

HANDBOOK FOR CYBER STRESS TESTS

MAY 2025

ENISA について

欧州連合サイバーセキュリティ機関（ENISA）は、欧州全体で高い共通レベルのサイバーセキュリティを実現することを目的とした欧州連合の機関である。2004年に設立され、EU サイバーセキュリティ法によって強化された欧州連合サイバーセキュリティ機関は、EU のサイバー政策に貢献し、サイバーセキュリティ認証制度によって ICT 製品、サービス、プロセスの信頼性を高め、加盟国および EU 団体と協力し、欧州が明日のサイバー課題に備えるのを支援する。知識の共有、能力開発、意識向上を通じて、ENISA は主要な利害関係者と協力し、コネクテッドエコノミーに対する信頼を強化し、EU のインフラのレジリエンスを高め、最終的には欧州の社会と市民のデジタルセキュリティを維持することを目指している。ENISA とその活動の詳細については、www.enisa.europa.eu

著者への連絡は、enisa-nis-directive@enisa.europa.eu。

本紙に関するメディアの問い合わせは、press@enisa.europa.eu。

法的

本書は、別段の記載がない限り、ENISA の見解と解釈を代表するものである。規則（EU）2019/881 に基づく ENISA または ENISA 団体の規制義務を支持するものではない。

ENISA は、本書またはその内容を変更、更新、削除する権利を有する。本書は情報提供のみを目的としており、無料でアクセスできなければならない。本書の全部または一部への言及またはその使用には、出典として ENISA を明記しなければならない。

サードパーティーの情報源は適宜引用している。ENISA は、本書で言及されている外部ウェブサイトを含む外部情報源の内容に対して責任を負わない。

ENISA および ENISA を代理する者は、本書に含まれる情報の使用について責任を負わない。

ENISA は本書に関する知的財産権を保持する。

ルクセンブルク：欧州連合出版局、2025 年

著作権表示

欧州連合サイバーセキュリティ機関（ENISA）、2025 年

特に断りのない限り、この文書の再利用はクリエイティブ・コモンズ 表示 4.0 国際（CC BY 4.0）ライセンス (<https://creativecommons.org/licenses/by/4.0/>) の下で許可されている。

つまり、適切なクレジットを付与し、変更点を示すことを条件に、再利用が許可される。

欧州連合サイバーセキュリティ機関が所有していない要素の使用または複製については、それぞれの権利者に直接許可を求める必要がある場合がある。

ISBN: 978-92-9204-700-9, DOI: 10.2824/8248517, カタログ番号：TP-01-25-009-EN-N

目次

1. 序論

1.1 スコープと対象読者

1.2 政策の背景

2. サイバーセキュリティとレジリエンスのためのストレステスト

2.1 サイバー・ストレステストの定義

2.2 監督ツールキットの一部としてのサイバー・ストレステスト

3. サイバー・ストレステストのためのステップバイステップ・ガイド

4. 国、地域、連合のサイバー・ストレステスト

5. 結論

附属書 A：医療セクターの例

附属書 B：ケーススタディ-金融とエネルギー

金融セクター - 欧州中央銀行（ECB）の 2024 年サイバーレジリエンス・ストレス・テスト

エネルギーセクター - 2024 年ハイブリッド脅威ストレステスト

参考文献

エグゼクティブサマリー

ストレステストが有名になったのは、2007年から2009年にかけての世界的な金融危機の後である。バーゼル銀行監督委員会の下、銀行規制当局が銀行の資産ポートフォリオをより綿密に監督し、金融ショックシナリオに耐えるだけの十分な強度があるかどうかを分析しようと考えたからである。

ストレステストは最近、サイバーセキュリティのテストに利用されるようになり、サイバーセキュリティとレジリエンスを評価するための軽量版的な新しい手法を提供している。例えば、2022年にはイングランド銀行が英国のリテール決済サービスのサイバー・ストレステストを実施し、2024年には欧州中央銀行（ECB）がEUの銀行の大規模なサイバーレジリエンスストレステストを実施した。昨年、欧州委員会はEU加盟国を支援し、重要事業体レジリエンス（CER）指令の範囲内で、物理的脅威に焦点を当てたEUのエネルギー部門のレジリエンスに関するEU協調ストレステストを実施した。

本ハンドブックでは、サイバー・ストレステストを「個々の組織のレジリエンスと、さまざまなリスクシナリオにおいて、重要なサービスの提供を確保しつつ、重大なサイバーセキュリティインシデントに耐え、そこから回復する能力を対象としたアセスメント」と定義している。ストレステストはレジリエンスに焦点を当て、レジリエンスの評価指標を使用し、準備対策と対応回復対策の両方をテストするために使用できる。

本ハンドブックには、サイバー・ストレステストの簡単な5ステップガイドが含まれている（図参照）：

1. テスト範囲と目的を定義し、利害関係者と関わる
2. テストの設計、手法の選択、シナリオの洗練
3. 実施
4. 結果を分析し、ギャップを特定
5. ストレステストで特定されたギャップや問題をフォローアップする。

また、このステップバイステップのガイドを実際の例に当てはめ、医療セクターでどのようにサイバー・ストレステストを実施できるかを説明する。また、国、地域、EUレベルでどのようにサイバー・ストレステストを実施できるかも説明する。

監督機関にとって、サイバー・ストレステストは、より技術的な問題だけでなく、戦略的リスクとシステミックリスクの両方について、セクターとの対話を開始する良い方法となり得る。ストレステストによって明らかになったギャップは、協調的かつ自主的な場においてオープンに議論することができるが、より厳格な監督の状況においてもフォローアップすることができる。

EUが準備態勢とレジリエンスにより重点を置き、NIS2指令⁽¹⁾の移管が完了しつつある現在のEUの政策状況を考慮すると、サイバー・ストレステストは今後数年間、NIS当局のツールキットにおける重要な新たなツールとなる可能性がある。ENISAでは、国レベル、地域レベル、EUレベルのサイバー・ストレステストの実施において、国およびEUレベルの監督機関や機関を支援することを楽しみにしている。



1. 序論

重要インフラは、現代社会の機能にとって不可欠である一方、ますます高度化し相互接続された技術に依存することで、システム障害や破壊的脅威へのエクスポージャーを高めている。欧州連合（EU）は、高水準のサイバーセキュリティを達成し、重要インフラ部門全体のレジリエンスを強化するための取り組みを強化している。

サイバー連帯法⁽²⁾は、サイバーセキュリティの脅威やインシデントを検知し、それに備え、対応するための連邦内の能力を強化するための措置を定め、こうした取り組みをさらに支援するものである。

サイバー・ストレステストはサイバーセキュリティの領域では比較的新しい概念であるため、我々は、主に重要部門のサイバーセキュリティとレジリエンスを監督する国家当局を対象として、このハンドブックを作成した。このハンドブックは、さまざまなタイプのストレステストが実施されている重要セクターのサイバーセキュリティの専門家やその他の専門家との机上調査と議論に基づいている。

サイバーセキュリティの領域では、監査、侵入テスト、倫理的ハッキング、レッドチーム、脆弱性スキャン、サイバー演習など、さまざまなサイバーセキュリティのアセスメントやテストの方法がすでに幅広く存在している。作成機関や監督機関は、環境やニーズに応じて、適切な方法を見つける必要がある。また、さまざまな方法を混ぜたり、組み合わせたりすることもできる。

このように、サイバー・ストレステストは、重要なセクターのサイバーセキュリティとレジリエンスを監督する各国当局の規制ツールキットの中で、他のよりよく知られた監督活動を補完する新たなツールとして浮上している。

本ハンドブックでは、サイバー・ストレステストの定義を提供し、共通の特徴について議論し（セクション 2）、サイバー・ストレステストのためのステップバイステップのガイドを提供し（セクション 3）、EU レベルでストレステストを実施する方法を説明し（セクション 4）、サイバー・ストレステストの実施方法の実践例を共有する。

1.1 対象範囲と対象読者

本ハンドブックの目的は、重要セクターの事業者（典型的には重要インフラの運用者や重要サービスのプロバイダ）のサイバーセキュリティとレジリエンスのストレステストについて、当局を指導することである。サイバーセキュリティ以外の領域で実施されたストレステストのケーススタディもいくつか掲載しているが、これらについてはあまり詳しく論じていない。

本ハンドブックは、改正 EU NIS 指令である NIS2 に基づき、国レベル、地域レベル、EU レベルで、重要部門のサイバーセキュリティとレジリエンスを監督する国またはセクターのサイバーセキュリティ監督機関および国のサイバーセキュリティ作成機関を対象としている。このハンドブックは、EU の金融セクターのオペレーショナル・レジリエンスに関する規制であるデジタル・オペレーショナル・レジリエンス法（DORA）に基づく監督当局や、CER 指令に基づく各国当局にとっても有用であろう。このハンドブックは、国レベルでも EU レベルでも、その他の監督機関、作成機関、政策立案者にとっても有用であろう。

