IPA Better Life with IT

【公表予定】
資料6

サイバーセキュリティ対策

2017年6月14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
センター長　江口　純一

IPA/ISEC(セキュリティセンター)の使命と事業の支柱

【使命】
経済活動、国民生活を支える情報システムの安全性を確保すること

①ウイルス・不正アクセス及び脆弱性対策

- ウイルス・不正アクセスの届出・相談受付
- 脆弱性関連情報の届出受付・分析、提供
- 標的型サイバー攻撃への対応支援
- 重要インフラにおけるサイバーセキュリティ対策強化

②セキュリティの第三者認証

- IT製品のセキュリティ評価・認証制度（JISEC）（コモンクライテリア）
- 暗号モジュール試験認証制度（JCMVP）

③暗号技術

- 暗号アルゴリズムの安全性監視活動
- 暗号世代交代の普及促進

④情報セキュリティの分析活動

- 情報セキュリティ関連の社会経済的分析
- 情報セキュリティ白書
- 意識調査、被害実態調査

⑤普及啓発

- 情報セキュリティの普及、啓発
- 中小企業のセキュリティ対策強化
- 情報セキュリティ対策ベンチマーク

⑥独法監視・監査

- 独法等の情報システムの監視の実施
- 助言型の情報セキュリティ監査の実施

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

世界中でランサムウェア感染拡大

世界中で感染が拡大中のランサムウェア"Wanna Cryptor "
⇒Microsoft製品の脆弱性を悪用

2017年5月14日 「IPA 重要なセキュリティ情報」として緊急告知
2017年5月22日 感染実演デモ公開（IPA安心相談窓口だより）

図：感染した場合に表示される画面の一例

YouTube：ランサムウェア「WannaCry （WannaCryptor）」感染実演デモ

IPA安心相談窓口だより https://www.ipa.go.jp/security/anshin/mgdayori20170515.html

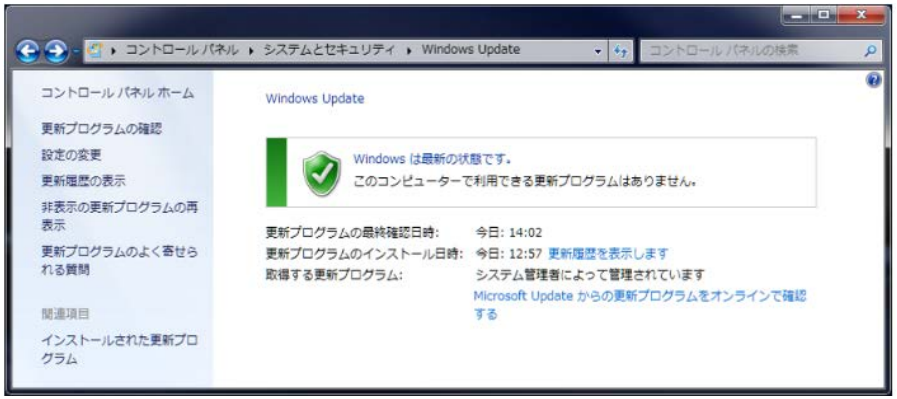
Wanna Cryptorの感染防止のために 今すぐWindows Updateを

Wanna Cryptorは、感染拡大を図る自己増殖型である。

- 脆弱性(Microsoft Windows の脆弱性) を悪用
- ネットワーク上に当該脆弱性が残る端末がないか探索

☒ 至急、下記の対策を実施してください。☒

- ✓ ネットワーク接続をしていない状態で必要なファイルをバックアップ
- ✓ ネットワークに接続し、Windows Updateを実行
- ✓ 更新プログラムが適用されたことを確認



