ENISA

# 年次報告書

# 2024 年

# トラストサービス・セキュリティ・インシデント

2025 年 6 月

# ENISA について

欧州連合サイバーセキュリティ機関（ENISA）は、2004 年以来、欧州のサイバーセキュリティ強化に取り組んでいる。ENISA は、EU、加盟国、民間セクター、および欧州市民と協力して、情報セキュリティの優れた実践方法に関する助言や勧告を策定している。

ENISA は、EU、加盟国、民間セクター、欧州市民と協力して、情報セキュリティの優れた実践に関する助言と勧告を策定している。ENISA は、EU 加盟国が関連する EU 法を実施するのを支援し、欧州の重要な情報インフラとネットワークのレジリエンス改善に取り組んでいる。ENISA は、EU 全体のネットワークおよび情報セキュリティの改善に取り組む国境を越えたコミュニティの発展を支援することにより、EU 加盟国の既存の専門知識を強化することを目指している。

ENISA とその活動の詳細については、www.enisa.europa.eu を参照。

## 連絡先

本報告書の内容に関するお問い合わせは、incidentreporting@enisa.europa.eu まで電子メールでご連絡ください。本紙に関する報道関係者のお問い合わせは、press@enisa.europa.eu まで電子メールでご連絡ください。

## 認可者

ロッセン・ナイデノフ、ENISA

ヌノ・ロドリゲス・カルバーリョ、ENISA

エドガース・タウリンス、ENISA

## 謝辞

ENISA European Competent Authorities for Trust Services からいただいたレビューと意見に感謝する。ECATS 専門家グループは、EU 加盟国、欧州自由貿易連合（EFTA）、欧州経済地域（EEA）および EU 加盟候補国の 30 カ国の監督機関の専門家で構成されている。現在、RTR オーストリアの代表者が議長を務めている。

## 法的通知

本書は、別段の記載がない限り、ENISA の見解および解釈を代表するものであることに留意されたい。本出版物は、規則（EU）2019/881 に従って採択されない限り、ENISA または ENISA 団体の法的措置と解釈されるべきではない。本出版物は必ずしも最新技術を代表するものではなく、ENISA は随時更新することがある。

サードパーティーの情報源は適宜引用している。ENISA は、本書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は責任を負わない。

本書は情報提供のみを目的としている。無料でアクセスできなければならない。ENISA および ENISA を代理する者は、本出版物に含まれる情報の使用について責任を負わない。

## 著作権表示

© 欧州連合サイバーセキュリティ機関（ENISA）、2025 年

特に断りのない限り、本書の再利用はクリエイティブ・コモンズ 表示 4.0 国際（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、適切なクレジットを付与し、変更を示すことを条件に、再利用が許可されることを意味する。

欧州連合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、各権利所有者に直接許可を求める必要がある場合がある。

ISBN 978-92-9204-711-5, doi: 10.2824/3699305, ISBN: 2599-9435

# 目次


エグゼクティブサマリー ..... 5

1. 序論 ..... 7

1.1 範囲 ..... 7

1.2 eIDAS 規則 ..... 7

1.3 免責事項 ..... 7

1.4 構成 ..... 7

2. インシデント報告の枠組み ..... 8

2.1 インシデント報告プロセスの概要 ..... 8

2.2 インシデント報告ツール ..... 9

2.3 セキュリティインシデントの匿名化された例 ..... 10

3. インシデント分析 ..... 13

3.1 根本原因のカテゴリー ..... 13

3.1.1 システム障害 ..... 14

3.1.2 ヒューマンエラー ..... 16

3.1.3 悪意ある行為 ..... 18

3.2 技術的原因 ..... 20

3.3 影響を受けたサービス ..... 20

3.4 影響を受けた資産 ..... 21

3.5 適格サービス対非適格サービス ..... 22

4. 複数年ごとの傾向 2017-2024 ..... 23

4.1 根本原因の傾向 ..... 23

4.2 インパクトの重大性の傾向 ..... 25

4.3 サービスへの影響傾向 ..... 26

5 結論 ..... 27

# エグゼクティブサマリー

各国の監督団体は、eIDAS[1] 規則の第 19 条に従い、ENISA および欧州委員会に対し、毎年、被認定違反に関する年次報告書を送付しなければならない。

これは、ENISA が EU のトラストサービス部門向けに作成した、根本原因、統計、傾向を分析した第 8 回目の報告である。これは、EU 加盟国 21 カ国および EFTA 加盟国 3 カ国から ENISA に報告された、2024 年に報告された違反の概要をまとめたものである。

2024 年には、これらの国から合計 **44 件のインシデントが**報告された。

2024 年のインシデント報告から**得られた主な知見は**、以下のリストにまとめられている。

- EU の監督団体（SB）の半数（24 カ国中 **12 カ国**）は、報告されたインシデントが 0 件であったとして、それぞれの報告書を送付した。
- 報告されたインシデントは、2023 年の 63 件から **44 件に減少した**。しかし、2023 年にはインシデントを報告した MS が 6 つ多かったことに留意すべきである。
- インシデントの分布は、システム障害が 63%（2023 年は 64%）、人為的ミスが 23%（2023 年も同じ）、悪意ある行為が 14%（2023 年も同じ）となっており、2023 年と比較すると、割合的にはほぼ同じである。
- インシデントによる全体的な影響は **6 億 1,800 万**ユーザー時間の損失で、**2023 年の 31 億 8,400 万ユーザー時間の損失と**比べると 5 分の 1 に減少している[2] 。
- **悪質な行為による影響が**最も大きく、5 億 7,100 万時間が失われ、全喪失時間の 92%以上を占めた。2023 年には全喪失時間の 98%（3 億 1,400 万時間）が失われたが、それと比べて減少している。

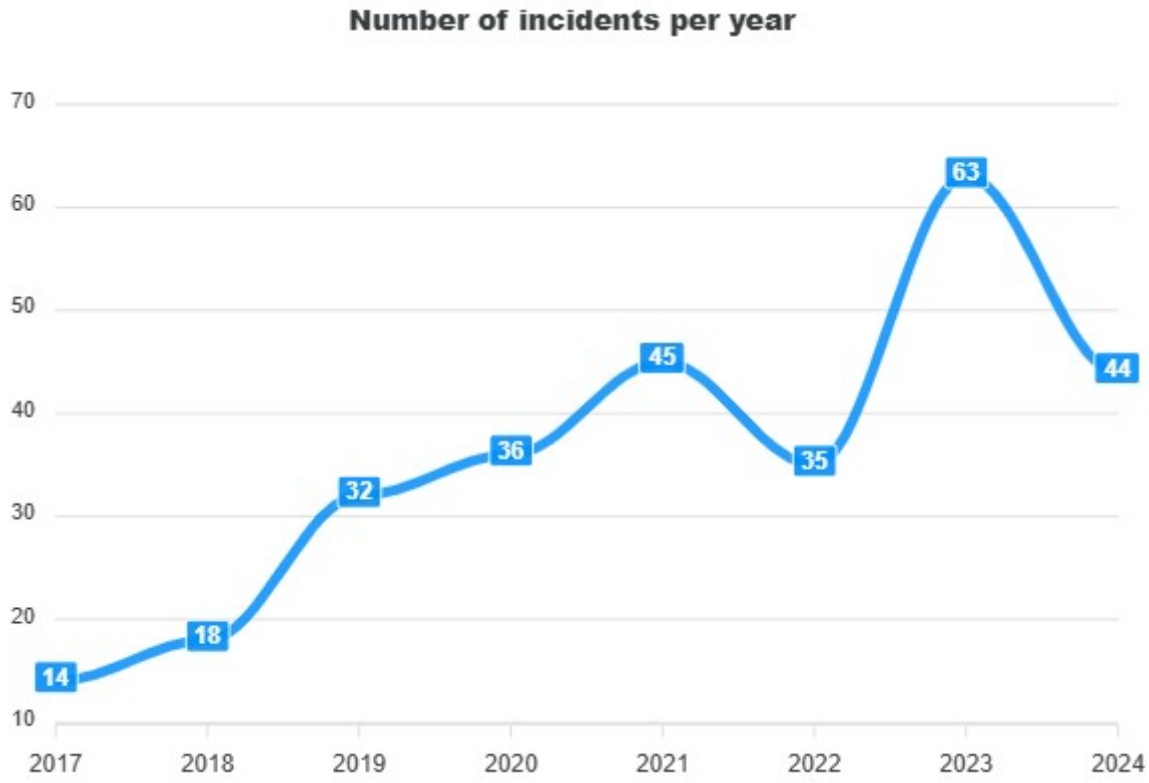
**ハイライト 2024**

**システム障害が**インシデントの半数以上を占め、過去 8 年間のインシデント報告の主な根本原因となっている。

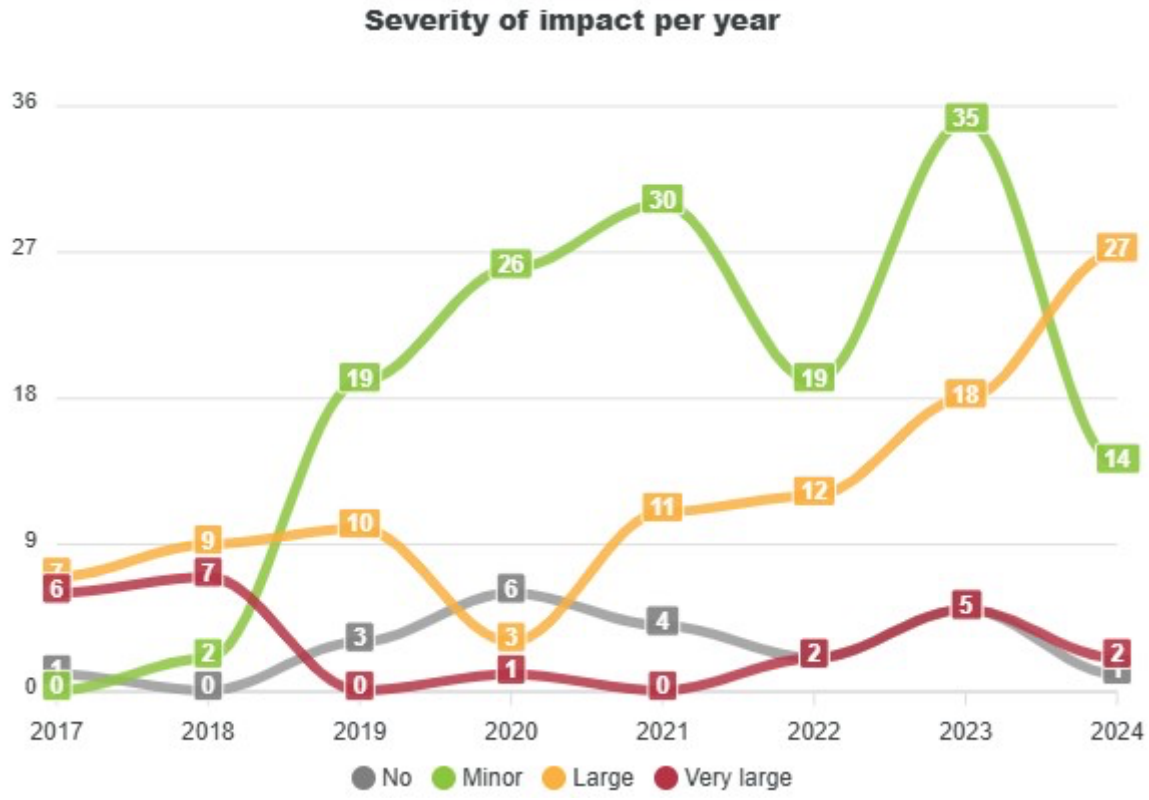
**悪意のある行為は**、ユーザー損失時間の点で最も影響力のある根本原因であり、全ユーザー損失時間の 92%以上がこの根本原因によるものである。

