SecureAge

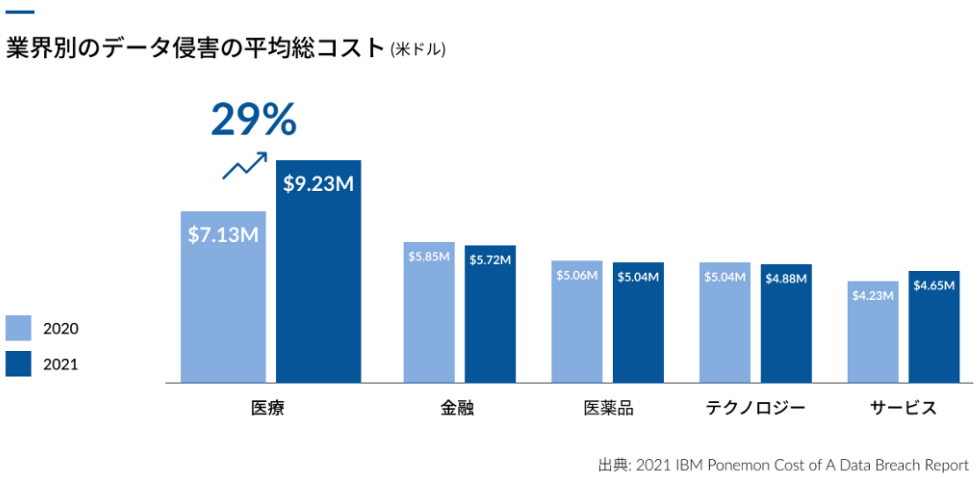
医療業界：
データ漏洩が大流行？

SecureAgeホワイトペーパー2021

情報漏えいのトップは医療業界

医療業界は11年連続して、どの業界よりも情報漏えいに高いコストを費やしています。2021年だけでも平均923万米ドルの情報漏えいが発生しており、その件数は年々増加して、状況は悪化しています。

2020年から2021年にかけて、米国の医療情報漏えいの平均総費用は、29%も急増しました。[1]



出典: 2021 IBM Ponemon Cost of A Data Breach Report

HIPAA(Health Insurance Portability and Accountability Act)は、1996年に米国連邦政府によって制定された、医療記録の適切な保存を保証するための法律です。このような規制が整えば、医療業界の情報漏えいは減少すると思われますが、実際は逆のことが起きています。医療機関　は、HIPAAの遵守に苦労しており、HIPAA監査や調査に対応できていないことが、医療保険スポンサー団体の調査によって確認されています。[2] 3割の医療機関は、最後にいつHIPAAリスクまたは脅威の評価が行われたを知らない上に、その10%は、分析が5年以上前のものであると述べています。HIPAAを常に遵守することは、ベテランの人材から予算まで多くのリソースを必要とする ことから、すでにリソース不足の医療業界にとっては大変難しい課題となっています。

しかし、もしすべてのコンプライアンス項目が守られたとしても、データは本当に安全と言えるでしょうか?

医療セキュリティにおける3つの問題

医療業界おけるデータセキュリティの重要性は非常に高いと言えますが、業界の役割の性質上、情報漏えいを防止し、被害をおさえることはますます困難になっています。医療システムで生成および保存されるデータは、多くの利益を生む搾取の機会を提供します。その理由は、システムに組み込まれた新しいテクノロジーへの依存度が高いことに加え、この業界のさまざまな部署をまたぐデータの流れが、サイバー犯罪の機会を無数に広げているからです。

ここでは、医療におけるデータセキュリティを困難にしている3つの問題を紹介します。

1.データの性質

闇市場では、個人を特定できる情報(PII)よりも、個人の医療情報(PHI)のほうが価値があることがわかっています。非医療関連の機関におけるデータ漏えいにかかる平均コスト(政府からの罰金、事業継続および事故対応計画の策定、従業員のトレーニングおよびCISOの雇用)が、盗まれた記録1件あたり158米ドルに対し、医療情報となると363米ドルに増加します。[3] PHIはサイバー犯罪者にとってより価値があるのです。

