

ゼロトラストネットワークアクセス

Cloudflare Accessはコンテキスト（ID、デバイスポスチャなど）を検証して、お客様の環境全体でアクセスの安全を確保します。VPNは不要です。

ハイブリッドの勤務環境に簡単かつ安全なアクセスを

高速で信頼性の高いゼロトラストネットワークアクセス (ZTNA)

現代の分散した勤務環境では、安全面でも分散型のアプローチが必要です。もはや会社の内外を隔てる「壁」はなく、VPNのような従来のリモートアクセスソリューションでは、現代の人々が抱くセキュリティやパフォーマンスの期待を満たすことはできません。

ZTNAは、リソースごとにIDやデバイスポスチャーなど、細かな背景情報を継続的に検証することで、デバイスや場所を問わずにあらゆるユーザーとアプリを簡単かつ安全に接続します。全く新しいアプローチをとることにより、セキュリティとユーザーエクスペリエンスの間で「妥協する」必要はなくなりました。ZTNAなら、セキュリティとユーザーエクスペリエンスの両方を高めてビジネスに活かします。

また、クラウド移行、M&A活動、急速な革新やスケーリングといった変化にも、より俊敏で効果的な対応が可能になります。Cloudflareはゼロトラスト（セキュリティ最新化）戦略の中核であり、プログラム可能なグローバルコネクティビティクラウドでZTNAを提供しています。

80%

VPN使用に関するリモートアクセスサポートチケットの解決に費やされる平均時間を短縮¹

72%

以前のベンダーと比べ、毎月のポリシー設定にかかる時間を節約¹

68%

従業員や請負業者の認証手順の合理化に多大な効果を確認¹

最新化されたアクセスでビジネスに力を与える



ユーザーエクスペリエンスを強化

最新化されたセキュリティによって、オンプレミスアプリがSaaSアプリと同じ感覚で使用できるようになり、チームの生産性が向上します。遅くて不便なVPNは不要となり、従業員からの苦情もありません。



ラテラルムーブメントを排除

ネットワークレベルのアクセス許可ではなく、リソースごとにコンテキストに基づいて最小特権アクセスを認めることによって、サイバーリスクを軽減し、攻撃対象領域を縮小します。



ゼロトラストのスケールが容易

まずは重要アプリや最もリスクの高いユーザーグループを保護し、その後にインターネットネイティブのZTNAを拡張してビジネス全体を保護することにより、技術効率を高めます。

Accessの主な使用例

Zero Trustを導入してハイブリッドワークの安全を確保

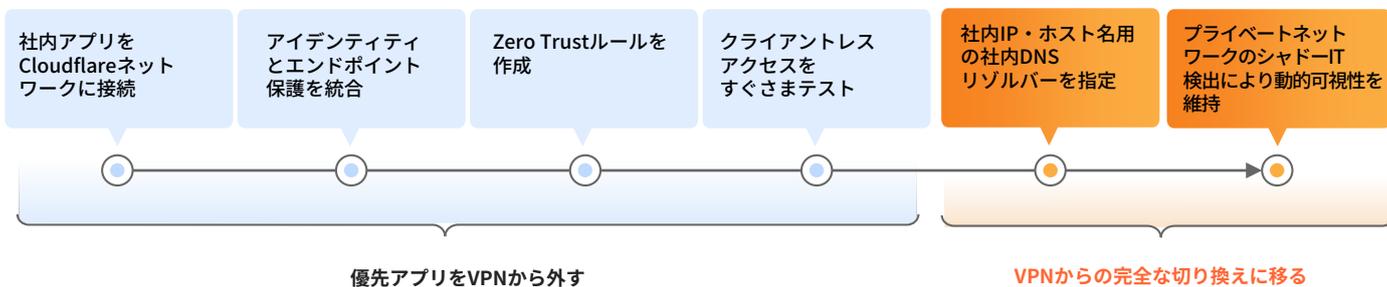
- ★ **VPNの増強と置き換え** — Accessは従来のVPNに比べよりスピーディで安全です。セキュリティとエンドユーザーエクスペリエンスを向上するために重大なアプリの移行を開始しましょう。
- ★ **請負業者のアクセス** — クライアントレスのオプションやソーシャルIdPなどを用いて、請負業者などのサードパーティユーザーを認証します。
- **開発者のアクセス** — 権限のあるテクニカルユーザーが、パフォーマンスに影響を与えることなく、重要なインフラストラクチャに、安全にアクセスできます。