[1] 2014 年 7 月 23 日付欧州議会および理事会規則（EU）第 910/2014 号「域内市場における電子取引のための電子的本人確認およびトラストサービスに関する規則であり、指令 1999/93/EC を廃止するもの」 https://eur-lex.europa.eu/legalcontent/EN/TXT/HTML/?uri=CELEX:32014R0910

[2] 報告書作成時点では、2023 年時点よりも 6 加盟国の報告が少ないことを考慮されたい。




- **影響という**点では、大規模なインシデントが引き続き**増加している。**



# 1. 序論

## 1.1 範囲

eIDAS 規則の第 19 条に基づき、EU 内のトラストサービス・プロバイダ（TSP）は、セキュリ ティインシデントが発生した場合、各国の監督機関に報告しなければならない。監督団体は、これらのインシデント報告の要約を欧州連合サイバーセキュリティ機関（ENISA）に年 1 回送付し、ENISA は報告されたセキュリティ・インシデントの集約された概要を公表する。

ENISA は、トラストサービスのセキュリティ・インシデントに関する詳細な統計を、オンラインの視覚的ツールである ENISA 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）（[3]）で公表している。このツールは、傾向とパターンのカスタム分析を可能にし、収集したデータの定量的・定性的分析を支援する。

本レポートは、2024 年中に監督団体から ENISA に提出されたインシデントの概要をまとめたものである。

## 1.2 eIDAS 規則

EU 規則 910/2014（eIDAS）は、欧州における電子 ID スキームおよびトラスト・サービス、国 内電子 ID スキーム、国境を越えた相互運用性および承認に関する規則を定めている。第 19 条は、適格および非適格トラスト・サービス・プロバイダ（TSP）に対し、提供されるトラスト・サービスまたはそこで保持される個人データに重大な影響を及ぼすセキュリティ違反または完全性の損失を報告する義務を定めている。

eIDAS 規則は以下を**目的として**いる：

- 電子署名が従来の署名と同等の法的効力を持つようにする；
- トラストサービスの欧州域内市場構築を視野に入れ、EU における電子商取引およびあらゆる種類の電子取引に対する障壁を取り除く；
- 電子署名が国境を越えて機能し、従来の紙ベースの同等のものと同じ法的地位を有することを保証する。

## 1.3 免責事項

第 19 条に従い、本文書にはインシデントに関する集計され匿名化された情報のみが含まれ、個々の国や個々の TSP に関する詳細は含まれない。

## 1.4 構成

本文書の構成は以下のとおりである：

- セクション 2 では、CIRAS ツールを含むプロセスを簡単に概説し、報告されたインシデントの匿名化された例を説明する；
- セクション 3 では、根本原因のカテゴリー、詳細な原因、影響を受けたサービスを示す。 - セクション 4 では、2017 年から 2024 年にかけてのインシデントの複数年にわたる傾向を示す。

[3] 詳細は https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-systemvisual-analysis/visual-tool; ツールのウェブサイトはこちら: https://ciras.enisa.europa.eu/

# 2. インシデント報告の枠組み

本節では、eIDAS 規制第 19 条に基づくインシデント（違反）報告の形式と手順について概説する。

## 2.1 インシデント報告プロセスの概要

強制的なセキュリティ侵害の通知プロセスには、**図 A に**示すように 3 つのステップがある。

1. TSP 団体は、重大な影響を及ぼすセキュリティ侵害について、各国の監督機関に通知する。
2. 国境を越えた影響がある場合、各国監督団体は相互および ENISA に通知する。
3. 各国監督団体は、報告された侵害に関する年次概要報告書を ENISA および欧州委員会に送付する。

**eIDAS 第 19 条は、EU の TSP に以下を求めている：**

**1)リスクをアセスメントする；**

**2)セキュリティ侵害を緩和するために適切なセキュリティ対策を講じること。**

**3)違反を各国の監督団体に報告すること。**

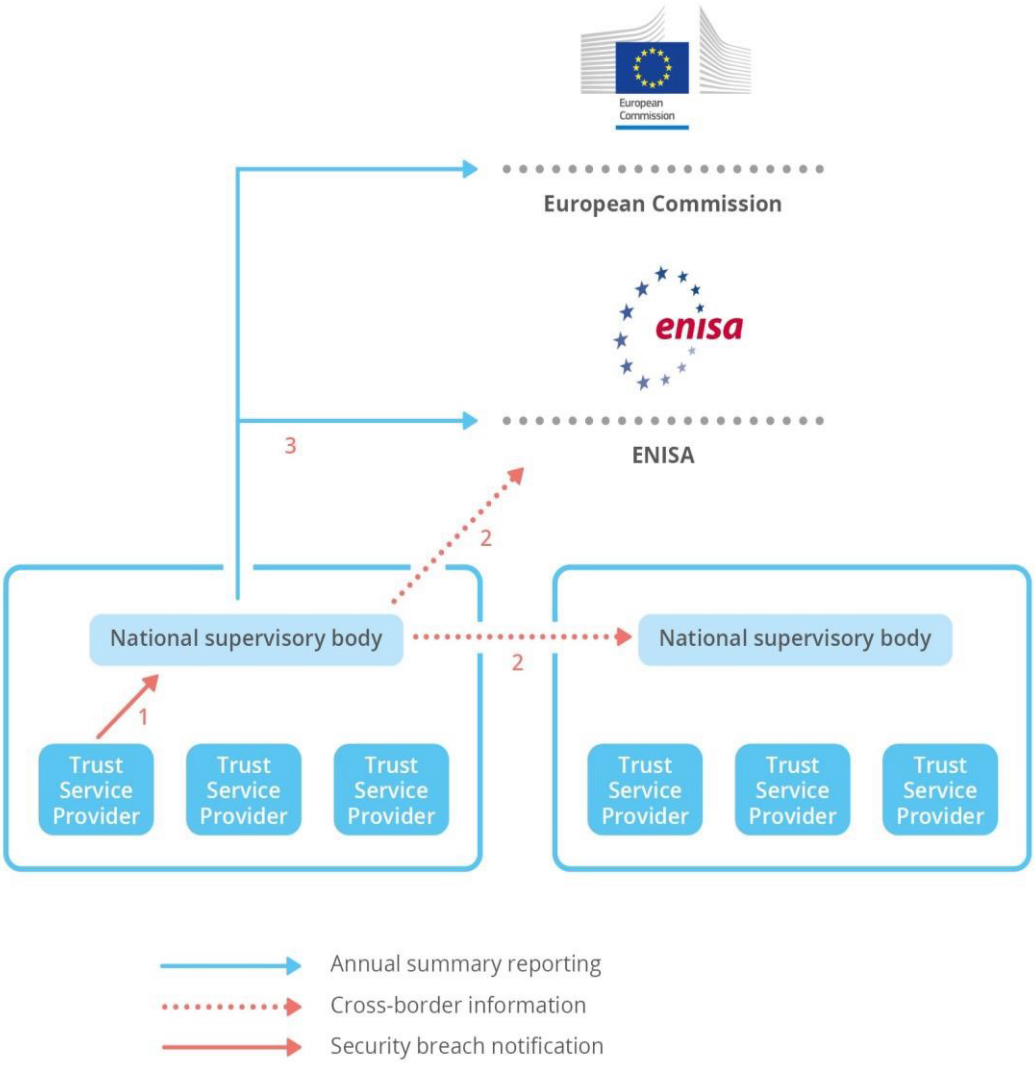



**図 A.** セキュリティ侵害の通知プロセス

## 2.2 インシデント報告ツール

各国当局の専門家は、ENISA のインシデント報告ツールである CIRAS にアクセスし、インシデント報告をアップロードしたり、特定のインシデントを検索して調査したりすることができる。

ENISA の報告テンプレートは、タイプセレクタで始まり、以下の 3 つのパートから構成される。

1. **インシデントの影響**：どのトラストサービスがどの程度影響を受けたか？
2. **インシデントの性質**：インシデントの原因は何か？
3. **インシデントの詳細**：簡単な説明、サービスや資産の種類、重大度レベルなど。

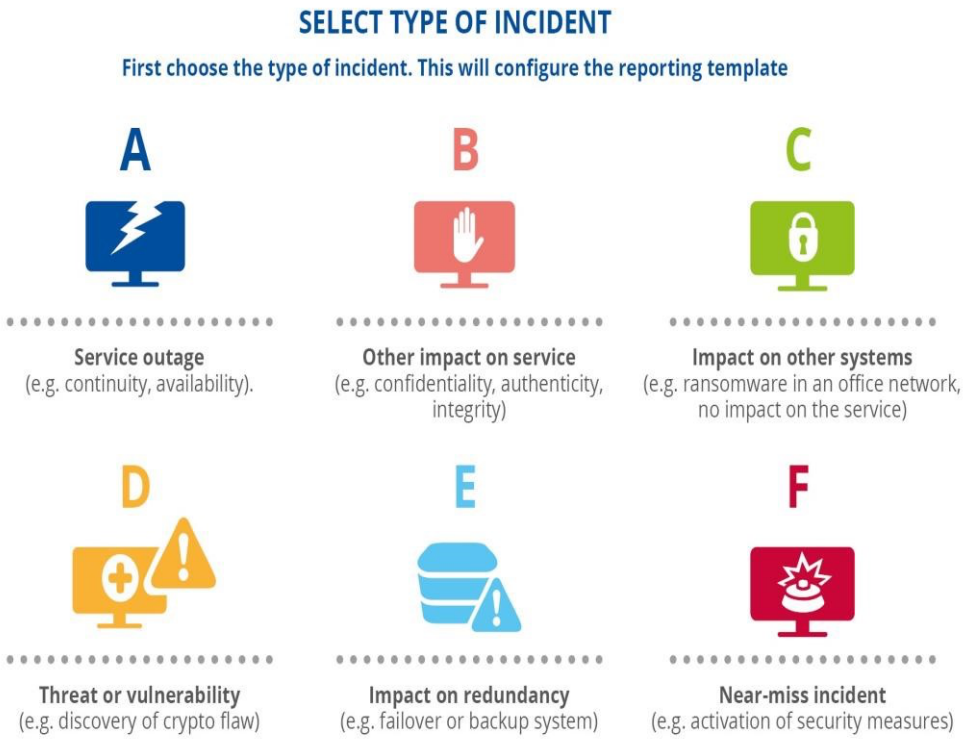



**図 B.** インシデント報告ツール

- **タイプ A**：サービス停止（継続性、可用性など）。たとえば、新しい道路の建設に使用する掘削機のオペレーターが誤ってケーブルを切断したために発生した障害は、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（機密性、認証性、完全性など）に対するその他の影響。例えば、人気のあるコラボレーションツールは、共有セッションに参加するエンドポイント間でセッションが開始されたときに確立されるメディアチャンネルのコンテンツを暗号化していない。このため、中間者攻撃（man-in-the-middle attack）によってメディア（音声、写真、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 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内のランサムウェア、サービスへの影響はない）。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と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）。例えば、暗号の脆弱性が発見された場合、タイプ D のインシデントに分類される。

