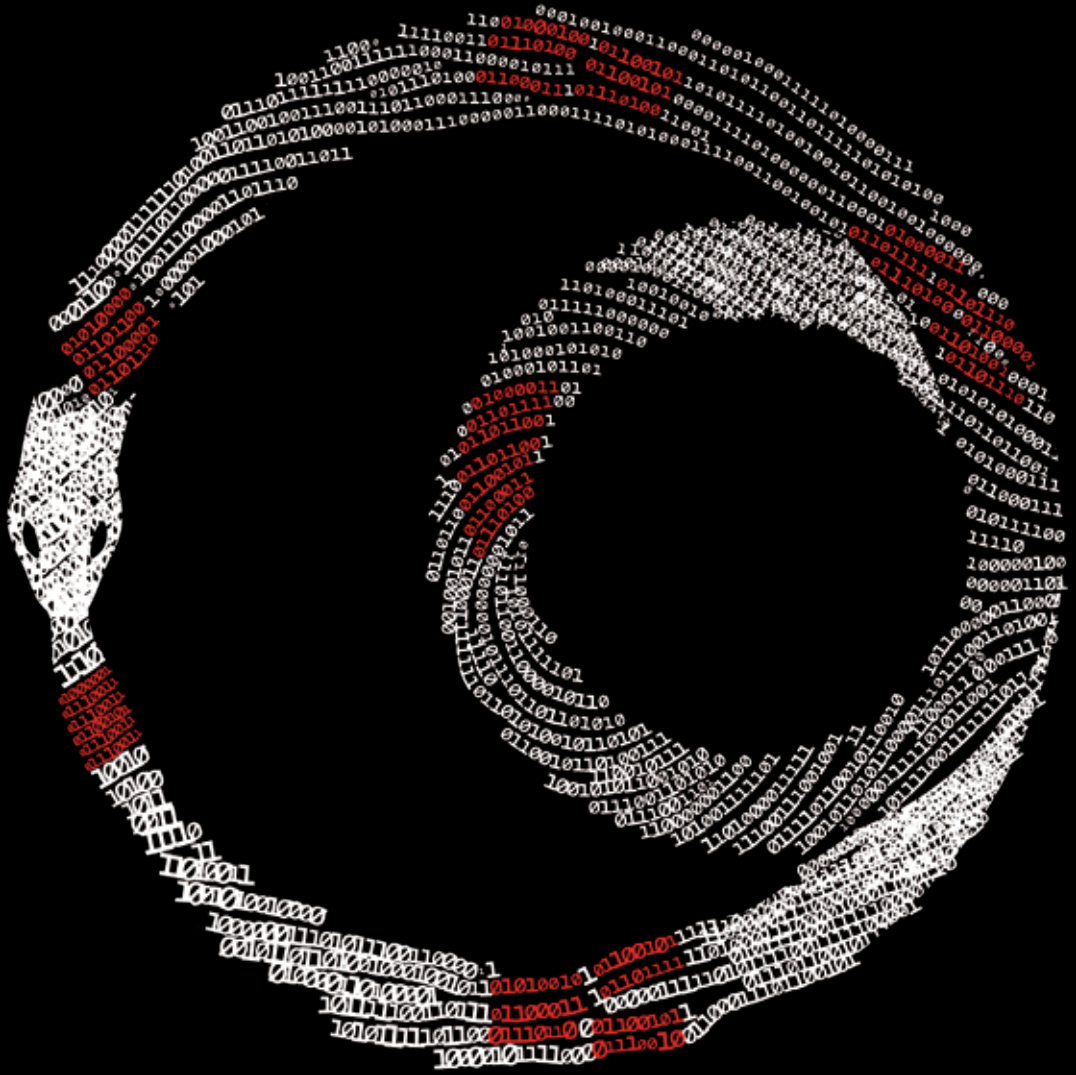
インシデントへの準備と対応についての報告書

エグゼクティブサマリー

データ侵害の脅威への対処



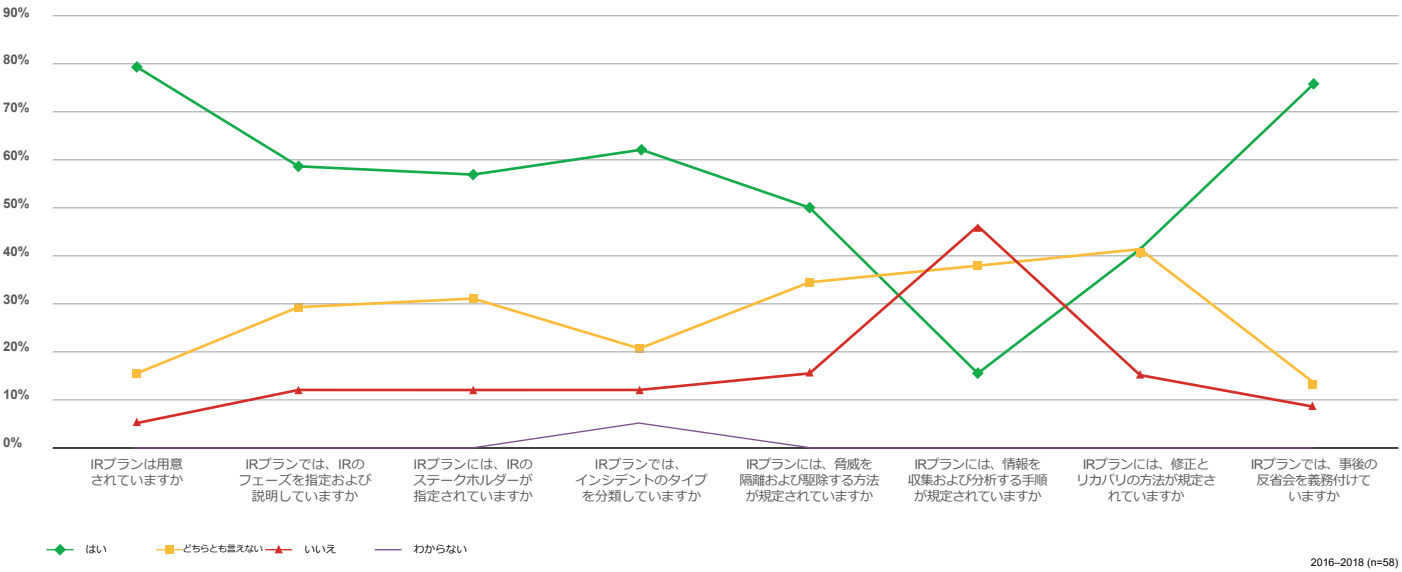
verizon

危機管理室

データ侵害やサイバーセキュリティインシデントの発生に備えて準備をすることや、これらの問題に対処することは容易ではありません。自社の環境や個々の脅威の特性を知っていなければならず、役割を十分に果たせるチームワークも必要です。そして、それらと同じくらい重要ものにIR(Incident Response:インシデント対応)プランがあります。

まさにそのようなIRプランの重要性ゆえに、ベライゾンでは、Verizon Incident Preparedness and Responseレポート（VIPRレポート：インシデントに備える準備とインシデント対応についてのレポート）を発行しています。このレポートでは、インシデントに備える準備とインシデント対応に、データとシナリオをもとに取り組んでおり、そのベースとなっているのは、2016年から2018年の3年間に行った各種IRプランの評価と、その評価に基づくアドバイスです。

プランの評価
フェーズ1〜6：IRプランの要素の選択



2016–2018 (n=58)

