参考資料5-4-1

欧州における
通信事故報告制度の最新動向

令 和 ３ 年 ４ 月 ２ ６ 日
事故報告・検証制度等TF
事　　務　　局

欧州電子通信コード(EECC)指令による事故報告制度の改正

- 事故報告制度を規定していた枠組指令について、欧州電子通信コード(EECC:European Electronic Communication Code)指令により改正され、2020年12月より施行。
- 新たな事報告制度においては、対象となる電気通信ネットワーク/サービスとしてOTTサービスへの拡大やセキュリティインシデントの具体化、「重大な影響」に関する要考慮指標の設定や質的基準等が追加。

枠組指令 (2002/21/EC) 13a条3項

- 2009年通信改革パッケージの「Better Regulation指令」(2009/140/EC)により追加。2011年より施行。
- 電気通信ネットワーク/サービス(Electronic communication network/service。主に、固定電話/インターネット接続、移動電話/インターネット接続等)の運用に重大な影響を及ぼすセキュリティインシデント(security breaches及びintegrity losses)について、通信事業者が規制当局に報告する義務等を規定。なお、対象となるネットワーク/サービス、重大な影響やセキュリティインシデントの詳細は加盟国が独自に設定。
- 上記セキュリティインシデントについて、各加盟国が欧州理事会(EC)と欧州ネットワーク・情報セキュリティ庁(ENISA)に対し、その概要を毎年報告する義務を規定。
- ENISA等への各年報告につき、相対基準(継続時間1h超かつ影響利用者数が15%超・同2h超かつ同10%超等)又は絶対基準(100万ユーザ時間超)を設定。なお、当面の間、セキュリティインシデントのうち、integrity losses(電子通信ネットワーク/サービス提供の継続性に影響を及ぼすoutage)のみが対象。
- ENISAにて、2012年以降、年次報告書を取りまとめ。2019年に発生したインシデントについて2020年7月に公表。

参考1(P8~16)

詳細は、ENISA「Technical Guideline on Incident Reporting:Technical guidance on the incident reporting in Article 13a ver. 2.1, October 2014」参照

参考2(P17~18)

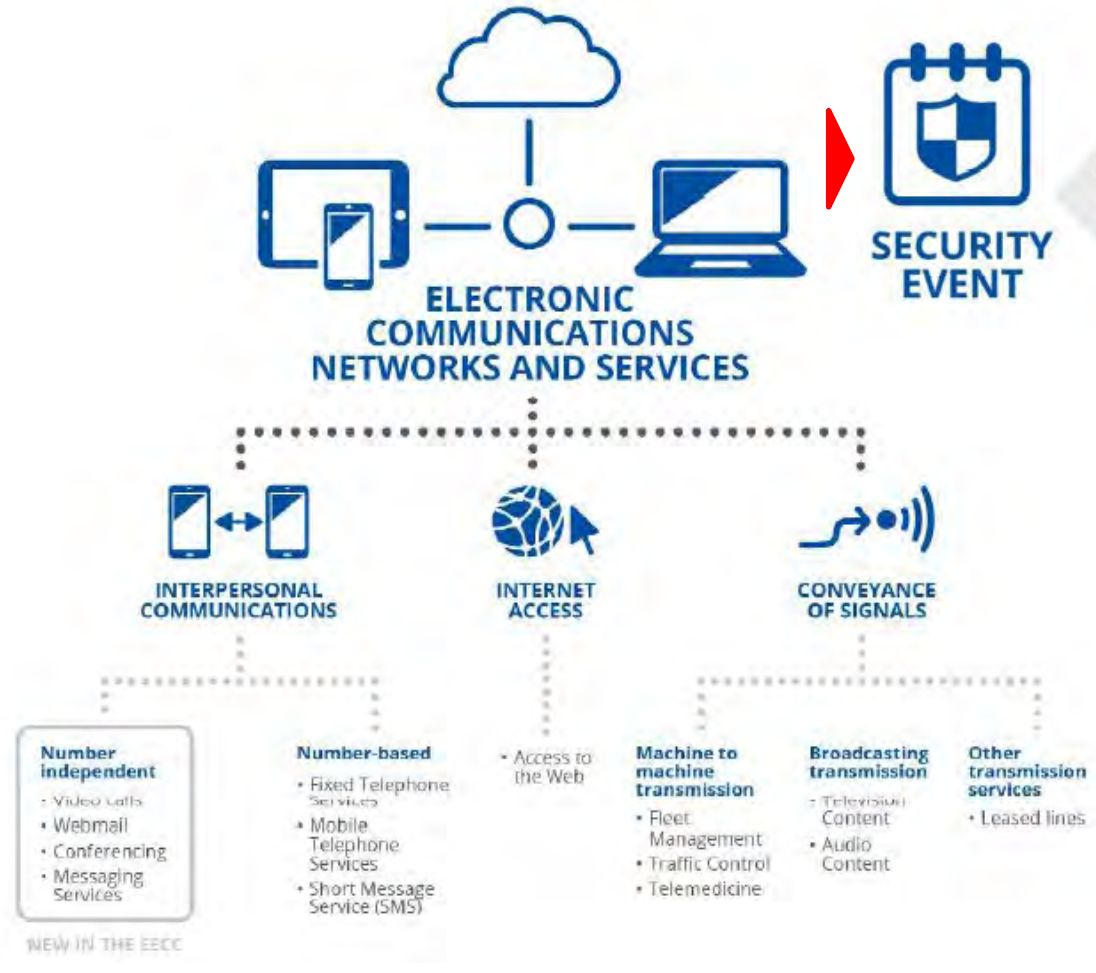
EECC指令 (2018/1972) 40条2項

- 枠組指令13a条3項を改正。2020年12月21日より施行。
- 対象となる電気通信ネットワーク/サービスについて、「番号に依存しない個人間通信」(Number-independent Interpersonal Communications)サービスとして、OTTサービス(WhatsApp、Viber、Slack、Gmail、Outlook、Skype-to-Skype等)も追加。
- 対象となるセキュリティインシデントにつき、電子通信ネットワーク/サービスのセキュリティ(confidentiality, authenticity, integrity, availability)に実際の悪影響を及ぼす事象(2本で冗長化された海底ケーブルのうち1本の切断や新発見の脆弱性等も含む)と具体化。
- 対象となる「重大な影響」につき、加盟国が特に考慮すべき指標(影響利用者数、継続時間、地理的範囲、電子通信ネットワーク/サービスの機能への影響の程度、経済社会活動への影響)を規定。
- 通信事業者は、規制当局等のセキュリティインシデントに関する主務官庁に対し、不当な遅延なく報告する旨を規定。
- ENISA等への年次報告につき、量的基準(影響利用者数及び継続時間)のみならず、新たに質的基準(地理的範囲や社会経済等への影響)を規定。

詳細は、ENISA「SECURITY SUPERVISION UNDER THE EECC, JANUARY 2020」、「Technical Guideline on Incident Reporting under the EECC, March 2021」参照

EECC指令における事故報告制度の概要

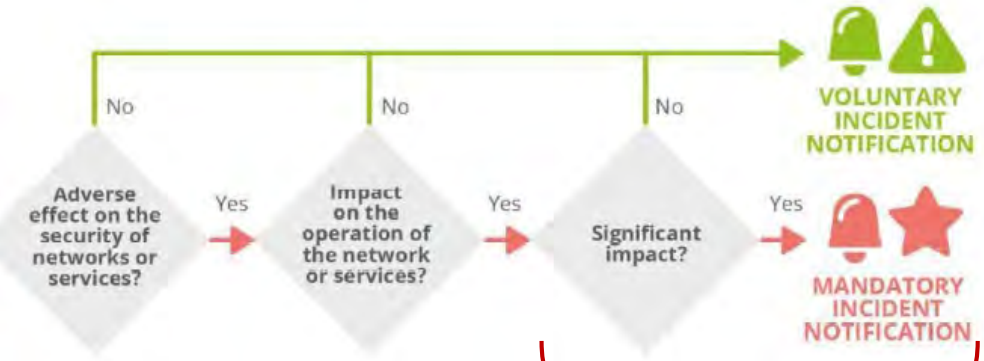
対象となる電気通信ネットワーク/サービス



新規追加（EECC指令）

従来（枠組指令）からの電気通信サービス

事業者が主務官庁に報告する際の基準等



●事業者が主務官庁に報告すべき「重大な影響」につき、各加盟国が特に考慮すべき指標は次の通り
- ▶ 影響利用者数
- ▶ 継続時間
- ▶ 地理的範囲
- ▶ 電子通信ネットワーク/サービスの機能への影響
- ▶ 経済社会活動への影響

●以下の量的・質的基準の両方に該当するセキュリティインシデント※につき、加盟国からENISA等に毎年報告（EECC指令により、質的基準が追加）【詳細は次頁】
- ▶ 量的基準（相対基準又は絶対基準に該当する場合）
- ▶ 質的基準（地理的範囲や経済社会への影響など）

※（枠組指令と異なり）integrity losses（電子通信ネットワーク/サービス提供の継続性に影響を及ぼすoutage）以外のセキュリティインシデントも対象

EECC指令における報告対象（セキュリティインシデント）

impact on the availability;

電気通信役務の「提供停止」又は「品質低下」

when the incident affects the continuity of supply of services, degrades the performance of the service, the network or service is “completely” or “partially” down. This is often called ‘outage’ or ‘disruption’.

e.g.

50% of phone calls dropped in the last 15 minutes’ or 50% of internet bandwidth lost, customers experiencing service degradation to the point where the customer feels the service is not fit for purpose.

impact on the integrity;

when there is a compromise of the integrity of the communications data or metadata.

e.g.

