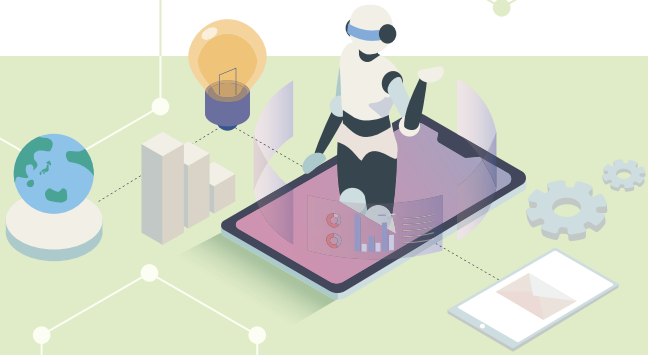
注目テクノロジー⑨

未来予想図ダイジェスト

サイバーセキュリティー

国家防衛の問題と捉え 対処すべき時代へ！

元陸上自衛隊通信保全監査隊長、日立製作所顧問
村田和美



新たな脅威も発生

サイバーセキュリティーとはコンピューターで稼働するデバイスやシステム、ネットワークなどいわゆるサイバーと呼ばれるシステムが障害や攻撃により不具合になること、データ窃取やシステムダウンなどの犯罪行為から個人、組織、国家、そして国際社会を守ることである。

そのシステムの脅威には、愉快犯によるハッキング攻撃、企業や組織の機密データの窃取、身代金目的のランサムウエア攻撃、電子金融資産の横取りなどがある。加えて新たな脅威となっているのが、国の行政・経済ネットワークや電力網、交通網など重要インフラに障害を加え、虚偽の情報を流すことにより他国の行政・経済・外交などを混乱させる行為だ。国の政情不安を煽り、侵攻の足掛かりにするなど「国家が支援するサイバー攻撃」も顕著になっている。

注目される5つの商品トレンド

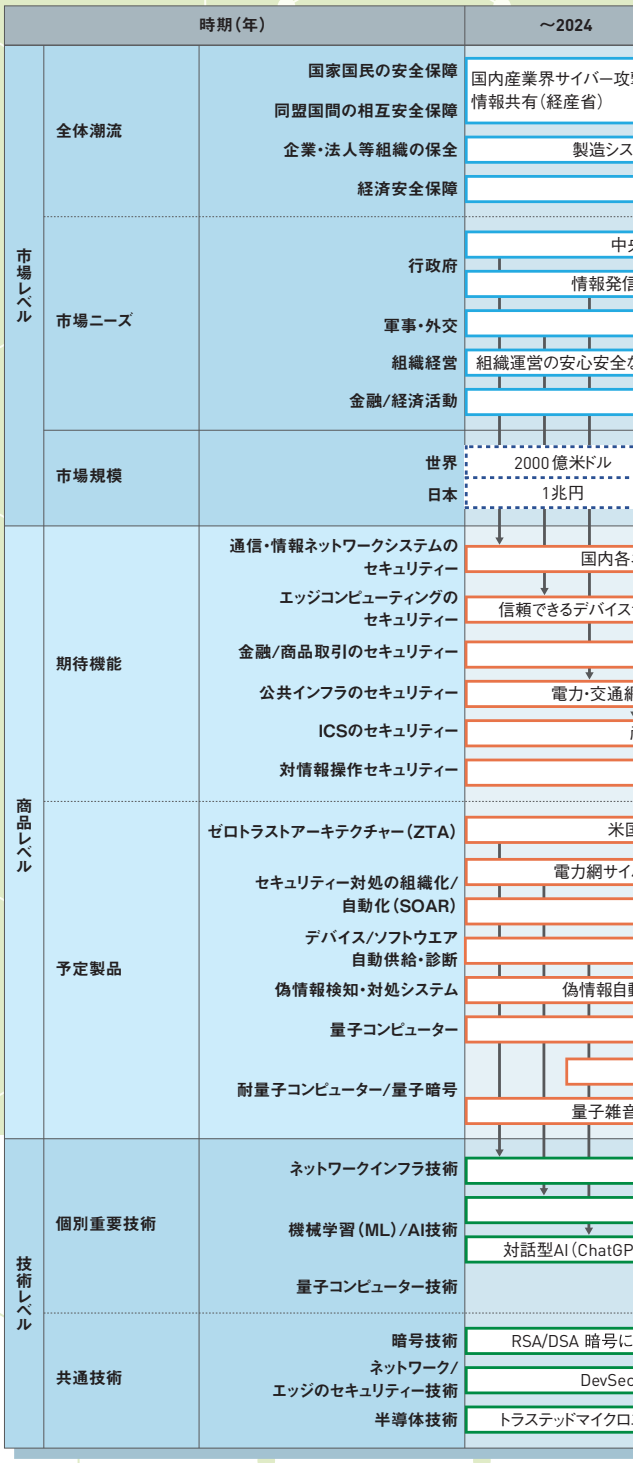
サイバーセキュリティーの「10年後の目標」を「自由で開かれた資本主義世界における安心安全な情報化社会の実現」と想定した場合、どんな商品開発が求められるのか、ポイントを見ていこう。

1つ目は「通信・情報ネットワークのセキュリティー」。この分野ではデータを分散保管するクラウド化が進む一方、そのデータの機密性を確保するため、ゼロトラストネットワークや量子コンピューターネットワークの商品化が望まれる。

