サイバーセキュリティ・インシデントへの対応に不可欠な 3 つの事項

インシデントが起こる前に、エンド・ツー・エンドのインシデント対応プランを策定

Gartner

インシデント発生時にすぐに行動を起こせるよう備える

サイバーセキュリティ上の脅威となる事象 (サイバーセキュリティ・インシデント) は、「発生するかどうか」ではなく、「いつ発生するか」の問題です。その結果、メディアではかつてないほどのマイナス論調が展開されています。そして、監査役、規制当局をはじめとするステークホルダーからは、組織のブランド、評判、従業員、顧客、株主への影響を最小化するために、組織に明確なインシデント対応プランがあることを実証するよう求められています。

セキュリティとリスク・マネジメントのリーダーにとって不可欠なのは、「準備」することです。準備に重要なのは、インシデント対応プランと、インシデントの種類に応じた詳細なプレイブックです。

本ガイドは、ガートナーのツールとプレイブック * から抜粋して作成したものです。具体的な項目はすべて例示です。

* ガートナーのサービスをご利用のお客様は、ツールの完全版として、「Toolkit: Cybersecurity Incident Response Plan」「Toolkit: Creating a Ransomware Playbook」「Toolkit: Tabletop Exercise for Cyberattack Preparation and Response」をご覧いただけます。また、ガートナーのサービスをご利用のお客様は、テンプレートをダウンロードし、カスタマイズしてからガートナーに提出いただければ、ガートナーのエキスパートによるレビューを受けることができます。エキスパートは、プランを進める中で生じた質問にもお答えします。

2021 年は過去 17 年間で最も高いデータ侵害の平均コストが発生しました。また、**データ侵害の 10% がランサムウェアに関係しており**、発生頻度は 2020 年の 2 倍に増えました。

出典：IBM の 2021 年「データ侵害のコストに関する調査」レポート、Verizon の 2021 年データ漏洩／侵害調査報告書

正しく理解すべき 3 つの要素

01

インシデント対応プランを策定する

サイバーインシデント対応のための基本プラン

データ侵害のコストは、2020 年の 386 万ドルから、2021 年には **424 万ドル**へと増加しました。

出典：IBM の 2021 年「データ侵害のコストに関する調査」レポート

02

インシデント対応のための詳細なプレイブックを作成する

具体的なインシデント・シナリオに対処するための詳細なガイド

ランサムウェア攻撃の **80%** 以上に、ファイル暗号化のほか、データ盗難が含まれます。

出典：Ransomware attackers downshift to “Mid-Game” hunting in Q3 2021 (Coveware、2021 年 10 月)

03

定期的に机上演習を行う

定期的な検査として、インシデント対応プランに基づいて演習を行う

ランサムウェア攻撃が原因のダウンタイムは平均 **23 日間**です。

出典：Q2 Ransom Payment Amounts Decline as Ransomware Becomes a National Security Priority (Coveware、2021 年 7 月)

