**[勘違いしやすいセキュリティ](http://tech.nikkeibp.co.jp/atcl/nxt/column/18/00164/)**

**情報セキュリティとサイバーセキュリティにまつわる誤解**

[⾼橋 宏之](http://tech.nikkeibp.co.jp/search/?q=%E2%BE%BC%E6%A9%8B%E5%AE%8F%E4%B9%8B)＝デロイト トーマツ リスクサービス

[日経 xTECH](http://tech.nikkeibp.co.jp/)

この記事は日経 xTECH有料会員限定ですが、2018年3月15日5時まではどなたでもご覧いただけます。

　組織におけるセキュリティ対策への関心は急速に高まっている。セキュリティコンサルタントである筆者の元には、相談や依頼が次々と舞い込んでいる。そうした方々と話をしていて、セキュリティの考え方が誤解されていると感じる機会も増えている。

　色々な人と会話をする機会があり、勉強熱心な人ですらよく勘違いしている事項があると分かってきた。そのトップ3が（1）情報セキュリティとサイバーセキュリティの違い、（2）セキュリティとセーフティの違い、（3）セキュリティガバナンスとは何かの理解、だ。会話ですれ違いやギャップが生じ、提案活動やプロジェクト支援が進む過程で障壁となるケースもある。

　今回は、情報セキュリティとサイバーセキュリティという2つの言葉にまつわる誤解を取り上げよう。コンサルタントとして経営層やIT部門のトップと会話をしていると、次のような発言をよく耳にする。

**経営者A氏「最近サイバーセキュリティという言葉をよく聞くが、情報セキュリティ対策はこれまでも行ってきた。同じ『セキュリティ』だし、今のままで問題ないのではないか」**

　言葉の定義だけを見ると、サイバーセキュリティは情報セキュリティに内包される包含関係にある。ただ、実際に起こっている現象を見ると、サイバーセキュリティには従来の情報セキュリティの枠組みではカバーできない要素がある。情報セキュリティとサイバーセキュリティを同一と考えると、見逃してしまうポイントがあるのだ。

**言葉の定義だけを見ると包含関係**

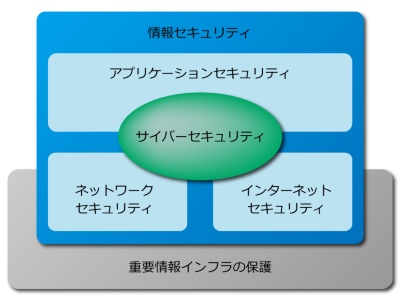
　まずは情報セキュリティとサイバーセキュリティの定義に立ち返ってみよう。

　情報セキュリティは、情報セキュリティマネジメントシステムの管理基準「JIS Q 27002（ISO/IEC 27002）」において「情報の機密性・完全性・可用性を維持すること」と定義されている。この3つの観点で被害を受けるかどうかで脅威を捉え、対策要件を検討して対策を実施する。脅威事象がITかどうかを問わず、包括的に捉える。

　機密性（confidentiality）とは、情報へのアクセスを認められた者だけがアクセスできる状態を確保すること。完全性（integrity）は情報が破壊、改ざんまたは消去されていない状態を確保すること。可用性（availability）は情報へのアクセスを認められた者が、必要時に中断することなく、情報および関連資産にアクセスできる状態を確保することだ。これらは各英単語の頭文字を取って「CIA」と呼ばれる。

　サイバーセキュリティは2014年11月に成立した「サイバーセキュリティ基本法」に定義がある。要約すると、IT（法律上の表現は「電磁的方式」）という特定の脅威の発生手法にフォーカスして、情報の機密性・完全性・可用性を維持することだ。

　両者の関係は、国際標準化機構（ISO）が発行するサイバーセキュリティのためのガイドライン「ISO/IEC 27032」が図で示している。サイバーセキュリティは情報セキュリティの一部で、情報セキュリティはほかのセキュリティを包含する概念との位置付けだ。

[](http://tech.nikkeibp.co.jp/atcl/nxt/column/18/00164/021600003/?SS=imgview&FD=2638409)

