個人情報不正アクセスに関する
調査報告書

２０１６年7月１４日

日本テレビ放送網株式会社　個人情報不正アクセス調査委員会

第１　調査の概要

１　委員会設置の経緯

日本テレビ放送網株式会社（以下「NTV」という。）は、NTV の個人情報の取扱い委託先の一つである株式会社フォアキャスト・コミュニケーションズ（以下「フォアキャスト」という。）において発生した、フォアキャストが NTV から受託した NTV の視聴者等の個人情報の一部に係る情報漏えい事故（以下「本件事故」という。）について、その事実関係の調査、本件事故の原因究明、責任の所在の明確化、再発防止策に関し、専門的及び客観的な見地からの調査及び検討が必要であると判断し、以下の委員により構成される委員会（以下「本委員会」という。）を設置した。

委員長　大井 哲也　（TMI 総合法律事務所　弁護士）
委　員　佐藤 力哉　（TMI 総合法律事務所　弁護士）
委　員　星澤 裕二　（PwC サイバーサービス合同会社　パートナー）
委　員　草間 嘉幸　（NTV　コンプライアンス推進室法務部長（兼）情報保護推進事務局長）
委　員　鈴木 重利　（NTV　技術統括局 IT 推進部長（兼）サイバーセキュリティ推進事務局長）

その後、NTV における人事異動に伴い、2016 年 5 月 31 日をもって草間委員が退任し、同年 6 月 1 日付けで以下の委員が本委員会の委員に新しく就任した。

委　員　横山 武信　（NTV　コンプライアンス推進室法務部長（兼）情報保護推進事務局長）

２　調査の目的、受任事項、調査期間及び調査方法

本報告書は、本件事故の事実関係の調査、その原因調査、責任の所在の明確化及び再発防止策の提言の受任事項に関して、2016 年 4 月 25 日から 7 月 13 日までを調査期間とし、本報告書提出時における本委員会の見解を報告することを目的としたものであり、本委員会は、本報告書を作成するに当たり、インタビューによる調査、ドキュメントレビュー、各種ログによる調査、実地による技術調査及び Q&A シートによる質疑応答に基づいて調査を実施し、上記調査期間内に開示等された情報の範囲内で、その情報の真正及び正確性を前提として本報告書を作成した[1]。

[1] 本報告書は、本委員会において作成した詳細な調査報告書を基に、一部匿名化処理を行った上、NTV の情報セキュリティ体制等の企業機密に関わる記載等の公表に適さない内容を削除する方針で作成された要約版である。

第２　本件事故の概要及び経緯

１　本件事故の概要

本件事故により漏えいした個人情報（以下「本件情報」という。）は、番組の視聴者参加イベントの応募者等に関する情報である。調査の結果、現時点で本件情報以外に本件事故による個人情報の漏えいは確認されておらず、本件事故による漏えい件数は、延べ数で合計 42 万 8138 件となる。

２　本件事故の経緯

本件事故に関連して発生したイベントの時系列の概略は、以下の表のとおりである。

日時		当事者	イベント
2016 年 4 月 20 日	13:39	攻撃者	攻撃者が OS コマンドインジェクションによる攻撃を開始
	16:24	フォアキャスト	サーバ負荷上昇の監視アラートを受信
	17:08	フォアキャスト	フォアキャストマネジメントシステム委員会の委員長へ事象を報告
	17:09	フォアキャスト	管理職、システム担当者等による対策会議を開始
	17:32	攻撃者	サーバ上で不正圧縮ファイル作成完了（後に判明）
	17:35	攻撃者	不正圧縮ファイルのダウンロード時に発生したと思われる http レスポンスが正常終了（後に判明）
	17:42	フォアキャスト	遠隔操作プログラムのソースコード解析作業及びケータイキット for Movable Type（以下「ケータイキット」という。）を設置している場所のリストアップ作業を開始
	18:09	フォアキャスト	サイバーセキュリティ推進事務局に第一報メール
	18:12	NTV	サイバーセキュリティ推進事務局より情報保護推進事務局へ情報共有のメール 情報保護推進事務局より情報資産保護最高管理責任者へ一報メール
	19:04	フォアキャスト	サイバーセキュリティ事務局に「報告書（第一報）」送付
	19:18	フォアキャスト	全てのケータイキットを無効化する作業を開始
	20:21	フォアキャスト	一般財団法人放送セキュリティセンタープライバシーマーク推進部にメールにて報告 ケータイキットの提供元である A 社とその販売代理店である B 社に電話連絡
4 月 21 日	0:28	フォアキャスト	サイバーセキュリティ事務局に「報告書 V0.9」、「応募フォーム取得項目」送付
	2:35	フォアキャスト	個人情報データを安全な領域へ退避させる
	8:00	NTV	情報資産保護最高管理責任者から社長へ報告
	9:00	NTV	インシデント対応ガイドラインに基づき、危機レベル S の緊急対策会議（各セクション緊急招集・インシデント対応責任者・情報資産保護最高管理責任者）
	11:00	NTV	緊急対策会議第 2 回招集
	15:30	NTV	委員就任予定の外部専門家を含めた緊急対策会議第 3 回招集
	16:30	NTV	危機管理委員会拡大実務者会合（外部専門家を含めた調査委員会の設立が承認され、本委員会を設立、本件事故の公表と夕方ニュースでの報道を決定）

