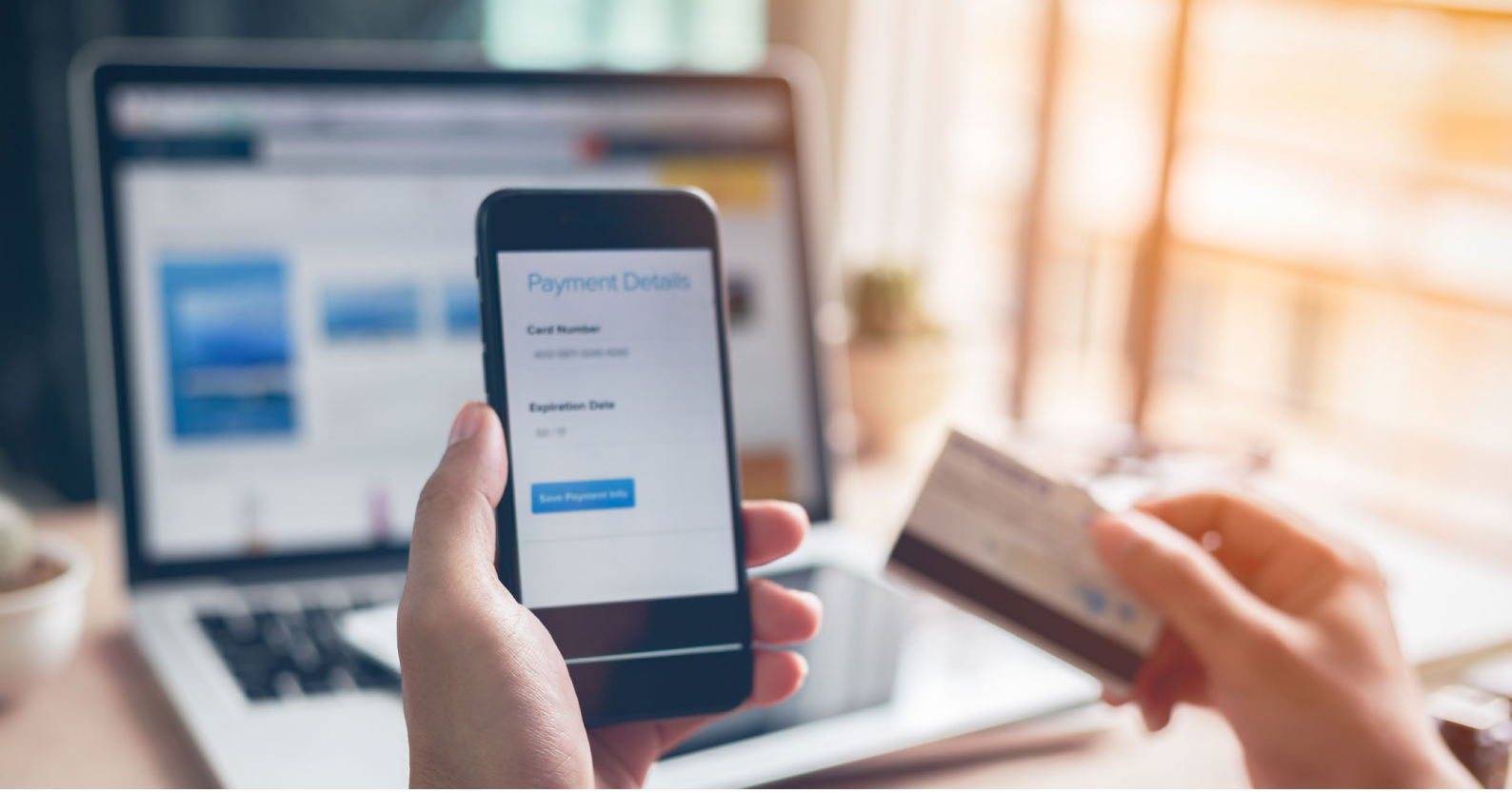
PCI DSSコンプライアンスとその後：企業リスクの評価と軽減

APACのセキュリティリーダー向けガイド

verizon business



アジア太平洋地域（APAC）は、主にキャッシュレス決済と即時決済の急増により、2030年[1]までに1兆ドル規模のデジタル経済圏になると予測されています。最高経営責任者（CEO）、最高財務責任者（CFO）、最高情報セキュリティ責任者（CISO）は、データ漏洩/侵害の報告義務化と世界的かつ普遍的なPCI DSS（Payment Card Industry Data Security Standard）v4.0の実施が間近に迫っていることの影響について依然として不安を抱いています。

不透明な情勢の中、ベライゾンのアドバイザリーサービスは、企業がこうしたコンプライアンス上の課題に対処するためのサポートを行っています[2]。

サイバー攻撃の3分の1以上がAPACで発生しており、世界で最も頻繁に狙われる地域となっているため、セキュリティリーダーの役割は重要性を増しています。

金融サービスは2番目に攻撃が多い業種であり、10件の攻撃のうち9件は日本が標的とされています[3]。

PCI DSS v4.0では、64の新しい要件[4]という技術的なハードルだけでなく、データ漏洩/侵害やゼロトラストの進展に関するより高い透明性とセキュリティを求める大企業の株主の期待にも応えなくてはなりません。

オーストラリアでは、組織のデータを効果的に保護できなかった場合にCEOが直面する罰則がかつてないほど厳しくなっており、Australian Information Commissioner（OAIC）は、2023年末にはデータ漏洩/侵害の届け出が確実に増加すると指摘しています[5]。

最近、シンガポールのオンライン小売プラットフォーム[6]で重大なデータ漏洩/侵害が発生し、276万人の顧客のクレジットカード情報が漏洩し、不正な取引や金銭的損失が発生しました。

その後、同社は評判の失墜と規制当局による制裁金の可能性に直面し、デジタル決済エコシステムにおけるデータセキュリティの重要性を強調することになりました。

