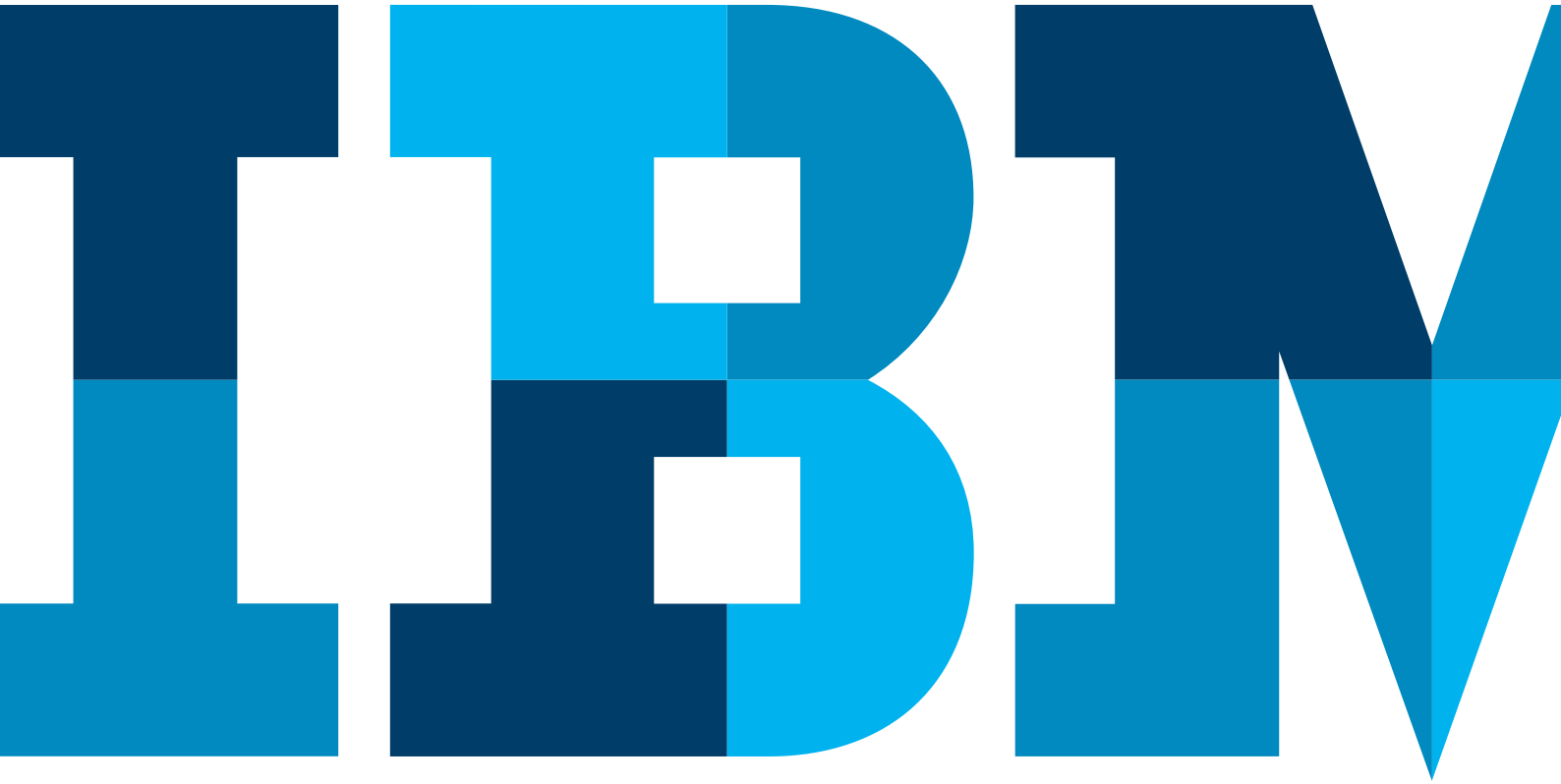
IBM Security
ホワイト・ペーパー

強固なインシデント対応能力を築くための 6 つのステップ

インシデント対応の課題



IBM

目次

はじめに:今はインシデント対応の時代

世界中の組織が、サイバー攻撃の予防と検知の対策だけではサイバー・セキュリティーの脅威から身を守ることができないと気付いています。IBM Resilient® はその声に応えるために開発され、インシデント対応 (IR) プロセスの管理、調整、合理化を実現するプラットフォームでセキュリティー・チームをしっかり支えます。

IBM Security は、あらゆる規模と産業の組織と連携する特権に恵まれてきました。これらの組織は、より高度で強固なインシデント対応能力を開発するために Resilient ソリューションを実装しているからです。これらの組織は、その場限りのものではなく、一貫性があり、再現/測定可能な IR プロセスを構築しており、コミュニケーション、調整、協働を組織全体の優先事項にしています。また、対応チームの仕事を迅速化し、正確性を上げるテクノロジーを利用しています。

