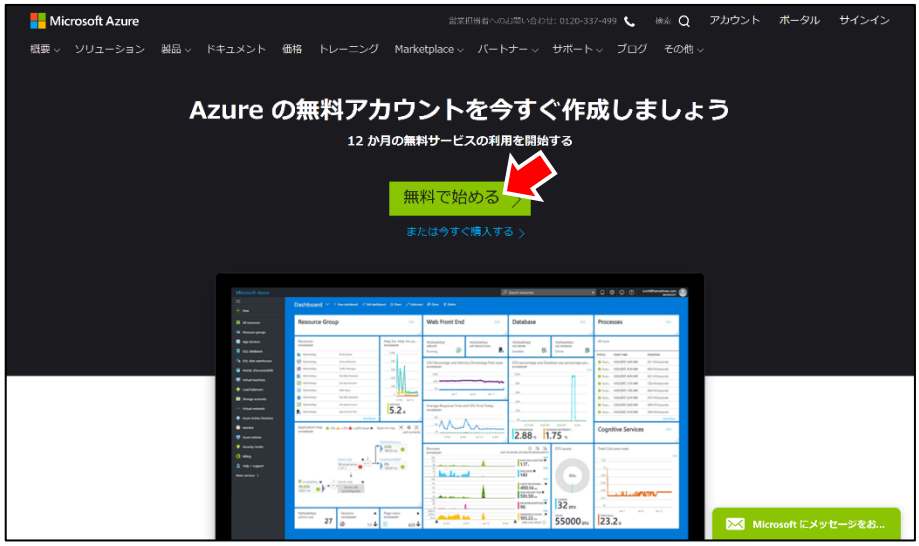
また、Windows Analytics の各サービスは、Microsoft Azure から提供されるため、本書の解説に基づき評価を行うには、Microsoft Azure のテナントが必要です。お持ちでない場合は、マイクロソフトアカウントまたは Azure Active Directory ユーザー (Office 365 のアカウント) を用意の上、「3.1 Microsoft Azure 無料試用版の取得」の手順に従って、評価版を取得してから開始してください。

3.1 Microsoft Azure 無料試用版の取得

本節では、Microsoft Azure を 30 日間無料で利用できる、無料試用版を取得します。

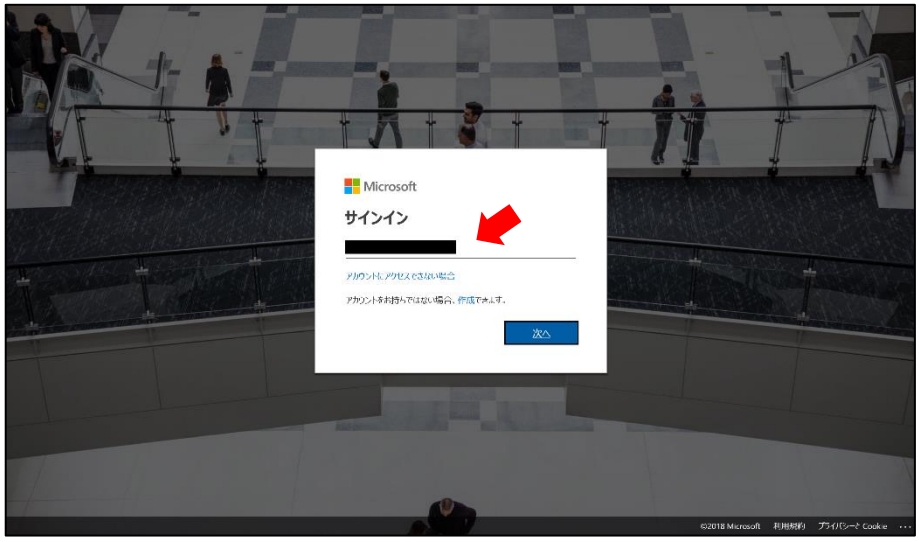
1) ブラウザー画面で、「https://azure.microsoft.com/ja-jp/free/」にアクセスします。

2) Microsoft Azure 画面で、[無料で始める] をクリックします。

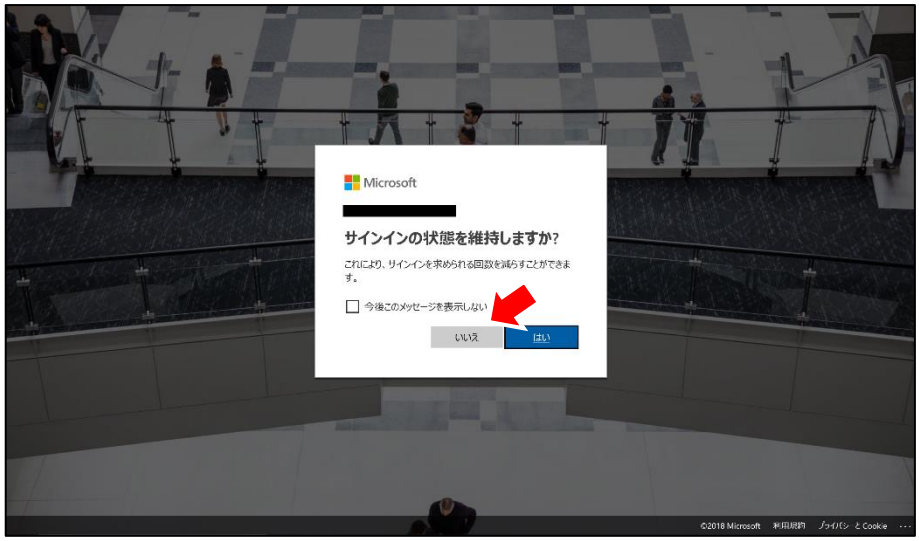


NOTE:
業務で使用する Microsoft Azure テナントを取得する場合、[または今すぐ購入する] をクリックして始めます。また、無料試用版を取得した場合でも期限終了の後、本契約に移行することもできます。

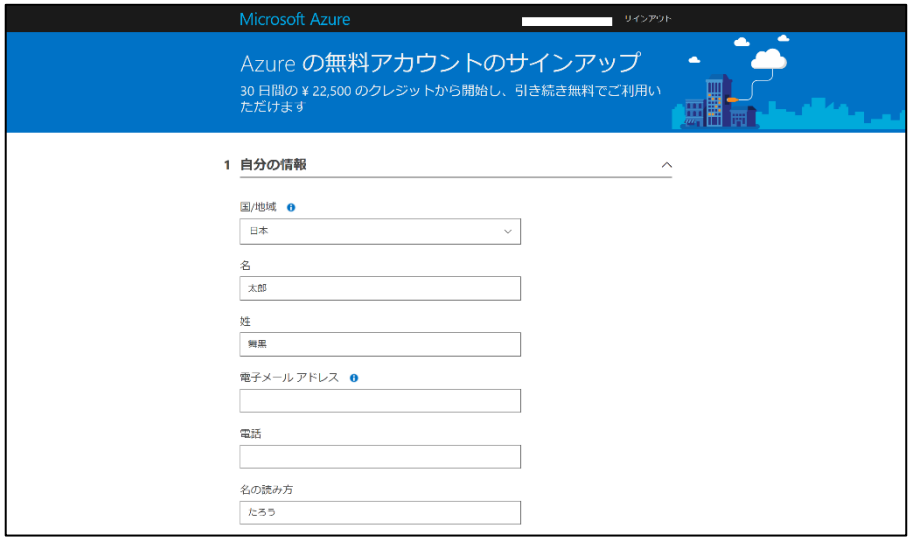
3) サインイン画面で、Azure Active Directory ユーザーまたはマイクロソフト アカウントのユーザー名とパスワードを入力し、サインインします。



4) [サインインの状態を維持しますか？] 画面で、[いいえ] をクリックします。



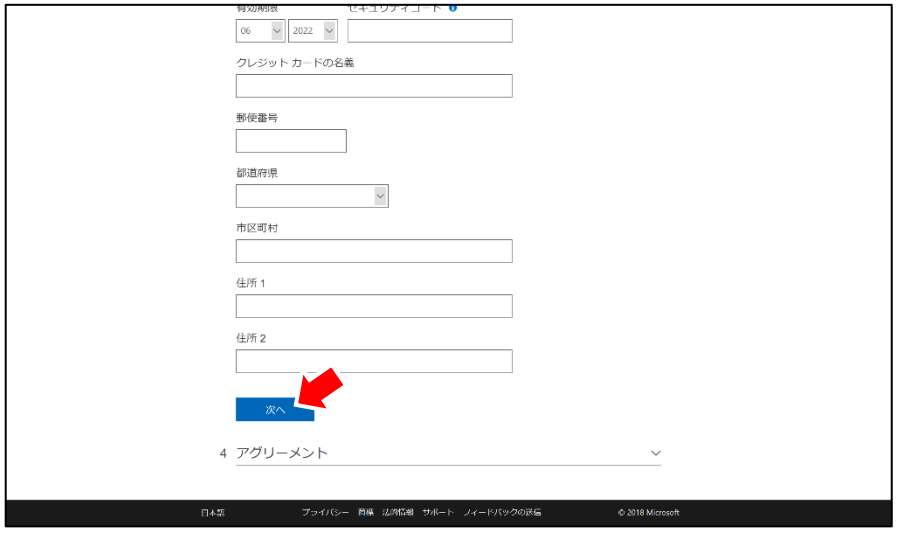
5）[Azure の無料アカウントのサインアップ] 画面で、自分の情報を入力し、[次へ] をクリックします。



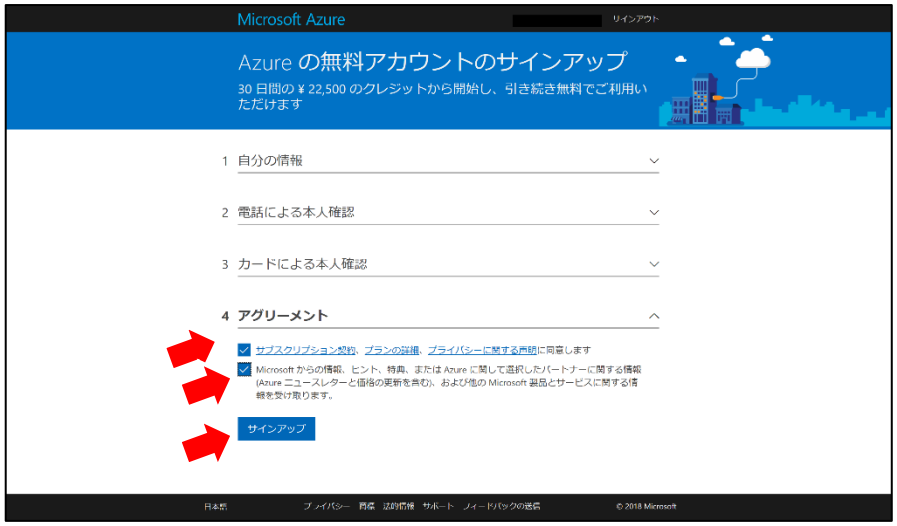
6) [Azure の無料アカウントのサインアップ] 画面で、[電話による本人確認] 欄から自分の電話番号を入力し、[テキスト メッセージを送信する] をクリックします。

7) 電話番号宛にテキスト メッセージが届いたら、メッセージに書かれた番号を [確認コード] 欄に入力し、[コードの確認] をクリックします。

8) [Azure の無料アカウントのサインアップ] 画面で、[カードによる本人確認] 欄からクレジットカード番号とカード番号に登録の住所をそれぞれ入力し、[次へ] をクリックします。

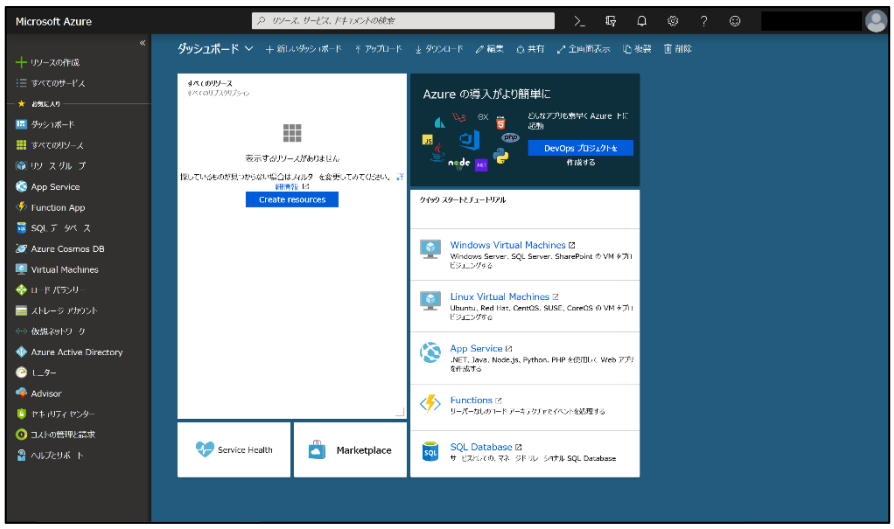


9) [Azure の無料アカウントのサインアップ] 画面で、[アグリーメント] 欄で 2 か所のチェックボックスにチェックをつけ、[サインアップ] をクリックします。



10)Microsoft Azure 画面で、[ポータルに移動] をクリックします。

11)Microsoft Azure 管理ポータル画面にアクセスできたことを確認します。



4 Windows Analytics の初期設定

本章では、Upgrade Readiness と Update Compliance を Microsoft Azure から利用できるように構成します。Upgrade Readiness と Update Compliance はそれぞれ Microsoft Azure 側の操作とクライアント デバイス側での操作がありますが、次のステップで初期設定を行います。

① Log Analytics ワークスペースの作成 (4.1 節)
Microsoft Azure の Log Analytics サービスから提供される、Upgrade Readiness と Update Compliance の各サービスを利用開始する場合、Log Analytics サービスが動作するワークスペースを最初に作成する必要があります。

② ソリューションの追加 (4.2 節)
Log Analytics 用のワークスペースを作成したら、Upgrade Readiness と Update Compliance をそれぞれソリューションとして追加します。

③ Upgrade Readiness Deployment スクリプトの実行 (4.3 節)
Upgrade Readiness と Update Compliance による監視ができるようにするために各クライアント デバイスで Upgrade Readiness Deployment スクリプトを実行します。

本章では、①から③までの各ステップについて解説します。

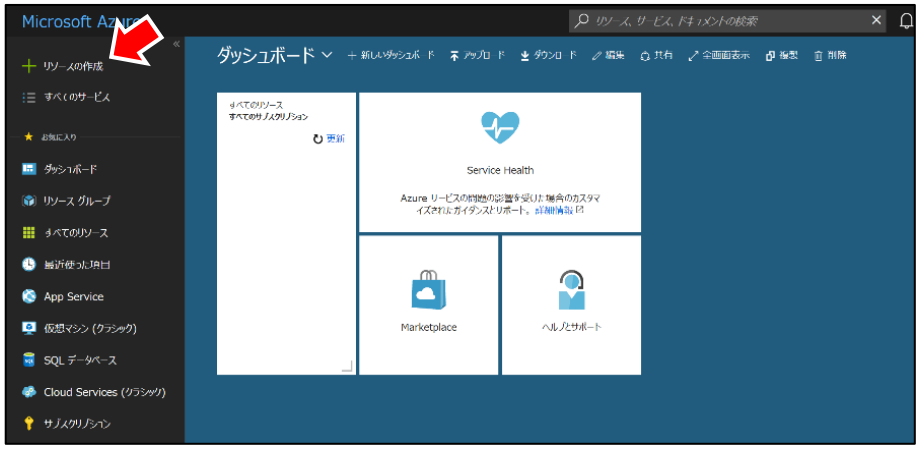
4.1 Log Analytics ワークスペースの作成

本節では、Windows Analytics を使用するための初期設定として、Microsoft Azure 管理ポータルから Log Analytics ワークスペースの作成を行います。

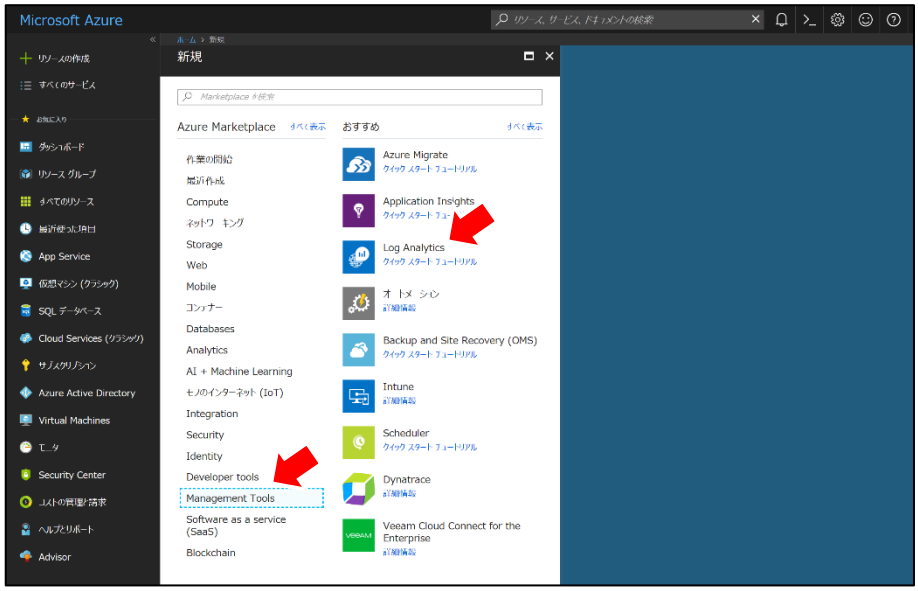
1) ブラウザー画面で、「https://portal.azure.com/」にアクセスします。

2) サインイン画面で、Microsoft Azure テナントを保有するユーザーでサインインします。

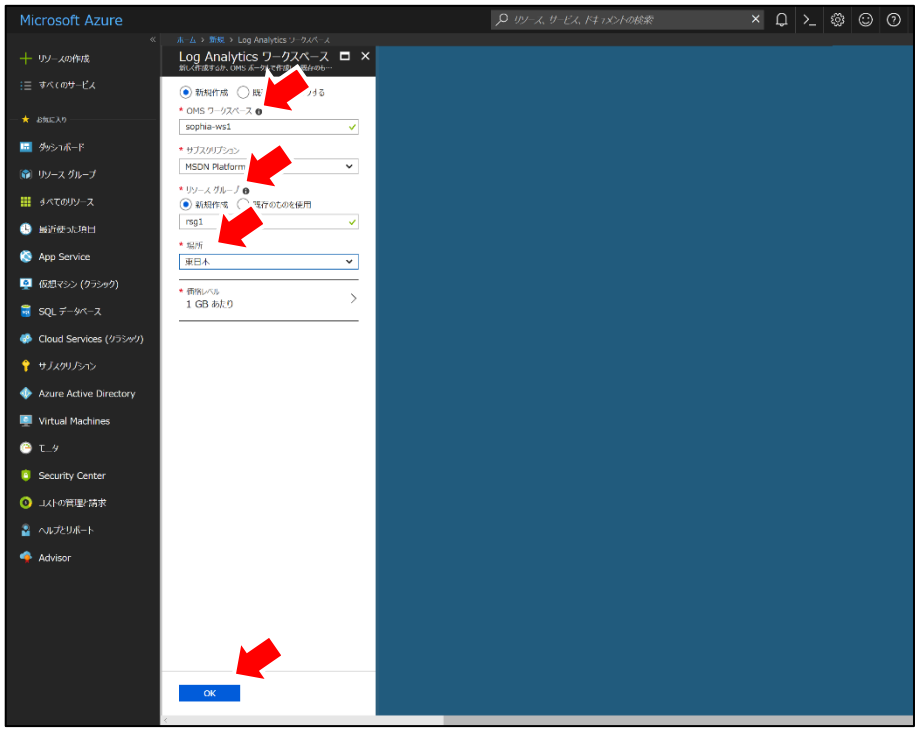
3) Microsoft Azure 画面で、左ペインの [リソースの作成] をクリックします。



4) [新規] 画面で、Azure Marketplace の一覧から [Management Tools] をクリックし、[Log Analytics] をクリックします。



5) [Log Analytics ワークスペース] 画面で、[OMS ワークスペース] 欄に任意のワークスペース名を入力し、[リソース グループ] 欄に任意のリソース グループ名を入力し、[場所] 欄から任意の場所を選択して、[OK] をクリックします。

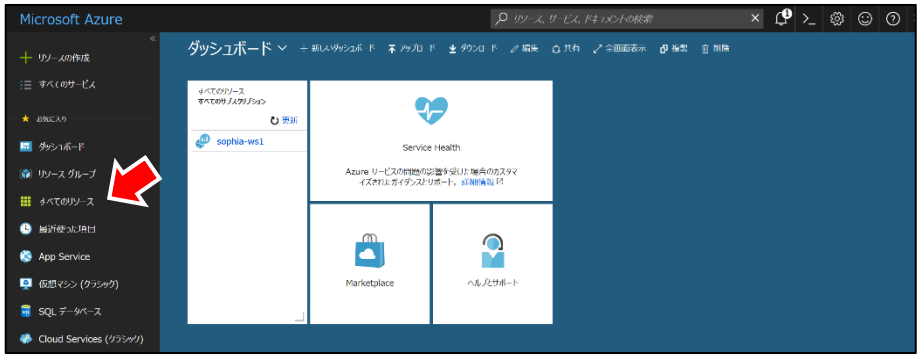


6) しばらくすると、Log Analiytics の展開が完了します。

4.2 ソリューションの追加

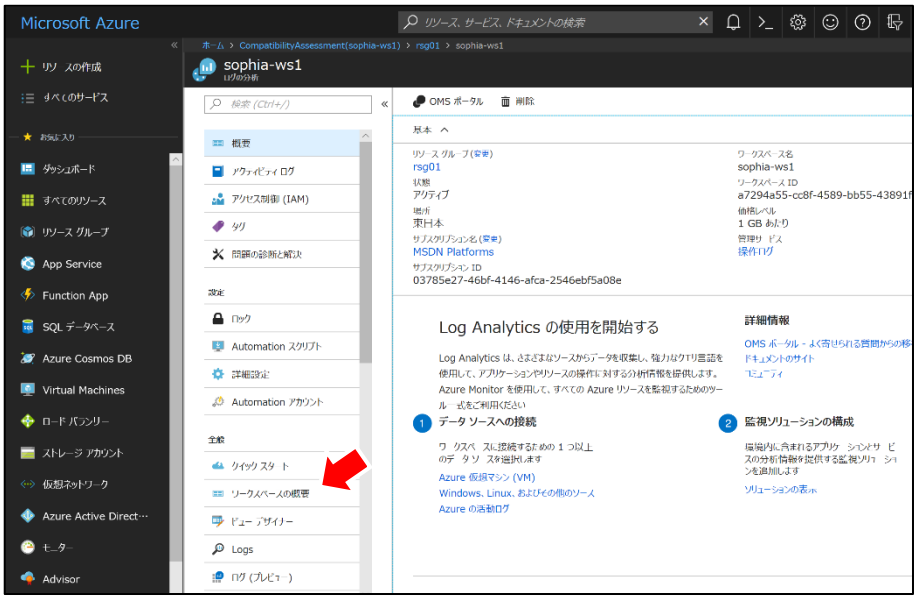
本節では、Upgrade Readiness と Update Compliance を使用するために、前の手順で作成したワークスペースに対してソリューションの追加を行います。なお、Upgrade Readiness のソリューション名は CompatibilityAssessment (追加時の名称は「Upgrade Readiness])、Update Compliance のソリューション名は WaaSUpdateInsights (追加時の名称は「更新プログラムのコンプライアンス]) という名前で表示されます。

