IPAが取組む情報セキュリティ対策と中小企業向け普及啓発活動について

2017年4月19日

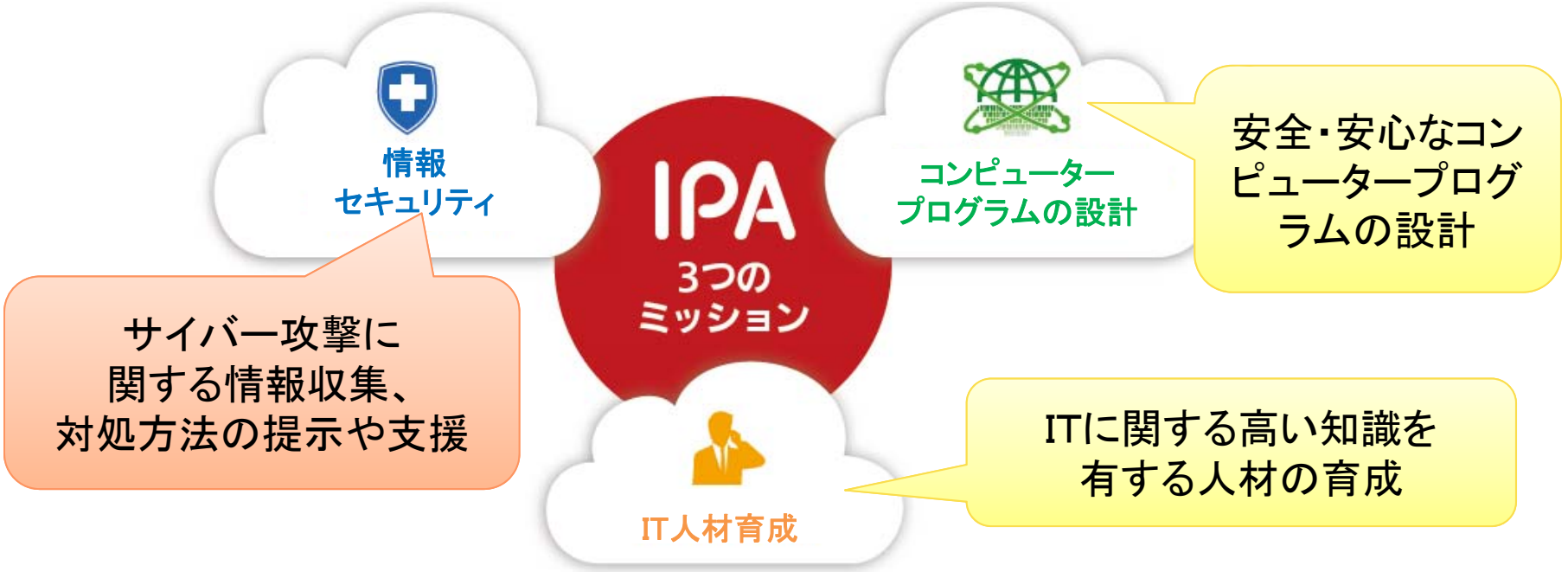
独立行政法人情報処理推進機構
技術本部 セキュリティセンター

目次

IPA概要紹介

- **独立行政法人　情報処理推進機構**
- **IPA: I**nformation-technology **P**romotion **A**gency, Japan
  - 1970年に「情報処理の促進に関する法律」に基づき設立

- **3つの責務: “頼れるIT社会”の実現を目指して**



IPA/ISEC(セキュリティセンター)の全体像

1. 情報セキュリティに関する情報収集・分析、攻撃対応支援
2. 各種情報・対策ツール等の提供
3. 普及・啓発
4. 基盤的な情報セキュリティ対策

情報の収集・分析、攻撃対応支援

- コンピュータウイルス
- 不正アクセス
- 脆弱性
- 標的型攻撃対応支援　等

組織向けに提供される情報等

- 標的型攻撃対策、不正アクセス対策
- 内部不正対策
- 脆弱性対策
- セキュリティマネジメント　等

普及
啓発

個人向けに提供される情報等

- 相談窓口による相談受付
- マルウェア、ウイルスへの注意喚起
- ワンクリック(詐欺)、SNSの注意点　等

基盤的な情報セキュリティ対策

- 評価・認証(Common Criteria等)
- 暗号　等

脅威の現状
情報セキュリティ10大脅威 2017

- 10大脅威とは？ https://www.ipa.go.jp/security/vuln/10threats2017.html
  - 2006年よりIPAが毎年発行している資料
  - 「10大脅威選考会」約100名の投票により、
    情報システムを取巻く脅威を順位付けして解説

脅威の現状

情報セキュリティ10大脅威 2017

昨年順位	「個人」の10大脅威	順位	「組織」の10大脅威	昨年順位
1位	インターネットバンキングやクレジットカード情報の不正利用	1位	標的型攻撃による情報流出	1位
2位	ランサムウェアによる被害	2位	ランサムウェアによる被害	7位
3位	スマートフォンやスマートフォンアプリを狙った攻撃	3位	ウェブサービスからの個人情報の窃取	3位
5位	ウェブサービスへの不正ログイン	4位	サービス妨害攻撃によるサービスの停止	4位
4位	ワンクリック請求等の不当請求	5位	内部不正による情報漏えいとそれに伴う業務停止	2位
7位	ウェブサービスからの個人情報の窃取	6位	ウェブサイトの改ざん	5位
6位	ネット上の誹謗・中傷	7位	ウェブサービスへの不正ログイン	9位
8位	情報モラル不足に伴う犯罪の低年齢化	8位	IoT機器の脆弱性の顕在化	ランク外
10位	インターネット上のサービスを悪用した攻撃	9位	攻撃のビジネス化（アンダーグラウンドサービス）	ランク外
ランク外	IoT機器の不適切な管理	10位	インターネットバンキングやクレジットカード情報の不正利用	8位

