官公庁・自治体向け

# セキュリティとコンプライアンス態勢を強化するためのサイバーレジリエンスの重要性

～ 米国のコンプライアンスを参考に ～

ABSOLUTE®

2023年1 月、米国国家安全保障局 (NSA)、サイバーセキュリティおよびインフラセキュリティ局 (CISA)、および多州情報共有・分析センター (MS-ISAC) は、複数の連邦民間行政機関に影響を与える一連の攻撃を発見した後、共同勧告を発表しました [1] 。

IBM の「Cost of a Data Breach Report 2022[2]」によると、この調査に含まれる公共部門のデータ漏洩の平均コストは 207 万ドルでした。政府機関は、いくつかの理由から、脅威行為者にとって魅力的なターゲットとなります。まず、国民のデータが大量に保管されていることが挙げられます。そのため、情報を盗み出そうとするサイバー犯罪者だけでなく、データを人質に取って破壊工作を行うランサムウェアの標的にもなっています。政府機関が魅力的なターゲットである理由のひとつには、IT インフラのアップグレードを行う際の動きが、予算の問題や役所特有の身長さのために鈍くなってしまうことが珍しくないことが挙げられます。

日本でも、2022 年 9 月 6 日に、政府が運営する電子サイト「e-Gov」など計 4 省庁 23 サイトと、地方税の手続きサイト「eLTAX」が一時閲覧できなくなったり[3]、2023 年 3 月以降、DDoS 攻撃を応用した特殊な手段を用いた大規模なサイバー攻撃を、中央省庁や自治体など複数の官公庁が受けている状況が 4 月 29 日に明らかになったりする[4]など、官公庁や自治体を狙った攻撃は多く確認されています。

公共の安全を守るために、サイバーセキュリティのガイドラインや規制があります。日本では、各公共団体が個人情報保護法に基づいてそれぞれ個人情報保護条例を策定し、施行しています。米国では、公共部門が強固なセキュリティ体制を維持するために、いくつかのコンプライアンス指令が制定されています。**このレポートでは、公共機関での個人情報保護の参考としていただくため、米国のコンプライアンス要件の一部を簡単に説明し、組織が直面する課題に対抗するためのエンドポイントおよびネットワークの回復力の重要性について説明します。**

出展：

1 CISA, Protecting Against Malicious Use of Remote Monitoring and Management Software.

2 IBM, Cost of a Data Breach Report 2022, pg.11

3 日経新聞 https://www.nikkei.com/article/DGXZQOUA072LT0X00C22A9000000/

4 Cyber Security.com https://cybersecurity-jp.com/news/82450

## コンプライアンスのニーズを理解する

公共機関は、多くの場合、サイバーセキュリティに関して、レガシーな IT インフラから人員不足に至るまで、複雑な課題を抱えています。このような課題を解決するために、コンプライアンス規定が強化されています。セキュリティに対する効果的なリスクベースのアプローチには、これらの要件が公共機関に与える影響の評価を含める必要があります。ここでは、今日の米国政府機関におけるサイバーセキュリティの意思決定を促進する主要な規制とフレームワークを紹介します。

### 1.2014 年制定 連邦情報セキュリティ管理法 (FISMA)

2014 年、米国政府は 2002 年連邦情報管理法 (FISMA 2002) を改正する連邦情報セキュリティ管理法を制定しました。米国国立標準技術研究所 (NIST) によると、FISMA は「各連邦機関は、他機関、請負業者、またはその他のソースから提供または管理されるものを含め、機関の業務および資産を支える情報および情報システムに対して情報セキュリティを提供するための機関全体のプログラムを開発、文書化、および実装することを要求する」とあります[5]。2014 年の改正では、連邦行政府の文民機関の情報セキュリティ方針の実施を監督することに関連する米国国土安全保障省 (DHS) の権限の成文化など、2002 年の法律に対して多くの変更が行われました。