- **タイプ E**：冗長性（フェイルオーバーやバックアップシステムなど）への影響。例えば、冗長化された 2 本の海底ケーブルのうち 1 本が断線した場合、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・ネットワークに悪意ある企てが行われた場合、タイプ F のインシデントに分類される。

選択されたタイプに応じて、テンプレート内のいくつかのフィールドは非アクティブになる。例えば、タイプ A のインシデントの場合、「脅威の重大度要因」と「脅威の重大度」フィールドはアクティブにならない。

## 2.3 セキュリティインシデントの匿名化された例

この段落では、報告されるいくつかの種類のインシデントについて、詳細かつ匿名化された例を示す。

| **インシデント例 1** | |
|---|---|
| **インシデントタイプ** | A - 基幹サービスの停止 |
| **影響を受けたサービス** | 電子署名、電子印鑑、電子タイムスタンプ |
| **根本原因** | システム障害 |
| **技術的原因** | 過負荷 |
| **影響を受けた資産** | 生成的（署名、捺印、タイムスタンプ）<br>証明書管理（証明書の登録、作成、一時停止、失効） 妥当性確認 |
| **コメント** | バックエンドシステムの過負荷による電子署名、電子印鑑、電子タイムスタンプサービスの利用不能。 |

| **インシデント例 2** | |
|---|---|
| **インシデントタイプ** | A - コアサービスの停止 |
| **影響を受けたサービス** | 電子署名、電子シール |
| **根本原因** | 悪意のある行為 |
| **技術的原因** | ランサムウェア |
| **影響を受けた資産** | 認証局（CA）プラットフォーム、署名/シールの生成および妥当性確認プラットフォーム、ネットワークプラットフォーム |

| | |
|---|---|
| **コメント** | プロバイダはランサムウェア攻撃を受けたが、トラストサービスをサポートするシステムに影響はなかった。<br>予防措置として、すべてのシステムをネットワークから切り離した。<br>証明書を失効させる必要はなかった。 |

| **インシデント例 3** | |
|---|---|
| **インシデント・タイプ** | A - コアサービスの停止 |
| **影響を受けたサービス** | 電子署名、電子タイムスタンプ |
| **根本原因** | システム障害 |
| **技術的原因** | ソフトウェアのバグ、設定の問題 |
| **影響を受けた資産** | 署名/シールの生成と妥当性確認プラットフォーム、ソフトウェア |
| **コメント** | サポートシステムの設定に問題があり、電子署名と電子タイムスタンプのサービスが利用できなくなった。 |

| **インシデント例 4** | |
|---|---|
| **インシデントタイプ** | B - 基幹サービスへのその他の影響 |
| **影響を受けたサービス** | 電子署名 |
| **根本原因** | 悪意のある行為 |
| **技術的原因** | マルウェアとウイルス |
| **影響を受けた資産** | シグネチャ/シールの生成と妥当性確認プラットフォーム |
| **コメント** | このインシデントは、適格な署名の認証情報の漏洩に関するものである。影響を受けた適格証明書は失効され、利用者に通知された。 |

| **インシデント例 5** | |
|---|---|
| **インシデントタイプ** | D - アクティブな脅威または脆弱性 |

| | |
|---|---|
| **影響を受けたサービス** | シグネチャ/シールの生成的プラットフォーム |
| **根本原因** | ヒューマンエラー |
| **技術的原因** | 誤ったソフトウェアの変更/更新 マルウェアとウイルス |
| **影響を受けた資産** | ソフトウェア |
| **コメント** | 適格な署名作成デバイスのミドルウェアにマルウェアの可能性あり。 |

# 3. インシデント分析

このプロセスに参加している 21 の EU 加盟国と 3 つの EEA 加盟国による 2024 年の年次サマリー報告には、合計 44 件のセキュリティインシデントが含まれている。

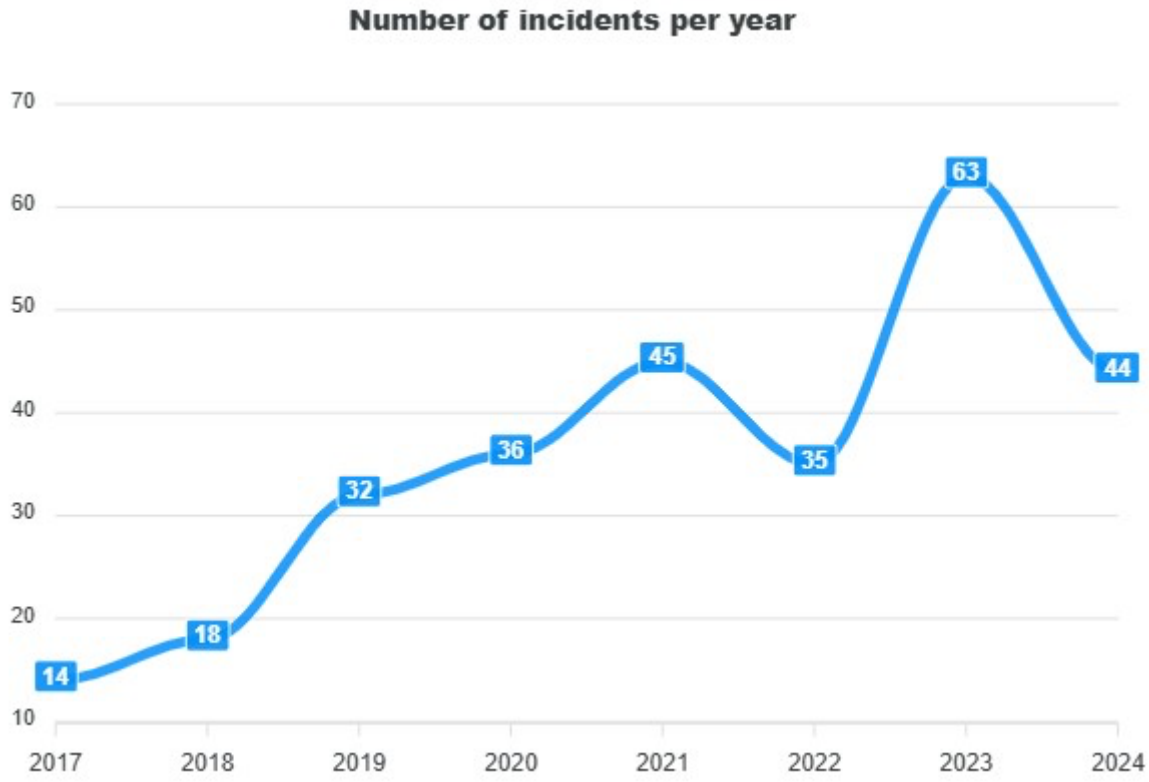



**図 1.**2017 年から 2024 年に報告されたインシデント数

## 3.1 根本原因のカテゴリー

**図 2 は**、根本原因別にインシデントの分布を示したものである。

インシデントによる全体的な影響は **6 億 1800 万時間のユーザー**損失で、うち 4200 万時間がシステム障害、400 万時間がヒューマンエラー、**5 億 7100 万時間が悪質行為によるもの**だった。一方、2023 年には 3 億 1,800 万時間のユーザー時間が失われ、システム障害が 100 万時間、ヒューマンエラーが 4,300 万時間、悪意ある行為が **3 億 1,400 万時間であった。**

インシデントの根本原因は 4 つのカテゴリーに分けられる。

- **システム障害**は 2024 年も引き続き主要な根本原因であり、2023 年の 40 件のインシデントの 63%に対し、28 件のインシデントのうち 64%を占めている。通常、システム障害はハードウェアの故障かソフトウェアのバグが原因である。
- **ヒューマンエラー**は 10 インシデントで 23%を占め、2023 年と同じ 22%であった。
- **悪意ある行為による**インシデントが 6 件で 14%を占め、これは 2023 年の 9 件と同じ割合である。
- **自然現象による**インシデントは報告されておらず、これは過去 3 年間の傾向である。

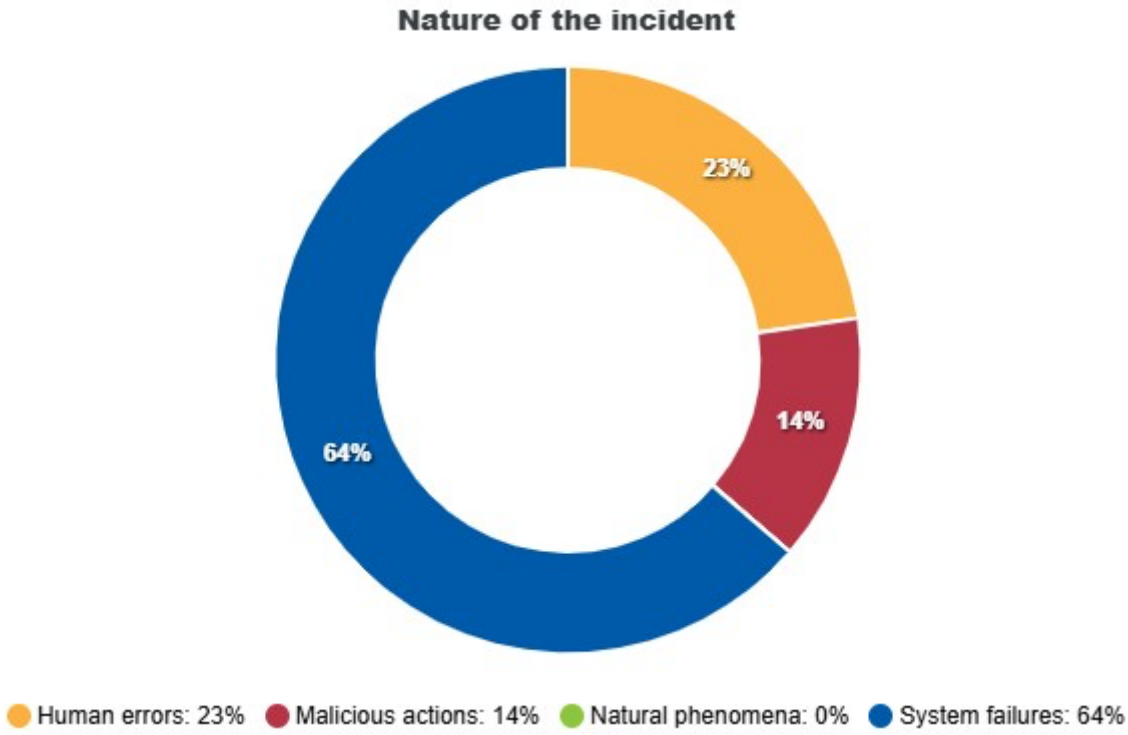



**図 2.**TSP セキュリティ・インシデントの根本原因 - 2024 年

**サードパーティによる障害**、すなわちインシデントがサードパーティに起因する場合も、サプライヤーやプロバイダへの影響をアセスメントする観点から追跡している。

2024 年には、報告された 44 件のインシデントのうち、7 件がサードパーティによる障害とマークされているのに対し、2023 年には 63 件のインシデントのうち 19 件がサードパーティによる障害とマークされている。