1.2 政策的背景

ストレステストに関連する EU の政策イニシアチブをいくつか挙げる。

- **NIS2** : 改正 NIS 指令である NIS2 は、重要分野における情報通信技術（ICT）のサイバーセキュリティとレジリエンスを改善することを目的としている。NIS2 は、重要セクターの範囲を拡大し、これらの重要セクターの事業者に対するリスクマネジメントと報告要件を強化し、加盟国のサイバーセキュリティ能力を高め、EU レベルでの連携を強化することを目的としている。国家レベルおよび EU レベルのサイバー・ストレステストは、ネットワークと情報システム部門を監督する監督機関にとって新たなツールとなり得る。
- **欧州連合のリスク評価** : 欧州委員会、加盟国、および ENISA は、リスクシナリオを作成し、連合リスク評価を実施してきた。例えば、5G toolbox、Nevers risk assessment、Cyber risk posture report³ を参照された

²

³

い。これらの連合リスク評価は、サイバー・ストレステストに使用できる戦略的／システムのサイバーリスクシナリオの作成につながっている。

- **サイバー連帯法 (CSoA)** : サイバー連帯法は、サイバーセキュリティの脅威やインシデントを検知、準備、対応する EU の能力を強化することを目的としている。加盟国による「協調的な準備テスト」のためのサイバー予備資金メカニズムおよび EU の資金援助が導入され、これらのテストは、重要部門および特定のリスクシナリオに焦点を当て、国または地域におけるサイバー・ストレステストを含む。
- **ニニストの報告書** : ニニストの報告書「Safer Together - Strengthening Europe's civilian and military preparedness and readiness」は、欧州の民間および防衛の準備と態勢を強化する方法についていくつかの勧告を行い、広範なオールハザード、オールセクターのリスク評価を含む、連合のリスク評価を求めている。
- **DORA** : DORA (デジタル・オペレーショナル・レジリエンス法) は、NIS2 の特別法であり、EU の金融部門のデジタル・レジリエンスを強化することを目的としている。DORA は、銀行から報告された主なインシデントの分析などを通じて、金融セクター全体に共通するサイバー脆弱性やリスクを特定する仕組みを導入している。
- **CER** : CER (重要事業体指令) は、物理的攻撃や自然災害に直面した場合の重要インフラ全般のレジリエンスに焦点を当て、NIS2 を補完するものである。CER は、加盟国に対し、人為的脅威と自然災害リスクの両方を考慮したオール・ハザード・アプローチの一環として、国家戦略を採用し、リスクアセスメントを実施することで、必要不可欠なサービスの中断の影響を防止または最小化することを求めている。CER のもとで特定された重要事業体は、自動的に NIS2 の対象となる。NIS2 は、(より広範な) CER のサイバーセキュリティの *lex specialis* として機能することを意図しており、ICT システムを保護するためのサイバーセキュリティの脅威とサイバーセキュリティ対策が NIS2 の対象であることを意味する。

2. サイバーセキュリティとレジリエンスのためのストレステスト

2.1 サイバー・ストレステストの定義

ストレステスト⁽⁴⁾(⁵)とサイバーストレステスト⁽⁶⁾(⁷)には異なる定義があり、異なる文脈や目的で使用されている。本ハンドブックでは、サイバー・ストレステストを以下のように定義する：

サイバー・ストレステスト：サイバー・ストレステストは、個々の事業体のレジリエンスと、さまざまなリスクシナリオにおいて、重要なサービスの提供を確保しつつ、重大なサイバーセキュリティインシデントに耐え、そこから回復する能力に関する的を絞ったアセスメントである。

実際には、ストレステストはほとんどが「机上ベース」であり、1つ以上のリスクシナリオを中心とし、テスト対象の事業体／組織が独自に記入する技術的なアンケートに依存している。ストレステストは、準備措置と対応・回復措置の両方をテストすることができる。アセスメントは、すべてのサイバーセキュリティの側面ではなく、特定のリスクシナリオと特定の脅威に焦点を当てるため、対象を絞ったものとなる。ストレステストで特定されたギャップは、よりオープンで協調的なプロセスの中で、様々な利害関係者との協議の中で、あるいは潜在的により厳格な監督アプローチの中で、各国当局がフォローアップすることができる。ストレステストは、国、地域または EU レベルで実施することができる。

サイバー・ストレステストの特徴

サイバー・ストレステストの主な特徴を以下に挙げる

- 1. レジリエンスに焦点を当てる。**ストレステストは、さまざまなサイバー脅威に直面した場合の組織のレジリエンスを評価するために設計されている。ストレステストは予測ではなく、失敗のポイントを理解し、準備、対応、回復を改善するためのツールである。
- 2. シナリオベース。**もしもの場合」を想定し、もっともらしく、可能な限り現実の世界に近いリスクシナリオを構築する。
- 3. ストレスレベル。**ストレステストには、様々なシナリオにおける組織の準備態勢を理解するために、様々なストレスレベルがある。最も高いストレスレベルでは、ストレステストのシナリオには、「ブラックスワン」とも呼ばれる、確率が低く、影響が大きいインシデントが含まれる。
- 4. レジリエンス・メトリクス。**ストレステストでは、事業体のレジリエンスを定性的および定量的に「測定」するためにレジリエンスメトリクスを使用する。サイバーストレステストで使用されるメトリクスの例は、「検知までの時間」と「回復までの時間」である。
- 5. 個別かつ独立。**ストレステストは、多くの場合、詳細な質問票の使用を通じて必要な証拠を提供する組織によって、個別に、独立して実施される。
- 6. システミック・リスクの視点。**ストレステストは、そのセクターのシステミック・リスクの視点から出発し、連鎖効果や相互依存関係を特定するためにも用いられる。

サイバー・ストレステストではないもの

以下はサイバー・ストレステストではない：

⁴ECB ストレステスト、<https://www.bankingsupervision.europa.eu/activities/stresstests/html/index.en.html>。

⁵共同研究センター-Institute for the Protection and Security of the Citizen, Galbusera, L., Ward, D. and Giannopoulos, G., *Developing stress tests to improve the resilience of critical infrastructures - A feasibility analysis*, Publications Office of the European Union, Luxembourg, 2014, <https://data.europa.eu/doi/10.2788/954065>。

⁶Danish Financial Supervisory Authority (n.d.), 'Cyber stress testing', [https://www.dfsa.dk/Media/638665595227077818/Cyber %20stress %20testing_v4.pdf](https://www.dfsa.dk/Media/638665595227077818/Cyber%20stress%20testing_v4.pdf)。

⁷イングランド銀行(2024)、「英国銀行システムのストレステストに対するイングランド銀行のアプローチ」、<https://www.bankofengland.co.uk/stress-testing/2024/boes-approach-to-stress-testing-the-uk-banking-system>。

- **ペネトレーション・テストとは**、攻撃のライブ・シミュレーションのことで、多くの場合、実際のライブ・インフラ上で行われ、テスターは実際に防御を突破しようとする
- この種のテストはデスクトップ・ベースで行われるため、**リアルタイムで実施され**、通常、主なアセスメントは技術的なアンケートに依存する
- というのも、この種のテストは事業者が個別に実施するものであり、サイバー演習のように、プレーヤーが情報を共有し、他の事業者と協力するような、事業者間の作戦上の協力関係をテストするものではないからである。

サイバー・ストレステストの利点

サイバー・ストレステストには、他のサイバーセキュリティのアセスメント手法と比較していくつかの利点がある。

- **軽量である**。作戦上の協力を焦点を当てたサイバー演習では、全員がオンラインでシナリオを実行し、サイバー演習の他のプレーヤーと同じ瞬間に関与する準備が整っていることを確認するために、膨大な量の準備と調整が必要である。しかし、サイバー・ストレステストは個別かつ独立したものであるため、事業者は独自のタイミングと計画を用いて、より柔軟にストレステストを実施することができる。紙ベースであるため、サイバー・ストレステストは、例えばシナリオや攻撃をライブシミュレートするための複雑なツールを必要としない。
- **対象を絞る**。監査は、サイバーセキュリティの脅威や対策を幅広くカバーすることが多い。このため、監査のプロセスは、監査人と被監査人の両方にとって、リソースを大量に消費することになる。サイバー・ストレステストでは、いくつかの非常に具体的なリスクシナリオに焦点を当てるため、よりの絞ることができ、しかも容易である。
- **客観的である**。企業のリスクマネジメントやセキュリティ対策を監査することは、例えば、企業のリスクリストや講じた対策、講じなかった対策など、どちらかといえば主観的な作業になりかねない。サイバー・ストレステストでは、レジリエンスマトリクスを使用するため、全体的な評価プロセスがより客観的になる。
- **協力的である**。重要セクターの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は、国家当局と重要インフラの所有者・運営者とのパートナーシップが必要である。この文脈では、監査に基づくコンプライアンスベースの監督アプローチは、セキュリティ対策の広範なコンプライアンスチェックリストによって希少なサイバーセキュリティリソースを消費し、逆効果になる可能性がある。サイバー・ストレステストは、システムリスクの観点から、特定のリスクシナリオについて、セクターとの対話を開始することを可能にする。

