セキュリティ診断サービス

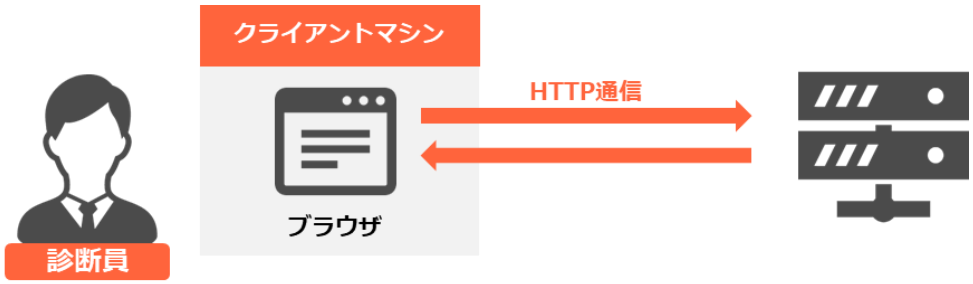
サービス概要

経験豊かなセキュリティ診断員が、攻撃者目線での疑似攻撃をツールと手動で行い、お客様システムの脆弱性を徹底的に洗い出します。

- ✓ 大手企業からのセキュリティ診断業務の実績多数
- ✓ 最速1週間で診断対応可能
- ✓ 診断要件のヒアリングから診断後の対策方法までサポート

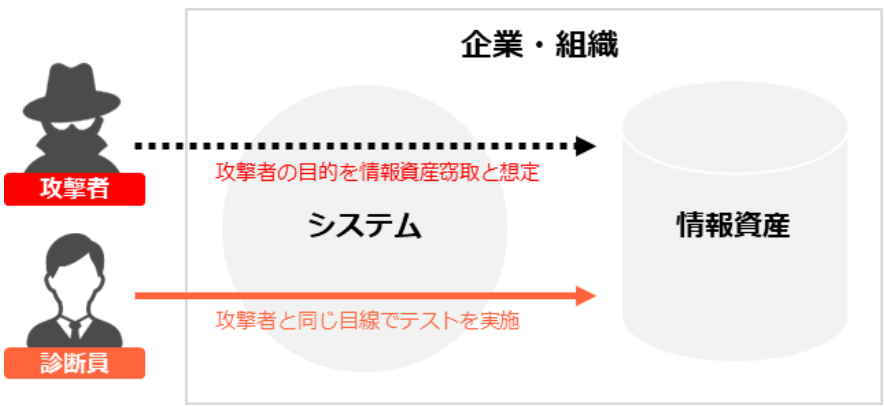
Webアプリケーション診断

診断対象	Webブラウザを介して動作するアプリケーション
診断概要	Webアプリケーションに潜在する**SQLインジェクションやクロスサイトスクリプティングなどのセキュリティ診断を実施**します。ツールに依存した診断手法ではなく、ロジック上の問題点、最新の技術に起因する問題など、**セキュリティエンジニアが攻撃者の観点でツールと手動を併用した診断**を行います。
診断期間	1週間～（規模により変動）



ペネトレーションテスト

診断対象	お客様のシステム全般　※主に運用中のシステム向き
診断概要	最新のハッカー事情に精通したセキュリティエンジニアが、**お客様の運用する機器やネットワークに疑似攻撃**をして、脆弱性を診断するペネトレーションテスト(侵入テスト)を行います。 **既に導入している機器や対策に対しても、想定通り機能するのか再確認できます。**
診断期間	1週間～（規模により変動）



