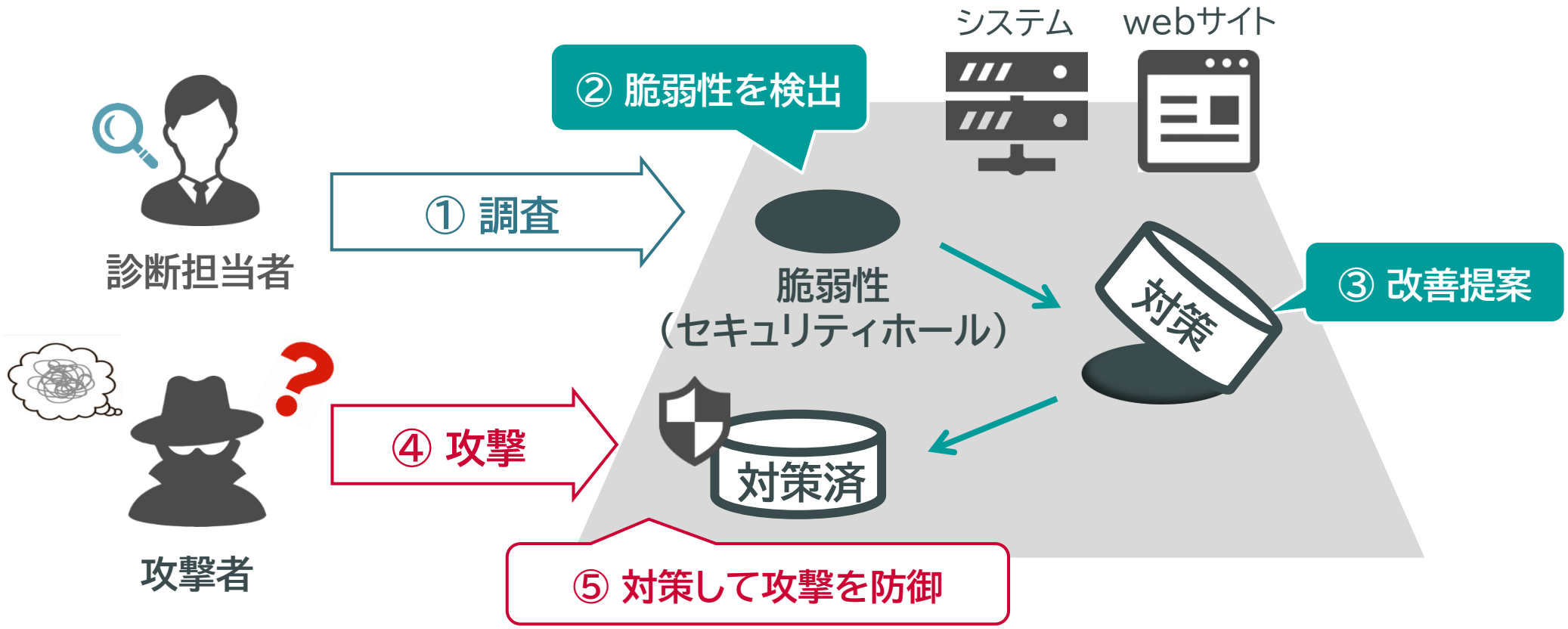


サイバー保険付き
脆弱性診断サービスのご紹介

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

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。



Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

企業様がご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？

セキュリティ対策評価制度の導入

経済産業省は、サプライチェーン全体の安全性向上を目的に、企業の**セキュリティ対策状況を共通基準で可視化**する評価制度を導入します。

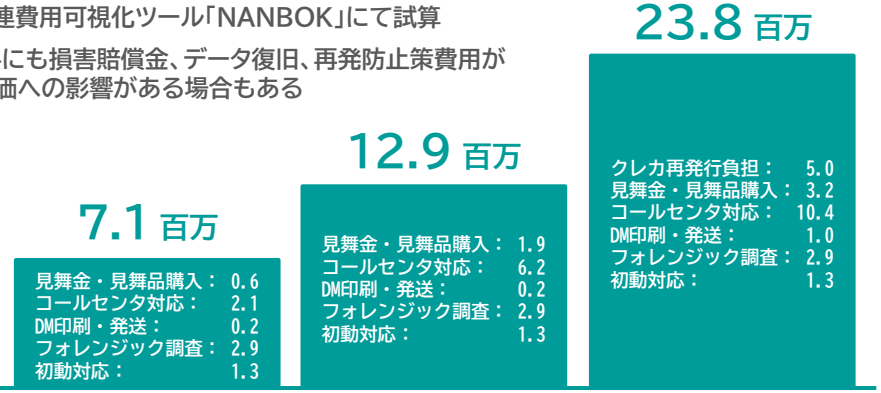
どうする？

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	7.1 百万	12.9 百万	23.8 百万
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

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

【補足】ECサイト構築・運用セキュリティガイドライン「実践編」

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

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

【補足】サプライチェーン強化に向けたセキュリティ対策評価制度

独立行政法人
情報処理推進機構　　経済産業省

サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針

（2025年12月26日）
https://www.meti.go.jp/press/2025/12/20251226001/20251226001.html

構築する評価制度（案）

成熟度の定義	★3	★4	★5
想定される脅威	• 広く認知された脆弱性等を悪用する一般的なサイバー攻撃	• 供給停止等によりサプライチェーンに大きな影響をもたらす企業への攻撃 • 機密情報等、情報漏えいにより大きな影響をもたらす資産への攻撃	• 未知の攻撃も含めた、高度なサイバー攻撃
対策の基本的な考え方	全てのサプライチェーン企業が**最低限実装すべき**セキュリティ対策： • 基礎的な組織的対策とシステム防御策を中心に実施	サプライチェーン企業等が**標準的に目指すべき**セキュリティ対策： • 組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等包括的な対策を実施	サプライチェーン企業等が到達点として目指すべき対策： • 国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善工程を整備、システムに対しては現時点でのベストプラクティスの対策を実施
評価スキーム	**専門家確認付き自己評価**	**第三者評価**	第三者評価

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

【参考】直各省庁から発信されている注意喚起の例

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。

国家サイバー統括室（NCO）	サイバーセキュリティ対策の強化に関する注意喚起 https://www.cyber.go.jp/news/press/tyuuikanki.html
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 https://www.meti.go.jp/policy/netsecurity/message.html
警察庁	サイバー空間をめぐる脅威の情勢など https://www.npa.go.jp/publications/statistics/cybersecurity/index.html
厚生労働省	医療分野のサイバーセキュリティ対策について https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