正しく理解すべき 3 つの要素

01

インシデント対応プランを策定する

サイバーインシデント対応のための基本プラン

02

インシデント対応のための詳細なプレイブックを作成する

具体的なインシデント・シナリオに対処するための詳細なガイド

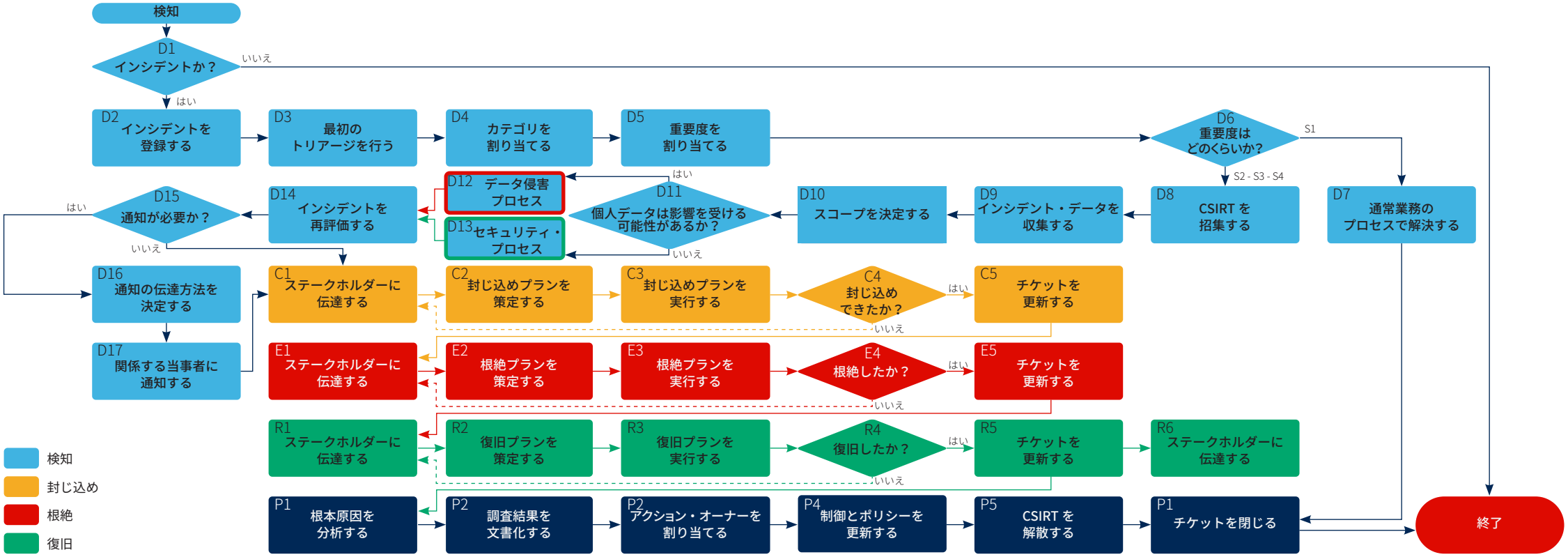
03

定期的に机上演習を行う

定期的な検査として、インシデント対応プランに基づいて演習を行う

インシデント対応プロセスのマップを作成する

インシデント対応プランでは、一連の手順を具体的に規定して、インシデント発生時にそれに沿って行動できるようにする必要があります。インシデント対応の担当者 (または同様の職務担当者) は、このプロセスの各ステップが完了していること、そして、進捗が随時、追跡および伝達されていることを確認すべきです。



インシデントの重要度の階層を定義する

すべてのセキュリティ・インシデントをトリアージ (訳注：基準に基づいて選別すること) し、重要度で階層を割り当てる必要があります。階層を明確にしておくと、インシデントのエスカレーションの誘導、サービス・レベル合意の割り当てのほか、組織に対するインシデントの潜在的または実際の影響についてステークホルダーに情報を提供する上でも役立ちます。また、重要度によって、通知先、今後のエスカレーション経路が決まるため、伝えるべきプレイブックも決まります。

重要度	ビジネスへの影響					テクノロジの属性	
階層	安全性	法務	規制	財務	評判	データ分類	オペレーション
04 サイバー危機	重傷者／死亡者	大きな影響	罰金：多額	損失額：多額	グローバルなメディア	極秘	壊滅的な機能停止
03 高	重傷者	中程度の影響	罰金：中～多額	損失額：中～多額	国内のメディア	機密	大規模な機能停止
02 中	応急処置	低い影響	罰金： 小～中程度の額	損失額： 小～中程度の額	地域のメディア	内部	軽微な機能停止
01 低	負傷者なし	影響なし	違反なし	損失なし	無害	公	機能停止なし