FISMA の義務を果たすために、IT リーダーは組織のリスク状況を理解し、環境を継続的に監視し、システムとデータを保護するために適切なセーフガードを適用する必要があります。米国の政府機関は、毎年独立監査人による年次監査に合格しなければなりません。FISMA への準拠を達成・維持できない場合、政府との契約や資金を失うなどの結果を招く可能性があります。コンプライアンスへの取り組みを支援するため、NIST は Special Publication (SP) 800-37.[6] などのガイダンスを発行しています。

### 2. 連邦リスク・権限管理プログラム (FedRAMP)

FedRAMP は、政府機関が安全なクラウドサービスを採用することを目的としたプログラムです。クラウドサービスプロバイダーが連邦政府によってサービスを利用されるために満たすべき要件をまとめています。クラウドサービスプロバイダーが FedRAMP を通じて認可されるには、ふたつの方法があります。ひとつは、JAB (Joint Authorization Board) が P-ATO (Provisional Authority to Operate) を付与することです。もうひとつは、エージェンシーと直接交渉して ATO (Authority to Operate) を取得する方法です。FedRAMP.gov によると、FedRAMP と FISMA はともに NIST SP 800-53 のセキュリティ管理を活用しており、FedRAMP にはクラウドコンピューティング特有の要素に対応する NIST ベースラインを超える管理、パラメータ、ガイダンスも含まれています[7]。

FISMA
Federal Information Security Management Act

5 NIST, NIST Risk Management Framework.

6 NIST, Risk Management Framework Update: NIST Publishes SP 800-37 Revision 2.

7 FedRAMP, FAQs: General.

## 3.CDM ( 継続的診断・緩和 ) プログラム

CDM プログラムは、政府機関の攻撃対象領域の縮小、セキュリティの可視化、連邦政府のインシデント対応能力の強化、FISMA 報告の合理化を目的として開発されました。CISA は、「CDM プログラムは、サイバーセキュリティツール、統合サービス、ダッシュボードを参加機関に提供し、ネットワークの可視性と認知度を向上させ、サイバー敵対者から防御することによって、それぞれのセキュリティ態勢を改善することを支援する」と述べています。「CDM プログラムは、4 つの能力分野を通じて、最終的に脅威の表面を減らし、連邦政府のサイバーセキュリティへの対応を改善するものです。資産管理、アイデンティティとアクセス管理、ネットワークセキュリティ管理、データ保護管理です。」[8]。このプログラムに関連するソフトウェアとハードウェアは、CDM 承認製品リスト (APL) に追加されるために、DHS CISA 認定プロセスを受けます。DHS CISA 資格認定プロセスを通過した製品は、CDM 承認製品リストに追加されます。

## 4.NIST SP 800 シリーズ

NIST SP 800 シリーズは、サイバーセキュリティに関連するガイドライン、技術仕様、およびその他の情報を備えています[9]。連邦政府のセキュリティへの取り組みやコンプライアンスニーズをサポートするために設計されています。FISMA に関連する要件も含まれます。800 シリーズで注目を集めてる資料のひとつが NIST SP 800-53 です。一般に、米国のすべての連邦政府機関およびコントラクタは、情報システムおよびデータを保護するために、このフレームワークを順守しなければなりません。ただし、国家安全保障システムは例外で、そのシステムに関する政策的権限を持つ連邦政府高官が明示的に承認した場合にのみ、このフレームワークに準拠する必要があります。NIST 800 シリーズの資料は、政府機関だけでなく、公共部門以外の組織でもよく利用されています。

