

最終段階影響アセスメント

タイトル：サイバーセキュリティ及びレジリエンス（ネットワークと情報システム）法案

措置の種類：基本法

担当省庁：科学技術革新省

影響評価番号：DSIT002(FIA)-25-DTI

RPC 参照番号：RPC-DSIT-25054-IA (1)

問い合わせ先：Kelly.North@dsit.gov.uk

日付：2025年11月12日

目次

1. 提案の概要	3
2. 提案規制の戦略的根拠.....	6
3. 介入の SMART 目標.....	8
4. 提案された介入選択肢の説明と、SMART 目標を達成する論理的变化プロセスの説明	23
5. 候補リストと代替案の概要.....	27
6. 選定された政策選択肢の説明.....	56
7. 社会的正味現在価値（NPSV）：各最終候補選択肢の金銭的・非金銭的成本と便益（行政負担を含む）	58
8. 便益	60
9. コスト	71
10. 広範な影響	93
11. 優先案の規制スコアカード	96
12. 優先案のモニタリングと評価	99
13. 優先案における行政コストとコンプライアンスコストの最小化	104
14. 宣言	105
附属書 A. 要約：分析と根拠	106

1. 提案の概要

サイバー脅威はより深刻化、頻発化、高度化しており、英国の企業や重要な公共サービスは敵対的なサイバー攻撃者の標的となるケースが増えている。政府は、我々に危害を加えようとする者から国家安全保障、経済、社会を防御するために必要な決定を下すことを明確にしている。サイバーセキュリティ・レジリエンス（ネットワークと情報システム）法案（以下「本法案」）は、英国のサイバー防衛を強化し、重要インフラを保護するとともに、これまで以上に多くの企業を、過度な負担をかけずに、コストのかかるサイバー攻撃からより良く守るものである。

本法案は、可能な限り国際的なパートナーと連携しつつ、英国のサイバーセキュリティ法規制を強化するための均衡のとれた措置を講じる。本法案は、1972年欧州共同体法に基づき欧州連合法から移行された、英国唯一のセクター横断型サイバーセキュリティ法規制である「2018年ネットワークと情報システム規則（NIS規則）」を更新するものである。NIS規則は、5つの分野（運輸、エネルギー、飲料水、医療、デジタルインフラ）における重要サービスと、一部のデジタルサービス（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、クラウドコンピューティング・サービス）を対象とする。これは、小売業など全ての分野やサービスが規則の対象外であることを意味する。現在、12の規制当局（「管轄当局」と呼ばれる）が規則の施行を担当している。

サイバー環境は絶えず変化しており、敵対的な主体は防御策を回避するため戦術を変えている。NIS規則は悪化するサイバー脅威の動向に追いついておらず、政府は現在、規則を迅速に更新する必要な権限を有していない。一方、EUはネットワークと情報システム指令第2次改正（NIS2）を通じてサイバー規制を更新しており、オーストラリアなどの他国もサイバーセキュリティ法を改正中である。これにより英国は国際的なパートナー国に後れを取っている。本法案は、英国が直面する特定のサイバーセキュリティ課題に対処すると同時に、適切な範囲でEUのNIS2指令のアプローチと整合性を図る。より多くの事業体を規制対象に含めることで英国規制を最新化し、規制当局にその責務を果たすための均衡のとれた権限を与え、政府に将来のNIS規則改正に必要な十分な権限を提供する。

本法案は、NIS規制の対象となるサービス種別を拡大し、より多くのサービスのサイバーレジリエンスを強化するとともに、現在サイバー犯罪者が悪用している隙間を埋めるものである。

- 本法案は、関連するマネージドサービス・プロバイダー（RMSP：他の組織に継続的な管理型ITサービスを提供する組織）¹、データセンター（スマートフォンで撮影した写真から患者の国民保健サービス（NHS）記録まで、英国で生成されるデータの多くを収容・処理する施設）、および大規模負荷制御装置（電力使用信号に対応し、機器に必要な電力供給を継続的に確保する装置）をNIS規制の対象範囲に組み入れる。これらの事業体は、それぞれ情報コミッショナー、科学技術革新省（DSIT）／通信規制庁（Ofcom）の共同、およびエネルギー規制庁（Ofgem）によって規制される。適用範囲に組み入れることで、サイバーリスク管理措置の実施と規制当局へのインシデント報告が義務付けられ、サイバー攻撃の影響からより効果的に保護されると同時に、悪意ある攻撃者にとっての標的としての魅力を低下させる。結果として、国民や企業が日常生活を送る上で依存するサービスの安全が確保される。
- 本法案は、重要サービス事業者（OES）及び関連デジタルサービスプロバイダ（RDSP）のサプライチェーンにおける脆弱性強化策を講じる。規制当局が「重要供給者」を指定しNIS規則の適用対象とすることで、潜在的な弱点を特定・強化する。これにより重要供給者へのサイバー攻撃から重要サービスを防御し、サービス利用者に影響が及ぶ事態を防ぐ。現行の中小零細エンタープライズ（SME）に対する包括的免除規定は改正され、サイバー攻撃の影響から供給網を保護する必要が生じた場合、規制当局が中小企業を「重要供給者」に指定できるようになる。

¹「関連マネージドサービス・プロバイダー」または「RMSP」とは、本影響評価において、本措置の対象となるMSPを指す。

本法案は、規制当局がコンプライアンスを推進し、その職務遂行に必要な資源と重要な情報確保を可能にすることで、より強固な規制環境を実現する。

- 本法案は、被害をもたらすサイバー攻撃の形態をより広く捕捉するための規準拡大、インシデント報告時間の更新、規制当局および英国に影響を与える重大なサイバーインシデントに対応する国家サイバーセキュリティセンター（NCSC）への報告の効率化により、インシデント報告を改善する。これにより、規制当局、NCSC、政府は規制遵守状況をより適切にアセスメントし、発生中のインシデントを早期に把握できるようになり、組織のインシデント対応を支援することが可能となる。時間の経過とともに、改善されたインシデント報告はサイバー環境の全体像をより明確にし、悪意ある行為者に対する防御体制を構築する。
- 本法案はまた、規制当局が公的機関と情報を共有できることを保証し、その逆も同様とする。これにより政府と規制当局は、サイバー脅威に対して効率的かつ効果的に対策を計画できるようになる。
- 本法案は、情報委員会（旧情報コミッショナー事務局、ICO）が規制対象のデジタルサービスにおけるサイバーリスクを事前に識別するため、情報提供を要求する既存の権限を拡大する。
- 本法案は、コスト回収制度をより包括的かつ柔軟に改善することで、規制コストを納税者に転嫁する必要性を低減し、規制当局がサイバーセキュリティ要件の遵守を効果的に推進・支援するための資源を充実させる。
- 本法案は NIS 規制の範囲を拡大し監督を強化するため、セクター間の整合性がますます重要となる。これにより国務大臣は「戦略的優先事項声明」を指定し、規制当局が達成すべき統一目標を設定するとともに、規制実施に対する期待値を明確化できる。
- 本法案は、規制当局が NIS 規則を執行する能力を向上させ、より効果的な制度を実現する。罰金の上限額が改正され、制度の重要性を反映して、適切な場合には現行よりも高額な罰金が科される可能性がある。これは類似の法令を考慮して策定された。さらに、罰則区分は公平性・明確性・実効性を高めるため簡素化され、罰金決定時には組織規模との均衡性や違反のパターンを含む、より包括的な事情が規制当局によって考慮される。

本法案は、規制対象事業体のサイバーセキュリティ基盤を強化し、NIS 規則が刻々と変化するサイバー環境に対応し続けられるようにするとともに、政府が国家安全保障を守るための断固たる措置を講じられるようにする。

- 新技術と新たな脅威には柔軟な規制が必要だ。規制が時代遅れになるのは時間の問題である。本法案は国務大臣に対し、二次立法を通じて NIS 規則を更新する比例的な権限を与える。これにより、NIS 規則が現在および将来の英国が直面する進化するサイバー脅威に対して効果を維持できる。
- 本法案により、政府は規制対象事業体に対する既存のセキュリティ要件を更新・強化し、NCSC の勧告や国際的なベストプラクティスとの整合性を高められる。また二次立法を通じてサプライチェーン義務を強化し、公共サービスがサプライチェーンの混乱からより良く防御されるようにする。
- さらに差し迫った脅威から守るため、本法案は国家安全保障上必要かつ均衡のとれた場合に、国務大臣が規制当局または規制対象事業体に対して指示を発する権限を付与する。これにより政府は国家安全保障にリスクをもたらすサイバー脅威に迅速に対応し、国民の利益と安全を守ることができる。

本法案の措置の大半は 2024 年国王演説で既に発表済みであるため、選択肢アセスメントには含まれていない。本法案で新たに追加された措置は、データセンター及び大規模負荷制御装置を適用対象に含めること、NIS 規則の執行メカニズムを強化すること、国家安全保障の利益のために国務大臣が戦略的優先事項声明を指定し指示を発出することを可能とすることである。政府は昨年、データセンターを適用対象に含めることについて協議を行い、2024 年 2 月に完

了した²⁾。また、データインフラ四半期フォーラムを含む業界との継続的な協議が行われている。政府は 2022 年 7 月、大量の電力負荷（合計 300MW 以上）を遠隔制御する全ての組織に対し、NIS 規則の規定遵守を義務付け、指定重要経済インフラ（OES）とみなす方針について協議した。³⁾ 2024 年 4 月の第 2 回協議では、これらの提案を基に、大規模負荷制御事業者向けサイバーセキュリティ保証枠組みの構築原則を提示した。⁴⁾ 両協議とも業界との継続的対話を通じ支持を集めた。執行メカニズム強化策については、NIS 実施後レビューで改善が必要と識別された分野であり、規制当局と緊密に連携して策定した。戦略的優先事項声明の指定権限に関しては、法案において国務大臣が規制当局と協議し、議会の承認を得た上で初めて声明を指定できることを明記している。

²⁾[協議：英国データインフラのセキュリティとレジリエンスの防御・強化](#)

³⁾[スマートで安全な電力システムの実現：エネルギー効率家電と遠隔負荷制御の相互運用性とサイバーセキュリティ - GOV.UK](#)

⁴⁾[スマートで安全な電力システムの実現：実施 - GOV.UK](#)

2. 提案規制の戦略的根拠

悪意あるサイバー攻撃者による重要サービス及びデジタルサービスへの脅威が増大している。サイバー攻撃は頻度と高度化が進み、犯罪者は新たな手法で防御を回避し、複雑化するサプライチェーンの脆弱な環を狙っている。同時に、国家支援を受けた攻撃者が英国企業・サービスを標的とした諜報活動や恐喝を増加させており、国家安全保障と生活様式を脅かしている。一方、英国唯一の分野横断的サイバー法である NIS 規制は時代遅れとなり、2025 年以降の英国が直面するサイバー脅威に対処するには不十分だ。2025 年 9 月までの 1 年間で、NCSC は 429 件のサイバーインシデントを管理し、うち 204 件は国家的に重大な影響を及ぼすものだった。つまり国家安全保障、経済安定、公共の安全に重大な影響を与えたのである。これは前年度の 89 件から急増した数値である。⁵ これらのインシデントのうち 18 件は「極めて重大」と分類され、前年度比 50% の増加を示した。公共サービスの混乱や経済成長を阻害する不安定なビジネス環境など、こうした攻撃の代償を払うのは一般市民である。

サイバーインシデントは英国の企業に年間数十億ポンドの損失をもたらしている。最近のサイバー攻撃ではジャガー・ランドローバー、マークス・アンド・スペンサー、ロイヤルメール、大英図書館などの組織が深刻な混乱に見舞われた。2015 年から 2019 年の間に、英国企業は資産損害、罰金、生産性低下を考慮すると約 870 億ポンドを失った。⁶ 昨年、43% の企業が過去 12 ヶ月間に何らかのサイバーセキュリティ侵害や攻撃を経験したと報告している。⁷ これは約 61 万 2000 社の英国企業に相当する。⁸ サイバー攻撃は企業に多大なコストを強いるだけでなく、事業拡大や成長を阻害する不安定な環境を生み出す。この不安定性は企業の競争力を損ない、英国の経済発展を妨げる。企業が繁栄できる安定かつ安全な環境を構築するには、強固でありながら均衡の取れたサイバー規制が必要だ。何もしないことの代償は大きすぎる。

技術への依存度が高まるにつれ、サプライチェーンは脆弱化している。ランサムウェアやデータ強要が重大な脅威として台頭しているのだ。こうした脆弱性は英国市民に現実的な影響をもたらしている。2024 年には、NHS の主要サプライヤーに対するランサムウェア攻撃により、11,000 件以上の急性外来予約と選択的手術が延期された。本法案の重要サプライヤー規制措置は、最も重要なサプライヤーのみを対象としており、企業に不必要な負担を課すことなく、サプライチェーンの脆弱性の高まる脅威に対抗することを目指している。

また、旧態依然とした規制は英国の国家安全保障をも脅かしている。同盟国への攻撃は、公共の安全と国家機能に不可欠な重要国家インフラ（CNI）を標的とする国家支援アクターによる深刻な脅威を浮き彫りにした。こうしたインシデントは、英国が防衛体制を近代化・レジリエンス化し、進化する課題に対応できる態勢を整える緊急性を示している。中国国家が支援する脅威アクターは既に米国の重要分野を標的にしている。例えば「ボルト・タイフーン」は中国に代わって活動するサイバー脅威であり、米国のエネルギー・運輸・水道分野を標的とし、将来の破壊的サイバー攻撃の基盤整備を進めている可能性がある。さらにロシアはウクライナ政府に対し破壊的攻撃を仕掛けている。例えば 2022 年 2 月、米衛星通信会社ビアサットに対するサイバー攻撃は、ロシアがウクライナへのさらなる侵攻を開始する約 1 時間前に始まった。これはウクライナ軍の作戦とコミュニケーションを麻痺させる試みであり、欧州にも波及して組織と市民の両方に影響を与えた。その後、ウクライナの重要インフラ、通信プロバイダ、政府事業体に対する破壊的・妨害的サイバー攻撃が続発し、電力網への攻撃も試みられた。本法案は、規制当局や政府が利用可能な情報を強化し、指示権限を通じて国家安全保障に対する重大な脅威に政府が迅速に対応できるようにすることで、長期的に英国がこうした脅威に対するレジリエンスを高めるものである。

⁵行動の時だ - NCSC 年次レビュー 2025

⁶Beaming, 'Five Years in Cyber Security', 2020

⁷サイバーセキュリティ侵害調査 2025 - GOV.UK

⁸同上

非立法措置は効果が認められないため、この分野では立法化が必要だと考える。問題の規模が大きすぎるため、企業と規制当局向けに明確に定められた最新の規制枠組みにより、保護策が迅速かつ一貫して実施されるようになる。過去 12 か月間、サイバーリスクを識別する活動を実施した企業はわずか 49%に留まる。これは、72%の企業がサイバーセキュリティを最優先課題と認識しているにもかかわらずである。また、取締役会レベルでサイバーセキュリティ責任者を配置している企業は 27%に過ぎない。⁹ これは、NCSC の「Cyber Aware」キャンペーンや「10 Steps」ガイダンス、Cyber Essentials など、企業のサイバー意識とセキュリティ向上に利用できる多様なツールが存在しているにもかかわらずの結果である。2025 年サイバーセキュリティ侵害調査で、10 ステップガイダンスやサイバーエッセンシャルズを認識していたのは、調査対象企業のわずか 12%、慈善団体の 15%に過ぎなかった。¹⁰ これは、ガイダンスや自主的措置だけではサイバー環境の安全確保が不十分であることを示している。

さらに、2022 年の NIS 規制実施後第 2 回レビュー（PIR）では、インシデント報告など複数の分野で規制が意図した効果を発揮していないことが判明した。¹¹ 2019 年、2020 年、2021 年に報告された NIS インシデントはそれぞれ 13 件、12 件、22 件に過ぎない。¹² これは重大インシデントの定義が狭すぎるためだ。報告不足は規制当局が指摘する問題だ。複数の重大なインシデントが報道される一方で、規制当局には重要な詳細が報告されていない。¹³ これにより規制当局は、重要な情報を活用して効果的な計画立案やガイダンス発行、事業者のサイバーレジリエンス強化支援を行う能力が制限される。NIS 規制の有効性を維持するには変更が必要だ。

介入がなければ、英国の重要サービス及びデジタルサービスはサイバー攻撃に対する脆弱性を継続し、それらに依存する市民や企業に現実的な影響を及ぼし続ける。企業や国民が日常的に依存するサービスは、通信や金融といった他の重要分野で既に実施されているような強固な保護の対象とすべきだ。これらの制度の成功事例から学び、重要サービス及びデジタルサービスのレジリエンスを確保するためにそれらを適用することが重要である。さらに、介入がなければ我々は国際的なパートナーに遅れを取る。EU は既に規制対象組織を拡大し、オーストラリアは重要サプライチェーンの指定を可能にする法改正を実施している。企業は英国での技術革新や投資を躊躇する可能性があり、これは政府の成長目標を阻害する。安定なくして成長はありえないのだ。

規制枠組みの更新は、基本法による改正によってのみ可能である。英国の EU 離脱に伴い、1972 年欧州共同体法は廃止され、新たな基本法なしでは枠組みを更新する適切な権限を我々はもはや有していない。

表 3.2 は、変更の戦略的根拠を施策ごとに列挙している。

⁹[サイバーセキュリティ侵害調査 2025](#)

¹⁰同上

¹¹DSIT、[ネットワークと情報システム規制 2018 の第二回年次報告書](#)（2022 年）

¹²同上

¹³スカイニュース、[「英国の運輸部門に対する 9 件のサイバー攻撃が義務的報告法で捕捉されず」](#)（2021 年）

3. 介入の SMART 目標

本法案は NIS 規則に重要な更新を加える。これらの更新は、重要デジタルサービスと英国国家安全保障を防御するため、英国のサイバー防衛を強化するという本質的な必要性和、短期的な企業コストを最小限に抑えることのバランスを取るものである。各措置の SMART 目標は表 3.2 に示されているが、英国のサイバーセキュリティとレジリエンス強化の背景には、いくつかの包括的な目標がある。

第一に、国民や企業が日常生活を妨げられることなく営めるよう、彼らが依存するサービスを防御することが極めて重要である。サイバー犯罪者はデジタルサービスや重要サービス、そのサプライチェーンを標的とするケースが増加しており、働く人々や企業の生活に混乱をもたらす、政府や経済に多大なコストを強いている。サイバー犯罪者は重要インフラ（CNI）への攻撃を増加させており、重要サービスとそのサプライチェーンを収益性の高い標的と見なしている。プライドウェル・コンサルティングが委託した独立報告書によれば、調査対象となった CNI の 86%が過去 12 ヶ月間にシステムへのサイバー攻撃を検知している。¹⁴ この 86%のうち、93%が過去 12 ヶ月間に少なくとも 1 回の攻撃成功を経験している。¹⁵ 法案の目的は、より多くの事業体を規制対象に含め、規制当局が責務をより適切に果たせるようにすることで、こうした脆弱性に対処することにある。これによりサイバー攻撃者の意欲を削ぎ、組織が標的となった場合の影響を最小限に抑える。具体的な目標は、NIS 法による規制対象事業体を増やし、サイバーセキュリティリスクの評価・軽減策を講じる事業体を増やすことだ。結果として、企業・重要サービス・エンドユーザーに対するサイバー攻撃の影響を低減できるはずである。

第二に、サイバーセキュリティは経済成長の重要な基盤である。安定なくして成長はありえない。サイバー攻撃は企業活動に混乱と多大な損害をもたらす。企業が標的とされる状況では、経営者が事業拡大や革新に消極的になるのは明らかだ。本法案は、対象範囲を拡大しデジタルサービスの基本セキュリティ要件を強化することで、経済全体にわたる企業活動に甚大な混乱をもたらすサイバー攻撃の発生確率と影響を低減することを目指す。これにより、壊滅的なサイバー攻撃を恐れることなく企業が活動できる、より安全で強固な環境が創出される。これは経済成長に不可欠である。したがって本法案の主要目的は、投資と革新が育まれる環境を促進するため、企業をサイバー攻撃から防御することにある。より多くの事業体を対象範囲に含め、規制当局がより効果的に職務を遂行できるようにすることで、サイバー攻撃に対する防御力を強化する。これにより、企業はサイバー攻撃への対応に要する時間を短縮でき、サービス停止を余儀なくされるケースを減らせる。攻撃が発生した場合、改善されたインシデント報告により、規制当局と NCSC は情報を活用して他の企業や組織に助言・指導を行い、連携を図れるようになる。これにより、各組織は自らを防御し、特定の攻撃や攻撃種別による広範な影響を緩和する措置を講じられる。ここでの測定可能な目標は、より多くのサイバー攻撃を防止すること、そしてインシデント発生時には、企業が対応する過程での混乱、コスト、ダウンタイムを削減することである。

第三に、サイバーセキュリティは英国の国家安全保障の防御にとって不可欠だ。NCSC の 2024 年度年次報告書は脅威状況を「拡散し危険な状態」と表現し、敵対国や組織犯罪による持続的な攻撃を指摘している。¹⁶ NCSC の 2025 年次報告書は、この脅威の激化を強調している。¹⁷ 法案の主要目的は、政府が比例原則に基づく権限を通じてサイバー脅威に断固として対処できるようにすることだ。英国の横断的なサイバーセキュリティ規制を強化するだけでなく、将来にわたって枠組みが停滞しないことを保証する。本法案はまた、国家安全保障に対する予期せぬ差し迫った脅威に対し、規制当局及び規制対象事業体に対して特定の行動を取るよう指示する権限を通じて適切に対応することを保証する。測定可能な目的は、政府が必要に応じて二次立法を通じて変更を加えられる比例的な委任権限を創設し、

¹⁴CNI サイバー報告書：リスクとレジリエンス（プライドウェル・コンサルティング委託）

¹⁵同上

¹⁶2024 年度年次レビュー

¹⁷行動の時だ - NCSC 年次レビュー 2025

将来的に一次立法の時間枠に縛られることなく、国家安全保障が脅かされる差し迫ったサイバー脅威に対応できるようにすることである。

介入の根拠

現行の規制体制は時代遅れであり、英国のサービス及び重要国家インフラ（CNI）にサイバー攻撃に対する脆弱性を残している。これにより個人と企業の双方に重大な影響が生じている。英国の現行サイバーセキュリティ体制の結果として、経済の異なる分野にまたがる 5 つの市場失敗が識別されている。

- a. **外部性**とは、財の生産や消費が取引外のサードパーティにコストや便益をもたらす現象である。サイバーセキュリティの便益は、セキュリティを実施する組織だけにとどまらない。個人や組織に対する各サイバー攻撃は、被害者へのコスト以外にも、消費者、商業顧客、サードパーティなどへの影響を及ぼすからだ。例えば、ユーザーの個人情報情報を漏洩させる攻撃はユーザーに悪影響を与え、攻撃を受けた組織（ ）はネットワーク復旧の全コストを負担せず、顧客に転嫁する可能性がある。個人やサードパーティ事業者は、あらゆる組織に対するサイバー攻撃のコストを負担せざるを得ない場合が多い。
- b. **公共財**は市場によって供給不足に陥るか、全く提供されない。サイバーセキュリティは以下のような場合に公共財の一形態となる：
 - **排除不能性**：安全なデジタルインフラの恩恵は、その安全性に直接貢献した個人に限定されない。組織や個人を含む全員が、個々の行動や財政的貢献に関わらず、より安全な環境の恩恵を受ける。
 - **非競争性**：ある事業者が安全なデジタルインフラを利用しても、他の事業者の利用可能性や品質は損なわれない。例えば安全なネットワークは、一部のユーザーが直接セキュリティ維持に関与していなくても、全てのユーザーにとって安全な状態を維持する。
- c. **情報非対称性**とは、取引において一方の当事者が他方よりも多くの情報を持つ状態を指す。サイバーセキュリティ分野では情報非対称性が非常に一般的であり、例えば組織は自社のサプライチェーン全体におけるサイバーセキュリティの強固さに関する情報を把握していないことが多い。
- d. **不完全情報**とは、企業が管理するサイバーリスクに関する情報が不完全な状態を指す。
- e. **調整失敗**とは、個人や企業がより望ましい結果から共同で利益を得られる可能性があるにもかかわらず、行動が調整されず、非効率的または最適でない結果を招く場合を指す。ネットワークとサプライチェーンは相互接続されているため、一方の失敗が広範な混乱を引き起こす可能性がある。以下の表は、英国のサイバーセキュリティ体制の特定部分に見られる具体的な市場の失敗を強調している。

表 3.1：サイバーセキュリティ体制における市場失敗の概要

市場	外部性	公共財	情報の非対称性	不完全情報	調整の失敗
対象範囲内の MSP	✓	✓	✓	✓	✓
対象となるデータセンター	✓	✓	✓	✓	✓
新規エネルギー必須サービスが対象範囲に含まれる	✓	✓	✓	✓	✓
規制当局が重要供給業者を指定できるようにする	✓	✓	✓	✓	✓
インシデント報告の改善			✓		✓
情報共有を強化する		✓	✓		✓

RDSP におけるリスク情報提供の義務				✓	
規制当局のコスト回収メカニズム	✓				
執行メカニズムを強化する		✓			✓
戦略的優先事項に関する声明		✓			✓
政府が将来的に NIS 規制の枠組みを 更新できるようにする	✓	✓	✓	✓	✓
セキュリティとレジリエンスに関する要件	✓			✓	
サプライチェーンの安全性を向上させる	✓	✓	✓		✓
国家安全保障のために必要かつ均衡 のとれた場合、国家安全保障担当大 臣が規制当局に指示する権限				✓	
国家安全保障のために必要かつ均衡 のとれた場合に、国務長官が規制対象 事業体を指示する権限				✓	

表 3.2 は、各施策ごとの SMART 目標、変更の戦略的根拠、および対応する市場失敗の詳細情報を示している。

表 3.2 : 変更の戦略的根拠、SMART 目標、および対策が対処する市場失敗

措置	変更の戦略的根拠	SMART 目標	対処する市場の失敗
NIS 規則を改正し、より多くの事業者、業種、サービスを適用範囲に含める。			
<p>関連するマネージドサービス・プロバイダー (RMSP) を NIS 規制の対象範囲に含める</p>	<p>MSP は我が国の重要インフラ (CNI) と経済に不可欠なデジタルサービスを提供する。顧客ネットワークへの広範かつ信頼されたアクセス権を持つため、サイバー攻撃の魅力的な標的となる。これらのネットワークにより、サイバー犯罪者はたった 1 つの MSP を攻撃するだけで、数百から数千もの組織を混乱させることが可能だ。</p> <p>RMSP を NIS 規制の対象範囲に含めることで、RMSP は現在対象となっている RDSP と同様のサイバーセキュリティ標準を維持することが義務付けられる。これによりサイバー攻撃者を抑止し、万が一インシデントが発生した場合の影響を最小限に抑えることができる。</p> <p>「オペレーション・クラウドホッパー」と呼ばれる戦術的キャンペーンで明らかになったように、MSP に対する持続的な攻撃は、サプライチェーン内の 1 つの MSP を攻撃するだけで、多くのエンドユーザーに重大な影響を与える可能性がある。¹⁸</p>	<p>管理サービスの侵害が当該事業者または顧客の事業に及ぼすリスクを低減するとともに、MSP が顧客システムを侵害する攻撃経路として悪用されるリスクを軽減する。これにより、英国の重要サービスや重要インフラ (CNI)、経済、社会全体への混乱を緩和できる。</p>	<p>外部性 – RMSP を規制対象に含めることで、政府は事業者が経済全体にわたる適切なレジリエンス対策を講じ、私的インセンティブと公共の利益を整合させられるようにする。規制は最低標準とリスク緩和を義務付けることで、サイバー攻撃が経済全体に及ぼす悪影響を軽減する。</p> <p>公共財 – さらに、広範なデジタルエコシステムに利益をもたらす基盤的保護を義務付けることで、公共財としてのサイバーセキュリティの供給不足に対処する。</p> <p>情報の非対称性 – RMSP を規制対象に含めることで、サプライチェーンで関わる関係者がサイバーセキュリティリスクに関する情報をより適切に把握できるようになる。</p> <p>不完全な情報 – RMSP を規制対象とすることで、政府は組織が自らのサイバーセキュリティリスクに関する知識を向上させることを保証する。</p> <p>調整の失敗 – MSP は重要サービスやデジタル供給網と深く相互接続されている。規制は調整を改善し、一貫した標準を設定し、ネットワーク全体でのリスクと情報の共有を可能にする。</p>

¹⁸オペレーション・クラウドホッパー、PwC (2021 年)。

措置	変更の戦略的根拠	SMART 目標	対処する市場の失敗
<p>2. データセンターインフラを NIS 規制の対象範囲に含める</p>	<p>データセンターは、デジタル生活に必要な技術とデータを収容し支える。これらは必須サービスを含むほぼ全ての経済活動を支えている。データセンターはまた、AI やその他の技術開発を含むイノベーションを支えている。その重要な役割を認められ、データセンターは 2024 年に CNI（重要国家インフラ）に指定された。しかし現在、他の CNI 公益事業や関連インフラとは異なり、直接規制されていない。これによりデータインフラはサイバー攻撃に対して脆弱性がある。データセンターインフラの混乱や侵害は、国民、企業、国家・経済安全保障に重大な悪影響を及ぼしうる。</p> <p>例えば、2022 年に Google と Oracle のデータセンターで発生した障害は、NHS（英国国民保健サービス）の大規模なデータ障害を引き起こした。</p>	<p>データセンターの機能停止や侵害リスクを低減するため、適切かつ均衡のとれたリスクマネジメント措置を整備する。これにより、対象事業者におけるセキュリティとレジリエンスのリスク緩和策の一貫性が強化され、他の重要サービスや CNI と同等の水準となる。第二に、データセンター事業者と当局間の情報流通を改善する。これにより規制当局と政府は業界の動向・リスク・トレンドを把握し、政策立案が可能となる。第三の目的は、安全な成長と投資のための基盤を提供することである。本規制の影響は業界の大半に比例して適用されるため、市場歪曲のリスクを最小化し、確信を持って成長と革新を図るための公平な競争環境を創出する。</p>	<p>外部性 - データセンターを正式に CNI と指定し直接規制へ移行することで、政府は対象事業者に経済全体にわたる適切なレジリエンス対策を講じさせ、私的インセンティブと公共の利益を整合させられる。規制は最低標準とリスク緩和を義務付けることで、サイバー攻撃が経済全体に及ぼす悪影響を軽減する。</p> <p>公共財としての役割 - さらに、広範なデジタルエコシステムに利益をもたらす基盤的保護を義務付けることで、公共財としてのサイバーセキュリティの供給不足にも対処する。</p> <p>情報の非対称性 -</p> <p>セキュリティとレジリエンスはデータセンターのビジネスモデルにおいて重要だ。競合他社の同様の公開情報が存在しない状況では、自ら脆弱性や障害を公表するインセンティブはほとんどない。データセンターを規制対象に含めることで、規制当局と政府は業界の可視性を得られる。規制対象化により、サプライチェーンの他の部分におけるデータセンター関連のサイバーセキュリティリスクへの認識が向上する。</p> <p>不完全な情報 - データセンターを規制対象に含めることで、政府は組織が自らのサイバーセキュリティリスクに関する知識を向上させることを保証する。</p> <p>調整の失敗 - データセンターは重要サービスやデジタルサプライチェーンと深く相互接続されている。規制は調整を改善し、一貫した標準を設定し、ネットワーク全体でのリスク共有と情報共有を可能にする。</p>

措置	変更の戦略的根拠	SMART 目標	対処する市場の失敗
<p>3. 電力分野における新たなエネルギー重要サービス（負荷制御）を NIS 規制の対象範囲に追加する</p>	<p>負荷制御は、電力使用信号に対応することで、商業・産業・家庭環境における消費者家電（エネルギースマート家電）を遠隔操作する技術である。大規模負荷制御事業者は、合計 300MW 以上の電気負荷を制御し、エネルギースマート家電との間で負荷制御信号を送受信する組織を指す。急成長するスマート柔軟性サービス市場において重要な役割を担うにもかかわらず、これらの制御事業者には現在、サイバーセキュリティ要件が欠如している。これは重大なリスクをもたらす。大規模負荷制御事業者へのサイバー攻撃は深刻な混乱や停電を引き起こす可能性があるからだ。こうした攻撃は消費者の信頼を損ない、スマートで柔軟なエネルギーソリューションの導入を阻害し、ひいては英国の「グリーンパワー 2030」及び「ネットゼロ」目標に影響を及ぼす。さらに、電力系統への広範な混乱は重大な経済的・社会的影響を招き、より広範な英国政府の目標にも悪影響を与える恐れがある。</p> <p>事例研究：エネルギーシステムへのサイバー攻撃は停電、経済的損失、国家安全保障上の脅威を引き起こしうる。</p> <p>例えば、2021 年に米国で発生したコロナル・パイプライン攻撃は、米国東部全域の燃料供給を混乱させた。エネルギー市場への混乱の影響は、2025 年 3 月のヒースロー空港変圧器火災の際にも見られた。</p>	<p>大規模負荷制御装置にサイバーセキュリティ要件を課すことで、広域電力網への障害リスクを低減する。これにより、重要インフラ（CNI）や他の必須サービスと同様に重大な影響を及ぼし得るこれらの組織を同列に扱う。当該組織はサイバーセキュリティ標準を満たし、規制当局（Ofgem）への報告が義務付けられる。これにより、増大する脅威環境に対するセクターのレジリエンスが保証され、規制当局及び英国政府がセクターのリスクや動向を把握できるため、情報に基づいた政策立案が可能となる。この分野のサイバーセキュリティ強化は、スマートエネルギー分野の成長と投資を促進し、政府のグリーンエネルギー目標を推進すると同時に、英国エネルギーシステムの信頼性に対する確信を維持する。これにより持続可能なエネルギー実践の導入が加速される。</p>	<p>外部性 – 大規模負荷制御事業者を規制対象に含めることで、政府はこれらの組織が経済全体にわたる適切なレジリエンス対策を講じ、私的インセンティブと公共の利益を一致させられるようにする。規制は最低標準とリスク緩和を義務付けることで、サイバー攻撃が経済全体に及ぼす悪影響を軽減する。</p> <p>公共財 – 適切な規制がなければ、市場参加者はスマートエネルギーへの投資を怠る可能性がある。なぜなら、安全でレジリエントな送電網がもたらす社会的便益の全てを享受できないからだ。大規模負荷制御事業者に対するサイバーセキュリティ基準と規制を導入することで、政府は安全で信頼性の高い送電網がもたらす社会的価値が実現されることを保証する。</p> <p>セキュリティ標準と規制を導入することで、政府は安全で信頼性の高い電力網の社会的価値が実現されることを保証する。</p> <p>情報非対称性 – 明確なサイバーセキュリティ要件を実施し、リスクや脆弱性に関する情報共有を促進することで、政府はこの情報の非対称性を是正し、全ての関係者がリスクを理解し適切な行動を取ることを保証できる。これにより信頼が強化され、ネットゼロ目標達成に必要なスマートで柔軟なエネルギーソリューションの導入が加速される。</p> <p>不完全な情報 – 大規模負荷制御装置を規制対象に含めることで、政府は組織が自社のサイバーセキ</p>

措置	変更の戦略的根拠	SMART 目標	対処する市場の失敗
			<p>ユリテイルスクに関する認識を向上させることを保証する。</p> <p>調整の失敗 - 大規模負荷制御装置はサプライチェーンと深く結びついている。規制は調整を改善し、一貫した標準を設定し、ネットワーク全体でのリスクと情報共有を促進する。</p>
<p>4. 規制当局による重要供給業者の指定を可能にする</p>	<p>サプライチェーンの脆弱性は、重要サービスやデジタルサービスの供給業者に対するサイバー攻撃、あるいはそのネットワークと情報システムの侵害は、大規模な混乱やデータ漏洩を引き起こし、経済的レジリエンスや国家安全保障を脅かす可能性がある。</p> <p>例えば 2024 年 6 月、NHS のサプライヤーである Synnovis がランサムウェア攻撃を受け、11,000 件の外来予約と選択的手術が延期され、緊急の献血要請が発生した。これはサプライチェーンへのサイバー攻撃が労働者に与える現実的な影響を実証した事例である。</p>	<p>当該分野における過度な依存、依存関係、または集中化によってサードパーティがもたらす、重要サービス及び主要デジタルサービスの提供に対するリスクを効果的に管理するためである。本措置は、特定サプライヤーを指定する枠組みを確立する。当該組織が重要サービスまたはデジタルサービスのプロバイダに物品またはサービスを提供する場合、当該供給のためにネットワークと情報システムに依存しており、かつ当該供給業者のネットワークと情報システムに影響を及ぼすインシデントが発生した場合、それらに依存する重要サービスまたはデジタルサービス（あるいは重要サービス・デジタルサービス全般）に混乱が生じ、その混乱が英国全体またはその一部における経済または社会の日常的な機能に重大な影響を及ぼす可能性が高い場合を指す。指定サプライヤーは、リスクの一貫した効果的な管理を確保するため、比例原則に基づく義務を負うことになる（ただし、これらの要件は二次立法で導入される）。この対象を絞ったアプローチにより、主要サプライヤーの可視性が向上し、セクター横断的なリスク対応の一貫性が確保され、経済成長、国家安全保障、経済的回復力に関する英国の戦略的優先事項に沿った国家のレジリエンスが強化される。これは、セクター横断的な脆弱性に対処し、新たな脅威により効果的に対応するための戦略的ツールを提供するものである。</p>	<p>外部性 - これらの供給者を対象範囲に含めることで、政府は民間組織が経済全体にわたる適切なレジリエンス対策を講じ、私的インセンティブと公共の利益を整合させられるようにする。規制は最低標準とリスク緩和を要求することで、サイバー攻撃が経済全体に及ぼす負の影響を軽減する。</p> <p>公共財 - 重要供給業者への適用範囲拡大は、企業と個人の防衛・福祉に必要な公共インフラとサービスの保護強化につながる。</p> <p>不完全な情報 - 重要サプライヤーを規制対象に含めることで、政府は組織が自らのサイバーセキュリティリスクに関する認識を向上させることを保証する。</p> <p>情報の非対称性 - 指定サプライヤーを規制対象に含めることで、規制当局と政府はこれらの重要組織に対する可視性を高められる。規制対象化により、サプライチェーンの他の部分も、これらのサプライヤーに関連するサイバーセキュリティリスクへの認識が向上する。</p> <p>調整の失敗 - 指定サプライヤーは、NIS 規制対象セクター内の主要組織と深く結びついている。これらのサプライヤーを規制することで、調整が改善され、一</p>