この情報漏洩は、PCI DSS v4.0標準（合計12の中核的なデータセキュリティ要件）に照らし合わせると、小売企業のサイバーセキュリティアプローチにおける4つの具体的なギャップを浮き彫りにしました。

1. 要件3（アカウントデータの保護）：保存された決済データの適切な暗号化またはマスキングの不備。
2. 要件7（カード会員データへのアクセスの制限）：アクセス制御対策が不十分なため、機密情報への不正アクセスが可能。
3. 要件9（カード会員データへの物理的アクセス）：カード会員データが処理または保存される物理的なシステムおよび環境のセキュリ ティの不備により、不正な物理的アクセスが発生する可能性。
4. 要件11（セキュリティテスト）：セキュリティシステムとプロセスの定期的なテストが不十分なため、侵害やさらなる脆弱性にさらされる可能性。

このデータ侵害の例はコンプライアンスにおける具体的なギャップを示していますが、より重大な課題は、時間の経過とともに動的に進化するコンプライアンスとリスク管理に対して、統一された効率的なアプローチを構築することです。

多くの企業は、加盟店、サードパーティ、顧客全体でカード会員データを保護するために設計された標準の要件を満たすために、少ないリソースで試行錯誤を繰り返しながら運営しています。

1 https://www.cnbc.com/2023/11/29/southeast-asia-may-be-on-the-cusp-of-a-cashless-payments-revolution.html

2 https://www.ptsecurity.com/ww-en/analytics/asia-cybersecurity-threatscape-2022-2023/

3 https://www.verizon.com/business/resources/reports/verizon-vision-for-banks-enterprise-intelligence-anz.pdf

4 https://listings.pcisecuritystandards.org/documents/PCI-DSS-v3-2-1-to-v4-0-Summary-of-Changes-r1.pdf

5 https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-july-to-december-2023

