M&Aがデータセキュリティに及ぼす影響

EquifaxとMarriottのデータ漏洩が示すもの

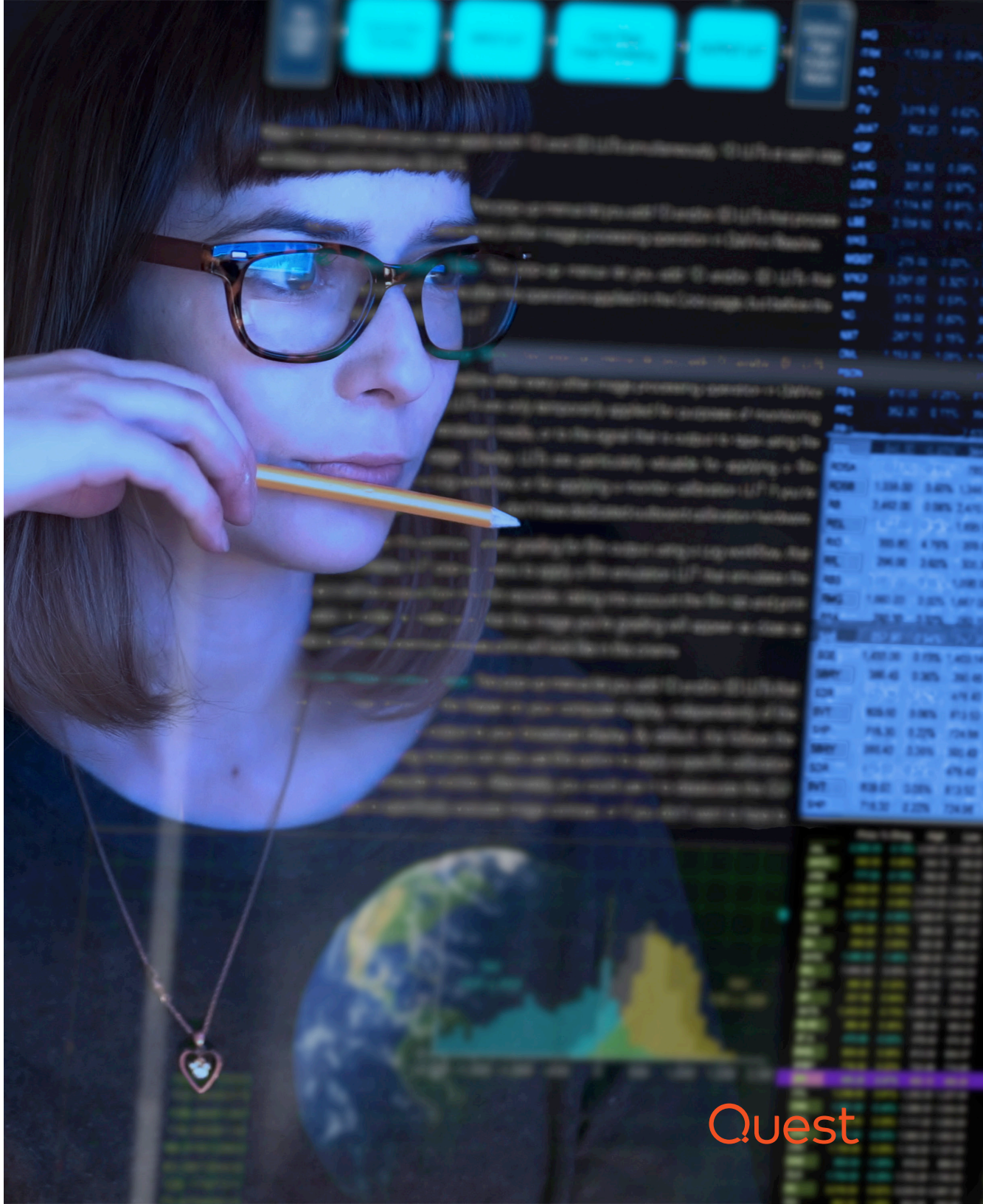
Quest

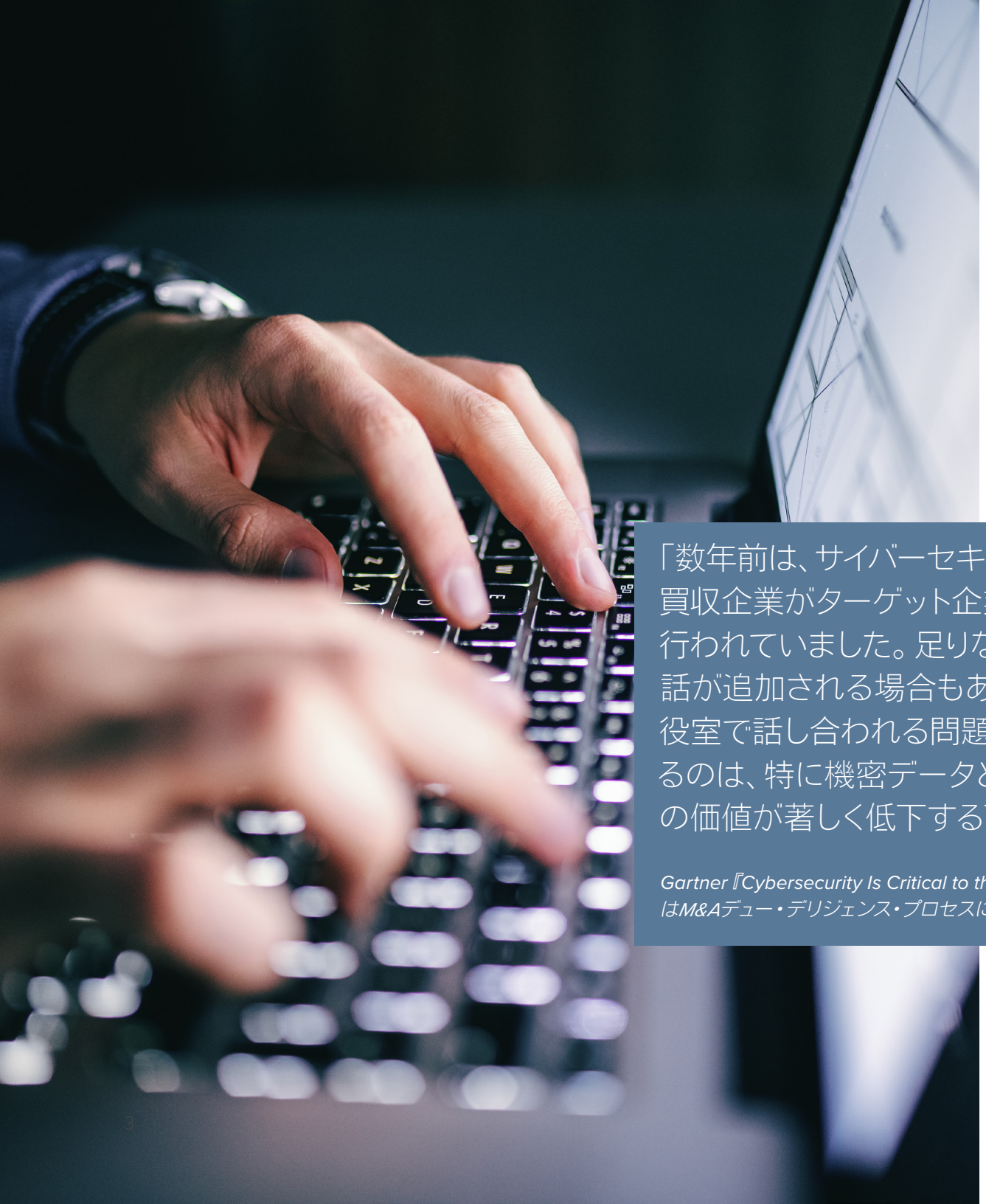
はじめに

適切なIT統合は、M&Aのシナジーを達成するために不可欠

2018年は大型で複雑なM&Aの当たり年であり、今年はさらに大型化することが見込まれています。Deloitteの2019年M&Aトレンドレポートによると、米国に本社を置く企業のM&A担当幹部の76パーセントおよび国内未公開株式投資会社のM&Aリーダーの87パーセントが、自社の取引の成立数が翌年も増加すると予測しています。さらに、回答者の70パーセントが、そうした取引が2018年より大型化すると予想しています。

