TATA CONSULTANCY SERVICES JAPAN
A Tata Consultancy Services and Mitsubishi Corporation Joint Venture

TATA

White Paper

日本のサイバーセキュリティー政策と TCS が推奨するベストプラクティス

タタコンサルタンシーサービシズ
サイバーセキュリティプラクティス
アジア太平洋地域 セールス＆ソリューション部門統括
プラシャント D. デオ

日本タタ・コンサルタンシー・サービシズ株式会社
サイバーセキュリティ本部長
酒寄 孝側

デジタライゼーションの急速な進展により新しいテクノロジーが幅広く採用され、多くの企業にとってこれまでになかった新しいビジネスチャンスが生まれています。同時に、実空間とサイバー空間が融合されたことにより、サイバーセキュリティーのリスクが著しく増大しています。最近では、企業だけでなく政府も攻撃の危険にさらされるようになってきました。これは、ハッカーたちが非常に熟練し創造性を高めていることの現れでもあります。また、AI や IoT など進化するテクノロジーの影響は計り知れないほど広範にわたり、いまだその全体像は解明されておらず、悪意のあるエージェントは脆弱性を見つけ出し標的にしてきます。テクノロジーが社会のあらゆる側面に浸透するにつれ、サイバーセキュリティーの重要性がますます高まることは間違いありません。

サイバーセキュリティーを確保するためには、サイバー空間における脅威を制御し、軽減するシステムの構築が不可欠となります。その第一歩となるのが、レジリエントなサイバーセキュリティー戦略を確立することです。

本稿では、日本の政府主導の新しいサイバーセキュリティー戦略と、テクノロジー主導のビジネス変革「Business 4.0™」について考察します。政府の戦略は、企業がサイバーセキュリティーリスクを緩和するプロセスを構築、あるいは見直すためのフレームワークとなるものです。これをサイバーセキュリティーの基盤とするために、サイバーセキュリティーに関するさまざまな取り組みが自律的に行われるための三つのアプローチについて詳しく説明し、政府の戦略に沿って企業がこのアプローチを運用するための運用指針と、対策の具体例を提示します。

サイバー空間の拡大とともに増幅する脅威

東京では、2020 年の世界的スポーツイベントに向けて準備が進められており、開催まで 1 年を切りました。1964 年以来の東京での開催となるこのイベントは、世界中の人々に見守られ、AI、IoT、自動化、クラウドなどの新しいテクノロジーが幅広く採用されることになります。これらの Business 4.0 を支えるテクノロジーは、イベントにおいて重要な役割を果たし、その効果は計り知れないものになると予想されます。競技者や聴衆の体験を向上させることはもちろん、サイバーセキュリティーに対する意識も大幅に高めることになるでしょう。

企業は、Business 4.0 を支える新しいテクノロジーを活用することで、生産性や効率性、敏捷性を向上させる一方で、サイバー脅威に対する警戒もしなければなりません。前述のように、相互接続性の増加、インターネットの普及により、実空間とサイバー空間が融合してきています。このことは、社会に大きなメリットをもたらしますが、同時に悪用されるリスクをもたらし、実社会における被害もサイバー空間の拡大にともなって増幅します。

重要性が高まるサイバーセキュリティー計画

2018 年冬季イベント中に発生した攻撃では、開催国で数百台のコンピューターが停止し、インターネットやテレビのシステムは数時間にわたり停止状態に追い込まれました。2020 年の東京大会の準備においても、大至急でサイバーセキュリティーを強化しなければなりません。

スポーツの世界ではさまざまな新しいテクノロジーが採用されています。選手たちは、IoT 対応のスマートベストを着用し、リアルタイム分析ソフトウエアを駆使して競技力を高め、また、採点と時間調整のシステムは全てデジタルになっています。さらに観客の移動や身元確認の調査はコンピューター化され、電力や通信システム網などの重要な公共インフラのほか、サプライチェーンや輸送の面も併せてテクノロジーに依存しています。

このサプライチェーンの複雑な性質は、標的となる可能性がある対象の数が膨大であり、脅威が広範囲に及ぶことを意味しています。テクノロジーを使用することは、サイバー攻撃の標的になる可能性があり、脆弱性が伴います。その攻撃を防御するためには、迅速な行動が必要です。日本政府は、東京大会の計画に関わるかどうかに関係なく、全ての企業に対し、この機会を利用してサイバーセキュリティー計画を策定すること、あるいは見直すことを奨励しています。

