CA2061

公共図書館におけるサイバーセキュリティ対策の実践方法について

米田（よねだ）　渉（わたる）*

1. はじめに

本稿は、サイバー攻撃が企業だけでなく病院や図書館といった公共施設にも及ぶこととなった昨今の状況を踏まえ、公共図書館におけるサイバー攻撃の事例と併せ、地方自治体情報システムと比較した公共図書館の図書館システムの特徴を概観し、そのセキュリティ対策を提案するものである。また、公共図書館の運営に係るセキュリティ対策だけでなく、利用者へのリテラシー向上のために公共図書館が気を付ける点についても言及している。

2. 一般的なサイバー攻撃と図書館における被害及び発生事例

独立行政法人情報処理推進機構（IPA）の『情報セキュリティ白書2023』[(1)]で主要なサイバー攻撃として挙げられているものの内、公共図書館に関連のあるものとしては、1）ランサムウェア攻撃、2）標的型攻撃、3）DDoS攻撃、4）Webサイトの改ざん、5）フィッシングと思われる。これらの特徴と図書館における発生事例については、次のとおりである。

2.1 ランサムウェア攻撃

近年のランサムウェアは攻撃者が対象組織のネットワークに密かに侵入し、大量のデータを暗号化するという攻撃となっており、事業継続に大きな影響を与える脅威となっている。急増している理由は、ランサムウェアをサービスとして提供するものが出てきているからである。身代金要求だけでなく、暗号化する前のデータを公開するという二重の脅迫が行われる例もある。

感染経路としては、インターネット上に公開されたVPN機器等の脆弱性や強度の弱い認証情報等を悪用し、ランサムウェアに感染させる手法が多くみられた。それ以外では、攻撃対象組織へ遠隔操作ウイルス等を添付したメールや、遠隔操作ウイルス等をダウンロードさせるURLリンクを記載したメールを送り付けることもある。

国内におけるランサムウェアによる被害は、2022年度と2021年度を比較すると58%増であった。その内団体等の被害は156%増となっている[(2)]。

図書館については、2022年10月に那覇市立図書館[(3)]、同年12月に日野市立図書館[(4)]、また海外では2023年10月に英国図書館（BL）[(5)]が攻撃を受けている。

2.2 標的型攻撃

標的型攻撃は、事前調査、初期潜入、攻撃基盤構築、システム調査、攻撃最終目的の遂行と計画的に行うものである。初期潜入では、事前調査で得られた情報を元に、組織の端末へのウイルス感染を試みる。海外拠点や取引先組織といったサプライチェーン上のセキュリティに弱い組織を狙う手法に加え、VPN製品やWebサーバ等といったインターネットとの境界にある装置の脆弱性を悪用し、侵入する手口もある。攻撃基盤構築段階では、組織内の端末を遠隔操作するため、遠隔操作ウイルスに感染させる。その後、システム調査として、組織内ネットワークの調査、管理者権限の奪取、目的とする情報の探索を行う。攻撃最終目的の遂行では、目的とする情報の搾取等を行う。

海外の事例では、システム破壊を目的とするインフラ攻撃も確認されている。

2.3 DDoS（Distributed Denial of Service）攻撃

DDoS攻撃とは、Webサーバ等の攻撃対象に複数の送信元から同時に大量のパケットを送信することでリソースに負荷をかけ、サービス運用を妨害する攻撃である。VPN製品やルータを悪用したボットネットによる攻撃が増加傾向となっている。

2022年上半期に全世界で確認されたDDoS攻撃は、過去最多となる約602万回と、前年比で205%に増加した。

2019年には、川崎市立図書館において機械的大量アクセスによりホームページ閲覧不可となる障害が発生している[(6)]。

2.4 Webサイト改ざん

アカウントの不正な取得等によるWebサイト改ざんは、2022年度と2020年度を比較すると50%増であった。

公共図書館においては、2016年に宮城県図書館[(7)]、2017年に千代田区立図書館に発生している[(8)]。

2.5 フィッシング詐欺

偽のホームページに接続させる等の方法で、クレジットカード番号やユーザID、パスワードといった重要な情報を盗み出すフィッシング詐欺の報告件数は、2022年度と2020年度を比較すると3倍増であった。

