欧州連合

NIS2指令

(Directive EU 2022/2555)

EU全域における高水準のサイバーセキュリティ共通基準のための措置

CISOおよびコンプライアンス担当者向け日本語サマリー

文書参照情報

項目	内容
正式名称	Directive (EU) 2022/2555
採択日	2022年12月14日
公布日	2022年12月27日 (OJ L 333/80)
発効日	2023年1月16日
各国法令への転換期限	2024年10月17日
廃止される法令	Directive (EU) 2016/1148 (NIS1)

> 本文書は2022年12月14日付EU NIS2指令の非公式サマリーです。拘束力を持つ解釈については、OJ L 333/80（2022年12月27日）所収の公式テキストをご参照ください。

目次

1. エグゼクティブサマリー

NIS2指令（Directive EU 2022/2555）は、2022年12月14日に欧州議会および欧州理事会によって採択されたEUの包括的サイバーセキュリティ基準指令です。2024年10月18日をもって、旧NIS1指令（2016/1148）を廃止・代替します。

レビュープロセスの結果、NIS1はEU全域のサイバーレジリエンス向上に貢献した一方で、現在および将来のサイバーセキュリティ脅威に対処するには不十分であることが判明しました。NIS2は適用範囲を大幅に拡大し、統一的な基準を導入するとともに、リスク管理・インシデント報告義務を強化し、より抑止力のある執行規定を設けています。

指令の5つの柱

1. **適用範囲の拡大**：規制対象となるセクターおよび企業の増加。
2. **リスク管理の強化**：Article 21に基づく10の最低限の技術的・組織的措置の義務化。
3. **迅速かつ段階的なインシデント報告**：24時間以内の早期警告、72時間以内のインシデント通知、1か月以内の最終報告。
4. **経営陣の責任**：上級管理職が個人として法的責任を負う可能性があります。
5. **抑止的制裁**：年間グローバル売上高の2%またはEUR 1,000万を上限とする行政罰。

2. 目的および法的根拠

本指令の法的根拠は、域内市場の確立および機能確保のために各国規則の近似化措置を認める**欧州連合機能条約（TFEU）第114条**です。

指令の主要目的は次のとおりです。

- 加盟国間の大きな格差を解消し、共通の最低限のサイバーセキュリティ規則を確立すること。
- 国境を越えた協力および情報共有のための実効的なメカニズムを構築すること。
- 今日の脅威環境を反映し、サイバーセキュリティ義務の対象となるセクターおよび活動のリストを更新すること。
- 義務の実効的な履行を確保するための執行・救済メカニズムを整備すること。
- 重要インフラ事業者およびデジタルサービスプロバイダーのサイバーレジリエンス能力を強化すること。

本指令は、個人データ保護に関するEU法（GDPR、Regulation EU 2016/679）および電子通信プライバシーに関するEU法（Directive 2002/58/EC）を侵害することなく、これらに準拠して適用されます。

3. NIS1からNIS2へ：新規制が必要な理由

2016年に発効したNIS1は、EUにおける最初の横断的サイバーセキュリティ規則でした。レビューの結果、加盟国間で実施に深刻な差異が生じていることが判明し、適用範囲の決定が加盟国の裁量に大きく委ねられていたため、域内市場の分断を招いていました。

NIS1の課題として特定された事項

課題領域	NIS1の状況	NIS2による解決策
適用範囲の決定	加盟国の裁量に委ねられており、実務上大きなばらつきがある。	EU全域で統一的な「規模上限」ルール（中規模・大規模企業）を適用。
セクターリスト	対象セクターが限定的で、デジタル経済の大部分が除外されている。	はるかに広いセクター範囲。デジタルインフラ、公共行政、宇宙など含む。
インシデント報告	単一段階であり、期限と内容が加盟国ごとに異なる。	多段階報告：24時間早期警告 + 72時間通知 + 1か月最終報告。
リスク管理	一般的な文言にとどまり、具体的な最低限措置が不明確。	Article 21が10の義務的最低限措置カテゴリを列挙。
制裁	加盟国ごとに非常に異なるレベルで実施されている。	EU全域で統一された上限罰則（EUR 1,000万 / 売上高の2%）。
上級管理職の責任	不明確。	経営陣がコンプライアンスについて個人責任を負う。必須トレーニング。

