LAC

2019春

セキュリティ診断レポート

特集

「IoTセキュリティ」の実態と対策

スマートフォンアプリケーション診断

ペネトレーションテスト活用例

セキュリティ診断レポート

2019 春

目次

2020年に向け全員参加で取り組むIoTのサイバーセキュリティ対策

木村 雅弘
セキュリティ診断部　部長
2008年よりWebアプリケーションセキュリティの研究、ソースコード診断、インシデントレスポンス支援業務に従事。2011年にラックのJSOC監視システム開発を経て、2018年4月からセキュリティ診断部の責任者を務める。

さまざまなものがインターネットにつながるIoTの普及が進んでいます。接続される機器は、従来からあるPCやスマートフォンにとどまらず、家電や自動車にも拡大しています。今後は、医療分野や、工場、インフラといった産業用途でIoT機器が増えると予測されており(※a)、IoTの利活用はあらゆる分野・産業に広がることが見込まれます。

IoT機器を狙ったサイバー攻撃の常態化

2018年にラックのJSOC(Japan Security Operation Center)(※b)で観測した攻撃を集計したところ、IoT機器を狙った攻撃の割合が全体の2割弱を占めました(図1)。月別の攻撃件数をみると、IoT機器を狙った攻撃は一年を通して観測されており、攻撃が一過性のものではなく常態化していることがわかります(図2)。

2016年、監視カメラやビデオレコーダーなどのIoT機器を標的としたマルウェア「Mirai」が確認されました。感染したIoT機器は攻撃用ボットネットの一部となり、他のWebサイトへのDDoS攻撃や、感染拡大を行うための踏み台になっています。感染したIoT機器による攻撃の中でも、2016年10月に行われたアメリカのDNSサービス事業者に対するDDoS攻撃では、Twitterなどのサービスが数時間にわたって接続しにくくなるといった被害が発生しました(※c※d)。

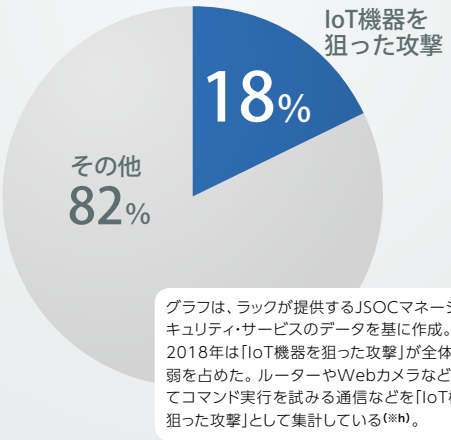
IoT機器は便利な反面、「管理が行き届きにくい」「利用者等においてインターネットにつながっている意識が低い」(※e)といった課題があります。

意識改革が求められるIoTのセキュリティ対策

2020年の東京オリンピック・パラリンピック開催を迎えるにあたり、総務省および国立研究開発法人情報通信研究機構(NICT)は、IoT機器の調査と利用者への注意喚起を目的とした取り組み「NOTICE」を始めました。インターネット上のIoT機器に対して、サイバー攻撃に悪用される恐れがあるかを調査し、インターネットプロバイダー経由で利用者の特定や注意喚起を実施します(※f)。加えて、総務省がIoT機器に不正アクセスを防ぐ機能を設けることを義務化する動きもあります(※g)。これらの国主導の取り組みにより、IoTを悪用したサイバー攻撃による被害が減ることが期待されます。IoTをビジネスの発展に活用しようとする企業側も、IoTを使ったインフラやシステムを設計、実装、運用する観点から個々にリスクを洗い出し、対策を検討していく必要があります。

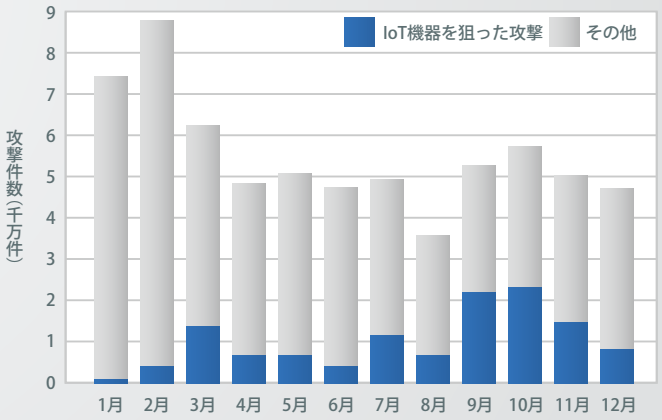
本レポートでは、IoTセキュリティ診断の結果から特に注意すべき問題を解説するとともに、IoT機器を利活用する際に参考になるガイドラインを紹介しています。他に、スマートフォンアプリケーション診断の2018年の問題点検出状況や、ペネトレーションテストの活用例も紹介しています。ラックはこれからも、本レポートをご覧の皆様とともに、より安全なITシステムを実現することに注力していきます。

図1：2018年に観測した
IoT機器を狙った攻撃割合(JSOC)



グラフは、ラックが提供するJSOCマネージド・セキュリティ・サービスのデータを基に作成。
2018年は「IoT機器を狙った攻撃」が全体の2割弱を占めた。ルーターやWebカメラなどに対してコマンド実行を試みる通信などを「IoT機器を狙った攻撃」として集計している(※h)。

図2：2018年に観測した
IoT機器を狙った攻撃件数(JSOC)



※a　**総務省「平成30年版情報通信白書」：**http://www.soumu.go.jp/menu_seisaku/hakusyo/index.html#johotsusintokei
※b　**JSOC(Japan Security Operation Center)：**ラックが運営するセキュリティ監視センターのこと。「ジェイソック」と呼ぶ。
※c　**Dyn Analysis Summary Of Friday October 21 Attack：**https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
※d　**日本経済新聞 2016年10月22日：**米で大規模サイバー攻撃　ツイッターやアマゾン被害　https://www.nikkei.com/article/DGXLASGM22H1P_S6A021C1MM0000/
※e　**総務省「平成30年版情報通信白書」：**第2部基本データと政策動向　第6章ICT政策の動向　第5節サイバーセキュリティ対策の推進（3）IoTに関する取組
http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/html/nd265230.html
※f　**総務省 IoT機器調査及び利用者への注意喚起の取組「NOTICE」の実施：**http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00011.html
※g　**日本経済新聞 2019年1月31日：**IoT機器、防御を義務化　サイバー攻撃入り口封じ　https://www.nikkei.com/article/DGXMZO40724420310120 19MM8000/
※h　「JSOC INSIGHT vol.22」「4.3 IoT機器を狙った攻撃通信の急増」では、2018年7月から9月におけるIoT機器を狙った攻撃について詳しく解説している。
https://www.lac.co.jp/lacwatch/report/20190206_001764.html

