【講演レポート】第99回JIPDECセミナー

増大するなりすましによる不正ログイン・不正利用リスクへの対抗策
～最近のインシデント事例から見えた「効果的な対策方法」とは～

S&J株式会社　取締役 コンサルティング事業部
事業部長　上原　孝之 氏

相次ぐ不正ログイン・不正出金・個人情報流出等の被害

最近の不正アクセス被害の状況

今年になって規模や業種を問わず、さまざまな組織をターゲットとした二重脅迫型ランサムウェアによる被害が多発しています。従来からの、ファイルを勝手に暗号化して身代金を要求する手口から、情報を盗み取った上で暗号化し、その解除（復号）のための身代金要求に応じないと、攻撃者のサイトで情報を小出しに公開しながら、より高額な身代金を要求するといった手口に変わってきています。

最近はVPN機器の脆弱性を突いて侵入し、Active Directory（AD）の管理者権限を奪取して重要情報を盗んだり、暗号化したりするパターンが典型化しており、脅迫の平均額も日本円で1,000万円以上に吊り上げられています。中には11億円を支払ったとされるケースもあり、ますます悪質化してきています。

主にダークウェブ上にある各種の攻撃者グループのサイトには、被害を受けた組織の情報が次々と追加されており、攻撃に成功した証拠として、盗み出した情報の一部やフォルダ内を一覧表示したキャプチャ画像等が公開されています。

不正引出し・送金被害事例と原因

最近はQRコード等によるキャッシュレスサービスと連携した銀行口座からの不正引出し、不正送金被害も増加しています。大きく報じられたドコモ口座の不正引出しは、携帯電話の契約者以外であっても口座開設が可能となった直後から起きていたようですが、その根本的な原因は、被害を受けた顧客の銀行口座情報や暗証番号等がどこかから漏えいしており、それを攻撃者が入手していたことです。それに加えて、メールアドレスのみでドコモ口座が開設できたり、銀行口座との紐づけ時に二段階認証が行われていなかったりしたことなどが被害の発生原因として挙げられます。

SBI証券の場合は、悪意のある第三者が偽造した本人確認書類を使って顧客と同姓同名の銀行口座を不正に開設した後、何らかの手段で入手した顧客のユーザネームやパスワードで証券口座にログインし、出金先口座を変更して不正引出しが行われました。被害が発生した当時、６文字程度の単純なユーザネームやパスワードが設定可能であったことから、それらが脆弱な設定であったことも原因と考えられます。

ゆうちょ銀行では、即時振替サービスでの不正出金や、デビットカード・プリペイドカードmijicaのWebサイトへの不正ログイン・不正送金被害等が発生しましたが、その後に行ったセキュリティ総点検で、実施することが必須とされる22の対策項目のうち、14項目が未実施、もしくは不十分であったことが明らかになりました。

サイバー攻撃が増加し続ける要因

被害増加の要因

では、なぜこのような被害が多発しているのでしょうか。

報道されている被害事例や当社が行ったインシデント対応事例から、次のような事項が要因として考えられます。

①被害を受けやすいサービス／システム仕様例

攻撃や被害を受けやすいサービス／システム仕様例としては、銀行口座登録時等の本人確認の不備、二段階認証／二要素認証が実装されていない、単純なユーザIDやパスワード設定が可能、ログイン試行回数の制限がない、不正ログイン・不正利用の可能性がある事象がモニタリング対象になっていないなどが挙げられます。

