

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

2022年12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

① KDDI株式会社・沖縄セルラー電話株式会社に対する行政指導のポイント

2

長時間かつ大規模な通信障害という事故の重大性に鑑み、令和4年8月3日に総務大臣名で行政指導を実施

行政指導のポイント

- 緊急通報を取り扱う音声伝送役務に関する事故であることに加え、61時間25分の間、音声伝送役務及びデータ伝送役務が利用しづらい事象を生じさせており、携帯電話サービスが国民生活の重要なインフラとなっている状況を踏まえれば、社会的影響は極めて大きい。
- 一般の利用者に加え、物流・交通・金融・公共等の分野のサービスやMVNOにも多大な影響。
- 重大な事故の発生は、利用者の利益を阻害し、かつ、社会・経済活動に深刻な影響を及ぼすものであり、**同様の事故を発生させないよう厳重に注意。**
- 再発防止の観点から、**次の事項を確実に実施するよう指導。**

1 メンテナンス作業時の 事前準備の徹底	● 作業手順書管理ルール・作業承認手法の見直し ● 作業リスク評価と作業抑制基準・期間の見直し
2 事故の大規模化の防止	● VoLTE交換機により詳細な輻輳検知ツール開発 ● 輻輳制御の設計見直し(点検、計画策定)
3 事故の長期化の防止	● 輻輳発生時の復旧手順の見直し ● VoLTE交換機の輻輳解消ツールの開発
4 周知広報の強化	● 周知広報の内容・頻度の改善 ● 事故発生時の緊急通報機関への連絡の徹底 等
5 今回の事故で得られた 教訓の他事業者との共有	● 他の携帯電話事業者に対して、発生原因や再発防止策を説明し、情報共有すること。
6 電気通信事故検証会議 の検証結果の取組	● 電気通信事故検証会議の検証の結果、追加的な再発防止策があれば取り組むこと。
7 実施状況報告	● 上記の実施状況は、本年10月末時点における状況を11月10日までに報告すること。 ● 当分の間、3か月毎に実施状況をとりまとめ、翌月15日までに報告すること。

- KDDIは、11月2日(水)の中間決算報告の中で、行政指導への対応状況を発表。
- 本報告は11月1日(火)に総務省に提出されており、同日の電気通信事故検証会議で事前説明し、翌2日、総務省HPでも概要を公表済み。**指導内容は概ね実施済み。** 今後は3ヶ月毎に報告を求めていく予定。

主な報告内容		
1	【メンテナンス作業時の事前準備の徹底】 ①作業手順書管理ルール・作業承認手法の見直し【実施済】 ②作業リスク評価と作業抑制基準・期間の見直し【実施済】	※赤字は未完了
2	【事故の大規模化の防止】 ①VoLTE交換機により詳細な輻輳検知ツール開発【実施済】 ②輻輳制御の設計見直し【実施済】 ③ VoLTE以外のネットワークについて通信が1/2の確率で失敗する問題が無い点検(令和4年10月31日点検実施済み、令和5年3月31日是正処置完了予定)	
3	【事故の長期化の防止】 ①VoLTE交換機の輻輳解消ツールの開発【実施済】 ② AIを活用した復旧対処の自動化(令和5年度以降に段階的に実装)	
4	【周知広報の強化】 ①周知広報の内容・頻度の改善【実施済】 ②事故発生時の緊急通報機関への連絡の徹底【実施済】	
5	【事業者横断的な対応】 他の携帯電話事業者に対して、発生原因や再発防止策を説明し、情報共有すること。【実施済】	
6	【電気通信事故検証会議の検証結果の取組】 ①人為的ミス防止する品質管理体制の強化【実施済】 ②VoLTE 交換機及び加入者データベースの動作検証及びリスク評価の徹底【実施済】 ③輻輳の自動制御が機能しない事故への対応訓練 の実施【実施済】 ④ 端末仕様によるサービス影響の違いについての仕様見直し(令和4年12月末までにメーカー各社と協議完了予定)	

※パブリックコメントを経て12月20日(火)開催の会合にて、第1次報告書を取りまとめ

1. 基本方針

- 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。**



- 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。**

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、**来年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**

自然災害や通信事故等の非常時

携帯電話事業者
(A社=被災事業者)

携帯電話事業者
(B社=救済事業者)



