Hitachi Solutions Create

HITACHI

「“診断をしていない”が最大のぜい弱性」

経営リスクを低減するためのぜい弱性診断、最善の選択とは

株式会社日立ソリューションズ・クリエイト

目次

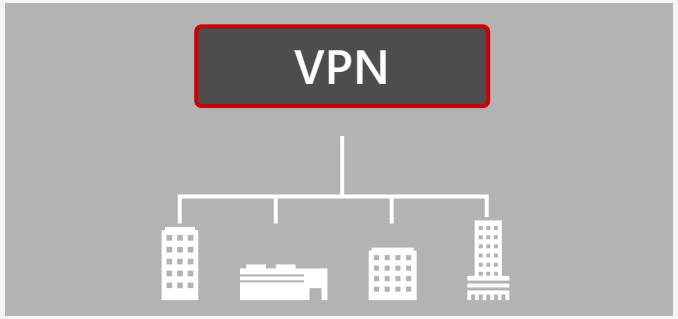
HITACHI

1-1.ぜい弱性とは

ぜい弱性とは、コンピューターシステムやソフトウェアに存在する、サイバー攻撃の標的となりうるセキュリティ上の欠陥や弱点のことです。不正アクセス、情報漏えい、システム停止などの深刻な被害を引き起こす可能性があります。

ECサイトなどのWebアプリケーションのぜい弱性を突いた、情報漏えいやWebページの改ざん

1 SQLインジェクション
2 クロスサイトスクリプティング（XSS）
3 クロスサイトリクエストフォージェリ（CSRF）
4 セッション管理の不備
5 ディレクトリ・トラバーサル
6 アクセス制御の不備
etc



VPNなどのネットワーク機器のぜい弱性を利用した侵入・攻撃

1 VPNの設定ミスによるぜい弱性
2 VPN認証機能のぜい弱性
3 VPNプロバイダーが提供するソフトウェアのぜい弱性
4 暗号化プロトコルのぜい弱性
etc

取引先などのサプライチェーン企業のぜい弱性を利用した侵入・攻撃

1 外部パートナー企業のVPN機器のぜい弱性を突かれた情報漏えい・ランサムウェア攻撃
2 業務委託先が攻撃され機密情報が漏えい
3 データ・ファイル転送ソフトのぜい弱性を悪用され、機密情報が漏えい
etc

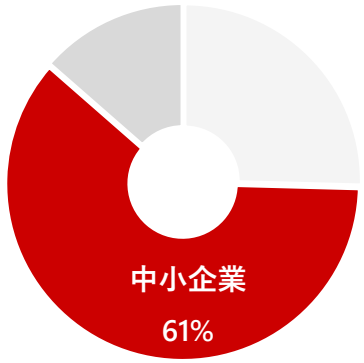
HITACHI

1-2.ぜい弱性を突いた攻撃の「標的」となりやすいのは

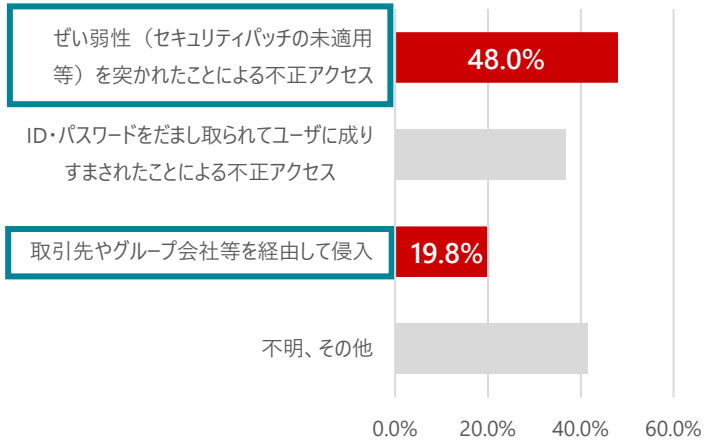
Webサイトの情報漏えい被害・ランサムウェア攻撃による被害の大半は中小企業で発生しており、双方ともに攻撃者はぜい弱性を利用した攻撃手法を多く用いています。また、サプライチェーン攻撃の入口として利用されるケースも多く報告されています。