1 2021 IBM Ponemon Cost of a Data Breach
2 Health Plans Struggle with HIPAA Compliance, Unprepared for Audit: https://healthitsecurity.com/news/health-plans-struggle-with-hipaa-compliance-unprepared-for-audit
3 https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/

なぜなら、罪のない犠牲者が、プライベートな知られたくない医療情報と引き換えに、金銭を払うよう強要されて、それに応じる可能性があるためです。

詐欺は、もう一つの一般的なPHIの悪用の例です。サイバー犯罪者は、被害者の病状や医師の診断書を利用して処方薬を購入し、それを転売して利益を得ることができます。あるいは、病状や被害者の示談金を利用して、偽の保険金請求書を作成する詐欺もあります。データロンダリングも、サイバー犯罪者がPHIを盗まれた機関に売り戻すことで利益を得る、一般的な方法の一つです。

理解すべきもう一つの重要なことは、盗まれてすぐに無効にできる金融機関の口座やパスワードとは異なり、医療データは永久に存続するということです。クレジットカードは盗まれてもすぐにカード番号を変えることができますが、病気、疾病、および医療処置に関する医療データは変更が効かず、その人の生涯にわたって保持されます。PHI情報には、個人の医療履歴について数多くの機密情報が含まれているため、サイバー犯罪者が医療データベースを標的にするインセンティブが高くなります。

2.業界はレガシーシステムを使用

多くの医療機関は、新しいアプローチが困難なエコシステムの中で機能しています。これらの機関で、すべてが順調に回っているように見える時は問題はありません。問題となるのは、オペレーティングシステムのサポートが終了したレガシーシステムが、ネットワークセキュリティにリスクをもたらしていることです。こうした機関では、厳しい予算と限られたITサポートで運営されている傾向があり、既に時代遅れであってもまだ動くといったレガシーシステムのアップグレードを求めることは困難と思われます。米国の医療システムで使用されている83%のデバイスは、時代遅れの安全でないオペレーティングシステムで実行されています。[4] 設計時よりもオープンな環境で稼働しているレガシーシステムは、サイバー攻撃に対して非常に脆弱な状態にあります。実際、医療機関では、毎日使用しているデバイスがどのシステムで動　いているのか、十分な注意を払っていません。その事例として、2017年、パッチを適用していないシステムが原因で、世界中がWannaCry攻撃の被害を受けました。[5] 同様に、2020年には、「広く使われている商用アドオンソフトウェア」の脆弱性により、ドイツの病院が機能不全に陥りました。[6]

更新もサイバーセキュリティのもう一つの重要な部分です。レガシーシステムは新しいセキュリティー対策を組み込むためのアップデートができない場合が多く、新しいオペレーティングシステムを採用している機関は、これらの脆弱性を常に修正し、パッチを適用しているため、優位に立つことができま す。しかし、インターネットに常時接続された技術に更に依存し、機器もハイテク化しているこの業界においては、小さな脆弱性がシステム全体に影響を及ぼします。しかし、医療機関が迅速にITシステムにパッチを適用し、頻繁なアップグレードや更新のために資金を確保すれば、ハッカーに対応することができるのか？というのは別の問題です。