診断メニュー

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

脆弱性診断メニュー

ネットワーク診断



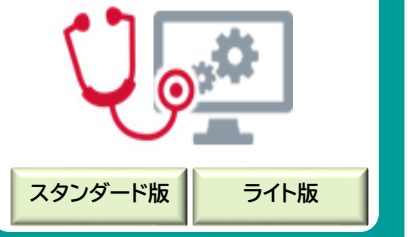
インターネットに公開しているWebサーバやNW機器等、社内ネットワークに接続しているサーバ等を対象に、ネットワーク経由でサーバ等に内在する脆弱性を洗い出す検査です

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



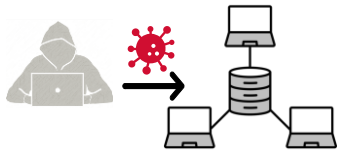
Webアプリケーション（動的に遷移するWebページ）を対象に、Webアプリケーションに内在する脆弱性を診断技術者がツールと手作業できめ細かく洗い出す検査です

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

ペネトレーションテスト



対象システムへの侵入／侵害可否をを確認するため、専門家が疑似サイバー攻撃を実施し、セキュリティ課題やサイバー攻撃耐性を確認する検査です

サイバー保険

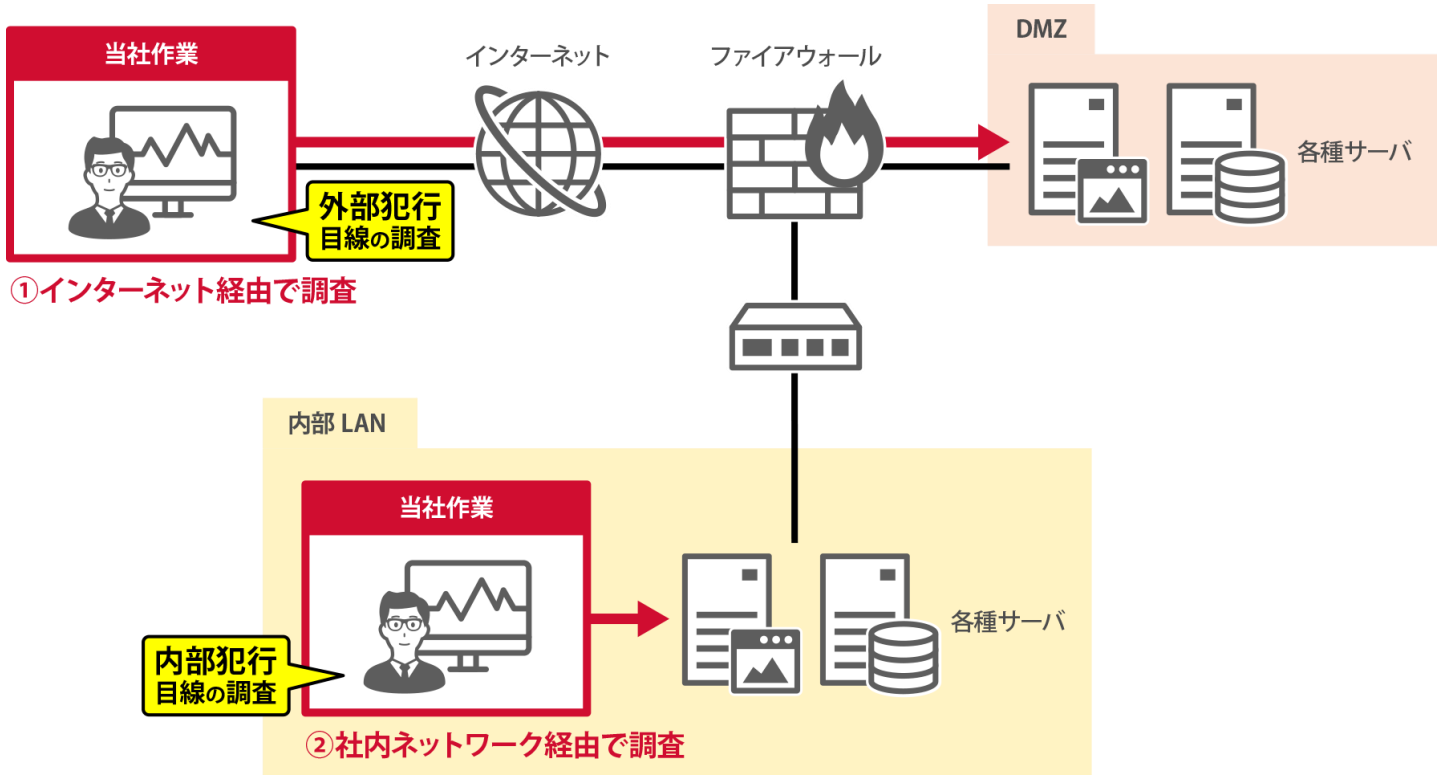
診断対象システムに起因して発生した情報漏えい等の損害リスクを**サイバー保険で補償**します。

※サイバー保険の補償範囲は診断メニューにより異なります

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

ネットワーク診断　概要

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)

