elastic

Elasticを活用してデータセキュリティコンプライアンスを強化

エグゼクティブサマリー

サイバー攻撃がより頻繁に、標的を絞って、ステルス的になり、そして技術的に高度化するなど、サイバーセキュリティの脅威がますます複雑化する中、堅牢で包括的なデータセキュリティの必要性はかつてないほど重要になっています。サイバーセキュリティに関連する法的要件と潜在的な責任も同様に複雑で厳しいものになりつつあり、セキュリティに対するリスクベースのアプローチが不可欠となっています。

拡大を続けるセキュリティ関連の規制要件に対応し、ビジネスに深刻な影響を及ぼしかねない中断を防ぎ、セキュリティ侵害による高額な訴訟のリスクを回避するために、企業はサイバーセキュリティに対して包括的かつ戦略的なアプローチを採用する必要があります。これを怠ると、企業は重大な法的および財務的影響を受けるだけでなく、業務上および評判上の回復不能な損害を招くおそれがあります。

このホワイトペーパーでは、組織がElasticを活用してセキュリティ上の義務を果たし、サイバー脅威に対する真のレジリエントな防御を構築する方法を探ります。Elasticの強力で柔軟かつ拡張性のあるソリューションは、企業が多様で多面的なコンプライアンスおよび運用上のサイバーセキュリティニーズ要件に対応することを支援します。主な内容は次のとおりです。

- 攻撃対象領域全体でのデータの可視性と検索性の向上
- コンプライアンス対応に向けたデータ抽出の簡素化
- 脅威を解決するための検出と自動化の効率化
- セキュリティ態勢の監視と実証
- 強化された脅威インテリジェンス

以下では、各法的フレームワークに共通する基本的なセキュリティ概念の概要を説明し、これらの概念をリスクベースかつコンプライアンスに準拠した形で実装しなかった場合に起こりうる結果を検証するとともに、Elasticのプラットフォームとソリューションを利用して、コンプライアンス義務を果たし、セキュリティリスクを軽減する方法を説明します。

注意：*このホワイトペーパーは情報提供のみを目的としており、法的助言を構成するものではありません。法的助言については、ご自身の法律顧問にご相談ください。*

基礎的なセキュリティ原則と関連するコンプライアンス義務

現代のセキュリティコンプライアンスの状況は、管轄区域固有、業界固有、およびデータ固有の要件が入り組んだ状況となっています。そのため、組織の責任は、その組織が所在する場所、ビジネスを行う場所、処理するデータの種類と方法（そのデータの機密性やビジネスの性質を含む）によって異なります。

たとえば、グローバルな金融機関は、米国連邦のGramm-Leach-Bliley Act（GLBA）、ニューヨーク州金融サービス局（NYDFS）のCybersecurity Regulation、EUのDigital Operations Resiliency Act（DORA）、EUのNetwork and Information Security Directive 2（NIS2 Directive）など、複数の法令の適用を同時に受ける可能性があります。

一方、上場している米国を拠点とする小売業者は、決済カードのセキュリティに関するPCI Data Security Standards（PCI-DSS）、財務報告システムのセキュリティに関するSarbanes-Oxley（SOX）の要件、米国各州の侵害通知法など、さまざまな要件が適用される場合があります。もちろん、個人情報の保護に関するプライバシー法と情報セキュリティ要件も忘れてはなりません。

これらの必須要件に加え、多くの企業は、ISO 27001、SOC 2、NIST CSF、またはUK Cyber Essentialsなどの様々な第三者セキュリティフレームワークに基づく任意の認証も取得しています。

これらの違いはあるものの、法令、規制、自主規制、および業界のフレームワーク、加えて一般的なセキュリティのベストプラクティスは、主にコアとなる一連のセキュリティ原則に収束しています。以下では、これらの原則の主要部分を確認するとともに、さまざまなフレームワークとどのように整合しているかの例をご紹介します。

