金融分野の事例
金融分野における インシデントレスポンスチームの活動

宮崎 真理 Miyazaki Mari
畑中 寛之 Hatanaka Hiroyuki
高橋 克典 Takahashi Katsunori
永田 桃子 Nagata Momoko

インターネットバンキングを狙ったマルウェア感染の拡大，DDoS攻撃の発生など，国の重要インフラ分野の一つ「金融」において，サイバー攻撃の脅威が深刻になっている。このような背景の下，各金融機関においてサイバー攻撃対応態勢の確立が急速に進み，金融機関間でのサイバー攻撃関連情報の共有なども活発になっている。

日立グループ全体のインシデントレスポンスチームHIRTの金融分野サブセットであるHIRT-FISでは金融分野におけるインシデントレディネス活動を推進している。また日立の運営するインターネットバンキング共同センターサービス「FINEMAX」ではサービス開始以来，常に新しい脅威へのセキュリティ対策を提供し続けている。

1. はじめに

日々報道されるソフトウェアなどの脆（ぜい）弱性，セキュリティ事件・事故の発生は，重要インフラ企業はもとより，重要インフラ企業のシステムを担う側にとっても大きな脅威である。日立の金融システム事業では公益財団法人金融情報システムセンター（FISC：The Center for Financial Industry Information Systems）の発刊する「金融機関等コンピュータシステムの安全対策基準・解説書」（以下，「FISC安全対策基準」と記す。）の改訂にかかわり，またこれを意識したシステム構築・運用を行うなど安全・安心な金融システムの実現に寄与してきた。

しかし，昨今のマルウェアを使ったインターネットバンキングにおける不正送金の多発，脆弱性情報展開の活発化などを受け，今までとは違うアプローチが現場では求められている。ここでは金融分野における日立のセキュリティ対策の取り組みを述べる。

2. 金融業界におけるセキュリティ動向

2.1 金融庁の動き

2015年4月，金融庁はシステムリスクおよびインターネットバンキングに係る「主要行等向けの総合的な監督指針」および「金融検査マニュアル」などの一部改正を行った。

この改正にて強くうたわれたのは，インターネットバンキングにおけるセキュリティ確保，およびCSIRT（Computer Security Incident Response Team）などのサイバーセキュリティ管理態勢の整備である。また不正侵入検知システム，DDoS（Distributed Denial of Service）攻撃への対応策，不適切な通信の検知・遮断といった具体的な技術策の導入についても言及している。

同庁はさらに同年7月，「金融分野におけるサイバーセキュリティ強化に向けた取組方針」を公表した。この方針に基づき，各金融機関に対しサイバーセキュリティ管理態勢の取り組み状況やその実効性の実態把握のためのヒアリングを実施している。

2.2 FISCの動き

FISCが「金融機関におけるサイバー攻撃対応に関する有識者検討会」を立ち上げたのは2013年6月のことである。産・学（官もオブザーバとして参加）の有識者にて金融機関に対するサイバー攻撃の現状把握と今後の取り組みについて検討を行い，最終的に報告書が取りまとめられた。この報告書を基に同センターが発行する「FISC安全対策基準第8版追補」の改訂について検討がなされ，サイバー攻撃対応態勢の整備に関する項目が新たに追加された。

さらに2015年7月には「FISCサイバーセキュリティ参考情報」の運用が同センターの新たな取り組みとしてスタートしている。これはセキュリティインシデントの発生時などにFISC安全対策基準での解釈運用が適切に行われ

ることを目的とし，有用な留意点，参考情報を公表するものである。

2.3　情報共有コミュニティの動き

近年，金融機関は情報共有コミュニティへの加盟によりサイバー攻撃関連情報の連携を活発に行っている。

大手金融機関どうしのセキュリティに関する勉強会が起点となり，2014年11月，国内金融機関間のサイバーセキュリティに関する情報を共有するための組織，一般社団法人金融ISAC（Information Sharing and Analysis Center）が活動を開始した。

金融ISACのホームページによれば，2016年4月末時点での会員数は正会員・準会員を合わせ222会員となっている。インシデントや脆弱性情報などの共有が行われ，特定の重要課題についてはテーマごとのワーキンググループ活動が行われているようである。

また社内にCSIRTを立ち上げた金融機関が日本コンピュータセキュリティインシデント対応チーム協議会（NCA：Nippon CSIRT Association）へ加盟する動きもある。NCAは2007年に国内CSIRT間の情報共有・連携を目的とし発足したコミュニティであり，2016年4月現在の加盟総数は137チームである。このうち金融機関のCSIRTの数は27チームとなっており，今後も加盟が増加する見込みである。

