不正アクセスに伴うお客様情報流出に関するお詫びとお知らせ

2008年4月18日(金)

株式会社サウンドハウス

代表取締役社長　中島尚彦

この度、弊社 WEB サーバーへの不正アクセスにより、お客様の大切な個人情報が流出する事態が生じ、多くのお客様に多大なるご迷惑、ご心配をおかけ致しましたことを深くお詫び申し上げます。弊社では、今回の事態を厳粛に受け止め、お客様の信頼回復に社員一同、全力で取り組む所存です。

今回の個人情報流出の対象となる、2007年1月1日～2008年3月22日までに新規会員登録をいただいた122,884名 全てのお客様に、以下を、弊社の補償とお詫びとさせて頂きたく提示し、お客様のご理解を頂きたく存じます。

※　実際の個人情報流出対象のお客様は、延べ人数で最大97,500名分となりますが、今回の不正アクセスは特殊な方法でデータを抽出されている為、実際に情報が流出した個人の特定ができません。従いまして対象期間内に新規会員登録を頂いた全てのお客様を対象とさせていただきます。

1.　この度の個人情報流出に関連して、万が一、お客様がカード不正利用などの直接被害を受け、カード会社、またその他の機関によって補償が受けられない場合には、弊社が責任を持って対処致します。

2.　個人情報流出の可能性がある 122,884 名 全てのお客様に、サウンドハウスでご利用できる 1,000 円相当分のクレジットを進呈させて頂きます。本クレジットはお客様のサウンドハウス会員情報に既に反映されており、サウンドハウスでのお買い物代金に充当する形で、ご利用頂けます。尚、このクレジットは2009年4月末まで有効となります。

3.　クレジットカードが使用できず、そのポイントや、カードメリットを活用できない上、不便であるという声が多くのお客様より寄せられているため、商品ご購入の際、その合計代金の 3%を、お客様の弊社ご登録口座にクレジットし、次回購入時にお使い頂けるリベートプログラムを4月30日まで実施致します。

尚、累積されたクレジットの合計は、4月20日前後より、弊社ホームページにて、ご注文時にご確認、ご利用頂けるよう、プログラムの変更を進めております。また、今回の不正アクセスに伴うお客様の個人情報流出に関して、時系列情報、関連情報、並びに、会社の代表として私自身が見聞きしたこと、感じたこと、そして反省点を、ありのままに書かせていただきました。ご一読頂ければ幸いです。

この度の件につきまして、重ねてお詫び申し上げますとともに、今後とも変わらぬお引き立てのほど、何卒よろしくお願い申し上げます。

1. はじめに

この度、多くのお客様の個人情報が流出してしまったこと、謹んでお詫び申し上げます。今回のプレスリリースにあたり、これまでの経過、弊社がとった対応と対策、及び今後の計画などを含め、その詳細をできるだけ分かり易くまとめてみました。また、一連の事件から浮かび上がってきた事実や、状況証拠にも目を向けて、事の成り行きを可能な限り検証してみました。これらのデータを元に、お客様や関係者の間で、日本が直面するサイバー社会の盲点についての認識が改められ、そこから新たなる警告が発信され、セキュリティ対策を始めとして、様々なシステムの改善が推進され、各種対策が活発に協議されるようになることを願ってやみません。

2. これまでの経過

お客様から寄せられている何千件にも上るメールに対して、自らも多くの返事を書かせて頂き、お客様の生の声も聞くことができました。その中には、いつ不正アクセスの情報を得たのか、また、なぜ情報の開示が 4 月 3 日まで始まらなかったのか、という疑問の声も多く、様々な憶測が飛び交うことを防ぐ為にも、この際、何がどういう順番で起きたのかを時系列で記載し、お客様に実際の状況を理解して頂きたく思います。

3 月 21 日にクレジットカード会社、2 社が突然来社され、弊社をご利用頂いたお客様において、クレジットカードの不正使用の疑惑があり、ハッキングされている可能性があるとの指摘を受けました。翌 22 日には早速、第 3 者調査機関である株式会社 LAC（以下 LAC）が来社し、調査が開始されます。そして 3 月 30 日夜には、ログの検証に基づく流出情報の分析をもって、サイバーテロの被害を確認できる第一次レポートがあがってきました。そこで目にしたものは、「SQL インジェクション」、「発信元　中国」、「悪性プログラム」、「約 97,500 件のクレジットカード情報を含む顧客情報が流出」という言葉の数々でした。以下、詳細です。

3/21(金)　11:50　三菱 UFJ ニコス株式会社（以下三菱 UFJ ニコス）より「サウンドハウス（以下 SH）のサーバーがハッキングされている可能性がある」と電話にて連絡あり。

16:00　三菱 UFJ ニコス、クレジットカード不正使用のリストと LAC の名刺のコピーを持参。ハッキング詳細を確かめてほしいとの依頼で、調査機関である LAC を紹介。

18:00　株式会社ジェーシービー（以下 JCB）が来社、不正使用されたクレジットカード情報のリストと文章を持参。三菱 UFJ ニコス同様、外部機関による調査をしてほしいとの依頼を受け、LAC の名前を出したところ、そこです、とのことで同じく LAC を推薦。

20:43　SH は何らかの不正プログラム、及びシステム障害があることを懸念し、ホームページのクレジットカード決済を停止。

23:05　LAC と電話打ち合わせ開始

3/22(土)　0:51　ログ診断「Secure Site Checker Free」での解析開始。

10:20　LAC より 3 名、緊急調査の為来社。調査開始。

13:00　暫定調査の結果、昨今攻撃が増えた SQL インジェクションとの関係が推測されると報告を受ける。緊急のセキュリティ対策として、下記内容の提案を受け、即実行する。