措置	変更の戦略的根拠	SMART 目標	対処する市場の失敗
			貫した標準が設定され、ネットワーク全体でのリスクと情報の共有が促進される。
規制当局がコンプライアンスを推進し、その職務を遂行するために必要な資源と重要な情報を確保できるようにする			
5. インシデント報告の改善	<p>効果的なインシデント報告は、規制当局が自部門全体への即時影響を把握し、セキュリティ要件の遵守状況を監視するために不可欠である。これにより、NCSC による迅速な支援・サポートの促進、政府全体の脅威状況への理解深化、（透明性通知を通じて）依存するサービスが中断された場合や自システム侵害の媒介として悪用された場合に、ユーザーが緩和措置を講じることが可能となる。2019 年、2020 年、2021 年に報告された NIS インシデントは、それぞれ 13 件、12 件、22 件に過ぎない。¹⁹ によると、昨年サイバー侵害を経験したと報告した企業は 43% に上り、英国で重大な影響を与え得る多くのインシデントが報告されていないことが明らかである。²⁰ 現行の報告基準値では報告がなされない事例が存在する問題は、規制当局と、NIS 規則に基づき規制当局には報告されなかったが報道機関には報じられた複数の注目すべきインシデントの両方によって指摘されている。²¹ 本法案は報告対象となるインシデントの範囲を比例的に拡大し、事業者に過度の負担をかけないよう配慮する。また現行の 72 時間報告要件に内在するリスクに対処するため、</p>	<p>規制当局への報告対象インシデントの拡大と発生中のインシデントの早期通知を通じて、インシデント・セクターへの影響・規制遵守に関する包括的かつ即時的な理解を支援する。第二に、インシデント報告を NCSC と迅速に共有することで、インシデント管理に必要な支援を適時に提供することを促進する。第三に、インシデント報告後の透明性通知発行を通じて、影響を受けた事業者の顧客が適切な緩和措置を講じられるようにする。</p>	<p>情報非対称性 – 主要関係者（規制当局、NCSC、企業）は、進化するサイバー脅威に関するリアルタイムまたは完全なデータを欠いている可能性がある。インシデント報告が規制当局と NCSC に同時に提供されることで、正確かつ最新の情報を迅速に共有でき、規制当局が脅威を監視し、タイムリーに支援を提供できるようになる。</p> <p>調整の失敗 – これはまた、効果的な意思決定、規制監督、そして全体的なサイバーセキュリティのレジリエンスを妨げる調整上の問題を修正するものである。</p>

¹⁹ DSIT、[ネットワークと情報システム規制 2018 の第二回 PIR](#)（2022 年）

²⁰ [サイバーセキュリティ侵害調査 2025 - GOV.UK](#)

²¹ スカイニュース「[英国の運輸部門に対する 9 件のサイバー攻撃が義務的報告法で捕捉されず](#)」（2021 年）

措置	変更の戦略的根拠	SMART 目標	対処する市場の失敗
	<p>初期通知の迅速化を義務付ける。さらにインシデント発生時の利用者通知義務化という規制上の空白を解消する。</p> <p>例えば 2023 年、ランサムウェア攻撃者がファイル転送プラットフォーム「MoveIt」の脆弱性を悪用し、英国企業や米国エネルギー省に影響を与えた。これは 2018 年 NIS 規則では報告対象外であった。</p>		
<p>6. 情報共有規定の強化。例えば、規制当局が特定の目的で相互に、また公的機関と情報を共有できるようにすること、その逆も同様とする。</p>	<p>NIS に基づく情報共有規制は、制度が効果的に機能することを保証するのに役立つ。</p> <p>効果的に機能することを保証する。NIS 規制の実施に関わる組織間で情報を共有するための明確な経路と、その情報の使用に関する適切な保護措置が存在する事が極めて重要である。しかし、現行の情報共有規定は、規制当局が情報を NIS 規則の実施に関わる事業者間で共有するための明確なゲートウェイと、その情報の使用方法に関する適切な保護措置が存在することが極めて重要である。しかし、現行の情報共有規定では、規制当局が英国の公的機関（DSIT を含む）と情報を共有するための明確なゲートウェイが規定されておらず、その逆も同様である。</p>	<p>NIS 規則に基づく情報共有規定を強化・拡大し、これにより、規制当局の機能遂行を支援し、国家安全保障・重要インフラ・サイバーレジリエンスに関する政府政策立案に情報を提供するとともに、NIS 枠組みとその実施の効果的な評価を可能とする。</p>	<p>公共財 - サイバーセキュリティに関する情報の共有は公共財である。なぜなら、ある事業者が情報共有から利益を得ても他の事業者の利益を妨げず、ある事業者が情報を利用しても他の事業者の情報利用能力を損なわないからだ（適切な保護措置を前提とする）。したがって、介入がなければ情報共有は供給不足に陥り、NIS 規制体制の 効果に影響を及ぼす可能性がある。</p> <p>情報の非対称性 - これらの変更は、規制当局と公的機関間の現行データ共有の有効性を向上させ、脅威への対応におけるより効果的な連携を可能にする。変更によりデータ共有の取り決めにおける確実性が向上する。</p> <p>調整の失敗 - これは、効果的な意思決定、規制監督、およびサイバーセキュリティの全体的なレジリエンスを妨げる可能性のある調整上の問題を修正するのに役立つ。</p>
<p>7. 情報委員会がリスクに関連する適切な情報を確保すること</p>	<p>法案の措置が発効すると、推定 2,000 の組織が情報委員会の規制対象となる。情報委員会は、リスクを考慮して、これらの規制対象事業者それぞれに対する適切な監督レベル</p>	<p>情報委員規制対象事業者からリスクアセスメントに関連する情報を確実に受け取るため、RDSP（登録データ処理事業者）に対するより柔軟で積極的な監督体制の導入を支援する。本法案の権</p>	<p>不完全な情報 - 現在、自主的なデータ提出に依存する態勢は不十分であり、リスクアセスメントと監督に不備が生じている。本法案により明確なデータ共</p>

措置	変更の戦略的根拠	SMART 目標	対処する市場の失敗
	<p>を決定することが求められる。これを効果的に行うため、情報委員会は十分なデータを必要とする。これにより、規制対象のデジタルサービス／管理サービスがもたらす広範なリスクを評価できる。情報委員会が現在行っているように、この情報に関する個別の自発的要請に依存するだけでは、全てのデータ収集には不十分である。</p> <p>委員会は、規制対象のデジタルサービス／管理サービスがもたらす広範なリスクを評価するための十分なデータが必要となる。情報委員会が現在行っているように、個別の自発的な情報提供依頼に依存するだけでは、情報委員会の規制対象事業体全体からデータを収集し、関連するリスクを評価するには不十分である。</p> <p>例えば、MSP を介した、あるいは MSP が関与した攻撃により、国防省の給与システムや英国政府資産 (FCDO/HMT) が影響を受けた事例がある。MSP が政府機関を顧客に抱えているかどうかを把握することで、情報委員会は適切な執行手段をより効果的に講じることができる。</p>	<p>限により、RDSP および RMSP (登録管理サービス事業者) は情報委員会に対しリスクベースの情報を提供する一般的な義務を負い、必要に応じてその情報を更新することが可能となる。これにより、英国の重要サービス、重要国家インフラ (CNI) 、および広範な経済への混乱を軽減することが期待される。</p>	<p>有メカニズムを確立することで、情報委員会は規制対象事業体全体にわたる包括的な情報を受け取ることが可能となり、リスクアセスメント能力と適切な監督実施能力が向上する。</p>
<p>8. 規制当局のコスト回収メカニズムの改善</p>	<p>英国の重要サービスがレジリエンスを保つためには、組織が適切なサイバーセキュリティ水準を達成・維持できるよう支援できる、より十分な資源を備えた規制当局の存在が不可欠だ。現在、規制当局は NIS 規則の監督・執行に伴う全コストを回収する能力、及びその回収方法 (手数料ではなく直接請求による) において制約を受けている。これは規制体制の有効性を損なうリスクがあるだけでなく、規制当局が公的資金に依存する場合、コストが納税者に転嫁される恐れがある。</p>	<p>第一に、規制当局がコスト回収方法の制約を軽減し、その責務と機能を十分に遂行できるようにすることで、規制体制の有効性とセキュリティ・レジリエンス要件への全体的な順守を強化する。第二に、サイバーリスクを生み出す組織にそのリスク規制に関連するコストを負担させることで、コスト配分を公平化し、納税者と公的資金への負担を最小化する。第三に、直接請求に加え、手数料ベースのコスト回収方法を可能とすることで、規制対象事業体と規制当局に明確性と予測可能性を提供する。</p>	<p>外部性 - これによりサイバーセキュリティ規制の提供がより持続可能かつ効率的となり、規制コストを納税者に転嫁する必要性を減らすことで公衆に利益をもたらす。</p>

措置	変更の戦略的根拠	SMART 目標	対処する市場の失敗
<p>9. 戦略的優先事項の声明を指定する権限を国務大臣に付与する</p>	<p>NIS 規則は複数の異なる分野に適用され、現在 12 の異なる規制当局によって施行されている。これまでのところ、NIS 規則の実施と成果は一貫していないと評価される。これにより、一部の NIS 分野は他の分野に比べて敵対的活動や混乱に対して比較的脆弱性のある状態にある。</p> <p>例えば、戦略的優先事項の声明により、規制当局は NIS 規則の執行においてリスクベースのアプローチを追求するよう求められる可能性がある。これにより、全ての規制当局がリスクが最も顕著な分野に資源を集中させることが保証される。</p>	<p>NIS 規則が業種を問わず一貫して効果的に適用されるよう、本措置により国務大臣は規制当局が達成を目指す成果を設定できる。本措置の成功は、規制当局がこれらの成果に向けて講じる措置と、規制当局が機能を果たす際の一貫性によって測定される。国務大臣は年次報告書を公表し、戦略的優先事項声明における成果達成に向け規制当局が講じた措置を明示する。規制当局は本報告書作成支援のため、DSIT の要請に応じて情報提供を義務付けられる。規制当局から提供された情報に基づく国務大臣の報告書により、本措置の成果評価が可能となる。</p>	<p>調整の失敗 - この措置により、規制当局／セクター間のアプローチの一貫性が向上する。全てが同一の成果に向けて取り組むことが求められるためである。</p> <p>公共の利益 - 異なるセクター間で NIS 規則の施行・実施が不統一であったため、特定のセクターではサイバーレジリエンスという公共の利益が他より著しく不足する状況が生じていた。本措置により、サイバーレジリエンスはより均等に分配される公共の利益となり、攻撃者に悪用される可能性のある隙間は最小限に抑えられる。これにより、より安全で公平な環境が促進され、サイバーセキュリティの集会的利益が全セクターで共有され、脆弱性が低減され、広範な社会的リスクが軽減される。すべてのセクターに共有されるより安全で公平な環境を促進し、脆弱性を減らし、より広範な社会的リスクを緩和する。</p>
<p>10. NIS 規則における執行メカニズムの強化</p>	<p>効果的な規制体制には、違反を抑制し、事業者が義務を履行するよう促すための制裁枠組みが不可欠である。規制当局によれば、NIS 規則に基づく執行は、罰則体系が不明確であること、および全 NIS 分野における違反を抑制するには不十分な最高罰金額によって制約を受けている。違反から生じる重大なリスクを考慮すれば、規制の成功と重要インフラのレジリエンスを確保するため、執行体制の改善が極めて重要である。</p>	<p>規制当局が、違反行為に対して効果的かつ比例的で予測可能な執行措置を講じられるようにするためである。</p> <p>成功は、コンプライアンスの向上と違反抑止に与える効果によって測定される。</p> <p>措置は既存の判例に沿って策定され、NIS 制度に関連する要素を考慮する。その運用は国務大臣が定期的に見直し、有効性と比例性の両方を維持することを保証する。</p>	<p>公共の利益 - 執行体制の有効性向上は、NIS セクター全体における非遵守を抑制し、国家安全保障とレジリエンスの保護に不可欠である。</p> <p>調整の失敗 - 罰則帯域構造が不明確であるため、規制当局間で執行措置に一貫性がなく、効果的な規制執行を妨げている。</p>
<p>NIS 規則が絶えず変化するサイバー環境に対応し、政府が国家安全保障を防御するための断固たる措置を講じられるよう確保する</p>			

措置	変更の戦略的根拠	SMART 目標	対処する市場の失敗
<p>11. 政府が将来的に NIS 規制枠組みを更新するための委任権限</p>	<p>英国の EU 離脱と 1972 年欧州共同体法の廃止により、政府は NIS 規則を改正する適切な権限を失った。これにより、我が国のサイバーセキュリティ法制度は、広範なサイバー環境における新たな脅威や動向に対応できなくなっている。これは最終的に、英国経済と社会が依存するサービスのサイバーレジリエンスにリスクをもたらす。</p> <p>例えば、政府は特定の分野におけるサイバーリスク低減に必要であるという確固たる証拠がある場合、NIS 規則の適用対象に新たな分野を追加したいと考えるかもしれない。この権限が存在していれば、政府は国民や企業が依存するデータセンターを、より早期に適用対象に含めることができたはずだ。</p>	<p>政府がタイムリーに対応し、英国経済が依存する適切なサービスを確実にカバーするよう NIS 規則を変更できることを保証するため、また規制対象事業者と規制当局の双方が、これらのサービスに対するリスクマネジメントに必要な能力と自信を備えることを保証するためである。本法案は、対象となる規制対象事業者が規則の要件を満たすことを支援するため、明確なガイドラインと優良事例を定めた実践規範を国務大臣が公表することを認めている。</p>	<p>不完全な情報 – 政府に NIS 規則を更新する権限を与えることで、集团的レジリエンスを確保し、情報の流れを改善し、枠組みの有効性、比例性、対応力を維持する。</p> <p>外部性 – NIS 規制を更新する権限を持つことで、政府は引き続き関連組織が経済全体にわたる適切なレジリエンス対策を取るよう確保し、私的インセンティブと公共の利益を整合させられる。規制は最低基準とリスク軽減を要求することで、サイ</p> <p>規制を更新する権限を持つことで、政府は関連組織が経済全体にわたる適切なレジリエンス対策を継続的に講じ、私的インセンティブと公共の利益を整合させることで、サイバー攻撃が経済全体に及ぼす悪影響を軽減する。</p> <p>公共財 – NIS 規則を更新する権限を持つことで、政府は関連組織に対するサイバーセキュリティ標準と規制が将来にわたって目的に適合するよう継続的に確保できる。</p> <p>情報の非対称性 – NIS 規制を更新し、サイバーセキュリティ要件とリスク・脆弱性に関する情報共有の継続を確保することで、政府は将来にわたる情報の非対称性を是正できる。</p> <p>不完全な情報 – NIS 規制を更新することで、政府は組織が将来にわたって自らのサイバーセキュリティリスクに関する知識を向上させることを保証する。</p>

措置	変更の戦略的根拠	SMART 目標	対処する市場の失敗
			<p>調整の失敗 – 組織はサプライチェーンを通じて相互接続性を高め続けている（）。最新の規制を維持することで調整が改善され、一貫した標準が設定され、ネットワーク全体でのリスクと情報の共有が促進される。</p>
<p>12. セキュリティとレジリエンス要件</p>	<p>デジタルサービスを提供する事業者や企業に対するセキュリティ要件は、比例的かつ適切であることが極めて重要だ。既存のセキュリティ要件は時代遅れで、NCSC の推奨水準を下回っており、十分なリスク緩和を提供できない可能性が高い。したがって更新が必要だ。OES には「リスク管理のための比例的な技術的・組織的措置」を講じる広範な義務があるものの、より詳細なセキュリティ要件は現在 RDSP にのみ適用されている。これらを更新または適用範囲を拡大する仕組みは存在しない。本法案により、リスク管理のための比例的な技術的・組織的措置を設定する二次立法が可能となる。</p> <p>「リスクマネジメントのための比例的な技術的・組織的措置」を講じる広範な義務を負っているが、より詳細なセキュリティ要件は現在 RDSP にのみ適用されている。これらを更新したり適用範囲を拡大したりする仕組みは存在しない。本法案により、二次立法を通じてセキュリティ要件を設定し、現在の脅威や脆弱性に対応できるようになる。同時に、将来さらに脅威が識別され更新が必要となった場合に、政府が柔軟に要件を引き上げられるようになる。</p> <p>例えば EU は NIS 2 を更新し、対象セクターの範囲を拡大するとともに、規制対象事業者が満たすべき追加的なセキュリティ要件を導入できた。この権限により英国も同様の対応が可能となる。</p>	<p>特定された脅威レベルに見合ったセキュリティ要件を国務大臣が設定する権限を確保し、これらを一貫して適用できるようにするためである。</p>	<p>外部性 – より優れたセキュリティ要件は、組織がサイバー侵害を含むセキュリティ・レジリエンスリスクの影響を軽減・最小化する最善の準備を整えることを保証する。私的インセンティブと公共の利益を整合させる。規制は最低標準とリスク緩和を要求することで、サイバー攻撃が経済全体に及ぼす負の影響を低減する。</p> <p>不完全な情報 – 付随法令を通じてセキュリティ要件の設定・更新を可能にすることで、本法案は標準が現在のリスクと整合性を保つことを保証する。これにより規制対象事業者は期待される内容に関するより明確な指針を得られ、不確実性が低減され、実際の脆弱性に応じた投資が可能となる。また透明性が向上し、企業・規制当局・公衆間の情報格差が縮小されるため、より情報に基づいた意思決定と、全体としてより安全なデジタル市場が実現する。</p>

措置	変更の戦略的根拠	SMART 目標	対処する市場の失敗
<p>13. 政府によるサプライチェーンの安全強化を可能にする</p>	<p>サプライチェーンの脆弱性は、重要サービスやデジタルサービスにとって重大なリスクである。重要サービスやデジタルサービスの供給業者に対するサイバー攻撃、あるいはそのネットワークと情報システムの侵害は、重大な混乱やデータ漏洩を引き起こし、経済的レジリエンスや国家安全保障を脅かす可能性がある。重要サービス事業者は NIS 枠組みの下で義務を負っているが、サプライチェーンリスクを効果的に管理するための明確性や能力が不十分である。したがって、体系的なサイバーリスクを低減し、重要分野・サービスのレジリエンスを強化するためには、サプライチェーン全体のセキュリティ向上が不可欠である。</p> <p>事例研究：2020年12月、ネットワーク管理ソフトウェア企業 SolarWinds がハッキングされ、複数の政府機関や民間企業に広範な侵害が発生した。影響を受けた顧客と企業は合計 18,000 に上った。</p>	<p>重要なデジタルサービスを防御するためのより良い実践を促進するため、事業者に必要なサプライヤーから生じるリスクを管理する義務を組み込む。介入策は、明確な説明責任を組み込み、サプライヤーリスクガバナンスを改善することで、サプライチェーン関連のサイバーインシデント発生の可能性と影響を低減する。目的には、安全で回復力のある調達慣行の普及促進、サードパーティリスクに対する監視と透明性の向上、サプライヤー障害による混乱の発生件数と深刻度の低減が含まれる。これらの成果は、規制当局との連携強化、セクター全体の準備態勢向上を支え、英国の経済成長、国家安全保障、経済的回復力に関する戦略的優先事項と整合する。</p>	<p>外部性 - サプライチェーンの脆弱性は、個々の企業だけでなく個人や広範な経済にも影響を及ぼすコストを生み出す。セキュリティ強化はこうしたコストを内部化させ、広範なシステムリスクを低減する。</p> <p>公共財 - サプライチェーンのセキュリティは、関与する事業者だけでなく経済全体の利益となる。義務的なサイバーセキュリティ対策はこの公共財の提供を保証し、国家と経済のレジリエンスを高める。</p> <p>情報の非対称性 - 企業はサプライチェーンリスクを認識できず、不適切な判断を招く可能性がある。本法案によるリスクマネジメントの改善と明確なガイドラインは情報格差を解消し、より良いセキュリティ計画を可能にする。</p> <p>調整の失敗 - サプライチェーンは相互に接続されており、一つの失敗が広範な混乱を引き起こす可能性がある。この措置は調整と情報共有の改善を可能にし、ネットワーク効果を是正し、システム全体のレジリエンスを高める。</p>
<p>14. 国家安全保障上必要と判断した場合、国務大臣が規制当局に指示する権限を導入する</p>	<p>地政学的・技術的進展により、規制対象事業者のネットワークやシステムに対する脅威が急激に高まる可能性がある。政府には、各セクターが脅威増大に対応し厳格なセキュリティ対策を導入することを保証する権限がない。これは規制当局が実施するのに最も適した分野だが、国家安全保障を脅かす予期せぬ状況下で規制当局に措置を要求する政府の権限は不十分である。</p>	<p>国家安全保障上必要となる場合、脅威情勢の急変に対し規制当局が迅速に対応できるよう、規制対象事業者への規制要件を調整する。これにより NIS 規制対象事業者は緊張が高まった時期に悪意あるサイバー活動からより効果的に防御され、サービスへの混乱レベルが低減される。本政策の成功は、規制当局が指示に応じて実施する措置の有効性と、その措置がサイバー攻撃による混乱をどの程度抑制したかで評価される。</p>	<p>不完全な情報 - 脅威が高まった際に規制当局が各セクターに対し、より強力なセキュリティ対策の採用を促すよう政府に権限を与えることで、この措置は不完全な情報に対処する。規制当局が、そうでなければ入手できないかもしれない重要な情報に基づいて行動することを保証し、システム全体のレジリエンスを強化する。</p>

措置	変更の戦略的根拠	SMART 目標	対処する市場の失敗
	<p>例えば、国際紛争などにより英国が直面する脅威環境全体が悪化した場合、国務大臣はこの権限を行使できる。</p>		
<p>15. 国家安全保障上必要と判断される場合、情報通信大臣が規制対象事業体に指示する権限を導入する</p>	<p>現在、政府は国家安全保障の保護に不可欠と判断される場合であっても、規制対象事業体に重要インフラサイバー脅威への対応を指示する権限を有していない。高度な能力を持つ主体や敵対国による脅威の増大は、この欠陥がより頻繁に、より大きな影響をもって悪用され、重要インフラの運用にリスクをもたらす可能性があることを意味する。</p> <p>例えば、政府が重要サービス事業者のネットワーク上で発生したサイバーインシデントを把握した場合、そのインシデントがサービスの提供を妨害し、国家安全保障上の脅威を構成する程度に達する可能性がある場合、国務大臣はこの権限を行使できる。</p>	<p>規制対象事業体が、自社のネットワークと情報システムに対する脅威（国家安全保障リスクを伴うもの）に迅速に対応することを確認するためである。これらの権限の有効性は、組織が指示に従ったか否か、及び（指示で要求された）脅威対処措置の有効性を評価することで測定される。また、権限の存在自体が、指示発出前に組織が自主的に国家安全保障上の脅威に対処する行動を取るよう促すことも期待される。</p>	<p>不完全な情報 – 政府が国家安全保障上の脅威に対応するため、対象事業体に特定の措置を講じるよう指示することを可能にすることで、この措置は、事業体が認識していない可能性のある脅威に対処することを要求することにより、不完全な情報に対処するものである。</p>

4. 提案される介入選択肢の説明と、SMART 目標を達成する論理的変更プロセスの説明

優先案 – NIS 規則を改正し将来対応型とする。提案措置は以下の通り：

1. RMSP を NIS 規則の適用範囲に含め、情報コミッショナー事務局による規制対象とする。
2. 1MW 以上の容量を有するデータセンター及び 10MW 以上の容量を有するエンタープライズデータセンターを NIS 規則の適用範囲に含め、Ofcom と DSIT が共同規制機関として規制する。
3. 電力分野において負荷制御を必須サービスとして導入し、大規模負荷制御事業者（潜在的な総負荷が 300MW 以上の事業者）を NIS 規制の対象範囲に含め、Ofgem による規制を受けるようにする。
4. 規制当局が特定の高影響度供給業者を「指定重要供給業者」として識別・指定できるようにし、OES や RDSP と同等の義務を課す。
5. インシデント報告規準の拡大、報告時間の更新、NCSC との情報共有方法の効率化、RDSP・新規規制対象となる RMSP・データセンターに対する透明性要件の強化により、インシデント報告を改善する。
6. 情報共有規定を強化する。例えば、規制当局が公的機関と情報を共有するための明確なゲートウェイを提供し、その逆も同様とする。
7. 二次立法における RDSP の義務を拡大し、情報委員会への情報提供を義務付ける。これにより、情報委員会は RDSP 及び適用範囲に組み込まれる RMSP のリスク評価において、より積極的なアプローチを取ることが可能となる。
8. 柔軟なコスト回収メカニズムを通じて、NIS 関連機能の全コストを回収可能とすることで、コスト回収を改善する。
9. 国務長官に戦略的優先事項声明を指定する権限を付与し、規制当局が達成を目指す統一的な目標体系を提供する。
10. NIS 規則の執行メカニズムを強化するため、最高罰則額の上限を改正し、段階構造を簡素化する。これにより効果的かつ均衡のとれた制度を実現し、コンプライアンスの向上を図る。
11. 国務大臣に、将来的に規制枠組みを更新する権限を付与する。具体的には、NIS 規制の対象となる適切な業種・サブ業種を確保すること、NIS 規制の実施方法の改善、あるいは効果を維持するための義務・責任の変更などを行う。
12. 国務大臣が二次立法を通じてセキュリティ及びレジリエンス要件を更新できるようにする。
13. 政府が二次立法により、重要経済サービス事業者（OES）及び重要デジタルサービス事業者（RDSP）に対してより強力なサプライチェーン義務を設定できるようにする。
14. 国家安全保障上必要かつ均衡のとれた場合に限り、国務大臣が規制対象事業体に対し脅威やインシデントへの対応措置を指示する権限を付与する。
15. 国家安全保障上必要かつ均衡のとれた場合に、国務大臣が規制当局に対し行動を指示する権限を付与する。

表 4.1 : 法案の変革理論

政策	目的	投入要素	活動	前提条件	成果	成果
データセンターを適用範囲に含める	データセンターの障害や侵害リスクを低減する	NIS 規則の対象範囲にデータセンターを含める	データセンターは、法令で定められた関連義務を満たす。これには、特定の情報の通知と提供、リスクマネジメントのための適切かつ均衡のとれた措置の実施、重大なインシデントの報告が含まれる。	NIS 規則の対象となることで、これらの企業のサイバーセキュリティが向上すると想定される。NIS 実施後レビューで実証済み。	データセンターのサイバーセキュリティとレジリエンスの向上	公共サービスと企業を防御し、市民が日常生活を送れるようにする
関連するマネージドサービス・プロバイダー (RMSP) を適用範囲に含める	侵害された RMSP がエンドビジネスを含む対象に及ぼすリスクを低減する	NIS 規則の対象となる RMSP	RMSP はデジタルサービスプロバイダと同等の義務を負う		RMSP のサイバーセキュリティとレジリエンスの向上	
大規模負荷制御装置を適用範囲に含める	大規模負荷制御装置の障害や侵害リスクを低減する	NIS の対象となる大規模負荷制御装置規制	大規模負荷制御装置は、関連法規で定められた義務を満たす必要がある。具体的には、特定の情報の通知と提供、リスクマネジメントのための適切かつ均衡のとれた措置の実施、重大なインシデントの報告などが含まれる。		大規模負荷制御装置のサイバーセキュリティとレジリエンスの向上	
重要供給業者の指定	重要供給者を規制の対象範囲に含めることで、重要供給者が重要インフラシステム (OES) 及び重要通信システム (RDSP) に及ぼすリスクを低減する	規制当局が最も重要な供給業者を NIS 規制の対象範囲に含めることを可能にする	規制当局は最も重要な供給者を指定でき、これは小規模・零細 DSP にも適用される。重要依存関係は、中核的なセキュリティ要件とインシデント報告義務の対象範囲に含まれる。		サプライチェーンリスクの監視強化	
戦略的優先事項の説明	全セクターにわたり、サイバーセキュリティ 規制のための明確かつ一貫性のある枠組みを提供する	戦略的優先事項に関する声明を公表する権限を SoS に付与する	戦略的優先事項に関する声明を公表し、規制当局と協議の上、3 年から 5 年ごとに更新する。優先事項に関連する規制当局の活動に関する年次報告書を公表する。		一貫した目標設定が規制のより効果的な実施につながるという前提。	

情報共有	NIS 制度の効果的な機能を実現するため、情報共有を改善する。	情報共有の窓口を強化・拡大する	規制当局は政府を含む公的機関と情報を共有でき、その逆も同様である。	情報共有の強化が NIS 制度の機能向上につながるという前提。	NIS 実施に関わる事業者間の情報共有のための明確なゲートウェイと、情報の利用方法に関する強化された保護措置	安定した環境を構築する
インシデント報告	規制当局と NCSC がインシデントや新たなリスクに対処するための基盤を強化する	現行の報告要件を更新・強化する。	インシデント報告規準の拡大、報告期限の更新、報告手続きの簡素化、規制対象のデジタルサービス、マネージドサービス、データセンターを提供する事業者に対する透明性要件の強化。	NIS 規則の下で報告対象となるインシデントが増加し、現在これらのインシデントが報告されていないと想定される。	規制当局と NCSC は脅威の状況をより包括的に把握できる	
情報収集	情報委員会のサイバーリスクを積極的に識別・対処する能力を向上させる	情報委員会に対し、最重要企業を識別するための追加情報を提供する	RDSP および RMSP に対し、登録時およびその後の情報通知を通じて、情報委員会にリスクベースの情報を提供するプロバイダとしての義務を課す。	より積極的なアプローチがサイバーリスクの識別と緩和に役立つという前提。	情報委員会はサイバーリスクを識別・緩和するため、積極的なアプローチを取る	
コスト回収	規制当局が柔軟なコスト回収メカニズムの下で全ての義務を遂行できるようにする	コスト回収制度の抜本的見直し	規制当局が手数料制度の設定、コストの回収、またはこれらを組み合わせたプロセスにより、執行を含む規制の経費を賄えるようにする。	財政的制約は規制当局の有効性を阻害する障壁と見なされる。	規制当局は職務を効果的に遂行する資源を有している	
執行改革	より効果的かつ比例的な執行を通じて順守を促進する	規制当局が売上高の%に基づくより高い上限罰金を科すことを可能にする。	規制当局は、意味があり比例した罰則を調整して発動する。規制対象事業者は、コンプライアンス違反の誘因が減り、事業コストとして罰金を吸収する意欲が低下する。	効果的な制裁制度は、比例性を持ち、確実に適用され、迅速に運用できるものであることが前提であり、これによりコンプライアンスが向上すると考えられる。	NIS へのコンプライアンス強化	
		罰則帯域構造を簡素化する。	規制当局は、より透明性が高く、予測可能で一貫性のある方法で罰則を科す。		規制当局による執行手段のより一貫した適用	
					制裁の透明性と予測可能性を高めること	

政府が将来的に NIS を更新できるようにする	規制枠組みが新たな脅威に 適応可能であることを確保 する	国家安全保障担当 大臣に規制枠組み を更新する権限を 与えること	政府は、適切な協議を経て、規制対象事業体 に対して新たな要件や義務を導入し、適切かつ均衡 のとれたと判断される場合には、新規分野・サブ分 野を規制対象範囲に組み入れることができる。	これらの権限により、立法 が変化するサイバー環境 に適応できるという前提。	法令が関連性と有効性を 維持する	英国の国家安全保障 を強化し、脅威環 境の変化の中で規 制が効果を維持す ることを確保する
セキュリティとレジリエンス 要件	企業がベストプラクティスに従 うための明確な原則と目標 を確立する	規制における既存 要件を更新する権 限を国務長官に付 与する	政府は、適切かつ均衡のとれた範囲で、RDSP (登録データ保管サービスプロバイダー) に適用さ れるセキュリティ要件を規制により設定し、RDSP を 超えて拡大することができる			
指示権限	政府が国家安全保障上の リスクを伴うインシデントや脅 威に迅速に対応できるよ うにする	国務長官が規制対 象事業体に指示を 発出する権限を付 与する	国家安全保障上の理由により、特定のサイバーイ ンシデントまたは脅威に関連して規制対象事業体 に指示が発出される	指示発出権限により、政 府が国家安全保障上の 脅威から英国を防御す るため迅速かつ断固たる対 応が可能となるという前 提。	規制対象事業体は、国 家安全保障に重大なリス クをもたらす脅威やインシ デントに迅速に対処する。 リスクが高まった時期に は、各セクターがより厳格 な安全対策を講じる	
	リスクが高まった時期に、業 界全体のレジリエンスを高め る	国務長官が規制当 局に措置を指示す る権限を付与する	規制当局は指示を受け、脅威情勢の悪化に対応 して業界全体で取られる行動を支援する形で、自 らの機能を行行使するよう求められる。			

5. 候補リストと代替案の概要

本節では、法案の各措置について検討された政策選択枝のロングリストを提示する。これらのロングリスト選択枝は、「重要成功要因」(CSF)を用いて体系的に分析された。CSFとは、提案が目的を成功裏に達成するために必須の属性である。各改革を評価するために使用されたCSFのセットは下記の通り：

- **戦略的適合性** – 政策は我々の目標を満たしているか？英国政府及び国際的な他の取り組みと調和しているか？
- **有効性** – 選択枝は問題解決に効果的か？具体的には、各選択枝は以下の規準のうち少なくとも一つを満たす必要がある（全ての選択枝が三つ全てに該当するわけではない）：
 - 国民が依存し、経済安定と国家安全保障の基盤となる最重要国家インフラの防御に不可欠な事業体が、適切に対象範囲に含まれているか（他の国内法で既にカバーされていない場合）
 - ネットワークと情報システム規制に関する規制当局の職務遂行能力を向上させるか？
 - 絶えず変化するサイバー環境において、規制自体が適切であることを確実にするか？
- **実現可能性** – すべての関連ステークホルダーにとって、その選択枝は現実的に達成可能かつ均衡が取れているか？

NIS 規制の対象範囲に追加する事業体に関する措置

5.1 関連するマネージドサービス・プロバイダー（RMSP）を NIS 規制の対象範囲に含めるための措置

政策選択枝	戦略的適合性	有効性 - 国民が依存し、経済安定と国家安全保障の基盤となる最重要国家インフラの防御に不可欠な事業体が、適切に対象範囲に含まれているか？	有効性 - ネットワークと情報システム規制に関する規制当局の職務遂行能力を向上させるか？	有効性 - 絶えず変化するサイバー環境において、NIS 規制自体が適切であることを確実にするか？	実現可能性
選択枝 1 - 何もしない	低	低	該当なし	低	高
選択枝 2 - ガイダンス	低	低	該当なし	低	高
選択枝 3 - 顧客への認知度	低	低い	該当なし	低	中
選択枝 4 - 中小企業を除く MSP を対象範囲に含める	高	高	該当なし	高	高
選択枝 5 - すべての MSP を対象範囲に含める	低	高	該当なし	中	中

選択肢 1：何もしない

何もしないことは、現在の市場失敗に対処する上で効果的ではなく、最も適切かつ社会的・経済的に重要な分野が重要なサイバーセキュリティ規制の対象となることを保証しない。ひいては、NIS 規制を時代遅れにし、絶えず変化する状況に適さないものとする。公的機関も民間組織も、重要な内部業務サービスを提供するために MSP への依存度を高めている。MSP のサイバーセキュリティとレジリエンス、および彼らが提供するサービスの質は、サービスを受ける組織の事業継続にとってしばしば決定的に重要である。MSP は顧客の IT システム、ネットワーク、インフラ、データに前例のないアクセス権を持つ。このため、悪意ある攻撃者にとって魅力的な標的となり、サイバー攻撃に対して脆弱である。これには MSP に対する Cloud Hopper 攻撃や国防省人事システムへの攻撃が含まれる。これらは MSP の脆弱性、ひいては彼らが支える重要サービスの脆弱性を浮き彫りにしている。MSP は現在、NIS 規則の下で直接規制されていない。したがって、MSP にとって「何もしない」選択肢はあり得るが、英国政府が彼らを現状のまま放置することは不可能だ。つまり、ネットワークと情報システムのセキュリティリスクマネジメントを義務付けず、サイバーインシデントを規制当局に報告させる義務も課さない状態を継続することはできない。NCSC が発行した最低限のセキュリティ標準に関する自主的ガイドラインは存在するが、これは強制力を持たない。つまり多くの MSP が対応を取っていない。最近の攻撃の頻発と自主的対策の遅れた普及は、規制措置が必要であることを示している。

