

IT 運用管理、 ヘルプデスク、MSP、 IT チームの生産性 改善への近道



目次

IT 運用管理、ヘルプデスク、MSP、IT チームの生産性改善への近道3

API によるインテグレーションへの依存とその長所、短所、課題4

無秩序な運用管理ツールの増加によるコスト増5

求められる統合ソリューション6

IT ソリューションベンダーの成熟度が重要8

まとめ10

参考資料.....11

追加リソース.....12



IT 運用管理、ヘルプデスク、MSP、IT チームの生産性改善への近道

Karl W. Palachuk 執筆

2019 年 12 月にボーイング社が国際宇宙ステーションとのドッキングを目指すスターライナー宇宙船を打ち上げました。このミッションは単純で、宇宙船の打ち上げを成功させて国際宇宙ステーションとドッキングし、無事地球に帰還するというものです。

打ち上げの 55 分後に NASA はスターライナーが「軌道投入失敗」に陥ったと発表しました。これは技術的な問題により宇宙船の軌道が狂ったためです。

このため国際宇宙ステーションとのドッキングができなくなりました。つまり、ミッションが失敗したということです。ただ幸いなことに宇宙船は無人のテスト飛行でした。

絶対的な精度が求められる世界でどうして「失敗」が起きたのでしょうか。答えは非常に単純で、2 つの異なるソフトウェアシステムがお互いに通信が出来なくなったというものです。完全でオープンな通信を提供するよう想定されていましたが、それでも欠陥がありました。搭載されている時計の時間が違っていたために、宇宙船が所定の時間にいるべき空間にいなかったのです。

少し検証してみましょう：NASA、SpaceX、ボーイングは 3 社とも協力的でオープンに連携して一緒に働くことを約束していました。そして、意欲的に同じ目標に向かって取り組んでいました。誰もが同じ方向を向いて、同じ結果を求めていました。

ボーイング社はそのために総額で 15 億ドル費やしました。それでも失敗してしまいました。

この話から複雑性、相互交流、ソフトウェアの有効利用の難しさについての教訓が得られます。チームメンバ全員が設計仕様に合意し、完全にオープンで良く文書化されたプラットフォーム上にシステムを構築したとしても、失敗する可能性があります。

ここで、開発者がチームではなく競合であるような環境を考えてみましょう。各当事者は、アプリケーションプログラミングインターフェイス（API）を通じて接続する方法についての仕様を公表しますが、お互いのプログラムのインターフェースや仕様は開示しません。

その結果、システムはより複雑かつ非効率になりリスクが増大します。

API によるインテグレーションへの依存とその長所、短所、課題

技術は日々進化し続けています。一般的に、技術の革新は 10 年単位と言われている中で、IT は 18 か月から 24 か月で技術の革新が登場します。IT の世界では、5 年間新技術の追従を怠ると時代に取り残されます。

近年のシステムは、API によるインテグレーションへの依存度が高まっています。API は、2000 年代初めから、アプリケーションの連携、情報交換、プロセスの自動化を実現する手法として利用されています。

現に、API は多くのマネージドサービスで利用され、さまざまなツールの連携を可能にしてきました。しかし API は、システム連携の機能や動作連携を実現する一方、その導入費用は、高額になることもあり、サービスコストの負担も大きくなります。

当初は、戦略的で優れた API も、今日においては、システムを「つぎはぎだらけのフランケンシュタインのような怪物」を造ってしまう原因とも考えられます。

現在の API の課題について考えてみましょう。API は非常に成熟しています。しかし、最高のプログラミングを伴う最高の状況下でさえ、API 接続を管理する必要があります。2 つの異な



る企業のソフトウェアを接続する場合、どちらかの側で変更を加えると API による連携が取れなくなる可能性があります。2 つの企業間をサードパーティで使って接続する場合、さらに複雑になります。

どのような接続にも最低限の管理が必要になります。また、どの接続もセキュリティホールになるリスクがあるため、監視する必要があります。ランサムウェアはサイバー犯罪者の中では、今やビジネスとなり IT サービスプロバイダーがデータ盗難やコード拡散において格好の標的になることを知っています。すべての攻撃と同様に、犯罪者は最適な侵入ポイントを探し、そこに攻撃を集中します。つまり、考えられるすべての侵入ポイントを防御しなければなりません。

