資料5

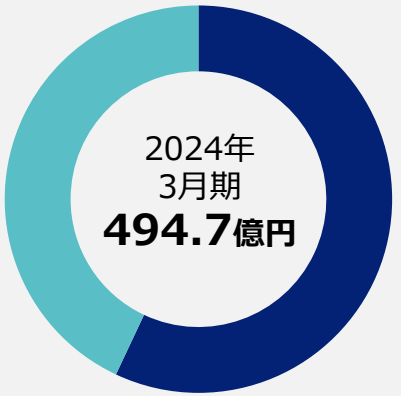
産業界のセキュリティ対策強化とセキュリティ産業の振興の好循環（仮題）に向けて

2024/11/20

株式会社ラック
倉　持　　浩　明

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	494億円（2024年3月期）※連結
上場市場	東京証券取引所スタンダード



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

セキュリティ事業

業界をリードする技術力で、様々な大手企業や行政機関に
高度なセキュリティサービスを総合的に提供

セキュリティ人材層の厚さ

セキュリティ事業
従業員数　約**764**名

情報処理安全確保支援士
登録者数　**175**名

最新のサイバー攻撃に関する知見

情報セキュリティ
事故対応（年間）　約**500**件

AIを使用したマネージドサービス
AIクラウドセキュリティ運用支援

※2024年3月現在

システムインテグレーション事業

金融機関など大手企業を軸とした、基幹システム開発を担う技術力
セキュリティサービスの複合的な提供で、セキュアなエンジニアリングを提供

信頼されるシステム開発力

大手金融機関など
継続的な取引企業
約350社

システム開発における
大手企業の売上割合
約75%

※大手企業は、従業員数が2,000人、売り上げ高1千億以上の企業を指す

システム開発
一次受け案件の割合
約60%

金融機関向け
AI活用金融犯罪対策
ソリューション
ZeroFraud

※2024年6月現在

株式会社ラック

中期経営計画

（2024-2026年度）

2024年5月13日

ラックを取り巻く事業環境認識

IT環境

