資料４

# 総務省のサイバーセキュリティ政策の紹介

サイバーセキュリティ統括官室

令和２年５月13日

# Ⅰ. 政府情報システムのためのセキュリティ評価制度(ISMAP)

# Ⅱ. 実践的サイバー防御演習(CYDER)

# Ⅰ. 政府情報システムのためのセキュリティ評価制度（ISMAP）

# Ⅱ. 実践的サイバー防御演習（CYDER）

# クラウド・バイ・デフォルト原則



■ **2018年6月より、政府調達においてクラウド・バイ・デフォルト原則を採用**。

## 政府情報システムにおけるクラウドサービスの利用に係る基本方針

(2018 年6月7日 ＣＩＯ連絡会議決定)

2 基本方針

2.1 クラウド・バイ・デフォルト原則

政府情報システムは、クラウド・バイ・デフォルト原則、すなわち、クラウドサービスの利用を第一候補として、その検討を行うものとする。

クラウドサービスの安全性評価の必要性

## 未来投資戦略2018(2018 年6月15日 閣議決定　抜粋)

クラウドサービスの多様化・高度化に伴い、官民双方が一層安全・安心にクラウドサービスを採用し、継続的に利用していくため、情報資産の重要性に応じ、信頼性の確保の観点から、クラウドサービスの安全性評価について、諸外国の例も参考にしつつ、本年度から検討を開始する。

➡ 2018年８月より、**「クラウドサービスの安全性評価に関する検討会」**(座長：工学院大学名誉教授　大木榮二郎、事務局：総務省・経済産業省)を開催。

# 2019年度の政府決定



■ 成長戦略2019、デジタル・ガバメント実行計画において、2020年度内の制度利用開始を決定。

## 成長戦略(2019年)

(2019 年6月21日　閣議決定　抜粋)

５．スマート公共サービス
（２）新たに講ずべき具体的施策
ⅱ)行政機関におけるデジタルトランスフォーメーション(DX)の推進
② 国の行政機関における先進技術のさらなる活用
- 官民双方が一層安全・安心にクラウドサービスを採用し、継続的に利用していくため、**クラウドサービスの安全性評価制度について、2020年秋の全政府機関での利用開始に向け、2019年度中に実証を行いつつ、評価基準や制度を確立**する。

## デジタル・ガバメント実行計画

(令和元年12月20日 閣議決定　抜粋)

データの安全・安心・品質
3 デジタル・ガバメントの実現のための基盤の整備
3.3 行政機関におけるクラウドサービス利用の徹底
（２)クラウドサービスの安全性評価(◎内閣官房、◎総務省、◎経済産業省、全府省)

クラウドサービスの導入に当たっては、情報セキュリティ対策が十分に行われているサービスを調達する必要があることから、政府がクラウドサービスを導入する際の安全性評価基準及び安全性評価の監査を活用した評価の仕組みの導入に向けて、総務省及び経済産業省が連携し、クラウドサービスの安全性評価に関する検討会を設置して検討を進めている。

内閣官房、総務省及び経済産業省は、**2020 年度（令和２年度）内に、全政府機関において、上記の仕組みを活用して安全性が評価されたクラウドサービスの利用を開始できるよう**、引き続き、環境整備等について検討を進める。

# 2019年度の政府決定



■ サイバーセキュリティ戦略本部第２３回会合において、①本制度の基本的な枠組み、②本制度の利用の考え方、③本制度の所管と運営体制を決定。

**政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて**

令和２年１月３０日　サイバーセキュリティ戦略本部決定

**１．本制度の基本的な枠組み**

本制度で定められた評価プロセスに基づいて、要求する基準に基づいたセキュリティ対策を実施していることが確認されたクラウドサービスを、本制度が公表するクラウドサービスリストに登録。

**２．各政府機関等における本制度の利用の考え方**

各政府機関は、クラウドサービスを調達する際は本制度において登録されたサービスから調達することを原則とし、本制度における登録がないクラウドサービスの調達や、経過措置の詳細は、サイバーセキュリティ対策推進会議、各府省情報化統括責任者（CIO）連絡会議において定める。

**３．本制度の所管と運用体制**

本制度の所管は内閣官房（NISC、IT室）・総務省・経済産業省とし、本制度の最高意思決定機関として、有識者と所管省庁を構成員とした制度運営委員会を設置し、事務局をNISCに置く。

