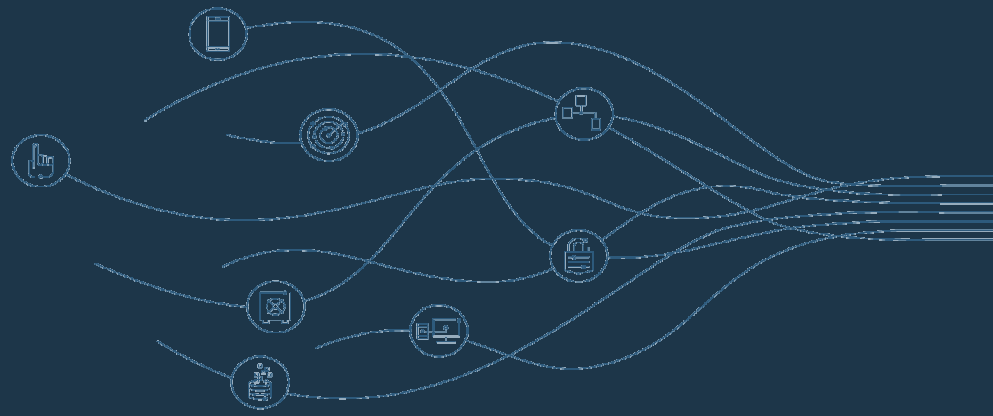
IBM Japan Security Forum 2017

IBM Security

セキュリティー事故対策は事前が肝心
IBM X-Force IRISを徹底解剖



日本アイ・ビー・エム株式会社
X-Force IRIS担当部長
徳田敏文

IBM

セキュリティー事故（インシデント）に対する事前対策に必要な要点

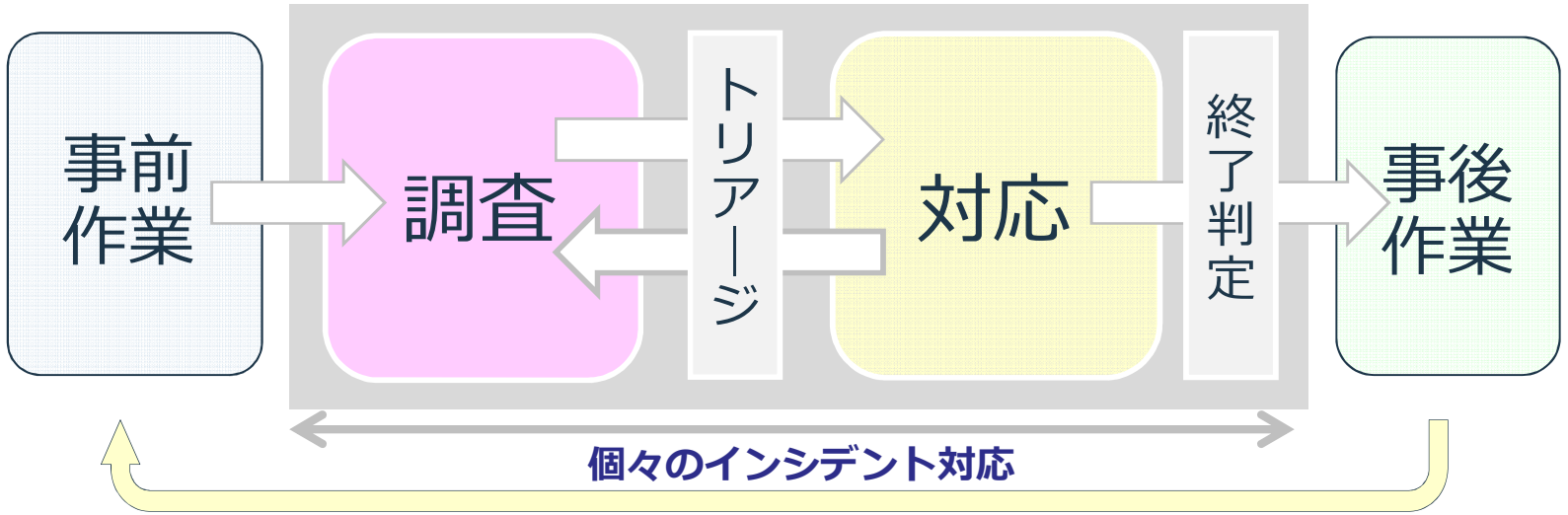
- セキュリティー設定、ログ取得の設定を行うこと
- イベントの収集・監視を行う仕組みの構築
- インシデント対応態勢の確立（組織、連絡体制の確保、メンバーの確保）
- インシデント対応手順の作成・見直し

