

NTTコムウェア「サイバー保険付き脆弱性診断サービス」

日々巧妙化するサイバー攻撃に備え、脆弱性診断とサイバー保険で対策を！

近年、日本へのサイバー攻撃は急増しており、攻撃を防御、対策できなかった場合、業務停止・免許剥奪・取引停止・信用失墜等、企業が受ける被害は想像以上に甚大です。損害賠償・データ復旧・再発防止策等にかかる費用も巨額に上ります。企業はこうした状況を理解し、万が一の事態に備えて対策を講じておく必要があります。こうした背景の下、NTTコムウェア株式会社（以下、NTTコムウェア）は「サイバー保険付き脆弱性診断サービス（以下、本サービス）」を提供しています。本サービスは、脆弱性検出と対策に加え、リスクファイナンスとしてサイバー保険が付帯している点に特長があります。

様々な脆弱性診断ツールが提供されています。その中において、本サービスは2つの優位性を誇ります。1つは、脆弱性診断サービス。脆弱性診断はいわば“情報セキュリティの健康診断”。診断時の最新の脅威について第三者目線でチェックし、問題が検知された箇所をお客さままで適切に対処いただくことでシステムの安全性を引き上げます。そしてもう1つは、サイバー保険。脆弱性診断を実施し、万全な対策を施しても、攻撃手段は日々進化しており100%対応できるとは言い切れません。本サービスは、診断直後からの空白期間を保険※¹でカバーし（図1）、万が一サイバー攻撃に遭った際も、リスクファイナンスすることが可能です。

サイバー保険付き脆弱性診断でリスクに備える

企業がインターネット上に公開しているシステムやWebサイトはシステムに潜在する脆弱性を突いて様々な手口で攻撃されています。企業として情報セキュリティを確保し社会的信用を守るためには脆弱性診断と適切な対策が必須です。増大するサイバーセキュリティ被害に対して法制度・規制等も強化される昨今、各社から多

脆弱性診断の特徴

本サービスには4つの特徴があります。

●高い品質と培ったスキルによる診断実績

国内外で発生した脆弱性を調査し、外部のセキュリティ専門会社と技術連携してスキルの向上を図っています。また、ドコモグループを中心にさまざまな業界で年間約750システムの脆弱性診断の実績があります。

●的確な診断報告書の提示

検出した脆弱性ごとに具体的な検出箇所を記載した当社作成の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ます。脆弱性対応後の確認にもお役立ていただけます。

●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、お客さまにて対策をとられた後に、お客さまと調整の上、対策状況の確認（再診断）を実施します※²。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さまのセキュリティ対策をフォローします。

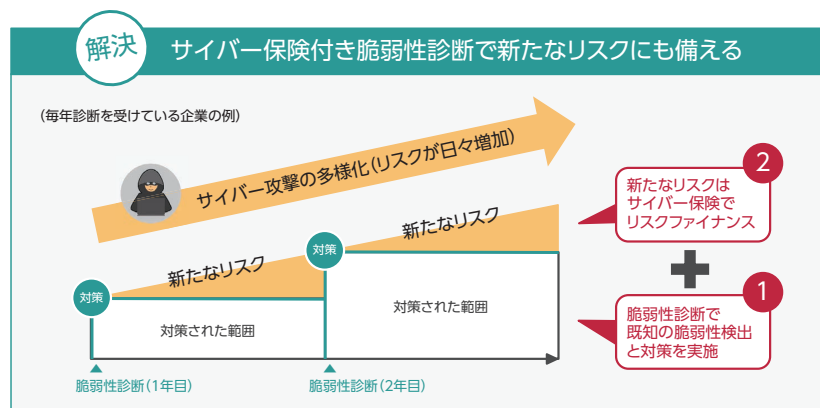


図1 「サイバー保険付き脆弱性診断サービス」概要

●サイバー保険を無償で自動付帯

脆弱性診断を受けたシステムがサイバー攻撃等により、情報漏洩やそのおそれが生じた場合には、お客さまが負う損害賠償責任や対応費用を保険で補償します。保険は、ご契約の総額が80万円以上（税抜）の場合（キャンペーン期間除く）に無償で自動的に付帯されます。^{※3}