不正侵入につながる「IoT機器」の問題

小松 奈央
セキュリティ診断部
スマートデバイス診断グループ
さまざまな業種の顧客に対するIoTセキュリティとスマホアプリの診断サービスを担当。セキュリティカンファレンスや勉強会に積極的に参加し、情報収集をしている。診断ツール開発にも取り組んでいる。

篠原 崇宏
セキュリティ診断部
スマートデバイス診断グループ
技術派遣先のIPAにて脆弱性分析やセキュリティ対策の啓発活動に従事後、ラックへ帰任。IoTセキュリティとスマホアプリの診断サービスを担当。セキュリティイベントにおける講演や新サービスの企画開発なども行う。

ラックは2018年5月末に、多種多様なIoT機器に対して、ソフトウェア、ハードウェア、ネットワークに至るまでの総合的な脆弱性診断を行う「IoTセキュリティ診断サービス」の提供を開始しました。本稿では、IoTセキュリティで留意すべき問題を3つ取り上げて、IoTセキュリティの実態と製品開発者向けの対策をご紹介します。

留意すべき問題

監視カメラやネットワーク家電などのIoT機器が抱えるセキュリティリスクは、機器内の重要情報・知的財産の漏えい、機能停止や誤作動など、深刻な問題につながる恐れがあり、製品の企画設計段階から対策の検討が求められます。

問題1 デバッグ用の設定が有効になっている

IoTセキュリティ診断で検出される問題のうち、特にリスクが高く注意が必要なのは、IoT機器上で「デバッグ用の設定が有効になっている」です。

例えば、IoT機器の開発時に利用するSSH、Telnetといったデバッグ用のサービスが有効になっているケースです。この状態でIoT機器がリリースされると、攻撃者によってデバッグ用のサービスにリモートからアクセスされ、そこからIoT機器を遠隔操作される恐れがあります。

[対策]

リリース前には必ずデバッグ用のサービスが無効になっていることを確認してください。またプラットフォームによっては、初期設定でデバッグ用のサービスが有効になっている場合があります。開発時に使用しているプラットフォームが、初期設定でデバッグ用のサービスを有効にする設定になっていないかも併せて確認してください。

問題2 初期パスワードが変更不可

次に注意が必要な問題は「初期パスワードが変更不可」です。IoT機器は、他の機器やアプリケーションとの通信、機器の管理画面、メンテナンス用のサービスに、パスワードによる認証を利用することがあります。これらのパスワードが変更できない場合、初期パスワードのままIoT機器を利用することとなり、初期パスワードを何らかの方法で入手した攻撃者によって不正ログインされてしまう恐れがあります。また、初期パスワードを変更できても利用者が変更しない場合は、同様の問題が発生します。

[対策]

パスワードの変更機能を実装してください。その上で、利用者に対して、初期設定時に適切なパスワードに変更するよう促し、初期パスワードでは運用できないようにすることが有効です。

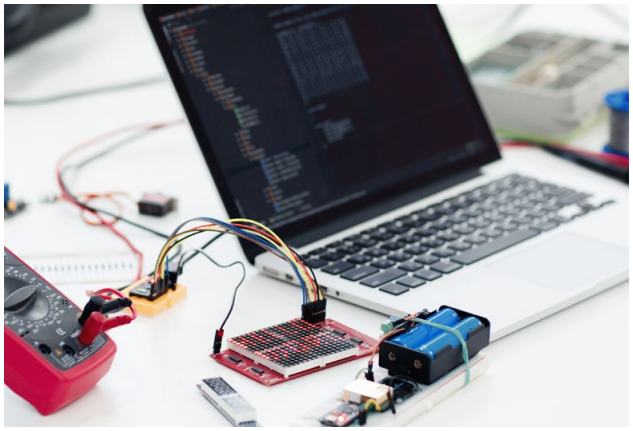
問題3 基盤上のシリアルポートから侵入可能

最後に、IoT機器特有の問題の１つである、IoT機器が攻撃者によって悪用される「基盤上のシリアルポートから侵入可能」について説明します。これは、基盤上のUARTやJTAGといったシリアルポートにケーブルを接続すると(※i)、IoT機器のファームウェアにアクセスされroot権限などでIoT機器内に侵入できてしまうというものです。

[対策]

IoT機器のファームウェアにアクセスされることがリスクとなる場合は、IoT機器の出荷時にUARTやJTAGといったシリアルポートを無効化することを推奨します。

また、シリアルポートに簡単にアクセスできないように、ハードウェア自体に耐タンパー性(※j)を持たせるなどのセキュリティ対策が考えられます。



IoTセキュリティには、今回ご紹介した３つの問題以外にもOSコマンドインジェクションといったIoT機器上で稼働するWebアプリの脆弱性(※k)など、気を付けるべきことが多くあります。問題が開発後に発見されると修正コストがかさむため、企画設計段階からセキュリティ対策を検討する必要があります。その際に有効なのが、ガイドラインの活用です。次ページでは、代表的なIoTセキュリティガイドラインをご紹介します。

※i **シリアルポートにケーブルを接続すると：**「CYBER GRID JOURNAL Vol.6」7ページ「IoT機器の安全性はどうやって破られるのか」では、機器を分解してシリアルポートに接続していく様子を写真入りで解説している。
https://www.lac.co.jp/lacwatch/report/20180912_001687.html
※j **耐タンパー性：**ハードウェアやソフトウェアにおいて、内部構造や記録されたデータなどを外部から解析・改変することが難しいこと。
※k **IoT機器上で稼働するWebアプリの脆弱性の例：**LAC WATCH「BUFFALO社ネットワークカメラWNC01WHの脆弱性（JVN#48790793）」
https://www.lac.co.jp/lacwatch/alert/20170426_001281.html

