



CAPTAIN

セキュリティ可視化サービス

—攻撃者の視点でセキュリティ対策を総合評価—

知らず知らずのうちに高まるセキュリティリスク

放置された脆弱性



古いバージョンのOSやソフトウェアを放置していませんか？

把握していないIT資産



インターネット上に公開されたIT資産を把握していますか？

設定ミス



不要なポートがネットワーク機器に設定されたままになっていませんか？

不十分なITリテラシー



不審なメールが送られてきた時に社員は適切に対処できますか？



攻撃者の視点で調査を実施

御社のセキュリティ対策を総合的に評価し、レポートを作成します

IT資産状況

ポート開放状況

脆弱性状況

SSL構成状況

メールアドレス
認証情報漏洩状況

IPA情報セキュリティ
自社診断

標的型攻撃メール訓練



サービス内容



インターネット上に公開されているIT資産について、「不要なポートの開放」「脆弱性の放置」「SSL設定の不備」といったセキュリティリスクを調査します。合わせて、メールアドレスをもとに「ID・パスワード」などのクレデンシャル情報が漏洩していないかを調査します。

弊社技術者が
攻撃者視点で調査



様々なツール・サービスを活用し、外部から御社に関連する情報を収集



結果レポートの内容をもとに、セキュリティ対策を検討

- 利用していないサーバがインターネットからアクセス可能となっていた
- 社内にリモートデスクトップ接続可能な状態となっていた
- WEBサーバやルータの脆弱性が放置されたままになっていた
- 多くの社員が不審なメールを開いてしまった など

他社と比較して、セキュリティ対策はどのレベルなのか？
どこから対策を行うべきか？総合的に評価します！

評価項目	詳細	標準価格
IT資産状況	インターネットからアクセス可能な御社のIT資産(サーバ、ルータ等)を調査します。	500,000円
ポート開放状況	インターネットからアクセス可能な御社資産に不要且つ危険性のあるポートが開放されていないかを調査します。	
脆弱性状況	インターネットからアクセス可能な御社資産に脆弱性がないかを調査します。	
SSL構成状況	御社WebサーバのSSL構成状況に脆弱性がないかを調査します。	
メールアカウント 認証情報漏洩状況	御社社員が利用しているサービスの認証情報が漏洩していないかを調査します。(※メールアドレスのリストをご提供いただきます)	
IPA情報セキュリティ 自社診断	IPAの診断項目にご回答いただき、御社の強化ポイントを抽出します。(※25項目の診断にご回答いただきます)	
標的型攻撃メール訓練	疑似攻撃メールの訓練を通じて、社員のセキュリティ意識向上に繋がります。	

※評価対象の公開資産のASETは10までとします。
※価格は税抜きです。

※メール訓練の送信先メールアドレスは100までとします。

類似サービスとの違い

①ASM

攻撃者の視点から、攻撃対象となり得るデジタル資産を継続的に監視、変化を通知

②脆弱性診断

既知の脆弱性を検出する
ツール/サービス

本サービス

①②を含む幅広い
項目で現状を把握！