しかし、より強固な IR プログラムを構築し、管理する課題があります。特に 3 つの課題が際立っています。

1. **サイバー・セキュリティー・インシデントの数が増えている**
   Enterprise Strategy Group によると、サイバー・セキュリティー専門スタッフの 42 パーセントが、セキュリティー・アラートの数が多すぎて対処しきれないので、自社組織ではかなりの数のアラートを無視していると回答しています[1]。
2. **セキュリティー・チームが人出不足に苦しんでいる**
   CyberSeek[2] によると、2016 年時点で業界全体で 20 万のサイバー・セキュリティーの仕事が埋まらないままです。
3. **組織が複雑すぎて、効果的な対応の準備が不足している**
   不十分な計画と準備、IT と業務プロセスの複雑さが、サイバー攻撃への対応の最たる障壁です[3]。

これらの課題を解決するため、多くの IBM Resilient のお客様は、人、プロセス、テクノロジーの調整を図ることで、IR アナリストがタスク担当者が誰なのか、どのタスクを終わらせる必要があるのか、タスクを完了させる方法を理解できるように支援しています。この新しいコンセプトは、インシデント対応編成として知られています。

インシデント対応編成によって、セキュリティー・アナリストは IR の対応とツールをすぐに利用できるようになります。彼らは重要なインシデント情報に瞬時にアクセスし、正確な決定を下し、決定を行動に移すことができます。自動化を利用して、自身とテクノロジーの生産性を高め、スキルのギャップとアラートの量を軽減しています。

しかし、IR 編成はプロセスであって、製品ではありません。人々の教育、実証済みのプロセス、統合テクノロジーという強固な基盤ブロックが必要です。編成はこれらの主要な要素の上に築かれ、組織の編成作業の効果は完全に、これらの基本的なピースの質にかかっています。

自社組織の IR 成熟度の確認

IBM Resilient のお客様は長年の間、さまざまな成熟度のレベルで IR に磨きをかけてきました。ほとんどの場合、成熟度のレベルは業界、利用可能なリソース、または経験により必要とされますが、IBM Resilient の大半のお客様は IR 能力を常に進化させてより高度な段階に押し上げようとしています。

これらのお客様の力を借りて、IBM Security の Resilient チームはインシデント対応成熟度モデルを開発しました。このモデルは、その場限りの不十分なインシデント対応能力から、十分に調整、統合され、継続的な改善と最適化に備えたインシデント対応能力までの進化を示します。

調整されたインシデント対応への工程は、人、プロセス、テクノロジーの開発から始まります。強固な IR 機能を構築するプロセスにおける主なステップを紹介すること、それがこのガイドの目的です。

成熟度		その場しのぎの対応		成熟		戦略的
既存の機能		必要に応じて	専門のパートタイム・スタッフ	フルタイム	SOC/IR+	融合
	人	• 0–1	• 1–3 • 専門スタッフ	• 2–5 • 正式な職務	• ~10 • シフト制 (24 時間 7 日間体制が可能)	• 15+ • インテル、SOC、および IR チーム
	プロセス	• まとまりがなく、個人が後手に回って対処 • ごく一般的な手順書 • 独学的な知識	• 状況に応じた手順書。ある程度まとまっている • メールベースのプロセス	• 標準的な業務プロセスとして要件とワークフローが文書化されている • 長期にわたってある程度改善されてきた	• プロセスを基準を基に測定 • 脅威に関する情報共有が最小限 • シフト制 • SLA	• プロセスは常に改善され、最適化されている • 脅威に関する情報を広く共有 • 追跡チーム
	テクノロジー		• SIEM • サンドボックス	• 継続的な監視 • エンドポイントの科学捜査 • 戦術的な情報	• マルウェア分析 • その他の情報 • IT 運用	• インテルと IR がセキュリティー・プログラムを推進 • 戦略的な情報 • 物理的セキュリティーと調整
CMM 相当		初期段階	再現可能	定義済み	マネージド	最適化

表 1: インシデント対応成熟度モデル

ステップ 1: 内部と外部双方の脅威を理解する

どの組織もそれぞれ独自の脅威の状況に直面しており、インシデント対応能力を築くための最初のステップは、その状況の詳細な理解を育むことです。

驚異の状況の一部は、組織が闘っているサイバー攻撃の性質で構成されています。その中には、組織が過去に対処してきた特定の脅威 (マルウェア感染やフィッシング攻撃など)、業界に広く影響することが知られている脅威 (医療機関へのランサムウェア攻撃、またはインターネット・インフラ企業への DDoS 攻撃など) が含まれるかもしれません。

さらに、しっかりした脅威モデルで、可能性のあるすべての関係者とインシデントを考慮する必要があります。たとえば、12 の医療機関を対象とした最近の調査によると、多くの医療機関が「不適切な脅威モデル」で四苦八苦し、「ほぼ患者の医療記録の保護だけ」に力を注いでいます。[4]この調査からは、医療機関のスタッフは IT 環境と潜在的な脅威について包括的な視点を育もうとせずに、米国の HIPAA 法のような規制ばかりを気にしてそれ以上のことを試みようとしないことが判明しました。また、患者の医療情報に直接影響しないもっと深刻な脅威、たとえば医療機器を狙うランサムウェアなどが組織の死角に潜んでいました。

組織が直面するかもしれない潜在的なサイバー・インシデントの範囲は広範におよび、それぞれに独自の IR プロセスを設けることが必要です。
手始めに、次のような問いを自問してみるといいでしょう。

