LAC

セキュリティ診断レポート

2018 陽春

特集

Webアプリケーション診断とプラットフォーム診断
検出された脆弱性から見えた最近の傾向

目次

introduction

20年の歴史から見えてくる セキュリティ診断の状況とこれから

渡 部 友 一
システムアセスメント部　部長
2002年ラック入社。JSOCでのセキュリティ監視業務を経て2015年にセキュリティ診断事業に従事。現在は、セキュリティ診断サービスを提供する部門の長を務める。

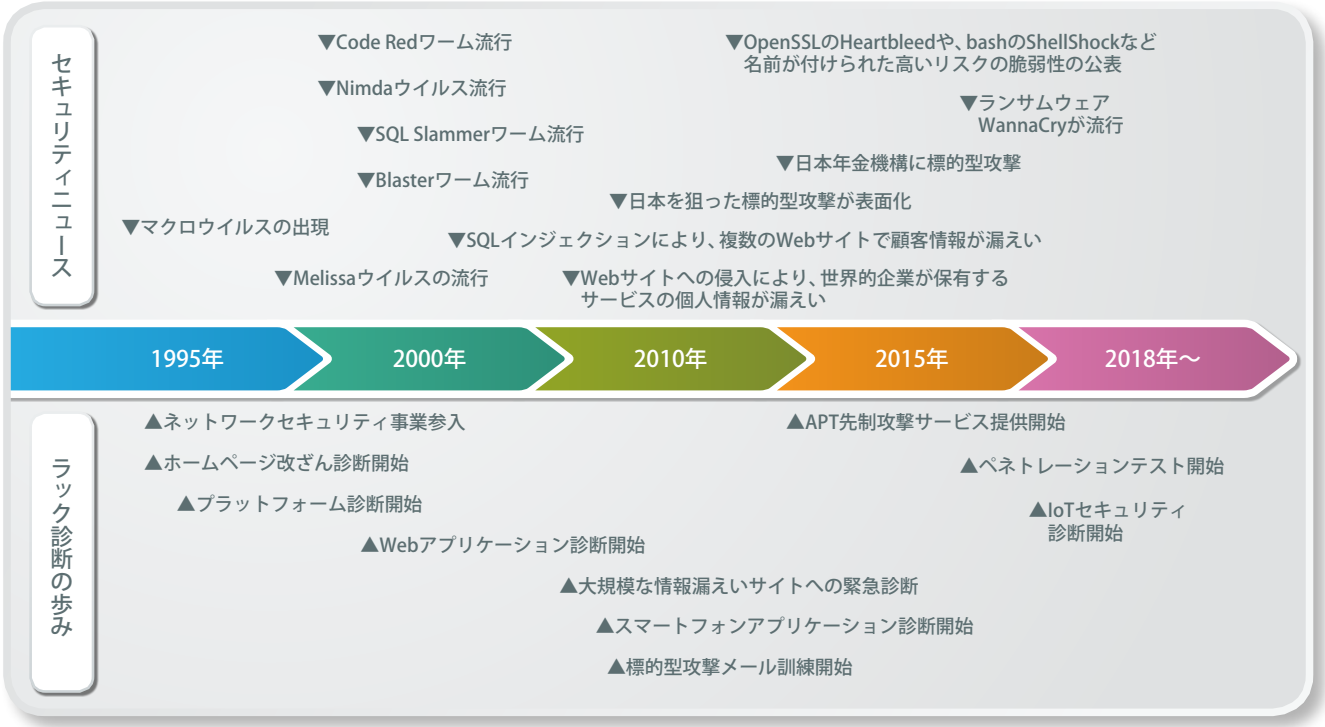
20年。これは、ラックが国内において「セキュリティ診断事業」を立ち上げ、歩んできた期間です。攻撃者の視点からシステムの問題を洗い出すことで、お客様システムのセキュリティレベルの向上に取り組んできました。

ラックはインターネットが急速に商業利用され始めた1995年に、「ネットワークセキュリティ事業」を立ち上げました。このとき提供し始めたサービスが日本で初めての「セキュリティ診断（当初はホームページ改ざん診断）」です。当時はまだ認知度が低いものでしたが、今では多くの企業や組織で当たり前のように利用されています。セキュリティ診断の開始後は、セキュリティ脅威の変化に合わせ、各分野に特化した診断サービスを順次立ち上げてきました。コンピュータウイルスが猛威を振るった1996年には、OSやミドルウェアのセキュリティリスクを洗い出す「プラットフォーム診断」をサービス化しました。2002年にリリースした「Webアプリケーション診断」は、2005年に起きたSQLインジェクションによる複数サイトの情報漏えい事件がきっかけとなって認知度が高まり、需要が急増しました。2011年には、スマートフォンの普及と高機能化によって顕在化した新たな脅威に対応すべく「スマートフォンアプリケーション診断」を開始。同年中には、特定の組織を狙う標的型攻撃の増加を受けて「標的型攻撃メール訓練サービス」もスタートさせました。これにより、セキュリティ診断サービスで評価する範囲が、システムの問題に加えてITを利用する人へと広がりました。

ラックがセキュリティ診断を提供してきたこの20年は、お客様の意識が大きく変化した期間でもあります。前述した2005年の情報漏えい事件では、多くのお客様がセキュリティ対策の必要性に気づきました。近年では個別のシステムのセキュリティ対策だけではなく、自組織全体で総合的にセキュリティ対策を行うように意識が変わっています。ラックでは、お客様のこのような意識変化に加え、高度化する標的型攻撃の増加というサイバーセキュリティの脅威や攻撃手法の移り変わりを踏まえ、2015年にラック独自開発の疑似マルウェアを使用した「APT先制攻撃サービス」、2017年に「ペネトレーションテストサービス」の提供を開始しました。

そして、これまで積み重ねてきた実績をベースに、ラックならではの分析により見えてくる脅威の時流やセキュリティ上の課題を「セキュリティ診断レポート」という形にまとめ、システムのセキュリティを維持運用している皆様へ直接発信しています。通算2号となる本レポートでは、ラックのセキュリティ診断サービスの核となる「Webアプリケーション診断」と「プラットフォーム診断」にフォーカスします。診断技術者がこれまでの診断結果をもとに導き出したセキュリティ向上のための提言が、今後もセキュリティ診断を活用される皆様にとって少しでも参考になれば幸いです。

診断の歩み



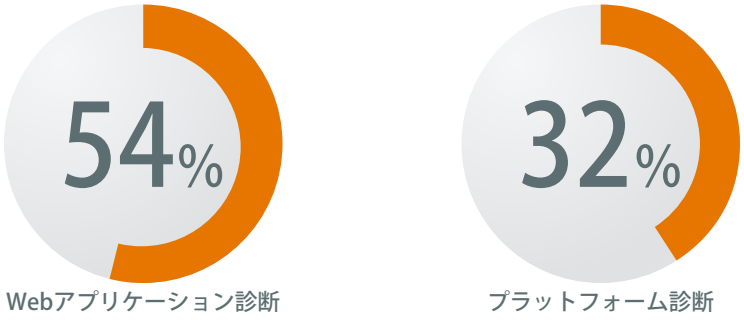
1 Webアプリケーション診断とプラットフォーム診断結果の傾向分析

花 岡 顕 助
システムアセスメント部
サービスマネジメントグループ GL
2002年ラック入社後、セキュリティ監視センターJSOCで監視サービス業務に従事。2013年よりWebアプリケーション診断グループにて診断業務を行う。海外のセキュリティカンファレンスに参加するなど、日々セキュリティ情報を収集している。

佐 宗 万 祐 子
システムアセスメント部
サービスマネジメントグループ GL
2008年ラック入社後、プラットフォーム診断を担当。現在は新規診断サービスを立ち上げるグループのリーダーに従事。その他、ラックの教育セミナー講師や、雑誌・書籍での執筆も行う。日本セキュリティオペレーション事業者協議会(ISOG-J)にも参画。

1−1 54%のWebアプリと、32%のホストにMediumリスク以上の脆弱性あり

図1-a 重要な問題点(High／Mediumリスク)を検出した診断対象



Webアプリケーション診断の対象Webサイトの半数、また、プラットフォーム診断の対象ホストの3割で、重要な問題点(High／Mediumリスク)を検出した。

ラックの診断サービスを利用するお客様の傾向を把握するため、Webアプリケーション診断とプラットフォーム診断の結果を分析したところ、興味深いデータが得られました。

図1-aは2017年に実施したWebアプリケーション診断とプラットフォーム診断において重要な問題点(High／Mediumリスク)が検出された診断対象の割合を示しています。集計データを見ると、半数のWebサイトに重要な問題点が内在していることがわかります。プラットフォーム診断についても同じように集計したところ、3割のホストで重要な問題点が検出されました。

ラックでは検出した問題点(※1a)のリスクレベルをHigh、Medium、Lowの3段階で評価しています。Highリスクに分類される問題点は、情報漏えいなどの実害に結び付くものであり、早急に対策が必要です。Mediumリスクは、複数の条件が組み合わさることで実害に結び付く可能性があり、早急ではないものの対策を必要とします。Lowリスクは直接的な被害につながる可能性は低く、対策は推奨レベルです。

1−2 セキュリティ診断を実施するお客様の状況

ここでは、全体を俯瞰するため診断件数の過去10年の変化を集計した後、業種、開発形態など個別の傾向を見るために直近の5年に焦点を絞って分析しました。

診断件数が10年で倍以上に

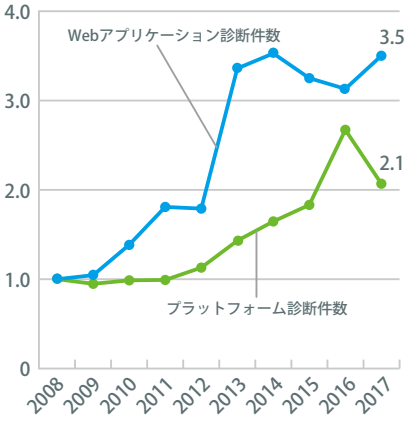
過去10年にラックが実施したWebアプリケーション診断とプラットフォーム診断の件数を集計しました図1-b。Webアプリケーション診断は対象となったWebサイト、プラットフォーム診断は依頼を受けた案件数を年ごとに合計しています。2017年は2008年に比べ、Webアプリケーション診断は3.5倍、プラットフォーム診断は2.1倍に増加しています。特にWebアプリケーション診断は2013年に急激な伸びを見せ、前年から倍増しました。これは新規のお客様が増えたことに加え、監査目的で診断の対象範囲を社内やグループ会社のWebサイト全体へと拡大する既存のお客様が同年以降、急増したことによります。一方、プラットフォーム診断では、2011年から診断件数が増加しています。背景として、この年に国内の大手企業や政府機関など標的型攻撃を受け、大変な話題になったことが挙げられます。このことをきっかけとして、多くの組織が自組織の対策状況を確認し始めたためだと考えています。

