



IDC PERSPECTIVE

サードパーティによるエンタープライズソフトウェアサポート： 主要なリスクと確認すべきポイント

Rob Brothers

Elaina Stergiades

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot : エンタープライズソフトウェアに対するサードパーティのサポートを検討する際の考慮事項

デジタルトランスフォーメーションは2017年の重要な戦略的命題であるが、多くの企業にとって既存のITインフラの単純なリプレイスでは意味のある投資にはならない。CIOはクリティカルなビジネスプロセスのためのITインフラの革新、進化、最適化を進める必要がある。適切なサポートサービスプロバイダーは、パフォーマンスの最大化を支援できる。エンタープライズソフトウェアのサードパーティのサポートサービスプロバイダーについて、IT部門では5つの基準で評価し、自社のITロードマップに最適なプロバイダーを決定すべきである。

Key Takeaways

- 多くのIT部門にとって、「セキュリティおよびコンプライアンス／ガバナンス」がサポートプロバイダーを選択する際の重要な要素になる。規制業種においてはセキュリティパッチへのアクセスの維持とITコンプライアンスの実証が最優先事項である。
- ある種の状況においては、ソフトウェアサポートの特徴と全般的なITの専門知識が、エンタープライズソフトウェアのパフォーマンスを最大化できる適切なプロバイダーを決定する際の主たる基準となる。
- IT予算の状況を考慮すると、IT部門がシステムの稼働の維持とイノベーションへの投資を同時に試みの中で、「年間サポート費用」が引き続き最大の関心事になる、とIDCではみている。

Recommended Actions

- ビジネスプロセスおよびワークロードに応じた適切な検討事項に基づいた、エンタープライズソフトウェアスタック全体に渡るサポートプロバイダーの評価
- 1年、3年、5年後のITの状況に特に重点を置いたデジタルトランスフォーメーションの計画を含む、IT利用実績とロードマップに対する慎重な検討
- デジタルトランスフォーメーションの過程におけるソフトウェアベンダーとの関係に関する計画と、その計画が、移行期間におけるレガシーインフラストラクチャの維持に及ぼす影響の検討

Source: IDC, 2017

概況

エンタープライズ ITはデジタルトランスフォーメーション（DX）の達成に向けて歴史的な変化を遂げつつあり、エンタープライズソフトウェアがその成功を左右する重要な要素となっている。しかし、新規およびレガシーのITインフラストラクチャの保守と最適化は、依然としてCIOとITマネージャーにとって主要な懸念事項である。大半のIT部門では、ITインフラストラクチャのパフォーマンスを最大化するために、エンタープライズソフトウェアのサポートを外部プロバイダーに依存している。過去には、このサポートサービスを提供できるのは開発元のソフトウェアベンダーだけであっ

た。しかし、近年は、エンタープライズソフトウェアに対するサードパーティのサポートサービスという選択肢も浮上している。

ハードウェア市場ではサードパーティのサポートサービスは十分に確立されているが、エンタープライズソフトウェアにはベンダーの独自技術という特性があるため、サードパーティのサポートサービスは比較的新しいコンセプトである。このモデルでは、IT 部門は特定のビジネスアプリケーションに関して、元のソフトウェアベンダーとの保守およびサポート契約の代わりにサードパーティのサポートサービスプロバイダーと契約を結ぶ。エンタープライズソフトウェアの知的財産権によって、サードパーティプロバイダーが提供できるサポートは限られており、ソフトウェアのパッチプログラムを含めて、元のベンダー独自のソフトウェアコードを利用できないため、そのコードで発生するいかなる問題も修正できない。ただし、サードパーティのサポートサービスプロバイダーはその代わりに応急処理やカスタムコードによる解決策などを通じて IT 部門への支援を提供している。

DX のロードマップを計画している CIO や IT マネージャーは、ソフトウェアベンダーおよびサードパーティのエンタープライズソフトウェアサポートの潜在的なメリットとリスクを詳細に検討する必要がある。この作業を進めるに当たって、IDC では、以下のセクションで示す 5 つの主要な分野について慎重な検討を推奨する。

