CSIRTを進化させる次の一手
インシデントの発生を前提とする時代 サイバーセキュリティプレイブックの整備

PwCコンサルティング合同会社　ディレクター　辻 大輔
PwCコンサルティング合同会社　マネージャー　松原 翔太

サイバーセキュリティの施策や投資と言えば、セキュリティインシデントの発生に対する「予防」策や「検知」策を中心とする企業が多く、発生し得るインシデントへの「対処」を改善するための施策や投資は、まだ一部のセキュリティ先進企業に留まってしまっているのが現実です。サイバーセキュリティ対策の考え方の主流は、「インシデントを予防する」ではなく、「インシデント発生を前提として対策する」にシフトしており、インシデントへの「対処」についてあらためて検討を行うべき時期に来ていると言えます。今回は、インシデントへの「対処」を強化するためのツールである「サイバーセキュリティプレイブック」を整備するポイントについて解説します。

1. サイバーセキュリティプレイブックとは

サイバーセキュリティプレイブック（以下、プレイブック）は、サイバーセキュリティインシデント発生時に「いつ、誰が、何を、どのように対応すべきか」について定めた、SOC（Security Operation Center）やCSIRT（Computer Security Incident Response Team）に向けた、より高度な手順書のことです。

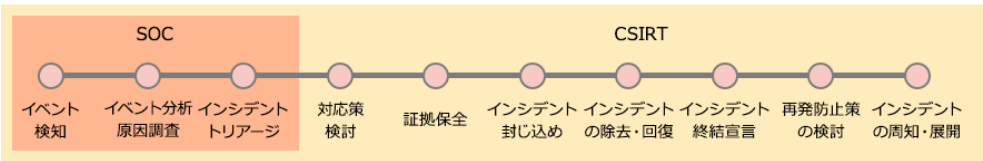
一般的に、SOC／CSIRTがサイバーセキュリティインシデントの兆候を検知した場合、図表1のようなフローに沿って対応が行われます。

多くの組織ではこのフローに基づいて、共通の調査手順や対応手順を定めていることでしょう。しかしこの手順は、果たしてどこまで機能するのでしょうか。

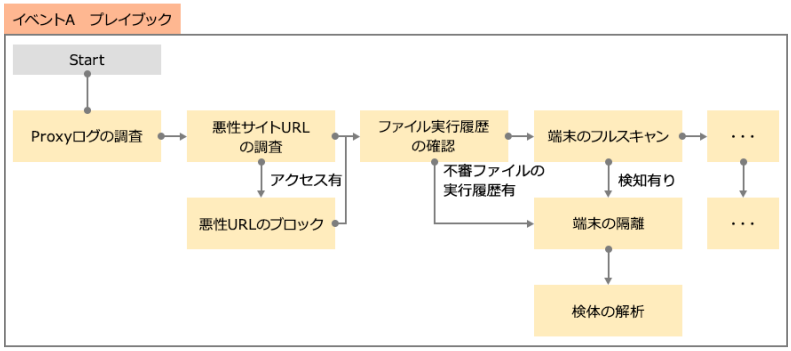
実際のインシデント発生現場では、発生したインシデントの性質、あるいは刻々と変化する状況に合わせて臨機応変に対処することが求められ、共通の調査手順は機能しないことがほとんどです。代表例として、情報漏洩の疑いによる調査では事実確認や原因調査が優先され、ランサムウェアの感染では、感染拡大の防止を目的にインシデント封じ込め（嫌疑端末の隔離）が優先されます。また、こうした臨機応変な対応は、十分な知識と経験を持つ上級のアナリストによって判断されることが多く、俗人化しているがゆえに、上級アナリストの不在時にはインシデントが深刻化し、企業に大きなダメージを与えるリスクを抱えています。

プレイブックは、自社に発生し得るインシデントの種類やそのシナリオに鑑み、それぞれの対応手順や判断のポイントおよび基準を整理したものを指します。プレイブックの整備により、経験の浅い担当者でも上級者の判断を仰ぐことなく対応ができ、また、後述のSOAR（Security Orchestration Automation and Response）によって、インシデント対応を自動化することも可能になります。