これらの多くはサービスやシステムの要件を決めて設計する時点で潜在的に生まれてしまうため、企画・設計段階からセキュリティを十分考慮して構築することが必要です。

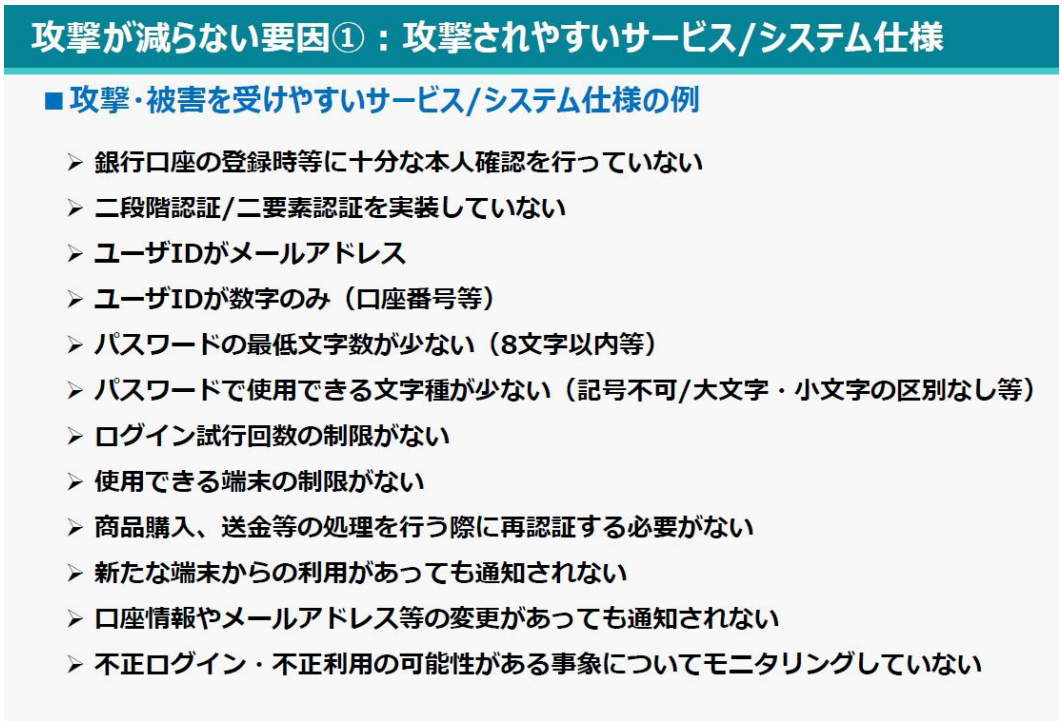

図1．攻撃されやすいサービス／システム仕様例

②脆弱なWebサイトの存在

上記のサービス／システム仕様の問題に加え、SQLインジェクション等、重大な脆弱性のあるWebサイトが依然として数多く存在することも要因の１つでしょう。このような脆弱性が生まれてしまう主な理由として、費用や時間の制約、セキュリティ対策の要件や基準が不明確、システム開発者のスキル・経験不足などが挙げられます。

③クレデンシャル情報の大量流出

2018年に「日本企業の社員情報約16億件が流出」などと大きく報じられたケースでは、約10年にわたり流出したクレデンシャル情報（ID／パスワード等のユーザ認証情報）が蓄積された延べ27億件ものデータセットがネット上に出回っていました。このような大量の流出事件は後を絶たず、不正ログイン攻撃を助長する大きな要因となっています。

④攻撃のビジネスモデル化

昨今、サイバー攻撃の分業化が進んでいます。ブラックマーケットに流れたクレデンシャル情報を入手した者が実際にそれを試して有効なID、パスワードをリスト化して再びブラックマーケットに流す。そのリストを購入した者が他人になりすまして不正送金や不正なポイント交換等を行う、というように、サイバー攻撃が一連のビジネスモデルとして確立されています。

⑤VPN機器やサーバ等の重大な脆弱性

当社が対応した事例では、昨年公表されたPulse Secure社のVPN機器の重大な脆弱性への対応が行われていなかったためにVPNから侵入され、Active Directory（AD）が乗っ取られてランサムウェアによる被害を受けたケースがありました。また、今年の7月、8月には「SIGRed」「Zerologon」と呼ばれるWindows Serverの重大な脆弱性が相次いで公表されています。こうした脆弱性の存在が攻撃の増加や被害を大きくする要因となっています。

従来からの対策の限界とその解決策

サイバー攻撃の脅威動向

従来からの対策がなぜ機能しないのか、そして有効な解決策として何が考えられるでしょうか。

これまで見てきたように、サイバー攻撃の動向として、会員向けWebサイトへの不正ログインや不正利用が増加するとともに、VPNから侵入されてADが陥落し、内部情報の大量流出や大規模なシステムダウンが発生するケースも急増しています。マルウェアの感染力も高まっており、いわゆるラテラルムーブメント（組織内部での横方向への感染拡大）の被害も増加しています。また、WebサイトのHTTPS化は上場企業の8割がすでに実施（※）しており、セキュリティ上好ましくはありますが、同時にサイバー攻撃を含む通信の「見えない化」も進行し、通信経路上の多くのセキュリティ対策が無力化してしまう状況になってきています。

※フィードテイラー社による調査結果より
https://www.feedtailor.jp/company_summary/

セキュアなWebアプリ／スマホアプリを実現するための対策

不正ログインやなりすましによる不正利用に屈しないサービス／システムを実現するためには、Webアプリケーションやスマホアプリの開発において次のような対策が求められます。

・アプリセキュリティに対する十分なスキル・能力を有する人材の確保
・アプリ開発のためのセキュアなルール・プロセス・体制整備
・開発するアプリのリスクアセスメントの実施とセキュリティ機能要件、テスト要件、運用要件等の明確化
・サービス設計、開発段階からのレビューの実施とセキュリティ要件を満たしているかの確認
・リリース前のテスト、脆弱性検査の実施と問題個所の改修
・リリース後もアプリの追加開発時や改修時にセキュリティ観点でのレビューや脆弱性検査の実施

