

IP Meeting 2015 ～手を取り合って、垣根を越えて。～

企業における教育の実際 ～セキュリティ人材の育成～

NTTコミュニケーションズ株式会社

NTT Com-SIRT / 技術開発部

畑田 充弘

スコープ

	マネジメント系	エンジニア系
上級	製造や金融等の業界毎のドメイン知識を持って経営課題を解決できる	マルウェア解析やフォレンジック等の技術分野で新技術を生み出し、高度な分析ができる
中級	情報セキュリティマネジメントの推進、脆弱性管理等でリスクを低減できる	個々の技術分野を理解し、技術を駆使してインシデント対応やシステム開発ができる
初級	ICTシステムの基礎技術とセキュリティの概念を理解し、セキュリティ向上に向けた業務を遂行できる	

スキルレベル



Global ICT Partner
Innovative. Reliable. Seamless.

企業のセキュリティ人材育成における課題認識

■ 前提スキル

- サーバ、アプリケーション、ネットワーク等々

■ リアリティ

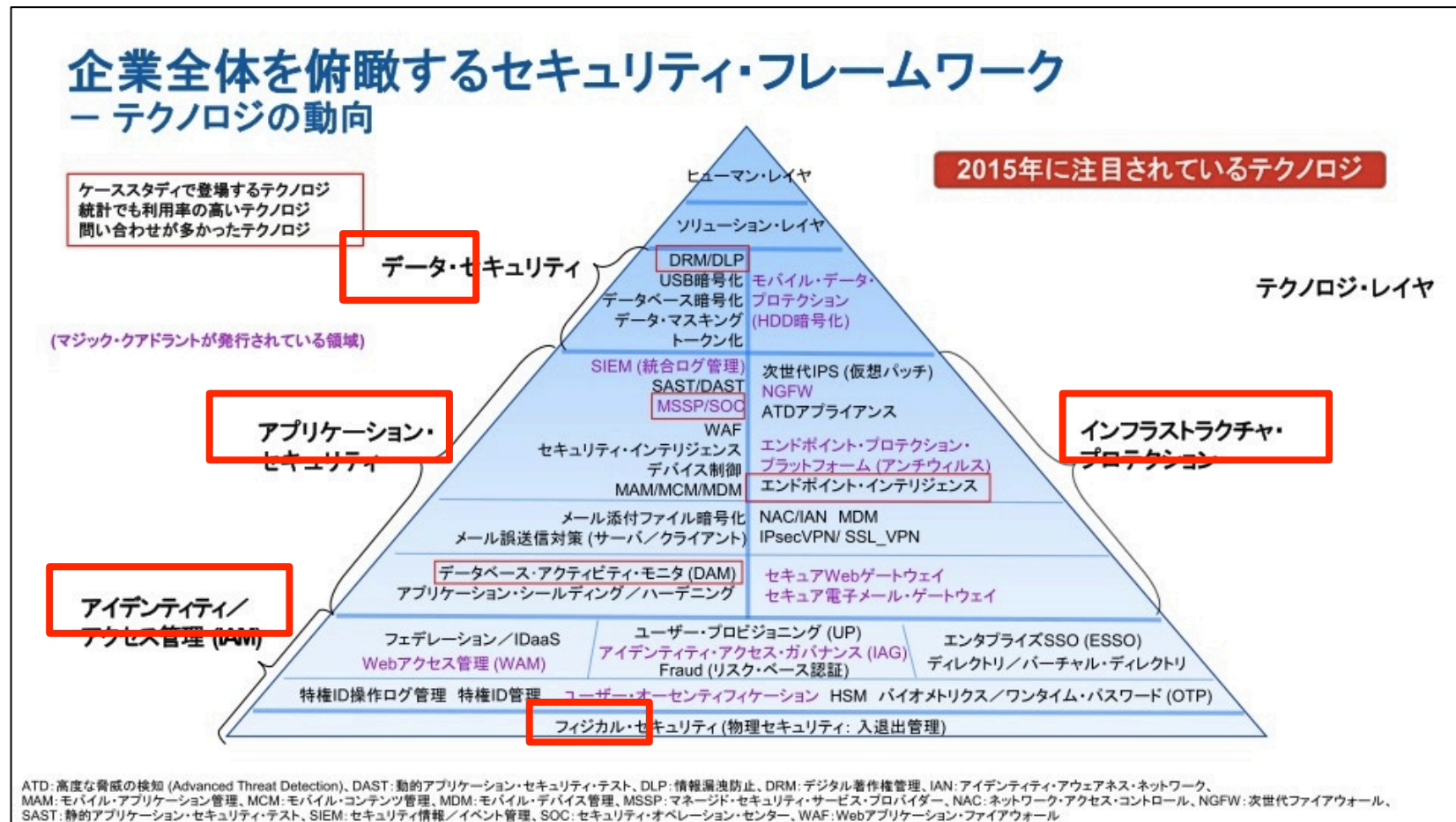
- 一般論ではなく自社に適した演習不足

■ キャリアパス

- スペシャリストとして生きるモチベーション

前提スキル

守る対象（構成要素）の技術の理解が必須



ATD: 高度な脅威の検知 (Advanced Threat Detection), DAST: 動的アプリケーション・セキュリティ・テスト, DLP: 情報漏洩防止, DRM: デジタル著作権管理, IAN: アイデンティティ・アウェアネス・ネットワーク, MAM: モバイル・アプリケーション管理, MCM: モバイル・コンテンツ管理, MDM: モバイル・デバイス管理, MSSP: マネージド・セキュリティ・サービス・プロバイダー, NAC: ネットワーク・アクセス・コントロール, NGFW: 次世代ファイアウォール, SAST: 静的アプリケーション・セキュリティ・テスト, SIEM: セキュリティ情報/イベント管理, SOC: セキュリティオペレーション・センター, WAF: Webアプリケーション・ファイアウォール