日時		当事者	イベント
	18:00	NTV	プレスリリース初報を発表及び HP で告知 東証への適時開示を実施
	18:12	NTV	夕方のニュース（news every.）で報道
	18:24	NTV	総務省関東総合通信局に「報告書」を送付
	19:00	NTV	コールセンター設置
	23:30	NTV	プレスリリース続報（漏えいのあった番組名）を発表
4 月 22 日		NTV	サイバーセキュリティ推進事務局から警視庁サイバーテロ対策特別捜査隊（サイバーテロ対策協議会事務局）へ電話で報告
			漏えいのあった視聴者等へお詫びのメール配信
		A 社	「緊急パッチファイルの提供を開始」と題するプレスリリースを公表
4 月 23 日		A 社	「[重要]ケータイキット for Movable Type 1.65 の提供を開始」と題するプレスリリースを公表
4 月 25 日		NTV	本委員会第 1 回全体会議開催
4 月 26 日		JPCERT/CC	「ケータイキット for Movable Type の脆弱性(CVE-2016-1204）に関する注意喚起」を公表
5 月 6 日		JPCERT/CC	「ケータイキット for Movable Type の脆弱性(CVE-2016-1204）に関する注意喚起」を更新
5 月 10 日		A 社	「[重要]ケータイキット for Movable Type 1.66 の提供を開始」と題するプレスリリースを公表
5 月 17 日		NTV	郵送でのお詫び文書送付開始
5 月 19 日		NTV	総務省関東総合通信局に「個人情報漏えい等事故報告書」を送付
5 月 20 日		A 社	「[重要] ナビゲーションの不具合に対応したケータイキット for Movable Type Ver.1.661 の提供を開始」と題するプレスリリースを公表
6 月 15 日		フォアキャスト／PwC	新システムについての脆弱性診断終了（即時対応すべき脆弱性は確認されなかった）
6 月 15 日		フォアキャスト	被害届が愛宕署（警視庁サイバー犯罪対策課）にて受理

第３　本件事故の原因調査

本件事故は、フォアキャストが、ウェブシステムの未知の脆弱性を突く攻撃を受けたことに起因して、個人情報が外部に送信されたものであり、その直接の原因は、未知の脆弱性という一見不可避とも思える偶発的な事象であった。もっとも、未知の脆弱性という点を措いても、その他の情報セキュリティ施策が有効に機能していれば避けられた事故であったともいえる。そこで、以下では、まず、本件事故の原因調査として、フォアキャストのウェブシステムの情報セキュリティに関し、技術的観点に基づく検証をするとともに、NTV 及びフォアキャストにおける個人情報の管理体制についても検証した。

1　技術的観点からの調査結果

⑴　攻撃に関するログ調査

本件事故は、A 社が提供するモバイルサイトを構築するソフトウェアのケータイキットが設置されたウェブサーバ（以下「本件システム」という。）に対するサイバー

攻撃によるものであった。本委員会にて入手したログより、攻撃内容を調査した結果、攻撃は以下の 3 種類の段階によって実施されたことが判明した。

① ケータイキット最新版（v1.641）における OS コマンドインジェクションの未知の脆弱性を利用し、本件システムへ遠隔操作プログラムを設置
② 本件システム上の遠隔操作プログラムを操作して、本件システム内部を探索
③ 本件システムから個人情報データを外部に不正持ち出し