Windows Updateが適用されている（最新の状態となっている）例

IPA安心相談窓口だより https://www.ipa.go.jp/security/anshin/mgdayori20170515.html

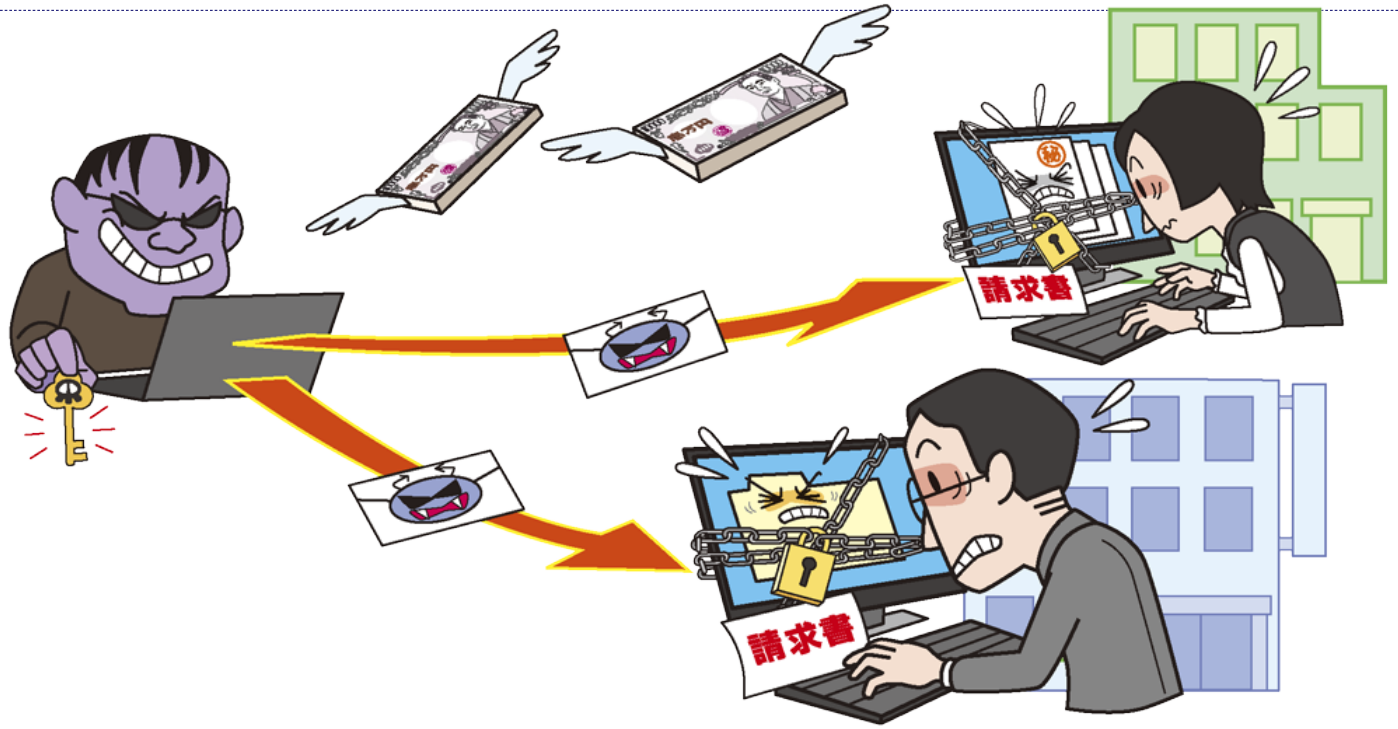
攻撃は忘れたころにやってくる

- WannaCry 以外の攻撃も続いています
  - 組織の10大脅威
    - 1位：標的型攻撃による情報流出
    - 3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
- 共通な手口に対して十分な備えを
  - 共通に使われるソフトウェア（OpenSSL、Apache Struts、WordPress等）の脆弱性の悪用
  - ウェブアプリケーションの脆弱性の悪用
  - リモート管理用のサービスからの侵入
  - 顧客情報の窃取やその情報の悪用

