日本シーサート協議会
「人材の定義と確保」を読み解く

2017年2月18日

ANAシステムズ株式会社

品質・セキュリティ監理室
ANAグループ情報セキュリティセンター
ASY-CSIRT
エグゼクティブマネージャー
阿部恭一

ANA Group 概要

世界をつなぐ心の翼


安心と信頼を基礎に、
世界をつなぐ心の翼で夢にあふれる
未来に貢献します



グループ経営理念

「安心と信頼」はANAグループとお客様との約束であり、経営の根幹に位置づけられる私たちの責務です。
エアライン事業を中核とするANAグループは、「挑戦し続ける」「強く生まれ変わる」「いつもお客様に寄り添う」気持ち、「心の翼」をもって、永続的にこれからの社会の発展に貢献し、「夢あふれる未来」創りの一翼を担っていきます。

グループ経営ビジョン

ANAグループは日本発のエアライングループとして、2機のヘリコプターからはじまり、今やアジアと世界の国々をつなぐエアライングループとなりました。私たちが次に目指していくのは、数あるエアライングループの中からお客様に選ばれ、世界をリードし続ける確固たる地位を築くことです。
お客様の満足を高め、ひとつでも多くの笑顔を生み出し、価値創造を通じ自立した強い企業として発展していきます。経営から従業員まで一人ひとりが力を合わせ、グループ全ての事業活動において、より一層高い品質を追求し続けることでこの目標を必ず実現します。

グループ行動指針(ANA's Way)

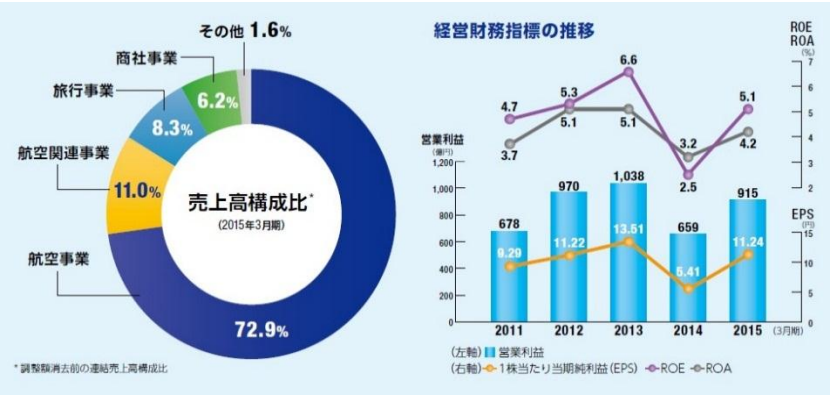
グループ行動指針は、企業グループANAの全社員が理念・ビジョンの達成に向け、持つべき心構えや、取るべき行動をあらわしたものです。
「あんしん、あったか、あかるく元気！」は、ANAらしさとはなにかを探していた私たちがたどり着いた言葉であり、いつも変わらぬ心構えです。

Copyright © 2017 ANA Systems Co.,Ltd., All rights reserved.

ANA Group 概要

ANAグループの事業

ANAホールディングスは、全日本空輸（ANA）、ANAウイングス、エアージャパンという既存のフルサービスの航空事業を行う会社や、LCC事業を担うバニラ・エア、旅行事業を行うANAセールス、商社事業を行う全日空商事などの株式を保有する持株会社です。既存のANAブランドとLCCブランドとの「マルチブランド戦略」の推進、スピード経営の実現、自律的経営を推進し、グループ全体の視点で最適なグループ経営戦略の立案、経営資源の最適配分を目指します。
ANAグループは、これまで以上に安全性の維持・向上を図りつつ、お客様に選ばれ続けるために日々変化するマーケットに機動的に対応し、企業価値・株主価値の向上を目指します。