M&Aの主な目的はシナジーです。つまり、新しく統合された会社の価値と業績が、個々の企業の価値と業績の合計を上回るようにすることです。合併会社がシナジーを達成するのが早いほど、財務実績を早く改善できます。そしてこのようなメリットを達成するために最も重要な要素は、IT統合の成功です。事実、Gartnerは次のように報告しています。「典型的なM&A関連の統合の取り組みの25%はITに由来し、シナジー関連の統合活動の半分以上がITに大きく依存





している。つまり、CIOにはM&Aの遂行を加速する大きなチャンスがある。」[1]

予想されるシナジーに期待が高まりますが、残念ながら企業はしばしば重大な間違いを犯し、適切なIT統合に失敗します。その結果、新しく創設された企業を危険にさらす深刻なセキュリティ問題に苦しめられるのです。このe-bookでは、そのような失敗を回避し、M&Aから期待通りのメリットを享受するために必要なセキュリティを確立する方法について明らかにします。

「数年前は、サイバーセキュリティのデューデリジェンスは、買収企業がターゲット企業に一連の質問を提示する形式で行われていました。足りない場合は、これに現地訪問や電話が追加される場合もありました。今日、セキュリティは重役室で話し合われる問題であり、それに関連して予想されるのは、特に機密データと知的財産に関して、将来の組織の価値が著しく低下する可能性です。」

Gartner『Cybersecurity Is Critical to the M&A Due Diligence Process（サイバーセキュリティはM&Aデュー・デリジェンス・プロセスに不可欠）』（Sam Olyaei）2018年4月30日。

1 Gartner『The CIO's Role in Making Mergers and Acquisitions Faster（M&Aの高速化におけるCIOの役割）』（ID G00226390）（Ansgar Schulte）。2012年2月1日発行、2018年12月5日改訂。

