



## 2016年度「分野横断的演習」について

内閣官房 内閣サイバーセキュリティセンター

# 分野横断的演習の実施経緯

## 第1次行動計画（2006～2008年度）

### 【目標】 官民連携の充実

官民連携の  
仕組みづくり

官民連携  
体制の  
機能向上

官民連携  
体制の  
実効性向上

年度	2006年度	2007年度	2008年度
人数	90名	120名	136名
テーマ	災害 災害に伴う IT障害の発生	意図的要因 サイバー攻撃 に伴う IT障害の発生	意図的要因 IT障害の発生 原因を関係者間の 情報共有で特定

## 第2次行動計画（2009～2013年度）

### 【目標】 重要インフラ事業者におけるBCP等の実効性の確認・問題点抽出

- ① 分野横断的な脅威に対する共通認識の醸成
- ② 他分野の対応状況把握による自分野の対応力強化
- ③ 官民の情報共有をより効果的に運用するための方策

年度	2009年度	2010年度	2011年度	2012年度	2013年度
人数	116名	141名	131名	148名	212名
テーマ	広域停電	大規模 通信障害	電力・ガス等の 重要インフラ 複合障害	電力・通信等の 重要インフラ 複合障害 + 便乗型IT インシデント	大規模な情報 セキュリティ インシデント

## 第3次行動計画（2014年度～2016年度）

### 【目標】 事業者等による情報セキュリティ対策の実施及び実効性の確認等を通じ重要インフラ全体の防護能力の向上を図る。

- ✓ 事業者等による障害対応能力の向上
- ✓ 重要インフラ全体の対策水準の底上げ
- ✓ 関係主体間の連携・維持の強化
- ✓ 国は事業者等の自律的かつ継続的な取組を支援

年度	2014年度	2015年度	2016年度
人数	348名	1,168名	2,084名
テーマ	IT障害発生時の対応に関する事項を軸とし、 情報共有を含む障害対応体制の実効性を検証		

## <事前説明会>

- 日程：2016年10月28日（金）、11月1日（火）、2日（水）  
場所：東京会場、地方会場（説明会の模様について、演習当日まで動画配信）  
内容：①重要インフラ防護施策の概要説明  
②分野横断的演習の事前説明  
③有識者による講演（「情報セキュリティの現状と課題」（金野委員））

規程類の事前確認、個別検証課題の確認・調整

## <演習当日>

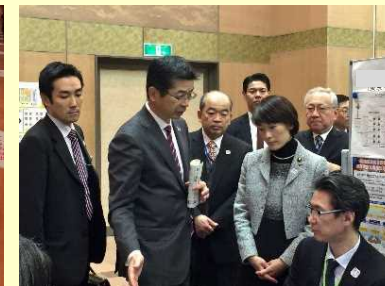
- 日時：2016年12月7日（水）12:15～17:00  
場所：東京会場、地方会場、自職場  
参加者：505組織2,084名  
【重要インフラ事業者等：13分野 合計446機関】  
【セプター：13分野18セプター】  
【政府機関 等】

### 演習内容：

- 第1部 各分野においてサービスへの影響が小さいIT障害が発生したケースを想定し、分野間・官民間での連携を図ることによる情報共有体制の実効性を検証。（ランサムウェア）
- 第2部 サービスへ影響が生じるIT障害が発生し、事業継続が脅かされるケースを想定し、事業継続計画の発動方法や、その手順を確認するなど、事態への対処を検証。（DDoS攻撃、OS脆弱性、制御システム）



演習の様様



丸川大臣による視察

演習を通じた内規・体制等の課題抽出

## <意見交換会>

- 日時：2017年1月24日（火）14:00～17:30  
場所：東京会場、大阪会場  
内容：①分野を超えた事業者間でのグループディスカッション  
②有識者による講演（「最近のサイバー攻撃の傾向と情報連携の促進」（真鍋委員））

他事業者等との情報共有を通じた改善の促進

- セキュリティ意識の高まりと多様なニーズに応える演習の企画
- 各事業者のセキュリティ対策に資する演習の運営

## 事前準備

### <参加募集>

- ✓ 複数の参加形態を活用した柔軟な参加モデルを提示  
(例:会場参加、自職場参加 等)
- ✓ 参加するプレイヤー選定に応じた社内の検証課題を例示

### <事前説明会／サブコン説明会>

- ✓ 東京会場、地方会場にて説明会を実施
- ✓ サブコンの配置のあり方について事例紹介し、サブコンの活用による演習効果の向上を促進  
(例:仮想1社、複数社に共通するサブコンの配置 など)



### <セプター訓練の実施>

- ✓ セプター訓練を本演習の前に実施し、分野内の情報共有体制における課題・改善事項を抽出

## 演習当日

### <演習取組み>

- ✓ 東京会場、地方会場、自職場間で相互に連携可能な演習環境を設営
- ✓ 多様な参加者への適合と、CSIRTアクションを盛り込んだシナリオ整備

### <見学会>

- ✓ 多数の見学参加を可能とする会場設営、時間割の設定
- ✓ 経営層向けの見学参加の呼びかけ、経営層向けの内容を含む講演の実施



## 事後の 振り返り

### <意見交換会>

- ✓ 東京会場、大阪会場にて分野横断的に編成されたグループをベースとしたディスカッションを実施
- ✓ セキュリティに関する対策や課題等に関する意見交換や人脈形成を促進



## 演習を踏まえた気づき(取組の視点)

- 演習参加を踏まえた**PDCAの日常的な実践**
- 組織内におけるセキュリティ対策の改善や必要なリソースの確保に関する**経営層による理解の促進**
- セキュリティ対策レベル、サービス内容等を異にする事業者が有する多様な**演習ニーズへの対応**
- 情報**共有**すべき具体的な**内容の再確認・徹底**

## 2017年度に向けた諸課題

### ➤ セキュリティ意識の高まりと旺盛なニーズに応える演習企画

- 地方会場(九州)の内容充実
- (例) □ 重要インフラ事業者の裾野拡大に加え、密接に関連する外縁の事業者の参加拡大
- 他関係機関や他演習／訓練との相互連携

### ➤ 各事業者のセキュリティ対策のPDCAに資する演習運営

- 経営者の理解／直接参加の増進
- (例) □ 見学会スタイルの在り方検討
- 最新の攻撃手法対策やCSIRT能力向上を目指したシナリオ整備

### ➤ 情報共有体制の実効性向上に係る施策

- 情報伝達ルートの有効性に関わる検証
- (例) □ プレイヤー以外の各主体に対する演習テーマの設定 (NISC／所管省庁／セプター事務局など)

### ➤ 演習運営ノウハウや知識等の還元

- 自社演習実施に資する演習ノウハウの還元
- (例) □ (E-learning等の仮想演習環境の検討)
- 国際対応 (海外組織への施策紹介)