令和 2 年 12 月 1 日

一般社団法人コンピュータソフトウェア協会(CSAJ)
セキュリティ委員会/Software ISAC

ソフトウェア出荷判定セキュリティ基準チェックリストをバージョンアップ
新しく発見された脆弱性を追加するなど項目数・使いやすさが大幅 up

一般社団法人コンピュータソフトウェア協会（略称「CSAJ」、東京都港区赤坂）は、2016 年に公開した、パッケージソフトウェアや Web サービスのセキュリティ品質を向上させるための「ソフトウェア出荷判定セキュリティ基準チェックリスト」について、新しく発見された脆弱性に関する記述を追加するなど、内容を全面的に見直した「Ver.1.2」を発表しました。

＜開発プロセスに応じたセキュリティ要件は 48 項目から 113 項目へ＞

本チェックリストは初版が 2016 年に公開され、ソフトウェア開発を行う技術者や品質管理担当者より好評を博しておりましたが、4 年間の時を経て、「プロトコルやアルゴリズムに脆弱性が発見され推奨されなくなった」、「新たな脆弱性が発見された」、「利用者の要求に変化がみられた」、などの要因から、CSAJ セキュリティ委員会および Software ISAC メンバーにて全面的な見直しが図られました。
本チェックリストを活用することで、セキュリティをソフトウェア品質の一環として捉え、開発現場での仕様策定や出荷テストの際の評価項目として幅広く利用できるほか、技術者のスキルアップにも活用できる内容となっています。

チェックリストは、CSAJ の以下 Web サイトからダウンロードでき、クリエイティブコモンズライセンスに基づき、CSAJ 会員のみならず誰もが自由に利用でき、自社利用はもとより、改変や商用利用も可能となっています。

○「ソフトウェア出荷判定セキュリティ基準チェックリスト Ver.1.2」は、以下 URL よりダウンロードできます。

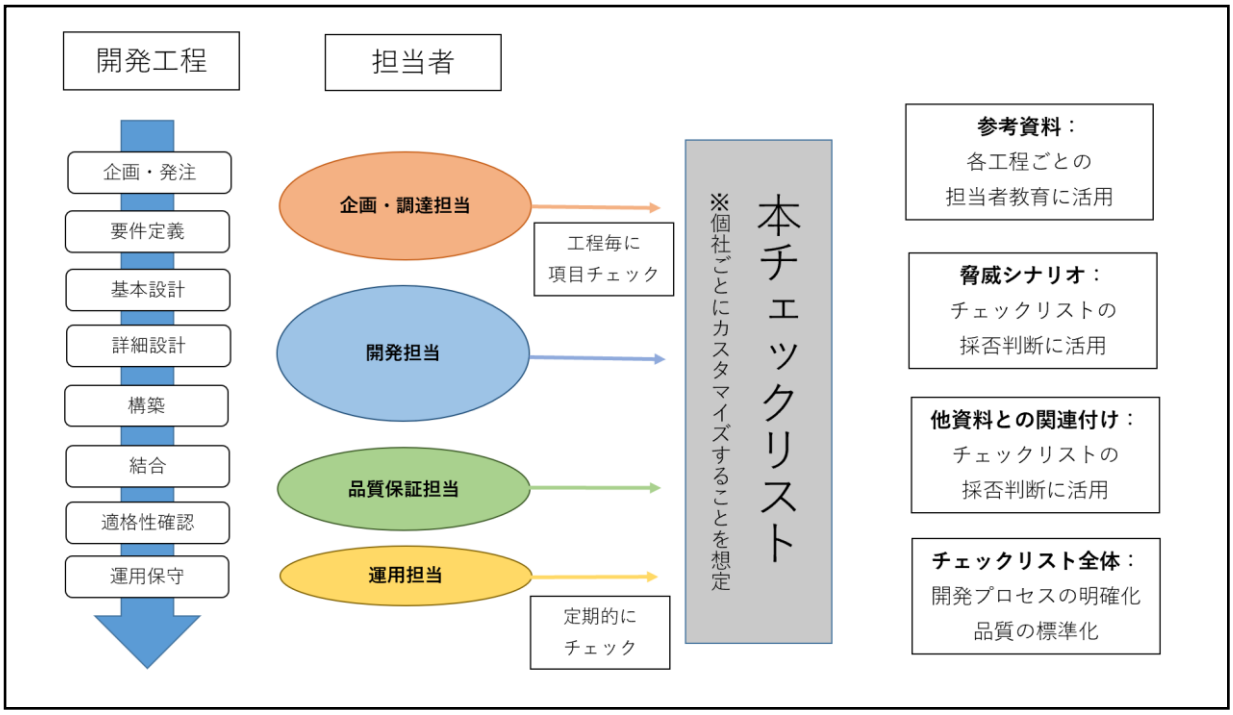
https://www.csaj.jp/NEWS/pr/201201_sec-release-decision.html