業種別診断件数の割合

2013年から2017年にかけてラックが実施したWebアプリケーション診断について、対象Webサイトの割合を業種別に見たのが図1-cです。この5年を見る限り、「情報・通信」「流通」「金融」「製造」の4分野合計で全体の約8割を占める傾向が続いています。

これに対し、プラットフォーム診断では対象ホストの割合の推移に一貫した傾向は見受けられませんでした。過去5年で比較的割合が大きかった業種は「情報・通信」と「官庁・公共」でした図1-d。

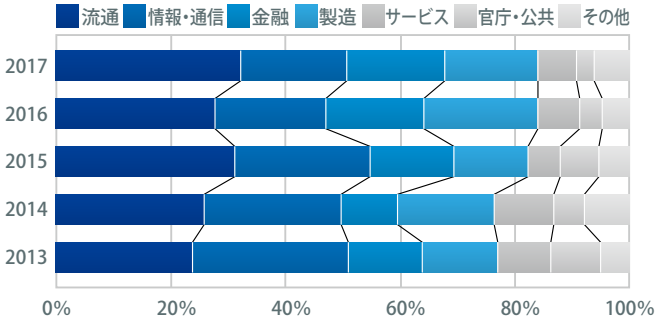
図1-b 診断件数の推移



ラックが実施した過去10年の診断件数の推移。2008年の診断件数を1とすると、2017年のWebアプリケーション診断は3.5倍、プラットフォーム診断は2.1倍になっている。

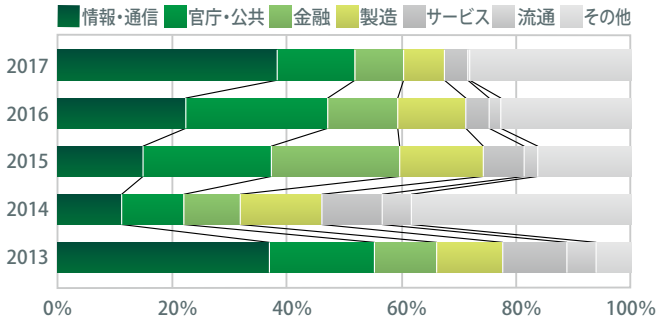
※1a **問題点**：ラックでは、脆弱性とまではいえない軽微な問題(補足事項)も調査し、「問題点」として報告している。

図1-c 業種別対象Webサイトの割合推移（Webアプリケーション診断）



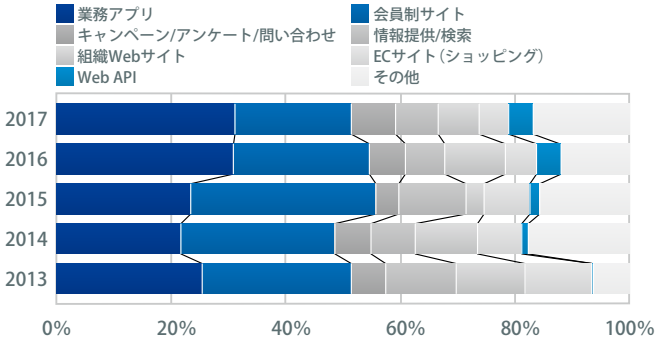
ラックが実施した診断の対象Webサイトの割合を、業種別にグラフにした。2017年は「流通」「情報・通信」「金融」「製造」の4分野で全体の約8割を占めている。

図1-d 業種別対象ホストの割合推移（プラットフォーム診断）



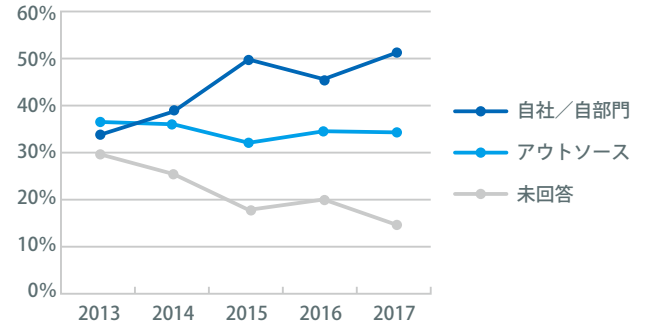
ラックが実施した診断の対象ホストの割合を、業種別にグラフにした。過去5年で一貫した傾向は見られないが、比較的「情報・通信」「官庁・公共」の割合が大きい。

図1-e 診断対象Webサイト種別の割合推移（Webアプリケーション診断）



診断対象のWebサイトを分類した。業務アプリと会員制サイトで全体の約半数を占めている。Web APIが近年徐々に増えている点も特徴的である。

図1-f 開発形態別 診断対象Webサイトの割合推移（Webアプリケーション診断）



ラックが診断を実施したWebアプリの開発形態を示しており、アウトソースが横ばいなのに対し、自社／自部門が増加傾向にあることがわかる。

近年Web APIの診断が増加傾向

過去5年のWebアプリケーション診断の対象をWebサイトの種類で分類しました図1-e。いずれの年も、上位2つは業務アプリと会員制サイトであり、合わせて全体の約半数を占めています。目立った変化として、2014年頃から従来のWebブラウザでアクセスするサイトの診断に加え、Web APIの診断が増え始め、2014年にはわずか1.1%だったものが2017年には4.4%に伸びていることが挙げられます。これは、Web APIの活用が、Webサイト同士のデータのやり取りから、スマートフォンアプリケーションから呼び出されるWeb APIまで広がったことによるものです。

自社開発がアウトソースを上回る

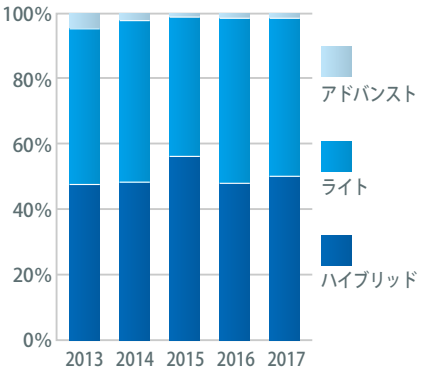
診断対象となったWebアプリケーション（以下、Webアプリという）の開発形態について、ラックのお客様にアンケートした結果が図1-fです。2014年を境に、自社開発とアウトソースの比率が逆転し、自社開発が増加傾向にあることがわかります。

バランス型の診断が主流

お客様が選択した診断サービスの割合を調べました。Webアプリケーション診断では、全ての箇所を手動で精密に診断を行う「アドバンスト診断」の割合は2%未満とごく少数であり、ツール診断と手動診断を組み合わせた「ハイブリッド診断」「ライト診断」でほぼ100%となっています図1-g。お客様は診断の精密さよりも、診断費用と精密さのバランスを求めていることがわかります。

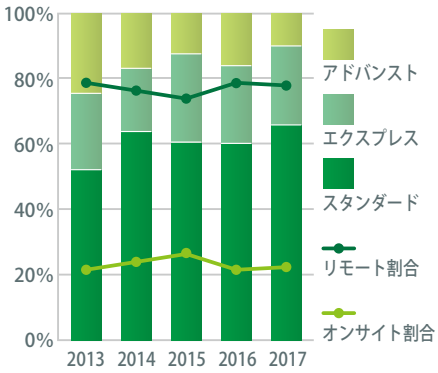
プラットフォーム診断では、市販の脆弱性スキャナとラックの独自開発ツールを使う「スタンダード診断」が過去5年を通して半数以上を占めています図1-h。スタンダード診断より疑似攻撃の種類を増やしたり、問題を組み合わせた場合の実害を専門家の目で調査したりする「アドバンスト診断」は1割程度、市販の脆弱性スキャナを使って素早く問題点の有無を確認する「エクスプレス診断」は2割程度となっています。

図1-g サービス別診断件数の割合（Webアプリケーション診断）



ラックが実施した診断のサービス別割合である。ライト診断とハイブリッド診断で、ほぼ100%を占めており、診断費用と精密さのバランスを重視するお客様が多いことがわかる。

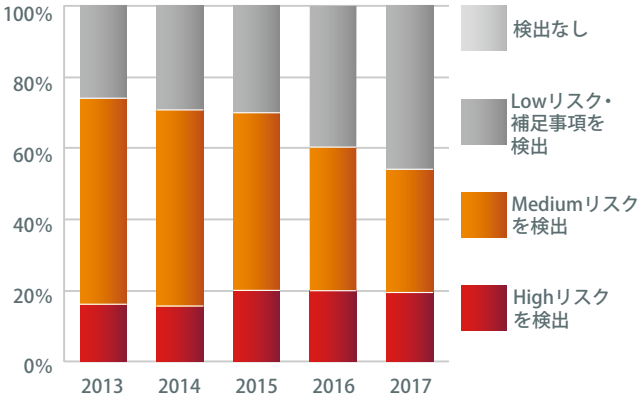
図1-h サービス別診断件数の割合（プラットフォーム診断）



ラックが実施した診断のサービス別割合である。過去5年を通じ、スタンダード診断の実施割合が一番多く、リモート診断とオンサイト診断の実施件数は4対1である。

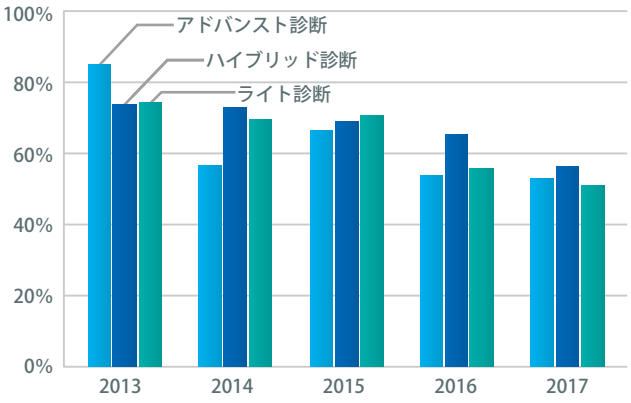
1−3 検出された問題点の分析結果（Webアプリケーション診断）

図1-i 最も高いリスクの問題点別 診断対象Webサイトの割合推移



2017年に重要な問題点（High／Mediumリスク）が検出されたWebサイトは約半数まで減少したものの、いまだHighリスクは2割前後で推移。

図1-j サービス別 重要な問題点を検出したWebサイトの割合推移



重要な問題点（High／Mediumリスク）の検出Webサイトを集計した。同一サイトを3つの診断方法で診断して比較したものではなく、各診断サービスで対象としたWebサイト全体を集計したものである。

