VARONIS ホワイトペーパー

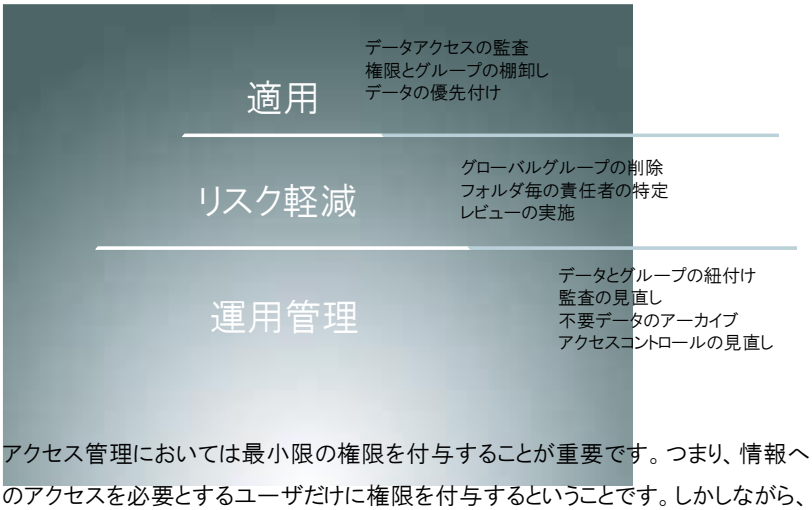
IT 部門が実行すべき 11 の課題とは

目 次

IT 部門が実行すべき 11 の課題とは

概要

ファイルサーバ、SharePoint、Exchangeのメールボックスやパブリックフォルダには、スプレッドシートや文書、画像などのデータが保存されています。このようなデータを適切に保護しているかと問えば、ほとんどの企業が現行のプロセスとリスク対策は不十分であるとすぐに認めるでしょう。データのアクセス権や使用方法について、データの所有者よりもITスタッフが多くの判断を下す立場にあることが問題になっているケースもあります。非構造化データ及び半構造化データが増大しているのはビジネス上の理由であり、ITスタッフがその原因を作り出しているわけではありません。ITスタッフができることは、データやセキュリティを設定し運用することだけです。データの管理が現場に移行するまで、IT部門はファイルのアクセス権を適切な状態に維持したり、データの増大やユーザ権限を変更したりなど、さまざまな処理に多くの労力を費やし続けることになります。



アクセス管理においては最小限の権限を付与することが重要です。つまり、情報へのアクセスを必要とするユーザだけに権限を付与するということです。しかしながら、急速なデータの肥大化や、頻繁な人事異動が発生する多くの企業にとって最小限の権限を付与するという原則を適用することはほぼ不可能となっています。小規模な組織であっても多くの場合は組織が頻繁に変更され、IT部門はアクセス権限リストやグループメンバーの情報を適切に維持・管理することが困難な状況です。どのような組織であってもアクセス権限を組織の役割に合った形とし、それらが日常的なデータ管理業務の一つとなるように、後述する管理タスクを自動化することが理想です。但し自動化によって運用できたとしても、非構造化データと半構造化データを最大限に管理するにはIT部門は11の課題に取り組む必要があります。

11の課題

1. データアクセスの監査

データを効果的に管理するには、アクセスログが不可欠です。ITスタッフが信頼性の高い方法でデータの使用状況を監視できなければ、不正利用があっても検出できません。データのアクセスログがないと、「誰が私のファイルを削除したのか」、「どのデータをこのユーザ(またはグループ)は使用しているのか」、「どのデータが使用されていないのか」といった極めて基本的な質問から、「どのユーザがデータの所有者なのか」、「どのデータがどの部門のデータなのか」、「どのようにしたら業務を停止させずにデータの保全ができるか」といった複雑な質問までの回答は困難になります。

2. アクセス権及びディレクトリサービスのグループオブジェクトのインベントリを作成する

どのようなデータでも効果的に管理するにはユーザのアクセス権を把握する必要もあります。Active DirectoryやLDAPなどにおけるアクセスコントロールリストとグループは、非構造化/半構造化データの全てのプラットフォームにおいての基本的な要素ですが、データ保護に関する基本的な質問「誰がこのデータにアクセスできるのか」、「どのようなデータにユーザやグループがアクセスできるのか」などに対してIT部門が直ぐに回答できない状況が多く見られます。このような質問に対して該当する情報に直ぐにアクセスでき且つ正確に回答できることがデータの保護・管理において重要になります。

