第194回

情報セキュリティポリシーとネットワークモデル

立命館大学情報理工学部教授　上原哲太郎

情報セキュリティポリシーとは

平成13年3月に策定された総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」（以下ガイドライン）は、情報セキュリティポリシー（以下ポリシー）を「組織内の情報セキュリティを確保するための方針、体制、対策等を包括的に定めた文書」と定義している。このガイドライン策定以来、各自治体はそれぞれの責任で自らのポリシーを定めることになった。特に平成14年に稼働を開始した住民基本台帳ネットワーク（以下住基ネット）への接続に当たっては情報セキュリティの確保が強く求められたため、比較的短期間でほとんどの自治体においてポリシーの策定が進んだ。

ガイドラインはその後もサイバーセキュリティの情勢変化や、ガイドラインの基となっている「政府機関等のサイバーセキュリティ対策のための統一基準群」の改定に合わせ毎年のように更新されており、各自治体も常に最新ガイドラインへの対応が求められている。その一方で、ポリシーはあくまでも自治体が自らの意思で定めるものであって、ガイドラインは地方自治法上の技術的助言とされてきた。しかし令和6年成立、本年4月に施行された改正地方自治法においては「地方公共団体は、サイバーセキュリティの確保の方針を定め、必要な措置を講じることとする。総務大臣は、当該方針の策定等について指針を示すこととする。」とされた（第二百四十四条の六）。この「方針」がまさにポリシーであり、以来その策定は自治体にとって法的義務となった。とはいえ、法施行に先行して総務大臣が示した指針は、従来のガイドライン中からポリシーの基本的事項を切り出したものとなり、新しいガイドラインはそれらを除く具体的なポリシー策定に資する例文などとなった。よって従来ガイドラインに沿ってポリシーを策定・運用してきた自治体にとっては、地方自治法改正に当たり特に新たな負担が生じることはなかった。しかし今後は、ガイドライン改定への追従が法的義務となっていることは注意を要する。

自治体情報システム強靱化と三層分離

ポリシーは本来マネジメントのための文書であるので、ガイドラインも特定のセキュリティ対策技術の導入を義務付けたりするものではない。しかし実際のガイドラインには具体的な対策技術が例示され、自治体への導入を強く促すものとなっている。特にその傾向が強まったきっかけは平成27年5月に発覚した日本年金機構に対するサイバー攻撃である。この攻撃者は日本年金機構以外の多数の組織に同様に攻撃を行っていたが、その中にある中規模自治体が含まれていた。折しも、同年10月には全住民に対する個人番号（マイナンバー）の付番が開始され、各基礎自治体の住基システムとマイナンバーコアシステムの連携が始まる時期だったため、この事件は自治体情報システムに対する信頼を揺るがしかねないものとなり、早急に再発防止策が必要とされた。

この事件を受け、総務省内に専門家による

自治体情報セキュリティ対策検討チームが組織され、自治体を高度なサイバー攻撃から守るための抜本的対策が検討された。高度な攻撃に対しマルウェア対策ソフトウェアの効果は限定的であるが、攻撃を受けた際にマルウェアが行う通信はある程度検出可能である。特に後者は、日本年金機構への攻撃に使われたマルウェアによる通信が、セキュリティ監視を行うGSOCによって検出された経緯から裏付けられている。そこで検討チームが打ち出したのが「自治体情報システム強靱性向上モデル」、いわゆる三層分離モデルである。

現在の自治体は、インターネット、総合行政ネットワーク（LG-WAN）、住基ネットの3種類の通信回線を介して外部接続されている。これらの3種類の通信回線に併せて自治体内のネットワーク（LAN）を3分割した上で相互の通信を制限し、特にインターネット接続LANと他のLANを完全に分離するのが三層分離モデルである。攻撃者は多くの場合、マルウェアを用いてインターネット側から自治体内のシステムを遠隔操作しようとする。よってマルウェアが侵入しても、インターネットとの接続を分離してしまえば、重要な情報を保持する住基ネットやLG-WAN接続システムは遠隔操作されず情報の窃取もできなくなる。さらに、どうしてもインターネット経由でLG-WAN接続LAN側に送られてくるファイル中からマルウェアが潜み得る領域を徹底的に除去する「無害化」と呼ばれる処理をする技術も導入された。加えて、都道府県単位でインターネット回線を集約し、その集約点に各自治体のインターネット向けサーバを移設可能な自治体情報セキュリティクラウドを構築すると共に、集約した通信路をGSOCと同様の仕組み（SOC）で監視する技術も導入された。この三層分離の効果は絶大であり、導入以降、この対策下にある自治体情報システムでは重大事故は現在まで発生していない。

ゼロトラストへの対応

三層分離モデルが自治体情報システムへのサイバー攻撃リスク低減に大いに貢献した一方で、多くの職員にとってインターネット利用は限定され、生成AIなどのクラウドサービスとの連携も困難になった。そこで、マルウェア対策を強化した上で、職員が通常業務を行う端末をLG-WAN接続LANからインターネット接続LANに移すことが考えられた。このようなネットワークモデルをガイドラインではβモデルと呼び、従来のようにLG-WAN接続端末で業務を行うモデルをαモデルと呼んでいる。インターネット接続端末は高度なセキュリティ対策を導入してもマルウェア感染するリスクが完全には排除できない。このような環境では同一LAN内の他の端末やシステムも信用できないという意味で、ゼロトラストアーキテクチャと呼ばれている。

βモデルへの移行に伴いLANをゼロトラスト化するとEDRなどの技術で端末の常時監視が必要になり、コストは必然的に上昇する。そこで、αモデルの安全性という利点を保ったまま、LG-WAN接続端末であっても安全性が確認されたクラウドサービスのみ利用可能にするネットワークモデルが令和6年にガイドラインに付け加えられた。これはα´（ダッシュ）モデルと呼ばれており、ローカルブレイクアウトやCASBと呼ばれる技術を用いて実現される。自治体の規模にもよるが、α´モデルはクラウド利用の利点を享受しつつ、コストやセキュリティリスクを比較的低く抑えられる。

ネットワークモデルをαモデルにとどめるかβモデルに移行するかは各自治体の判断である。クラウド活用の圧力が高まる中、自治体にもβモデルを求める声が少なくないと思われるが、各自治体においては情報システム運用に割けるリソースを勘案した上での慎重な移行可否判断が求められる。

筆者プロフィール

上原哲太郎（うえはら てつたろう）

京都大学博士（工学）。1995年京都大学大学院工学研究科博士後期課程研究指導認定退学。京都大学大学院工学研究科助手、和歌山大学システム工学部講師、京都大学大学院工学研究科助教授、京都大学学術情報メディアセンター准教授を経て、2011年総務省技官。通信規格と情報セキュリティ施策に従事。2013年より現職。総務省やデジタル庁でセキュリティ確保に関わる委員会の委員を務める。内閣府公文書管理委員会委員。暗号技術検討会（CRYPTREC）委員。NPO情報セキュリティ研究所代表理事、NPOデジタル・フォレンジック研究会会長、（一財）情報法制研究所理事、京都府警察サイバーセキュリティ戦略アドバイザー、和歌山県警察サイバー犯罪対策アドバイザー、滋賀県警察サイバーセキュリティ対策委員会アドバイザー、芦屋市CIO補佐官。