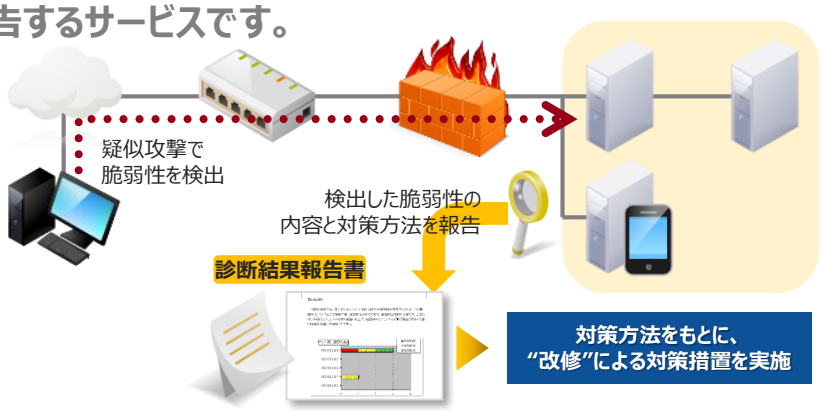
GSX
GLOBAL SECURITY EXPERTS

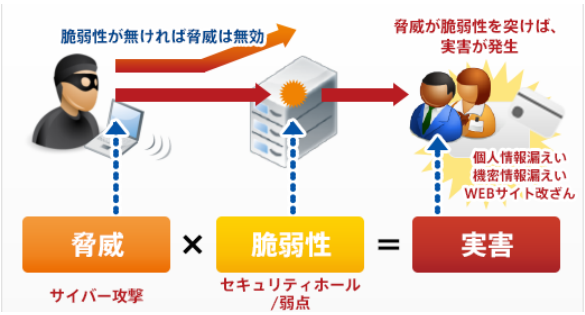
タイガーチームサービス

タイガーチームサービスとは

タイガーチームサービスとは、GSXのホワイトハッカーが対象のネットワークシステムに対しハッカーと同じ手法を用いて擬似攻撃を実施し、実害につながりうるシステム内の脆弱性を検出し、対策方法を含めてご報告するサービスです。

インターネット経由の脅威（ハッカーの攻撃など）を想定したリモート診断、内部からの脅威（内部犯行やマルウェア感染端末からの攻撃）を想定したオンサイト診断の2種類の方法にて診断が可能です。





漏洩や改竄と言ったセキュリティの実害は、サイバー攻撃等の脅威とセキュリティ対策に潜在する脆弱性の両方の存在があるため発生します。つまり、脅威か脆弱性のどちらかがゼロになれば、実害は発生しません。
脅威、つまり攻撃者をゼロにするのは困難ですが、脆弱性をゼロにするのは可能であり、そのひとつのアプローチがタイガーチームサービスです。

タイガーチームサービスの歴史

20年の実績を誇る、高度な脆弱性診断サービスです。タイガーチームのメンバーがハッカーと同じ手法を用いて、手動診断サービスをご提供致します。

1997年～ **システム監査の一環として、ペネトレーションテストを開始**
(脆弱性診断サービスの提供開始)
「タイガーチーム」として商標登録済

2001年　Webアプリケーション脆弱性診断サービスを開始

名称の由来は、軍事用語。

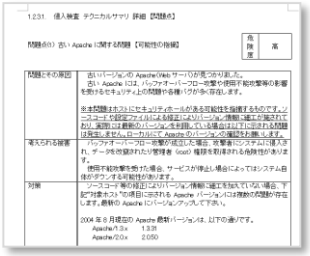
元々、米海軍の特殊部隊を表す軍事用語からきており、アメリカでは現在、ハッカーと同様の手口を用いて、ネットワークシステムの欠陥を調査する専門家チームを表すようになりました。

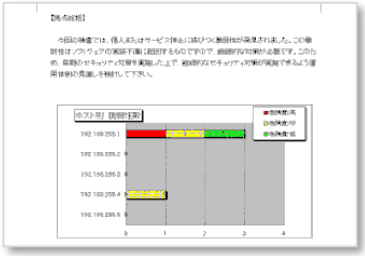
サービスステップ

タイガーチームサービスの流れは下記のようになります。ご要望に応じて、個別対応を提供することも可能です。

事前調整& 内容確認書作成	診断実施	速報	結果分析/ 報告書作成	報告会
診断対象などを伺ってスケジュールを決定します。決まった内容を基に診断内容確認書を作成します。	営業時間の平日10:00～18:00で診断します。ご要望に応じ、 夜間・深夜・休日などにもオプション対応が可能です。	診断中に緊急度の高い脆弱性が発見された場合、速報としてご連絡します。	診断結果を、“タイガーチーム報告書”として取りまとめます。	診断を実施した専門エンジニアが内容をご説明する報告会を開催します。

