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

今、わが国のセキュリティ産業に求められる変革とは何か

2017年6月12日

セキュリティ被害調査ワーキンググループ
長崎県立大学 情報システム学部情報セキュリティ学科

自己紹介

所属：株式会社 NTTデータ セキュリティ技術部
情報セキュリティ推進室 NTTDATA-CERT

セキュリティ被害調査ワーキンググループ リーダー

- リスクアセスメント、社内セキュリティ施策
- ネットワークセキュリティ、検知技術
- セキュリティ診断、セキュア開発
- CSIRT、インシデントハンドリング、フォレンジック
- セキュリティ分野の研究開発

論点１

わが国の情報セキュリティ産業の弱点と強みについて

- 日本のセキュリティ産業の弱点/強み
  - （弱点）海外進出が弱い。限定的 /（強み）技術力は悪くない
- 自社の弱点/強み
  - （弱点）セキュリティ製品開発
  - （強み）ベンダ非依存の構築・運用ニーズがある製品、良い製品を採用
- 日本のCSIRT の弱点/(強み?)
  - 隠蔽体質、依存体質
  - 分野内、分野間の情報共有が弱い。
    縦割りの情報共有。SEPTERで脅威情報が分断されている

論点２

最近のIoT・ビックデータ・AI時代を踏まえて、その活路は何処にあるのか

- IoT・ビックデータ・AIに国内企業の活路はあるのか？
  - 企業におけるセキュリティ研究開発の減少
  - 海外ベンダ（ベンチャー）のビジネス化スピードが早い

  →（今から巻き返すなら）研究開発から商用化までの速度アップ

- 国内企業がセキュリティビジネスを伸ばすためには？
  - 国内だけでなくグローバルなビジネスをめざす
  - 地域（北米、欧州、アジア、南米etc）によってニーズに差がある

  →狙うエリアによって戦略が変わるため・・・

論点２

最近のIoT・ビックデータ・AI時代を踏まえて、その活路は何処にあるのか

- 東京オリンピックを契機に
  - 「検知～対応技術」と「情報収集～分析～共有技術」の向上

- セキュリティ人材が足りないなら
  - 機械学習・AIによる高速化と自動化(省力化)
  - ただし、単に機械学習・AI技術を採用するだけでは、日本が有利になりにくい。国内製のセキュリティ機器(センサやネットワーク機器)が無いため、導入済製品の拡張や連携はできない。既存製品の置き換え。目新しい製品が出ても、国内企業は性能よりも実績やシェアを重視