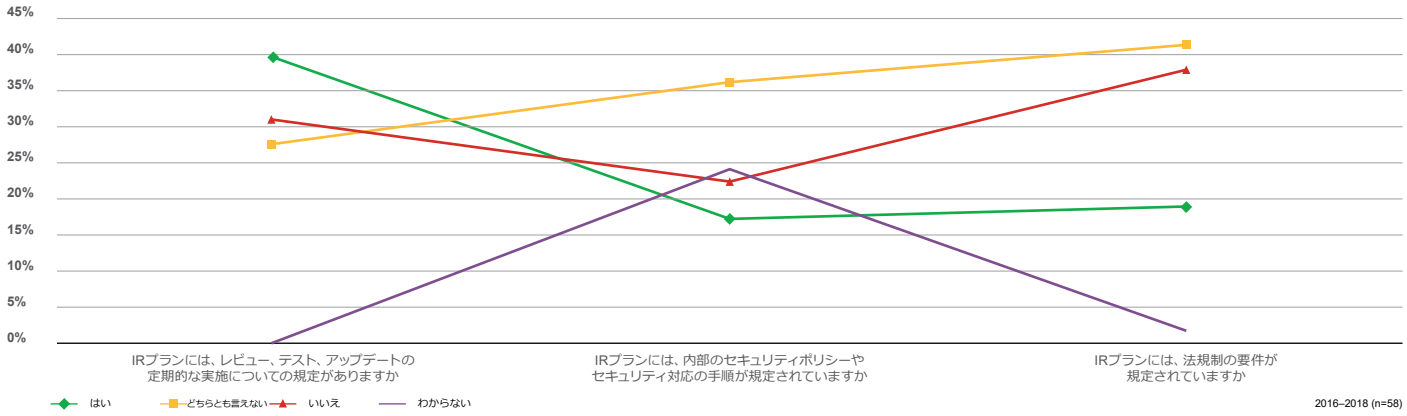
本レポート「データ侵害の脅威への対処」では、お客様がご自身のサイバーセキュリティ/インシデント対応の活動を計画、改善するうえで役立つ手法を、さまざまなIRステークホルダーの視点に立って考察します。

このレポートでは、侵害シミュレーションキットを使用して5つのデータ侵害シナリオを扱っており、これらを通じて、IRプランの特定のフェーズで必要となる事柄とその基盤となる要素を説明しています。お客様ご自身のIRプランと関連するIRプレイブックを作成、アップデートするためのフレームワークとしてご活用ください。また、これらのシナリオは、データ侵害のシミュレーションワークショップや机上訓練を円滑に行うためのコンテンツの作成にご利用いただけます。

プランニングと準備

サイバーセキュリティインシデントの対応において、その実効性を上げるためには、プランニングと準備が欠かせません。このフェーズでは、内部のIRステークホルダーや戦術担当者のほか、サービスプロバイダーや監査人、外部のコンサルタントなどの第三者も関係者に含めたIRプランの作成を扱います。

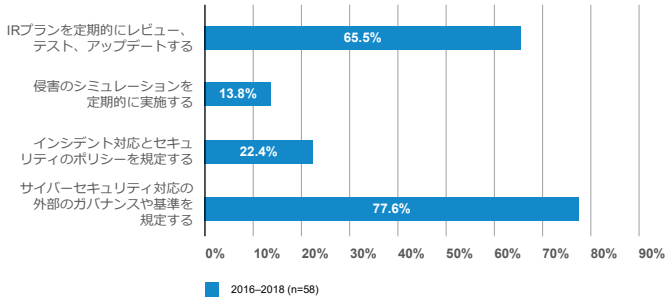
プランの評価
フェーズ1：プランの妥当性



評価の所見

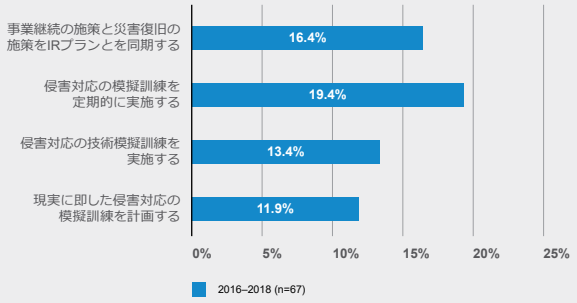
2016年から2018年に評価を行ったIRプランのうち、プランのレビュー、テスト、アップデートの定期的な実施について明確に規定しているものはわずか40%にとどまり、一方、31%では、そのような規定がありませんでした。また、調査対象となったIRプランの22%が内部のセキュリティポリシーやセキュリティの手順を定めておらず（30%は部分的に規定）、38%がサイバーセキュリティやインシデント対応、データ侵害の報告に関する法規制の要件を定めていませんでした（41%は部分的に規定）。