8 CISA, CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM ASSET MANAGEMENT – What is on the Network?, pg.1.

9 NIST, NIST Special Publication 800-series General Information.

## 5.Center for Internet Security (CIS) Critical Security Control ( 重要なセキュリティコントロール ) およびベンチマーク

CIS Security Controls は、組織がセキュリティ態勢を改善するために取るべき行動のリストであり、どこから手をつけるべきかの優先順位をつけることができます。このコントロールは、NIST SP 800-53 や ISO/IEC 27000 シリーズなどの他のコンプライアンスフレームワークや、HIPAA や FISMA などの規制の要件やガイドラインに対応しています。CIS コントロールは、さまざまなシステムやデバイスを保護するための推奨されるプラクティスを集めたものです。ただし、CIS ベンチマークは、特定の OS、ソフトウェア、ミドルウェア、ネットワーク機器を安全に構成するためのガイドラインです。

## 6. 刑事司法情報サービス (CJIS) セキュリティポリシー

CJIS セキュリティポリシーは、法執行機関にとって重要なコンプライアンス義務です。連邦捜査局の刑事司法情報サービス部門は、権限を与えられた組織や個人が、仕事を効果的に行うために必要な刑事司法情報 (CJI) データベースへのアクセスを提供します。情報の機密性を考慮し、データを安全に保存、伝送、処理するためのルールが必要です。CJIS セキュリティポリシーの役割は、適切なポリシーとサイバーセキュリティコントロールの実施を含む、CJI を保護するための基本要件を確立することです。従わない場合は、深刻な影響を及ぼす可能性があります。

## 7.PCI DSS (Payment Card Industry Data Security Standard)

PCI DSS は、クレジットカード情報をどのように保護しなければならないかを定めた業界標準です。クレジットカードの不正利用のリスクを軽減し、カード利用者のデータを保護するために、クレジットカードブランドから義務づけられています。PCI DSS は、カード会員情報を処理、保存、または送信するすべての組織に適用されます。公共部門では、クレジットカード決済を利用する政府機関も、PCI の義務に従わなければなりません。

## 8.HIPAA および HITECH

1996 年の医療保険の相互運用性と説明責任に関する法律 (HIPAA) と 2009 年の経済的および臨床的健康のための医療情報技術 (HITECH) 法は、ヘルスケア業界にとって最も重要な規制のひとつです。HITECH は、異なる目的で作成されたものの、新たな違反報告要件を義務付け、HIPAA のプライバシーおよびセキュリティ規定を、法律の対象となる組織の業務提携先にまで拡大することで、HIPAA の目標をサポートしました。2013 年、Omnibus Rule は、HIPAA のプライバシー、セキュリティ、および施行規則の修正を最終決定し、セキュリティとプライバシー保護を強化するための HITECH の多くの条項を実施しました。

HIPAA と HITECH は、患者情報の保護とプライバシーを確保するために、組織が持つべき保護レベルを定めています。政府機関もこれに倣い、一般市民から収集したデータも含め、健康情報を安全に保つための適切な方針と管理を実施しなければなりません。

## 9.OMB サイバーセキュリティの義務化

米国行政管理予算局 (OMB) は、サイバーセキュリティに関連する多くの義務づけを行っています。この要件は、データプライバシーに関連する問題や、機密データおよびシステムに対する適切なセキュリティ保護を含んでいます。たとえば、2022 年に OMB M-22-09 が発行され、連邦政府機関が 2024 会計年度末までに実施するゼロトラスト・アーキテクチャ戦略を策定しました。別の例として、OMB M-22-18 があります。これは、ソフトウェアのサプライチェーンのセキュリティを改善するための指令で、省庁のシステムでサードパーティーのソフトウェアを使用する場合や、省庁の情報に影響を与える場合には、NIST のガイダンスに従うことを義務づけるものです。

## 10. ゼロトラスト・アーキテクチャ

ここ数年、ゼロトラストは、政府機関や民間企業にとって、単なるバズワードから現実的な重要な戦略的優先事項へと変化しています。ゼロトラストアプローチでは、ユーザー、サービス、デバイスは、組織のネットワーク内外を問わず、デフォルトで信頼されません。厳密なアクセス管理が必要で、セキュリティや生産性の向上が期待できます。OMB の覚書 OMB M-22-09 により、ゼロトラスト･アプローチは、連邦空間におけるサイバーセキュリティ計画の推進力のひとつとなっています。OMB M-22-09 において、OMB は連邦政府が「重要なシステムやデータを保護するために、従来の境界ベースの防御にもはや頼ることはできない」[10] と指摘しています。