3. データに優先順位を付ける

もちろん全てのデータを保護する必要がありますが、応急措置としてIT部門が最初に取り組むべきことは、どのようなデータを「機密性の高いデータ」として扱うかということです。管理者が明確で、保護や制御の方法が決められているデータもありますが、多くのデータは明確化されていません。監査ログの追跡やデータの分類、アクセスコントロール情報をもとに企業は有効なデータと不要なデータ、機密/社外秘/部外秘と見なされるデータ、公開データを識別することができます。重要なデータは、初期段階でリスクを軽減させておく必要があります。コンテンツ、アクセス頻度、アクセス権、その他メタデータに基づいてデータの移動やアーカイブ、削除の自動化を検討すべきでしょう。

4. 機密データが保存されているフォルダでは “Everyone” といったアクセス権を削除する

ファイル共有のフォルダアクセス権が「全てのユーザ」または「ドメインユーザ」(事実上はEveryone) になっており、そのフォルダ内のデータにほとんどのユーザからアクセスできる状態になっているケースがあります。SharePointにも同様の問題があり、Exchangeではさらに、「匿名ユーザ」というアクセス権も存在します。これは、大きなセキュリティリスクになります。ディレクトリアクセス設定をあいまいにしておくと、フォルダ内に保存される全てのデータがこの「無防備な」アクセス権を継承することになります。これらのフォルダ内に、個人を特定できる情報(PII)や、クレジットカード情報、知的所有権、人事情報などの機密データが含まれていると、重大な問題発生時に企業責任を問われることになります。機密性の高い情報が入っている場合はグローバルアクセスを削除しこれらの情報へのアクセスを本当に必要とするグループのみにアクセス権を付与する必要があります。

5. データの管理者を特定する

IT部門は自らの責任の下で、データの管理者、フォルダ、SharePointサイトの最新リストを管理しておく必要があります。このリストを「直ぐに使える状態」にしておくことでアクセス権の失効の確認及び見直し、アーカイブ対象データの特定など、多数のタスクを効率よく処理できるようになります。結果として、データのアクセス権の精度が大幅に向上し適切なデータの保護が実現できます。

6. アクセス権限の見直しや未使用または不適当なアクセス権に対するレビューを定期的に実施する

WindowsまたはUNIXのファイル及びフォルダ、SharePointサイト、メールボックス、パブリックフォルダは全てアクセスコントロールリスト(ACL)が適用されており、それによって、データにアクセス可能なユーザとアクセスレベル(読み取り、書き込み、実行、リスト表示など) が決まります。これらのアクセスコントロールリスト(ACL)は、データの管理者及びセキュリティポリシー監査担当者が適切かどうか確認できるように定期的に見直しを行い、状態を文書化する必要があります。業務に関係のないユーザにそのデータへのアクセス権が付与されていた場合は企業にとってセキュリティリスクとなります。大部分のユーザが必要なデータは、ファイルサーバに保存されているデータのほんの一部だけです。レビューを行い、使用されていないアクセス権があれば削除するか、失効させることが重要となります。

7. セキュリティグループとデータを適切に組み合わせる

グループに属するユーザはそのグループのアクセス権が設定されているフォルダに対してアクセスが許可されます。しかしながら、Active Directory、LDAP、SharePoint、NISのグループ管理については企業ではほとんど追跡されていません。このような不確定要素があると、アクセスコントロールの見直しやロールベースのアクセスコントロール(RBAC) が困難な状況になります。ロールベースのアクセスコントロールでは、各ロールにグループリストが関連付けられており、ユーザはロールが割り当てられるとそのロールに関連付けられているグループに属することになります。グループからどのデータにアクセスできるのか確認できない状態では、ロールとデータを適切に組み合わせることはできません。

8. アクセス権とグループメンバシップの変更を監査する

アクセスコントロールリスト(ACL) は、紛失、改ざん、漏洩からデータを保護するための基本的な防御手段です。IT部門ではアクセスコントロールに関する変更を検出及びレポートを行う仕組みが必要です。機密性の高いファイルがあるフォルダの場合は特に必要とされ、アクセス権が不適切に割り当てられた場合や、正当な理由無しにアクセスコントロールが緩和された場合には、IT部門とデータ管理者に直ぐにアラートを通知して対処できるようにする必要があります。またディレクトリグループ(Active Directory、LDAP、NISなど) は、アクセスコントロールリスト(ACL)における基本情報であり、サーバ内にも監査すべき独自のローカルグループがあります。ユーザは既存グループに加えて新しく作成されたグループに追加されることがありますが、これらのグループに対して追加/削除されたユーザの監査証跡がなければ、アクセスコントロールプロセスを運用することは困難です。アクセス権が適用されているグループまたはデータの所有者がグループメンバーの許可及び見直しを行うことが理想的です。

