SecureAge

データ漏洩の温床となるデータベース

- セキュリティギャップを解消をする暗号化

SecureAge ホワイトペーパー2021年

データベースのセキュリティは最重要事項

企業においてデータの重要性が高まり、データに依存するようになるにつれてデータベースはデジタル資産を格納する規定の貯蔵庫として利用され、データの整理や検索、分析に大いに活用されています。新型コロナウイルスに伴うリモートワークやハイブリッドワークへの移行により、データベース、中でもクラウド技術を利用した分散型データベースの需要がさらに高まっています。しかしながら、このように情報が集中した状態となることにより、便利ではあるもののデータベースは攻撃の格好の標的となり、セキュリティ上の大きな懸念材料となります。

Forrester ResearchのVP兼主席アナリストで、ビッグデータおよびデータウェアハウスの専門家であるNoel Yuhanna氏は、新型コロナウイルスの世界的大流行の中、データベースやデータウェアハウスのデータセキュリティに関する問い合わせが著しく増加したと話しています。「コロナ禍において、多くの組織がデータセキュリティを最優先の課題としています。特に、非常に機密性の高い個人識別情報や個人の健康データ、コンプライアンスデータを扱っている組織に多くその傾向が見られます」と同氏は指摘しています。[1]

データベースセキュリティに関するよくある誤解

データベースは規模を問わずどのような企業でも業務を行う上で、まさに中心となるものです。また、データベースへの侵入が日常的に発生していることを考えると、どの企業も影響を受ける可能性があります。データベースセキュリティに関するよくある誤解を解くことで、データ流出による時間やコストを節約でき、また信用の低下を防ぐことができます。以下に、セキュリティに関する思い込みをいくつかご紹介します。

1. 会社が小規模であるため、誰もわざわざハッキングしようとはしないだろう

調査によると、中小企業は誤った安心感を抱いているようです。過半数（66%）は、自社のデータやデバイスは安全でハッカーからも守られていると確信しており、また77%は不正侵入や攻撃を受けたことはないと回答しました。しかし、それに反して、デジタルフォレンジックに関する研究によると、データ漏洩の発生件数のうち、72%は従業員数が100人未満の企業で発生していることが明らかになっています。

こういった規模のデータ漏洩がニュースで報じられることは滅多にないため、中小企業は攻撃を受け、データを失ったとしても気が付かないのが現状です。詳しくは、当社の中小企業向けホワイトペーパーをご覧ください。

2. ITスタッフはデータベースセキュリティを最優先している

最近は自動化やボタンを押すだけで導入できる形式が主流となっていて、ベンダーは標準的な工場出荷時の設定のままデータベースアプリケーションを提供しています。ITインフラ管理者やデータベース管理者が適切な設定方法やデータ保護の方法を習得するまでの間、迅速に使い始めるための一時的な措置として、データベースはデフォルト設定の状態で使用されています。ただし、大抵の場合、セキュリティは最優先事項ではありません。データベース管理者のうち、セキュリティに時間を費やしているのは推定7%のみで、その他の管理者はデータの整理やアクセス、パフォーマンスを優先しています。[2]

3. 大手事業会社運営のクラウドベースなら安全だろう

データベースアプリケーションのセキュリティ機能はより強固になってきていますが、すぐに使える商用のデータベースアプリケーションは、単純なパスワードが使用されており、エンドユーザー用と管理者用のアカウントでデフォルトのパスワードとして同じものを使用するなど、セキュリティ管理機能があまり有効になっていない状態で提供されています。クラウドベースのデータベースを導入することの魅力の一つは、大規模で資金力のあるクラウド事業者が提供するセキュリティを利用できると考えられるこ

1　コロナ禍をきっかけにDBaas環境でデータセキュリティを確保するように変化：https://searchdatamanagement.techtarget.com/feature/Pandemic- triggered-data-security-movement-to-DBaaS

