Japan Information Security Management Systems User Group

JNSA 標準化部会　日本ISMSユーザグループ

ISMSとサイバーセキュリティとの関係について

JNSA 標準化部会
日本ISMSユーザグループ　リーダー
インプリメンテーション研究会　主査

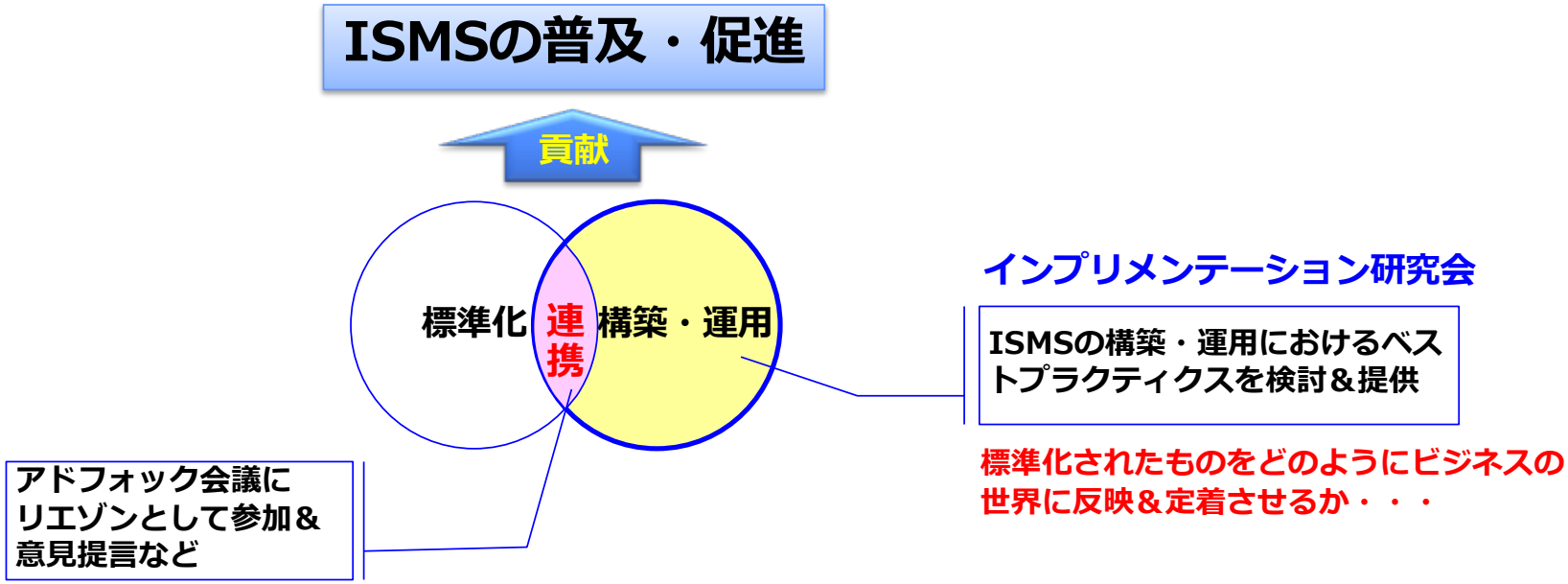
2021年1月15日

魚脇　雅晴

日本ISMSユーザグループの活動紹介

■活動目的と活動概要

日本ISMSユーザグループではISMSを構築・運用する上で規格をどう読み解いて、企業活動にISMSを積極的に実践活用する方法を検討、研究し、国内外へ発信します。具体的にはISMS認証取得企業（ユーザ）とISMSの専門家が連携し、意見交換・議論を進めることで**ISMSの構築・運用に関わるユーザ視点でのベストプラクティスを提供**し、日本における**健全かつ効果的なISMS普及・促進**に貢献する活動を行っています。



