NTTデータ 先端技術株式会社

企業による「脅威インテリジェンスサービス」の活用が本格化
～ 新型コロナウイルスに便乗したサイバー攻撃にも注意 ～

2020年1月以降、日本を代表する企業の大規模な情報漏えい事件が相次いで発覚するなど、サイバー攻撃による被害が深刻化しています。高度なセキュリティ対策を施していると考えられる企業でさえ防御に苦慮しているということからも、手口の多様化・巧妙化が進んでいる状況がうかがえます。こうしたなか、サイバーセキュリティリスクを早期に特定して、その後の対応策までを提示する「脅威インテリジェンスサービス」の活用に対する企業の注目が高まっており、2020年に導入の動きが本格化することが予想されています。

日本国内でも重大な脅威としての認識が高まる「サプライチェーン・リスク」

脅威インテリジェンスとは、組織に対するサイバー攻撃を防止および軽減するための知識と定義付けられ、具体的には、注意すべき攻撃者、攻撃の動機、攻撃者が使用する技術・戦術・手順、攻撃の対象となり得るシステムや知的財産などの情報を指し、企業内におけるセキュリティ対策の意思決定に寄与するものです。こうした脅威インテリジェンスの必要性が高まっている背景には、サプライチェーン・リスクの存在が挙げられます。情報処理推進機構が公開している「情報セキュリティ10大脅威 2020」でも第4位にラインインしており、重大な脅威としての認識が高まっています。

サプライチェーン・リスクとは、組織が特定の業務や製品を外部組織に委託したり調達する際に、委託先組織がセキュリティ対策を適切に実施していないと、委託元組織への攻撃の足がかりとして狙われ、その結果、預けていた個人情報や機密情報の漏えい、委託元の製品やサービスに影響を与えるなどの事態を指します。これらリスク回避のためには、委託先組織におけるセキュリティ対策の実施状況の確認が重要ですが、委託先組織の先に再委託先組織がある場合、その管理は委託先組織が行うため、委託元にとってのセキュリティ対策管理はさらに難しくなるという課題もあります。

こうしたなか、日本の企業では、SOCやCSIRTの設置に加えて、外部の脅威インテリジェンスを取り込んで対応能力を高めるなどの動きが、今後ますます浸透していくものと思われます。

情報セキュリティ10大脅威 2020

順位	「組織」向け脅威
1	標的型攻撃による機密情報の窃取
2	内部不正による情報漏えい
3	ビジネスメール詐欺による金銭被害
4	サプライチェーンの弱点を悪用した攻撃
5	ランサムウェアによる被害
6	予期せぬ IT 基盤の障害に伴う業務停止
7	不注意による情報漏えい
8	インターネット上のサービスからの個人情報の窃取
9	IoT 機器の不正利用
10	サービス妨害攻撃によるサービスの停止

（出典：独立行政法人 情報処理推進機構）

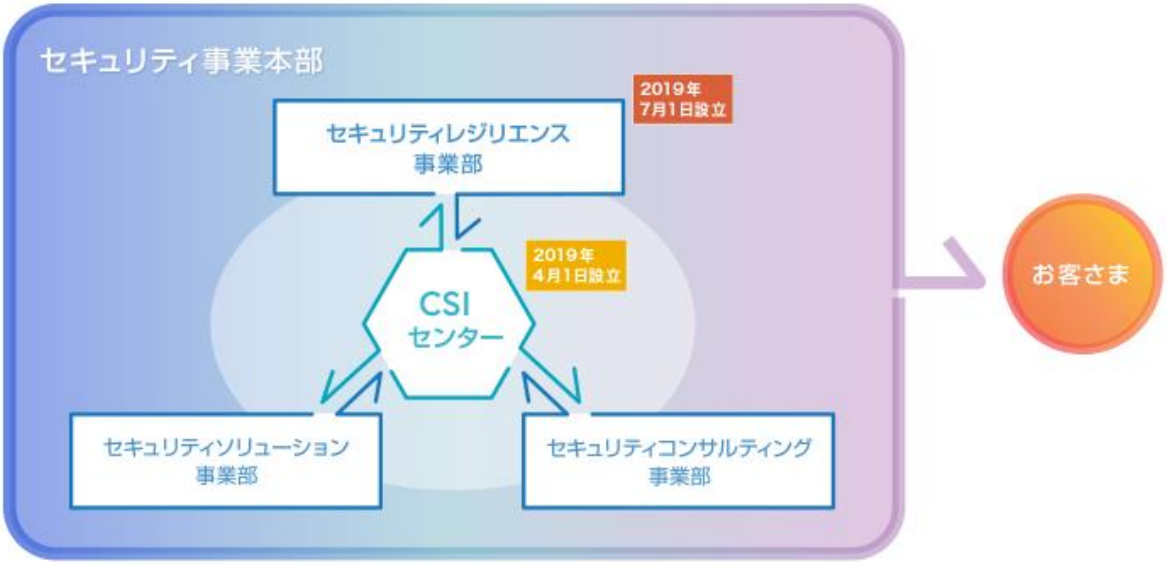
セキュリティ事業の創設から20年、「サイバーセキュリティ・インテリジェンスセンター」設立