このように国内金融機関においてサイバーセキュリティ関連情報の共有を行う文化が急速に醸成されつつある。

3.　インターネットバンキングにおけるセキュリティの取り組み

3.1　不正送金被害への対応

インターネットバンキングを取り巻く状況はここ数年の間に劇的に変化している。警察庁の広報資料によれば，2013年頃から国内金融機関における不正送金被害が急増しており，2015年には被害額が初めて30億円を超えた。現在，銀行において最も重要視されるセキュリティ対策が不正送金被害への対策であることについては疑いの余地がない。

多様化するサイバー攻撃に対して，インターネットバンキング共同センターサービス「FINEMAX」では，1999年のサービス開始以来，常に新しい脅威へのセキュリティ対策を提供し続けてきた。将来起こりえる未知の脅威までを予測して事前に対策を取ることは困難だが，現在までに確認されている脅威に対して有効なセキュリティ対策については，ホールセール／リテールともに2016年度中のリリースを予定している。これにより，一般社団法人全国銀行協会の「セキュリティ対策向上・強化等に関する全国銀行協会の『申し合わせ』」に準拠したセキュリティ対策機能のリリースを完了する予定である。

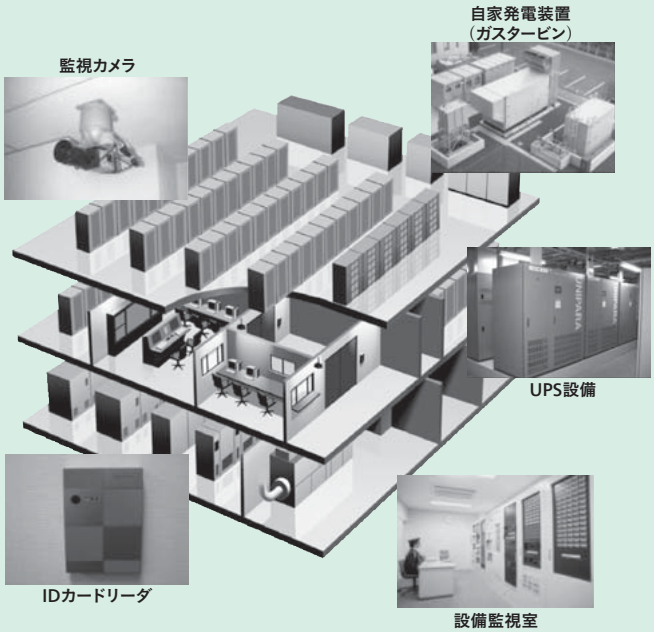
また運用面での不正送金対策については，被害の早期発見と予防に努めている。万一預金者が不正送金被害に遭ったときは，他の銀行にて過去に同様の不正送金被害が発生していないかを調査し，疑わしい取り引きを確認した場合は速やかに各行へ連絡を行っている。さらに，将来同様の

立地・建屋
- 天災の少ない安全性に恵まれた地域・地盤環境
- 直接基礎方式の採用により東日本大震災クラス（震度7相当）の地震に耐えうる耐震性を確保
- 警察署，消防署に隣接
- 金融業界「FISC基準」に準拠した設備

電源・空調設備
- 発電所より地下埋設にて直接受電
- 電源設備の2重化により無停電化を実現
- UPS，非常用自家発電設備などによる停電対策を実施
- 災害時の水道供給停止に備えた空冷式空調設備を設置

情報セキュリティ
- ISMS認証基準に準拠したセキュリティマネジメント
- 品質管理システム「ISO9000」に準拠した運用管理体制

その他
- 同建屋内にハードウェア保守部隊が駐在



注：略語説明　FISC（The Center for Financial Industry Information Systems），UPS（Uninterruptible Power Systems），ISMS（Information Security Management System）

図1｜FINEMAXのデータセンター設備
FISC基準，ISO27001，ISO9000などの業界基準，公的基準に準拠したデータセンター設備により高い信頼性・安全性・機密性を実現している。

不正送金が発生する場合を想定したアクセス監視を行い，監視対象からのアクセスがあった場合についても速やかに連絡し，早期発見に努めているところである。

3.2　FISCへの対応

インターネットバンキングの包括的なセキュリティ対策として，FISC安全対策基準に沿って，設備面・運用面・技術面それぞれの観点でのセキュリティ対策を推進している。

まず設備面においては，ISO（International Organization for Standardization）など公的基準に準拠したデータセンター設備により，高い信頼性・安全性・機密性を実現している（図1参照）。

