事業活動報告 NO. 4

2021年度 大学情報セキュリティ研究講習会 開催報告

新型コロナウイルス対策により遠隔授業やリモートワークを早急に実施する中で、情報セキュリティの不備を狙う攻撃が増加している。また、コロナ禍によりDX（デジタルトランスフォーメーション）に向けた取組みが加速するとともに、セキュリティの備えが求められている。

そこで本協会では、構成員全員がサイバー攻撃の脅威を再確認し、各自の防御行動、組織的な防御対策が進展するよう、大学での対策事例、ベンチマークリストを用いた自己点検・評価・改善、DXに向けたセキュリティの考え方などを通じて、大学の対応力に沿った情報セキュリティ対策の考察を目指して、研究講習会を令和３年11月18日（木）オンラインで開催し、64名（44大学、２賛助会員企業）の参加があった。

（1）情報セキュリティ関連の最新動向

岩本　真人　氏

（トレンドマイクロ株式会社プロジェクト推進本部）

トレンドマイクロ社の「2021年上半期セキュリティラウンドアップ」という公開資料を基に、最新の情報セキュリティの脆弱性、それを狙った脅威、事故事例などについての解説があった。初めに、依然として猛威を振るうランサムウェア攻撃の新たな侵入手口や、暗号化の前に機密情報を持ち出す二重脅迫の紹介があり、続いて、VPN装置やExchange Serverの脆弱性を狙った攻撃事例についても触れた。次にクラウドサービスの脆弱性や、利用者の設定ミスに起因する情報漏えいが急増していることが、国内での事故事例とともに報告された。また、一般利用者を狙ったネット詐欺の手口が変遷しており、SMS（ショートメッセージサービス）やLINEなどのSNSを使うもの、ブラウザ通知機能を使う攻撃手法（BNS）などが紹介された。最後にまとめとして、IT技術や業務プロセス、内外の環境などが変化することで、そこに新たな脆弱性が生まれ攻撃手口も進化するので、それらの情報を入手し対応をし続けることが必要であるとの示唆があった。

（2）クラウドセキュリティ対策と在宅セキュリティ対策の事例紹介

楠　仁志　氏（早稲田大学情報企画部）

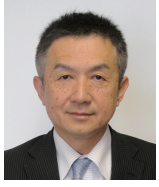
早稲田大学が今後３年間（2021～2023年）で重点的に実行を計画している情報化施策の柱である教育DX推進、研究DX推進、大学運営DX推進の基盤となる情報セキュリティ対策について、全体像および、その具体的な取組みの１つであるクラウドセキュリティ対策と在宅セキュリティ対策の事例が紹介された。

セキュリティ対策の全体計画の策定にあたっては、NIST（米国標準技術研究所）のフレームワークを活用したセルフアセスメントを実施し、重点対策領域を特定することで、より実効性のある評価とゴール設定につなげることに留意している。また、クラウドセキュリティ対策では、Web関連サービスを取り上げ、管理コストとセキュリティレベルの維持向上を目指せる仕掛け作りを目的とし、在宅セキュリティ対策では、物理的な制約を完全に排除し、職員のDXを後押しするゼロトラストの実現を目的とし、それぞれで導入したセキュリティ対策製品の画面を提示しつつ対策状況が紹介された。

（3）大学情報セキュリティベンチマークリストの結果報告と課題

中嶋　卓雄　氏

（東海大学学長補佐、情報セキュリティ研究講習会担当理事）



経営執行部の危機意識に対する共有化は、７％程度は向上しているが、主体となっているのは情報センターなどの運用部門に限定している状態が続いている。しかし、学部単位の管理責任者による危機意識や防御体制

については、数％程度は向上している。ほぼ半数の組織が情報資産の把握と管理対策を実施しており、昨年と比較しても数％は増加しているので、資産管理についての重要性の認識が広がってきている。統括責任者を置き、情報セキュリティに関する専門の検討組織を設置し、実施組織として情報センター等部門を設置している割合および脅威となる事象の学内連絡体制及び処理の責任体制を確立した割合が７％ほど向上しており、体制については徐々に強化されているようである。今回、攻撃に対する防御対策として、「クラウドに対する利活用の注意惹起」が急に23％増加したのが特徴的であり、リモートワークが増加してクラウドの利用が活発化したことによると思われる。また、VPN装置やクラウドに対する直接的な攻撃が増加したことから、エンドポイントセキュリティの重要性が指摘された。

（４）クラウドストレージによるセキュリティ強化の事例紹介～メール添付やファイル共有対策

髙島　伸治　氏

（金沢工業大学情報処理サービスセンターシステム部長）

金沢工業大学におけるクラウドストレージ導入事例が紹介された。これまでの問題点として機密情報が持ち出し可能な機器であるノートPC、USBメモリ、NASなどに保存されているということと、学内および連携する研究機関とデータの共用が困難ということがあった。これらの問題を解決するために当初はオンプレミスのストレージを検討したが、学内に設置すると学外からアクセスできないこと、動画教材が普及し始めていることからデータ容量が膨大になること、機器の更新の際にデータ移行作業が大変などの問題があげられたことによりクラウドストレージであるBoxを2019年10月より導入した。Boxのメリットとして、容量が無制限、専用ソフトは不要でブラウザでアクセス可能、学内外からアクセス可能、ファイルに関する各監査証跡が保存される、セキュリティが強固ということが挙げられる。Boxのセキュリティ対策の内容は複数の認証方式によるなりすまし防止、冗長化されたデータセンターによる災害対策、SSL／TLS通信による傍受対策などがあり、国際的なコンプライアンス・セキュリティ規格に準拠している。Boxによりセキュリティ強化、オンライン授業での動画コンテンツ共有、ペーパーレス化などの効果があった旨の報告があった。

