東京都

令和６年度
中小企業サイバーセキュリティ
特別支援事業説明会

～セキュリティ事故発生に備えた体制整備を支援します～

本日の内容

第１部　セキュリティセミナー

『インシデント被害を最小化！
中小企業向けインシデント対応力の強化』

第２部　事業説明

**『中小企業サイバーセキュリティ
特別支援について』**

東京都関連事業について

セキュリティ成熟度の各段階に応じたメニューを通じて網羅的に支援

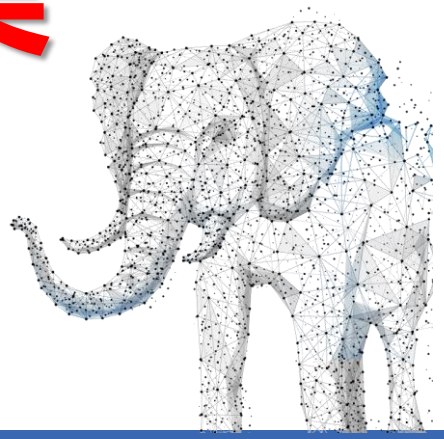
成熟度レベル１	成熟度レベル２	成熟度レベル３	成熟度レベル３以降
普及啓発	**機器規程整備**	**社内体制整備**	**インシデント対応力強化**
中小企業サイバーセキュリティ **啓発事業**	中小企業サイバーセキュリティ **基本対策事業**	中小企業サイバーセキュリティ **社内体制整備事業**	中小企業サイバーセキュリティ **特別支援事業**
セキュリティ対策をこれから検討する中小企業へサイバー攻撃対応演習セミナー、標的型攻撃メール訓練、ネットワーク調査を通して必要性を認知する支援を行います。	セキュリティ対策をこれから始める中小企業に対し、機器の導入や規定策定など一歩目を踏み出す支援を行います。	セキュリティ対策の自走を目指す中小企業を対象に、継続的なセキュリティ対策ができる人材を育成します。	サイバー攻撃を受けたときの的確な対応方法や事業の復旧までを考慮した、セキュリティ対策を支援します。 **対策が進んだ企業への追加サポート**

東京都関連事業WEBサイト

成熟度レベル１ 啓発事業	https://keihatsu.metro.tokyo.lg.jp/	
成熟度レベル２ 基本対策事業	https://kihontaisaku.metro.tokyo.lg.jp/	
成熟度レベル３ 社内体制整備事業	https://shanaitaisei.metro.tokyo.lg.jp/	

中小企業サイバーセキュリティ特別支援事業とは

インシデント対応体制整備事業



支援内容

企業の状況に応じて、
どちらかのコースを選択

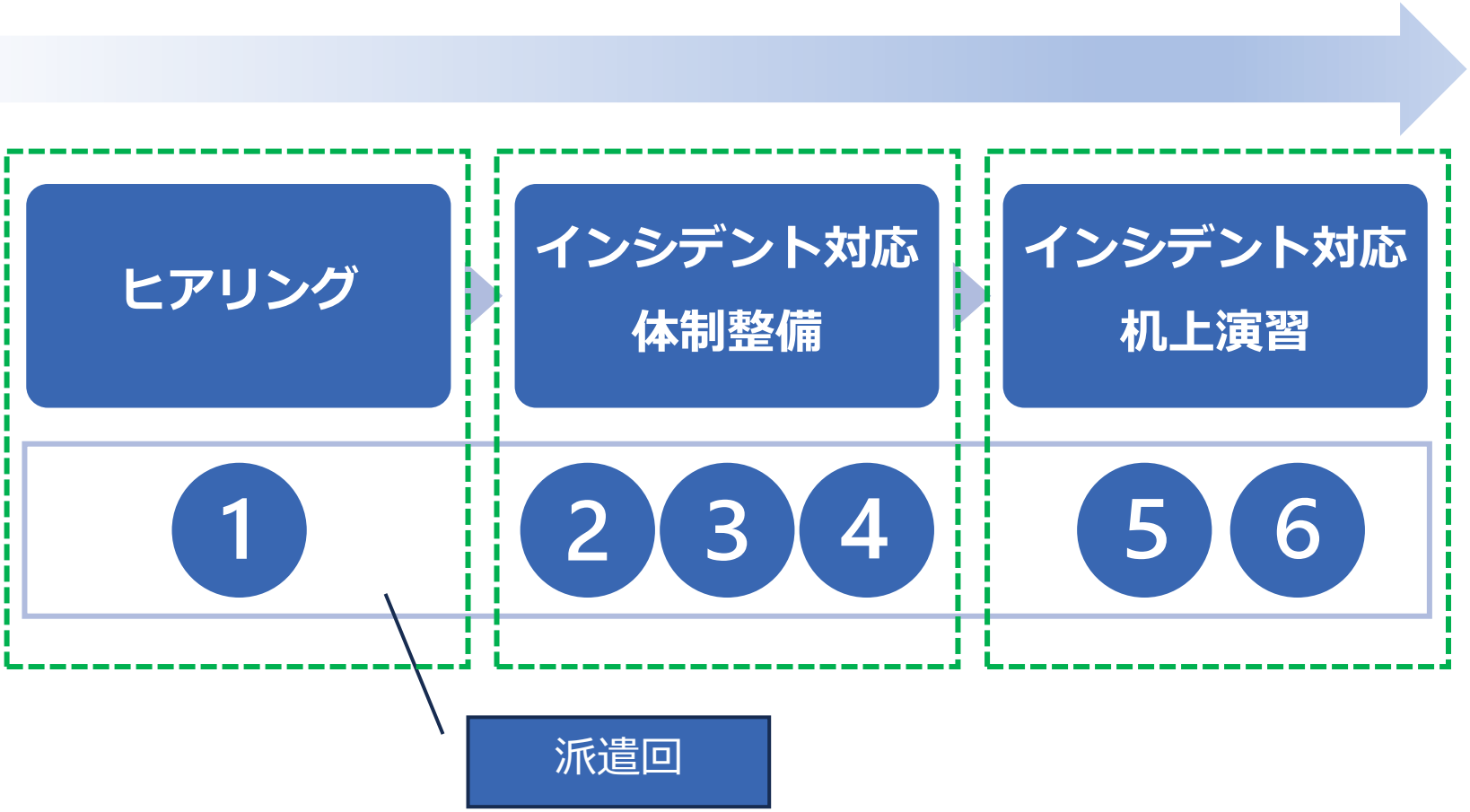
IT-BCP 策定コース

ITシステムに対する事業継続、早期復旧活動の計画策定（組織ルールの整備）

CSIRT 構築コース

サイバー攻撃に対応する検知と対応方法の確立（実施手順の整備）

支援の流れ



ヒアリング

● IT環境

- 組織のIT環境の概要
- 主要なビジネスプロセスとそれに依存するITシステム
- 過去のランサムウェアやフィッシング攻撃の経験（あれば）

● 現在の予防策

- 技術的対策：セキュリティ対策、パスワードポリシー、アクセス権設定、バックアップの取得
- 組織的対策：ポリシー、手順書、見直し
- 人的対策：教育、教育の繰り返し、効果測定
- 物理的対策：サーバの所在（オンプレ環境の場合）、施錠管理