おすすめ情報

「IoTセキュリティ」ガイドライン5選

●IoT セキュリティガイドライン ver1.0

発行元：IoT推進コンソーシアム、総務省、経済産業省 2016年7月5日
対象：IoT機器やシステム、サービスの供給者および利用者
URL：https://www.meti.go.jp/press/2016/07/20160705002/20160705002.html

IoT機器やIoTシステム、IoTサービスについて、その関係者がセキュリティ確保等の観点から求められる基本的な取り組みを、セキュリティ・バイ・デザインを基本原則としつつ明確化。IoT機器の開発からIoTサービス提供までの流れを5つの指針（「方針」「分析」「設計」「構築・接続」「運用・保守」）に分け、それぞれのセキュリティ対策指針を示しています。また、全体を通して、章・節・要点ごとの対象読者が明確になっています。

●IoT開発におけるセキュリティ設計の手引き

発行元：独立行政法人情報処理推進機構（IPA） 2016年5月12日（2018年4月2日 内容更新）
対象：開発者（IoT開発においてセキュリティ設計を担当する人）
URL：https://www.ipa.go.jp/security/iot/iotguide.html

IoTのセキュリティ設計において行う、脅威分析・対策検討・脆弱性への対応方法を解説しています。また、セキュリティを検討する上で参考となる、IoT関連のセキュリティガイドを紹介。デジタルテレビ、ヘルスケア機器、スマートハウス、コネクテッドカーを題材として、具体的な脅威分析と対策の実施例を示しています。付録にある暗号技術の利用に関するチェックリストが便利です。

●GSMA IoTセキュリティ・ガイドライン

発行元：GSM Association（GSMA） バージョン1.0 2016年2月8日（現 バージョン2.0 2017年9月29日）
対象：IoTサービス事業者、IoTデバイス製造業者、IoT開発事業者、ネットワーク通信事業者
URL：https://www.gsma.com/iot/gsma-iot-security-guidelines-and-assessment-japanese/

携帯通信事業者の業界団体から発行されているガイドラインです。IoTサービスの安全な設計、開発、展開に関する推奨事項を以下の観点に分けて解説しています。
●IoTサービスのエコシステム
●エンドポイントのエコシステム
●ネットワーク事業者向け
通信事業者がIoTサービスを提供するための技術や機器・端末の観点を独立して記載しているのが特徴です。

●CCDS 製品分野別 セキュリティガイドライン v2.0

発行元：重要生活機器連携セキュリティ協議会 2017年5月29日
対象：IoT機器やシステムの開発に関わる設計者、開発者、経営者
URL：https://www.ccds.or.jp/public_document/#guidelines2.0

製品分野横断的なセキュリティ指針である『つながる世界の開発指針』（IPA発行）を車載・IoTゲートウェイ・金融端末（ATM）・決済端末（POS）といった製品分野別にして、より具体的なセキュリティ対策を示しています。2018年11月にはスマートホーム分野のドラフト版も公開されるなど、ガイドラインの対象が広がっています。

●IoT Security Guidance

発行元：OWASP（Open Web Application Security Project）
対象：製造者、開発者、消費者
URL：https://www.owasp.org/index.php/IoT_Security_Guidance

製造者向け、開発者向け、消費者向けという3部構成になっています。対象者ごとに、IoTセキュリティにおいて考慮すべき事項が記載されており、各対象に次の知見向上が期待できます。
●製造者：安全な機器を構築するのに役立つ
●開発者：安全なアプリケーションを構築するのに役立つ
●消費者：安全な商品を購入するのに役立つ

スマホアプリの半数で実害につながる問題点を検出

ますますニーズが拡大するスマホアプリ。しかし、その約半数で対策が必要なリスクが検出されたことが、ラックの分析でわかりました。スマホアプリの開発に際しては、適切なセキュリティ対策を施す必要があります。

山本 精吾
セキュリティ診断部
スマートデバイス診断グループ
システム開発業務を経て、Webアプリケーション診断に従事。現在はスマホアプリおよびIoTセキュリティの診断を担当するグループのリーダーを務める。

対策が必要なスマホアプリが5割超。減ったものの、依然として対策の促進が課題

図3は、2017年（2016年4月から2017年9月まで）および2018年（2017年10月から2018年9月まで）において、ラックに依頼された「スマートフォンアプリケーション診断」の結果を集計したものです(※l)。グラフを見ると、Mediumリスク以上の問題点(※m)を検出したスマートフォンアプリケーション（以下、スマホアプリ）の割合は2018年で52%となっており、2017年の74%から減少していることがわかります。減少した主な要因は、「端末内部に重要情報が保存（Mediumリスク）」の検出率が63%からから27%へ減ったことであり、この問題に対するセキュリティ対策が進んだといえます。

ラックでは検出した問題点のリスクレベルをHigh、Medium、Lowの3段階で独自に評価しており、図3で集計したMediumリスク以上の問題点は「対策が必要なレベル」です。

●Highリスク

情報漏えいやスマホアプリの不正利用などの実害に結び付く恐れがあり、早急な対策が必要です。

●Mediumリスク

複数の条件が組み合わさると、情報漏えいやスマホアプリの不正利用などの実害に結び付く恐れがあります。攻撃が成立するには端末のroot化(※n)や、攻撃者が通信経路上で盗聴可能な状態にあることなどが必要とされるため、Highリスクの問題点より悪用される可能性は低くなっています。ただし、これらMediumリスクについても攻撃に転用され得ることから、対策が必要です。

検出率が高くリスクの高い問題点は2017年と変わらず

「スマートフォンアプリケーション診断」で検出されたリスクが高い問題点のうち、検出率上位6項目を図4にまとめました。2018年において、検出率が高かった問題点の上位３つは、「端末内部に重要情報が保存」、「SSL証明書の検証不備」(※o)、「通信改ざんのチェック不備」でした。この３つの問題点は2017年でも1位から3位を占めており、開発時には引き続き注意が必要です。

さらに2017年と詳しく比較してみると、前述したように「端末内部に重要情報が保存」の検出率が大きく減少（63%→27%）しており、「通信改ざんのチェック不備」も減少（21%→11%）しています。