標的型サイバー攻撃の脅威と対策

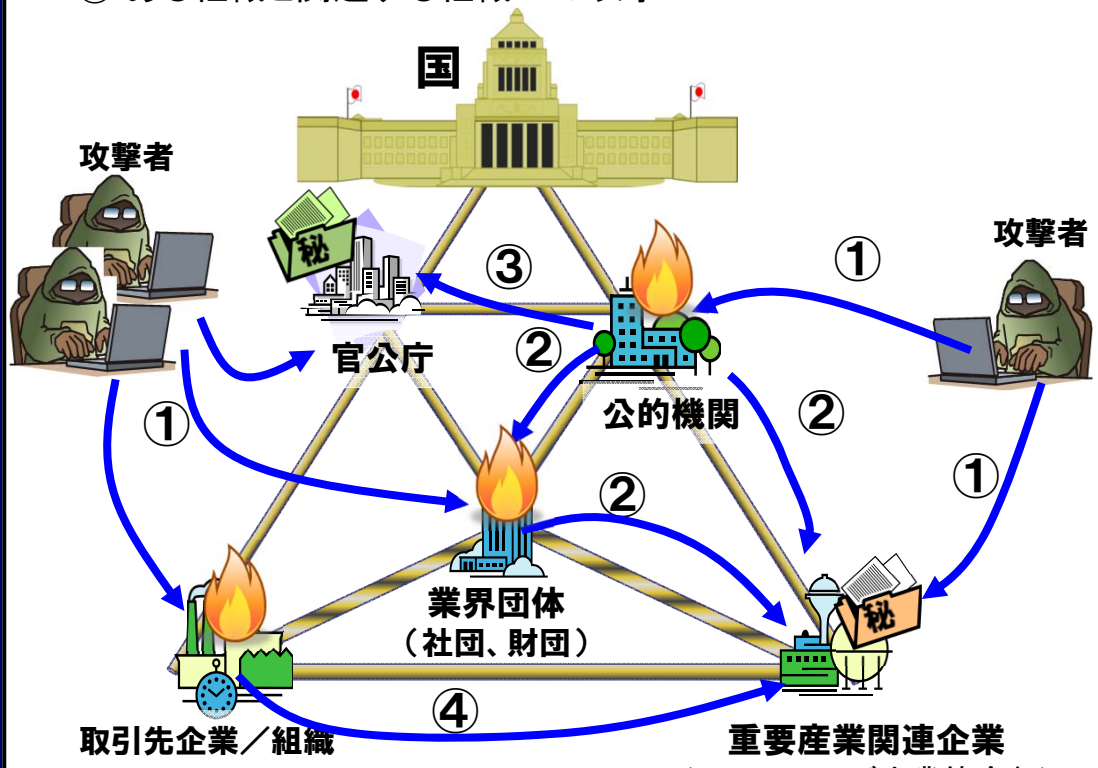
～標的型サイバー攻撃の構造～

IPA

標的型攻撃のルート・連鎖

メールの窃取、メールアカウントの乗っ取り、組織詐称など、
標的型攻撃は様々なルートから仕掛けられる：

① 標的組織への直接攻撃や踏み台としての攻撃
②ある組織から傘下の組織への攻撃
③ある組織から上流の組織への攻撃
④ ある組織と関連する組織への攻撃



こうした攻撃に対して：

1．各組織の対応力の向上
→ 組織・システム両面での対策強化

2．業界としての対応力の向上
→ 情報共有
・J-CSIP

3．社会組織全体としての対応力の向上
→ 攻撃連鎖の解明と遮断
・J-CRAT

の三位一体での対応が重要

標的型サイバー攻撃の脅威と対策

年	攻撃観測	代表的な事件
2005	国内政府で標的型メールを観測	
・・・		
2012		重工業界で情報漏洩、政府機関攻撃
2013	水飲み場型攻撃登場	農水省へのサイバー攻撃
2014	やり取り型攻撃登場	ソニー子会社情報漏洩
2015		年金機構情報漏洩
2016	より一層の巧妙化	JTB顧客情報流出