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

ネットワーク診断　診断項目一例

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。

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

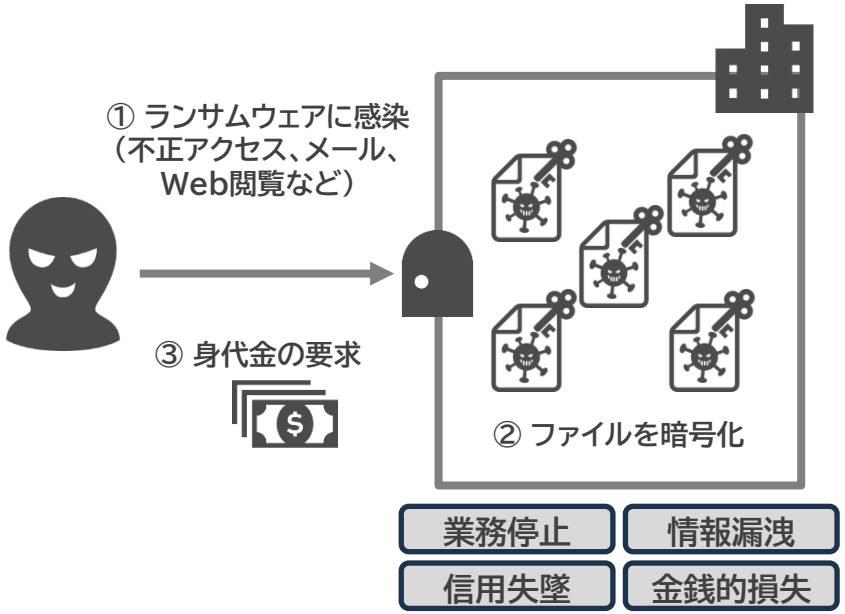
【参考】ランサムウェアによる被害が1位

IPA(独立行政法人 情報処理推進機構)「セキュリティ10大脅威2026」において、
ランサム攻撃(※)による被害が**6年連続で第1位！**

ランサム被害額
平均:1億7千万円

【セキュリティ10大脅威2026(上位5つ抜粋)】

順位	被害内容
1位	ランサム攻撃による被害
2位	サプライチェーンや委託先を狙った攻撃
New 3位	AIの利用をめぐるサイバーリスク
4位	システムの脆弱性を突いた攻撃
5位	機密情報等を狙った標的型攻撃



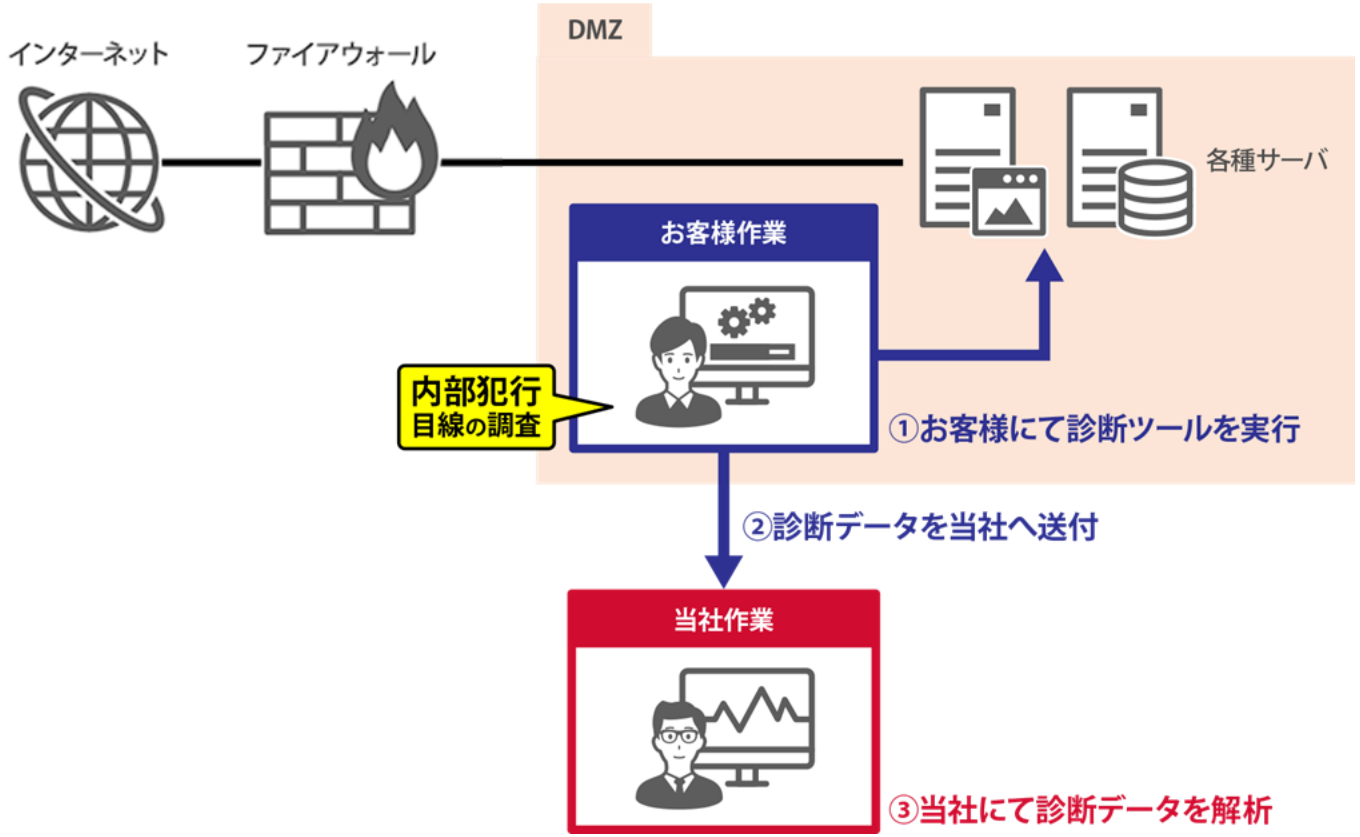
(※)ランサム(身代金)攻撃 ・・・ 被害者から金銭を要求するサイバー攻撃全般。
技術的な攻撃方法を限定するものではなく、フィッシングなどを含む様々な方法で金銭を要求する。
ランサム攻撃のなかで、特にマルウェア(不正なソフトウェアの総称)を使用した攻撃を、ランサムウェア攻撃という。

