高度化するサイバー攻撃への取り組み「サイバーセキュリティ・ファクトリー」

矢野 由紀子　高橋 完樹　樋口 健　有松 龍彦

要 旨

NECは巧妙化するサイバー攻撃に対抗するため、人材・技術・ナレッジを集結したサイバー攻撃対策の中核拠点「サイバーセキュリティ・ファクトリー」を設立し、2014年6月から本格的に稼働を始めました。高度で総合的なサービスを、セキュリティ専門会社と連携して提供するとともに、サービスや技術の開発、サイバーインテリジェンスの拡充、要員の育成を行っていきます。

KeyWords
サイバーセキュリティ／サイバー攻撃／標的型攻撃／セキュリティ監視／サイバーインテリジェンス
サイバーセキュリティ・ファクトリー／インターポール

1. はじめに

昨今、標的型攻撃などを中心としたサイバー攻撃による情報流出の被害が拡大しており、特に公的機関の機微情報、企業の最新技術、個人情報などが組織的なプロのサイバー犯罪集団に狙われています。被害によって、企業の社会的信用の失墜、損害・補償などの金銭的損失、更には企業活動の継続が困難になるなど、影響は甚大であり、情報セキュリティ対策強化の必要性がますます高まっています。

NECの「サイバーセキュリティ・ファクトリー」は、こうした攻撃に対抗するための専門組織として設立されました（写真）。

写真　サイバーセキュリティ・ファクトリー

本稿では、サイバーセキュリティ・ファクトリーの目指す方向を示すとともに、実際の活動について紹介します。

2. サイバー攻撃の現状

近年のサイバー攻撃は、2000年頃に流行した、愉快犯や自身の技術力をアピールするための不特定多数への攻撃から、官公庁や重要インフラ、企業などの知的財産や機密情報を狙ったものや、抗議・デモを目的としたWeb改ざん・サービス停止など、特定の組織を狙った攻撃が主流となってきています。ひとたびサイバー攻撃にさらされて社会システムがダウンするなどの事象が発生すると、該当する組織などの社会的信頼の失墜だけでなく、社会問題にまで発展してしまいます。

昨今の新聞で取りざたされているサイバー攻撃は、氷山の一角でしかなく、なかには何らかの理由により社会に公開されていないインシデントもあります。更には、経営者・システム管理者が気付かないまま、現在も攻撃者から攻撃が続いていることもあるかもしれません（図1）。

近年のサイバー攻撃は、Webサーバやネットワーク、OS、ゲートウェイ製品、アプリケーションなどの脆弱性を狙うものや、“なりすまし”、“個人の興味・関心”による個人の“隙”

