LAC
ともに、イキル

Little eArth Corporation

株式会社ラック

—ネットワーク社会の進展により、
時間的にも空間的にも地球は小さくなっていく—

第12期 中間報告書 2018.4.1～2018.9.30

証券コード：3857

事業紹介

当社は、他社に先駆けて始めたセキュリティ対策サービスと、独立系のITベンダーとして幅広い領域のSIサービスを提供しています。これら高い競争力を有する独自のサービスと、大手企業を中心とした確固たる顧客基盤を有していることを強みとしています。

2018年4月より製販一体で対応する事業部制としており、業界や地域特性にあわせた最適なソリューションを提供していきます。本体制のもと、セキュリティを切り口に両サービスを融合し、お客様のITによる変革「デジタルトランスフォーメーション」の実現に貢献します。

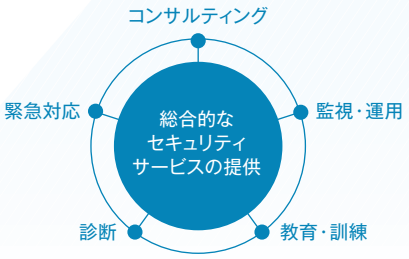
お客様

**セキュリティを切り口に経営層へ
アプローチ、事業課題へのIT提案**

SSS
セキュリティソリューションサービス

他社に先駆けサイバーセキュリティ
対策サービスを展開

**セキュリティエンジニアによる
専門的なサービスを提供**



SIS
システムインテグレーションサービス

金融機関や官公庁向けシステム開発で培った
技術力で幅広い領域のシステム開発

**基盤からアプリケーションの開発まで
一貫したSIサービスを提供**

製販一体で対応する事業部制

金融事業部	エンタープライズ事業部	通信インフラソリューション事業部	中部事業部	エリアビジネス開発部	アジャイル開発センター（2018年10月1日～）
サイバーセキュリティ事業部					

変革に向け、力強く前進し続けています。

『TRY 2021 ステージ 2』をスタート

当期からスタートした新たな3カ年中期経営計画『TRY 2021 ステージ 2』では、独自の強みであるセキュリティ対策を切り口とした、総合的なITソリューションを提供するビジネスモデルへの変革を進めています。2019年3月期第2四半期は、SSS事業が好調に推移した一方、SIS事業におけるHW／SW販売の減少等により減収となりました。営業利益は、サービス売上が伸長したことにより大幅な増益となりました。中間配当につきましては、記念配当を除き前年同期比1円の増配となる1株当たり10円とさせていただきました。

2018年10月23日、株式会社日本貿易保険から「次期貿易保険システム開発の入札等における不正について」の発表がございました。株主の皆様にご心配をおかけしましたことを深くお詫び申し上げます。10月25日に公表しましたとおり、当社調査委員会の調査では、不適切行為に当社社員が不当に関与したとは認識しておりません。新しい事実が判明した場合には、誠意をもって対応いたします。

お客様の真のパートナーとなるために

『TRY 2021 ステージ 2』では、働き方改革や生産性向上、業務効率化等のデジタルトランスフォーメーションを進めるお客様の事業を支える「真のパートナー」となることを目指しています。4月に実施した「事業部制」への移行もその一環です。新たな体制では、業界・地域特性に合わせてお客様視点でセキュリティ対策とシステム開発を総合的に提供しています。7月のアジャイル開発センターの新設も、お客様と一体となって社会の変化に応じたシステムをタイムリーに開発していくことを目的としています。

