資料７

# 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

2016年12月12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**



3

# 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

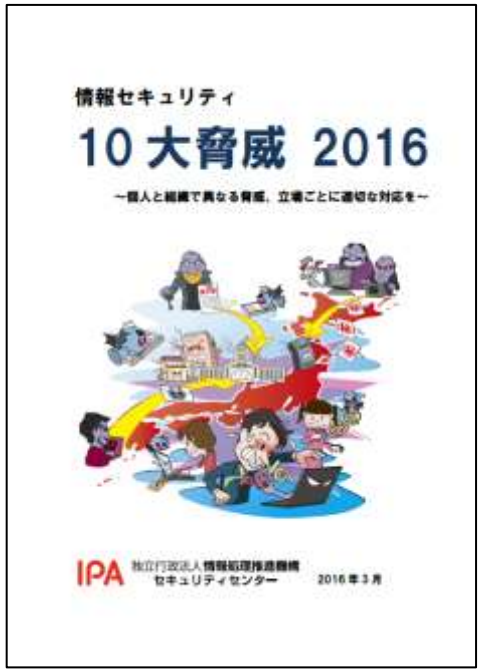
**基盤的な情報セキュリティ対策**

- 評価・認証(Common Criteria等)
- 暗号　等

情報セキュリティの変遷

# ～情報セキュリティ10大脅威 2016～

- 10大脅威とは？ https://www.ipa.go.jp/security/vuln/10threats2016.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




情報セキュリティの変遷

# ～10大脅威の順位の変遷～

| | 10大脅威 2012 | 10大脅威 2013 | 10大脅威 2014 | 10大脅威 2015 | 10大脅威 2016 |
|---|---|---|---|---|---|
| 1位 | 機密情報が盗まれる！？新しいタイプの攻撃 | クライアントソフトの脆弱性を突いた攻撃 | 標的型メールを用いた組織へのスパイ・諜報活動 | 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 | 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 |
| 2位 | 予測不能の災害発生！引き起こされた業務停止 | 標的型諜報攻撃の脅威 | 不正ログイン・不正利用 | 内部不正による情報漏えい | 標的型攻撃による情報流出 |
| 3位 | 特定できぬ、共通思想集団による攻撃 | スマートデバイスを狙った悪意あるアプリの横行 | ウェブサイトの改ざん | 標的型攻撃による諜報活動 | ランサムウェアを使った詐欺・恐喝 |
| 4位 | 今もどこかで・・・更新忘れのクライアントソフトを狙った攻撃 | ウイルスを使った遠隔操作 | ウェブサービスからの利用者情報の漏えい | ウェブサービスへの不正ログイン | ウェブサービスからの個人情報の窃取 |
| 5位 | 止らない！ウェブサイトを狙った攻撃 | 金銭窃取を目的としたウイルスの横行 | オンラインバンキングからの不正送金 | ウェブサービスからの顧客情報の窃取 | ウェブサービスへの不正ログイン |
| 6位 | 続々発覚、スマートフォンやタブレットを狙った攻撃 | 予期せぬ業務停止 | 悪意あるスマートフォンアプリ | ハッカー集団によるサイバーテロ | ウェブサイトの改ざん |
| 7位 | 大丈夫！？電子証明書に思わぬ落とし穴 | ウェブサイトを狙った攻撃 | SNSへの不適切な情報公開 | ウェブサイトの改ざん | 審査をすり抜け公式マーケットに紛れ込んだスマートフォンアプリ |
| 8位 | 身近に潜む魔の手・・・あなたの職場は大丈夫？ | パスワード流出の脅威 | 紛失や設定不備による情報漏えい | インターネット基盤技術を悪用した攻撃 | 内部不正による情報漏えいやサービス停止 |
| 9位 | 危ない！アカウントの使いまわしが被害を拡大！ | 内部犯行 | ウイルスを使った詐欺・恐喝 | 脆弱性公表に伴う攻撃 | 巧妙・悪質化するワンクリック請求 |
| 10位 | 使用者情報の不適切な取扱いによる信用失墜 | フィッシング詐欺 | サービス妨害 | 悪意のあるスマートフォンアプリ | 対策情報の公開に伴い公知となる脆弱性の悪用増加 |

凡例：

| 脆弱性 | ウェブサイト<br>不正ログイン<br>パスワード | 標的型攻撃 | インターネット<br>バンキング | 情報漏えい<br>内部不正 | スマートフォン |
|---|---|---|---|---|---|

