資料１

「AI人材」・「セキュリティ人材」・「AIセキュリティ人材」

セキュリティ人材育成とAI活用の取り組み

株式会社ラック

2025/12/18

Summary

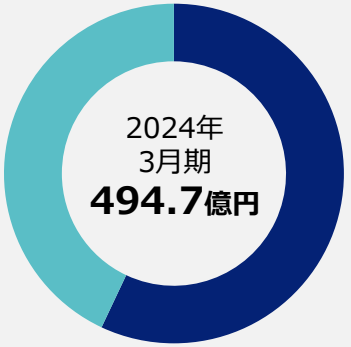
本書では、日本国内におけるサイバーセキュリティ黎明期といえる1990年代中期からセキュリティサービスを提供する株式会社ラックにおける、近年の「AI人材」「セキュリティ人材」「AIセキュリティ人材」の育成方針についてご紹介を差し上げるものです。

急速なデジタル利活用シーンの増加やAIをはじめとする技術の進歩は、生産性向上や働き方の多様化に大きく貢献する一方、サイバー攻撃による被害は深刻さを増す状況となっております。

サイバーセキュリティ人材の不足が課題となる中、当社の提供するサイバーセキュリティサービスにおいても、セキュリティ人材の確保・育成はもちろん、AI技術の利活用の加速により専門能力をこれまで以上に発揮するための環境づくりに取り組んでいます。

会社概要・事業所

名　　称	**株式会社ラック**（LAC Co., Ltd.）
事 業 概 要	■ セキュリティ事業 ■ システムインテグレーション事業 ■ 情報システム関連商品の販売及びサービス
本社所在地	〒102-0093 東京都千代田区平河町2-16-1 平河町森タワー
事　　業　　所	東陽町オフィス 名古屋オフィス 福岡オフィス ラックテクノセンター秋葉原 ラックテクノセンター北九州 シンガポール支店
従 業 員 数	2,192名（2024年3月31日現在）
設　　立	2007年10月1日　※創業：1986年9月
資　　本　　金	26億4,807万5,000円
売　　上　　高	569億円（2025年3月期）※連結



セキュリティ事業
45%　221.6億円

システムインテグレーション事業
55%　273.1億円

セキュリティサービス

1995年から 30年超 に渡り、ITセキュリティ対策の先駆者として全方位のサービスを提供

セキュリティ人材育成とAI活用の取り組み

専門人材を育成する「実戦」と「体験」

セキュリティ専門人材の育成においては、サイバー攻撃の実態に触れる「実戦」と、体系的かつ最新の知見に触れる「体験」の両軸を重視しています。

実戦＝顧客へのサービス提供フィールドから得られる経験

サイバー攻撃の生の情報に触れる機会のある「セキュリティ運用監視サービス」「サイバー救急センター」「脆弱性診断」「セキュリティコンサルティング」では、実際の攻撃痕跡やゼロデイ攻撃で悪用される脆弱性の情報がセキュリティ人材の感性や知見を育てる。

さらに官公庁や重要顧客との人材交流により企業や組織の実情を理解する取り組みも推進。

体験＝インテリジェンスやコミュニケーションから得られるインサイト

脅威インテリジェンスに基づくトレンド観測や、業界で推進されるセキュリティコンセプト、セキュリティベンダーのサービス・プロダクト理解、セキュリティ競技会への参加、社外業界団体活動、各種セキュリティ研修の受講など、最新の情報と専門家とのコミュニケーションから、コンピュータサイエンスに基づく体系立てられたセキュリティ対策のインサイトを育てる。

社員相互によって行われるスキルアッププログラムの充実

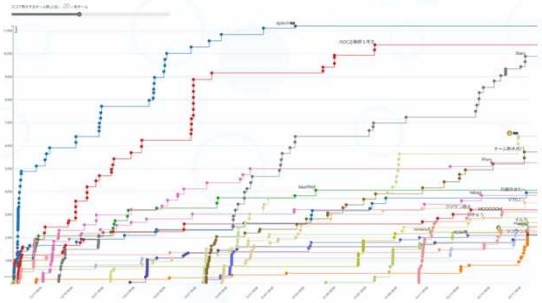
セキュリティ教育コンテンツを社員自らが作成。参加型・体験型のプログラムにより、相互にスキルを高めあうことで、技術に対して探求とリスペクトを培うカルチャーを醸成しています。

