

ENISA

電気通信分野 セキュリティインシデント: 2024 年

2025 年 7 月

ENISA について

欧州サイバーセキュリティ機関（ENISA）は、欧州全域で高いレベルのサイバーセキュリティを実現するために設立された欧州連合の機関だ。2004年に設立され、EU サイバーセキュリティ法によってその権限が強化された ENISA は、EU のサイバー政策に貢献し、サイバーセキュリティ認証制度を通じて ICT 製品、サービス、プロセスの信頼性を高め、加盟国や EU 団体と協力し、欧州が将来のサイバー課題に備えるための支援を行っている。知識の共有、能力開発、意識向上を通じて、同機関は主要な利害関係者と協力し、ネットワーク化された経済に対する信頼を強化し、EU のインフラのレジリエンスを高め、最終的にはヨーロッパの社会と市民のデジタルセキュリティを維持することを目指している。

ENISA およびその活動に関する詳細情報は、www.enisa.europa.eu を参照のこと。

お問い合わせ

この報告書の内容に関するお問い合わせは、incidentreporting@enisa.europa.eu まで。

この文書に関するメディアや一般的なお問い合わせは、info@enisa.europa.eu まで。

著者

Rossen Naydenov（ENISA）、Nuno Rodrigues Carvalho（ENISA）、Edgars Taurins（ENISA）

謝辞

EU および欧州経済領域、欧州自由貿易連合、EU 加盟候補国の各国の電気通信規制当局（NRA）で構成される ENISA ECASEC 専門家グループのメンバーから、レビューと意見を提供していただいたことに感謝する。

法的通知

特に明記されていない限り、この出版物は ENISA の見解および解釈を反映したものである。この出版物は、規則（EU）No 526/2013 に基づいて採択された場合を除き、ENISA または ENISA 団体の法的措置として解釈されるべきではありません。この出版物は、ENISA により随時更新される場合がある。

サードパーティの情報源は、必要に応じて引用している。ENISA は、この出版物で参照されている外部ウェブサイトを含む外部情報源の内容について責任を負わない。

この出版物は情報提供のみを目的としている。無料でアクセス可能でなければならない。ENISA またはその代理として行動するいかなる者も、この出版物に含まれる情報の利用について責任を負わない。

著作権表示

© 欧州サイバーセキュリティ機関（ENISA）、2025

特に明記されていない限り、この文書の再利用は、クリエイティブ・コモンズ・アトリビュション 4.0 インターナショナル（CC BY 4.0）ライセンス（<https://creativecommons.org/licenses/by/4.0/>）の下で許可されている。これは、適切な出典を明記し、変更点を明示する限り、再利用が許可されることを意味する。

表紙の画像の著作権：© Shutterstock

欧州サイバーセキュリティ機関が所有していない要素の使用または複製については、それぞれの権利者に直接許可を求める必要がある場合がある。

ISBN: 978-92-9204-717-7 DOI: 10.2824/3702896

目次

1. 序論

2. 背景と文脈

2.1 政策の背景

2.2 インシデント報告の枠組み

2.3 インシデント報告ツール

3. 根本原因の分析

3.1 根本原因のカテゴリ

3.2 各根本原因カテゴリにおけるユーザー時間損失

3.2.1 詳細な技術的原因とユーザーが失った時間

4. 影響を受けたサービスの概要

5. 影響を受けた技術資産の概要

6. 技術的な原因の概要

7. 複数年にわたる傾向

7.1 根本原因の複数年傾向

7.2 複数年トレンド – サービスへの影響

7.3 複数年トレンド – インシデントの影響の深刻度

7.4 複数年にわたる傾向 – インシデントの数と失われたユーザー時間

8. 結論

エグゼクティブサマリー

本報告書は、2024年に発生した主要な通信セキュリティインシデントに関する匿名化および集約化された情報を提供する。インシデントの報告は、サイバーセキュリティの監督を可能にする重要な要素であり、各国およびEUレベルでの政策立案を支援するツールである。

EUでは、通信事業者は重大なセキュリティインシデントを自国の当局に報告する。各国当局は、その概要をENISAに報告する。第40条に基づき、欧州電子通信コード（EECC 2018/1972）は、インシデントの報告に関する規定⁽¹⁾を強化し、その適用範囲⁽²⁾および技術的ガイドライン⁽³⁾と報告規準を明確にしている。CIRASは、統計情報を提供し、各国当局からデータを収集し、特定のグラフを用いてインシデントを表示する視覚的なツールを提供するプラットフォームだ⁽⁴⁾。2024年のインシデント報告期間は、2024年1月1日から2025年2月24日までだった。

なお、2024年10月18日付で、NIS2指令によりEECCの第40条から第41条が廃止され、公衆電子通信網のプロバイダや公衆が利用可能な電子通信サービスのプロバイダなど、複数のセクターにおける完全性および可用性の侵害の報告が統合される予定である。本報告書は、EECCの第40条から第41条がまだ有効である2024年のみを対象としている。

2024年要約報告書の主要な発見事項

2024年の年次要約には、EU加盟26カ国および欧州自由貿易連合（EFTA）加盟2カ国の国家当局から提出された**188件のインシデント**の報告が掲載されている。これは、EU加盟26カ国およびEFTA加盟1カ国から提出された156件のインシデント（2023年）に比べ、20.5%の増加となっている。

2022年と2023年と比較して、2024年はユーザーが失った時間数が大幅に減少している。

2024年は2023年と比較して、ユーザーが失った時間数が50%以上減少した。受け取ったデータによると、2024年には17億4,300万時間⁽⁵⁾のユーザー時間が失われたのに対し、2023年には39億600万時間のユーザー時間が失われた。これは明らかに昨年と比較して大幅に減少しており、**図1**に示すように10年前のレベルに戻っている。妥当な仮説としては、この傾向は、停止管理の改善、インフラの強化、システムのレジリエンスの向上を示している可能性がある。

¹セキュリティインシデントの報告は、2011年に施行された枠組み指令（2009/140/EC）の第13a条に基づき、2009年の電気通信パッケージの改正以来、EUの電気通信に関する規制の枠組みの一部となっている。

²2016年以降、eiDAS規則第19条に基づき、EU内のトラストサービス・プロバイダもセキュリティインシデントの報告が義務付けられていることは注目に値する。2018年、NIS指令第14条および第16条に基づき、EU内の重要サービス事業者およびデジタルサービス・プロバイダもセキュリティインシデントの報告が義務付けられた。

³EECCに基づくインシデント報告に関するENISA技術ガイドライン（しきい値や損失時間の計算方法など）。

⁴<https://ciras.enisa.europa.eu> で入手可能

⁵各インシデントについて、ユーザー数に時間数を乗じて算出。

Number of outages and userhours lost per year

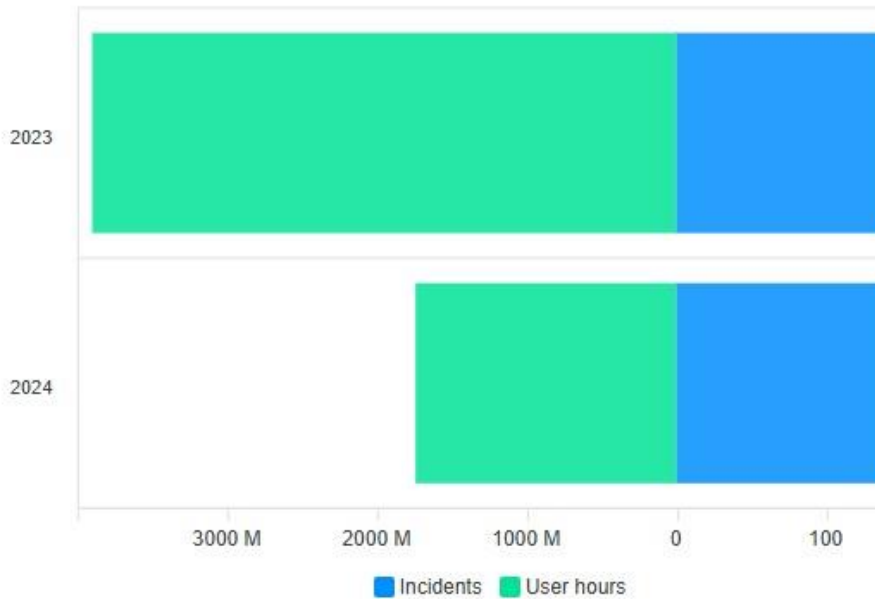


図 1 : 各国から報告されたインシデント件数と損失ユーザー時間 (2023 年~2024 年)

さらに、以下の点も注目すべきだ。

- ENISA に報告された電子コミュニケーションのインシデントは、過去最多の 188 件に達した。報告されたインシデントは増加したものの、ユーザーの損失時間はそれに見合った増加は見られなかった。
- インシデントの分布は、サービス停止 178 件、サービスへのその他の影響 4 件、他のシステムへの影響 1 件、脅威または脆弱性 1 件、冗長性への影響 2 件、ニアミス 1 件となっている。
- 非常に大きな影響を与えた**インシデントは**、77 件 (2023 年) から 92 件 (2024 年) へと **19.5% 増加した**。
- 根本原因の主要統計 :
 - 影響の点では、**システム障害**が引き続き大部分を占め、2024 年には 113 件で 60% に達したが、2023 年 (61%) からはわずかに減少した。これは 5 億 4,800 万時間のユーザー時間損失に相当し、2024 年のユーザー時間損失全体の 3 分の 1 近くを占めている。
 - **人為的ミス**によるインシデントの割合は、2023 年の 21%から 19%へとわずかに減少しましたが、2024 年には失われたユーザー時間は 1 億 8,100 万時間から 4 億 200 万時間へと 2 倍以上に増加している。
 - **自然現象**によるインシデントは 25 件に増加し、その割合は 13% に達し、6 億 500 万時間のユーザー時間損失につながった。これは、前年の 7,200 万時間のユーザー時間損失の 9 倍近くの増加だ。
 - **悪意のある行為**によるインシデントは 15 件で、全インシデントの 8% を占め、1 億 8,400 万時間のユーザー利用時間が失われました。これは、2023 年の 16 件 (10%) および 2 億 1,400 万時間のユーザー利用時間の損失に比べ、減少している。

- 影響を受けたサービスの主要統計
 - 携帯電話および**モバイルインターネット**は、それぞれ 100 件および 86 件のインシデントが発生し、2023 年と同様、57% および 49% の割合を占め、再び最も影響を受けたセクターとなった。
 - 固定インターネットのインシデントの割合は、2023 年の 16%から 2024 年には 26%に増加した。
- 技術的な原因
 - 2024 年には、**41 件のインシデントがケーブル切断（23%）と分類され**、ソフトウェアの変更/更新の不具合（14%）およびソフトウェアのバグ（13%）という、次の 2 つの技術的な原因を 10% 上回った。ケーブルの切断とソフトウェアの変更/更新の不具合は、その結果として失われたユーザー時間数を考慮すると順位が逆転する。ソフトウェアの変更/更新の不具合によるインシデントでは 5 億 1,500 万時間のユーザー時間が失われたのに対し、ケーブルの切断では 3 億 3,100 万時間だった。
- 2024 年には、65 件のインシデントが**サードパーティによる障害**として報告され、2023 年の 52 件から 25% 増加した。
- 国境を越えたインシデントは報告されていない。**

