2021 年 4 月 16 日

民事訴訟の IT 化とセキュリティ

湯淺　墾道
（明治大学公共政策大学院ガバナンス研究科）

1　セキュリティの概念

1992 年　OECD 情報セキュリティガイドライン[1]

Confidentiality（機密性）

Integrity（完全性）

Availability（可用性）

日本産業規格（旧・日本工業規格）JIS Q 27002「情報セキュリティマネジメントの実践のための規範」

情報セキュリティ：「情報の機密性、完全性および可用性を維持すること」、「さらに、真正性、責任追跡性、否認防止および信頼性のような特性を維持することを含めてもよい。」

Confidentiality（機密性）

日本産業規格（旧・日本工業規格）JIS Q 27002「情報セキュリティマネジメントの実践のための規範」

「情報へのアクセスを認められた者だけが、その情報にアクセスできる状態を確保すること」

Integrity（完全性）

情報および処理方法が正確かつ完全であることの保護[2]。

情報の不正な改竄がないこと、情報処理結果の誤りがないこと、情報に欠損がないこと[3]

Availability（可用性）

JIS Q 27002「情報へのアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保すること」

---

[1] OECD, OECD GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS (1992), http://www.oecd.org/internet/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm.

[2] OECD ガイドラインにおいては、integrity について、「データ及び情報の性質が正確で完全であり、かつ正確性及び完全性を保護すること」と定義している。*Id*. at III.

[3] 情報セキュリティの領域における integrity の定義の変遷については、岡村久道『情報セキュリティの法律（改訂版）』（商事法務、2011 年）2 頁以下を参照。

2　従来の実証実験等

裁判所

Lotus Notes を用いたデータベース化等

司法制度改革と先端テクノロジィ研究会

「サイバーコート」

法のライフライン・コンソーシアム

「法律サービスにおける ICT 利活用推進に向けた調査研究調査研究報告書」（2010 年）

なりすましの防止（本人性の確保）

改ざんの防止等

当事者が裁判所へ提出する訴訟資料を、申立行為（を行うために裁判所に提出する訴訟資料。訴状その他）、主張その他の陳述（を行うために裁判所に提出する訴訟資料。準備書面その他）、証拠の 3 種類に大別

申立行為関係と申立行為関係については、必ずしも高度なセキュリティは要求されない

「裁判官や裁判所職員が作成する一定の書面につき、記名押印・署名押印が要求されるものや、当事者が提出した訴訟資料を訴訟記録として正式に扱うに際しては、電子署名を用いた真正性担保がなされるべき」

訴訟記録の長期保存「その真正性を担保するために、裁判所書記官の電子署名を必要とすべきである。」

「裁判所が作成する情報には、一般に改ざんの余地を最小限にしなければならない」、「裁判所内で用いられる押印についても、さらにその性質に応じて区別を行う必要がある。」

「裁判長の認印は、決済的機能を持つ」ので、電子署名を付与すべきであるかどうかの検討が必要

3　民事訴訟システムとセキュリティ

インシデントの実例

PACER の障害

2014 年 1 月　システムが約 4 時間停止

DOS (Denial of Service attack)攻撃を受けたとみられる[4]

[4] Debra Weiss, *Was Pacer shutdown due to a cyberattack? Group claims responsibility,* ABA

2017 年 2 月　PACER の脆弱性が判明[5]

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

2018 年 3 月　ジョージア州のアトランタ市が大規模なサイバー攻撃

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感染

Atlanta Municipal Court

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

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った

アメリカ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

2016「サイバー攻撃への対処」

サイバー攻撃による被害の発生を防止

サイバー攻撃を受けて被害が発生することを前提とした事前の対処計画の重要性を指摘

裁判所のデータ資産の確定、ログ取得及びモニタリング体制の整備、データ収集及びプライバシー保護に関する法令の遵守、予想される攻撃の可視化、システムのベンダーとの契約の確認、サイバー攻撃を受けた場合の対処計画

裁判所独自のインシデント対処計画「ABCD 対処」[6]

日本経済再生本部　裁判手続等の IT 化検討会「裁判手続等の IT 化に向けた取りまとめ」[7]

情報セキュリティ水準と情報セキュリティ対策（本人確認、改ざん・漏洩防止等）は、訴訟の各手続段階や訴訟記録等である情報の内容、性格等により異なるので、適切な水準と対策が必要

証拠の電子化に対応し、改ざん防止のためのデジタル･フォレンジック技術（電磁的記録の調査･解析等を通じ、その調査・分析を行う技術・手法）の活用等

JOURNAL, JAN 27 2014, http://www.abajournal.com/news/article/was_pacer_shutdown_on_friday_due_to_a_cyberattack_group_claims_responsibili/.