ソフトウェア開発には知られたくない秘密があります。それは、メンテナンスとサポートのコストが常にソフトウェア自体のコストを超えるということです。(IT サービスプロバイダーとして、サポートを一部おこないビジネスをしているため、このことを理解しています。)これに加えて、一連の接続によって、監視やメンテナンス、サポートの必要性が増加します。

無秩序な運用管理ツールの増加によるコスト増

さまざまなベンダーの運用管理ツールの導入コスト加えて、「無秩序な運用管理ツールの増加」（ツールスプロール）によってトレーニングや統合、メンテナンスのコスト増加につながります。Gartner の調査によると、ツールが複雑になると複数の領域でコストが増えることが指摘されています。つまり、API の「課題」が明らかになり、さまざまな個別のソフトウェアを導入すると効率性が落ちるということです。各接続ごとに複雑さや文書化作業、トレーニングが増え、さらにはメンテナンスを必要とするインテグレーションが必要になるためです。

複雑で相互接続されたシステムのメンテナンスを実行するということは、全体的な生産性を直撃するということでもあります。メンテナンスに費やす 1 時間は、エンドユーザーへの支援が絶たれる 1 時間ということです。

Forrester Research がおこなった最近の調査では、レガシーツールへの依存が、テクノロジーのモダナイゼーションやデジタルトランスフォーメーションの大きな障壁となっているのが分かっています。

さらに、その調査で 86% の企業が少なくとも 1 つのレガシーツールを使用しており、完全に統合された最新の運用管理ツールを使用しているのはわずか 12% でした。

このような旧式で接続機能が十分でないツールに依存することで、環境のサポートコスト増加、サービス提供の低下、セキュリティリスクの増大につながっています（詳しくは以下で説明）。複数のツールを使用する際のもうひとつの頭痛の種となるのは、インテグレーション費用です。ほぼ半数の企業（46%）が、「ツールごとのさまざまなセキュリティプロトコルを維持し、統合するのにコストと時間がかかりすぎる」と報告しています。

それに加えて、複数のツールによる機能重複が発生しています。言葉を変えると、同じ機能に 2 回も 3 回もコストをかけているということです。いずれの場合でも、少なくとも 1 つのツールは他のツールで同様の機能を使用しているため、統合された機能を完全に使用しているわけではありません。このような重複した機能は、ほとんどのツールが複雑さやリソース不足のために十分活用されていないということを意味します。

つまり、ほとんどの企業は、シームレスにインテグレートされていない様々なベンダーの複数のツールを使用しています。また、重複した機能をもつツールに費用をかけているため、メンテナンスコストや初期ライセンス料金が増加しています。各製品をツールセットに追加すると、オペレーション運用により多くのトレーニングや監視、ドキュメント管理が必要になります。

しかしこの状況に悲観する必要はありません。

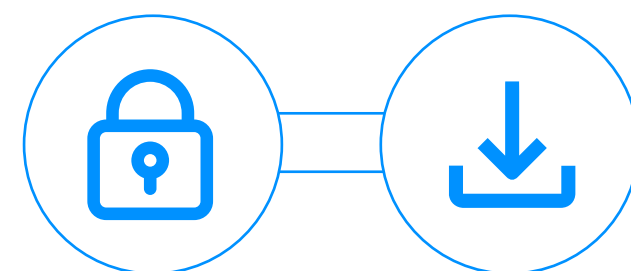
求められる統合ソリューション

今や API がすべての解ではありません。いま IT の世界では、IT ツールの組み合わせではなく、インテグレートされた統合ソリューションが求められています。つまり、API の支配から解放される方向です。

複雑さはソフトウェア開発とメンテナンスにおいて非効率の要因です。予想される通り、複雑さはメンテナンスやセキュリティ、サポート業務のコスト増加につながります。

例 1

2 つのソフトウェア・ソリューションと 1 つのコネクタがある場合、1 社から 3 社のパートナーと連携する必要があります。ベンダーのいずれかが、API の変更をおこなったり、悪用される可能性のある脆弱性をもたらしたりするリスクもあります。



