サイバー保険付き

脆弱性診断サービス

750
システムの
検査実績*

※2021年度実績

ハッカーによる攻撃が企業に与える影響

インターネットに公開されているシステムは、ハッカーがシステムの脆弱性を突いて日々攻撃をしかけてきます。もし攻撃が成功してしまった場合、企業に与える影響は想像以上に甚大です。

想定される攻撃

- データ改ざん
- 情報搾取
- データ削除
- システム停止
- 盗聴
- サービス妨害
- サイト改ざん
- なりすまし
- 踏み台
- システム破壊

企業のインターネット公開システム

企業に与える影響

- 信用の失墜
- 取引停止
- 競争力喪失
- 機会の損失
- 株価下落
- 風評被害
- 行政指導
- 費用損害
- 業務停止
- 賠償責任
- 免許はく奪

企業が理解しておくべき状況

増大するサイバーセキュリティ被害に対して、法制度・規制等が強化されるとともに、漏えい事故が発生した場合の費用損害額も会員情報数に比例して増大しています。

どうする？

改正個人情報保護法による影響

2022年4月の「個人情報保護法の改正」により個人情報漏洩時の報告義務・罰金刑が中小企業も対象に強化されています。

どうする？

全EC系サイトの脆弱性対策が必須化

経済産業省通達により全てのEC系サイトを対象に、サイト自体の脆弱性対策（システム上の設定不備改善、脆弱性診断、ウイルス対策等）が必須化されます。

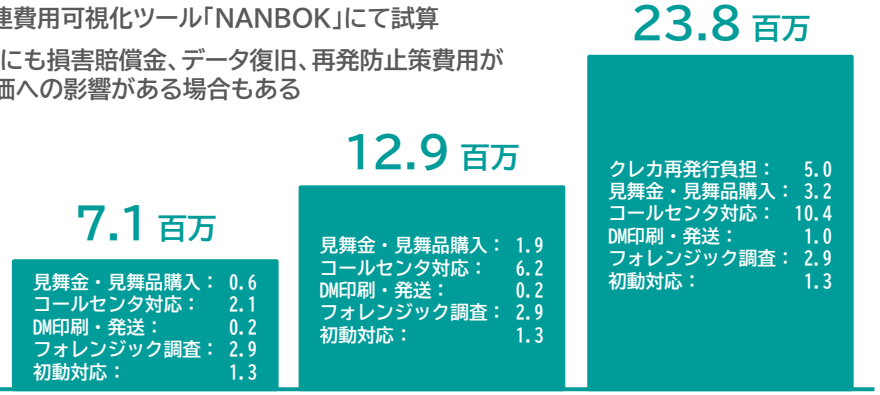
どうする？

サイバー攻撃を受けた場合に必要となる費用の想定

会員情報を保持数に比例して費用損害額は増大する

※ IPA発行のセキュリティ関連費用可視化ツール「NANBOK」にて試算

※ 記載している費用項目以外にも損害賠償金、データ復旧、再発防止策費用が必要になる場合、さらに株価への影響がある場合もある