● リスク管理

- ランサムウェアやフィッシング攻撃のリスク評価
- 攻撃の可能性とその影響度
- 脆弱性の特定

● ビジネス影響評価

- 各ビジネスプロセスに対するランサムウェアやフィッシング攻撃の影響
- 影響の程度（高、中、低）
- 復旧時間目標（RTO）とデータ復旧点目標（RPO）

ヒアリング

● 既存のインシデントに関する検討

- 過去のランサムウェアやフィッシング攻撃の経験（あれば）

● インシデントハンドリングに必要な情報の所在に関する検討

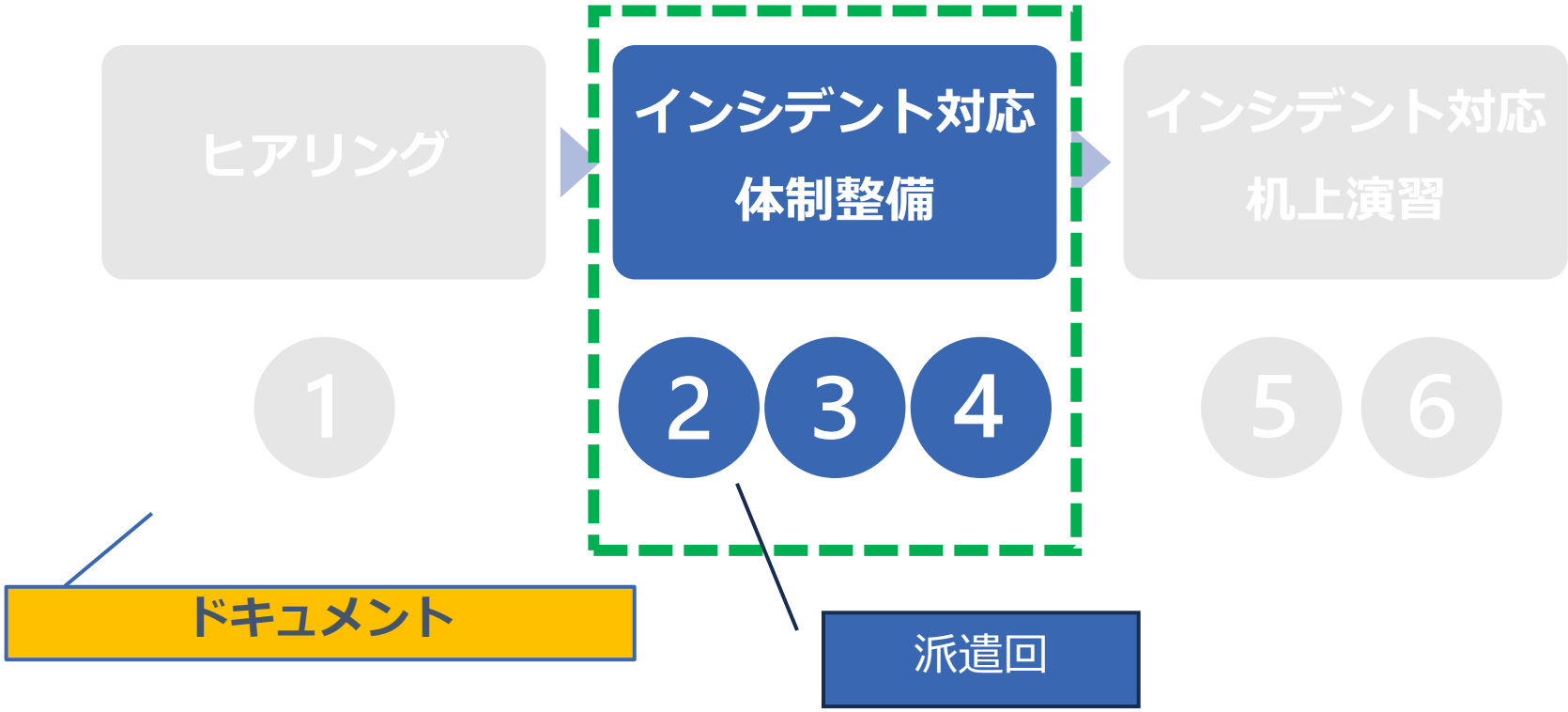
<ヒアリング>

- 経営層、IT 部門、法務部門、人事部門、広報部門
- 物理セキュリティを担当する部門
- 既存のセキュリティチーム
- 監査部門およびリスクマネージメントの専門家
- サービス対象の代表者
- 外部（組織外およびサービス対象外）の利害関係者
- その他の利害関係者

<文書確認>

- 事業や特有の事業機能のための組織図
- 組織またはサービス対象のシステムとネットワークの形態
- 重要なシステムと資産目録
- 既存の災害復旧計画と事業継続計画
- 既存の物理セキュリティ侵害を対策する組織への通知に関するガイドライン
- 既存のインシデント対応計画
- 親組織等の規則
- 既存のセキュリティポリシーと手順

