KPMG
cutting through complexity

2015年2月

新たなITリスクに立ち向かう 連載シリーズ 第11回

サイバーセキュリティに必要な3つの変化

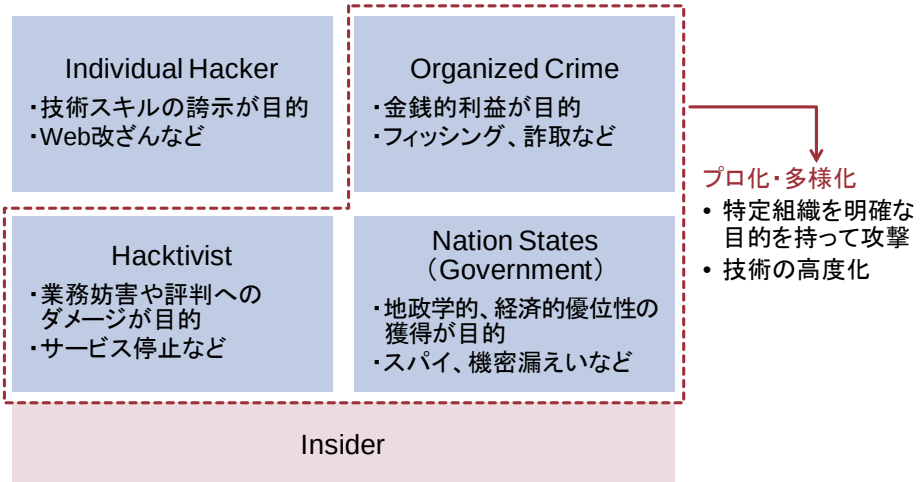
サイバーセキュリティという言葉をメディアで見かけない日はないが、一方でサイバーセキュリティという概念には確定的な定義や解釈が存在しない。サイバーセキュリティと企業がこれまで取り組んできた情報セキュリティとは一体何が違うのだろうか。

サイバーセキュリティという言葉で表現されることの多い現在の状況を的確に把握し、対応していくためには、情報セキュリティの分野で起こっている3つの変化について理解しておくことが重要である。

1. 行為者の変化

図表1は情報セキュリティを侵害する行為者を整理したものである。企業がインターネットに接続し始めた当初、セキュリティ侵害を行う行為者として最も注視されていたのは左上の「Individual Hacker」(個人で活動するハッカー)だった。いたずらあるいは腕試しや技術力の誇示を目的に、インターネット上を広くスキャンし、脆弱なサイトを見つけて攻撃を行うタイプである。その後、業務のシステム化が進展し、世の中が個人情報や機密情報には金銭的な価値があると気付き始めると、脅威の対象は図中1番下の「Insider」(内部関係者)に移る。この傾向は現在でも続いており、「Insider」が行為者であるセキュリティ事故は今も数多く見かける。さらに、ここ数年で一気にクローズアップされてきた行為者が、「Hacktivist」(ネット活動家)「Organized Crime」(犯罪組織)「Nation States」(民族・国家)の3つに分類される高度化、多様化した外部の第三者である。「Individual Hacker」との違いは、それぞれ目的と攻撃対象が明確で、よりプロ化、多様化していることにある。