2024 年に報告されたインシデントのうち

- **6** 件が**システム障害に**分類された。
- **1** 件が**悪意ある行為に**分類された。

### 3.1.1 システム障害

システム障害は全 44 インシデントのうち 28 インシデントで、2024 年のシェアは 64%である。システム障害によって最も影響を受けたサービスは、全システム障害の 85%を占める電子署名である。

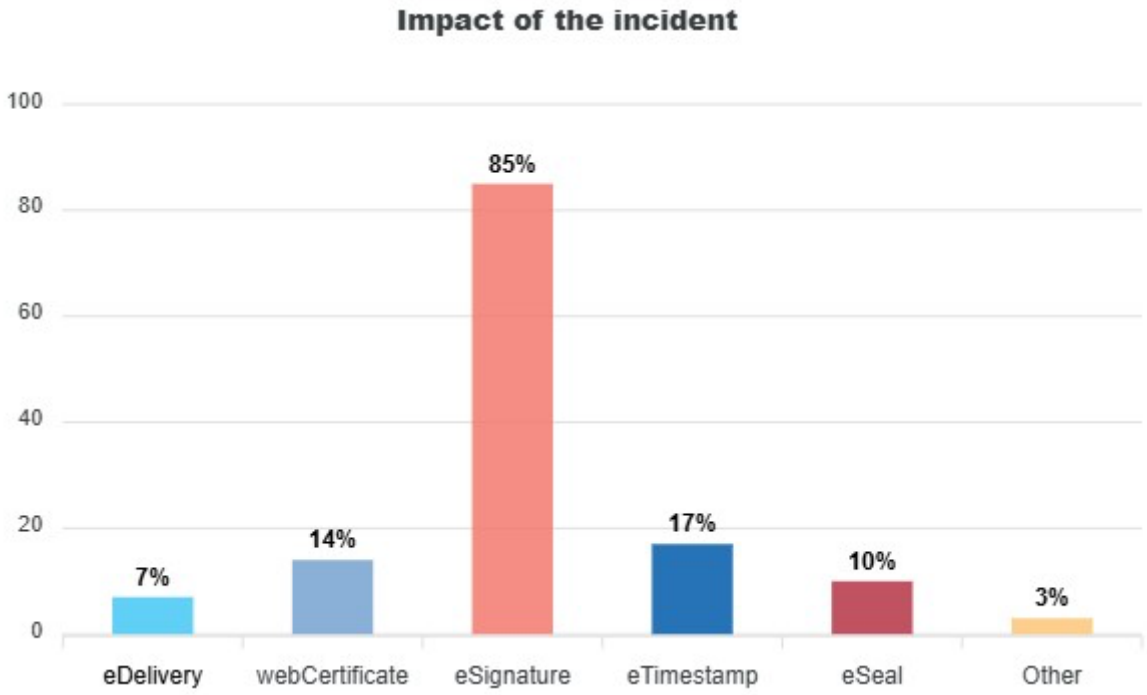



**図 3.**システム障害がサービスに与える影響 - 2024 年

システム障害の技術的原因のトップ 3 は、ハードウェア障害が 32%、ソフトウェアのバグが 28%、ポリシー手順の欠陥が 14%である。上位 2 つの原因は 2023 年と同様であるが、異なる点は、ポリシー・プロシージャが 5%でスコアの最下位であったのに対し、ソフトウェア変更の欠陥が 25%で 3 位であったことである。

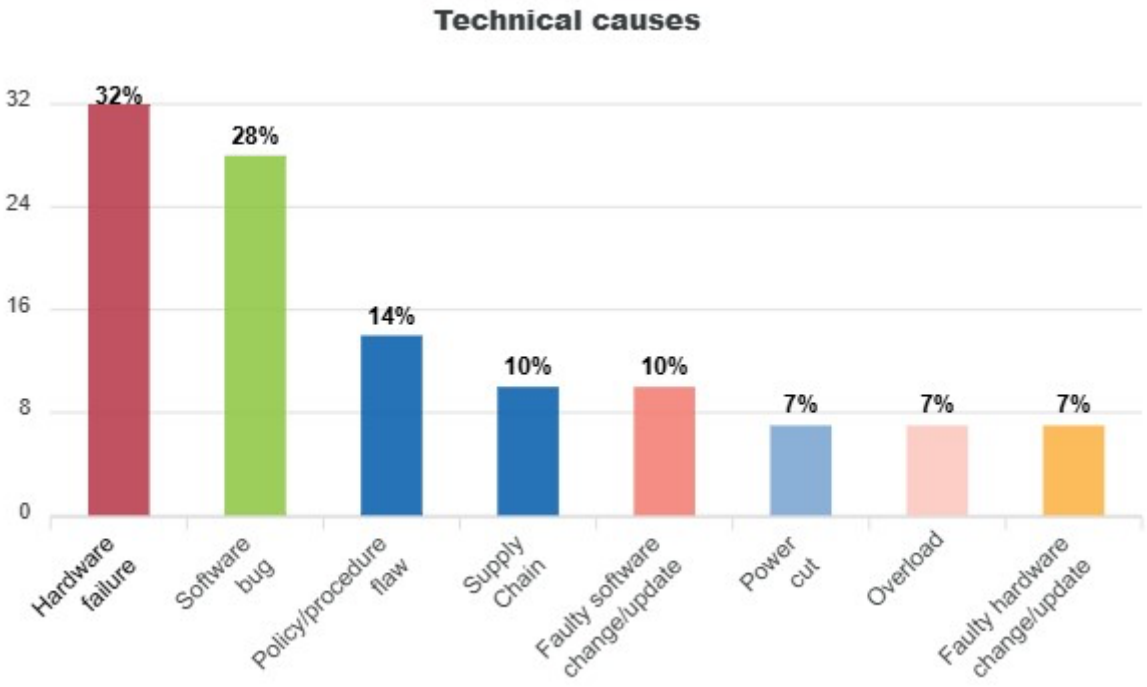



**図 4.**システム障害の技術的原因-2024 年

2024 年にシステム障害の影響を受けた技術的資産の上位 3 つは、認証機関プラットフォーム（32%）、登録機 関（32%）、署名/シールの生成と妥当性確認プラットフォーム（29%）であった。2023 年との違いは 2 位と 3 位の変化で、署名・シールの生成と妥当性確認プラットフォームが 30%で 2 位、ネットワークプラットフォームが 25%で 3 位となっている。

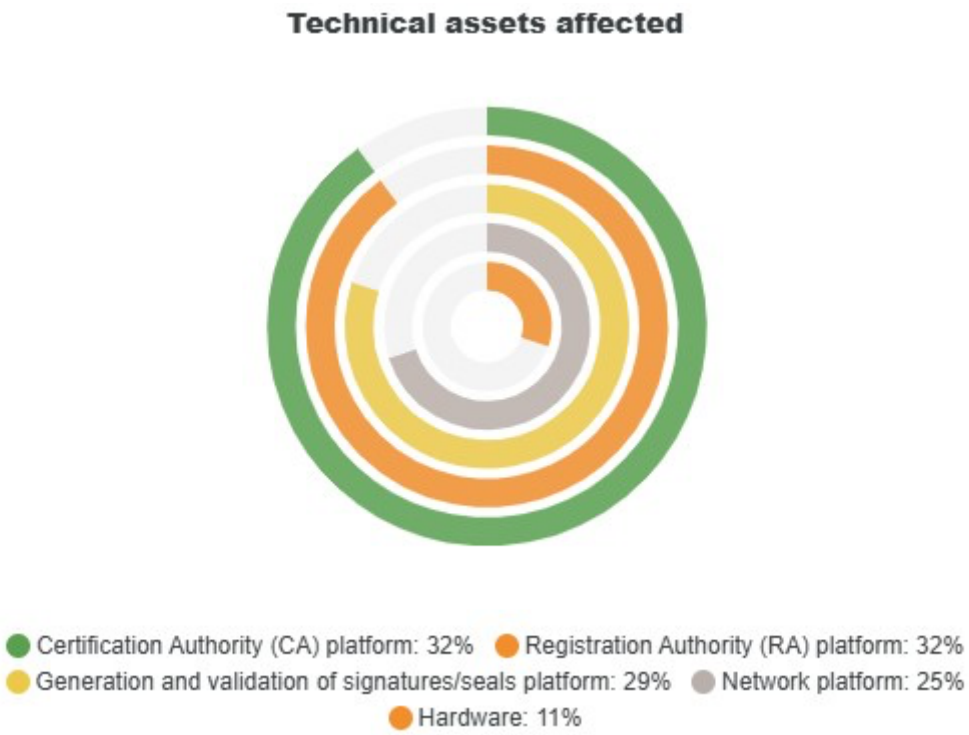



**図 5.**システム障害によって影響を受ける技術資産-2024 年

### 3.1.2 ヒューマンエラー

ヒューマンエラーのインシデントは合計 10 件で、2024 年の全インシデントの 23%を占める。

ヒューマンエラーは、システム障害に比べ、2024 年に影響を受けたサービスという点では限定的である。影響を受けたのは 3 件のみで、電子署名が 80%でトップ、これは 2023 年の 92%と同様である。2 番目と 3 番目は eTimestamp と webCertificate で、同じ 10%という結果であった。比較のため、2023 年には eSeal も 14%の影響を受けており、この年は 2 番目に影響を受けている。