選択肢 2：MSP 向け自主的サイバー標準・指針の利用促進

この選択肢は英国政府にとって実現可能である。NCSC は既に、MSP がサイバーセキュリティとレジリエンスを強化するために利用できる世界水準の自主的ガイダンスを幅広くプロバイドしている。これには NCSC とオーストラリア、カナダ、米国のサイバーセキュリティ当局が共同で発表した「サイバーセキュリティアドバイザリー」が含まれる。²² また「Cyber Essentials」のような自主的サイバー標準や製品も MSP が利用可能だが、これらは義務ではない。

しかしながら、MSP による本ガイダンスの採用実績や一貫した適用事例が確認されていないため、この選択肢は効果的でないと考えられる。政府は、自主的なガイダンスやサイバー標準だけでは、MSP の広範な利用に伴う特定のセキュリティリスクに対処するには不十分であると認識している。さらに言えば、これにより NIS 規則は時代遅れとなり、MSP への依存度が高まるデジタル環境の変化に対応できなくなる。結果として、この分野が適切な保護の対象外となる空白が生じ、多くの重要デジタルサービス事業者がリスクに晒されることになる。EU が NIS 2 により MSP を規制対象に含める中、この分野で立法化しないことは国際的な先例との戦略的整合性に欠ける。結果として、この選択肢は最終候補評価に進められなかった。

選択肢 3：MSP 顧客向け啓発・教育の推進

代替案として、MSP の顧客を対象とした教育・啓発キャンペーンを展開する選択肢がある。キャンペーンでは、マネージドサービスの購入者に対し、MSP に関連するリスクの理解促進や、独自のセキュリティニーズに沿った調達判断の方法を指導・教育することに焦点を当てられる。需要側にサイバーセキュリティへの関心を高めるよう働きかけることで、市場の行動変容を促す可能性がある。この選択肢は英国政府、MSP、およびその関係者にとって実行可能だが、教育プログラムの開発とキャンペーンの実施には多大なリソースを要する。さらに、適切なセクターをサイバー規制の対象範囲に含めることを保証する効果はなく、市場の失敗を解決する効果もない。結果として、多くの事業者や重要・デジタルサービスが依存する重要セクターが適切な保護の対象外となる空白が残される。ひいては、NIS 規制が時代遅れとなり、変化し続ける状況に適応できなくなる。この政策選択肢を 2021 年の意見募集で検証した際、回答者のわずか 31%が「MSP 向けサイバーセキュリティ・レジリエンスの将来枠組み導入促進に非常に効果的」と回答した²³。完全に効果的と答えたのは 1%に過ぎなかった。政府は、過去のキャンペーンやガイダンスの普及率が低かったことから、このアセスメントに同意している。例えば、Cyber

²²[サイバーセキュリティ勧告](#)

²³[図 7 サプライチェーンのサイバーセキュリティに関する意見募集への政府の対応 - GOV.UK](#)

Aware キャンペーンを知っていた企業はわずか 24%、10 Steps ガイダンスや Cyber Essentials を知っていた企業は 12%に過ぎなかった。²⁴

したがって、この選択肢は最終候補リストに進められなかった。

選択肢 4：法案により、大規模・中規模プロバイダが提供する全てのマネージドサービスを NIS 規制の対象範囲に含める。規制当局により重要供給業者に指定されない限り、小規模・零細企業は免除される（推奨選択肢）

この介入は前述の市場失敗に対処するのに効果的である。MSP は現在 NIS 規制の下で直接規制されておらず、従ってネットワークと情報システムのセキュリティ標準確保やサイバーインシデント報告が義務付けられていない。この介入は重要分野をサイバーセキュリティ法規制の対象範囲に組み込む上で効果的である。これにより、RMSP（リセラー型 MSP）は、自社のサービスが依存する関連ネットワークと情報システムへのリスクを管理する効果的な措置の実施、および関連インシデントの報告を法的に義務付けられる。情報コミッショナー事務局は、最も重要なサービスを提供する小規模・零細組織を含め、コンプライアンスを評価し必要に応じて介入できるようになる。英国政府にとってこの選択肢は実現可能である。英国 MSP 市場への理解が十分であり、本法案がこの変更を実現する規制手段を提供するからだ。脆弱性が最も高い MSP を対象とする比例原則を確保するため、小規模・零細 MSP は免除される。ただし、法案の戦略的目標に沿い、重大な脆弱性低減に重要と認められる場合、重要供給者として指定される例外がある。このアプローチは比例原則に合致し、EU の対応とも整合する。適切な場面では国際的な整合性という戦略的適合性を満たすものである。

2022 年に実施された英国のサイバーレジリエンス強化案に関する協議では、デジタルサービスプロバイダ（DSP）に関する提案が圧倒的に好意的な評価を得た。²⁵ 回答者の 84%が DSP 規制拡大策を支持し、79%が DSP 監督体制改正策を支持した。さらに回答者の過半数（70%）は、少数の重要プロバイダを NIS 規則の適用対象に含めるため、免除規定を修正すべきとの見解を示した。²⁶

この選択肢は、効果的で実現可能性が高く、戦略的適合性が強いと見込まれるため、最終候補評価に進められた。また、2024 年の国王演説における一連の措置の一部として発表された。

選択肢 5：小規模・零細企業を含む全てのマネージドサービスを NIS 規制の対象範囲に組み入れる

概して、サイバーリスクによる外部影響が最も大きい企業は、NIS 規制の対象となる中堅・大企業である。これらは顧客数が最も多い企業だからだ。中小・零細 MSP がプロバイダとして提供する全てのサービスを規制するのは不均衡である。多くの場合、深刻な脆弱性を生じさせないからだ。したがって DSIT は、現行の RDSPs における小規模・零細企業向け免除措置を維持し、情報委員会やその他の規制当局が重要供給者と判断した場合に限り適用対象とする方針である。これにより法案が経済・社会的に最も重要な分野に適切な防御を提供できるよう確保する。よって本案は最終候補選定プロセスに進まない。

重要成功要因に基づくロングリスト案の検討の結果、ショートリストに進める唯一の現実的な選択肢として、選択肢 4 と「現状維持」案が識別された。したがって、本措置における優先案は選択肢 4 である。

5.2 データセンターを NIS 規制の対象範囲に含めるための措置

政策選択肢	戦略的適合性	有効性 - 国民が依存し、経済安定と国家安全保障の基盤となる最重要国	有効性 - ネットワークと情報システム規制に関する規制当局の職	有効性 - 絶えず変化するサイバー環境において、NIS 規制自体が適	実現可能性

²⁴ サイバーセキュリティ侵害調査 2025 - GOV.UK

²⁵ 英国のサイバーレジリエンス強化提案に関する意見募集への政府回答 - GOV.UK

²⁶ 同上

		家インフラの防御に不可欠な事業者が、適切に対象範囲に含まれているか？	務遂行能力を向上させるか？	切であることを確実にするか？	
選択肢 1 - 何もしない	低	低	該当なし	低	高
選択肢 2 - デフォルトの進路	低	低	該当なし	低	高
選択肢 3 - 1MW/10MW のデータセンターを対象範囲に含める	高	高	該当なし	高	中
選択肢 4 - 0.5MW/5M W のデータセンターを適用範囲に含める	中	中	該当なし	中	低
選択肢 5 - すべてのデータセンターを対象範囲に含める	中	中	該当なし	中	低

選択肢 1：何もしない

何もしない場合、データインフラは NIS 規則の適用範囲外となる。このアプローチはデータセンター運営者に対する直近の規制負担を回避し、追加のコンプライアンスコストや管理要件なしに事業を継続できる。データセンターにとっては実行可能な方法ではあるが、重要なサイバーセキュリティ規制の適用対象として適切な事業者やサービスを確実に包含する効果はない。ひいては、データセンターが私たちのデジタル生活（ ）においてますます依存されるようになる変化し続ける状況において、NIS 規則は時代遅れで不適切なものとなる。これによりデータセンターは魅力的な脅威の媒介となる。何もしないことは、データセンターに関連する脆弱性とリスクが対処されないことを意味し、サイバー脅威に対して脆弱な状態を放置することになる。データセンターは、国民が依存するサービスの日常的な運営を含む、ほぼ全ての経済活動を支えている。データセンターインフラの混乱や侵害は、国民、企業、国家・経済安全保障に重大な悪影響を及ぼしうる。例えば、2022 年の Google と Oracle のデータセンター障害が NHS（国民保健サービス）の大規模なデータ障害を引き起こした事例がこれに該当する。

選択肢 2：デフォルトの進路（商業的緩和策、自主的措置、段階的な部分的規制）

法案により、多くのデータセンターが特定セクターとして指定されずとも NIS 規制の対象範囲に含まれる可能性が高い。これはデータセンターが多くの重要サービスや重要インフラ（CNI）のサプライチェーンにおいて不可欠な部分であり、規制当局が重要供給者を指定する措置（措置 5.4）の下で対象範囲に組み込まれる可能性があるためだ。これにより一部のデータセンター施設・サービス及びそれらに依存する顧客に対して、有益なセキュリティ・レジリエンス保護が導入される。しかし、適切なデータセンター全てが重要なサイバーセキュリティ規制の対象となるよう確保する上で、不一致で非効率な規制による脆弱性が残る可能性が高い。さらに言えば、デジタル生活においてデータセンターへの依存度が高まる中、NIS 規則は時代遅れで非効率なまま放置されることになる。DSIT は、NCSC/国家保護保安庁による共同ガイダンスの発行や標

準引き上げの奨励といった自主的措置を通じて、業界のリスク緩和を図ることができる。この選択肢はデータセンターにとって実現可能だが、自主標準の採用にもかかわらず、業界全体での標準の不統一や脆弱性の継続発生といった意図せぬ結果を招く可能性が高い。データセンターは公衆が依存するサービスの日常運営を含むほぼ全ての経済活動を支えているため、この選択肢は我々の目的を達成できず、結果として最終候補評価に進められなかった。

選択肢 3：1MW 以上の容量を有するデータセンター及び 10MW 以上の容量を有するエンタープライズデータセンターを NIS 規則の規制対象に指定する（推奨選択肢）

NIS 規則に基づき、1MW 以上の容量を有する（非企業向け）データセンター及び 10MW 以上の容量を有するエンタープライズ向けデータセンターを指定することで、これらの施設を規制枠組みに組み込み、特定のセキュリティ及びレジリエンス標準への準拠を確保する。

サービス	定義	推奨閾値	根拠
データセンター	複数の組織にサービスを提供する	1MW 以上	これにより、規制枠組みがサードパーティデータセンターの大半を網羅しつつ、最小規模の施設のみを除外し、オフィス内のサーバーームなどの対象化を防ぐ。この閾値により、英国のデータセンターの約 81%が対象範囲に入り、既知の 224 サイト中 182 サイトをカバーする。
エンタープライズデータセンター	自社組織へのサービス提供を唯一の目的とする	10MW 以上	1MW で対象となるサードパーティデータセンターとは異なり、エンタープライズデータセンターは単一組織の内部 IT ニーズのみに対応し、多くの場合厳格な内部ガバナンスの対象となる。より高い閾値を設定することで、国家のレジリエンスと安全保障に最も重大な影響を及ぼす可能性のある、最大かつ最も重要なエンタープライズ施設のみを対象範囲に含めることが保証される。

この優先アプローチにより、市場の約 81%が NIS 規制の対象となる一方で、小規模事業者は依然として過大なコンプライアンスコストを負担することなく事業を継続できる。したがって、政府の目的達成に効果的であると同時に、の主要関係者にとって実現可能な選択肢を提供する。さらに、閾値を下回る規模で運営されるデータセンターが重大なリスクとみなされる場合、重要供給者として指定され、NIS 規制の対象となる可能性がある（措置 5.4 に基づく）。

この措置は、データセンターが攻撃による混乱の可能性から脅威ベクトルとしてますます注目される現状を踏まえ、重要なサイバーセキュリティ規制の対象範囲を適切に設定し、現在のサイバー脅威を反映させる上で有効である。重要データ及びインフラの保護を強化し、サイバー攻撃やその他のセキュリティインシデントのリスクを低減する。一部のデータセンター事業者には追加のコンプライアンスコストと管理要件が生じるが、このアプローチは事業者にとって比例原則に合致し実現可能であると確信している。このアプローチは比例原則に合致し、EU の対応とも整合性がある。適切な場面では国際的な整合性という戦略的適合性も満たす。セキュリティとレジリエンスの向上による利益は、実現可能性に伴う欠点を上回る。したがって、データセンターのセキュリティ強化において本案が最推奨選択肢となる。第 1 回データインフラフォーラム（2024 年 10 月）及びフォローアップワークショップにおける業界代表者との協議では、本アプローチへの広範な支持と合意が確認された。代表者らは、本規制が業界に規制の確実性と安定性をもたらし、「公平な競争環境」を確立することで大きな利益をもたらす点で一致した。

本案は、効果的かつ実現可能であり、戦略的整合性も高いと期待されるため、最終候補評価に進められた。また、2025年4月1日に公表された「サイバーセキュリティ・レジリエンス政策声明」の一環として政策が発表された。

選択肢 4：0.5MW 以上の容量を有するコロケーション・共同ホスティングデータセンター及び 5MW 以上の容量を有するエンタープライズデータセンターを NIS 規制の対象として指定する

NIS 規則に基づき、0.5MW 以上の容量を有するデータセンター（非エンタープライズ向け）および 5MW 以上の容量を有する企業向けデータセンターを指定することで、これらの施設を規制枠組みに組み込み、特定のセキュリティおよびレジリエンス標準への準拠を確保する。

このアプローチにより、市場の約 91%が NIS 規制の対象となる。これにより、ごく小規模な事業者（合計 MW 容量 3MW）のみが規制遵守義務なしに事業を継続できる。ただし、多くの小規模サイトは依然として規制遵守の課題に直面する。

これは政府の目的達成に効果的な選択肢ではあるが、主要な利害関係者はこの措置が過度に厳格であると指摘している。閾値未満で稼働するデータセンターが重大なリスクとみなされる場合、依然として重要供給者として指定され、NIS 規則の適用対象となる可能性がある（措置 5.4 に基づく）。

この措置は、データセンターが攻撃による混乱の可能性から脅威ベクトルとしてますます注目される現状を踏まえ、重要なサイバーセキュリティ規制の対象範囲を適切に確保し、現在のサイバーセキュリティ脅威を反映する上で有効である。

重要データとインフラの保護を強化し、サイバー攻撃やその他のセキュリティインシデントのリスクを低減する。しかし、一部のデータセンター運営者には大幅な追加コンプライアンスコストと管理要件を課すことになり、このアプローチがこれらの運営者にとって比例原則に合致し実現可能であるとは確信できない。

このアプローチは EU の対応よりも強硬であり、戦略的リスクを全く有さない多くの施設を含む、英国のほぼ全てのデータセンターを対象とする。この選択肢は、オフィス内のサーバーールームなど、通常データセンターとは分類されない多数の小規模事業者も対象に含む可能性があるため、実現可能とは考えられない。また、イノベーションを促進する環境づくりによる経済成長という政府の広範な目標とも整合性が低い。中小企業に不必要かつ不均衡な負担を強いるため、最終候補評価には適さず、最終候補評価の対象とはならなかった。

選択肢 5：全てのデータセンターを指定

全てのデータセンターを NIS 規制対象に指定すれば、「公平な競争環境」が確立され、所有者・運営者が満たすべきサイバー標準について業界に明確な期待値を設定できる。この選択肢には、選択肢 3 で定めた NIS 規制の適用範囲基準を下回るものの、重要インフラ（CNI）に分類される可能性のある小規模データセンターも含まれる。この選択肢は、通常データセンターとは見なされない多数の小規模事業者（オフィス内のサーバーールームなど）を規制対象に含める可能性があるため、実現可能とは考えられない。また、イノベーションに適した環境整備による経済成長促進という政府の広範な目標との戦略的整合性が低い。中小企業にとって不必要かつ過大な負担となるため、最終候補リストへの選定には適さない。

これらのロングリスト案を重要成功要因と照らし合わせて検討した結果、選択肢 3 が「何もしない」案と共にショートリストに進める唯一の実現可能な案と識別された。したがって、本措置における優先案は選択肢 3 である。

5.3 大規模負荷制御装置を NIS 規制の対象範囲に含めるための措置

政策選択肢	戦略的適合性	有効性 - 国民が依存し経済安定を支える最重要国家インフラの防御に不可欠な事業者	有効性 - ネットワークと情報システム規制に関する規制当	有効性 - 絶えず変化するサイバー環境において、NIS 規制自体	実現可能性

		が規制対象に含まれることを適切に保証しているか？	局の職務遂行能力を向上させるか？	が適切であることを確実にするか？	
選択肢 1 - 何もしない	低	低	該当なし	低	高
選択肢 2 - 自主標準	中	低	該当なし	低	高
選択肢 3 - 300MW 以上を支配する LLC を対象範囲に含める	高	高	該当なし	高	中
選択肢 4 - 対象範囲内の全ての負荷制御装置を起動する	低	中	該当なし	中	低

選択肢 1：何もしない

何もしない場合、規制当局や大規模な負荷制御事業者にとって追加コストは発生しない。しかし、重要なサイバーセキュリティ規制の対象となるべき全セクターが確実にカバーされるわけではなく、成長市場における主要組織が規制対象外となり、結果として消費者を含め重大なサイバーリスクに晒されることになる。内部調査では、負荷制御事業者が電力システムに不可欠なサービスを提供しており、侵害された場合、システムレベルへの影響や地域的な停電を引き起こす可能性が指摘されている。規制枠組みがほとんど、あるいは全く整備されていない状況では、大規模な負荷制御組織の侵害は脅威アクターにとって魅力的な標的となり得る。エネルギー環境の変化とエネルギー分野全体での負荷制御装置の普及拡大を考慮すると、何もしないことは重大なサイバーセキュリティリスクと電力システム安定性のリスクをもたらす、NIS 規制に重大な抜け穴を残すことになる。この選択肢は関係するステークホルダーにとっては実行可能だが、政府の広範な目標との戦略的整合性は低い。

選択肢 2：自主的なサイバー標準の利用を促進する

政府は、Cyber Essentials などの自主的なサイバー標準の利用が負荷制御事業者からのリスク緩和に十分かどうかを検討した。この措置は規制当局にほとんどコストがかからず、企業への追加コストも任意であるため、英国政府にとって実行可能な選択肢となる。しかし、既存の自主的取り組みは技術的なサイバー要件を規定しているものの、NCSC の評価によれば、この市場から生じる潜在的なリスクを管理するために必要な、適切かつ一貫したサイバーレジリエンスの水準を促進する可能性は低い。さらに、この措置の任意性は業界全体でサイバー標準の適用状況や水準にばらつきを生じさせる可能性が高く、結果として効果を発揮せず、負荷制御事業者がエネルギー分野でますます重要な役割を担う変化し続ける状況において、NIS 規則を時代遅れのものにしてしまう。加えて、政府の目標や国際的な慣行、特に EU との整合性が戦略的に不十分である。したがって、この選択肢は最終候補評価に進めることはできない。

選択肢 3：大規模負荷制御事業者を NIS 規制の対象に指定する（推奨選択肢）

この選択肢は、負荷制御を既存の規制枠組みに統合することで、一貫性と均衡性を備えたアプローチを提供する。政府の戦略目標と国際慣行（特に EU）との強力な整合性を確保し、負荷制御市場における最重要事業者をサイバーセキュリティ法規制の対象範囲に組み込む。これにより、規制が進化する重要エネルギーサービスの性質と歩調を合わせ続けることが保証される。

負荷制御が電力システムの重要な構成要素となりつつある現状、特に脱炭素化・柔軟なエネルギーシステムにおいて、この選択肢は規制が技術進歩とそれに伴うサイバーリスクの変化に追随することを保証する。この選択肢では、大規模な負荷制御事業者がサイバー攻撃を防止・緩和する効果的な措置を実施していることを証明する必要がある。これにより政府は、進化する脅威環境に対するセクターのレジリエンスを確保され、実現可能な選択肢となる。対象となるのは 300MW 以上を制御し、電力システムに個別に重大な影響を与え得る事業者だけだからだ。

重要なのは、このアプローチが関係者に目的を絞った達成可能なものである点だ。明確な閾値（300MW 以上を管理する負荷制御事業者）を設定することで、電力システムに重大な混乱を引き起こす可能性のある組織のみを対象範囲に含める。これにより、業界と規制当局の双方にとって均衡が取れ管理可能な選択肢となる。

300MW という閾値は、国家エネルギーシステム運営機関（NESO）との協議を経て設定されたものであり、送電網管理の運用上の現実に基づいている。NESO は、送電網への最大電力供給者が喪失した場合を想定し、高周波・低周波予備力を維持している。NESO は送電網のレジリエンスに応じてこれらの予備力を調整する。

サイバー攻撃により電力需要が急減し、システムが想定する範囲を超える場合、システムのバランスが崩れ、全国的な電力供給に深刻な混乱を招く可能性がある。需要が低い時間帯などシステムのレジリエンスが低下している状態では、300MW の需要減少がシステム安定性に影響を与えると NESO は指摘している。

したがって、300MW 以上を制御する大規模負荷制御装置への攻撃により予期せぬ負荷変動が生じると、NESO がシステム安定性を維持できる限界を超える周波数変動を引き起こし、電力供給に重大な混乱をもたらす可能性がある。この閾値は、公的協議を経て業界から広く支持されている。

英国で負荷制御活動を行う組織の数は現在比較的少ないが、今後 10 年間でスマート技術を採用する消費者が増加するにつれ、大幅に増加すると予想される。固定閾値を導入することで、脆弱性のあるシステム状況下でエネルギー供給に影響を与える可能性のあるレベルの負荷管理を開始した組織が、速やかに規制対象となることが保証される。

このアプローチは、NIS 規則下における他のエネルギーサブセクターの既存規制対応と整合する。また、最も関連性が高く影響力の大きい組織のみが規制対象となることを保証し、比例原則とリスクベースのアプローチを維持する。さらに、絶えず変化するサイバー脅威環境において、対応力と適切性を保ち続ける規制枠組みを支援し、長期的なレジリエンスと適応性を確保する。

この選択肢は、効果的かつ実現可能であり、政府の広範な目標との戦略的整合性が高いと期待されるため、最終候補評価に進められた。

選択肢 4：NIS 規則の対象として全ての負荷制御装置を指定する

この選択肢は、負荷制御事業者が効果的なサイバーセキュリティ対策を確実に実施するという望ましい効果を達成する。ネットワーク全体の全ての負荷制御事業者を指定することで、一貫性のある「公平な競争環境」が実現される。

しかし、このアプローチには重大な欠点がある。負荷制御事業者は新興かつ急速に進化する分野であり、全ての事業者に NIS 規制要件を課すことは、特に中小企業に対して過大な負担となり、イノベーションや市場の成長を阻害する可能性がある。また、規制当局（Ofgem）に多大な負担をかけ、執行に多大なリソースを要し、管理不能となる恐れがある。

この一律的なアプローチは、イノベーションの促進、新興技術の支援、クリーンパワー 2030 ミッションの達成といった政府の広範な目標と戦略的に整合しない。リスクが事業体間で大きく異なる現在のサイバーセキュリティ環境を反映していない。小規模な負荷制御事業者が個別にエネルギー供給にリスクをもたらす可能性は低く、大規模事業者と同じ規制標準を適用することは必要でも比例原則にも反する。

この選択肢のコストは便益を上回り、全ての関係者にとってコスト対効果が低いと推定される。小規模負荷制御事業者は高いコンプライアンスコストに直面し、規制団体は追加的な資源需要の負担を強いられる。

上記の表にまとめた重要成功要因に基づき、多数の選択肢を評価した結果、選択肢 3 が「何もしない」というベースラインと共に、最終候補として選定可能な唯一の現実的な選択肢であると識別された。したがって、本措置を推進する上で選択肢 3 が優先される。

5.4 規制当局が必須サービス及びデジタルサービスの提供に不可欠な重要供給者を指定することを可能とする措置

政策選択肢	戦略的適合性	有効性 - 国民が依存し、経済安定と国家安全保障の基盤となる最重要国家インフラの防御に不可欠な事業者が、適切に対象範囲に含まれているか？	有効性 - ネットワークと情報システム規制に関する規制当局の職務遂行能力を向上させるか？	有効性 - 絶えず変化するサイバー環境において、NIS 規制自体が適切であることを確実にするか？	実現可能性
選択肢 1 - 何もしない	低	低	低	該当なし	高
選択肢 2 - アドバイス、ガイダンス	低	低	低	該当なし	高
選択肢 3 - 規制当局が「重要供給者」を指定できるようにする	高	高	高	該当なし	中
選択肢 4 - DSIT SoS が「重要サプライヤー」を指定できるようにする	中	中	低	該当なし	低

選択肢 1：何もしない

サプライチェーンはますます複雑化しており、サイバー犯罪者にとって魅力的な標的となっている。彼らはサプライチェーンの一部に攻撃を仕掛けるだけで、重要なデジタルサービスの継続性に広範な影響を及ぼし得る。重要サプライヤーに対する最近の攻撃例としては、2024 年の Synnovis 攻撃が挙げられる。この攻撃により 11,000 件の外来予約と選択的手術が延期され、緊急の献血要請が行われた。影響を受けた NHS トラストは重大インシデントを宣言し、単一サプライヤーへの攻撃が公共サービスの提供に及ぼす広範な影響を浮き彫りにした。

何もしないことは、重要なサイバーセキュリティ規制の対象範囲に適切な事業者を含める上で効果的ではない。近年、英国が直面するサイバー脅威がより深刻化・頻発化・高度化し、攻撃者がサプライチェーンの脆弱性を悪用して重大な混乱を引き起こそうとしていることが明らかになっている中、必須サービスやデジタルサービスに生じる重大なリスクに対処できない。これは 2022 年 PIR が 2018 年 NIS 規制の重大な欠陥として指摘した点であり、最近の事例（上記で強調したようなもの）は、何もしないことの人間への影響を示している。²⁷。したがって、これは進化するサイバー環境におけるリスクに対処しておらず、戦略的にも適切ではない。なぜなら、サービスの継続性や、壊滅的なサイバー攻撃の影響から国民と企業を防御するという、本法案で達成しようとしている成果を損なうリスクがあるからだ。

選択肢 2：自主的な助言とガイダンス

²⁷2018 年ネットワークと情報システム規制に関する第 2 回 PIR - GOV.UK

既存のサイバーアセスメント枠組み（CAF）は、NIS 規制対象企業が契約手段を通じてサプライチェーンを保護するための助言を提供している。政府は規制当局と連携し、既存のCAFを改正するか、追加の助言・指針を発行することで、「重要サプライヤー」に起因する脅威への認識を高められる。これには、規制当局と自主的に連携して依存関係を識別・管理する方法に関する指針が伴う。政府と規制当局にとって実現可能な選択肢であり、財政的負担も小さい。

NIS 法は既に規制対象事業体にサプライチェーンのセキュリティを考慮するよう義務付けており、CAFはその実施方法に関する助言を提供している。しかし CAF はサプライチェーンリスクの識別と確保において効果的でないことが判明しており、助言・ガイダンスの有効性は以下の理由から限定的である：

- 「重要サプライヤー」は、高度に集中した市場において必須サービスを提供する多くの企業にとって唯一の供給源であるという性質上、強い市場支配力を有している。この構造的な不均衡により、必須サービス提供に直接関与する企業は、契約手段を通じて「重要サプライヤー」にサイバーセキュリティの改善を要求する能力が著しく制限されている。したがって、この市場の失敗に対処するには、効果を上げるために業界全体の規制介入が必要となる（選択肢 3）。
- ガイダンスは、リスクマネジメントに必要な特定情報を「重要サプライヤー」から要求する法的報告義務を OES に課すことはできず、また「重要サプライヤー」にサイバーセキュリティ管理の改善を強制する必要な執行手段も提供しない。サプライチェーンの脆弱性を悪用しようとする敵対的攻撃者による重要サービスへの脅威の規模、およびそのような攻撃の負の外部性を考慮すると、重要サービスプロバイダによる自主的行動への依存は不十分であると判断する。

この選択肢は、サプライチェーンがもたらす増大する脆弱性に対処しない。サプライチェーンは、重要サービスやデジタルサービスに混乱を引き起こす可能性のある攻撃経路としてますます魅力的になっている。したがって、重要サービスの継続性を防御するという政府の目標に貢献しない。よって、戦略的適合性が低く、最終候補評価に進めることはできない。

選択肢 3：規制当局が特定の供給者を「重要供給者」に指定し、NIS 規制の適用対象とする（推奨選択肢）

この選択肢は、適切な事業者が重要なサイバーセキュリティ規制の対象となることを確保する上で最も効果的である。規制当局による重要供給業者の指定には一定の作業を要するが、供給業者が指定されるには法定の閾値規準を満たす必要があり、最も重要な少数の供給業者のみが対象となることが保証される：当該供給のためにネットワークと情報システムに依存していること；当該供給業者のネットワークと情報システムに影響を与えるインシデントが、それらに依存する重要サービスまたはデジタルサービス（あるいは重要サービス・デジタルサービス全般）に混乱を引き起こす可能性があること；そして、その混乱が英国全体または一部において、経済または社会の日常的な機能に重大な影響を与える可能性が高いこと。これまで NIS 規則の適用除外となっていた小規模・零細 RDSP も、閾値規準を満たせば「重要供給者」に指定可能となる（これにより重要サービスにとって重要とみなされる）。中小企業除外規定を廃止し、指定に厳格な規準を適用することは、有効性と実現可能性の適切な均衡を図るものと判断する。

さらにこの選択肢は、情報収集権限の強化を通じて各分野のサプライチェーンリスクを深く把握できるようにすることで、規制当局の職務遂行能力を向上させる。規制対象事業者による合理的な管理が困難な重大なリスクが存在する場合、規制当局は指定を通じて直接リスクに対処できる。このアプローチは NIS 規則全体の趣旨と整合しており、各分野の専門家である規制当局が、重要サービスへの脅威となり得る脆弱性を有する最も重要な供給者を特定する最適な立場にあることを示している。指定された重要供給業者は、適切なサイバーセキュリティ対策を講じる法的義務を負う。規制当局は、指定供給業者がこれらの義務を履行していることを確認する手段を有する。この対象を絞ったアプローチは、主要供給業者の可視性を高め、分野を横断したリスク対応の一貫性を確保し、経済成長、国家安全保障、経済的レジリエンスに関する英国の戦略的優先事項に沿って国家のレジリエンスを強化する。

これにより、特定の重要サプライヤーへの過度の依存や集中に起因する、サプライチェーン経路を通じた攻撃による重要デジタルサービスへのリスクが軽減される。サプライチェーンは多様化を続け、重要サービスの日常運営においてより多くのデジ

タルサービスが依存されるようになるだろう。したがって、我々は本案が、サプライチェーンの複雑化と脆弱化が進む現在および将来のサイバー環境において、適切な規制を確保する最も効果的な選択肢であると考えます。本案はまた、セクター横断的な脆弱性に対処し、新たな脅威に効果的に対応するための戦略的手段を提供する。これにより重要サプライヤーのサイバーレジリエンスが向上し、重要サービス及びデジタルサービスへの混乱リスクが大幅に低減されると評価する。

この分野では既に国内で実施された事例があり、主要サービスがサプライチェーンから受けるリスクと対応策を反映している。例えば 2023 年の金融サービス・市場法改正では、重要サードパーティがサイバー要件の対象範囲に追加された。これは本案が戦略的に適切であり、政府がサプライチェーン脆弱性対策として進める他の取り組みとも整合することを示している。

この措置は関係者及び業界の支持を得ている。2022 年の意見募集では、回答者の圧倒的多数（90%）が政府の重要供給業者指定権限を支持し、2018 年 NIS 規制の対象範囲内にある組織からは満場一致（100%）の賛同が得られた。²⁸ これが、本措置が 2024 年国王演説における一連の対策の一部として発表された理由である。

上記の表にまとめた重要成功要因に基づき、多数の選択肢を評価した結果、選択肢 3 が「何もしない」というベースラインと共に、最終候補として選定可能な唯一の現実的な選択肢であると識別された。これは、国民と国民が依存する重要サービスを防御するという政府の目標と強く戦略的に合致している。したがって、選択肢 3 がこの措置を進めるための推奨選択肢である。

選択肢 4：DSIT 担当国務大臣による「重要供給者」指定権限の付与

本案は重要供給者の指定において、より広範なセクター横断的な整合性と調整を確保する手段として検討した。このアプローチでは、DSIT 担当国務大臣が全ての指定権限を担い、選択肢 3 と同様の法定規準を適用し、指定供給者を NIS 規制の対象範囲に組み入れる。この中央集権モデルでは、セクター別規制当局ではなく DSIT が全ての指定権限を掌握する。

これにより統一的なアプローチが促進される可能性がある一方、最終的には選択肢 3 よりも効果的ではないと考える。規制当局は、規制対象事業者との既存の関係性、自部門内のサプライチェーンに対する理解、部門固有の技術的専門知識を有しているため、重要供給業者の識別・指定・監督に最も適している。これらの要素は、情報に基づいた均衡のとれた指定決定を行い、供給業者が適用範囲に入った後の効果的な監督を確保するために不可欠である。NIS 枠組みは、責任と分野別専門性を連動させる連合モデルに基づいて構築されており、この選択肢はその構造から逸脱するものである。

中央集権的な指定は原則として一貫性を支える可能性があるが、我々は選択肢 3 においても、DSIT 発行のガイダンスを通じて規制当局間の協力と調整を促進しつつ、業界主導の実施の利点を維持することで、これを達成できている。重要な成功要因に対して、この選択肢は選択肢 3 よりも評価が低い。セクター別の洞察と専門知識が欠如しているため、サプライチェーンリスクを効果的に対処する可能性が低いからだ。これにより、重要サービス及びデジタルサービスのレジリエンス向上、サイバー脅威からの国民・経済防御への影響が弱まり、したがって戦略的適合性も低下する。したがって、選択肢 4 は規制当局主導モデルからの移行を正当化する十分な付加価値を提供しない。

²⁸[英国のサイバーレジリエンス強化に向けた立法案 - GOV.UK](#)

規制当局がコンプライアンスを推進し、その職務遂行に必要な資源と重要な情報を確保するための措置

5.5 サービス継続性の限界を超えて、対象組織のインシデント報告義務を改正・強化する措置

政策選択肢	戦略的適合性	有効性 - 国民が依存し、経済安定と国家安全保障の基盤となる最重要国家インフラの防御に不可欠な事業者が、適切に対象範囲に含まれているか？	有効性 - ネットワークと情報システム規制に関する規制当局の職務遂行能力を向上させるか？	有効性 - 絶えず変化するサイバー環境において、NIS 規制自体が適切であることを確実にするか？	実現可能性
選択肢 1 - 何もしない	低	該当なし	低	該当なし	高
選択肢 2 - 任意報告	低	該当なし	低	該当なし	中
選択肢 3 - 報告規準を拡大する	高	該当なし	高	該当なし	中
選択肢 4 - 全てのインシデントの報告を義務付ける	低	該当なし	低	該当なし	低

選択肢 1：何もしない

何もしない場合、現状が維持される。つまり、規制当局に正式に報告されるインシデントはごくわずかであり、当局は職務を遂行するために必要な重要な情報を得られない状態が続く。

現行制度では、ランサムウェア、事前配置型攻撃、スパイウェアなどのサイバー攻撃は、重要サービスやデジタルサービスの提供を直ちに妨害しない限り報告義務がない。しかしこれらの攻撃は重大な混乱や侵害を引き起こす可能性がある。このため制度は本来の目的を果たせておらず、規制当局と NCSC は脅威の全体像を把握できていない。是正措置や予防措置に必要な十分な情報も得られていない。報告枠組みを改正し、より広範なインシデントを報告対象に含めることで、規制当局と NCSC は企業が重要サービスの混乱リスクを緩和するための適切な措置を講じていることを確認しやすくなる。

現状維持（すなわち何もしない）では、組織がインシデントを認識してから 72 時間経過するまで報告されない可能性があり、NCSC や規制当局が組織を支援し、進行中のインシデントの影響を管理する機会が制限される。さらに、NCSC は規制当局と同時にインシデント通知を受け取らないため、NCSC のインシデント対応支援能力がさらに遅延する。

現行制度では、RDSP、RMSP、データセンター運営者は、顧客に悪影響を及ぼす、あるいは及ぼし得るインシデントについて通知する義務を負わない。これは、顧客がリスクに晒されていることに気づかず、そのリスクの緩和措置を講じられない可能性があり、結果として自社のサービス提供に波及効果をもたらす恐れがあることを意味する。

我々は現行制度は実現可能ではあるが、規制当局と NCSC が職務を遂行する能力を確保する上で効果的ではないと判断する。規制当局が徹底的かつ信頼性の高いデータを持たない問題に対処しないことは、規制対象者を支援し、重要なサイバーセキュリティ規制の遵守を監視する能力を規制当局に備えさせるという戦略的目標を損なう。国家安全保障と公共サービスをより良く保護するために、サイバー環境がどのように進化しているかをより深く理解することを保証できていない。