支援の流れ



インシデント対応体制整備 ①

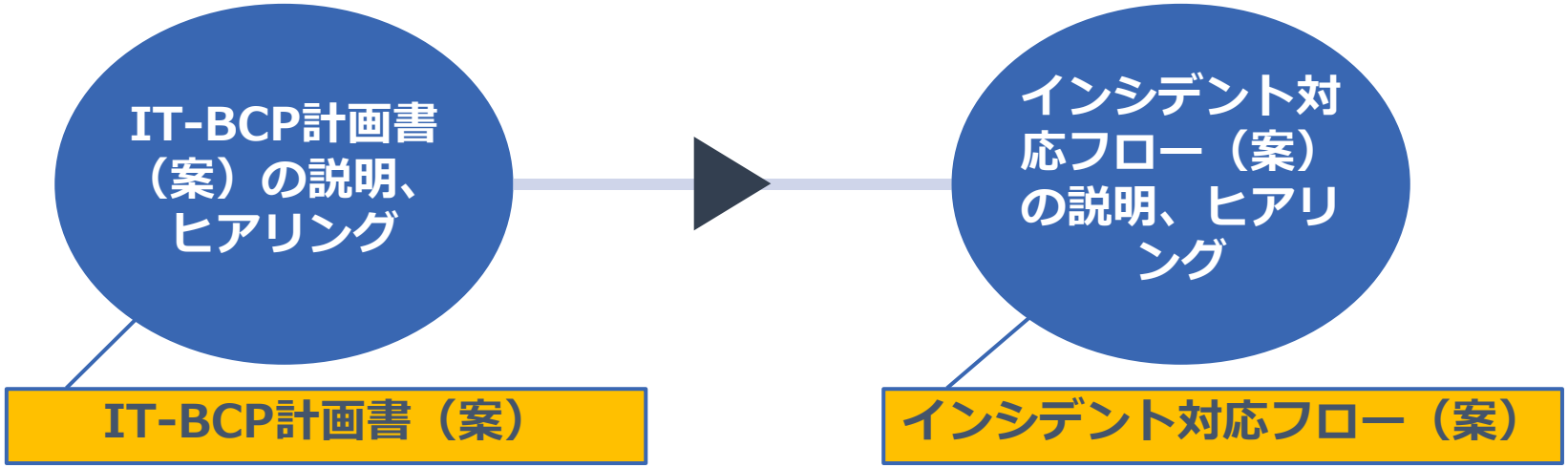
ヒアリング結果
フィードバック

策定にあたっての検討事項の説明、ヒアリング

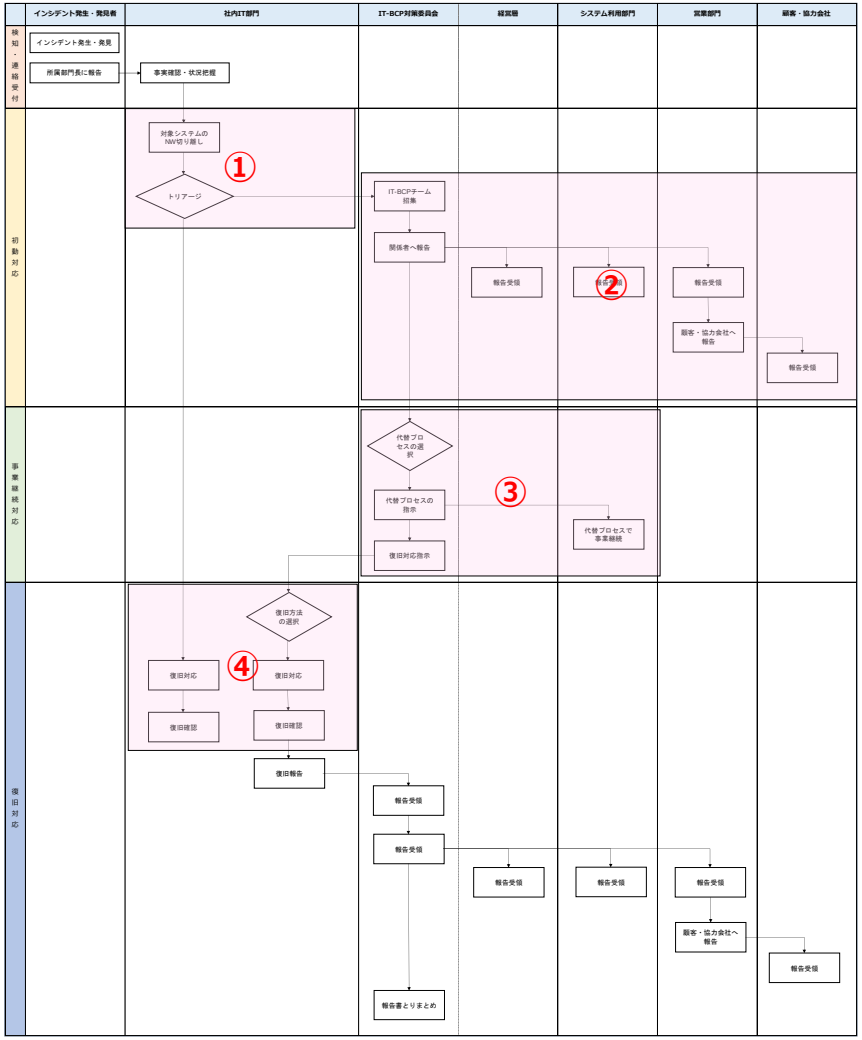
ヒアリングシート結果報告書（事業影響分析など）

- システム停止系対策か情報漏えい系対策か
- 復旧時間目標（RTO）と復旧ポイント目標（RPO）
- 復旧の優先順位

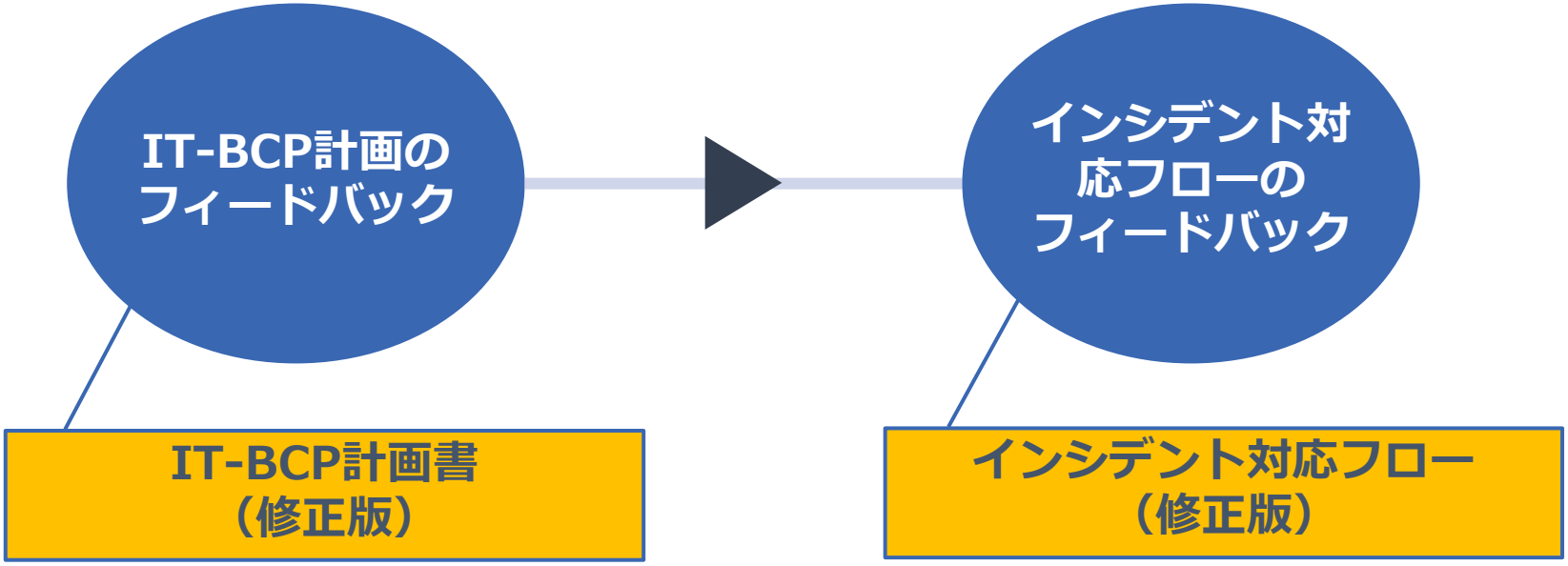
インシデント対応体制整備 ②



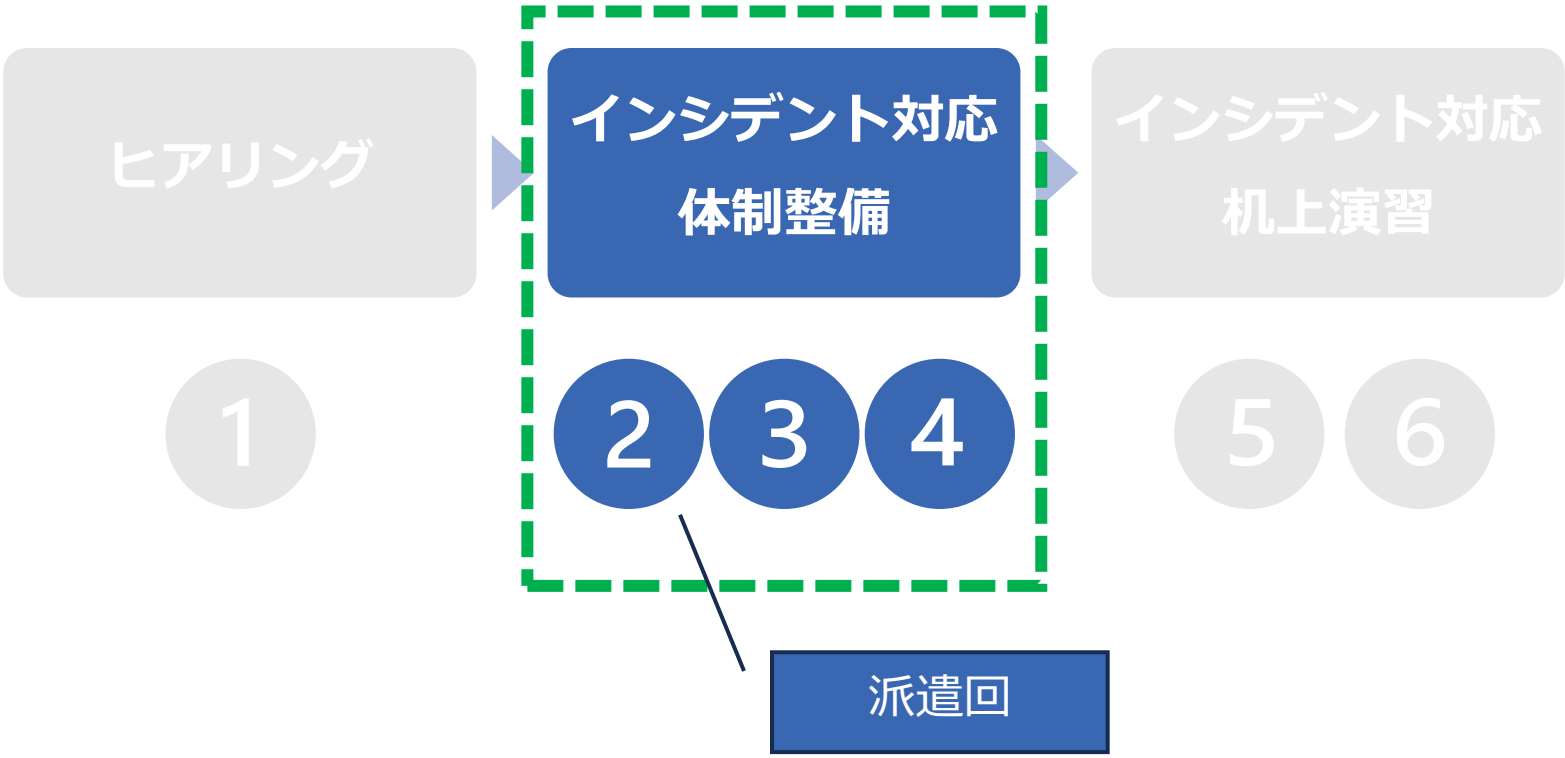
インシデント対応フロー（案）



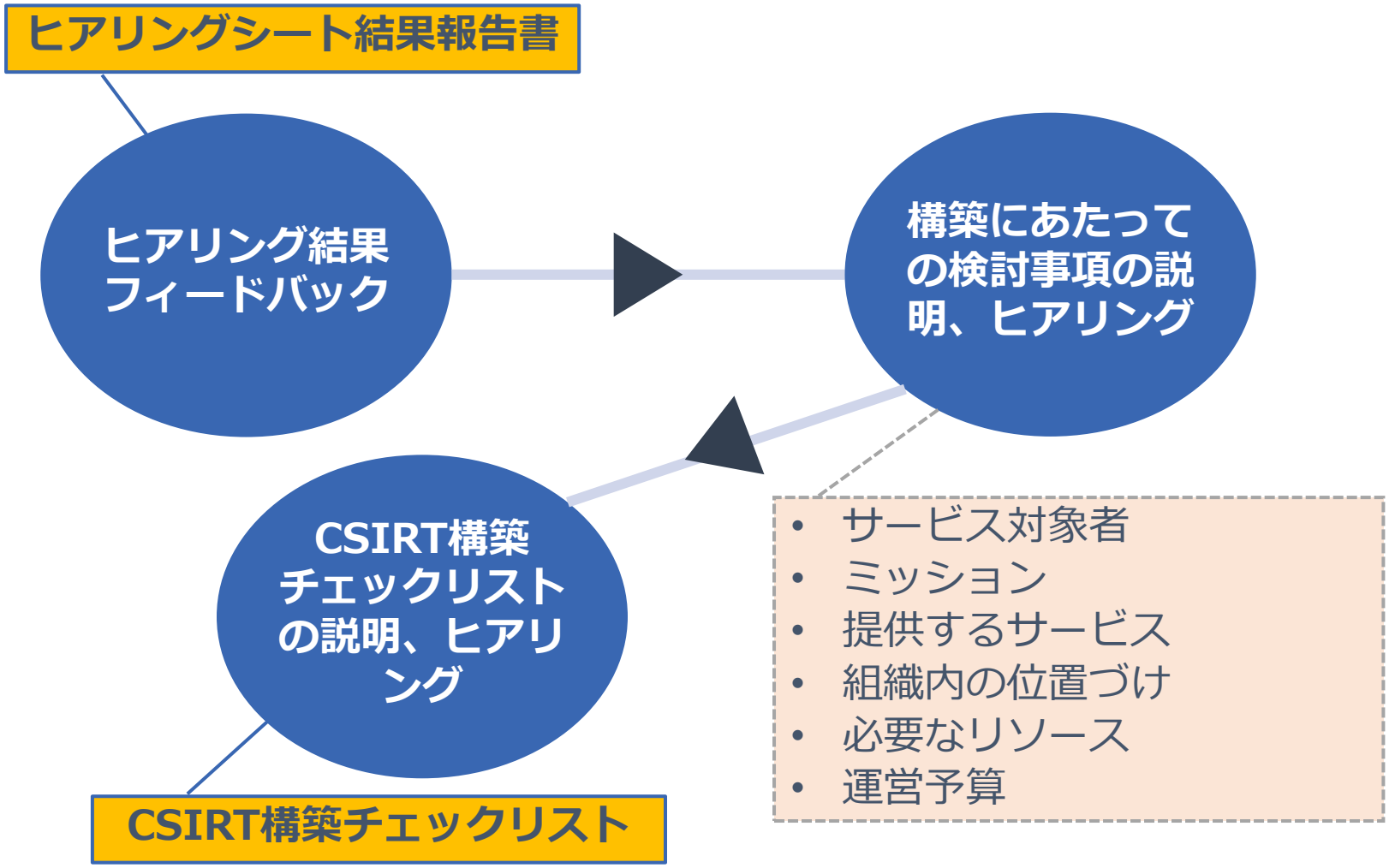
インシデント対応体制整備 ③



支援の流れ



インシデント対応体制整備 ①



CSIRT 構築チェックリスト（例）

大項目	中項目		内容	構築前（検討内容）
提供サービス			**CSIRTが管轄する主なサービス**	
	関連部門		各部門においてCSIRTとどのような連携を求められるか	
		経営層/意思決定層	CSIRT構築の承認による、資金やリソースの確保や、CSIRTに必要な責務と権限の社内の体制への反映。また、インシデントの最終報告先	
		情報システムの主幹・運用部門	サービス対象に位置付けられることもあり、インシデントハンドリング機能を持っている場合もある	
		内部統制部門	インシデントレスポンスと内部統制的活動との連携	
		法務部門	インシデントレスポンスにおける法的対応	
		広報部門	インシデントレスポンスにおけるマスコミ対応	
		人事部門	CSIRTのスタッフの配置・雇用。インシデント発生元の人事的処置実施	
