「CSIRT人材の定義と確保」趣旨説明

2016年2月23日

日本シーサート協議会 CSIRT人材SWG
主査 松本

このセッションでは・・・

- 日本シーサート協議会 CSIRT人材SWGのご紹介
- 「CSIRT人材の定義と確保」作成の背景
- 「CSIRT人材の定義と確保」の特徴
- 「CSIRT人材の定義と確保」の解説（阿部）

このセッションでは・・・

- 日本シーサート協議会 CSIRT人材SWGのご紹介
- 「CSIRT人材の定義と確保」作成の背景
- 「CSIRT人材の定義と確保」の特徴
- 「CSIRT人材の定義と確保」の解説（阿部）

CSIRT人材SWG – 概要

正式名称	日本コンピュータセキュリティインシデント対応チーム協議会 シーサート人材サブワーキンググループ
目的	各CSIRTにおける人材に関する悩み・問題を解決に導く
活動期間	2014年10月～
運営担当	SoftBank CSIRT　松本　（責任者） MBSD-SIRT　大河内　（副責任者） NTT-CERT　杉浦　（副責任者）

CSIRT人材SWG – 活動成果

CSIRT人材の定義と確保 Ver.1.0

2015/11/26 リリース（全44ページ）

- 新たにCSIRTを構築する、CSIRTの役割の一部をアウトソーシングする、あるいは、CSIRTを担う人材を定義・確保する等の参考になる情報の提供
- 社内向けのCSIRT人材の募集要項作成、あるいは、CSIRTの機能や人材を社外に求める場合のRFP(提案依頼書)や人材の募集要項作成のための参考になる情報の提供

（参考）資料の入手

CSIRT 日本シーサート協議会

（参考）資料の入手

CSIRT 人材

検索

このセッションでは・・・

- 日本シーサート協議会 CSIRT人材SWGのご紹介
- 「CSIRT人材の定義と確保」作成の背景
- 「CSIRT人材の定義と確保」の特徴
- 「CSIRT人材の定義と確保」の解説（阿部）

資料作成の背景

こんなことは、ないでしょうか？

資料作成の背景 – これからCSIRTを作る場合

いきなりCSIRTを作れと言われたけど、どんな人を集めればいいのかわからない

資料作成の背景 – 作った直後の場合

CSIRTはとりあえず作ったけど、名ばかり。はやく適切な人員構成にしたい

資料作成の背景 – 数年たった場合

CSIRTを運営して早N年。気が付けば平均年齢が+N歳。後継者をどうしよう。

資料作成の背景 – 陥りやすい罠

セキュリティ（何でも）出来る人
寄越して

（サイバー攻撃を防いでくれる）
ホワイトハッカーください

そんな人は、まずいない

このセッションでは・・・

- 日本シーサート協議会 CSIRT人材SWGのご紹介
- 「CSIRT人材の定義と確保」作成の背景
- 「CSIRT人材の定義と確保」の特徴
- 「CSIRT人材の定義と確保」の解説（阿部）

特徴1：CSIRTの役割を定義

グループ	役割名称	業務内容
情報共有	PoC(社外)	NCA、FIRST、CSIRT、警察、監督官庁、等々との情報連携
	PoC(社内)	法務、渉外、IT部門、広報、各事業部、等々との情報連携
	IT部門との連携	適格で要領を得た文書の作成
	リーガルアドバイザー	コンプライアンス、法的内容とシステム間の翻訳
	ノーティフィケーション	各関連部署との連絡ハブ、情報発信
情報収集・分析	リサーチャー、キュレーター	定例業務。インシデントの情報収集、各種情報に対する分析、国際情勢の把握
	脆弱性検査、診断	NW、OS、セキュアプログラミングの検査、診断
	脆弱性分析、評価	NW、OS、セキュアプログラミング診断結果の評価
	セルフアセスメント	平時のリスクアセスメント。有事の際の脆弱性の分析、影響の調査
	ソリューションアナリスト	ソリューションマップ作成、FiT&Gap分析、リスク評価、有事の際の有効性評価
インシデント対応	コマンダー	全体統括。意思決定。社内PoC。役員、CISO、または経営層との情報連携
	インシデント管理	インシデントの対応状況の把握。コマンダーへの報告。対応履歴把握。
	インシデントハンドラー	インシデント現場監督。セキュリティベンダーとの連携
	インベスティゲーター	社内捜査に必要な論理的思考、分析力、社内システム理解力を使った内偵
	トリアージ	事象に対する優先順位の決定。
	フォレンジックス	証拠保全、システム的な鑑識、足跡追跡。マルウェア解析。
社内教育	教育、啓発	社内のリテラシー向上、底上げ。

特徴2：CSIRTをパターン分け

パターン	定義
例A	ユーザ企業で総務部門等を主体として構築・運用されているCSIRT
例B	ユーザ企業でIT系子会社、または情報セキュリティに関する専門部門を主体として構築・運用されているCSIRT
例C	IT系、セキュリティベンダー系企業において構築・運用されているCSIRT
例D	その他(学術機関、政府機関、法執行機関など)

※資料において例Dは対象としていない

特徴3：現役CSIRT関係者による執筆、監修

阿部 恭一	ASY-CSIRT	ANAシステムズ株式会社
羽場 満	Canon-CSIRT	キヤノン株式会社
橋村 泰慶	DIR-CSIRT	株式会社大和総研ホールディングス
青木 一郎	DMM.CSIRT	株式会社DMM.comラボ
寺西 一平	DMM.CSIRT	株式会社DMM.comラボ
佳山 こうせつ	FJC-CERT	富士通株式会社
寺田 真敏	HIRT	株式会社日立製作所
沼田 亜希子	HIRT	株式会社日立製作所
徳田 敏文	IBM-CSIRT	日本アイ・ビー・エム株式会社
吉田 香織	iD-SIRT	株式会社インフォメーション・ディベロプメント
高杉 秋子	JPBank CSIRT	株式会社ゆうちょ銀行
森下 明宏	JPBank CSIRT	株式会社ゆうちょ銀行
満永 拓邦	JPCERT/CC	一般社団法人JPCERTコーディネーションセンター
佐藤 芳紀	MB-SIRT	森ビル株式会社
大河内 智秀	MBSD-SIRT	三井物産セキュアディレクション株式会社
鳥島 由美子	MBSD-SIRT	三井物産セキュアディレクション株式会社
渡辺 隆志	mixirt	株式会社ミクシィ
杉浦 芳樹	NTT-CERT	日本電信電話株式会社
関戸 直生	NTT-CERT	日本電信電話株式会社
二関 学	NTT-CERT	日本電信電話株式会社
溝口 和寛	NTT-CERT	日本電信電話株式会社
大山 千尋	NTTDATA-CERT	株式会社NTTデータ
松本 勝之	SoftBank CSIRT	ソフトバンク株式会社
萩原 健太	TM-SIRT	トレンドマイクロ株式会社
六宮 智悟	TM-SIRT	トレンドマイクロ株式会社
大内 和博	YIRD	ヤフー株式会社
山賀 正人	専門委員	

このセッションでは・・・

- 日本シーサート協議会 CSIRT人材SWGのご紹介
- 「CSIRT人材の定義と確保」作成の背景
- 「CSIRT人材の定義と確保」の特徴
- 「CSIRT人材の定義と確保」の解説（阿部）