SQAT® Security Report

2026年 春夏号

座談会
AIを生み出した〝人〟はAIを使いこなす〝人〟になる

知る・守る
続ける

BBSecは内閣サイバーセキュリティセンターの
「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

サイバー攻撃のニュースが日常となった状況は、2025年下半期においても変わることはありませんでした。むしろ、その影響は企業活動の枠を超え、市民生活にまで及ぶかたちで顕在化し、サイバーセキュリティが社会基盤の一部であることを強く印象付けた半年であったと言えるでしょう。

下半期を象徴する出来事の一つとして、大手酒造メーカーにおいて発生したサイバーインシデントが挙げられます。システム障害の影響により、商品の出荷や流通に支障が生じ、一部の小売店ではビール商品が棚から消えるといった事態が報じられました。サイバー攻撃が「情報漏洩」や「業務停止」にとどまらず、消費者が日常的に目にする商品供給にまで影響を及ぼし得るということを、多くの人が実感する出来事であったと言えます。これは、製造業や流通業におけるIT・OTの依存度の高まりと、サイバーリスクが直結してしまっているという現実を浮き彫りにしました。

また、技術的観点では、世界的に利用されているソフトウェアや基盤技術における深刻なゼロデイ脆弱性が相次いで明らかになり、その影響範囲の広さが改めて問題となりました。特定の製品や業種に限らず、多数の組織が同時にリスクにさらされる状況は、脆弱性情報の把握や初動対応の遅れが、被害拡大に直結することを示しています。こうした事柄は、「自社は直接狙われていない」という考えが、もはや限界にきていることを示唆しています。

一方で、2025年下半期は、AIを巡るリスクの捉え方にも新たな段階が見られました。現在、ITエンジニアの約9割が生成AIを日常的に利用し、その多くがコード補完やレビュー支援といった開発業務に活用しているとされています。そんな中、とりわけ懸念されるのが、学習データや参照データに意図的または偶発的な改ざんが混入する「データ汚染攻撃（データポイズニング攻撃）」です。汚染された情報をもとに生成されたコードや設定例が、開発者に疑われることなく採用され、そのまま製品やシステムに組み込まれてしまう可能性も否定できません。こうしたコードは一見すると正当で有用に見えるため、結果として脆弱性や不正な挙動が知らないうちに持ち込まれてしまう危険性があります。AIを業務に組み込むからこそ、その出力をどのように検証し、どこで人が責任を持って判断するのかという統制の設計が、これまで以上に重要になっています。

このように、2025年下半期のサイバーリスクは、「被害の身近化」と「影響範囲の拡大」という二つの側面から、私たちに強い警鐘を鳴らしました。攻撃手法や技術は変化し続けますが、攻撃者が狙うのは往々にして、「棚卸や管理が適切になされていない資産」や「管理責任の所在が曖昧な領域」、そして「形骸化した運用」です。

本レポートでは、こうした下半期の動向を踏まえ、現場で直面する課題や今後の対策検討に役立つ視点を整理しています。本誌が、読者の皆さまにとって自組織のリスクを見つめ直し、次の一手を考えるための一助となれば幸いです。

CONTENTS

※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

巻頭企画

座談会
AIを生み出した〝人〟は AIを使いこなす〝人〟になる
～上野 宣氏を迎えてAIの今とこれからを語る～

SQAT® Security Report 編集部

本稿では、長年脆弱性診断に携わり、セキュリティ人材の育成や情報配信、提言活動における中心的な役割を果たされてきた上野 宣氏を招き、AIをとりまく現状と展望について弊社社員とさまざまな角度から語り合った座談会の模様をお届けする。
（2026年1月下旬　オンライン取材）

【座談会メンバー】
株式会社トライコーダ　代表取締役
兼　株式会社ブロードバンドセキュリティ　社外取締役　上野 宣

株式会社ブロードバンドセキュリティ
セキュリティサービス本部　神保 冬和子

情報セキュリティプロフェッショナルサービス本部
コンサルティング事業戦略部　コンサルティング事業戦略課　吉原 百里可

マネジメントサービス本部
セキュリティオペレーション2部　クラウドソリューション課　渡邊 寛昭

＜上野 宣氏プロフィール＞
奈良先端科学技術大学院大学で山口英教授のもと情報セキュリティを専攻、2006年にサイバーセキュリティ専門会社の株式会社トライコーダを設立。