NIS2はNIS1の更新ではありません。EU全域で**統一された執行可能なサイバーセキュリティフレームワーク**を実現するための代替法令です。

4. 適用範囲と除外領域

本指令は主に、EU域内で**Annex I（高度重要）**またはAnnex II（その他重要）**セクターで事業を行い、少なくとも中規模企業の定義を満たす事業者を対象とします。委員会勧告2003/361/EC附属書のArticle 2に基づき、中規模企業とは従業員数250人未満かつ年間売上高がEUR 5,000万以下（または貸借対照表合計がEUR 4,300万以下）の企業を指します。NIS2の適用対象となる実質的な最低基準は、従業員50人以上または売上高EUR 1,000万以上（同勧告における「小規模企業」の上限）です。

規模にかかわらず対象となる事業者

- 公衆向け電子通信ネットワーク提供者および公衆向け電子通信サービス提供者。
- トラストサービスプロバイダー（eIDAS規則 EU 910/2014 に基づく）。
- トップレベルドメイン（TLD）名登録機関およびDNSサービスプロバイダー。
- ある加盟国においてサービスの唯一の提供者である事業者、またはサービス中断が公共の安全、健康もしくは安全保障に重大な影響を与えうる事業者。
- すべての中央政府機関（各加盟国が国内法で定義）。

適用範囲から除外される領域

活動が主に**国家安全保障、公共安全保障、防衛または法執行**（犯罪の防止、調査、探知および訴追）の分野で行われる公的機関は、本指令の適用範囲から除外されます。第三国における加盟国の外交・領事代表機関および閉鎖システムで使用されるトラストサービスも除外されます。

5. 主要定義

本指令を正確に解釈するために、以下の基本概念を明確に理解する必要があります。

用語	定義
ネットワークおよび情報システム	電子通信ネットワーク、デジタルデータを処理するすべてのデバイスまたはデバイス群、ならびにその運用・使用・保護・保守のために処理されるすべてのデジタルデータ。
サイバーセキュリティ	ネットワークおよび情報システム、ユーザーならびにその他の人々をサイバー脅威から保護するために必要なすべての活動。
インシデント	ネットワークおよび情報システムを通じて提供またはアクセス可能なサービスによって保存・送信・処理されるデータ、またはそのサービスの可用性、真正性、完全性もしくは機密性を損なう事象。
重大インシデント	対象事業者のサービスに重大な業務上の支障もしくは財務上の損失を引き起こしたまたは引き起こすおそれのあるインシデント、あるいは相当の有形・無形の損害をもたらすことで他の自然人または法人に影響を与えたまたは与えるおそれのあるインシデント。
サイバー脅威	ネットワークおよび情報システムに損害を与え、これを妨害し、またはその他の悪影響を及ぼすおそれのある潜在的な状況、事象または行為。
重大なサイバー脅威	その技術的特性に基づき、事業者のネットワークおよび情報システム、そのユーザー、またはその他の者に対して、相当の有形・無形の損害をもたらすことで重大な影響を及ぼす可能性があると想定されるサイバー脅威。
脆弱性	サイバー脅威によって悪用される可能性のある、ICT製品またはサービスの弱点、感受性または欠陥。
ニアミス	ネットワークおよび情報システムを通じて提供またはアクセス可能なサービスによって保存・送信・処理されるデータ、またはそのサービスの可用性、真正性、完全性もしくは機密性を損なう可能性があったが、実際には発生を防ぐことができた事象。
CSIRT	Computer Security Incident Response Team（コンピューターセキュリティインシデント対応チーム）。インシデントの検知・対応・復旧を担当する専門技術チームです。
ENISA	European Union Agency for Cybersecurity（欧州連合サイバーセキュリティ機関）。本指令の実施において中心的な助言・支援の役割を担い、欧州脆弱性データベースの管理も行います。