3. 分散された非構造化データへの依存

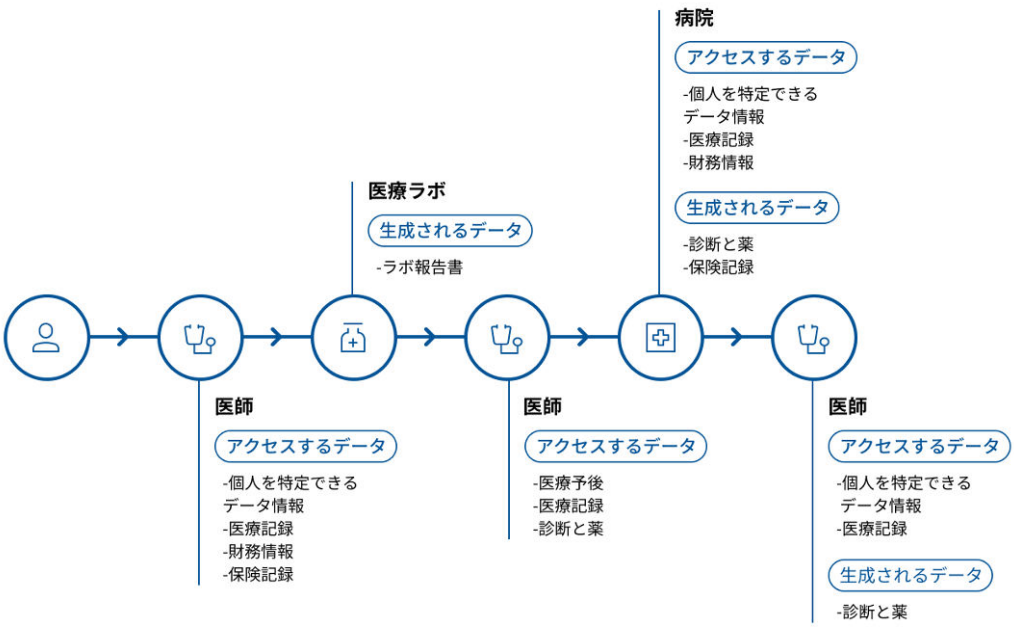
最近の医療サービスは、診療や薬の処方にとどまりません。そのため、初診から治療終了まで、時には数年にわたり、膨大な量の情報にアクセスし、データを作成する必要があります。この情報には、医療記録、予後、処方箋などがあり、これらには名前、住所、ID番号、財務情報、保険の詳細などの個人を特定できる情報も含まれています。

4 https://sea.pcmag.com/mobile-operating-system/36589/while-us-fights-covid-19-83-percent-of-healthcare-systems-run-outdated-software

5 WannaCry Ransomware Targeted Outdated HIT Infrastructure: https://hitinfrastructure.com/news/wannacry-ransomware-targeted-outdated-hit-infrastructure

6 German hospital hacked, patient taken to another city dies: https://www.nbcnews.com/tech/security/german-hospital-hacked-patient-taken-another-city-dies-rcna125

医療施設における1人の患者の取引について、どれだけのデータが生成、保存、アクセスているのかを下記に示します。



上記のデータフローは、すべてのプロセスが自動化され、すべてのシステムがスムーズに稼働していることを前提としていますが、実際には一時的な(つまり安全でない)パッチや、正式なワークフローで計算されないデータなどが発生することもよくあります。

データベースに保存されたデータは、診療所、研究所、病院、金融機関などの間を常に移動しており、サイバー犯罪者によるデータ盗難の機会が数多く存在するのが現実です。

医療データのセキュリティは、更に厳しい状況へ

新型コロナウイルスの状況が進むにつれ、いずれは全ての人の医療状態を追跡する対策が多く講じられるでしょう。ワクチンパスポートと遠隔医療は、情報漏えいが増加し続ける中で、規制とコンプライアンスのハードルが上がる可能性があるという事実とともに、対応が迫られている課題の2つです。

ワクチンパスポート

多くの国が予防接種プログラムを開発していますが、世界はすでにワクチンパスポートの使用によって再び門戸を開くことを検討しています。残念ながら、偽の予防接種証明書が、既にダークウェブ上で150米ドルほどで販売されており、この市場がいかに儲かるかを示しています。[7] 記録的なスピードで稼働する必要があるこの新しいシステムには、まだ多くの課題が残っており、ワクチンパスポートを完全に信頼するまでに、解決しなければならないデータセキュリティの問題が数多く存在します。

ワクチンパスポートに関するいくつかの疑問は次のとおりです。

- 個人の予防接種の状況が保存され、世界の医療機関、政府、および第三者がアクセスできるようになる中、どのように個人のプライバシーを守るのか?
- 異なるシステムに分散する医療記録に誰がアクセスできるのか?
- 予防接種証明書の漏えいをどのように防ぐのか?
- 身元の虚偽、偽造ワクチンパスポートの流通をどのように防ぐことができるのか?

