X-Force

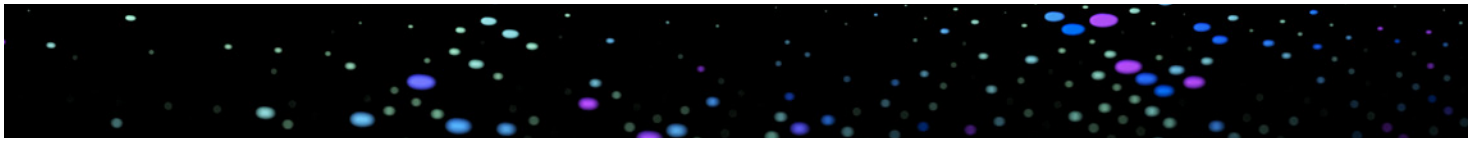
2021 IBM Security X-Forceインサイダー脅威レポート

IBM Security X-Force 脅威インテリジェンス

2021 年第 2 四半期スペシャル・インテリジェンス・レポート

IBM

目次



はじめに

サイバー脅威では、攻撃側と防御側が共に新しいテクノロジーとプロセスを取り入れて進化するため、その状況は絶え間なく変化しています。企業では、資産保護や、攻撃の防止とその対応のための人材確保に、年間約 600 億ドルを投入しており、2021 年にはセキュリティー・コストがさらに 10% 増加すると言われています。[1]

企業におけるセキュリティー対策では、外部からの攻撃を阻止することばかりに多額の費用が投入されており、社内関係者からの脅威は見落とされがちです。つまり、組織の内側から発生する脅威です。内部関係者による脅威の場合、悪意がなかったり、偶発的であったことが判明しても、データの窃盗、金銭的損失、知的財産の窃盗、風評被害といった形で壊滅的な損害を被る可能性があります。2020 年の調査において、Ponemon Institute 社は、インシデントの発生源にかかわらず、インサイダー脅威のインシデントから回復するために、企業は平均 644,852 ドルの費用が必要になると見積もっています。[2] これには、疑わしいインサイダー事案の監視と調査、およびインサイダー事案のインシデント・レスポンス、封じ込め、根絶、改善のためのコストが含まれます。

本ドキュメント内で、IBM Security X-Forceはインサイダーを以下のように定義しています。

- 偶発的なインサイダー：過失による行為をした従業員、または第三者であるベンダー/請負業者。[3]
- 悪意のあるインサイダー：犯罪者または悪意を持った従業員や 第三者であるベンダー/請負業者。

1. https://www.infosecurity-magazine.com/news/global-cybersecurity-spending-to/
2. https://securityintelligence.com/posts/gaining-insight-into-the-ponemon-institutes-2020-cost-of-insider-threats-report/
3. 過失によるインサイダーとは、組織内のデータやシステムの機密性、完全性、可用性に影響を与えるインシデントを偶発的に引き起こしたインサイダーとして定義されます。フィッシング/ソーシャルエンジニアリングのインシデントは含まれません。

X-Force は、実際のインシデント/レスポンス調査から入手した独自のデータを用いて、2018 年から 2020 年にかけて組織に影響を与えたインサイダー脅威の疑いがあるインシデント (偶発的なものと悪意によるものの両方) を分析しました。本ドキュメントでは、最も顕著なインサイダー脅威による攻撃に関するオープン・ソースのレポートと組み合わせて、そのデータから以下のような重要事項を検証します。