日本政府のサイバーセキュリティー戦略

日本政府は、サイバー空間を大きな価値が眠っている未開拓地と考えており、持続可能な開発とセキュリティーを国家の優先事項としています。そこで政府は、ネットユーザーを保護するために抜本的な対策を講じようとしています。その一つとして、国内にあるインターネット上の IoT 機器の脆弱性をテストするために、2019 年 2 月に、およそ 200 万台の機器に対してサイバー攻撃を仕掛ける前例のない壮大なスケールの 「NOTICE (National Operation Towards IoT Clean Environment）」 を実施しました。攻撃の対象となったのは、センサー、ウェブカメラやルーターなどで、これらの機器が攻撃を受けやすいことを証明しようとしたものになります。この結果、調査対象となった IoT 機器の IP アドレス約 9,000 万件のうち、 ID・パスワードが入力可能であったものが、約 3 万 1,000～4 万 2,000 件、そのうち、ID・パスワードによりログインでき、注意喚起の対象となったものが延べ 147 件ありました。[i]

IoT 機器は、組織の運用管理対象から外されているのか、例えばパスワードが初期設定のまま利用されているなど、基本的な対策が実施されていないことも見受けられます。さらにライフサイクルが長いことから、サイバー攻撃を受けた場合、長期間攻撃を受けていることが発見されない可能性もあります。このような状況を避けるには、IT 部門の担当者だけで管理を行うのではなく、システム運用管理の投資を決定する経営陣も関与し、IoT 機器類の適切な設定やセキュリティー対策の徹底に努めることが重要となってきます。[ii]

NOTICE の結果を受け、政府は 2020 年に向けた包括的なサイバーセキュリティー戦略[iii]を策定しました。その目的は、重要なインフラ対策を改善し、全ての日本企業がベストプラクティスを追求することを奨励し、動機付けすることです。日本の全ての民間企業およびサプライチェーン内のサイバーセキュリティーを改革することが、この計画の中心です。

ベストプラクティスへの三つのアプローチ

日本政府からの指示は、次の三つの広範囲なアプローチに基づいています。

1) **サービス提供者の任務保証** - 業務・サービスの着実な遂行-
組織の経営陣が自ら「任務」として業務やサービスを識別することが期待されています。さらに、これらサービスの信頼性とサイバーセキュリティー向上に向けて努力しなければなりません。その実現のためには、組織はまず、提供するビジネスサービスの中で不可欠なサービスを把握しなければなりません。サプライチェーンパートナーを含めて、これらのサービスの提供に関わるパートナーエコシステムを認識する必要があります。これらのサービスの提供に寄与する関連の IT / OT / IoT 資産をマッピングすることも重要です。これらの資産に対する脅威と脆弱性、緩和策に対する既存の管理、さらにサイバー攻撃の発生に対する準備について、評価も必要です。

2) **リスクマネジメント** -不確実性の評価と適切な対応-
組織の「任務」の内容に応じて、関連するリスクを識別、分析、および評価し、組織がリスクを最小限に抑えることが求められています。組織の全社レベルのリスクマネジメントプログラムおよび ISO 31000 などの業界標準と密接に連携すべき包括的なリスクマネジメント手法の採用が必要です。その目的は、不可欠なサービスに対しリスクを定期的に評価し、そのリスクを特定し、許容可能なレベルまでリスクを低減することです。リスクマネジメントは、サプライチェーン、ビジネスパートナー、IT パートナー、製品およびクラウドベンダーを含む組織のエコシステム全体を網羅します。

3) **参加、連携、協働** - 個人・組織による平時からの対策と連携・協働-
組織や個人がサイバー空間の脅威から、生じ得る損害やその拡大を防ぐために、平時より対策を実施することを想定するものです。情報サービス、業界セキュリティー団体、および政府サイバーインシデント対応チームを始めとする各関係者間の緊密な調整と連携が必要です。各関係者は共に、脅威を理解し、関連情報を交換し、そして既知の/未知のサイバー攻撃を阻止するために連携し、この活動には、多数の関係者の参加、連携や協働が求められます。

この三つのアプローチは、個々の企業内のサイバーセキュリティーの範囲を定めるフレームワークを提供しています。これらのアプローチを現在のサイバーセキュリティー手順に整合させ、日本企業における次世代ベストプラクティスの基礎を形成しなければなりません。ベストプラクティスの導入とコンプライアンスは、企業の投資計画の中核となるものです。

タタコンサルタンシーサービシズ（TCS）では、企業がこのアプローチを運用するための運用指針と、対策の具体例を作成しました。

a. セキュリティ組織に対する経営陣の支援と必要な資金で基本的なサイバー衛生（cyber hygiene）を確立する。具体的には「サイバーセキュリティ経営ガイドライン」に基づいたセキュリティに関する経営陣のコミットと、明確な役割と責任の定義をする。経営者は、同ガイドラインの 3 原則を理解した上で、組織全体のセキュリティに責任を持つ最高情報セキュリティ責任者（CISO：Chief Information Security Officer）を役員または上級管理職の位置に設置し、人や資金等の経営資源を配分する。