6. 事業者区分：重要事業者と重要性の高い事業者

本指令は、適用対象のすべての事業者を2つの主要区分に分類します。この区分は、義務の適用方法および監督・執行体制を決定します。

基準	重要事業者	重要性の高い事業者
セクター	Annex I、高度重要セクター	Annex II、その他重要セクター（およびAnnex Iの中規模企業）
規模	大規模企業（従業員250人以上または売上高EUR 5,000万以上）	中規模企業（従業員50人以上249人以下）
監督体制	事前・事後の両方の監督	証拠または苦情に基づく事後監督のみ
行政罰の上限	EUR 1,000万またはグローバル年間売上高の2%（いずれか高い方）	EUR 700万またはグローバル年間売上高の1.4%（いずれか高い方）
上級管理職への制裁	一時的な経営禁止命令が適用される場合があります	一時的な経営禁止命令は適用されません

> **重要：** NIS1において「重要サービス事業者」として特定されていた事業者は、加盟国の判断により、NIS2においても直接「重要事業者」として扱われる場合があります。また、Directive 2022/2557（CER）に基づき「重要事業者」として特定されたすべての事業者は、自動的にNIS2の「重要事業者」とみなされます。

7. 適用範囲のセクター（Annex IおよびAnnex II）

Annex I、高度重要セクター

これらのセクターの大規模企業は重要事業者となり、中規模企業は重要性の高い事業者となります。

セクター	サブセクター / 事業者の種類
エネルギー	電力（発電、送電、配電、供給）；地域暖冷房；石油（パイプライン、生産、貯蔵、輸送）；天然ガス；水素の生産・貯蔵・輸送
輸送	航空（航空会社、空港、航空交通管制）；鉄道（インフラ管理者、鉄道事業者）；水運（海上・内陸水路事業者）；道路（高度道路交通システム、道路事業者）
銀行	Regulation (EU) 575/2013 に基づく信用機関
金融市場インフラ	取引所等の取引場所および中央清算機関（CCP）
医療	医療サービス提供者；EU参照検査機関；医薬品の研究開発を行う機関；製薬企業；公衆衛生上の緊急事態において重要とみなされる医療機器製造業者（Regulation (EU) 2022/123 に基づく）
飲料水	人の消費向けの水の供給者および配給者
廃水	都市排水、生活排水または産業排水の収集、処理または処分を行う事業者
デジタルインフラ	インターネットエクスチェンジポイント（IXP）；DNSサービスプロバイダー（ルートDNSを除く）；TLD名登録機関；クラウドコンピューティングサービスプロバイダー；データセンターサービスプロバイダー；コンテンツデリバリーネットワーク（CDN）プロバイダー；トラストサービスプロバイダー；公衆向け電子通信ネットワーク・サービスプロバイダー
ICTサービス管理（B2B）	マネージドサービスプロバイダー（MSP）；マネージドセキュリティサービスプロバイダー（MSSP）
公共行政	加盟国が定義する中央および地域の政府機関
宇宙	加盟国または民間セクターが運営する地上インフラの運用者

Annex II、その他重要セクター

セクター	サブセクター / 事業者の種類
郵便・宅配便	郵便サービスプロバイダー（宅配便サービスを含む）
廃棄物管理	廃棄物の収集、リサイクルおよび処分サービスを提供する事業者
化学品	化学品の製造、加工および流通に従事する事業者
食品	食品の生産、加工および卸売流通に従事する大規模企業
製造	医療機器・体外診断用医療機器；コンピューター・電子・光学製品；電気機器；機械・設備（他に分類されないもの）；自動車・トレーラー・セミトレーラー；その他の輸送機器製造
デジタルプロバイダー	オンラインマーケットプレイス；オンライン検索エンジン；ソーシャルネットワーキングサービスプラットフォーム
研究	商業目的の研究を行う研究機関

