ISOG-J WG6 脆弱性管理推進チーム 概要

2026-07-22

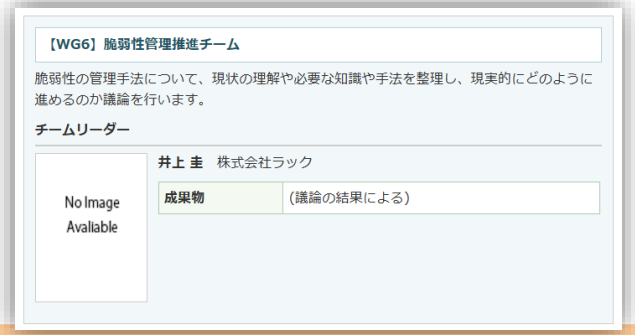
井上圭
株式会社ラック

ISOG-J とは

- 日本セキュリティオペレーション事業者協議会
  - the Information Security Operation providers Group Japan
  - 2008年創立、2023年9月現在 63組織が加盟
  - プロのセキュリティオペレーター、事業者の集まり
  - 業界の発展のために課題を議論したり、互いに情報を出し合うことで外部へ成果を発表する団体です
  - 親団体は日本ネットワークセキュリティ協会(JNSA)
- http://isog-j.org/
  - Facebook ページ: /isogj
  - ISOG-J の読み方: いそぐじぇい

脆弱性管理推進チームの活動の位置づけ

- ISOG-J WG6配下の活動
- 2025年度にメンバーを募集して活動中
- 脆弱性管理の現状整理、必要な知識手法を検討
- 一番脆弱と思われる中小企業に対する「脆弱性管理の始め方」という観点で整理中
- 2026年度内に成果を公開予定



なぜ脆弱性管理を検討するのか

脆弱性管理は更新作業だけではない

- 何を使っているかを把握する
- 関係する脆弱性を確認する
- 対応の優先順位を決める
- 業務影響を考えて実行する
- 対応しない理由も記録する
- 定期的に見直して継続する

大企業はともかく、
中小企業においては
すべて対応するのは
難しい内容

1. はじめに — 本書の目的と背景

1.1 本書の目的

本書は、中小企業が自社の現有システムと限られた人員・予算を前提に、脆弱性管理を小さく始め、継続できる形へ育てていくための実践ガイドです。ここでいう脆弱性管理とは、単にソフトウェアを更新する作業ではなく、自社の資産、関係する弱点、優先して下げるべ記録して見直す活動を指します。

中小企業では、専任のセキュリティ担当者や十分な予算を確保することが難し当、総務、管理部門、業務部門が兼任で対応していることが少なくありません管理は「何から始めればよいか分からない」「更新すると業務が止まるかもし に何を依頼できるか分からない」という理由で後回しになりやすい活動です。

本書は、そのような組織が、高価な脆弱性管理製品や高度な専門運用を前提に囲から取り組みを始められるようにすることを目的としています。主な読者は する担当者、情シス・総務などの兼任担当者、経営層に説明する立場の管理者

重視するのは、「すべての脆弱性を直す」ことではありません。限られた時間と ら順にリスクを下げ、対応するもの、計画的に対応するもの、受容して見直す す。対応しない場合でも、気づかずに放置するのではなく、理由と再評価の時 重要です。

1.2 なぜ中小企業に脆弱性管理が必要なのか

中小企業も、サイバー攻撃や不正利用の対象になり得ます。攻撃者は企業規模 ではありません。インターネットに公開されたVPN機器、Webサイト、クラウ フトウェア、設定不備のある機器など、侵入や悪用の入口になり得るものを探 狙われる場合だけでなく、取引先や関連企業へ侵入するための踏み台として利 ます。

取引先との接続、VPN、クラウド、外部委託、ファイル共有やメールを介した と、自社の管理範囲は社内のPCやサーバだけでは済まなくなります。重要な情 扱う場合や、Webサイトの運用を委託する場合でも、事故が起きれば自社の事 に影響が及ぶ可能性があります。

一方で、脆弱性が放置される背景には、担当者の怠慢ではなく、仕組みの不足 べき資産が一覧化されていない、情報源が決まっていない、業務停止を伴う更 ない、委託先との役割分担が曖昧である、といった状態では継続的な対応は困