		人材開発部門	セキュリティのノウハウやポリシーをサービス対象に教育やトレーニング、啓発活動を行う	
		経営企画部門	事業継続性計画・災害復旧計画とインシデントレスポンスの反映	
		ヘルプデスク	インシデントへの対応時の一次窓口	
		物理セキュリティ部門	物品(特にPC)の盗難。入退出制限の管理・実施	
CSIRT基本構想の定義			**CSIRTをどういった組織にするかを決める**	
	サービス対象の定義		サービス対象を決める	
	ミッションの定義		CSIRT構築のミッションを決める	
	取り扱うインシデントの定義とインシデント分類		何をもってインシデントの種類を特定するのか、またその分類	
サービスの検討			**CSIRTが管轄する主なサービスを検討**	
	インシデント事後対応サービス		インシデントの被害局限化を目的とした、インシデントハンドリング	
	インシデント事前対応サービス		インシデントの発生抑制を目的とした、インシデント検知や、発生の可能性を減少させるためのサービス	
	セキュリティ品質向上サービス		セキュリティ品質を向上させ、間接的にインシデントの発生抑制をする	
社内体制の検討			**CSIRT構築にあたり、社内の体制をどうしていくかの検討**	
	CSIRTモデル		様々なモデルから、会社にあっているモデルを選ぶ	
	対応範囲		CSIRTで対応する範囲を決める	
社外連携の検討			**社外組織との連携検討**	
	外部CSIRTとの連携		外部CSIRTとの連携を検討	
	外部組織との連携		外部組織との連携を検討	
リソースの検討			**CSIRT構築に必要なリソースの検討**	
	人的リソースの検討		必要な人員の割り当てを検討	
	細分化した役割		詳細な役割を検討	
	設備的リソースの検討		CSIRT構築に必要な設備の確認	
	予算		CSIRTの構築にどれくらいの予算がいるか検討	