ストレステストの目的

国のサイバーセキュリティ監督機関や機関は、サイバー・ストレステストを次のような目的で利用することができる：

- 重大なインシデントに直面した場合、たとえ不利な状況であっても、個々の事業者の準備態勢をアセスメント
- 重要セクター全体の準備態勢をアセスメントし、システムリスクの把握に役立てる
- 特定のリスクやリスクシナリオを指摘する国家リスクアセスメントに対応する
- 同じようなリスクシナリオを用いて、利害関係者間の国境を越えた分野横断的な業務協力をテストするサイバー演習に備える
- システム的な問題を特定し、監督上の優先順位を設定する際に認可を支援する。

サイバー・ストレステストを受ける事業者にとっても、ストレステストに参加することは、重大なサイバーセキュリティインシデントに直面した場合の備えとレジリエンスを理解するのに役立つというメリットがある。

2.2 監督ツール一部としてのサイバー・ストレステスト

NIS2 の下で、各国当局や作成機関は重要セクターの事業者のサイバーセキュリティとレジリエンスを監督する必要がある。このために国家監督機関が取り得るアプローチには様々なものがあり、サイバー・ストレステストはそのツールキットの一部となり得る。

監査を超えた監督

セクターに対するサイバーセキュリティの詳細な要件が何であるかを認可した後、国家当局はこれらの要件が満たされていることを監督し、保証する必要がある。監督機関は、そのセクターの事業体を監査したり、サードパーティに監査を依頼したりすることが多い。監査は事前にも事後にも、つまりインシデントが発生する前にも後にも行うことができる。監査は、紙ベース、オンライン、またはオンサイトで行われる。歴史的に、サイバーセキュリティ領域における監査は、主に ISO27001 や SOCS への準拠など、コンプライアンス上の理由から実施されており、通常、かなり広範で、コストがかかり、時間のかかる評価プロセスである。しかし、認可事業者は、脅威情報の提供、ガイダンスの提供、サイバーセキュリティの意識を高めたり共通の問題を議論したりするためのワークショップの開催、共通のサイバーセキュリティ問題のための官民パートナーシップの開始、サイバー演習の開催など、他の多くの方法でその部門と関わることができることを強調しておくことが重要である。また、サイバー・ストレステストは、認可がこのセクターと関わるために利用することもでき、特定の脅威やリスクシナリオについて対話を始めるのに適している。

サイバー・ストレステストを他のサイバーセキュリティ評価手法と混合する。

サイバー・ストレステスト以外にも、サイバーセキュリティ領域には、オンサイト監査、侵入テスト、倫理的ハッキング、レッドチーム、脆弱性スキャンなど、当局が利用できる幅広いサイバーセキュリティ評価・テスト手法がある。監督機関や作成機関は、その環境やニーズに応じて、適切な方法を見つける必要がある。海底ケーブルはペースメーカーとは全く異なるため、電気通信分野と医療分野では全く異なるアプローチが必要になるかもしれない。例えば、監査の前に脆弱性スキャンを行ったり、サイバー・ストレステストの後にサイバー演習を行ったりすることができる。

義務的／厳格なサイバー・ストレステストと任意的／探索的なサイバー・ストレステストの比較

セクターのサイバーセキュリティの成熟度によって、またニーズによって、当局はサイバーストレステストに対してより義務的／厳格なアプローチを採用するか、より自発的／探索的なアプローチを採用するかを決定することができる。当局がストレステストの対象となる事業体に対する輸入事業者の意図を明確にすることは重要である。当局は、ストレステストの結果によって何が起こるのか、ギャップがフォローアップされるのかなどを前もって明確にすべきである。

監督機関は、ストレステストを実施する際に、より厳格な／強制的なアプローチをとることと、より探索的な／自発的なアプローチをとることの長所と短所を比較検討する必要がある。いくつかの長所と短所を挙げる：

より厳格な／強制的なサイバー・ストレステスト - より正式な、多くの場合強制的な、このセクターに対する厳格な詳細法的要件に裏打ちされたものである：

- 事前監督のための新しい方法を提供する。
- 同じリスクシナリオにさらされる複数の事業体の満期を捉える
- 事業体の能力とセクターの特殊性についての洞察が深まる

短所

- 事業体は、ストレステストをコンプライアンス（法令遵守）のための訓練と見なす可能性がある。
- 事業体は、制裁を回避するために、十分なストレステストを実施することを控えるかもしれない。

より探索的／自発的なサイバー・ストレステスト - 監督機関と事業体との間の協調的アプローチで、洞察の獲得に重点を置き、対話と協力の開始を目指す Pros：

- 自主的で監督的でないアプローチは、より多くの協力と、よりオープンな議論をもたらす。
- 納得感が高まり、能力と弱点について開示する意欲が高まった
- 監督機関やセクターの知識がまだ不足している斬新なテーマにも、より柔軟に対応できる。
- よりオープンなアプローチにより、予期せぬ依存関係や影響力を特定し、議論することができる：
- 自主的なアプローチは、事業体の関与や参加の欠如につながる可能性がある。
- ストレステストで収集されたデータは、正確性に欠けるか、不完全である可能性がある。

- 事業体は、ストレステストの結果の勧告に対処することに消極的である可能性がある。

3. サイバー・ストレステストのためのステップバイステップ・ガイド

このセクションでは、サイバー・ストレステストを行うためのステップバイステップのガイドを提供する。以下の用語を使用する。

- **監督機関**：サイバー・ストレステストを実施する監督機関、例えばサイバーセキュリティ機関や部門別／国別のサイバーセキュリティ当局などである。
- **事業者**：サイバー・ストレステストを受ける事業者とは、ストレステストを受け、ストレステストの課題に対応する重要インフラ事業者を意味する。事業者とは、NIS2 の用語で、この分野の企業を指す。
- **利害関係者**：サイバー・ストレステストの結果に関心を持つ、あるいはストレステストの設計に関連する専門知識を持つ他の組織、例えば、セクターの業界団体、セクターの専門家、セクターの専門知識を持つがサイバーセキュリティのマンデートは限定的なセクターの当局など。ストレステストのプロセスを監督するために、監督機関と利害関係者でストレステストのワーキンググループまたは委員会を形成することはグッドプラクティスである。

下図は、サイバー・ストレステストを実施するための 5 つのステップをまとめたものである。

5 steps in organising a cyber resilience stress test



以下では、そのステップをより詳細に説明し、トレードオフといくつかのグッドプラクティスについて論じる。

1	サイバー・ストレステストの範囲と目的	サイバー・ストレステストの範囲と目的は、セクター、対象事業体およびインフラストラクチャー、高レベルのリスクシナリオを選択することによって定義される。このステップでは、サイバー・ストレステストの設計をサポートし支援する利害関係者が特定される。
----------	---------------------------	--

1a. 対象分野、事業体、インフラを定義する。

まず、事業分野、事業体の種類、対象となる ICT インフラを決定する必要がある。テストが実行可能であることを確実にするためには、範囲を明確に定義することが極めて重要である。セクター全体のストレステストは実行不可能である可能性があり、事業体のサブセットを選択する必要がある。例えば、電気通信セクターでは、大手モバイルネットワーク事業者のみにストレステストを実施する。

重要なことは、対象範囲が広がれば、事業体はより多様になり、すべての事業体に対して効果のあるストレステストを設計することが後で難しくなるということである。より広いスコープの利点は、より多くのシステム・リスクをアセスメントできることであるが、スコープに含まれる事業体ごとにいくつかのバージョンのストレステストを設計することが必要になる可能性がある。例えば、スコープが電気通信事業者と電力サブセクターに設定されている場合、相互依存関係も評価することができる（電気通信事業者はグリッドに依存し、グリッドはネットワークに依存する）が、この場合、電気通信事業者と電力生産者の両方に適切

であるように、2つのバージョンのストレステストが確実に必要になる。ストレステストの範囲が電気通信事業者のみに限定される場合、電気通信事業者の電力網への依存度がアセスメントされ、おそらく単一障害点が明らかになる可能性があるが、電力部門自身の電気通信ネットワークへの依存度は評価されない。

ストレステスト設計の最も重要な側面の1つは、どの事業体をいくつテストするかを決めることである。広さと深さはトレードオフの関係にある。より多くの事業体が関与する場合、ストレステストはそのセクターのより広範な全体像を生み出すことになるが、多様性は具体的な内容に踏み込むことをより困難にする。結果の収集は統計に集中する可能性が高く、具体的なギャップや問題を特定することはより困難になる。より多くの事業体が参加することの利点は、ストレステストによって、そうでなければ見られないような単一の障害点が示される可能性があることである。例えば、多数の企業がストレステストを行う場合、あまりにも多くの企業が同じサプライヤーに依存していることが明らかになる可能性がある。事業体の数が少ないと、このような依存関係は隠れたままになる可能性がある。