コンピューターにおけるインシデントの特徴

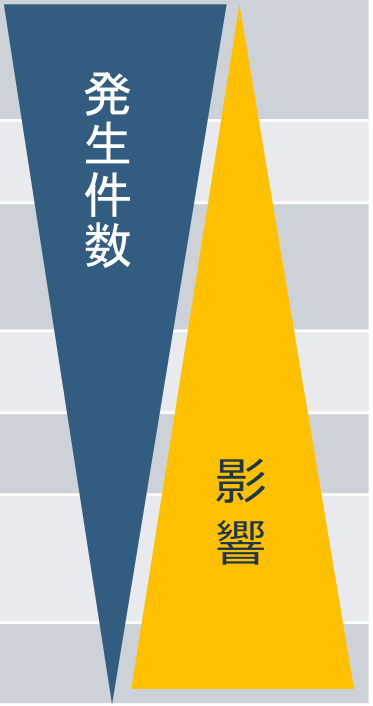
物理的なインシデントであれば、何らかの痕跡が残る可能性があり、科学的な調査で検出できる可能性があるが、コンピュータの場合には、データが時間の経過や再起動などを通じて消去または上書きされてしまう。

セキュリティーインシデント対応の手順

- インシデント・ハンドリング・プロセスの一般例



セキュリティーインシデント対応例

事故事象	被害例	規模
メール経由によるマルウェアへの感染	外部不審サーバーとの通信発生（C2通信等）	
ランサムウェアなどによる局所被害	職員端末および業務データの喪失	
WEB改ざん等による被害	マルウェアの組み込み、WEBシステムからの情報漏えい	
マルウェア大規模感染	情報系システムの停止	
遠隔操作ウイルスによる情報漏えい	機密情報が外部へ漏えい	
内部犯行による被害	情報の持ち出し漏えい、システムや情報の破壊	
基幹システム、制御系システムへの被害	クローズドネットワークへの侵入	

脅威・リスクは存在し成長する中、対応は後手に回りがち

- 従来からのセキュリティーに関する考え方は、「受動的(Reactive)」であり、「能動的(Proactive)」ではない
- 多くの組織は、事件・事故が起きてからセキュリティーリソースを投資するという状況
- 段階的に投資して強化していく流れになっておらず、　グローバル対応を含めて、脆弱な部分が放置されてきている

「事故が発生してから対応」の考え方が中心・・・か

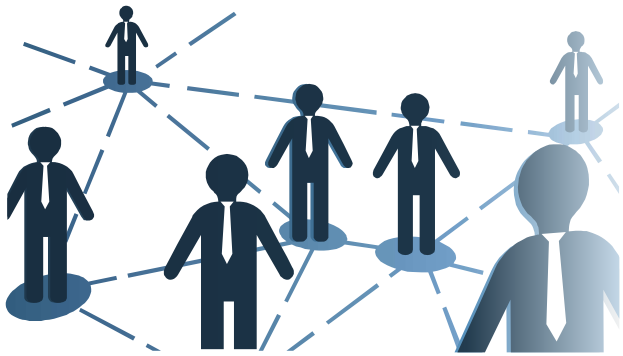
IBM X-Force Incident Response and Intelligence Services　(X-Force IRIS)

IBM エックスフォース　インシデント　レスポンス & インテリジェンス　サービス　（エックスフォース　アイリス）

- 「受動的（Reactive）な対応」から「能動的（Proactive）な対応」への変革を支援

- グローバルワイドのインシデント対応支援

- 熟練した専門家を世界レベルで情報共有しながら増強



IBM X-Force Incident Response and Intelligence Services　(X-Force IRIS)

IBM エックスフォース　インシデント　レスポンス & インテリジェンス　サービス　（エックスフォース　アイリス）

X-Forceメンバーが常勤

セキュリティー分野での研究開発体制（X-Force）

リサーチセンター:	9拠点
特許取得件数:	3,000件以上
年間投資額:	15億ドル以上
セキュリティーエンジニア:	約6,000名

IBM セキュリティー・オペレーション・センター（SOC）

監視拠点 SOC:	8拠点
サービス提供国:	133カ国
顧客数:	約4,000社
監視機器数:	約20,000台

IBM X-Force Incident Response and Intelligence Services　(X-Force IRIS)