6 https://www.pdpc.gov.sg/all-commissions-decisions/2023/03/breach-of-the-protection-obligation-by-eatigo-international

さらに、関係者の同意が不十分であったり、プログラムの目的が不明確であったり、プログラムの複雑さが過小評価されていたりすると、セキュリティ標準に準拠し、体系的に先行し続けることがさらに困難になる可能性があります。

決済データを継続的に保護するには、PCI DSS v4.0の変更を実装しながら既存のセキュリティ制御を維持する必要があります。

年間100億ドル以上の収益を上げている世界中の大企業の半数以上が、過去2年間に被害にあっています。さらに衝撃的なことは、これらの企業の約5分の1が、5000万ドル以上の損害を被っています[7]。

今日、情報開示とコンプライアンスを最重要課題にしなければ、デジタルの不確実性が非常に高まっている時期に会社を機能不全に陥れる危険性があります。

しかし、コンプライアンスに焦点を絞った行動計画を採用することで、企業はセキュリティプログラムの設計においてセキュリティを強化することができます。

ギャップを好機に変える

米国の例を通して、APACにおけるコンプライアンスのギャップと好機に焦点を当ててみます。

APACにおける国外の取引の約17%は米国からのもので、デジタル商取引のグローバルな性質と、国境を越えた安全な取引を確保するために、PCI DSS v4.0などの国際セキュリティ標準に準拠することの重要性が浮き彫りになっています[8]。

米国のほとんどの組織はPCI DSS v4.0の導入に1年以上の準備期間があったにもかかわらず、多くの企業は依然として不安を抱えており、米国証券取引委員会（SEC）の新しいサイバー開示規則では、企業はサイバーインシデントが重大であると判断してから4日以内にSECに報告することが求められています[9]。

同様の規制の傾向がAPAC全体に波及しており、持続可能な管理環境を維持する、透明性の高い組織を構築することの重要性と緊急性が指摘されています。

決済データの適切かつ継続的な保護を確保するために、継続的な改善も必要です。

コンプライアンスを達成するためのロードマップを構築し、それを維持することは、多くの米国およびAPACの企業にとって大きな課題です。

PCI準拠へのギャップを特定している段階であっても、すでにこれらのギャップを認識して解決策を模索している段階であっても、現在のコンプライアンス状況を徹底的に評価する必要がある場合でも、あるいは革新的なツールとプロセスを活用して決済のセキュリティを強化したいと考えている場合でも、次のステップに進むべき時が来ています。

7 https://www.pymnts.com/news/b2b-payments/2023/incoming-payments-fraud-costs-companies-millions-every-year/#:~:text=Fraud%20is%20both%20costly%20and,costs%20more%20than%20%2450%20million.

8 https://www.enterprisetimes.co.uk/2021/10/28/digital-payments-in-europe-to-grow-by-70-says-new-ppro-research/

9 https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2023/july/SEC-Adopts-New-Cyber-Disclosure-Rules/

コンプライアンスの複雑さを解消

この複雑な枠組の中で重要な部分は事前評価です。

ベライゾンは、組織が優れている部分、標準的な部分、または後れを取っている部分のそれぞれのバランスをとるお手伝いをします。

この事前評価は、模擬試験アプローチを活用して、PCI評価を徹底的に準備する機会を提供します。

多くのCEOは、この事前評価で自社のセキュリティの弱点を知る良い機会が得られます。

しかし、これはセキュリティの変革の第一歩であり、ばらばらな活動から正式なプログラムの作成へと移行する第一歩なのです。

コンプライアンスの成功を推進する原則

過去20年間、絶えず変化し発展する環境の中で、ベライゾンは、次の4つの基本原則に基づいて、PCIコンプライアンスと予測可能なパフォーマンスへのアプローチを開発し、継続的に改善してきました。

