Nomura Research Institute Group

NEWS RELEASE

2025 年 6 月 26 日

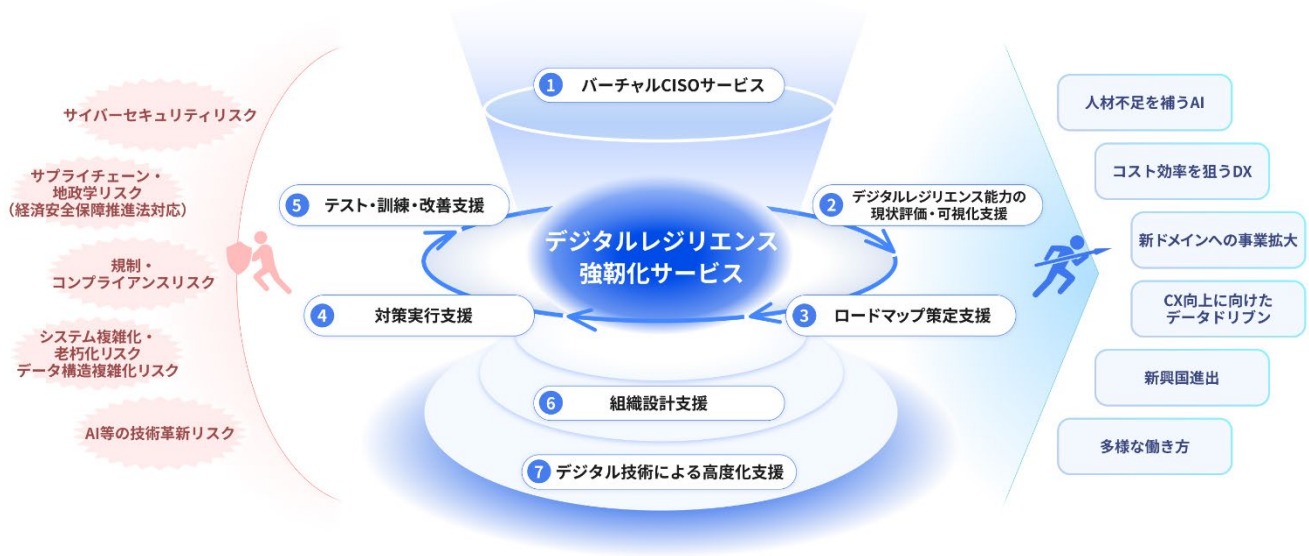
株式会社野村総合研究所

野村総合研究所、企業の経営層を支援する デジタルレジリエンス強靭化サービスを開始

～サプライチェーン全体のサイバーセキュリティから IT 障害まで、
企業を取り巻く複合的なリスクに対応～

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」）は、企業が直面するサイバーセキュリティとオペレーショナル・レジリエンス（業務の強靭性・復旧力）において、経営層が取り組むべき課題の解決を支援する「デジタルレジリエンス[1]強靭化サービス」（以下「本サービス」）を、2025 年 7 月に提供開始します。本サービスは、経営者の視点でリスクの可視化、計画的なリスクコントロール、組織・プロセスの最適化、ステークホルダーへの説明など、デジタルレジリエンス強靭化の支援を行うとともに、現場での着実な実行と定着を支援するものです。

図：デジタルレジリエンス強靭化サービスのイメージ



■ 高度化・複雑化するリスクが経営課題に －デジタルレジリエンスの必要性

近年、企業が直面するリスクはますます高度化・複雑化しています。地政学リスクの高まりや、経済安全保障への対応が求められる中、デジタル主権の確立やサプライチェーン全体でのサイバーセキュリティとオペレーショナル・レジリエンスの確保は、重要な経営課題となっています。具体的には、ランサムウェア被害時の復旧期間や費用の長期化と高額化、システムの老朽化や複雑化による障害対応の困難化、システムの複雑化によるリリース遅延、規制違反による罰則・制裁など、リスク対応の不備が事業継続に影響を及ぼすケースが増えています。

経営層は直面するリスクに対して「知らなかった」では済まされず、対策および説明責任がステークホルダーから求められます。CISO（Chief Information Security Officer：最高情報セキュリティ責任者）が、幅広いリスクを把握し、組織横断的に優先順位をつけてデジタルレジリエンス強靭化に取り組むことが望まれますが、多くの日本企業では CISO が設置されていません[2]。さらに CISO が設置されていても十分機能していない場合も含めると、組織としてリスクの全体像を把握できておらず、優先度の高いリスクへの対応が漏れているケースが、相当程度あると想定されます。