1) Microsoft Azure 画面で、左ペインの [すべてのリソース] をクリックします。

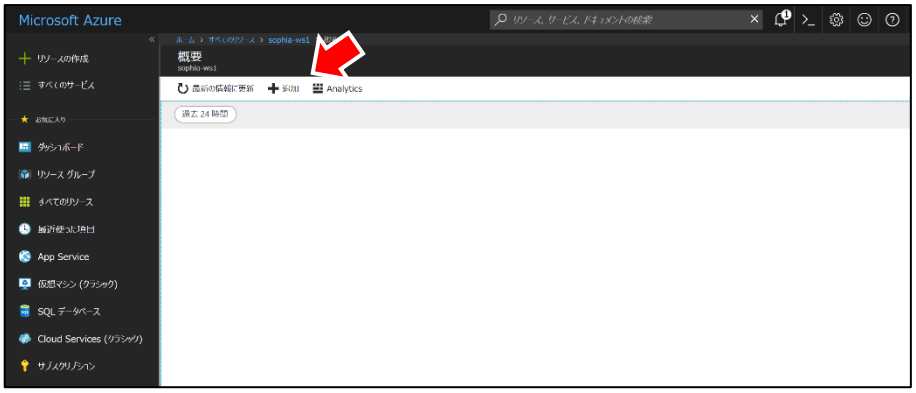


2) [すべてのリソース] 画面で、前の手順で作成したワークスペースをクリックします。作成したワークスペースの種類は、この画面で [ログの分析] という種類で表示されます。

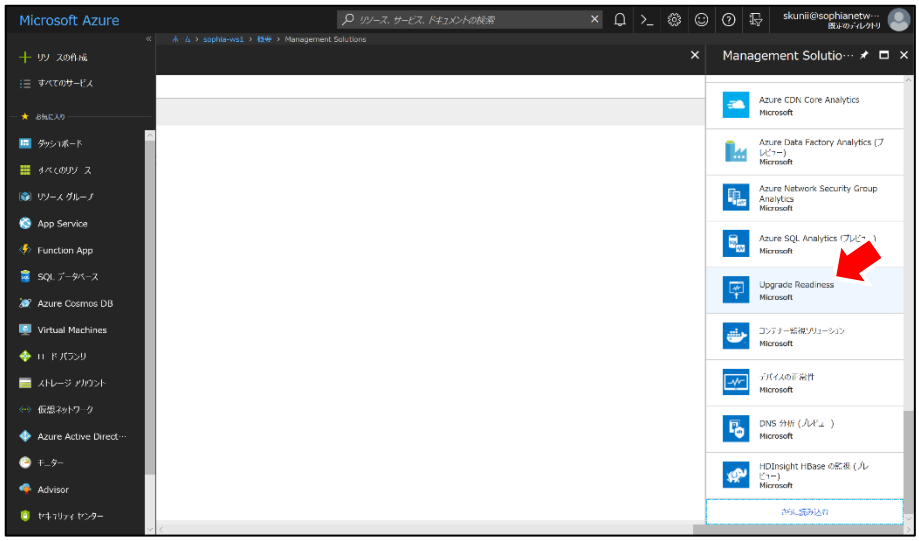
3）［ログの分析］画面で、左ペインの［ワークスペースの概要］をクリックします。



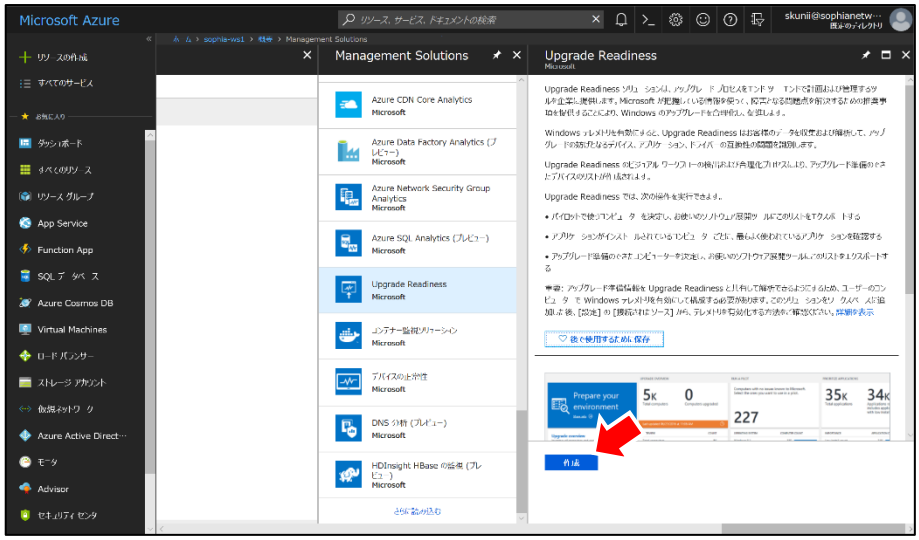
4）［概要］画面で、［追加］をクリックします。



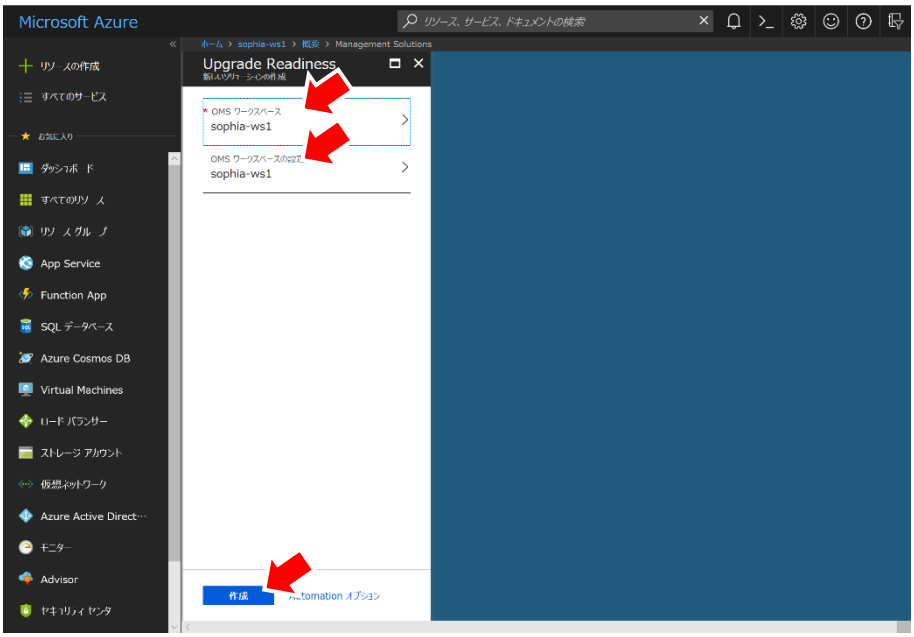
5）[Management Solutions] 画面で、[Upgrade Readiness] をクリックします。



6）[Upgrade Readiness] 画面で、[作成] をクリックします。

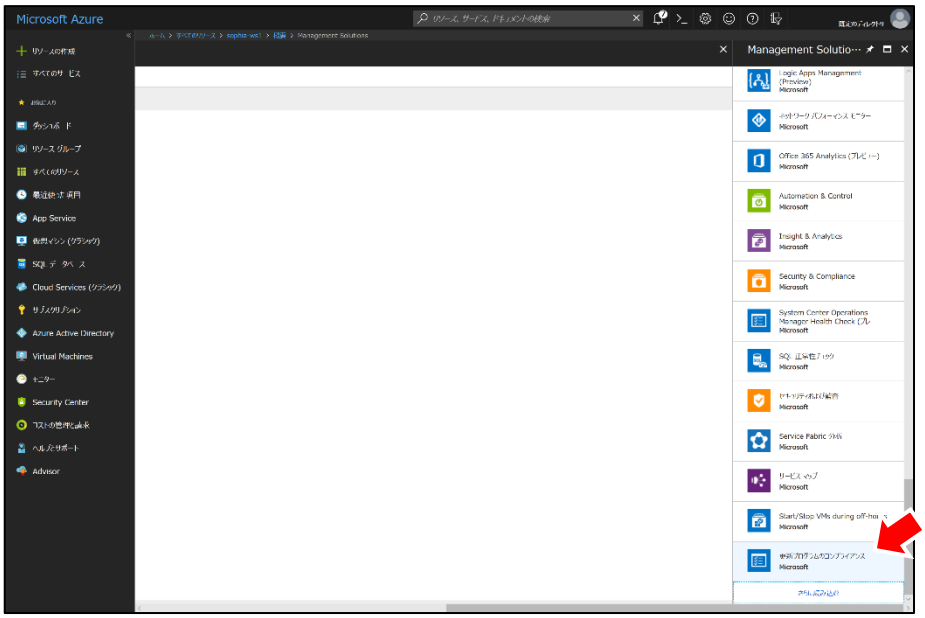


7) [Upgrade Readiness] 画面で、[OMS ワークスペース] 欄と [OMS ワークスペースの設定] 欄からそれぞれ前の手順で作成したワークスペースを選択し、[作成] をクリックします。



8) しばらくすると、ワークスペースに Upgrade Readiness ソリューションが追加されます。

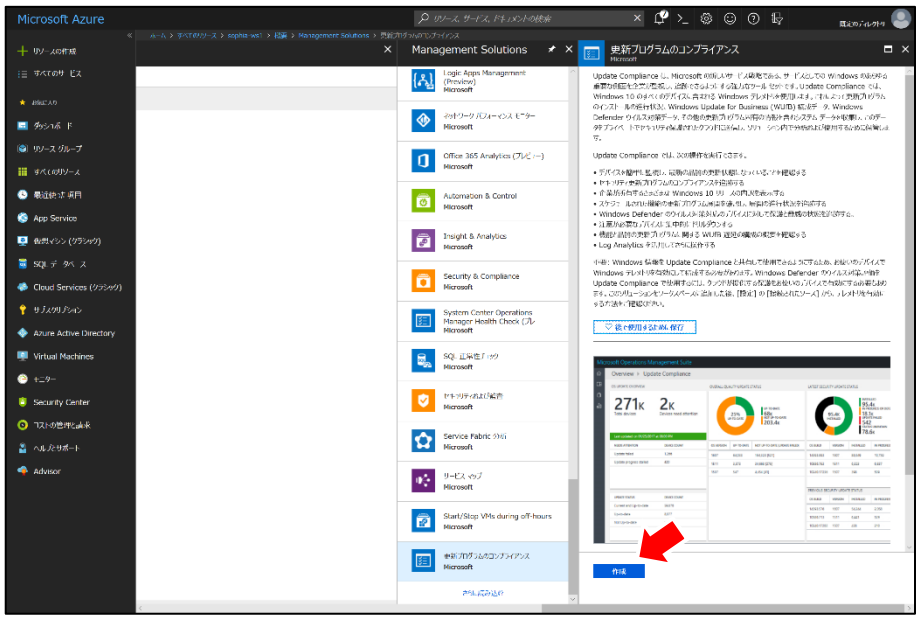
9) Azure 管理ポータル画面で、画面を左にスクロールさせ、[Management Solutions] メニューに戻り、[更新プログラムのコンプライアンス] をクリックします。



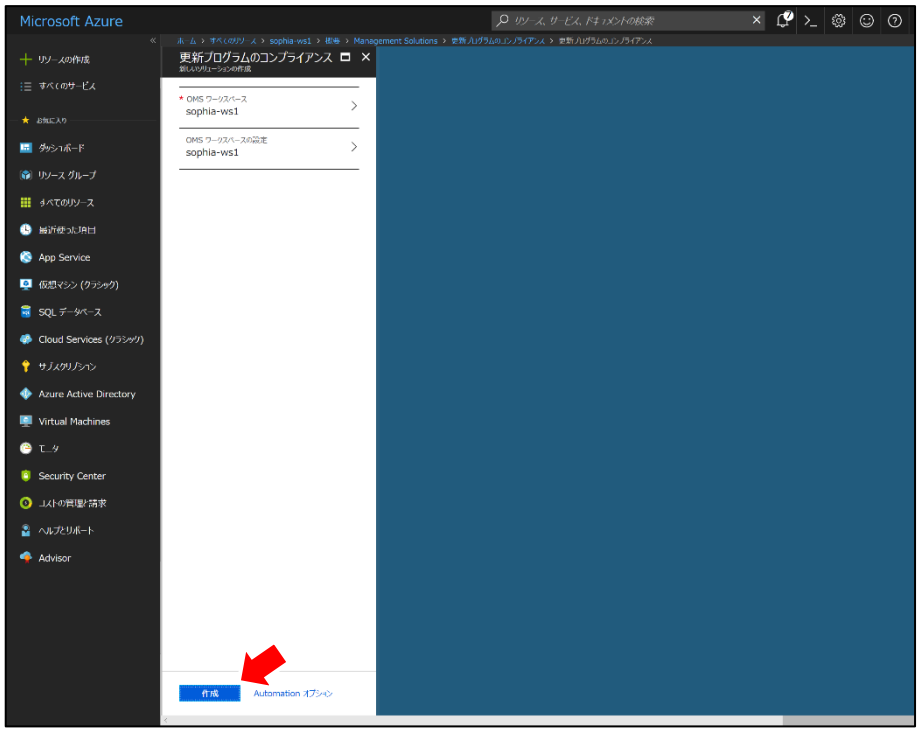
NOTE:

なお、[更新プログラムのコンプライアンス] は一覧の下の方にあるため、下にスクロールして [さらに読み込む] をクリックしないと表示されない可能性があります。

10) [更新プログラムのコンプライアンス] 画面で、[作成] をクリックします。



11)[更新プログラムのコンプライアンス] 画面で、[OMS ワークスペース] と [OMS ワークスペースの設定] 欄に、前の手順で作成したワークスペースが選択されていることを確認し、[作成] をクリックします。



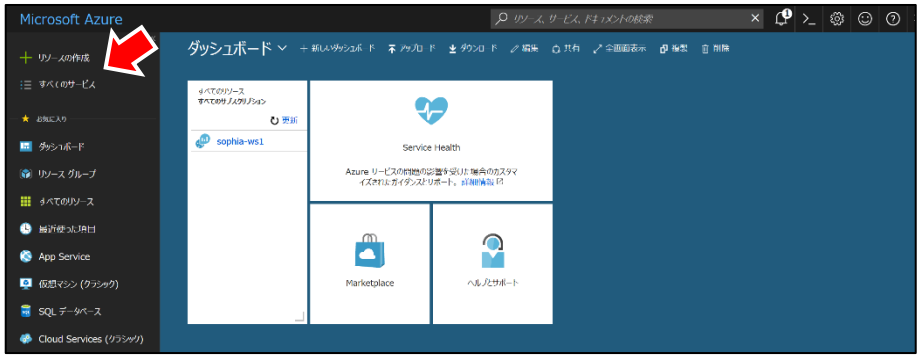
12)しばらくすると、ワークスペースに Update Compliance ソリューションが追加されます。

13)Azure 管理ポータル画面で、画面を左にスクロールさせ、[概要] メニューに戻り、[最新の情報に更新] をクリックすると、[Upgrade Readiness] と [Update Compliance] が表示されることを確認します。

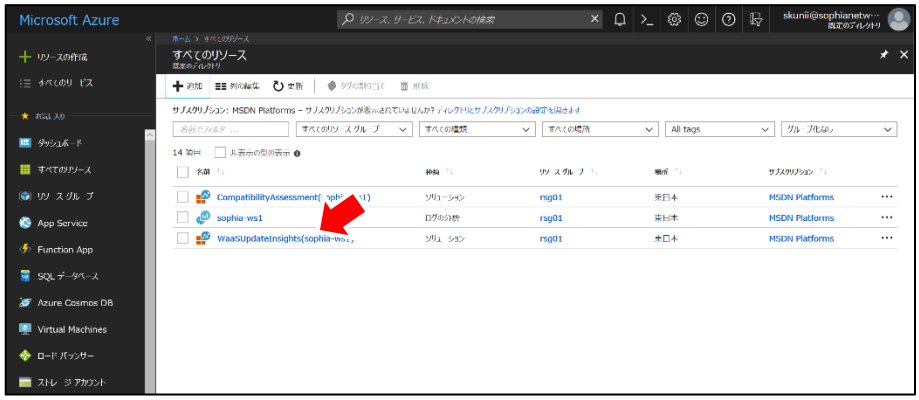
4.3 Upgrade Readiness Deployment スクリプトの実行

本節では管理対象となる、すべてのコンピューターに対して Update Compliance から提供されるスクリプトを実行し、接続先となるテナントの指定を行います。Upgrade Readiness Deployment スクリプトを実行することによって、Upgrade Readiness と Update Compliance の両方で必要となる情報をテレメトリから利用できるようになります。なお、手順では Windows 10 コンピューターに設定する方法を解説しますが、Windows 8.1 や Windows 7 コンピューターに対しても同様の手順で設定することができます。

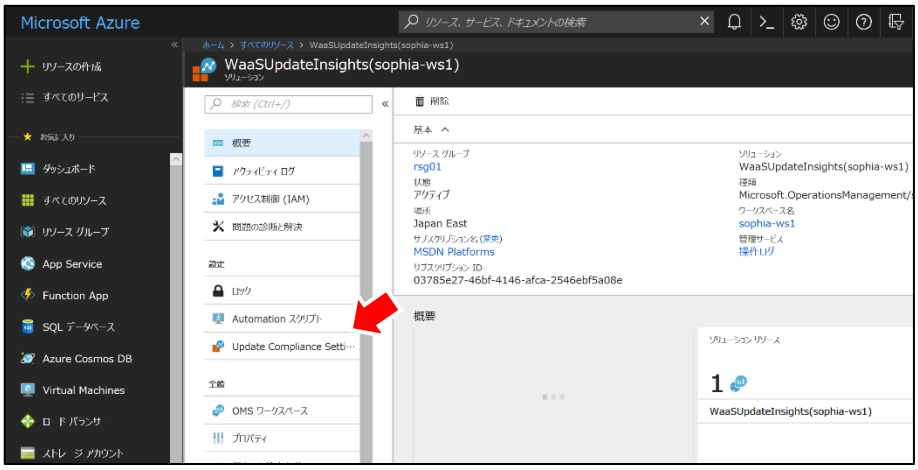
1) Microsoft Azure 画面で、左ペインの [すべてのリソース] をクリックします。



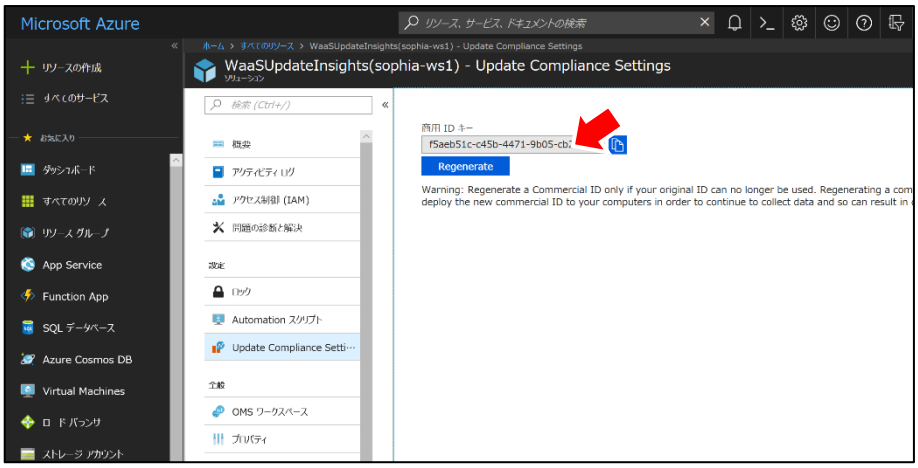
2) [すべてのリソース] 画面で、[WaaSUpdateInghts～] で始まるソリューションをクリックします。



3) [WaaSUpdateInghts] 画面で、左ペインの [Update Compliance Settings] をクリックします。

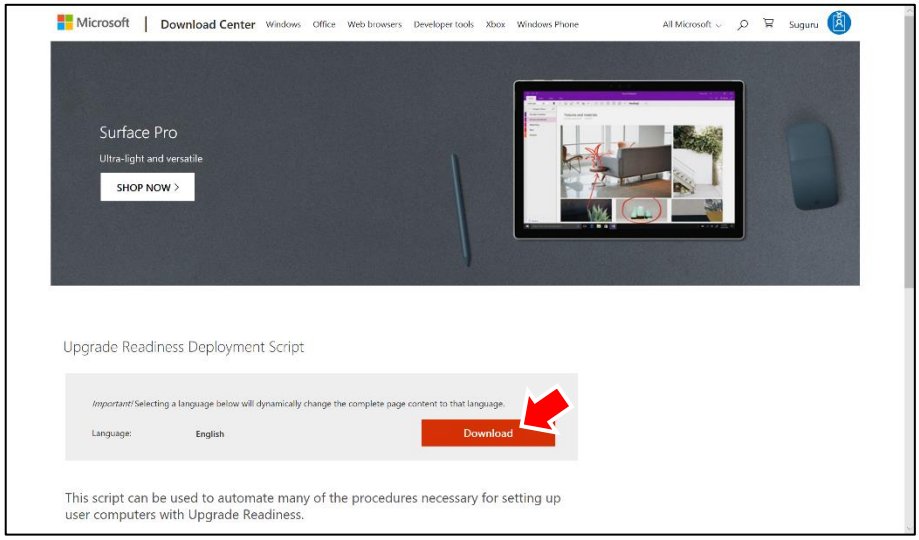


4) [Update Compliance Settings] 画面で、[商用 ID キー] 欄に表示されているキーをコピーしておきます。

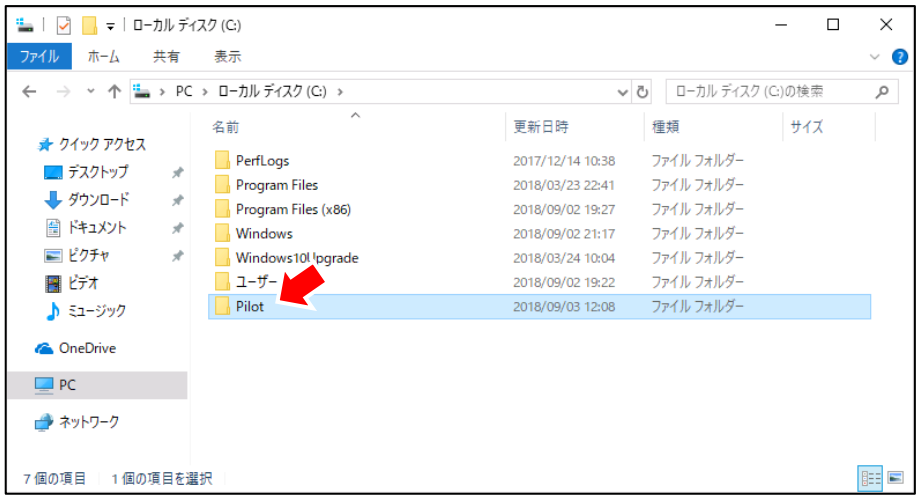


5) ブラウザー画面で、新しいタブを開き、URL として「https://www.microsoft.com/en-us/download/details.aspx?id=53327」にアクセスします。

