

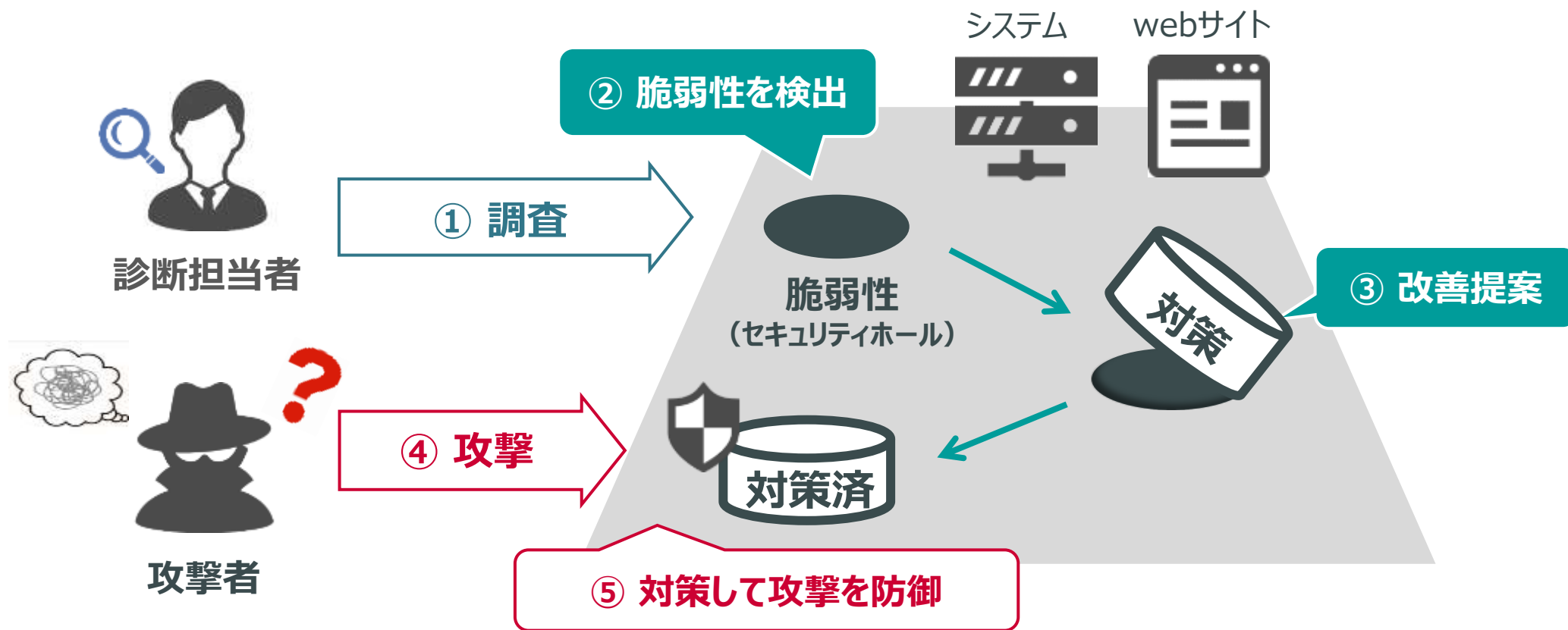
サイバー保険付き

脆弱性診断
サービス



※2021年度実績

システムやWebサイトのセキュリティリスクにつながる**脆弱性を調査**します。
脆弱性が検出された場合、**改善方法をご案内**しますので、セキュリティ対策にお役立て頂けます。



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

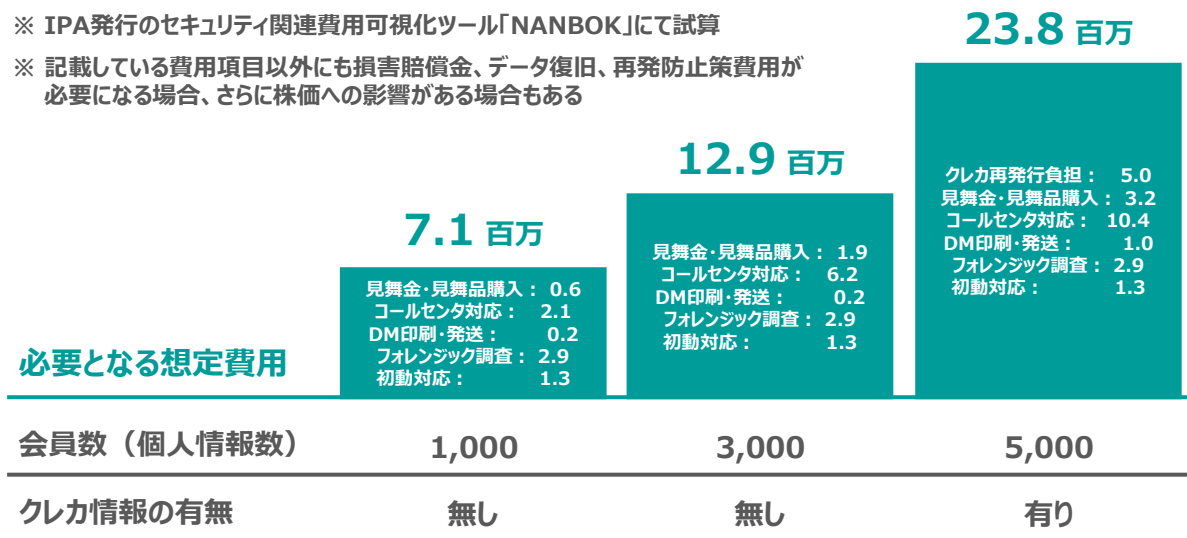
経済産業省通達により**全てのEC系サイトを対象**にサイト自体の脆弱性対策（システム上の設定不備改善、**脆弱性診断**、ウイルス対策等）が**必須化**されます。

