巧妙化するサイバー攻撃に向けて
～CSIRT運用で陥りがちな点とANAグループのセキュリティ対応～

2019年８月7日
ANAシステムズ株式会社

品質・セキュリティ管理部
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システムズ株式会社
品質・セキュリティ管理部
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

Certified SIM3 Auditor
阿部恭一

＜外部団体メンバー＞
日本シーサート協議会：シーサート人材ＷＧ、机上訓練ＳＷＧ、トレーニングＳＷＧ
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
国際化サイバーセキュリティ学　Ｃｙｓｅｃ講師
産業サイバーセキュリティセンター　中核人材育成プログラム講師
経済産業省　セキュリティサービス審査登録制度に関する有識者検討会　委員
交通ISAC　セキュリティマネージメント共有ＷＧ　主査

＜外部講演2018年度～＞
アシスト　セキュリティ・プレミアム・ラウンドテーブル
大阪府立大学
情報セキュリティExpo
フォーティネット　Security World 2018
AKAMAI　セキュリティカンファレンス2018
Interop TOKYO 2018
JPCERT/CC第21回情報共有会
セプターカウンシル相互理解WG
情報処理学会連続セミナー2018
翔泳社　Secrity Online Day 2018
JUASリスクマネジメント部会
FireEye 重要インフラセミナー
関西情報センター　GDPRセミナー
越後湯沢セキュリティシンポジウム
Itmediaエンタープライズセキュリティセミナー
警視庁第22回サイバーテロ対策協議会総会
マイナビ　セキュリティシンポジウム
ＩＳＡＣ国際会議
日独セキュリティフォーラム
損保ジャパン　サイバーセキュリティセミナー
ガートナー　セキュリティ＆リスク・マネジメントサミット

ITMedia CSIRT小説「側線」

ANA グループ概要

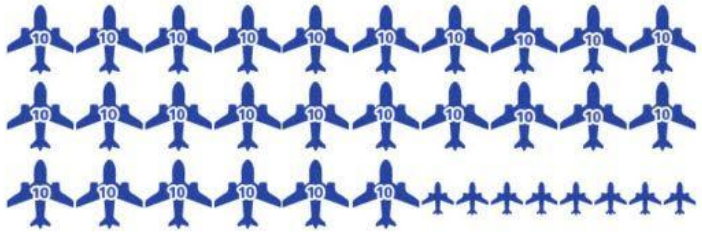
世界をつなぐ心の翼

数字で語るANAグループ

268

運用航空機数

安全性や燃費効率を含む経済性、快適性などに優れた機材を調達・運用しています。



39,243人

連結の従業員数

さまざまな事業を展開するグループ企業で、多彩な人材が一人ひとりの個性とスキルを発揮しながら活躍しています。

5,200万人

年間輸送旅客数

国内線で 4,296 万 7,000 人、国際線では 911 万 9,000 人のお客様にご搭乗いただきました。一人ひとりのお客様に寄り添い、快適な空の旅をご提供しています。

