トピックス

脆弱性ハンドリングにおけるSOC利用
―企業CSIRTがSOCサービスを活用すべき理由―

脆弱性の公開から攻撃の発生までの時間は非常に短いため、その対応は経営課題となりつつある。本稿では、インシデント検知分析を担うSecurity Operation Centerサービス（以下、SOCサービス）における脆弱性ハンドリングの実態について説明するとともに、迅速かつ網羅的な対応を行うためになぜCSIRTがSOCサービスを活用すべきかについて解説する。

NRIセキュアテクノロジーズ マネージドセキュリティサービス事業本部
SOC事業推進部 主任セキュリティアナリスト
天野 一輝
専門はセキュリティログ監視による脅威分析、運用、人材育成

脆弱性公開から攻撃開始までの時間は非常に短い

基幹システムやクライアント端末など、企業が利用しているシステムに影響度の高い脆弱性があった場合、一般的な対策はベンダーが提供するパッチを適用することである。しかし、パッチ適用によるシステムへの影響は、検証に時間を要する。そのため、対策が完了するまでに、深刻な被害を引き起こす攻撃を受けることがある。特にインターネットに公開されているシステムでは、脆弱性の発表から攻撃が行われるまでの時間は、年々短くなる傾向にある（『日経コンピュータ』2017年6月6日付）。そのため企業は、被害の拡大を防ぐために迅速な初動が求められており、根本的な対策を行えるまでの期間をどうしのぐかは、経営課題といえる。

脆弱性への対応組織には2つある。インシデントハンドリングを担うComputer Security Incident Response Team（CSIRT）と、インシデント検知分析を担うSecurity Operation Center（SOC）である。ログ監視やデバイス管理にSOCサービスを利用することで、企業のCSIRTは、脆弱性への対策や有事の際の社内対応にリソースを集中できる（図1参照）。

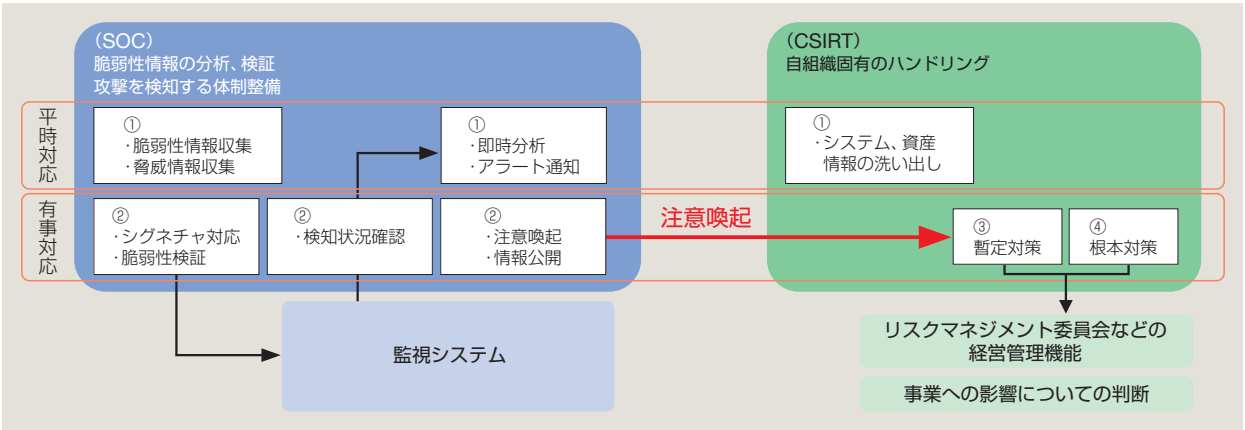
SOCサービスの脆弱性ハンドリング

SOCサービスの対応例として、NRIセキュアテクノロジーズ（以下、NRIセキュア）が提供するSOCサービスの脆弱性への取り組みを紹介する。NRIセキュアのSOCサービスでは、脆弱性認知時に、全社の専門家を集めて危険度の判定を行っており、年間5～10件程度の重大な脆弱性をハンドリングしている。対応の対象は主に、誰でもアクセスできるWeb上のシステムに関連する脆弱性だが、近年ではクライアント端末の脆弱性やマルウェアに対する緊急対応も実施している。

（1）情報収集、脆弱性の認知

公開される重大な脆弱性を迅速に認知するには、継続的な情報収集が必要である。NRIセキュアではRSS（ブログやニュースなどについて、Webサイトの更新情報を配信する

