LAC

証券コード
3857

第17期
中間報告書

2023.4.1 – 2023.9.30

特集

身近なサイバー攻撃と
その対策

ランサムウェア×フィッシング詐欺

INDEX

操作ガイド

タブキーの使い方　クリックすると該当のページへ移動できます。

目次に移動

トップメッセージ | 業績ハイライト | 身近なサイバー攻撃とその対策 | ラックニュース | INDEX

https://www.lac.co.jp/ir/library/nenji.html

クリックすると詳細ページや外部サイトなどのリンク先に飛びます。

トップメッセージ

持続的な収益拡大に向けた事業の成長戦略と社内の生産性向上に取り組みます

代表取締役社長　西本 逸郎

POINT 1

セキュリティ事業は製品販売や運用監視サービス、
SI事業は開発サービスなどが伸長し増収増益

POINT 2

期初に掲げた主要施策について
両事業ともに着実に進捗

POINT 3

中間配当金は予定通り1株当たり12円に決定
通期業績予想は期初予想から変更なし

トップメッセージ

両事業とも着実に施策が進捗し増収増益

新型コロナウイルス感染症の位置づけが5類へ移行し、社会・経済活動は正常化に向けた動きが進められた一方で、円安やウクライナ情勢の長期化の影響により資源・エネルギー価格が高騰するなど依然として不透明な情勢が続きました。

このような状況において、当社は期初に掲げた事業の主要施策を着実に進めました。セキュリティ事業では、デジタル庁や大手小売業向けに高度な対策を行う個別監視のサービス運用を開始するとともに、エンドポイント対策支援サービスも順調に拡大しました。診断サービスは、期末での一括計上を予定しているペネトレーションテストサービスの大型案件が第１四半期から着実に進捗しました。緊急対応サービスは、大規模化、複雑化する緊急対応案件に対して協業による事業体制の強化を進めました。

SI事業においては、クラウド型サービスの導入支援に関わるシステム開発案件の提供とともに、技術者単価の押し上げに向けたリスキリングを着実に進めました。

これらを踏まえ、上期の業績は、セキュリティ事業において製品販売や運用監視サービスなどが拡大したこと、またSI事業において開発サービスやHW／ＳＷ販売などが伸長したことにより、売上高、営業利益とも増収増益となりました。なお、中間配当金は予定通り1株当たり12円に決定いたしました。

生産性向上など全社的な取り組みを推進

当社は全社的な取り組みとして、社内生産性向上のための生成ＡＩの活用を進めています。全社横断組織を設立し、社内ルールの整備等を進めるとともに、当社専用の対話型生成AIを開発しており、活用を具体化していく考えです。

また、新たな働き方に対応したオフィス戦略として、平河町オフィスの減床を含む全面リニューアル等の計画を進めています。契約更改に伴う短期的な費用計上はあるものの、2026年3月期以降に大幅なコストダウンを見込んでいます。

通期業績予想については、オフィス戦略による計画外の費用負担が見込まれるものの、上期の事業の進捗として概ね順調に推移していることから変更はありません。引き続き、セキュリティ事業において競争力の向上を目指した成長戦略を進めるとともに、ＳＩ事業における収益力の強化に取り組んでまいります。

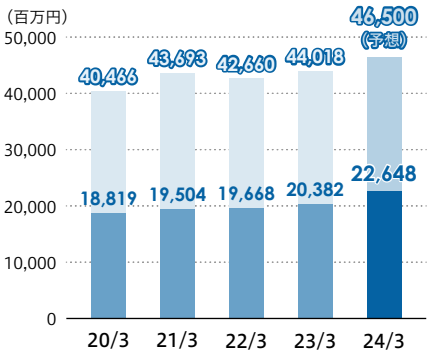
今後とも当社は、「たしかなテクノロジーで『信じられる社会』を築く。」というパーパス（存在意義）のもと、持続的な成長に向けて取り組んでまいります。株主の皆様におかれましては引き続き中長期的な視点でご支援いただきますよう、よろしくお願い申し上げます。

