NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

セキュ女WG 活動報告会

～脆弱性を紐解く　サブWGの活動について

ドコモ・システムズ(株)　北澤　麻理子
日本マイクロソフト(株)　村木 由梨香
(株)NSD　大鐘　博子

セキュ女WGについて

活動目的　WGへの期待

- 会社枠を超えた女性セキュリティエキスパートの交流場所を提供。セキュリティに関する専門スキルを持ちたい女性を応援する。
- (呑み会ではない)業務上の悩みごとなどを話せる場としても意義がある。
- 登録メンバ　39名

2016年度活動実績

開催月	会場	主な内容
6月	ドコモ・システムズ	年度方針ディスカッション
8月	富士通	富士通テクノロジーホール見学会
8月	日本マイクロソフト	脆弱性ハンズオン勉強会
10月	JNSA	マイクロソフトが見た　情報セキュリティ「あるある事例」からの考察
12月	日本マイクロソフト	脆弱性ハンズオン勉強会
2月	新橋	JNSAボードゲーム体験会
3月	DIT	アウトプットし続ける技術。毎日書くためのマインドセットとスキルセット 勉強会

サブWG	脆弱性情報を紐解く…	
全4回	JNSA	脆弱性対応の悩み共有、情報サイトのリスト作成

サブWG　経緯

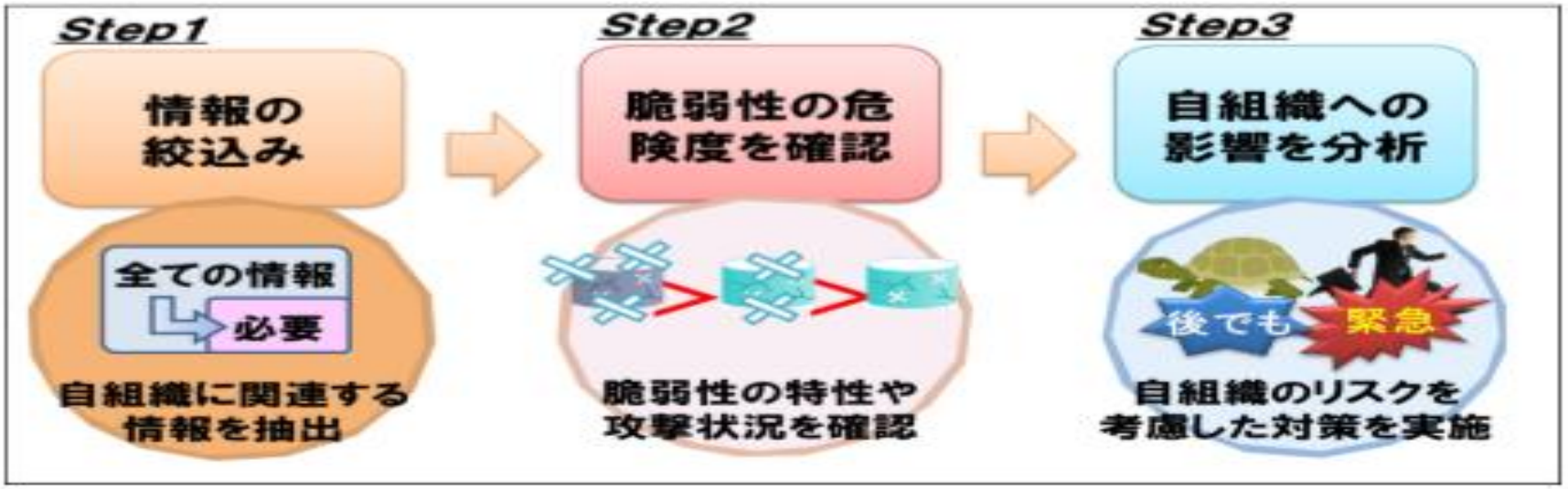
JNSA

- セキュ女WGメンバーの脆弱性対応にまつわる悩み
  - ベンダーから情報が出ていない段階でキャッチした脆弱性をどう判断する？そもそも脆弱性？
  - お客様に、わかりやすく、正確に、脆弱性の影響度や適用へのアドバイスをするにはどうしたら？
  - そもそもこのシステムにこの脆弱性のパッチの適用は必要なの？どうやって判断したらいいの？
  - セキュリティ会社から脆弱性情報のアラートをもらっているけど、これをそのまま適用評価にしてもいいの？どのように判断したらいいの？