94都市

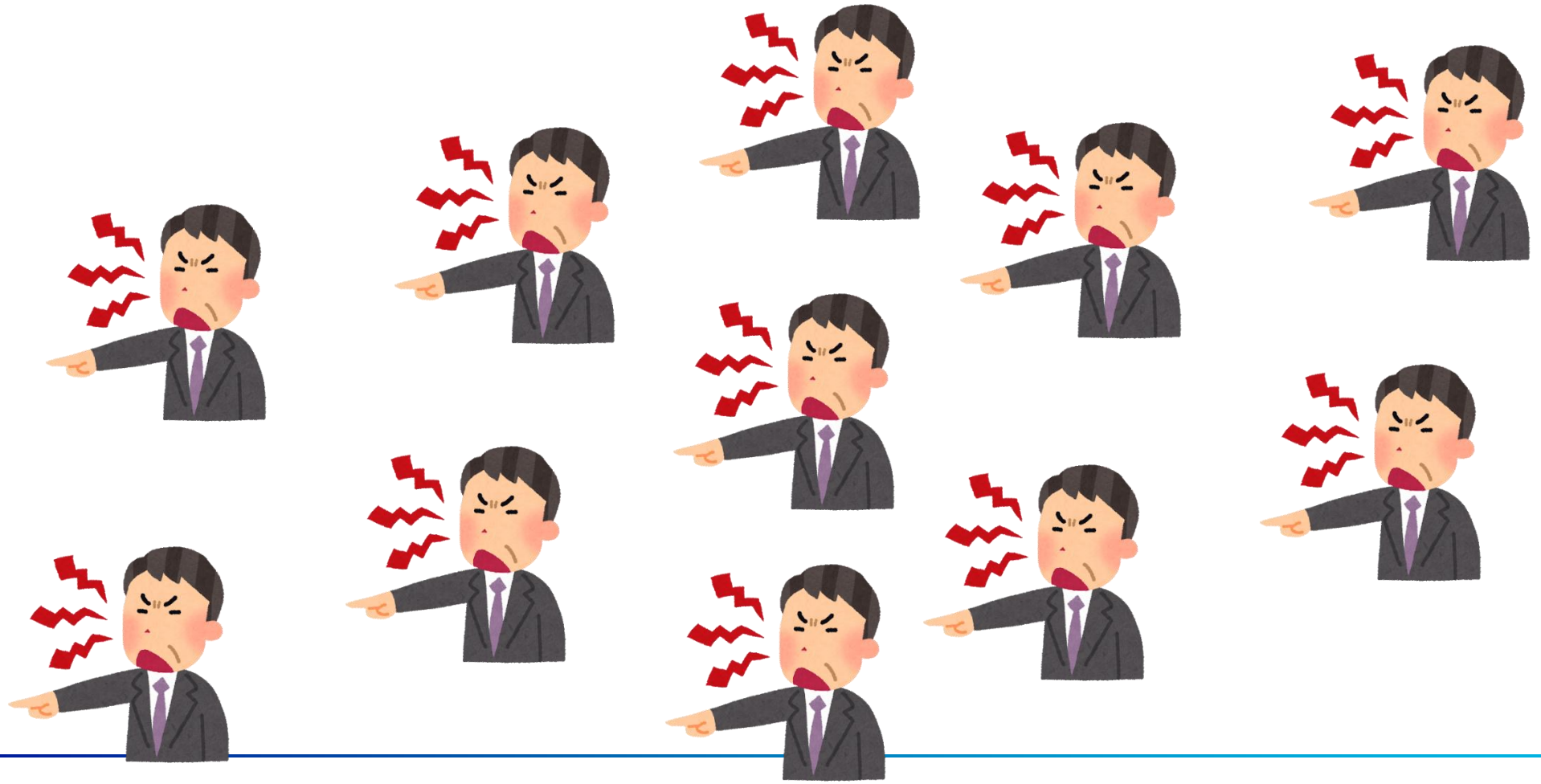
就航都市

国内線で 52 都市、国際線で 42 都市に就航。空のネットワークを充実させ続けています。

国際線の時刻表・ネットワークを見る

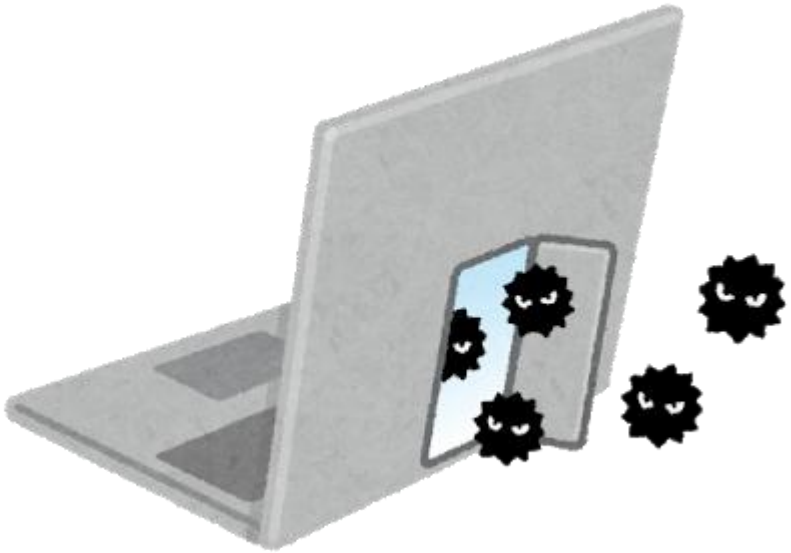
こんなＣＳＩＲＴはいやだ

指示を出す人ばかりで、誰も手を動かさない

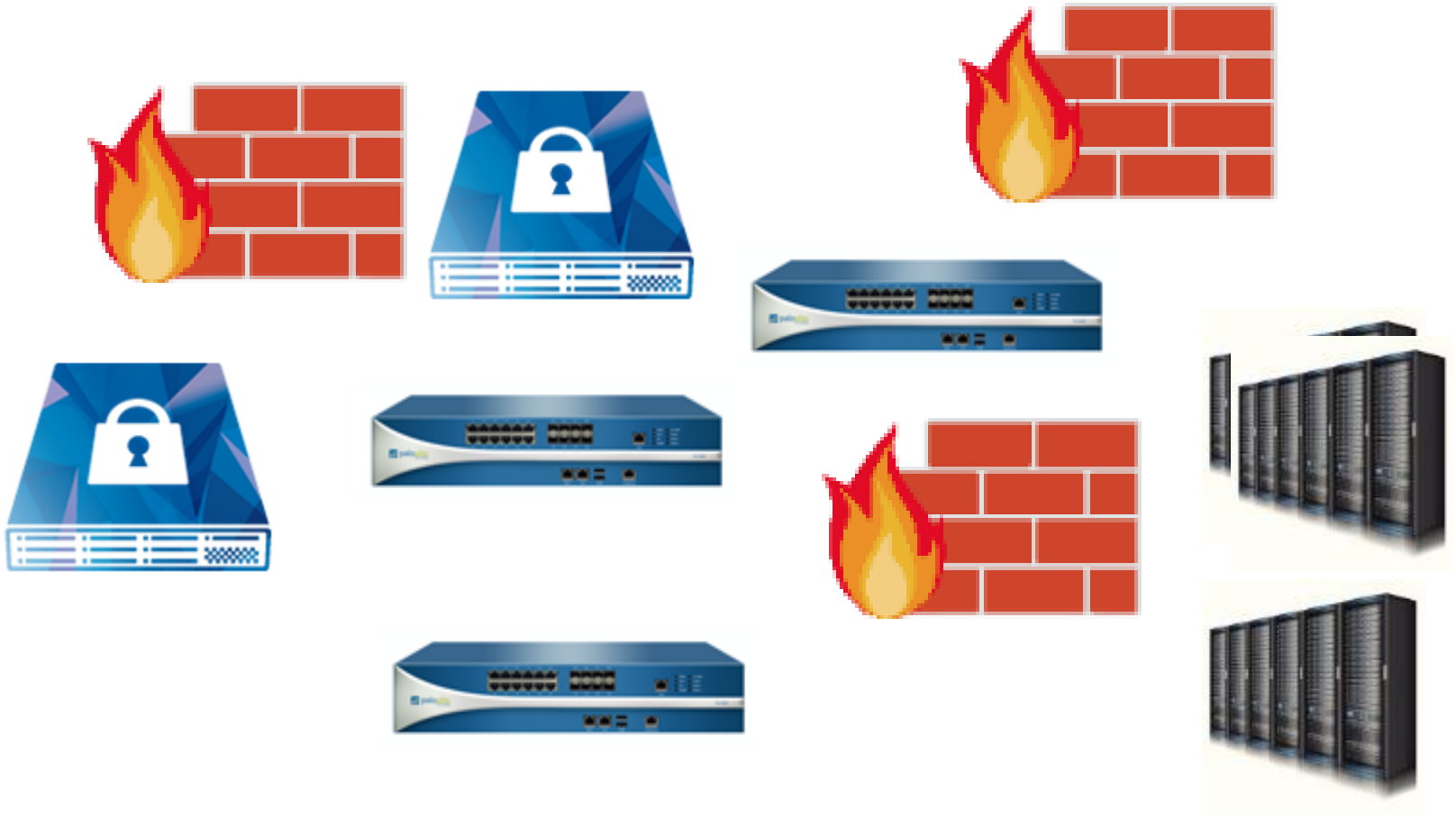


金にものを言わせて、機器を大量購入して満足してしまう。

でも初期設定のままなので、やられる。

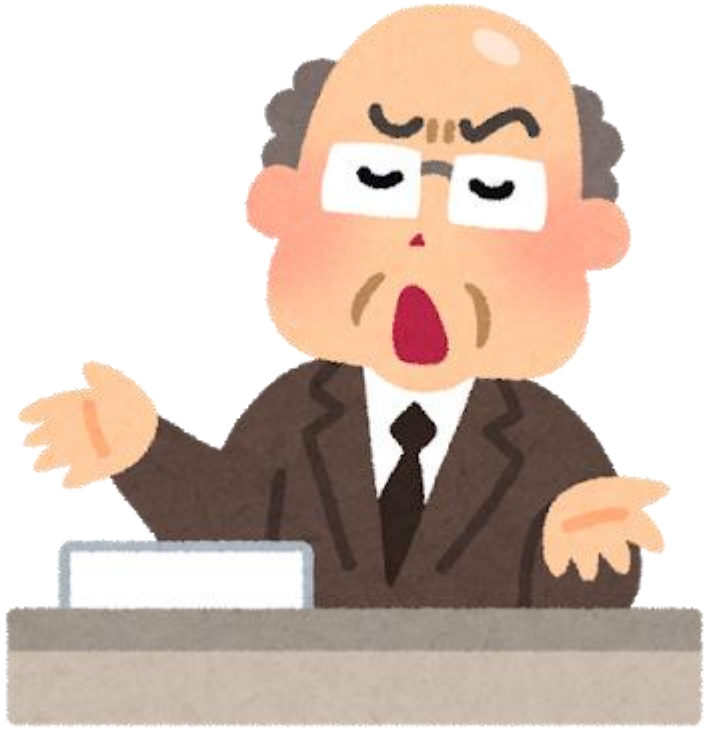


がんばっていろいろ設定してみた。



