サイバーセキュリティ対策推進による金融サービスの安全性向上

宮川 晃一　佐藤 高道　阿河 浩一　杉山 洋平

要 旨

近年、ITやインターネットの高度化及びサービス適用範囲の拡大によって金銭や事業サービス妨害を目的としたサイバー犯罪が増加の傾向にあり、その対策については大きな課題になっています。特に重要インフラを狙った攻撃は世界的に増加しており、なかでも金銭を目的とした金融機関を狙った攻撃が増加傾向にあります。

本稿では、最新のサイバーセキュリティの脅威トレンドを解説し、金融庁の方針をもとに金融機関への提言と課題について整理し、NECの金融機関向けサイバーセキュリティの取り組みについて紹介します。

KeyWords

サイバーセキュリティ／IoT／DDoS／マルウェア／ランサムウェア／不正送金／AI／金融

1. はじめに

昨今、サイバー攻撃・犯罪は世界的に見ても増加の傾向にあり、その被害が拡大を続けています。特に国の重要インフラと言われている情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット及び石油に属する13分野の「重要インフラ事業者等」においては、サイバー攻撃によって国民生活に甚大な被害を及ぼす可能性があることから、国家戦略としての「サイバーセキュリティ戦略」が2015年9月4日に閣議決定され、サイバーセキュリティの施策を計画的に進めています。

しかしながら、今後日本で開催される国際的なビッグイベントに向けて、日本自体が大きな注目を集める一方で、悪意ある者の関心の対象ともなり、サイバー攻撃などのリスクが更に高まりつつあります。

2. 最新の脅威トレンド

2016年12月に、日本ネットワークセキュリティ協会（JNSA）が「JNSA2016　セキュリティ十大ニュース」[1)]を発表しました（**表1**）。

このなかで、金融機関向けサイバーセキュリティの脅威として特出すべきものとしては、1位の「IoT機器による史上最大規模のDDoS攻撃の実態が明らかに」と2位の「独立行政法人情報処理推進機構（IPA）から“ランサムウェア感染を狙った攻撃に注意”と注意喚起」及び、攻撃目標として重要省庁を狙った6位の「防衛省と自衛隊の情報基盤へのサイバー攻撃」（国家重要インフラへの攻撃）があげられます。いずれも、今年の脅威のトレンドとして

表1　JNSA2016　セキュリティ十大ニュース

順位	2016 セキュリティ十大ニュース
【1位】	10月14日 IoT 機器による史上最大規模の DDoS 攻撃の実態が明らかに ～防犯カメラなどの IoT デバイスのセキュリティは喫緊の重要課題～
【2位】	4月13日 IPA から「ランサムウェア感染を狙った攻撃に注意」と注意喚起 ～ランサムで　資料使えず　キョウハクシ（今日白紙 / 脅迫し）～
【3位】	7月20日 政府機関から「ポケモン GO」の利用者向けに注意喚起 ～国民全体のセキュリティ意識向上へ GO!～
【4位】	3月12日 人工知能が囲碁の世界トップ棋士に完勝 ～AI はビッグブラザーの夢を見るか ?～
【5位】	10月24日 IPA 新設国家資格「情報処理安全確保支援士」の初回申請受付を開始 ～セキュリティ人材不足の切り札となるか～
【6位】	11月28日 防衛省と自衛隊の情報基盤へのサイバー攻撃 ～外に開かれた防衛系大学 PC を踏み台に本丸へ侵入か？～
【7位】	11月8日 アメリカ大統領選挙はドナルド・トランプ氏が勝利 ～トランプ現象は日本のセキュリティに向かい風か？～
【8位】	6月27日 佐賀県教育委員会は不正アクセス被害を公表 ～17 歳の少年の犯行、ダークサイドとゲーム感覚の狭間～
【9位】	6月14日 JTB グループの Web サイトから大量の個人情報流出か ～巧妙化する標的型攻撃メール、問われる日頃からの備え～
【10位】	4月14日 EU、一般データ保護規制 (EU プライバシー規制) 正式に採択 ～個人データの変化と脅威の遍在化に対応した新しいルール～

（出典：日本ネットワークセキュリティ協会（JNSA））

引き続き警戒をする必要があります。

また、このランキングにはありませんが、2016年、金融機関における脅威として、インターネットバンキングを利用した不正送金が大きなニュースになりました。次節より、金融機関に関連する主な脅威について解説いたします。

