病院・医療機関向け

ネットワーク脆弱性診断サービス

BBS BUSINESS BRAIN GSX GLOBAL SECURITY EXPERTS

情報漏えいを防ぐために病院・医療機関が行なうべきこととは？

昨今、海外からの不正アクセスを含むサイバー攻撃による情報漏えい事故が増えており、病院・医療機関においても不正アクセスの実害が発生した事例が出ています。ネットワークを活用した医療連携等、今後ますます病院を取り巻くネットワークサービスの重要性は増していきますが、同時に情報漏えいのリスクも増えることになります。
情報漏えいを防ぐために、まずは、現在の病院ネットワークとシステムの弱点（脆弱性）を見極めることが必要です。
それを可能とするのが、GSXのタイガーチームによる、ネットワーク脆弱性診断サービスです。

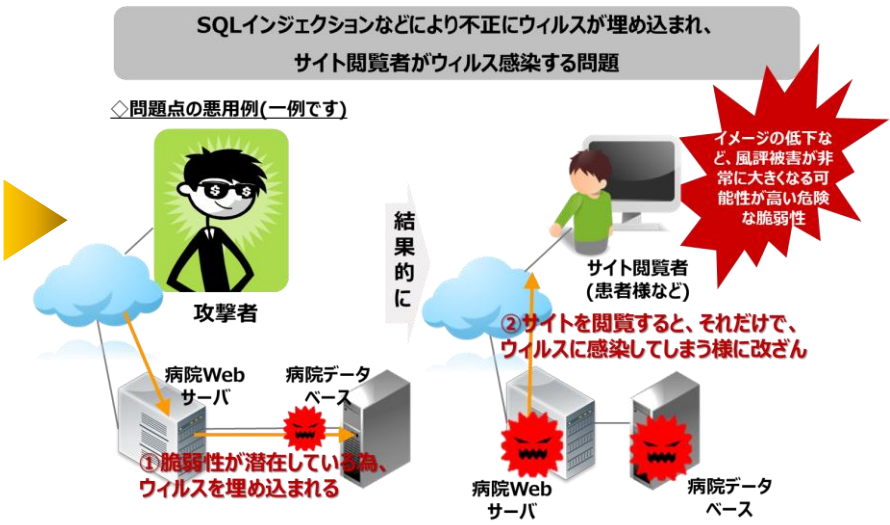
GSXのタイガーチームは、元々米海軍の特殊部隊を表す軍事用語に由来しており、アメリカでは現在、ハッカーと同様の手口を用いてネットワークシステムの欠陥を調査する専門家チームを表すようになっています。GSXでも、豊富な経験と高度なセキュリティ技術を持った専門家チームを編成してタイガーチームを発足させ、ペネトレーションテスト(外部からの侵入テスト)を行なうサービスを提供しています。

病院・医療機関を狙う攻撃、その手法をご存知ですか？

実際にあった事件

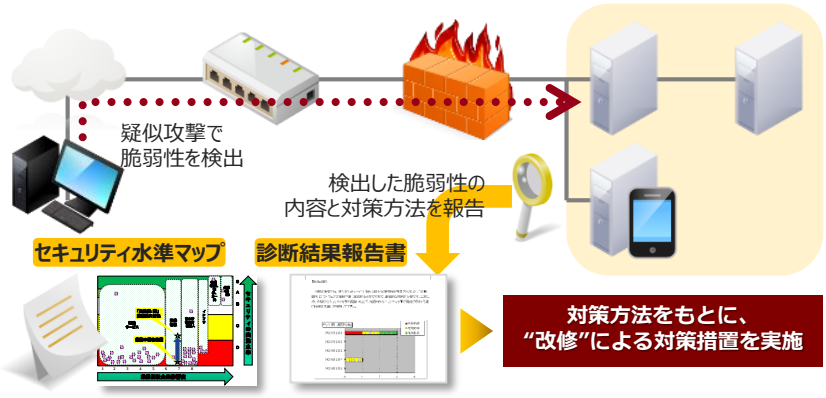
国内病院において、HPの内容が改ざんされ、Webサイトの特定のページを見ると、自動的に別のページに移されて不正なプログラムを実行する仕組みとなっていた事件がありました。