実施例

社内CTF
LACCON

セキュリティ競技会

・年1回開催され、ラックグループ社員のチームにより勝敗を争う技術競技大会
・参加社員によって作成される問題は毎回全問新作
・毎年約50チームが参加



CTF開催時のスコアグラフ

トップガン演習

座学　ハンズオン

・診断／監視／インシデント対応／研究所の現場トップエンジニアが自らコンテンツを作成し、ハンズオンでテクニックを指導
・現場で磨かれた実践的なテクニックを伝授

社内カフェテリアでの勉強会開催

LAC AI Day他
LT会・勉強会

社内イベント

・AIの活用にたけたエンジニアが、自らの利用ケースや業務活用事例を共有
・セキュリティ技術やトピック、日常の知見などをLT大会で発表

社外での活動を通じた人材の育成

サイバーセキュリティコミュニティの形成支援を通じた人材育成活動事例

- サイバー犯罪に関する白浜シンポジウム　協賛・セキュリティ道場提供
- 情報セキュリティワークショップin越後湯沢　協賛・大会運営副委員長
- サイバーセキュリティシンポジウム道後　協賛
- 九州サイバーセキュリティシンポジウム　協賛・実行副委員長
- 旭川セキュリティシンポジウム　協賛・実行委員会
- サイバー防衛シンポジウム熱海 協賛
- セキュリティキャンプ 協賛・事務局
- Hardening Project 協賛・運営支援

全国各地で開催されるセキュリティシンポジウム・各種育成イベントの活動支援や参加を通じて、産官学／ユーザ・ベンダーの結びつきを強化。

国際的なサイバーセキュリティコンテスト（CTF）への参加を通じた人材育成事例

※社員チーム、社員個人、社外との混成チームを含む、代表的なもの。

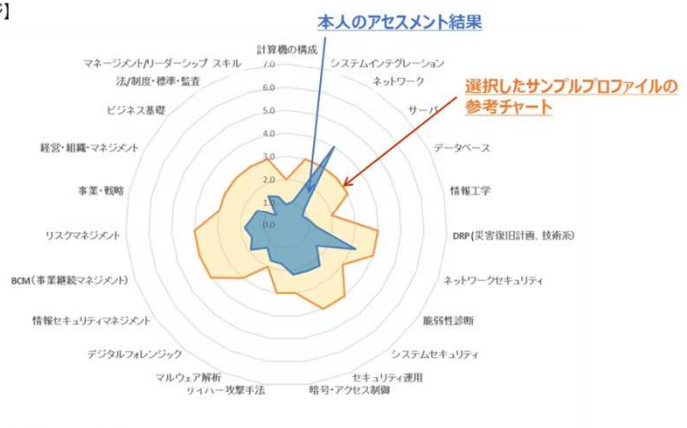
- CODE BLUE 2019 ICS Cyber Hacking Challenge　優勝
- International Cybersecurity Challenge 2022 準優勝、Attack & Defense部門優勝
- CODE BLUE 2022 CTF for Connected Cars　優勝
- International Cybersecurity Challenge 2023　総合3位、Attack & Defense部門優勝
- HTB Business CTF 2024: The Vault Of Hope　国内参加チーム内で２位、総合８位入賞
- Converge Japan CTF 2024　準優勝
- DiceCTF2024　世界4位

若手人材を中心にチームを編成。世界の強豪と肩を並べて競うことで、技術の手ごたえを感じる取り組みを支援。

JTAG/Visumeを活用したキャリアプラン支援

JTAG財団(一般社団法人日本サイバーセキュリティ人材キャリア支援協会：https://www.j-tag.or.jp/)が提供する、人材スキルスコア可視化サービス「Visume」を用い、従業員の専門性を共通指標化・見える化。市場価値を意識することで、一人ひとりのキャリア形成支援、組織内での適材適所への配置や業務分担の適正化、自己学習・自己啓発に向けたレベルの確認における参考情報のひとつとして活用。

