SecureAge

銀行業務のデータセキュリティ - 発想の転換が必要な時代

SecureAge ホワイトペーパー2020年

エグゼクティブサマリー

銀行の歴史は古く、何世紀にも渡りその業務を続けていることを考えれば、金融機関がセキュリティに精通しているのは当然といえます。取引と預金の保護に長け、セキュリティはそのDNAの一部であり、現代の金融機関は、このDNAを現代の技術に適用し続けています。

データセキュリティは、伝統的にストレージリポジトリを中心に構築されてきました。データベース内の情報を保護し、フルディスク暗号化とアクセス制御を使用して、誰がどのデータを利用できるかを管理しています。

問題は、データが想定された保管場所の外に移動すると、導入されているセキュリティ管理の効力を失うことです。そして、データは保護されていない状態になります。金庫から現金を取り出すようなものです。

ハッカーは非常に狡猾で、保護された場所にアクセスし、データを移動、窃取するエキスパートです。新型コロナウイルス危機により、安全な組織ネットワークの外で仕事をする従業員が何千人も増え、データの脆弱性が高まっています。また、この新しい環境では、多くのセキュリティコントロールを突破する必要すらない、悪意ある内部関係者の存在の可能性も忘れるわけにはいきません。

このホワイトペーパーでは、これらの問題をさらに詳しく解説し、データ自体にセキュリティを組み込むアプローチを検証します。その結果、データがどこに移動しようとも、データは常に保護されたままで、内外の悪意のある攻撃者による読み取りができなくなります。

データ侵害による評判とブランドの損害

現代の規制において、データ漏えいは確実に公にしなければなりません。罰金、損害、そして結果として生じる費用は相当なものになりますが、最も大きな打撃を受ける可能性が高いのは金融機関の評判とブランドです。Ponemon Instituteのレポート[1]は、データ漏えい後、顧客の65%が金融組織に対する信頼を失い、31%は実際に別の企業へ資産を移し換えており、8%の株価下落が見込まれることを示しています。

したがって、金融サービスのITプロフェッショナルの思考に、レジリエンス（回復力）、リカバリ（復元）、レピュテーション（評判）というスローガンが組み込まれていることは、それほど驚くべきことではありません。しかし、システムには回復力があっても、データが盗まれてしまうと、その制御は失われ、盗まれた情報は悪用される可能性があります。データが漏えいしているという噂が出ると、評判に続き、ブランドのダメージは避けられません。

> Desjardins Groupは、特権アクセス権を持つ悪意のある内部関係者が個人情報を窃取したことにより、データ侵害に起因するコストが1億800万ドルにのぼることを報告。回復案の一部は、自らも情報漏えいの経験を持つEquifax社によるクレジット監視であった。

機密データへの正当なアクセスの難しさ

金融機関は、顧客情報と取引の大規模なデータベースに加えて、取引報告書、人事記録、会議メモ、事業計画、財務諸表、アプリケーションとデータベースによって生成されたレポート、スプレッドシート、社内メモなど幅広いデータとドキュメントを保持しており、その多くは機密性が高いものです。ほとんどの国の銀行は顧客に対して機密保持義務を負っており、知的財産も他のデジタル資産とともに管理および保護する必要があります。

たとえば、企業との金融取引など価格の扱いがセンシティブな業務において、個々のドキュメントは暗号化され、パスワードでも保護されているでしょう。しかし、複数のチームメンバーが作業に関わり、時間的プレッシャー下でドラフトを作成したりその訂正に追われていたりする時などは、人的ミスを排除することはできません。これらのドキュメントの暗号化は手動で行われており、その都度個々のドキュメントを保護を選択し、忘れずにデータを暗号化を行うこと全てが、ユーザー任せになっているためです。それぞれに個別の決定をしなければならないことで、ファイルが保護されないまま保存され、窃取の危険にさらされる可能性があるというリスクを生み出します。

この複雑さのため、機密として分類された情報にはより強力な保護を適用し、重要性の低いデータにはより弱い保護を適用するなど、組織は主観的な判断に基づいてデータを分類します。そして、コストの問題、かつての不十分なテクノロジーの経験、規制当局がこの考え方を後押ししています。たとえば、Payment Card Industry Data Security Standard（PCIデータセキュリティスタンダード）は、カード会員データを保存と送信の両方で暗号化し、その他の機密性の低い情報はアクセス制御によってのみ保護することを推奨しています。