1b. テストの目的とハイレベルのリスクシナリオを定義する。

次に、ストレステストの目的を決定し、策定し、リスクシナリオを選択する必要がある。サイバー・ストレステストは、予防的サイバーセキュリティ対策だけでなく、インシデント対応や復旧対策も対象とすることができる。ニーズに応じて、ストレステストの焦点は、予防と準備に重点が置かれることもあれば、対応と復旧に重点が置かれることもある。例えば、ストレステストの目的は、ランサムウェアグループによる標的型サイバー攻撃に対する大病院の準備とレジリエンス、およびケアを提供し続ける能力を評価することである。

サイバー・ストレステストは、ランサムウェアの準備、大規模スパイ攻撃、ネットワークインフラの物理的破壊工作、冗長性とフェイルオーバーなどに焦点を当てることができる。一般的に、ストレステストのリスクシナリオを選択する際には、複数のサイバー脅威や脅威の種類に対応するのが良い。しかし、リスクシナリオを複雑にしすぎると、例えば異なる脅威を増やしすぎると、ストレステストが広範になりすぎる可能性がある。焦点を失い、サイバー・ストレステストが一般的な情報セキュリティマネジメントシステムの監査アンケートになってしまうリスクがある。

1c. 関連する利害関係者の関与

第三に、セクター、対象とするICTインフラストラクチャー、目的、リスクシナリオが決まったら、例えば貴重な専門分野の知識を持つなど、ストレステストをサポートできる他の利害関係者や、ストレステストから利益を得ることができる利害関係者を関与させることが重要である。

利害関係者は、非サイバー当局、分野別機関、分野別の専門家または作業部会、国家コンピュータセキュリティ・インシデント対応（CSIRT）チーム、法執行機関、市民有事機関などである。セクターの選択にもリスクシナリオの選択にも依存する。例えば、エネルギーセクター、特に電力生産を支えるICTインフラストラクチャーをストレステストする場合、関連する利害関係者は、グリッドオペレータ（送電システムオペレータ、配電システムオペレータ）である可能性がある。例えば、ハイレベルのリスクシナリオに組織犯罪グループによるサイバー攻撃が含まれる場合、法執行機関を関与させ、過去のサイバー犯罪事例に関するインプットを提供することが有用である。

サイバー・ストレステストの残りの部分、特にテストの設計、シナリオの精緻化、適切なメトリクスの定義、結論の段階でのフォローアップにも利害関係者を参加させることは良いアイデアである。利害関係者グループは、運営委員会または監督委員会として機能することもできる。

利害関係者のためのグッドプラクティス：「サイバーセキュリティおよびセクター別の事項に関する、さまざまな分野の専門家で構成される監視委員会を設置する。」

2

サイバー・ストレステストの設計

監督機関がストレステストを設計し、手法を選択し、シナリオを精緻化し、ストレステストの目的に連動したレジリエンス指標を開発する。

2a. テストの方法論

ストレステストの方法を選択することは、先に特定した目的とスコープとの整合性を確保する 鍵となる。すでに述べたように、バリエーションはあるものの、ストレステストはほとんどが "デスクトップベース"であり、1 つ以上のリスク () シナリオを中心としたテクニカル なアンケートに依存し、テストされる組織によって独自に記入される。以下に、このようなストレステストの質問票の簡略化した例を示す。ストレステストは、現場訪問や予定された構造化されたインタビューによっても実施される。

ストレステスト・アンケート - EU の医療セクターの例

ストレステレベル 1

マルウェアを含むフィッシング・メールがバックオフィスのスタッフを標的にしたらどうなるだろうか？

- どのような対策を取っているか？(意識向上トレーニング、エンドポイント検知、メールフィッシングフィルターなどから選ぶ)

こうした予防措置が失敗したり、回避されたりして、マルウェアがダウンロードされ、インストールされてしまったらどうするか？

- 患者データと医療記録のリスクを評価する (非常に低い - 非常に高い) 。

ストレステレベル 2

攻撃者が他の PC を感染させようとしたらどうなるか？

- 横移動を防ぐために、どのような対策があるのか？

これらの対策が失敗したり、回避された場合はどうするか？

- 患者のケアと安全に対するリスクを評価する (1~10) 。
- 検知の速度はどれくらいで、反応はいつ始まるのか？
- どれくらいのスピードで復旧・復元できるのか？

ストレステレベル 3

もし攻撃者が医療機器や運用技術 (OT) 機器に横移動しようとしたらどうなるだろうか？

- どのような防止策を講じているか (エアギャップ、ゼロトラスト、ファイアウォールなどから選択) 。

何をすべきか？

- 患者のケアと安全に対するリスクを評価する (非常に低い) 。
- クリティカルケア業務 (長期治療室、集中治療室など) のリスクを評価する。
- ...

2b.シナリオの詳細化

このステップでは、特定のインフラストラクチャー、ビジネスプロセス、情報技術 (IT) アーキテクチャー、ICT システムを対象として選択し、ハイレベルのリスクシナリオを精緻化する必要がある。最も関連性の高いインフラストラクチャーと主なりスクにストレステストを集中させることが重要であり、アセスメントを確実かつ効果的に行うことができる。

シナリオ作成におけるアセスメントは、増大する圧力下でのレジリエンスを現実的に評価するための鍵である。深刻度を徐々にエスカレートさせるには、1 つのシナリオの影響を拡大する方法と、バリエーションごとに複数のシナリオを重ねる方法がある (最初の回答が得られた後に追加情報をインジェクトする方法、あるいはデータ収集テンプレートに「what if」の質問を使用する方法) 。

必要とされる詳細度は、対象事業体の数や種類、また、テストの監督手法が厳格なものか、探索的なものかによって異なる。テストが特定の障害点に焦点を当てるのであれば、十分な詳細が必要である。より探索的なアプローチでは、リスクシナリオはより一般的なものとし、より広範な潜在的影響と緩和戦略について事業体にフィードバックを求めることができる。

優れたストレステストのシナリオは、異なる影響や異なるタイプの脅威に対応する複数のサブシナリオを持つべきであり、これによって異なる側面のストレステストが可能になる。オールハザードの NIS2 指令の場合、特に重要インフラ事業体のレジリエンスをストレステストする場合、サイバー脅威とサイバーフィジカル脅威をミックスしたものに対してストレステストを行うことは良いアイデアである。しかし、あまりにも多くの脅威がスコープに含まれ、シナリオが非常に複雑で、多くのサブシナリオがある場合、ストレステスト自体が長時間になり、時間がかかることになる。

2c. レジリエンスの指標。

ストレス目標に基づき、準備、レジリエンス、およびシナリオの影響のレベルを測定する適切なレジリエンス指標を選択する必要がある。たとえば、ベルギーのストレステストのケーススタディ（附属書 B を参照）では、事業体は 3 つの主要分野（準備、インシデント対応、復旧）のレジリエンス指標を使って評価された。

レジリエンスの指標は、定性的または定量的であることがあり、その範囲内で枠を設定し、ストレステストの目的とリンクさせる必要がある。例えば、レジリエンスの指標は、インシデントを検知するまでの時間、回復するまでの時間、あるいは予防対策の洗練度である。

2d. ストレステストの計画とスケジュール

サイバー・ストレステストの方法論が定義された後、より詳細な計画とタイムラインを設定し、ストレステストを受ける事業体の期限を決定し、ストレステスト結果の収集と分析を計画し、フォローアップフェーズを計画することができる。ストレステストを実施する事業体には、いつまでにストレステストを完了する必要があるのか、フォローアップの内容、およびどのように関与するのかを前もって説明しておくことが良いプラクティスである。

シナリオ詳細化のためのグッドプラクティス： 重要なビジネスプロセス及び／又は重要なサイバーシステム及び物理システムのカテゴリーを識別する。

リスクシナリオのグッドプラクティス： セクター別の脅威のランドスケープ、セクター別の依存関係、セクター別のサプライチェーンリスクに基づくセクター別の要素を含める。

メトリクスのグッドプラクティスアセスメント規準は、テスト対象事業体のパフォーマンスとレジリエンスを評価することに重点を置くべきである。

3

サイバー・ストレステストの実施

監督機関は、サイバー・ストレステストを実施する事業体に関与し、テストの目的、全体的なスケジュールと計画、結果の分析とギャップのフォローアップ方法についてガイダンスと説明を提供する。

3a. 事業体との関与。

このステップでは、認可はサイバー・ストレステストを実施する事業体と関わり、全体的な目的とタイムライン、ガイダンスと説明を提供する。いくつかの側面が重要である。

- ストレステストの目的と主なリスクシナリオを説明する。
- どの専門家が事業体側でテストを実施することになっているかを説明する。
- 質問や懸念事項に対する窓口をプロバイダとして提供し、事業体側の窓口を一本化するよう求める。

- ・ 秘密保持と使用法を明確にすることは極めて重要である。検査結果は多くの場合機微なものであり、細心の注意を払って取り扱われるべきである。回答がどのように処理されるか、誰がアクセスできるか、などについて説明することが重要である。事業体と認可の間の信頼関係の構築は、今度のサイバー・ストレステスト自体のためだけでなく、将来の相互作用のためにも重要である。
- ・ 対応期限を含む詳細な対応計画とスケジュールを提供することが重要であり、予期される場合には、特定されたギャップと発見事項について話し合うための合同ワークショップを開催する。
- ・ 事業体内の窓口を一本化し、専用のコミュニケーション・チャンネルを確立する。

