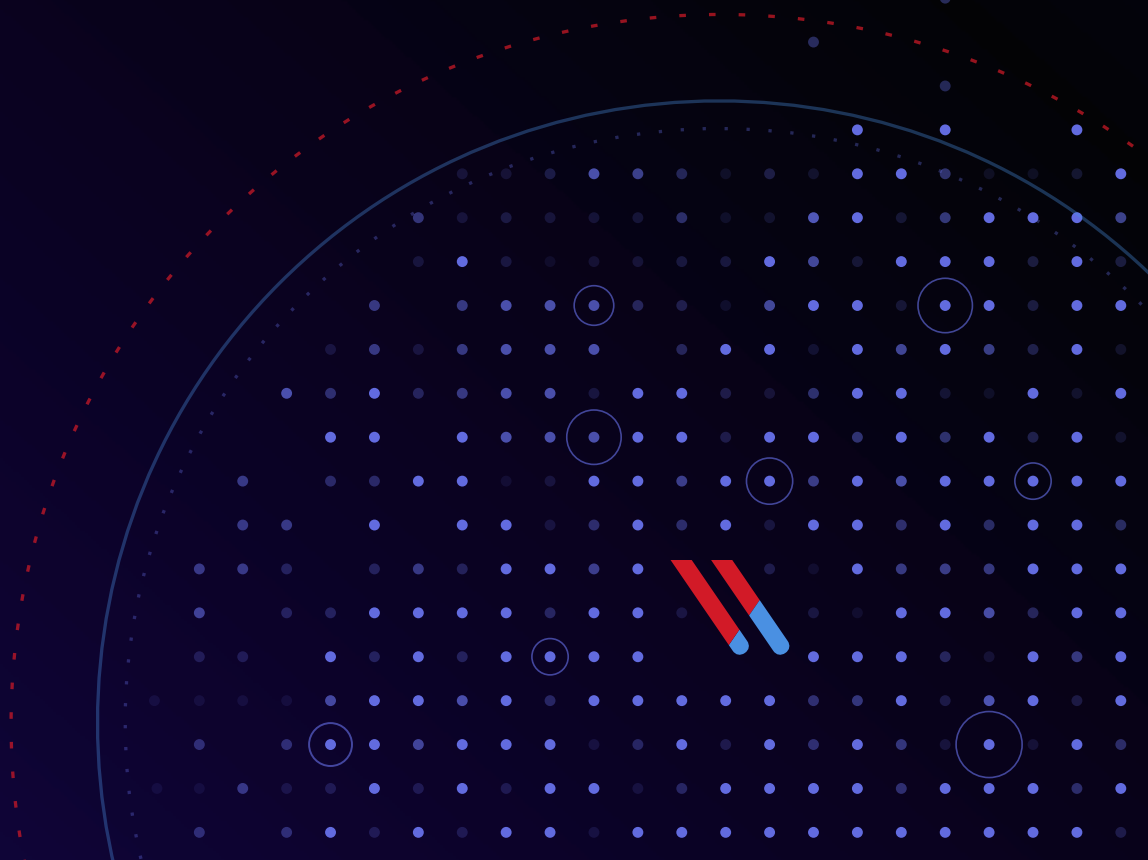
VARONIS

Varonisの戦い方は違います

サイバーセキュリティに対する
Varonis独自のアプローチ



はじめに

組織がデータ主体になるにつれ、オンプレミス環境やクラウドストレージに保管するデータも増えました。従業員はスマートフォンやタブレット、ノートパソコンを使用することで、どこからでもこのデータにアクセスできます。セキュリティの境界の定義があいまいになり、エンドポイントも脆弱になる中で、お使いのスマートフォンやノートパソコンだけに「留まる」データは少なくなっています。

このデジタル改革は、境界やエンドポイントに焦点を合わせた、従来のセキュリティモデルを覆しました。組織は外から内への攻撃に集中するのではなく、内から外への対策やデータ第一のセキュリティを検討し始めています。

データ保護はシンプルなように見えて、非常に複雑なものです。

なぜデータ保護はシンプルなように見えるのでしょうか。

以下の質問に「はい」と答えることができ、今後も継続的に「はい」と答えることができれば、お客様のデータは安全であると言えるでしょう。

1. **重要なデータが保管されている場所**を把握していますか?
2. **適切なユーザーだけにアクセス権限が付与されているかどうか**を把握していますか?
3. **ユーザーが正しくデータを使用しているかどうか**を把握していますか?

