アンラボ・セキュリティレター

Press Ahn

2017.2　Vol.38

2017 年のトレンドを読み解くキーワード

TREND REVIEW

2017 年のトレンドを読み解くキーワード

新年になると各業界では市場動向やトレンドレポートが発表されるが、これはセキュリティ業界も同じで脅威動向や市場の動きを調査したレポートが次々発表される。情報セキュリティの脅威は常にIT技術と歩を共にし、今年はこの傾向が一層強く現われるとされる。デジタルトランスフォーメーションが加速化する社会に突入してからAI、IoT、VRは ITトレンドにおける常連キーワードとして浮上した。デジタルトランスフォーメーションをリードする概念や主要キーワードは、今やIT業界を超えて社会全般に影響を及ぼしている。今回のプレスアンでは、今年のセキュリティトレンドを読み解くための必須用語をまとめた。

ITトレンド関連主要キーワード

■ 人工知能 (Artificial Intelligence)

人工知能とは、人の思考、学習、推論、知覚、言語理解などをコンピュータープログラムで実現した技術を指す。英語では『Artificial Intelligence』、略して「AI」という。AIは弱いAIと強いAIに区分され、弱いAIは自ら問題を認知して解決することは不可能だが、与えられた条件下で合理的な結論を導き出すことができる。強いAIは知覚力と自我を持ち、与えられた課題に対して自ら判断できる。弱いAIを実現する際に機械学習を使うとされる。深層学習(ディープラーニング)と機械学習(マシンラーニング)は混同される場合が多いが、正確に言えば機械学習のほうが上位概念である。

■ 機械学習 (Machine Learning)

機械学習は、人工知能の一分野であり、膨大なビックデーターを分析して未来を予測する技術を指す。コンピューターが与えられたデーターから意味ある情報を自動で抽出するすべての技術領域を意味する。人がいちいち基準と解答を教えなくても、数多くのデーターを通じてコンピューター自ら方法を探ることが特徴だ。データーを収集・分析して未来を予測する点ではビックデーター分析に似ているが、コンピューター自ら膨大な量のデーターを収集及び学習する点で差がある。翻訳機、ボイス認識、ポータルサイトの検索語自動入力機能などは機械学習を応用した例である。

■ 深層学習 (Deep Learning)

深層学習は、コンピューターが人のように考えて学ぶ人工神経網をベースにした機械学習技術を指す。人の頭脳が膨大なデーターの中からパターンを見つけて物事を区分する情報処理方式を模して機械を学習させる。深層学習技術の代表的なものには、Googleの「AlphGo」がある。

■ バーチャルリアリティー (Virtual reality)

あたかも現実のように見せるバーチャルリアリティ、略して「VR」と言う。仮想環境の中に入り込んでいるような感覚に加えて操作もできる。バーチャルリアリティーが初めて登場した1938年以降、何度目かのブームを繰り返していたが最近また注目を集めているのはスマートフォンの普及により、仮想現実デバイスが拡散しているところが大きい。

■ 拡張現実 (Augmented Reality)

拡張現実とは、ユーザーの目に見える現実世界に仮想の物体やイメージを重ねて見せる技術を指す。仮想現実と拡張現実を混同する場合がよくあるが、この二つはまったく異なる概念だ。VRは背景や環境すべてに『仮想のイメージ』が使用されるが、ARは現実のイメージや背景に3次元仮想イメージを重ねることで他のイメージや映像を実現する技術なのだ。拡張現実を活用した代表的なデバイスに「Google Glass」がある。このスマートグラスを一般のメガネのようにかけると、メガネを通してネット検索やカメラ機能、道案内、SNS機能を使用できる。

■ インダストリー4.0 (Industry4.0)