データのインベントリ、マッピング、分類

組織は、リスクベースのセキュリティ制御をデプロイする前に、どのようなデータを保有しているか（データインベントリと呼ばれるプロセス）、データがどこにあるか（データマッピング）、およびそのデータの機密性（データ分類）を理解する必要があります。

これらのプロセスは、データ侵害インシデントが発生した場合にも重要であり、企業が影響を受けたデータが法令、規制、または契約上の侵害通知義務を引き起こすかどうかを適切に判断するために役立ちます。これらの理由から、データインベントリ、マッピング、および分類は、複数のフレームワークに準拠するために明示的に必要とされるか、必要な前提条件となっています。以下に例を示します。

- *FTC Safeguards Rule*（16 CFR § 314）は、GLBAの対象となる特定の金融機関に対する要件を実装するもので、対象となる金融機関に対し、リスク評価プロセスの一環として顧客情報の機密性を特定し評価することを要求しています。
- HIPAA *Security Rule*（45 CFR § 164.308）も同様に、対象となる事業体に対して、電子的に保護された医療情報（ePHI）を保管し、保護することを義務付けています。
- EUの一般データ保護規則（GDPR）の第30条の下では、組織は処理活動の記録を保持する義務があり、コンプライアンスを実証するためにデータインベントリとマッピングを事実上義務付けています。
- 米国各州の侵害通知義務は、通常、その州の居住者に関連する特定の種類の機密個人データが侵害された場合にのみ発生します。したがって、データ侵害が発生した場合、企業は侵害されたデータセットに含まれるデータの種類を特定できる必要があります。
- NIST SP 800-53やCIS Controlsのようなフレームワークは、データの機密性に合わせた保護を確実にするために、データの分類を重視しています。明確なインベントリと分類スキームを確立することで、企業はより自信を持ってアクセス制御を実装し、機密データの流れを監視し、規制上の義務を満たし、不正漏洩のリスクを軽減できます。

ロールベースのアクセス制御

ロールベースのアクセス制御（RBAC）は、個人が職務を遂行するために必要なシステムとデータにのみアクセスできるように設計された対策です（この概念は「最小権限」とも呼ばれます）。一貫して適用されるRBACは、悪意のある内部者による不正アクセスのリスクを低減し、侵入の範囲を制限するのに役立ちます。多くの法的および業界フレームワークでは、次の通り、RBACが明示的に要求または強く推奨されています。

- EU GDPRの下では、正当な権限を持ち、知る必要のある者のみが個人データにアクセスできます。さらに進んで、この規制では、不正アクセスをデータ侵害の事例として定義しています。
- マサチューセッツ州のStandards for the Protection of Personal Information（201 CMR 17.04）は、マサチューセッツ州でビジネスを行う企業に対し、機密性の高い個人情報を含む記録やファイルへのアクセスを、職務を遂行するために必要な人に限定する安全なアクセス制御対策を導入することを義務付けています。
- HIPAA Security Ruleでは、ePHIへのアクセスを正当な理由がある人に限定することが義務付けられています。
- EUのDORA第9条4項では、対象となる金融機関に対し、資産への物理的または論理的なアクセスを、合法的かつ承認された機能および活動に必要なものに限定するポリシーを実装するよう求めています。
- NIST SP 800-53、ISO/IEC 27001、CIS Controls（CIS Control 6など）のような業界標準も、基礎となるアクセス管理の実践としてRBACを重視しています。

ロギングと監視

セキュリティイベントログは、企業がセキュリティインシデントを検出するために必要な最も重要なリソースの1つです。アクセス日時、実行されたアクション、およびそれらのアクションを実行したユーザーなどの情報を含むログは、システムアクセスが許可されたものであるかを確認し、潜在的な不正アクセスを調査するために不可欠です。リアルタイムまたはほぼリアルタイムでログを監視することも、脅威をタイムリーに検出して対処するうえで重要です。

しかし、複雑で多様なシステムを持ち、毎日大量のログを生成する組織にとって、ログ管理は大きな課題となる場合があります。そのような組織は、ログを効果的に集約し、異常なアクティビティを監視するために技術的なソリューションに頼る必要があります。法的および業界のフレームワークは、次のようにログ取得および監視の重要性を強調しています。