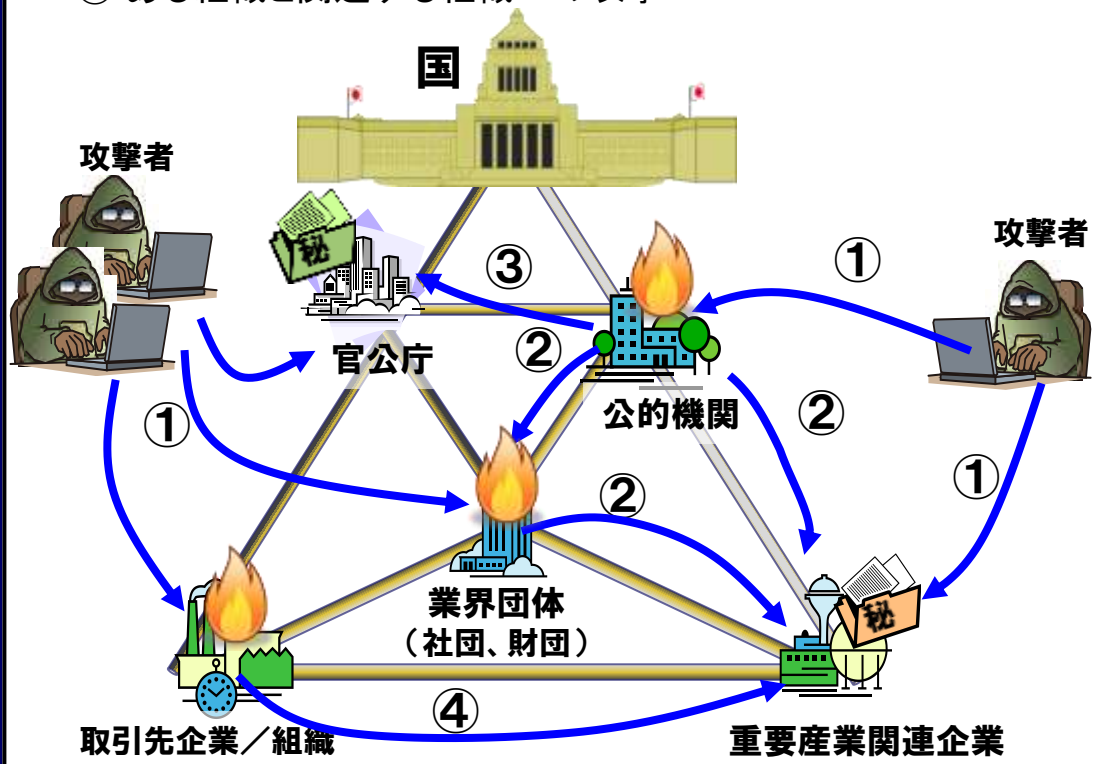
標的型サイバー攻撃の脅威と対策

# ～標的型サイバー攻撃の構造～

## 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

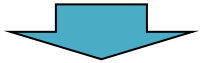
2. 業界としての対応力の向上
   → 情報共有
   ・J-CSIP

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 |



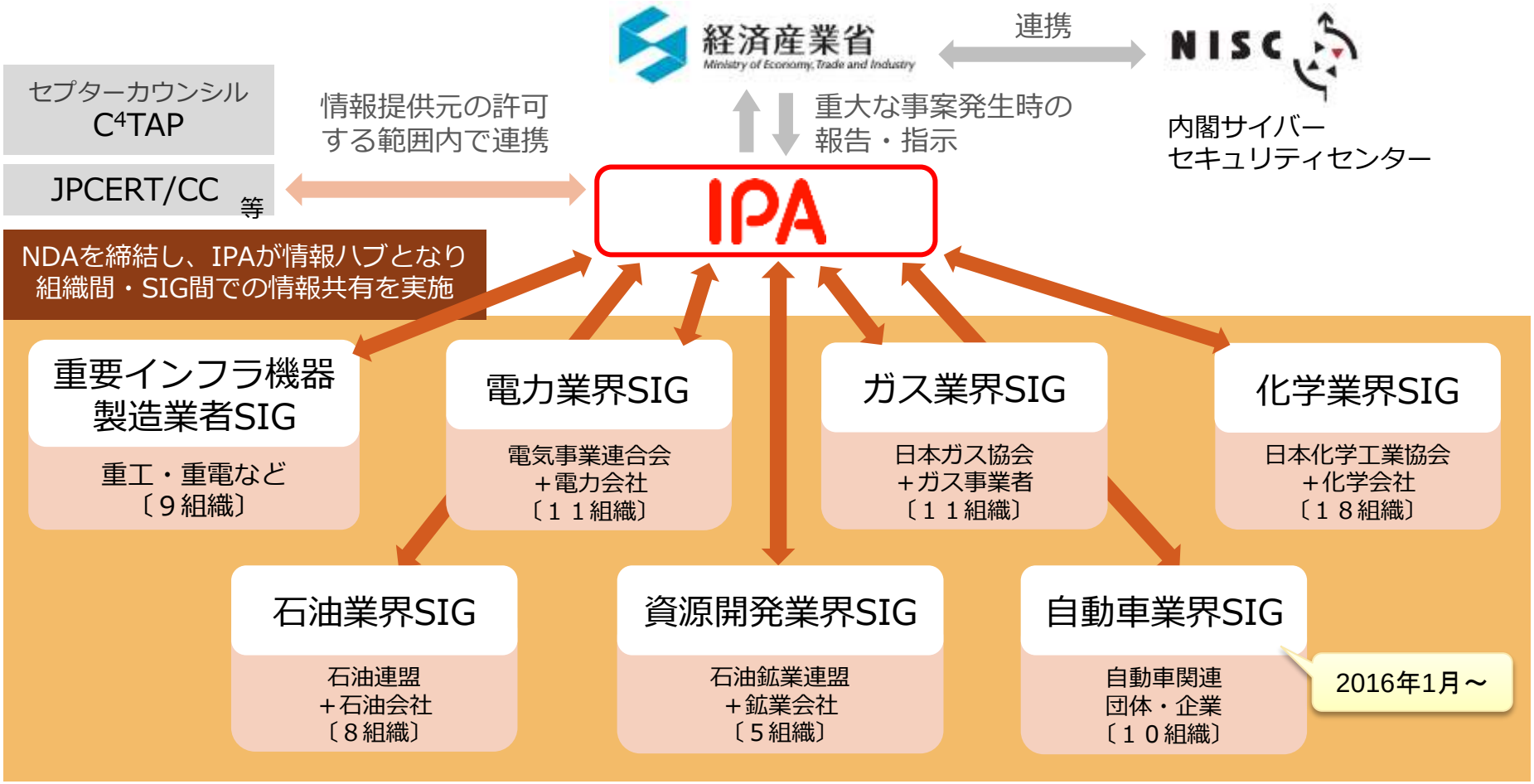
✓ 標的型サイバー攻撃の脅威は増大の一途
✓ 企業・法人・業界における「対策強化」が必要