**情報セキュリティとサイバーセキュリティの関係**

ISO/IEC 27032を基に筆者作成

[画像のクリックで拡大表示]

　さて、規定やガイドラインを見ると情報セキュリティとサイバーセキュリティは包含関係だ。しかし、実務で起こっていることを見ると、「情報セキュリティはサイバーセキュリティを完全に包含する」と理解すると重大な見落としの危険性がある。「両者は共通部分も多いが、サイバーセキュリティ固有の観点も存在する」と考えたほうがいい。

#### 「被害」が従来の定義に収まらない

　なぜサイバーセキュリティは情報セキュリティに完全に包含されないのか。これを端的に示す例が、「サイバー犯罪予告」や「踏み台攻撃」といったサイバーセキュリティに特有の脅威だ。

　サイバー犯罪予告では、攻撃集団が特定の組織に対するサイバー攻撃をほのめかす書き込みをインターネット上で行う。恐喝や脅迫にまで踏み込んだ悪質な要求の場合もある。踏み台攻撃では、攻撃者がセキュリティ管理の脆弱なIT資産（PCやサーバー）をマルウエアに感染させたりして、それを経由して別のIT資産に攻撃を仕掛ける。

　情報セキュリティは情報の機密性・完全性・可用性の維持が目的だ。ところが、サイバー犯罪予告や踏み台攻撃では、これらの観点で見た被害は発生していない。サイバー犯罪予告は“兆候段階”であり、その時点では情報の機密性・完全性・可用性の侵害には至っていない。そもそもどのような被害が発生しうるのかも分からない。

　踏み台攻撃では、自社の情報資産への侵害が発生するわけではない。実際、ある企業から「セキュリティ対応で困っている」と打診を受けたことがある。その企業は機微な技術情報や顧客情報を保有しているとは思えず、会うまでは少し不思議に感じていた。話を聞いてみると、その企業のサーバーが踏み台となり、他社のサーバーを攻撃していた。その企業が実際に困っているセキュリティ対応とは、踏み台攻撃に対する他社からのクレーム対応だった。

　これらのケースは、従来型の情報セキュリティの侵害に当てはめて考えるのが難しい。従来の情報セキュリティの枠組みで対策を検討すると、サイバーセキュリティ特有の脅威の考慮漏れが起こり得る。冒頭の経営者A氏のような発言が出てくるのはそのためだ。

　ISO/IEC 27032が示す情報セキュリティとサイバーセキュリティの関係は理論としては正しい。しかし実務では、情報セキュリティとサイバーセキュリティの間で違いがあると考えるアプローチを推奨したい。

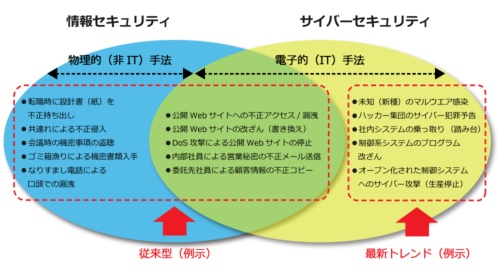
#### 両者の関係の理解しやすい見せ方

　サイバーセキュリティ特有の脅威に対応するには、新たな対策が必要になる場合もある。代表例は「SIEM」（セキュリティ情報イベント管理）や「サイバーインテリジェンス」だ。

　SIEMは複数のセキュリティ機器のログを相関的に分析したり、ユーザーID単位で一連の挙動をトレースするような高度な監視をしたりするソリューションである。従来のIDS/IPSによる個別のログ監視のみでは、近年の進化したサイバー攻撃の不審な挙動を見つけるのが難しくなっている。サイバーインテリジェンスはダークウェブ（インターネット上で一般に公開されていないアンダーグラウンドのコミュニティ空間）などでのサイバー犯罪者の動向を分析して、将来起こり得るセキュリティ被害を分析・予測する情報収集サービスだ。

　従来の情報セキュリティの枠組みだと、これらに投資する理由をうまく説明できない。ここからは情報セキュリティとサイバーセキュリティの関係と差分をシンプルに捉え、経営層や利用部門に伝える2つのテクニックを紹介しよう。いずれも実際のプロジェクトで経営層にサイバーセキュリティの必要性を訴求するために使用して、うまく伝わったという手応えを得た方法だ。