出典:情報セキュリティ10大脅威 2026｜情報セキュリティ｜IPA 独立行政法人 情報処理推進機構

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

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

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

サーバ構成診断　診断項目一例

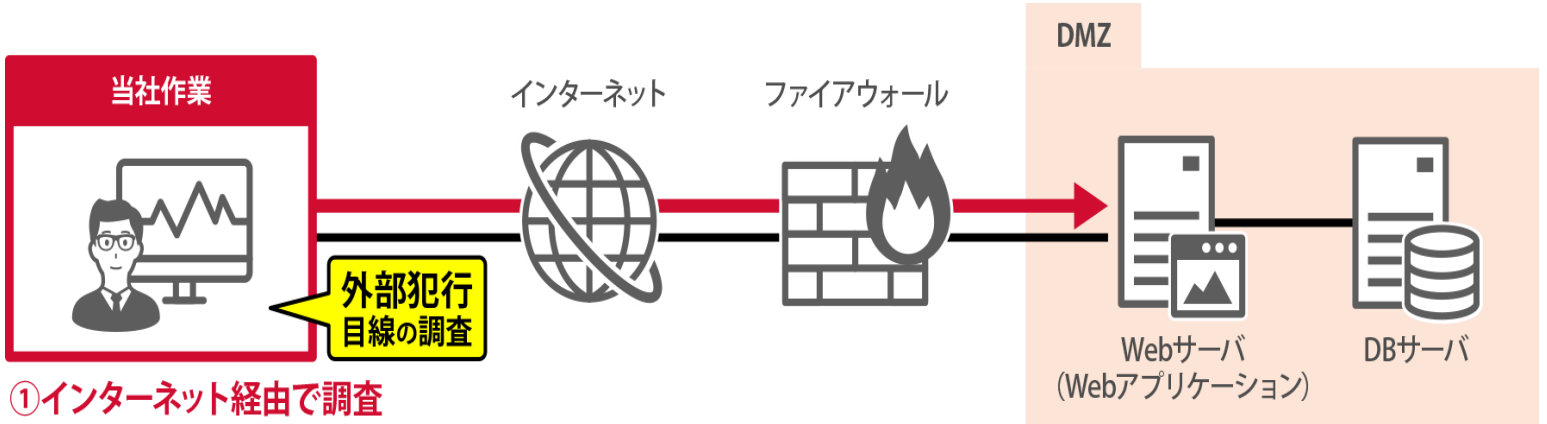
診断項目	内容
脆弱なパスワード	パスワード設定なし、アカウントと同じパスワード、桁数が極端に少ない パスワード等々の脆弱なパスワードに設定されているアカウントの確認
セキュリティパッチの未適用	OSのセキュリティパッチ（Microsoftのセキュリティ修正プログラム、 RedHatのRPM等）の適用状況を確認し、未適用パッチの確認
ウイルス対策ソフトの導入チェック	ウイルス対策ソフトが導入されているかどうか、 またウイルス定義ファイルが更新されているか確認
アクセス権の設定不備	共有フォルダ等に不適切なアクセス権が付与されていないか確認 ※Everyoneグループにフルアクセス権付与　等
セ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

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

Webアプリ診断（スタンダード版） 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（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）

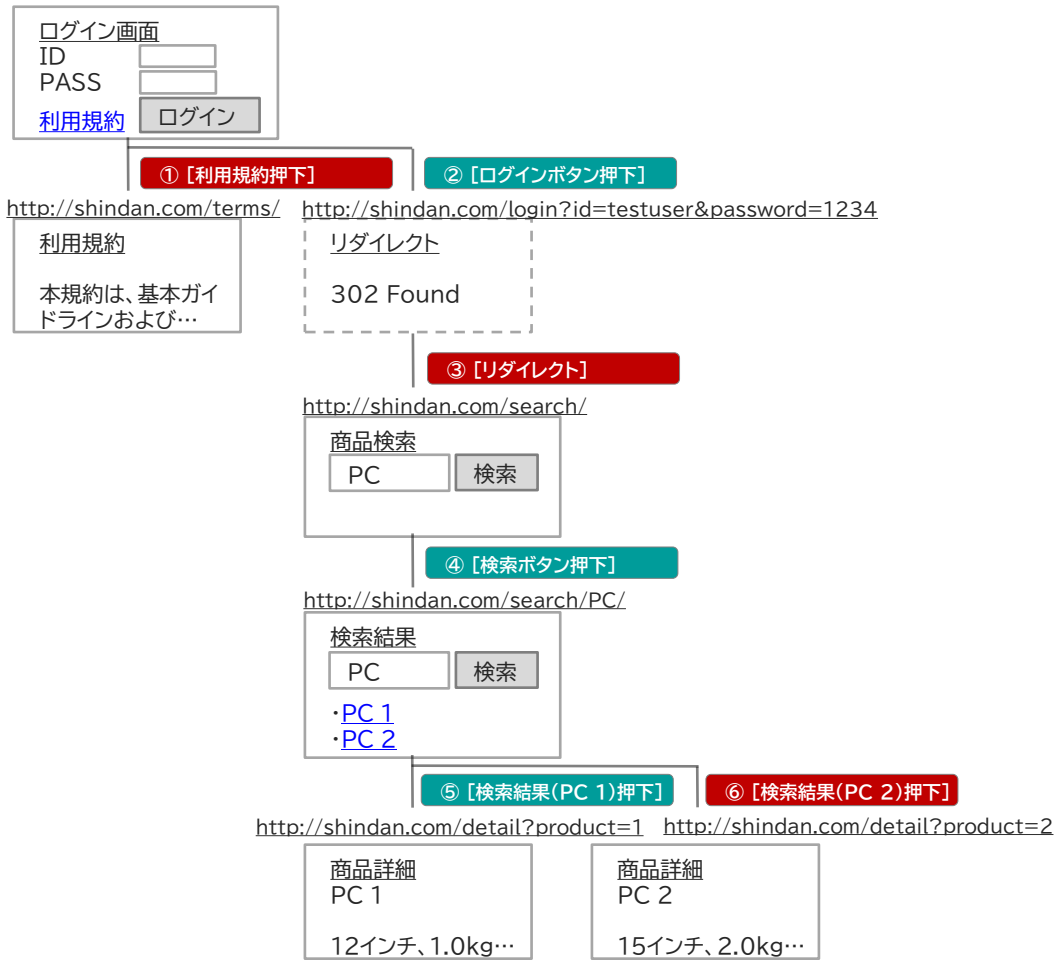
診断の単位 ：リクエスト数

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

【参考】Webアプリ診断(スタンダード版)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
①	×
②	○
③	×
④	○
⑤	○
⑥	×

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

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

Webアプリ診断（ライト版） 概要

「低コスト」、「短納期」などのお客様ニーズに応えるべく、新たに「Webアプリ診断（ライト版）」の提供を開始しました。



「ライト版」を求めるお客様ニーズ	
ニーズ①	診断に掛かる費用を極力抑えたい
ニーズ②	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
ニーズ③	一般的なセキュリティの問題や既知の脆弱性を特定したい
ニーズ④	大規模アプリケーションの診断を短期間で実施したい

診断の単位：画面数

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

Webアプリ診断「ライト版」と「スタンダード版」の違い

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
診断期間（診断開始から報告書の提示まで）	約4営業日	約1～2か月 （サイトの規模に比例）
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。