- 過去にどのような種類の攻撃または悪影響を及ぼすインシデントが発生したか?
- 最近、マルウェア感染に対応したことがあるか?その場合、どのような種類のマルウェアか (ボットネット、データの窃盗、ランサム)?インシデントはどのくらい長く続き、どのように解決したか?
- 従業員の認証情報を窃取する目的のフィッシング・メール詐欺の被害を受けた従業員がいるか?その場合、被害を受けた従業員は誰か?
- 人気のあるオンライン・フォーラムまたは *ハクティビスト* のグループ、または他のオンライン・パーソナリティの批判の対象になったことはあるか?
- DoS 攻撃や他の形の意図的なオンライン妨害で具体的に狙われたことがあるか?

自社が直面している脅威を理解する中で、競合他社、ビジネス・パートナー、同業他社が経験した攻撃の種類について考えてみてください。同様の攻撃を見たことはありませんか?

プライバシー漏洩の対策

サイバー攻撃そのものが大きな被害をもたらしかねない一方、規制違反で罰金を受ける可能性もサイバー攻撃と同じかそれ以上の打撃になるかもしれません。自身の業界でデータ漏洩が発生したときにどのような規制が適用され、所有しているどのデータが対象になるのか、規制に確実に遵守するための最善策をセキュリティー・チームで評価することが必要不可欠です。以下の問いを自問してみましょう。

- プライバシー保護義務には、業界規制、州/連邦のデータ漏洩法、契約の合意を含めてどのようなものがあるか?
- プライバシー漏洩の通知はいつ行う必要があるか (ほとんどの場合、漏洩の規模、データが暗号化されていたかどうかといった要因などがあるが、ー地域や業界によって異なる)?
- 誰にどのような方法で通知する必要があるのか (顧客、検事当局など)?
- 通知の期限はいつか?

プライバシー保護はすでにセキュリティーおよびプライバシーを扱うプロフェッショナルにとって大きな問題となっていますが、2018 年 5 月に施行される EU の一般データ保護規則 (GDPR) の登場でますます大きくなるでしょう。

「GDPR はこの数十年で、プライバシーにおける最大の発展の1 つです。ほとんどの組織にとって、データ漏洩通知要件を満たすことはすでに大きな課題となっています。GDPR はそうした感情をさらに複雑化します」

— Ponemon Institute の会長および創設者、Larry Ponemon 博士

GDPR は劇的な変化を急速にもたらすグローバル規模のプライバシー法です。EU の民間人または組織とビジネスを行うどの組織にもグローバルに適用され、データ漏洩の通知期限を 72 時間に定め (米国の最新の法律よりもはるかに厳しい)、遵守しない場合は非常に大きな罰金が科せられる可能性があります (2 千万ユーロ、または組織の年間収益の 4 パーセント)。組織は今すぐ対策を講じて、GDPR 遵守に対応するための役割、責任分担、プロセスを決める必要があります。

組織の評価

また、脅威の状況は、影響を及ぼしかねない外部の要因とリスクだけでなく、内部の課題と短所も問題です。前述したように、サイバーセキュリティー・スキルの不足は、予測可能な将来のために私達の業界で対処する必要がある課題と捉えられます。また、組織は今日、これらの要因からどのような影響を受け、どのように対処するのかを評価する必要があります。

内部のスキル不足を特定するには、現在のスキル、自社が直面する外部の脅威と効果的に闘い、対処するために必要なスキルを評価します。個々のタスクの完了までに時間やワークロード・バランスなどのパフォーマンス基準は、現時点で持っているスキルとスキル不足の特定を明確に示してくれます。また、机上訓練や分析を使用することで、評価をさらに検証し、見落としたかもしれないその他のスキル不足を見つけることができます。

最後に、自社が直面している攻撃、注視が必要な規制、組織のスキル不足といった脅威の状況は、常に進化する評価の対象になります。サイバー犯罪史上、プライバシー保護規制、業界におけるその他の傾向が変化すれば、自社を取り巻く状況も変化します。必ず定期的に検証し、脅威の状況を適宜更新してください。

顧客事例:
上位 10 の欧州の銀行
ある IBM Resilient のお客様は独自の課題に直面していました。世界中に 3 つのセキュリティー・チームを配して、それぞれ独自のプロセスでインシデントに対応していました。そのため、貴重な脅威の情報がサイロ化され、中央管理と監視が欠け、IR プロセスをしっかりテストし改善する方法もありませんでした。

組織のセキュリティー・リーダーは、組織全体で IR 計画を標準化し、一元的なインシデント対応と監視を実現する必要があることを知っていました。

計画: セキュリティー・リーダー・チームは全グループに招集をかけて、特定のインシデント・タイプへの標準化した複合的な対応計画を共に策定して、3 つのグループの中で最も効果的で実証されたプロセスを組み入れました。また、3 グループで共通の単一インシデント対応プラットフォーム (IRP) を実装しました。

- 組織全体でインシデントを一元的に管理
- コンテキストの収集と協働を改善
- 対応の可視化を改善
- 新しい IR 計画、テスト、改善策を組織全体で確実に共有できるフィードバック・ループを作成