✓ 標的型サイバー攻撃の脅威は増大の一途
✓ 企業・法人・業界における「対策強化」が必要

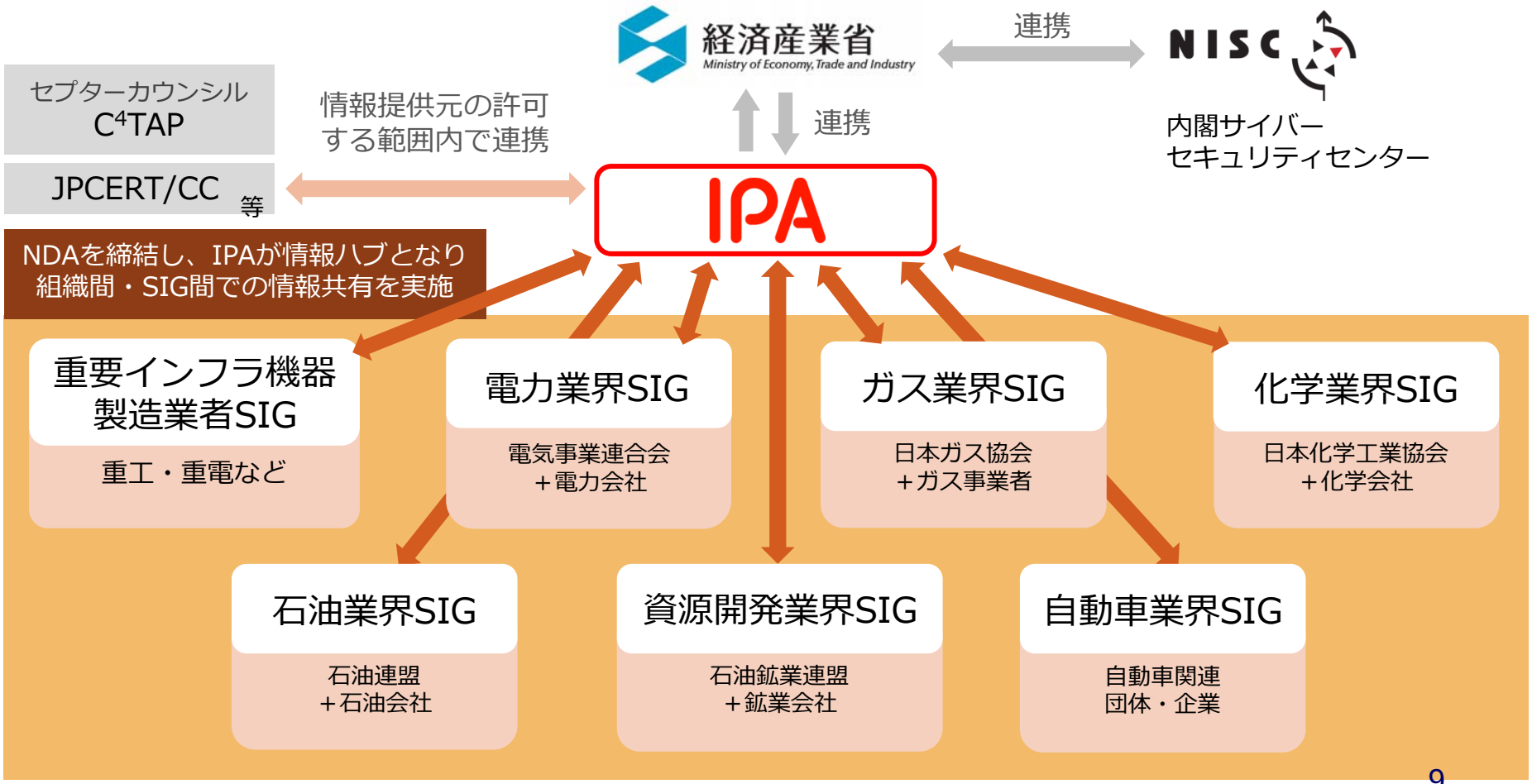
IPAでは情報共有活動【J-CSIP】、対策支援（レスキュー）活動【J-CRAT】を実施中

標的型サイバー攻撃の脅威と対策

J-CSIP（サイバー情報共有イニシアティブ）

J-CSIP：Initiative for Cyber Security Information sharing Partnership of Japan

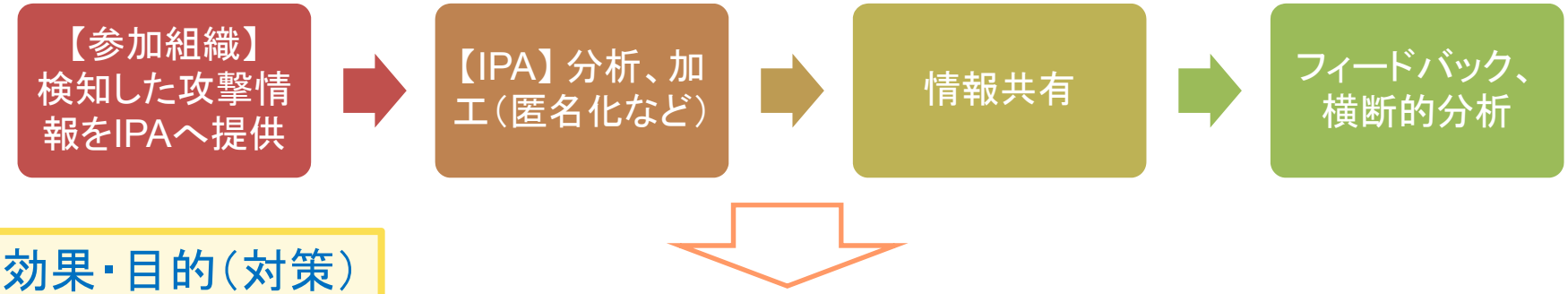
- 7つのSIG（Special Interest Group）、87の参加組織
- IPAとの間で秘密保持契約（NDA）を締結、各種関連機関とも連携



