サイバーセキュリティを取り巻く社会動向とNECの取り組み

サイバー攻撃やサイバー犯罪の被害が重大化し、大きな社会課題となっています。この状況のなか、政府もサイバーセキュリティ対策に関するさまざまな施策を打ち出しています。一方、NECは自社のセキュリティを守るためにサイバー攻撃防止システムや情報漏えい対策基盤などさまざまな技術を開発し、近年ではAI技術の応用を進めています。また、セキュリティインテリジェンスの獲得についても積極的な取り組みを行っています。NECはこれらの技術や情報、高度なセキュリティ人材を背景に、さまざまなソリューションを提供しています。本稿では、このような社会動向とNECの取り組みを紹介します。

ビジネスクリエイション本部 シニアエキスパート **鈴木 幹雄**
サイバーセキュリティ戦略本部 マネージャー **山井 忠則**
サイバーセキュリティ戦略本部 主任 **鈴木 哲也**
セキュリティ研究所 主席技術主幹 **宮内 幸司**

1. はじめに～サイバーセキュリティの動向

サイバー攻撃は、時代とともに変化しています。当初は、愉快犯など個人的なサイバー攻撃が主流でしたが、組織・重要インフラ・国家を標的とした経済犯・組織犯的なものに移行し、次第に高度化・複雑化してきました。なかでも、特定の対象を狙った「標的型攻撃」による被害や、社会的・政治的な主張を目的とした団体による攻撃が表面化し、DDoS攻撃やWebサイトが改ざんされることも多くなってきています。また、クレジットカード情報・個人情報の窃取や、インターネットバンキングでの不正送金が多発するなど、社会全体の問題として認識されてきました。

このような状況において、政府は2014年に「サイバーセキュリティ基本法」を制定し、行政機関や重要インフラにおけるサイバー対策の重要性、民間事業者・教育研究機関などにおける自発的な取り組みの必要性、人材確保の重要性を指摘し、基本方針を示しました。

最近では、IoTなどの新しい技術が普及し、ICTの利活用が拡大するなか、脆弱なIoT機器を踏み台にした大規模なサービス停止攻撃（DDoS攻撃）や重要インフラへの攻撃で大規模停電も発生しています。そのなかで、2015年5月に「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第4版）」が公開され、攻撃による障害を可能な限り削減するとともに、障害発生時の早期検知や迅速な復旧と再発防止を図る取り組みを推進する重要性が示されました。

こうしたなかで、企業の経営者層に対して、サイバーセキュリティ対策の推進が企業戦略であるとの意識改革を目的とした「サイバーセキュリティ経営ガイドライン」が策定されました。そこに記載されている攻撃に対応するためのセキュリティ人材確保について、経済産業省のデータでは2016年時点で13.2万人不足しており、2020年では19.3万人に拡大するとの推計が出ています。人材育成を通じて、サイバーセキュリティ対応人材を増やすことが急務となっています。

人材育成については、産官学でそれぞれ取り組みが推進されています。大学では、企業との連携や経済産業省の促進事業などでセキュリティ関連講座が複数開設されました。産業界では、サイバーセキュリティ人材を育成・雇用・活用し続ける循環（エコシステム）の実現を目指した「産業横断サイバーセキュリティ人材育成検討会」が発足して活動を続けており、成果が期待されています。

2. NECの取り組み

このような社会の動きに対して、NECは早くからさまざまな取り組みを行ってきました。

2000年初頭、Nimda/CodeRedという、周囲に感染を広げて自己増殖するウイルスが猛威を振るいました。これらのウイルスへの対応の経験を通じて、「数えるマネジメント」というコンセプトを立案し実践しました。「数えられないものは管理できない」という考え方に基づいて開発したのが、CAPS（Cyber Attack Protection System）と呼ぶサイバー攻撃防止システムです。CAPSでは、PC/サーバにインストールされたOSの種別やバージョン、プログラムの内容、セキュリティ対策の適用状況、ウイルスへの感染状況など、多様な情報を網羅的に収集・可視化し、それに基づいて適切なパッチを迅速に適用することで、脆弱性の排除や攻撃に対する事前防御を図っています。このコンセプトは、NECのセキュリティ対策の基礎となっています。

