ISOG-Jの2015年度成果物あれこれ

ISOG-J WG6
武井 滋紀
（NTTソフトウェア株式会社）

2016年6月17日（金）

はじめに

1. WG1, WG6の紹介
2. 脆弱性診断士スキルマップ＆シラバスの紹介
3. 「やられたかな？その前に」ガイドの紹介
4. Internet Week 2015の発表報告
5. 2016年度の予定

WG1, WG6の紹介

- WG1：セキュリティオペレーションガイドラインWG
  - OWASP Japanと共同の脆弱性診断士スキルマッププロジェクトを主催
  - 脆弱性診断士について、スキルマップとシラバスを公開
- WG6：セキュリティオペレーション連携WG
  - 旬な各種共通課題を抽出して議論し、可能であれば成果物を公開
  - 2014,2015年度はプロジェクトとして単年度で活動していたが、2016年度からはWGとして活動を開始

脆弱性診断士
スキルマップ&シラバス

ISOG-J WG1

ISOG-J WG1活動内容

- セキュリティオペレーションガイドラインWG
  - –ユーザー向けの脆弱性診断のガイドラインなどの作成を目指す
- 脆弱性診断士関連
  - –脆弱性診断士（Webアプリケーション）スキルマップ＆シラバス
  - –脆弱性診断士（プラットフォーム）スキルマップ＆シラバス
  - –OWASP Japanとの共同プロジェクト「脆弱性診断士スキルマッププロジェクト」

脆弱性診断はどうしてる？

脆弱性診断サービスを提供する専門業者に外注

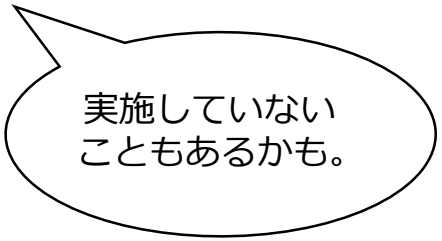
- コストは決して安くない

脆弱性診断の自動診断ツールを利用

- 自動診断ツールには得意分野と不得意分野があり、自動診断ツールだけでは完結しない
- コストも決して安くない

開発者自身が実施

- 十分なスキルがある？



脆弱性診断サービスの問題点

顧客には品質の違いがわからない

- 各社の診断サービスには品質にばらつきがある
  - –特にWebアプリケーション脆弱性診断
- 自動診断ツールだけ？手作業の品質は？
  - –そもそも品質があるとか知らないかもしれない
- 利用者にはもっとわからない
  - –安全なWebサイトかどうか判別がつかない

脆弱性診断の品質は

会社で決まる？診断する個人で決まる？

- 診断技術は個人スキルに大きく依存する
  - –顧客からの指名買いがあることも

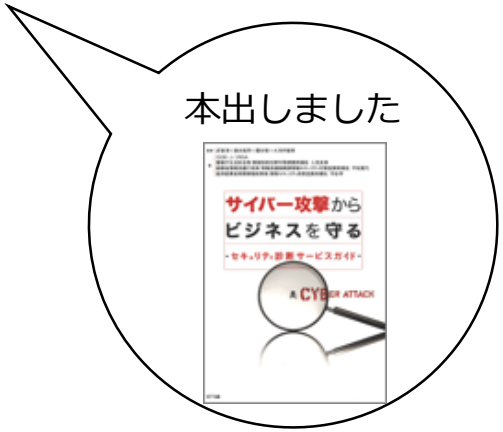
しかし、技術レベルの
可視化が行われていない

問題解決に必要なもの

- 品質の良いサービスが選べない
  → **品質の良い脆弱性診断を選べる基準作り**

- 必要な技術や知識を明確にしたい
  → **スキルマップ、シラバス**

- 技術力の向上や人材育成
  → **ガイドライン**



そこで

脆弱性診断士
スキルマップ＆シラバス
Webアプリケーション編
プラットフォーム編

作りました！

脆弱性診断士

- 高い倫理を持ち、適切な手法で IT システムの脆弱性診断を行える者
- 求める技術や知識をスキルマップ化
- Webアプリケーションの脆弱性診断にフォーカスした内容