次に運用面においては，運用管理基準を定め，内部監査や外部監査を通じて管理基準の実効性確認や実施内容の検証を行っている。

技術面においては，インターネットへの公開サーバや情報資産の保護のため，ネットワークレベルとアプリケーションレベルで複数の対策を取り，さらには定期的な脆弱性診断の実施により実効性の検証を行っている。

4.　金融分野におけるCSIRT活動「HIRT-FIS」

2012年10月，日立グループのCSIRTであるHIRT（Hitachi Incident Response Team）の金融分野サブセットとしてHIRT-FIS（Financial Industry Information Systems HIRT）を設置した（図2参照）。

金融分野に特化したCSIRTプロフェッショナルチームをめざし，金融庁・FISCのレギュレーションやガイドといった業種特有の背景，動向を踏まえつつ，この分野におけるインシデントレディネス活動を推進している。

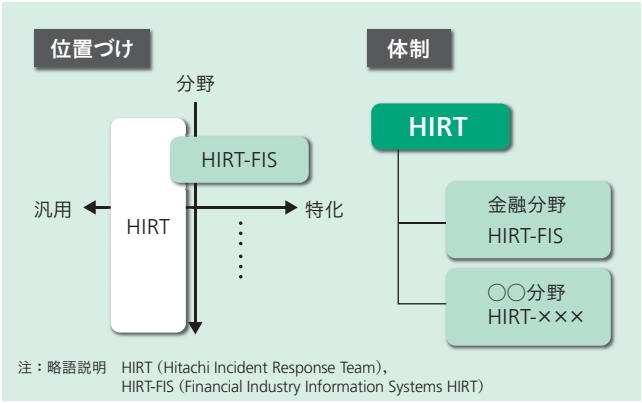


図2｜HIRT-FISの位置づけ
HIRTの金融分野サブセットとして金融システム事業部内に設置した。

4.1　組織内における活動

サイバー攻撃対応においては，脅威についてキャッチアップし，早期に対策を検討して展開することが欠かせない。HIRT-FISでは公表されているインシデント情報を日々チェックし，イントラネットサイトへ掲載している。

この活動の目的は，金融分野に携わる日立グループの営業担当者・SE（System Engineer）に最新のセキュリティ関連情報を提供することで，想定される脅威を減じる活動を少しでも早く開始することにある。