7 https://www.dataguidance.com/opinion/international-vaccine-passports-and-privacy-concerns

- ワクチンパスポートを使用により、一般データ保護規則（GDPR）またはHIPAAへの準拠が 複雑にならないか？

以上のことから、個人的リスク、ビジネス上リスク、どちらも高いことがわかります。

急増する遠隔医療

対面接触を最低限に抑える必要性により、新型コロナウイルスのロックダウン中には、遠隔医療の機会が増えました。米国疾病予防管理センター（CDC）の報告によると、2020年の第1四半期の遠隔医療受診者は前年同期比で50%増加しました。興味深いことに、受診患者はこのまま遠隔医療を好み、そのうち73%がパンデミック後もこのようなサービスを利用し続けたいと言っています。[8]

遠隔医療へのアクセスを迅速に拡大することが重要である一方、その過程でセキュリティやプライバシーの問題は見過ごされる傾向があります。商用のビデオ会議プラットフォームはHIPAA規制に準拠していないだけでなく、医療従事者は自宅から自分のデバイスを使用して仕事をしています。つまり、PHIは医師個人のデバイスに保存されることが多く、盗難に遭いやすいのです。

研究によると、2020年の遠隔医療企業上位20社に関する言及を含むダークウェブ、およびディープウェブの検索結果の数は、大幅に増加しています。[9] 結局のところ、医療記録はダークウェブにおいて非常に有益な資産であり、記録1件につき250米ドルから1,000米ドルで販売されています。[10] 遠隔医療にはメリットがあることは否定できませんが、患者がシステム、ひいては医療従事者を信頼できるよう、セキュリティリスクを考える必要があります。最近の調査はこれを裏付けており、回答者のほぼ半分が、個人の医療データが漏えいした場合、遠隔医療を使用したくないとしています。[11]

ご覧のとおり、遠隔医療のメリットには、患者のプライバシーとデータセキュリティに関する大きな懸念が伴います。

規制の強化、コンプライアンスのハードル引き上げ

HIPAA規制の導入に伴い、関連するセキュリティ基準が設けられました。医療機関（医療計画、医療提供者、医療保険のクリアリングハウス）は、PHIおよび電子保護医療情報（ePHI）のデータ漏えいがあった場合、すべて報告することが義務付けられています。

ただし、懸念されるのは、この義務化以降、報告される医療データ漏えいが驚くべき速度で増加していることです。HIPAAジャーナルによると、6年前と比較して、現在では2倍以上のデータ漏えいが報告されているとのことです。これは、2010年に発生したデータ漏えいの3倍にも相当します。[12] 2020年だけでも、2,900万件を超える医療記録が漏えいしました。また、500件以上の記録の侵害が642件報告されており、このような記録の漏えいが毎日1.76件報告されたことになります。

1996年の制定以来、HIPAAは2003年、2009年、2013年の3回しか強化されていません。テクノロジーや遠隔医療への依存度が高まるにつれ、プライバシーを保護するために、遅かれ早かれ規制がさらに強化されることになります。

現状では、多くの医療機関がHIPAAに準拠を急いでいます。しかし、医療機関は、相変わらずリスク分析の実行と、サイロ単位のセキュリティ実装を続けているため、これは必要事項のチェックボックスをチェックするのみの準拠となる傾向があります。このチェックボックスコンプライアンスの問題は、脆弱性評価を解読せず、実際の問題がどこにあるかを見つけられないことです。

先の「チェックボックスはすべてチェックしたけれど、自分のデータは本当に安全なのか？」という問いには、まだ答えられないでいます。ネタバレになりますが、データが盗まれても持続するセキュリティこそが、真のセキュリテイの証です。

8 https://www.healthcareitnews.com/news/sound-security-practices-key-fulfilling-telehealths-promise-study-shows
9 https://www.healthcareitnews.com/news/telehealth-biggest-threat-healthcare-cybersecurity-says-report
10 https://www.forbes.com/sites/louiscolumbus/2019/10/20/5-strategies-healthcare-providers-are-using-to-secure-networks/?sh=4f92688b4b40
11 https://healthtechmagazine.net/article/2021/02/how-keep-telehealth-secure
12 HIPAA Journal https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/