⑵ ケータイキットに関する調査

本件事故の原因となったケータイキットについて調査結果は以下のとおりである。

① 2016 年 4 月 20 日当時のケータイキット最新版には、OS コマンドインジェクションの未知の脆弱性があった。この未知の脆弱性は、攻撃者が不正な HTTP リクエストを送信すると、OS が利用する任意のコマンドを実行してしまう問題があった。
② 当時のケータイキットのプログラムコードを分析したところ、IPA（情報処理推進機構）が広く公開している「安全なウェブサイトの作り方」[2]に示されているような基本的なセキュリティ対策を実装していなかった。

⑶ 被害対象ネットワーク・システム構成に関する調査

本調査は以下の 2 つの観点に基づいて実施した。

A) 侵入を検知・防御する対策（入口対策）
B) 侵入された後に情報の探索・流出を防ぐ対策（内部対策、出口対策）

A) 侵入を検知・防御する対策（入口対策）

① ツールによる脆弱性診断を約 2 年前に実施済みであった。しかし、今回の攻撃に悪用された脆弱性は、当該診断時には発見できなかった。また、上記時点以降は脆弱性診断を実施していない。
② IDS（不正侵入検知システム）を導入しており、常時監視をしていた。しかし、今回の OS コマンドインジェクションは検知できなかった。
なお、IPA が提供している「ウェブサイトの攻撃兆候検出ツール iLogScanner」において、当該ログを調査したところ、OS コマンドインジェクション攻撃を一部検出できた。
③ 不要なウェブリクエストがプログラム上で制限されていなかった。
④ プログラム言語の設定として不要な呼び出し関数の実行が制限されていなかった。
⑤ ファイルが不要に設置されたことを検知する仕組みがなかった。

[2] https://www.ipa.go.jp/security/vuln/websecurity.html

⑥　プログラムが動作する範囲が適切ではなかった。

B)　侵入された後に情報の探索・流出を防ぐ対策（内部対策、出口対策）

①　サーバ上に不要なプログラムが残っていた。

②　ウェブサーバのアカウントで、サーバ上のデータに自由にアクセスできていた。

③　ウェブサーバから個人情報データが保存されたディスクが直接マウントされ閲覧操作できる状態にあった。なお、ウェブサーバに不正侵入しない限り、インターネット側から当該ディスクにアクセスすることはできなかった。

④　個人情報データは、暗号化されておらず、平文で保存されていた。

⑤　削除すべき過去の個人情報データがディスクに残っていた。

⑥　個人情報データが保存されていることを推測されやすいフォルダ名を利用していた。

⑦　サーバのネットワーク設定が実装されていなかった。

⑧　ウェブサーバから外部への通信が全て許可されていた。

2　管理体制からの調査結果

⑴　全般的な情報管理体制等について

ア　NTV

NTV においては、2015 年 6 月より個人情報を含む情報資産保護のための組織及び規程の見直しがなされ、各種規程・ガイドライン等が設けられているほか、情報資産保護最高管理責任者の下、情報保護を推進するための事務局（以下「担当事務局」という。）やセキュリティを推進する事務局等が設けられ、各局・室から責任者を選任し、各局・室の下に位置する部から担当者が選任されるなどしていた。

イ　フォアキャスト

フォアキャストにおいては、個人情報保護に関する各種規定等も設けられ、組織体制として、個人情報保護管理責任者が任命され、これを委員長とする委員会（以下「担当委員会」という。）が設けられ、個人情報保護に関する管理責任者等が指名され、個人情報に関する業務を担当している。

フォアキャストは、2013 年 8 月に、保守体制が整っていること等を踏まえ、当時、同種ソフトウェアの中で最も著名なケータイキットの採用を決定した。また、同社に特段のルールや規程はなかったものの、日々セキュリティ情報発信機関の情報を確認し、業務に影響のあるものについては都度検討・対応するという運用がなされていた。

フォアキャストにおいては、情報セキュリティレベルを上げるべく、古くなったシステムを置き換えるため、2015 年 12 月より、新システムを稼働させ、順次、新システムへ移行を行っている途中であり、本件事故は、これらの移行の実施中に発生した。なお、フォアキャストの新システムに係るセキュリティ調査を実施したところ、新システムについて即時対応すべき脆弱性は確認されなかった。

