情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

2019年12月10日（火）

民事訴訟手続のIT化とデジタル・フォレンジック

湯淺　墾道
情報セキュリティ大学院大学　教授

裁判手続等のIT化検討会における検討

「裁判手続等のIT化に向けた取りまとめ」

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 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
- 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
- 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

外国における訴訟ITシステムに対するサイバー攻撃

PACER

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■2014年1月

- ●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害
- ●DOS (Denial of Service attack)攻撃が原因

■2017年2月

- ●クロスサイトリクエスト攻撃に弱い脆弱性が判明
- ●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
- ●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

Featured news

- Europol: Spear phishing the most prevalent cyber threat affecting orgs across the EU
- People are the very first element in a pragmatic cybersecurity strategy
- Organizations fail to maximize use of Microsoft 365 security features
- Companies should disclose cybersecurity risk management efforts
- Risky transactions on mobile devices increase 138% since 2017
- Together, AI and the IoT are having a bigger-than-expected impact
- Whitepaper: SIEM + Threat Intelligence
- Keeping up with the evolving ransomware security landscape
- New infosec products of the week: November 1, 2019
- How has your organization's risk level changed in the past 12 months?
- IT teams are embracing intent-based networking, investing in AI technologies
- Security services and network security still top spending priorities for CISOs in MENA

Zeljka Zorz, Managing Editor
August 10, 2017

Share

PACER vulnerability allowed hackers to access legal docs while sticking others with the bill

A CSRF flaw that made it possible for attackers to access court documents on the PACER system while making legitimate users pay for it has finally been plugged.

What is PACER?

PACER is an electronic public access service of United States federal court

https://www.helpnetsecurity.com/2017/08/10/pacer-vulnerability/

ジョージア州

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■2018年3月

- ●アトランタ市が大規模なサイバー攻撃を受ける
- ●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に大規模感染
- ●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不能
  - ◆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不能

サイバー攻撃への対処

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■2016年

- 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
- 「サイバー攻撃への対処」
- 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

■サイバー攻撃を受ける前の段階

- ●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
  - ◆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
  - ◆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

■裁判所独自の対処計画（ABCD対処）

- ●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

■攻撃後の対処

- ●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
- ●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
  - ◆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収集