メンバ間で共通認識を持つ

JNSA

- 自社サービス・システムなどが影響を受ける可能性のある、他社の脆弱性が公表され、セキュリティパッチなどを適用しなければならないケースで、どのように情報を収集し、分析し、適用を判断しているのかについて、それぞれの経験や悩みを話し合う



出典：脆弱性対策の効果的な進め方（実践編） ～脆弱性情報の早期把握、収集、活用のスヽメ～
http://www.ipa.go.jp/security/technicalwatch/20150331.html

事前課題

(例)ワークシート

自身の役割：脆弱性情報を収集し、顧客に対して情報を提供している

	STEP 1 情報の絞込み	STEP 2 脆弱性の危険度(深刻度)を確認	STEP 3 組織への影響を分析
実施した事項	1次情報元を確認。 ・Cisco Security Advisory ・Bug Search ・SHIELDインテリジェンスサービスから対象製品、対策方法を確認。 ・NVD、JVN等を確認⇒情報なし ・セキュリティニュースサイト確認。 ・攻撃観測があり、攻撃ツールが流通していることを確認。 ・Exploit DBにはPoCなし。	危険度としては高いと判断。 攻撃ツールも出ているため、通常ならば「速報」としてお知らせするものだが、対応策がないため、しばらく顧客への通知を控えた。	CiscoのIKEv1を使用している想定で影響度を判断。 以下の観点で影響を分析。 ・リモートから任意のコード実行可能？ ・リモートからサービス運用妨害可能？ ・構成上脆弱性対応できなくないか⇒結果、「high」と判断。
悩み	ニュースサイトやSNSからの情報を契機に調査を開始しているが、情報の信憑性について悩むことが多い。	危険度が高いが、セキュリテイパッチがリリースされておらず、ワークアラウンドもなかった。 情報提供のタイミングで悩んだ	お客様の環境を全て把握できないため、組織への影響度の分析ができないことが多い。
ほかの参加者に聞きたい点	・どのようなサイトを見ているか？ ・攻撃ツールやPoCなどが出ている場合、検証を行っているか？また、どこから入手しているか。	・対応策がない場合でも顧客や社内に対して情報を提供しているか？ ・対応策がない場合の、独自の臨時対応方法はあるか？	・お客様がサポート切れの製品を使用していて、ベンダページには該当バージョンの情報がない場合に、影響度調べる方法はあるか？ ・サポート切れの製品への問合せがあった場合、どのような対応を取っているか？

4回の活動を通じて…

JNSA

- 脆弱性対応の実際の体験や悩みを共有
  - IPA 脆弱性ハンドリングガイドを読む
  - 日々、業務で対応している体験を元に、脆弱性にまつわるハンドリングの流れ、悩みを共有

- 脆弱性ハンドリングにおいて利用している情報サイトや利用の仕方を共有し、一覧を作成した
  - フェーズ、ソースタイプ、情報タイプでグループ分けしてリストを作成
  - 作成したリストをもとにどのようなサイトか、利用しているシーンなどを共有

フェーズ
情報の絞り込み
脆弱性の危険度を確認
組織への影響を分析

ソースタイプ	
カンファレンス	注意喚起
データベース	ベンダーサイト
Twitter	ニュースサイト
セキュリティ教育サイト	ブログ

情報タイプ
攻撃手法
脆弱性公式情報
マルウェア検体
ニュース記事
リサーチャー見解

リスト

JNSA会員メンバのみ公開

セキュ女WG　メンバー募集中!!

◘今後の勉強会予定

- PKIの濃い話 勉強会（6月）

◘今後の勉強会テーマ(昨年度案の抜粋)

- セキュリティコンサル業務においてリスク対応をどこまで求めるか（リスクレベルや組織事情によるさじ加減）
- 脆弱性情報に関して、製品提供側と利用側とのディスカッション
- 監査時のヒアリングのコツ
- ポートスキャン等のハンズオン(昨年度から継続)
- 役に立った本やサイト等の情報共有(⇒サブWGへ)

ありがとうございました