1.5 本書の構成

本書は、第2章から第6章、付録、補足コラムで構成しま で、必要な章から読み進められるようにしています。

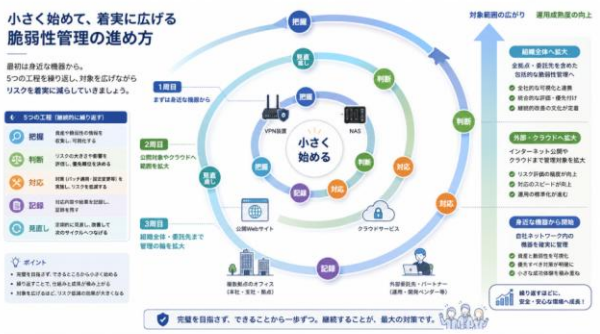
構成	内容
第2章： 脆弱性管理とは何か	脆弱性管理の基本的な考 リスク、対応方針を整理
第3章：実践ステップ	STEP1からSTEP5までの 最初の1周で作る成果物
第4章：ケーススタディ	第3章のSTEPを、複数の
第5章： 経営層への説明と合意形成	脆弱性管理を事業リスク 優先順位、例外基準、人 協力体制を合意する考え
第6章：おわりに	本書全体を振り返り、 最初の1周を次の1周につ 脆弱性管理を一度きりの 継続的な運用として定着
付録	用語集、情報源一覧、参 資産台帳、情報源リスト 脆弱性対応記録、 各種レビュー記録のテン
補足コラム	IPA情報セキュリティ6か すべての脆弱性に対応す 国際標準との関係などを

はじめて読む場合の推奨順は、目的によって異なります。 第3章の順に読むと、本書の考え方と実践手順を把握でき を読み、必要に応じて第4章を参照してください。経営層 内容を確認したうえで、第5章を読むと説明の組み立てがしやすくなります。背景知識を深めたい人 は、第2章、補足コラム、付録の順に読むと、用語や関連資料との位置づけを確認できます。

6. おわりに — 最初の1周を、次の1周につなげる

本書では、中小企業が限られた人員・予算の中で脆弱性管理を始めるための考え方と手順を整理しました。脆弱性管理は、すべての脆弱性を一度に直す活動ではありません。自社にとって重要な資産を把握し、関係する脆弱性情報を確認し、対応するもの、計画的に対応するもの、受容して再評価するものを分け、記録し、見直していく活動です。

最初の1周では、十分に整っていない部分が残っていても構いません。資産台帳に不明な項目がある、委託先との役割がまだ曖昧である、受容した案件の判断に迷いが残る、といった状態は、脆弱性管理を始めた組織では自然に発生します。重要なのは、それらを担当者の記憶や個人の努力に閉じ込めず、次に確認すべき課題として残すことです。



本書で示した初回合意メモ、資産台帳、情報源リスト、突合記録、脆弱性対応記録、月次レビュー記録、四半期レビュー記録、年次見直しメモは、いずれも立派な書類を作ることが目的ではありません。次に同じ確認を行うときに、何を見ればよいか、誰に相談すればよいか、前回どのように判断したかを分かるようにするための道具です。

脆弱性管理を継続するうえで大切なのは、完璧な体制を待たないことです。最初は、公開しているVPN機器、重要なNAS、外部公開Webサイト、主要なクラウドサービスなど、把握できている重要な範囲から始めます。その結果を月次・四半期・年次で見直し、次の1周で対象を少しずつ広げます。こうした小さな繰り返しが、組織としての脆弱性管理の土台になります。

なぜ中小企業向けなのか

検討対象を中小企業へ具体化

- 専任担当者がいないことが多い
- 情シス・総務などが兼任
- 高価な製品の導入は難しい
- 委託先への依存度が高い
- 全ての対応は困難
- 現実的な始め方が必要　←ここのガイドが少ない

何もしていない企業も多く、「まずは始めた」状態に持っていく必要がある

作成しているガイドの基本方針

「全部直す」ことを目標にしない

- 重要な資産から始める
- 把握できる範囲から始める
- 緊急・計画・受容を分ける
- 対応しない理由も記載する
- 一度で完成させようとしない
- 見直しながら対象を広げる

小さく始めて、
次の一周へつなげる

脆弱性管理を始める5つのSTEP

小さく始める脆弱性管理の5つのSTEP

1. 開始の合意
2. 資産の把握
3. 脆弱性情報の把握
4. 優先度の判断と対応
5. 振り返りと改善

一周ごとに対象と運用を
広げていける構成

成果物と今後の予定

- 公開を予定している成果物
- 中小企業向け実践ガイド
- ケーススタディ
- 資産台帳等のテンプレート
- 脆弱性情報源の一覧
- 参考資料や用語集

現場で最初の一周を始められる成果物へ

概要説明は以上です。
ご意見等ありましたら、お声がけ下さい。