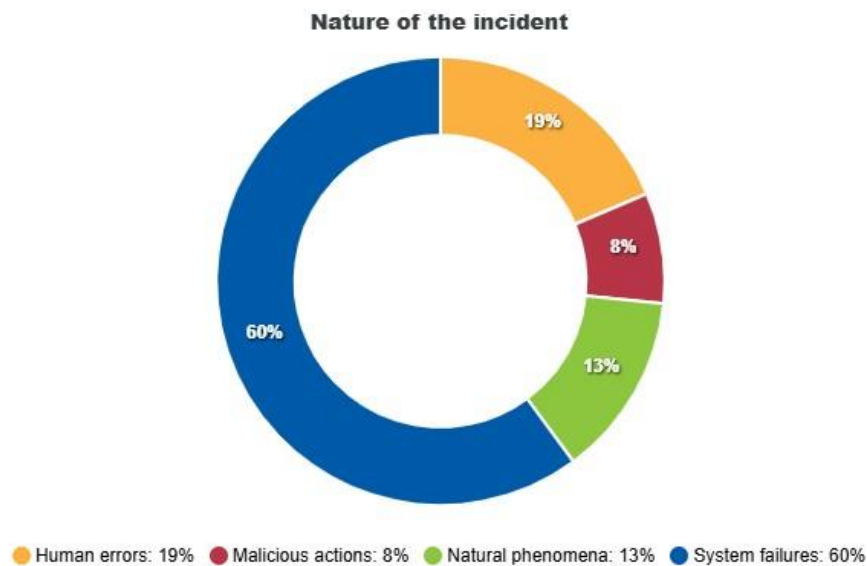


図 2 : 根本原因のカテゴリ

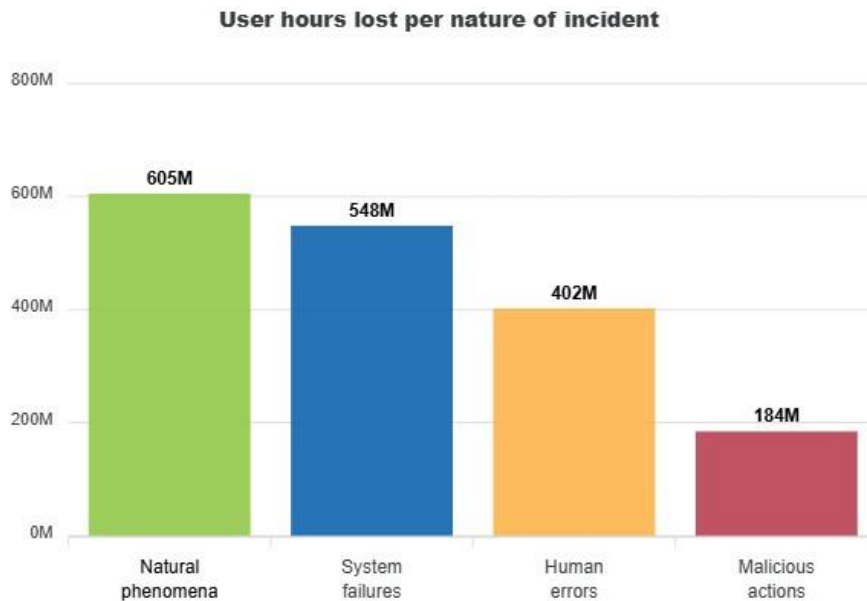


図 3 : 各根本原因カテゴリーにおけるユーザー時間の損失割合

2012 年から 2024 年までの複数年傾向

13 年間に、EU 加盟国は 1,930 件の通信セキュリティインシデントを ENISA サイバーセキュリティインシデント報告・分析システム (CIRAS) に報告した。この統計は、⁶ でオンラインで閲覧できる。

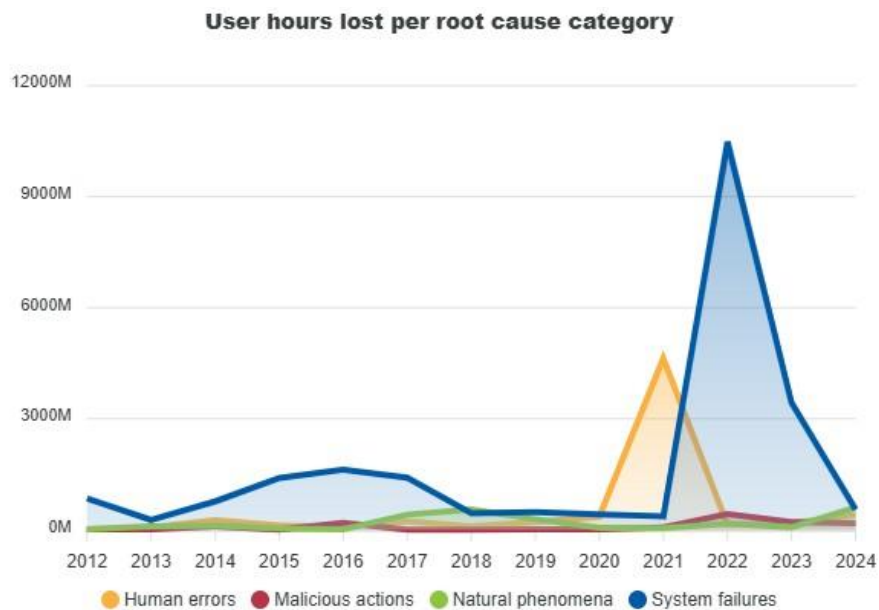


図 4 : 2012 年から 2024 年にかけて報告された EU における電気通信セキュリティインシデントの根本原因カテゴリー

⁶各国における報告のしきい値は年ごとに変化するため、傾向や前年との比較については慎重な結論を下す必要があることにご留意ください。実際、近年、ほとんどの国で報告のしきい値が引き下げられており、報告の対象は最も重大なインシデントのみ（より頻発する可能性のある軽微なインシデントは対象外）となっている。

長年にわたるインシデント報告の分析によると、インシデントの件数が増加しても、ユーザーの損失時間は増加していないことから、欧州の通信ネットワークはより堅牢でレジリエンスが高まっていると考えられる。

特に、以下の傾向が顕著になっている。

- **システム障害（青）**は、長年を通じて最も多い根本原因となっている。
- **悪意のある行為（赤）**は、時間経過とともに比較的安定しており、影響も最小限に留まっていることから、重大な障害の主要な原因ではないと考えられる。
- **最も影響を受けたサービス**は、過去 8 年間と同様、**携帯電話およびモバイルインターネット**である。

ENISA は、通信セキュリティを担当する各国当局および NIS 協力グループと引き続き協力し、特に国境を越えたインシデントを含むインシデントの報告に関して、EU のさまざまな法律間の相乗効果を見出し、活用していく。

1. 序論

EU の電子通信プロバイダは、電子通信サービスの継続性に重大な⁽⁷⁾ 影響を与えるセキュリティインシデントを、各 EU 加盟国の国内電気通信規制当局 (NRA) に報告する義務がある。

NRA は、EU 全体で合意された一連の閾値に基づき、毎年、最も重要なインシデントの概要を ENISA に報告している。本文書「2024 年電気通信セキュリティインシデント報告書」は、2024 年に受け取った **188** 件のインシデント報告をまとめ、EU における電気通信セキュリティインシデントの概要を紹介している。

欧州電子通信コード⁽⁸⁾ (EECC 第 40 条) は、インシデント報告の要件の範囲を拡大し、各カテゴリーの電気通信サービスの機能に重大な影響を与えるセキュリティインシデントに特に焦点を当てたインシデント報告を義務付けている。

長年にわたり、規制当局 (EECC 第 41 条) は、主にネットワーク/サービスの停止に焦点を当てることで合意してきた。ENISA は、EECC に基づくインシデント報告に関するガイドライン⁽⁹⁾ を公開している。このガイドラインでは、国境を越えたインシデント報告および年次要約報告の形式と手続きの概要が記載されている。このガイドラインは、2 種類の報告、すなわち、管轄当局と ENISA 間の臨時の報告、および各国当局から欧州委員会および ENISA への年次要約報告に特に焦点を当てている。

これは、電子通信分野におけるインシデント報告に関する ENISA の年次報告書である。

インシデントの報告義務は、2009 年以来、EU の電気通信規制の枠組みの一部となっている。

欧州電子通信コード第 40 条が、この文書の法的根拠となっている。

⁷各国当局に報告される通信セキュリティインシデントは、重大な影響のある重大なインシデントのみであることに留意ください。

⁸[https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX %3A32018L1972](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L1972)

⁹<https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-theeccc>

2. 背景と文脈

この章では、各国当局と共同で作成された ENISA 技術ガイドライン「インシデント報告」⁽¹⁰⁾ に記載されている、インシデント報告プロセスの主な特徴とともに、政策の背景について説明する。

2.1 政策背景

2018 年に採択され、2020 年後半から施行された欧州電子通信コード (EECC)⁽¹¹⁾ は、WhatsApp や Skype などの OTT (Over-The-Top) 通信プロバイダも規制の対象に含めることで、EU の電気通信規則を近代化した。EECC の重要な柱は、すべての電子通信サービスにおけるサイバーセキュリティの強化であり、事業者および OTT プロバイダに対して、ネットワークとユーザーデータを保護するための強力なセキュリティ対策とインシデント報告の実施を義務付けている。本報告書は、加盟国が ENISA に年次概要報告書を提出することを義務付ける EECC 第 40 条に基づいて作成されている。

2.2 インシデント報告の枠組み

インシデント報告には 3 種類ある。

- 1) プロバイダから国家管轄当局 (NCA) への国内インシデント報告
- 2) NCA と ENISA 間の臨時のインシデント報告
- 3) 各国当局から欧州委員会および ENISA への年次要約報告。

この仕組みでは、ENISA が収集拠点として機能し、インシデント報告を匿名化、集約、分析していることに留意すべきである。

各報告の種類は、次のページの **図 5** に示されている。

¹⁰<https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting>

¹¹新しい EU の通信法におけるセキュリティ監督の変更 - ENISA (europa.eu)

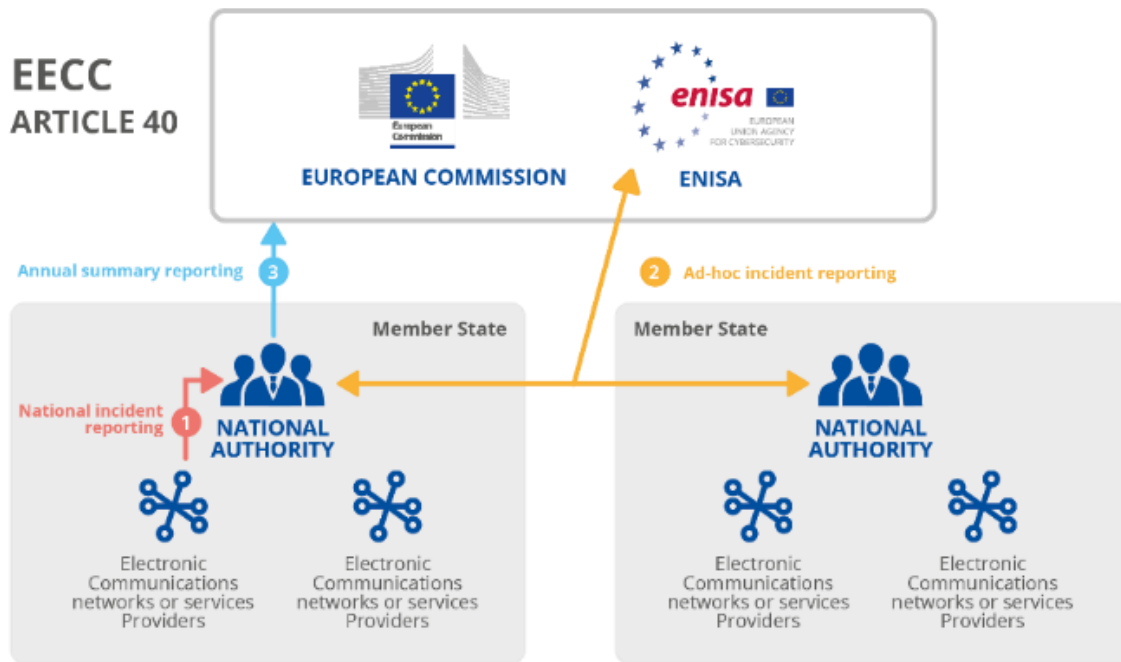


図 5 : EEC 第 40 条に基づくインシデント報告

2.3 インシデント報告ツール

ENISA は、当局が報告をアップロードし、特定のインシデントを検索・調査するためのサイバーセキュリティインシデント報告・分析システム（**CIRAS**）を運営している。

また、ENISA は、一般市民向けに、オンラインの視覚的ツールも公開しており、このツールは、データのカスタマイズ分析に使用できる。このツールは、関係する国や事業者を匿名化する。

リンク : <https://ciras.enisa.europa.eu/>



CIRAS は、ENISA が報告されたインシデントを保存し、年次および複数年分の統計情報を提供する無料のオンラインツールだ。

報告テンプレートは、インシデントの種類（6 種類のサイバーセキュリティインシデントから選択、図 6 で説明）から始まる。

このフィールドは 3 つの部分で構成されている。

1. **インシデントの影響** : 影響を受けたコミュニケーションサービスとその程度
2. **インシデントの性質** : インシデントの原因

3. **インシデントの詳細**：インシデントに関する詳細情報（簡単な説明、ネットワークの種類、資産の種類、重大度など）。

SELECT TYPE OF INCIDENT

First choose the type of incident. This will configure the reporting template.



