NIST OSCALのISMSにおける活用方法

標準化部会　日本ISMSユーザグループインプリメンテーション研究会
ISO/IEC SC 27/WG 1小委員会 委員　井崎 友博
（SecureNavi株式会社 代表取締役CEO）

2024/12/06

自己紹介

井崎 友博

1993年生、兵庫県出身

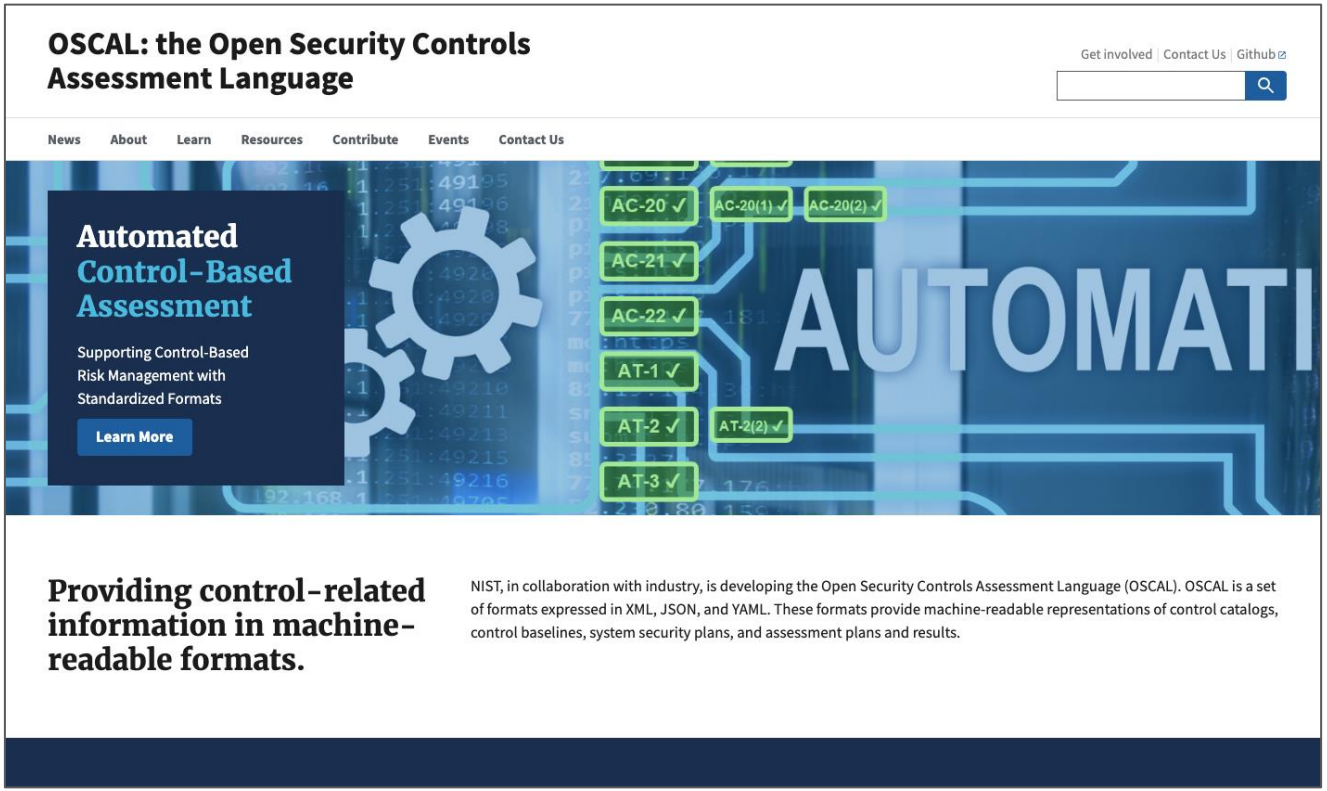
経歴

3年	ISMSコンサルタント
2年	事業会社のISMS事務局
5年	ISMSの会社を立ち上げCEOを務める
2年	SC27 / WG1 国内小委員会 委員

参加団体

- 日本ISMSユーザグループ（JNSA）
- ISO/IEC JTC1/SC27 WG1小委員会
- 一般社団法人スタートアップ協会

NIST OSCALとは...？



https://pages.nist.gov/OSCAL/

O S C A L

Open **S**ecurity **C**ontrols **A**ssesment **L**anguage

オープンなセキュリティ管理策の評価**言語**

NIST OSCALとは...？

情報セキュリティの取り組みを...

