資料４－２

# 総務省におけるサイバーセキュリティ施策の取組状況について

2023年３月

総務省サイバーセキュリティ統括官室

# （１）通信障害の発生を踏まえた対応

# 通信事故が多発する構造的要因と新たな取組



**事故発生**

| | |
|---|---|
| KDDI（7月2日）<br>重大事故 | NTT西日本（8月25日）<br>重大事故 |
| KDDI（8月24日）<br>事故 | 楽天モバイル（9月4日）<br>重大事故 |
| NTTドコモ（12月17日）<br>重大事故 | NTTドコモ（12月20日）<br>重大事故 |

→ 個別事案の対応

**今後の新たな事故**

事 故　事 故
事 故　事 故

個別事案の対応では今後の潜在的な事故発生を防げない

## 事故が多発する構造的な課題

①通信設備が抱える**潜在的リスクの洗い出し不足**　②システムの**保守・管理態勢及び社内情報共有体制の不備**

③**教育・訓練の不足**　④利用者への**初報の遅れ**　⑤**事業者間連携による対策の不足**　等

## 新たな取組

■ **構造的な課題に対応し、連続する事故の根源を改善させるため、新たに以下の取組みを行う。**

### 1.構造問題検証

**構造的問題に踏み込んだ検証**　【年度内に報告書をとりまとめ】

✓ KDDI、NTT西日本、楽天モバイルNTT等に対して、電気通信事故検証会議において、個別の事故の背景にある組織・体制面等の構造的問題を含め検証を行い、適切なモニタリングのルール等について検討を行う。

### 2.利用者利益保護

**利用者に対する周知広報の強化**　【本年１月に報告書をとりまとめ、年度内にガイドライン策定】

✓ 事故発生時において電気通信事業者が行うべき周知広報の内容及び情報伝達手段の多様化、関係機関等に対する緊急連絡体制等について環境整備を行う。

### 3.代替手段確保

**非常時における事業者間ローミング等の実現**　【昨年12月に第１次報告書をとりまとめ済み】

✓ 非常時における通信手段の確保に向けて、携帯電話の事業者間ローミングの導入方策等について検討。

# 通信事故の背景にある構造的問題への対応



- ✓ 最近、大規模な電気通信事故が多発。その背景にある**保守運用態勢に対するガバナンスの不足等、共通する課題（構造的問題）について、令和４年12月より電気通信事故検証会議において検証開始。2月22日(水)に報告書案を取りまとめ**、意見公募を経て、**年度内に報告書を決定する**予定（※下記**赤字①～⑦等を新たに導入**する予定）
- ✓ 当該結果を踏まえ、総務省において、**今春以降、省令**（電気通信事業法施行規則、事業用電気通信設備規則）**の改正等、必要な制度の見直しを行う**予定。

## 電　気　通　信　事　業　者

### 設備故障リスク対策

- 設備管理の方針
- 情報セキュリティ対策
- ソフトウェアの信頼性確保
- ふくそう対策
- ③設備におけるリスク管理・リスクの洗い出し
- ④予備系設備への切替え不能時等の対処　等

### 人的リスク対策

- 法令遵守
- 統括管理者・責任者等の職務
- 組織内外の連携
- ⑤メンテナンス訓練・復旧訓練
- ⑥ヒューマンエラー防止対策
- ⑦適切な利用者周知　等

**(委託先含む)対策を実行する態勢等（ヒト,モノ,カネ,組織等）**

①経営層による実行状況・態勢等への点検義務

**経営層によるガバナンス**

②事業者による点検結果へのモニタリング

**行政による外部モニタリング**

※当面の間、電気通信役務を提供する指定公共機関である、NTT東西、NTTドコモ、NTTコミュニケーションズ、KDDI、ソフトバンク、楽天モバイルの７者を対象とする予定

# 電気通信サービスにおける障害発生時の周知・広報に関するガイドライン



✓近年、社会のデジタル化が進展しており、通信障害が社会全体に与える影響も増大。

✓このため、電気通信分野における周知広報等の在り方について検討するため、**昨年10月から「電気通信事故検証会議　周知広報・連絡体制WG」を開催**し、**本年1月に報告書が取りまとめられた。**

✓本取りまとめを踏まえ、**事業者による自主的なガイドラインに代わり、総務省において新たにガイドライン案を策定**し、意見公募手続きを経て、**3月に「電気通信サービスにおける障害発生時の周知・広報に関するガイドライン」として決定**した。

