セキュリティ総論 D レポート No.7

大学図書館の図書管理システムのセキュリティ分析

慶應義塾大学 理工学部物理学科 61908697 佐々木良輔

1 システムの目的

大学図書館の図書管理システムの主要な目的, 機能は以下の通りであると考えられる.

蔵書管理 所蔵されている図書の配架, 貸出状況をデータベース (蔵書 DB と呼称) で管理する.

貸出, 返却 蔵書の貸出, 返却処理を行い, 蔵書 DB を更新する.

配架移動 蔵書を現在の書架から別の書架に移動し, 蔵書 DB を更新する.

予約 蔵書の予約を受け付ける.

表示 蔵書の状況 (配架場所, 貸出中, 予約中) などを表示する.

2 業務の特性から特に注意すべき事項

前節で述べた通り, 本システムの目的は蔵書を管理することである. 図書館の利用者は学生などの図書館利用者及び司書となり, それぞれ以下のようなユースケースが考えられる.

1. 図書館利用者
   (a) 蔵書の閲覧
   (b) 蔵書の貸出, 返却
   (c) 蔵書の予約
   (d) 蔵書の取り寄せ
   (e) 蔵書の状況の検索 (web システム)
2. 司書
   (a) 貸出, 返却処理
   (b) 返却された蔵書の配架
   (c) 取り寄せされた本の書架移動
   (d) 蔵書の状況の検索

特に 1.(a), 1.(b), 2.(a), 2.(c) などの機能を実現するには蔵書 DB に記録された配架状況が現実の

蔵書の配架状況と一致している (完全性) が担保されている必要がある．この完全性が担保されていない場合, 図書に対する可用性も同時に損なわれる．

3　保有資産情報

本システムの保有する情報は前節で定義した蔵書 DB に集約される．蔵書 DB は具体的に以下の情報を保有する．

蔵書の配架状況　蔵書がどの書架に配架されているか, あるいは貸し出されているか.
蔵書の情報　蔵書のタイトルや著者. また図書分類や貸出の可否 (これらは配架とも関連する).
蔵書の予約状況　蔵書が予約されているか.
蔵書の取り寄せ状況　蔵書がどこで取り寄せられ, どの書架に移動が必要か.
利用者情報　蔵書の貸出情報と紐付けられる利用者の情報 (氏名, 学籍番号など).

これらの情報によって蔵書が現在どこにあり, 今後どこに移動するべきかを判断できる．利用者情報は個人情報を含む場合があり, 秘匿性が担保されるべき情報である．それ以外の情報は前節で述べたとおり, 実際の蔵書の情報と一致させるべき情報である．

4　想定される脅威

本システムにおけるトップ事象として以下が考えられる．

貸出, 閲覧の障害　蔵書 DB と実際の蔵書の状況の乖離,web システムの障害
検索, 予約の障害　web システムの障害
個人情報の流出　システムに対する攻撃, 盗聴

したがって本システムのセキュリティを考える上で重要な脅威は以下のようなものが考えられる．

1. 蔵書 DB の改ざん
2. 貸出手続きを経ない蔵書の持ち出し (盗難)
3. 他の利用者 ID での利用 (なりすまし)
4. web システムに対する妨害
5. 個人情報の盗聴, 漏洩

ここで盗難やなりすましは攻撃者が実際に図書館に出向く必要があり, 攻撃者一人あたりが持ち出せる本の数がそこまで多くないことから数量的に見れば影響は比較的小さいと考えられる．一方で蔵書 DB の改ざんや web システムに対する妨害, 個人情報の盗聴, 漏洩は影響が蔵書全体や利用者全体に広がり得る．

しかし蔵書 DB が改ざんされた場合はバックアップなどが存在すれば復旧の可能性があるのに対して, 盗難の場合は蔵書の再購入などが必要になる．この費用を蔵書 DB の改ざんやシステムが

攻撃された場合の費用と比較しないことには影響度の単純な比較は困難である.

5 想定される脆弱性

前節で議論した脅威について, 関連しうる脆弱性は以下のように考えられる.

SQL インジェクション
: SQL インジェクションを用いて蔵書 DB を書き換えることで, 実際の蔵書状況と蔵書 DB を乖離させることができる

コマンドインジェクションなど任意コード実行が可能なもの
: 任意コード実行が可能な脆弱性がある場合, 蔵書 DB の改ざんや web システムに対する妨害, また個人情報の漏洩などが起こりうる.

盗難防止ゲートの透過
: 図書館には出入り口に盗難防止ゲートが設置されているが, 蔵書のタグを取り外したり, 金属製の容器にしまうことで盗難防止ゲートを通り抜けできる可能性がある. 盗難が成立した場合, 実際の蔵書状況と蔵書 DB を乖離させることができる.

なりすまし利用
: 図書館の貸出, 返却処理時の本人確認は学生証で行われる. 職員による本人確認が不十分な場合, 別人の学生証を用いて不正に貸出などを行われる可能性がある.