— 大部分のインサイダー攻撃を、どのように検出するか。

— インサイダー攻撃において、アクセス・レベルが果たす役割。

— インサイダー脅威を軽減するためのベスト・プラクティス。

主な調査結果

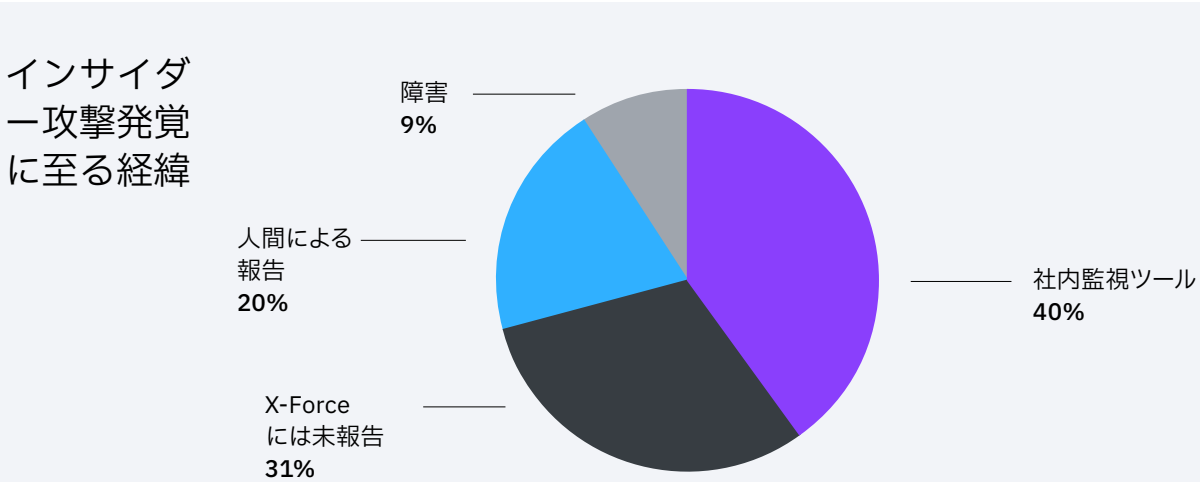
社内監視ツールによるアラートで、40%　のインシデントが検出されました。

インシデントの　40%　は、会社の資産へのアクセス権限を持つ従業員が関与しています。

内部関係者が管理アクセス権を持っている、または持っていると考えられるインシデントでは、100%　この特別なアクセス権が悪用されていました。

インサイダー攻撃発覚に至る経緯

インサイダー脅威とは、一般的に、企業の資産にある程度アクセスできる正規のユーザーが、悪意を持って、または偶発的にそのアクセス権を利用することで、最終的に組織に損害を与える攻撃と定義されています。このような脅威は、現従業員もしくは元従業員、あるいは特定のビジネス上の役割を果たすためにアクセス権を有している第三者の請負業者やベンダーから生じることがあります。



X-Force が 2018 年以降に対応したインサイダー脅威を分析したところ、その40%が内部監視ツールからのアラートによって検出されたことが明らかになっています。また、従業員が組織に対して異常を報告したような、社内からの通報が20%、システム停止によりセキュリティー・チームへ通報が届いたケースが 9%ありました。

2020 年のインサイダー脅威のコスト: ObserveIT と IBM の協賛による Ponemon Institute　社のグローバル・レポートでは、ユーザー行動分析　(UBA)、特権アクセス管理 (PAM)、セキュリティー情報およびイベント管理 (SIEM) などのツールや脅威インテリジェンスの共有、ユーザーのトレーニングと認知などのプログラムを取り入れることで、インサイダー・リスクの軽減または削減に効果が期待でき、平均 300 万ドルの節約が可能になると予測しています。[4]

300 万ドルのコスト削減

UBA、PAM、SIEMsなどのツールや、脅威インテリジェンスの共有、ユーザーのトレーニングや啓発といった対策により、インサイダー・リスクが軽減または削減され、企業にかかるコストも平均 300 万ドル削減されると推定されました。[4]

4. https://securityintelligence.com/posts/gaining-insight-into-the-ponemon-institutes-2020-cost-of-insider-threats-report/

X-Force の研究におけるエビデンスの欠如と未知の領域

発見方法が「X-Forceに報告されていない」または「証拠不十分」とされたインサイダー・インシデントについては、X-Forceのインシデント対応チームは発見に関する判断を下すのに十分な情報を得られていませんでした。これは、多くの組織において、ベースライン環境がどのようなもので、どのように運用されているのかが可視化されていないことが原因です。システム内の異常を検出するためには、正常なアクティビティーがどのようなものかを理解することが重要であり、そうすることで外れ値をより容易に、自信を持って検出することができます。2019 年、IBM は組織に対する高度な脅威の状況を調査した SANS のレポート[5] を提供しました。この調査では、以下が確認できました。

- 48% の組織が、インフラストラクチャーの可視化不足がセキュリティー上の最大の欠点だと認識していました。
- 35% の組織が、企業の内部関係者による不正使用を検出する能力が不足していると感じていました。
- 47% の組織が、ネットワーク内の通常のベースライン・アクティビティーがどのようなものかを理解する能力が不足していることを認めていました。

