AI時代の防衛戦略：日本のICTを守る最新サイバーセキュリティ

テクノロジーの進化が加速する中、次世代の情報通信技術（ICT）を守るうえで、サイバーセキュリティは不可欠となってきている。

AI（人工知能）、5G、IoTといった新興技術は、サイバーセキュリティの在り方を大きく変えつつある。これらの技術は新たな可能性を広げる一方で、困難な課題ももたらしている。なかでもAIは「諸刃の剣」だ。脅威の自動検知、大規模データの分析、脆弱性の予測といった面で防御を強化する一方で、サイバー犯罪者もAIを利用し、ディープフェイクや進化型マルウェアなど、より巧妙な攻撃を仕掛けてきている。また、サイバーセキュリティへのAI導入には、敵対的AI、AIモデルに内在するバイアス、規制対応といった新たな課題もつきまとう。

日本では、5Gの急速な展開、製造業におけるIoTの活用拡大、企業システムへのAI導入の進行により、技術革新と同時に脅威にさらされる状況も拡大している。JPCERTの2025年第1四半期レポートによると、確認されたサイバーインシデントのうち87%（6,081件中5,267件）がフィッシングによるもので、フィッシングリンクのクリック数は前年比で2倍に増加している。こうした状況は、AIを活用した防御策の早急な導入が求められていることを物語っている。

革新の時代におけるサイバーセキュリティの課題

2025年以降、サイバーセキュリティの状況は急速に変化しており、技術革新や攻撃手法の多様化により、新たな脅威や脆弱性が次々と現れている。

以下は、次世代ICTにおける主要な新興脅威の一部である：

AIによる脅威

サイバー犯罪者はAIを武器として活用し、標的型フィッシング、ポリモーフィックマルウェア、ディープフェイク詐欺といった極めて高度な攻撃を仕掛けている。

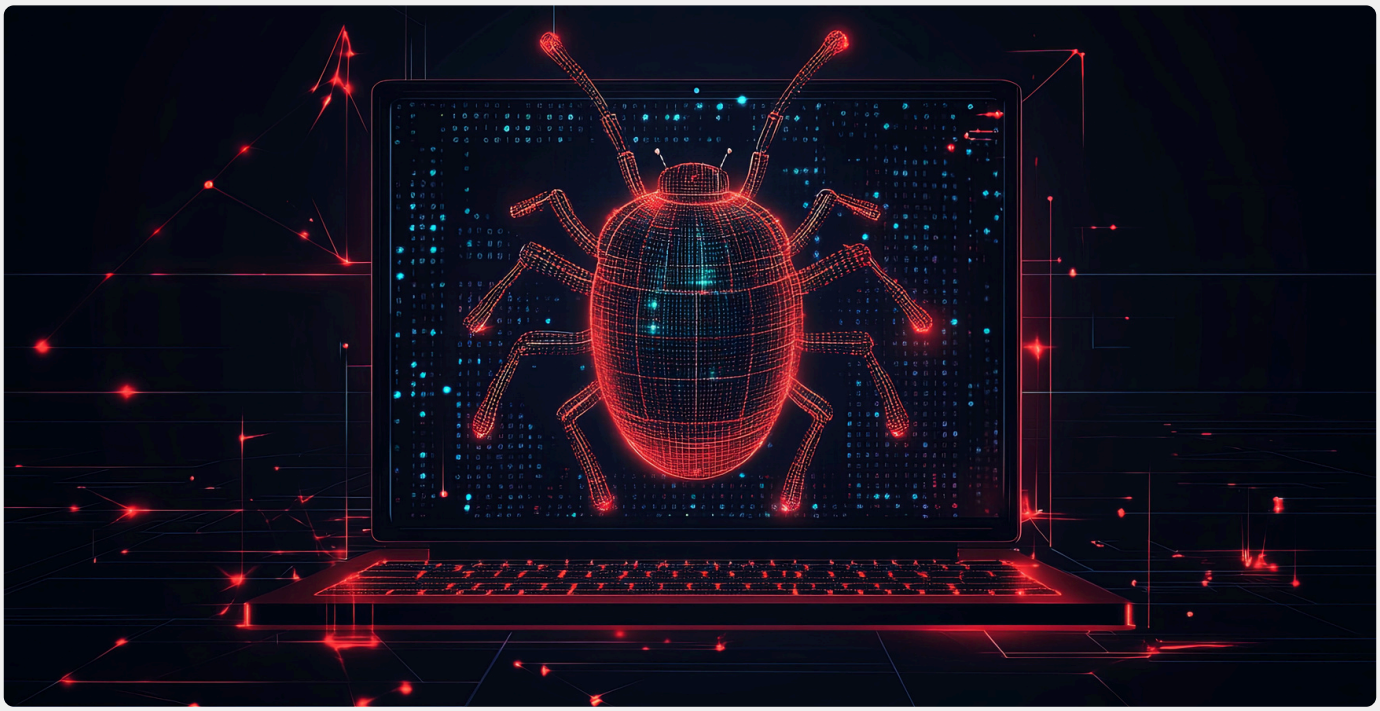
特にChatGPTが2022年末に一般公開されて以降、生成AIの影響でフィッシング攻撃は4,151%という驚異的な増加を記録している。

フィッシングキャンペーン

AIは、巧妙かつ個別性の高いフィッシングメールを自動生成できるため、従来よりも検知が難しくなっている。日本国内では、フィッシングを経由して侵入するインフォスティーラー型マルウェアの検出数が2024年に84%増加、さらに2025年初頭には週単位で180%の増加が報告されている。