図 6：サイバーセキュリティインシデントの種類

- **タイプ A.** サービス停止（例：継続性、可用性）。
例えば、新しい道路の建設に使用されている掘削機オペレーターのミスによるケーブルの切断によって生じた停止は、タイプ A のインシデントに分類される。
- **タイプ B.** サービスへのその他の影響（機密性、信頼性、完全性など）。例えば、人気のあるコラボレーションツールが、セッションの開始時に確立されるメディアチャネルのコンテンツを、共有セッションに参加しているエンドポイント間で暗号化していない場合、中間者攻撃によってメディア（音声、画像、ビデオ、ファイルなど）が傍受される。このインシデントは、タイプ B のインシデントに分類される。
- **タイプ C.** 他のシステムへの影響（例：オフィスネットワークにおけるランサムウェア、サービスへの影響なし）。例えば、通信プロバイダのオフィスネットワークの複数のワークステーションおよびサーバーでマルウェアが検知された場合、このインシデントはタイプ C に分類される。
- **タイプ D.** 脅威または脆弱性（暗号の欠陥の発見など）。
たとえば、暗号の脆弱性の発見は、タイプ D のインシデントに分類される。
- **タイプ E.** 冗長性への影響（例：フェイルオーバーまたはバックアップシステム）。
たとえば、2 本の冗長海底ケーブルのうち 1 本が切断された場合は、タイプ E のインシデントに分類される。
- **タイプ F.** ニアミスインシデント（セキュリティ対策の発動など）。
例えば、通信プロバイダのハニーポットネットワークに侵入した悪意のある試みは、タイプ F のインシデントに分類される。

インシデント報告プロセスに関する詳細については、[EECC のインシデント報告に関する技術ガイドライン](https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc) ⁽¹²⁾ を参照すること。

¹²<https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc> を参照

3. 根本原因の分析

2024 年は、EU 加盟 25 カ国と欧州自由貿易連合 2 カ国が年次プロセスに参加し、**188** 件の重大なインシデントが報告された。一方、2023 年は EU 加盟 26 カ国と EFTA 1 カ国が参加し、156 件のインシデントが報告された。

3.1 根本原因のカテゴリー

2024 年には、**システム障害**に関連するインシデントが 113 件とわずかに増加し、2023 年の 96 件（61%）に比べ、全体の 60% を占めた。2024 年のシステム障害の 2 大技術的要因は、ソフトウェアのバグとハードウェアの故障で、それぞれ 19% を占めた。

人為的ミスは、システム障害に次いで 2 番目に多い原因であり、2024 年には 35 件（19%）が報告されており、2023 年の 32 件（20%）と割合的にはほぼ同じだ。2024 年の人為的ミスの主な技術的原因は、ケーブルの切断が 40%、ソフトウェアの欠陥/変更の更新が 37% だった。

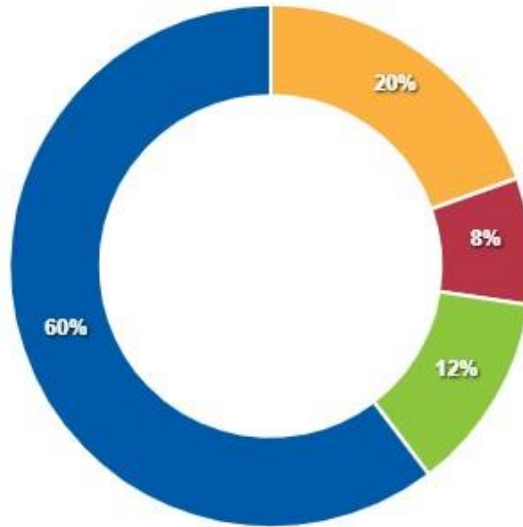
自然現象は 2023 年の 7% から 12% に増加し、インシデントも 2023 年の 12 件から 2024 年には 25 件と 2 倍以上に増加した。最も一般的な技術的な原因は、強風（44%）と外的要因（36%）だった¹³。

悪意のある行為は、2024 年には 15 件（8%）で、2023 年の 16 件（10%）から増加した。悪意のある行為の主な技術的原因は、全原因の 46%を占めるケーブルの切断だった。

**2024 年に EU 加盟国から報告された通信セキュリティインシデントは
188 件だった。**

¹³1 件のインシデントで複数の原因を報告することができる

Nature of the incident

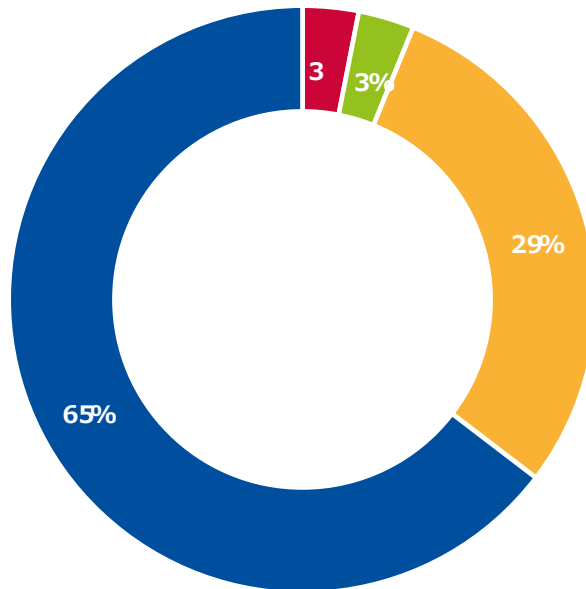


● Human errors: 20% ● Malicious actions: 8% ● Natural phenomena: 12% ● System failures: 60%

2024 年、188 件のインシデントのうち 65 件がサードパーティによる障害として報告され、インシデント全体の 37% を占めた。2023 年には 38 件が報告され、インシデント全体の 24% を占めていた。これにより、2024 年のサードパーティによる障害によるインシデントは 70% 以上増加した。

インシデント報告の大部分、42 件はシステム障害（65%）によるもので、19 件は人為的ミス（29%）、2 件は悪意のある行為（3%）、2 件は自然現象（3%）によるものでした（図 8 を参照）。

インシデントの性質



■ 悪意のある行為 ■ 自然現象 ■ 人為的ミス ■ システム障害

図 8 : 根本原因のカテゴリ - サードパーティの障害

3.2 根本原因の 카테고리別ユーザー損失時間

- **システム障害**によるユーザー時間損失は 5 億 4,800 万時間で、2023 年の 3 億 4,390 万時間に比べ、6 倍以上の減少となった。不具合のあるソフトウェアの変更/更新は、1 億 8,300 万時間の損失で上位 3 位に入った。停電が 1 億 6,000 万時間の損失で 2 位、ソフトウェアのバグが 1 億 4,200 万時間の損失で 3 位となった。
- **人為的ミス**による損失は、2023 年の 35 件のインシデントで 4 億 200 万時間だったのに対し、2023 年は 32 件のインシデントで 1 億 8100 万時間だった。このうち、ソフトウェアの変更/アップデートの不具合が 3 億 4100 万時間の損失で最大の要因となっている。2 位は、2700 万時間の損失という大きな差をつけて、ポリシーおよび手順のミスだった。
- **自然現象**によるユーザー時間の損失は、2023 年の 72 百万時間から 605 百万時間に大幅に増加した。その主な原因は、洪水（3 億 1,800 万時間）、強風（2 億 7,700 万時間）、外部環境要因（2 億 4,300 万時間）、ケーブル切断（2 億 1,600 万時間¹⁴）である。自然現象は、2024 年に報告された 25 件のインシデントで、1 件あたりのユーザー損失時間が 2,420 万時間と、最も影響の大きい根本原因でもある。
- **悪意のある行為**によるユーザー時間の損失は 2024 年も減少し続け、2023 年の 2 億 1,400 万時間（16 件）から 1 億 8,400 万時間（15 件）に減少した。これらの損失の主な原因は、放火（9,300 万時間）、ケーブルの切断（6,100 万時間）、ケーブルの盗難（3,000 万時間）の 3 つだった。

2024 年に最も影響の大きかった根本原因は**自然現象**である。

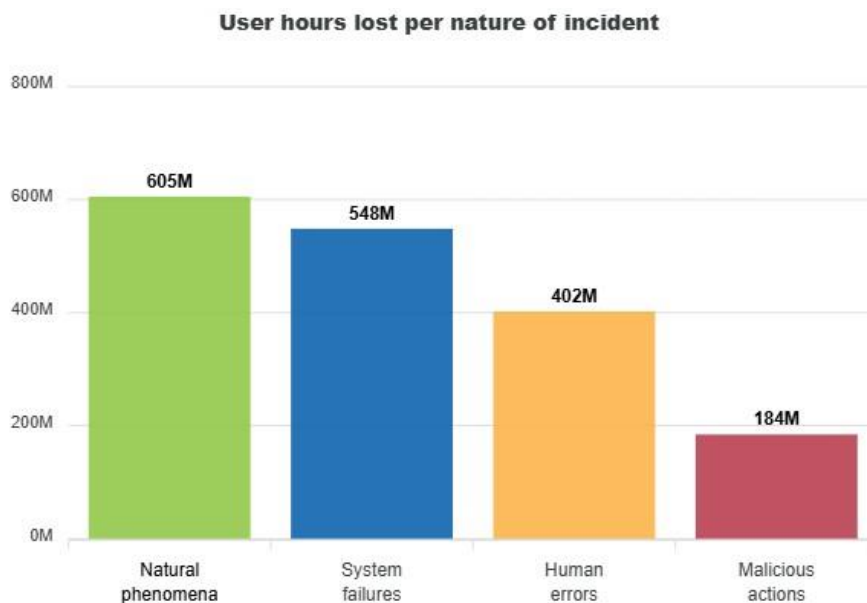


図 9 : 2024 年の根本原因カテゴリー別損失時間割合

¹⁴1 つのインシデントに複数の原因がある場合

3.2.1 詳細な技術的原因とユーザー時間損失

すべてのインシデントの詳細な技術的原因は、**図 10** のすべての根本原因カテゴリで追跡されている。インシデントは多くの場合、一連の出来事（¹⁵）であるため、1 つのインシデントには複数の技術的原因が含まれる場合がある。

2024 年のインシデント報告で最も多く見られた技術的な原因は、41 件のケーブル切断だった。ユーザー時間の損失が最も多かったのは、ソフトウェアの変更/更新の失敗だった。

最も影響の大きい技術的な原因は洪水で、8 件のインシデントにより 3 億 1,800 万時間のユーザー時間の損失という損害が発生している。1 件あたりの影響は 3,900 万時間以上のユーザー時間の損失に及ぶ。

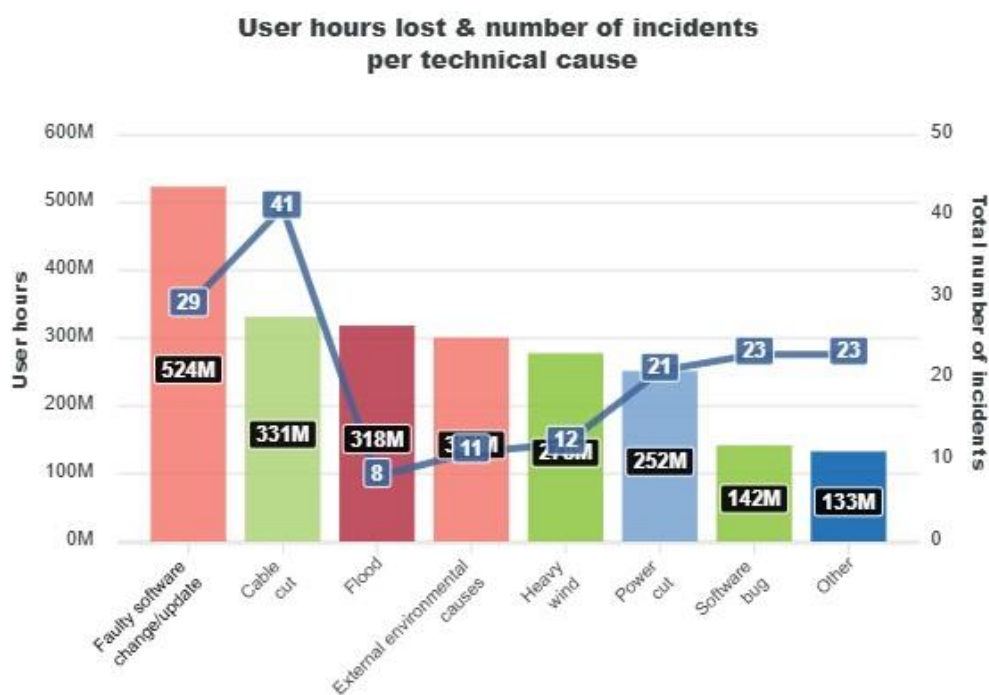


図 10 : 詳細な技術的根本原因

システム障害の最も影響の大きい技術的な原因は、外部環境要因である。

以下は、各インシデントのカテゴリ別の詳細な原因とユーザー時間の損失の概要で、各根本原因を正確に把握するために、影響を受けたサービス、資産、技術的な原因について詳しく説明している。

3.2.1.1 システム障害の分類

システム障害は 113 件のインシデント報告があり、これは全インシデントの 60% に相当し、5 億 4,800 万時間のユーザー損失につながった。

¹⁵たとえば、暴風により電力供給インフラが破壊され、ケーブルが切断されて停電が発生し、その結果、通信障害が発生した場合。この例の場合、インシデントの根本原因は自然現象であり、詳細な原因は強風、ケーブルの切断、停電、バッテリーの消耗となる。

ユーザー利用時間の損失では、**ソフトウェアの変更/更新の誤り**が 1 億 8,300 万時間で依然として最大の技術的原因となっている。しかし、インシデント件数では、**ソフトウェアのバグとハードウェアの故障**が 22 件で同率 1 位となっている。

外部環境要因によるインシデントは 2 件のみであるが、失われたユーザー時間は 5,800 万時間に達しており、システム障害の根本原因として最も影響が大きい要因となっていることは注目に値する。