⑵　本件情報の取得・管理・利用・削除フローについて

以下では、時系列に従って、NTV 及びフォアキャストによる本件情報の取得、管理、利用及び削除の各フローについての規程・運用と実態についてその概要を記載する。

ア　取得

①　NTV

視聴者等の個人情報の取得をする場合、ガイドライン上、番組制作部門が必要事項を決定し、委託先がある場合には、その選定の留意点、契約の締結・内容、指導・監督等について具体的な定めが設けられている。そして、番組制作部門は、個人情報の取得前に、台帳登録用紙に必要事項を記入し、必要な確認を得た上で、台帳に記載されることとされている。

番組制作部門が NTV の HP 上に、投稿フォームを設ける場合、NTV は、フォアキャストとの業務委託契約等に基づき、同社にその制作を委託し、個人情報の取得についてもフォアキャストに委託するのが通常の運用となっていた。番組制作部門は、フォアキャストとの間で、打ち合わせシートに基づき必要事項（利用目的、取得情報詳細、取得情報の保存期間等）を定めていた。

複数の番組関係者にヒアリングを実施した結果、本件情報の廃棄予定期限については、企画の趣旨及び取得する個人情報の性質によって様々であったことが判明した。また、本件情報の一部には、NTV と委託先との間でどちらが本件情報の取得主体となるかについての認識が共有されていなかったなどの理由から台帳登録がなされていないものもあった。

②　フォアキャスト（投稿フォームの構築と運用）

投稿フォームの構築については、業務フローを定めた書面に則り業務が行われる運用となっている。同社が NTV の投稿フォームの制作等について受託する際には、NTV の番組制作部門とミーティングを実施して打ち合わせシートを作成し、NTV の承認を得た後、担当委員会等の承認を得る。この時点で個人情報管理番号が発番され、フォアキャストの台帳に記録すべきこととされている。以上の手続の後、実際に使用する投稿フォームにつき所属部署の確認及び NTV の承認を得た上で、本番環境へのリリースを行う。

なお、以上のプロセスにおいて、フォアキャストでは複数のチームで個人情報の取扱いに関する確認事項を含んだチェックシートを用いてチェックを行う運用とされているが、実態として、同チェックシートの全項目をチェックする方法が用いられていたわけではなかった。

イ　管理・利用等

①　NTV

取得した個人情報の管理については、ガイドライン上、委託先に預託する場合には、委託先から受領証等の授受を行うこと等とされ、委託業務の実施状況や安全管理対応等を確認し、適宜報告を求めるなど、委託先を指揮、監督するものとされている。本件情報はフォアキャストへ委託したものであるが、担当事務局において、その管理に関してフォアキャストに一定の指揮・監督を行うとともに、番組制作部門に対しても指揮・監督を行うよう指示をしていたが、番組関係者にヒアリングを実施した複数の番組制作部門については、その取得当時、番組制作部門において当該指示が認識されていることは確認できなかった。取得した個人情報の利用については、ガイドラインにおいて、利用目的の範囲内で行うこと、共同利用等の場合には、担当事務局に問い合わせることなどとされている。本件情報について、NTV は、セキュリティ管理された NTV の社内システムにより閲覧・DL するか、又はフォアキャストから個人情報を保存した CD-R 等を受領して利用していた。

台帳の登録内容に変更があった場合、番組制作部門は、変更を届け出て、台帳に変更された内容を反映することとされている。また、定期的に棚卸が実施されていたが、本件情報には、正確な内容での変更届出がなされていないものや、一部台帳登録がなされていないものがあった。

②　フォアキャスト

個人情報の管理等については、取得した個人情報について、原則としてパスワード設定・暗号化を行わなければならない旨の定めこそあるものの、個人情報を取得する場合に用いるチェックシートにおいて、個人情報の暗号化についてチェックする項目はなかった。これに対し、新規にデータベースを構築する際に適用されるチェックシートには、個人情報の暗号化についてのチェック項目が存在した。前者のチェック項目として暗号化の項目が含まれていなかったのは、データベースを利用せずにファイル保存を行う場合には、非公開ディレクトリに配置することで、セキュリティが担保されているとの認識があったためだと考えられる。