付録

【10大脅威2位】ランサムウェアによる被害

～ランサムウェアによる被害が急増～



- ランサムウェアにより、PC内のファイルが暗号化され、ファイルの復元に身代金を要求
- 2016年はランサムウェアの被害が急増している

【10大脅威2位】ランサムウェアによる被害

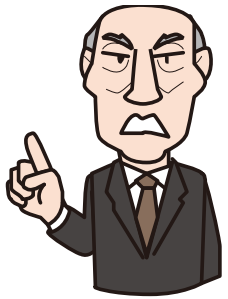
～ランサムウェアによる被害が急増～

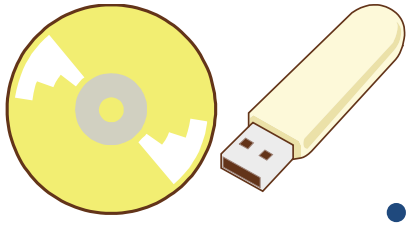
- 手口/影響
  - メールの添付ファイルやリンクからランサムウェア感染
  - ウェブからランサムウェアに感染（脆弱性等を悪用）
  - 感染したPCだけではなく、共有サーバー等別の機器にも影響
- 2016年の事例/傾向
  - ランサムウェアの日本語化・被害拡大
    - 検出されたランサムウェアの件数が2015年の9.8倍
    - その中には日本語表記のランサムウェアを確認
  - ランサムウェア復号ツールの登場
    - 暗号化されたファイルを復号するツールが登場し、万が一暗号化されてもファイルを復元できる可能性

【10大脅威2位】ランサムウェアによる被害

～ランサムウェアによる被害が急増～

- 対策一覧
  - 経営者
    - 組織としての対応体制の確立
      - 問題に対応できる体制（CSIRT等）構築
      - 予算の確保
      - セキュリティ対策の指示

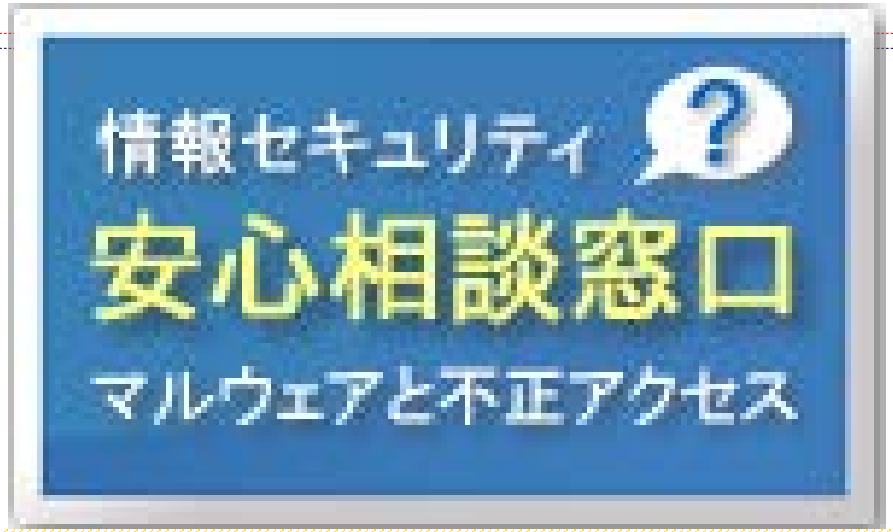




  - システム管理者
  - PC・スマートフォン利用者
    - 情報リテラシーの向上
      - 受信メール（添付ファイル・リンク）ウェブサイトの十分な確認
    - 被害の予防
      - OS・ソフトウェアの更新
      - セキュリティソフトの導入
      - フィルタリングツールの活用
    - 被害を受けた後の対策
      - バックアップからの復旧（自PCだけではなく、共有サーバーも）
      - 復元できるかの事前の確認
      - 復元ツール・機能の活用

定期的なバックアップ、併せて脆弱性対策もすることで安全に

情報セキュリティ安心相談窓口



電　話　**03-5978-7509**
(オペレータ対応は、平日の10:00～12:00 および 13:30～17:00)