2.1 IoT機器によるDDoS攻撃

DDoS攻撃は攻撃手法としては旧来からあるものですが、その発信元がIoT機器になっている点が特徴です。

2016年9月下旬、米国の情報セキュリティサイト「Krebs on Security」が、史上最大規模のDDoS攻撃によってダウンしました[2)]。この時に使用されたマルウェア（ボットネット*）は、「Mirai」と呼ばれ、主にWebカメラやルータやデジタルビデオレコーダーなどのIP化されたIoTデバイスを踏み台としたボットネットを形成し、攻撃を仕掛けました（**図1**）。サイトオーナーのKrebs氏のブログ記事によれば、サイトを保護していたAkamaiが、ピーク時には今までに経験した最大規模の約2倍近いトラフィック量（最大620Gbps）を観測したそうです。サイトへの攻撃後、ハッカーフォーラム上でMiraiのソースコードが公開されたことも話題となりました。このソースコードはGitHub（ソフトウェア開発者のための共有ウェブサービス）上に転載され、誰でも中身を見ることができるようになっています。このことから、今後はある程度ITの知識のあるエンジニアであれば同様の攻撃を行うことも容易であることを示唆しており、大きな脅威としてとらえる必要があります。

また、この攻撃の基本的な原因となっているのは、IoT機器の初期のID/パスワードが変更されない状況や、ハードコーディングされたビルトインアカウントによる脆弱なID/パスワードの組み合わせです（**表2**）。

金融機関においては、例えばATM機器を監視する監視カメラが前述のようなID/パスワードの組み合わせになっていないかを再度点検する必要があります。

金融機関が大規模なDDoS攻撃を受けた場合、インターネットバンキングサービスの停止などの障害が想定され、利用者へ直接的な被害が及ぶことも考えられます。

2.2 ランサムウェア

ランサムウェア（**図2**）とはマルウェアの一種で、感染したPCをロックしたり、特定のファイルを開けなくしたりします。ランサムウェアの「ランサム（RANSAM）」とは「身

表2　よく使われているIoT機器の安易なパスワード例（一部）

ユーザー名	パスワード	ユーザー名	パスワード
666666	666666	administrator	1234
admin	（なし）	Administrator	admin
admin	1111	guest	12345
admin	1234	guest	guest
admin	12345	mother	fucker
admin	54321	root	（なし）
admin	7ujMko0admin	root	0
admin	admin	root	1111
admin	admin1234	root	1234
admin	pass	root	54321
admin	password	root	7ujMko0admin

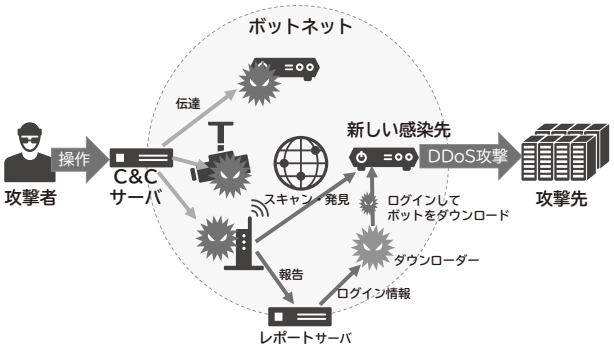


図1　Miraiボットネットのイメージ

図2　ランサムウェア Crypt Locker の画面例

* ボットネット：インターネット経由の命令によって遠隔操作をされてしまっているコンピュータ群のこと

代金」という意味で、感染すると、これを解除する身代金を支払うように要求してきます。また、身代金の要求には仮想通貨を指定されることが多く、容易に足がつきにくく現金化しやすい手段がとられているのが特徴です。

ランサムウェアは、開発者が直接犯行に及ぶのではなく、多くのアフィリエイターを経由し、メーリングリストなどを使って配布されます。

ランサムウェアが実行されて開発者に入金が行われると、アフィリエイターに一部がキックバックされる仕組みです。

ランサムウェアは手っ取り早く金銭化できるメリットがあり、攻撃者にとっては非常に都合のいい手段であるため、急激に増加しています。

ランサムウェアに感染した場合は、決して金銭の要求には従わず、速やかにバックアップからの復元を検討することを推奨します[3]。これは、PC以外のサーバ機器やスマートフォンデバイスなども含めて、全体的なバックアップ計画を見直すことも含まれます[4]。