IBM エックスフォース　インシデント　レスポンス & インテリジェンス　サービス　（エックスフォース　アイリス）

- **X-Force IRIS Vision Retainer（インシデント・レスポンス支援サービス）**
  コンピューター・セキュリティー・インシデント発生時に、的確かつ迅速なインシデント対応を行い、被害の拡散を防ぎ、早急に復旧することでお客様業務および全体ビジネス、ブランドイメージへの影響を極小化するための支援を提供します

- **Active Threat Assessmentサービス**
  独自の診断手法を利用して、既存のアンチウィルスやパーソナルFirewallなどでは対応できない未知のマルウェアを想定した攻撃の成功の可否（痕跡）を検査します

- **Incident Response Planningサービス**
  インシデント発生時に的確かつ迅速なインシデント対応を行うための、対応計画の構築を支援します
  （※日本では2018年以降展開予定）

- **Cyber Security対応Trainingサービス**
  CSIRT研修サービス　：　CSIRT概要、インシデント対応の概要をインシデント対応の専門家が教示します

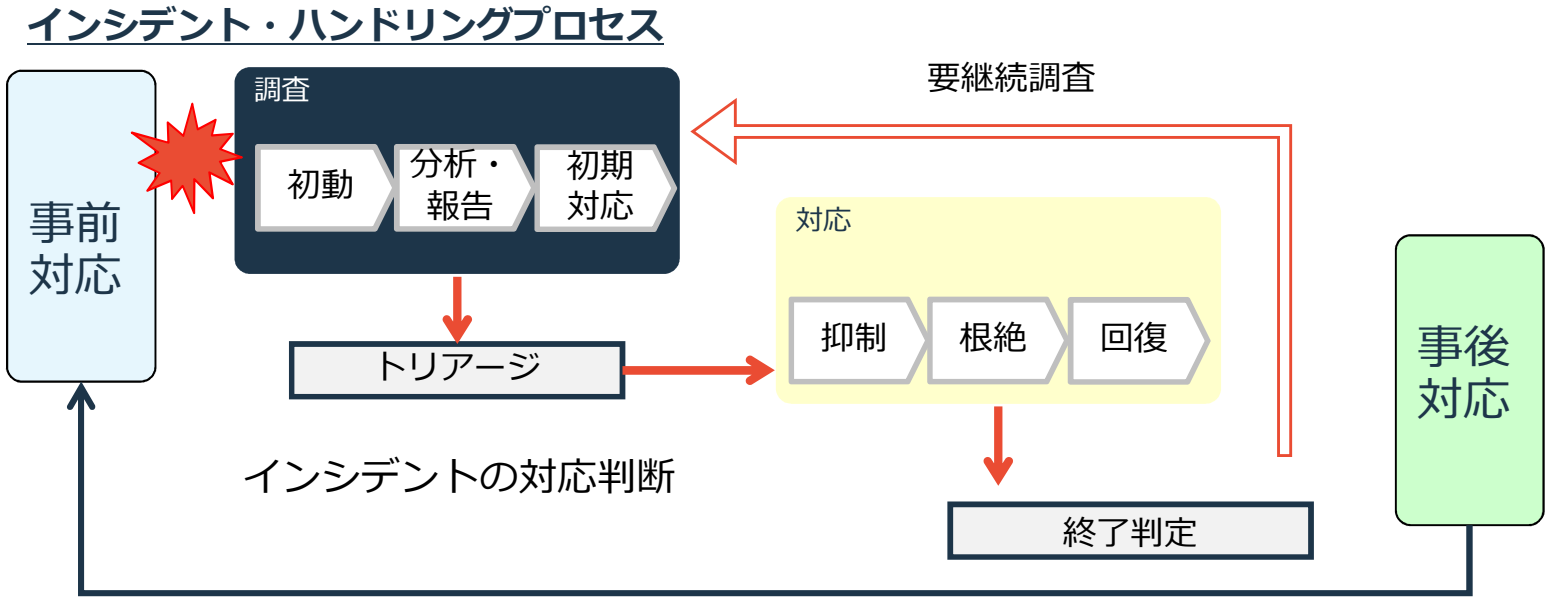
IBM X-Force IRIS Vision Retainer

エックスフォース　アイリス　ビジョンリテーナー

IBM X-Force IRIS Vision Retainer（インシデント・レスポンス支援サービス）

エックスフォース　アイリス　ビジョンリテーナー

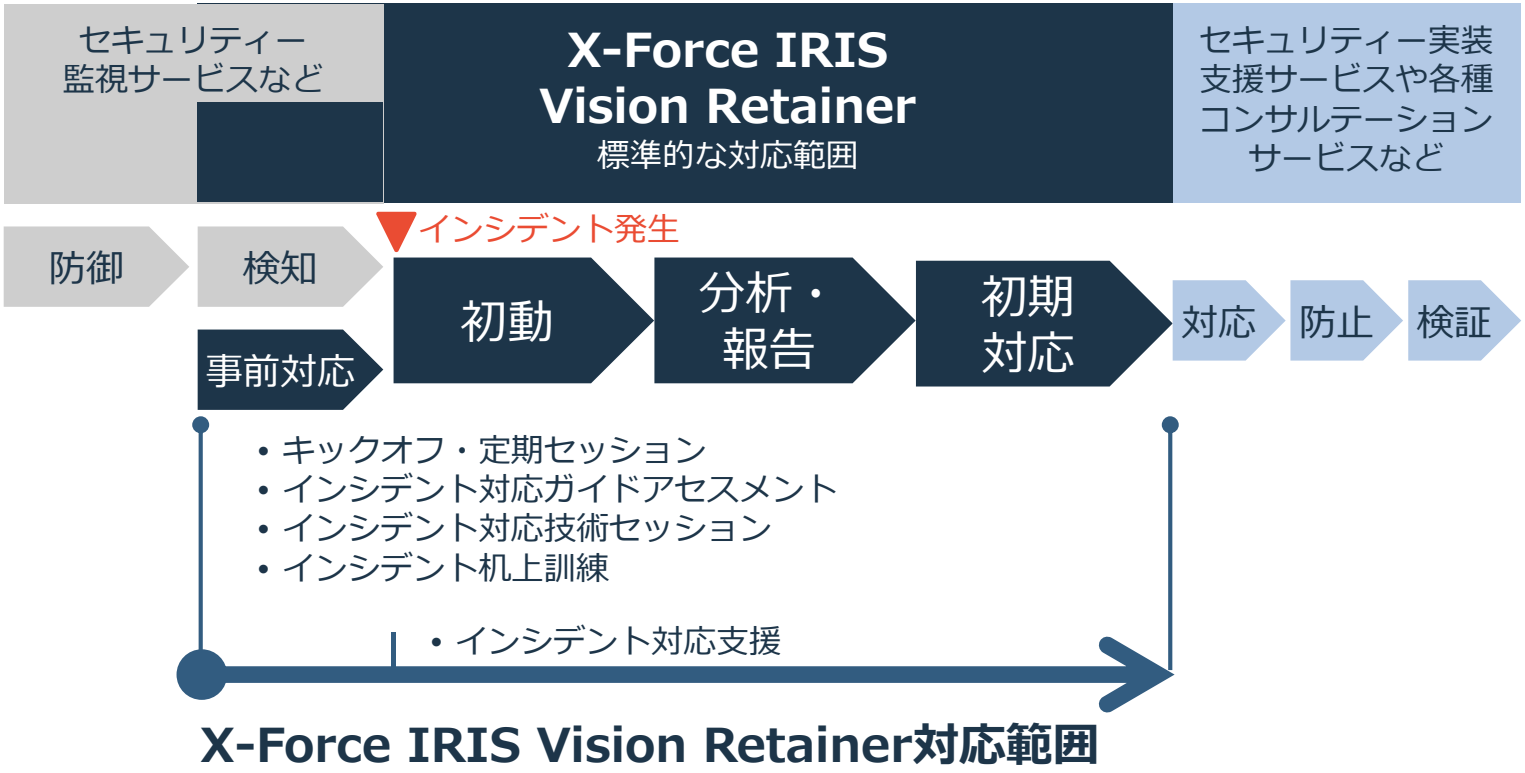
IBM X-Force IRIS Vision Retainerは、お客様で発生するセキュリティーインシデントに対して、事前の対応から、インシデント発生時の初動・分析・対応・報告等の様々な局面においてIBMの専門家が支援し、お客様業務およびブランドイメージへの影響を極小化することを目指します。インシデント発生の際を想定した机上訓練など事前の「Proactiveな」対応の支援や、日本国外への対応も提供いたします。