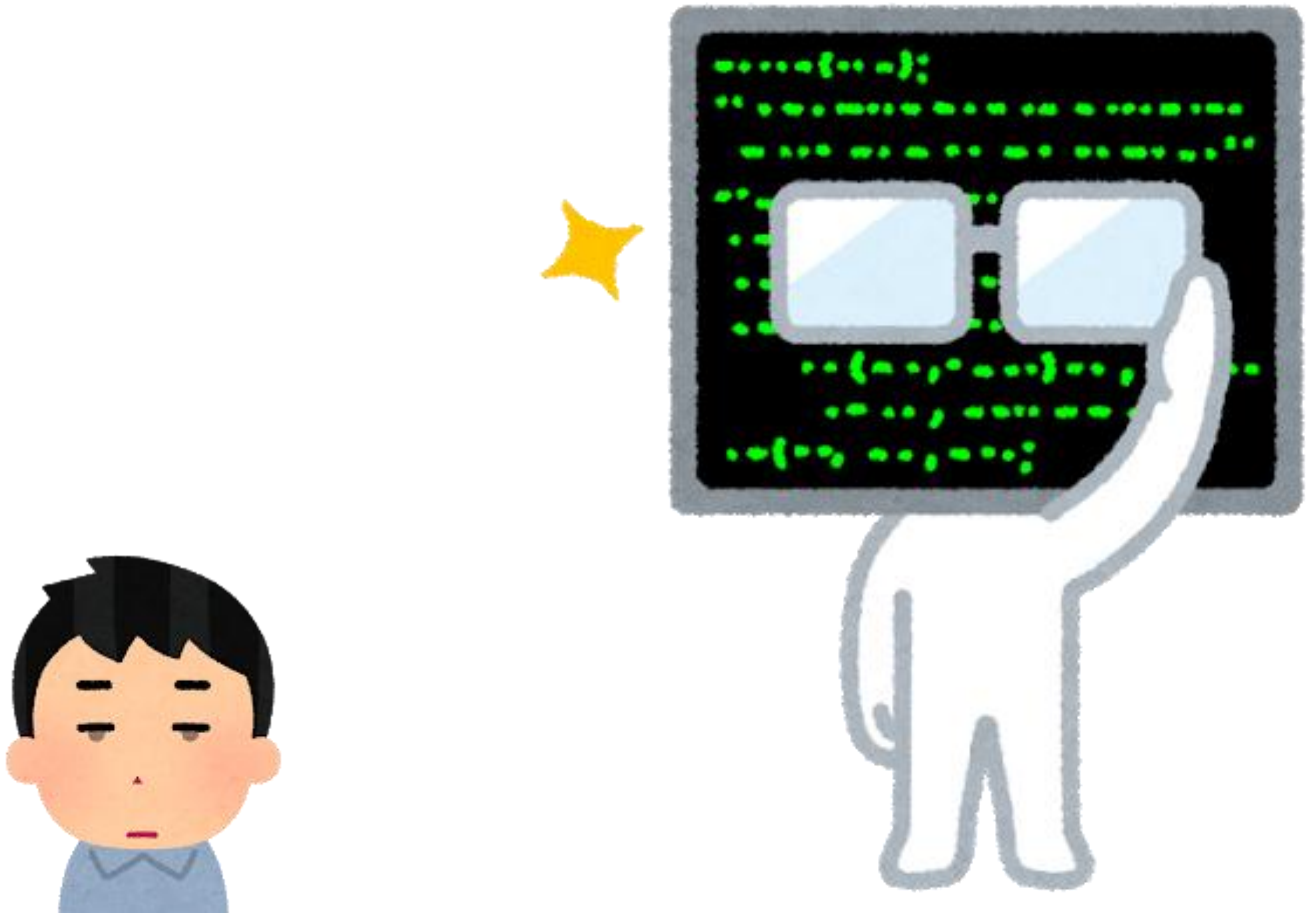
アラートが多すぎて仕事が終わらない。

コンサルのいわれるままにCSIRTを作らされる。

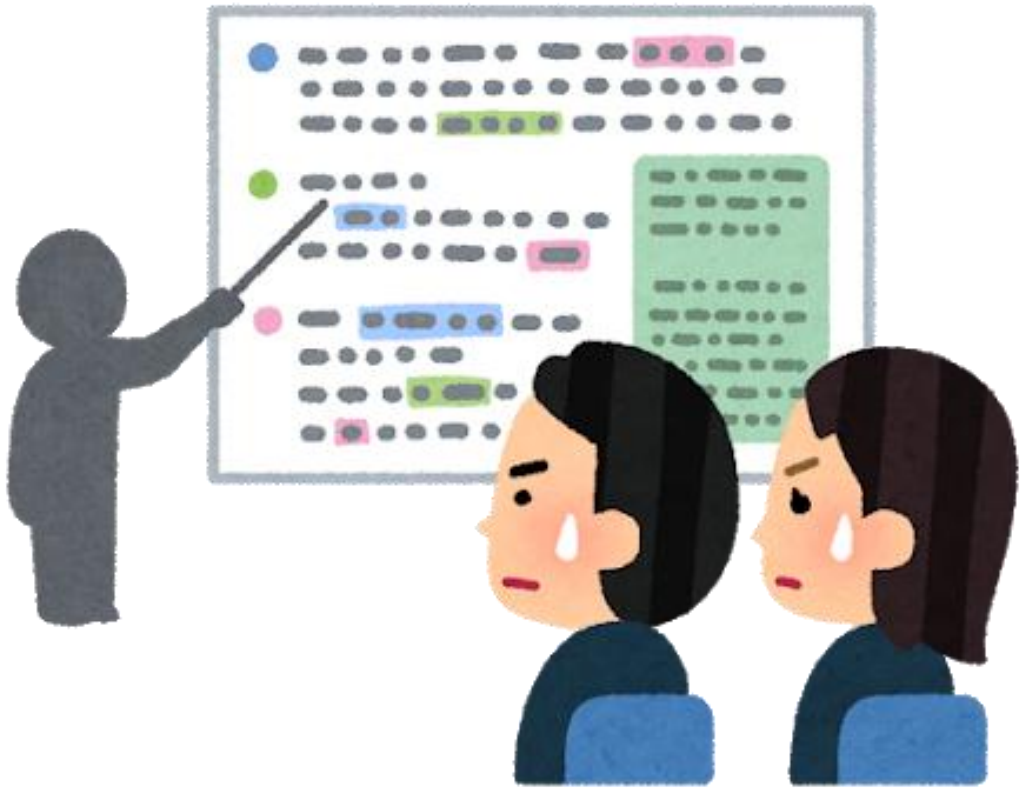


リサーチャーが妙なところをリサーチしている。

SOCと話が通じない。



報告が細かすぎて、経営者もわからない。



CSIRTは、がんばっているが、
何をやっているのか理解されない。

経営者が存在をしらない。

従業員もしらない。

CSIRT？
何ソレ？
美味しいの？

敵が多すぎる。

でも守っているのはひとりだ。

いやになってしまう。

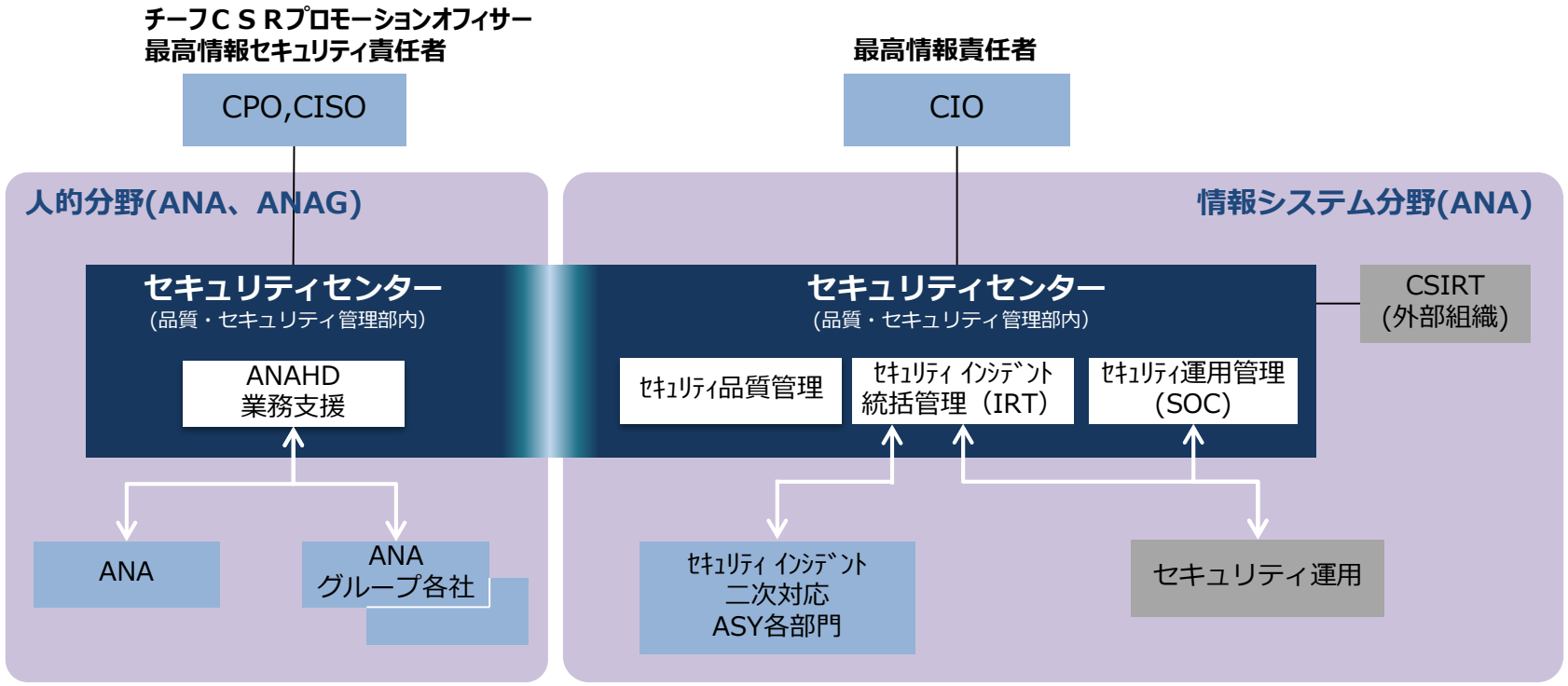