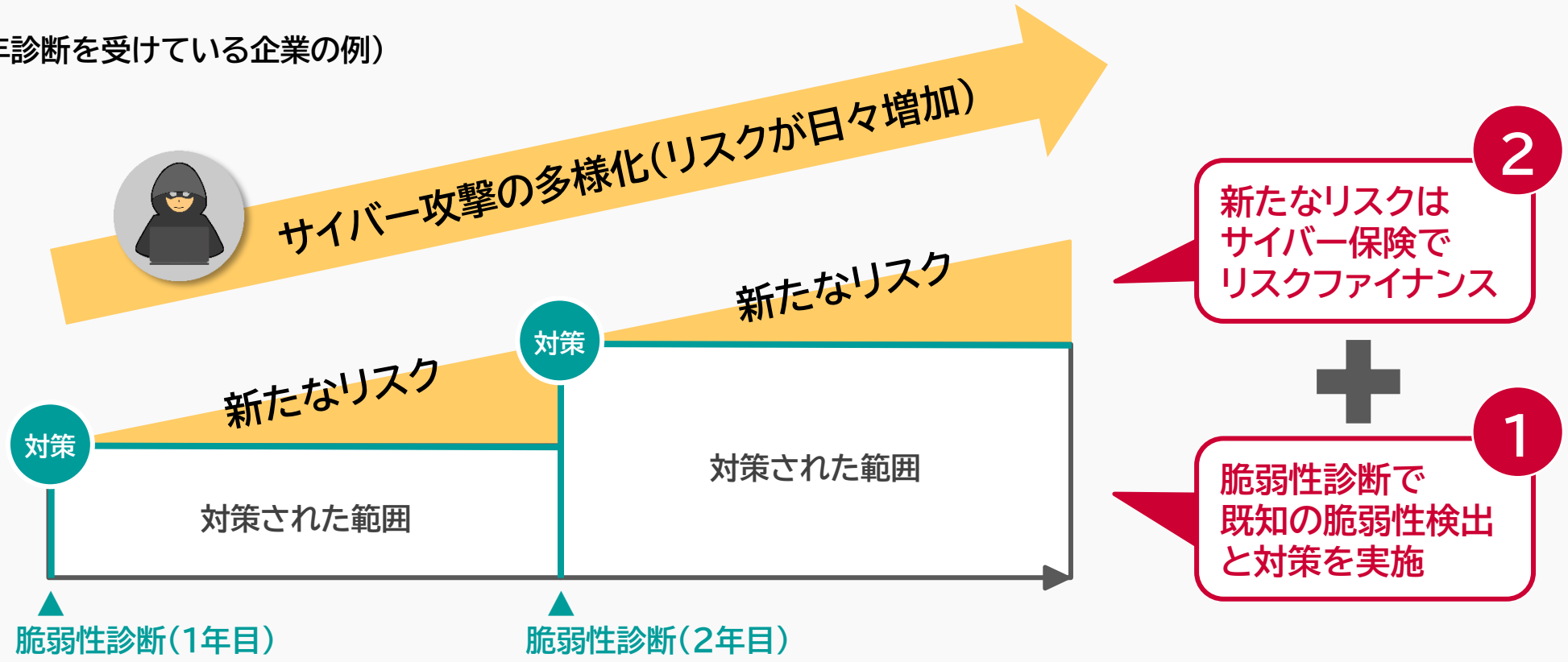


必要となる想定費用			
会員数（個人情報数）	1,000	3,000	5,000
クレカ情報の有無	無し	無し	有り

ハイリスクなインターネット公開サーバを守るには？

解決 サイバー保険付き脆弱性診断で新たなリスクにも備える

（毎年診断を受けている企業の例）



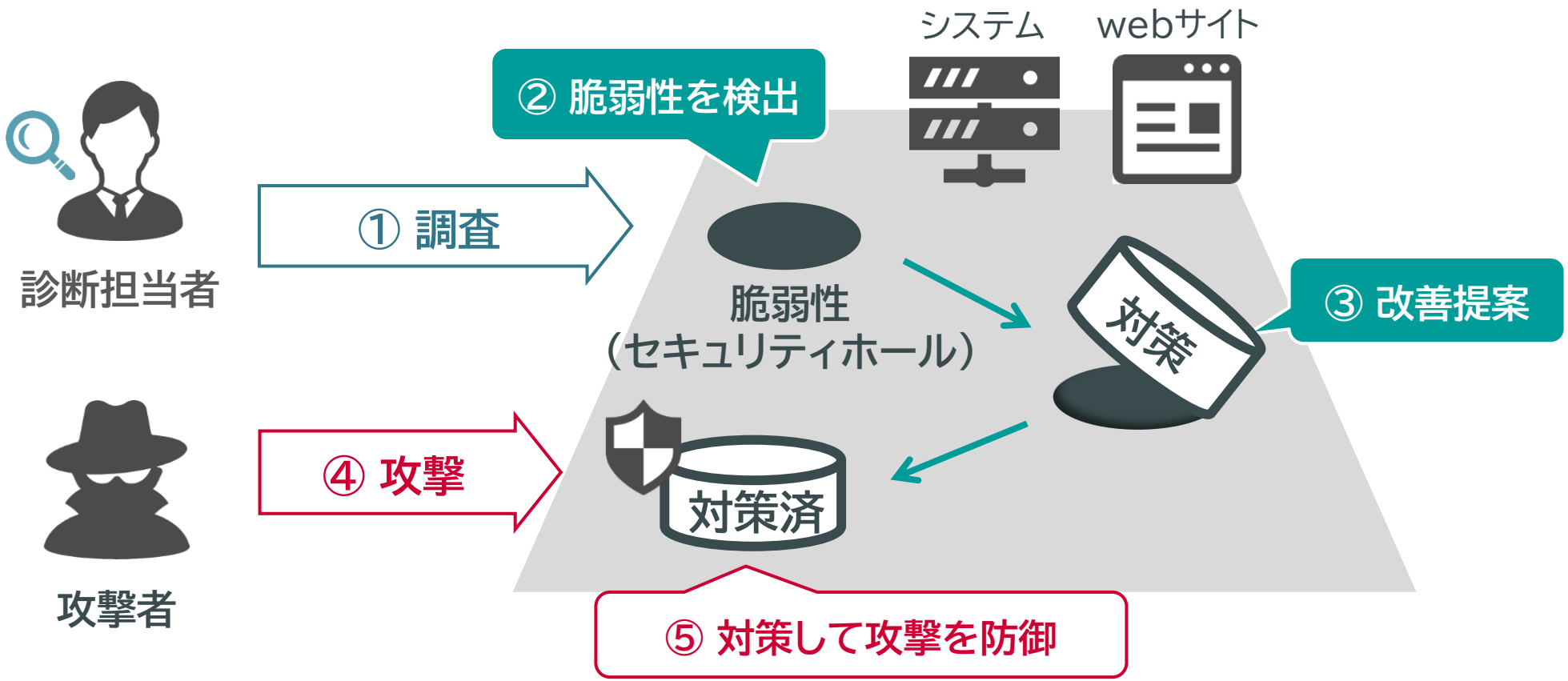
2 新たなリスクは サイバー保険で リスクファイナンス

＋

1 脆弱性診断で 既知の脆弱性検出 と対策を実施

脆弱性診断とは

システムやwebサイトのセキュリティリスクにつながる脆弱性を攻撃者の視点で調査します。
検出脆弱性の改善提案を行うことで、お客様は効果的なセキュリティ対策が実施できます。



脆弱性診断メニュー

ネットワーク診断

インターネットに公開しているWebサーバやNW機器等、社内ネットワークに接続しているサーバ等を対象に、ネットワーク経由でサーバ等に内在する脆弱性を洗い出す検査です

サーバ構成診断

対象サーバ上で診断ツールを実行し、パスワード設定情報やセキュリティ設定情報等を取得し、設定情報等から脆弱性を洗い出す検査です

Webアプリ診断

Webアプリケーション(動的に遷移するWebページ)を対象に、Webアプリケーションに内在する脆弱性を診断技術者がツールと手作業できめ細かく洗い出す検査です

スマホアプリ診断

Android/iOSアプリケーションを対象に、アプリ単体の端末検査やアプリ⇔サーバ間の通信路検査を行うことで、Android/iOSアプリに内在する脆弱性を洗い出す検査です

サイバー保険

診断対象システムに起因して発生した情報漏えい等の損害リスクをサイバー保険で補償します。(全メニューに無償で自動付帯)