選択肢 2：規制当局に対し、セクター別ガイダンスにおいてより広範なインシデントタイプの自主的報告を盛り込むよう促す

選択肢 2 は、NIS で義務付けられている範囲を超えて、例えばサービスに重大な混乱を引き起こす可能性のあるインシデントを含めるよう報告を促すことを提案する。これは既にほとんどの NIS セクター（例：水道セクター）で進められており、規制当局はガイダンスを通じて、企業が自主的に情報を提出しても罰せられないことを明確に述べている。しかし、規制当局は、規制対象事業者が依然としてこれらのインシデントを報告していないことを確認している。法的義務が明示されていないため、企業はこうしたインシデント情報を共有したがる。規制対象団体のシステムの脆弱性を規制当局に発見され、是正措置を求められるのを避けるためだろう。したがって、この選択肢は規制当局の職務遂行能力向上に効果的ではなく、選択肢 1 と同様に、政府の戦略目標である「規制当局が各セクターを支援し、コンプライアンスを監視し、進化する脅威環境を深く理解して国家安全保障と公共サービスを最善に防御する」ことを損なう。これらの理由から、本選択肢は最終候補リストの評価対象から除外される。

選択肢 3：規制対象の重要サービス、デジタルサービス、管理サービス提供に依存するネットワークと情報システムの運用またはセキュリティに影響を及ぼしたインシデントについて、重大な影響を及ぼしている、または及ぼす可能性がある場合に報告義務を導入する（推奨選択肢）

重要サービスのレジリエンスを確保するには、組織が適切なサイバーセキュリティ水準を達成・維持できるよう支援する能力を備えた規制当局の存在が不可欠である。そのためには情報収集が重要だ。前述の通り、報告枠組みの改正こそが、規制対象事業者のインシデント報告を確実にし、規制当局がサイバーセキュリティインシデントの規模と深刻度を明確に把握する最善策だと考える。これには、ランサムウェア、事前配置型攻撃、スパイウェアなどのインシデントも含まれる。これらは、サービスの中断や機密情報の侵害を通じて英国に重大な影響を与える可能性があるが、発見時点では重大な影響を及ぼしていなかったかもしれない。

選択肢 3(a) データセンター事業者に対する追加要件（推奨）

上記で定めた閾値に加え、データセンター運営者は以下の事項も報告することが求められる：

本規制において「データセンターインシデント」とは、以下のいずれかを引き起こす可能性があった、引き起こした、引き起こしている、または引き起こす可能性が高いインシデントを意味する：

- a) 英国の OES が提供するデータセンター・サービスの基盤となるネットワークと情報システムの運用またはセキュリティに重大な影響を与える可能性があった、与えた、与えている、または与える可能性のあるもの、
- b) 英国の OES が提供するデータセンター・サービスの継続性に重大な影響を与える可能性があった、与えた、与えている、または与える可能性のあるもの、
- c) 英国全体または一部において重大な影響を与える可能性があった、与えた、与えている、または与える可能性のあるもの。

法案にサービス継続性を明示的に盛り込むことで、データセンターの中核的機能——ネットワークと情報システムのホスティングおよびサイバーレジリエンス支援——が強化される。これにより、データセンター・サービスの継続性に影響を与えるインシデントは、ネットワークと情報システム自体に直接的な影響を及ぼさない場合でも対象範囲内に留まり、監督体制の整合性が維持される。

同様に、潜在的な影響（混乱を引き起こす可能性があったインシデント）を含むことで、管轄当局が新たな傾向を検知し、体系的な脆弱性を評価し、積極的に対応する能力が向上する。データセンターにとっては、進化するリスクに

対するレジリエンスを強化し、EU の NIS2 指令に基づくニアミス報告といった国際的なベストプラクティスと整合する。既存の「重大」という閾値は自然なフィルターとして機能し、事業者を過負荷にすることなく関連事象を確実に捕捉する。

インシデント報告制度を強化するさらなる措置も検討すべきだ。これには報告時間の更新、規制当局への報告と同時に NCSC への共有を義務付けること、デジタルサービスとデータセンターに対する透明性要件の強化が含まれる。

インシデント報告時間を更新し、二段階報告構造（インシデント認知後 24 時間以内の初期通知、その後 72 時間以内の詳細報告）を導入すれば、規制当局へのインシデント認知が早まり、必要な措置（もしあれば）を評価する時間を確保できる。初期通知は簡素な形式とし、規制対象事業者が重要な初期段階で可能な限りインシデントの影響緩和にリソースを集中できるようにする。その後 72 時間経過後、現行制度と同様にインシデントの理解が深まった段階で、より詳細な情報共有を求めることが可能となる。この二段階モデルは、24 時間以内に完全な報告書を提出させる方式よりも企業にとってコスト対効果が高く（実現可能性を確保）、危機対応からリソースを逸らすこともない。

現在、事業者は規制当局に報告を提出し、規制当局がこれを NCSC と共有する仕組みだ。報告プロセスを合理化し、規制当局への報告と同時に NCSC が情報を受け取れるようにすれば、迅速な連携が可能となり、NCSC はインシデント対応中の事業者に対し早期支援を提供できる。インシデント報告書の写しを NCSC に提出することを義務付ける場合、規制対象事業者の負担は最小限に抑えられる。規制当局に送付するインシデント報告書に NCSC 宛での写しを添付するだけで済むからだ。

最後に、デジタルサービス、マネージドサービス、データセンター・サービスに対する新たな透明性要件を導入することで、重大なインシデントの影響を受ける可能性のある顧客にそのインシデントが通知されるようになる。これにより、各セクター内の透明性が促進され、顧客はインシデントの影響を緩和するための措置を講じることができる。このアプローチは均衡が取れており、EU が採用しているアプローチと一致している。適切な場合には、国際的な整合性という戦略的適合性を満たすものである。

選択肢 4：規制対象事業者に、自社のネットワークと情報システムに影響を与える全てのインシデントを報告する義務を導入する。

理論上、全てのインシデントを規制当局に報告させることは、規制当局と NCSC（国家サイバーセキュリティセンター）に英国が直面する脅威の全体像を提供し、英国の重要サービス及びデジタルサービスを防御するための計画と準備を最も効果的に行うことを可能にする。しかし、英国が直面するインシデントの膨大な数を考慮すると、規制当局が受け取る情報を処理することは困難であり、実現不可能である。報告の大半は、事業者によって適切に処理された低レベルのインシデントに関するものとなり、より高度なインシデントや成功した攻撃の報告という重要な情報から注意をそらす可能性がある。これにより政策の有効性が低下する。また、この選択肢は対象事業者にとっても実行不可能である。特に規制当局にも困難をもたらすことを考慮すると、報告負担が過度に高く、不均衡であると判断されるからだ。

上記の表にまとめた重要成功要因に基づき、多数の選択肢を評価した結果、選択肢 3 が「何もしない」というベースラインと共に、最終候補として識別された唯一の実現可能な選択肢であると判断された。2022 年の協議では、この措置に対する支持が確認され、回答者の 68%がインシデント報告義務の拡大案に賛成した。これには 2018 年 NIS 規制の対象となっている組織の 67%も含まれている。²⁹したがって、本措置を推進する推奨選択肢は選択肢 3 である。本選択肢は効果的かつ実現可能で、戦略的適合性も高いため、最終候補評価に進められた。2024 年国王演説における一連の措置の一部として発表された。

²⁹[英国のサイバーレジリエンス強化に向けた立法案 - GOV.UK](#)

5.6 情報共有規定の強化策（例：規制当局間の情報共有、規制当局と公的機関間の情報共有を可能にする措置）

政策選択肢	戦略的適合性	有効性 - 国民が依存し、経済安定と国家安全保障の基盤となる最重要国家インフラの防御に不可欠な事業者が、適切に対象範囲に含まれているか？	有効性 - ネットワークと情報システム規制に関する規制当局の職務遂行能力を向上させるか？	有効性 - 絶えず変化するサイバー環境において、NIS 規制自体が適切であることを確実にするか？	実現可能性
選択肢 1 - 何もしない	低	該当なし	低	該当なし	高
選択肢 2 - 情報共有規定の改正	高	該当なし	高	該当なし	高

選択肢 1：何もしない

2018 年 NIS 規則には、規制体制の機能を支える情報共有を可能にする規定が含まれている。しかし、NIS 規制当局、業界、中央政府部門からは、これらの規定が十分かどうかについて懸念が示されている。NIS 規則の実施、関連政策（サイバーレジリエンスや国家安全保障など）の策定、規制枠組みの評価に関わる主要事業者間でデータを共有できる範囲には、重大な曖昧さと制限がある。規制当局との協議では、特定の事業者との特定情報の共有に関する法的明確性の欠如が、規制対象事業者からの法的異議申し立てリスクを規制当局に生じさせていることが明らかになった。

何もしなければ、これらの欠陥は残ったままとなり、NIS 規制の効果的な機能を支える情報共有が制限される。つまり、NIS 規制が適切に機能し目的を達成するために必要な情報が、規制体制の主要関係者間で共有されないことになる。規制対象事業者は規制当局との情報共有に消極的であり、政府は NIS 規制の影響を正確に把握するための情報や、国家安全保障と公共サービスを最善に防御するための進化する脅威環境に関する理解を深めるために必要な情報を得られない。また、NIS 制度外の他の規制当局と調整できない場合、規制の重複や二重化のリスクも存在する。

選択肢 2：識別された欠陥に対処するため、NIS 規則の情報共有規定に的を絞った改正を行う（推奨選択肢）

この選択肢は、識別された情報規定の欠陥に対処し、規制当局が職務を遂行する能力を向上させるため、以下の 4 つの変更を行うことを目指す：

- NIS 規制当局が英国公的機関と情報を共有できるようにするため、NIS 規則に英国公的機関を明示的に言及する。
- 情報共有の目的を拡大し、政府と規制当局間の情報共有を可能にすることで、NIS 規則に関連する政策立案の参考とし、その評価を支援する。
- NIS 規則に基づく情報共有後の利用方法に関する保護措置を強化するため、二次共有規定を明確化・制限する。
- 情報委員会に対し、登録された RDSP および RMSP のリストなど特定情報を NCSC とより容易に共有するよう義務付けることで、NCSC の RDSP および RMSP 情報へのアクセスを改善する。

これらの変更は、共有可能な情報の範囲と共有主体・対象について明確性を高めることで、NIS の有効性を向上させる。これにより英国公的機関と規制当局は明確な情報共有メカニズムを確保し、規制体制の効果的な機能を実現する。共

有可能な情報とその経路を明確化するため、規制当局にとって実現可能な選択肢と考える。最後に、プロバイダから提供された情報の使用方法および二次共有に関する保護措置が設けられる。これにより規制対象事業者は、規制当局と情報を共有した後も、自社のデータが適切に防御・共有・使用され、二次共有には比例原則に基づく制限が課されるという確信を得られる。こうした限定的かつ的を絞ったな変更は、NIS 規則の情報共有規定を強化すると同時に、保護措置の堅牢性も確保するものである。

情報共有は、NIS 規則の効果的な機能に不可欠である。現行の情報共有体制を包括的に改善し、情報の共有・利用方法に対する適切な保護措置を確保するためには、これら 4 つの変更全てが必要である。これにより、規制当局が情報にアクセスし交換する能力が向上し、その職務をより効果的に遂行できるようになる。政府は政策立案に資する情報へのアクセスが改善され、RDSP および RMSP に関するより多くの情報を受け取ることで、NCSC が規制対象事業者へのよりの支援提供など、その機能を遂行する上で支援される。記載された変更点のうち 1 つまたは 2 つ（4 つ全てではない）のみを実施した場合、変更範囲が限定的となり、この分野における目的が損なわれる。したがって、この選択肢（4 つの措置全てを含む）が最終候補リスト評価に進められた。

5.7 情報委員会の情報収集権限強化策

政策選択肢	戦略的適合性	有効性 - 国民が依存し、経済安定と国家安全保障の基盤となる最重要国家インフラの防御に不可欠な事業者が、適切に対象範囲に含まれているか？	有効性 - ネットワークと情報システム規制に関する規制当局の職務遂行能力を向上させるか？	有効性 - 絶えず変化するサイバー環境において、NIS 規制自体が適切であることを確実にするか？	実現可能性
選択肢 1 - 何もしない	低	該当なし	低	該当なし	高
選択肢 2 - 特定の情報をプロバイダする義務	高	該当なし	高	該当なし	中

選択肢 1：何もしない

何もしない場合、情報委員会は現行の規則 15 に基づく情報通知権限、または個別の自発的な情報提供要請に依存せざるを得ない。このデータ収集方法、および現行の規則 15 の適用範囲は、リスクの適切な把握に必要なデータを収集するには不十分と見なされている。リスクを適切に評価できなければ、情報委員会はサイバーインシデントに対して事後対応的な規制に留まり、攻撃を予防・緩和するための積極的な規制機能を発揮できない。

選択肢 2：登録時に RDSP および RMSP に対し特定情報の提供を義務付ける権限を情報委員会に付与し、登録後には情報通知（IN）を通じて追加情報を収集することを認める（推奨選択肢）

この選択肢では、リスクアセスメントを目的として、RDSP および RMSP に対し、登録時に提供されるサービスの種類や具体的な連絡先などの関連情報を提供する義務を課することが可能となる。

例えば、RDSP および RMSP は、従業員数や売上高などの企業情報、供給先セクター（例： の場合、政府調達枠組みを通じたサービス提供の有無、CNI セクターへの供給の有無）などの顧客情報を提供することが求められる可能性がある。要求される情報は基本的なものであり、組織に重大な負担を追加することはない。この種の登録情報は現在整備されていないが、他のインフラ事業や非インフラ事業（例：通信プロバイダの Ofcom 登録）では一般的である。

さらに、本法案は情報委員会に対し、登録後に情報通知を通じてリスクを判断するための追加情報請求権限を拡大する。

本措置の目的は、情報委員会がサイバーリスクを積極的に識別し、攻撃を防止するための適切な措置を講じることを支援することである。この選択肢は、情報委員会が NIS 法に基づく責務を適切に履行できる効果的な方法であると考えられる。本選択肢により、情報委員会はサイバーリスクが顕在化する前に識別・緩和する能力を強化し、攻撃を防止するとともに、将来のサイバー脅威に対するデジタルサービスの耐性を高めることができる。

この選択肢は、情報委員会の機能遂行能力向上に効果的であるため、最終候補評価に進められた。RDSP および RMSP に対する積極的アプローチにより、より多くのデジタルサービスを防御し、安定したビジネス環境を通じた経済成長を支援するという政府目標との戦略的整合性が強い。

5.8 規制当局のコスト回収メカニズム改善策

政策選択肢	戦略的適合性	有効性 - 国民が依存し、経済安定と国家安全保障の基盤となる最重要国家インフラの防御に不可欠な事業者が、適切に対象範囲に含まれているか？	有効性 - ネットワークと情報システム規制に関する規制当局の職務遂行能力を向上させるか？	有効性 - 絶えず変化するサイバー環境において、NIS 規制自体が適切であることを確実にするか？	実現可能性
選択肢 1 - 何もしない	低	該当なし	低	該当なし	中
選択肢 2 - 回復メカニズムの拡大	中	該当なし	中	該当なし	高
選択肢 3 - 回復メカニズムを拡大し、執行コストの回収を可能にする	高	該当なし	高	該当なし	高

選択肢 1：何もしない

何もしない場合、NIS 規則における既存のコスト回収規定に変更はない。これにより、個々の事業者規制に関連する特定のコストは回収できるが、ガイダンス作成や組織のスキル向上といった NIS 規制機能の遂行に伴うより一般的なコスト、あるいは執行コストの回収は認められない。同様に、規制当局が利用できるコスト回収方法にも変更はない。つまり、規制当局は引き続き直接請求に依存することになる。これらの両面が、規制当局が自らの役割を適切に果たす能力を損なっている。

現状維持は可能だが、コスト回収可能な活動範囲に関する規則のため効果的ではない。

何もしないことは、非遵守コストが不当に納税者に転嫁されるリスクの継続と、規制当局が機能を十分に遂行する能力の制約を意味する。これは、納税者に対する規制コスト削減を目指す政府の目標との戦略的整合性が低い。現状維持は、規制当局が執行措置を講じる能力に制約があると予測される場合、規制対象事業者が規制当局の要求する行動への遵守を遅らせるインセンティブを残す。これもまた、英国のサイバーレジリエンス強化という政府の目標との戦略的整合性に欠ける。

直接請求への依存を維持することは、規制対象事業者にとって、請求の有無や金額が不明確な状態を継続させることにもつながる。また、規制当局にとって、請求書に基づくコスト回収メカニズムに伴う行政負担を永続させることになる。

選択肢 2：既存のコスト回収メカニズムの範囲を拡大し、NIS 機能全般のコスト（執行コストを除く）をカバーするとともに、手数料徴収の選択肢を設ける。

この選択肢により、規制当局は NIS 機能の遂行に伴う一般経費（ガイドライン作成やスキル向上関連コストなど）を回収可能となる一方、執行経費の回収免除は現行通り維持される。さらに、直接請求に代わる、あるいは併せて、手数料徴収によるコスト回収の選択肢を規制当局に提供する。この仕組みでは、規制当局が料金体系を策定し、規制対象セクターと協議した上で、期末報告書を公表する必要がある。この方法は規制当局にとって実現可能である。なぜなら、より簡素であり、各セクターに最適なコスト回収制度を実施できるからである。

この選択肢は、規制当局が規制活動（ただし執行活動は除く）の大部分において、他の資金源への依存度を低減することを保証する。これにより、当局が職務の遂行に臨む姿勢や計画立案において、より確固たる基盤を得られるようになる。同様に、一部のコストが納税者に転嫁される可能性も低減し、手数料徴収の規定を通じて、規制対象事業者にとってより透明性が高く予測可能な規制環境を創出する。したがってこの選択肢は、規制当局の職務遂行能力向上においてより効果的だが、規制当局の主要な職務である執行活動は依然として業界自身による資金提供の対象外であるため、その効果は部分的なものに留まる。

この選択肢は「何もしない」シナリオに比べれば改善となる。規制当局が職務を遂行するための資源が確保されるからだ。しかし依然として、執行コストは回収されない。これは重大な欠落である。規制当局が執行義務を完全に遂行する能力が制約されるリスク、および関連するコストが納税者に転嫁されるリスクに対処できていないからだ。また、コンプライアンス遅延の誘因も残る。したがってこの選択肢は政府の戦略目標には改善をもたらすが、執行コストという根本的問題が未解決のため、我々は最終候補リストへの選定を見送った。

選択肢 3：既存のコスト回収メカニズムの範囲を拡大し、NIS の一般機能コストと執行コストをカバーする。さらに手数料徴収の選択肢を設ける（推奨選択肢）

この選択肢により、規制当局は NIS 機能の遂行に関連する全コスト（現行では除外されている執行活動コストやその他の一般規制コストを含む）を回収可能となる。さらに、直接請求ではなく手数料徴収によるコスト回収の選択肢を規制当局に提供する。執行コストの回収を最終候補に含めることは極めて重要である。これを除けば、規制当局は NIS 規制の執行からコストを回収する動機付けも能力も持たない。効果的な執行がなければ、NIS 規制への順守は限定的となり、重要サービス及びデジタルサービスのサイバーレジリエンス構築に影響を及ぼす恐れがある。この選択肢は政府が表明したサイバー目標に沿うものと見なされる。

この選択肢は、規制当局が最も効果的かつ包括的にその責務を果たすことを可能にする。規制当局は、執行を含む NIS 関連の全規制活動資金の調達方法について確実性を得られ、公的資金に依存してコストを納税者に転嫁する必要がなくなるため、政府の目標との戦略的整合性が強い。この仕組みは規制対象事業者にとって透明性と予測可能性が高く、NIS 規則に関連する業務のコストのみを賄うという安全装置によって防御される。規制当局が利益を得ることはできない。さらに、執行コストの組み込みにより規制対象事業者の負担増となるが、料金徴収の透明性と予測可能性の向上によって相殺される。規制当局は料金算定手法に基づき、事業規模に応じた比例配分（例えば売上高に応じた調整）など、各セクターに最適な方法でコストを割り当てる裁量権を持つため、実現可能である。

上記の表にまとめた重要成功要因に基づき、多数の選択肢を評価した結果、選択肢 3 が「現状維持」のベースラインと共に、最終候補として選定可能な唯一の選択肢であると識別された。したがって、本措置を推進する上で優先すべき選択肢は選択肢 3 である。この選択肢は、実現可能性、規制当局の職務遂行を保証する有効性、納税者への規制負担軽減という政府目標との強い戦略的整合性から、最終候補評価に進められた。また、2024 年国王演説における一連の措置の一部として公表されている。

5.9 政府（国務大臣）による戦略的優先事項声明の指定を可能とする措置

政策選択肢	戦略的整合性	有効性 - 国民が依存し、経済安定と国家安全保障の基盤となる最重要国家インフラの防御に不可欠な事業体が、適切に対象範囲に含まれているか？	有効性 - ネットワークと情報システム規制に関する規制当局の職務遂行能力を向上させるか？	有効性 - 絶えず変化するサイバー環境において、NIS 規制自体が適切であることを確実にするか？	実現可能性
選択肢 1 - 何もしない	低	該当なし	低	該当なし	高
選択肢 2 - 戦略的優先事項の声明	高	該当なし	高	該当なし	中

選択肢 1：何もしない

何もしないことは、NIS セクター全体で規制当局が一貫してその責務を果たすことを確保する上で効果的ではない。規制当局による NIS 規制の実施は、そのアプローチにおいて一貫性を欠いている。例えば、NCSC が規制対象事業体へのガイダンスの基礎としてサイバー評価枠組みを使用すべきだと助言しているにもかかわらず、規制当局は異なるサイバー評価ツールや異なる頻度のサイバー評価を義務付けている。規制当局の執行姿勢にもばらつきがあり、DSIT の助言通り積極的なアプローチを取る当局もあれば、従来通りの受動的な姿勢を続ける当局もある。NIS 執行の不統一は、各セクターが異なるセキュリティ対策を採用し、悪意あるサイバー活動に対する防御レベルに差が生じることを意味する。現状維持は、推奨ガイダンスの積極的实施など政府のサイバー戦略目標との整合性が低い。DSIT と NCSC がガイダンス発行や協力フォーラム創設でこれらの問題を解決しようとした努力は失敗に終わった。ガイダンスは任意の指針であり、無視される可能性があるからだ。したがって、さらなる任意のガイダンスは効果的な解決策とは考えられない。

選択肢 2：国務大臣に「戦略的優先事項声明」を指定する権限を付与する（推奨選択肢）

前述のように、裁量的ガイダンスではセクター間でのアプローチの一貫性を保証できないことから、執行の一貫性と有効性を確保するためには、政府による直接的かつ具体的な介入が必要であることが示唆される。戦略的優先事項声明には、規制当局が達成を目指す義務を負う目標が明記される。これにより、全ての規制当局が同一の成果に向けて取り組むことが義務付けられるため、規制当局間およびセクター間のアプローチの一貫性が向上する。これは、規制当局が政府の優先事項を認識し効果的に対応できるよう確保するという政府の総合的アプローチとも整合する。したがって本案は、政府が規制当局へ方向性を示し、政府の広範な目標との整合性と一貫性を確保できる点で、戦略的に極めて適合している。

規制の自律性を維持するため、戦略的優先事項の声明は規制当局との協議を経て作成され、規制当局は最も適切と考える方法で目標達成を目指す自由が認められる。現行の政策目標では、規制当局が効果的に計画を立てられる十分な時間軸を確保するため、戦略的優先事項の声明を 3 年から 5 年ごとに作成する方針である。これらのプロセスにより、声明が規制当局にとって実行可能な内容となることが保証される。本法案では、急速に変化する環境下で声明が規制当局にとって適切かつ実行可能であるよう、必要に応じて 3 年以内に修正することを認める。公的監視の機会を提供するため、国務大臣は戦略的優先事項声明の目標達成に向けた進捗状況を年次報告書として公表することが義務付けられ、その情報提供のために規制当局に情報提供を求めることができる。

本措置は二者択一の決定であるため、さらなる長リスト案の検討は不可能である。選択肢 2 は「何もしない」案と共に短リスト評価に進められた。これは戦略的整合性が強く、規制当局が効果的かつ一貫して職務を遂行することを可能とする

ためである。協議要件と公平な実施期間により、戦略的優先事項声明の遵守が求められる規制当局にとって本案が実行可能であることが保証される。

5.10 NIS 規則における執行メカニズム強化のための措置

政策選択肢	戦略的適合性	有効性 - 国民が依存し、経済安定と国家安全保障の基盤となる最重要国家インフラの防御に不可欠な事業者が、適切に対象範囲に含まれているか？	有効性 - ネットワークと情報システム規制に関する規制当局の職務遂行能力を向上させるか？	有効性 - 絶えず変化するサイバー環境において、NIS 規制自体が適切であることを確実にするか？	実現可能性
選択肢 1 - 何もしない	低	該当なし	該当なし	低	中
選択肢 2 - 新たな罰金上限の導入	中	該当なし	該当なし	中	中
選択肢 3 - 新たな罰金上限額を導入し、罰則区分を簡素化する	高	該当なし	該当なし	高	高

選択肢 1：何もしない

何もしない場合、NIS 規則に基づく制裁制度が維持される。規制当局はこれを非効率的と報告している。PIR では、執行根拠の限界、制裁制度全体の不明確さ、規制権限行使の制約を指摘し、将来検討すべき分野として強調された。これらの報告は、NIS 執行・制裁制度の内部アセスメントによってさらに裏付けられている。

効果的な制裁制度とは、意味があり、比例原則に則り、確信と確実性をもって執行されるものである。現在、我々は、金銭的罰則の水準が新たなサイバーリスク環境に見合っておらず、全ての NIS セクターにおける非遵守を抑制するには低すぎると考えている。一部分野では、最大罰金額がコンプライアンスコストを下回る可能性がある。1700 万ポンドは規制対象組織の年間売上高の 1%未満に過ぎない。これにより大企業はコンプライアンスを怠るインセンティブが生じる。経済・社会に及ぼす重大な影響と比較すると、こうした罰金額は他国制度に後れを取っており、十分な抑止効果を発揮していない。また、罰金は秘密裏に執行されていないことも明らかだ。2022 年の PIR（年次報告書）によれば、2018 年に「規則」が発効して以降、規制当局による罰金賦課は一度もなかった。その後、規制当局との協議を通じて、賦課された罰金はごくわずかであり、PIR で指摘された問題が依然として存在していることが判明している。

何もしない場合、現行の最高罰金額が維持される。これは長期的には各セクターにおける抑止力の低下を招き、英国経済・社会が依存する重要サービスのサイバーレジリエンシー向上に向けた追加的インセンティブを生み出さない。この選択肢は、特にコンプライアンスコストが潜在的な制裁を上回る状況において抑止力を高められないため、制度の効果を低下させ、規制当局が国家インフラの重大リスクに対処する能力を損なうと考える。規制対象組織が罰金を「事業コスト」として吸収する可能性があり、コンプライアンス遵守への追加的インセンティブは生まれない。この意味で、個別の抑止力（反復違反の低減という意味）も公共的抑止力（全セクターにおけるコンプライアンス遵守の総合的インセンティブとして理解される）も増大せず、制度全体の成功は長期的に停滞あるいは低下する可能性がある。

現行の罰則帯構造も不明確であり、規制当局が確信を持って一貫した罰則執行を行えず、規制対象事業者も非遵守時の制裁予測に必要な明確性・透明性を欠いている。特に、違反がサービス継続性に与える影響（または潜在的影響）に基づいて罰則を決定する現行要件は、罰金の賦課方法について十分な指針を提供せず、規制当局と規制対象事業

体に不必要な複雑さとコストをもたらしている。この選択肢は遵守促進や一貫した執行罰則を促さないため、効果的で透明性のある規制体制という政府の目標との戦略的整合性が低い。

選択肢 2：罰則構造の改革なしに罰金上限のみを改正する

この選択肢では、罰金上限額を売上高の一定割合に基づく基準に改定することで、規制当局がより高額な罰金を科すことが可能となる。現行規制では、当局が科せる金銭的罰則は最大 1700 万ポンドに限定されており、これは大規模事業者にとって売上高のごく一部に過ぎない。このため規制対象事業者は、事業継続のコストとして罰則を受け入れるインセンティブが強まり、特に故意または悪意のある違反行為に対しては、この制度では不遵守に対処する手段が不十分である。

売上高比率に基づく高額罰則を可能にすることで、コスト便益分析をコンプライアンス方向に転換し、英国経済・社会にとって重要なサービスにおけるコンプライアンスに対する社会的・規範的期待を明確に示すことになる。これにより抑止効果が強化され、規制枠組みの成功と国家インフラ・重要サービスへのリスクマネジメントという政策目標に直接寄与すると期待される。同時に、売上高に関連付けて罰金を調整することで、小規模組織に対する過剰な罰金の可能性を低減する。

ただしこの選択肢は、罰則構造の改革を含まないため、法制度上の重大な制約が維持される。これにより金銭的制裁の執行はより煩雑化し、解釈の余地が生じる。不要な訴訟の可能性が高まり、規制対象事業者が非遵守時に直面する結果について明確性がほとんど得られない。効果的な制裁制度は、以下の三要素で構成されると一般に認められている：違反行為に対する比例性、制裁適用における確信度、執行の迅速性である。本案は制度の厳格化を図るものの、枠組み構造上の課題（制度の確実性・迅速性向上に関わる部分）には対応しないため、効果的な制裁枠組み構築への影響度は中程度に留まる。

選択肢 3：罰金上限の改正と罰則段階の簡素化（推奨選択肢）

この選択肢では、NIS 規則に基づく 3 段階の罰則構造を簡素化・合理化するとともに、罰金の上限額を売上高の一定割合に基づく基準に改正する。現行の段階構造に伴う不明確さを解消するため、明確な基準値を設定した 2 つの新たな罰則段階を創設し、全ての重大な違反行為を上位段階の罰則対象とする（現行の罰則段階判定における問題点の一つ）。

この選択肢は、罰金の比例性と適用における確信・確実性を同時に高めることで、最も効果的な執行体制を実現する。規制当局が特定の違反行為に対して適切な水準の罰則を課す際の確信と明確性を高め、実質的な執行措置を講じる可能性を高めると同時に、上限罰則額の引き上げにより規制対象事業者の規制遵守インセンティブを強化する。これにより英国最重要サービス全体のセキュリティとレジリエンス標準が向上する。

したがって本案は、強力かつ効果的な執行メカニズムを通じて英国のサイバーレジリエンスを強化するという政府目標に最も戦略的に適合する。選択肢 2 が効果的執行の重要条件の一つを整備する一方、現行執行体制の的限界を包括的に解決し、罰則が効果的・予測可能・一貫した方法で適用されることを保証するのは本案のみである。

NIS 規則が絶えず変化するサイバー環境に対応し、政府が国家安全保障の防御のための断固たる行動を取れるようにするための措置

5.11 政府が議会の法律なしに NIS 規則を更新できるようにする措置

政策選択肢	戦略的適合性	有効性 - 国民が依存し、経済安定と国家安全保障の基盤となる最重要国家インフラの防御に不可欠な事業者が、適切に対象範囲に含まれているか？	有効性 - ネットワークと情報システム規制に関する規制当局の職務遂行能力を向上させるか？	有効性 - 絶えず変化するサイバー環境において、NIS 規則自体が適切であることを保証しているか？	実現可能性

選択肢 1 - 何もしない	低	低	低	低	高
選択肢 2 - 非立法	低	低	低	低	中
選択肢 3 - 比例的な委任権限	高	高	高	高	中

選択肢 1：何もしない

何もしないことは、政府が変化する脅威に対応し規制枠組みを更新する能力を制限し、制度の有効性を維持できなくなる。これにより英国は変化する新たなサイバー脅威に晒され、国際的な他国に後れを取る。

サイバー脅威は進化しているが、本影響評価の第 2 節で述べたように、それに伴う問題は未解決のままである。例えば、市場原理や自主的なガイドラインは、MSP の事例に見られるように、重要サービスやデジタルサービスのサイバーセキュリティを、企業の信頼性、経済、国民が日々依存するサービスの継続的な提供に対する脅威を軽減するほどには効果的に向上させていない。これらの分野は一般データ保護規則（GDPR）の適用対象となることが多いが、これは個人データの保護を強化したに過ぎず、重要サービスの運営に関わるシステム自体のセキュリティ向上にはつなげていない。

この選択肢は、国家安全保障と重要サービスが直面する脅威に対処できるサイバーセキュリティとレジリエンスを確保するという政府の目標との戦略的整合性が極めて低い。

選択肢 2：ガイダンスやその他の非立法的手段を通じて、より広範な組織による優れたサイバー慣行を促進する

このアプローチはこれまで効果がないことが証明されている。OES や RDSP は、自社の業務におけるサイバーセキュリティのコストや便益を包括的に理解していないことが多い。その結果、サイバーセキュリティとレジリエンスを向上させるための投資や自主的な取り組みは、しばしば優先順位が下げられる。

最近の報告書は、英国全土で事業を展開する企業のサイバーレジリエンス水準が依然として低いことを強調している。2024 年時点で、大企業の 7 割（70%）が正式なサイバーセキュリティ戦略を策定していたのに対し、中堅企業では大幅に少ない 57%しか策定していなかった。³⁰セキュリティ監視ツールの展開は減少している（2024 年は 30%³¹ 対 2023 年は 33%³²）。一方、何らかのユーザー監視を実施する企業の割合（30%³³³⁴）は変化がない。これは、制度が効果的かつ目的に適合した状態を維持するためには政府の介入が必要であることを示しているに過ぎない。

英国政府は、産業界におけるより良いサイバーセキュリティ慣行を推進するための一般的なガイダンスを提供している。産業界向けガイダンス（NCSC の「Cyber Essentials」など）は、特定のセクター向けに調整されているわけではなく、産業界は自組織に最適な形でガイダンスを適用できる。また、特定のセクターに対する具体的な脅威に関する助言も提供していない。

³⁰[サイバーセキュリティ侵害調査 2025](#)

³¹[サイバーセキュリティ侵害調査 2025](#)

³²[サイバーセキュリティ侵害調査 2024](#)

³³[サイバーセキュリティ侵害調査 2025](#)

³⁴[サイバーセキュリティ侵害調査 2024](#)

NIS 規則は指定セクターに適用され、規制当局は規制対象事業者と協力してネットワークと情報システムのセキュリティや脆弱性を評価し、リスクマネジメント・緩和のための具体的助言を提供する。NIS 規則の対象となるほど重要なセクターであれば、積極的な監督や個別助言を伴わない一般的な指針だけでは不十分だ。サイバーセキュリティ改善策の実施には多額のコストがかかるため、たとえ業種特化型であっても、企業はガイダンスのみに基づいて行動する可能性は低い。したがって、英国の消費者を重要サービスの混乱から防御するという確固たる意思があるならば、非規制的アプローチは現実的ではない。このため、本案は最終候補リストの評価対象から除外された。

選択肢 3：NIS 規則の関連性と有効性を維持するための適切な安全装置を伴う委任権限の導入（推奨選択肢）

この措置により、政府は適切な協議を経た上で、議会の法案成立を待たずに規制枠組みを更新できるようになる。これにより、規制の対象となる事業者を拡大し、規制当局の機能と責務を更新することで、その任務遂行能力を向上させることが可能となる。結果として、NIS 規則は進化するサイバー脅威に対応し続けられる。これらの権限には一定の制限と安全装置が設けられる。例えば、改正が英国経済や社会の機能に不可欠なサービスの規制に関連する特定の範囲内で行われるよう制限される。この権限は、規制対象事業者に対する新たな要件や義務の導入、NIS 規制当局の責任や機能の変更などの変更を行うために使用される可能性がある。本法案はまた、規制対象事業者が規則の要求事項を順守するための支援として、従うべき明確な指針と優良事例を定める実践規範の公表を認めている。

EU は、NIS 規制の対象となるべき業種が増えていることを識別している。NIS 指令 2 の実施において、EU は NIS 規制の対象業種を 8 業種追加して拡大した。これは国際的に、各国が他の業種への脅威の高まりを認識していることを示しており、この選択肢は強力な戦略的適合性を持ち、国際的なアプローチと一致している。法案に盛り込まれた委任権限により、英国は将来的に NIS 規則の適用範囲を拡大することが可能となる。その際には十分な根拠が必要となる。

2022 年の意見募集では、回答者の大多数（88%）が、英国政府が二次立法を通じて NIS 規則の特定要素を改正する権限を持つことに同意した。さらに回答者の大多数（81%）が、政府が NIS 規則を改正して新たな分野を追加することを可能にする委任権限の提案に同意した。³⁵

この選択肢は、政府が市場の失敗に迅速に対応できることを最も確実に保証する。これは、敵対的な主体に対する英国のサイバーレジリエンスを強化するという政府の目標と戦略的に強く合致する。したがって、この選択肢は最終候補として評価を進めることとなった。

上記の表にまとめた重要な成功要因に対して、多数の選択肢を評価した結果、選択肢 3 が「何もしない」というベースラインと共に、最終候補として適した唯一の現実的な選択肢として識別された。したがって、この措置を進める上で選択肢 3 が優先される。

