QRadar SIEM構築プロジェクト成功の秘訣

QRadar導入の現場から

「IBM Security QRadar SIEM」(以下、QRadar)は、単体のセキュリティー製品では検知が困難な高度で複雑な攻撃の検知や、ログ調査や分析を効率化する製品です。QRadarの導入において最も重要なのは、十分な情報を含むログやネットワーク・フローを、できるだけ多く、できるだけリアルタイムに収集すること、そして、サイバー攻撃の痕跡を見つけるルールや検索条件を組織に合わせて適切に設定し、継続的な見直しやチューニングを行うことです。しかし、現実には、さまざまな課題により、QRadarの導入効果を十分に引き出しきれていないこともあります。

本稿では、QRadar導入時に直面する課題を洗い出し、QRadar導入を成功に導き、その機能を最大限に活用するための秘訣を解説します。

1. QRadar導入をめぐる状況

厳しさを増すセキュリティー情勢を背景に、企業や組織でのSIEM(Security Information and Event Management)製品の導入が進んでいます。複数機器のログを総合的に分析するSIEM製品は、単体のセキュリティー製品では検知が困難な、高度で複雑な攻撃の検知に効果を発揮するとともに、インシデント発生時のログ調査や分析の効率を飛躍的に高めます。

そうしたSIEM製品であるIBM Security QRadarは、複数のログやネットワークのフロー情報をリアルタイムに組み合わせ、高度な相関分析を行うことができます(**図1**)。OSとアプリケーションとストレージが統合されたアプライアンス製品で、インシデント検知のためのルール、分析結果のレポート生成のためのテンプレート、さまざまなログの検索条件があらかじめ多数用意されており、容易な構築が可能です。

しかし、QRadar構築プロジェクトの現場には、いくつかの課題も見られます。そこで本稿ではこれらの課題を整理し、QRadar導入を成功させる秘訣である「構築作業に

