参考資料２

民事訴訟の IT 化に伴うセキュリティについて

湯淺　墾道（情報セキュリティ大学院大学）

1.　諸外国の訴訟システムにおけるインシデントの事例

1.1.　アメリカの連邦民事訴訟関係書類の電子閲覧システムである PACER の障害

2014 年 1 月にシステムが約 4 時間停止し、その間ユーザーがアクセスできなくなるという障が発生
障害の原因としては、DOS (Denial of Service attack)攻撃を受けたとみられる
2017 年 2 月には、PACER の脆弱性が判明
クロスサイトリクエストと呼ばれる攻撃に弱いというもので、この攻撃によってデータ漏えい、なりすまし、アプリケーションデータの読み取り等の被害が発生
本来はユーザーが有償で PACER からダウンロードする各種の書面類を、無償でダウンロードできることが判明

1.2.　ジョージア州のアトランタ市への大規模なサイバー攻撃

ジョージア州のアトランタ市が大規模なサイバー攻撃を受け、市の重要システムの多くが被害を受け裁判所システムも停止
ランサムウェアと呼ばれる身代金型コンピュータウィルス
Atlanta Municipal Court では、電子令状発付システム、訴訟手数料の電子納付システム、交通違反反則金電子納付システムが使用できなくなったほか電子的に管理された裁判手続のスケジュール情報も参照できなくなり、書面や対面による手続に切り替え
裁判のスケジュールはすべて再設定せざるを得なくなるなど、影響は長期化

2.　サイバー攻撃への対処

2.1.　アメリカの事例

アメリカの州裁判所管理者会議(Conference of State Court Administrators, COSCA)、全国裁判所管理協会(National Association for Court Management, NACM) 及び全国州裁判所センター(National Center for State Courts, NCSC)の合同技術委員会が「サイバー攻撃への対処」を採択
サイバー攻撃による被害の発生を防止と、実際にインシデントが発生する場合を予期してそれに対処する組織や手法を事前に整備しておくことの重要性を指摘

2.1.1.　事前段階

- 裁判所のデータ資産の確定

漏えい・滅失した場合に被害が生じる文書やデータ類（裁判官の命令、証人尋問録、デジタル証拠、個人情報など）の確認と、漏えい・滅失した場合の被害の予測。

- ログ取得及びモニタリング体制の整備

アクセスログを取得し、不正なアクセスやデータの異常な送受信についてモニタリングする体制の整備。

- データ収集及びプライバシー保護に関する法令の遵守

データ収集及びプライバシー保護に関する連邦法及び州法（漏えい時の通知義務を含む）を遵守する体制の確立。

- 予想される攻撃の可視化

どのような攻撃が行われる蓋然性が高いかを分析し攻撃を可視化することにより、脅威分析に基づくシステムのアップデートを実施。

- システムのベンダーとの契約の確認

サイバー攻撃によりインシデントが発生した際の責任分担について、ベンダーとの契約書を確認。

2.1.2. インシデント対処

裁判所特有の組織の性質や法律上の制約・義務を勘案して裁判所独自のインシデント対処計画を立案する必要があると指摘
裁判所独自の対処計画について「ABCD 対処」と名付けている

- A Assess the situation

インシデントの性質、範囲等についての確定

- B Block further damage

被害拡大の防止

- C Collect evidence

フォレンジック・イメージ作成、メディアの保護、アクセスの一時的制限、被害の連鎖の確定

- D Disseminate information

裁判官への通知、職員への通知、警察への連絡と捜査要請、当事者への通知、メディア対応

2.1.3. インシデントが発生した場合

- サイバーセキュリティ・インシデント・レスポンスチームの編成

最高裁判所長官、裁判所事務局 CEO、CIO（最高情報責任者）、IT セキュリティ専門家、弁護士らによるレスポンスチームをあらかじめ編成し、インシデント発生時にはこのチームが対応を主導する。

- 連絡手段の収集

サイバー攻撃によって電子メール等が使用できなくなることが考えられる。このため、関係者（訴訟当事者、ベンダー、警察等）の二次的な連絡手段をあらかじめ集取しておく必要がある。

3. 民事訴訟の情報セキュリティ水準の設定に当たって考慮すべき点

情報セキュリティに関するレベルは、民事訴訟に関するさまざまな段階・場面で異なる
訴訟の各手続、プロセスごとに、CIA 概念にも即しながらセキュリティレベルを検討する必要
サイバー攻撃を受けるのは裁判の電子化システムだけではなく、当事者も含まれることに留意する必要
代理人がサイバー攻撃を受けて訴訟関係情報が流出する、ランサムウェアに感染して開くことができなくなる等の事態を想定する必要

