SecureAge

様々な脅威にさらされるデータ

- ATMセキュリティに対するSecureAgeの取り組み

SecureAge 事例紹介2021年

はじめに

銀行や金融業界のIT担当者は、「モグラ叩き」ゲームのような作業に多くの時間を費やす傾向があります。ゲームセンターで遊んでいるのならまだしも、銀行·金融業界における複雑なインフラやシステムで日々不規則に発生する問題を解決しながら、さらにモグラ叩きのような作業に取り組んでいます。

最も一般的な（しかし忘れられがちな）例として挙げられるのは、ATM機のセキュリティです。もう誰も使っていないのではと思われるかもしれませんが、実際はまだ使われており、米国のATMでは毎年100億件以上の取引が実行されています。[1]恐ろしいことに、これらの取引の一つ一つが侵入口となり、データ侵害が起きる可能性があります（Ponemon Instituteは2020年に、データ侵害が起きた場合、1件あたり386万ドルの費用が掛かると推定しています）。そのため、ニュースではデジタル通貨やフィンテックばかりが取り上げられているように見えますが、銀行・金融業界では、ATM機のセキュリティのような、ニュースでは取り上げられないセキュリティリスクにも注意を払う必要があります。

タイの大手銀行はATMのセキュリティの重要性を認識

タイのある大手銀行では、コスト削減への取り組みを強化していたものの、ATMネットワークで損失が続いたことにより、減収を報告しました。この銀行は全国で5,000台のATMを展開しており、ベンダーから徐々にサポートを受けにくくなっていたことから、ATM維持費がコストの大半を占めている状態でした。このように物理的なシステムに依存していたことで、社内および社外において重大なセキュリティ上の脆弱性が生じたのです。

内部者によるセキュリティ侵害

多くの銀行と同様、この銀行のATMネットワークでは、十分なファイル暗号化ソリューションは採用されておらず、技術者による内部脅威が発生した場合、すべてのファイルがリスクにさらされる状態でした。そして、物理的に分散したシステムに依存する企業でよくある問題ですが、既存のインフラにファイルレベルの暗号化ソリューションをマッピングすることは容易ではないという誤った認識を持っていました。

その結果として、データへのアクセスを条件に買収された保守担当者から、定期的に内部攻撃を受けたのです。ATMの維持管理には、手作業による処理が必要であり、また複数のタッチポイントが存在するため、非常に攻撃しやすい環境でした。社員や第三者は、不正アクセスを簡単に隠蔽することが可能で、外付けメディアのハードディスクを接続しても、発覚するリスクはほとんどありませんでした。それゆえ、事件が起きてから犯罪が発覚するまでに、長い時間が経過してしまったのです。

包括的なファイルレベル暗号化が採用されていなかったため、顧客データや銀行情報にアクセスするサーバー犯罪者を阻止するものは何もありませんでした。ファイルレベルでデータを保護するセキュリティソフトウェアが導入されていない状態は、サイバー犯罪者にデータ不正アクセスや、第三者へのデータ販売などを簡単に許しているようなものです。銀行や顧客が気づくとしても、すべてが終わったあとでしょう。

外部からのセキュリティ上の脅威

銀行は、「モグラ叩き」のような複雑な保守作業に加え、マルウェアを介したなりすましカードによる感染など、巧妙な外部からのさらなる脅威に持続的にさらされていました。これは、悪意のある攻撃を防げるよう、レガシーハードウェアが適切にアプリケーション制御されていなかったことが原因です。

ATMが表面上はトランザクションを実行するインターフェースとして機能する単純な機械に見えるため、このセキュリティリスクは見落とされていました。しかしながら、銀行はすぐにATM機が自行の幅広いネットワークへのポータルとしても機能していること、また偽装カードを用いられた場合、ATMと中央サーバとの接続は簡単に切断され、アラートやログが出力されることなく、同一ネットワーク上の他のマシンが簡単に乗っ取られる可能性があることに気が付きました。アプリケーション制御されていない状態では、銀行への攻撃を検知できず、脅威をブロックすることもできず、ATMの中身をすべて奪われてしまう可能性があったのです。

