【テーマ】
「セキュリティ最新情報」
【主催】次世代情報システム検討分科会　　活動報告

日　時：2022年11月28日（月）15:00 –17:00
場　所：オンライン分科会
出席者：77名

１．研究内容

「セキュリティ最新情報」をテーマとして、次世代情報システム検討分科会主催のオンラインイベントを開催しました。
当日は、はじめに富士通Japan様より大学特有のネットワークへの対応方法や、最新事例やソリューションについてご紹介いただき、次に大学での取り組み事例として、早稲田大学様より「Webサービスセキュリティ強化の取り組み」と題してご紹介いただきました。
イベント後半は講演を受けて、グループに分かれての意見交換を行い、他校のセキュリティ対策の状況やセキュリティ対策の課題などを共有する場となりました。
（内容詳細については「3項概要レポート」をご参照下さい。）

２．スケジュール

15:00　分科会開始　開催挨拶

○ご紹介 「富士通の考える大学を取り巻くセキュリティ事情とその対策」
富士通Japan株式会社　インフラ戦略企画部
部長　吉岡　亮平　様

15:20　○ご講演 「Webサービスセキュリティ強化の取り組み」
早稲田大学　情報企画部情報企画課
小泉　幸広　様

16:00　（休憩）

16:10　○グループワーク（意見交換）

16:40　○全体会（グループでの意見交換内容の共有）

17:00　分科会終了　終わりの挨拶

3．概要レポート

※当日の資料は「CS研・IS研情報交換サイトhttps://csis.ufinity.jp/shared 」に掲載（会員限定公開）。詳細は5頁「事務局より」をご参照下さい。

「セキュリティ最新情報」

私立大学キャンパスシステム研究会次世代情報システム検討分科会が、11月28日にオンラインで開催されました。今回は「セキュリティ最新情報」をテーマに、富士通Japanから大学を取り巻くセキュリティ事情をご紹介いただいた後、早稲田大学からWebサービスセキュリティ強化の取り組みについてご講演いただきました。その後グループに分かれて意見交換を行い、その全体共有と質疑応答を行いました。

まず分科会運営委員の追手門学院大学 小島氏から、開会の挨拶がありその後講演に移りました。

■ご紹介：

「富士通の考える大学を取り巻くセキュリティ事情とその対策」
富士通Japan株式会社 インフラ戦略企画部 部長　吉岡 亮平様 より

○サイバー攻撃がある前提で侵入前後の対策を

サイバー攻撃は年々増加、巧妙化の一途をたどっておりセキュリティの運用に悩みを抱える組織が多くなっています。昨年度は大学で50件のセキュリティ事故が報告されており、大学数を鑑みるとかなり多い数字です。文部科学省からもセキュリティ対策強化の通知が出ています。

富士通では漏洩時のリスクに応じて大学のデータのセキュリティレベルを格付けしています。大学には「軍事転用も可能な機微な情報AAA」、「研究、入試・成績情報等の個人情報AA」、「人事、財務等の情報A」、「一般情報BBB」の4レベルのデータがあると捉えています。それぞれのレベルに合わせ、可用性を高めつつ安全に運営する対策が求められています。

最近よく耳にする「ゼロトラスト」とは、従来のように「学内は安全、学外は危険」と境界で防御するのではなく、すべてを信用せずに安全性を検証し情報資産を守る概念です。弊社ではゼロトラストの領域を「エンドポイント」「ネットワーク」「アプリ/ワークロード」「認証・認可」とそれを管理する「オペレーション」の5つに分類しています。例えば「エンドポイント」では学生個人所有の端末を完全に信用せずに、管理や監視を行います。ゼロトラストありきではなく、この5つの領域を意識してソリューションの選定を行うことが重要です。

また富士通では、セキュリティ投資に対して3つの側面からの仕組みづくりをご提案しています。

1. 従来対策の棚卸
既存のウィルス対策の見直し、バックアップの確認、ファイアウォールの設定確認、脆弱性の管理等。
2. 新たな攻撃への対応
未知のマルウェア対策、サイバー攻撃への対策検討等。
3. 運用負荷の軽減
効率化の仕組み、復旧対策の構築、人材育成等。