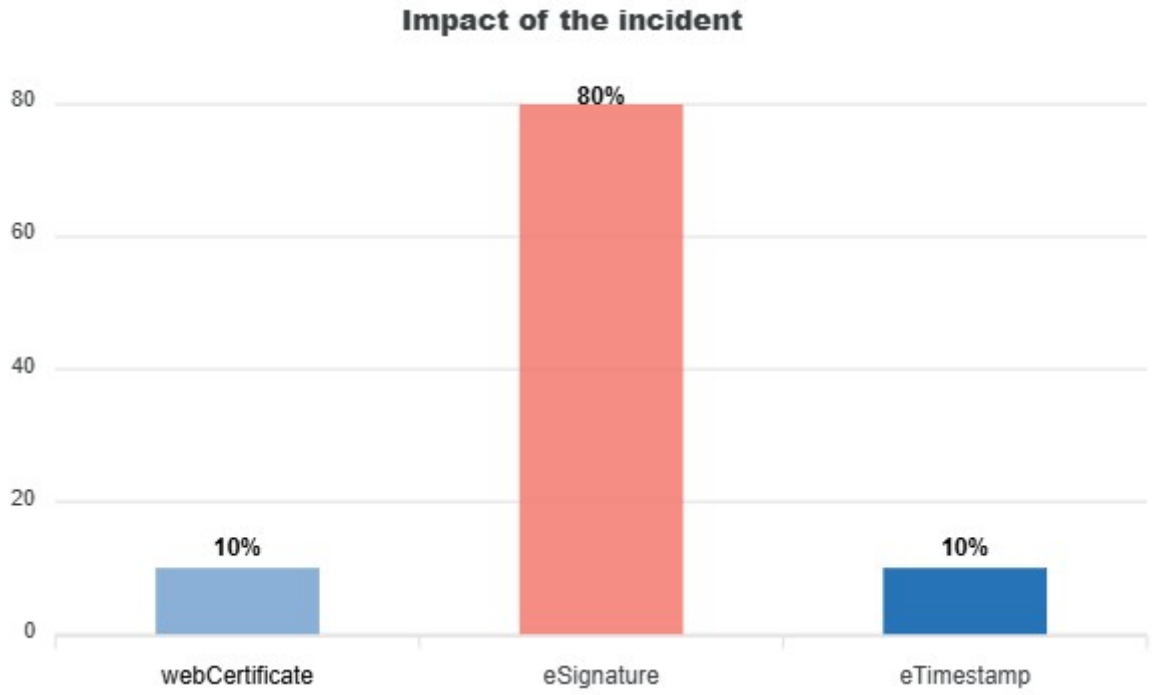



**図 6.**ヒューマンエラーによるサービスへの影響 - 2024 年

2024 年におけるヒューマン・エラーの技術的原因のトップ 3 は、ポリシー/手順の欠陥で 60%を占め、この原因が 42%であった 2023 年と同様であった。第 2 位はソフトウェアの変更/更新の不具合で 30%、最後がソフトウェアのバグで 10%であった。2023 年と比較すると、個人データの改ざんは 7%で最下位だった。

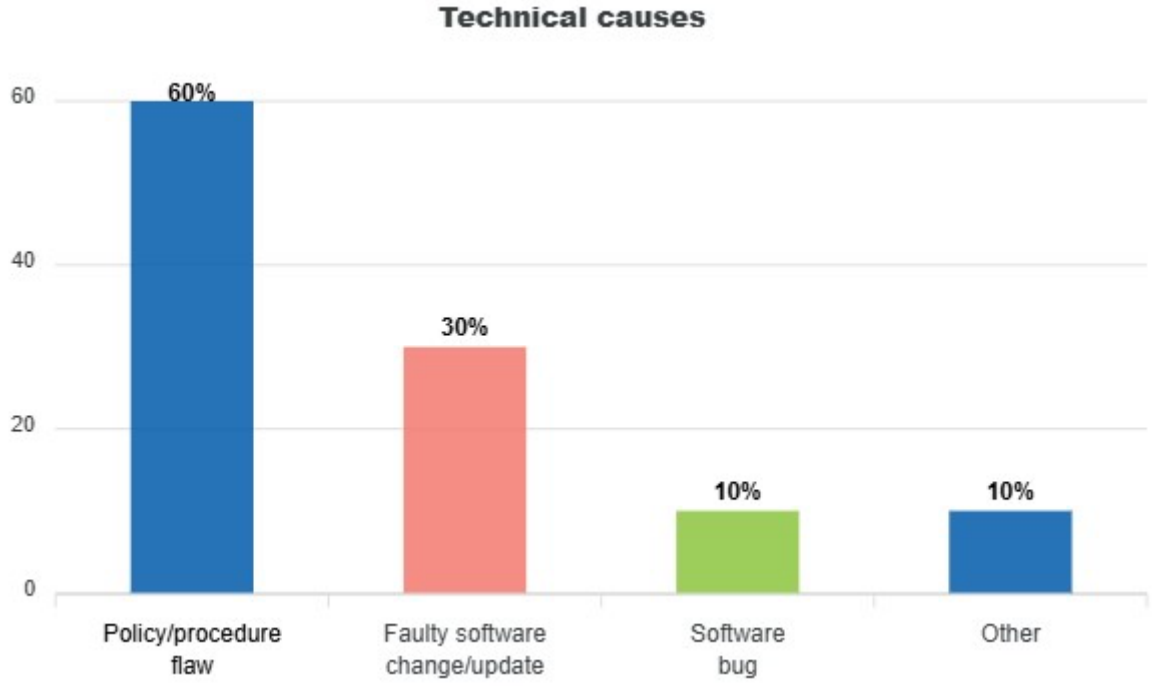



**図 7.**ヒューマンエラーの技術的原因-2024 年

2024 年にヒューマンエラーの影響を受けた技術的資産のトップ 3 は、署名/シールの生成と妥当性確認プラットフォームで 50%、2 位は認証局で 40%、最後がタイムスタンプと妥当性確認局でどちらも 10%であった。

2023 年との比較では、認証局が 29%でトップであり、残りの署名・捺印プラットフォームの生成と妥当性確認、登録局とソフトウェアはすべて 21%であった。

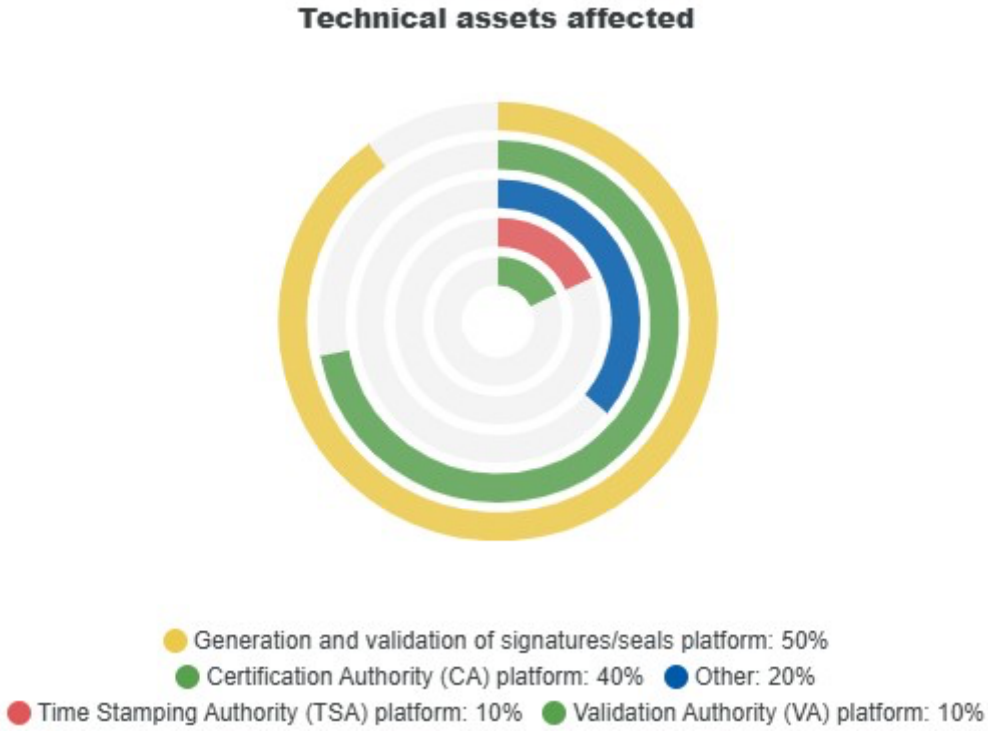



**図 8.**ヒューマンエラーによって影響を受けた技術資産-2024 年

### 3.1.3 悪意ある行為

悪意のある行為は、2024 年に 6 件のインシデントで 14%のシェアを占めている。2024 年の悪意ある行為には、非常にターゲットとなるサービスがあり、これは eSginature サービスであり、すべてのインシデントがこの特定のサービスで報告されている。

2024 年における悪意ある行為の技術的原因のトップ 3 は、個人データの改ざんが 50%、2 位がマルウェアとウイルスで 33%、最後がデータの盗難・紛失と機器の盗難・紛失でともに 16%であった。

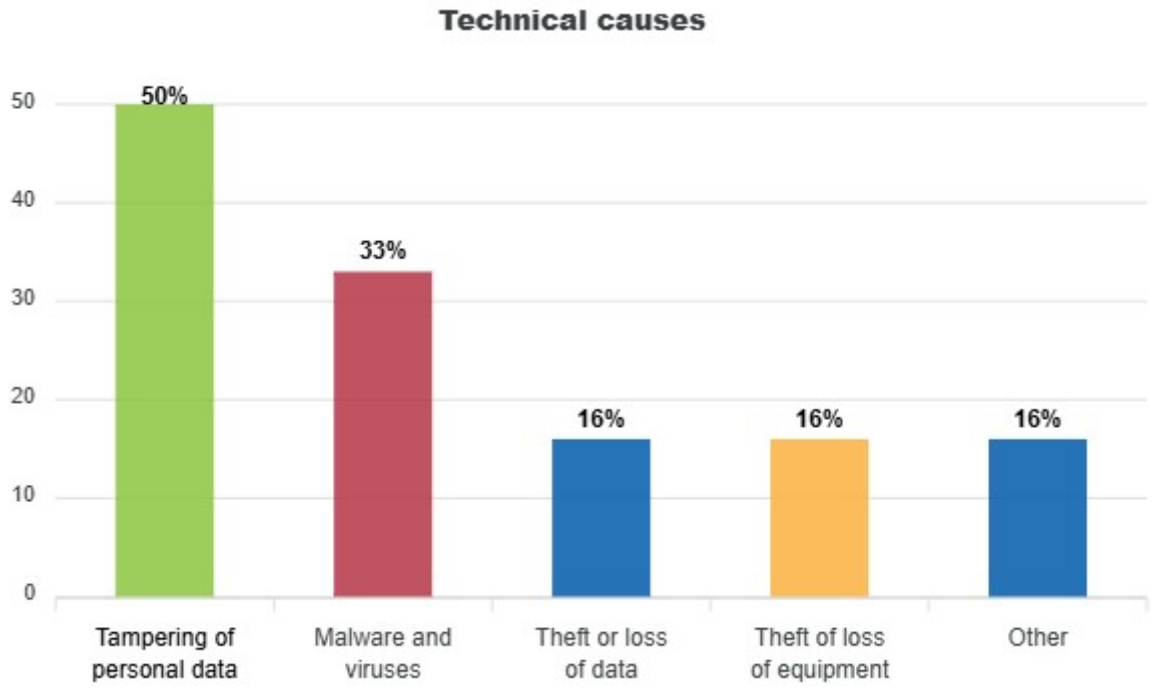



**図 9.**悪意ある行為の技術的原因 - 2024 年

2024 年に悪意ある行為によって影響を受けた技術的資産の上位 3 つは、Archive が 33%、署名/シールの生成と妥当性確認プラットフォームが 33%、認証局とネットワークプラットフォームが 17%であった。 2023 年と比較すると、影響を受けた資産のトップは認証局で 44%、2 位は署名/シールの生成と妥当性確認プラットフォームで 33%、3 位は登録局で 22%であった。