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



独立行政法人
情報処理推進機構

経済産業省

ECサイト構築・運用セキュリティガイドライン

(2023年3月16日)

<https://www.meti.go.jp/policy/netsecurity/guideforecsite.html>

・ ECサイトの運用時におけるセキュリティ対策要件一覧

No	セキュリティ対策要件 (運用時)	区分
要件 1	サーバ及び管理端末等で利用しているソフトウェアをセキュリティパッチ等により最新の状態にする。	必須
要件 2	EC サイトへの脆弱性診断を定期的及びカスタマイズを行った際に行い、見つかった脆弱性を対策する。	必須
要件 3	Web サイトのアプリケーションやコンテンツ、設定等の重要なファイルの定期的な差分チェックや、Web サイト改ざん検知ツールによる監視を行う。	必須
要件 4	システムの定期的なバックアップの取得及びアクセスログの定期的な確認を行い不正アクセス等があればアクセスの制限等の対策を実施する。	必要
要件 5	重要な情報はバックアップを取得する。	必要
要件 6	WAFを導入する。	推奨
要件 7	サイバー保険に加入する。	推奨

(2) 「実践編」

<セキュリティ対策要件及び具体的な実践内容>

・ ECサイトの構築時におけるセキュリティ対策要件一覧

No	セキュリティ対策要件 (構築時)	区分
要件 1	「安全なウェブサイトの作り方」及び「セキュリティ実装チェックリスト」に準拠して、ECサイトを構築する。	必須
要件 2	サーバ及び管理端末等で利用しているソフトウェアをセキュリティパッチ等により最新の状態にする。	必須
要件 3	EC サイトの公開前に脆弱性診断を行い、見つかった脆弱性を対策する。	必須
要件 4	管理者画面や管理用ソフトウェアへ接続する端末を制限する。	必須
要件 5	管理者画面や管理用ソフトウェアへ接続する端末のセキュリティ対策を実施する。	必須
要件 6	クレジット取引セキュリティ対策協議会が作成する「クレジットカード・セキュリティガイドライン」を遵守する。	必須
要件 7	サイト利用者情報の登録時及びパスワード入力時における、不正ログイン対策を実施する。	必須
要件 8	サイト利用者の個人情報に対して安全管理措置を講じる。	必須
要件 9	ドメイン名の正当性証明と TLS の利用を行う。	必須
要件 10	サイト利用者のログイン時における二要素認証を導入する。	必要
要件 11	サイト利用者のパスワードの初期化及び変更といった重要な処理を行う際、サイト利用者へ通知する機能を導入する。	必要
要件 12	Web サーバや Web アプリケーション等のログや、取引データ等のバックアップデータを保管する。	必要
要件 13	保管するログやバックアップデータを保護する。	推奨
要件 14	サーバ及び管理端末において、セキュリティ対策を実施する。	推奨

ロシアによるウクライナ侵攻直前(2022年2月)頃から、日本に対してもサイバー攻撃が急増したことから、**各省庁から対策強化に関する注意喚起やメッセージが発信されています。**

内閣サイバーセキュリティセンター (NISC)



サイバーセキュリティ対策の強化に関する注意喚起
(2022年3月)
https://www.nisc.go.jp/pdf/press/20220301NISC_press.pdf

経済産業省



サイバーセキュリティに関する産業界へのメッセージ
(2022年4月)
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/20220411.pdf

警察庁



サイバー空間をめぐる脅威の情勢の情報共有
(2023年3月)
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf

厚生労働省



医療機関等におけるサイバーセキュリティ対策の強化についての注意喚起
(2022年11月)
<https://www.mhlw.go.jp/content/10808000/001011666.pdf>