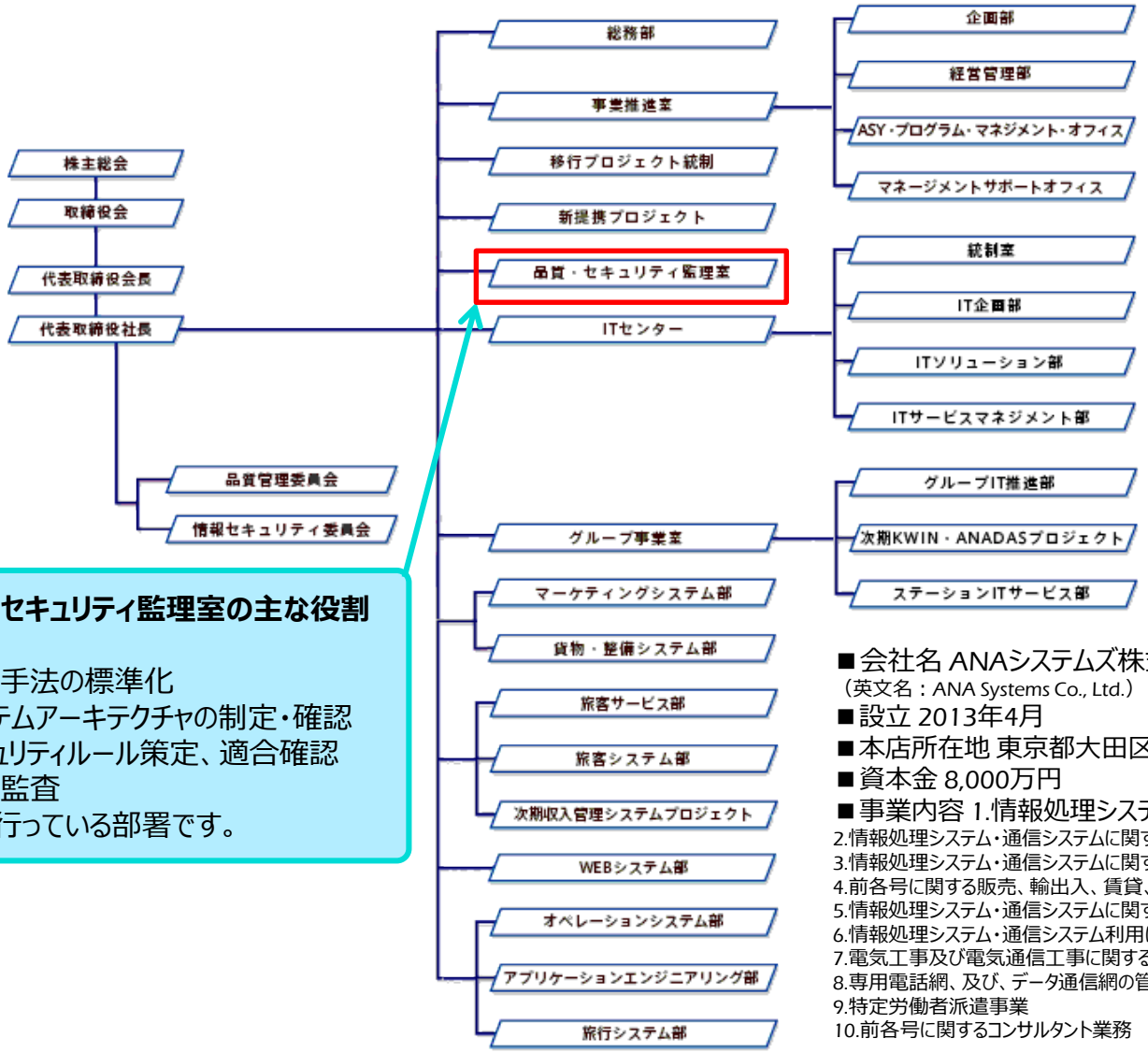


単位：億円（増減率を除き、単位未満は切り捨て）

【連結経営成績】	平成28年3月期	平成27年3月期	増減	増減率(%)
売上高	17,911	17,134	777	4.5
営業費用	16,547	16,219	328	2.0
営業損益	1,364	915	449	49.1
営業外損益	▲57	▲244	186	——
経常損益	1,307	671	635	94.7
特別損益	3	108	▲105	▲96.9
親会社株主に帰属する当期純損益	781	392	389	99.2

Copyright © 2017 ANA Systems Co.,Ltd., All rights reserved.

ANA Group 概要



品質・セキュリティ監理室の主な役割

・開発手法の標準化
・システムアーキテクチャの制定・確認
・セキュリティルール策定、適合確認
・内部監査
などを行っている部署です。

■会社名 ANAシステムズ株式会社
（英文名：ANA Systems Co., Ltd.）
■設立 2013年4月
■本店所在地 東京都大田区東糀谷六丁目7番56号
■資本金 8,000万円
■事業内容 1.情報処理システム・通信システム利用に関する設計及び開発
2.情報処理システム・通信システムに関するソフトウェアの設計及び開発
3.情報処理システム・通信システムに関する設備、機器及び部品の設計、製造、工事
4.前各号に関する販売、輸出入、賃貸、保守及び運用業務
5.情報処理システム・通信システムに関する教育及び訓練業務
6.情報処理システム・通信システム利用による各種情報の収集、処理、及び提供業務
7.電気工事及び電気通信工事に関する設計、施工及び施工監理
8.専用電話網、及び、データ通信網の管理及び再販
9.特定労働者派遣事業
10.前各号に関するコンサルタント業務

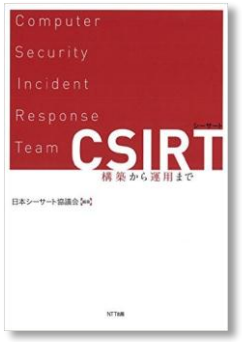
Copyright © 2017 ANA Systems Co.,Ltd., All rights reserved.

ANAシステムズ株式会社
品質・セキュリティ監理室
ANAグループ情報セキュリティセンター
ASY-CSIRT
エグゼクティブマネージャー

阿部恭一

＜外部団体メンバ＞
日本シーサート協議会：CSIRT評価WG、人材WG、机上訓練ＷＧ、トレーニングＷＧ
日本ネットワークセキュリティ協会：情報セキュリティ知識分野（SecBoK）改訂委員
日本情報システム・ユーザ協会：企業リスクマネジメント研究会 サイバーセキュリティ分科会長

＜外部講演２０１６年度＞
ITMediaエンタープライズソリューションセミナー
Interop Tokyo 2016 カンファレンス
AKAMAI セキュリティカンファレンス
FireEye Cyber Defence LIVE Tokyo 2016
国土交通省：観光庁 旅行業界向けセミナー
日経ビジネス経営シンポジウム 会社を滅ぼすITリスクへの対応 セキュリティ編
翔泳社　Security Online Day
AKAMAI カンファレンス2016
ISEPA セキュリティ人材育成セミナー
マイナビ セキュリティセミナー
日経Ｂ Ｐ情報セキュリティマネジメントSummit
大日本印刷 プライベートセミナー
ABC協会セキュリティセミナー
フォーティネットセキュリティセミナー
内閣セキュリティセンター　NISC、各府省庁CSIRT担当向けセミナー
関西CIOカンファレンス



＜著書＞
CSIRT :構築から運用まで（NTT出版：日本シーサート協議会：共著）

Copyright © 2017 ANA Systems Co.,Ltd., All rights reserved.