情報は以下の4つのカテゴリーに分けて掲載している（図3参照）。

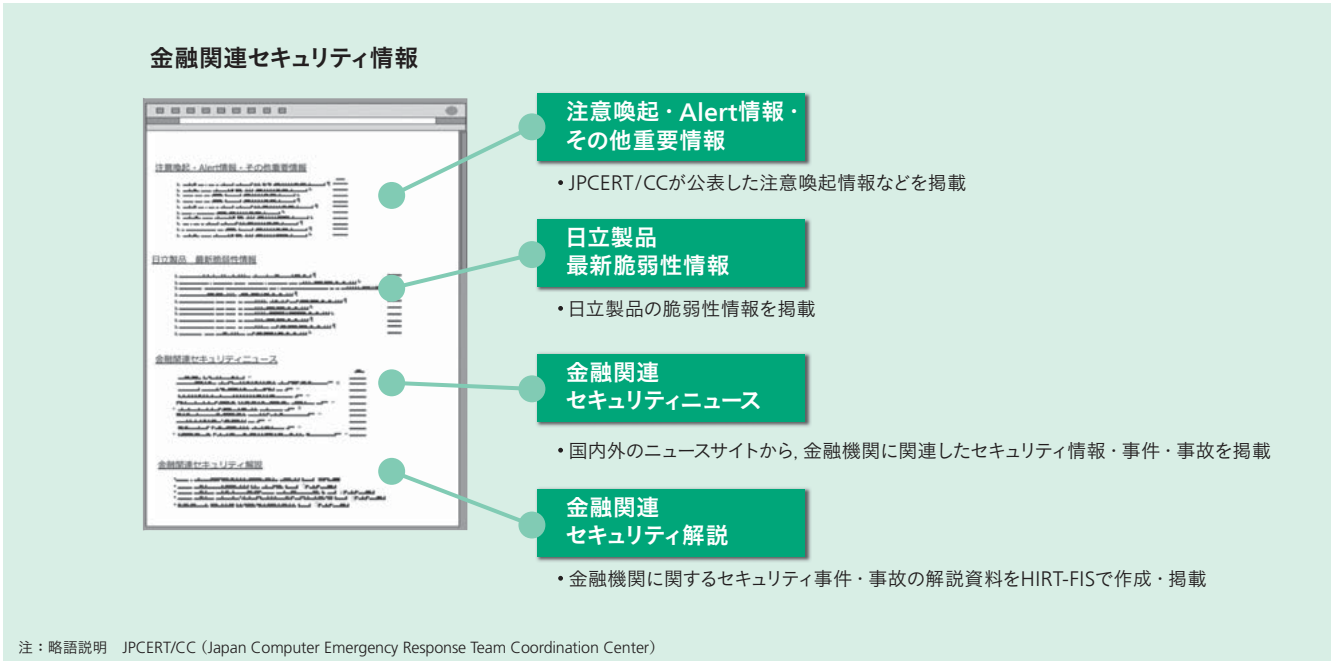


図3｜HIRT-FISポータル
イントラネットで金融関連のセキュリティ情報を公開している。

(1) 注意喚起・Alert情報・その他重要情報

一般社団法人JPCERTコーディネーションセンター(Japan Computer Emergency Response Team Coordination Center：JPCERT/CC) が公表したアラート情報を中心に掲載

(2) 日立製品　最新脆弱性情報

日立が公表した脆弱性情報を掲載

(3) 金融関連セキュリティニュース

国内外の金融機関関連のインシデント情報を掲載

(4) 金融関連セキュリティ解説

関心の高いテーマごとに解説資料を作成し掲載

これらの情報を基に，社内より寄せられる問い合わせの対応をはじめ，セキュリティ設計書・セキュリティ運用手順書などのレビュー，脆弱性診断結果の評価などの支援を行っている。

またSE向けのセキュリティガイドの整備，メールマガジンによる社内への情報発信，さらには金融分野におけるセキュリティ人材の育成も当チームの活動となっている。

4.2　組織間の連携活動

HIRTは日立グループの対外的なCSIRT窓口としてサイバーセキュリティ対策への協力を行っており，NCAを通じた組織間CSIRTの連携強化を推進している。これは異なる組織のCSIRTどうしが連携し，サイバー攻撃を鳥瞰（かん）することで問題解決を図り，互いの活動に寄与することを意図したものである。

HIRT-FISは，HIRTの金融分野サブセットとして，本活動において金融機関CSIRTとの連携を担当している。

5.　おわりに

ここでは金融システムを取り巻くサイバーセキュリティの状況と，FINEMAXのセキュリティへの取り組み，またHIRT-FISの取り組みについて述べた。

金融機関は従来，ローテーションでの要員異動が行われており，情報システムにかかわる従業員もこの中に含まれていた。しかし「セキュリティ人材」という極めて専門性の高い職種については「特任職」として扱うなど金融機関の人材施策も柔軟に変化してきている。このことは，金融業界におけるサイバーセキュリティ対応態勢が確実に整ってきていることを示しており，また専門性の高いCSIRT間の連携を行うための環境が熟してきたことをも示している。

日立が提供するサービスにおける取り組みと，セキュリティ専門部門による取り組みという両輪を備えた日立のセキュリティ活動は，金融機関のパートナーとして安全・安心な金融システムの実現に寄与できるものと考える。

参考文献など

1)　金融情報システムセンターホームページ，https://www.fisc.or.jp
2)　金融庁ホームページ，http://www.fsa.go.jp
3)　一般社団法人金融ISACホームページ，http://www.f-isac.jp
4)　日本コンピュータセキュリティインシデント対応チーム協議会ホームページ，http://www.nca.gr.jp
5)　警察庁ホームページ，https://www.npa.go.jp

執筆者紹介

宮崎 真理
日立製作所 金融ビジネスユニット 金融システム事業部
事業推進本部 システム統括部 所属
現在，HIRT-FISにおいてCSIRT活動に従事

畑中 寛之
日立製作所 金融ビジネスユニット
金融チャネルソリューション事業部 チャネルソリューション本部
チャネルソリューション第一部 所属
現在，日立の金融チャネルの新規企画立案に従事

高橋 克典
日立製作所 金融ビジネスユニット 金融システム事業部
事業推進本部 システム統括部 所属
現在，HIRT-FISにおいてCSIRT活動に従事

永田 桃子
日立製作所 金融ビジネスユニット 金融システム事業部
事業推進本部 システム統括部 所属
現在，HIRT-FISにおいてCSIRT活動に従事