ペネトレーション・テスト（侵入テスト）：攻撃者の視点を利用して重要な資産を保護

犯罪者が使うツール、手法、手口を用いて重大な脆弱性を特定する

目次

エグゼクティブ・サマリー

貴重なデータの量とそれを保護する規制の増大に伴い、サイバー犯罪者からビジネスを守ることの重要性がますます高まっています。2017 年 8 月から 2018 年 11 月にかけて IBM X-Force Red が実施した 183 件の侵入テストでは 1,099 個の脆弱性が特定され、うち 12% がリスクが高い、または重大な脆弱性に位置付けられるものでした 1。その 12% に含まれる脆弱性の 1 つでも犯罪者に利用されることがあれば、ビジネスは手痛い打撃を被るに違いありません。

CIO (最高情報責任者)、CISO (最高情報セキュリティー責任者)、およびセキュリティー担当者などにとって、重大な脆弱性の特定とその修復はえてして非常に大きな難題です。脅威の対象はネットワーク、ハードウェア、アプリケーション、デバイス、社員であり、組織の内外を問いません。X-Force Red では、これまで請け負った侵入テストの結果から、システムにおけるセキュリティー侵害の 50% は脆弱なパスワードやデフォルトのパスワード、ハードコーディングされた資格情報が原因であるとみています。X-Force Red のチームが 2017 年 10 月から 2018 年 11 月にかけて 1,176 通のフィッシング・メールをお客様の組織に送信したところ、198 人がそのリンクをクリックし、196 人が有効な資格情報を送信していました 2。

そのような脅威に対処するための予算、リソース、時間が限られていることから、自動ツールで自社環境をテストする組織もあります。しかしそのようなツールは、そもそも隙に乗じて侵入してくる未知の脅威を発見するようには設計されておらず、時に侵入を許してしまいます。

手動による侵入テストは、組織の環境全体で特に重大な既知/未知の脆弱性を発見するために作られたテストです。テストはネットワークやアプリケーション、ハードウェアから、ATM、自動車、飛行機、IoT (モノのインターネット) デバイスといった他のシステムに至るまで、あらゆるものに実施できます。手動テストの価値を認める組織は増え続けており、例えば X-Force Red に ATM の侵入テストを依頼した銀行の割合は、2017 年から 2018 年の間に 300% 増加しています 3。
侵入テストは、製品設計段階からセキュリティーを重点的に考慮することはもとより、規制基準の継続的な遵守や機密データの保護にも役立ちます。

侵入テストのニーズに結び付くセキュリティー上の課題

ビジネスにおけるセキュリティーの脆弱性が急増している理由は複数あります。企業はセキュリティーのベスト・プラクティスに従わず、保有する全資産へのアクセスを、社員、請負業者、ベンダーに無制限に許可しています。しかもそのアクセスは、資産の重要度レベルやアクセスするユーザーの役割に関係なく行われています。さらに厄介なことに、ネットワーク、デバイス、アプリケーション、ユーザーの間でやり取りされるデータにはかつてないほどの価値がありますが、その大半が各事業部門でサイロ化して管理されています。この複雑なインフラストラクチャーが、保有する最も重要な資産に対する脅威とそこに潜在する脆弱性の把握を難しくしています。

また、脅威者の種類は犯罪者集団から国家、そして単独犯から悪意のある、あるいは悪意のないインサイダーに至るまでさまざまです。多くの犯罪者は従来よりさらに洗練されたツール、手法、手順を使ってセキュリティーの管理をくぐり抜け、ユーザーを騙して機密データを流出させています。

テストの件数	発見された脆弱性の数	そのうち重大および高リスクな数
183	1,099	136

図 1. X-Force Red が 2017 年 8 月から 2018 年 11 月にかけて行った 183 件のテストでは、1,099 個の脆弱性が発見されました。それらのうち 136 個、すなわち 12% は高リスクまたは重大な脆弱性でした 4。

規制要件もデータ保護を取り巻く圧力と複雑さを増大させている一因です。例えば、PCI DSS (Payment Card Industry Data Security Standard) により設定されたセキュリティー要件は、支払いカード取引を扱うすべての組織に適用されます。取引の規模や数に関わらず、この分類に属するビジネスはいずれも、PCI DSS を何らかのレベルで遵守しなければなりません。

その他にも、EU 一般データ保護規則 (GDPR) では、ヨーロッパのデータ主体の個人データとプライバシーの保護が組織に求められています。GDPR の違反には、最大で 2,000 万ユーロ、またはその企業の全世界での年間売上高の 4% のうち、いずれか高い方の制裁金が科せられます。

