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)

はじめに

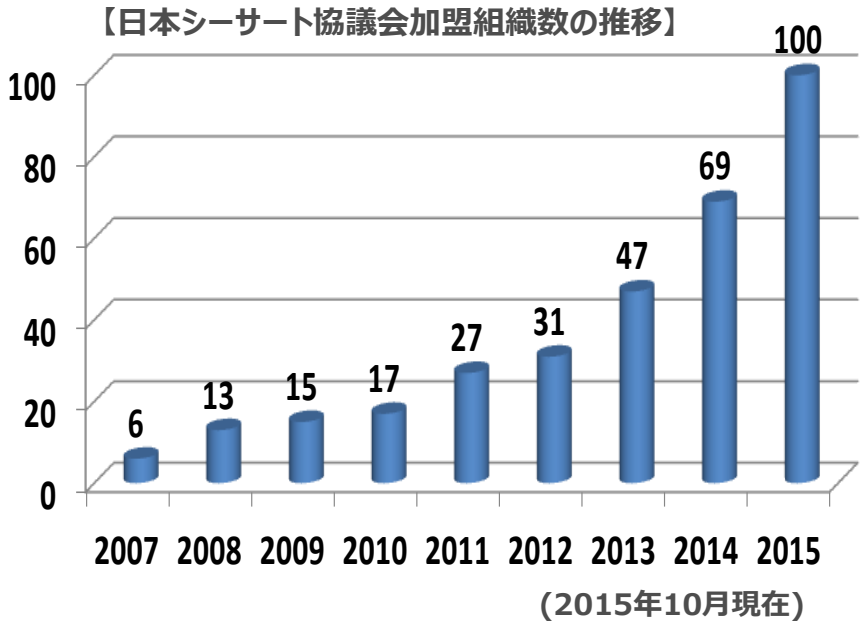
サイバー攻撃の増加や内部犯罪による被害も見受けられる現在、日本企業では、セキュリティ管理部署の設立やセキュリティ管理者を配置するなど、人材面の投資を増やす傾向がある。日本シーサート協議会への加盟組織数も右図のとおり、順調に伸びている。

しかしながら、CSIRT組織が何をすべきか、必要な人材はどのように確保するのか、確保した人材をどのように育成するかも明確化されないまま、セキュリティ人材の不足という言葉だけが叫ばれている。

本資料はその混沌とした課題をひも解き、CSIRTに求められる役割と実現に必要な人材のスキル、キャリアパスについて、対象企業を3つのパターン例に分けて解説している。

なお、CSIRT人材SWGでは継続的に議論を行い、またCSIRT活動に関わる多くの方々からのフィードバックを参考にしながら、改訂を行う予定である。

本資料が、日本に芽生えて間もないCSIRT組織の活動に少しでも役立つことになれば幸いである。



目次

本資料の取り扱いについて

- 本資料の著作権は日本シーサート協議会に帰属する
- 著作権法で正当な範囲において引用することを認める
  - 引用の範囲は必要な部分に限り、範囲を明確にすること
  - 出典を明記すること　等
- なお、引用の範囲を超えると思われる場合は、日本シーサート協議会の了解を得ること

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

本資料で対象とするCSIRTの役割と業務内容

■ 本資料で想定する組織が保有すべきCSIRTの役割とその業務内容

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。

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

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。

CSIRTのパターン

- 本資料ではCSIRTを以下のように区分し、例A～例Cに関して人材の定義と確保について記載する。

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)

※本資料において例Dは対象としていない

パターン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を想定

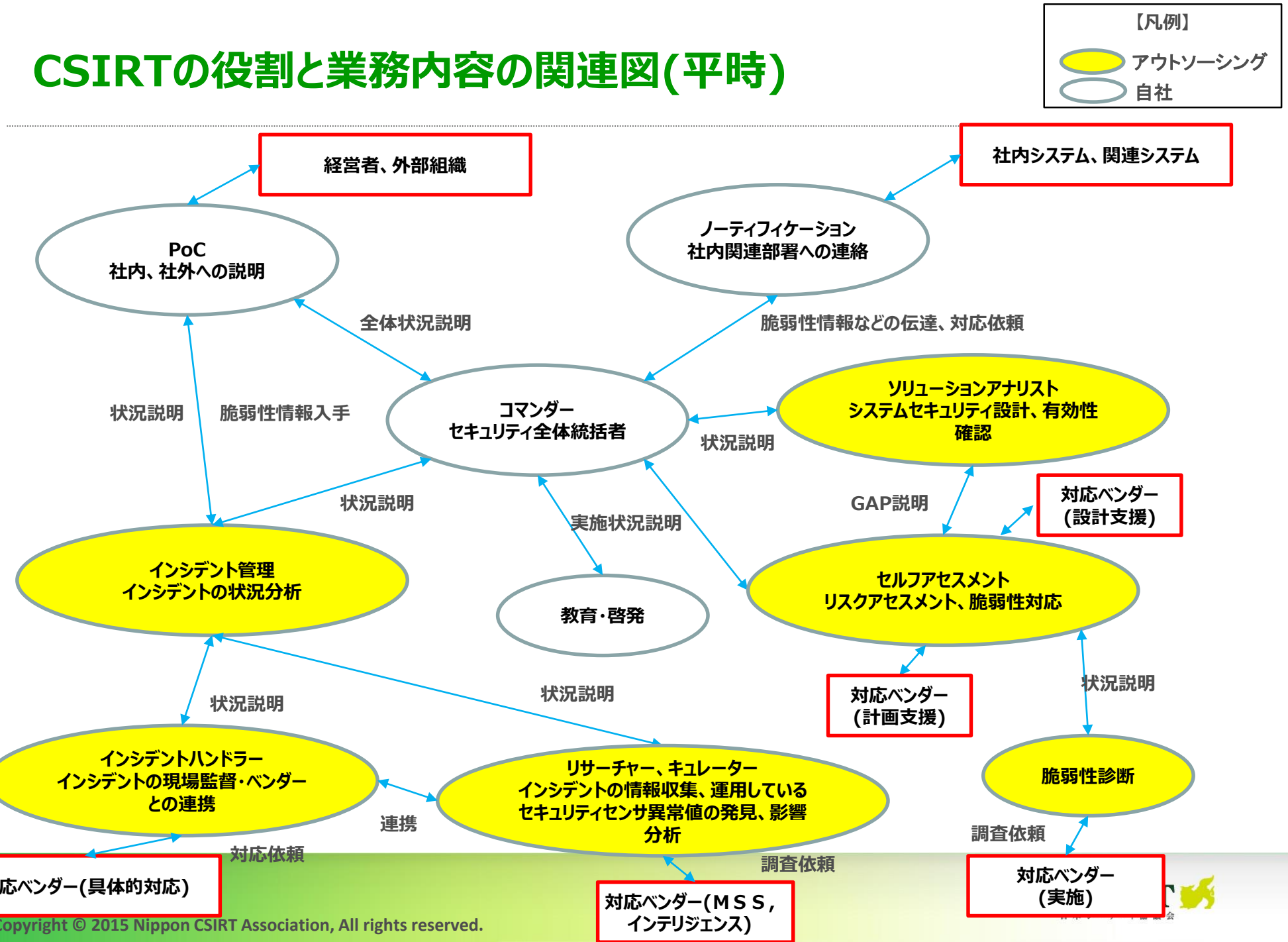
社内で情報共有はするが、システム維持についてはベンダーにお任せする。ミッションとしてはベンダーの報告を受け、プロアクティブな予防処置を行い、インシデント発生時には社として守るべき優先順位の判断を行う。最低限の自警団の機能として活動する。
手に負えなくなった場合にのみ、セキュリティ専門ベンダーに支援を要請する。