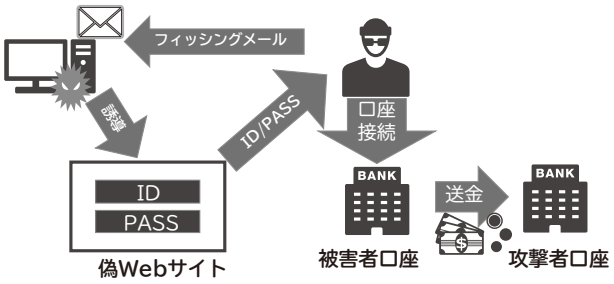


図3　不正送金詐欺の手口

2.3 マルウェアによる不正送金

2016年、インターネットバンキングを狙ったマルウェア「Gozi」（別名：「Ursnif」、「Snifula」、「Papras」）が流行し、多くの金融機関で不正送金被害がありました[5]。

特徴としては、請求書を装ったフィッシングメールを利用者に送信してマルウェアに感染させ、利用者がインターネットバンキングを利用するとID/パスワード情報を奪取し、その情報を使って不正送金を行うものです（**図3**）。更に感染した端末からは、その他の個人情報が奪取される恐れがあります。この他、不正送金をマルウェア自身が行うものも流通しており、今後はさまざまな手法による攻撃が出てくると思われます。

バンキングマルウェアの被害に遭わないためには、利用者の注意や多要素認証の利用など、基本的には利用者側の対策が主になりますが、最近はAIを活用した防御の技術も研究開発されています。

3. 金融機関への提言

金融庁は、「平成28事務年度金融行政方針」において[6]、FinTechへの対応と併せ、サイバーセキュリティを一層強化することを求めています。また、2016年6月15日の内閣

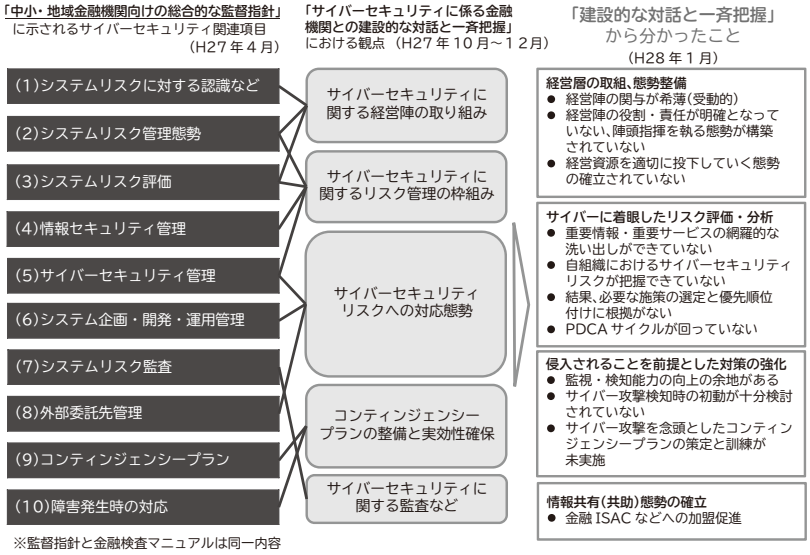


図4　金融庁監督指針に示されるサイバーセキュリティ管理

サイバーセキュリティセンター（NISC）の重要インフラ専門調査会（第7回会合）において、金融庁から「金融機関におけるサイバーセキュリティの対応状況」が報告されました[7]。その内容は以下の通りです（**図4**）。

NECとしてはこの方針を受け、以下のような課題があると考えています。

(1) 金融機関の経営層のサイバーセキュリティに関する理解を深める必要がある。

(2) サイバーセキュリティは一過性のものではなく継続的に強化が必要であり、今後日本で開催される国際的なビッグイベントを見据え、業界を越えた連携が必要である。

(3) サイバーセキュリティ対策は、大手金融機関の対応は進んでいるが中小金融機関は進んでいない。サイバーセキュリティ予算が経営上厳しい中小金融機関に対する廉価サービスや人材育成サービスの提供が必要である。

(4) 現在のサイバーセキュリティベンダーの支援体制は、東京のベンダーに集中しているため、全国を網羅できていない。

サイバーセキュリティ対策は後付けで検討されることが多い課題ですが、本来はサービス企画や設計の段階から想定されるリスク分析を適切に行い、開発予算もその対応を見越したものであるべきです。また、リスクは一定ではないため随時見直しを行い、新たな脅威と向き合っていくべきものです。すなわちサイバーセキュリティは金融機関の経営者が積極的に関与していくべき領域の課題であり、そのリスクについて一層の理解を深めていくことが必要です。