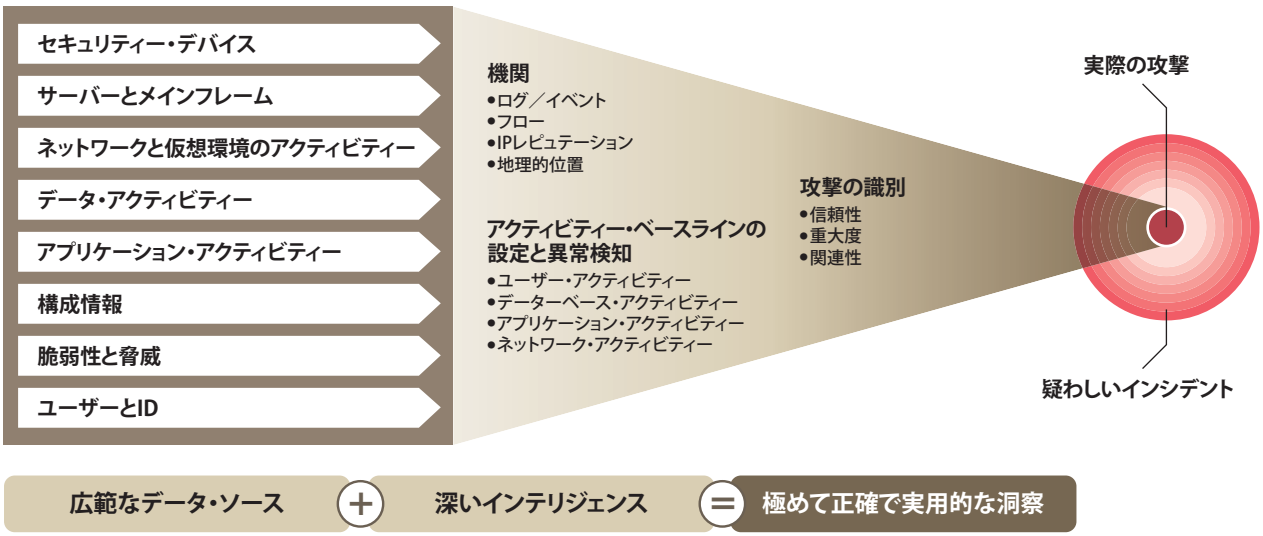

図1. QRadarの概要

かける工数を見極めること」「ログの鮮度と中身には妥協しないこと」「QRadarの機能を最大限に生かすこと」について解説します。

2. 構築作業にかける工数を見極める

●QRadar構築に関する2つの考え方

QRadarのようなSIEM製品の導入が進んだのはここ数年であり、多くの組織にとってSIEM構築は初めての経験です。そのため、構築作業の進め方や、可用性能、運用方法などに関する考え方が関係者間で統一されていないことがあります。

QRadarの構築に際しては、2つの考え方があります。「一般的な業務システムと同様の方法で構築・運用する」とする考え方と、「分析ツールであるQRadarは、構築・運用にそれほど手間をかけなくてよい」とする考え方です（**図2**）。

一般的な業務システムの場合、システムの障害や処理遅延は甚大な業務影響を与え、処理のデータ整合性の確保も必須です。必然的に、高可用性を実現するHA構成をとることはもちろん、性能監視、障害監視などの綿密な監視・運用設計が行われます。システムの設計情報はドキュメントに網羅的に記載され、システム運用で発生しうるすべての作業についての洗い出し、テストや手順のドキュメント化が行われます。

一方で、QRadarを業務システムではなく、業務を効率化するためのツールの一つと見なすと、構築そのものよりも使い勝手や効果の最大化に重点が置かれます。すなわち、障害の発生は望ましくないにしても、万が一の障害時に使えないことや、ログが欠損することを気にするよりも、1日も早く使い始められることや、使いやすいカスタマイズがなされていること、使って効果を出すことの方が重要度が高くなります。

インシデント検知やその解析作業に有効なQRadarを単なるツールと呼ぶのは語弊があるかもしれませんが、QRadarにどのような障害が発生しても、基幹業務に影響を与えるわけでも誰かに損失を与えるわけでもありません。そのため、多くのQRadar構築プロジェクトでは、一般的な業務システムよりも低いシステム要件、簡素なテスト、運用監視やドキュメントで十分という想定で、

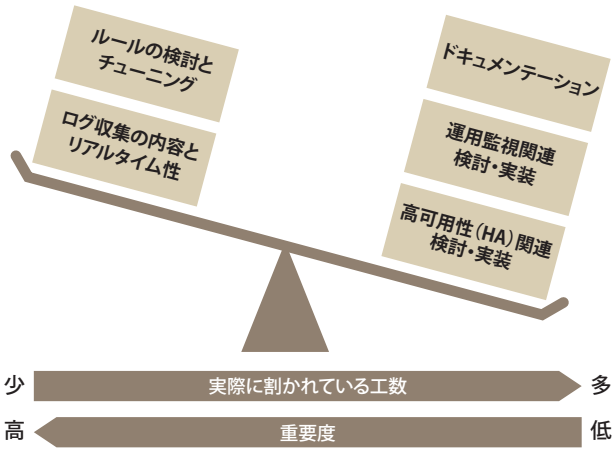

図2. QRadar導入の現状

プロジェクトの作業内容と工数が見積もられます。

しかし、プロジェクト開始時に、関係者間で構築作業の進め方や作成ドキュメントのレベルについて合意されていないまま進めていると、一般的な業務システムと同一の評価基準に立つ人の目から見ると「設計書や運用監視方法が不十分」という判断となり、その対応に想定外の工数がかかってしまいます。一方、早期に構築可能なアプライアンスのツールと見なしている人からすれば、「構築に期間と工数がかかりすぎ」と見えてしまうこともあります。