E-mail　**anshin@ipa.go.jp**
※このメールアドレスに特定電子メールを送信しないでください。

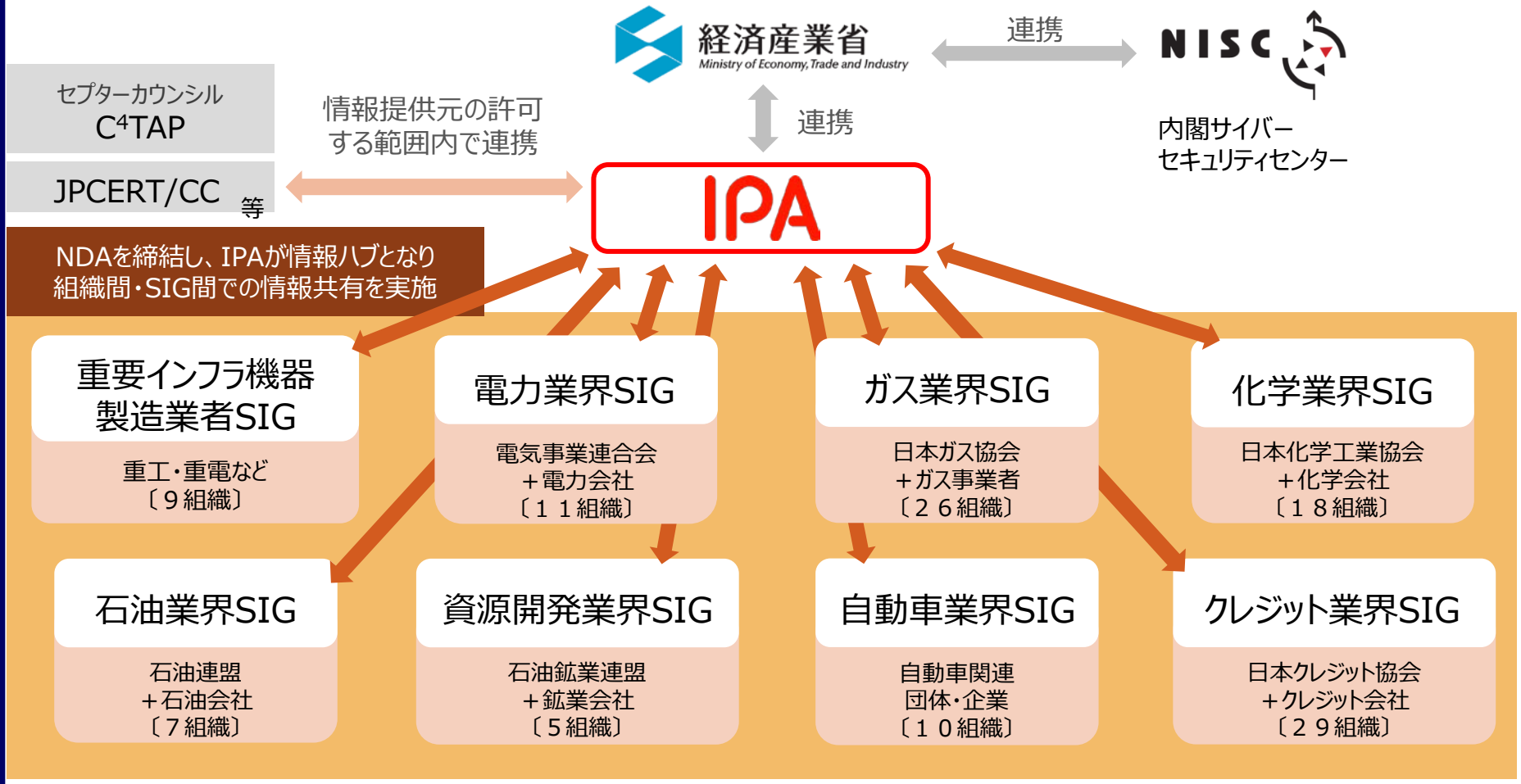
ＦＡＸ　**03-5978-7518**

郵　送　〒113-6591
東京都文京区本駒込2-28-8
文京グリーンコート　センターオフィス
IPAセキュリティセンター　安心相談窓口

J-CSIP ～情報共有の有効性～

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

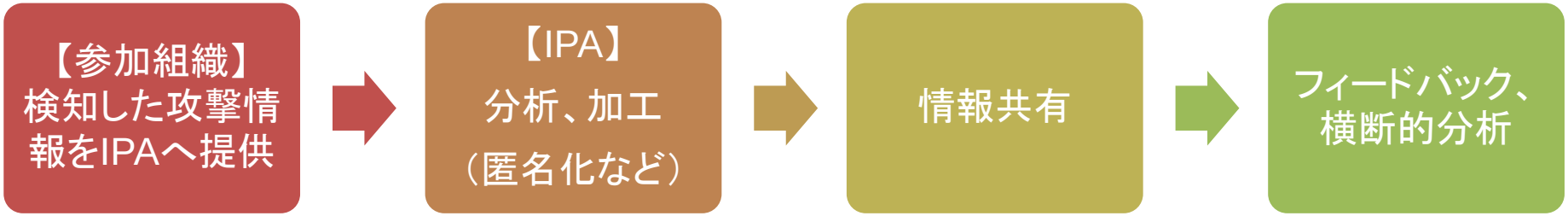
- 8つのSIG（Special Interest Group）、115の参加組織
- IPAとの間で秘密保持契約（NDA）を締結、各種関連機関とも連携



