SecureAge

内部犯行による情報漏洩を防止するSecureAgeの次世代暗号化技術

SecureAgeホワイトペーパー2020年

現在のITセキュリティと当社の見解

いろいろな分野の企業が厳格かつ制御された方法で、ITセキュリティの実装を手助けするために、さまざまなサイバーセキュリティフレームワークが存在します。たとえば、ISO IEC 27001/ISO 27002、米国NISTサイバーセキュリティフレームワーク、英国NIS規制サイバー評価フレームワークなどがあります。フレームワークとは、プロセス、プラクティス、技術を含む限定された構造を通じて、効果的なサイバーセキュリティ戦略を実施・維持するためのプロセスを形式化するのに役立つ優れた手法です。企業は、これらのフレームワークをを使用して、セキュリティの脅威からネットワークおよびコンピューターシステムを保護できます。

それでも攻撃はすり抜ける: たとえサイバーセキュリティフレームワークに予算と時間が費やされても、攻撃はそれをすり抜けて、データは簡単に盗まれてしまいます。すべてのデータ侵害を排除することは難しいものの、このホワイトペーパーでは、情報の損失と組織への影響を最小限に抑えるために暗号化テクノロジーを使用する方法を説明します。

> 「一部の『マルウェア』は、すり抜けてくるという事実を受け入れることが、攻撃を受けたその日の内に計画を立て、引き起こされた損害を最小限に抑えることに繋がります。」
>
> 英国国家サイバーセキュリティセンター

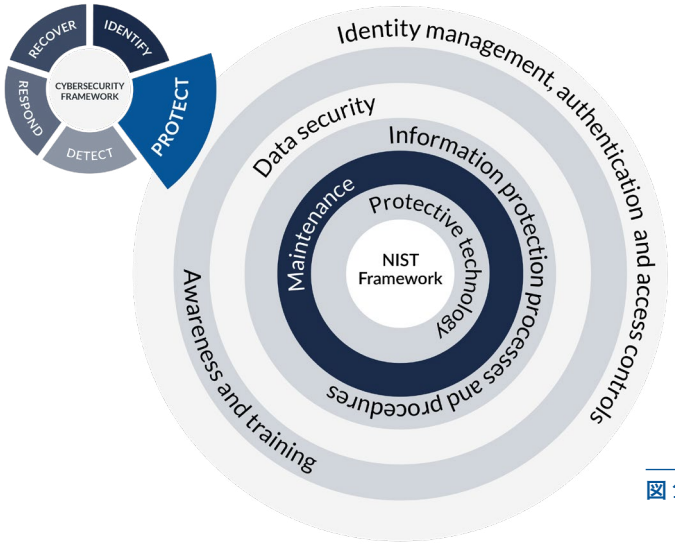

図 1 NIST フレームワーク

ドキュメント構造

サイバーセキュリティフレームワークには、コア機能が含まれる: サイバー攻撃からの防御について、これからNISTフレームワークを使用して議論を行いますが、ここで提起された問題は、サイバーセキュリティフレームワークのいずれにも等しく適用されます。

次のセクションでは、「防御」フレームワーク機能の6つのNISTカテゴリーをリスト化し、それぞれの中で一般的に導入されているテクノロジーについて説明します。各テクノロジーについて、一般的なデータ漏洩のシナリオをご紹介し、データの損失や盗難に焦点を当てた、より広範なセキュリティ上の懸念事項についてみていきます。それに続いて、SecureAgeの製品であるSecureDataが、ハイライトされた問題に対して具体的にどのようなソリューションを提供できるのか、ご紹介します。

SecureAgeのSecureDataは、最も基本的なファイルレベルの暗号化で情報を保護します。データへの不正アクセスをブロックしたり、保護するデータを選択したりするような他のサイバーセキュリティ製品とは根本的に異なり、暗号化によりファイル内のすべてのデータを本質的に保護します。

NISTカテゴリー1
ID管理とアクセス制御

ID管理と認証システム

さまざまなユーザーログイン、シングルサインオン、マルチファクター認証システムが存在しますが、これらは権限を持つユーザーだけがシステムやネットワークにアクセスできるように設計されたものです。強力な認証は、特に脆弱なリモートデスクトップ環境下でも重要となります。なぜなら、リモートマシンが既にマルウェアに感染している可能性があり、アクセスを試みるユーザーは誰もが、物理的に自分のアクションを隠すことなく、これを行うためです。