脆弱性は日常的なビジネスの圧力からも生まれます。製品やサービスの方向転換や市場投入の期限が厳しく、それがデータのセキュリティーより優先されることもあります。企業合併や買収の結果、欠陥のあるデータが再編時に継承されることもあります。

このような要因を考慮すると、企業が積極的にデータ保護に取り組むには、侵入テストの採用を検討する必要があります。

侵入テストで何が得られるか

侵入テストは、特定の対象が持つセキュリティー上の脆弱性を割り出すために作られた、擬似攻撃と悪用のシミュレーションです。これらのテストは、犯罪者が環境に侵入して貴重な資産のセキュリティーを侵害する際に使用すると思われるツール、手法、手順を用いて、ハッカーが行います。

侵入テストは、社内/社外のいずれでも行われ、機密データにアクセスされたり、システムの欠陥が悪用されたりする可能性が評価されます。テストで発見された結果は、重大、高リスク、中リスク、低リスクにランク付けされます。重大または高リスクにランク付けされた結果は、単に理論上可能性があるという域を超えて、実際にシステムのセキュリティーを侵害する可能性が高いイベントです。

侵入テストを行うことにより、組織は、どの資産が攻撃に対して耐性があり、そしてどのような種類の脆弱性が存在するのかを把握できます。また、テスターは、犯罪者による脆弱性の悪用方法を実際に示すことで、犯罪者が察知する前に、組織がそれらの脆弱性を修正できるよう支援します。このような攻撃型の取り組みにより、組織は犯罪者より先に手を打つことができます。

また、侵入テストを行うことで、脆弱性のスキャンだけではカバーできない種類の脆弱性を検知できることがあります。スキャンでは既知の欠陥は発見できるものの、犯罪者が複数の脆弱性を組み合わせて攻撃するシナリオは見逃してしまう可能性があります。また、犯罪者が、データセンターにとって未知の攻撃手法を使用した場合も、スキャンによる検知から漏れるおそれがあります。さらに、スキャンが一部のシステムやハードウェア・コンポーネントに対応していない場合もあります。手動テストはスキャンが見落とした脆弱性の検知に有効です。

自力で行う侵入テストにはおのずと限界があります。重大な脆弱性の検知に必要なテストの量は、少人数のスタッフでは手におえないほど膨大です。セキュリティー・チームは担当する組織にのみ集中しており、他の同様のビジネスを攻撃している脅威を把握していないケースがほとんどです。離職率の高さとスキル不足も社内チームが力を発揮する妨げとなっています。

社外の侵入テスト・チームは、基本的にすべてをテストできます。このチームは既知/未知の脆弱性をより効果的に見つけられるよう、手動テストと自動ツールを組み合わせて使用します。チームの規模も専門知識も充実しているため、スケールアップも簡単です。また、社外の侵入テスト・チームは数多くの組織での実績があるため、脅威を取り巻く状況をより広い視点で理解しています。これらのグループは独自の調査チームを持つのが普通で、脅威インテリジェンス・フィードも利用しています。

さらに、多くの社内テスト・チームには自動車、IoT デバイス、ATM に関する専門知識がないことから、コンピューターをテストする場合と同じ要領で扱っています。しかしながら、これらの専門分野には、社外の侵入テスト・チームが持つ、その分野特有の専門知識、手法、ツールを活用した検証が必要です。

IBM のソリューション: IBM X-Force Red 侵入テスト・サービス

IBM Security の X-Force Red 侵入テスト・サービスは、特に危険な脆弱性の発見と修正に役立つスキル、スケール、スコープをお客様に提供します。X-Force Red チームには、数十年にわたって犯罪者と同じツール、手法、手順、そして発想を用いて組織に侵入してきた経験を持つ、何百人というハッカーが所属しています。また、熟練したスペシャリストと開発者は、コードとデバイスの構築方法と攻撃者の攻撃手法を熟知しています。X-Force Red チームのテスト方法にはバーチャル/オンサイトでの手動テストと自動スキャンが含まれ、これが適宜利用またはサブスクリプションによるサービスで提供されます。

X-Force Red 侵入テスト・サービスは、世界的に有名な企業から小規模事業者に至るまで、ほぼすべての業界のお客様に使用されています。X-Force Red チームは、組織が望むあらゆるネットワーク、アプリケーション、ハードウェア、人員、デバイスを、規模を問わずテストできます。テストは開発中と市場投入後の両方で実施できます。X-Force Red は数百の組織に対して侵入テストを実施しており、その数は今も増加しています。

