HITACHI
Inspire the Next

インシデント発生時の対応支援

MDRサービス インシデントレスポンス

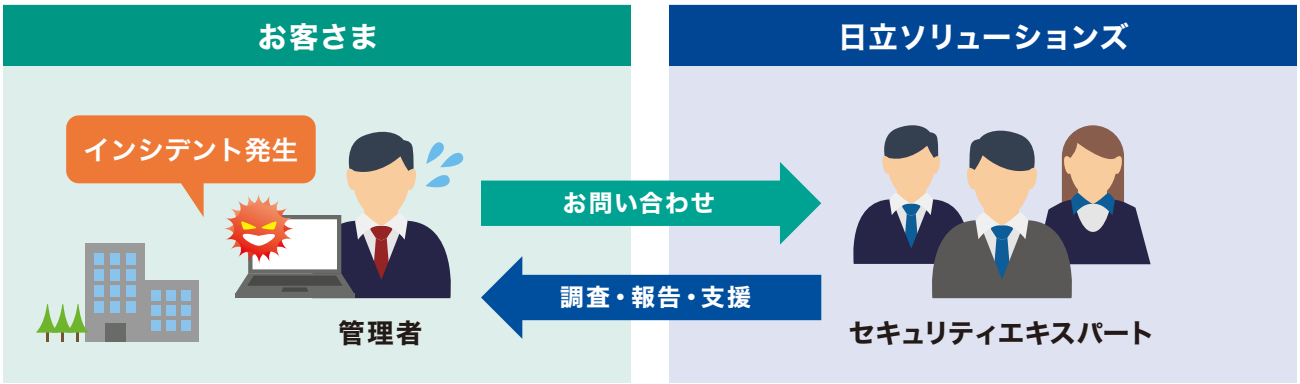
情報漏洩やマルウェア感染、不正アクセスなどのセキュリティインシデント発生時、
被害の拡大を防ぐためには、インシデント状況の把握から被害範囲の特定や対応方針の決定まで、
早急かつ適切な初動対応を行うことが重要です。
しかし、企業によってはセキュリティ人材が不足していたり、十分なインシデント対応スキルが
ないことから、被害がさらに深刻な状況になってしまうケースもあります。
MDRサービス インシデントレスポンスは、高度なセキュリティ知識を持つ専門家が、
お客さまのインシデント対応を支援、被害の拡大を防止します。

課題❶
インシデント発生時の対応体制やスキルに不安がある

課題❷
マルウェアによる被害範囲を把握したい

課題❸
情報の不正流出がないか調査したい

インシデント発生時の対策立案から被害状況の調査までセキュリティエキスパートが支援



早急かつ適切なインシデント対応支援

発生した事象がインシデントかどうかの判断から、お客さまの対応体制や暫定対策の確認まで、高度なセキュリティ知識を持ったエキスパートが支援します。

原因や被害範囲をエキスパートが特定・調査

感染の可能性がある端末の調査から影響範囲の洗い出しまで支援します。端末にEDRが導入されていない場合でもマルウェアによる侵害状況の調査が可能です。

情報流出の痕跡などを調査・報告

お客さまのハードディスクをお預かりし、個人情報漏洩や不正アクセスの痕跡などの調査を行います。調査結果の詳細はレポートにまとめ、報告します。

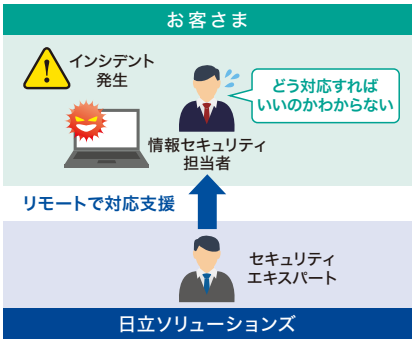
株式会社 日立ソリューションズ

提 供 内 容

対応方針策定支援

インシデント発生時にセキュリティエキスパートがオンラインで以下内容を確認します。

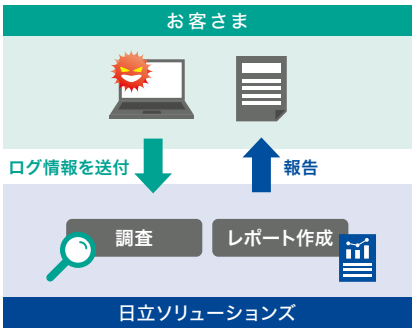
実施項目	内容
インシデント判断支援	発生した事象の内容をヒアリングし、セキュリティインシデントかどうかの判断を支援します。
お客さま体制確認	お客さまのインシデント対応体制について、セキュリティエキスパートが確認・提案します。
対策判断支援	お客さまが実施された暫定対策について、セキュリティエキスパートが確認、不足事項があった場合には提案します。



侵害調査支援

調査用スクリプトを配布し、そのログ情報をもとにマルウェア感染の原因や被害状況などの調査を支援します。

実施項目	内容
端末調査	マルウェア感染の可能性がある端末に対して、不審なファイルや痕跡など感染の原因調査を支援します。
脅威判定	端末調査で発見された不審なファイルの調査を支援します。
影響範囲調査	脅威の可能性が高いファイルの潜伏範囲を調査、感染端末を洗い出します。

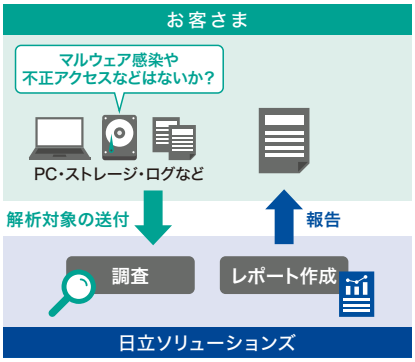


コンピュータフォレンジック

ハードディスクに残る痕跡を調査し、情報の不正流出などインシデントの詳細把握を支援します。

実施項目*	内容
マルウェア感染調査	マルウェアの痕跡調査や、ほかのサーバーや端末への被害の有無などを調査します。
不正アクセスに関する調査	アクセスを許可していないサーバーや端末、不審なWebサイトなどへの不正アクセスの有無を調査します。
情報の不正流出に関する調査	ログや残存しているファイルなどから、不審な情報の持ち出しの痕跡がないかを調査します。

＊実施項目や重点的に調査する項目については調査開始時にご相談のうえ決定します。



インシデント対応支援のご相談はこちら

事前に当社とのご契約がない場合でも、スポット契約により本サービスをご利用可能です。
まずはご相談内容をお送りください。

www.hitachi-solutions.co.jp/cgi-bin/form/security/contact/

株式会社 日立ソリューションズ
www.hitachi-solutions.co.jp

本カタログ掲載商品・サービスの詳細情報
www.hitachi-solutions.co.jp/security/sp/solution/task/mdr_incident_response.html

S23S-01-00 2023.12