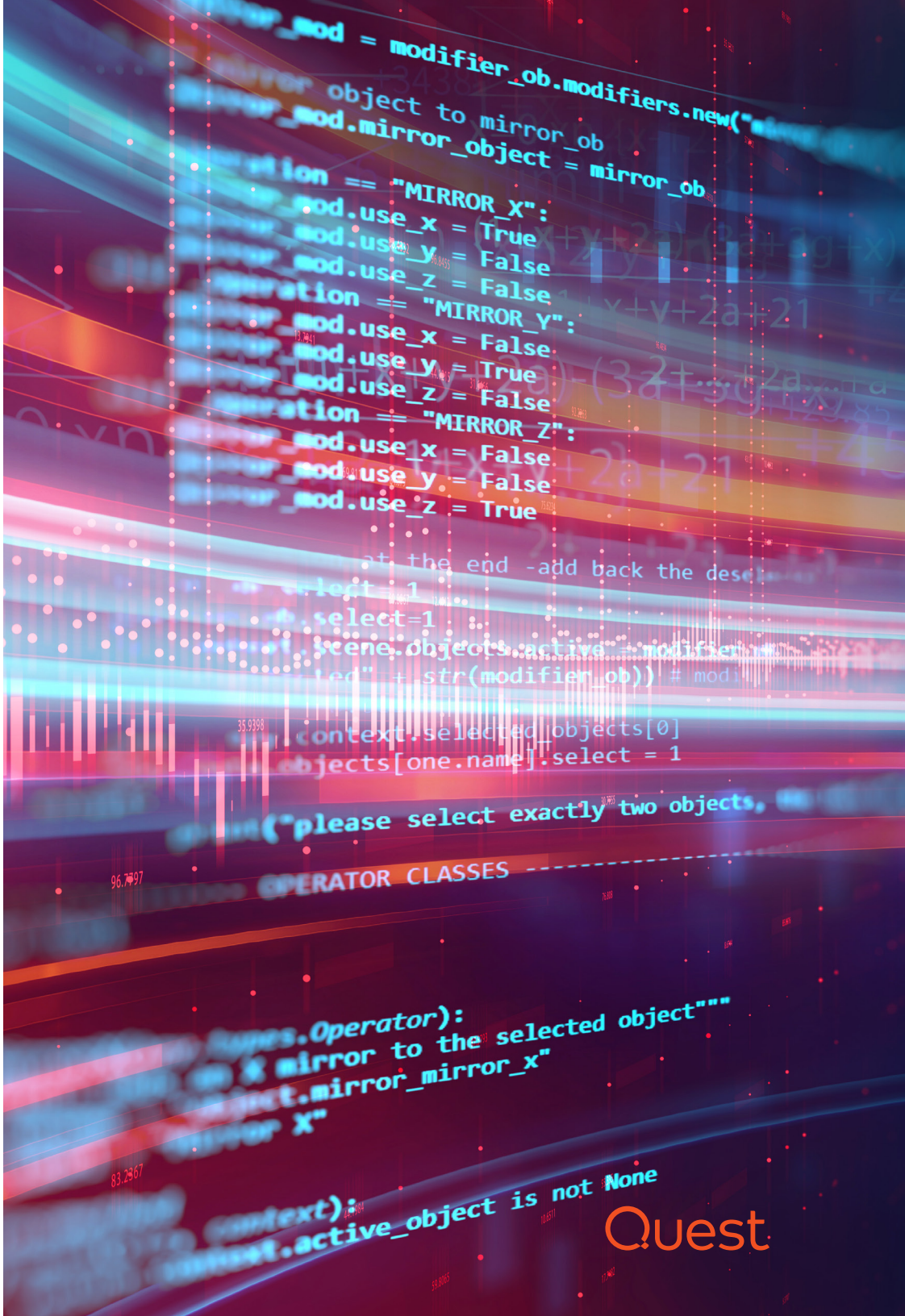
Quest

M&Aがセキュリティに及ぼす影響

LD1前

合併や買収が発表されると、Legal Day 1（LD1）に向かって全力疾走が始まります。IT統合を迅速に完了させることのプレッシャーがITチームにのしかかり、適切なITデューデリジェンスはビジネスアジリティのために犠牲にされます。以下は、いずれ危険なセキュリティ問題に発展する可能性がある、一般的な間違いの例です。

- **移行の範囲を設定しない —** LD1の目標は、M&Aに関係する組織を完全に統合することではありません。最小レベルの相互運用性と通信を確立し、外部との一体化を表すことです。移行の範囲を慎重に指定しないと、セキュリティに深刻な影響を及ぼす可能性があります。移行する必要があるクラウド内のB2Cアカウントをすべて除外してしまうなど、範囲が狭すぎると、LD1に生産性を確保するために必要なアクセス許可がユーザに与えられない可能性があります。範囲が広すぎることは、ほとんどの場合、さらに望ましくありません。例えば、HRの人員削減に含まれる従業員のユーザアカウントを移行すると、その従業員、または他の従業員が悪意のある目的でそのアカウントを悪用する機会が生じます。
- **サイバーセキュリティ分析を実行する前にActive Directoryの信頼関係を確立する —** Active Directoryは、Windows環境の中心的な認証および承認メカニズムです。2つのADドメイン間でリソースを共有するには、両者の間でAD信頼関係を確立しなければならないため、M&Aで統合されるIT環境のADドメイン間で信頼関係を確立することは非常に大きなプレッシャーと



なるでしょう。しかしながら、他のドメインとの信頼関係を確立すると、そのドメイン内の誰でも（悪意のある内部関係者や感染したアカウントを含む）が環境に侵入できる経路が生まれます。そのリスクを冒す前に、他のADドメインで実施されているセキュリティポリシーと手順を徹底的に確認する必要があります。

- **ダーティデータの使用 —** 数年以上経過したADインフラストラクチャは大幅な成長と変化を重ねている可能性が高く、多くの場合、十分な監視と管理が行われていません。つまり不規則に追加変更されている可能性があります。その結果、M&Aに関与するあらゆるADインフラストラクチャには、重複データ、陳腐化データ、不要データがある程度存在します。このようなダーティデータをすべてクリーンアップしなければ、IT統合プロジェクトのコストと複雑性が増加し、ITの専門家には、LD1までに実施する必要があるタスクに対応する時間がさらに足りなくなります。さらに、クリーンアップを注意深く行わなければ、さまざまな形でセキュリティリスクが増加します。まず、使用されてないコンピュータやアカウントが適切に無効化または削除されていないと、攻撃者が悪用するための格好の標的となってしまいます。次に、ITチームはSIDの履歴に大きく依存しすぎてしまいがちで、それにより、ユーザに対して古い環境と同じアクセス権を、そのアクセス権が適切かどうかを考慮することなく、新しい環境でも与えてしまいます。これは、購入したばかりの家の鍵を交換しないのと同じことです。