これらを踏まえ、セキュリティ対策を行う際には、費用対効果が高く既存環境への影響が少ない対策から検討しましょう。例えば現状把握やセキュリティ教育による人的リテラシーの向上は、既存環境への影響がなく、比較的安価に行える効果的な対策の一つです。ネットワークの振る舞い検知も、環境への影響が少なく、効果の高いセキュリティ投資です。これらの対策を行ったうえで、システム全体を統合管理する等のセキュリティ対策を考えると良いでしょう。

また最近の巧妙なマルウェアは完全に侵入を防ぐのは難しく、侵入されることを想定した検知、対応、復旧対策も必要です。防御への対策と共に事前に資産管理等を徹底することで、驚異の特定や復旧、対応の時間と費用が下がります。検討すべきセキュリティ対策を図にまとめましたのでご確認ください。

文科省から通知があったように、CSIRT（Computer Security Incident Response Team）/SOC（Security Operation Center）/CISO（Chief Information Security Officer）等の専門組織、責任者は必須です。またゼロトラストは、領域や目的に応じて検討することに留意しましょう。

■ご講演：
「Webサービスセキュリティ強化の取り組み」
早稲田大学 情報企画部情報企画課　小泉 幸広様 より

○多彩なセキュリティソリューションを導入しインシデント減少を実現

本学では、「世界に輝く早稲田」というビジョン達成に向けた情報化重点施策の中でセキュリティ対策にも取り組んでおり、その一部をご紹介します。

本学には大きく分けて、オフィシャルサイトとWaseda-net WWWという2種のサイトがあります。後者にはwaseda.jpの下に5つのサブドメインがあり、用途ごとに約300のサイトが稼働しており複雑な構成です。2018年から年数回のセキュリティ関連の集中討議、アセスメントを行っており、これを受けて様々な対策を行ってきました。

現在、Webサービスに関連する通信としては、①Webアクセス、②DNSクエリ（権威への問い合わせ）、③DNSクエリ（学内キャッシュへの問い合わせ）の3種類があり、それぞれにセキュリティ対策を行っています。①Webアクセスに関しては、CDN（Content Delivery Network）製品のCloudflareというソリューションを導入しました。プロキシとして働き、WAF（Web Application Firewall）やDDoS検知を行います。②権威への問い合わせに関してもCloudflareが提供しているDNS Firewallという製品を導入しています。③学内からの問い合わせに関しては、Cisco Umbrellaというゲートウェイを使用しています。またこれに関連し、Sumo LogicとDatadogの2つのソリューションを導入しました。それぞれの機能と利用方法をご説明します。

● Cloudflare（WAF）

CDN製品で、利用者がCloudflareを介してWebサーバーにアクセスするプロキシとして働きます。トライアルで攻撃検知、ブロックの効果が確認でき導入が決まりました。Cloudflareでは、「何を検知するか」「そのレベルは」「検知したらどうするか」等の細かい設定も可能で、独自のWAFルールを設定することもできます。