目次

Copyright © 2017 ANA Systems Co.,Ltd., All rights reserved.

出典：日本シーサート協議会

CSIRT人材の定義と確保(Ver.1.0)

2015年11月16日

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
CSIRT人材サブワーキンググループ(CSIRT人材SWG)

本資料の目的

- 本資料は、各企業のCSIRTにおいて必要な機能、体制、人材を明確にすることによって、CSIRTの継続的な活動を支援することを目的としている。
  特に、次の2点に着目した資料構成としている。
  - 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

Copyright © 2015 Nippon CSIRT Association, All rights reserved.

概要

- 企業のCSIRT活動で対象となる業務範囲は企業によって幅と深さの違いはあるが、前頁の役割と業務内容の策定による。
  本資料は企業の特性によってCSIRTをパターン分けし、CSIRTの役割の自社保有部分、及びアウトソーシング部分を想定した人材の定義と確保に関する情報を例示する。
- 例示には以下を含む。
  - 自社におけるセキュリティ対応の全体像、CSIRTの位置づけ
  - CSIRTの役割
  - 業務の洗い出しとグルーピング、チームのマッピング
  - 有事、平時の体制、業務内容
  - 役割と必要となるスキル
  - 自社保有する役割とアウトソーシングする役割
  - キャリアパス

Copyright © 2015 Nippon CSIRT Association, All rights reserved.

出典：日本シーサート協議会

人材の視点で見たCSIRT構築の流れ

■ 企業内におけるCSIRTの構築は概ね以下のように行うことを想定している。

1. **自社におけるセキュリティ対応の全体像、CSIRTの位置づけの作成**
   自社でのセキュリティに関する社としての要求事項の全体図を概念的に図で表す。会社によって全体像は異なる。
2. **全体像の中で実施する役割の洗い出し**
   全体像の中で社として対象とする役割概要を書き出す。
   また、同時に企業の特性に合わせてその役割を自社保有するのかアウトソーシングするのかを方針を決定する。
3. **役割のグルーピング**
   育成や人材確保に対してはこのグループ単位に行うということを念頭におく。
   グルーピングができたら、その属性毎に組織投入前提条件や、育成計画、スキルパスなどを検討する。
4. **セキュリティ組織に必要な役割の平常時、有事時別の洗い出し**
   企業によっては不要な役割もあり得る。
5. **体制図のデザイン**
   平常時、有事のあるべき体制図を役割をもとに作成する。
   役割のグルーピングより、自社のどのグループの人にどの役割を充てるかがわかりやすくなる。
   時短や女性の活用、高齢者雇用も必要な場合には方針を決定する。
6. **人材募集**
   体制図の中で不足している、強化すべき役割が発見されたら、その役割を充足できるように募集要項を作成する。

Copyright © 2015 Nippon CSIRT Association, All rights reserved.

出典：日本シーサート協議会

組織が保有すべきCSIRTの役割とその業務内容

機能分類	役割名称	業務内容
情報共有	社外PoC：自組織外連絡担当	NCA、 JPCERT/CC、CSIRT、警察、監督官庁、等々との情報連携
	社内PoC：自組織内連絡担当、IT部門調整担当	法務、渉外、IT部門、広報、各事業部、等々との情報連携
	リーガルアドバイザー：法務部CSIRT担当	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担当：自組織内調整・情報発信担当	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：情報収集担当、キュレーター：情報分析担当	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
	脆弱性診断士：脆弱性の診断担当	NW、OS、セキュアプログラミングの検査、診断
	脆弱性診断士：脆弱性の評価担当	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担当	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：セキュリティ戦略担当	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：CSIRT全体統括	CSIRT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
	インシデントマネージャー：インシデント管理担当	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：インシデント処理担当	インシデント現場監督。セキュリティベンダとの連携
	インベスティゲーター：調査・捜査担当	捜査に必要な論理的思考、分析力、自組織内システム理解力を使った内偵
	トリアージ担当：優先順位選定担当	事象に対する優先順位の決定。
	フォレンジック担当	証拠保全、システム的な鑑識、足跡追跡。マルウェア解析。
自組織内教育	教育担当：教育・啓発担当	自組織のリテラシー向上、底上げ。

出典：日本シーサート協議会
CSIRT人材の定義と確保 Ver.2

Copyright © 2017 ANA Systems Co.,Ltd., All rights reserved.

役割別任用前提スキルと追加教育スキル「PoC（Point of Contact）」

出典：日本シーサート協議会

自組織外・自組織内連絡担当、ＩＴ部門調整担当

社外窓口として、JPCERT/CC、NISC、警察、監督官庁、NCA、他CSIRT等との連絡窓口となり、情報連携を行う。

社内窓口として、IT部門、法務、渉外、IT部門、広報、各事業部等との連絡窓口となり、情報連携を行う。

任用前提スキル

- ✓ 情報を正しく伝えるコミュニケーション能力
- ✓ ITSSレベル２程度の基礎的なITリテラシー
- ✓ 情報を適切に判断する能力

追加教育スキル

- ✓ 情報を収集し、インテリジェンスを生成・報告できる能力
- ✓ サイバーセキュリティ問題に関する外部組織と学術機関に関する知識
- ✓ 既知の脆弱性に関する知識

出典：日本シーサート協議会
CSIRT人材の定義と確保 Ver.2

Copyright © 2017 ANA Systems Co.,Ltd., All rights reserved.