IP address and caller id spoof, log files have been tampered; configuration files or routing files have been found altered (integrity of files); malware or unauthorised software has been found installed into a server capable to identify and alter data from various files (violation of integrity of the systems software that then causes violation of the integrity of retained information).

impact on the confidentiality;

when the confidentiality of communications, communications data or metadata has been compromised.

e.g.

encryption does not work and content of communication is hacked, private messages and exchanged content have been accessible by attackers, IMSI catchers, provider’s database with communications logs has been compromised, emails are forwarded to unknown recipients, configuration files or routing files have been accessible by attackers and have been disclosed.

impact on the authenticity;

when there is a compromise of user’s identity (identity fraud).

e.g.

man-in-the-middle attacks or eavesdropping on applications lead to theft and misuse of authentication credentials, user accounts become accessible and taken over by attackers.

EECC指令における報告基準(年次報告:各規制当局⇒ENISA)①

- Availabilityに係るセキュリティインシデント:次のいずれかの基準に該当する場合
  - ▶ 相対基準・・・継続時間1h超かつ影響利用者数※15%超、同2h超かつ同10%超 など
  - ▶ 絶対基準・・・100万ユーザ時間超又は6千万ユーザ分超(影響利用者数2.5万未満又は1時間未満除く)
- その他(Confidentiality等)に係るセキュリティインシデント:次の基準のみに該当する場合
  - ▶ 相対基準・・・継続時間にかかわらず、影響利用者数1%超

量的基準

Quantitative Parameters

Availability

1: Relative threshold based on the percentage of the user base ※ (nationally) and the duration (nationally)

	1h-2h	2h-4h	4h-6h	6h-8h	> 8h
1%-2%					
2%-5%					
5%-10%					
10%-15%					
> 15%					

2: Absolute threshold of > 1M user hours (nationally)

Confidentiality, Integrity, Authenticity

3: Relative threshold based on the percentage of the user base of the service (nationally)※

Number of users affected > 1% of the user base of the service (nationally)※

▶ 以上の量的基準に該当しない場合は、更に質的基準で判断(次頁参照)

※「影響利用者数」(user base (nationally))…
セキュリティインシデントが発生したサービス(当該発生に係る事業者以外の事業者によるサービスも含む)に関する全国の利用者数

①固定音声・インターネットサービス:
・契約者数又はアクセス回線数

②携帯音声サービス:
・有効(active)SIM数

③携帯インターネットサービス:
・標準的な携帯契約数
(音声サービスとインターネットサービスの双方を提供)
・インターネットサービス専用の携帯契約数
(スタンドアローン又は既契約の音声サービスに追加)

④OTTサービス等:
・一定期間の期末におけるアクティブユーザ数(当該期間に少なくとも1回サービスを利用したユーザ)

EECC指令における報告基準（年次報告：各規制当局⇒ENISA）②

● 量的基準については、常に影響の重大性に係る主要な要素になるとは限らないことから、当該基準に該当しない場合であっても、質的基準（地理的影響や社会経済等への影響）に該当する場合には報告が必要。

質的基準 Qualitative Parameters	Availability	4: Significant due to the geographical spread of the incident. i.e. cross-border, or if large remote/rural areas, or a capital/critical region affected etc. 5: Significant due to the impact on economy and society, or on users i.e. lack of access to 112, national emergency numbers, impact on public warning systems, high costs, high material damage, high risks to public safety, public security or of loss of life , media coverage (evening news), impact on the continuity of essential services or critical sectors/operators, impact on especially critical days, such as election or referendum days.
	Confidentiality, Integrity, Authenticity	

地理的な影響範囲

- 広範囲で地方や島等
- 都市部や重要地域
- 相互接続響（又は多くの国際相互接続）

など

社会経済又は利用者への影響

- 112（欧州共通の緊急通報用番号）や各国の緊急通報への接続
- 公共警報システム（public warning systems）
- 公衆の安全とセキュリティ（public safety, public security）への高リスク、人命の損失、又は、高い物質的な損害（レピュテーション、モラル、消費者データの損失、生産性など）
- 特に重要な日（選挙や国民投票等）
- 報道ぶり（夕方ニュース等）
- 社会の重要機能（省庁、政府機関等）
- 注目を集める（high profile）利用者（首相、議員等）
- 重要サービスや重要分野・事業者（essential services or critical sectors/operator）の継続性

など

ネットワーク・情報システムセキュリティ（NIS）指令による事故報告制度

- NIS指令（2016/1148）において、①「デジタルインフラ」等の「重要インフラ運営者」、②「デジタルサービス提供者」を対象として、その「サービス提供の継続性に重大な影響を及ぼすインシデント報告制度」が規定。
- 2020年12月の「新たな「サイバーセキュリティ戦略」」にて「NIS2指令案」等公表。「EECC指令の報告制度も含めNIS指令を全面改正」。今後、EU理事会等との調整を経て、採択後18ヶ月以内に加盟国で措置予定。

NIS指令（2016/1148）14条・16条

参考3（P19）

- 2013年2月の「サイバーセキュリティ戦略」において、NIS指令（Directive on security of network and information systems）が提案。2018年5月より施行。
- 重要インフラ運営者（OES）及びデジタルサービス提供者（DSP）は、主務官庁やCSIRTに対し、不当な遅延なく報告する義務等を規定。
- OESとして、エネルギー、交通、金融、医療、水道、デジタルインフラの7分野を規定。うち、デジタルインフラにつき、IXP、DNSサービスプロバイダ、TLD名前レジストリを規定。
- DSPとして、オンライン市場、オンライン検索エンジン、クラウドサービスを規定。なお、零細企業等は対象外。
- 対象となる「重大な影響」につき、加盟国が特に考慮すべき指標として、影響利用者数、継続時間及び地理的範囲を共通に規定。
- DSPについては、次も規定。
  - 「重大な影響」の要考慮指標として、提供サービスの機能への影響及び経済社会活動への影響も追加。
  - 「重大な影響」のみなし規定（①提供するサービスが500万ユーザ時間超の利用不可、②提供するサービスやデータのCIAの侵害が10万ユーザ時間超、③公共の安全や人命損失等の危険等）
- OESがそのサービス提供にあたり第三者のDSPに依存する場合、当該DSPに影響及ぼすインシデントによる重要インフラサービスの継続への重大な影響全てについて、OESが報告する義務を規定。

詳細は、「Commission Implementing Regulation（EU）2018/151」参照

NIS2指令案20条

参考4（P20）

- OESとDSPの区分を見直し、重要性等に応じ異なる規制枠組みが適用される「不可欠主体（EE：essential entities）」と「重要主体（IE：important entities）」に見直し。重要インフラの対象を拡大。
- EEとして、「デジタルインフラ」が規定。NIS指令のOESとしてのデジタルインフラ（IXP、DNSサービスプロバイダ、TLD名前レジストリ）、EECC指令の電気通信ネットワーク/サービスに加え、新たに、データセンタサービス、CDN、トラストサービス、NIS指令のDSPの1つであるクラウドサービスが対象。
- IEとして、「デジタル提供者」が規定。NIS指令のDSP（オンライン市場、オンライン検索）に加え、新たに、SNSプラットフォームが対象。
- EE及びIEは、主務官庁やCSIRTに対し、サービス提供に重大な影響を及ぼすいかなるインシデントを不当な遅滞なく報告する義務（24h以内の速報、求めで中間報告、30日以内の最終報告）を規定。
- EE及びIEは、主務官庁やCSIRTに対し、重大なインシデントをもたらす可能性があると確認されるいかなる重大なサイバー脅威を不当な遅滞なく報告する義務を規定。
- 「重大」につき、当該主体に相当な運用上の混乱又は金銭的損失をもたらす（恐れも）がある場合、相当な物質的又は非物質的な損失により他の自然人・法人に影響を及ぼす（恐れも）がある場合と規定。
- 上記インシデント及びサイバー脅威等について、各加盟国がENISAに対し、その概要を毎月報告する義務を規定。

参考資料

「通信サービスセキュリティインシデント年次報告書2019」の概要①

- 枠組指令(2002/21/EC)第13a条のセキュリティインシデント報告制度に基づき、各加盟国の規制当局は、電気通信ネットワーク/サービスの提供者から報告された、重大な影響を及ぼすセキュリティインシデントのうち一部について、その概要を欧州理事会(EC)と欧州ネットワーク・情報セキュリティ庁(ENISA)に毎年報告。
- 2020年7月、ENISAにより、2019年に発生したセキュリティインシデントに関する年次報告書(Telecom Services Security Incidents 2019 Annual Analysis Report)が公表。EU・EFTA加盟国28カ国から報告された153インシデントについて分析。今後、EECC指令等を踏まえ、報告内容等の変更可能性あり。