QRadar構築プロジェクトの開始時には、“暗黙の了解”はないものと肝に銘じて、その組織がQRadarに求める本当に必要な要件、運用監視方法、必要なドキュメントを関係者で合意しておくことが重要です。一般的な業務システムと同等とするならそれなりの構築期間と工数が必要となり、ある程度ツールと割り切って最低限必要な要件、作業、ドキュメント作成のみを行うなら、一般的な業務システムよりはるかに短い構築期間で運用を開始することも可能です。

●ドキュメントは必要なものだけにする

QRadarに設定する各種パラメーターは、IPアドレスなどの最低限の設定情報以外は、分析の状況に応じて設定を調整・変更しながら使用していくものがほとんどです。通常はシステムの設定値を変更するのはシステム管理者や運用担当者に限られますが、QRadarの場合は解析を行うセキュリティー・オペレーター（分析者）も、日常運用の中でさまざまな設定の変更や追加をします。

このようなシステムでは、詳細かつ網羅的な設計書やパラメーター・シートを作成して管理してもあまり意味がありません。障害時の復旧という観点では、バックアップを取得しておけばよく、それ以外の設計や設定内容については、網羅的なドキュメントを作成するのではなく、情報共有が必要な内容や恒久的に変更しない内容など、そのプロジェクトや組織の状況に合わせて、必要なタイミングで必要な内容に絞って作成することが効果的です。

●高いシステム要件を求めすぎない

QRadarの分析は、数十万、数百万というデータから脅威を探し出す作業です。インシデント調査では、ネットワーク・フロー、認証ログ、プロキシやファイアウォールのログなどさまざまなイベントを時系列に並べ、何が起こったのかを解析していきます。さまざまなログを横断的に、かつ早期に解析できることは大変重要ですが、そのうちいくつかのログが何らかの問題で欠損していたとしても、解析への影響は限定的です。また、ここでいう「早期」とは、5分や10分といった話ではなく、ほとんどの場合半日程度のレベルで十分でしょう。そう考えると、QRadarに必須となる可用性要件は、一般的な業務システムに比べると低いと言えます。多少のログ欠損やシステム停止は許容して、例えば、「QRadarが障害中に収集できなかったログを障害復旧後に転送し、分析する仕組み」を検討するという設計も有効です。

QRadarの詳細な運用監視や、必要以上の可用性の実現のために工数を割くより、一つでも多くの機器のログをQRadarに連携することや、QRadarでの検知条件を精査することの方が、QRadarの導入の効果は高くなります。一般的な業務システムでやってきた「当然」をそのままQRadarに当てはめず、QRadarに本当に必要なシステム要件を見誤らないよう注意してください。

3. ログの鮮度と中身には妥協しない

●ログ収集の現状

QRadarでログを統合的に収集し分析するためには、既存のサーバーやセキュリティー機器のログをQRadarに送信する必要があります。望ましいのは、QRadarが解析できる方式に従いsyslogなどでリアルタイムにログを連携することです。しかし現実には、本番運用中の機器の設定変更は、たとえログ出力設定だけであっても容易ではありません。既存システムのログ出力機器の運用担当者にとって、本場環境に変更を入れることへの抵抗は大きく、そもそもログの内容を理解し、出力方法の設定変更を行える担当者がいないことさえあります。現在出力しているログをそのままの形式で1日数回ファイル転送するケースや、既存のログ出力には分析に必要な情報が含まれていないケースも多くあるのが現状です。

●リアルタイム性にこだわる

インシデントの早期検知には、イベント発生時に、イベント発生時の外部脅威情報を参照し、他のイベントやネットワーク・フローとリアルタイムで相関分析を行うことが最も有効です。ログの取り込みが遅れれば、それはそのまま脅威の検知の遅れに直結します。検知の遅れは調査や対処の遅れにもつながります。

リアルタイムのログと日次バッチのログが混在しているより、すべてリアルタイムでログが収集される方が、複数のログの前後関係を含む相関分析もリアルタイムに行われるため、分析の効果が高くなります。