■ 経営層を支援するデジタルレジリエンス強靭化サービスの内容

本サービスはこのような背景を踏まえ、NRI グループがこれまで培ってきたサイバーセキュリティおよびオペレーショナル・レジリエンス支援の経験とノウハウを活かし、近年急速に活用が進む AI のセキュリティ・ガバナンスのリスクを含め、CISO の観点でリスクを統合的に評価および可視化し、事業部門および IT 部門での個別活動支援に至るまで、企業のデジタルレジリエンス強靭化を一貫してサポートします。本サービスの主な支援内容は以下の通りです。

① バーチャル CISO サービス

CISO は、経営計画に基づいてデジタルレジリエンス強靭化の戦略を構築し、日々変化する脅威や技術動向に対応することになります。CISO は、経営と技術両面の幅広い知識とスキル、CEO や取締役会・株主・顧客・事業部門など社内外のステークホルダーからのプレッシャーを受けながら施策を推進する実行力と、コミュニケーション能力が求められる難易度の高いポジションです。そこで本サービスが「バーチャル CISO」となり、経営層が以下②～⑦の各施策を推進する際の支援、社内外のステークホルダーに対するリスク説明の支援などを行います。

② デジタルレジリエンス能力の現状評価・可視化支援

企業が AI 活用やデジタルトランスフォーメーション（DX）などの新たな取り組みを進める際、新たに生じるリスクに加え、潜在的なリスクの発現も考慮することが必要です。本支援はこれらのリスクに対するサイバー攻撃や IT 障害など、デジタル上の脅威に対する対応力（デジタルレジリエンス能力）を評価し、課題を明確にしたうえで、対策方針を整理します。

③　ロードマップ策定支援

デジタルレジリエンスのあるべき姿を定義した上で、サービスやシステムのリリース・更改などのイベント、組織横断での優先度を考慮し、②の対策方針を実行するロードマップ策定を支援します。

④　対策実行支援

デジタルレジリエンス強化のため、各課題への対策実行を支援します。詳細は末尾の【ご参考】をご覧ください。

⑤　テスト・訓練・改善支援

対策の妥当性を確認するためテストや訓練を実施し、評価・改善を行います。

⑥　組織設計支援

デジタルレジリエンスを高度化するための組織やマネジメント体制の構築を支援します。

⑦　デジタル技術による高度化支援

現在の業務・システムに対して、デジタル技術を活用してデジタルレジリエンスの高度化や自動化による効率化を支援します。

高度化・自動化にあたっては、NRI および NRI セキュアテクノロジーズ株式会社のプラットフォームサービス「NRI デジタルトラスト」を活用することが可能です。NRI デジタルトラストの詳細は末尾の【ご参考】をご覧ください。

企業が直面するリスクはこれからも更に高度化・複雑化が予想されます。NRI グループはこれからも本サービスを進化させ、企業のデジタルレジリエンス強靭化に貢献していきます。

---

[1] デジタルレジリエンス：デジタルサービスやシステム、データへの脅威（サイバー攻撃やシステム障害、自然災害など）から組織を守り、あらゆる種類の妨害に効果的に対応し、事業継続を確保して迅速に復旧できる能力のこと。

[2] 詳細は、NRI セキュアテクノロジーズ株式会社「企業における情報セキュリティ実態調査 2023」https://www.nri-secure.co.jp/download/insight2023-report　をご参照ください。

【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　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　IT アーキテクチャーコンサルティング部　下田、鶴田、板田、野村、原田

E-mail：digital-resilience@nri.co.jp

【ご参考】

（1）対策実行支援の詳細

デジタルレジリエンス強化にあたっては、企業にとって優先度の高いリスクに対し、現場での確実な対応が求められます。本サービスの「対策実行支援」においては、事業部門や IT 部門に対し、以下のような支援を組み合わせて提供し、確実な実行をサポートします。

