

BIGLOBE の個人情報保護とセキュリティ

BIGLOBE's Action toward Private Information Protection and Security

福村 和悦*
Kazuyoshi Fukumura

板倉 和治*
Kazuharu Itakura

大知 俊基*
Toshiki Ohchi

要 旨

BIGLOBEでは、お客様に安心してサービスをご利用していただくために、個人情報保護およびセキュリティの重要性を早くから認識し、維持・向上に努めてきました。

BIGLOBEの個人情報保護および情報セキュリティ管理の特徴は、データセンターおよびオフィスのセキュリティ区画を明確に区別した上でオフィスにおいては個人情報および企業情報のセキュリティ対策を同じ枠組みで実施し、個人情報については全サービスに対する漏れのない個人情報の特定の仕組みや業務委託先の管理を行うことなどにあります。さらにこれらの活動に対し、事故訓練や監査を定期的に実施することにより、継続的改善を図っています。

BIGLOBE has recognized the importance of private information protection and information security management for secure services to customers.

The characteristics of BIGLOBE's activities are; first, the same framework for both customer's and company's information protection based on physical area; secondly, the private information lifecycle management system in every service provided by BIGLOBE. Continual improvement on these activities is obtained by the incident response training and NEC's internal audit.

1. まえがき

インターネットは、今日の社会・経済活動のなかで、個人から企業まで広く活用され、重要な社会インフラとなりつつあります。昨今、インターネットのブロードバンド化に代表される通信や情報処理の速度の高速化、大容量化などの情報通信技術の急速な進展に伴い、サービスプロバイダは、お客様の個々のニーズが的確に反映されたサービスの実現をめざしており、収集する個人情報も多様化しています。

他方、電子化されたデータは容易に持ち出すことが可能

であり、その管理を十分に徹底していない場合、個人情報が外部に流出する恐れがあり、サービスプロバイダには利用者の信頼を得られるような個人情報保護の取り組みが求められています。

一方、企業内には自社の事業活動に有用な技術上または営業上の企業情報やパートナー企業との契約に基づいて入手した情報があり、これらの情報は、個人情報と同様に、漏えい、滅失、およびき損の防止などのために、安全管理措置を講じる必要があります。

BIGLOBEでは、個人情報の重要性を早くから認識し、その保護管理に努めてきました¹⁾。以下では、BIGLOBEにおける個人情報保護とセキュリティについて紹介します。

2. NECの個人情報保護と情報セキュリティの取り組み

NECは、よき企業市民として社会的責任を果たすべく、個人情報保護ポリシー、情報セキュリティ基本方針を公開し、お客様に関する情報資産、お客様やお取引先様からお預かりした情報資産、NECの情報資産の取扱い方をこれらに従って行うとともに、全社への徹底を図っています²⁾。BIGLOBEでの取組みは次のとおりです(図1)。

- ・1986年：データセンターが、通商産業大臣により情報処理サービス業情報システム安全対策実施事業所認定(安対制度)を受ける。以来、会員情報や通信の秘密保持に組織的な対応を行う。
- ・2000年10月：日本情報処理開発協会のプライバシーマーク使用許諾証取得。
- ・2001年3月：日本データ通信協会の個人情報取扱業務と



図1 BIGLOBE で取得したマーク類

Fig.1 Marks acquired for BIGLOBE.

* BIGLOBE カスタマリレーション本部
BIGLOBE Customer Relations Division

して登録。

- ・2002年9月：データセンターにおいて、安対制度の後継である「情報セキュリティマネジメントシステム（ISMS）適合性評価制度」の認証取得。
- ・2002年11月：セキュリティ面での安全度とお客様への安心度が評価される「安全・安心マーク制度」のマーク取得。

3．BIGLOBE における情報セキュリティの特徴

BIGLOBEでは、インターネット事業としての様々なサービスをお客様に提供しています。したがって、通常の企業で扱う企業情報に加えて、お客様からお預かりした情報資産を厳重に管理していく必要があります。

BIGLOBEでは、以下の2つの特徴的な視点からこれらの情報管理を推進しています。

第一に、物理的なセキュリティ区画を明確化し、それぞれのセキュリティ区画ごとにセキュリティ対策を実施していることです。そのセキュリティ区画は大きく分けてデータセンターとオフィスの2つがあります。