自社におけるセキュリティ対応の全体像、CSIRTで実施する役割
自社保有する役割とアウトソーシングする役割

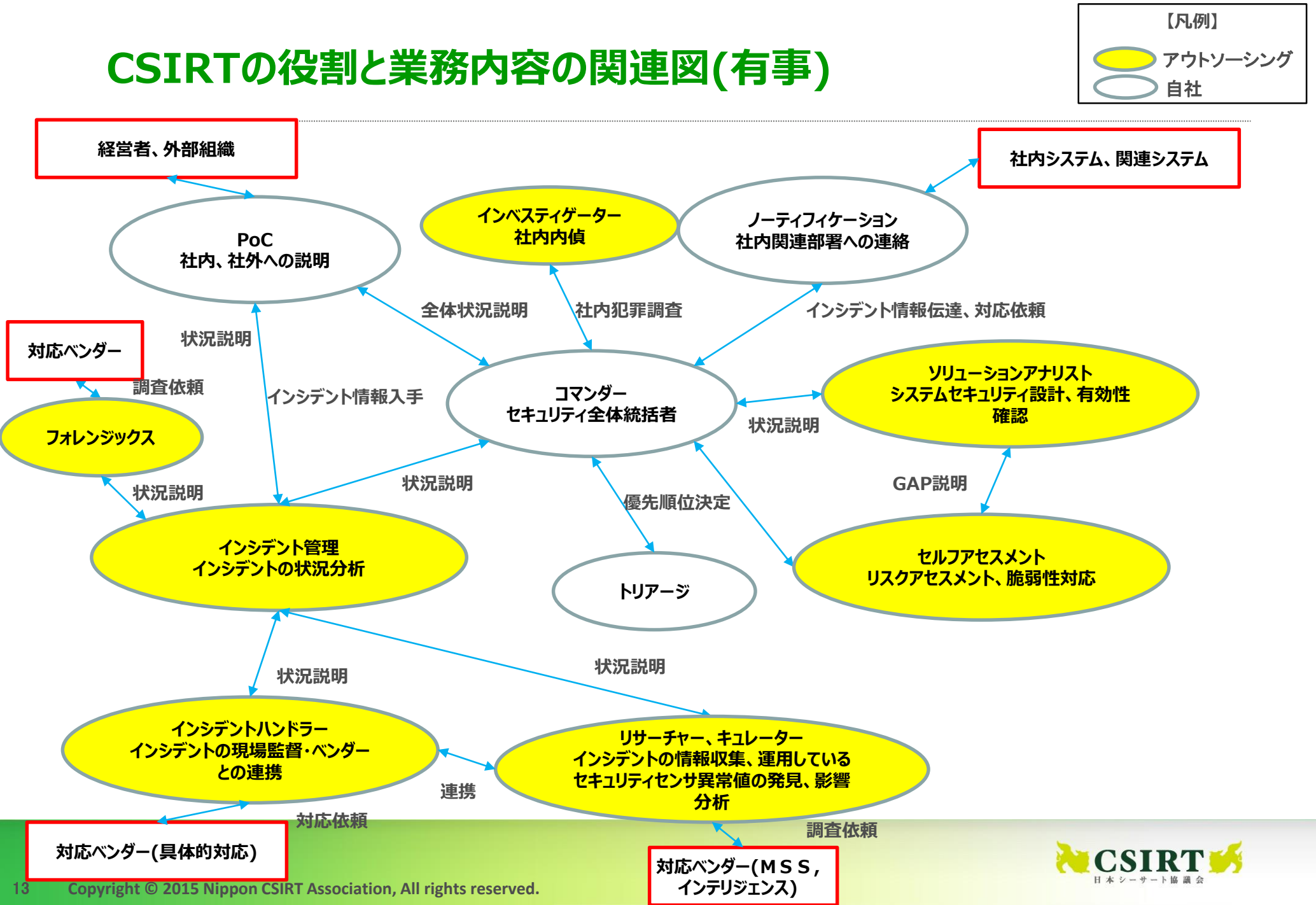
以下の役割はすべて実施するが、黄色の部分はアウトソーシングする。ベンダーと会話できるスキル、社内情報共有としてベンダーの言葉を伝えられるスキル、優先順位を決定できるスキル、社内教育ができるスキルが必要となる。

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。

CSIRTの役割と業務内容の関連図(平時)



CSIRTの役割と業務内容の関連図(有事)



役割と必要となるスキル、キャリアパス

【凡例】
アウトソーシング
自社

役割と業務内容	必要スキル	キャリアパス
PoC 社内、社外への説明	経営者、マスコミへの説明能力	一般事務とのローテーション可
ノーティフィケーション 社内関連部署への連絡	システム担当向けの文章作成	一般事務とのローテーション可
コマンダー セキュリティ全体統括者	プロジェクトマネジメント インシデント全体統制スキル、全体方針策定・説明能力 自社内システム内容の把握力 ベンダーとの会話能力	一般事務とのローテーションは可能であるが、 ある程度システムに関する理解力が必要となる。
教育・啓発	自社社員への教育、ガイドライン作成 教育資料作成、プレゼン、情報発信(一般向け文章作成)	一般事務とのローテーション可
トリアージ 優先順位の決定	自社システムの全体像を考慮し上での ビジネスインパクト判断による優先順位の決定	一般事務とのローテーション可

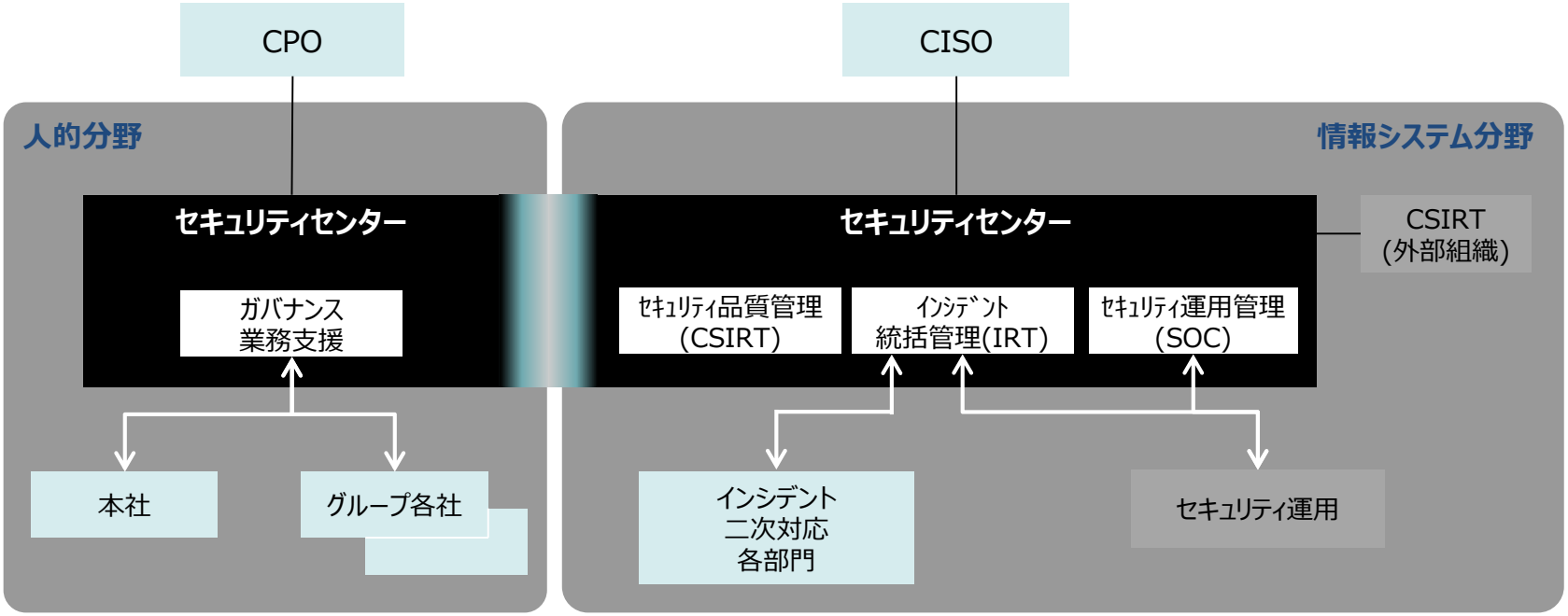
パターンB

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の一例。この例ではCSIRTだけでなく、自社全体におけるセキュリティについて記載する。

システム維持管理を社内で運用しているが、SOCの一部をアウトソーシングしている。
ベンダーの報告を受け、プロアクティブな予防処置を行い、インシデント発生時には社として守るべき優先順位の判断を行い、ある程度のインシデント対応を行う。
社内のインシデント対応で賄えない場合、もしくは対応内容の有効性の検証のためにセキィリティ専門ベンダーに支援を要請する。