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

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、設定情報等から脆弱性を洗い出す検査

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

スマホアプリ診断

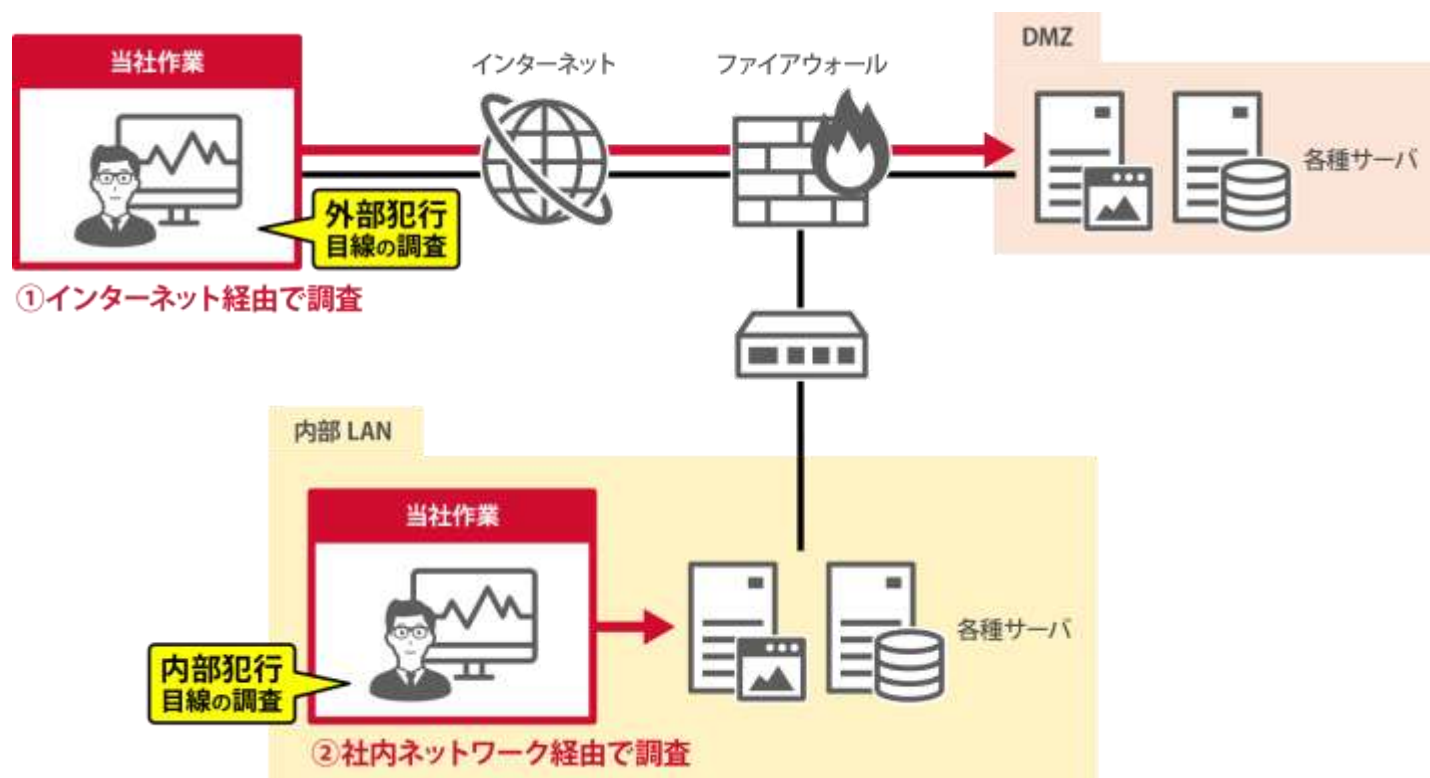


Android/iOSアプリケーションを対象に、アプリ単体の端末検査やアプリ⇔サーバ間の通信路検査を行うことで、Android/iOSアプリに内在する脆弱性を洗い出す検査

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。

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**ネットワーク機器やサーバの脆弱性**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)

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
暗号化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

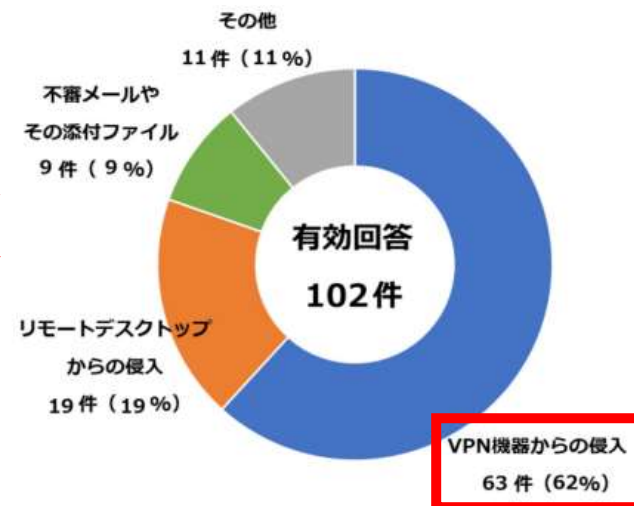
※ インターネット公開サーバ向けの診断項目の一例です。

セキュリティ10大脅威ではランサムウェアによる被害が1位となっており、感染経路としてはVPN機器からの侵入が最も多い。

セキュリティ10大脅威2023(抜粋)

順位	組織
1位	ランサムウェアによる被害
2位	サプライチェーンの弱点を悪用した攻撃
3位	標的型攻撃による機密情報の窃取
4位	内部不正による情報漏えい
5位	テレワーク等のニューノーマルな働き方を狙った攻撃

ランサムウェアの感染経路



関係省庁からの注意喚起

ランサムウェアによる被害の発生やサイバー攻撃事案のリスクの高まりを踏まえ、内閣官房内閣サイバーセキュリティセンター（NISC）や関係省庁から、サイバーセキュリティ対策を強化するよう注意喚起がなされている。