2　中小企業のデータセキュリティに関するよくある4つの思い込み：https://www.whoa.com/4-common-misconceptions-about- small-business-data-security/

とです。ただし、サービスの規定には、セキュリティに関しては事業者と利用者である顧客の共同責任であると記載されています。[3]

クラウド事業者はクラウドのセキュリティ（ハードウェアやインフラ、ソフトウェアなど）の責任を負う一方、利用者はクラウド内のセキュリティ（自社のデータやプラットフォーム、アプリケーション、IDおよびアクセス管理、OSなど）の責任を負います。

4. データベースのセキュリティ管理は、専門の管理者が行うのが一番である

データベース管理者は、バックアップやリカバリー、パッチのやソフトウェアのアップデートなどの作業を常に検討する必要があります。時には他のシステムとの互換性を維持するために、一部のシステムにパッチを当てずに放置しなければならず、結果として脆弱性やデータ侵害の可能性が生じることになります。データベース管理者は新旧のITシステムが混在する中、管理すべきデータ量にどうにか対応する必要があるため、今日の全てが相互接続された環境でデータを保護するという複雑な作業よりも、システムを稼働し続けることに重点を置いています。適切なツールやトレーニング、人材、そして取り組むための動機が与えられない限り、データベース管理者はセキュリティを確保するのに最適な立場ではないと思われます。

ファイルレベルの暗号化でデータベースを保護

大抵の企業は、支払い情報や個人を特定できる情報などの顧客情報や、自社の業務·財務記録、知的財産などをデータベースに保存しています。データが流出した場合、どのような規模であっても企業の評判や規制上の立場、法的立場に悪影響を及ぼすことになります。ファイルレベルの暗号化により、最も基本的なレベルでデータを保護することは、正しく選択して適用すれば、セキュリティの確保と規制遵守の両方を実現する効果的なソリューションとなります。

ファイルレベルの暗号化を採用する企業の増加

Ponemon Instituteの『2021年の世界における暗号化の動向に関する調査』では、組織全体で暗号化戦略を採用する企業が着実に増加していることが確認されました。[4]最近では、ネットワーク境界のセキュリティを保護するだけでは企業を守りきれなくなっています。安全だと思われていた境界内にも、脆弱な社員や技術的な脆弱性が存在するためです。ほとんどのケースでは、ファイルレベルでデータ自体を暗号化することが最も良い対応策です。外部からの攻撃や内部からの情報漏洩などのデータ侵害が発生した場合でも、データを保護することができます。

ファイルレベルの暗号化を行うことで、内部および外部の脅威からデータを守る

最近の効果的なデータセキュリティ戦略は、内部リスクと外部攻撃の両方に対応しています。2020年から学んだことは、ITセキュリティにゼロトラストを前提としたアプローチを採用することが不可欠になりつつあるということです。2020年の前半だけで、2019年の年間件数を上回る件数の攻撃が発生しました。[5]最近発表された『2021年データ流出に関する報告』によると、社内の従業員によって機密ファイルが社外に流出する可能性は、コロナ禍前に比べて85%も上がっていることが判明しました。[6]

データそのものを保護することで、ゼロトラストを実現することができます。全データファイルにおいて、内容を表示する前にアクセス権があるかどうか確認が行われるため、ファイルが悪意のある人物の手に渡った場合でも、情報はすべて保護されます。SecureAge Security Suite for Databaseを使用してファイルレベルの暗号化を行うと、すべてのデータファイルを保護することができます。偶然または意図的にデータベースが侵害された場合でも、データファイル全体が暗号化されたままとなるため、関係者以外はデータを理解することができません。さらに、データベース管理者のような社内の特権ユーザーは、データベースの中身にアクセスせずに、システムのメンテナンスやバックアップを引き続き行うことができます。これはすべて各ファイルに追加されるPKI（公開鍵基盤）技術により実現されます。

3 責任共有モデルの説明：https://cloudsecuritvalliance.org/blog/2020/08/26/shared-responsibility-model-explained/