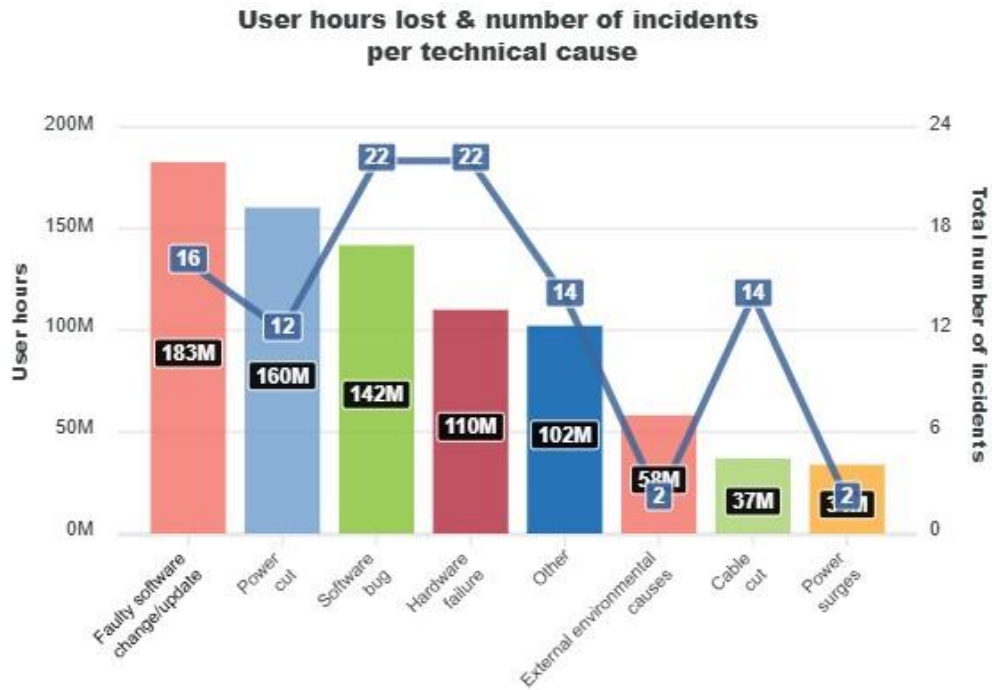


図 11 : システム障害インシデントの根本原因と損失ユーザー時間

システム障害の影響を受けたサービス

システム障害の影響を最も受けたサービスは、携帯電話（インシデントの 53%）とモバイルインターネット（インシデントの 45%¹⁶⁾）だ。オーバーザトップ（OTT）サービスプロバイダは、システム障害に関連するインシデントの 23% を占めている。固定インターネットと固定電話は、それぞれ 20% と 19% で、システム障害の影響を 4 番目と 5 番目に受けている。

¹⁶⁾ 1 つのインシデントが複数のサービスに影響を与える場合

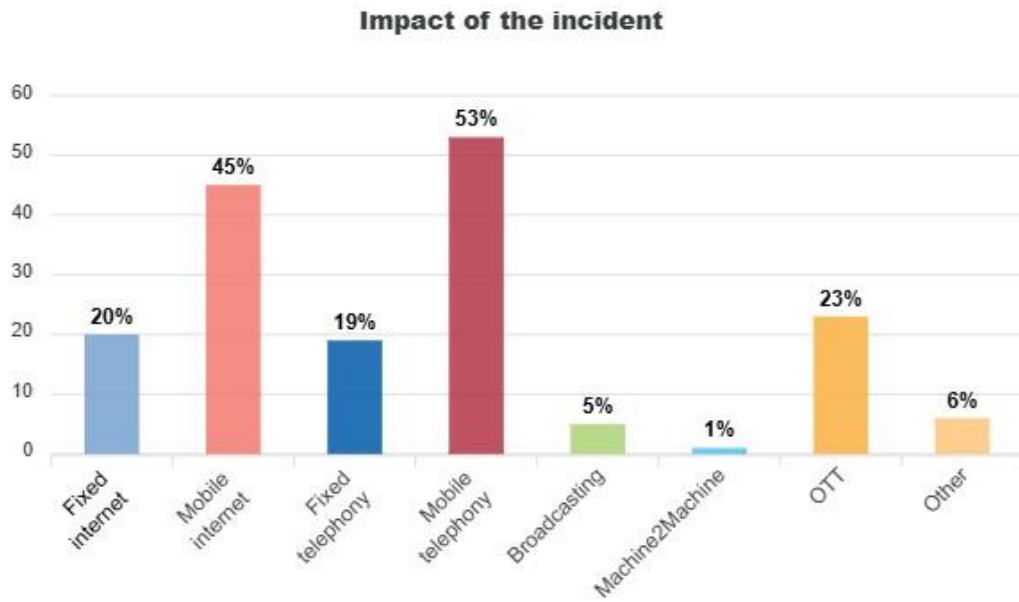


図 12 : システム障害の影響を受けるサービス

システム障害の影響を受ける資産

システム障害により最も影響を受けた技術資産はスイッチとルーター（18%）で、2023 年の 30%から減少した。モバイル基地局とコントローラーは 2023 年と同じ 17%で変わらない。伝送ノードは 2023 年に報告されておらず、2024 年も 16%で最下位を維持している。モバイルスイッチは、2023 年の 15%から 13%に小幅減少している。

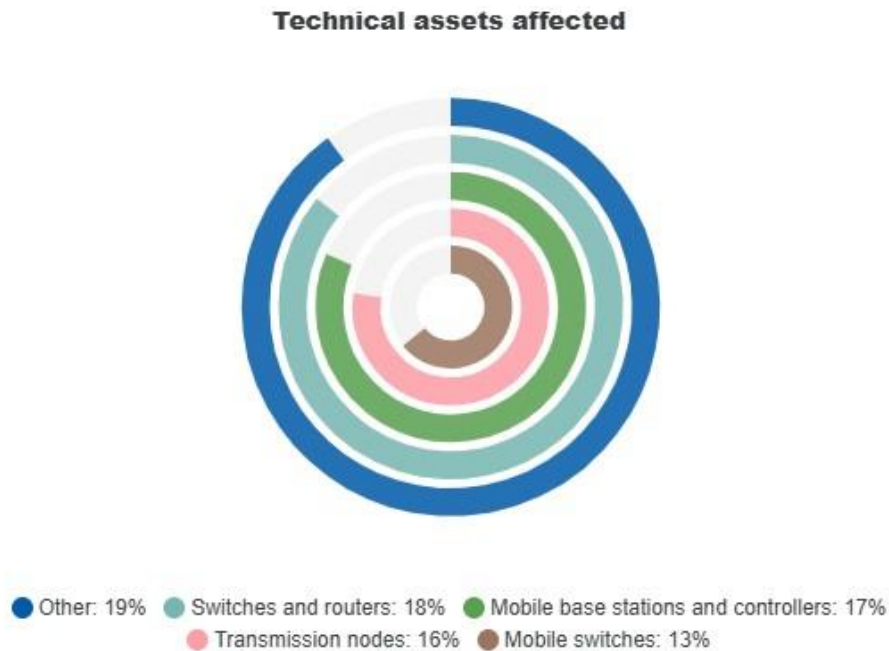


図 13 : システム障害の影響を受ける資産

3.2.1.2 人為的エラーの内訳

人為的ミスは、前年と同様、インシデント全体の 19% を占めている。35 件のインシデントにより、4 億 200 万時間のユーザー時間が失われた。これは、2023 年の 32 件のインシデントによる損失（1 億 8000 万時間）の 2 倍以上である。

ユーザー時間の損失数では、**ソフトウェアの変更・更新の誤り**が 13 件でトップとなっている。この原因は、1 件あたりのユーザー時間の損失が 2,600 万時間以上と、最も影響が大きい原因でもある。

ユーザー時間損失数では、**ポリシー/手順の欠陥**が 2,700 万時間で 2 位となっているが、報告されたインシデントは 3 件のみである。

ケーブルの切断は 14 件、1,700 万時間のユーザー時間損失で 3 位となっている。

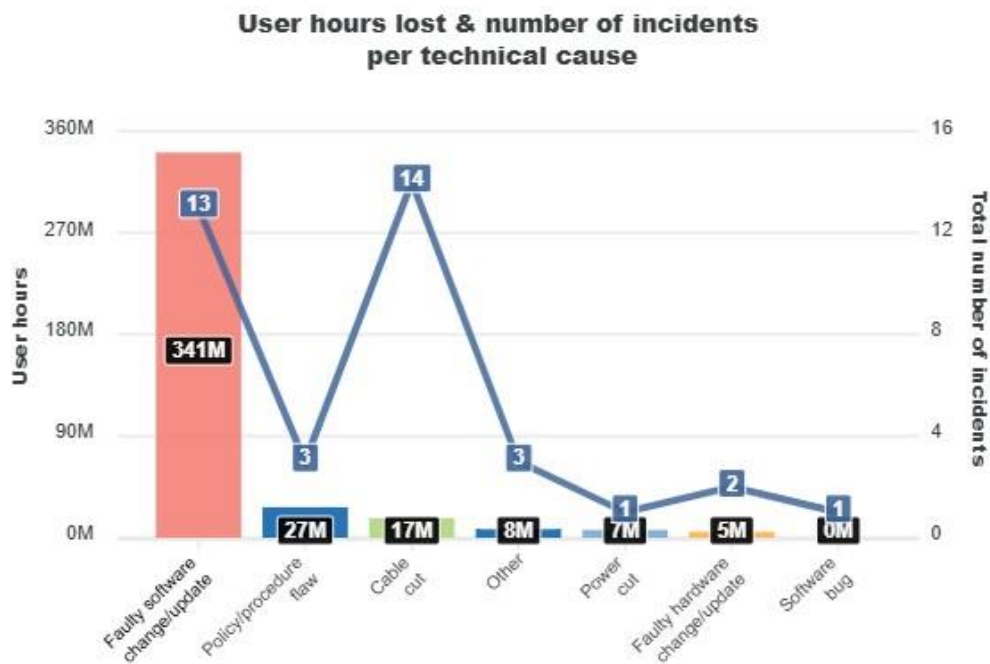


図 14 : 技術的な原因 - 人的ミス

人的ミスによる影響を受けたサービス

人的ミスで最も影響を受けたサービスはモバイル電話で 57%で、2023 年の 62%から減少している。2 番目に影響を受けたサービスはモバイルインターネットで 48%で、こちらも 2023 年の 53%から減少している。3 位と 4 位は固定電話と固定インターネットで、2024 年は 28%に増加した。一方、2023 年は固定電話が 25%、固定インターネットは 15%と大幅に低かった。OTT は両年で 25%を維持している。

人的ミス根本原因に最も影響を与える技術的要因は、**ソフトウェアの変更または更新の故障である。**

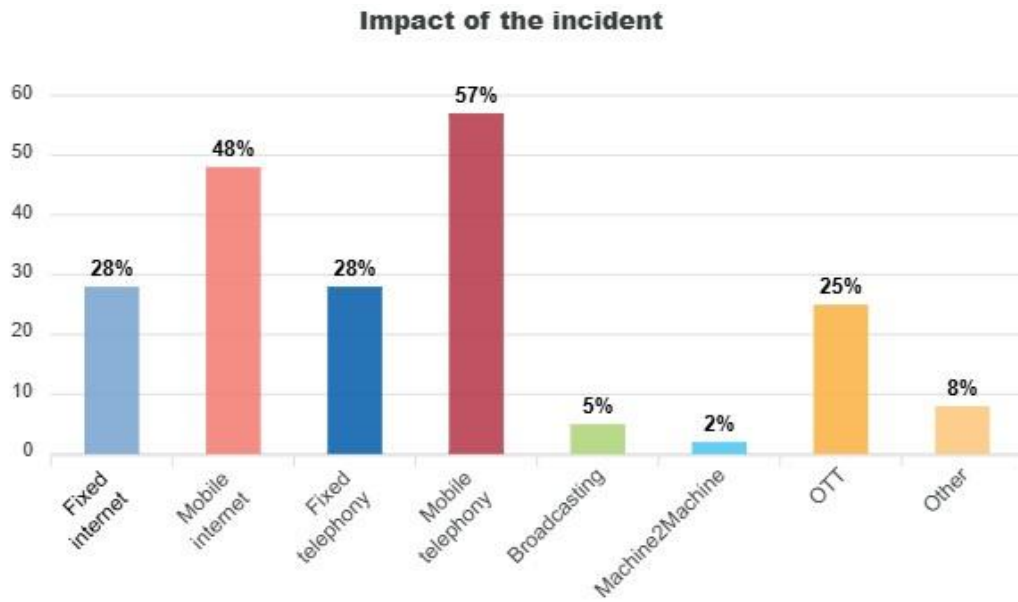


図 15 : 人的エラーの影響を受けるサービス

人的エラーの影響を受けた技術資産

人為的ミスによって最も影響を受けた資産は、2023 年の 28% から 31% に増加したモバイル基地局およびコントローラだ。2 位は地下ケーブルで 31% だが、2023 年にはこのようなインシデントは報告されていなかった。モバイルスイッチは 2023 年と同様、14% で 3 位を維持している。スイッチおよびルーターは、2023 年の 25% から 11% に減少している。アドレスサーバーは 9% で最下位であり、2023 年には同様のインシデントは報告されていない。

