資料6

産業横断サイバーセキュリティ人材育成検討会
人材育成に関する各種取り組みとの
連携の在り方について

2018/11/09

産業横断サイバーセキュリティ人材育成検討会 事務局

第二期活動

- **対外活動**
  - 米国NIST Cybersecurity Risk Management Conference 登壇　2018年11月
    - 「人材定義リファレンス」における NIST Cyber Security Framework / SP800-181 活用事例
  - IPA共催 「今なすべきサイバーセキュリティ対策とそれに必要な人材とは」開催　2018年6月
    - 登録セキスペ の普及に向けたシンポジウム
  - CRIC CSF主催 学生向けセミナー 開催　2018年6月
    - 会員企業のセキュリティスペシャリスト5名による、対談形式の仕事解説セミナー
- **成果物**（2018年11月21日に公開予定）
  - セキュリティ統括室キット
    - ユーザ企業における、全社のセキュリティを統括する組織と人材のあり方について
  - OTセキュリティ人材定義
    - SP800-53に基づく、OT領域のセキュリティ機能の配置について
  - セキュリティ人材育成 研修データベース
    - 国内1000弱のセキュリティ講座、国内の過去3年の各種ガイドライン、世界中のセキュリティイベント等をDB化し、公開中。

日本企業の特性を踏まえた「人材定義リファレンス」

- 「人材定義リファレンス」は3種類のリファレンスで構成。
  - 日本特有の産業構造や、日本企業の組織及び役割のあり方を踏まえて策定。
    - A1.産業横断 人材定義リファレンス～機能と業務に基づくセキュリティ人材定義～　：役割分担 ／ 業務区分・知識区分
    - B.産業横断 セキュリティ対策カレンダー ～セキュリティ対策A to Z～　：CISO等向けチェックリスト
    - C.産業横断 セキュリティオペレーション アウトソーシングガイド　：業務委託等 参考資料

- C. アウトソーシングガイドの取り扱い
  - 日本企業の特性とNICEフレームワークを活用し2016年に策定
    - NICEフレームワークの想定する範囲がこれまではCSIRT／SOCに重きを置いていたため参考情報として活用。
  - NICEフレームワークがSP800-181に改定されたことにより再定義を実施
    - 日本国内でもNIST文書の活用が意識され始めたため、継続的に改定を行っている。

- C.アウトソーシングガイドの特徴

1. アウトソーシング先は以下の3つに分類

   ①構築・運用委託先インテグレーター、②製品・サービスベンダー、③セキュリティ専門事業者

2. インソースには、以下を想定

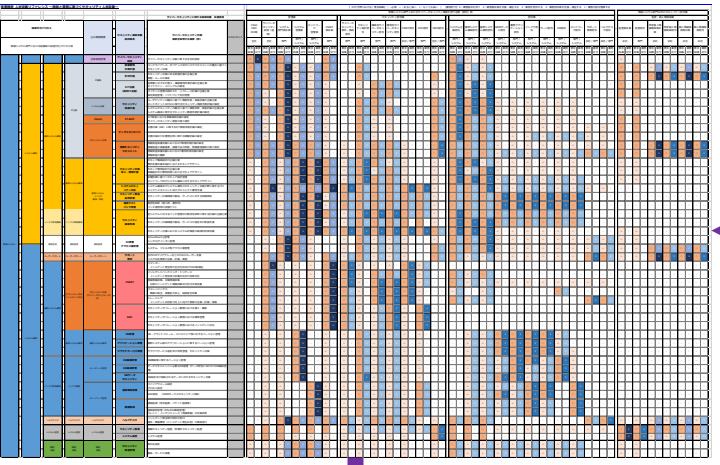
   ①情報システム部門（情報システム子会社を含む）管理者、②担当者、③常駐者（技術者派遣／コンサルタント）