機密性が高く脆弱なデータを特定する（非）現実的側面

しかし、脅威が進化を続けるなかで、その脅威すべてを軽減するには、どのような種類のデータに価値があって常に保護するに値するのか、どの情報はそれほど保護する必要がないのかを決定することは、全く現実的ではありません。

たとえば、ある幹部の旅行計画は特に重要とは思われないかもしれませんが、ハッカーはソーシャルエンジニアリング攻撃の形でこの情報を使用し、その人物または同僚の一人をだまして大口取引や支払いを持ちかけ、またはうっかりマルウェアをインストールしてしまうように仕掛けることができます。

理想の世界では、ITセキュリティマネージャーが継続的にデータ脅威の状況を確認し、それを最新のテクノロジポリシーに変換して、新たに機密として指定されたデータの保護レベルを強化するでしょう。しかし、現実的にはこの期待は大きすぎます。他の作業や、問題が発生時の火消し活動に時間を取られて、実行することはまず不可能です。

1　Ponemon Institute: The impact of data breaches on reputation and share value（データ侵害が評判と株価に与える影響）

組織の進化がもたらした複雑なITセキュリティパッチワーク

大規模な金融機関は20年や30年に及ぶ合併や買収の結果として、幅広い法域にある数十（数百ではないにせよ）の異なる企業体を抱えているだけでなく、多数のレガシーITシステムを所有している傾向があります。

その結果、ITプロフェッショナルは、銀行のATMネットワークのセキュリティの抜け穴など、すぐに対応する必要がある問題がレガシーシステムで発生した場合の対応に、かなりの時間を割かなければなりません。このホワイトペーパーのためにインタビューした、業界で豊富な経験のある最高情報責任者は、このプロセスを、複雑なインフラストラクチャ管理の現実に起因する「モグラたたき」と表現しています。

データセキュリティサイロ

現在のITセキュリティでは、フルディスク暗号化、データベース暗号化、アプリケーションセキュリティに加え、門番として機能するアクセス制御を使用して、データストアの場所を保護することに重点を置いています。問題は、ドアの向こうにあるデータが本質的に保護されていないため、門番をかわして入り込んだ人はデータを盗むことができるということです。

> 暗号化ストレージメーカーApricorn社のレポートによれば、リモートワーカーはデータのセキュリティを気にしていません。IT意思決定者の半数以上が、リモートワーカーをデータ窃盗のリスクとみなしています。

このサイロ化されたアプローチが取られているのは、それが実用的なソリューションだからです。重要なのはデータであることはわかっていても、データ自体を保護するよりも、各データストアを保護する方が簡単です。私たちはこの問題を認識していますが、ファイルの暗号化やパスワードなど、セキュリティを強化するために追加の手順を人々に強制しようとしても、せいぜい生産性が低下するだけで、人的ミスが発生するか、単に無視されるだろうということも知っています。

もちろん、ネットワークで不正なデータ転送や異常な動作を監視することはできますが、これはセキュリティサイロアプローチがデータストア間の脆弱なギャップを残していることを受け入れているだけです。

ITセキュリティは難しいのです。

ITセキュリティ教育

ITセキュリティ教育を使用してスタッフをITセキュリティに関与させ、脅威を認識させることは、データ、システム、およびネットワークを保護するための極めて重要な部分です。

ただし、ソーシャルエンジニアリングなどの技術の高度化に伴い、スピアフィッシングやディープフェイクが増加し、人的ミスの可能性も高まっています。ランサムウェアやその他のマルウェアを投下するリンクを誤ってクリックするのはあまりにも簡単です。

新型コロナウイルスが新次元を追加

そして、パンデミックがやってきました。組織は、従業員による在宅勤務のサポートに迅速かつ見事なまでに対応してきました。従来の災害復旧計画ではこの状況は想定されていませんでした。

これは単なる短期的な危機管理の問題ではありません。在宅勤務の成功は、それをコスト削減の潜在的な源と捉える雇用者と、通勤時間と諸々の費用を削減できる方法と捉える従業員の両者にとって、転換点として機能するかもしれません。

> 「私たちのロケーション戦略は長期的に調整されるでしょう。建物に7,000人を配置するという考えは、今や過去のものなのかもしれません。」
>
> ジェス・ステイリー、Barclays Bank CEO