事務局は、本制度の運用状況について、サイバーセキュリティ戦略本部に報告を行う。

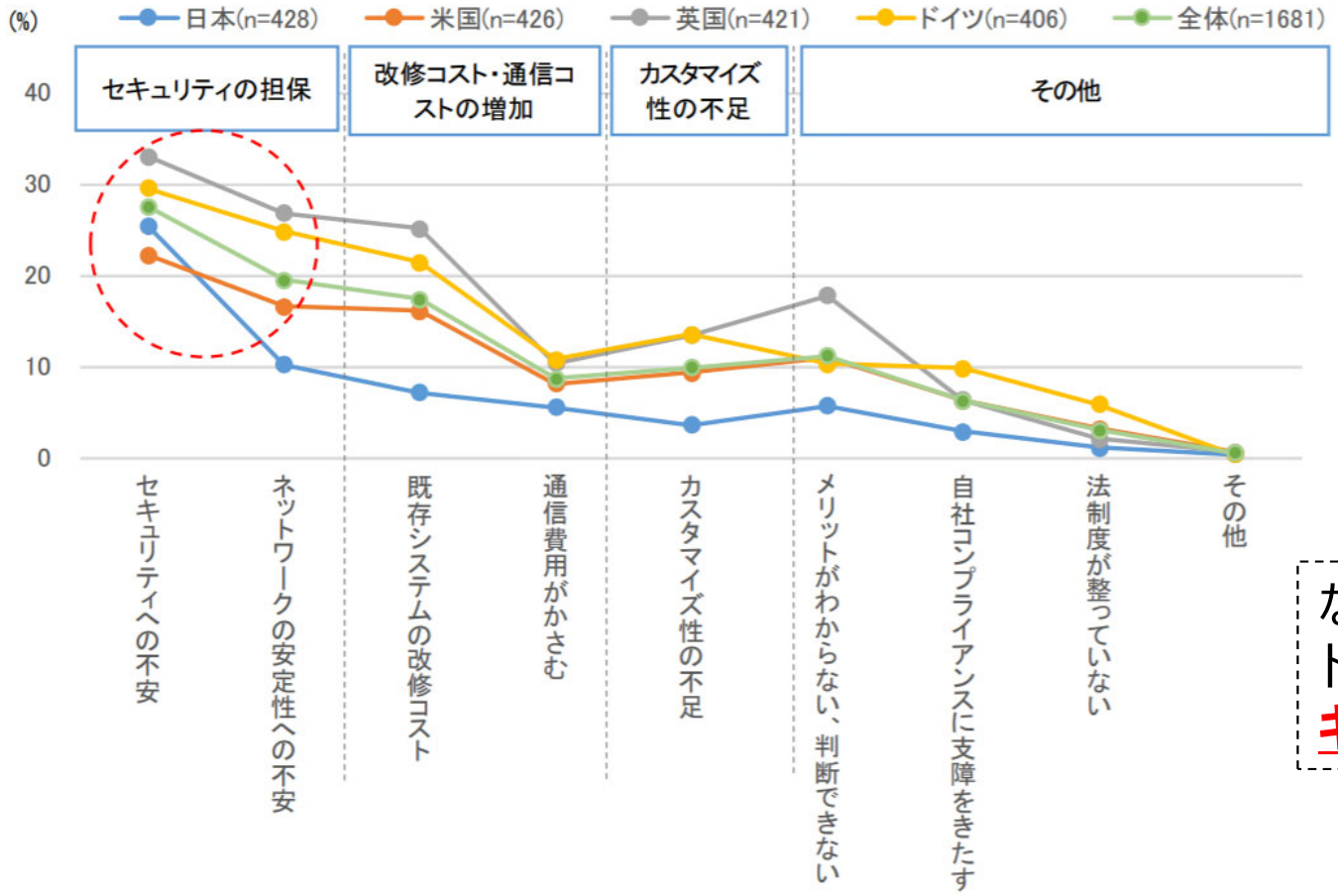
本制度の運用に当たっては、（中略）独立行政法人情報処理推進機構（以下「IPA」という。）において、制度運用係る実務及び評価に係る技術的な支援を行うものとする。ただし、IPAは制度運用のうち、監査機関の評価及び管理に関する業務については、（中略）情報セキュリティ監査制度及び監査機関の質の確保に精通した民間団体に、（中略）委託すること。