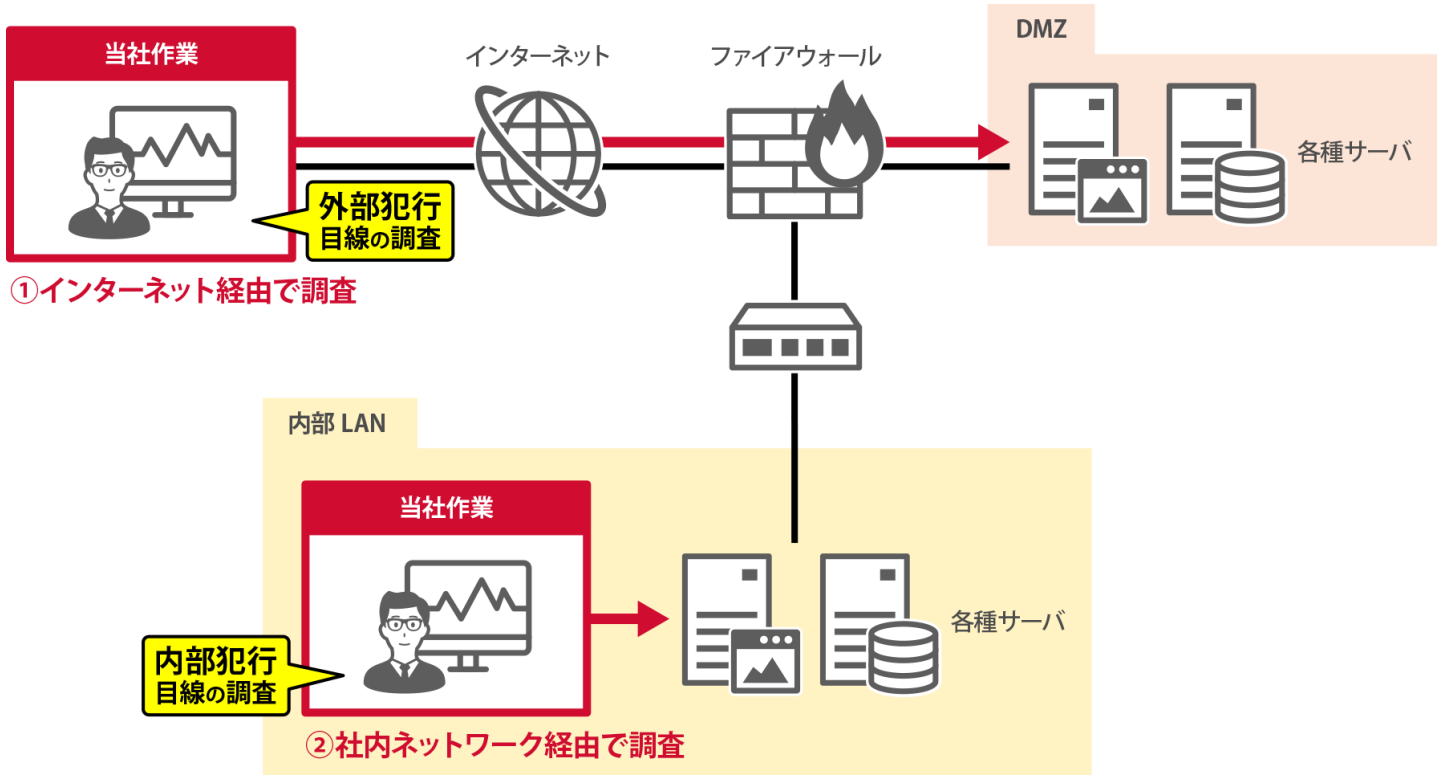
【事例】脆弱性診断＋適切な対策により防げてたはず

ハイリスクなインターネット公開サーバはシステムに潜在する脆弱性を突いて様々な手口で狙われます。脆弱性診断と適切な対策をすることで、企業としての社会的信用を守ることが可能です。

事例1	官公庁関連のWEBサイトおいて、**Apache Struts2の脆弱性**を利用して不正アクセスを受けていたことを確認。その結果3か月の間にWEBサイト上で作成された情報（氏名・法人名、契約日、取引価格など）が**4千件流出した可能性**があると発表。（2018年）	**ネットワーク診断**による脆弱性検出と対策が適切に出来てれば回避できたはず
事例2	人材アウトソーシング企業が運営するWEBサイトにおいて**SQLインジェクションの脆弱性**を突いて海外から不正アクセスを受けていたことを確認。その結果、メールアドレスが**約30万件流出した可能性**があると発表。（2020年）	**Webアプリ診断**による脆弱性検出と対策が適切に出来てれば回避できたはず