スキルマップ　2:POC（Point of Contact）　　出典：JNSA セキュリティ知識分野（SecBoK）人材スキルマップ2016年版

※「前提スキル」「

分野	大項目	中項目	小項目	前提スキル	必須スキル
基礎	ICT基礎	ネットワークインフラ	組織のLAN/WANの経路に関する知識		●
			ネットワーク通信の相異なる種類（例：LAN、WAN、MAN、無線LAN、無線WAN）に関する知識		●
		通信プロトコル・サービス	ネットワークプロトコル（例：TCP/IP、DHCP）およびディレクトリサービス（例；DNS）に関する知識		●
		オペレーティングシステム	サーバとクライアントのOSに関する知識	●	
			適用可能なシステム構成要素（Windowsおよび/またはUNIX/Linux）の識別、修正及び操作（例：パスワード、ユーザアカウント、ファイル）に関するスキル		●
			ファイル拡張子（例：dll, .bat, .zip, .pcap, .gzip）に関する知識	●	
			関連する情報を含むシステムファイル（例：ログファイル、レジストリファイル、設定ファイル）が何であり、そのシステムファイルはどこにあるかに関する知識		●
			ミドルウェアに関する知識		●
		システム運用	災害復旧及び運用継続計画に関する知識		●
		その他	計算機の基本的操作に関するスキル	●	
			ITSSレベル2程度の基礎的なITリテラシー	●	
	ビジネス基礎		組織のデータ資産のソース、特徴及び利用に関する知識		●
			リスクマネジメントフレームワークの要件に関する知識		●
			リスクを評価するための手順と手法を含む、リスクマネジメントプロセスに関する知識		●
			情報を収集しインテリジェンスを生成、報告及び共有することに関する基本的な手法、手続き及び技術に関する知識		●
			情報を効率的に伝達するための他者とのコミュニケーションに関するスキル	●	
			情報を適切に判断する能力	●	
セキュリティ基礎	総論		情報またはデータの利用、処理、蓄積及び移送に関連するリスクを管理するために用いられる情報保証の原理に関する知識		●
			サイバーセキュリティ問題に関する外部組織と学術機関に関する知識		●
			出現するセキュリティ問題、リスク及び脆弱性に関する知識		●
セキュリティガバナンス	総論		組織のリスク受容および/またはリスク管理のアプローチに関する知識		●
セキュリティマネジメント	総論		セキュリティマネジメントに関する知識		●
			組織上の情報技術ユーザのセキュリティポリシー（例：アカウント作成、パスワードルール、アクセス制御）に関する知識	●	

Copyright © 2017 ANA Systems Co.,Ltd., All rights reserved.

スキルマップ　4:コマンダー、トリアージ

※「前提スキル」「必

分野	大項目	中項目	小項目	前提スキル	必須スキル
セキュリティ運用	総論		運用上のセキュリティに関する知識		●
			新興の情報技術と情報セキュリティ技術に関する知識	●	
			システム診断ツールと障害識別技法に関する知識	●	
			主要ベンダの製品と用語（例：セキュリティスイート：トレンドマイクロ、シマンテック、マカフィー、アウトポスト、パンダ、カスペルスキー）及びエクスプロイト／脆弱性にどのように作用するかの相違点に関する知識	●	
			サイバー運用と活動の衝突回避に関するスキル	●	
			リスク脅威の評価に関する知識		●
	インシデント対応		インシデントのカテゴリ、インシデントレスポンス及び応答のタイムラインに関する知識		●
			インシデントレスポンスとハンドリングの方法論に関する知識		●
			インシデントハンドリング手法の利用に関するスキル		●
			インシデントの根本原因分析に関する知識		●
			インシデントに関連したネットワークセキュリティの報告のためのプロセスに関する知識	●	
			企業のインシデントレスポンスプログラム、役割及び責任に関する知識		●
			インシデントの根本原因分析の実施に関するスキル		●
			報告されたインシデントの文書化と問い合わせに用いられるデータベース手続きに関する知識	●	
	その他		内部不正の検出、報告、検出ツール及び法規制に関する知識と経験	●	
暗号・認証・電子署名	総論		アクセス時の認証手法に関する知識	●	
サイバー攻撃手法	総論		現在及び新興の脅威/脅威ベクトルに関する知識		●
			攻撃者に悪用される可能性のある新興のコンピュータベースの技術に関する知識	●	
			一般的な攻撃ステージ（例：フットプリンティング及びスキャン、列挙、アクセス権取得、特権の昇格、アクセス権の保持、ネットワークのエクスプロイト、追跡回避）に関する知識		●
			責任を割り当てられた範囲内での一般的な攻撃者の戦術、技術及び手順（例：歴史的な国別の戦術、技術及び手順、新興の能力）に関する知識		●
			脆弱性の種類と関連する攻撃の認知とカテゴライズに関するスキル	●	
	マルウェア		マルウェアの取扱いに関するスキル	●	
			マルウェアからのネットワークの保護に関するスキル	●	
	その他		模倣型脅威の振る舞いに関するスキル	●	
			ソーシャルエンジニアリング技術の利用に関するスキル	●	
			運用上の脅威環境の違い（例：第一世代（スクリプトキディ）、第二世代（非政府機関による支援）、第三世代（政府機関による支援）に関する知識	●	

Copyright © 2017 ANA Systems Co.,Ltd., All rights reserved.