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

Webアプリ診断「ライト版」と「スタンダード版」の違い

「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

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

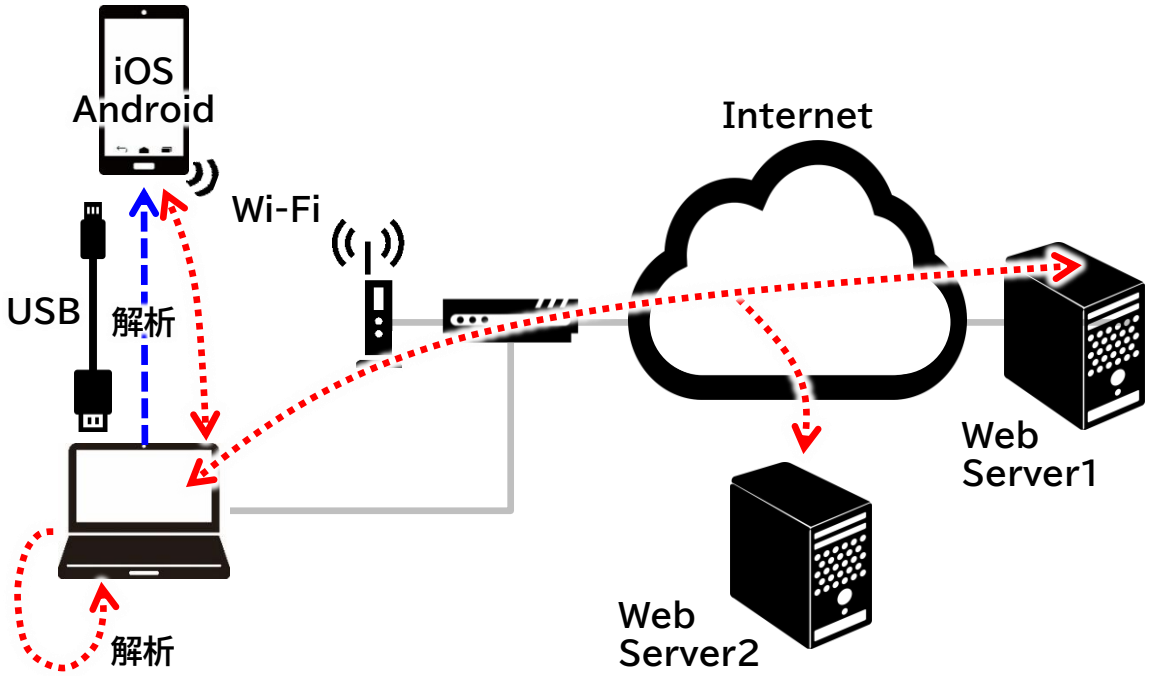
Webアプリ診断（ライト版/スタンダード版） 診断項目例

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

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

スマホアプリ診断　概要

端末にDLするスマホアプリの診断では、スマホアプリが通信するWebサイト側で発生する問題を診断する**「通信路検査」**と、端末側の問題を診断する**「端末検査」**があります。





① 通信路検査

スマホアプリのWebAPIに対する脆弱性を診断します。診断項目はWebアプリ診断と同様の項目になります。

診断の単位：リクエスト数



② 端末検査

スマホアプリを動作させ、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。

診断の単位：画面数

※当社では、原則として**「通信路検査」**、**「端末検査」**の両方の実施を推奨しておりますが、お客様のご要望/ご予算に応じて、いずれか一方のみの診断についても、ご相談に応じます。

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

スマホアプリ診断「通信路検査」 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

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

スマホアプリ診断「端末検査」 診断項目例

診断項目	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。

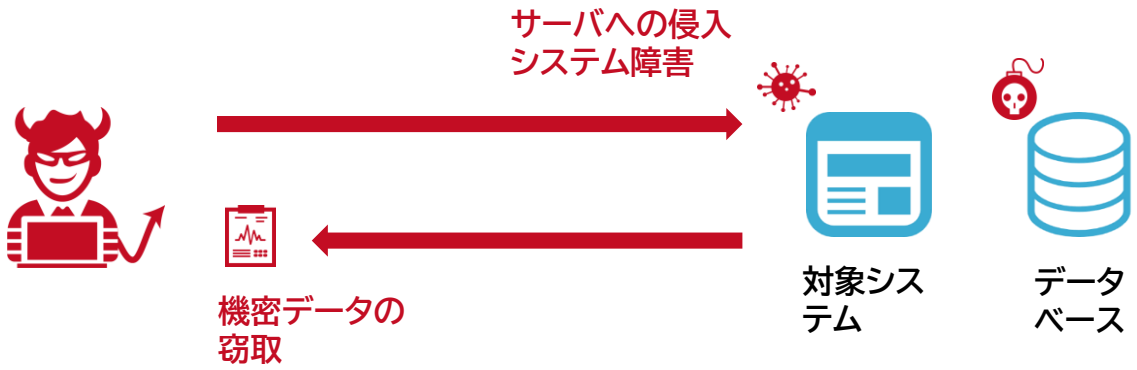
Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

ペネトレーションテスト　概要

実際の攻撃を想定した検証を行い、システムに侵入できるか、侵入された場合にどのような影響が及ぶかを実践的に確認するテストです。

① 外部ペネトレーションテスト

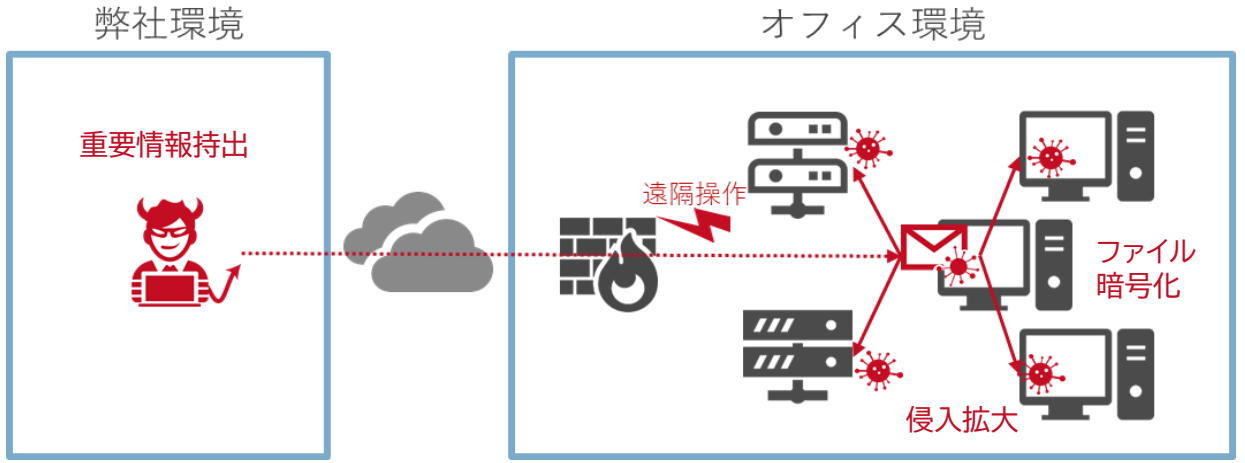
主に「侵入可否の検証」という点に焦点を当てた、対象のサーバーへNWの外部から侵入/攻撃するテストです。