個人情報の利用について、取得個人情報の受渡しは、フォアキャストに個人情報の取得を申請した情報利用者に対してのみ可能とされており、個人情報を

閲覧・利用・削除するための管理ツールを用いて利用等させる方法と、CD-Rで受け渡す方法があった。

なお、規程上、取得個人情報の台帳への登録、定期的な台帳の維持・更新等に関する定めがあるが、台帳の管理に特化した定めはない。実際の台帳の管理は、担当委員会によって行われていた。しかしながら、フォアキャストにおいて、NTV に個人情報の廃棄等に係る証明書を提出したことに伴いフォアキャストの台帳から対象個人情報を削除するという運用はなかったなど、台帳管理の運用は十分ではなかった。

ウ　削除

①　NTV

個人情報の利用が終了した場合、ガイドライン上、委託先が保有する個人情報については、番組制作部門が、委託先に廃棄を指示し、委託先から廃棄証を提出してもらい、廃棄記録とともに、担当事務局に届け出ることとされている。

NTV がフォアキャストに委託した個人情報については、個人情報の保存期間について取り決めが行われており、担当事務局へもフォアキャスト側から削除方法についての説明がなされるなどしていたが、番組関係者にヒアリングを実施した結果、一部の番組制作部門において削除方法が具体的には認識されていないものがあり、また、本件情報の一部には、廃棄記録及び委託先であるフォアキャストからの廃棄証が適正に提出されていないものもあった。

②　フォアキャスト

個人情報の利用が終了した場合又はその保存期間が満了した場合には、所定の手続に従い、当該個人情報は削除することとされていた。削除に当たっては、管理ツール等による削除作業が行われ、完了後に作業完了報告がなされることとされていた。削除作業は、NTV の番組制作部門も、管理ツールを用いた遠隔操作により行うことができた（なお、これらの削除処理を台帳に反映させることを含め、フォアキャスト内に、削除作業と台帳の管理の関係について定めるルールは存在しない。）。個人情報の最大保存期間の定めはあるが、打ち合わせシートではそれ以外の保存期間を設定できた。

また、削除処理を実行した場合、対象情報は、特定のフォルダ（以下「本件フォルダ」という。）にいったん移動するのみであった。NTV は、このような処理の運用については知らされていなかった。業務フロー書には本件フォルダに関する記載は一切なく、本件フォルダのことを知っている者自体かなり限定されており、個人情報は、結果的に、本件フォルダ内に大量に残存していた。

さらに、廃棄証明は、NTV から指示を受けた場合に限って提出していたが、NTV から廃棄証明の提出依頼があった場合に、対象個人情報が本件フォルダ

に移行したのみの段階で廃棄証明を提出していたものが存在している。また、NTV が、管理ツールを使用して遠隔操作により個人情報を削除しても、フォアキャストにおいて都度確認を行っておらず、企画終了時に削除の有無を確認したり、台帳からの削除処理を行ったりしていた。

⑶　監査・点検及び教育・研修について

ア　NTV

NTV においては、2015 年 9 月から 10 月にかけて、業務監査室により、対象部局に対して、ガイドラインに基づく個人情報保護体制に関する監査が実施され、また、2015 年 6 月に新体制に移行して以降、個人情報保護を含む情報資産管理についての活動実施等について定期的に報告されるという体制が設けられている。さらに、グループ会社の管理体制の点検については、担当事務局等がアンケート調査や、外部専門家を含めた個別のヒアリング等を実施し、フォアキャストに対しても、アンケート・ヒアリング等を行い、指摘事項の共有等をしていた。

社内研修・教育等に関しては、ガイドラインにおいて、個人情報保護教育の教育計画、実施等が定められ、実際に、担当事務局が開催する研修に加えて、昨年度は特定の局の責任者等に対する集合研修が別途実施され、周知されている。また、昨年 6 月より、情報セキュリティに関する注意喚起及び啓発を目的としたメールを、定期的に社内配信している。

イ　フォアキャスト

システム全般の運用の監視は、各種規程に基づき、担当委員会及び品質管理に関する委員会が行っている。ただし、上記各委員会の構成員の中には、実際にシステムのコーディングを行う者も数名存在している。担当委員会は、内部監査を行い、個人情報に関わる規程やルールの不遵守がある場合に適時に是正勧告を行っており、必要に応じて都度開催されていた。品質管理に関する委員会は、個人情報に関する問題に特化した委員会ではないが、定期的に開催され、トラブルについて原因分析や対策等の情報共有及び検討を行っていた。

