2018 年 10 月 24 日

日本電気株式会社
株式会社日立製作所
富士通株式会社

NEC・日立・富士通、サイバーセキュリティ技術者の共通人材モデル「統合セキュリティ人材モデル」を策定

～14 種類の人材像を体系化・標準化し、IT・セキュリティベンダー向けに公開～

日本電気株式会社（注 1、以下、NEC）、株式会社日立製作所（注 2、以下、日立）および富士通株式会社（注 3、以下、富士通）は、実践的なスキル・ノウハウを持つサイバーセキュリティ技術者の共通人材モデル「統合セキュリティ人材モデル」を策定し、本日から IT・セキュリティベンダー向けに公開します。

近年、サイバー攻撃の増加のみならず、その手口も高度化・巧妙化が進む中、国内において高度なセキュリティ対策を担うセキュリティ技術者が不足しており、こうした課題を解決するために政府機関などによるセキュリティ技術者の育成・確保に向けた取り組みが加速しています。

一方、IT・セキュリティベンダーにおけるセキュリティ技術者の人材像はそれぞれで異なり、人材の育成も各社独自で行っているため、適切なセキュリティ技術者を効率的に育成するには限界がありました。

今回、NEC・日立・富士通は、2017 年 12 月に開始した「サイバーセキュリティ人材育成スキーム策定共同プロジェクト」(注 4)の一環として、国内における実践的なスキルやノウハウを持つセキュリティ人材の育成に向けて、3 社のセキュリティ対策の技術やシステム構築実績を活かし、共通的な 14 種類の人材モデルを定義した「統合セキュリティ人材モデル」を公開します。また、各人材像のスキル習得に必要となるコースマップ仕様書（コースマップ：注 5、シラバスなど）も本日より順次公開します。

NEC・日立・富士通は、共通人材モデルの公開により、高度なセキュリティ対策を行える人材像を体系化・標準化することで、企業に必要となるセキュリティ人材を効果的・効率的に教育するための仕組みづくりに貢献していきます。

【「統合セキュリティ人材モデル」】

「統合セキュリティ人材モデル」では、14 種類の人材像を定義し、各人材像に、セキュリティ事故対応やサイバー攻撃監視などといったセキュリティ人材として習得すべきスキルセットを体系化しています。具体的には、米国国立標準技術研究所(以下、NIST)のセキュリティ対策基準「NIST SP800-181」（注 6）が定めるセキュリティ対策への対応をベースとし、アプリケーションなどの脆弱性診断を実施するペネトレーションテスターや、サイバー攻撃による被害範囲を分析・調査するフォレンジックエンジニア、セキュリティインシデント時に初動対応するインシデントレスポンダーなど 14 種類の人材像と各々のスキルセットを体系化・標準化しています。

今後、NEC・日立・富士通は、自社でのセキュリティ人材育成において 2019 年度から「統合セキュリティ人材モデル」の活用を予定しています。また、3 社のみならず IT・セキュリティベンダーにおけるセキュリティ人材の育成活動と連携し、国内における実践的なスキルやノウハウを持つ高度なセキュリティ技術者の育成に貢献するとともに、国内でのセキュリティ人材モデルの標準化にも取り組んでいきます。

※「統合セキュリティ人材モデル」の公開情報については、以下の問い合わせフォームより入手可能です。
http://www.hitachi.co.jp/security-inq/

以上

（注 1）日本電気株式会社：
本社：東京都港区、代表取締役 執行役員社長 兼 CEO：新野 隆
（注 2）株式会社日立製作所：
本社：東京都千代田区、執行役社長兼 CEO：東原 敏昭
（注 3）富士通株式会社：
本社：東京都港区、代表取締役社長：田中 達也
（注 4）「サイバーセキュリティ人材育成スキーム策定共同プロジェクト」：
2017 年 12 月 14 日プレスリリース
NEC・日立・富士通、「サイバーセキュリティ人材育成スキーム策定共同プロジェクト」を開始
http://www.hitachi.co.jp/New/cnews/month/2017/12/1214a.html
（注 5）コースマップ：
「統合セキュリティ人材モデル」の人材像ごとに作成された、講座・試験を時間軸（講座順番や期間）で表した計画（履修）表。
（注 6）NIST SP800-181:
2017 年 8 月に NIST が発行した、サイバーセキュリティ業務の役割・専門分野と必要とされる知識・能力に関する共通用語と分類法を提供する資料。1007 のタスク、630 の知識、374 のスキル、176 の能力から構成される。

＜本件に関するお客様からのお問い合わせ先＞

日本電気株式会社　サイバーセキュリティ戦略本部
E-Mail：inquiry@secl.jp.nec.com

株式会社日立製作所　セキュリティ事業統括本部
マネジメント本部 事業管理部
URL：http://www.hitachi.co.jp/security-inq/

富士通株式会社　オファリング推進本部
セキュリティオファリング統括部
プロモーション推進部
電話：(03)6441-0151

【別紙】

統合セキュリティ人材モデル

人材像	説明
【CT】セキュリティコンサルタント	セキュリティエンジニアリングの上流に位置し、経営課題や業務要件から、セキュリティに関するシステム仕様や運用仕様の方針を策定する。
【PL】セキュアシステムプランナー	求められるセキュリティ要件を満たすシステムやアプリケーションの上流設計を担当する。対象領域は、システムアーキテクチャー、ネットワーク、サーバ、アプリケーション、データベースなど。
【DV】セキュアシステムデベロッパー	セキュアシステムプランナーのアウトプットを引き継ぎ、セキュリティ要件を満たすシステム基盤の開発を担当する。対象領域は、システムアーキテクチャー、ネットワーク、サーバ、データベースなど。
【AD】セキュアアプリケーションデベロッパー	セキュアシステムプランナーのアウトプットを引き継ぎ、セキュリティ要件を満たすアプリケーションの開発を担当する。対象領域はアプリケーション、データベースアクセスなど。
【MG】セキュリティマネージャー	ISMSに代表されるセキュリティマネジメントシステムの整備および運用を担当する。
【AU】セキュリティオーディター	ISMSに代表されるセキュリティマネジメントシステムのマネジメント監査を担当する。
【SR】システムリスクアセッサー	対象のICTシステムが直面するセキュリティリスクを分析し、適切なセキュリティ対策選択の指針を示す。
【PT】ペネトレーションテスター	対象のICTシステムに対して攻撃者視点で攻撃を試み、ICTシステムの弱点（脆弱性や危険性等）を把握し報告する。
【NR】ネットワークリスクアセッサー	対象のICTシステムが直面するセキュリティリスクを分析し、適切なセキュリティ対策選択の指針を示す。
【RE】リサーチャー	セキュリティ技術に関する各種の研究を行う。
【FE】フォレンジックエンジニア	セキュリティインシデント発生時に、コンピュータ・フォレンジックプロセスに基づく詳細な調査を実施する。すでに侵害されたディスクイメージなどを採取し、また取得したイメージなどを解析し、攻撃者によっていつどのようなことが行われたのか解析を実施する。
【IA】インテリジェンスアナリスト	セキュリティに関する外部情報を収集・分析し、ICTシステムへの影響度を把握する。また、インシデント発生時にその背景などを分析し、インシデントの重大性に対する判断材料を提供する。
【IR】インシデントレスポンダー	セキュリティインシデントへの１次対処を行う。必要に応じて、インシデントハンドラーなどの他の人材像へのエスカレーション・引継ぎを行う。
【SP】セキュリティオペレーター	ICTシステムのセキュリティに関連する運用を担当する。