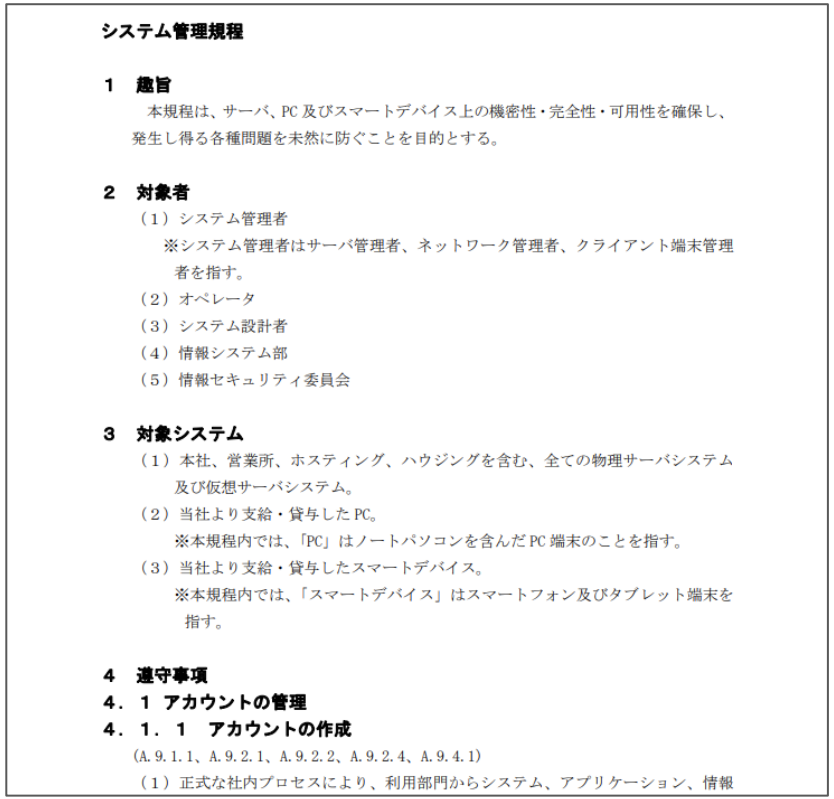
人間が読めるように記載する

＜今まで＞

機械が読めるように記載する

＜OSCALの考え方＞

NIST OSCALとは...？



システム管理規程

1　趣旨

本規程は、サーバ、PC 及びスマートデバイス上の機密性・完全性・可用性を確保し、発生し得る各種問題を未然に防ぐことを目的とする。

2　対象者

（1）システム管理者

※システム管理者はサーバ管理者、ネットワーク管理者、クライアント端末管理者を指す。

（2）オペレータ

（3）システム設計者

（4）情報システム部

（5）情報セキュリティ委員会

3　対象システム

（1）本社、営業所、ホスティング、ハウジングを含む、全ての物理サーバシステム及び仮想サーバシステム。

（2）当社より支給・貸与した PC。

※本規程内では、「PC」はノートパソコンを含んだ PC 端末のことを指す。

（3）当社より支給・貸与したスマートデバイス。

※本規程内では、「スマートデバイス」はスマートフォン及びタブレット端末を指す。

4　遵守事項

4．1 アカウントの管理

4．1．1　アカウントの作成

(A.9.1.1、A.9.2.1、A.9.2.2、A.9.2.4、A.9.4.1)