IBM X-Force IRIS Vision Retainerのサービス概要

エックスフォース　アイリス　ビジョンリテーナー

IBM X-Force IRIS Vision Retainerは、事前の年次契約をもとに、事前の準備対応とインシデント発生時には初動対応・分析・報告・初期対応作業の支援を事前定義された時間数に基づき提供します。その後の対応や防止策の実施・検証の提供が可能です。



IBM X-Force IRIS Vision Retainerの内容 ① 標準の事前セッション

エックスフォース　アイリス　ビジョンリテーナー

キックオフではインシデント対応支援要請の手順を双方で確認します。
定期セッションでは、キックオフで定義された情報の更新や確認を行い、インシデント対応をお客様と円滑に実施するための準備を行います。

事前セッション

初回会議（キックオフ）

- サービス内容の詳細についてご説明
- インシデント対応支援を要請するための手順を確認
- インシデント対応支援に向けたディスカッション

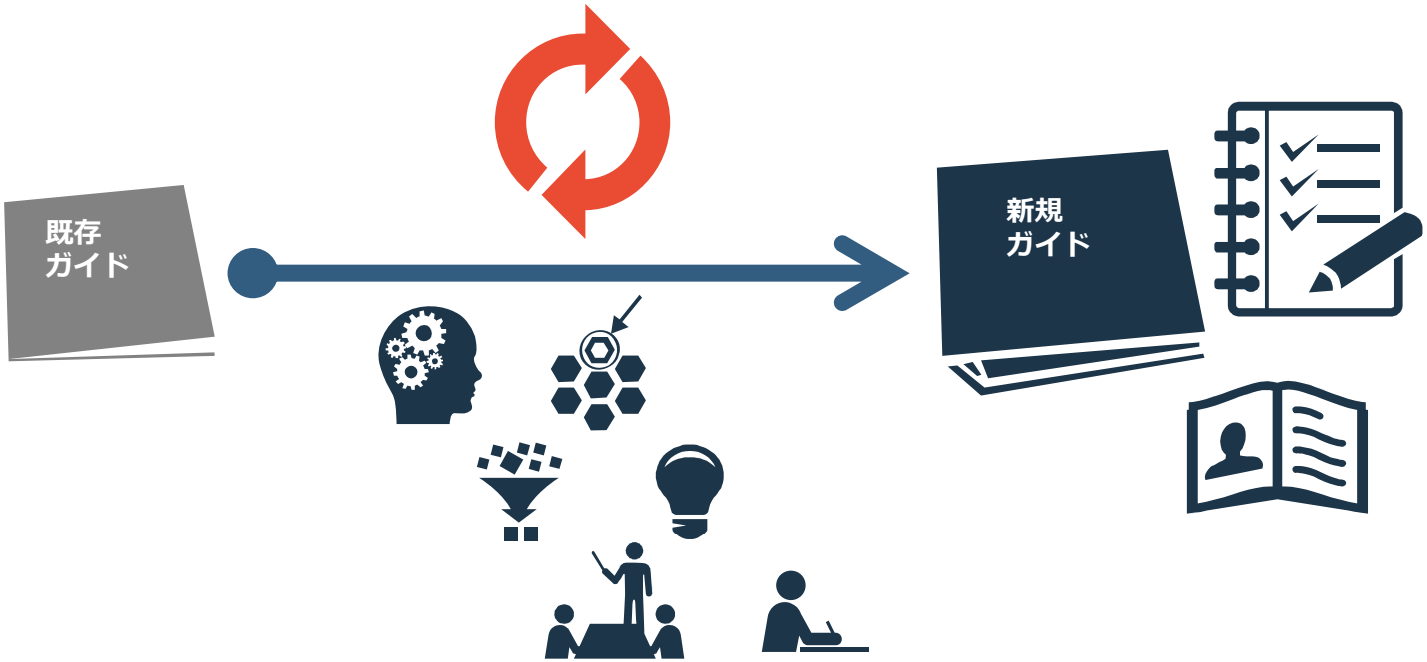
定期セッション

キックオフで定義・確認されたインシデント対応の連絡手順や連絡先など、お客様とIBM間で必要な基本情報や、お客様のシステム環境情報などを確認し必要に応じて更新します。インシデント発生時の連携に支障がなく、スムーズに対応が進められることを確認します。