この新しい手法により、組織のセキュリティー・チームは組織全体の経験と情報から常に価値を得ることができます。

ステップ 2: 標準化、文書化した反復可能なインシデント対応計画を策定する

調査によると、不十分な計画と準備が依然として、今日のサイバー・レジリエンスへの最大の障壁となっています。ほとんどの組織で適切なインシデント対応計画が練られていないのも、驚くにはあたらないでしょう。Ponemon Institute が 2016 年に実施したサイバー・レジリエント組織調査によると、サイバー・セキュリティー・インシデント対応計画 (CSIRP) を準備し、組織全体で常に実施しているのはわずか 25 パーセントの組織でした。残りの 75 パーセントは、計画がまったくないか、対処療法的な内々のプロセスに従っているか、または組織全体で計画を実施していません。

その結果、多くの IR 機能がスローで非効率的、非効果的であり、被害を与えて高額な損失を生むサイバー攻撃の可能性が増し、従業員の不満と燃え尽き症候群が増え、セキュリティー・リーダーの仕事をリスクにさらすことになります。ただし、標準化、文書化され、反復可能な IR 計画を策定すれば、これらのリスクに対処し、チームはいつ何をどのようにすればいいのか正確に知ることができます。また、継続的な改善のプラットフォームとなり、組織は、絶えず進化するサイバー犯罪の脅威に先手を打つことができます。

課題: 適切な IR 計画の策定は時間がかかり、組織全体で専念する必要があります。最終的には、セキュリティー・リーダーがインシデント計画策定の優先順位を引き上げていく必要があります。インシデント対応計画ワークショップを実施すれば、チームの全関係者が集まって、整合性のある文書化、標準化した対応計画を作り上げることができます。

セキュリティー・チームは管理職、および重役とも協力し合って、リスクに関する彼らの理解を深め、他の関連部署リーダーにも協力が必要なことを知ってもらう必要があります。協力部署には、人事、法務、IT などの部署が含まれます。

ワークショップの間、あなたのチームは (セキュリティー・リーダーの指導下で) 協力し合いながら、特定のインシデント・シナリオを進めて、次のことを行います。

- インシデントの発生から最後に解決するまでに必要な特定のステップを詳細に作成する
- 役割と責任範囲を決める
- 対応中に利用する主なテクノロジーとコミュニケーション・チャンネルを特定する
- 許可と上申に関するプロセスを作る

NIST、SANS、CERT のようなリソースは、これらの協議と計画で役立つフレームワークとなりますが、最終的には、IR 計画を組織に合わせて具体化する必要があります。したがって、組織の全関係者が関与することが重要です。既存の IT チームとセキュリティー・チーム、組織内の主な利害関係者、管理職、法務およびコンプライアンス職の知識と経験を活用する必要があります。ビジネス・パートナーやサプライヤーのような外部関係者も協議に参加してもらうことができます。

これらの演習と協議の最後には、あなたのチームは、十分に考え抜かれ、文書化した反復可能な計画を策定しているはずです。これらの計画は一元化することができ、チームの全員が従い、長期的に絶えず改善できるものです。

顧客事例: フォーチュン 100 のテクノロジー企業

ある IBM Resilient のお客様は SOC に大きな技術的投資をし、人とプロセスも同様に発展させる必要がありました。彼らは、シミュレーションを使ってプロセスをテストし、SLA と経営幹部への報告を進化させる計画を立てました。

このお客様は、複雑でめったに起こらないイベントに特化した 3 か月ごとの定期的なシミュレーションを確立して、最も深刻な脅威にも無防備にならないよう万全を期しました。組織のサポートを得るために、セキュリティー・リーダーはインシデント対応 SLA を作成しました。これらの基準はインシデント・タイプと重大度別に分類され、インシデント対応チームが達成すべき標準となりました。さらに、これらの SLA により、CISO は重役会に業績を実証し、予算を得ることができました。今日、このお客様は相変わらず、毎日数百件のインシデントに遭遇していますが、十分に訓練を受けたチームで合理的かつ効果的に対処し、解決することができています。

ステップ 3: 先見的に IR プロセスをテストして改善する

サイバー犯罪者は絶えず新たな優位性を得ようと目論んでいます。サイバー・セキュリティー・チームは先を見越した対策を優先的に講じる必要があります。

IR の能力を前進させ続ける最も効果的な方法の 1 つは、シミュレーションを実行すること、特定の目的に特化した結果主導の方法で行うことです。

IR シミュレーションは、「不十分な計画と準備」の障壁に打ち勝つ有効な手段となります。シミュレーションにより、IR 能力全体 (人、プロセス、テクノロジー) で実世界のインシデントにしっかり対応しながら、将来の改善の機会も発見することができます。

セキュリティー・リーダーにとって鍵となるのは、シミュレーションを効果的に行うこと、チームが常に改善し団結するための特定の手順を用意することです。

セキュリティー・リーダーはまず、効果的なシミュレーションを実現するための計画を事前に立てる必要があります。よくあるインシデントの演習を行うのか、何か予期しないインシデントに備えるのかを決めます。両タイプとも調査する上で有効です。