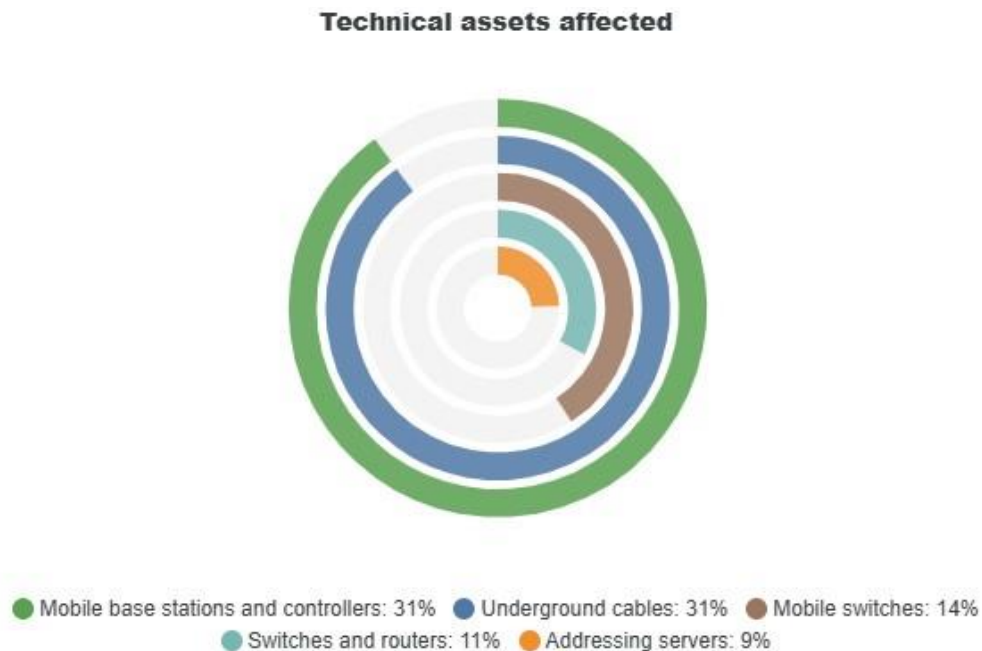


図 16 : 人的ミスによる技術資産の影響状況

3.2.1.3 自然現象の内訳

自然現象は 25 件、全インシデントの 13% を占め、6 億 500 万ユーザー時間の損失につながった。これは、7,200 万ユーザー時間の損失、12 件のインシデントだった前年に比べ、ほぼ 9 倍の増加だ。

洪水は 3 億 1,800 万時間のユーザー時間損失で最大の要因であり、2023 年の 600 万時間のユーザー時間損失に比べ、驚異的な増加となっている。この技術的な要因は、1 件あたりのインシデントによるユーザー時間損失が 4,000 万時間に近く、最も影響が大きい要因でもある。

強風は自然現象における第 2 位の要因で、2 億 7,700 万時間のユーザー時間損失が発生しました。これは前年の 300 万時間と比較してほぼ 100 倍の増加である。

外部環境要因は 3 番目に多い原因で、2 億 4,300 万時間のユーザー時間損失が発生した。これは昨年は自然現象の原因として記録されていなかった。

4 番目に多い原因は**ケーブル切断**で、2 億 1,600 万時間のユーザー時間損失が発生している。ケーブル切断は、過去 6 年間、技術的な原因として識別されていなかった。

自然現象の根本原因における最も影響の大きい技術的原因は**洪水**である。

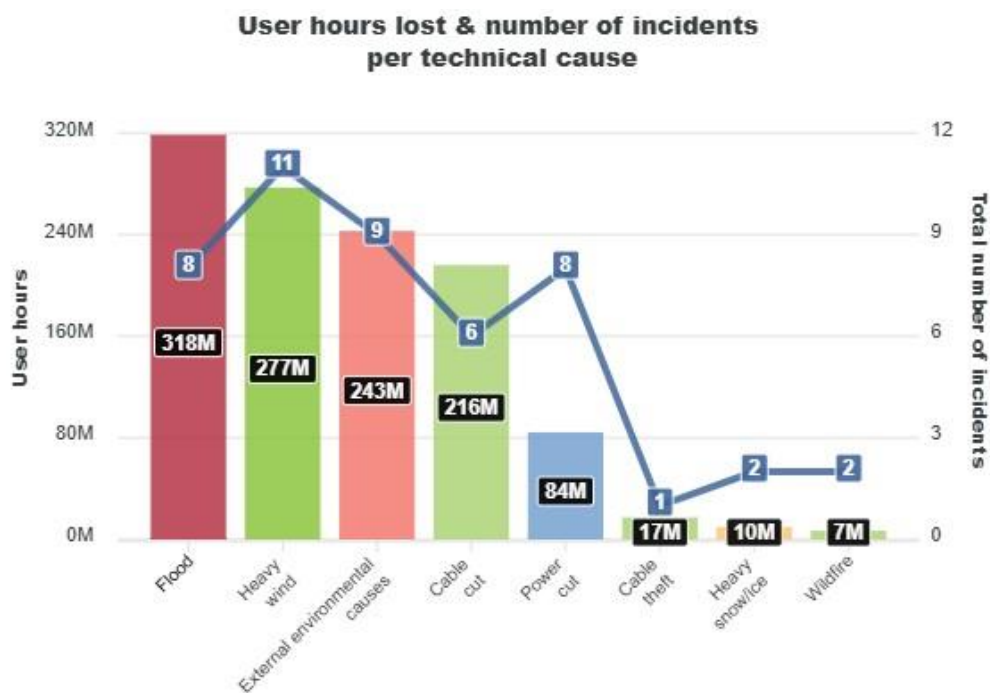


図 17 : 自然現象によるインシデントの根本原因と損失ユーザー時間

自然現象の影響を受けたサービス

自然現象の影響を受けたサービスで最も影響が大きかったのは、80%を占めるモバイル電話で、2023 年の 91%から減少している。モバイルインターネットも、2023 年の 91%から 68%に大きく減少している。固定インターネット (52%) と固定電話 (44%) は、2023 年の 41%と 33%と比較して、2024 年に影響を受けたサービスの割

合が増加している。放送も、2023年の8%から20%に増加している。自然現象による影響が最も少ないサービスはOTTサービスで、2023年の8%から4%に減少している。

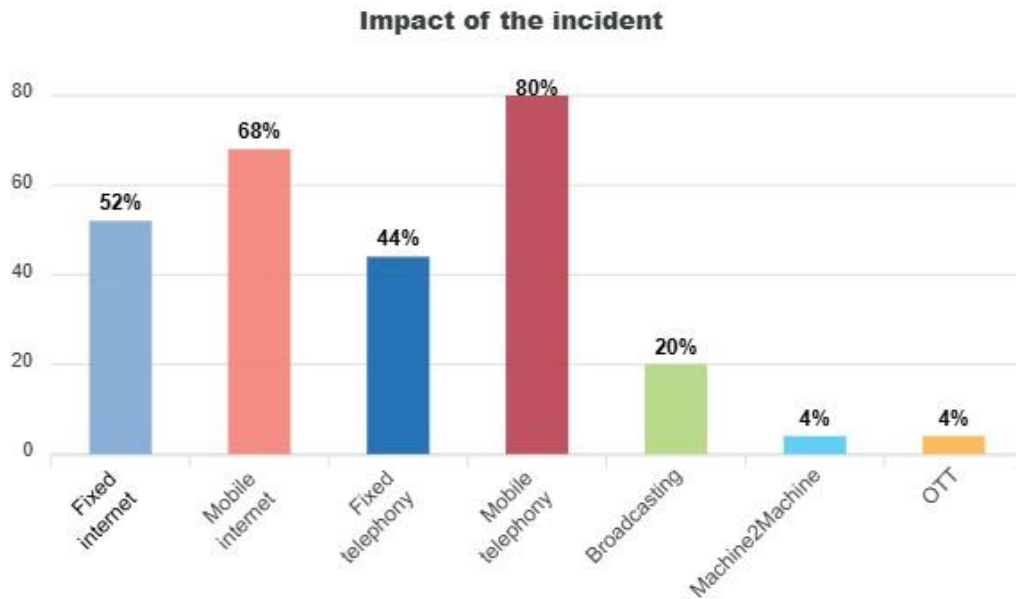


図 18 : 自然現象の影響を受けるサービス

自然現象の影響を受けた技術資産

自然現象の影響を最も受けやすい資産は、2023年の83%から2024年には80%へと減少した、モバイル基地局およびコントローラである。2位は、2023年の25%から44%へと増加した電源である。3位は、自然現象の影響を受けたインシデントの28%を占める伝送ノードであり、2023年にはこのようなインシデントは報告されていない。

バックアップ電源は、2023年の17%から2024年には12%へと減少している。架空ケーブルは、自然現象によるインシデントの12%を占め、2023年には報告はなかった。

Technical assets affected

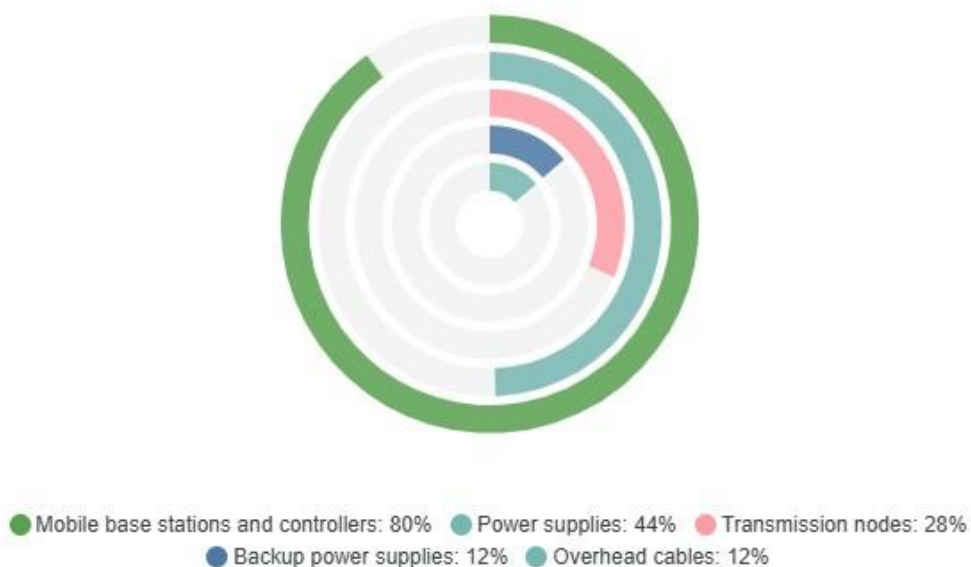


図 19 : 自然現象の影響を受けた技術資産

3.2.1.4 悪意のある行動の内訳

悪意のある行為は 15 件、全インシデントの 8% を占め、2023 年の 10% から減少したが、インシデントの数は実際には 16 件と増加している。悪意のある行為によるユーザー時間の損失は、2023 年の 2 億 1,400 万時間から、2024 年は 1 億 8,400 万時間に減少している。

悪意のある行為の最大の要因は放火で、9,300 万ユーザー時間分の損失と 3 件のインシデントが発生しました。これは、1 件のインシデントで 200 万ユーザー時間分の損失にとどまった 2023 年と比較して増加している。放火は、1 件あたりの平均損失ユーザー時間が 3,000 万時間以上と、最も影響の大きい技術的な要因でもある。これは、火災によって物理的な資産が甚大な被害を受け、その交換や再構築に時間がかかるためと考えられます。

悪意のある行為の 2 番目に多い原因は、**ケーブルの切断**で、7 件のインシデントが発生し、6,100 万時間のユーザー時間が失われました。前年は、悪意のある行為によるケーブルの切断は 1 件も報告されていませんでした。

悪意のある行為の 3 番目に多い原因は、3 件の**ケーブル盗難**で、3,000 万時間のユーザー利用時間が失われました。これは、4 件のインシデントで 3,300 万時間のユーザー利用時間が失われた 2023 年とほぼ同じ結果である。