最近のサイバー攻撃については、脅威に対するリスク分析を行い、それに基づいて対策を実施しています。特に注力しているのは、未知攻撃の検知、ログの統合管理・監視、GCAPS（Global Cyber Attack Protection System）の導入、CSIRT（Computer Security Incident Response Team）体制の確立です。CSIRT体制のなかでは、インシデント対応に加えて、NECで開発した先端技術の価値実証も行っています。こういった取り組みによって、サイバーセキュリティ経営を実現しています。

サイバーセキュリティ対策では、セキュリティインテリジェンス（攻撃に関する知識）も重要です。攻撃者は常に同じ攻撃を仕掛けてくるわけではなく、新たな攻撃手法を使ってきます。したがって、防御する側も新たな手法を研究し、効果的な対策を編み出す必要があります。また、攻撃者によって攻撃手法に特徴、癖があるため、攻撃者のアトリビューション（攻撃者像を浮び上がらせること）を行ったり、攻撃手法を研究することによって次の段階の攻撃を予測したりすることも可能となります。NECでは、社内CSIRTで社内に対する攻撃やインシデント事案を収集しています。また、自社での情報収集に加え、国際的なサイバー犯罪を取り締まる組織との提携や、サイバー犯罪の情報の集約、分析、対処を推進する日本サイバー犯罪対策センター、セキュリティベンダー各社とも情報を共有したり、共同の研究を行ったりしています。更に、米国国土安全保障省が推進する、官民でサイバー攻撃の脅威情報を迅速に共有する枠組みにも日本企業として最初に加入しています。これら社内外、国内外から集めた情報を分析し、サイバーインテリジェンスと呼ばれる知見としてサイバーセキュリティ対策に活用しています。

このように、NECグループで実践するサイバーセキュリティへの取り組みをお客様へのソリューションとして提供しています。したがって、NECが提供するサイバーセキュリティソリューションは、NECグループで実証し、利便性と安全性の効果を検証したものとなっています。更に自社での運用で得たノウハウを、お客様にフィードバックし、保守運用においても可用性及び品質面の向上に生かしています。

3. NECが提供するサイバーセキュリティソリューション

サイバー攻撃の高度化、多様化に伴い、セキュリティ対策はどこか一点で実施すればよいというものではなく、複数の箇所で異なる観点での対策が必要になってきています。いわゆる、多層防御です。このため、お客様で実施すべきセキュリティ対策も多様化しています。

セキュリティ人材が大幅に不足していると言われる現在、多くのお客様にとっては、このような多様なセキュリティ対策を自社の要員で実施していくことは困難であり、外部の専門家に期待するところが大きくなっています。そのため、NECでは、これらのセキュリティ対策を製品だけではなく、サービスとしても提供しています（一部はサービスのみ）。

NECのサイバーセキュリティソリューションは、**図**にあるようないくつかのサービスから成り立っています。

主にサイバー攻撃への対策を提供するものとして、（a）事前対策、（b）セキュリティ監視、（c）事後対策があります。また、サイバーセキュリティ対策をNECが運用する（d）セキュリティSaaSも提供しています。

（a）事前対策

未対処の脆弱性など、組織内のリスクを見える化し、対処を行うための脆弱性情報管理サービスを提供します。

（b）セキュリティ監視

インシデント発生を検知するセキュリティ監視サービスを、提供しています。従来のセキュリティ監視サー

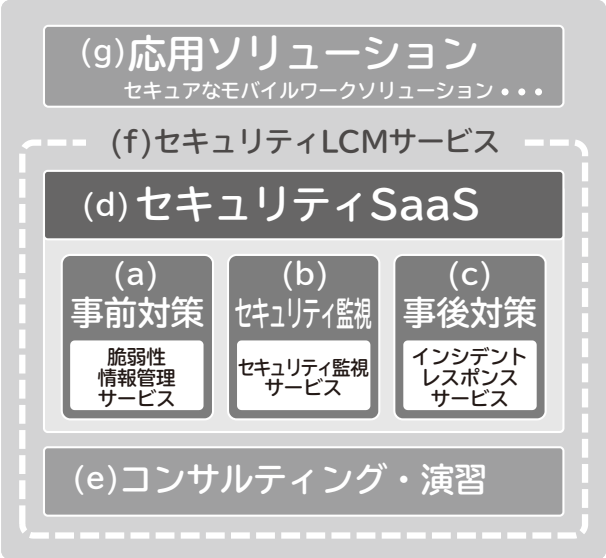


図　NECのサイバーセキュリティソリューション

ビスは属人的で、多くのお客様に精度の高いサービスを提供することは困難でした。このためNECでは、AI技術の活用や、世界三極体制でお客様の環境を監視するなどの取り組みを行っています。