本日のお話

ISMSとサイバーセキュリティ

との関係について

最初に・・・

サイバー攻撃の怖さと
組織として
対応が必要な要素

あなたの会社（組織）は大丈夫だと言えますか？

問い掛け

サイバー攻撃に対する組織的な危機管理が出来ていると社内やお客さまに対して宣言出来ますか？

一例ですが・・・

- **機密データの取り扱い＆保管管理**
- **社員教育（脅威の認識と有事の際の行動）**
- **攻撃の検知や不審トラヒックのモニタリング**

等々

ISMS事務局の悩み・・・（サイバー攻撃対応は難しい）

ISMSは導入しているが、
サイバー対応するには
CSIRT体制の構築？

ISMSの運用も兼務・・・

ISMSは構築運用しているが・・・

CSIRT体制の構築？

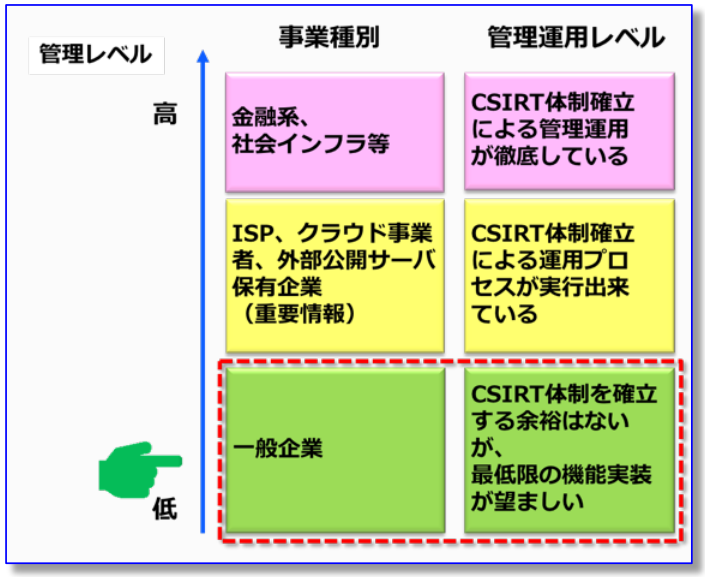
人／物／金はない！

サイバー関連スキルの人材はいない！

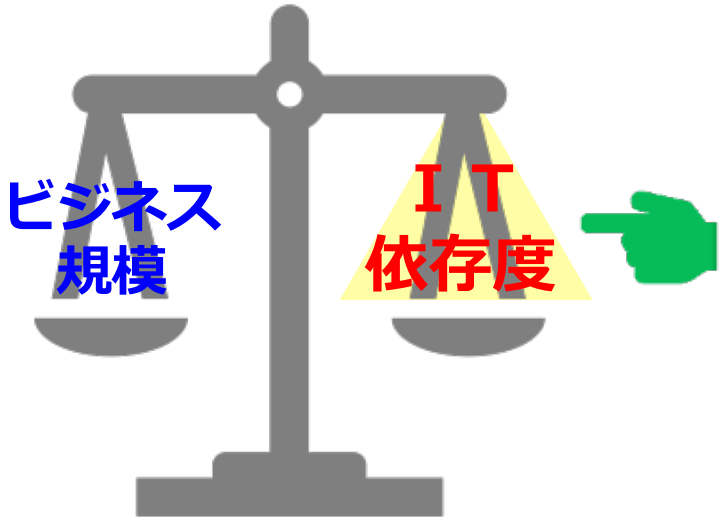
ネット接続なしでは仕事にならない・・・

中小企業でもサイバー攻撃の対象・・・

事業規模だけでは判断出来ないサイバー対応の要求レベル



ビジネス規模だけでなく
ＩＴ依存度も加味！！



小さな会社にCSIRTを構築する余裕はない！！

○CSIRTに必要な人数は？（CSIRT協議会アンケート）

設置時　5名未満37%　5～10名未満46%　10～20名未満15%　20名以上2%

活動後　5名未満11%　5～10名未満37%　10～20名未満37%　20名以上15%

○CSIRT機能の実装に必要な要員とスキルは？

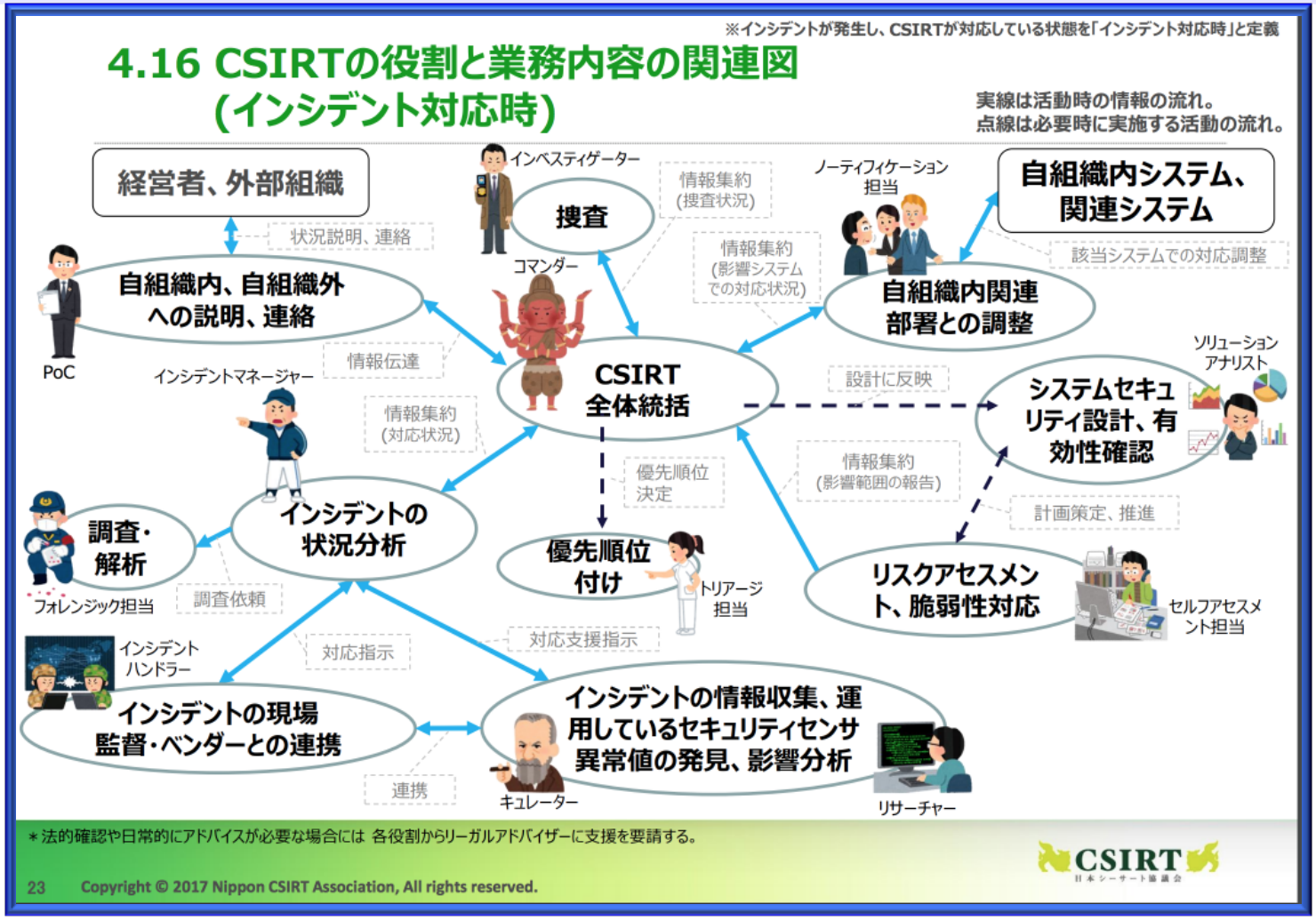
・高度なスキルを要求
（次ページ参照：CSIRTの役割と業務内容の関連図）

・企業の業種、業態、ビジネスの要求事項に応じて様々なCSIRT体制

・会社規模の小さい組織はCSIRT体制を構築するのが困難

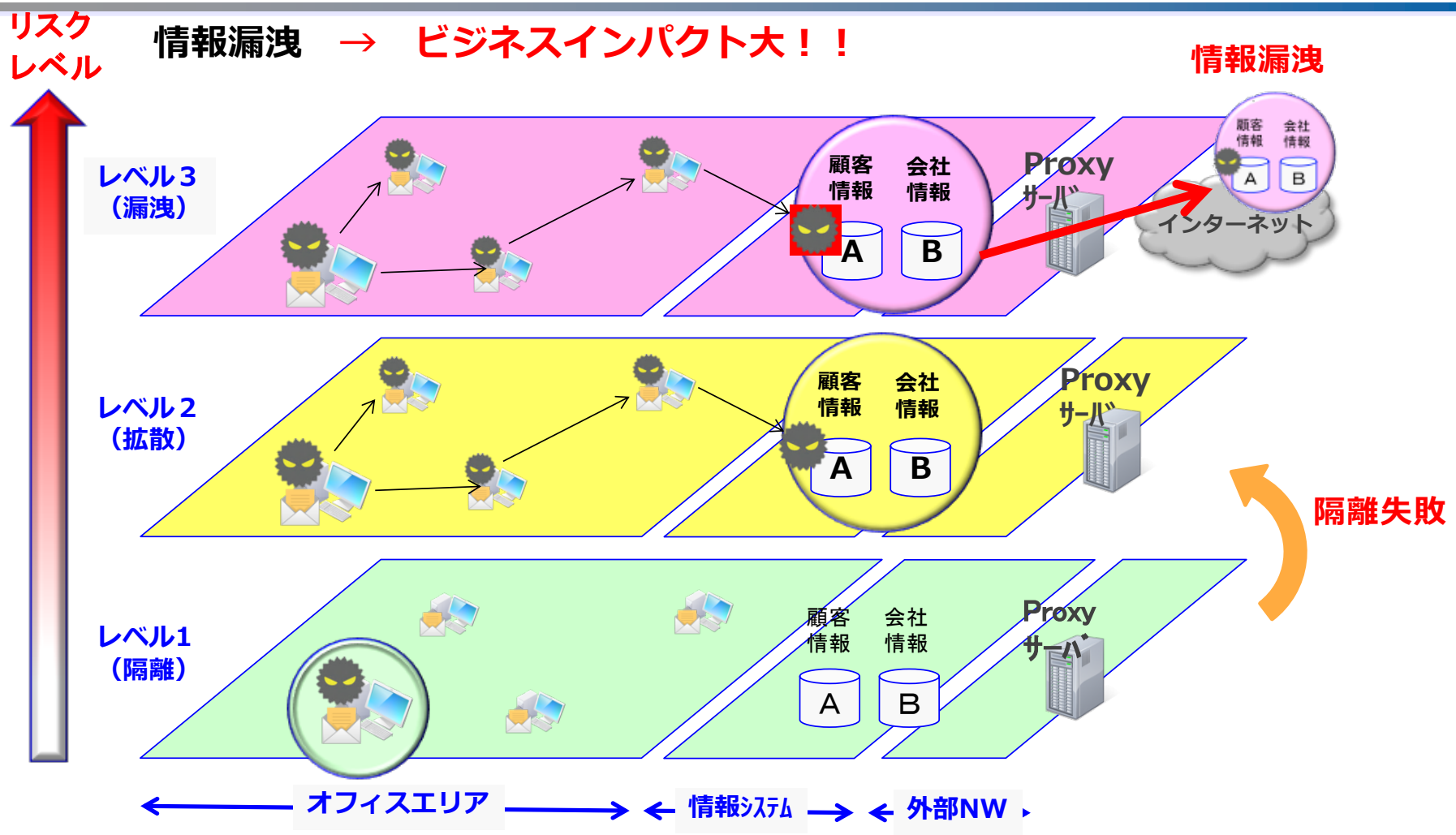
引用　JPNIC https://www.nic.ad.jp/ja/newsletter/No65/0800.html

