

Acronis

MSP サービスの パッケージングと 価格設定の手引き

MSP 事業者向けガイド



目次

03	04	06	07
はじめに	MSP 事業者のチャレンジと課題	MSP に不足しているのは何か？	MSP サービススタックとプロセス
09	17	21	
収益機会を理解する	MSP がアプローチを変えるのに役立つソリューションは何か？	総括	

はじめに

今日のビジネスの状況と技術トレンドは、マネージドサービスプロバイダー（MSP）への期待を高めています。MSPが提供するサービスに対する需要はかつてないほど増加していますが、需要によってもたらされる複雑さも増加しています。つまり、多くのMSPは収益性とビジネスゴールのギャップの間の微妙なバランスを取っているということです。

収益ソースは、誰なのか、何なのか？ オペレーションをより効率的に管理して高品質なサービスを提供しつつ、収益性を維持する方法とは何でしょうか。

このガイドを使って、MSPがPL（損益）の計算とその応用を最適化することで、収益性を確保する方法をご覧ください。



MSP 事業者のチャレンジと課題

脆弱性を突く攻撃経路がかつてないほど多くなっています。特に、世界的なパンデミックの影響でリモートワークのトレンドが始まってからはなおさらです。COVID-19の猛威が広がった時期から、サイバー犯罪が300%増と驚異的に増加しており、MSPは顧客を確実に保護することが急務となっています。

MSPの対応をより困難にしているのは何か？ 1つは、今やデータはいたるところにあるため、保護がより難しくなっています。これによって、MSPが通常使用するセキュリティツールの有効性が弱くなっており、従来の方法では57%の攻撃が見逃されています。

関連する手動による作業も、この新しいより分散した環境で調整を図れるよう多数のベンダーやシステムが関与しているため、増加の一途をたどっています。69%のセキュリティ専門家は脅威を管理することよりも、多くの時間をツールの管理に費やしています。

しかし、これは残念な側面ばかりではありません。 顧客は環境の保護と管理に役立つソリューションをますます求めるようになってきているため、MSPにとっては、ここにチャンスがあります。貴社の顧客はサイバーセキュリティの重要性をますます認識するようになってきているものの、ほとんどの企業にはこうした複雑な脅威に対応するための十分な知識が不足しています。



要するに、MSPは顧客のリスクの削減と信頼関係の構築に努めながら、同時に複雑性、セキュリティ、コストと戦う必要があるのです。

ワークロードやデバイス、リモートワークが増えることで、MSPは以下の問題に直面します

- セキュリティインフラの限界に挑む高度な脅威や攻撃
- ますますリスクにさらされる境界、そして異質で分散したリモートワークやセキュリティインスタンス
- セキュリティ人材の不足

そしてMSPの顧客はサービスプロバイダーに要求する自社の課題とゴールをもっています

- デジタルトラストは革新を可能にするものとみられています
- SMBのリーダーはセキュリティの運用コストが予測可能であることを求めています
- 従業員の生産性が高く、データ損失やダウンタイムから確実に復元できるようにします

過去においては多くの企業が、セキュリティを革新を阻むものと考えていました。現在では、デジタルトラストをビジネスの重要な特性として利用しています。このような考え方の変化は、MSPがより良いデジタルトラストの構築によって収益を増やす機会をもたらしています。セキュリティの運用コストを予測可能にし、顧客の事業予算に適合する必要があります。「専門用語」と増え続けるセキュリティコストは終わりを知りません。

今こそセキュリティサービスを最新化するチャンスです 顧客を保護し、顧客と貴社のリスクを減らすことができます。

サイバー脅威の状況はより複雑になっています

300%

COVID-19 パンデミック中にサイバー犯罪が急増

57%

の攻撃が従来のウイルス対策ソリューションで見逃されています

69%

が脅威に対する防御よりもツールの管理に時間をかけています

出典: Acronis Cyberthreats Report 2020、
Acronis Cyber Readiness Report 2020、FBI



MSP に不足しているのは何か？

どの組織もセキュリティ侵害から完全に保護されることはありませんが、必要不可欠なセキュリティソリューションは今日容易に入手することができます。残念ながら、このようなソリューションは特定の機能やカテゴリーに偏っている傾向があり、統合や相互運用がほとんどなされていません。これは脆弱性診断やパッチ管理、システムヘルスおよびパフォーマンス監視、ディザスタリカバリなどに当てはまります。

また、ベンダー間のばらつきも問題です。ソリューションどうしの相性が良くないとセキュリティに重大なギャップやオーバーラップを残し、貴社の人員やプロセスにリソース負担を掛けます。各ベンダーのソリューションで必要となる、さまざまなセキュリティおよび管理手順の数、トレーニング時間、文書量などを考えてみましょう。さらに、コストや複雑さ、脆弱性も加わります。

各種コンソールの管理、請求やオンボーディング/オフボーディングのセットアップによってタスクは膨れ上がります。こうした状況はどの企業も、MSP も、当然ながら望みません。



MSP サービススタックとプロセス

平均的なMSPのサービススタックやプロセスを考える場合、ベンダー間のまとまりのなさが今日のビジネス拡大に対する最大の脅威になることが容易にわかります。

システムヘルスおよび
パフォーマンス監視

バックアップと
ディザスタリカバリ

ランサムウェア対策/
マルウェア対策

報告

リモート管理および
アシスタンス

パッチ管理

脆弱性診断



人的リソース/プロセス

- › セキュリティおよび管理の手順
- › トレーニング
- › ドキュメント

運用管理コスト

- › コンソール
- › 課金
- › オンボーディング/オフボーディング

技術

- › ライセンス
- › メンテナンスおよび変更管理



過剰なサービス提供の場合、ツールが適合しない可能性があり、これらのソリューションの責任がすべてチームの上にのしかかります。この種のベンダーのばらつきは内部リソースを消耗するため、エンドポイント膨張と呼ばれます。