●主な兼職
・OWASP Japan 代表
・GMO Flatt Security 株式会社 社外取締役
・グローバルセキュリティエキスパート株式会社 社外取締役
・株式会社ブロードバンドセキュリティ 社外取締役
・株式会社TRUSTDOCK 社外監査役
・情報処理安全確保支援士 集合講習講師、カリキュラム検討委員会
・一般社団法人セキュリティ・キャンプ協議会 理事
・情報セキュリティ専門誌 ScanNetSecurity 編集長
・Hardening Project 実行委員
・JNSA ISOG-J セキュリティオペレーションガイドラインWG（WG1）サブリーダー
・SECCON 実行委員
・NICT 実戦的サイバー防御演習 CYDER 推進委員
・一般社団法人 ITキャリア推進協会（JAIC）アドバイザリーボードメンバー
・情報経営イノベーション専門職大学（iU）客員教員

●主な受賞歴
・第16回「情報セキュリティ文化賞」受賞
・第11回　ISC2「アジア・パシフィック情報セキュリティ・リーダーシップ・アチーブメント（ISLA）」受賞
・2025年　総務省「サイバーセキュリティに関する総務大臣奨励賞」受賞（Hardening Project）

●主な著書
・セキュリティ1年生
・セキュリティエンジニアの知識地図（監修・共著）
・Webセキュリティ担当者のための脆弱性診断スタートガイド – 上野宣が教える情報漏えいを防ぐ技術
・HTTPの教科書
・めんどうくさいWebセキュリティ
・今夜わかるシリーズ（TCP/IP, HTTP, メール）
他多数

■座談会参加の弊社社員自己紹介など

神保：上野様は弊社の社外取締役でいらっしゃるので、弊社内の組織はご存知かと思うのですけれども、まずは我々座談会出席者3名が主に何を担当しているのか等お話をします。渡邊さん、吉原さん、まずは担当業務についてお話しいただきたいです。また、本日のトークテーマはAI（用語解説1）についてですので、ご自身のAI関連の業務にも触れていただければと思います。
では、渡邊さんからお願いします。

渡邊：マネジメントサービス本部（以降MS本部）の渡邊寛昭と申します。私は、MSS（マネージドセキュリティサービス）をSOC（Security Operations Center）機能を含めてお客様に提供する業務を担当しています。サービス企画、開発などがメインです。

社内のAI推進のプロジェクトチームにも参加しており、参加することになった経緯としましては、AIを個人的に使用していたことからAI関連の業務に携わってみないか、とお誘いがあった次第です。このプロジェクトに参加していることから、この座談会にも参加する運びとなりました。

私の部門を一言で表現するなら、セキュリティを24時間監視対応する集団という感じですかね。日々PCに向かってセキュリティ監視をしているようなイメージです。セキュリティの人材不足などと叫ばれていますが、私の部門も例外ではありません。なんだかんだいっても基本的にSOCは労働集約型のビジネスですから、特に人材不足についての課題があります。人材不足の解決策のうちにAIも挙がっていまして、動いているというところになります。中長期的には未定ですが、まずは人を支援する位置づけでAIを利用しようということを考えています。

吉原：情報セキュリティプロフェッショナルサービス本部（以降：PS本部）の吉原　百里可です。私たちPS本部では情報セキュリティのコンサルティングサービスを提供しておりまして、リスクの可視化から、課題の抽出、解決などを目的としたセキュリティ対策の支援をしています。

AI関連のサービスメニューとしては、AIサービス提供者および利用者向けのAI事業者ガイドラインをベースにしたガイドライン整備支援ですとか、AIサービス利用者向けの教育提供などをしております。

お客様からの情報セキュリティ対策推進に関するご相談に寄り添い、ご助言を提供するアドバイザリーサービスを提供しているのですが、最近はAIに関する相談を数多く受けています。例を挙げますと、AIサービスの利用に関する社内規定ですとか申請プロセスの整備について、他にはガイドライン策定に関するご相談を受けることもあります。

お客様からAI利用に関する実務的なご相談を受けることもあります。AIサービスのAPI（用語解説2）連携の設定に関するご相談ですとか、あとは生成AI（用語解説3）による著作権侵害の対策についてもご相談を受けた事例があります。

私たち自身も生成AIを使っています。コンサルタントのアシスタントみたいな感じで、日々利用しています。実は、本日の座談会へ参加するにあたって複数の資料からトピックに使えそうな統計データを抽出したのですが、その作業にも生成AIを利用しました。

私はサービスの企画開発ですとか、サービスの平準化について主に対応しております。サービスデリバリーのほうに参画することもあり、現場での対応をサービスに反映させて改善する活動にも取り組んでいます。また、AIを活用したサービスの提供にも積極的に取り組んでいます。