新たに購入したハードウェアや、従業員所有のデバイスを使用したリモートワークへのこの大規模な移行によって、ハッカーや悪意のある内部関係者に対する監視が弱くなり、より脆弱な攻撃ベクトルが提供されることになります。

このことを踏まえて、「ニューノーマル」に対応するには、データセキュリティを再検討する必要があるでしょう。

すべての組織がハッキングされる

「組織には3つのタイプがあります。侵害され、それを知っている組織。侵害され、それを知らない組織。そして、まだ侵害されていない組織です。」- 最高情報責任者いつの日か、複雑なパッチワークのセキュリティサイロの間をすり抜けて、システムに悪意ある人物が侵入し、意図的に操作を行うかもしれません。彼らは現代版銀行強盗の実行を目論んでいる可能性があります。

> 1億600万人の個人情報が盗まれたCapital One社のデータ侵害は、サードパーティのクラウドサービス従業員が得た内部情報によるものだった

ランサムウェアを仕掛け、データと引き換えに身代金を要求してくるかもしれませんし、出張の予定や個人的な関心、スタッフの昇進など、一見無害に見えるデータを収集蓄積して、サイバー攻撃の緒を探しているのかもしれません。

攻撃は、ハッカー、犯罪者グループ、さらには国家が関わる可能性もあります。しかし、侵害されたユーザーアカウント、悪意のある内部関係者、または正当に内部組織に在籍する悪意のあるサードパーティサービスの従業員は、保護されていないデータが、簡単に手の届くところにあるのですから、セキュリティコントロールをハッキングする必要はありません。サイロの外にそれを移動するだけで、データ盗難は完了です。

データが本質的に安全であれば、それがどこに持ち出しされたか、複製されたかに関わらず、データを盗難されることはありません。

発想の転換が必要な時代

データを保護する障壁とアクセス制御は重要ですが、データ自体の保護にも焦点を当てる時がきています。

これには、人的ミスや悪意というリスク要素のほとんどを取り除く、事後対応型から事前予防型データセキュリティアプローチへの切り替えが必要です。データをシームレスに暗号化することで、情報はシステムから移動された瞬間に使用できなくなり、データ侵害の被害を確実に抑えることができます。

SecureAge – 予防型のデータセキュリティ

SecureAgeはセキュリティを再考し、単にデータの保存場所を保護するのではなく、データ自体を保護する予防型セキュリティを提案します。SecureAgeの哲学は、セキュリティをデータに内在するプロパティにすることです。実際には、そのデータのDNAを微調整しながら、日々データを生成し使用している人達が気づかないような形で、セキュリティを内在させます。

> 南アフリカのNedbankの顧客170万人の個人情報が、データ暗号化を採用していないサードパーティプロバイダーのデータ漏洩によって、犯罪者の手に渡った

つまり、セキュリティを損なうことなく、データを他の場所に移動やコピーすることができます。データベースのエクスポートなど新しく生成されたデータでさえも内在的、本質的に保護されています。

データ保護とは、本来こうあるべきだったのです。

SecureAgeは暗号化を使用して、基本的なデータコンテナであるファイル内の情報を保護します。これはバックグラウンドで行われるため、アクセス権のあるユーザーも、アプリケーションも、暗号化アクティビティが行われていることに気づきません。ファイル内のデータを暗号化することにより、権限のあるユーザー以外には復号できなくなりますから、ファイルは流出しても役に立ちません。レガシーも、現在または新規のアプリケーションも、そしてデータベースもすべて、一切の変更を必要とせず、またパフォーマンスに大きな影響を受けることもなく、この100%暗号化の恩恵を享受することができます。

認証された暗号化

ユーザーごとまたはサービスごとの暗号化キーを使用することにより、権限のある個人またはプロセスのみがデータにアクセスできます。この認証された暗号化により、データのセキュリティと認証の両方がデータ自体に組み込まれます。権限のあるユーザーのみがデータを読み取ることができます。管理者でさえ、自分の鍵を含まない情報を解読することはできません。

特権ユーザーは引き続き、必要に応じてファイルを移動したり復元したりして、自らの任務を遂行することができますが、ファイルの内容にアクセスすることはできません。これにより、通常データを盗むのに最適なポジションにいる特権ユーザーとデータベース管理者という、組織が直面している最も困難な脆弱性の1つが解消されます。