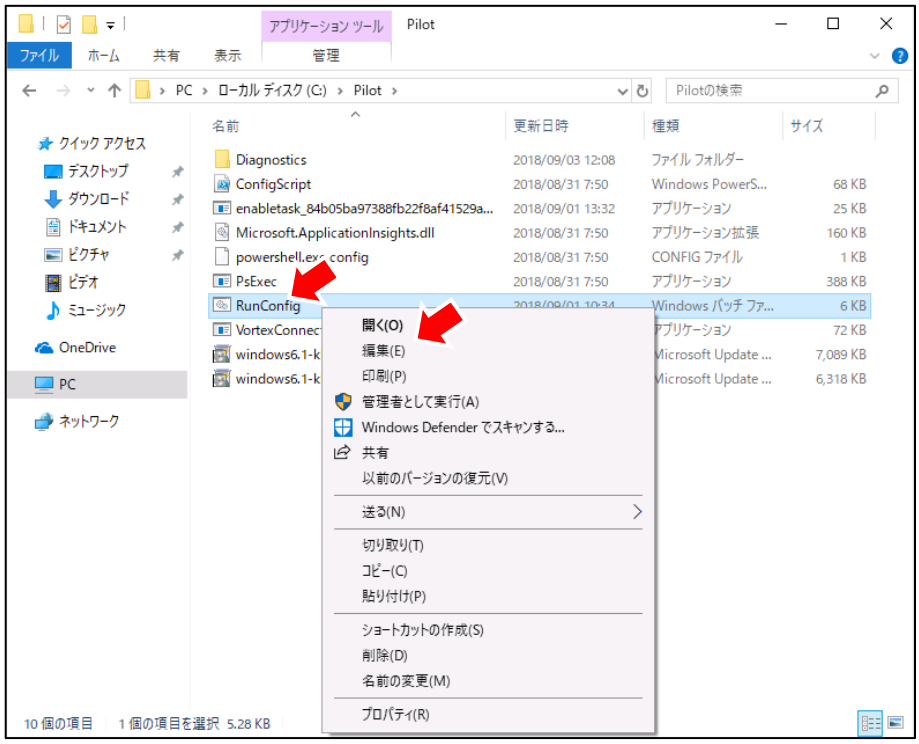
6) ブラウザー画面で、[Download] をクリックし、ダウンロード フォルダーにファイルをダウンロードします。



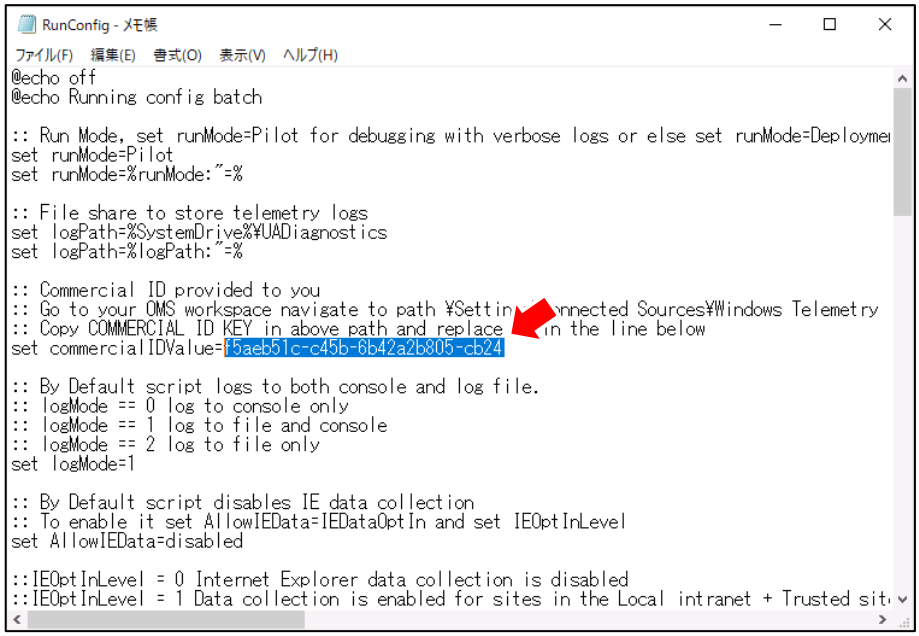
7) Windows エクスプローラー画面で、ダウンロードした zip ファイルのうち、zip ファイル内の Pilot フォルダーを c:¥ フォルダーに解凍します。



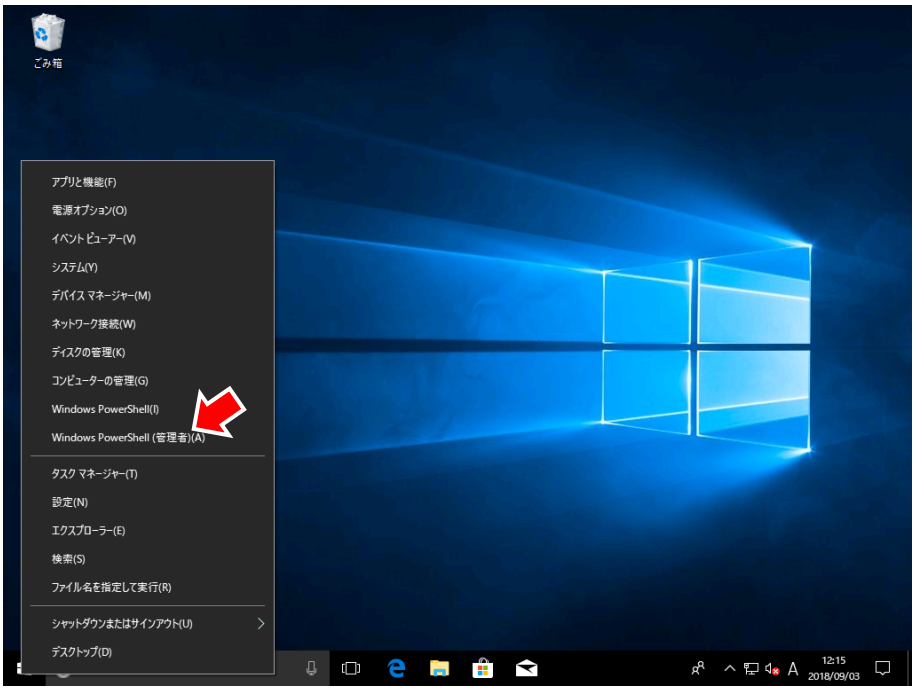
8) Windows エクスプローラー画面で、C:¥Pilot フォルダーを開き、RunConfig.bat ファイルを右クリックし、[編集] をクリックします。



9) メモ帳画面で、「set commercialIDValue=」で始まる行の=以降の部分に前の手順でコピーした商用 ID 番号を張り付け、上書き保存します。

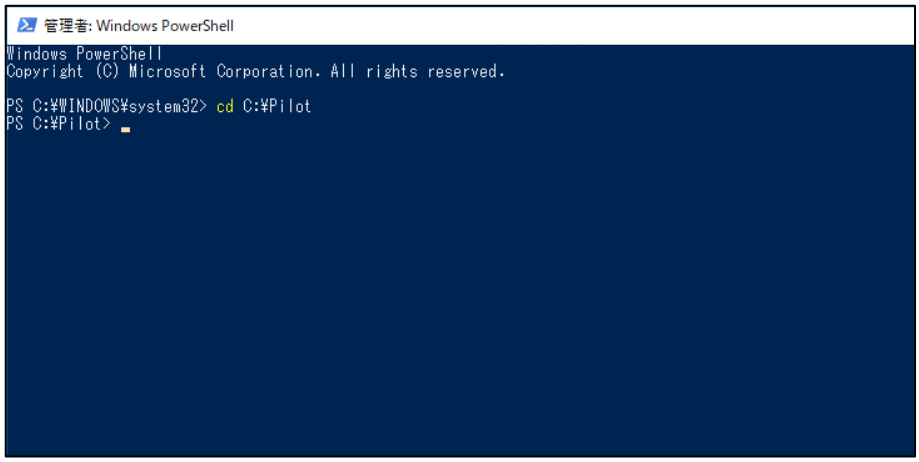


10)スタートボタンを右クリックし、[Windows PowerShell (管理者)] をクリックします。

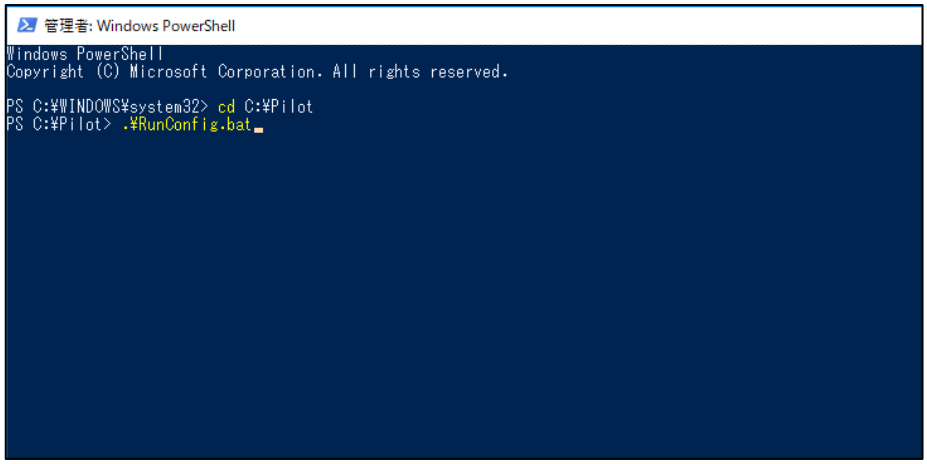


11)[ユーザー アカウント制御] 画面で、[はい] をクリックします。

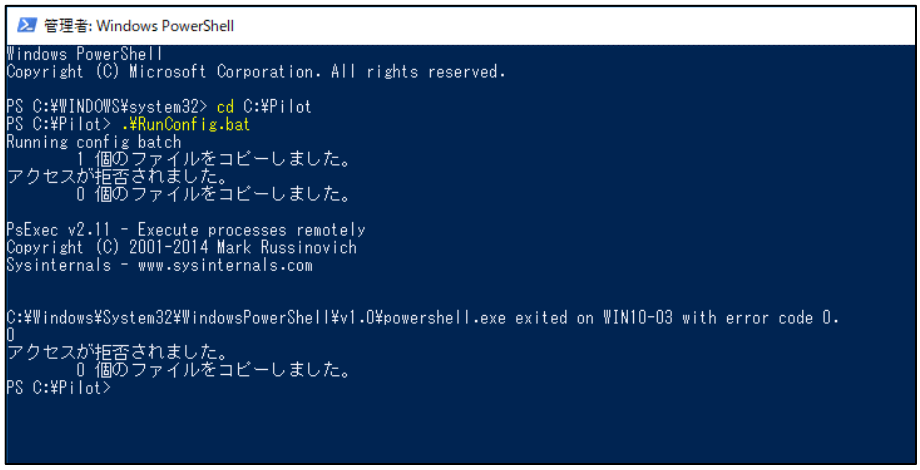
12)[Windows PowerShell] 画面で、「cd C:¥Pilot」と入力し、Enter キーを押します。



13)[Windows PowerShell] 画面で、「.¥RunConfig.bat」と入力し、Enter キーを押します。



14)[Windows PowerShell] 画面で、スクリプトの実行結果として error code 0 と表示されることを確認します。



NOTE:

error code が 0 以外で表示される場合、スクリプトの実行に失敗している可能性があります。それぞれのエラーコードに対応するトラブルの原因については、マイクロソフトの Web サイト「Upgrade Readiness deployment script」を参考にしてください。

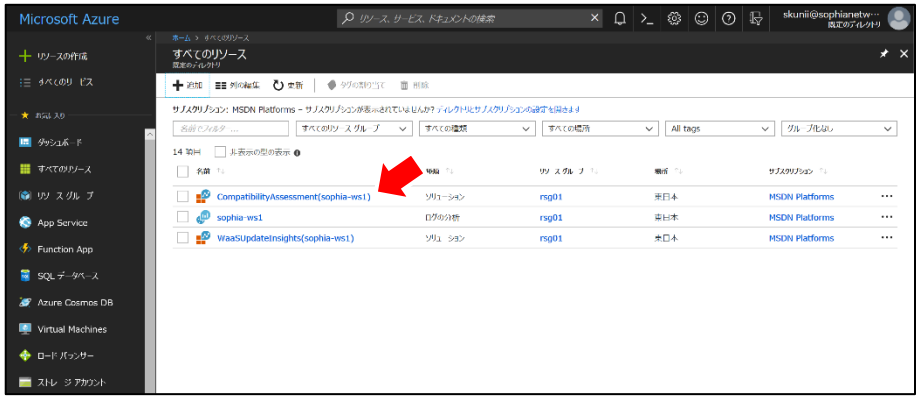
■Upgrade Readiness deployment script

https://docs.microsoft.com/en-us/windows/deployment/upgrade/upgrade-readiness-deployment-script

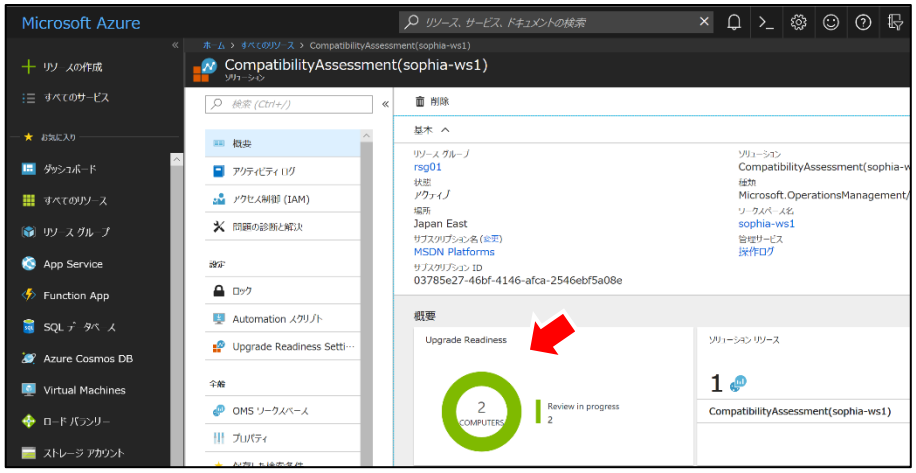
15)スクリプトの実行結果を確認します。

Microsoft Azure 画面で、左ペインの [すべてのリソース] をクリックします。

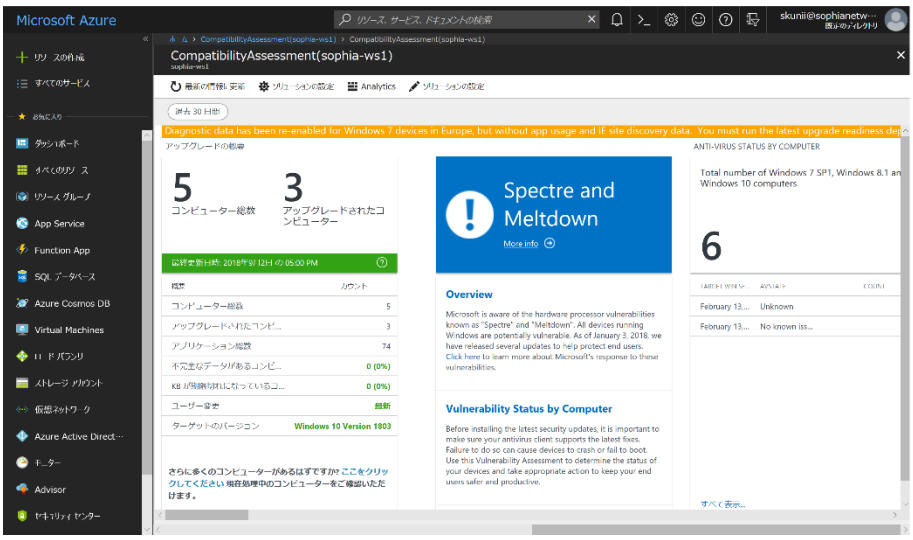
16)[すべてのリソース] 画面で、[CompatilityAssessment～] で始まるソリューションをクリックします。



17)[CompatilityAssessment] 画面で、[Upgrade Readiness] のエリアをクリックします。

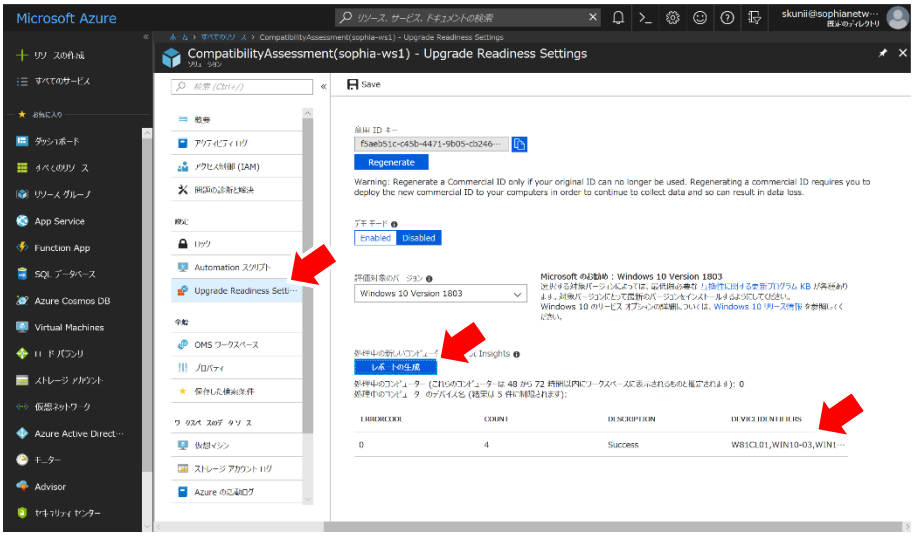


18)[CompatilityAssessment] 画面で、クライアント デバイスからアップロードされた情報が参照できることを確認します。



NOTE:

スクリプトが実行されてから、画面に表示されるまでに最大で 48 時間程度要する場合があります。スクリプト実行によるソリューションへの登録状況については手順 17 の画面で左ペインの [Upgrade Readiness Settings] をクリックし、[レポートの生成] ボタンをクリックすると確認できます。

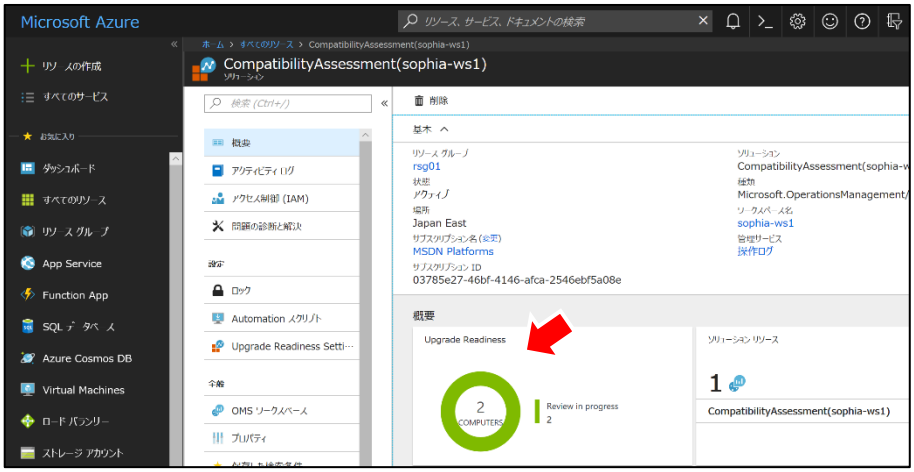


5　Upgrade Readiness による現状分析

本章では、Microsoft Azure から Upgrade Readiness が利用できるようになった状態から、参照可能なダッシュボード（レポート）の内容とその見かたについて解説します。

Azure 管理ポータル画面上で、CompatibilityAssessment のソリューション名称で提供される Upgrade Readiness は、Azure 管理ポータル画面のソリューションを作成したリソースグループから CompatibilityAssessment ソリューションにアクセスし、画面 5-1 の Upgrade Readiness のエリアをクリックすることで、画面 5-2 のようなダッシュボード画面を参照できます。

画面 5-1 Azure 管理コンソールの CompatibilityAssessment ソリューション



画面 5-2 Azure 管理コンソールの Upgrade Readiness 項目

私たちがアップグレードの作業を行う際、アップグレードのための準備、先行して展開するデバイスの決定とその展開（パイロット展開）、問題がなければ残りのデバイスへの展開（ブロード展開）、の順の作業が一般的な手順になります。パイロット展開とブロード展開では、それぞれのデバイスをどのタイミングで展開するかについて、Upgrade Readiness の中ではデバイスをグループ化し、管理することができます（「5.5 ステップ 3：展開」を参照）。

図 5-1 一般的なアップグレード ステップ

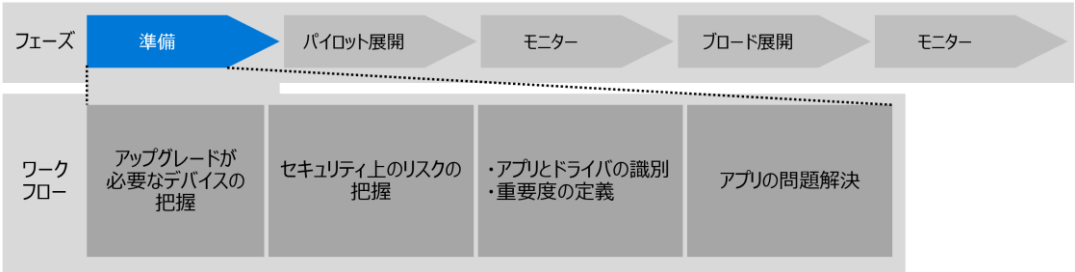
また、パイロット展開とブロード展開では、展開が成功したかについての確認も大事な作業です。Upgrade Readiness の中では［モニター］の項目でその結果について追跡します（「5.6 モニター」を参照）。