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

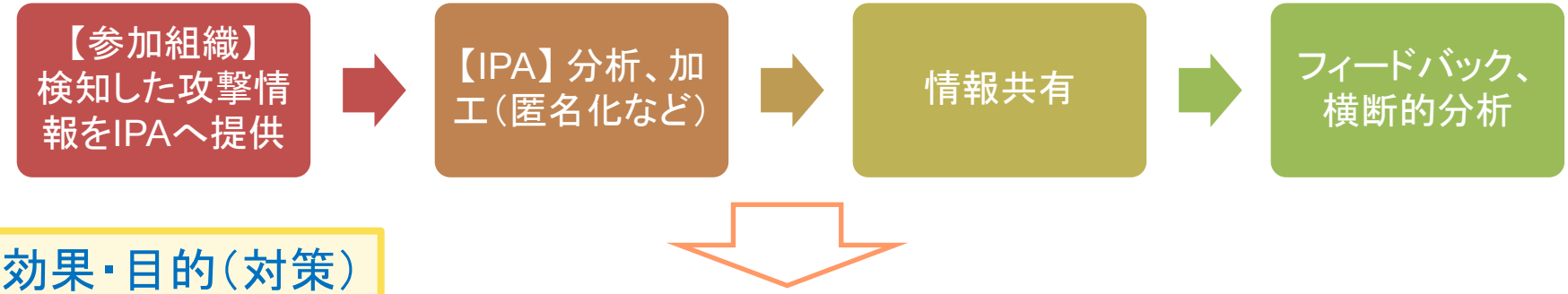
- 7つのSIG（Special Interest Group）、72の参加組織
- IPAとの間で秘密保持契約（NDA）を締結、各種関連機関とも連携