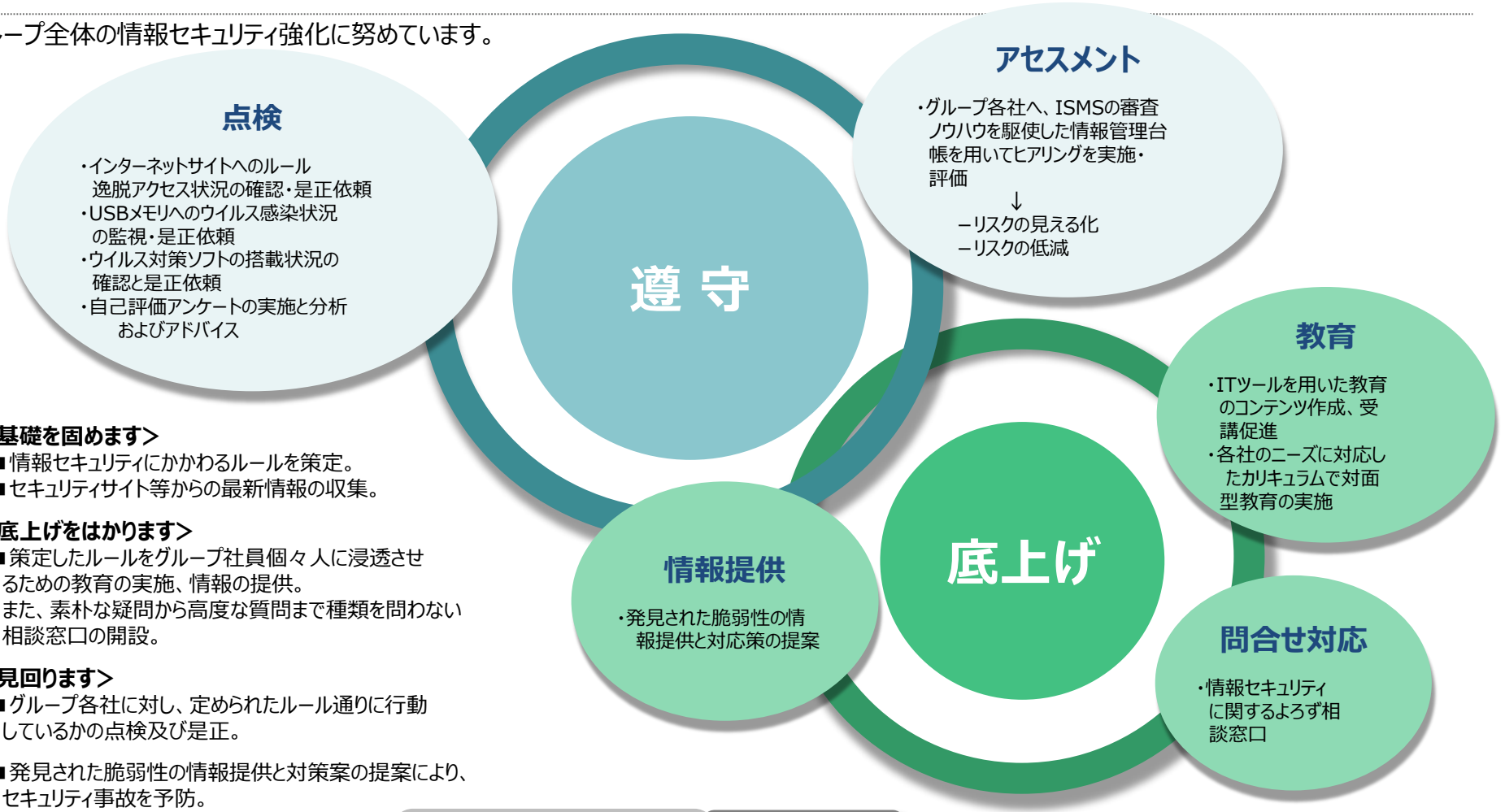
自社におけるセキュリティ対応の全体像、CSIRTの位置づけ

グループ各社におけるセキュリティに関する事柄を一元的に対応する。
CSIRTのスコープは右の情報システム分野であるが、左の人的分野もセキュリティ対応のスコープとしている。
情報システム分野とガバナンスを含めた人的分野をセキュリティ推進の両輪として活動している。



セキュリティセンター(人的分野)の機能概要

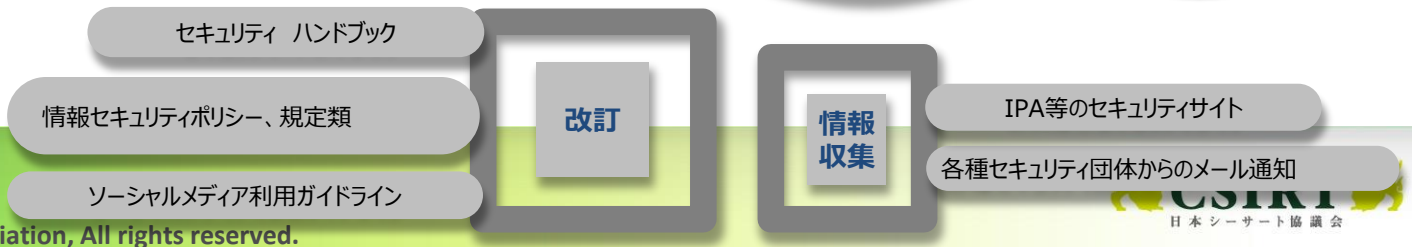
グループ全体の情報セキュリティ強化に努めています。



＜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＞
- ■策定したルールを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。



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、24時間365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	
CSIRT	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。

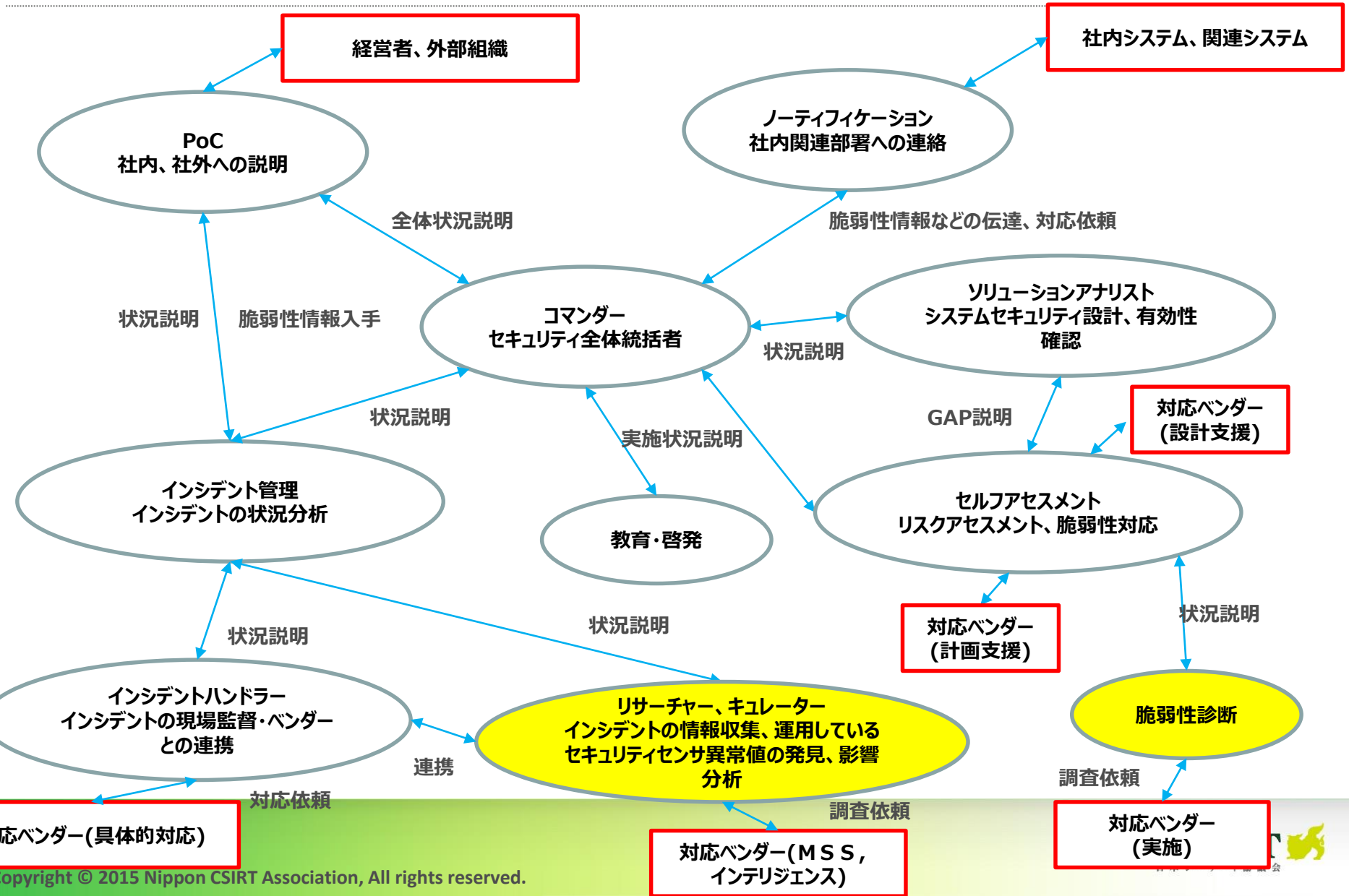
＊1：手順書化されたインシデント対応については、セキュリティ・センターにて対応を実施する。
アプリや基盤担当者にて都度判断が必要な(手順化できない)二次対応については、セキュリティ・センターは、インシデント統括管理として各主管部署と協力しながら対応にあたる。