【事業者→規制当局】

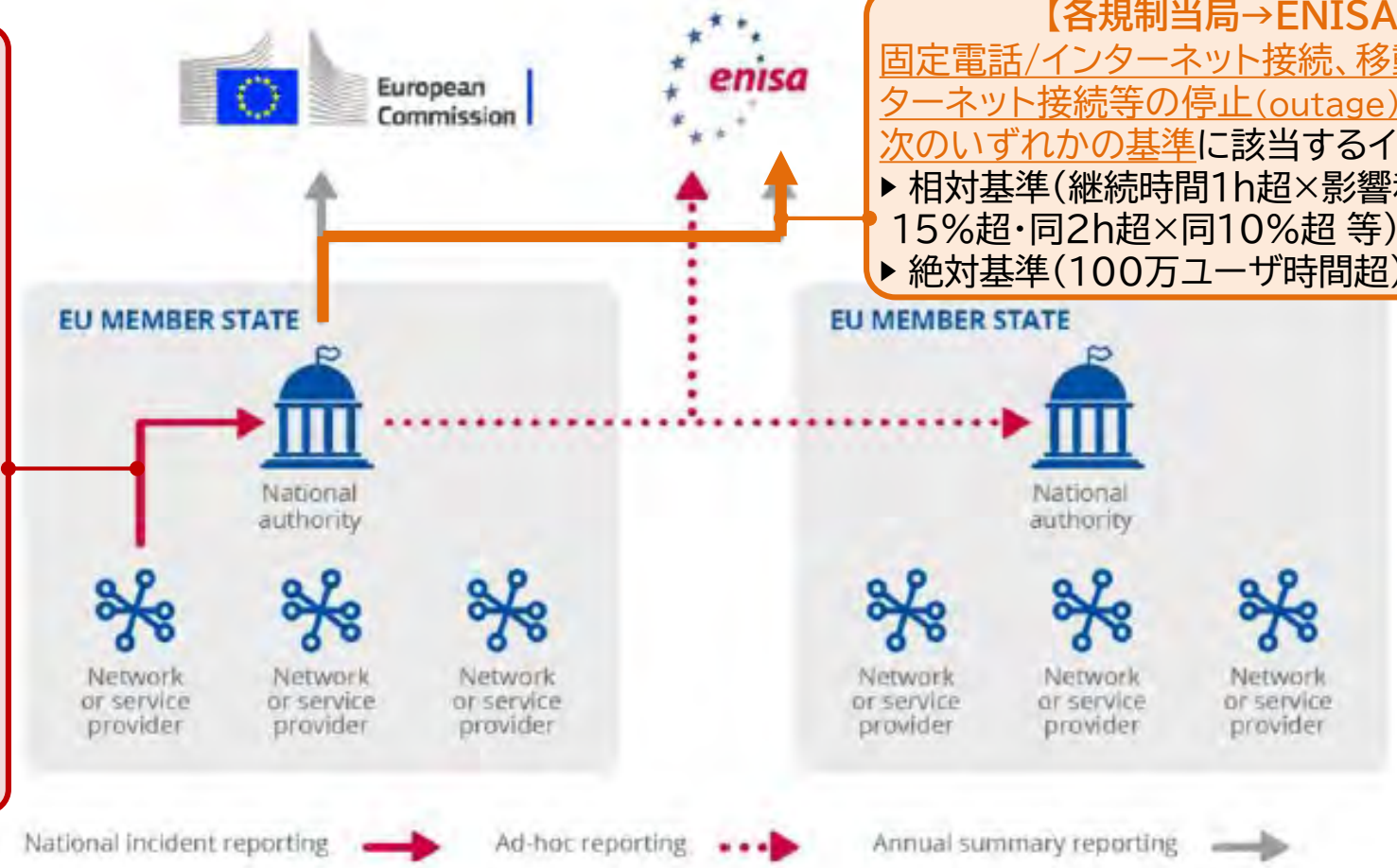
電気通信ネットワーク/サービス(固定電話/インターネット接続、移動電話/インターネット接続等)に重大な影響を及ぼすセキュリティインシデント

※対象となる電気通信ネットワーク/サービス、重大な影響やセキュリティインシデントの詳細は加盟国が独自に設定。

【各規制当局→ENISA】

固定電話/インターネット接続、移動電話/インターネット接続等の停止(outage)のみにつき、次のいずれかの基準に該当するインシデント

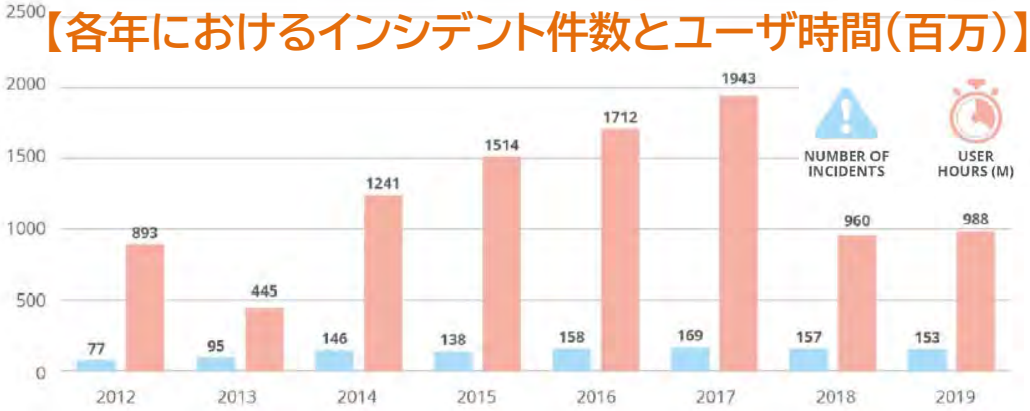
- 相対基準(継続時間1h超×影響利用者数15%超・同2h超×同10%超 等)
- 絶対基準(100万ユーザ時間超)



「通信サービスセキュリティインシデント年次報告書2019」の概要②

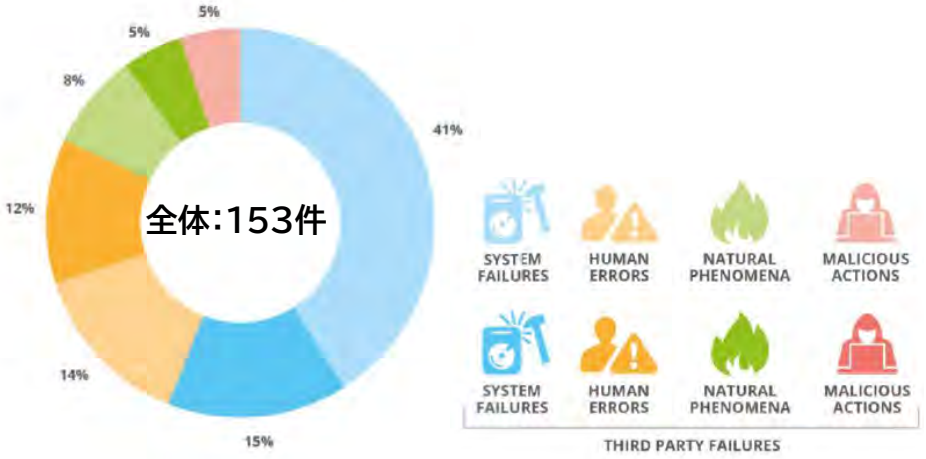
- 各年のインシデント件数は160前後で安定。報告制度について、関係者間の理解が進む等成熟し、注目されるべきインシデントが報告されていると分析。2019年の影響受けたユーザ時間は2018年から急減し、は988百万時間（欧州における1年間のユーザ時間全体※のうち約0.026%）。※5億時間（EU人口×365日×24時間）
- 2019年の153件について、システム障害が例年同様に最多で6割弱、人為的エラーが昨年から50%増で3割弱、第三者要因が昨年から3倍増で約3割、サイバー攻撃は1割未満。経年では、システム障害が微減、人為的エラーと自然災害が微増の傾向。ユーザ時間では、システム障害が5割弱、自然災害が3割。

【各年におけるインシデント件数とユーザ時間（百万）】

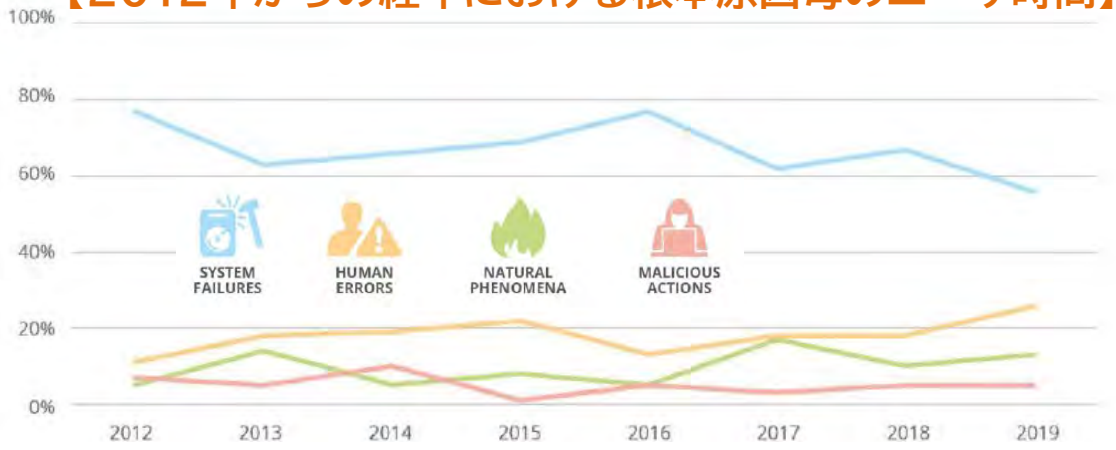


【2019年における根本原因毎のユーザ時間】

【2019年における根本原因と第三者要因】



【2012年からの経年における根本原因毎のユーザ時間】



「通信サービスセキュリティインシデント年次報告書2019」の概要③

- 各規制当局からENISAに報告された、重大な影響を及ぼすセキュリティインシデントについて、主なものとして、大容量光ファイバケーブルの工事等による切断、ソフトウェアバグによる緊急通報の利用不可、VoIPサービスへのDDoS攻撃、第三者のソフトウェアバグによるOTTサービスの停止や停電を例示。
- ENISAにより、セキュリティインシデントに関する統計分析や個別事案（加盟国名や事業者名は匿名）の研究等を可能とするCIRAS（Cybersecurity Incident report and Analysis System）が提供。

▸ 3本の大容量光ファイバケーブルが同時に切断。
移動及び固定の電話/インターネット接続が全国的に3時間停止。うち2本は、第三者による道路工事による切断、残りの1本は、土砂崩れによる切断。