セキュリティ

ハッカーや国家によるサイバー攻撃の脅威の増大に伴い、CIO は IT インフラストラクチャの脆弱性が自社にもたらす潜在的なリスクを痛感している。データ漏洩、消費者の個人情報の流出、知的財産の盗難は、直ちに評判への打撃や収益の損失につながる可能性がある。残念ながら、エンタープライズソフトウェアを最新のセキュリティパッチにより更新することは、IT 部門にとって依然として困難な課題である。IDC では、脆弱なエンタープライズシステム全体に渡るセキュリティの最新のベストプラクティスが、セキュリティのポリシーおよび手続きに組み込まれていることの確認を推奨する。

自社の IT 環境に対する潜在的なリスクは何か？

- 外部および内部のサイバー攻撃リスクを最小化する定期的なセキュリティパッチおよびアップデートが利用できなくなる
- 潜在的な脆弱性に対するソリューションのプロアクティブなモニタリング、およびそれに対応する「緊急」セキュリティパッチを含む、ベンダーによるソフトウェアの直接的な監視がなくなる
- ソフトウェアの対応状況に関する規制およびコンプライアンス要件に関する潜在的な問題（特に高度に規制された業種で重要）
- サードパーティのサポートサービスプロバイダーから提供される「エッジ周辺」のセキュリティが限定されるために生じる、外部および内部の攻撃に対して脆弱なビジネスアプリケーションのカバレッジのギャップ

サードパーティサポートサービスプロバイダーに確認すべき質問

- エンタープライズソフトウェアにおけるセキュリティの課題に対して、当該サードパーティプロバイダーはどのように対処するのか。特に新たな脅威の発生時や新たな脆弱性の発見時においてはどうか
- 当該サードパーティプロバイダーのセキュリティ関連サービスの具体的な詳細。コンプライアンスを実証できる事例や顧客のケーススタディを提示できるか
- 当該サードパーティプロバイダーによるデータプライバシーの管理方法。機密保持のポリシーとトレーニングの有無。ソフトウェアに関する知的財産の機密情報を保護できるか。当該プロバイダーが自社のカスタムコードを利用したことで得た情報や洞察をどのように保護するか

コンプライアンスおよびガバナンス

大半の CIO や IT マネージャーにとって、コンプライアンスとガバナンスは IT 運用の極めて重要な要素である。また、2017 年以降は、コンプライアンスとガバナンスはソフトウェアの保守範囲だけに関

わるものではなくなっている。懸念が高まっている領域として、コンプライアンスを実証するための基本的な要素である監査証跡がある。これらの監査証跡を維持するためには、ビッグデータやアナリティクスに関する十分なスキルがますます必要とされている（手作業による対応では困難な可能性がある）。サイバーセキュリティにおける脅威の増大や全業種に渡る規制強化の中で、企業は政府／業界のコンプライアンス手続きへの違反に対する潜在的な罰金や罰則に直面する可能性がある。セキュリティインシデントへの注目の高まりと発生頻度の増加に伴い、売上、ブランド、顧客の信頼に対する潜在的な打撃は言うまでもなく、これらの処罰のコストは、はるかに大きいと言える。

自社のIT環境に対する潜在的なリスクは何か？

- 継続的なセキュリティやコンプライアンスの問題にとって極めて重要なベンダーのオンラインパッチのネットワークやソフトウェアアップデートを利用できなくなる
- サードパーティのサポートサービスプロバイダーは、ベンダーのソフトウェアを顧客に提供、再ライセンス、またはサブライセンスする権利を有していない可能性が高い
- ベンダーのテクニカルサポートのリソース、技術文書、その他の重要な知的財産へのアクセスが極めて限定される
- ハードウェアの拡張、統合、アップグレードの際における、システム全体に渡るライセンスおよび規制コンプライアンスを維持できる能力

サードパーティサポートサービスプロバイダーに確認すべき質問

- 当該サードパーティプロバイダーは、自社の監査およびコンプライアンスチームが要求する手続きと規制を満たす能力があるか。自社のガバナンスのガイドラインに従うことができるか
- 当該サードパーティはセキュリティおよびコンプライアンスに関する要件を満たす監査証跡に関するスキルを実証できるか
- 契約には当該サードパーティによるソフトウェアベンダーの知的財産の扱いに関する詳細で明確かつ簡潔な記載があるか。そのプロセスが知的財産権法に従っていることを証明できるか
- 当該サードパーティプロバイダーは、「ベンダー知的財産」と呼ばれる可能性のある要素や機能を利用できる法的権利の証明を提示できるか
- 当該サードパーティプロバイダーは、ソフトウェアベンダーの知的財産に関する潜在的な訴訟が発生した場合に誰が責任を負うかを規定する契約条件を提示できるか

