SQAT® Security Report

2026-2027年 秋冬号

AIとセキュリティ

知る・守る
続ける

BBSecは内閣官房国家サイバー統括室の
「サイバーセキュリティ普及啓発」に賛同しています

便利で安全なネットワーク社会を創造する
株式会社ブロードバンドセキュリティ

ごあいさつ

株式会社ブロードバンドセキュリティ
取締役兼 セキュリティサービス本部 本部長　齊藤 義人

2026年上半期も、企業や組織を取り巻くサイバー脅威は衰えることなく、さまざまな業種で被害が確認されました。個人情報を扱うWebサービス、医療機関のシステム、海外拠点、さらには企業内の人間関係や指揮命令系統まで、攻撃者が狙う対象は広がり続けています。こうした状況は、サプライチェーンを含め、組織を取り巻くさまざまな「接点」にサイバーリスクが潜んでいることを改めて示しています。

上半期を象徴する事案の一つとして、6月に発覚した大手保険会社への不正アクセスが挙げられます。その後の調査では、約440万人分の個人情報が漏洩したことが公表されました。また、首都圏の大学病院では、医療機器の保守に利用されていたVPN装置を侵入経路とするランサムウェア攻撃が発生し、患者情報の漏洩が確認されました。いずれも、顧客向けサービスや保守用ネットワークなど、業務上必要な外部との接点をどのように管理するかという課題を浮き彫りにしています。

企業グループ全体の管理という観点では、国内大手製造業のイタリアおよびモロッコのグループ拠点への不正アクセスも注目されました。事業のグローバル化が進む中、本社だけでなく、海外拠点やグループ会社を含めた一貫したセキュリティ管理が求められています。

一方で、攻撃者が狙うのはシステム上の弱点だけではありません。2025年末から2026年にかけては、実在する社長や会社名をかたり、送金などを指示する詐欺メールが相次ぎました。技術的な対策に加え、人の心理や組織内の信頼関係を悪用する攻撃に備え、確認手順や運用面での対策を整えることも重要です。また、下半期に入っておりますが7月には、大手食品関連企業へのサイバー攻撃により、冷蔵倉庫の入出庫や冷凍食品の出荷に影響が生じ、大きく注目されました。サイバー攻撃の影響が情報システムの内部にとどまらず、物流や商品供給といった実際の事業活動へ波及することを、改めて印象付ける出来事でした。

このように2026年上半期は、組織と外部をつなぐさまざまな「接点」が、利便性を支える一方で攻撃の起点にもなり得ることを強く意識させる半年でした。本レポートが、読者の皆さまにとって自組織のリスクを見つめ直し、今後のセキュリティ対策を考えるための一助となれば幸いです。

一般社団法人　日本ハッカー協会主催
「Hack Fes. 2026」の様子（2026年7月開催）

専門知識を学んだり、スキルを磨いたりするためのセキュリティエンジニア対象のイベント「Hack Fes. 2026」に弊社は協賛企業として参加しました。

※写真は弊社撮影。撮影および掲載許可を得ています。

CONTENTS

＜巻頭企画＞
AIとセキュリティ
奈良先端科学技術大学院大学
門林 雄基教授 寄稿記事 ——— 02

＜注目テーマ＞
企業や組織が取り組むべき情報セキュリティ
～「サプライチェーン強化に向けたセキュリティ対策評価制度」について～ —— 09

診断の現場から ——— 13

＜情報セキュリティコラム＞
APTとは何か
長期・執拗に狙うサイバー攻撃の特徴と対策 ——— 15

＜現状分析＞
診断結果にみる情報セキュリティの現状
～2026年上半期　診断結果分析～ ——— 17

カテゴリ別脆弱性検出状況 ——— 19

業界別診断結果レーダーチャート ——— 21

※本レポートは、弊社セキュリティサービス本部のホームページ
「SQAT®.jp（URL：https://www.sqat.jp/）」
https://www.sqat.jp/sqat-securityreport/からダウンロード可能です。

SQAT.jp

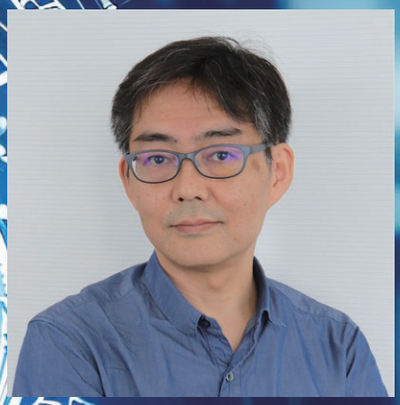
※ 本誌において記載されている会社名、商品名、サービス名は各社の商標又は登録商標です。なお、本文中では商標又は登録商標を表すマークを特に提示していない場合があります。

本誌は、別途記載のある第三者の著作物を除き、クリエイティブ・コモンズ 表示－非営利4.0国際（CC BY-NC 4.0）ライセンスの下で提供しています。
非営利目的での複製、再配布および改変は、同ライセンスの条件に従って行うことができます。営利目的での利用は許諾しておりません。二次利用にあたっては、出典〔株式会社ブロードバンドセキュリティ発行『SQAT® Security Report 2026-2027年 秋冬号』〕、ライセンスを明示し、改変した場合はその旨を表示してください。　ライセンスの詳細：https://creativecommons.org/licenses/by-nc/4.0/deed.ja　　SQAT®はBBSecの登録商標です。登録商標第5146108号