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 |

# サイバーレスキュー隊J-CRAT～早期対応の重要性～

IPA

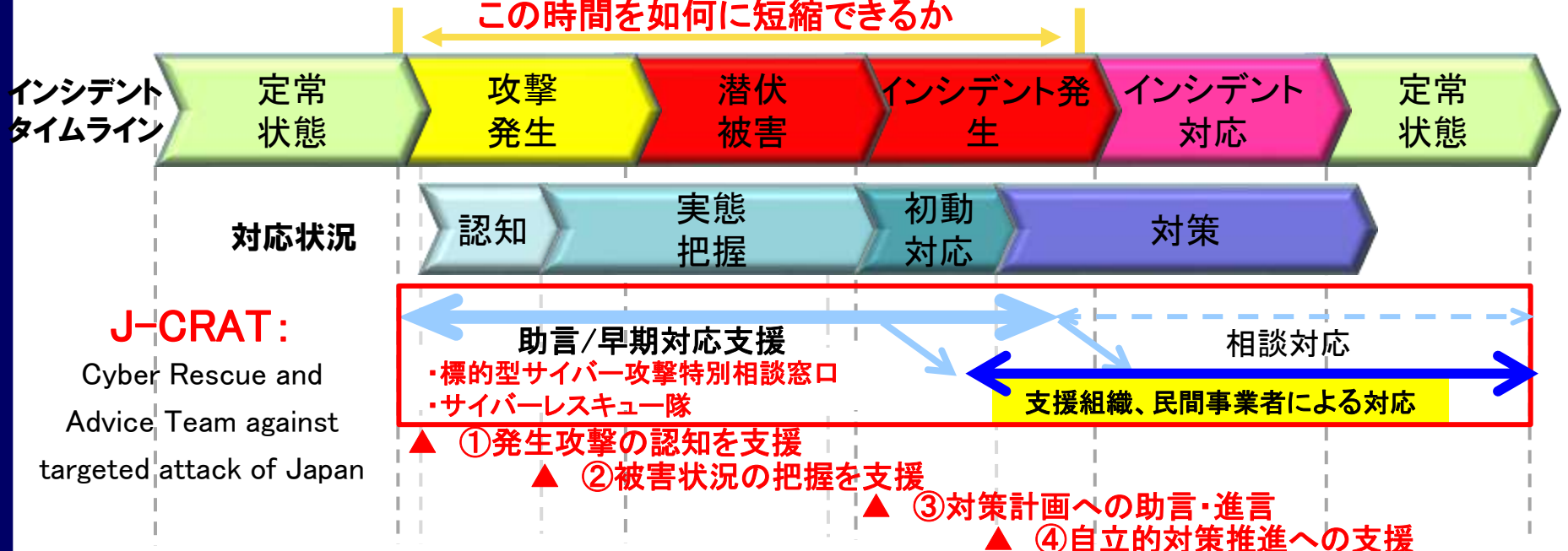
**活動内容**：　攻撃を検知できずに「潜伏被害」を受けている組織や、検知した「インシデント発生」の状況や深刻度が認識できずにいる組織を支援：