2つ目は、利用者のコンピューターとIoT機器など「エッジコンピューティングのセキュリティー」。デバイスを構成する半導体などの信頼できるサプライチェーンの構築、脆弱性検出に伴うソフトウエアのアップデートを自動的に検証/修復する商品が望まれる。

3つ目は「電子マネー/商取引のセキュリティー」。量子コンピューターにより現状の公開鍵暗号などが解読される脅威もある。それに対抗できる解読・盗聴不可能な暗号商品に期待が寄せられる。

この他、4つ目の「公共インフラ・製造工場などICS（産業用制御システム）のセキュリティー」や、5つ目「対情報操作のセキュリティー」も商品の開発・進化が不可欠となる分野だ。後者では、偽情報を迅速に検知し、WEB、SNSなどの情報の真偽の判定（ファクトチェック）と対処ができる商品に期待が寄せられる。



SUMMARY サマリー

商品トレンド

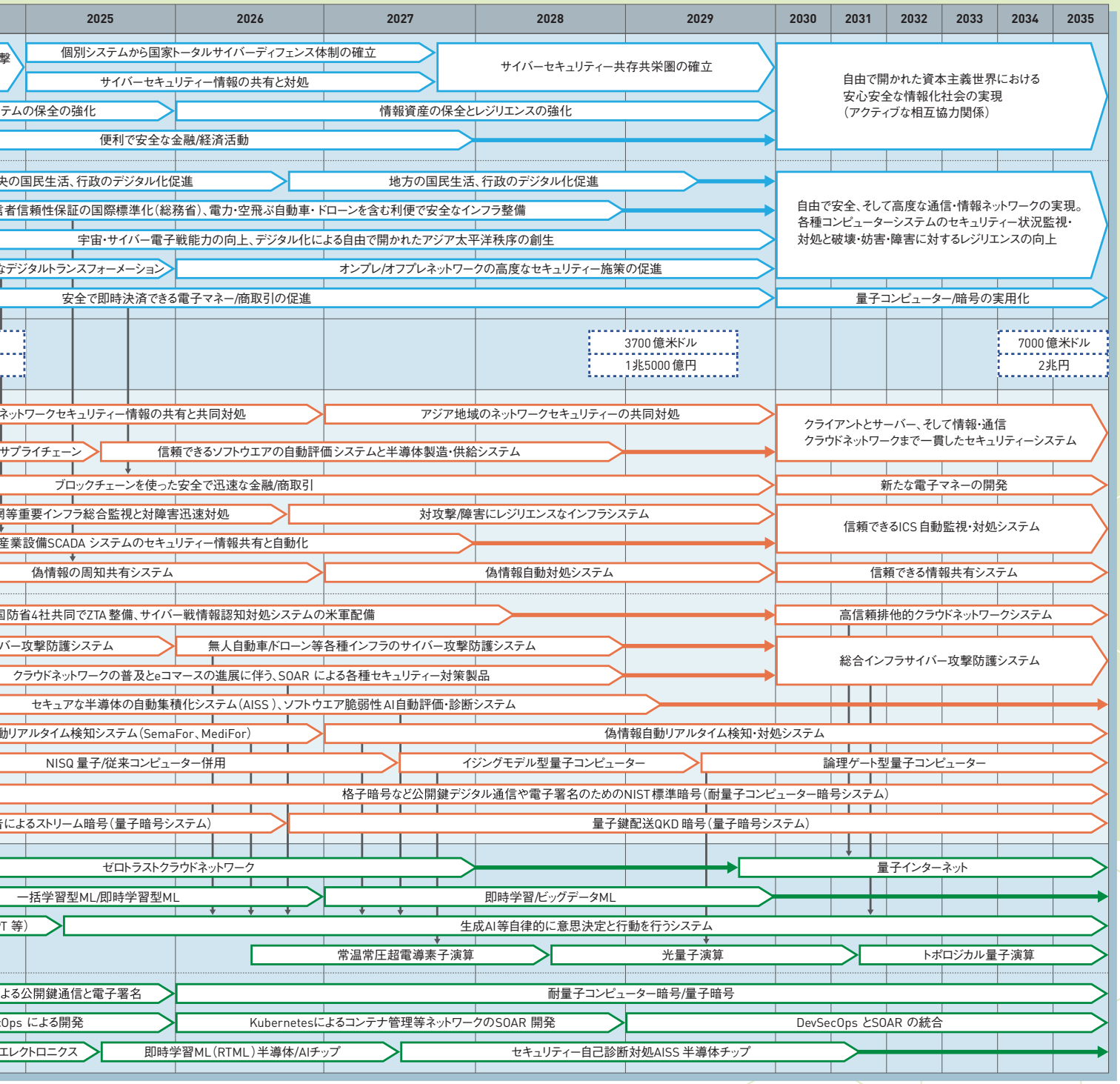
1 デジタル化の進展に伴い、情報ネットワークなどコンピューターで制御するシステムの障害や破壊が社会に重要な影響を及ぼす

2 信頼できる情報ネットワーク、エッジコンピューティング、デバイスなどのセキュリティー自動監視、対処の製品が普及する

技術トレンド

1 クラウドネットワーキング、生成AI、量子コンピューターなどの個別重要技術が進化する

2 組織/国家/利害共有国間で情報発信者の信頼性保証、サイバー攻撃情報の共有と共同対処に向けてのシステム構築が進む



（出典）『テクノロジー・ロードマップ2025-2034〈全産業編〉』（日経BP社）の一部を抜粋・再編集し当社作成

※本コラムは日経BP社の協力のもと、著者の見解をもとに作成しています。将来の予測に関しては当社の公式見解と異なる場合があります。