（５）ゼロトラストの実現に向けて

中田　寿穂　氏

（日本マイクロソフト株式会社パブリックセクター事業本部文教営業統括本部スペシャリスト）

大学のクラウド活用が進むにつれ、従来のような「学内ネットワークは安全である」という前提に立って境界を守るやり方が通用しなくなってきている。そこで登場した概念が「ゼロトラスト」である。これは「信頼されないことを前提とし、全てのトラフィックを検査、ログ取得を行う」というものである。

本セッションでは、ゼロトラストを実現するためのセキュリティ技術が紹介された。

これによると導入すべき技術は、①認証、②監視とモニタリング、③サービスのハードニング、④デバイスのハードニングに分けられる。

①では多要素認証などを導入して本人確認を強化するばかりでなく、リソース（全てのデータソースと処理サービス）へのアクセスをセッションごとに認可する仕組みが必要となる。②ではリソースに対する不審なアクセスや異常な認証イベントなどを検知し、通知する仕組みが必要となる。③はリソースに対する適切なセキュリティの設定を指し、リソースへの攻撃に対する影響を下げるために必要である。④はエンドユーザが使用するPC等のデバイスに対するセキュリティを指し、適切なパッチの適用やマルウェア対策、セキュリティログの収集などが必要となる。

教育機関のメールアドレスは、乗っ取られていても気づかれにくく、ソフトをアカデミックディスカウント等で購入するのに便利など、闇市場で取引されている。昨今はOffice365等のクラウド型メールサービスを利用している大学が多いが、ゼロトラスト的な考え方の下、今一度、学内のセキュリティを検証する必要がある旨の報告があった。

（６）セキュリティ強化のネットワーク構築が気付いたらゼロトラストだった

山北　英司　氏

（同志社大学総務部情報企画課情報ネットワーク係長）

学外からのアクセスにはVPNを利用していたが、緊急時連絡に用いるコンテンツマネジメントシステムや海外キャンパスの業務の運用を維持する必要性が生じると予想された。運用上で重要な要件をあげると、学内

外からの認証や特定ユーザへの特定アプリの利用許可といったゼロトラスト＆クラウドの機能との親和性が高いことがわかり、これにマッチしたアイデンティティー認識型プロキシー（IAP）を導入している。

コロナ禍対応の在宅勤務では、IAPを利用しリモートデスクトップ接続することで業務効率を落とすことなく利用できたこと、また、多要素認証やセキュアWebゲートウェイを導入することで個人パソコンを使うセキュリティリスクを最小化にすることができたことが報告された。いろいろな要因に対応できるゼロトラストの重要性が強調された。

（7）グループによる意見交換

４名（一部５名）が１グループとなり、グループディスカッションを35分程で２回実施した。

１回目は、USB紛失事故のケーススタディに基づいて、自大学のセキュリティ対策・対応力を振り返る事前課題の共有、および改善点についてグループでディスカッションをして５つ以上あげた。くわえて、実際に実施できる改善策は、リスクの大きさや組織のリソースに依存するためできる対応は限られることになるので、それぞれに「緊急」、「重要」、「今後の課題」などのラベル付けを行いグループ内で優先順位の決定を行った。

２回目は、大学DXについての意識合わせをした後に、クラウドストレージの利用に限った内容でDXを推進するために注意しなければならないセキュリティ対策についてディスカッションをした。続けて、大学のDXを推進するために注意しなければならないセキュリティ対策についてディスカッションをして、グループで５つ以上をあげた。

グループディスカッションの結果の共有は、後日グループごとのまとめを送付して行った。

本講習会では、具体的な事例に則って実践的な検討が活発にされていた。そして、これらの活動を通して、セキュリティ関連規程の策定・改定、体制整備、在宅勤務やクラウド利用などの新たな技術の利用についての注意、ユーザ教育など、多岐に亘り他大学と整備状況を共有して、今後の報告性を参加者個々人が獲得することができていたと推測される。

（8）参加者からのアンケート結果について

オンライン開催であったため、講習会終了後にオンラインで自由記述の２つの設問でアンケートを実施した。30名から収集したすべての記述をSCAT手法で集計した。その結果、情報提供について６件、グループ意見交換について61件、受講後のアクションプラン24件、今後の取り扱いテーマの希望７件、日程・時間・開催方法５件（自由記述であるため複数回答あり）であった。件数の多かったグループ意見交換について、および受講後のアクションプランの集計結果は表１、２のとおりである。

表１　グループ意見交換について

分類項目	件数
参加者・自組織の技量不足	5
他大学との意見交換・議論の時間がもっと欲しかった	10
他大学との情報・意見交換/他大学の事例からの学び	15
有意義・参考になった・勉強になった	25
研修内容・設計・手段への不満/提案	6

表２　受講後のアクションプラン

分類項目	件数
規程の策定・見直し	6
学内への情報共有	5
クラウドサービスのセキュリティ対策	3
自組織への展開・提案	3
ゼロトラスト	2
その他	5

その他、情報提供では、大学の事例への評価が３件、今後の取り扱いテーマの希望は、多岐に亘った。また、日程・時間・開催方法はオンラインでの午後の開催が評価されているが、名刺交換ができないデメリットも指摘された。

これらのことから、グループ意見交換による他大学の状況を学べることは私情協で実施する講習会ならではの特徴であり、受講者に非常に有意義であったと捉えられている。さらに受講後のアクションプランの記述も多数あり、短い時間ではあったが受講者にとって有意義な研究講習会であったことがうかがえる。