4 Ponemon Institute『2021年の世界における暗号化の動向に関する調査』

5 https://www.darkreading.com/attacks-breaches/more-cyberattacks-in-the-first-half-of-2020-than-in-all-of-2019/d/d-id/1338926

6 https://beta.darkreading.com/vulnerabilities-threats/insider-data-leaks-a-growing-enterprise-threat

ファイルレベルの暗号化で、クラウドサービス展開時の設定ミスを軽減

クラウドサービスは迅速に展開することができ、簡単に導入できるため、便利だと考えられています。しかしながら設定を間違えた場合、広範囲に影響を及ぼすセキュリティの脆弱性をもたらす可能性があります。ガートナー社によると、クラウドのセキュリティ障害のうち、99%は設定ミスが原因とされています。[7]ある研究者グループがテスト目的で、意味がないデータを数メガバイト分だけ格納したデータベースをきちんと構成されていない状態でインターネット上で公開しました。

誰がデータベースに接続し何を盗むかを調査したところ、データに価値がないにもかかわらず、データベースを公開してから8時間半程で攻撃を受け、1か月弱で合計610回の攻撃を受ける結果となりました。[8]

ファイルレベルでデータをリアルタイムに保護することで、データベースの保存場所に関係なく、すべてのデータを安全に保つことができます。

一般的なデータベース暗号化により生じるセキュリティギャップ

大抵の場合、データベースの暗号化は、透過的データ暗号化（TDE）、列レベルの暗号化、またはトークン化を用いて実装されています。これらの方法では、構造化データしか保護できず、非構造化データは無防備で脆弱なままとなります。また、データ列をそのままにしておくと、情報を識別するのに十分な情報を得られてしまうだけでなく、漏洩した場合に重大な損害が生じてしまいます。構造化データと非構造化データの両方を保護するためには、企業は追加のソリューションを導入する必要があり、そのためのコストを追加で投資する必要があります。

SecureAge Security Suite for Databaseが提供するファイルレベルの暗号化は、スケーラブルで拡張性のあるデータ保護アプローチであるため、企業はデータ保護の運用コストを最小限に抑えることができます。

構造化データと非構造化データの両方を暗号化することができ、種類の異なるデータベースやアプリケーション上のあらゆる種類のデータ（一時ファイルやログファイルを含む）を保護できる、単独のオールインワンソリューションとして機能します。

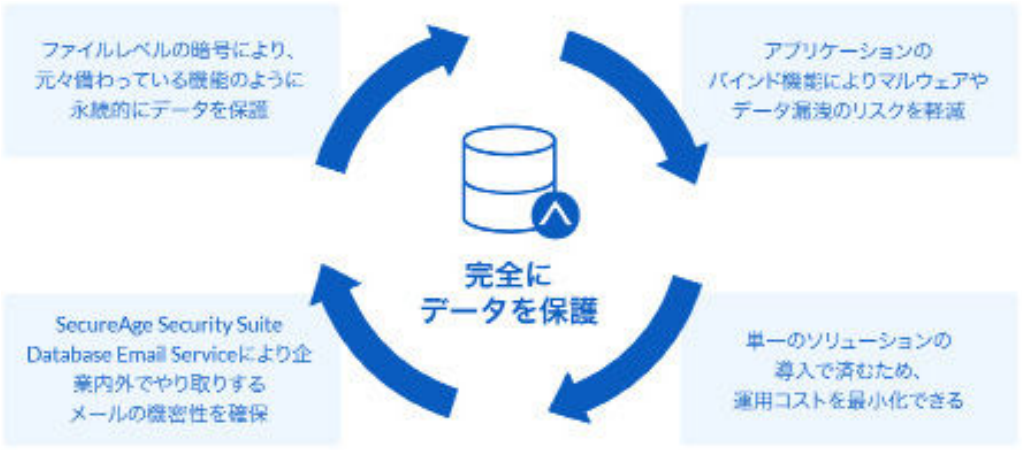
SecureAge Security Suite for Database - 完全なソリューション