ネットワーク診断　概要

診断技術者が、診断ツールを利用しネットワーク（インターネットや社内ネットワーク）経由で、サーバやネットワーク機器の脆弱性を洗い出します。



実施手順

1. サービススキャン（ツール）
2. 脆弱性調査（ツール）
3. ツール結果精査＋手動調査（手動）

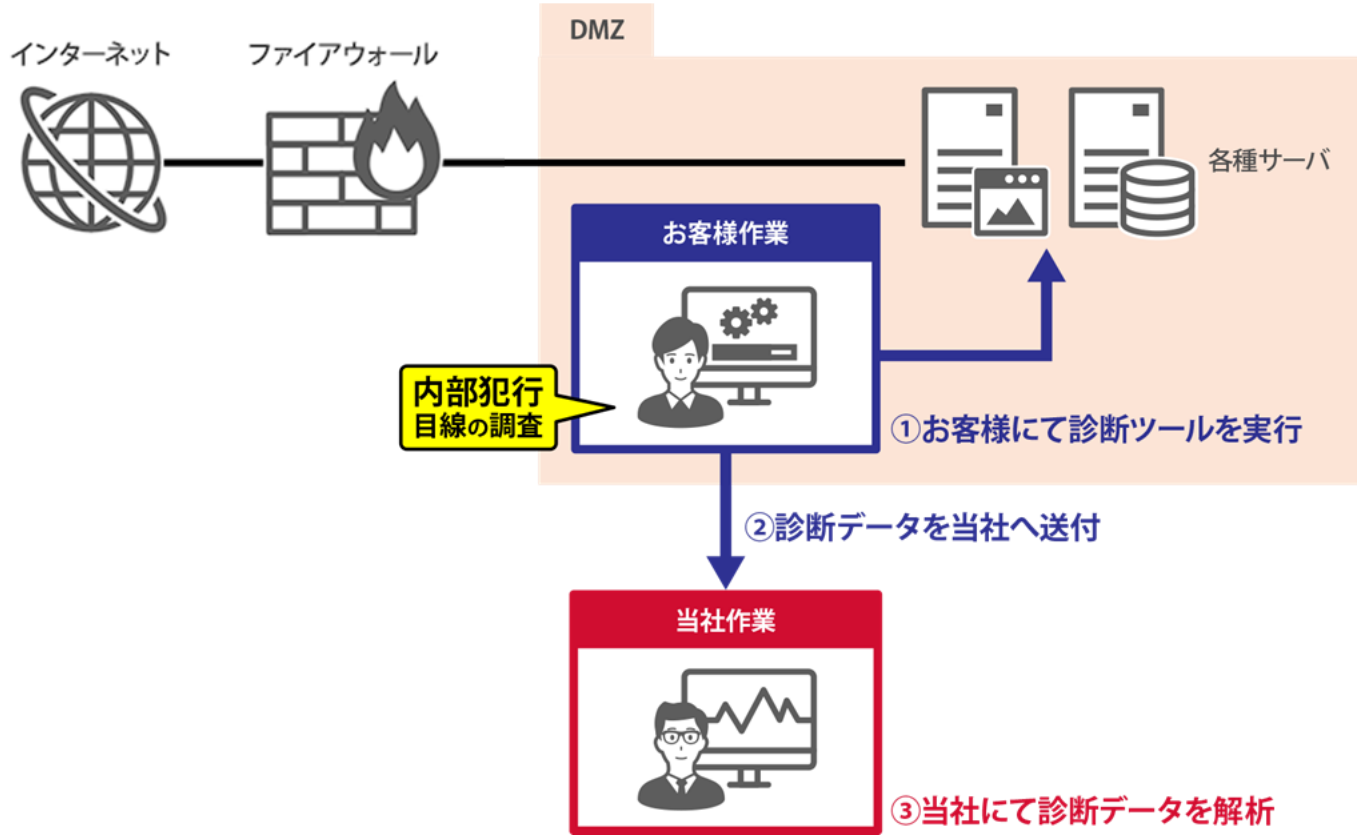
ネットワーク診断　診断項目例

診断項目	内容
不要なサービスの稼働	インターネットに公開不要とされるサービスが公開されていないか確認 例 データベースサービス、リモートデスクトップサービス、FTPサービス　等々
ソフトウェアのバージョン漏洩	Apache・PHP等のサーバソフトウェアのバージョンがインターネットに公開されていないか確認 ※HTTPヘッダー内やエラーページ内にバージョン表示
ソフトウェアの脆弱性	ソフトウェアのバージョンが漏洩した上で、該当バージョンに起因する脆弱性が存在しないか確認 また、サポート終了しているソフトウェアを利用していないか確認
管理者画面の公開	一般ユーザがアクセス不要な画面がインターネット上に公開していないか確認 例 Webコンテンツ作成画面（CMSツール含む）、ルータ管理画面　等々
暗号アルゴリズムの問題	暗号化強度の低いアルゴリズムの利用していないか確認 例 DES、MD5、SHA-1　等々

※ インターネット公開サーバ向けの診断項目の一例です。

サーバ構成診断　概要

お客様にて対象サーバ上で診断ツールを実行していただき、実行結果を弊社へ送付いただいた後、
診断技術者がサーバ（OS）上のセキュリティ設定不備等の脆弱性を洗い出します。



実施手順

1. お客様にて診断ツールの実行（管理者権限）
2. 出力された診断データを弊社へ送付
3. 弊社にて診断データを解析し報告書作成

サーバ構成診断　診断項目例

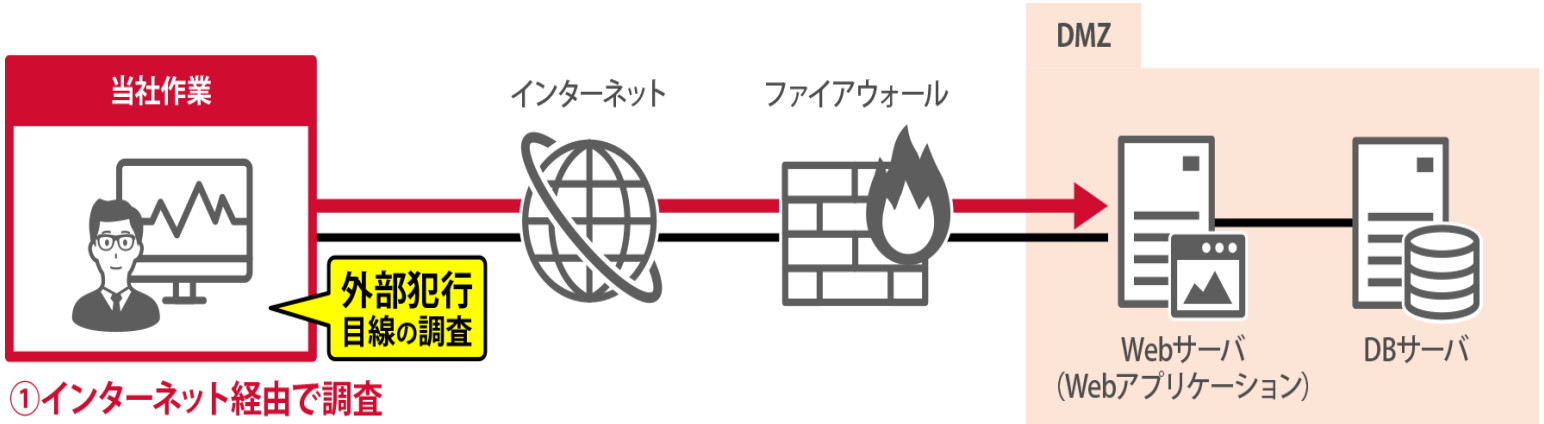
診断項目	内容
脆弱なパスワード	パスワード設定なし、アカウントと同じパスワード、桁数が極端に少ない パスワード等々の脆弱なパスワードに設定されているアカウントの確認
セキュリティパッチの未適用	OSのセキュリティパッチ（Microsoftのセキュリティ修正プログラム、 RedHatのRPM等）の適用状況を確認し、未適用パッチの確認
ウイルス対策ソフトの導入チェック	ウイルス対策ソフトが導入されているかどうか、 またウイルス定義ファイルが更新されているか確認
アクセス権の設定不備	共有フォルダ等に不適切なアクセス権が付与されていないか確認 ※Everyoneグループにフルアクセス権付与　等
セキュリティポリシーの設定	イベントログ等の取得有無、アカウントポリシーの設定内容を確認し 不備がないかどうか確認（Microsoft製品のみ）