ソフトウェアサポートの特徴と機能

ソフトウェアサポートの特徴と機能を比較すると、ベンダーとサードパーティプロバイダーのそれぞれが提供する一連の能力は明確に異なっている。元のソフトウェアベンダーは高度な専門知識を持つエンジニアへの問い合わせサービス、そして機械学習や自動化を組み込んだ機能のサポートサービスを提供することが可能である。これに加えて、ソフトウェアベンダーは、エンドユーザーに影響を及ぼす前に問題を検出、特定、診断、修復する高度なサポートのための知的財産を一貫して開発している。また、ユーザー企業は、拡張ポータル、ナレッジベース、トレーニング、エキスパートガイダンス、カスタムコードから標準機能への移行支援、アップグレード支援などを含む、ソフトウェアベンダーからの広範な拡張ツールセットやユーティリティを利用することが可能である。

ただし、エンタープライズソフトウェアのサードパーティのサポートサービスプロバイダーにも特記すべき特徴があり、ほとんどのプロバイダーは大半のサポートのやり取りに関して専任のサポートエンジニアへの直接問い合わせサービスを提供している。これらのプロバイダーは少数の顧客にサービスを提供しているため、カスタマーダイレクトのサポートモデルを利用することが可能であり、顧客の環境に関して直接的な知識を持つハイレベルなエンジニアへの問い合わせサービスを即座に提供できる。さらに、サードパーティのサポートの範囲には、カスタムコードの対応も含まれる。エンタープライズソフトウェアで発生する問題は、カスタムコードに起因するケースが多いが、これは通常はベンダーサポート契約の対象範囲外である。また、ほとんどのサードパーティのサポートサービスプロバイダーは、ソフトウェアのライセンスやインストールに関係なく、サポートパッケージの一部としてサポートアカウントマネージャーへの問い合わせサービスを提供する。

自社の IT 環境に対する潜在的なリスクは何か？

- 将来に渡ってユーザーのニーズが大きく変化しないと仮定した場合（カスタムコードの変更を除いて）、エンタープライズソフトウェアのベンダーが提供する新たな特徴や機能の利用が制限されること
- コードの欠陥に対処するためのソフトウェアベンダーの開発エンジニアへの問い合わせが限定されること
- 自動化の進むリモートサポート機能を通じて潜在的な問題の検出、診断、解決をサポートできる高度なベンダーのサポート機能の利用が限定されること
- ポータル、コミュニティ、ナレッジベースなどのベンダーサポート機能を利用できないこと

サードパーティのサポートサービスプロバイダーに確認すべき質問

- 当該サードパーティプロバイダーは、電話によるすべての問い合わせに対しハイレベルのエンジニアがその場で支援するカスタマーダイレクトのサポートモデルを提供しているか
- 当該サードパーティのサポートサービスプロバイダーは、エンタープライズソフトウェアに関連するすべてのカスタムコードをサポート範囲に含めることができるか。これには既存のコードの変更は含まれるか、あるいはサポート範囲には、必要に応じた（すなわち、問題の回避や失われた機能を補うための）新規コードの開発が含まれるか
- 当該サードパーティのプロバイダーは、契約期間を通じて同一のチームへのアクセスを保証できるか
- 当該サードパーティのプロバイダーは、社内または外部の顧客に必要とされる特定の SLA を満たすことができるか

全般的な IT の専門知識とサポート

全般的な IT の専門知識とサポートを比較すると、ソフトウェアベンダーとサードパーティのサポートサービスプロバイダーが提供するサービスの利用メリットは状況によって異なる。DX の実現のために要求される劇的な変革には、ハイブリッド IT 全体に渡る IoT、モバイル、コグニティブソリューションなどの高度な新技術に関する具体的な専門知識が必要とされる。もともとソフトウェアベンダーは、IT 環境における新たなテクノロジーの活用、特に自社の知的財産の活用において優位性を持っている。ソフトウェアベンダーは拡張された高度なサポートテクノロジーとアプリケーションライフサイクル管理ツールによって、IT 部門が DX に関する移行管理をサポートできる有利な位置にある。