シンプルに思えますよね?

この3つの質問は、データ保護の基本的な次元、「重要性」、「アクセシビリティ」、「使用状況」を表しています。ITまたはITセキュリティ部門で働いている方は、この次元が全くシンプルでないことをご存知かと思います。

これらの質問に「はい」と答えられない、または答えが全く分からないということは、CISO、コンプライアンス担当者、取締役会、株主にとって喫緊の問題となりうる以下の質問につながることもきっとご存知でしょう。

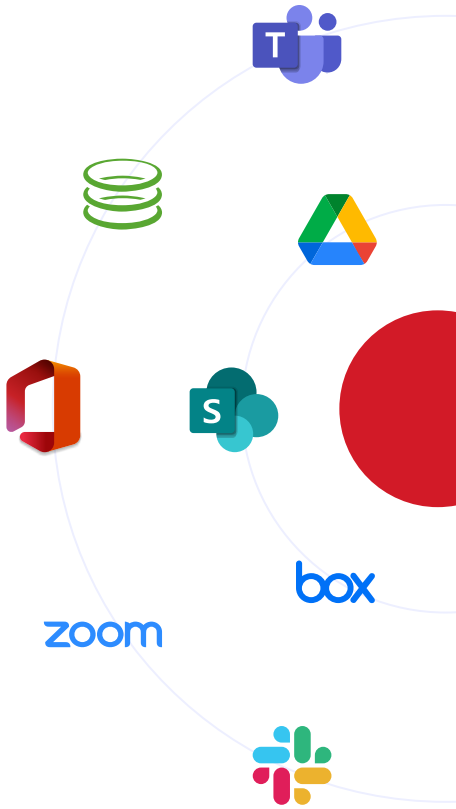
- 機密性の高いデータや規制対象のデータはどこにありますか?
- アクセス権限が過剰に付与されていて最もリスクの高い場所はどこですか?
- アカウントや従業員のデータが侵害された場合の「爆発範囲」はどこまでですか?
- データが盗難、暗号化、削除されたことを、どうやって検出しますか?
- データを削除することはできますか?

データの量が増える一方のオンプレミス環境やクラウド環境、アプリケーションやデータストアでは、それぞれ独自のセキュリティモデルを持っており、なかなか答えが見つかりません。たった1つの企業プラットフォームであってもデータ保護は十分難しいのに、同時に多くのプラットフォームでデータ保護を実現するのは大変です。

データのあるべき場所はどこでしょうか?

過去数年間でデータを保管できる場所の数は爆発的に増えており、さまざまなデバイスやエンドポイントでデータをアクセスすることも一般的になりました。このため、エンドポイントは、データの本当の「在処」(現代では通常クラウドアプリケーション)へのゲートウェイのような働きが主となりました。

現在ではほとんどの組織がオンプレミス型のインフラストラクチャに加えて、クラウドアプリケーションとクラウドインフラストラクチャの組み合わせに頼っています。Microsoft 365、Box、Googleドライブ、またはSlackをコラボレーションに使用したり、ソースコードにGitHubまたはJiraを使用したり、AWS、Azure、またはGoogleクラウドを使用してコンピューティングやストレージの負荷を抑えたり、Salesforce.comなどのCRMソリューションを使用したりすることを承認しない組織は珍しくなっています。



重要なデータはどこにありますか?