エンドポイント膨張は、複数のベンダー技術を取り扱うために企業が費やさなければならない、拡張を続けるリソースのことです。各顧客が異なるソリューションを実行する可能性があると考えてみましょう。顧客が10社あるとすると、それぞれのワークステーションは10種類の異なるベンダーソリューションによって占有されています。これらの複数のシステムそれぞれが、独自の、時に相反するシステム要件と要求を持っています。

それが脆弱性の入り込む余地を与えます。 [Absoluteの2021 Endpoint Risk Report](#)によると、70%の侵害はエンドポイントから発生し、多くのセキュリティツールが競合し、マシンのリソース競合が発生するため、デバイスが1年以内に、暗号化の失敗をひき起こす可能性が高くなっています。

この問題はMSPだけのものであることに**注意すべきでしょう**。大企業には単一のベンダーを使う余裕があり、社内チームが1つの画面からすべてのオペレーションを処理することもできます。そのため、こうした組織がコンプライアンスや監査の要件を満たすのが容易になります。

MSPは労力をかけずに管理する必要があります。 MSPは大企業が購入するような大規模なセキュリティチームを持たず、しかも予算面での制約があります。そのため監査やコンプライアンスが大幅に複雑になります。MSPがサービスを提供する小規模なビジネス顧客のほとんどでは、サイバーセキュリティの予算が年間\$5,000を超えることは稀です。これはMSPにとってかなり大きな問題です。

MSPが成功するためには、より明確なシナリオが必要です。

収益機会を理解する

MSPはサービス価格の仕組みを最適化することで。これらの問題を解決できます。まずMSPが提供できるさまざまな種類の価格プランを考察しましょう。

ア・ラ・カルトの価格設定

顧客は、自分に関連性のある個々のサービスを、使わないサービスへの支払い義務なしで選択できるようにします。

ユーザー単位の価格

これには各ユーザーに対する一律料金が含まれます。ユーザーの複数デバイスのすべてが対象で、台数は関係ありません。

一律料金

一律料金形式ベースの標準モデルは「AYCE (all-you-can-eat)」と短縮されることがあります。一律価格には、単一料金で顧客に提供されるすべてのサービスが含まれます。使用されるサービス数には関係ありません。

バンドル価格またはポートフォリオティア価格

別名SLAベースの価格とも呼ばれ、このモデルはさまざまなレベルのサービスパッケージを提供します。一部のサービスは他のものより優れており、この構造により顧客は購入するサービスを選択できます。



バンドル価格またはポートフォリオ価格は、必要なサービスのレベルによって変わります。MSP顧客によっては、Eメールセキュリティやファイルバックアップを必要とする倉庫担当者がいたり、ディザスタリカバリも含む、より大型のパッケージ化されたサービスを必要とする財務や人事、法務の担当者がある場合があります。

さまざまなMSPがサービスを、顧客に提供する方法に応じて異なる選択を行っています。1つあるいは2つの価格オプションを提供する場合もあれば、すべてのオプションを提供する場合もあります。最終的には、収益性を維持しながらサービスを提供できるかどうかで貴社ビジネスに最適なサービスが決まります。

利益と利益転嫁

価格設定において収益性にかかわる考え方を明確にします。

売上総利益率は、純粋な利益として残る売上の割合です。売上総利益率は、売上から総売上原価（Cost of goods sold 略してCOGSまたは直接コスト）を引いて、それを売上で割ることで計算できます。割った値が売上総利益率になります。この割合は売上に対してどれくらいの利益を得たかを示します。

売上総利益率 =
$$\frac{\text{売上} - \text{COGS}}{\text{売上}}$$

マークアップは、原価よりも高く設定した商品とサービスの価格で、ビジネスが利益を得るための一般的な方法です。基本的にマークアップは、原価に上乗せして顧客が支払う金額です。マークアップは利益を総原価で割ることで把握できます。

マークアップ =
$$\frac{\text{利益}}{\text{コスト} \times 100\%}$$

希望する利益を得ていますか？

サービスはMSPの主要な収益源であるため、できるだけ多くの利益を得ることが重要です。経常収益モデルを使用した場合、平均的なMSPは、提供するサービスの40%の売上総利益率を期待できます。しかし、更なる改善は可能でしょうか？

サービスの利幅を設定するときに注意深く検討しましょう。マークアップはビジネスを行う上でのシンプルな現実です。商品を原価で販売する場合、利益は出ません。実際には損失を出す可能性があります。基本原価の150%で売値を決めた場合、損益は五分五分でしょう。

150%を超えるマークアップだと、そこで初めて実際の利益が出ます。さらに、基本原価の175%～200%のマークアップだと、高収益性を実現できます。





価格についてよく聞かれる質問

MSPが2つの主要な問題に直面していることは明確です

- 最適なサービス提供プラットフォームの構築と保守
- 自社と顧客の両方が導入可能な バランスのとれたコストと価格フレームワークの作成

最適なサービスプラットフォームによって、顧客はお手頃な価格ですぐれたサービスを得たと実感でき、同時に収益性を維持できます。これはとても重要なポイントです。

質の低いサービスプラットフォームの場合、価格を安価に設定しないと顧客が不満を感じます（この場合、収益率と長期的成功が犠牲になります）。同様に、サービスの質は高くても価格が高すぎる場合、顧客はより安価なオプションを探すようになります。これも収益性に悪影響を及ぼします。

