3. 脆弱性管理について

要約

- 脆弱性管理とは、システムで稼働するソフトウェアの脆弱性を特定し、修正など必要な対策を講じるプロセスのことで、昨今のランサム攻撃の台頭などにより重要性が増している。
- 脆弱性管理に用いられる指標・フレームワークである「CVSS」「KEV」「EPSS」「SSVC」の概要とそれぞれの有用性・課題について、および脆弱性管理の今後について解説する。

脆弱性管理とは

脆弱性管理は、システムで稼働するソフトウェアの脆弱性を特定し、アプリケーションの修正やパッチの適用などの必要な対策を講じる一連のプロセスのことです。脆弱性管理は、セキュリティリスクを低減し、システムやデータの安全性を確保するため、継続的に実施する必要がある重要な活動です。

脆弱性管理は、一般的に以下の表のようなプロセスで実施されます。

項番	プロセス	プロセス概要
1	情報収集・発見	最新の脆弱性情報を幅広く収集する。収集においては、ベンダーサイト、セキュリティ情報サイトからの情報に加え、JPCERT/CC、IPA、米国 CISA（Cybersecurity and Infrastructure Security Agency：サイバーセキュリティ・インフラセキュリティ庁）などからの注意喚起情報にもアンテナを張る必要がある。
2	分類・評価	収集した脆弱性情報について、自組織に関係するものであるか、分類・評価する。
3	方針決定	分類・評価された脆弱性について、トリアージ(*1)を行い、脆弱性対応の方針・スケジュールを決定する。脆弱性対応のリソースは限られることから、全ての脆弱性に対して一律に対応することは現実的ではない。リスク受容を含めた実効性のある対応を効率的に行うためにトリアージが重要となる。
4	適用	決定した方針に従い、「修復（アップデート）、軽減（緩和策実施）、リスク受容」の対応を実施する。

出典：大和総研作成

脆弱性管理においては、上記のプロセスに加え、システムの定期的な監視と評価が必要です。加えて、システムやソフトウェアの変更、新たな脆弱性の出現に備えて、定期的な脆弱性スキャンやペネトレーションテストを行うことも推奨されます。昨今では、効率的なセキュリティ対策・脆弱性管理を推進するために、インターネットからアクセス可能な IT 資産を調査・管理する ASM と呼ばれるキーワードが注目されています。ASM については、本冊子の第 3 部-2.「ASM（Attack Surface Management）の動向について」で詳しく紹介していますので、ご参照ください。

なお、脆弱性管理に先立ち、システムで稼働しているソフトウェアを特定・可視化し把握する必要があります。把握していないソフトウェアの脆弱性に対処することは、当然ながら困難となります。もし、ソフトウェアの把握が困難である場合は、セキュリティベンダーによる脆弱性診断の受診やツールの使用などが推奨されます。脆弱性管理は、セキュリティを継続的に向上させるために欠かせないプロセスです。脆弱性管理の運用には専門的な知識と経験が必要ですが、適切に実施することでセキュリティリスクを最小限に抑え、システムやデータの安全性を確保することが可能となります。

(*1) トリアージ（triage）：一般的には、災害発生時などにおいて傷病者の緊急度や重症度に応じて治療優先順位を決めることです。サイバーセキュリティ対策においては、当該脆弱性に対して重要性や緊急度を見極め対応の優先順位を決定する意味合いで使用されます。

脆弱性管理の重要性が増した背景

従来ソフトウェアの脆弱性対応は、たとえば後述の CVSS スコアが「7.0 以上の脆弱性について全て対応する」といった運用が主流でした。しかし、近年 CVSS の対象となる脆弱性が急増し、報告された脆弱性全てに対応するのは人的リソースの不足などにより困難になりました。加えて、記憶に新しい 2021 年の Apache Log4j の脆弱性を悪用する攻撃や、ランサム攻撃の台頭などで、脆弱性対応の緊急性も増しており、迅速かつ効率的な対処が必要になりました。このような状況では、「CVSS スコア 7.0 以上の脆弱性は全て対応する」といった単純な視点だけでなく、たとえば PoC コード(*1)の存在や、悪用の状況、システムの設置状況などの新たな視点を考慮した上で、総合的に脆弱性管理を行う必要があります。

脆弱性管理に用いられる代表的な指標・フレームワークについて（CVSS、KEV、EPSS、SSVC）

脆弱性管理の指標としては、「CVSS」の活用が一般的ですが、「CVSS」と併せてここ数年注目されている指標である「KEV」「EPSS」と、昨今注目の脆弱性管理フレームワークである「SSVC」を紹介します。

CVSS （Common Vulnerability Scoring System：共通脆弱性評価システム）

脆弱性管理において広く活用されている指標で、脆弱性の深刻度を数値化し、それに基づいて対策や優先付けを行うために使用される、国際的な指標です。CVSS は、脆弱性の影響度、攻撃の容易さ、攻撃の範囲などの要素を考慮して、ベンダーに依存しない中立的な基準でスコアを算出します。スコアは 0～10.0 の範囲で数値化され、高いスコアほど脆弱性の深刻度が高いことを示し、客観的に評価することが可能です。CVSS はセキュリティ専門家や組織にとって重要な指標であり、セキュリティの脆弱性を効果的に管理するために活用されています。なお、CVSS については、『DIR SOC Quarterly vol.7 2024 spring(*2)』で詳しく取り上げています。

KEV （Known Exploited Vulnerabilities Catalog）

米国 CISA が公開している、実際に攻撃に悪用された脆弱性のリスト(*3)です。KEV に登録されるには、「(1)CVE ID が割り当てられていること」、「(2)悪用されている証拠があること」、「(3)ベンダーが提供するパッチやアップデートなど、脆弱性に対する明確な修復アクションがあること」の三つの条件を満たす必要があります。KEV に登録された脆弱性については、リスクが非常に高く速やかに対策を講じる必要があります。

