Computer Report
Vol.53　No.6　　６月号　（通巻 705 号）

はじめの言葉

■ますます利用が浸透するネットワークサービスの活用である。その一方でサービス提供業者のサイトをターゲットとする不正行為もますます猛威をふるってきているようだ。Yahoo の 2200 万件にものぼるかと言われる ID 情報流出は、明らかに単なる流出／漏洩事象ではなく犯罪事件であり、サイバーテロ行為だと言っていい。深刻なのは、流出件数の 2200 万件はほんの一部にすぎないという観測も出ていることだ。

■問題は、サイバーテロを仕掛ける側は言うに及ばず、管理責任を十分に果たせなかったサービス運営側にもある。ネットワークインフラを競うのが、情報システム産業の世界的傾向だと言ってしまえばそれまでだが、あまりにも脆弱な情報システムテクノロジーをベースにしたインフラ産業であることを、改めて痛感する。これほど危ない社会的インフラの上にあるサービスだということを、利用する側は今一度、再認識しなくてはならない。

■加えて、OS、ミドルウェアなどの中枢ソフトウェアからネットワークインフラまでの基幹部分は、ほとんどが海外勢力のコントロール下にあることも確認しておきたい。このことでの、個々人から企業等組織、さらには日本という国家全体のセキュリティ（安全性）についても、非常に危ういものがあると言える。国家として、企業等組織として、個人として、サイバーテロの脅威にどう取り組んでいくべきか。

■安倍政権による様々な取り組みのなかに、国家としての諜報活動態勢の確立を目指す考えが含まれていることが明らかになっている。ナショナルセキュリティ＝国家の安全確保のためだということのようだが、この延長線上にサイバーテロ対策も含まれていて何の不思議もない。いきなりの諜報活動という表現は、ぶっきらぼう極まりないものだが、情報収集活動の第一歩はネットワークインフラの活用にあるだけに当然過ぎる話である。

■Yahoo、Google など、ネットワーク上での情報検索／情報収集エンジンの提供企業が、その収益をバナー広告収入に依存しているという定説が支配的である。がしかし、利用者の検索行動情報そのものが特定のスポンサーに提供され、その対価が膨大な収益を構成しているというのも定説である。現政権の目指す諜報活動がどんなところから始められるかは別にして、検索エンジン提供事業者による諜報活動は、すでに定着している。

■何をもって情報提供サービスとされるのか、はたまたサイバーテロによる情報流出だとされるのか、ネットワーク利用者の側からすると、本人の意思／意図と関係なく第三者に利用者個人に関わる情報が流されてしまうことに相違はない。どちらも、大きな脅威＝リスクである。ネット上で買い物をしたところ、類似商品の案内を別の業者から受ける経験をしたという話は結構あるものだ。

■情報漏洩事件があるたびに「流出情報が悪用されたということは明らかになっていない」というフレーズが注釈される。悪用が即座に分かるようなら、悪用者は即座に検挙されることだろう。明らかにならないところで使われることを悪用というのである。便利だから、導入コストが安いからなど、安直な動機でのネットワークリソースの導入／活用は、利用者のリスク感覚をますます鈍化させていく危険性がある。（藤見）