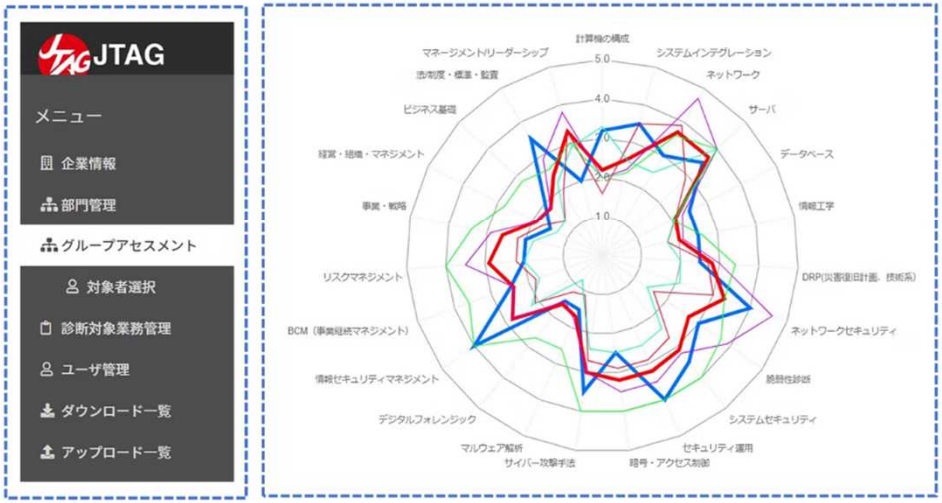
【診断結果のイメージ】



【自動計算で算出されるレベルについて】

個人のアセスメント結果

【左：グループアセスメントの選択機能】　【右：レーダーチャートの表示画面（例）】

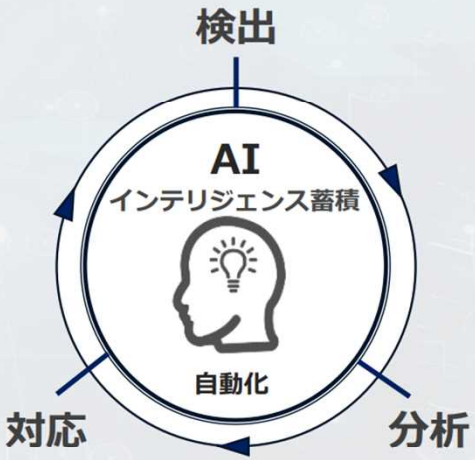


組織全体のスキル成熟状況

個人ごとのキャリアレベルの客観的な把握ともに、組織全体の成熟状況を可視化。

AI×セキュリティの基本コンセプト

人による対応をＡＩ・自動化によりサービスの高度化と急拡大するニーズに対応
市場競争力強化とともに費用対効果の高い新サービスにより中小企業向けにも対応



優位性を確保する
大手企業を軸とした高い実績

- JSOC顧客数　約1,000社
- 診断実施数　累計約27,500件
- 緊急対応件数　累計約4,800件

サービスポイント（提供価値）

- 大量に蓄積されている脅威データを高度分析
- 人手で行っている対応をAI／自動化により生産性向上
- 巧妙化・深化する攻撃への新たな分析手段を開発
- 自動化によって費用対効果の高い新サービス開発につなげ
  中小企業向けにも対応したサービスを提供

AI環境を中心とした「AI人材」の育成

GAI CoE（Generative AI Center of Excellence）組織横断の生成AI利用の支援組織

戦略立案
生成AI対応戦略を立案し
推進・支援・監督

人材育成
生成AIに対応し業務改善をリードする
人材を社内で広く育成

ラボ機能
実証環境を準備して社内に提供

業務活用促進
各業務における生成AI活用の支援

ガバナンス
生成AIの利用や自社開発における
ガイドやルールの整備

プレゼンス
エバンジェリストの生成と輩出および、
社外広報活動

（出典）ラックでの生成AI活用の最前線～組織横断の推進チームが目指す企業での活用とは　https://www.lac.co.jp/lacwatch/media/20230928_003519.html

サイバーセキュリティ人材フレームワーク（案）について①

ご提示いただきました「サイバーセキュリティ人材フレームワーク（案）」につきましては、多岐に渡るサイバーセキュリティ人材の情報共有や共同作業の実施において意思疎通やチームビルディングの円滑化を図る観点でぜひ活用を推進いただきたいと存じます。
さらなるフレームワーク活用を図る観点で、以下を提言させていただきます。