EPSS （Exploit Prediction Scoring System）

FIRST(Forum of Incident Response and Security Teams)が開発した、脆弱性対応の優先度を判断するための指標(*4)です。EPSS は、EPSS Probability(EPSS スコア)と、EPSS Percentile(EPSS パーセンタイル)の二つで構成されます。EPSS スコアは、今後 30 日以内に脆弱性が悪用される可能性を独自の機械学習モデルに基づき 0～1(0～100%)のスコアで算出します。EPSS パーセンタイルは、当該脆弱性の EPSS スコア全体におけるランクを表します。たとえば EPSS パーセンタイルが 0.90 の脆弱性は、当該脆弱性より EPSS スコアが低い脆弱性が 90%存在することを表します。EPSS スコアは、「脆弱性の天気予報」に近いイメージです。CVSS が脆弱性そのものの深刻度を評価するのに対して、EPSS は脆弱性が悪用される可能性を算出する点が異なります。

(*1) Proof of Concept(概念実証)コード：脆弱性の存在や悪用可能性を証明するための実証コードのことです。

(*2) CVSS の歴史と最新版(v4.0)での改善点（『DIR SOC Quarterly vol.7 2024 spring』 pp.17-20）

(*3) CISA『Known Exploited Vulnerabilities Catalog』

(*4) FIRST『Exploit Prediction Scoring System』

SSVC　(Stakeholder-Specific Vulnerability Categorization)

米国カーネギーメロン大学ソフトウェア工学研究所と米国 CISA と共同で作成された脆弱性管理フレームワーク(*1)です。脆弱性の有する技術的な深刻度だけでなく、どのように対策するかを決定することが可能となります。SSVC では、文字通りステークホルダー(サプライヤー、デプロイヤー、コーディネーター)ごとに決定木を用いて、「Exploitation(脆弱性の悪用状況)」、「Exposure(システムの露出度)」、「Utility(悪用の有用性)」、「Human Impact(攻撃によるインパクト)」を基に、脆弱性へのアクションを、「Immediate(即時対応)」、「Out-of-Cycle(通常よりも早く、緩和策・改善策を適用)」、「Scheduled(定例のメンテナンス時に対応)」、「Defer(現在は対応不要)」として決定します。SSVC は CVSS などの指標だけでは不足する点を補完するフレームワークであり、昨今は「脱 CVSS」に向けての一手法として注目されています。

各指標・フレームワークの有用性・課題

前述の各指標・フレームワークには、以下の表に示されるような有用性・課題があります。各指標の有用性と課題を理解した上で、複数の指標を併用して脆弱性管理を行うことが望ましいものと考えられます。

用語	有用性	課題
CVSS	・脆弱性の深刻度を定量的に評価できる。 ・ベンダーに依存しない中立的な評価基準である。	・脆弱性の理論上の深刻度を表現したものであり、悪用の状況などリアルタイムの脅威についての考慮が不十分である。
KEV	・実際に悪用された脆弱性のリストである。 ・米国の政府機関である CISA が公開したリストであり、米国政府機関では期日までに対応が求められるなど精度が高い。	・日本独自の製品などは掲載される期待が薄い。 ・掲載された脆弱性は、CVE ID が付与された脆弱性の 0.5%程度と少ない。
EPSS	・今後 30 日以内に脆弱性が悪用される蓋然性(確率)をスコア化しており、攻撃発生の予測が可能となる。 ・当該脆弱性における脅威情報の取得が困難な場合でも脅威を簡易的に評価できる。	・予測には機械学習などが用いられているが、モデルの詳細が開示されておらずスコアの説明が困難。また、現時点では精度が必ずしも高くない。 ・既存の攻撃手法を基に算出しており、未知の攻撃や新たな攻撃手法に対する予測は困難である。 ・EPSS を管理する FIRST が米国中心のフォーラムである性質上、日本独自の製品などは脅威情報の不足によりスコアが低く出る傾向がある。
SSVC	・脆弱性に対してどのように対応すべきかの対応方針を決定できる。 ・ステークホルダーごとに対応方針を決定できる。	・決定木のパラメーターや評価基準が組織やシステム環境により異なるため、各関係者と十分な意思共有を図る必要があるなど運用開始までのハードルが高い。

出典:大和総研作成

脆弱性管理の今後について

システムの脆弱性については、昨今のゼロトラストセキュリティモデルやマイクロセグメンテーションなどの推進により、機器個別のアクセス制御が強化され、当該システムへの攻撃自体が抑制される方向に進んでいます。これに加え、AI の活用などにより、脆弱性の検出と対応についても自動化が進むものと想定されます。現時点でも SOAR(*2)と呼ばれるソリューションの中で一部の対応について自動化が実現されています。

脆弱性情報が増えるとシステム部門の対応負荷が上がるため、自動化などにより負荷を下げる必要があります。そのためにも適切な指標を活用し、自組織のシステムの状態(インターネット接続の有無、動作権限、攻撃緩和策の有無など)を踏まえた適切な脅威評価とトリアージを行い、必要な対策を速やかに実施することが今後ますます重要になるものと考えられます。

(土田　将弘)

(*1) CISA『Stakeholder-Specific Vulnerability Categorization (SSVC)』

(*2) Security Orchestration, Automation and Response:「脅威と脆弱性の管理」、「セキュリティインシデント対応」、「セキュリティ運用の自動化」の三つの主要なソフトウェア機能を実現する製品・サービスのことです。