会社は金も人もださない。

応援だけはする。

やっと要員がアサインされたが人ではないような気がする。

メンバーが続々と闇落ちする。

ANAグループ情報セキュリティセンターの位置づけと全体構造



人的分野と情報システム分野の横断的な範囲をスコープとしている。

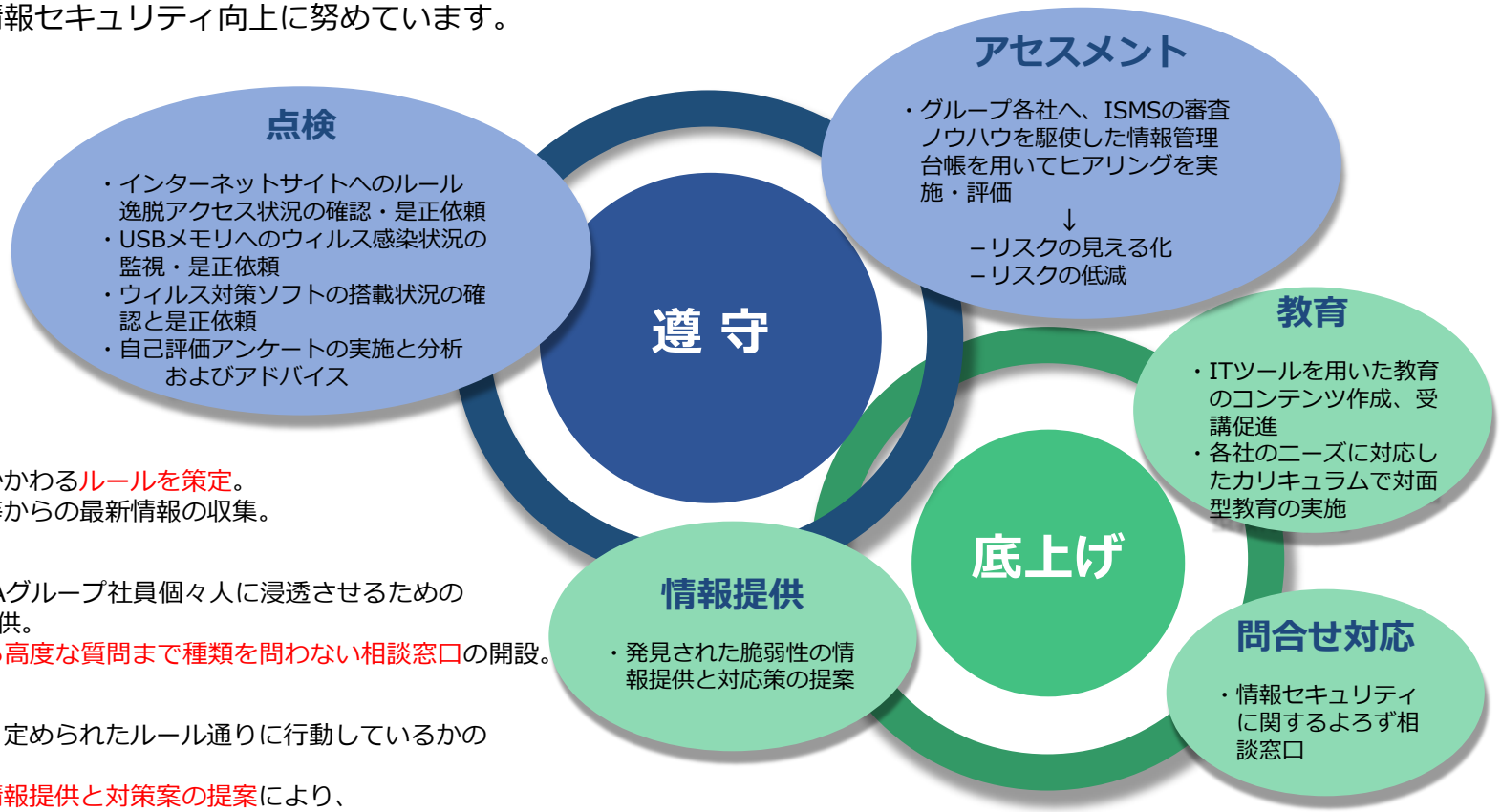
ANAグループ情報セキュリティセンター（情報システム分野）の機能概要

機能	主な実施内容	備考
SOC	インシデントの予兆分析及び未然防止策検討 −各種ログ情報からの予兆分析 −各種ログからの異常検知（閾値） −対応策実施	重大セキュリティ事故を未然に防止する目的で実施する。