【参考】日本シーサート協議会「CSIRTスタータキット」https://www.nca.gr.jp/imgs/CSIRTstarterkit.pdf

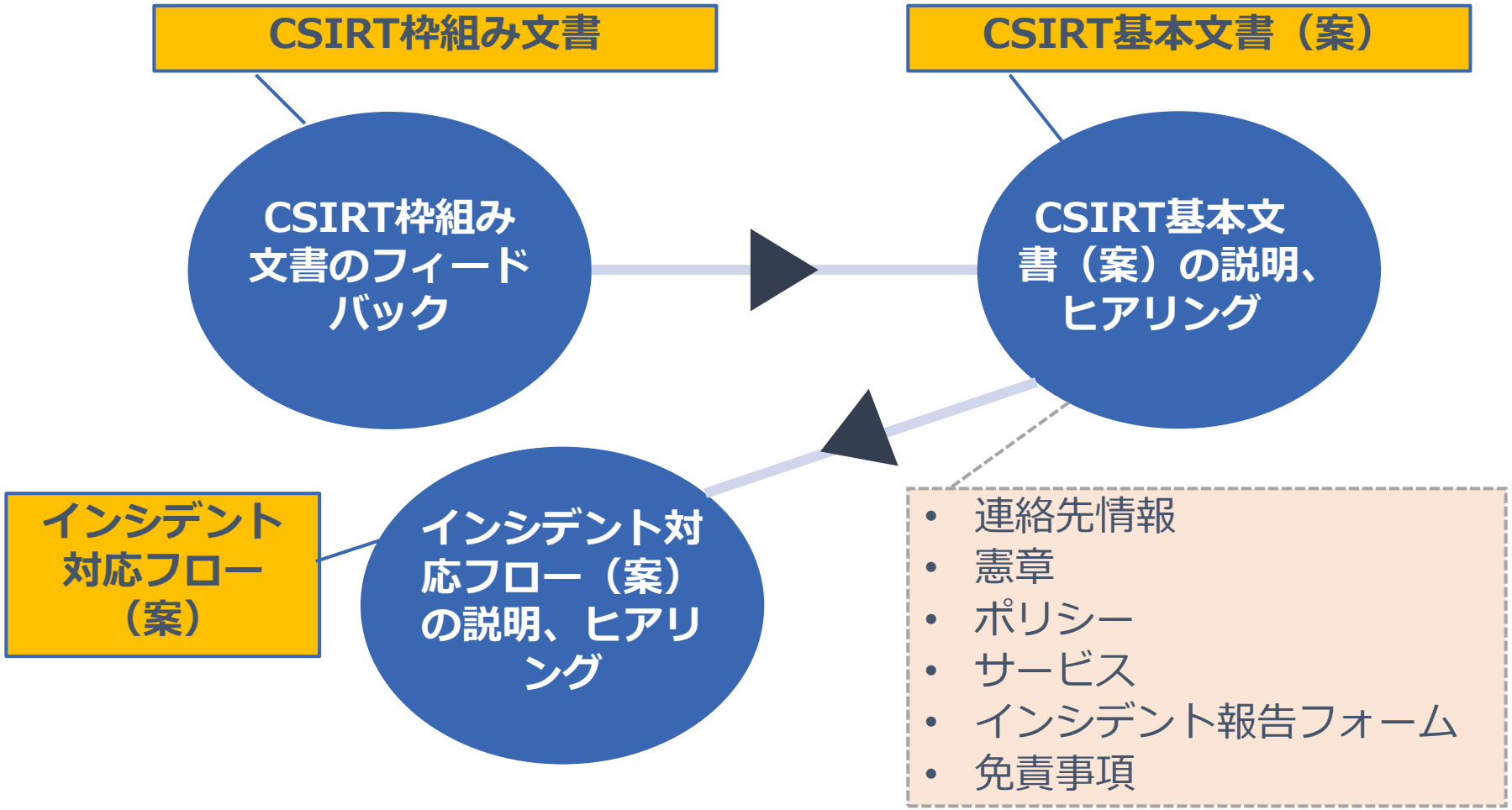
CSIRTのサービス

本事業の支援

インシデント事後対応サービス	インシデント事前対応サービス	セキュリティ品質向上サービス
インシデントの被害局限化を目的とした、インシデントハンドリング	インシデントの発生抑制を目的とした、インシデントやセキュリティイベントの検知や、発生の可能性を減少させるためのサービス	社内セキュリティの品質を向上させることを目的としたサービス

【出典】日本シーサート協議会CSIRT スタータキット　https://www.nca.gr.jp/imgs/CSIRTstarterkit.pdf

インシデント対応体制整備 ②



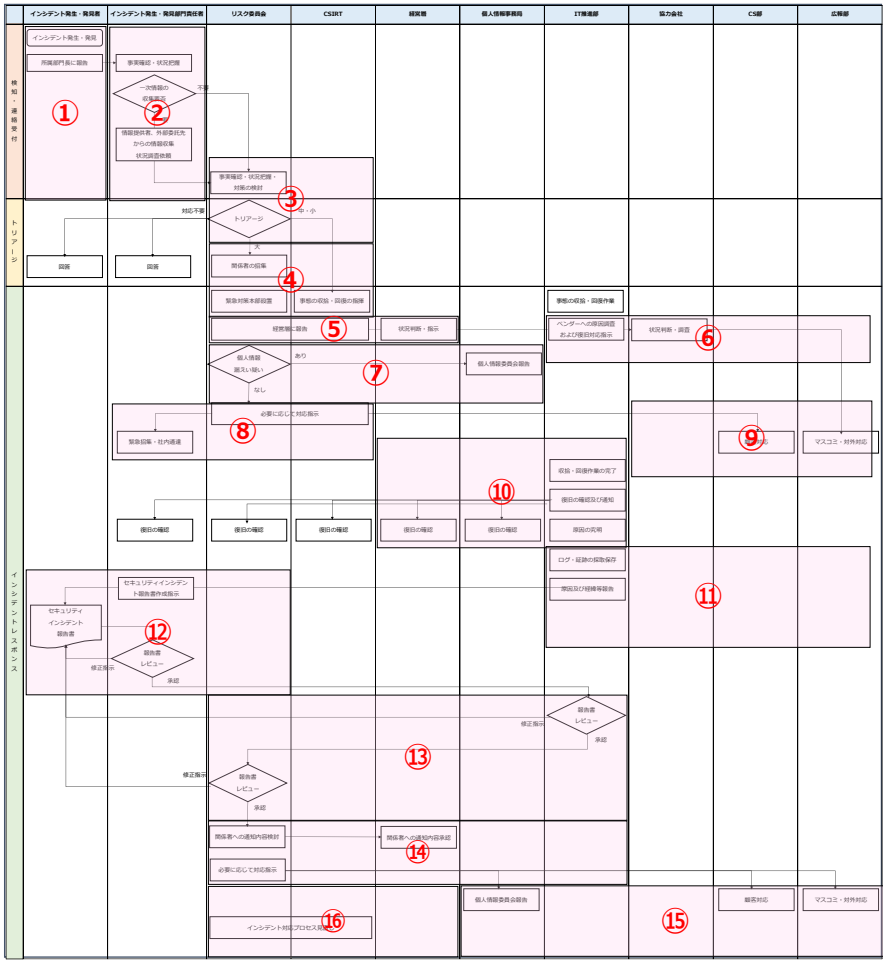
CSIRT 基本文書

以下の内容を定める

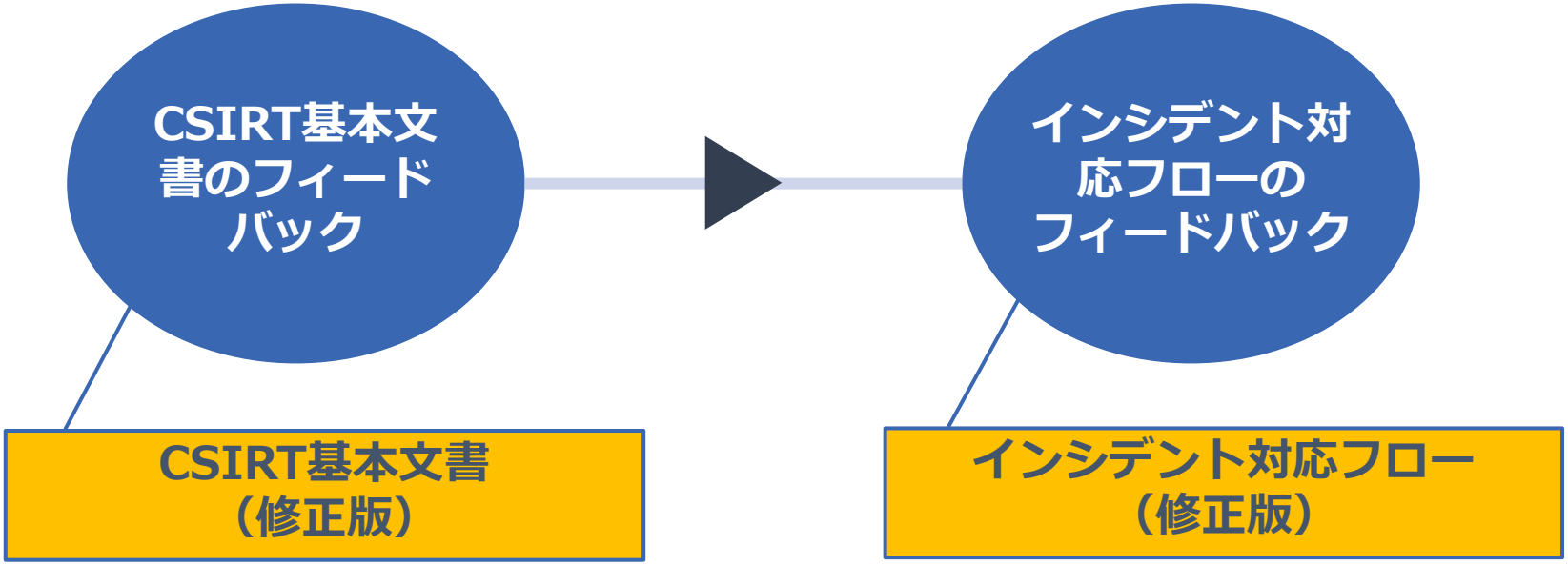
連絡先情報	(1)チーム名 (2)所在地 (3)時間帯 (4)電話番号 (5)ファクシミリ番号 (6)他の音声通信手段 (7)電子メールアドレス (8)公開鍵と他の暗号化情報 (9)チームメンバー (10)業務時間 (11)他の情報 (12)顧客連絡先	**憲章**	(1)ミッションステートメント (2)サービス対象者 (3)スポンサーシップと提携 (4)権限
		ポリシー	(1)インシデントの種類とサポートレベル (2)協力、連携、情報開示 (3)コミュニケーションと本人認証
		サービス	(1)インシデント対応 (2)予防的活動
		インシデント報告フォーム	(1)インシデント報告用のフォーム
		免責事項	(1)免責事項

