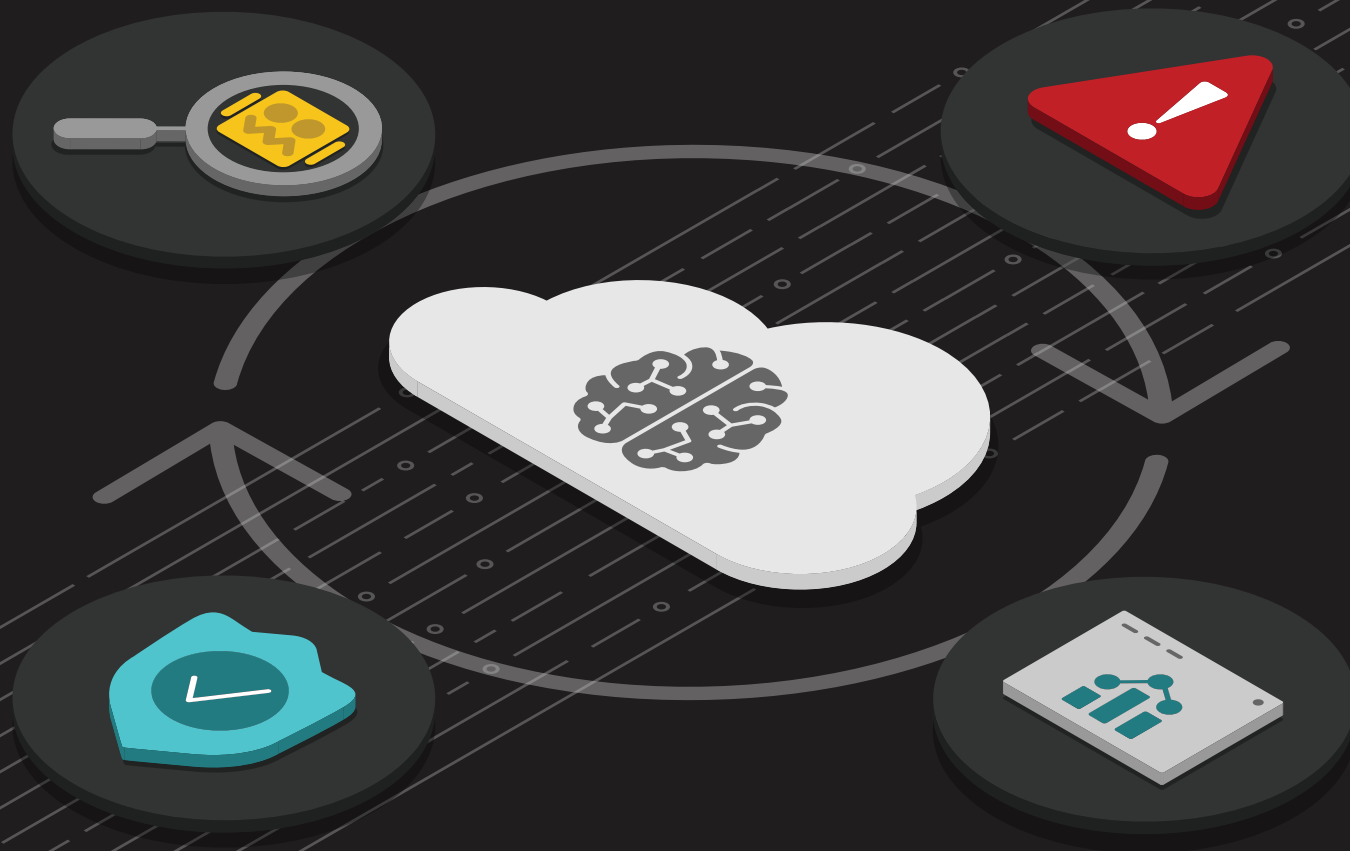




コンプライアンスライフサイクルの 4 つのステップ

F5® Distributed Cloud App Infrastructure Protection (AIP)、Distributed Cloud AIP Managed Security Services、Distributed Cloud AIP Insights、ThreatML™を使用して、セキュリティ機能を自動化し、コンプライアンス監査を簡素化します