【出典】

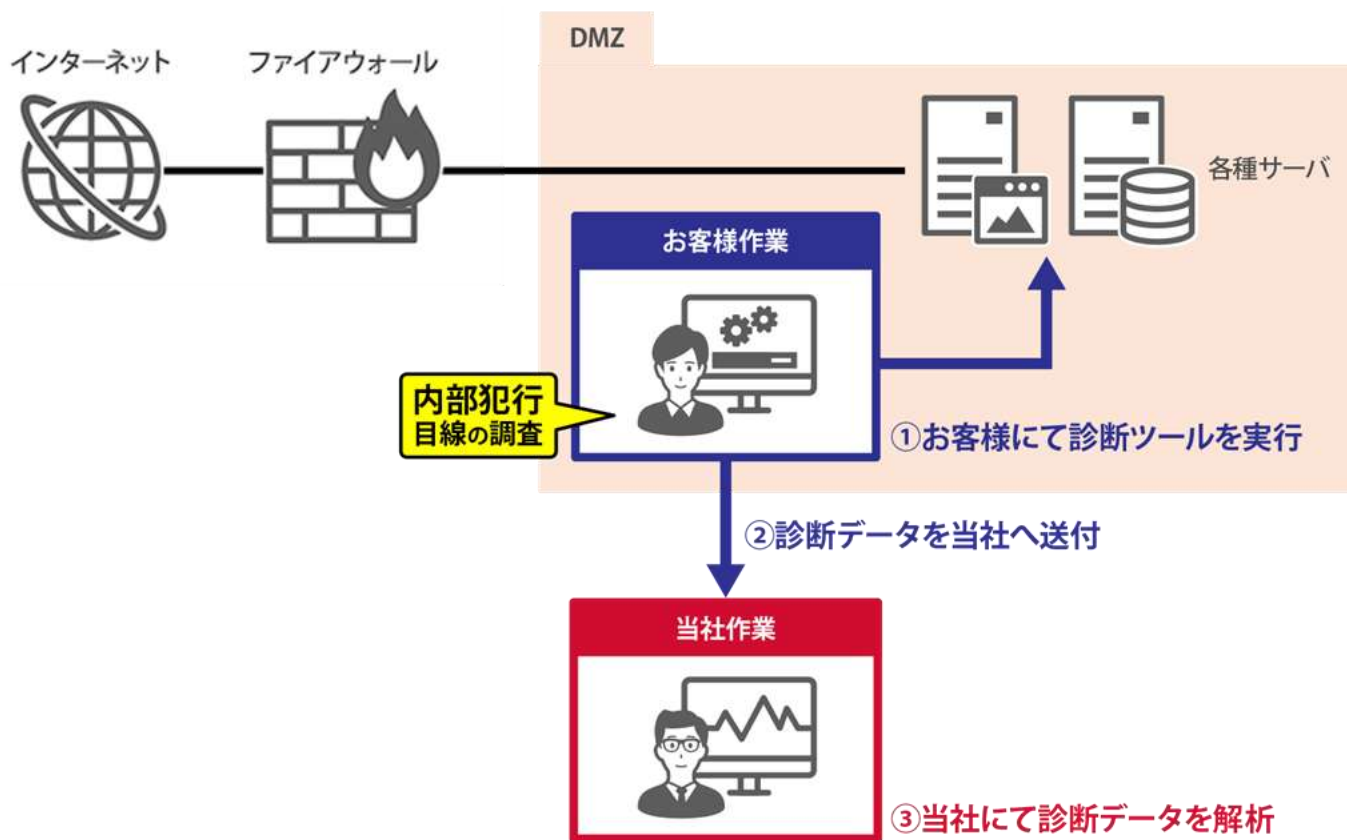
IPA セキュリティ10大脅威 2023

<https://www.ipa.go.jp/security/10threats/10threats2023.html>

警察庁 令和4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/R04_cyber_jousei.pdf

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。



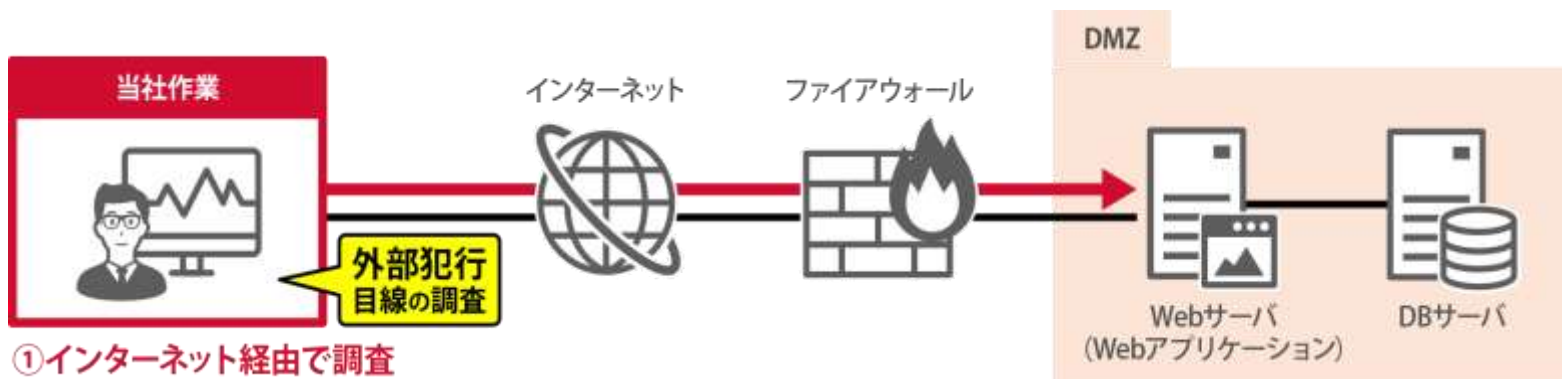
実施手順

- 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

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）

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(HPやECサイト)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

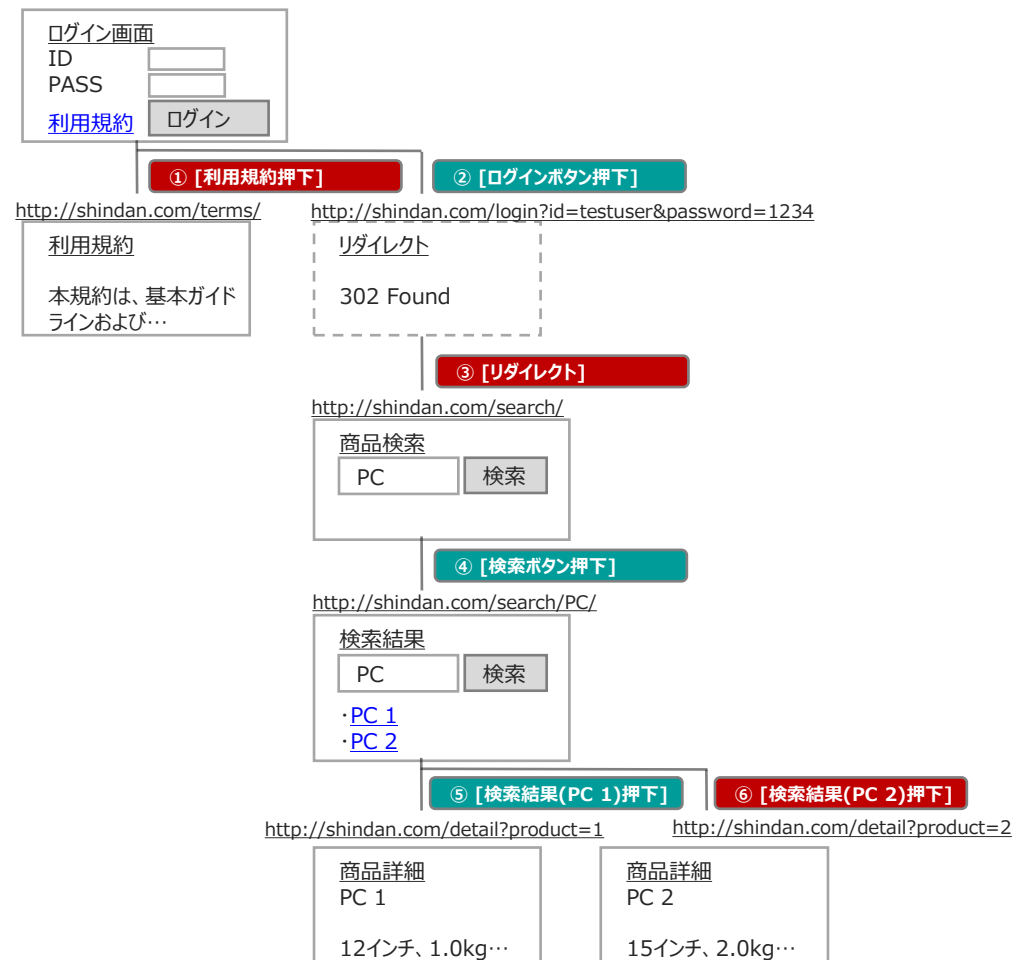
パラメータ毎の脆弱性調査 (手動)