SecureAgeの使用によりデータは本質的に保護されるため、職場ではファイルを閲覧できる正当な権限を持つユーザーであっても、一度組織の外にファイルを持ち出すとそのデータは暗号化されたままであり、読み取ることができないことに気付きます。これは、認証された暗号化がデータストアの属性ではなく各ファイルの一部であるためです。

クラウドデータセキュリティ

SecureAgeを使用すれば、クラウドがセキュリティのリスクを高めることはありません。データは、クラウド、サーバー上、在宅勤務者のラップトップで生成されたレポートなど、保存場所を問わず暗号化されたままです。

このアプローチのさらなる利点は、データストアへのアクセス制御が不正確であっても、それほど重要ではなくなることです。また、設定ミスのリスクや、クラウドサービスプロバイダーなどのサードパーティによる特権ユーザーアクセスのリスクが軽減されます。

クラウドセキュリティ会社Ermeticのレポートによれば「パブリッククラウドは動的なオンデマンド環境であるため、ユーザーとアプリケーションが不要なアクセス権を蓄積することがよくあります。企業の80%は、機密データへの過剰なアクセスを特定できていません。」[2]

正確なアクセス制御が重要なのは明らかですが、SecureAgeを使用すれば、不適切に保護されたストアからデータを盗むハッカーや悪意のある内部関係者は、データが暗号化されていて読めないことに気付くでしょう。

2. 過去1年半の間に、5社中4社近くの企業がクラウドデータ漏洩に見舞われています: https://www.itproportal.com/news/nearly-four-in-five-businesses-suffered-a-cloud-data-breach-in-past-year-and-a-half/

プロセス実行制御

SecureAgeは、マルウェア、ランサムウェア、キーロガーなどの不正なプロセスの実行をブロックし、さらなるレベルの保護を提供します。プロセス実行制御により被害の発生を確実に防ぐことができれば、サーバーは稼働を続け、スタッフは作業を継続することができる上、データはいつも通り利用できます。

この「許可リスト」機能は、外部からの攻撃と内部関係者からの脅威の両方を防ぎ、すべての不要なソフトウェア、スクリプト、ファイルレス攻撃が実行できないようにします。

最近注目を集めたランサムウェア事件には、Travelex社やDiebold Nixdorf社、またレディー・ガガに関するファイルがハッカーグループによって漏洩したニューヨークの法律事務所Grubman Shire Meiselas & Sacksなどがある

データを盗み、脆弱性を特定して悪用し、企業ネットワークへのバックドアを開こうとする、ハッカーからのマルウェアの実行をブロックします。

SecureAge – 本来あるべき形の透過的データ暗号化

SecureAgeは、ユーザーに向けて、セキュリティを自然で、内在的かつ自動的なものにするシームレスな体験ができるよう設計されています。データ暗号化に関連するプロセスを完全に非表示にすることで、人的ミスとその可能性は大幅に減少し、誰かが誤って悪意のあるリンクをクリックした場合でも、許可されたプロセスしか実行されません。

保存場所を問わず、暗号化をすべてのデータに拡張することにより、保護レベルを選択する目的でデータ分類する必要がなくなります。これにより、ITセキュリティマネージャーは、どのデータがより重要であるかを決定する責任と負担から解放されます。

クラウドサービスの急増に加え、新型コロナウイルスの影響で、制御されていないネットワークやエンドポイントからの広範なデータ使用せざるを得ない状況から、単にストレージサイロを保護するのではなく、データ自体を保護すべき時が到来しました。SecureAgeは、人によるセキュリティに関する意思決定を排除することにより、ファイルレベルのデータ暗号化を主流とする時代を現実にします。

よくあるご質問

SecureAgeとは？

SecureAge Technologyはシンガポールに本社を置くデータセキュリティ企業です。2003年の設立以来、政府および企業のデータを、最新の執拗なサイバー脅威から保護する実績を積み重ねています。SecureAgeのクライアントには、シンガポール金融庁をはじめ、すべてのシンガポール省庁、法定機関、シンガポール軍および日本の国立研究法人などがあります。事業法人顧客は、成田エアポートテクノ、ソニー（マレーシア）、ブリティッシュ・アメリカン・タバコ、Temasek Holdings、タイ政府貯蓄銀行、およびGRG Bankingなどです。