「端末内部に重要情報が保存」が減少した理由として、ラックのお客様の中で、端末内部に保存する重要情報の暗号化対策およびスマホアプリのキャッシュ対策(※p)が進んだことが挙げられます。

「通信改ざんのチェック不備」が減少した理由は、お客様の中で、この問題点は個人情報流出や金銭的な被害に結び付く可能性が高く、対策が必要だとの認識が広まったためだと考えられます。

図3 Mediumリスク以上の問題点を検出したスマホアプリの割合

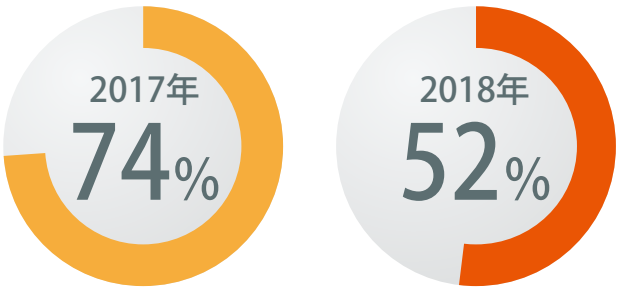
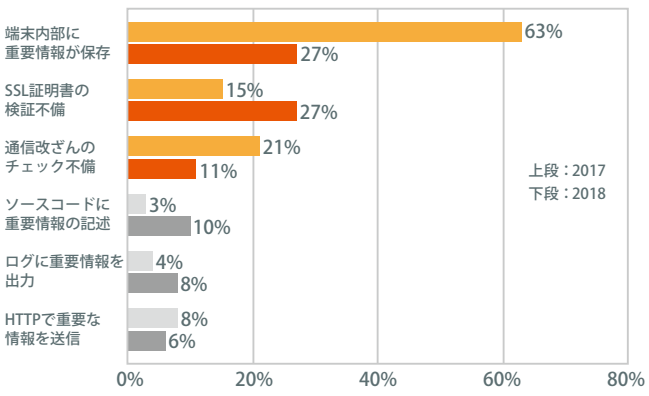


図4 Mediumリスク以上の問題点検出率上位6項目

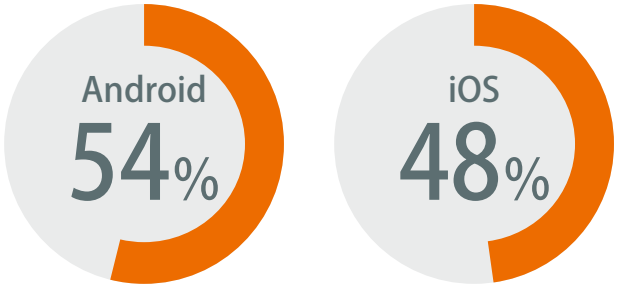


※l 「2017年（2016年4月から2017年9月まで）」は「セキュリティ診断レポート 2018早春」における集計対象期間である。https://www.lac.co.jp/lacwatch/report/20180309_001590.html
※m **問題点**：ラックでは、脆弱性とまではいえない軽微な問題も調査し、「問題点」として報告している。
※n **端末のroot化**：スマホ端末には通常、機能制限が施されており、いわゆる管理者権限を利用者は取得できないが、特殊な手法によってその管理者権限を取得する方法をroot化と呼ぶ。とりわけiOS（iPhone、iPad）で管理者権限を取得する手法は、Jailbreakと呼ばれることが多い。
※o **「SSL証明書の検証不備」**：「セキュリティ診断レポート 2018早春」では「中間者攻撃が可能」と表記していたが、ここでは「SSL証明書の検証不備」に変更している。
※p 開発者の意図に反して、スマホアプリとサーバ間の通信に含まれる重要情報がキャッシュされる問題を頻繁に検出していたため、2018年2月に「重要情報の漏えいにつながるスマホアプリのキャッシュ問題と対策」をラックのホームページで紹介した。 https://www.lac.co.jp/lacwatch/people/20180228_001581.html

Androidアプリだけでなく、iOSアプリへも診断が必要

図5は、診断においてMediumリスク以上の問題点が検出されたスマホアプリの割合を、OS別に集計した結果です。それぞれの割合を見ると、Androidで54%、iOSで48%となっており、OSによる差は小さいことがわかります。「iOSアプリは安全だから診断しなくてもいい」と思われることがありますが、AndroidアプリだけでなくiOSアプリもリリース前に診断することをお勧めします。

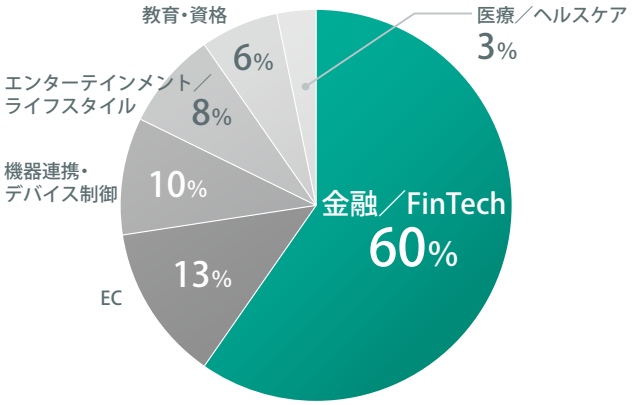
図5 スマホOS別Mediumリスク以上の問題点検出割合
（対象期間：2017年10月～2018年9月）



「金融／FinTech」系スマホアプリが診断対象の6割を占める

図6は、ラックが診断したスマホアプリをカテゴリごとに分類した結果です。グラフを見ると「金融／FinTech」系スマホアプリが60%を占めています。近年、現金を使わないキャッシュレス化の進展に伴い、業種を問わずに金融サービスへの新規参入が相次いでいます。その決済手段としてスマホ決済が欠かせないことから、「金融／FinTech」系スマホアプリは今後も高い割合を占めると予測されます。