▸ DDoS攻撃により、VoIPサービスが13時間停止し、40万人に影響。
システムの堅牢化やファイヤウォールに関するルールの整備等の是正措置が実施。

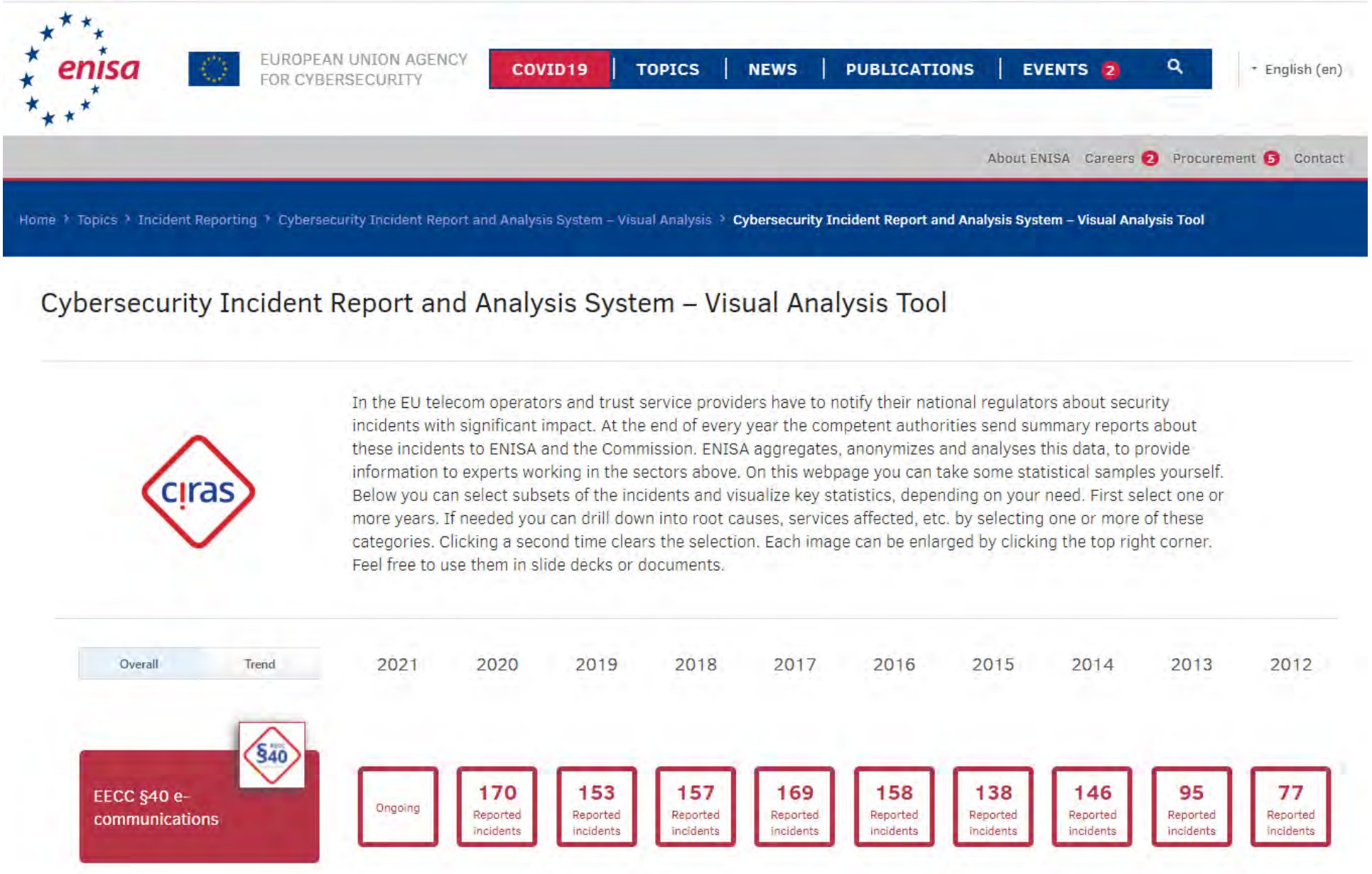
▸ 停電により、移動電話/インターネット接続とSMSサービスが10時間停止し、10万人に影響。
嵐による停電により、国全体の端末装置の機能停止が発生。全ての復旧手順が成功し、予備の電源供給が実施。

▸ 事業者の固定ネットワークが他の全てのネットワークから3時間孤立。
全ての緊急通報センターが固定ネットワークに接続されていたため、他の全てのネットワークからの緊急通報について、数百万の利用者が3時間利用不可。
原因は、ソフトウェアバグによる相互接続プラットフォームの機能停止。

▸ 第三者のインターネット接続サービス事業者におけるソフトウェアバグにより、データセンターで障害が発生し、eメールサービス（OTTサービス）が8時間停止し、100人以上に影響。

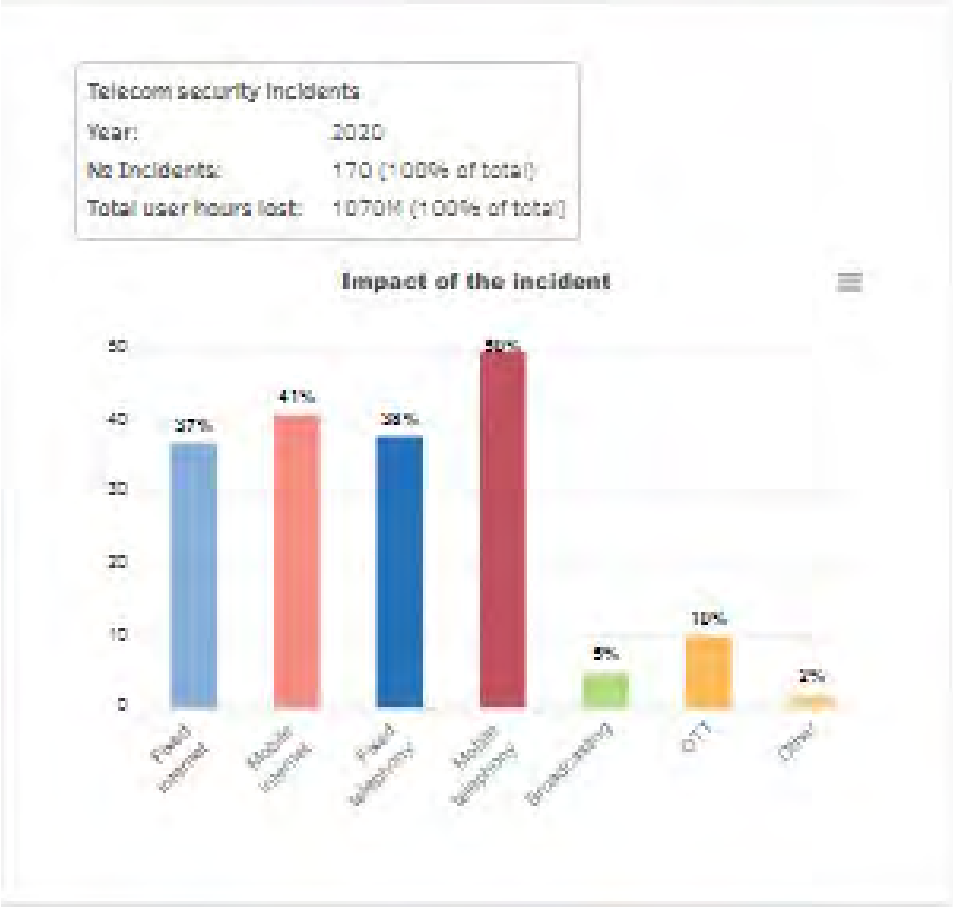
https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

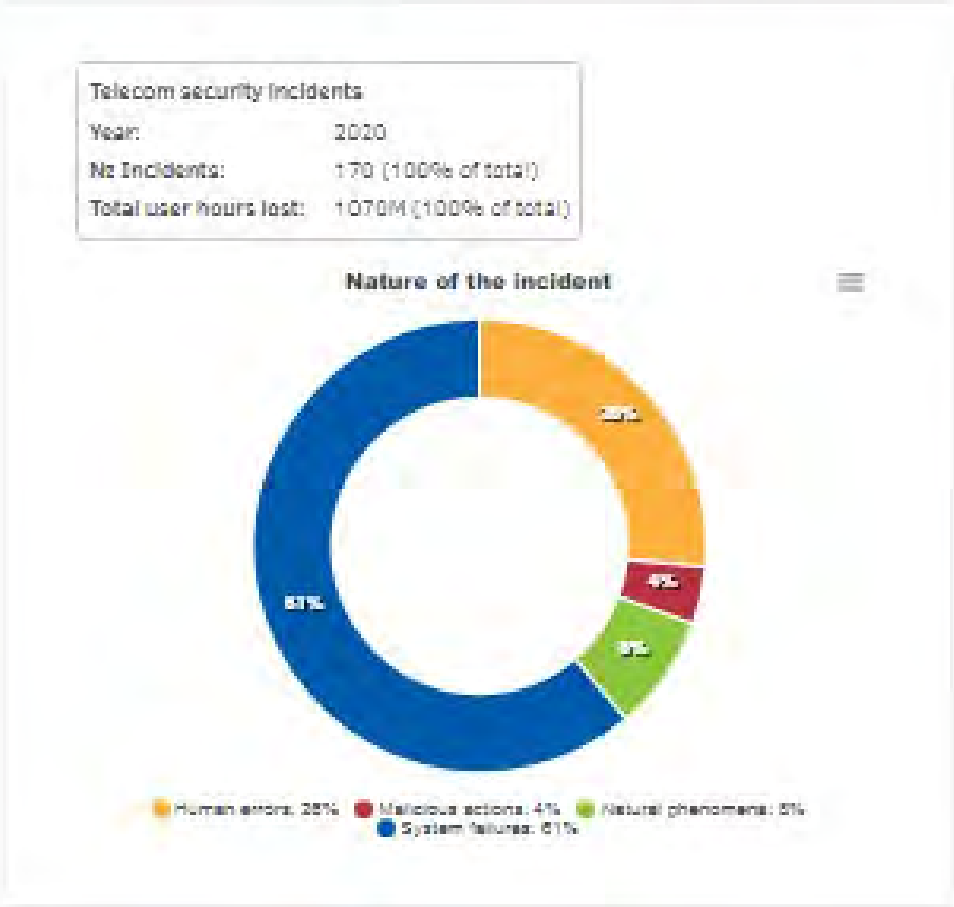
欧州における報告等システム「CIRAS」①



https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

欧州における報告等システム「CIRAS」②





https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

欧州における報告等システム「CIRAS」③

EECC §40 e-communications

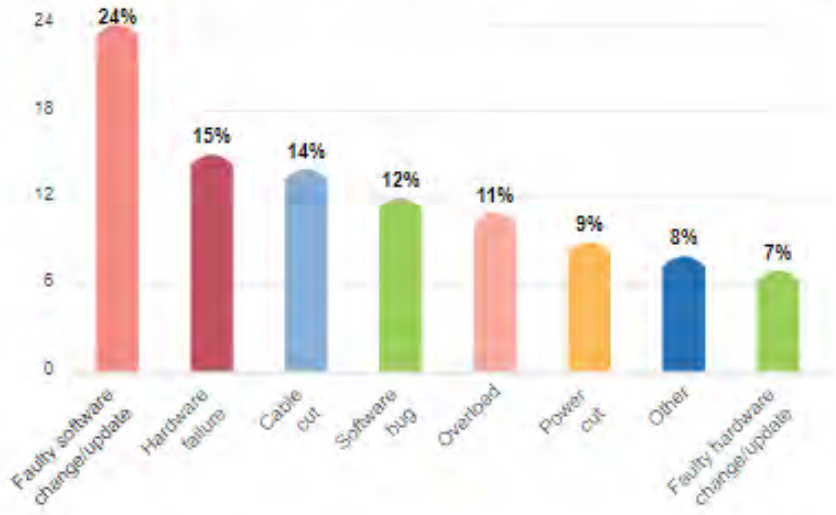
Ongoing	170 Reported incidents	153 Reported incidents	157 Reported incidents	169 Reported incidents	158 Reported incidents	138 Reported incidents	146 Reported incidents	95 Reported incidents	77 Reported incidents