デジタルモダナイゼーションの実行

- **M&Aを迅速化** — 従来のネットワークを完全に統合することは避けましょう。複数のIdPと統合し、M&A進行中はアプリごとに内部アクセスするアプローチを取ります。
- **フィッシングに耐性があるMFA** — 強力な認証（FIDO2準拠のセキュリティキーなど）をあらゆる場所に展開します。
- **セキュアなDevOpsワークフロー** — メッシュ/P2P接続で双方向トラフィックをサポートし、サービス間のワークフローを保護します。

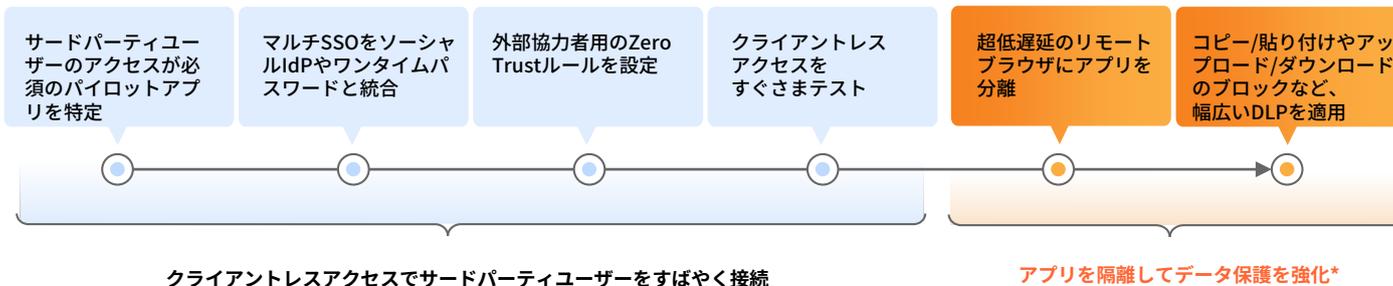
VPNの増強および置き換えを始める

重要なアプリや高リスクユーザーを優先してZTNAをパイロット導入し、VPNを補強します。テストを促進するために、WebアプリケーションやインブラウザのSSHにクライアントレスアクセスを使用します。徐々に高度な機能を導入し、VPNを完全に脱却する方向へ向かって、ネットワークの変化に合わせて動的な可視化を実現します。



請負業者（サードパーティ）アクセスを始める

円滑なユーザーエクスペリエンスを提供しつつ、管理対象外のデバイスに起因するリスクを軽減します。請負業者にエンドユーザーソフトウェアを必要としないシンプルな認証オプションを設定します。さらなるデータ保護を適用するために時間をかけて高度な機能を導入します。