IBM X-Force IRIS Vision Retainerの内容 ② インシデント対応ガイドアセスメント

エックスフォース　アイリス　ビジョンリテーナー

インシデント対応用に事前作成されているガイドを、IBMのインシデント対応プロフェッショナルの知見を持ってアセスメントいたします。より的確なガイドとなることを目指し、最適な初動が実施できることを目的とします。



IBM X-Force IRIS Vision Retainerの内容 ③ インシデント対応技術セッション

エックスフォース　アイリス　ビジョンリテーナー

インシデント対応において想定される技術的な懸念や疑問を解消し、的確な初動実施を妨げる恐れのある事柄を、可能な限り事前に払拭します。セッションは、IBMのインシデント対応プロフェッショナルが参加し、その経験に基づいた知見を持ってアドバイスを提供します。より的確な初動対応が実施できることを目的とします。

セッションの内容事例:

- 事例分析
- フォレンジック解析に必要なデータ取得
- マルウェア感染の初期分析
- マルウェア動作の確認実習
- インシデントハンドリング講義
- サイバー関連法に関する講義

IBM X-Force IRIS Vision Retainerの内容 ④ インシデント対応机上訓練

エックスフォース　アイリス　ビジョンリテーナー

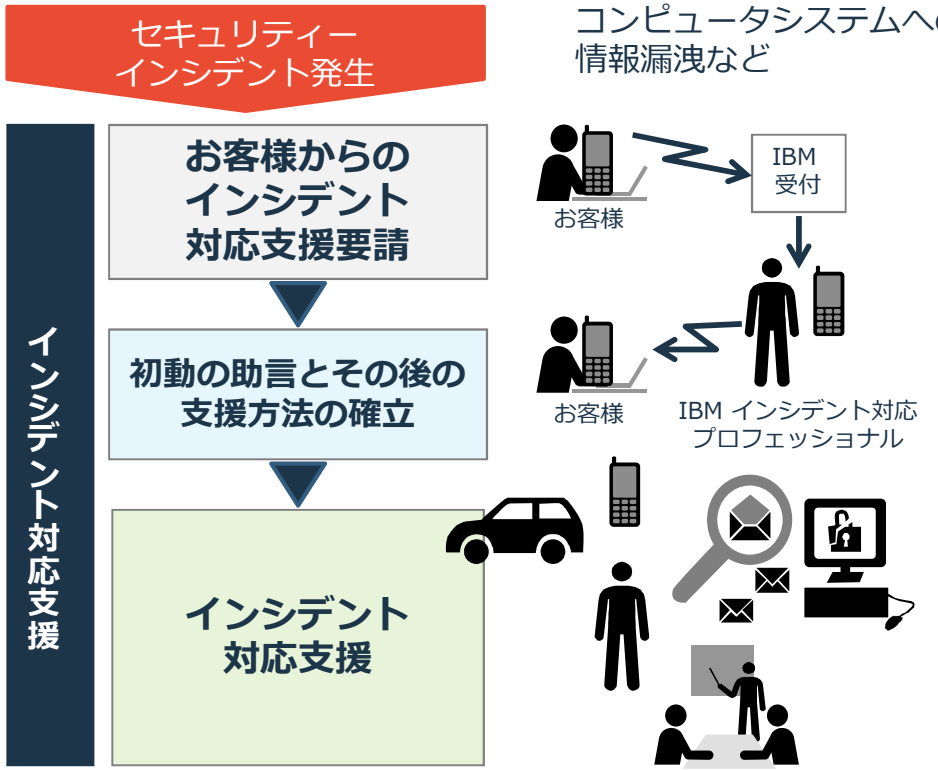
インシデント対応机上訓練では、実際の攻撃が発生する前に、想定シナリオに基づいたインシデント対応プロセスの確認を実施し、連絡態勢や初期対応の手順の見直しを図ります。これにより、インシデント発生時の対応をより的確なものにし、被害の最小化と対応時間の短縮を目指します。事故を経験せずに企業の「対応力・回復力(Resiliency)」を向上させます。