デジタル活用はより多様で広範囲に深く

システム間連携が浸透し、相互依存性がより複雑かつ深化
至る所でサイバーセキュリティが必須に

▶サイバーセキュリティはデジタル社会の基幹産業といえる
▶桁が違う水準でのセキュリティ人材の不足

サイバー脅威がより深刻に

業務停止が現実的脅威に、金融犯罪も急拡大
AIなどの先端テクノロジの悪用（フェイク等含む）が顕著に

▶攻撃者以上のテクノロジー活用が必至

安全保障上の要求も高まる

社会基盤となったIT環境でビジネスや生活を行うために、
サイバー空間において自由主義・民主主義を守るための
安全保障の観点が必須に

▶サイバーセキュリティが安全保障の要となる

社会（お客様）の課題

デジタル活用に見合った費用対効果の追求

▶AIや自動化による対策の効率化
▶わかりやすく求めやすい対策

複雑化・高度化する脅威への対抗

▶点（個別対策）から線や面（総合対策）へ
▶高度な金融犯罪対策の要請

サプライチェーン全体のレジリエンス確保

▶中堅・中小企業へのセキュリティ対策
▶海外拠点のセキュリティ対策
▶業務停止への考慮と対策

セキュリティ対策の継続性担保

▶デジタル・セキュリティ投資戦略の策定と継続運用

経済安全保障の担保

▶重要インフラ事業者へのサプライチェーン対策
▶海外でも通用するセキュリティベンダー

社会の課題に対するラックへの要請

約30年にわたり磨き続けてきた現場経験からの知見(インテリジェンス)をもつ

サイバーセキュリティ対策の専門集団として

自動化・AIを活かした対応

AI活用により人のノウハウをデジタル化し
高度で費用対効果の高いサービスを提供

総合サービス力による対応

従前以上に複雑化・高度化するサイバー脅威に
ワンストップで最適なサービスを提供

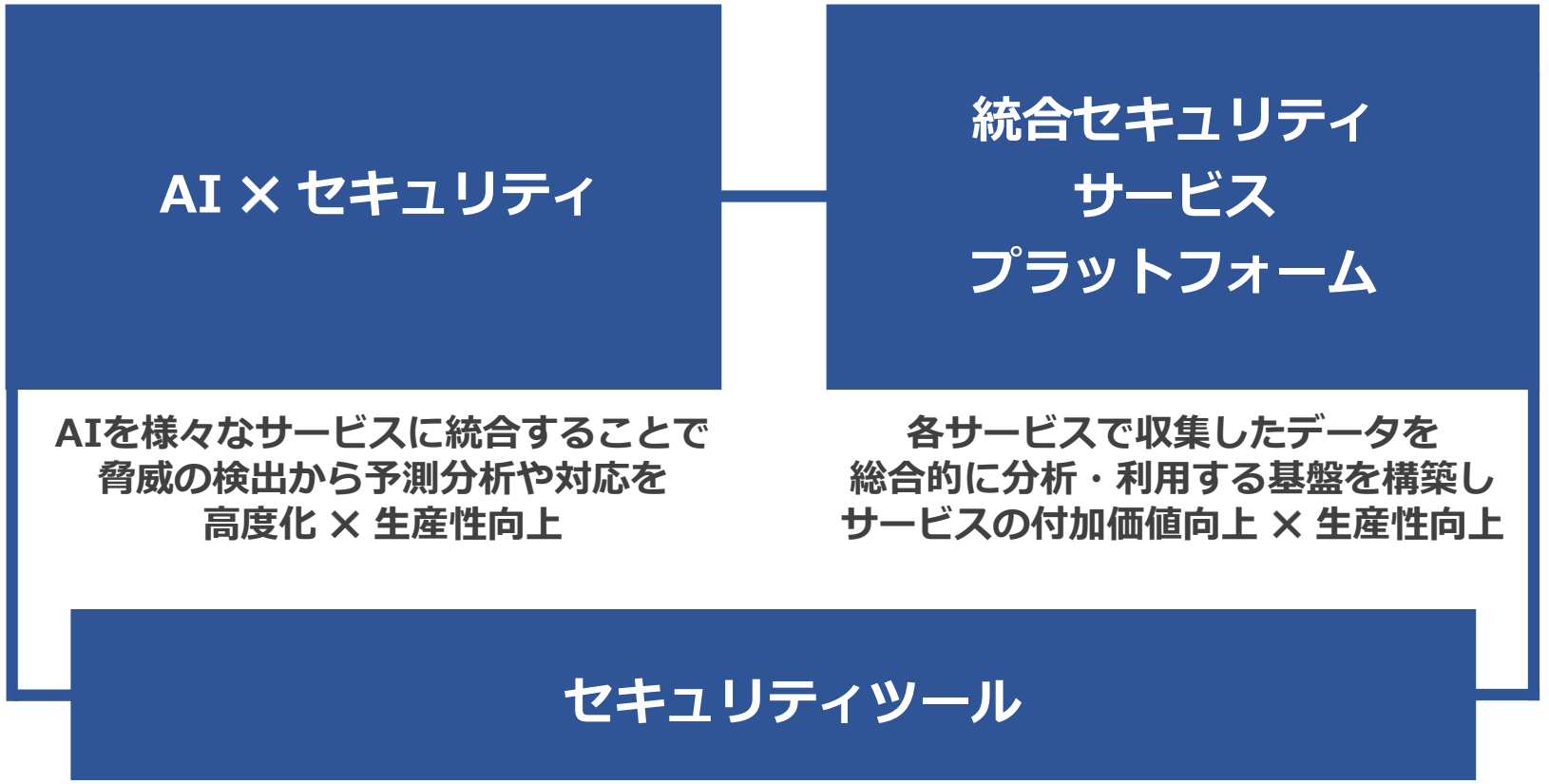