評価に基づくアドバイス



GLBA、ISO 27001などの外部のガバナンスや基準を規定する（78%）ことや、IRプランを定期的にレビュー、テスト、アップデートする（66%）ことが、最優先の推奨事項でした。

シミュレーション関連のアドバイス



2016～2018年の期間に行った調査に基づくシミュレーション関連のアドバイスでは、その上位に、侵害対応の模擬訓練の実施（20%）や侵害対応の技術模擬訓練の実施（13%）がありました。

検知と検証

実効性の高いインシデント対応を実現するには、IRプロセスの早い段階でサイバーセキュリティインシデントを検知、分類することが求められます。

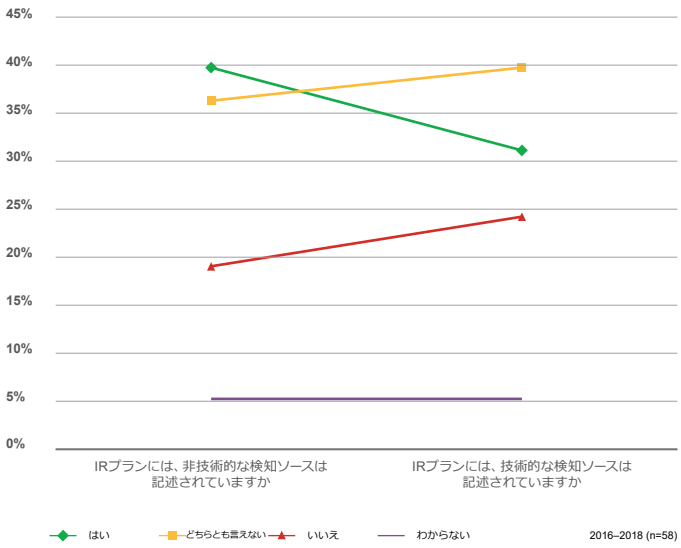
評価の所見

評価の対象となったIRプランの40%が、インシデントを検知するためのソースとして非技術的なソースについて十分に触れており、36%が部分的な記述をしていました。一方、検知ソースとして技術的なソースについて十分な記述を行っていたIRプランは31%にとどまり、部分的な記述をしていたIRプランは40%ありました。

評価に基づくアドバイス

技術的、非技術的なインシデント検知ソースを記述する

プランの評価
フェーズ2：検知のソース



隔離と駆除

このステージは、損害を最小限に抑えるためにサイバーセキュリティ上の脅威を隔離することと、新たな被害の発生を防ぐために脅威を駆除することに重点を置いています。

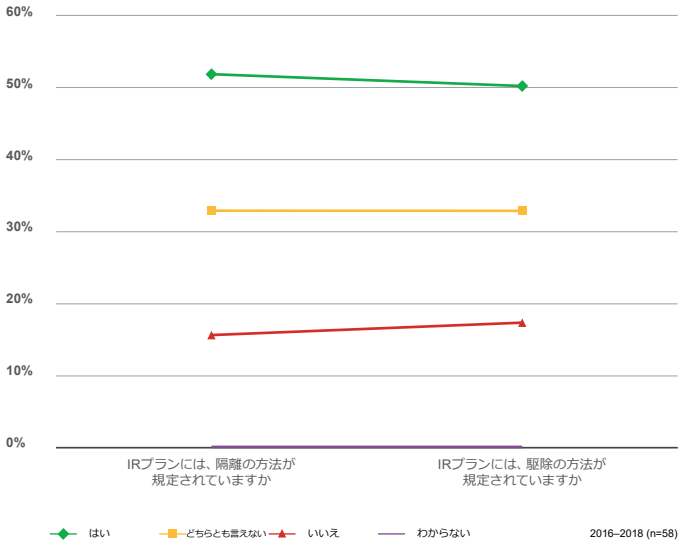
評価の所見

隔離と駆除の面でのIRプランの評価では、52%が隔離の方法を十分に規定しており、50%が駆除の方法に十分に触れていました。その他33%は部分的に隔離の手順を規定しており、別の33%は部分的に駆除の手順を定めています。

