サイバーレジリエンスと事業継続

CYBER RESILIENCY TECHNIQUES

• Adaptive response	•適応応答
• Analytic monitoring	•分析モニタリング
• Coordinated protection	•協調的な保護
• Deception	• 欺くこと
• Diversity	•多様性
• Dynamic positioning	•動的ポジショニング
• Dynamic representation	•動的な表現
• Non-persistence	•非永続性
• Privilege restriction	•特権の制限
• Realignment	•再調整
• Redundancy	•冗長性
• Segmentation	•セグメンテーション
• Substantiated integrity	•実証された完全性
• Unpredictability	•予測不能

引用： Draft NIST Special Publication 800-160 Systems Security Engineering：
Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems

企業がセキュリティ強化する目的は、事業継続にあります。
BCP（事業継続計画）の中でも、情報システムの維持ができないと、事業が成り立ちません。そうした中で、「サイバーレジリエンス (Cyber Resilience)」が注目されています。
レジリエンスとは、弾力、復元力、回復力を意味する言葉で、変化に対処する能力のことです。反対語は、脆弱性（vulnerability）です。よって、サイバーレジリエンスは、サイバー攻撃に対する耐性、あるいは強靭性といった回復力の強さや、復旧する能力ということになります。
標的型攻撃や、DDos 攻撃など、サイバー攻撃が激しさを増してきた現代において、セキュリティ対策によって全てを防御できるという保証は、残念ながらどこにもありません。そうであれば、万が一サイバー攻撃に見舞われたとしても、被害を最小限に留め、一刻も早い復旧ができる仕組みが必要です。
そのためには、セキュリティ強化についても、サイバー攻撃を受けたとしても可能な限りビジネスインパクトがないように、重要な業務より優先順次を付けて、対策を施します。ディザスタリカバリーの考え方と同様に、早期に回復が必要なもの、復旧に時間的猶予が見込めるものを判別し、それぞれの回復手順まで明確に規定します。場合によっては、業務を中断せざるを得ないケースもあるため、経営層まで一緒にサイバーレジリエンスに取り組む必要があります。
サイバーレジリエンスの手法は、システムズエンジニアリング標準の「ISO/IEC 15288」に基づいた、米国立標準技術研究所（NIST）の「Systems Security Engineering：Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems」というガイドラインのドラフトの中にも、CYBER RESILIENCY TECHNIQUES として 14 種類の手法が公開されています。
手順としては、課題に優先順次をつけ、ニーズやシステム、アーキテクチャの要件定義をし、設計します。そして、システムを分析し、実装し、それぞれを統合します。それを、検証し、トレーニングを提供して、妥当性を確認します。最終的に運用に乗せ、保守や廃止ができるようにします。
こうした手法を参考に、企業はそれぞれの環境に合わせ、リスクマネージメントの戦略に応じてサイバーレジリエンスを向上させる必要があります。そのためには、会社あげて常に最新情報を把握し、適宜レビューをすることが大切です。