フィッシングサイトのURL件数は2022年度と2017年度を比べると約40倍となっており、情報を詐取す

* 成田市役所，日本図書館協会認定司書2052号（2022.4～2032.3）

る手口はインターネット上に横行していることが分かる。

3. 地方自治体の情報システムの特徴

図書館システムの特徴に触れる前に、地方自治体の情報システムについて概観する。

2015年に起きた日本年金機構での外部からの不正アクセスによる個人情報流出事件[9]後、「LGWAN（統合行政ネットワーク）接続系ネットワーク」と「インターネット接続系ネットワーク」を同一のネットワーク内に設置していたものをLGWAN接続系ネットワーク、インターネット接続系ネットワーク、個人番号利用事務系ネットワークの三層に分離することでセキュリティを強化した。これが自治体情報システム強靭性向上モデルである[10]。

2020年8月に総務省によりこの三層モデルの見直しが行われた。セキュリティ対策を実施した上で、インターネット上のクラウドサービスの活用や、業務端末をインターネット接続系に配置するモデルも示されている[11]。これによりセキュリティクラウドを経て、パブリッククラウドの活用や、テレワークの実施が容易になるものとされている。また、マイナンバー利用事務系では、ガバメントクラウドにより住民基本台帳、戸籍、附票管理システムが標準化されると共に、自治体のサーバ構築運用コストが下がると言われている[12]。

このように地方自治体の情報システムは、国の主導の下に包括的なセキュリティ体制が構築されている。

4. 公共図書館の図書館システムの特徴

図書館システムの特徴として挙げられることは、国や日本図書館協会等の全国レベルでのシステムの標準化や統制がないことである。そして、地方自治体の行政サービスの中では、インターネットサービスが進んでいる分野であり、個人情報が登録されているサーバがインターネットに接続したネットワーク上にあることも特徴である。これは、検索-予約、利用者のページでの貸出期間の延長、予約確認等のため、利用者が自身の登録情報、貸出・予約情報をインターネット経由で閲覧可能とする必要があるからである。これにより、自治体情報システムの三層モデルに準拠した対策が取れず、別の手段によるセキュリティの確保が必要となっている。

サーバの設置場所については、クラウド、データセンター、図書館内（オンプレミス）と、システムの規模や自治体の方針によって異なる設置方法が選択されている。

また、クラウドシステムを活用している場合では、ドメインを「lg.jp」いわゆる「LGドメイン」にし難い問題がある。セキュリティ対策として、本来、地方自治体サービスであればその真正性を保証できるLGドメインで提供されているべきだが、公共図書館（自治体）においては、そのようなセキュリティ意識はさほど高くなく、例えば指定管理者にホームページの運用だけでなく、ドメインも含めたWebサイト自体を用意させている例もある。

そして、自治体直営館の場合は、館に図書館システムのネットワークと、地方自治体庁内システムのネットワークの2系統が分離されて配置されていることが多く、業務委託館や指定管理館の場合は、図書館システムのネットワークと、業者が設置したネットワークの2系統が分離されて配置されているところもある点も特徴であろう。

それ以外の特徴として挙げられるのは、オンプレミスの場合は、独自のシステムを自館で維持管理しているにも関わらず、ネットワークやシステムを理解しているシステム管理者を配置できない館が多いことである[13]。

5. 昨今の公共図書館のシステムの脅威への提言

大石は、現在図書館における危機管理は、物理的、人的な危機への管理が中心で論じられているが、情報セキュリティ管理、対策に力点を置くことが必要と述べている[14]。

6. 公共図書館のシステムの特徴を踏まえたセキュリティ対策

公共図書館で取り得る対策を以下に挙げる。

6.1 インターネットに接続している図書館システムの安全策

6.1.1 ネットワークからの侵入を防ぎ、検知し、リカバリーする仕組み

・調達要件にハードウェア、ソフトウェアの防衛対策（FWの設置、WAFの設置等（IPAの安全なウェブサイトの作り方のチェックポイント[15]等参照））を行う。
・運用期間中はサーバとクライアント、ネットワーク機器のセキュリティアップデートを実施し、端末ごとにネットワークやインターネットへのアクセス制御を行う。
・端末の周辺機器との接続機能の制御（保守等でのアクセスについてはVPNを都度接続とし、通常は切断する等）を行う。
・システムのバックアップ、ジャーナル等のデータの3-2-1対応（データを3種類、メディアを2種類、1

