Hitachi Solutions Create

HITACHI

ペネトレーションテストの紹介

株式会社日立ソリューションズ・クリエイト

目次

HITACHI

Contents

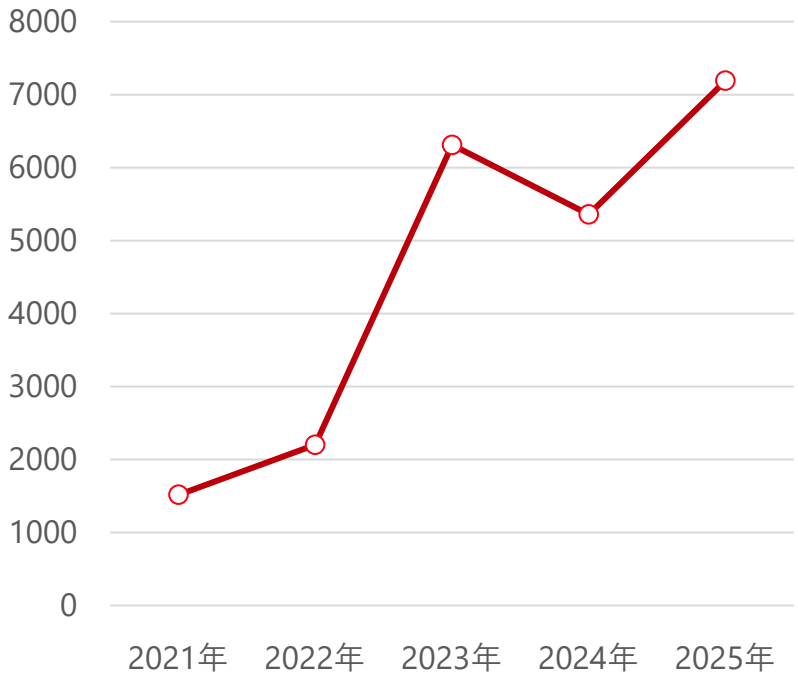
1. ペネトレーションテストの必要性

1－1. サイバー攻撃被害の状況

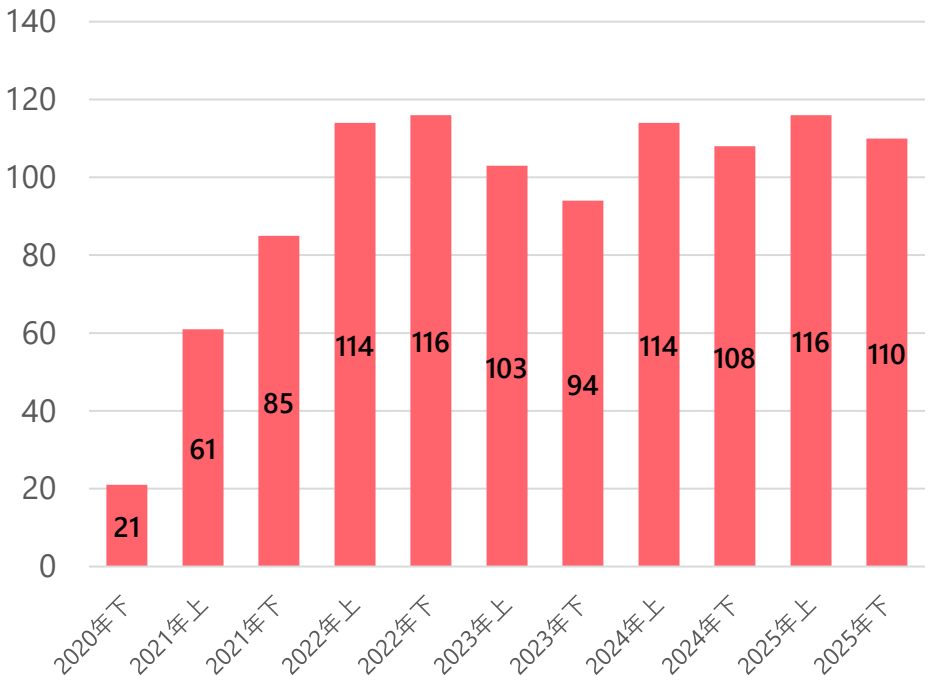
HITACHI

サイバー攻撃は増加傾向にあり、対策の必要性が高まっています。
「自社のシステムは本当に安全なのか」「攻撃を受けた場合、どこまで侵入されてしまうのか」を、攻撃者と同じ視点で確認することが、これからのセキュリティ対策に求められています。