図 5-2 一般的なアップグレード ステップとその監視

一方、準備段階では各種展開が成功するように問題点を把握し、解決するため、次のような作業が一般的に行われます。そして、Upgrade Readiness では、それぞれの作業に対応した監視が行えるようになっています。

- ✓ アップグレードが必要なデバイスの把握（「5.1 アップグレードの概要」を参照）
- ✓ セキュリティ上のリスクの把握（「5.2 Spectre と Meltdown」を参照）
- ✓ アプリとドライバーの識別/重要度の定義（「5.3 ステップ 1：重要なアプリを識別する」を参照）
- ✓ アプリの問題解決（「5.4 ステップ 2：問題を解決する」）

図 5-3 準備フェーズにおける具体的な作業



以上のように、Upgrade Readiness ではアップグレードの展開に欠かせない、チェック項目が用意されており、それぞれの項目を順番に確認することで適切な展開とその準備が行えます。次節からは、Upgrade Readiness に記録される、各項目について解説します。

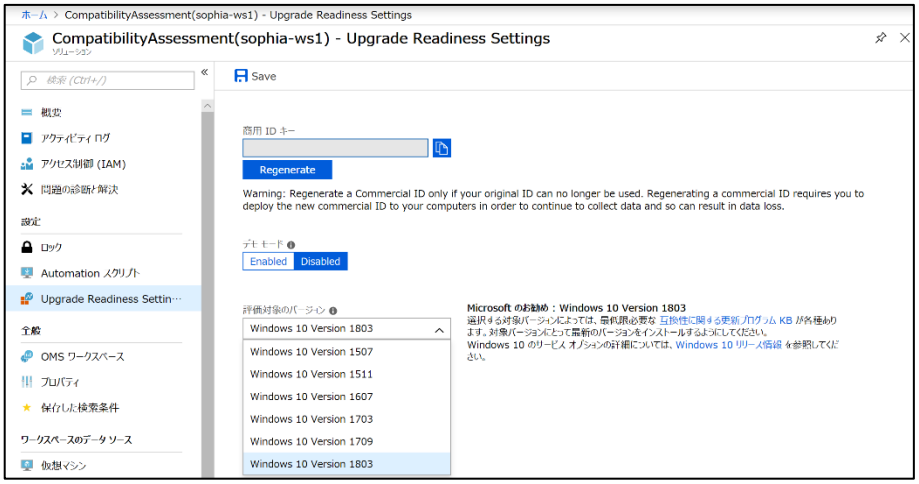
5.1 アップグレードの概要

Upgrade Readiness のダッシュボード左側に表示される [アップグレードの概要] 項目は、スクリプトが実行され、情報が収集されたコンピューターの総数と、画面では [アップグレードされたコンピューター] と表示される、Windows 10 がインストールされたコンピューターの総数をそれぞれ参照できます。

画面 5.1-1 [アップグレードの概要] 項目

なお、Windows 10 がインストールされたコンピューターのうち、[アップグレードされたコンピューター] にカウントされるには、対象のバージョン（1803, 1709 などのバージョン）の Windows 10 がインストールされている必要があります。対象のバージョンの設定については、ダッシュボード画面内の [ソリューションの設定] をクリックし、続く画面で [Upgrade Readiness Settings] をクリックすることで、[評価対象のバージョン] から定義できます。

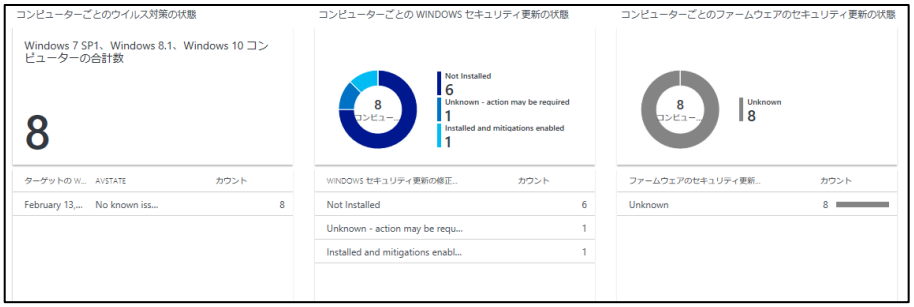
画面 5.1-2 [評価対象のバージョン] 項目



5.2 Spectre と Meltdown

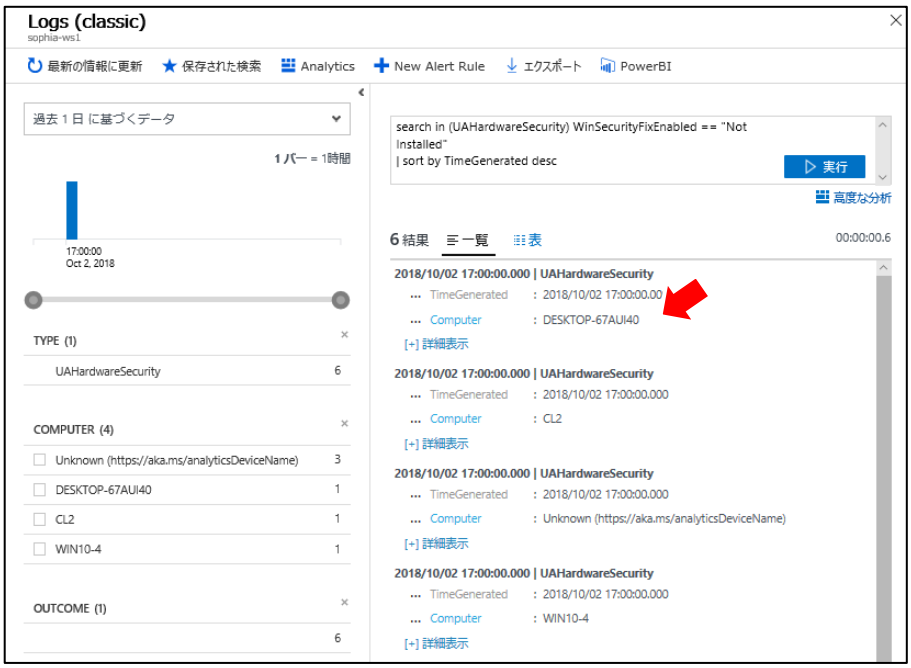
Windows 10 へのアップグレードを行う場合、セキュリティ上の問題がないことを事前に確認しておくことは非常に重要なポイントとなります。
Upgrade Readiness 項目内に表示される [Spectre と Meltdown] 項目は、Windows Defender ウイルス対策による保護対象となっているコンピューターの総数と、セキュリティ更新プログラムのインストール状況、ファームウェアのセキュリティ更新プログラムのインストール状況をそれぞれ参照できます。これらの情報を参照することにより、アップグレード対象のコンピューターがセキュリティ上の問題がないことを確認できます。

画面 5.2-1 [Spectre と Meltdown] 項目



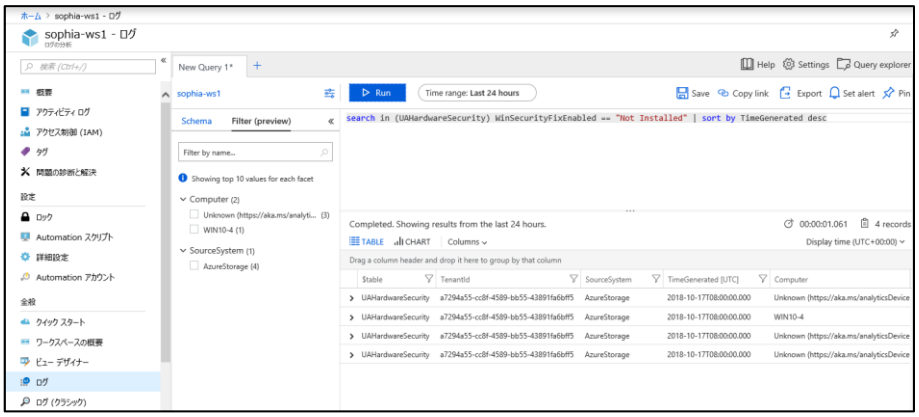
Windows Analytics で参照可能な項目は、すべて Log Analytics サービスを通じて収集したものであり、収集したデータに対してクエリを実行して一部の情報を抽出したものです。そのため、ダッシュボードで表示される、個々の内容をクリックすると、ダッシュボードに表示されている内容に対応する Log Analytics のクエリ結果が表示され、該当するコンピューターの名前が確認できます (画面 5.2-2)。

画面 5.2-2 [コンピューターごとの Windows セキュリティ更新の状態] 項目をクリックすると、該当するコンピューター名が確認できる



NOTE:

本稿執筆時点 (2018 年 10 月) では、画面 5.2-1 からの操作によって Logs (classic) にアクセスすることになりますが、将来的に [ログの分析] リソースの [ログ] 項目のユーザーインターフェイスに切り替わる予定です。



5.3 ステップ 1： 重要なアプリを識別する

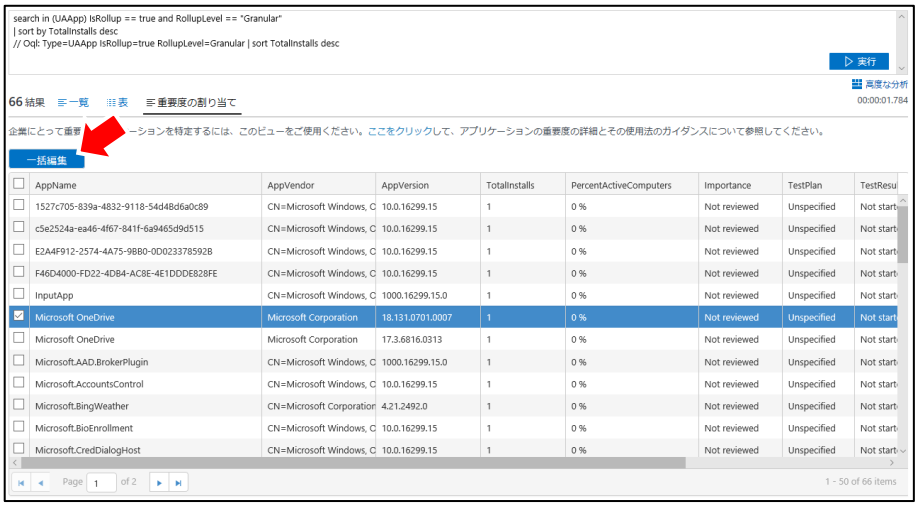
Windows 10 へのアップグレードを行うための最初のステップとしてチェックする項目に、組織で使用しているアプリの識別があります。

Upgrade Readiness 項目内に表示される [重要なアプリを識別する] 項目は、スクリプトが実行されたコンピューターにインストールされているアプリの一覧を表示します。このとき、個々のアプリに対して重要度やテストのステータスなどを設定し、アプリを分類することができます。これにより、アップグレードに際して互換性テストを行う必要のあるアプリの識別や、テスト結果の情報共有などに利用できます。

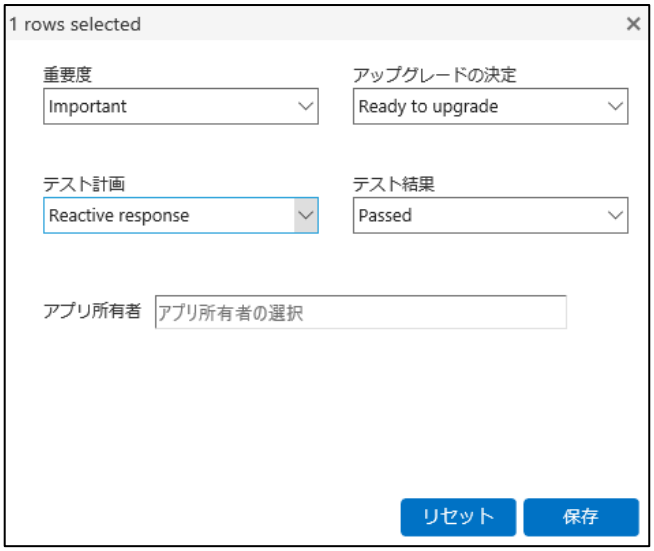
画面 5.3-1 [ステップ 1:重要なアプリを識別する] 項目

画面 5.3-1 のように、エージェントから収集された、すべてのアプリは Not reviewed と分類されます。画面下部の [重要度の割り当て] をクリックすると、画面 5.3-2 のようにアプリ一覧が表示されるため、[一括編集] をクリックして、アプリの重要度 (Importance)、テストの方法 (TestPlan)、テストの結果 (TestResult) などを画面 5.3.-3 から変更できます。

画面 5.3-2 アプリ一覧画面



画面 5.3-3 アプリの分類設定の変更画面



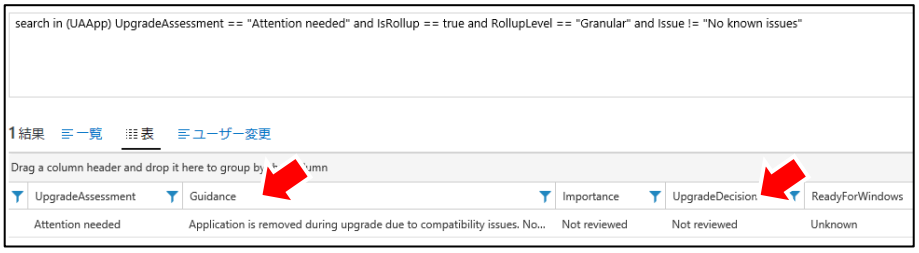
5.4 ステップ 2： 問題を解決する

ステップ 1 で識別したアプリに対して、互換性の問題がないか確認し、その結果を確認できる項目が [問題を解決する] 項目です。この項目では、既知の問題のあるアプリやデバイスドライバーの一覧や、そのアプリやドライバーに対する優先度を参照することができます。

画面 5.4-1 [ステップ 2:問題を解決する] 項目

画面 5.4-1 の項目のうち、[既知の問題のあるアプリケーションのレビュー] 項目と [既知のドライバーの問題のレビュー] 項目については、既知のアプリの問題またはドライバーの問題を表示します。個々の項目をクリックすると、問題の詳細を確認できます (画面 5.4-2)。

画面 5.4-2 [既知の問題のあるアプリケーションのレビュー] 項目の詳細

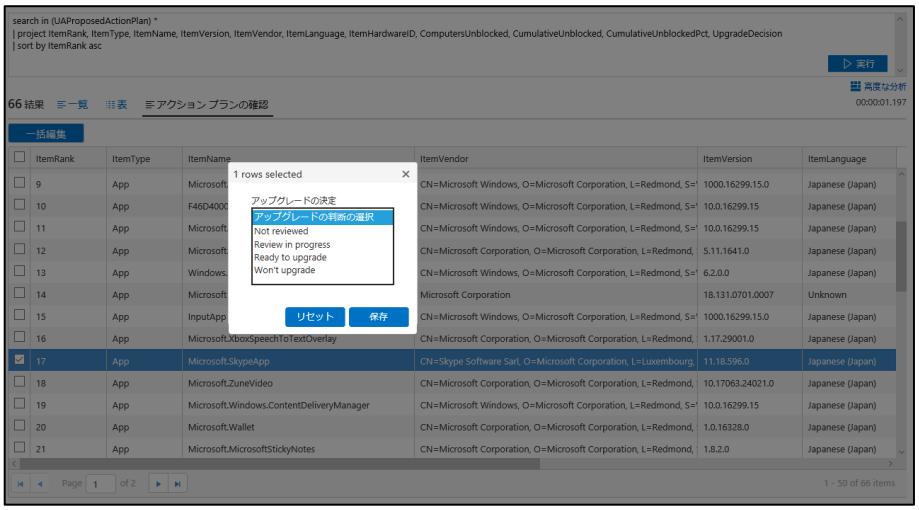


画面 5.4-2 の [Guidance] 項目に問題の原因が書かれているため、この内容を参照し、アップグレードの判断を行います。もし、問題があってもアップグレードに影響はないと判断した場合には、[Upgrade decision] 項目を書き換えておくことができます。

画面 5.4-3 [ステップ 2:問題を解決する] 項目 (続き)

一方、画面 5.4-1 を右にスクロールすると表示される、画面 5.4-3 では [危険度 - 低のアプリとドライバーのレビュー] 項目と [アプリとドライバーのテストの優先順位を付ける] 項目があります。[危険度 - 低のアプリとドライバーのレビュー] 項目では、デバイスから収集されたアプリ/ドライバーのうち、追加情報としてマイクロソフトから提供されている情報を一覧で確認できます。
[アプリとドライバーのテストの優先順位を付ける] 項目は、エージェントから収集されたアプリをリスト化した項目で、[テスト対象のアイテムの一覧を順番に表示] リンクをクリックすると、OS アップグレードによる各アプリの移行をさせても問題ないかについて、最終的な判断結果を書き込んでおくことができます (画面 5.4-4)。

画面 5.4-4 [アプリとドライバーのテストの優先順位を付ける] 編集画面



5.5 ステップ 3： 展開

ここまで登場した Upgrade Readiness の項目の問題をクリアし、アップグレード可能な状態にあるか？について識別する項目が [展開] です。

画面 5.5-1 [ステップ 3:展開] 項目

[展開] 項目内の [条件に適合するコンピューターを展開] 項目では、ステップ 1 とステップ 2 で登場した、すべてのアプリとドライバーのテストが完了したか？問題が解消されたか？について確認することができます。[条件に適合するコンピューターを展開] 項目では、以下のステータスでコンピューター内のアプリとドライバーへの対応状況が確認できます。

表 5.5-2 [条件に適合するコンピューターを展開] 項目のステータス

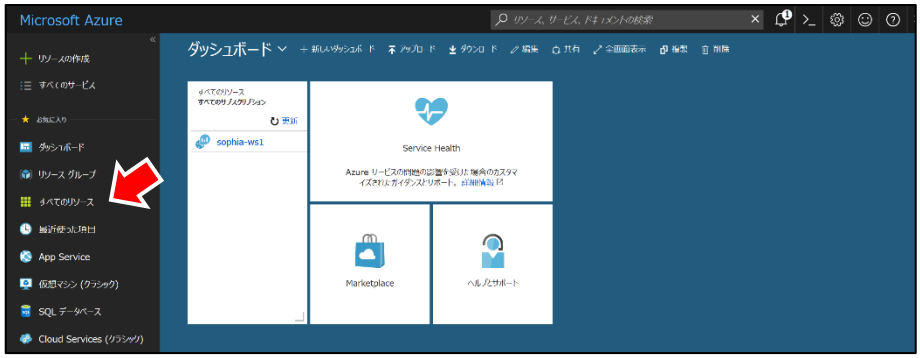
Ready to upgrade	ステップ 1 とステップ 2 で、すべてのアプリとドライバーに対してアップグレード可能な状態であることを指定した場合に表示されるステータス。明確にアップグレードが可能な状態。
Review in progress	ステップ 1 とステップ 2 で、1 つ以上のアプリとドライバーに対して対応をまだ行っていない場合に表示されるステータス。この場合、ステップ 1 またはステップ 2 の見直しが必要。
Won't upgrade	ステップ 1 とステップ 2 で、1 つ以上のアプリとドライバーに対して [Won't upgrade] を選択した場合に表示されるステータス。ステップ 1 またはステップ 2 でアップグレードしないと管理者が宣言しているため、これに該当するデバイスへのアップグレードは行うべきではない。

一方、[グループごとにコンピューターを展開する] 項目では、管理者定義でコンピューターを分類し、分類した内容に沿ってコンピューターの総数などを確認するときに利用できます。グループの作成とグループの分類設定は、OMS ワークスペース画面から行います。具体的な設定方法については、次の節で解説します。

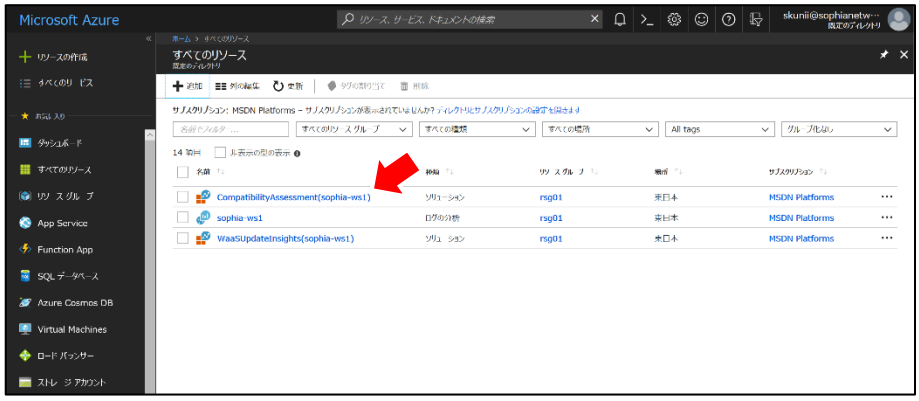
5.5.1 コンピューター グループの作成

本節では Upgrade Readiness の [ステップ 3:展開] 項目からコンピューター グループを使って展開の最終判断ができるよう、コンピューター グループを作成します。ここでは、例として Windows 8.1 コンピューターが含まれるコンピューター グループを作成します。

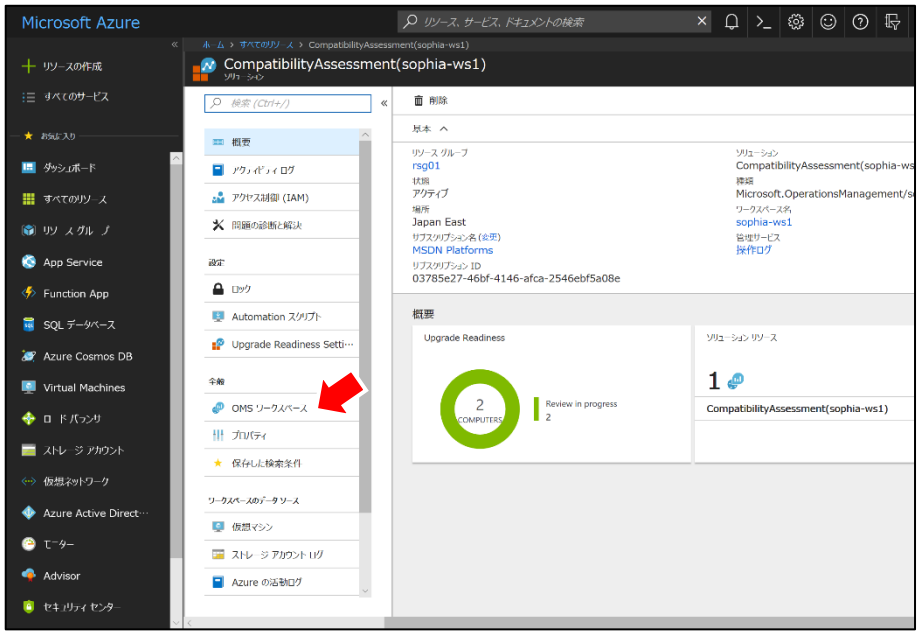
1) Microsoft Azure 画面で、左ペインの [すべてのリソース] をクリックします。