- CSIRTメンバーを中心にシナリオに基づいたインシデント対応を机上にて実践します
- CSIRTメンバーは、攻撃によって受けるビジネス上の被害をインシデント対応プロセスのなかで体験し学習します
- プロセスやガイドの改善のための推奨事項についてディスカションします

IBM X-Force IRIS Vision Retainerの内容 ⑤ インシデント対応支援

エックスフォース　アイリス　ビジョンリテーナー

お客様からのご要請に基づき、IBMインシデント対応プロフェッショナルによるインシデント対応支援を提供します。インシデントの内容や状況に応じてリモートまたはオンサイト含め、その時点での最適な対応を実施します。

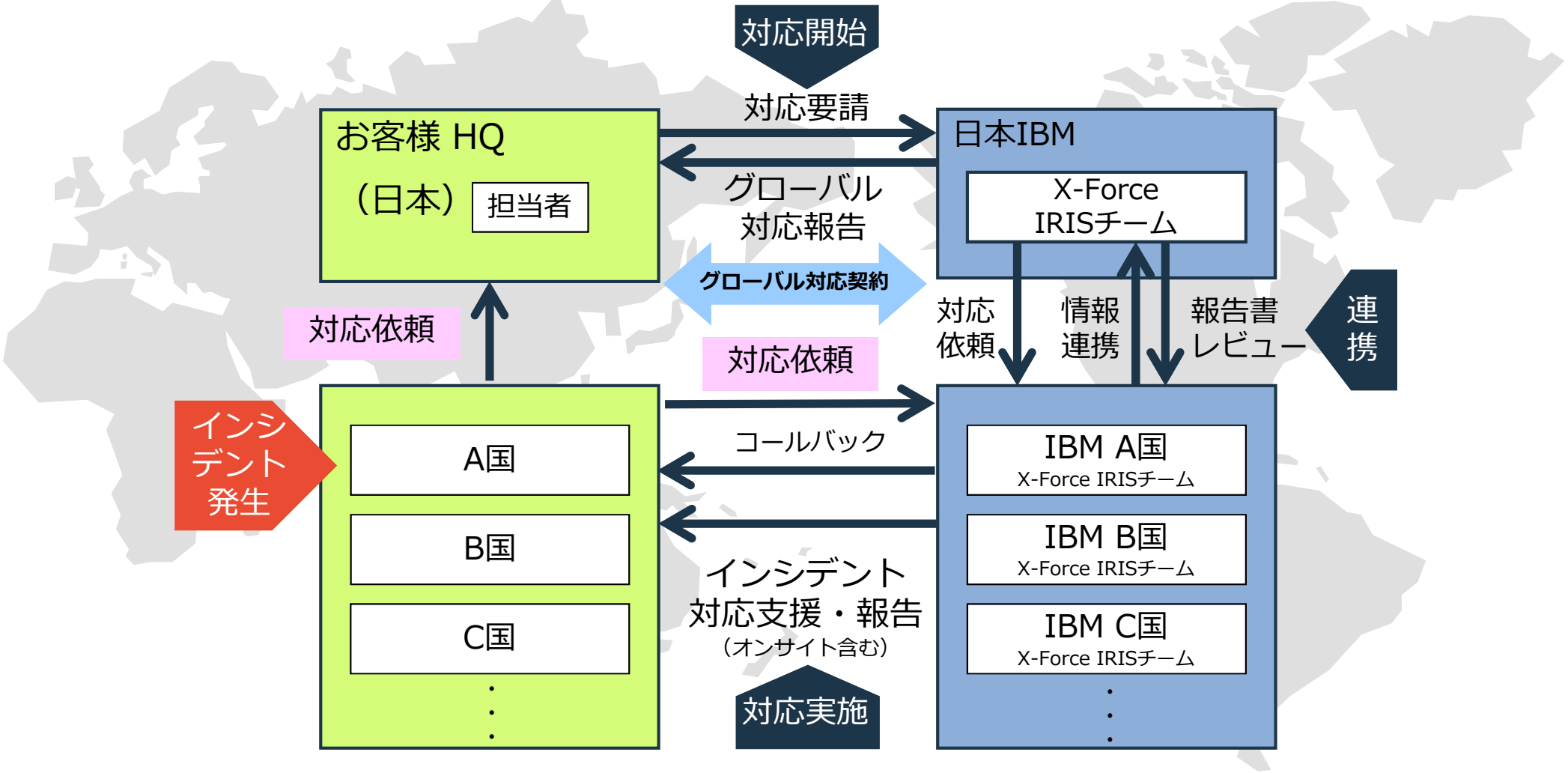


コンピュータシステムへの不正侵入、コンピュータウイルス・マルウェアの感染、
情報漏洩など

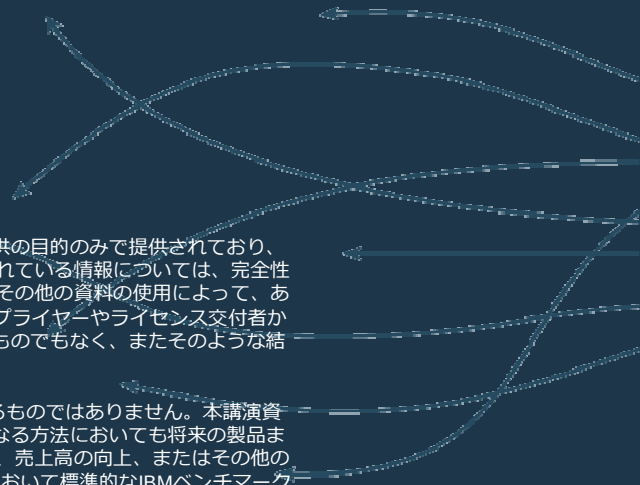
1. お客様からインシデント対応支援要請の連絡を受付。
2. インシデント対応支援を行うIBMプロフェッショナルよりコールバックし、電話による状況確認および初動の助言を行い、現地訪問を含めた対応について時間も含めてお客様と相談・確立します。
3. 契約時に定義した物理的所在地にIBMインシデント対応プロフェッショナルが訪問またはリモートによりインシデント対応支援を行います。
4. インシデントの状況に応じて、その時点で最適な対応を実施します。

IBM X-Force IRIS Vision Retainerのグローバル対応

エックスフォース　アイリス　ビジョンリテーナー



IBM Security



ワークショップ、セッション、および資料は、IBMまたはセッション発表者によって準備され、それぞれ独自の見解を反映したものです。それらは情報提供の目的のみで提供されており、いかなる参加者に対しても法律的またはその他の指導や助言を意図したものではなく、またそのような結果を生むものでもありません。