不正アクセス行為の認知件数の推移(過去5年)※1



ランサムウェア被害報告件数の推移※2



※1出典：国家公安委員会･総務省･経済産業省
不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況　https://www.soumu.go.jp/main_content/001059979.pdf
※2出典：警察庁
令和７年におけるサイバー空間をめぐる脅威の情勢等について　https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7/R07_cyber_jousei.pdf

1－2．ペネトレーションテストとは／業界の動向

HITACHI

ペネトレーションテストとは、疑似的なサイバー攻撃を実施することで
システムのぜい弱性を発見し、セキュリティレベルを向上させるためのセキュリティ診断手法です。
特に機密性の高い情報を扱う業界では、ペネトレーションテストの必要性が高まっています。

ペネトレーションテストに関する各基準・ガイドラインと動向

分野	ガイドライン、記事	概要
金融	金融庁サイバーセキュリティガイドライン※1	金融業界では、脅威ベースのペネトレーションテスト (TLPT) の実施が推奨されています。 2.2.4【対応が望ましい事項】 b. 定期的に脅威ベースのペネトレーションテスト（TLPT）を実施すること。
金融	PCI DSS v4.0※2	クレジットカード情報を取り扱う企業は、外部および内部への ペネトレーションテストを定期的に実施する必要があります。 要件11.4 外部および内部へのペネトレーションテストを定期的に実施し、 悪用可能なぜい弱性およびセキュリティ上の弱点を是正している。
公共	自治体DX推進計画※3	自治体が実施するペネトレーションテストやリスクアセスメントについて、 総務省が支援することが記載されています。
ベンダー	情報セキュリティサービス基準適合サービスリスト※4	経済産業省が定めた情報セキュリティサービス基準を満たしたサービスのリストに、 ペネトレーションテスト（侵入試験）サービスが新たに追加されました。

※1出典：金融庁　金融分野におけるサイバーセキュリティに関するガイドライン　https://www.fsa.go.jp/news/r6/sonota/20241004/18.pdf
※2出典：PCI Security Standards Council　Payment Card Industry データセキュリティ基準 v4.0　https://listings.pcisecuritystandards.org/documents/PCI-DSS-v4_0-JA.pdf
※3出典：総務省　自治体デジタル・トランスフォーメーション（DX）推進計画【第5.1版】　https://www.soumu.go.jp/main_content/001053408.pdf
※4出典：経済産業省　「情報セキュリティサービス審査登録制度」の対象に「ペネトレーションテスト（侵入試験）サービス」を追加しました
https://www.meti.go.jp/press/2024/04/20240404001/20240404001.html

2. 当社サービスの紹介

2－1.手動診断と自動診断、2つのアプローチ

HITACHI

当社のペネトレーションテストは自動化ツールによる自動診断と、高度な資格を持つホワイトハットハッカーが攻撃者の視点でシステムに侵入を試みる手動診断の2つを提供しています。
お客さまの目的・予算・体制に応じて、最適なサービスをお選びいただけます。

項目	自動診断	手動診断
診断手法	自動ペネトレーションテストツール	ホワイトハットハッカー
検出方法	既知パターンに基づく検出 （シグネチャベース）	既知パターン＋業務文脈・攻撃者視点を踏まえた検出
検出可能なぜい弱性	主に既知のぜい弱性 （典型的なパターン）	既知＋未知（業務ロジックぜい弱性など）
特徴	テスターのスキルに依存せず同条件で何度でも実施可能（定期診断の場合）	攻撃シナリオを細かくカスタマイズ可能かつ人手による高度なテストが実施可能
実施期間	1カ月～	4カ月程度を目安に個別相談
価格	比較的安価	自動診断より高価
適用ケース	・予算や時間の制約がある場合 ・広範囲のIT資産に対する定期的な検査	・機密性の高い重要システムの評価 ・カスタマイズした攻撃シナリオの実施