中堅・中小企業の対策につながるサービス提供

セキュリティ・SI事業の付加価値をさらに向上させ

中長期的な観点で新たな価値創造を推進

新たな価値創造への着実な推進

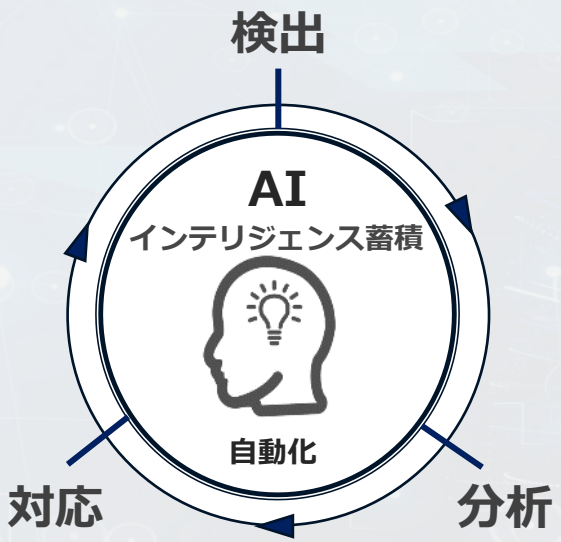
AIとエンジニアリングを組み合わせ、セキュリティサービスの付加価値や生産性を向上
世界に通用するセキュリティツールへの挑戦



セキュリティツールベンダーとの戦略的連携も視野に世界に通用するツールの獲得

ＡＩ×セキュリティ

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

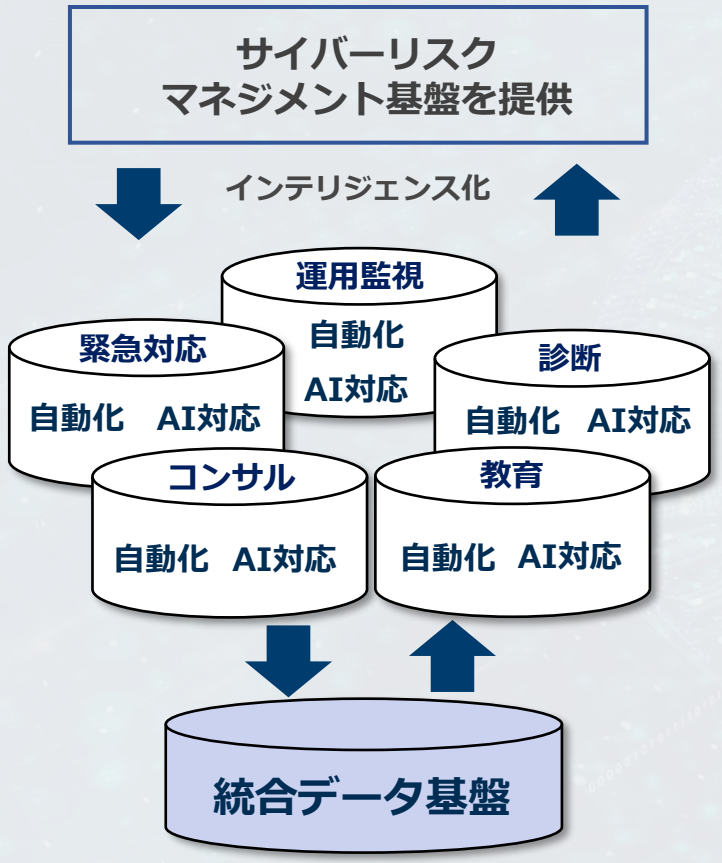
・JSOC顧客数　約1,000社
・診断実施数　累計約27,500件
・緊急対応件数　累計約4,800件

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

統合セキュリティサービスプラットフォーム

運用監視からサイバーリスクマネジメントへと昇華
各種セキュリティサービスのデータ分析・活用基盤を統合



サービスポイント（提供価値）

- ネットワーク、アプリケーション、端末などに分断されているサイバーリスクを統合し可視化
- 様々なツールを導入しているお客様へ統合したプラットフォームを提供し利便性を向上
  （ツール例：SASE、UEBA、CASB等）
- 統合データ基盤による知見を活用しお客様に最適な対策を提供
- 大規模グループ企業にも提供予定

SASE：Secure Access Service Edge、UEBA：User and Entity Behavior Analytics、
CASB：Cloud Access Security Broker