自社保有する役割とアウトソーシングする役割

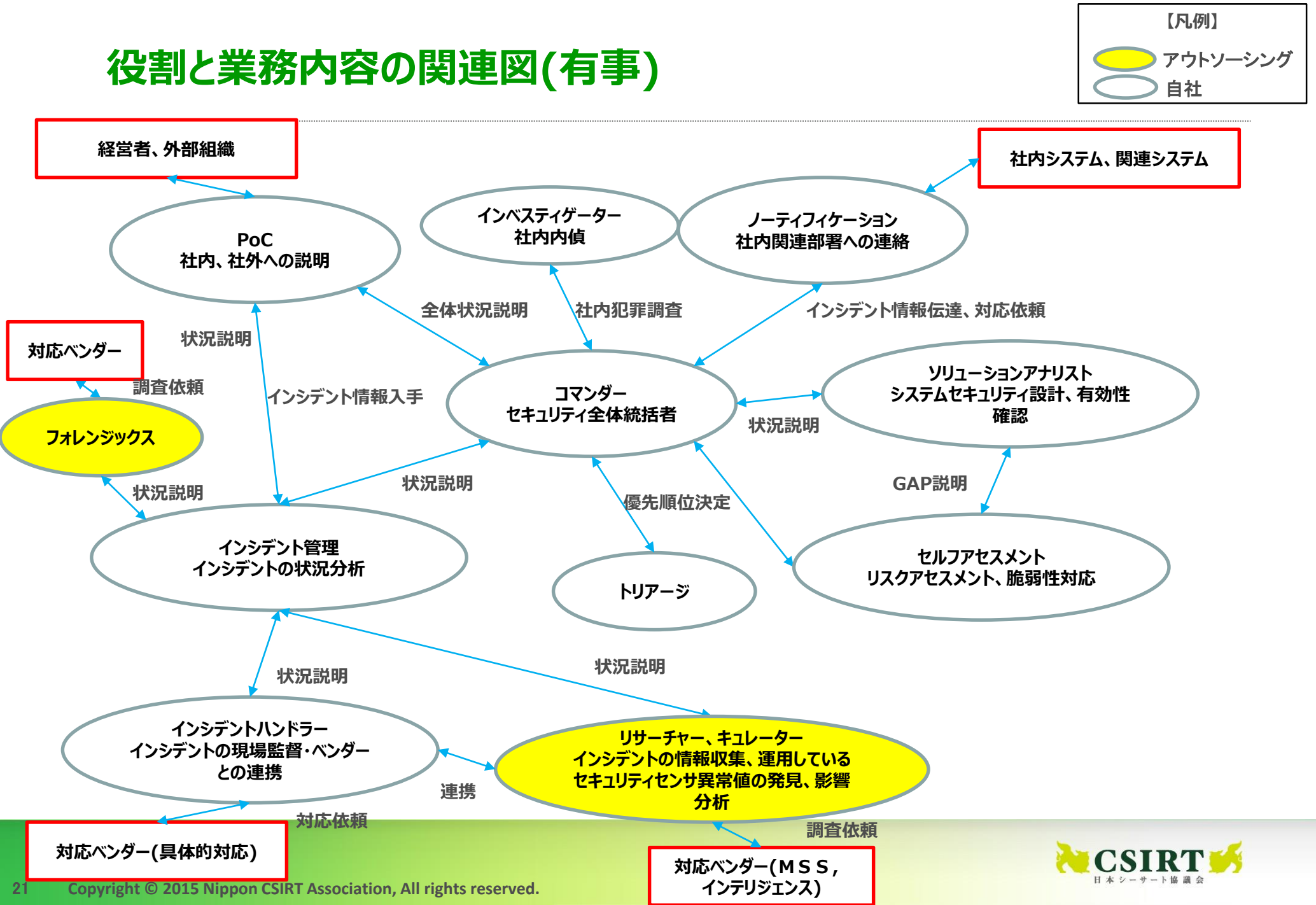
以下の役割はすべて実施するが、黄色の部分はアウトソーシングする

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。

役割と業務内容の関連図(平時)



役割と業務内容の関連図(有事)



役割と必要となるスキル、ベンダーに要求するスキル(平時)

		ベンダーに要求するスキル
PoC 社内、社外への説明	経営者、マスコミへの説明能力	
ノーティフィケーション 社内関連部署への連絡	システム担当向けの文章作成	
コマンダー セキュリティ全体統括者	プロジェクトマネジメント インシデント全体統制、全体方針策定、承認	
インシデントハンドラー インシデントの現場監督・ベンダーとの連携	リサーチャー、キュレーターの意見を理解し、方針に基づいたインシデント対応(定型化されたインシデント)のベンダーへの指示、進捗管理	⇔ インシデントハンドラー
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	セキュリティ機器(FW類、サーバ類、端末類)のログ類による分析、異常値の発見(新技術を使ったＳＩＥＭ類のスキル)他会社の情報収集	⇔ アナリスト
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	セキュリティ機器の全体設計 有効性評価	⇔ ＩＴスペシャリスト アプリケーションスペシャリスト
セルフアセスメント リスクアセスメント、脆弱性対応	自社システムのリスクアセスメント 脆弱性対応させるための文書、交渉	⇔ コンサルタント (実施支援)
脆弱性診断	脆弱性診断 インフラ、アプリ、モバイル	⇔ 脆弱性診断士
教育・啓発	自社社員への教育、ガイドライン作成 教育資料作成、プレゼン、情報発信(シロート向け文章作成)	

役割と必要となるスキル、ベンダーに要求するスキル(有事)

【凡例】
アウトソーシング
自社

		ベンダーに要求するスキル
コマンダー セキュリティ全体統括者	プロジェクトマネジメント インシデント全体統制、全体方針策定、承認	
トリアージ 優先順位の決定	自社システムの全体像を考慮し上での ビジネスインパクト判断による優先順位の決定	
インシデント管理 インシデントの状況分析	インシデントの影響と対応状況を 聞いて上での方針策定	
インシデントハンドラー インシデントの現場監督・ベンダー との連携	リサーチャー、キュレーターの意見を理解し、 方針に基づいたインシデント対応のベンダーへの指示 影響調査、復旧対応(暫定、恒久)	⇔ インシデントハンドラー
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	セキュリティ機器(FW類、サーバ類、端末類) のログ類による分析、インパクト調査 世界情勢の把握、犯人プロファイルの調査	⇔ アナリスト
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	セキュリティ機器類の有効性確認	
セルフアセスメント リスクアセスメント、脆弱性対応	対象システムの脆弱性対応状況確認	
フォレンジックス	仮説の立案、フォレンジックスによる仮説の検証 フォレンジックス機器の選択、フォレンジックス依頼内容の指示 シグニチャ、ワクチンの作成依頼	⇔ フォレンジックアナリスト マルウェアアナリスト ネットワークアナリスト
インベスティゲータ 社内内偵	内部犯行調査、内偵作業	

業務の洗い出しとグルーピング、キャリアパス

経過年数	適合確認系	SOC,CSIRT,IRT系	ドキュメント、教育、アセスメント・監査系	備考
11	セキュリティ知識の向上	ＩＲＴ能力の向上 マネジメント力の向上		
10	情報収集 説明力 向上	情報収集 説明力 向上		
9				
8	ポリシー・ガイドライン 規定策定 適合確認	ポリシー・ガイドライン 規定策定 ＩＲＴ業務		
7			説明力向上	
6	関連法律知識 セキュリティマネジメント	セキュリティ知識の習得	教育資料作成 教育実施	
5	セキュリティ知識の習得			赤線の年度から実務開始
4		障害対応経験 (統制者)	セキュリティ知識の習得 関連法律知識 セキュリティマネジメント	
3	システム開発経験 (基盤系、アプリ系)			青線の年度から教育開始
2		システム開発経験 (基盤系、アプリ系)	スタッフ経験 プレゼン経験	
1				着任のベースライン
	業務グループＡ	**業務グループＢ**	**業務グループＣ**	

セキュリティ業務に要求される業務を３つのグループに分け、グループ毎にキャリアパスを示す。
Ａグループの場合には一般開発組織とのローテーションは可能。
Ｂグループはインシデント統制とのローテーション可能。または、セキュリティ専門家として育成する。
Ｃグループは高齢者雇用、時短勤務も可。