3b. ストレステスト中の事業体に対するサポートとガイダンス。

円滑な実施のためのサポートとガイダンスを提供し、回答の質と一貫性を改善することが重要である。監督機関は、ストレステストを説明し、フィードバックに対応するために、事業体とのキックオフ・ワークショップを開催することを検討すべきである。短い"よくある質問"を作成することは、問題や質問が取り上げられ、その回答がストレステストを受けたすべての事業体が利用できるようにするための良い戦略である。ストレステストの実施中に、ヘルプデスクやサポートコンタクト（直接のEメールや電話番号）を提供することも検討されるべきである。

4 ギャップ分析

データ分析は、個々の事業体および／またはセクター全体のギャップ、弱点および改善点を特定するために使用される。ストレステストの結果は、事前に定義されたレジリエンス指標に照らして定性的・定量的に評価される。

4a. ストレステストの結果を評価する

全体的なストレステストの結果の分析により、関係事業体の一般的なベースラインについての良いアイデアが得られる。データ分析ツールを利用して、事前に定義された測定基準に照らして評価するのがよい。このステップでは、機密性と匿名化が重要である。単一の事業体のテスト結果は非常に機密性が高く、他の事業体や一般聴衆に開示すべきではない。匿名化され、集計された結果は、より広範な聴衆と共有することは興味深いかもしれないが、脅威アクターが将来のサイバー攻撃にこの情報を使用することを避けるため、注意が必要である。

4b. セクター横断的または国境横断的な性質を含むギャップを識別する。

ギャップや問題は、さまざまなレベルで特定することができる

- ・ 個々の事業体における格差である
- ・ 複数の事業体に共通する問題やギャップがある
- ・ セクター内の特定の事業体に依存している
- ・ セクターを越えた、あるいは国境を越えた依存関係である
- ・ サプライチェーンの依存関係
- ・ 共有インフラや共有サービスプロバイダを利用する。

ギャップや依存関係を特定することは重要だが、事業体やセクター全体がどの分野で成熟し、十分な準備が整っているかを強調することも有効だろう。このようなアプローチは、当局と事業体との間に信頼と協力関係を築くの役に立つ。

予備的な調査結果は、まず事業体と監督機関との間で、非公開の場で議論されることが重要である。場合によっては、このような議論を拡大したり、利害関係者や専門家の双方に結論のドラフトを提示したりすることで、調査結果の妥当性を確認し、発行される勧告に対する賛同をさらに得ることができる。サイバーセキュリティの問題は、解決に時間と予算を要することが多い。相互理解、信頼関係、オープンさを醸成することで、フォローアップのプロセスが容易になる。

5

結論

最終段階では、監督機関がテストの結果を報告する。必要であれば、個々の事業体またはセクター全体に対する勧告を行う。監督機関は、このような勧告が実施されることを監督し、教訓を引き出す。

5a. 提言

サイバー・ストレステストの主な目標は、何がギャップや問題であるかを理解し、それらに対処するための的を絞った提言でフォローアップすることである。これらの提言は、早急な改善と長期的な改善に焦点を当てるべきである。サイバー・ストレステストが実際の改善につながるようにするためには、タイムラインと提言への対応計画を確立することが極めて重要である。

提言はさまざまなレベルで行うことができる。

- **個々の事業体に対する個別の提言。** 個々のギャップや発見事項については、すでに述べたように慎重に扱うべきであり、当該事業体とより詳細に話し合うべきである。
- **セクター全体への提言** セクター全体の問題は、利害関係者やストレステストに参加した事業体を含むより広範なフォーラムで議論されるべきである。これらの問題に対処するためには、集団行動、政府からの資金提供、または官民パートナーシップが必要となる場合がある。
- **分野横断的、国境横断的な提言** サイバー・ストレステストは、セクター横断的あるいは国境を越えた問題に関連する勧告につながる可能性もあり、そのような勧告は、例えば NIS 協力グループにおいて、他のセクターの当局あるいは他の国の国家当局と議論され、フォローアップされるべきである。

監督機関は、行われた勧告をフォローアップし、サイバー・ストレステスト後に勧告が対処されていることを定期的に確認すべきである。当局は、厳格な強制的アプローチよりもむしろ、事業体に対して、是正措置の状況を詳述した定期的な進捗報告書の提出を促すことに重点を置くべきである。サイバーレジリエンスの構築は、高度に成熟したセクターであっても、継続的な改善プロセスである。

5b. 教訓を学ぶ。

ストレステストの完了後、ストレステストのプロセス全体について学んだ教訓を文書化することが重要である。この最後のステップでは、ストレステストの組織と実施そのもの、テストの有効性と効率性、テスト方法の妥当性が分析される。ストレステストを実施した事業体だけでなく、他の利害関係者からもフィードバックを収集することは良いアイデアかもしれない。このフェーズでは、例えば、次のストレステストが同じような同じストレステストのシナリオに基づくべきかどうか、あるいは、異なるリスクセットに対してストレステストを行うべきかどうかなど、ストレステストの繰り返しについて議論することができる。

グッドプラクティス：「組織がストレステストの結果をリスクマネジメント手順に統合するためのガイダンスと枠組みを提供する。」

4. 国、地域、連合のサイバー・ストレステスト

本ハンドブックおよびステップバイステップ・ガイドでは、国家当局が実施する国家サイバーストレステストに焦点を当て、国内の重要なセクターの事業体に対してストレステストを実施する。もちろん、サイバー・ストレステストは、複数の当局が関与する地域レベル、あるいはすべての国家当局が関与する連合レベルで実施することもできる。このセクションでは、サイバー・ストレステストのさまざまな可能性について簡単に説明する。

国家サイバー・ストレステスト

サイバー・ストレステストを実施する最も簡単な方法は、国家レベルで実施することであろう。特定のセクターに対するサイバーセキュリティの権限を持つ国の監督機関が、そのセクターの主要な事業体に関与し、これらの事業体とともにサイバー・ストレステストを実施することができる。

すでに述べたように、テストする事業体の選定にはトレードオフがある。大規模な事業体グループのストレステストは、より多くの事業体を対象とすることを意味するが、ストレステストの質問票は、ほとんどが定量的な質問で、より一般的なものにならない可能性がある。少人数のグループであれば、ストレステストはより個別化されたものとなり、フォローアップはより詳細なものとなる。

簡単な例を3つ挙げる：

- **1 セクター内の5 事業体。**ある国の電気通信認可局が、大規模な危機や大規模なネットワーク停止時の緊急通信のレジリエンスに焦点を当て、大手モバイルネットワーク事業者のストレステストを実施することを決定した。ストレステストは義務であり、結果は個別に分析され、フォローアップされるだけである。
- **1 セクター50 事業体。**ある国の保健監督機関が、病院、診療所、研究所を含む保健セクターの広範な事業体に対してストレステストを実施することを決定した。ストレステストは必須であるが、一般的なものであり、セクターの全体的な成熟度に関する統計を収集することが主な目的である。
- **2 セクター20 事業体。**エネルギー部門と電気通信部門の国家監督機関が協力して、大手電気通信事業者10社と大手エネルギープロバイダー10社を対象にストレステストを実施し、一般的な準備態勢を理解するとともに、特定の部門間依存関係を理解する。ストレステストの主な目的は、両部門間の協力関係を強化し、部門横断的な問題を議論することである。

例えば、金融の分野や物理的／自然的脅威とレジリエンスの分野などである。このような他の監督機関は、共有すべき有益な知識を有している可能性がある。例えば、金融セクターでは、様々なレベルの金融／経済リスクシナリオでソルベンシーのアセスメントを行うためにストレステストが実施されてきました。

地域サイバー・ストレステスト

計画や調整は複雑になるが、特に経済が密接につながり、インフラを共有している場合には、域内の他国と協力することに価値があるかもしれない。

簡単な例を挙げよう：

- **2 カ国 2 監督機関、各国 5 事業体。**2カ国の電力網は密接にリンクしており、隣国の2つの監督機関は、地域ストレステストにおいて、いくつかの重要な事業体をストレステストすることを決定した。焦点は、当局レベルだけでなく事業体レベルでも、国境を越えた協力関係を強化することである。キックオフ・ワークショップは一方の国で開催され、結論となるワークショップはもう一方の国で開催される。

最近採択されたサイバー連帯法は、加盟国に対し、協調的な準備態勢テスト活動の実施を奨励していること、欧州委員会がかつた活動のための専用資金（デジタル・ヨーロッパ・プログラム）を確保しており、欧州サイバーセキュリティ・コンピテンス・センター（European Cybersecurity Competence Centre）が開始する資金募集で利用可能になる予定であることに留意することが重要である。準備態勢テストには、さまざまなアセスメント手法を含めることができ、また、国や地域のサイバー・ストレステストを含めることもできる。