例 2

3 つのソフトウェア・ソリューションと 2 つのコネクタがある場合、1 社から 5 社のパートナーと連携する必要があります。ここでもベンダーのいずれかが、API の変更をしたり、悪用される可能性のある脆弱性をもたらすリスクがあります。



例 3

それでは、新しく登場したセキュリティアプリケーションの「統合された」世界を見てみましょう。これらのアプリケーションは最初から連携するように設計されています。そして、同一ベンダーによってすべてが設計構築されています。



バックアップ用、マルウェア対策用、リモートデスクトップサポート用、管理用に別個のシステムを持つと多数の接続を持つことにもなり、それぞれの接続が脆弱性や環境内の潜在的な脅威ベクトルに相当します。例を挙げて説明すると以下の通りです。

バックアップとウイルス対策のような 2 つのアプリケーションとサービスを接続したいとしましょう。これにはいくつかのバリエーションがあります。これらは同じ企業によって構築されているのか？最初から連携するように設計されているのか？2 つのシステムの間には接続がある場合、当該企業によって書かれたのか？またはサードパーティか？

ソフトウェアの複雑さを改善すると、効率性改善、メンテナンス削減、セキュリティ強化という恩恵を受けられるようになります。また、アプリケーションスタックを連携させるサードパーティのミドルウェアに対する支払いがなく、追加のアプリケーションを管理するのに必要な追加の管理時間がないため、最初からコストを削減できます。

サービスプロバイダーの間でベンダー疲労と呼ばれる問題が大きくなっています。これはつまり、システムを想定通りに稼働させようとする結果、多数の企業からコストが殺到するために起こります。

1 つの企業がこの問題に正面から取り組みました。アクロニスは相互にシームレスに動作する製品スタックを構築しました。Acronis Cyber Protect はボトムアップで設計されており、複雑さを減らし、総所有コスト（TCO）を削減することで最大の効率を得ています。アクロニス製品マーケティングマネージャーである Lauren Beliveau は「当社は単に各製品を提供するだけでなく、ソリューションスタックを提供しています」と述べています。

これは単に理論的な問題ではありません。セキュリティの世界では、レガシーツールの古い「寄せ集め」では深刻な脅威となり、監視を強化する必要があります。それぞれの接続は潜在的な脆弱性になりますが、パッチやアップデートもそうです。パッチを適用するだけでなく、

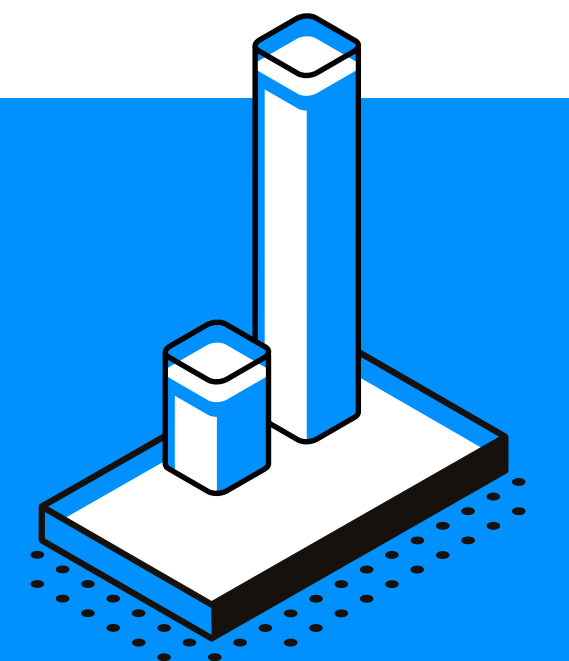
問題が発生しないように監視が必要です。時には、脆弱性が発生したためパッチを削除して再パッチする必要があります。