Webサイトへのサイバー攻撃

Webサイトの情報漏えい被害組織の規模別割合

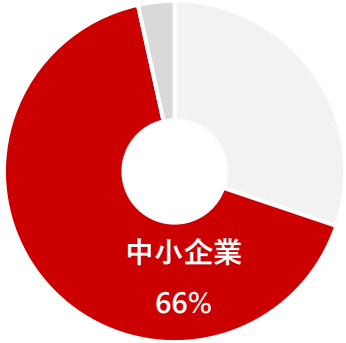


不正アクセスの原因となった攻撃の手口

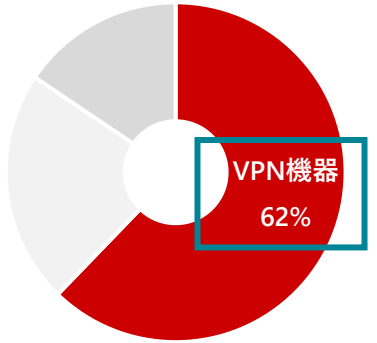


ランサムウェア被害

被害企業・団体等の規模別／業種別報告件数



感染経路



Webサイトへの攻撃、ランサムウェア攻撃ともに中堅中小企業での被害が多く報告され、どちらも放置されてしまったぜい弱性を利用した攻撃手法が用いられています

出典：IPA「2024年度 中小企業における情報セキュリティ対策に関する実態調査」

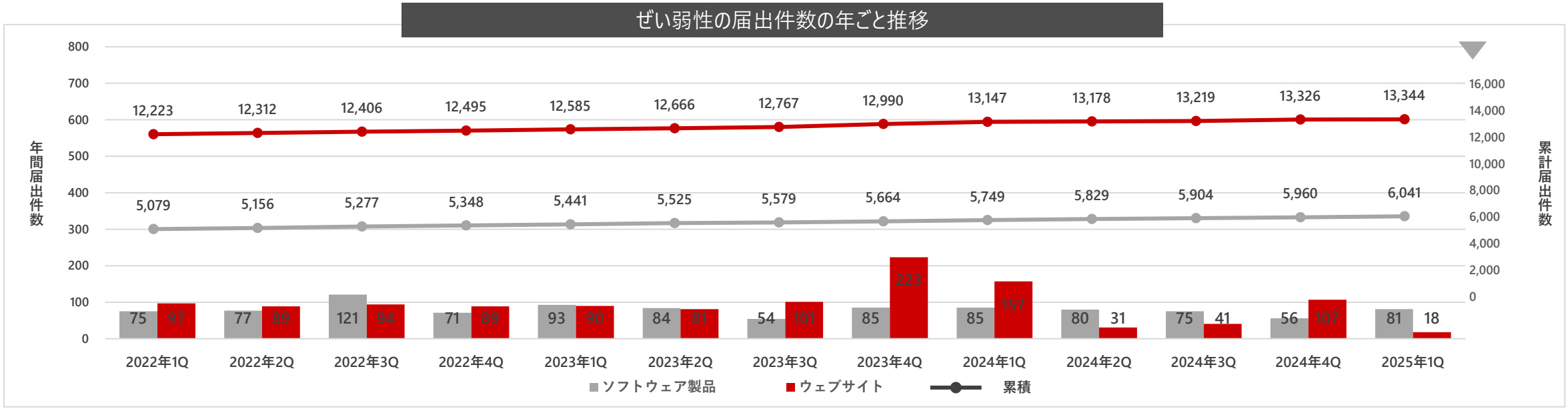
出典：JNSA「2025年7月 インシデント損害額調査レポート」

出典：警視庁広報資料「令和7年度上半期におけるサイバー空間をめぐる脅威の情報等について」を基に作成

HITACHI

1-3.ぜい弱性診断はどの程度の「サイクル」が望ましいのか

ぜい弱性はソフトウェアやシステムが進化または変更が加えられるたび、設計時には予期できなかった欠陥や設計ミスが生じてしまうことで発生します。発見後に解消するためのプログラムがリリースされますが、なくなることはありません。



年平均80件を超えるぜい弱性が新たに発見されています。定期的なチェック（診断）が欠かせません

出典：IPA「ソフトウェア等のぜい弱性関連情報に関する届け出状況」を基に作成

HITACHI

1-4.法規制・ガイドラインでの取り扱い

法令やガイドラインは安全管理措置との一環として“ぜい弱性診断”を明確に求めています。また、近年のサプライチェーンのセキュリティ強化の流れもあり、取引先企業へセキュリティ評価・ぜい弱性診断の実施を要求するケースも増えてきています。