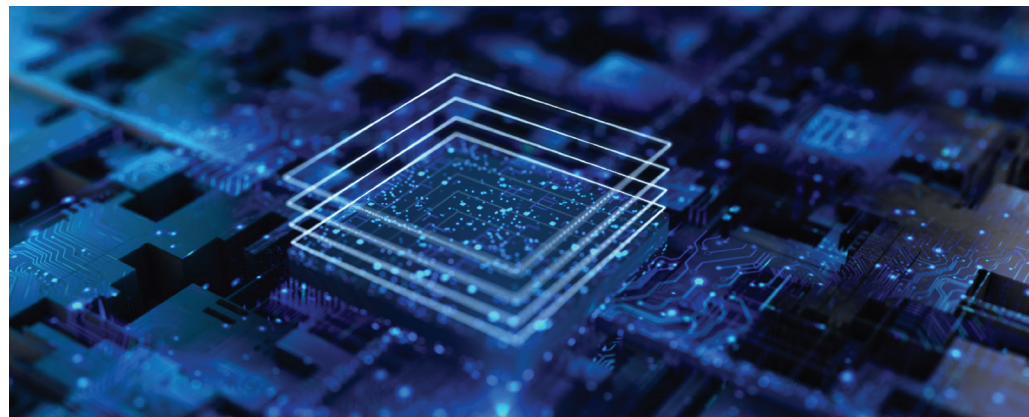
規制変更への対応

セキュリティとコンプライアンスがますます相互に関連し合っていることは否定できません。顧客データの保護に対する規制がますます厳しくなる中、組織はコンプライアンスを維持するために IT セキュリティとデータ管理プロトコルを徹底的に点検することが求められています。その結果、コンプライアンスを遵守することは、単に作業のチェックリストをマニュアル通りに完了することではなく、インフォセキュリティの専門家が変更に伴う対応を常に取り続けなければならないものとなっています。

特に今の時代の複雑なクラウド環境では、さまざまなコンプライアンス要件を満たすことは簡単ではありませんが、それは、新市場の開拓、顧客満足度の向上、販売プロセスの高速化、企業全体のセキュリティ体制の改善にも繋がるものです。セキュリティの完成度を高めることに関して言えば、コンプライアンスはその戦略上、とても重要なものであることがわかっています。ビジネスの対象が特定の業種または海外の顧客であろうが、新しい市場に参入する際には、継続的な教育や最新のコンプライアンスと規制基準への遵守が必要不可欠です。

サイバーセキュリティに興味がありこの電子ブックをご覧になるということは、お客様の組織はすでにクラウドネイティブを採用なさっていると考えられます。クラウドネイティブの組織は、テクノロジーの進化に合わせてインフラストラクチャを柔軟に適応させることができるため、コンプライアンスへの取り組みや達成において大きな利点を得られます。しかし、組織にとっては、クラウドファーストであることは、処理する膨大な量のデータの保護に大きな責任が伴うことでもあります。

したがって、SOC 2、HIPAA、PCI DSS、ISO 27001 などの一般的フレームワークのコンプライアンスを遵守することは、クラウドネイティブの組織にとって不可欠なマイルストーンです。顧客データを保護することは、顧客の信頼を得て満足度を高めるためには極めて重要であり、多くの場合、見込み客は顧客になる前提としてデータ保護を必要とします。ただし、リソースが限られている組織にとって、コンプライアンス監査のセキュリティ分野において、合格に向けての準備をし、それを勝ち取ることは容易なことではありません。1 つまたは複数のコンプライアンス基準に合格する任務を負うセキュリティ担当のリーダーは、監査に先立って適切な制御を設定し、特定の要求を満たすためにサイロ化されたデータポイントから新しいレポートを生成するために、骨の折れる手作業に追われるという課題に直面しています。