悪意のある行為の根本原因における最も影響の大きい技術的原因は**火災**である。

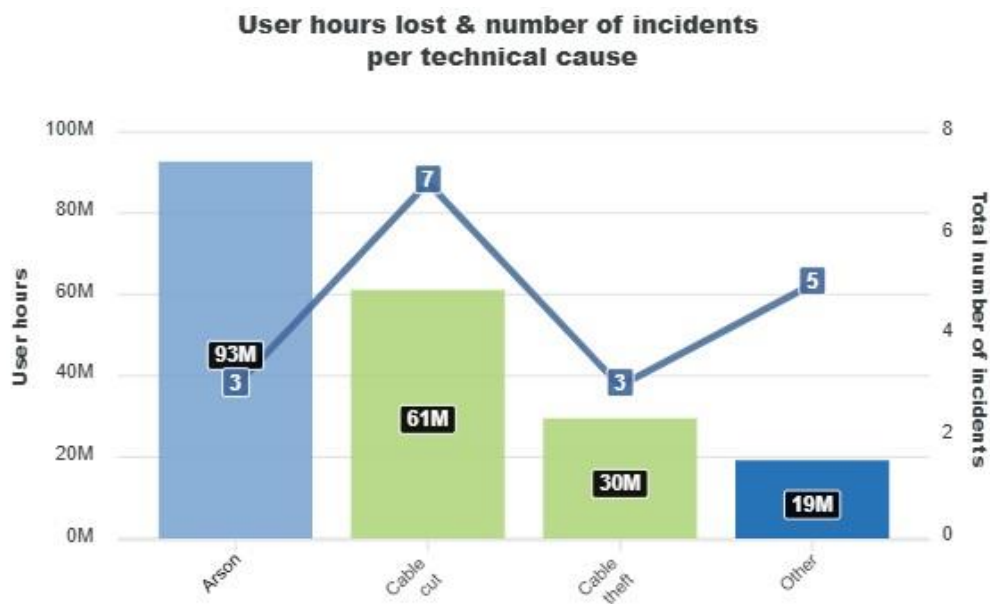


図 20 : 悪意のある行為によるインシデントの根本原因と損失ユーザー時間

悪意のある行為の影響を受けたサービス

2024 年に悪意のある行為の影響を最も受けたサービスは、モバイル通信で 66%を占め、2023 年の 56%から増加した。OTT サービスは、2023 年の 31%から 60%に増加し、強い 2 位につけた。モバイルインターネットは 60%に増加し、2023 年の 50% から 3 位となった。固定インターネットは 26% に減少し、2023 年の 37% から最も影響が少ないサービスとなった。放送および固定電話については、2024 年にはインシデントは報告されていないが、2023 年にはそれぞれ 18% および 31% を占めていた。

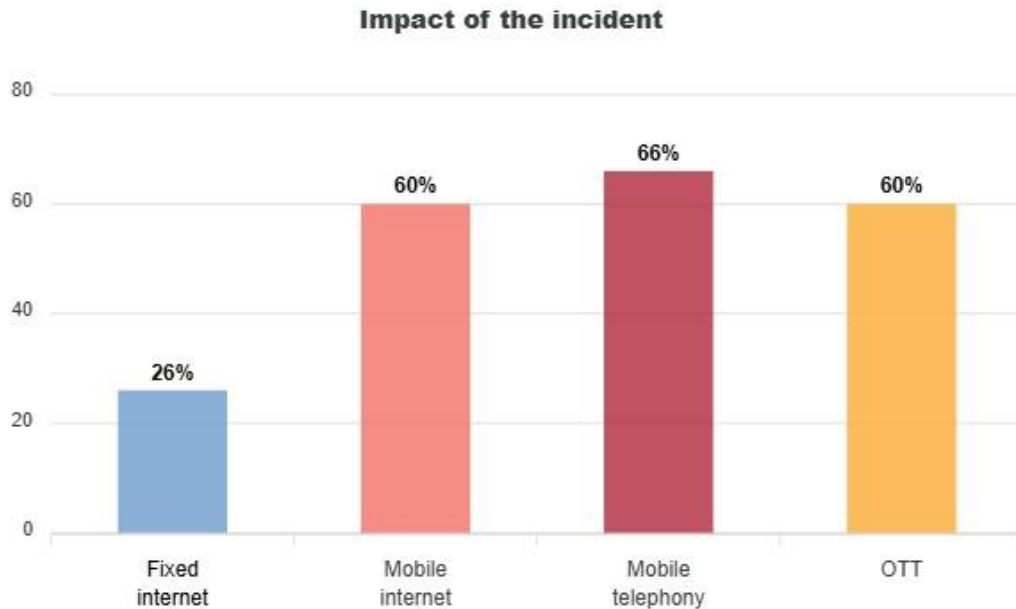


図 21 : 悪意のある行動の影響を受けたサービス

悪意のある行動の影響を受けた技術資産

移動式基地局およびコントローラは、2023 年の 31%から 27%へと減少したものの、依然として悪意のある行為の影響を最も受けやすい資産である。移動式スイッチは、2024 年も 27%と、2023 年と同じ割合のインシデントが発生しており、2023 年にはインシデントは報告されていない。次の 3 つの資産は、悪意のあるアクションによるインシデントの 20% を占めており、2023 年とほぼ同じだ。アドレス指定サーバーは、2023 年の 6% から増加している。海底ケーブルについては、2023 年には同様のインシデントは報告されていない。スイッチおよびルーターは、2023 年と同じ 19% の割合でほぼ横ばいだ。

Technical assets affected



● Mobile base stations and controllers: 27% ● Mobile switches: 27% ● Addressing servers: 20%
● Submarine cables: 20% ● Switches and routers: 20%

図 22 : 悪意のある行動の影響を受けた技術資産

4. 影響を受けたサービスの概要

この段落では、**図 24** を用いて、EECC タイプのサービスごとに、モバイルおよびインターネット電話、固定インターネットおよび電話、放送、OTT サービスなど、インシデントの影響を受けたサービスについて検証する。

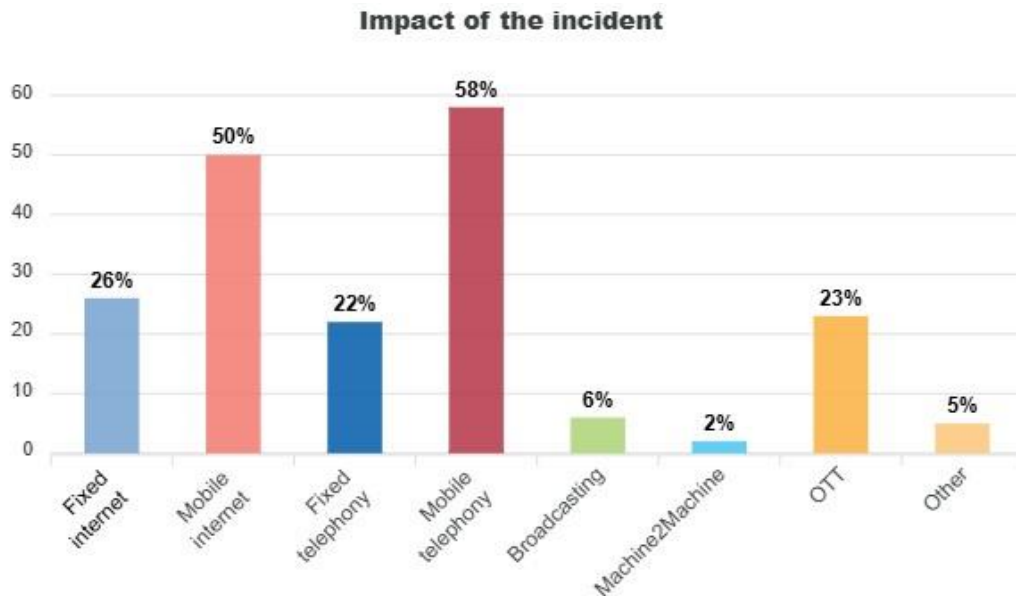


図 24 : 影響を受けたサービス⁽¹⁷⁾ - 2024 年の全インシデント

ここでも、報告されたインシデントのほとんどは**モバイルサービス**に影響を及ぼしている。2024 年には、報告されたインシデントの **58%** が**モバイル電話**に影響を及ぼしており、2023 年の 57% とほぼ同じである。モバイル電話は、過去 8 年間で最も影響を受けたサービスである。

モバイルインターネットは 2024 年に 50%を占め、2023 年の 47%からやや増加した。モバイルインターネットは過去 8 年間で 2 番目に影響を受けたサービスであり、2016 年には最も影響を受けたサービスだった。

OTT サービス⁽¹⁸⁾ に影響を与えたインシデントの報告は、2023 年の 22%から 23%へとわずかに増加した。OTT サービスは、3 年前の報告期間以来、22%から 25%のレベルで推移している。

固定インターネットサービスなどの従来のサービスは、2023 年の 16%から 26%へとインシデントが増加している。**固定電話**は、2023 で 21%、2024 で 22%と、インシデントの割合はほぼ横ばいである。**放送**関連のインシデントは、2023 年の 12%から 6%へと減少している。

¹⁷「方法論」に関する注意。報告されたインシデントのほとんどは複数のサービスに影響を及ぼしており、図の合計が 100% を超える理由を説明していることにご留意ください。

¹⁸新たに導入されたサービスおよびデータは、3 年間にわたって統合および標準化される必要がある。2022 年には、これらのサービスはインシデント全体の 26% を占めたが、2021 年には OTT は 4% を占めていた。

5. 影響を受けた技術資産の概要

各インシデント報告書には、インシデントの際に影響を受けた（二次的な）資産についても記載されている。

図 25 は、最も影響を受けた資産を示している。「その他」は、詳細な情報が提供されなかったことを意味する⁽¹⁹⁾。

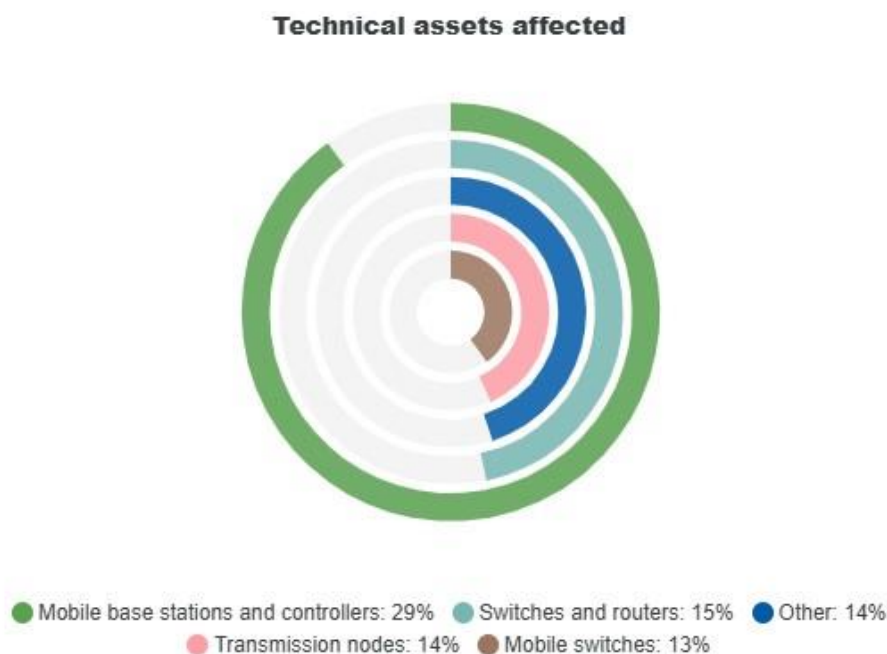


図 25 : 影響を受けた資産 – 2024 年の全インシデント

モバイル基地局とコントローラーが最も影響を受けた資産で 29%を占めており、2023 年の 26%からわずかに増加している。これらの資産は過去 3 年間で最も影響を受けた資産となっている。

スイッチとルーターは 2024 年に 15%と減少しており、2023 年の 26%から減少している。これらの資産は過去 3 年間で 2 番目に影響を受けた資産であり、2021 年には最も影響を受けた資産だった。

伝送ノードは 14% で 3 位ですが、2023 年には報告は 1 件もありませんでした。

モバイルスイッチは、2023 年と同じ 13% のインシデントで、ほぼ横ばい。過去 3 年間で、モバイルスイッチが占めるインシデントの割合は、2022 年の 8% から増加している。

¹⁹「その他」に関する注意事項。将来は、インシデントの分析を改善するために、加盟国からより多くの情報を提供してもらう必要がある。分類に関する注意事項。ちなみに、インシデントの報告を改善するためには、資産分類の再評価も必要になる。

6. 技術的要因の概要

このセクションでは、報告されたインシデントの背後にある最も注目すべき技術的要因について、2024年と前年を比較しながら詳しく検証する。ここでは、上位3つの要因に焦点を当てる。

