



Nomura Research Institute Group

NEWS RELEASE

2026 年 10 月 22 日

株式会社野村総合研究所

NRI セキュアテクノロジーズ株式会社

野村総合研究所と NRI セキュア、 AI 駆動型サイバー攻撃への経営層の対応力強化を支援

～「能動的なシステム停止」の判断と説明責任の体制を、経営とセキュリティの両面から整備～

株式会社野村総合研究所（本社：東京都千代田区、代表取締役 社長：柳澤花芽、以下「NRI」）と NRI セキュアテクノロジーズ株式会社（本社：東京都千代田区、代表取締役社長：池田泰徳、以下「NRI セキュア」）は、「サイバーレジリエンス経営支援」（以下「本サービス」）の提供を本日、開始します。

本サービスは、AI 駆動型サイバー攻撃¹への対応力を強化したい企業・組織のうち、とくに EC・デジタル事業者、グローバル製造業や金融機関を含む重要インフラ事業者等を主な対象とします。外部に提供しているサービスや社内のシステムが停止した場合の事業に与える影響を定量・定性の両面から分析したうえで、対策として行う能動的な停止²・再開の判断基準を平時のうちに定め、有事の際の迅速かつ正確な経営判断を支援します。経営コンサルタントとセキュリティの専門家による合同チームが、経営層の意思決定に必要な根拠の可視化とプロセスの整備にあたります。

■ 背景：サイバー攻撃の期間短縮化に伴い、迅速な経営判断が課題に

NRI セキュアの分析によれば、セキュリティ上の脆弱性が公開されてから悪用されるまでの期間は、2018 年時点の平均約 2.3 年であった一方、近年では公開後数時間から 1 日程度で悪用が確認される事例も見られるなど、大幅に短縮しています³。背景には、フロンティア AI⁴の性能が向上し、脆弱性の偵察から発見、攻撃コードの生成・実行までを、AI が自律的に実行できる水準に近づいてきたことが挙げられます。

国内でも、攻撃によるシステム停止が長期化し、業績に重大な影響が生じた事例が出てきました。機微な個人情報が漏洩する事例も確認されています。被害は情報漏洩にとどまらず事業と企業価値の毀損にも及び、セキュリティ対策は「侵入を防げたか」から「事業影響を最小化できたか」が問われています。これに伴い、事業への影響を避けるためには、能動的にシステムを停止することも選択肢の一つとした備えが求められつつあります。金融庁と日本銀行は 2026 年 5 月、金融機関に短期的な対応として、「優先サー

ビス／IT システムの停止に備える」ことを要請しました⁵。

これらの環境変化を受けて、経営層には、システム停止の要否を含め、事業継続と被害抑制の双方を踏まえた迅速な意思決定が求められています。意思決定の主体も、CISO（情報セキュリティ担当役員）、CIO（情報システム担当役員）から、CEO（最高経営責任者）および取締役会を含む経営全体が担うべき事項となりました。

■ 本サービスの概要

本サービスでは、NRI の経営コンサルタントとシステムエンジニア、NRI セキュアのセキュリティ専門家が合同チームを組み、経営・セキュリティ・システムの 3 領域について、短期・中期・長期のそれぞれの視点で必要な対応力の強化を目指した包括的な支援メニューを提供します（表 1）。

とくに短期では、約 2～3 か月の期間で、現状把握から経営合意までを 4 つのステップで進めます（表 2）。ゴールは、AI 駆動型サイバー攻撃への対応の必要性和方針について、経営陣の合意を形成し、能動的なシステム停止を含めた経営判断の基準と意思決定プロセスを整備することです。停止判断を経営レベルで事前に定めることで、被害の拡大・長期化や社会への波及と、不要な停止による機能低下を抑えます。本サービスは、この両立を目指します。

短期での対応後は、パッチ適用プロセスの再構築、AI を活用したセキュリティ診断、セキュリティ運用の自動化、AI 利用状況の可視化などを、中長期の取り組みとして継続的に支援します。