個人情報保護法

委員会ガイドラインにて「安全管理措置」の一環として、
不正アクセス対策、ぜい弱性診断に実施が具体例として記載

クレジットカード・セキュリティガイドライン（ver.6.0）
-クレジット取引セキュリティ対策協議会 -

EC加盟店に対しWebアプリケーションやアシステムの
ぜい弱性診断を明示的に要求

サイバーセキュリティ経営ガイドライン

経営者が取組べき具体策の一つに
「ぜい弱性情報の収集・診断・対策」を明記

PCI DSS

四半期ごとの外部ぜい弱性スキャン（診断）、
定期的なペネトレーションテストの実施を要求

FISC安全対策基準

金融機関は定期的なぜい弱性診断・ペネトレーションテストを
実施するよう規定

**法令やガイドラインでは、近年の深刻な被害状況を背景に
不正アクセス対策としてぜい弱性診断の実施を求める動きがみられます**

HITACHI

1-5.適正な診断により、防げた可能性のあった「被害事例」

▶ Webサイトのぜい弱性診断を突いた攻撃事例

Case1	Case2	Information
【2025年4月】某教育サービス企業でSQLインジェクション攻撃が確認され、塾関係者約8,000件、模試受験者**約28万2千件**と保護者等約1万6千件の個人情報が流出した可能性	【2024年10月】子ども向け職業体験型テーマパークのWebサイトが不正アクセス被害を受け、個人情報 **2万4,644 件**が流出。 不正アクセスの原因は、Webサイトのプログラムの一部にぜい弱性があったと報告	【2025年8月】Webサイト等を作成できるコンテンツ管理システム（CMS）「**WordPress**」のプラグインに深刻なぜい弱性が発見。 マルウェア混入→悪意コードの挿入や情報収集が可能な状態にあると報告

▶ VPN機器のぜい弱性を突いた攻撃事例【2022年】

Phase1	Phase2	Phase3
病院に給食を提供する事業者の運営システムに設置されたVPN機器のぜい弱性を悪用し、不正アクセス	侵入後、**某医療機関へランサムウェア攻撃**を実行。 電子カルテを含むデータの暗号化	診療業務停止。**全システム復旧に73日間**を要す

出典：愛知 模試運営企業に不正アクセス 約30万件個人情報流出可能性 （https://www3.nhk.or.jp/news/html/20250702/k10014851431000.html）

出典：キッザニア Webサイトに不正アクセス、24,644 件の個人情報が流出(https://scan.netsecurity.ne.jp/article/2024/12/19/52061.html)

出典：委託事業者経由でランサムウエア被害　外来診療の全面再開に2カ月超 (https://xtech.nikkei.com/atcl/nxt/mag/nc/18/020600011/012600125/)