またQRadarは、外部脅威情報としてIBMのセキュリティー研究開発チーム「X-Force」が提供するレピュテーション情報（悪意のある既知のIPアドレスやURLのリスト）を取り込んで分析に使用する機能を備えており、このレピュテーション情報は数分単位で常に更新されています。セキュリティー・イベント発生時にその時点でのレピュテーション情報で分析するのが最も精度が高く、時間の差が広がれば検知の精度は下がります。これらの理由から、ログの収集はできるだけリアルタイムにこだわるべきなのです。

●出ていないログは解析できない

QRadar導入の成否を左右するのが、分析に必要な内容がログに含まれているか否かです。QRadarを導入しさえすれば相関分析ができて脅威の検知ができるわけではなく、解析に必要なログが出力されて、それを適切なルールで分析してはじめて検知が可能となります。ログの内容が不十分であれば、QRadarがどんなに高度な解析ができても意味がありません。

ログ出力については、組織内でガイドラインが定義されていることもあれば、それぞれのシステムで個別に設

定されていて内容が統一されていないこともあります。例えば、Windowsシステムであれば、イベント・ログは解析に欠かせませんが、QRadarを構築することとWindows系サーバーのイベント・ログを収集することだけが決まっていて、イベント・ログに今何が出力されているか、何を出力すべきかという議論が皆無ということもあります。認証ログでは認証の失敗だけが出力されていることがありますが、侵入が成功したのかどうかの解析には、むしろ認証の成功ログが重要ですし、マルウェアの検知や解析であれば、マルウェアの遠隔管理によく使用されるPsExecといったツールの実行状況を参照できるシステム・ログの取得が有効です。

●根本的な解決のために

これらの課題は、QRadar構築担当者と、ログを出力するサーバーやネットワーク機器の担当者間の調整だけで解決できる問題ではありません。QRadarの導入効果を高めるためには、プロジェクトよりも上の組織のレベルで、ログの出力内容とリアルタイム連携の方針を定義し、トップダウンで決断することが必要です。

仮に、QRadarの運用開始のタイミングでログのリアルタイム連携やログ出力内容の変更が実施できなくても、後にログ取得方式や出力内容の変更計画を立て、可能な限り移行するよう努めてください。

4. QRadarの機能を最大限に生かす

●検知機能と検索機能

QRadarの基盤構築が完了し、ログやネットワーク・フローが収集されるようになったら、いよいよQRadarをいかに活用するかを考えていきます。

QRadarには大きく2つの機能があります。1つはリアルタイムに分析を行い分析結果をまとめてアラートを生成する、いわゆる「検知機能」。もう1つは、手動もしくは定期的にQRadarの内部に取り込まれた情報を横断的に検索して分析を行い、レポートを生成する「検索機能」です。ただし、検索結果を基に検知してアラート生成なども行えるため、双方の機能は密接に関連しています。

検知機能では、ログやネットワーク・フローをどう組み合わせて検知するかという条件と、条件を満たした場合に実施するアクションをルールによって定義します。例えば「認証失敗のログが出てから5分以内に同じIPアドレスに対する認証が成功した場合」や、「既知のC&Cサーバー(Command and Control server)との通信が発生した場合」などを条件とします。そして代表的なアクションが、「オフェンス」と呼ばれるアラートの生成です(**図3**)。オフェンスは、QRadarがルールによって検知したさまざまな疑わしいアクティビティーを自動的に解析して関連付け、優先順位を付けてまとめたもの

図3. QRadarのオフェンス画面

です。生成されたオフェンスは、直感的な操作で詳細を確認することができます。

検索機能は、ログやネットワーク・フローを詳細に確認する作業を強力に支援します。さまざまなフィルター条件の指定や、SQLのようなクエリー言語（AQL）を用いて膨大なログから自在に参照したいデータを取得できます。QRadarでは、データが正規化されログの内容が分類・意味付けされているため、ログの意味（例えば「認証失敗」）による検索や、ログ出力時間や宛先IPアドレス、宛先ポート番号などさまざまな要素を検索条件に指定できます。ネットワーク・フローについては、ペイロード情報を基にアプリケーションを自動的に識別できるため、例えば「80番以外のポートを使用したHTTP通信」を検索することも可能です。