2－2. 自動ペネトレーションテストのメニュー

HITACHI

自動化ツール「Immortal Cyber Teams AutoPT」（以下AutoPT）を活用し、
低コスト・短期間で実施できます。
お客さまの体制やニーズに合わせて、3つのメニューからお選びいただけます。

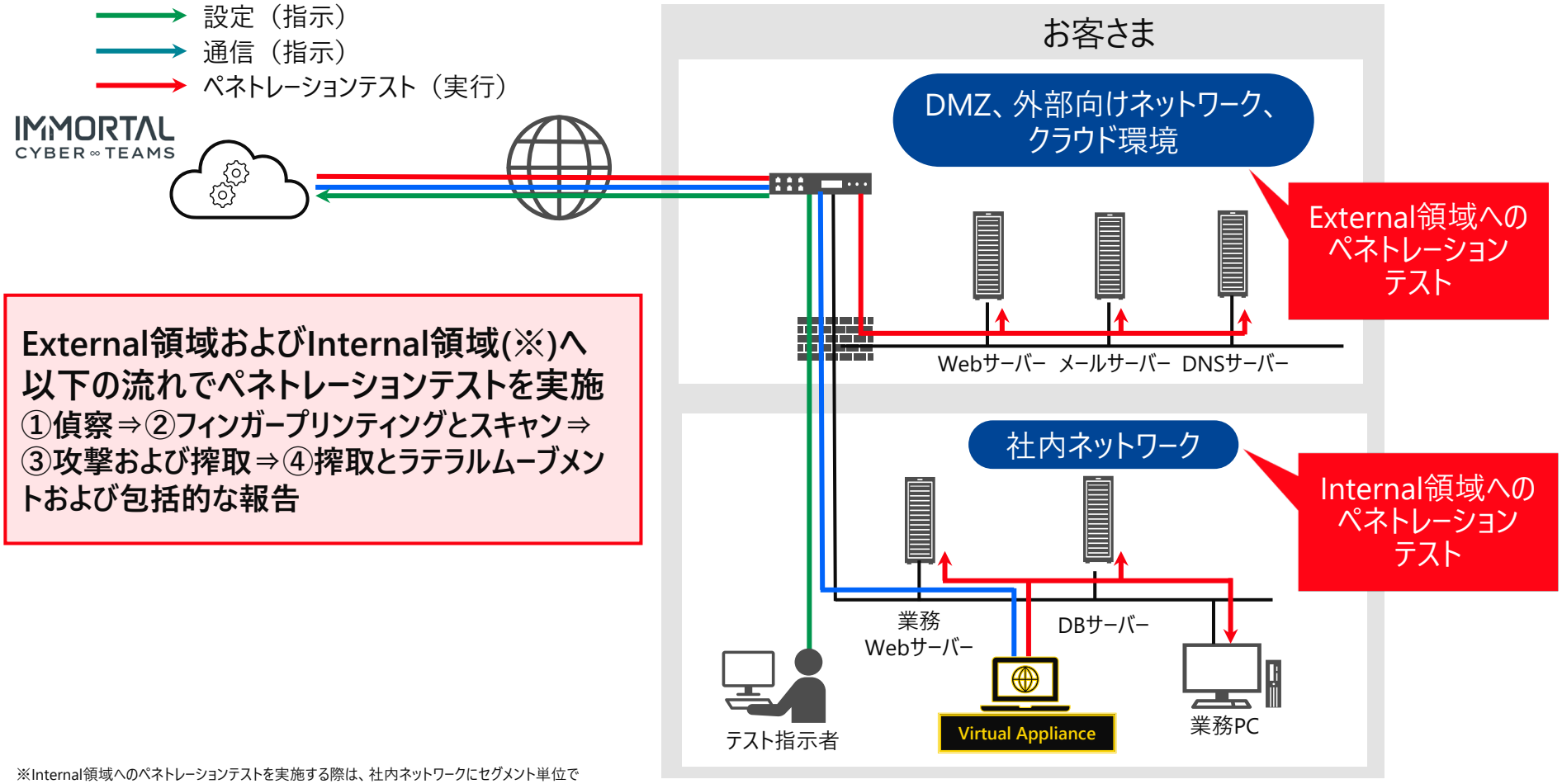
メニュー名	概要	ライセンス	このような方におすすめ
Immortal Cyber Teams AutoPT ライセンス	年間利用ライセンスです。お客さまの目的や実施したいタイミングに合わせて、ご利用いただけます。料金は対象のIPアドレス数に応じて決定。AutoPTに関する問い合わせサポートも提供します。	必要	自社でツールを運用し、必要なタイミングで自由に診断を実施したい方、英語の操作画面・報告書での運用が可能な方※
Immortal Cyber Teams AutoPT 活用支援 サービス	ご購入いただいたAutoPTライセンスを安心してご活用いただくために、当社のホワイトハットハッカーがテスト環境のセットアップ、ペネトレーションテストの実施、テスト結果報告書の作成を代行します。	別途必要	自社でのテスト運用を始めたいが、立ち上げや実施に不安をお持ちの方
ペネトレーション テストサービス スタンダード版	AutoPTを活用して、当社のホワイトハットハッカーがテスト環境のセットアップ、ペネトレーションテストの実施、テスト結果の報告までを実施します。	不要	ペネトレーションテストをお試しになりたい方、必要なタイミングで柔軟にご依頼されたい方