データセンターにはお客様にサービスを提供するために必要なサーバやデータベース、その他のネットワーク機器が管理されており、特に厳重に管理されなければなりません。データセンターにおけるセキュリティ対策を以下に示します。

- ・入退室制限
- ・サーバへのアクセス制限
- ・サーバ/ネットワーク機器への定期的なセキュリティ診断実施
- ・メンテナンス管理基準に従った保守作業
- ・消火/防火設備、水害対策、停電対策
- ・データバックアップ/復旧手順の確立
- ・ディザスタリカバリ（遠隔地分散保管）
- ・場所の非公開

オフィスのセキュリティ対策に関しては、次章で述べます。

第二には、管理対象の情報資産の特性によるセキュリティ対策の実施です。情報資産のなかで一番重要なものは、お客様からお預かりした個人情報です。企業による情報漏えい事件・事故が多発する昨今、BIGLOBEでは4年前から個人情報保護管理システムを構築し、その運用を行ってきました。個人情報には、それ以外の情報資産とは異なり「利用目的」「収集」「開示」「訂正」「同意に基づく提供」などの概念が存在します（図2）。これらの特性を踏まえ、個人情報特有の安全対策と、その他の情報資産にも共通な安全対策を融合し、情報セキュリティマネジメントを推進しています。

4．事務所の安全管理

我々が執務するオフィスには、様々な情報資産が存在し、

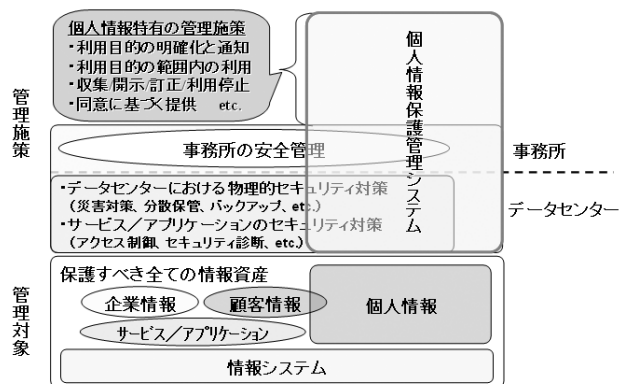


図2 個人情報保護と情報セキュリティとの関係

Fig.2 Relationship of private information protection and security controls.

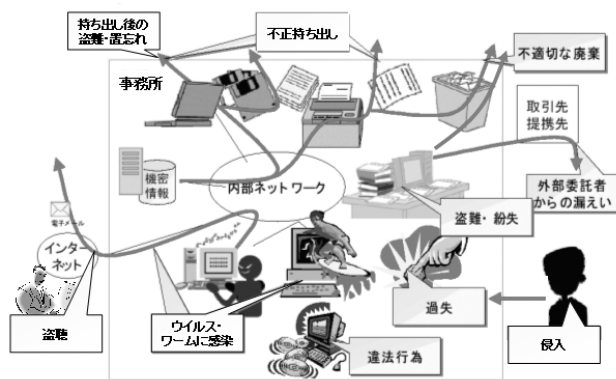


図3 事務所におけるリスク

Fig.3 Risks in office.

そのなかには、個人情報以外にも管理すべき情報資産が多数あります。たとえば、サービスにかかわる仕様書や価格情報、お客様からお預かりしたデータや契約書、取引先の企業からお預かりしている資料などです。同時にそれらの情報資産に対しては様々な脅威とリスクが存在し（図3）、特にお客様からお預かりしている情報が漏えいするといった事態に陥ると、お客様に迷惑や損害を与え、ひいてはNECの信用問題にもなります。こういった事態は絶対に避けなければなりません。

NECには、「企業秘密管理規程」というこれらの情報を管理する規程があります。BIGLOBEではこの規程に則り、現場レベルでの管理を強化する目的で「事務所における情報セキュリティ安全管理標準」を2003年に策定しました。これは、基本的な管理の枠組みは個人情報保護管理システムと共通であり、具体的な管理レベルや安全対策も個人情報と整合させ、現場の担当者が無用の混乱を与えないようになっています。

「事務所における情報セキュリティ安全管理標準」は全62項目からなり、情報資産の機密レベルを3段階で定義し、それぞれの機密レベルに応じて安全対策を規定しています（表）。

表 事務所における安全対策
Table Safety controls in office.