5. https://www.ibm.com/account/reg/us-en/signup?formid=urx-39989

特権アクセスと管理アクセス

X-Force　では、インサイダー脅威のインシデントを分析する際に、ユーザーを 2 種類に分けています。

特権ユーザーとは、企業内で機密データにアクセスできる人と定義されています。このデータは、知的財産、顧客データ、または人事情報である場合があります。このようなユーザーは、M&A　データやその他の法的情報など、機密性の高いビジネス情報にアクセスできる可能性もあります。

管理者権限を持つユーザーは、アドミニストレーターやアドミンとも呼ばれ、ネットワーク内の　IT　システムへの高いアクセス権限を持つ人として定義されています。理論上、このタイプのアクセスは重複することはありません。しかし、X-Force の調査では、IT 環境においてエンド・ユーザーがしばしばオーバー・プロビジョニングされている可能性が確認されています。

管理アクセス権を持つ内部関係者は、企業環境の機密アクセス権を持つ内部関係者とは異なります。こうした人には、企業の IT 環境にアクセスできる従業員、請負業者、ベンダーが含まれており、ネットワーク権限が高いことにより、企業に独自のリスクが生じることになります。

特権アクセスを持つ役職の例

- 人事担当
- 上級管理職
- 財務関連業務
- 法的業務
- 研究職
- その他、組織の知的財産、「重要部門」、またはお客様のデータにアクセスできる役職

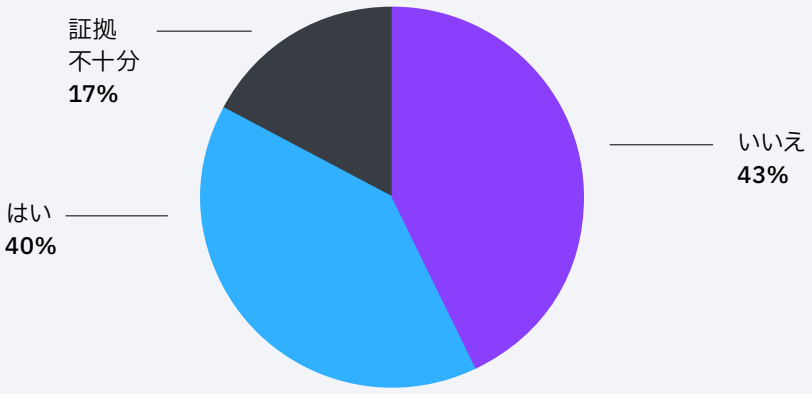
管理アクセス権を持つ役職の例

- サーバー管理者
- IT 管理者
- ヘルプ・デスク
- 第三者の IT ベンダー
- その他、IT システムの構成/設定を変更できる役職

ウォッチャーを監視しているのは？

インシデントを起こす内部関係者は、通常、特権的なアクセス権を持っているのでしょうか。答えは「はい」です。

内部関係者はデータへの特権アクセス権を持っていたのでしょうか。



X-Force のデータ分析によると、内部関係者が引き起こしたインシデント のうち 40%　は、会社の機密資産への特権アクセスを持っている従業員が関与していることが明らかになっています。
今回の X-Force 調査では、IT 部門、人事、財務、セキュリティーなどの分野や管理職として働く人々に特権アクセスがあることが判明しました。

内部関係者が機密データへ特権的にアクセスできたかどうかが不明である割合が 17%　もあり、特権アクセスを持つユーザーによるインシデントの数は大幅に増加する可能性があります。

ネットワーク共有、セキュリティー機器、Eメール・システム、従業員や顧客の個人識別情報　(PII)、知的財産、財務データなどの重要な資産への特別なアクセス権を持つユーザーは、より限定的な権限を持つユーザーよりも、インシデント関与のリスクが高まる可能性があります。

そうだとすると、特権アクセスを持つ内部関係者が引き起こす偶発的なインシデントの方が、アクセス権のレベルが低い内部関係者が引き起こす偶発的なインシデントよりも、組織の損失が大きくなるのは当然といえるでしょう。より高度な特権的アクセスを持つ悪意のある内部関係者　が関与するインシデントは、さらに重い代償を伴うことになり、これらのユーザーが関与するインシデントは、大規模なデータ侵害に発展してしまう可能性があります。例えば、2018　年には、地元有数の代理店に勤務していたオーストラリアの不動産業者が、この代理店を辞める前に機密データベースにアクセスしたことが発覚しました。システム内で、見込み客の関心度を下げるなど、販売見込みのレベルを操作していました。さらに、新しい代理店で契約を取るために、200 件以上のお客様の記録が持ち出されていたと、同代理店が報告しています。このインサイダー攻撃により、被害を被った代理店の見込み不動産売却額は 3,000 万ドル に上ると推定されました。[6]