HITACHI

1-6.まとめ

Point 1

近年、ぜい弱性を突いたサイバー攻撃は
中堅中小企業をターゲットとしたケースが多い

Point 2

ぜい弱性をついたサイバー攻撃は、年間80件超、発生しており、
定期的なチェック（診断）を行い、是正することが必要

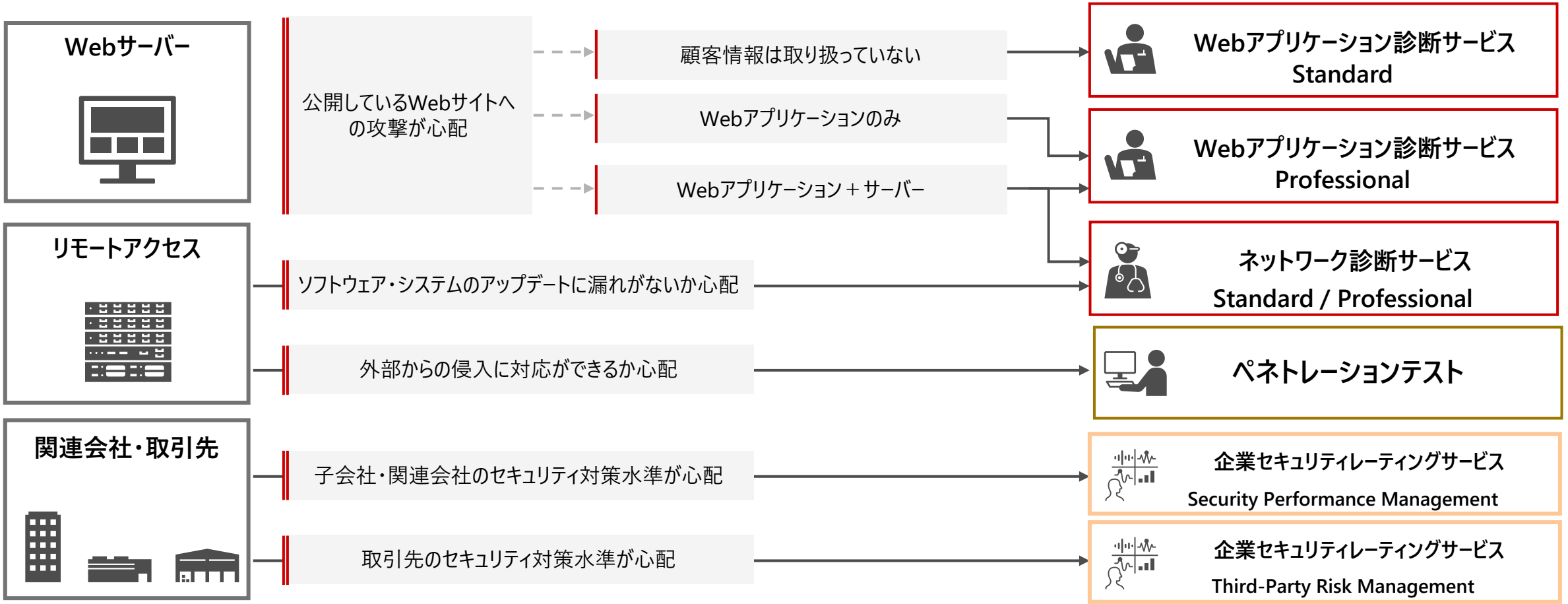
Point 3

サプライチェーン攻撃の「入口」となる可能性がある

事業規模に関わらず、定期的にぜい弱性診断をすることが大切です

HITACHI

2-1.自社に必要な診断サービスとは？



HITACHI

2-2.サービス概要 ①

Webアプリケーション診断サービス
Standard / Professional

確認できるリスクの例

- Webアプリケーションの設計・実装上のぜい弱性の有無
- アプリ経由での不正アクセス、情報漏えいのリスクの有無

Standard プラン	■ Webアプリケーション検査ツールによる疑似攻撃診断 ■ 報告書の作成・送付
Professional プラン	■ ホワイトハットハッカーによる手動診断 ■ 危険度大のぜい弱性について速報の作成・送付 ■ 手動にて発見されたぜい弱性を再現手順を含めて報告書に記載

ネットワーク診断サービス
Standard / Professional

確認できるリスクの例

- サーバー・ネットワーク機器などのぜい弱性の有無
- 不要なポート・サービスの開放による侵入のリスクの有無

Standard プラン	■ サービスポートの確認（1～65535番） ■ ぜい弱性スキャナツールによる通常攻撃診断 ■ ぜい弱性スキャナツールによる使用不能（DoS）攻撃診断 ■ 報告書の作成・送付
Professional プラン※	■ オープンポートに対する手動確認（OS種別・アプリケーション種別の確認） ■ 危険度大のぜい弱性について速報の作成・送付 ■ メール診断（メールサーバーの不正中継診断・メールアカウントの類推） ■ DNS診断（ゾーン転送・再帰問い合わせ）

※Professionalプランには、Standardプランの内容が含まれます。

HITACHI

2-2.サービス概要 ②

ペネトレーションテスト

攻撃手法を模倣した侵入テストを行い、ぜい弱性の有無のだけではなく、攻撃者が実際にどこまで侵入できるかや操作できるかを検証。攻撃の「実行の可能性」と「被害・影響」を確認できます

Step1.テスト対象範囲と内容のお打ち合わせ	Step2.攻撃者が用いる技術を模倣し侵入テスト	Step3.報告書のご提供

企業セキュリティレーティングサービス

攻撃者が標的を選定する上で用いる「インターネット上の公開情報」を用い、関連会社・取引先企業が攻撃者にとって標的となりうる可能性を数値化。課題改善に向けたアドバイザリーを行い、リスク低減を支援します