図1　脆弱性ハンドリングにおけるCSIRTとSOCの関係



ための文書フォーマット）、Twitter、ニュースアラートを通じて、脆弱性に関する情報収集を絶えず行っている。国内で広く利用されるシステムに関連する脆弱性情報を認知した場合は、危険の程度に関わらず、全社員が閲覧可能な情報共有基盤で即座に情報共有を行っている。

（2）緊急対応の要否判断

脆弱性が認知されたら、緊急対応の要否を主に以下の観点で検討する。

・対象のシステム、バージョン
・顧客環境での利用有無
・攻撃シナリオと影響度
・攻撃コード公開有無
・攻撃の観測事例有無

ここでの判断を誤ると、致命的な対応遅延に直結する。そのため、迅速かつ慎重な見極めが必要である。

（3）緊急対応実施

脆弱性ハンドリングでは、社内外に存在する多数のステークホルダー（利害関係者）を統率するための強力なリーダシップと、それぞれの持ち場の窓口が明確になっていることが必須である。

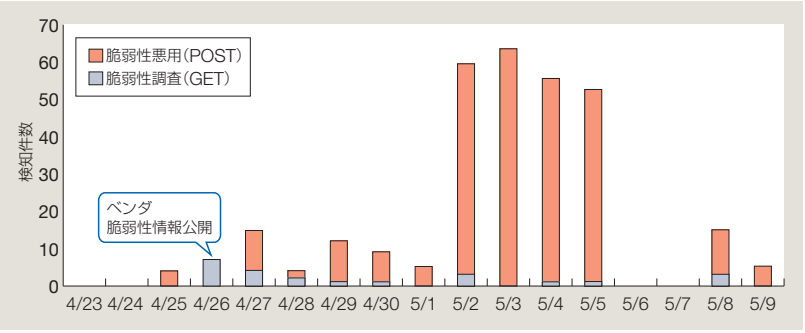
SOCが対応すべき項目も多岐にわたり、指令役とそれぞれの調査役に担当が分かれる。各項目の対応内容を、2019年4月に公開されたWebLogic（米国Oracle社のWebアプリケーションサーバ製品）の脆弱性（CVE-2019-2725）についての対応事例とともに説明する。

①セキュリティデバイスの検証

SOCでは、IPS（Intrusion Prevention System：侵入検知システム）、WAF（Web Application Firewall。脆弱性を悪用した不正な攻撃からWebアプリケーションを防御するシステム）などのセキュリティデバイスに対して、公開された攻撃コードを再現した通信を流し、既存シグネチャ（攻撃の検出に用いる攻撃パターン情報）での検知可否を確認する。既存シグネチャで検知できない場合、各デバイスのメーカーに対し、当該脆弱性に対応したシグネチャのリリース予定を確認する。しかしながら、メーカーが新たにシグネチャを公開するまでは、通常1日以上かかる。そのためSOCは、脆弱性情報や攻撃コードからカスタムシグネチャを作成する必要がある。NRIセキュアのSOCサービスでは、早い場合

は脆弱性認知から数時間以内にはシグネチャのプロトタイプを開発している。これを、インターネットからの通信をモニタリングできる環境に設置したセキュリティデバイスに試験導入することで、実環境ベースでの検証と改善(チューニング）を行う。

図2　WebLogicの脆弱性（CVE-2019-2725）を悪用する攻撃検知状況



②顧客の環境へシグネチャ適用

顧客の環境にあるセキュリティデバイスにシグネチャを適用する際は、一定の期間、検知モードで検知状況を確認した後、遮断化を行い、通常通信の誤遮断のリスクを低減する。これにより、対応速度と品質を担保している。

なお、CVE-2019-2725のケースでは、メーカーが提供するシグネチャ回避の手法が公開されていた。そのため、NRIセキュアのSOCサービスでは、メーカーが提供するシグネチャの実装と並行して、カスタムシグネチャの作成も実施した。

③攻撃コード検証

SOCでは、セキュリティデバイスを用いた検証と並行して、攻撃コードの有効性を確認する各種検証を実施する。この検証には「脆弱性が存在するシステム」と「パッチを適用した対策済みシステム」の2つの環境を利用し、攻撃コードの有効性や攻撃時のシステム挙動の違いを確認する。

また、攻撃コードの一部を書き換えることで攻撃バリエーションを増やし、シグネチャの検知パターンを回避する手法が存在していないかなど、シグネチャの網羅性と改善点を確認する。