●「とりあえずデフォルト・ルール」の意味

QRadarには、デフォルトでルールが350種類以上用意されています。何もないところからルールを作成していくのは非常に大変な作業ですが、このデフォルト・ルールを活用することで早期の運用開始が可能です。

そのため、QRadar構築プロジェクトでは、「とりあえずルールはデフォルトで」という声がよく聞かれます。しかし、デフォルト・ルールはそのまま何もせずに利用できるものではなく、監視対象や組織のポリシーに合わせて最適化してはじめて効果を発揮します。例えば、組織で禁止されている特定のアプリケーションや通信を検知したければ、ポリシー違反の検知ルールは組織のポリシーに沿って設定されていなければ意味がありません。

デフォルト・ルールを出発点として、どれを使用するかを判断し、各ルールの適用条件やしきい値を調整し、検知時にアラートを上げるべきルールの選定をする作業まで含めて、「とりあえずデフォルト・ルール」と言えるのです。何も検討せずにルールはデフォルト設定のままでよい、という意味ではないことに留意し、プロジェクト計画の段階でルールの検討を計画に組み入れてください。

●チューニングは必須

350種類以上もあるデフォルト・ルールから選定しようとするとき、検知漏れを恐れるあまりついついすべてのルールを有効にしたくなります。さらには、有効にするだけでなく、検知されたらすべてアラートを出すように設定しがちです。しかし、想像してみてください。すべてのルールを有効にすると場合によっては1日に何百～何千件もの大量のアラートが生成されてしまいます。セキュリティー・オペレーターが数人の組織で毎日数百ものアラートが上がったら、確認が追いつかず本当に重要な事象が埋もれてしまったり、QRadarが生成できるアラート数の上限を超えてアラート生成さえできなくなることもあります。

QRadarのルールを最適化するにあたっては、そのルールがその組織の脅威検知に有効であるかどうかという議論に加え、その組織の運用体制で調査・対応ができるアラート件数となるように絞ることが重要です。「ルールで検知はするがアラートは上げずにQRadarのコンソールで検索して参照する」「ルールではなく定期的にレポート生成して確認する」など、参照や確認方法を考慮するとよいでしょう。

- when the local network is one of the following networks
- when the destination network is one of the following networks
- when the IP protocol is one of the following protocols
- when the Event Payload contains this string
- when the source port is one of the following ports
- when the destination port is one of the following ports
- when the local port is one of the following ports
- when the remote port is one of the following ports
- when the source IP is one of the following IP addresses
- when the destination IP is one of the following IP addresses
- when the local IP is one of the following IP addresses

図4. ルールを構成する条件（一部）の例

QRadarの提供するアノマリ検出ルール

しきい値ルール
一定時間におけるしきい値で異常性を判断
検出例：8時～17時の間にログインできるユーザー数を220以下とし、221人目がログインしたらアラート生成

アノマリ・ルール
トラフィックやイベントの頻度に関連する異常を判定。一定時間内に発生したイベントの頻度を学習し、異なる挙動を検出。
検出例：過去5分間と1時間の平均のトラフィック・ボリュームが40%以上異なった場合アラート生成

振る舞い型ルール
ホルト・ウィンターズ法アルゴリズムを利用し、トラフィック・レベル／季節／トレンドを考慮した予測を行う。次のインターバルの統計量を予測し、実際の値と比較することでアラート生成。
検出例：業務時間外に毎秒100ホストと通信するメールサーバーが毎秒1000ホストと通信した場合アラート生成

図5. アノマリ検出ルール

QRadarの運用開始直後は、多くの場合、大量のオフェンスが生成されますが、そのオフェンスの大半はFalse Positive(誤検知)です。その組織の環境に合ったルールの条件や、検知除外の条件の設定を時間をかけてQRadarに組み込んでいき、検知精度を高めて実運用に乗るようにチューニングしていくことが非常に重要です。

