事務連絡

令和３年４月３０日

各局等情報化推進担当課長　殿

デジタルサービス局総務部

情報セキュリティ担当課長

東京2020大会に向けたサイバーセキュリティ対策等について

記

１　概要

本注意喚起は情報資産を所管する者（サイバーセキュリティ管理者及び情報システム管理者）、及び情報システム担当者向け情報になります。

東京2020オリンピック・パラリンピック競技大会の開催を目前に控えていますが、過去にオリンピック開催都市を狙ったサイバー攻撃が多発していることから、所管する情報システムへのサイバー攻撃が通常より増加することが予想されます。

所管する情報システムがサイバー攻撃の標的となるおそれがあるため、情報システムの管理者は、セキュリティ対策の実施やインシデントが発生した際の対処手順を改めて確認することが重要です。

２　サイバー攻撃の例

　　以下のようなサイバー攻撃が想定されます。

1. OSやソフトウェアの脆弱性を突いた攻撃によるWebサイトの改ざん
2. DDoS攻撃によるサービス停止
3. アカウント情報の窃取、不正なログイン試行等による不正アクセス
4. 情報システムを管理する施設・設備等への不正侵入
5. 攻撃の起因となる不審な添付ファイルやリンク先を含んだ標的型メール攻撃

３　対策

以下に記載する対策の実施をお願いいたします。

(1)　脆弱性情報の収集

管理している情報システムに関係する脆弱性情報を収集し、脆弱性の影響を受ける場合はソフトウェアのアップデート等を対応してください。なお、デジタルサービス局により定期的な注意喚起を全庁ポータルのセキュリティ情報にて配信しているため、そちらもご参照ください。

(2)　必要なセキュリティ更新プログラムの適用

ネットワーク機器、ファイアウォール、サーバのＯＳ及びソフトウェア等に最新のセキュリティ更新プログラムが適用されていることを確認してください。

また、Ｗｅｂサーバ上で動作するＷｅｂアプリケーションについても最新のセキュリティ更新プログラムが適用されていることを確認してください。

(3)　アクセス制御情報の確認

情報システムに対するアクセスは最低限となっていることを確認してください。管理用サーバやデータベースサーバ等、通常のアクセスが想定されていない機器については、特に注意してアクセスが最低限となっていることを確認してください。

(4)　不要なアカウントの削除

情報システムにて登録されているアカウントに不要なものがないかを確認してください。サーバやデータベース、ネットワーク機器等の管理に必要な特権アカウントについては特に留意して、情報システムにおいて限定的な登録がされていることを確認してください。

(5)　不要なサービスの停止

サーバ上で不要なサービスが起動している場合、そのサービスの脆弱性等が悪用されるおそれがあります。最低限必要なもの以外は停止してください。

(6)　連絡体制の確認

サイバーセキュリティインシデント等の発生時に備え、外部委託事業者や外部機関を含む連絡網が整備・周知されていることをあらためて確認してください。

(7)　インシデント対処方法の確認

サイバーセキュリティインシデント等の発生時に備え、インシデント対処方法を確認してください。

（例）

・攻撃元IPアドレスからの通信を拒否する方法

・海外IPアドレスからの通信を拒否する方法

・ネットワークの遮断方法

(8)　不信な通信等の確認

不審な通信がないかアクセスログ等を確認してください。

（例）

・システムへのログイン認証エラーの多発や深夜等利用者がいない時間帯のログイン

・サーバやアプリケーション等の脆弱性を狙った痕跡等

・Ｗｅｂサーバで公開しているコンテンツの異常（改ざん、不正なスクリプトの埋め込み、不審なファイルの保存）

・システムから外部へ向けた想定されない不審な通信

(9)　 情報システムを管理する施設・設備等における物理セキュリティの確認

許可されていない者の立入りを防止する等、物理セキュリティが確保されているか確認してください。

【連絡先】

デジタルサービス局総務部企画計理課

情報セキュリティ担当（東京都ＣＳＩＲＴ）  
　市毛、芹澤、田村

メール：S1100102@section.metro.tokyo.jp