スキルマップ　9:脆弱性診断士

詳細は
http://www.jnsa.org/result/2016/skillmap/index.html
をご確認ください。

※「前提スキル」「

分野	大項目	中項目	小項目	前提スキル	必須スキル
システムセキュリティ	総論		アプリケーションの脆弱性に関する知識	●	
			システムとアプリケーションのセキュリティ上の脅威と脆弱性に関する知識	●	
			システムとアプリケーションのセキュリティ上の脅威と脆弱性（例： バッファオーバフロー、モバイルコード、クロスサイトスクリプティング、PL/SQL及びインジェクション、競合状態、秘密の通信路、リプレイ、リターン指向攻撃、悪意のコード）に関する知識	●	
			ウェブメールの収集、検索／分析技術、ツール及びクッキーに関する知識	●	
セキュアシステム設計・構築	総論		セキュリティシステムと設計の頑健性の評価に関するスキル	●	
			セキュリティシステムがどのように動作すべきか（レジリエンスとディペンダビリティ性能を含む）、及び条件、運用または環境の変化がそれらのアウトカムにどのように影響するかの決定に関するスキル		●
			安全、パフォーマンスおよび信頼性の観点から局所固有となるシステムの要件（例： 標準的なITを使えない重要インフラシステム）に関する知識		●
	セキュアプログラミング		セキュアコーディング技術に関する知識		●
セキュリティ運用	総論		運用上のセキュリティに関する知識	●	
			新興の情報技術と情報セキュリティ技術に関する知識		●
			システム診断ツールと障害識別技法に関する知識		●
			主要ベンダの製品と用語（例： セキュリティスイート：トレンドマイクロ、シマンテック、マカフィー、アウトポスト、パンダ、カスペルスキー）及びエクスプロイト／脆弱性にどのように作用するかの相違点に関する知識		●
暗号・認証・電子署名	総論		暗号化アルゴリズム（例：IPSEC、AES、GRE、IKE、MD5、SHA、3DES）に関する知識	●	
			暗号に関する知識	●	
			暗号化手法に関する知識	●	
			アクセス時の認証手法に関する知識	●	
			一方向性ハッシュ関数（例： SHA、MD5）に関するスキル	●	
サイバー攻撃手法	総論		一般的な攻撃ステージ（例： フットプリンティング及びスキャン、列挙、アクセス権取得、特権の昇格、アクセス権の保持、ネットワークのエクスプロイト、追跡回避）に関する知識	●	
			脆弱性の種類と関連する攻撃の認知とカテゴライズに関するスキル	●	
	その他		模倣型脅威の振る舞いに関するスキル		●
			ソーシャルエンジニアリング技術の利用に関するスキル		●
			WindowsまたはUnix/Linux環境におけるハッキング手法に関する知識	●	
			攻撃クラスの相違（例： 受動的、能動的、内部、近接、分散）に関する知識	●	
			運用上の脅威環境の違い（例： 第一世代（スクリプトキディ）、第二世代（非政府機関による支援）、第三世代（政府機関による支援）に関する知識		●

Copyright © 2017 ANA Systems Co.,Ltd., All rights reserved.

出典：日本シーサート協議会

「リーガルアドバイザー」

法務担当

情報技術やサイバーセキュリティなどにおける法課題やコンプライアンス問題が発生した時に法的アドバイスを行う。法務部がITスキルに乏しい場合にはIT担当が法務部向けに翻訳して橋渡しする形でもよい。

任用前提スキル

- ✓ セキュリティに関わる関連法の知識、もしくはITSSレベル２程度の基礎的なITリテラシー
- ✓ サイバーセキュリティに関連する技術的動向、法的なトレンドの追跡、解析ができる能力。
- ✓ 情報を正しく伝えるコミュニケーション能力

追加教育スキル

- ✓ セキュリティに関わる関連法、ITリテラシーのさらに深い知識
- ✓ インシデントレスポンスとハンドリングの知識
- ✓ 調達、サプライチェーン、業務委託をセキュアに行うための知識

Copyright © 2017 ANA Systems Co.,Ltd., All rights reserved.

出典：日本シーサート協議会

「ノーティフィケーション担当」

自組織内調整・情報発信担当
自組織内を調整し、各関連部署への情報発信を行う。
自組織システムに影響を及ぼす場合にはIT部門と調整を行う。

任用前提スキル

- ✓ 情報を正しく伝えるコミュニケーション能力
- ✓ ITSSレベル２程度の基礎的なITリテラシー
- ✓ 情報を適切に判断し、説明する能力
- ✓ 自組織システムに関する知識
- ✓ 折衝能力

追加教育スキル

- ✓ ITセキュリティ、セキュリティマネジメントの基礎
- ✓ インシデントレスポンスとハンドリングの知識
- ✓ 自組織セキュリティガイドライン、遵守事項の知識
- ✓ 既知の脆弱性に関する知識
- ✓ 事象に対するリスク把握と優先順位を説明出来る能力

Copyright © 2017 ANA Systems Co.,Ltd., All rights reserved.

出典：日本シーサート協議会

「リサーチャー」

情報収集担当

セキュリティイベント、脅威情報、脆弱性情報、攻撃者のプロファイル情報、国際情勢の把握、メディア情報などを収集し、キュレーターに引き渡す。単独機器の分析は行うが、相関的な分析はしない。

任用前提スキル

- ✓ 基礎的なセキュリティに関する知識
- ✓ 情報を鵜呑みにしないメディアリテラシー
- ✓ 英語を正しく読む能力

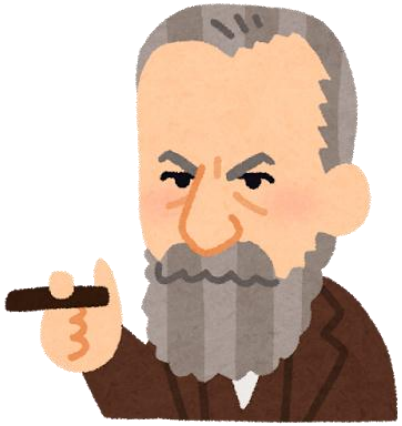
追加教育スキル

- ✓ 国家間の関係、ハクティビストに関する知識
- ✓ メディアの特性を知り、活用できる能力
- ✓ セキュリティ機器で検出される情報を正しく読む能力
- ✓ 攻撃戦術、ステージ、技術、手順に関する知識

Copyright © 2017 ANA Systems Co.,Ltd., All rights reserved.