標的型サイバー攻撃の脅威と対策

J-CSIP（サイバー情報共有イニシアティブ）

情報共有の基本的な流れ



効果・目的（対策）

① 類似攻撃の早期検知と被害の低減
② 事前防御の実施（ブラックリストへの追加等）
③ 複数の攻撃情報を基にした横断的分析

実績（件数）

項目	2012年度	2013年度	2014年度	2015年度
IPAへの情報提供件数	246件	385件	626件	1,092件
参加組織への情報共有実施件数	160件	180件	195件	133件

標的型サイバー攻撃の脅威と対策

サイバーレスキュー隊J-CRAT～早期対応の重要性～

IPA

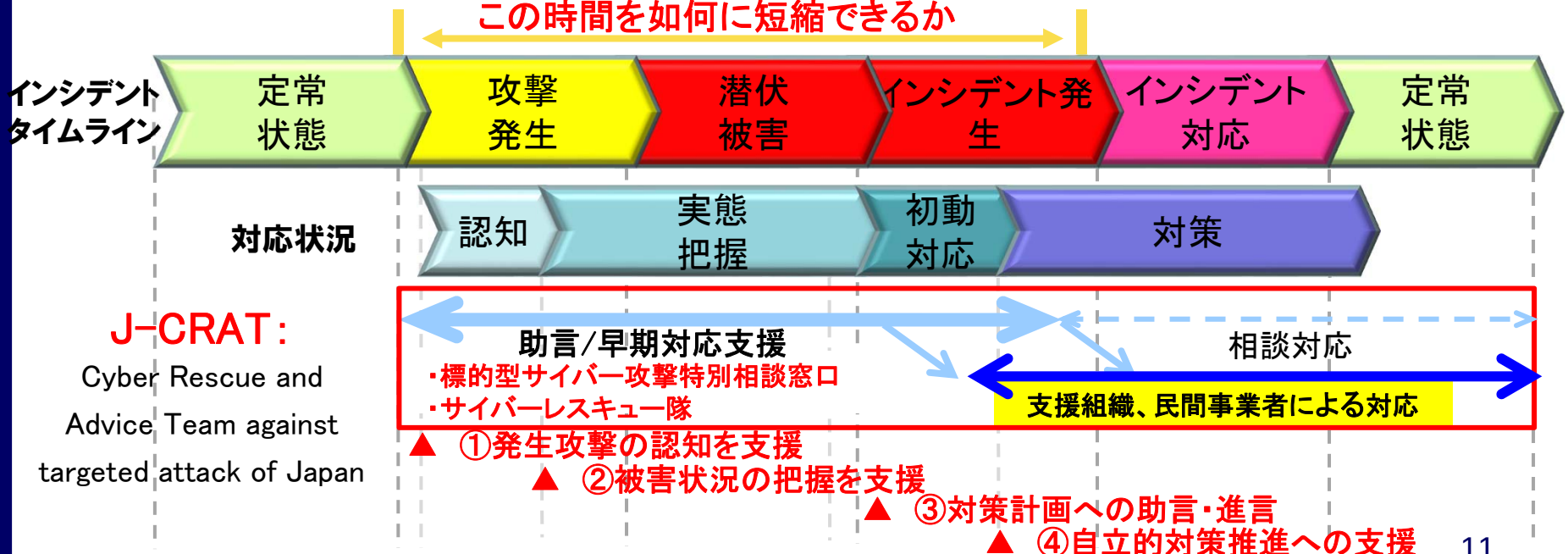
活動内容：　攻撃を検知できずに「潜伏被害」を受けている組織や、検知した「インシデント発生」の状況や深刻度が認識できずにいる組織を支援：