出展: ガートナー / <http://www.sbbt.jp/article/cont1/30214>



リアリティ

研修 ≠ 演習・訓練

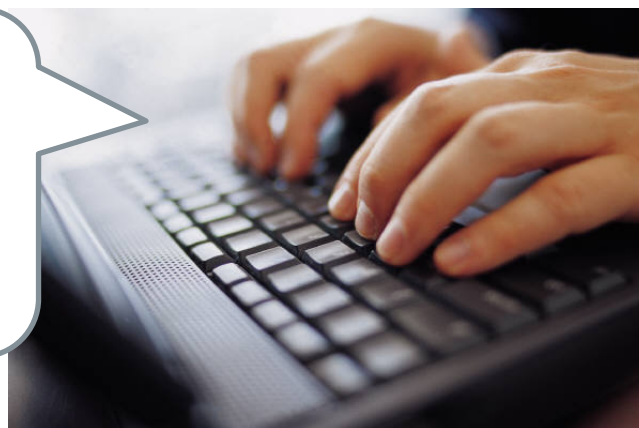
あなたはある組織のセキュリティ管理者です。インシデント発生 of 報告を・・・



ふ～ん、このフォーマットを埋めればいいのね

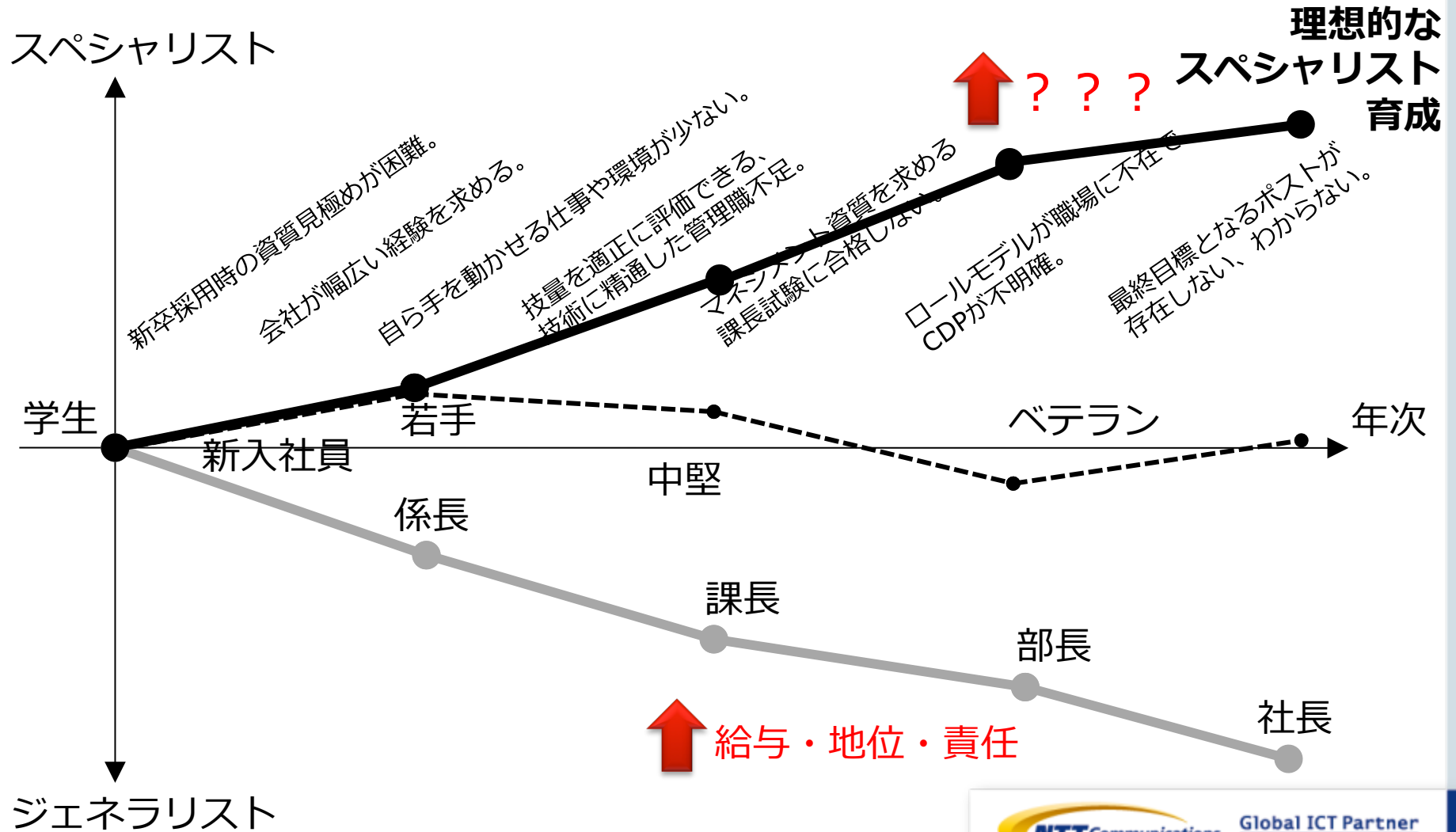


単純なSQLiね、
へー、こういう
ツール使えばお手
軽！
メモメモ



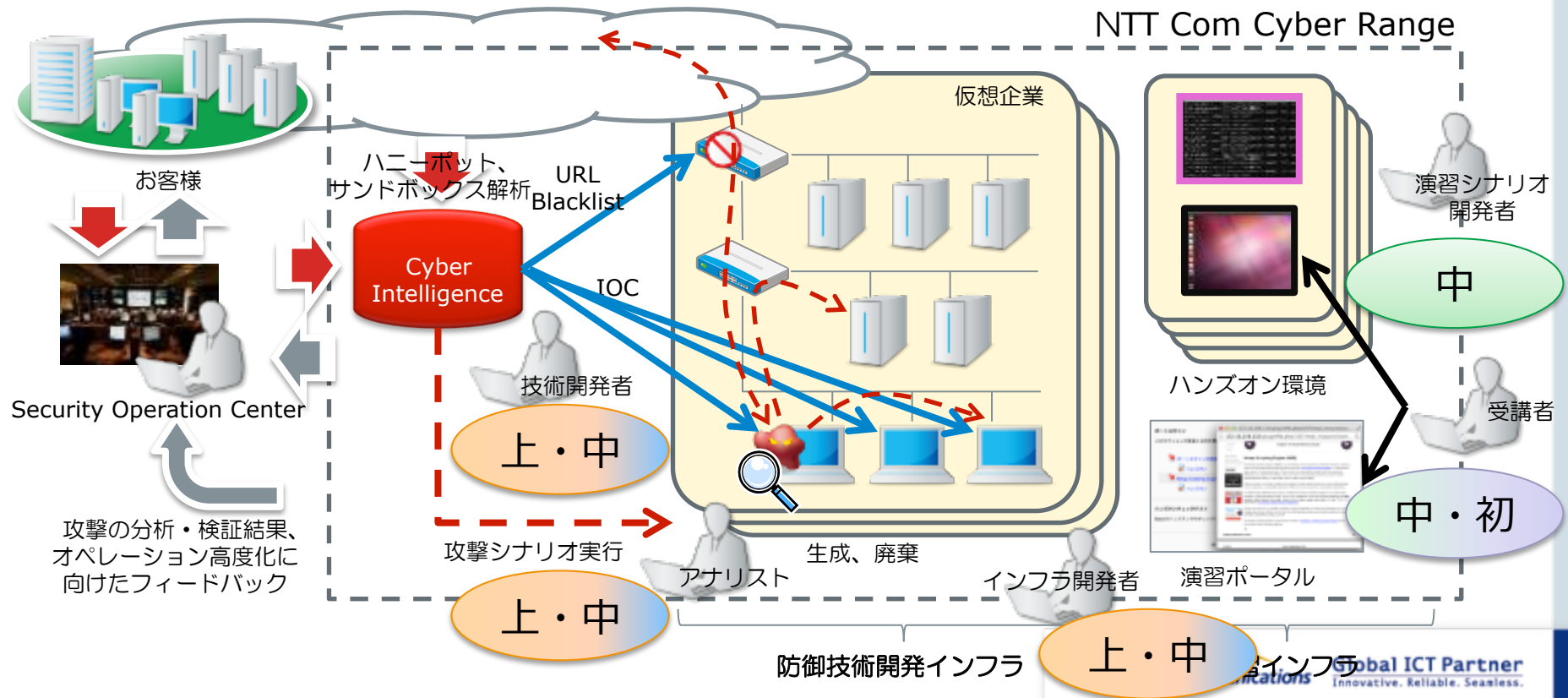
キャリアパス

スペシャリティとモチベーションのバランス



Cyber Rangeでの人材育成の取り組み～Security Bootcamp～

- セキュリティ技術の習得をハンズオン中心に行い、インシデントレスポンスやフォレンジック等の実務に応用可能な実践力を習得
 - 基本的な脆弱性への攻撃・防御手法の習得（BASICコース）
 - インシデント事例を基に防御対象・攻撃手法・対策を通じて、「調べ方」「考え方」「試し方」など応用力を習得（ADVANCEDコース）



Security Bootcamp カリキュラム例

知識確認テスト（自己分析）

BASIC	基礎・NW	暗号、ハッシュ、電子署名
		認証、パスワード
		ポートスキャン
		プログラミング基礎
		パケットキャプチャ・パケット生成
	SSL	
	Webアプリ	SQLi、XSS、CSRF
		Webアプリ構築、セキュアコーディング
	スマホ 無線LAN	Android
		無線LAN