8. 加盟国の義務

本指令は、民間企業と同様に加盟国にも義務を課します。各加盟国は以下の措置を講じる必要があります。

国家サイバーセキュリティ戦略。 明確な戦略目標、優先事項およびガバナンスフレームワークを含む国家サイバーセキュリティ戦略を採択すること。当該戦略は、サプライチェーンセキュリティ、ランサムウェア、中小企業支援、オープンソースおよび積極的サイバー防衛などの課題を取り上げます。

所轄当局。 本指令の実施および監督を確保するために、1つ以上の所轄当局を指定または設立すること。

単一窓口（SPOC）。 EUレベルでの国境を越えた調整を担当する単一窓口を指定すること。

CSIRT。 インシデント対応、プロアクティブな監視、脆弱性の協調的な開示、ならびに国内・国際的な協力を担当する1つ以上のCSIRTを設立または指定すること。

事業者リスト。 重要事業者、重要性の高い事業者、およびドメイン名登録サービスを提供する事業者のリストを維持・定期的に更新し、欧州委員会に提出すること。

脆弱性の協調的な開示。 CSIRTをコーディネーターとして指定し、脆弱性調査者のための法的明確性を促進すること。

相互支援。 国境を越えた監督・執行において他の加盟国に相互支援を提供すること。

中小企業支援。 小規模・零細企業向けのガイダンス、無料ツールおよび国内・地域の窓口を提供すること。

9. サイバーセキュリティリスク管理措置（Article 21）

本指令において最も重要な技術的規定はArticle 21です。重要事業者および重要性の高い事業者が実施しなければならない最低限の技術的・運用的・組織的措置を列挙しています。このアプローチは**「オールハザード」アプローチ**に基づいており、サイバー攻撃のみならず、物理的損害、自然災害、機器の故障、人的エラーなどの脅威もカバーしています。

Article 21、10の最低限措置

#	措置	説明
1	リスク分析および情報システムセキュリティポリシー	すべてのリスクの分析と一般的な情報セキュリティポリシーの文書化。
2	インシデント対応	インシデントの予防、検知、対応および復旧のためのプロセス。
3	事業継続性	バックアップ管理、災害復旧およびクライシスマネジメント。
4	サプライチェーンセキュリティ	サプライヤーのセキュリティ慣行を含む。直接サプライヤーとの契約へのサイバーセキュリティ条項の盛り込み。
5	ネットワークおよび情報システムの調達・開発・保守におけるセキュリティ	脆弱性の対処と開示を含む、ライフサイクル全体にわたるセキュリティ。
6	措置の有効性の評価	リスク管理措置の有効性の定期的な評価。
7	基本的なサイバーハイジーン慣行とセキュリティトレーニング	従業員向けのサイバーハイジーン慣行と意識向上トレーニング。
8	暗号化	暗号化の使用に関するポリシー。必要に応じたエンドツーエンド暗号化。
9	人的資源セキュリティ、アクセス制御および資産管理	人員のセキュリティ審査、認可および資産目録。
10	多要素認証とセキュアな通信	適切な場合のMFA、継続的認証、セキュアな音声・映像・テキスト通信、緊急時のセキュアな通信システム。

これらの措置は、事業者のリスクエクスポージャー、規模、セクターの重要性およびインシデントの潜在的な影響を考慮した**比例原則**に基づいて適用されます。

10. インシデント報告義務（Article 23）

本指令の最も重要な運用上の革新点は、多段階インシデント報告体制です。重要事業者および重要性の高い事業者は、重大な業務上の支障、財務上の損失、または他者への相当の影響を引き起こすものとして定義される**重大インシデント**を、以下の期限内にCSIRTまたは所轄当局に報告しなければなりません。