リリース前なので詳しくは申し上げられませんが、現場のセキュリティ対応力強化を支援するツールの開発を進めています。

神保：神保 冬和子と申します。脆弱性診断業務とフォレンジック業務を行っているセキュリティサービス本部（以降：SS本部）に所属しております。脆弱性診断業務に関連する業務のうち、新しいサービス開発に向けたPoC（Proof of Concept）や調整、SS本部内では引き取り手のない業務の引き受けを主に担当しています。

渡邊と同じような経緯で、現状の業務をAIで効率化を図ったり、AIを駆使した新しいサービスの企画をしたりするプロジェクトに参加しています。先ほど渡邊も申し上げましたが、労働集約型になっている業務は、今の工程が人の手でやる前提で作られているので、定型的なプロンプトで固められるような内容にするというのが前提としても、どのように自動化するかといった見極めが難しいですよね。また、新規のサービス企画をする際に悩ましい点でいうと、特に現状の生成AIの情報の精度が100%ではない点でしょうか。

最近は「AIのバブル」などといわれていますけれども、今私たちが申し上げた「AI」にはさまざまなものがあって、例えば、自動車関連の画像認識の技術もAIが絡んでいますし、身近なものだとメールのスパム判定などに使われるものも、AIの技術のひとつの応用ですよね。セキュリティ面での注意点や今後AIはどういう方向に進んでいくのかなど、上野様からお伺いしたいです。

■セキュリティやAIエージェントの話題など

上野：セキュリティ面での注意点については、「OWASP Top 10 for Large Language Model Applications」（以降：Large Language ModelをLLMと表記）（用語解説4）（*1）などが参考になると思います。プロンプトインジェクション（用語解説5）によって機密情報が漏洩する可能性がある、などが例に挙げられます。

今後のAIの動向については、最近（座談会は2026年1月下旬実施）でいうと、クロードボット（Claudebot）（*2）というエージェント型のAI（用語解説6）の話題が気になったのですが、エージェント型のAIが普及していった時にさまざまなセキュリティの問題が出てくることが予想できます。今後もAIの発展に付随して、問題も尽きることはないのかなと思います。
エージェント型のAIについて少々お話しますと、端末にインストールして、自律して動くことを謳っていますけれども、権限管理が非常に難しいですよね。それが特にビジネスシーンで浸透していった場合、自分が使っているAIエージェント（用語解説6）が持っている権限であるとか、ある会社のシステムのAIの権限であるとか、人ではないものが権限持って自律して動く、というようなことですので。

そこでセキュリティの問題や事件が起きることが予想されます。プロンプトインジェクションなどのLLM特有の問題も大きな問題になるのではないかと、セキュリティエンジニアとしての危惧がありますね。

とはいえ、我々はAIによる発展を受け入れるべきです。ただし問題点も認識するべきであるということです。セキュリティ専門家としては、ちゃんと警鐘を鳴らしておいたほうがいいなと思っています。

神保：デジタル化のそもそもの課題のところで、NHI（用語解説7）の管理…まあ、APIの制御などのセキュリティの問題が解決されないうちに、AIエージェントなどが出てきてしまいましたよね。

上野：自律型のAIといっても、何かと連携して使うはずなので、詰まるところはアクセス制御などでよくいわれる、「最小権限の原則」（用語解説8）がいかに守られるかというようなところが肝要になってくると思うのです。

しかし、個人で使うものって、ユーザが最小権限の原則を守らないような気がします。適当にインストールして、全権限を与えて何でもさせる。そうなると、事故が起こる可能性も高そうだなと思いますね。

神保：事故が起こってから大慌て、といった感じで進んでいくのですかねえ…。

上野：まだ企業や組織でAIエージェントが広く活用されているという話はそこまでは聞きませんが、今後は企業や組織のAIエージェントの導入は進んでいくのかなと思います。RPA（用語解説9）の代わりに広まってくるのではないかなと。まあ、既に一部のRPAには、多分AIが入っていると思いますけどね。

神保：RPAの中でもAIを許容しやすいというか、制御しやすいものとしづらいものがあるのかなと思うのですよね。限定的な機能のためのAIエージェントであれば、それに必要最小限の権限を設定するのは難しくないですけれども、汎用性が高くなると権限もいろいろなところに及ぶと思うので、判断がつかなくなって設定するのが困難になりそうかなと。

上野：おそらく、判断がつかない場合は全権限をつけてしま