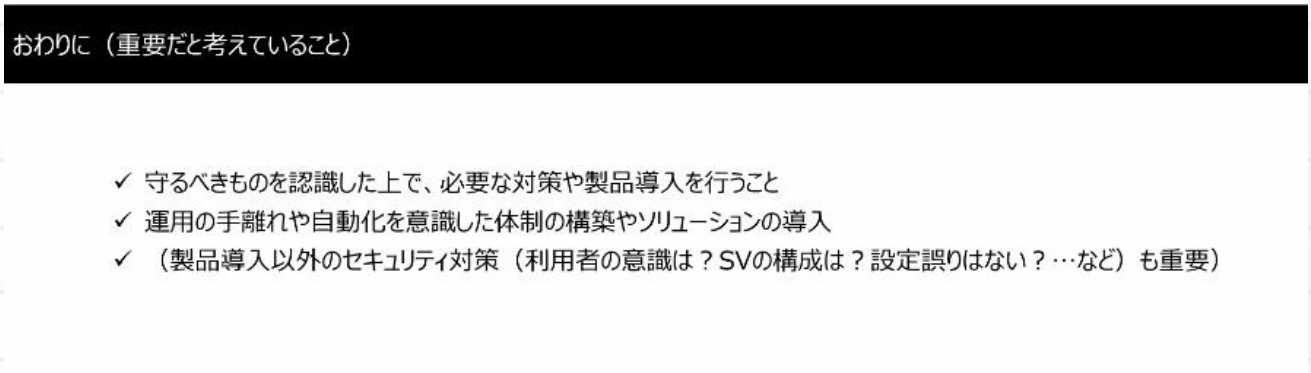
● **Cloudflare（CDN）**
セキュリティとは少しずれますが、CDN製品としてサーバーの負荷を軽減しています。20～200%がCloudflareのキャッシュを使っており、特に学祭、入試等アクセスが集中する時期には効果が高いです。Webサーバーの台数を減らすこともできました。

● **Cisco Umbrella**
DNSの名前解決を利用してSIG（Secure Internet Gateway）を提供するソリューションです。主にキャンパス内からの通信保護を目的に導入し、フィッシングサイト等危険なサイトへのアクセスを検知してアクセスする前に遮断します。違法ダウンロード等もブロックでき、ソフトウェアの不正利用防止や訴訟リスク軽減にもつながると考えています。

● **Datadog**
Webサーバーに関してシナリオを組んで、サイトの死活を監視しています。監視結果は管理者だけでなく利用者にも公開し、サイトが正常稼働しているか確認できるようになっています。

● **Sumo Logic**
SIEM（Security Information and Event Management）ソリューションで、本学ではCloudflareとWebサーバーのログを使って相関分析を行っています。怪しい動きを検知するとアラートが出て、対策を取ることができます。

セキュリティ対策が強化され、重大なインシデントは減少傾向にあります。今後は導入した製品をより便利に使って、重複している機能は整理し、サーバーの構成見直し等Webサービス運用全般の省力化を図っていきたいと考えています。終わりに、重要と考えるポイントを3点まとめましたので画像をご確認ください。



■インシデントはセキュリティ対策強化の契機にも

4グループに分かれて30分程度の意見交換を行った後、全体共有と小泉氏への質疑応答が行われました。その中からいくつかピックアップしてご紹介します。

まず、「セキュリティ対策の重要性は理解しているが、人的リソースやコストが課題」「セキュリティ製品は多種多様で、自分の大学にとってどれを選ぶべきかとても難しい。ベンダーに聞いてもすべての製品に対しての回答は得られない」といったお悩みの声がありました。また「セキュリティ事案はあってはならないが、起こったときには対策を強化する契機と捉えることもできる」という意見もありました。

小泉氏への「教員からネットワークに関しての要望があったときにはどうしているか」という質問に対しては、「教室のネットワークは強固なセキュリティにしていますが、一方で研究室では申請制である程度自由に外部へのアクセスができるようレベル別の管理をしています」と回答をいただきました。

結びに、運営委員長の京都産業大学 大島氏が「大学のセキュリティ対策は民間企業と異なる点もあり、皆さん悩まれていると思います。早稲田大学の貴重な事例も聞けたのでぜひ参考にしてください」と述べ閉会となりました。

4. 参加校 [32校42名] ・参加企業[7社35名] ・参加総数[77名]