このように、銀行が導入していたセキュリティソリューションは、データの保護には効果的でない上に、銀行の中央ネットワークを危険にさらす事態となっていました。そして、当時は新しいシステムへの移行

1 http://www.nationalcash.com/statistics/

を進めており、それに伴い、リモートでも作業を行えるよう、セキュリティインフラの変更を考えていたのです。当時のCEOは、この状況を「家に新しいパイプや部屋を増築する」と表現していました。変更後まもなく、長く利用してきた技術には隠れた欠陥があり、加えて、古い技術が必ずしも新しい技術と上手く連携して機能するとは限らないことに気が付きました。新しく導入した技術と旧技術の連携が必須となるにつれて、セキュリティ上のギャップはさらに表面化し、連携部分や土台となる部分の保護を強化する必要性があることが明らかになりました。

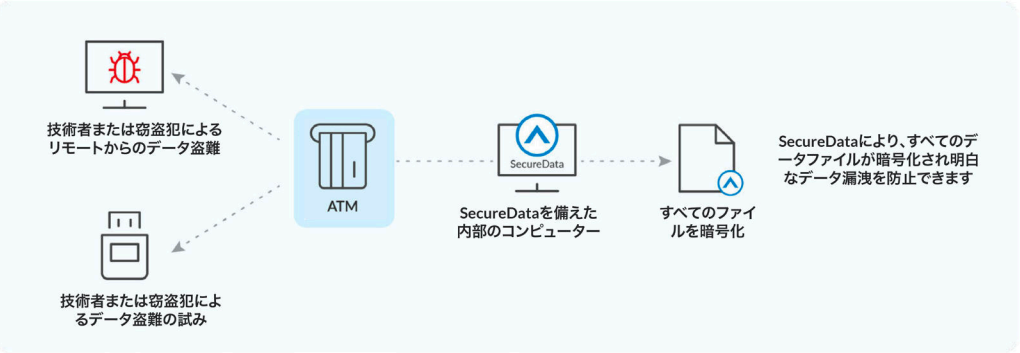
シンプルで実績のあるSecureAgeのアプローチ

タイの銀行のATMネットワークは、課題が山積みな状態でした。理由は単純で、物理システムが別の時代に構築されたものであったからです。顧客の行動が変化しただけでなく、システムがさらされる脅威の状況も進化しました。

銀行は、データそのものを保護するという当社の取り組みに興味を示され、また現状ではいかなる規模の侵入行為があった場合でも防御できないという事実を把握されていたため、当社にATMネットワークを保護するための新しい方法について、弊社にお問い合わせされました。そして、銀行にとって最も貴重な資産であるデータに焦点を当てたセキュリティソリューションを導入すれば、使用するハードウェアやシステムの種類や新旧にかかわらず、どこにあるデータでも保護できることに気付かれました。銀行が直面している脅威に対抗するために、当社からは二種類のセキュリティソリューションを提案しました。どちらも既存のインフラストラクチャに追加でき、ワークフローの変更が必要となるものではありませんでした。

オプション1：データを完全に保護

SecureAge Security Suiteにより、すべてのデータを暗号化し、盗まれたファイルを使えないようにすることで、内部脅威の影響を最小限に抑えることが可能です。