数多くの暗号化ソリューションが販売されていますが、すべてのソリューションが同じように作られているわけではありません。SecureAge Security Suite for Databaseは、SecureDataテクノロジーを用いてデータを暗号化する、独自のアプローチを提供します。PKI（公開鍵基盤）を進化させたSecureDataでは、非対称暗号化を透過的に適用して、ユーザーごと、またファイルごとに固有の鍵を密接に結びつけることでデータを保護します。SecureDataテクノロジーにより、保存場所を問わず、すべてのファイルを常に積極的かつ持続的に保護することができます。使いやすさこそが重要な防御手段であるという考えに基づき、SecureDataはユーザーに作業方法の変更を強いることなく、元々備わっている機能のようにデータを保護できるように設計されています。SecureDataテクノロジーの詳細については、こちらのリンクをご覧ください。

SecureAge Security Suite for Databaseは、以下に示す機能を通して、組織が使用中、転送中、および保管中の状態にあるデータを保護できるように支援する完全なソリューションです。

7 責任共有モデルの説明：https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained/

8 正しく構成されていないデータベースの展開後、数時間で狙われる：https://www.darkreading.com/cloud/misconfigured- databases-targeted-hours-after-deployment/d/d-id/1338052



ファイルレベルの暗号化は、データに備わる永続的な保護

SecureAge Security Suite for Databaseは、どのデータが機密性が高いもので保護する必要があるかを判断するのではなく、すべてのファイルを機密性が高いものだと捉え、ユーザーのワークフローに影響を及ぼすことなく、全データを自動的に保護します。データベース全体を保護し、構造化データと非構造化データの両方を含む、データベース内に格納されているあらゆる形式のデータを保護します。データベースから出力したレポートや、ダウンロードしたデータも保護対象に含まれます。暗号化プロセスはデータベースやアプリケーションに対して透過的に行われます。そのため、認証されたユーザーは暗号化されたすべてのデータにアクセスし、クエリ結果をリアルタイムで確認でき、データへの変更が発生した場合でも問題なく反映されます。

アプリケーションバインド機能によりマルウェアやデータ漏洩のリスクを軽減

SecureAge Security Suite for Databaseのアプリケーションのバインド機能を使用すると、ユーザーはルールを指定して、特定のデータベースファイルを特定のアプリケーションにのみ紐づけることができます。これにより、アプリケーションが侵害された場合でも、そのアプリケーションがバインドされていなければ、データベースにアクセスすることはできません。事実上、企業のサーバーにマルウェアが侵入しても、正しい複合鍵と必要な権限がない限り、暗号化されランダムな状態になったデータの内容にアクセスすることはできません。同様に、システム管理者がメンテナンスやバックアップを行う際も、データベース内の機密情報にアクセスすることはできません。

単一のソリューションの導入で済むため、運用コストを最小化できる

前述のように、すべてのデータベース暗号化ソリューションが同じように作成されているわけではありません。最も一般的に使用されている透過的データ暗号化やカラムレベルの暗号化ソリューションでは、特定のトークン化された値や構造化データ内の列しか保護することができないため、プレーンなカラムや構造化されていないデータファイルは完全に脆弱なままになります。それに加え、データベースベンダーが独自に開発した暗号化ツールは、導入や維持のためのコストが追加で必要となります。当然ながら、データベースのセキュリティ上のギャップを埋めるために追加でソリューションを導入するとなると、それなりにコストがかかります。SecureAge Security Suite for Databaseは、ファイルを暗号化することにより、構造化の有無に関わらず、あらゆる種類のデータを保護します。単一のソリューションで必要な機能をすべて提供するため、企業は運用コストを最小限に抑えながら、様々なデータベースやアプリケーション間で日々変わっていくセキュリティ要件を満たすことができます。