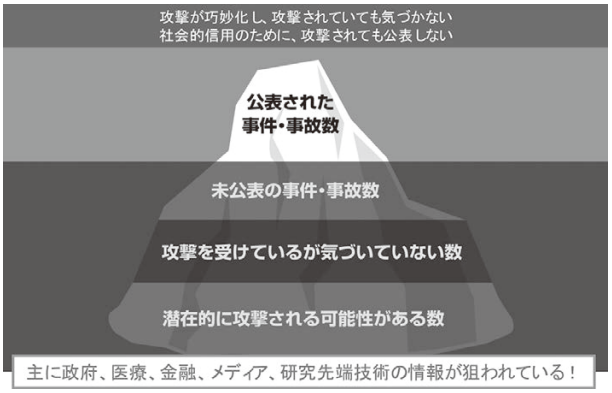

図１　サイバー攻撃の実際

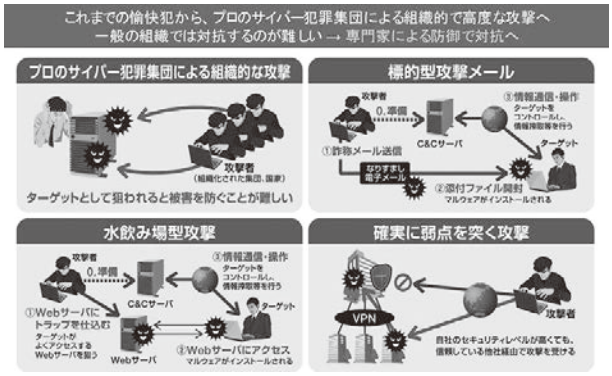

図２　巧妙化するサイバー攻撃

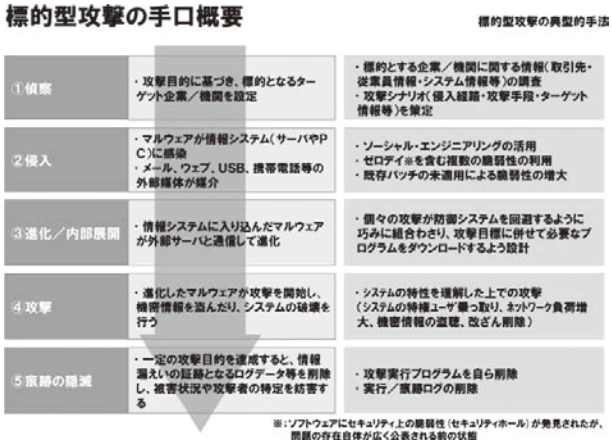

図３　標的型攻撃の手口概要

を狙うものなど、攻撃手法もさまざまであり、次から次へと形を変えて高度化しています（図2）。

これらの攻撃手法を用い、まず攻撃者は欲しい情報や標的となる相手に対して、攻撃開始の1年以上前から偵察活動を行い、攻撃のシナリオ・手法などを検討し、攻撃してきます。その後、標的となる相手に巧妙な攻撃手段を持ってシステムに入り込み、外部のC＆C（Command and Control）サーバと通信しながら攻撃コードを送り込み、情報搾取やシステム停止などを行います。その後、インシデント発覚を遅らせるため、システムのログ情報や端末内の攻撃コード、ログ並びに搾取用に圧縮したデータを強制削除します（図3）。

上記の攻撃手法、標的型攻撃の流れにより攻撃が行われるため、標的となる官公庁や重要インフラ、企業などは、巧妙かつ精錬された攻撃から自組織を守るため、従来の防御方法ではない新たな手法により対処する必要があります。

3. サイバーセキュリティ・ファクトリー

サイバーセキュリティ・ファクトリーは、サイバー攻撃対策の導入・運用を支援するために必要な仕組みを備えたサイバー対処の中核拠点です（図4）。NECグループ、及び外部のセキュリティ専門会社との連携により「サイバー攻撃対策の専門家」を集結させ、サイバー攻撃の監視業務やインシデントの詳細解析といったサービスの提供を実際に行いながら、サイバー攻撃情報を収集・分析し、対応に必要な技術やノウハウを創出・蓄積しています。

3.1 セキュリティ監視

お客様のネットワークやウェブサイトを、専門のセキュリティアナリストが24時間365日体制で監視しています。攻撃が検知された場合には分析を行い、お客様へ報告を行います（図5）。

攻撃検知の報告は、セキュリティ機器が出したアラートをそのまま伝えるわけではなく、それらのアラートを分析エンジンでフィルタリングをし、最後にセキュリティアナリストが内容を精査したうえで報告を行います。攻撃が日々巧妙化していくなか、それらに対抗するためには日々の技術の向上が不可欠です。

3.2 インシデントレスポンス

もし自組織内外からサイバー攻撃が仕組まれ、サイバーインシデントが発生した場合、その攻撃を無力化するとともに、インシデントの原因追及や分析、被害を受けたシステムの復旧、再発の防止を行う必要があります。