一方で、サードパーティのサポートサービスプロバイダーは、多くの IT 環境において重要な構成要素であるレガシーの IT インフラストラクチャに対するサポートを提供できる。ソフトウェアサポートの分野における大半のサードパーティプロバイダーはダイレクトアクセスのモデルを利用しているため、ほとんどのユーザー企業には自社の IT 環境に関して広範な知識を有する主たる担当者が割り当てられている。これらのサポート専門家は、既存の IT 資産やカスタムコード管理の今後の戦略に関する質問に答えることが可能である。現実のシナリオにおけるこれらのアプリケーションに関する知識は、レガシーのインフラストラクチャを長期間に渡って維持する予定の CIO や IT マネージャーにとって役立つ可能性がある。

自社の IT 環境に対する潜在的なリスクは何か？

- DX の計画と実施の間に既存の環境を管理するための元のソフトウェアベンダーの専門知識を利用できなくなること
- 特にコグニティブコンピューティング、人工知能（AI）、IoT、ビッグデータ／アナリティクスにおける高度なイノベーションのための移行や統合において、ソフトウェアベンダーからの提案を直接受けられないこと
- サポート対象外となった関連するテクノロジーの新しい実装や配備に関するベンダーからの知見が限定されること

サードパーティのサポートサービスプロバイダーに確認すべき質問

- 自社のレガシーなインフラストラクチャソフトウェア環境に対して、当該サードパーティプロバイダーはどのようなサポートを提供できるか。具体的にどのソフトウェアをサポートできるか
- 将来における当該ソフトウェアのサポートにおいて、カスタムコードの修正あるいは拡張はどの範囲まで対応できるか。当該サードパーティプロバイダーは、ユーザー企業からの推薦や既存の業務のケーススタディを提示できるか
- 当該サードパーティプロバイダーは、元のベンダーや実装に関係なく、対象となるすべてのエンタープライズソフトウェアに関するダイレクトアクセスモデルを保証できるか
- 当該サードパーティプロバイダーは、サポートの詳細とサポート提供に関する細目を契約に記載できるか。これには、エスカレーション、解決不能の問題（特にソースコードにおける問題に関する詳細な計画）、カスタムコードの修正による問題回避策へのアクセスに関する規定が含まれる
- 当該サードパーティのサポートには、DXの取り組みを支援できる具体的な提言、特徴、サービスが含まれているか

年間サポート費用

ソフトウェアベンダーの年間サポート費用は長年に渡って一貫している。エンタープライズソフトウェアのベンダーから購入する基本サポートの料金はライセンス料の18～22%であり、追加機能には追加の年間料金が必要である（たとえば、指定されたエンジニアやテクニカルアカウントマネージャーへの直接問い合わせなど）。大半のエンタープライズソフトウェアベンダーのサポートでは、定期的なパッチとアップデートといった基本サポートに加えて、自動診断／解決から拡張ポータルやチャットテクノロジーによるサポート専門家への即時の問い合わせなど、広範なサポート機能のポートフォリオが含まれている。

これに対し、ほとんどのエンタープライズソフトウェアのサードパーティサポートサービスプロバイダーにおける年間サポート料金は、ソフトウェアベンダーの料金に比べ25～50%下回っており、これは大半のユーザー企業にとって大幅なコスト節減となる。これらのプロバイダーは広範な独自のコードベースを維持しているわけでもなく、新たな製品の特徴や機能の構築に投資しているわけでもない。これらのプロバイダーのユーザー企業数は少なく、低コストモデルであるため、これらのサポートパッケージでは、一般的に基本パッケージの一部としてサポートエンジニアやアカウントマネージャーへの直接問い合わせサービスが提供されている。ただし、ユーザー企業はソフトウェアのアップグレード、特にセキュリティパッチを放棄する潜在的なコストを、将来におけるこれらの価格に織り込んで検討する必要があることに留意しなければならない。

自社のIT環境に対する潜在的なリスクは何か？

- ソフトウェアのアップグレードや新機能、特にセキュリティパッチやコードの修正に対応できなくなることの潜在的コスト
- サードパーティのサポートに関し予期しないコンプライアンスまたはガバナンス上の問題が発生した場合に対する追加的なリスク軽減の計画
- サードパーティとの契約後に再度ベンダーのサポートに戻る場合にソフトウェアベンダーから課されるペナルティの可能性