こういった承認済みアプリケーションの範囲であっても、攻撃表面は大きく、リスクの大きさを可視化したり、評価したりすることは困難です。データ保護の取り組みを優先することを期待して、従業員にファイルのタグ付けを依頼したり、自動化を使用して規制対象のデータや機密性の高いデータを特定、分類したりする取り組みに集中することを選択している組織もあります。

大きな問題を小さな断片に分割するのは確かに理にかなっていますが、問題がより大きくなれば、小さな断片でも破壊的な損害をもたらす可能性があります。

ほとんどの組織が、検出された機密性の高いファイルやレコードの数に驚きます。ある場所では数千ファイル、他の場所でも数千、数万ファイルと見つかり、明日や明後日になれば、またリストが変わっていきます。

明確なアクションプランなしに保管場所を訪れたならば、いったい何をすればいいのか分からなくなるでしょう。検出したものすべてを他の場所(オンプレミスのデータストアなど)に移動させるブルートフォース型の手法を試みる組織もあれば、すべてを削除しようとする組織もあり、すべてを暗号化して従業員や少人数のグループメンバーのみが閲覧できるようにする組織もありますが、これは大きな問題を継承しただけです。

この手法では根本的な問題の解決にはなりませんが、適切なユーザーのみがデータへのアクセス権限を持つこと、いわゆる「最小権限の原則」や 最近では「ゼロトラスト」としても良く知られている原則は確実にすることができます。

機密情報など、あらゆるデータに対して正しいアクセス権が付与されていることを確実にするには、まず最初に、誰がアクセス権を持っているのかを確認する必要があります。これは、特にクラウドにおいては、想像するよりもずっと難しいものです。

重要なデータへのアクセス権を持つユーザーは誰ですか?誰がアクセス権を持つべきユーザーですか?

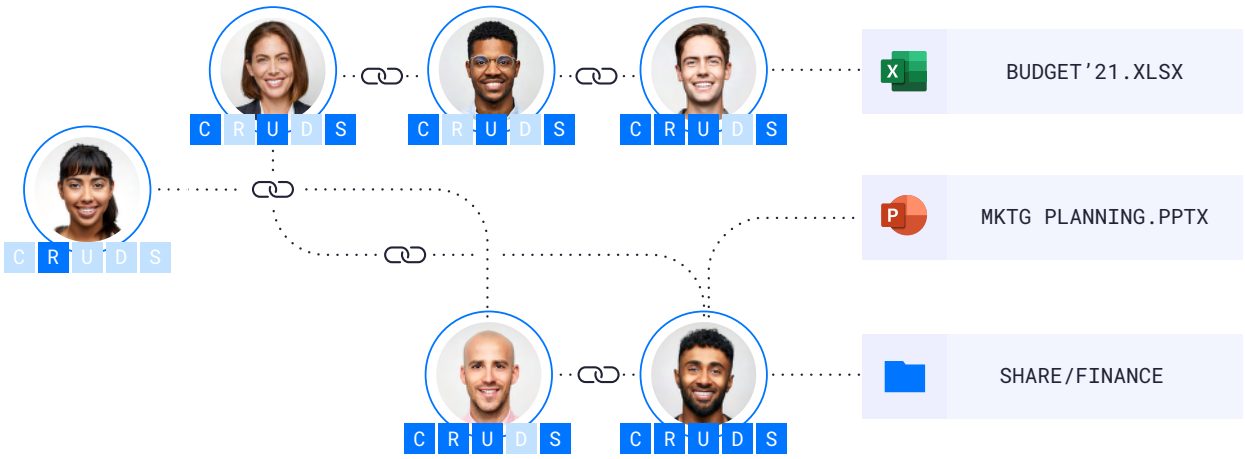
どのデータが規制対象でどのデータが機密であるかを理解できていなければ、非常に重要な文脈無しに、誰がアクセス権を持つべきかという判断をしなければならなくなってしまうというのは当然のことです。
しかし、驚くべきことに、そもそも誰がアクセス権を持っているかを知ることが難しいのです。