データ漏洩のシナリオ

正当なユーザーが、アプリケーションデータをローカルファイルにコピーします。このファイルは、アプリケーションまたはデータベース内の制御では、もはや保護されません。ファイルは簡単に盗まれる可能性があります。

> Morrisons Supermarketのある上席監査役が、会社への恨みから同社に損害を与えようと、約 10万人分の従業員の給与データ を漏洩。データベースアプリケーションからエクスポートされた後、ローカルファイルに保存され、流出した。

セキュリティ上の懸念

内部犯行によるデータ盗難や漏洩したユーザーアカウント: ユーザーは、業務遂行のために機密情報にアクセスする必要があります。したがって彼らはデータを盗むのに理想的な立場にいるのです。これは、悪意のある従業員だけでなく、漏洩したユーザーアカウントも同様です。

ソリューション

情報は、コピー先にかかわらず流出を防ぐ必要があります。ファイルが内部関係者によって盗まれた場合や、ユーザーアカウントが漏洩した場合も、情報データを保護する必要があります。ファイル内のデータの基本的な保護は、盗まれた情報の保護につながります。

SecureAgeのSecureDataを使用すると、認可されたユーザーはいつもと同じように作業を続けることができますが、その裏でファイルは暗号化され続けます。このため、ファイルを盗んだとしても、データは暗号化されたままなのです。盗まれたドキュメントを開こうとする試みは失敗に終わります。リモートデスクトップ環境ではSecureDataによってデータの暗号化が強制され、その間SharePointやその他のWebDAVベースのサービス情報は、アプリケーションの権限からサーバーまたはクラウドストレージに至るまで暗号化され、セキュリティ保護されます。

アクセス制御リスト(ACLs)

アクセス制御リスト(ACLs)と最小特権の原則は、個人が業務を遂行するために必要な情報にのみアクセスできるように設計されています。この手法は、データベースやアプリケーション内にも適用されます。GDPRなどのデータ保護規制では、データを処理する正当な理由のある個人だけがデータ処理できるようにする必要があると定めています。管理者に正当な必要性を持たせず、そのアクセスを制限する制御の対象となるべきです。

データ漏洩のシナリオ

権限をもつユーザーが、知的財産を含むファイルにアクセスし、データを窃取します。ファイルへの正当なアクセス権を持っている個人は、業務のためアクセスする必要がありますが、その際に彼らはファイルを盗むことができます。NSAでのエドワード・スノーデンの行動は、おそらくこの種の最も知名度の高い出来事でしょう。

> ケベック州の教員約36万人の個人情報が漏洩。ハッカーは、ユーザーコードとパスワードを盗んでデータへのアクセスを可能にし、容易に情報を窃取。

セキュリティ上の懸念

権限をもつユーザーによるデータへのアクセス: ACLsでは、本来会社が閲覧を許可していない場合でも、権限をもつユーザーがファイルにアクセスしてしまうという事態がよく起こります。権限を持つユーザーはACLsを設定し、管理者にファイルの移動、バックアップの復元などを行うことを可能にしますが、不正な管理者によって悪用される可能性のあるACLsを自由自在に変更できるのも、権限を持つユーザーです。組織から一旦削除されてしまえば、もはやどのファイルもACLsの対象ではなく、保護されません。

ソリューション

SecureAgeのSecureDataでは、アクセスする権限を持つ個人のみが、各ファイルを復号できます。もちろん、これはアクセス制御に沿っている必要があります。その個人にデータが盗まれた場合でも、SecureDataで保護された環境から流出したファイルは暗号化されたままであり、組織外では役に立ちません。普段よりデータへのアクセス権をもっている内部者の犯行であっても、組織外では復号できません。

NISTカテゴリー2
意識とトレーニング

サイバーセキュリティ意識

サイバーセキュリティ啓発トレーニングは、あらゆる組織のITセキュリティアプローチにおける重要な要素です。従業員、請負業者、関連する第三者が、ネットワーク、システム、データを保護する行動をとるように教育することは、シンプルですが強力なステップです。しかし、新人スタッフに対してプライバシーとデータ保護啓発トレーニングを課している企業は49%に留まり、定期的なリフレッシュ・トレーニングを行っている企業は4分の1未満に留まります[1]。

データ漏洩のシナリオ

攻撃者は、ソーシャルメディア、会社のプレスリリース、ブログを利用して、企業の上層部を念入りに監視しています。この知識を武器に、ターゲットにされた人にEメールが送信されます。Eメールには、特定の情報が含まれており、一見本物にみえることから、社員は有害なリンクをクリックします。悪いことは何も起こっていないようにみえますが、背後ではハッカーの侵入を許すマルウェアが導入され、データの漏洩が始まります。