代表取締役社長　西本逸郎

業績ハイライト

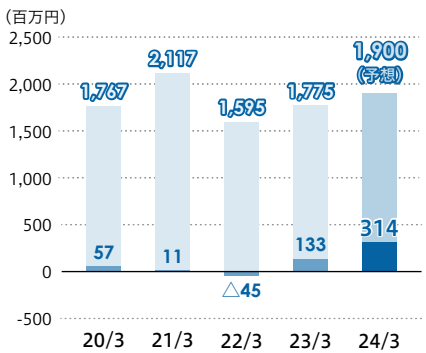
売上高

226億48百万円　前年同期比 +11.1%



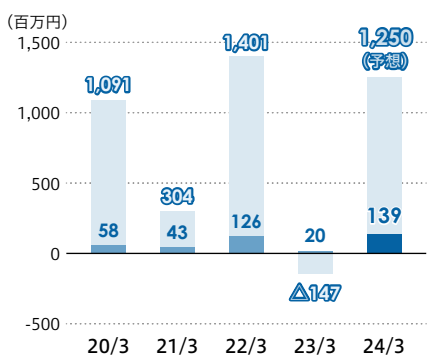
営業利益

3億14百万円　前年同期比 +135.8%



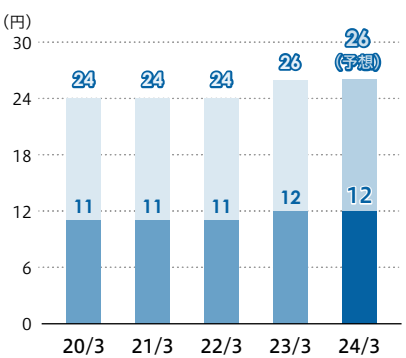
親会社株主に帰属する四半期(当期)純利益

1億39百万円　前年同期比 +589.0%

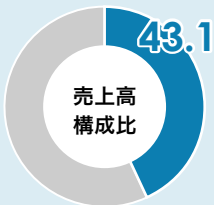


1株当たり配当金

12円



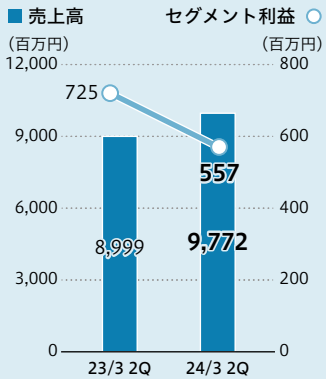
SSS(セキュリティソリューションサービス)



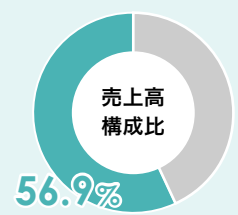
売上高
97億72百万円　前年同期比 +8.6%

セグメント利益
5億57百万円　前年同期比 △23.1%

クラウド対応製品等で製品販売が大幅に拡大したほか、個別およびエンドポイント向けの運用監視サービスが拡大したことなどにより増収となりました。利益は、大型案件での先行稼働や事業体制強化のための先行投資等の影響により減益となりました。



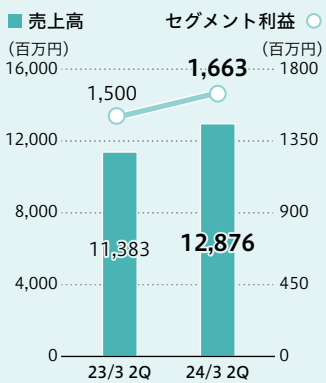
SIS(システムインテグレーションサービス)



売上高
128億76百万円　前年同期比 +13.1%

セグメント利益
16億63百万円　前年同期比 +10.9%

金融業や公共向けに開発サービスが大きく伸長し、更新案件等の獲得でHW/SW販売が大幅に拡大するとともに、サイバーセキュリティ対策にも寄与するクラウドソリューション製品が拡大したことなどにより、増収増益となりました。



身近なサイバー攻撃とその対策

情報セキュリティ10大脅威2023

https://www.ipa.go.jp/security/10threats/10threats2023.html

組織

- 1位 ランサムウェアによる被害
- 2位 サプライチェーンの弱点を悪用した攻撃
- 3位 標的型攻撃による機密情報の窃取
- 4位 内部不正による情報漏えい
- 5位 テレワーク等のニューノーマルな働き方を狙った攻撃

個人

- 1位 フィッシングによる個人情報等の詐取
- 2位 ネット上の誹謗・中傷・デマ
- 3位 メールやSMS等を使った脅迫・詐欺の手口による金銭要求
- 4位 クレジットカード情報の不正利用
- 5位 スマホ決済の不正利用