近年、予防のためのセキュリティ対策を実現する「サイバー・ハイジーン」と、侵入されることを前提に可用性の確保を最重視したリスク最小化による事業継続を目指す「サイバー・レジリエンス」の重要性が高まっているなか、セキュリティ事業の創設から20年の実績を持つNTTデータ先端技術では、2019年4月に「サイバーセキュリティ・インテリジェンスセンター（以下：CSIセンター）」を開設しました。

CSIセンターでは、様々な情報源から脅威情報の収集を行っています。例えば、脅威情報にはサイバー攻撃者の次なる攻撃対象や攻撃ツール、また、すでに流出してしまっている企業の機密情報などがあります。その他、海外を含む外部のインテリジェンスベンダーとの連携などにより脅威情報を収集して、それらを高度な専門スキルを持つアナリストが分析を加え、顧客にとって有用となるセキュリティ情報を提供する脅威インテリジェンスサービスを展開しています。

また、それらの脅威インテリジェンスをNTTデータ先端技術が提供するセキュリティ関連サービスに組み込んで高度化していく取り組みも行っており、セキュリティ事業全体の中核を担う存在となっています。

NTTデータ先端技術のセキュリティ事業における「CSIセンター」の位置付け



日本企業を狙う新型コロナウイルスに便乗した新たな脅威

新型コロナウイルスの感染拡大に便乗したサイバー攻撃が世界各地で増えています。2011年に起きた東日本大震災の際にもサイバー攻撃が多発したことから、「便乗」による新たな脅威に備える必要があります。例えば、品薄状態が続くマスクを無料配布するといった内容の不審なメールが多くみられ、メール本文に記載したURLをクリックさせて偽のWebサイトに誘導することで、個人情報やクレジットカード情報など重要な情報を詐取するフィッシング詐欺が観測されています。その他、サイバー攻撃と思われる活動としてはフィッシング詐欺に加え、新型コロナウイルスに関連する情報を利用する新しいランサムウェア亜種の作成、新型コロナウイルスに関連するドメイン名の登録などがあり急増しています。

企業は、新型コロナウイルスの感染拡大から事業継続と従業員を守るために様々な対応を行っていますが、サイバー攻撃者の活動は、個人および企業等を狙うことが想定されるため注意が必要となります。時差通勤や在宅勤務（テレワーク）などを実施する企業の増加に伴って、在宅勤務の環境を狙うようなサイバー上の脅威が増加しています。短期間で在宅勤務の環境準備を余儀なくされ、十分なサイバーセキュリティ対策を施すことができなかった企業等が狙われることも考えられます。新型コロナウイルスに便乗したサイバー攻撃は急増しており、病院等のシステムなども狙われることが想定されるため、IT部門はシステムのセキュリティ監視およびセキュリティ自体の監視強化を行うことが望まれます。

NTTデータ先端技術について

NTTデータ先端技術は、NTTデータグループの技術面を支える中核会社として1999年に設立されました。基盤・ソフトウェア・セキュリティの3本柱のソリューション事業を通じて、お客様に価値を提供することを目指しています。NTTデータ先端技術に関する詳細な情報については、https://www.intellilink.co.jp/ をご覧ください。