- 決済カード業界データセキュリティ基準（PCI-DSS）は、決済カードデータを格納、送信、処理するすべての企業に対し、システムコンポーネントおよびカード保有者データへのアクセスをすべてロギングし、監視することを義務付けています。
- HIPAA Security Ruleでは、ePHIを含むシステム内の活動を記録および検証するための監査コントロールの実施を義務付けています。
- SOX法404条は、経営陣と監査人に対して、財務報告に対する上場企業の内部統制の有効性を評価して報告することを義務付けています。そのような監査人は、COBITなどのフレームワークに対してそれらの制御を評価します。これらのフレームワークは、ユーザーアクティビティの監査ログ、財務システムへのアクセス、および財務データの変更を必要とします。
- NIST CSFの「Detect」コンポーネントは、企業がセキュリティイベントをログに記録し、継続的なセキュリティ監視を維持することを規定しており、これはEU GDPR第32条、EU NIS2第23条、EU DORA第19条などで通知対象のインシデントをタイムリーに報告するうえでも不可欠です。

侵入検知と対応

残念なことに、今日の脅威の状況では、あらゆる組織がサイバー攻撃の潜在的な標的となります。組織は、侵入の試みが発生することを前提に、セキュリティインシデントに対応するための侵入検出システムとプロセスを保守する必要があります。このようなシステムは、攻撃が重大なインシデントに発展する前に、企業が迅速に特定し、対応するために重要です。しかし、侵入検知システムやインシデントレスポンスプロセスは、そのままでは十分な効果を発揮するものではありません。企業は活動のベースラインを確立し、企業固有の特性に応じてアラート基準を調整する必要があります。このような調整により、アラートの精度が向上し、インシデントの重要度に応じて適切にトリアージされ、対処されるようになります。侵入検出と対応は、多くの法的および業界のフレームワークにおいて中心的な役割を果たしています。

- 米国の連邦、州、および国際的な侵害通知法では、データ侵害を特定の期間内に報告する必要があります。GDPRが報告のための最も短い時間期限（報告対象となるデータ侵害が発生したと判断されてから72時間以内）を課していると思われがちですが、DORAは主要な情報通信技術（ICT）関連のインシデントを発見から4時間以内に報告を求めている点にも留意する必要があります。
- NYDFS Cybersecurity Regulationのセクション500.16では、規制対象団体に対して、サイバーセキュリティインシデントに迅速に対応し、復旧するためのインシデントレスポンス計画を立てることを義務付けています。
- DORAはまた、規制対象の金融機関に詳細なインシデントレスポンス計画の策定を義務付けています。
- NIST CSFでは、企業がセキュリティインシデントを検知し対応するために、詳細な「Detect（検知）」および「Respond（対応）」のコントロールを維持することを規定しています。

不遵守のコスト

コンプライアンスに沿った効果的なセキュリティ制御を実装しない場合、企業、その経営陣、および取締役会が重大な法的、財務的、および評判上のリスクにさらされる可能性があります。実務的な観点からすると、効果的な監視ツールやプロセスを備えていない組織は、長期間にわたる不正アクセスのリスクにさらされます。これにより、攻撃者は企業の偵察を行い、正規の活動をより正確に模倣し、データを漏洩させたり、ランサムウェア攻撃の基盤を築いたりする可能性があります。ログが不完全な場合、疑わしいまたは予期しないアクティビティが許可されたものかどうかを判断できなくなる可能性があり、これは過剰通知と通知不足の両方を引き起こす可能性があります。

データ侵害やサイバーセキュリティインシデントが発生した場合、データのマッピングやインベントリが不十分だと、影響を受けたデータの特定が困難になる可能性があります。その結果、影響を受けた関係者や規制当局への通知が遅れる可能性があります。このような遅延は、被害者が被る可能性のある損害を増大させ、規制当局に対する報告期限違反にもつながり、回復や是正の負担に加え、追加の損害賠償請求、規制当局からの制裁、さらなる法執行や訴訟コストを増大させる結果となります。企業間取引の事業者にとっては、インシデントの影響を受けた顧客を特定することも難しくなります。