※AutoPTの操作画面と出力される報告書の言語は英語となります。

2－3. 自動ペネトレーションテストの実施イメージ

HITACHI

自動ペネトレーションテストでは、最新のぜい弱性を悪用した攻撃が発見された際に、攻撃者と同じ手法を用いて実際の攻撃をリアルタイムで再現します。AIを活用した最新の攻撃手法に加え、実際のサイバー犯罪者が使用している手口も取り入れることで、より実践的な診断を実施します。



External領域およびInternal領域(※)へ以下の流れでペネトレーションテストを実施
①偵察⇒②フィンガープリンティングとスキャン⇒③攻撃および搾取⇒④搾取とラテラルムーブメントおよび包括的な報告

※Internal領域へのペネトレーションテストを実施する際は、社内ネットワークにセグメント単位でVirtual Applianceの設置とVirtual Applianceから自動化基盤へのhttps(443)接続許可が必要です。

2－4．専門家による手動ペネトレーションテスト

HITACHI

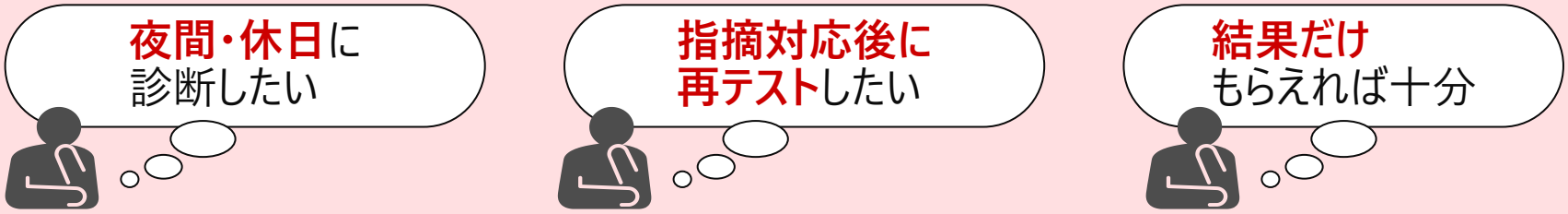
ホワイトハットハッカーによる高度な診断を実施します。

メニュー名	概要	ライセンス	このような方におすすめ
ペネトレーション テストサービス プロフェッショナル 版	最新の攻撃手法と多様なツールを駆使して システムの潜在的なぜい弱性を確認し、具体的な 対策を提案します。	不要	機密性の高いシステムを評価し たい方、攻撃シナリオをカスタマイ ズしたい方