カテゴリ	機密レベル			安全対策（概要）
	1	2	3	
運用管理	○	○	○	機密レベルを表示する
	○	○	○	事故が発生した場合、定められた手順で処理する
			○	管理者を定め、運用ルールの教育・自主点検を実施する
入出力管理		○	○	印刷/コピー/FAXは放置しない
			○	電子情報の場合、サーバのログインログを採取する
保管/廃棄管理	○	○	○	保管場所を定め、持ち出す場合は暗号化する
	○	○	○	電子情報を廃棄する場合、ツールを使用し完全に消去する
入退室管理	○	○	○	別途定める入退館ルールに従う
輸送/送受信管理			○	直接手渡しする
			○	電子データをやり取りする場合は、暗号化する
情報システム管理	○	○	○	セキュリティパッチ/ウイルス対策を実施する
	○	○	○	パスワード管理を徹底する
	○	○	○	インターネットとイントラネットの同時接続しない

5. BIGLOBEにおける個人情報保護管理の特徴

5.1 保護管理の単位

BIGLOBEでは個人情報の保護管理を「個人情報取扱業務」と呼ぶ業務単位で実施しています。

BIGLOBEではインターネット接続サービスのために収集する会員情報だけでなく、各種キャンペーンなどでもユーザから個人情報を直接収集して、サービスのために利用しています。これらのサービスを実現する業務では、収集した個人情報を複数の個人情報ファイルやデータベースに形を変えて利用するのが一般的です。

このように収集後に業務のなかで形を変えて内部利用される個人情報を、その完全な廃棄まで適切に管理するためには、その業務で利用するファイルやDBの管理を、それらを取り扱う業務単位で束ねて業務の発生から終了のサイクルのなかで管理するのが効率的です。この個人情報保護管理の業務単位を「個人情報取扱業務」と呼んでいます。

5.2 個人情報取扱業務の一生

お客様向けの新しいサービスや、それらを実現するための内部管理業務が企画された時、これを実現する業務を「個人情報取扱業務」とし、この担当業務責任者は「業務内容概念図」と「個人情報取扱業務管理票」を作成して部門の「個人情報取扱責任者」に登録の申請を行います。申請が許可されると「個人情報取扱業務番号」が定まり、「管理台帳」に登録されます。この登録から始める管理プロセスを図4に示します。

「管理台帳」に登録されたことで個人情報保護の観点から許可された業務では引き続き（当該業務の）「運用マニュアル」を作成して業務運用開始に備えます。また、「個人情報ファイル/DBの保管・廃棄処理管理表」を作成し、当該業

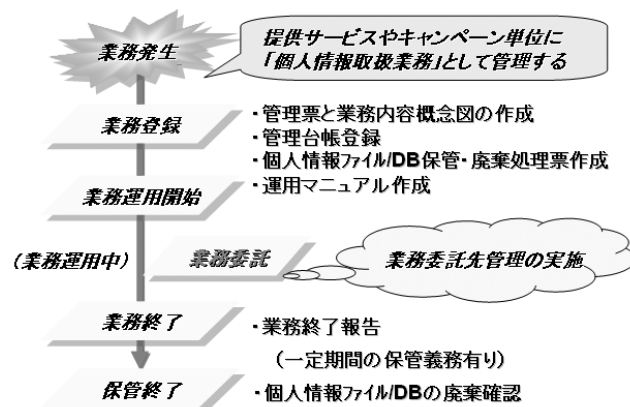


図4 メイン管理プロセス

Fig.4 Main management process.

務の運用のために必要な個人情報ファイル・データベースを定義して記入します。この「個人情報ファイル/DBの保管・廃棄処理管理表」はその名のとおり、その業務で作成した個人情報ファイル・DBを最終的に完全消去もしくは廃棄するまで管理するためのものです。

サービスなどが終了し、個人情報取扱業務としても終了すると「個人情報取扱業務終了報告書」を作成し、業務委託先での廃棄確認なども含む当該業務の終了点検結果を取扱責任者に報告します。

しかし一般的には、これで個人情報の保護管理が終了したわけではありません。一部の個人情報ファイル・DBはお客様からの問合せなどに備えて、必要とする一定期間保管しなければなりません。これらの保管ファイル・DBは「個人情報ファイル/DBの保管・廃棄処理管理表」で引き続き管理され、すべての個人情報ファイル・DBが完全消去もしくは廃棄された時点で、当該業務に関する個人情報保護管理は完了します。