5.12 政府が規制枠組みにおけるセキュリティ及びレジリエンス要件を更新するための措置

政策選択肢	戦略的適合性	有効性 - 国民が依存し、経済安定と国家安全保障の基盤となる最重要国家インフラの防御に不可欠な事業者が、適切に対象範囲に含まれているか？	有効性 - ネットワークと情報システム規制に関する規制当局の職務遂行能力を向上させるか？	有効性 - 絶えず変化するサイバー環境において、NIS 規制自体が適切であることを確実にするか？	実現可能性
選択肢 1 - 何もしない	低	該当なし	該当なし	低	中

³⁵ [英国のサイバーレジリエンス強化に向けた提案に関する意見募集への政府の回答 - GOV.UK](#)

政策選択肢	戦略的適合性	有効性 - 国民が依存し、経済安定と国家安全保障の基盤となる最重要国家インフラの防御に不可欠な事業者が、適切に対象範囲に含まれているか？	有効性 - ネットワークと情報システム規制に関する規制当局の職務遂行能力を向上させるか？	有効性 - 絶えず変化するサイバー環境において、NIS 規制自体が適切であることを確実にするか？	実現可能性
選択肢 2 - セキュリティとレジリエンスに関する要件	高	該当なし	該当なし	高	中

選択肢 1：何もしない

NIS 規則は、RDSP がサイバーレジリエンスを高めるために満たすべき最低限のセキュリティ要件を定めている。PIR からは、NIS がなければ、英国のデジタルサービスおよび重要サービスにおけるサイバーセキュリティの改善ははるかに遅いペースで進んでいたであろうという強い示唆がある。³⁶ しかし、現行の NIS 規則の下では、セキュリティ要件を更新し、新たな脅威や脆弱性に対応させることはできない。このため英国では、対象組織への規制負担最小化を優先したセキュリティ要件が維持されるが、2025 年に英国が直面するサイバー脅威に十分に対処できない可能性がある。したがってこの選択肢は、絶えず変化する環境下で NIS 規則の適切性を確保する上で効果的ではない。また EU を含む国際的な先例に英国が後れを取るリスクも生じ、国際的な進展との戦略的整合性が損なわれる。

選択肢 2：国務大臣に二次立法によるセキュリティ・レジリエンス要件の更新権限を付与する（推奨選択肢）

この選択肢では、国務大臣が二次立法を通じてセキュリティ及びレジリエンス要件を更新する権限を付与される。これらは従来「技術的・方法的セキュリティ要件」と呼ばれていたが、名称を「セキュリティ及びレジリエンス要件」に変更することで、関係者がその目的をより明確に理解できるようになる。国務大臣には以下の権限が付与される：

- 規制により RDSP に適用されるセキュリティ要件を設定する権限
- 適切かつ均衡のとれた範囲で、これらの要件を RDSP 以外の対象に拡大する権限

これらの要件により、政府は RDSP 向け既存セキュリティ要件を更新できる。選択肢の一つとして、サイバー評価フレームワーク基本プロファイル（CAF）の要素を反映させるため、セキュリティ要件を調整する権限を行使することが考えられる。CAF は、例えばサイバーガバナンス、資産管理、リスクマネジメント、インシデント対応などに関する基本要件を定めるものである。CAF は効果的な成果ベースのリスクアセスメントツールであり、対象事業者への個別対応型助言に依存する。これにより規制当局は組織のサイバーセキュリティ体制を審査し、適切な対策（ ）が実施されていることを確認できる。この手法は主要組織のシステムにおける脆弱性を効果的に低減し、悪用される可能性を排除する計画の改善に寄与してきた。これらの要件は、RDSP 向け NIS で既に規定されている既存のセキュリティ要件を基盤としつつ、CAF 基本プロファイルの要素を反映し、必要に応じて EU NIS 2 規制で全規制対象事業者に定められたセキュリティ要件と整合させるべきだ。したがってこの選択肢は、国際的な先例との戦略的整合性が強い。

規制を通じてセキュリティ及びレジリエンス要件を設定する権限を付与することは、現行の NIS 規制をより柔軟にし、絶えず変化するサイバー環境や新たな脅威に適応させる上で効果的である。これにより将来の脅威に対する改正が可能となる。

³⁶ [ネットワークと情報システム規制 2018 の第二回 PIR - GOV.UK](https://www.gov.uk/government/consultations/network-and-information-security-regulation-2018)

選択肢 2 は、規制の適切性を確保し強力な戦略的整合性を維持する効果から、最終候補リスト評価へ進められた。

5.13 サプライチェーンのセキュリティ強化策

政策選択肢	戦略的整合性	有効性 - 国民が依存し、経済安定と国家安全保障の基盤となる最重要国家インフラの防御に不可欠な事業者が、適切に対象範囲に含まれているか？	有効性 - ネットワークと情報システム規制に関する規制当局の職務遂行能力を向上させるか？	有効性 - 絶えず変化するサイバー環境において、NIS 規制自体が適切であることを確実にするか？	実現可能性
選択肢 1 - 何もしない	低	該当なし	該当なし	低	高
選択肢 2 - 任意のガイダンス	低	該当なし	該当なし	低	中
選択肢 3 - サプライチェーン業務	高	該当なし	該当なし	高い	中

選択肢 1：何もしない

我々の重要サービスの供給網はますます複雑化し、サイバー攻撃に対して脆弱性が増している。サプライヤーは悪意ある者にとって格好の標的だ。彼らは組織のサプライチェーン内のどこかでセキュリティが弱い箇所を突くことで、重要サービス自体を攻撃せずに、そのサービスに甚大な混乱を引き起こすことができる。このリスクにもかかわらず、昨年、直近のサプライヤーがもたらすリスクを評価した企業は 1 割強（14%）に過ぎず、より広範なサプライチェーンを調査していた企業は 1 割未満（7%）だった。³⁷ 大企業ではこの割合が高く、直接取引先を調査しているのは 45%、広範なサプライチェーンを調査しているのは 25%であった。しかし、大規模なサプライチェーンの脆弱性がもたらすリスクや、それが顧客やサービス利用者にも与える影響に対処するには依然として不十分である。何もしないことはこれらの問題を解決せず、重要サービスやデジタルサービスを保護するためにサプライチェーンのサイバーレジリエンスを強化するという政府の目標との戦略的整合性も低い。

何もしないことは可能であり、OES や RDSP に対する追加的な規制負担を回避できる。これにより、追加のコンプライアンスコストや行政要件なしに事業を継続できる。しかし、それは同時に、サプライチェーンに関連する脆弱性とリスクが対処されないことを意味し、NIS 規則はサイバー脅威のレベルに見合ったものとはならず、サイバー脅威やその他のセキュリティインシデントに対して脆弱な状態を放置することになる。これは、重要サービスや CNI のセキュリティとレジリエンス、ひいてはこれらのサービスを利用する人々にとって、より広範な影響を及ぼす可能性がある。

選択肢 2：自主的ガイダンス

NCSC は既に、サプライチェーンセキュリティに関する世界水準の自主的ガイダンスを幅広く提供している。これは OES や RDSP だけでなく、サプライヤーも利用可能だ。これには自主的サイバー標準や「サイバー評価枠組み」「サイバー・エッセンシャルズ」などの製品が含まれる。

エッセンシャルズなどのサイバー基準・製品が含まれる。

³⁷[サイバーセキュリティ侵害調査 2025 - GOV.UK](#)

この選択肢は政府や規制当局にとってほとんどコストがかからないため、実現可能だ。政府は、自主的ガイドラインやサイバー標準だけでは、サプライチェーンに関連する増大するセキュリティ・レジリエンスリスクに対処するには不十分であると認識している。この選択肢では、業界内で標準が不均一になり、ガイドラインに従う企業と従わない企業が混在する可能性が高い。その結果、「公平な競争環境」の確立が妨げられる。したがって、重要サービス及びデジタルサービスに対する強力かつ一貫したサイバー規制という政府の目標との戦略的整合性が低い。このため、この選択肢は最終候補評価に進められなかった。

選択肢 3：政府が二次立法において OES 及び RDSP に対するより強力なサプライチェーン義務を設定することを可能とする（協議を条件とする）（推奨選択肢）

OES および RDSP に対し、強制力のある義務を通じてサプライチェーンのセキュリティを識別・管理するよう明確な期待を設定することで、自主的なガイダンスよりもサプライチェーン全体でのコンプライアンス水準の向上が見込まれる。政府の見解では、NCSC がこれまで発行してきた任意の助言に対するコンプライアンス水準が不均一であったことから明らかなように、純粋に自主的なアプローチでは推奨措置へのコンプライアンスは限定的となる。

この選択肢は、NIS 規則が安全でないサプライチェーンの脅威増大に対応できる適切なものとなるよう効果的に機能する。規則に定められた強制力のある期待事項は、契約上の取り決めの活用を促進し、OES や RDSP がより広範なサプライチェーン全体でリスクを包括的に管理することを可能にする。これは、自社のサプライチェーンと脆弱性の所在を最もよく理解している OES や RDSP にとって実現可能なはずだ。

ただし、少数の供給業者への依存集中など、特定の重大なサプライチェーンリスクは、個々の OES や RDSP が単独で合理的に管理できる範囲を超える可能性がある。こうした状況では、重要供給業者の指定に焦点を当てた措置 5.4 を採用すべきである。措置 5.4 により、規制当局は重要供給業者を NIS 規制の対象範囲に含めることで、これら業者に関連する脆弱性に直接対処できる。

これらの補完的な措置を組み合わせることで、サプライチェーンリスクマネジメントの実践を強化すると同時に、規制上の指定を通じて最も重要なリスクを具体的に対象とすることで、サイバーレジリエンス全体を強化する。

上記の表にまとめた重要成功要因に基づき、多数の選択肢を評価した結果、選択肢 3 が「何もしない」というベースラインと共に、最終候補として選定可能な唯一の選択肢であると識別された。したがって、本措置を推進する上で選択肢 3 が優先される。選択肢 3 が最終候補として選定された理由は、NIS 規則の適切性を維持する効果、強力な戦略的適合性（特に措置 5.4 と組み合わせた場合）、および OES および RDSP にとっての実行可能性によるものである。

5.14 国家安全保障の利益のために、必要かつ均衡のとれた範囲で、政府が規制当局に指示を行うことを可能とする措置

政策選択肢	戦略的整合性	有効性 - 国民が依存し、経済安定と国家安全保障の基盤となる最重要国家インフラの防御に不可欠な事業体が、適切に対象範囲に含まれているか？	有効性 - ネットワークと情報システム規制に関する規制当局の職務遂行能力を向上させるか？	有効性 - 絶えず変化するサイバー環境において、NIS 規制自体が適切であることを確実にするか？	実現可能性
選択肢 1 - 何もしない	低	該当なし	低	該当なし	中
選択肢 2 - 政府を除く規制当局への権限付与	高	該当なし	高	該当なし	中

選択肢 3 – 全ての規制機関を指揮する権限	高	該当なし	高	該当なし	低
------------------------	---	------	---	------	---

選択肢 1：何もしない

この選択肢では、政府は規制対象事業者のネットワークと情報システムがより高いリスクに晒される脅威環境の急変に対し、規制当局に対応を要求できなくなる。現行制度では、規制対象事業者はサイバー脅威から自らを守るため「適切かつ均衡のとれた」措置を講じる義務を負い、規制当局は各業界に対しこの義務の解釈を支援する指針を発行している。しかし政府には、国家安全保障リスクが高まった際に必要となる具体的な措置を反映させるため、規制当局が指針を更新することを確保する能力が欠けている。さらに、規制当局は政府と同等の重要情報へのアクセス権限や速度を持たないため、差し迫った脅威への対応能力が阻害される可能性がある。これにより規制当局にとって何もしない選択肢は現実的ではなくなる。規制対象事業者がプロバイダとして提供するサービスがサイバー攻撃で混乱するリスクが軽減されないため、国家安全保障上の脆弱性が生じる。この選択肢は、国家安全保障の強化と国民保護のための断固たる対応という政府の優先課題との戦略的整合性が極めて低い。

選択肢 2：国務長官に政府外の規制当局への指示発出権限を付与する（推奨選択肢）

この選択肢は、国家安全保障上のリスクをもたらす脅威やインシデントに対し、政府が迅速に対応できることを保証する。複数の分野にまたがる対応が必要な場合、規制対象事業者に対して個別の指示を必要な数だけ作成・発行し、その遵守状況を監視することは現実的ではない。したがって、規制当局に対して指示を発行し、脅威の高まりを反映した形で各分野のガイダンスを更新するよう求める方が現実的である。

この権限は、国家安全保障上必要であり、かつ指示の影響が比例的と認められる場合にのみ行使できる。例えば、2022年のロシアによるウクライナ侵攻後、政府は規制当局に対し、NIS セクター全体の規制対象事業者が脅威環境の高まりに対応するために必要な措置を講じるよう促すため、ガイダンスを更新するよう指示を出すことを検討した可能性がある。この選択肢は、政府の国家安全保障目標との戦略的整合性が強い。

この権限が国務大臣によって頻繁に行使されるとは想定していないため、規制当局にとって実行可能な選択肢となる。指示は NCSC からの情報に基づいて行われる可能性が高く、各セクターが国家安全保障リスクを緩和するための適切な措置を採用することを保証する。政府からのこの情報により、規制当局は効果的にその責務を果たすことができる。

この権限は、王室大臣や地方分権政府に対して指示を出すために使用できないよう制限される。

選択肢 3：国務大臣に全ての規制当局への指示発出権限を付与する

選択肢 2 と同様に、この選択肢は政府が国家安全保障上のリスクをもたらす脅威やインシデントに迅速に対応できることを保証する。国務大臣が政府内に設置された規制機関を含む全ての規制機関に指示を発出できるようにすることは、理論上、より広範な脅威への対応能力を高めるだろう。しかし、ある国務大臣が別の国務大臣（ ）に特定の行動を指示することは不可能であるため、この選択肢は実現可能ではない。また、国務大臣が地方分権政府に指示を出すことも現実的ではないと考えられる。

選択肢 2 は政府目標との戦略的整合性が極めて強いため、最終候補リスト評価へ進められた。

5.15 国家安全保障の利益のために必要かつ均衡のとれた範囲で、政府が規制対象事業体に指示を行うことを可能とする措置

政策選択肢	戦略的適合性	有効性 - 国民が依存し、経済安定と国家安全保障の基盤となる最重要国家インフラの防御に不可欠な事業体が、適切に対象範囲に含まれているか？	有効性 - ネットワークと情報システム規制に関する規制当局の職務遂行能力を向上させるか？	有効性 - 絶えず変化するサイバー環境において、NIS 規制自体が適切であることを確実にするか？	実現可能性
選択肢 1 - 何もしない	低	該当なし	該当なし	該当なし	高
選択肢 2 - すべての規制対象事業体を指揮する権限	高	該当なし	該当なし	該当なし	中
選択肢 3 - OES のみを直接制御する権限	低	該当なし	該当なし	該当なし	中

選択肢 1：何もしない

2018 年 NIS 規則は、規制対象の事業体が自社のネットワークやシステムに影響するサイバーセキュリティリスクを管理するため、「適切かつ均衡の取れた」措置を講じることを義務付けている。規制対象事業体はサイバーリスクから自らを守るため、適切かつ均衡の取れた措置を導入する義務を負っているが、そうした措置は高度なサイバー攻撃から事業体を防御するには必ずしも十分ではない。規制対象事業体、特に重要インフラ（OES）を標的としたサイバー攻撃が成功した場合、英国の国家安全保障に深刻な影響を及ぼす。2024 年の年次レビューで NCSC は、英国が直面するサイバー脅威の状況を「拡散し危険な状態」と表現した。³⁸ 同レビューは、サイバーインシデントの件数が増加していること、またそれらの影響も拡大していることを指摘した。さらに国家主体のアクターが、英国の NIS セクターを標的とした悪意ある活動を増加させていることも記されている。

何もしなければ、政府は NIS 規制対象事業体に対し、自機関のネットワークと情報システムに関連するサイバー脅威やインシデントへの対応を強制できなくなる。たとえそれが国家安全保障の保護に不可欠と判断された場合であっても。高度な能力を持つ主体や敵対的な国家による脅威の増大は、この隙間が悪用される可能性を高め、悪意ある活動による混乱を悪化させ、英国の重要国家インフラ（CNI）の運用をリスクに晒す。この選択肢は、国家安全保障の強化と国民保護のための断固たる対応という政府の優先事項との戦略的整合性が極めて低い。

選択肢 2：国務大臣に規制対象事業体への指示発出権限を付与する（推奨選択肢）

英国に影響を及ぼすサイバー脅威の増大を踏まえ、この選択肢は政府が 規制対象事業者に影響する脅威やインシデントに迅速に対応できることを保証することで、既存の国家安全保障上の脆弱性に対処する。この選択肢は、国民が日常的に依存する重要サービス及びデジタルサービスを防御するという政府の目標と極めて強く戦略的に合致する。この権限は国家安全保障上必要不可欠な場合にのみ行使され、指示の影響が比例原則に合致すると判断される場合に限り適用される。この措置は、特定のサイバー脅威への対応や英国の国家安全保障上必要な場合にのみ行使されるよう設計され

³⁸2024 年度年次レビュー

ているため、国務大臣が頻繁に利用することは想定していない。これにより規制対象事業者にとって実行可能性が確保される。指示は NCSC からの情報に基づいて行われる可能性が高い。

選択肢 2 は政府目標との戦略的整合性が極めて強いため、最終候補評価に進められた。

選択肢 3：国務大臣が OES のみに指示を発出する権限を付与する

この選択肢は、優先案と同様の影響をもたらす。すなわち、国務大臣が OES に対し、国家安全保障上の脅威やインシデントに対処するための措置を講じるよう指示する権限を付与するものである。ただし、この選択肢は RDSP、RMSP、指定重要供給者を対象外とする。OES のみを対象とすることで、RDSP、RMSP、指定重要供給者への脅威が OES の混乱を招くリスクがあり、結果として付与を意図する権限を制限することになるため、国家安全保障リスクの緩和という政策目的を著しく損なう。したがって、重要サービス及びデジタルサービスの防御という政府の優先事項との戦略的整合性は低い。

本案は意図した権限を制限し、国家安全保障上のサイバー脅威に効果的に介入する必要性に対応できないため、推奨しない。したがって、最終候補評価の対象とはならなかった。

上記の表にまとめた重要成功要因に基づき、選択肢のロングリストを評価した結果、選択肢 2 が「何もしない」というベースラインと共に、最終候補として選定される唯一の現実的な選択肢であると識別された。したがって、この措置を進める上で選択肢 2 が優先される。

6. 次段階へ進んだ政策案の概要

重要成功要因を用いた選定

前節で述べた通り、各分野において可能な限り潜在的な改革案のロングリストを作成した。各案は識別された課題に対処するよう設計されている。これらを合意された重要成功要因に基づいて評価し、戦略的適合性、予想される有効性、実現可能性を明らかにした。この分析の結果、各分野で 1 つの実行可能な介入案が残った。これらを総合すると、以下の最終候補評価に進む優先案を構成する。「何もしない」という選択肢も最終候補評価に持ち越された。これは選択肢評価における標準的な手法である。ただし、後述の通り、これは推奨される選択肢ではない。

選択肢 1：現状維持

「何もしない」シナリオでは、英国における 2018 年 NIS 規則は現状のまま変更されない。これは、重要サービス及びデジタルサービスのサイバーレジリエンス強化と英国の国家安全保障保護という政府目標との戦略的適合性が低い。本シナリオは優先案に対する対照事例として機能する。

この選択肢では、NIS 規則を更新し、新たな事業体や分野を適用範囲に含めるための十分な権限が得られない。そのため、主要な立法措置なしでは NIS 規則を効果的に運用できず、変化し続けるサイバー環境において規則の適切性を維持することが困難となる。このシナリオでは、EU が NIS 2 を推進し新たな事業体を追加し、オーストラリアが重要サプライチェーン指定を法改正で盛り込む一方で、英国はサイバーセキュリティ規制において国際的なパートナーに後れを取る。このため、選択肢 1 は国際的な先例との戦略的整合性が弱い。

英国における敵対的サイバー活動は、その強度・頻度・高度化が進み、公共の安全、経済、国家安全保障に具体的な影響を与えている。NIS 規則を変更しなければ、サイバー攻撃による混乱や業務停止がより頻繁に発生する可能性が高い。これは個々の企業の競争力とビジネス環境全体の双方に悪影響を及ぼす。

さらに、サプライチェーンの脆弱性は悪用され続け、英国市民に被害をもたらす。このシナリオでは、2024 年に NHS 主要サプライヤーを襲ったランサムウェア攻撃（外来予約・選択的手術 11,000 件以上が延期）と同様のサイバー攻撃に対し、英国は不十分な防衛状態を継続することになる。OES と「重要サプライヤー」間の市場力の不均衡により、これは契約手段では解決できない。サプライチェーンが拡大・複雑化するにつれ、NIS 規則のこの欠陥は敵対的アクターに悪用される可能性が高まる。

NIS 規則を更新しなければ、英国の国家安全保障は国家支援型脅威アクターに対する脆弱性を抱え続ける。NCSC の 2024 年次報告書は脅威環境を「拡散し危険な状態」と表現し、敵対国家や組織犯罪による持続的攻撃を指摘している。³⁹ 2018 年 NIS 規則は、英国が現在直面するサイバー脅威に対して既に時代遅れであり、サイバー犯罪者が手法を進化させ続ける中でこの脆弱性は悪化する一方だ。

選択肢 2：基本法による対応

推奨される選択肢は、第 5 節で概説した優先改革案の一次立法パッケージである。この一連の選択肢は、絶えず変化するサイバー環境において、サイバーレジリエンスと 2018 年 NIS 規則の将来対応性を確保するという政府の目標を達成すると同時に、企業や重要サービスに過度の負担をかけない環境を維持することが期待される。本影響評価では、今後、推奨選択肢のコストと便益を、ベースラインとなる「何もしない」シナリオと比較して評価する。下表は、最終候補となった二つの選択肢が重要成功要因（CSF）に対してどのように評価されるかを示す。

³⁹NCSC [年次レビュー](#)、2024 年

表 6.1 : 重要成功要因に基づくパッケージの順位付け

政策選択肢	戦略的適合性	有効性 - 国民が依存し、経済安定と国家安全保障の基盤となる最重要国家インフラの防御に不可欠な事業者が、適切に対象範囲に含まれているか？	有効性 - ネットワークと情報システム規制に関する規制当局の職務遂行能力を向上させるか？	有効性 - 絶えず変化するサイバー環境において、NIS 規制自体が適切であることを確実にするか？	実現可能性
何もしない	低い	低い	低い	低い	高
基本法	高	高	高	高	高

7. 社会的正味現在価値（NPSV）：各候補案の金銭的・非金銭的コストと便益（行政負担を含む）

コスト

表 7.1：施策別コスト内訳

コスト、現在価値、2025年、中央推定値（百万ポンド）	施策	金銭的価値？ 非金銭的価値？ 両方か？	直接？ 間接？ 両方か？	二次立法が 続くか？
7億9600万ポンド	1. 関連するマネージドサービス・プロバイダー（RMSP）をNIS規則の適用範囲に含める。	金銭的価値	直接	いいえ
1億4900万ポンド	2. データセンターインフラをNIS規制の対象範囲に含める。	金銭的価値	直接	いいえ
4000万ポンド	3. 電力部門向けの新たなエネルギー必須サービス（負荷制御）をNIS規制の対象範囲に含める。	金銭的価値	直接	いいえ
該当なし	4. 規制当局が重要供給業者を指定できるようにする。	非金銭的価値	直接	はい
2億100万ポンド	5. インシデント報告の改善。	金銭的価値	直接	はい
該当なし	6. 情報共有規定を強化する。例えば、規制当局同士や規制当局と公的機関が相互に情報を共有できるようにする。	非金銭的	直接	いいえ
該当なし	7. 情報委員会がリスクに関連する情報を収集できるようにする。	非金銭的価値	直接	いいえ
該当なし	8. 規制当局のコスト回収メカニズムを改善する。	非金銭的価値	直接	いいえ
該当なし	9. 戦略的優先事項の声明を指定するために SoS を有効にする。	非金銭的価値	直接	いいえ
該当なし	10. 執行メカニズムを強化する	非金銭的価値	直接	はい
該当なし	11. 委任された権限 - 新たな脅威に対応できるよう規制枠組みを適応させること。	非金銭的	直接	はい - 将来必要に応じて
該当なし	12. セキュリティとレジリエンスの要件。	非金銭化	直接	はい
該当なし	13. 政府がサプライチェーンの安全性を向上できるようにする。	非金銭的価値	直接	はい
該当なし	14. 国家安全保障上必要である場合、国務長官が規制当局に指示する権限を導入する。	非金銭的価値	直接	いいえ
該当なし	15. 国家安全保障上必要である場合、国務長官が規制対象事業体に指示する権限を導入する。	非金銭的価値	直接	いいえ

広範な影響

表 7.2：カテゴリー別の広範な影響の内訳

広範な影響 (百万ポンド)	カテゴリー	金銭的価値？非金銭的価値？ 両方か？	直接？間接？両方か？
該当なし	中小企業（SMEs）	非金銭的価値	間接
該当なし	データセンター事業者向け小規模・零細企業アセスメント	非金銭的価値	間接
該当なし	競争への影響	非金銭的価値	間接的影響
該当なし	平等への影響	非金銭的価値	該当なし
該当なし	個人への影響	非金銭的価値	該当なし
該当なし	環境への影響	非金銭的価値	該当なし
該当なし	国家安全保障への影響	非金銭的価値	直接
該当なし	セクター別影響	非金銭的価値	間接
該当なし	貿易への影響	非金銭的価値	間接的

一部の措置に伴う負の正味現在価値にもかかわらず、サイバー攻撃の発生率と影響が「何もしない」選択肢と比較して減少すると予想される点を中心に、重要な非金銭的便益が識別されている。この便益は、NIS 規制の対象となる事業体を拡大し、規制の執行を強化し、情報共有を促進することで実現される。

前提条件、リスク及び方法論

優先される改革パッケージを分析した結果、潜在的なコストと便益の推定値を以下に示す。これらは 2026 年から 2035 年までの 10 年間で評価され、グリーンブックが推奨する割引率 3.5%を用いて割り引かれている。

法案に含まれる特定の政策について既に分析が公表されている場合は、それに応じて参照している。本影響評価は、これらの特定措置による追加的影響に焦点を当てており、既に施行されている NIS 規制から生じる既存のコストは評価対象外である。

政策の予想される影響は、主に NIS 規制の対象となる組織、NIS の実施を担当する規制当局、および NIS 規制対象組織のサービスを利用する一般市民に及ぶ。

十分な確固たるデータが利用可能な場合、DSIT は各種改革の金銭的影響を推定した。この証拠がまだ利用できない場合、DSIT は潜在的なコストと便益の詳細な概要を提供し、関連する二次立法の前に証拠の不足が対処されるか、本影響評価の末尾にある我々のモニタリング及び評価計画で参照されることを確保した。

サイバー分野の特性上、金銭的便益に関する証拠は現時点で限定的である。本節ではまず、「何もしない」選択肢と比較した改革パッケージ実施の直接的な非金銭的便益を検討する。これは当初、定性的に、かつ期待される便益を示す関連事例研究を用いて行われた。便益の潜在的な規模を示すための定量化も一部提供されている。

本法案は、重要デジタルサービスのサイバー防御を強化し、英国に対する増大・新興脅威へのレジリエンスを構築する。これは長期的な成長と英国の国家安全保障を守る上で不可欠である。より明確なセキュリティ標準と期待値を設定することで、本法案はサイバーインシデントに対する英国のレジリエンスを高め、「何もしない」選択肢と比較してサイバー攻撃によるコストを削減する。進化する脅威への対応が困難な中小企業は、特にこの改革の恩恵を受ける可能性がある。

これらの政策により英国企業や規制当局が直面する可能性のある直接的・間接的コストの概要は、「コスト」セクションで示されている。

8. メリット

要約 – 何もしない選択肢

「何もしない」選択肢は現状維持を意味するため、追加的な直接的・間接的利益は生じない。

概要 – 選択肢 1

1. 直接的便益：
 - a. 非金銭的：
 - i. セキュリティ上の利益
 - ii. サイバー攻撃の影響を軽減する
 - b. 定量化
 - i. 参考となる損益分岐点分析
2. 間接的便益
 - i. 競争上の利点

直接的利益

非金銭的価値

企業が壊滅的なサイバー攻撃を恐れることなく事業を展開できる、安全で強固な環境は経済成長に不可欠である。だからこそ、何もしない選択肢と比較した場合、本法案の主な利点は、投資と革新が育まれる環境を促進するため、企業をサイバー攻撃から防御することにある。より多くの事業体を対象範囲に含め、規制当局がより効果的に職務を遂行できるようにすることで、サイバー攻撃に対する防御力を強化する。これにより、企業はサイバー攻撃への対応に要する時間を短縮でき、サービス停止を回避できる場合が多い。攻撃が発生した場合、改善されたインシデント報告により、規制当局や NCSC は情報を活用して他の企業や組織に助言・指導を行い、連携を図ることができる。これにより、各組織は自らを防御し、特定の攻撃や攻撃の種類による広範な影響の緩和のための措置を講じられるようになる。

より具体的には、これらの措置は本影響評価で先に識別された主要な市場の失敗に対処する利点を持つ：

- **外部性** – 規制執行方法の改善、適用対象となる事業体の拡大、規制標準の更新といった措置は、サイバー攻撃の発生頻度と影響、および経済全体への波及効果を低減する効果を持つ。
- **不完全情報** – 規制対象事業体間および政府／規制当局との情報共有を強化する措置は、市場における情報非対称性を含む不完全情報を減らし、これもまたセキュリティを向上させる。
- **調整の失敗** – 関連するより多くの事業体を規制対象に含め、情報共有を促進する措置により、ネットワークのより大きな割合でセキュリティが強化される。

本法案の期待される便益を金銭換算することは不可能であったが、ケーススタディを用いて便益を定性的に説明し、損益分岐点分析の概念を用いて便益規模の指標的定量化を行った。

これらの措置の具体的な便益は、法案の変革理論（表 4.1）に示される期待される成果と結果に由来する：

表 8.1：期待される成果と結果

成果	成果
RMSP のサイバーセキュリティとレジリエンスの向上	公共サービスと企業を防御し、市民が日常生活を送れるようにする
データセンターのサイバーセキュリティとレジリエンスの向上	
大規模負荷制御装置のサイバーセキュリティとレジリエンスの向上	
サプライチェーンリスクの監視体制強化	
全セクターの規制当局が NIS 規則を一貫した方法で実施する	規制当局が NIS 規則を実施する十分な体制を整え、経済成長を促進する安定した環境を創出する
企業が規制当局による監視の効率化を通じて、法的要件をより明確に理解する	
規制当局と NCSC が脅威の状況を包括的に把握する	
情報委員会はサイバーリスクの識別と緩和に積極的なアプローチを取る	
規制当局は職務を効果的に遂行する資源を確保する	
罰則体系の改善とより均衡の取れた金銭的制裁により、規制当局の規制執行能力が向上する	
法令は関連性と有効性を維持している	英国の国家安全保障を強化し、脅威の状況が変化する中で NIS 規制が効果を維持することを確保する
規制対象事業者は、国家安全保障に重大なリスクをもたらす脅威やインシデントに迅速に対処する	
より高く、より比例した最高罰金の抑止効果の結果として、NIS 義務への遵守が向上する	
リスクが高まった時期に、各セクターがより厳格なセキュリティ対策を採用する	

各個別措置は、以下に示す期待される効果をもたらす。

表 8.2：各措置の要約された効果と関連する根拠

措置	効果の概要	該当する場合の根拠
規制枠組みの対象となる事業者を拡大する		
	IT システムのセキュリティを強化し、サイバー攻撃のリスクを低減する。これにより、外部不経済を減少させる。	オペレーション・クラウドホッパー：数年かけて実施され、2016 年に激化したこのキャンペーンは、
関連するマネージドサービス・プロバイダー (RMSP) を NIS 規制の対象範囲に組み入れる。	IT システムのセキュリティを強化し、サイバー攻撃のリスクを低減する。これにより、RMSP の顧客に対する攻撃の悪影響という負の外部性を軽減する。これらの投資は、デジタル経	オペレーション・クラウドホッパー：数年にわたるキャンペーンで、2016 年に活発化した作戦である。APT10 と呼ばれるグループによって実行された。MSP (マネージド

	<p>済における信頼できるパートナーとしての RMSP の立場を強化する</p>	<p>サービスプロバイダー) を標的とし、それらの MSP および世界中の顧客が保有する知的財産や機密データへのアクセスを狙った。⁴⁰ 英国及びその同盟国は、APT10 が中国国家安全部の代理として活動していると公に断定している。</p> <p>このキャンペーンの主目的は、即時の金銭的利益（ランサムウェア攻撃に見られるような）ではなく、長期的な優位性と利益を得るための諜報活動と知的財産窃取であった。持続的アクセスの除去、フォレンジック調査の実施、強化されたセキュリティ対策の導入といった修復作業には、数か月あるいは数年を要する場合がある。必要な膨大な人件費と相まって、その財務的コストは数百万単位にまで膨れ上がる可能性がある。</p>
<p>2. データセンターインフラを NIS 規制の対象範囲に含めること。</p>	<p>データセンター及びその支援・稼働基盤の保護を強化し、障害や侵害リスクを低減するとともに、ネットワーク全体への波及影響を軽減する。この措置により、事業者は経済全体にわたる適切なレジリエンシー対策を講じ、私的インセンティブと公共の利益を整合させる。データセンターを規制対象に含めることで、インシデント報告義務も課され、データセンターと政府／規制当局間の情報格差が縮小される。</p>	<p>2022 年 7 月、ガイズ・アンド・セント・トーマス NHS トラストにサービスを提供する 2 つの別々のデータセンターが、猛暑に関連した障害に見舞われた。これにより、ガイズ病院、セント・トーマス病院、エヴェリナ・ロンドン病院の臨床 IT システムの大半と、関連する地域医療サービスが停止した。IT システムの喪失は、トラスト内の臨床サービス運営と患者ケアに大規模かつ広範な混乱をもたらし、さらにこのインシデントへの対応として技術サービスに計画外の支出 140 万ポンドを発生させた。⁴¹</p>
<p>3. 電力部門向けの新たなエネルギー重要サービス（負荷制御）を NIS 規制の対象範囲に追加する。</p>	<p>大規模負荷制御事業者に対しサイバーセキュリティ要件を課すことで、堅牢な防御への投資を促す。負荷制御事業者と政府／規制当局間の情報共有を促進することで、における情報の非対称性を改善する効果もある。これによりサイバー攻撃リスクと広域送電網への混乱が軽減される。スマート家電の利用促進につながり、政府のネットゼロ目標達成に寄与する。</p>	<p>ロンドンにおける電力配電網へのサイバーフィジカル攻撃による GDP 損失は、2,060 万ポンドから 1 億 1,140 万ポンドの範囲に及ぶ可能性がある。⁴²</p> <p>2024 年 IBM データ侵害コスト報告書によると、エネルギー分野におけるデータ侵害の平均コストは 488 万ポンドに達した。</p> <p>488 万ドルに達した。⁴³</p>
<p>4. 規制当局が重要供給業者を指定できるようにする。</p>	<p>重要サプライヤーの指定を可能にすることで、この措置は重要サービスのセキュリティを向上させ、サイバー攻撃に伴う負の外部性を低減</p>	<p>NHS 病理検査プロバイダ Synnovis へのサイバー攻撃は、推定 3,270 万ポンドの損失をもたらし、2024 年と 2025 年の</p>

⁴⁰[オペレーション・クラウドホッパー](#)

⁴¹[ガイズ・アンド・セント・トーマス病院重大インシデント検証報告書](#)

⁴²保守的なシナリオに基づく。「電力配電インフラネットワークに対するサイバーフィジカル攻撃」、Oughton, E, 2019 年

⁴³[IBM, 2024 年](#)

	<p>する。主要サプライヤーの可視性を高め、セクター横断的なリスク管理の一貫性を確保し、経済成長・国家安全保障・経済的回復力という英国の戦略的優先事項に沿った国家レジリエンスを強化する。</p>	<p>利益を損なった。これは 2023 年の報告利益 430 万ポンドと比較される。患者や広範なサプライチェーンにも重大な追加コストが生じた。</p>
<p>規制当局がコンプライアンスを推進し、その職務を遂行するために必要な資源と重要な情報を確保できるよう権限を与える。</p>		
<p>5. インシデント報告の改善。</p>	<p>NIS（ネットワーク・情報セキュリティ）分野におけるインシデント発生時、規制当局と NCSC（国家サイバーセキュリティセンター）が迅速に通知を受ける体制を確立し、英国のサイバー攻撃レジリエンスを強化する。これにより、規制当局、NCSC、企業などの主要関係者が、進化するサイバー脅威に関する必要なリアルタイムデータまたは完全なデータを入手できるようになり、市場における情報の不完全性が減少する。ユーザーは、サービス中断やシステム侵害への対応時に、適切な緩和措置を講じられるようになる。さらに、透明性要件はサービス提供者全体の基準を引き上げ、顧客は利用するサービスについてより正確な情報を得られるようになる。</p> <p>サービス中断やシステム侵害への対応として、緩和措置を講じられるようになる。さらに、透明性要件によりプロバイダの標準が向上し、顧客は依存するサービスが影響を受ける可能性がある場合に、より適切な情報を得られるようになる。</p>	<p>インシデントの報告は攻撃被害を最小限に抑えるために不可欠である。ENISA によれば、報告されない、あるいは遅れて報告されるインシデントは復旧が困難となる。⁴⁴</p>
<p>6. 情報共有規定を強化する。例えば、規制当局同士や規制当局と公的機関が相互に情報を共有できるようにする。</p>	<p>共有可能な情報の範囲、共有主体及び共有先について、より明確な基準を設ける。これにより、規制当局の機能発揮が支援され、国家安全保障・重要インフラ・サイバーレジリエンスに関する政府政策の策定に資する。さらに NIS 枠組みとその実施状況の効果的な評価を可能にする。これもまた、市場に存在する情報の非対称性を軽減する。</p>	<p>これらの措置は、効果的な規制体制を促進し、本節で述べたセキュリティ上の利点を支えるために必要である。</p>
<p>7. 情報委員会がリスク関連情報を収集できるようにする。</p>	<p>市場に存在する不完全な情報のレベルを低減し、情報委員会がより積極的な監督アプローチを取れるようにする。これにより、情報委員会は規制対象のデジタルサービス及び管理サービスに対するリスクアセスメントを向上させ、組織がシステムを保護するための措置を講じるよう積極的に支援することが可能となる。</p>	