・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

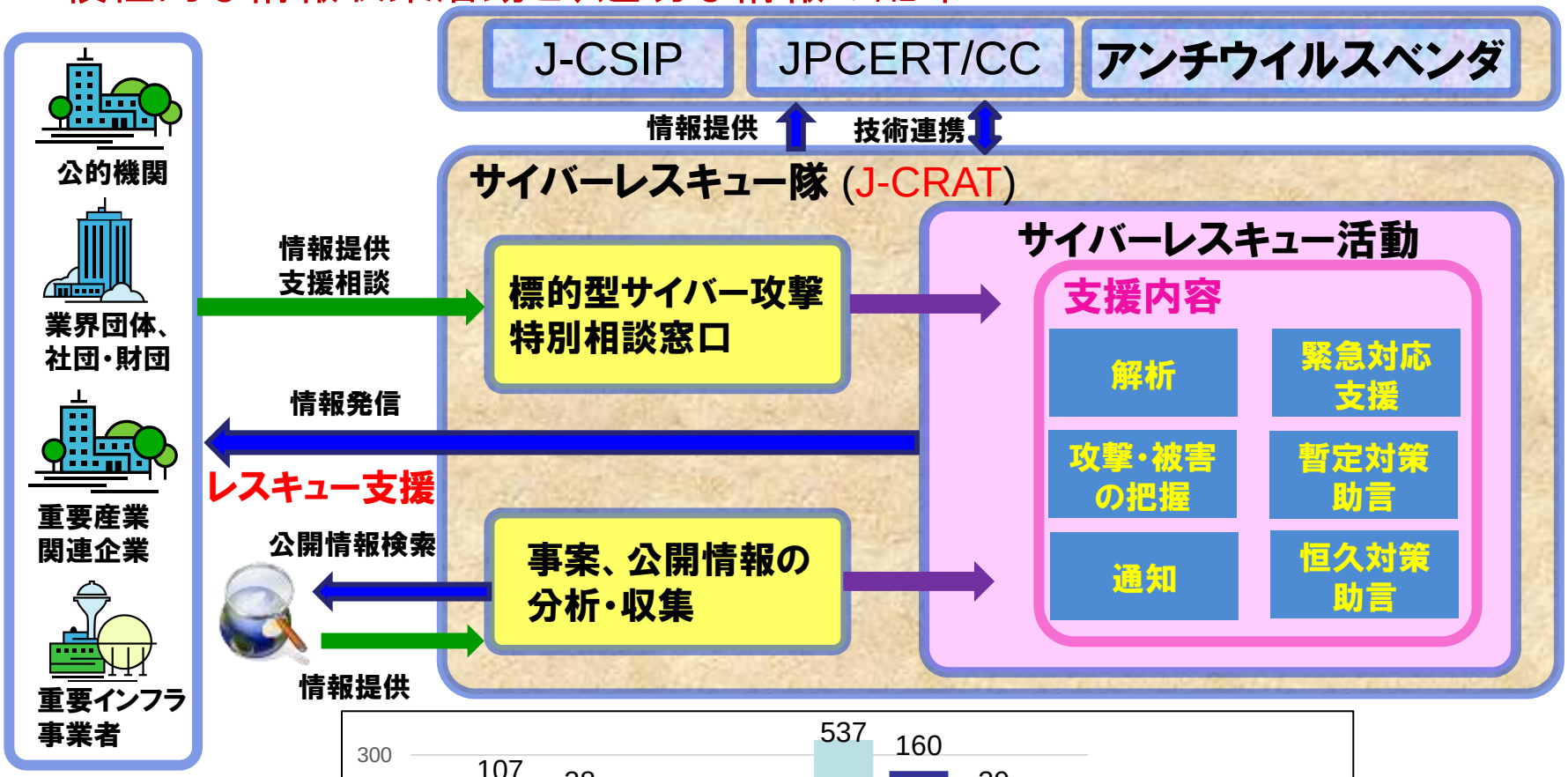
② 攻撃の連鎖を解明、遮断する



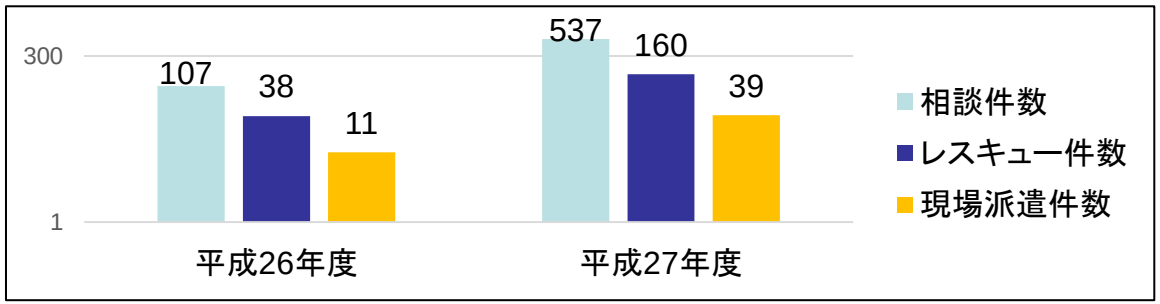
# サイバーレスキュー隊J-CRAT～早期対応の重要性～

IPA

✓ 積極的な情報収集活動と、適切な情報の配布

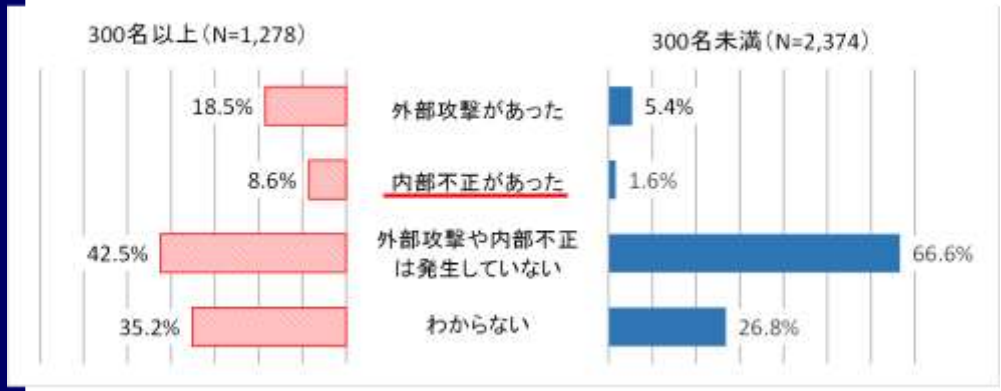



**J-CRAT 活動実績**



# 内部不正によるセキュリティインシデント

- 所属する企業組織で外部攻撃や内部不正が発生しているかどうか （報告書 P.12 図1）




- 故意ではない違反が多いが、故意も一定程度存在
（報告書 P.16 図10）


- 情報の持ち出しには、**USBメモリ**、**電子メール**が多く用いられる （報告書 P.19 表10を編集）
  - ➢ 組織での対策は**USBメモリ等の外部記録媒体に関する利用ルールの徹底**、および**利用制限**が有効と考えられる

| 項目 | 1位 | | 2位 | | 3位 | |
|---|---|---|---|---|---|---|
| 行為者 | システム管理者 | 23.5% | 技術者・開発者 | 22.1% | 経営層・役員 | 17.4% |
| 不正行為の動機 | 業務が忙しく終わらせるため持ち出した | 38.1% | 処遇や待遇に不満があった | 26.1% | 持ち出した情報や機材で転職を有利にしたかった | 16.7% |
| 対象情報 | 顧客情報 | 48.3% | 技術情報 | 36.9% | 営業計画 | 32.9% |
| 持ち出し手段 | USBメモリ | 53.0% | 電子メール | 28.9% | 紙媒体 | 18.8% |