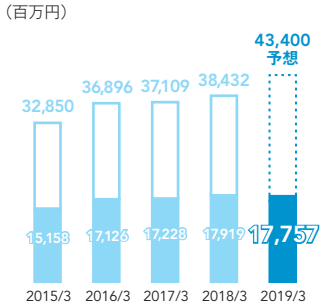
業績ハイライト

第2四半期連結累計期間
通期

売上高

177億57百万円

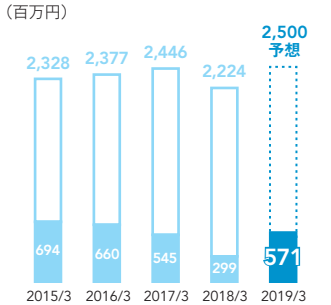
前年同期比0.9%減↘



営業利益

5億71百万円

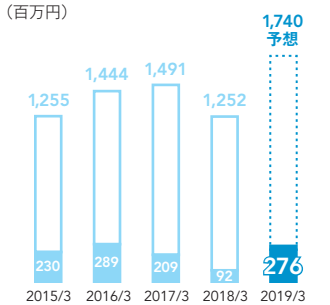
前年同期比91.1%増↗



親会社株主に帰属する当期（四半期）純利益

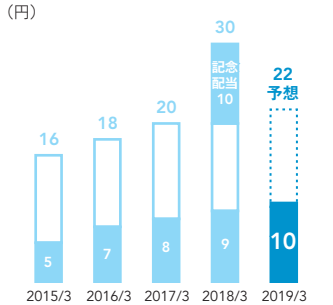
2億76百万円

前年同期比197.9%増↗



1株当たり配当金

10円



競争力のあるサービスの提供

環境変化を好機と捉えて成長を続けるため、数々の競争力のある独自サービスを打ち出しています。

近年、サイバー攻撃はますます巧妙化・複雑化しています。「サプライチェーン攻撃」はその一例です。大企業のみならず関連子会社や中堅・中小企業などの取引先も脅威にさらされていますが、人材確保や費用が大きな課題となり、セキュリティ対策が十分に行き届いていないことも少なくありません。10月にサービスを開始した「CloudFalcon（クラウドファルコン）」は、そうした課題を解決する低価格で高品質なサービスです。これは、大手企業向けに提供してきた当社の事業基盤「LAC Falcon®」をもとに独自に開発した自動セキュリティ監視システムで、全国の中堅・中小企業をカバーします。このほか「IoTセキュリティ診断サービス」や「産業制御システム向けリスクアセスメントサービス」をメニュー化するなど（➔NEWS）、日本のお家芸である工場など産業分野向けのサービス拡充にも取り組んでいます。また6月には、ASEAN地域で成長を目指す日系企業のセキュリティ対策を支援する拠点として、シンガポール支店を設立しました。これを足掛かりに、海外市場の開拓に取り組んでいく考えです。

業界のリーダーとして

技術の進化を背景とした社会変革に加え、来年のラグビーワールドカップや2020年の東京オリンピック・パラリンピックなどの世界的なイベントも控えるなど、セキュリティ対策ニーズは今後も拡大が見込まれます。当社は、『TRY 2021 ステージ2』の4つの基本方針に基づく取り組みを着実に進めていくとともに、新たな事業の柱の構築にも挑戦していきます。10月に新設した新規事業開発部では、ベンチャー支援や他社とのコラボレーションを通じ、まったく新しい領域での事業開発も模索していく方針です。

これまで当社は、ベンチャー気質の強い企業として様々な挑戦を行ってきました。これからもセキュリティ対策の「リーダー」として、『TRY 2021 ステージ 2』で掲げた目標の達成と、ビジネスモデルの変革に引き続き邁進し、日本のセキュリティ対策の底上げに広く貢献してまいります。