SVG、PNG及びCSVデータのダウンロードが可能

Telecom security incidents

Year:	2020
№ Incidents:	170 (100% of total)
Total user hours lost:	1070M (100% of total)

Technical causes



Telecom security incidents

Year:	2020
№ Incidents:	170 (100% of total)
Total user hours lost:	1070M (100% of total)

Technical assets affected

https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

欧州における報告等システム「CIRAS」④

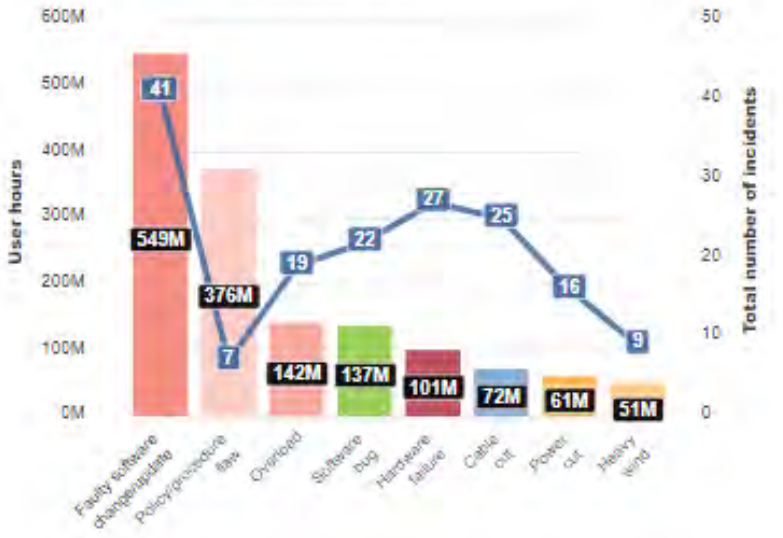
EECC §40 e-communications

Ongoing	170 Reported incidents	153 Reported incidents	157 Reported incidents	169 Reported incidents	158 Reported incidents	138 Reported incidents	146 Reported incidents	95 Reported incidents	77 Reported incidents

Telecom security incidents

Year:	2020
№ Incidents:	167 (98% of total)
Total user hours lost:	1070M (100% of total)

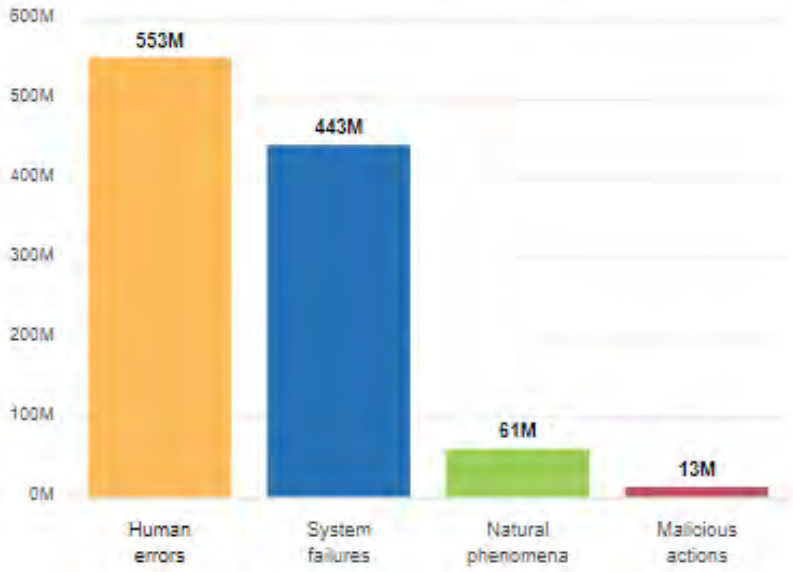
User hours lost & number of incidents per technical cause



Telecom security incidents

Year:	2020
№ Incidents:	167 (98% of total)
Total user hours lost:	1070M (100% of total)

User hours lost per nature of incident



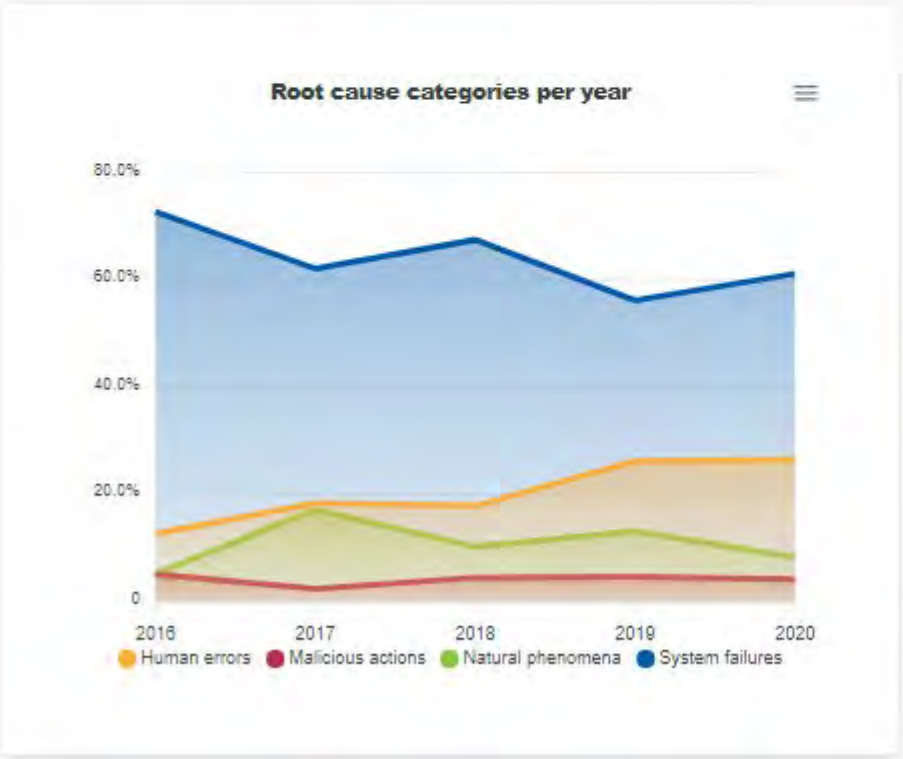
https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

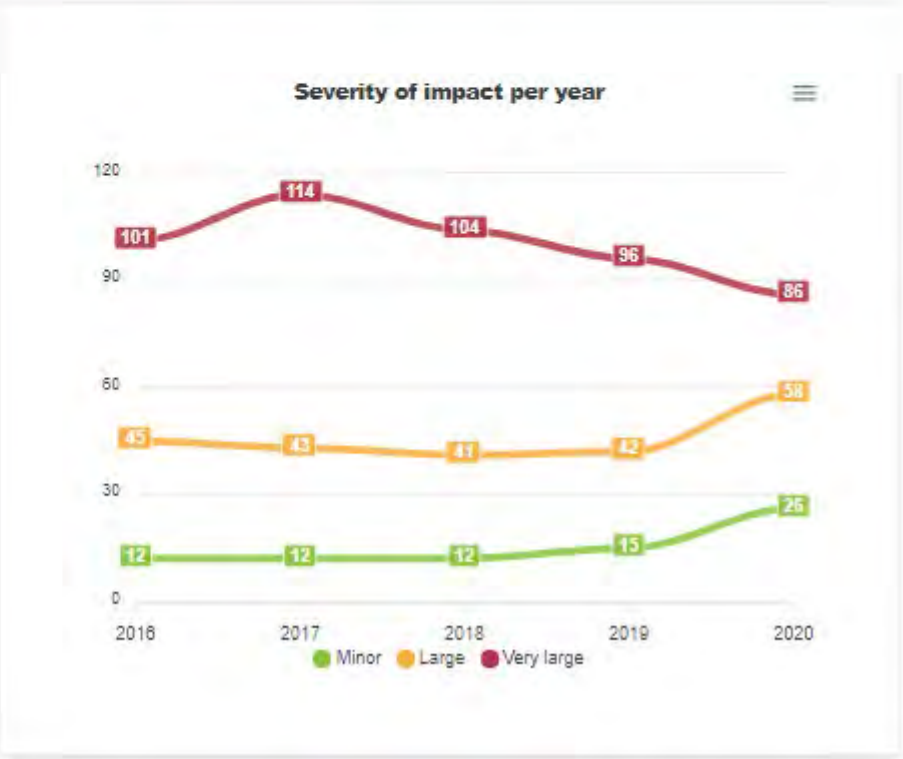
欧州における報告等システム「CIRAS」⑤

Overall | Trend

EECC §40 e-communications

2021	2020	2019	2018	2017	2016	2015	2014	2013	2012
Ongoing	170 Reported Incidents	153 Reported Incidents	157 Reported Incidents	169 Reported Incidents	158 Reported Incidents	138 Reported Incidents	146 Reported Incidents	95 Reported Incidents	77 Reported Incidents