か所別の場所に保管）[16]を行う。また、業務で作成したデータのバックアップも同様の対応を行う。特に別メディアで物理的にネットワークから切り離した状態でのバックアップは重要である。

以上のバックアップ等の対策の前提として、米国の電子図書館連合の収集データのリスク評価ガイドで自館のシステムがどのような利用者データを収集しているのかまとめておくことの必要性を挙げている（E2303参照）ように、どのレベルの個人情報ファイルをどこに保存しているのかを把握、管理していることが必要である。

6.1.2 メールからのマルウェア等の侵入を防ぎ、探知し、リカバリーする仕組み

・職員のリテラシー向上は必要であるが、それのみに頼らず、リスクを下げる仕組みの導入が望ましく、図書館システムのインターネット、又はメールアクセス端末が、図書館システムネットワークとセグメントを分けて構築することを検討する。
・図書館システムベンダーと運用期間中のファイルのやり取りについては、ファイル転送ツールを活用するなど、メール添付ファイルを極力削減するようにする。

6.1.3 ファイルを安全に移動できる仕組み

・図書館システムと庁内システム等との二つ以上のネットワークをまたがってファイルをやり取りすることが実務上必要になっていることが、セキュリティ対策上のポイントである。これについては、ファイルの移動に使う方法とメディアを限定し使用履歴の管理と共に、メディア単位での毎回のウイルスチェックにより運用すること等が考えられる。
・Microsoft Office のファイルは、2007 年以降の拡張子の標準方式に変更して、マクロ付きファイルを分かるようにする。例えば、Word の「.doc」や Excel の「.xls」という拡張子を使用不可とし、マクロ付きファイルが拡張子で明確に分かる運用とするのが望ましい。また、図書館システムベンダー等とのファイルのやり取りがあってもマクロ付きファイルは使用しない等、安全対策を取ることを調達時から要件とすることが望まれる。

6.2 図書館 Web サイトや送信するメール等の安全性の確保

6.2.1 LG ドメインでの図書館 Web サイトの構築

・オンプレミスはもちろんのこと、クラウドのシステムでの調達においても LG ドメインでの構築を進めていく。また、公共図書館のホームページとして使っていたドメインを利用しなくなり放棄したものを第三者が取得して、フィッシング詐欺に利用されるリスクはあるため、LG ドメイン以外のドメインを採用している図書館にはその注意も必要である。

6.2.2 図書館から発信するメールの安全性の確保

・図書館から発信するメールについて URL リンクを付けないこととするよう、フィッシングメールとの違いを明確化することを検討する[17]。これは利用者のリテラシーを向上させる取組みでもある。

6.2.3 パスワード管理等の仕組み

・利用者のページ等の図書館利用に関わるパスワードについて、初期パスワードを生年月日等にしない運用に変えることや、桁数上限をなくすこと、記号を使えるようにすること、最低桁数を 6 桁、できれば 8 桁以上とすることを進める。これも利用者のリテラシーを向上させる取組みである。

