「ジャパンネット銀行流のセキュリティ対策
～サイバー攻撃の進化に備えて～」

株式会社ジャパンネット銀行
IT 統括部
サイバーセキュリティ対策室長
岩本　俊二　氏

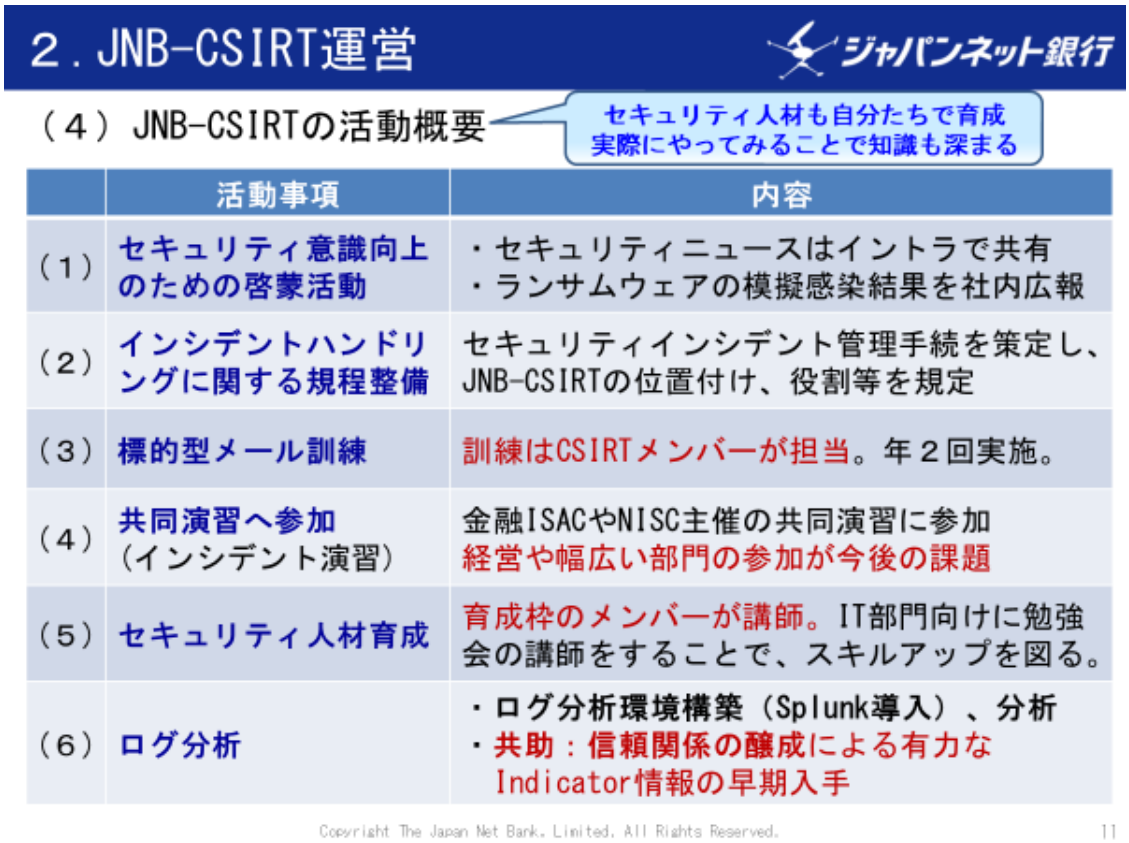
■はじめに

当行は 2000 年に日本初のインターネット専業銀行として開業した。システムは 24 時間 365 日取引可能で、サービス停止時間は年間 30 分のみ、実態は 15 分程度でメンテナンスを終えてサービスを稼働している。2013 年 9 月の設置当時 7 名だった当社の C-SIRT のメンバーは現在 11 名、リスク管理委員会の下部組織として位置付けられ、私は元々IT 統括部の中でシステムリスク管理グループ長をやっていたが、2015 年 9 月、セキュリティをより強化するため、インフラのメンバー等も加えサイバーセキュリティ対策室を立ち上げた。