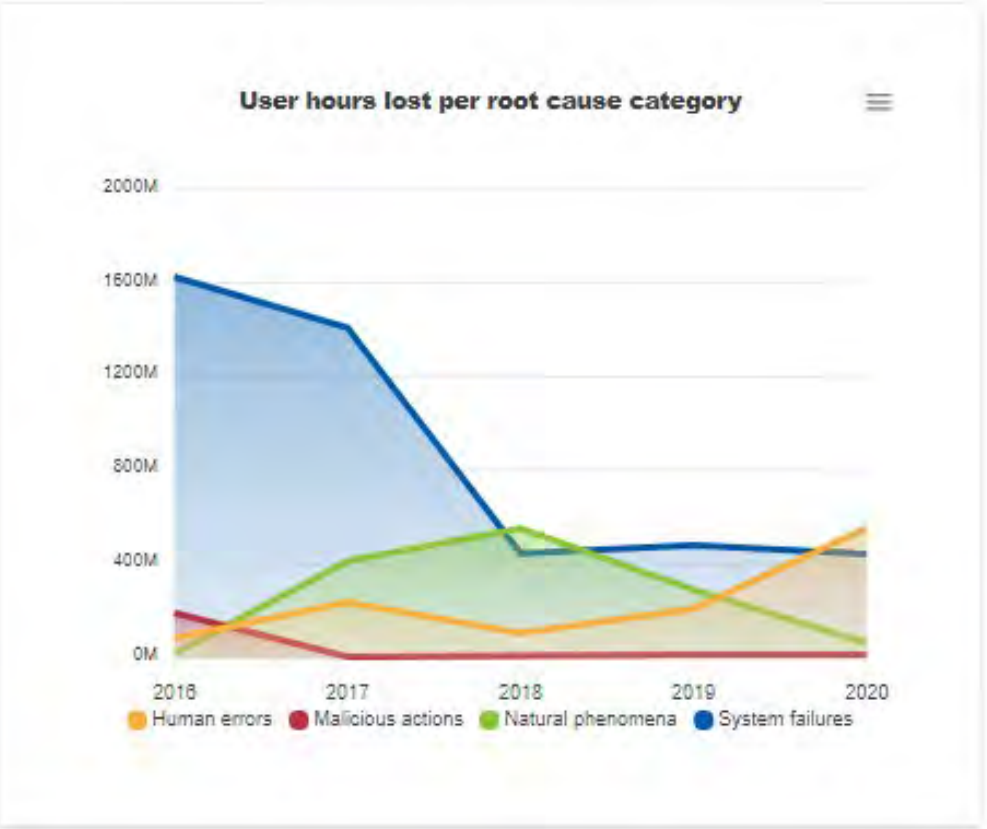


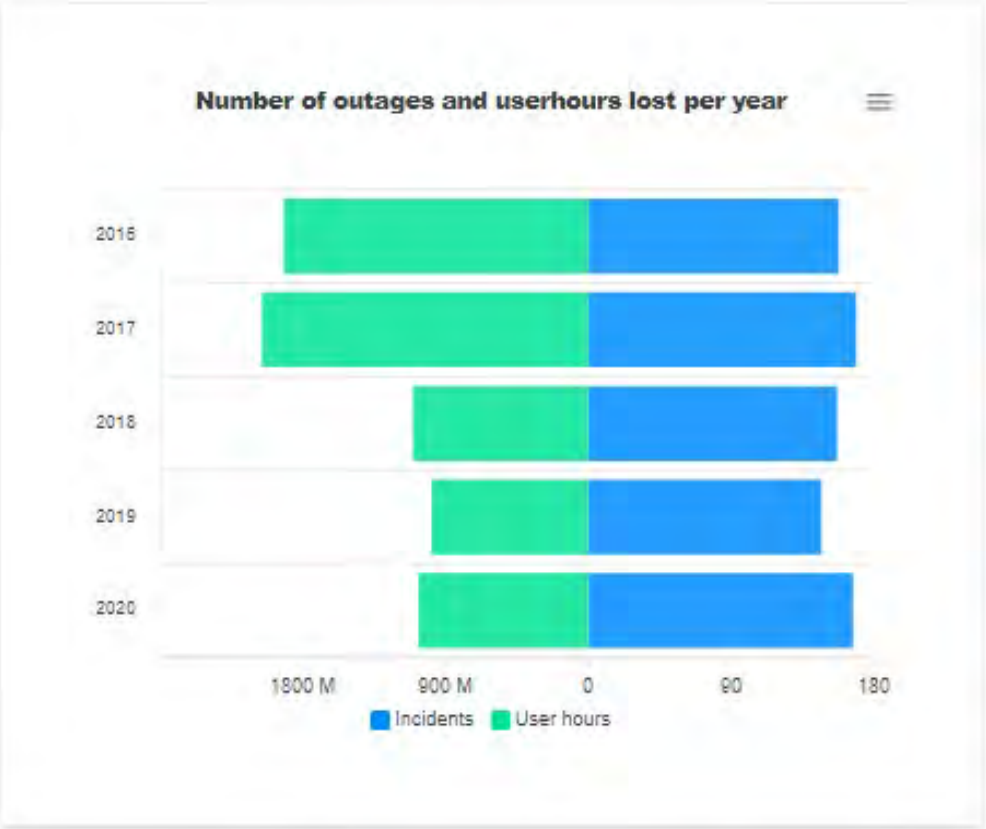
https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

欧州における報告等システム「CIRAS」⑥

Overall | Trend

EECC §40 e-communications	2021	2020	2019	2018	2017	2016	2015	2014	2013	2012
	Ongoing	170 Reported Incidents	153 Reported Incidents	157 Reported Incidents	169 Reported Incidents	158 Reported Incidents	138 Reported Incidents	146 Reported Incidents	95 Reported Incidents	77 Reported Incidents

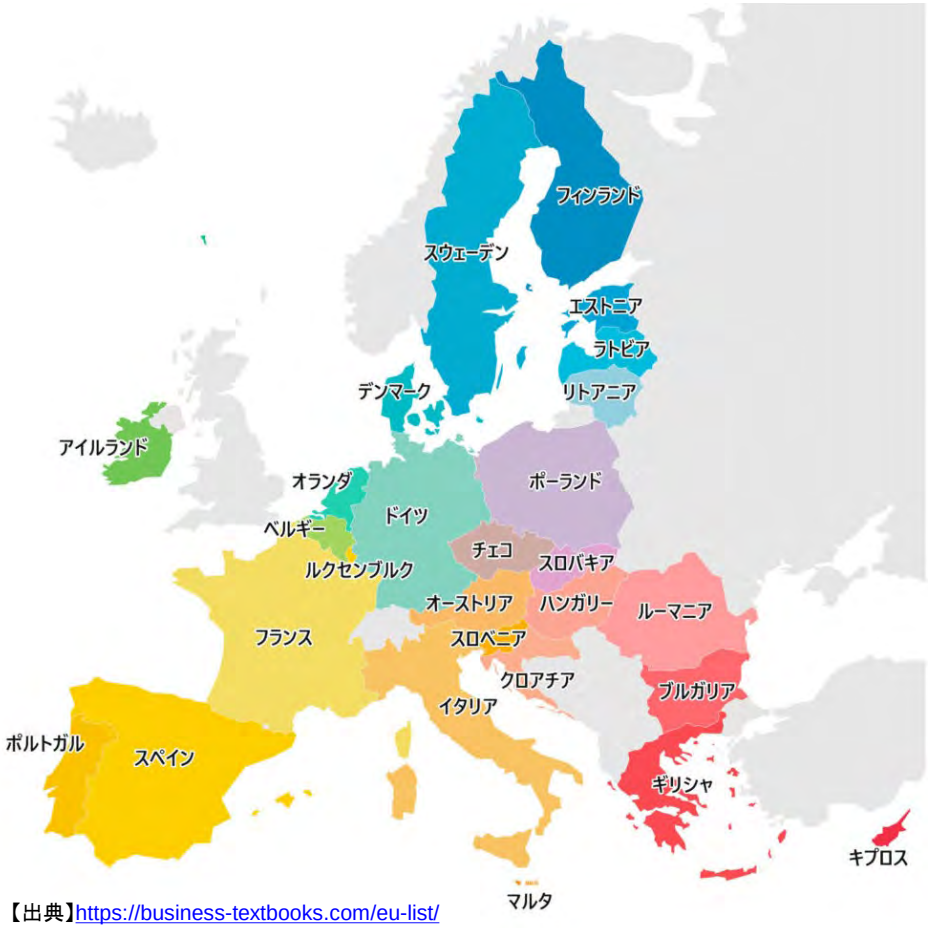




https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

欧州電子通信コード（EECC）指令の施行

- 近年のICTの進展等に対応し、①EU 域内における通信規制の更なる調和、②市場の公平性の確保、③高速ブロードバンド網への投資促進等を目的として、**欧州電子通信コード（EECC：European Electronic Communication Code）**指令が採択（2018年12月3日EU理事会）。
- EECCにより、4指令（枠組指令・認可指令・アクセス指令・ユニバーサルサービス指令）が見直し・一本化。**2020年12月21日より各加盟国において施行**。同日までに、各加盟国は、この指令を遵守するために必要な法律等を措置。なお、現状では、当該措置を**対応済みの加盟国は一部のみ**。



【出典】https://business-textbooks.com/eu-list/

現状※

※Backer McKenzieブログ「CONNECT ON TECH」の投稿より（https://www.connectontech.com/2021/01/22/european-electronic-communications-code-implementation-status/）