4. NECの金融機関への取り組み

前述の課題認識から、今後のNECの金融機関への取り組み施策として、以下を展開しています。

(1) 経営層への働きかけと人材育成支援

各種セミナー開催や個別訪問による啓蒙活動などを実施し、経営層への働きかけを随時行っています。また、人材育成プログラムによる人材育成支援を展開しています。

(2) サイバーセキュリティリスク管理支援と技術対応策

サイバーセキュリティに関するリスク分析などのリスク管理の支援を行い、それに基づいた具体的な対応策の検討を行っています。また、技術対応策としてNEC the WISE のAI技術を応用した対策を推進しています。

(3) 関連団体との情報交換と情報提供サービス

一般財団法人日本サイバー犯罪対策センター（JC3）、公益財団法人金融情報システムセンター（FISC）などの関連団体との情報交換により、最新の脅威情報やインシデント情報など迅速に取得し、その関連情報を含めた情報提供を行っています。

(4) サイバーセキュリティ総合運用支援（SOCサービス）

NEC独自にセキュリティオペレーションセンター（SOC）サービスを展開し、中小金融機関向けには、地方拠点を活用した共同SOCサービスの提案を行っています。また大手金融機関へは、SOC業務にAIを活用した検知能力の高度化などの支援を行っています。

5. むすび

2016年7月、NEC金融システム開発本部及び金融ソリューション事業部では、金融領域における、サイバーセキュリティ対策推進体制を構築しました。この体制により、金融機関に対して、安全・安心なセキュリティソリューションを提供していくとともに、新しい価値の創造を実践していきます。

参考文献

1) JNSA 2016セキュリティ十大ニュース
http://www.jnsa.org/active/news10/index.html
2) IPA: 安心相談窓口だより
https://www.ipa.go.jp/security/anshin/mgdayori20161125.html
3) IPA:【注意喚起】ランサムウェア感染を狙った攻撃に注意
https://www.ipa.go.jp/security/topics/alert280413.html
4) IPA: パソコン内のファイルを人質にとるランサムウェアに注意!
https://www.ipa.go.jp/security/txt/2015/06outline.html
5) JC3: インターネットバンキングマルウェア「Gozi」による被害に注意
https://www.jc3.or.jp/topics/gozi.html
6) 金融庁「平成28事務年度金融行政方針」
http://www.fsa.go.jp/news/28/20161021-3/02.pdf
7) NISC: 金融機関におけるサイバーセキュリティの対応状況
http://www.nisc.go.jp/conference/cs/ciip/dai07/pdf/07shiryou04.pdf

執筆者プロフィール

宮川 晃一
金融システム開発本部
シニアエキスパート

佐藤 高道
金融システム開発本部
シニアエキスパート

阿河 浩一
金融システム開発本部
マネージャー

杉山 洋平
金融システム開発本部
主任

関連URL

NEC Cyber Security Solution
http://jpn.nec.com/cybersecurity/

NEC 技報のご案内

NEC技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報(日本語)　　NEC Technical Journal(英語)

Vol.69 No.2　デジタルトランスフォーメーションを加速するFinTech特集

デジタルトランスフォーメーションを加速するFinTech特集によせて
NECが目指すFinTechの全体像

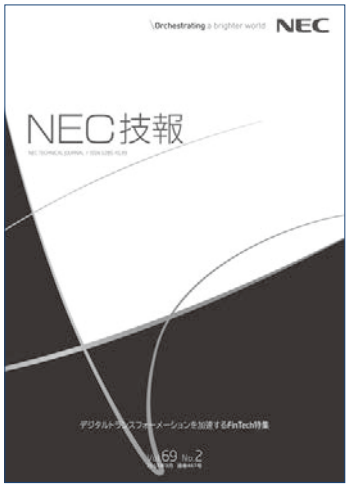
◇ 特集論文

FinTech時代の新しい金融と技術の関係
AIがもたらす金融サービスの変革
ブロックチェーンによる企業間連携の実用化に向けた取り組み
ロボットとAIの組み合わせによる顧客コミュニケーションの高度化
ウェアラブルデバイスを用いた安全・安心・便利な見守りサービス
生体認証によるモバイルサービスのセキュリティと利便性の両立
新たなサービスのスピーディな提供を可能にするモバイルアプリ高速開発
サイバーセキュリティ対策推進による金融サービスの安全性向上
FinTechのセキュリティ強化に貢献するマルチパーティ計算技術

◇ NEC Information

C&Cユーザーフォーラム&iEXPO2016　Orchestrating a brighter world
基調講演
展示会報告

NEWS
2016年度C&C賞表彰式開催



Vol.69 No.2
（2017年3月）

特集TOP