## 電気通信サービスにおける障害発生時の周知・広報に関するガイドライン

① 指定公共機関※は、**事故等の発生後、原則30分以内にHPで初報を公表。**
**総務省にも原則30分以内に連絡**、緊急通報受理機関等には、初報の公表後速やかに連絡。

② 事故の発生日時、影響を受ける地域・サービス、原因、復旧見通し等に加え、「**代替的に利用可能な通信手段とその利用方法**」等についても周知。

③ 災害時等においては、**障害発生後、遅くとも数日以内に復旧見通しを示す**。

④ 通信障害情報等は、**トップページのわかりやすい位置で常時掲載。障害時は**少なくとも**１時間ごとを目安に情報更新。**

⑤ ホームページ、SNS、デジタルサイネージ、報道機関との連携等、**多様な媒体で情報提供を行う。**

⑥ **周知・広報で使用する用語については、用語集を踏まえて記載。**利用者の体感に基づく平易な言葉を使い、利用者目線の丁寧な説明及び情報発信を徹底する。（例：流量規制⇒通信の制限、輻輳⇒通信の集中等）

※電気通信分野では、NTT持株、NTT東西、NTTドコモ、NTTコミュニケーションズ、KDDI、ソフトバンク、楽天モバイルの８者

# 非常時における事業者間ローミング等に関する検討会　第１次報告書の概要



## １．基本方針等

- 携帯電話事業者（NTTドコモ、 KDDI、ソフトバンク、楽天モバイル、沖縄セルラー電話）は、一般の通話やデータ通信、緊急通報機関からの呼び返しが可能な**フルローミング方式による事業者間ローミングをできる限り早期に導入**する。
- 事業者間ローミングは、**被災事業者のコアネットワーク（加入者データベース等）の機能に障害が起きていない場合**において、**他の全ての事業者が設備容量の逼迫が起きない範囲で運用**することとし、**今後、作業班で具体的な運用ルールを検討**する。

  ➢ 昨年１２月に作業班を設置し、運用ルール（ローミング開始・終了の条件等）や導入費用、スケジュール等について検討。
  ➢ 運用ルールは総務省のガイドラインとして策定する。

- コアネットワークに障害が発生した場合においては、事業者間ローミングの実施に限界があることから、複数SIM対応端末の利用等、**ローミング以外の非常時の通信手段の利用を利用者に促す**。
- **MVNOの利用者**に対してもローミングサービスを**同様に提供**する。
- 回線の切り替えに必要な端末操作等に関して、**利用者に対する丁寧な周知広報の方策を検討**する。
- 事業者間ローミングの公共性に鑑み、**公的支援の可能性について検討**する。
- **IoTサービスやテレマティクスサービス等**についてもローミングにより**サービスが維持**されるように取り組む。

## ２．継続課題

次の項目について、引き続き検討会において議論を進め、**本年６月頃までに第２次報告書を取りまとめ**。

- コアネットワークに障害が発生し、緊急通報機関からの呼び返しができない場合の**「緊急通報の発信のみ」を可能とするローミング方式の導入**
- **事業者間ローミング以外の通信手段**（複数SIM対応端末、公衆Wi-Fi、衛星通信、HAPS等）に関する**事業者や関連団体の取り組みのフォローアップ**
- フルMVNOの事業者間ローミングへの参加に向けた**フルMVNO・MNO間のローミングの枠組み**

# （２）その他施策

# 実践的サイバー防御演習（CYDER）



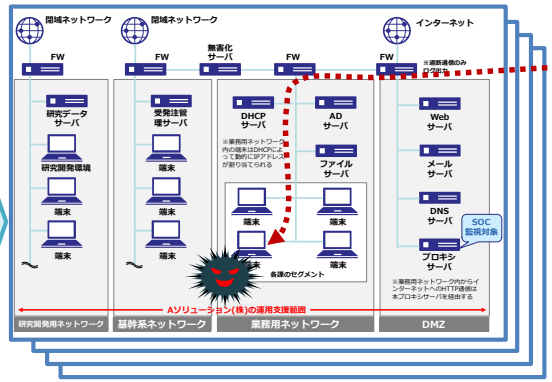
CYDER: CYber Defense Exercise with Recurrence

- 総務省は、NICTにおいて、**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、**外部のセキュリティ事業者の支援を受けることを前提とし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3000名規模**で実施。
  ※2017年度:100回・3009名、2018年度:107回・2666名、2019年度:105回・3090名、2020年度:106回・2648名、2021年度: 105回・2454名、2022年度: 108回・3327名

## 演習のイメージ

我が国唯一の情報通信に関する公的研究機関である**NICTが有する最新のサイバー攻撃情報を活用**し、実際に起こりうるサイバー攻撃事例を再現した**最新の演習シナリオ**を用意。