本講演資料に含まれている情報については、完全性と正確性を期するよう努力しましたが、「現状のまま」提供され、明示または暗示にかかわらずいかなる保証も伴わないものとします。本講演資料またはその他の資料の使用によって、あるいはその他の関連によって、いかなる損害が生じた場合も、IBMは責任を負わないものとします。 本講演資料に含まれている内容は、IBMまたはそのサプライヤーやライセンス交付者からいかなる保証または表明を引きだすことを意図したものでも、IBMソフトウェアの使用を規定する適用ライセンス契約の条項を変更することを意図したものでもなく、またそのような結果を生むものでもありません。

本講演資料でIBM製品、プログラム、またはサービスに言及していても、IBMが営業活動を行っているすべての国でそれらが使用可能であることを暗示するものではありません。本講演資料で言及している製品リリース日付や製品機能は、市場機会またはその他の要因に基づいてIBM独自の決定権をもっていつでも変更できるものとし、いかなる方法においても将来の製品または機能が使用可能になると確約することを意図したものではありません。本講演資料に含まれている内容は、参加者が開始する活動によって特定の販売、売上高の向上、またはその他の結果が生じると述べる、または暗示することを意図したものでも、またそのような結果を生むものでもありません。 パフォーマンスは、管理された環境において標準的なIBMベンチマークを使用した測定と予測に基づいています。ユーザーが経験する実際のスループットやパフォーマンスは、ユーザーのジョブ・ストリームにおけるマルチプログラミングの量、入出力構成、ストレージ構成、および処理されるワークロードなどの考慮事項を含む、数多くの要因に応じて変化します。したがって、個々のユーザーがここで述べられているものと同様の結果を得られると確約するものではありません。

記述されているすべてのお客様事例は、それらのお客様がどのようにIBM製品を使用したか、またそれらのお客様が達成した結果の実例として示されたものです。実際の環境コストおよびパフォーマンス特性は、お客様ごとに異なる場合があります。

IBM