コンプライアンス遵守に向けて

以前は Threat Stack と呼ばれていた F5 Distributed Cloud AIP に不慣れな場合は、まずは、F5 がクラウドセキュリティ企業であることをご理解いただくことが大事です。ただし、コンプライアンスとセキュリティは相互関連にあるため、F5 のルール手法をお客様のコンプライアンスイニシアチブに適用することができます。これをコンプライアンスクラシファイアと呼びます。では、なぜこれが重要なのでしょうか？まず、クラウドのセキュリティ体制を完全に整えることで、コンプライアンスの目標をより迅速に達成することができます。その内容については、次をご覧ください。

多くの SaaS 企業と同じように、お客様の組織も Amazon Web Services (AWS) で運用なさっているとします。その場合、CIS ベンチマークと AWS セキュリティチェックリストに従ってインフラストラクチャが構成されていることを確認する必要があります。そうすることで、多くのセキュリティやコンプライアンスの要件を満たすことができ、コンプライアンスへの取り組みを初期の段階から簡素化することができます。

AWS インフラストラクチャを保護したら、次に行うべきことは、現在および将来採用するコンプライアンス規制を判断することです。そして、すでにコンプライアンスに対応している場合は、変更と更新に対する注意点を見極めます。こうすることで、企業では、ビジネスを拡大する中、コンプライアンスのどの部分に力を入れるべきかを特定することができます。

Distributed Cloud AIP の 4 つのステップからなるコンプライアンスライフサイクルへのアプローチ

これまで説明してきたように、コンプライアンスとは到達点ではなく過程です。この継続的なライフサイクルには、組織のビジネス価値を高めるフレームワークに準拠するための初期段階の取り組みから、監査および継続的なコンプライアンス体制の維持に至るまでの全過程が含まれます。

Distributed Cloud AIP は、セキュリティとコンプライアンス機能を自動化することで、組織がコンプライアンスを促進し、監査を合理化するお手伝いをします。F5 では、一般的なフレームワークに事前に構築した独自のルールセットを提供することで、お客様がコ

ンプライアンスを迅速に遵守し、維持できるようにします。さらに、自動化された包括的なコンプライアンスレポートを提供することで、お客様が監査要件を満たし、プロセスを加速化できるようにいたします。コンプライアンスへの取り組みを簡素化するために、F5 ではライフサイクルを4つのステップ（観察、分類、実証、維持）に分けています。では、詳しくご説明します。

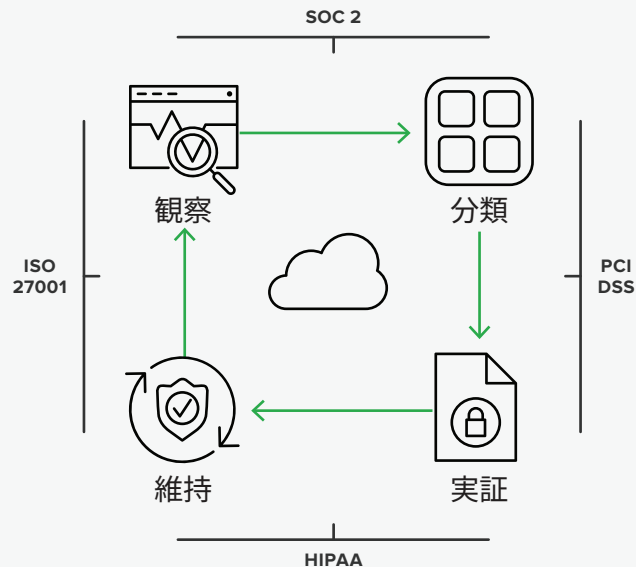


図 1：4 つのステップからなるコンプライアンスのライフサイクル



「Stratason 社では、評価者が F5 の取り組みを簡単に**検証できるようにする**必要があります。[Distributed Cloud AIP] を使用することで、監査人に渡すことができる監査証跡とレポートだけではなく、誰が、どこで、いつ、何を行っているのかについてのインサイトも手に入れることが出来ています」