「脆弱性診断士」ランク

JNSA

２つのランクを定義

- Silver ランク
  - –脆弱性診断業務に従事する者が全員知っておくべき技能

- Gold ランク
  - –単独で診断業務を行うために必要な技能

分野	大分類	中分類	小分類	Silver	Gold	スキル	用語例（修得すべき用語、キーワード）
基礎知識（技術）	標準的なプロトコルと技術	プロトコル	IP	○	○	IPアドレスの形式を理解している(S/G) IPv6アドレスの形式を理解している(G) ブロードキャストアドレスを理解している(S/G) サブネットマスクの計算ができる(S/G)	IPアドレス、グローバルIPアドレス、プライベートIPアドレス、サブネットマスク、ルーティング、デフォルトゲートウェイ、ネットワークアドレス、NAT/NAPT、IPマスカレード、static NAT、dynamic NAT
			TCP	○	○	ローカルアドレスとグローバルアドレスの区別がつく(S/G)	コネクション指向、制御フラグ、3wayhandshake、ポート、確認応答、順序制御、再送制御、ユニキャスト
			UDP	○	○	ブラウザにURLを入れてから画面が表示されるまでの一連の流れを理解している(S/G)	トランザクション指向、ポート、リアルタイム性、マルチキャスト、ブロードキャスト
			SSL/TLS	○	○	SSLの役割（機密性・完全性）を理解している(S/G) TCP接続上で任意のデータを送受信できる(G)	認証、暗号化、改竄検出、OpenSSL、鍵共有、証明書、ネゴシエーション、サーバ認証、クライアント認証、デジタル証明書
			HTTP	○	○	SSL/TLS上で任意のデータを送受信できる(G) HTTPの基本的な役割、機能を理解している(S/G)	クライアント、サーバー、リクエスト、レスポンス、ステートレス、持続的接続、パイプライン
			HTTPS	○	○	HTTP上で任意のデータを送受信できる(S/G)	SSL、TLS、公開鍵、証明書
			HTTP/2	×	○	HTTPS の基本的な動作を理解している(S/G)	サーバプッシュ、HPACK
			WebSocket	×	○	HTTP/2の基本的な役割、機能を理解している(G)	ws:、wss: 、双方向通信
			IPv6	×	○	WebSocketの基本的な役割、機能を理解している(G) WebSocket上で任意のデータを送受信できる(G)	IPv6アドレス、サブネットマスク、近隣探索、ユニキャストアドレス、エニーキャストアドレス、マルチキャストアドレス、グローバルユニキャストアドレス、リンクローカルユニキャストアドレス、ユニークローカルユニキャストアドレス
		名前解決	トップレベルドメイン(TLD)	○	○	hostsファイルなどの書き換えができる(S/G) OSの名前解決の仕組みを理解している(S/G)	トップレベルドメイン(TLD)、gTLD、ccTLD、sTLD
			ICANN	×	○	ドメインの階層構造（ホスト名・サブドメイン）を理解している(S/G) 名前解決の仕組みを理解している(S/G)	ICANN、APNIC、JPNIC、JPRS
			静的な名前解決（hostsファイル）	○	○		hostsファイル、名前解決、別名定義
			DNS	○	○	コマンドを用いて、任意のDNSレコードの正引き・逆引きができる(S/G) Whoisで提供される情報を理解している(S/G)	正引き、逆引き、レコード、権威サーバ、キャッシュサーバ、ゾーン転送、再帰問い合わせ、DNSSEC
			ドメイン管理の仕組み	×	○	ドメイン管理の仕組みを理解している(G)	レジストラ・レジストリ
		文字コード		○	○	一般的に使われる文字エンコーディングを理解している(S/G) ブラウザや診断ツールのエンコーディングの設定が適切にできる(S/G)	UTF-8、Shift_JIS、EUC-JP、ISO-2022-JP、ASCII
		メール	SMTP/POP/IMAP	○	○	SMTPの基本的な役割、機能を理解している(S/G) メールの送受信に必要なMUAの設定ができる(S/G) SMTPコマンドを用いて任意のメールメッセージを送信できる(G)	MTA、MUA、MAIL FROM、RCPT TO、SMTP/POP/IMAP、メールヘッダー