故意の不正行為経験者のみ（n=98、「不正行為の動機」はn=84） 「不正行為の動機」以外は複数回答

- 経営者等が重要視していない対策が内部不正行為の抑止に有効（報告書 P.42 表13）

| 内部不正経験者 | | 対策 | 経営者・システム管理者 | |
|---|---|---|---|---|
| 順位 | 割合 | | 順位 | 割合 |
| 1位 | 50.0% | ネットワークの利用制限がある（メールの送受信先の制限、Webメールへのアクセス制限、Webサイトの閲覧制限がある） | 2位 | 30.3% |
| 2位 | 46.5% | 技術情報や顧客情報などの重要情報にアクセスした人が監視される（アクセスログの監視等を含む） | 4位 | 27.0% |
| 3位 | 43.0% | 技術情報や顧客情報などの重要情報は特定の職員のみがアクセスできる | 1位 | 43.9% |
| 4位 | 25.0% | 職務上の成果物を公開した場合の罰則規定を強化する | 12位 | 12.8% |
| 5位 | 23.5% | 管理者を増員する等、社内の監視体制を強化する | 11位 | 13.1% |

（内部不正経験者：n=200、経営者・システム管理者：n=1500）

# 新国家資格「情報処理安全確保支援士」

IPA

【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

**経過措置**
期間限定
現在登録申請受付中

**資格試験**
2017年春よりスタート

**登録簿へ登録**
（要申請）

- **登録情報の公開**
- **資格名称の使用**
- **講習受講**

### 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**

**経過措置対象者初回登録申請受付中！（2017年4月1日登録分）**

・受付期間：2016年10月24日（月）～ 2017年1月31日（火）消印有効
・対　　象：情報セキュリティスペシャリスト試験合格者
　　テクニカルエンジニア（情報セキュリティ）試験合格者