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）

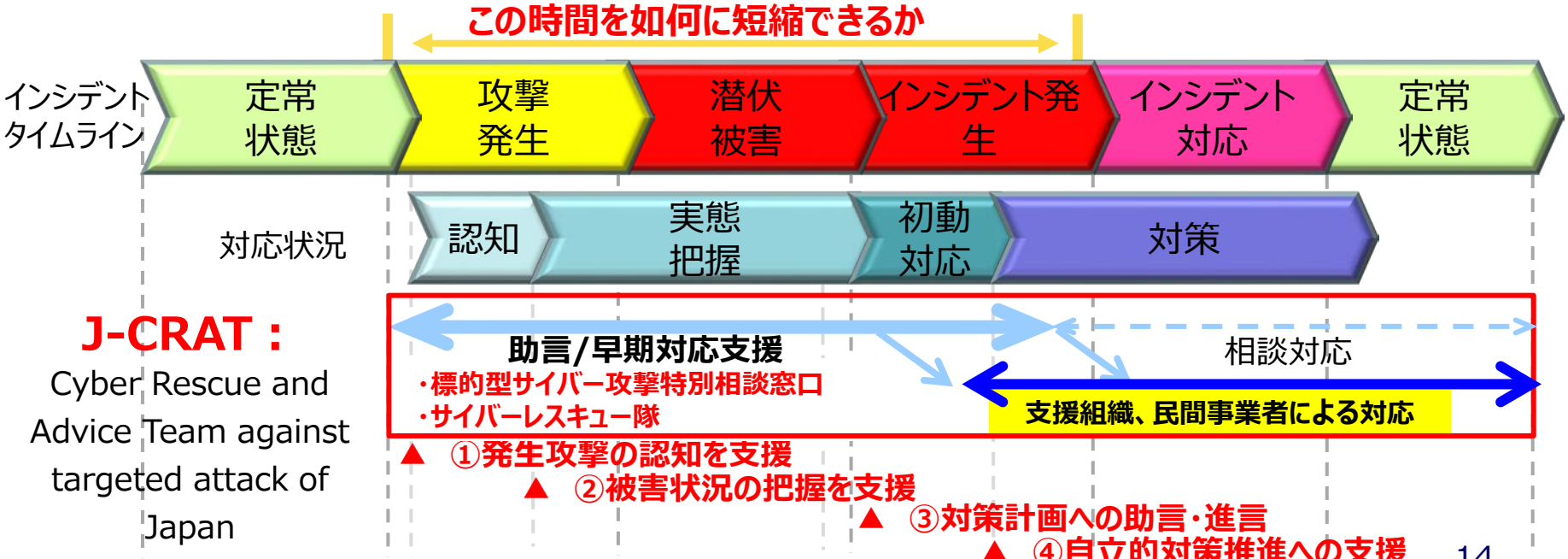
項目	2012年度	2013年度	2014年度	2015年度
IPAへの情報提供件数	246件	385件	626件	1,092件
参加組織への情報共有実施件数	160件	180件	195件	133件