参考資料：　CSIRTの役割と業務内容の関連図（CSIRT協議会）

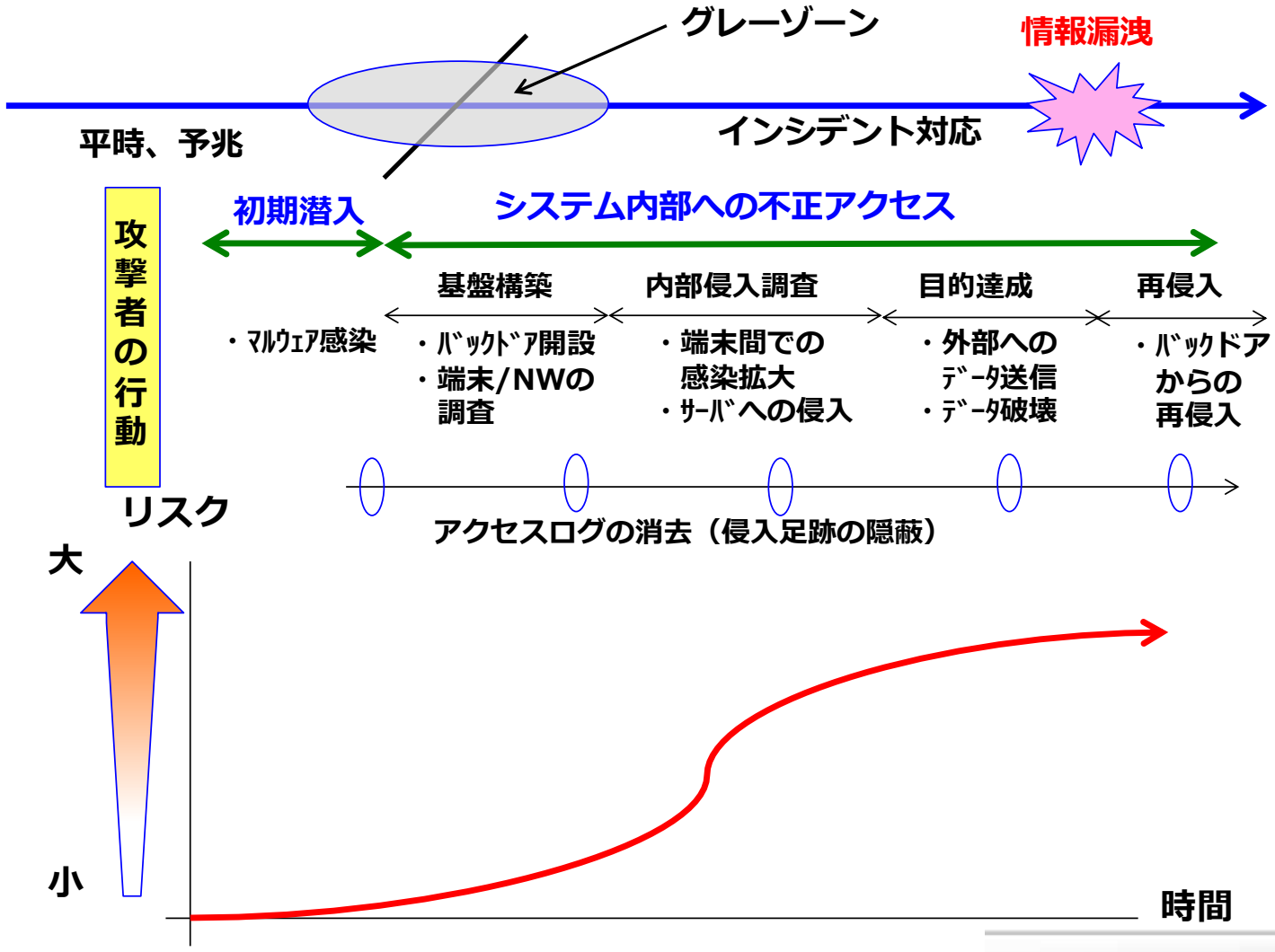


引用：CSIRT協議会資料　CSIRT人材の定義と確保http://www.nca.gr.jp/activity/imgs/recruit-hr20170313.pdf

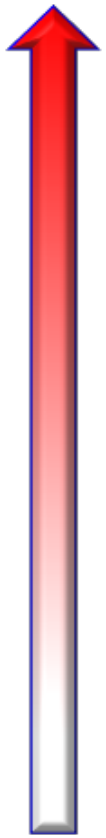
標的型攻撃メールにおけるリスクとは？



攻撃者の行動とリスクの変化



標的型攻撃メールによるビジネスインパクト



リスク レベル	ビジネスインパクト		
	影響度	インシデント対応作業	対応稼働
レベル3（漏洩） ウィルス感染したが、気づかずそのまま放置した結果、顧客情報や会社情報の漏洩	影響度　大 感染PC内の情報漏洩（複数台）＆ファイルサーバに保管した情報漏洩 ・顧客情報、会社機密情報 ・メールアドレス情報	下記の対応に加えて ・外部へのNW遮断（全社内） ・ｻｲﾊﾞｰ攻撃対応BCP発動	上記の対応に加えて ・報道対応 ・復旧対応稼働
レベル2（拡散） 標的型攻撃メールによりウィルス感染し、気づかずに二次感染	影響度　小～中 感染PC内の情報漏洩 ・顧客情報、会社機密情報 ・メールアドレス情報	下記の対応に加えて ・Proxyﾛｸﾞから情報漏洩の確認＆影響度確認 ・該当URL/ﾄﾞﾒｲﾝのﾌﾞﾛｯｸ（Proxy等）	上記の対応に加えて ・上長/事務局のｲﾝｼﾃﾞﾝﾄ対応稼働 ・IT部門の対応稼働 ・お客様謝罪対応
レベル1（隔離） 標的型攻撃メールを開いた（感染）がすぐにLANケーブルを抜線	ほぼ無し 情報漏洩は無し	・注意喚起 ・ｳｨﾙｽの検体入手＆分析 ・標的型攻撃ﾒｰﾙ削除 ・開封者の有無確認 ・ｳｨﾙｽの特定＆特性分析（必要に応じて検体提供） ・情報流出の有無確認	・感染PCはｳｨﾙｽ除去出来ない限り、数日～2W程度利用不可 ・注意喚起案内稼働 ・ｳｨﾙｽ解析作業 ・ﾛｸﾞ解析作業