これまでのサイバーセキュリテイアプローチ

社会的な動物として、私たちは、長い間使っていた、身の回りにあって親しみのある方法に依存する傾向にあります。IT標準操作マニュアルの内容として、サイバーセキュリティ意識向上のトレーニング実施やサイバー保険加入、大手ベンダーの最新のソリューションを定期的に導入している企業も多くあります。しかし、そのようなアプローチがデータ保護に成功しているかどうか、自問自答する必要があります。

「サイバーセキュリティの意識を高めましょう」

サイバーセキュリティにおいて最も脆弱なのは、間違いなく人的要因です。あまりにも長い間、企業は従業員に対しサイバーセキュリティートレーニングを義務付けて、セキュリティはIT部門だけの責任ではないことを皆に教えてきました。しかし、従業員の意識向上とトレーニングは、これ以上効果を上げることはありません。Journal of the American Medical Associationの調査によると、フィッシング詐欺にかかる病院職員は驚くほど多いことがわかっています。このシミュレーションでは、300万通のフィッシングメッセージのうち、なんと422,062件、つまり14%が病院職員によってクリックされたとのことです。[13]

2020年のセキュリティ会議で発表された別の調査によれば、再教育は6か月ごとの頻度で行う必要があります。[14] 企業の文化にセキュリティのDNAを浸透させるには、大変な労力が必要で、結局のところデータ漏えい防止のための従業員教育は効果的とは言えず、毎日漏えいが発生している状態です。教育トレーニングでできることは限られており、実際のところ、医療従事者が人の命を救おうとする時間を使ってまで、サイバーセキュリティに時間を費やして欲しくはありません。

「サイバー保険で安心を手に入れましょう」

サイバー攻撃による被害軽減を期待し、企業がサイバー保険に加入するケースが増えています。2016年から2020年の間に、サイバー保険の顧客は60%増加しました。[15] しかし、保険会社は保険料を引き上げる一方で、医療を含む一部の業種への補償範囲を縮小しています。この応急処置的ソリューションは、誤った希望を与えています。実際に、多くの保険会社はサイバー攻撃への補償を停止し、かわりにサイバーリスクをカバーする保険へとポリシーを調整しています。これらの用語は定義が曖昧であるため、サイバー保険でカバーされる内容が不明確なことが多く、その結果、企業が思っているような補償を受けられない可能性が高いと思われます。また、保険請求が支払われる前に、データセキュリティーのベストプラクティスに従った証拠を示す必要があることは、多くの人に知られていません。たとえ保険会社がサイバー攻撃による罰金を支払い、規制上の罰金をカバーしたとしても、時間も企業としての評判も失います。

「大手ベンダーや専門家推奨の最新のソリューションを導入しましょう」

テクノロジーに関わるものは何でもそうですが、アナリストや大企業が推奨する新しいトレンドやツールが常に存在します。攻撃後のクリーンアップという従来の方法ではなく、現在ゼロトラストなどの幅広いフレームワークから、特定の脅威に対する絞り込んだソリューションまで、さまざまなアプローチで、攻撃に先手を打ちたいと、多くの人は望んでいます。人工知能（AI）と機械学習は、常に快適さを追求するための手段であり、新たなクラウドソリューションであり、私たちを「やり直そう」「正しくやろう」という 気持ちにしてくれます。しかし、残念ながら、私たちがニュースで目にするような情報漏えいを防いだものは ありません。ゼロトラストのようなフレームワークは十分でなく、すべての脅威を特定して、事前に備えることはできないのです。善悪両方の人物がAIにアクセスし、クラウドソリューションはベンダーが責任を放棄する（そしてデータを自分たちの目的のために使う）など、実際は、解決するよりも多くの問題を引き起こしています。

13 Journal of the American Medical Association, Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions, 2019: https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2727270
14 https://securityboulevard.com/2020/10/security-awareness-training-how-often-should-your-employees-get-retrained/
15 Healthcare Organisations Facing Higher Insurance Costs for Less Coverage: https://www.hipaajournal.com/healthcare-organizations-facing-higher-cyber-insurance-costs-for-less-coverage/

では、どのようにサイバー攻撃の問題を解決すればよいのでしょうか?