※ サーバ構成診断の診断項目の一例です。

Webアプリケーション診断　概要

診断技術者が、Webブラウザとローカルプロキシ※を利用しWebアプリケーションに対して
疑似攻撃を試行することで、Webアプリケーションの脆弱性を洗い出します。

※ローカルプロキシ：ブラウザとサーバの間に入り、ブラウザから送られるHTTPリクエストをキャッチし内容を変更してサーバへ送信するツール



実施手順

1. Webサイト全体の脆弱性調査(手動)
2. パラメータ毎の脆弱性調査(手動)
3. 診断ツールによる脆弱性調査(ツール)

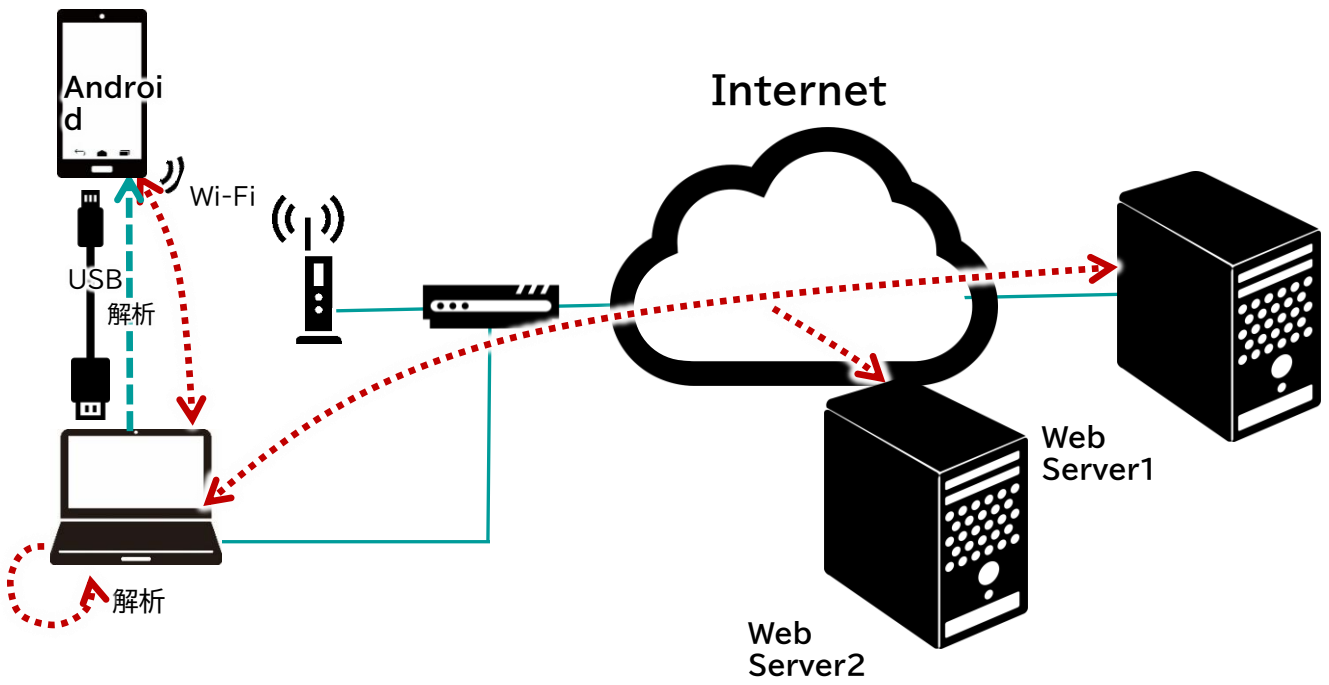
Webアプリケーション診断　診断項目例

診断項目	内容
クロスサイトスクリプティング	JavaScriptやHTTPで使用される特殊記号(”‘＜＞ &)が、Webアプリケーションサーバ上で無害化せずに認識し、スクリプトが実行されないか確認 攻撃例 スクリプトを実行させ、攻撃者サーバへCookie情報を転送
SQLインジェクション	SQL文を挿入してWebアプリケーションと連動しているデータベースを操作できないか確認 攻撃例 データベースを操作し、個人情報を抜き取る
データアクセス権の欠如	権限を越えて、他人の情報へアクセスできないか確認 攻撃例 パラメータを改ざんし、他人の情報へアクセスして情報採取や改ざんを行う
セッション管理の不備	セッション情報が更新されない・セッションがタイムアウトしない　等のセッションに関する設定に不備がないか確認 攻撃例 セッションを乗っ取り、他人のログイン後画面にアクセスして情報採取を行う
ディスクキャッシュの不備	Webブラウザ上に、個人情報がキャッシュされていないか確認 攻撃例 共有PCの場合、キャッシュ情報からID/PASSを盗み出す

※ Webアプリケーション診断の診断項目の一例です。

スマホアプリ診断　概要

診断技術者が、アプリ単体の端末検査・サーバ間通信の通信路検査を行うことで、
Android/iOSアプリの脆弱性を洗い出します。



① 端末検査

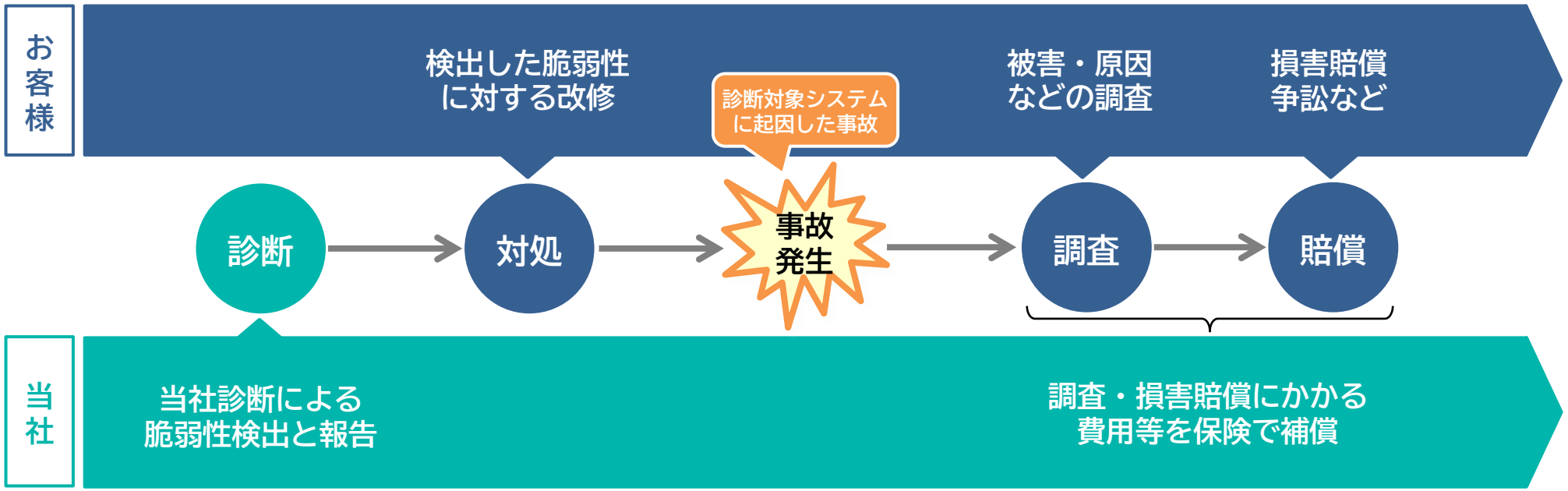
アプリを動作させ、その結果の確認を行います。生成データ/通信後のデータに認証情報/利用者情報が含まれていないかなどの確認を行います。