セキュリティー・リーダーは、よく練った特定のシミュレーションも開発する必要があり、それらのシミュレーションには、アナリストが見つける必要がある重要な詳細を含めます。つまり、シミュレーションについてチームにじっくり考えさせ、チェック項目からなる単なる演習以上のものにします。

また、シミュレーションは測定可能なものにしてください。目標を設定し、完了までの時間や完成度など主要な基準を追跡します。シミュレーションを再現して、改善度 (または後退度) を測定します。

最後に、IR シミュレーションを組織全体で実施してください。人事、法務、マーケティングなどのグループからの参加者を含めて、本当にインシデントが発生したときに自分たちの役割を果たせるように備えさせます。同様に、シミュレーション後の分析結果を組織全体で共有してください。これにより、チームは常に率直になり、どのリソースがどこに必要なのかリーダーシップを学べるようになります。

ステップ 4: 脅威に関する情報を利用する

サイバー犯罪者は集団で動いており、ダーク・ウェブで協力し合い、情報を共有しています。セキュリティー専門スタッフは力を合わせて働くことも必要です。

Ponemon Institute は 2016 年のサイバー・レジリエント組織調査の一環として、業績の高い回答者 (サイバー・レジリエンスが前年向上した回答者) と平均的な組織を比較して、主な相違を特定しました。多くの所見の 1 つに、業績の高い組織は脅威共有プログラムに参加する確率が高いことがあります (平均的な組織が 53 パーセントだけなのに比べて 70 パーセントが参加)。

脅威情報 (TI) 業界は、近年さまざまな動きを見てきており、それにはもっともな理由があります。つまり、セキュリティー・チームは、自らの環境の動きについてより的確な知見と認識を求めているのです。

脅威情報の利用は、認識を高める上で大きな部分を占めます。しかし、それには課題もあります。セキュリティー・チームは、さまざまな質の無数のフィードを探り、真偽を見分ける問題にも対処する必要があることがほとんどです。

幸運にも、多くの IBM Resilient のお客様は長年にわたって、さまざまな脅威情報フィードを実装し、実験しています。これらのお客様の経験全体を基にした、TI を効果的に利用してインシデント対応を改善する 3 つの主な方法があります。

- **インシデント対応計画に脅威情報を根づかせる** 大手メディア・ネットワークのある IBM Resilient のお客様は、脅威情報データの調査の分析に時間がかかりすぎることを発見しました。自分たちに当てはまらない問題を追跡して、リソースを使いはたし、仕事の効率がひどく落ちてしまいました。

  この問題を解決するため、チームは脅威情報データを既存のインシデント対応プロセスに組み込みました。アナリストは IoC (攻撃の痕跡情報) をインシデントに格上げし、直面している状況に関連する場合に利用可能な情報を必要に応じて使って、潜在的な脅威に関する重要な情報をアクセスできます。これにより、時間管理とチームの効率が大きく向上しました。

- **統合と相関関係を利用して、脅威情報を実践的な情報に変える**
  脅威情報を SIEM ツールや EDR ツールなどの他のデータ・ソースと統合することで、アナリストはより完全なインシデントの前後関係情報を得ることができ、その情報はより実践的になります。前後関係、重大度、パターンを考慮することで、データの範囲を絞り込むことが可能です。その結果、アナリストは闘う対象と最善の対処方法について詳細を知ることができます。

- **ソースの有用性を追跡し、測定する**
  情報フィードは大量にあり、その種類は多岐に及びます。たとえば、オープンソース、閉鎖的なコミュニティー、商業ソースなどがあり、脅威情報プラットフォームがあります。個々のフィードがどのくらいの頻度で情報を提供し、提供される情報の質と重大度を記録しましょう。そうすれば、特定のフィードが冗長か、または何らかの方法で調整する必要があるかどうかをすぐに判断できるようになります。

以降のセクションでさらに詳しく見ていきますが、インシデント対応プラットフォーム (IRP) は、サイバー・インシデント調査と対応の手動作業の大部分を自動化できます。そのような改善方法の中でも、IRP はデータ分析と専用ロジックをアーチファクト可視化というアプローチで使用します。このアプローチでは、関連する IT 資産、使用された悪意のあるソフトウェア、通信した悪意のあるインフラストラクチャーなど、インシデント間の共通性に注目することで、一見してつながりのないインシデントがいかにつながるかを見ることができます。

インシデントを特定し、データ漏洩の各部を成す個々のアーチファクトを把握できれば、対応時間を数日や数週間から数時間に短縮できるでしょう。また、ユーザー・アクセス、データ・セキュリティー、通信などの領域に実用的な制御を実装して、今後インシデントが起こらないように防止することも可能になります。

「81 パーセントの回答者が、情報共有によって組織のセキュリティー体制が改善し、75 パーセントがインシデント対応計画の効果が向上したと答えています」

— The 2016 Cyber Resilient Organization、The Ponemon Institute

ステップ 5 インシデントの調査と対応を合理化する

「Verizon Data Breach Investigation Report」にあるように、Verizon が審査した全インシデントの 1/4 未満が検出までに「数日以内」、大半が数日、数週間、または数カ月かかりました。[5]. サイバー・インシデントが数週間あるいは数カ月も気付かれずにいるまま、悪意のある犯罪者には、侵入したネットワークに足掛かりを築くチャンスがあり、その足掛かりを排除するのは困難な場合があります。