9. 未使用の古いデータを使用禁止、削除、アーカイブする

非構造化/半構造化プラットフォームに含まれているデータの多くは未使用データになっているケースが多く、古いデータや使用されていないデータをオフラインストレージにアーカイブまたは削除することによってIT部門は貴重なリソースを確保しながらも古いデータが不適切なユーザにアクセスされるリスクを減らし、他のデータについての管理を簡素化することができます。

10. グループとアクセスコントロールの項目を整理する

不必要に複雑な状態を放置しておくと、運用管理負荷が上昇し、トラブルが発生し易くなります。企業では大量のグループを作成したままその多くを空の状態にしていたり、使用していなかったりという状態が散見されます。グループに別のグループが含まれ、さらにそれに別のグループが含まれるなど、複数のグループが入れ子になっている場合もあります。(親グループが子グループに含まれると、循環参照が形成されることがあります)。 アクセスコントロールリスト(ACL) には、以前に削除されたユーザとグループへの参照が含まれていることがよくあります (「孤立したセキュリティID」とも呼ばれます)。こういった古いグループと間違って構成されているアクセスコントロールオブジェクトを特定し修正することが重要です。

11. そして最後に、パブリッククラウドサービスを制御する

数百万のユーザがDropboxなどのパブリッククラウドサービスを業務で利用している今日、企業は適切なアクセスコントロールや監視環境が無ければデータそのものを失うリスクも抱えてしまうことになります。それでもユーザは自分のノートPCやデスクトップPCとのファイル同期、モバイルデバイスや他のアプリケーションとのファイル共有を望んでいます。企業としては、自社のコンプライアンスとセキュリティ要件に合致するプライベートクラウドサービスを許可して使用させるか、逆にユーザがITのポリシーを無視することがないように既存のシステム構成を変更または拡張し、企業管理下においてパブリッククラウドとのコラボレーションを導入するかを選択する必要があります。

IT部門で対応すべき11の課題は、Varonisで全て解決！

Varonis DatAdvantageは、IT部門で対応すべき11の課題を解決します。
DatAdvantageは非構造化データにアクセス可能なユーザ、既にアクセスしているユーザ、アクセスすべきユーザ、機密性が高いデータの可視化と監査機能を提供することができます。
サーバのパフォーマンスを低下させることなく、既存環境から継続的に最新情報が抽出され、個人ユーザと所属グループ、ファイルサーバやSharePoint Server、Exchange Serverのメールボックスとパブリックフォルダ、ユーザの各データアクセス（開封、削除、名前変更、メールの送受信など）が表示されます。アクセス権とグループの変更は全てログに記録され、データ管理者を指定して権限の承認や見直しを行うことができます。
Varonis DatAdvantageのGUI画面ではファイルサーバやSharePoint、Exchangeなどの全フォルダが表示され、隣接するウインドウにはユーザやグループなどのDirectory情報が表示されます。Varonisならではの双方向からの可視化機能によって、フォルダ、サイト、メールボックスのいずれかをクリックすると、そのアクセス権を持つユーザ、割り当てられているアクセスタイプ（読み取り、書き込み、実行など）、アクセス権の継承元などを確認することができます。またデータアクセスの詳細な情報が表示され、どのユーザのアクセス権を安全に失効できるかを表示することができます。DatAdvantageでアクセス状況を把握、その情報を基に分析を行いデータの管理者を設定するとIT管理者はそのデータ管理者に対して、DataPrivilegeオプションを用いた現場での権限付与や削除といった「権限管理の委譲」を行うことが可能になります。

Varonis METADATA FRAMEWORK について

スケーラブルなデータ保護と管理を継続するには、増え続けるデータ量とその複雑さに対応するテクノロジが必要となります。
そのテクノロジがVaronisが持つMetadata Frameworkです。
データガバナンスには、以下の4つのタイプのメタデータが重要になります。