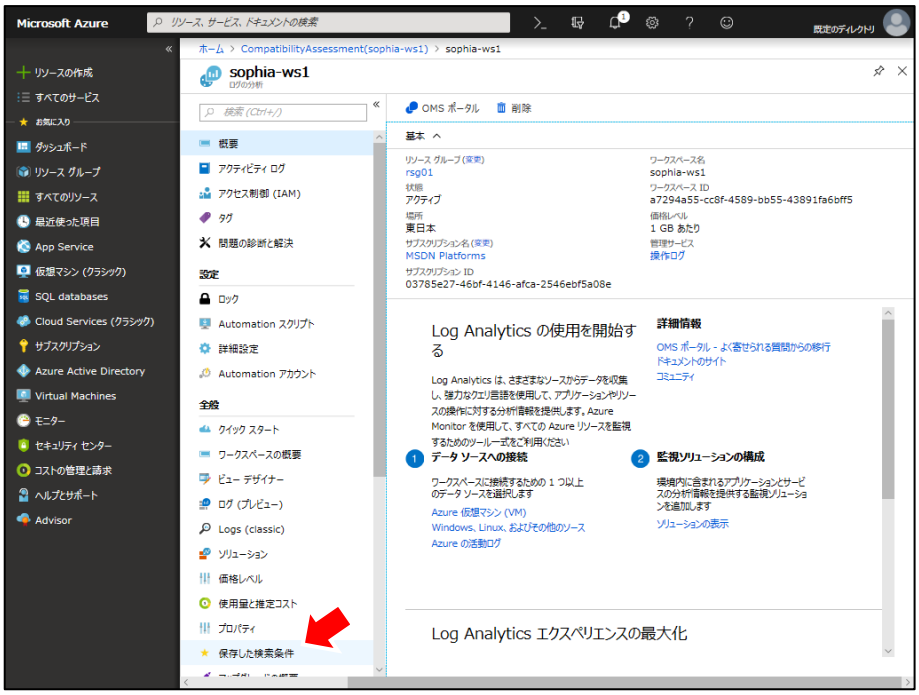
2) [すべてのリソース] 画面で、[CompatilityAssessment～] で始まるソリューションをクリックします。



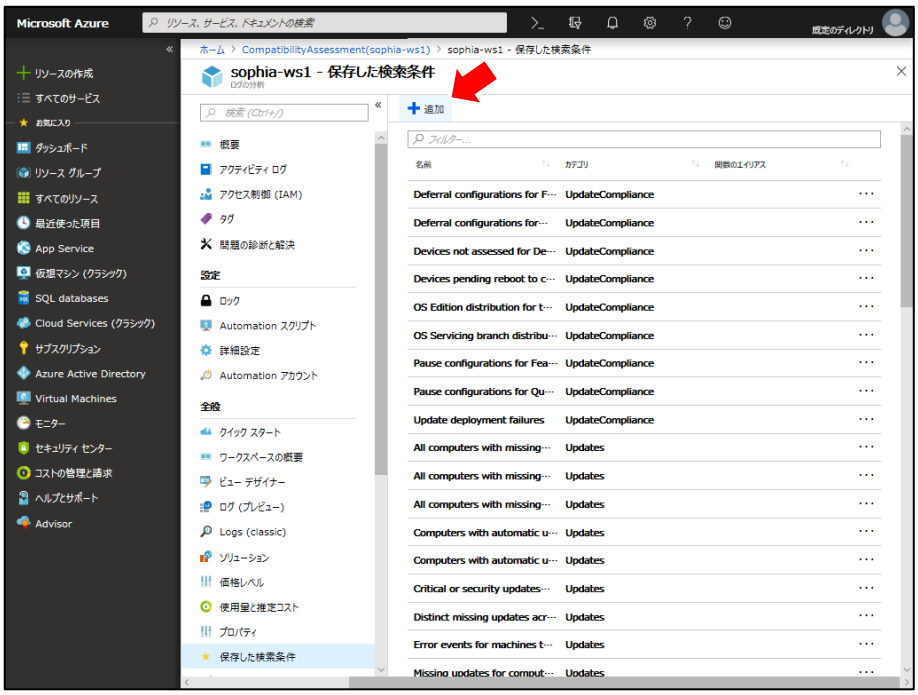
3）[CompatilityAssessment] 画面で、左ペインの [OMS ワークスペース] をクリックします。



4）[<ワークスペース名>] 画面で、[保存した検索条件] をクリックする。



5) [保存した検索条件] 画面で、[追加] をクリックする。



6) [保存した検索条件の追加] 画面で、以下のように入力し、[OK]をクリックする。

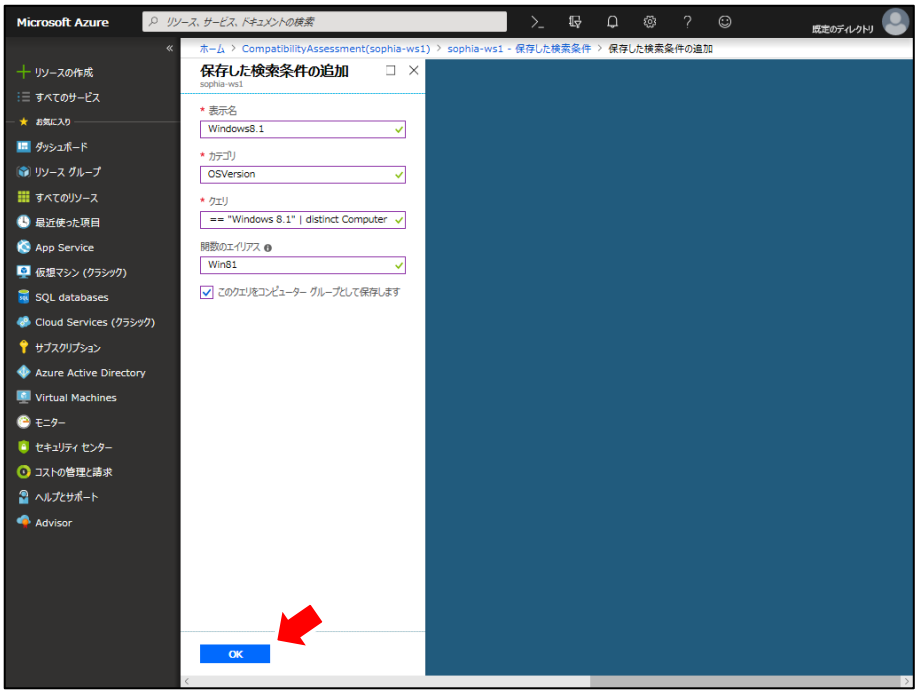
■表示名：Windows8.1

■カテゴリ：OSVersion

■クエリ：search in (UAComputer) OSVersion == "Windows 8.1" | distinct Computer

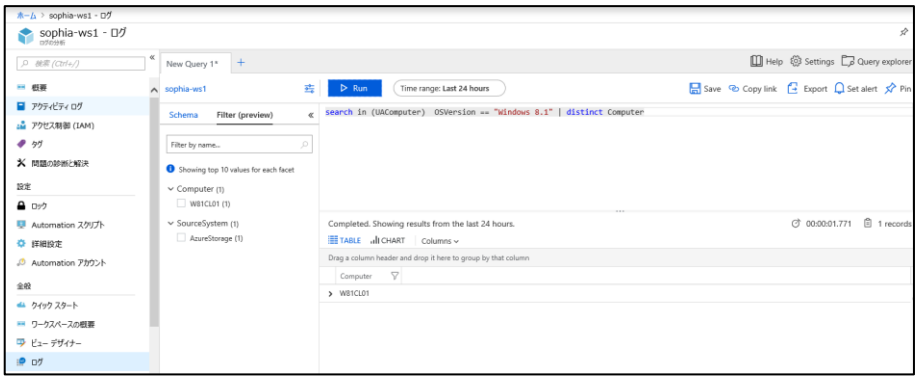
■関数のエイリアス：Win81

■このクエリをコンピューター グループとして保存します：オン

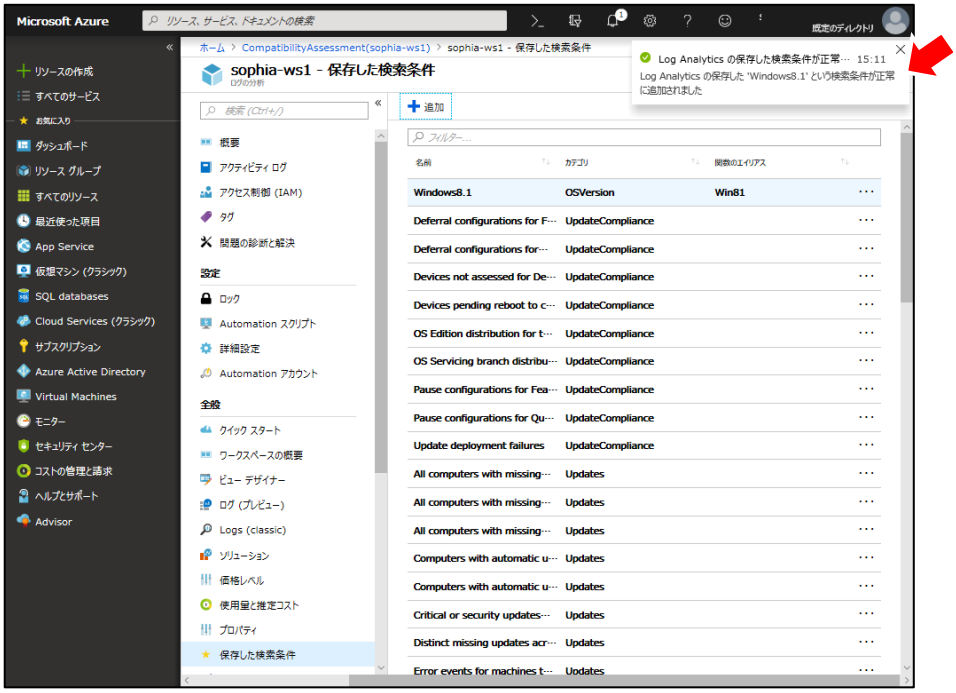


NOTE:

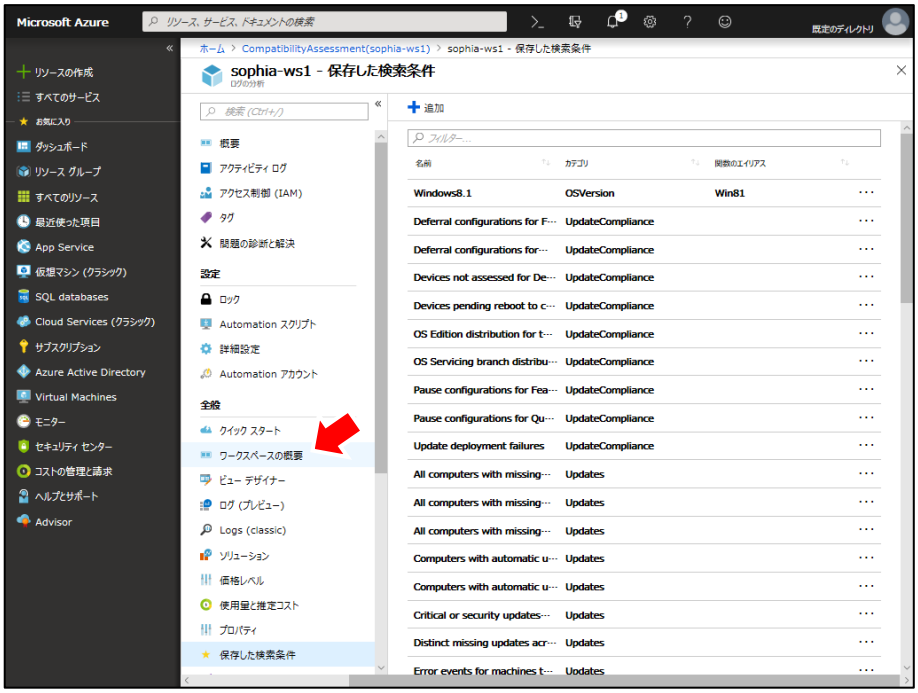
クエリの動作については、[< ワークスペース名 >] - [ログ] 画面内で、[Type your query here…] にクエリを入力して [Run] をクリックすることによって確認することができます。この画面からクエリを保存することはできますが、現在はこの画面からコンピューター グループの作成はできません。

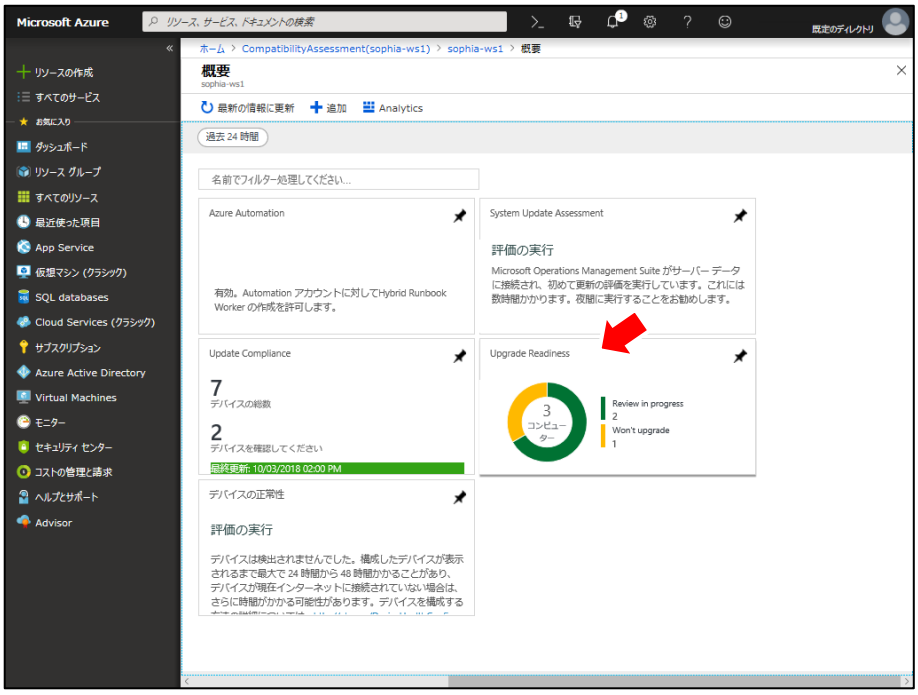


7) [Log Analytics の保存した検索条件が正常に追加されました] の通知およびその検索条件が一覧に追加されたこと確認する。

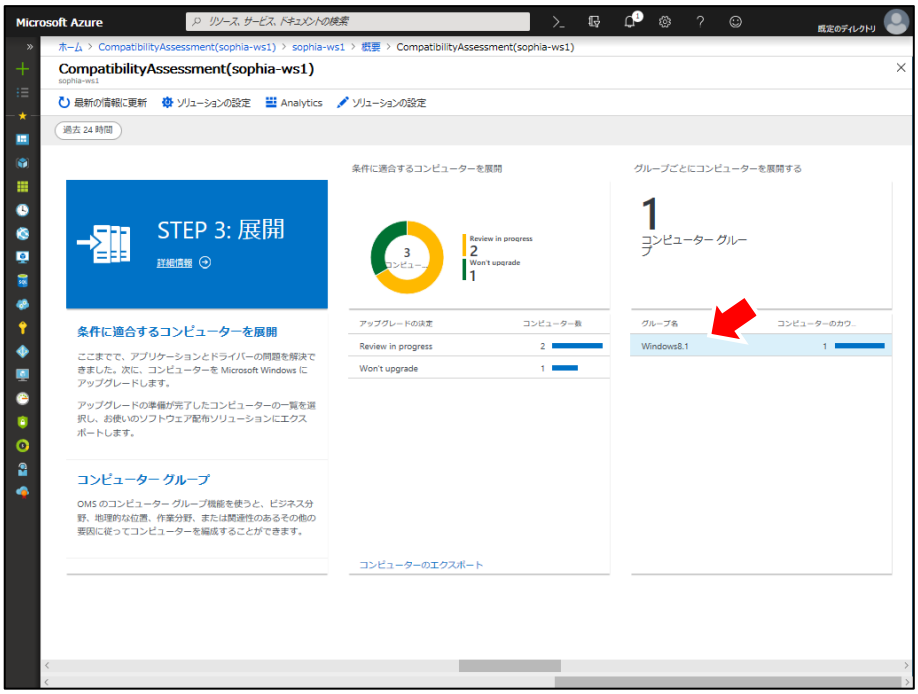


8) 左ペインから [ワークスペースの概要] をクリックし、[概要] 画面で [Upgrade Readiness] をクリックする。

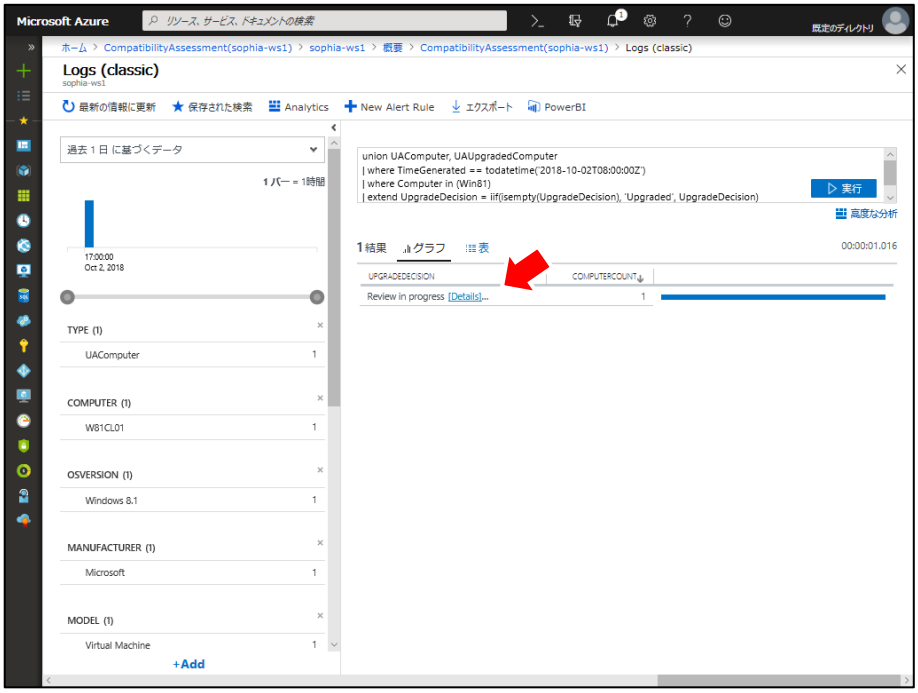




9) [CompatilityAssessment] 画面で右にスクロールし、[グループごとにコンピューターを展開する] 項目にグループが作成されていることを確認して、グループ名をクリックします。ここでは、[Windows8.1] をクリックします。



10)[Logs (classic)] 画面で、[結果]から Review in progress などの状態を確認できます。



NOTE:

本稿執筆時点（2018 年 10 月）では、手順 9 からの操作によって Logs (classic) にアクセスすることになりますが、将来的に [ログの分析] リソースの [ログ] 項目のユーザーインターフェイスに切り替わる予定です。

5.6 ステップ 4： モニター

[ステップ 3:展開] 項目の結果を受けて、各コンピューターで OS アップグレードを行ったり、Windows 10 の機能更新プログラムを使ってアップグレードを行ったりした結果を確認するために利用できるのが [モニター] 項目です。[モニター] 項目ではアップグレードの状態 (展開状態) やアップグレード時に発生したデバイスドライバーに関する問題などを一覧できます。

画面 5.6-1 [ステップ 4:モニター] 項目

[モニター] 項目の [展開の進行状況 (過去 30 日間)] 項目では、現在のバージョンの Windows 10 にアップグレードされたコンピューターの総数を [Upgrade Completed]、アップグレード最中のコンピューターの総数を [In progress]、アップグレード開始前のコンピューターの総数を [Not started] でそれぞれ確認できます。なお、エージェントがインストールされた時点で既に最新のバージョンの OS になっているコンピューターも [Upgrade Completed] にカウントされることに注意してください。

5.7 Office アドイン

スクリプトが実行されたコンピューターのうち、コンピューターにインストールされた Office アドイン プログラムを識別するために使用するのが [Office アドイン] 項目です。インストールされている Office アドインを事前に把握しておくことにより、Office 365 ProPlus の展開やアップグレード時に互換性の問題を引き起こさないか、事前に確認できるようになります。

5.8 サイト検出

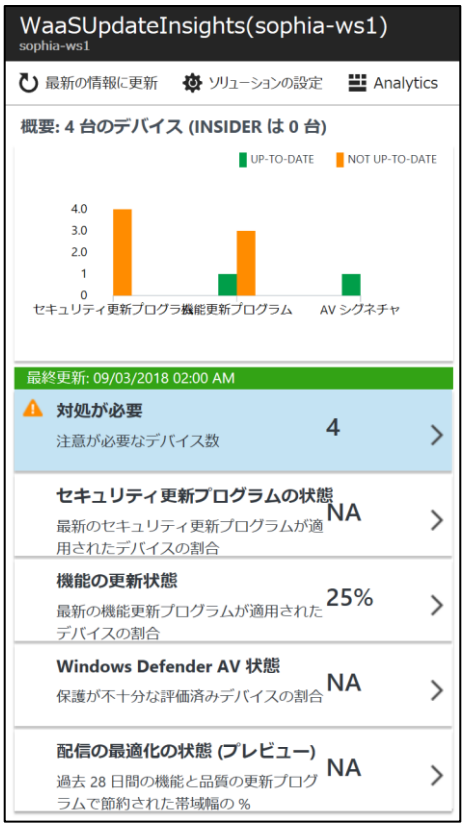
スクリプトが実行されたコンピューターがこれまでにアクセスした Web サイトやドキュメントモードの識別に利用可能な項目が [サイト検出] 項目です。[サイト検出] 項目に表示される Web サイトやドキュメントモードの情報を把握することにより、ユーザーがよくアクセスする Web サイトにおいて互換性の問題から描画の問題が発生していないか、把握することができます。

6　Update Compliance による現状分析

本章では、Microsoft Azure から Update Compliance が利用できるようになった状態から、参照可能なダッシュボード（レポート）の内容とその見かたについて解説します。

Azure 管理ポータル画面上で、WaaSUpdateInsights のソリューション名称で提供される Update Compliance は、Azure 管理ポータル画面から WaaSUpdateInsights ソリューションにアクセスすることで、Update Compliance のダッシュボードを参照できます。ダッシュボードには画面 6-1 のような情報が表示され、その画面からアップグレード対象を見極めるうえで重要な、様々な情報を参照できます。

画面 6-1 Azure 管理コンソール画面内の Update Compliance 概要項目



Update Compliance では、ソリューション内に複数のカテゴリが用意されており、カテゴリごとに詳細な内容を参照できるようになっています。次の節からはそれぞれのカテゴリをクリックした時に表示される内容について、概要を解説します。