② 通信路検査

Webアプリケーション診断と同様の項目を診断します。

特徴1　サイバー保険を無償で自動付帯

一過性対策にすぎない脆弱性診断と修正対策だけでは、日々進化するサイバー攻撃等に対しては、新たなリスクが生まれてしまいます。診断対象システムに起因して発生した情報漏えい等の損害リスクをサイバー保険で補償します。



※ サイバー保険は全ての脆弱性診断メニューを対象に、ご契約頂いた金額（総額）が80万円以上（税抜）の場合に無償で自動的に付帯されます。

特徴2　高い品質・培ったスキルによる診断実績

品 質

■ 国内外のセキュリティ基準に準拠

・独立行政法人 情報処理推進機構 ウェブ健康診断仕様

・OWASP Foundation Application Security Verification Standard

■ 情報セキュリティサービス基準に適合

・ネットワーク診断・Webアプリケーション診断は、経済産業省が定める「情報セキュリティサービス基準」に適合。
IPA(独立行政法人情報処理推進機構)が情報提供する「情報セキュリティサービス基準適合サービスリスト」にも掲載

019-0013-20

■ 複数人によるクロスチェックすることで高品質を確保

スキル

■ 情報処理安全確保支援士、CISSP、CISA、CISM、CEH 等

■ 国内外で発生した脆弱性・攻撃手法を調査・取り込み

■ 社外セキュリティ専門会社と技術連携によるスキル向上

実 績

■ ドコモグループを中心に数多く脆弱性診断を実施

・ネットワーク診断：年間 約750システム 5,800.IP

・Webアプリ診断：年間 約750サイト 18,500リクエスト

（2021年度実績）

脆弱性診断サービスの特徴③

特徴3　充実したセキュリティ対策フォロー

当社作成の報告書に記載した「対処すべき脆弱性」について、お客様にて対策された後、お客様と調整の上
対策状況の確認を実施します。**（再診断は、診断報告書提出後、3カ月以内に3回まで）**
また、危険度の高い脆弱性が発見された場合には、別途速報によりお客様のセキュリティ対策をフォローします。

事前調査 お見積り

ヒアリングシートをもとに診断対象や環境条件面の確認等を実施し、お見積書を提出します。

診断作業

お客様と合意した診断内容にて、脆弱性診断を実施します。開始・終了時にはメール連絡します。

診断結果の精査 速報でのフォロー

診断中も随時診断結果を精査し、危険度が高い脆弱性が検出された場合は速報としてご提示します。

報告書作成

検出した脆弱性毎に、具体的な検出箇所や対策方法、さらに再現方法等も記載した報告書を提出します。

報告会 検出内容・対策説明

専門の診断アナリストより、的確な報告書で分かりやすくご説明します。対策方法のアドバイスなども実施します。

対策確認 再診断

検出された脆弱性が対策されたかの確認を実施します。脆弱性の危険度に合わせて再診断も行います。

特徴4　的確な診断報告書の提示

検出した脆弱性毎に、具体的な検出箇所記載した報告書を提出します
的確な内容により脆弱性の詳細や再現方法を分かりやすく解説し、脆弱性対応後の確認にもお役立ていただけます。

総合評価をABCの3段階に分けて報告

評価	評価基準
A	緊急に対策が必要な脆弱性が存在せず、危険性の低い状態
B	緊急度の高い脆弱性は存在しないが、将来的に高危険度に推移する可能性があり、設定の見直しや改善等の対策が必要
C	情報漏洩や改ざんにつながる脆弱性があり、緊急の対策が必要