> Travelexはランサムウェア攻撃を受けた結果、数週間のあいだ手動処理で業務をするはめに。取引先は外貨両替をできず、一般客は自己負担を強いられた。顧客情報が盗まれたとの情報もある。

セキュリティ上の懸念

有害なアイテムをクリック: 多忙な人やプレッシャーを感じている人は間違いを犯します。そして、スピアフィッシング攻撃、ソーシャルエンジニアリング、いくつかのマルウェア・ステルスの先鋭化に伴い、攻撃のいくつかが成功してしまうのは驚くことではありません。マルウェアが配置されると、ネットワークからファイルが静かに流出し、システムやネットワークに大きな損害を与える可能性があります。

内部者による、マルウェアのインストール: 従業員や契約社員が買収されるなど、組織のネットワークにマルウェアをインストールするよう説得されるかもしれません。事実、この手口はAT&Tで行われ、この仕掛けられたマルウェアは、5年間検出されませんでした。

ソリューション

SecureAgeのSecureDataを導入しても、マルウェアはデータを流出できます。しかし、盗まれたファイルは暗号化されたままなので、悪意のある犯行者の役には立ちません。また、SecureAgeのSecureAPlusは、すべての不正プロセスの実行をブロックします。これは、シナリオに登場する社員が有害なリンクをクリックしたとしても安全であることを意味します。マルウェアが万一ダウンロードされたとしても、実行しようとするとSecureAPlusがそれをブロックします。

1　エクスペリアン/ポネモンデータ漏洩調査では、49%が新入社員の研修を実施しています。毎年トレーニングを実施しているのはわずか24%でした。

NISTカテゴリー3
データセキュリティ

データ損失/漏洩防止 (DLP)

DLPは、ユーザーが組織外に重要な情報や機密情報を送信することを防ぎます。実際には、ネットワークを通過する際に機密データを認識してブロックします。DLPの実装は、すべてのネットワーク資産とストレージロケーション、および認可されたビジネスプロセスを包括的かつ正確に識別する必要がある重要なプロジェクトです。

データ漏洩のシナリオ

内部犯行者は、そのアクションが正当であることをDLPシステムに示します。DLPはビジネスコンテクストを認識しないため、これらのアクティビティは許可され、データは漏洩します。

> 産業機密がゼネラル・エレクトリック社から盗まれ、情報は夕日の画像のバイナリーコードに隠されて外部に流出。ステガノグラフィー（データ隠蔽技術）がDLPシステムを回避。

セキュリティ上の懸念

未完了のDLPコンフィギュレーション: DLPのデプロイメントを成功させるには、多くの変数が関与します。データ損失のすべての可能性を考慮しない限り、機密情報の漏洩につながります。十分な努力を払わずにシステムの微調整に取り組むと、不注意なデータ漏洩を招く可能性があります。DLPが機密データの流出を認識できない場合、情報は漏洩し続け、ユーザーはコントロールできません。

ソリューション

SecureAgeのSecureDataでは、すべてのデータファイルが常に暗号化されるので、DLP構成の偶発的または意図的な抜け穴のいずれでもデータ損失を招くことがありません。SecureAgeを使用してもパフォーマンスや運用上の影響はありませんので、すべてを暗号化することは理にかなっています。ユーザーがDLPに悪意のあるアクティビティを許可し、データを失った場合でも、組織外では役に立たない、暗号化されたデータを失うだけです。

データ分類と権限の管理

データ分類システムは、一部では、アクセス範囲と情報のセキュリティを定義するために使用されますが、暗号化はデジタル権限を行使するために、適切に分類されたデータに適用されます。しかし、暗号化は実装が難しく、動作が遅く、使用しにくいと考えられているため、通常はあまり使用されていません。

データ漏洩のシナリオ

ユーザーが機密文書を誤って分類すると、データ保護レベルの低下を招きます。ユーザーが情報分類することを許すと、プライバシーと情報セキュリティの因果関係を誤解し、これが誤った判断につながる可能性があります。さらに、自動分類プロセスは誤解の余地がないものではなく、企業は、今日「通常」であったデータが、明日は「機密」になる可能性を認識する必要があります。

> Desjardins Groupの悪質な社員が、自分の正当なユーザー資格情報を悪用して、約290万件の顧客アカウントデータの記録を窃取。DLP(情報漏洩対策)があっ たと推定されるが、なぜか機密データエクスポートの検出には失敗。

