「Software ISAC」の活動について

2019年11月11日

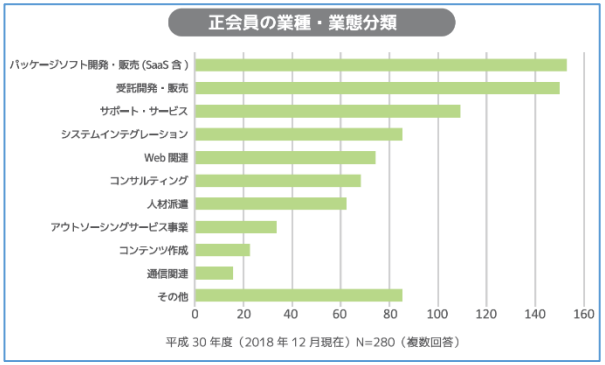
Software ISAC
（コンピュータソフトウェア協会）

agenda

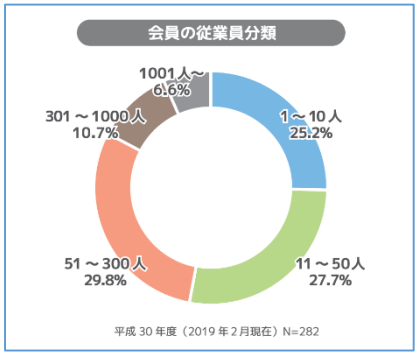
- Software ISACについて
- Topics
  - PSIRT Service Frameworkについて
  - ソフトウェア管理手法の検討について
- 最近の活動
  - ワーキンググループ活動

Software ISACについて

- Software ISAC (Information Sharing and Analysis Center)
  - 目的：　ソフトウェアのよりセキュアな開発や更新の促進
    ソフトウェア開発や脆弱性管理等の工数最適化
    日本のより安全・安心な社会への貢献
  - 実施概要
    - 国内ソフトウェア産業に必要な脆弱性・脅威情報等の集約、分析、展開
    - 開発の上流工程からのセキュリティ組み込み
    - 開発ソフトウェアに係る外部連携の支援
    - 脅威情報の早期把握と発見



- CSAJ
  - 団体名　一般社団法人コンピュータソフトウェア協会
  - 所在地　〒107-0052 東京都港区赤坂1-3-6　赤坂グレースビル
  - 会長　荻原 紀男 （株式会社豆蔵ホールディングス 代表取締役会長兼社長）
  - 設立年月　1986年（昭和61年）2月
  - 会員数　624社・団体（うち正会員499社、平成31年4月現在）



PSIRT Service Framework

PSIRT Services Framework

Version 1.0 Draft

日本語抄訳

日本語抄訳は Software ISAC(一般社団法人コンピュータソフトウェア協会)と一般社団法人 JPCERT コーディネーションセンターによって翻訳された後、Panasonic PSIRT と Sony PSIRT によってレビューされました。FIRST.Org は関係者の協力に深く感謝します。

https://www.first.org/education/FIRST_PSIRT_Services_Framework_v1.0_draft_ja.pdf

ソフトウェア管理手法の検討について

本TFにおける検討の方向性

- **ソフトウェア管理手法、脆弱性対応、OSSの利活用等**に関する検討を行う。

ソフトウェア管理手法の検討

- ソフトウェアの開発から、運用中の脆弱性発見まで
- 構成管理・脆弱性管理に求められるソフトウェア管理手法のあり方
- SBoM等ソフトウェア管理スキームの活用に求められる技術面・制度面の課題

第1回検討事項

脆弱性対応手法の検討

- 脆弱性が発見された場合のソフトウェアへの対応
- 脆弱性発覚時に必要な脆弱性への対応手法・体制のあり方
- 運用中システムへの脆弱性対応に求められる技術面・制度面の課題

OSSを利活用する際のビジネス的な側面の検討

- OSS利用に関連するライセンスや契約
- OSS活用のベストプラクティス／OSSコミュニティへの発信

次回以降検討予定事項

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/001_04_00.pdf

民法改正に伴う活動

- 経済産業省モデル契約
  - 2005年 東京証券取引所のシステムトラブルが発端
  - 2006年 産業構造審議会
    - 契約の不透明性を指摘、情報システム取引の可視化、信頼性向上につながる契約の在り方を提言
  - 2007年 METIモデル取引・契約書(第一版)
    - 対等に交渉力のあるユーザ・ベンダを想定し、ウォーターフォールモデルによる重要インフラ・企業基幹システムの受託開発、保守・運用
  - 2008年 METIモデル取引・契約書(追補版)
    - 中小企業・ベンダを想定し、パッケージ・SaaSのカスタマイズの受託開発・保守
  - 2009年
    - 判例研究（ソフトウェア情報センター）
    - 各団体での啓発普及活動

- 2020年 民法（債権法）改正
  - 改正の目的
    - 明治29年制定以来、120年間実質的な見直しがなく、社会の変化に対応するべく、過去の判例反映、実情にあわない条項の改正、学説と実務が通用している基本的なルールを明文化
  - 経産省DXレポート*の指摘をもとに、IPA社会基盤センター部会でモデル契約改訂の議論が開始
    - 改正法への対応
    - アジャイル開発契約の策定

* https://www.meti.go.jp/shingikai/mono_info_service/digital_transformation/20180907_report.html

ガイドライン策定における基本方針

- **ユーザーとベンダーが具体的な脅威とその対処方法を検討するためのベースを策定する**
- **実際の脅威に対して、攻撃数、攻撃の容易さで重みづけ**
- **対策の容易さを重みづけ**
- **有識者、ISACによるコミュニティコミットを経て公開**

ガイドラインの特長と意義

- 特徴
  - 脅威はCVE採番を行っているMITRE ATT＆CK (CVE) をベース
  - 緩和策は ATT＆CK 及び国防総省セキュリティ実装ガイド(STIG)を活用
  - 脅威の絞り込みは、有識者の実戦的経験をもとに実施
  - 各産業ISACと連携して策定、IPAがパブリックコメントをかけリファー

- 特長
  - 実際の脅威をベースにタクティクスを策定されている
  - STIGの緩和策はOSの基本機能をベースとしているため、低コストで実装が可能
  - 契約の付属文書であり、責任分界点や仕様が明確になる

- メリット
  - 国内を代表する重要インフラユーザー企業が、具体的なセキュリティ仕様をベンダーに提示することで、産業全体が底上げ
  - サプライチェーン全体で「セキュリティ仕様」を考える必要が出てくる

タスクフォース・ワーキンググループ

- **タスクフォース（TF）**
  - OSS DB TF
    - OSSを中心としたソフトウェア管理の在り方検討
  - 検証センター TF
    - 中小規模の事業者が検証できる環境の検討

- **ワーキンググループ（WG）**
  - PSIRT推進WG
    - 製品セキュリティを組織的に対応できる体制の推進
  - セキュア開発WG
    - セキュア開発を行える企業や人材の強化

Thank you