段階	期限	内容
早期警告	インシデントを認識してから24時間以内	インシデントが不法・悪意のある行為によって引き起こされたとの疑い；国境を越えた影響の可能性；CSIRTが認識できる基本情報。
インシデント通知	インシデントを認識してから72時間以内	早期警告の更新；重大性、影響、および利用可能な場合は侵害指標（IoC）。
中間・最終報告	インシデント通知後遅くとも1か月以内	インシデントの詳細な説明、その重大性と影響；悪用された脅威の種類；講じた・予定している緩和措置；国境を越えた影響（ある場合）。
進捗報告	最終報告の期限においてインシデントが継続中の場合	インシデントの現状に関する進捗報告；インシデント対応の完了から1か月後に最終報告。

サービス受領者への通知： 重大なサイバー脅威が発生するおそれがある場合、事業者は不当な遅延なく、かつ無償で、サービス受領者に対して可能な緩和措置、および適切な場合には脅威自体について、明確かつ分かりやすい言葉で通知しなければなりません。

ニアミスと自発的な報告

インシデントに加え、事業者はニアミスおよび重大なサイバー脅威をCSIRTまたは所轄当局に**自発的に報告することができます**。本指令の適用範囲外の事業者も自発的に報告することができます。自発的な報告は報告者に追加の義務を課しません。

> **実務上の影響：** 24時間早期警告は、事業者がインシデント検知後ただちに起動できるサイバーインシデント対応計画および通信フローを整備することを求めます。手動かつ断片的なプロセスでこの期限を遵守することは極めて困難です。

11. サプライチェーンセキュリティ

近年の主要なサイバー攻撃の多くは、組織への直接攻撃ではなく、サプライヤーやソフトウェアプロバイダーを経由して標的組織に到達しています。そのため本指令は、サプライチェーンリスクをリスク管理義務の中心に位置づけています。

- 事業者は、サプライヤーおよびサービスプロバイダーの製品・サービスについて、その**品質、セキュリティ慣行および安全な開発プロセス**を評価しなければなりません。
- **直接サプライヤーとの契約にサイバーセキュリティ要件を盛り込まなければなりません。**
- **マネージドセキュリティサービスプロバイダー（MSSP）**の選定に際しては特別な注意を払う必要があります。これらのプロバイダーは攻撃者にとって高価値な標的となるからです。
- 協力グループは、欧州委員会およびENISAとともに、重要なサプライチェーン（5Gネットワークに対して実施されたものと同様）について**協調的なセキュリティリスク評価**を実施します。
- サプライヤーに対する第三国の潜在的な不当な影響、隠れた脆弱性・バックドア、プロバイダー依存など、**非技術的なリスク要因**も評価の対象となります。

12. 経営陣の責任

本指令は、サイバーセキュリティが技術部門に限定された課題から、**上級管理職の直接的な責任領域**へと移行することを確保しています。Article 20に基づき、重要事業者および重要性の高い事業者の経営陣は以下の責任を負います。

- Article 21に基づく**リスク管理措置の承認**とその実施の監督について責任を負います。
- これらの義務違反に対して**個人として法的責任を問われる**可能性があります。
- 十分な知識とスキルを習得するためにサイバーセキュリティトレーニングを定期的に受講しなければなりません。
- 従業員に対しても同様のトレーニングを奨励すべきです。

> **重要：** 重要事業者においては、所轄当局がCEOまたは法定代理人レベルの上級管理職に対して**一時的な経営禁止命令**の適用を求めることができます。これは最後の手段であり、他のすべての執行手段が尽くされた後にのみ適用されます。

13. EU域内の協力体制

本指令は、加盟国間の実効的な協力を確保するさまざまな体制を規制または強化しています。

組織・体制	機能
協力グループ	戦略レベルでの協力を支援；2年ごとの作業プログラムを策定；ガイダンス文書を発行；重要サプライチェーンの協調リスク評価を実施。
CSIRTs Network	運用レベルでの協力；インシデント情報の共有；相互支援；共同対応。
EU-CyCLONe	欧州サイバー危機連絡組織ネットワーク；大規模インシデントおよび危機において技術レベルと政治レベルを橋渡しする；影響分析を策定。
ENISA	欧州脆弱性データベースの設立・維持；技術支援の提供；ガイダンスの策定；加盟国のサイバーハイジーンポリシーの監視。
IPCR体制	EU統合政治危機対応体制（Council Implementing Decision 2018/1993）。大規模危機に対するEUレベルの危機管理。
EU-CSIRTs CVDコーディネーター	各加盟国において、国境を越えた脆弱性協調開示を管理するCSIRTがコーディネーターとして指定されます。