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～

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

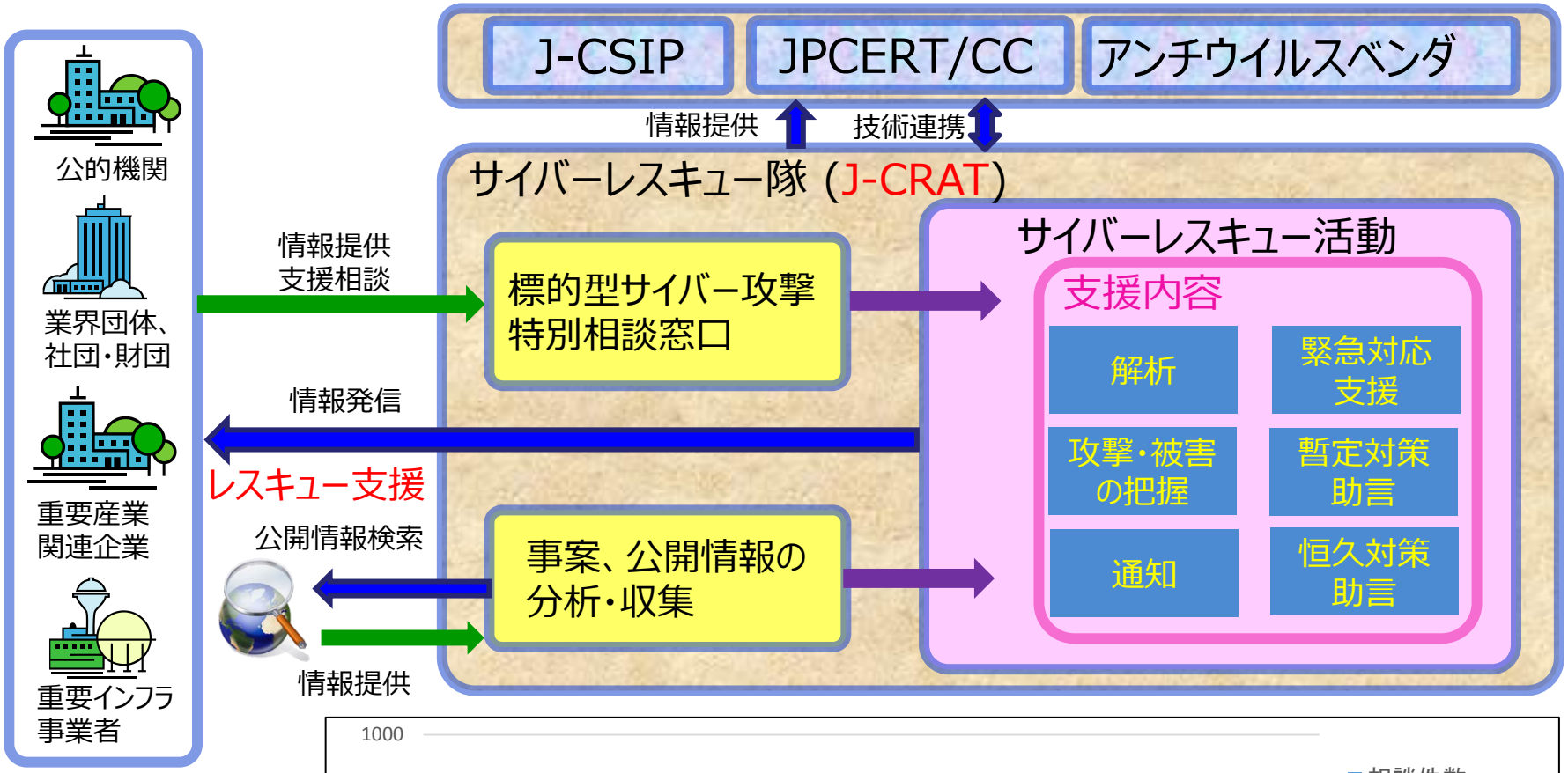
活動の目的： 標的型サイバー攻撃に対する相談対応、
事案によりレスキュー活動を実施することで、以下を達成する：
① 標的型サイバー攻撃被害の拡大防止、被害の低減を図る
② 攻撃の連鎖を解明、遮断する



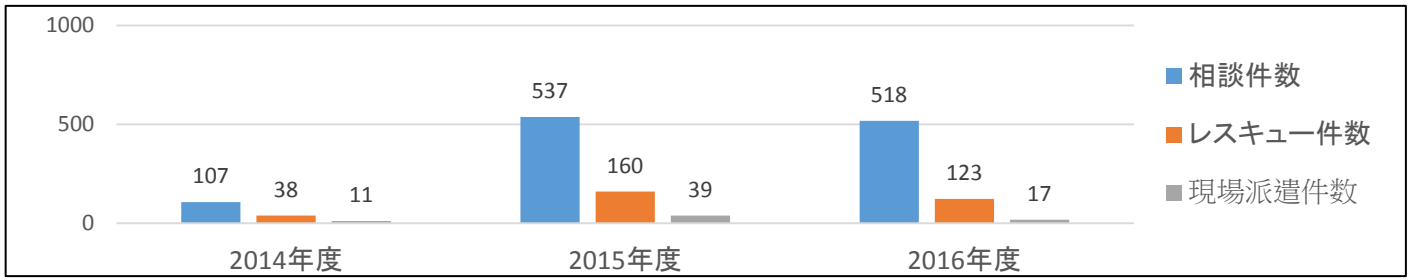
J-CRAT：
Cyber Rescue and Advice Team against targeted attack of Japan