よく聞かれる質問例 MSPが自問し、自社サービスが十分な価格付けがされているかどうかを判断できます

- ❓ **利益が出ているかどうかはどうしたらわかるか？**
- ❓ **収益化が可能なサービスの部分はあるか？**
- ❓ **顧客への値上げをどのように合理的に説明できるか？**

利益につながる価格設定

利益を得るために適性な価格設定を行うことは、MSPが成功するための基本です。**サービスの価格設定では、以下3点について考慮する必要があります。**

- 人件費
- 製品コスト
- 必要な利益率

適正価格の決定は複数のステップから構成されるプロセスです。最適な料金を計算するためにこれらの数値を使用する方法

ステップ1 人件費の計算

最初のステップは単なる給与や従業員に支払われる料金ではありません。例えば、従業員が時給\$25とすると、年間の基本給は\$52,000となりますが、この従業員の年間人件費はは実質的にもっと高くなります。

人件費の内訳

- › 基本給
- › その他収入
- › 所得税
- › 諸経費
- › トレーニングおよび教育
- › 諸手当

右の表に示されるように、時給\$25の従業員は年間\$52,000の基本給の負担ではなく、年間約\$72,000の人件費になります。これが従業員の**実際**のコストです。

また、**人件費を計算するよりシンプルな方法があります**。従業員の基本給を1.3倍（30%増）すると、従業員の人件費の実際のコストに近い数値が算出されます。平均以上の生活費がかかる一部の地域では（ニューヨークやサンフランシスコなど）、より正確で簡略化されたコストを反映するために、35%に近い、より大きな値を掛ける必要があります。都会から離れた地域では、この値をより現実的な25%に下げることができます。最も重要なことは、事業運営の状況を正確に反映することです。右表の計算に基づくと、時給\$25の従業員は実際には、時間当たり\$34のコスト負担になります。これは利益の出るサービスの価格設定方法を決定するために使用できる信頼性の高い数値です。

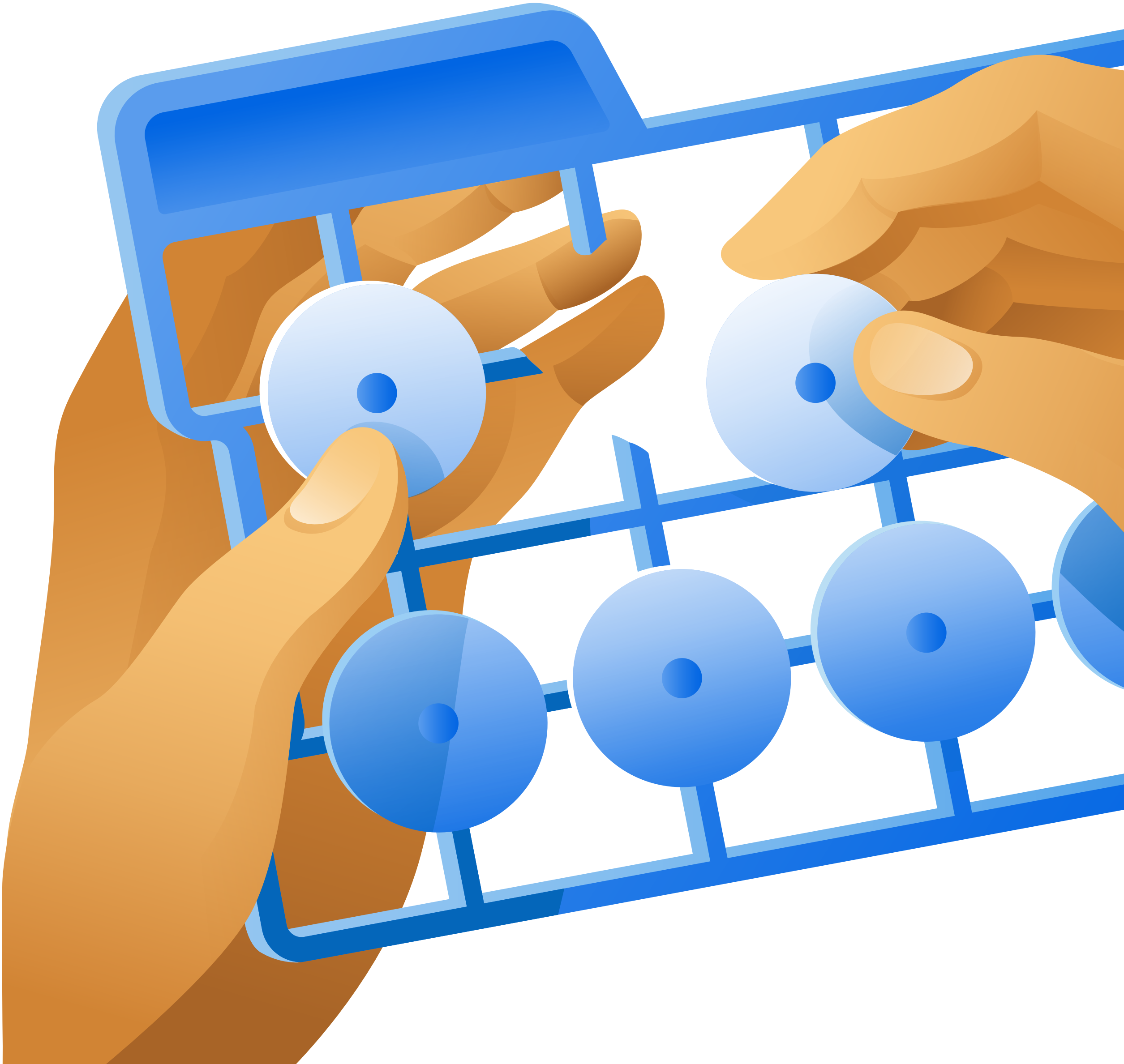
		月間	年間	人件費ベース
給与		4,333.33	51,999.96	70,199.95
手当	率			
従業員の税金 - 社会保障	6.200%	268.67	3,224.00	
従業員の税金 - 医療保険	1.450%	62.83	754.00	
従業員の税金 - FUTA	0.600%	26.00	42.00	
従業員の税金 - SUTA	1.000%	43.33	80.00	
諸経費	5.000%	216.67	2,600.00	
労災費	5.600%	242.67	2,912.00	
医療 / 歯科費用		750.00	9,000.00	
年金 / 退職	3%	130.00	1,560.00	
福利厚生総額		1,740.17	20,171.99	
人件費総額		6,073.50	72,171.95	70,199.95
年間作業時間			2,080	2,080
時間単位の人件費			34.70	33.75