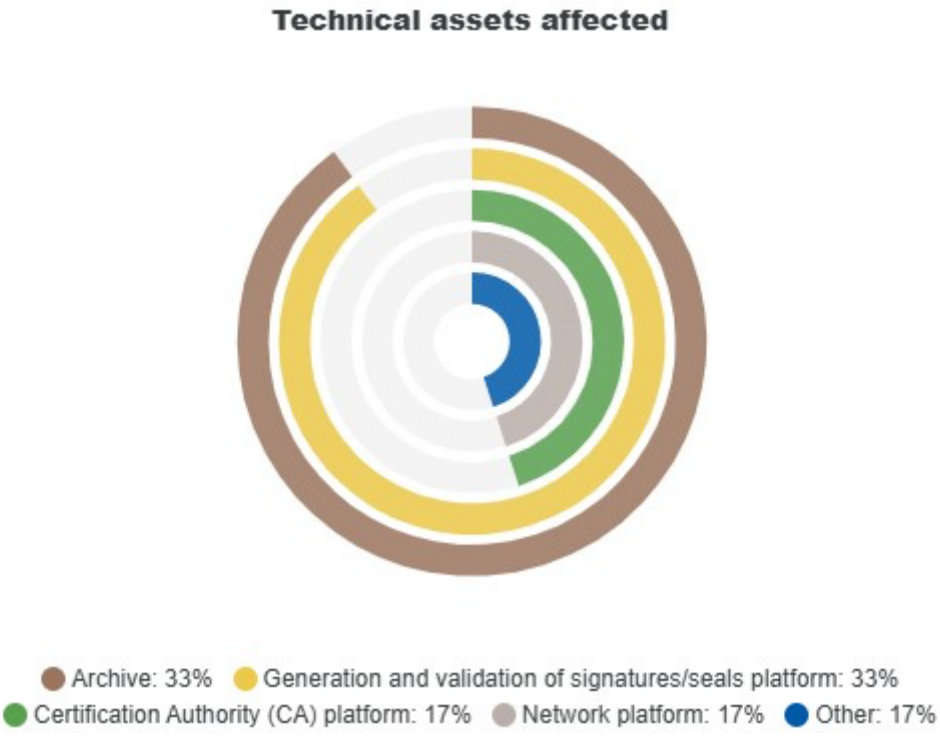



**図 10.**悪意ある行為によって影響を受けた技術資産 - 2024 年

## 3.2 技術的原因

インシデントは多くの場合、1 つの原因（[4]）によってのみ引き起こされるのではなく、複数の詳細な原因（すなわち、イベントの連鎖）によって引き起こされることに注意することが重要である。

2024 年のインシデントの**詳細原因のトップは、ポリシー／手順の欠陥で**あり、10 件のインシデントで全インシデントの 22%を占めた。これは、ポリシーの欠陥が 13 インシデントで 15%と 3 番目の技術的原因であった 2023 年と比較して増加している。

ソフトウェアのバグが 9 件で全体の 20%を占め第 2 位となったが、これは 11 件で 17%であった 2023 年よりもシェアが増加している。

ハードウェアの不具合は 20%、9 インシデントで 3 位。

**ソフトウェアの変更/更新の**不具合は 13%、6 インシデントで 4 位となっており、2023 年に 20%、13 インシデントでトップだったのと比べると大きな変化である。

報告されたインシデントの詳細な原因の内訳は、**図 11 で**見ることができる。

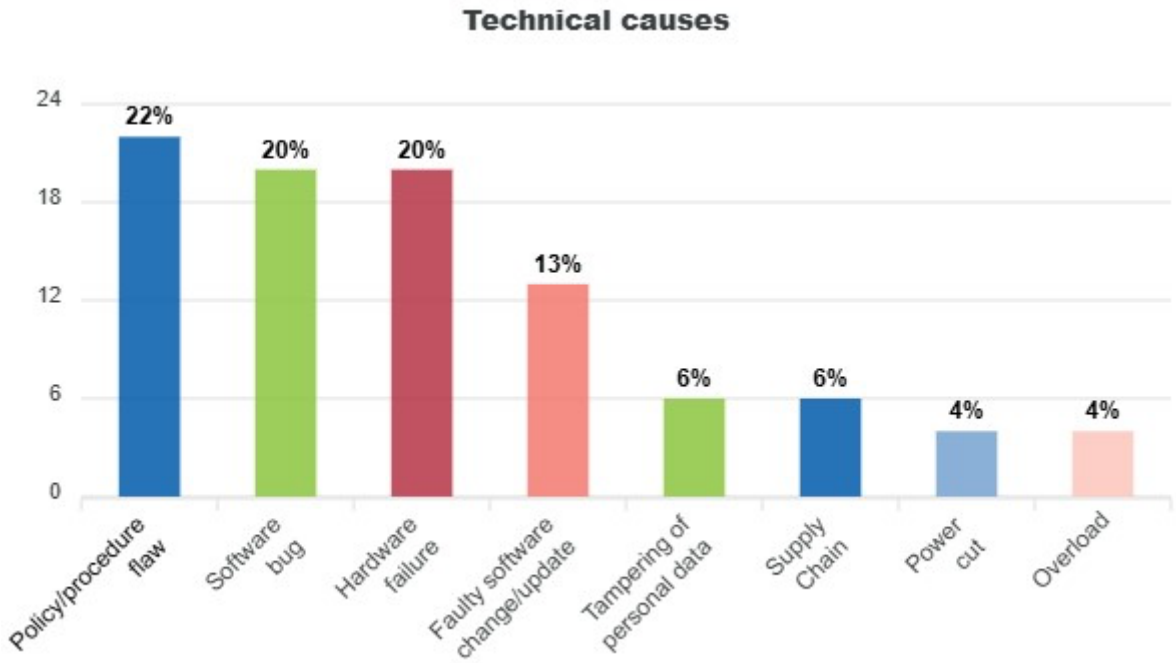



**図 11.**トラストサービスのセキュリティ・インシデントの詳細な原因 - 2024 年

## 3.3 影響を受けたサービス

2024 年に最も影響を受けたサービスは、電子署名、電子タイムスタンプ、ウェブ証明書である。

**図 12 に**見られるように、報告されたインシデントのほとんど（**86%**）は**電子署名**（[5]）に影響を及ぼしており、2023 年には 95%が電子署名に影響を及ぼしていた。

[4] 「その他」はここでは定義されていない。

[5] 第 3 条(10)「電子署名」とは、電子形式のデータであって、電子形式の他のデータに添付され、または論理的に関連付けられ、署名者が署名するために使用するものをいう。

eTimestamps はわずか 13%で 2 位、代表者は 6 インシデントで、これは 2023 年の 12%、8 インシデントと同様である。

これは 2023 年の 4%、3 インシデントから増加している。

eSeal は 6%と 3 インシデントで最も減少したが、2023 年には 26%と 7 インシデントであった。

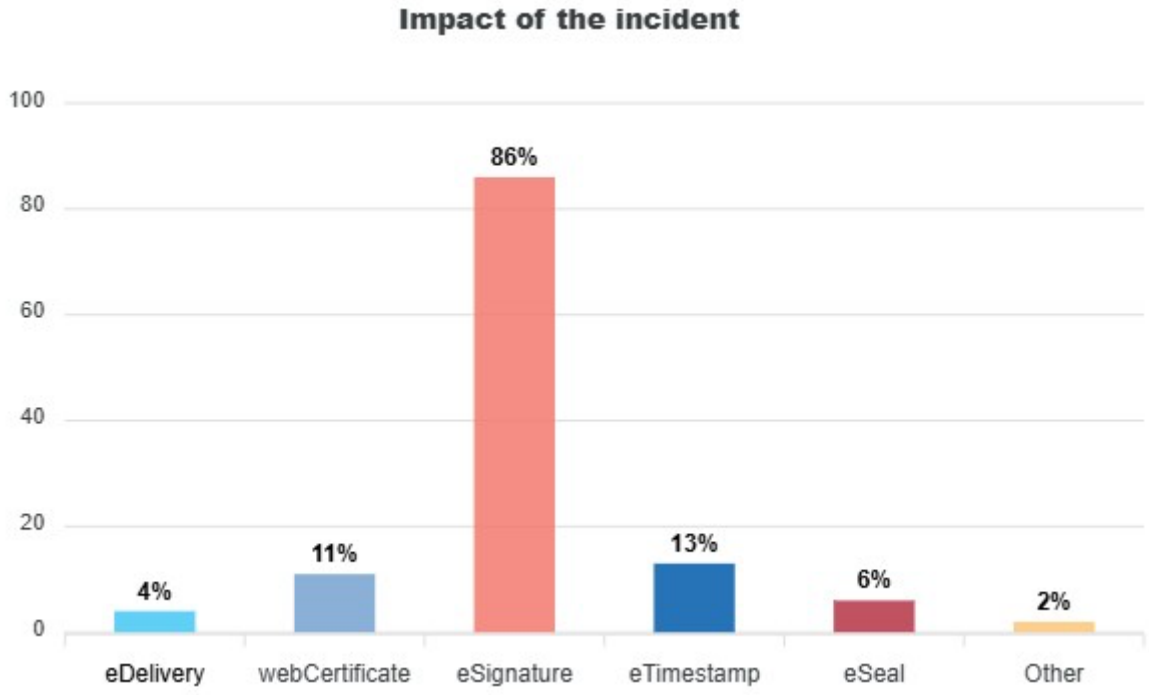



**図 12.**トラストサービスへのインシデントの影響 - 2024 年 [6]

## 3.4 影響を受けた資産

最後に、インシデントによって影響を受けた**原資産も**追跡しており、**図 13 で**見ることができる。

影響を受けた資産のトップは、署名／シールの生成と妥当性確認プラットフォームで、34%、インシデント数 15 件となっており、2023 年の 28%、インシデント数 18 件と比較して割合が増加している。

2024 年に最も影響を受けた資産の第 2 位は、認証機関プラットフォームで 32%、インシデント 14 件。

登録機関プラットフォームは 23%、10 インシデントで 3 番目に影響を受けた資産であり、これは 21%、13 インシデントであった 2023 年と同様である。