・NICEフレームワークの活用はセキュリティ人材の考え方のデファクトを海外規準に合わせる意味でも、適切に整理されている意味でも有効であると思慮。
・当社は人材育成において事業における実戦と訓練、コミュニケーションから得られる知見とつながりに重きを置いております。海外機関とも連携できるセキュリティ人材のキャリア形成において、若手～シニア～トップガンといったキャリア形成時期に応じた国際的な訓練の場の提供に期待する。
・近年セキュリティ人材のフレームワークについては、Google社が中心となって設立されたJapan Cybersecurity Initiativeによる中小企業を対象にしたトレーニングプログラムの提供や、国内のサイバーセキュリティサービス業者が立ち上げたCyber Security Initiative Japanにおけるサービスベンダー側人材育成を目的とした「プロフェッショナル人材フレームワーク」の策定など、同様のキーワード下に異なる目的にフレームワークが点在している実情がある。本サイバーセキュリティ人材フレームワークがその中心として鎮座し、各団体が目的に応じて引用する、不足点を追加するなどのスキームができあがることを期待します。また、これら業界団体の活動へのご支援に期待する。

サイバーセキュリティ人材フレームワーク（案）について②

（続き）

・セキュリティ人材のスキル定義に関して、これまでの業界団体の取組としてJNSAの「セキュリティ知識分野（SecBoK）人材スキルマップ」などの先行事例もある。NICEフレームワークに準拠しつつも、これらの成果や策定過程における議論には活かせるものがあるのではないか。

・今回のフレームワークについては官民共通のフレームワークというテーマであるが、業界全体の指標となりうることから、業界を志望する学生を擁する教育機関などにも大いに影響するものと考える。大学や専門教育を行う現場のご意見もヒアリングいただければと思慮します。

・フレームワークに対して、具体的な教育カリキュラム・プログラムのマッピングをどのように行うかが課題と思慮する。代表的なセキュリティ資格であるCISSPと情報処理安全確保支援士制度については、現在以下のような観点での発展余地がある。

①支援士の更新プログラムは良く出来ている反面、国際的な評価が相対的に得られていない
②国内では、情報処理安全確保支援士（＝上位）と、セキュリティマネジメント（＝入門）があるが、その間の専門職層がカバーする体系が無い課題があるものと思慮
③NICEフレームワークに準拠することで、資格についても欧米セキュリティベンダーの資格に独占されることが推察されるが、国内民間企業が提供する教育コースや資格要件を認定し、その職種要件を満たすための「受講必要要件」とするなどの取り組みに期待する

まとめ

サイバーセキュリティを体系的に会得するためには、コンピュータサイエンスを基礎とし、ネットワーク構築・システム開発・システム運用の知識が必須であり、セキュリティ知見と合わせて「基礎体力」として考えられる。合わせてAI技能という「筋力」を強化することで、今後求められるAIセキュリティ人材育成につながるものと考える。

基礎体力
セキュリティ知見・技能

サイバーセキュリティ人材育成 ＝ 基礎体力
- サイバーセキュリティサービスの提供を通じた実戦経験
- 体系的かつ最新のセキュリティ情報をもとにしたインサイトの醸成
- 社員相互によって行われるスキルアッププログラムの充実
- 社外コミュニティでの活動を通じた結びつきの強化
- 国際的セキュリティイベント・競技会への参加を通じた経験の強化
- JTAG/Visumeを活用したキャリアプラン支援

筋力
AI技能

AI人材育成 ＝ 筋力
- 業務利用可能なラボ環境の提供を中心とした実践的利用の推奨
- AIガバナンスの明確化と利用ケースの周知

国際的なセキュリティ知識獲得の機会創出や業界団体の取り組みへの支援をお願いしたい

※本資料は作成時点の情報に基づいており、記載内容は予告なく変更される場合があります。
※本資料に掲載の図は、資料作成用のイメージカットであり、実際とは異なる場合があります。
※本資料は、弊社が提供するサービスや製品などの導入検討のためにご利用いただき、他の目的のためには利用しないようご注意ください。