[5] Zeljka Zorz, *PACER vulnerability allowed hackers to access legal docs while sticking others with the bill*, https://www.helpnetsecurity.com/2017/08/10/pacer-vulnerability/.

[6] 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）

[7] http://www.kantei.go.jp/jp/singi/keizaisaisei/saiban/pdf/report.pdf

経済社会一般で通用している IT 技術や電子情報に対する信頼性等を前提とする制度設計

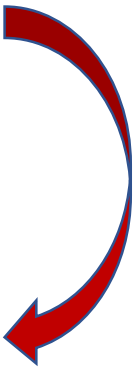
API 連携（複数システム間の連携や外部サービスの機能活用・共有等）、クラウド化、データ形式のオープン化等の様々な可能性を検討

民事訴訟における手続とセキュリティの考え方

民事訴訟において必要となる手続・フローを整理

民事訴訟法等により要求される手続内容の明確化

検討項目	検討内容
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。
セキュリティ対応策	リスクや脅威への対応策の事前策定。 多様なセキュリティ対策技術、各種サービスの中から適切な対策の選定。
被害発生時の対応	被害を生じさせるインシデントの可及的迅速な検知（SOC の設置）。 被害拡大の防止。 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。



検討が必要となる点

セキュリティ水準の設定

デジタル・フォレンジック技術の利用を前提としたメタデータの保存

プライバシー保護

本人確認とアクセス制限

民間事業者の提供するシステムを利用する場合の SLA、当該事業者が当事者となる場合の措置、ベンダロック

5　政府におけるセキュリティ対策との関係

2014 年サイバーセキュリティ基本法

原則として行政機関等を対象とした構造

第 11 条「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。」

第 12 条　サイバーセキュリティ戦略「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」立法府及び司法府は対象外

第 25 条第 1 項第 2 号　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

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

GSOC

内閣サイバーセキュリティセンター（NISC）において運用されている政府機関情報セキュリティ横断監視・即応調整チーム[8]

「サイバーセキュリティ戦略」（平成 30 年 7 月 27 日閣議決定）

「政府機関等と GSOC による効果的かつ効率的な連携の高度化による横断的な対応の発展を目指す」

政府機関の情報セキュリティを常時監視

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 の監視下に入れることが可能かの検討、できない場合には独自にそれに代わる監視体制を整備

6　民事訴訟における AI の利用とセキュリティ

利用可能性の研究

多様な情報の処理

メールの自動分類、メールや文書の自動発出、文書類の分類や適格性の判定

助言

カナダの Civil Resolution Tribunal (CRT)など

予知・予測

裁判官支援 Correctional Offender Management Profiling for Alternative Sanctions

[8] https://www.nisc.go.jp/conference/cs/taisaku/ciso/dai05/pdf/05shiryou0101.pdf

（COMPAS）
州裁判所の一部（ニューヨーク、ウィスコンシン、カリフォルニア、フロリダ等）で、裁判官が有罪判決を出すに当たり、AI が判断した再犯可能性を参考
リスク分析ツール、被告人の再犯確率の予想を行い、裁判官による量刑の決定を支援
批判（バグ、非透明性、適切でない学習、人種やジェンダーバイアス）

7　訴訟代理人のセキュリティ

サイバー攻撃（マルウェア感染、不正侵入）
内部要因（設定ミス、誤操作、紛失、盗難等）
漏洩、流出、滅失発生時の責任
個人情報保護法とベネッセ事件における注意義務
不正競争防止法（限定提供データ）
Cybersecurity due diligence

参考

湯淺墾道「民事訴訟手続の IT 化にデジタル・フォレンジックはどう活かされるか」安冨潔・上原哲太郎編『基礎から学ぶデジタル・フォレンジック』（日科技連、2019 年）171 頁以下
湯淺 墾道「デジタルトランスフォーメーション時代の本人確認の意義と課題」月報司法書士 573 号（2019 年）
湯淺墾道「裁判手続と IT 化の重要論点(NUMBER 009)民事訴訟の IT 化を実現するシステムとセキュリティ」ジュリスト 1552 号（2020 年）
湯淺墾道「訴訟記録のデジタル化とその利活用範囲」法とコンピュータ　次号掲載予定