・攻撃の把握　・被害の分析　・対策の早期着手

活動の目的：　標的型サイバー攻撃に対する相談対応、事案によりレスキュー活動を実施することで、以下を達成する：

① 標的型サイバー攻撃被害の拡大防止、被害の低減を図る

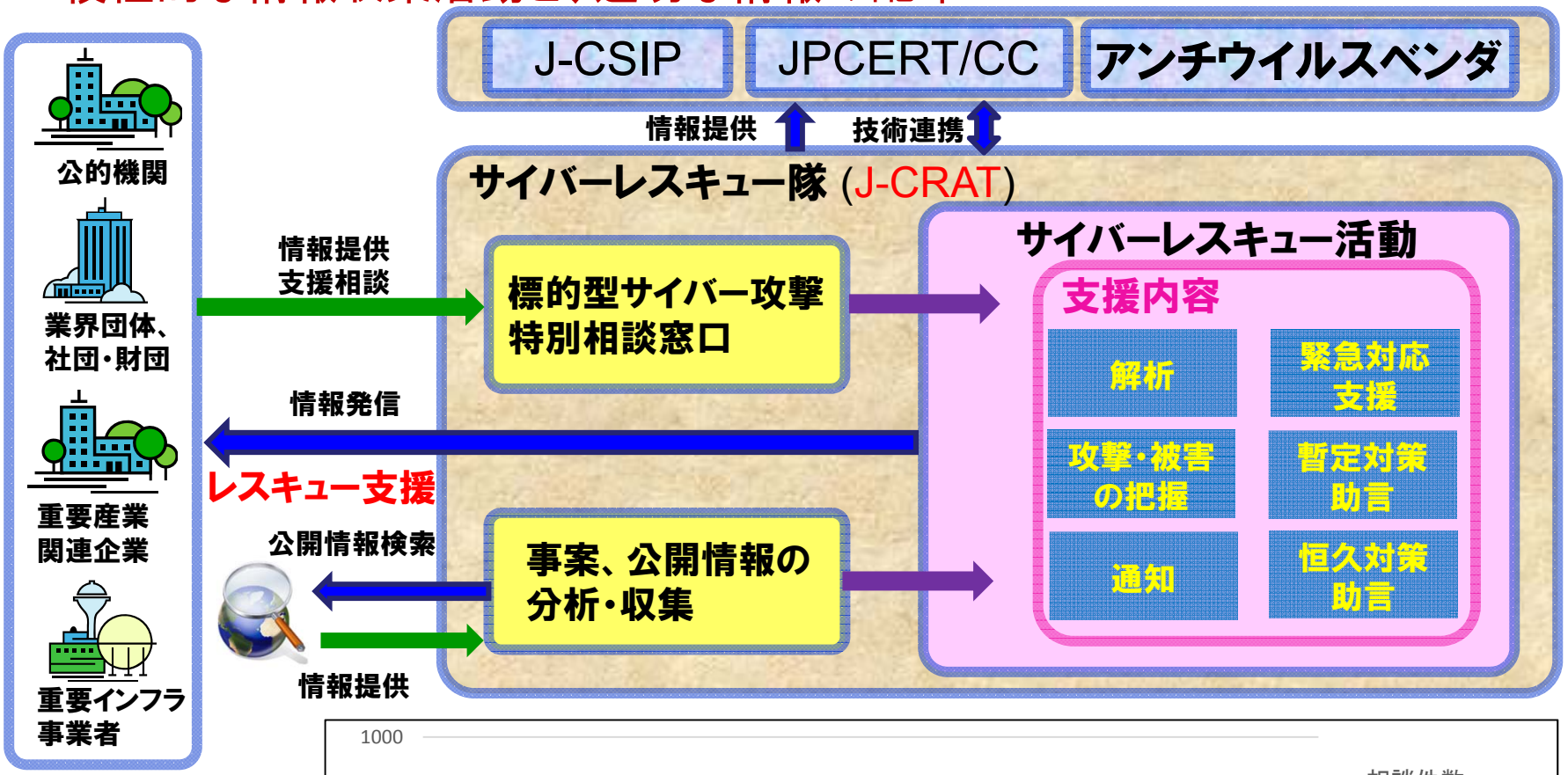
② 攻撃の連鎖を解明、遮断する



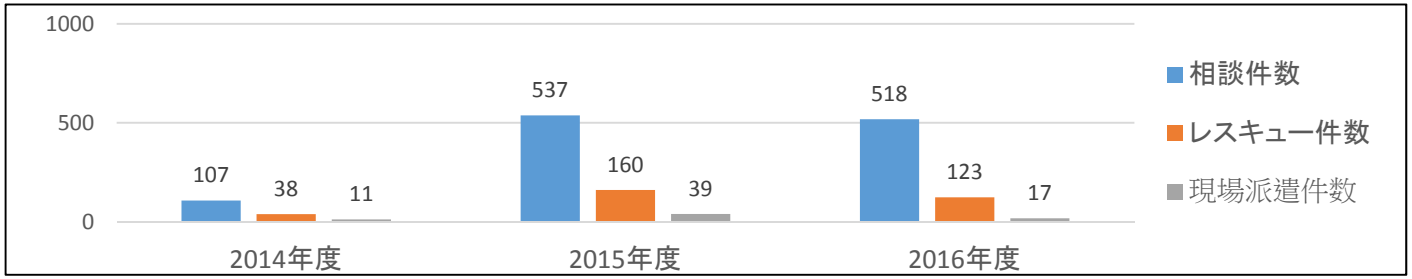
サイバーレスキュー隊J-CRAT～早期対応の重要性～

IPA

✓ 積極的な情報収集活動と、適切な情報の配布



J-CRAT 活動実績



新国家資格「情報処理安全確保支援士」

【設立の目的】
サイバーセキュリティに関する実践的な知識・技能を有する専門人材を育成・確保

①人材の質の担保
- 「情報セキュリティスペシャリスト試験」をベースとした新たな試験の合格者を登録
- 継続的な講習受講義務により、最新の知識・技能を維持

②人材の見える化
- 資格保持者のみ資格名称を使用
- 登録簿の整備・登録情報の公開（希望しない者を除く）

③人材活用の安心感
- 国家資格として厳格な秘密保持義務、信用失墜行為の禁止義務

【支援士の活動】
企業における安全な情報システムの企画・設計・開発・運用を支援、
サイバーセキュリティ対策の指導・助言を実施

■第１回(2017年4月1日)登録者数：4,172名(平均年齢40.5歳)
※経過措置対象者(「情報セキュリティスペシャリスト試験」または「テクニカルエンジニア(情報セキュリティ)」合格者)
■初回試験(2017年4月16日実施)応募者数：25,130名(平均年齢38.5歳)