これまで誰もこのサービスを提供しなかったのはなぜですか？

初期の暗号化技術は、その複雑さ故に大変使いにくく、ユーザーにもアプリケーションにも混乱を引き起こすような代物であり、その結果ユーザーは強力な保護が必要だと思われるデータカテゴリのみを選択して、暗号化せざるを得ないアプローチにつながりました。暗号化は難しいものだとみなされてきたのです。こうした観点から、データ暗号化の実装によりユーザー、アプリケーション、またはサーバーに影響を与えることのない「フルディスク暗号化」が広く展開され、これにより、組織は「データ暗号化」をしているとされてきました。問題は、フルディスク暗号化は電源がオフになっているマシンのみを保護し、暗号化は暗号化が有効になっているディスクドライブにのみ適用されることです。別のドライブに保存されたデータは、まったく安全な状態ではないのです。

SecureAgeの次世代製品はデータの暗号化を適切に実装し、システムの実行中やデータの変更中でも情報は暗号化されたまま保たれます。重要なのはデータです。従って、SecureAgeでは、情報の保護と認証が、データに内在するように設計されています。SecureAgeは、ファイルシステムレベルで動作することにより、すべてのアプリケーション、データベース、およびサービスを透過的にサポートするため、ユーザーやアプリケーションは作業方法を一切変更する必要がありません。

SecureAgeはパフォーマンスにどのような影響を与えますか？

SecureAgeはCPUに特別な暗号化機能を採用しているため、通常のデータ処理は暗号化操作を待つ必要がありません。さらに、データ使用時には、システムメモリに格納する必要があるデータの部分のみが復号され、ディスク上のファイルは常に暗号化されたままになります。SecureAge暗号化エンジンを介した、このデータのストリーミングとハードウェア暗号化機能の組み合わせにより、ユーザーはパフォーマンスへの影響に一切気づくことはありません。

SecureAgeは、どのファイルタイプ、フォーマット、データベースに対応していますか？

SecureAgeはファイルシステムレベルで機能するため、アプリケーションに影響を与えることなく、すべてのファイルタイプ、データストア、およびすべてのデータベースに対応しています。ソフトウェアを変更する必要はありません。データのセキュリティと認証は各ファイルに組み込まれているため、使用前にファイル全体を復号することなく、ファイルを読み取り、変更ができます。

SecureAgeで暗号化されたファイルの内容を検索できますか？

はい。データへのアクセス権があるユーザーは、Microsoft Word、Excel、PowerPoint、Adobe PDFなどすべてのファイルの内容を検索できます。

GDPR（EU一般データ保護規則）およびその他のデータプライバシー規則に基づく義務は、どのような影響を受けますか？

組織が個人データ漏洩を被っている場合でも、攻撃者が暗号化されたデータセットを取得した場合には、GDPRの第33条に基づくICO[3]への通知が必要となります。ただし、盗まれたデータをアクセス権のない人物が読み取れないように組織がデータの暗号化を実装している場合には、個人への通知は必要ありません。

SecureAgeはどのコアバンキングシステムで動作しますか？

SecureAgeの暗号化に対するファイルシステムレベルのアプローチは、Finastra、Finacle、Flexcube、Temenos、およびその他の現在およびレガシーシステムを含む、幅広いコアバンキングシステムに適用できます。

一部の領域でより高レベルのセキュリティを実装できますか？

SecureAgeによって暗号化されたすべての情報は、最高のデータセキュリティを提供する最新の標準的な暗号化アルゴリズムによって保護されます。ただし、認証のセキュリティレベルは、異なるセキュリティ要件を満たすように選択できます。たとえば、非常に機密性の高い情報にアクセスできるスタッフは、多要素認証付きのスマートカードを使用して復号キーを保護を行い、それ以外はソフトトークンとパスワード認証をキーの保管に使用するなどです。

SecureAgeの展開は、「ビッグバン（一括導入）」方式で行う必要がありますか？

いいえ。SecureAgeは、ご都合に合わせて段階的に実装できます。仕事に影響を与えたり、組織内の他部署と連携する必要なく、個人、グループ、部門、または部署が製品をインストールして、データのセキュリティを強化できます。

次にすべきことは？

制御されていない環境から情報がアクセスされ、サイバー攻撃の件数が増大し、ますます巧妙になって、内部関係者によるデータ窃盗の脅威がある現在、現状に疑問を投げかける必要があります。