クロスサイトスクリプティング
: web システムに XSS 脆弱性がある場合, 攻撃者が利用者になりすまして予約処理などを不正に行うことができる.

以上の脆弱性の中で盗難防止ゲートの透過は現在のシステムでは防御することが出来ず, 最も脆弱な状態に思える. 対して SQL インジェクションや任意コード実行脆弱性などは, セキュリティ対策ソフトウェアやシステムの更新によって防御が可能である.

6 リスクシナリオと対策

以下で想定されるリスクシナリオと対策を述べる.

6.1 盗難

6.1.1 シナリオ

前節で述べた通り, 蔵書に対する加工や金属製容器の利用などによって盗難防止ゲートが透過され, 蔵書を盗難される可能性がある.

6.1.2 頻度

この攻撃にはセキュリティに関する高度な知識は必要なく, 潜在的な攻撃者が非常に多く存在するため頻度は大きいと考えられる. また本が数冊抜き取られていても, その本を利用したい別の利用者が現れるまでは被害に気づけない可能性がある.

6.1.3 起こりうる影響

盗難によって蔵書 DB 上は存在する本が実際には存在しないという状況が発生しうるため, 閲覧や貸出などの図書館の基本的な機能に影響を与える. また, 盗難された本は再購入が必要になる. 一方で多くの本を同時に盗難することは困難なことから, 冊数で言えば影響は少ないと考えられる.

6.1.4 対策

国立国会図書館での例を挙げる. 国会図書館では貴重品を除き荷物は施設外のロッカーに預ける必要がある. これによってゲートを透過するための金属容器などの持ち込みを防止することができるものと考えられる. また国会図書館は本の多くが書庫に格納され, 閲覧, 貸出時には必ず記録が残るため, 盗難防止タグの加工などをしても直ぐに犯人が特定できる.

大学の図書館において, 金属製容器などの不審物の持ち込みを制限することは対策として有効に思える. 一方で蔵書をすべて書庫に移すのは莫大な時間とコストがかかるため困難に思える. しかし大学図書館では入退場の記録が残っているため, 施設内で盗難防止タグに対する加工や万引きが行われたとしても, 防犯カメラなどが設置されていれば入退場記録と照らし合わせることで犯人を特定できる. 以上から大学図書館での現実的な盗難対策としては

- 不審物の持ち込み禁止
- 防犯カメラの設置

などが考えられる.

6.2 なりすまし利用

6.2.1 シナリオ

攻撃者が他人の学生証を利用して貸出処理を行うことで, 蔵書が不正に持ち出される可能性がある.

6.2.2 頻度

この攻撃にはセキュリティに関する高度な知識は必要ないが, 他人の学生証を入手する必要があるため, 攻撃は多少困難に思える. 一方で友人同士で学生証を貸し借りするような場合は, 比較的容易に攻撃が行われる可能性がある.

6.2.3 起こりうる影響

なりすましが可能な場合, 責任追跡性や否認拒否性が著しく損なわれる. またなりすましは結果的に盗難に繋がりうるため, 前節で述べた盗難による影響と同様の影響が起こりうると考えられる.

6.2.4 対策

根本的な対策として学生証が他人の手に渡る自体を避ける必要がある. これにはすでに行われていることではあるが, 学生に対して学生証の貸し借りを避けるよう呼びかけることや, 学生証を紛失した場合早めに申告することが対策になる. また図書館の職員も学生証の顔写真による本人確認を厳粛に行うことで対策になる. 以上から

- 学生証の取り扱いにたいする周知
- 本人確認の厳格化

が対策として考えられる.

6.3 個人情報の盗聴, 漏洩

6.3.1 シナリオ

図書館 web システムを模したフィッシングサイトなどにより keio.jp アカウントが盗聴され, 紐付けられた個人情報が漏洩する可能性がある.

6.3.2 頻度

攻撃にはある程度のセキュリティに関する知識が必要だが, keio.jp を模したフィッシングサイトはすでに何件か報告されており, 攻撃自体は頻繁に行われているものと考えるべきである.

6.3.3 起こりうる影響

keio.jp アカウントには Google Workspace や本名, 授業支援システムなど非常の多くの情報が紐付けられているため, 漏洩は蔵書管理システムに限らず甚大な影響を引き起こしうる. 当然蔵書管理システムに関してもなりすましによる予約や貸出履歴の流出などの影響が起こりうる.

6.3.4 対策

システム管理者側には利用者に対するフィッシング詐欺対策の周知や,XSS 対策, 証明書の適切な運用などが求められる. また利用者側も管理者からの周知を受け, 偽造されたサイトにアクセスしていないか注意する必要がある. 以上から

- 利用者に対するフィッシング詐欺対策の周知
- XSS 対策
- 証明書の適切な運用

が対策として考えられる.