ISOG-J 2022年度活動報告

JNSA活動報告会

2023/6/7

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6月現在 62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

現在活動中のWGなど

- セキュリティオペレーションガイドラインWG(WG1)
- セキュリティオペレーション技術WG(WG2)
- セキュリティオペレーション認知向上・普及啓発WG(WG4)
- セキュリティオペレーション連携WG(WG6)
- 新技術とオペレーションプロジェクト

セキュリティオペレーションガイドラインWG(WG1)

リーダー：上野宣さん（株式会社トライコーダ）

活動概要

- セキュアWebアプリケーション要件定義書、脆弱性診断講座スキルマッププロジェクトなどの各種成果物の次バージョン作成
- Webシステム/Webアプリケーションセキュリティ要件書の改訂作業
- アジャイル開発における脆弱性診断の検討
- 脆弱性診断士の倫理綱領についての検討
- 新技術に対する脆弱性診断手法の検討

セキュリティオペレーションガイドラインWG(WG1)

2022年度活動実績

4/18, 5/10, 5/17, 5/23, 6/13, 6/14, 6/20,
7/12, 7/19, 8/23, 9/13, 10/11, 11/22, 1/17

成果物

6/23, Webシステム/Webアプリケーションセキュリティ要件書 Ver.4.0

7/5, アジャイル開発におけるセキュリティ|パターン・ランゲージ

（本発表後半で紹介します）

セキュリティオペレーション技術WG(WG2)

リーダー：川口洋さん（株式会社川口設計）

活動概要

- 最新の技術動向を調査し、最適なセキュリティオペレーション技術を探求、技術者の交流を図る。
- 各社持ち回りで勉強会を開催

2022年度活動実績
5/18，7/22，9/9

セキュリティオペレーション認知向上・普及啓発WG(WG4)

リーダー：阿部慎司さん
（GMOサイバーセキュリティ byイエラエ株式会社）

活動概要

- 新型コロナウイルス感染拡大に関する緊急アンケートの実施、結果の集計
- 運営会議、事業者連絡会検討
- 警察庁様不正アクセス行為対策等の実施調査に関する意見交換会
- 新規の活動について検討

2022年度活動実績
6/1， 6/30， 10/17， 11/30, 12/26， 1/10

セキュリティオペレーション連携WG(WG6)

リーダー：武井滋紀さん（NTTテクノクロス株式会社）

活動概要

- セキュリティオペレーション事業者間の共通の課題の認識及び、課題の対応や対処について検討を行い、必要に応じて成果物を外部への公開を行う。
- セキュリティ対応組織の教科書の改版
- ISOG-J内アンケート実施
- InternetWeekなどにおける各種発表や講演

セキュリティオペレーション連携WG(WG6)

2022年度活動実績
4/18, 6/3, 9/29, 10/26, 11/21, 12/23, 2/17

成果物

2/13, セキュリティ対応組織の教科書　第3.0版

（本発表後半で紹介します）

新技術とオペレーションプロジェクト

リーダー：ももいやすなりさん（株式会社IIJ）、亀田勇歩さん(SCSK株式会社)

活動概要

- 各種技術トピックとセキュリティオペレーションに対する影響の調査

2022年度活動実績
4/21，5/23

成果物： Webシステム/Webアプリケーションセキュリティ要件書 Ver.4.0

- 2022年6月23日、WG1より公開
- 概要
  - 安全なWebアプリケーションの開発に必要なセキュリティ要件書
  - 発注者、開発者、テスト実施者、セキュリティ専門家、消費者が活用することで、以下のことを達成することを目的としています。
    - 開発会社・開発者に安全なWebシステム／Webアプリケーションを開発してもらうこと
    - 開発会社と発注者の瑕疵担保契約の責任分解点を明確にすること
    - 要求仕様やRFP（提案依頼書）として利用し、要件定義書に組み込むことができるセキュリティ要件として活用していただくこと
- 見どころ
  - 2013年の初版から10年継続リリースしています！

本ドキュメントがカバーする範囲

- 本要件書はWebシステム／Webアプリケーションに関して一般的に盛り込むべきだと考えられるセキュリティ要件について記載
  - 「認証・認可」「セッション管理」「入力処理」「出力処理」「HTTPS」「Cookie」など
- 開発言語やフレームワークなどに依存することなく利用できる
  - ネットワークやホストレベル、運用などに関するセキュリティ要件については記載なし
- 対象とするWebシステム／Webアプリケーションは、インターネット・イントラネット問わず公開するシステムで、特定多数または不特定多数のユーザーが利用するシステムを想定
  - 特に認証を必要とするシステムが主なターゲット
- 本要件書はセキュリティ要件としての利用しやすさを優先して記載
  - 一般的であろうというシステムを想定し、例外の記載を少なくしたセキュリティ要件
  - 要件定義書に記載する内容は開発者と折衝することを想定