プラン	
サーバ侵入 外部公開しているサーバに対して侵入可否を検証	**Webアプリ侵入** Webアプリに対して侵入可否を検証

②内部ペネトレーションテスト

主に侵入できている前提で「どこまでの範囲に侵入／侵害が可否の検証」という点に焦点をあてたテストです。



プラン	
マルウェア感染検証 標的型攻撃に対して検知／除去できるかを検証	**オフィスハッキング** オフィス内ネットワークの耐性を検証

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

①外部ペネトレーションテスト　検査項目例

検査項目	内容
設定不備への攻撃	OSや各種サービス設定の不備を利用し、情報収集/侵入を図ります。
ソフトウェアの欠陥への攻撃	サービスに想定しないデータを与え、サービスやOSの制御を奪取します。
メールの不正中継	メールサービスが迷惑メールの踏み台に利用されないか調査します。
パスワードクラッキング	対象ホストのパスワードハッシュを入手した場合、解析を試みます。
辞書攻撃	認証サービスに対しID/パスワードを推測し、ログインを試みます。
侵入後の活動	侵入に成功したホストを操作し、情報収集/権限昇格を試みます。

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

②内部ペネトレーションテスト　検査項目例

検査項目	内容
マルウェア検知	疑似的にマルウェアを送付・起動し、EDR/NDR製品の検知性能を検証します。
C2通信	C2（Command & Control）通信の確立可否を検証します。
情報持出・実行影響	感染後の情報持ち出しや暗号化（ランサムウェア）実行の影響を確認します。
AD／サーバ侵害	Active Directoryやファイルサーバへのアクセスを試行します。
メール・プロキシ設定	メールフィルタやプロ式設定の有効性を検証します。
IDS／IPS効果	IDS/IPS導入有無による攻撃成功率の差異を検証します。

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

診断の流れ

事前調査から診断、報告、対策確認までを一連の流れとして実施します。当社作成の報告書に基づき、お客様にて対策を実施いただいた後、対策状況の確認（再診断）まで対応します。
※本フローはすべての診断メニューに共通する基本フローです。

目的の決定

- 診断目的の明確化
- 実施プロセスの定義

セキュリティ対策に対する不安や状況を打ち合わせにより明確にします。

範囲の特定

- 診断範囲を特定
- 調査機関の確定
- 見積書の提出

ヒアリングシートに基づいて仕様を決め、契約となります。

実施の調整

- スケジュール確定
- 診断事前準備
- 診断実施

診断実施するシステムの起動や調査に必要な対応をお願いします。

結果の報告

- 報告会の開催
- 報告書提出

緊急性の高い脆弱性が判明した場合には、診断途中でも報告をすることがあります。

対策の実施

- システム対策実施

お客様にて報告書に基づき対策を実施していただきます。

再診断

- 対策後の再診断

対策後、再度診断を実施し、有効な対策が実施されているか確認します。

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

価格の目安

	参考価格(税別)	診断内容(基本料含む)
ネットワーク診断	¥550,000～	グローバル3IP含む
サーバ構成診断	¥600,000～	サーバ3台含む
Webアプリ診断（スタンダード）	¥700,000～	1リクエスト～
Webアプリ診断（ライト）	¥400,000～	65画面含む
スマホアプリ診断	¥950,000～	1画面～
ペネトレーションテスト	個別見積	別途お問合せください

※ 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。

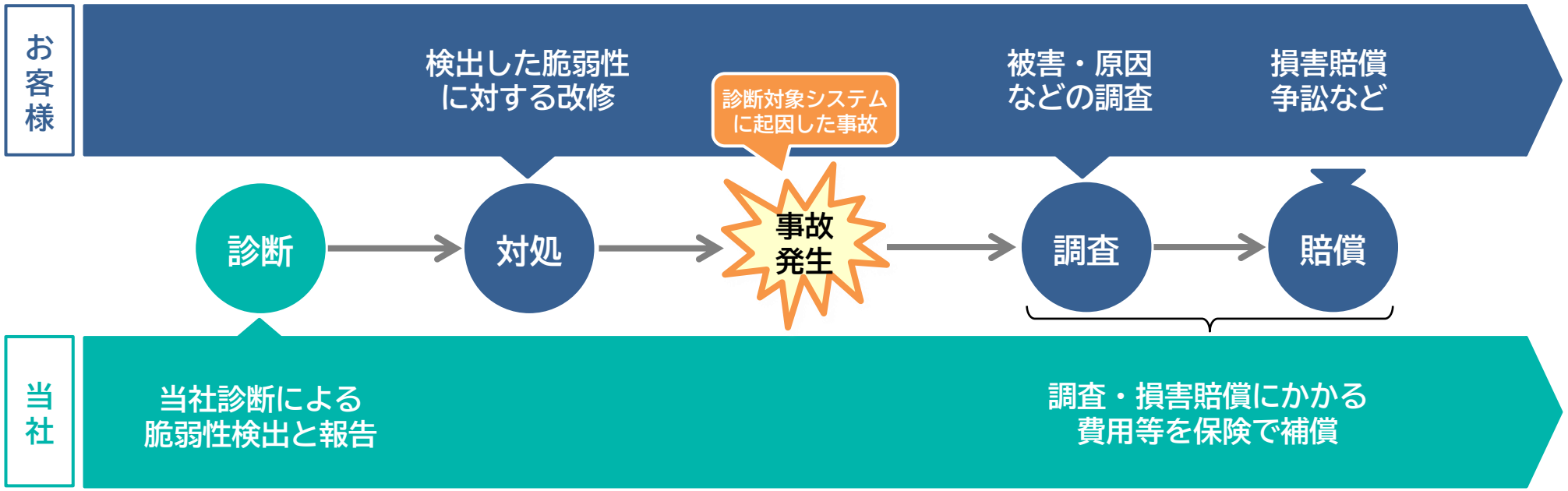
Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