⁴⁴ENISA, 2024 年

8. 規制当局のコスト回収メカニズムを改善する。	回収可能な規制コストの制限に対処し、規制違反の財政的負担が納税者に転嫁されるのを防ぐ。これにより、より透明性が高く、強固で信頼できる規制環境を促進する。サイバーセキュリティ規制の提供をより持続可能かつ効率的にし、国民と経済に利益をもたらす。	
9. 戦略的優先事項声明の指定を可能とする。	NIS 規則が各セクターで一貫性を持って効果的に適用されるよう、適切かつ可能な範囲で確保する。制度の一貫した執行不足の是正に取り組むことで、規制対象事業者ネットワークの一部で現在不足している良好なサイバーセキュリティの提供を改善する。これにより規制がより均等に分配され、ネットワーク全体のサイバーセキュリティに攻撃者に悪用される可能性のある最小限の隙間しか生じなくなる。	
10. NIS 規則の執行メカニズムを強化する	規制当局が比例的かつ一貫した罰金を科すことを可能にすることで、効果的な規制体制を促進する。これにより規制への順守が向上し、ひいては英国のサイバーレジリエンスが強化される。	
NIS 規制が絶えず変化するサイバー環境に対応し、政府が国家安全保障の防御のための断固たる措置を講じられるよう整備する。		
11. 委任権限 - 新たな脅威に対応可能な規制枠組みを確保する	NIS 規則が関連性・強固性・比例性を維持できるよう更新を可能にし、重要サービスに対するサイバー攻撃からの継続的な防御を確保する。これにより政府と国民双方が利益を得る。	これらの措置は、政府が規制対象事業者のセキュリティ要件を更新し、英国が現在および将来直面するサイバー脅威に対して十分な防御を確保するために必要である。
12. セキュリティ及びレジリエンス要件。	政府がデジタルサービスを提供する企業に対して明確な期待値を設定することを可能にし、脅威環境の変化に応じてこれらの要件を更新する手段を提供しながら、適切かつ最新のセキュリティ要件が整備されることを保証する。これにより、標準が現実世界のリスクに適合し、不確実性が低減され、サイバーセキュリティが向上する。また、企業、規制当局、一般市民間の透明性が向上し、情報の非対称性が減少するため、より情報に基づいた意思決定が可能となり、デジタル市場全体の安全性が向上する。また、政府がこれらの要件をデジタルサービスプロバイダ（例：OES）を超えて拡大することを可能にし、より幅広い事業分野におけるサイバー衛生の水準向上を図る機会を提供する。	
13. 政府がサプライチェーンの安全性を向上させることを可能にする。	サプライチェーンの効果的な監視を確保し、重要サービスやデジタルサービスへの重大な混乱リスクを低減する。これにより国家のサイバーレ	昨年、直近のサプライヤーがもたらすリスクを評価していると回答した企業は 1 割強（14%）に過ぎず、より広範なサプライ

	レジリエンスが強化され、重要インフラへの信頼が向上する。	チェーンを検討している企業は 1 割未満であった ⁴⁵
14. 国家安全保障上必要と判断される場合、国務長官が規制当局に指示する権限を導入する。	脅威が高まった際に政府が規制当局に指示する権限を与えることで、国家安全保障の防御のための迅速な行動を規制当局が取りやすくなる。	近年の出来事は、紛争時のサイバー攻撃が世界経済に与える損害を明らかにした。政府はこうした紛争への対応として、リスク最小化のための指示発出が必要と判断する可能性がある。クリミア附属書後のロシアは、関連組織による持続的なサイバー攻撃を継続した。2015 年のウクライナ電力網攻撃では 23 万世帯が停電し、2017 年のランサムウェア攻撃は予算責任局の試算で世界経済に最大 100 億ドルの損害をもたらした。 ⁴⁶
15. 国家安全保障上必要と判断される場合、国務長官が規制対象事業体に指示する権限を導入する。	脅威が高まった際に政府が規制対象事業者に強力なセキュリティ対策を義務付ける権限を与えることで、規制対象事業者が重要な情報に基づいて行動することを強制し、システム全体のレジリエンスを強化する。これにより、緊張が高まった時期に NIS 規制対象事業者が悪意のあるサイバー活動からより良く防御され、サービスへの混乱レベルが低減される。	

これらの措置を総合することで、経済のサイバー攻撃に対するレジリエンスが強化され、関連コストが削減される。

セキュリティ上の利点

これらの措置は、組織内におけるサイバーセキュリティへの理解と支援の促進が期待される。これは NIS 2 指令の成果であり、重要経済サービス事業者の 71%が取締役会によるサイバーセキュリティ支援の増加を、43%が規制により組織の総合リスク理解が改善したと報告している。⁴⁷

サイバー攻撃の影響を軽減する

何もしない場合と比較して、サイバー攻撃の頻度と影響を軽減することは、マクロ経済レベルでの利益だけでなく、影響を受けた個々の組織にも利益をもたらす。過去 12 ヶ月間に何らかのサイバーセキュリティ侵害や攻撃を経験したと報告した企業は 43%である。中規模・大規模企業ではこの割合がそれぞれ 67%、74%に上昇する。侵害や攻撃を識別した 43%の企業のうち、約 5 社に 1 社が金銭やデータの損失といった悪影響を経験している。⁴⁸

さらに、サイバー犯罪者は重要インフラ（CNI）を攻撃対象として増加させており、重要サービスを収益性の高い標的と見なしている。プライドウェル・コンサルティングが委託した独立調査によると、インタビュー対象の CNI の 86%が過去 12 ヶ月間にシステムへのサイバー攻撃を検知していた。この 86%のうち、93%が過去 12 ヶ月間に少なくとも 1 回の攻撃成功を経験している。⁴⁹

以下の事例研究は、サイバー攻撃が一般市民に与える壊滅的な影響と、これらの対策が影響軽減にどう役立つかを示している。重大なサプライチェーンにおける供給業者の混乱が、英国の市民に広範な影響を及ぼし得ることを、実際のインシデントが証明している。

⁴⁵[サイバーセキュリティ侵害調査 2025 - GOV.UK](#)

⁴⁶[ロシアのウクライナ侵攻時のサイバー攻撃 - 予算責任局](#)

⁴⁷NIS PIR 2022

⁴⁸[サイバーセキュリティ侵害調査 2025 - GOV.UK](#)

⁴⁹[CNI サイバー報告書：リスクとレジリエンス（プライドウェル・コンサルティング委託）](#)

サプライチェーンの責務 - Synnovis ランサムウェア攻撃（2024年6月）

NHS 病理検査プロバイダ Synnovis へのサイバー攻撃は、推定 3,270 万ポンドの損失をもたらし、2024 年と 2025 年の利益を損なった。これは 2023 年の報告利益 430 万ポンドと比較される。このランサムウェア攻撃により、ロンドンでは数ヶ月にわたりサービスが混乱し、ガイズ・アンド・セント・トーマス NHS 財団トラストおよびキングス・カレッジ NHS 財団トラストでは数千件の選択的手術と外来予約が延期された。この攻撃による人的影響は明らかであり、11,000 件以上の急性期外来予約と選択的手術が延期された。本法案により、政府は規制対象事業体にサプライチェーンリスクマネジメントの義務を課し、規制当局は少数の重要供給業者を指定できるようになる。

本影響評価で示された対策の一部は、連携強化、インシデント報告、情報共有の改善を目的としている。脅威や脆弱性に関する情報共有の拡大は、例えば公共機関における予防措置の実施や規制当局の機能向上を通じて、影響規模の縮小に寄与する。報告体制の改善により、規制当局、政府、NCSC は変化する状況をより深く理解できるようになる。これにより必要な支援が提供され、将来の政策立案に資する情報を得られる。

インシデント報告の改善 - NHS トラスト

2023 年、ランサムウェア攻撃がファイル転送プラットフォーム「MoveIt」の脆弱性を悪用し、英国企業と米国エネルギー省が被害を受けた。同年、サイバー犯罪者がダークウェブに身代金要求文を掲載し、NHS トラストから個人データを盗んだと主張した。現行の NIS 規則では、いずれも重要サービスの継続性に重大な影響を与えなかったため報告対象外であった。法案下では、これらのインシデントは報告対象となる。サービス継続性を妨害する可能性、あるいはシステムの機密性・可用性・完全性に影響を与える可能性があるためだ。これにより規制当局は、将来の NHS サービス提供を妨害する戦術を理解し、防御策を講じることが可能となる。

国際的なインシデントは、国家のサイバー活動主体が国家安全保障を脅かす能力を有することを示している。政府に指示権限を与えることは、差し迫った脅威が生じた際に断固たる行動を取る能力を政府に与えるという重要な利点をもたらす。

指揮権限 - ボルト・タイフーン

中国政府が支援するサイバー作戦「ボルト・タイフーン」が最近、米国の重要インフラを侵害した。ボルト・タイフーンは「現地調達」戦術を用い、攻撃者が目立たず活動できるようにしている。悪意のある活動が正当なシステム・ネットワーク動作に紛れ込むため、検知が困難だ。米国情報機関は、このサイバー攻撃主体が、米国との重大な危機や紛争発生時に米国インフラを攻撃するため、IT ネットワーク上に潜伏しようとしていると評価した。法案の指示権限措置により、国務長官は規制対象事業体に対し攻撃の影響緩和を指示できる。この指示権限は重要国家インフラへの有害な攻撃の影響を防止・軽減し、国家安全保障上の利益を保護する。これにより、規制対象サービスへの攻撃による重要サービスの混乱や機密データの侵害リスクが低減される。

成長の便益

安全で堅牢なデジタルサービスは、企業が繁栄するための安定した安全な環境を創出し、投資を呼び込み、最先端技術の開発を促進する。この安定性は、個々の企業の競争力を高めるだけでなく、ダウンタイムや業務中断を減少させることで、経済全体の進歩を推進する。

レジリエンスのあるサイバーインフラは、新たなアイデアや技術を構築するための安全な基盤を提供することでイノベーションを促進し、英国が世界の技術進歩の最前線に立つ地位を維持するために不可欠である。必須のサイバー防御策の導入を拡大することで、より多くの事業体をサイバー攻撃から防御し、投資とイノベーションが育まれる環境を醸成する。

直接的な便益 - 定量化

対策への準拠には企業にとってコストが発生する可能性があるが、セキュリティとレジリエンスを強化することで、「何もしない」選択肢と比較した場合のサイバー攻撃による推定コスト削減に寄与する。ただし、回避された攻撃の数を推定できないため、これらの特定対策によって回避されるコストの割合を算出することは不可能である。NIS PIR で示されている通り、NIS 対策に直接起因するインシデント減少に関する証拠は不十分である。したがって、2018 年 NIS 規則が導入されなかった場合、あるいはこれらの追加対策が導入されなかった場合に発生したであろうインシデント数を、確固たる対照事例として構築することは不可能である。

影響評価で概説された更新版 NIS 規制の主な利点は、「何もしない」選択肢と比較して、セキュリティの改善が期待され、それにより重要サービスに対するリスクが低減される点である。これは、経済生産と社会の福祉を支えるためにこれらのサービスに依存しているため、ひいては英国の経済的繁栄に寄与する。これらの利益は、保護対策の強化による重大な混乱を招くインシデント数の減少と、適切なインシデント対応計画の整備による影響の軽減の両方から生じると予想される。

本法案の具体的便益を正式に金銭換算することは不可能であったが、DSIT は 2024 年から 2025 年にかけて政府横断的な関係者と連携し、サイバー攻撃の経済的コストを定量化する手法、ひいてはその防止による潜在的価値の把握に努めてきた。これらの知見を活用し、本措置による便益の指標的定量化が可能となる。

DSIT は本「サイバー定量化プロジェクト」⁵⁰を開始した。これは消費者、政府、企業を含む全ての事業体に対するサイバー攻撃の経済的コストを定量化しようとするものである。本プロジェクトの最終成果物は、英国経済に対するサイバー攻撃の潜在的影響に関する包括的見解を提供する。本作業の初期知見は、DSIT が発注した以下の初期報告書に基づいている：

- サイバー攻撃のセクター別コスト経済モデリング（KPMG、2025 年） — 本報告書からの知見は、以下の企業分析における利益を裏付けるために使用されている。

結果は重要な仮定に基づいており、したがって洞察はあくまで参考として扱うべきである。以下の推定損益分岐点は、平均的な年間スナッフショットに基づいており、今後数年間におけるサイバー攻撃の発生頻度やコストの潜在的な変化は考慮されていない。

ビジネスへの便益

⁵¹KPMG の推計によれば、英国における個々の企業に対する重大なサイバー攻撃の平均コストは 194,729 ポンド（2024 年価格）である。重大なサイバー攻撃を経験すると推定される英国企業の割合に基づいて規模を拡大した場合、モデル化により、英国経済レベルでの企業への総コストは 147 億ポンドと推計される。これは英国経済全体の 0.5% に相当する。

⁵²ただし、経済全体へのサイバー攻撃の総コスト推定値は手法によって大きく異なり、直接的な混乱や二次的影響から生じる広範な経済的・福祉的コストを考慮するかどうかで結果が大きく左右される点に留意が必要だ。⁵³

KPMG はまた、業種別・企業規模別にサイバー攻撃が企業に与える平均コストを推定している。報告書には全業種の情報が含まれるが、NIS 規制の対象となる企業にとって最も関連性が高いのは 3 業種である。すなわち公益事業、運輸、医療である。情報セクターは、新規規制対象となる MSP（マネージドサービスプロバイダー）およびデータセンターに分類さ

⁵⁰<https://www.gov.uk/government/publications/independent-research-on-the-economic-impact-of-cyberattacks-on-the-uk>

⁵¹サイバーセキュリティ侵害調査の数値を使用している

⁵²この図は 2024 年の市場価格および現行価格による GDP を使用している

⁵³[サイバーインシデントのコスト：系統的レビューと交差妥当性確認](#)

れる事業者にも最も関連性が高い。一方、公益事業は新たに導入された大規模負荷制御事業者にとって最も関連性が高い。中小企業は一般的に NIS の対象外であるため、注目すべき企業規模は大企業となる。企業当たりの推定コストは下記の表に示す通りである：

表 8.3 : 公益事業、運輸、医療セクターの大企業に対するサイバー攻撃の推定コスト

業種	当該セクターの大企業に対するサイバー攻撃の推定コスト
公益事業	436,443 ポンド
運輸	951,443 ポンド
医療	483,312 ポンド
情報	1,101,588 ポンド

KPMG の試算によれば、特定の種類の攻撃は特に多大なコストを伴う可能性がある。これには詐欺・不正行為、システム障害、システム侵入が含まれる。これらの攻撃を回避できれば、攻撃 1 件あたりの利益はさらに大きくなる。水・エネルギー・交通機関の混乱が人や企業に与える影響、医療予約のキャンセルなど、より広範な回避可能な影響もコストに反映されれば、攻撃 1 件あたりの利益はさらに増大するだろう。

新規規制対象企業

本影響評価で推定されたコストの大部分は、本法案により NIS 規制の対象範囲に組み込まれる事業者が生じる。以下のコスト項目では、MSP、データセンター、大規模負荷制御装置の 3 事業グループに対するコストを金額化した。これらの事業者に対する年間直接コストは 1 億 2500 万ポンドと推定される。内訳は MSP とデータセンターが合計 1 億 2000 万ポンド、大規模負荷制御装置が 500 万ポンドである。

しかし、本法案は「何もしない」選択肢と比較して、これらの企業が被ると予想されるサイバー攻撃のコスト削減を通じて、大きな利益をもたらす。これらの利益を金銭換算することは不可能だが、損益分岐点分析により、これらの企業にとってコストを正当化するために必要な利益の規模を示すことができる：

$$\text{損益分岐点} = \frac{\text{規制順守による企業の年間コスト}}{\text{個別企業へのサイバー攻撃推定コスト}}$$

KPMG による関連セクターへの攻撃コスト推計値は、新規規制対象企業へのサイバー攻撃コストの代用指標として使用できる。MSP やデータセンターについては情報セクターの攻撃コストを、大規模負荷制御事業者については公益事業セクターのコストをそれぞれ適用する。両セクターとも、表 8.3 に示す攻撃コストの推定値を中心値として用い、高値推定には 20% 増、低値推定には 20% 減のコストを適用する。コストを正当化するために回避すべき攻撃回数は次のように推定できる：

表 8.4 : 新規規制対象企業における損益分岐点分析の結果

MSP およびデータセンター

シナリオ	攻撃あたりのコスト	損益分岐点に達するまでに回避すべき攻撃回数（年間）
------	-----------	---------------------------

低	881,270 ポンド	136
中	1,101,588 ポンド	109
高	1,321,906 ポンド	91

大型負荷制御装置

シナリオ	攻撃あたりのコスト	損益分岐点に達するまでに回避される攻撃数（年間）
低	349,154 ポンド	14
中	436,443 ポンド	11
高	523,732 ポンド	9

したがって、中央シナリオでは、MSP やデータセンターが規制を順守した結果、年間 109 件以上の追加攻撃を回避できた場合、順守コストは順守による利益を上回る。大規模負荷制御装置については、11 件の攻撃回避が必要となる。参考までに、中央シナリオでは新規規制対象企業が 863 社と推定される。2024 年には英国経済全体で 6,000 の大企業がサイバー侵害または攻撃を受けた⁵⁴。

この介入による利益の規模を示す別の方法は、本影響評価における「何もしない」選択肢の下での潜在的コストを検討することだ。新規規制対象企業各社がサイバー攻撃を受けたという仮定シナリオでは、総コストを推定できる。その数値は下表 8.5 に示す通りである。NIS 規制遵守によるこれらの企業への年間コスト 1 億 2500 万ポンドと比較すると、理論上の潜在的利益が明らかに大きいことが明らかだ。

表 8.5 : 本法案により NIS 規制の対象となる事業者が被る年間総コスト（各事業者が 1 回の攻撃を受けるという理論的状況下での中心推定値）

事業種別（中央値）	事業者数	攻撃 1 件あたりのコスト（中央値）	総コスト（1 事業者あたり 1 回の攻撃）
MSP	788	1,101,588 ポンド	8 億 6800 万ポンド
データセンター	64	1,101,588 ポンド	7100 万ポンド
大型負荷制御装置	11	636,443 ポンド	480 万ポンド
合計			9 億 4300 万ポンド

⁵⁴サイバーセキュリティ侵害調査、2025 年

既に規制対象となっている事業者

本法案により、既に規制対象となっている事業者に追加コストが発生する。主に、下記の「コスト」セクションで説明する通り、これらのコストは新たなインシデント報告のタイムライン要件に起因するものである。既存規制対象事業者への年間直接コストは、OESとRDSPの両方を含め1,200万ポンドと推定される。NIS PIR 2022から、特定業種に該当する規制対象企業の数を推定できる。この割合を用いることで、各業種内の事業者へのコストを推定可能であり、これを当該業種におけるサイバー攻撃の推定コストで割ることで、各企業ごとの損益分岐点を識別できる。

表 8.6 : 既存規制対象事業者における損益分岐点分析

セクター	推定企業数	これらの企業にかかる推定追加コスト	当該セクターにおけるサイバー攻撃の推定コスト	損益分岐点
公益事業 (OES)	210	240 万ポンド	436,443 ポンド	5
運輸 (OES)	171	190 万ポンド	951,443 ポンド	2
医療 (OES)	132	150 万ポンド	483,312 ポンド	3
情報 (RDSP)	513	680 万ポンド	1,101,588 ポンド	6

この分析では、公益事業セクターの既存規制対象企業が年間 5 件の追加攻撃を回避できれば、新たな報告期限のコストは正当化される。運輸、医療、情報セクターでは、それぞれ 2 件、3 件、6 件の追加攻撃回避が必要となる。より強力なインシデント報告アプローチは、実施年度における攻撃を防止することは難しいが、NCSC と規制当局への迅速な報告により、より速やかな復旧を支援できる。これにより直接コストと広範な二次的影響が軽減され、成功したインシデント事例、規制順守状況、最も効果的な緩和に関するセクター内およびセクター間の包括的な状況把握が可能となることで、将来の攻撃を防止できる。

経済全体への便益

上記の分析は英国企業への便益のみを考慮している点に留意すべきだ。実際には、本法案の便益は NIS 規制の対象企業だけでなく、経済全体に広く及ぶ。これはサイバー攻撃に伴う負の外部性によるものである。攻撃の負の影響は攻撃を受けた組織のみに留まらず、強化されたセキュリティの便益は経済全体に及ぶのだ。

間接的便益

競争上の利益

本法案は、規制対象事業者間のセキュリティと透明性を促進する適切なインセンティブを育む規制枠組みを提供する。その結果、この市場における高度なプレイヤーにとって、より予測可能で一貫性のあるビジネス環境が整うことで、品質に基づく競争力の促進、ひいては投資の誘致につながる可能性がある。同様に、より安全なビジネス環境は、デジタル企業が英国で事業を展開することを促すかもしれない。EU や他国との規制アプローチの一貫性も、英国への投資拡大を可能にするだろう。

9. コスト

概要 – 何もしない選択肢

何もしない選択肢は現状維持を意味するため、追加的な直接・間接コストは発生しない。何もしない場合、対象組織や影響を受けた消費者にとってサイバー攻撃に関連する重大なコストの改善は見込めない。サイバー攻撃が企業や広範な経済に与えるコストの定量的な見積もりは、上記の便益セクションで概説されている。

概要 – 推奨選択肢

提案された改革パッケージのコスト分析は以下のように区分されており、詳細は後述のセクションで確認できる。

各施策について、可能な限りコストの説明と貨幣換算を行った：

目次

新規事業体の追加

1. 関連するマネージドサービス・プロバイダー（RMSP）を NIS 規則の適用範囲に組み入れる。
2. データセンターインフラを NIS 規則の適用範囲に組み入れる。
3. 電力セクター向けの新たなエネルギー重要サービス（負荷制御）を NIS 規則の適用範囲に追加する。
4. 規制当局が重要供給者を指定できるようにする。

規制当局がコンプライアンスを推進し、その職務を遂行するために必要な資源と重要な情報を確保できるようにする。

5. インシデント報告の改善。
6. 情報共有規定を強化する。例えば、規制当局同士や公的機関との情報共有を可能にし、その逆も同様とする。
7. 情報委員会がリスク関連情報を収集できるようにする。
8. 規制当局のコスト回収メカニズムを改善する。
9. 国務長官が戦略的優先事項に関する声明を指定できるようにする。
10. NIS 規則の執行・制裁の枠組みを強化する。

NIS 規則が絶えず変化するサイバー環境に対応し、国家安全保障の防御のための断固たる措置を政府が講じられるよう確保する。

11. 委任権限 – 新たな脅威に対応可能な規制枠組みを確保する。
12. セキュリティとレジリエンスの要件。
13. 政府がサプライチェーンの安全性を向上させることを可能にする。
14. 国家安全保障上必要と判断される場合、国務長官が規制当局に指示する権限を導入する。
15. 国家安全保障上必要と判断される場合、国務長官が規制対象事業体を指示する権限を導入する。

合計

表 9.1 : 該当する場合の措置ごとの総金銭的価値コスト

これは、10年間の評価期間における一時コストと年間コストを、2025年価格でのコストの現在価値総額として統合したものである。

対策	総コスト（百万ポンド） 現在価値 低シナリオ	総コスト（百万ポンド） 現在価値 中央シナリオ	総コスト（百万ポンド） 現在価値 高シナリオ
1. 関連するマネージドサービス・プロバイダー（RMSP）をNIS規制の対象範囲に含める	5億5200万ポンド	7億9600万ポンド	10億5800万ポンド
2. データセンターインフラをNIS規制の対象範囲に含める	1億1800万ポンド	1億4900万ポンド	2億1400万ポンド
3. 電力部門向けの新たなエネルギー重要サービス（負荷制御）をNIS規制の対象範囲に含める	2700万ポンド	4000万ポンド	6400万ポンド
4. インシデント報告の改善	5800万ポンド	2億100万ポンド	3億8400万ポンド

RMSP、データセンター、大規模負荷制御装置のインシデント報告コストは全て、インシデント報告対策に計上されていることに留意せよ。

表 9.2 : 種類別コスト

	説明	適用対象
単発		
習熟	新規規制の読解・理解に伴うコスト。DSITは時間コスト法を用いて、更新されたNIS規制の読解にかかる管理コストを算出した。	新規規制対象事業体全て規制当局
追加的な物理的セキュリティコスト	事業体に対する一時的な追加物理的セキュリティコスト。これらの一時的な追加セキュリティコストは、追加セキュリティ要件を満たすためのコストであるため、措置が実施される初年度に帰属させる。	新規規制対象事業体全て
契約変更コスト	NIS規則の関連事項を反映させるため、顧客向け契約を変更するコスト。	新規規制対象事業体全て
継続的コスト		
インシデント報告	新規企業におけるインシデント報告義務に伴うコスト、及び改正NIS規則により拡大されたインシデント報告範囲に伴う既存規制対象企業のコスト。	新規規制対象企業全て既存企業全て

追加のサイバーセキュリティコスト	新規措置への対応に伴う規制対象事業者による追加的なサイバーセキュリティ支出の継続的コスト	新規規制対象事業者全体
コンプライアンスコスト	関連規制当局へのコンプライアンス証明（CAFの提出を含む）を提供するプロバイダのコスト。要件は業種や規制当局によって異なり、金銭的コストにその差異を反映させることは不可能である。	新規規制対象となる全ての事業者
規制当局のコスト	新規事業者を規制するために規制当局が負担する継続的コスト	規制当局

対象範囲内の組織

本節の収益化分析の多くは、対象となる関連組織の総数の推定値に依存している。本節では、各措置の対象となる事業者の数の概要を示し、各シナリオにおける推定値の根拠となる証拠を強調する。

表 9.3：実施初年度における各措置の対象組織総数。これらの推定値の説明は表の下部を参照のこと。

組織グループ	組織数 - 低シナリオ	組織数 - 中間シナリオ	組織数 - 高シナリオ	シナリオの根拠となる証拠
関連するマネージドサービス・プロバイダー	556	788	1019	フロンティア・エコノミクス 2025
データセンター	64	64	64	DSIT のデータ政策チームが委託した研究
大型負荷制御装置	8	11	22	DSIT 内部推定値
重要サプライヤー - <u>関連デジタルサービスプロバイダ (RSDP)</u>	該当なし	該当なし	該当なし	
重要サプライヤー - <u>「重要サービス事業者」 (OES)</u>	56	93	130	二つの規制当局のプロバイダによる推定値に基づく
インシデント報告	1,756	1,991	2,223	これは、既に規制対象となっている企業グループと新規に規制対象となった企業グループの全グループにわたる推定値の合計である
規制当局	13	13	13	2018 年 NIS 規制には 12 の規制当局が存在する。データセンターが追加されたことで、Ofcom と DSIT が共同で規制を行うため、追加で 1 つの規制当局 (DSIT) が加わる。

マネージドサービス・プロバイダー

フロンティア・エコノミクス社の推計によれば、英国で活動中または登録済みの MSP は 12,867 社である。

中小企業は NIS の対象外であるため、フロンティア社は、英国で従業員 50 人以上を雇用し、売上高が 1,000 万ユーロを超える MSP が 977 社から 1,214 社存在すると推定している。このうち 658 社はクラウドサービスプロバイダと推定され、既に法案の対象範囲に含まれている。したがって、これらを除外した更新版 NIS 規制の対象となる MSP 数は 556 社から 1,019 社と推定される。これらの数値は低・高シナリオに用いられ、中央値（788 社）は中位シナリオに採用された。継続のコストに関しては、対象 MSP 数は期間中に増加すると見込まれる。10 年間の評価期間において、MSP の数は全シナリオで年率 3.6% のペースで増加すると予測される。この数値は、過去 10 年間の通信情報分野における企業総数の平均年間成長率を用いて概算したものである。この分野が MSP の成長率を最も適切に代表すると想定されている。

データセンター

本規制の対象となるデータセンターは 64 施設である。規制施行時点の対象施設数が確定しているため、全シナリオで同一の数値とする。継続のコストについては、低シナリオでは一定と仮定する。中央シナリオでは他の措置と同様に 3.6% の成長率を想定し、高シナリオではこの分野の成長加速可能性を考慮し 10% の高い成長率を想定する。

英国で予測されるデータセンターの容量と数の大幅な増加は、それ自体では企業数の大幅な増加にはつながらない可能性が高い。この成長の多くは既存企業、特に大規模な外資系企業によって牽引されているためだ。これは高度に専門化された産業であり、新規参入は歓迎されるものの、多くの新規参入の可能性をさらに制限している。

大規模負荷制御装置

低シナリオでは 8 組織、中央シナリオでは 11 組織、高シナリオでは 22 組織が、実施初年度の対象範囲に含まれると見込まれる。これは 2023 年に内部で実施した市場分析と、300MW 以上を制御する負荷アグリゲーターの既知数（5 組織）を組み合わせたものである。大規模負荷制御事業者の数は評価期間中に増加すると予想される一方、負荷アグリゲーターの数は増加しないと見込まれる。これは負荷制御事業者が新興市場であるのに対し、アグリゲーターは既に確立された大規模組織であるためだ。

重要供給者の指定

本措置では、重要サービス事業者（OES）に加え、地域配電システム事業者（RDSP）及び地域配電システムプロバイダー（RMSP）に関連して重要供給者を指定する可能性がある。重要供給者とは、重要サービスまたはデジタルサービスのレジリエンスに不可欠な製品・サービスを提供する企業を指す。セクター規制当局は、供給者を指定し、規制対象事業者へのリスク低減のため比例的なサイバーセキュリティ義務を課す権限を有する。指定は法定閾値規準を満たす場合にのみ可能であり、最も重要な少数の供給者のみを対象とする。

重要な点として、これには小規模・零細な MSP や DSP（例えば小規模クラウドプロバイダなど）も含まれる。これらは従来 NIS 規則の適用除外とされていたが、閾値規準を満たし重要サービスに不可欠と認められた場合、重要供給者として指定される可能性がある。

- 小規模／零細 DSP および MSP は規模基準により直接規制の対象外となるが、その障害が必須サービス、デジタルサービス、管理サービスに重大な影響を与える可能性がある場合には指定されることがある。

DPS および MSP（中小企業）

現段階では、指定対象となる小規模・零細 DPS および MSP の数を推定することは不可能である。これは二次立法段階で更新される予定だ。

OES

低シナリオでは 56 社、中央シナリオでは 93 社、高シナリオでは 130 社の OES が想定される。これらのシナリオ予測は、2 つの規制プロバイダによる推計値を基に、DSIT が全 13 規制プロバイダに外挿して算出された指定対象となる OES の総数である。重要供給業者の数は、評価期間中に変化しないと予想される。これらの組織は供給チェーンにおいて確立されているためである。

この措置は、二次立法（重要供給業者に対する義務を定めるもの）が発効した時点で施行される。これに先立ち、DSIT は指定される見込みの重要供給業者の数と、供給業者 1 社あたりの指定コストについて、包括的な分析を実施する。

インシデント報告の改善

対象となる企業の数、2018 年 NIS 規制の対象組織数と、本法案により新たに適用範囲に組み込まれた組織数の合計である。初年度における低シナリオでは 1,756 社、中央シナリオでは 1,991 社、高シナリオでは 2,233 社となる。継続的コストについては、前述の通り MSP 数は 3.6% のペースで増加すると見込まれる。現行の対象範囲内の RDSP 及び OES 数は変わらず、重要供給業者の数も一定と仮定する。

規制当局

NIS 規則の対象となる規制当局は現在 12 機関である。法案発効後は 13 機関に増加する。データセンターインフラが Ofcom と DSIT の共同規制対象となるためである。後者は現在 NIS 規制当局ではない。

1. 関連するマネージドサービス・プロバイダー（RMSP）を NIS 規制の対象範囲に組み入れる。

この措置により、法案を通じて大規模・中規模プロバイダが提供する全ての管理サービスが NIS 規制の対象となる。規制当局により重要供給者として指定されない限り、小規模・零細企業は免除される。RMSP を NIS 規制の対象に含めることで、現行対象である RDSP と同等のサイバーセキュリティ標準を維持することが義務付けられ、サイバー攻撃者を抑止し、万が一インシデントが発生した場合の影響を最小限に抑えることになる。

直接コスト

金銭換算された直接コスト

一時的なコスト

習熟コスト

RMSP への定量化可能な影響には、新措置導入に伴う習熟コストが含まれる。DSIT は時間コスト法を用いて、改正 NIS 規制の読解に伴う管理コストを推計した。

DSIT は委託研究により識別された関連 MSP 数を 556～1,019 の範囲（中間推定値 788）と算定した。DSIT は全組織が新ガイドラインを読むため、習熟コストは初年度に発生すると想定している。証拠は 2022 年 NIS PIR（政策影響報告書）から引用した。同報告書は 2018 年 NIS 影響評価内の分析を基にコスト見積もりを更新したものである。2018 年影響評価の当初見積もりは、2018 年 ONS 労働時間・賃金年次調査（ASHE）に基づく法律専門職（時給 26 ポンド）及び IT・通信部門責任者（同 37 ポンド）の時給を用いて算出された。⁵⁵ これらを、更新された NIS 規則に慣れるための各職業の平均労働時間、および措置の対象となる企業数（法務専門家は 12 社、取締役は 6 社）と乗算した。対象企業数は、省内部の法務部門との協議に基づいて設定された。過去の NIS 影響アセスメントと同様に、22%の間接費も適用した。2022 年 PIR 分析ではこれに加え、当初の NIS 影響アセスメントにおける習熟コスト見積もりに異議を唱えた 12 の回答者に対し、調査回答者から提供された加重平均コストを割り当てた。PIR はこれら 2 つの見積もりを統合し、組織あたりの総合習熟コストを算出。その結果は 1,133 ポンド（2025 年価格に調整済み）となった。本 IA では、この金額を下表 9.4 に示す対象 MSP 数で乗算した。

表 9.4 : MSP 向け習熟コスト計算（2025 年価格）

	低	中央	高
MSP 数	556	788	1019
MSP あたりのコスト	1,133 ポンド	1,133 ポンド	1,133 ポンド
総習熟コスト	63 万ポンド	89 万ポンド	115 万ポンド

追加物理的セキュリティコスト

⁵⁵所得と労働時間、4 桁 SOC 別職業：ASHE 表 14 - 英国国家統計局

DSIT はまた、MSP に対する一時的な追加物理的セキュリティコストをモデル化した。この一時的な追加セキュリティコストは、対策が実施される初年度に帰属する。これらは NIS 規則の追加セキュリティ要件を満たすためのコストである。

MSP 向けの一時的な追加セキュリティコストは、各デジタルサービスプロバイダへの投資額を適用して見積もられている。DSIT は、調査対象組織からの回答率が低かったため、2022 年 PIR プロセス中に物理的セキュリティの企業別コストを更新できなかった。したがって、MSP 向けコストの最善の推定値は、関連組織調査で識別された 2020 年 PIR 時点の RDSP 当たりコスト（58,012 ポンド）を 2025 年価格（70,281 ポンド）に更新し、各シナリオの対象 MSP 数で乗算するものである。

表 9.5 : MSP 向け追加物理的セキュリティコストの算出（2025 年価格）

	低	中央	高
MSP 数	556	788	1,019
MSP あたりのコスト	70,281 ポンド	70,281 ポンド	70,281 ポンド
追加物理的セキュリティコスト総額	3,908 万ポンド	5,538 万ポンド	7,176 万ポンド

契約変更コスト

DSIT は、RMSP が更新された NIS 規制の関連事項を反映させるため、契約変更 に一定の時間を費やすと想定している。契約更新は今後通常業務（BAU）として組み込まれるため、これは一時的なコストと見込まれる。DSIT は、組織が全クライアントに適用される単一の契約変更ドラフト作成コストのみを負担すると想定している。

このコストは、更新された NIS 規制の関連要件を反映した契約変更 に要する法務専門家の時間と時給を用いて算出される。2023 年 ASHE 調査のデータに基づき、法務専門家の時給は約 29 ポンド⁽⁵⁶⁾ であり、2025 年価格に更新すると 34 ポンドとなる。全対策の契約変更 に要する法務専門家の作業時間は、低シナリオで 1 日（8 時間）、中央シナリオで 1 週間（40 時間）、高シナリオで 2 週間（80 時間）と想定した。