（1）正式な社内プロセスにより、利用部門からシステム、アプリケーション、情報

```
{
  "system-security-plan": {
    "uuid": "5e139edd-86aa-4b65-8431-1192bd276658",
    "metadata": {
      "title": "IFA GoodRead System Security Plan",
      "published": "2023-05-19T14:46:54-04:00",
      "last-modified": "2024-03-01T13:57:28.355446-04:00",
      "version": "1.1",
      "oscal-version": "1.1.2",
      "roles": [
        {
          "id": "owner",
          "title": "IFA GoodRead Owner"
        },
        {
          "id": "developer",
          "title": "IFA GoodRead Developer"
        },
        {
          "id": "system-engineer",
          "title": "IFA GoodRead System Engineer"
        },
        {
          "id": "public-affairs-office",
          "title": "IFA Public Affairs Office"
        }
      ],
      "parties": [
        {
          "uuid": "ba9c12bd-e5ef-46b6-95a2-4d8e7f864c1a",
          "type": "person",
          "name": "Owen Stilskin",
          "member-of-organizations": [
```

https://www.jnsa.org/result/2016/policy/

https://github.com/usnistgov/oscal-content/blob/main/examples/ssp/json/ifa_ssp-example.json

NIST OSCALの構造

レイヤー	管理策		実装	評価		
モデル	カタログ	プロファイル	システム セキュリティ計画	評価計画	評価結果	行動計画と マイルストーン
概要	規格やガイドライン	組織が実施する管理策	管理策の実装状況	監査や診断などの計画	監査や診断などの結果	結果を踏まえた対応計画
記載できる情報の例	• 規格タイトル • 項番 • 本文	• 採用管理策	• 対象システムの情報 • 採用管理策の実装状況	• 評価対象システムと管理策 • スケジュール	• 評価結果 • ログ	• 対応計画 • 対応の進捗状況

※ 説明の便宜上、コンポーネント定義モデルは省略しています。

NIST OSCALの構造

レイヤー	管理策		実装	評価		
モデル	カタログ	プロファイル	システム セキュリティ計画	評価計画	評価結果	行動計画と マイルストーン
概要	規格やガイドライン	組織が実施する管理策	管理策の実装状況	監査や診断などの計画	監査や診断などの結果	結果を踏まえた対応計画
記載できる情報の例	• 規格タイトル • 項番 • 本文	• 採用管理策	• 対象システムの情報 • 採用管理策の実装状況	• 評価対象システムと管理策 • スケジュール	• 評価結果 • ログ	• 対応計画 • 対応の進捗状況

※ 説明の便宜上、コンポーネント定義モデルは省略しています。

NIST OSCALの構造（カタログモデルの例）

5.1 情報セキュリティのための方針群

管理策
情報セキュリティ方針及びトピック固有の...

目的
事業、法令、規制及び契約上の要求事項...

手引
組織は、方針群の最も高いレベルに、...

その他の情報
トピック固有の方針は、組織によって...

```
<control id="s5.1">
  <title>情報セキュリティのための方針群</title>
  <prop name="label">5.1</prop>
  <part id="s5.1_ctl" name="control">
    <p>情報セキュリティ方針及びトピック固有の...</p>
  </part>
  <part id="s5.1_pps" name="purpose">
    <p>事業、法令、規制及び契約上の要求事項...</p>
  </part>
  <part id="s5.1_gdn" name="guidance">
    <p>組織は、方針群の最も高いレベルに、...</p>
  </part>
  <part id="s5.1_inf" name="infomation">
    <p>トピック固有の方針は、組織によって...</p>
  </part>
</control>
```

