4. NCA、「脆弱性管理の手引書 システム管理者編1.0 版」を公開

要約

- 一般社団法人 日本シーサート協議会(NCA)が、『脆弱性管理の手引書』を公開した。公開された手引書は、システム管理者編で、「ユーザ(システム管理者)」の立場での脆弱性管理手法について解説されている。本手引書について脆弱性管理の流れを中心に紹介する。
- 本手引書は、脆弱性管理の実施に際して必要な事項が体系的に整理・解説されており有用である。

概要

一般社団法人 日本シーサート協議会(NCA)は、2024 年 10 月 25 日、『脆弱性管理の手引書 システム管理者編 1.0 版』(以下、「本手引書」)を公開しました(*1)。NCA の脆弱性管理ワーキンググループでは、脆弱性管理に必要な事項を立場ごとに、ユーザ(システム管理者)、IT サービス/製品の提供者、システムインテグレータ(SIer)の三つに分類しており、本手引書は、「ユーザ(システム管理者)」の立場での脆弱性管理について解説されています。なお、本手引書の活用に際しては、ある程度の IT 資産の識別(IT 資産管理)がされていることが前提となります。また、現時点ではインシデント対応はスコープ外とされています。

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や設定/設計の脆弱性を特定し、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。

脆弱性管理については、本冊子前号の DIR SOC Quarterly vol.9 2024 autumn「脆弱性管理について」(*2)で詳しく紹介しております。本手引書と併せてご参照ください。

本手引書における脆弱性管理の流れについて

本手引書では、システム管理者観点での脆弱性管理を、下図の流れで実施するよう解説されています。

出典:NCA『脆弱性管理の手引書 システム管理者編 1.0 版』から転載

(*1) NCA『「脆弱性管理の手引書 システム管理者編 1.0 版」を公開』

(*2) 大和総研『脆弱性管理について』(『DIR SOC Quarterly vol.9 2024 autumn』pp.20-22)

各項目における実施概要は下表の通りです。詳細につきましては、本手引書をご参照ください。

項番	項目	実施概要（抜粋）
1	脆弱性管理対象の識別	・脆弱性管理対象の識別の際には、「ソフトウェア名/製品名」、「バージョン情報」、「機能カテゴリ/保持情報」、「構成」、「外部アクセス可否・ポート情報」、「設置場所」、「管理者/責任範囲」の事項を把握することが必要。 ・ ソフトウェア情報の確認には仕様書、設計書等の確認、担当者へのヒアリングが必要。 ・ 管理区分の例→「サービス・機能を起点」、「ソフトウェアを起点」、「システム・サーバを起点」、「その他」 ※どのような管理区分を起点とするかは、各組織の既存の IT 資産管理方法、責任分担、管理対象の規模/種類を考慮して検討する必要がある。 ・ 脆弱性管理対象の識別において、SBOM(*1)を活用することを期待。
2	脆弱性情報の内容把握 ・ソフトウェア/製品の脆弱性の把握 ・設定/設計の脆弱性の把握	・ 脆弱性情報は「ソフトウェア/製品の脆弱性」、「設定/設計の脆弱性」に大別できる。 ・ ソフトウェア/製品の脆弱性の把握には、「CVE・脆弱性の名称」、「対象ソフトウェア・製品」、「対象バージョン」、「脆弱性発露の条件」、「影響」、「対応策・対応手順」、「緩和策・回避策」の事項を押さえた検査が必要である。 ・ソフトウェア/製品の脆弱性を把握する際の情報収集には、「セキュリティ関連の団体/組織から」、「ソフトウェア/製品の開発ベンダから」、「セキュリティベンダが運営するサイトから」、「脆弱性情報配信サービス」のような手段が考えられる。 ・設定/設計の脆弱性の把握には、「保持/流通情報」、「ユーザ権限（管理/一般）」、「アプリケーション ミドル・OS 設定」、「NW 設定/設計」、「設置場所」の事項を押さえた検査が必要である。 ・脆弱性の内容把握に、ペンテストツール、ASM(*2)、CSPM(*3)などの活用について紹介。 ・デフォルト設定と推奨設定について解説。
3	組織におけるリスク評価	・ 大量に報告される脆弱性のすべてに対応するのは非現実的であり、各組織においてどのような脆弱性に対応するかの判断基準が必要。報告される脆弱性に対する絞り込みの基準例としては、「共通の指標」および「脆弱性スキャナー/脆弱性 DB サービス」によるものがある。 ・リスク評価基準は各組織のリスク選好性・業務特性によって異なるが、「リスクの発生可能性」と「想定被害」を軸に決定する方法を例示。 ・CVSS(*4)、EPSS(*4)等を活用したリスク評価基準も考えられる。 ・リスク評価の基準については事前に経営層との合意を取ることが望ましい。 ・リスク評価結果については具体的なアクションに結び付いた表現が必要。 ・「把握した情報」と「事前に定めた判断基準」を照らし合わせ、リスク評価を実施する。 ・ KEV(*4)を参照することでリスク評価をより効果的に行うことができる。
4	対処・対策	・ 取りうる対処・対策について、把握事項（「実施内容（パッチの適用、等）」、「効果（脆弱性の解消、発生可能性の低減、等）」、「対処案実施の影響（不明のため要検証、等）」、「実施可能スケジュール（〇月×日（検証後）、等）」）を押さえ、リスク評価がどう変わるのかを確認する。 ・実施する対処計画の決定に関しては、関係者とのコミュニケーションを通して実施の影響、実施可能スケジュールを検討する必要がある。業務への影響等を考慮するとリスク解消する対処がすぐには実施できないことも想定すること。リスクを緩和する暫定対処策も含めて対処計画を検討する必要がある。 ・影響が広範囲・深刻な脆弱性対応においては、通常時とは異なる対応態勢（例：CISO をトップ、セキュリティ部門の長をトップ、システム担当チームとセキュリティ担当者で対応）が必要。
–	脆弱性管理とガバナンス	・項番 1～4 の脆弱性管理の流れを継続的に実施し、実効性の維持・改善をするには組織的なガバナンスが必要。「組織における脆弱性管理の位置づけ、判断基準、緊急時の態勢に関する経営層の合意」、「必要なスキルセットの整理と人材の育成」、「脆弱性管理に必要な手順の整理」、「脆弱性管理に必要なツール（連絡手段、管理・効率化ツール）の整備」の事項を文書化し定期的に見直しを図ることが望ましい。 ・SSVC(*4)の導入により対応者の立場や環境要因を加味して対処の優先順位付けを行うことができる。ダッシュボード等を活用した効率的な管理の検討も必要である。

出典：NCA『脆弱性管理の手引書 システム管理者編 1.0 版』を基に大和総研作成

最後に

本手引書は、昨今重要性が増している脆弱性管理の実施に際して必要な事項が体系的に整理・解説されています。セキュリティ担当者、特に脆弱性管理の担当者の方は内容をご確認いただくことをお勧めします。

（土田　将弘）

(*1) 大和総研『サプライチェーンリスクマネジメントを支援する SBOM とは？背景や導入の注意点を解説』

(*2) 大和総研『ASM（Attack Surface Management）の動向について』（『DIR SOC Quarterly vol.9 2024 autumn』pp.17-19）

(*3) 大和総研『クラウドセキュリティポスチュア管理（CSPM）』

(*4) 大和総研『脆弱性管理について』（『DIR SOC Quarterly vol.9 2024 autumn』pp.20-22）