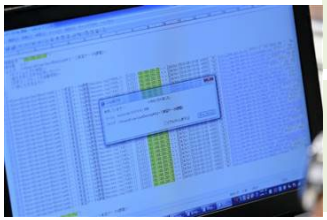
北陸StarBED技術センターの大規模高性能サーバ群を活用




**擬似攻撃者**

企業・自治体の**社内LANや端末を再現**した環境で演習を実施

**受講チームごと**に独立した演習環境を**構築**



演習模様 **専門指導員**による補助

チーム内での議論を通じた相互理解

**本番同様のデータ**を使用した演習

**インシデント（事案）対処能力の向上**

## 2022年度の実施状況

| コース名 | 演習方法 | レベル | 受講想定者（習得内容） | 受講想定組織 | 開催地 | 開催回数 | 実施時期 |
|---|---|---|---|---|---|---|---|
| A | 集合演習 | 初級 | システムに携わり始めた者<br>(事案発生時の対応の流れ) | 全組織共通 | ４７都道府県<br>※出前、サテライト形式も試行 | ７２回 | ７月～翌年２月 |
| B-1 | | 中級 | システム管理者・運用者<br>(主体的な事案対応・ｾｷｭﾘﾃｨ管理) | 地方公共団体 | 全国１１地域 | ２０回 | 10月～翌年１月 |
| B-2 | | | | 地方公共団体以外 | 東京・大阪・名古屋・つくば | １３回 | 翌年１月～２月 |
| C | | 準上級 | セキュリティ専門担当者<br>(高度なセキュリティ技術) | 全組織共通 | 東京 | ３回 | 10月～翌年２月 |
| オンライン標準 | ｵﾝﾗｲﾝ演習 | 初級相当 | システムに携わり始めた者<br>(事案発生時の対応の流れ) | 全組織共通 | (受講者職場等) | 随時 | ５/24～７/19 |
| オンライン入門 | | 入門 | | | | | 翌年1/17～３/2 |

# 情報通信ネットワークにおけるサイバーセキュリティ対策分科会



## 目的

- サイバー空間があらゆる主体が利用する公共空間となり、デジタル化を支える情報通信ネットワークは、今や国民生活や経済活動の重要かつ不可欠な基盤となっている中、サイバー攻撃により情報通信ネットワークの機能に支障が生じた場合には、社会・経済に多大な影響を及ぼすおそれがあり、その安全性・信頼性の確保は喫緊の課題。
- 本年８月にとりまとめられた「ICTサイバーセキュリティ総合対策2022」を踏まえ、依然としてIoT機器を狙ったサイバー攻撃が多く発生している状況等に対応するため、NOTICEや「電気通信事業者による積極的なサイバーセキュリティ対策に関する総合実証」等の取組みを含めた情報通信ネットワークにおけるサイバーセキュリティ対策について検討を行うことを目的として、「サイバーセキュリティタスクフォース」の下に分科会を設置。

## 主な検討事項

- IoTにおけるサイバーセキュリティの確保に向けた取組（NOTICE等）の現状と課題
- 情報通信ネットワークにおけるサイバーセキュリティ対策の現状と課題（総合実証の検討等）
- 上記課題の解決に向けた必要な方策

## 構成員

| | | | |
|---|---|---|---|
| 後藤　厚宏 | 情報セキュリティ大学院大学　学長 | 井上　大介 | NICTサイバーセキュリティ研究所 サイバーセキュリティネクサス長 |
| 河村　真紀子 | 主婦連合会　会長 | 小塚　荘一郎 | 学習院大学法学部　教授 |
| 小山　覚 | (一社)ICT-ISAC　ステアリング・コミッティ運営委員長<br>NTTコミュニケーションズ（株）　情報セキュリティ部長 | 齋藤　衛 | (株)インターネットイニシアティブ　セキュリティ本部長 |
| 田中　暁 | KDDI(株)　情報セキュリティ本部　セキュリティ管理部長 | 辻　伸弘 | ＳＢテクノロジー(株)　プリンシパルセキュリティリサーチャー |
| 藤本　正代 | 情報セキュリティ大学院大学　教授 | 吉岡　克成 | 横浜国立大学大学院環境情報研究院　准教授 |

（オブザーバ）ＮＩＳＣ、経産省

## スケジュール

| | |
|---|---|
| 令和４年１２月 | 第41回サイバーセキュリティタスクフォース（分科会設置を決定） |
| ５年　１月 | 第１回分科会（以降月１回程度のペースで開催） |
| 令和５年夏 | とりまとめ |