インダストリー4.0はドイツから始まった新たな産業システムパラダイムで、製造業にCyber Physical Systemsを融合して競争力を強化することを提唱している。これは2011年ドイツ産業博覧会(Hannover Messe 2011)で初めて登場した。伝統的な製造大国ドイツが、日本の精密ロボット技術とアメリカのインターネット/IT技術、中国の低コスト大量生産に対抗すると同時に、高コスト、高齢化、製造業の海外移転など、国家的懸案を解決する戦略としてインダストリー4.0を打ち出した。インダストリー4.0が主に生産と物流のスマート化に注目したことに比べて、第4次産業革命はこれによって引き起こる産業社会全般の変化に当たる概念といえる。

■ ビットコイン (Bitcoin)

ビットコインは、2009年に中本哲史を名乗るプログラマーが作った仮想貨幣の一種である。公開鍵の暗号方式と所有権管理のためのアルゴリズムが結合されたもので、従来の貨幣を数学的・暗号の厳密性に基づいてオンライン上に実現したものだ。ビットコインの最も革新的な点は、利用者同士のP2P(Peer to Peer、ファイル共有システム)ネットワークベースで脱中央格納の形で有効性を確認し、二重支払い問題を解決した点であった。

■ ブロックチェーン (Blockchain)

ブロックチェーンは公開鍵の暗号化をベースにしたdistributed ledger technologyの一種であり、従来の中央集中型ネットワークベースのインフラよりも強化されたセキュリティ性と、取引の透明性、コスト面における強みを持っている。ブロック(block)はビットコインに関する特定のデータを永久記録する一種のファイルであり、取引情報が記録される帳簿のようなものだ。各ブロックを以前のブロック情報も含めていて鎖(chain)のように繋げているため、ブロックチェーンと呼ばれる。

■ デブオプス (DevOps)

TTA(韓国情報通信技術協会)用語辞典によると、デブオプスは『Development』と『Operations』の合成語で、システム開発と運用を並行、協力する方式を意味する。これは適時ソフトウェア製品やサービスをリリースするため、開発と運用の各部門が有機的に相互依存することを指す。
ソフトウェア開発と運用管理の協力と統合によるビックデータービジネスが注目され、ある特定分野の優れた能力を持つ人材ではなく、統計、プログラミング、開発、オペレーションのような融合的な能力に対するニーズが高まっている。

■ バイモーダルIT (Bimodal IT)

バイモーダル(Bimodal) ITは、デブオプスとともによく登場する用語で、『未来のIT組織は二つの異なる方向性を持つ方法論を両立させる』ことを指す。第一のタイプは、安全性と効率性に焦点を当てた伝統的なITだが、第二のタイプは適期発売(Time to Market)を重視し、アプリケーションの発達周期の短縮とビジネス部門との密接な繋がりをベースにした実験的かつスピーディなITを目指す。この概念は、伝統的なIT投資と運用システムが次のステップに移る過程で、従来の方法と実験的で新しい方法の共存・混在している状態を意味する。

セキュリティトレンド関連の主要用語

■ EDR (Endpoint Detection & Response)

最近セキュリティ業界でホットな用語といえば「EDR(Endpoint Detection & Response)」がある。ガートナーはEDRを『エンドポイントレベルにおける持続的なモニタリングと対応を提供するセキュリティソリューション』と定義している。加えて、インシデント検知(Detect security incident)、エンドポイントのインシデント制御(Contain the incident at the endpoint)、インシデント調査(Investigate security incident)、感染前の状態にエンドポイントを復元(Remediate endpoint to a preinfection state)するまでの4つの機能を提供しなければならないと強調した。

■ EPP (Endpoint Protection Platform)

EPPとはPC、スマートフォン、タブレットPCなど業務環境で使用するエンドポイント向けデバイスを、多様な脅威から保護するソリューションを意味する。ガートナーは、エンタープライズEPPについて▲アンチマルウェア(Anti-malware)、▲パーソナルファイヤーフォール(Personal firewall)、▲ポート&デバイスコントロール(Port and device control)、▲脆弱性管理(Vulnerability assessment)、▲アプリケーションコントロール及びアプリケーションサンドボックス(Application control and application sandboxing)、▲EMM(Enterprise mobility management)、▲メモリー保護(Memory protection)、▲EDR(Endpoint detection and response)、▲データー保護(Data protection such as full disk and file encryption)、▲DLP(Endpoint data loss prevention)を含むべきであると定義した。