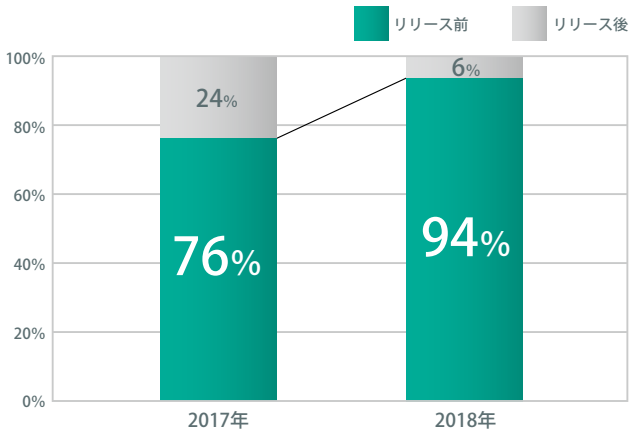
図6 診断対象スマホアプリの種別
（対象期間：2017年10月～2018年9月）



リリース前の診断実施が9割へ増加

図7は、診断実施のタイミングについてラックのお客様にアンケートした結果を示しています。2018年における「リリース前」の診断実施は94%で、2017年の76%から増加していることがわかります。背景として、Webアプリケーションと同様に、スマホアプリに対するリリース前診断をルール化している組織の増加が挙げられます。

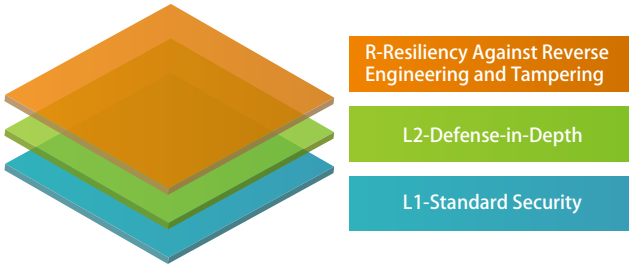
図7 診断のタイミング



結局、スマホアプリのセキュリティ対策はどこまでやればいいのか

診断結果の報告会では、お客様から「スマホアプリのセキュリティ対策はどこまでやればいいのか？」という質問をよく受けますが、スマホアプリにどういった機能があり、どういった種類の情報を扱うかによって答えは異なります。そこで参考になるのがOpen Web Application Security Project（OWASP）[※q]が公開している『OWASP Mobile Application Security Verification Standard 1.0』（以下、MASVS）[※r]です。MASVSはスマホアプリの設計や開発、テストをするときに必要とされるセキュリティ検証要件の基準を定めたドキュメントです。ラックでは、この日本語版を社員有志により作成し、ホームページで公開しています[※s]。

図8 セキュリティ検証レベル



出典：OWASP Mobile Application Security Verification Standard 1.0
https://github.com/OWASP/owasp-masvs

MASVSでは、3つのセキュリティ検証レベルが定義されています（図8）。標準的なMASVS-L1は全てのスマホアプリが対象で、多重防御のMASVS-L2は機密情報を取り扱うスマホアプリを対象としています。また、MASVS-Rには、エンドユーザが悪意を持っている場合や、モバイルOSが脆弱であるといった場合における、特定のクライアントサイドの脅威を防ぐリバースエンジニアリング耐性要件が定義されています。

上記3つのセキュリティ検証レベルを組み合わせるとMASVS-L1、MASVS-L2、MASVS-L1+R、MASVS-L2+Rの4つの検証方式を利用することができます。それぞれの検証方式にどういった種類のスマホアプリが該当するか記載されていますので、スマホアプリの企画・設計や開発、テストに役立つ内容となっています。

※q **Open Web Application Security Project**：「OWASP - Open Web Application Security Project とは、Webをはじめとするソフトウェアのセキュリティ環境の現状、またセキュアなソフトウェア開発を促進する技術・プロセスに関する情報共有と普及啓発を目的としたプロフェッショナルの集まる、オープンソース・ソフトウェアコミュニティです。」（https://www.owasp.org/index.php/Japanより引用）
※r **OWASP Mobile Application Security Verification Standard 1.0**：https://github.com/OWASP/owasp-masvs
※s **モバイルアプリのセキュリティ検証標準であるOWASP MASVSの日本語訳を公開**：https://www.lac.co.jp/lacwatch/people/20180831_001686.html

「サイバーセキュリティ対策の実効性を評価」ペネトレーションテスト活用例

「ペネトレーションテスト」は、サイバーセキュリティ対策の実効性を評価する手法として注目されています。疑似攻撃によってわかるセキュリティのポイントや、テストの活用方法を代表的な事例から紹介します。

吉田 聡
セキュリティ診断部
ペンテスト技術グループ
ペネトレーションテストを担当するグループのマネージャに従事。日本セキュリティオペレーション事業者協議会（ISOG-J）のWG1に参画。

「セキュリティ対策はしているが、本当に大丈夫か？」～ペネトレーションテストという選択

ラックでは、お客様から「現状のセキュリティ対策はどこまで機能しているのだろうか」や「どこまでセキュリティ対策をすればよいのだろうか」という不安の声をいただくことがあります。このような声にこたえるべく、セキュリティ対策の実効性を評価するペネトレーションテストサービスを2017年12月にリリースしました。

今回は、ペネトレーションテストを現在検討中、またはこれから検討するお客様へ、ペネトレーションテストの活用例を３つご紹介します。

ペネトレーションテストとは

ラックのペネトレーションテストでは、実際の攻撃手法を用いてシステム全体に疑似攻撃を実施します。どこから侵入できるか、どこまで侵入できるか、機密情報を外部へ持ち出すことが可能かどうかを調査します。