役割と業務グループのマッピング

グループA：適合確認系
グループB：SOC,CSIRT,IRT系
グループC：ドキュメント、教育系

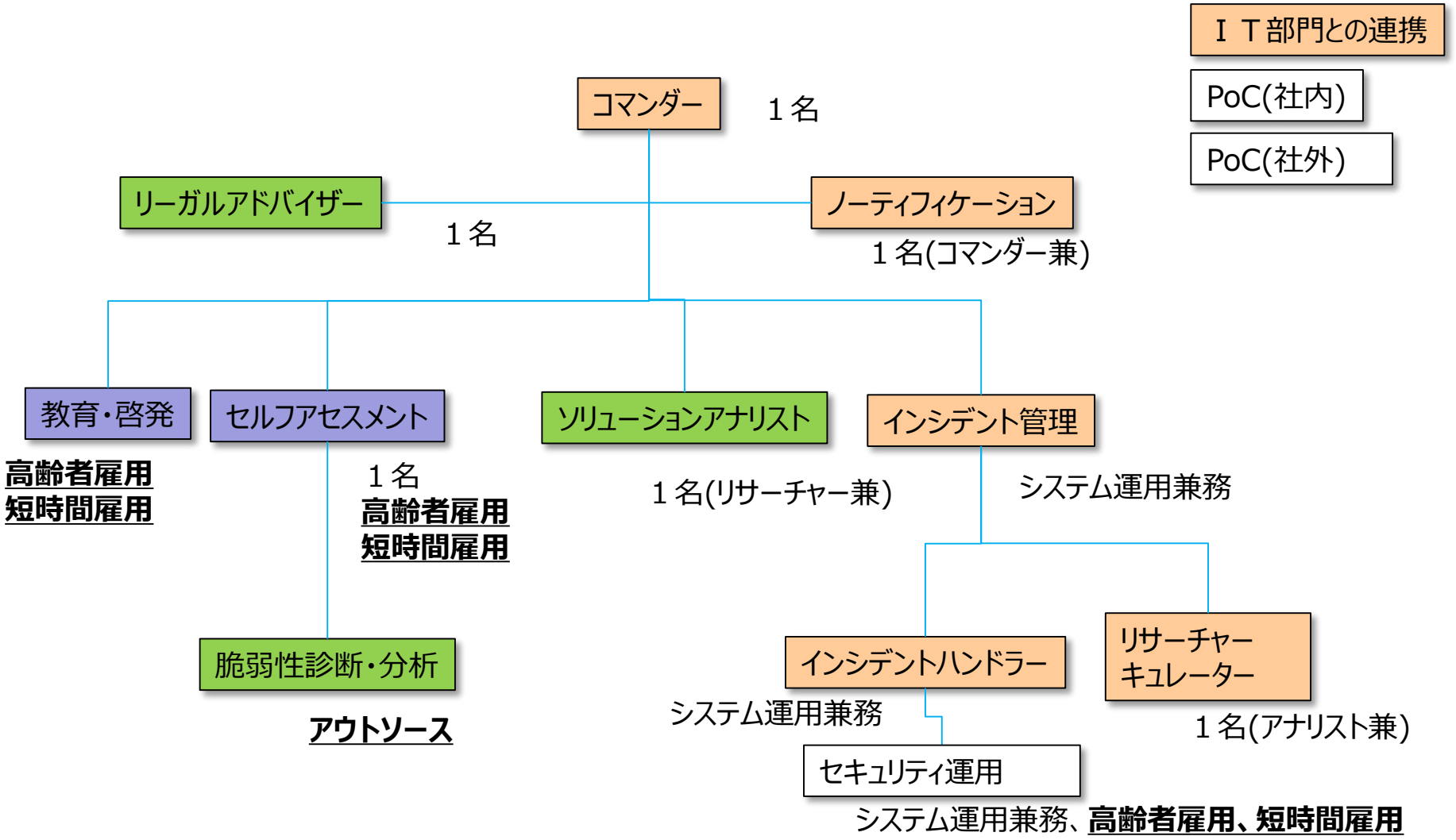
グループ	役割名称	業務内容
情報共有	PoC(社外)	NCA、FIRST、CSIRT、警察、監督官庁、等々との情報連携
	PoC(社内)	法務、渉外、IT部門、広報、各事業部、等々との情報連携
	IT部門との連携	適格で要領を得た文書の作成
	リーガルアドバイザー	コンプライアンス、法的内容とシステム間の翻訳
	ノーティフィケーション	各関連部署との連絡ハブ、情報発信
情報収集・分析	リサーチャー、キュレーター	定例業務。インシデントの情報収集、各種情報に対する分析、国際情勢の把握
	脆弱性検査、診断	NW、OS、セキュアプログラミングの検査、診断
	脆弱性分析、評価	NW、OS、セキュアプ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。

赤字はセキュリティ専門家特有のスキルを必要とする業務

平時の体制

平常時体制図(セキュリティセンサー類の規模によって人数は変動)

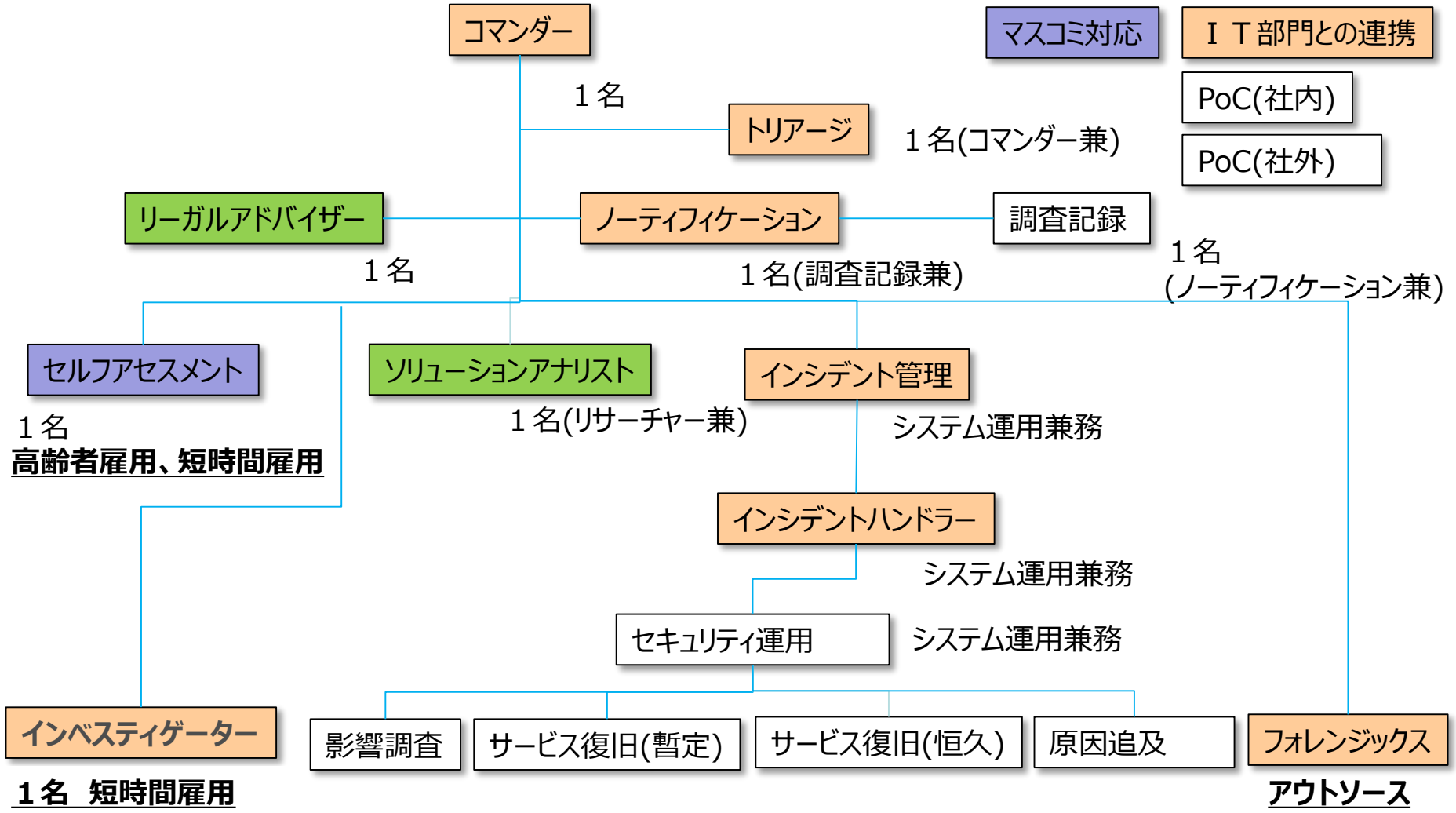
グループA：適合確認系
グループB：SOC,CSIRT,IRT系
グループC：ドキュメント、教育系



有事の体制

有事体制図(同時発生の多重度によって保持すべき人数は変動)