2020年に登録者3万人が目標

All Rights Reserved, Copyright©IPA2017

中小企業への情報セキュリティ普及の取組み

○中小企業のセキュリティの課題

「2016年度　中小企業における情報セキュリティ対策に関する実態調査」より

○中小企業の情報セキュリティ対策ガイドライン（第2版）

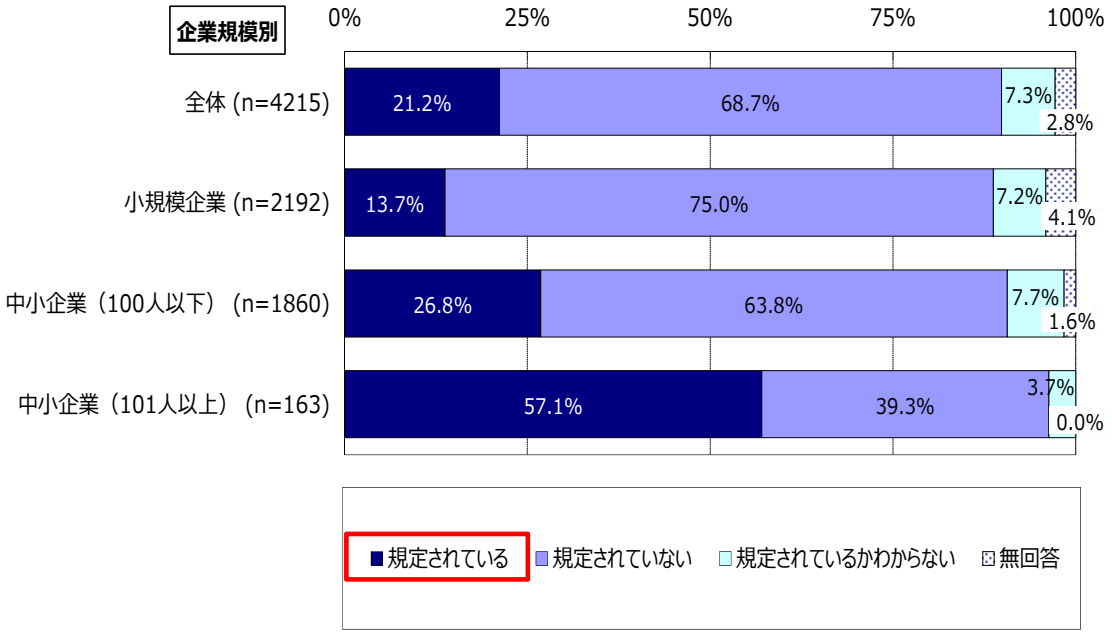
○共同宣言

○「SECURITY ACTION」制度

中小企業のセキュリティの課題
情報漏えい等の措置

- 情報漏えい等のインシデント又はその兆候を発見した場合の対応方法を規定しているのは、小規模企業では13.7%のみ
  - 企業規模別では、小規模企業が13.7%、100人以下の中小企業が26.8%、101人以上の中小企業が57.1%である。

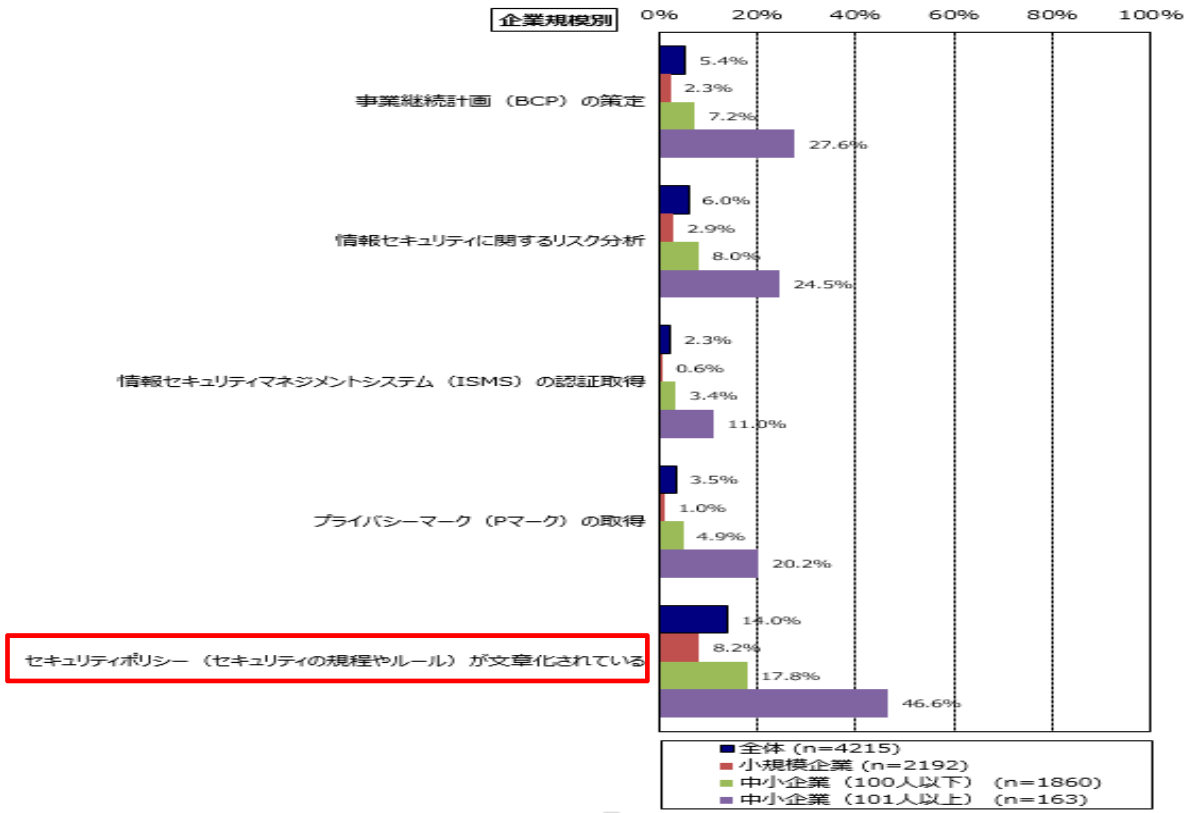
Q14　貴社において、情報漏えい等のインシデント又はその兆候を発見した場合、対応方法は規定されていますか。