データへのアクセス権はアクセス許可やアクセス制御リストにより管理されます。その仕組みはアプリケーションであってもデータストアであっても基本的には同じです。

- ファイルやフォルダー、レコードといった**オブジェクト**があります。
- オブジェクトを使用して操作を実行できるユーザー、アカウント、ユーザーやアカウントのグループに対応する**デジタルID**があります。
- 作成、共有、削除など、**実行可能な操作の記述**があります。

Slack、Box、SharePoint Online、オンプレミス環境、またはUNIXファイルシステムで仕組みが大体同じだとしても、実装方法はすべて異なります。

- オブジェクトが似ていても、アプリケーションによってオブジェクトタイプ(例、ファイル、サイト、レコード、バケットなど)が異なります。
- ユーザー/アカウントとグループはクラウド内で複数の場所に保管され、各データストアは、通常、独自のユーザーとグループのデータベースを持っています。他のアカウント(Oktaアカウントなど)と接続していることもあれば、個人アカウントと職場アカウントの両方を追跡する必要があることもあります。こういったアプリケーションはそれぞれ、ユーザーやグループオブジェクトに、役職や役割、場所といった属性を割り当てることができます。



実行可能な操作の記述は各アプリケーションごとに異なりますが、作成、読み取り、更新、削除、共有が主なものです。

こういった違いに加え、特定のオブジェクトやユーザーの実効権限の計算は非常に複雑になることが多く、データストアによっても大きく異なります。特定のオブジェクトに対する実効権限を判断するには、以下のような複数の属性を考慮する必要があります。

- **オブジェクト固有のアクセス許可。**上述の通り、各オブジェクトにはユーザー、グループ、または役割エンティティをリスト化したアクセス制御リストがあります。その可能性は広範囲に及びますが、例えば基本的なUNIXアクセス許可の場合、3つのユーザー/グループ（ルート、所有者、グループ）に対し、3つのアクセス許可（読み取り、書き込み、実行）が考えられます。SharePoint Onlineの場合、7つのデフォルトレベル（追加も可能）に分類された33のアクセス許可が考えられ、オブジェクト上の**複数の**ユーザーやグループに割り当てることができます。
- **グループの関係。**グループにはユーザーまたはその他の「入れ子」のグループが含まれる場合があります。オブジェクトやユーザーに対する実効アクセス許可を判断するには、こういった関係を計算する必要があります。あるディレクトリサービスのグループが、他のディレクトリサービスのユーザーやグループを参照する場合があり、その場合の計算はより複雑になります。例えば、SharePoint OnlineにはAzure ADのユーザーやグループを含めることができるローカルグループがあります。
- **階層的な継承。**多くのデータストアでは、アクセス許可は階層の上から下に流れます。そのため、フォルダー内のすべてのオブジェクトがその親（複数可）のアクセス制御エントリーを「継承」します。子オブジェクトで継承を止められるデータストアもありますが、すべてがそうではありません。例えばBoxでは、子オブジェクトでのアクセス制御エントリーの追加のみをサポートしているため、子オブジェクトのアクセス許可が親オブジェクトよりも少ないということはありません。
- **役割と役割の階層。**役割に基づいてオブジェクトにアクセス権を付与することができます。役割に他の役割を含めたり、他のアプリケーションでは異なる役割を割り当てることがあります。例えば、AWSでは通常、必要に応じて役割を想定していきますが、Salesforceの役割はより静的に割り当てる傾向があります。
- **システム全体の設定。**すべてのオブジェクトへのアクセス権に影響する設定があります。例えばGoogleドライブでは、「リンクの共有」設定はすべてのアクセス許可を上書きし、新しく作成したオブジェクトはドメイン全体からアクセスできるようになります。Salesforceでは、「組織全体のデフォルト(OWD)」により、すべてのオブジェクトに対する基本レベルのアクセス権を設定できます。

アクセス権を可視化するには、すべての属性や機能的な関係を事前に計算し、データストアやアプリケーション全体で正規化する必要があります。このような自動化の仕組みが無いと、オブジェクトへのアクセス権を持つユーザー、またはユーザーやアカウントがアクセス権を持つ対象（攻撃に遭った場合の実質的な爆発範囲）を判断するのに不可能なほど時間がかかり、インシデント対応からトラブルシューティング、監査レポートまで、日常業務に支障をきたすことになります。

アクセス操作アクティビティの把握は アクセス許可の把握よりも簡単でしょうか?