LD1に向かって全力疾走する中で、企業はしばしばビジネスアジリティのために適切なITデューデリジェンスを犠牲にしてしまい、その結果、深刻なセキュリティ問題に苦しみます。

Quest

適例: MarriottによるStarwoodの買収

2015年、MarriottのCEOは、事務管理と運用効率を活用することによって、Starwood Hotelsの買収から年間2億ドルのコストシナジーがもたらされると予測しました。しかし契約成立から2年後、Marriottは、Starwoodの宿泊客データベースを介してハッカーが侵入し、2014年以降に最大5億人の顧客の個人情報が、アクセス、暗号化、およびダウンロードされたことを発見しました。明らかに、MarriottがM&A IT統合プロジェクトの間、適切なサイバーセキュリティのデューデリジェンスを怠っていたことの表れです。そうでなければ、Starwoodのセキュリティプロセスに関する大きな問題に気付き、おそらく侵入そのものさえ検出できたでしょう。

現在、M&Aのシナジーを享受する代わりに、Marriottはとてつもない規模の嵐に苦しめられています。データ漏洩に関する直接的な費用は2億ドルから6億ドルと見積もられていますが、これは単なる始まりにすぎません。規制機関により、EU一般データ保護規則（GDPR）の不順守に対して9億1500万ドルもの罰金が追加される可能性があり、訴訟費用としておそらく数百万ドル以上が必要になるでしょう。さらに、米国 証券取引委員会は、漏洩を速やかに開示しなかったとして、Marriottを告訴する可能性があります。最後に、ブランドのダメージや顧客ロイヤルティの喪失など、目に見えにくい損失があります。

全体として、被害額は35億ドルを上回る可能性があります。いずれも、Marriottが慎重に徹底的なIT統合プロセスを実施していれば、避けることができたはずです。

MarriottはM&A中に適切なITデューデリジェンスを怠った結果、35億ドルもの費用が請求されるでしょう。

LD1にたどり着くためには、応急措置と回避策が必要なことはよくあります。しかし、後でこれらをクリーンアップしておかないと、やがて災厄を招きます。

LD1後

基本的な通信と相互運用性というLD1の目標を達成するために、ITチームはしばしば、レガシーシステムをそのままにしたり、関連付けられたワークフローを有効にするために回避策を使用したりするなど、なんらかの妥協を行う必要がありますが、これらの応急措置はすべてクリーンアップする必要があります。そしてもちろん、さまざまなサーバ、アプリケーション、ワークステーションの移行など、LD1の範囲に含まれなかったあらゆる作業がまだ残っています。

残念ながら、組織はLD1後のフェーズ中にも、次のようなセキュリティ問題に発展する可能性がある間違いをしばしば犯します。

- **レガシーアプリケーションを移行しない —** レガシーアプリケーション（特にADに依存する自社製アプリケーション）の移行は、しばしば労力に見合う価値がないと見なされます。それに伴う作業と煩雑さを嫌って、組織はレガシー環境と連携するために古いディレクトリをそのままにして、古いADとプライマリADの間にある種の共存を設定することを選びます。しかし、古いADがプライマリADと同期しなくなったり、古いサーバに適切にパッチを適用できなかったりすることは、ほとんど避けることができません。その結果、内部関係者や侵入者が利用できるセキュリティギャップが生じるのです。
- **ネイティブツールを使って済ませようとする —** ネイティブツールは無料ですが、機能は限定的で、ほとんどのADやOffice 365の移行の規模や複雑性に合わせて拡張することができません。さらに、テナントからテナントへの移行用のネイティブツールはありません。したがって、特定用途向けに設計された移行ツールと信頼できるベンダーのサポートのROIを検討する際は、ITチームが手動プロセスと限定的な可視性に対応する必要があること、また、基本ツールに頼った結果、セキュリティインシデントの直接的/間接的コストが発生する可能性があることについて、必ず考慮してください。
- **想定外の事態に備えない —** 前述のすべての落とし穴を無事回避できたとしても、まだ安心できません。物事はうまくいかないものです。予想通りに機能しない場合に素早くかつ簡単に移行タスクをロールバックできるようにしておかなければ、業務に支障が生じます。不具合を適宜ロールバックし、情報が失われないようにするために、移行前、移行中、移行後に適切なバックアップおよびリカバリシステムを準備しておく必要があります。