- 上記2分類は、日本企業のシステム管理の現状を踏まえ、欧米のIT人材の考え方をそのまま導入することなく、現実に即したものとするための調整弁として策定。

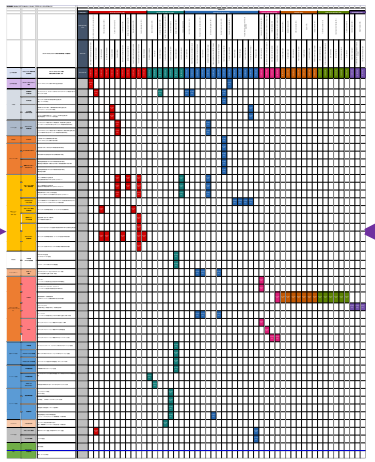
SP800-181を中核とした外部との人材モデルの連携について

- 人材定義リファレンスに基づく外部連携の在り方

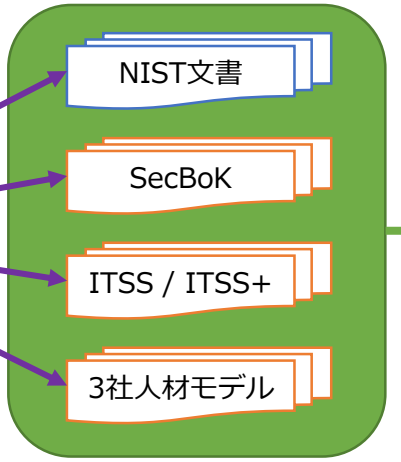
A.人材定義リファレンス



機能関係図とSP800-181

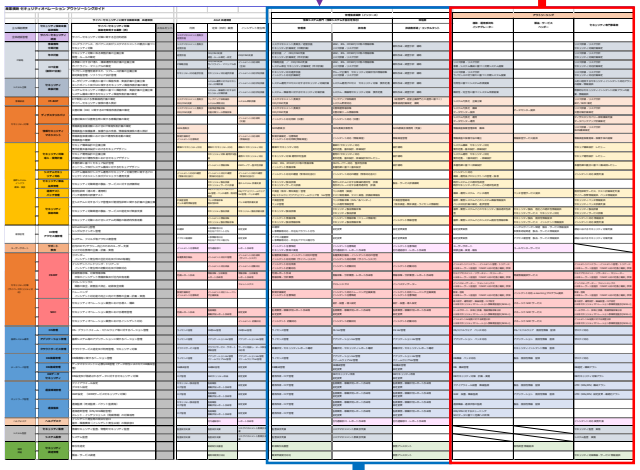


外部人材モデル（例）

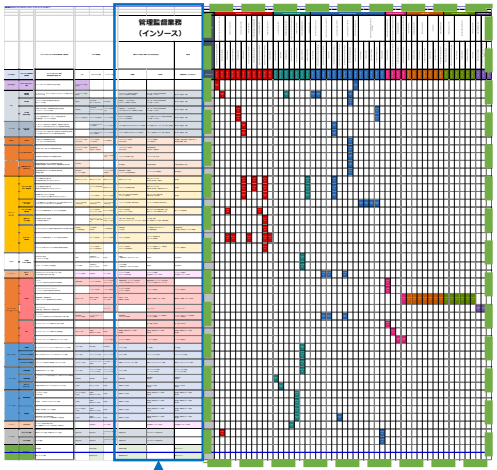


必要に応じて、参照先を入れ替える

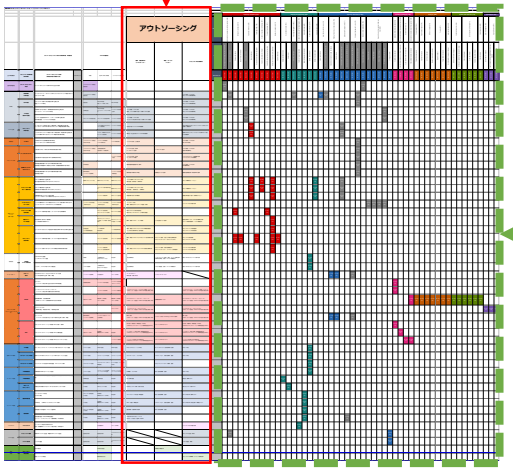
C.アウトソーシングガイド



C.アウトソーシングガイド インソース



C.アウトソーシングガイド アウトソース



上記表の拡大版は、統括室キットをご確認下さい。