役割と責任を割り当てる

効果的なインシデント対応は、チーム・スポーツです。RACI (R：実行責任者、A：説明責任者、C：協業先、I：報告先) 図の中に、インシデント対応時の組織全体の役割と責任のすべてを示し、これを維持します。この図に加える一般的なステークホルダーとして、経営幹部、法務、プライバシー、人事の各チームがあります。

ステップ	CIO	CISO	DPO	ヘルプデスク	インシデント対応の担当者	IT	SOC	データ・オーナー	法務	PR	人事	カスタマー・オペレーション
インシデントを登録する				AR	CI	I						
最初のトリアージを行う		I			AR	C		I	I			
カテゴリを割り当てる		I	I		AR			C	C			
重要度を割り当てる		I	I		AR			C	C			
重要度に基づいて次のステップを決定する	I	CI	CI		AR	C						
通常業務のプロセスで解決する				I	I	AR		CI				
CSIRT を招集する	I	I		I	AR	CI						

正しく理解すべき 3 つの要素

01

インシデント対応プランを策定する

サイバーインシデント対応のための基本プラン

02

インシデント対応のための詳細なプレイブックを作成する

具体的なインシデント・シナリオに対処するための詳細なガイド

03

定期的に机上演習を行う

定期的な検査として、インシデント対応プランに基づいて演習を行う

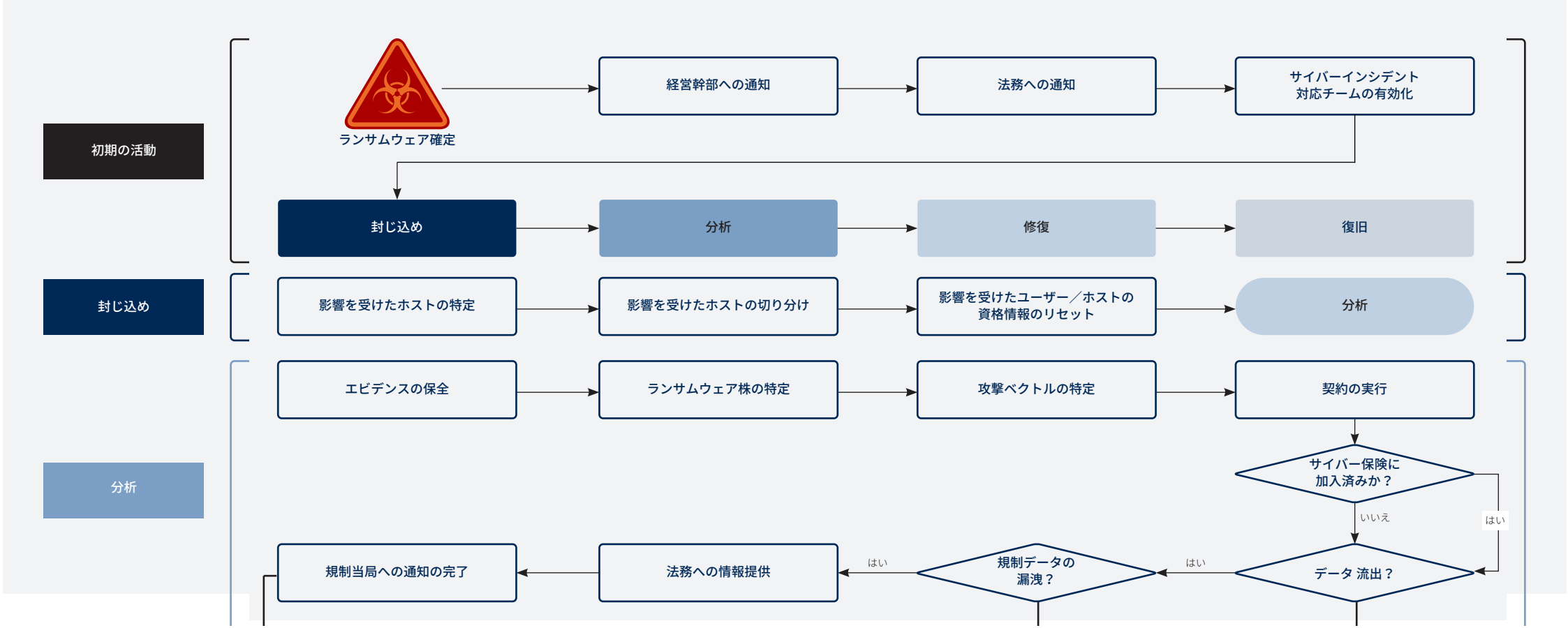
インシデント対応のためのプレイブックを作成する

CSIRT (Computer Security Incident Response Team：コンピュータ・セキュリティ・インシデント対応チーム) は、以下の例に示すランサムウェアのような一般的あるいは影響度の大きい種類のインシデントのために、具体的なプレイブックを策定すべきです。セキュリティの基本的なインシデント対応プランを超える、詳細な手引きと手順を示せるように設計します。

内容

ランサムウェア対応プロセスを策定する

ランサムウェア対応のためのプロセスとデシジョン・ツリーを作成します。その後、このプロセスを使って詳細な対応手順を策定し、役割と責任を割り当て、CSIRT 対応の指針となる追加文書を策定します。



詳細な対応手順を文書化する

特定分野の専門家 (SME) と連携して、詳細なランサムウェア対応手順を文書化します。これらの手順には、具体的な手引き、ツール、事例、設定などを含め、各ステップで責任を負う当事者を明確に特定すべきです。

