SC3 会員及び会員団体所属企業を担う方々

SC3 会長　遠藤 信博
令和 3 年 7 月 7 日

東京 2020 オリンピック・パラリンピック競技大会に向けて
～SC3 会員企業・組織の経営者へのサイバーセキュリティ対策に関するメッセージ～

7 月 23 日～8 月 8 日の日程でオリンピックが、8 月 24 日～9 月 5 日の日程でパラリンピック（以下、「オリパラ」ということがあります。）が開催されます。過去の競技大会でも競技会場やホスト国企業・団体に対するサイバー攻撃が多く観測されており、今般の日本における競技大会中及びその前後の期間において SC3（サプライチェーン・サイバーセキュリティ・コンソーシアム）会員企業・組織を標的とする悪質なサイバー攻撃が多発する可能性は極めて高いと考えられます。

サイバー攻撃に対して適切に対処ができない場合には、事業活動の継続が困難になるなどの深刻な被害を受ける可能性があることに加え、自社のみならず関係する事業者や顧客にまで影響を及ぼすことで、企業の信用問題、即ち、経営責任に直結する重大な問題にもなり得ます。

サイバー脅威が増大し、更に、大きなイベントに関連してサイバー攻撃の増加が懸念される中、改めて経営者が現状のリスクを正確に認識し、経営者の責任において、適切な判断・指揮を取ることが求められます。以下を参考に、SC3 会員及び会員団体所属企業の経営を担う方々におかれては、事案は発生するものと考え、今一度、SC3 規約第 3 条第 1 項に定める「サプライチェーンのサイバーセキュリティ強化のため企業に求められる基本的な行動（①企業間における高密度な情報共有、②機微技術情報の流出懸念がある場合の報告、③多数の関係者に影響する恐れがある場合の公表）」の徹底を含め、十分に備えるようにしてください。

■ サイバー攻撃の経営へのインパクト

- 自社のシステムに障害が発生し、事業が継続できなくなる恐れがある。
- 取引先や顧客に関する情報の漏えいや、自社が取引先等への攻撃の侵入口となり、取引先や顧客に深刻な被害を与えてしまう恐れがある。
- 被害発生に対して、取引先や顧客との適切なコミュニケーション、必要に応じた当局への報告や公表等の正しい対応をしなければ、企業・組織そのものの社会的な信用を失墜させることになる。

■ 想定される攻撃の例

- 標的型攻撃（※）による社内システムへの侵入を通じて、情報を窃取・改ざんされたり、自社システムが攻撃の踏み台とされたりする。
  ※海外拠点や取引先を経由して侵入してくるケースが増加する傾向にあります。
- DDoS 攻撃（分散型サービス妨害攻撃）や、ネットワーク機器の脆弱性等を使ってシステムに直接侵入してランサムウェアなどを仕掛けることにより、システムが停止させられる。ランサムウェア攻撃はシステムを停止させるだけでなく、知的財産情報や顧客の情報が窃取され、オンライン上に漏洩されることで大きな二次被害が出る可能性もある。

- オリパラやワクチン接種を騙る偽アプリや詐欺サイト、フィッシングメール/SMS を通じたアプローチに対して、騙されて情報・金銭が窃取される。

■ **推奨される対策（対策済みであるか、関係部署とコミュニケーションをお願いします。）**

防御力強化のための対策だけではなく、攻撃を受け被害が発生することも想定し、事案が発生した場合に取るべき対策の準備を行っておくことも重要です。

なお、経済産業省からは、昨年 4 月以降、4 度に渡って注意喚起が発出されており（2020 年 4 月 17 日、2020 年 6 月 12 日、2020 年 12 月 18 日、2021 年 4 月 2 日）、こうした注意喚起に推奨される詳しい対策が紹介されており、具体的な対策を検討する際の参考としてください。

防御力強化のための対策

- 内閣サイバーセキュリティセンター（NISC）や情報処理推進機構（IPA）、JPCERT コーディネーションセンター等の専門機関からの注意喚起(末尾参照)を定期的に確認すること。
- オリパラ期間中は、不要なシステムは電源を落としたりネットワークから遮断したりするなど、攻撃の影響を受けない対策を徹底すること。
- 機器・システムに対して、アップデート等の基本的な対策をできるだけ実施すること。ただし、十分な試験をしないままのパッチ適用やシステム変更は、想定外のシステムトラブルを引き起こす可能性があることにも注意すること。
- オリパラやワクチン接種を騙る不正アプリや詐欺サイト、フィッシングメール/SMS に注意すること。
- 社内教育・広報などを通じて、セキュリティに関する社内ルールや、基本動作の徹底を図ること。

上記対策を行った上で、事案発生に備えた準備

- 「おかしい」と思ったら、隠さずに、すぐにシステム担当者やセキュリティ担当者に報告することを社員に徹底すること。
- ランサムウェアの被害に備えて、システムやデータをバックアップし復旧手順を確認すること。
- サイバー攻撃による影響を局所化するために、システムの緊急停止や、インターネット遮断などの緊急対応を実施するための手順、基準、権限を確認すること。
- PC のマルウエア感染やシステムトラブルの発生に備えて、土日夜間を含めた緊急対応のための連絡先を最新化し、連絡手段、社内・ベンダの体制、駆けつけ対応方法を確認すること。
- システムトラブルの長期化に備えて、手動運用などの代替プランを準備すること。
- インシデント対応チーム内で新型コロナウィルス感染者がでる可能性も想定し、事業継続を意識した十分な対策をとること。

そしてオリパラが終わっても

- オリパラ期間が終わっても、脅威環境が好転するかは分からない。「オリパラが終わるまでは特別体制」ではなく、今回の体制・確認を日常の基本動作にしていくこと。
- オリパラ期間に得た経験を活かし、今後脅威が強くなることが予想される事態に向けた備えを検討すること。

■ **政府機関等の注意喚起**

- 内閣サイバーセキュリティセンター（NISC)
  - 注意・警戒情報 https://twitter.com/nisc_forecast
- 独立行政法人情報処理推進機構（IPA）
  - セキュリティ関連情報サイト https://www.ipa.go.jp/security/
  - 情報セキュリティ安心相談窓口 https://www.ipa.go.jp/security/anshin/
  - その他（届出・相談・情報提供）窓口一覧
    https://www.ipa.go.jp/security/outline/todoke-top-j.html
- JPCERT/CC (Japan Computer Emergency Response Team Coordination Center)
  - 注意喚起サイト：https://www.jpcert.or.jp/at/2021.html
  - インシデント対応依頼：https://www.jpcert.or.jp/form/
- 経済産業省
  - 2020 年 4 月 17 日 「産業界へのメッセージ」
    https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/20200417.pdf
  - 2020 年 6 月 12 日 「昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取組の方向性についての報告書」
    https://www.meti.go.jp/press/2020/06/20200612004/20200612004.html
  - 2020 年 12 月 18 日 「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起」
    https://www.meti.go.jp/press/2020/12/20201218008/20201218008.html
  - 2021 年 4 月 2 日 「2020 年 12月18日発出「注意喚起」の Update ～最新事例から得られる教訓」
    https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/006_03_00.pdf