ステップ2 製品コストの計算

サービスのコストはいくらですか？顧客に信頼できる機能を提供するために、統合されたヘルプデスクサービス、Microsoft 365、エンドポイント監視、税金管理、バックアップ保護、およびその他多数のサービスが必要になります。

これらのコストは負担となりますが、こうしたサービスの価格をカバーする際にアクロニスのサービススイートはMSPに競争優位性を提供します。

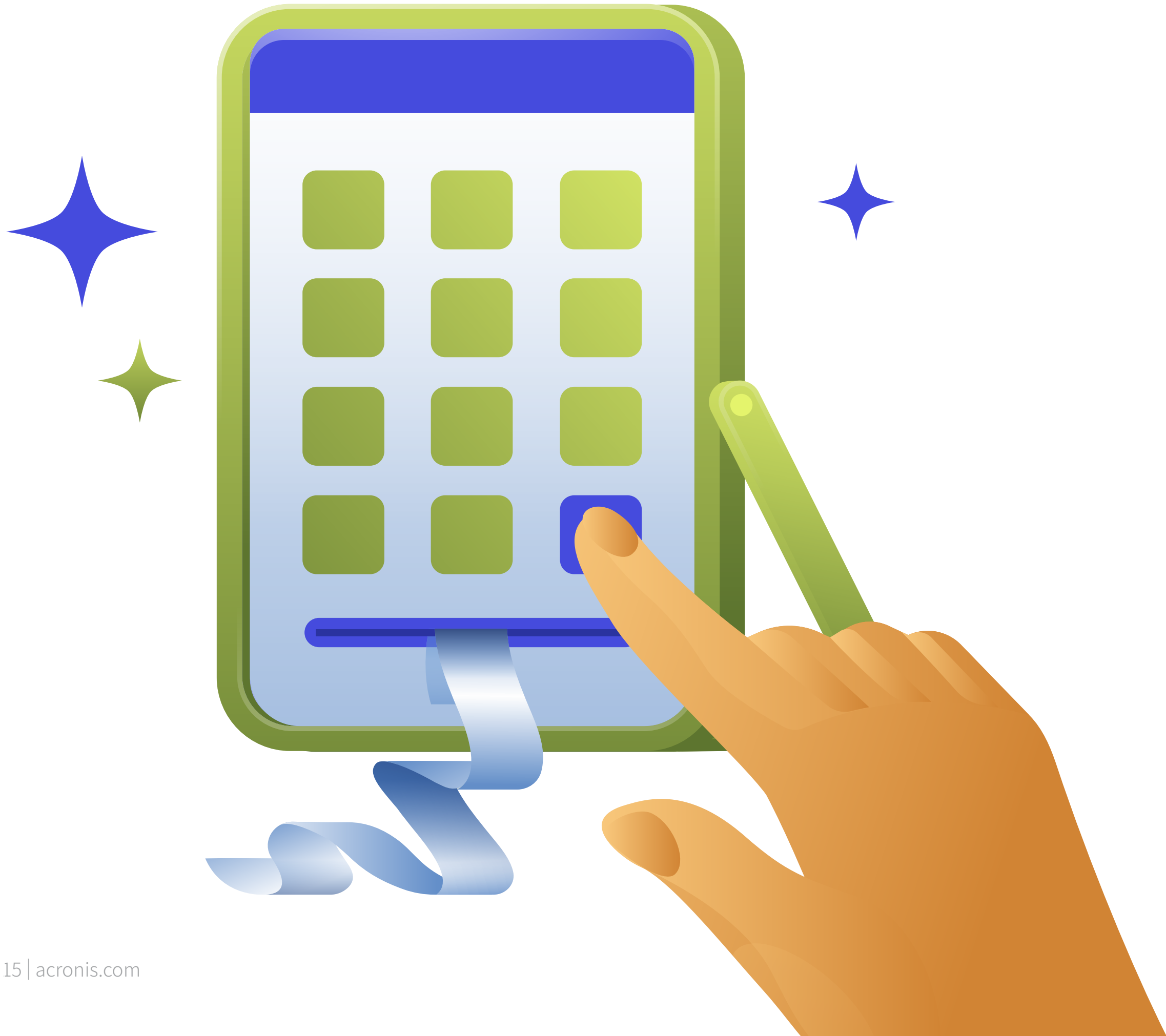
現在の価格設定およびサービススケジュール	アクロニスが提供するサービス
ヘルプデスクサービス	—
Microsoft 365 ライセンス	Acronis Cyber Protect Cloud + Advanced Email Security、Microsoft 365バックアップ
Windows ライセンス	—
バックアップライセンス	Acronis Cyber Protect Cloud + Advanced Backup
エンドポイント保護ライセンス	Acronis Cyber Protect Cloud + Advanced Security
ネットワーク監視および管理ライセンス	—
デバイスおよびパッチ管理ライセンス	Acronis Cyber Protect Cloud + Advanced Management
トレーニングコスト	アクロニス #CyberFit アカデミー