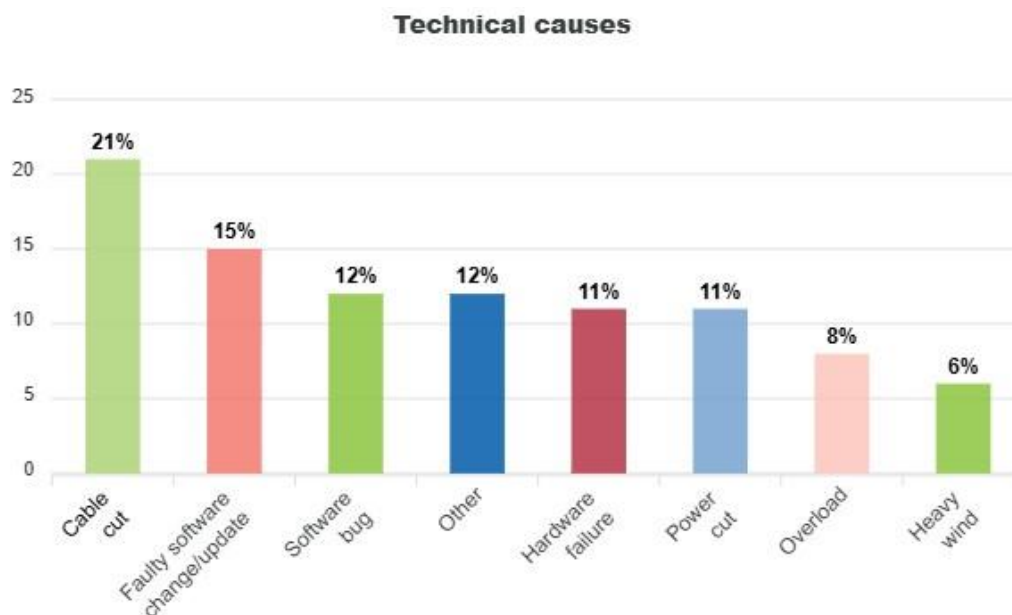


図 26 - 技術的な原因 - 2024 年の全インシデント

2024年には、合計41件のケーブル切断インシデントが報告された。ケーブル切断は、2022年の5%から2023年の11%、2024年には21%と、インシデントの割合が着実に増加している。ケーブル切断は、2024年のユーザー損失時間3億3,100万時間にも相当し、ソフトウェアの変更やアップデートの不具合に次いで2番目に多い損失時間となっている。2023年は、ケーブル切断による損失時間はほぼゼロだったことに留意してほしい。

ソフトウェアの変更またはアップデートの不具合は、インシデントの15%を占めており、2023年とまったく同じ割合である。これは、過去5年間で24%（最大の要因）を占めていた割合から徐々に減少している。2024年は29件のインシデントが発生し、5億2,400万時間のユーザー時間損失につながった。これは、原因別では最も多いユーザー時間損失だ。しかし、2023年の27億3,100万時間の損失に比べれば、5倍以上も減少している。

ソフトウェアのバグは、インシデントの割合が2023年の10%から12%に増加しており、インシデントの数も2023年の16件から2024年には23件に増加している。ただし、ユーザーが失った時間への影響は縮小しており、2024年は1億4,200万時間に対し、2023年は2億2,200万時間だった。

7. 多年度トレンド

ENISA は 2012 年からインシデント報告の収集と集計を行っている。

これは、ENISA が電子通信インシデントの報告でこれまでに記録したインシデントの件数としては最も多い。

このセクションでは、2012 年から 2024 年までの 13 年間の複数年にわたる傾向を紹介する。このデータセットには、**図 27** に示すように、合計 **1930** 件のインシデントが報告されている。

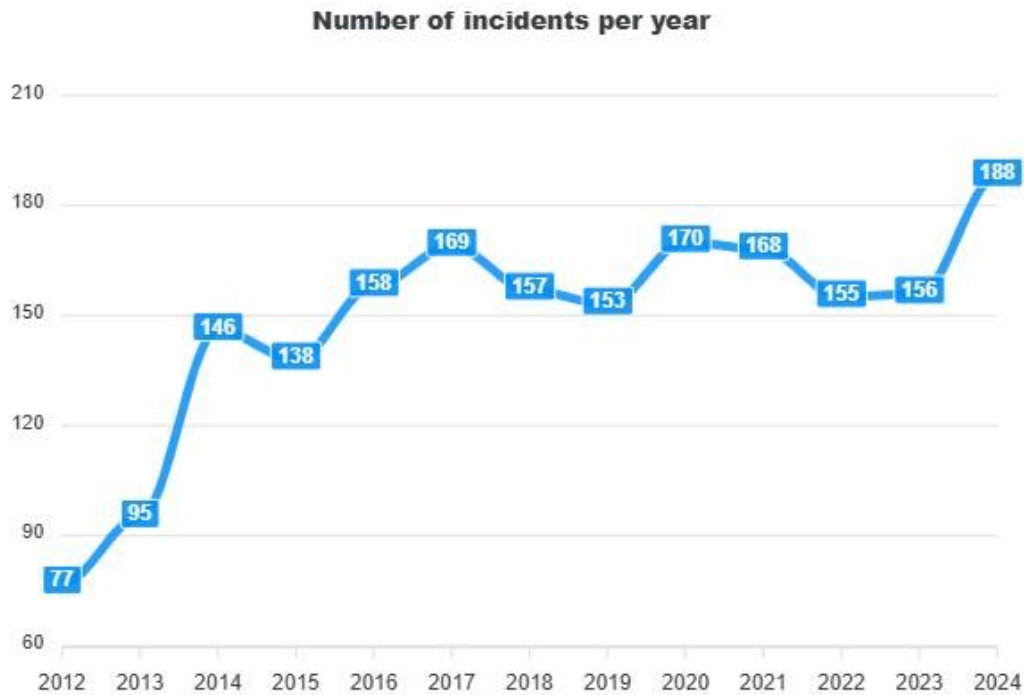


図 27 : 年間報告インシデント件数 (2012 年~2024 年)

過去 10 年間で、報告されたインシデントの数は着実に増加している。それにもかかわらず、ユーザーが失った時間は増加しておらず、実際には 10 年前と同じレベルにとどまっている。インシデントの数から、平均して 2 日に 1 件のインシデントが発生していることになる。2021 年と 2022 年にインシデントがピークに達したのは、インシデント報告の対象範囲に、新しいタイプのオーバーザトッププロバイダが追加されたためと考えられる。

Number of outages and userhours lost per year

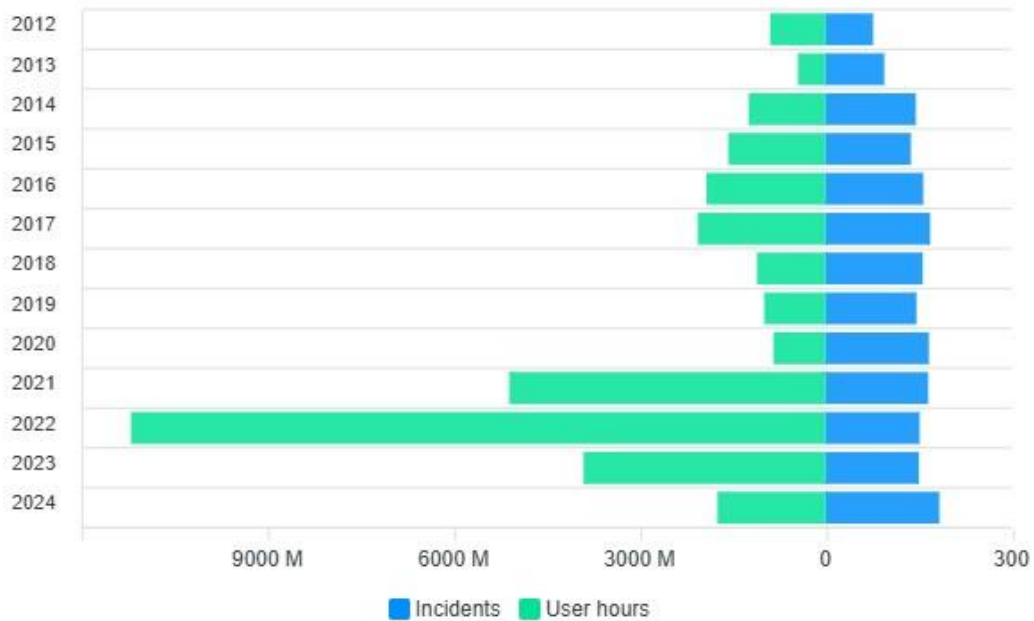


図 28 : 2012 年から 2024 年までの障害件数とユーザーが失った時間

7.1 根本原因の複数年トレンド

長年にわたり、特に過去 3 年間で、自然現象によるインシデントが着実に増加していることがわかります。人為的ミスは 20% の水準で推移しており、悪意のある行為やシステム障害は、前年と比較してわずかに減少している。

Root cause categories per year

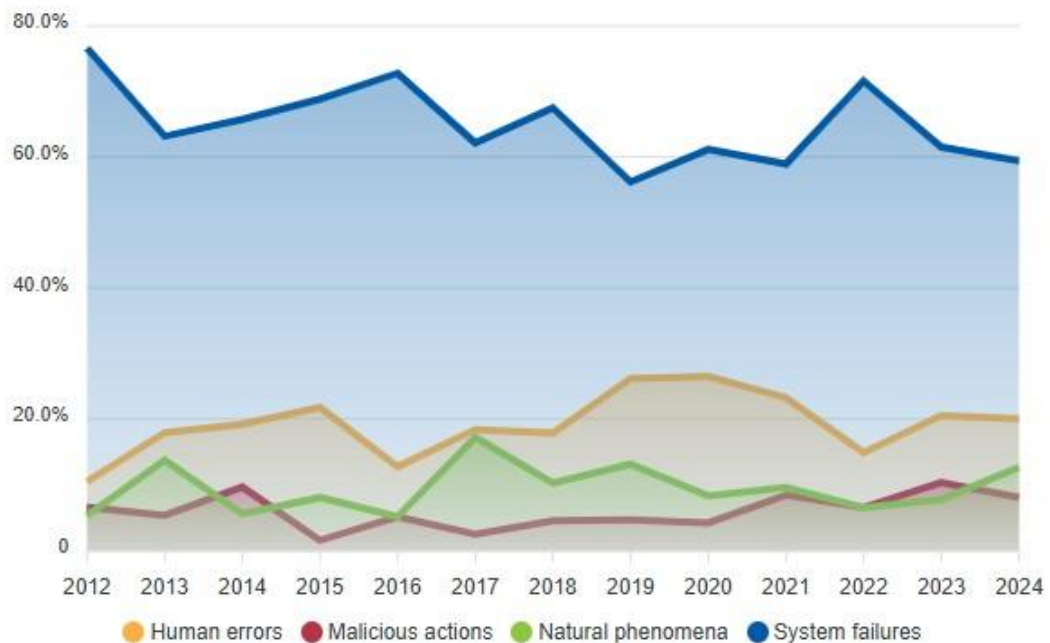


図 29 : 根本原因のカテゴリ – 2012 年から 2024 年までに報告された EU における電気通信セキュリティインシデント

2012 年から 2024 年まで、**システム障害**は毎年、全インシデントの 65% を占め、最も一般的な根本原因でした。システム障害は、合計 **1,245** 件のインシデント報告を占めている。13 年間のシステム障害の 3 大原因は、ハードウェアおよびソフトウェアのバグ、ソフトウェアの変更またはアップデートの誤りである。

2 番目に多い根本原因は**人為的ミス**で、全インシデントの 5 分の 1 近く（20%、合計 376 件）を占めた。人為的ミスの上位 3 要因は、ソフトウェアの変更やアップデートの誤り、ケーブルの切断、ポリシーや手順の欠陥だった。

3 番目に多いのは自然現象で、全インシデントの 10%（186 件）を占めている。この 13 年間で最も多かった 3 つの原因は、停電、強風、大雪または氷だった。

悪意のある行為に分類されたインシデントは 6% に留まり、13 年間で 114 件だった。

2012 年から 2024 年の期間において、悪意のある行為のほぼ半数はサービス拒否攻撃（48%）で、次に多い原因はケーブルの切断（16%）と放火（9%）だった。脆弱性の悪用（旧マルウェアおよびウイルス）によるものは 2% に留まっている。さらに、技術的な原因の 28% は「その他」に分類されている。このことは、これまで指摘されてきた、悪意のある行為の分類体系の更新の必要性を浮き彫りにしている。

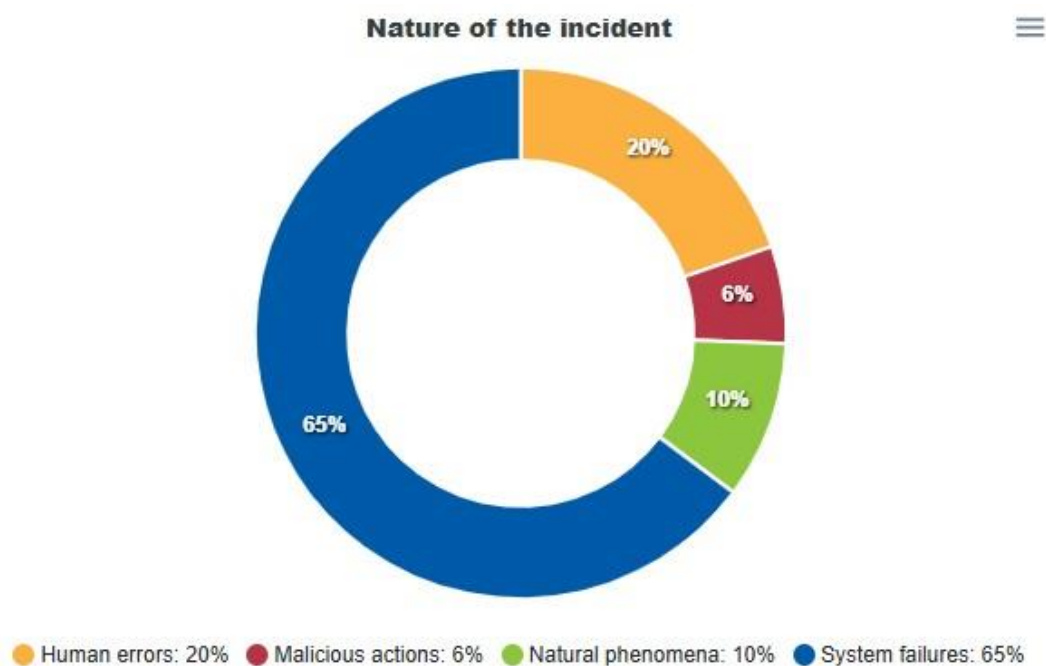


図 30 : 根本原因の категория – 2012 年から 2024 年までに報告された EU における通信セキュリティインシデント

興味深いことに、悪意のある行為の影響を受けた**資産**は、影響を受けた資産全体の分類とは大きく異なっている。1 位はサーバーで 20%、2 位はスイッチおよびルーターで 19% だった。4 位はモバイル基地局で 13%、5 位は地下ケーブルで 9% だった。「その他」の категорияは 19% を占めている。