	プロセス	タスク	責任を負う当事者
封じ込め	影響を受けたホストの特定	1. ランサムウェアが報告されたすべてのホストを特定する 2. 感染している可能性のある他のデバイスを特定する調査を実施する。 IoC (セキュリティ侵害の指標) の候補は以下のとおり。 • 異常なファイル・アクティビティ：大量のファイル名変更、ローカル・ディスクへの大量の書き込み、ディスクの暗号化 • エンドポイント上での CPU ／ディスク・アクティビティの増加 • ファイルへのアクセス不能 • アプリケーションの失敗 • 疑わしいネットワーク・トラフィック：非標準ポートを利用するトラフィック、一般的なパケット・サイズの変化、トラフィックを生成する上位ホストの変化、ファイアウォール・ログにおける「阻止」「拒否」エントリの増加。 • 特権ユーザー・アカウント・アクティビティの異常：アカウントの新規作成、既存のユーザー／グループのアクセス許諾の変更、所有権の変化 • 地理的不規則性：通常と異なる場所からのアクセス • レジストリやシステム・ファイルにおける疑わしい変化 • DNS リクエストの異常：これまで見たことがない IP へのトラフィックの急上昇	CSIRT CSIRT
	フォレンジック調査機関から指示があった場合を除き、マシンの電源をオフにしないようにしてください。メモリに保管中またはディスク上で実行中の貴重なフォレンジック・データが破壊されることがあります。		
	影響を受けたホストの切り分け	1. 感染したコンピュータ、ノート PC、タブレットを、有線、無線、携帯電話ベースを問わずすべてのネットワーク接続から切断する。 2. Wi-Fi のオフ、基幹ネットワーク接続機器 (スイッチを含む) の無効化、インターネットからのネットワーク全体の切断が必要かどうかを検討する。	CSIRT CSIRT

正しく理解すべき 3 つの要素

01

インシデント対応プランを策定する

サイバーインシデント対応のための基本プラン

02

インシデント対応のための詳細なプレイブックを作成する

具体的なインシデント・シナリオに対処するための詳細なガイド

03

定期的に机上演習を行う

定期的な検査として、インシデント対応プランに基づいて演習を行う

議題を作成し、当事者を集める

机上で実施するインシデント対応には、組織全体のリーダー層と意思決定者を参加させるべきです。
成功する机上演習とは、目的が具体的に定義され、参加者が対応する計画済みのシナリオを盛り込んで十分に構成されたものです。