3

診断ツールによる脆弱性調査 (ツール)

◆ 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。



ステップ	説明	診断対象
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）	×

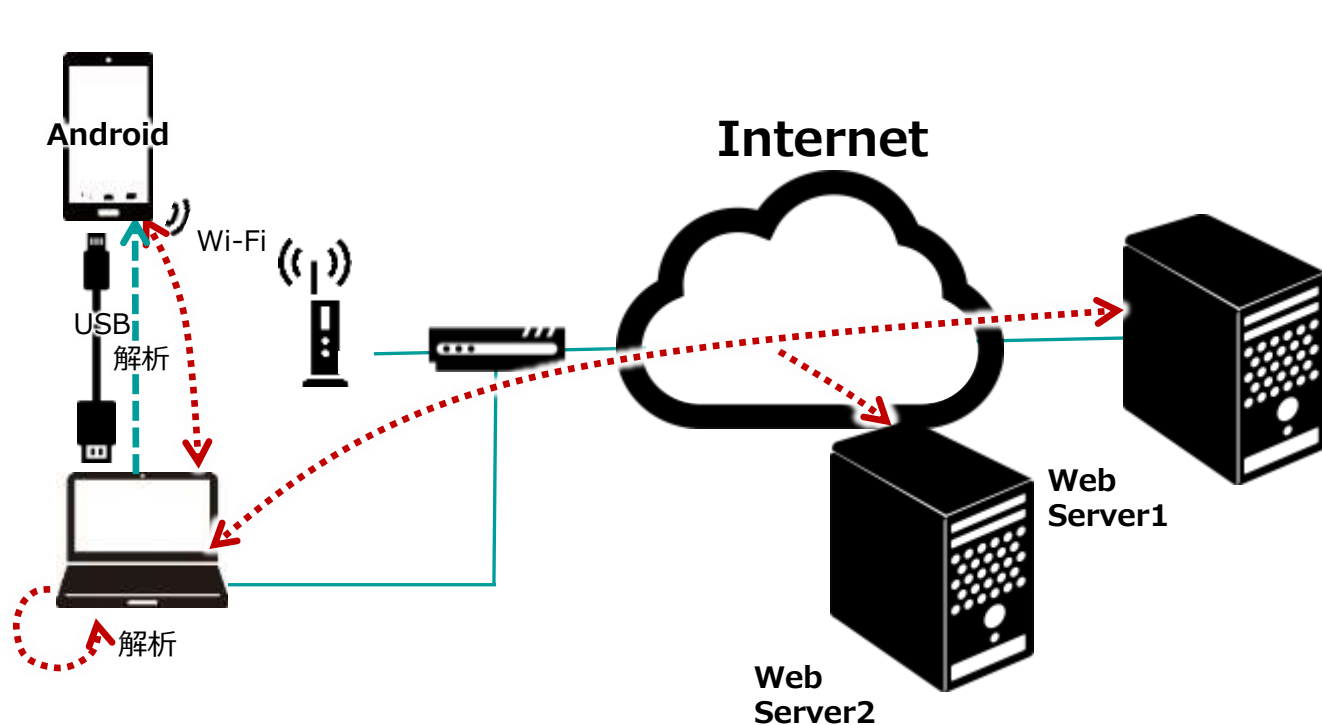
※GET・POSTパラメータ、及びURLの一部に埋め込まれたパラメータ。Cookieは対象外。

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

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

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。

項目名	内容
データ保存の危険性	秘匿とすべき情報の保存場所や保存方法が適切であるか、サードパーティアプリケーションを経由した情報漏えいが発生しない構成であるかを評価します。
クライアント側でのインジェクション攻撃	クライアント側アプリケーションに対するクロスサイトスクリプティングやSQLインジェクション攻撃が可能であるか、電話やSMS等端末特有機能の悪用が可能であるかを評価します。
認証や認可の問題	認証および認可処理が適切に実施されているか(端末IDにのみ依存した認証となっていないか等)を評価します。
信頼できない入力の取り扱い	アプリケーションが外部から呼び出し可能なインターフェース (Intent)を提供する場合の悪用可能性について評価します。
横道(副経路)からのデータ漏えい	サードパーティアプリケーションを経由してログやキャッシュ等から秘匿とすべき情報が漏えいする作りとなっていないかを評価します。
不適切な暗号化	使用している暗号アルゴリズムの強度について評価します。暗号化データの復号を試行し、復号した値に秘匿とすべき情報が含まれているかどうかを評価します。
(リバースエンジニアリングによる)秘匿とすべき情報の漏えい	リバースエンジニアリングの結果、取得可能な情報について評価します。リバースエンジニアリングにより秘匿とすべき情報が取得出来るかどうかを評価します。
過剰なパーミッションの付与	インストール時に過剰なパーミッションが要求される構成となっていないかを評価します。