ステップ3 サービス価格の算出

シンプルなサービス価格試算ツール

より良いサービス価格の設定を支援します。



定数	利益率	掛け率				
売上総利益率	40%	1.40				
希望する利益率	50%	1.50				
人件費掛け率		3.50				
ユニット単位 またはデバイス 単位	ユニット	ユニットコスト	コスト合計	ユニット価格	最低価格	利益率
Acronis バンドル サービス	15	25.47	382.05	38.21	573.08	
物理サーバー	1	–	–	–	–	
高度バックアップ サーバー	1	–	–	–	–	
仮想マシン	4	–	–	–	–	
労働時間/ ユニット/月	0.25	32.50	121.88	28.44	426.56	
合計			\$503.93	\$66.64	\$999.64	49.6%
推奨バンドル 価格				\$99.00	\$1,485.00	66.1%

サービスで50%の利益獲得が目標である場合、ステップ1で決定した人件費乗数を使用する必要があります。この場合、人件費の乗数は3.5で、これは3.5–4の適正ゾーンに入っています。これは諸経費をカバーし、納得できる利益率であることを保証します。

次に、顧客向けに提供するサービスについて詳述します（前段落の例には多くのアクロニスサービスが含まれます）。各サービスに対して使用中のユニット数、各サービスの総原価、当該サービスで顧客に請求する価格を入力します。これにより、サービスの請求可能な最低価格が自動的に得られ、さらに利益を計算します。

この例では、49.6%の利益率を維持するために顧客に請求する最小額は\$999.64です。しかし、試算ツールの最終行では、初期結果より若干高い推奨バンドル価格になることに注意してください。この場合、\$1,485のバンドル価格を請求することで、66.1%の利益を出します。

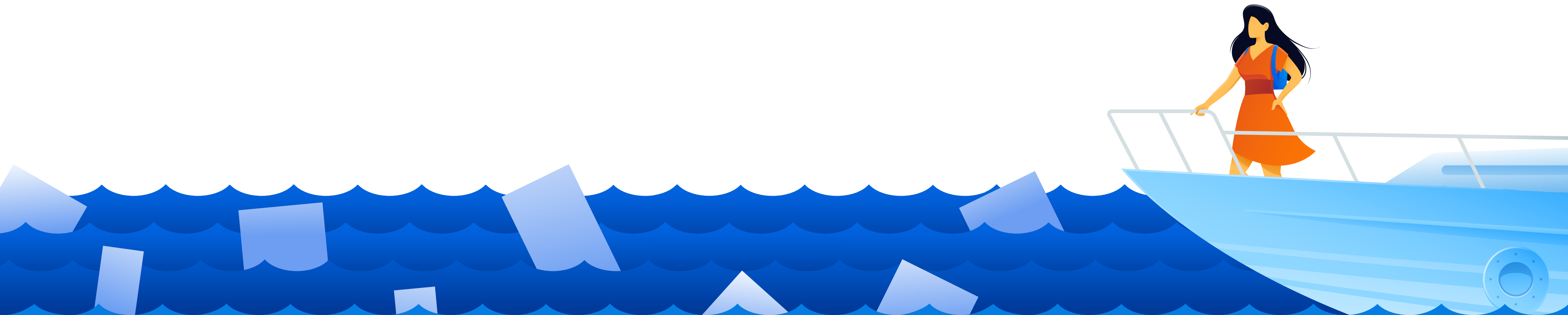
ビジネスコストをカバーし、初期費用の2倍以上の見返りがあるため、**MSPにとってこれはかなり良い利益率です**。以上がMSPが次のレベルの利益を達成する仕組みです。

定数

- › 会社全体の売上総利益率
- › 希望する製品利益率
- › 請求率用の人件費乗数

価格計算

- › ユニット単位
- › 拡張



MSP がアプローチを変えるのに役立つソリューションは何か？

増加する複雑さと変化を続ける需要によって、MSP は微妙な立場に置かれています。最近の Forrester の調査結果によれば、MSP の利益率は平均すると現在 17% ほどです。収益性低下の主な問題は、MSP がより柔軟なビジネスモデルに移行できなかったことです。

典型的なデバイス単位やユーザー単位の価格モデルを使えば、顧客はシンプルに「イエス」、「ノー」を判断することができます。代わりに、個別のサービスオプションを提供する場合（基本的に「良い」「もっと良い」「最高」の判断になります）、顧客が購入する際の判断基準は「購入すべき」や「購入すべきでない」から「最適なソリューションはどれか」に変わります。これらの追加オプションも、長期的には顧客へのアップセルの機会を増やします。

これはより良い市場参入戦略です。この戦略は、顧客の 15% は最小のオプションを選択していること、60% は中位のオプションを、25% は最高オプションを選択することを想定しています。このパターンは顧客の事業規模と一致しています。