Step1.インターネット上の公開情報を収集	Step2.対象企業のぜい弱性を含んだ分析	Step3.ご報告・改善に向けたアドバイザリー

Open-Source Intelligence
OSINT

数値化

HITACHI

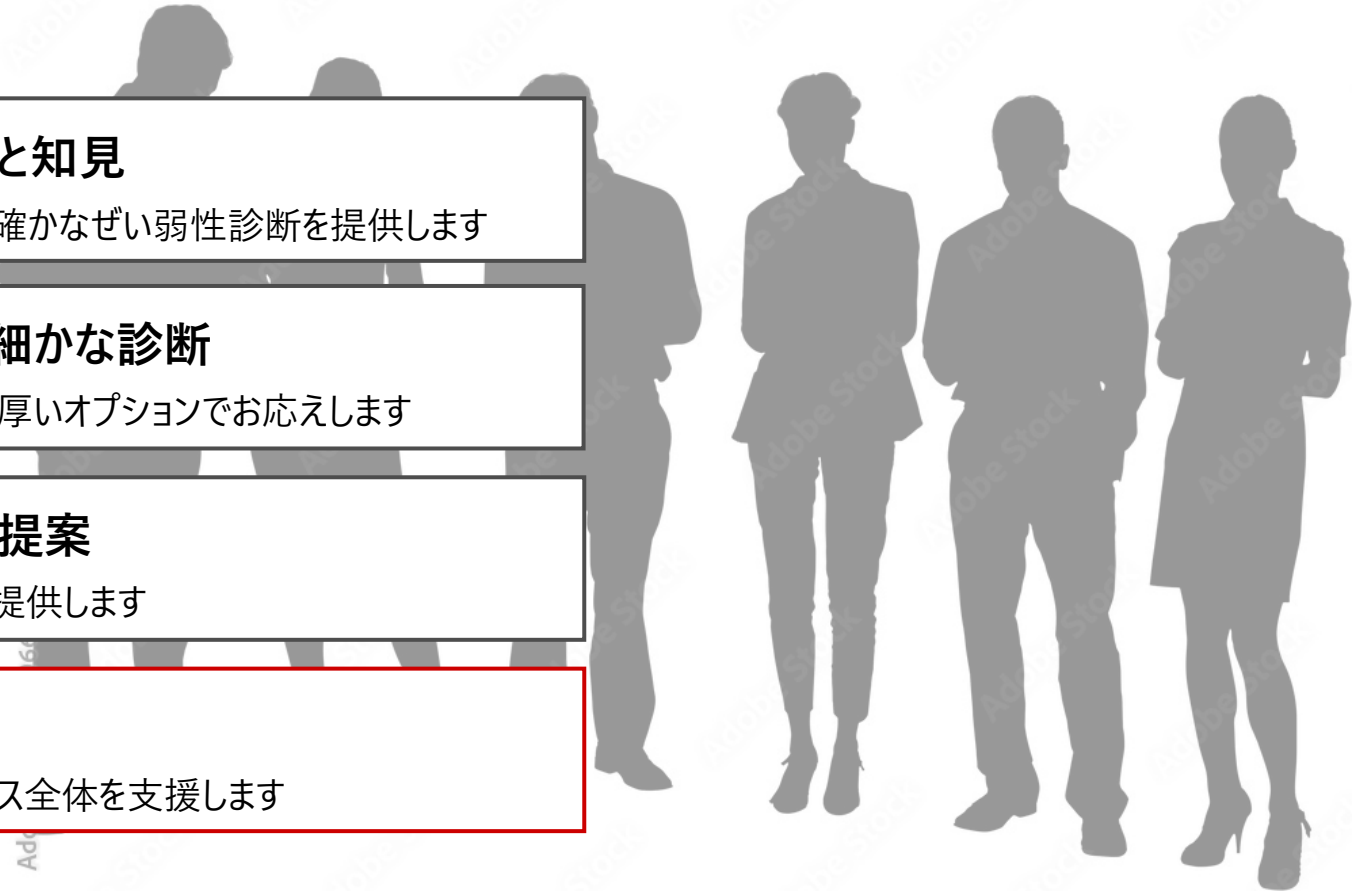
当社が選ばれる理由

1 **日立グループで長年培った豊富な実績と知見**
日立グループの一員として蓄積した経験を基にした確かなぜい弱性診断を提供します

2 **高度な技術を持つ専任者による、きめ細かな診断**
お客さまのさまざまなご要望に、専任の技術者が手厚いオプションでお応えします

3 **詳細な報告と、改善に向けた適正なご提案**
診断結果を基に、お客さまに合わせた改善提案を提供します

4 **包括的なITサービスのご支援**
インフラ構築など、セキュリティにとどまらないITサービス全体を支援します



より詳しいご相談、お問い合わせ

HITACHI

ご相談・お問い合わせ

ご相談・お問い合わせは専用メールアドレス宛にお問い合わせください。
ご不明点やご要望も受け付けております。
お客さまの環境に最適なご提案をいたします。

hsc-contact@mlc.hitachi-solutions.com

株式会社 日立ソリューションズ・クリエイト
代表者:取締役社長　南　章一
社員数: 4,013名（2025年4月1日時点）
所在地:東京都品川区東品川四丁目12番6号
（品川シーサイドキャナルタワー）

■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（共同利用含む）することがあります。
取り扱いには充分注意し、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。

■サービス・製品の仕様に関する表示

本資料に記載しているサービス・製品の仕様は、2025年11月現在のものです。
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