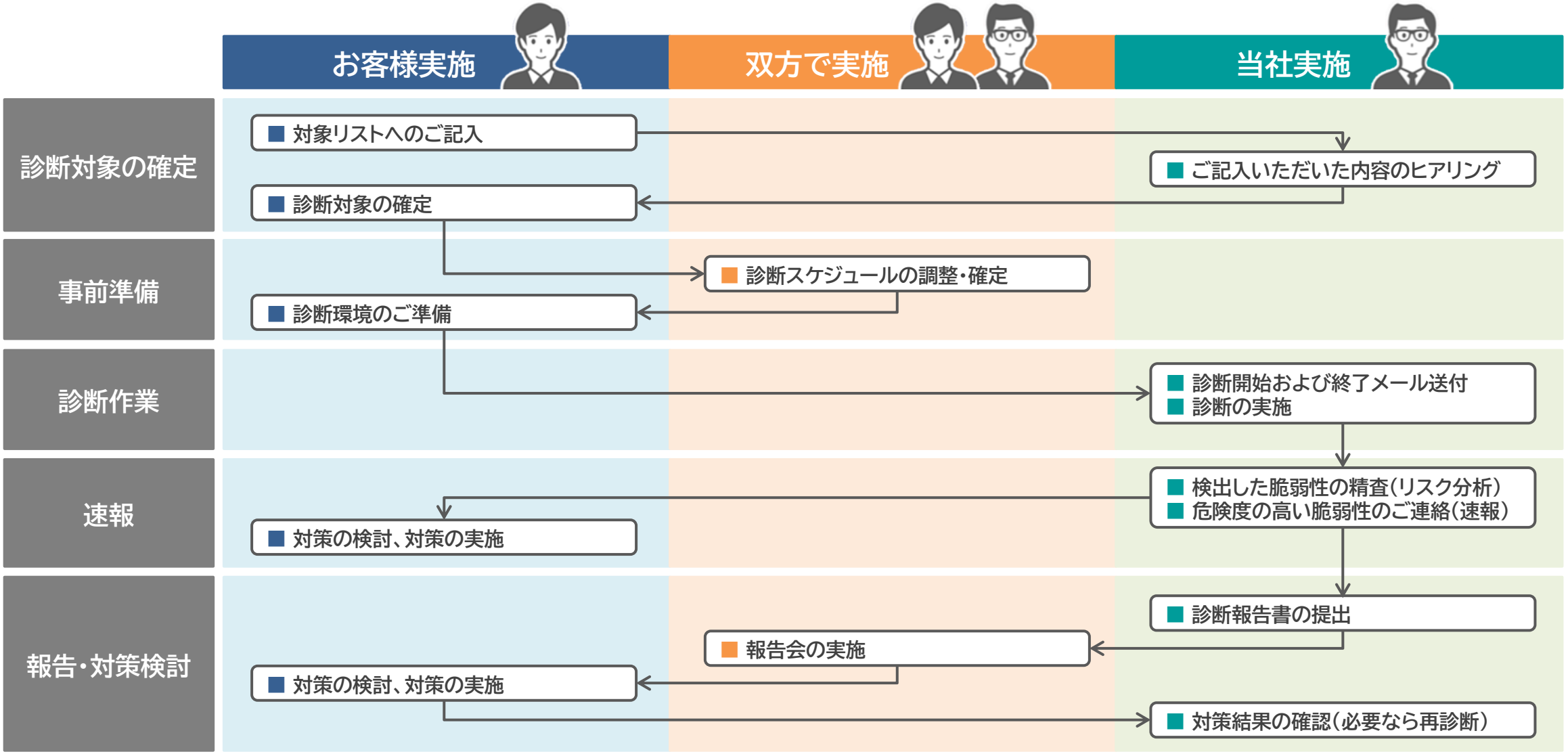
具体的な検出箇所や対策方法を網羅した報告書

CVSS※による脆弱性毎の評価

対策状況を管理できる対策チェックシート付き

※CVSS(Common Vulnerability Scoring System):特定ベンダの評価に依存しない世界基準による評価方法

脆弱性診断実施の流れ



価格の目安

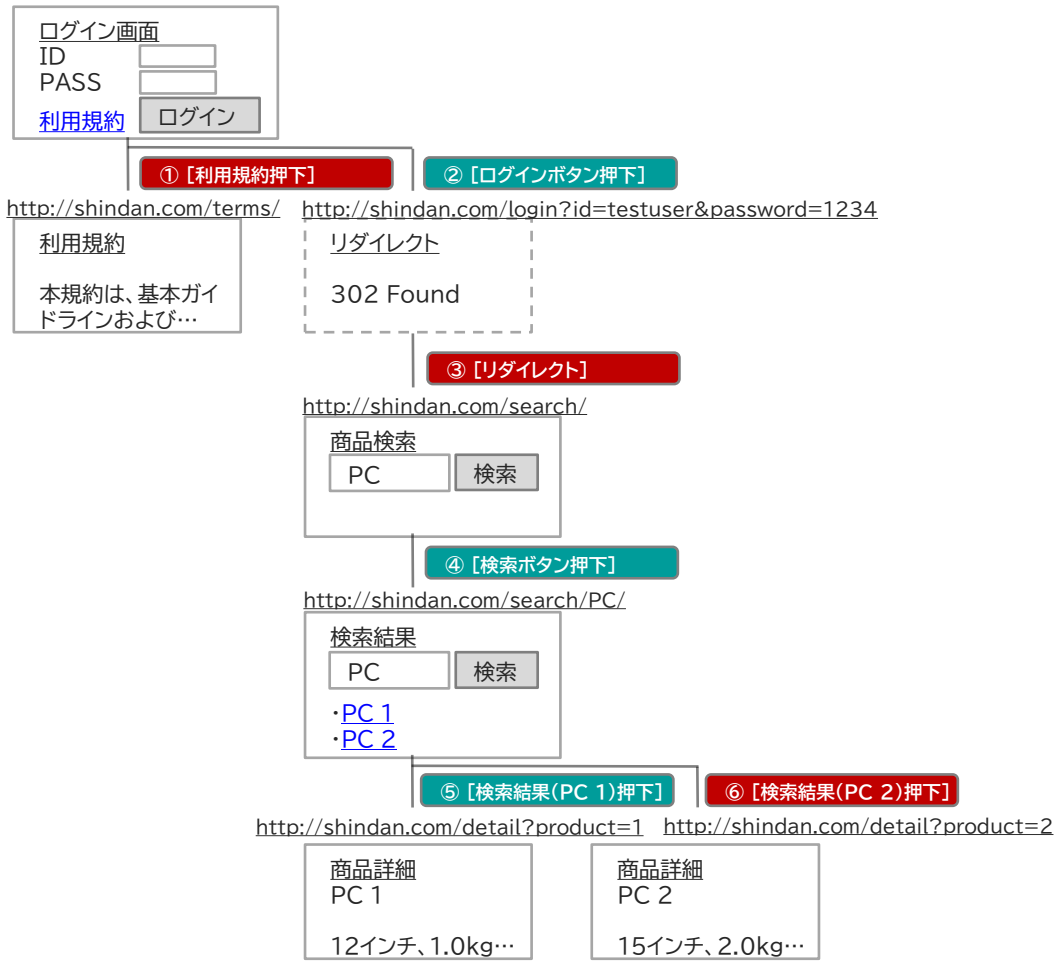
- ネットワーク診断：　　約50万円～
- サーバ構成診断：　　約55万円～
- Webアプリ診断：　　約70万円～
- スマホアプリ診断：　　約85万円～

※ 詳細は、診断対象システムをヒアリングのうえ別途お見積りさせていただきます

【補足】Webアプリ診断の対象HTTPリクエストの考え方

◆診断対象HTTPリクエスト例(ショッピングサイトの画面遷移図)