開発後の改修は難しいので、初期の段階で対応することが重要ですが、現実にはコスト、人材等の問題でなかなか理想どおりにはならないことが多いようです。

Firewall（FW）／IPS／Web Application Firewall（WAF）で対処できない攻撃

OS・ミドルウェアへの攻撃や不正な入力値によるWebアプリケーションへの攻撃など、従来からのFW／IPS／WAFで検知／防御できる攻撃はありますが、1つのIDに対して1つのパスワードしか試さないパスワードリスト攻撃、パスワードを固定して何通りものユーザIDの組合せを試行するリバースブルートフォース攻撃、時間をかけてゆっくりとログイン試行を行うスローブルートフォース攻撃、なりすましによるログイン成功後の不正送金、不正なポイント交換などは、これらの対策では十分に対処できず、多くの被害が発生しています。

境界防御モデルの限界

従来からの境界防御モデルでは、外部と内部の境界にFWやVPNを設置することでセキュリティを確保していましたが、昨今、テレワークの普及等によって境界が曖昧になり、従来からの対策では防御しきれなくなってきています。また、このモデルでは「内部は安全な領域」と考えられていたため、内部ではアクセス制限や通信内容の監視等が行われていないことも多く、一旦内部に侵入されると被害が一気に拡大する、といった問題もあります。