ホワイトハットハッカーによる診断

情報処理安全確保支援士資格保有者等の
高度なセキュリティ資格を保有する診断員が担当します。

柔軟なオプション

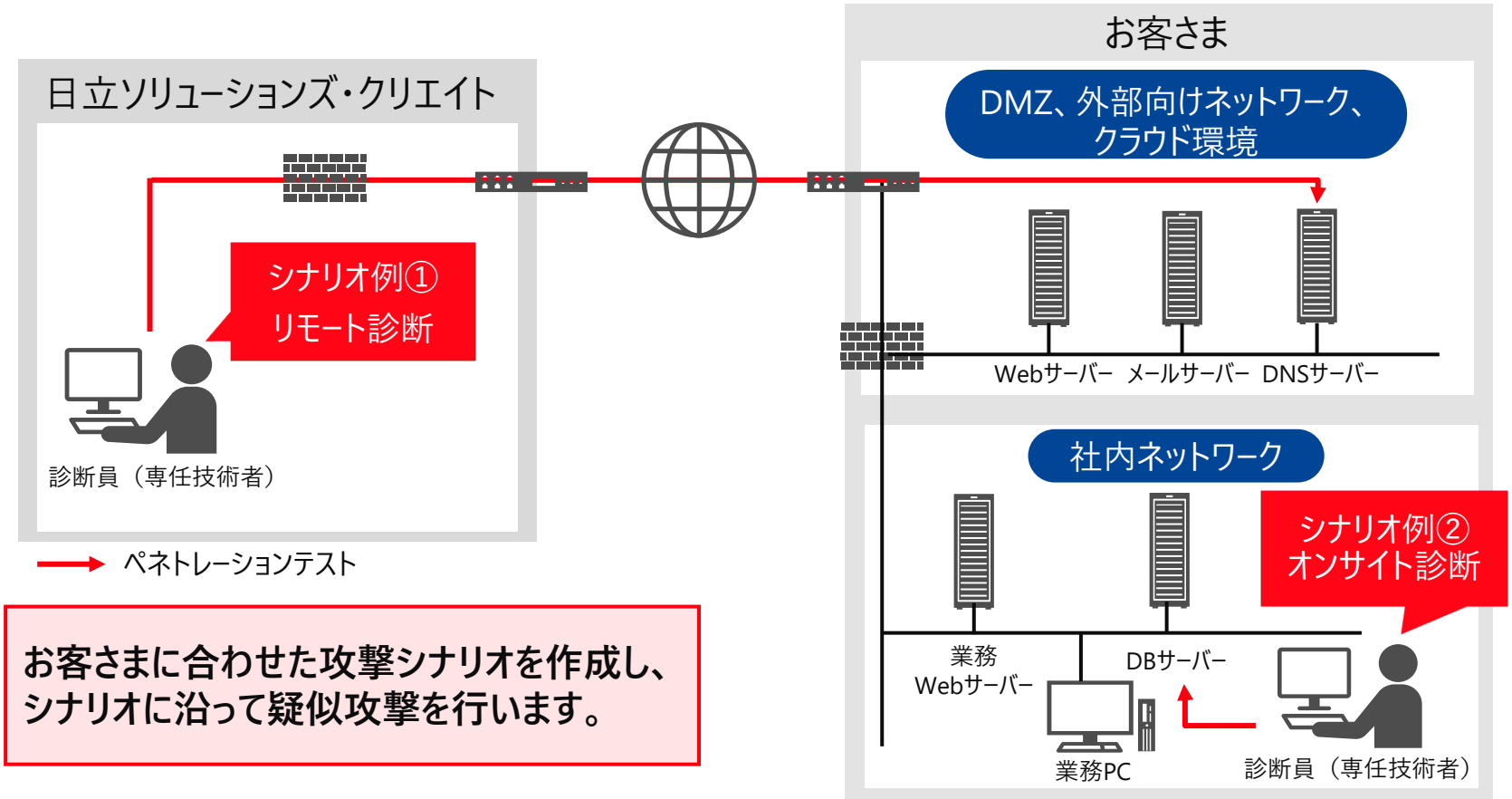


さまざまなご要望に応える、手厚いオプションを用意しています。

2－5．手動ペネトレーションテストの実施イメージ

HITACHI

手動ペネトレーションテストでは、お客さまに合わせた攻撃シナリオを作成します。
作成した攻撃シナリオに沿って、ホワイトハットハッカーが疑似的なサイバー攻撃を実施します。