MSP 向けの一時的な契約変更の総コストを算出するため、法律専門家の時給に各シナリオにおける契約変更所要時間を乗じる。このコストを各シナリオの対象となる MSP 数で乗算する。さらに間接費を考慮し 22% の上乘せを適用した。

表 9.6 : MSP 向け契約変更コスト計算（2025 年価格）

	低	中央	高
MSP 数	556	788	1,019
時給（2025 年価格）	34 ポンド	34 ポンド	34 ポンド
時間数	8	40	80
MSP あたりのコスト	270 ポンド	1,348 ポンド	2,695 ポンド
契約変更総コスト	15 万ポンド	106 万ポンド	275 万ポンド

⁵⁶英国の従業員所得 - 国立統計局

契約変更コスト総額（22%の諸経費を含む）	18 万ポンド	130 万ポンド	335 万ポンド
-----------------------	---------	----------	----------

継続的コスト

継続的コストとは、NIS 規制への継続的な遵守に関連する事業者および規制当局のコストを指す。これらは 10 年間の全評価期間にわたって査定される。

インシデント報告

インシデント報告コストについては、下記のインシデント報告サブセクション 5 で説明する。

追加のサイバーセキュリティ支出

追加のサイバーセキュリティ支出とは、新規制への対応に伴う事業者の追加的なサイバーセキュリティ支出の継続的コストを指す。

RMSP は NIS 規則への準拠を図るにあたり、追加的なサイバーセキュリティ支出を負担する必要がある。これには内部・外部の人的費用が含まれ、2022 年 PIR では調査データを用いて推計された。この推計値には既に間接費として 22%の上乗せが含まれている。

RDSP の場合、組織当たりの内部コストは全シナリオで 64,460 ポンドと推定された。一方、外部コストは中央シナリオで 28,175 ポンド、低シナリオで 26,297 ポンド、高シナリオで 30,054 ポンドと推定された。⁵⁷ これは MSP にとって最も適切な推定値であるため、各シナリオの MSP 数にこの値を乗じて総コストを算出した。10 年間において、MSP の数は情報通信セクターの事業成長率に基づき、全シナリオで年率 3.6%のペースで増加すると予測される。

コンプライアンスコスト

コンプライアンスコストは、規制当局への報告義務を履行するための継続的コストである。これにはサイバー評価枠組み（CAF）報告書の作成やその他の報告要件などのプロセスが含まれる可能性がある。要件は業種や関連規制当局によって異なるため、対象組織の全てがこのコストを負担する必要はない点から、本分析は過大評価の可能性があると見なせる。

RMSP の 10 年間の総コンプライアンスコストは、2022 年 PIR で判明した企業当たりの年間平均コンプライアンスコストに、各シナリオで規制対象となる見込みの MSP 数を乗じて算出される。企業当たりの年間平均コンプライアンスコストは 429 ポンドから 644 ポンドの範囲で、2025 年価格ベースでは 519 ポンドが中央シナリオとして推定されている。この見積もりには既に間接費として 22%の上乗せが含まれている。これらの見積もりは、2022 年 PIR において、調査回答と ONS ASHE 2018 データを用いた推計値を組み合わせて作成された。後者では、コンプライアンス活動に法律専門家 10 時間（£26.07）と企業管理者 14 時間（£22.58）が必要と仮定している。時間見積もりは、2018 年影響評価書作成時に部門内部の法務チームとの協議により算出された。

情報通信セクターの事業成長率に基づき、全シナリオにおいて 10 年間で RMSP 数は年率 3.6%のペースで増加すると予測される。

非金銭的 direct コスト

⁵⁷ [ネットワークと情報システム規制 2018 の第二回実施後レビュー - GOV.UK](#)

本措置に関連する追加の非金銭的 direct コストは存在しない。

間接コスト

この措置に関連する追加の金銭的・非金銭的 direct コストは存在しない。

2. データセンターインフラを NIS 規制の対象範囲に組み入れる。

NIS 規則において、1MW 以上の容量を有するデータセンターおよび 10MW 以上の容量を有するエンタープライズデータセンターを指定することで、これらの施設を規制枠組みに組み込み、特定のセキュリティおよびレジリエンス標準への準拠を確保する。

直接コスト

金銭的 direct コスト

一時的なコスト

習熟コスト

データセンター事業者への定量化可能な影響には、新措置の実施に伴う習熟コストが含まれる。DSIT は時間コスト法を用いて、更新された NIS 規則の読解にかかる管理コストを推定した。

本規制実施時に適用対象となるデータセンター数が確定しているため、データセンター全体の習熟コストは低・中・高の各シナリオで同額と見込まれる。NIS の対象となるのは、要件を満たすデータセンターを少なくとも 1 つ保有する 64 の事業者である。事業者全体の習熟コストは、各組織の予想習熟コストに、措置対象となるデータセンターを保有する事業者数を乗じて算出した。間接費を考慮し、既に 22% の上乘せが適用されている。2022 年 PIR で使用された見積もり額 1,133 ポンド（2025 年価格に調整済み）を再利用する。前節の RMSP に関する説明通り、これは新規規制対象となる全事業者に適用されるものである。

表 9.7 : データセンター向け習熟コスト計算（2025 年価格）

	低	中央	高
データセンター事業者数	64	64	64
データセンター事業者あたりのコスト	1,133 ポンド	1,133 ポンド	1,133 ポンド
総習熟コスト	7.2 万ポンド	7.2 万ポンド	7.2 万ポンド

追加物理的セキュリティコスト

DSIT はまた、データセンター事業者に対する追加的な物理的セキュリティコストをモデル化した。この追加コストは対策実施初年度に計上される。更新された NIS 規制の追加セキュリティ要件を満たすためのコストである。

データセンター事業者に対する物理的セキュリティコスト総額は、OES（重要電子サービス事業者）の物理的セキュリティ投資平均コストを適用し、さらにこの数値を対策導入時に少なくとも 1 つのデータセンターが対象範囲に含まれると見込まれるデータセンター事業者の数に適用することで推定される。これは 2022 年 NIS PIR において、調査結果に基づき低

シナリオで 86,973 ポンド、中シナリオで 94,474 ポンド、高シナリオで 101,976 ポンドと推定された。これらは 2025 年価格に換算され、下記の表 9.8 に示されている。データセンター運営事業者の数は全シナリオで一定であるため、シナリオ間の差異は平均投資コストのみに起因する。

表 9.8 : データセンター向け追加物理セキュリティコストの算出 (2025 年価格)

	低	中央	高
データセンター運営者数	64	64	64
データセンター事業者あたりのコスト	105,356 ポンド	114,454 ポンド	123,542 ポンド
追加物理的セキュリティコスト総額	674 万ポンド	733 万ポンド	791 万ポンド

契約変更コスト

RMSP と同様に、契約変更コストは 2023 年 ASHE 調査に基づく法務専門家の時給を用いて算出される。これを 2025 年物価に換算し、契約変更に要した時間を乗じる。間接費を考慮し 22% の上乘せも適用されている。

表 9.9 : データセンター向け契約変更コストの算出 (2025 年価格)

	低	中央	高
データセンター事業者数	64	64	64
時給 (2025 年価格)	34 ポンド	34 ポンド	34 ポンド
時間数	8	40	80
データセンターオペレーター 1 人あたりのコスト	270 ポンド	1,348 ポンド	2,695 ポンド
契約変更総コスト	17 万ポンド	9 万ポンド	17 万ポンド
22% の諸経費を含む契約変更コスト総額	21 万ポンド	11 万ポンド	21 万ポンド

継続的成本

継続的成本とは、NIS 規制への継続的な遵守に関連する事業者および規制当局のコストを指す。これらは 10 年間の評価期間全体にわたって査定される。

インシデント報告

インシデント報告コストについては、下記のインシデント報告セクション 5 で説明する。

追加のサイバーセキュリティ支出

データセンター事業者における継続的なサイバーセキュリティコストを推定するため、DSIT は 2022 年 PIR (調査により収集) に記載された、重要サービス事業者 (OES) が従来の NIS 措置に準拠するために要した外部・内部セキュリティ

要員コストを適用した。OES 全体のこれらのコストは、2025 年価格ベースで年間 181,464 ポンドから 211,363 ポンドの範囲である。次に、このコストを今後 10 年間で各シナリオごとに予想されるデータセンター運営事業者数で乗算した。この見積もりには既に間接費として 22%の上乗せが含まれている。10 年間において、データセンター運営事業者数は情報通信セクターの事業成長率を用いて、全シナリオで年率 3.6%の成長が見込まれる。データセンター事業者は OES となるため、ここでの内部・外部コストは 2022 年 PIR で定められた RDSP よりも高くなる。

コンプライアンスコスト

コンプライアンスコストとは、規制当局への報告義務を履行するための継続的コストを指す。これには CAF（共通評価フレームワーク）の提出やその他の報告要件の履行といったプロセスが含まれる可能性がある。

要件は業種や関連規制当局によって異なるため、対象組織の全てがこのコストを負担する必要はない点から、本分析は過大評価の可能性があると見なせる。

データセンターにおける 10 年間の総コンプライアンスコストは、2022 年 PIR で示された事業体当たりの年間平均コンプライアンスコストに、各シナリオで規制対象となる見込みのデータセンター事業者数を乗じて算出される。この見積もりには既に間接費として 22%の上乗せが含まれている。企業当たりの年間平均コンプライアンスコストは 429 ポンドから 644 ポンドの範囲で、中央シナリオでは 2025 年価格換算で 519 ポンドと推定される。10 年間において、データセンター事業者の数は情報通信セクターの事業成長率に基づき、全シナリオで年率 3.6%の増加が見込まれる。これらの見積もりは、2022 年 PIR において、調査回答と ONS ASHE 2018 データを用いた推計を組み合わせで作成された。後者では、コンプライアンス活動に法律専門家 10 時間（1 時間あたり 26.07 ポンド）と企業管理者 14 時間（同 22.58 ポンド）が必要と仮定した。

非金銭的価値直接コスト

この措置に関連する追加の非金銭的価値直接コストは存在しない。

間接コスト

この措置に関連する追加の金銭的・非金銭的価値直接コストは存在しない。

3. 電力セクター向けの新規エネルギー重要サービス（負荷制御）を NIS 規則の対象範囲に追加する。

この選択肢では、大規模負荷制御事業者は、サイバー攻撃を防止・緩和するための効果的な措置を実施していることを証明する必要がある。これにより、進化する脅威環境に対するセクターのレジリエンスについて政府に保証を提供する。

直接コスト

金銭的価値直接コスト

一時的なコスト

習熟コスト

負荷制御事業者への定量化可能な影響には、新たな対策の実施に伴う習熟コストが含まれる。DSIT は時間コストアプローチを用いて、更新された NIS 規則を読むための管理コストを推定した。

NIS の対象となる大規模負荷制御装置の総数は、低・中・高の各シナリオで推定された。これらの組織における総習熟コストは、各組織の予想習熟コストに措置対象のデータセンター数を乗じて算出された。2022 年 PIR で使用された見積

もり額 1,133 ポンド（2025 年価格に調整済み）が再び用いられ、これは各シナリオで共通である。間接費を考慮するため、既に 22%の上乗せが適用されている。

表 9.10 : 負荷制御装置の習熟コスト計算（2025 年価格）

	低	中央	高
負荷制御装置の数	8	11	22
負荷コントローラーあたりのコスト	1,133 ポンド	1,133 ポンド	1,133 ポンド
総習熟コスト	9 万ポンド	12 万ポンド	25 万ポンド

追加物理的セキュリティコスト

DSIT はまた、負荷制御事業者に対する一時的な追加物理的セキュリティコストをモデル化した。この一時的な追加セキュリティコストは、対策が実施される初年度に帰属する。これらは、更新された NIS 規制の追加セキュリティ要件を満たすためのコストである。

負荷制御事業者に対する物理的セキュリティコスト総額は、重要サービス事業者向けの物理的セキュリティ投資平均コストを適用して算出される。これは新規規制対象組織群にとって最も適切な見積もりである。これらは 2022 年 PIR において、調査結果に基づき低シナリオで 86,973 ポンド、中シナリオで 94,474 ポンド、高シナリオで 101,976 ポンドと推定され、2025 年価格に更新された。その後、対策導入時に適用範囲と想定されるデータセンター数に適用した。

表 9.11 : データセンター向け追加物理的セキュリティコストの算出（2025 年価格）

	低	中央	高
負荷制御装置数	8	11	22
負荷制御装置あたりのコスト	105,356 ポンド	114,454 ポンド	123,542 ポンド
追加物理的セキュリティコスト総額	84 万ポンド	126 万ポンド	272 万ポンド

契約変更コスト

MSP と同様に、契約変更コストは 2023 年 ASHE 調査に基づく法務専門家の時給を用いて算出される。これを 2025 年物価に換算し、契約変更に必要な時間を乗じる。間接費を考慮し 22%の上乗せも適用されている。

表 9.12 : 負荷制御装置の契約変更コスト計算（2025 年価格）

	低	中央	高
負荷制御装置の数	8	11	22
時給（2025 年価格）	34 ポンド	34 ポンド	34 ポンド

時間数	8	40	80
負荷コントローラーあたりのコスト	270 ポンド	1,348 ポンド	2,695 ポンド
契約変更総コスト	0.22 万ポンド	1.5 万ポンド	5.9 万ポンド
22%の諸経費を含む契約変更コスト総額	0.26 万ポンド	1.8 万ポンド	7.2 万ポンド

継続的コスト

継続的コストとは、NIS 規制への継続的な遵守に関連する事業者および規制当局のコストを指す。これらは 10 年間の評価期間全体にわたって算定される。

インシデント報告

インシデント報告コストについては、下記のインシデント報告セクション 5 で説明する。

追加のサイバーセキュリティ支出

追加のサイバーセキュリティ支出とは、負荷制御事業者が NIS への準拠のために負担する追加のサイバーセキュリティ支出の継続的コストを指す。

負荷制御事業者における継続的サイバーセキュリティコストを推定するため、DSIT は 2022 年 PIR（調査報告書）に基づき、調査で収集された過去の NIS 措置遵守に要した外部・内部セキュリティ要員の件数 OES を適用した。これらのコストを合算すると、2025 年価格ベースで年間 181,464 ポンドから 211,363 ポンドの範囲となる。この見積もりには既に間接費として 22%の上乗せが含まれている。次に、今後 10 年間に各シナリオで想定される負荷制御事業者の数にこれらのコストを乗じる。10 年間にわたり、情報通信セクターの事業成長率を用いて、全シナリオで負荷制御事業者の数は増加すると予想される。負荷制御事業者は OES となるため、ここでの内部・外部コストは RDSP よりも大きい。

コンプライアンスコスト

コンプライアンスコストとは、規制当局へのコンプライアンス報告に伴う継続的なコストである。これには CAF の記入やその他の報告要件といったプロセスが含まれる可能性がある。

要件は業種や関連規制当局によって異なるため、対象となる全ての組織がこのコストを負担する必要はない点から、本分析は過大評価の可能性があると見なせる。

負荷制御事業者に対する 10 年間の総コンプライアンスコストは、2022 年 PIR で示された事業者当たりの年間平均コンプライアンスコストに、各シナリオで規制対象となる見込みの負荷制御事業者数を乗じて算出される。この見積もりには既に間接費として 22%の上乗せが含まれている。企業当たりの年間平均コンプライアンスコストは 429 ポンドから 644 ポンドの範囲で、中央シナリオでは 2025 年価格換算で 519 ポンドと推定される。10 年間に於いて、データセンターの数は情報通信セクターの事業成長率に基づき、全シナリオで年率 3.6%の増加が見込まれる。これらの見積もりは、2022 年 PIR において、調査回答と ONS ASHE 2018 データを用いた推計を組み合わせで作成された。後者では、コンプライアンス活動に法律専門家 10 時間（1 時間あたり£26.07）と企業管理者 14 時間（同£22.58）が必要と仮定した。時間見積もりは、2018 年 NIS IA に先立ち、省内部の法務チームとの協議に基づいて算定された。

非金銭的価値直接コスト

本措置に関連する追加の非金銭的価値直接コストは存在しない。

間接コスト

この措置に関連する追加の金銭的・非金銭的直接コストは存在しない。

4. 規制当局による重要供給業者の指定を可能とする

これにより、規制当局は規制対象事業体に対して重要供給者を指定する権限を得る。供給者が指定されるには法定の閾値規準を満たす必要があり、これによりごく少数の最重要供給者のみが対象となることが保証される。2018 年 NIS 規則から従来免除されていた小規模・零細 RDSP も、閾値規準を満たす場合（つまり必須サービスまたはデジタルサービスにとって重要とみなされる場合）は「重要供給者」として指定される可能性がある。

重要供給業者の指定は、政府が後日、二次立法において指定重要供給業者に対する義務を定めるまで効力を生じない。以下の分析では、指定重要サプライヤーに生じるコストの推定値を示し、二次立法において指定される可能性のあるサプライヤー数の目安を提示する。ただし、対象企業の正確な数が不確実なため、コストは金額換算されておらず、本影響評価（IA）の主要数値には含まれていない。この分析は二次立法に先立ち更新される予定である。

直接コスト

DSIT は、この措置が一次立法段階で直接コストを発生させない見込みだ。この措置は、二次立法（重要供給業者への義務設定）が発効した時点で施行される。

非金銭的成本

組織当たりのコスト

現段階では、指定された重要供給業者ごとに以下の一時的なコストが発生すると見込まれる：

- **NIS 規則の理解にかかるコスト**（2025 年価格ベースで企業あたり 1,133 ポンドと見積もられる）
- **指定初年度の追加物理的セキュリティコスト**。これらの組織は独自のカテゴリとして指定され、OES（重要電子サービス事業者）や RDSP（重要通信サービス事業者）と同様の義務を負う。具体的な義務は二次立法で設定されるため、セキュリティ対策の正確なコストは見積もれない。NIS PIR 2022 で識別された OES へのコストを最も近い代用値として採用した場合、企業当たりのこのコストの中央値見積もりは 114,451 ポンドとなる。本影響評価では、OES へのコストは RDSP よりも高いと見積もられているため、慎重を期してこちらの高コストを採用した。
- **契約変更コスト**は、1 件あたり 329 ポンドから 3,288 ポンドと見積もられ、2025 年価格ベースの中央値は 1,644 ポンドである。措置 1～3 と同様に、契約変更のコストは 2023 年 ASHE 調査に基づく法務専門家の時給を用いて算出される。これを 2025 年物価に換算し、契約変更に要した時間と乗算する。間接費を考慮し 22%の上乗せも適用されている。

また、以下の年間継続コストが発生する：

- **インシデント報告**（詳細は下記対策 5 で説明）
- NIS に関連する**追加のサイバーセキュリティ支出**。前述の通り、これらの組織は独自のカテゴリとして指定される。ここでも OES へのコストを慎重な代用値として用いれば、各企業へのコストの中央値は 190,435 ポンドとなる。

- 更新された NIS 規制への**準拠に伴うその他のコスト**。企業当たりの年間推定コストは 429 ポンドから 644 ポンドの範囲。2025 年価格ベースで 519 ポンドが中央シナリオとして推定され、他の新規規制対象企業と同水準となる。

指定される組織数

DSIT は、重要供給業者として指定される可能性のある企業数について、2 つの規制当局から証拠を入手している。これらの推定値を全 13 規制当局に外挿すると、低ケースシナリオでは 56 社、高ケースシナリオでは 130 社、中央ケースシナリオでは 93 社が指定されると識別される。

現段階では、重要供給業者として指定される中小企業（SME）や中小企業 DSP の数を DSIT は推定できない。これらは NIS や本法案で導入される新措置の対象外となる小規模・零細企業である。ただし規制当局は、重要供給業者のみを確実に包含するため、指定対象組織に関する厳格なガイドラインに従う。したがって中小企業へのコスト負担は、主要供給網の安全確保に不可欠である。

これらの見積もりは、二次立法に先立って更新される。

5. インシデント報告の改善

本措置は、企業がインシデントを確実に報告し、規制当局がサイバーセキュリティインシデントの規模と深刻度を明確に把握できるよう、報告枠組みを改正するものである。

インシデント報告のタイミングを更新し、二段階報告構造（インシデント発生の認識後 24 時間以内の初期通知、その後 72 時間以内の報告）を導入することで、規制当局がインシデントを早期に把握できるようになる。これにより、必要な措置（もしあれば）を評価する時間を確保できる。初期通知は簡素化され、規制対象事業者が重要な初期段階で可能な限りインシデントの影響緩和にリソースを集中できるようにする。

インシデント報告は二つの方法でコストを生む：

- 既存の規制対象事業者は、本措置により導入される新たなインシデント報告要件から追加コストのみを負担する。
- 本法案により改正 NIS 規制の対象となる組織は、インシデント報告の全コストを負担する。これには新規に適用範囲に含まれる RMSP、データセンター、大規模負荷制御事業者も含まれる。重要供給事業者もこのコストを負担するが、現段階では当該事業者のコストは算定されていない。

直接コスト

直接コストの現金化

一時的なコスト

表 9.13 : 対象企業数

	低	中央	高
MSP	556	788	1,019
データセンター	64	64	64
負荷制御装置	8	11	22

新規規制対象事業体合計	628	863	1,105
既存の規制対象事業体	1,128	1,128	1,128
合計	1,756	1,991	2,233

習熟コスト

新規規制対象事業体を含む対象範囲内の全企業は、改訂された NIS 規則に定められたインシデント報告要件を習得する必要がある。新規規制対象企業については、このコストは RMSP、データセンター、負荷制御装置における習熟コストとして計上される。既存対象事業体については、DSIT が 2023 年 ASHE 調査に基づく法務専門職 (£29) および IT・通信部門責任者 (£43) の中央賃金を基に習熟コストを推計した。更新された NIS 規則の習熟に必要な時間数は、法律専門家が 3 時間、IT・通信部門責任者が 1.5 時間である。中央値賃金に時間数と企業総数を乗じる。間接費を考慮し、既に 22%の上乗せが適用されている。

表 9.14 : 既存規制対象企業におけるインシデント報告の習熟コスト計算 (2025 年価格)

	低	中央	高
既存規制対象企業数	1,128	1,128	1,128
企業あたりのコスト	380 ポンド	380 ポンド	380 ポンド
既存企業総コスト (百万ポンド)	43 万ポンド	43 万ポンド	43 万ポンド

継続的成本

継続的成本とは、NIS 規制への継続的な遵守に関連する事業体および規制当局のコストを指す。これらは 10 年間の評価期間全体にわたって査定される。

インシデント報告のコスト

既存の規制対象企業については、インシデント報告は既に義務付けられているため、追加コストは発生しない。追加コストは、以下で説明する新たな報告期限と定義から生じる。

新規に規制対象となる企業は、インシデント報告義務により以下のコストが発生する可能性が高い。報告対象インシデントの定義範囲が異なるため、データセンターのインシデント報告コストは別途検討する。

各インシデントの報告コストは、2023 年 ONSASHE 調査に基づく時間給 (IT・通信専門家 : 27.20 ポンド、法務専門家 : 29.08 ポンド、企業管理者・取締役 : 32.66 ポンド) を用いる。これに DSIT が想定するインシデント対応所要時間 (IT・通信専門家および法務専門家 : 0.75 時間、企業管理者・取締役 : 0.33 時間) を乗じる。これらの前提条件は、2018 年 NIS 規制影響アセスメント及び 2022 年 PIR で使用されたものと同一である。平均賃金は、2013 年から 2023 年までの年間平均賃金上昇率を用いて算出した成長率で、評価期間中に増加すると仮定する。

次に、賃金時間推計値に組織当たりのインシデント発生件数を乗じる。低・中・高シナリオではそれぞれ 2 件、7 件、16 件と推定される。これは 2018 年 NIS 規則下での年間インシデント発生件数を規制対象組織総数で割って算出された

値である。さらに各シナリオにおける新規規制対象企業の数で乗算する。これにより、データセンターを除く新規規制対象企業におけるインシデント報告の総コストが算出される。間接費として 22%の上乗せが適用されている。

表 9.15.1 : 2026 年における新規規制対象企業（データセンターを除く）のインシデント報告総年間コスト。賃金上昇により年々増加すると予想される。

	低	中央	高
インシデント 1 件あたりのコスト（22%間接費を含む）	89 ポンド	89 ポンド	89 ポンド
年間インシデント数	2	7	16
新規規制対象企業総数（データセンターを除く）	564	799	1,041
新規規制対象企業（データセンターを除く）のインシデント報告総コスト	10 万ポンド	50 万ポンド	160 万ポンド

データセンターにおける組織当たりのインシデント数は、報告対象インシデントの定義拡大を考慮して上方修正された。したがって、データセンターにおける組織当たりのインシデント数は、低シナリオ、中央シナリオ、高シナリオにおいてそれぞれ 7 件、16 件、25 件と推定される。改訂された低シナリオと中シナリオは、上記で示したベースラインの中シナリオと高シナリオから採用した。改訂された高シナリオは、ベースラインの中シナリオと高シナリオの絶対増加分を改訂された中シナリオの推定値に適用して算出した。これにより、データセンターにおけるインシデント報告の総コストの推定値が得られる。間接費として 22%の上乗せが適用されている。

表 9.15.2 : 2026 年におけるデータセンターのインシデント報告総年間コスト。賃金上昇により年々増加すると予想される。

	低	中	高
インシデント 1 件あたりのコスト（22%間接費を含む）	89 ポンド	89 ポンド	89 ポンド
年間インシデント数	7	16	25
データセンターの総数	64	64	64
データセンターにおけるインシデント報告総コスト	4 万ポンド	9 万ポンド	14 万ポンド

新たに適用範囲に含まれる全ての組織（データセンターを含む）のコストを集計すると、2026 年のインシデント報告にかかる総コストは、低シナリオで 14 万ポンド、中央シナリオで 60 万ポンド、高シナリオで 170 万ポンドと推定される。

インシデント報告のタイムライン

改善されたインシデント報告措置は、報告スケジュールにも変更を加える。新たな措置では、24 時間以内の通知と 72 時間以内の完全な報告が義務付けられるため、組織はインシデント対応のため週末もスタッフを配置する必要性が生じる可能性がある。DSIT は、全ての組織がインシデント対応に 1 名のスタッフを必要とすることを前提としている。

この変更に伴うコストを算出するため、DSIT は週末勤務のコスト、オンコール要員・週末勤務者を配置する企業の割合、および残業代を支払う企業の割合を推計した。週末勤務者もオンコール要員も配置しない企業は、フルタイムの残業代を支払う必要があった。中規模・大規模企業では、59%がオンコール要員を配置、13%が週末勤務者を配置、63%が残業代を支払っていた。中小零細企業では、61%が待機要員を、28%が週末勤務者を配置し、56%が残業代を支払っていた。これらの割合は 2024 年 NIS 調査の推計値に基づく。週末勤務者を配置している企業には追加コストは発生しない。週末勤務者は配置せず待機要員のみ配置している企業は、待機手当を支払う。待機要員を配置する企業のコストは 50.57 ポンドと算出された。

週末勤務者とオンコール勤務者を抱える企業の割合、および NIS 規制対象企業数に基づき、週末 1 日あたりの適正総コストを算出する。これを各年の週末日数で乗算する。さらに間接費として 22%の上乗せを適用する。

このコストは既存規制対象企業と新規規制対象企業の両方に適用される。

2026 年の全企業における年間総コストは、最善の推定シナリオでは 1,740 万ポンド（企業平均 9,000 ポンド）となり、2036 年までに 2,900 万ポンド（企業平均 14,000 ポンド）に増加する。

非金銭的価値直接コスト

指定重要供給業者へのインシデント報告コストは、指定数が不確実なため貨幣換算されていない。本法案により NIS の対象となる RMSD、データセンター、大規模負荷制御事業者と同様のコストが発生すると予想される。

間接コスト

追加の間接コストは発生しない。

6. 情報共有規定の強化（例：規制当局間の情報共有、規制当局と公的機関間の情報共有を可能とする）

NIS 規則に基づく情報共有規定を強化・拡大し、共有可能な情報の範囲、共有主体及び共有先について明確性を高める。本法案は、識別された情報規定の欠陥に対処するため、4 つの変更を提案する。

この措置は、企業に直接的・間接的なコストを発生させないと見込まれる。ただし、規制当局には、以下の「規制当局へのコスト」セクションで評価する慣れ親しむためのコストが発生する。

7. 情報委員会がリスクに関連する適切な情報を確保すること

この選択肢では、情報委員会が規制する RDSP および RMSD に対し、NIS 規則に基づく登録時に追加の特定情報（提供サービス種別や具体的な連絡先など）の提供義務を課す。

事業者には直接的なコスト負担は生じない見込みである。規制当局へのコスト負担の項で詳述する通り、情報委員会には一定の慣れ親しみのためのコストが発生する。

8. 規制当局のコスト回収メカニズムを改善する。

これにより、規制当局は NIS に基づく全ての活動（違反行為への対応を含む）を適切に資金調達できるようになり、各セクターに最も適した方法でコストを回収できるようになる。

執行措置の追加により規制対象事業者のコストが増加する可能性があるが、コストの透明性と予測可能性にはプラスの影響を与える。現行の請求モデルでは、事業者が規制当局から請求されるか否か、またその金額が不明確である。新たな課金制度に関する規制当局の協議義務は、規制対象事業者が意見を表明し、将来の予想コストを把握できることを保証する。さらに、規制当局がコスト回収制度を設計する際に満たすべき規準を通じて、業種間の一貫したアプローチを促進しつつ、より個別対応的で比例的なコスト回収メカニズムを導入する機会を提供する。

これにより企業には直接的なコストが発生するが、各規制当局がコスト回収制度をどのように設計するか不確実なため、現段階ではそのコストを算出することは不可能である。NIS 規則には既にコスト回収規定が含まれており、NIS 規則に基づく規制当局の機能行使に伴うコストの大部分は既に回収可能となっている。回収されるコストは規制当局によって異なり、その一因はコスト回収権限の利用状況にばらつきがあることにある。

9. SoS が戦略的優先事項の声明を指定できるようにする。

戦略的優先事項の声明は、規制当局が達成を目指す義務を負う成果を詳細に定めるものである。これにより、全ての規制当局・セクターが同一の成果に向けて取り組むことが求められるため、アプローチの一貫性が向上する。規制の自律性を維持するため、戦略的優先事項の声明は規制当局との協議を経て作成され、規制当局は最も適切と考える方法で成果達成を目指す自由を有する。現行の政策目標では、戦略的優先事項声明は 3 年から 5 年ごとに作成される。これにより規制当局は効果的な計画立案に十分な時間軸を確保できる一方、NIS 規制の執行方針を事後対応型から事前予防型へ転換するなど、規制当局と政府は必要に応じてアプローチを調整できる。公的監視の機会を提供するため、国務大臣は戦略的優先事項声明の目標達成状況に関する年次報告書を公表することが義務付けられ、その作成に際し規制当局から情報提供を求めることができる。

これにより企業にコスト負担が生じることはない。規制当局は、規制当局へのコスト負担の項で説明した通り、戦略的優先事項声明の内容を熟知する必要がある。

10. NIS 規則の執行メカニズム強化

この措置により、規制当局は規則違反に対してより高額かつ比例的な罰金を科すことが可能となる。また、罰金制度を簡素化し、罰金の明確性と予測可能性を高めると同時に、適切な罰金額を決定する際に規制当局が考慮できる状況の範囲を拡大する。

完全な順守が前提であるため、本措置に関連するコストは発生しない。

11. 委任権限 – 新たな脅威に対応可能な規制枠組みを確保する

この措置により、政府は適切な協議を経た後、議会の法律制定なしに規制枠組みを更新できるようになる。これらの権限には一定の制限と安全装置が設けられる。例えば、改正が英国経済や社会の機能に不可欠なサービスの規制に関連する特定の目的に限定されるよう制限される。この権限は、規制対象事業者に対する新たな要件や義務の導入、NIS 規制当局の責任や機能の変更などの変更を行うために使用される可能性がある。NIS 規制の変更に伴う事業者の負担は、二次立法が提出される前に評価される。

12. セキュリティ及びレジリエンス要件。

我々は、大臣が規制を通じてセキュリティ及びレジリエンス要件を更新する権限を付与することを意図している。大臣には以下の権限が付与される：

- RDSP に適用されるセキュリティ要件を規則で設定する。
- 適切かつ均衡のとれた範囲で、RDSP 以外の対象に拡大する。

これらの要件は、RDSP に対する既存のセキュリティ要件に取って代わるものである。国務大臣は、サイバー評価フレームワーク基本プロファイル（例：サイバーガバナンス、資産管理、リスクマネジメント、インシデント対応に関する基本要件を定めるもの）の要素を反映させるため、セキュリティ要件を調整する権限を行使することが期待される。

現段階では、この措置が企業に直接的なコストを発生させることは想定されていない。更新が行われる場合は二次立法を通じて実施され、その時点で政府は企業へのコストをアセスメントする。

13. 政府によるサプライチェーンセキュリティの強化を可能にする

OES（義務的執行サービス）及び RDSP（規制開発支援プログラム）に対し、強制力のある義務を通じてサプライチェーンのセキュリティを識別・管理するよう明確な期待を設定することで、自主的なガイダンスよりもサプライチェーン全体でのコンプライアンス水準の向上が見込まれる。明確な法的期待は、サプライヤーとの契約上の取り決めに活用したサプライチェーンリスクマネジメントを促進する。

これは企業に直接的な影響を与えると予想されるが、その影響を推定するには時期尚早である。将来の義務は二次立法で定められ、政府は企業へのコストについてアセスメントを行う。

14. 国家安全保障の利益のために必要かつ均衡のとれた場合、国務大臣が規制当局に指示する権限を導入する

15. 国家安全保障の利益のために必要かつ均衡のとれた場合に、国務大臣が規制対象事業体を指示する権限を導入する。

現段階では、これら二つの措置が企業に直接的なコストをもたらすとは予想されない。規制当局または規制対象事業体への指示発出が必要となった場合、その指示内容に応じて企業にコストが生じる可能性がある。この権限は国家安全保障が脅かされる例外的な状況においてのみ、かつ稀にしか行使されないことが予想されるため、指示内容や指示遵守に伴う企業コストを予測することは不可能である。政府は、指示を発出するか否か、また指示の範囲をどこまで広げるかを決定する際に、関連企業にかかるコストをアセスメントする。

規制当局へのコスト

NIS 規則の対象となる規制当局は現在 12 機関であるが、法案施行後は 13 機関に増加する。

直接コスト

金銭換算された直接コスト

一時的なコスト

習熟コスト

DSIT は、全ての規制当局が新法を読むため、習熟コストは初年度に負担されると想定している。習熟に必要な時間については、NIS PIR から証拠を引き出した。規制当局の習熟コストは、2018 年 ONS 労働時間・賃金年次調査 (ASHE) における法律専門家 (時給 26 ポンド) および IT・通信部門責任者 (同 37 ポンド) の時給を用いて算定した。これに、法令の習熟に必要な各職種平均時間数、および対象当局数 (法律専門家 12 機関、責任者 6 機関) を乗じた。また、過去の国民保険制度 (NIS) 影響評価と同様に 22%の間接費が適用された。これにより各管轄当局あたり 1,133 ポンド (2025/26 年度価格に調整済み) と算定され、対象規制機関数で乗算した。**表 9.16 :** 規制機関の制度理解コスト

	低	中央	高
規制当局数	13	13	13
規制当局あたりのコスト	1,133 ポンド	1,133 ポンド	1,133 ポンド
総習熟コスト	1 万ポンド	1 万ポンド	1 万ポンド

継続的なコスト

規制コスト

規制当局が組織を規制するための継続的なコストは、PIR 2022 に示されている通り、2025 年価格ベースで 1 企業あたり 1,411 ポンドと見積もられている。これは情報委員会が 2022 年 PIR 作成のために提供したコスト見積もりに基づくものであり、全ての管轄当局に適用するのに最も適切な見積もりである。これには間接費として 22%の上乗せが含まれる。10 年間の評価期間において、MPS、データセンター、大規模負荷制御装置を対象に新規規制対象となる組織の総数に、この組織当たりのコストを乗じることで、規制当局の総コストを推定する。このコストの現在価値は 10 年間で 1,800 万ポンドとなる。

更新された報告期限に伴うコスト

規制当局は、規制対象事業体に対する新たな報告スケジュール要件に関連するコストを負担することになる。24 時間以内の通知と 72 時間以内の完全な報告を義務付ける新措置により、組織はインシデント対応のため週末も職員を配置する必要が生じる可能性がある。DSIT は、インシデント報告対応に伴う週末業務の規制当局負担コストを算出した。このコストの現在価値は、2025 年価格ベースで 10 年間にわたり 199 万ポンドとなる。

非金銭的価値直接コスト

措置 13 および 14 (指示権限) はコストを伴うが、現段階ではこれらのコストを貨幣換算することは不可能である。規制当局は重要供給者の識別・指定に関連するコストも負担する可能性があるが、本法案は規制当局にこれを義務付けていないため、このコストは間接的である。