	バイナリ	x86アセンブリ、デバッガ、シェルコード
		スタックバッファオーバーフロー
ヒープオーバーフロー、フォーマットストリング攻撃		

ハンズオンテスト

ADVANCED	Webアプリケーションフレームワーク脆弱性への攻撃、対策
	DbD&RAT、Forensic
	DDoS攻撃、対策
	標的型メール攻撃、対策

演習振り返り（自己分析+フィードバック）

Security Bootcamp実績 (2015/8末時点)

会社名		人数	期間	内容
NTTコム	NTTコム グループ会社	4名	2014/5/19~8/末	・ BASIC、ADVANCEDコース ・ 週3回、実質31営業日
	〇〇部	4名	2014/8/6~10/末	・ 2014年度新入社員 ・ BASICコース+個別カリキュラム ・ 実質58営業日
	NTTコム グループ会社			
	NTTコム グループ会社	4名	2015/5~8	・ 2015年度新入社員 ・ BASICコース+個別カリキュラム
	〇〇部	3名	2015/5~	・ BASIC、ADVANCEDコース ・ 毎週火曜数時間程度
NTTコム グループ会社	2名	2015/5/11~6/26	・ BASIC、ADVANCEDコース ・ 平日週3回、実質21営業日	
NTT〇△社	△△部	2名	2014/7/22~9/5	・ BASIC、ADVANCEDコース ・ 平日日勤帯、実質28営業日
	□□部			
	△△部	2名	2014/11/11~12/25	・ BASIC、ADVANCEDコース ・ 平日日勤帯、実質32営業日
	□□部			
	△△部	2名	2015/2/2~3/27	・ BASIC、ADVANCEDコース ・ 平日日勤帯、実質40営業日
