標的型攻撃時代に求められる
組織のサイバーセキュリティ対策

富士通株式会社　サイバーディフェンスセンター　奥原雅之
okuhara@jp.fujitsu.com
平成 28 年 1 月 18 日

いわゆる「標的型サイバー攻撃」は 2009 年ごろから出現し、2011 年からは我が国でもこれに該当する攻撃の事例が知られるようになった。以降、標的型攻撃の脅威が衰えることはなく、今日のあらゆる組織は、例外なく標的型攻撃の危険性にさらされていることを認識する必要がある。

しかしながら、標的型攻撃に対抗できる情報セキュリティ対策を組織として確立することは必ずしも簡単なことではない。従来の情報セキュマネジメントシステム（ISMS）に代表される、セキュリティポリシーに基づく情報セキュリティ管理のフレームワークは、適切に運用しないと変化が激しい今日の脅威には十分に対抗できないこともあり得る。

富士通では、2015 年にサイバーディフェンスセンターを設立し、標的型攻撃に代表される今日のサイバーセキュリティリスクに対応するための各種セキュリティ対策活動を行っている。本講演においては、富士通社内で 15 年以上にわたって取り組んできたセキュリティ対策の実践に基づき、サイバー脅威に対抗するために組織に求められる CSIRT などの機能や、今日の組織に求められるセキュリティポリシーのあり方について論じる。