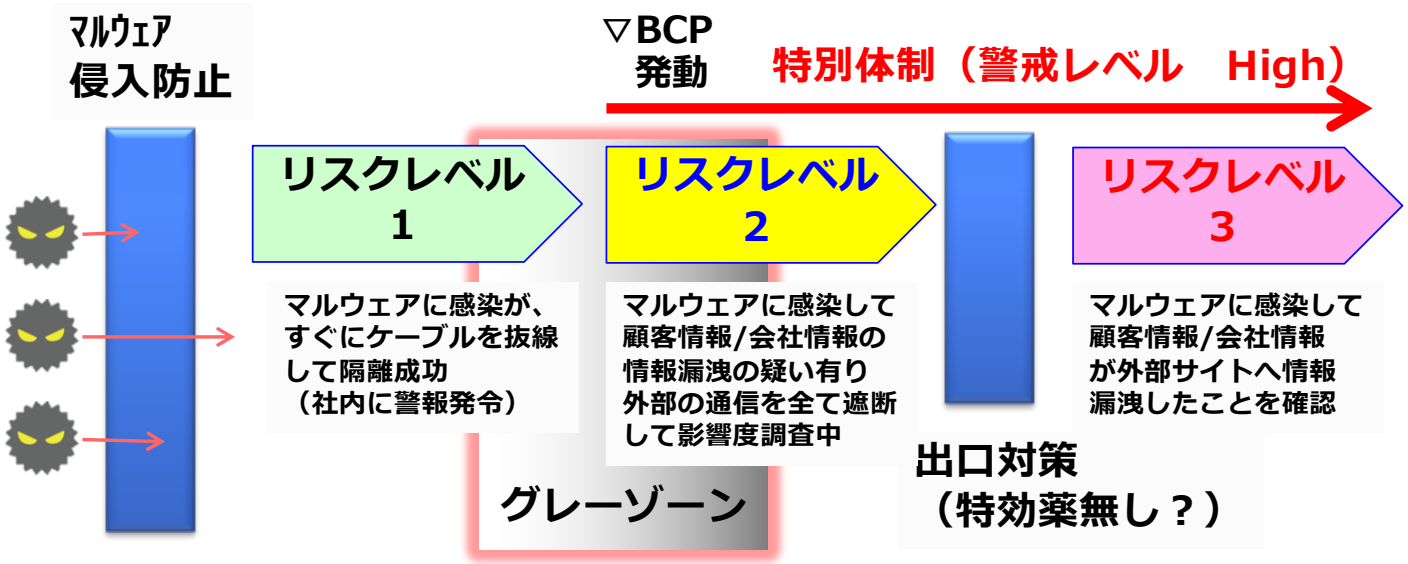
リスクレベル移行の判断ポイントと判断基準の策定

リスクレベル1からリスクレベル２への移行はグレーゾーンの領域で判断が難しいが、下記のような判断ポイントと判断基準を確立し、文書化することで緊急時にもタイムリーな判断がしやすくなる。