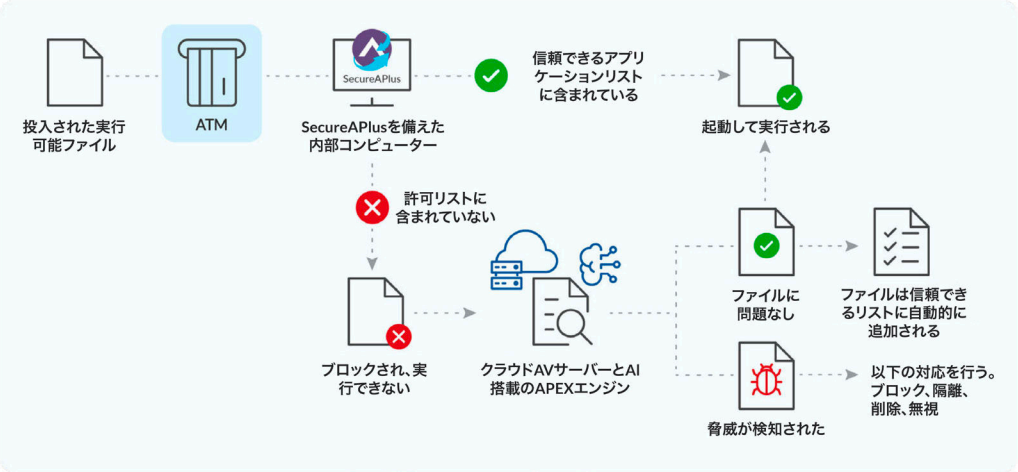


PKIをベースにした独自のファイルレベルの暗号化アプローチにより、すべてのデータは「転送中」、「使用中」、「保管中」の3つの状態すべてにおいて100%保護されます。SecureAge Security Suiteは、信頼性の高い防御を提供するだけでなく、偽装カードを用いた攻撃など、許可されていないプロセスの実行をすべてブロックするといった攻撃力も備えています。現在のセキュリティに対するデータの視点では、「機密性の高いデータ」というものは存在せず、境界防御やデータの検出·分類は効果がないと考えられています。SecureAge Security Suiteは、あらゆる環境に導入でき、完全で汎用性の高いデータセキュリティを提供します。

オプション2：マルウェアを完全に検出

銀行に提案したもう片方のアプローチは、AI搭載エンジンに加え、中央管理サーバーからニーズに応じて設定された「許可リスト」を取得して、直感的なアプリケーションコントロール機能を提供するSecureAPlusでした。SecureAPlusは、ATMネットワークのような物理的に分散した複雑なシステムでも同様に効果を発揮できる、柔軟なオプションです。アンチウイルスは、既知の脅威に対する「拒否リスト」であり、現在市販されている最高のAIは既知および未知の脅威のうち、約99%を検出することができます。それに対して、SecureAPlusではどのような環境でもマルウェアから100%保護することができます。

SecureAPlusは、99%の検出率を誇るAI搭載エンジンで認識されなかった脅威について、すべてデフォルトで拒否してから、推奨される対応とともに、管理者に通知を送ります。未知の脅威に直面した場合、競合他社のアプローチでは、削除や検疫などの包括的なルールが適用されますが、それだと意図しない重大な結果を招く可能性があります。SecureAPlusでは、まずはブロックして、必要であると判断した場合にどのように対応するか確認するという流れをとっています。



貴社のセキュリティギャップはどこにありますか？

物理的に分散したシステムは、アクセスを取り巻く一部のセキュリティ機能（多要素認証、シングルサインオン、役割ベースのアクセスなど）と相容れない場合があります。しかしながら、デジタル化を進めるには、従来のシステムを廃棄して一から作り直す必要があるというのは間違った考えです。SecureAge Security SuiteおよびSecureAPlusは、どちらも他のアプリケーションに影響を与えることなく、また新しいインフラを必要とすることなく、お客様の環境のセキュリティギャップを埋めることができます。当社が提供するセキュリティソリューションは、様々な脅威からデータを保護し、あらゆる場所のセキュリティギャップを解消できるよう設計されています。どのようにお手伝いできるか、是非ご相談ください。

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。

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下で負う義務にどのように影響しますか？

組織が個人データの漏洩による被害を受けた場合でも、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[2]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？

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、およびその他の現行システムや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。

今こそ情報セキュリティに予防的アプローチを取り、データを管理すべき時代です。詳細については、お問い合わせください。

2　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ており、それらの措置が個人データ侵害によって影響を受ける個人データに適用されていた場合。特に暗号化のように、個人データへのアクセスを認められていない者には理解ができないようにする措置。」

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。contactus@secureage.co.jp

ウェブサイト www.secureage.com
お問い合わせ contactus@secureage.co.jp

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