NTTドコモソリューションズの脆弱性診断とは

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

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。

（ サイバー保険の補償範囲は診断メニューにより異なります ）

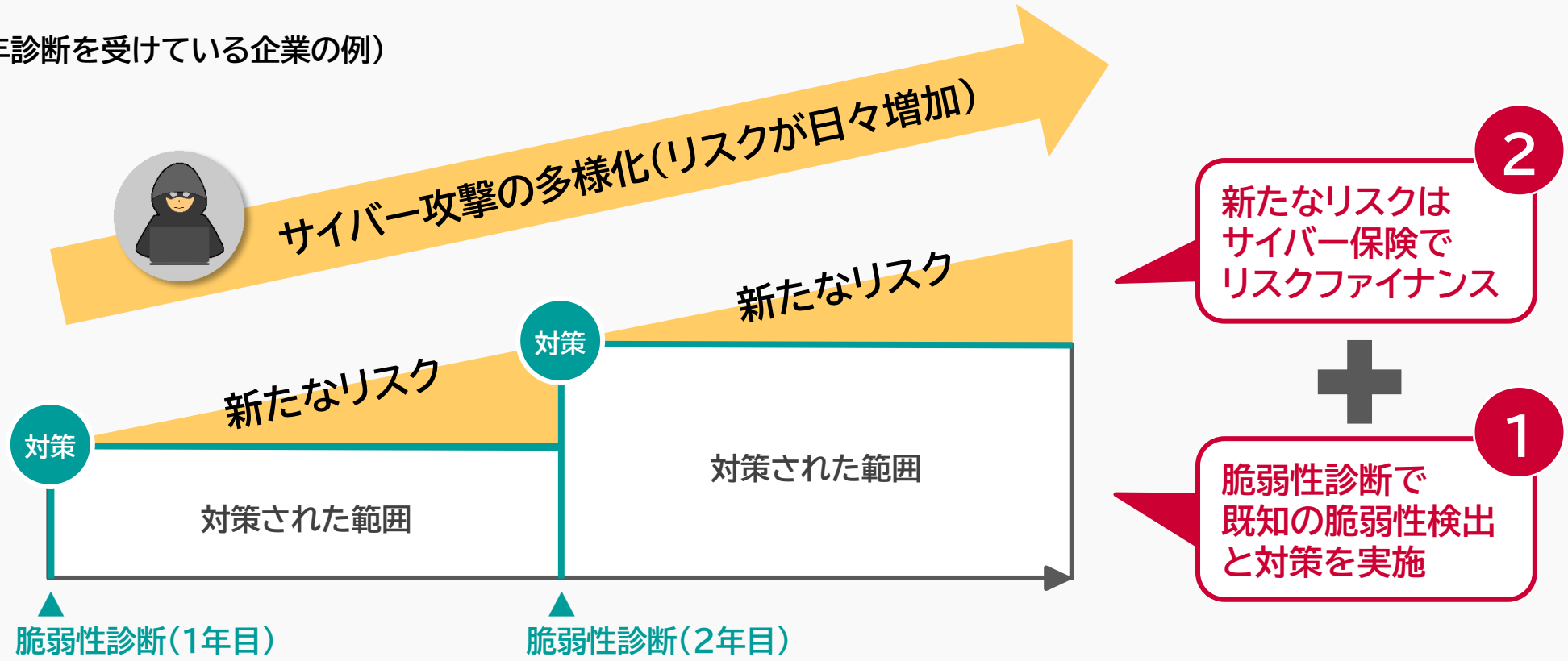
Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

ゼロディ(未知の脆弱性)に備える必要があります

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

（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

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

【参考】 サイバー保険仕様

■ 対象事故

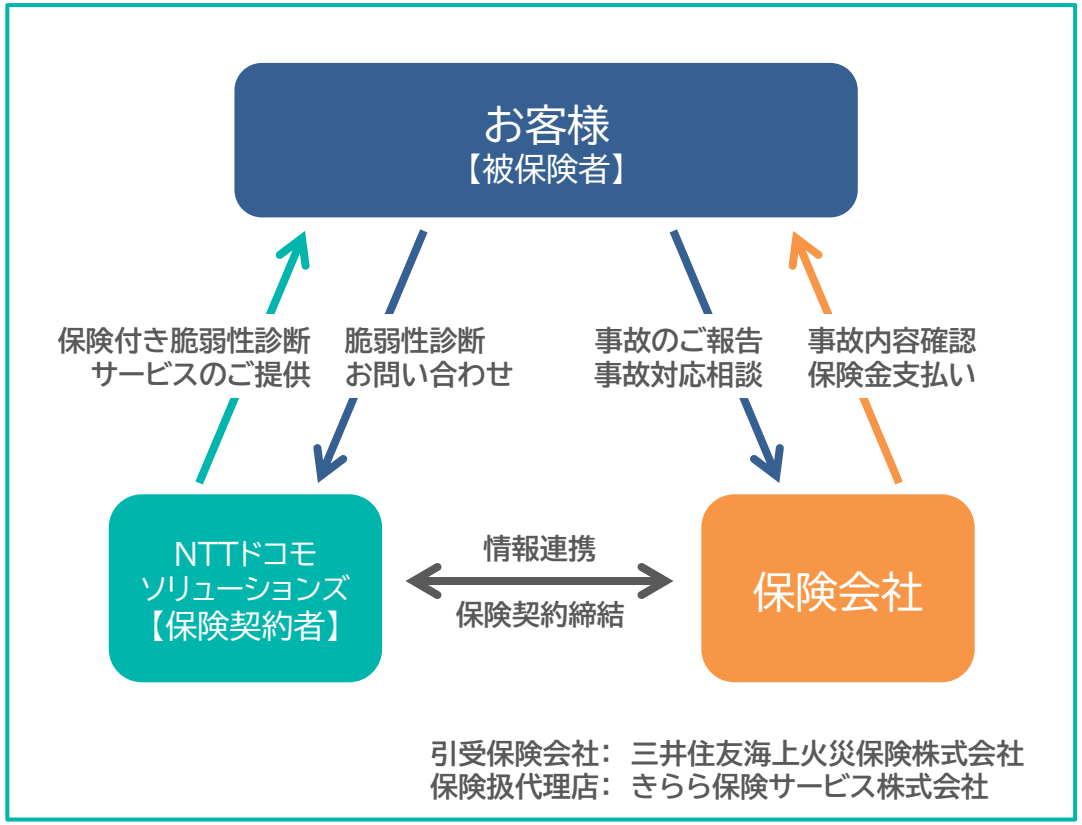
脆弱性診断を受けたシステムがサイバー攻撃等を受け、情報漏えいやそのおそれが生じた場合に、企業が被る損害賠償責任や対応費用を保険で補償