議題とタイム・スケジュール：90 分間の机上演習

01	開会の挨拶と紹介	<5 分間 >
02	机上演習の目的とルール	<5 分間 >
03	机上演習の準備	<5 分間 >
04	シナリオ主導の机上演習	<60 分間 >
05	各グループによる報告／教訓	<15 分間 >

インシデントのシナリオと場面を作成する

サイバーセキュリティの机上演習は、最初のシナリオ (マルウェアなど) に続いて、一連の場面で構成するのが最も効果的です。各場面の中で、参加者が対応するこのインシデントに新たな情報を追加していきます。この構成は、実際のインシデントのように、不確実な状況下でインシデントが進展していく様子を再現しています。

	各場面の開始時間：合計 5 時間	実際の所要時間：合計 60 分
場面 No. 0：最初のシナリオ	8:00 a.m.	10 分
場面 No. 1：開始時間から 30 分後	8:30 a.m.	10 分
場面 No. 2：開始時間から 1 時間後	9:00 a.m.	15 分
場面 No. 3：開始時間から 3 時間後	11:00 a.m.	5 分
場面 No. 4：開始時間から 4 時間後	12:00 p.m.	8 分
場面 No. 4：開始時間から 4.5 時間後	12:30 p.m.	7 分

難易度の高いインシデントを想定する

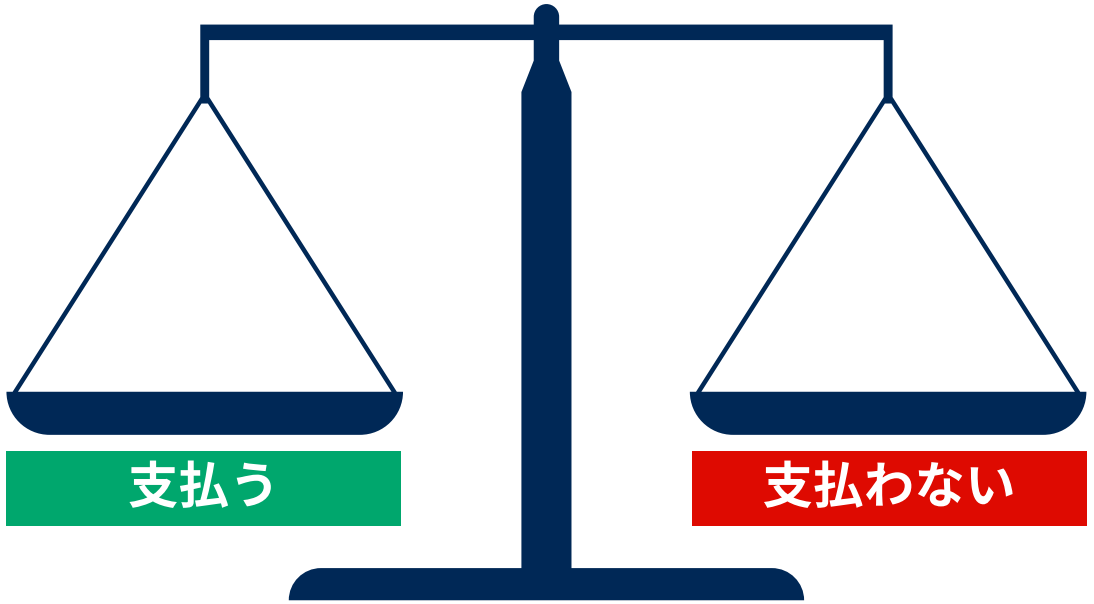
机上演習では、実際のサイバー攻撃でステークホルダーが対処しなければならない難易度の高い問題を再現すべきです。