主要な対策実行支援一覧

カテゴリ	#	テーマ	詳細説明
サイバーセキュリティ	1	デジタルクライム	サイバー攻撃や不正アクセスなどのデジタル犯罪に対する最新の脅威動向を踏まえたリスクアセスメント、対策立案、ならびにインシデント発生時の対応支援を提供。サービス設計段階からのリスク低減と、被害最小化・早期復旧を実現。
	2	セキュリティレジリエンス（ランサムウェア対応）	ランサムウェアをはじめとする高度なサイバー攻撃に備え、事前の脆弱性診断や多層防御の設計、インシデント発生時の対応計画策定・訓練を支援。事業継続性を確保するための体制強化を実現。
	3	グローバルセキュリティ	海外の子会社・関連会社・拠点に対するセキュリティアセスメントおよび対策の立案と実行。
	4	IT デューデリジェンス（M&A・業務提携）	M&A や業務提携時における IT・サイバーセキュリティリスクの調査と評価。
	5	サプライチェーン（経済安全保障・地政学リスク対応）	経済安全保障・地政学リスクの観点を踏まえ、業務継続のために、取引先・委託先を含むサプライチェーン全体のリスク管理体制構築を支援。
	6	TLPT（脅威ベースのペネトレーションテスト）	サイバー攻撃をシミュレーションし、実機・実環境を利用したテストを通じて、組織のサイバーセキュリティ体制およびレジリエンスの評価・強化を支援。
プライバシー	7	プライバシーガバナンス	個人情報保護関連法、GDPR などに対応しつつ、顧客情報の安全で、適切な管理を行う仕組みを構築。さらに、データ活用によるビジネス価値創出とプライバシーリスクのバランスを最適化し、企業およびサービスの信頼性を向上。
AI	8	AI セキュリティ・ガバナンス	AI 活用に伴うセキュリティ・プライバシーリスクの評価や、AI ガバナンス体制の構築を支援。AI システムの安全性・信頼性確保に向け、最新のセキュリティ技術と規制動向を踏まえた支援を実施。

カテゴリ	#	テーマ	詳細説明
開発	9	次世代開発 （テスト自動化）	自動テストツールの導入による開発プロセス効率化・品質向上を支援。迅速なリリースと高品質なシステムを実現。
	10	セキュア開発	「セキュリティ・バイ・デザイン」を標準化したセキュア開発プラットフォームを活用し、要件定義から設計・実装・テスト・運用まで、システム開発ライフサイクル全体で脆弱性対策を徹底。DevSecOps や CI/CD、SBOM 管理など最新の開発手法にも対応。
運用	11	次世代運用 （運用自動化）	AI や自動化ツールを活用した運用プロセスの効率化・自動化を支援。運用負荷の軽減とサービス品質向上を両立し、次世代の IT 運用体制を実現。
	12	セキュリティ 運用・監視	CSIRT、24 時間 365 日の SOC（セキュリティオペレーションセンター）の構築を支援し、これをもとに脆弱性情報管理、インシデント対応体制の構築・運用や運用プロセスの最適化を支援。
インフラ・アーキテクチャー	13	ゼロトラスト	ゼロトラストの現在の成熟度を評価し、認証・認可の強化やアクセス制御の最適化を支援。企業実態に合わせて導入計画策定から実装、運用まで一貫してサポート。
	14	レガシー・ モダナイゼーション	老朽化したシステムの現状分析から、最新技術への移行計画策定・実行までを支援。セキュリティと運用効率を両立した移行を実現。
障害対応	15	障害対応高度化	システム障害発生時の初動対応や復旧プロセスの高度化を支援。アーキテクチャー改善、体制とプロセス構築、人材教育の観点で高度化を実現。
ビジネス継続	16	BCP	自然災害やサイバー攻撃などの緊急事態に備えた事業継続計画（BCP）の策定・運用を支援。リスク評価から復旧手順の整備、訓練の実施を一貫してサポート。

（2）NRI デジタルトラストの詳細

企業におけるシステムライフサイクル全体でのサイバーセキュリティと、サイバーリスクに対するオペレーショナル・レジリエンス（業務の強靭性・復旧力）の確保を目的とし、関連する各種ガイドラインや法規制に準拠するセキュリティ機能をあらかじめ組み込んだプラットフォームサービスです。詳細は次の発表資料をご覧ください。

野村総合研究所、マルチクラウド戦略に基づくサービスを拡充し、顧客企業のガバナンス強化と利便性向上を加速 https://www.nri.com/jp/news/info/20250212_1.html

NRI セキュア、野村総合研究所と共同でサイバーセキュリティ機能を組み込んだプラットフォームサービスを提供開始 https://www.nri-secure.co.jp/news/2025/0212