論点３

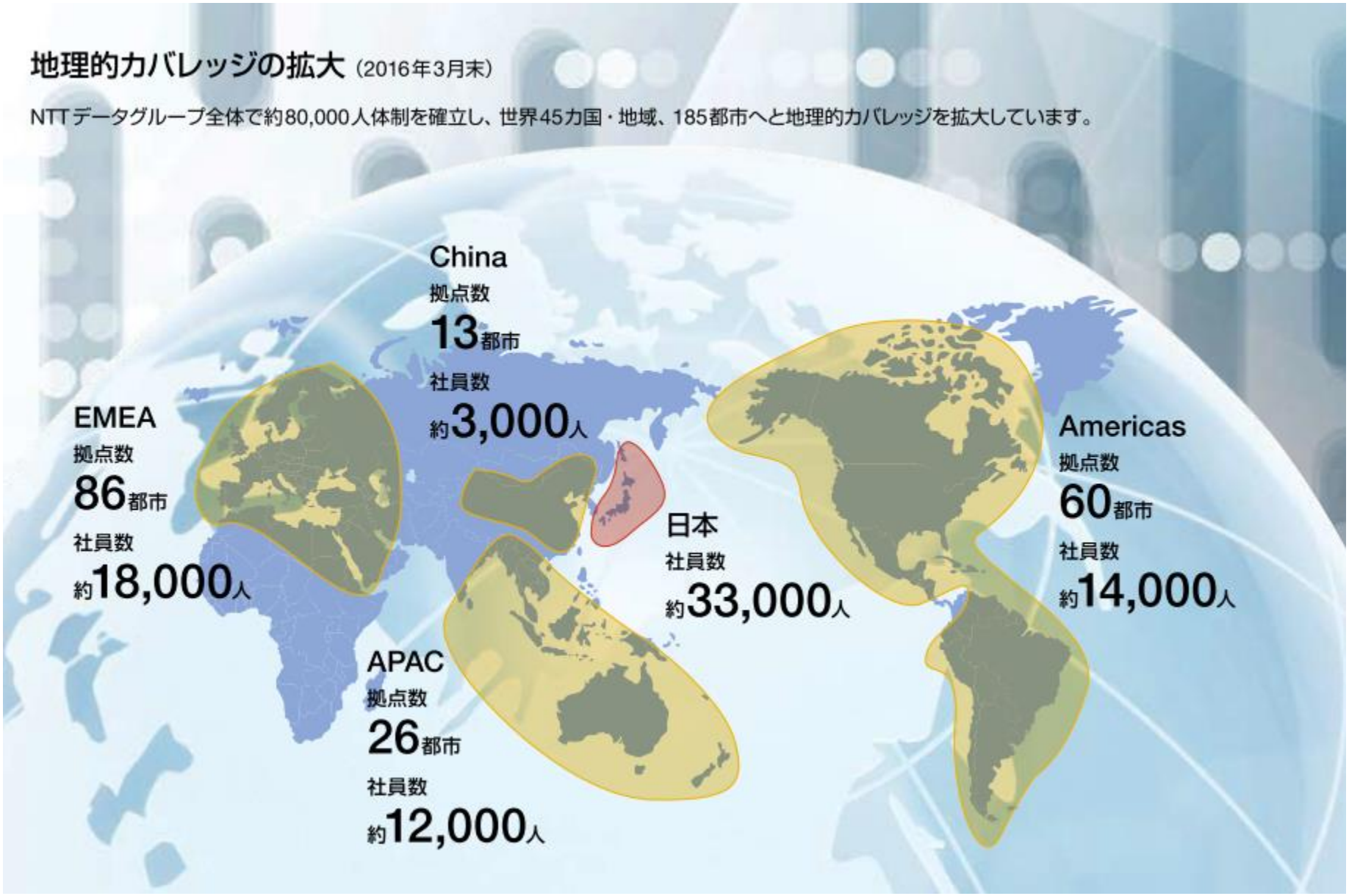
国内のみの人材育成は効果があるのか、間に合うのか

- 弊社の場合
  - 海外グループ会社へCSIRT相当の組織を育成中。
    人材は現地登用。育成 or 有スキル人材採用
  - CSIRT機能や人財スキルのグローバル共通化

  →グローバルなセキュリティ活動のため、国内のみの人材育成ではない

  →海外は終身雇用ではないので、育てても転職してしまう。
  育成よりも採用中心

- 国内企業のセキュリティ人材教育
  - 一般的なセキュリティ技術は、世界共通なので国内のみの育成は意味が無い
  - 国内法やその国の商習慣など、一部の知識は国内依存



論点４

国に期待する施策とは何か（官民学の責任とは）

- 法律（国内/海外）による問題
  - GDPR(EU保護規則)、ワッセナー条約等によってグローバルなセキュリティ活動が制約されるおそれ
    例）海外インターンシップ受け入れに輸出管理に手続きが必要
    　　国をまたいだインシデント対応は、GDPR対応が必要
  - 電気通信事業法「通信の秘密」によって脅威情報共有が制約されるおそれ
    例）標的型攻撃メール/ばらまき型攻撃メールの情報を早期に検知して共有したいが・・・

- インターネット接続システムやソフトウェア製品の安全性基準
  - 電気用品安全法（PSEマーク）、自動車検査登録制度（車検）に相当するものが、ソフトウェアには無い
  - あわせてコスト増に対する支援（減税など）

論点４

国に期待する施策とは何か（官民学の責任とは）

- 突発的に発生する大規模インシデントの対応費用確保の問題
  - 企業の場合、大規模インシデント用に対応費用をプールしておいても、インシデントが発生しないと税金がかかってしまう
  - 保険で転嫁して毎年の固定費にする方法が一般的
  - 保険以外の方法がない

  →インシデント対応費用の積立制度（非課税）

  →インシデント対応費用の無利子融資制度