- 無駄をなくす
- 生産性の低さに対処する
- コスト高を防ぐ
- 関係者の不満を予防する

多くの企業は、PCIセキュリティ チェックを全体的なガバナンスプランとは別のものとして扱っています。これらのチェックを組み合わせることで、アクティビティが効率化され、異なるプログラムでどのように同じタスクが2度実行されるのを防ぐことができるかを理解する必要があります。

年1回は見直す

さまざまなPCI DSS規則と規制を1つの包括的なガバナンス戦略の下で調整することにより、PCI DSSコンプライアンスを強化し、リスクを効果的に管理できるようになります。

企業は毎年ガバナンス戦略を見直し、目標、要件、制限事項を確認する必要があります。これにより、物事がスムーズかつ効率的に進むようになります。

認定セキュリティ評価機関（QSA）のチームは、企業や公共機関が次のような障害を克服できるようサポートすることを目的としています。

- 縦割りの組織の継続（コミュニケーション、パフォーマンス、持続可能性の妨げとなる）
- テクノロジーへの偏重およびプロセスや手順の軽視
- 忘れる、投資不足、性急など不十分な組織能力開発
- 不十分な研修と教育の取り組み

統一されたアプローチにより、決済システムを最新化し、攻撃者に対する強力な防御の提供を目的とした長期的なセキュリティプログラムへとプロジェクトを進化させられます。

APACにおけるコンプライアンスに準拠したサイバーシールドの構築

定期的なチェックと安全のための明確で共通の計画は、毎年発行されるベライゾンのデータ漏洩/侵害調査報告書（DBIR）で注目されているサイバー攻撃から企業を守るのに役立ちます。

ソーシャルエンジニアリング

APACでは、セキュリティ侵害の93%がソーシャルエンジニアリング、システムへのハッキング、重要なWebアプリケーションの脆弱性の悪用などに起因しています[10]。

これらの脅威に対抗するために、PCI DSS v4.0では、ネットワークセキュリティの強化、決済情報の保護、データアクセスの厳格な規制、定期的なセキュリティ評価の実施など、厳しいルールが義務付けられています[11]。

金銭目的

昨年のDBIRでは、金銭目的でこれらの侵害の61%が引き起こしていることが指摘されており、クレジットカード詐欺から決済データを保護する必要性が強調されています。PCI DSSは、インターネット経由で送信される決済データの暗号化を義務付け、データの安全な保管を確保することで、この問題に対処します[12]。

人的要因

侵害には、社内データ、企業秘密、認証情報などの機密情報の窃取を伴うことが多く、データ暗号化、安全なデータ保存、堅牢な認証メカニズムの実装など、PCI DSSの求める要件の必要性が浮き彫りになっています。

2024年のDBIRデータセット内の侵害の92%は外部の攻撃者による組織化されたものであり、PCI DSSで設定されているような、強力な外部防御の必要性が強調されています。

しかし、同じデータセットにおける侵害の9%は内部攻撃者によるものであり、内部の脅威を軽減するためにアクセス制限やアクティビティ監視などの内部管理を重視するPCI DSSの姿勢を裏付けています。

強力なパスワードポリシーの実装や各ユーザに固有のIDを割り当てるなどのPCI DSSガイドラインを採用すると、企業は重要な決済情報を不正アクセスからより効果的に保護し、より安全なデジタルペイメント環境を確保することができます。

10 https://www.verizon.com/business/resources/T42/reports/2023-data-breach-investigations-report-dbir.pdf

11 https://listings.pcisecuritystandards.org/documents/PCI-DSS-v3-2-1-to-v4-0-Summary-of-Changes-r1.pdf

12 https://www.verizon.com/business/resources/T42/reports/2023-data-breach-investigations-report-dbir.pdf

業界のコンプライアンス

DBIRでは、金融、保険、小売、宿泊、医療などの業種を含む世界中のデータが含まれていますが、これらの調査結果は、APACに貴重なインサイトを提供します。

これらの業種のデータ漏洩/侵害の傾向を調べることで、APACの企業は自社の市場内で同様の傾向と脆弱性を予測することができます。

ただし、これらのインサイトをAPAC各国の独自規制、文化、経済情勢を深く理解した上で適応させることが重要です。

このアプローチは、PCI DSSなどのグローバルコンプライアンス標準を満たすだけでなく、地域固有のリスクと改善の機会にも対応する包括的なセキュリティビジョンを可能にします。