サードパーティのサポートサービスプロバイダーに確認すべき質問

- 当該サードパーティプロバイダーは契約全期間中のサポート費用に関する具体的な詳細を提示できるか。これらのソフトウェアアプリケーションに関するコスト節減をどの程度の期間保証できるか
- 当該サードパーティプロバイダーは、ベンダーから入手可能なすべてのパッチおよび更新プログラムに関して、ユーザー企業に対してダウンロードや保存、またそれらへのアクセスの維持を要求するか。これらのダウンロード、またはこのプロセスに料金はかかるか
- セキュリティ侵害が発生した場合、当該サードパーティプロバイダーはリスク軽減の支援が可能か

- 当該サードパーティプロバイダーは自社の成長および計画／予測を提示できるか。エンジニアへの直接コンタクトのモデルは維持が困難となる可能性があるが、当該サードパーティプロバイダーは成長に対して十分な人員を確保しているか

IDC の見解

IT 部門は DX の取り組みを計画する中で、極めて困難な課題に直面している。CIO や IT マネージャーにとって、容易な保守と堅牢なサポートが可能で、管理可能な TCO を提供できる環境の構築は、DX の実現への極めて重要なステップである。レガシーのオンプレミス IT や As-a-Service 型のインフラストラクチャから、最新のクラウドアプリケーションや IoT およびエッジでのモバイルに至るまで、IT 利用に広範な選択肢が存在する中で、そして特に犯罪的なハッカーや国家からの継続的な脅威を考慮すると、IT 環境の管理は年々困難さを増している。

大半の IT 部門にとってセキュリティが重要な懸念事項となる中で、CIO はエンタープライズシステムとデータの保護の確保に関しては特に慎重になっている。IDC では、堅牢でプロアクティブな変更管理プロセスから、必要に応じた適切なパッチ適用とセキュリティ修正に至るまで、適切なセキュリティレベルによる IT プロセスの更新がコンプライアンスを維持する上で極めて重要であると考えている。ハッカーが IT インフラストラクチャに侵入した場合の責任と過失への注目が高まる中で、企業の評判と利益への重大な影響を回避するためには、システムとデータに対する適切なセキュリティポリシーが不可欠である。

しかしながら、適切な状況においては、一部のエンタープライズソフトウェアに関してサードパーティサポートサービスプロバイダーを検討することは合理的な判断と言える。IDC では、自社の IT 環境を取り巻く特別な状況および自社の DX のロードマップに重点を置き、前述の特定のシナリオにおけるメリットに特に留意することを推奨する。現在の IT 利用状況の慎重な検討と、1 年、3 年、および 5 年後における自社の IT 環境の状況を総合的に検討することが適切な出発点となる。

また、IDC では、企業に対してレガシー資産を保持する期間について慎重に検討するように注意を促している。デジタルへの移行は現実であり、AI と機械学習を活用する完全に自動化されたシステムのメリットは極めて大きなものとなる可能性がある。テクノロジーの急速な拡大によって、エンタープライズ IT の状況は大幅に複雑化しており、人間だけで管理するのは不可能となっている。クラウド、オンプレミス、仮想ネットワーク、IoT ソリューション、そして特にセキュリティ要件などの間の複雑な相互関係を管理するには、高度で自律的、かつ遠隔管理可能な機能が必要とされる。コグニティブコンピューティング、人工知能、機械学習は、特にサポートの分野において将来のエンタープライズ IT の鍵である。

IT バイヤーへの提言

データセンターのあらゆるレベルで進行しているクラウドテクノロジーへの市場シフトにおいて、ソフトウェアサポートの状況が今後数年のうちに大幅に変化すると IDC では予測している。エンタープライズ IT の動きは依然として緩慢であるが、PaaS（Platform as a Service）、IaaS（Infrastructure as a Service）、SaaS（Software as a Service）の導入のペースは日々加速している。さらに、大半の IT 部門ではビジネスプロセスのサポートが重要な成果物となりつつあり、問題はもはや単なるアップタイム（稼働時間）やシステムパフォーマンスの最大化だけではない。CIO や IT マネージャーはビジネス部門のマネージャーと密接に協力して導入と使用率を改善し、ソリューションから期待される価値を企業が実現できるように万全を期す必要がある。

ソフトウェアベンダーは、これらの取り組みにおいて IT 部門を支援するために、サポートサービスのための高度な知的財産に対する投資の拡大によって、顧客エクスペリエンスの改善と機械学習および自動化の活用に取り組んでいる。驚くべきペースでのテクノロジーの変化は、AI、コグニティブコンピューティング、自動化、および IoT ソリューションが、現在予測されているよりも早期にソフトウェアサポートサービスに組み込まれる可能性が高いことを意味している。前述した 5 つの項目をそれぞれ慎重に検討し、評価プロセスにおいてサードパーティのサポートサービスプロバイダーの候補