例：ランサムウェア
机上演習で、攻撃者からの身代金要求に対応するという課題を与えることができます。

検討事項

身代金の支払いについては、以下のような実態があります。

- 復旧できるデータは全データのうち平均でわずか 65%、
  全データをどうにかして復旧する組織はわずか 8%。
- 暗号化されたファイルは復旧不能な場合が多い。
- 攻撃者が提供する復号化ツールは、クラッシュや失敗することがある。
- データの復旧には数週間を要することがある。
- 盗んだデータをハッカーが削除してくれる保証はない。
  価値あるデータなら、後に売却または公開される可能性がある。
- バックアップから復旧するよりも身代金を支払う方が簡単で低コストに
  なることもあるが、それは犯罪行為を助長するだけである。
- 身代金の支払いが違法となるケースさえある。



ガートナーのサイバーセキュリティ・チーム *

Director Analyst
Security & Risk
Management

サイバーセキュリティの専門知識：

- サイバーセキュリティ・インシデント対応プランをレビューし、セキュリティ意識の向上、評価指標、セキュリティに関するガイダンスを提供。
- CISO とそのチームに対して、セキュリティ／リスクのプラクティスとコミュニケーションに関してアドバイスを提供。
- アナリストおよび調査担当として 10 年の実務経験がある。

拠点：米国。

Paul Furtado
Senior Director Analyst
Security & Risk
Management

サイバーセキュリティの専門知識：

- サイバーセキュリティ戦略、リスク、インシデント対応についての知見とアドバイスを提供。
- 中規模企業のセキュリティの専門知識。
- CIO および CISO として 25 年以上の実務経験者。

拠点：カナダ。

Wam Voster
Senior Director Analyst
Security & Risk
Management

サイバーセキュリティの専門知識：

- オペレーショナル・テクノロジ (OT) のセキュリティのほか、セキュリティ・マネジメント、組織、ガバナンスについてアドバイスを提供。
- 30 年以上にわたり、複雑な環境 (石油／ガス、変化の速い消費財部門) でセキュリティ・プログラムを指揮および助言してきた IT 実務経験者。

拠点：オランダ。

* ガートナーのサブスクリプション・サービスによっては、ガートナーのエキスパートにサイバーセキュリティ・インシデント対応プランのレビューを依頼したり、プランを進める中で生じた質問をしたりすることもできます。

実用的で客観的な知見

成功に向けて、企業の皆様は、以下のようなセキュリティ／リスク・リーダーのための リソース／ツールを無償でご利用いただけます。

eBook

3 Steps to Stop Employees Taking Cyber Bait

従業員の行動を変え、効果的なリスク・マネジメントを行うことができます。

eBookをダウンロード (英語)

Roadmap

Protect Your Business Assets With a Roadmap for Maturing Information Security Program

サイバーセキュリティ・リスクを効果的に軽減するための成熟したプログラムを構築できます。

ロードマップをダウンロード (英語)

Webinar

Identify and Embrace New Collar Workers to Boost Cybersecurity

トレーニングを中心としたWebinarを視聴できます。

今すぐ視聴 (英語)

Research

How to Prepare for Ransomware Attacks

組織が今直面しているセキュリティの難題に備えることができます。

今すぐダウンロード (英語)

ガートナーのお客様は クライアント・ポータルでさらに多くのリソースをご利用いただけます。ログイン

Connect With Us

ガートナーは、経営幹部およびそのチームに対し、実行可能かつ客観的な知見を提供しています。ガートナーの深い専門知識によるガイダンスやツールは、組織が最優先のビジネス課題についてより迅速でスマートな意思決定を下し、より大きな成果を獲得することを可能にします。

弊社サービス全般に関するお問い合わせ先
TEL：03-6430-1850 (営業本部)
E-Mail：japan.sales@gartner.com

ビジネスを成功に導くガートナーのサービス
www.gartner.co.jp/ja/information-technology

最新の知見をご確認ください

Gartner