セキュリティ上の懸念

誤分類は、不適切なセキュリティにつながる: 前述のように、機密性の高いドキュメントまたは機密情報に分類されるドキュメントは、暗号化によって保護されてる必要があります。しかし、このレベルのセキュリティを使用することが難しい場合、そのままにしてしまうことがあるでしょう。スタッフは、簡単だからといった理由で文書を誤って分類することがあります。自動分類プロセスは有効ですが、ファイルが「検出」されない場合、それらは分類されないため、適切に保護されません。さらにデータベースファイル、一時ファイル、ログファイルは、多くの場合機密情報を含みますが、通常これらも分類されません。多くの分類および権限管理システムは、一般的に使用されるファイルタイプに対してのみ適用されます。今後は、すべてが機密であると仮定してみるのはどうでしょうか？そうすれば、データのセキュリティははるかにシンプルになります。

ソリューション

SecureAgeのSecureDataでは、ファイルの種類を問わず、すべてが暗号化されるため、ITセキュリティの観点から、データが正しく分類されているかどうかといったことは問題になりません。SecureDataは、ユーザーの期待どおりに動作し続け、透明で見えない暗号化を提供するように設計されています。パフォーマンスの低下やアプリケーションへの干渉も無く、ユーザーの手を煩わせずに、データを強力に保護します。

データベースの暗号化

ほとんどの商用データベースは、暗号化のオプションがあり、通常は透過的データ暗号化(TDE)です。ただし、これは多くの場合、高価な上にバージョン固有であり、ベンダー独自のデータベースのみを暗号化し、それぞれが独自の管理システムを持ちます。

データ漏洩のシナリオ

データベース ログまたは機密情報を含む一時ファイルは、USBストレージにコピーされます。これらのファイルは、他の非構造化ファイルと共に保護されません。他の選択として、データベースはクラウドサービスに保持されますが、そのほとんどが安全に構成されていません。多くのメディアが、クラウドデータベースは適切に保護されていないと報告しています。

> 欧州最大手のホテル予約プラットフォームGekko Groupは、セキュリティ保護のないデータベースが原因で、顧客、クライアント、パート ナーに関する1TB超のデータを漏 洩し、被害者を口座盗取詐欺、な りすまし詐欺、金融詐欺の危険に さらした。

セキュリティ上の懸念

非構造化ファイル、一時ファイル、もしくはログファイルの盗難: :多くのデータベース アプリケーションは、データベースの外部にある非構造化ファイルを保管および管理していますが、TDEはこれらのファイルを暗号化しません。

また、機密情報を含む一時ファイルおよびログ ファイルが作成されますが、これらのファイルもまたTDEでは暗号化されません。

データベース ファイルの盗難: データベース自体を構成するファイルにアクセスでき、データベースが暗号化されていない場合、データは簡単に盗まれ、再構築される可能性があります。

ソリューション

SecureAgeのSecureDataを使用すると、どのベンダーであるかは問わず、データベースまたはアプリケーションに影響を与えることなく、すべてのデータベースを暗号化できます。データベース操作中でも、すべてのデータはディスク上で暗号化され続けるため、データベースファイルの盗難の脅威に対応できます。

SecureDataは、ファイルタイプに関係なく、すべてのファイルを自動的に暗号化します。すべての非構造化ファイル、レポート、ログ、一時ファイルは、データ盗難から保護されます。データベースからエクスポートされ、ローカルファイルに保存されたデータであっても、盗まれたデータが組織外では無意味なものになるように暗号化されます。

暗号化されたバックアップ

データバックアップ テクノロジーは、バックアップメディアを日常的に暗号化するか、少なくともパスワード保護を提供します。これにより、バックアップ メディアの盗難からデータを保護できます。

データ漏洩のシナリオ

管理者は、バックアップ内の機密ファイルにアクセスするために、「キー」を使用します。バックアップ メディアは暗号化されますが、管理者は暗号化キーを保持しているため、保護されていないファイルをバックアップからダウンロードできます。

セキュリティ上の懸念

管理者は、バックアップを読み込み可能: 管理者は、必要に応じてファイルを復元できるように、バックアップの暗号化を解除する方法を知っている必要があります。つまり、特権ユーザーがバックアップからファイルにアクセスし、ファイルを盗み出すのは簡単です。

米国のラジオ大手Entercomは、不正者が第三者のクラウドホスティングに保存されたRadio.comのユーザー認証情報を含むデータベースバックアップファイルにアクセスしたと報告。
Cathay Pacificは、バックアップファイルが保護されていない場所に保存されていたことが発見されたため、50万ポンドの罰金。