	□□部	3名	2015/5/11~6/26	・ BASIC、ADVANCEDコース ・ 平日日勤帯、実質35営業日
△△部				
NTT△□社	〇△室	3名	2014/9/25~12/25	・ BASICコース、ADVANCED短縮コース ・ 平日週3回、実質25営業日
	△□部			
	□〇部			
	〇△室	3名	2015/2/2~3/27	・ BASICコース、ADVANCED短縮コース ・ 平日週2日、実質16営業日
	△□部			
	□〇部	2名	2015/6/4~7/31	・ BASICコース、ADVANCED短縮コース ・ 平日週2日、実質18営業日
□□部				
△〇部				
NTT□〇社	□□部	3名	2014/11/11~2015/1/9	・ BASIC、ADVANCEDコース ・ 平日週2日、実質15営業日
(参考) enPiT SecCap PBL演習 (学生向け)		20名	2014/8/25	・ BASICの2単元、ADVANCEDの1単元の短縮コース ・ 実質1営業日
		28名	2015/8/31	

企業のセキュリティ人材育成における課題認識 →対策

- 前提スキル →演習内でも構築
 - サーバ、アプリケーション、ネットワーク等々
- リアリティ →社内等事例を再利用
 - 一般論ではなく自社に適した演習不足
- キャリアパス →by nameでのロールモデル
 - スペシャリストとして生きるモチベーション
- Security Bootcampからの教訓
 - モチベーション →好き or 使命感の共有
 - 現業との兼ね合い →（技術で遊ぶ）時間の占有
 - 仲間作り、教え合う相手 →場の共有

手を取り合って、垣根を越えて、攻撃者に立ち向かおう！