追手門学院大学[2]	神戸大学[1]	東京富士大学[3]	株式会社セールスフォース・ジャパン[1]
大阪工業大学[1]	実践女子大学[1]	東洋大学[1]	サイバーリーズン合同会社[1]
大阪産業大学[1]	城西大学[1]	東洋学園大学[1]	電子システム株式会社[1]
大阪公立大学[1]	常翔学園[1]	新潟大学[1]	東京コンピュータサービス株式会社[1]
神奈川工科大学[1]	女子栄養大学[1]	兵庫県立大学[1]	Manabie Japan 合同会社[1]
鹿屋体育大学[3]	摂南大学[1]	福岡大学[1]	有限会社ハーティサービス[1]
関西大学[1]	専修大学[1]	宮崎大学[1]	富士通Japan株式会社[29]
京都産業大学[1]	大東文化大学[2]	横浜国立大学[1]	
共立女子大学[1]	千葉工業大学[1]	流通経済大学[1]	
金城学院大学[1]	東海大学[1]	早稲田大学[5]	
神戸学院大学[1]	東京都市大学[1]		

5. 所感（次世代情報システム検討分科会運営委員会）

今年度第2回目となる今回は「セキュリティ最新情報」をテーマとして開催した。はじめに、富士通Japan株式会社の吉岡氏より「富士通の考える大学を取り巻くセキュリティ事情とその対策」と題してサイバー攻撃の現状、大学でのセキュリティ事故、「ゼロトラスト」の考え方、セキュリティ投資など最新の情報についてご説明いただいた。つづいて、早稲田大学の小泉氏より「Webサービスセキュリティ強化の取り組み」の題目で「世界に輝く早稲田」というビジョン達成に向けた情報化重点施策の中でセキュリティ対策の取組として、多彩なセキュリティソリューションを導入しインシデント減少を実現している具体的な事例をご紹介いただいた。大学の規模の違いはあるものの具体的にご紹介いただいたことで各大学の事情に応じて参考にすることができたのではないかと思われる。最後に、参加者を４つのグループに分けて他校のセキュリティ対策の状況やセキュリティ対策の課題などを共有するグループワークを行った。グループワークの内容については再度全体会において共有を行った。 今回の参加者は77名となり，「セキュリティ」への関心の高さが覗えた。分科会終了後の全体満足度のアンケートは満足、大変満足を合わせると88.4%という結果であった。参加者の意見として「セキュリティ最新情報として、BYOD対策や新たな攻撃への対策など、他大学の状況がお聞きでき大変参考になりました」「インフラ、セキュリティに関して大学での事例、他大学での導入状況、苦労話が聞けたことがよかったです。モチベーション向上につながりました」等があり、「セキュリティ」に関する情報共有を目的として開催した今回の研究会の目標は達成できたと考える。一方で，グループワークの意見交換の時間をもっととり、他校の事例を共有したいという意見があり，今後の研究会実施の課題としたい。

【分科会の様子】

【事務局より】
次頁以降に開催後アンケート結果（抜粋版）を記載しています。
開催後のアンケート結果詳細版や当日プレゼン資料ご覧になりたい方は、「 CS研・IS研情報交換サイト」に掲載しておりますのでそちらをご覧ください。

「CS研・IS研情報交換サイト」について
○CS研・IS研の会員向けに情報・資料をご提供し、会員の皆様で情報交換をする会員専用のサイトです。
（新規入会ご希望の方は、右下の事務局まで、お手数ではありますがご連絡ください。）
URL： **https://csis.ufinity.jp/shared**