# 官民におけるクラウド利用の現状の課題



- クラウドサービスの導入における課題としては、官民ともにセキュリティ不安が最多。
- クラウドサービスの導入円滑化の観点から、セキュリティに対する統一的な評価を実施することが有効。特にセキュリティ確保が求められる政府の情報システムを念頭においた制度の構築が急務。

**クラウドサービス導入に対する課題の内容（民間向け調査）**




出典：2018年3月　三菱総合研究所
ICT によるイノベーションと新たなエコノミー形成に関する調査研究

なお、政府内での調査においても、クラウドサービス導入に係る**不安事項**として、**セキュリティ**を上げた者が最多であった。

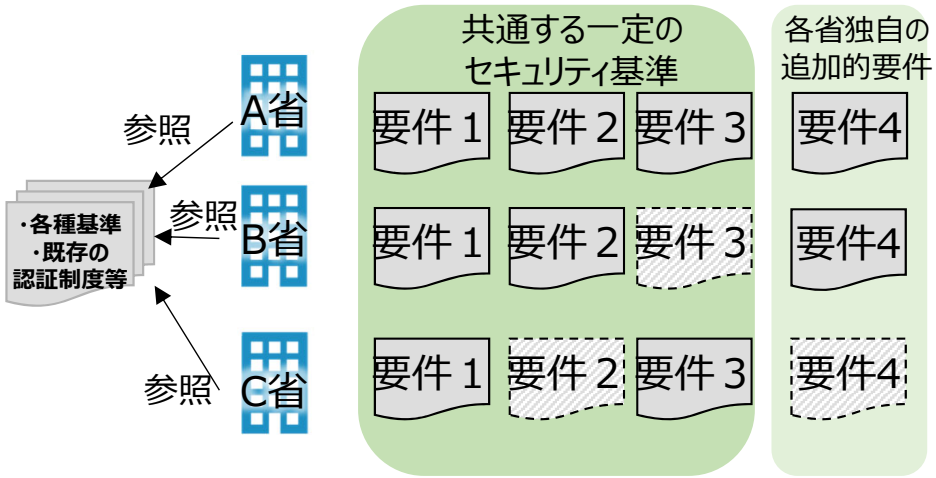
# ISMAPの目指す姿



■ クラウドサービスの導入に係る様々な方針やガイドライン等が存在するが、同じクラウドサービスに対して**各政府機関等が独自に、全てのセキュリティ要件を最初から確認することとなり、非効率**。

⇒**クラウドサービスについて、統一的なセキュリティ基準を明確化し、実効性・効率性のあるクラウドのセキュリティ評価制度(ISMAP：Information system Security Management and Assessment Program)を検討。**

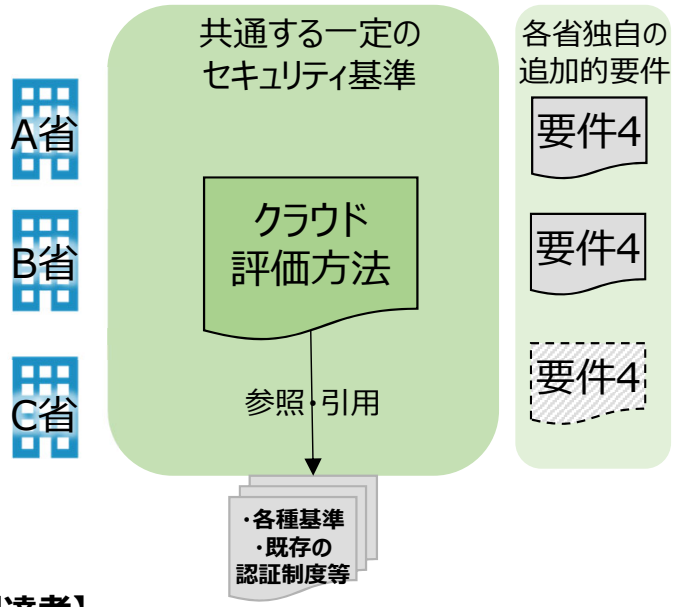
## 現状




**【調達者】**
- 各省が基準等を参照して最初から個別に要件を指定
- 調達担当によって、同じシステムでも要件の設け方にばらつきが生じ、必要なセキュリティ基準を必ずしも満たせていない可能性
- 各省共通の要件であっても、各々で確認しており非効率

