EU サイバーセキュリティ強化法「 NIS2 指令」
― 日本企業への影響

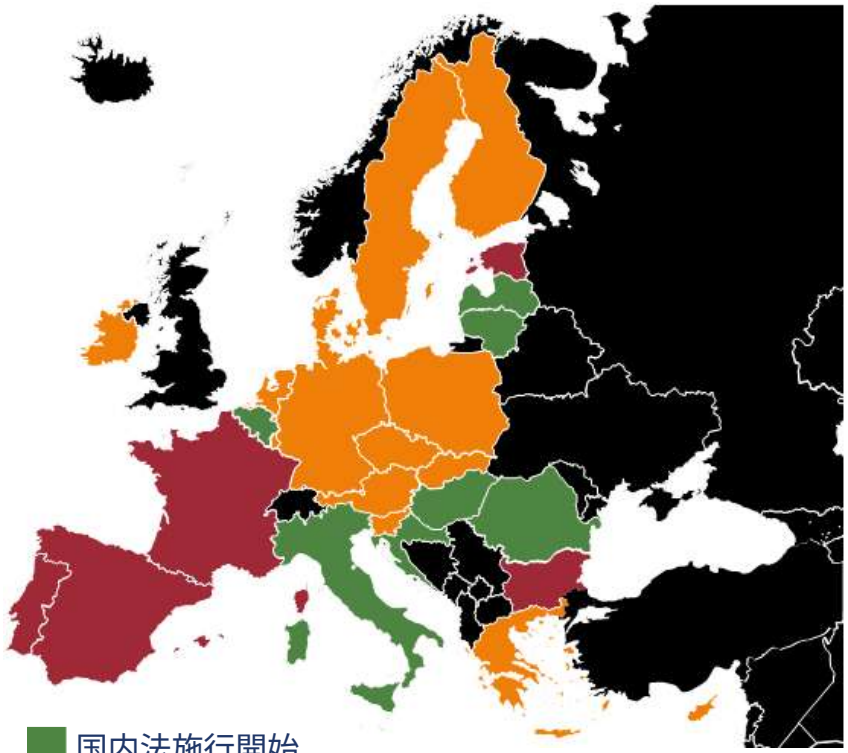
2025 年 7 月 17 日（木）
ミュンヘン日本人会 法人セミナー

Enobyte
Data Protection

NIS2 について

NIS2 指令（ネットワーク及び情報システム指令）は、 EU 全域でのサイバーセキュリティレベルの強化を目指し、 EU 加盟国に対して 2023 年 1 月 16 日に施行されました。 NIS2 指令は各 EU 加盟国により国内法に移管され、国内法の施行と同時に適用範囲に該当する企業は規制対象となります。

加盟国によっては国内法の法制化に大幅な遅延が発生していますが、 Enobyte は**国内法を待たずに、NIS2 指令の第 21 条で要求されている 10 項目の「リスクマネジメント対策」に着手すること**を強く推奨しています。



（参照： https://www.cyber-regulierung.de/nis-2-umsetzung/ ）

セミナー概要

- NIS2 の対象に該当するかどうかの判断基準
- 当局への登録
- リスクマネジメント対策（第 21 条）
- コンプライアンスまでの道のりと罰則

NIS2 の概要

Network and **I**nformation **S**ystems
（ネットワーク及び情報システム）

正式名称： Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)

リンク： https://eur-lex.europa.eu/eli/dir/2022/2555

目的

ネットワークおよび情報システムの保護
＝　持続的な経済・社会機能の確保

- 企業ごとのサイバーセキュリティの標準化
- サプライチェーン攻撃からの防御力向上
- インシデント発生時の迅速な対応促進　等

NIS2 の重要点

- 適用範囲の拡大
- 経営責任者の義務と責任の厳格化
- インシデント報告義務の厳格化
- リスクマネジメント対策

適用範囲

第２条（１）

本指令は、勧告 2003/361/EC の附属書第 2 条に従い中堅企業に該当する、または同条第 1 項に定める中堅企業の閾値を超える、**附属文書 I または II に記載される**タイプの公的または私的事業体であり、**域内へサービスを提供または域内で活動を実施するもの**に適用されるものとする。(仮日本語訳)