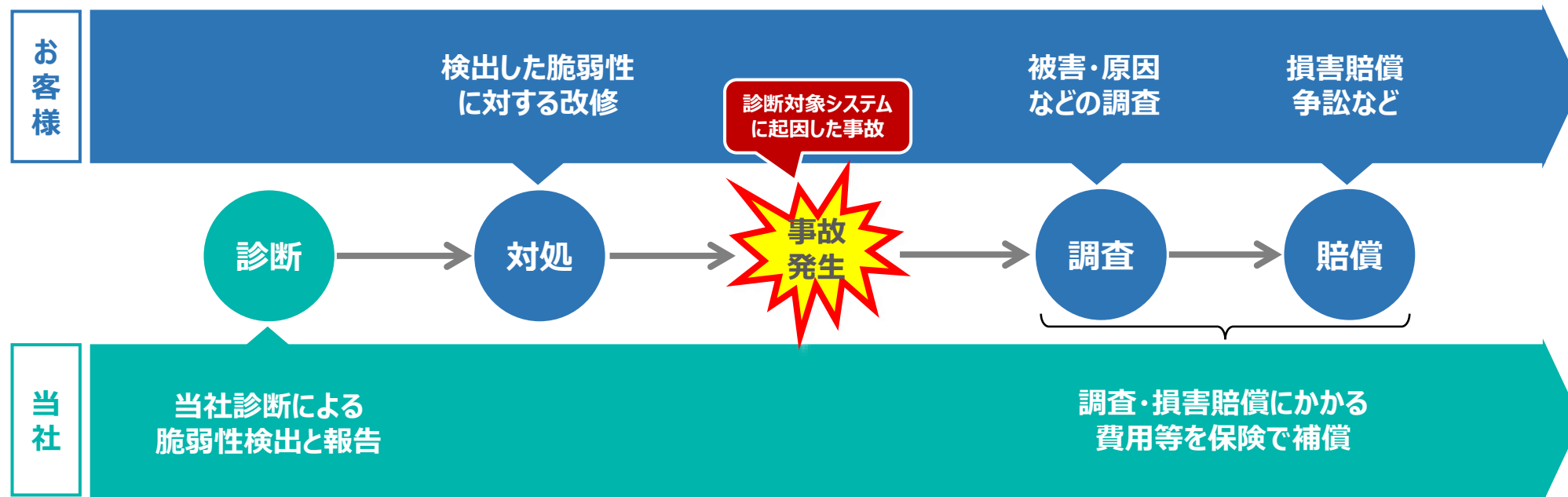
	参考価格（税別）	診断内容（基本料含む）
ネットワーク診断	¥520,000～	グローバル3IP含む
サーバ構成診断	¥590,000～	サーバ3台含む
Webアプリ診断 (スタンダード)	¥730,000～	1リクエスト～
NEW Webアプリ診断 (ライト)	¥380,000～	65画面含む
スマホアプリ診断	¥950,000～	1画面～

※ 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。
 ※ サイバー保険付帯条件は、ご契約額80万円以上(税抜)とさせていただきます。

ドコモの脆弱性診断とは

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。



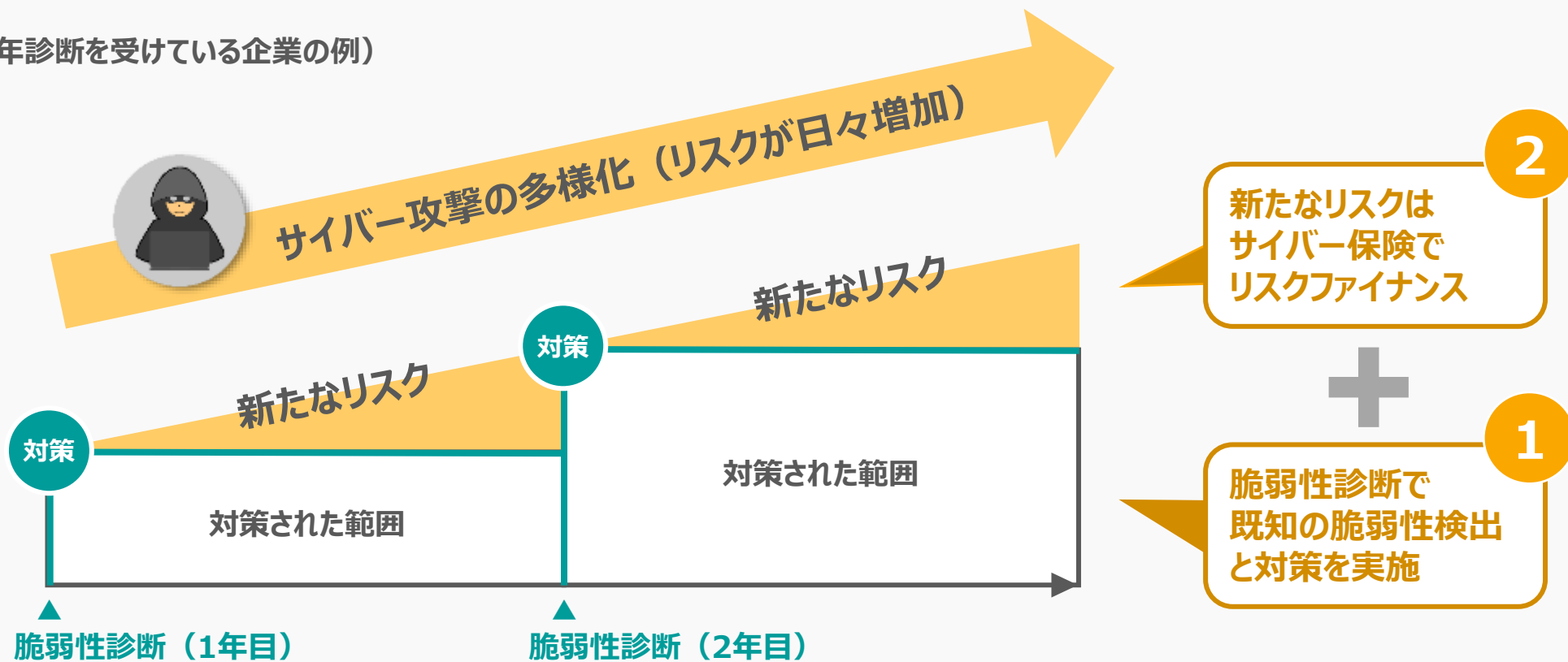
※ サイバー保険は全ての脆弱性診断メニューを対象に、ご契約頂いた金額（総額）が80万円以上（税抜）の場合に無償で自動的に付帯されます。