■ジャパンネット銀行及び JNB-CSIRT（ジャパンネット銀行 CSIRT）について

JNB-CSIRT（ジャパンネット銀行 CSIRT）のミッションは①お客様の資産を守る、②お客様の情報をサイバー攻撃から守ることであり、これらのミッションは各メンバーの活動すべてに優先される。また、リスクは隠さずに経営にタイムリーに報告し、関連部署長に適切な対処を勧告することとしている。さらに、外部の関係組織と信頼関係を構築し、サイバー犯罪に対する社会的責任を果たすこと、例えばこうした外部講演を行いノウハウを出すとともに、外部からノウハウをいただくことも重要である。

JNB-CSIRT の日頃の活動は主に、①セキュリティ意識向上のための啓蒙活動、②インシデントハンドリングに関する規程整備、③標的型メール訓練、④共同演習へ参加、⑤セキュリティ人材育成、⑥ログ分析である。②のインシデントハンドリングに関する規程整備については、個人のノウハウに依存しないことを目的として決めごとを定義している。具体的には、管理スコープの対象、情報共有範囲（TLP : Traffic Light Protocol）の設定を定義し、それに基づき社内外でやりとりをしている。さらに当行は③標的型メール訓練も自前で行っている。例えば送信元を自社ドメインに改ざんし、新入社員が一通り各部署での研修を終えた頃、新入社員からの懇親会の誘いを装った偽のメールを送ったりもしている。こうした巧妙なメールの開封は完璧に防御するのは不可能なため、不正通信を検知し、初動対応を徹底化することがカギである（図）。



（図）

■DDoS 対策について

残念ながら我々も 2006 年、2011 年に DoS、DDoS 攻撃によるサイトダウンを経験した。2006 年当時、キャッシュサービスを導入済みであったが、この時の対象が HTTP のみであったため負荷分散装置の許容セッション数を超過し通信不能に陥った。この経験から DDoS 対策サービスを新たに導入したものの、2011 年には Web サーバへのセッションに対する応答を待たずにセッションを張り逃げされるという事案に見舞われ、セッション数枯渇によりサイトがダウンした。負荷分散装置や Web サーバの設定値に細かい閾値、設定をしていなかったことがこの時の反省点である。しかし、閾値調整は難しく、閾値のみでの対策には限界があることや、攻撃規模の拡大に伴い対策基盤のキャパを超えるという課題もある。そこで、2014 年には Akamai のサービス、CDN（Content Delivery Network）と WAF（Web Application Firewall）機能を導入し、WAF 機能によって Web アプリケーションに対する攻撃を防御、CDN 機能によりレスポンスを高速化するとともに、Akamai を経由しない IP アドレスを直接指定した攻撃に対しては ISP の DDoS 対策サービスを導入するなど穴がないよう対策を施した。さらに、なりすましが疑われる IP アドレスからのログインやフィッシングサイトへの誘導のブロックといった不正送金対策にも Akamai のサービスを活用している。

これまでの経験から、①サービス仕様を自社の状況やニーズに照らして詳細まで理解し、ベンダー任せにしないこと、②他社と対策／対策製品の情報交換をする、③自らの弱点を詳らかにし、経営と共有することが重要といえる。そうすることで、セキュリティチームとしてのスキルが上がり、当社が知らない対策や良い対策製品を把握でき、経営との風通しもよくなる。

■標的型攻撃対策について

2015 年 5 月の日本年金機構の事案が起きた際に、同様の攻撃を受ければ当社も同じ事態になりかねないという強い危機意識を持ち、全社プロジェクトチーム（PT）を設置し対策を立案・推進した。この時には、一斉点検（個人情報がしかるべき場所に配置されているか）、人的チェック強化策の検討など、現対策の総点検とリスク再確認、出口対策、内部対策の強化、対策製品の追加導入といった追加対策等を行った。

