

ネットワークセキュリティの最新動向

小特集編集にあたって

編集チームリーダー 中尾康二
サブリーダー 吉田裕志

近年、マルウェア感染、DDoS 攻撃、標的型攻撃等、様々な脅威により日常的に脅かされています。これらの多くの脅威の根幹的なものとして、マルウェア（不正かつ有害に動作させる意図で作成された悪意のあるソフトウェアの総称）の感染があります。マルウェアの感染方法は巧妙かつ多岐にわたっており、その感染に気付かない場合が多いのが現状です。更に、感染後の活動も多く、攻撃（DDoS や情報詐取等）と関連しており、攻撃による被害（資産に対する影響）は攻撃内容によって異なりますが、情報漏えいによる保証金や DDoS によるシステム停止起因のビジネスロスなど、被害の規模は年々増大している状況です。

これらの脅威や被害の状況をネットワークの視点で俯瞰し、それらに対する適切な対策を理解するために、本会誌では、小特集として「ネットワークセキュリティの最新動向」を企画しました。「ネットワークセキュリティ」には多くの定義や解釈が存在するため、その内容には幅がありますが、本小特集では、その定義を「通信の観点から、ネットワーク境界やノード間を流れる情報の機密性、完全性、可用性を確保すること。ネットワークそのものや接続する情報システム（ノード）の機密性、完全性、可用性を確保することも含む。」としています。したがって、エンドポイントとなる情報システム（ノード）のハードウェア、OS・ソフトウェアに直接関連するセキュリティについては、最低限の記載にとどめています。また、本小特集では、ネットワークセキュリティの技術的側面だけではなく、ネットワークセキュリティに関連する政策・法律といった制度的側面からも捉えており、幅広い視点から見たネットワークセキュリ

ティについて解説しています。

本小特集では、第1章で「ネットワークセキュリティの全体像」を理解してもらうため、本小特集の2章以降で解説しているネットワークにおける脅威、技術的な対策、標準化、及び関連する法制度について概観しています。

第2章では、「インターネットに潜む脅威」と題し、サイバー攻撃による被害がなぜ防げないのか等の視点で攻撃の実例を交えて解説しています。

第3章は3部構成となっており、「標準化動向」、「バックボーンにおける対策」、及び「企業ネットワークにおける対策」について解説しており、各部において具体的な標準成果物、各環境における脅威や対策について分かりやすく解説しています。

第4章では、「国内のネットワークセキュリティ関連の法制度」、及び「国際社会におけるネットワークセキュリティ政策の動向」について解説します。国内の法令に抵触しないセキュリティ対策実施のため、関連国内法令の整理を行うとともに、国際社会の視点から、ネットワークセキュリティに関連する各国の政策について最新動向をまとめています。

最後の第5章では、「これからのネットワークセキュリティ」と題し、今後のIoT環境を取り上げ、そこにおける脅威、セキュリティ対策を概説し、これらの事例等から今後ネットワークセキュリティ技術に求められる役割について提言しています。

以上の構成により、本小特集は、ネットワークセキュリティに関連する技術的側面、制度的側面を俯瞰していますので、ネットワークセキュリティを初めから理解したい読者、更に、最新のネットワークセキュリティの技術、制度などを体系的に整理した形で理解されたい読者にとって一助になることを期待します。なお、本小特集では、差別化が難しい「サイバーセキュリティ」に関する内容が含まれていることを御容赦頂きたい。

小特集編集チーム	中尾 康二	吉田 裕志	植松 芳彦	札幌 伸和	今村浩一郎
	小泉 健吾	高橋 清隆	瀧川 道生	豊田 雅宏	中台 光洋