6.1 対処が必要

インストール対象となっている更新プログラムがまだインストールされていない場合や、サポート期限である 18 か月を超えて特定の機能更新プログラムのバージョンが使われ続けている場合に [対処が必要] 項目ではお知らせをします。

画面 6.1-1 [対処が必要] 項目

[対処が必要] 項目のうち、[デバイスの問題] 項目では以下の情報をお知らせします。

表 6.1-2 [デバイスの問題] 項目のステータス

Out of support OS Version	サポート対象のバージョンが使われているコンピューター
Missing multiple security updates	2 つ以上のセキュリティ更新プログラムがインストールされていないコンピューター

サポート対象のバージョンが使われている場合は機能更新プログラムを、セキュリティ更新プログラムがインストールされていない場合は品質更新プログラムをそれぞれインストールして解決します。機能更新プログラムに関する詳細は Update Compliance の [機能の更新状態]、品質更新プログラムに関する詳細は Update Compliance の [セキュリティ更新プログラムの状態] から、それぞれ確認できます。

一方、更新プログラムのインストールを行おうとしたときにトラブルが発生した場合、[対処が必要] 項目の [更新に関する問題] からトラブルの詳細を確認できます。[更新に関する問題] では、トラブルを次のような項目で分類を行い、表示します。

表 6.1-2 [更新に関する問題] 項目のステータス

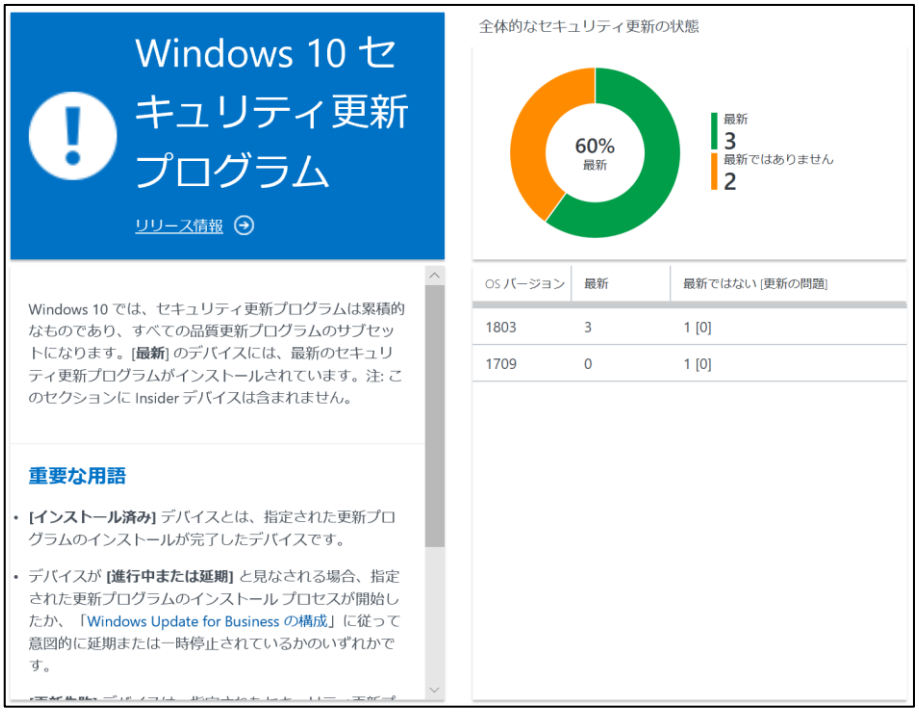
Failed	更新プログラムのダウンロード・インストールに失敗した場合にカウントされる
Progress stalled	更新プログラムのダウンロード・インストール中の状態から 10 日経過しても結果が確認できない場合にカウントされる
Canceled	ユーザーの操作によって更新プログラムの適用がキャンセルされた場合にカウントされる
Rollback	更新プログラムの適用に問題があり、ロールバックされた場合にカウントされる
Uninstalled	意図的に更新プログラムがアンインストールされた場合にカウントされる

以上のステータスは、個々の項目をクリックすると、Log Analytics のクエリ画面に移動し、該当するコンピューター名を確認できます。

6.2 セキュリティ更新プログラムの状態

特定バージョンの Windows 10 での品質更新プログラムのインストール状況を把握するために [セキュリティ更新プログラムの状態] 項目を使用します。概要画面の [セキュリティ更新プログラムの状態] をクリックすると表示される [Windows 10 セキュリティ更新プログラム] から内容を確認できます。

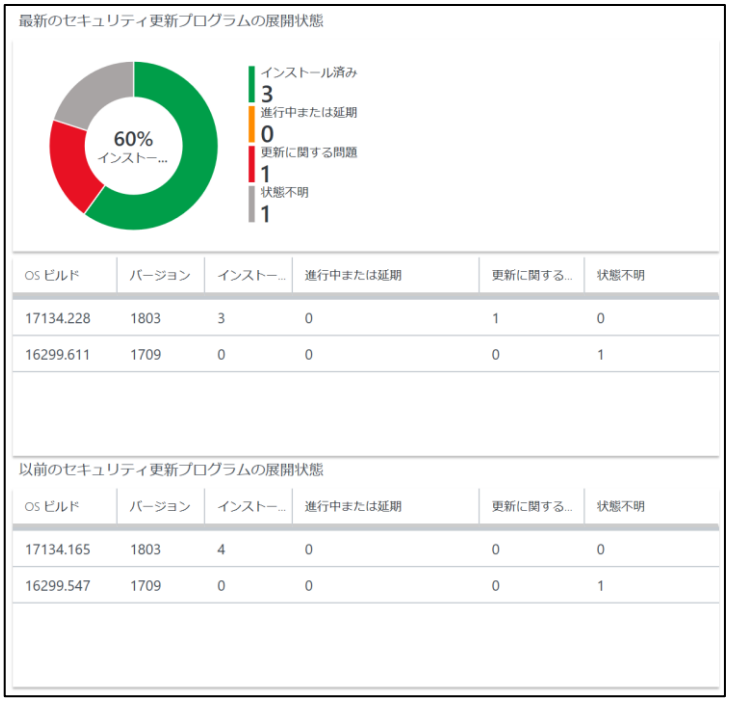
画面 6.2-1 [Windows 10 セキュリティ更新プログラム] 項目



[Windows 10 セキュリティ更新プログラム] 項目内の [全体的なセキュリティ更新プログラムの状態] 項目では、Windows 10 のバージョンごとに、マイクロソフトから提供される、すべてのセキュリティ更新プログラムが適用されているコンピューターの総数を確認できます。

一方、セキュリティ更新プログラムの適用に関わるトラブルがある場合、[Windows 10 セキュリティ更新プログラム] 項目内の [最新のセキュリティ更新プログラムの展開状態] 項目から確認します。[最新のセキュリティ更新プログラムの展開状態] 項目では、直近の品質更新プログラムのインストールの状態 (画面 6.2-2 上段) と、1 回前の時点での品質更新プログラムのインストール状態 (画面 6.2-2 下段) をそれぞれ確認できます。それぞれの項目では、インストール済み、進行中または延期、更新に関する問題、状態不明の 4 つに状態が分類されますが、[進行中または延期] 項目に表示されているコンピューターがある場合、インストールが進行中または Windows Update for Business の設定によりインストールが延期されていることを示します。そのため、意図せず延期されているようなコンピューターがいないか確認するとよいでしょう。

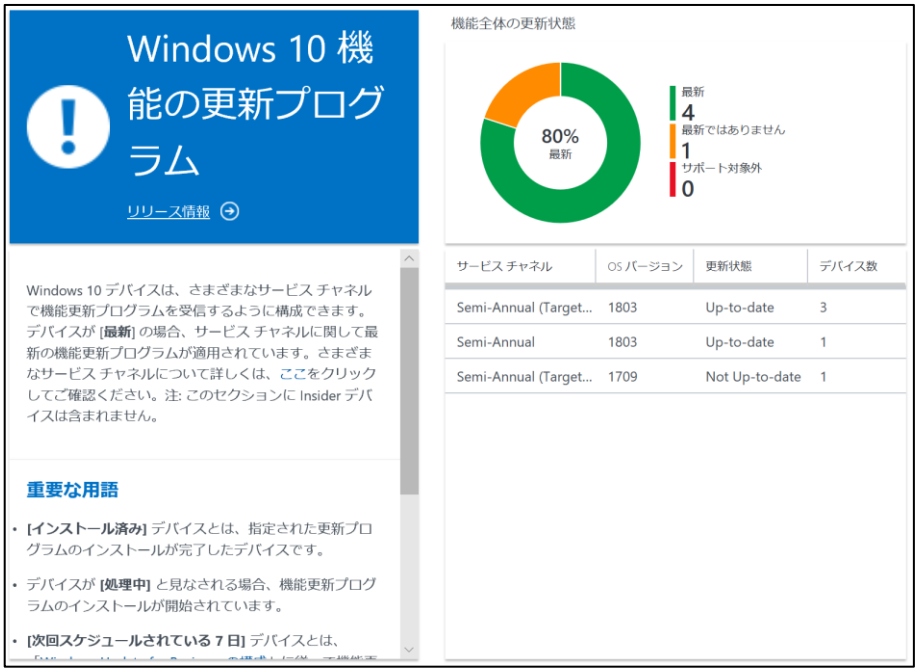
画面 6.2-2 [Windows 10 セキュリティ更新プログラム] 項目 (続き)



6.3 機能の更新状態

Update Compliance の [機能の更新状態] 項目では、機能更新プログラムのサービスチャネルのうち、どのチャネルが選択されているかについて参照できます。[機能の更新状態] 項目では、半期チャネル (対象指定)、半期チャネル、長期的なサービス チャネルの 3 つのモデルに分けて、それぞれのモデルになっているコンピューターでの機能更新プログラムの展開状況 (ステータス) を確認できます。内容は、概要画面の [機能の更新状態] をクリックすると表示される [Windows 10 機能更新プログラム] から確認できます。

画面 6.3-1 [Windows 10 機能更新プログラム] 項目



[Windows 10 機能更新プログラム] 項目内の [機能全体の更新状態] 項目では、サービスチャネルごとにインストールされているコンピューターの総数が確認できます。

機能更新プログラムの適用状況は、[Windows 10 機能更新プログラム] 項目内の [展開ステータス] 項目から確認します。[展開ステータス] 項目は画面 6.3-2 のようにサービスチャネルごとに分かれており、表 6.1-2 の一覧にあるようなステータスメニューで機能更新プログラムの適用に関わるトラブルがないか確認できます。

画面 6.3-2 [Windows 10 機能更新プログラム] 項目 (続き)

半期チャネル (対象指定) 展開ステータス

機能更新プログラム	インストール...	処理中	次回スケジュールされてい...	更新に関する問題	状態不明
1803	3	1	0	0	0
1709	1	0	0	0	0

半期チャネル展開ステータス

機能更新プログラム	インストール...	処理中	次回スケジュールされてい...	更新に関する問題	状態不明
1803	1	0	0	0	0

長期的なサービス チャネル展開ステータス

機能更新プログラム	インストール...	処理中	次回スケジュールされてい...	更新に関する問題	状態不明

表 6.3-1 [展開ステータス] 項目のステータス

インストール済み	機能更新プログラムのインストール済みが完了した場合にカウントされる
処理中	機能更新プログラムが現在、ダウンロード・インストール中の状態のときにカウントされる
次回スケジュールされている 7 日	1 週間以内に半期チャネルで設定した延期期間を終了し、更新プログラムの展開を行う場合にカウントされる
更新に関する問題	機能更新プログラムのインストールに失敗したときにカウントされる
ステータス不明	機能更新プログラムのインストール結果についてエージェントから収集されない場合にカウントされる

以上のステータスは、個々の項目をクリックすると、Log Analytics のクエリ画面に移動し、該当するコンピューター名を確認できます。

6.4 Windows Defender AV 状態

Update Compliance の [Windows Defender AV 状態] 項目では、スクリプトが実行されたコンピューターの Windows Defender ウイルス対策機能の状態について参照できます。[Windows Defender AV 状態] 項目では、有効なシグネチャがインストールされているか (インストールされている場合は signature up-to-date に表示)、リアルタイム保護が有効できあるか (有効である場合は Real-time protect is on に表示)、脅威が発見されたときにその修復を行ったか (修復した場合は Remediated に表示) をそれぞれ確認できます。

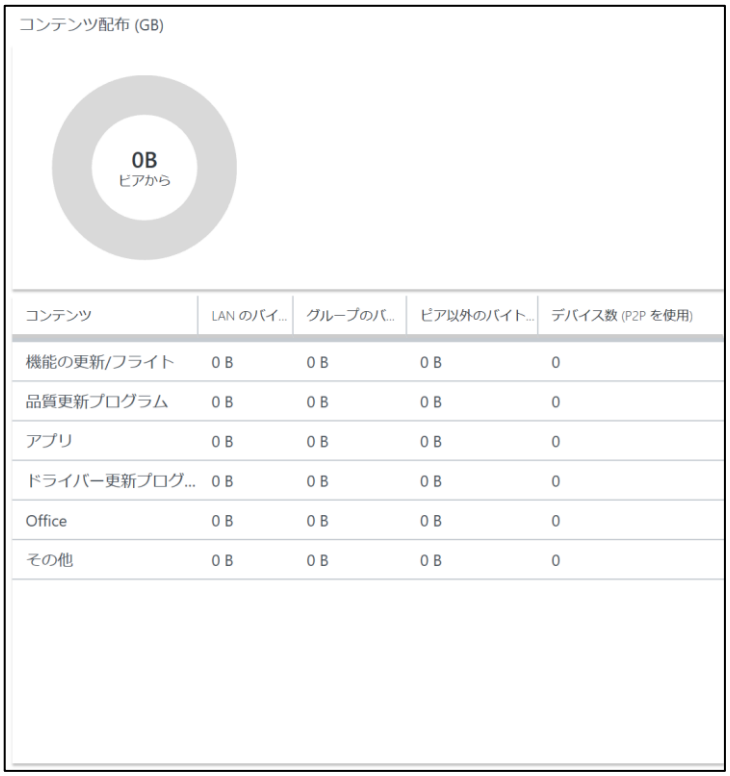
画面 6.4-1 [Windows Defender AV Assessment] 項目

6.5 配信の最適化の状態

Update Compliance の [配信の最適化の状態] 項目では、Windows 10 の更新プログラム ダウンロードに利用可能なテクノロジーである「配信の最適化」の設定値と、配信の最適化によってどの程度のデータがキャッシュ利用したかについて確認できます。

画面 6.5-1 [配信の最適化の状態] 項目

画面 6.5-2 [配信の最適化の状態] 項目 (続き)



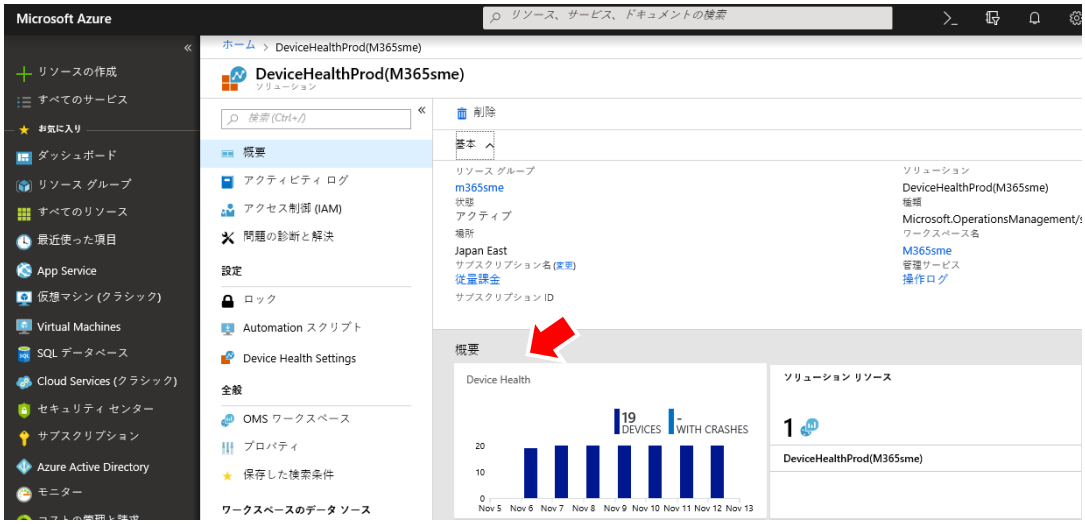
コンテンツ	LAN のバイ...	グループのバ...	ピア以外のバイト...	デバイス数 (P2P を使用)
機能の更新/フライト	0 B	0 B	0 B	0
品質更新プログラム	0 B	0 B	0 B	0
アプリ	0 B	0 B	0 B	0
ドライバー更新プログ...	0 B	0 B	0 B	0
Office	0 B	0 B	0 B	0
その他	0 B	0 B	0 B	0

7　デバイスの正常性 による現状分析

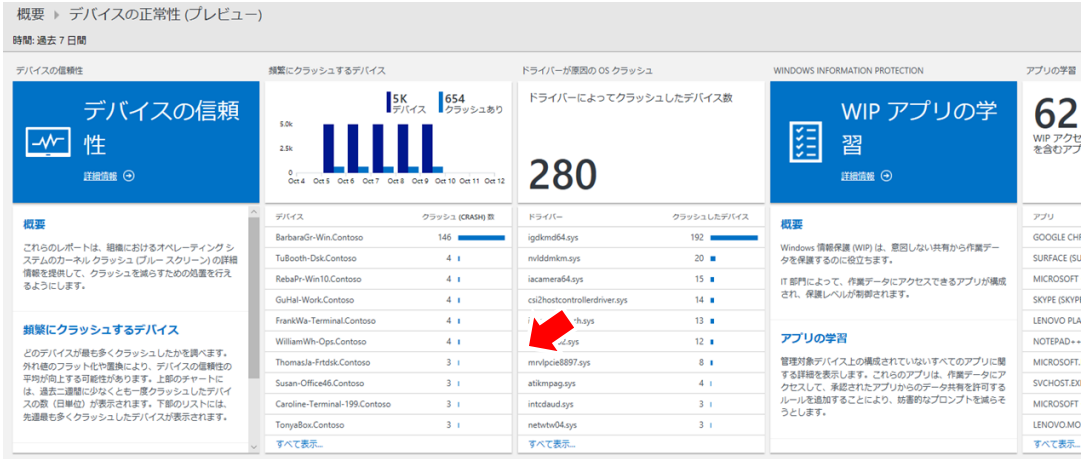
本章では、Microsoft Azure から デバイスの正常性 が利用できるようになった状態から、参照可能なダッシュボード（レポート）の内容とその見かたについて解説します。

Azure 管理ポータル画面上で、DeviceHealthProd のソリューション名称で提供される デバイスの正常性 は、Azure 管理ポータル画面から DeviceHealthProd ソリューションにアクセスし、画面 7 の デバイスの正常性 のエリアをクリックすることで、デバイスの正常性 のダッシュボードを参照できます。ダッシュボードには画面 7-1 のような情報が表示され、この画面から利用されているデバイスの正常性に関する重要な、様々な情報を参照できます。

画面 7 Azure 管理コンソールの DeviceHealthProd ソリューション



画面 7-1 Azure 管理コンソールの デバイスの正常性 項目



デバイスの正常性 では、ソリューション内に複数のカテゴリが用意されており、カテゴリごとに詳細な内容を参照できるようになっています。次の節からはそれぞれのカテゴリをクリックした時に表示される内容について、概要を解説します。

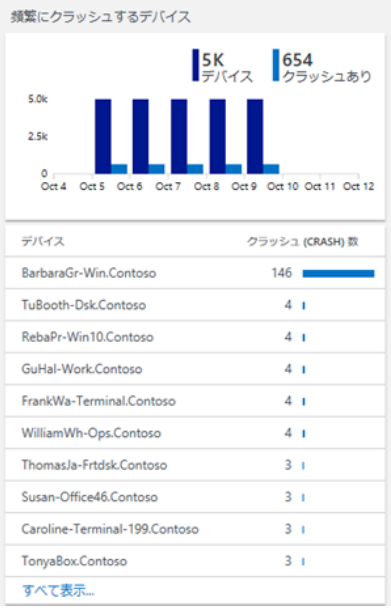
7.1 デバイスの信頼性

組織におけるオペレーションシステム（OS）のカーネル クラッシュ（ブルースクリーン）の詳細情報を確認することで、クラッシュを減らすための対応が行えるようにします。

画面 7.1 [デバイスの信頼性] 項目

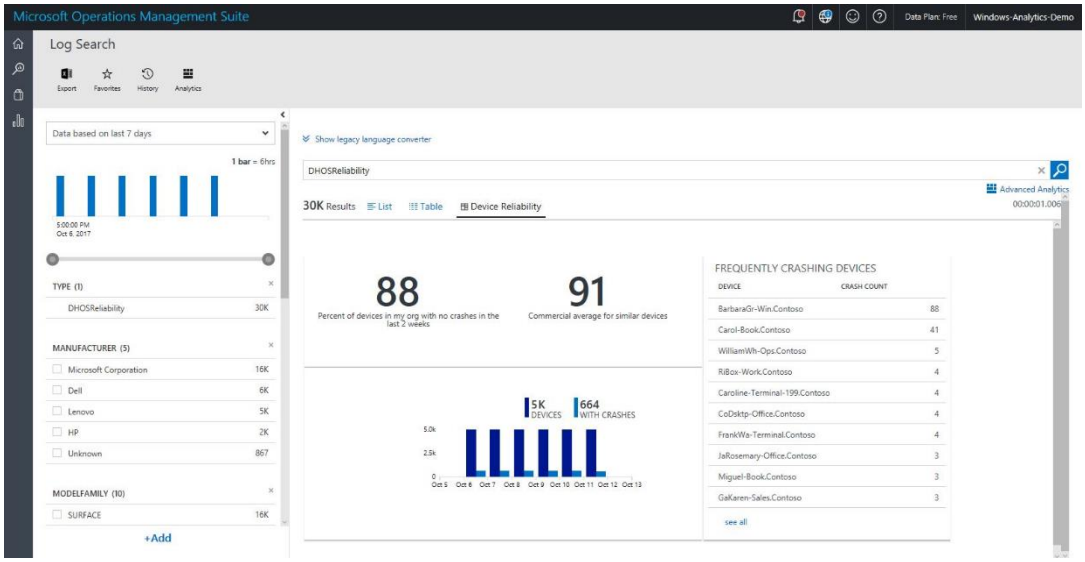
画面 7.1-1 の[頻繁にクラッシュするデバイス] 項目の上の表には、過去二週間に少なくとも一度クラッシュしたデバイスの数（日単位）が表示されます。下の表には、先週最も多くクラッシュしたデバイスが表示されます。