(c) 事後対策

セキュリティインシデントが発生した場合の対応として、インシデントレスポンスサービスを提供しています。一般的なインシデントレスポンスサービスは、お客様のところに駆けつけて調査を行いますが、これには時間を要します。NECでは、リモートから一次調査を行い、簡単なケースはその場で判断するようなサービスを行っています。

(d) セキュリティSaaS

メールセキュリティ、ファイル暗号化、Web Application Firewallなどのさまざまなセキュリティ機能をクラウド上で提供し、お客様の管理業務を軽減します。

(e) コンサルティング・演習

セキュリティ対策は計画的に強化することが重要であり、経営視点での対策も要請されています。NECは、経済産業省発行のサイバーセキュリティ経営ガイドラインをもとにしたセキュリティ対策を支援するコンサルティングサービスを提供しています。また、セキュリティ対策を実施するためには、お客様側での人材育成も重要です。NECではセキュリティ人材を強化する演習にも取り組んでいます。

(f) セキュリティLCMサービス

お客様のサイバーセキュリティ対策の持続的な向上を目的に、コンサルティングから、システム構築、監視、インシデント対応までを包括的に提供するサービスを開始しています。

(g) 応用ソリューション

今回ご紹介したサイバーセキュリティ対策製品・サービスをさまざまなソリューションに組み込んだ、セキュアなソリューションの企画開発も進めており、その一例として、セキュアなモバイルワークソリューションを提供開始しました。

このように、お客様へ直接提供するサイバーセキュリティソリューションの他、お客様に提供するシステム、製品、サービスを安全・安心なものにするためのセキュア開発・運用や、お客様にセキュリティソリューションを提供するための人材獲得、育成にも取り組んでいます。

4. サイバーセキュリティソリューションを支える研究開発

近年、サイバー攻撃は攻撃手段の多様化や巧妙化が進むとともに、その件数も増加しています。このため、従来のセキュリティ専門家による対応は質・量の両面で限界を迎えつつあり、AI技術の活用によりサイバーセキュリティを強化する取り組みが活発化しています。

NECでは、セキュリティ専門家が担っているサイバー攻撃の検知、分析、対処方法立案の各業務を、AI技術を活用して自動化することにより、人では発見・対処が困難な高度なサイバー攻撃にも対処可能とするとともに、セキュリティ専門家の不足を解消する、新しいセキュリティ技術の研究を進めています。

高度化・巧妙化が進むサイバー攻撃は、現在のセキュリティ技術では検知することすら難しいという問題があります。そこで、NECは、詳細なシステムの動作状況を常時AI分析することで未知攻撃を検知する技術を確立し、対策サービスを開発しました。更に、サイバー攻撃を検知した際、セキュリティ専門家は自らの深い知見・経験を基に、断片的なサイバー攻撃の痕跡から攻撃の全容を推測し、攻撃手法を解明、被害範囲を特定し、適切な対処方法を立

案します。現在実用化されているAI技術を活用したサイバーセキュリティ技術は、蓄積された過去の攻撃に関する膨大な知識から特定のサイバー攻撃に対する対処方法を検索することは可能ですが、前述したようなセキュリティ専門家の高度な業務を担うことはできません。NECは、独自の論理推論型AI技術を活用することで、セキュリティ専門家の業務を担うことが可能なセキュリティ技術の確立に取り組んでいます。

