自動化にはセキュリティ対策が前提条件

自動化に必要なセキュリティ対策

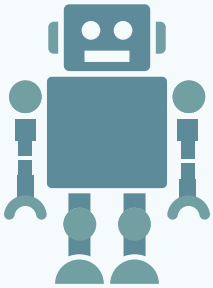
① リスクを洗い出し分析する

② セキュリティポリシーを見直す

③ リスク対策の仕組みを ロボット開発時から組み込む

④ 運用後知識ベースを適宜更新する

ロボット用に
セキュリティポリシー
の見直し



セキュリティポリシー
の遵守

業務の自動化を進める場合、その仕組みに必須の前提条件としてセキュリティ対策を組み込む必要があります。
数年前ロシアでヒト型ロボットが逃げだすという事件がありましたが、RPA でも野良ロボットが問題視されています。
サイバーセキュリティ対策などを、既存の開発システムと同等なレベル以上でセキュリティ対策を施すのは当然ですが、ヒトの代行をさせるためには、ヒトの目線で就業規則などと同様に、ロボットの行動がセキュリティインシデントを起こさせない対策が必要になってきます。
ロボットに自律した判断をさせるためには AI を組み込むことになりますが、それはまさしくロボットに知能を持たせることと同じになります。
となると、子供を育てる時と同様、善悪を教えなければ、平気で不正や暴走をはじめるかもしれません。善悪の判断は、その時代や民族に違いで異なってくるものです。何が正しくて、何が悪いのか、それを断定することはなかなか難しいことです。それでは、何をよりどころにしてロボットを教育すべきでしょうか？
将来、いろんな組織や団体で AI やロボットのセキュリティに対して、統一的なガイドラインや規則を作ろうという動きがありますが、現時点では、企業は、その企業のセキュリティ―ポリシーをロボットを採用する前提で見直し、それを適用すべきです。
つまり、総務省や経済産業省、IPA などが出している AI や IoT 等を含めたセキュリティ対策のガイドラインを元に、その企業に則したセキュリティポリシーを決め、想定外なインシデントが発生した場合には、セキュリティ対策の知識ベースを更新し、適宜見直してポリシーをアップデートすることが重要です。そうすれば、その時点で最良と考えられるセキュリティ対策を施すことが可能になります。
ポイントは、ロボットを作成したあとの運用フェーズでセキュリティ対策を考慮し始めるのではなく、ロボット開発時よりリスク分析して、その対応計画をセキュリティ―ポリシーに則って作成し、ロボットを開発することです。そうでなければ、エラーハンドリングなどがタイムリーに処理できず、結果、自動化する前より時間がかかったり、かえって業務に悪影響を及ぼす危険があるからです。