Stratason 社共同創設者兼 CTO
ブライアン・デイリー（Brian Daiely）氏



ステップ 1: テレメトリ収集でスタックを観察

Distributed Cloud AIP は、顧客ベース全体で 1 日あたり 600 億件のイベントを処理し、真に包括的なクラウドセキュリティとコンプライアンスのモニタリングを実現します。F5 では、お客様のクラウド管理コンソール、ホスト、コンテナ、Kubernetes、そしてアプリケーション全体をモニタリングし、環境への十分な可観測性を提供し、コンプライアンス遵守に向けての取り組みをサポートします。

提供するサービスは次のとおりです。

- クラウドインフラストラクチャとアプリケーションスタックの各レイヤへのセキュリティとコンプライアンスのテレメトリ (Linux サーバー、Windows サーバー、Kubernetes クラスタ、AWS Fargate、EC2 ワークロード、Node.js、Python、Ruby のフレームワーク対応)
- 既知の脅威、リスクの高い動作、確立されたセキュリティやコンプライアンスポリシーからの逸脱に関連付けられた、構成可能な事前構築のルールセット
- 平均検出時間 (MTTD) と平均認識時間 (MTTK) の短縮を実現する、API サポートとデータレイク統合によるフレキシブルな検出結果の利用



ステップ 2: カスタムルールで動作を分類

クラウドインフラストラクチャとアプリケーションスタック全体からの完全なテレメトリ収集は、堅牢なルールセットに反映され、顧客がクラウドセキュリティの運用とコンプライアンスの体制を完全に可視化できるようにします。これらはコンプライアンスクラシファイアと呼ばれます。

F5 のプラットフォームは、組織に次のものを提供します。

- コンプライアンスフレームワーク (SOC 2、PCI DSS、HIPAA、および ISO 27001) に合わせて調整されたルール。これにより、お客様はセキュリティコンプライアンス認定への準備を整え、進行中の監査要求を満たすことができます。
- ルールを活用する機能と、詳細な検出を可能とする教師あり学習モデルを組み合わせることで、セキュリティチームは検知能力を向上させ、既知および未知の脅威に対するリスクの可視性を高め、コンテキストも改善します。
- コンテキストの提供により、コンプライアンスクラシファイアはコンプライアンスに焦点を当てたルールと効果の高いアラートを作成するので、セキュリティ担当のリーダーはコンプライアンス認定合格を目指し、必要なセキュリティ制御を変更・実装することができます。



ステップ 3:

高度なレポート作成でコンプライアンスを実証

Distributed Cloud AIP の最新かつ包括的なコンプライアンスレポートは、コンプライアンス監査に合格するために必要な情報を収集し一元化する月次レポート（アプリケーション内で配信）です。たとえば、必要な情報とは、特定のデータを保護するためのルールの証明や、規制実施に向けて対応する制御などです。レポートは、特定のコンプライアンスフレームワークに合わせて作成され、監査中のその他の要求に対応するために簡単にアクセスできるようになっています。

主なレポート作成機能とは、次のとおりです。

- レポート作成と視覚化のワークフロー：収集したデータを高度なコンプライアンス分析と脅威ハンティングのアクティビティに組み込みます。
- セキュリティ情報およびイベント管理ツール（SIEM 統合）：Distributed Cloud AIP イベントを、他のインフラストラクチャのモニタリングおよびオーケストレーションシステムからのデータと共に集計します。
- コールドストレージ：Distributed Cloud AIP データを Amazon などのサービスに長期保存します。



ステップ 4:

プロフェッショナルなサービスで体制を維持する

F5 が提供するサービスである Distributed Cloud AIP Managed Security Services および Distributed Cloud AIP Insights は、セキュリティプログラムを強化しコンプライアンスを継続的にサポートする上で、役に立ちます。

たとえ、最高のルールや ML テクノLOGYであっても、人間の直感、推論、意思決定の能力に取って代わることはできません。そこで、365 日 24 時間体制の SOC とアドバイザリーサポートを利用することで、コンプライアンス体制の維持と監査への合格を実現します。