評価に基づくアドバイス

隔離と駆除の手順を整備する

プランの評価
フェーズ3：隔離と駆除



情報の収集と分析

エビデンス(証拠)の収集と分析では、隔離、駆除、修正、リカバリで十分な効果を上げられるよう、サイバーセキュリティインシデントの内容を詳しく調査します。

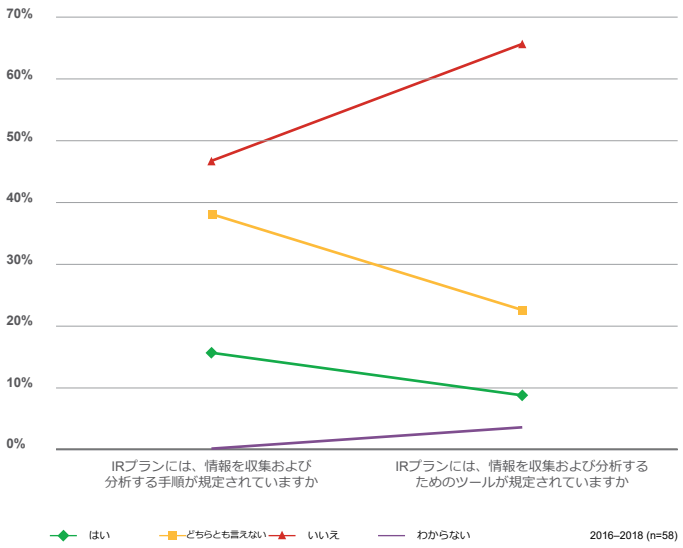
評価の所見

エビデンスの収集とデータの分析については、それらの手順を十分に記述しているのは、調査対象となったIRプランの16%にとどまり、38%が部分的な記述を行っていました。一方、データ収集や分析のツールについては、わずか9%しか、それらについて十分に記述しておらず、部分的に記述しているIRプランは22%ありました。

評価に基づくアドバイス

エビデンスの収集とデータの分析に関してツールと手順を規定する

プランの評価
フェーズ4：情報の収集と分析



修正とリカバリ

このステージでは、達成すべきことが2つあります。1つは、インシデントの発生時に明らかになった脆弱性を修正して問題の再発防止と将来のリスクを減らすことであり、もう1つは、運用を通常の状態に戻すリカバリを実施することです。

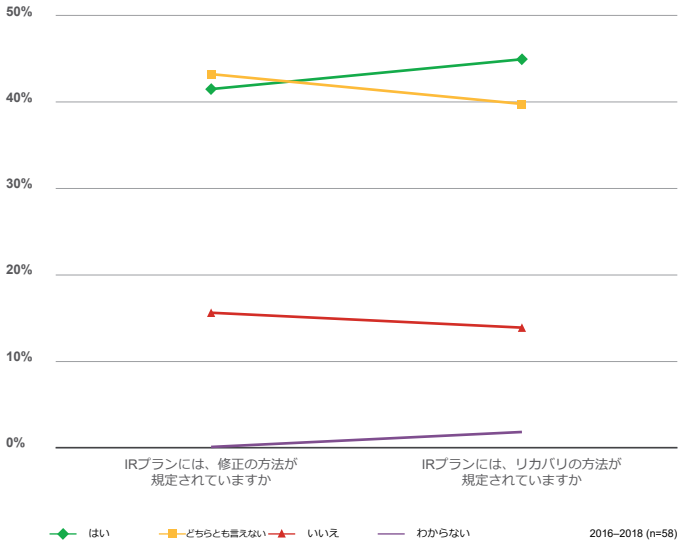
評価の所見

修正とリカバリの面でのIRプランの評価では、修正の方法を十分に記述しているIRプランは41%にとどまり（43%は部分的に記述）、45%がリカバリの方法に十分に触れていました（40%は部分的に言及）。