携帯電話事業者A社(被災事業者)の利用者

- ✓ 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の在り方について検討するため、**本年10月から「電気通信事故検証会議 周知広報・連絡体制WG」を開催しており、12月14日（水）に報告書案を取りまとめた。**
- ✓ 今後は、パブリックコメントの手続きを経て報告書を確定した上で、**総務省において、本報告書を踏まえ、年度内を目途にガイドラインの策定を行っていく予定。**

電気通信事故検証会議 周知広報・連絡体制WG 報告書案のポイント

※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

- ① ガイドラインの対象者は**電気通信事業者**を広く対象。「**指定公共機関※**」には、一部高い内容を求める。
- ② 対象とする事案は、**軽微な事故及び障害を除き、役務の提供に影響が生じた事故及び障害（自然災害含む）**
- ③ 指定公共機関は**事故等の発生から原則30分以内に初報の公表**。指定公共機関以外もこれに準じて対応。
- ④ 利用者へ周知すべき内容は、**事故の発生日時、影響を受ける地域・サービス、影響の具体的内容、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。
- ⑤ 通信障害情報等は、**平時よりトップページのわかりやすい位置及び大きさで常時掲載**。事故時は、深夜早朝を除き、少なくとも**1時間ごとに更新**、災害時は、地図を通じたエリア障害情報を含め概ね1日3回以上更新。
- ⑥ 障害発生時には、初報も含め**報道発表資料等で問い合わせ先を掲載**。
- ⑦ 自社ホームページ、SNS等に加え、例えば、販売代理店におけるデジタルサイネージの活用、報道機関への情報提供、放送事業者による字幕表示等を通じた周知を可能とするための放送事業者へ情報提供（Lアラートへの登録発信含む）等、情報伝達手段を多様化。
- ⑧ 指定公共機関は、**総務省に対しては原則30分以内に連絡、緊急通報受理機関、MVNO/FVNO、他の指定公共機関に対しては、初報の公表後速やかに連絡**。指定公共機関以外もこれに準じて対応。
- ⑨ 周知広報で使用する用語の共通化等は、まずは事業者間で協議を行い、協議結果を本WGに報告。

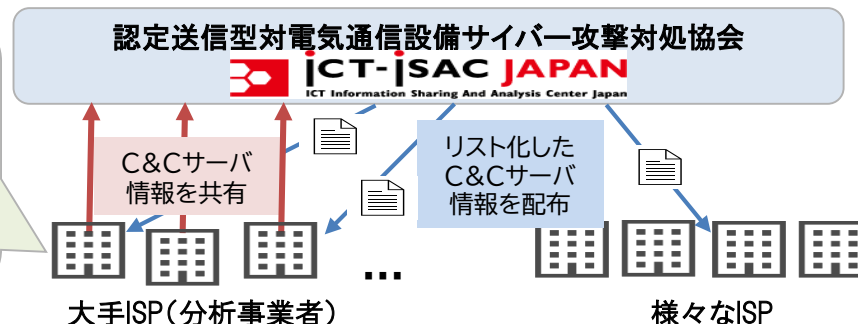
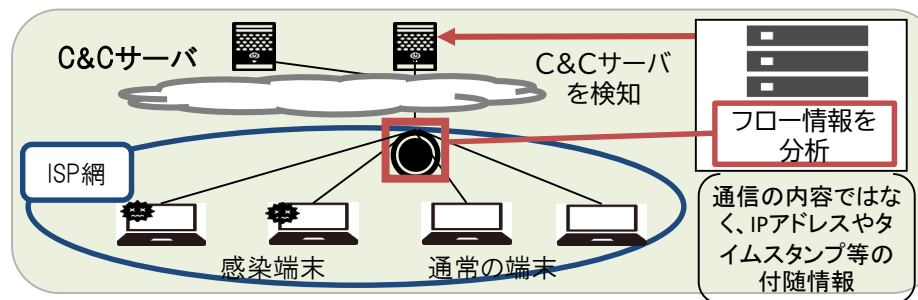
(2) 関連する予算施策

- 大規模化・巧妙化・複雑化するサイバー攻撃・脅威に、電気通信事業者が、より効率的・積極的に対処できるようにするため、①サイバー攻撃の指示を出す管理サーバ(C&Cサーバ)検知技術の実証、②フィッシングサイト等の悪性Webサイトの検知技術・共有手法の実証、③ネットワークセキュリティ対策手法の導入に係る実証等を実施。