第三国との協力： EUはTFEU第218条に基づき、第三国または国際機関と国際協定を締結することができます。かかる協定は、EUの利益およびデータ保護を守りながら、当該当事者が協力グループ、CSIRTs NetworkまたはEU-CyCLONeの活動に参加することを認める場合があります。

14. 監督と執行

本指令は、2つの事業者区分に対して異なる監督体制を定めています。**重要事業者**は事前・事後の両方の監督に服しますが、**重要性の高い事業者**は証拠または苦情に基づく事後監督のみに服します。

所轄当局の監督権限

- 実地検査および遠隔監督の実施。
- 標的型セキュリティ監査の要求（事業者がコストを負担する場合があります）。
- セキュリティスキャンの命令。
- リスク管理措置のコンプライアンスに関する文書の要求。
- 本指令への違反が疑われる行為に関する情報の要求。
- 必要な場合に個人データおよびトラフィックデータへのアクセスを要する情報の要求。

適用可能な執行措置

- 警告および拘束力のある指示の発出。
- 指定期間内に特定の措置または脆弱性の是正を実施するよう命令。
- リスク管理措置を検証するための独立監査を命令。
- 事業者に対してサービス受領者に違反の性質を通知するよう命令。
- 公開声明の発表（事業者名と違反の性質の公表）。
- 重要事業者（最後の手段）：認証・認可の一時停止および上級管理職への一時的な経営禁止命令。
- 行政罰の賦課または賦課の申請。

15. 行政罰

本指令は、加盟国が適用する行政罰について**EU全域で統一された上限閾値**を定めています。この閾値は、GDPRと同様に、事業者のグローバル売上高に連動しています。

事業者の種類	上限額（いずれか高い方が適用されます）
重要事業者	EUR 10,000,000 またはグローバル年間売上高の2%
重要性の高い事業者	EUR 7,000,000 またはグローバル年間売上高の1.4%

罰則額の決定要因

- 違反の性質、重大性および期間。
- 引き起こされた有形・無形の損害。
- 違反が故意によるものか過失によるものか。
- 損害の防止または軽減のために講じた措置。
- 責任の程度および過去の違反。
- 所轄当局との協力の程度。
- その他の加重・軽減要因。

罰則は**比例的**でなければならず、弁護権、無罪推定の原則および実効的な救済を受ける権利などの基本的権利が適用において尊重されなければなりません。加盟国は国内法違反に対して刑事制裁を設けることもできますが、**一事不再理（ne bis in idem）**の原則に反して同一の行為について二重に処罰することはできません。

16. 施行スケジュールと移行

日付	出来事
2022年12月14日	欧州議会および欧州理事会による指令の採択
2022年12月27日	EU官報への掲載（OJ L 333/80）
2023年1月16日	指令の発効（公布から20日後）
2024年10月17日	加盟国による国内法への転換期限
2024年10月18日	指令の適用開始
2024年10月18日	Directive (EU) 2016/1148 (NIS1)の廃止
2025年4月17日	重要事業者・重要性の高い事業者のリストを欧州委員会に提出する加盟国の期限
2027年10月17日以降	欧州委員会による指令実施の定期的な見直し（36か月ごと）

> **重要：** NIS2は指令であり、直接適用されません。各加盟国は指令を自国の国内法に転換しなければなりません。したがって、事業者に適用される具体的な義務と制裁は、その事業者が事業を行う加盟国が採択した国内転換法令に依存します。

17. EU域外企業への影響

NIS2はEUの指令ですが、特にEU市場にサービスを提供しているか、またはEUを拠点とする重要事業者にサービスを供給しているEU域外企業に対して、相当の影響を与えます。