附属文書Ⅰ・Ⅱ

＜附属文書Ⅰ：高重要分野＞

エネルギー、交通・運輸、銀行、金融市場インフラ、保健衛生、飲料水、廃水、デジタルインフラ、 ICT サービスマネジメント（ B2B ）、行政、宇宙

＜附属文書Ⅱ：その他重要分野＞

郵便・宅配サービス、廃棄物管理、化学物質の生産・製造・取引、食品の製造・加工・流通、商品製造、デジタルプロバイダー、研究

（※赤字… NIS から新たに追加、青字… NIS からセクターを拡大）

企業規模

原則：従業員 50 人以上または年間売り上げ 1,000 万ユーロ以上

企業規模	従業員数（フルタイム）	年間売り上げ
小	～ 49 人　かつ	～ 1,000 万ユーロ
中	50 ～ 249 人　かつ	～ 5,000 万ユーロ
大	250 人 ～　または	5,000 万ユーロ ～

（出典： COMMISSION RECOMMENDATION
of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003H0361 ）

適用対象の原則

附属Ⅰ 高重要分野	大	中	小
エネルギー、交通・運輸、銀行、金融市場インフラ、保健衛生、飲料水、廃水、デジタルインフラ、 ICT サービスマネジメント（ B2B ）、行政、宇宙	主要	重要	—
附属Ⅱ その他重要分野	**大**	**中**	**小**
郵便・宅配サービス、廃棄物管理、化学物質の生産・製造・取引、食品の製造・加工・流通、商品製造、デジタルプロバイダー、研究	重要	重要	—

主要および重要エンティティ

	主要エンティティ	重要エンティティ
説明	欠如すると社会に深刻かつ大規模な影響を及ぼすエンティティ	欠如しても社会や経済は持続可能である可能性が高いエンティティ。一般的な機能を維持するのに役立つ
監査の種類	実地監査、抜き打ち監査	実地監査
いつ	事前、事後	事後（根拠付けられた不審点がある場合のみ）
制裁金	1,000 万€以下、または全世界年間総売上の 2 %以下のうち、いずれか高い方	700 万€以下、または全世界年間総売上の 1.4 %以下のうち、いずれか高い方

原則例外→実質対象「例外からの除外」

- 主要インフラ法
- デジタルインフラ
- グループ企業、関連企業
- サプライチェーン　など

NIS2 適用範囲簡易診断 （日本語）

https://assessments.enobyte.com/index.php?r=survey/index&sid=783196&lang=ja

要求事項

1. 当局への登録

当局への登録

- 企業名
- 連絡先（Ｅメール、 IP アドレス範囲、電話番号）
- 附属ⅠまたはⅡのうち該当する部門
- ビジネスを展開する EU 加盟国

※ **国内法施行開始から３ヶ月以内**

2. リスクマネジメント対策

第 21 条 リスクマネジメント対策

- 技術的、運用的および組織的対策の実装
- 最低要件 10 個（第 21 条 2 項 a ～ f ）
- 対策への決定およびリソースの提供責任は経営責任者にある

第 21 条 リスクマネジメント対策

- リスク分析
- 対策の効果性評価
- インシデントハンドリング
- サイバー衛生、トレーニング
- 事業継続
- 暗号学
- サプライチェーンセキュリティ
- 人的措置、アクセス管理
- ICT の取得、開発、維持ためのセキュリティ
- 安全な緊急時のコミュニケーション、多要素認証

第 21 条 リスクマネジメント対策

- リスク分析
- 対策の効果性評価
- インシデントハンドリング
- サイバー衛生、トレーニング
- 事業継続
- 暗号学
- サプライチェーンセキュリティ
- 人的措置、アクセス管理
- ICT の取得、開発、維持ためのセキュリティ
- 安全な緊急時のコミュニケーション、多要素認証