社会的に影響が大きかったと考えられる情報セキュリティにおける事案からIPA（独立行政法人情報処理推進機構）が10大脅威を選出し、「組織」と「個人」の立場別に発表しています。「組織」においては、「ランサムウェアによる被害」が１位となっており、ラックが脅威への課題解決に貢献しています。また、「個人」では「フィッシングによる個人情報等の詐取」が１位となり、2023年上半期の被害額が30億円に達しています。

本特集では、各１位の脅威の概要とともに、組織に対するラックの取り組みや、個人への被害対策について解説します。

身近なサイバー攻撃とその対策

ランサムウェアとは？

ランサムウェアとは、何らかの方法で企業内ネットワーク内に侵入し、サーバを暗号化（ロック）することで事業停止に追い込み、解除のために仮想通貨などの金銭を要求する身代金要求型ウイルスです。盗んだ機密データを公開すると脅す「二重脅迫型」と呼ばれる攻撃も常態化しています。

日本国内で報道されている最近の被害事例として、病院内の多くのPCやサーバが感染し、2か月にわたって電子カルテのシステムや医事サーバが利用できなくなったり、ある企業が１か月にわたって約3,400の法人・企業顧客へ正常にサービスが提供できなくなったりした事例があります。影響度合いが大きいことから「経営上のリスク」にもなっており、ラックでも取り組みを強化しています。

ランサムウェア

対策に貢献する主なサービス事例

対策その❶

被害の予防

サーバなどがセキュリティ上問題ない設定になっているかを調査するセキュリティ診断が予防に役立っています。また、エンドポイント対策サービスも被害予防につながっています。

対策その❷

攻撃を意識した運用

人がリスク対策の原点であるとの認識のもと、標的型メール訓練などの教育サービスを提供しています。加えて、不正な通信を常時監視する監視サービスが運用面で大きく貢献しています。

対策その❸

被害への対応

被害にあった際は感染の影響度合いを調査する必要があり、サイバー救急センターによる支援を行っています。また、コンサルティングサービスによる再発防止対策の提供も行っています。

フィッシング詐欺

フィッシング詐欺とは？

フィッシング詐欺とは、実在する企業やブランドをかたり、サービス利用者情報の確認などと謳って、偽の電子メールやSMS（ショートメッセージサービス）などを配信し、本物と酷似した偽物のWebサイトで利用者情報を入力させて金銭などを騙し取ろうとするサイバー犯罪です。

被害事例として、銀行やカード会社などのなりすましに気が付かず利用者情報を入力してしまい銀行の口座情報やクレジットカード番号などを盗まれたり、携帯電話会社や宅配業者の偽サイトへ誘導されIDやパスワードを入力してしまい利用者情報を盗まれたりする事例があります。いずれも引き落としができなかったなど危機感をあおる手口が多くみられます。

当社セキュリティ啓発担当者が伝える 身の守り方

ポイント❶

メールやSMSのリンクは開かない

銀行やクレジットカード会社などが電子メールやSMSで個人情報の入力を求めることはないため、本文中のリンクはクリックせず、必要な場合は正規のURLを確認してアクセスください。