【図表1】情報セキュリティを侵害する行為者



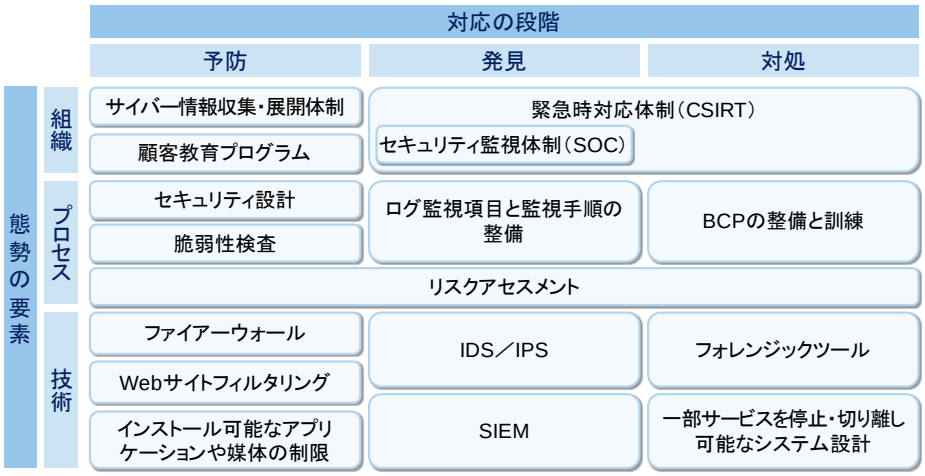
2. 攻撃手法の変化

2つ目の変化は攻撃手法の変化である。サイバーセキュリティという語感から、ともすればインターネット経由のIPネットワークばかりを想像しがちであるが、その目的を勘案すれば、これまでは聖域と考えられていた制御系システムがターゲットになる可能性も十分に考えられる。実際に制御系システムを狙ったサイバー攻撃も多数発生している（最も有名な事件はイランの核燃料施設を狙ったStuxnetであろう）。また、攻撃目的と対象が明確ということは、その攻撃対象のシステム環境に特化したオーダーメイド型の攻撃手法がとられる可能性があるということだ。ご存知のとおり、アンチウィルスソフトや侵入検知システムなど多くのセキュリティツールは、シグネチャー方式と呼ばれる既知の攻撃手法とのパターンマッチによって異常を検出する仕組みだ。オーダーメイド型の攻撃を仕掛けられると、これらのセキュリティツールが無力化されてしまう恐れがある。

3. 対応の変化

図表2は企業としてとるべきセキュリティ対策を、その対策レイヤと対応フェーズで整理したものである。これまで企業は主に予防のフェーズにコスト投下を行ってきた。しかし、前述のとおり攻撃手法が高度化、個別化の傾向にある今、100%の防御は困難であり、ある程度攻撃を受けて侵入されることを前提として物事を考えておかなければならないということが言われ始めている。今後、企業は侵入を許してもその被害が軽減される対策（例えばLANの暗号化、イントラネットのセグメント化、データベースの分散化等）、および侵入された際にはすぐに発見し対応できる対策（例えばSIEMシステムの導入、CSIRTの組成、インシデントレスポンスプランの作成等）によりコスト投下をしていくべきであり、これが3つ目の変化である。

【図表2】企業としてとるべきセキュリティ対策の対策レイヤと対応フェーズ



4. まとめ

多くの企業は2000年代初頭から常に情報セキュリティに取り組んできている。その過程において、情報セキュリティ対策の潮目が大きく変わることはこれまでにも何度かあった。そして、今また大きな潮目の変化が訪れようとしている。サイバーセキュリティとは、そんな世の中の趨勢を端的に表している言葉である。

サイバーセキュリティに対応していくためには、世の中のスタンダードやガイドラインに合わせた対策を講じているだけでは不十分である。企業によって、狙われる理由、狙われるモノ、仕掛けられる手段がそれぞれ異なるのがサイバーセキュリティの特徴の1つである。個社ごとに自社固有のリスクシナリオを作成し、自社特有の事情を反映した対応を実施していくことが、企業には求められている。

KPMGコンサルティング株式会社
パートナー　田口　篤

KPMGコンサルティング株式会社

東京本社
〒100-0004
東京都千代田区大手町1丁目9番5号
大手町フィナンシャルシティ　ノースタワー
TEL ： 03-3548-5305
FAX ： 03-3548-5306

名古屋事務所
〒451-6031
名古屋市西区牛島町6番1号　名古屋ルーセントタワー
TEL ： 052-571-5485

kpmg.com/jp/kc