サイバーレスキュー隊J-CRAT～早期対応の重要性～

✓ 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



2017年4月発足
産業サイバーセキュリティセンター

IPA

産業サイバーセキュリティセンターの事業内容

人材育成事業

●社会インフラ・産業基盤事業者において、自社システムのリスクを認識しつつ必要なセキュリティ対策を判断できる人材を育成するプログラムを提供。

●情報系システムから制御系システムまでを想定した模擬プラントを設置。専門家と共に安全性・信頼性の検証や早期復旧の演習を行う。

●最新の技術・ノウハウを学び、他業界のセキュリティ責任者や専門家、海外との連携を促進するコミュニティなどを創出する。

●海外との積極的な連携において、海外専門家との知見交流の場を創出し、グローバルな知見を蓄積していく。

●企業等の経営層に対して、サイバー攻撃の実態や産業サイバーセキュリティ対策の必要性を啓発するためのトレーニング提供・情報発信を行う。

3つの事業内容

実際の制御システムの安全性・信頼性検証事業

●我が国の社会インフラ・産業基盤に係る制御システムの安全性・信頼性に関するリスク評価を行う。

●あらゆる攻撃可能性を検証し、必要な対策立案を行う。

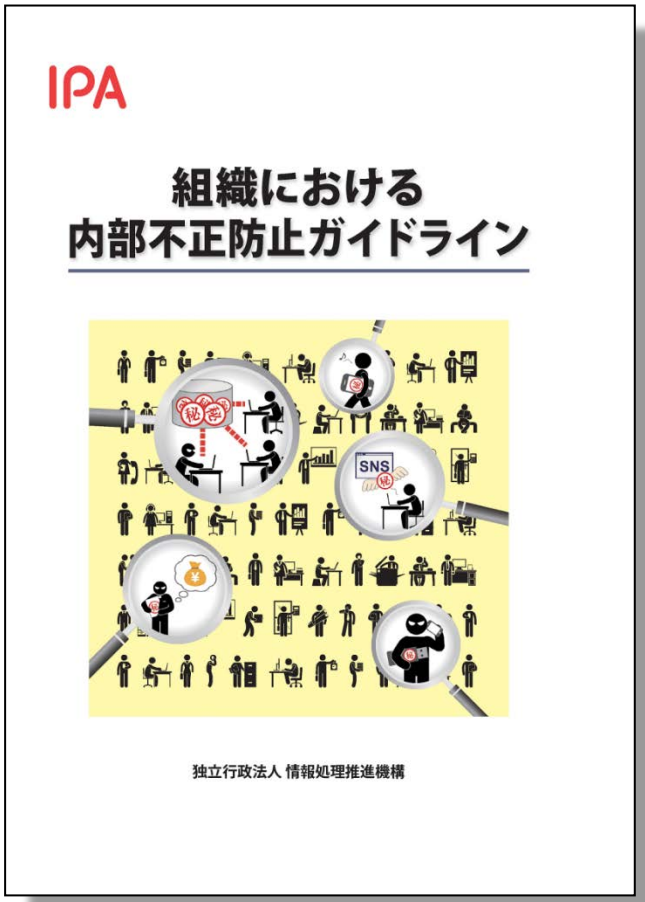
攻撃情報の調査・分析事業

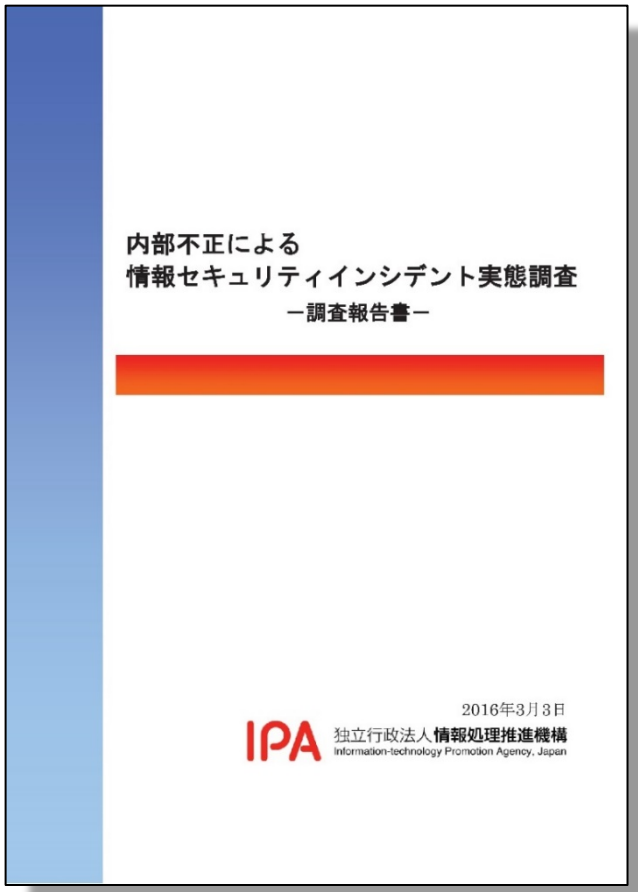
●最新のサイバー攻撃情報を収集。（例えば、おとりシステムの観察や民間専門機関が持つ攻撃情報を集積）

●新たな攻撃手法等を調査・分析し、人材育成事業やシステム検証事業に活用。

ガイドラインのご案内