Quest

参考事例: Equifaxによる複数のM&A

2005年、信用調査会社Equifaxは、積極的な成長戦略に着手しました。2018年までに18の企業を買収し、世界最大の民間信用追跡会社の1つになったのです。ある意味では、このM&Aアプローチは大きな成功を収めました。Equifaxの市場価値は4倍以上に跳ね上がり、2005年12月の1株当たり約38ドルから、2017年9月には1株当たり138ドルを記録しました。

ただし、これらの買収の間に実施されたIT統合の方法は、2017年に同社が被った、1億4800万人分の個人情報流出という、大規模なデータ漏洩の大きな要因になったのです。米国 下院監視・政府改革委員会では、次のように報告されています。「Equifaxの収益と株価に関して言えば、買収戦略は成功であったが、この成長によりEquifaxのITシステムの複雑性が増し、データ・セキュリティ・リスクが拡大した。」[2]

この辛辣なレポートでは、この漏洩は「完全に防止可能」であったとされています。具体的な問題としては、1970年代にカスタム構築されたインターネット向け消費者紛争ポータルに使用されていたApache Strutsのバージョンにパッチを適用していなかったことや、証明書の期限が切れており、インターネットとの間のトラフィックの流れが19ヶ月もの間、侵入検出または侵入防止システムによって分析されないようになっていたことがあります。

「これは、史上最高額のデータ漏洩となるでしょう」と、サイバー攻撃のコストを追跡する研究グループ、Ponemon InstituteのLarry Ponemon会長は述べています。[3] Ponemon会長は、データ漏洩に関する総費用は「優に6億ドルを超える」と見積もりました。これには、技術やセキュリティのアップグレード、弁護士費用、およびデータ盗難被害者に対するなりすまし犯罪監視の無料サービスのほか、インシデントに対する政府の調査の解決費用や会社に対する民事訴訟費用が含まれています。

EquifaxがM&Aから生じたITの複雑さに対処しなかったことで、史上最も高額なデータ漏洩の1つが発生しました。

2 米国 下院監視・政府改革委員会Majority Staff Report『The Equifax Data Breach（Equifaxのデータ漏洩）』2018年12月。

3 ロイター通信『Equifax breach could be most costly in corporate history（Equifaxのデータ漏洩は史上最も高額となる可能性）』2018年3月2日。

自分を守る方法

このように、M&AのIT統合の部分が思わぬ方向に進む原因はいくつもあります。—しかも、ここですべての原因を説明したわけではありません。この時点で、頭を抱えてしまう方もいるかもしれません。しかし、明るいニュースが2つあります。

まず、これは決して誰も足を踏み入れたことがない領域ではないということです。既に多くの組織がADの移行と統合や、Office 365またはAzure ADのテナントからテナントへの移行を実施してきており、その経験から非常に多くのことを学ぶことができます。2つ目は、関連するプラットフォームや移動するデータの量など、移行によって詳細は異なりますが、ほぼすべての移行に、同じ基本的なベストプラクティスが適用されることです。大まかに言うと、次のことができるようにする必要があります。

- **検出の実行 —** ソースとターゲットの両方の環境のユーザ、アプリケーション、システム、許可、その他の詳細、さらに相互作用と相互依存性について、十分に理解してください。次に相手先企業と連携して、移行する必要のない、未使用のメールボックス、アカウント、サービスや、アーカイブする必要がある