NIST OSCALの構造

※ 説明の便宜上、コンポーネント定義モデルは省略しています。

レイヤー	管理策		実装	評価		
モデル	カタログ	プロファイル	システム セキュリティ計画	評価計画	評価結果	行動計画と マイルストーン
概要	規格やガイドライン	組織が実施する管理策	管理策の実装状況	監査や診断などの計画	監査や診断などの結果	結果を踏まえた対応計画
記載できる情報の例	• 規格タイトル • 項番 • 本文	• 採用管理策	• 対象システムの情報 • 採用管理策の実装状況	• 評価対象システムと管理策 • スケジュール	• 評価結果 • ログ	• 対応計画 • 対応の進捗状況

ISMSのプロセス	附属書A	適用宣言書	リスク対応	監視測定計画 監査計画	監視測定結果 監査結果	是正処置表

OSCALを理解する上での注意

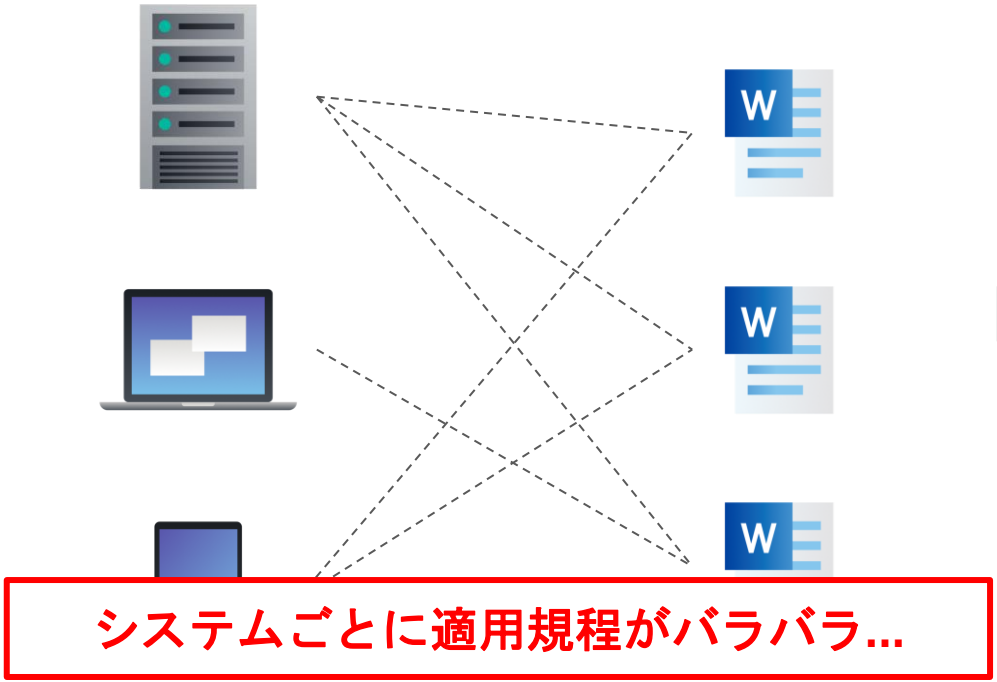
- OSCALは、あくまで「新しい記法」を提供しているのみである。
  - **できること**
    - 複雑な Word/Excel（例えば、リスク管理表・監査記録など）を、OSCALという標準的な記法で表現できる
  - **できないこと**
    - 監査の自動化が実現できる（OSCALは記法を提供するのみで、自動化技術ではない）
    - ISMSに必要な書類が自動生成できる（OSCALは記法を提供するのみで、書類の自動生成技術ではない）