セキュリティツール

約30年に及ぶ現場経験からのインテリジェンスの知見を活かし
他社とのアライアンスを含めた新たなセキュリティツールの獲得を推進

アライアンス推進例

運用監視

AI・自動 × 脅威情報
（NRI社との合弁会社）

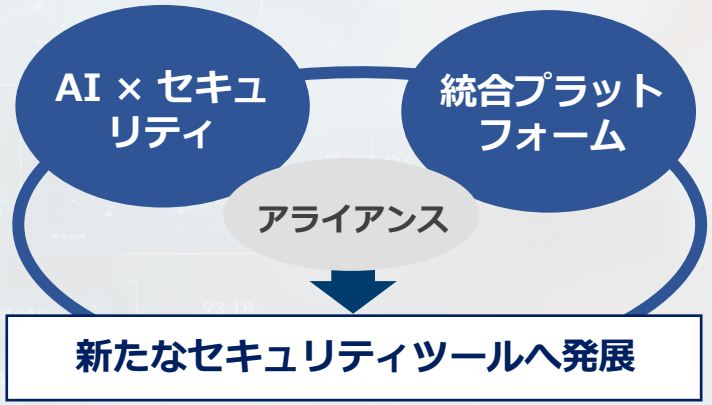
診断

AI・自動 × ノウハウ
（エーアイセキュリティラボ社と協業）

自社開発ツール例

マルウェア調査ツール
「FalconNest」

PC自己診断ツール
「自診くん」



サービスポイント（提供価値）

- AI × セキュリティ、統合セキュリティサービスプラットフォームなどの脅威情報と連携したセキュリティツールの獲得

  自社開発だけでなく、戦略的提携や買収も選択肢

- 中堅・中小企業向けのセキュリティ市場にも展開

  領域を広げてインテリジェンスを蓄積しサービスをさらに高度化

今後に向けた提言

サイバーセキュリティ”立国” 日本を目指して

日本はかつて低価格・高品質なモノづくりで世界をリードしてきたが、デジタル分野での取り組みには残念ながら出遅れている。一方で、日本は他国から「信頼できるパートナー」として認識されており、胸を張れる財産である。この信頼性を軸として、日本は「自由で開かれた経済圏」を支える重要なプレイヤーとして、その存在価値を世界に示していくべきである。

今後、日本にとってサイバーセキュリティは単なる重要分野ではなく、国際社会に対して我が国の存在価値を指し示すものとして捉えることが必要なのではないか。そのためには、民主主義的な価値観を共有する国々と連携し、サイバーセキュリティを基盤とした国際連携を基軸に経済圏を確立する大きな役割を果たすことで、世界における日本の存在感を高めることが必要である。そのための大局的な打ち手として以下を提言する。

（ア）国際的なサイバーセキュリティのフレームワークに日本のセキュリティ製品を組み込む

国際的なサイバーセキュリティのフレームワークに日本のセキュリティ製品を組み込み、世界に向けてその優位性を発信する。
日本製品のグローバル市場での地位を強化する。

（イ）人材育成と資格制度のパッケージ化

サイバーセキュリティ分野において即戦力となる人材を育成し、資格制度を通じて能力構築を支援する。

（ウ）同志国との協力枠組み構築

民主主義的価値観を共有する同志国と、政府レベルでサイバーセキュリティ分野の協力枠組みを構築する。
日本はサイバー安全保障における重要な役割を担いながら、セキュリティ産業の市場拡大を目指す。

今後、重要と思われる取組分野

今後、産業界が持続的に発展していくためには、IoT、AI、サイバー脅威インテリジェンス、ソフトウェア品質管理の各分野でのセキュリティ対策が不可欠である。これらの分野での強固なセキュリティ対策が、デジタル技術を安全に活用し、産業界全体の競争力と信頼性を高める要となる。

➢ データ収集基盤としてのIoT、AI、およびコミュニケーションツール

あらゆるモノがネットに接続される時代（IoT）において、データの収集基盤は産業界の競争力を左右するカギとなる。また、AIが適切に機能し価値を発揮するためには、大量かつ高品質なデータが不可欠であり、AIのデータ基盤も重要な役割を果たす。

- IoTを活用したデータ収集基盤を整備し、センサーやデバイスからのデータを効率的かつ安全に収集すること。
- AIシステムが必要とする高品質なデータの収集と管理を実現し、データの信頼性とセキュリティを確保すること。
- 安心して使えるマルチモーダルなコミュニケーションツールの育成とセキュリティ確保。

➢ サイバー脅威インテリジェンスを支えるエンドポイントでの情報収集

エンドポイントでの情報収集は、インテリジェンスの精度や迅速性を高め、より的確な脅威対応を可能にする重要な手段である。また、セキュリティ対策が行き届かず標的にされやすい中小企業は、限られたリソースの中でサイバーセキュリティ対策を強化する必要がある。