グループA：適合確認系
グループB：SOC,CSIRT,IRT系
グループC：ドキュメント、教育系

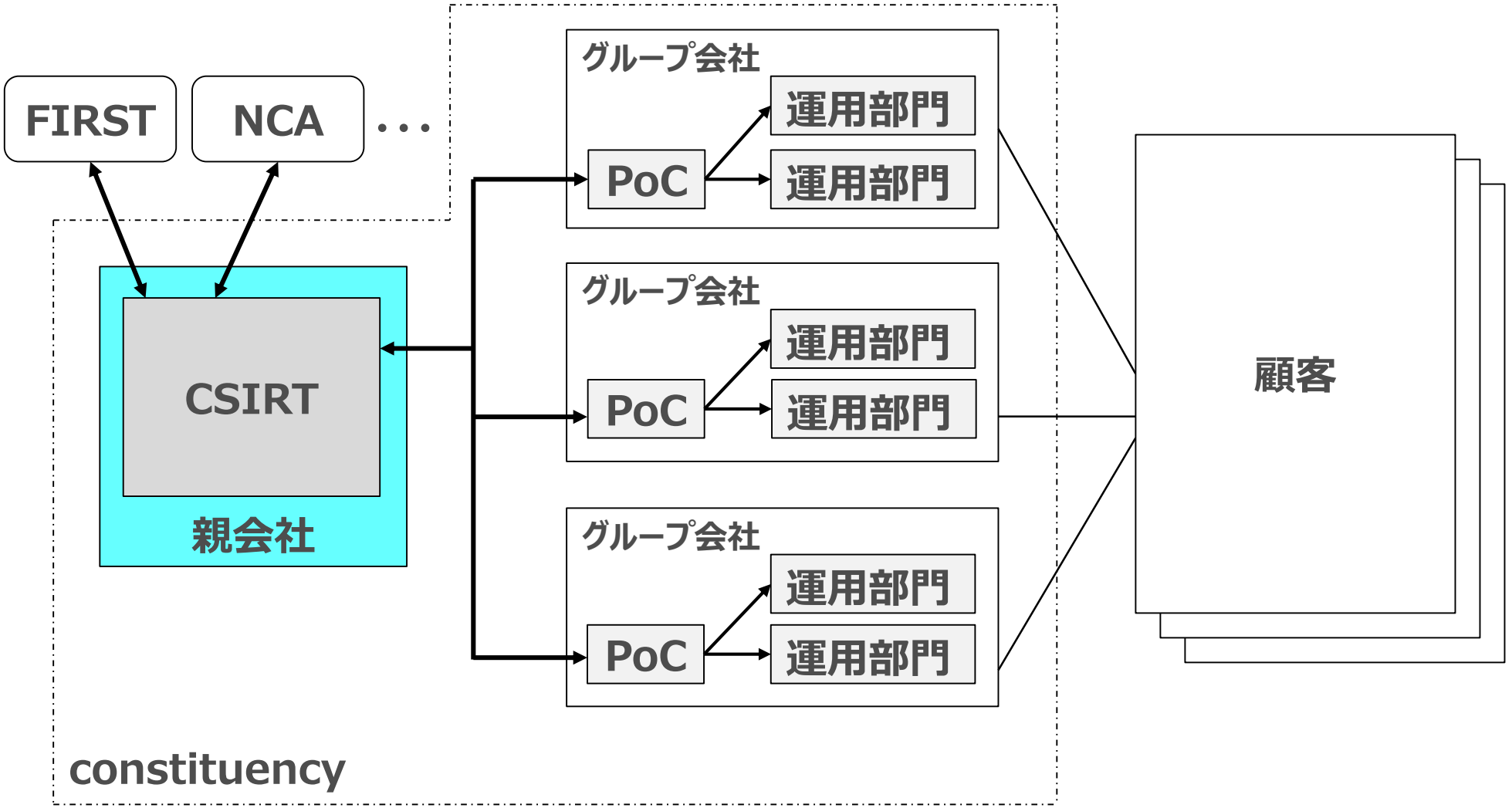


パターンC

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の一例

自社グループ向けCSIRTや企業向けのCSIRTサービスを行う。
ほとんどすべてのCSIRT機能を自社保有し、研究・開発・未知の脅威の発見、情報発信なども公的に行う。