図6のとおり、処置には3つのフェーズ（緊急処置、調査・

図４　サイバーセキュリティ・ファクトリーの概要

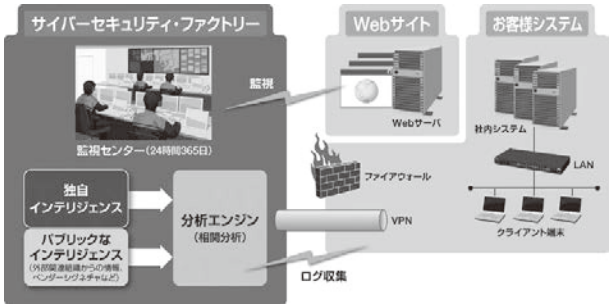

図５　セキュリティ監視体制

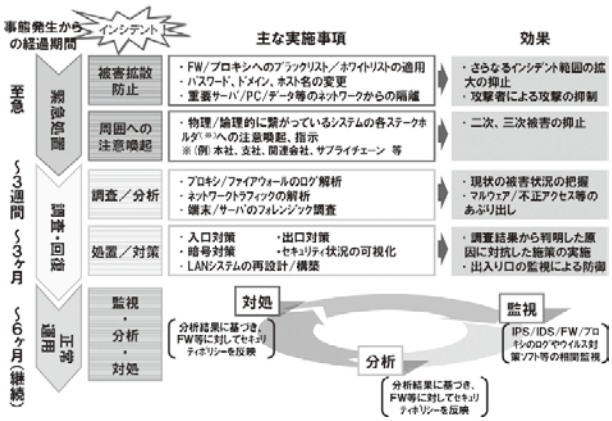

図６　サイバーインシデント発生から正常運転までの流れ

回復、正常運用）に分けられます。これらのフェーズごとに記載されている主な実施事項を行うことにより、被害拡散の防止や将来に向けたシステムの対処を行うことができます。

自組織で体制・態勢がないもしくはスキルが不足している場合は、JPCERT/CCやセキュリティ・ベンダとNDAを締結して、対処を実施することも可能です。最終的には自組織にCSIRT（Computer Security Incident Response Team）を設け、自組織を守るとともに、社会貢献的な位置付けで自組織CSIRTをアピールする企業もあります。

3.3 サイバーインテリジェンス

急速に高度化するサイバー攻撃を検知・防御するには多種多様な情報を収集・分析し、防御力強化のために役立てる必要があります。ハッカーコミュニティの動向や攻撃の予兆に関する情報、最新の攻撃テクニックや攻撃ツールに関する情報、攻撃元に関する情報（ブラックリスト）、未発表の脆弱性に関する情報、攻撃を発見するための判別方法（シグネチャ）などを総称して「サイバーインテリジェンス」と呼びます。

弊社は、サイバーインテリジェンス拡充のため、国際刑事警察機構（インターポール）を通じた各国法執行機関との連携、日本国政府との連携を進めるとともに、海外のインテリジェンス情報企業との業務提携などを積極的に進めています。

3.4 技術開発

サイバー攻撃に対抗していくには、セキュリティ監視の現場の知見とノウハウや、サイバーインテリジェンスを集めて、活用できるナレッジに形に変えていくことが必要ですが、情報の量は膨大です。そこで、技術開発の取り組みの1つとして、アナリストが行っている分析・知見化の作業を自動化する技術を開発しています。アナリストの分析作業をツールで補助することにより、アナリストはより高度な分析対応に注

力できるようになります。その他にも、検知精度を上げる技術の開発などにも取り組み、巧妙化・高度化する攻撃に対応していきます。

3.5 人材育成

監視オペレーションやサイバーセキュリティ・ファクトリーのさまざまな活動のなかで人材の育成を行うとともに、実際の運用経験をサイバー演習に活用して、効果的な育成手法の開発に取り組みます。

サイバー攻撃に関しては、実地経験を積む機会がなかなかありません。そこで、実際の企業などのICT環境に近い模擬環境を作って、そのうえで対処を経験して実践に備えます。2013年度には、総務省の「サイバー攻撃解析・防御モデル実践演習」というプロジェクトのなかで、サイバー演習を10回実施し、情報セキュリティシステムの管理者や運用者の方々数百名に受講していただきました。

また、NECグループが保有するさまざまな教育プログラムについて「サイバーセキュリティ人材の育成」の観点で整理し、上記のようなサイバー演習も含めて、人材育成プログラムとして提供していく予定です。

4. グローバルへの取り組み

インターポールは、最先端のテーマを扱う新しい拠点として、the Interpol Global Complex for Innovation（IGCI）の設置をシンガポールで進めています。ここでは、サイバー犯罪を中心テーマに据えていて、the Interpol Digital Crime Center（IDCC）がその活動を担うセンターとなっています。IDCCは2014年度中にシステムインフラを整備し、実稼働を始める予定です。

弊社は、IDCCのインフラ整備から情報分析、トレーニング、技術評価など、活動の立ち上げに協力しています。今後IDCCの活動が軌道に乗るにつれ、周辺国の警察機関を含めて、サイバー犯罪に対する協力活動が多く出てくると期待されます。