○判断ポイント
- ｻｲﾊﾞｰｾｷｭﾘﾃｨ事案BCP発動（ﾚﾍﾞﾙ1　→　ﾚﾍﾞﾙ2）
- 外部との通信全て全遮断
- IRTの立ち上げ

&

○判断基準
- 感染端末の数、増加傾向
- 社外への不正アクセスの確認or疑い



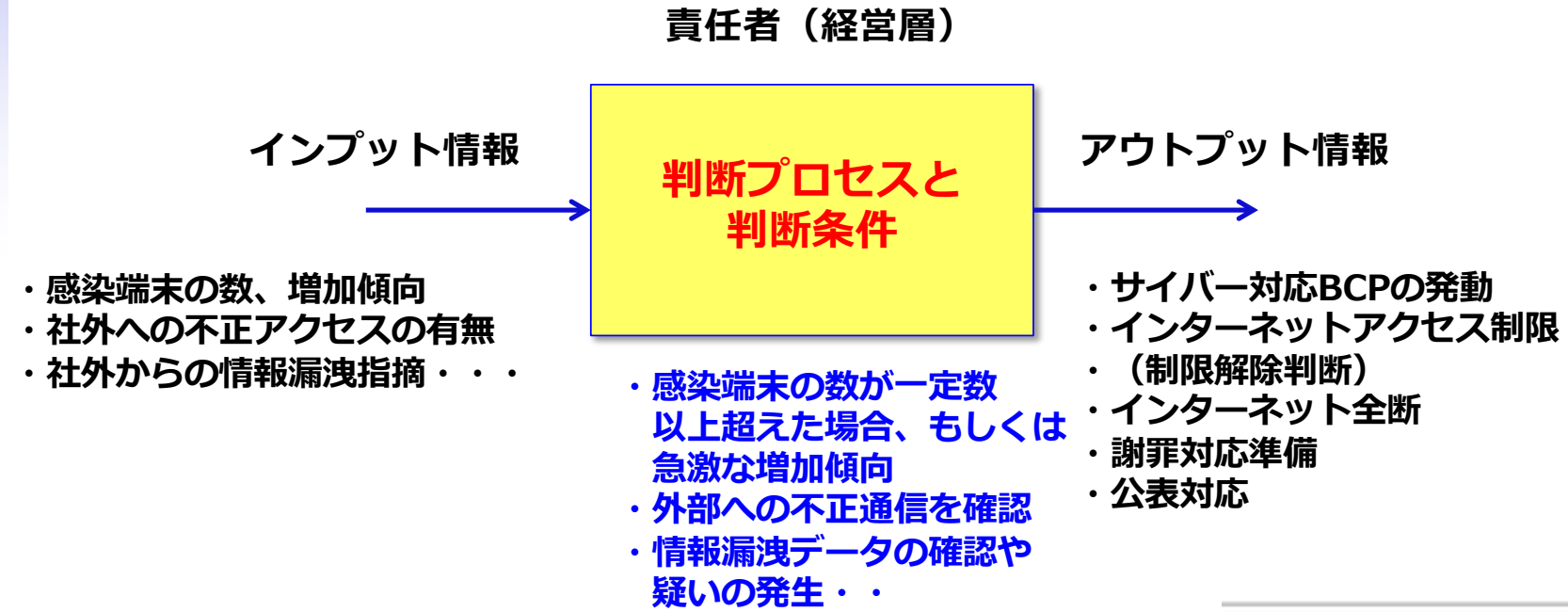
役割と責任の明確化

有事の際の判断が有効に働くためには下記の２点が重要

①役割と責任の明確化
②責任者にインプットする情報や判断プロセスの確立

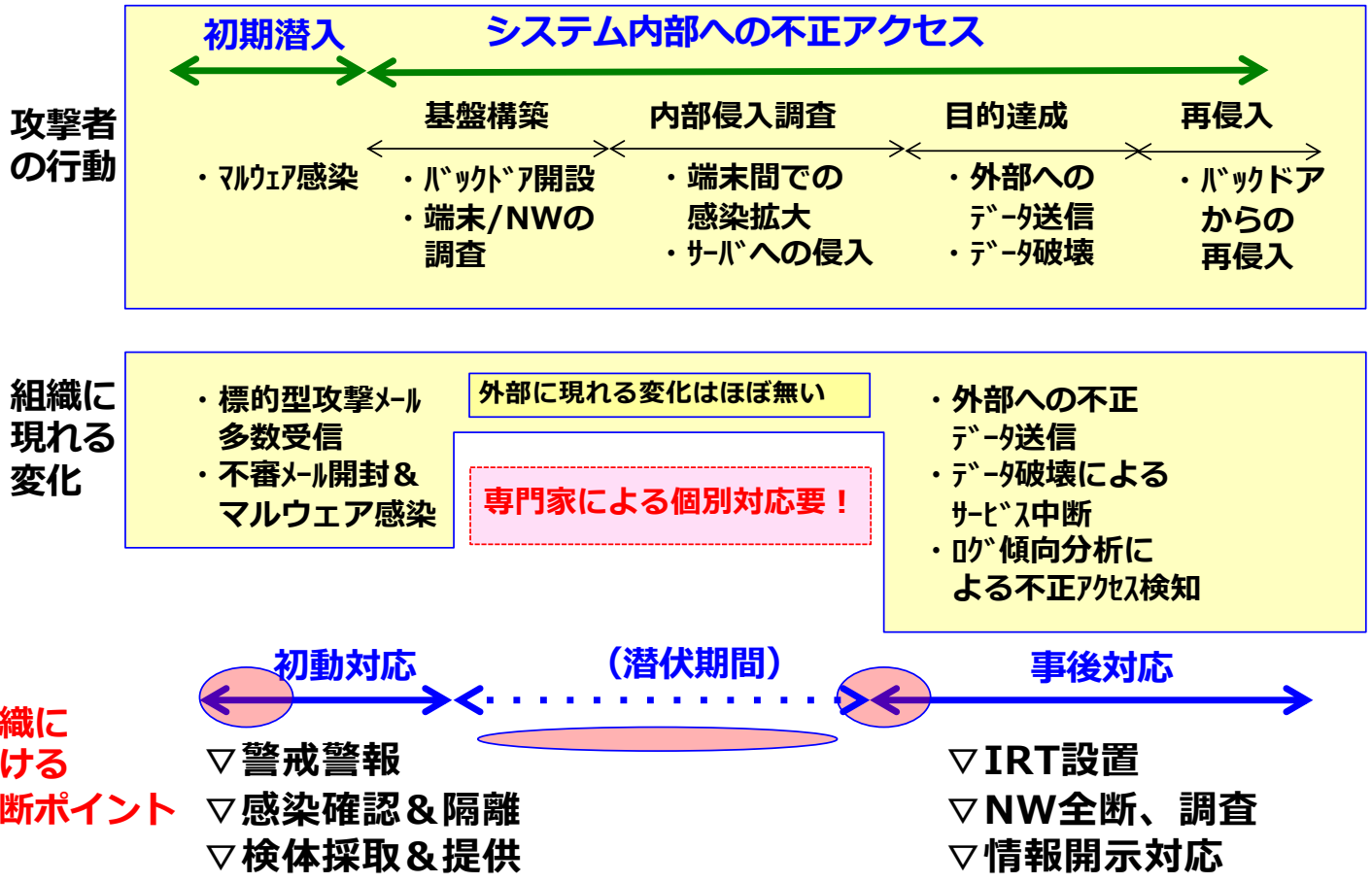
※：少ない情報で即断が求められる！（不在時の委譲含む）

※：通常のBCPと違い自らサービスを停止する判断が必要！



参考資料：　有事のマネジメント（判断基準＆プロセス）

○攻撃者の行動＆組織としての対応プロセス



ISMSとサイバーセキュリティとの関係についての考察

1. システム系とマネジメント系の管理策とのバランス

2. ISMSとサイバーセキュリティの相違点

→サイバーセキュリティは**外部との連携**が重要
→ISMSは**自組織**を守る

3. ISMS認証を取得済みの組織に最低限必要なCSIRT機能

→**ISMS＋α**

システム系の管理策と
マネジメント系の管理策
をバランスよく併用

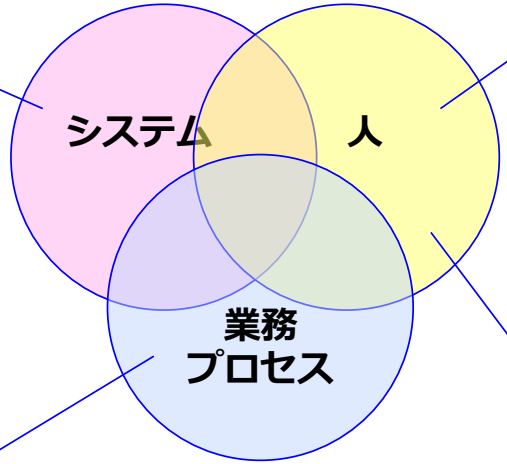
システム/業務プロセス/人から見た分析

従来の対策とサイバー特有の対策

・脆弱性情報の入手＆
システムの最新化徹底
・不審メールの排除
（フィルタリング）
・ウィルス対策ソフト
未登録のパターンには
効果ゼロ
・SandBoxによるふるまい
検知
・SIEMによるﾛｸﾞ傾向分析
・Proxy等の出口チェック

基本動作の徹底

・不審メールを開かない
・万が一開いたら、即ケーブル抜線＆報告
→研修＆意識付けが重要
但し、社員/派遣/請負
全てに徹底することは
難しい
0か1かの世界
（99%OKでも残り1%が大きなリスクとなる）