また、サイバー攻撃の被害を極小化するためには、今後発生しうるサイバー攻撃を予測し事前対策することが非常に有効です。更に、サイバー攻撃を受けた際に迅速かつ適切に対処するには、サイバー攻撃に関する知識（セキュリティインテリジェンス）が重要な役割を果たします。NECは、攻撃者が情報交換に利用するソーシャルメディアから得た膨大な情報をAI分析し、セキュリティインテリジェンスを自動生成する技術、更に今後多発すると見込まれるサイバー攻撃を事前に予測し、その対処方法を立案する技術を確立し有効性を評価しています。

以上の取り組みに加えて、セキュリティ脅威が急速に高まりつつある、重要インフラを支える最先端の暗号技術にも取り組んでいます。これらの技術については、「IoTにおける多様なデバイスに適用可能な軽量暗号」（NEC技報 Vol.70 No.1「デジタルビジネスを支えるIoT特集」pp.64-pp.67）、「FinTechのセキュリティ強化に貢献するマルチパーティ計算技術」（NEC技報 Vol.69 No.2「デジタルトランスフォーメーションを加速するFinTech特集」pp.50-pp.54）で紹介しています。

5. まとめ ～Futureproof Security 安心の先へ。

NECグループは、豊かなグローバル社会の実現のために不可欠な「安全」「安心」「効率」「公平」という4つの社会価値の適用のため、社会インフラの高度化に注力しています。社会にとって必要不可欠なインフラを支えてきた実績を蓄積・活用し、サイバーセキュリティにおいては「Futureproof Security 安心の先へ。」というスローガンを掲げ、すべてのシステムに当たり前の「安全」「安心」を提供し、暮らしと社会を、より良い未来につなげていきます。

関連URL

サイバーセキュリティソリューション
http://jpn.nec.com/cybersecurity/index.html

Cyber Security Solutions
http://www.nec.com/en/global/solutions/cybersecurity/index.html

NEC 技報のご案内

NEC 技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報（日本語）　NEC Technical Journal（英語）

Vol.70 No.2　ビジネスの安全・安心を支えるサイバーセキュリティ特集
～Futureproof Security　安心の先へ。～

ビジネスの安全・安心を支えるサイバーセキュリティ特集によせて
増大するサイバー犯罪の根源的な解決へ～“産学官”のオールジャパンで立ち向かう第三者機関の姿とは？～
サイバーセキュリティを取り巻く社会動向とNECの取り組み

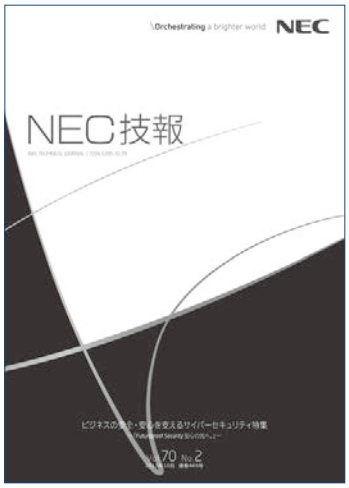
◇ 特集論文

社会の動向とNECの取り組み
重要インフラに対するサイバー攻撃の実態と分析
2017 サイバー攻撃最新動向 NEC Cyber Threat Intelligence活用モデル
サイバーセキュリティ対策の社内事例

サイバーセキュリティソリューション
複雑化 / 高度化するサイバー脅威に対抗するSOCとセキュリティ監視サービス
攻撃被害を極小化するためのインシデント対応支援ソリューション
サイバー演習によるインシデントハンドリング能力の強化
セキュリティ統合管理・対処ソリューション「NEC Cyber Security Platform」
クラウド型ファイル暗号化サービス －ActSecureクラウドセキュアファイルサービス－
セキュリティLCMサービス
EMMを活用したセキュアなモバイルワークソリューション
IoT 時代の経営を支援するサイバーセキュリティコンサルティング

サイバーセキュリティへのAI技術の活用
AI（人工知能）を活用した未知のサイバー攻撃対策
採るべき対策の「なぜ？」に答えるAIの可能性
オープンソースインテリジェンスを活用したサイバー脅威の検出と自動分析
犯罪捜査支援のためのサイバー・フィジカル統合分析技術

お客様に安全・安心を届けるための社内の取り組み
安全・安心な製品・サービスをご提供するための取り組み ～セキュア開発・運用～
サイバーセキュリティ人材のタレントマネジメント



Vol.70 No.2
（2017年10月）

特集TOP