出典：日本シーサート協議会

「キュレーター」



情報分析担当
リサーチャーの収集した情報を分析し、その情報を自組織に適用すべきかの選定を行う。リサーチャーと合わせてSOC（セキュリティオペレーションセンター）で実施することが多い。

任用前提スキル

- ✓ 自組織のセキュリティアーキテクチャ、ビジネスに関する知識
- ✓ 情報を鵜呑みにしないメディアリテラシー
- ✓ 英語を正しく読む能力

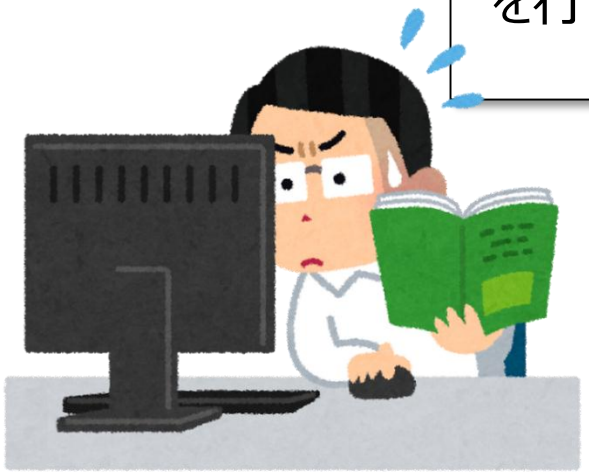
追加教育スキル

- ✓ 情報を収集し、インテリジェンスを活用できる能力
- ✓ 国家間の関係、ハクティビストに関する分析能力
- ✓ メディアの特性を知り、活用できる能力
- ✓ セキュリティ機器で検出される情報を相関分析できる能力
- ✓ 攻撃戦術、ステージ、技術、手順に関する知識
- ✓ 自組織のセキュリティ対策に適用すべきか判断できる能力

Copyright © 2017 ANA Systems Co.,Ltd., All rights reserved.

出典：日本シーサート協議会

「脆弱性診断士」



脆弱性の診断、評価担当
NW、OS、ミドルウェア、アプリケーションが安全かどうかの検査を行い、診断結果の評価を行う。

任用前提スキル

- ✓ OS、NW、アプリ、DBの脆弱性に対する知識
- ✓ パケットレベルの解析ができる能力
- ✓ ペネトレーションテストやツールに関する知識
- ✓ 一般的な攻撃手法に関する知識

追加教育スキル

- ✓ 自組織のセキュリティアーキテクチャに関する知識
- ✓ 新興の情報セキュリティ技術に関する知識
- ✓ 脅威情報に関する知識
- ✓ コンピュータ、ネットワーク防衛と脆弱性の評価ツールを活用できる能力

Copyright © 2017 ANA Systems Co.,Ltd., All rights reserved.

出典：日本シーサート協議会

「セルフアセスメント担当」

セルフアセスメント担当
自組織環境や情報資産の現状分析を行う。平常時の際にアセスメントを実施しておき、インシデント発生時にはアセスメント結果に基づいて影響範囲を特定する。

任用前提スキル

- ✓ ITSSレベル２程度の基礎的なITリテラシー
- ✓ リスクアセスメントのためのヒアリング能力、文書化能力

追加教育スキル

- ✓ 個人情報保護法、PCIDSS、ISMSの公的規約の知識
- ✓ 自組織セキュリティポリシーやシステム構築に関するガイドライン、遵守事項の知識
- ✓ リスクマネジメントプロセスに関する知識
- ✓ インテリジェンスや最新の技術を読み取る能力

Copyright © 2017 ANA Systems Co.,Ltd., All rights reserved.

出典：日本シーサート協議会

「ソリューションアナリスト」

セキュリティ戦略担当

自組織の事業計画に合わせてセキュリティ戦略を策定する。現在の状況とあるべき姿のFit&Gapからリスク評価を行い、ソリューションマップを作成して導入を推進する。導入されたソリューションの有効性を確認し、経営層と情報共有を行い、改善計画に反映する。

任用前提スキル

- ✓ 自組織ビジネスビジョンに合わせて計画化する能力
- ✓ 自組織セキュリティガイドライン、遵守事項の知識
- ✓ リスクマネジメントプロセスを活用できる能力
- ✓ 自組織システムに関する知識

追加教育スキル

- ✓ 個人情報保護法、PCIDSS等の公的規約の知識
- ✓ インテリジェンスや最新の技術を読み取る能力
- ✓ セキュリティ要求事項と製品・運用を組合わせる能力

Copyright © 2017 ANA Systems Co.,Ltd., All rights reserved.

出典：日本シーサート協議会

「コマンダー」

CSIRT全体統括

自組織で起きているセキュリティインシデントの全体統制を行う。重大なインシデントに関してはCISOや経営層との情報連携を行う。また、CISOや経営者が意思決定する際の支援を行う。

任用前提スキル

- ✓ システム障害の全体統制を行える能力
- ✓ 自組織のセキュリティアーキテクチャ、ビジネスに関する知識
- ✓ 自組織のシステム停止、復旧時の業務影響に関する知識
- ✓ 経営層に説明できるコミュニケーションスキル

追加教育スキル

- ✓ リスク影響とビジネス継続を考慮して優先順位を決定できる能力
- ✓ 攻撃戦術、ステージ、技術、手順に関する知識
- ✓ セキュリティに特化したインシデント統制能力

Copyright © 2017 ANA Systems Co.,Ltd., All rights reserved.