サイバー攻撃に強い業務プロセス

・インターネットから重要システムのデータを分離
（無法地帯と聖域の分離！）
・外部とのアクセスと内部プロセスの分離

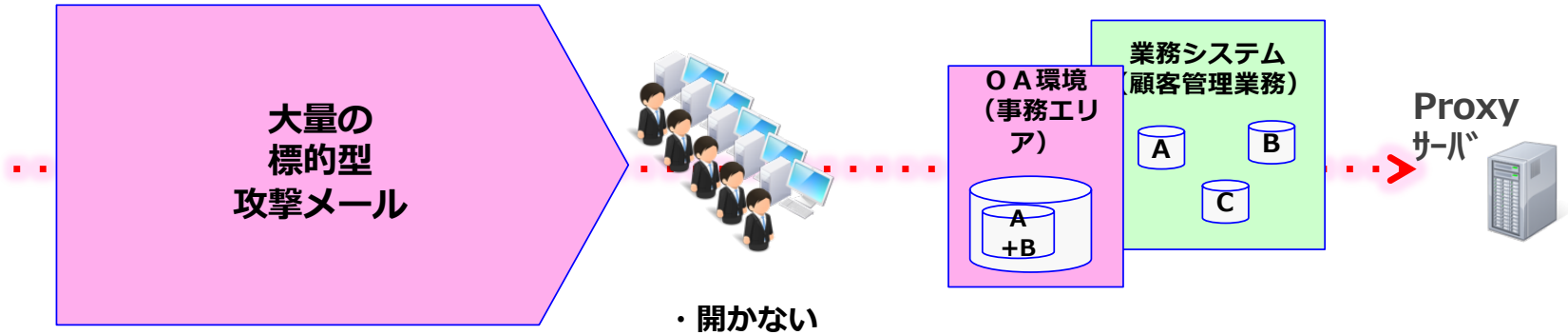
サイバー特有スキル

解析者
・検体の入手、分析手配
・ログ分析
・侵入検知・・・

仕事のやり方の見直し
そのためには情報資産＆業務プロセスの面から詳細リスクアセスメントが必要！

人とシステムとのコラボレーション

＜　連携プレイによる防御ライン　＞



メールの
ｽｸﾘｰﾆﾝｸﾞ

SandBox
振る舞い
検知

・開かない
・開いたらｹｰﾌﾞﾙ抜線＆
報告
・全体へ注意警報
・検体採取＆提供

ｼｽﾃﾑｱｯﾌﾟﾃﾞｰﾄ
（脆弱性対応）

ﾛｸﾞ分析等

・脆弱性を突いた
ｼｽﾃﾑへの侵入防止

・不正通信の
監視

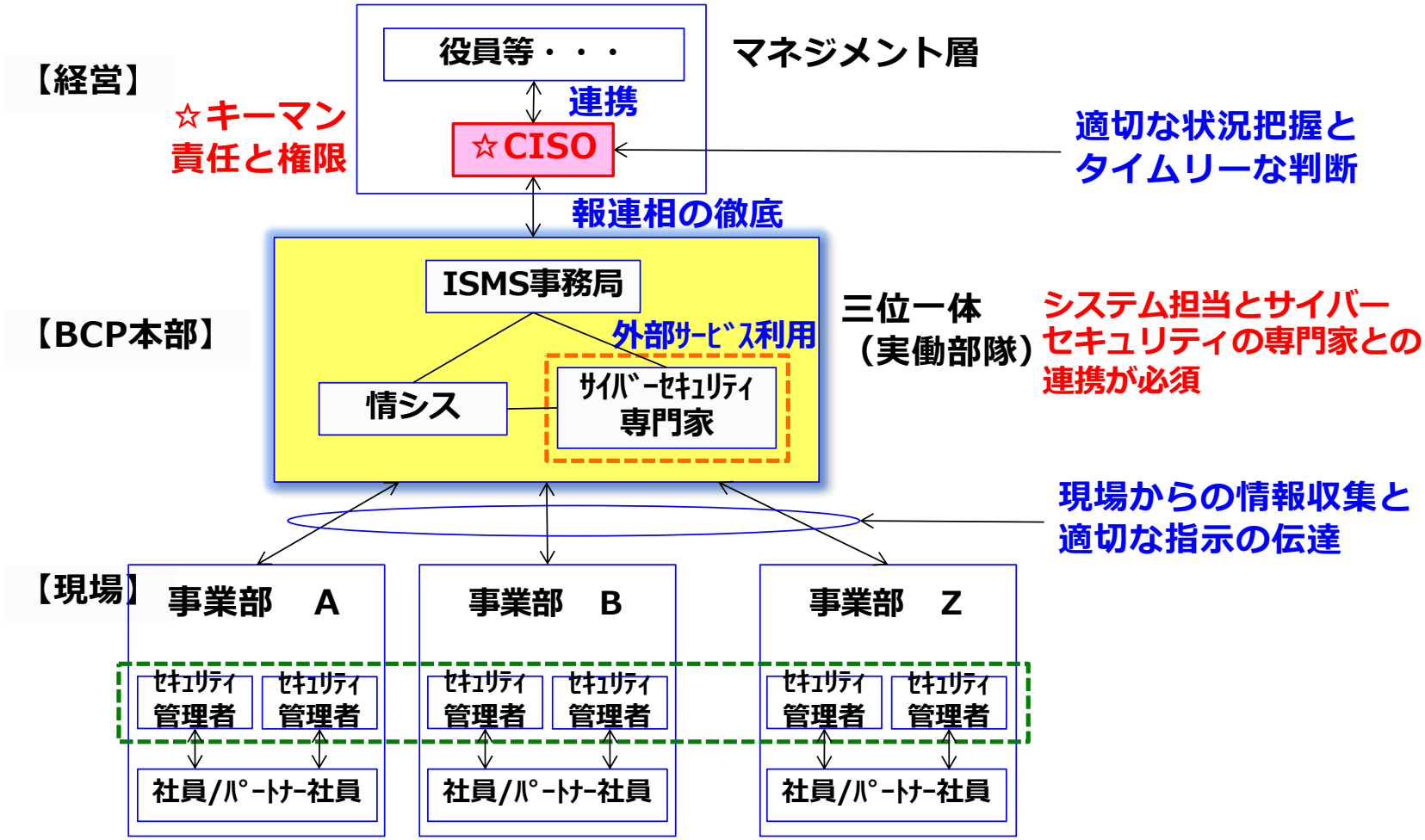
システムで支援

・OAｴﾘｱに機密ﾃﾞｰﾀを
放置しない
・ﾃﾞｰﾀの暗号化

人の意識

システムで支援

サイバーセキュリティ体制と役割（案）

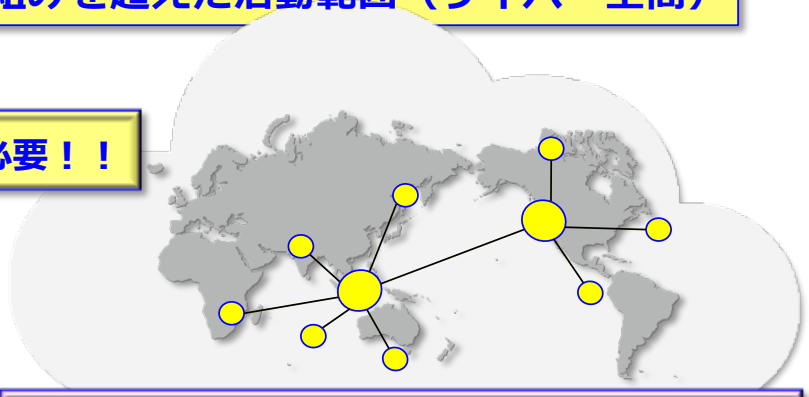


ISMSとサイバーセキュリティの相違点

ISMSの活動範囲とサイバー空間について

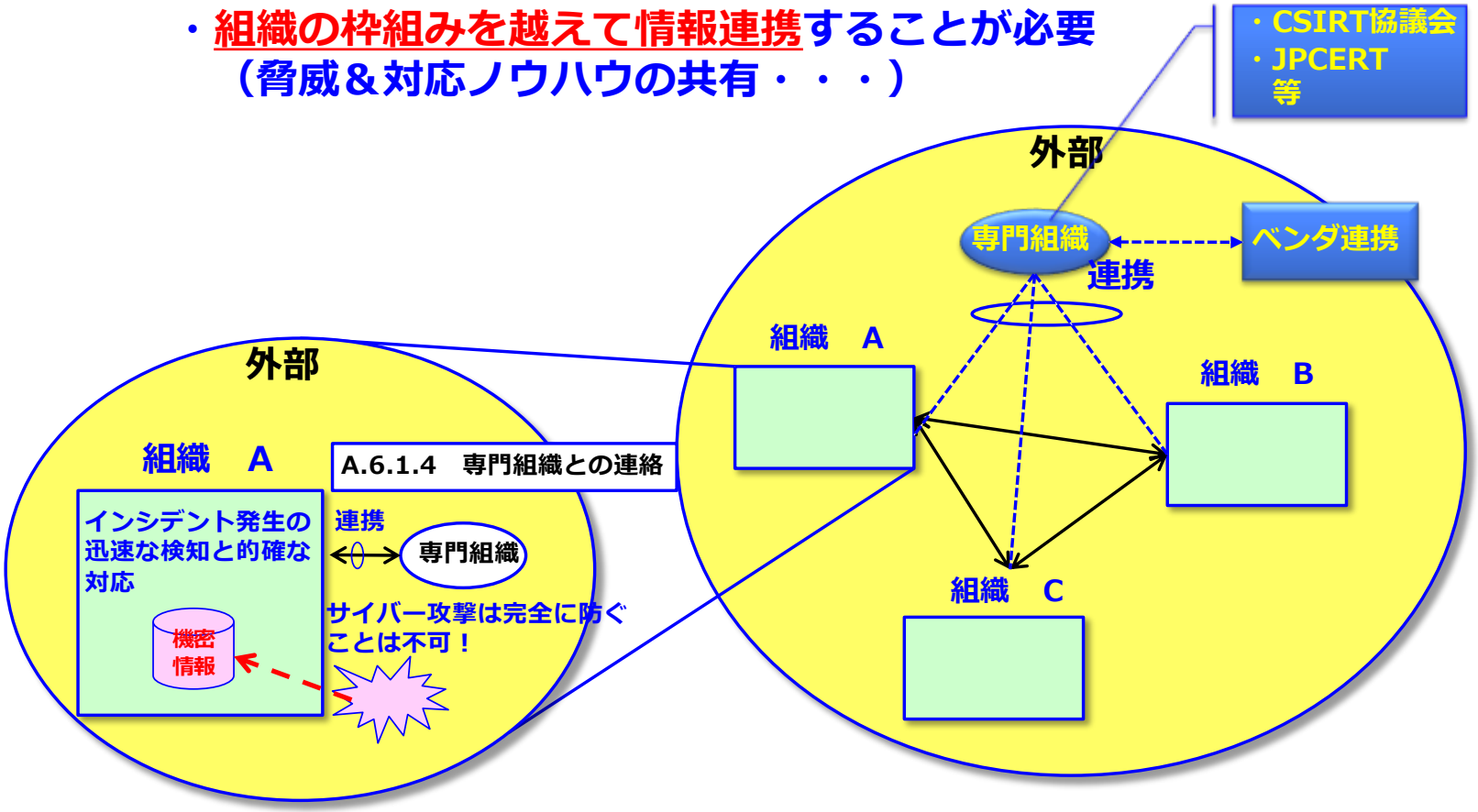
・ISMSは認証組織を中心とした活動範囲
・サイバー攻撃対応は組織の枠組みを超えた活動範囲（サイバー空間）