画面 7.1-1 [頻繁にクラッシュするデバイス] 項目



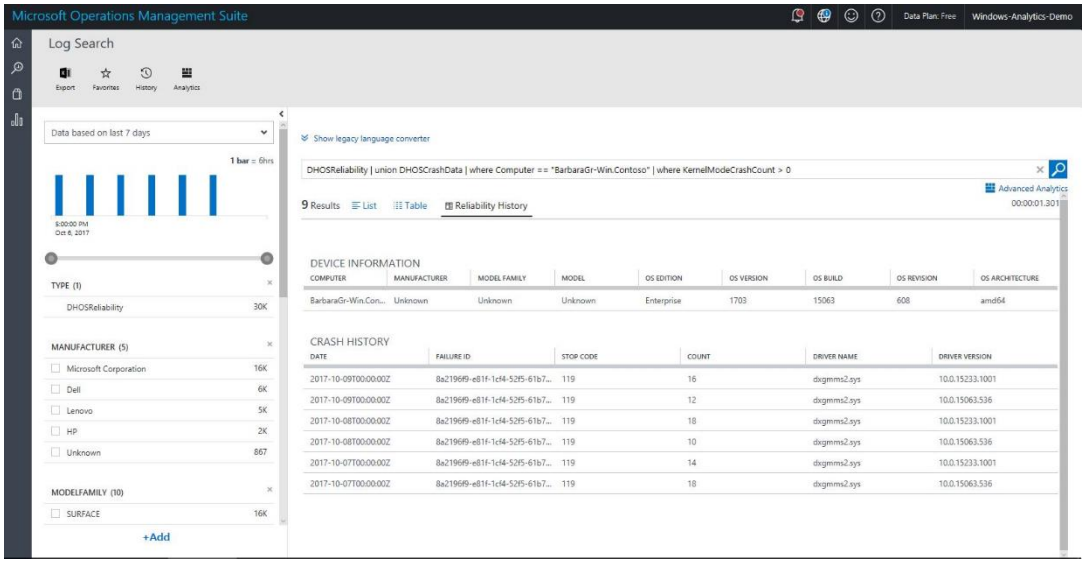
画面 7.1-1 の[頻繁にクラッシュするデバイス] の上の表をクリックすると、画面 7.1-2 が開き、同様の OS とドライバーを利用している組み合わせで収集されたデータ（商用平均）と比較することができます。

画面 7.1-2



画面 7.1-1 [頻繁にクラッシュするデバイス] の下の表で特定のデバイスをクリックすると、そのデバイスのクラッシュの履歴が確認できます。

画面 7.1-3 特定のデバイスのクラッシュの履歴

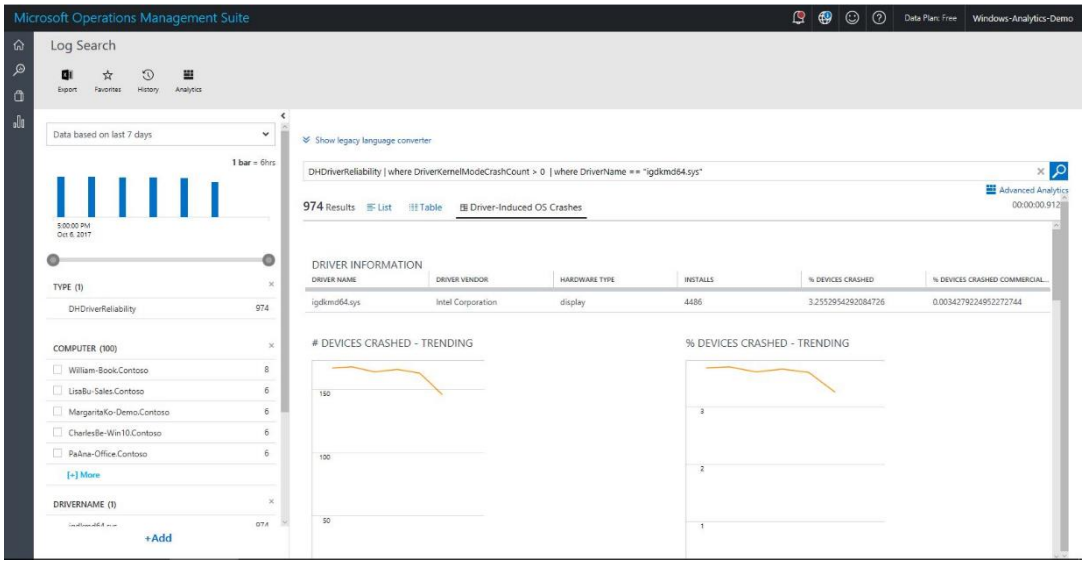


[デバイスの信頼性] 項目のうち、画面 7.1-4 の[ドライバーが原因の OS クラッシュ] 項目では過去二週間にクラッシュの原因となったドライバーが表示されます。それらのドライバーをアップグレードすることで、全体的な OS クラッシュの減少が見込まれます。

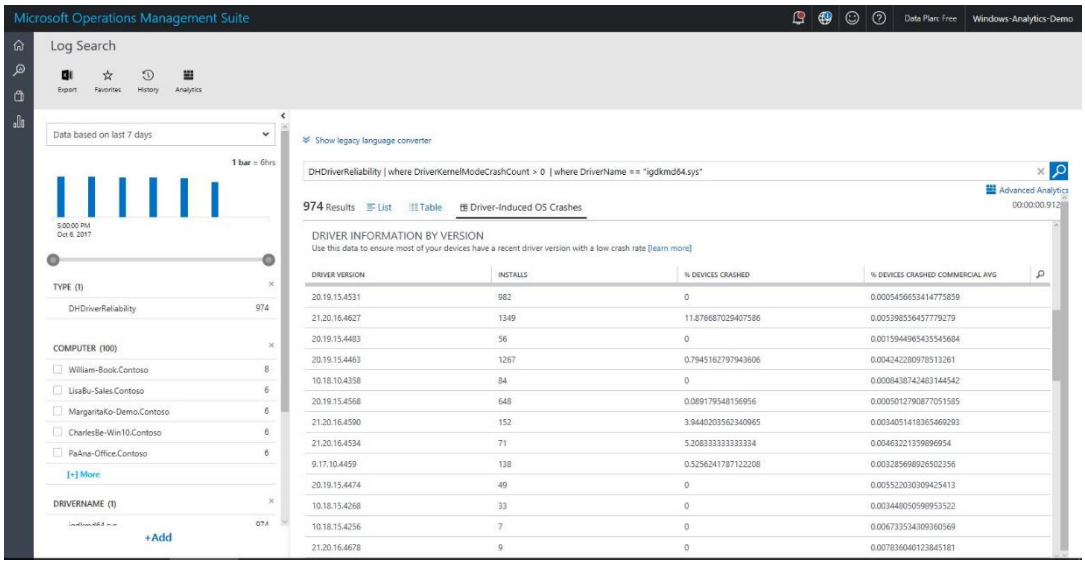
画面 7.1-4 [ドライバーが原因の OS クラッシュ] 項目

画面 7.1-5 の[ドライバーが原因の OS クラッシュ] 項目で一覧表示されているドライバーをクリックすると、画面 7.1-6、そのドライバーの傾向や代替バージョンが表示されるビューに切り替わります。
ドライバーのバージョンのリストでは、どのバージョンにすればクラッシュレートが下がるのかについて確認することができます。

画面 7.1-5 [ドライバーが原因の OS クラッシュ] 項目



画面 7.1-6 特定のドライバーの傾向や代替バージョンが表示されるビュー

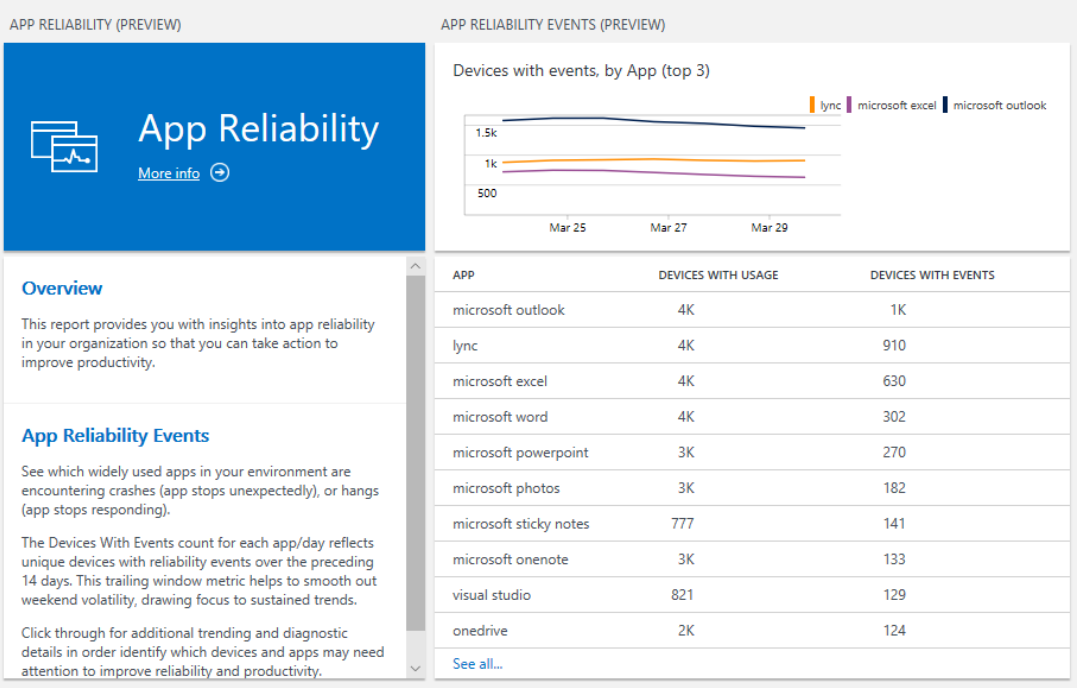


7.2 アプリの信頼性

アプリの使用状況や動作に関するデータが表示されます。これにより誤作動しているアプリを特定して問題を解決するための手段が確認できます。

既定のビューには、過去 14 日間の特定のアプリケーションの「信頼性イベント」を記録した組織内のデバイスの数（DEVICE WITH EVENTS）が表示されます。
「信頼性イベント」は、アプリケーションが予期せず終了するか、応答が停止することで発生します。
なお、この表にはアプリが同じ期間にどのくらい広く使用されているかを見ることができる数字（DEVICE WITH USAGE）も含まれています。

画面 7.2-1 [アプリの信頼性] 項目



特定のアプリをクリックすると、画面 7.2-2 詳細なアプリの信頼性を表示します。
ビューの最初の要素は、アプリ情報の要約を示し、表 7.2-3 にあるような項目が表示されます。

画面 7.2-2 [アプリの信頼性] の詳細

APP	PUBLISHER	DEVICES WITH USAGE	DEVICES WITH EVENTS	% WITH EVENTS	% WITH EVENTS (COMMERCIAL...
Mail & Calendar	Microsoft Corporation	1873	152	8.1	0.9

表 7.2-3 [アプリの信頼性] の詳細項目

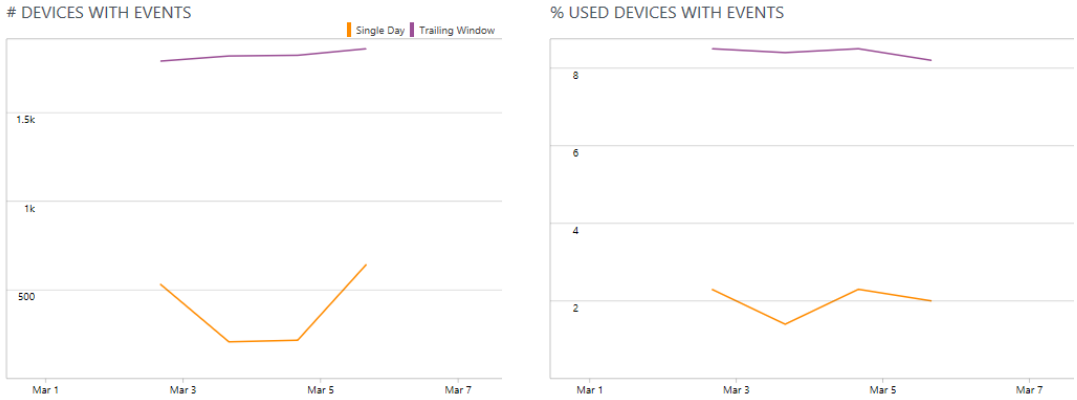
APP	
Publisher	
DEVICE WITH USAGE	アプリの使用状況が記録された一意のデバイスの数
DEVICE WITH EVENTS	アプリの「信頼性イベント」ログが記録された一意のデバイスの数
% WITH EVENTS	「イベントが記録されたデバイス」と「使用しているデバイス」の比率
% WITH EVENTS (COMMERCIAL)	オペレーティングシステムのバージョンとデバイスモデルが混在している展開から収集されたデータ内での「イベントが記録されたデバイス」と「使用しているデバイス」の比率。 これは、特定のアプリがあなたの環境に特有の問題を抱えているのか、ほかの多くの環境でも問題があるのかを判断するのに役立ちます。

画面 7.2-4 [トレンド セクション]では、アプリ情報の傾向の要約が表示されます。
これらのトレンドグラフを使用すると、問題が拡大しているのか、縮小しているのか、または安定しているかを簡単に判別することができます。
左側のトレンドグラフには、何らかのアプリの「信頼性イベント」が記録したデバイスの数が表示されます。
右側のトレンドグラフは、「イベントが記録されたデバイス」と「使用しているデバイス」の比率を示しています。

各グラフには 2 つの行が表示されます。

Trailing Window：
　毎日の値は、その日までの 14 日間に発生した「信頼性イベント」を反映しています。
　これは、週末および少人数によるボラティリティの低下を伴う長期的傾向の評価に役立ちます。
Single Day：
　毎日の値は、1 日に発生した信頼性イベントを反映しています。
　これは、問題が急速に浮上している（または解決されている）場合に便利です。

画面 7.2-4 [トレンド セクション]



画面 7.2-5 アプリと OS のバージョン表 は、アプリ と OS のバージョンの組み合わせでメトリックを解説しています。これにより、どの組み合わせでデバイスの更新または構成の変更が必要ななのか識別することができます。

たとえば、後のバージョンのアプリが環境内の以前のバージョンよりも信頼性が高いことが表に示されている場合は、後のバージョンのアプリを優先して適用、利用していくようにするのが最適な方法となります。
アプリの最新バージョンを既に使用しているにもかかわらず、「信頼性のイベント」が増えている場合は、トラブルシューティングを行うか、Microsoft またはアプリのベンダーからサポートを受ける必要があります。

既定では、テーブルは使用環境で最もよく使用されるバージョンの組み合わせに制限されています。すべてのバージョンの組み合わせを表示するには、テーブル内の任意の場所をクリックしてください。

画面 7.2-5 [アプリと OS のバージョン表]

APP VERSION	OS VERSION	DEVICES WITH USAGE	DEVICES WITH EVENTS	% WITH EVENTS	% WITH EVENTS (COMMER...
17.8827.21855.0	1709	1590	129	8.1	1.2
17.9029.21675.0	1709	757	17	2.2	0.4
17.8827.21855.0	1703	91	7	7.7	1.2
17.9029.21675.0	1703	38	1	2.6	0.4
17.9029.21735.0	1709	18	0	0	NaN

画面 7.2-6 信頼性イベント履歴テーブル、ビューの次の要素は、信頼性イベント履歴テーブルとなります。

この表は、最も詳細な情報を示しています。デバイスの正常性 はデバッグツールではありませんが、この表にて、「信頼性イベント」の特定のデバイス、バージョン、および日付などの詳細情報がわかることにより、トラブルシューティングに役立てることができます。

この表には、診断シグネチャ列も含まれています。
この値は、製品サポートやトラブルシューティングを自分で行っている場合に役立ちます。
値（Failure ID または Failure Name とも呼ばれます）は、マイクロソフトおよびパートナー開発者のクラッシュ統計を要約するために使用されるのと同じ識別子です。
診断シグネチャ値には、信頼性イベントのタイプ、エラーコード、DLL 名、および関与する関数名が含まれます。この情報を使用して、トラブルシューティングの範囲を絞り込むことができます。
たとえば、
APPLICATION_HANG_ThreadHang_Contoso-Add-In.dll ! GetRegistryValue（）

のような値は、Contoso-Add-In がレジストリ値を読み取ろうとしたときにアプリケーションが応答を停止したことを意味します。
この場合、アドインの更新または無効化の優先順位を設定するか、プロセスモニターを使用して読み取ろうとしていたレジストリ値を特定し、ウイルス対策除外、不足しているキーの修正などを行います。

既定では、テーブルはいくつかの最近の行に制限されています。
すべての行を表示するには、テーブル内の任意の場所をクリックします。

画面 7.2-6 [信頼性イベント履歴テーブル]

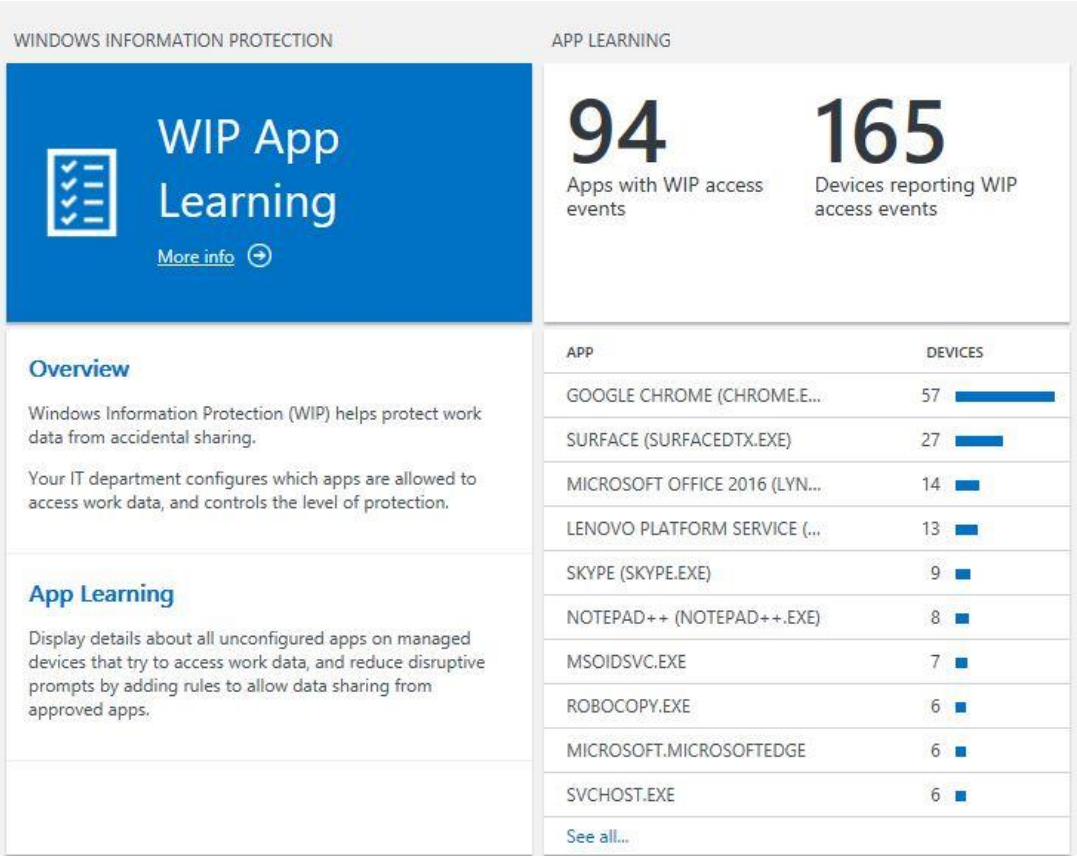
DATE	COMPUTER	PROCESS NAME	APP VERSION	OS VERSION	DIAGNOSTIC SIGNATURE
2018-03-06T08:00:00Z	JudyHo-Box.Contoso	microsoft.windowscommuni...	17.9029.21675.0	1709	NULL_POINTER_WRITE_c000...
2018-03-06T08:00:00Z	PatriciaHe-Work.Contoso	microsoft.windowscommuni...	17.9029.21675.0	1709	INVALID_POINTER_READ_c0...
2018-03-06T08:00:00Z	JovitaMc-Box.Contoso	microsoft.windowscommuni...	17.9029.21675.0	1709	APPLICATION_FAULT_59379...
2018-03-06T08:00:00Z	OlgaPa-Office.Contoso	microsoft.windowscommuni...	17.9029.21675.0	1709	NULL_POINTER_WRITE_c000...
2018-03-06T08:00:00Z	FIDon-Work.Contoso	microsoft.windowscommuni...	17.9029.21675.0	1709	NULL_POINTER_WRITE_c000...