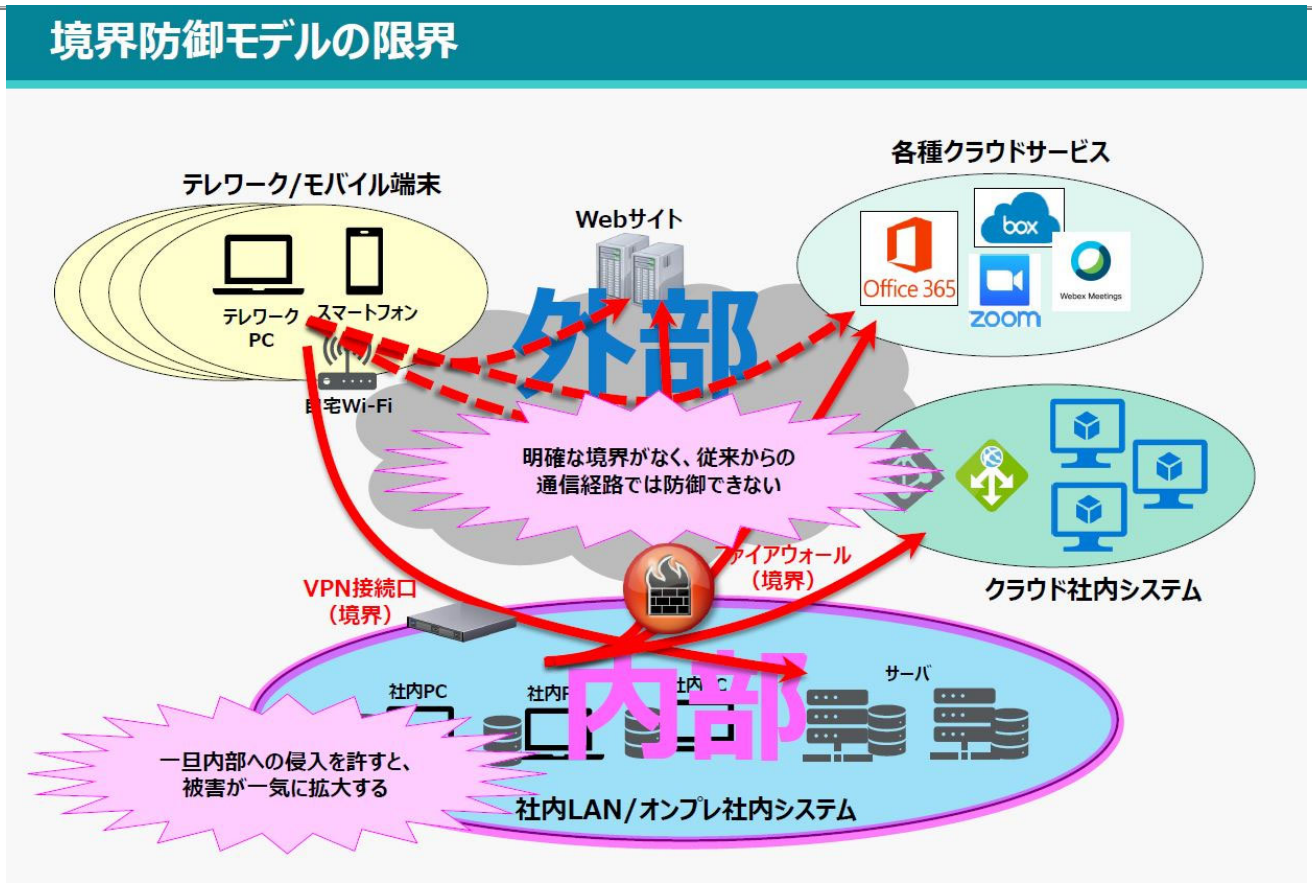

図2. 境界防御モデルの限界

対策

（1）Webサイトへの不正ログイン／不正利用対策

Webサイトへの不正ログイン／不正利用対策として、端末認証／ユーザ認証の強化のため、二段階認証および二要素認証の採用や複数端末からの利用制限、クレジットカード決済時の3Dセキュアなどが有効です。

不正ログイン／不正利用を検知するためには、認証失敗回数の大幅な増加や、同一IPからの複数IDへのリクエストなどをリクエストログ／認証ログの分析によって検知したり、アプリケーションログの分析により、不自然な出金処理や出金先口座情報の変更等を検知したりすることなどが有効と考えます。

（2）ADに対する攻撃の防御／検知対策

ADに対する攻撃への防御対策としては、既知の脆弱性への迅速な対処（セキュリティ更新プログラムの適用等）、ドメイン管理者アカウントの管理強化、AD管理端末の専用端末化（固定して他の業務には使用しない）と防護（別セグメントに設置してアクセス制限）等が有効です。また、ADに対する攻撃を検知するため、必要なADログが取得できるよう監査ポリシーを設定してログ出力領域を拡張し、取得したログを定期的に分析するのが有効と考えます。

まとめ

昨今、クレデンシャル情報を悪用した不正ログイン・不正利用や、不正入手した組織の機密情報を暴露するランサムウェアなどによる被害が多発しており、従来からのセキュリティ対策ではこうした攻撃に対処できなくなってきています。

不正ログイン／不正利用に対しては、二段階認証、二要素認証、複数端末からの利用制限などの認証システムの強化や、Webサイトの認証ログ、アプリケーションログ等の定期的な分析が有効と考えます。また、VPNや組織内ネットワークの要となるADサーバの対策強化が重要です。

以　上

Q：なりすましを確実に見つける方法はありますか？

A：なりすましか否かをシステム上で判断することは難しいので、まず各々のサービスやサイトの仕様・特性に応じた「正常な利用」のパターンを定義した上で、アプリケーションログ等を定常的に分析し、正常でないものを見つけ出して確認するしかないと思います。

Q：本人確認用の画像データ（免許証やマイナンバーカード）を流出した事例紹介がありましたが，それをさらに悪用して他組織で個人確認資料に利用された事例はありますか？

A：悪用される可能性は十分ありますが、事例としてご紹介した件を含め、サイバー攻撃で流出した本人確認情報が実際に悪用されたことが確認された実例までは認識しておりません。たとえば、本日ご紹介したSBI証券のケースでは、偽造した本人確認書類を使って他人になりすまし、不正に銀行口座を開設したとのことですが、たとえばこのようなケースで実際に流出した本人確認情報が悪用される可能性は高いと思われます。

Q ：社内システムから外部へのパケットの監視は有効ですか？

A：マルウェアがPC等に感染すると、インターネット上の指令サーバと通信して攻撃指示を受けたり、別なマルウェアをダウンロードしたりしますので、社内から外部への通信を監視することは有効です。（こうした攻撃を早期に検知し、被害の拡大を防げる可能性が高まります）とはいえ、最近ではマルウェアの通信もHTTPSで暗号化されていることも多く、その場合はプロキシサーバのログ等を監視しても、通信先のドメイン名までしか確認できず、詳細がわからないという制約などもあります。

S&J株式会社 取締役 コンサルティング事業部 事業部長
上原　孝之 氏

1996年より、株式会社ラックにて情報セキュリティ関連事業の立上げ、推進に携わり、コンサルティングサービスを主導する傍ら、執筆や講演活動を通じて人材育成にも注力。
2015年より、S&J株式会社にて企業等のサイバーセキュリティ強化、インシデント対応支援に従事しており、2017年より神奈川県警察のCSIRTアドバイザーも務める。

【主な著書】
情報処理教科書　情報処理安全確保支援士（翔泳社）
ネットワーク危機管理入門（翔泳社）
社長のためのインターネット防犯マニュアル（すばる舎）

本内容は、2020年11月20日に開催された第99回JIPDECセミナー「ビジネスモデル変革に伴うなりすましリスク対応－オンライン本人認証となりすまし対策」講演内容を取りまとめたものです。