具体的には、以下に示す４種類のテストを行い、セキュリティ対策の効果を検証します。

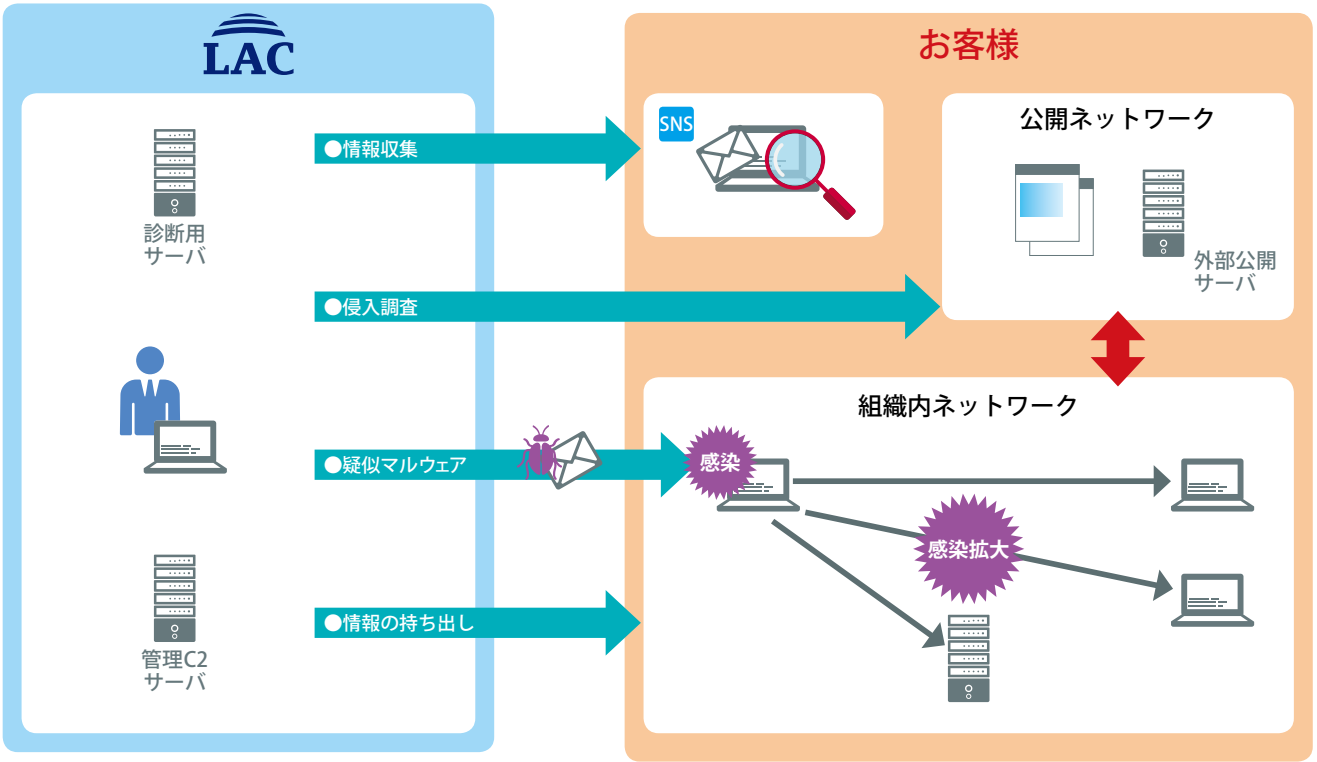
●情報収集
検索サイトなどを利用し、攻撃の糸口となるメールアドレスやIPアドレスを調査。

●侵入調査
プラットフォームやWebアプリケーションの脆弱性を突いて、実際に侵入できるかを調査。

●疑似マルウェア
標的型メールが届いた場合に、PCが攻撃者に遠隔操作されるかを調査。

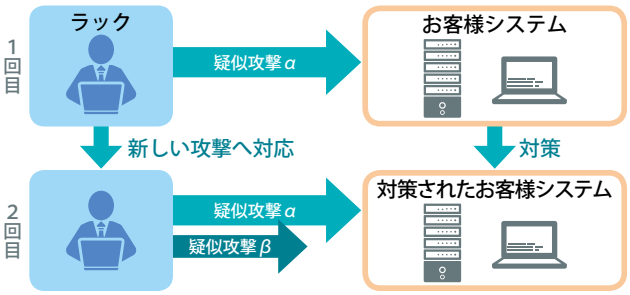
●情報の持ち出し
お客様の組織内ネットワークにあるPCがマルウェアに感染した場合に、攻撃者に情報を持ち出されたり、システムを停止されたりしないかを調査。

ペネトレーションテストサービス概要



活用例1　マルウェア感染時の影響を調査

PCのマルウェア感染がきっかけで感染時の影響を把握できていないことに気付いたお客様から、実害が出るような攻撃パターンを検証したいと相談があり、ペネトレーションテストを実施しました。このときに検出された問題に対策を施した上で、次年度には対策の妥当性を評価する2回目のテストを行っています。



前提条件とシナリオを変えずに2回実施

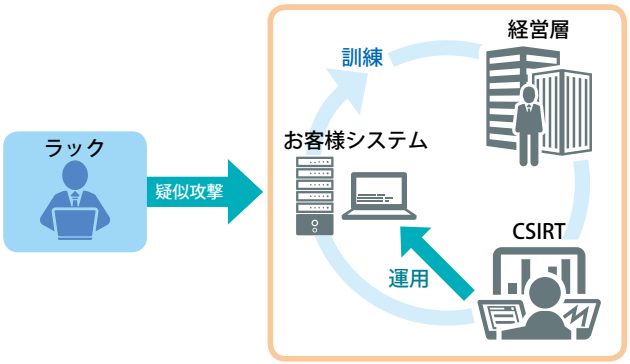
[実施結果]

１回目のテストにより、機密情報を持ち出し可能な問題が検出されたため、お客様はリスクが高いと判断し、対策を行いました。次年度、対策の妥当性を確認するため、同じシナリオで２回目のテストを実施しました。１回目で指摘された問題は修正されているものの、その修正によって新たな問題が発生していることがわかり、さらなる対策を講じました。

２回目のテストでは、１回目の後に実施した対策の妥当性確認に加え、１回目の後に出てきた新しい攻撃への耐性も確認できます。PCを遠隔から操作する手法や権限昇格の手法などは日々高度化しているため、定期的なテストの実施をお勧めします。

活用例2　CSIRT(※t) の運用を評価

インシデント対応に関する机上演習を毎年実施しているお客様から、「演習がマンネリ化している」との相談を受けました。そこで、演習にペネトレーションテストを組み合わせ、CSIRTの運用評価をより現実に近い形で実施してはどうかと提案しました。お客様は、予定していたセキュリティ演習の一環としてペネトレーションテストを実施し、CSIRTのマルウェア感染に対する検知・対応プロセスを評価することに決めました。



セキュリティ訓練と一緒に実施

[実施結果]