・ユーザとグループの情報
Active Directory、LDAP、NIS、SharePointなどから取得。
・アクセス権情報
「どこに保存されているどのデータに、どのユーザがアクセスできるか」を把握。
・ アクセス状況
「どのユーザがどのデータにいつアクセスし、どういう操作を行ったか」を把握。
・ 機密コンテンツ情報の管理
「どのファイルに機密性の高い重要なデータが含まれ、どこに保存されているか」を把握。

Varonis Metadata Framework は、ファイルサーバに影響を及ぼすことなく、この重要なメタデータを収集しメタデータがない場合はメタデータを生成して前処理、標準化、分析、保存を行い、IT管理者が確認できるようにします。
Varonis Data Governance Suiteは新しいプラットフォームやメタデータが登場しても、Varonis Metadata Frameworkにシームレスに且つ容易に取り込むことができ、生産性の高い方法でデータを管理・保護することができます。

Varonis DATA GOVERNANCE SUITE

Varonisでは、ファイルサーバ、NASデバイス、Exchangeメールボックス、SharePoint Serverに存在する非構造化データを管理するための総合的な製品とメタデータフレームワークを提供しています。
Varonis DatAdvantage、DataPrivilege、IDU Classification Frameworkを使用すると、企業は実用的な運用管理、複雑なITタスクの自動化、高度なワークフロー管理の機能を導入することが可能となり、より効果的にデータを管理することができます。

Varonis DatAdvantage® for Windows
Varonis DatAdvantage® for UNIX/Linux
Varonis DatAdvantage® for SharePoint
Varonis DatAdvantage® for Exchange
Varonis DatAdvantage® for Directory Services

DatAdvantageのインターフェイスは統一されており、1つのインターフェイスを通じて管理者はデータガバナンスに関する処理を実行できます。

可視化

- 非構造化/半構造化ファイルシステムのアクセス権の構造を双方向のインターフェイスで確認できます。
- 任意のユーザまたはグループのデータアクセス権、及び任意のフォルダやSharePointサイトに対してアクセス権のあるユーザやグループを表示できます。
- ディレクトリサービスから抽出したユーザとグループの情報は、ファイル及びフォルダのアクセス権限データと連動表示されます。

総合的な監査ログ

- 監視対象サーバ全てのファイルに対して有効な監査を実施できます。
- 全てのファイルのイベントの検索が可能で、各イベントに関する詳細情報を取得できます。
- ファイルサーバへの影響を最小限に抑え、WindowsやUNIXの標準監査ログ機能を使用することなくデータ収集を行うことができます。

シュミレーションと適用

- 業務に支障を与えることなく、過剰なファイルアクセス権やグループメンバシップを削除することができます。
- 稼働環境に影響を及ぼすことなく、アクセス権の変更をシミュレーションすることができます。

データ所有者の把握

- ユーザアクティビティの統計分析により、データ管理者を効率よく特定できます。
- データ管理者単位でレポートを自動作成することができます。
- DataPrivilegeによって権限管理を現場へ委譲し、IT運用を効率化することができます。

Varonis
DATA PRIVILEGE

DataPrivilegeは、ユーザ及びデータ管理者(フォルダ毎の管理者) がアクセス権の変更や適用に関するワークフローに直接関与できるフレームワークを提供することで、データガバナンスを自動化します。ユーザ、データ管理者、IT管理者向けのWebインターフェイスにより、ユーザからのアクセス権限付与の要求及び、承認者による権限変更の承認、権限の確認・修正、ポリシーの適用(他の組織のユーザからの権限申請時は自動で棄却する設定など)が自動化されます。また総合的な監査機能によって、確実にデータガバナンスポリシーの適用と順守が可能になります。

アクセス権限の確認・修正の自動化

・データ管理者は定期的な権限のレビューが可能で、アクセス権の削除を推奨するレポート(DatAdvantageが生成)も取得可能です。
・ビジネスポリシーに基づいて、権限の状態確認レポートをスケジュール設定することができます。

アクセス権限申請のワークフロー

・アクセス権を申請するユーザはその申請理由と権限の使用期間を記入して、アクセス権を申請することができます。
・データの管理者が承認者となり、フォルダ単位やグループ権限単位で個別に承認者を指定することができます。
・承認の要件が満たされると、アクセス権の変更が自動的に実行されます。
・有効期限を指定した場合、アクセス権の失効は自動的に実行されます。

ビジネスポリシーの適用

・企業やITポリシーに基づき、複数の承認者を設定することができます。
・対象外の部門やユーザからの権限申請があった場合に自動的に申請を棄却するといったEthical Wall機能を使用することができます。