※経過措置対象者登録申請は、制度開始から2年間となります。経過措置期間終了後は、登録資格を失います。

# 中小企業への情報セキュリティ普及の取組み

〇中小企業のセキュリティの課題

〇中小企業の情報セキュリティ対策ガイドライン（第2版）

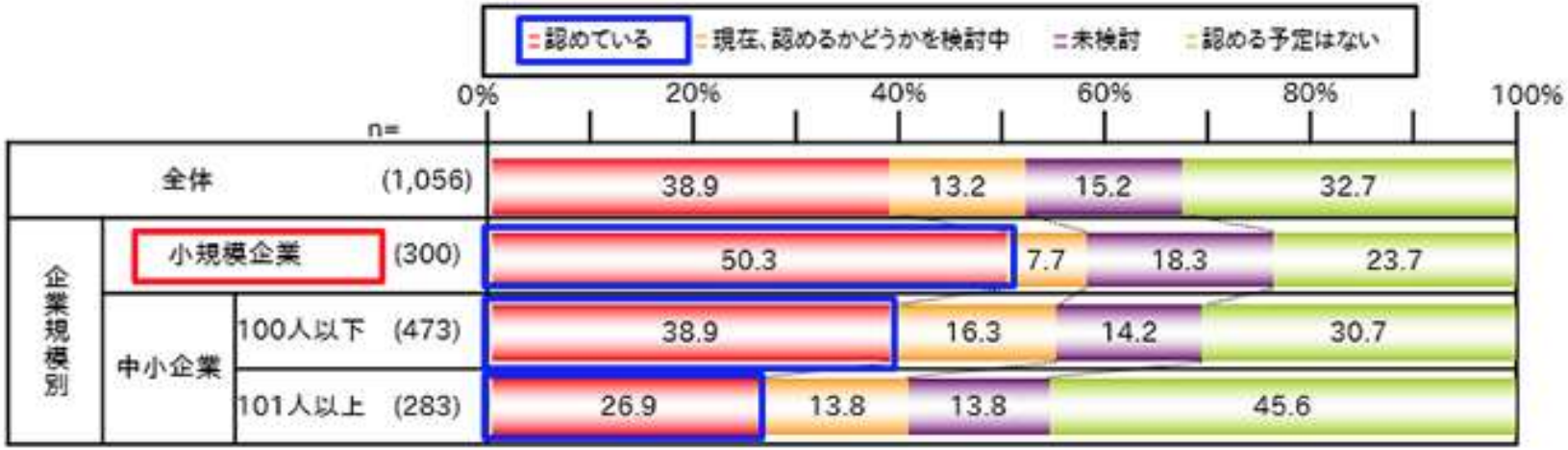
〇セキュリティプレゼンター制度

〇全国キャラバン

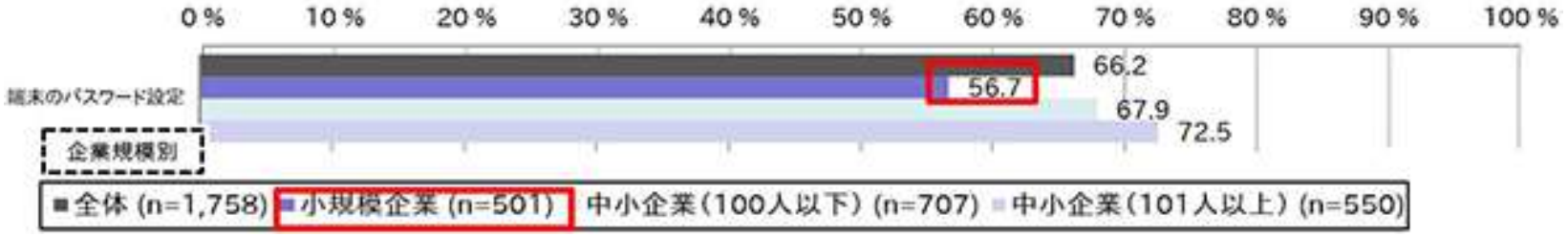
〇今後の取組み

# 中小企業のセキュリティの課題①（私用端末、PSの設定不足）

- 小規模企業の過半数（50.3%）が社員の私物のスマートフォンやタブレット端末の業務利用を認めている

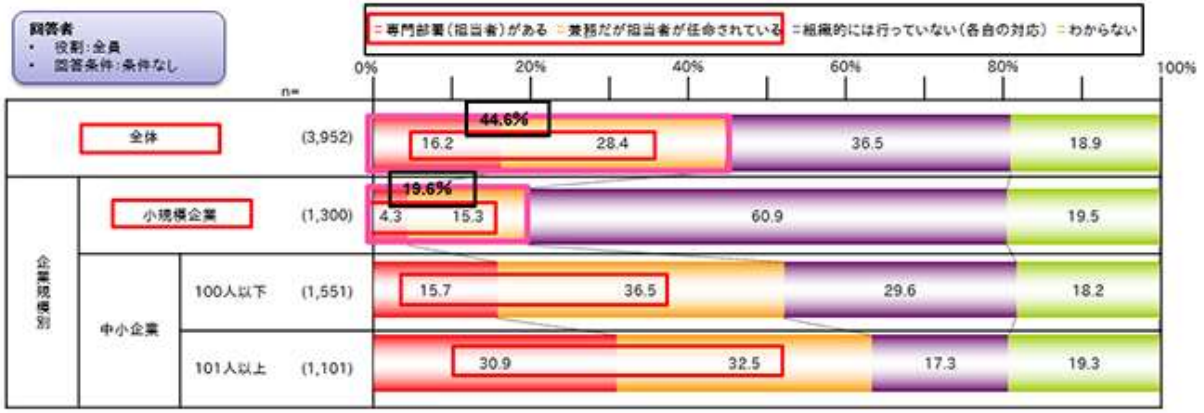



- その一方で、小規模企業の端末のパスワード設定の実施割合は56.7%と中小企業に比べて実施率が低い

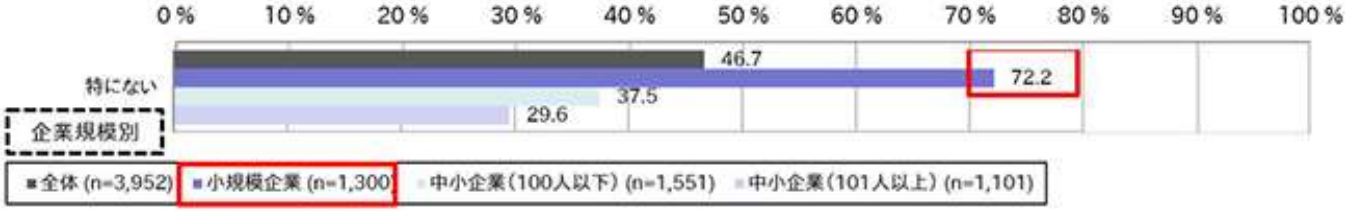


# 中小企業のセキュリティの課題②（担当者・相談先・教育なし）

「情報セキュリティ対策担当者がいる」: 44.6% （うち小規模企業19.6%）




「情報セキュリティの相談窓口なし」: 46.7% （うち小規模企業72.2%）




「情報セキュリティ教育の実施なし」: 58.2% （うち小規模企業80.9%）

# 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

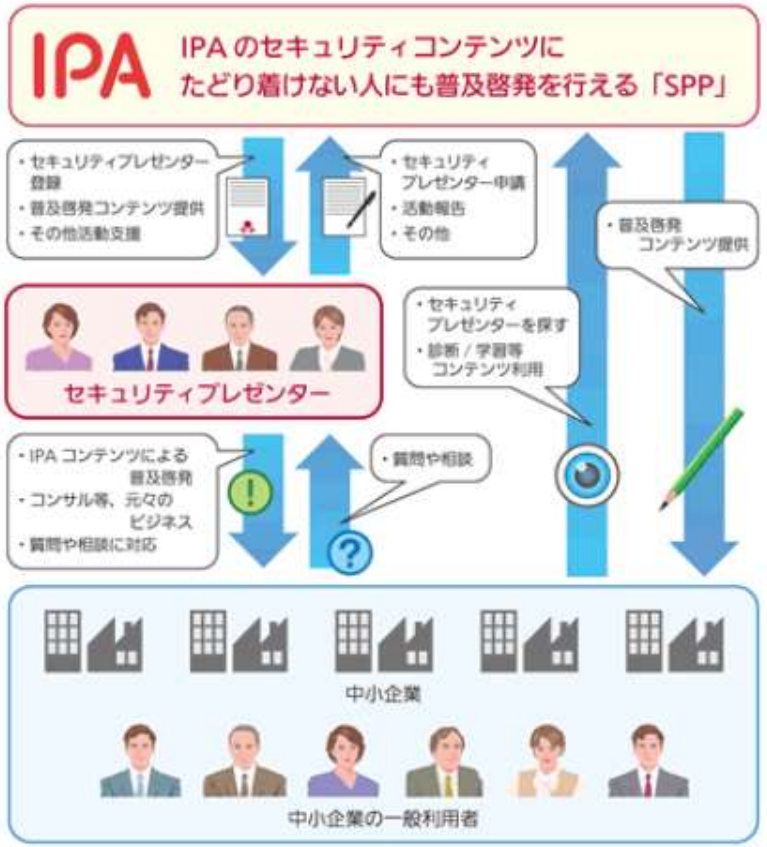
- 経営者への対策の必要性訴求。専任部門・担当が置けない企業を意識
- 導入のための実践手順、管理台帳等のひな型を提供
- クラウドサービス、スマートフォンをはじめとするモバイル端末の普及等、IT環境の変化への対応

| 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。<br>• 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<br>• 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。<br>• 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

# 「セキュリティプレゼンター」制度

- IPAが開発・作成した情報セキュリティコンテンツ等を使用し、企業に対して情報セキュリティの普及啓発を行う方にセキュリティプレゼンターとして登録いただき、その活動を支援。
  - コンテンツ等キットの提供
  - 専用サイトの利用
