

なぜサイバー攻撃から
企業を守れないのか？

AI時代 の セキュリティ 教育

LRM株式会社

坪井暁人

AKIHITO TSUBOI

LRM株式会社

藤居朋之

TOMOYUKI FUJII

はじめに

「セキュリティ対策はコストがかかるだけで、売上には繋がらない」

「セキュリティ教育の効果は曖昧で、可視化できないものだ」

「セキュリティは情報システム部門（情シス）が対応すべき仕事だ」

多くの日本企業において、**情報セキュリティに関する話題は、いまだに「守り」や「コスト」、あるいは「義務」の文脈で語られることが大半です。**しかし、AI技術が急速に進化し、サイバー攻撃が巧妙かつ大量に襲ってくる時代。**その認識のままでは、企業にとって最大の脆弱性になりかねません。**

AIの進化は、仕事のやり方、情報の利活用方法、そして情報セキュリティに大きな影響を与えています。例えば、私たちはいま、Claude Coworkで事業KPIの整

理や日程調整を行い、Claude Code Agent Teams や Codex を使ったマルチ AI エージェントで開発を行っています。これらのツールは 2026 年 1 月から 2 月にかけてリリースされたもので、流行りのツールは今後も変わっていくでしょう。

AI エージェントの導入に必要なセキュリティへの投資をためらっている間に、準備を終えた競合は意思決定のスピードを何倍にも速めています。サイバー攻撃に備えるためには確かに投資が必要ですが、AI を使えない企業が失うのは毎日の競争力です。

AI の能力が上がれば上がるほど、使うことのリスクも大きくなります。一方で、AI を使わない場合の機会損失のリスクがますます大きく、そして現実的なものになりつつあります。いま、本当に怖いリスクはどちらでしょうか。

私たちは、年間約 600 社へのセキュリティに関するコンサルティングと、2500 社以上へのセキュリティ教育ツールを提供しています。現場で得た、「セキュリティで組織を強くする」知見を共有するために、本書を出版しました。

ストーリー

A1時代のセキュリティ教育
なぜサイバー攻撃から企業を守れないのか？

はじめに

組織を揺るがす一雫 セキュリティ意識の変革物語

第1部 金曜日の1クリック、一雫の雨がもたらした絶望…… 14
 第2部 終わらない雨、あるいは凡庸な悪意の正体…… 30
 第3部 雨上がりの誓い、明日への道標…… 47

第1章

「人」への教育が組織を強くする

巧妙かつ大量の脅威

68

2

行動変容を生み出す 教育プログラム

AIエージェント時代における新たな脅威	74
リスクを遠ざける「脅威インテリジェンス」	84
設計段階からリスクに備える	92
攻撃者が狙うのは「人」の脆弱性	97
サプライチェーン全体が狙われる	103
なぜ従業員に「教育」が必要なのか	109
どのように攻撃を把握するのか	118
セキュリティ教育の3つの領域	129
組織成熟度に応じたロードマップ	135
セキュリティ教育に必要な3つの視点	145
セキュリティ教育の構造を設計する	149
行動変容を生み出す「TEACHモデル」	160
教育効果を最大化する4つの主要施策	170

第3章

セキキュリティカルチャーを
根付かせる

- セキキュリティ対策を明文化する……………182
- セキキュリティ教育の指標を決める……………188
- 指標は教育レベルに合わせて変化させる……………195
- データ活用による教育の「高度化」……………199
- 段階的にデータ分析を進める……………209
- 「教育」を「カルチャー」に変えるために……………216
- セキキュリティと心理的安全性……………226

第4章

セキキュリティで会社を伸ばす

- 企業規模に合わせた教育戦略……………232
- 事業領域から考えるセキキュリティ戦略……………245
- 情報が経営を動かすA I時代のセキキュリティ……………252

情報の「質」と利活用の「速度」	256
ROEの構造で情報経営を考える	261
情報もP・L・B・S・C・Fの関係にある	266
情報リターンと情報セキュリティリスク	271
セキュリティは経営そのものである	278
おわりに	282
参考文献	286