「この戦略は、政府全体のアクセス制御の新しい基準を設定し、高度なフィッシングに対する防御を優先し、保護と監視を一貫して適用できるように ID システムを統合するよう機関に指示する」[11] と続けています。

10 OMB, “M-22-09 MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES” , Pg. 2.
11 Ibid.Absolute Software, “Strengthening Security & Compliance Posture Through Cyber Resilience” , Pg. 5.

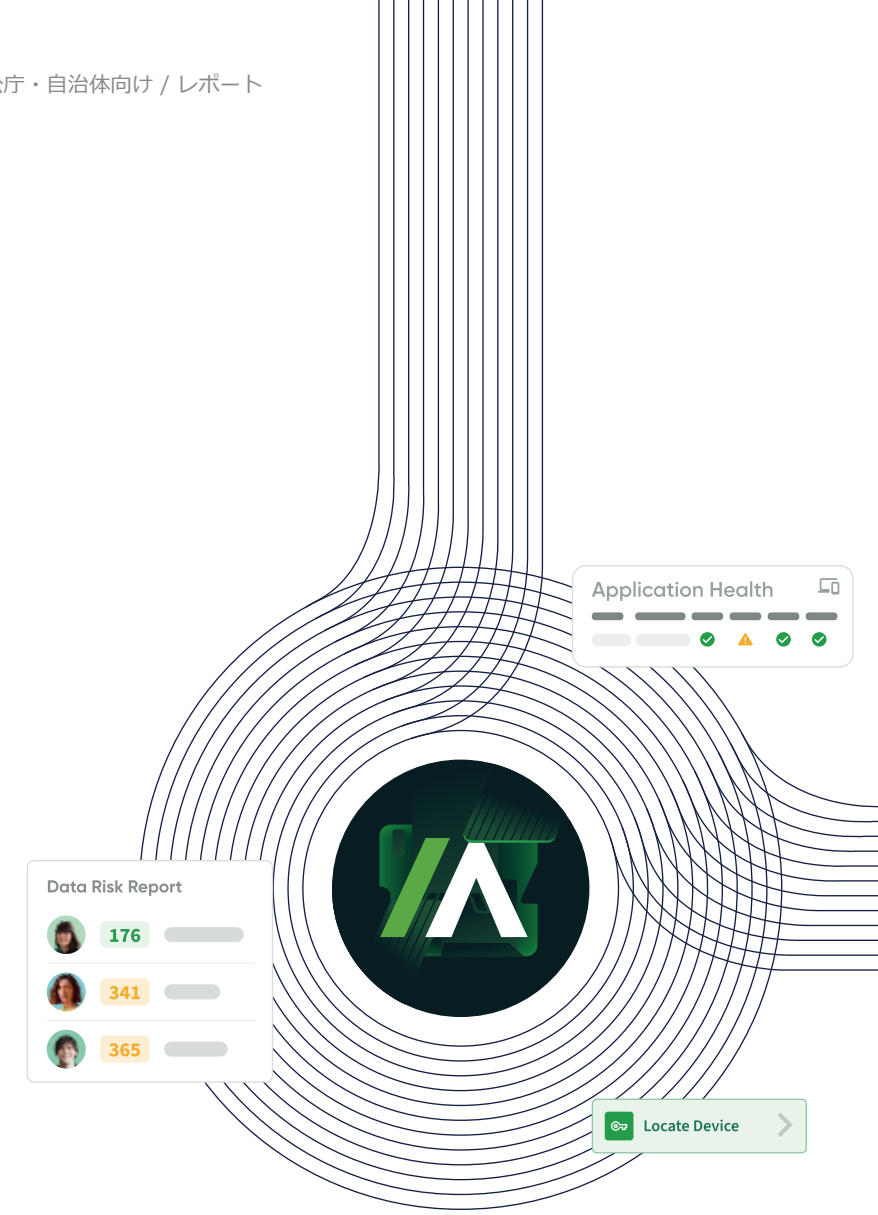
## どこから始めるべきか

公共部門が考慮すべき規制、標準、フレームワークのリストは膨大な数にのぼります。何から手をつければいいのかわからないこともあります。しかし、組織が直面している課題は非常に明確です。Absolute がまとめた「サイバーレジリエンスを通じたセキュリティとコンプライアンス態勢の強化」レポートによると、公共部門 ( 連邦および地方 ) の組織におけるエンドポイントの 81%が機密データを保有しています[10]。さらに、多くのデバイスがパッチ未適用であり、政府機関ではアップデートの遅れが大きな問題となっていることも、この現実を物語っています。Absolute の分析によると、政府機関向けの Windows 10 のパッチは平均 214 日経過していることが判明しました[13]。

モバイルワークの増加に伴い、脆弱なデバイスと機密データが混在することで、炎上しやすい状態になる可能性があります。対策として、脆弱性管理、強力なアクセス制御、暗号化などのデータ保護対策など、エンドポイントセキュリティに重点を置く必要があります。デバイスとデバイス上のデータのセキュリティ態勢を完全に把握できなければ、組織はコンプライアンスに関連する以下のような重要な質問に答えることができないままです。組織の機密データはどこに管理されているか？安全性を保つためにどのような管理が行われているか、またその状況は？各種規制に準拠しているか？効果的なコンプライアンス・プログラムを確立・維持し、CIS Security Controls などの基準やフレームワークを遵守するためには、これらの質問に的確に答える必要があります。