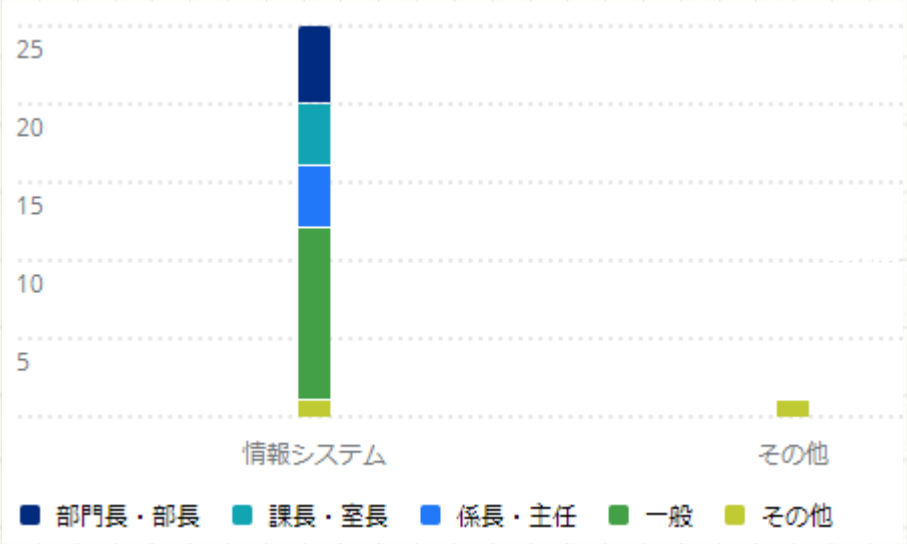
○情報交換サイトをご覧になるにはIDとパスワードが必要となります。お持ちでない場合は以下のサイトにてお申込みください。
お申込みサイト：https://seminar.jp.fujitsu.com/public/seminar/view/46757

【連絡先】

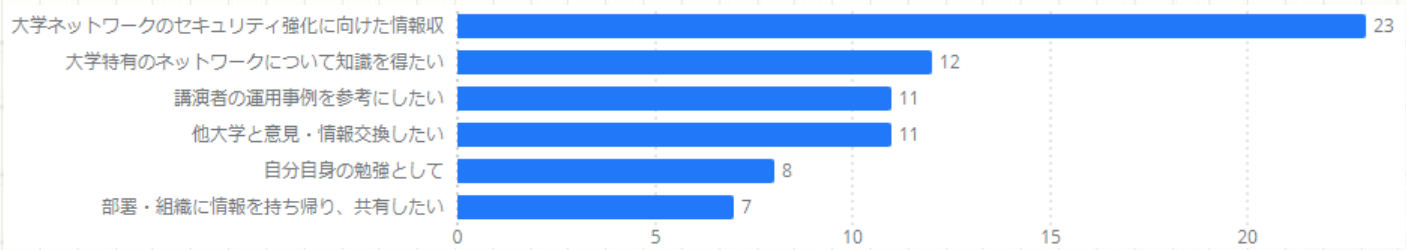
私立大学キャンパスシステム研究会　事務局
〒105-7123　東京都港区東新橋1-5-2 汐留シティセンター
富士通Japan株式会社　戦略企画統括部内
E-mail：contact-csisken@cs.jp.fujitsu.com