●デフォルト・ルールの一歩先、独自ルール

昨今の巧妙な標的型攻撃を考えると、デフォルト・ルールに加えて、独自にルールを作成することが望まれます。独自のルール作成といっても、決して難しい作業ではありません。QRadarのルールはすべて、Webコンソールから使用したい条件を選んでクリックして追加し、パラメーターを入力して作成するため、複雑な文法や記載方法を勉強する必要はありません。条件には簡単なものから、複数のイベントの前後関係や時間間隔を定義するもの、複数のルールの前後関係や相関を指定するものまで、さまざまなものが用意されています(**図4**)。

例えばIPA(独立行政法人 情報処理推進機構)で公開されている「『高度標的型攻撃』対策に向けたシステム設計ガイド」[1]に定義されている攻撃シナリオや攻撃ツールを検知するルールを作成するのも一案です。それ以外にも、マルウェア感染対策であれば、「プロキシを経由せずに直接インターネット接続を試みる通信や定期的に発生する同一宛先へのリクエストの検知」、データ漏洩対策であれば、「一定サイズ以上のファイル転送の発生や退職予定者による外部クラウド・サービスへのファイル・アップロードの検知」なども有効かもしれません。QRadarでは、このような検知のアイデアを、簡単にルールで表現することができます。

さらに、高度なアノマリ検出ルールもぜひご活用ください(**図5**)。アノマリ検出ルールは、デフォルト・ルールには含まれない、イベントやネットワーク・フローの集計値に対して条件を設定するルールです。「しきい値ルール」「アノマリ・ルール」「振る舞い型ルール」の3種類が提供されており、トラフィック量の通常状態との乖離や、特定のイベントの発生件数の異常などを検出できます。どのような振る舞いを行うかわからない未知の攻撃の検知には、通常状態からの乖離の検知ができるアノマリ検出ルールが有効です。

QRadarは多種多様な事象を検知する能力に加え、ルールの作成が非常に容易で自由度が高いのが特徴です。「とりあえずデフォルト・ルールで」で始めたとしても、ぜひ一歩先の独自ルールを作成してQRadarの機能をフル活用してください。

5. 終わりに

QRadarを導入する目的は、外部からの脅威をいち早く検知し、被害状況や原因の解明を迅速に行うことです。QRadar基盤を構築しても、ログの中身と分析ルールが伴わなければ、目的は達成できません。QRadarシステムの稼働開始が導入完了ではなく、その組織に合った有効なルールが、その組織の体制下で運用できるように適切にチューニングされてはじめて導入完了と言えます。QRadar導入に関わるメンバーは、この最終ゴールを認識し、優先順位と工数配分を誤らずにプロジェクトを遂行することが重要です。

そして、進化するサイバー攻撃に対応していくためには、QRadar導入完了後も常にルールを見直し、最適化を続けることが必要です。サイバー攻撃は日々高度化、巧妙化しています。今は有効なルールでも半年後には役に立たないかもしれません。その組織に合ったルールの作成とチューニングを促進すること、そして一度作成したルールを放置せず、状況に合わせて常に見直していくことが、なによりも重要です。

[参考文献]
[1] IPA:「『高度標的型攻撃』対策に向けたシステム設計ガイド」の公開, http://www.ipa.go.jp/security/vuln/newattack.html

日本アイ・ビー・エム システムズ・エンジニアリング株式会社
セキュリティー・ソリューション
アドバイザリー・アーキテクト

寺嶋 朋子
Tomoko Terashima

日本IBM入社以来、数多くのSIプロジェクトに参画し、システム基盤およびアプリケーション開発の両方の経験を積む。日本アイ・ビー・エム システムズ・エンジニアリングに出向後BPM製品、モバイル製品担当を経て、2014年より現職。QRadar担当としてQRadarの製品検証やQRadar案件への技術支援を行う。