■ 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. 協力費用 オ. 訴訟対応費用 カ. 損害防止費用 キ. 緊急措置費用	ア. 事故対応費用 イ. 事故原因・被害範囲調査費用 ウ. 広告宣伝活動費用 エ. 法律相談費用 オ. コンサルティング費用 カ. 見舞金・見舞品購入費用 キ. クレジット情報モニタリング費用 ク. 公的調査等対応費用 ケ. コンピュータシステム等復旧費用 コ. 風評被害拡大防止費用 サ. 再発防止費用 シ. 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。

※ サイバー保険の補償範囲は診断メニューにより異なります

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

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

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470システム**　5,970.IP

・Webアプリ診断：**年間 約530サイト**　10,230リクエスト

（2024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

・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

・15～20年の経験のあるベテラン診断士多数在籍。

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

【参考】IPAの「情報セキュリティサービス基準適合サービスリスト」



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)（ー

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… ール ル…
  - 安全な… 方

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

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

特徴3　的確な診断報告書の提示と充実したアフターフォロー

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。

診断中に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。

診断報告書提出後、
・ネットワーク診断、Webアプリケーション診断は**3カ月以内に3回まで無料で再診断**を実施します。
・ペネトレーションテスト（Webアプリ侵入、オフィスハッキング）は**3カ月以内に1営業日で対応可能な範囲※に限り再テストを無料**で実施します。※15～20箇所程度



＜報告書サンプル＞

- 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
- 脆弱性対策後のフォロー

※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
ネットワーク/サーバ構成/Webアプリケーション/スマホアプリ診断に適用

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

Appendix

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

【参考】診断メニューの比較

診断メニュー	ネットワーク/サーバ構成/Webアプリ/スマホアプリ診断	ペネトレーションテスト
概要	**「対象システムの弱点を見える化」**	**「攻撃者視点で防御力を試す」**
目的	既知の**脆弱性・設定不備の網羅的検出**	**侵入可否および侵入後の影響度を検証**
対象	特定のシステム （NW機器やWebサイト等）	システム・組織・プロセス
アセスメント方法	公開されている既知の脆弱性が対象システムにないか、自動診断ツールや専門家の知見により評価	個別にシナリオを作成して**目標に対する侵入が可能かどうかテスト**し、対象のシステムや組織に潜むリスクを顕在化
実施頻度	半期～年次 随時 （リリース前、監査要件や取引先要求など）	半期～年次 随時 （リリース前、監査要件や取引先要求など）
成果物	診断結果報告書 （CVSS等のスコア、再現手順、修正推奨、優先度/危険度 など）	テスト結果報告書 （侵害シナリオ、到達できたデータ/権限、改善計画 など）

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

【参考】検出した脆弱性のTop5（ネットワーク診断）

システムの**現状を可視化する事**で以下の様な脆弱性に対し、対策の検討が可能となり、的確な措置を講じることで**社内のセキュリティ強化**に繋がります。

順位	脆弱性名称	危険度	詳細
①	**サポート終了製品の使用**	High	サポート終了後は修正プログラムの公開等がされず、各種の脆弱性が内在している可能性がある。 想定被害は、脆弱性の内容により様々である。
②	**脆弱性のあるソフトウェアの利用 および ソフトウェアのバージョン情報漏えい**	High および Medium	使用しているソフトウェアバージョンに脆弱性が存在している状態。また、外部（インターネット上）にソフトウェアバージョン情報が公開されてしまっている状態。 攻撃者はバージョン情報から脆弱性を調べ、攻撃される可能性がある。
③	**Web Serverで平文認証フォームを使用**	Medium	Web Server上でパスワードを含む認証情報を平文でサーバに送信している。 攻撃者は通信を盗聴し、ログインユーザとパスワードを取得することが可能である。 これにより、ユーザ情報を不正に利用される恐れがある。
④	**システムのログイン画面が公開**	High	システムのログイン画面がインターネット上に公開されてしまっている状態。 辞書攻撃等でパスワードを解析されることにより、不正にログインされる恐れがある。
⑤	**SSLv3 プロトコルの使用を許可**	Medium	サーバ上、既知の脆弱性が存在する暗号化プロトコル SSL v3 を使用している状態。 攻撃者は脆弱性を悪用して、中間者攻撃（man-in-the-middle attack）で通信内容を解読する恐れがある。

＜危険度＞High：不正アクセスやシステム停止のリスクが高い脆弱性／Medium：一定の条件がそろった際に不正アクセスやシステム停止につながる脆弱性

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.

【参考】検出した脆弱性のTop5（Webアプリ診断）

システムの**現状を可視化する事**で以下の様な脆弱性に対し、対策の検討が可能となり、的確な措置を講じることで**社内のセキュリティ強化**に繋がります。

順位	脆弱性名称	危険度	詳細
①	**Webサーバソフトウェアの脆弱性**	High	サーバで使用しているソフトウェアバージョンに脆弱性が存在している状態。 想定被害は脆弱性の内容により様々である。
②	**任意のスクリプトが実行可能 （クロスサイトスクリプティング）**	Medium	不正な HTML や JavaScriptなどが実行できてしまう状態。 これにより画面内容の改ざんなどによりユーザが不正なサイトへ誘導される恐れがある。
③	**アクセスコントロールの欠如**	High	本来権限の無いページにアクセスできてしまう状態。また本来ユーザで操作できないはずの操作ができてしまう状態。 これにより本来参照不可な情報の閲覧およびデータを改ざんされる恐れがある。
④	**データアクセス権の欠如**	High	パラメータの操作やSQLの実行などができてしまうことにより、他ユーザの情報を参照/更新できてしまう状態。 これにより本来参照不可な情報の閲覧およびデータを改ざんされる恐れがある。
⑤	**クロスサイトリクエストフォージェリ**	Medium	ユーザを特定のURLに誘導し意図せず特定のサイト上で何らかの操作を行わせるもの。 これによりサイト上でユーザが意図しない処理を実行してしまうことや、不特定多数のユーザからのリクエスト受信によるシステムリソース逼迫などを起こす恐れがある。

＜危険度＞High：不正アクセスやシステム停止のリスクが高い脆弱性／Medium：一定の条件がそろった際に不正アクセスやシステム停止につながる脆弱性

Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.



Copyright © NTT DOCOMO SOLUTIONS, Inc. 2026. All Rights Reserved.