両者の違いを意識したリスク対応が必要！！



他組織との攻撃情報や攻撃対応情報の共有

・サイバー空間に境界線は無い！
・<u>組織の枠組みを越えて情報連携</u>することが必要
（脅威＆対応ノウハウの共有・・・）

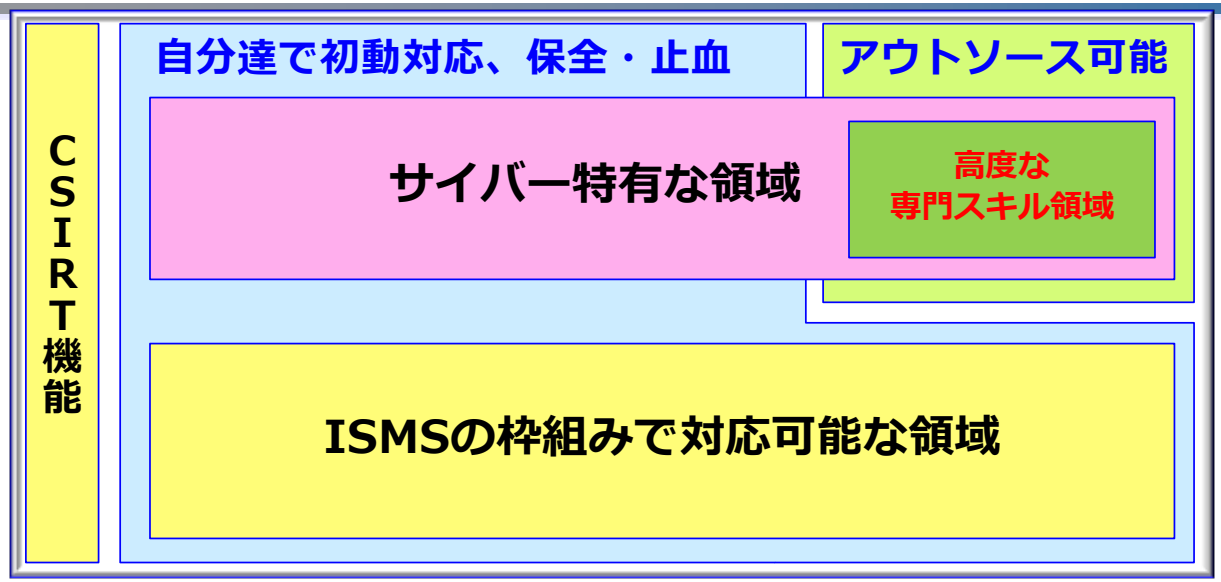


・<u>自組織内だけでなく他組織との攻撃情報や攻撃対応情報の共有</u>
（脆弱性情報の入手＆対応プロセス）

23

ISMS認証を取得済みの組織に
最低限必要なCSIRT機能を
　実装するためには・・・
　→ISMS＋α

ISMSの実装＋α（サイバー特有の視点を加味）



可視化

ISMSの実装で対応可能な領域
とサイバー特有の領域

具体的な
実装の
例示
（次頁～）

CSIRT機能	機能項目	対応管理策（1）	対応管理策（2）
インシデント事後対応の機能	・インシデントハンドリング ・コーディネーション ・コンピュータ・フォレンジックス　等	ISMSの枠組みで対応可能	サイバー特有の対応が必要 高度な専門スキルが必要
インシデント事前対応の機能(事前準備)	・セキュリティ関連情報提供 ・インシデント/セキュリティイベント検知 ・技術動向調査　等		
セキュリティ品質向上の機能（平時のとき）	・リスク評価分析 ・事業継続性、災害復旧計画作成・改変 ・セキュリティコンサルティング　等		

ISMSの実装＋α（サイバー特有の視点を加味）

具体的な実装の例示（次頁～）

CSIRT機能	機能項目	対応管理策（1）	対応管理策（2）
インシデント事後対応の機能	・インシデントハンドリング ・コーディネーション ・コンピュータ・フォレンジックス　等	ISMSの枠組みで対応可能	サイバー特有の対応が必要 高度な専門スキルが必要
インシデント事前対応の機能(事前準備)	・セキュリティ関連情報提供 ・インシデント/セキュリティイベント検知 ・技術動向調査　等		
セキュリティ品質向上の機能（平時のとき）	・リスク評価分析 ・事業継続性、災害復旧計画作成・改変 ・セキュリティコンサルティング等		

参考：ISMSの実装に加味するサイバー特有機能

機能	機能項目	ISMSの枠組みで対応可能	サイバー特有な対応（＋α）
インシデント事後対応	インシデントハンドリング	発生したインシデントへの 対応を行い、被害局小化・復旧のための活動 ・インシデントハンドリングの手順策定＆実施 ・トリアージ基準（合否判定、対応優先度） ・解決時に実施した手順等のエビデンス保存 ・情報共有や管理ツールの環境維持 ・再発防止手順	概ねISMSの枠組みで対応可能だが、下記の項目はサイバー特有の観点での補足が必要 ・インシデントハンドリングの手順策定＆実施 ・トリアージ基準（合否判定、対応優先度）
	コーディネーション	組織を跨ったインシデント対応はISMSの枠組みでも発生するが、それぞれの責任でインシデントハンドリングを行うのはサイバー特有。	複数の組織（社内外）にて、それぞれの責任の下でインシデ ントハンドリングを行うことが必要となってくる場合があり、一貫した効果的なインシデントハンドリングを行うためには、CSIRT がインシデン ト全体を把握したコーディネータの役割を果たす必要がある。
	コンピュータ・フォレンジックス	ISMSの実装にサイバー特有機能加味する事例	インシデントが発生したコンピュータから、証拠となりうるデータを保存し、インシデントハンドリングを行う。 高い専門性が要求され、専用ツールの準備が必要。 ①どのような被害を受けたか ②どこから侵入を受けたか ③誰が侵入者か
	オンサイトインシデントレスポンス		インシデントが発生したシステムやネットワークに対して、CSIRTが直接復旧作業を行う。（システムの運用担当者との責任分解点設定）
	インシデントレスポンスサポート	CSIRT がメール・電話・ドキュメントの提供等を行うことによるインシデントハンドリングを行う。	
	アーティファクトハンドリング		インシデントハンドリング時に発見された不審なプログラムを解析するサービス。不審なプログラムのソースコードの解析や、隔離した環境でのプログラムの挙動解析を実施し、不審なプログラムがインシデントの原因であるかどうかの調査を行う。専門のスキルを持ったメ ンバのCSIRTへの配置や、他のNWから隔離されたアーティファクトハンドリング専用の設備が必要。