株主の皆様におかれましては、中長期的な視点で持続的成長に向けて突き進む当社に、引き続きご支援を賜りますよう、お願い申し上げます。

代表取締役社長

セグメント別概況

SSS事業

サービスを中心に大幅増収
利益も大幅に伸長

売上高

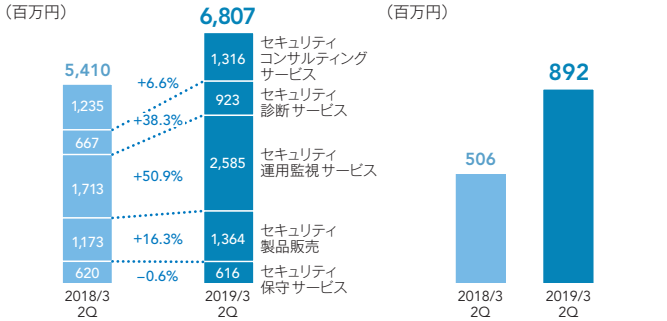
68億7百万円

前年同期比25.8%増↗

セグメント利益

8億92百万円

前年同期比76.2%増↗



SIS事業

HW／SW販売が低調で減収
のれん償却額負担減等もあり増益

売上高

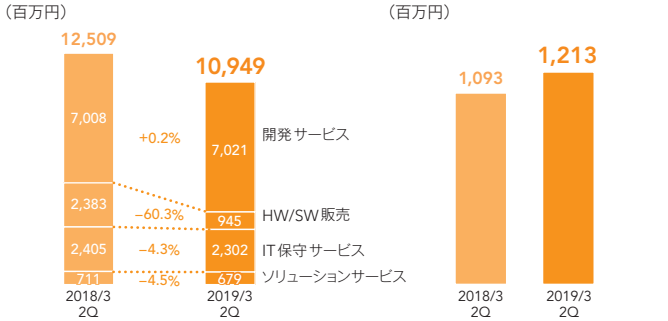
109億49百万円

前年同期比12.5%減↘

セグメント利益

12億13百万円

前年同期比11.0%増↗



アンケート結果

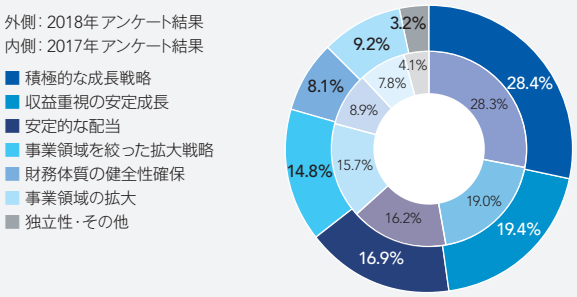
今回の調査では、前回とほぼ同数の1,053名の株主様よりご回答をいただきました。

当社の経営に対しては、前回に続き当社の積極的な成長に大きく期待を寄せられる結果となりました。また、自由記入欄では、「セキュリティ事業の将来性」を期待される声が多く寄せられました。

今後も株主の皆様のご期待にお応えできるよう、企業価値の向上に努めてまいります。

当社の経営に対して期待すること

外側：2018年アンケート結果
内側：2017年アンケート結果



会社情報

会社概要（2018年9月30日現在）

商　号	株式会社ラック
英文名	LAC Co., Ltd.
所在地	〒102-0093 東京都千代田区平河町2丁目16番1号 平河町森タワー
設　立	2007年10月1日
資本金	10億円
従業員数	連結：2,137名（SSS事業:832名、SIS事業:1,151名、管理部門:154名） 個別：1,444名 ※連結・個別ともに契約社員含む

役員（2018年6月19日現在）

取締役会長	髙梨 輝彦		
代表取締役社長	西本 逸郎		
取締役	英 秀明	齋藤 理	小林 義明
	三木 俊明	川本 成彦	
社外取締役	西川 徹矢	村井 純	
常勤監査役	伊藤 信博		
社外監査役	高井 健弐	斎藤 昌治	

株式情報（2018年9月30日現在）

株式の状況

発行可能株式総数	100,000,000株
発行済株式の総数	26,683,120株
株主数	10,556名

大株主

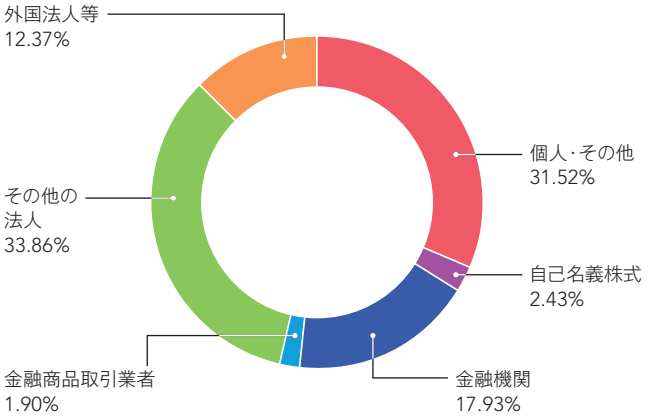
	所有株式数（株）	所有比率（%）
有限会社コスモス	6,889,800	25.82
日本トラスティ・サービス信託銀行株式会社（信託口）	3,380,700	12.66
KDDI株式会社	1,414,200	5.29
ラック従業員持株会	903,810	3.38
三柴 照和	760,000	2.84
NORTHERN TRUST CO. (AVFC) RE HCR00	694,800	2.60
株式会社ベネッセホールディングス	500,000	1.87
資産管理サービス信託銀行株式会社（信託E口）	477,000	1.78
資産管理サービス信託銀行株式会社（証券投資信託口）	299,600	1.12
髙梨 輝彦	264,300	0.99