労働組合のサイバー・ストレステスト

序論や附属書のケース・スタディなどですでに述べたように

ECB は最近、EU の金融部門を対象としたサイバー・ストレステストを実施した。同様に、欧州委員会は加盟国とともに、最近、物理的脅威と自然災害に焦点を当てたエネルギー部門のストレステストを実施した。

ストレステストに EU のアプローチを採用することは、非常に有益かつ効果的である。EU は、全プロセスの組織化、質問票の作成、データの収集、結果の分析などの詳細について各国当局に負担をかけることなく、各国レベルでストレステストを実施する際に各国当局を支援することができる。EU 連合のストレステストは、主要な脅威に関する EU 全体の対話を開始することができる。

簡単な例を挙げよう：

20～30 の監督機関、各国から 2～5 事業者が参加する。 EU 全域の液化天然ガス基地におけるランサムウェアへの備えを評価するため、複数の国家当局が EU レベルでサイバー・ストレステストを実施することに合意する。関係する各当局は、サイバー・ストレステストの対象となる最大規模の事業者 2～5 社を選定する。ストレステストの主な焦点は、EU 全体の問題を理解することである。ストレスの評価中、グッドプラクティスが事業者や当局によって共有される。ストレステストそのものとその結果は、共通の問題についての EU 全体の対話の引き金となり、特定の脅威についての認識を高め、当局や政策立案者に監督の優先順位や政策の優先順位について情報を提供する。

5. 結論

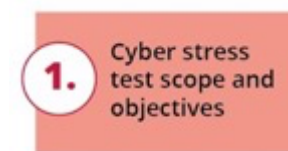
本ハンドブックでは、サイバー・ストレステストの概念を紹介し、説明し、ストレステストのステップバイステップ・ガイドを提供し、様々なケーススタディやグッドプラクティスを参照した。

ストレステストはサイバーセキュリティの領域では比較的新しい概念であるが、他の領域で使用されることが増えている。サイバー・ストレステストは、重要セクターのサイバーセキュリティとレジリエンスを監督する各国 NIS 当局の規制ツールキットにおける新たなツールとなり得る。金融・経済およびサイバー・ストレステストが実施された金融セクターのような成熟したセクターの経験から、サイバー・ストレステストは複雑な相互接続システムの監督に適しており、システミックリスクの評価に役立ち、レジリエンスを共に構築するのに役立つことが示されている。

サイバー・ストレステストは、重要セクターのレジリエンスを評価するための新しい軽量で的を絞ったメカニズムになりつつあり、サイバーセキュリティのギャップがどこにあるかを理解するのに役立つ。ENISA では、国家レベルまたは EU レベルのサイバー・ストレステストの実施において、国家レベルおよび EU レベルの国家当局や機関を支援することを楽しみにしている。

附属書 A : 医療セクターの例

このセクションでは、セクション 4 で詳述したステップ・バイ・ステップのガイドを使用して、国家認可が医療セクターでどのようにサイバー・ストレステストを実施できるかの実践例を示す。



この例では、ストレステストは医療セクターで実施される。

- 対象事業体：
 - 病院や大規模クリニックである
 - 国内および EU 内の保健当局、団体、機関である
- 重要インフラの範囲：
 - IT 資産 - ワークステーションやノートパソコン、ネットワークインフラ、電子カルテシステム（EHR）、病院管理システム、医療画像・画像保存・コミュニケーションシステム、遠隔医療・リモートアクセスプラットフォーム、クラウドベースの医療プラットフォームなど、
 - OT 資産 - 一般的には、接続された医療機器（8）、モノのインターネット機器（9）、建物のインフラとユーティリティ（暖房、換気、空調、主電源、バックアップシステム（10）など）、緊急システム、救急車、緊急コミュニケーションなどである。

この例では、ストレステストの目的は次のように定義される：

- インシデントを検知・防止するための防御手段を評価する
- 対応策と復旧策、特にケアの継続性を維持し、患者の安全への影響を最小限に抑える能力を評価する
- 医療分野のサイバーレジリエンスを強化するために、今後予定されている分野別の規制や資金調達の優先順位の指針となるよう、調査結果を活用する。

この例では、関係者は公表されている EU 保健分野の脅威状況報告書⁽¹¹⁾を考慮に入れている。それによると、この分野の脅威のトップは以下の通りである：

- ランサムウェアは病院の IT および OT 環境に影響を及ぼしている
- データ関連の脅威は、患者データに影響を及ぼす
- 病院の IT および OT 環境へのネットワーク侵入
- サプライチェーン攻撃（プロバイダ、機器サプライヤ、マネージドサービス・プロバイダ経由）。
- この例では、国営医療機関がランサムウェアに絞ってストレステストを実施することにした。
- また、国の保健当局は、ストレステストについて以下の利害関係者を特定している：
- 国家衛生局である

⁸例えば、輸液ポンプ、ペースメーカー、磁気共鳴画像装置などである。

⁹例えば、スマートセンサー、ウェアラブル、患者監視システムなどである。

¹⁰例えば、暖房、換気、空調ユニット、電源ユニットなどである。

¹¹ENISA 脅威情勢レポート - 健康分野 <https://enisa.europa.eu/publications/health-threat-landscape>.

- 国の CSIRT がある
- 国のサイバー犯罪対策部門である
- サイバーセキュリティのための官民パートナーシップで
- 国家保健 CSIRT である
- 医療機器サプライヤーと病院 ICT ソリューションプロバイダーである。

2. Cyber stress test design

この例では、リスクシナリオは次のように書くことができる：

病院へのランサムウェア攻撃により、IT ネットワークがロックされ、電子カルテが暗号化される。攻撃者はまた、患者の機密データ（保護された医療情報、財務情報）を流出させ、身代金を支払わない限り、それを公に漏らすと脅迫する。

エスカレーションの第一段階は、接続された医療機器の侵害である。ランサムウェアを足がかりに、攻撃者は複数のネットワーク接続された医療機器へのアクセスをロックダウンするが、まだそれらを管理することは可能である⁽¹²⁾

第二段階のエスカレーションは、病院の外部ネットワークと緊急対応に対する分散型サービス拒否攻撃であり、オンライン患者ポータル、スケジュール管理システム、遠隔医療サービスを混乱させる。緊急対応システム（救急車の調整、遠隔監視）に深刻な遅延が発生する

セクション 3 では、このような設定で使用可能なストレステストのアンケートの詳細な例を示した。以下の表では、考えられるレジリエンスの指標の例をいくつか示す。



対象資産	レジリエンス指標
<ul style="list-style-type: none"> - 病院 IT ネットワーク - セキュリティ監視とログシステム (SIEM、IDS / IPS) - ファイアウォール、ルーター、スイッチ - コネクテッド医療機器 	<ul style="list-style-type: none"> - ネットワーク・セキュリティ・ポリシーが適用されているシステムの割合 - 検知した脅威に対する平均応答時間 - 月にフラグが立てられたセキュリティ・イベントの数 - ネットワーク接続された医療機器の数
<ul style="list-style-type: none"> - 病院と医療スタッフ 	<ul style="list-style-type: none"> - フィッシングに関する研修を受けた従業員の割合 - 検知に成功したフィッシング・シミュレーションの割合 - フィッシングメールのクリック率
<ul style="list-style-type: none"> - ID およびアクセス管理システム - EHR システム - ワークステーションとノート 	<ul style="list-style-type: none"> - 多要素認証を使用しているアカウントの割合 - 月間不正アクセス試行回数 - 解雇された員のアクセス権を取り消すのに要した時間
<ul style="list-style-type: none"> - ワークステーションとノートパソコン 	<ul style="list-style-type: none"> - 最新のセキュリティ・パッチで更新されたシステムの割合

¹²例えば、輸液ポンプが使用不能になったり、誤った投与量に設定されたり、人工呼吸器や心臓モニターが停止したり、誤った数値を表示したり、磁気共鳴画像装置や放射線装置が作動不能になり、診断が遅れたりする。

対象資産	レジリエンス指標
<ul style="list-style-type: none"> - EHR と重要なアプリケーションをホストするサーバー - ストレージ・システム 	<ul style="list-style-type: none"> - 重要なセキュリティ・パッチの平均適用期間 - エンドポイントセキュリティ遵守
<ul style="list-style-type: none"> - セキュリティ監視とロギングシステム（セキュリティ情報とイベント管理、侵入検知システム/侵入防御システム） 	<ul style="list-style-type: none"> - セキュリティインシデントの平均検知時間（MTTD） - セキュリティインシデントへの平均対応時間（MTTR） - 緩和に成功したインシデントの割合
<ul style="list-style-type: none"> - バックアップと災害復旧システム - ストレージ・システム 	<ul style="list-style-type: none"> - 回復時間目標（RTO） - 回復時点目標（RPO） - テストシナリオにおいて、重要データの復元に成功した割合 - 病院はランサムウェア対応計画を確立しているか？ - 医療機器が故障した場合、医療処置のマニュアルはあるのか？ - 病院は災害復旧手順をどのくらいの頻度でテストしているのか？