から詳細な回答を得るべきである。予見し得る将来において、これらの高度なテクノロジーを利用できるソフトウェアサポートは、元のソフトウェアベンダーのみが提供できるとみられる。

実際、多くの企業では、DXのロードマップを策定し、ソフトウェアベンダーからの他のソリューションを検討する中で、これらのソフトウェアベンダーとの関係の維持を望むとみられる。特にセキュリティパッチやアップデートの利用と規制への確実なコンプライアンス上の理由から、CIOやITマネージャーの多くが、ソフトウェアベンダーとの直接サポートの契約を望んでいる、とIDCではみている。また、CIOやITマネージャーは、ソフトウェアベンダーと協力し、そのサポートチームの専門知識を利用して新しい革新的なテクノロジーを可能な限り早期に導入することも望んでいる。ソフトウェアベンダーは新しい実装と配備に関する直接的な経験を有しており、レガシーのインフラストラクチャのサポートに必要とされるバックエンドとの統合についての方針を提供することが可能である。

しかし、エンタープライズソフトウェアのサードパーティサポートサービスプロバイダーは、レガシーのエンタープライズソフトウェアのサポートに関して特定の限定された要件を有するIT部門にとっては引き続き魅力的であるとみられる。ソフトウェアのサードパーティサポートサービスプロバイダーは、主要な特徴としてコスト節減と、魅力的な「エンジニアによる直接サポート」のダイレクトアクセスモデルに重点を置いており、システムが安定していて新たな機能を望まないか、あるいは必要としておらず、また現在のセキュリティ手続きによって、今後セキュリティパッチが利用できなくなるリスクを負う用意がある場合には、魅力がある。ただし、サードパーティサポートサービスプロバイダーの規模の拡大に伴い、ユーザー企業はサポートサービスプロバイダーがダイレクトアクセスサービスのモデルを維持するために必要な適格なエンジニアへの問い合わせを保証できることを確認する必要がある。IDCでは、これらの決定を行う上でのガイドとして、本調査レポートに記載されている基準および質問を利用することを推奨する。

参考情報

関連調査

- *SAP DBS:Can Enterprise Software Support and Services Really be Transformational?* (IDC #EMEA43190217、2017年11月発行)
- *Market Analysis Perspective:Worldwide Software and Hardware Support and Deployment Services, 2017* (IDC #US43058016、2017年9月発行)
- *Worldwide Storage Support and Deployment Survey:TPMs* (IDC #US42991716、2017年8月発行)

調査概要

本調査レポートでは、エンタープライズソフトウェアに対するサードパーティのサポートサービスを評価する際に考慮すべき事項を提示している。

「大部分の企業はDXの取り組みに多大なリソースを投入しているが、ほとんどの企業にとって既存のITインフラストラクチャを置き換えることは選択肢にならない。CIOはクリティカルなビジネスプロセスのためのレガシーITインフラストラクチャの維持とイノベーションのバランスを取る必要がある。適切なサポートサービスプロバイダーは、この重要な時期において、リスクの最小化とパフォーマンスの最大化を支援できる。エンタープライズソフトウェアに対するサードパーティのサポートが登場する中で、IT部門では5つの基準によって潜在的なサポートサービスプロバイダーを評価し、自社のITロードマップに最適なプロバイダーを選定すべきである」と、ソフトウェア/ハードウェアサポートサービス担当のリサーチマネージャーであるElaina Stergiades（エレーナ スタジアディス）は述べている。

IDC 社 概要

International Data Corporation (IDC) は、IT および通信分野に関する調査・分析、アドバイザリーサービス、イベントを提供するグローバル企業です。50 年にわたり、IDC は、世界中の企業経営者、IT 専門家、機関投資家に、テクノロジー導入や経営戦略策定などの意思決定を行う上で不可欠な、客観的な情報やコンサルティングを提供してきました。

現在、110 か国以上を対象として、1,100 人を超えるアナリストが、世界規模、地域別、国別での市場動向の調査・分析および市場予測を行っています。

IDC は世界をリードするテクノロジーメディア（出版）、調査会社、イベントを擁する IDG（インターナショナル・データ・グループ）の系列会社です。

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or web rights.

Copyright 2017 IDC. Reproduction is forbidden unless authorized. All rights reserved.