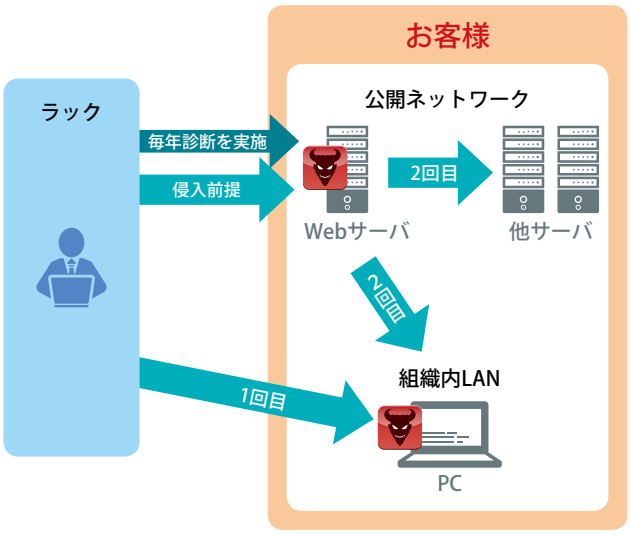
調査対象のシステムで見つかったいくつかの大きな問題を攻撃すると、機密情報を持ち出すことが可能な状態となっていました。

感染したPCからの攻撃について、お客様は重要なサーバへのアクセスは気付くことができていました。しかし、気付いた担当者からCSIRTのメンバーや経営層への報告がなく、コミュニケーションや報告手順に問題があることがわかりました。また、機密情報が持ち出されたこと自体に気付けなかった点も問題です。

このような結果を踏まえて、お客様は機器の設定や運用フローを見直しました。ペネトレーションテストをうまくお客様の施策に組み込んだ実例といえます。

活用例3　侵入口を変えて実施

あるお客様は、セキュリティ対策の対象範囲を広げ、対策レベルの底上げを進めていました。その一環として実施したのが、侵入口が違うシナリオを用いた計２回のペネトレーションテストです。１回目はPCのマルウェア感染を、２回目はWebサーバへの侵入をそれぞれ前提として、機密情報の持ち出しが可能かを調査しました。



侵入口を変えて実施

[実施結果]

１回目のテストでは、PCから機密情報が持ち出し可能な問題が検出されました。

２回目のテストでは、公開ネットワーク内の他サーバーから情報を持ち出せることと、想定していないネットワークへアクセスが可能なことがわかりました。公開サーバには定期的にセキュリティ診断を実施しているものの、「感染したら」という前提でペネトレーションテストを実施したことにより、新たなリスクに気付くことができました。

侵入口を変えることで、検出される結果もそれぞれ異なったものとなり、想定していなかったリスクを把握できた好例となりました。

最後に

セキュリティ対策は、実装して終わりとせず、その対策の実効性を評価することが大切です。今回ご紹介した活用例を参考に、ペネトレーションテストの実施の検討をお勧めします。

実施の際は、お客様ごとの事情を踏まえて内容を調整する必要があります。計画の段階から技術者による攻撃観点を加えることで、より実践的な評価や対策をご提案できるのが、ラックのペネトレーションテストの特長です。ご検討の際は、お気軽にご相談ください。

※t　**CSIRT**：Computer Security Incident Response Teamの略で、コンピュータセキュリティに関する事故対応チームのこと。

FAQ

ペネトレーションテスト 10の疑問

Q1.セキュリティ診断とペネトレーションテストの違いは?

A. セキュリティ診断は、対象システムの問題点を網羅的に洗い出すことを目的とします。一方、ペネトレーションテストは、対象システムへの侵入可否や、セキュリティ対策の実効性の確認などを目的とします。

Q2.ペネトレーションテストを実施するとどんな効果が得られるの?

A. 導入したセキュリティ対策が「期待した通り攻撃を防げているか」を確認できます。また、セキュリティ演習と一緒に実施することで、CSIRTの運用フローやその効力も確認できます。

Q3.ペネトレーションテストにおけるゴールって何?

A. お客様によって異なりますが、入口、内部、出口対策を全て実施している上での「機密情報の持ち出し可否」や、一部のネットワークに潜入されたことを前提とした「目標のネットワークまでの侵入」などがゴールの一例です。

Q4.ペネトレーションテスト実施のガイドラインとなるオススメの資料はある?

A. 金融庁が公表している、『諸外国の「脅威ベースのペネトレーションテスト(TLPT)」に関する報告書』(https://www.fsa.go.jp/common/about/research/20180516.html)が参考になります。この報告書では、諸外国におけるペネトレーションテストのフレームワークの紹介や、費用や期間、活用状況などが記載されており、一読に値します。

Q5.ペネトレーションテストの調査範囲はどうやって決めればいいの?

A. ペネトレーションテストでは、想定していなかったリスクの検出や対策の実効性評価などが本来の目的となるため、最初に定めたゴールに関係する本番環境全てをテスト担当者に制約を設けず調査させることを推奨します。ただし、どうしても外部に公開できない機密情報を含むPCやネットワークが存在する場合は、事前に調査対象外の範囲を設定します。

Q6.ペネトレーションテストを実施する上で通常業務への影響はないの?

A. シナリオにもよりますが、通常、データの破壊行為やサービス停止攻撃は実施しません。事前に関係する部署に対し、「いつ」「どのような目的で」「どのような内容の」調査を実施すると周知することで、通常業務への影響を最小限に抑えつつ、ペネトレーションテストを実施できます。

Q7.ペネトレーションテストの調査内容に合わせて費用を見積もることはできる?

A. 可能です。ラックではペネトレーションテストを「情報収集」「侵入調査」「内部感染」など、各場面に分けて実施しています。優先すべき場面を選定し、調査期間を調整することによって費用をお見積りできます。

Q8.ペネトレーションテストのサービス全体でどれくらいの期間がかかるの?

A. ラックでは調査前の事前準備から報告書の提出まで、約1〜3カ月で実施しています。期間に大きな差があるのは、調査範囲の設定、事前準備、調査期間の違いによるものです。調査そのものの期間は、約5〜20営業日です。

Q9.ペネトレーションテスト実施当日までに何を準備しておけばいいの?

A. ペネトレーションテストのゴールによって準備していただくことが変わります。準備すべき内容については、ペネトレーションテスト実施前の準備の段階で、お客様のご要望を伺いながらラックからもご提案させていただきます。提案の一例としては、Q6の回答でご案内したように、「事前に調査を実施することを関係する部署に知らせておく必要がある」などです。

Q10.いろいろなセキュリティ対策製品を既に導入しているけど、ペネトレーションテストまで実施する必要はある?