5.3 業務委託先管理

必ずしもすべてに当てはまるわけではありませんが、個人情報を取り扱う業務を実行する組織がサービスの大多との責任組織からの管理距離が遠くなるに従い、個人情報に関わる事件/事故の発生確率は高くなる、と言われてます。実際、再委託先、再再委託先で発生する事故/事件をニュースなどでしばしば目にします。

しかし、現在では下請けという概念ではなく、業務のパートナーとして専門性を持った企業へ業務委託を行うことは、お客様へ提供するサービスの質を高める上でも必要なこととなっており、BIGLOBEでもこれらの企業なしには質の良い事業提供はできません。

このためBIGLOBEでは業務委託を行うに当たり、個人情報保護に関して極めて厳格な業務委託先管理を実施しています。以下はBIGLOBEが行っている主要な業務委託先管理項目です。

- ① 個人情報保護に関する条項を含んだ業務委託基本契約を締結。
- ② 個別の発注に際して、その業務が個人情報取扱業務であることを文書で通告。
- ③ 業務委託先が再委託を行う時は文書で承認。
- ④ 業務委託先の個人情報取扱の適正管理状況を1年に1回以上評価。
- ⑤ 業務委託先と個人情報の授受をオンラインで行う時は、通信の仕組み、受信確認方法、送受信ログの内容、などをあらかじめ定めて書類で確認。
- ⑥ 業務委託先と個人情報の授受をオフラインで行う時は、その都度授受確認を行い、記録として保管。
- ⑦ 委託業務終了時は、委託先にある個人情報を完全に処理したことを書面で報告してもらい、確認。

6. 管理システムの改善

個人情報保護管理およびその基盤となるセキュリティマネジメントや品質管理の管理システムを、組織の成長や提供するサービスの変化に合わせて更新していく目的で、下記の2つの仕組みを定常的に運用しています。

6.1 事故訓練

BIGLOBEでは「個人情報事故対応フロー」を制定し、毎年、訓練を実施しています。個人情報事故が起きたときに事故に関する情報を適切に速やかにエスカレーションさせるとともに、できるだけ迅速に必要な処置が取れることを狙っています。

事故訓練はこの事故対応フローに沿って行いますが、事故状況を具体的に想定して訓練を行うので、現状での個人情報管理上の問題点があぶりだされることが期待されます。

実際、過去の訓練では、暗号化されるべき個人情報ファイルで現実には暗号化されていないものが発見され、個人情報取扱業務のなかで管理されるべき個人情報ファイル・DBの特定の仕組みに漏れがあることが判明し、直ちに改善しました。

6.2 監査

監査は、NECの内部監査組織である経営監査本部によって、年に1回実施されます。

監査指摘事項は各事業部の個人情報取扱責任者が改善実施をフォローし、最終的に経営監査本部による翌年の監査実施時にその実行を点検されます。

7. むすび

BIGLOBEでは、お客様に安心してサービスをご利用していただけるよう、個人情報保護および情報セキュリティ管理に組織的にかつ継続的に取り組んでいます。2005年4月から「個人情報保護法」が施行予定で、総務省などの関係省庁ではガイドラインを整備中です。BIGLOBEは、今後もお客様に多様なサービスを提供する上で、法およびガイドラインを遵守し、お客様の個人情報をより効果的に

つ適正に管理するよう取り組みます。

参考文献

- 1) 後藤はか；「BIGLOBEの個人情報保護管理」, NEC 技報, Vol.54, No.12, pp.17～20, 2001.
- 2) NEC ホームページ, <http://www.nec.co.jp>

筆者紹介



Kazuyoshi Fukumura

ふくむら かずよし

福村 和悦 1977年, NEC 入社。現在, BIGLOBE 事業本部 BIGLOBE カスタマリレーション本部 シニア エキスパート。情報処理学会会員。



Kazuharu Itakura

いたくら かずはる

板倉 和治 1969年, NEC 入社。現在, BIGLOBE 事業本部 BIGLOBE カスタマリレーション本部 マネージャー。



Toshiki Ohchi

おおち としき

大知 俊基 1991年, NEC 入社。現在, BIGLOBE 事業本部 BIGLOBE カスタマリレーション本部 エキスパート。