医療および社会福祉業

概要：医療および社会福祉業は依然としてサイバー攻撃の主な標的となっています。2023年のDBIRでは、「システム侵入」、「基本Webアプリケーション攻撃」、「多種多様なエラー」が主な原因で、525件のインシデントと436件のデータ漏洩/侵害が確認されています[13]。これらの脅威は、医療におけるサイバーセキュリティの強化が急務であることを浮き彫りにしています。

主要な問題：「ランサムウェア」は引き続きこの業種を悩ませているとともに、患者データを危険にさらす誤送信などの内部エラーもそれに拍車をかけています。

PCI DSS v4.0による保護：[14]

- 要件5.1：最新のウイルス対策 – ランサムウェア攻撃の初期段階であることが多いマルウェアをブロックするために重要です。

- 要件9.4：物理的なアクセス制御 – 機密エリアへのアクセスを制限すると、外部からの侵入と内部の大きな脅威である偶発的なデータ漏洩/侵害の両方を防ぐことができます。

コンプライアンスは免責を保証するものではありませんが、医療情報システムと機密性の高い患者データを保護するための強力な防御フレームワークを提供します。

製造業

概要：製造業はリスクの高い業種であり、2023 年のDBIRでは1,817件のインシデントと262件のデータ漏洩/侵害が報告されています。「システム侵入」、「ソーシャルエンジニアリング」、「基本Webアプリケーション攻撃」の脆弱性が重大な脅威となっています[15]。

主要な問題：金銭とスパイ活動が目的の攻撃者は、ハッキング、マルウェア、ソーシャルエンジニアリングを悪用して、脆弱な製造システムを標的にします。

13 https://www.verizon.com/business/resources/T73c/reports/2023-data-breach-investigations-report-dbir.pdf

14 https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf

15 https://www.verizon.com/business/resources/T73c/reports/2023-data-breach-investigations-report-dbir.pdf

PCI DSS v4.0 保護：

- 要件4.1：安全なデータ転送 - ネットワーク転送中に機密データを暗号化することで攻撃のリスクを軽減します。
- 要件12.6：セキュリティ意識向上プログラム - 従業員が、主要な攻撃手法であるソーシャルエンジニアリングを識別して回避できるようにサポートします。

要件対応は一度きりの修正ではありません。PCI DSS v4.0に合わせて進化することで、最新の脅威に対する耐性が強化され、製造データを保護するのに役立ちます。

金融および保険業

概要：2023年のDBIRでは、主に「基本Webアプリケーション攻撃」による1,832件のインシデントと480件のデータ漏洩/侵害により、この業種の脆弱性が強調されています。これは、堅牢な脆弱性管理とパッチ適用が極めて重要であることを示唆しています[16]。

主要な問題：「基本Webアプリケーション攻撃」は依然として大きな脅威であり、金融データや保険データが潜在的に危険にさらされています。

PCI DSS v4.0による保護：

- 要件6.4：ベンダー提供のセキュリティパッチの適用 – ベンダーからのセキュリティパッチで、すべてのシステムコンポーネントとソフトウェアを最新の状態に確保することにより、攻撃のリスクが軽減します。

巧妙化する脅威に対処し、機密性の高い金融データを保護するためには、定期的なパッチ適用が依然として不可欠です。

小売業

概要：小売業は依然として脆弱であり、2023年のDBIRでは、主に「システム侵入」、「ソーシャルエンジニアリング」、「基本Webアプリケーション攻撃」による406件のインシデントと193件のデータ漏洩/侵害が確認されています。これは、特に決済カード情報に関して、安全なデータ保存と保護の重要性を浮き彫りにしています[17]。