2サイトに1サイトは対策が必要

Webサイトで検出された問題点のうち、最もリスクレベルが高いものをそのサイトのリスクとして集計し、割合の推移を図1-iにまとめました。重要な問題点（High／Mediumリスク）が検出されたWebサイトは、2013年が74.0%だったのに対し、2017年は54.1%まで減少しています。それでもなお、2サイトに1サイトは対策が必要な状況です。2013年に比べ2017年が低い値となっているのは、セキュアプログラミングや安全なWebサイトのノウハウが体系化され、コーディング規約に反映されるといった品質改善への取り組みが、お客様の開発現場に浸透しつつあるためだと考えられます。

サンプリング診断でも問題点を検出

ラックではお客様から、「ライト診断は問題点が検出されにくいのではないか」という問い合わせを受けることがあります。これは、ハイブリット診断では診断対象の箇所が網羅的なのに対し、ライト診断は対象をサンプリングによって絞り込むからですが、結論としては、検出される問題点の種類にさほど差は生じません。

このことを裏付けるため重要な問題点が検出されたサイトの割合をサービス別に調べたところ、図1-jのようになりました。診断対象Webサイトが異なるため一概に比較することはできませんが、2017年ではいずれのサービスも50%台となっています。

サービス種別に関わらず、検出される問題点はログイン画面、検索画面、登録更新画面に集中する傾向にあります。「ライト診断」ではこのような画面を集中的にサンプリングして診断するため、「期間内で問題点を多く発見する」という観点においては、「ハイブリッド診断」「アドバンスト診断」と遜色のない数字になっています。

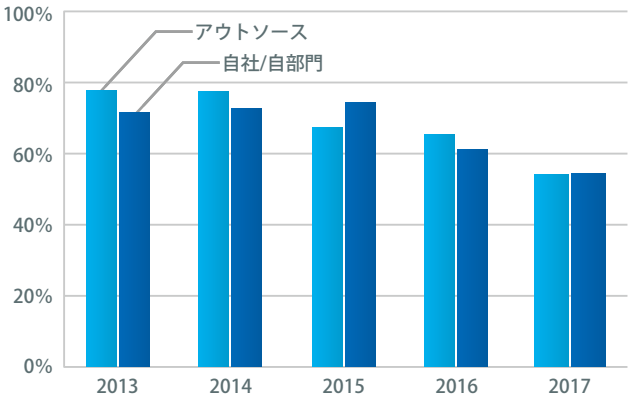
開発形態による検出割合に差はない

Webアプリの開発形態別に、重要な問題点の検出割合を集計しました図1-k。「アウトソース」と「自社開発」で特に大きな差は見られず、「アウトソース」は2014年以降、「自社開発」は2016年以降減少傾向にあり、2017年はともに約半数となっています。

業種別は概ね緩やかな改善傾向

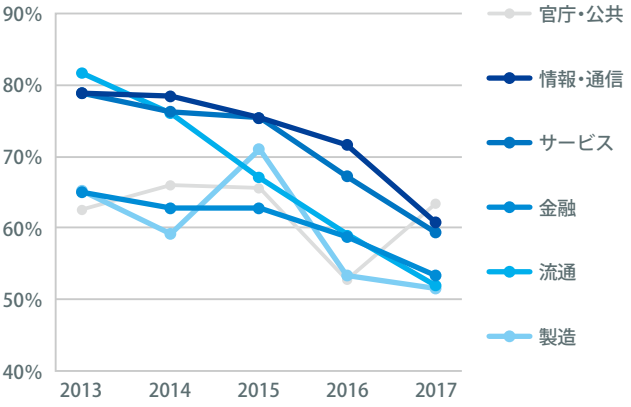
業種別に集計した重要な問題点の検出サイトの割合を図1-lに示します。2013年は、全ての業種において60〜80%程度だったのに対し、2017年は50〜60%程度になっています。「官庁・公共」はほぼ横ばいであるものの、他の業種では緩やかな改善傾向が見られます。これは、Webアプリケーション開発時におけるセキュリティを意識した設計・構築のノウハウが、業種を問わず浸透しているためだと考えられます。

図1-k 開発形態別 重要な問題点を検出したWebサイトの割合推移



開発形態別の重要な問題点（High／Medium）の検出割合は、アウトソース、自社／自部門ともに近年は減少傾向にあり、2017年は約半数である。

図1-l 業種別 重要な問題点を検出したWebサイトの割合推移



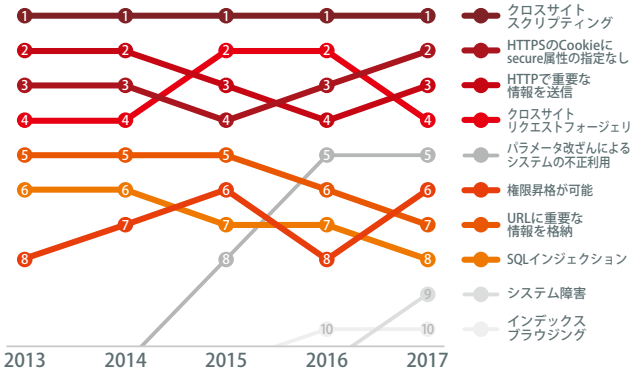
重要な問題点を検出したサイトの割合を見ると、「官庁・公共」以外の業種で緩やかな改善傾向が見られる。

表1-a 2017年に検出した問題点の割合 上位10件

順位	問題点名	リスクレベル	割合
1	クロスサイトスクリプティング	Medium	16.8%
2	HTTPSのCookieにsecure属性の指定なし	Medium	15.6
3	HTTPで重要な情報を送信	Medium	13.2
4	クロスサイトリクエストフォージェリ	Medium	12.5
5	パラメータ改ざんによるシステムの不正利用	High	9.6
6	権限昇格が可能	High	8.9
7	URLに重要な情報を格納	Medium	8.8
8	SQLインジェクション	Medium※	6.0
9	システム障害	High	1.9
10	インデックスブラウジング	Medium	1.8

※Highリスク(2割)を含む

図1-m 2017年 問題点別検出数 上位10件の過去5年の順位



クロスサイトスクリプティングを始め上位1〜4位、6〜8位では、過去5年で常に検出上位にランクインしていることがわかる(線がない箇所は圏外を示す)。

問題点のランキング上位に変化なし

2017年にWebサイトで検出された重要な問題点について、上位10件を一覧にしました表1-a。また、2017年時点での上位10件について、過去5年の順位変動を示したものが図1-mです。2017年に上位10件にランクインしている問題点のうち７件は、5年連続で上位10位以内にランクインしています。Webアプリでよく検出される問題点は、過去5年で大きな変化がないことが見てとれます。

次に、2017年の上位10件の問題点について、過去5年に検出されたサイトの割合を表したものが図1-nです。この図から上位４件が顕著な減少傾向にあることがわかります。2013年には「クロスサイトスクリプティング」の37.2%を筆頭に、他の問題点(「HTTPSのCookieにsecure属性の指定なし」「HTTPで重要な情報を送信」「クロスサイトリクエストフォージェリ」)でも25%前後のサイトで検出していたものが、2017年にはいずれも15%前後まで減少しています。これはそれぞれの問題点の検出割合が、2013年は約3〜4サイト中1サイトだったものが、2017年は6〜7サイト中1サイトにまで改善していることを意味します。スコア改善につながった要因としては、実装方法が体系化されていることや、対策事例が多く公開されていること、またWebアプリケーションフレームワークでも対策が進んでいることが考えられます。

減らない権限関連の問題

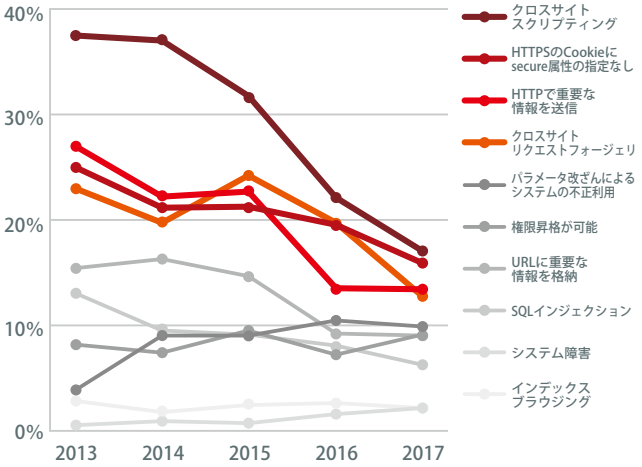
問題点の検出傾向を分析したところ、Webアプリの設計段階において、権限に関する問題に特に注意する必要があることがわかりました。

権限関連の問題点は、情報漏洩や不正利用など実害に発展しやすいため、ラックでは通常Highリスクで報告します。表1-aにある「パラメータ改ざんによるシステムの不正利用(５位)」「権限昇格が可能(６位)」の他、圏外順位にもいくつかあります。重要な問題点の検出サイトの割合が減少するなか、権限関連の問題点の検出サイト割合は、図1-oに示すとおり、2013年以降、わずかながらも年々増えていることがわかります。

権限関連の問題点は、クライアント側の操作をサーバ側のWebアプリでチェックしていないことに起因します。このようなチェックの仕組みは非機能要件であり、アプリケーションの設計段階で考慮漏れが生じていることが、問題点が減らない原因であると考えられます。

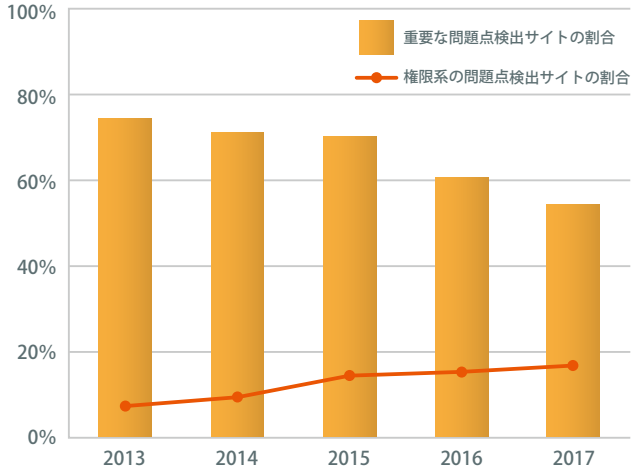
対策は、権限チェックの仕組みを開発の設計段階で組み込むことが必要です。その際、サーバ側Webアプリで権限チェックを行うこと、クライアント側に重要情報(データ識別子など)を渡さないことが重要です。