■ 脅威インテリジェンス(TI、Threat Intelligence)

ここ数年セキュリティ関連イベントにて最も多く言及される単語は「TI」といえる。TIは「脅威インテリジェンス(Threat Intelligence)」の略字で、GTI(Global Threat Intelligence)、TIP(Threat Intelligence Platform)、TISS(Threat Intelligence Security Service)などの表現も並行して多く使用されてきた。ガートナーでは『証拠をベースにした知識であり、企業ITや情報資産において脅威になりえる部分に対して実行可能なアドバイスを示す情報』と定義している。
またIDCでは『企業のインシデント履歴記録だけでなく企業コミュニティ、関連アンチウイルスや脆弱性関連情報を持ったベンダーとのコミュニティ、国家セキュリティコミュニティの情報を脅威の対応に活用すること』として「interactive Intelligence」とも表現している。

■ RaaS(Ransomware as a Service)

ランサムウェアは2017年も猛威を振るうと予想される。大規模なランサムウェア攻撃が相次いで発生しているのは、サービス型ランサムウェア(RaaS)の登場によるところが大きい。RasS（Ransomware as a service）は、ランサムウェアを作成から配布までしてくれるサービスで、すでに一つのビジネスとして成り立ち依頼を受けるページまで作ってある始末。また依頼を受けて作成したランサムウェアがどの位拡散して感染されたか現況報告までしているのだから、依頼人の信頼を得るためのアフターケアもしっかり提供しているようだ。

■ ウォータリングホール攻撃(Watering Hole Attack)

ウォータリングホール攻撃は、ライオンが獲物を襲うために水たまり(watering hole)近くで身を潜める様子からその名がきており、標的型攻撃とも言う。攻撃者はターゲットが主に利用するサイト情報を事前に把握して、ゼロデイ脆弱性などを突いて該当するサイトにマルウェアを潜ませておく。ユーザーはそのサイトにアクセスするだけで感染してしまうのだ。

■ マルバタイジング(Malvertising)

マルバタイジングは、マルウェア(Malware)とアドバタイジング(Advertising)の合成語で、オンライン広告にマルウェアを挿入してユーザーを攻撃する手法である。

■ エクスプロイト(Exploit)

TTA(韓国情報通信技術協会)用語辞典によるとエクスプロイト(Exploit)を『コンピューターやコンピューター関連電子製品の脆弱性を利用した攻撃方法』としている。主に攻撃対象の権限の奪取やサービス拒否攻撃(DoS)などを目的とし、攻撃タイプによって「BOF脆弱性攻撃」「CSRF脆弱性攻撃」「XSS脆弱性攻撃」などに区分される。

■ サイバーキルチェーン(Cyber Kill Chain)

APT(Advanced Persistent Threat)と呼ばれる知能型攻撃を説明する時に、よく使用される用語の中で『サイバーキルチェーン(Cyber Kill Chain)』がある。キルチェーン(Kill Chain)はもともと軍事分野で使用された単語で、敵のミサイルをリアルタイムに検知して攻撃する一連の攻撃型防衛システムのことを意味していた。現在サイバーキルチェーン戦略は、サイバー攻撃の最も広く知られた分析モデルの一つであり、各セキュリティ企業はサイバーキルチェーンをベースにした段階別防御戦略を構築している。サイバーキルチェーンの 7段階は、▲偵察(Reconnaissance)、▲攻撃コード作成(Weaponization)、▲伝達(Delivery)、▲脆弱性攻撃(Exploitation)、▲インストール(Installation)、▲コマンド及び制御(Command and Control)、▲目標システムの掌握(Actions on objectives)となっている。

http://jp.ahnlab.com/site/main.do

http://global.ahnlab.com/site/main.do

http://www.ahnlab.com/kr/site/main.do

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。
アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒108-0014 東京都港区芝4丁目13- 2 田町フロントビル3階 | TEL: 03-6453-8315 (代)