【参考資料】JPCERT「CSIRT記述書 作成例」https://www.jpcert.or.jp/csirt_material/files/12_csirt_description_sample_20211130.pdf

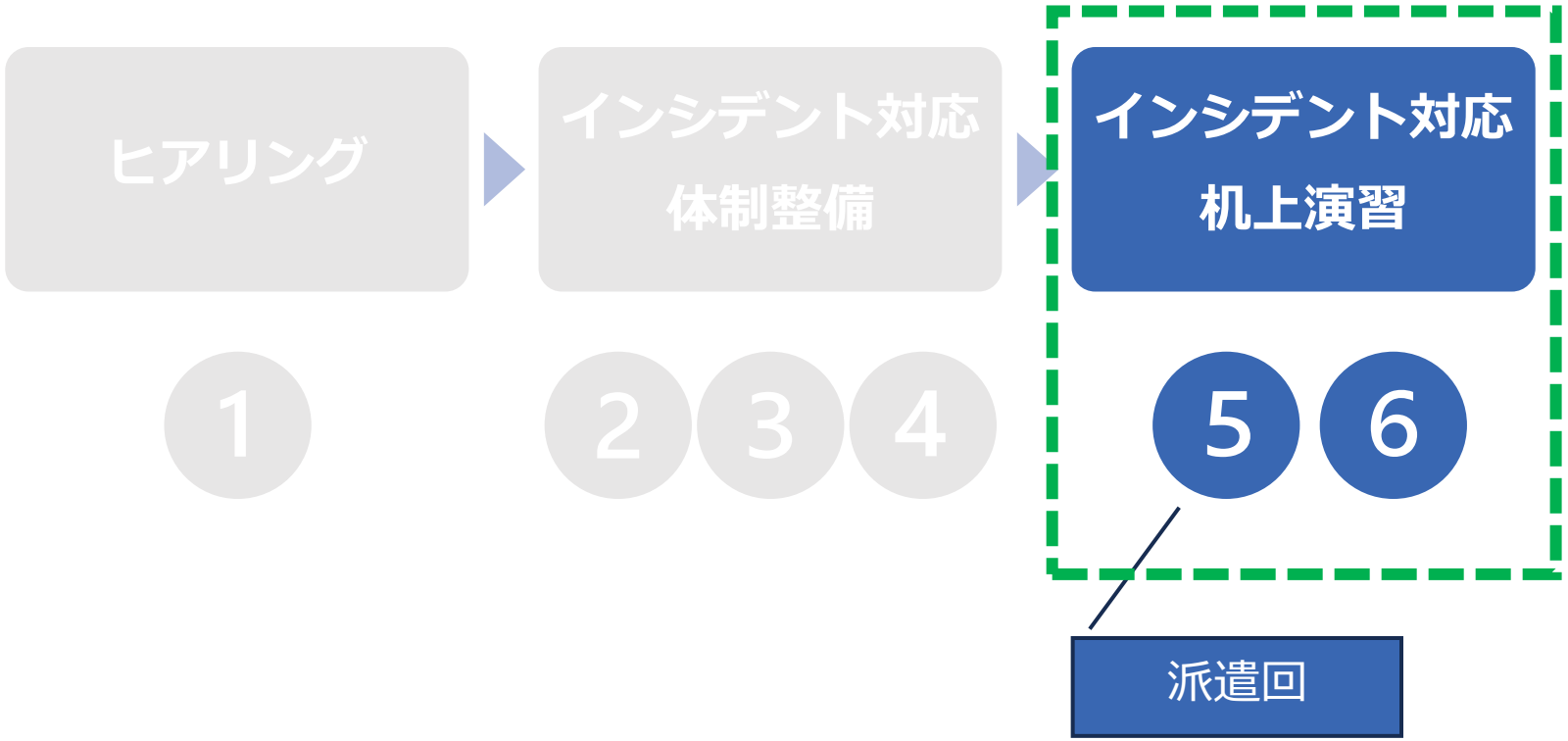
インシデント対応フロー（案）



インシデント対応体制整備 ③



支援の流れ



インシデント対応机上演習 ①

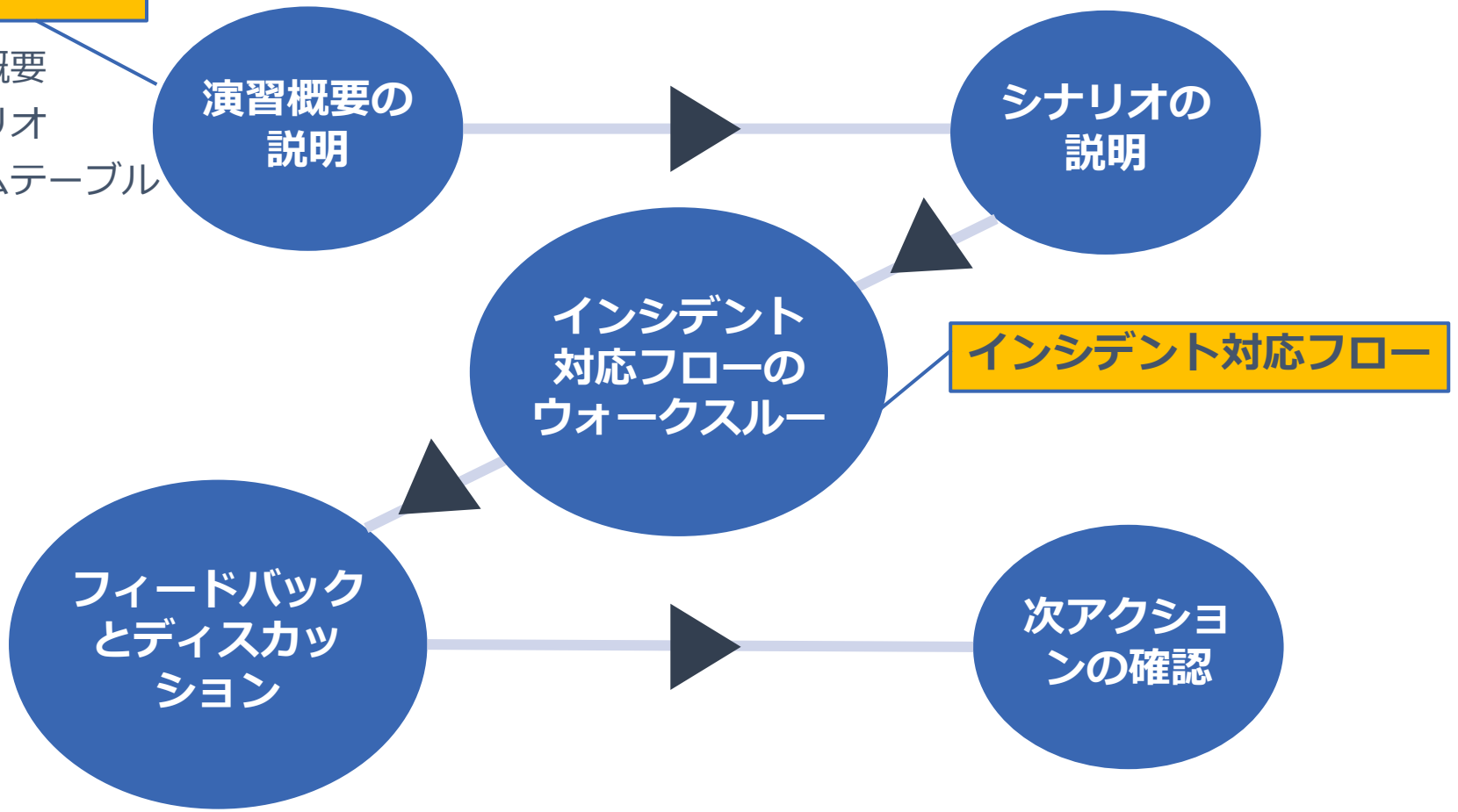
机上演習説明資料

- 机上演習の背景と必要性
- 机上演習の概要
- 机上演習後想定する次ステップ
- 机上演習スコープ・シナリオ
- タイムテーブル
- 机上演習の確認観点
- 机上演習準備資料