※ OSCALによって記法が標準化されることで、「できないこと」を実現する技術開発が進む可能性はある。

NIST OSCAL のメリットと期待（1）

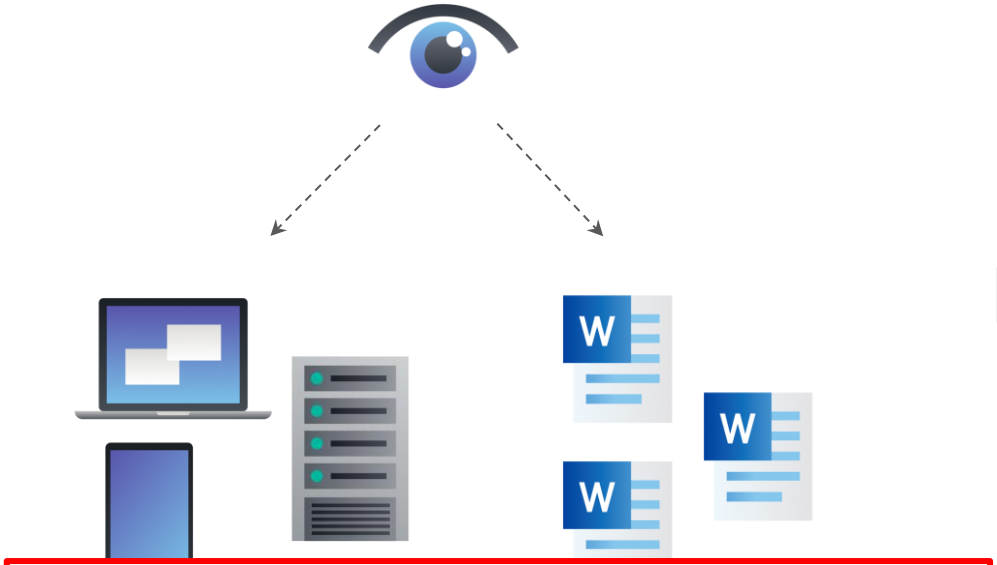
共通の
フォーマットで
表現！

NIST OSCAL のメリットと期待（２）



各管理策の
対象システムを
明確化！

NIST OSCAL のメリットと期待（３）



システム監査・内部監査の負担増...

機械による
監査効率化の
実現

OSCAL の採用によるメリット

対象者	メリット
経営者・CISO	客観的な指標を用いた、自社のセキュリティレベルの把握
セキュリティ担当者	複数の規格・ガイドラインに効率的に対応可能 面倒な書類作業を削減
コンサルタント	支援に必要な書類の量を削減
外部の監査員	監査作業の効率化

OSCAL の採用によるデメリット

- OSCAL はあくまで「管理策の評価言語」であり、マネジメントシステムの取り組みを記述するものではない。
  - リスクベースで管理策を採用するような記述は難しい。
  - ISMSで求められる組織の状況や、役割などを記述することは難しい。
- 習得と実践が難しい。特に日本では、OSCALを採用しているコンサルタントやセキュリティベンダーがいない。

日本国内での現在の動き

2021年	SecureNavi株式会社がレポートを公開
2023年	デジタル庁が「セキュリティ統制のカタログ化 に関する技術レポート」の中で、OSCALに関して言及
2024年	PwC が「OSCALの概要と国際的影響」レポートを公開 デジタル庁が、「政府機関等の対策基準策定のためのガイドライン」をOSCALフォーマットで公開

デジタル庁の事例

DS-231 セキュリティ統制のカタログ化に関する技術レポート

本文（PDF／599KB）
統合版（PDF／Wordファイル）（ZIP／769KB）

- 最終改定：2023年3月31日
- ドキュメントの位置づけ：Informative
- 概要：セキュリティ統制のカタログ化とは、独立したセキュリティ管理策に対し一意な識別子を付与し、機械可読形式で分類することを指す。
  これにより、統制要素たる管理策間でのトレーサビリティを確保することや、システム設定自動化などを促進することができ、システムセキュリティ評価の効率、適時性、正確性、および一貫性を向上させることが可能となる。本文書ではセキュリティ統制のカタログ化に関する概要について説明する。
  セキュリティ統制のカタログ化に関する取組みとしては、本文書で述べたOSCAL （Open Security Controls Assessment Language）があり、その活用が注目されている。 OSCALは、セキュリティ統制を機械可読言語で表現するためNISTによって開発された言語であり、XML、JSON、
- 実例： OSCALフォーマット記述例「政府機関等の対策基準策定のためのガイドライン（令和5年7月4日版）」（ZIP／298KB）（2024年9月20日掲載）
  OSCALを用い「政府機関等のサイバーセキュリティ対策のための統一基準群」のうち「政府機関等の対策基準策定のためのガイドライン（令和5年度版）（PDF）」をXML、JSON、YAMLの形式に記述したものを掲載している。