※有限会社コスモスは、KDDI株式会社の100%子会社であります。

株主メモ

事業年度	4月1日～翌年3月31日
期末配当金受領株主確定日	3月31日
中間配当金受領株主確定日	9月30日
定時株主総会	毎年6月
株主名簿管理人特別口座の口座管理機関	三菱UFJ信託銀行株式会社
同連絡先	三菱UFJ信託銀行株式会社 証券代行部 東京都府中市日鋼町一丁目1番 Tel: 0120-232-711（通話料無料）
上場市場	東京証券取引所JASDAQ（スタンダード）
公告の方法	電子公告により行う。 公告掲載URL https://www.lac.co.jp/ （ただし、電子公告によることができない事故、その他のやむを得ない事由が生じたときは、日本経済新聞に公告いたします。）

所有者別株式分布状況



株式事務手続き

1. 当社株式に関する以下のお手続きにつきましては、口座を開設されている証券会社等にお問合せください。株主名簿管理人（三菱UFJ信託銀行）ではお取り扱いできませんのでご注意ください。

住所変更	氏名変更	相続
配当金振込指定	株式異動状況等証明発行	単元未満の買増・買取

など

2. 特別口座に記録された株式に関する各種お手続きにつきましては、三菱UFJ信託銀行が口座管理機関となっておりますので、上記特別口座の口座管理機関（三菱UFJ信託銀行）にお問合せください。なお、三菱UFJ信託銀行全国各支店でもお取次ぎいたします。

3. 未受領の配当金につきましては、株主名簿管理人連絡先へお問合せください。

お問合せ
コーポレート・コミュニケーション室
Tel: 03-6757-0107 / E-mail: ir@lac.co.jp

当社ホームページでは、IR情報のほか、自社メディア「LAC WATCH」において、最新のセキュリティ情報やラックの取り組みを発信しています。是非ご覧ください。https://www.lac.co.jp/

執行役員インタビュー

セキュリティ事業の「次の20年」に向けた変革

**IT利活用の進展を背景に、国家として
サイバーセキュリティレベルの向上が急務となっています。
今回の特集では、日本全体のセキュリティ対策の底上げに向けて、
事業モデルの変革に踏み出したセキュリティ事業の取り組みを、
事業全体を統括する常務執行役員の中間に聞きました。**

常務執行役員
サイバーセキュリティ事業部長
SSS事業統括部長
中間 俊英

ラックのサイバーセキュリティ事業の生い立ちと、サイバー攻撃のこれまでの変化について教えてください。

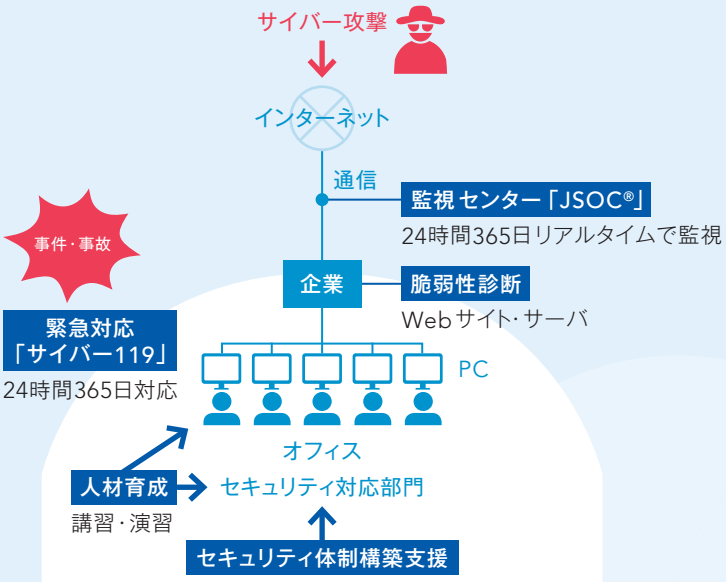
ラックのサイバーセキュリティ事業は、1995年に、ネットワークに侵入した攻撃者から、PCなどから情報を持ち出されるようなセキュリティホールがないかを診断するサービスからスタートしました。その後、2000年にネットワークを監視する運用監視、サイバー攻撃に遭った際に企業へ駆けつけて対応する緊急対応など、日本では他社に先駆けてサービスを提供してきました。

