KPMG あずさ監査法人

情報システムの
セキュリティ脆弱性診断

昨今のサイバー攻撃の事例を引くまでもなく、情報システムに対するセキュリティ上の脅威は複雑化、高度化の一途をたどっています。サイバー間におけるセキュリティを継続的に確保するための取組みは、保護すべき情報やサービスを保有する組織にとって共通の課題といえます。

一方で、情報システムがおかれる環境によって、求められる防御策はそれぞれ異なります。組織全体レベルでのリスクアセスメントやリスク対応が適切に行われていても、個々の情報システムレベルでセキュリティ上の防御策を十分な水準に維持することは、困難を伴います。組織にとって重要な情報システムを保護するためには、多様化する攻撃手法を踏まえ、情報システム個別に、実際に攻撃を受け得る脆弱性にどのようなものがあるかを確認し、必要な防御策を講じることが有効です。

あずさ監査法人は、疑似攻撃手法およびセキュリティ設定チェックを中心として、情報システムが内包するセキュリティ上の脆弱性の洗い出しを可能にするための適切な手法を提案したうえで、種々の財務に関する情報システムのアドバイザリーや脆弱性診断経験を有する技術者が診断を行い、防御策についてアドバイスします。

サービス概要

情報システム脆弱性診断サービス

- システムの不適切な設定などに起因するセキュリティ上の脆弱性について、外部からの疑似攻撃手法を用いた自動化診断ツールによる脆弱性スキャン、実際の攻撃手法を取り入れて侵入可能性をはかるペネトレーションテスト等、複数の手法を組み合わせてチェックします。
- 外部ネットワークからの攻撃者を想定したインターネット経由での診断、内部ネットワーク経由での診断等、クライアントのネットワーク構成に応じた診断方法を提案します。

Webアプリケーション脆弱性診断サービス

- SQL/OSコマンドインジェクション、クロスサイトスクリプティングをはじめとするWebアプリケーションの脆弱性について、外部からの疑似攻撃手法をベースに、複数の手法を組み合わせてチェックします。
- Webアプリケーションの脆弱性につながるWebサーバ、サーバOSの問題点について、外部からの疑似攻撃手法と、サーバにログインし操作する手法の組合せによりチェックします。

組織内セキュリティ脆弱性診断サービス

- 組織内ネットワークを調査し、組織の重要な情報を保存するサーバ等で適切なアクセス制御が行われているか、外部からの疑似攻撃手法や、サーバにログインし設定を確認する手法をベースに、複数の手法を組み合わせてチェックします。
- 組織内ネットワークで利用されるPCやモバイルデバイス、BYOD※1、無線LAN等について、組織の情報セキュリティポリシーに従い適切に使用されているか、主にネットワークスキャン手法を応用してチェックします。
- インターネットに公開されているWebアプリケーションを含むWebサイトの情報について、インターネット上の検索エンジンに不要な情報がキャッシュされていないかチェックします。
- 組織内ネットワークでのeメールやWebサイトの利用がセキュリティルールに従い使用されているか、主にソーシャルエンジニアリング※2的手法（疑似ウイルスメールの送信など）を用いてチェックします。

※1. BYOD（Bring Your Own Devices: 私的デバイス活用）：
主に組織外での業務遂行を目的として、個人所有の機器を用いて組織の情報システムにアクセスし、情報の閲覧や入力を可能にすること。

※2. ソーシャルエンジニアリング：
人間のミスや心理につけこんでコンピュータを操作させたり、情報漏えいを狙ったりする攻撃手法のこと。

©2016 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

診断サービス実施により改善が期待される課題例

本サービスは、下記のような、組織が抱える情報セキュリティに関連するさまざまな課題を改善するために利用できます。

- 情報セキュリティ管理態勢を整備、運用しているが、情報システムが直近の攻撃手法や脆弱性に適切に対応できているか、不安がある。
- 自社のネットワーク機器およびサーバのセキュリティ設定が一定のルールに則り構築されておらず、脆弱性対策の実施状況もまちまちであり、どの脆弱性にどこから対策を実施すべきか悩んでいる。
- 情報セキュリティポリシーに従ってネットワークが構築、維持されているか、不安がある。
- 情報システムへのペネトレーション（疑似侵入）テストをテーマに組み入れて内部監査を実施する事になったが、どのような項目をどのようなツールを利用してチェックすればよいか悩んでいる。
- 無線LANを導入したが、情報セキュリティの対策レベルが安心できるレベルかどうか不安がある。

期待される効果

情報システムのセキュリティ上の課題把握と改善ポイントの明確化

第三者の客観的な診断により、情報システムの現状、改善すべき情報セキュリティ課題が把握でき、組織として対応する方向性を明確にすることができます。

- 情報システムごとでの管理レベルのバラつき、無駄を把握し、必要な施策やリソースを検討できる。
- 組織内ネットワーク、または情報システムに対する陳腐化した対策を発見し、必要な対策を検討できる。
- マンネリ化した情報セキュリティ目標を見直し、新たな管理態勢を検討できる。

その他関連サービス

あずさ監査法人では、情報セキュリティ管理に関する課題について、さまざまなソリューションサービスを提供しています。

- 情報セキュリティ管理態勢診断サービス
- 情報セキュリティ関連文書診断サービス
- 情報セキュリティ内部監査支援サービス
- 情報セキュリティ管理態勢構築支援サービス

有限責任 あずさ監査法人
IT監査部

〒100-8172
東京都千代田区大手町1丁目9番7号
大手町フィナンシャルシティ サウスタワー
TEL ： 03-3548-5315
FAX： 03-3548-5316

AZSA-ITAUDIT@jp.kpmg.com
www.kpmg.com/jp

本リーフレットで紹介するサービスは、公認会計士法、独立性規則及び利益相反等の観点から、提供できる企業や提供できる業務の範囲等に一定の制限がかかる場合があります。詳しくはあずさ監査法人までお問い合わせください。

ここに記載されている情報はあくまで一般的なものであり、特定の個人や組織が置かれている状況に対応するものではありません。私たちは、的確な情報をタイムリーに提供するよう努めておりますが、情報を受け取られた時点及びそれ以降においての正確さは保証の限りではありません。何らかの行動を取られる場合は、ここにある情報のみを根拠とせず、プロフェッショナルが特定の状況を綿密に調査した上で提案する適切なアドバイスをもとにご判断ください。

© 2016 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. 16-1197

The KPMG name and logo are registered trademarks or trademarks of KPMG International.