アクセス・レベルに関わるインサイダー・インシデントを防止する最善策の一つは、最小権限の原則を遵守し、ユーザーが組織に対して職務を遂行する上で必要最小限のアクセス権のみを付与するようにすることです。これは、ゼロ・トラスト・モデルを中心に構築されるような特権アクセス管理 (PAM) ソリューションの形として提供されることがあります。[7,8]　このモデルでは、ユーザー・アカウントを持つすべての人に可能な限り最小限のアクセス権のみを与え、内部関係者がデータや資産に意図しない形でアクセスする可能性を低減することを目指します。より多くのデータが存在し、人と人以外のリクエスターの両方が運用し、アクセスする必要があるクラウドでは、このコンセプトがさらに重要になります。

2020 年 インサイダー脅威によるコスト：グローバル・レポートによると、組織で何らかの形で特権的アクセス管理を採用している企業は、わずか 39% に過ぎないことが分かっています。[9] さらに、PAM の採用により 310 万ドルのコスト削減を実現しており、この手法の高い有効性が示されています。

39%

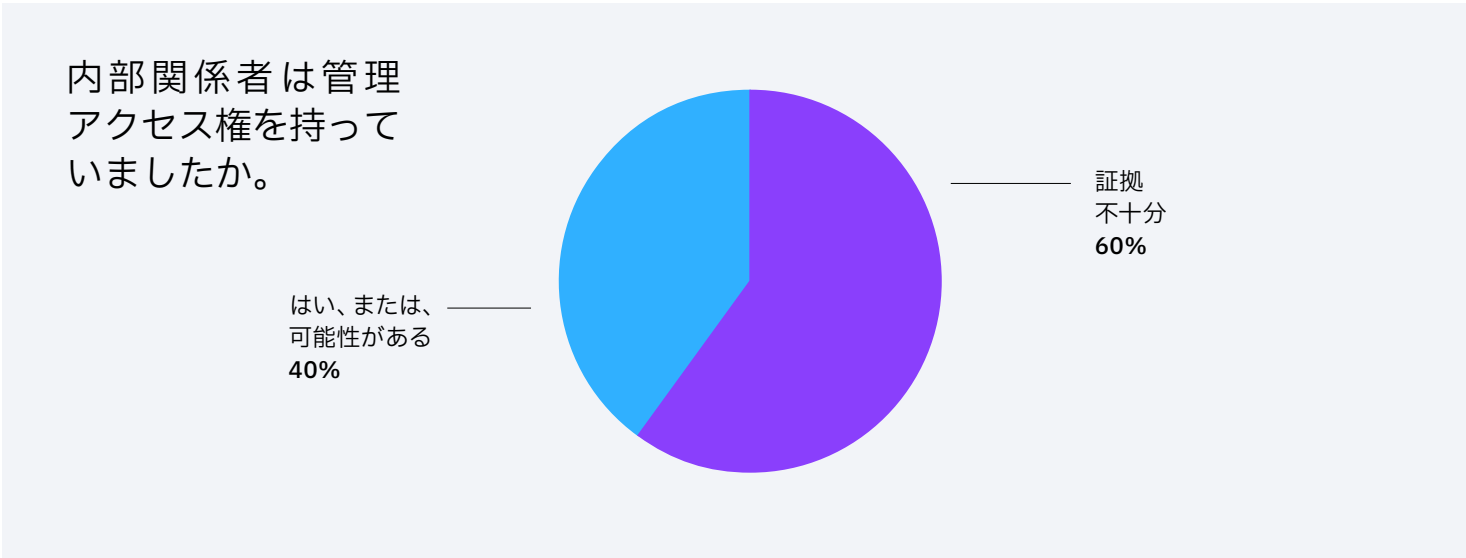
何らかの形で PAM を自社に導入している企業は、39% に上ります。[9] この導入により、コストが 310 万ドル削減されました。

6. https://indaily.com.au/news/2018/10/23/harris-director-resigns-from-top-real-estate-post/
7. https://www.ibm.com/security/identity-access-management/privileged-access-management
8. https://www.ibm.com/security/zero-trust
9. https://www.ibm.com/security/digital-assets/services/cost-of-insider-threats/