ポイント❷

メールの連絡先に電話しない

フィッシングなのか判断に迷う場合は、送られてきたメールに記載の連絡先ではなく、お気に入り登録している正規のWebサイトや郵便物で連絡先を確認してください。

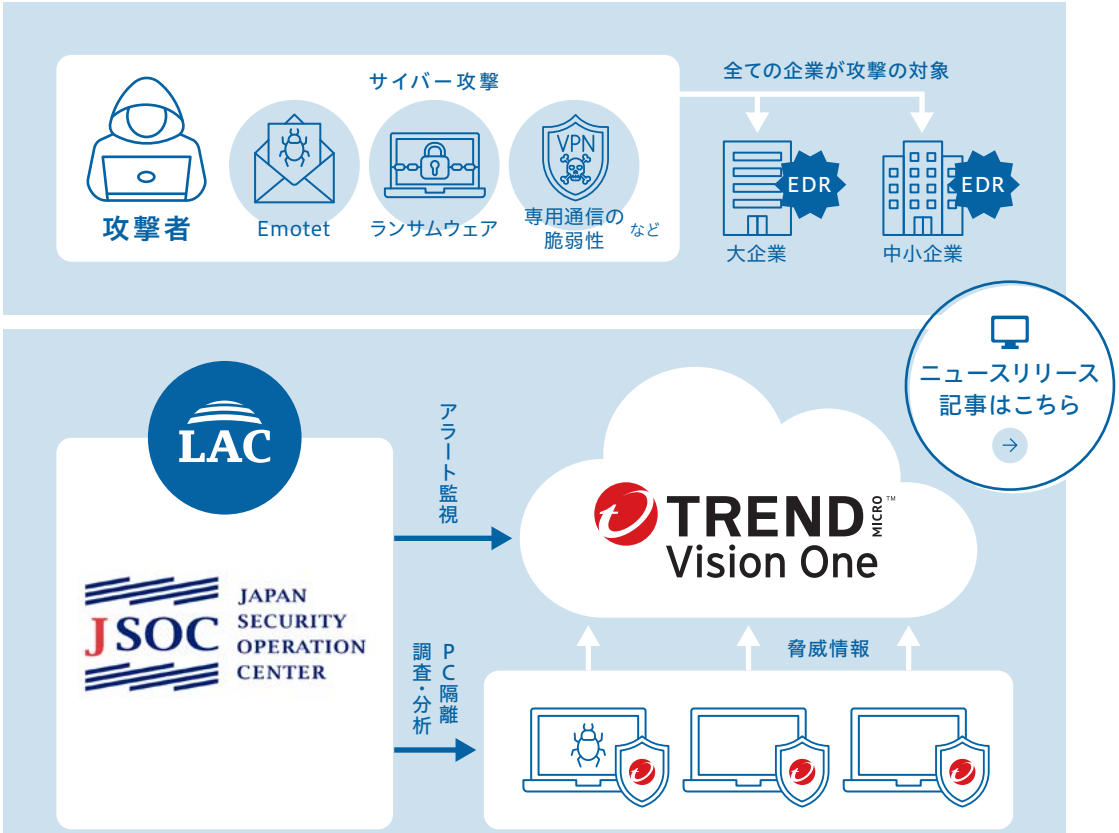
ポイント❸

セキュリティ上の欠陥をつくらない

セキュリティ上の欠陥を狙われる場合もあるため、ウイルス対策ソフトを導入し、OSやWebブラウザ、ソフトウェアなどを常に最新のものに更新してください。

ラックニュース

エンドポイント対策ビジネスの拡大



マネージドEDRサービス for Trend Micro™ のサービスイメージ

中堅・中小企業のランサム攻撃被害を防ぐエンドポイント対策支援サービスにトレンドマイクロ製品を追加

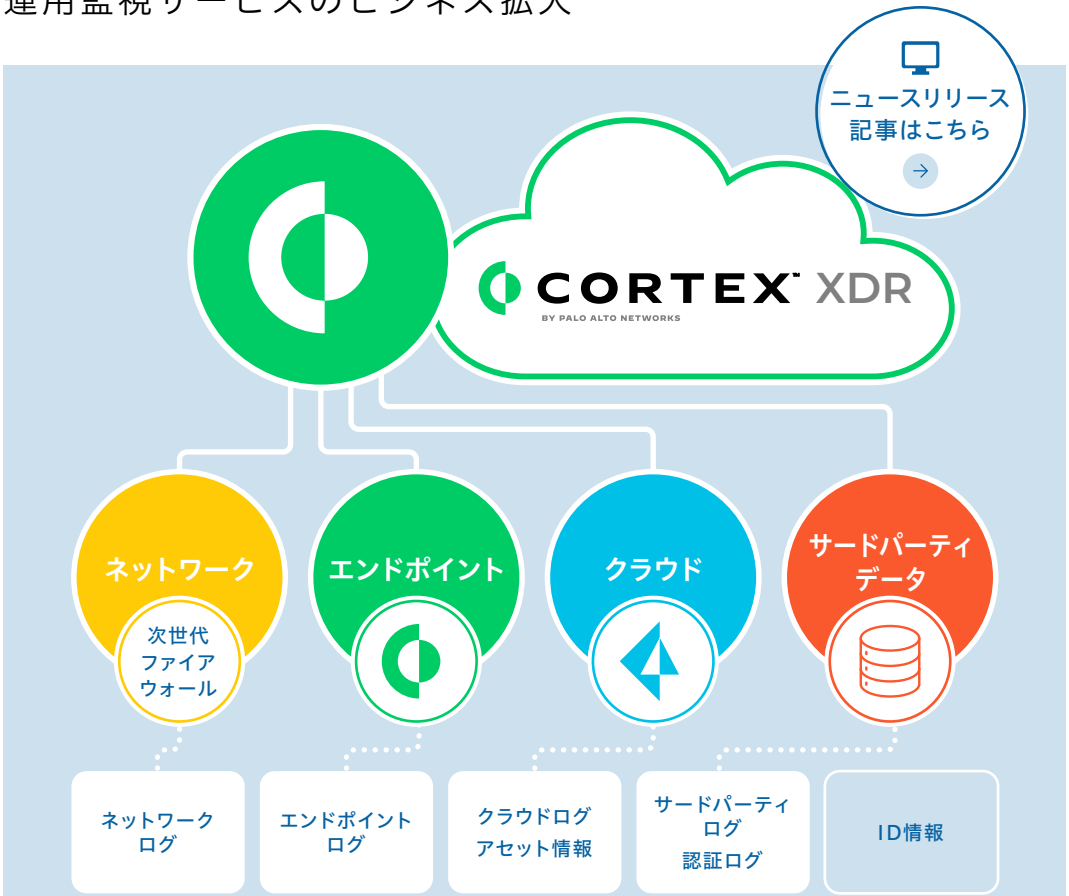
当社はランサム攻撃への有効な対策として、これまで大企業を対象にエンドポイント対策支援サービスを提供しています。