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

ゼロデイ(未知の脆弱性)に備える必要があります

(毎年診断を受けている企業の例)



■ 対象事故

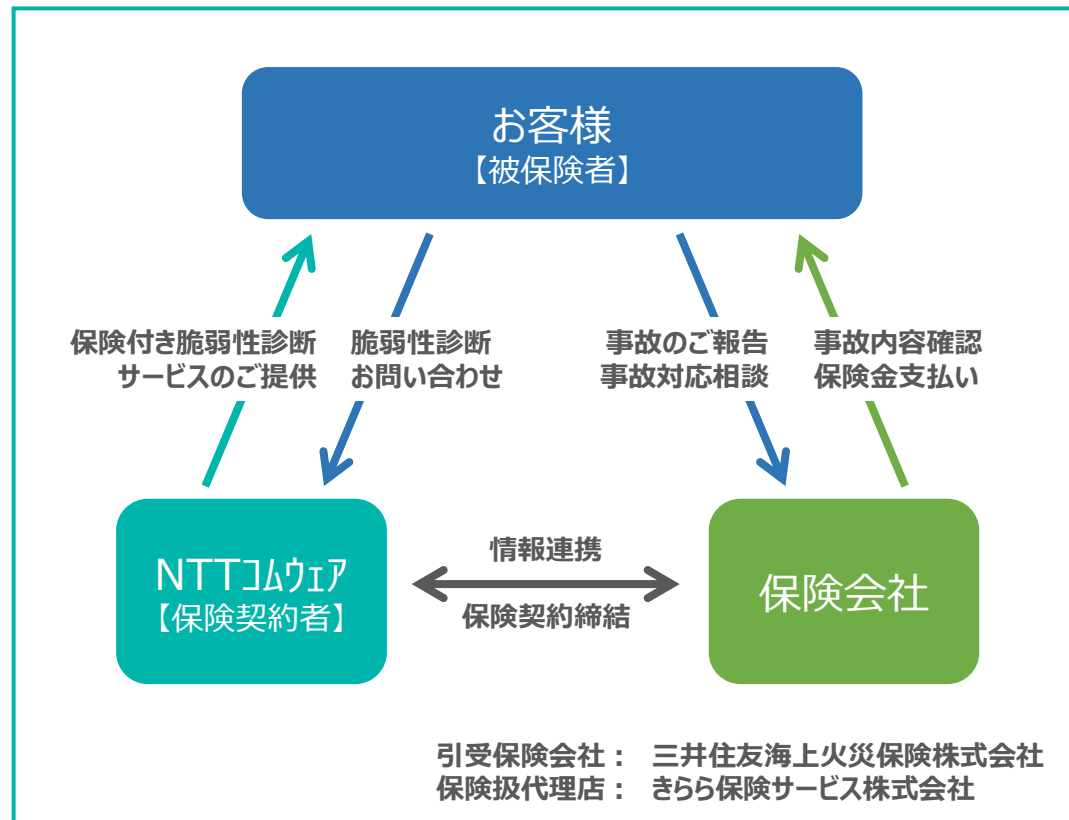
脆弱性診断を受けたシステムがサイバー攻撃等を受け、情報漏えいやそのおそれが生じた場合に、企業が被る損害賠償責任や対応費用を保険で補償

■ 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



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

特徴2 高い品質・培ったスキルによる診断実績

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)

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

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 
019-0013-20
 - ・ 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
- 複数人によるクロスチェックすることで高品質を確保
 - ・ 15～20年の経験のあるベテラン診断士多数在籍。

IPA Better Life with IT 情報処理推進機構

文字サイズ 標準 拡大 検索

・ IPAについて ・ お知らせ一覧 ・ サイトマップ ・ お問い合わせ ・ ENGLISH

HOME 情報セキュリティ 産業サイバーセキュリティセンター 社会基盤センター 未踏/セキュリティキャンプ IT人材の育成 情報処理技術者試験 情報処理安全確保支援士試験

HOME > 情報セキュリティ > 特集コンテンツ > 情報セキュリティサービス基準適合サービスリストの公開

本文を印刷する

情報セキュリティ

情報セキュリティサービス基準適合サービスリストの公開

最終更新日：2022年10月26日
掲載日：2018年6月5日
独立行政法人情報処理推進機構
セキュリティセンター

IPA（独立行政法人情報処理推進機構）では、経済産業省が策定した「[情報セキュリティサービス基準](#)」に適合する情報セキュリティサービスの提供状況について調査を行い、情報セキュリティサービスを利用しようとする者が参照することができるように、調査の結果を以下のとおり情報セキュリティサービス基準適合サービスリストとして公開しております。

情報セキュリティサービス基準適合サービスリスト

情報セキュリティサービス基準適合サービスリストは、経済産業省が策定した「[情報セキュリティサービス基準](#)」への適合性を各審査登録機関^{(*)1}により審査され、同基準に適合^{(*)2}すると認められ、各機関の登録台帳に登録され、併せて、「誓約書」をIPAに提出頂いた事業者の各情報セキュリティサービスを掲載するものです。本リストの掲載期間は、審査登録機関の定める登録有効期間又は2年間のうち短い方の期間となります。本リストの内容は、各登録台帳の登録内容を原則としてそのまま掲載^{(*)3}（一