- サプライチェーンの強靭化の観点から、官公庁や重要インフラ事業者に加え、中小企業に対するセキュリティ対策を政府が支援し、国内のエンドポイント全体のセキュリティを高めること。
- 政府が官公庁や重要インフラ事業者において、国産のエンドポイント検知・対応（EDR）製品の導入を積極的に後押しすること。これにより、国内のエンドポイントにおける脅威検知の迅速化とサイバー脅威インテリジェンスの強化が期待される。中小企業を含む多様なエンドポイントから収集される脅威情報を分析することで、インテリジェンス能力を強化し、早期の脅威検知や迅速な対応を実現することが可能である。

➢ ソフトウェアの品質管理と安全性確保：ソフトウェアに対する監査フレームワークの必要性

製造業におけるソフトウェアの役割は拡大しており、今後はAIの活用も加速していくと考えられる。目に見える部分だけでなく、搭載されている多数の見えない制御プログラムの妥当性や正当性、記録データの正確性や真正性を確認・保証するためのフレームワーク整備が急務と考えられる。

- ソフトウェアの妥当性や正確性を検証するための監査フレームワークを整備し、制度的な保証を確立する。
- 世界標準をリードしながら、適切な監査仕様に基づき、透明性と真正性を確保するエビデンスを残すような制度の整備。

今後に向けた提言

- **国産サイバーセキュリティツールの開発と普及**
  国産サイバーセキュリティツールを、データ保護や脅威検知機能において世界水準を上回る品質で開発し、官公庁での導入から民間企業へと展開することで、国内外での競争力を強化する。海外市場での競争力強化を視野に入れ、国際標準とグローバル市場を意識した製品開発と展開が求められる。

- **サイバーセキュリティ専門人材の大規模育成**
  新卒エンジニアから既存のIT技術者、さらには経営層に至るまでを対象にしたサイバーセキュリティ教育訓練パッケージを国策で整備・運用する。年間数千人規模の専門人材を育成し、即戦力を持つ人材を安定的に輩出し、常に最先端のサイバーセキュリティスキルを堅持できるように運用される体制を構築する。また、国内での成果を基に同志国への能力構築支援プログラムも提供し、国際的なセキュリティ基盤の構築を支援する。

- **サイバー脅威インテリジェンス収集分析基盤の強化**
  中小企業を含む多様なエンドポイントからの情報収集を通じて、内外の脅威情報を高度に分析し、リアルタイムで活用できるインテリジェンス基盤を整備する。特に、セキュリティ対策が行き届かず標的にされやすい中小企業に対しては、政府が積極的に支援を行い、サプライチェーンの強靭化を図る。また、収集した脅威情報の正確性とデータ保護を担保するためのガイドラインを策定し、安全な運用体制の構築を推進する。加えて、信頼に基づく国際的なサイバー脅威インテリジェンス共有ネットワークを構築し、国際的なサイバー脅威に迅速かつ効果的に対応する体制を築く。

- **サイバーセキュリティのグローバルなコミュニティにおけるリーダーシップの発揮**
  国際標準化機関やアジア太平洋地域のセキュリティ連携の推進など、日本がリーダーシップを発揮できる場で積極的に関与し、国際会議での提案や他国との共同研究を通じた技術共有を推進する。こうしたリーダーシップを担う次世代人材を輩出するための育成プログラムを整備し、持続可能なリーダーシップを構築する。サイバーセキュリティ立国としてのプレゼンスを強化し、国際社会において信頼されるリーダーとしての地位を確立することを目指す。

- **スタートアップ企業と大企業間の協働を促進する枠組みの構築**
  日本には、特徴のあるセキュリティ製品開発を行っている中小企業やスタートアップも多くあるが、こうした企業が事業を推進する上で必要となる資金や販路などの経営リソースには限界がある。大企業が実績のないスタートアップ企業の技術を調達しやすくするため、政府や公的機関がスタートアップのサービスを先行導入することで信頼性を証明し、実績を積む場を提供する機会の提供も求められる。

たしかなテクノロジーで
「信じられる社会」を築く。

※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。