HTTPリクエストに、GET・POSTパラメータが付与されている箇所が基本的に対象となります。



① 利用規約押下(静的ページへ遷移)
- パラメータ※が無いため、診断対象外です。

② ログインボタン押下(ID・パスワードを送信)
- パラメータ※(id, password)があるため、診断対象です。
- ブラウザに表示されないページやWeb-APIもパラメータ※があれば診断対象になります。

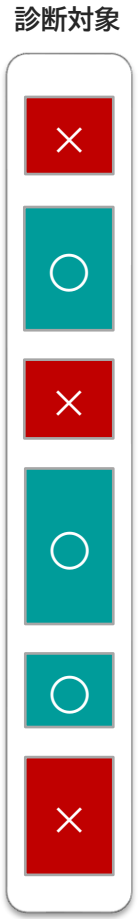
③ リダイレクト(検索ページへ遷移)
- パラメータ※が無いため、診断対象外です。

④ 検索ボタン押下(検索ワードを送信)
- URLの一部にパラメータ※(検索ワード=PC)が埋め込まれているため、診断対象です。
- 画面遷移上、自分自身に戻るような遷移も、パラメータ※があれば診断対象です。

⑤ 検索結果「PC 1」押下(商品コードを送信)
- パラメータ※(product)があるため、診断対象です。

⑥ 検索結果「PC 2」押下(商品コードを送信)
- リクエスト⑤と重複(URLとパラメータ※が同じ組み合わせ)しているため、診断対象外です。(リクエストが重複している場合、何れか1リクエストのみ診断対象とします)

※GET・POSTパラメータ、及びURLの一部に埋め込まれたパラメータ。Cookieは対象外。



診断対象リクエスト数
3リクエスト

①～⑥のように判定し
3リクエストが診断対象

診断対象:②④⑤
診断対象外:①③⑥

【補足】 サイバー保険仕様

■ 対象事故

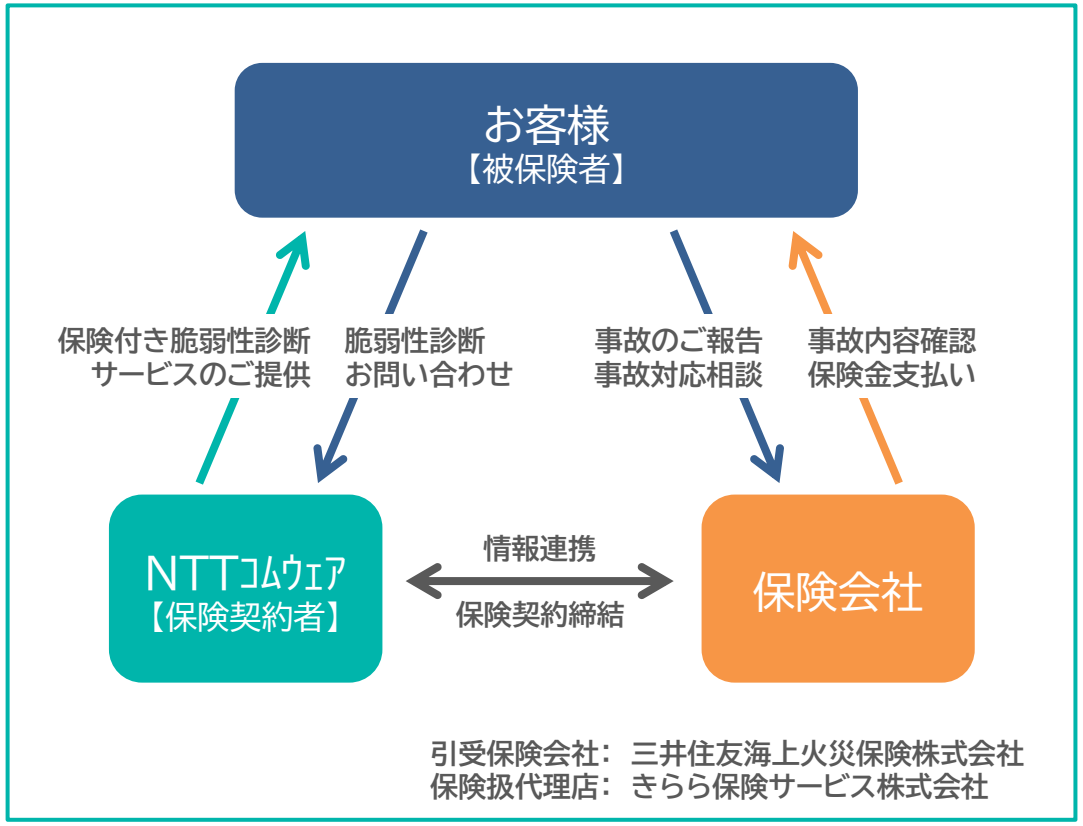
脆弱性診断を受けたシステムがサイバー攻撃等を受け、情報漏えいやそのおそれが生じた場合に、企業が被る損害賠償責任や対応費用を保険で補償

■ 補償内容

賠償損害	費用損害
ア. 法律上の損害賠償金 イ. 争訟費用 ウ. 権利保全行使費用 エ. 訴訟対応費用	オ. 事故対応費用 カ. 事故原因・被害範囲調査費用 キ. 広告宣伝活動費用 ク. 法律相談費用 ケ. コンサルティング費用 コ. 見舞金・見舞品購入費用 サ. クレジット情報モニタリング費用 シ. 公的調査対応費用 ス. コンピュータシステム等復旧費用 セ. 被害拡大防止費用 ソ. 再発防止費用 タ. サイバー攻撃調査費用

支払い限度額：1,000万円（診断契約日から1年間）

■ 対応フロー



引受保険会社：三井住友海上火災保険株式会社
保険扱代理店：きらら保険サービス株式会社

サイバー保険の付帯条件 ▶ 全ての脆弱性診断メニューを対象に、ご契約頂いた金額（総額）が80万円以上（税抜）の場合に無償で自動的に付帯されます。

サイバー保険の条件事項説明 ▶ https://www.nttcom.co.jp/dscb/diagnosis/pdf/imp_matter.pdf