自社におけるセキュリティ対応の全体像、CSIRTの位置づけ



業務の洗い出しとグルーピング

事前対応型サービス

- セキュリティアドバイザリ
- インシデント検知
- 脆弱性情報配信
- セキュリティレポーティング

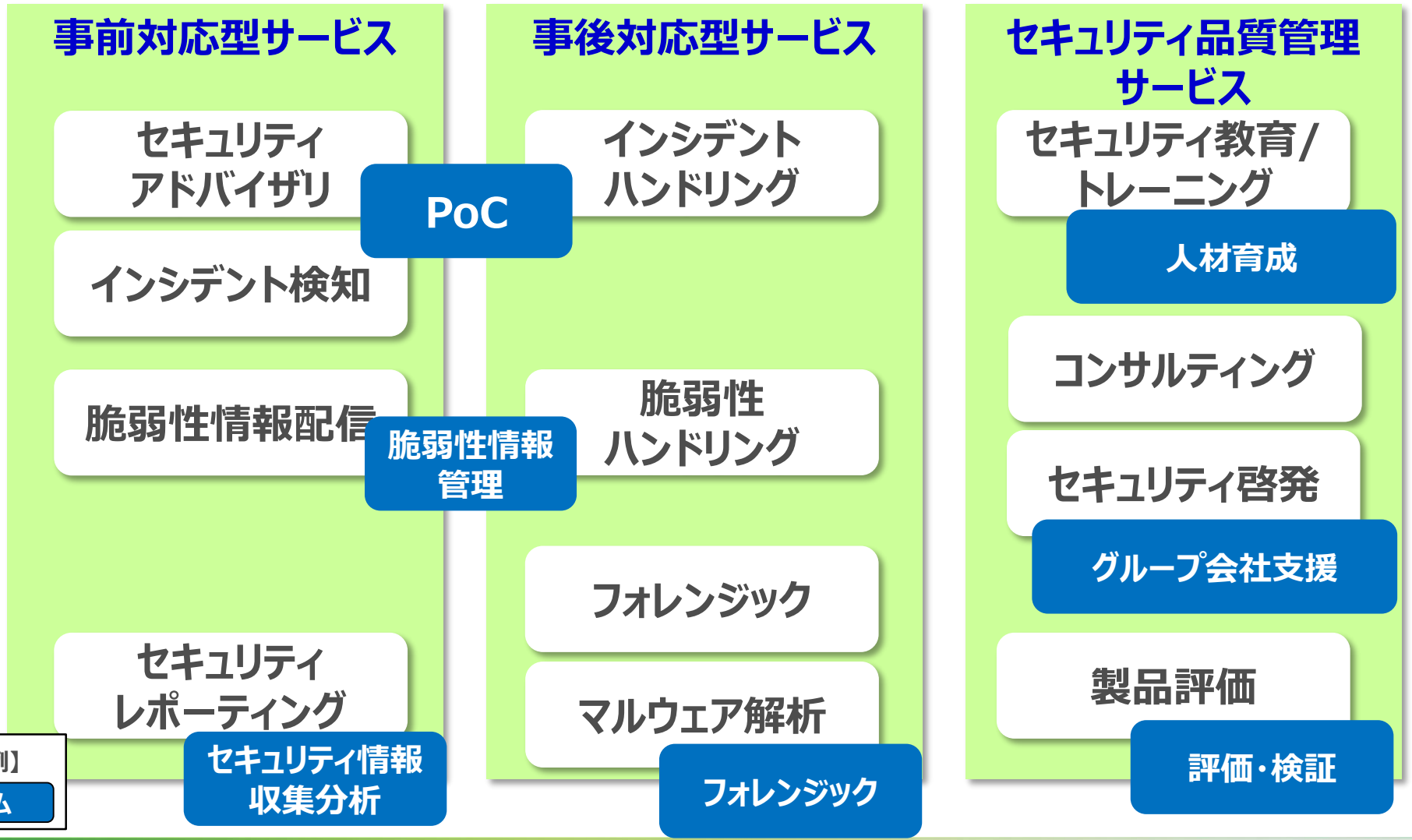
事後対応型サービス

- インシデントハンドリング
- 脆弱性ハンドリング
- フォレンジック
- マルウェア解析

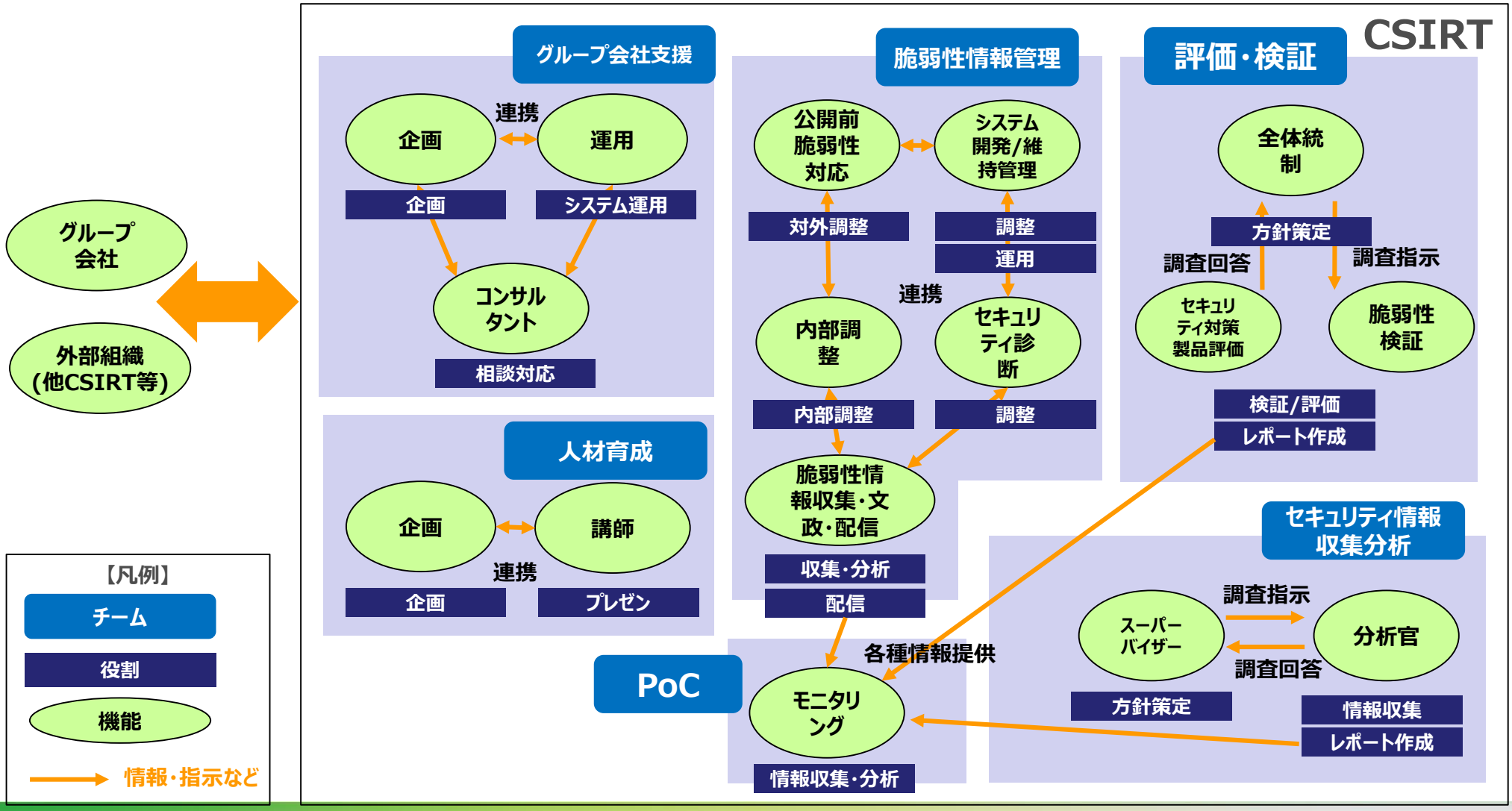
セキュリティ品質管理サービス

- セキュリティ教育/トレーニング
- コンサルティング
- セキュリティ啓発
- 製品評価

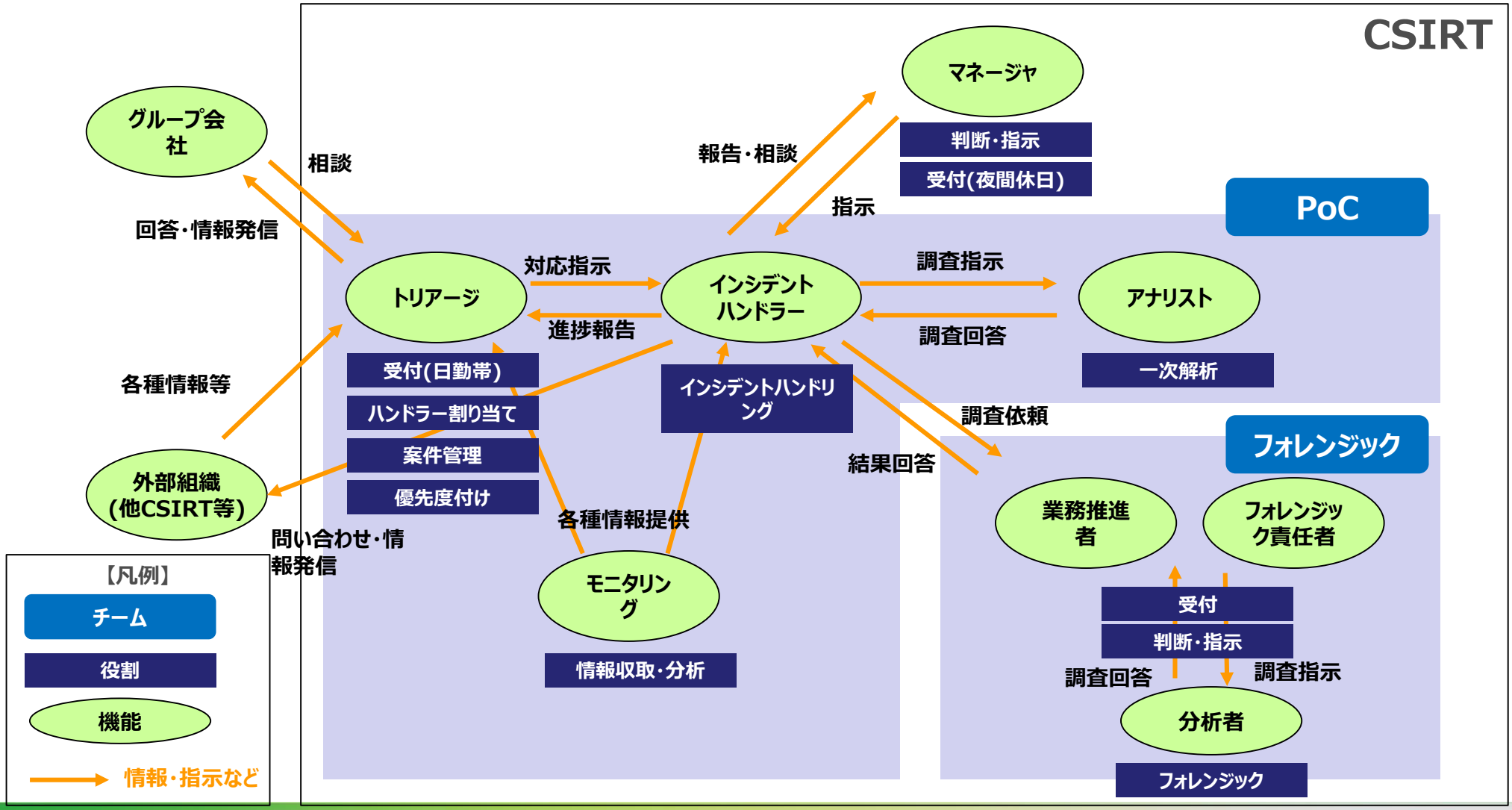
業務の洗い出しとチームのマッピング



CSIRTの役割と業務内容の関連図(平時)



CSIRTの役割と業務内容の関連図(有事)



役割と必要となるスキル(1/3)

チーム	役割	定義	スキル	有事	平時
PoC	トリアージ	インシデントの優先順位付けを行い、そのインシデントに対してハンドラーを割り当てる	・危機管理能力 ・マネジメント能力 ・コミュニケーション能力 ・コーディネーション能力 ・グループ内体制/システムに関する知識	○	
	インシデント ハンドラー	トリアージしたインシデントに対してのインシデントハンドリングを実施する	・インシデントハンドリング能力 ・コミュニケーション能力 ・情報セキュリティ技術に関する知識	○	
	アナリスト	インシデントの際の、一次解析を実施する	・OS/ファイルシステム/アプリケーション等に関する知識 ・各種ソフトウェア/NW解析ツールおよび製品に関する知識・経験	○	
	モニタリング	サイバー攻撃情報、Webサイト改ざん情報等を収集し、ハンドラー/トリアージ担当者に提供する	・情報収集/分析能力	○	○
人材育成	企画	教育プログラム等の企画を行う	・コーディネーション能力 ・グループ内システムの立ち位置の理解 ・情報セキュリティに関する知識・経験		○
	講師	教育プログラム等の説明を行う	・プレゼンテーション能力 ・コミュニケーション能力 ・プログラム策定/教材製作/プレゼン資料作成に関する能力・経験 ・セキュリティに関する知識・経験		○
フォレンジック	フォレンジック 責任者	業務管理、業務実施に伴う情報セキュリティ管理を行う	・情報セキュリティ監査能力 ・マネジメント能力 ・OS/ファイルシステム/アプリケーション/プロトコル/攻撃手法等に関する知識 ・フォレンジック用ツールに関する知識	○	
	業務推進者	分析方針策定、作業指示、結果取りまとめ指示、分析環境整備/改善を行う	・情報セキュリティ監査能力 ・マネジメント能力 ・OS/ファイルシステム/アプリケーション/プロトコル/攻撃手法等に関する知識 ・フォレンジック用ツールに関する知識・経験	○	
	分析者	個々の案件についての分析実施、結果整理報告を行う	・レポート作成能力 ・分析能力 ・OS/ファイルシステム/アプリケーション/プロトコル/攻撃手法等に関する知識 ・フォレンジック用ツールに関する知識・経験	○	

役割と必要となるスキル(2/3)

