開催報告書

文教サイバーセキュリティボードメンバー会 第 0 回

令和 7 年 3 月　Japan Education Community

1. 開催概要

名称	文教サイバーセキュリティボードメンバー会 第 0 回
開催日	令和 7 年 3 月 25 日 / 3 月 27 日（各日前半・後半の 2 部構成）
開催場所	東京都内（クローズド環境）
主催	Japan Education Community
目的	文教機関のサイバーセキュリティ課題に関する現場レベルでの共有・情報交換（ベンダー提案主体とせず、ユーザーである大学側の実態と課題を中心とする会）
運営方針	チャタムハウスルール適用（発言者・所属組織を特定する形での外部公開を禁ずる）

2. 参加概要

本会は、実効性のある議論を行うため、特定の大学に限定した少人数制のクローズドミーティングとして実施しました。参加機関は学校規模・設置形態ともに多様であり、以下の規模感の大学が参加しました。

開催日	参加機関（学生規模）
3 月 25 日	学生規模 約 8,000 名の理工系大学 ／ 学生規模 約 8,000 名の総合大学 ／ 学生規模 約 26,000 名の大規模総合大学 ／ 学生規模 約 2,000 名以下の体育系単科大学（主催校）
3 月 27 日	学生規模 約 13,000 名の総合大学 ／ 学生規模 約 10,000 名の総合大学 ／ 学生規模 約 5,000 名の女子大学 ／ 学生規模 約 2,000 名以下の体育系単科大学（主催校）

3. アドバイザー

本会では、以下のアドバイザーが参画し、議論・知見の提供を行いました。

氏名	所属・役職
諸角 昌宏 氏	日本クラウドセキュリティアライアンス（CSA Japan）理事
大越 いづみ 氏	チェンジホールディングス株式会社 執行役員
斯波 彰 氏	NTT ドコモビジネス / IPA 10 大脅威選考委員

4. 会の構成・運営方針

前半（参加大学のみ）

各大学のセキュリティ担当者のみで、「セキュリティあるある」や直近発生したインシデントの共有を実施しました。

後半（全体ディスカッション）

アドバイザーも交え、前半で出た課題に対する深掘りディスカッション、技術的助言、および事例紹介を実施しました。

5. 主要議題と議論の要点

各参加機関より共有された実態およびインシデント事例は多岐にわたりました。本項目では個別機関を特定しない（匿名化）形式にて、主な議論の要点を整理します。

(1) VPN・認証周りのインシデント事例

- 複数機関で VPN アカウントの ID・パスワード漏えいおよびそれを利用した不正アクセス事例が報告されました。
- 海外出張中ユーザーの接続元監視において管理の死角が生じていたケースが指摘されました。
- Active Directory（AD）に対する不審なクエリを端緒として、システムへの侵入を検知した事例が報告されました。
- 卒業生のアカウントが有効なまま残存し、VPN 認証を通過できる状態になっていた事例が確認されました。

【対策の方向性】多要素認証（MFA）の強制適用、AD の最新バージョンへの移行、パスワード漏えい監視サービスの導入が有効な対策として共有されました。

(2) 外部委託先経由のサイト改ざん・侵害

- 大学サイトの外部委託先、さらにその再委託先のアカウントが侵害され、大学関連サイトが改ざんされる事案が発生しました。

- 文部科学省への規定に基づく報告（第 1 報〜第 4 報等）が求められ、事態の収束まで約 1 ヶ月を要した事例が共有されました。
- 外部委託先との契約においてセキュリティ要件や再委託時のルールが不十分な場合があり、サプライチェーンリスクの管理が急務であることが指摘されました。

(3) フィッシング・Teams 悪用・サポート詐欺

- Microsoft Teams の外部チャット機能を悪用し、学内者に不審な金銭要求メッセージが送付された事例が複数報告されました。
- 教職員が「サポート詐欺」に遭い、プリペイドカード購入直前まで誘導された事例がありました。
- フィッシングメールの文面精度が年々向上しており、標的の関心事に合わせた巧妙な文面が用いられていることが共有されました。