図1-n 2017年 問題点別検出数 上位10件の過去5年の割合



2017年に検出された問題点上位10件の過去5年の順位の推移を示した。「クロスサイトスクリプティング」をはじめとした上位4件は、2013年以降一貫して上位を占めているものの、減少傾向が顕著である。

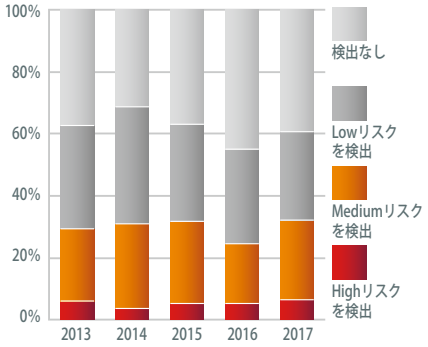
図1-o 権限系の問題点を検出したWebサイトの割合推移



権限系の問題点(圏外順位も含む)を検出したサイトの割合推移。全体的に重要な問題点の検出割合が低下する中、権限系の問題点は2013年以降、検出サイトの割合がわずかながらも年々増えていることがわかる。

1−4 検出された問題点の分析結果（プラットフォーム診断）

図1-p 最も高いリスクの問題点別 診断対象ホストの割合推移



重要な問題点（High／Mediumリスク）が検出されたホストの割合は3割前後で推移している。対策漏れや資産管理の不備により、脆弱なホストが存在するものと考えられる。

3ホストに1ホストは対策が必要

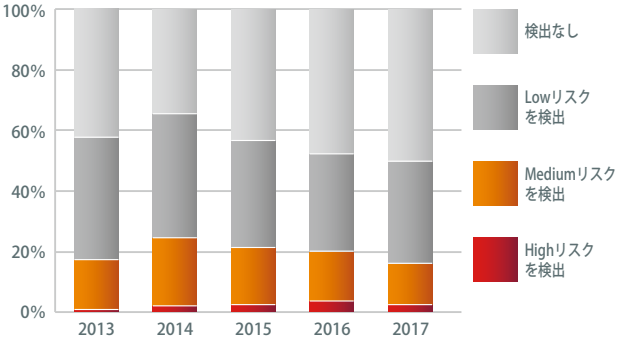
プラットフォーム診断で検出された問題点のうち、最もリスクレベルが高いものをそのホストのリスクとして集計し、割合の推移を図1-pにまとめました。2013年から2017年までの過去5年において、重要な問題点（High／Mediumリスク）が検出されたホストの割合は3割前後で推移しました。OSやソフトウェアに対するセキュリティ対策のポイントは、Webアプリに比べ一般的に認知されてきてはいるものの、対策漏れや資産管理の不備、パッチの適用頻度により、脆弱なホストが存在するものと考えられます。

全体の傾向に続けて、問題点の検出割合をリモート診断とオンサイト診断に分けて集計した結果をそれぞれ説明します。

リモート診断では、重要な問題点が検出された割合は過去5年のいずれの年も20%前後です図1-q。そのなかでもHighリスクが検出されたホストでは、ソフトウェアがアップデートされていない、パッチが適用されていないなどの理由で、パスワードハッシュの開示やコード実行といった問題点が検出される傾向にあります。Highリスクが検出されるホストは全体の数%しかありませんが、ネットワーク上に1台でも危険性の高いホストがあった場合、その1台を踏み台にして他のホストへ侵入される場合があります。ネットワーク変更などにより公開状態のままセキュリティ対策が施されない可能性もあるため、定期的な診断によりホストの洗い出しや対策をしましょう。

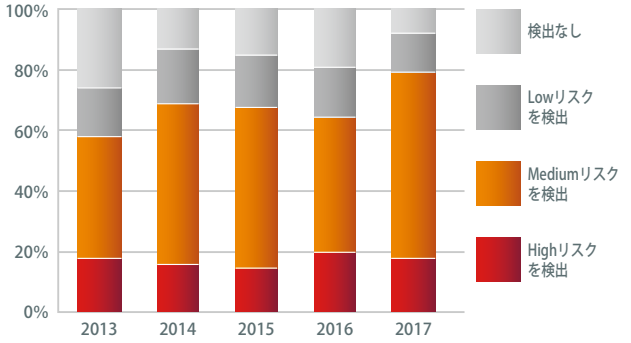
オンサイト診断では、リモート診断に比べ重要な問題点が検出されているホストが多く、各年60%〜80%を占めていました図1-r。オンサイト診断ではネットワーク機器などによるアクセス制限がない状態で診断するため、ホスト単体での診断結果が取得できます。重要な問題点が検出されているホストでは、ミドルウェアの管理用WebコンソールやSSHやTELNETなどの管理用サービスといったアクセス制御に関する問題点がMediumリスクで検出されることが多くなっています。Highリスクを検出したホストでは、リモート診断と同様の問題点に加え、管理用サービスのパスワード認証において単純なIDとパスワードの組み合わせでログイン可能などの、管理ミスに関する問題点が検出されます。これは、製品やソフトウェアの導入時に、管理用サービスが自動で起動していることにユーザが気づいておらず、対策がとれていないことが原因だと推察されます。

図1-q リモート　最も高いリスクの問題点別 診断対象ホストの割合推移



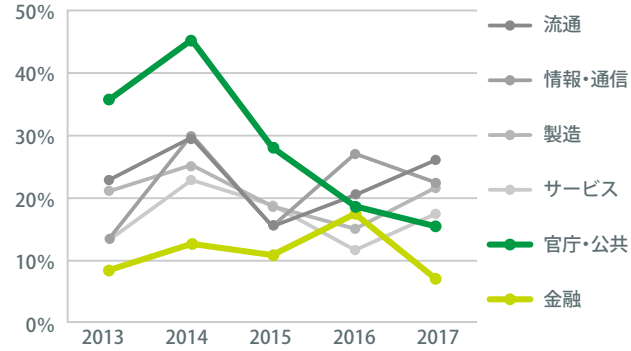
リモート診断では、重要な問題点が検出された割合はいずれの年も20%前後にとどまる。しかし、この中には数%ながらHighリスクの問題点が検出されるホストが含まれており、そのホストを侵入口として被害が拡大する可能性がある。

図1-r オンサイト　最も高いリスクの問題点別 診断対象ホストの割合推移



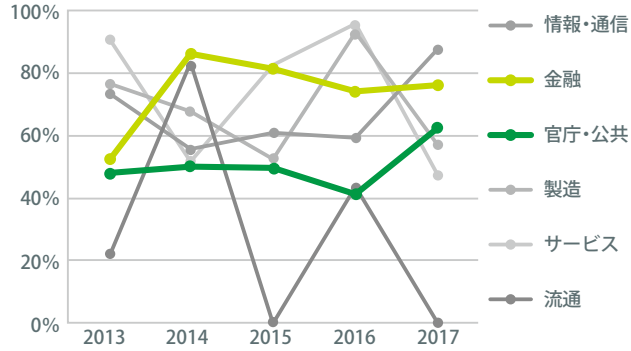
オンサイト診断では、重要な問題点が検出された割合は60%〜80%の間で推移。アクセス制限がない状態で診断するため、リモート診断より問題点が見つかりやすい。

図1-s リモート　業種別 重要な問題点を検出したホストの割合推移



検出割合が最も低いのは「金融」。「官庁・公共」は年々検出割合が下がっている。

図1-t オンサイト　業種別 重要な問題点を検出したホストの割合推移



リモート診断とは違い、「金融」の検出割合が高い傾向にある。「官庁・公共」はオンサイト診断では検出割合が低い。

業種別 重要な問題点の検出割合

重要な問題点の検出割合を業種別に集計しました。過去5年において、リモート診断では「金融」が他業種に比べ検出割合が低い状態にあることが見て取れます図1-s。また、「官庁・公共」については、重要な問題点の検出割合がこの5年で最も多かった2014年の4割強から、2017年は2割弱まで下がっており、セキュリティレベルが改善されてきていることがわかります。一方オンサイト診断では、「金融」における重要な問題点の検出割合が他業界より多い傾向にあります図1-t。「官庁・公共」についてはリモート診断、オンサイト診断ともに、他業種に比べて評価がよい傾向にありました。

問題点が検出されやすいポートは

2017年に実施した診断の結果から、問題点が検出されやすいポートを調べるため、各ポートの問題点検出割合を算出し、上位10件を表にまとめました表1-b。

リモート診断で最も問題点検出割合が高いポートは110/tcpで、68.6%です。7割にも上るのは、このポートでPOP3サービスが提供されていることが多く、パスワード認証が試行可能という問題点が報告されるためです。一方、オンサイト診断では623/udpが97.5%で1位となりました。これほど高い割合で検出されるのは、ポート623/udpはIPMI(※1b)を稼動していることがほとんどで、そのIPMIにリモートの攻撃者がユーザのパスワードハッシュを取得できる問題点があり、IPMIをデフォルト設定のまま稼動していると必ずこの問題点が報告されるためです。

SSHサービスが稼働している22/tcpは、どちらの診断方法においても上位(リモート6位、オンサイト2位)に入っているものの、検出割合はリモート診断では3割、オンサイト診断では9割と開きがあります。この差の大部分は、SSHサービスで利用されている認証方式の違いから生じています。リモート診断の場合、SSHサービスが稼働していても、接続元IPを制限したり、公開鍵認証を利用した高度な認証方式を採用したりすることが多いため、パスワードクラック(※1c)やその他の攻撃手法も利用できず、問題点が報告される可能性は低くなっています。しかしオンサイト診断では、パスワード認証が利用されることが多く、パスワードクラックが行われてしまう可能性から問題点が報告されます。

また、SSHサービスの問題点検出割合に差が出ている原因として、2015年に発見されたOpenSSHにおいて認証回数制限の回避が可能な脆弱性(CVE-2015-5600)の検出割合の差が考えられます。この問題点についての検出割合は、リモート診断が4.2%であるのに対し、オンサイト診断では12.1%でした。多くの組織でインターネット側への対応はすでに実施しているものの、内部ネットワークとなると対応工数などを鑑みて対策を保留しているケースがあることが考えられます。