感度分析

分析全体を通じて、使用した仮定に不確実性がある範囲を示すため、低・中・高の推定値を提供している。

加えて、影響評価で推定された最高コストについて感度分析を実施した。最も重要なコストは、新規規制対象事業体が規制遵守のために必要とする継続的な追加サイバーセキュリティ支出の推定値である。推定コストが 20%変動すると、推定 NPSV (正味現在価値) と EANDCB (経済的純追加コスト) は 15%変動する。

新規規制対象事業者の中で、RMSP（登録管理サービスプロバイダー）が最大の構成要素である。したがって、規制対象となる RMSP 数の推定値を変更すると、推定コストに重大な影響を与える。推定コストが 20%変化すると、推定 NPSV（正味現在価値）と EANDCB（経済的損失の許容限界）は 13%変化する。

より軽微な影響として、分析は新たな報告スケジュールに伴う推定インシデント報告コストに敏感である。これらのコストが 20%変動すると、NPSV と EANDCB は 3%変動する。

10. 広範な影響

小規模・零細企業への影響

2018年 NIS 規則は現在、小規模・零細企業への影響は最小限である。小規模・零細デジタルサービスプロバイダ（DSP）は免除対象であり、また多くの中小規模 OES が適用範囲に含まれる可能性は低い。2022年 PIR 調査では、適用範囲内の小規模・零細 OES は 1 社のみであった。⁵⁸ 本法案では、この免除規定を改正し、小規模・零細 DSP および MSP が重要供給者と認定された場合、規制当局により NIS 規則の適用対象に指定されることを提案している。これにより、高リスク供給者に対する比例原則に基づく規制が確保される。

この改正が必要とされる理由は、規模に関わらず全ての重要供給者が CNI（重要国家インフラ）、重要サービス、英国経済にリスクをもたらす得るためである。中小企業連盟（FSB）が 2019 年に実施した調査によれば、中小企業は 1 日あたり約 1 万件のサイバー攻撃を受けている。同報告書では、こうした攻撃による中小企業コミュニティへの年間コストを 45 億ポンドと推計している。⁵⁹ また「サイバーセキュリティ侵害調査 2025」によれば、過去 1 年間に侵害や攻撃を識別したと報告した企業は、零細企業の 41%、中小企業の 50% に上った。⁶⁰ これらの調査結果は、我が国の CNI 及び重要サービス供給網を構成する中小・零細企業がもたらす潜在リスクを緩和する必要性を浮き彫りにしている。

選定されたアプローチには大きな支持がある。2022 年のサイバーレジリエンス法に関する政府協議では、回答者の 70% が、小規模・零細 DSP（指定セキュリティプロバイダー）の免除規定を修正し、最も重要な少数の組織を NIS 規則（ネットワーク情報セキュリティ規則）の規制対象とすべきだと同意した。さらに、零細企業の 100%、中小企業の 75% が免除規定の修正に賛成した。⁶¹ DSIT は中小・零細 MSP との協議を実施したが、彼らは概ね、一部の中小零細 DSP/MSP を法案の対象範囲に含めることに支持を示した。規制強化による中小企業がプロバイダとして提供する商品・サービスの価格上昇リスクは低いと見なされている。2022 年 PIR の証拠によれば、NIS 規制対象事業体の 93% は、2018 年 NIS 規制の結果として商品・サービスの価格を引き上げていない。⁶²

DSIT は、規制当局と緊密に連携し、この措置の実施において小規模・零細企業向けの適切なガイダンスを策定する。

データセンター事業者向け SAMBA

データセンター事業者（DCO）向けには別途 SAMBA が実施された。昨年委託した調査によると、英国で事業を行う DCO は 68 社あり、そのうち 64 社は（国務長官により確認済み）適用対象となる 1MW 以上のデータセンターを少なくとも 1 つ保有している。従業員数は 2 つの情報源から取得した：

- 主に Beauhurst 社によるもので、同社の情報は大部分が会社登記所（Companies House）のデータに基づいている。45 社の DCO について従業員数が判明した。
- 追加の 8 社の従業員数は、2023 年に The Data City がウェブスクレイピングで取得したデータから得た。

このうち 49 社が対象範囲の閾値を満たしている。⁶³ このサンプルによると、対象範囲内と推定される中小企業数は、これら 49 社のうち以下の通りである。

⁵⁸[2018年ネットワークと情報システム規制の第二回実施後レビュー - GOV.UK](#)

⁵⁹「中小企業は 1 日あたり約 1 万件のサイバー攻撃を受けている」FSB（2019 年）[中小企業への 1 日 1 万件のサイバー攻撃 - CPA | 信用保護協会](#)

⁶⁰[サイバーセキュリティ侵害調査 2025 - GOV.UK](#)

⁶¹[英国のサイバーレジリエンス強化に向けた立法提案 - GOV.UK](#)

⁶²[2018年ネットワークと情報システム規制の第二回政策影響評価 - GOV.UK](#)

⁶³MW IT 容量に閾値を適用しなかった場合、追加で 2 社の中小企業 DCO（雇用者数推計がある 49 社のサンプル内）が包含される（非中小企業も追加で 2 社）。ただし割合はわずかに変化するのみである——79%となる——なぜならサンプル内の DCO 総数は 49 社ではなく 53 社となるためだ。

表 10.1 :

	対象範囲内の中小企業数	49 社に占める割合	95%信頼区間 (パーセンテージポイント)
中小企業 (従業員数 500 人未満)	38	78%	13%
小規模及び零細企業 (従業員 50 人未満)	21	43%	21%
中規模 (50 以上 500 未満)	17	35%	23%

これらの推定値にはいくつかの注意点がある :

- 信頼区間は、推定値における実際の誤差の規模を過小評価している。これは単なる標本誤差に過ぎないからだ。従業員数の不正確さは定量化できないが、a) その基本的な性質と b) 所有構造を考慮すると、おそらく重大なものである。
- 数値自体が中小企業の負担の実態を過大評価している理由はいくつかある :
 - データセンター業界は雇用密度が低い一方で、比較的高い収益を生み出している。登録やインシデント報告の管理負担に追加の従業員が必要となる場合、大半のデータセンター事業者 (DCO) は関連コストを賄えると予想される (彼らが現在これを行っていない理由は、単に本法案が対処しようとする例外扱いを受けているからに過ぎないことを忘れてはならない) 。
 - 雇用者数は英国で登録された事業者には雇用されている者だけを表している。多くの場合、これらの事業者ははるかに大規模な企業 (しばしば米国の大手テック企業) に所有されている。特定のデータセンター運営を目的に設立された事業者もあり、関連する従業員数はエンタープライズの真の雇用をある程度人工的に表現したものだ。Beauhurst で確認された関連企業の 75%は最終親会社ではない。

DCO が一定の標準を満たすことが期待される場合、その負担は最小限に留まると見込まれる。業界は省庁に対し、既にあらゆる関連標準を満たしていることを明確に伝えており、小規模事業者が例外であるとの示唆はない。

競争への影響

この市場の高度なプレイヤーにとって、より予測可能で一貫性のある事業環境は、品質に基づく競争力の促進、ひいては投資誘致に寄与する可能性がある。同様に、より安全なビジネス環境は、デジタル企業が英国で事業を展開する動機付けとなるだろう。

本法案は、規模や業種を問わず全ての事業者が一貫した最低限のサイバーセキュリティ標準を遵守することを保証することで、競争にプラスの影響を与えると期待される。これにより、レジリエンスへの投資を怠ることでコスト優位性を得る、セキュリティ対策が不十分な企業の能力が低下し、より公平な市場条件が促進される。結果として中小企業の参入障壁が低下する。本法案はまた、サイバーセキュリティへの期待値のばらつきに伴う複雑さや不確実性を減らすことで、デジタル経済

全体における信頼を向上させ、イノベーションを促進し、中小企業の競争力を高める。さらに、サプライチェーンのセキュリティを強化することで、より安定的で競争力のあるデジタルサービスを支援する。

環境への影響

本法案の措置は、物理的運用や環境資源ではなく、主にデジタルインフラ、規制順守、リスクマネジメントに焦点を当てている。したがって、直接的な環境影響はないと見込まれる。

国家安全保障への影響

本法案は、エネルギー、運輸、医療、通信などの重要分野において、より強固なサイバーセキュリティ対策の実施を義務付けることを目的としている。これらの分野はサイバー攻撃の標的となり得るため、レジリエンスを強化することで国家規模の混乱リスクを最小化する。インシデント対応とレジリエンス計画に関する明確な義務を定めることで、サイバーインシデントの検知、対応、復旧に向けた国家の備えを強化する。これにより、国家システムの弱点を悪用しようとする敵対国やサイバー犯罪グループの戦略的優位性を低下させる。

本法案は、サードパーティサプライヤーもセキュリティ標準を満たすことを求める。これによりエコシステム全体が強化され、セキュリティ対策が不十分な請負業者を通じて攻撃者が機密システムに侵入するのを防ぐ。

セクター別影響

本法案は、より安全で信頼性の高いデジタル運用環境を提供することで、特にデジタルビジネスに有益であると期待される。義務化されたサイバーセキュリティ標準は、セクター横断的な脆弱性を低減し、システムリスクの低下を通じて全てのデジタルビジネスに利益をもたらす。複雑なサプライチェーンやデジタルインフラに依存する競争力のある企業は、パートナーも安全であることを認識することで恩恵を受ける。

本法案の標準への準拠は、顧客や投資家に対する信頼の証となる可能性がある。特にサイバーセキュリティが調達における主要要素となる企業間取引（BtoB）環境では、レジリエンスを示す企業が顧客や契約を維持する可能性が高まる。

レジリエンス強化策の奨励と実施は、サイバーインシデントによる事業中断を最小限に抑えるのに役立つ。これは、ダウンタイムが直接的な収益損失に直結する電子商取引、SaaS プラットフォーム、フィンテック企業などのデジタルビジネスにとって特に価値がある。

貿易への影響

高いレジリエンス標準は、特に規制産業において、英国のデジタル企業を国際的な顧客やパートナーにとってより魅力的にする。これは英国企業を進展するサイバーセキュリティの国際基準に適合させ、サービス輸出や国際投資誘致を支援する。

11. 優先案の規制スコアカード


パート A : 全体的およびステークホルダーへの影響

(1) 総福祉への全体的影響		方向性評価
		注：以下はあくまで例である
全体的な予想影響の説明	非金銭的価値便益は、これらの措置を総合した福祉への影響を適切に表現している。サイバー攻撃の悪影響を軽減することは、企業と社会全体にとって有益である。	プラス 全ての影響（非金銭的価値影響を含む）に基づく
金銭的価値影響	2025年現在価値における総正味純便益（NPSV）： 最善推定値：-12億300万ポンド 低推計値：-7億6800万ポンド 高推計値：-17億4100万ポンド	マイナス 想定される正味現在価値（£）に基づく - 金銭化されていない便益
非金銭的価値の影響	サイバー攻撃の発生率と影響の減少を中心に、重要な非金銭的価値便益が識別されている。これは、NIS規制の対象となる事業体を拡大し、規制の執行を強化し、情報共有を促進することで実現される。	プラス
重大な分配的影響または悪影響はあるか？	ない	プラス
(2) 企業への予想される影響		
事業全体への影響の説明	対策への準拠には企業にとってコストが発生する可能性があるが、セキュリティとレジリエンスを強化し、サイバー攻撃による推定コストの削減に寄与する。ただし、回避される攻撃の数を推定できないため、これらの対策によって回避されるコストの割合を算出することは不可能である。 影響評価で概説された改正 NIS 規則の主な利点は、セキュリティの改善が期待され、それにより重要サービスに対するリスクが低減されることである。これは経済生産と社会の福祉を支えるためにこれらのサービスに依存しているため、ひいては英国の経済的繁栄に寄与する。これらの利益は、以下の二つの要因から生じると予想される：保護対策の改善による重大な混乱を伴うインシデント数の減少、および適切なインシデント対応計画の整備による影響の軽減である。	プラス 規制コストによる負の影響はあるが、サイバー攻撃の防止による企業への影響は大きいと見込まれる。
金銭的価値に換算した影響	事業 NPV：2025年現在価値 最善推定値：-11億8600万ポンド EANDCB：1億3770万ポンド（2025年現在価値）	マイナス 予想される事業 NPV と便益の欠如に基づく
非金銭的価値の影響	これらの対策の便益は、回避されたサイバー攻撃の数を正確に見積もることが不可能であるため、貨幣換算されていない。しかし、この対策は、保護措置の改善により重大な混乱をもたらすインシデントの数を減少させる。また、適切なインシデント対応計画が整備されることで、影響の軽減につながる。	プラス
重大な分配的影響または悪影響はあるか？	ない	プラス

(3) 世帯への予想される影響		
世帯への全体的な影響の説明	更新された NIS 規制により、世帯は直接的な影響を受けない。世帯は、サイバー攻撃の防止強化と、それらが個人に及ぼす負の波及効果の軽減という間接的な恩恵を受ける。	プラス
金銭的換算による影響	該当なし	中立 世帯への影響なし
非金銭的価値の影響	サイバー攻撃による負の波及効果の減少 - 間接的な利益	プラス
重大な分配的影響や悪影響はあるか？	ない	中立

パート B : 政府全体の優先事項への影響

カテゴリー	影響の説明	方向性評価
ビジネス環境： 本措置は英国における事業活動の容易さに影響を与えるか？	本法案の長期的な影響は、英国のビジネス環境にとってプラスになると予想される。サイバー攻撃は事業に混乱と多大なコストをもたらす、成長と革新を行う上で不安定な環境を作り出す。本法案は、対象範囲を拡大し規制当局にセキュリティ要件の執行強化権限を与えることでサイバー攻撃を減らすことを目指す。また、規制当局と政府が利用可能な情報を強化し、サービスが迅速に回復できるようにすることで、成功したサイバー攻撃の影響を軽減する。破壊的なサイバー攻撃を恐れることなく、企業が拡大と革新に自信を持って取り組めるよう環境を安定化させることで、本法案は政府の最優先課題である経済成長と国民全体の利益に貢献する。	支持する
国際的配慮： 本措置は国際貿易・投資を支援するか？	2018 年 NIS 規則は、英国に設立されているか否かを問わず、規制対象サービスを提供するあらゆる事業体に適用されることを常に意図していた。これは現在も変わらないが、本法案により MPS、データセンター、大規模負荷制御装置（LLC）分野でより多くの事業体が適用対象となり、その一部は英国国外の企業となる。したがって、これら 3 つのグループに属する英国国外の企業にとっては、規制遵守に伴う追加コストが発生する可能性があり、英国での事業展開意欲に影響を与える恐れがある。 しかしながら、高いレジリエンス標準は、特に規制産業において、英国のデジタル企業を国際的な顧客やパートナーにとってより魅力的にする可能性がある。これは英国企業をサイバーセキュリティに関する進化する国際基準に整合させ、サービス輸出や国際投資誘致を支援するものである。 貿易への悪影響は予想されない。	支持する
自然資本と脱炭素化： この措置は環境改善と脱炭素化への取り組みを支援しているか？	負荷制御は、エネルギー使用を最適化し、再生可能エネルギー源をより効果的に統合することで、脱炭素化を支援する上で重要な役割を果たす。負荷制御市場にサイバーセキュリティ要件を義務付けることは、新興分野における消費者の信頼を高め、スマートで柔軟なエネルギーソリューションの導入を促進する。これは脱炭素化と英国政府のグリーンエネルギー目標の達成に寄与する。 負荷制御市場にサイバーセキュリティ要件を求めることは、新興分野における消費者の信頼を高め、スマートで柔軟なエネルギーソリューションの導入を促進	支持する

<p>する。これは脱炭素化と英国政府の「クリーンパワー2030」および「ネットゼロ」目標の達成に寄与する。さらに、安全でレジリエントな負荷制御市場と広範な英国電力網は、スマートエネルギーへの投資をさらに促進し、同分野の成長と持続可能なエネルギー実践の導入を加速させる。</p>	
--	---

12. 優先案のモニタリングと評価

本法案は、NIS 規則 2018 を更新し、より多くの事業体を適用範囲に含め、規制当局が職務を遂行するための権限を強化し、政府が緊急のサイバー脅威に対応するための比例的な権限を盛り込むものである。2018 年 NIS 規則は、2020 年⁶⁴と 2022 年⁶⁵の 2 回の PIR（政策実施レビュー）を通じて評価された。これらは、2018 年 NIS 規則が当初の目的をこれまでの程度達成できたか、それらの目的が依然として適切であるか、また 2018 年 NIS 規則の実施状況と発生した費用・便益を分析したものである。これらのレビューは、NIS 規則 2018 が「ネットワークと情報システムインシデントに対する保護水準を（可能な限り）防止し、改善する」という目的の達成において、おおむね成功裏に機能していることを示した。ただし、改善すべき点も示された。NIS 規則自体への改善提案も含まれる。PIRs はまた、セキュリティの改善が進められている一方で、組織がサイバー攻撃からシステムを防御するための十分な措置を講じていないことも明らかにした。これに対し、前保守政府は、PIRs で識別された課題に対処し、当時のサイバー環境に対応するための立法措置案について協議を行い、その後分析を実施した。⁶⁶ 提案された立法措置は法案の基礎を形成したが、2025 年における英国の固有の課題と将来を見据えた対応を確保するため、さらに発展・拡充された。当初の立法措置のコストと便益は、2022 年の協議で示された。しかし、2022 年の協議終了後、コンプライアンス活動のコスト、組織（中小企業を含む）による差異、企業が法令を理解するために要する時間など、今後監視が必要なさらなる証拠の不足が識別された。こうした課題の把握に向けた作業は既に始まっている。本影響評価の策定プロセスを通じて、今後追跡・測定可能な主要指標が識別された。これにより提案措置の成果を測ることが可能となる。

国務大臣には、NIS 規則を 5 年を超えない間隔で見直す法的義務がある。2018 年 NIS 規則の次回の PIR は現在、2027 年に実施予定である。DSIT は、法案が完全に実施され、国王の裁可を受けた後に効果を発揮する時間を確保するため、このタイミングが適切かどうかを検討中である。次回の PIR では、以下の比例的かつ適切な調査を実施する予定である：

- a. **プロセス評価**：施策の実施状況の評価し、意図しない結果を識別する。これは将来の改革実施を改善するための変更方法にも情報を提供する。
- b. **影響評価**：介入とその成果の因果関係を、措置の当初の目標と比較して確立する。これにより計画された変更がもたらした効果の規模を評価する。

今後の PIR 準備及び法案の継続的实施・評価を支援するため、DSIT は常設フォーラムを通じた NIS 規制当局との定期的な連携、並びに業界・団体（techUK、中小企業連盟等を含むがこれらに限定されない）との連携を実施する。DSIT はデータと知見収集のための正式な調査を実施し、分析結果を評価に反映させることで将来の PIR に貢献する。

提案されている法案の措置の下では、政府は NIS 規制当局に対する戦略的優先事項声明を指定する権限を持つ。国務大臣は、戦略的優先事項声明に含まれる成果の達成に向けた規制当局の進捗状況を年次報告する義務を負い、この報告に資するため規制当局からの情報提供を要求できる。国務長官の年次報告書は、関係者が NIS 規制の実施における規制当局の進捗状況を把握できるよう、適切な方法で公表される。これらの年次報告書は、法案及び NIS 規制の監視・評価を支援し、制度の有効性を向上させるための政府の将来的な介入に情報を提供する。

影響評価とプロセス評価の基礎は、アセスメントの初期段階で提示された「変化の理論」（表 4.1）の詳細版に基づく。

表 4.1 で概説した通り、優先改革パッケージの期待される長期的成果と影響は以下の通りである：

⁶⁴[ネットワークと情報システム規制 2018 の PIR](#)

⁶⁵[ネットワークと情報システム規制 2018 の第二回 PIR - GOV.UK](#)

⁶⁶[英国のサイバーレジリエンス強化に向けた立法提案 - GOV.UK](#)

- 成果 1：国民が日常生活を送れるよう、重要サービスと企業を防御する
- 成果 2：規制当局が NIS 規則を実施する十分な能力を備え、経済成長を促進する安定した環境を創出する
- 成果 3：英国の国家安全保障を強化し、NIS 規制が効果を維持できるようにする

以下の表は、法案内で提案されている政策の成功を正確かつ効率的に測定するために必要な手法と資源を詳細に示すものである。

表 12.1：改革パッケージの長期的影響と、その監視・評価方法

長期的な影響	監視・評価方法
公共サービスと企業を防御し、市民が日常生活を送れるようにする	NIS PIRs 戦略的優先事項に関する年次報告 NCSC サイバースリスク評価フレームワークの集計データ分析 評価枠組み提出データの分析（特定分野における事業者のサイバースリスクマネジメント状況と規制要件遵守度を示す）
規制当局が NIS 規則を実施する十分な体制を整え、経済成長を促進する安定した環境を創出する	NIS PIRs 戦略的優先事項に関する年次報告。 NIS 規制当局に対する定期的な調査 NIS 規制当局との定期的な連携 NCSC サイバーの分析 アセスメント枠組み提出データの分析
絶えず変化する脅威環境において、英国の国家安全保障を強化し、NIS 規制が効果を維持することを確保する	NIS PIRs 戦略的優先事項に関する年次報告書の提出 NIS インシデント総数 - サイバーインシデントを含む 自主報告

多くの影響評価は、DSIT などが新たなデータソースやモデリングを開発し、現在の証拠の不足を補うことに依存する。本影響評価のリスクと仮定のセクションでは、既存の証拠不足によりモデリングの仮定がなされたことが強調されている。この場合、DSIT は今後これらを記録する戦略を確保する。以下の表は、これらの仮定と、そのモニタリング・評価に関する提案された今後の方向性をまとめたものである：

表 12.2：証拠の不足箇所と提案されるモニタリング・評価手法

長期的な影響	証拠の不足点	提案されるモニタリングと評価
サイバー攻撃に対するサプライチェーンのレジリエンス向上	規制対象となる英国のエンタープライズデータセンター数の把握	英国 BDS の詳細分析

英国の国家安全保障の強化と NIS の確保 絶えず変化する脅威環境において規制の有効性を維持する	サイバー攻撃の反事実的および現在の実態への影響の把握	サイバー定量化プロジェクトはサイバー攻撃の経済的コストを定量化する サイバーアセスメント 枠組みの見直し DSIT によるデータの年次非公式かつ内部レビューの検討
重要サプライヤーの数	各セクション内で重要サプライヤーとして指定され、NIS の対象範囲に組み込まれるべき企業の数を把握する	各規制当局による、自部門内で重要と認定したサプライヤーに関する年次報告

本モニタリング・評価戦略は、NIS PIR（重要インフラ保護指令）の活用と、NCSC サイバーアセスメント枠組みの集計データ分析に依存する。これらのデータソースに変更が生じた場合、証拠の不足を補うべく、既存の DSIT リソースを評価目的に比例配分するか、新たな一次データ収集のための競争入札を実施し、既存の二次データソースを統合する独立調査機関を通じ、必要な情報・データへのアクセスを確保する。

本影響評価の便益セクションで概説した通り、確固たる対照事実が欠如しているため、サイバーインシデントやサイバーリスクの低減効果を検証することは不可能であった。インシデント件数などのトップダウン指標は依然として収集が重要だが、NIS 規制のパフォーマンスを単独で測る適切な尺度ではない。サイバーセキュリティの改善は、インシデントの減少ではなく、組織による検知件数の増加につながる可能性がある。なぜなら、脆弱なサイバーセキュリティを持つ組織は侵害に気づかない場合があるからだ。2020 年及び 2022 年の PIR（年次報告書）では、改善計画などの措置を通じて、2018 年 NIS 規制が重要経済インフラ（OES）のサイバーセキュリティ向上に寄与しているか評価可能な情報が収集された。

DSIT は現在、4 つの異なる分野において規制当局から主要業績評価指標を毎年収集する計画を有している：

1. 保証と理解
2. 改善
3. インシデント
4. 能力

保証と理解は、サイバー評価枠組みのレビューと、基本プロフィールおよび強化プロフィール（該当する場合）を満たす組織の数に焦点を当てる。これは、NIS 規則の結果として規制当局と組織双方が持つ理解度を評価するのに役立つ。また、規制当局が自らが管轄するセクターや地理的地域のサイバーリスクプロフィールを十分に理解しているのかも評価する。

改善は、組織がいつサイバー評価フレームワークのプロフィールを満たすか、改善計画が実施・完了しているかに焦点を当てる。執行措置もこのセクションに含まれ、NIS 規則を通じて組織に変化が強制されているかを検証する。追加のコンプライアンスにつながる成功

枠組みのプロフィールを満たす時期、および改善計画が実施・完了されているか否かに焦点を当てる。執行措置もこのセクションに含まれ、NIS 規則を通じて組織に変化が強制されたかを確認する。追加的なコンプライアンス達成につながる成功した執行活動は、全体の改善の目的において成功としてカウントされる。また、失敗の理由に関するより深い洞察を提供し、将来の非コンプライアンス発生源の監視を改善する。

インシデントでは、NIS 関連のインシデント総数だけでなく、特にサイバーインシデントに関連する件数を把握する。DSIT は、自主的に報告されるサイバーインシデントの増加も望んでいる。

最後に、能力とは規制当局が規制機能を遂行する能力を指す。これにより DSIT は、どの規制当局が資源面で苦戦しているか、またその理由を理解できる。

DSIT によるこの年次非公式内部データレビューは、より早期の正式レビュー実施の必要性を浮き彫りにする。また、NCSC や規制当局から NIS 規則が意図した通りに機能していないとの助言を受けた場合、DSIT は NIS 規則の実施状況評価を早期に実施することも検討する。

主要業績評価指標のこの年次データ収集に加え、DSIT は監視計画において以下の個別分野の影響を把握する必要がある：

- a. コスト
- b. 効果
- c. 他の規制との相互関係（2021 年電気通信（セキュリティ）法、2018 年データ保護法、2023 年オンライン安全法、および「設計段階からのセキュリティ」） 防御法 2018、オンライン安全法 2023、および「設計段階からのセキュリティ」との相互関係）
- d. イノベーションへの影響
- e. 貿易への影響
- f. 競争への影響

コスト

DSIT は、過去 2 回の PIR および 2018 年 NIS 規制の対象組織との直接対話を通じて、既にコストに関する良好なデータを保有している。追加要件のコストは次回の PIR で把握する必要がある。DSIT が、2018 年 NIS 規制の当初コストと、その後の改正による更新 NIS 規制の変更に伴うコストを明示できる質問を選択すべきである。より詳細な把握が必要なコスト例：

- NIS 規則による指定を受けた結果生じた契約変更のコスト（存在する場合）。
- 組織によるインシデント報告のコスト。新たな報告期限を考慮し、組織によるインシデント報告コストと楽観度推定値の両方をより深く理解するため、将来的に追加データ収集が必要である。
- 指定対象となる重要供給業者の数と、これらの事業体にかかるコスト。
- 規制当局が執行活動のコストを回収した結果、組織が負担するコスト。これには、規制当局と協議してこの権限の行使方法を理解すること、および組織から発生したコストの規模と影響に関するデータを収集することが含まれる。

NIS 規制のコスト評価手法は、過去の PIR と同様となる。これらの措置により新たに指定された組織の数、措置の結果として報告されたインシデントの数、重要サプライヤー措置の初期コストが正確であったか否かを考慮する必要がある。コストは措置ごとに細分化される。

前述の通り、NIS 規則の便益を金銭的価値で把握することは困難であるが、DSIT はこれらの課題の克服を目指している。DSIT は政府横断的な関係者と連携し、サイバー攻撃の経済的コスト、ひいてはその防止価値を定量化する手法の理解を深めている。

サイバーリスク定量化プロジェクトは、消費者、政府、企業を含む全ての事業者に対するサイバー攻撃の経済的コストを定量化することを目指す。本プロジェクトの成果は、NIS 規則の対象分野を含む英国経済へのサイバー攻撃の潜在的影響に関する包括的な見解を提供する。⁶⁷

他の規制との相互関係

デジタル分野における規制の数が増加しており、組織は異なる領域にわたって遵守が求められる。規制の増加は、それらが日常生活においていかに重要になったかを反映している。これらの規制が互いにどのように相互作用するかを監視し、大規模組織であっても過重な負担になっていないかを確認すべきである。

このため、NIS 規則と重複する可能性のある規制を洗い出す。DSIT は、他の規制と重複する組織の意見を確実に収集する。規制の重複が個別対応時よりもコスト増加をもたらすか、あるいは単一のサイバーセキュリティ標準を満たすだけで節約効果が生じるかについて、コストを検証する必要がある。

イノベーションへの影響

DSIT は既に組織のイノベーション能力への影響に関する情報を収集しており、今後の見直しでも収集を継続する。質問はイノベーションの様々な領域に踏み込み、NIS 規則がサイバーセキュリティ分野のイノベーション能力、より広くは組織が提供するサービス内容に影響を与えるかどうかを検証すべきだ。

貿易への影響

DSIT は、規制が価格に及ぼす潜在的影響を把握するため、引き続き情報を収集する。これは英国サプライヤーの競争力への潜在的影響を理解する材料となる。これに加え、今後のレビューでは、NIS 規制の結果として組織が貿易能力への影響を認識しているかどうかの情報収集も行うべきだ。これにより、価格以外の経路を通じて貿易活動が影響を受けたかどうかを評価するのに役立つ。

競争への影響

DSIT は今後 1 年間、法案で提案された変更の影響を受ける市場の集中度に関する情報を収集し、競争審査のベースラインを設定する。その後は毎年情報を収集し、市場に大きな変化があるかどうかを監視する。変化があった場合、DSIT はその変化が NIS 規制によるものかどうかを深く掘り下げて理解する。

NIS 規則が組織の価格設定に影響を与えているかどうかの情報を収集することは、NIS 規則が組織の市場競争力に何らかの影響を与えているかどうかを評価するのに役立つ。企業がコストを増加させないか、わずかな増加のみの場合、規則が競争に大きな影響を与えている可能性は低い。

世帯への影響

規制の影響をより広く評価するため、DSIT は NIS 規則が貿易、イノベーション、競争に与える影響に関する証拠を検討し、世帯への影響の程度を評価する。

⁶⁷<https://www.gov.uk/government/publications/independent-research-on-the-economic-impact-of-cyberattacks-on-the-uk>

13. 優先案における行政コストとコンプライアンスコストの最小化

サイバー攻撃は、前述の「メリット」セクションで述べたように、企業やサービス事業者にとって多大なコストを伴う。本法案の主目的は、サイバー攻撃の件数を減らし、万が一インシデントが発生した場合でも個人や企業への影響を最小限に抑えることである。長期的には、本法案の措置により企業のコスト削減を図り、成長と革新が可能なビジネス環境を安定させる。これにより経済成長を促進し、働く人々の利益につなげることを目指す。

短期的には、政府は本法案の措置が規制当局の責任を拡大し、企業や重要サービス事業者がネットワーク保護のため追加措置を講じる必要が生じることを認識している。更新された NIS 規則への対応や拡充されたインシデント報告枠組みへの参加に伴い、組織には一定の行政負担が生じると予想される。NIS 規則の適用対象となる組織（例：データセンター事業者）は、2018 年 NIS 規則の適用対象組織が既に実施している措置と同様に、ネットワークの保護とサイバーセキュリティ対策の評価を講じる必要がある。政府は適切な場合、組織の順守を支援するガイダンスを作成し、更新された NIS 規則の実施状況を監視するため、業界と緊密に連携し続ける。法案成立時には移行期間が設けられ、影響を受ける組織が変更し備える十分な時間が確保される。移行期間の長さは関係者と協議の上決定され、小規模・零細企業への影響が考慮される。さらに、二次立法で定める措置（更新されたサプライチェーンセキュリティ対策を含む）については正式な協議が行われ、その過程で企業へのコスト負担が慎重に検討される。

要するに、政府は実施期間の設定、ガイダンスの提供、適切な場面での正式な協議を通じて、企業へのコスト負担を最小限に抑える方針だ。本法案の措置は、広範な規制対象事業者のセキュリティ強化が急務であることと、規制が企業にとって過重な負担とならないことの適切なバランスを図るよう設計されている。更新された NIS 規制の実施に伴う組織のコストは、英国で最近発生したサイバー攻撃事例が示すように、破壊的なサイバーインシデントの潜在的影響と比較すれば軽微である。

14. 宣言

省庁：

科学技術革新省

問い合わせ先：

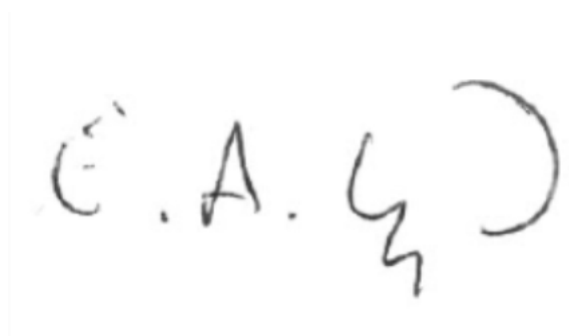
ケリー・ノース、法案担当副部長、kelly.north@dsit.gov.uk

担当大臣：

リズ・ロイド、国務大臣（デジタル経済担当）

私は影響アセスメントを読み、入手可能な証拠に基づき、主要な選択肢の予想されるコスト、便益、影響について合理的な見解を示していると判断した。

署名：

Handwritten signature in black ink, appearing to read "E.A. Lloyd".

日付：

2025年10月31日

附属書 A. 要約：分析と証拠

最終段階の影響アセスメントのため、これらのセクションを完全な証拠基盤を含めて最終化すること。

価格基準年：2025年

PV 基準年：2026年

	1. 現状維持（ベースライン）	2. 優先的な進め方（最小限の対応でない場合）
正味現在価値（社会的価値） （個々のコストと便益の範囲を含む簡潔な説明付き）	該当なし	最善の推定値：-12億100万ポンド 低推計値：-7億6600万ポンド 高推計値：-17億4000万ポンド 影響評価において金銭的便益が算定されていないため、NPSV（正味現在価値）は著しくマイナスとなる。これは本報告書全体で正当化されている。最も大きなコストは、NIS規制の対象となる新規事業体と、同規制に準拠するために継続的に発生するサイバーセキュリティコストに起因する。
公共部門の財務コスト （範囲を含む簡潔な説明付き）	該当なし	13の規制当局には一定のコストが発生する。うち12機関は既に2018年NIS規則の執行を担当している。新規制への対応コストが発生し、規制対象事業体の増加により一部ではコスト増となる。ただし本措置により規制当局はコンプライアンス推進能力を強化され、職務遂行に必要な資源と重要情報を確保できる。また、これらの措置は政府が国家安全保障の防御のための断固たる行動を取るための手段を提供する。 さらに、本法の適用対象となる公共部門組織も、理解促進とコンプライアンス対応のコストを負担することになる。これらは分析において個別に考慮されておらず、OES（公共サービス機関）への総コスト額に含まれている。
定量化されていない主な便益とコスト （説明、可能な場合は規模）	該当なし	これらの措置からは、計量化・金銭的価値されていない重要な便益が生じる。本法案の主たる便益は、企業をサイバー攻撃から防御し、投資と革新が育まれる環境を醸成することにある。より多くの事業体を適用範囲に含め、規制当局の職務遂行能力を強化することでサイバー攻撃に対する防御力を高めれば、企業がサイバー攻撃に対処するために要する時間（多くの場合、サービス停止を伴う）を短縮できる。攻撃が発生した場合、改善されたインシデント報告により、規制当局とNCSCはこの情報を活用して、他の企業や組織に助言や指導を提供し、連

		携することができる。これにより、各組織は自らを防御し、特定の攻撃や攻撃の種類による広範な影響の緩和を講じることが可能となる。これらの措置への準拠には企業にとってコストが発生する可能性があるが、セキュリティとレジリエンスを強化し、サイバー攻撃のコスト削減に寄与する。ただし、回避される攻撃の数を推定できないため、これらの特定対策によって回避されるコストの割合を算出することは不可能である。
主なリスク (関連する場合、リスクコストおよび楽観バイアスを含む)	該当なし	<p>主なリスクは、本影響評価におけるコストの過小評価の可能性に起因する。ただし、仮定は 2018 年 NIS 規制の初期影響評価策定時の証拠収集を通じて裏付けられ、規制施行後に行われた 2 回の PIR を通じて改善されている。</p> <p>本法案の重要なコストは、規制の対象範囲に新たに含まれる RMSP に生じる。DSIT は対象となる RMSP の数を推定するため特別調査を委託しており、これらの事業体に対するコストの誤った見積りに伴うリスクを低減している。</p>
感度分析の結果		<p>最も大きなコスト負担は、NIS 規制に新たに組み込まれる事業体にかかる。これらは RMSP、データセンター、大規模負荷制御事業者、指定重要供給事業者である。これらのコストは、規制に準拠した十分なサイバーセキュリティを確保するためのコストと、インシデント報告のコストである。指定される重要供給事業者の数を正確に見積もることは不可能であった。他の 3 つのグループについては分析が行われ、低・中・高のシナリオを用いてコスト範囲が提示されている。</p> <p>コストセクションで概説した追加の感度分析によれば、新規対象企業の年間追加サイバーセキュリティ支出の推定コストが、NPSV（正味現在価値）に特に敏感に反応することが示された。企業当たりの想定値を 20%変更すると、NPSV と EANDCB（経済的損失調整後純現在価値）は 15%増減する。</p> <p>より軽微な影響として、新たな報告スケジュールに伴うインシデント報告コストの推定値にも分析は敏感である。これらのコストが 20%変動すると、NPSV と EANDCB は 3%変動する。</p>