ネットワーク・プラットフォームは 18%、インシデント 8 件で、2023 年の 24%、倍増の 15 件に比べるとシェアは減少している。

[6] いくつかのインシデントが複数のサービスに影響を与えたため、図中の数字が 100%を超えていることに注意してください。

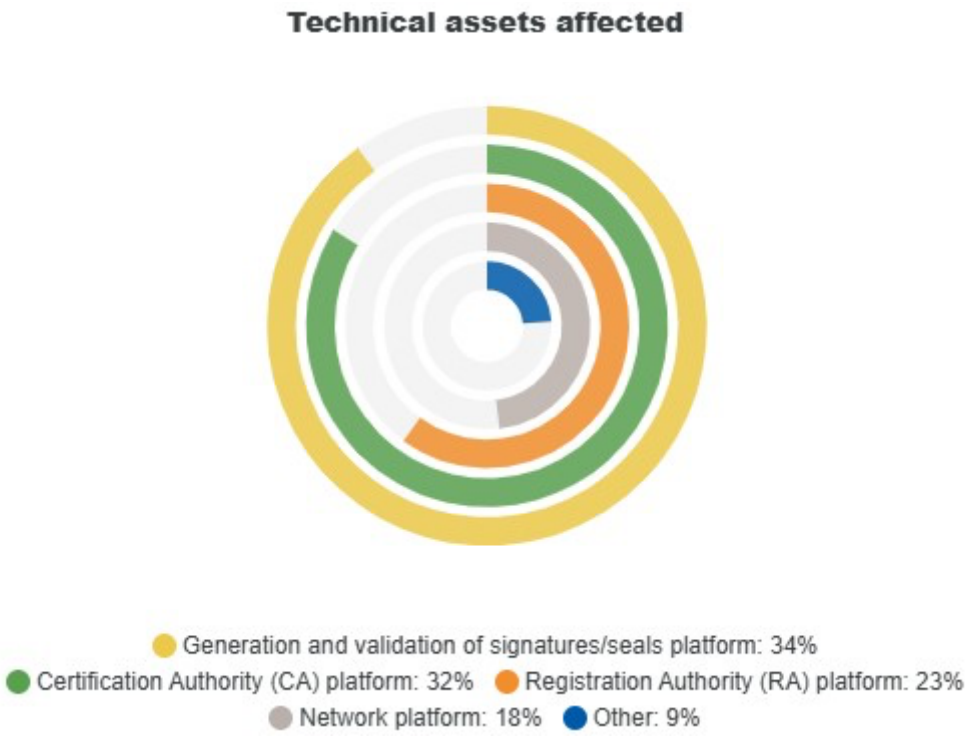



**図 13.**影響を受けた技術資産 - 2024 年の TSP セキュリティ・インシデント

## 3.5 適格サービス対非適格サービス

今年は、トラスト・サービス・セキュリティ・インシデント全体の 84%近くが適格サービス（適格署名 証明書作成、適格印鑑証明書作成など）に影響を及ぼし、適格サービスでは **37 件**、非適格サービスでは 7 件のインシデントが発生した。この分布は 2023 年と全く同じで、割合も同じ数字である。

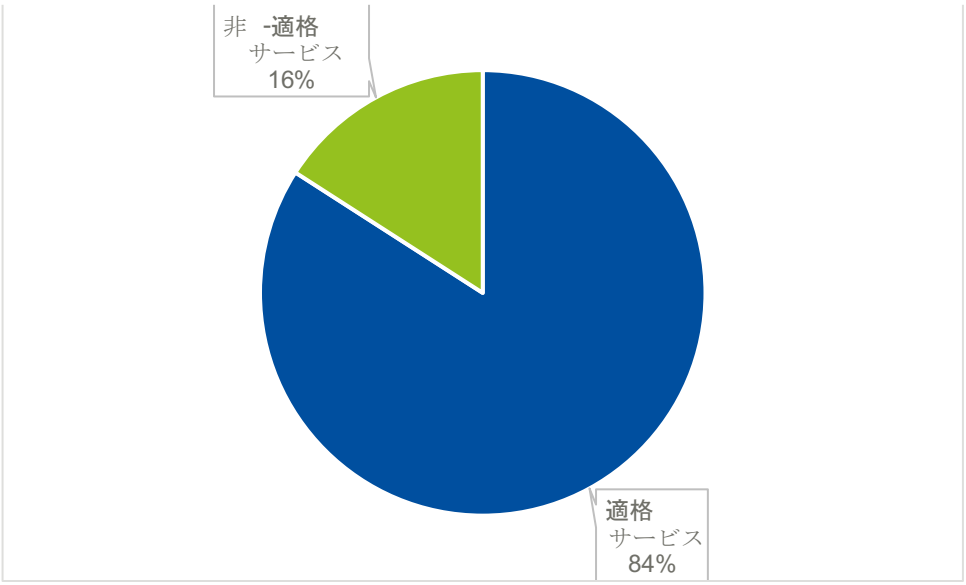



**図 14.**適格サービス対非適格サービスに影響を与えたインシデントの報告 - 2024 年

# 4. 複数年ごとの傾向 2017-2024

ENISA は 2016 年からトラストサービスのインシデント報告を収集・集計している。本セクションでは、2017 年から 2024 年までの過去 8 年間の多年次動向を見ていく。データセットには、報告された合計 287 件のインシデントが含まれている。

## 4.1 根本原因の傾向

根本原因のカテゴリー、すなわち、システム障害、ヒューマンエラー、悪意ある行為、自然現象について、2017 年から 2024 年までの期間にわたって分析する。

2017 年から 2024 年にかけて、システム障害は報告された全インシデントの 58%を占め、ヒューマンエラーは報告された全インシデントの 26%を占め、15%が悪意ある行為に関与し、1%が自然現象であった（**図 15** に表示）。

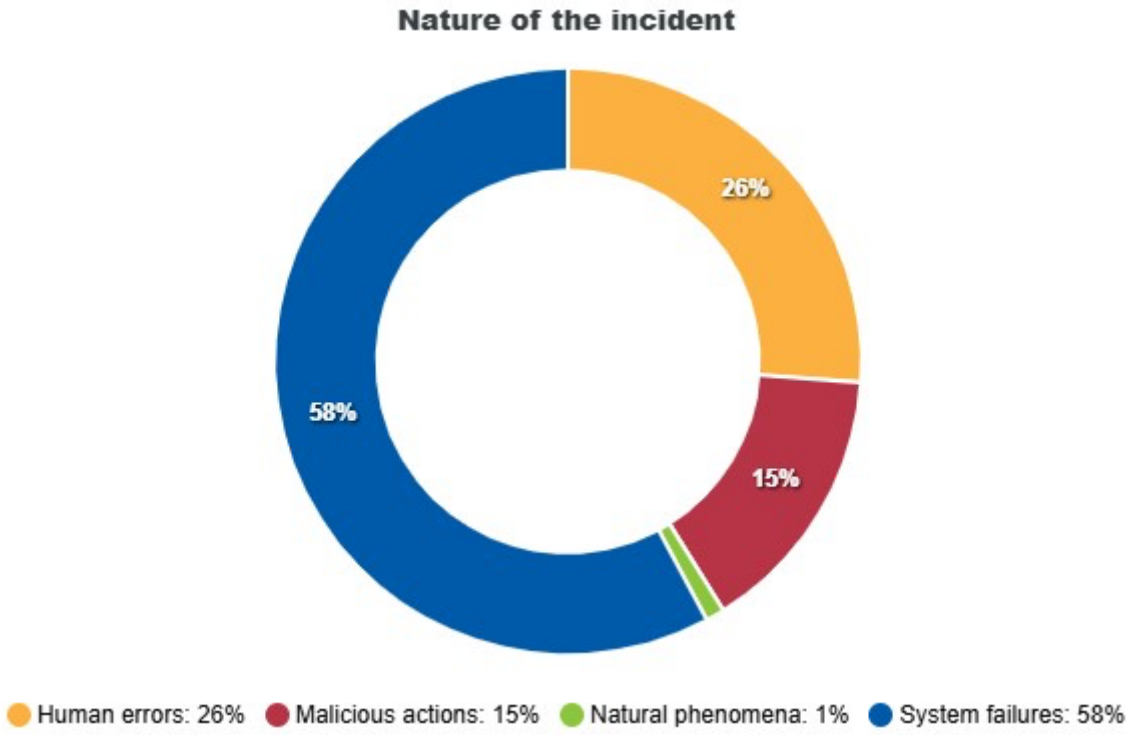



**図 15.**報告されたインシデントの性質-EU におけるトラストサービスのセキュリティインシデント（2017～2024 年に報告されたもの）

参照期間中、報告された 287 件のインシデントのうち：

- 報告されたインシデントのうち、システム障害が 166 件を占めた、
- 報告されたインシデントのうち、人為的ミスが 75 件、
- 43 件が悪意のある行為、そして
- 3 件が自然現象であった。

過去 8 年間の関連インシデントの割合の推移をカテゴリー別に**図 16 に示す。**

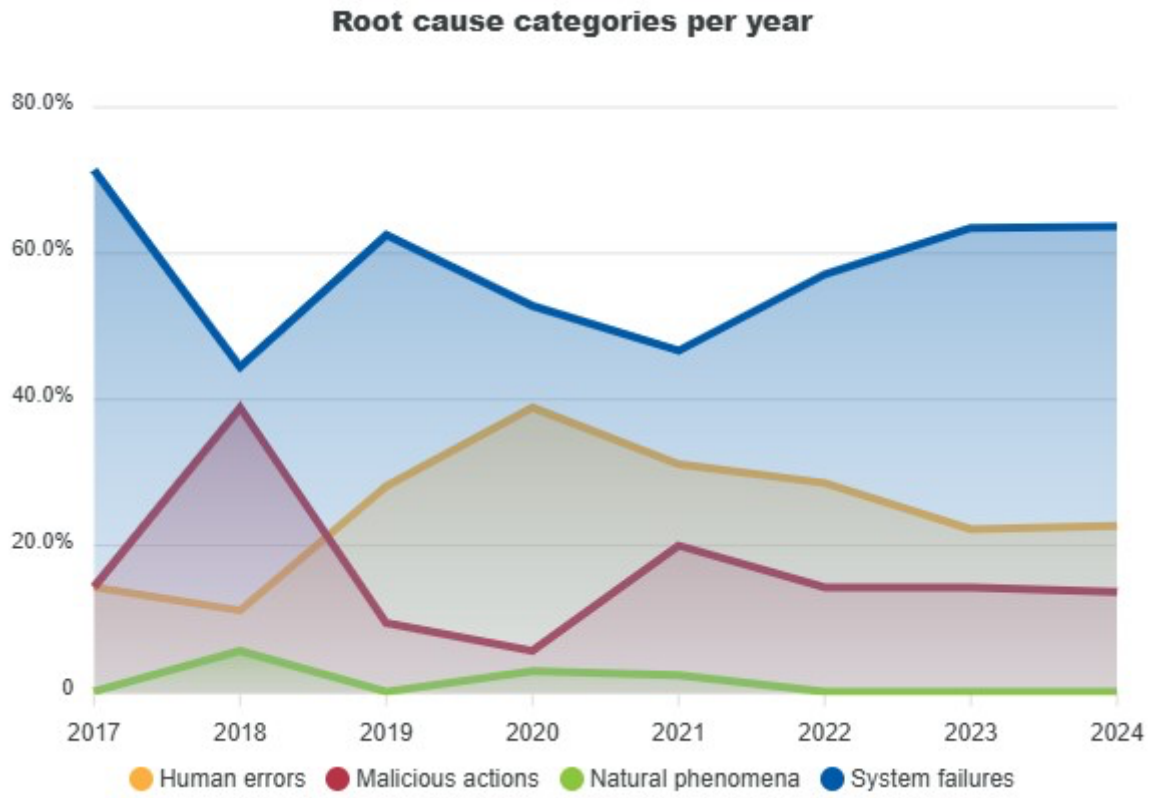



**図 16.**根本原因のカテゴリー-EU におけるトラストサービスのセキュリティインシデント（2017～2024 年に報告されたもの）

長年にわたるトラストサービスのセキュリティインシデント報告の中で、最も一般的な根本原因は**システム障害**であり、合計 **166 件のインシデントが報告されている**。過去 5 年間、システム障害に関連するインシデントの割合は着実に増加している。