大企業のサプライチェーンや取引先となっている中堅・中小企業にまでランサム攻撃の脅威が広がるなか、企業規模を問わず利用しやすいトレンドマイクロ製品を当社のエンドポイント対策支援サービスのラインアップに追加し提供を開始しました。

本サービスは、①24時間365日でサイバー脅威を監視できること、②危険性の高いサイバー脅威に対し自動隔離できること、③取引先などへの説明や今後の対策に利用可能な詳細調査報告書を作成できることなど、中堅・中小企業が抱えるサイバーセキュリティに対する課題にも対応しているのが特徴です。

※EDR：Endpoint Detection and Responseの略。PC端末等のエンドポイントを狙った標的型攻撃など高度な脅威への対策手法のこと。

運用監視サービスのビジネス拡大



Cortex XDRの機能イメージ

パロアルトネットワークスのXDR製品向けの運用監視サービスの提供を開始

サイバー脅威の複雑化や働き方の変化により、サイバー攻撃手法は多様化しています。単一のセキュリティ製品だけでは、多様な脅威を検出し、脅威の全体像を把握することが難しくなっており、複数の情報を統合して検知・分析することが求められています。

こうしたなか、当社はエンドポイント、ネットワーク、クラウドなどの異なる監視領域で収集したデータを統合管理・分析し、サイバー攻撃を迅速かつ効率的に可視化できる機能をもつ、パロアルトネットワークスのXDR製品向けの運用サービスの提供を開始しました。

これまで対応が難しかったネットワークへの侵入後のサイバー脅威を検出でき、セキュリティ製品単体では見つけられない不審なふるまいなどからサイバー脅威を監視・分析できます。

※ XDR：Extended Detection and Responseの略。エンドポイント、ネットワーク、クラウドなどの異なる監視領域で収集したデータを統合管理・分析し、サイバー攻撃を迅速かつ効率的に可視化できる機能。

ラックニュース

社内生産性向上への取り組み

生成AIに対する主な活動内容

戦略立案
会社としての生成AI対応戦略を立案し推進・支援・監督する

ラボ機能
生成AIに関する実証環境を準備して社内に提供する

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

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する

プレゼンス
エバンジェリストの生成と排出および、社外広報活動

生成AIに対する施策の一例

- 生成AIの利用や自社開発におけるガイド、ルールの整備
- ChatGPT Plus（有償版）を希望する社員に利用料金を会社で負担
- 生成AIを社員が安全に利用することができる独自アプリの提供
- ChatGPTをシステム実装する場合のリファレンスモデルの提供
- 生成AIの社内活用推進サポート（勉強会など）

ニュースリリース記事はこちら

ラックでの生成AI活用を積極推進

当社は、すべての社員が生成AIを自らの業務で活用し、高い生産性を発揮して事業に活用することを目的に、2023年6月に組織横断の生成AI利用の支援組織「GAI CoE」を立ち上げました。

同組織には、経営幹部をはじめ、エンジニア部門、管理部門、営業マーケティング部門などから選ばれた約30人が所属しています。会社としての生成AI対応戦略の立案、実証環境の準備と提供、自社開発におけるガイドやルールの整備、業務改善をリードする人材の社内育成など様々な活動を行っています。