日本では、多くの場合、IT システムの管理を、官公庁や自治体と契約した企業が担当しています。個人情報を搭載したデバイスやメディアを企業の担当者が持ち出して紛失する事案も発生しており、自治体が多額の損害賠償を委託先に請求したケースもみられます[14]。この事例では、委託先企業が契約に反して再委託や再々委託を繰り返して自治体に発覚しないように工作していたなど、企業による悪質な対応も指摘されています[15]。この自治体では事件後、ハード、ソフト、研修の面で再発防止策が策定、実施されていますが、自治体はもちろん、自治体に関わる企業においても、厳格なコンプライアンス意識と具体的な施策の実施が求められます。

多くの場合、コンプライアンス違反が発覚した後に発生するコストは、コンプライアンスのコストよりも高くなります。セキュリティ対策が不十分で情報漏えいにつながったとして罰金を科されたり、損害賠償を請求されたりした場合、その代償は金銭的な問題にとどまらない可能性があることを考慮する必要があります。たとえば、世間や職員から見た組織の風評被害は、永く続く可能性があります。




12 Absolute Software, “Strengthening Security & Compliance Posture Through Cyber Resilience” , Pg. 5.
13 Absolute Software, “2023 Resilience Index: A False Sense of Security Imperils Digital Enterprise” , Pg. 7.
14 ScanNetSecurity https://scan.netsecurity.ne.jp/article/2023/06/19/49538.html
15 神戸新聞 NEXT https://www.kobe-np.co.jp/news/sougou/202211/0015846732.shtml

## サイバーレジリエンスによるセキュリティとコンプライアンスの強化

組織のリーダーは、必要な専門知識にアクセスできなければなりません。Absolute Software は、政府機関や企業がセキュリティとコンプライアンスを確保するために役立つリソースのひとつです。Secure Endpoint 製品ポートフォリオは、独自の技術である Application Resilience™ を活用し、デバイス群全体のセキュリティ制御の確立と維持を支援し、レジリエンスを高めます。さらに、ガバナンスや監査に必要なエビデンスを、効率的かつ拡張可能な方法でチームに提供します。これは、管理者がアクセス可能なひとつのプラットフォームで、組織全体のインサイトと可視性を提供することによって実現されます。