理由の 1 つは、ほとんどの組織が、従業員へのフィッシング攻撃のようなわかりやすいサイバー・インシデントの調査にも対処療法的なプロセスに依存していることがあります。また、スキル不足のため、適切なツールとテクノロジーを持つ組織は、大量のインシデントに効率的に対処するリソース不足に悩むことがあります。

組織が、統合されたデータと脅威情報ソースを IR プロセスに追加すれば、下位のタスクの自動化からスタートして、高度な方法で対応を調整できる機会が拡大します。

自動化は、単調な繰り返し作業を合理化し、チームの迅速化とスマート化を実現する便利な手法です。幅広いインシデント対応調整手法で使用した場合 (調整については次のセクションを参照)、自動化によってチームは戦略的な意思決定者へと成長することができます。

マルウェアが発生した場合など、あるエンドポイントで検出された疑わしいサンプルを自動的に掴んで、エンドポイント・エージェントまたは次世代脅威検知プラットフォームに送り、観察と分類を行うことができます。分析結果に基づき、次々と自動プロセスと手動プロセスにかけることができます。たとえば、ネットワーク上の他の感染ホストの特定と検疫への許可要請、そのマルウェア感染に関連した脆弱性の特定と脆弱なシステムへの緊急パッチ適用のスケジューリング、または内部スタッフや外部モニターへの必要な通知の送信などといったプロセスがあります。また、各段階での要請、対応、行動を文書化すると、将来の参照に使うことができます。

自動化を開始するには、合理化すべき適切なプロセスをピンポイントで特定します。これらはほとんどの場合、時間がかかる単調で非効率的な作業で、アナリストの時間を法外に消費しますが、これらの作業は安全、確実に自動化できます。セキュリティー・リーダーは、プロセスを自動化した場合のリスクと複雑さ、および自動化によって得られそうな効率性を比較分析する必要もあります。

安全で確実な自動化を実現するには、プロセスの忠実性をテストします。人の意思決定と承認が関わり続ける手動アクションをスクリプト化してください。チームにとってプロセスが正しく、テクノロジーが適切に機能する快適レベルを築いたら、完全な自動化を決定できます。

ただし、テクノロジーベースの自動化で時間を節約できる一方、その効果は IR 能力の高さによって左右され、調整されたインシデント対応手法で最も効果的に利用できるということに留意することが重要です。

「ローマは一日にして成らず、しかし、データ漏洩は一日で起こることがよくあります…。合法的な認証情報を持っていれば、扉の鍵を開けて中に入り、冷蔵庫の中をつまみ食いするのは簡単です」

— The Verizon 2016 Data Breach Investigations Repory

ステップ 6　人、プロセス、テクノロジーを協調させる

インシデント対応調整が約束する成果、つまり対応の迅速化と自動化の増加は、業界の多くのセキュリティー・エキスパートの注目と関心を集めました。しかし、最後のセクションで説明するように、調整と自動化を成功させ、効果的に利用するには、全体的に高い IR 能力が求められます。効果的な調整を実現する鍵は、完全に組織の IR 基盤である人、プロセス、テクノロジーの質次第です。

本ガイドの前のセクションでは、これらの基本的な構成要素を熟考して強固なものにし、将来の改善に対応する方法について説明しました。ここではあらためて、IR 基盤の強さを評価する際に自問すべき基本的な問いを列挙します。

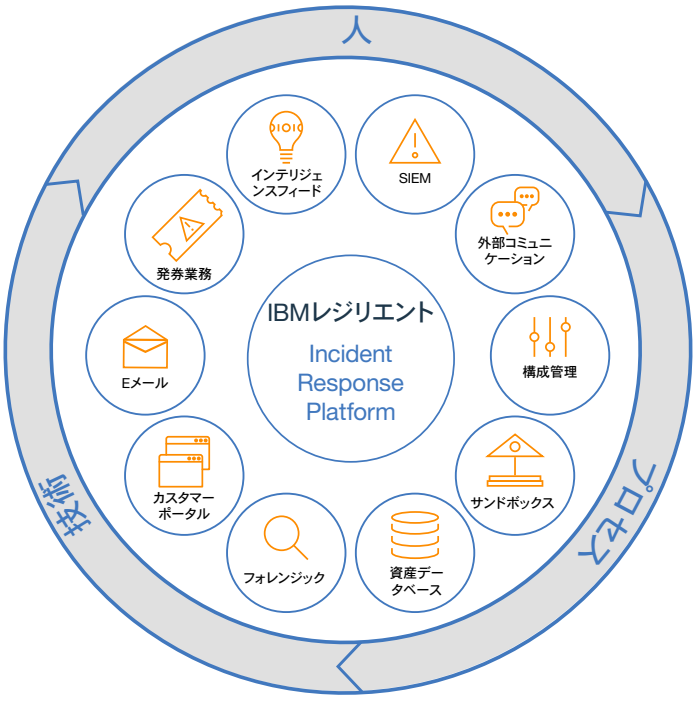


図 1: Resilient IRP が IR 調整の中央ハブとして機能する仕組み

人: IR チームの十分な連携と訓練が確実に行われているか?インシデントのライフサイクルのあらゆる側面に対処するための適切なスキルがチームにあるか?協働と分析の手段はあるか?