出典：日本シーサート協議会

「インシデントマネージャー」

インシデント管理担当
インシデントハンドラーに指示を出し、インシデントの対応状況を把握する。対応履歴を管理するとともにコマンダーへ状況を報告する。

任用前提スキル

- ✓ システム運用知識
- ✓ インシデントに関する管理や報告ができる能力
- ✓ 自組織のセキュリティアーキテクチャの知識
- ✓ 自組織業務システムの知識

追加教育スキル

- ✓ セキュリティインシデント対応能力
- ✓ セキュリティインシデント後の復旧に関する知識
- ✓ 出現するセキュリティ問題、リスク、脆弱性の知識
- ✓ 脆弱性診断に関する知識
- ✓ マルウェア等各種攻撃に対する取り扱いの知識

Copyright © 2017 ANA Systems Co.,Ltd., All rights reserved.

出典：日本シーサート協議会

「インシデントハンドラー」

インシデント処理担当
インシデントの処理を行う。セキュリティベンダに処理を委託している場合には指示を出して連携し、管理を行う。状況はインシデントマネージャに報告する。

任用前提スキル

- ✓ システム運用知識
- ✓ インシデントに関する管理や報告ができる能力
- ✓ 自組織のセキュリティアーキテクチャの知識
- ✓ 自組織業務システムの運用経験

追加教育スキル

- ✓ セキュリティインシデント対応能力
- ✓ セキュリティインシデント後の復旧を行う能力
- ✓ 出現するセキュリティ問題、リスク、脆弱性の知識
- ✓ 脆弱性診断結果に対応する能力
- ✓ マルウェア等各種攻撃に対する対応能力

Copyright © 2017 ANA Systems Co.,Ltd., All rights reserved.

出典：日本シーサート協議会

「インベスティゲーター」

調査・捜査担当

外部からの犯罪、内部犯罪を捜査する。
セキュリティインシデントはシステム障害とは異なり、悪意のある者が存在する。通常の犯罪捜査と同様に、動機の確認や証拠の確保、次に起こる事象の推測などを詰めながら論理的に捜査対象を絞っていくことが要求される。

任用前提スキル

- ✓ 情報を収集し、インテリジェンスを活用できる能力
- ✓ 国家間の関係、ハクティビストに関する分析能力
- ✓ 証拠の押収・保存の知識
- ✓ ITSSレベル2程度の基礎的なITリテラシー
- ✓ 自組織システムに関する知識

追加教育スキル

- ✓ 犯人特定のための捜査能力
- ✓ 尋問に関するコミュニケーション能力と知識
- ✓ 攻撃者の戦術・技術・手順に関する知識
- ✓ サイバー犯罪に関する法律的知識

Copyright © 2017 ANA Systems Co.,Ltd., All rights reserved.

出典：日本シーサート協議会

「トリアージ担当」

優先順位選定担当
発生している事象に対して優先順位を決定する。被害がある場合の復旧優先順位や、拡散している場合にはどのシステムから停止していくべきか等の判断を行う。

任用前提スキル
- ✓ 自組織のセキュリティアーキテクチャ、ビジネスに関する知識
- ✓ 自組織のシステム停止、復旧時の業務影響に関する知識

追加教育スキル
- ✓ リスク影響とビジネス継続を考慮して優先順位を決定できる能力

Copyright © 2017 ANA Systems Co.,Ltd., All rights reserved.

出典：日本シーサート協議会

「フォレンジック担当」

フォレンジック担当
システム的な鑑識、精密検査、解析、報告を行う。
悪意のある者は証拠隠滅を図ることもあるため、証拠保全とともに、消されたデータを復活させ、足跡を追跡することも要求される。

任用前提スキル

- ✓ OS、コマンド、システムファイル、プログラミング言語の構造とロジックに関する知識
- ✓ 脆弱性診断に関する知識

追加教育スキル

- ✓ デジタルフォレンジックに関する知識
- ✓ メモリダンプ解析能力
- ✓ マルウェア解析能力
- ✓ リバースエンジニアリングの能力
- ✓ バイナリ解析ツールを利用できる能力
- ✓ セキュリティイベントの相関分析を行える能力

Copyright © 2017 ANA Systems Co.,Ltd., All rights reserved.

出典：日本シーサート協議会

「教育担当」

教育・啓発担当
主に役職員向けの教育を実施し、リテラシーの向上を図る。
CSIRT向けの専門トレーニングについては別担当にしてもよい。

任用前提スキル
- ✓ 情報を正しく伝えるコミュニケーション能力
- ✓ ITSSレベル３程度のITリテラシー
- ✓ 情報をわかりやすく伝えるコミュニケーション能力

追加教育スキル
- ✓ 自組織セキュリティポリシーやシステム構築に関するガイドライン、遵守事項の知識
- ✓ 情報を収集し、インテリジェンスを生成・報告できる能力
- ✓ 既知の脆弱性に関する知識

Copyright © 2017 ANA Systems Co.,Ltd., All rights reserved.