b. CISO はセキュリティガバナンスとセキュリティ保証プロセスの構築を実施する。NIST Cyber Security Framework などの世界標準に従って、組織のセキュリティ対策の目標と構造を整備し（同フレームワークであれば、コア、ティア、プロファイル及びそれらを利用した経営と現場の対話）、セキュリティ対策推進を具体的な計画に落とし込む。

c. CISO は計画に従ってポリシーや標準を策定し、企業プロセスへの組み込みを実施する。ポリシー策定には、各業界の規制事項や政府からの要請を把握した上で、ISO 27000 シリーズ、CIS CSC、IEC62443 などの世界標準を活用する。

d. CISO は計画に従った対策推進に責任を持つ。具体的には以下を例とする対策にリソースを割り当てる。

1. 重要なビジネスサービスとそれを支える IT 資産を特定する。関連するセキュリティ管理策を適用して、リスクを許容レベルまで低減する。

2. ゼロデイ攻撃や事前攻撃等のセキュリティ侵入の試みを監視するセキュリティ監視および分析ツールを構築する。

3. ほぼリアルタイムでサイバー攻撃を監視し、それに対応するためのサイバーセキュリティコマンドセンターを設立し、コマンドセンターの一部として予防的な運用（脅威ハンティング）を実施する。

4. オープンソースフィード、ダークウェブやディープウェブなどの商用フィード、さらにその他の独立系企業から関連する脅威情報を特定する方法をまとめる。

5. セキュリティテスト、内部統制テスト、外部統制の検証、および第三者による外部統制の認証などの必要な保証プロセスを考案する。

6. さまざまなセキュリティ団体/コンソーシアム、ISAC、業界/政府 CIRT との関係を構築して、情報を交換し、危機に際し協力を仰ぐ。

7. すべての関連する関係者が参加する組織全体のセキュリティ意識向上プログラムを作成する。訓練と教育の一環として、模擬訓練とソーシャルエンジニアリングキャンペーンを実施する。

TCS が推奨するベストプラクティスの実現に向けて

企業が前述のアプローチを実現するには、サイバーレジリエンスへの投資をすることが必要です。サイバーレジリエンスとは、組織が防御できなかったサイバー攻撃を速やかに検出でき、それに対応し、そのダメージから回復できる能力です。組織はビジネスリスクの一部としてサイバーセキュリティーリスクを考えることで、事業継続計画（BCP：Business Continuity Plan）の一部にサイバーレジリエンスを据え、対策のアプローチを反応的なものから、BCP に従った予測的および予防的なアプローチに変えていくことができます。

また、リスクマネジメントの過程をマッピングする、「ガバナンス、リスクおよびコンプライアンス（GRC）プログラム」も考案しなければなりません。プログラム内の活動には、リスクマネジメント方針、リスクマネジメント基準、定期的なリスクレビュー、リスクを許容レベルまで低減するためのリスク軽減策の実施、報告およびサイバーセキュリティー全体のガバナンスの確立が含まれる必要があります。リスクおよびコンプライアンスプログラムをさらに成熟させるために、リスク評価、監査および管理テスト活動の手作業を自動化する IT GRC ツールの導入も検討すべきです。

さらにリスクマネジメント活動の一部であるサプライチェーンリスクは、ビジネスサービスを提供するためのパートナーエコシステムがますます拡大するに伴い、その重要性が高まっています。従って、サードパーティーベンダーからのリスクを評価し、管理することが不可欠となります。サードパーティーシステムの脆弱性が原因で攻撃を受ける場合もあります。組織は、サプライチェーンにおいてサードパーティーから発生するリスクを評価し、適切に軽減しなければなりません。これらの活動を形式化するために

「ベンダーリスク管理プログラム」を策定することが必要です。製品 OEM およびサービスプロバイダもサプライチェーン全体の中で重要な存在となります。組織は、それぞれの製品およびサービスについてセキュリティーとプライバシーを順守していることを確実に保証しなければなりません。

※　　※　　※　　※　　※

2020 年の東京大会を見据えて策定された日本政府主導の新しいサイバーセキュリティー戦略により、イベントの開催中だけでなく今後何年にもわたりサイバー攻撃から起因するさまざまな危険性を軽減することが期待されています。これを実践する手段の一つとして、TCS では「Business 4.0」の概念を交え、新しい、かつ、安全なテクノロジーを組織のエコシステムに組み込み、スピーディな経営とテクノロジーを柔軟に取り入れるための企業の取り組みを支援しています。

ⅰ 2019 年 6 月 28 日 総務省／国立研究開発法人情報通信研究機構／一般社団法人 ICT-ISAC 報道資料：脆弱な IoT 機器及びマルウェアに感染している IoT 機器の利用者への注意喚起の実施状況

ⅱ 2019 年 6 月 総務省：IoT 機器調査及び注意喚起の実施状況について

ⅲ 2019 年 5 月 23 日 内閣サイバーセキュリティ戦略本部：サイバーセキュリティ 2019（2018 年度報告・2019 年度計画）