「認可・権限・アクセス制御」の問題を多く検出

検出された重要な問題点の上位20件を対象に、共通脆弱性タイプ一覧CWE(※1d)を使って脆弱性の種別を調査しました。その結果、リモート診断図1-u、オンサイト診断図1-vともに検出割合が最も高かった種別は「認可・権限・アクセス制御」でした。これにはSSHやTELNETなどの管理サービスにアクセス可能な問題や、ソフトウェアの管理用Webコンソールにアクセス可能な問題点などが含まれます。リモート診断で2番目、オンサイト診断で3番目に検出割合が高かった種別は「情報漏えい」であり、HTTPサービスにおけるアカウント情報の取得や、SNMPサービスにおいてコミュニティ名が推測可能などの問題点が検出されています。

●設計段階から権限系の問題点を考慮することが重要

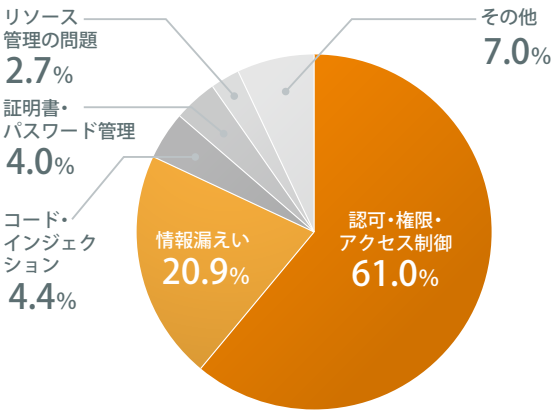
Webアプリケーション診断やプラットフォーム診断の結果を分析したところ、Webアプリでは権限系の問題が増加する傾向が、プラットフォームでは「認可・権限・アクセス制御」の問題が多く検出される傾向が見られました。これらの問題は、設計段階での考慮漏れから生じることが多いため、早い段階から取り扱いに注意することが重要です。

表1-b 問題点が検出されやすいポート上位10件

順位	リモート診断		オンサイト診断	
	ポート	問題点検出割合	ポート	問題点検出割合
1	110/tcp	68.6%	623/udp	97.5%
2	139/tcp	64.6	22/tcp	89.0
3	3389/tcp	42.1	139/tcp	79.0
4	445/tcp	36.7	445/tcp	76.7
5	21/tcp	27.8	3389/tcp	75.4
6	22/tcp	27.2	1433/tcp	66.0
7	587/tcp	24.3	21/tcp	62.9
8	143/tcp	17.8	23/tcp	60.3
9	8080/tcp	12.2	8080/tcp	26.5
10	993/tcp	12.2	8081/tcp	15.4

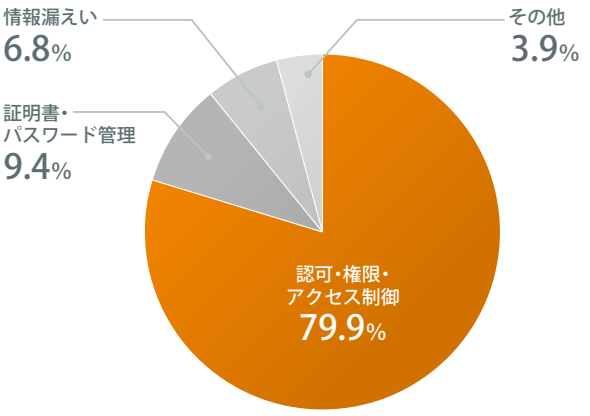
2017年に実施した診断の結果から、ポートが稼動しているホスト数を分母とし、そのポートで重要な問題点が検出されたホスト数を分子として、問題点検出割合を算出した。ただし、稼動しているホスト数が100未満のポートは除外した。

図1-u リモート診断で検出された問題点の種別



検出された重要な問題点上位20件についてCWEで分類した。リモート診断では「認可・権限・アクセス制限」の問題が6割、「情報漏えい」の問題が2割となっている。

図1-v オンサイト診断で検出された問題点の種別



検出された重要な問題点上位20件についてCWEで分類した。オンサイト診断では「認可・権限・アクセス制限」が8割を占めている。

※1b IPMI：Intelligent Platform Management Interfaceの略。サーバのインターフェース仕様であり、サーバの温度、電圧、ファンなどの状態を監視、制御するために利用される。
※1c パスワードクラック：パスワードを推測するための攻撃。ありとあらゆる文字列の組み合わせを試す総当たり攻撃や、あらかじめ用意したパスワードのリストなどを使う辞書攻撃などがある。
※1d 共通脆弱性タイプ一覧CWE：米国政府の支援を受けた非営利団体のMITREが中心となり仕様策定をした、脆弱性の種別を識別するための世界的な共通基準。Common Weakness Enumerationの略。

2 クラウド環境の脆弱性傾向分析 アクセス制御の問題を見落としがち!?

天 川 知 子

システムアセスメント部　プラットフォーム診断担当

2014年ラック入社。プラットフォーム診断を担当。官公庁案件のリーダーや、教育セミナーの講師にも従事。HardeningやPacSecなどの各種セキュリティイベントに参加し、業界のトレンドを追いかけている。

総務省調査によると、クラウド環境(以下、クラウドという)を利用している企業の割合(「全社的に利用している」「一部の事業又は部門で利用している」の合計)は2016年に46.6%と全体の半数近くに及び、2014年、2015年の同調査結果(それぞれ38.1%、44.0%)と比べても、増加傾向にあることがわかります(※2a)。

クラウドの利用増加に伴い、OS／ミドルウェアをクラウドに構築しているお客様から、ラックへプラットフォーム診断を依頼されるケースが増えてきています。その診断結果を分析したところ、クラウドに見落としがちな問題がある現状が見えてきたため、その結果を紹介します。

オンプレミス同様に対策が必要

クラウドを利用する際に見落としがちな問題を分析するため、ラックが2017年に実施したプラットフォーム診断の結果からクラウドのデータを抽出しました(※2b)。

診断対象となったクラウドのうち、重要な問題点(High／Mediumリスク)が検出されたホストの割合を調べたところ、2017年は19.6%でした図2-a。同年のオンプレミス環境での検出率は16.1%であり、クラウド、オンプレミス環境共に2割弱となりました。オンプレミス、クラウドに関わらず、対策が必要と言えます。

見落とされるアクセス制御の脆弱性

共通脆弱性タイプ一覧CWEを使い、クラウドで検出された重要な問題点の特徴を分析しました図2-b。検出した問題のうち、「認可・権限・アクセス制御」が8割と大部分を占めています。具体的には、サービスやWebコンテンツへのパスワード認証試行が可能、設定ファイルにアクセス可能などです。

これらの問題は、ソフトウェアをアップデートすれば解決するというものではありません。クラウド利用者側の設定不備に起因する問題のため、利用者自身が意識してセキュアな設定をする必要がありますが、この対策は見落とされがちです。アクセス制御の不備は、リモート診断全体でも6割と最も多く検出されており、特に注意する必要があります。

ラックのサイバー救急センター(※2c)が対処した事例に、アクセス制御の不備が原因で、クラウドのサーバでroot権限が奪取され、DDoS攻撃用ボット(※2d)を仕込まれていたものがありました。クラウドでは、利用者側で設定変更できる箇所やインストールしたOS・ソフトウェアなどは利用者側でセキュリティを保つ責任があるため(※2e)、セキュリティ対策に抜けがないか確認する必要があります。

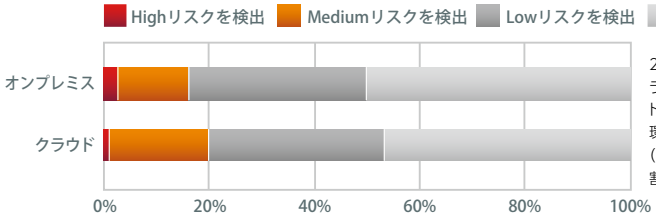
クラウドへの診断は申請有無を確認

クラウドにセキュリティ診断を実施する時は、利用規約に違反していないか、診断の事前申請が必要かをあらかじめ確認してください表2-a。申請が必要な場合は、許可までに要する期間を考慮して手続きすることをお勧めします。

プラットフォーム診断を活用してクラウドを安心して使おう

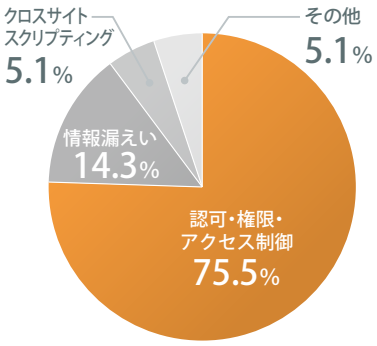
前述したように、クラウドにおいても実際にプラットフォームの脆弱性が検出されています。プラットフォーム診断をはじめとするセキュリティ診断を実施し、便利なクラウドを安心して利用できるよう、利用者自らが取り組むことが重要です。

図2-a 重要な問題点の検出割合



2017年にラックが実施したプラットフォーム診断結果(リモート)を集計(※2b)。オンプレミス環境、クラウド共に重要な問題点(High／Mediumリスク)を2割弱のホストで検出している。

図2-b 検出された問題の種別



2017年の診断結果から、クラウドで検出された重要な問題点を抽出し、CWE別に整理した。「認可・権限・アクセス制御」の割合が一番多い。

表2-a クラウド事業者ごとの申請要否

クラウド	診断可否	事前申請	申請期限	備考
AWS	可能	必要	3営業日前	2017年にCloudFront、API ゲートウェイ、Lambdaなど診断対象が拡大。m1.smallなど診断禁止もある
Microsoft Azure	可能	任意	(非公開)	侵入テストのルール事項を遵守する必要がある
Google Cloud Platform	可能	不要	-	利用規定ポリシーと利用規約を遵守する必要がある
サクラのクラウド	可能	不要	-	他のお客様への影響やサービス継続に支障があると判断された場合に、制限等を実施される場合あり
NIFCLOUD	可能	不要	-	利用規約を遵守する必要がある

主なクラウド事業者ごとの申請の要否一覧(ラック調べ。2018年2月時点)。セキュリティ診断を実施する前に、各クラウド事業者の利用規約や事前申請の要否を確認すること。各クラウド事業者の規約については注釈参照(※2f)。