直接的な影響を受けるEU域外企業

- EUでサービスを提供するEU域外の**DNSプロバイダー、クラウドサービスプロバイダー、データセンター事業者、CDNプロバイダー、マネージドサービス・マネージドセキュリティサービスプロバイダー、オンラインマーケットプレイス、検索エンジンおよびソーシャルネットワーキングプラットフォーム**は、EUの代表者を任命し、指令の義務を遵守しなければなりません。
- EU子会社または支社を持つEU域外企業は、これらの拠点を通じて指令の適用を受ける場合があります。
- EUの重要事業者・重要性の高い事業者に製品・サービスを提供するEU域外のサプライヤーは、顧客から課される**サプライチェーンセキュリティの契約上の要件**（Article 21(2)(d)）の対象となります。
- EUのデジタルインフラや金融機関にサービスを提供するEU域外のMSP・MSSPは、直接適用範囲に該当する場合があります。

間接的な影響

- EU顧客によるサプライチェーンリスク評価が、EU域外サプライヤーにサイバーセキュリティ基準の引き上げを迫ります。
- 本指令が導入する基準（ISO/IEC 27001、ENISAガイダンスなど）は、グローバル市場で**事実上の参照基準**となりつつあります。
- EU域外の法域では、自国のサイバーセキュリティ法制を整備する際にNIS2を参照するケースが増えています。

18. 実践的コンプライアンスロードマップ（10ステップ）

以下の10ステップのロードマップは、EU域内で事業を営む企業および自発的にNIS2基準に準拠することを希望する企業の双方に向けた実践的なガイドとして機能します。

ステップ	活動内容
1. 適用範囲の確認	自社がAnnex IまたはAnnex IIのセクターに該当するか、規模基準を満たすかを確認し、区分（重要/重要性の高い事業者）を特定する。
2. ギャップ分析	既存の情報セキュリティマネジメントシステムをArticle 21の10の措置カテゴリと照らし合わせて評価し、ギャップをマッピングする。
3. ガバナンス体制の構築	取締役会・上級管理職レベルでの責任、報告ライン、承認プロセスを確立し、定期的なトレーニングプログラムを整備する。
4. ポリシーと文書化	情報セキュリティポリシー、リスク管理ポリシー、インシデント対応ポリシー、利用規程、その他の文書を作成または更新する。
5. リスク評価	オールハザードアプローチで資産目録、脅威分析およびリスク評価を実施し、リスク受容基準を確立する。
6. 技術的コントロールの実装	MFA、暗号化、ネットワークセグメンテーション、ゼロトラストアーキテクチャ、ログ管理、SIEM、EDR/XDR、バックアップおよびディザスタリカバリソリューションを実装する。
7. インシデント対応能力の整備	インシデント対応計画を文書化し、役割・責任を割り当て、24時間早期警告の通信フローを確立し、机上演習を実施する。
8. サプライチェーン管理	サプライヤーを目録化し、リスクレベルで分類し、契約テンプレートにサイバーセキュリティ条項を追加し、定期監査を実施する。
9. トレーニングと意識向上	全従業員を対象とした年次サイバーハイジーントレーニングを実施し、経営陣への専門トレーニングを提供し、フィッシングシミュレーションを実施する。
10. 継続的改善	内部・外部監査を実施し、KPIを追跡し、各インシデントから学び、リスク評価を年次更新し、認証（ISO/IEC 27001、EUサイバーセキュリティ認証）を取得する。

19. 結論と評価

NIS2指令は、欧州連合のサイバーセキュリティベースラインを大幅に引き上げます。技術的要件を課すにとどまらず、サイバーセキュリティを**企業のガバナンス構造と事業運営の不可欠な要素**とします。