図表1：SOC／CSIRTの対応フロー例



図表2：プレイブックのイメージ（フローのみ）



2. プレイブック整備のポイント

先述の通り、プレイブックには自社に発生し得るインシデントの事象ごとに、漏れなくそれぞれの対応手順や判断基準が整理されていることが重要です。ここからは、どのようにしてプレイブックを整備するべきかについて紹介します。

Step1. 自社で起こり得る脅威シナリオの把握

初めに、自社で発生し得るインシデントと当該インシデントが与える影響範囲を漏れなく特定することが重要です。これには、さまざまな攻撃手法が成立し得るかといった観点からインシデントの影響を机上で評価する「脅威シナリオベースのリスクアセスメント」を用いることが一般的です。

プレイブックに記すべきインシデントを特定し、当該インシデントが与え得る影響を知ることによって、プレイブック内で確認するべきポイントや必要なアクションの概要が見えてきます。

Step2. 脅威を検知する仕組みの構築

次に、インシデントシナリオの開始、つまり攻撃の予兆を検知する仕組みを検討します。

自社で発生し得るインシデントのシナリオが把握できたとしても、それらを検知する仕組みがなければ、その後の対処に移ることはできません。一般的なインシデント検知の仕組みにはログメッセージが利用されますが、システムのステータス変化やプロセスの起動／停止、特定アカウントでのログインといった状態の変化も、攻撃の予兆を検知するためのトリガーとして活用することが可能です。

Step3. 検知後のアクションと必要な情報の整理

最後に、インシデントシナリオに基づき、プレイブック内に、取るべきアクションを整理していきます。

例えば調査を行う場合は、必要な情報は何か、またその情報がどのようになっていれば期待値／異常値であるのかを整理し、次のアクション、またその次のアクションと、それぞれを有機的にひも付けて、具体的な作業内容を記載していきます。

プレイブックでは、対処する要員の数も考慮しながら、システム調査などのメインストリームに並行して、当事者への聞き取りや関係者への報告などのアクションを実施し、それぞれの合流地点と各アクションにおける判断ポイントを整理しておくことが重要です。

3. SOARによる手順の自動化

インシデント対応においては最近、SOAR（Security Orchestration Automation and Response）と呼ばれるソリューションが注目されています。SOARでは、プレイブックに定めた手順をツール上に登録することで、その処理を自動で実行することができます。例えば、「悪性サイトへのアクセス」が疑われるイベントが発生した場合、そのURLについて、脅威インテリジェンスに関する情報を記した外部サイトなどで影響を確認し、脅威があると判断した場合、当該URLへのアクセスをURLフィルターなどと連携してブロックすることや、マルウェアをダウンロードした可能性がある場合は、当該端末の切り離しを自動で行うことができます。SOARツールの多くはあらかじめ、多くのセキュリティインシデントに対する対応手順をテンプレートとしてまとめており、当該テンプレートを自社向けにカスタマイズすれば、容易に導入することが可能です。

しかしながら、SOARは自社で発生し得る脅威を検知でき、かつその対処手順が定まっていることを前提としたソリューションです。導入したからといって即座に全てのインシデント対応を自動化できるわけではありません。そのため、プレイブック整備のポイントに記載したように、リスクアセスメントなどを通じて自社で発生し得る脅威を特定し、それらを検知・調査する手順を整備した上で導入することが重要です。

4. 最後に

プレイブックの整備は、一度手順を定めたら終わりではありません。レッドチーム演習に代表されるセキュリティ診断や、実際のインシデントに対処した場合の経験や知見などに基づいて都度アップデートを行うことが必要です。そうしてプレイブックの実用性・実効性を高めていくことで、より強靭かつ属人的な対応が発生しないインシデント対応体制を築くことができるでしょう。

お問い合わせ

PwCコンサルティング合同会社
〒100-6921　東京都千代田区丸の内2-6-1 丸の内パークビルディング
Tel : 03-6250-1200（代表）　Mail : jp_cyber_inquiry@pwc.com