想定している利用用途

人事関連分野

- 採用基準、能力判定、人事評価基準、セキュリティエンジニアの人材育成

開発関連分野

- リリース前の要件、システムの品質向上

発注関連分野

- 入札仕様、診断サービス依頼先の選定

今後

- 今後は脆弱性診断ガイドラインを出す予定
- 資格化できるかな？
  - 開発者が自分たちで診断ができる時代がくる
  - 診断会社のレベルが上がり、可視化できる
  - 入札時や発注時の要件として盛り込める

セキュリティオペレーション連携WG

ISOG-J WG6

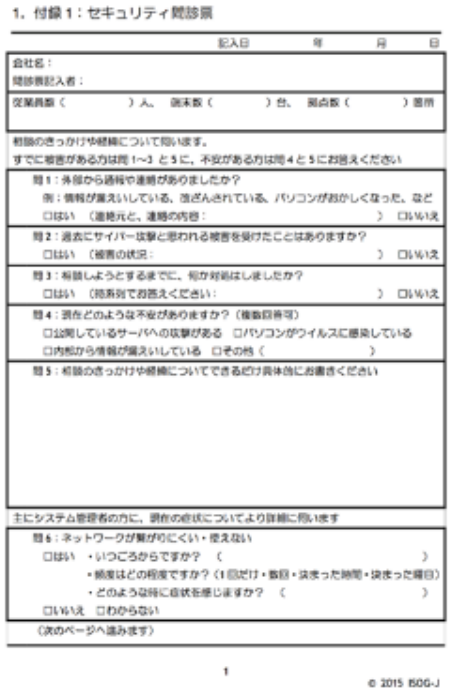
「やられたかな？その前に」ガイドの紹介

- 2015年10月に公開
- PDF形式の利用ガイドと、セキュリティ問診票のdocx形式の2つのファイルを公開

- 2015年度初頭の個人情報流出事件を受けて、セキュリティ事業者への相談、問い合わせが増えたため、あらかじめ確認しておくべき事項や、普段から注意しておいて欲しい事項を「セキュリティ問診票」という形式で取りまとめた

セキュリティ問診票

- 設問は全27問
- ISOG-J HPにて公開中
- http://isog-j.org/activities/result.html



1. 付録1：セキュリティ問診票

記入日　　年　　月　　日

会社名：
問診票記入者：

従業員数（　　）人、　端末数（　　）台、　拠点数（　　）箇所

相談のきっかけや経緯について伺います。
すでに被害がある方は問 1～3 と 5 に、不安がある方は問 4 と 5 にお答えください

問 1：外部から通報や連絡がありましたか？
例：情報が漏えいしている、改ざんされている、パソコンがおかしくなった、など
□はい　（連絡元と、連絡の内容：　　）　□いいえ

問 2：過去にサイバー攻撃と思われる被害を受けたことはありますか？
□はい　（被害の状況：　　）　□いいえ

問 3：相談しようとするまでに、何か対処はしましたか？
□はい　（時系列でお答えください：　　）　□いいえ

問 4：現在どのような不安がありますか？（複数回答可）
□公開しているサーバへの攻撃がある　□パソコンがウイルスに感染している
□内部から情報が漏えいしている　□その他（　　）

問 5：相談のきっかけや経緯についてできるだけ具体的にお書きください

主にシステム管理者の方に、現在の症状についてより詳細に伺います

問 6：ネットワークが繋がりにくい・使えない
□はい　・いつごろからですか？（　　）
・頻度はどの程度ですか？（1 回だけ・数回・決まった時間・決まった曜日）
・どのような時に症状を感じますか？（　　）
□いいえ　□わからない