7. むすびに

国レベルでは、地方自治体の情報システムの一つとして、セキュリティ対策への情報と、補助等、都道府県立、市町村立図書館を支援する仕組みを構築することが必要である。

また、ネットワークセキュリティ監査、侵入テスト、訓練等についても、国から地方自治体へ実施を促すと共に、予算上の支援を実施してもらいたい。

更に、図書館システムの標準化についても推し進めていってほしい[18]。

これらによって、図書館システム構築のベストプラクティスや、標準的な対応を情報共有できるようになり、より安全な図書館システムの構築に資するだろう。

(1) 情報処理推進機構. 情報セキュリティ白書2023. 2023, 255p. https://www.ipa.go.jp/publish/wp-security/t6hhco00000014r1-att/2023_All.pdf, (参照 2024-03-29).
(2) 第2章でとりあげている数値は脚注1の文献に依る。
(3) 那覇市立図書館. “【緊急】図書館システム障害のお知らせ”. WARP. https://warp.da.ndl.go.jp/info:ndljp/pid/12707186/www.city.naha.okinawa.jp/lib/n-information/20221013.html, (参照 2024-03-29).
(4) 日野市立図書館. “市立図書館におけるコンピュータウィルス感染について(第一報)”. WARP. https://warp.da.ndl.go.jp/info:ndljp/pid/12543962/www.lib.city.hino.lg.jp/news/important/20221219-post_234.html, (参照 2024-03-29).
(5) “Cyber incident update – last updated 18 December 2023”. Knowledge Matters blog. 2023-11-29. https://britishlibrary.typepad.co.uk/living-knowledge/2023/11/cyber-incident.html, (accessed 2024-03-29).
(6) 川崎市立図書館. “川崎市立図書館ホームページでの障害発生について(第2報)”. WARP. https://warp.ndl.go.jp/info:ndljp/pid/11426528/www.library.city.kawasaki.jp/main/0000003151/default.html, (参照 2024-03-29).
(7) “宮城県図書館ウェブサイトの改ざんに関するお詫びとご報告”. 宮城県図書館.

https://www.library.pref.miyagi.jp/latest/news/675-2016-1-14-12-34-38.html,（参照 2024-03-29）.
(8) 千代田区．“千代田区立図書館ホームページの公開停止に関するお知らせ”．WARP.
https://warp.da.ndl.go.jp/info:ndljp/pid/11050096/www.city.chiyoda.lg.jp/koho/bunka/bunka/toshokan/dokushochosa/kokaiteishi.html,（参照 2024-03-29）.
(9) 日本年金機構不正アクセスによる情報流出事案に関する調査委員会．不正アクセスによる情報流出事案に関する調査結果報告．2015, 35p.
https://www.nenkin.go.jp/oshirase/topics/2016/0104.files/F.pdf,（参照 2024-03-29）.
(10) 総務省地域力創造グループ．新たな自治体情報セキュリティ対策の抜本的強化に向けて～自治体情報セキュリティ対策検討チーム報告～．概要版．2015, 6p.
https://www.soumu.go.jp/main_content/000387560.pdf,（参照 2024-03-29）.
(11) “「自治体情報セキュリティ対策の見直しについて」の公表”．総務省．2020-05-22.
https://www.soumu.go.jp/menu_news/s-news/01gyosei07_02000098.html,（参照 2024-03-29）.
(12) 総務省．地方公共団体における情報セキュリティポリシーに関するガイドライン（令和 5 年 3 月版）．2023. 346p.
https://www.soumu.go.jp/main_content/000873096.pdf,（参照 2024-03-29）.
(13) 株式会社三菱総合研究所．“図書館システムの現状に関するアンケート　調査結果～システム経費の負担感大きく、図書館側のIT 人材も不足～”．Internet Archive.
https://web.archive.org/web/20100901104935/http://www.mri.co.jp/NEWS/press/2010/2021657_1395.html,（参照 2024-03-29）.
(14) 大石正人．自分事としてランサムウェア攻撃など情報セキュリティ対策を強化する．図書館雑誌．2023, 117(5), p. 276-277.
(15) “安全なウェブサイトの運用管理に向けての20ヶ条 ～セキュリティ対策のチェックポイント～”．情報処理推進機構．2019-03-06.
https://www.ipa.go.jp/security/vuln/websecurity/sitecheck.html,（参照 2024-03-29）.
(16) Ruggiero, Paul; Heckathorn, Matthew A. Data Backup Options. 2012, 6p.
https://www.cisa.gov/sites/default/files/publications/data_backup_options.pdf,（accessed 2024-03-29）.
(17) “URL リンクへのアクセスに注意”．情報処理推進機構セキュリティセンター．2021-08-31.
https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20210831.html,（参照 2024-03-29）.
(18) 日本図書館協会図書館システムのデータ移行問題検討会編著．図書館システムのデータ移行問題検討会報告書：学習会「図書館システム個人パスワードの管理と移行の課題」記録．日本図書館協会．2019, 83p.,（JLA Booklet, 5）.

［受理：2024-04-10］

Yoneda Wataru

Cyber Security Practices in Public Libraries