※2a **総務省「平成28年 通信利用動向調査報告書」(企業編)**：http://www.soumu.go.jp/johotsusintokei/statistics/statistics05b2.html
※2b **クラウドのデータを抽出**：診断対象のドメイン名からクラウドと判断できるものを集計している。
※2c **ラックのサイバー救急センター**：セキュリティに係るお客様の緊急事態に対応するエキスパート集団。
※2d **DDoS攻撃用ボット**：ボットとは、PCなどに感染し、自動的に不正な処理をするプログラムのこと。分散型サービス妨害をDDoSと呼び、ここではDDoS攻撃をするボットという意味。
※2e **責任共有モデル**：AWSでは、クラウド上でも自身が構築したサーバなどのセキュリティはユーザの責任だと位置付けている。 https://aws.amazon.com/jp/compliance/shared-responsibility-model/
※2f **各クラウド事業者の規約**：各クラウド事業者のセキュリティ診断に関する規約のURLは次の通り。
AWS：https://aws.amazon.com/jp/security/penetration-testing/?nc1=h_ls
Google Cloud Platform：https://cloud.google.com/security/
NIFCLOUD：https://cloud.nifty.com/cs/catalog/cloud_faq/catalog_170619003040_1.htm
Microsoft Azure：https://blogs.msdn.microsoft.com/dsazurejp/2017/07/01/microsoft-azure-12/
サクラのクラウド：https://manual.sakura.ad.jp/cloud/support/support/others.html#support-others-01

3 Webアプリケーション診断　ツールと手動の違い システムに適したサービスの選び方

佐 久 間 泰 地
システムアセスメント部　Webアプリケーション診断担当
2013年ラック入社。入社してから現在までWebアプリケーション診断を担当。現在は、チームリーダとして案件をとりまとめる。その他、セキュリティイベントでの講演や、診断技術者の育成などを担当。

Webアプリは利用者の個人情報を扱うことが多いため、脆弱性などセキュリティ上の問題があると個人情報が流出する恐れがあります。個人情報の流出は、企業や組織の信用失墜につながり、場合によっては訴訟問題に発展することもあります。このような事態を未然に防ぐためにも、システムに内在するセキュリティ上の問題を発見し、適切に処置する必要があります。

ラックに依頼されたWebアプリケーション診断の件数は、「1-2 セキュリティ診断を実施するお客様の状況」で説明したように2017年は2008年に比べ3.5倍に増加しています。

ここでは、ツール診断と手動診断の違いを述べつつ、システムに適したサービスの選び方を解説します。

ツール診断と手動診断の違いを把握しよう

ツール診断と手動診断の共通点と違いを説明します。いずれも疑似攻撃文字列の送信先を特定するため、トップページからリンクをたどって巡回し、診断対象の画面やパラメータを洗い出すところまでは同じです。その後、ツール診断では、Webアプリ内でツールが巡回できた画面に対してツールが疑似攻撃の文字列を送信し、システムの挙動から脆弱性の有無を確認します。これに対して手動診断では、Webアプリ内の各画面において機能の仕様や送信される項目に合わせて疑似攻撃の文字列を送信し、システムの挙動から診断員が脆弱性の有無を確認する点が異なります。ツール診断に比べると手動診断は脆弱性の検出精度が高くなりますが、診断に必要な期間が長くなるため費用もかさみます。

診断ベンダの多くは、費用を抑えながらも高い検出精度は維持できるよう、ツール診断と手動診断を併用する方法でサービス提供しています。各診断の特徴を表3-aにまとめました。ラックのサービスメニューでも、手動診断でWebサイトの隅々までを徹底的に検査する「アドバンスト診断」に加え、ツール診断と手動診断を併用してコストパフォーマンスを高めた「ハイブリッド診断」をそろえています(※3a)。

ツール診断の中でも品質の違いがある

ツール診断と言っても、全ての工程を自動化しているケースはほとんどありません。Webアプリの巡回や診断を行う際に、診断員が手作業でどのようなツール設定をするかによって、診断の品質や期間、費用が変わります。そこで、巡回方法（対象画面の設定方法）の違いを次ページ表3-bに、診断結果の精査方法の違いを次ページ表3-cにまとめました。

ラックの「ハイブリッド診断」では、大半の診断項目をツールで診断していますが、巡回方法と診断結果の精査方法ではどちらも最も品質の高いレベル4の方法で実施しています。

診断項目と画面の絞り込みで診断期間・費用を圧縮

巡回方法と診断結果の精査方法のほか、「診断項目」と「画面の範囲」を絞り込むことでも、診断期間と費用を抑えられます。絞り込みにより、診断に必要な工数が変わってくるからです。診断項目と画面範囲を絞り込むにあたって考慮すべき点を示します。

●**診断項目**：ツール診断でもある程度検出が可能な脆弱性（クロスサイトスクリプティング やSQLインジェクションなど）のみとするか、セッション管理に関係するものやWebアプリ固有のものまで手動で確認するか

●**画面の範囲**：Webアプリの全ての画面を対象にするのか、サンプルとして選んだ画面だけを対象にするのか

●**「ツール＋手動」診断の場合**：手動診断するのは対象システムの全ての画面か、サンプルとして選んだ画面だけか

また、診断対象のWebアプリが大規模な場合、全画面を診断しようとすると診断期間は長くなり、費用も高くなります。この

表3-a　ツール診断、手動診断、「ツール+手動」診断の長所と短所

ツール診断	長所	●一定の期間内に多くの画面を診断できる。 ●一画面あたりの費用が安い。 ●一定のルールに従った診断項目（クロスサイトスクリプティング(※3b)やSQLインジェクション(※3c)等）は得意。
	短所	●Web画面の作りによっては、自動巡回できない。 ●脆弱性の見落とし(※3d)や誤検知が発生しやすい。 ●同じ処理が一度しか出来ない画面は不得意。 ●ツールが大量の通信や登録処理を発生させるため、システムへの負荷や登録完了メールによる業務への負荷が高くなりやすい。
手動診断	長所	●画面の仕様に合わせて診断できる。 ●ツール診断が苦手な診断項目を含めて調査できる。 ●処理が複雑なWebアプリも診断できる。
	短所	●一画面あたりの診断にかかる時間が長い。 ●一画面あたりの費用が高い。 ●診断ベンダ・診断員の技術レベルによって、検出できる脆弱性に差が出る可能性がある。
ツール＋手動診断	長所	●ツール診断と手動診断の長所を併せ持つ。 ●手動診断より安く、ツール診断より脆弱性を多く検出できる。
	短所	●全てを手動診断するのに比べ、検出されない脆弱性が残る可能性がある。 ●診断ベンダ・診断員の技術レベルによって、検出できる脆弱性に差が出る可能性がある。

※3a **ラックのセキュリティ診断**：https://www.lac.co.jp/service/consulting/#cat4
※3b **クロスサイトスクリプティング**：ユーザからの入力値に対してエスケープ処理が行われずに、そのまま次画面等に出力されるため、ユーザのWebブラウザ上でスクリプトを実行することができる脆弱性。攻撃者が任意のスクリプト文字列を構成し、ユーザのCookie情報を窃取したり、Webブラウザを不正に操作したりする恐れがある。
※3c **SQLインジェクション**：攻撃者がSQL文として意味を持つ文字列をWebアプリに送信することにより、任意のSQL文を実行させることができる脆弱性。攻撃者にデータベース内の情報を改ざんされたり、窃取されたりする恐れがある。
※3d **脆弱性の見落とし**：ツール診断は、システム挙動として一律に定義できない設計に起因する脆弱性（セッション管理に関係するものやWebアプリ固有のもの）は見落としやすい。

ようなケースでは、画面をサンプリングして診断を実施し、検出された脆弱性について全体で対策することがあります。ただし、これにはWebアプリ全体で同じ実装をしていることが前提となります。ラックで対象を選定する際は表3-dに基づき優先度を判断し、重要な画面かつWebアプリの実装パターンを網羅できるように画面を選定しています。

目的に合った診断サービスを選ぼう

ここまで、診断方法によって品質や費用が変わることを説明しました。診断ベンダは、経済産業省の平成29年度「情報セキュリティ監査台帳」に登録されているだけでも154社あります(※3e)。サービスレベルも費用も異なるベンダの中から、自社の対象システムに適したセキュリティ診断サービスを選択する際は、次に挙げる4つの判断材料を元に検討します。

1 診断の目的は「脆弱性の傾向把握」か「隅々までの脆弱性チェック」か

2 対象システムが取り扱う情報はどの程度重要か

3 ログインの有無など、対象システムの機能や仕様はどの程度複雑か

4 セキュリティ診断にどの程度、費用を掛けられるか

自社のシステムに合った適切なサービスを選択しないと、診断期間と費用が無駄にかかったり、最も診断が必要な画面で診断ができていないという事態になったりしかねません。例えば動的なページが少なく、公開情報のみを扱う公式ホームページに手動診断を行ったとしても、検出される脆弱性は自動巡回のみのツール診断と大差ありません。逆に、重要な個人情報やクレジットカード情報を取り扱っている会員制サイトに自動巡回のみのツール診断を実施したとしても、正常に巡回できる画面はほとんどありません。この場合、リスクの高い脆弱性がシステムに潜んだままとなる可能性があるため、いずれその脆弱性を狙った攻撃を受ける恐れがあります。

ここまで見てきたように、セキュリティ診断を検討する際はその目的や対象システムの機能、取り扱っている情報などを十分に把握したうえで、診断ベンダが提供しているサービスの品質や具体的な実施内容を確認し、最も自社に適したサービスを選択することをお勧めします。

表3-b ツール診断の巡回方法

レベル	巡回方法(対象画面の設定)	診断範囲の網羅性	費用	期間	品質
1	トップのURLを指定し、ツールが自動で巡回を行う。	●セッション管理されている画面に遷移できない ●個人情報などのツールで設定できない入力項目がある画面に遷移できない	低	短	低
2	自動巡回の途中でセッション切れやエラーが発生した際に、再度ログインを行うようにツールを設定する。	●個人情報などのツールで設定できない入力項目がある画面に遷移できない	↑↓	↑↓	↑↓
3	診断員がブラウザを操作して巡回を行う。巡回した内容をツールに引き継ぎ、ツールで診断する。	●巡回時は全画面を網羅 ●診断時は、遷移する際に特定の値を引き継ぐ必要がある画面に遷移できない	↑↓	↑↓	↑↓
4 ※	診断員が手動で巡回後、セッションやWebアプリが使う特定の値を引き継ぐ設定を行う。	●巡回時も診断時も全画面を網羅	高	長	高