Absolute Secure Access は、さらに一歩進んで、ZTNA を提供する製品です。Absolute Secure Access は、各デバイスに関する動的なコンテキストデータを使用して、リソースへのアクセスを認証します。不要な接続や危険な接続はブロックされ、ユーザーはオンライン上の脅威や危険なコンテンツから安全に保護されます。さらに重要なことに、アクセスを許可されていないエンタープライズリソースの安全が守られます。これにより、ID ベースのリスクエクスポージャーを最小化するのに役立つ Comply-to-Connect ( 順守して接続する ) アプローチを実施することができます。

Absolute Platform は、組織のセキュリティとコンプライアンス態勢を強化するために効果的に機能します。同時にエンドユーザーエクスペリエンスの向上、トラフィックの最適化、ネットワーク接続のレジリエンスの強化も実現します。セキュリティやコンプライアンスを強化することで、職員の生産性が阻害されることはありません。

## ケーススタディ：米国環境保護庁 (EPA)

資産管理と追跡に自作のシステムを使用していた EPA の IT チームは、ソフトウェアとハードウェアの監査を手作業で行わなければならず、各ユーザーを個別に調査しなければ、ソフトウェアライセンスの制限内か制限外かを把握することができませんでした。そのため、ソフトウェアベンダーとの契約に準拠しないリスクを抱えているのが実情でした。また、このマニュアル作業では、パッチ管理に時間がかかるという問題がありました。

2011 年、EPA は Absolute の導入を決定しました。EPA のデスクトップ技術管理者兼情報専門家である Walter Williams 氏は、「Absolute Secure Endpoint は、我々が非常に有効だと思う多くの機能を備えています」と述べています。「どのソフトウェアがどのマシンにロードされているかを確認することで、ソフトウェアライセンスを最大限に活用しているか、あるいは十分に活用できていないかを判断できるようになりました。活用されていないソフトウェアライセンスを、それを必要とするユーザーに割り当てることで、不要なライセンスを追加購入することがなくなり、その分を他の支出に回すことができるようになりました。」

Williams 氏はさらにこう言います。「より多くのデータがユーザーの手に渡り、ユーザーがより頻繁にリモートで作業するようになった状況でも、Absolute が安心感を与えてくれています。モバイルデバイスが行方不明になったり、紛失したりすることがないとは言い切れません。しかし、データが危険にさらされることがないことを保証する措置を講じていることは重要です。Absolute で保護されているデバイスが行方不明になっている場合、デバイスをフリーズするか、特定のファイルをリモートで削除するか、ハードディスクを完全に消去するかという選択肢があり、回収された場合の復旧の可能性は高くなります。」

## コンプライアンスが組織にとって負担である必要はない

セキュリティ上の課題は常に何らかの形で存在しますが、それを致命的問題だと捉える必要はありません。適切なテクノロジーと専門知識、そしてエンドポイントとネットワークの回復力に焦点を当てることで、政府機関はコンプライアンスの達成に伴う問題を解消することができます。

ABSOLUTE®

Absolute Software は、約 21,000 社のお客様から信頼いただいている、自己復活型のインテリジェント・セキュリティ・ソリューションの唯一のプロバイダです。Absolute は、6 億台以上のデバイスに搭載され、エンドポイント、アプリケーション、ネットワーク接続にインテリジェントかつダイナミックに可視化、制御、自己修復機能を実現します。ランサムウェアや悪意のある攻撃の脅威が高まる中、サイバーレジリエンスを強化するための永久デジタル接続を実現する唯一のプラットフォームです。

**お問合せまたは**
**デモのリクエストは**
**こちら**