チーム	役割	定義	スキル	有事	平時
脆弱性情報管理	内部調整	脆弱性情報の共有ルート、共有方法などについて、予め情報共有先や必要な場合には内部統制組織等と調整する	・コーディネーション能力 ・リスクマネジメント能力 ・CVE/CVSS等に関する知識 ・グループ内システムや環境の十分な理解(OS/DB/アプリケーション等含む) ・その他、一般的なITセキュリティの知識		○
	情報収集・分析・送付	脆弱性情報の収集および分析を行い、配信すべき脆弱性を決定し、送付する	・リスクマネジメント能力 ・OS/ファイルシステム/アプリケーション等に関する知識 ・CVE/CVSS等に関する知識 ・グループ内システムや環境の十分な理解(OS/DB/アプリケーション等含む) ・その他、一般的なITセキュリティの知識		○
	公開前脆弱性対応	JPCERT/CC等の他組織と連携し、公開前脆弱性情報およびそれに類する情報を開発関係者に通知する 関係組織と当事者の間にたち、脆弱性の公開日の調整等の仲介を行う	・リスクマネジメント能力 ・コーディネーション能力 ・CVE/CVSS等に関する知識 ・グループ内システムや環境の十分な理解(OS/DB/アプリケーション等含む) ・その他、一般的なITセキュリティの知識		○
	システム開発/維持管理者	配信判定支援システムやアセット情報管理システムなど、業務に必要なシステムを開発し、維持管理する	・システム開発管理 ・セキュリティ設計 ・セキュリティ運用 ・その他、一般的なITセキュリティの知識		○
グループ会社支援	システム開発/維持管理者	配信判定支援システムやアセット情報管理システムなど、業務に必要なシステムを開発し、維持管理する	・システム開発管理 ・セキュリティ設計 ・セキュリティ運用 ・その他、一般的なITセキュリティの知識		○
	運用	ポータルサイトの運用を行う	・Webシステム運用能力 ・データモデリング能力 ・CSIRT連携システムに関する知識		○
	企画	ポータルサイトの企画・改善を行う	・Webシステム運用能力 ・データモデリング能力 ・コーディネーション能力 ・CSIRT業務改善能力		○
	コンサルタント	各種相談受付を行う	・プレゼンテーション能力 ・コミュニケーション能力 ・コンサルティング能力 ・グループ内システムの立ち位置の理解 ・セキュリティに関する知識・経験		○

役割と必要となるスキル(3/3)

チーム	役割	定義	スキル	有事	平時
セキュリティ情報収集分析	分析官	一般公開されている情報ソースからサイバーセキュリティに関する情報を抽出し、専門的知見に基づき整理・分析を行う 収集した情報のデータベース化を行い、週次/月次/四半期/年次などの単位で情報の整理やレポートの作成を行う また、関連組織との情報交換を行う	・情報収集/分析能力 ・レポート作成能力 ・コミュニケーション能力		○
	スーパーバイザー	情報収集方針、分析テーマ設定を行う また、分析レポートのレビュー行う	・レポート作成能力 ・情報収集/分析能力 ・マネジメント能力		○
評価・検証	検証	セキュリティ製品の評価・検証、脆弱性の検証を行い、レポーティングを行う	・脆弱性に関する知識 ・セキュリティ製品/脆弱性の評価/検証に関する技術/ノウハウ ・レポーティング能力		○
	全体統制	検証方針策定、作業指示、結果取りまとめ指示、検証環境整備/改善を行う	・マネジメント能力 ・脆弱性に関する知識 ・セキュリティ製品/脆弱性の評価/検証に関する技術/ノウハウ ・レポーティング能力		○

役割毎のキャリアパス

年数	PoC	グループ会社支援	人材育成	フォレンジック	セキュリティ情報収集分析	評価・検証	脆弱性情報管理
5	・国内外の動向やセキュリティ技術に精通し、過去のナレッジや類似案件をもとに、複雑なインシデントハンドリング業務を遂行可能	・システム化による業務改善能力の向上	・マネジメント能力の向上	・マネジメント力の向上	・マネジメント能力の向上 ・各種トピックのこれまでの経緯、各種団体の活動状況の把握	・マネジメント能力の向上	・脆弱性ハンドリングにおいて、外部で指導的な役割を果たす ・脆弱性ハンドリングにおいて、将来にむけた新しい取組みを創出
4							
3	・社内、グループ会社の体制やルールに精通し、複雑なインシデントハンドリング業務を遂行可能 ・インシデントを適切に解釈し、管理職が判断できるよう説明・報告を実施可能					・攻撃の成立条件の明確化 ・暫定対処策の策定能力 ・説明能力の向上	・国内外の動向やセキュリティ技術に精通し、複雑な脆弱性ハンドリング業務を遂行可能。 ・脆弱性ハンドリングのマネージャ代行の役割を果たせる
2	・一般的なインシデントハンドリング業務を遂行可能 ・コミュニケーション能力、ネゴシエーション能力の向上	・プレゼンテーション能力の向上 ・コンサルティング能力の向上 ・マネジメント能力の向上	・プレゼンテーション能力の向上 ・コーディネーション能力の向上 ・マネジメント能力の向上	・フォレンジックに関するスキルの向上 ・レポート作成能力の向上	・情報収集/分析能力の向上 ・レポート作成能力の向上 ・特定のセキュリティトピックの経緯の把握		・社内、グループ会社の体制やルールに精通し、脆弱性ハンドリングの定型的な業務は自律的に遂行可能。
1	・指導者による指示のもと、インシデントハンドリング業務を遂行可能 ・コミュニケーション能力の向上	・ポータルサイト/CSIRT連携システムの構築・運営の経験 ・データモデリング能力の向上 ・CSIRT構築支援等の経験	・セキュリティ教育資料、セキュリティ運用資料の経験 ・プレゼン資料作成能力の向上 ・セキュリティ関連講師の経験	・解析対象の基礎知識の取得(レジストリ、ファイルシステムの仕組みなど) ・解析ツールの基礎知識および解析ノウハウの取得 ・フォレンジック業務への従事	・情報収集分析業務の経験	・脆弱性検証業務の経験 ・セキュリティ対策製品検証業務の経験 ・各種レポート作成業務の経験	・指導者による指示のもと、脆弱性ハンドリング・セキュリティ診断業務を遂行可能 ・実務能力の向上
前提条件	・IT技術基礎知識 ・セキュリティ技術基礎知識 ※あるとよい経験：障害対応、ソフトウェア開発	・セキュリティ技術基礎知識	・セキュリティ技術基礎知識	・セキュリティ技術基礎知識	・セキュリティ技術基礎知識	・セキュリティ技術基礎知識・検証環境構築スキル (Linux, NW, Web/AP/DBサーバ等)	・セキュリティ技術基礎知識

募集要項のサンプル

【サンプル】XX-CSIRT担当者募集

募集件名	【急募】CSIRT担当者(リサーチャー、キュレーター)
採用数	若干名
職務内容(ロール)	セキュリティログを確認し、特異点を見つけて担当にエスカレーションしてください。高齢者、第二新卒歓迎！ 典型的な職務内容(ロール)：PCオペーレーション ヒューマンスキル：緻密な作業が得意な方。会話が苦手な方も可。
必要な経験、能力、資格	経験：サーバ、NW構築・運用経験 能力：PC、Linux操作一般 資格：特に規定なし
あると望ましい経験、能力、資格	経験：サーバログ、FWログ等のログ分析経験 能力：持久力、集中力 資格：特になし
導入教育	ログの分析の仕方を要領書を基に教育します。
休日・休暇	週休2日制、短時間勤務、シフト勤務も要相談。
備考	成長産業！企業のリスク回避につながる注目の仕事です！

【サンプル】XX-CSIRT担当者募集

募集件名	【急募】CSIRT担当者(ソリューションアナリスト)
採用数	若干名
職務内容(ロール)	セキュリティに関する機器類の全体設計やポリシーキープをしてください。 また開発案件についてガイドラインを遵守しているかどうかのチェックを行ってください。 ヒューマンスキル：開発者と会話できる持久力、対応力
必要な経験、能力、資格	経験：サーバ、NW構築・運用経験 能力：PC、Linux知識一般 資格：特に規定なし
あると望ましい経験、能力、資格	経験：サーバログ、FWログ等のログ分析経験 能力：本質を見極める力、応用力 資格：情報処理関係
導入教育	現在のポリシーやガイドラインの背景・内容を教育します
休日・休暇	週休２日制、短時間勤務、シフト勤務、自宅勤務も要相談。
備考	成長産業！日々発展するＩＴを活用する最先端の仕事です。

【サンプル】XX-CSIRT担当者募集

募集件名	【急募】CSIRT担当者(セルフアセスメント・教育)
採用数	若干名
職務内容(ロール)	各職場で培ってきた経験を生かして、職場のリスクアセスメントを行い、資料を作成してください。また、ガイドラインに基づいた教育を各地で行ってください。 ヒューマンスキル：コミニュケーション能力、温和で学習熱心な方
必要な経験、能力、資格	経験：要件調整、仕様調整の経験 能力：ヒアリング力、分析力、表現力、プレゼン力 資格：特になし
あると望ましい経験、能力、資格	経験：リスクアセスメント、監査などの経験、教育経験 能力：人と打ち解ける、安心させられる能力 資格：ISMS審査員、監査員
導入教育	アセスメント方針やチェックポイント、ガイドラインは事前に教育します。セキュリティ教育も実施します。
休日・休暇	時短・在宅勤務も要相談。
備考	セキュリティ教育制度あり。高齢者も可。

略称について

略称	詳細
CSIRT	Computer Security Incident Response Team
PoC	Point of Contact
NCA	Nippon CSIRT Association
FIRST	Forum of Incident Response and Security Teams
CISO	Chief Information Security Officer
SOC	Security Operation Center
CPO	Chief Privacy Officer

改版履歴

- 2015.11.16 Ver.1.0 初版作成

CSIRT人材サブワーキンググループ著者一覧

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	