*Zero Trustプラットフォームの他の部分で機能を使用

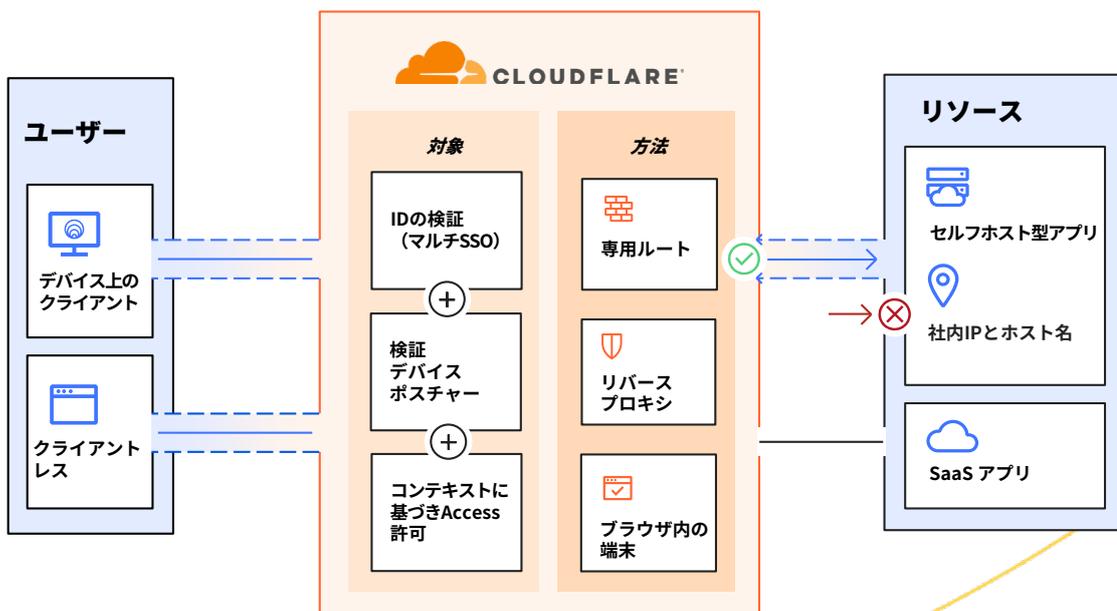
Accessの仕組み

Cloudflare Accessはアイデンティティやデバイスポスチャーなど細かな背景情報を継続的に検証する柔軟な集約レイヤーで、ソフトウェア定義による境界を作り出すことにより、組織のリソース全体に簡単かつ安全なアクセスを個別に提供します。ユーザーが認証を受け、すべてのアクセスポリシーの条件を満たすと、Accessは指定したセッション期間中に有効な署名付きのJSON Webトークンを発行します。Cloudflareでは構成可能なプラットフォームを介してすべてのユーザーリクエストにシングルパス検査を実施し、一元化されたポリシー管理エクスペリエンスがポリシーの変更を数秒でグローバルに拡散します。これを可能にするのが、CloudflareのユニークなAnycastネットワークアーキテクチャです。

統合されたクライアントレス操作とクライアントベースの操作が、すべてのデバイスタイプを処理します。顧客データのプライバシーを保持するために、ネットワークへのトラフィックを暗号化するZero Trustサービス全体に1つのデバイスクライアントを使用します。また、クライアントレスセットアップを通じて企業外のデバイスにも簡単かつ安全にアクセスできるようにします。ZTNA、DNS、市場最先端のWAF、DDoS保護サービスが一体となって、サードパーティのユーザーとハイブリッド環境で勤務する従業員があらゆるデバイスからアクセスできるパブリックホスト名を作成し、保護します。Cloudflareのユーザーレス認証オプション（トークンまたはmTLS証明書）は自動化されたサービスやIoTデバイスの事例にも対応します。

リソースのZero Trustコントロールのため、セルフホストアプリ（クラウド/オンプレミス）やインブラウザSSH/VNCのリバースプロキシ、SaaSアプリのアイデンティティプロキシ、プライベートサブネット内のWeb/非Webリソース（任意TCP/UDP）へのクライアント/トンネル方式プライベートルーティングで経由するL4-7フォワードプロキシには、パブリックホスト名を使用します。Cloudflareのグローバルネットワークとアプリコネクタソフトウェアは、Kubernetesやコンテナを含めたパブリッククラウド、オンプレミスのレガシーネットワークリソースなど、あらゆるコンピューティング環境を総合的にサポートします。VMインフラストラクチャは必要なく、他のZero Trustベンダーのようなスループット制限もありません。

ID認証、エンドポイント保護、ネットワークオンランプ、ログ作成/分析、SIEMのサードパーティ製ツールは、当社のデバイスクライアントおよび分析と共に、Cloudflareのダッシュボードに組み込まれています。これにより、管理者は俊敏に対応できるほか、すでに使用しているツールを使って構築できます。