中小企業のセキュリティの課題
組織面・運用面の被害防止対策

- 情報セキュリティ関連の被害を防止するために実施している組織面・運用面の対策として、セキュリティポリシーの文章化を実施している小規模企業の割合は8.2%であり、中小企業に比べて実施率が低い。

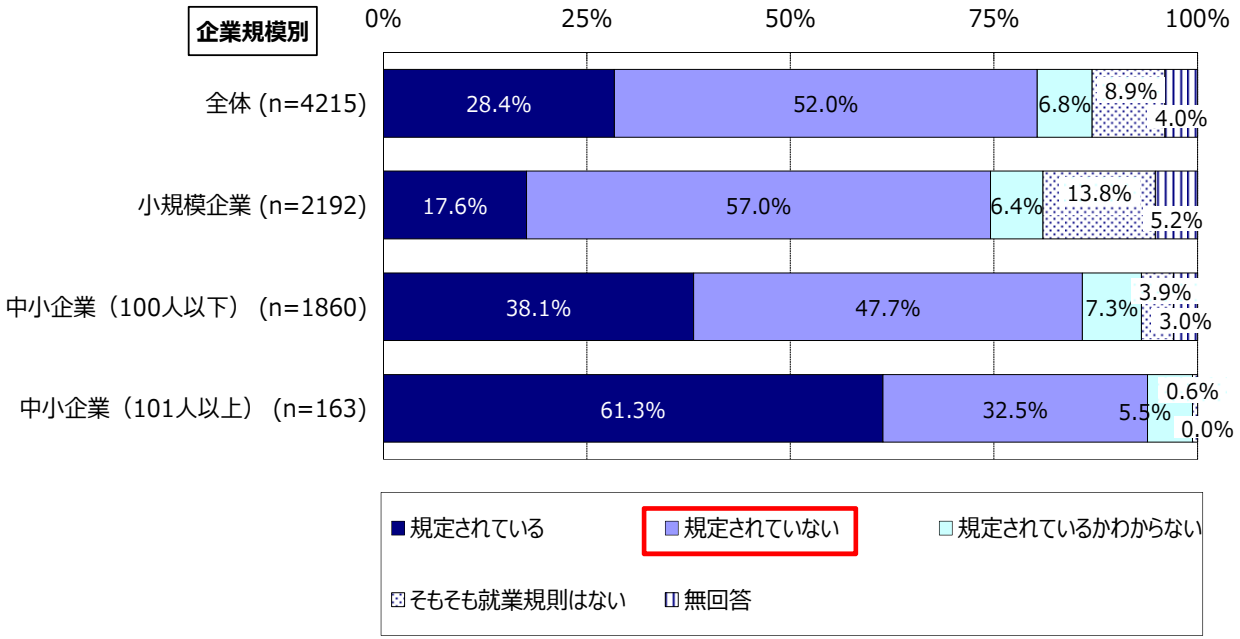
Q16　貴社では情報セキュリティ関連の被害を防止するために、どのような組織面・運用面の対策を実施していますか。実施している対策をお答えください。（いくつでも）



中小企業のセキュリティの課題
ルールから逸脱した場合の措置

- 全体では、「規定されていない」が最も多く52.0%、次いで「規定されている」が28.4%、「そもそも就業規則はない」が8.9%の順である。企業規模別で見ると、小規模企業で最も多いのは「規定されていない」で57.0%、中小企業（100人以下）で最も多いのは「規定されていない」で47.7%、中小企業（101人以上）で最も多いのは「規定されている」で61.3%である。

Q15　社内の情報セキュリティに関するルールから逸脱した場合の措置について、就業規則等で規定されていますか。



中小企業の
情報セキュリティ対策ガイドライン第2版

本ガイドラインのポイント

- 経営者への対策の必要性訴求。専任部門・担当が置けない企業を意識
- 導入のための実践手順、管理台帳等のひな型を提供
- クラウドサービス、スマートフォンをはじめとするモバイル端末の普及等、IT環境の変化への対応

構成	特徴
経営者編	• “経営者がなぜ情報セキュリティに取り組む必要があるのか”に力点、取り組まない場合の経営面の影響、法的・道義的責任について解説。 • 経営者が認識すべき「3原則」、経営者として取り組むべき「重要7項目の取組」を記載
管理実践編	• 専門知識のない実務者や経営者自らも取り組めるように、図表を多用 • 情報セキュリティ対策の具体的な導入手順から、課題の改善手順を記載
付録	• 管理実践編への取り組みを容易なものとするためのツール・資料などで構成。 • 取り組みの端緒となる「情報セキュリティ5か条」をはじめ、「5分でできる自社診断シート」、情報セキュリティポリシー策定にあたって用いる「リスク分析シート」として「情報資産管理台帳」のひな型や「対策状況チェックシート」および「情報セキュリティポリシーサンプル」などを用意