3. Cyber stress test execution

この例では、監督機関は病院と事前に連携し、病院の最高情報セキュリティ責任者を集めたキックオフ・ワークショップを開催する。監督機関は「質問と回答」のウェブページも作成し、ワークショップ終了後、対象となるすべての事業体に正式な招待状を送付した。

試験中、監督機関は、リアルタイムのヘルプデスク/サポートラインという形で、また、新しい質問が寄せられると FAQ ページを更新するという形で、さらなるサポートとガイダンスを提供する。質問と回答のページには、以下のような質問が含まれている：

- テストの目的は何か？
- どのスタッフがテストに関わるべきか？
- 個人の成績は評価されるのか？
- 参加をやめることはできるか？

4. Gap analysis

この例では、ストレステストの後にギャップの特定と分析が行われる。より広範なセクターに対する潜在的なストレステスト結果の例をいくつか示す：

- 意識と防御：ほとんどの病院で意識は高いが、技術的対策は不足しており、しばしば不十分である。このような環境では、非技術的な対策や利用者のスキルに頼りすぎている。
- IT から OT へ：ランサムウェアはしばしばオフィスの IT 環境から始まり、そこから特にレガシー ICT のリスクが高い医療機器環境に容易に拡散する。

- 最も弱いリンクさまざまな大病院のスタッフやシステムは密接に相互接続しており、ある病院でのランサムウェア攻撃は他の病院にも容易に広がる可能性がある。多くの場合、システムは共有されており、異なる病院のスタッフが同様のシステムを使用している。

5. Conclusion

この例では、ストレステストの結果、病院に対する具体的な勧告が出される。勧告はフォローアップ行動計画に盛り込まれる。ストレステストの結果への対応として、政府はまた、特に a) ランサムウェアに対する緩和策の実施、b) レガシーICT システムの段階的廃止を行う病院を対象とした国家的資金提供プログラムを開始する。

この例では、利害関係者はストレステストのプロセス全体に関する教訓も引き出している。その教訓とは、ストレステストが有用で成功したこと、事業者が短期的に類似のシナリオまたは異なるシナリオでストレステストを実施することを望んでいることである。

附属書 B : ケーススタディ-金融とエネルギー

本セクションでは、過去のストレステストのケーススタディを 2 つ紹介する：

銀行セクターのサイバー脅威に焦点を当てた連合ストレステスト - エネルギーセクターのハイブリッド脅威に焦点を当てた連合ストレステスト
エネルギー部門のハイブリッド脅威に焦点を当てた連合ストレステスト

金融セクター - 欧州中央銀行 (ECB) の 2024 年サイバーレジリエンス・ストレス・テスト

2024 年、ECB が直接監督する銀行 109 行 (合計 109 行) は、すべての予防措置が失敗し、銀行の主要な基幹システムが損なわれたシナリオに対処する能力についてテストされた。ストレステストを実施した銀行群は、ユーロ圏システム全体の金融安定性を把握し、他の監督活動との十分な連携を確保するため、規模、ビジネスモデル、地理的位置が異なっていた。すなわち、実際の IT 復旧テストを実施し、それが成功した証拠を提出することである。さらに、監督当局による実地監査も行われた。このテストでは、特定された主なギャップや弱点が記載され、その緩和のための措置が提案された報告書が、テストされた事業者ごとに提出された。

参加した全銀行は、⁽¹³⁾に関するフィードバックを求められた。

1. シナリオの影響

- 主要な経済機能に影響を与える、
- 間接的な損失も含めた、オペレーショナル・ロスの見積もり：

2. 社内の危機管理手順や事業継続計画を含む、危機対応計画を活性化する、

- 顧客、サービスプロバイダー、法執行機関など、すべての外部利害関係者とコミュニケーションをとる、
- どのようなサービスがどのように影響を受けるかを特定するための分析を行う、
- IT システムの完全復旧に必要な時間中、銀行の業務を支援する回避策を含む緩和策を実施する

3. 銀行がシナリオから立ち直る能力があったことを示す：

- バックアップされたデータの復旧や、インシデントへの対応について重要なサードパーティーのサービスプロバイダーとの連携など、復旧計画を活性化させる、
- 被災地が復旧し、稼働できるようにした、
- 例えば、対応計画や復旧計画を見直すなどして、学んだ教訓を実行に移す。

エネルギー部門 - 2024 年ハイブリッド脅威ストレステスト

このケーススタディでは、ベルギーの SPF Economie - DG Energie ⁽¹⁴⁾ が実施した、エネルギー部門の重要インフラに関するストレステストについて詳しく見ていく。このストレステストの目的は、事業者が重大な障害にどの程度対応できるかを評価し、事業を迅速に復旧し、国境を越えて を効果的に調整する能力を測定することであった。ストレステストの目的は、サイバー脅威と物理的脅威の両方からの防御をストレステストすることであった：

- 物理的保護の妥当性
- セキュリティ管理の妥当性
- 攻撃を緩和し、抵抗する能力を持つ

¹³<https://www.bankingsupervision.europa.eu/press/pr/date/2024/html/ssm.pr240726~06d5776a02.en.html>。より抽出

¹⁴SPF 経済-エネルギー総局-市場・インフラ批評の厳正な監視。

- 攻撃から回復する能力（事業継続性） - 必要不可欠なサービスを提供し続ける能力
- 当局とのコミュニケーション能力。

ベルギーのストレステストの実施は、欧州委員会が提案した方法論に従ったもので、ベルギーのエネルギー・ネットワークの特定の特性に適合させ、3つのレジリエンス分野（**準備、インシデント 対応、復旧**）に焦点を当てた。主なステップには以下の要素が含まれる。

脅威とシナリオ

ストレステストの対象となったサイバー脅威およびハイブリッド脅威は以下の通りで

- 送電線の妨害行為、
- SCADA システムのような重要インフラに対するサイバー攻撃、
- 物理的な内部脅威
- 社会・政治不安

ストレステストでは、エスカレーションレベルの異なる3つのシナリオ（完全サイバー、完全物理、ハイブリッド）が用いられた。

- シナリオ A：つまり、脅威レベルは低く、複雑ではなく、小型の銃器による攻撃など、ほとんどが物理的なものである。
- シナリオ B：脅威レベルが高まり、サイバー脅威や物理的脅威がさらに強まり、破壊工作が行われ、スペアパーツの不足が重なり、社会不安も発生する。
- シナリオ C：非常に高い脅威レベル、地政学的不安定、組織的な物理的・サイバー攻撃、ネットワークやコミュニケーションの大規模な混乱、エネルギー供給不足、広範な社会不安。

ストレステストの方法、および主なデータ収集方法は、オペレータに送付された構造化された自由形式のストレステスト質問票であった。質問は、準備、インシデント管理、復旧の3つの主要分野/フェーズに均等に分けられた。アンケートは事業者のタイプに合わせて調整され、たとえば電力会社とガス会社では異なる質問を行ったが、レジリエンスの指標は同じに保たれた。回答はレジリエンス指標を用いて定量的に評価され、事業者の平均レジリエンススコアが算出された。

ストレステストから得られた主な発見と教訓

ストレステストの結果に基づき、ベルギー当局はいくつかの重要な発見を行った：

- 極端なリスクシナリオを緩和するためには、官民の緊密な協力が必要である。
- 連鎖的な失敗を効果的に緩和するためには、国境やセクターを越えた依存関係についてもっとよく議論し、分析する必要がある。
- ドローンのような新たな脅威は、重要インフラ事業者に新たな具体的緩和策を求める。
- 極端なシナリオにおける影響を緩和するためには、再供給と修理が鍵となる。サプライチェーンの問題は、インシデント対応と事業継続計画で取り組む必要がある。

ベルギーのストレス・テストは、ストレス・テストそのものについても、いくつかのグッド・プラクティスと教訓をもたらした

- サイバー脅威と物理的脅威の両方を取り入れることで、より現実的で包括的なテスト環境を作り出すことができる。
- すべての事業者がストレステストの対象となるインフラを持っていたわけではないため、統計的な比較は必ずしも可能ではなかった。
- より一般的で標準的なレジリエンス指標を維持しつつ、特定のインフラ向けにアンケートをカスタマイズすることで、適切で実行可能な洞察が得られるようになった。
- 定期的な協議と共同でのフィードバックにより、回答の質が向上し、透明性が促された。
- 事業者は詳細なセキュリティ計画の共有に消極的な場合があり、データ収集の深度に影響を与えていた。