(1) リスク分析

対策手順

- 全 IT システムの棚卸し
- 潜在的なリスクの洗い出し（自然災害を含む）
- リスクの割り当て（システム、データ、情報）
- 発生確率 × 重大性 = リスクの程度
- 対策の優先順位付け
- 防御策を**予め**実装

発生確率 × 重大性 = リスクの程度

発生確率 / 重大性	低い	可能性あり	高い	ほぼ確実
致命的	低リスク	中リスク	高リスク	超高リスク
重大	低リスク	中リスク	高リスク	高リスク
中程度	低リスク	低リスク	中リスク	中リスク
軽微	低リスク	低リスク	低リスク	低リスク

例：顧客からの注文受付システム

- **① 水害**
  - サーバールームが地下
  - 上の階はトイレ
- **② 不正アクセス**
  - システムのモニタリング
  - 従業員のトレーニング
  - 鍵付きキャビネット

① 水害

発生確率 / 重大性	低い	可能性あり	高い	ほぼ確実
致命的	低リスク	中リスク	高リスク	超高リスク
重大	低リスク	中リスク	高リスク	高リスク
中程度	低リスク	低リスク	中リスク	中リスク
軽微	低リスク	低リスク	低リスク	低リスク

例：顧客からの注文受付システム

- **① 水害**
  - サーバールームが地下
  - 上の階はトイレ
- **② 不正アクセス**
  - システムのモニタリング
  - 従業員のトレーニング
  - 鍵付きキャビネット

② 不正アクセス

重大性＼発生確率	低い	可能性あり	高い	ほぼ確実
致命的	低リスク	中リスク	高リスク	超高リスク
重大	低リスク	中リスク	高リスク	高リスク
中程度	低リスク	低リスク	中リスク	中リスク
軽微	低リスク	低リスク	低リスク	低リスク

① 水害、②不正アクセス

発生確率 / 重大性	低い	可能性あり	高い	ほぼ確実
致命的	低リスク	中リスク	高リスク	超高リスク
重大	低リスク	中リスク	高リスク	高リスク
中程度	低リスク	低リスク	中リスク	中リスク
軽微	低リスク	低リスク	低リスク	低リスク

(2) インシデント ハンドリング

概要

- 社内報告
- 各関連当局への報告
- 技術的及び組織的な救済措置
  - 必要に応じて外部の応援要請
- 対策の見直し・強化

準備

- 社内報告

  コミュニケーション経路の決定と周知、インシデント対応チームの編成と育成

- 各関連当局への報告

  管轄当局の特定、連絡先、報告内容および時間制限の確認

- 技術的及び組織的な救済措置

  - 必要に応じて外部の応援要請

  緊急時に即時対応可能な外部と予め契約を締結（オンコール規定）

- 対策の見直し・強化

推奨例：

IT緊急時対応ガイド

落ち着いて、まずは報告を！

不審な点がある場合は、小さなインシデントでも報告を。
迅速な報告がインシデントによる影響の抑制、縮小に繋がる。

緊急に対応が必要な状況

- マルウェア感染
- 怪しいリンクへのアクセス
- 電子機器や鍵の紛失
- 詐欺、なりすまし
- オフィスの不審者侵入
- 盗聴、盗難　等

確認事項

WHEN	いつインシデントが発覚したか
WHERE	どこでインシデントが発生したか
WHO	誰に報告するか
HOW	どのようにインシデントが発覚したか
WHAT	なにが影響を受けたか

連絡先

データ保護オフィサー (DPO) :
IT 担当者 :
:

経営責任者が報告する関連機関

インシデントの種類によって報告先が異なる

個人データ漏洩 ⚠72時間以内
データ保護監督当局 (LDI)
0211 / 38 424 - 0
https://www.ldi.nrw.de

犯罪行為または詐欺など
警察庁　サイバー犯罪中央窓口
0211 / 939 - 4040
cybercrime.lka@polizei.nrw.de

Enobyte
Data Protection

0211 / 822 68 67 - 0
support@enobyte.com
https://enobyte.com

どんな時に報告するか

何を報告するか

誰に何で報告するか

どんな時どの当局に
いつまでに報告するか

監督当局への報告義務

重大なインシデントが発生した場合、**経営責任者**が報告を行う。

- 早期報告（２４時間以内）
- 報告（７２時間以内）
- 中間報告（リスク管理チームまたは当局の要求に応じて）
- 最終報告（１ヶ月以内）
  - インシデント発覚から１ヶ月以内にインシデントが解決されない場合引き続き進捗を報告。インシデント解決後、最終報告を行う。