管理アクセス権の乱用はコストがかかります

組織の管理者である内部関係者が権限を乱用し、復讐、金銭的な利益、またはその他の悪意ある意図で利用する例が数多く報告されています。2020 年 2 月、マイクロソフトの元エンジニア、Volodymyr Kvashuk が、特権的アクセスを悪用して、同社から 1,000 万ドル以上のデジタル資産を盗んだとして有罪になっています。[10] Kvashuk は、自分が管理を担当していた小売販売プラットフォームの管理アクセス権を持っていたため、盗難が行われてしまったのです。[11] Kvashuk は、同僚のEメール・アドレスとシステム上の有効なテスト・アカウントを使用して、デジタル・ギフト・カードを流出させるなど、アクティビティーを混乱させました。盗んだこれらのギフト・カードやその他の資産をインターネット上で転売して個人的に利益を得ており、その後、その利益で 160 万ドルの自宅と 16 万ドルのテスラ車を購入していました。[12]

数字で見る管理アクセス権の乱用



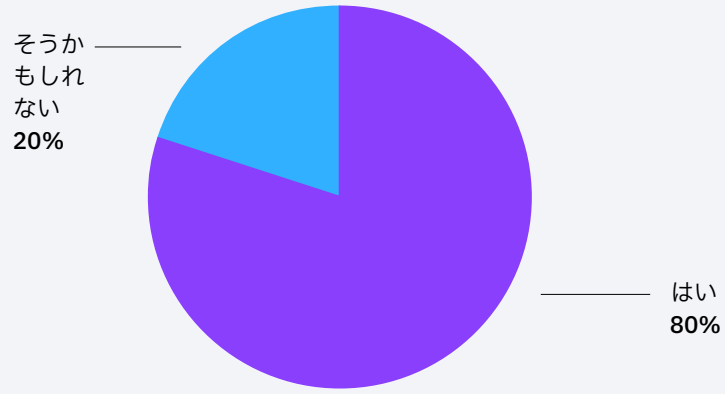
2018 年から 2020 年にかけて X-Force が対応したインシデントのうち 40% において、内部関係者がネットワークへの管理アクセス権を持っていると確認された、あるいはその可能性が高いことが判明しています。X-Force のアナリストは、お客様からユーザーの具体的な役職が知らされていない場合、各インシデントの詳細情報に基づいてインサイダー・アクセスの種類を判断しました。

10. https://www.justice.gov/usao-wdwa/pr/former-microsoft-software-engineer-sentenced-nine-years-prison-stealing-more-10-million
11. https://apnews.com/article/seattle-retail-sales-james-robart-13f5a86053533b40034246ef37ecad8d
12. https://www.redmond-reporter.com/news/former-microsoft-employee-convicted-of-18-federal-felonies/

これらのインシデントには、データの流出、機密データの漏洩および削除、不正なソフトウェアのインストールなどが含まれていました。具体的には、管理アクセス権を持つ内部関係者の犯行により、サーバーから削除されたペタバイトのログが失われたり、意図的にソース・コードを流出させたり、損害額の大きなシステム停止に見舞われている組織があります。

さらに興味深いことに、管理アクセス権を持っている内部関係者の犯行であることが確認されたり、その可能性が高いインシデントでは、100% この特別なアクセス権が悪用されていました。(下のチャートを参照してください)

インサイダー・インシデントには、特別なネットワーク・アクセス権が関連していたのでしょうか。



言い換えると、もし内部関係者が管理アクセス権を持っていなければ、インシデントが組織に与える影響ははるかに少なかったか、多くの場合、まったく発生しなかった可能性が高いということです。X-Force では、サーバーから重要なデータベースやログが削除されるようなインサイダー・インシデントに何度も対応してきました。内部関係者がこれらのシステムへの管理アクセス権を持っていなければ、これらのインシデントは起こらなかったでしょう。

推奨事項

X-Force では、第三者機関のデータにおけるインサイダー・インシデントの発生件数が過小評価されていると考えています。この種のインシデントは、組織内で処理され、責任や風評被害を恐れて公表されないものが、まだ多くあるためです。[13]

X-Force の調査とデータは、これらのインシデントが組織に与える影響に基づき、潜在的なインサイダー脅威を情報セキュリティー・プログラムの重要な要素として位置づける必要があることを強調しています。IBM Security では、インサイダー脅威に関して具体的に以下のことを推奨しています。