X-Force Red チームはそのサービスを「ギフトカード型」の形式で販売しています。お客様はサブスクリプション・サービス内で毎月一定額を支払えば、テスト対象をいつでも変更できます。テスト期間は環境の規模とテストの領域、例えばコードの行数などに応じて異なります。

お客様のニーズに最適なテストの種類は、コンサルタントがお客様を支援して決定できます。テスト終了後に、X-Force Red チームが結果、使用した方法論、改善に向けた推奨事項の報告を行います。お客様は最も深刻な脆弱性が悪用された場合にビジネスが被るであろう最悪の影響と、その弱点を直ちに改善するには何が必要かを確認できます。

X-Force Red チームは、アプリケーション、ネットワーク、人員、ハードウェアなどをテストします。また、ATM、車、組み込みデバイスや IoT デバイスもテストできます。

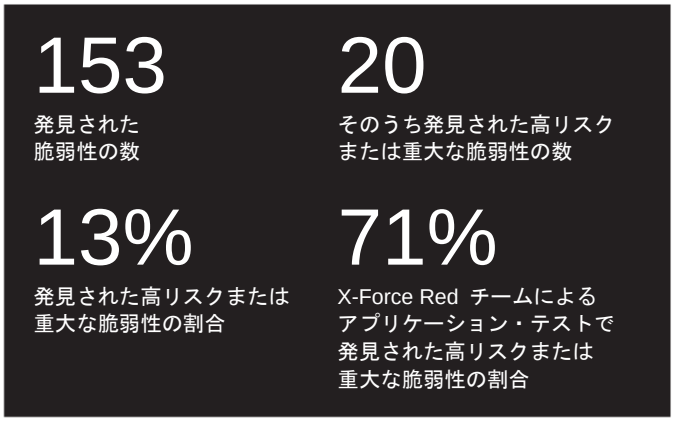
アプリケーション・テスト

アプリケーションは多くのビジネスの中核を担っています。基幹系アプリケーションが停止すればビジネスも停止します。

アプリケーションを保護するためにセキュリティーの自動管理機能を利用している組織もありますが、それらの管理機能が対処できるのは自動化された攻撃だけです。人間による手作業での攻撃を検知し、それに対応できるのは人間だけです。

アプリケーション・ファイアウォールを使用している組織もあります。しかし、それらはロジックの欠陥、すなわちアプリケーションが何を、どのような理由で実行しているかを捉えることができないため、犯罪者はしばしばこれを回避して悪用します。さらに、アプリケーションにマルウェアが仕込まれている場合もあり、それがインストールされれば、組織のシステムが感染する恐れがあります。

X-Force Red チームは 2018 年の 8 月から 11 月にかけて、24 件のアプリケーション・テストをさまざまな組織で実施しました。そこでは以下のような結果が得られました



テストの件数	発見された脆弱性の数	そのうち重大および高リスクの数
24	153	20

図 2. アプリケーション・テストについては、2018 年 8 月から 11 月までの間に 24 件のテストが行われ、153 個の脆弱性が見つかりました。それらのうち、テストの 20 件、すなわち 13% が高リスク、または重大な脆弱性でした。

これらの欠陥を軽減するために、X-Force Red チームはアプリケーションを手動でテストし、開発者が見逃したであろうセキュリティー・プロセスと管理の脆弱性を特定します。テスターは既知の脆弱性と「今のところ未知」の脆弱性を検証し、誤検知をなくします。

X-Force Red はアプリケーション・ソース・コードのレビューも行うことができます。お客様にソース・コードを提供していただくことで、時間的にもコスト面でもより効率的なテストが可能になります。

ビジネスを動かすのは基幹系アプリケーションです。そのため取締役会がアプリケーション・セキュリティーのテストを求めるケースが増えています。同時に、業界規制の遵守義務においても、PCI DSS などの侵入テストが求められるようになりつつあります。X-Force Red のアプリケーション・テストは、アプリケーションの市場投入の前後を通じてお客様が遵守義務に対応し、セキュリティー要件に対応できるよう支援します。

ネットワーク・テスト

サード・パーティー・ベンダーのテクノロジーの使用は、企業ネットワークをリスクにさらすことになりかねません。ベンダーがセキュリティー・ポリシーとその手続きに従っているとは限らないからです。また、企業がそれらのテクノロジーをセキュリティーのベスト・プラクティスに従わずに導入している場合もあります。