注：各組織の状況によりISMSの実装レベルが異なることから標準的な参考例として提示

参考：ISMSの実装に加味するサイバー特有機能

機能	機能項目	ISMSの枠組みで対応可能	サイバー特有な対応（+α）
インシデント事前対応の機能(事前準備)	セキュリティ関連情報提供	セキュリティ情報をサービス対象に情報提供するサービスである。 提供する情報を以下に例示する。 - CSIRT の活動内容周知/連絡先周知 - ポリシー/プロシージャ/セキュリティ関連のチェックリスト - 流行しているウイルス/ワーム情報や攻撃手法 - インシデントレスポンスの一般的手法 - インシデント統計情報	通常の事務局対応作業のプロシージャにサイバー対応の情報を盛り込んで発信を行う
	脆弱性情報ハンドリング	ISMSの枠組みで実施することも可。	SW/HWの利用状況を把握し、関連する脆弱性情報を分析し、入手サービス対象へ伝達する ・情報先の管理と適切な情報提供 ・対処要否の判断、対応手順の策定、実施
	インシデント/セキュリティイベント検		インシデント/セキュリティイベントなどを検知するサービス。 検知方法は、IDS やハニーポット の設置、各種サーバ群のログの解析、P2P ファイル共有アプリケーションを経由した情報漏えい検知のための専用環境等がある。
	技術動向調査	セキュリティ向上のための技術やインシデント検知技術、もしくは侵 入技術等の最新のセキュリティ技術動向調査や目利きを実施し、サービス対象への有用性を確認するサービス。	通常事務局対応作業の延長でサイバー特有の技術動向を盛り込む。
	セキュリティ監査/査定		ドキュメントの確認やペネトレーションテストを通じて、監査/査定 するサービスである。
	セキュリティツールの開発		CSIRTやサービス対象が利用するセキュリティツールを開発するサービス。 例：新しいインシデント検知ツールや、 暗号化技術を容易に利用することのできるスクリプトや、自動化さ れたパッチ配信の開発など

ISMSの実装に
サイバー特有機能
加味する事例

注：各組織の状況によりISMSの実装レベルが異なることから標準的な参考例として提示

参考：ISMSの実装に加味するサイバー特有機能

機能	機能項目	ISMSの枠組みで対応可能	サイバー特有な対応（＋α）
セキュリティ品質向上の機能（平時）	リスク評価分析	企業や対象となる情報システムの機密性、完全性、可用性を阻害 する様々なリスクを洗い出し、その影響度を分析するサービス。（現状のリスクの認識と、リスクを受容範囲にメネジメントする） ・情報資産の洗いだし、リスク分析手順の策定 ・リスク分析結果に基づく是正対応	サイバー特有な項目の盛り込み
	事業継続性、災害復旧計画作成・改変	通常のBCPに加えてCSIRTとしてのインシデントレスポンス機能を事業継続性、災害復旧計画として反映させるサービス。	サイバー特有の特徴として、外部への情報漏洩の疑いがある場合は自らNWの遮断等を実施することで、被害拡大を防ぐ判断が必要となること。 ・BCPにサイバー対応計画を反映 ・フィージビリティの確認の演習の実施
	セキュリティコンサルティング		CSIRT としてのノウハウをサービス対象の事業へ反映させるための コンサルティングを行うサービス。 ・情報システムの企画設計、運用中のシステムに対するセキュリティ相談窓口の設置＆実施 ・知見の体系化＆蓄積（文書化含む）
	セキュリティ教育/トレーニング/啓発活動	CSIRTでのノウハウや、そのノウハウを反映させたポリシー・プロシージャ等をサービ ス対象に教育やトレーニング、啓発活動を行うサービス。 ・社員/P社員にセキュリティ啓発/教育計画を策定し、実施	・通常の事務局の営みで実施するセキュリティ研修に加えて、サイバー対応の項目の盛込み
	製品評価・認定		製品・ツール・プロダクト・サービス等に関して、それらをサービス対 象がセキュアに利用できるものかどうかをCSIRT が評価・認定するサ ービス。

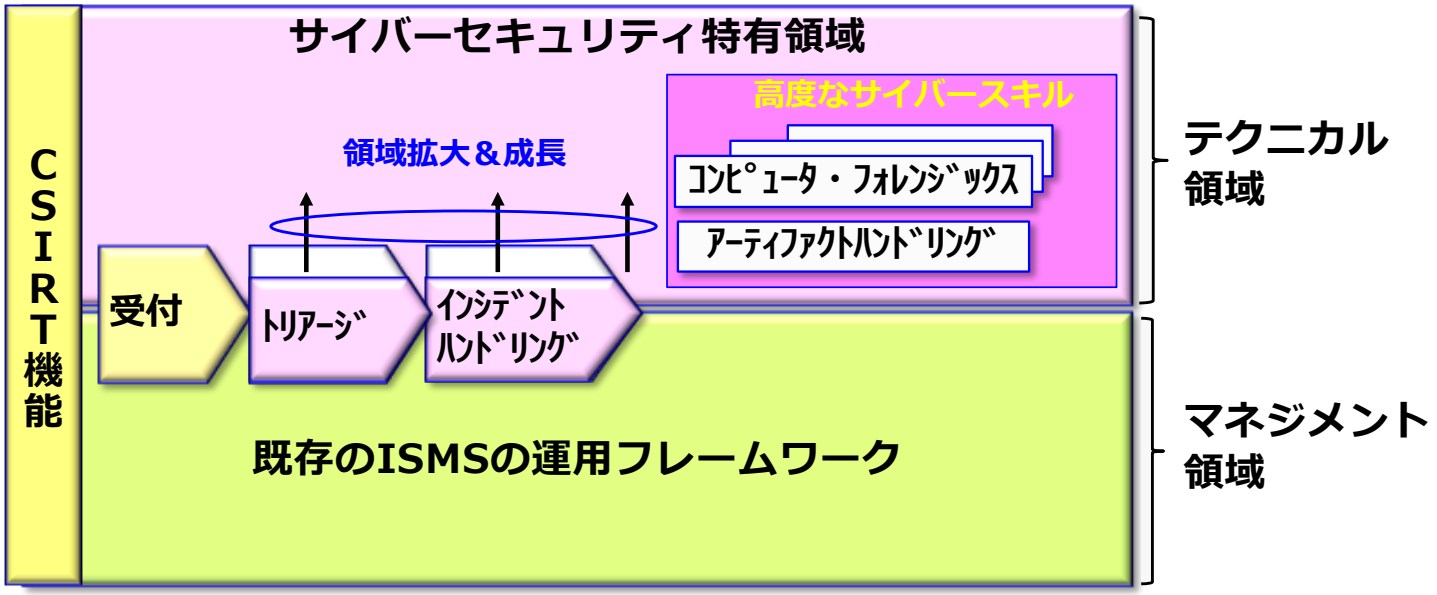
ISMSの実装にサイバー特有機能加味する事例

注：各組織の状況によりISMSの実装レベルが異なることから標準的な参考例として提示

CSIRT機能導入におけるSTEP論（スモールスタート）

STEP1：まずは入り口となる受付機能から始める
STEP2：基本的な機能の実装　(ﾄﾘｱｰｼﾞ、ｲﾝｼﾃﾞﾝﾄﾊﾝﾄﾞﾘﾝｸﾞ等)
STEP3：サイバー対応スキルUPを図りながら、組織に必要な対応領域を拡大

- 無理をせず、身の丈にあった実装を！
- ISMS構築＆運用＋α（サイバー特有のもの）を追加実装
- フォレンジックス等の高度なサーバースキルはアウトソーシングを視野に！



協調

ISMS  CSIRT

出来ないことを探すより、出来ることから少しずつ始めるサイバーセキュリティ対策