インサイダー脅威を検出するためには、深層防護戦略が有効です。

従来、外部からの脅威に対しては、企業が導入する技術やプロセスへの多層的アプローチが検討されてきました。しかし、X-Force の調査によれば、セキュリティー情報およびイベント管理 (SIEM) ソリューションをはじめとする、こうしたツールの多くは、インサイダー脅威の行為を検出する上でも極めて重要であったことが示されています。

ご使用の環境で、どのような状態が正常であるかを把握しておいてください。

あらゆる種類の攻撃者からの不審な行為を検知する最善策は、ネットワーク内ではどのような行為が正常とされているかを把握しておくことです。ベースライン・アクティビティーをしっかりと理解しておくことで、異常な行動を迅速かつ効果的に検出し、対応することが容易になります。堅牢なユーザー行動分析 (UBA) ソリューションは、このような機能を提供し、時間の経過とともに変化する環境に順応できます。

管理アクセス権を定期的に見直してください。

X-Force では、管理者が関与するインサイダー・インシデントの幾つかが、過剰な特権を持つユーザーによるものである可能性が高いことを突き止めました。ミッション・クリティカルなサーバーの管理アクセス権については特に、厳格な変更およびプロセス管理を実施する必要があります。機密性の高いシステムや機能への一時的な管理アクセスを記録、許可する技術ソリューションを検討してください。

13. https://www.darkreading.com/edge/theedge/fbi-encounters-reporting-an-insider-security-incident-to-the-feds-/b/d-id/1340016

情報セキュリティー・チームと IT 管理チームを分離します。

X-Force の経験から、セキュリティー・チームと管理チームの独立性とガバナンスを管理する上でバランスの取れたアプローチがあることで、より優れたセキュリティーを実現できることが証明されています。また、管理チームが、必要な柔軟性と創造性を持ち合わせることで、正確なリスク調査と検出を実施できます。それにより、チーム内のリスクが軽減され、社内で十分な監督と監視を実行することができます。

機密性の高い組織の役割について、リスク・プロファイルを構築します。

X-Force が対応したインサイダー・インシデントでは、高いアクセス権が鍵となっているため、組織内でシステムやデータへの機密アクセスや管理アクセスを持つ役職については、リスク・プロファイルを作成することをお勧めします。ゼロトラスト・モデルを中心に構築された特権アクセス管理 (PAM) ソリューションを導入し、ユーザーに対して最小限の特権アクセスのみを与えることで、インサイダー・インシデントの発生を最小限に抑えることができます。

インシデント対応プレイブックを更新し、インサイダー脅威を含めます。

このようなインシデントの場合、通常のトレーニングでは不十分です。ほとんどのインシデント対応プレイブックでは、外部からの攻撃が原因であるとしていますが、偶発的な、または悪意のあるインサイダー脅威のシナリオを含めることを検討する必要があります。サイバー攻撃への備えと対応を強化するために、インシデント対応計画や個別の攻撃プレイブックを開発できるパートナーを検討してください。

継続的に社員のトレーニングを実施してください。

ほとんどの組織の年間トレーニング・プログラムには、ソーシャル・エンジニアリングのトレーニングと並んで、倫理的なビジネス慣行が含まれています。X-Force が対応したインサイダー・インシデントの多くは、テクノロジーではなく、他の従業員によって発見されたものでした。内部関係者によるインシデントの疑いがある場合、その報告方法を、毎年のビジネス倫理やソーシャル・エンジニアリングのトレーニングに取り入れることをお勧めします。また、特権的アクセスを持つ従業員に、役割に応じたトレーニングを受けてもらうことで、周囲の異変やその兆候への意識が高まるでしょう。

評価の高い脅威インテリジェンス・サービスを活用してください。

ほとんどのお客様は、脅威インテリジェンスの作成、管理、運用に課題があると感じています。脅威インテリジェンスを大規模に運用するために必要な集約、自動化、統合を実現するソリューションの導入をご検討ください。

マネージド検知レスポンス・サービスにより、24時間体制の保護が可能となります。

マネージド検知レスポンス・サービス　(MDR)　セキュリティー・サービスは、インサイダー脅威の予防、検知、迅速な対応を提供するために不可欠なものです。従来の保護にとどまらず、行動ベースのブロック、調査、継続的なポリシー管理など、次世代 AV を使用したソリューションが重要な鍵となります。

非常に複雑で重要な環境を外部および内部の脅威から保護するために、IBM　Security　が、どのようにお客様をサポートしているかをご覧ください。

IBM Security についての詳細を見る

IBM Security

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 -21

米国で制作
2021 年 5 月

IBM