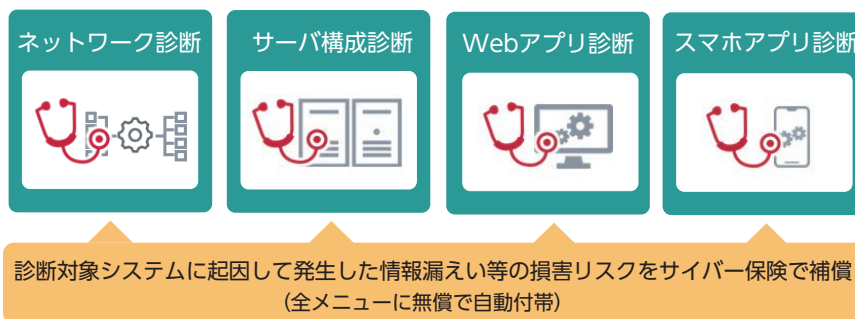


図2 診断メニュー

4つの脆弱性診断メニュー

本サービスには、4つの診断メニューがあります。お客さまの環境やご要望をヒアリングした上で最適なメニューをご提案いたします（図2）。

●ネットワーク診断

診断技術者が、診断ツールを活用し、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。

●サーバ構成診断

お客さまにて対象サーバ上で診断ツールを実行していただき、実行結果を当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。

●Webアプリ診断

診断技術者が、Webブラウザとローカルプロキシ^{※4}を利用しWebアプリに対して疑似攻撃を試行することで、Webアプリの脆弱性を洗い出します。

●スマホアプリ診断

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。

より強固な対策をめざして

NTTコムウェアでは新たに「Webアプリ診断ライト版」の提供を開始しました。ライト版は、これまでのスタンダード版のサービス内容を極力スリム化し、価格を抑えたサービスです。今や、ハッカーの攻撃ターゲットは大手企業に留まらず、サプライチェーンを担う中堅中小企業にまで拡大しています。本サービスを試してみたいとお考えの企業には、まずは低コスト/短納期のライト版からのスタートをお勧めいたします。

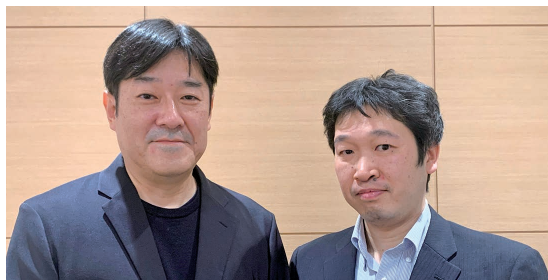
NTTコムウェアは、今後ペネトレーションテスト、クラウド設定診断等のサービス化も予定しています。脆弱性診断は健康診断同様、1回受診して終わりではなく、定期的な診断と継続的な対策が重要です。日々増大するさまざまなセキュリティリスクに備え、お客さまのご要望にあわせた診断メニューを提供し、支援していきます。また、あわせて、脆弱性診断から得られる課題の解決にむけたサービスを提案することでお客さまのビジネス拡大にも貢献していきます。

※1 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

※2 再診断は診断報告書提出後3か月以内に3回まで

※3 条件等詳細は商品HPを参照ください

※4 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



脆弱性診断サービスは各社からさまざまなタイプが提供されていますが、サイバー保険を付帯して提供するものはまだ多くはありません。当社では診断はもとより保険についても検討を重ね、お客さまのセキュリティ対策を実現しリスク軽減可能なサービスとしました。

NTTコムウェア株式会社

ドコモシステム事業本部

(左) クラウドビジネス部コンサルティング部門 担当部長 永井 隆氏

(右) クラウドビジネス部セールスサポート部門 担当課長 山村 一郎氏

お問い合わせ先

NTTコムウェア株式会社 ドコモシステム事業本部 クラウドビジネス部

製品 HP : <https://www.nttcom.co.jp/dscb/diagnosis/> (商品 HP お問い合わせフォームよりお願いします)