ここで基本に立ち戻り、私たちが本当に守りたいのものは一体何なのか、自問自答してみましょう。時間、人的資源、資金を割いて、従業員プログラムを導入したり、保険に加入したり、単に最新のテクノロジーの波に乗るのではなく、私たちが実際に守りたいものに焦点を当てるべきです。それは、データそのものです。とてもシンプルなことです。

今こそ新しいアプローチを!18年間データ漏えい「0」

SecureAgeは、データを機密性によりレベル分類したり、データを保護 のために「ゲート(門)」を追加するのではなく、すべてのデータを機密データとして扱うというア プローチをとっています。これにより、データ管理は非常にシンプルで簡単になります。2020年のPonemon社のレポートでは、回答者の約67%が、機密データが企業組織内のどこにあるかを発見することは難しいと回答しています。

暗号化は古代文明以来存在し、数多くの研究と文献が、その有効性と、データ漏えいの影響を事前に抑制する力を裏付けています。暗号化は、攻撃されてもファイルを解読不可能な文字列で覆い隠し、使い物にならなくします。暗号化は、データを保護するための安価で効果的な手段ですが、ITセキュリティ計画における暗号化の導入は、現在行われている保護に関する誤解や、より良いものを導入するためのコスト(金銭的およびシステムパフォーマンスの両方)により、残念ながらそれほど普及していません。2021年のHIPAAコンプライアンスチェックリストによると、ほとんどのePHIの漏えいは、暗号化されていないデータを含むデバイスの紛失または盗難、ネットワークを介したセキュリティで保護されていない記録の送信に起因しています。[16]

ファイルレベルの保護:重要なデータを根本から保護

結論として、セキュリティは可能な限りソースに近いところで適用されて初めて効果を発揮するものなのです。例えば、宝石をテーブル上に置いたまま玄関だけ施錠しておくよりも、できることならば、宝石自体にロックをかけてしまいたいと思いませんか?この例えを借りるなら、ファイルレベルの保護は、データを保護することで機能します。つまり、設計とデフォルト機能によって、データ自体に潜在的な内在する保護(暗号化)を持たせてしまえば良いのです。

SecureAgeのSecurity SuiteはSecureDataテクノロジーを使用し、いつでも、どこでも、すべてのデータを暗号化して守ります。このように常に積極的にデータを保護する方法であれば、万一境界から侵入された場合でも、データは如何なるハッカーであっても読み取られることはありません。盗まれても、理解で きないデータは何の価値もありません。また、保護はコンピュータの電源がオン/オフ、ファイルのオープン/クローズに関係なく、終始一貫して継続します。他のデータセキュリティソリューションとは異なり、保護が一定の時間だけ機能するものではありません。

> **米国のバイオテクノロジー研究所がSecureAgeのデータ保護を採用**
>
> 医療分野の研究や臨床試験を行っている米国のバイオ分析受託研究機関は、内部監査に対応するため、社内従業員による試験データや患者データの漏えいから保護を行うソリューションを求めていました。
>
> SecureAgeの秘密鍵ベース公開鍵暗号基盤(PKI)技術により、すべてのデータは、あらゆる場所、そしてすべての状態(輸送中、使用中、保管中)で保護され、適切なレベルまたは権限を持つ従業員のみが特定のデータにアクセスできるようにすることで、問題が解決しました。

16 HIPAA Compliance Checklist: https://www.hipaajournal.com/hipaa-compliance-checklist/

SecureAge Security Suiteは、100%のデータ保護を実現

SecureAge Security Suiteは、長年培われた技術と設計により、以下のような方法でデータ保護を実現しています。

永続的なデータ保護

サイバー攻撃発生後に復旧作業を行うのではなく、ファイル1つ1つを完全に保護することで、権限のない人間には情報が伝わらないようにします。

データの存続期間全体にわたるプロアクティブな保護

ファイルの移動中、使用中、保存中の3つの状態全てにおいて、データ保護が保証されます。他のセキュリティソリューションとは異なり、すべてのファイルが、いつでもどこでも保護されます。

法規制に準拠

暗号化は、HIPAAに遵守するための簡単な方法です。暗号化はHIPAAコンプライアンスの必須条件ではありませんが、組織はリスクアセスメントを実施し、データ保護のために講じた措置を文書化することが求められています。