＜ソフトウェア開発のセキュリティ課題＞

ソフトウェアの脆弱性や不具合を狙ったサイバー攻撃は、近年ますます増加の様相を呈しています。さらにオリンピック・パラリンピックの開催を迎える 2021 年にはさらなる攻撃の増加が懸念されています。こうした中、ソフトウェア製品・サービスにセキュリティの問題が発生すると、企業の事業継続が困難になる可能性もあることから、製品・サービスのセキュリティ品質の維持は、ソフトウェア開発会社にとって大変重要な経営課題となっています。

＜セキュリティ品質を確保する管理対象項目と管理手法を定義＞

本チェックリストでは、ソフトウェア製品・サービスの企画、仕様策定、方式設計、詳細設計、テスト、運用に至るライフサイクルのなかで、一定レベルのセキュリティ品質を確保する観点から、管理対象項目と管理手法を定義しました。さらに、本バージョンでは、開発における各ステップ単位でチェックリストを作成することもできます。こうすることで、社内のエンジニアだけでなく、企画担当者や品質管理担当者、外部の協力会社も含めた、セキュリティ品質の管理が可視化でき、出荷されるソフトウェア製品・サービスの信頼性の一層の向上が期待できます。



<Ver.1.2 の特徴>

・開発段階ごとに分類されているので順を追って確認することが可能
・脅威シナリオの充実
　項目ごとに脅威シナリオが記載されており、その脅威シナリオを確認し、当該シナリオが該当しない、経営リスクに直結しないなどの判断に至れば除外可能
・項目ごとにテスト方法が記載されているので、なにをすべきかが明確
・項目ごとに関連付けられた参考文書（各種公開文書）の記載が充実しており、開発者自身でさらなる深掘りが可能

<Ver.1.2 の使い方>

　文書の中から、自社に必要な要件をチョイスする、自社プロダクト出荷時のチェックリストに適用する、あるいは、記載されているテスト方法を利用してチェック項目を確認する、といった使い方を想定していますが、その他に以下のような使い方も考えられます。
・次のステップに進む前のチェックに
　発注前/要件定義終了時/基本設計終了時/運用前/運用中に定期的にチェックが行える
・社内に公開、必要な開発成果物を明示
　開発に必要な成果物が開発者に伝わる/開発工程に必要なプロセスなどが明確に/社内の開発プロセスの標準化に利用
・社内のスキル向上に
　自社で採用したチェック項目の参考資料・脅威シナリオを確認し、脆弱性が発生する仕組み、対応方法、実際に脆弱性が発火したときの被害想定などができるようにする
・チェックリストを活用することで開発の各工程でやるべきことが明確になる
　公開されている文書に準拠しやすくセキュリティ対策のレベル感を判断しやすい
・スキルアップにも利用可能

なお、Software ISAC では、今後もこの「ソフトウェア出荷判定セキュリティ基準チェックリスト」を見直し、改善を継続していくため、本リストに対するご意見をお待ちしています。また、Software ISAC では、一緒に本リストの更新や各種活動を進めていくメンバーを募集しています。詳細は Web サイトをご参照ください。

○一般社団法人コンピュータソフトウェア協会（略称「CSAJ」）とは
自社で市場ニーズを分析し、企画、開発、商品化した既製ソフトウェア（企画開発型ソフトウェア）を販売、あるいはそれを利用したサービスを提供している企業を中心とした業界団体です。われわれ CSAJ は、「シンクタンク化」、「グローバル化」、「ビジネスチャンス拡大」の 3 つの方針を掲げ、イノベーションと IT 化の促進を通じて我が国経済の発展と国民生活の向上に寄与しています。

○Software ISAC とは
IoT デバイスの普及に伴い、サイバー空間の脅威は非常に高まっています。また、OSS の活用が進む上で、脆弱性ハンドリングはますます難しくなっています。開発者は 安全で安心なソフトウェアの提供をするために、脅威の手法や脆弱性情報を素早く入手する必要があります。そこで、セキュア開発や脆弱性管理の工数最適化や、ソフトウェアサプライチェーンの強靭化の研究を行い、安心・安全な日本への貢献を行う開発者のための情報交換基盤を提供することを目的に、CSAJ セキュリティ委員会の下部組織として発足しました。
以下、Software ISAC 公式 Website では、組織概要の詳細や規則についてもご覧いただけます。

https://softwareisac.jp/

■お問い合わせ先
一般社団法人コンピュータソフトウェア協会
事務局　担当：戸島、中野　E-mail：gyoumu1@csaj.jp　TEL：03-3560-8440
〒107-0052　東京都港区赤坂1-3-6 赤坂グレースビル4F　URL：https://www.csaj.jp/