IRT	手順化されたインシデント対応（＊1） −アラート受信 −アラート内容調査 −対応策実施	手順書化されたインシデント対応(*1)については、 24H365日で実施する。
	インシデント二次対応（各主管部署にて実施） −インシデント統括管理 -対応方針策定支援 −対応策実施支援	
品質管理 情報収集	システム構築に関する支援 −ガイドライン作成 −セキュリティ適合確認 最新の脅威動向に関する情報収集 −外部団体からの情報収集 −攻撃傾向及び対応策 −脆弱性情報及び対応策 −影響分析 -セキュリティリスクに対する基本方針の策定と通達	システム構築のための各種ガイドラインの作成・改訂 システム構築時にセキュリティ適合確認を行う。 JPCERTや日本シーサート協議会などを通じた情報収集を継続する。

＊1：手順書化されたセキュリティ・インシデント対応については、セキュリティ・センターにて対応を実施する。
アプリや基盤担当者にて都度判断が必要な（手順化できない）二次対応については、セキュリティ・センターは、
インシデント統括管理として各主管部署と協力しながら対応にあたる。

ANAグループ情報セキュリティセンター（人的分野）の機能概要

ANAグループ全体の情報セキュリティ向上に努めています。



＜基礎を固めます＞
■情報セキュリティにかかわるルールを策定。
■セキュリティサイト等からの最新情報の収集。

＜底上げをはかります＞
■策定したルールがANAグループ社員個々人に浸透させるための教育の実施、情報の提供。
また、素朴な疑問から高度な質問まで種類を問わない相談窓口の開設。