100%のデータ暗号化は、すでにあなたが受け入れている原則であり、フルディスク暗号化はこれを実現します。ただし、実行中のシステム上にあるファイルをサイロから別の場所にコピーしても、暗号化が維持されるように、この原則をより適切に実装する必要があります。さらに、認証は暗号化されたファイルに組み込む必要があります。これにより、悪意のある人ではなく、権限のある個人のみがデータを復号できるようになるからです。

ついに、データセキュリティは、事前に予防的なアプローチで管理される時がきました。

3　第34条(3)(a)は、組織が次に当てはまる場合には、個人への通知は不要であると規定しています。「適切な技術的および組織的保護措置を実装し、かかる措置が個人情報漏洩を被った個人情報に適用されていること。特に、暗号化などの方法で、個人情報にアクセスする権限のない人には個人情報が理解できないようにしていること。」

SecureAge Technology

SecureAge Technologyは、シンガポールに本社を置き、真のセキュリティと使いやすさを両立させるデータセキュリティ企業です。SecureDataは、改良されたPKIセキュリティ技術をベースとして、2003年にシンガポール政府のために初めて発売されました。SecureAgeは、自社特許であるPKIベースの暗号化を、内在する透過的なデータ保護コンポーネントとしてまとめ上げたもので、瞬く間にデータ暗号化パートナーとしてその他の政府機関や公共機関から選ばれるようになりました。こうした長期的かつ深い密接な関係から、SecureAgeは大規模かつ複雑な組織のデータを保護する広範な経験を蓄積してきました。

SecureAgeのデータセキュリティソリューションは、公共機関や民間企業がそのネットワーク内のデータ移動を完全に制御できるようにします。すべてのファイルを、いつでも、どこでも。

SecureAgeのセキュリティ製品は、最高レベルのデータ保護を必要とする組織にお選びいただいています。顧客には、シンガポール、香港、および日本の政府系機関や、ブリティッシュ・アメリカン・タバコ、ソニー（マレーシア）、成田エアポートテクノ、タイ政府貯蓄銀行、GRG Bankingなどが含まれます。

SecureAge Technology:
データセキュリティへのアプローチ

予防的な保護とは

データセキュリティ

データセキュリティとは、遍在的な暗号化を意味します。データは、最も基本的な自己完結型の単位であるファイル上で保護する必要があります。競合する他のソリューションは、一部のデータのみを非恒久的に保護していたり、セキュリティよりもコンプライアンスを重視していたり、複雑化して逆にリスクをもたらしています。また元から内部にいるユーザー（どのシステムでも最も脆弱な部分）に対して、境界防御を施すだけでは不十分です。

アプリケーションの整合性

アプリケーションの整合性とは、「許可リスト」と、アプリケーションへのデータの結び付けによる制御を意味します。認証されたプロセスのみが、特定の目的で特定のデータにアクセスすべきです。従来のマルウェア対策システムは受け身的な保護の代表的なもので、それでは手遅れです。このようなシステムの焦点は既知のマルウェアに置かれ、すでにアクティブな悪意のあるプロセスを阻止しようとするためです。

ユーザビリティ

ユーザビリティとは、本質的で意識されない透過的テクノロジーを意味します。ソリューションにおいては、人的要素を構成部分にしたり、変えようとするのではなく、完全に排除する必要があります。トレーニングやモニタリングは常に機能するわけではなく、ソリューションが自然でないと、人は独自の（セキュアではない）方法を編み出すものです。ユーザーは、追加の検討事項なく、思い通りにまたは必要に応じて作業できる必要があります。

トレードオフなし

SecureAgeでは、これらの原則の間にトレードオフはありません。特に、データセキュリティを強化するためにユーザビリティが犠牲になることはありません。適切な方法が難しいと、人は何かを達成するために他の方法を見つけるものです。これを認識することがSecureAgeの製品設計の基本原則です。

詳細はこちら

SecureAgeのエンタープライズデータセキュリティソリューションの詳細は、当社までお問い合わせください。SecureAgeの使用によって貴社のデータセキュリティを強化する方法や、無料トライアルについても、お気軽にお問い合わせください。

ウェブサイト www.secureage.com

SecureAge

シンガポール 3 Fusionopolis Way, 05-21 Symbiosis, Singapore 138633
英国 74 Mackie Avenue, Brigton, BNI 8RB, Company No. 11734665
日本 105-0001 東京都港区虎ノ門1-16-6 UCF7F
北米 1801 Old Reston Ave Suite 301 Reston, VA 20190, USA