  - IPAサイトでご紹介
  - 限定イベントへの参加
  - 地域の講習会開催の支援




**登録者数 755名**（12/6現在）

ITコーディネータが約6割。そのほかに中小企業診断士など

# 全国キャラバンセミナー

## ● 講習能力養成セミナー

- 中小企業向けに、社内情報セキュリティ講習会の実施スキルを養成するためのセミナーを全国30カ所程度で実施予定。3万人程度の参加。

## ● セキュリティプレゼンターカンファレンス

- セキュリティプレゼンター（普及協力者）向けに、専門家育成のためのカンファレンスを全国8カ所で実施。スキルアップトレーニングを実施。

■講習能力養成セミナー概要

| | |
|---|---|
| 主催 | 独立行政法人情報処理推進機構 |
| 後援 | 日本商工会議所、全国商工会連合会、全国中小企業団体中央会、NPO法人ITコーディネータ協会、一般社団法人中小企業診断協会 |
| 日程 | 2015年7月～2016年1月 |
| 参加対象者 | 中小企業のIT・情報セキュリティ担当者、中小企業に対して情報セキュリティ対策を支援する者 |
| 開催概要 | 3.5時間（13:00～16:30）でセキュリティの最新動向を学ぶとともに、IPAの啓発ツールを使った社内講習会を実施できる能力を育成する |

■セキュリティプレゼンターカンファレンス概要

| | |
|---|---|
| 主催 | 独立行政法人情報処理推進機構 |
| 日程 | 2016年8月～12月（7回）、2017年2月（東京） |
| 参加対象者 | ・セキュリティプレゼンター登録者<br>・セキュリティプレゼンター登録を希望する中小企業支援者（ITコーディネータ、中小企業診断士等） |
| 開催概要 | 3時間（14:00～17:00）でセキュリティに関する支援スキルを習得し、地域における講習会講師として活動する能力を養成する |

## ● 研修会への講師派遣

- 商工会議所、商工会、よろず支援拠点等へ講師派遣（66カ所）

# 今後の取り組み

- 課題
  - “問題意識が低い”、“問題意識はあってもやり方がわからない”中小企業へのリーチ
  - 中小企業が自ら率先して取り組む仕組みづくり
- 商工団体等関係各団体とさらなる連携の強化を図り、中小企業への普及啓発活動を積極的に実施する
  - 全国商工会連合会、全国中小企業団体中央会、日本商工会議所、全国社会保険労務士会連合会、中小企業診断協会、日本税理士会連合会、ITコーディネータ協会、日本ネットワークセキュリティ協会、中小企業基盤整備機構

（団体種別毎の50音順）

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