ソリューション

SecureAgeのSecureDataは、ファイルのライフサイクル全体を通じて暗号化を維持し、ソース内のすべてのファイルを暗号化します。これは、バックアップのファイルも暗号化されていることを意味します。

管理者がこのようなバックアップからファイルを盗んだ場合でも、権限のあるユーザーしか復号できないため、それが無意味なものであることに気付くことになります。

NISTカテゴリー4
情報保護プロセスと手順

クラウドサービスのセキュリティ

クラウドサービスのセキュリティは、クラウドベースのシステム、データ、インフラストラクチャを保護するために連携する一連のポリシー、管理、手順および技術で構成されます。クラウドサービスは第三者によって実行されるため、データの安全性確保は、その第三者に依存します。

データ漏洩のシナリオ

クラウドサービスに雇われている管理者は、特権を持つ立場を利用して、ストレージバケット内のファイルにアクセスし、盗むことができます。

セキュリティ上の懸念

クラウドサービスのクラウドサービスの特権ユーザー: クラウドセキュリティーは、第三者の特権ユーザーによる不正な外部アクセスと不正使用を防ぐ必要があります。ただし、利用者はこれらの特権ユーザーを直接制御したり、その情報を得ることは出来ません。

AWSに保存されていたCapital One顧客レコード1億件を、Amazonエンジニアが盗む。誤構成されたファイアウォールを利用し、700以上のデータフォルダにリモートアクセスした手口によ る。継続的な犯行は4か月もの間未発覚。

ソリューション

SecureAgeのSecureDataを使用して、組織のシステムからデータが出る前に暗号化が行われれば、情報は完全に保護されます。クラウド管理者はファイルを表示できますが、データを閲覧したりアクセスしたりすることはできません。また、サービス、データベース、インフラストラクチャの設定を誤ると、ファイルが盗まれる可能性がありますが、その中のデータは暗号化されたままであるため使用できません。

NISTカテゴリー5
メンテナンス

基本的なITセキュリティに関するアドバイスとして、システムの定期的なパッチ適用とメンテナンスが提唱されています。これはもちろん優れたアドバイスです。しかし、SecureAgeのSecureDataを使用してすべてのファイルを暗号化すれば、セキュリティパッチが未適応で最新の状態になっていないサーバーやデスクトップ機器であっても、使用可能なデータの盗難はできません。

NISTカテゴリー6
保護技術

フルディスク暗号化

BitLockerおよび同様のシステムは、ディスクの内容全体を暗号化します。

セキュリティ上の懸念

フルディスク暗号化を使用するシステムは、起動実行中であれば、すべてのユーザーとプロセス (正当か不正か問わず) が、暗号化解除されたデータの形式となり、任意のファイルにアクセスできるようになります。つまり、フルディスク暗号化は、電車の中で紛失したラップトップのデータを保護するためには最適ですが、実行中のシステムではセキュリティ上の利点はありません。

ソリューション

SecureAgeのSecureDataは、アクセスまたは編集中でも、ファイルを常に暗号化し続けます。システムの実行中にこのデータを復号できるのは、権限のある人のみです。その上、他の場所にコピーされたファイルは暗号化されたままです。

SSLとTLS

SSLとTLSは転送中のデータを暗号化し、保護します。ほとんどのウェブサイトは、この種のセキュリティを使用して、トラフィックを傍受しているユーザーが有用なデータにアクセスできないようにします。

セキュリティ上の懸念

情報はサーバーからクライアントに渡される際に暗号化されます。サーバーに保持されているデータ、およびクライアントシステムに保管されている情報は、SSL/TLSによって保護されません。

ソリューション

SecureAgeのSecureDataを使用すると、ファイルは常に暗号化されます。転送中だけでなく、使用中および休止時にも暗号化により保護されています。

> Nedbankの顧客170万件が対象 となったセキュリティ侵害は、サー ドパーティ サービスプロバイダー で生じた。データはサードパーティにSSL/TLSで暗号化送信され たが、保管時には非暗号化のまま だった。

アンチマルウェア

私たちはアンチマルウェアシステムに依存して「悪意あるもの」を識別して排除しますが、なぜ「成功した」マルウェアやランサムウェアの攻撃に関する多くのメディア報告があるのでしょうか。アンチマルウェアだけではすべてをブロックできないことに気付き、組織はサイバーセキュリティやクリックの危険性、悪意のあるものを開く危険性についてスタッフを教育するために時間と費用を費やしています。