重大なインシデントとは

- **サービスの重大な運営障害**を引き起こしている
- 関連する施設に**金銭的損失**を与えている
- 他の自然人または法人に重大な**物質的または非物質的**な損害を与えている
- または、これらを引き起こす**可能性**がある場合

(3) サイバー衛生、トレーニング

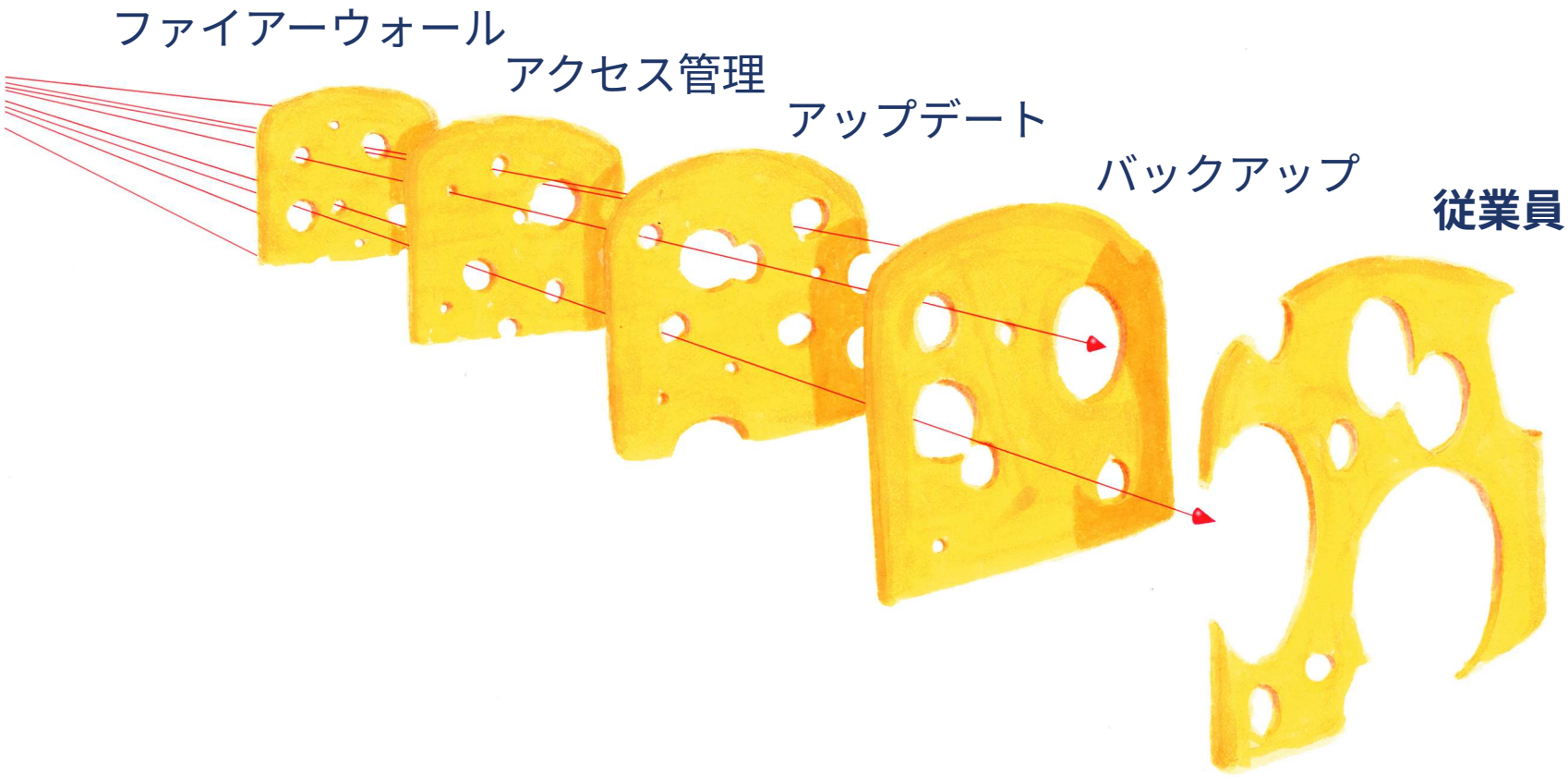
サイバー衛生

- ゼロトラストセキュリティ
- ネットワークのセグメント化
- アクセス管理
- アップデート
- デバイスの設定
- 強いパスワードの使用
- ダウンロード管理
- バックアップ
- 従業員トレーニング　等

従業員トレーニング

従業員はセキュリティ対策の**最後の砦**

従業員トレーニング

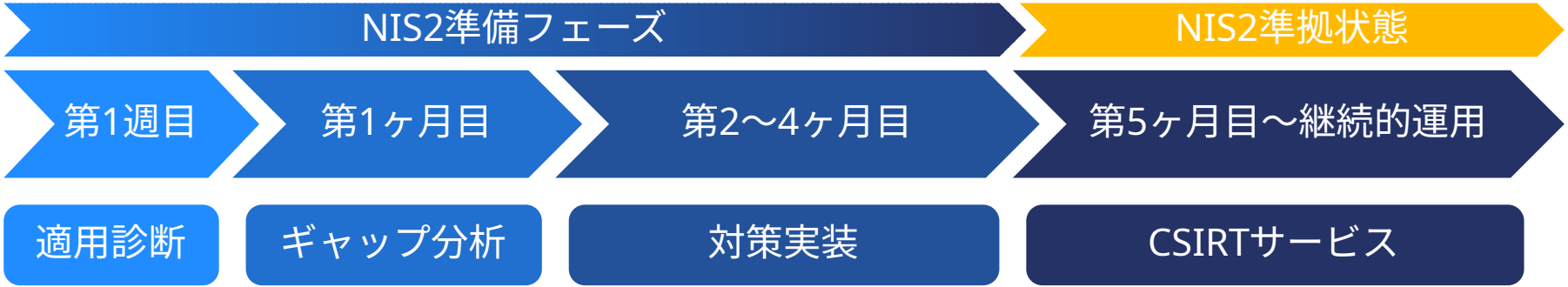


従業員トレーニング

- 経営責任者の義務
  - 年に一度トレーニング受講する義務
  - 従業員にトレーニングを受講させる義務

コンプライアンスまでの道のり

コンプライアンスまでの道のり



サービス一覧

お客さまの着実かつ確実な NIS2 対応のために、以下の 3 つのサービスで支援を行います。

	NIS2 適用対象簡易診断	NIS2 アセスメント	CSIRT サービス
概要	企業が NIS2 に該当するか、該当する場合は主要、重要のどちらのエンティティに該当するのかを明らかにします。 ● 質問数 13 項目 ● 所要時間 10 分 ● 無料	対応状況を NIS2 の要求事項と照らし合わせ、リスクの程度と実践すべき対策を明確にします。 ● 質問数約 200 項目 ● 回答の途中保存可能 ● 10 日以内のレポートお渡し ● サイバーセキュリティ専門家の推奨事項付き ● フォローアップミーティング	NIS2 対応を各 EU 拠点へ一貫して支援。 CSIRT が対策実装からインシデント対応まで丁寧にサポートします。 ● 対策実装サポート ● 技術的アドバイス ● 24 時間 365 日ホットライン ● 12 時間以内のレスポンス ● 各種テンプレートお渡し ● トレーニング実施

Enobyte
Data Protection

ご清聴ありがとうございました。

Enobyte GmbH
Augustenstraße 49
80333 München

sales@enobyte.com

enobyte.com