当時の状況は、多段であり一定の防御が可能とも思われたが、ゼロデイ標的型攻撃等でマルウェア感染するとすり抜けてしまうといったシナリオが考えられた。そこで、①犯罪者が個人情報に辿り着くハードルを上げることを目的として、認証ゲートウェイの導入やファイルサーバの点検強化を行い、②犯罪者の内部偵察行為を検知し侵入拡大を抑止することを目的としてふるまい検知機導入といった内部対策、③マルウェアの C&C サーバとの通信のハードルを上げることを目的としてプロキシ認証追加、④大量な情報漏洩の阻止を目的として POST サイズ制限、⑤情報窃取（外部送信）の抑止を目的とした仮想ブラウザの導入といった出口対策を追加的に講じることとした。

JNB 流対策の特徴の 1 つは、無償でできる対策もフル活用することである。例えば、フィッシング対策に WAF を活用するといったベンダーが想定しない利用方法をする、入力サイズの制限や認証要求といったプロキシの設定変更をするといったセキュリティ製品を使い倒すこと、また、新製品導入前に既存製品での対応可否を確認することが重要である。さらに、Office の保護されたビューの設定や、不要なファイル共有プロトコルの無効化（SMBv1）、C ドライブの管理共有無効化、悪性 TLD（Top Level Domain）のブロックといったプロキシの設定など無償の対策、機能の無効化などでも脆弱性を突いた攻撃やマルウェア感染も有効な防御方法の 1 つになり得る。

■不正送金対策

当行は 2017 年 8 月、大量のなりすましログインの被害に遭い、当行を騙るお客様への不審な電話が数十件あった。高額預金者への架電が優先されていたとのことで、なりすましによる銀行サイトへのログインをする者、ログインに成功した口座残高の中身を調べる者や預金者の電話番号を調べて電話をかける者等、犯罪者の分業化が進んでいるという印象であった。

また、最近は不正アプリのインストールと、音声によるフィッシング（ヴィッシング）を

合わせた事件も 2018 年 1 月以降国内でも確認されている。これは、犯罪者が宅配業者等を騙る SMS を送信､不正アプリをインストールさせお客様のスマホの連絡先をアップロード、正規銀行のアプリを削除して偽銀行のアプリを追加、犯罪者が詐取した電話番号に電話しお客様から認証情報（One Time Password）を聞き出し不正送金を実行するというものである。

これらの事例から、スマホアプリへの攻撃を考慮する必要性も増しており、また、攻撃内容も多様化していると言える。スマホアプリへの対策は、不正送金対策としてももちろんのこと、登録連絡先に知人を装ってばらまかれた不正な SMS を開封、応答する確率が高く、被害が拡大する危険性が高いことからも重要である。

また最近は、IoT 機器を踏み台にした不正アクセスも増えており、空きポートのある IP からは不正ログインが繰り返し行われるケースが多いため、リモート操作系のポートが空いている IP アドレスをモニタリングし、こうした IP をブロックすることは金融機関の対策として重要である。

さらに、ブラウザ言語が急に変化している場合、不正取引を目的とした外国人によるなりすましログインである可能性が高いため、外国語設定による初回ログインの検知も重要な不正送金対策の 1 つである。また、人的なログ監視には限界があるので、PaloAlto 社の「MINEMELD」という情報収集ツールも利用し、各種サイトから Threat Intelligence を自動取得し機械的な監視を強化している。

■まとめ

現在 150 社 700 名超が参加する金融 ISAC における連携によって、複数金融機関における不正送金を未然に防げた事例もある。実は一番大切なのは顔の見えるネットワークによるリソースシェアリング／情報シェアリングである。金融 ISAC の強みは、信頼のおける相談相手、同じような悩みを持つメンバー、先生役みたいな人が見つかり、彼らとのネットワークによって 1 社では解決が困難な難しい諸般の問題に迅速かつ的確に対応可能なことである。

最後に、当行流のセキュリティ対策のポイントをまとめると、①リスクも隠さずに経営にこまめに報告し、経営層の理解を得ること、②先進的な技術／情報にもチャレンジし、工夫をし、柔軟な発想ができる好奇心を持ったメンバーであること、③社内外に信頼できる、協力できる顔の見えるネットワークを構築していることである。