サイバーセキュリティ・ファクトリーでは、インターポールで使われる同じ分析システムを設置し、知識ベースを活用しながらバックエンドで活動を支援します。また、要員教育や人材交流などによる連携も積極的に行っていきます。

図7　サイバーセキュリティ総合支援サービスの概要

5. サイバーセキュリティ総合支援サービス

「サイバーセキュリティ総合支援サービス」では、サイバー攻撃による情報流出などを防ぐため、サイバー攻撃対策システムの設計・構築からセキュリティシステムの運用監視、異常検知時の対応までをワンストップでサポートします（図7）。

導入時には、脆弱性の診断やペネトレーションテストにより、お客様に最適なソリューションを提案します。また、端末までの監視や、定期診断などの運用サービスを充実させています。異常を検知した時には、「サイバーインシデント駆けつけサービス」により、事件・事故発生時に適切な初動対応をとれるような体制を整えています。

6. おわりに

サイバーセキュリティ・ファクトリーでは、日々進化する脅威に対応するため、情報共有・技術開発・人材育成の相乗効果を図りながら、サイバー攻撃に対応するよりよいソリューションやサービスの提供を目指して、活動を進めていきます。

執筆者プロフィール

矢野 由紀子
ナショナルセキュリティ・ソリューション事業部
プロジェクトディレクター

高橋 完樹
ナショナルセキュリティ・ソリューション事業部
マネージャー

樋口 健
株式会社インフォセック
営業本部長

有松 龍彦
株式会社インフォセック
サイバーインテリジェンスセンター
センター長

関連URL

NEC、「サイバーセキュリティ・ファクトリー」が本格稼働
～ 官公庁や企業のサイバー攻撃対策向け支援を強化 ～
http://jpn.nec.com/press/201406/20140616_01.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.67 No.1　社会の安全・安心を支えるパブリックソリューション特集

社会の安全・安心を支えるパブリックソリューション特集によせて
NECが目指すパブリックソリューションの全体像
NECのパブリックセーフティへの取り組み

◇ 特集論文

効率・公平な暮らし

マイナンバー制度で実現される新しいサービス
ワールドカップを支えた「NECのスタジアム・ソリューション」
魅力あふれるフライトインフォメーションシステムの実現
駅の新サービス実現を加速するSDNソリューション
マルチデバイス対応テレビ電話通訳の通訳クラウドサービス
カラーユニバーサルデザインを採用した使いやすいスマートフォン向けネットバンキングサービス
安全・安心を実現する世界一の顔認証技術
顔認証製品と社会ソリューションでの活用

安全・安心な暮らし

ICTを活用したヘルスケアへの取り組み
組織間の安全な情報共有を実現する「MAG1C」の情報ガバナンスソリューション
「MAG1C」における大規模メディア解析及び共有デジタルサイネージ機能
シンガポールにおけるより安全な都市「セーファー・シティ」の構築
アルゼンチン ティグレ市の未来を守るビデオ解析ソリューション
群衆行動解析技術を用いた混雑推定システム
音声・音響分析技術とパブリックソリューションへの応用
昼夜を問わず24時間監視を実現する高感度カメラ
人命救助を支援するイメージソリューション
Emergency Mobile Radio Network based on Software-Defined Radio

重要インフラの安全・安心

新幹線の安全・安定輸送を支える情報制御監視システム
水資源の有効利用をICTで実現するスマートウォーターマネジメント技術の研究開発
センサとICTを融合させた漏水監視サービス
沿海域の重要施設へ接近する不審対象を監視する港湾監視システム
インバリアント解析技術(SIAT)を用いたプラント故障予兆監視システム
赤外線カメラの画像処理技術と応用例
高度化するサイバー攻撃への取り組み「サイバーセキュリティ・ファクトリー」

社会の安全・安心を支える先端技術

国家基盤を支える指紋認証の高速高精度化技術
次世代放送を支える超高精細映像圧縮技術とリアルタイム4K映像圧縮装置

◇ NEC Information

NEWS

NEC「衛星インテグレーションセンター」の稼働を開始
陸上自衛隊の活動を支える「浄水セット・逆浸透2型」の開発

Vol.67 No.1
(2014年11月)

特集TOP