※ラックの「ハイブリッド診断」では、巡回方法(対象画面の設定)の品質が一番高いレベル4を採用している

表3-c ツール診断の結果の精査方法

レベル	診断結果の精査方法	検出できる問題の精度	費用	期間	品質
1	ツールの検出結果をそのまま診断結果として報告する。	ツールによる見落としがあり、誤報が含まれる。	低	短	低
2	ツールの検出結果を確認した後、診断員が誤報を精査する。 その結果を診断結果として報告する。	ツールによる見落としはあるが、誤報は一部無くなる。	↑↓	↑↓	↑↓
3	ツールの検出結果を確認した後、診断員が誤報の精査と再現性の調査を行う。 その結果を診断結果として報告する。	ツールによる見落としはあるが、誤報はほぼ無い。	↑↓	↑↓	↑↓
4 ※	ツールの検出結果を確認した後、診断員が誤報の精査と再現性の調査を行う。 さらに、再現条件の難易度や、漏えいや改ざんされ得る情報の重要度などを踏まえ、実害発生時の影響を評価して診断結果として報告する。	ツールによる見落としはあるが、誤報はほぼ無い。 実害発生時の影響を含めたリスクがわかる。	高	長	高

※ラックの「ハイブリッド診断」では、診断結果の精査方法の品質が一番高いレベル4を採用している

表3-d 画面サンプリング時の優先度

※表中の数字が「優先度」(1:高い〜5:低い)

	個人情報・重要情報を扱う			個人情報・重要情報を扱わない		
	ログイン前	ログイン後		ログイン前	ログイン後	
	-	一般ユーザ	管理者画面	-	一般ユーザ	管理者画面
データベースと連携する画面	1	2	5	2	3	5
ユーザが入力した値を表示する画面	2	3	5	3	4	5
セッション管理機能がある画面	4	4	5	5	5	5

優先度	主な画面の例
1	ログイン、会員登録、パスワード再発行
2	検索、お問い合わせ、資料請求、会員情報表示・変更・削除、決済処理、注文履歴表示
3	掲示板、ブログ、ショッピング機能(商品選択、カート)、お届け先の入力
4	アンケート入力、ログアウト
5	管理者用画面全般(一般ユーザがアクセス不可能)

※3e 経済産業省 平成29年度「情報セキュリティ監査企業台帳(2017年11月27日版)」から、「リスク評価/脆弱性評価サービス」を条件に抽出した。http://www.meti.go.jp/policy/netsecurity/is-kansa/

4 セキュリティ診断の現状とこれからペネトレーションテストの使いどころ

吉 田 聡
システムアセスメント部　ペンテストグループ　GM
2003年ラック入社後、Webアプリケーションの診断を担当。現在は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)に参画。

セキュリティ診断の昔と現状

ここでは、セキュリティ診断(以下、診断という)に携わる技術者の視点から、診断をうまく使いこなしているお客様の事例と、システムをより安全に運用するためのヒントとなるペネトレーションテストについて紹介します。

前章までに述べたように、ラックの診断サービスは多くのお客様への提供実績があります。システムを利用する企業にとって、診断をはじめとするセキュリティ対策は直接利益を生み出すものではありません。しかし、システムを安全に運用するために、診断を実施してセキュリティ上の問題を把握し、対策するという考え方は、現在では一般的になっています。

過去を振り返ると、2000年頃から積極的に診断を実施してきたのは、システムが保有する情報の漏えいやシステム停止などが起きたときに多大な被害の発生が懸念される企業(金融業やECサイトを運営している企業)でした。それ以外の企業は、十分な予算が確保できずに簡易的な診断で済ませるか、まったく実施しないかのどちらかでした。

最近では、自社で実施すべきセキュリティ対策を適切に把握し、対策に優先順位を付けて対応する企業が増えています。このような企業では、計画的に対策を進めるため診断を適切なタイミングで実施しています。例えばラックのお客様の中には、システムの公開前と改修時に診断を受けるというルールを作り、システムのリリース判定基準に診断結果を含めていることがよくあります。これまで多くのお客様に対して診断を実施し、検出した問題の対策を共に検討してきた経験から、診断とセキュリティ対策の活用度合いには、4つの段階があると考えています図4-a。

診断を使いこなす4つの段階

Step1は診断を実施していない状態です。2018年現在では少数派ですが、1990年代の企業ではこれが一般的でした。

Step2は、一部の重要システムに対して診断を実施している状態です。この状態の企業では、各システムの担当者が個々に診断を依頼してきます。診断時期や実施方法に全社的なルールがないため、診断を実施する目的やタイミングはさまざまで、担当者が必要性を考えてというケースのほか、同業他社で事件が起きたときに不安にかられてといったケースなどもありました。その結果、一つの企業内で対策にばらつきが生じ、あるサイトではセキュリティがしっかりしているが、あるサイトでは不十分なままという状況が生まれました。

2005年になると、政府が「政府機関の情報セキュリティ対策のための統一基準(※4a)」の初版を公表しました。この統一基準を参考に、民間でも脆弱性対策が行われた結果、自社が保有する全ての公開システムを診断対象とする企業が増えていきました。このときに、Webサイトが保有する個人情報の漏えい事件が多発したことも診断を実施する企業が増えた要因です。また、企業が保有する全システムを効率的に診断するために、セキュリティ対策部門や品質管理部門が窓口となり、自社のWebサイトを一元的に管理して診断するようになりました。こうして診断の目的や実施のタイミングがルール化され、企業として一元管理できている状態をSTEP3としています。

一元的な管理を実現して、ルールに沿った診断を実施すると、明らかになった問題へのセキュリティ対策や運用を企業判断で行うことができます。図4-bは、ある製造業のお客様が管理する約40のWebアプリに対して、診断と検出した問題の対応を3年間続けたときの結果です。1年目は、評価結果が良かった(AAA、AA)Webアプリは15%、HighリスクやMediumリスクの問題を検出したアプリ(A、B、C)は85%でした。しかし、3年目にはAAA、AAの合計が約80%になるまでに改善しました。全社的に取り組んだ結果、Webサイトのセキュリティが底上げできた好例です。

図4-a　企業のセキュリティ診断の活用度合い

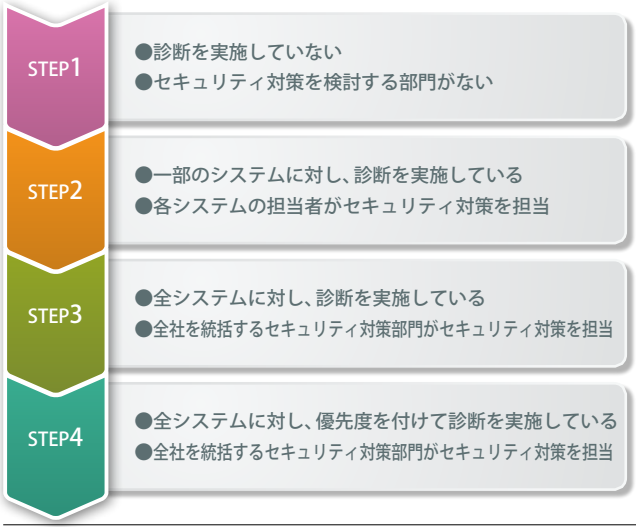
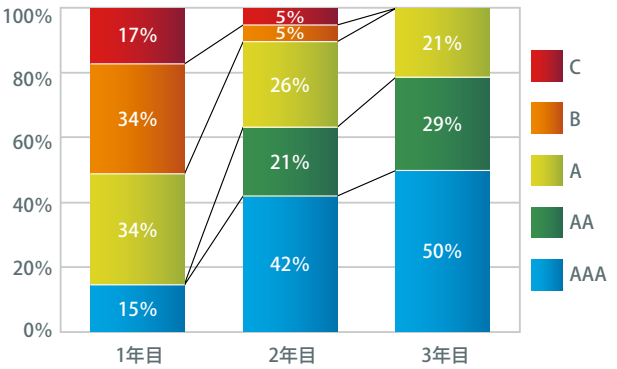


図4-b　Webアプリを継続的に診断したときの評価結果例



あるお客様のWebアプリ(数は約40)に対して、3年間にわたって診断した結果の推移。評価は、Webアプリごとに「良い」から「悪い」の順にAAA、AA、A、B、Cの5段階。1年目は、AAAとAAのWebアプリの割合が15%だったが、診断と対策を継続した結果、3年目にはAAAとAAのアプリが約80%を占めるまでに改善した。

※4a 政府機関の情報セキュリティ対策のための統一基準：https://www.nisc.go.jp/active/general/kijun01.html

このように、診断の活用が成熟してくると、診断の目的は脆弱性を見つけることではなく、脆弱性がないことを確認することになります。さらには効率のよい管理を目指し、Webサイトが担う業務の重要性や情報自体の重要性を判断し、Webサイトやシステムに優先順位を付けて診断するようになります。この状態がSTEP4です。診断にかかる費用に対して、より効果の高い診断を実施できる状態になります。近年は、大企業を中心にSTEP4に達しているケースが増えています。

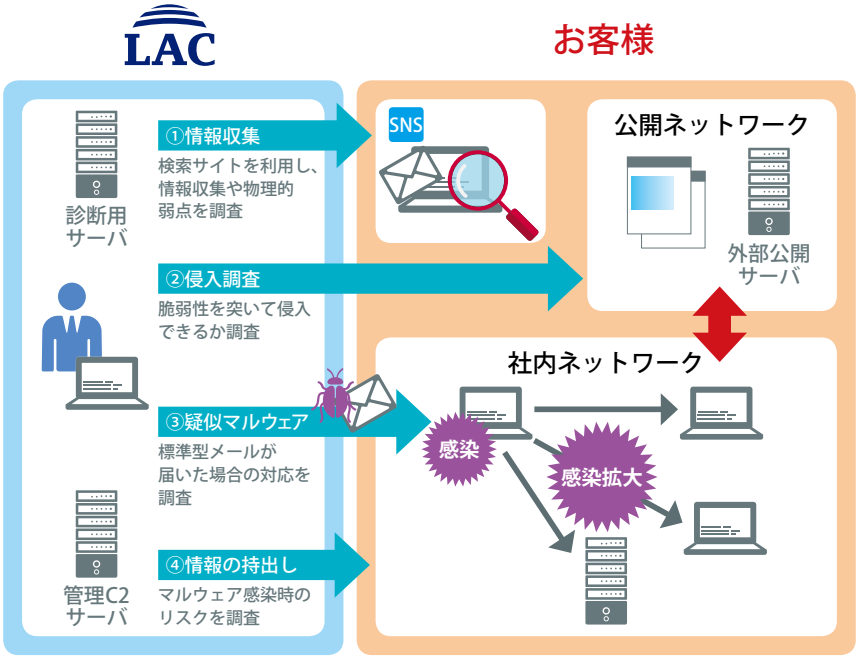
ペネトレーションテストの活用

ここで、攻撃者に視点を移します。攻撃者は、インターネットに公開されているシステムに対し、手当たり次第に攻撃を仕掛けているものの、より効率的に重要な情報を奪いたいとも考えています。そのため、特定の業種や企業に狙いを定め、その企業の社員が利用するPCをマルウェアに感染させて内部の重要情報を奪う攻撃を実施します。それが、2009年ごろから被害が報道され始めた標的型攻撃(※4b)です。