ポータルWeb

・ポータルを使うことで、データの管理者はフォルダやグループに対するアクセス権限を管理することができます。
・データ管理者はポータル上でアクセス状況の確認や統計情報を確認することができます。

総合的な監査とレポート作成

・承認ワークフローのイベントは全て記録されており、監査のために使用することができます。
・承認/棄却、権限の確認・修正を始めとする管理レポート機能により、ポリシーとプロセスの順守を証明することができます。

Varonis IDU CLASSIFICATION FRAMEWORK

Varonis IDU Classification Frameworkはファイルシステム全体でデータコンテンツを可視化し、機密データの保存場所について高度な情報を提供します。搭載している分類エンジンまたはサードパーティの分類製品からのファイル分類情報も統合させることができ、機密性の高いデータが存在するにも関わらず過度なアクセス権が付与されているフォルダレポートを出力できるなど、データガバナンスにおける実用的な機能を提供します。

実用的な機能

・分類機能により、機密性の高いコンテンツ情報を可視化することができます。
・機密性の高いデータを持つフォルダに不必要なアクセス権が付与されている場合などに、アクセス権限レベルを変更した際のシミュレーションを行うことができます。

拡張可能なアーキテクチャ

・IDU Classification Framework自身が提供するデータ分類エンジンでは、正規表現や辞書検索機能を用いて柔軟性の高い優れた方法で機密データを分類することができます。
・IDU Classification Frameworkでは、他社製の分類製品やDLP製品でのコンテンツ分類データを統合することができ、高度な分類処理を行うことができます。
・DatAdvantageによるリアルタイム検出機能により、ファイルの作成及び変更についての差分のみがスキャンされ、従来のソリューションよりも極めて高速に処理することができます。
・機密データに対するアクセス状態の確認やアクセス権の変更/削除といった操作を容易に行うことができます。

既存インフラストラクチャを活用

・導入済みの他社製の分類エンジンを使用できます。
・Varonis Intelligent Data-Use(IDU) Frameworkによって作成される独自のメタデータレイヤを使用します。
・Varonis IDU Framework機能はサーバやストレージを追加する必要はありません。
・Varonis DatAdvantage及び、Varonis DataPrivilege(今後対応予定)に結果を反映することができます。

簡単かつ強力な分類ルール

・ルール設定ではコンテンツとメタデータの両方の条件を組み合わせてマッチング(作成者、アクセス中のユーザ、アクセス権セットなど) させることができます。
・優先付けが可能です。(特定のフォルダを最初にスキャンするなど)
・キーワード、語句、正規表現のパターンでファイルを検索することができます。
・自動更新される辞書を用いたマッチング機能を搭載しています。

Varonis DATA TRANSPORT ENGINE

データの移行とアーカイブは人による作業でも簡易的なツールを用いてもIT部門にとっては時間と労力のかかる作業でした。ファイルサーバの統合の際にデータの移行や整理を行うケースが多いのですが、いざそれを実行しようとすると常に膨大な量の移行計画やテスト、調整、検証といったことが必要になり、最後は運任せといったことも散見されます。

Windows及びUNIXのファイル共有、SharePoint、Exchangeメールボックス/パブリックフォルダなどから横断的にアクセス権やアクセス状況、コンテンツメタデータを収集することで、Varonis Metadata Frameworkは、「使用しているどのデータが古いのか」、「どのコンテンツが機密性の高いまたは規制対象の可能性があるのか」、「どのアクセス権が過大または不適切に適用されている可能性があるか」など、データ移行・統合の効率性と安全性を向上させるにおいて重要な判断要素を提供することができます。

Varonis Data Transport Engine(DTE)には高度なルールエンジンとスケジューリング機能が備わっており、ITスタッフは、移行が必要なデータ、移行先、移行するタイミング、アクセス権を設定すれば、全てのデータ移行を自動的に実行できるようになります。例えば、メンテナンスのスケジュールを設定しデータとメタデータをコピーする、移行元のデータが「使用中」であっても差分のコピーによって移行元と移行先を同期する、プラットフォーム及びドメイン間でアクセス権を変更する、進捗状況をレポートする、といった作業を自動化することができます。
DTEは、Varonis Metadata Frameworkのアーキテクチャとの連動により、全てのデータが管理可能となります。対象データは適切なユーザのみがアクセスでき、使用状況が全て監視され、移行前後に不正使用があった場合にはフラグが立てられます。また、移行後のサーバを使用しているユーザは誰か、移行前のデータを未だに使用しているユーザは誰なのかも把握することができます。