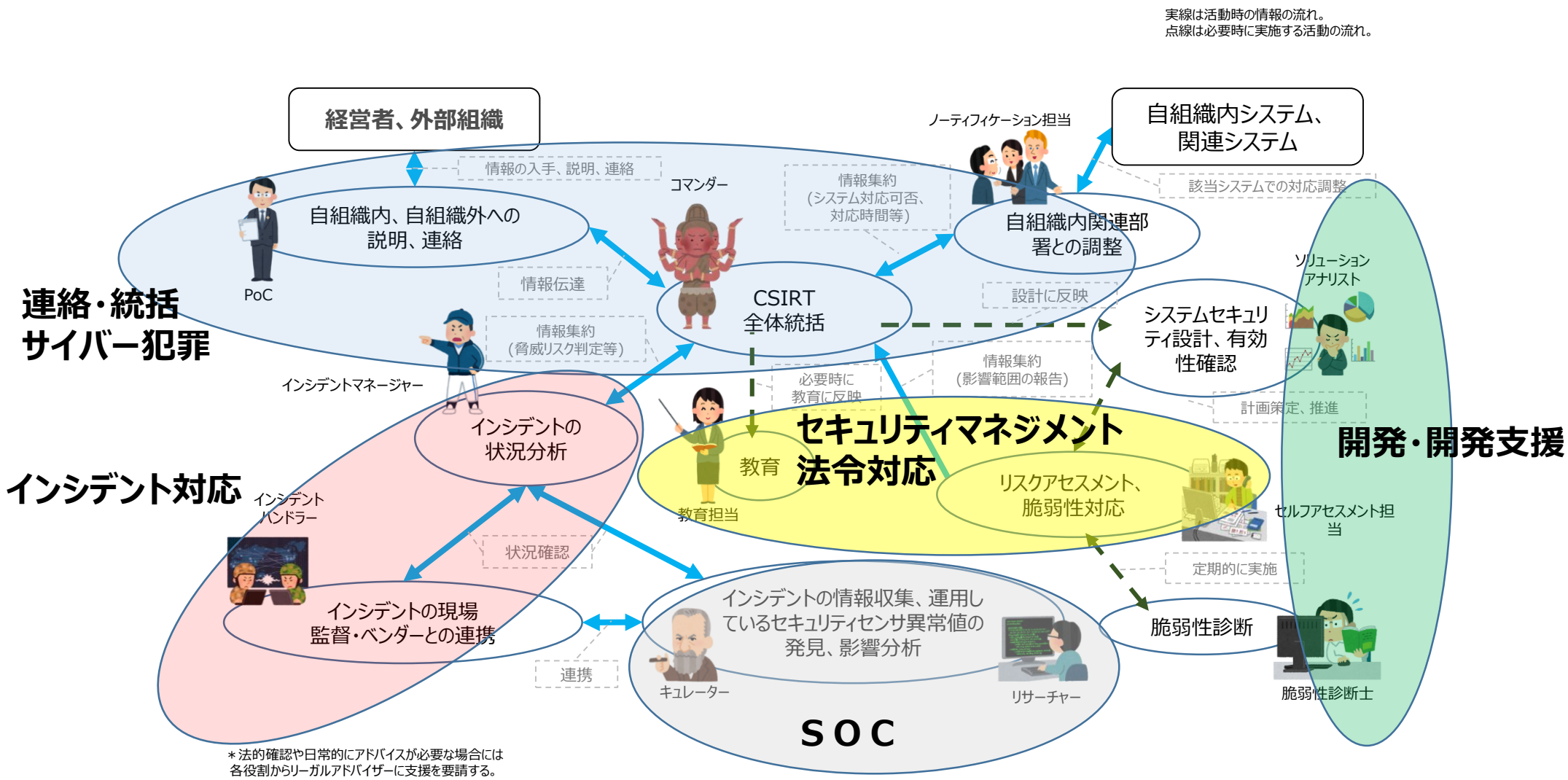
＜見回ります＞
■グループ各社に対し、定められたルール通りに行動しているかの点検及び是正。
■発見された脆弱性の情報提供と対策案の提案により、セキュリティ事故を予防。

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、FIRST、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：インシデント統制担当	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 Ver1．5

CSIRTの役割と組織の中でのグループ分け



CSIRTの訓練とインシデントレスポンスナレッジの蓄積

訓練ケース

1)脆弱性情報を入手した場合
2)ＤＯＳ、ＤＤＯＳのようなサービス妨害を受けた場合
3)不正コマンド（ＳＱＬインジェクションなど）をインターネット側から受信した場合
4)自組織内に不審な添付つきのメールが着信したとの情報を得た場合
5)自組織外から自組織を名乗ったウィルスメールが着信したとの報告を受けた場合
6)自組織の環境がランサムウェアの被害を受けたとの報告を受けた場合
7)自組織の端末から不審なサイトへの通信を観測した場合
8)自組織のＷｅｂページが改ざんされて、ウィルスが仕込まれていると報告を受けた場合

サプライチェーン：インシデントを起こさないために

- ✓ 安全なシステムの開発
  - ガイドライン、適合審査
  - チェックリスト（改正個人情報保護法、GDPRのDPIA）
  - 委託先チェックリスト、GDPRチェックリスト、サプライチェーンへの確認
- ✓ 現地アセスメント
- ✓ 脅威情報の活用、情報連携