SecureAge Security Suite Database Email Serviceはメールの機密性を確保

企業では、請求書や銀行口座明細、保険の契約書類など、日常的に取引上必要なメールを顧客との間でやり取りしています。必然的に電子メールや添付ファイルには、個人を識別できる情報が含まれるため、指定した受信者のみが閲覧できるように暗号化する必要があります。SecureAge Security Suite Database Email Serviceを使用すると、メールの内容と添付ファイルの両方を安全にエンドツーエンドで暗号化することができます。復号化の際には、受信者は一意なパスワードを入力する必要があります。パスワードは、ユーザーの信頼性を確認するための簡単なメール認証手続きを行った後に提供されます。

政府機関がSecurity Suite for Databaseを採用

> 東南アジアのある政府機関は、Elasticsearchデータベースに格納されている全データを保護できる単一のソリューションを探していました。内部脅威（IT管理者やデータベース管理者）によるデータ漏洩に加え、バックアップ時の漏洩も防御したいと考えていたため、SecureAge Security Suite for Databasesのファイルレベルの暗号化に興味をお持ちいただき採用に至りました。
> その結果、ユーザーやデータの格納場所に関わらず全てのデータを永続的かつ完全に保護することが可能になり、「もぐら叩き」のような複雑なメンテナンス作業は不要になりました。また、暗号化されていないプレーンなデータを複製する際には、データ作成者からの承認が必要となるプロセスをPKI技術によって確立し、データ漏洩が生じる可能性も最小限に抑えることができたのです。

セキュリティギャップを埋めましょう

システムおよびデータのセキュリティを確保するには、複数のレベルで保護する必要があります。しかし、各セキュリティレイヤー内またレイヤー間には、必ずギャップが存在すること、そのため完全に脅威を排除することは不可能であるということを理解する必要があります。

SecureDataテクノロジーを用いてファイルレベルの暗号化を行うことで、データそのものを保護することができます。SecureAge Security Suite for Databaseでは、このアプローチが拡張されており、データ漏洩やデータ盗難の防止を強力に支援するため、ご安心いただけます。従業員やアプリケーション、データベースの動作に影響を及ぼすことなく、大切なデータをデータ侵害から保護することができます。

データを安全に保護しましょう。

SecureDataの暗号化テクノロジーの詳細については、こちらをご覧ください。

Security Suite for Databaseソリューションの詳細については、こちらをご覧ください。

お問い合わせやデモのご希望、またパートナーシップのご相談については、contactus@secureage.co.jpまでご連絡ください。

よくあるご質問

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、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、組織はひとまず「データ暗号化」を行うことができるようになりました。問題は、フルディスク暗号化では電源がオフになっているマシンのみ保護され、暗号化が有効になっているディスクドライブにのみ、暗号化が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、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、変更することができます。

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。

Security Suite for Databaseは、データ保護ソリューションとしてどの程度包括的なものでしょうか？

Security Suite for Databaseは、単独で様々な種類のデータベースやアプリケーションにまたがる、あらゆる種類の構造化データと非構造化データの両方を保護できるオールインワンソリューションです。スケーラブルで完全にデータを保護することができるため、データ保護のために複数のソリューションのメンテナンス・管理を行う必要がなくなり、運用コストを最小限に抑えることができます。

Security Suite for Databaseは、規制の遵守にどのように役立ちますか？

全世界で施行されている個人情報保護規制により、企業は自社で保存しているデータのセキュリティレベルを求められるレベルまで引き上げる必要があります。

Security Suite for Databaseは、すべてのデータを暗号化して保護することにより、データ転送やサイバー攻撃などのリスクを軽減します。万が一、攻撃を受けてデータが流出したとしても、復号鍵なしでは暗号化されたデータは意味をなさないため、被害を受けた企業は規制に違反していないとみなされます。