［対応済み］　5カ国

- 全部施行：デンマーク、フィンランド、ギリシャ、ハンガリー
- 一部施行：オランダ（アクセス規制・スイッチング円滑化等のみ）

［未対応］　22カ国

- フランス：2021年6月3日までに施行予定
  （executive orderによる施行を議会が承認）
- ドイツ：2021年夏頃に関連法案が成立予定。
- アイルランド：2021年夏頃に関連法案が成立見込み。

【その他参考】 Bird & Bird法律事務所「EECC Implementation Tracker」等
https://www.twobirds.com/en/in-focus/european-electronic-communications-code/eecc-tracker
https://www.twobirds.com/en/news/articles/2021/global/status-and-pain-points-in-implementing-the-new-telecoms-code

欧州電子通信指令（EECC）の概要

以前

①枠組指令（2002/21/EC）
各国規制機関の権限、事業者間の紛争解決、SMP事業者規制、周波数・番号管理等を規定。

②認可指令（2002/20/EC）
事業参入に関する手続・条件等を規定。

③アクセス指令（2002/19/EC）
通信網へのアクセス・相互接続に関し、事業者の権利・義務、SMP事業者の義務等を規定。

④ユニバーサルサービス指令（2002/22/EC）
ユニバーサルサービスの定義、範囲、費用算定、財源、関連する利用者の権利（番号ポータビリティ等）等を規定。

見直し・一本化

EECC

規律対象となるサービス
- 規律対象となるサービスとして、①インターネット接続サービス、②個人間通信サービス（電話、メール、SMS等）の２種類を新たに定義
- ②**個人間通信サービス**については、番号型・非番号型に分類した上で、**非番号型サービス（Viber、WhatsApp、Slack、Gmail、Outlook、Skype-to-Skype等OTTサービスも含む）**に対しても、**重大な影響のあるセキュリティインシデント報告制度**等セキュリティ措置や相互運用性の確保について新たに規律　等

アクセス規制
- 規制要件の明確化及びそれに伴う市場分析手続の見直し
- 過疎地域におけるネットワーク開放規制の拡大
- 統一された着信料算定メカニズムの導入
- 下り100Mbpsのネットワークが整備されない「非デジタル地域」の指定
- 新たなネットワークの共同投資や卸売事業者に対する規制緩和
- 既存の通信網の廃止及び新たな通信網への移行に係る手続を新たに規定　等

周波数政策
- 免許期間（最低25年）、周波数オークション、再免許及び免許廃止等に係る要件及び手続等の更なる調和及びこれを進めるための欧州委員会の権限強化

ユニバーサルサービス
- ユニバーサルサービスの定義については加盟国に委ねつつ、確保すべきサービスの範囲を拡大（Functional Internet Services及びVoice Communications）

消費者保護
- 横断的な消費者保護に関するルールとの重複は削除した上、①契約内容の簡易化、②料金等のサービスの比較が可能なツールの提供、③契約更新に係る事前通知（最低1か月前）義務、④バンドルサービスに対しても同等のルールを適用、等を新たに規定。

その他
- 加盟国規制機関の役割強化
- BERECの権限強化によるEU域内における法執行の更なる調和

NIS指令の概要

● 「サイバーセキュリティ戦略」（2013年2月7日欧州委員会）において、主要な立法措置として、NIS指令（Directive on security of network and information systems）が提案され、欧州議会にて、最終的に採択（2016年7月6日）。加盟国において、2018年5月までの国内法制化等を実施。

1.各加盟国におけるサイバーセキュリティへの対処能力の向上

○ 加盟国に対し、セキュリティ戦略の策定、本指令を運用・執行する主務官庁及びCSIRT（Computer Security Incident Response Team）の指定を義務付け（7～8条）。

2.加盟国間の協力強化

① 加盟国間における協力や情報交換を支援するため、協力グループ（Cooperation Group）を創設（11条1項）
・主な役割は、CSIRTsの活動戦略の提供、インシデント通知・リスク管理等のベストプラクティス共有、加盟国の能力・対策の評価等（11条3項）

② 特定のサイバーセキュリティ事案やリスクの迅速な対応を図るため、CSIRTsで構成されるネットワークを構築（12条1項）
・加盟国の代表者の要求に応じて、インシデントやリスクに関する商業的でないセンシティブ情報（non commercial sensitive information）を交換。ただし加盟国は、自国に不利益（prejudice）がある場合は、情報の提供を拒むことができる。（12条3項(b)）
・個々の事案に関して、非機密情報（non confidential information）を任意的に（on voluntary basis）提供（12条3項(c)）

3.デジタル・サービス提供者（digital service providers）の義務

① 適切なセキュリティ対策や重大なインシデントが発生した場合の各加盟国の監督機関への報告等の義務について、対象となる重要インフラ運営者（※1）の範囲を拡大し、新たにデジタル・サービス提供者（※2）の義務も規定（14条～18条）
※1 エネルギー、運輸、銀行、金融、医療、水道、デジタルインフラ（IXPs、DNSサービスプロバイダ、TLD名前レジストリ）
※2 オンライン市場、検索サービス、クラウドサービス

② デジタル・サービス提供者に対し、リスク管理に関し、以下の要素に考慮して適切な措置を取ることを義務付け。（16条）
・システムと施設のセキュリティ（Security of systems and facilities）
・インシデント管理（incident management）
・事業継続マネージメント（business continuity management）
・監視（monitoring）、監査（auditing）、検査（testing）
・国際標準の順守（compliance with international standards）

③ EU域内にデジタルサービスを提供している事業者のうち、域内に事業所を設置していない事業者は、セキュリティを担当する代表者（representative）を域内に設置することを義務付け。（18条2項）

欧州の新たなサイバーセキュリティ戦略の概要

- 2020年12月16日、欧州委員会とEU外務・安全保障政策上級代表が新たなサイバーセキュリティ戦略（EU's Cybersecurity Strategy for the Digital Decade）を公表。
- 重要インフラ間の相互依存やネットワーク・情報システムへの依存の高まり、オープンなインターネットやサプライチェーンを巡る地政学的な緊張、デジタルサービス等がサイバー攻撃による主要な標的化、脅威に関する集団的な状況把握・認識能力の欠如等の課題に対応。

1. レジリエンス、技術覇権とリーダーシップ

※Directive on measures for high common level of cybersecurity across the Union

①**強靭なインフラと重要サービス**（重要インフラ防護を強化するためのNIS2指令案（※）の提案）
②**欧州サイバーシールドの設立**（EU全体のセキュリティオペレーションセンターネットワークの設置提案）
③**超安全な通信インフラ**（欧州各国間の安全な通信のための量子通信インフラの構築）
④**安全な次世代のブロードバンドモバイルネットワークの確保**（第2四半期までの5Gツールボックスの各国における実行）
⑤**安全なIoT**（コネクテッドな製造端末における新たな注意義務の導入）
⑥**グローバルなインターネットセキュリティ**（DNSルートシステムの可用性に影響する事態に対応するための緊急計画、欧州DNSリソルバサーバ設置）
⑦**サプライチェーン技術の強化**（5G等技術覇権に関する産官によるサイバー産業・技術・研究センター及びネットワーク調整センターの立ち上げ）
⑧**サイバー人材**（知財窃取に対抗するための人材育成）　等

2. 防止、抑止、対処のための運用能力の構築

①**新たな共同サイバーユニット（Joint Cyber Unit）の立ち上げ**　（加盟国・関係機関の連携等におけるNeed-to-Shareマインドの必要性）
②**サイバー犯罪への対応**　（サイバー犯罪調査能力の強化）
③**EUサイバー外交ツールボックスの強化**　（EUサイバーインテルワーキンググループの設置、抑止の姿勢の強化）
④**サイバー防御能力の向上**　（既存のサイバー防御政策フレームワークの見直し、欧州軍事戦略におけるサイバー空間に関する記載の強化）　等

3. 協力強化を通じたグローバルでオープンなサイバー空間の推進

①**標準・規範・枠組の形成におけるEUのリーダーシップ**（オンラインでの人権と基本的自由の保護、既存のブダペスト条約の尊重）
②**パートナー国及びマルチステークホルダーコミュニティとの協力**（アフリカ連合・ASEAN・米州連合等との対話の促進、NATOとの協力）
③**グローバルな強靭性を高めるためのグローバルな能力強化**（EU対外サイバー能力育成アジェンダにより第三国への能力育成及び対話を強化）　等

4. 欧州関係機関におけるサイバーセキュリティ

〇より円滑な情報共有に向けた情報セキュリティの共通ルールの策定　等

Appendix:「5Gネットワークのサイバーセキュリティにおける次のステップ」

参考条文

Article 13a **Security and integrity**

3. Member States shall ensure that undertakings providing public communications networks or publicly available electronic communications services notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services.

Where appropriate, the national regulatory authority concerned shall inform the national regulatory authorities in other Member States and the European Network and Information Security Agency (ENISA). The national regulatory authority concerned may inform the public or require the undertakings to do so, where it determines that disclosure of the breach is in the public interest.

Once a year, the national regulatory authority concerned shall submit a summary report to the Commission and ENISA on the notifications received and the action taken in accordance with this paragraph.

【出典】EUR-Lex https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32002L0021

参考条文②：欧州電子通信コード指令(2018/1972)

Article 2 **Definitions**

(21) 'security of networks and services' means the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of those networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or services;

(42) 'security incident' means an event having an actual adverse effect on the security of electronic communications networks or services.

Article 40 **Security of networks and services**

2. Member States shall ensure that providers of public electronic communications networks or of publicly available electronic communications services notify without undue delay the competent authority of a security incident that has had a significant impact on the operation of networks or services.

In order to determine the significance of the impact of a security incident, where available the following parameters shall, in particular, be taken into account:
(a) the number of users affected by the security incident;
(b) the duration of the security incident;
(c) the geographical spread of the area affected by the security incident;
(d) the extent to which the functioning of the network or service is affected;
(e) the extent of impact on economic and societal activities.

Where appropriate, the competent authority concerned shall inform the competent authorities in other Member States and ENISA. The competent authority concerned may inform the public or require the providers to do so, where it determines that disclosure of the security incident is in the public interest.