プロセス: 反復可能で一貫した明確な IR 計画が策定されているか?それらの計画は更新と改善がしやすいか?定期的に計画をテストし、測定しているか?

テクノロジー: テクノロジーを使って貴重な知見と情報を直接的に提供しているか?テクノロジーにより、チームは賢い決定を下し、それらの決定に迅速に行動できているか?

上記の問いに対応することで、これらの構成要素に合わせて調整を行い、真の効果を上げることができます。この基盤を築いていない場合、調整のメリットはごく限られたものになります。

インシデント対応調整の目標は、セキュリティー・インシデントが発生したときに、適切な対処方法を関係者に確実に把握させ、迅速、効果的、適切な対応に必要なプロセスとツールを整えることで、対応チームの能力を強化することです。

調整と自動化は両方ともサイバー・セキュリティー・プロフェッショナルの間で人気を増していますが、調整についていうと、前後関係と意思決定の理解を助けるといった、サイバー・セキュリティーの人間主体の要素をサポート、最適化する点で異なり、セキュリティー・オペレーションの中心的要素として人的要素を強化します。

セキュリティーの脅威は不確かな問題なので、これは重要な区別になります。脅威への対応が、お決まりの問題であることはめったにありません。自動化は、特定の作業を迅速、効果的に行うための優れたツールになりますが、大抵の場合、脅威は進化し続け、犯罪者は戦術を変えるので、問題の上申やトラブルシューティングには人による意思決定が必要です。

自動化は広範な調整プロセスにおいて有効なツールになりますが、調整によって大きな変革をもたらすのは人的要素です。

調整のあり方はそれぞれの組織によってさまざまです。その組織独自の脅威の状況、IT とセキュリティー環境、企業の優先順位に応じて行う必要があります。ただし、簡単な例を挙げると、以下が典型的な使用事例で、IBM が協力した組織の多くで採用されている調整を示しています。