個人情報を保護するためのプライバシー法などで課される積極的なセキュリティ要件を遵守しない場合、重大な罰則、罰金、その他の法的責任が生じる可能性があります。また、すべての企業は、情報漏洩の原告から過失、契約違反、またはその他の訴訟（多くの場合、集団訴訟）のリスクにも直面しています。特に、カリフォルニア州消費者プライバシー法（CCPA）は、企業が「合理的な」セキュリティ対策を維持しなかったことにより機密データが侵害された場合、原告が個人訴訟を起こす権利を認めています。HIPAA、CCPA、EU GDPRなどの規制に基づく制裁や損害賠償は、すぐに7桁規模に達することもあります。

直接的なコンプライアンス違反による制裁に加え、セキュリティの不備による評判へのダメージも深刻になる可能性があります。データ侵害を受けたり、セキュリティ規制に違反した企業は、顧客の信頼を失い、世間から批判を受け、事業に大きな混乱をきたし、ブランド価値に長期的な影響を与える可能性があります。上場企業は、セキュリティ上の失敗が広く報道されることで、株価への影響を受けるリスクも抱えています。リスクには、顧客の解約や、顧客データを適切に保護できなかったことに対する補償要求が含まれ、ビジネスと収益の損失につながります。これらの重大な影響を踏まえて、企業はコンプライアンス義務に適切に投資し、セキュリティリスクを軽減することで、セキュリティに真剣に取り組む必要があります。

コンプライアンスのためのElastic活用

Elasticsearch Platformは、Elasticのすぐに使える2つのソリューションであるElastic ObservabilityとElastic Securityの基盤となっています。組織はElasticのオープンで柔軟なプラットフォームを活用することで、コンプライアンス義務を果たし、複数のチャネルにまたがる主要なサイバーセキュリティリスクに対処することができます。最も重要なのは、Elasticのソリューションが本質的にアジャイルで拡張性があることです。これらは幅広いシステムやプラットフォームに導入してデータを収集できるだけでなく、その検索機能は無数のユースケースに活用できます。以下に、Elasticがセキュリティプログラムの主要原則をサポートするために活用できる例をいくつか示します。

データマッピングと分類

Elasticは、環境全体で構造化データと非構造化データをインデキシングすることで、組織がデータの種類や所在を一元的に把握できるようにし、データマッピングの取り組みをサポートします。Elasticは、カスタムタグ、メタデータ、機械学習を使用してデータ（個人データ、財務記録、システムログなど）のパターンを識別し、機密性や規制上の義務に基づいてデータを簡単に分類できるようにします。Elasticは専用のデータ分類エンジンではありませんが、その強力な検索と分析機能を活用して、クラウドとオンプレミスシステム全体でデータを追跡およびインベントリ管理するためのより広範なデータガバナンスプログラムに統合できます。

ロールベースのアクセス制御（RBAC）

ElasticはRBACツールではありませんが、このプラットフォームは組織のシステム全体のログを取り込み、権限管理のギャップを特定するのに役立ちます。組織は、アクセスパターンを分析して、ユーザーグループがアクセスする必要のあるシステム、またはアクセスする必要のないシステムを特定し、アクセス権限の割り当てに役立てることができます。Elasticはまた、お客様がシステム全体からグループアクセスポリシーを取り込むのを支援し、そのデータからレポートを作成して、監査やコンプライアンス調査においてアクセス権の行使を証明することを可能にします。そして、Elasticでは、Elastic SecurityとKibanaインターフェースにRBAC機能が組み込まれています。管理者は、特定のインデックス、ダッシュボード、またはアクション（表示と編集など）へのユーザーアクセスを制限するロールを定義し、最小権限の原則をサポートすることができます。

