JIG-SAW

報道関係者各位

2015年8月17日
ジグソー株式会社
https://www.jig-saw.com/

９月よりサイバーセキュリティ分野に進出：「Auto Shutdown Service」開始

ジグソー株式会社は、この度、サイバーセキュリティ分野に進出いたします。今回はまず第一弾として、インターネットにおいて大きな脅威になっているサイバー攻撃等による情報漏洩リスクに対して、ゼロデイアタック(※注記１)など未知の攻撃(セキュリティソフト対応範囲外)やヒューマンエラーによる不可避な状況で侵入を許した場合に備えた、侵入自動検知・自動シャットダウン・自動通報・自動処理の一連の流れをロボット型ソフトウェアによってシームレスに制御するオリジナルサービス「Auto Shutdown Service」のご提供を９月より開始いたします。

従来より情報漏洩の主因は、様々なセキュリティソフトやツール等の対策の有無に関わらず、設定ミス・漏れ・アップデート不備などセキュリティソフトウェア等の性能や機能とは全く次元の異なるヒューマンエラーが引き起こしているのが現実であり、このような原因によって外部からの不正侵入やウイルス感染、標的型攻撃等による甚大な被害へつながっております。当社は、未然に防ぐことができずに侵入を許した場合において、即時にシステムの停止やネットワークの遮断を行ない、指定された特定の宛先に対して自動的にメッセージとコールで通知するとともに、予め決められた対処まで全てを自動で行うリアルタイムサービスになります。これは侵入が意図したものであるか否かの判断を待たず、情報管理・保全を最優先とし、即時にシステムの停止やネットワークを遮断するものであり、膨大な個人情報や機密情報の漏洩を最大リスクとして捉え、その漏洩リスクを最小限にとどめる(場合によっては漏洩を回避する)ものであります。

また侵入の証拠保全、影響範囲の特定までの迅速化、Linux カーネルレベルの技術をベースにしたファイル改竄検知を視野に入れており、情報漏洩の極小化とその後の迅速な対応に大きく寄与するサービスになります。全てのモノがインターネットに繋がる IoT の世界においては、このようなニーズは爆発的に増加すると想定されており、今後は意図したアクセスか否かの判断についても人工知能を活用し、ユーザーの様々な要望に対応してまいります。

※注記１：ゼロデイアタック

ソフトウェアにセキュリティ上の脆弱性(セキュリティホール)が発見され、問題の存在自体が広く公表される前にその脆弱性を悪用して行われる攻撃(アタック)を指す。外部の攻撃から守るには、公開されるパッチを、公開後即座に適用するのが基本だが、ゼロデイアタックの場合は対応策が公表される前に攻撃が行われるため、このような対策では実質上防ぎきれない。実際、対策を取る前に、発見された脆弱性の情報が流通し、攻撃用ツールが配布される事例が多数報告されており、この「時間差」が大きな問題である。このような攻撃に使用されるパケットの特徴を分析し、遮断するソフトウェアの研究も各所で行われているが、有効で万能な解決策は今のところない。

【ジグソー株式会社について】

ジグソー株式会社はIoTビッグデータを活用した自動運用(オートパイロット)サービスと、人工知能およびロボット型ソフトウエアをベースとした自動制御システムをクラウド提供。そのほかにも、システム監視、障害対応からシステム運用全般までトータルサポートなどを行っている国内唯一の次世代総合システム運用カンパニーです。

■会社概要

会社名： ジグソー株式会社(URL：https://www.jig-saw.com/)
証券コード：3914
所在地： 東京本社/東京都港区三田2-10-6 9F
札幌本店/北海道札幌市北区北8条西3丁目32番7階
SCCおよびサテライトオフィス、A&Aラボ/札幌市内
代表者： 代表取締役 山川 真考
設　立： 2001年11月
資本金： 3億1,410万円(2015年5月29日現在)