標的型攻撃によって深刻な被害が発生していることを受け、各企業は出口対策やエンドポイントのセキュリティ対策など何らかの対応を行っているように思います。しかし、標的型攻撃の事案が絶えないのは、実際に攻撃されるまで対策が有効に働いているかどうかの評価ができていないことが原因の一つです。対策を評価できない理由は主に次の二点です。

●具体的な攻撃内容がわからない
●適切な評価方法がわからない

図4-c　ペネトレーションテストサービス概要



そこで効果を発揮するのがペネトレーションテストです。診断では脆弱性があることまでは確認しますが、本番環境に影響を与えるような脆弱性を利用した侵入を試みることはしません。一方、ラックのペネトレーションテストサービス(※4c)では、ときには、お客様と調整のうえ本番環境に影響が及ぶようなことも行い、できる限りの侵入を試みます 図4-c。具体的には、お客様のシステムへ侵入するため、情報収集を行い、疑似攻撃を実施します。その結果、公開サーバから機密情報を取得したり、社内PCからC2サーバ(※4d)と通信して機密情報を漏えいさせたりするなど、お客様が把握していない抜け穴を見つけることができます。

ペネトレーションテストと診断の使い分け

ペネトレーションテストと診断では実施目的が異なります。ペネトレーションテストはあくまで攻撃者目線に立ち、ある特定の範囲を中心に実害を起こし得るかを綿密に調査して侵入可能な範囲を確認します。一方、診断はシステムを網羅的に調べ、脆弱性をできる限り洗い出します。表4-aに、目的や評価対象、期間・金額など、ペネトレーションテストと診断の内容を一覧にしました。システムを評価する目的に応じて、ペネトレーションテストと診断を使い分けることをオススメします。

最後に

診断に対するお客様の意識が成熟するのに伴い、診断の活用法も変化してきました。

今後、IoT機器のような新しいモノが生まれると、それを安全な状態でユーザに利用してもらうために、サービスや機器を提供する側はセキュリティを検討する必要があります。車のセキュリティも最近注目されていますが、人命に関わるものはより慎重な検討が必要でしょう。

ラックは、お客様の変化に応え、寄り添い続けていくために、新しいモノに対する情報を収集して技術を磨き続けています。もし、セキュリティに関して不安な点がありましたら、いつでもご相談ください。

表4-a　ペネトレーションテストと診断の比較

	ペネトレーションテスト	診断
目的	対象システムへの侵入可否、侵入後の実害の度合いを検証	対象システムの脆弱性や問題を網羅的に洗い出すこと
対象	●システム・サーバ ●クライアント（PC・端末） ●各種データ（機密情報、個人情報など） ●人的セキュリティ（正社員、派遣社員） ●建物・設備（オフィス、データセンター）	●システム・サーバ ●クライアント（PC・端末）
網羅性	●検証内容に合わせて、特化した疑似攻撃を実施。脆弱性や問題の網羅的な検出はしない	●診断対象の脆弱性や問題を網羅的に検出する
期間と金額	●実施シナリオに依存 ●2か月～半年 ●一案件あたり、1千万円～2千万円程度	●サーバのIP数やWebアプリの画面数などに依存 ●数週間～数か月 ●一サイトあたり、数十万円～数百万円
ラックのサービス	●ペネトレーションテスト ●APT先制攻撃	●Webアプリケーション診断 ●プラットフォーム診断 ●スマートフォンアプリケーション診断 ●IoT診断 など

※4b **標的型攻撃**：海外ではAPT（Advanced Persistent Threat）と呼ばれるサイバー攻撃の手法の一つ。海外では2009年頃からさまざまな事案が報道されるようになり、国内でも2011年以降、大手企業や政府機関等を対象にした事案が明らかになっている。
https://www.lac.co.jp/library/guidebook/3.html
※4c **ペネトレーションテストサービス**：https://www.lac.co.jp/service/consulting/penetration_test.html
※4d **C2サーバ**：遠隔操作ウイルスが、攻撃者からの指令を伝達する指令サーバ

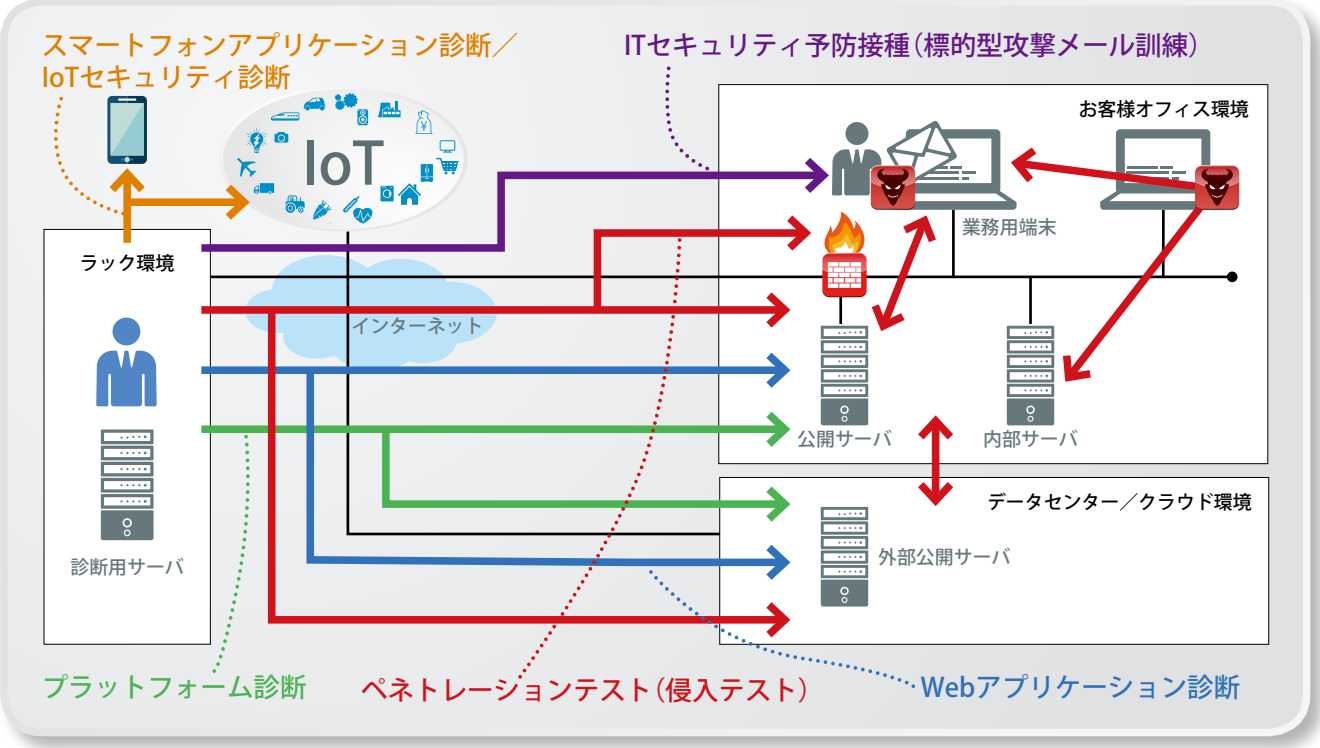
5 ラックのセキュリティ診断ラインナップ

ラックでは、「Webアプリケーション診断」や「プラットフォーム診断」「スマートフォンアプリケーション診断」など、多様なセキュリティ診断サービスを提供しています図5-a。1995年に日本で初めてセキュリティ診断サービスを開始し、そこから培った長年の経験と多数の実績を基に、セキュリティ診断のエキスパートがお客様のシステムの脆弱性を徹底的に調査します。

提供するセキュリティ診断のラインナップには、定番の上記3サービスに加え、近年のITの発展や、サイバー攻撃の脅威の深刻化に合わせて新たなものも用意しています。その代表的なものとして、爆発的な勢いで生活に広がりつつある、IoTを活かしたスマート技術やデバイスを対象とした「IoTセキュリティ診断」、標的型攻撃を代表とする高度なサイバー攻撃の耐性を評価する「ペネトレーションテスト」が近年ラインナップに加わりました。「ペネトレーションテスト」では、お客様のIT環境に対して疑似攻撃を仕掛けて実際に侵入し、情報漏えいや機能停止など実害の可能性があるかを実証します。

お客様のIT資産を安全に守るため、多様化・高度化するサイバー攻撃に対抗してラックは今後も先手を打ち、診断対象範囲をより一層拡充していきます。

図5-a ラックが提供するセキュリティ診断の一覧



サービス名	概要
Webアプリケーション診断	Webアプリの問題を網羅的に検出する目的の診断サービスです。 専門家ならではの視点で問題を洗い出し、その詳細や対応案を報告します。
プラットフォーム診断	サーバ／ネットワーク機器の問題を網羅的に検出する目的の診断サービスです。 専門家ならではの視点で問題を洗い出し、その詳細や対応案を報告します。
ITセキュリティ予防接種 （標的型攻撃メール訓練）	標的型攻撃メールに対する実践的な対応力を高めることを目的とした体験型教育プログラムです。 疑似的な攻撃メール（訓練メール）を従業員に送付し、メール開封率や訓練後のアンケート結果を集計して報告します。
スマートフォン アプリケーション診断	スマホアプリのセキュリティ対策が適切であるかを網羅的に診断し、問題の有無について報告するサービスです。 アプリケーションの操作、サーバとの通信、端末に保存するデータなどに問題がないかを実機で検証します。
IoTセキュリティ診断	IoT機器のセキュリティ対策が適切であるか、問題の有無を確認するための診断サービスです。 各種センサー、通信装置、スマート家電、スマートホーム、医療機器など多種多様なIoT機器を診断対象とします。
ペネトレーションテスト （侵入テスト）	お客様のITシステムに対して疑似攻撃を行い、実装済みのセキュリティ対策の有効性や システム全体の耐性を確認します。また、侵入できた場合には、被害拡散リスクを評価します。

株式会社ラック システムアセスメント部

〒102-0093 東京都千代田区平河町 2-16-1 平河町森タワー
TEL：03-6757-0113（営業）　E-MAIL：sales@lac.co.jp　https://www.lac.co.jp