残念ながら、パッチ適用で広く使われているアプローチは、追加の問題や非互換の問題、弱点が発生しないことを確認するために、一定の期間待ってパッチを適用するというものです。このやり方は、アプリケーションを既知の脆弱性に長時間さらしてしまいます。

さらに、さまざまなベンダーからの寄せ集めで、アプリケーションの統合が不十分だと、データ、アラート、自動化、文書、ユーザーインターフェース、エージェントなどの共有ができない恐れがあります。接続の弱点はセキュリティの弱点です。今日、こうした弱点のリスクとコストは無視できないほど大きくなっています。

Acronis Cyber Protect を使うと、アンチウイルスはバックアップがあることを認識し、それをスキャンします。完全に統合されたソリューションとともに、バックアップやアンチウイルスのようなツールがより効率的に連携します。バックアップは、ウイルスやマルウェア、ランサムウェアのような脅威がないかスキャンされ、データがクリーンであることを保証します。パッチはライブシステムだけでなくバックアップにも適用されます。すべては文字通りシームレスに行われます。

ソフトウェアの複雑さの軽減は、効率の向上、メンテナンスの低減、生産性の向上、およびセキュリティの強化を意味します



IT ソリューションベンダーの成熟度が重要

忘れてはならないというひとつの要因は、IT ソリューションベンダーの成熟度です。企業がスタートアップから十分に成熟した企業に成長するにつれて、いくつかの段階を通ります。最初は、単一機能（例えば、ウイルス対策）の未成熟な製品を提供します。時がたつと、製品が十分に機能するようになります。企業がスタートアップから確立された企業になると、市場への製品投入に焦点を合わせ、さらには収益を得ることもあります。

確立したスタートアップは機能の充実と接続性に注力します。そのため、なんでもできる API を利用するようになります。この段階の目標は、だれとでも接続することです。この段階は、おそらくもっとも暫定的なものです。ほとんどの場合うまくはいきますが、API は成熟していないため、すべてが常に変化します。API 連携に成功すると、ユーザーはより多くの機能を求めるために次の段階に進み、基盤を拡張することになります。

基盤の拡張に注力する企業は、新機能の購入や構築にも注力します。この段階での戦略は、機能の拡張と競合他社との協力を通じて顧客を得ることです。最終的なビジョンはユーザーの要求に応え、ツールセットをより多くしてマーケットシェアを獲得することです。また、この拡張段階は、大きな内部変化を迎える時であり、API の進化に常に対応するときでもあります（進化は内的なもの、購入したり統合したりする製品間のもの、製品と競合製品間のものがあります）。

次の段階は財務の拡大です。ベンチャーキャピタルを通じてか、または他の資金調達元を通じてかを問わず、企業を拡大するために資金が必要になる時期があります。その結果顧客への対応力低下につながります。マネジメントが機能から資金調達にフォーカスをシフトするにつれて、問題解決や機能追加よりも売上が重要になります。

これは何年にもわたって続けられてきた合併による問題にも見られます。顧客対応に優れたベンダーが突然方針転換し、製品戦略やロードマップが不透明になります。この段階では、企業内の活動が売上のみに集中し、開発（問題解決含む）は大幅に削減されます。

長期に生き残って十分に成熟し、またシームレスに連携してよく統合されたツールを開発し、重要となるのは企業の成熟です。技術上の問題に加えて、成熟した企業はセールスやカスタマーサポートと同様に開発の継続に必要な資金調達を行うというパターンに落ち着きます。

技術の変化が年々早くなるにつれて、新しい課題に対応する新しい機能が必要になります。この事実は他のどの分野よりもサイバーセキュリティに当てはまります。10 年前、ウイルスは迷惑で破壊的でした。今日では、ダウンタイムのコストに加えて、高額の身代金が必要になっています。

成熟しきれていない企業や合併・買収によって軌道がそれた企業は、旧式の製品にとらわれています。多くの場合これらの企業は時間がなかったり、資金がなかったり、あるいは進化し続けるセキュリティ環境の要求についていけなかったりすることがあります。