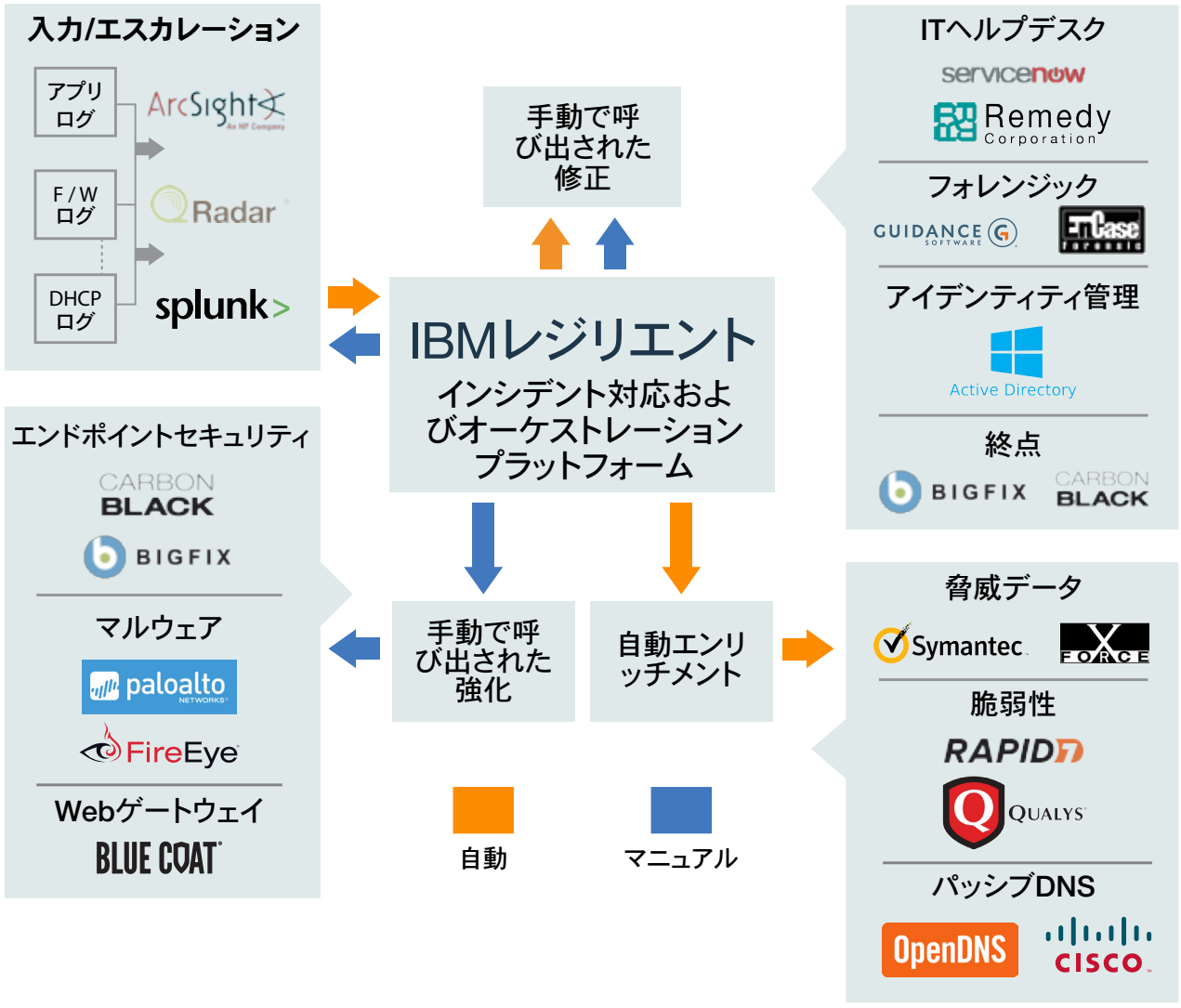


図 2: 統合 IRP を使って調整した 対応ワークフローの一例

図の左上には、インシデントが SEIM アラートに格上げされると、組織のインシデント対応プラットフォーム (IRP) でレコードが自動的に作成される流れが示されています。図の左上から右下に移ると、プラットフォームはインシデントの重要な前後関係情報を組み込みの脅威情報フィードなどのソースから収集し、提供しています。介入してコントロールする際、セキュリティー・アナリストは重要な情報をすでにここから得ています。これらのアナリストはその他の統合を利用して、必要と思われるその他の作業に手動で取り掛かることができます。そのような作業には、他のセキュリティー・ツール (エンドポイント・セキュリティー・ツールや Web ゲートウェイなど) からインシデントに関する他の情報を収集したり、IT ヘルプ・デスクにアラートを送信するか、ID 管理に進んでユーザーをネットワークからオフにすることで問題の修復を開始したりするといった作業が含まれます。

IR プロセスの調整方法は多種多様ですが、目標は常に同じです。つまり、脅威に対処できるようアナリストを最適な位置につかせることです。

結論: 立ち直りが早く、いつでも対応できる組織を築く

テクノロジーの進歩のおかげでインシデント対応がまもなく、準社員でも *プッシュ・ボタン 1 つで* 解決できるプロセスにならないかとつい想像してしまいますが、現実の IR はこれからも複雑かつ多面的であり続け、情報セキュリティー・アナリストの注意が求められます。

成熟したインシデント対応では、人、プロセス、テクノロジーが連続体の一部として組み合わせっています。テクノロジーの仕事は、人のアナリストの代わりになることではなく、特定の脅威に関するより正確な情報を提供し、対応プロセスを合理化し、セキュリティー・アナリストの対応準備を確実にすることで、アナリストの能力を強化してより多くの作業をこなせるようにすることです。

さらに、成熟したサイバー・セキュリティー・インシデント対応能力によって、組織内の社風を大きく変革することができます。セキュリティー・チームを IT 運営および管理ともっと緊密に連携させ、サイバー・インシデントへの対応プロセスに包括的な方法で積極的に参加させることが可能になります。

インシデント対応プロセスが成熟すると、組織は先見的な対応の段階に入り、インシデント対応から得た情報を組織にとって戦略的な方法で活用するようになります。先見的な対応の場合、IR チームから得た情報をセキュリティーと IT 組織にフィードバックできます。技術投資と買収を具体化し、従業員のスキル・セットを先鋭化し、組織のリスクの理解を広げて物理的なセキュリティー資産とプロバイダー、脅威情報提供者、規制当局、行政機関などの幅広いエコシステムを包括することが可能になります。

フォーチュン 500 の中でも、このレベルの成熟度に達している企業はほとんどいませんが、今後数年間で、成熟したインシデント対応プラットフォームに移行する企業が増えるにつれて、インシデント対応の戦略的な使用が一般的になることが予測されます。

詳細情報

インシデント対応を調整して、より迅速に賢く行動できるようにセキュリティー・チームの力を強化しましょう。

今すぐ、Resilient Incident Response Platform のデモにお申し込みください: **http://info.resilientsystems.com/incident-response-platform-schedule-a-demo**

IBM Resilient について

IBM Security の使命は、サイバー攻撃やビジネスの機器に直面する組織が目標に向かって前進できるように支援することです。Resilient Incident Response Platform (IRP) は、インシデントの分析、対応、緩和をさらに迅速に賢く効率的に行えるようにセキュリティー・チームを強化します。Resilient IRP は業界唯一の包括的な IR 調整および自動化プラットフォームであり、人、プロセス、テクノロジーを単一のインシデント対応ハブに統合することを可能にします。多くのフォーチュン 500 企業、および数百ものパートナー企業が世界中で IBM for Resilient の最高クラスのセキュリティー・ソリューションを利用しています。

IBM CorporationSecurity GroupRoute 100Somers,
NY 10589

Produced in the United States of America December 2017

1 http://www.esg-global.com/blog/dealing-with-overwhelming-volume-of-security-alerts

2 http://cyberseek.org

3 http://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2016_Cyber_Resilient_Organization_Executive_Summary_FINAL.pdf

4 https://securityledger.com/2016/02/focus-on-privacy-hobbles-security-at-healthcare-orgs

5 http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016

リサイクルにご協力ください。

BUW03068JPJA-00