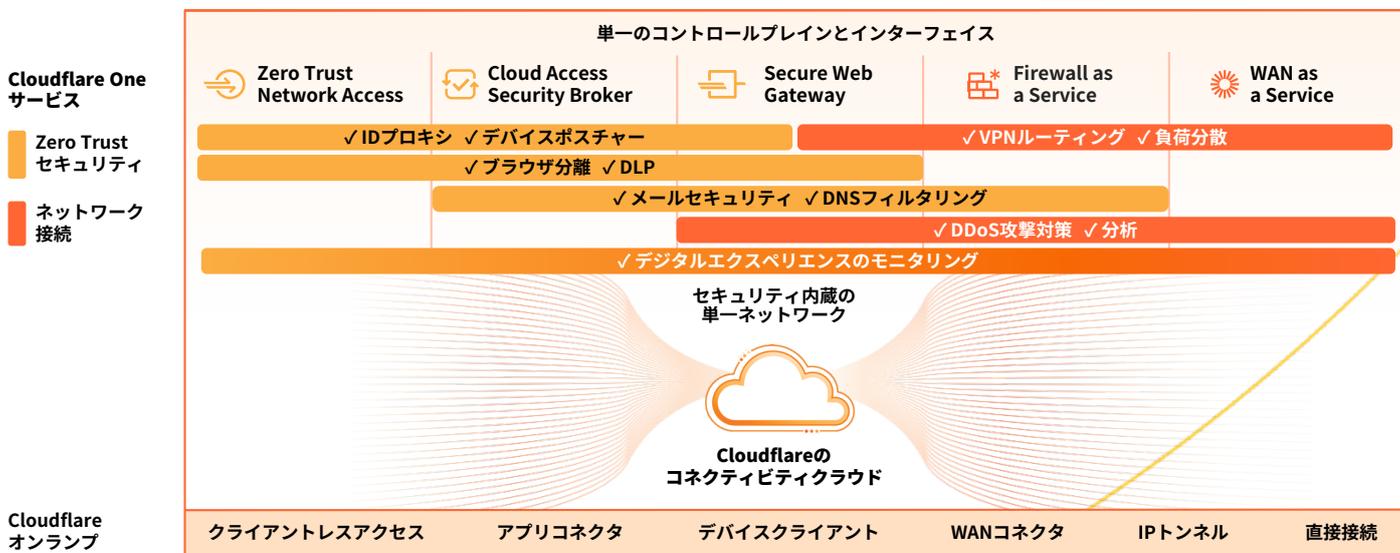
CloudflareのSSEとSASEプラットフォームの一部としてアクセス

SSEとSASEでは導入完了までに数年かかるような戦略的手順を要することもよくありますが、Cloudflareでは企業がZTNAから開始することも珍しくはありません。ZTNAでは、ITチームに実行しやすく、理解しやすいステップが使用されますが、これは、ビジネスの価値を短期間に示すことができるためです。ITリーダーはハイブリッド環境での勤務を保護し、脅威を防御し、統合のためにデータを守る方法を模索しています。また、信頼できるパートナーとしてCloudflareを選択するITリーダーが増えています。

Cloudflareのデプロイの柔軟性と構成可能なアーキテクチャにより、あらゆる企業がデバイス、アプリ、ネットワーク全体のパフォーマンスを保護およびスピードアップすることが可能で、同時にハイブリッド環境の勤務体制を保護し、生産性を向上させることができます。このため、Cloudflareでは、管理者やユーザーの接続元に関係なく、エンドユーザーのエージェントレスオンボーディング、危険なトラフィックを含むクライアントレスのWeb分離、セキュリティとネットワークサービス全体を可視化する統合管理ダッシュボードをサポートしています。Cloudflareの広大なグローバルネットワークにより、エンドユーザーに近い場所でセキュリティを適用し、遅延の最小化、従業員に対する円滑なエクスペリエンスの提供を実現しています。CloudflareのAnycastアーキテクチャは、インターネットの混乱を回避する役割を担い、それによってチームのオンライン状態を維持し、ビジネス継続性の確保につながります。

Cloudflareの統合されたSSEとSASEプラットフォーム、そしてZTNA、CASB、DLP、およびSWGとの間で環境を共有することにより、セキュリティポスチャーを強化すると同時に、終始一貫した管理ワークフローを通じて実装を簡略化しています。アイデンティティとデバイスポスチャー属性を同一にすることで、ZTNAとCASBの両アクセスポリシーと、SWGポリシーへの通知が可能になり、企業全体でのポリシー管理がシンプルになります。

ZTNA、リモートブラウザ分離、メールセキュリティは、リソースに条件付きのアクセスを提供するために併用できます。その一方でメールやコラボレーションツールを通じて忍び寄る悪意のあるコンテンツ（リンクや添付ファイル）から隔離します。管理対象でないデバイスを使用する請負業者とユーザーには、コーポレートリソースへのユーザーによる操作（アップロード/ダウンロード、コピー/貼り付け、キーボード入力など）を無効にする制限付きアクセスを提供し、データの侵害を回避して、機密データを検出するために他のL7 DLPポリシーを提供することもできます。



お客様の声



Cloudflareは、2024年度Gartner® Peer Insights™ Voice of the Customerのゼロトラストネットワークアクセス（ZTNA）部門でカスタマーズチョイス認定を獲得²

「Cloudflare Accessは従来のVPNサービスの代替品として素晴らしい製品です。ユーザーはブラウザを開いてログインするだけ。追加のソフトウェアをダウンロードして設定する必要はありません」