Once a year, the competent authority concerned shall submit a summary report to the Commission and to ENISA on the notifications received and the action taken in accordance with this paragraph.

【出典】EUR-Lex https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L1972

Article 4 **Definitions**

(1) 'network and information system' means:
(a) an electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC;
(b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or
(c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;

(2) 'security of network and information systems' means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems;

(7) 'incident' means any event having an actual adverse effect on the security of network and information systems;

(13) 'internet exchange point (IXP)' means a network facility which enables the interconnection of more than two independent autonomous systems, primarily for the purpose of facilitating the exchange of internet traffic; an IXP provides interconnection only for autonomous systems; an IXP does not require the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic;

(14) 'domain name system (DNS)' means a hierarchical distributed naming system in a network which refers queries for domain names;

(15) 'DNS service provider' means an entity which provides DNS services on the internet;

(16) 'top-level domain name registry' means an entity which administers and operates the registration of internet domain names under a specific top-level domain (TLD);

(17) 'online marketplace' means a digital service that allows consumers and/or traders as respectively defined in point (a) and in point (b) of Article 4(1) of Directive 2013/11/EU of the European Parliament and of the Council (18) to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace;

(18) 'online search engine' means a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found;

(19) 'cloud computing service' means a digital service that enables access to a scalable and elastic pool of shareable computing resources.

【出典】EUR-Lex https://eur-lex.europa.eu/eli/dir/2016/1148/oj

Article 14 Security requirements and incident notification

3. Member States shall ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident. Notification shall not make the notifying party subject to increased liability.

4. In order to determine the significance of the impact of an incident, the following parameters in particular shall be taken into account:
(a) the number of users affected by the disruption of the essential service;
(b) the duration of the incident;
(c) the geographical spread with regard to the area affected by the incident.

Article 16 Security requirements and incident notification

3. Member States shall ensure that digital service providers notify the competent authority or the CSIRT without undue delay of any incident having a substantial impact on the provision of a service as referred to in Annex III that they offer within the Union. Notifications shall include information to enable the competent authority or the CSIRT to determine the significance of any cross-border impact. Notification shall not make the notifying party subject to increased liability.

4. In order to determine whether the impact of an incident is substantial, the following parameters in particular shall be taken into account:
(a) the number of users affected by the incident, in particular users relying on the service for the provision of their own services;
(b) the duration of the incident;
(c) the geographical spread with regard to the area affected by the incident;
(d) the extent of the disruption of the functioning of the service;
(e) the extent of the impact on economic and societal activities.

The obligation to notify an incident shall only apply where the digital service provider has access to the information needed to assess the impact of an incident against the parameters referred to in the first subparagraph.

5. Where an operator of essential services relies on a third-party digital service provider for the provision of a service which is essential for the maintenance of critical societal and economic activities, any significant impact on the continuity of the essential services due to an incident affecting the digital service provider shall be notified by that operator.

【出典】EUR-Lex https://eur-lex.europa.eu/eli/dir/2016/1148/oj

参考条文④：NIS2指令案

【出典】欧州委員会ウェブページ「Proposal for directive on measures for high common level of cybersecurity across the Union」（2020年12月16日）
https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union

Article 4 **Definitions**

(1) 'network and information system' means:
(a) an electronic communications network within the meaning of Article 2(1) of Directive (EU) 2018/1972;
(b) any device or group of inter–connected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data;
(c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;

(2) 'security of network and information systems' means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems;

(3) 'cybersecurity' means cybersecurity within the meaning of Article 2(1) of Regulation (EU) 2019/881 of the European Parliament and of the Council;

(5) 'incident' means any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the related services offered by, or accessible via, network and information systems;

(7) 'cyber threat' means a cyber threat within the meaning Article 2(8) of Regulation (EU) 2019/881;

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (**Cybersecurity Act**))

Article 2 Definitions

(1) 'cybersecurity' means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats;

(8) 'cyber threat' means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons;

【出典】欧州委員会ウェブページ「Proposal for directive on measures for high common level of cybersecurity across the Union」（2020年12月16日）
https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union

Article 4 **Definitions**

(12) 'internet exchange point (IXP)' means a network facility which enables the interconnection of more than two independent networks (autonomous systems), primarily for the purpose of facilitating the exchange of internet traffic; an IXP provides interconnection only for autonomous systems; an IXP does not require the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic;

(13) 'domain name system (DNS)' means a hierarchical distributed naming system which allows end-users to reach services and resources on the internet;

(14) 'DNS service provider' means an entity that provides recursive or authoritative domain name resolution services to internet end-users and other DNS service providers;

(15) 'top–level domain name registry' means an entity which has been delegated a specific TLD and is responsible for administering the TLD including the registration of domain names under the TLD and the technical operation of the TLD, including the operation of its name servers, the maintenance of its databases and the distribution of TLD zone files across name servers;

(16) 'digital service' means a service within the meaning of Article 1(1)(b) of Directive (EU) 2015/1535 of the European Parliament and of the Council 35;

(17) 'online marketplace' means a digital service within the meaning of Article 2 point (n) of Directive 2005/29/EC of the European Parliament and of the Council36;

(18) 'online search engine' means a digital service within the meaning of Article 2(5) of Regulation (EU) 2019/1150 of the European Parliament and of the Council37;

(19) 'cloud computing service' means a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable and distributed computing resources;

(20) 'data centre service' means a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of information technology and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control;

(21) 'content delivery network' means a network of geographically distributed servers for the purpose of ensuring high availability, accessibility or fast delivery of digital content and services to internet users on behalf of content and service providers;

(22) 'social networking services platform' means a platform that enables end-users to connect, share, discover and communicate with each other across multiple devices, and in particular, via chats, posts, videos and recommendations);

Article 20 **Reporting obligations**

1. Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT in accordance with paragraphs 3 and 4 of any incident having a significant impact on the provision of their services. Where appropriate, those entities shall notify, without undue delay, the recipients of their services of incidents that are likely to adversely affect the provision of that service. Member States shall ensure that those entities report, among others, any information enabling the competent authorities or the CSIRT to determine any cross-border impact of the incident.

2. Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT of any significant cyber threat that those entities identify that could have potentially resulted in a significant incident.

Where applicable, those entities shall notify, without undue delay, the recipients of their services that are potentially affected by a significant cyber threat of any measures or remedies that those recipients can take in response to that threat. Where appropriate, the entities shall also notify those recipients of the threat itself. The notification shall not make the notifying entity subject to increased liability.

3. An incident shall be considered significant if:

(a) the incident has caused or has the potential to cause substantial operational disruption or financial losses for the entity concerned;

(b) the incident has affected or has the potential to affect other natural or legal persons by causing considerable material or non-material losses.

【出典】欧州委員会ウェブページ「Proposal for directive on measures for high common level of cybersecurity across the Union」（2020年12月16日）
https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union

Article 20 **Reporting obligations**

4. Member States shall ensure that, for the purpose of the notification under paragraph 1, the entities concerned shall submit to the competent authorities or the CSIRT:

(a) without undue delay and in any event within 24 hours after having become aware of the incident, an initial notification, which, where applicable, shall indicate whether the incident is presumably caused by unlawful or malicious action;

(b) upon the request of a competent authority or a CSIRT, an intermediate report on relevant status updates;

(c) a final report not later than one month after the submission of the report under point (a), including at least the following:

(i) a detailed description of the incident, its severity and impact;

(ii) the type of threat or root cause that likely triggered the incident;

(iii) applied and ongoing mitigation measures.

Member States shall provide that in duly justified cases and in agreement with the competent authorities or the CSIRT, the entity concerned can deviate from the deadlines laid down in points (a) and (c).

5. The competent national authorities or the CSIRT shall provide, within 24 hours after receiving the initial notification referred to in point (a) of paragraph 4, a response to the notifying entity, including initial feedback on the incident and, upon request of the entity, guidance on the implementation of possible mitigation measures. Where the CSIRT did not receive the notification referred to in paragraph 1 , the guidance shall be provided by the competent authority in collaboration with the CSIRT. The CSIRT shall provide additional technical support if the concerned entity so requests. Where the incident is suspected to be of criminal nature, the competent national authorities or the CSIRT shall also provide guidance on reporting the incident to law enforcement authorities.

【出典】欧州委員会ウェブページ「Proposal for directive on measures for high common level of cybersecurity across the Union」（2020年12月16日）
https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union

Article 20 **Reporting obligations**

6. Where appropriate, and in particular where the incident referred to in paragraph 1 concerns two or more Member States, the competent authority or the CSIRT shall inform the other affected Member States and ENISA of the incident. In so doing, the competent authorities, CSIRTs and single points of contact shall, in accordance with Union law or national legislation that complies with Union law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided.

7. Where public awareness is necessary to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest, the competent authority or the CSIRT, and where appropriate the authorities or the CSIRTs of other Member States concerned may, after consulting the entity concerned, inform the public about the incident or require the entity to do so.

8. At the request of the competent authority or the CSIRT, the single point of contact shall forward notifications received pursuant to paragraphs 1 and 2 to the single points of contact of other affected Member States.

9. The single point of contact shall submit to ENISA on a monthly basis a summary report including anonymised and aggregated data on incidents, significant cyber threats and near misses notified in accordance with paragraphs 1 and 2 and in accordance with Article 27. In order to contribute to the provision of comparable information, ENISA may issue technical guidance on the parameters of the information included in the summary report.

10. Competent authorities shall provide to the competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] information on incidents and cyber threats notified in accordance with paragraphs 1 and 2 by essential entities identified as critical entities, or as entities equivalent to critical entities, pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive].

11. The Commission, may adopt implementing acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to paragraphs 1 and 2. The Commission may also adopt implementing acts to further specify the cases in which an incident shall be considered significant as referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).

Article 40 **Amendment of Directive (EU) 2018/1972**

Articles 40 and 41 of Directive (EU) 2018/1972 are deleted.

【出典】欧州委員会ウェブページ「Proposal for directive on measures for high common level of cybersecurity across the Union」（2020年12月16日）
https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union