**【提案者】**
- 同じ要件であっても、各省別個に審査を受ける必要があり非効率
- 政府調達におけるベースラインが不透明

## 目指すべき姿




**【調達者】**
- 各省はクラウド評価に追加的な要件のみを指定
- 評価済みであれば、一定のセキュリティ基準を充足可能
- 各省共通の要件を相互利用可能

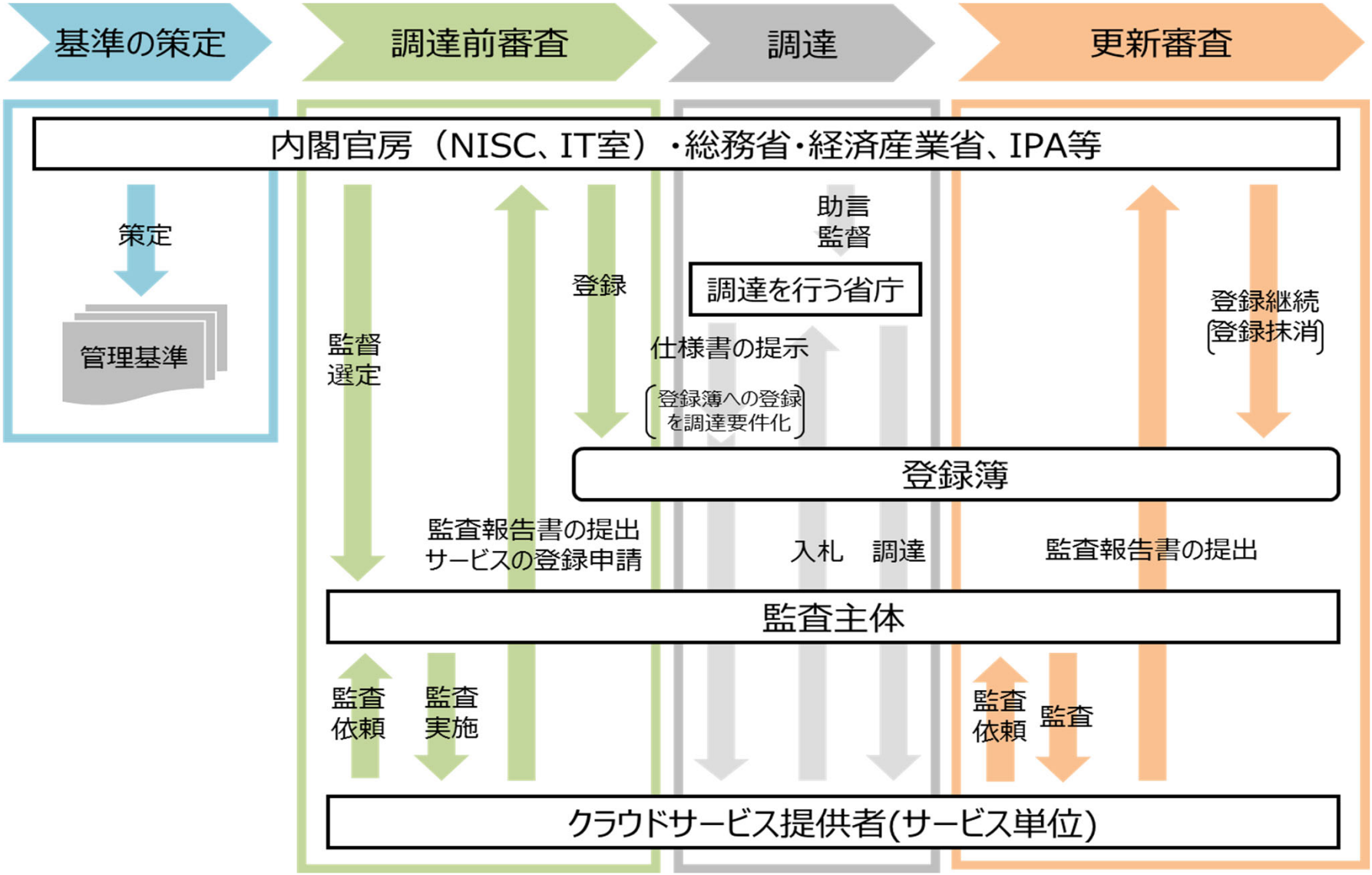
**【提案者】**
- 同じ要件について、一度の評価に共通化
- 政府調達におけるベースラインが透明化