PCI DSS v4.0による保護：

- 要件3.2：必要な認証データのみを保存 – 必須の認証データのみの保存を義務付けることで、攻撃対象領域を最小限に抑えます。

機密性の高い財務情報を保護するために、データ保存作業を定期的に確認し、最小限に抑えましょう。

宿泊および飲食業

概要：この業種では、254件のインシデントが報告され、68 件のデータ漏洩/侵害が確認されました。決済取引に大きく依存しているため、「システム侵入」、「基本Webアプリケーション攻撃」、「ソーシャルエンジニアリング」に起因する侵害の90%で使用されているマルウェアの「RAMスクレーパー」による重大なリスクに直面しています[18]。

主要な問題：決済カードのデータを標的とする「RAMスクレーパー」の蔓延により、高度なマルウェア対策戦略の必要性が注目されています。

PCI DSS v4.0による保護：

- 要件5.4：悪意のあるソフトウェアからシステムを保護 –「RAMスクレーパー」攻撃を効果的に検出し、防御するためにマルウェア対策ソリューションの導入と定期的な更新を義務付けています。

巧妙化する脅威に対する有効性を確保するために、マルウェア対策を定期的に更新およびレビューしましょう。

その他の業種

前述のインサイトはほんの一部に過ぎません。

2024年のDBIRは、これまで説明した業種を引き続き対象としています。また、教育サービス、鉱業、公務など、さらに多くの業種を対象としています。

読者の皆様には、これらのセクションを確認して知識を深め、特定の状況に適用できる業種横断的なパターンやソリューションを見出すことをお勧めします。

クラウド全体のコンプライアンス

カード会員データの処理、保存、送信をクラウドサービスに移行すると、PCI DSSコンプライアンスの達成に新たな複雑さが生じます。

複数のクライアント間でリソースを共有する場合、カード会員データの保護に関してクラウドサービスプロバイダー（CSP）とクライアントの両方の責任を明確に定義することが重要です。

たとえば、PCI DSS要件12.8では、組織がカード会員データにアクセスできるサービスプロバイダーのリストと、そのデータの保護に対するプロバイダーの責任の所在を明記した書面による契約を締結、維持することが義務付けられています。

Cloud Controls MatrixをPCI DSS[19]にマッピングすると、クラウドセキュリティ対策が決済データ保護基準に合致し、クラウドベースの決済システムのセキュリティ体制が強化され、業界の規制への準拠が確保されます。

Cloud Controls Matrix（CCM）は、ベライゾンがメンバーとなっているCloud Security Alliance（CSA）[20]によって開発されたサイバーセキュリティフレームワークです。このメンバーシップは、クラウドサービス内のセキュリティを促進し、クラウドセキュリティのベストプラクティスの開発に貢献するというベライゾンの取り組みに沿ったものです。

ベライゾンのクラウドセキュリティへのアプローチには、CCMとPCI DSSの詳細なマッピングが含まれ、共通の責任を強調し、包括的な保護戦略を確実にします。

ベライゾンのクラウドサービスは、PCI DSS要件を統合し、暗号化、アクセス制御、継続的な監視に重点を置いて、クラウドプラットフォーム内のカード会員データに強力なセキュリティを提供します。

16 https://www.verizon.com/business/resources/T73c/reports/2023-data-breach-investigations-report-dbir.pdf

17 https://www.verizon.com/business/resources/T73c/reports/2023-data-breach-investigations-report-dbir.pdf

18 https://www.verizon.com/business/resources/T73c/reports/2023-data-breach-investigations-report-dbir.pdf

19 https://cloudsecurityalliance.org/blog/2023/09/19/strengthening-cloud-security-mapping-the-cloud-controls-matrix-ccm-4-0-to-pci-dss-4-0

20 https://www.verizon.com/business/resources/solutionsbriefs/2020/security-risk-assessment.pdf