また、実施した施策例として、生成AIを社員が安全に利用することができる独自アプリの提供や、ChatGPTをシステム実装する場合の標準モデルの提供、社内勉強会などを行いました。

ラック専用の対話型生成AI「lacgai」やChatGPTを使ったAIアシスタント「ChottoChat（ちょっとチャット）」を開発するなど、AI活用を積極的に進めています。

※ GAI CoE：Generative AI Center of Excellenceの略。

ラックニュース

ラック社員の活躍

ニュースリリース記事はこちら

国際CTF大会「ICC 2023」に出場しAttack & Defense部門で優勝

当社のデジタルペンテスト部に所属する井手脩太が、2023年8月1日から4日にかけて、米サンディエゴで開催された「International Cybersecurity Challenge 2023（ICC 2023）」に、アジアチームのメンバーとして出場し、Attack & Defense部門で優勝しました。

ICCは、情報セキュリティのスキルを競い合う国際大会です。世界の地域ごとに編成されたアジア、アフリカ、カナダ、欧州、ラテンアメリカ、オセアニア、米国の7チームが参加し、井手はアジアチームの一人として出場しました。

情報システム部門エンジニアが「Microsoft Top Partner Engineer Award」を受賞

当社の情報システム部門に所属する谷口隼祐が、日本マイクロソフト株式会社（日本マイクロソフト）が2023年に新設したアワード「Microsoft Top Partner Engineer Award」を受賞しました。

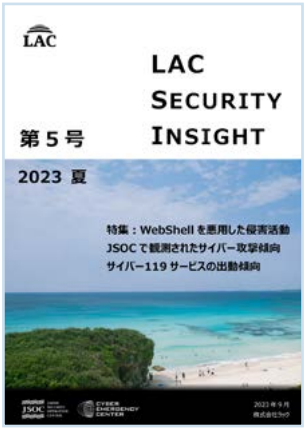
これまで当社は、日本マイクロソフトとEDRソリューションの販売連携などで協業してきた実績をもつほか、2023年3月には、様々な製品のログを集約し、インシデント情報などを一元的に管理できる機能をもつMicrosoft Sentinelの活用支援サービスの提供を開始するなど連携を強化しています。今後も日本マイクロソフトとの連携を通じて、日本国内の社内システム環境のセキュリティ向上に貢献していきます。

※ Microsoft Top Partner Engineer Award：
日本マイクロソフトのパートナー企業の中で活躍するエンジニアを表彰するもの。

ニュースリリース記事はこちら

ラックニュース

ランサムウェアに関する情報発信



LAC SECURITY INSIGHT

身代金交渉に関する提言書

ランサムウェア対策簡易チェック

サービス導入につなげるマーケティング活動を推進

ランサムウェア攻撃による被害が拡大するなか、企業がランサムウェア攻撃の被害にあった際に冷静な判断ができるよう様々な情報提供を行いました。

サイバー被害にあった組織の復旧を支援した当社の経験を踏まえ、ランサムウェアの攻撃傾向などを整理した「LAC Security Insight」や、被害を受けた際の攻撃者との交渉や支払いに向けて知るべきことを整理した「身代金交渉に関する提言書」などの冊子を発行しました。提言書については、当社が取材を受けてメディアにも取り上げられるなど、高い関心を集めました。

また、組織のランサムウェアに対する防御策の充足度を自己診断できる無料のWebサービス「ランサムウェア対策簡易チェック」の提供を開始しました。ランサムウェアによる被害を受けるリスクを低減して、安心してビジネスに取り組める環境の実現を目指しています。

各種情報

IRサイト

2023年９月1日に、IRトップページをリニューアルしました。最新のトピックスやコンテンツが検索しやすくなるようビジュアルを一新するとともに、アクセスランキングなどを新たに設置。加えて、情報を整理し使い勝手がよくなるように配慮しました。

ラックIRサイト　https://www.lac.co.jp/ir/

統合報告書

https://www.lac.co.jp/ir/pdf/integrated_report_2023.pdf

決算説明資料

https://www.lac.co.jp/ir/pdf/20231109_presentation.pdf

LAC WATCH

https://www.lac.co.jp/lacwatch/

株主様向け報告書 アンケート

報告書へのご意見等お聞かせください。

実施期間
2024年3月31日まで

https://krs.bz/lac/m/enq_chukan17

株式会社ラック　証券コード：3857
〒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
お問い合わせ　経営企画部 IR室
03-6757-0107　ir@lac.co.jp