データ漏洩のシナリオ

ハッカー(またはインサイダー)がネットワーク上にマルウェアを正常に展開し、バックドアを開きます。

マルウェアは、企業の防御を回避したり、被害者の特権を利用する方法がわかっています。いずれにせよ、データへのアクセスが達成され、ファイルの流出はそのまま進みます。

セキュリティ上の懸念

マルウェアは、先進の高度な技術: ランサムウェアは高度な持続的脅威(APT)に進化し、組織に損害を与え、将来に向けて金銭を強要し続ける「ディスラプションウェア」になりました。

> Norske Hydroのランサムウェア攻撃は、システムから締め出された後の回復に約6000万ポンドのコストを費やした。SecureAPlusをインストールしていれば、マルウェアの実行は許可されず、加害者はITサービスに損害を与えることができなかっただろう。

ゼロデイ攻撃と機械学習技術を使用するハッカーは、アンチマルウェア製品よりもかなり先に進んでいます。マルウェアを認識したり、進行中の悪意のある行動を特定しようとする従来のアプローチでは、常にに侵入される可能性があります。

ソリューション

SecureAgeのSecureDataは、すべてのデータファイルを常に暗号化しているため、データを盗もうとするマルウェアは暗号化された情報を流出させます。一度組織の外に出ると、このデータは役に立ちません。また、この時点で、SecureAgeのSecureAPlusがアプリケーション許可リストとアプリケーション制御を使用することで、すべての不正プロセスをブロックすることができます。実行を不可能にして、マルウェアの問題を回避します。

結論

サイバーセキュリティフレームワークの分野内で、一般的に使用されるITセキュリティ技術について議論しましたが、データを保護する技術を複数層使用しても、依然としてデータ盗難が成功していることがわかりました。加害者 (外部または内部) がこれらの保護を回避できる場合、盗まれたファイル内の情報は完全には保護されません。

SecureAgeは、データファイルがどこに保存されているかに関係なく、すべてのデータファイルを暗号化することで、既存のサイバーセキュリティレイヤーを補強し、盗まれたデータを無意味なものにします。盗まれたデータを組織外で無意味なものにすることで、規制、ブランドの損害、法的、事業回復などのデータ漏洩被害を軽減します。SecureAgeのアプローチは、機密情報を危険にさらすことはありません。

SecureAge Technology

SecureAge Technologyはシンガポールに本社を置く、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に、2003年にシンガポール政府のためにまず着手されました。SecureAgeは自社特許であるPKIベースの暗号化を、固有の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、すぐさま後続の政府機関や公共機関に推奨されるデータ暗号化パートナーになりました。こうした長期的な深い統合関係から、SecureAgeに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が備わっています。

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、および日本政府のさまざまな機関や、ブリティッシュ・アメリカン・タバコ、ソニー、成田エアポートテクノ、タイ政府貯蓄銀行、GRGバンキングなどが含まれます。

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

プロアクティブな保護

データセキュリティ

データセキュリティとは、遍在的な暗号を意味します。データは、最も基本的な自己完結単位であるファイル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では、一部のデータを一定期間だけ保護したり、セキュリティよりもコンプライアンスを重視したり、複雑化したりして逆にリスクをもたらします。また内部で働くユーザー（どのシステムでも最も脆弱な部分）に対しては、境界の防御を施すだけでは不十分です。

アプリケーション インテグリティ

アプリケーションの整合性とは、ホワイトリストそしてデータのアプリケーションへの結び付けによる制御を意味します。承認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と考えるからです。従来のマルウェア対策システムはパッシブ保護の代表的なものですが、それでは手遅れです。これらのシステムの焦点は、既知のマルウェアに置かれているため、常にアクティブで悪意のあるプロセスを阻止しようとするだけのものです。

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人的要素は、構成の一部にしたり変えようしたりとするのではなく、完全に排除する必要があります。なぜなら、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（セキュアでない）メソッドを編み出してしまうからです。ユーザーは、追加トレーニングや教育を必要とせず、思い通りに作業できる環境が必要です。

トレードオフなし

SecureAgeのこれらの原則の間には、トレードオフがありません。特にユーザビリティ面で、データセキュリティ強化のために妥協することはありません。「適切な」方法が難しいものであれば、人は何かを達成するために他の方法を見つけるもの、そう認識することが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の使用で貴社のデータセキュリティがどう改善されるかについて、また無料トライアルなどについてもお気軽にご連絡ください。

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