組織が以下に挙げる規制を遵守し、データ侵害を回避できるよう支援します。

a. PCI DSS（Payment Card Industry Data Security Standard）
b. データ保護法（EU一般データ保護規則、カリフォルニア州消費者プライバシー法など）
c. 機密機関の情報の保護（アメリカ合衆国ホワイトハウスの行政管理予算局）
d. 医療保険の携行性と責任に関する法律（HIPAA）
e. グラム・リーチ・ブライリー法（GLBA）
f. 上場企業会計改革および投資家保護法（SOX法）
g. シンガポール金融管理局が定めるテクノロジーリスク管理ガイドライン（TRM）

データアクセスを可視化することはできますか？

データアクセスを継続して監視できるように、Security Suite for Databaseから完全なデータアクセス監査ログを出力することができます。監査ログには、データベースにアクセスしたアプリケーション、外部デバイスへの情報の移動、ブロックされた操作などの詳細な情報が含まれます。

Security Suite for Databaseでは、二要素認証オプションを利用できますか？

はい、Security Suite for Databaseでは、スマートカードやUSBトークン、HSMを使用した二要素認証をオプションの一つとしてご利用いただけます。そのため、ユーザーの公開鍵と秘密鍵をPKCS#11に準拠したスマートカード、USBトークン、またはHSMに保存することができます。これにより、より強固な二要素保護を実現できます。

Security Suite for Databaseソリューションにより、マルウェアのリスクを軽減できますか？

Security Suite for Databaseソリューションには、ソリューションには、拡張機能としてアプリケーションのバインド機能が含まれており、ユーザーはルールをして特定のデータベースを特定のアプリケーションにのみ紐づけることができます。これにより、バインドされていないアプリケーションからのデータベースへのアクセスを防ぐことができます。

一部の領域でより高レベルのセキュリティを実装することはできますか？

SecureAgeによって暗号化された情報はすべて、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、様々なセキュリティ要件を満たせるように、認証のセキュリティレベルを選択することができます。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、復号キーを保護するために多要素認証付きのスマートカードを使用するようにし、それ以外のスタッフはキーの保管にソフトウェアトークンとパスワード認証を使用するなどです。

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、または部署単位で製品をインストールして、データのセキュリティを強化することができます。

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すると同時にますます巧妙になり、さらに内部関係者によるデータ盗難の脅威がある現在、現状に疑問を投げかける必要があります。データを100%暗号化することは、すでに必要だと考えられている原則であり、フルディスク暗号化はこれを実現するものです。ただし、サイロ化した稼働中のシステム上のファイルを別の場所にコピーした場合でも、暗号化された状態が維持されるよう注意して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。

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、PKIセキュリティ技術を改良したものがベースで、シンガポール政府向けに2003年に最初のバージョンがリリースされました。SecureAgeは、特許取得済みのPKIベースの暗号化を、まるで元々備わっているかのような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も選ばれるようになりました。こうした顧客との長期的かつ深く密接な関係を通して、SecureAgeは大規模かつ複雑な組織のデータ保護に関する幅広い経験を得ることができました。

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が求められ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、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

予防的なデータ保護

データセキュリティ

データセキュリティとは、広範な暗号化を意味します。データの保護は、最も基本的であり、自己完結型の単位であるファイル上で実施する必要があります。他社から提供されているソリューションでは、一部のデータのみを一定期間のみ保護したり、セキュリティよりもコンプライアンスに重点が置かれていたり、また導入することで複雑性が増し、逆にリスクが生じたりしています。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）に対しては、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できる状態にすべきです。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。システムの焦点は既知のマルウェアに置かれ、既にアクティブな状態である、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、人的要素を構成要素として含めたり、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、他の点について考慮することなく、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場合、人は何かを達成するために他の方法を見つけるものであることを認識し、それを基本原則としてSecureAgeの製品設計を行っています。

詳細はこちら

その他のホワイトペーパーは、こちらからご覧いただけます。SecureAgeのエンタープライズ向け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