**お客さまに合わせた攻撃シナリオを作成し、
シナリオに沿って疑似攻撃を行います。**

2－6．サービスの流れ

HITACHI

当社のサービスは、以下の3つのステップで構成されています。

ステップ 1

診断計画策定

お客さまのシステム構成、ビジネス要件、セキュリティに関する懸念事項などを詳細にヒアリングし、最適なテスト範囲、手法、スケジュールを決定します。

ステップ 2

ペネトレーションテスト実施

策定した診断計画に基づき、実際のペネトレーションテストを実施します。
システムのぜい弱性を攻撃者の視点で確認します。

ステップ 3

報告書作成

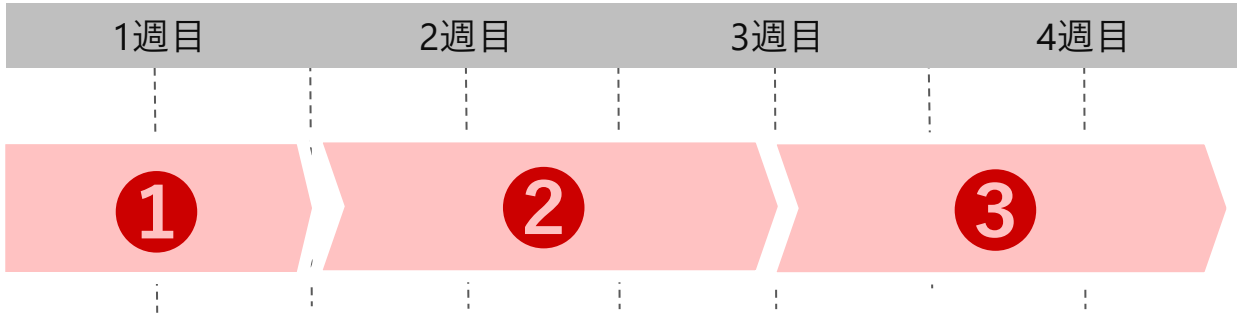
テスト結果を分析し、報告書を作成します。
検出されたぜい弱性の内容、具体的な対策方法などを記載します。
必要に応じて報告会を実施し、結果の詳細な説明や質疑応答を行います。

3. 作業スケジュール

3 － 1 . ペネトレーションテストサービス　スタンダード版

HITACHI

スケジュール（例）



❶ **計画**（1週間）　・・・・・・・・・診断・評価作業前の事前検証を実施

- 情報収集
- テスト環境・アプライアンスの準備

❷ **テスト実施**（1-2週間）　・・・・・・ベンダーが診断および評価を実施

- 攻撃の実施内容の記録

❸ **報告**（1-2週間）　・・・・・・・・・・・・報告会の実施

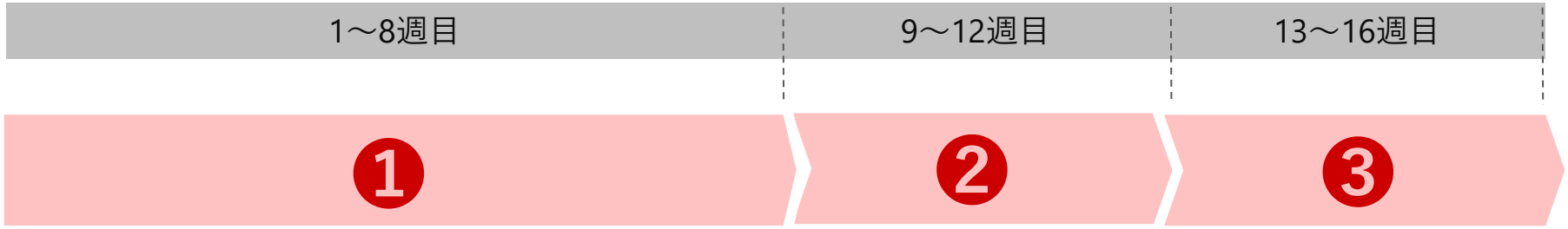
- 報告書作成
- 報告会

詳細は、別途相談のうえスケジュールを作成します。

3 － 2 . ペネトレーションテストサービス　プロフェッショナル版

HITACHI

スケジュール（例）



❶ 計画（8週間）　・・・・・・・・・診断・評価作業前の事前検証を実施

- 情報収集
- 攻撃方法の検討・準備

❷ テスト実施（4週間）　・・・・・・ベンダーが診断および評価を実施

- 攻撃の実施内容の記録

❸ 報告（4週間）　・・・・・・・・・・・・報告会の実施

- 報告書作成
- 報告会

詳細は、別途相談のうえスケジュールを作成します。

補足　スタンダード版のヒアリング事項(例)