サイバーセキュリティトレーニングは不要

SecureDataのテクノロジーは、公開鍵基盤（PKI）の力を利用しています。PKIベースの暗号化はバックグラウンドで静かに機能し、ファイルレベルの暗号化、デジタル署名、電子メールなど、一般的に使用される多くのアプリケーションをサポートします。

SecureAge Security Suiteでは、自然で安全なファイル保護が可能です。ユーザーの操作や意思決定なしですべてのユーザーファイルを暗号化し、ユーザープロセスを中断しません。追加のインフラストラクチャを必要としないため、新規またはレガシーシステムへの導入も、既存のアプリケーションと並行して導入するのも簡単です。これは、人的エラーのリスクを冒すことなくデータを保護し、利便性もセキュリティも犠牲にすることなく、従業員が通常どおりに作業できるようにするための簡単な方法です。

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。

SecureAge Security Suite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、パートナーシップの機会についてのご相談は、こちらから直接当社までご連絡ください。

よくある質問

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。当社の官公庁の顧客には、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政府などが含まれます。事業法人顧客は、NTT、成田空港、ソニー、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、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した。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は、ユーザーとアプリケーションまたはサーバーに影響を与えることが少ない「フルディスク暗号化」が広く展開され、ひとまず「データ暗号化」を行えるようになりました。問題は、フルディスク暗号化は、マシンの電源がオフの状態かつ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。他のドライブにコピーされてしまえば、データは安全ではありません。

SecureAgeの次世代のアプローチは、システムの実行中でもデータの修正中でも、データは暗号化が維持されます。重要なのはデータですから、データ自身に暗号を内在させることで、保護を行います。SecureAgeは、ファイル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しますから、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ます。これにより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、このような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一切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。

SecureAge Security Suiteは、医療保険の携行性と責任に関する法律（HIPAA）や経済的及び臨床的健全性のための医療情報技術に関する法律（HITECH）などの医療規制への準拠にどのように役立ちますか？

暗号化は明示的な要件ではありませんが、組織はリスクアセスメントを実施し、健康情報（PHI）を保護するための適切な対策を合理的に実施することが求められます。SecureAge Security Suiteは、ePHIを暗号化して、情報漏えいが発生した場合に、権限のない個人がデータを使用できない、読み取れない、または判読できないようにします。

暗号化は、デバイスの紛失または盗難時の情報漏えいに関連する罰金から、組織を保護するための最良の方法の1つです。2009年HITECH法では、適切な暗号化を行なったデバイスの盗難や紛失は、情報漏えいとは見なされません。

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？

管理されていない環境から情報にアクセスすること、サイバー攻撃の頻度と精巧さの両方が増加していること、内部からのデータ盗難の脅威など、現在の状況に疑問を持つことです。

そして、100%のデータ暗号化は、皆が受け入れる原則です。フルディスク暗号化はこれを満たすものですが、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ものであるのか、よく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します。今こそデータを積極的に管理できる時です。その方法を知るために、ぜひSecureAgeへご連絡ください。

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。当社のPKIベースのセキュリティ技術へのアプローチは、2003年シンガポール政府向けのSecureDataとしてリリースされました。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により、公共機関や民間企業はそのネットワーク内のデータを完全に制御、保護できるようになります。すべてのファイルを、いつでも、どこでも保護します。

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。当社の先進的なお客様には、シンガポール、香港、および日本の政府系機関、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

プロアクティブな保護とは

データセキュリティ

データセキュリティとは、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ると考えています。他社から提供されているソリューションは、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。トレーニングとモニタリングは常に機能するとは限りません。そして、解決策が自然でない場合、人々は独自の、通常は安全でない方法を作り出します。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のこれらの原則の間にトレードオフはありません。特に、データの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」方法が難しい場合に、個人が何かを達成するために他の方法を認識することは、SecureAgeがその製品を設計する上での基本です。

さらに詳しく

ホワイトペーパーの詳細については、こちらをクリックしてください。または、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。データのセキュリティを向上させ、無料トライアルを手配する方法について、喜んでご相談させていただきます。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

Copyright © 2021 SecureAge Technology. 不許複製・禁無断転載。