簡単ではありません。

データセキュリティを考えるにあたって、データ保護と直接関係するイベントが数種類あります。

- **データアクセスイベント。**セキュリティとの関連性が最も深いアクティビティのうちデータの直接的な操作が含まれるものには、ユーザーによるデータの作成、読み取り、変更/更新、削除と共有があります。残念なことに、アプリケーションやデータストアは、それぞれ独自の方法で、ユーザーがどのようにデータを直接的に操作したのかを記録します(しない場合もあります)。例えばSalesforceのログでは、データアクセスのアクティビティにアクセスしたオブジェクトの情報が含まれません。
- データのアクセシビリティに影響を与える**アクセス制御の変更と設定の変更**も関連性が高いものです。アクセス制御の変更も異なる方法でレポートされ、参照するユーザーやグループに関する予備知識なしでは不完全なものになります。例えば、アクセス許可を記録する多くのシステムがどのエントリーが変更されたのかではなく、アクセス制御リスト(ACL)が変更されたことのみを記録します。また、ACLで参照されるオブジェクトに対する変更は、ファイルシステムまたはアプリケーションでは記録されない場合があり、ディレクトリサービス (Azure Active Directoryなど) で記録しなければならない場合があります。データのアクセシビリティに関しても、設定の変更は同様に複雑になります。Active DirectoryでのGPOの変更は、パスワードポリシーやエンドポイントの機能など、さまざまな重要な事柄に影響することがあります。例えばGitHubではコードレポジトリーのアクセシビリティに対する変更を記録しますが、何が変更されたのかは示されません。
- **認証イベント**は、アプリケーションやデータストアに接続しているユーザーについて、そのユーザーがどこからアクセスしているか、どのような種類の認証を経ているのか(単一要素または多要素など)を、意味のある文脈を提供できます。認証イベントは、ディレクトリサービスやアプリケーションによって異なります。
- **境界イベント。**オンプレミス環境のインフラストラクチャーでは、DNS、VPNゲートウェイおよびプロキシーからの境界信号が、環境内への異常な接続や、環境から外へ向かう異常な接続に関する洞察を提供します。境界デバイスからのイベントは量が多く、不均一なので、多くの場所の境界データを取得できることは魅力的ではあるものの、信号とノイズの比率を壊さないように注意が必要です。最も実用的なものは、侵入を可視化できるDNSやデータの持ち出しを可視化できるWebプロキシーなど、データの観点から関連するテレメトリーです。詳細については、**「SIEMが上手く機能しない5つの理由(5 Ways Your SIEM Is Failing You)」**をご覧ください。

記述方法が大きく異なるデータストアとアプリケーションについて、両者を跨いだ質問に答えるのは非常に困難です。特定の日にある従業員がアクセスしたデータや、管理者が行ったアクセス制御の変更を理解するだけでも、簡単な質問では叶わず、壮大な調査プロジェクトになります。

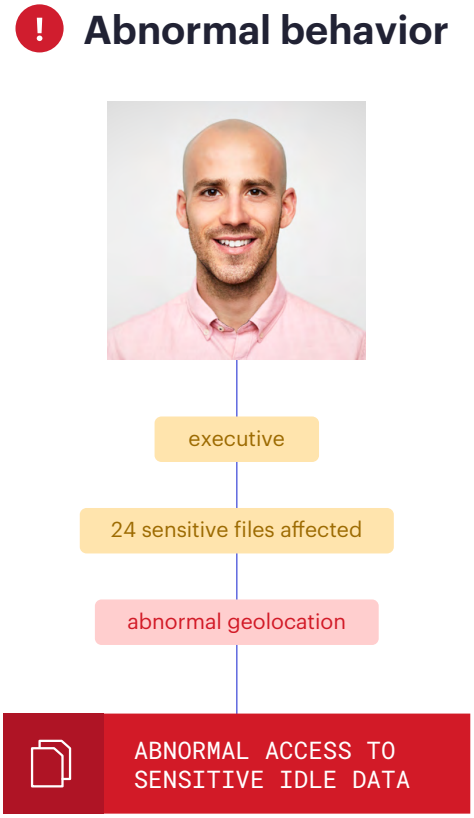
アラートはどうでしょうか?