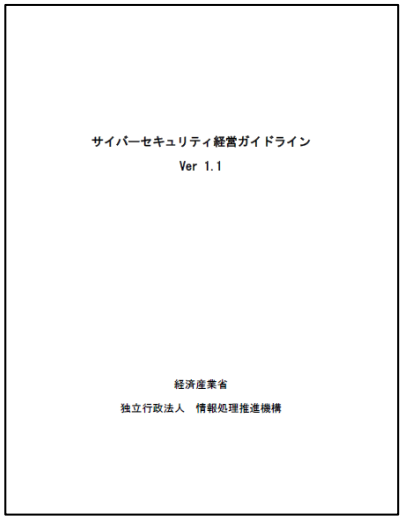
組織における内部不正防止ガイドライン（第4版）
内部不正による情報セキュリティインシデント実態調査





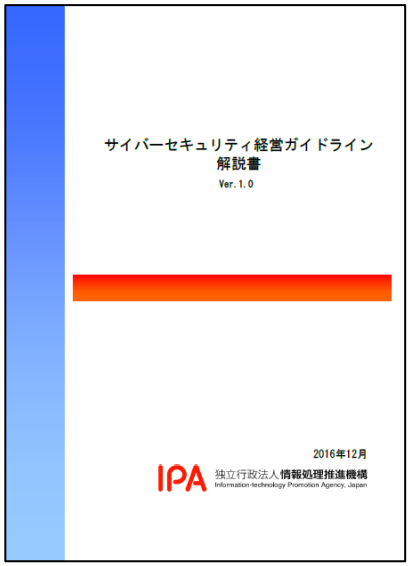
～組織における内部不正防止ガイドライン（2017年1月に第4版に更新（IPA））～
http://www.ipa.go.jp/security/fy24/reports/insider/index.html
～内部不正による情報セキュリティインシデント実態調査～
https://www.ipa.go.jp/security/fy27/reports/insider/

サイバーセキュリティ経営ガイドライン



- 経営者のリーダーシップによって対策推進
- 経済産業省とＩＰＡが策定（2015年12月）
  - ✓ 経営者が認識すべき３原則
  - ✓ 経営者がセキュリティの担当幹部（ＣＩＳＯ等）に指示をすべき重要１０項目

経済産業省のホームページからダウンロード可能
http://www.meti.go.jp/press/2015/12/20151228002/20151228002.html



IPAではガイドラインの解説書を公開

経営者のサイバーセキュリティの確保に向けた取り組みを推進
- ガイドラインの3原則と重要10項目の解説
- 仮想企業による取り組み事例の掲載
- サイバー攻撃による被害事例の一覧を作成

ＩＰＡのホームページからダウンロード可能
https://www.ipa.go.jp/security/economics/csmgl-kaisetsusho.html

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