インシデント対応机上演習 ②

机上演習計画

- 演習概要
- シナリオ
- タイムテーブル



机上演習の確認観点

1	判断責任者の明確化
2	判断基準の整備
3	関連資料の把握
4	連絡体制
5	役割ごと対応内容の明確化
6	社内外の情報連携
7	初動対応の検討実施
8	顧客への周知対応
9	復旧対応の検討実施
10	情報収集調査（発生したインシデント情報の収集）
11	情報収集調査（インシデント内容の調査）

机上演習シナリオ（例）

No	項目	攻撃者の手順
1	マルウェアの侵入	請求書を装った標的型攻撃のメールにてマルウェアを送り込み、添付ファイルを実行させる
2	マルウェアの拡散	PC利用のユーザーアカウントに管理権限が与えられているため、他のPCやサーバに拡散される
3	暗号化の実施	管理権限によってランサムウェアが実行され、暗号化処理が始まる
4	重要サーバのダウン	重要サーバ上でランサムウェアが起動し、業務で必要なデータが暗号化されてしまう
5	業務停止	業務データが暗号化されたことにより、重要業務が停止

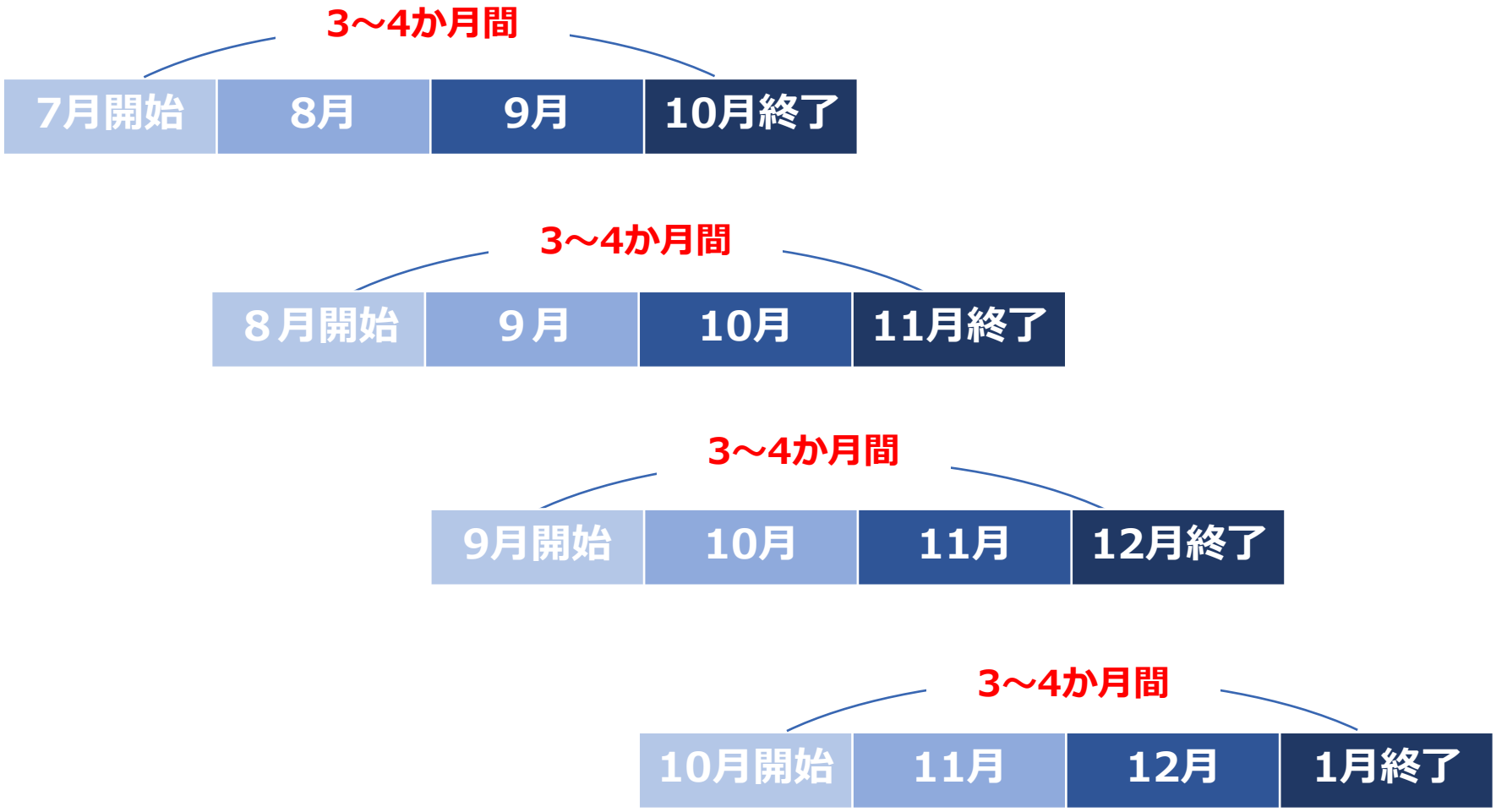
机上演習シナリオ（例）

No	項目	攻撃者の手順
1	外部委託事業者に侵入	事業者が外部委託し、リモート保守のために設置したVPN機器の脆弱性（または、漏洩され公開されていた IDPW情報）を用いて事業者内NWに侵入
2	事業者内探索情報窃取	事業者内データセンターのIDパスワードが脆弱だったことから、攻撃者に容易に不正アクセスされ、その後、システム情報（IPアドレスやパスワード情報など）を窃取されたため事業者内での攻撃拡大
3	サーバー侵入	事業者の端末から窃取した拠点A内サーバーの管理者認証情報により、RDP通信を用いて、業務サーバーに侵入。ウイルス対策ソフトのアンインストールも実施
4	拠点A内のシステム情報の窃取	サーバーを踏み台に拠点A内の他サーバーの認証情報をツールを用いて窃取。なお、サーバーと他サーバーのIDPWは共通で窃取は容易
5	他サーバー侵入	サーバーで窃取した他サーバー認証情報により、物流システムなどの業務システムや他システムのサーバーに侵入
6	クライアントへログオン試行	侵入されたサーバー等を経由して、クライアントにログオン試行した可能性
7	ランサムウェア感染	各サーバーでランサムウェア感染、永続化を行い、ランサムノート（身代金要求文書）を表示