3.1. Confidentiality 機密性

アクセス制限、不正アクセスの防止、内部からの情報流出の実施等によって機密性の維持が強く要請される

- 作成途中の裁判官の判決文、メモ等
- 裁判官同士の評議の秘密（裁判所法 75 条）
- 証拠
- 非公開で行われる審理の関係者のプライバシー、審理内容
- 非公開で行われた審理の書類
- 知的財産、営業秘密等に係る情報
- 原告・被告の利益に係る情報
  - 個人情報、プライバシー情報（戸籍や住民票、送達関係書類）
- 訴訟記録（閲覧等制限あり）
  - 謄写は当事者と利害関係人のみが可

3.2. Integrity 完全性

- 改ざんの防止
- 否認の防止
- 情報の滅失の防止

3.3. Availability 可用性

- システム障害時の対応を想定する必要

3.4. 検討のプロセス

民事訴訟において必要となる手続・フローの整理
それぞれについて具体的実現手段を技術的に検討した上で、それによって生じうるリスクと対策、セキュリティインシデントが発生した場合の対応策をあらかじめ考慮しておくことが有用ではないか

法令の要求	民事訴訟法等により要求される手続内容の明確化。
実現手段	民事訴訟法等の要求を遵守しつつ、電子的に代替する手段の技術的検討。
関係者の確定	当該手続に関わる関係者の確定と、それに基づくアクセス権限の設定。
リスク・脅威	当該手続に関わるリスクや脅威の分析。サイバー攻撃、システムの脆弱性、内部要因（人的要因）等を総合的に分析する必要がある。
対応策	リスクや脅威への対応策の事前策定。
被害発生時の対応	文書が滅失した、秘密とすべき情報が漏えいした等の被害が実際に発生した場合の対応手続の明確化。

4. サイバーセキュリティ基本法との関係

4.1. 政府統一基準群に関する問題

サイバーセキュリティ基本法の諸規定は、原則として行政機関等を対象とした構造

第 11 条では国の責務として行政組織の整備等を規定

「国は、サイバーセキュリティに関する施策を講ずるにつき、行政組織の整備及び行政運営の改善に努めるものとする。」とされており、この中にはいわゆる司法行政は含まれないと解するのが自然

第 12 条では国はサイバーセキュリティ戦略を策定しなければならないとしているが、戦略に定める事項として「国の行政機関等におけるサイバーセキュリティの確保に関する事項」（第 2 号第 2 号）を列挙

ここでは立法府及び司法府は対象外

サイバーセキュリティ基本法第 25 条第 1 項第 2 号は、サイバーセキュリティ戦略本部に対して、国の行政機関等のサイバーセキュリティに関する対策の基準を作成するように求める

2018 年 7 月 25 日、サイバーセキュリティ戦略本部は「政府機関等の情報セキュリティ対策のための統一基準群」（以下「統一基準群」という。）を決定

同基準群は、明確に適用対象を「サイバーセキュリティ基本法（平成二十六年法律第百四号。以下「法」という。）第二十五条第一項第二号に定める国の行政機関、独立行政法人及び指定法人（以下「機関等」という。）」に限定（政府機関等の情報セキュリティ対策のための統一規範第 1 条）

司法府に属する民事訴訟の IT 化システムは独自にセキュリティ対策を行わなければならないということを意味するが、統一基準群に準拠すべきか

4.2. GSOC に関する問題

内閣官房に設置された内閣サイバーセキュリティセンター（NISC）

政府機関情報セキュリティ横断監視・即応調整チーム（GSOC）を運用し、政府機関の情報セキュリティを常時監視する体制を整備

GSOC の監視対象は国の行政機関と独立行政法人､政府機関と一体となって公的業務を行う特殊法人等に限定

GSOC の監視下に入れない場合は、独自にセキュリティオペレーションセンター(SOC)等を設置することを検討する必要があるのではないか

5. その他

民間事業者の提供するサービスを利用することは、グローバル企業が有する高いセキュリティ技術を利用できるという利点

当該事業者が訴訟当事者になった場合を考慮する必要

データ管理部門と訴訟担当部門との完全な分離が求められる

訴訟後のサービス提供民間事業者におけるデータの取扱いとその確保について検討する必要

いわゆる「ベンダーロック」を防止するための方策について検討する必要

以上