表 1：本サービスの支援メニュー一覧

	短期（2～3 か月） 経営での対応必要性合意、 当面の対応方策検討	中期（半年程度） 本質的対応力の向上	長期（1 年以上） セキュリティ対応を競争力へ 昇華
経営の 対応力強化	○事業インパクト評価（金額 等の定量分析、事業影響リス ク等の定性分析を含む） ○能動的停止の対象システ ム・サービスおよび停止判断 基準の定義 ○経営上の対応課題の整理	○停止・再開方法の整備 ○ガバナンス、業務、ルール上 の課題対策ロードマップ策定 ○IR、ステークホルダーコミ ュニケーションの見直し ○経営層クライシストレーニ ング	○サイバーセキュリティ対策 の経営戦略への組み込み ○ステークホルダーマネジメ ント・統合報告書での情報開 示 ○AI・プライバシーガバナン ス強化
セキュリティの 対応力強化	○セキュリティ診断：機器／ 製品／バージョン／保守契 約／パッチ状況／サイバー BCP ⁶ の実効性	○パッチ適用／テストプロセ スの再構築、体制整備 ○AI 駆動型セキュリティ診断 ○セキュリティオペレーショ	○AI 駆動型防御への転換 (AI- SOC ⁷ 、自動パッチ) ○対策コストの最適化

	○パッチ適用高速化の課題 (構成情報管理、脆弱性情報 収集、トリアージ)と対応策 整理	ンのAI化 ○AI 利用状況の可視化／NHI (非人間ID) 管理	
システムの 対応力強化	○システム診断	○アーキテクチャ再設計 ○バックアップシステムの構 築	○システムモダナイゼーショ ン ○システム運用コストの最適 化

表2：短期（2～3 か月）での支援内容の詳細

ゴール：AI 駆動型サイバー攻撃への対応の必要性と方針について、経営陣が合意した状態			
STEP 1 現状把握	STEP 2 基準づくり	STEP 3 運用設計	STEP 4 経営合意
○セキュリティ診断によ る脆弱性の可視化と対応 方針の策定 ○事業インパクト評価 ○システム・サービス・事 業の連関整理	○外部公開の有無、接続 元制限、社会的影響度に 基づくシステム・サービ ス分類 ○到達難易度と事業影響 度による優先順位づけ ○システム・サービスご との停止・再開の判断基 準の定義	○検知から停止判断まで のアクションリストとフ ローの整備 ○停止中の顧客対応、再 稼働の判断フローの整備 ○グループ会社・委託先 への判断の伝達経路と役 割分担の整理 ○ステークホルダー別の 対外説明方針の策定	○経営上の対応課題の整 理（経営層の危機対応力、 ガバナンス・体制、サイバ ーBCP、企業価値・指標の 統合、情報開示） ○パッチ適用高速化の検 討（脆弱性トリアージ基 準の見直し案など） ○経営会議での報告と対 策ロードマップの策定

■ 本サービスの特長

1. 経営層の合意形成までを支援

従来多かった技術中心のセキュリティコンサルティングサービスと比べて、本サービスは経営トップも対象にしています（表3）。CEO、CISO、CIO、CFO（最高財務責任者）、IR 担当、法務担当、事業担当役員で構成する推進委員会を設置し、個別ヒアリングで認識の違いを可視化したうえで、対応方針の合意形成を支援します。「脆弱性対応の優先順位」、「対応を保留する場合の暫定策、承認者、見直し期限」、「外部提供サービスや社内システムを停止・再開する判断者と基準」の3点を平時のうちに確定することを目指します。

2. 事業への影響を定量・定性の両面で分析

システム停止によって生じる影響を、インシデント対応費用、停止に伴う臨時支出、契約不履行による違約金・損害賠償、顧客への補償、収益機会の損失、行政処分・制裁金、ユーザー離反、株価への影響などの類型に分けて試算します。あわせて、金額に換算しにくい社会的影響、顧客・取引先との信頼関係、ブランドへの影響といった定性的な事業影響リスクも整理します。どのシステム・サービスの停止がどの事業にどれだけの影響を与えるかを整理し、定量・定性の両面の根拠に基づく経営判断を可能にします。