詳細はこちら → http://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html

共同宣言

- 平成29年2月7日、**「中小企業における情報セキュリティの普及促進に関する共同宣言」**を発表
- 中小企業と関わりの深い商工団体、士業団体、IT関連団体、独立行政法人の強固な連携により、中小企業の自発的な情報セキュリティ対策への取り組みを促す活動を推進

一般社団法人中小企業診断協会 全国社会保険労務士会連合会 全国商工会連合会 全国中小企業団体中央会 特定非営利活動法人ITコーディネータ協会 特定非営利活動法人日本ネットワークセキュリティ協会 独立行政法人情報処理推進機構 独立行政法人中小企業基盤整備機構 日本商工会議所 日本税理士会連合会

- IPAにおいて“自発的な情報セキュリティ対策を促す”ための核となる取り組みとして、中小企業自ら取り組みを宣言する制度**「SECURITY ACTION」**を創設し、参加団体が協力して自己宣言企業拡大を目指した様々な活動を展開

「SECURITY ACTION」制度

- 中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度
- 「中小企業の情報セキュリティ対策ガイドライン」の実践をベースに2段階を用意

セキュリティ対策自己宣言

（商標登録申請中）

1段階目（一つ星）
ガイドライン付録の「情報セキュリティ5か条」に取り組むことを宣言

セキュリティ対策自己宣言

（商標登録申請中）

2段階目（二つ星）
ガイドライン付録の「5分でできる！情報セキュリティ自社診断」で自社の状況を把握したうえで、情報セキュリティポリシー（基本方針）を定め、外部に公開したことを宣言

中小企業におけるクラウドの活用

〇サービス活用の利点と留意事項

〇クラウドコンピューティングのセキュリティ

〇参考：安全利用のチェック項目

中小企業におけるクラウドの活用
サービス活用の利点と留意事項

- 利点
  - ITの調達に関わる負担からの解放または負担の軽減
  - ITの運用・保守の負荷からの解放または負荷の軽減
  - IT資源利用の柔軟性・拡張性の獲得
  - セキュリティ対策の負担と負荷からの解放または負担軽減
- 留意事項
  - コンピュータシステムを自ら管理しないことによる制約
  - データを自らの管理範囲外に置く、あるいは社外に預ける不安や制約
  - 利用量・処理量の異常な増加や意図せぬ増大に伴う使用料の急増のリスク
  - 利用できるアプリケーションのカスタマイズの制約
  - アプリケーション間のデータ連携実現への制約やコスト増の可能性

※　IPA「中小企業のためのクラウドサービス安全利用の手引き（2011年4月）」より

中小企業におけるクラウドの活用
クラウドコンピューティングのセキュリティ

- クラウド固有のセキュリティ課題は限られている
  - データセンター利用モデルと共通しているものが多い
  - 分散処理と仮想化環境がクラウドを特徴づけ
- クラウドコンピューティングのセキュリティに関する関心事項
  - データセンター施設の信頼性・耐障害性
  - クラウドを形成する技術要素における脆弱性の排除と安定性の確保
  - クラウド上のデータのセキュリティとプライバシー
  - クラウドサービスプロバイダーのセキュリティ管理能力
  - クラウド利用ユーザの利用能力とセキュリティ管理の及ぶ範囲
  - 国境を越えるデータに対する法的利害衝突
  - 外部からの攻撃に対する耐性と対応能力

※ 「IPAテクニカルウォッチ『クラウドコンピューティングのセキュリティ　その意味と社会的重要性の考察』（2012年4月）」より

中小企業におけるクラウドの活用
参考：安全利用のチェック項目

[A] クラウドサービスの利用範囲についての確認項目		
1	利用範囲の明確化	クラウドサービスでどの業務、どの情報を扱うかを検討し、業務の切り分けや運用ルールの設定を行いましたか？
2	サービスの種類とコスト	業務に合うクラウドサービスを選定し、コストについて確認しましたか？
3	扱う情報の重要度	クラウドサービスで取扱う情報の管理レベルについて確認しましたか？
4	ポリシーやルールとの整合性	セキュリティ上のルールとクラウドサービスの活用の間に矛盾や不一致が生じませんか？
[B] クラウドサービスの利用準備についての確認項目		
5	担当者	クラウドサービスの特徴を理解した担当者を社内に確保しましたか？
6	ユーザ管理	クラウドサービスのユーザについて適切に管理できますか？
7	パスワード	パスワードの適切な設定・管理は実施できますか？
8	データの複製	サービス停止等に備えて、重要情報を手元に確保して必要なときに使えるための備えはありますか？
[C] クラウドサービス提供条件等についての確認		
9	事業者の信頼性	クラウドサービスを提供する事業者は信頼できる事業者ですか？
10	サービスの信頼性	サービスの稼働率、障害発生頻度、障害時の回復目標時間などのサービスレベルは示されていますか？
11	セキュリティ対策	クラウドサービスにおけるセキュリティ対策が具体的に公開されていますか？
12	利用者サポート	サービスの使い方がわからないときの支援（ヘルプデスクやFAQ）は提供されていますか？
13	利用終了時のデータの確保	サービスの利用が終了したときの、データの取扱い条件について確認しましょう。
14	契約条件の確認	一般的契約条件の各項目について確認しましょう。

※　IPA「中小企業のためのクラウドサービス安全利用の手引き『中小企業のためのクラウドサービス安全利用チェックシート』（2011年4月）」より

独立行政法人**情報処理推進機構**
Information-technology Promotion Agency, Japan