指令の強み

- **広範な影響範囲**：EU-27全域でおよそ18のセクター、10万社以上の事業者が対象。
- **調和化**：EU全域での統一的な基準と執行体制により、域内市場でのイコールフッティングを実現。
- **ガバナンス重視**：上級管理職に説明責任を課すことで、サイバーセキュリティが企業のあらゆる階層に浸透することを確保。
- **サプライチェーンの重視**：現代の攻撃の大部分がサプライチェーン経由という現実に対応。
- **協力体制**：協力グループ、CSIRTs NetworkおよびEU-CyCLONeを通じた多層的なEUレベルの調整。

批判と課題

- 加盟国の転換における遅延と格差。EU-27全域での統一的な実施は実務上まちまちである。
- 特に中規模企業にとって、コンプライアンスコストと技術能力のギャップ解消は深刻な課題をもたらす。
- 十分な成熟度が達成される前の24時間早期警告期限の実施は、不十分または誤った報告フローにつながるおそれがある。
- セクター別規制（DORA（金融）、eIDAS（トラストサービス）、航空セクター別規制など）との重複領域が事業者にとって複雑さをもたらす場合がある。

総合評価

NIS2はサイバーセキュリティを技術的な懸念事項から、**事業継続性、コーポレートガバナンスおよび顧客信頼**の問題として再定義します。EUで事業を行うまたはEUと関わりを持つ事業者にとって、コンプライアンスは法的義務であると同時に、運用レジリエンスを強化する手段です。

EU域外企業にとって、NIS2はEU市場へのアクセスに向けた新たな**事実上の基準**を確立しつつあり、サイバーセキュリティへの期待をグローバルに引き上げています。早期のコンプライアンス対応は、契約上の義務の履行を容易にし、全体的なサイバーレジリエンスの向上につながります。

> **最終注記：** 本文書は指令の主要規定をまとめたものです。自組織に特有のコンプライアンス要件については、公式テキスト（OJ L 333/80、2022年12月27日）、事業を行う加盟国の国内転換法令、およびセクター別規制を参照し、必要に応じて法律・サイバーセキュリティの専門家に相談してください。

出典

- Directive (EU) 2022/2555, EUR-Lex CELEX番号 32022L2555
- Official Journal of the EU L 333/80, 27 December 2022
- ENISA, European Union Agency for Cybersecurity (www.enisa.europa.eu)
- European Commission Digital Strategy portal (digital-strategy.ec.europa.eu)

RediaccのNIS2関連情報

本サマリーは指令の構造と義務をマッピングしています。rediacc.comのコンパニオンガイドでは、これらの義務を具体的な運用上・調達上の決定に落とし込んでいます。

3つのコンパニオンガイド

- **Article 21(2)(d)とセルフホスティング。** データプレーンがテナントの外に出ない場合にサードパーティICT登録がどれほど縮小するか。2026年にDPAを再交渉するCISOおよび調達リード向け。
- **パフォーマンス管理のない継続的有効性。** Article 21(2)(e)、(f)および23を合わせて読み解く。週次ドリルを現実的にする定数時間フォークと、フォレンジックグレードのアーティファクトなしには対応できないArticle 23報告タイムライン。SREおよびオペレーションリード向け。
- **NIS2コンプライアンスの構造的コスト。** ミッドマーケットの重要事業者が静かに組み上げている5ツールスタック、セルフホステッドコントロールプレーンが何を集約するか、いずれにしても自社で担う費用項目。更新サイクルを迎えるCFOおよびバイヤー向け。

掲載場所

3つのガイドと本サマリーのダウンロード可能PDFは、以下で入手できます。

rediacc.com/resources/nis2-directive-summary

Rediacc OÜ はエストニア登録のセルフホステッドインフラプラットフォームです（登録番号17363830、VAT EE102920091）。本製品はセキュリティプログラムの代替ではありません。従来のバックアップ、DR、テストデータツールでは排除できないデータプレーンのベンダーリスクを取り除くツーリングレイヤーです。無料のCommunityティアと月額$349からの有料ティアをご用意しています。

> 本文書およびコンパニオンガイドは教育目的の資料です。自組織に特有のコンプライアンス判断には、法律の専門家への相談と事業を行う法域の国内転換法令の参照が必要です。