評価に基づくアドバイス

修正とリカバリの手順を整備する

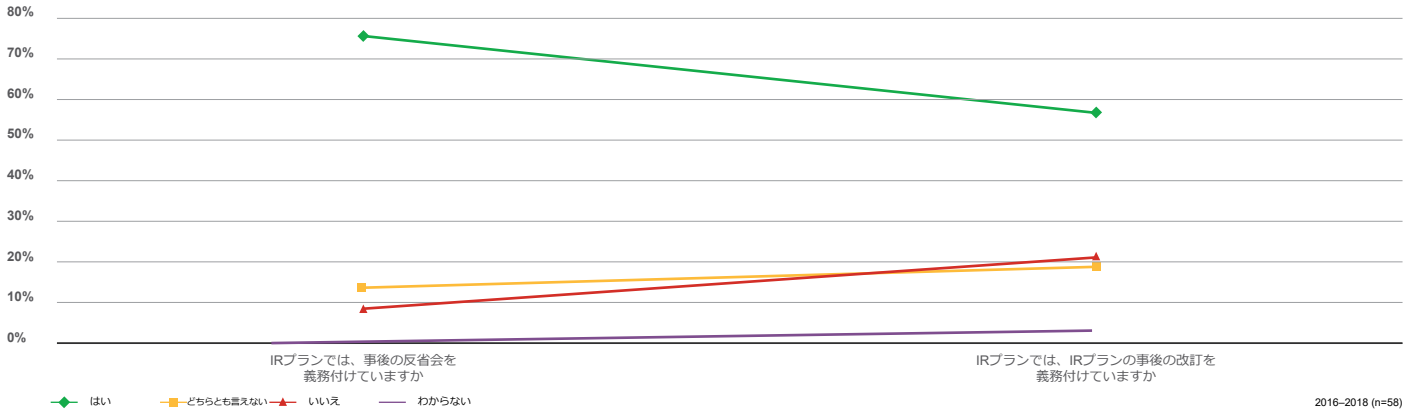
プランの評価
フェーズ5：修正とリカバリ



評価と修正

IRプロセスの最終ステージではIR活動を評価して、組織的な弱点や不備を特定し、サイバーセキュリティについての管理や手法を強化します。

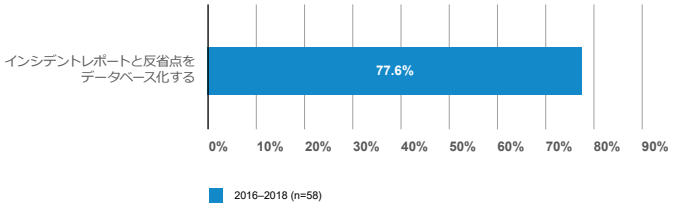
プランの評価
フェーズ6：反省会



評価の所見

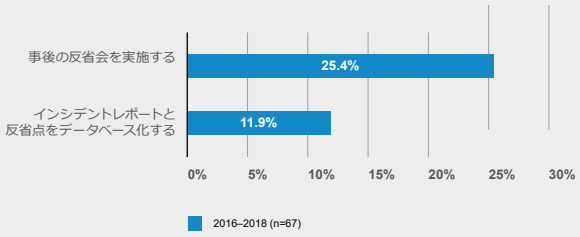
評価対象となったIRプランのうち、76%が事後の反省会を十分に義務付けており、14%が部分的な義務付けを行っていました。一方、IRプランの60%が、反省会に基づくIRプランの事後の改訂を完全に義務付けており、19%が部分的な義務付けを行っていました。