※政府機関・情報システムは多岐にわたるため、共通するセキュリティ基準では不足している内容が存在しうる。その場合は各自共通水準に追加して評価することを想定。(上図の要件４)

# ISMAPの基本的流れ



- 本制度の基本的な枠組みは、**国際標準等を踏まえて策定した基準**に基づき、各基準が適切に実施されているか**監査するプロセス**を経て、サービスを登録する制度
- 各政府機関は、**原則、安全性が評価され「登録簿」に掲載されたサービスから調達。**



# 【参考】 管理基準のイメージ

- 管理基準は、**統制目標とされる3ケタ管理策（A.x.x.x）**と、それを達成するための手段となる**詳細管理策である4ケタ管理策（A.x.x.x.x）**で構成される。
- 原則、**３桁管理策を必須**、**4ケタ管理策は選択性**とし、一部の重要な管理策を必須とする。

**３桁管理策：統制目標** ※全て必須

| 管理策番号 | 管理策 |
|---|---|
| 8.1.2 | 目録の中で維持される資産は、管理する。 |
| 8.1.2.1 | 資産の管理責任を時機を失せずに割り当てることを確実にするためのプロセスにおいて、資産が生成された時点、又は資産が組織に移転された時点で、適格な者（資産のライフサイクルの管理責任を与えられた個人及び組織）に管理責任を割り当てる。 |
| 8.1.2.2 | 資産の管理責任者は、資産のライフサイクル全体にわたって、その資産を適切に管理することに責任を負う。 |
| 8.1.2.3 | 資産の管理責任者は、資産の目録を作成する仕組みを整備する。 |
| 8.1.2.4 | 資産の管理責任者は、資産を適切に分類及び保護する仕組みを整備する。 |
| 8.1.2.5 | 資産の管理責任者は、適用されるアクセス制御方針を考慮に入れて、重要な資産に対するアクセスの制限及び分類を定め、定期的にレビューする。 |
| 8.1.2.6 | 資産の管理責任者は、資産を消去又は破壊する場合に、適切に取り扱う仕組みを整備する。 |

**４桁管理策：手段** ※原則選択性。全て必須に規定してしまうと、動的な変化への対応が困難。

Ⅰ. 政府情報システムのためのセキュリティ評価制度（ISMAP）

# Ⅱ. 実践的サイバー防御演習（CYDER）

# 実践的サイバー防御演習（CYDER）

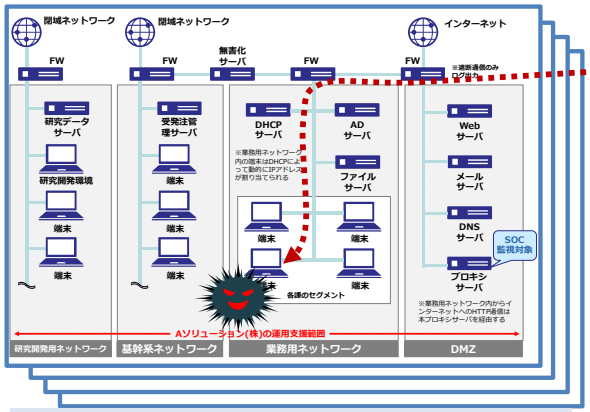


CYDER: CYber Defense Exercise with Recurrence

- 総務省は、情報通信研究機構(NICT)を通じ、**国の機関**、**指定法人**、**独立行政法人**、**地方公共団体**及び**重要インフラ事業者等**の情報システム担当者等を対象とした体験型の**実践的サイバー防御演習(CYDER)**を実施。
- 受講者は、**チーム単位で演習に参加。組織のネットワーク環境を模した大規模仮想LAN環境下で、実機の操作を伴って**サイバー攻撃によるインシデントの検知から対応、報告、回復までの**一連の対処方法を体験。**
- **全都道府県**において、年間**100回・計3,000名規模**で実施。
  ※平成29年度：年間100回・3,009名受講／平成30年度：年間107回・2,666名受講／令和元年度：年間105回・3,090名受講

