「2,6.4 アクセス制御とファイアウォール」に関するコラム
― ゼロトラストネットワーク ―

テキストの「2,6.4 アクセス制御とファイアウォール」では，セキュリティ上の脅威は組織外にあり，外部からのアクセスを制限することで，安全を守ることができるとの考え方で説明されている（これを境界防御(perimeter)モデルという）．しかし，利用環境が大きく変わってきており，内と外とを分けるとう考え方だけでは，安全が守れなくなっている．

たとえば，クラウド環境の利用が進み，アクセス先が内部だけとは限らないし，在宅勤務の普及で，組織外の多様な機器から内部がアクセスされるようになってきた．さらに，電子メールや Web サイトを通して，あるいは脆弱性のある通信機器を悪用して，コンピュータウイルスを内部に送り込まれることがある．このような環境では，境界防御モデルは有効ではない．

このような多様化した環境下で安全を守るために考えられたのが，すべてのアクセスは安全でないとするゼロトラストネットワーク(Zero Trust Networks)モデルである．このモデルでは，守るべきリソースにアクセするときは必ず認証を必要とし，ユーザやデバイス情報だけでなく行動履歴などからアクセスの可否を判断する．これにより，必要最小限のアクセス権限を付与でき，信頼できないアクセス先のある環境であっても，安全に運用できる．

ただ，すべてのアクセス先を確認し，その権限を認証するためには，複雑な制御システムの構築と，絶え間のない設定の見直しが必要である．運用中も適切に制限できているかをログで確認し，問題があれば修正し続けなければならないなど，システム構築と維持運用に多大な労力が必要となる．Google 社のように大きな組織でも，ゼロトラストネットワークの完成までに，８年かかったと言われている．