社内研修・教育等に関しては、定期的な教育の実施を謳っているほか、担当委員会の所管の下で各種規程が定められている。具体的には、業務フロー書等の遵守の周知、全体研修、入社時研修等を行い、また、社員に外部研修を受講させるなどしていた。

⑷　本件事故における事故対応マニュアルの遵守状況について

ア　NTV

ガイドライン及びマニュアルにおいて個人情報に係るインシデントへの詳細な対応が定められており、マニュアルでは、基本的な対応フローとともに、各段

階における対応が具体的に定められており、本件事故において、NTV は、フォアキャストから第一報を受けた後、直ちに必要機関に連絡を行い、ガイドラインに定める会議の開催、委員会の設立、事故の公表、本人への通知というマニュアルにおける対応フローに沿った対応がなされた。

イ　フォアキャスト

情報セキュリティ事象が発生した場合の対応に係る手順書において、個人情報に関する事故の監視や、個人情報に関する事故への対処の手順が定められている。同手順の内容は、抽象的なものであるが、本件事故において、フォアキャストの技術的な対応、担当委員会による初動、NTV との連携については、概ね同手順に沿い、かつ、適切になされた。

3　外部ベンダーについて

本件事故は、A 社が製造するケータイキットに潜んでいた未知の脆弱性が原因となって発生したものである。ケータイキットは、B 社が提供するプラットフォームのプラグインソフトとして製造されたものであり、B 社が代理店として販売を行っていた。

この点、A 社の開発したケータイキットには、IPA が広く公開している「安全なウェブサイトの作り方」に示されているような基本的なセキュリティ対策が実装されていなかった。

他方、B 社は、セキュリティに関するコーディングガイドラインを設けてはいないものの、自社が開発した製品については、ソースコードレビューのほか、ツールを利用した脆弱性調査を行っていた。しかし、ケータイキットについては、B 社が開発に関与していた製品ではないため、B 社において、かかるレビュー・調査は行われていなかった。

第４ 責任の所在

1　NTV について

NTV においては、各種規程により、明確な台帳管理等のフローに基づき個人情報が管理される仕組みとなっており、また、委託先からは、廃棄証を徴収した上で廃棄を確認する仕組みにもなっている。もっとも、番組制作部門の一部には、個人情報の取得主体としての意識が十分でなく、また、フォアキャストを指揮・監督する具体的なアクションがとられていないなど、各種規程に基づく運用は徹底されていなかった。このような状況が生じた理由の一つとしては、NTV 内での番組制作部門との関係におけるフォアキャストへの指導・監督、セキュリティ基準の提示、廃棄フロー等の運用及びそれらの周知が十分とはいえないという事情があった。高い公共性を有するテレビ局の事業の性質、大量に視聴者の個人情報を取り扱う業務の特性に鑑みても、上記の点において、NTV に委託者として落ち度がなかったとはいえない。

2　フォアキャストについて

フォアキャストは、上記のようなNTVの特に視聴者の個人情報を管理するウェブシステムの構築・運営を事業として行っているのであるから、もとより、外部からの攻撃者、内部者の持出し両面での個人情報の漏えい対策に関して求められるセキュリティの水準は高いというべきである。

フォアキャストにおいては、本件システムに対するファイアウォールやIDS（不正侵入検知システム）の導入、脆弱性診断、定期的なパッチ適用等の最低限のセキュリティ対策は実施していた。しかしながら、本件システム上に不要なプログラムが残っていた、ウェブサーバから外部への通信が全て許可されていたなど、入口対策、内部対策、出口対策が不十分であった。

また、フォアキャストの技術担当者は技術的なスキル等は持ち合わせているようであるが、組織的な管理体制の下に適切な運用がなされていないと見受けられる。特に、個人情報の暗号化の必要性に対する認識がなく、その旨の規程・ルール自体がなかった点や、台帳の管理に関する明確な規程・ルールがなかった点には問題がある。また、古いシステム・サービスに対する適切な管理が不足している傾向が見られる。