旧式のソリューションがあったとしても、そのソリューションは新しいツールと連携しません。

ツールセットの複雑さが増加するにつれて、効率性は下がります。複数 API の問題への対応に加えて、さまざまなレベルの成熟度の API や文書を持つ企業によってサポートされるさまざまなレベルで成熟したソフトウェアの内部動作を管理する必要があります。

ユーザーは、すぐれたスタックを構築したいと思っています。場合によっては、これは異なるベンダー製であったとしても「クラス最高」の選択肢を探すことを意味します。効率性と収益を増加させるために、可能な場合はいつでも、単一のスタックを購入します。

Acronis Cyber Protect を使えば、世界最高レベルのソリューションを手に入れることができます。アクロニスはデータ保護と復元のリーダーとして広く認められており、データ、アプリケーション、システムを保護する世界最高レベルのソリューションを構築し、トラブルの多いミドルウェアを排除しています。

Acronis Cyber Protect には、バックアップアップイメージへのパッチ適用を含めて、競合他社には追随できない機能が揃っているため、復元手順はクライアントマシンのセキュリティレベルをロールバックできません。

ランサムウェアによる数百万ドルの訴訟や政府規制が伴う 2020 年代は金銭や連携を望むセキュリティツールを構築する労力を無駄にする時代ではありません。最先端の機能とセキュリティを提供し、しかも複雑さ、メンテナンス、コストを削減するソリューションが必要です。完全な統合ソリューションとして設計構築されたセキュリティスタックにに向かって歩みだしましょう。

まとめ

「Acronis Cyber Protect によって、当社は他のソリューションなら 10 個のツールが必要なプロテクションを 1 つのソリューションでおこなっています」

Jason Menezes、
Datategra 社バックアップおよび
ディザスタリカバリ部長

セキュリティはもはやアプリケーションの追加機能ではありません。現在の技術コンサルタントは、ユーザーがビジネスを遂行できるようにしながら、比類のないセキュリティを提供する堅実で総合的なソリューションを持つ必要があります。

複雑さは効率性と生産性を低下させ、その一方でメンテナンス、文書化、トレーニングをおこなうコストを増やします。「部品」が増えればコネクタも増えます。戦略的にシームレスに動作するように設計構築された、完全に統合されたスタックは全体的なセキュリティを最大化するとともに、複雑さとコストを削減します。

API も従来からの選択肢の一つですが、いったんサーバーセキュリティとデータ保護のリーダーであるアクロニスの完全に統合されたスタックに移行すれば、複雑で相互接続されたシステムを生産的に管理することができるようになります。

システム連携は重要です。しかし、統合ソリューションはベストなソリューションです。

参考資料

* 参考資料は全て英語となります

<https://www.msn.com/en-us/news/technology/boeings-software-troubles-show-an-engineering-culture-clash/ar-BB16xEdq>

<https://www.forbes.com/sites/jonathanocallaghan/2019/12/20/boeing-starliner-spacecraft-launches-to-the-international-space-station-heralding-a-new-era-for-american-human-spaceflight/>

If This Then That

<https://ifttt.com/>

Zapier

<https://zapier.com/>

プログラム可能な Web

<https://www.programmableweb.com/>

Salesforce.com

www.salesforce.com

Harvard Business Review、「API の戦略的価値」

<https://hbr.org/2015/01/the-strategic-value-of-apis>

「Gartner によると、3 つのベストプラクティスを使えば組織はソフトウェアコストを 10% 削減可能」

<https://www.gartner.com/en/newsroom/press-releases/2016-07-19-gartner-says-organizations-can-cut-software-costs-by-30-percent-using-three-best-practices>

Forrester Research、「レガシーツールの普及によって企業の革新力が麻痺」

<https://sciencelogic.com/wp-content/uploads/sciencelogic-os.pdf>

「ツールチェーンの無秩序な増加に苦労していますか？それはあなただけではありません」

<https://dzone.com/articles/toolchain-sprawl-youre-not-alone>

執筆者について



Karl W. Palachuk は、カリフォルニア州サクラメントで 2 つのマネージドサービスビジネスを構築し販売しています。彼は Sacramento SMB IT Professionals Group の創立者兼社長で、『The Network Documentation Workbook and Managed Services in a Month』をはじめとする数冊の著書を執筆しています。