診断内容確認書





診断結果報告書

タイガーチームサービスの特徴

! 多様な診断対象への対応、診断メニューの豊富さ

お客様のご要望により多くの診断方法や対象を選択いただけます。スタンダードでは、ホワイトハッカーが手動オペレーションによる高レベルの診断(網羅性と検出精度が高い)を実施します。ライトでは、診断のスピードやボリュームを優先するお客様向けに診断ツールを利用したコストメリットの高いサービスをご提供します。 また、Webアプリケーションやプラットフォームの診断だけでなく、スマホネイティブアプリやPCクライアントアプリ等の特殊なアプリ、IPV6など、多様な対象への診断も実施可能です。さらに、データベース診断やパスワード解析などの特定の対象や内容に特化した診断サービスも提供しています。インターネット経由の診断だけではなく、お客様先に出向いてのオンサイト診断、夜間や休日を利用した診断など診断場所や日時などもお客様のご都合に合わせて対応が可能です。

! 診断後の改修・対策作業における、総合的な提案が可能

タイガーチームサービスで検出した脆弱性の改修や対策方法について、総合的なご提案が可能です。脆弱性の改修については、手厚いサポートをご提供するためにWebアプリケーション開発の経験を有するエンジニアを多く採用し、脆弱性対策や脆弱性診断のエキスパートして育成しております。また、以下のような総合的なご提案を実施し

- Webアプリケーションファイアウォールやや IDS/IPSといった攻撃防御機器のご提案
- お客様の内部に脆弱性診断の体制を構築する脆弱性診断ツール販売や教育
- 教育事業(EC-Council) ：ホワイトハッカー養成、セキュアプログラミング
- セキュア開発ガイドライン作成

多面的にお客様の脆弱性対策のご支援をいたします。

Webアプリケーション診断

スタンダード

ホワイトハッカーの手動オペレーションによる高度な診断を実施します。Webアプリケーションの脆弱性に対しては、手動オペレーションと商用診断ツールの精度/網羅性に明確な違いが発生することから、手動オペレーションを基本メニューとしています。
また、手動オペレーションなので、充分なインターバルをとった作業、目視での異常検知と負荷調整などが可能となり、診断時の障害発生について最大限に配慮した診断を実施します。

- **手動オペレーションによる高度な診断**
- **安全性への配慮**
- **網羅性重視の診断**

ライト

広範囲な業務アプリケーションのサイトを診断し最低限必要な脆弱性を未然に発見して、改修したい。という診断対象のボリュームを優先される企業様向けに、タイガーチームが長年の経験から選抜した、優秀な脆弱性診断ツールを利用したサービスです。
脆弱性診断ツールから出力された診断結果は、タイガーチームが確認精査して、よりわかり易い報告書にまとめ、お客様に納品いたします。

- **商用ツールによる高速診断**
- **より多くの範囲と短時間での診断**

診断項目

診断項目	スタンダード	ライト	診断項目	スタンダード	ライト
セッション管理の不備	◎	×	HTTPレスポンス分割	◎	○
セッションフィクセーション	◎	○	リモートファイルインクルード	◎	×
クロスサイトリクエストフォージェリ	◎	○	通信の暗号化	◎	○
クロスサイトスクリプティング	◎	○	証明書の不備	◎	○
SQLインジェクション	◎	○	Refererによる情報漏洩	◎	○
OSコマンドインジェクション	◎	○	ユーザID等の調査	◎	×
ディレクトリトラバーサル	◎	○	詳細なエラーメッセージ	◎	×
XMLインジェクション	◎	○	拡張子偽装	◎	×
SSIインジェクション	◎	○	コメント・デバッグ情報	◎	○
XPathインジェクション	◎	○	アプリケーション固有の問題	◎	×
XQueryインジェクション	◎	○	フォーマットストリング	◎	○
LDAPインジェクション	◎	○	バッファオーバーフロー	◎	○
MXインジェクション	◎	×			