具体的な例を挙げると、CVE-2019-2725において公開された手法は、ほとんどが過去のパッチを適用していれば防げる攻撃手法であったが、一部の攻撃パターンはパッチを回避するものであり、シグネチャの網羅性が問われるケースであった。

④検知状況確認

SOCは、脆弱性の公開時や対応シグネチャの適用後、攻撃通信の検知の有無を確認する。特定の脆弱性に特化したシグネチャの他、攻撃通信を汎用的に検知するよう設計されたシグネチャの検知状況を確認することで、脆弱性が公開される前から攻撃通信が発生していたことが分かる場合がある。実際にCVE-2019-2725では、ベンダーの公式情報公開前から、既存の汎用シグネチャで脆弱性を悪用する通信を検知していた（図2参照）。

⑤攻撃傾向に関する情報公開、注意喚起

SOCサービスは、脆弱性情報の把握および各種シグネチャの準備が整った段階で、注意喚起を兼ねて、対策方針について顧客に案内する。また脆弱性を悪用する攻撃通信を観測した場合、セキュリティベンダーは、その検知状況や攻撃の被害の有無を確認する方法を、ポータルサイトやブログなどを通じて公開する場合がある。

⑥脆弱性対応の振り返りと改善

脆弱性ハンドリングの実施後は、対応の振

り返りを行う。対応に不足はなかったか、対応の順序は望ましいものだったか、対応スピードに問題はなかったか、また良かった点はどこかを確認し、改善を重ねる。訓練・実践・改善を反復することでフローや対応内容は成熟する。そのため、SOCが円滑な対応が実行できるようになるまでには、年単位の経験の積み重ねを要する。

SOCサービスが脆弱性ハンドリングを行う意義とCSIRTに必要な対策

SOCサービスの脆弱性対応は、攻撃通信の検知遮断を主眼に行う。一方でシステムへの対策や有事の対応など、組織に特化した対応は、企業のCSIRTが取り組むべき事項である。本項では、SOCサービスを活用する意義と組織のCSIRTに求められる脆弱性対応を解説する。

・CSIRTの対応リソース集中化

CVE-2019-2725の事例では、ベンダーの情報公開以前に実際の攻撃が発生している。この事例が示すように、脆弱性の認知から暫定対策完了までの時間は短くなる傾向にあり、CSIRTが実施できる対策は限られたものとなる。SOCのサービスを利用することで、シグネチャのカスタマイズなど、セキュリティの専門知識が必要な作業を、SOCサービスに任せることができる。これによりCSIRTは、業務面でのすり合わせなど、暫定対策や根本対策の実施時に、組織主体でハンドリングすべきコア業務にリソースを集中できる。

CSIRTに求められる脆弱性への備えは、脆弱性公開時に迅速な対応ができるよう、SOCサービスから情報提供を受けた後に取るべきアクションを、あらかじめ定義しておくことである。脆弱性情報を受け取った際に、どのような意思決定をするのか、意思決定のために必要な情報はなにか、最終的な意思決定者は誰なのか。これらをガイドラインとして定義しておく。そして脆弱性ハンドリングの当日は、ガイドラインに従って、SOCサービスを含む関係各所との調整、意思決定、全体統括に専念することが望ましい。

・脆弱性への暫定対策としてのSOCサービス

脆弱性に対して、パッチ適用などの根本対策に時間がかかる場合や、有効な根本対策が見つかっていない脆弱性の場合、セキュリティデバイスを活用し、公開システムへの攻撃を遮断することが一定の暫定対策となり得る。

SOCサービスではさまざまな顧客にサービスを提供し、ノウハウを蓄積している。そのため、検知事例のバリエーションが豊富である。前章で紹介したセキュリティデバイスや攻撃コード検証を経たカスタムシグネチャの開発のほか、監視対象下で発生した攻撃検知のノウハウを反映してカスタムシグネチャを随時強化している。従って、公開済みの攻撃手法を変化させた攻撃にも、早期の対応が可能である。つまり、SOCサービスが緊急時にセキュリティデバイスを正しく運用できることや、専用シグネチャを早期に適用することが、被害防止の対策となる。

脆弱性公開から攻撃の発生までの時間は非常に短く、企業は限られた時間の中で暫定対策を完了させる必要がある。自社のビジネスにとってコアとなる業務に専念するためにも、CSIRTはSOCサービスを活用すべきである。■