A. ペネトレーションテストでは、システムの運用や設定などの不備を突いた攻撃も実施します。そのため、脆弱性診断では検出できない問題点や、セキュリティ対策製品の有効性を確認できます。ペネトレーションテストを通して、情報資産への新たなリスクを事前に確認しておくことによって、実際の攻撃を受ける前の対策が可能となります。

ラックの「セキュリティ診断」ラインナップ

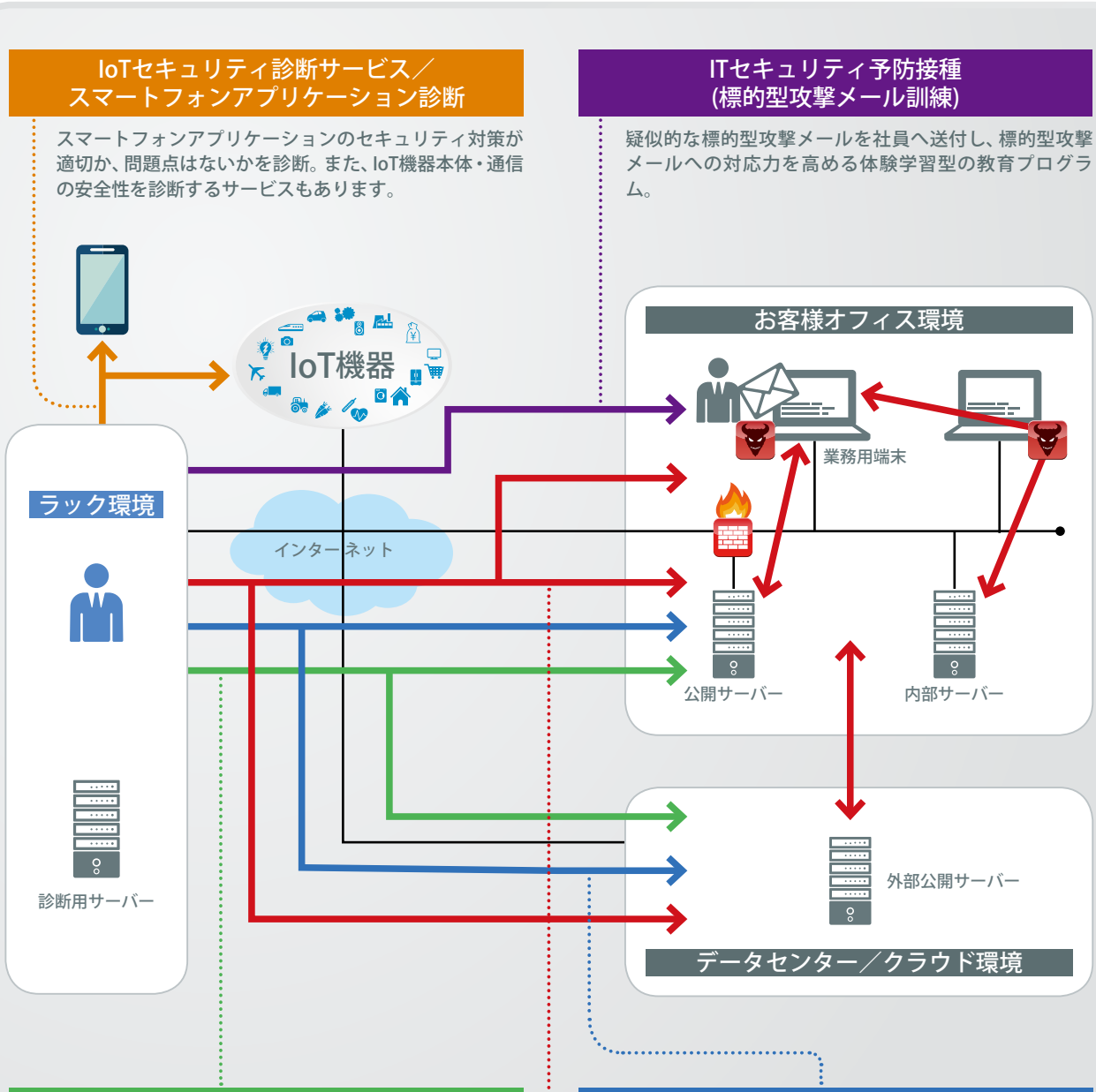
セキュリティ診断とは、お客様のITシステムに対して攻撃者の視点から考察した疑似攻撃を試行することで
リスクや脆弱性を見出し、対策を進めるためのサービスです。
ITシステムは多様な機器や製品、サービスを複雑に組み合わせて構築されています。
そのため、ラックではそれぞれの分野に細分化して、セキュリティ診断サービスを提供しています。

IoTセキュリティ診断サービス／スマートフォンアプリケーション診断

スマートフォンアプリケーションのセキュリティ対策が適切か、問題点はないかを診断。また、IoT機器本体・通信の安全性を診断するサービスもあります。

ITセキュリティ予防接種(標的型攻撃メール訓練)

疑似的な標的型攻撃メールを社員へ送付し、標的型攻撃メールへの対応力を高める体験学習型の教育プログラム。



プラットフォーム診断

サーバーやネットワーク機器に対して、不正アクセスの観点から侵入手法を考察・試行し、安全性を徹底的に調査します。ツールのみの低価格版も用意しています。

Webアプリケーション診断

攻撃者の視点からさまざまな疑似攻撃を考察・試行することで、ショッピングサイトや会員制サイトなど、Webアプリケーションの安全性を徹底的に調査します。

ペネトレーションテストサービス（侵入テスト）

お客様が運用しているITシステムに対して疑似攻撃を行います。成功した場合は、どこまで侵入でき、どのような情報を持ち出せるかを調査して、被害拡散リスクの評価を行います。

セキュリティ診断内製化支援サービス

お客様のセキュリティ診断の内製化を要所要所でバックアップし、運用の定着を手厚くサポートします。Webアプリケーション診断やプラットフォーム診断の両方に対応しています。

株式会社ラック セキュリティ診断部

〒102-0093 東京都千代田区平河町 2-16-1 平河町森タワー

E-MAIL：sales@lac.co.jp　https://www.lac.co.jp