当時のサイバー攻撃は、自身の主義主張や技術力を誇示することが主な動機で、オリンピックやサミットといった国際的・政治的な色彩があるイベントのタイミングに攻撃が増加していました。現在は、金銭の搾取を目的としたものが中心となり、時に特定の組織のITインフラ基盤を破壊する「サイバーテロ」の脅威も広がりつつあるなか、いつ攻撃を仕掛けてくるかわからないような状況となっています。しかも攻撃手法は巧妙化しており、ターゲットを特定して効率的・効果的に攻撃し、被害規模は拡大する傾向にあります。

2017年に猛威を振るった身の代金要求型ウイルス「WannaCry」

システム上の文書、画像、動画などのファイルを暗号化し、それらのファイルの復号を条件として金銭を要求したり、システムを機能停止させたりする攻撃です。ネットワークを通じて感染拡大を試みる機能があり、2017年には、150ヵ国に感染が広がり、海外では医療機関のシステムを停止させ、日本でも事業所や製造ライン全体へと感染が拡大した事例がありました。

ラックのセキュリティに関するトータルソリューション



導入実績数（2018年4月時点）

サービス名	累計導入件数	企業	官公庁・地方公共団体
コンサルティングサービス	1,320件	1,140件	180件
セキュリティ診断サービス	8,300件	7,500件	800件
救急対応サービス	2,600件	—	—

サービス名	導入数	企業	官公庁・地方公共団体
セキュリティ監視サービス	920社／団体	765社	155団体

ラックのセキュリティサービスの特徴はどこにありますか？

これまでラックはどちらかといえば大手企業や官公庁向けにサービスを提供してきました。特に金融関係などは、被害が大きくなることが想定されるため、大きな費用をかけてでもセキュリティ対策を取る必要があったためです。なかでも、ラックのセキュリティ運用・監視サービスは、より高度な対策として、専門のアナリストが24時間365日お客様のネットワークを監視・分析し、これまで重大な事件・事故となることを未然に防いできました。救急対応など事件・事故が起きた現場で経験を積んだセキュリティ人材をはじめ、高度なノウハウ・知見を持つ人材が高品質なサービスを提供していることが当社の強みとなっています。そして、お客様のセキュリティ部門の体制構築の支援から、その知識習得のための講習や実践的な演習、お客様がサービスを提供するためのネットワークやウェブサイトを立ち上げる際に、不正に侵入されるプログラム上の抜け道がないかの脆弱性診断、先にも述べたネットワークの常時監視など、総合的なラインアップでサービスを提供しているのが当社の特徴といえるでしょう。

専門のセキュリティアナリストが24時間365日、サイバー攻撃を監視する「JSOC®」

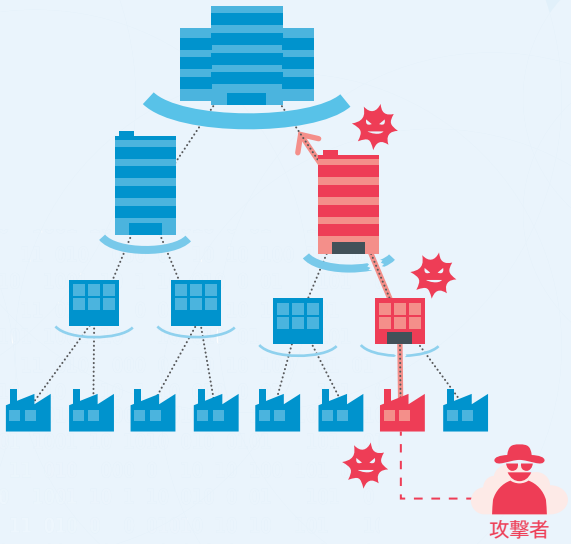
巧妙化するサイバー攻撃に対し、ラックはどのように取り組んでいくのでしょうか？

私はサイバーセキュリティ事業部長として、1年や2年といった時間軸で事業の舵取りを行う一方、兼務するSSS事業統括部長というセキュリティ事業全体の責任者の立場では、その先5年後といった中長期的な視点で、他の事業を含めてセキュリティ事業全体の戦略を策定・推進しています。