**ヒューマンエラーに関する**インシデントは、2020 年には約 40%であったが、2024 年には 23%と着実に減少している。

**自然現象**はトラストサービス分野では一般的な根本原因ではない。2017 年から 2024 年にかけて報告されたインシデントはわずか **3 件**で、全体の **1%を占めて**いる。2022 年以降はそのようなインシデントは報告されていない。

**悪意ある行為は**年によって異なり、2018 年には 38.9%のピークが観察され、2020 年には 5.6%と低い値が記録された。2024 年には、報告されたインシデントの 14%、9 件の根本原因が悪意のある行為であった。2022 年以降、悪意ある行為は 14%前後で安定している。

## 4.2 インパクトの重大性の傾向

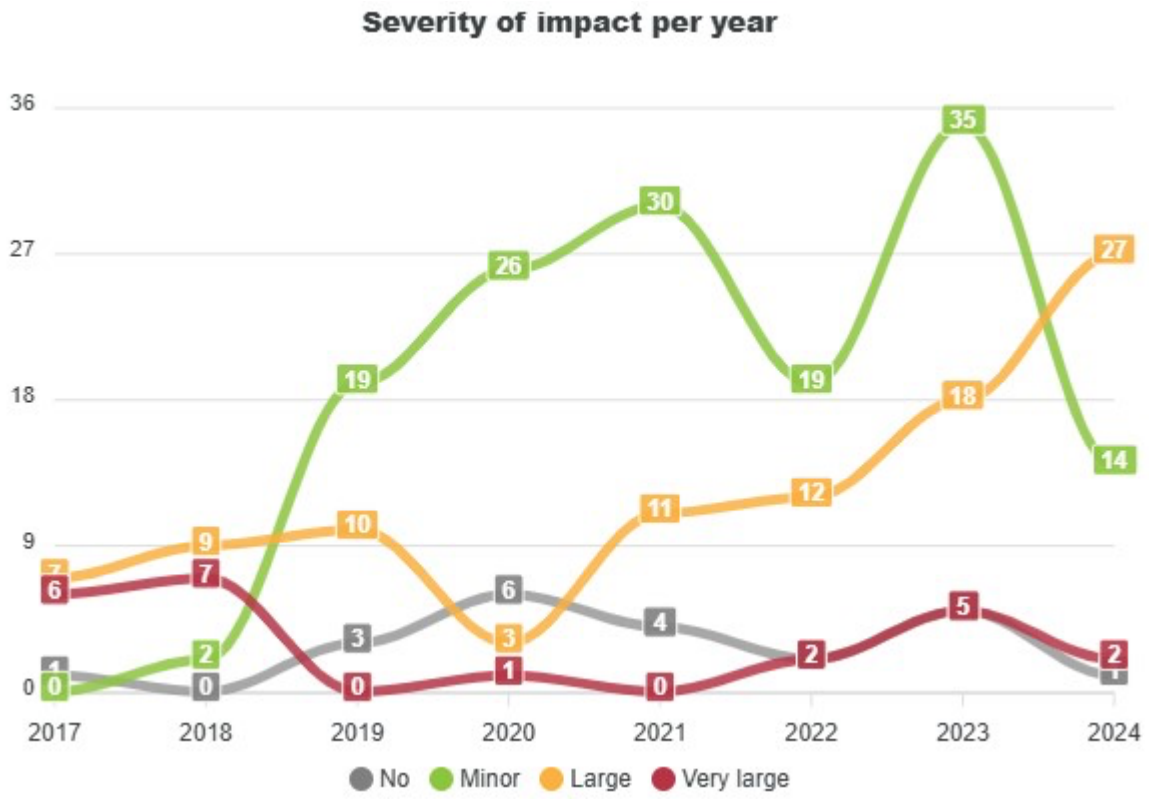
影響の深刻度に関する複数年ごとの傾向では、EU サイバーセキュリティインシデント分類法（[7]）が再び踏襲されており、影響の深刻度には、影響なし、軽微、重大、非常に重大の値がある。[8]時間の経過とともに、TSP はその深刻度に関係なく、より多くのインシデントを報告するようになっている。

**大きな影響のインシデント**（黄色）は、2020 年の 3 件から 2024 年の 27 件まで、過去 5 年間でほぼ直線的に増加している。

**大きな影響のインシデント**（黄色）を見ると、2020 年に減少したにもかかわらず、今年 27 件に達し、増加し続けていることがよくわかる。

長期にわたって報告された**非常に大きな影響のインシデントに関しては**、年間 2 件前後で落ち着いているようだ。

参考までに、2023 年には 27 の加盟国と 3 つの EFTA 加盟国からインシデントが報告されているが、2024 年には 21 の加盟国と 3 つの EFTA 加盟国からインシデントが報告されている。そのため、私たちが受け取ったインシデントや表示されるグラフに影響を及ぼしている。さらに、加盟国がインシデントを評価する際の支援となる影響アセスメント手法を合理化し、全加盟国で一貫した比較可能な影響理解を確保すべきである。




[7] サイバーセキュリティインシデント分類法（2018 年版）
http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53646 参照

[8] これは、執筆時点で 6 加盟国からの報告がないためである可能性があることを付記しておく。

**図 17.**影響の重大性-EU におけるトラストサービスのセキュリティインシデント（2017～2024 年に報告されたもの）

## 4.3 サービスへの影響傾向

このセクションでは、トラストサービスのインシデント報告について、2017 年から 2024 年までのサービスごとの影響度を**図 18 に**詳述する。

報告されたインシデントの大半が**電子署名に関する**ものであり、その数は平均 86%程度であることがわかる。これはおそらく、電子署名が金融またはその他のトランザクションの認可に使用される一方、電子印鑑は主にデータの完全性を確保するために使用されるという事実によるものであろう。さらに、電子印鑑では通常オートメーションが使用されるが、電子署名は人間もかなり広範囲に使用するため、インシデントが多くなる。

**電子シールは**着実に減少傾向を示しており、8 年間で最低の 6%のシェアとなった。

**電子タイムスタンプは、**8 年間のインシデント報告で **11%前後で推移している**ようだ。

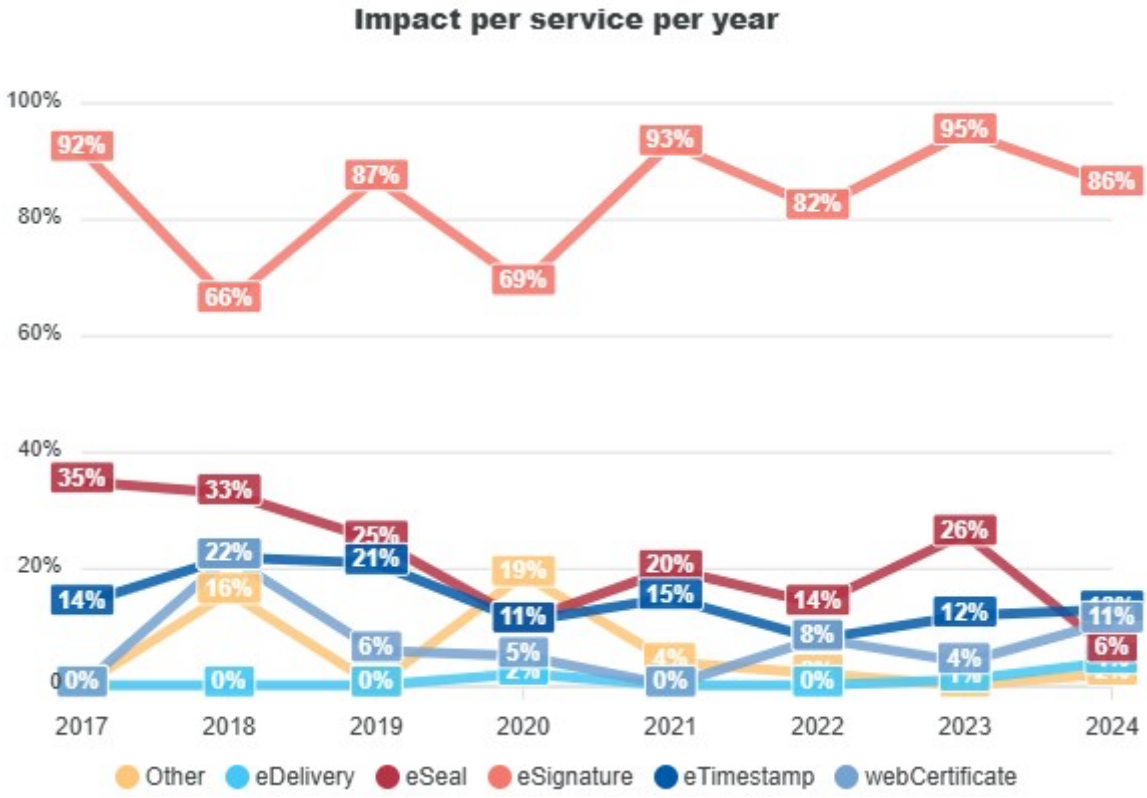



**図 18.**サービスへの影響-EU におけるトラストサービスのセキュリティインシデント（2017 年から 2024 年に報告されたもの）

# 5 結論

2024 年のインシデント報告から**得られた主なポイントは**以下の通りである。

- EU 監督団体の半数である 24 団体中 **12 団体**（報告済み）がそれぞれの報告書を送付し、報告されたインシデントは 0 件であった。[9]
- インシデントによる全体的な影響は 6 億 1,800 万ユーザー時間の損失であり、**3 億 1,800 万ユーザー時間の損失が**報告された 2023 年よりも 5 倍減少している。
- 2024 年には、6 億 1,800 万時間のうち 5 億 7,100 万時間が**悪意のある行為によって**失われ、全体の 92%を占めた。
- 大規模インシデントの数は過去 5 年間増加し続けている。
- **適格トラストサービスと非適格トラストサービスの比較** - 2024 年には、インシデント全体の 84%が適格トラストサービスに影響を与えた。

[9] 2022: 13/27; 2021: 17/27; 2020: 19/27; 2019: 17/27; 2018:18/27; 2017:17/27; 2016: 26/27.