7.3 WIP アプリの学習

Windows 情報保護（WIP）は、作業データを誤って共有するのを防ぎます。
WIP ポリシーが実際の作業の振る舞いと整合しない場合、ユーザーは混乱する可能性があります。
WIP App Learning は、どのコンピューターのどのアプリがポリシーの境界を越えようとしているかを示します。
WIP ポリシーの展開の詳細については、「Windows 情報保護（WIP）を使用した企業データの保護」を参照してください。

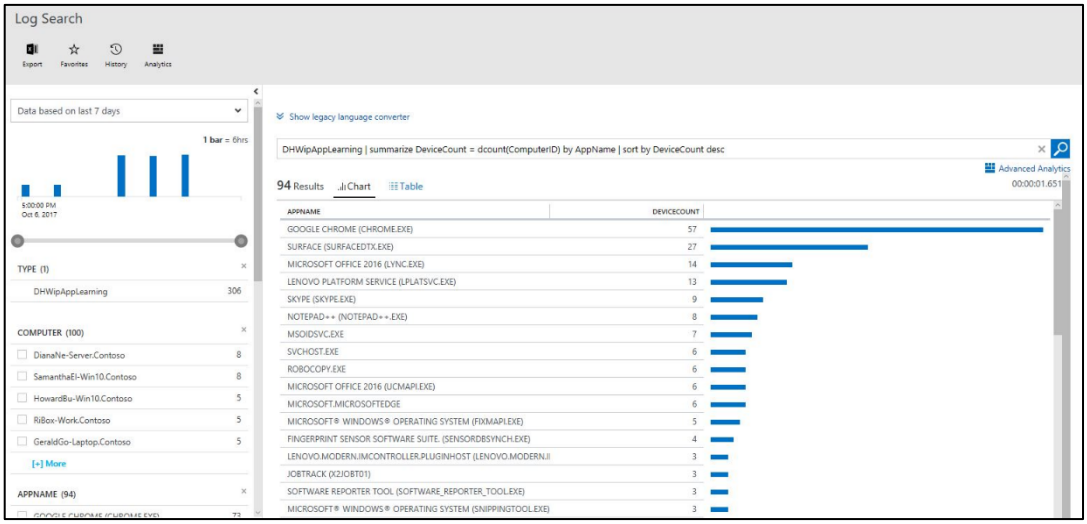
WIP ポリシーを作成することにより、デバイスの正常性 の WIP セクションを利用して以下が行えます。
・承認されたアプリケーションからのデータ共有を許可するルールを追加することで、混乱を招くプロンプトを削減します。
・たとえば、特定のアプリが現在のポリシーによって許可されているかどうかを確認するなどして、WIP ルールを調整します。

画面 7.3-1 [WIP App Learning] 項目



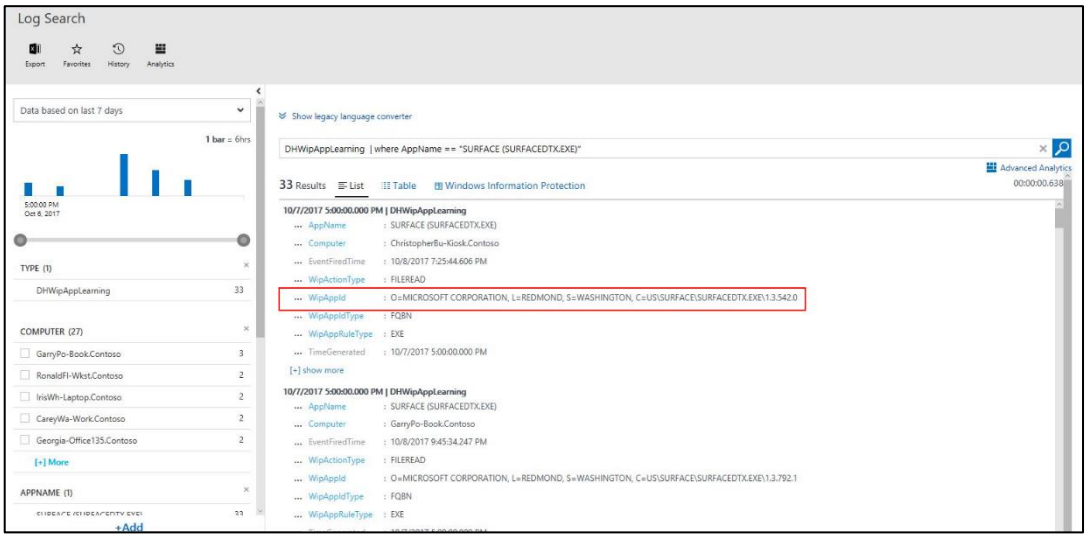
APP LEARNING タイルをクリックすると、画面 7.3-2 が開き、アプリ統計の詳細が表示され、各インシデントの調査を行ったり、アプリポリシーを更新するための App Locker または WIP AppID の確認ができるようになります。

画面 7.3-2



画面 7.3-2 で特定のアプリリストをクリックすると、画面 7.3-3 が開き、Windows 情報保護ポリシーを調整するために必要な詳細を含む、問題のアプリに関する追加の詳細が表示されます。
ここでは、WipAppid をコピーして WIP ポリシーを調整するために使用することができます。

画面 7.3-3



7.4 ログインの正常性

使用しているログイン方法（Windows Hello、顔認識、指紋認識、暗証番号（PIN）、またはパスワードなど）、Windows ログインの成功と失敗の割合とパターン、および特定の理由でログインに失敗した原因について特定できます。

ログインの正常性 のダッシュ ボードでは以下の項目が表示されます。

タイプ別のログインメトリック

タイプ別のログインメトリック では、デバイスごとの成功率と、オペレーティングシステムのバージョンとデバイスモデルが混在する他の環境での成功率（商用平均成功率）が表示されます。

テーブル（タイプ別）では、各ログインタイプの試行の程度、各ログインタイプを使用しているデバイスの数（最も使用されている）、成功率などが測定できます。

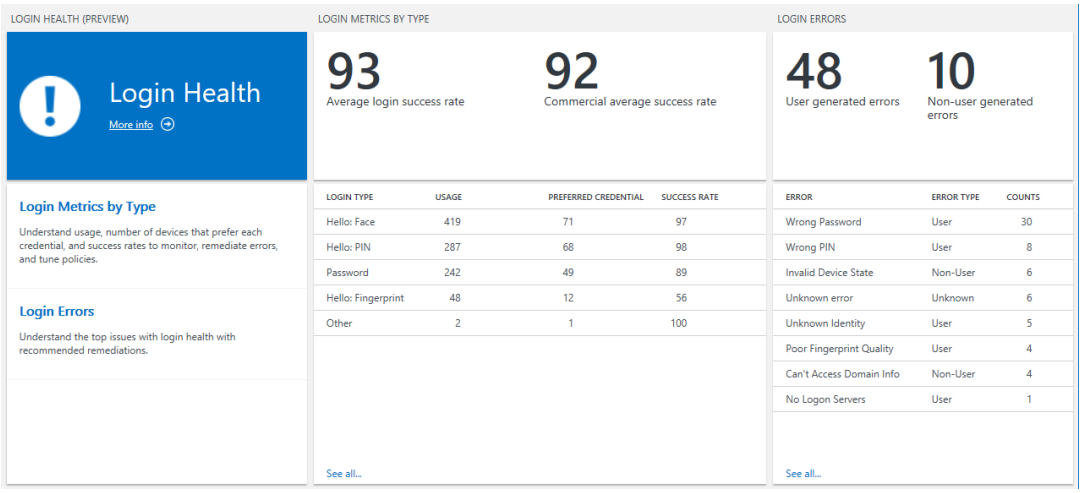
パスワードから PIN などの Windows Hello への移行がうまくいく場合、新しいタイプの使用率が高く成功率が高いことがわかります。

ログインエラー

ログインエラー では、ログインエラーの頻度とタイプ、特定のエラーに関する統計情報が表示されます。これらは、一般的には、ユーザーによるエラーか非ユーザーによるエラーかに分類されます。

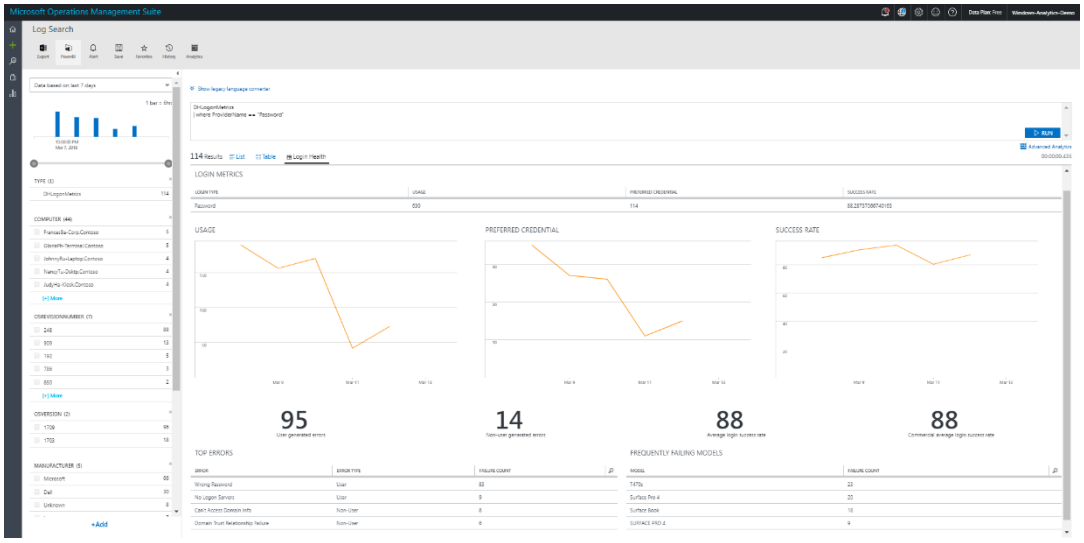
個々のエラーをクリックすると、指定した期間に発生したエラーをすべて表示します。

画面 7.4-1 [ログインの正常性] 項目



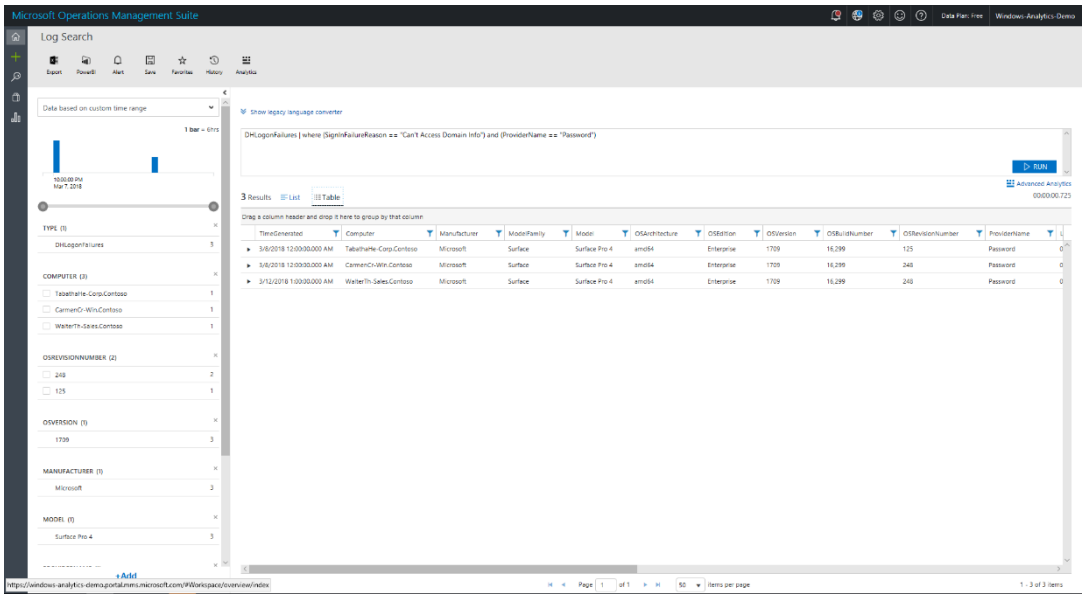
いずれかのログインタイプをクリックすると、画面 7.4-2 が表示され、そのタイプの詳細なログインヘルスデータが表示されます。このビューには、最も頻繁に発生するエラーと、そのログインタイプの頻繁に故障しているデバイスとともに、使用時間、優先認証情報、および成功率の傾向が表示されます。

画面 7.4-2 [ログインの正常性] ログインタイプごとの詳細



画面 7.4-2 で特定のログインエラーをクリックすると、画面 7.4-3 で指定した時間範囲内のエラーおよびログインタイプのすべてのリストが表示されます。

画面 7.4-3 [ログインの正常性] 指定された時間範囲内のエラーとログの詳細



画面 7.4-3 で特定のログインエラーをクリックすると、指定した時間範囲内のそのエラーおよびログインタイプのすべてのインスタンスのリストが表示されます。

このビューには、次のようなデバイス属性とエラー属性が含まれます。

LogonStatus / LogonSubStatus	ログイン試行のステータスコード
SignInFailureReason	ステータスまたはサブステータスから評価された既知の失敗の理由
SuggestedSignInRemediation	エラー時にユーザーに提示された推奨修復 左ペインのフィルターを使用すると、特定のオペレーティングシステム、デバイスモデル、またはその他のパラメータにエラーをフィルターすることができます。または、Login Health パースペクティブから最も頻繁に失敗するモデルをクリックすると、指定した期間内にログインタイプと指定されたデバイスモデルにフィルタリングされたエラーインスタンスのリストが表示されます。

注意： Windows Hello の顔認証エラーについては、ログイン正常性のレポートには現在含まれていません。

8　クエリの書き方

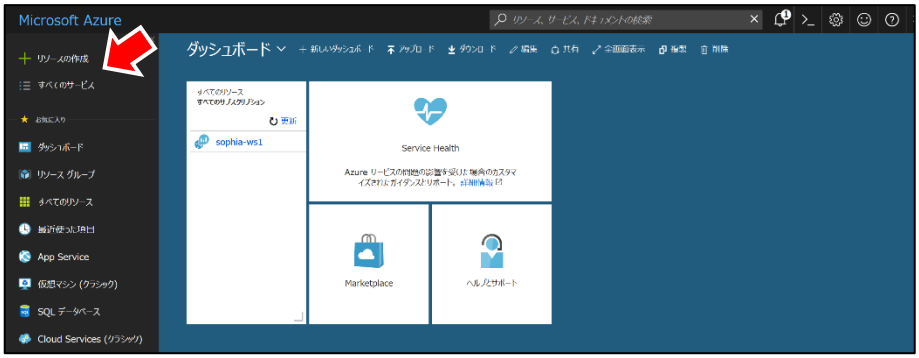
本章では、Upgrade Readiness と Update Compliance の元データに対して直接クエリを実行し、カスタム情報を参照する方法について解説します。

Upgrade Readiness と Update Compliance で扱うデータは Log Analytics を利用して収集したものです。Log Analytics では収集したデータに対してクエリを書いて実行することで、Upgrade Readiness と Update Compliance と同様の内容や、その他の情報を参照できます。そのため、クエリを実行するときは Azure 管理ポータル画面から Log Analytics にアクセスして行います。

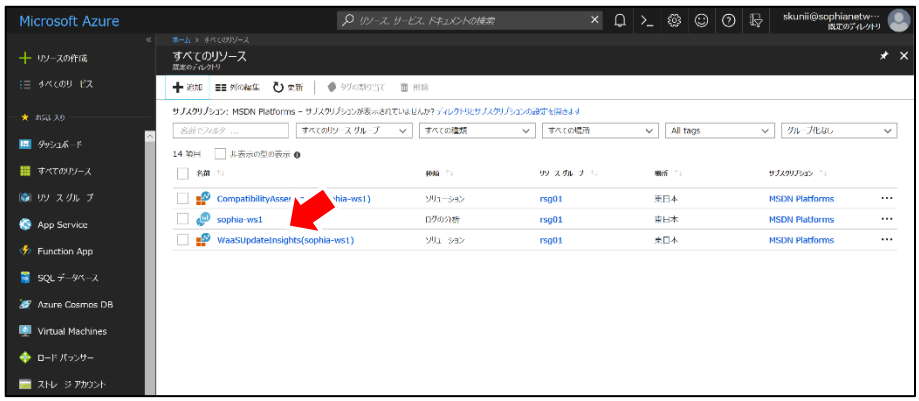
8.1 クエリ作成・実行ユーザーインターフェイスへのアクセス

Log Analytics では、クエリ作成・実行ユーザーインターフェイスとして、ログの分析リソースを用意しています。ここでは、ログの分析リソースにアクセスする方法について解説します。

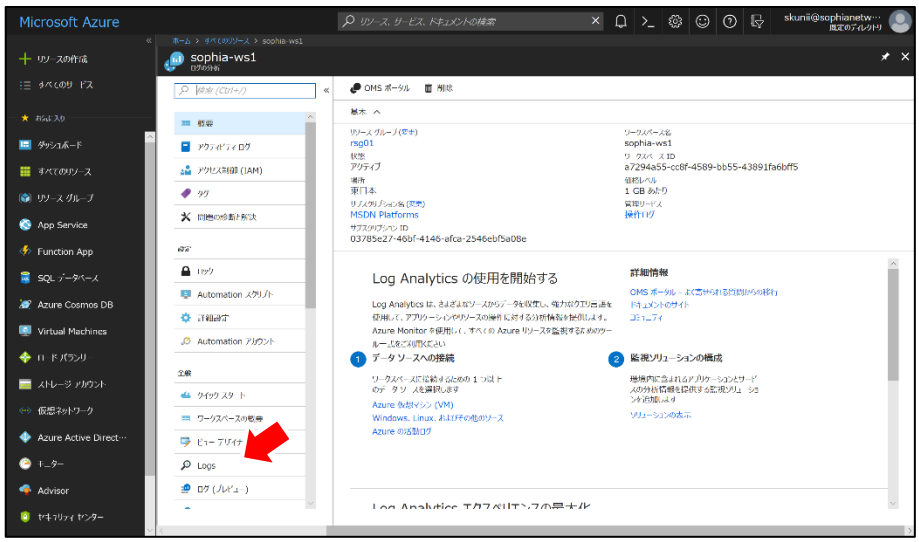
1) Microsoft Azure 画面で、左ペインの [すべてのリソース] をクリックします。



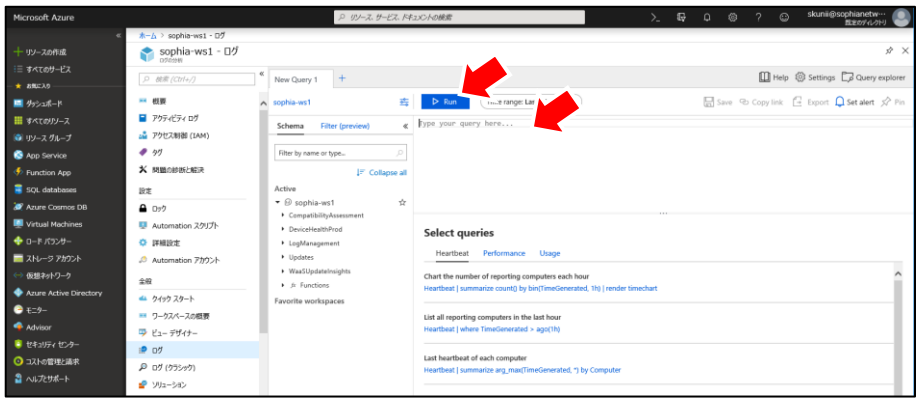
2) ［すべてのリソース］画面で、[ログの分析］種類のソリューションをクリックします。



3) ［CompatilityAssessment］画面で、左ペインの［Logs］をクリックします。



4）［ログ］画面で、クエリの作成窓が確認できます。



8.2 クエリの書式

Log Analytics で使用するクエリには、いくつかの書式（ルール）があり、それに沿って記述します。基本的な書式は以下のとおりです。

参照するレコード ｜ フィルター処理 ｜ カウント処理

8.2.1 参照するレコード

参照するレコード部分は「**Search**」で書き始めます。特定の条件に合致するレコードを出力する場合は「**Search in (オブジェクト) 条件**」となるように記述します。例えば、第 5 章で登場した Windows 8.1 コンピューターの一覧を出力する場合は、コンピューターに対するクエリを実行するため、オブジェクトとして **UAComputer** と指定して実行します。そのため、次のようなクエリになります。

search in (UAComputer) OSVersion == “Windows 8.1”

オブジェクトの種類として、どのような種類があるか調べる場合は「**Search ＊**」と記述して実行することで、すべてのオブジェクト種類（画面では Type と表記）を確認できます。
条件部分で指定可能な条件も「**Search ＊**」クエリで調べることができます。条件部分には等号として == を使いますが、不等号の != や >= <= < > の各記号も使うことができます。

一方、オブジェクトの種類を指定せず、特定のキーワードを持つオブジェクトを検索する場合、「**Search "キーワード"**」となるように記述します。例えば、品質更新プログラムや機能更新プログラムがすべてインストールされている場合、特定項目に「up-to-date」と記録されます。そこで、up-to-date と記録されているレコードを検索する場合、次のようなクエリになります。

search “up-to-date”

8.2.2　フィルター処理

フィルター処理部分は、参照するレコード部分と ｜ (パイプ) で区切って記述します。参照するレコード部分で指定した条件以外の条件をフィルター処理部分では指定します。フィルター処理部分は「**where**」で書き始めます。where に続けて条件を参照するレコード部分と同じような書式で指定します。例えば、Windows 10 コンピューターの中で Microsoft Surface のようなマイクロソフト製のデバイスに対するクエリを実行する場合、次のようなクエリになります。

search in (UAComputer) OSVersion == “Windows 10” | where Manufacturer == "Microsoft"

なお、フィルター処理部分は省略することも可能です。

8.2.3　カウント処理

カウント処理部分は、参照するレコード部分またはフィルター処理部分と ｜ (パイプ) で区切って記述します。参照するレコード部分/フィルター処理部分で指定したクエリに対して、合計を数える (カウント) などの処理を指定できます。処理可能な主な句には次のようなものがあります。

・ **count**
クエリ結果として表示されるレコードの数を数えて出力するときに使います。例えば、Windows 10 コンピューターの数をカウントする場合は次のようなクエリになります。

search in (UAComputer) OSVersion == “Windows 10” | count

・ **distinct**
クエリ結果から特定項目だけ表示するために使います。例えば、コンピューター名 (**Computer**) だけを表示させる場合は次のようなクエリになります。

search in (UAComputer) OSVersion == “Windows 10” | distinct Computer

・ **order by**

クエリ結果の並び替えを行うために使います。並び替えの基準となる項目と、昇順（**asc**)/降順（**desc**)、そして Null 値の並び順（「**nulls last**」または「**nulls first**」と指定）をそれぞれ指定します。例えば、OSBuild 番号の降順に並び替えする場合は次のようなクエリになります。

search in (UAComputer) OSVersion == “Windows 10” | order by OSBuild desc nulls last

・ **extend**

クエリ結果の数値から計算処理を行うために使います。例えば、Windows Defender AV で最後にマルウェアスキャンした日時（**LastScan**）から経過した日数/時間を計算する場合、現在の日時を表す now() 関数と共に指定します。その場合、次のようなクエリになります。

search in (UAComputer) OSVersion == “Windows 10” | extend now() - LastScan

計算結果は Column1 という名前の列に表示されます。そのため、前述のクエリを応用し、コンピューター名とスキャンした日時からの経過時間の 2 項目だけを一覧で表示する場合は次のようなクエリになります。

search in (UAComputer) OSVersion == “Windows 10” | extend now() - LastScan | distinct Computer, Column1

なお、カウント処理部分は省略することも可能です。

9 まとめ

Windows Analytics では、Upgrade Readiness、Update Compliance、デバイスの正常性 等を利用することで Windows 10 へのアップグレード、機能更新プログラムによるアップグレードの適用に必要な事前情報を参照したり、更新プログラムの適用状況を把握したり、できることを確認しました。これらの情報はアップグレードや更新プログラムを適用する前に参照し、問題があれば事前に解決することで、スムーズな運用を実現できるようになります。
本書が Windows Analytics を利用した検証と環境構築を行う際の参考になれば幸いです。

このドキュメントに記載されている情報は、このドキュメントの発行時点におけるマイクロソフトの見解を反映したものです。変化する市場状況に対応する必要があるため、このドキュメントは、記載された内容の実現に関するマイクロソフトの確約とはみなされないものとします。また、発行以降に発表される情報の正確性に関して、マイクロソフトはいかなる保証もいたしません。このドキュメントに記載されている情報は、このドキュメントの発行時点における製品を表したもので、計画のためにのみ使用してください。情報は、将来予告なしに変更することがあります。

このドキュメントに記載された内容は情報提供のみを目的としており、明示または黙示に関わらず、これらの情報についてマイクロソフトはいかなる責任も負わないものとします。
© 2018 Microsoft Corporation.　All rights reserved.
Microsoft、Windows、Windows ロゴ、及び Windows Server は米国 Microsoft Corporation の米国またはその他の国における登録商標または商標です。
このドキュメントに記載されている会社名、製品名には、各社の商標のものもあります。