巻頭企画

AI とセキュリティ

門林　雄基
奈良先端科学技術大学院大学
サイバーレジリエンス構成学研究室　教授



AIとセキュリティは数十年前から、切っても切れない関係にある。少なくとも学術の世界ではそうだったし、技術の深いところをおわかりの諸兄なら説明不要だろう。ここでは「AIって人工知能なんでしょう」という、ざっくりとした理解をお持ちの多数派の読者にとって「AIの性質」と「セキュリティの要件」がどのように絡み合っていたのか、また、今後どのように絡み合っていくのかを考える材料を提供できればと思う。

1. 研究室を飛び出した技術たち

AIとセキュリティは、いずれも研究室を飛び出した技術だという点で兄弟だとも言える。ただ、同じラボの出身ではないので、考え方も行動様式もまったく異なる。お互いのことを「そんなので実用レベルと言えるのか」と批判的な目で見ていたりもする。数十年も前から切っても切れない関係にあるのに、困ったものである。

原因の一つはサイロ化にある。多くの大学では、セキュリティ専門のラボとAI専門のラボは別々に存在しているし、両方に所属して脳みそを倍の速度でパンクさせたい奇特な学生は非常に少ない。企業はAIとセキュリティ両方がわかる人材が欲しいのに、である。

私はAIが専門ではないが、もう20年以上もセキュリティ業務にAIを活用するために研究を続けてきたので、それなりに癖はわかっている。世界中から優秀な学生が集まるが、これはAIとセキュリティを両方実践しているラボが少ないことの裏返しでもある。日本人ももっと、AIとセキュリティだけでなく、ロボティクスも、経済も、と知識とスキルに貪欲になったほうがいい。大学は教養を身につけるところである。AIもセキュリティも現代の教養だというのに、それぞれ専門のラボの教授に弟子入りしないと学べないとしたら、それは嘆かわしいことである。

ちなみに民間の資格でもある程度のところは学べるが、どうしても教える側のコスパであるとか、学ぶ側のタイパが優先されるので広く浅くなりがちである。必ずしも大学でなくても良いが、大学院の2年間つまり5000時間くらいは修行した者でないと、安全運転を任せることはできない。比較としてパイロットの世界では、副操縦士になるためには実技含め学習時間として3000時間くらい、一人前の機長になるためにはさらに3000から5000時間の実務経験が必要だそうである。産業界のリーダーと話すと、国内留学で1年や2年も必要なのか、と学習期間をケチる傾向があるが、御社の安全運行を任せるのが副操縦士でいいんですか、と思ってしまう。翻ってAIやセキュリティ業界の履歴書で総飛行時間に相当する数字は見たことがない。このあたり航空業界から学べることは多いだろう。

AIとセキュリティは研究室を飛び出した技術なので、知識とスキルをアップデートし続けないとあっという間に陳腐化してしまう。5年前の知識ではもはや太刀打ちできない。このあたり医学部に似ている。医師は知識をアップデートし続けるために、出身大学に時間を見つけて通うそうである。

我々も社会人むけにはリカレント教育に力を入れている。つまり共通の基礎教育を受け、倫理観や人間性について我々がよく知っている専門家に対して、AIやセキュリティに関する知識やスキルのアップデートのお手伝いをするということだ。まったく無資格の人間が、いきなりAIとセキュリティ両方に詳しくなれるわけではない。

2. 免許と実技、どちらも欠かせない技術たち

AIとセキュリティのもう一つの共通点は、体系的知識を持っていること（免許）に加えて、現場で一定品質の業務がこなせること（実技）が求められる点であろう。これはAIとセキュリティがどちらも、会社全体の生産性や機密性を担うようなハイパワーな技術であるため、自然とそうなる。クルマに例えるなら、普通自動車免許を持っているだけのペーパードライバーに5トントラックの運転を任せられないのと同じである。

研究室を飛び出した技術だから、というだけの理由で、かなり地頭のいい「AIの研究やってました」というAIエンジニアを雇うことの危険性はこのあたりにある。免許に相当する博士号なり、仮免許に相当する修士号は持っていたとして、気が遠くなるほど膨大なデータを分析する、あるいはそれを監督する業務を毎日、一定以上の品質でこなせるだろうか。地頭が良すぎると、社運がかかっている5トントラックの長距離運転が、仮にできたとしても、すぐに退屈になるのである。

それでいて危機は突然やってくる。なぜか今日だけ、AIの性能が急に悪くなった、という時にそれを直せるのは地頭くんかもしれない。ユーザ企業としては、そんな自動車でいうところのメカニックみたいな人はうちでは雇用できない、となるだろう。

高度な専門性をもつセキュリティを一手に引き受けるセキュリティ企業がこぞってAI分野に進出するのは、このようなタレントプールの集約ビジネスとしての類似性があるからなのだ。セキュリティの心配なく使えるAIを提供できるのは、当然であるがAIとセキュリティの両面で免許と実技をこなした人材を多く抱える企業ということになる。

5トントラックが日本車でもアメ車でも関係ない。それを安全に、一定以上の品質で毎日使いこなせる企業がAI時代の覇者である。もちろん安全に使いこなすためのノウハウは一般的なユーザ企業は持っていないであろうし、AIエンジニアだけでも、セキュリティエンジニアだけでも実現不可能だろう。幅広い分野にわたる高度な専門性を持ち、安全操業を長年支援してきた実績を証明できる会社が今日求められているのである。