均一で正規化されたイベントストリームがなければ、ルールベースのアラートの発報は困難であり、振る舞いベースのアラートは単一のアプリケーションに限定されるか、まったく利用できません。プロファイルを構築するために振る舞いをモデル化する場合、評価する意味のある切り口をAIに持たせるには、イベントも強化する必要があります。例えば、信頼できる正規化されたイベントストリームが無かったとしたら、誰かが1,000件を超えるファイルやオブジェクトを5分間の間に削除、更新、またはアクセスした際に発報する単純な閾値ベースのアラートであっても、アプリケーション単位にアラートを作成しなければならないでしょう。5分間のすべてのデータストアにおけるファイル操作イベントの総数が1,000件を超えた場合に発動するアラートを設定しようとすると、すでにかなり高度なクエリーが必要です。

さらに高度なアラートが必要な場合、例えば、データストア全体で5分間の間に機密性の高いファイルへのアクセスが1,000回あった場合に受け取るアラートなどでは、アラートロジックを処理する前に、ファイルの機密性情報を反映してイベントを強化する必要があります。閾値ベースのアラートにおいて、きれいで強化されたイベントがどれほど重要であるかをご理解いただけるようになったと思いますが、AIを活用したアラートではこれがさらに重要になります。

AIによって逸脱の評価に利用できる振る舞いのベースライン、すなわち平常時のプロファイルを構築するためのカギは、きれいで強化されたイベントストリームです。これらのデータ中心のプロファイルは、信号対ノイズ比(S/N比)が非常に高いアラートを生成します。例えば、通常、週に十数件のファイルにアクセスしていて重要なファイルをほとんど触らない役員が、そのユーザーとは関連付けされていないデバイス、あるいは通常はアクセスしない場所から、同僚ですらアクセスしない数十件の重要なファイルにアクセスし始めたら、すぐに注意を払う必要があります。

振る舞い分析は、関連性の高い、強化された、信頼性の高い振る舞いを使用して分析する必要があります。そのため、信頼性が低く、ノイズの多いストリームを分析するセキュリティテクノロジーは必然的に失敗します。