さらに、社内の通信や、そのネットワークを通過する他のアプリケーションを暗号化していない企業もあります。そういった欠陥があれば、犯罪者はパスワードを破り、企業のサーバー、仮想マシーン、顧客データ、データベースのバックアップなどにアクセスできるようになってしまいます。

X-Force Red チームは、手動のネットワーク侵入テストを使用してそれらの問題を特定できます。このアセスメントでは、リスクにさらされるサービス、構成、インフラストラクチャーに焦点を合わせて、ネットワークの観点からデバイスのセキュリティーを評価します。またテストでは、犯罪者が行う便乗攻撃や、スキャナーが検知できない脆弱性が特定されます。

X-Force Red のテスターは、犯罪者と同じツール、手法、手順、そして発想を用いて組織のネットワーク・インフラストラクチャーに侵入し、脆弱性を特定します。例えば、ネットワークのホストが、攻撃に弱い他のホストとの間にアクティブな信頼関係を持っているといった欠陥を特定します。テストは通常、社員がネットワークを使用しており、直ちに改善が必要な場合に即座に対応できる営業時間内に行われます。ネットワークの規模にもよりますが、プロジェクトには 1、2 週間かかるのが普通です。

ネットワーク・テストを実施することで、お客様は、すべてのネットワークとインフラストラクチャー全体の保護を強化するには、プログラムにどのような変更を加えればよいのかを把握することができます。ネットワーク・テストは、リスクを最小化するにはリソースのどこに投資すべきかを、セキュリティー・リーダーが理解するのにも役立ちます。

人員テスト

セキュリティー意識向上のトレーニングを実施する組織は増えているものの、社員教育をまったく行っていない組織や、その頻度が十分でない組織も存在します。 たとえ最高のセキュリティー管理を行っても、社員を対象とする一部の攻撃を阻止することはできません。

セキュリティー侵害の最大の原因は脆弱なパスワードやデフォルトのパスワード、そしてハードコーディングされた資格情報であるという X-Force Red による見解は先に述べたとおりですが、もう 1 つの課題として挙げられるのが、犯罪者が社員にメールを送りつけて個人情報を聞き出す、フィッシングとの戦いです。

X-Force Red チームはソーシャル・エンジニアリングの手法を使用して、犯罪者によるものと同様の策を練ります。テスターはどの社員が悪意のあるメールに反応したかを分析します。またビッシング、すなわちボイス・フィッシングの演習も実施し、社員がどの機密情報を未確認の相手に電話で漏らしたかを確認します。

この他にも、偽の内容を USB ドライブに読み込ませ、ユーザーを騙してそれをデバイスに接続させるテストも行います。物理的セキュリティー・テストとしては、X-Force Red チームは企業のサイト内にあるセキュリティー・エリアや機密情報へのアクセスを試み、ポリシーや手続きを評価します。

テストが終了すると、X-Force Red チームはお客様に合わせて優先順位を付けた推奨事項をリストにして提供し、特定された脆弱性の削減を支援します。

ハードウェア・テスト

犯罪者がデバイスのセキュリティー侵害を企んでいる場合、それを妨げる手立てはまずありません。彼らはそのデバイスと同じモデルを購入して内部を調べ、脆弱性を発見します。そしてその知識を使って欠陥を悪用し、ターゲットを丸裸にするのです。多くのハードウェア・デバイスには格納されているデータの暗号化機能がなく、しかも生産時の機能の情報がデバイス上に残ったままになっています。犯罪者はデバイスのモデルを 1 つ入手し、デフォルトの資格情報を取り出すと、その資格情報を使用して対象デバイスのセキュリティーを侵害することができます。

X-Force Red のテスターは、製品がどのように作られたかを最初から最後までレビューします。このテストの対象は、そのデバイスで使われるすべての電子部品と筐体やハウジングです。また、テスターは、セキュリティー対策を後から気付いて追加するのではなく最初から製品に組み込めるように、部品や制御装置の選択と実装を支援します。

X-Force Red チームが提供するハードウェア・テストには 2 つの種類があります。「ホワイト・ボックス」のテストでは、お客様が設計資料、ソース・コード、設計図を提供します。X-Force Red チームはソース・コードとシステム内外を流れるデータをレビューし、製品の実装と外部ライブラリーの脆弱性を特定します。 もう 1 つの「ブラック・ボックス」のテストでは、X-Force Red チームが製品をリバース・エンジニアリングし、そこから設計資料を再作成します。このプロセスによって、製品のライフサイクル内の脆弱性が、ソース・コードや実装を含めてテストされます。