スタートアップ

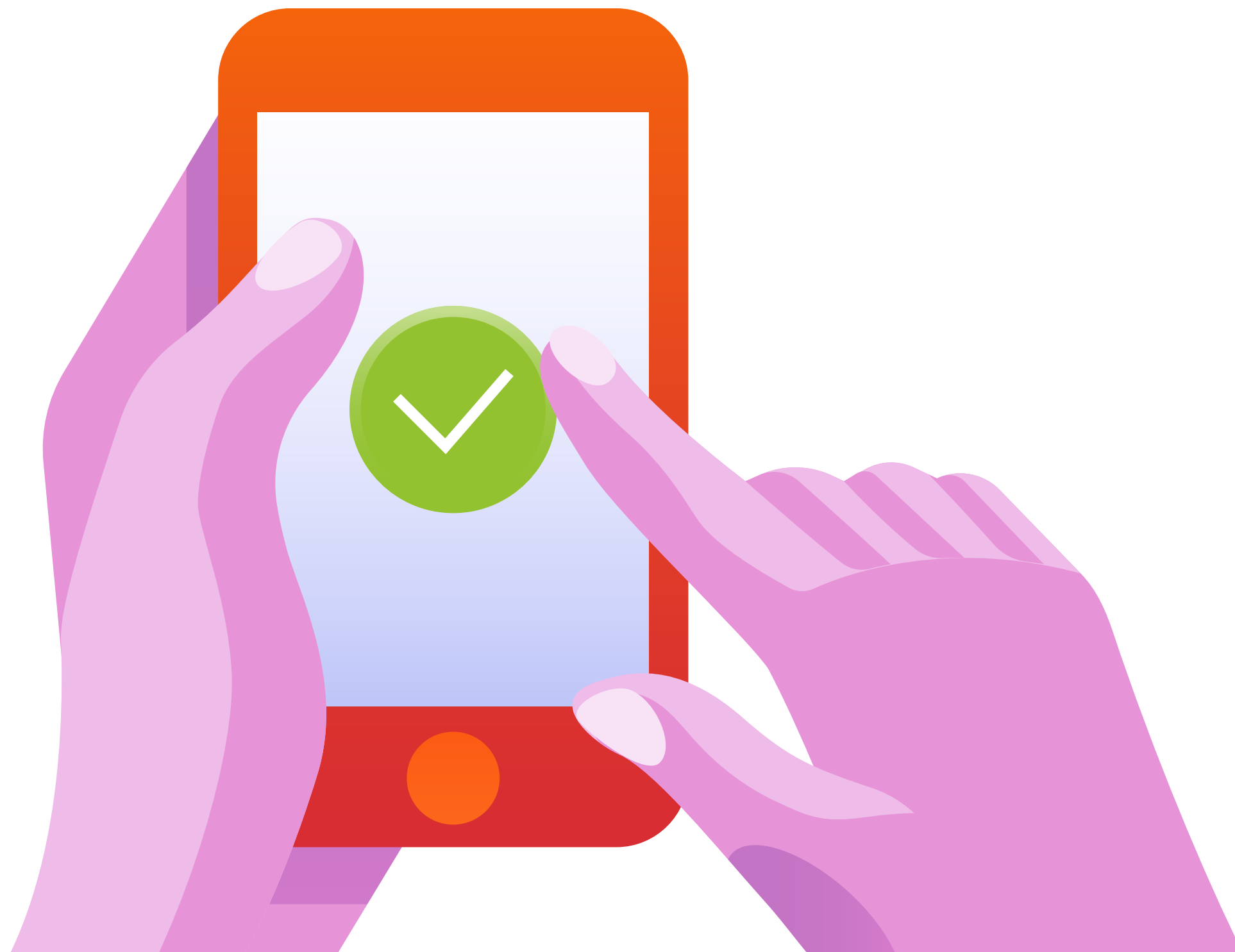
年間経常収益（ARR）\$100 万以下のビジネスに最適

急成長

年間経常収益（ARR）\$100 万 - 1000 万のビジネスに最適

エンタープライズ

年間経常収益（ARR）\$1000 万以上のビジネスに最適



異なるニーズに合わせたプラン

3種類のビジネスモデルに対してアクロニスの価格設定がどのように働くかを検討します。

\$69

Kiosk 従業員

- ✓ Eメールセキュリティ
- ✓ ウイルスおよびマルウェア対策保護
- ✓ VoIP (OmniVoice)

\$99

事務職員

- ✓ Eメールセキュリティ
 - ✓ ウイルスおよびマルウェア対策保護
 - ✓ VoIP (OmniVoice)
 - ✓ URL フィルタリング
- ネットワークセキュリティ
ハードウェアおよびソフトウェア管理
ファイアウォール
- ✓ パスワード管理
 - ✓ アップグレードおよびパッチ

\$159

事務職員

- ✓ Eメールセキュリティ
 - ✓ ウイルスおよびマルウェア対策保護
 - ✓ VoIP (OmniVoice)
 - ✓ URL フィルタリング
- ネットワークセキュリティ
ハードウェアおよびソフトウェア管理
ファイアウォール
- ✓ パスワード管理
 - ✓ アップグレードおよびパッチ
- 2FA
- ✓ ドライブのヘルスマニタリング
 - ✓ 継続的データ保護
 - ✓ 報告
 - ✓ ファイル同期と共有 + 電子署名
 - ✓ ディザスタリカバリ



これらは互いに矛盾するプランであるとは限りません。これらのオプションのすべてが1つの顧客に対して適用可能であるとともに、費用対効果が高いという状況になる可能性があります。

適切なベンダーの選択

貴社のサービス提供に対して顧客のベンダーパートナーを精査することが重要です。これは一般的レビューのプロセスとして使われるべきだと言えるでしょう。例えば、貴社が10年以上営業している場合、創業時に比べて現在では、さまざまなベンダーを使用している可能性が高くなっています。