さらに、悪意のある行動の影響を受けたサービスについては、52%が固定インターネットサービス、44%がモバイルインターネットサービスに関連し、15%が OTT サービスに関連していた。

Technical assets affected



● Addressing servers: 20%
 ● Other: 19%
 ● Switches and routers: 19%
● Mobile base stations and controllers: 13%
 ● Underground cables: 9%

図 31 : 悪意のある行動による影響を受けた技術資産 2012 年～2024 年

7.2 多年度トレンド – サービスへの影響

この期間、携帯電話とモバイルインターネットは、2024 年にはそれぞれ 58% と 50% と、再びインシデントの影響を最も受けた分野となった。

Impact per service per year

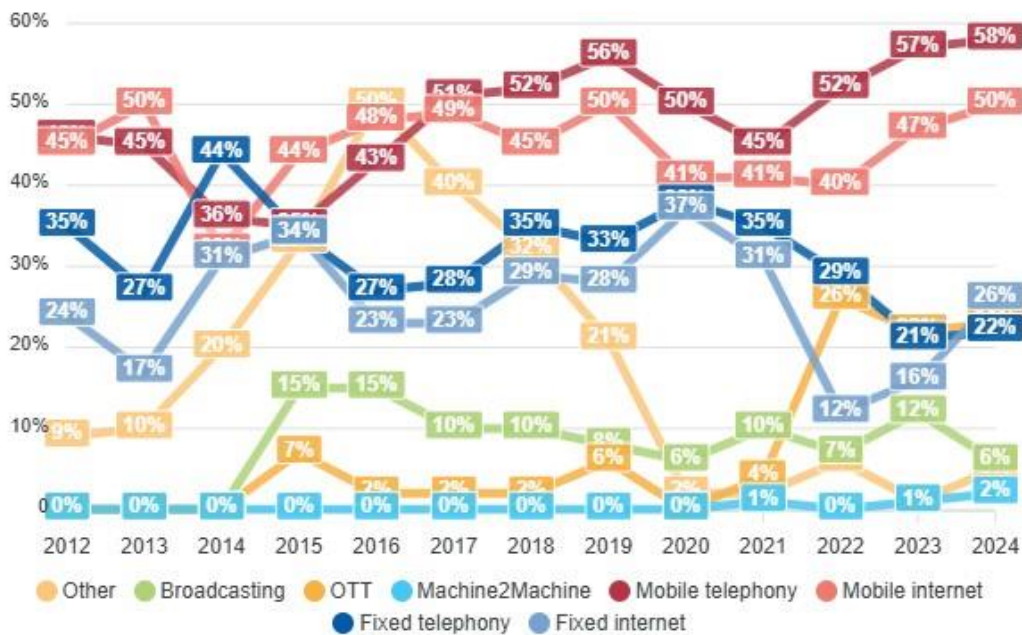


図 32 : 2012 年から 2024 年までの各サービスの影響動向

固定インターネットのインシデントは 2022 年以降も増加を続け、2024 年には 26% に達する一方、固定電話サービスは 2023 年とほぼ同じ水準にとどまっている。興味深いことに、マシン間通信のインシデントは、他のすべての分野に比べ依然として非常に低い水準にあるが、1% から 2% に増加している。

7.3 複数年にわたる傾向 – インシデントの影響の深刻度

ENISA は、EECC に基づくインシデント報告に関する技術ガイドライン⁽²⁰⁾ を公表しており、その中には、しきい値、重大度の推定、損失時間の計算などが含まれている。関連する複数年にわたる傾向は、**図 33** に示されている。

2021 年以降、**非常に大規模なインシデント**の報告件数は 2021 年の 62 件から 2024 年には 92 件へと増加している。非常に大規模なインシデントとは対照的に、**大規模なインシデント**は 2021 年以降、2021 年の 62 件から 2024 年には 52 件へと着実に減少している。**軽微なインシデント**は、約 3 年間にわたって着実に減少していたものの、2024 年には 26 件から 44 件へと、昨年と比較して増加している。

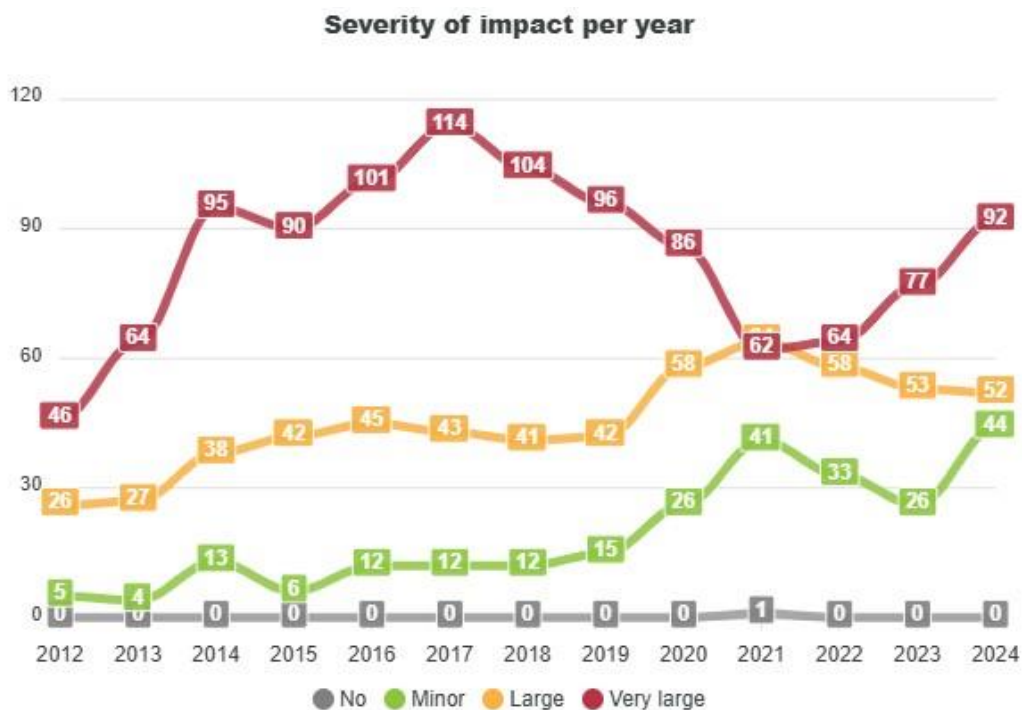


図 33 : 各年の影響の深刻度 – 2012 年から 2024 年までの複数年傾向（インシデント件数）

7.4 複数年トレンド – インシデント件数およびユーザー損失時間

長年にわたり、インシデントの数は着実に増加し、現在では 188 件と、これまでで最も多い件数となっている。インシデントの増加とは対照的に、損失時間は減少を続けており、10 年前とほぼ同じ水準にとどまっている。

²⁰ <https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc>, 2021 年 3 月。

Number of outages and userhours lost per year

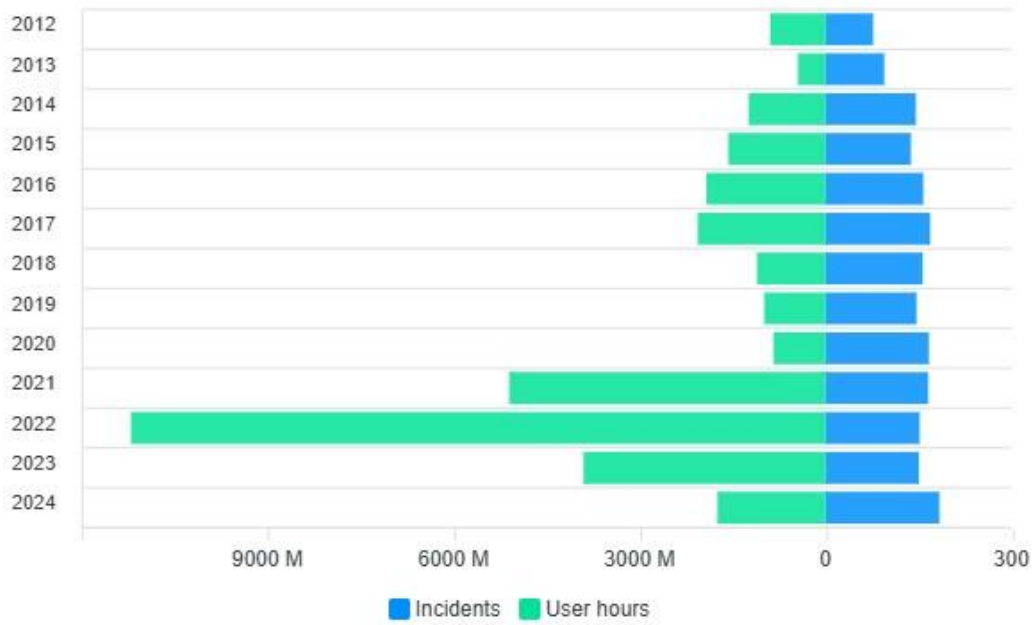


図 34 : 2012 年から 2024 年までの年間インシデント件数およびユーザー損失時間

8. 結論

結論として、このプロセスとより広範な政策の文脈に関する主な発見事項と一般的な観察結果を以下に示す。

主な発見

- ENISA に報告された電子コミュニケーションのインシデントは、過去最多の 188 件に達した。
- 過去 4 年間で、**非常に大きな影響**を与えたインシデントが 62 件から 92 件へと**着実に増加している**。
- インシデントの件数は増加しているが、ユーザーの損失時間は増加していない。実際、過去 3 年間で継続的に減少し、2014 年には 10 年前とほぼ同じ水準に戻っている。
- 2024 年には、**サードパーティによって** 65 件のインシデントが**障害**として報告され、2023 年の 52 件から増加した。
- 影響の点では、**システム障害**が引き続き大部分を占め、2024 年には 113 件で 60%に達した。これらは世界全体で 5 億 4,800 万ユーザー時間に相当し、2023 年と比較すると 6 倍（34 億 3,900 万時間）の減少となっている。
- インシデントは 2023 年の 156 件から 188 件へと増加したものの、失われた総ユーザー時間は大幅に減少した。このことから、通信インフラおよびプロセスはインシデントに対するレジリエンスが向上していると考えられる。
- **自然現象**によるインシデントは引き続き増加しており、その割合は 13% に達し、失われたユーザー時間は 7,200 万時間から 6 億 500 万時間に増加している。
- **人為的ミス**によるインシデントは、インシデントの割合では昨年と同じ 19% にとどまっている。しかし、失われたユーザー時間は 1 億 8,100 万時間から 4 億 200 万時間に増加している。
- **悪意のある行為**は、報告されたインシデントの割合（2024 年は 15 件、2023 年は 16 件）と、失われたユーザー時間（2024 年は 1 億 8,400 万時間、2023 年は 2 億 1,400 万時間）の両方で減少を続けている。
- 携帯電話と**モバイルインターネット**は、それぞれ 58% と 50% のインシデントを占め、最も影響を受けた分野でした。
- **固定インターネット**は、インシデントの報告件数および割合において、過去 3 年間で 12% から 2024 年には 26% へと増加を続けている。
- **国境を越えた**インシデントは報告されていない。

政策上の観察事項

- 2024 年 10 月 18 日をもって、NIS2 指令により EECC の第 40 条から第 41 条が廃止され、公衆電子通信網のプロバイダや公衆利用可能な電子通信サービスのプロバイダなど、複数のセクターにおける完全性および可用性の侵害の報告が統合されることに留意すべきだ。
- 2025 年の移行期間中、ENISA は、ECASEC 専門家グループおよび NIS 協力グループを通じて、各国当局と協力し、特にインシデントの報告と国境を越えた監督に関して、EU のさまざまな法律間の相乗効果を見出し、活用していく。

- さらに、新たな動向をよりよく反映し、報告を容易にし、事務負担を軽減するため、加盟国との定期的な協議において、CIRAS の方法論およびガイドラインの見直しも検討される可能性がある。

ENISA は、通信セキュリティを担当する各国当局および NIS 協カグループと引き続き協力し、セキュリティインシデントの報告を効率的かつ効果的に実施していく。また、本報告書作成にご協力いただいたすべての方々に、この場をお借りして感謝申し上げます。