開催後アンケート結果 【回答数／対象者数：26／42（大学関係者のみ）】

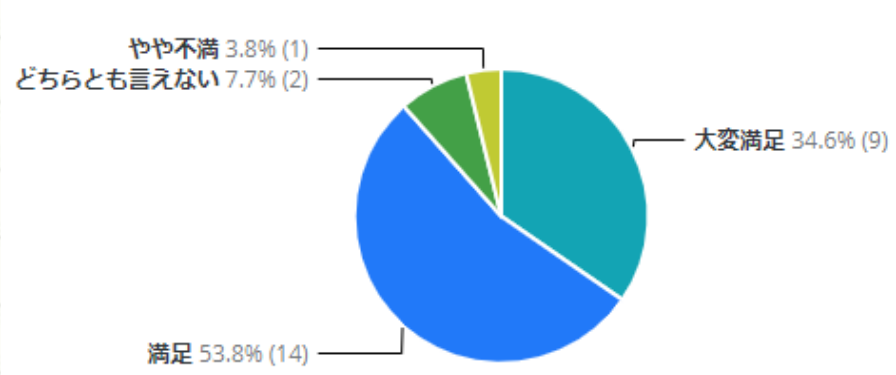
■担当業務と役職について



■参加した目的について



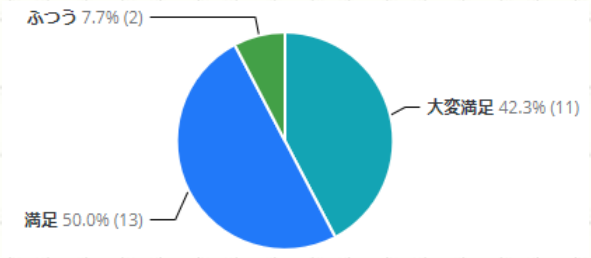
■本日の分科会の全体満足度について



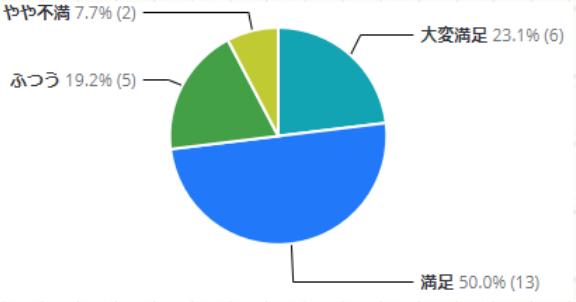
■全体満足度の評価理由について（一部省略・抜粋）

- 他大学の具体的な事例に触れることができ、またグループワークで色々な情報を得ることができました。
- 初めての参加でしたが、インフラ、セキュリティに関して大学での事例、他大学での導入状況、苦労話が聞けたことがよかったです。モチベーション向上につながりました。
- セキュリティ強化を考える上での物差しがなく困っていた。有識者の参考事例等を聞けたことで、今後どうすれば良いかの一つの物差しになった。
- 小規模のグループワークだったため、気軽に発言することができました。また、他大学の状況も知ることができ、大変勉強になりました。
- セキュリティ最新情報として、BYOD対策や新たな攻撃への対策など、他大学の状況がお聞きでき大変参考になりました。
- 早稲田大学の事例が具体的で分かりやすかった。とても参考になりました。
- もう少し深い部分までディスカッションができる時間があればよかったです。
- グループワークの意見交換の時間をもう少し頂きたかった。
- 大学特有のネットワークに対するセキュリティ対策についてもう少し詳しく話が聴ければよかった。
- 本学の規模には当てはめられない内容な部分もあり参考になりづらかった。グループディスカッションではそれなりに有用な情報交換ができたと思います。

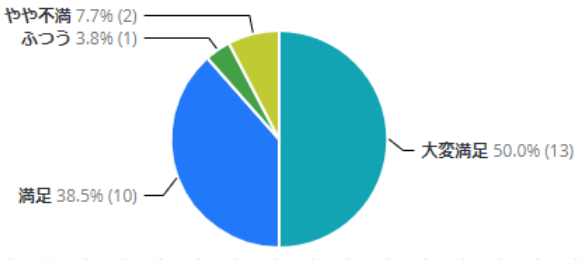
■満足度－開催テーマについて



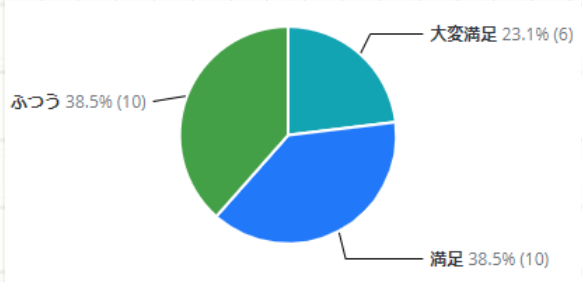
■満足度－富士通Japan様の講演について



■満足度－早稲田大学様の講演について



■満足度－時間配分について



■次回以降取り上げて欲しいテーマについて（一部省略・抜粋）

- グループウェア、ワークフローの導入事例。

■ＣＳ研についてのご意見・ご要望について（一部省略・抜粋）

- 本当のクラウド化
- 他大学の事例を多く吸収するために、様々な大学と交流できると良いと思います。
- 今回のような事例発表は、オンラインの方が聞きやすいです
- やはり、対面の方がいろいろと聞けて良いと思います。まだ、難しいとは思いますが。