◎：ツールによる機械的な診断では検出できない内容を、ホワイトハッカーが対象サイトの動きに合わせて診断を実施
○：商用診断ツールによる一定品質の診断を実施
×：診断不可

サービス比較

	スタンダード	ライト
診断手法	ホワイトハッカーによる手動	ツール＋確認精査
診断項目	全て	限定（※詳細は別表にて）
報告書	タイガーチームによるわかり易い報告書	タイガーチームによるわかり易い報告書
こんなお客様向けです	診断結果の品質や精度を優先されるお客様向け 例）サイトのリリース前にししっかり診断し脆弱性のない状態で公開したい。	診断対象のボリュームを優先されるお客様 例）広範囲の業務アプリのサイトを診断し最低限必要な脆弱性を改修したい。
同額コストにおける診断対象範囲		

プラットフォーム診断

スタンダード

ホワイトハッカーの手動オペレーション診断による、複数の脆弱性を組合わせた攻撃など、脆弱性診断ツールによる診断と比較して、実際のハッカーの攻撃手法に近い高度な診断を実施します。
実際のハッカーと同じ視点でブラックボックス方式のテストを実施し、充分なインターバルをとった作業、目視での異常検知と負荷調整などにより、診断時の障害発生について最大限に配慮した脆弱性診断を実施します。

- **二重診断による高精度な診断**
- **安全性への配慮**

ライト

関係会社すべての公開サーバーの脆弱性を発見し、脅威に対する体制の全体的な強化（ボトムアップ）を図りたい。など、診断対象のボリュームを優先される企業様向けに、診断項目範囲はそのままに、タイガーチームが長年の経験から選定した脆弱性診断ツールを利用した広範囲対応型サービスです。脆弱性診断ツールから出力された診断結果は、タイガーチームが確認精査して、よりわかり易い報告書にまとめ、お客様に納品いたします。

- **商用ツールによる高速診断**
- **より多くの範囲と短時間での診断**

診断項目

主に下記の項目を情報収集、診断致します。(約5,000項目以上)

ネットワークの設定不備	脆弱なサービスの存在	脆弱な古いバージョンのOS・サービス
OS・ミドルウェアの設定不備	不要なコンテンツやスクリプト	SSL証明書の不備
暗号化通信の不備	推測可能なパスワード	第三者によるメールの不正中継

サービス比較

	スタンダード	ライト
診断手法	ホワイトハッカーによる手動 （※一部ツール利用）	ツール＋確認精査
診断品質	◎	○
ポート範囲	TCP：1-65535 UDP：1-65535	TCP：1-1023 UDP：1-1023
報告書	タイガーチームによるわかり易い報告書	タイガーチームによるわかり易い報告書
こんなお客様向けです	診断結果の品質や精度を優先されるお客様向け 例）サイトのリリース前にししっかり診断し脆弱性のない状態で公開したい。	診断対象のボリュームを優先されるお客様 例）多数ある関係会社の公開サーバを診断して脆弱性状況のボトムアップをしたい。
同額コストにおける診断対象範囲		

いま、注目！

スマホアプリセキュリティ診断

スマホアプリセキュリティ診断サービスは、クライアントアプリに対して専門コンサルタントが手動による徹底的な診断を行い、その結果を分かりやすく報告するサービスです。

診断項目※一部抜粋

APKファイルまたはIPAファイルを解析する「静的解析」と、アプリを動作させることで生成される各種ファイルや機能の悪用可否を確認する「動的解析」の2種類の手法による診断を実施します。
下表は、一部抜粋になりますが、主な診断項目例になります。

スマホアプリ内情報の調査	スマホアプリ内で利用する情報に重要情報が含まれているか
TimeTraveler脆弱性	時刻操作によるスマホアプリの不正利用の可否
addJavascriptInterfaceの使用	WebView#addJavascriptInterface機能の使用有無
ログ出力内容の調査	スマホアプリが出力するログ情報に重要情報が含まれているか
不正Intentによる重要情報アクセス	Intentによる重要情報へのアクセス可否

What's new?

One-Dayパック

初めて脆弱性診断を実施される。お試しで診断してみたい。などのご要望をお持ちのお客様向けに、一日で診断できる対象をGSXが選定してご提供するタイガーチームサービスです。
（※1ip＋5画面遷移が標準目安です。）

One-Dayパックサービスステップ