安全なシステムの開発

ガイドライン、適合審査

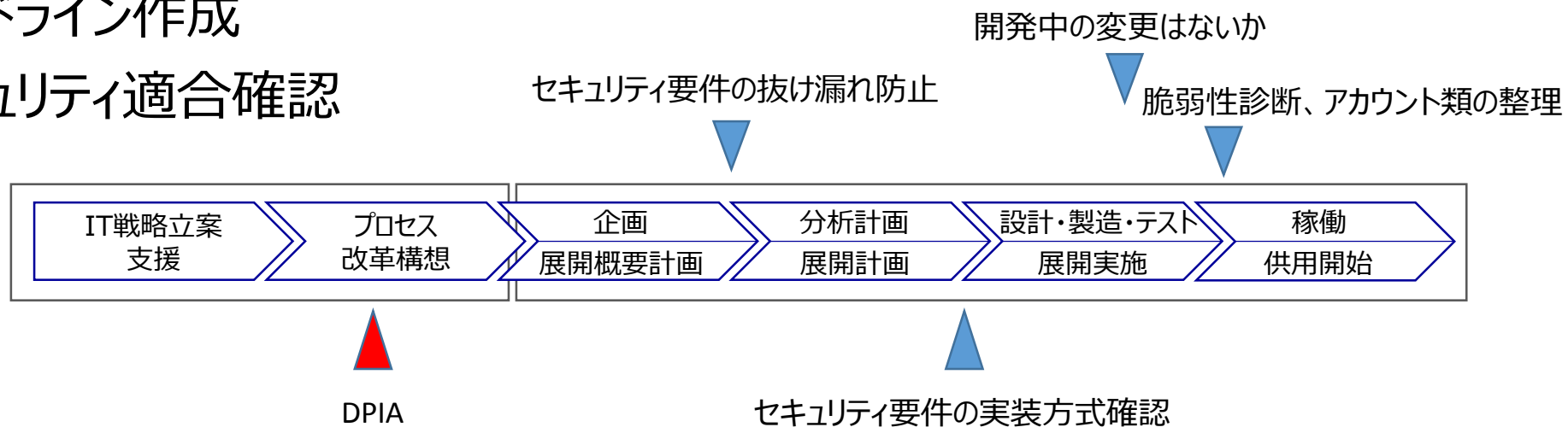
ガイドライン作成

品質管理

システム構築に関する支援

-ガイドライン作成

-セキュリティ適合確認



現地アセスメント

- 現地作業環境、ネットワーク環境の確認
- 情報資産管理台帳の確認
- 利用、作成しているシステムの適合確認
- ファシリティの確認
- セキュリティ教育
- 現地キャリアからの各国のセキュリティ事情などのヒアリング

ネットワーク統合

- ✓ グループ会社をネットワーク統合し、インターネットへの出入り口を一元管理して、SOCですべて観測できる体制をつくる。
- ✓ 最後まで残るのは端末の管理。

エンドポイント製品選択の難しさ

- ✓ 既存の数万台の端末は統制が取れていないことが多く、端末にインストールするタイプのエンドポイント製品だと、以下の状況を前提条件として導入・稼働をしなければならない。
  - ➢ 端末のOSやアプリケーションのバージョンが複数存在する。
  - ➢ 端末に搭載されているプログラムは業務アプリケーション含め、多種多様。
  - ➢ 当然、アンチウィルスソフトはすでに入っている。

  すでに稼働している業務アプリケーションは今までどおり動くのか、性能劣化はしないのか。
  その保証はどうやって行うのか、既存アプリケーション含めた確認テストを一通り行うだけで莫大なコストがかかる。

妥当性の確認

- ✓ シグニチャタイプだとロジックがわかりやすいが、ふるまい検知、AI判定など、ロジックがブラックボックス化してくると、自社の環境で運用してみないと比較できない。
  - ➢ POCもしてみるが、運よく検出できるような攻撃は来てくれない。
  - ➢ AIの場合、機械学習で最適化と聞くが、学習するためのデータは自社のデータで改善できるのか。また、もともと学習してあるデータは自社の環境にあっているのか。

初期値のまま使えば性能を発揮できないのでは？
頑張ってチューニングするとそれ自体が仕事になってしまうのでは？

EDR製品選択の難しさ

✓ 運用はどうするのか。今までもネットワーク境界SOCで同様の問題を経験しているはず。

- 高度な機能を持っていれば持っているほど、チューニングが必要。誤検知、過検知が落ち着かないと使い物にならない。
- 高度になればなるほど、高度なSOCが必要になる。なぜ、このような結果になっているのかを経営者向けにも答えられないと意味がない。
- 導入したEDRを使いこなすためにスキルが必要となれば、ただでさえ人が少ないCSIRTに余計な仕事が増えるだけ。
- だれがこの運用を行なえるのか、指示を出すだけでなく手を動かす運用者を考慮する。
- 端末数が多いため、資産管理と合わせた機能を持ち、調査スピードも重要。
- このあたりは手作業で行う話ではない。単純作業で負荷が高いと要員が闇落ちする。

エンドポイント製品やEDR製品のRFP

運用をシンプルに！

- ✓ ミニマムリクエストとして、自社では何が必要なのかを考える。（会社の既存の環境によって、CSIRTメンバのスキル、要員によって変わるはず。製品の組み合わせでも良い）
  - ➢ 運用に負荷がかからないこと。（アウトソーシング、サービス利用、RPAの提案も可）
  - ➢ 既存のアプリケーションとコンフリクトを起こさないアーキテクチャーであること。
  - ➢ 端末のプロファイルを調査、収集できること。
  - ➢ 相手が不在、海外時差も考えると、論理抜線後の操作が遠隔でできること。

高度な機能は運用者とセットで！

- ✓ 追加リクエストとして以下の内容を要求する。（製品の組み合わせでも良い）
  - ➢ 脅威を可視化し、端末間の関係性が一目瞭然であること。
  - ➢ 未知の脅威を発見し、自動的に封じ込めること。
  - ➢ 脅威や対処の説明ができること。
  - ➢ ネットワーク上のセキュリティ機器と相関分析ができること。
  - ➢ SOCにアウトソーシングしても良いが、アーキテクチャを理解してSOCと会話ができるスキル、経営者に説明できるコミュニケーション能力は企業側に必要。

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