

サイバーセキュリティトレンド2017

サイバー攻撃の多様化、高度化は衰えることなく、被害規模は増加の一途をたどっている。
企業は資金や人材のリソース不足といった逆風の中、ターゲットを定め新たな一歩を踏み出す必要がある。

本資料に掲載されている会社名、製品名などの固有名詞は、一般に該当する会社もしくは組織の商標または登録商標です。

●NTTテクノクロスは環境保護に取り組んでいます。

NTTテクノクロス株式会社 クラウド&セキュリティ事業部

TEL : 045-212-7577
Email : cs-trend@cs.ntt-tx.co.jp
URL : <https://www.ntt-tx.co.jp/products/cs-trend/>

Copyright© 2017 NTT TechnoCross Corporation

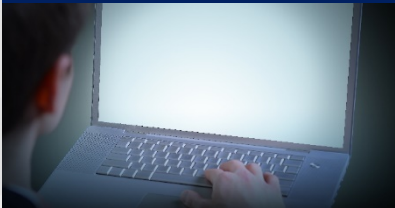


1 新たなボーダレス時代が到来し、サイバーフィジカルセキュリティが進化する

IoTデバイス数の急増とともに、IoTビジネスの普及が期待される一方、その脆弱性を悪用したサイバー攻撃が世界的規模で拡大している。サイバーとフィジカルが融合する新たなボーダレス時代においては、正当と不正の見極めが特に重要となり、「モノ」のアイデンティティ管理が求められる。



2 事業継続性を脅かすサイバー攻撃対策が必要となる



ランサムウェアやDoS攻撃が世界的規模で急増している。事業運営のために必要なシステム、データ、ネットワークリソースが突如として失われるリスクに直面している。サイバーセキュリティの観点からも、改めて事業継続計画の策定と実行が急務である。

3 サプライチェーン全体でのセキュリティマネジメントが求められる

ビジネスの多様化、高度化、効率化は企業間連携、サプライチェーンの拡大を促進する。攻撃者は最も効果的な攻撃対象を戦略的に攻めてくる。一企業のサイバー被害はサプライチェーン全体に波及する。サプライチェーン全体で連携したセキュリティ対策が必要である。



4 インシデント対応組織の実行力強化が求められる



インシデント対応強化のためCSIRTを設置する企業が増加している。しかしながら、実際のサイバー攻撃発生時には、その経験不足から十分な対応ができないCSIRTがほとんどである。訓練や演習等によるシミュレーションにより、自組織の実力把握、課題抽出を行い、継続的に改善を図っていくことが重要となる。

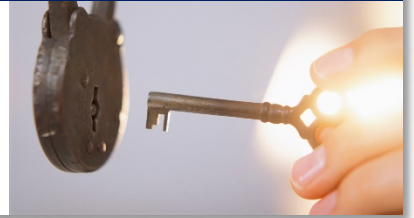
5 ソフトウェアの継続的かつ効率的な脆弱性マネジメントが益々重要となる

OSSをはじめとするソフトウェアは広く活用される一方、脆弱性の露見が後を絶たない。2016年度もApache Struts2やBIND9等、広く活用されているOSSで重大な脆弱性が多数発見され、実際の攻撃にも悪用された。日々発見される脆弱性情報を継続的かつ効率的に収集し対策し続ける基本動作が益々重要となる。



6 プライバシー保護とデータ利活用の対策が進化する

改正個人情報保護法の施行が2017年5月30日に決定され、より具体的な施行令、規則、ガイドライン等が次々と策定された。「個人情報」を適切に「匿名加工情報」に加工し、プライバシーに十分配慮したデータ利活用ビジネスを展開する企業が躍進する。



7 無線通信インフラが整備され、モバイルセキュリティが重要になる



2020に向けて、無線LANサービス等モバイルネットワーク、モバイルサービスが拡大していく。モバイル環境におけるセキュリティ対策は十分とは言えず、モバイルを標的にしたサイバー攻撃も増加している。モバイルサービスを提供する側、利用する側双方でのセキュリティ対策が必要となる。

8 セキュリティ技術者の育成が進み、セキュリティスマートソーシングが加速する

セキュリティ技術者の不足数は年々拡大し、セキュリティ要員の配置に苦慮する企業が多い。自社内に必要なインソースの人材定義と育成が急務であり、自社の実態、戦略に合わせて、インソース/アウトソースをバランスよく徐々に最適化していくスマートソーシング戦略の策定、実行が必要である。



9 AIを活用したセキュリティ対策が進化する



コンピュータ性能の飛躍的な向上を背景に、第三次AIブームが到来している。未知の攻撃、異常、脆弱性の自動検知等、AIを活用したセキュリティ技術も進化しつつある。攻撃側もAIによるサイバー攻撃が今後増加していくものと考えられ、マシン対マシンのサイバー攻防が繰り返される時代に突入していく。

10 加速するビジネススピードに対して継続的なセキュリティ確保も必須となる

加速するビジネススピードに対して、より柔軟、より迅速、より安全に開発・運用し続けるDevSecOpsが注目されている。高まるセキュリティ脅威に対して、開発プロセスの中に、継続的に安全性をチェックする仕組みを導入していく必要がある。