Quest

コンテンツを特定します。このプロセスにより、移行が簡素化され、ターゲット環境のセキュリティと管理が向上します。

- **データのバックアップとリカバリ —** 移行を開始する前に、移行中に問題が発生した場合に備えて、元のフォレスト、メールボックスリポジトリ、コラボレーションサイトの完全なバックアップを作成する必要があります。もちろん、信頼性の高いバックアップ/リカバリソリューションは、IT統合プロジェクトの完了後も、長い間、価値を提供し続けます。
- **生産性の確保 —** 移行プロセスは時間がかかります。さまざまな参加者がどのシステムに属しているかにかかわらず、ユーザが会議を開催できるようにし、全員がすべてのEメールに中断されることなくアクセスできるようにする必要があります。したがって、2つのシステムの間で、パブリック・フォルダ・コンテンツ、空き/ビジー情報、メールボックス、および重要なデータを確実に同期できるようにすることが不可欠です。さらに、新しいシステムに移行しようとしているすべてのユーザのアカウントと共に既存のパスワードが移行されるようにし、ユーザの移行後には、ユーザのADおよびOutlookのプロファイルを更新できるようにする必要があります。
- **経営陣への継続的な情報提供 —** さまざまな関係者に移行の進行状況を報告できるようにしておくか、必要に応じて関係者がその情報に自らアクセスできるようにセキュアなアクセス権を与えておきます。
- **ターゲット環境を適切に管理し、保護する —** 適切なガバナンスを確立し、異常または疑わしい変更やユーザの行動を追跡および警告することによって、新しく統合されたIT環境を保護します。理想的には、強力な管理グループなど、最も重要なオブジェクトの変更を防ぐことができるようにします。

IT統合の間、確立されたセキュリティのベストプラクティスに従うことで、御社が第2のMarriottやEquifaxになることを回避できます。

Questの実績のあるソリューションと一流のサポートにより、複雑なM&A IT統合を克服しましょう。

まとめ

M&Aは数も規模も増加しており、その成功はIT統合の適切な実施に大きく依存します。残念ながら、多くの組織はLD1に向かう途中とその後の数ヶ月の両方で、よくある間違いを犯してしまい、新しく統合された組織のセキュリティを大幅に低下させ、合併によりもたらされる節約よりも大規模な出費が発生する可能性があります。

しかし、ここで専門家の助言に従うことで、第2のMarriottやEquifaxになることを避けられます。また、社内だけで対応しなければならないわけではありません。Questは、オンプレミス、クラウド、およびハイブリッドのMicrosoft環境の効果的な統合と管理のための包括的なフレームワークを開発しました。これは何度も利用できるソフトウェアおよびサービスです。さらに優れているのが、繰り返しに適している点です。1セットのソリューション、1つのサポートチーム、1つのサービスチームに精通するため、次回のM&Aを任せられることになっても慌てることはないでしょう。

M&A IT統合のセキュリティへの影響についての詳細、ベストプラクティス、Questのソリューションが複雑さを克服するためにどのように役立つかを確認するために、当社のホワイトペーパー「IT Integration Best Practices in Mergers & Acquisitions (M&A) (M&Aにおけ るIT統合のベストプラクティス)」をお読みください。

Quest

QUESTについて

Questは、急速に変化するエンタープライズITの世界にソフトウェアソリューションを提供しています。データの爆発、クラウドサービスへの拡張、ハイブリッド・データ・センター、セキュリティ脅威、規制上の要件によって生じる課題のシンプル化を支援します。当社は100ヶ国における130,000社の企業に対するグローバルプロバイダです。これらの企業にはFortune 500の95 %とGlobal 1000の90 %が含まれています。1987年以来、現在ではデータベース管理、データ保護、IDおよびアクセス管理、Microsoftプラットフォーム管理、統合エンドポイント管理を含む、ソリューションのポートフォリオを築いてきました。Questは、組織がIT管理に費やす時間を削減し、ビジネスイノベーションにかける時間を増やせるように支援します。詳細については、www.quest.com/jp-ja/をご覧ください。

本書の使用に関して不明な点がありましたら、以下までお問い合わせください。

www.quest.com/JP-JA/company/contact-us.aspx

Ebook-M&AImpact-US-GM-JA-WL-38204

Quest