## 演習のイメージ

**NICTの有する技術的知見を活用**し、サイバー攻撃に係る我が国固有の傾向等を徹底分析し、現実のサイバー攻撃事例を再現した**最新の演習シナリオ**をコースごとに用意。



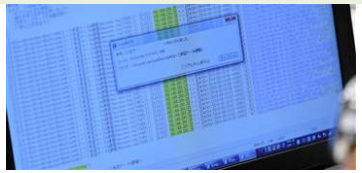

実際の**大規模LANを模した環境**を、**受講チームごと**に専用環境として**構築**

**擬似攻撃者**

NICT北陸StarBED技術センターに設置された大規模高性能サーバー群を活用

演習実施模様
専門の指導員による補助

**機材・データ**を使用して**本番同様の作業**を実施



**インシデント（事案）対処能力の向上**

## 令和元年度の実施状況

| コース | 受講対象組織 | 対象者 | 開催地 | 開催回数 | 開催時期 |
|---|---|---|---|---|---|
| Aコース（初級） | 全組織共通 | システムの運用担当者（システムの利用者レベルを含む） | ４７都道府県 | ６６回 | 6月～2月 |
| B-1コース（中級） | 地方公共団体 | セキュリティ管理業務を主導する立場の者 | 全国１１地域 | ２０回 | 9月～11月 |
| B-2コース（中級） | 国の機関等、重要インフラ事業者等 | | 東京・大阪・名古屋 | １９回 | 11月～２月 |

# CYDERの演習内容例



- 地方公共団体に対してサイバー攻撃が行われ、情報流出事案が発生した状況を実機を使って体験。
- 演習受講者は、仮想の市の情報担当職員として、迅速な調査や的確な報告・情報展開といった情報流出事案の対処方法について、演習を通じて体得。

## 演習の流れ

実機演習は1日で完結

### 事前学習（オンライン）

- オンラインで事前学習
- 最新のサイバー攻撃事案紹介
- 攻撃に利用されるツールや技術の紹介
- 演習で利用するネットワーク管理ツールや解析ツール等の説明

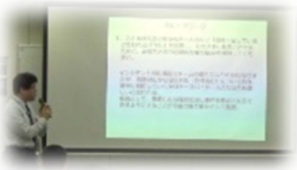
### 講義

- オンライン事前学習の振り返り
- サイバー攻撃対処の一連の流れの学習

### 演習

- 異常の検知、職員への注意喚起
- 不審なファイル解析、現状把握
- 状況のエスカレーション
- 内部感染の端末、原因の調査
- 情報漏洩報告

→ これら一連の作業を実機を用いて演習



### 振り返り

- 演習の振り返り、実機による作業確認
- 管理する際のポイントやベストプラクティス紹介
- 演習で学んだ結果や自組織へのフィードバックについてグループ発表

# 実践的サイバー防御演習（CYDER）の受講について



## 申し込み方法

https://cyder.nict.go.jp
から直接申し込みください。


※2020年度の演習日程確定や演習受付は
新型コロナウイルスの影響も踏まえ検討中です。

## よくある質問

### 受講者はどのような人か。

各組織の情報システム担当者やCSIRT要員の受講を想定しています。
※現に従事せずとも従事予定がある場合なども受講可能です。

### １人でも参加可能か。

組織当たり１名でも複数名でも参加可能です。人数制限はありません。
※他組織の参加者とチームになり4名1組で演習を実施します。1組織4名でのチーム参加も可能です。

### システム管理は外部委託しているが受講する意味があるのか。

インシデント発生時に委託先がどのような作業を実施しているかを予め理解・把握しておくことで、円滑な対応につながるため受講を推奨しています。
※なお、外部委託先が参加する場合（派遣労働者として指揮命令を受けている場合を除く。）は、民間事業者扱いとなるため有料での参加となります。

### 初級(Aコース)と中級(Bコース)の違いは何か。

初級は、これからネットワーク業務に従事するなど、サイバーセキュリティの基礎知識がない場合でも参加可能です。
※初級はステップ・バイ・ステップ形式で、指導員の手厚いサポートを含めた演習となります。
中級は、コンピューターとネットワーク（WindowsとTCP/IP）及びサイバーセキュリティに関する基礎知識を有する方を想定しています。
※中級では、簡易なログ解析や、ファイアウォール設定変更等を含んだ演習となります。

### 実機を使用する演習はハードルが高いのではないか。

演習前にオンライン教材を利用して学び、演習中は専門の指導員が補助します。無料で受講可能ですので、一度参加いただければと思います。

### NISCが実施する分野横断的演習とは異なるのか。

分野横断的演習は、情報共有体制の実効性検証等を主題としており、実機での操作演習を主題とするCYDERとは内容は全く異なります。
※分野横断的演習の参加有無に関わらずCYDERを受講いただくことをお願いしています。