また、Karl 氏は 15 年以上にわたって世界中でカンファレンスやセミナーで講演しており、ゴンザガ大学で学士号、ミシガン大学で修士号を取得し、Microsoft Certified Systems Engineer も取得しています。また、Microsoft Small Business Specialist でもあり、Microsoft の Small Business Specialist Advisory Panel のオリジナルメンバーです。

追加リソース

CASE STUDY

HomeBuys Looks to Do More with Less with Acronis Cyber Protect 15

Retail upstart able to consolidate multiple IT tools for backup, antimalware, remote desktop, and patch management into a single console.

INTRO

HomeBuys is a discount retailer established in 2015 with six locations in Ohio and one in Kentucky. Its founders, who have decades of experience in retail – most notably with the Big Lots brand – wanted to offer an uncommon experience to customers. To do so, HomeBuys utilizes closeout buying opportunities from major big box retailers and other sources, thereby passing the savings onto its customers on high quality items from food to wine to home décor. With a constantly changing inventory, the retailer lives by its tagline: “The Best for Less.”

CURRENT IT ENVIRONMENT AND SECURITY SOLUTIONS USED

HomeBuys’ IT environment encompasses its six stores, one distribution center, and its corporate office. Not surprisingly for a retailer, the most mission-critical application infrastructure is its ERP system, NetSuite, which was migrated to relatively recently from Microsoft Dynamics. In terms of data protection, the company uses Unitrends for bare metal backup and restore and an appliance from iDrive for backup and restore of virtual environments. For endpoint protection of workstations and laptops, HomeBuys uses a combination of LogMeIn and Windows Defender, while some servers use McAfee.

In total, HomeBuys’ network administrator Jorge Alexandres is responsible for protecting more than 1.5TB of historical data. The retailer does not currently use Acronis. Acronis Cyber Backup had been previously evaluated but at the time it did not have the right functionality and integration for Microsoft Dynamics.

Then Alexandres received an invitation to participate in the beta program of Acronis Cyber Protect 15. The product’s value proposition interested him, so he joined the beta.

BETA IMPRESSIONS

- Easy to install and use
- Powerful, multi-purpose tool

PROTECTED RESOURCES

- 1.5TB
- 30 workstations
- 4 servers

OPPORTUNITY AHEAD

- Consolidate three separate IT tools
- Gain operational and financial efficiencies

www.acronis.com

Copyright © 2002-2020 Acronis International GmbH.



アクロニスブログ：世界中のサイバープロテクションリーダーが発する最新情報とインサイトを提供

アクロニス YouTube チャンネル：事例、デモ、サイバー脅威分析および企業ニュースを頻繁に発信

アクロニスリソースセンター：サイバープロテクションに関するホワイトペーパー、電子書籍、詳細記事、チュートリアル、インフォグラフィックスなど

アクロニスイベント：参加に関する詳細を含むイベント、ウェビナー、インタビューなどに関する連続シリーズ

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](#)を組み合わせで統合され、自動化された[サイバープロテクション](#)を提供し、セーフティ、アクセシビリティ、プライバシー、真正性およびセキュリティ（[SAPAS](#)）の問題を解決します。サービスプロバイダーや IT のプロの要求に適う柔軟な配備モデルを使って、アクロニスは革新的な[次世代のウイルス対策](#)、[バックアップ](#)、[ディザスタリカバリ](#)、[エンドポイント保護管理](#)ソリューションを搭載する、データ、アプリケーションおよびシステム向けの優れたサイバープロテクションを提供します。受賞歴のある[AI ベースのマルウェア対策](#)および[ブロックチェーンベースのデータ認証](#)技術を採用して、アクロニスは[クラウドからハイブリッド、オンプレミス](#)にいたるまで、どのような環境でも保護します。

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アクロニスは現在、18 カ国に 1,500 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 万人以上のホームユーザーおよび Fortune 1000 や一流のプロスポーツチームを含む 50 万社以上の企業に信頼されています。アクロニスの製品は 150 カ国で 40 言語に対応し、50 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。