成果物：アジャイル開発におけるセキュリティ|パターン・ランゲージ

- 2022年7月5日、WG1より公開
- 概要
  - 『アジャイル開発におけるセキュリティ | パターン・ランゲージ』は、「アジャイル開発においてセキュリティをどのように担保するか」のヒントを過去の成功事例などを基にパターン・ランゲージという形式で解説したもの
- 見どころ
  - ウォーターフォール開発においては、要件定義のフェーズではセキュリティ要件があり、それに沿ったセキュアな設計や実装が行われ、脆弱性診断を行ってからリリースされるが、アジャイル開発ではそれらのフェーズが明確でないこともあり、セキュリティを如何に担保するかということが疎かになることもある
  - アジャイル開発のどの段階でどういった取り組みをすることでセキュリティを担保できるかといったヒントを得ることができる

項目

- チームビルディング
  - 1. セキュリティ・チャンピオンの役割定義と任命
  - 2. 各自がセキュリティに責任を持ったチームビルディング
  - 3. セキュリティ向上のためのルール整備
  - 4. セキュリティスキル底上げのための開発者向けトレーニング
- 開発計画・プロジェクト計画
  - 5. スプリント成果物に必要なセキュリティ要件の決定
  - 6. リスクに応じた脆弱性対応方針の策定
  - 7. 脆弱性トリアージ
- セキュリティテスト
  - 8. セキュリティテストの実施タイミングと方針検討
  - 9. スプリント内で実施するテスト内容の策定
  - 10. 利用環境の脆弱性管理
  - 11. セキュリティテストの自動化
- セキュリティ品質向上
  - 12. セキュリティの継続的向上のためのふりかえり

- それぞれの項目についてパターン・ランゲージを使い、項目の「概要」として「どういったことを目的とするものか」、「状況」では「どういった組織やチームが参考にすべきものか」、そこで起こる「解決したい問題」、それに対する「解決策」を提示

成果物：細かすぎるけど伝わってほしい脆弱性診断手法ドキュメント

- 2023年4月10日、WG1（新技術に対する診断手法分科会）より公開
- 概要
  - さまざまな技術に関する脆弱性診断手法ドキュメント
- 見どころ
  - クロスサイトスクリプティングやSQL Injectionなどの著名な脆弱性は診断手法や対策なども浸透し、日本語で読める良質なドキュメントが複数ある
  - 本ドキュメントでは、これらの脆弱性ではなく、一般に診断が困難であったり特有の確認方法が必要となるような脆弱性についてターゲットを絞って記載

項目

- NoSQL Injection
- OAuth/OpenID Connect
- Prototype Pollution
- TOCTOU/レースコンディション
- クラウドサービスにおけるWebサービスにまつわる脆弱性
  - IDaaSの活用に起因する脆弱性とその悪用
    - EDoS(Economic Denial of Sustainability) - IDaaS
    - アプリケーションの権限に関するカスタム属性の変更 - IDaaS
    - デフォルトエラーに起因するユーザーの開示 - IDaaS
    - 意図しないサインアップ経路の存在 - IDaaS
  - FaaSにおける設定不備と脆弱性の悪用
  - Webアプリケーションの脆弱性を利用した認証情報の窃取
  - クラウドストレージサービスにおける設定不備
- Web Cache Poisoning

成果物：セキュリティ対応組織の教科書　第3.0版

- 2023年2月13日、WG6より公開
- 概要
  - ビジネスリスクに対応するためのサイバーディフェンスセンター、セキュリティ統括を実現するフレームワークを活用した、新たなセキュリティ対応組織のために改版された教科書
- 見どころ
  - セキュリティ対応組織の教科書第2.1版からおよそ5年ぶりの改版
  - ITU-T勧告X.1060、TTC標準JT-X1060に準拠
  - 実用書としてフレームワークに記載しきれていない部分を多数加筆
  - 世界最速でリリースされた実用書と言って過言ではない

ポイント

- 対象者は、CISOやセキュリティ責任者。「これからのセキュリティ組織をどう構築するか」を考える人。
  - 経済産業省　サイバーセキュリティ経営ガイドライン　とマッピングする部分もあるので、対象者は近い
  - 既存の様々なドキュメントと組み合わせて組織づくりの参考にされたい
- セキュリティの組織でやるべき9つのカテゴリーと64のサービスがベストプラクティスとして整理されている
  - 実は2.1版の内容がX.1060に取り込まれてボリュームアップしたもの
- 継続的に組織を見直して改善することが明確になった