VaronisData Transport Engineは、こういった細かな作業を全て自動化できるインテリジェントシステムであり、最終的にIT部門は、理想的なデータ移行・統合に関する概要情報だけを策定し、設定管理するだけで済みます。これにより、週末や夜中にデータ移行や統合を実施するといった必要もなくなります。またデータの移行・統合を設定し、実施前にシミュレーションを行っておけば、迅速かつ安全にデータの移行を実施することができます。

Varonis DATANYWHERE

Varonis DatAnywhereを用いることで、企業で既に利用しているファイルサーバを拡張し、プライベートクラウドのファイル同期サービスを実現することができます。リモートアクセスユーザは企業内のローカルリソースにアクセスしているものの、クラウドベースのファイル共有サービスと同じようなユーザビリティを体感することができます。DatAnywhereを使用することで、以下のことが実現できるようになります。

・自動かつ安全に社内のファイルサーバとノートPCやスマートフォン、タブレット間でファイルを共有する・同期を行うことができます。
・既存のディレクトリサービス（Active Directoryなど）を使用して認証することができます。
・外部のビジネスパートナーと安全な方法でファイルを共有することが可能です。

Varonis DatAnywhereは、既存の社内ファイルサーバにシームレスなアクセスを行います。リモートアクセスするユーザに対してはセキュアなhttpsを用いて通信を行い、社内のディレクトリサービス、アクセスコントロール、データ保護もシームレスに適用することができます。
企業は、既存のファイルサーバからデータを移動することなく、あたかもクラウドファイル共有サービスを利用しているかのような操作を体感することができます。導入においては既存ファイルサーバのアクセスコントロールリスト(ACL)及びグループを再設定する必要はなく、追加の機器を使用することによる新たな設備投資やIT管理者の運用負荷が増えることもありません。

また、他のVaronis Data Governance Suiteのソリューションと組み合わせて利用することで、社内のLAN経由でファイルサーバにアクセスする場合であっても、リモートでクラウド的にDatAnywhereを使用してデータアクセスする場合であっても、総合的なデータ管理を行うことができます。全てのデータに関して、データの所有者の特定、アクセス監査、疑わしい挙動の検出を行い、データがどこに保存されていても機密性の高いコンテンツの把握や保護、管理を行うことができます。

Varonisについて

Varonisはファイルサーバの権限管理・最適化を提供するソフトウェア開発会社でありそのリーディングカンパニーです。ファイルサーバの権限管理を通してデータ環境を安全かつ最適なものにするデータガバナンスの実現を目指しています。Varonisが持つ特許技術のメタデータフレームワークと非常に強力な分析エンジンを用いてお客様に総合的なアクセス権限の可視化やファイル分析機能を提供します。いつでも、どのデバイスからでも、正しいファイルに正しいユーザのみがアクセス権を与えられ、すべてのユーザのファイルアクセスをモニターし、不正な動きを感知するデータマネジメントソリューションを提供します。

30日間の無償評価版：

DatAdvantageのインストール数時間後には

インストール後すぐにアクセス権の監査を実行し、ファイル及びフォルダのアクセス権、特定のユーザ及び、グループへのアクセス権の割り当て状況を確認することができます。

DatAdvantageのインストール翌日には

データにアクセスしているユーザやアクセス方法を表示、レポートできるようになります。

DatAdvantageのインストール3週間後には

不必要と思われるアクセス権限やアカウント情報の抽出が可能になります。

VaronisSystems,inc. 東京事務所
〒100-6162
東京都千代田区永田町2-11-1 山王パークタワー 3F エグゼクティブセンター
TEL: 03-6205-3298
http://www.varonis.com/
お問い合わせ：jp-info@varonis.com

本社
1250 Broadway, 31st Floor, New York, NY 10001
Tel：877-292-8767 email：sales@varonis.com
英国/アイルランド
Varonis UK Ltd. WarnfordCourt 29 ThrogmortonStreet London, UK EC2N 2AT
Tel：020 3402 6044 email：sales-uk@varonis.com
西ヨーロッパ
Varonis France SAS 4, rue Villaretde Joyeuse75017 Paris France
Tel：+33 (0)1.82.88.90.96 email：sales-france@varonis.com
ドイツ/オーストリア/スイス
Varonis Deutschland GmbH Robert Bosch Strasse7 64293 Darmstadt
Tel：+ 49-0-6257 9639728 email：sales-germany@varonis.com