ベンダー精査のプロセス中に問うべき質問

- ? 現在所有しているツールは何ですか？
- ? ツールは期待通りに動いていますか？
- ? ツールをどのように使用していますか？
- ? 現在のスタックはサイバー脅威から保護しますか？

上記回答に基づいて実行すべきこと

- ... 利益を得るために価格モデルを選択する
- ... 一連の適切なサービスを選択する
- ... 新規サービスをスタンドアロンまたはアップセル提供としてパッケージ化する
- ... 有望なリードを探す
- ... 成功する売り込みを作成する

予期せぬ運用管理負荷を管理し、計画外の作業を排除する

効率性が向上すると収益性も向上するのは周知の事実です。
今日効率性のカギになるのは自動化です。

人的ミスの可能性および非効率性を削減するためには、MSPはできるだけ多くのタスクを自動化する必要があります。PSA、RMAツール、さらにはセキュリティツールはすべて自動化できます。プロアクティブな修正手段を搭載するポリシーベースの自動化を配備すると、生産性が向上します。ソフトウェア配備を自動化し、パッチを管理し、環境全体の問題をプロアクティブに解決します。

リスクを軽減し、より良いサービスを提供して利益を増やす

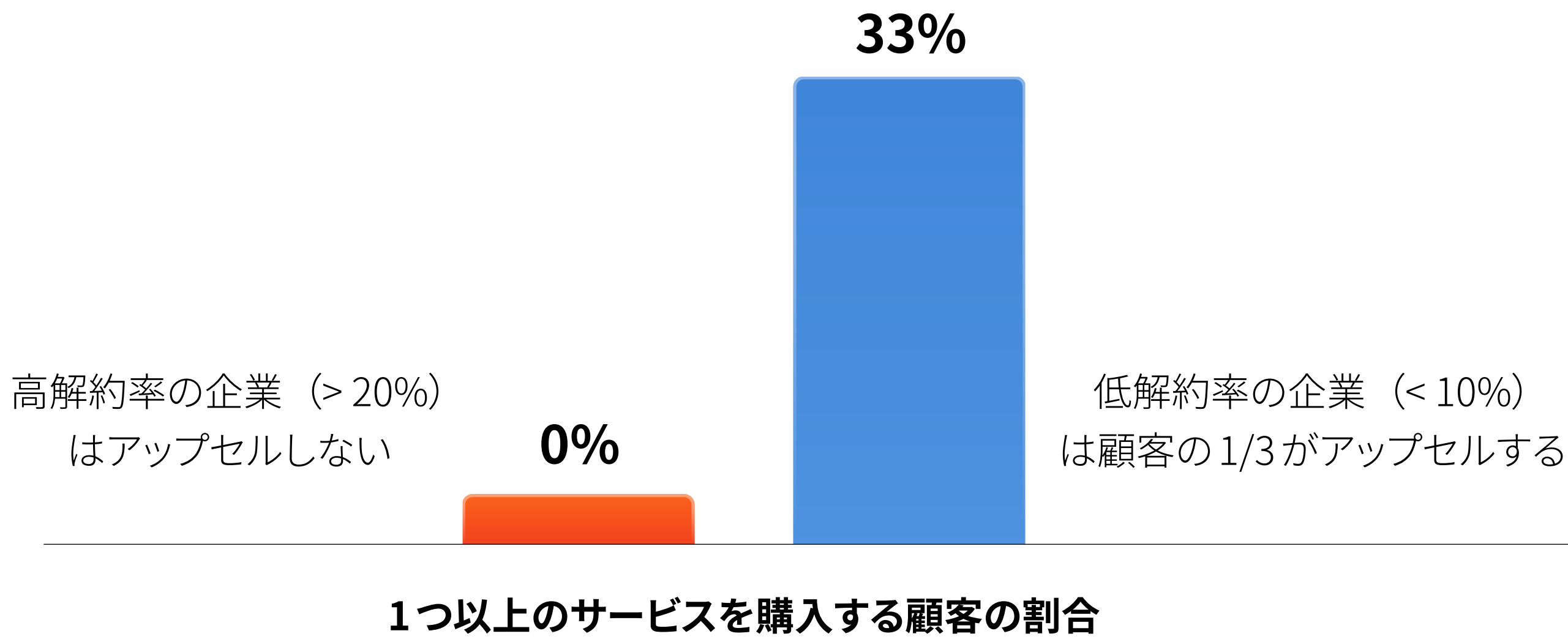
サービスオプションのアップセルが成長へのカギです。ほとんどの組織は、新規顧客の獲得がビジネス拡張を推進するカギとみなしています。しかし、サブスクリプションモデルを採用している場合はそれだけではありません。

サブスクリプションモデルでは、新規サインアップ数だけでなく、顧客の解約率や顧客獲得当たりのコストにも注目します。顧客の解約率や顧客獲得当たりのコストは、ビジネスの成長において新規顧客よりも大きな役割を演じます。特にアップセルは成長企業が顧客解約率を解決（獲得する新規顧客と解約する顧客との間の比率）する方法です。顧客にもう提供できるものはないと告げるのではなく、より良い