ポリモーフィックマルウェア

AIを活用したマルウェアは、自らのコードを変化させることで、従来型のセキュリティ対策をすり抜けようとする。



ディープフェイク詐欺

AIは、実在の人物や経営幹部になりすますリアルなディープフェイクを生成できるため、詐欺行為につながる可能性がある。

サプライチェーン攻撃

サイバー犯罪者は、第三者のベンダーやサプライヤーを標的とし、それらの外部組織に対して企業が与えている信頼やアクセス権を悪用して、大企業への侵入を図っている。

侵害されたベンダー

攻撃者は、第三者製のソフトウェアやハードウェアに存在する脆弱性を突くことで、機密性の高いシステムへのアクセスを得ている。

ソフトウェア部品表（SBOM）

組織は、依存関係に含まれる脆弱性を検出するために、自社で使用するソフトウェアの構成要素を追跡・検証する必要がある。

ランサムウェアの進化

ランサムウェア攻撃はますます高度化しており、暗号化、データの窃取や恐喝といった手法が組み合わされている。

二重恐喝（ダブル・エクストーション）

攻撃者はデータを暗号化したうえで、盗んだ情報を公開すると脅し、身代金の支払いを強要する。

三重恐喝（トリプル・エクストーション）

暗号化と情報公開の脅迫に加え、身代金が支払われない場合にはDDoS攻撃を仕掛けることもある。

2025年初頭に施行された能動的サイバー防御（ACD）法は、重要インフラ事業者に対しランサムウェアのインシデント報告を新たに義務付けるとともに、大規模攻撃を封じ込めるために当局が入出力トラフィックを積極的に監視できるようにしている。

クラウドセキュリティの課題

クラウドサービスの利用は拡大を続けているが、クラウド環境には設定ミスやデータ侵害、不正アクセスなど特有のセキュリティ課題が存在する。

設定ミス

正しく構成されていないクラウド設定は、機密データを攻撃者にさらす可能性がある。

APIの脆弱性

APIはクラウドセキュリティにおける最も弱い部分であることが多く、攻撃者の標的になりやすい。

2025年には、日本企業の76%が信頼性のあるクラウド基盤を悪用したマルウェア活動について毎月報告しており、APIの監視とセキュアな構成は国家的にも最優先課題となっている。

インサイダー脅威（内部脅威）

従業員、契約社員、パートナーなど、機密情報へのアクセス権を持つ人々は、その権限を不正に利用したり、ソーシャルエンジニアリング攻撃の被害者となったりすることで、リスク要因となり得る。

偶発的な情報漏えい

従業員が意図せずChatGPTのようなAIプラットフォームに機密情報を共有してしまい、データ漏えいにつながる可能性がある。

行動分析

ユーザーの行動を監視するツールは、内部脅威を示す可能性のある不審な活動を検知するのに役立つ。

個人情報保護委員会（PPC）は、現在、報告された漏えい事案の四半期ごとの要約を公表しており、2024年のインシデントの30.2%が不正アクセスによるものであり、内部者の不適切な取扱いが主要な要因として指摘されている。

量子コンピューティングの脅威

量子コンピューティングは、従来の暗号化方式を破る可能性を持っており、現在の暗号技術に対して深刻な脅威となっている。

将来への備え

組織は、量子コンピューティングの将来的な影響に備えるため、耐量子暗号ソリューションの検討を進める必要がある。

エッジデバイスの脆弱性

IoTデバイスやリモートワーク用ハードウェアの普及は、侵入や悪用のリスクが増加している領域を生み出しており、ゼロデイ脆弱性の増加も見られる。

IoTセキュリティ

IoTデバイスは一般にセキュリティが弱く、監視も難しいため、攻撃者にとって魅力的な標的となっている。

ネットワークセグメンテーション（ネットワーク分離）

IoTネットワークを重要なITインフラから分離することで、セキュリティリスクを軽減できる。

日本においては、製造業やスマートシティにおけるIoT展開は、今や主要な攻撃対象となっており、JPCERTは重要インフラに関連する産業用IoTデバイスへの攻撃が急増していることを確認している。

規制の断片化

世界各地でサイバー関連規制が乱立することで、複数の地域で事業を展開する組織にとっては複雑性が増している。

コンプライアンス上の課題

断片化した規制へのコンプライアンスを維持することは、組織にとって困難であり、法的な影響を招く可能性がある。

統一基準

国境を越えるデータフローに対応するため、世界的に統一されたデータ保護基準を求める声が高まっている。

ACD法およびPPCによる改正個人情報保護法（APPI）のより厳格な執行により、迅速な漏えい報告と透明性の向上が新たに求められており、EUのGDPR基準と部分的に整合している。

ソーシャルメディアの悪用

ソーシャルメディアと生成AIは、標的型詐欺やなりすましといった高度な攻撃を可能にしている。

AI生成コンテンツ

攻撃者はAIを利用して、詐欺やなりすましに使える説得力のあるコンテンツを作成できる。

ボットとディープフェイク

AI駆動型のボットやディープフェイクは、実際のやり取りと偽のやり取りを区別することを難しくしている。

サイバー人材のスキルギャップ

サイバーセキュリティ業界は高度なスキルを持つ専門人材の深刻な不足に直面しており、そのため高度なセキュリティソリューションの導入や運用が難しくなっている。

2025年時点で日本では約11万人のサイバーセキュリティ人材が不足しており、政府はAIセキュリティトレーニングや官民連携のインターンシッププログラムに多大な投資を行っている。

しかし、このギャップを埋めるには政府の取り組みだけでは不十分であり、専門家が高度なスキルを習得するための実践的な道筋が求められる。

PECBが提供する認証プログラムは、日本の労働力が新たなサイバー脅威に対応し、今後10年にわたり国家のレジリエンスを強化することに貢献している。