— Platzi、クラウドエンジニアリング部長

「絶妙なタイミングでCloudflare Accessに出会えたおかげで、面倒なVPNデプロイメントをしなくて済みました。当社にとっては選びやすく、デプロイは驚くほどシンプルでした」

— ezCater、セキュリティ責任者

「社内アセットへのアクセスを制限する場合、AccessはVPNより格段にシンプルで安全です。アクティブにしてユーザーを追加するだけなのに、完ぺきに機能します」

— Bitpanda、CTO兼共同創業者

「Cloudflareを実装する前は、アプリケーションを安全にデプロイするための準備に2週間から4週間必要でした。Cloudflare Zero Trustを導入してからこうした時間が約90%も削減されました」

— Creditas、ネットワークエンジニアリングチームリード

アナリストのコメント：



Cloudflareは2023年の『IDC MarketScape for Zero Trust Network Access (ZTNA)』で「リーダー」に選出

IDCは、Cloudflareの「企業のセキュリティニーズを満たすための積極的製品戦略」を理由として挙げています。この評価は、どんな規模の企業でもゼロトラストの導入を始められ、VPNを使わずにすべてのユーザーをすべてのリソースへ安全に接続できるように支援する姿勢の妥当性が認められたものと、当社は考えています。



Cloudflareは2024年の『KuppingerCole Leadership Compass for ZTNA』で「リーダー」に選出

KuppingerCole Analysts AGは2024年のZTNA市場分析で、有機的に開発された完全統合型セキュリティプラットフォーム、大規模なグローバルクラウドインフラストラクチャ、圧倒的な市場プレゼンスなど、Cloudflareの強みをいくつか挙げています。

Accessの機能

安全なアクセスのためにゼロトラストポリシーを作成/編集する	
きめ細かい、カスタムアクセスポリシー	一元化された ポリシー管理 エクスペリエンス。L7アプリはサブドメインとパスレベルでワイルドカードとマルチホスト名サポートにより保護、 CORSリクエスト をサポート。ポリシーの変更は数秒でグローバルに拡散。 ポリシーテスター を内蔵。
広範なリソース：保護される対象と仕組み	リソースは、 セルフホストアプリ （クラウド/オンプレミス）や インブラウザSSH/VNC のリバースプロキシ、 SaaSアプリ のアイデンティティプロキシ、 プライベートサブネット内のWeb/非Webリソース （任意TCP/UDP）へのクライアント/トンネル方式プライベートルーティングのL4-7フォワードプロキシ*に、パブリックホスト名を使用。 双方向トラフィック のリソースやワークフロー（VoIP/SIP、CI/CDパイプラインなど）もサポート。
ID	すべての大手企業とソーシャル アイデンティティプロバイダー （IdP）を通して認証。複数IdPの同時認証を含む。汎用 SAML と OIDC コネクタも使用可能。サポート（および適用可能）対象は、IdPが提供する任意の認証メソッド、 一時認証 、 目的正当化 、グローバルまたはアプリ/ポリシーセッションごとの再認証間隔、およびアプリまたはユーザーごとの即時セッション 無効化 オプション。 デバイスクライアント（WARP）を認証メソッド （WARPセッションごとにキャッシュされたアイデンティティ）として使用可能。
デバイスポスチャ	デバイスクライアントとサードパーティのエンドポイント保護プラットフォーム（EPP）統合を使用して デバイスポスチャ を検証。ゼロトラストポリシーにEPPリスクスコアを取り込むには、サービス間 統合 を使用。
ポリシーのコンテキストシグナル	メールグループ、IPアドレス範囲、ジオロケーション、ログイン方法（MFAタイプ、IdPタイプなど）、有効なmTLS/SSH証明書、サービストークン、シリアルナンバーリスト、デバイスポスチャ属性、インストールしたデバイスクライアント、セッション時間、SWGルール適用などの シグナル や、 外部API呼び出し からのシグナルを設定。 Microsoft Entra ID（Azure AD）の条件付きアクセス の認証コンテキストを直接参照することも可能。
他の関連するサポート	<ul style="list-style-type: none"> ● SCIM：セルフホスティングやSaaSアプリ（OktaおよびAzure ADなど）にユーザーを自動でプロビジョニング、またはプロビジョニング解除 ● 内部DNS：ローカルドメインフォールバックの設定とプライベートネットワークリクエストの解決 ● スプリットトンネリング：プライベートネットワークまたはVPNの反対側での実行にIPを含める/除外 ● mTLS認証：IoTおよび他のmTLSユースケース向けの証明書ベースの認証 ● アプリの分離：超高速リモートブラウザで1つのチェックボックスによりアプリを分離*
オンランプとオフランプ	
アプリコネクタ	シンプルなおークストレーション を実現する軽量なアプリコネクタ（ Cloudflare Tunnel ）がVMインフラストラクチャやスループットの必要なく、Cloudflareへのリソースの接続を円滑化。 モニタリング 、 仮想ネットワーク （IPオーバーラップ用）、 冗長性とフェイルオーバー の機能機能を含む。
デバイスクライアント：使用するタイミング	<ul style="list-style-type: none"> ● クライアントレス：ゼロトラストポリシーを非管理デバイスを使用するサードパーティユーザーに拡張適用。クライアントレスリモートブラウザ分離やL7 DLPポリシーとの併用も可*。WebアプリとインブラウザSSH/VNCに対応。 ● クライアントベース：デバイスクライアント（Cloudflare WARP）がプライベートネットワークへ安全なアクセスを拡張し、サービス間のデバイスポスチャの統合を実現。また、オンプレミスのユーザーに場合に依じたポリシーを適用するために位置認識機能を装備。プライベートネットワークを作成するために、2つまたは3つのWARPを実行する任意のデバイスに接続可能。ユーザーは自己登録またはMDM経由でデプロイ可能。
拡張性と可視性	
ページのカスタマイズ	自社のブランディング、またはエンドユーザーエクスペリエンスを効率化するために個々のアクセス手順を挿入するブロックおよびアプリランチャー画面にカスタムHTMLをアップロード。
ログ	包括的ログ ですべてのリクエスト、ユーザー、デバイスのログを記録。 logpush またはAPIを使用して既存のSIEM、おークストレーション、分析ツールと統合可能。不明なアセットについては、社内インフラストラクチャ用 Cloudflare Shadow IT Discovery がユニークなトラフィックを受動的にカタログ化することで、すべての配信元を表面化。
自動化	直感的なAPI と Terraformプロバイダー が利用可能で、Zero Trustの実装に伴うあらゆる側面をプログラマ的に管理。また、自動化されたサービスをサポートするユーザーレス サービストークン を提供。