HITACHI

ヒアリング事項(例)

DMZ、外部向けネットワーク、クラウド環境

#	パラメータ	値
1	ターゲットドメイン	
2	ターゲットIPまたはCIDRレンジ (IP指定：ターゲットを限定、CIDRレンジ指定：セグメント内で起動中のものがターゲット)	
3	ターゲット企業の商号（英語で記載が必要）	
4	テスト結果報告受信者情報（メールアドレス（複数指定可能））	
5	テスト実行日時（YYYY-MM-DD hh:mm で指定）	

社内ネットワーク

※Internal領域は、「仮想アプライアンス数」、「仮想アプライアンスアーキテクチャ」、「仮想アプライアンスのIPアドレス付与方式」の情報が必要です。

#	パラメータ	値
1	ターゲットドメイン	
2	ターゲットIPまたはCIDRレンジ (IP指定：ターゲットを限定、CIDRレンジ指定：セグメント内で起動中のものがターゲット)	
3	ターゲット企業の商号（英語で記載が必要）	
4	テスト結果報告受信者情報（メールアドレス（複数指定可能））	
5	テスト実行日時（YYYY-MM-DD hh:mm で指定）	
6	仮想アプライアンス数（セグメント単位で設置）	
7	仮想アプライアンスアーキテクチャ（OVAファイルが展開でき起動する環境） 例）Hyper-V、VMwareなど	
8	仮想アプライアンスのIPアドレス付与方式（固定 or DHCP）	

補足　ぜい弱性診断との違い

HITACHI

ぜい弱性診断とは以下の違いがあります。

比較項目	ぜい弱性診断	ペネトレーションテスト
目的	ぜい弱性の検出	侵入可能性の検証
手法	ツール・手動による検査	模擬攻撃
対象	システムの構成要素	システム全体
効果	ぜい弱性の把握と修正	現実的なセキュリティリスクへの対策

ペネトレーションテストは、以下に当てはまる組織での実施が効果的です。

- ぜい弱性診断を実施済み
- 自社が攻撃された際にどの程度の被害を受ける可能性があるか検証したい
- 効率的・効果的に、第三者視点からの自社環境の弱点を知りたい

補足　TLPTについて

HITACHI

脅威ベースのペネトレーションテスト（Threat-Led Penetration Testing）は、
テスト対象企業ごとに脅威を分析し、**個別にカスタマイズしたシナリオに基づいて防御・検知・対応結果まで確認する実践的な侵入テスト**であり、
以下のような特徴があります。

1. 実環境に対するサイバー攻撃により、攻撃対応能力を向上できます。
2. 攻撃側は、カスタマイズしたシナリオを基に検知されることなく目的達成することを目指し、防御側は現実のサイバー攻撃同様に防御・検知・対応を実施します。
3. サイバー攻撃に対する防御・検知・対応結果の確認を行うことで、人・組織・プロセスにおける課題を明確化できます。

お問い合わせ

HITACHI

■お問い合わせ先

株式会社 日立ソリューションズ・クリエイト

- **Webでのお問い合わせ**
  www.hitachi-solutions-create.co.jp/inq.html
  製品サイトのお問い合わせページより、ご連絡ください。
- **メールでのお問い合わせ**
  hsc-contact@mlc.hitachi-solutions.com

■お問い合わせ情報について

ご相談・ご依頼いただいた内容は回答などのため、当社の関連会社（日立ソリューションズグループ会社）
および株式会社日立製作所に提供（共同利用も含む）することがあります。
取り扱いには十分注意し、お客さまの許可なく他の目的に使用することはありません。

表示に関する注意事項

HITACHI

■他社商品名、商標などの引用に関する表示

- Hyper-Vは、米国Microsoft Corporationの、米国及びその他の国における登録商標または商標です。
- VMwareは、Broadcom Inc.の子会社であるVMware, Inc.の米国およびその他の国における登録商標または商標です。

■サービス・製品の仕様に対する表示

本資料に記載しているサービス・製品の仕様・価格は、2026年6月時点のものです。
サービス・製品の改良などにより予告なく記載されている仕様が変更になることがあります。

HITACHI