(4) 文部科学省等への報告対応の実態と負荷

- 軽微なインシデントであっても監督官庁への複数回の報告が必要となり、現場の対応負荷が極めて高い現状が訴えられました。
- インシデントの「クローズ判断（収束の基準）」が不明確であり、行政との折衝が長期化するケースが散見されます。
- 報告における「透明性」と「誠実な対応姿勢」が何より重要であるとの共通認識に至りました。

(5) 大学組織特有の「統制困難性」

- 私有端末の業務・学習利用（BYOD）が前提となっており、アクセス端末やブラウザを一律に制限することが技術的・運用的に極めて困難です。
- 教員や研究室ごとに独自の運用環境を構築しており、「研究活動の自由度」を担保しつつセキュリティを強化することの難しさが浮き彫りとなりました。
- 管理すべき対象が専任教職員のみならず学生・卒業生・非常勤講師・外部委託業者など広範にわたり、一律の企業型ガバナンスが通用しない環境にあります。

(6) 教育・訓練の取り組みと限界

- 年 1 回の教職員向けセキュリティ研修を実施しているものの、「他人事」として受講されがちであり、行動変容に結びついていない懸念が挙げられました。
- 標的型攻撃メール訓練を年 2 回実施している機関では、依然としてクリック率が 8〜9%程度で推移しているとの実証データが示されました。
- 【啓発の転換】「自分が被害者になる」という意識ではなく、「自身のアカウント侵害が組織に対する加害行為の起点になり得る」という当事者意識の醸成が有効との提言がありました。

(7) セキュリティ人材・予算・保険に関する課題

- 多くの大学において専門のセキュリティ担当者が 1〜2 名、あるいは他業務との兼務であり、極端な「属人化」がリスクとして懸念されています。
- セキュリティ投資は費用対効果の算出が難しく、予算獲得が現場担当者の熱量や交渉力に依存している状況です。
- 平時より、事案発生時に即応・相談可能な外部専門家（フォレンジック調査機関、サイバー法務に強い弁護士等）を確保しておくことの重要性が確認されました。

(8) ゼロトラスト・ID 管理の方向性

- 特に外部接続（VPN 等の入口）における「ID・アクセス管理（IAM）」の強化が最優先で取り組むべき事項として合意されました。
- ゼロトラストアーキテクチャの段階的な導入の必要性が議論されました。
- 退職教職員および卒業生のアカウント失効・ライフサイクル管理の徹底が、喫緊の課題として再認識されました。

6. 共通認識・提言

セキュリティ教育における「当事者意識（加害者意識）」の醸成

個々の教職員・学生が被害者となるだけでなく、アカウント侵害を通じて意図せず「加害的になる結果」を招く可能性があることへの理解促進が重要です。

インシデント対応訓練（サイバー避難訓練）の実施

人的要因によるインシデント発生を前提とした場合、事前の教育に加え、インシデント対応を想定した実践的な訓練の実施が不可欠です。

セキュリティ担当者の孤立解消とコミュニティ形成

大学等ユーザー組織の孤独な担当者を支援するため、セキュリティ専門家人材の流動化および横断的なコミュニティ形成が極めて重要との認識で一致しました。本ボード会自体が、そのコミュニティの核となることが期待されています。

7. 総括

本会合を通じて、参加した各大学は規模の大小を問わず、一様に「人（ID）に起因するインシデント」「報告等の運用負荷」「学術機関特有の統制の難しさ」という共通の悩みを抱えていることが明らかとなりました。

システム面でのゼロトラスト化（ID 保護や MFA の徹底）を推進すると同時に、現場教職員への「加害者になり得るリスク」の啓発、および担当者の属人化を排除するための横断的な

情報共有の場が、極めて有用であることが確認されました。

8. 今後の活動予定

開催時期	令和 7 年 秋頃（予定）
名称	文教サイバーセキュリティボードメンバー会 第 1 回
方針	参加対象の大学を広げつつも、本音での議論が可能な「少人数制・チャタムハウスルール」を維持し、インシデントの予防・対応策のノウハウ共有プラットフォームとして発展させる。

本報告書について

本報告書は Japan Education Community が主催した「文教サイバーセキュリティボードメンバー会 第 0 回」の議論内容を外部公開用にまとめたものです。チャタムハウスルールの適用により、個別の発言者・所属機関を特定できる情報は掲載していません。

お問い合わせ：contact@japan-education-community.org