評価に基づくアドバイス



事後の反省会に関するアドバイスでは、反省点のデータベース化が78%を占めました。

シミュレーション関連のアドバイス



このフェーズのアドバイスでは、最も大きな割合を占めたのが事後の反省会の実施（25%）であり、インシデントレポートと反省点のデータベース化（12%）がこれに続きます。

重要ポイント

2019 VIPRレポート全体に十分時間をかけて目を通されることをお勧めします。このレポートにはさまざまな洞察やデータ、IRプランのベストプラクティスが多数記載されています。しかしここでは敢えて、重点事項を要約してみましょう。侵害対応の能力を十分に高め、充実した内容のIRプランを作成するための重要ポイント上位20をご紹介いたします。

フェーズ	重要なポイント
1 – プランニングと準備	1. 論理的で実効性の高いIRプランを策定する 2. 特定のインシデントを対象としたIRプレイブックを作成する 3. IRプランを定期的にレビュー、テスト、改訂する 4. サイバーセキュリティ/インシデント対応の外部/内部のガバナンスや基準を規定する 5. 内部のIRステークホルダーの役割と責任を明確化する 6. IRサイバーセキュリティの脅威の現状を定期的に検討することを内部のIRステークホルダーに義務付ける 7. サイバーセキュリティの戦術担当者のトレーニングを実施し、担当者のスキルを維持する 8. サードパーティのサイバーセキュリティサービスとそのコンタクトの手順を定期的に評価する
2 – 検知と検証	9. サイバーセキュリティのイベントをインシデントとともに明確化する 10. インシデントをタイプや重大度に応じて分類する 11. 技術的、非技術的なインシデント検知ソースを記述する 12. インシデントとイベントの追跡メカニズムを規定する 13. エスカレーションと通知の手順を規定する
3 – 隔離	14. 隔離と駆除の手順を整備する
4 – 情報の収集と分析	15. エビデンスの収集とデータの分析に関してツールと手順を規定する 16. エビデンスの処理と提示の手順を規定する
5 – 修正とリカバリ	17. 修正とリカバリの手順を整備する
6 – 評価と修正	18. 事後の反省会を実施し、フィードバックをIRプランに反映する 19. データとドキュメントの保存に関するポリシーを策定する 20. インシデントの指標とインシデント対応の指標を追跡する

インシデントへの準備と対応についての報告書
エグゼクティブサマリー

データ侵害とサイバーセキュリティに関する参考資料
https://enterprise.verizon.com/resources/

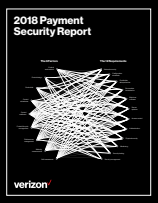
2019 Incident Preparedness and Response Report: Taming the data beast breach（2019年版 - インシデントへの準備と対応についての報告書：データ侵害の脅威への対処）

2019 Data Breach Investigations Report（2019年版 - データ侵害調査報告書）

2019 Insider Threat Report: Out of sight should never be out of mind（2019年版 - 内部脅威に関する報告書：見えない脅威を見逃さない）

2019 Mobile Security Index: It's time to tackle mobile security（2019年版 - モバイルセキュリティインデックス：今こそモバイルのセキュリティに取り組む）

2018 Data Breach Digest (18 x Scenarios)（2018年版 - データ漏洩/侵害ダイジェスト（18のシナリオ））



2018 Payment Security Report（2018年版 - 決済システムのセキュリティに関するレポート）

2019 CISO's Guide to Cloud Security: What to know and what to ask before you buy（2019年版 - CISO向けクラウドセキュリティガイド：導入前に知っておくべきこと、確認すべきこと）

5 Considerations for Evaluating a Modern Enterprise Security Platform（最新のエンタープライズセキュリティプラットフォームを評価するうえで考慮すべき5つのポイント）

Verizon Incident Preparedness and Responseレポート（VIPRレポート：インシデントに備える準備とインシデント対応についてのレポート）は以下のURLからダウンロードいただけます。
enterprise.verizon.com/resources/reports/vipr/

verizon