参考文献

1. AXIOMA. ストレストスト・ベストプラクティス : <https://www.hvst.com/posts/stresstesting-best-practices-X7QTObdI>
2. イングランド銀行、2024 年英国銀行システムのストレステストに対するイングランド銀行のアプローチ。
<https://www.bankofengland.co.uk/stress-testing/2024/boes-approach-to-stress-testing-the-uk-banking-system>
3. バーゼル銀行監督委員会、2018 年。サイバーレジリエンス：実践の範囲。
https://www.bis.org/bcbs/qis/biiiimplmoninstr_oct18.pdf
4. 連邦準備制度理事会、2021 年。ドッド・フランク法ストレステスト 2021 : Supervisory Stress Test Methodology. <https://www.federalreserve.gov/publications/files/2021-april-supervisory-stress-testmethodology.pdf>
5. 中央計画局、2020 年オランダ中小企業のストレステスト。
<https://www.cpb.nl/sites/default/files/omnidownload/CPB-Background-Document-June2020-A-stress-test-of-Dutch-SMEs.pdf>
6. サイバーセキュリティ・インフラセキュリティ庁（CISA）, 2024. インフラレジリエンス計画枠組み（IRPF）
<https://www.cisa.gov/resourcestools/resources/infrastructure-resilience-planning-framework-irpf> から入手できる。
7. デンマーク金融監督庁、2024 年サイバー・ストレステストは金融セクターのオペレーショナル・レジリエンスを強化する。
<https://www.dfsa.dk/news/2024/nov/cyber-stress-testing>
8. 国防総省、2018 年。サイバーセキュリティ試験評価ガイドブック。
<https://www.dau.edu/sites/default/files/Migrated/CopDocuments/Cybersecurity-Test-and-Evaluation-Guidebook-Version2-change-1.pdf>
9. ESMA - 欧州証券市場庁、2017 年。Methodological Framework - 2017 EU-Wide CCP Stress Test Exercise. <https://www.esma.europa.eu/document/methodological-framework-2017-ccp-stress-testexercise>
10. Esposito, S., Stojadinovic, B., Babic, A., Dolsek, M., Iqbal, S., Selva, J., Broccardo, M., Mignan, A., Giardini, D., 2018. A Risk-Based Multi-Level Methodology to Stress Test Critical Infrastructure Systems. <https://www.earth-prints.org/server/api/core/bitstreams/b5ca3c77-578d-4a2d-a70f-030765db93fb/content>
11. 欧州銀行監督機構、2020 年。2023 EU 全体のストレステスト。 <https://www.eba.europa.eu/risk-and-data-analysis/risk-analysis/eu-wide-stress-testing>
12. 欧州中央銀行（ECB）、2024 年。「ECB to Stress Tests Banks' Ability to Recover from Cyberattack」 - プレスリリース。 https://www.bankingsupervision.europa.eu/press/pr/date/2024/html/ssm.pr240103~a26e1930_b0.ja にて入手可能
13. 欧州中央銀行（ECB）、2023 年。2023 年ユーロ圏銀行のストレステスト-最終結果。
https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.Report_2023_Stress_Test~96bb5a3af8.en にて入手可能。
14. 欧州中央銀行（ECB）、2023 年。Supervisory Review and Evaluation Process (SREP) available at: https://www.bankingsupervision.europa.eu/banking/srep/2023/html/ssm.srep202302_supervisorymethodology2023.ja.

15. 欧州中央銀行（ECB）、2021年。コロナウイルス（COVID-19）パンデミックにおけるユーロ圏銀行システムのマクロプルデンシ・ストレステスト。https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4112397。
16. 欧州中央銀行（ECB）、2021年。ECB エコノミーワイド気候ストレステスト。
<https://www.ecb.europa.eu/pub/pdf/other/castmanual201408en.pdf>
17. 欧州中央銀行、2018年 TIBER-EU 枠組み。
https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf
18. 欧州中央銀行（ECB）、2015年。包括的アセスメントストレステストマニュアル。
<https://www.ecb.europa.eu/pub/pdf/other/castmanual201408en.pdf>
19. 欧州委員会共同研究センター（JRC）、2016。Harmonized approach to stress tests for critical infrastructural 重要インフラに対するストレステストのための調和されたアプローチ Available at:
https://publications.jrc.ec.europa.eu/repository/bitstream/JRC104663/jrc104663_online_05_01_ipo。
20. 欧州委員会、2016年自然災害に対する重要インフラのストレステストの調和されたアプローチ
<https://op.europa.eu/en/publicationdetail/-/publication/aa009c90-d6ff-11e6-ad7c-01aa75ed71a1/language-en>
21. 欧州委員会、2014年重要インフラのレジリエンス改善のためのストレステストの開発：A Feasibility Analysis。<https://ec.europa.eu/jrc/en/publication/developing-stress-tests-improve-resilience-criticalinfrastructures-feasibility-analysis>。
22. 欧州保険・職業年金機構、2019年。2019年職業年金ストレステスト。
https://www.eiopa.europa.eu/browse/financialstability/occupational-pensions-stress-test/occupational-pensions-stress-test-2019_en
23. 欧州原子力安全規制機関グループ（ENSREG）、2011年。EU「ストレステスト」仕様書。
https://www.ensreg.eu/sites/default/files/EU_%20Stress%20Test%20Peer%20Review%20Final%20Report_0。で入手可能
24. 欧州システミック・リスク委員会、2025年。金融セクターにおけるサイバーレジリエンスのシナリオテストに関するハンドブック。
25. 欧州連合（EU）、2019年。高度道路交通システムのセキュリティに関する規則（C-ITS）。https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=PI_COM%3AC%282019%20入手可能
26. 欧州連合（EU）、2022年デジタルサービス法（DSA）。<https://eurlex.europa.eu/legal-content/EN/TXT/?uri=CELEX>にて入手可能
27. 欧州連合（EU）、2019年サイバーセキュリティ法（CSA）。<https://eurlex.europa.eu/EN/legal-content/summary/the-eu-cybersecurity-act.html>
28. 金融安定理事会、2020年。Cyber Incident Response and Recovery Toolkit。
<https://www.fsb.org/2020/10/cyber-incident-response-and-recovery-toolkit/>
29. 国際通貨基金（IMF）、2023年。マクロ・プルデンシヤル・ストレス・テスト・モデル：A Survey。
<https://www.imf.org/en/Publications/WP/Issues/2023/08/25/Macro-Prudential-Stress-Test-Models-A-Survey-537990>
30. KPMG、2024年。Cyber Resilience Stress Test (CRST)。 <https://kpmg.com/xx/en/ourinsights/ecb-office/hacking-the-2024-ecb-cyber-stress-test.html>
31. Linkov, I., Trump, B. D., Trump, J., Pescaroli, G., Hynes, W., Mavrodieva, A., Panda, A., 2022。重要インフラのレジリエンス・ストレス・テスト。利用可能な場所：
<https://www.sciencedirect.com/science/article/abs/pii/S2212420922005428?via%3Dihub>
<https://doi.org/10.1016/j.ijdr.2022.103323>

32. 国立標準技術研究所、2020年。情報システムと組織のためのセキュリティとプライバシー管理。
<https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>
33. Pendleton, J., Levite, A., Kolasky, B., 2024.クラウドの安心感：レジリエンスと信頼を強化する枠組み。
<https://carnegieendowment.org/research/2024/01/cloudreassurance-a-framework-to-enhance-resilience-and-trust?lang=en>
34. リスクビジネス、2024年備え続ける：ストレステストの世界の動向。<https://riskbusiness.com/wp-content/uploads/2024/01/Stress-Testing-Report-Jan2024.pdf>
35. Seðlabanki Íslands, 2023.TIBER-IS 実施ガイド。
<https://www.seðlabanki.is/library/Skraarsafn/Fjarmalainnvidir/TIBER-IS-ImplementationGuide.pdf>
36. パキスタン国立銀行、2020年ストレステストに関するガイドライン 2020（FSD Circular No 01 of 2020の付属書A）。<https://lsecentralbanking.medium.com/anintroduction-to-stress-testing-15d7e933dfc1>
37. Tan, M., Sung Jae, P., Hazarudin, H. A., 2021.LSE SU Central Banking Society - ストレステスト序論。
38. De, R., Taft, J. P., Webster, M. S., Forrester, J. P., Bisanz, M., 2020.米国の銀行規制当局が発表した「オペレーショナル・レジリエンスのための健全な慣行」。<https://lsecentralbanking.medium.com/anintroduction-to-stress-testing-15d7e933dfc1>
39. 投資協会、2021年シナリオテスト：シビアだが可能性はある。<https://www.theia.org/node/32166>

ENISA について

欧州連合サイバーセキュリティ機関（ENISA）は、欧州全体で高い共通レベルのサイバーセキュリティを実現することを目的とした欧州連合の機関である。2004年に設立され、EU サイバーセキュリティ法によって強化された欧州連合サイバーセキュリティ機関は、EU サイバー政策に貢献し、サイバーセキュリティ認証制度によって ICT 製品、サービス、プロセスの信頼性を高め、加盟国および EU 団体と協力し、欧州が明日のサイバー課題に備えるのを支援する。知識の共有、能力開発、意識向上を通じて、ENISA は主要な利害関係者と協力し、コネクテッドエコミーに対する信頼を強化し、EU のインフラのレジリエンスを高め、最終的には欧州の社会と市民のデジタルセキュリティを維持することを目指している。ENISA とその活動の詳細については、www.enisa.europa.eu。

ISBN **ENISA**
European Union Agency for Cybersecurity

978-92-9204-700-9 doi: 10.2824/8248517



Athens Office

Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office

95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office

Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