近年、サイバー攻撃は、様々な対策を講じている大手企業だけではなく、セキュリティに費用をあまり割けない子会社や取引先を対象とし、そこから大企業への攻撃に繋げるなど巧妙化しており、サプライチェーン全体でのセキュリティ対策が大きな課題になっています。さらに、AIをはじめ技術の高度化・複雑化により、被害が広範囲にわたる危険性もあります。また今後、日本の労働人口が減少していくことは間違いありません。そのなかで、現場対応力に裏付けられた高度なノウハウを持つセキュリティ人材の確保は、年々困難になっていくことが予想されます。巧妙化するサイバー攻撃に対し、技術者によるサービスの高度化は当然必要となりますが、セキュリティ対策を実装する層を中堅・中小企業まで広げるには、なるべく人を介さずに、インフラとして誰もが使え、さらに安価なサービスが必要となります。そうしたなか、当社は20年以上蓄積してきたノウハウや情報を差別化要素として内部に抱えるのではなく、それらを活用しやすいソリューションに変えて幅広い方々にご活用いただき、

サプライチェーン攻撃

対策が脆弱な企業や取引先を標的としてサプライチェーンに侵入し、被害を拡散させる攻撃



日本全体のセキュリティ対策の底上げに貢献できるよう、事業の方向性を大きく変えていきます。

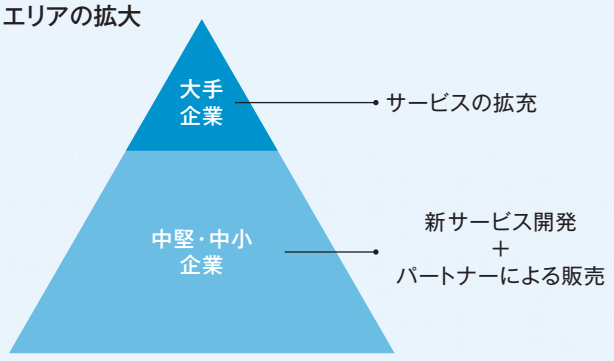
こうした考えを象徴するサービスが10月より提供を開始した「CloudFalcon（クラウドファルコン）」です。

「CloudFalcon」とはどのようなサービスですか。

「CloudFalcon」は、セキュリティアナリストによる高度な監視サービスのノウハウを投入した、自動セキュリティ監視システムです。クラウド上で稼働させることにより低価格を実現し、これまでセキュリティ対策に投資できなかった中堅・中小企業の課題解決に貢献します。

またこのサービスは、ラックが直接お客様に販売するものではありません。これまで中堅・中小企業へサービスを提供し、これらのお客様をよく知っているパートナー企業へ卸販売して広げていきます。導入企業の裾野を広げることで蓄積される脅威情報をもとに、セキュリティビジネスの付加価値を高める好循環を回していきたいと考えています。今後はAIによる分析ルール自動生成機能を拡張する予定です。

事業エリアの拡大



「CloudFalcon」の特徴

LAC Falcon®で開発してきた20万を超える分析ルールに加え、JSOC®やサイバー救急センター®などサイバー攻撃の最前線で得られる脅威情報から新たに生成される分析ルールを適用しています。クラウド上でシステム稼動させることにより費用・運用負荷の大幅低減も実現しています。

独自開発の分析システム「LAC Falcon®」

サイバー攻撃とみられる通信の中から危険度の高いものを抽出

約16億件／日 → 約1万件／日

専門のアナリストの分析

クラウド対応の自動分析エンジン開発

- LAC Falcon®の20万を超える分析ルールの適用
- 最新の脅威に対応した分析ルールの随時適用
- AIを活用した分析ルール自動生成機能の適用（予定）

大企業に留まらず
中堅・中小企業にも拡販

最後に今後の抱負をお聞かせください。

セキュリティビジネスに対する社会の関心が高まっています。しかし、セキュリティ事業は開始から20年以上経過し、一般的にいわれる30年という事業ライフサイクルの終盤に差し掛かっています。私の使命は、次の20年も発展するために、これまでの成功体験に基づく固定観念や先入観を捨て去り、新しい時代に合わせてビジネスのあり方を変えていくことだと考えています。