*ゼロトラストプラットフォームの他の部分で機能を使用

Cloudflareを選ぶ理由



簡単なセットアップと管理

アプリコネクタソフトウェアとトンネルオーケストレーションを使用して、プライベートリソースへのオンライントラフィックの設定と運用を根本から簡素化しましょう。



シームレスな常時接続体験

CloudflareのグローバルなAnycastテクノロジーにより、エンドユーザーのピークパフォーマンスとネットワーク障害への耐性を実現し、信頼性を確保しましょう。



アーリーアダプターによる迅速なイノベーション

常に同業他社を凌駕する革新によって高速で安全性の高いアプリケーションアクセスを提供するプロバイダーと共に、インターネット自体の進化に後れを取らず対応しましょう。

お客様の企業にとっての簡単かつ安全なアクセスについてご不明な点やご要望をお聞かせください

ワークショップを依頼する



担当者へのご相談前にさらに詳しい情報をご希望の場合は、

当社の[SASEレファレンスアーキテクチャ](#)で詳細をご確認ください。
また、その仕組みは[ゼロトラストプラットフォームを説明するインタラクティブツアー](#)でもご覧いただけます。



- 2023年調査: techvalidate.com/product-research/cloudflare/charts
- Gartner, Voice of the Customer for Zero Trust Network Access, 2024年1月30日にアクセス、同業者投稿 GARTNER、PEER INSIGHTS、およびThe Gartner Peer Insights Customers' Choiceバッジは、Gartner, Inc.ないしその関連会社の商標で、ここでは許可を得た上で使用しています。All rights reserved. Gartner Peer Insightsのコンテンツは、個々のエンドユーザーがプラットフォーム上に挙げられたベンダーを使ってみた経験に基づいて形成した意見で構成されており、事実の記述として解釈すべきではなく、Gartner社またはその関連会社の見解を表すものでもありません。Gartnerは、このコンテンツで記述するいかなるベンダー、製品、サービスも推奨しておらず、このコンテンツに関して、明示または黙示を問わず、正確性や完全性の保証（商品性や特定目的への適合性の保証を含む）もしていません。