3次元で考えなければ
平面しか守れません

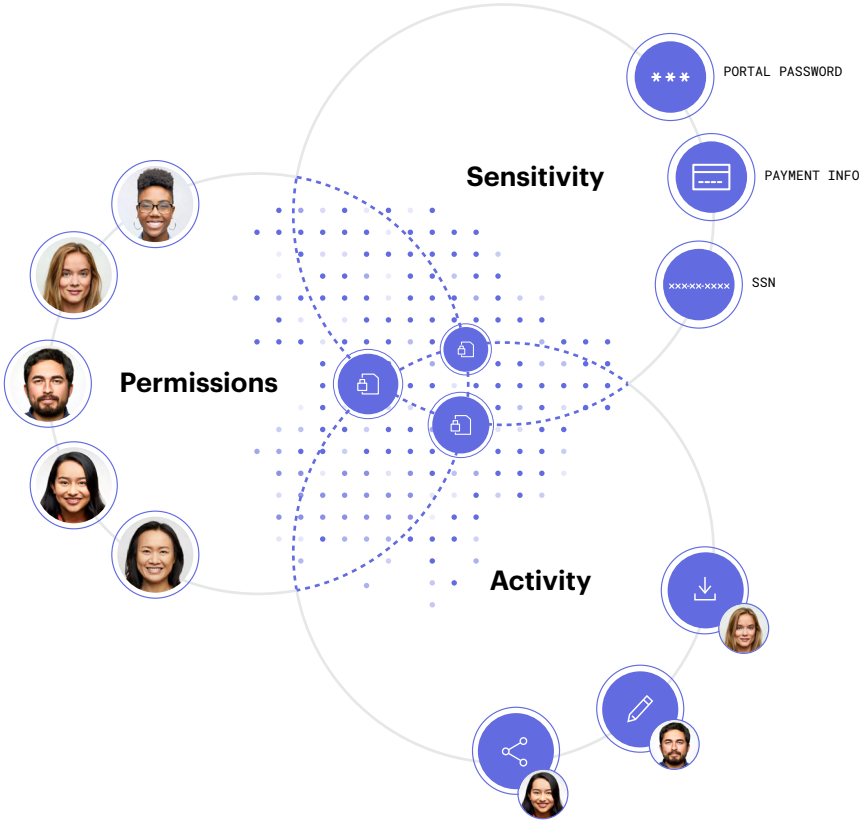
上述の機密性、アクセス許可、アクティビティの3つの次元が可視化されていない場合、多くの組織は1つまたは2つの次元から始めてみようと考えます。しかし、別の組み合わせを考えるうちに、3つすべてを組み合わせることが最も強力であるということがすぐに分かります。

前述の通り、どのデータが機密性が高いかだけを理解していても、アクセス許可の次元がなければ、そのデータがどこに集中し、どこで晒されているかを理解することはできません。アクティビティの次元がなければ、発見した晒されているデータを安全に修正する方法も、機密性の高いデータが盗難に遭っていないかどうかも、そのデータについて誰と相談すれば良いのかすらも分かりません。アクティビティの次元だけだと、侵害後にどのデータが持ち出されたかを把握したり、振る舞いの逸脱にアラートを発報することはできますが、持ち出されたデータの機密性がどれほど高かったのか、誰がそのデータにアクセスできる立場にあったのか、誤って社内の全員が（またはインターネット全体から）アクセスできる状態になっていなかったのかどうかを把握することはできません。

データの保護に関して、本書の冒頭で投げかけられた以下の質問に答えるには、3つの次元すべてが必要です。

1. **重要なデータが保管されている場所**を把握していますか?
2. **適切なユーザーだけにアクセス権限が付与されているかどうか**を把握していますか?
3. **ユーザーが正しくデータを使用しているかどうか**を把握していますか?

上記の質問に対して継続的に「はい」と答えられるようになれば、**「当社のデータは安全ですか?」**という最も重要な質問にも「はい」と答えられるようになります。



VARONIS

Varonisの違いを体験してみませんか?

リスクを取らずにリスクを軽減しましょう。**無償の**データリスクアセスメントについてVaronisチームにご相談ください。

お問い合わせ

VARONISについて

Varonisはデータセキュリティ解析の先駆者で、従来のサイバーセキュリティ企業とは異なる戦いをしています。Varonisはオンプレミス環境やクラウド上の企業データを保護することに注力しています: 機密性の高いファイルや電子メール; 機密性の高い顧客、患者や従業員のデータ; 財務情報; 戦略や製品計画; その他の知的財産。

Varonis Data Security Platformはデータの分析、アカウントのアクティビティやユーザーの振る舞いを分析して、内部者脅威とやサイバー攻撃を検出します; 機密性の高いデータや古いデータのロックダウンにより大事故を予防し想定範囲内に収めます;また、自動化により安全な状態を効率良く維持します。データセキュリティに特化した Varonis はガバナンス、コンプライアンス、分類、脅威分析などさまざまな用途にお使いいただけます。Varonisは2005年に事業を始め、全世界で数千社のお客様がいます — お客様は、テクノロジー、コンシュマー、小売業、金融サービス、ヘルスケア、製造、エネルギー、メディア、教育を含むさまざまな業界のリーダーから構成されています。