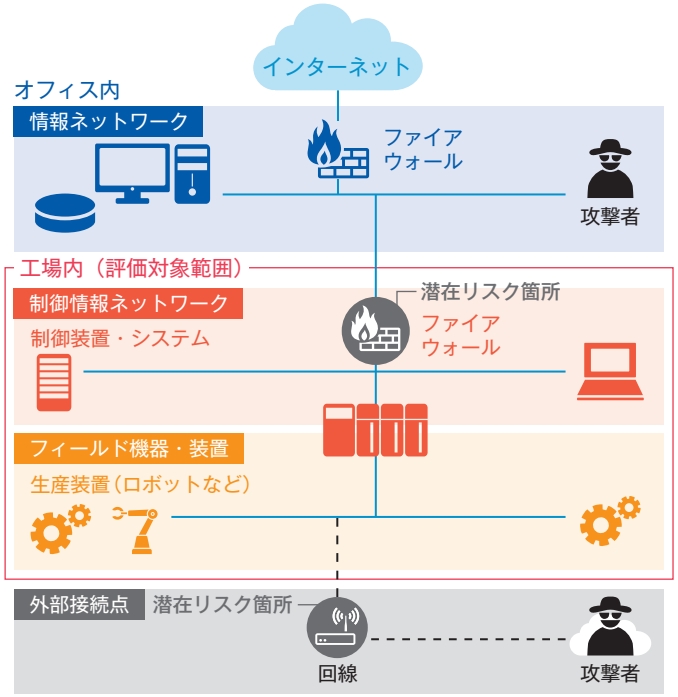
日本のすべての企業や人々をサイバー攻撃から守ることは、ラック1社ではできません。事業の立ち位置を競争から連携に移し、フィールドを大企業中心から社会全体に広げ、サービスの付加価値を高めながら、新たなステージに行くための10年に変えるべく、スピード感を持って変革を推進していきます。

NEWS

産業分野向けのセキュリティサービスを強化

工場の制御システムは、ネットワークが工場内で閉じられていることが多く、セキュリティ対策とは無縁とされてきました。しかしながら工場内でもネットワーク化が加速し、さらに品質や生産性向上のためIoTの活用が求められていることからセキュリティ対策を必要とする企業が増えています。このような背景のもと、当社はこれまで個別に対応していた総合的なリスク評価「産業制御システム向けリスクアセスメントサービス」をサービスメニュー化しました。日本の製造現場に存在する特有のリスクや潜在的なリスクを独自の手法で調査し、サイバー攻撃から企業を守ります。

また、社会に広がりつつある多種多様なIoT機器は、サイバー攻撃を受けると甚大かつ広範囲な被害が生じると想定されます。当社は、このような機器の脆弱性をソフトウェア、ハードウェア、ネットワークに至るまで総合的に診断する「IoTセキュリティ診断サービス」の提供も開始しました。



産業制御向けリスクアセスメント

「ラックテクノセンター北九州」を開設

地域における人材採用と事業展開を推進する一環として、2019年1月に「ラックテクノセンター北九州」を開設します。開設に際し、8月1日、北九州市役所本庁舎で福岡県北九州市の北橋市長と、社長の西本による記者会見が行われました。

2019年4月に、現地採用者10名と合わせて15名で運営を開始する予定です。本社での開発とは別に、セキュリティ監視センター「JSOC®」の基幹システム「LAC Falcon®」の開発および保守の一部を担います。

記者会見の様子

JSOC®にサイバー保険を付帯し、「守り」と「備え」を一体として提供

IT社会において、サイバー空間で事件・事故が実際に起きたときの影響は非常に大きいものの、自動車保険のような保険と連動した事故対策は未だ導入が進んでいないのが現状です。ラックは損害保険ジャパン日本興亜株式会社と、サイバー保険をセキュリティ監視サービスに付帯した国内初のパッケージ商品「事故補償パック for JSOC®」の提供を開始しました。JSOC®の品質と実績をもとにした保険料率での加入が可能であり、サイバー攻撃に遭った際には迅速な対応を取ることができるため、被害抑制にも貢献します。

事故補償パック for JSOC® サービス内容