ロギングと監視

Elasticのコアな強みの1つであり、最も一般的なユースケースは、ログを大規模に集約、格納、分析することです。Elastic Agentを使用することで、企業はエンドポイント、サーバー、クラウドサービス、アプリケーションからログを取り込むことができます。これらのログはElasticsearchでインデックス化され、Kibanaでリアルタイムの分析と可視化が可能になります。Elasticは、ログの長期保持、アラート、異常検知をサポートしており、理想的なログ集約およびセキュリティ監視ソリューションであるだけでなく、効果的なコンプライアンス報告ツールでもあります。そのオブザーバビリティスイートでは、インフラを全体的に可視化するためのアプリケーションパフォーマンス監視（APM）、メトリック、稼働状況の監視も提供します。

米国連邦政府機関のM-21-31のような多くの規制では、一定期間のログを格納することが義務付けられています。Elasticのデータ階層構造により、アクセス頻度や使用頻度に応じてデータをコスト効率よく格納することができます。Elasticsearch logsdbインデックスモード**はログデータのストレージ使用量を最大65%削減しつつ**、可視性とコンプライアンスを向上させるとともに、すべてのデータを即座に分析可能な状態で維持します。

一例を挙げると、ヨーク大学は、サイバーセキュリティ機能の強化、業務効率の向上、コストの削減を目的として、セキュリティ情報およびイベント管理（SIEM）システムをElastic Securityに移行しました。サーバー、デスクトップ、ノートPCに約9,000のElastic Agentを導入し、Google Cloud、AWS、Azure、オンプレミスサーバーを含む大学のハイブリッドクラウドインフラストラクチャー全体からログを収集することで、大学は1日あたり500ギガバイトのデータを取り込み、35テラバイトのログをストレージに取り込みます。また、Palo Alto Networksのファイアウォール、Cloudflare、Duoなどのセキュリティツールと接続して、さまざまなプラットフォームを包括的に監視できます。この設定により、膨大な量のデータをすばやく検索でき、クエリ時間を数時間から数秒に短縮できます。

侵入検知と対応

Elastic Securityには、エンドポイント検知と対応（EDR）機能が含まれ、侵入検知をサポートする脅威インテリジェンスフィードが統合されています。これにより、セキュリティチームは、行動分析、攻撃マッピング、カスタム検出ルールを使用して、既知および未知の脅威を監視できます。一元化されたロギングにより、アナリストはシステム間でイベントを迅速に相関付け、アラートをコンテキスト内で調査し、対応ワークフローを管理することができます。Elasticは、サードパーティのセキュリティオーケストレーション、自動化、対応（SOAR）プラットフォームとの統合を通じて自動化された対応もサポートしており、インシデントレスポンスの準備や脅威ハンティングを改善するための強力なツールとなっています。これらの高度な機能により、侵害の可能性を低減し、侵入された場合でも対応時間を短縮することで、インシデントに伴う法的責任のリスクを軽減できます。

デジタルプラットフォームおよびトランスフォーメーションの主要プロバイダーであるAHEADは、マネージドセキュリティサービスにElastic Securityを統合することで、侵入検知および対応能力を大幅に強化しました。現在、AHEADはクライアントのセキュリティデータをElastic Cloud上で稼働するElasticに取り込み、データを強化・集約し、脅威インテリジェンスフィードと連携させています。Elasticは組織のSOARシステムのデータソースとしても活用されています。AHEADのセキュリティアナリストは、セキュリティイベント内の関連情報をハイライトするAIを活用したアラームを利用でき、大量のデータを手作業で選別する時間を短縮し、誤検知の負担を軽減することにも貢献しています。

まとめ

サイバーセキュリティの脅威の状況が、組織に対してますます高度な課題をもたらし続ける中、拡大し続けるセキュリティおよびデータプライバシー関連の規制要件に準拠し、リスクを低減することも、より複雑になっています。これを怠ると、企業は重大な法的および財務的影響を受けるだけでなく、業務上および評判上の損害を招くおそれがあります。Elasticは、CIOやCISOが、特にデータマッピングと分類、RBAC、ロギングと監視、侵入検知と対応の分野において、これらの様々な法的要件へのコンプライアンスを強化するのを支援できます。