重要なベンチマーク

私たちは業界標準に準拠することは規制上の要件であり、戦略上の必要性も理解しています。

オーストラリアおよびその他の9か所のセキュリティオペレーションセンター（SOC）の稼働を含む、世界的な事業展開により、ベライゾンは50万台を超えるセキュリティおよびネットワークデバイスを管理し、国際的および地域的なサイバーセキュリティ標準に関する重要なインサイトと、潜在的な脅威に対処するために必要な情報およびサービスを提供しています。

ベライゾンのGovernance, Risk & Compliance（GRC）アドバイザリーサービスは、次の重要なベンチマークに基づいてセキュリティプログラムを測定し、向上させるのに役立ちます。

- ISO27001/ISO27002：これらの規格は、堅牢な情報セキュリティ管理システムの基盤形成、PCI DSSコンプライアンス強化、カード会員データの潜在的侵害からの保護にとって極めて重要です。
- アメリカ国立標準技術研究所（NIST）のフレームワーク：NISTテクノロジーサイバーセキュリティフレームワークと特別刊行物800-53によって提供される包括的なガイドラインは、コンプライアンスにとどまらず、リスク管理とセキュリティ制御に重点を置いてサイバー脅威に対する防御を強化し、PCI DSSの目標をサポートします。

APACのコンプライアンス：

APACでは、地域の規制や標準によりPCI DSSコンプライアンスに追加のレイヤーが導入され、次のような特有の課題が生じています。

- 豪州通信情報局のEssential 8：これらの戦略を実行すると、セキュリティ体制が強固になり、蔓延するサイバー脅威に対する防御が強化されることで、間接的にPCI DSSコンプライアンスが促進されます。
- オーストラリアおよびニュージーランドの2018年プライバシー法および情報セキュリティ登録評価者プログラム認定：これらのフレームワークは、データ保護への深い取り組みを意味し、PCI DSSの基本原則と一致し、機密情報のセキュリティを強化します。

ベライゾンは、Certified Information Systems Security ProfessionalやCertified Information Security Management Consultantなどの認定資格を保有することにより、こうした世界および地域の標準に対する深い理解を体現しています。この専門知識と、19,000件を超えるセキュリティ評価を実施した豊富な経験を併せ持つベライゾンは、コンプライアンスの達成と維持においてお客様をサポートする独自の立場を確立しています。

設計によるコンプライアンス

PCI DSS v4.0では、継続的な評価や検証方法の改善など、大幅な更新が行われています。

10回目のリリースでは、組織を固定ルールから柔軟で目標指向の戦略を可能にする方向へと移行させます。

苦情に関する規制の変化の規模とペースも、最高情報セキュリティ責任者（CISO）と社内IT部門に大きなプレッシャーをかけています。

私たちが数年前に決済セキュリティレポートを実施したところ、すべてのコンプライアンス基準を満たしていた企業はわずか43% でした[21]。

特に、境界をクラウドやIoT環境にまで広げる場合、近道をとったり、コンプライアンス違反に陥る恐れのある盲点を無視したりしないようにするのは、当然ながら難しいことです。

したがって、サイバーセキュリティのあらゆる側面を社内で管理するのはもはや意味のないことです。パートナーとの連携により、CISOは、通常では見つけて維持するのが非常に難しいオンデマンドの能力でコアチームを強化できます。

また、ベライゾンのアドバイザリーサービスが、さまざまなセキュリティ対策とその設定がどのように相互作用するかを理解しながら、見落とされている領域を明らかにするため、CEOや取締役会には安心していただけるのです。

これは、Fortune 500企業や多国籍企業を含む、あらゆる規模の企業におけるベライゾンの評価の重要な目標です。

結局のところ、データセキュリティとコンプライアンスの成功は運ではなく、設計によって達成されるということをセキュリティリーダーは決して忘れてはいけないのです。

21 https://www.verizon.com/business/reports/payment-security-report/2022/the-state-of-pci-dss-compliance/