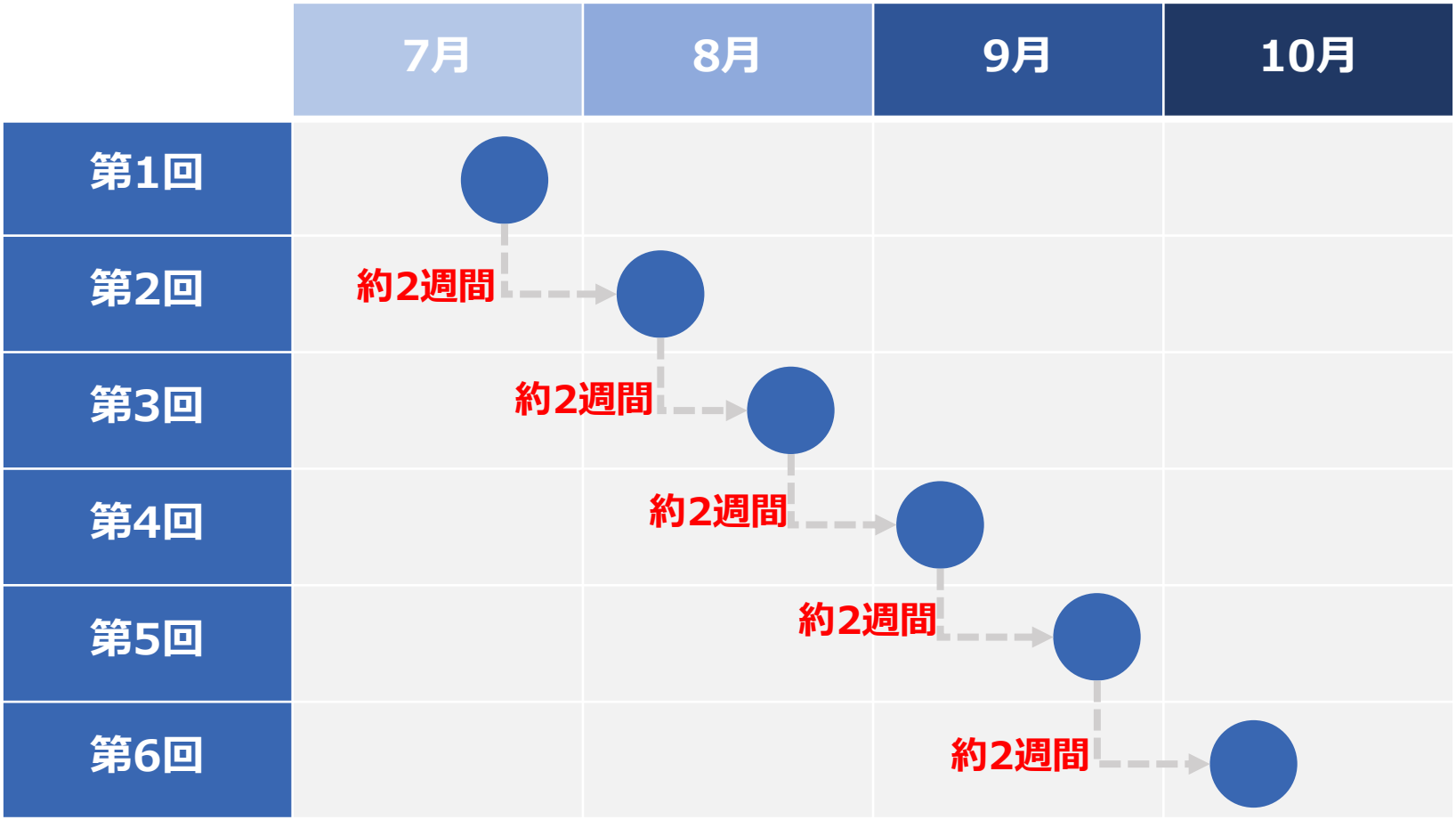
登録専門家

専門家	資格	実績・プロフィール
A	CEH（認定ホワイトハッカー）認定講師	セキュリティ業務歴10年以上（Webアプリケーション・ネットワーク脆弱性診断、ペネトレーションテスト、CSIRT構築支援、BCP策定支援、講師など）
B	【IPA資格】プロジェクトマネージャー、情報セキュリティマネジメント	セキュリティコンサル業務歴6年（CSRIT構築支援,BCP策定支援,ISMS導入支援,CIS Controls準拠支援、セミナー講師　など）
C	【IPA資格】情報セキュリティマネジメント	セキュリティコンサル業務歴6年（CSRIT構築支援,BCP策定支援,ISMS導入支援,CIS Controls準拠支援、セミナー講師　など）
D	ー	セキュリティ業務歴５年以上。インフラやWEBに関する開発、セキュリティに関する設定等。CSIRT構築支援、BCP策定支援や脆弱性診断業務経験有り。セキュリティコンサルやセミナーなどの講師としても活躍。
E	【IPA資格】情報セキュリティマネジメント、基本情報技術者	セキュリティコンサル業務歴3年（セキュリティアドバイザリー、ISMS導入支援、CSIRT構築支援、BCP策定支援　など）
F	【IPA資格】第二種情報処理技術者	業務経験18年（セキュリティ業務歴3年）CSIRT構築支援、BCP策定支援
G	ー	セキュリティ業務歴10年（ISMSコンサル、セミナー講師など）
H	CISSP、情報処理安全確保支援士	業務経験26年（セキュリティ経験：20年）ITインフラ設計・構築・テスト、移行設計、セキュリティ製品導入支援、ISMS導入支援

支援スケジュール①


3～4か月間
7月開始
8月
9月
10月終了
3～4か月間
８月開始
９月
10月
11月終了
3～4か月間
9月開始
10月
11月
12月終了
3～4か月間
10月開始
11月
12月
1月終了

支援スケジュール②



支援方法

訪問実施

原則、都内事業所へ
専門家が訪問して
対面で実施
※1回あたり約2時間

オンライン実施

参加企業の事情等により、オンラインでの実施も可能
※1回あたり約2時間

参加企業専用相談窓口

事業に関するご相談のほか、専門家（情報処理安全確保支援士）と連携して、
日常的なセキュリティ課題に関する相談に対応

（受付時間）　平日　9:00　～　17:00

	**050-4560-7553**
	**ade.jp.tokubetsu@jp.adecco.com**
	**https://tokubetsushien.metro.tokyo.lg.jp/**

コミュニティ形成支援

セキュリティセミナー

懇親会

参加企業同士の
ネットワーキング

令和6年11月～令和7年1月頃、都内会場にて開催予定

参加対象企業

(1) **東京都内**に主たる事業所を有する**中小企業**

(2) UTMやEDR等の**一定程度のセキュリティ対策機器・ソフトウェアを導入**し、**社内セキュリティポリシーを策定**した後、サイバーセキュリティ対策の継続や自走化に向けた**取組を実施している**中小企業

参加申込概要

- 申込期間　令和６年７月３日（水）まで
- 募集企業　40社（IT-BCP策定コース 20社
  CSIRT構築コース 20社）
- 参加費用　無料
- 申込方法　事業WEBサイトよりお申し込みください

東京都　セキュリティ　特別　検索

参加の流れ


7月初旬～中旬
申し込み
内容確認
抽選
結果通知
参加同意書提出
参加決定
支援日程調整
第１回支援
3営業日
支援コース決定

支援コース決定の流れ

募集企業　40社	
IT-BCP策定コース	CSIRT構築コース
20社 程度	20社 程度

申込事の希望	抽選枠	支援コース
IT-BCP	IT-BCP	IT-BCP または CSIRT
CSIRT	CSIRT	CSIRT または IT-BCP
専門家に相談してから決めたい	申込情報により決定	IT-BCP または CSIRT

参加同意書

募集要項 P.15

□ 支援期間中［令和６年７月中旬～令和７年１月下旬（予定）］に、全６回の専門家派遣（３～４か月で実施）を受け入れ可能です。
□ インシデント対応体制整備及びインシデント対応力向上に強い意欲があります。
□ 支援期間中は、運営事務局からの電話連絡やメールに迅速かつ適切に対応し、専門家（支援者）からの支援や助言を積極的に活用します。また、本事業で実施するコミュニティイベントに原則参加します。
□ 支援期間中及び支援期間終了後に運営事務局が実施するアンケートやヒアリング調査に協力します。
□ 東京都、運営事務局または専門家（支援者）から提供された情報を機密扱いし、第三者に漏洩せず、個人的な利益や目的に使用しないことに同意します。情報の使用や公開に関しては、東京都または運営事務局からの指示に従います。
□ その他、募集要項記載事項について、全て内容を理解し了承します。

お申し込み・お問い合わせ

中小企業サイバーセキュリティ特別支援事業運営事務局

050-4560-7553（平日 9:00～17:00）

ade.jp.tokubetsu@jp.adecco.com

https://tokubetsushien.metro.tokyo.lg.jp/

中小企業サイバーセキュリティ特別支援事業

参加申込はこちら

WEBサイトはこちら