ATM、IoT、自動車に関する固有のテスト

X-Force Red チームには ATM、自動車、IoT、POS などのデバイスをテストしてきた数十年に及ぶ実績があります。テスターはこれらのシステムを調査、テストし、それらのセキュリティーを保護するためのガイドを、その設計期間に留まらず提供します。X-Force Red チームは、これらのシステムで発生する欠点と悪用をグローバルな視点で捉え、必要に応じて実践的な支援を提供します。

ATM を例に挙げましょう。至る所に設置され、何千万円もの現金が入っている ATM は、犯罪者にとって格好の獲物です。

2018 年の 1 月から 10 月にかけてのテストで、X-Force Red チームは、ATM が持つセキュリティー上の最大の問題として、フルディスク暗号化が行われていないこと、およびキャビネットの鍵が貧弱であることをあげました。あるテスターは 20 秒で ATM のキャビネットの鍵を壊すことができました。

次の図に示すように、銀行はこれらの脅威の重大性を認識しています。

300%

X-Force Red チームに ATM のテストを要請した銀行の 2017 年から 2018 年の増加率。アジア太平洋地域単独では、ATM テストの要請は 5 倍に増加しています。

この増加には、ATM の「キャッシュ・アウト」攻撃が急増しているという FBI からの警告も一役買っています。以下の図はこの脅威を表したものです。

FBI の警告: キャッシュ・アウト攻撃

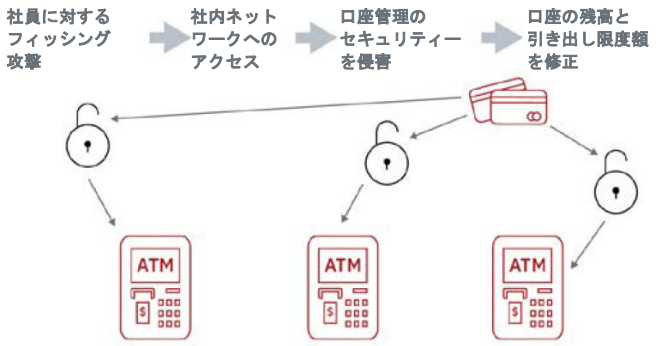


図 3. 「キャッシュ・アウト」攻撃では、犯罪者は引き出し限度額を操作して不正な ATM カードを作成し、現金を引き出します。この手口によって顧客口座の全額が引き出される可能性もあります。

X-Force Red チームは、お客様にオンサイトでの ATM テストと仮想テストを提供します。また、お客様が ATM (あるいは IoT や自動車固有デバイスといった同様の電子機器) を X-Force Red ラボに送り、テストを実施することも可能です。

X-Force Red は、4 つのラボを米国のオースティン (テキサス州) とジョージア (アトランタ州)、英国のハーズレー、オーストラリアのメルボルンに設置しています。これらのラボ内では、テスターが特定のハードウェア・デバイスを分解し、弱点を識別しています。テスターはハードウェアの構成とソフトウェアとの対話、そしてそれに関連する事柄を評価します。また、製品の目標を設定し、セキュリティー要件を作成し、脅威をモデル化して脆弱性を割り出します。そして、製品が市場に出る前にセキュリティーの欠陥を修正し、財務的な損失とブランドへのダメージを回避できるよう企業を支援します。

X-Force Red ポータル

X-Force Red ポータルでは、すべてのお客様がテスターと直接、手軽に、しかも安全に通信し、コラボレーションすることができます。このポータルはクラウド・ベースのプラットフォームで、お客様はこれを使用することにより、暗号化されたフォーム 1 つでテストを要請できます。お客様はこのポータルからテスターに直接コンタクトして、時間や内容を問わずに質問やコメントを送ることができ、メールや電話でのやり取りは不要です。

X-Force Red ポータルは、よりスピーディーかつリアルタイムの改善を可能にします。従来であれば、テスターはプロジェクトの終了後、1 週間から 2 週間かけてレポートを作成していました。このタイムラグはすなわちお客様の待ち時間であり、その間に新しい脆弱性が発生して、犯罪者に攻撃の時間を与えることにもなりかねません。テスターは X-Force Red ポータルを使用して、結果が特定されたタイミングでそれを提出するため、お客様には脆弱性を速やかに確認し、改善できる機会が与えられます。このポータルではテストの進捗と結果が 1 つのビューで提供されているため、お客様とテスターが状況を互いに伝え合うことができます。