診断実施までの流れ

ご要件確認 ▶ 診断の実施 ▶ レポート作成 ▶ ご報告

診断期間：1週間～（規模により変動）

診断レポートサンプル

診断結果は、発見された脆弱性を迅速に修正できるよう、具体的な内容・再現方法・リスク・対策方法を診断レポートにてご報告します。

2.2. 指摘事項一覧

指摘事項一覧は下表の通りです。

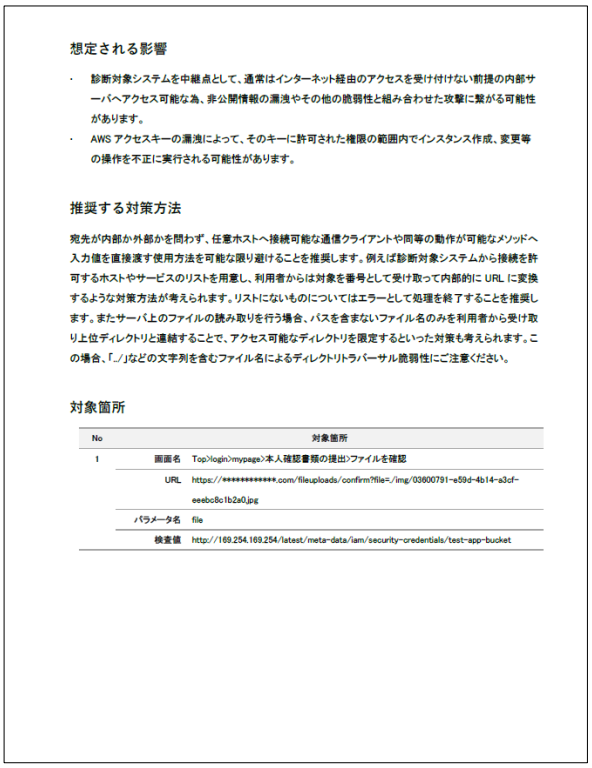
No	リスクレベル	指摘事項	対象
1	緊急	SQL インジェクション	Web
2	緊急	サーバサイド・リクエスト・フォージェリ(SSRF)	Web
3	高	GraphQL における認可制御の不備	Web
4	中	クロスサイトスクリプティング	Web
5	低	クロスサイト・リクエスト・フォージェリ	Web

2.2.1. リスクレベル別評価一覧

本報告書では各指摘事項について、以下のリスクレベルを設定しています。

レベル	基準および具体例
緊急	・任意コード実行など、診断対象システムへの侵入やその管理権限取得、制圧等につながる脆弱性 ・攻撃の成功により直接的に金銭およびそれに類するものの窃取等につながる脆弱性 ・実運用中のシステム上で現在進行中の不正アクセス行為の発見 など
高	・システムやその利用者にとって重要と考えられるデータや、大量の個人データの漏洩、改ざんにつながる脆弱性など
中	・情報漏洩や改ざん等につながるが、攻撃成立のために被害者自身による操作を要する受動的攻撃や、攻撃者には制御不能な前提条件を要する脆弱性 ・システムへの能動的な攻撃が可能だが、高レベルの影響に至らない脆弱性 など
低	・その脆弱性の単独の悪用では重大事に至らないと考えられる、軽微なシステム情報の出力など ・現実的でない前提条件を要するなど、実際の攻撃が困難な脆弱性
情報	・リスクではないが、ご確認頂く必要があると考える情報

- 指摘事項一覧、リスクレベル別評価 -



想定される影響

・診断対象システムを中継点として、通常はインターネット経由のアクセスを受け付けない前提の内部サーバへアクセス可能な為、非公開情報の漏洩やその他の脆弱性と組み合わせた攻撃に繋がる可能性があります。
・AWS アクセスキーの漏洩によって、そのキーに許可された権限の範囲内でインスタンス作成、変更等の操作を不正に実行される可能性があります。

推奨する対策方法

宛先が内部か外部かを問わず、任意ホストへ接続可能な通信クライアントや同等の動作が可能なメソッドへ入力値を直接渡す使用方法を可能な限り避けることを推奨します。例えば診断対象システムから接続を許可するホストやサービスのリストを用意し、利用者からは対象を番号として受け取って内部的に URL に変換するような対策方法が考えられます。リストにないものについてはエラーとして処理を終了することを推奨します。またサーバ上のファイルの読み取りを行う場合、パスを含まないファイル名のみを利用者から受け取り上位ディレクトリと連結することで、アクセス可能なディレクトリを限定するといった対策も考えられます。この場合、「../」などの文字列を含むファイル名によるディレクトリトラバーサル脆弱性にご注意ください。

対象箇所

No	対象箇所	
1	画面名	Top>login>mypage>本人確認書類の提出>ファイルを確認
	URL	https://**********.com/fileuploads/confirm?file=./img/03600791-e59d-4b14-a3cf-eeebc8c1b2a0.jpg
	パラメータ名	file
	検査値	http://169.254.169.254/latest/meta-data/iam/security-credentials/test-app-bucket

- 指摘事項に対する対策方法 -

ご提供価格

Webアプリケーション診断

¥400,000～ (税抜)

[構成例] リクエスト数10のアプリケーション

※価格は診断対象のリクエスト数に応じて変動するため詳細はお問合せ下さい

ペネトレーションテスト

¥3,750,000～ (税抜)

※価格はシナリオとゴールにより変動するため詳細は別途お問い合わせ下さい

CRESCO DIGITAL TECH
株式会社クレスコ・デジタルテクノロジーズ

クレスコDT

〒108-0075
東京都港区港南2-12-23 明産高浜ビル2階
TEL:03-5495-7981