情報セキュリティへの取り組み

INFORMATION SECURITY MANAGEMENT

豊かな
コミュニケーションを
広げるため、
提供サービスへの信頼を
獲得していきます。



執行役員 CISO*

亀山 直生

＊Chief Information Security Officer：最高情報セキュリティ責任者

私たちは、お客さまの情報をお預かりして事業を推進しています。情報をしっかりと守り、当社サービスへの信頼を獲得し、それを継続していくこともセキュリティ室における重要な役割のひとつだと考えています。一方で、私たちの仕事は事業部門やIT部門との緊密な連携が必要不可欠であり、それらの部署の従業員たちと協力して対策を行うことを心がけています。

セキュリティ室の役割と、他部門との連携

セキュリティ室は、情報セキュリティ対策を推進する組織です。主な役割には、自社サービスや社内のPC・システムに対するセキュリティ監視・脆弱性診断、従業員のフィッシング被害を防ぐセキュリティツールの導入といった、攻撃の対象となる領域への対策などがあります。さらに、セキュリティ問題に関する早期発見・対応を行う、当社のCSIRT※1である「mixirt」の運営も行っています。

CISOとしての意義、そして人づくりとは？

CISOという役割は、当社グループとして対外的にも、しっかりとセキュリティを重視していくという姿勢の表明です。CISOという役割が制定され、2年が経ちましたが前期は認証基盤の強化、および体制強化を引き続き重点的に行いました。PMI含めグループ会社のガバナンスを強化するために、既存の技術特化の部隊とは別に管理特化の部隊を前年度の期初に新設しています。管理部隊は技術部隊と連携し情報システムやリスクの管理、mixirt(CSIRT)の運営、新たなM&A案件への対応などを行い、情報セキュリティの維持管理をより盤石なものにすることができました。ガバナンスの強化、最新の脅威動向を鑑みた戦略の立案・実行のために、引き続き組織や体制の強化を行っていきます。



認証基盤の強化

社内システムの認証基盤の認証方式の強化を実施。所持要素を原則必須とすることで、フィッシングや不正アクセスの防止に努めています。

それら施策を担うセキュリティ室の「人づくり」も重要な任務です。当社グループは幅広いサービスを提供するため、同じ手順の作業の積み重ねではなく、広範囲に及ぶ業務を扱う必要があります。そのため新規加入メンバーには、今までやっていた分野から始めてもらい、軌道に乗ったら他の施策もできるように促し、徐々に幅を広げてもらうよう働きかけています。



監視体制の強化

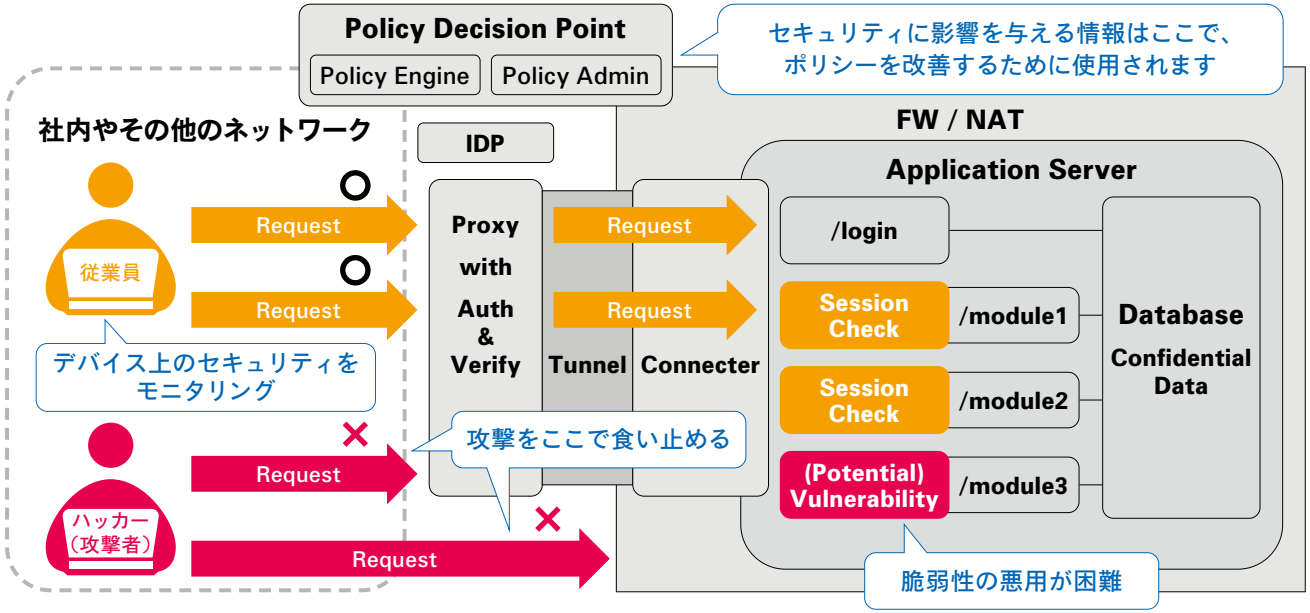
当社サービスのシステムのセキュリティ上の問題に「気付ける状態」の強化。監査や取引先に対するアカウンタビリティの強化に注力しています。

さらに、当社は「セキュリティ・キャンプ協議会※2」のオフィシャルメンバーでもありますが、社会貢献や人材発掘の観点からも、このような活動は今後も検討していきます。

※1 CSIRT（Computer Security Incident Response Team ：シーサート）：コンピュータセキュリティに係るインシデントに対処するための組織の総称。インシデントに関する情報収集、分析、対応方針や手順の策定などの活動を行う。
※2 セキュリティ・キャンプ協議会：セキュリティ技術等を扱う合宿形式の研修会（セキュリティ・キャンプ）のための協議会

情報セキュリティ領域における AI活用や自動化に関して

情報セキュリティの業務における自動化やAI活用を推進しています。既に情報セキュリティ研修の一部演習におけるAI活用、軽微なインシデントやアラート対応における自動化を行っていますが、生成AIの登場や進化により自動化の方法や適用範囲は拡大していると認識しています。ハルシネーション等のリスクを考慮した設計や運用が前提にはなりますが、今後はより一層AI活用や自動化に力を入れていく方針です。



ゼロトラストを取り入れたセキュリティの取り組み

ネットワークや場所に関わらずより厳密な認証・検証をすることで脅威を防ぐ「ゼロトラスト」の考え方に基づく情報セキュリティ基盤の整備に取り組んでいます。