（次のページへ進みます）

1

© 2015 ISOG-J

相談のきっかけや経緯について伺います。
すでに被害がある方は問 1～3 と 5 に、不安がある方は問 4 と 5 にお答えください

問 1：外部から通報や連絡がありましたか？
例：情報が漏えいしている、改ざんされている、パソコンがおかしくなった、など
□はい　（連絡元と、連絡の内容：　　）　□いいえ

問 2：過去にサイバー攻撃と思われる被害を受けたことはありますか？
□はい　（被害の状況：　　）　□いいえ

問 3：相談しようとするまでに、何か対処はしましたか？
□はい　（時系列でお答えください：　　）　□いいえ

問 4：現在どのような不安がありますか？（複数回答可）
□公開しているサーバへの攻撃がある　□パソコンがウイルスに感染している
□内部から情報が漏えいしている　□その他（　　）

Internet Week 2015の発表報告

- 2015年11月19日、Internet Week 2015の2つのセッションにてISOG-Jから発表（発表資料は公開中）
  - https://www.nic.ad.jp/ja/materials/iw/2015/proceedings/

- S13 150分でわかるセキュリティ対応できる組織にする10のコツ
  - 標的型攻撃に代表されるような攻撃の巧妙化、 複雑化とともに、 そのセキュリティ対応も難易度が高まり、 今までのSOC、 CSIRTといった枠組みを超えたものになりつつあります。 このような状況においても、 効果的なセキュリティ対応ができる組織になるための10のコツを、 セキュリティ対応の現場でのベストプラクティスをもとにご紹介します。

- S14 CSIRT時代のSOCとのつき合い方 2015
  - 「CSIRT構築後にセキュリティ監視はどうすべきなのか？」 「外部SOCを使っていれば大丈夫なのか？」 「SIEMを導入すればすぐにプライベートSOCで監視ができるのか？」 これらの疑問に対し、 CSIRTと外部SOC、SIEMの関係を整理した上で、 それぞれの立場からみた課題を抽出し、 社内CSIRTが外部SOCおよびプライベートSOCをどのように活用するべきかを議論します。

2016年度の予定

1. Internet Week 2016での発表
2. 「Ten Strategies of a World-Class Cybersecurity Operations Center」(MITRE) の日本語訳の作成
3. SOCの役割と人材の定義についての検討

Internet Week 2016での発表（の予定）

- IWのサイトにて、2016年11月29日（火）～12月2日（金）、ヒューリックホール＆ヒューリックカンファレンス（浅草橋）にて開催との発表がなされた
- 今年も発表に名乗りを上げます！
- 去年のアンケート結果を振り返りつつ、より良い発表ができるように準備を開始しています！

「Ten Strategies ～」の日本語訳

- MITRE社が無償で公開しているドキュメント
- 総ページ数 330ページ程度

- 世界規模のセキュリティ運用組織（SOC/CSIRT)を作り上げ、運用するための10のコツについて記載。
  - 10のコツに漏れたであろうノウハウも付録にあり、組織論や組織運営の概要を整理して理解するには良い
  - 一方、日本的な習慣に合うかどうか、組織規模に合うかどうかは議論の余地がある

- 去年の発表にて評判も良く、日本語訳のニーズがあるため、今年の活動にて日本語訳に取り組み、公開を目指す

SOCの役割と人材定義

- SOCの役割や必要なスキルを整理して公開を目指す
- ユーザ企業内でのセキュリティ運用組織(SOC/CSIRT)の設立の流れを受けて、ユーザ企業とセキュリティベンダ間での業務の相互理解や役割分担のガイドとなることを想定。
- アウトソース可能な部分、アウトソースが不可能な部分、そして担当者に必要なスキルの整理を行う予定

ご静聴ありがとうございました