ポータルに入力された対話式のレポートには、脆弱性に関する主な結果、悪用の証拠、優先順位の決定と改善のための詳しいガイダンスが含まれています。レポートをポータルに入力する際は、誰がその結果の閲覧権限を持つかをセキュリティー・リーダーが決定できるようになっています。レポートのセクションの一部を切り離し、関係者がそれぞれのスコープに含まれる脆弱性のみを確認できるよう設定することもできます。このプロセス全体を通して、その組織の修正を決定する主導権は常にセキュリティー・リーダーにあります。

X-Force Red ポータルは、お客様のすべてのレポートを保管する中央リポジトリーの役目を果たします。複数のテストを実行している組織は、すべてのレポートをリアルタイムでモニター、追跡、レビューできます。履歴レコードを取得して、これまでに見つかった欠陥と、行われた改良とを比較することができます。

このポータルは Secure Sockets Layer (SSL)、暗号化、2 要素認証などのセキュリティー管理機能も独自に備えています。

まとめ

セキュリティー侵害に端を発する訴訟、財務的な損失、ブランドのダメージの恐れが急激に高まる中、組織は何よりも貴重な資産を、先手を打って保護する必要に迫られています。IBM X-Force Red 侵入テスト・サービスを利用することで、お客様は重大な脆弱性を犯罪者に利用される前にそれらを特定し、修正できます。X-Force Red のテスターには、犯罪者と同じツール、手法、手順を使って欠陥を特定し、侵入を行ってきた数十年に及ぶ経験があります。X-Force Red のテスターは、攻撃者の発想で、これまで犯罪者に使われたことのない新しいセキュリティーの侵害方法を発見できます。X-Force Red 侵入テスト・サービスを使用して、インフラストラクチャー全体から重大な欠陥を探し、修正している組織は、セキュリティー対策の強化に役立つ管理能力を養い、常に犯罪者の一歩先を行くことができます。

詳細情報

侵入テストの詳細については、IBM 担当員または IBM ビジネス・パートナーにお問い合わせいただくか、**ibm.com/jp-ja/security/services/penetration-testing** をご覧ください。

日本アイ・ビー・エム株式会社
〒103-8510
東京都中央区日本橋箱崎町 19 番 21 号

Produced in Japan
2019 年 7 月

本資料の情報は最初の発行日の時点で得られるものであり、予告なしに変更される場合があります。すべての製品が、IBM が営業を行っているすべての国において利用可能なのではありません。

本書に含まれるパフォーマンス・データは、特定の動作および環境条件下で得られたものです。 実際の結果は、異なる可能性があります。 本書に掲載されている情報は特定物として現存するままの状態で提供され、第三者の権利の不侵害の保証、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されています。IBM 製品は、IBM 所定の契約書の条項に基づき保証されます。

お客様は自己の責任で関連法規を遵守しなければならないものとします。IBM は法律上の助言を提供することはいたしません。また、IBM のサービスまたは製品が、お客様がいかなる法規も遵守されていることの裏付けとなると表明するものでも、保証するものでもありません。

適切なセキュリティーの実施について: IT システム・セキュリティーには、企業内外からの不正アクセスの防止、検知、および対応によって、システムや情報を保護することが求められます。不正アクセスにより、情報の改ざん、破壊もしくは悪用や誤用を招くおそれがあり、またはシステムの損傷や、他のシステムに対する攻撃のための利用を含む悪用につながるおそれがあります。完全に安全と見なすことができる IT システムまたは IT 製品は存在せず、また単一の製品、サービスまたはセキュリティー対策が、不適切な使用またはアクセスを防止する上で、完全に有効となることもありません。IBM のシステム、製品、およびサービスは合法的で包括的なセキュリティーの取り組みの一部となるようにして設計されており、これらには必ず追加の運用手順を伴います。また、最大限の効果を得るためには、他のシステム、製品、またはサービスを必要とする場合があります。IBM は、何者かの悪意のある行為または違法行為によって、システム、製品、またはサービスのいずれも影響を受けないこと、またはお客様の企業がそれらの行為によって影響を受けないことを保証するものではありません。

1. X-Force Red 侵入テストの結果、2017 年 8 月から 2018 年 11 月まで
2. X-Force Red 侵入テストの結果、2017 年 10 月から 2018 年 11 月まで
3. X-Force Red ATM テストのプレゼンテーション、2018 年 11 月
4. X-Force Red 侵入テストの結果、2017 年 8 月から 2018 年 11 月まで

17023217JPJA-00