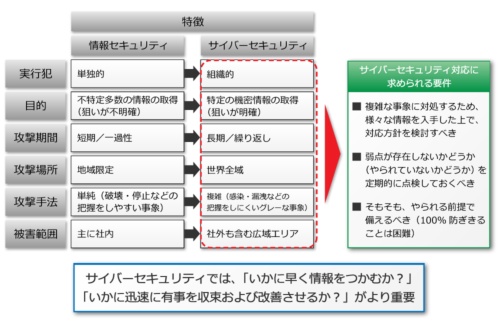
　1つめはベン図の活用だ。情報セキュリティとサイバーセキュリティが対象とする脅威の例示を用いて、共通するものと固有のものを明示する。その中で、サイバーセキュリティは最新のトレンドとして生じている脅威にフォーカスしていることを強調する。前述した通り、踏み台攻撃はサイバーセキュリティ特有の最新トレンドとして生じている脅威だ。

[](http://tech.nikkeibp.co.jp/atcl/nxt/column/18/00164/021600003/?SS=imgview&FD=3561930)

**ベン図による情報セキュリティとサイバーセキュリティの説明**

[画像のクリックで拡大表示]

　2つめは比較表の活用だ。情報セキュリティとサイバーセキュリティにおける攻撃の特性を列挙し、それぞれの違いを対比して説明する。その中で、サイバーセキュリティの対応として求められる要件を強調しておく。複雑な攻撃手法が特徴のサイバーセキュリティでは、継続的な情報の入手や定期的な脆弱性チェックなどがより重要になる。

[](http://tech.nikkeibp.co.jp/atcl/nxt/column/18/00164/021600003/?SS=imgview&FD=4485451)

**比較表による情報セキュリティとサイバーセキュリティの説明**

[画像のクリックで拡大表示]

#### 違いを理解して足りない部分の投資を判断

　サイバーセキュリティがどの程度の脅威になるのかは企業によって異なる。自社が受ける脅威の種類と大きさとの見合いで、既存の情報セキュリティの対策でカバーできるという判断もあり得る。自社に足りない部分があれば、それを見落とさずに適切な対策を実施しなければならない。

　セキュリティ対策は多額の投資が必要となる場合がある。経営層はその投資が妥当であるかどうか、適切に判断しなければならない。こうした判断を可能にするには、「情報セキュリティとサイバーセキュリティは共通する領域もあるものの、サイバーセキュリティでは固有の新たな観点が登場している」という情報を分かりやすく説明する必要がある。

　情報セキュリティとサイバーセキュリティの違いは、セキュリティの勉強している人ほど陥りやすい勘違いだ。記事の途中で触れたとおり、脅威による被害に着目すると両者は包含関係にある。規定やガイドラインの定義もそうなっている。これだけを見ると、サイバーセキュリティのための投資は不要に思えてくるほどだ。

　冒頭の経営者A氏は、以下のような認識をできていればよかった。

**経営者A氏「従来の情報セキュリティとサイバーセキュリティでは、共通する部分と違う部分があると考えている。サイバーセキュリティ固有の施策について、自社に何が足りないかを冷静に見極めたい」**

　情報セキュリティとサイバーセキュリティの関係を見誤ると、意思決定の方向性にも大きな影響を及ぼす。重大な見落としが起こる可能性もある。誤解なく理解するようにしたい。

**高橋宏之（たかはし　ひろゆき）**  
デロイト トーマツ リスクサービス　シニアマネジャー

国内SI企業で省庁関連の大規模システム開発やERP製品導入を経験後、デロイト トーマツ コンサルティングに入社し、ビジネスプロセス改善やCIO向けアドバイザリー業務に従事。2010年、デロイト トーマツ リスクサービスに転籍後は、セキュリティ全般のコンサルティング業務を担当する。近年は、自動車業界向けのセキュリティ管理のエキスパートとして、情報システム領域および自動車セキュリティ領域に関する様々な案件に関与。