3. 3つの専門性で実現する、AI時代のサイバー対応力強化

AI 駆動型サイバー攻撃の対応力を上げるには、経営・セキュリティ・システムの3つの専門性が必要です。NRI グループはこの3領域全てで高い専門性を有しているため、経営とセキュリティの現状を並行して診断し、中長期的なシステム対応力の強化を図ることができます。経営の意思決定体制、機器・パッチ適用状況などのセキュリティ、システム構成・アーキテクチャの課題を一度に洗い出し、相互の関係を踏まえた対応方針の策定から実装までを一貫して支援します。

表 3：従来の支援との違い

観点	従来（技術中心）の支援	本サービス
主な対象者	CISO、CIO、情報システム部門	CEO、取締役会（CISO・CIO・IR・法務などが参加）
支援の目標	侵入・被害の防止	侵入・被害の防止に加え、被害の連鎖と停止の長期化を抑え、事業価値への影響の最小化を目指す
判断の根拠	脆弱性の深刻度など技術指標	技術指標に加え、事業損益への影響額と事業影響リスク（どの事業の価値がいくら毀損しうるか、社会的影響はどの程度か）
成果物の範囲	技術的な対策方針、運用手順	左の項目に加え、停止・再開の判断基準、経営の意思決定フロー、对外説明方針（事業価値の毀損を抑えるための一連の仕組み）
想定される効果	技術的なリスクの低減	左の項目に加え、停止に伴う損失の抑制と、顧客・株主・当局への説明責任の強化

両社は、今後も、企業・組織のサイバーセキュリティ対策と経営基盤強化の支援を通じて、安全で安心な情報システム環境と社会の実現に貢献していきます。

-
- ¹ **AI 駆動型サイバー攻撃**：AI を悪用し、偵察、脆弱性の発見、攻撃コードの生成、攻撃の実行までを高速かつ自動的に行うサイバー攻撃。攻撃者の技能や人数に依存せず、短期間に大量の攻撃が可能になる点が特徴。
 - ² **能動的な停止**：被害が拡大する前に、脆弱性の公表や攻撃の兆候を検知した段階で、企業側の判断により対象のシステムやサービス（外部に提供しているサービスを含む）を意図的に停止すること。修復のための時間を確保し、被害の連鎖を防ぐことを目的とする。
 - ³ **Edgescan「Vulnerability Statistics Report 2026（11th edition）」**等をもとに、**NRI セキュア分析**。**CVE**（共通脆弱性識別子）の公開後、実環境での悪用が確認されるまでの期間を指す。調査時点や対象により変動する。
 - ⁴ **フロンティア AI**：現時点で最高水準の性能を持ち、社会に大きな影響を及ぼしうる汎用性の高い先端 AI モデル。高度な推論により、複数の工程にわたる作業を自律的に実行できる。
 - ⁵ **2026 年 5 月 22 日公表「フロンティア AI による脅威変化を踏まえた金融機関等の短期的な対応」**
(<https://www.fsa.go.jp/news/r7/sonota/20260522-5/20260522.html>)
 - ⁶ **サイバーBCP**：サイバー攻撃によるシステム停止を前提に、停止・再開の判断基準、意思決定の手順、システムを使わない業務運営、対外説明までを定めた事業継続計画。
 - ⁷ **AI-SOC**：脅威の検知、影響の分析、対応の一部を AI で自動化したセキュリティ監視・運用体制。人手による監視と組み合わせ、処理の速度と量を高めることを目的とする。

【ニュースリリースに関するお問い合わせ】

株式会社野村総合研究所 コーポレートコミュニケーション部 日下部、玉岡

TEL：03-5877-7100 E-mail：kouhou@nri.co.jp

【本件に関するお問い合わせ】

株式会社野村総合研究所 ICT・コンテンツ産業コンサルティング部 前原、紺谷、八木

NRI セキュアテクノロジーズ株式会社 事業戦略推進本部 山口

マネジメントコンサルティング事業本部 上田

E-mail：crmc@nri.co.jp