明らかに病院・医療機関もサイバー攻撃のターゲットになっている！



ネットワーク脆弱性診断サービスとは

ネットワーク脆弱性診断とは、タイガーチームの専門エンジニアが、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。
脆弱性診断の結果、検出した脆弱性の危険度をもとに評点化し、セキュリティの実施水準と業界別社会的影響度を考慮して分布図を作成し、評価結果の内容を病院幹部へご説明する報告会を開催します。



自病院のセキュリティレベルのポジショニングを知ることが出来る！

病院(組織)として実行すべきことが見えてくる！

有効度／優先度を考えてセキュリティ対策計画を立案／実行できる！

ネットワーク脆弱性診断サービス サービスメニュー

プラットフォーム診断

手動オペレーションでは、複数の脆弱性を組合わせた攻撃など、診断ツールと比較して、実際のハッカーの攻撃手法に近い視点による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診断を実施します。

- **二重診断による高精度な診断**
- **ブラックボックス方式**
- **安全性への配慮**

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)
※DoS攻撃診断についてオプションにて実施可能です

OSの脆弱性チェック	アプリケーションの脆弱性チェック
バックドアのチェック	第三者中継(SPAM)のチェック
推測可能なパスワードのチェック	サンプルスクリプトの 有無のチェック
ミドルウェアの脆弱性チェック	データベースの脆弱性チェック
ウイルス感染チェック	証明書の有効性チェック
通信の盗聴可否のチェック(暗号化)	

Webアプリケーション診断

専門エンジニアによる手動オペレーション診断で高度な診断を実施します。(プラットフォーム診断と比較すると、手動オペレーションと商用診断ツールの精度/網羅性に大きく乖離があることから、手動オペレーションを基本としています。)※ただしお客様のご希望や、内容・状況により、診断ツールを併用した診断についても対応可能です。

- **手動オペレーションによる高度な診断**
- **安全性への配慮**

診断項目

手動オペレーションによる診断は網羅性と検出精度が最も高く、診断結果に基づいたソースコード改修を実施できれば、もっとも高いセキュリティレベルを実現できます。

クロスサイトスクリプティング	クロスサイトリクエストフォージェリ
SQLインジェクション	MXインジェクション
OSコマンドインジェクション	なりすまし
ディレクトリトラバーサル	通信の暗号化
セッションフィクセーション	etc.

サービスステップ

ネットワーク脆弱性診断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、個別対応も可能です。

事前調整&内容確認書作成

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。

ネットワーク脆弱性診断

対象サーバにおける、内在する脆弱性(セキュリティ・ホール)を専門エンジニアがインターネット経由の擬似攻撃により検出します。

結果分析/報告書作成

診断結果を、"診断結果報告書"として取りまとめます。検出した脆弱性の危険度をもとに評点化し、"セキュリティ水準マップ"として分布図に配置します。

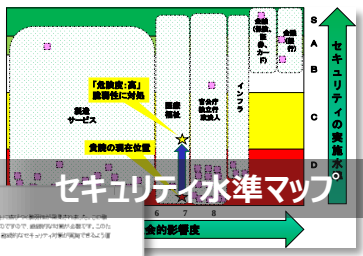
運用管理状況調査

診断結果報告書の内容を保守ベンダー様にご説明し、対策措置を促します。また、脆弱性の原因・発生要因を明らかにし、評価結果報告書として取りまとめます。

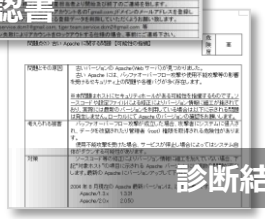
報告会

取りまとめた評価結果報告書の内容を、病院幹部にご説明する報告会を開催します。


診断内容確認書



セキュリティ水準マップ




診断結果報告書

GSX GLOBAL SECURITY EXPERTS
サービス提供元

グローバルセキュリティエキスパート株式会社
事業開発部
〒105-0003 東京都港区西新橋1-2-9
日比谷セントラルビル21F
TEL：03-3507-1360 FAX：03-3507-1361

BBS BUSINESS BRAIN
お問合せ

株式会社ビジネスブレイン太田昭和（BBS）
情報セキュリティ研究所 担当：新井
〒105-0003 東京都港区西新橋1-2-9
日比谷セントラルビル22F
TEL：03-3507-1310 FAX：03-3507-1311