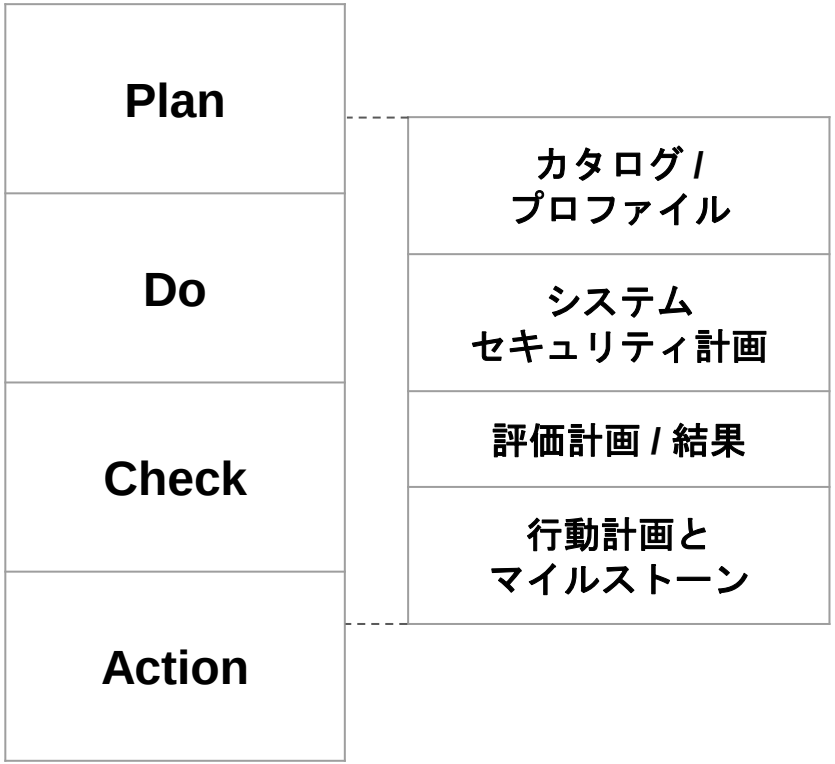
とになる。そのため、各政府機関におけるセキュリティ管理策について、OSCALを考慮した表現で構造化することで、その策定の自動化・機械化に寄与し、情報共有の効率化が見込めるほか、セキュリティ統制の評価の質の向上や、それらに係る労力の省力化が期待できる。

https://www.digital.go.jp/resources/standard_guidelines

ISMS と OSCAL との棲み分けに関する提案

ISMS

特徴：
- マネジメントシステム
- リスクベースアプローチ



OSCAL

特徴：
- 管理策の効率的管理
- 機械可読

ISMSにおける「文書化」のいち手段として、OSCALが採用できるのではないか？

OSCALの普及によって考えられるISMSの変化

監査や審査のデジタル化・AI化

- 人による監査→機械による監査へ
- 監査エビデンスとして、Word/Excelを提供するのではなく、OSCALで記述されたファイルを提出する
- 監査にかかる時間の短縮
- 監査の属人化の排除

ISMS担当者の工数削減

- Excelのシートと格闘する時間の削減
- 適用宣言書や内部監査記録などを自動作成
- OSCALフォーマットで記述された内容を取り込んだAIと会話しながら、ISMS活動を実施する

ご清聴ありがとうございました！