① フロー情報分析によるC&Cサーバ検知技術の実証

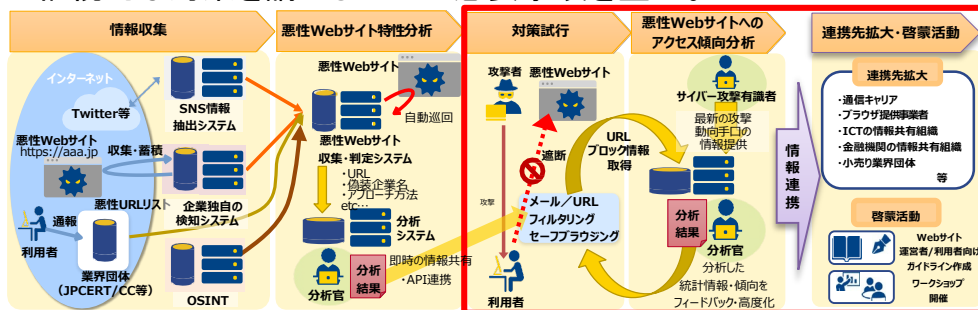
※C&Cサーバ:ボットネットを構成する各感染端末(ボット)にサイバー攻撃の指示を出す管理サーバ

インターネット利用者のトラフィックのうちフロー情報を大規模かつ統計的・相関的に分析し、C&Cサーバを検知する手法の有効性や、C&Cサーバの検知・共有に当たっての技術・運用面の課題を整理。



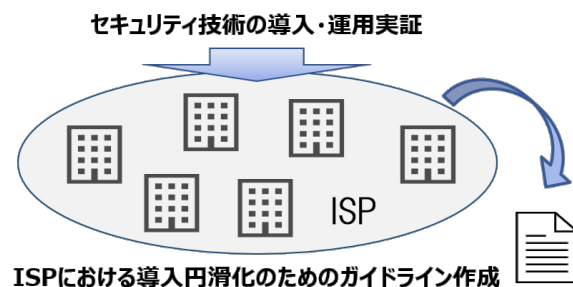
② 悪性Webサイトの検知技術・共有手法の実証

悪性Webサイト(フィッシングサイト等)の情報を収集・分析し、検知する手法の有効性を実証するとともに、検知結果を活用し継続的な対策を講じるための必要事項を整理。



③ ネットワークセキュリティ対策技術の導入実証

ISPにおけるセキュリティ対策を強化するため、ネットワークセキュリティ対策技術の円滑な導入、実装及び運用に係る技術的な諸課題を整理。



- スマートフォンアプリがユーザの意図に反してユーザ情報を送信しているのではないか等のデータセキュリティや安全保障上の懸念が生じた場合にその実態を確認する手段が限られている現状を踏まえ、対応の検討に資するため、第三者によるアプリの技術的解析等を通じて、アプリ挙動の実態把握に係る課題を整理。



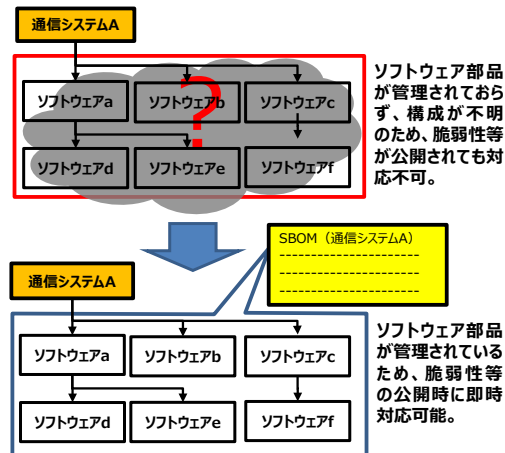
③ 通信分野におけるSBOMの導入に向けた調査

10

- 情報通信システムに普及したオープンソースソフトウェアに、悪意あるコードや深刻な脆弱性が発見され、それらを狙ったサイバー攻撃が発生していることから、ソフトウェア部品の把握や迅速な脆弱性への対応に欠かせない、SBOM(ソフトウェア部品構成表)の通信分野への導入に向けた調査を実施。