さらに、個人情報の削除に関し、削除実行後に特定のフォルダへ移行した個人情報は完全に消去されず、その後の削除については特段の明確なルールのない属人的な運用に委ねられていた。フォアキャストは、このような運用をNTV及びフォアキャストのマネジメント層にも知らせていなかったため、担当委員会や品質管理に関する委員会による監査によっても、このような状況を自覚的に認知し、必要な対処を行うことができなかった。これらの結果、削除が完了しているべき大量の個人情報が残存していた。

以上の点で、フォアキャストには、受託者として技術的側面及び運用的側面において不備があった。

3　外部ベンダーについて

A社は、ケータイキットの開発において、セキュリティに関する基本的な対策を行っておらず、ソフトウェア開発において落ち度があったものといわざるを得ない。

B社は、同社の製品のプラグインソフトとして開発されたケータイキットが、セキュリティに関する基本的な対策を実装していないものであることを看過したままケータイキットを販売していた。そのため、B社にも落ち度がなかったとはいえない。

第５　再発防止指針

1　フォアキャストにおけるシステム全体の強化

⑴　当面の対応

NTV がフォアキャストに委託した個人情報に関係する全てのシステム（以下「管理対象システム」という。）において、同様な不正アクセス被害を再発させないために速やかに次の対策を実装しているかを確認し、未実装の場合は対策を講じるべきである。なお、昨年 12 月から導入した新システムについては、対策の実装状況を確認済みである。

① 管理対象システムの脆弱性診断を速やかに実施し、脆弱性が発見された場合は速やかに修正を行うこと。
② 管理対象システムにおけるセキュリティパッチの適用及び不要なサービスの停止、並びに不要なプログラムの削除を徹底すること。
③ 管理対象システムにおいて必要のない通信（不要な外部への通信等）を遮断すること。
④ 管理対象システムのウェブサーバから個人情報データにアクセスするアクセス制御を適切に実施すること。
⑤ 管理対象システムにおいて保管する個人情報で、暗号化等の秘匿化が実施されていない情報は速やかに秘匿化を実施すること。

⑵ 今後の方向性

管理対象システムにおいて、セキュリティレベルを更に向上させるために次の対策を講じることを強く推奨する。

① 管理対象システムにおいて、脆弱性を悪用した攻撃からネットワークやウェブアプリケーションの保護を行うために、必要なシステム等を追加導入すること。
② 管理対象システムにおけるログ保管方法及び監視方法の見直しを行うこと。
③ 管理対象システムにおけるファイル改ざん検知の仕組みを強化すること。
④ 緊急時のフォアキャストの対応権限を見直すこと。
⑤ 定期的な管理対象システムのセキュリティレビュー（インタビュー、セキュリティ監査等）を行うこと。また、内部対策・出口対策も意識したセキュリティ対策の観点での評価も行うこと。
⑥ 管理対象システムの新規構築及び更改時には、セキュリティレビュー（インタビュー、設計書レビュー、脆弱性診断等）を行うこと。なお、新システムについては、即時対応すべき脆弱性は確認されなかったが、他システムに関しても脆弱性診断等を実施する必要がある。

2 フォアキャストにおける情報セキュリティ管理体制の強化

再発防止のための情報管理体制の強化として、以下の事項が考えられる。

① 個人情報の暗号化の必要性を認識し、その旨の規程・ルールを策定し、周知・遵守すべきである。

② 台帳の管理に関する明確な規程・ルールを策定し、周知・遵守すべきである。特に、保存期間を超えた個人情報の削除を励行する運用を定着させるべきである。

③ 取得した個人情報の削除処理につき明確な規程・ルールを策定すべきである。これに当たっては、個人情報の削除が完全な削除であることを担保するとともに、このような運用について、NTV と情報共有すべきである。

④ 組織横断的にセキュリティを管理する部門の再編を検討すべきである。

3 NTV における委託先管理体制の強化

再発防止のための委託先管理体制の強化として、以下の事項が考えられる。

① NTV は、番組関係者における個人情報の委託に関する意識啓発を引き続き積極的に行うとともに、委託先に対する具体的な指揮・監督について、特に実際に個人情報を取り扱う番組関係者に対する周知・徹底をより一層図るべきである。

② NTV は、委託先において遵守すべき個別具体的なシステムの実装レベルのセキュリティ基準を設けた上で、委託先の意向も確認・協議しつつ、委託先において当該基準を満たすセキュリティの導入を行わせるよう、積極的な要求をすべきである。

以上