- **Distributed Cloud AIP Managed Security Services:** このサービスにより、F5 のエキスパートであるセキュリティアナリストは、お客様の環境をモニタリングし、潜在的なセキュリティやコンプライアンスのインシデントを警告し、それらに優先順位を付けて解決のお手伝いをします。F5 の社内エキスパートは、Distributed Cloud AIP の自動化、リアルタイムのアラート、異常や脅威の検出、そして比類なき調査機能を活用しています。
- **Distributed Cloud AIP Insights:** F5 のセキュリティアナリストは、Distributed Cloud AIP から重要なセキュリティおよびコンプライアンスデータを収集し、お客様に環境内の危険な動作パターンを事前に特定し理解できるようアドバイスを行います。また、サードパーティの統合と高度なルール調整によるサポートにより、お客様は問題を効率的に検出して修正し、コンプライアンスを迅速に遵守して実証することで平均検出時間（MTTD）と平均認識時間（MTTK）を短縮します。



クラウドセキュリティ戦略を強化することで、 シームレスなコンプライアンスを推進

コンプライアンスを加速化することに加えて、クラウド管理コンソール、ホスト、コンテナ、オーケストレーション、アプリケーションなどのインフラストラクチャスタックの各レイヤをモニタリングします。こうすることで、お客様は、クラウドのビジネス上のメリットを自信を持って活用するために必要な、フルスタックのセキュリティとコンプライアンスの可視性や制御を実現することができます。これは、次のような実行可能なコンテキストを提供します。

- コンテキスト化されたシグナルにより、リスクの高い動作や侵害の兆候をリアルタイムで把握できます。
- インフラストラクチャとアプリケーションスタックの各レイヤで積極的にリスクを軽減します。
- 堅牢なルールセット、動作分析、ML ベースの脅威検出が連携し、内部および外部の脅威を特定します。
- リアルタイムでの脅威検知、コンテキスト、修正勧告により、インシデント対応を迅速化します。

F5 のセキュリティとコンプライアンスに関する豊富なインサイトは、既存のセキュリティ、コンプライアンス、DevOps ワークフロー内で利用することが可能です。これは、Distributed Cloud AIP、サードパーティのツール、または Distributed Cloud AIP Insights と Managed Security Services との共同マネージドサービスを介して行われます。

フルスタックのセキュリティ可観測性

- **アプリケーション**: 脆弱性をモニタリングし、アプリケーション、マイクロサービス、API に対する攻撃をブロックします。
- **オーケストレーション**: Kubernetes の危険な動作や設定ミスをモニタリングします。
- **コンテナ**: 自動化されたセキュリティ向けのコンテナとして展開され、Docker コンテナ全体で疑わしいアクティビティを追跡します。
- **ホスト**: ホストベースの侵入検知と、すぐに使用できるルールセット。
- **クラウド管理コンソール**: クラウドアカウントアクティビティのランタイムモニタリングのために、クラウドサービスプロバイダーと統合します。