情報セキュリティ

- > 脆弱性対策情報
- > 届出・相談・情報提供
- > 特集コンテンツ
 - > 今月の呼びかけ
 - > 内部不正対策
 - > セキュア・プログラミング講座
 - > ウェブサイト攻撃の検出ツール iLogScanner
 - > クラウドサービス安全利用のツール
 - > 安全なウェブサイトの作り方
 - > 知っていただく脆弱性



当社の脆弱性診断サービスは

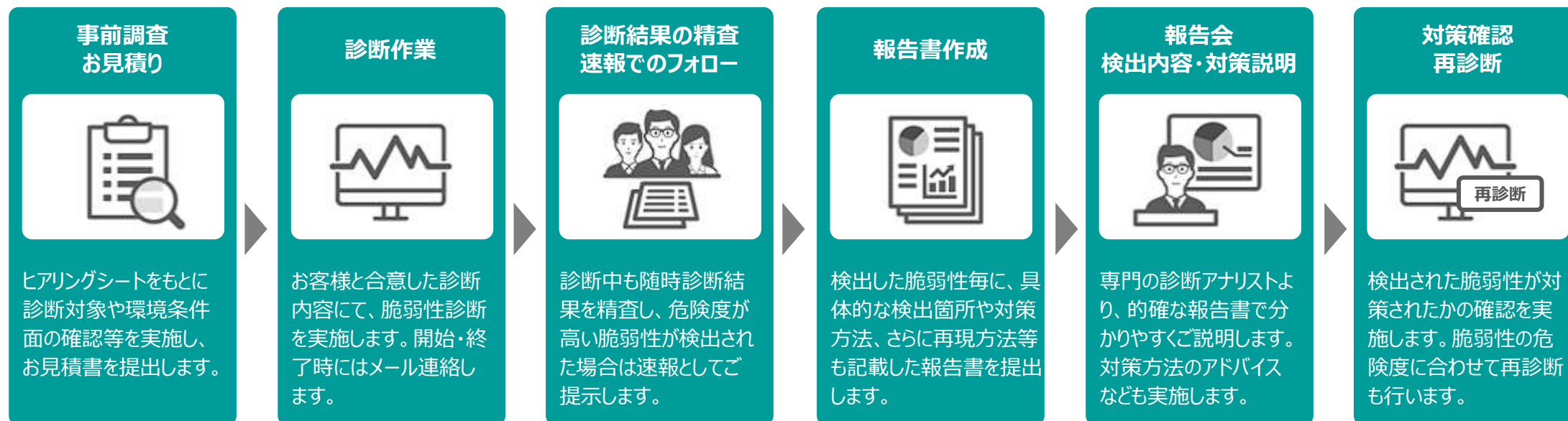
「情報セキュリティサービスに関する審査登録機関基準」

を満たしています

参照先：https://www.ipa.go.jp/security/it-service/service_list.html

特徴3 充実したアフターフォロー

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、対策状況の確認を実施します。
(診断報告書提出後、再診断は、3カ月以内に3回まで実施可能※ネットワーク診断、Webアプリケーション診断のみ)
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。



特徴4 的確な診断報告書の提示

検出した脆弱性毎に、具体的な検出箇所を記載した報告書を提出します
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

サイバー保険付き脆弱性診断サービス
Webアプリ診断ライト版のご紹介

「低コスト」のお客様ニーズに応えるべく、「Webアプリ診断ライト版」の提供を開始しました。
「ライト版」はツールのみの診断となり、「スタンダード版」は手動+ツールの診断となります。

NEW

Webアプリ診断 (ライト版)

診断に掛かる費用を極力抑えたい

定期的な診断の実施、及び診断結果の迅速性を優先したい

一般的(※)なセキュリティの問題や脆弱性を特定したい

大規模アプリケーションの診断を短期間で実施したい

Webアプリ診断 (スタンダード版)

アプリケーション全体を網羅的に診断したい

特定の条件や企業独自のビジネスルールに基づく脆弱性を検知したい

一般的な攻撃手法だけでなく、高度な攻撃手法にも備えたい

検知した脆弱性に対して、専門家のアドバイスをもらいたい

(※) OWASP (TOP10、ASVS4.0)、IPA (安全なウェブサイトの作り方) に対応

「ライト版」は、下記のようなサイトの診断に適しています。
「ライト版」での診断が難しい場合は、「スタンダード版」での診断をお勧めします。

「ライト版」が得意なサイト



- ✓ 認証方法がシンプル
- ✓ 入力項目が少ない、シンプル

例)

- コーポレートサイト
- オウンドメディア
- ブランドサイト
- コミュニティサイト

「ライト版」が不得意なサイト



- ✓ 認証方法が複雑
- ✓ 入力項目が多く、チェックが複雑

例)

- サービス/ECサイト
- 多要素認証（MFA）サイト
- 人事/会計などの業務系サイト
- 銀行/証券などの金銭取扱いサイト

それぞれに特長がありますので、お客様のご要望と当社の知見を踏まえ、最適なサービスをご提案させていただきます。

	ライト版	スタンダード版
診断対象	Webアプリケーション	Webアプリケーション
診断手法	ツール	ツール + 手動
誤検知/過検知の精査	なし（オプション対応）	セキュリティ専門家による精査
診断対象範囲	画面遷移図ベース（上限：65画面）	リクエストベース（上限：なし）
診断結果（速報）	なし	あり
診断結果報告書	あり（ライト版用）	あり
診断結果報告会（Web）	なし（オプション対応）	あり（無償）
再診断	なし	あり（無償）
IPA情報セキュリティサービス基準	適合	適合
サイバー保険	対象（上限1,000万円/件） （※ご契約金額：80万円以上）	対象（上限1,000万円/件） （※ご契約金額：80万円以上）

注）一般的にツールによる診断は、ツールの特性上、Webサイトの構成によって向き/不向きがあります。
「ライト版」のご契約締結前に、診断対象となるWebサイトの適合状況について確認/ヒアリングさせていただきます。