サービスレベルを提供することで顧客を維持し、新規顧客を獲得するプレッシャーから解放されます。

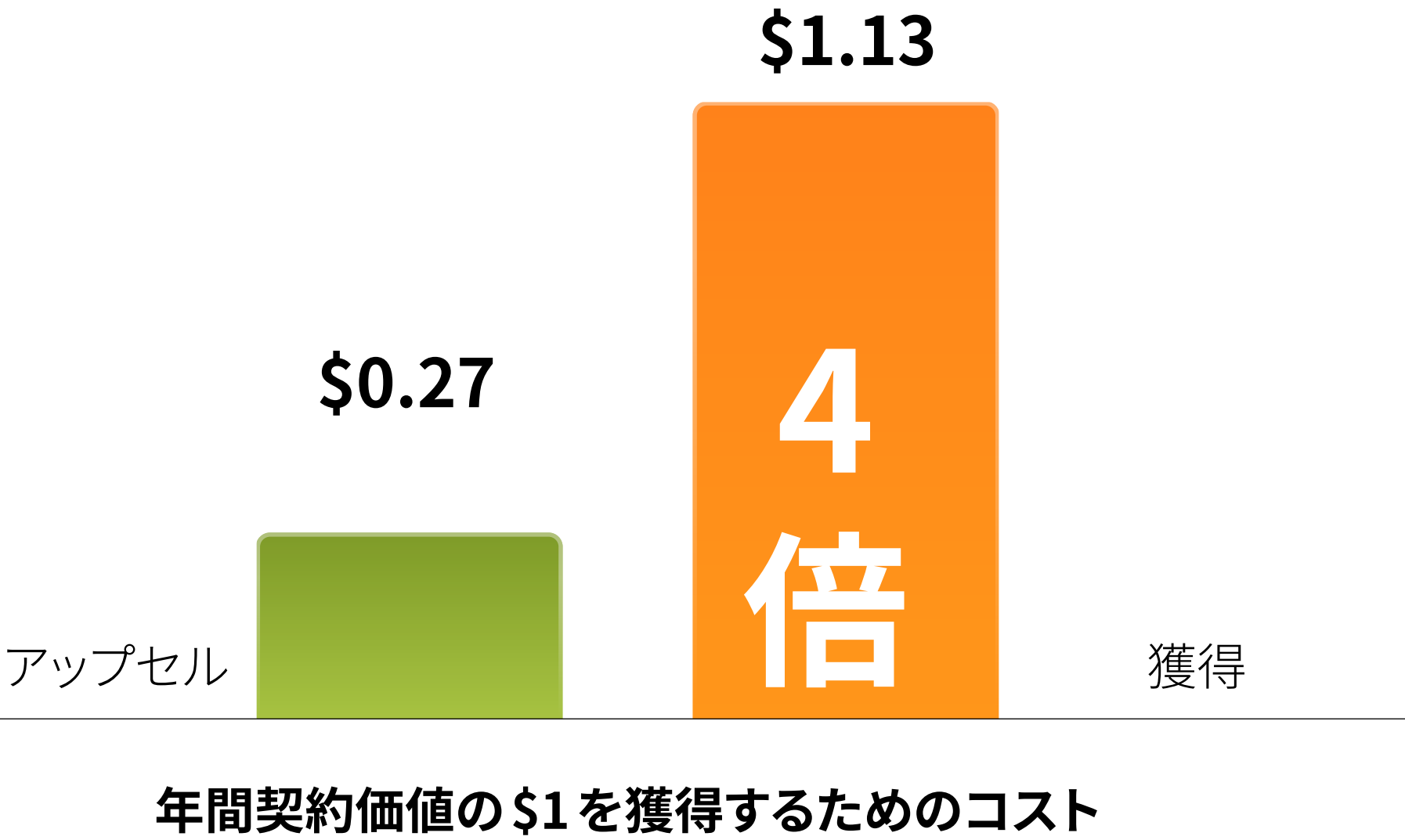
以下のグラフが示すように、新規顧客を獲得するのは既存顧客にアップセルするよりも4倍コストがかかります。このことから、次のサービスティアのメリットが一目瞭然であるため、継続を検討している顧客にアピールすべきです。

顧客の解約を防止



1/4 のコストで実現

新規顧客獲得とより高いサービスレベルの提供を比較



総括

収益性を得る道はMSPにとって困難であり、かつてないほど複雑になっています。ユーザーが求める変化に対応し続けるために、顧客のサービス導入の全体的な複雑さを削減することによって利益を最大化できるよう、アクロニスはMSPにシンプルで分かりやすいソリューションを提供します。

アクロニスが企業の収益性をどのように高めているのかについては、[収益性ワークショップビデオをご覧ください。](#)

Acronis

アクロニスについて

アクロニスは、データ保護とサイバーセキュリティを1つのソリューションに統合し、現代のデジタル社会の安全、アクセス性、プライバシー、真正性、セキュリティ (SAPAS) 問題の解として統合と自動化されたサイバープロテクションを提供します。サービスプロバイダーやITの専門家の需要に適う柔軟なデプロイメントモデルを用意し、アクロニスはデータ、アプリケーション、システムに革新的な次世代のアンチウイルス、バックアップ、ディザスタリカバリ、そしてAI応用エンドポイントの保護管理ソリューションなどの優れたサイバープロテクションを提供します。アクロニスは、最新のマシンインテリジェンスおよびブロックチェーンベースのデータ認証テクノロジーによる高度なソフトウェア対策で、クラウドからハイブリッド、オンプレミスまで、どのような環境でも予測可能な低コストで保護します。

2003年にシンガポールで設立され、2008年にスイスで法人登録されたAcronisは現在、19カ国の34拠点に2,000人以上の従業員を擁しています。アクロニスのソリューションは550万人以上の個人ユーザーおよび、50万社以上の企業や一流のスポーツチームに信頼されています。アクロニスの製品は150カ国で25言語に対応し、5万社のパートナーとサービスプロバイダーが販売・提供しています。詳細はwww.acronis.comをご覧ください。