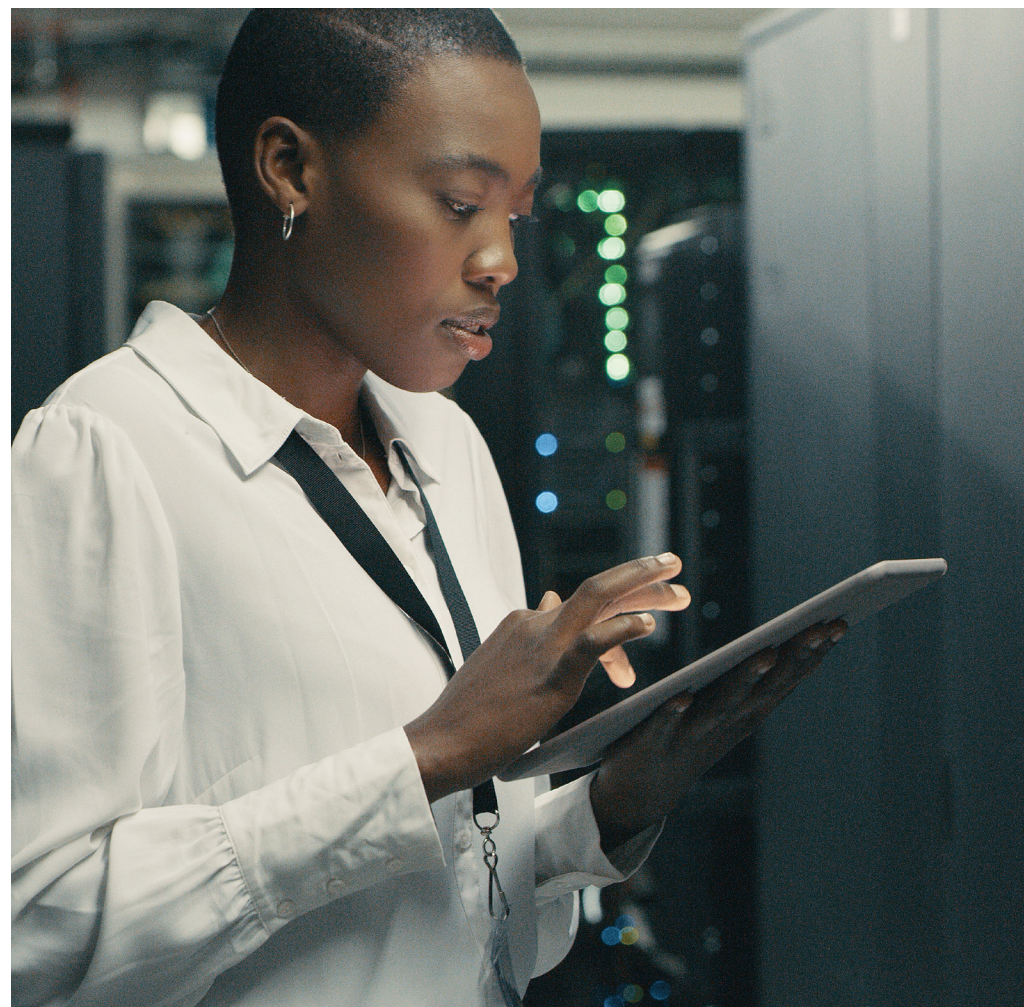
Distributed Cloud AIP のイノベーションへの取り組み

F5 では、この電子ブックから得られる最大のメリットとして、堅実で実行可能なコンプライアンスロードマップを作成することは、努力の価値があるご理解いただければと考えています。Distributed Cloud AIP ソリューションのようなテクノロジーにより、コンプライアンス要件を満たすことが可能となり、監査人と顧客にコンプライアンスをよりシームレスに伝えることができます。

コンプライアンスに対する従来のアプローチでは、もはや、今日の複雑で多様化したインフラストラクチャとアプリケーションのスタックに対応することができません。しかし、Distributed Cloud AIP ソリューションは、コンプライアンスを取り巻く煩わしさを軽減し、高度なレポート作成の機能を使って監査プロセスを加速化させます。

F5 では、コンプライアンスと包括的なレポート作成に向けた、脅威の予測と識別を目的とする教師あり機械学習と連動する高度なルールラベリングなど、主要な機能を改良し、プラットフォームやコンプライアンスの能力を強化することで、セキュリティとコンプライアンスの目標達成に向けて必要なサポートを追加提供し、革新への道を歩み続けます。

コンプライアンスは強力なビジネス推進力であり、競争の激しい SaaS 市場で際立つ信頼と自信を高めるものです。Distributed Cloud AIP ソリューションがお客様のセキュリティやコンプライアンスの要件にどのように対応できるのか、詳しい内容については、是非 F5 までお問い合わせください。



THREAT STACK：F5 ソリューションになりました

Threat Stack は製品名称変更し、現在、F5 Distributed Cloud App Infrastructure Protection (AIP) になりました。本ソリューション、F5 のセキュリティオペレーションセンター (Distributed Cloud AIP Managed Security Services、Distributed Cloud AIP Insights を含む)、およびその他につきまして詳しくは、F5 のクラウドセキュリティとコンプライアンスの専門家までお気軽にお問い合わせください。

クラウドセキュリティのお悩みは F5 のセキュリティ専門家にぜひお任せください。詳細およびデモのご予約については、[F5 のウェブサイト](#)をご覧ください。