出典：日本シーサート協議会

CSIRTの役割と業務内容の関連図(平常時)

実線は活動時の情報の流れ。
点線は必要時に実施する活動の流れ。

経営者、外部組織

情報の入手、説明、連絡

PoC
自組織内、自組織外への説明、連絡

自組織内システム、関連システム

該当システムでの対応調整

オペレーション担当
自組織内関連部署との調整

情報伝達

情報集約
（システム対応可否、対応時間等）

コマンダー
CSIRT全体統括者

設計に反映

ソリューションアナリスト
システムセキュリティ設計、有効性確認

情報集約
（脅威リスク判定等）

必要時に
教育に反映

情報集約
（影響範囲の報告）

計画策定、推進

インシデントマネージャー
インシデントの状況分析

教育担当

セルフアセスメント担当
リスクアセスメント、脆弱性対応

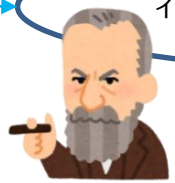
状況確認

状況確認

定期的に実施

インシデントハンドラー
インシデントの現場監督・ベンダとの連携

連携



リサーチャー、キュレーター
インシデントの情報収集、運用しているセキュリティセンサ異常値の発見、影響分析

脆弱性診断士

＊法的確認や日常的にアドバイスが必要な場合には
各役割からリーガルアドバイザーに支援を要請する。

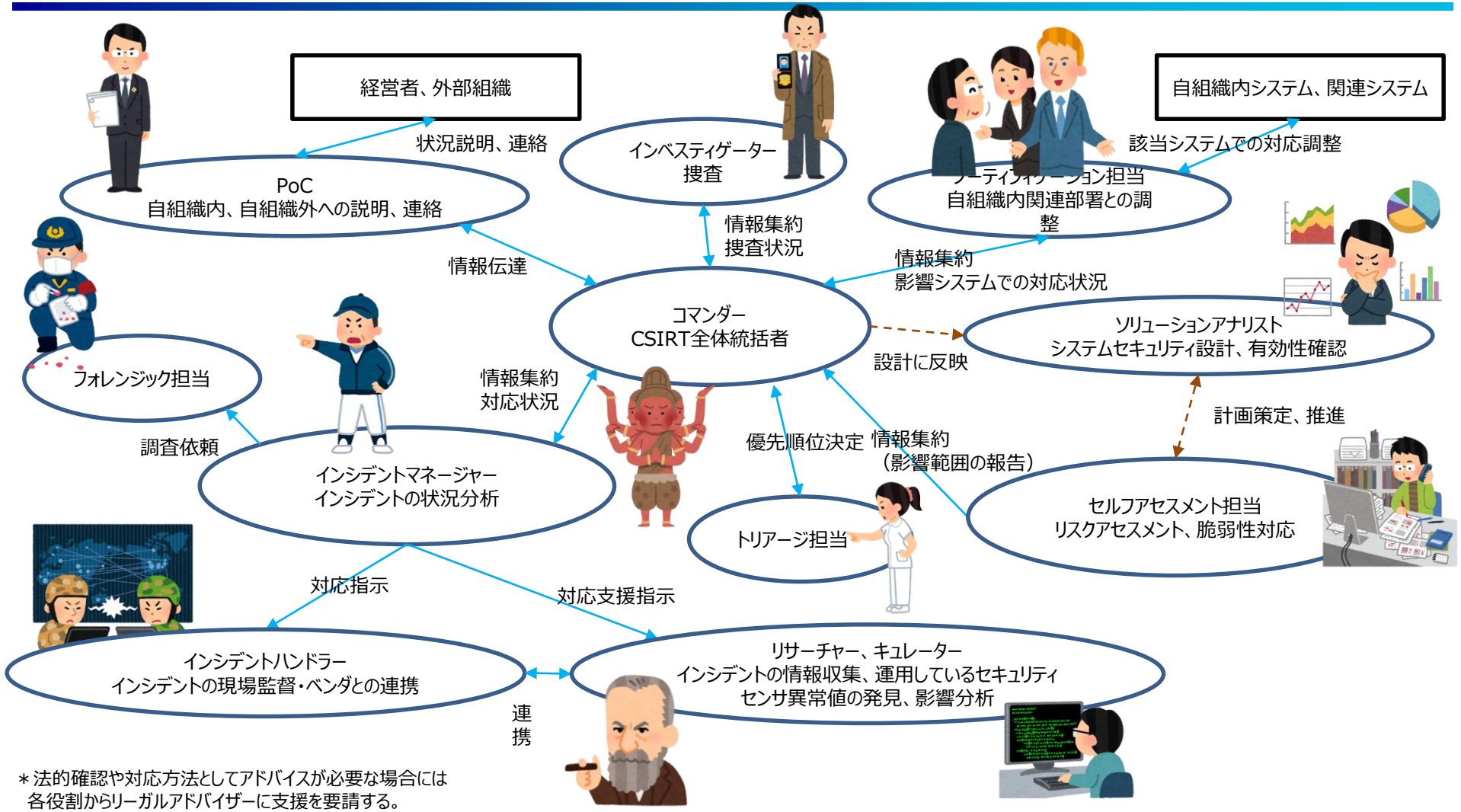
出典：日本シーサート協議会
CSIRT人材の定義と確保

Copyright © 2017 ANA Systems Co.,Ltd., All rights reserved.

出典：日本シーサート協議会

CSIRTの役割と業務内容の関連図(インシデント対応時)

実線は活動時の情報の流れ。
点線は必要時に実施する活動の流れ。



＊法的確認や対応方法としてアドバイスが必要な場合には
各役割からリーガルアドバイザーに支援を要請する。

出典：日本シーサート協議会
CSIRT人材の定義と確保

Copyright © 2017 ANA Systems Co.,Ltd., All rights reserved.

ご清聴、ありがとうございました。

ＡＮＡグループ情報セキュリティセンター
anag_infosec@ana.co.jp

Copyright © 2017 ANA Systems Co.,Ltd., All rights reserved.