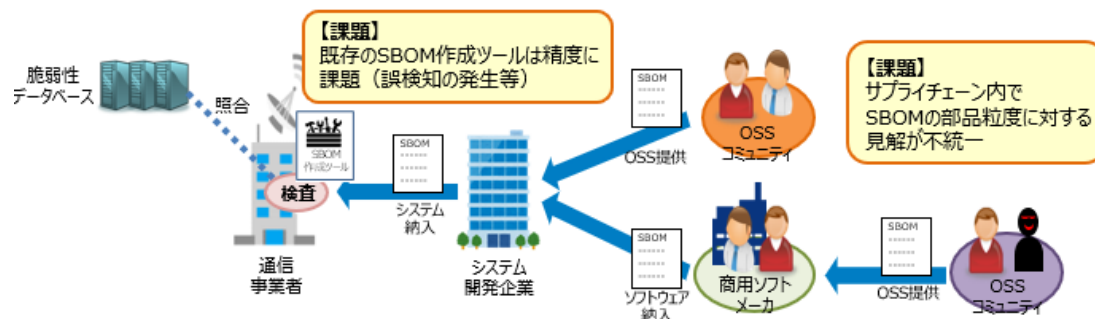
■ SBOM

- SBOM: ソフトウェア部品構成表
システムを構成する様々なソフトウェア部品の一覧とそのライセンス等の詳細をまとめたもの。
- SBOMの導入効果



■ 実証内容

- 通信分野へのSBOMの導入には、ソフトウェア部品の粒度やツールの精度といった技術面等に課題が存在。



- 通信事業者が実際に運用している設備の一部を対象として、実証事業としてSBOMを実際に作成し、SBOMの導入に向けた具体的な方策を整理。

＜SBOM作成イメージ＞

サプライヤ名	コンポーネント名	コンポーネントのバージョン	その他の一点の注記	依存関係	SBOMの作成者	タイムスタンプ
A社	光通信システム	Ver 2.0		Primary	電気通信事業者	2022/7/25 15:00
B社	ト通信制御システム	Ver 3.1		Included in	電気通信事業者	2022/7/25 15:00
C社	ト信号管理ソフトウェア	Ver 4.4		Included in	電気通信事業者	2022/7/25 15:00
D社	ト通信制御ソフトウェア	Ver 5.5		Included in	電気通信事業者	2022/7/25 15:00
	ト端末制御ソフトウェア					
C社	ト基地制御ソフトウェア	Ver 6.6		Included in	電気通信事業者	2022/7/25 15:00
D社	契約管理システム	Ver 1.0		Included in	電気通信事業者	2022/7/25 15:00

④ ナショナルサイバートレーニングセンターの強化

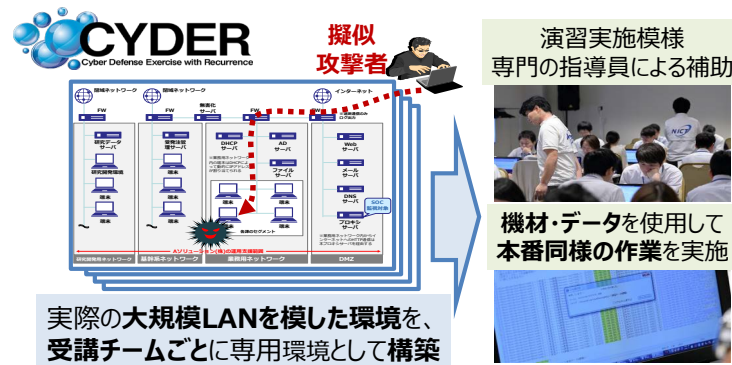
11

- 巧妙化・複雑化するサイバー攻撃に対し、国立研究開発法人情報通信研究機構(NICT)に設置した「ナショナルサイバートレーニングセンター」において、実践的な対処能力を持つセキュリティ人材等を育成し、我が国のサイバーセキュリティを強化。

①CYDER（実践的サイバー防御演習）

国の行政機関、地方公共団体、独立行政法人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実践的サイバー防御演習（CYDER）を実施。

※オンライン受講環境を令和3年度より本格稼働。



②SecHack365（若手セキュリティイノベータの育成）

25歳以下の若手ICT人材を対象として、新たなセキュリティ対処技術を生み出し得る最先端のセキュリティ人材を育成。



③万博向け演習プログラムの提供

2025年日本国際博覧会（大阪・関西万博）開催に向けて、万博関連組織の情報システム担当者等を対象に、CYDERを基にした人材育成の演習プログラムを提供。



令和5年度要求額予算(案) 12.7億円
(令和4年度予算額 11.9億円)

サイバー攻撃に対処可能な万博関連組織の人材育成
万博向け演習プログラムの提供