- WEB サーバー、データベース（以下 DB）サーバーを新規で入れ替え、もしくは OS からクリーンインストールされた新しい HDD への交換が必要
- 各サーバーのパスワード変更

・xp_cmdshell が使用不可状態になっているか確認
・ASP エラーが返される設定を無効に変更
・新規クレジットカード登録をできないように変更
・暫定で IDS をレンタルにて設置。後日 IPS 導入予定
・不審ファイルの検査

17:00　お客様へ第一報として、告知文章の作成に着手。

17:50　LAC のアドバイスにより、お客様へニュース配信する前に、クレジットカード会社に、その旨、告知が必要とのこと。電話するが土曜日の為、窓口につながらず。一般電話受付にてようやく折り返し電話をもらえるよう連絡ができ、配信する旨伝えるも、三菱 UFJ ニコス、JCB 共に、週末の対応が難しいこと、また流出範囲の特定をしてからでないと告知はできないので、調査結果が出てからということで、この時点での告知は見合わせることとなる。

19:00　WEB および DB サーバー再構築用の HDD を購入。

21:00　WEB プログラムで指摘された問題点を全て修正完了。LAC は IIS ログ（3/11 以降を除く 2008 年分全て）を持ち帰り分析。残りのログは外部記憶装置に移動出来次第、持ち込みとする。

21:30　千葉県警成田署へ一報を入れる。

22:54　JCB に対して夕刻の電話の通り、お客様への告知については、カード会社のアドバイスに従って、一時見合わせる旨の確認メールを送信。

22:58　三菱 UFJ ニコスに対しても夕刻の電話の通り、お客様への告知について、一時見合わせる旨の確認メールを送信。

3/23(日)　0:00　問題修正済み新プログラムをリリース。カードの使用は停止したまま。

7:00　サーバー内アクセスログの移動、およびデータバックアップが完了。サイトを停止し、新規に手配した HDD に OS をインストールしサーバーを再構築開始。元の HDD は厳重に保管

20:30　新プログラム、新サーバーにてサイト再開。IDS 設置完了まで、暫定的に 15 分毎にサイトログのチェックを行い 24 時間体制で監視を開始。

3/24(月)　10:08　お客様より「カード会社から、カード情報が流出したので、カードを停止する、と連絡があったが事実ですか？」と問い合わせあり。三菱 UFJ ニコスへメールにて確認。

11:07　JCB より、土曜日の確認メールの返答として、どの範囲の情報がどれ位流出したのか、特定するように要請を受ける。告知の内容、時期については、SH、三菱 UFJ ニコス両者と連携して進めたいとのコメントあり。

15:31　三菱 UFJ ニコスより、22 日（土）の弊社からの問い合わせについての返答として、お客様への告知に関しては、「情報流出の確定及びある程度、流出範囲が判明した時点での告知が望ましい」と、メール文書に

て依頼を受ける。同時に、クレジットカード取り扱い再開については、セキュリティレベルが十分に確保されたことが確認できてからということで、セキュリティ診断が必要であることが知らされる。

15:37　三菱 UFJ ニコスよりメール有り。カード発行会社と SH が流出元ではないか、という話をしていた際、カード再発行手続き中のお客様との会話の中で、流出の可能性がある、という表現を使用したとの報告。その他の会員様に案内はしていない。

16:00　千葉県警サイバー犯罪窓口に連絡。「調査結果等出たら、成田署まで連絡を」、ということで終了。

17:00　IDS 設置稼働確認。手動による 24 時間監視を解除。

19:30　内部ネットワークに配置されている DB、サーバー関係のパスワードを一斉変更。

21:32　カード利用の再開について、確認のメールを三菱 UFJ ニコスへ送る。お客様への告知は一刻も早く実行したい旨、SH の意向を明確に伝える。

3/25(火)　10:46　三菱 UFJ ニコスより、カード再開に向けての手順説明あり。「セキュリティ診断については、VISA/Master Card に定められている、所定の手続きが必要」とメールにて告知を受ける。情報流出原因を特定するための 1 ヶ月程の調査と、及び今後の対策、その他セキュリティ面での審査が 2 週間程度。いずれも高額な費用がかかる調査だが、この 2 つを行わない場合、VISA/Master Card のライセンスを剥奪され、今後クレジットカードの取り扱いができなくなると知らされる。

22:36　外部から過去に挿入されたと思われる、不審な悪性プログラムが発見されたことを LAC より連絡受ける。至急対応開始。サイト内の全ファイルを再検査開始。

23:00　全ファイル再検査完了。不審ファイルを発見し削除。

3/27(木)　18:00　LAC より中間報告あり。状況証拠により、2006 年から 2007 年 5 月にかけて SQL インジェクション攻撃があったと推測。しかしこの時点では、情報が流出した痕跡がみつからず。

3/28(金)　10:26　LAC より、SQL クエリが送信された形跡があるとの報告あり。発行された SQL 文について有効かどうかの確認連絡あり、弊社で確認したところ、これにより抽出される顧客情報は、・お名前　・フリガナ　・性別　・生年月日　・ログイン用メールアドレス　・ログイン用パスワード・クレジットカード情報（ご名義 /カード番号 /有効期限）であることが判明。引き続き調査を続行。

18:00　ファイアーウォールのポリシーを LAC のアドバイス通りに変更完了。

3/30(日)　20:10　LAC より、「緊急対応ログ調査報告書」を受け取る。顧客情報流出に関するデータの分析を踏まえ、「2007 年から 2008 年に新規登録された約 97,500 件のクレジットカード情報を含む顧客情報が流出した可能性が

ある」という報告内容。

3/31(月)	10:30	LAC による緊急対応ログの調査報告会を実施
	13:14	三菱 UFJ ニコスへ、クレジットカード情報が流出した可能性のある該当者リストを送信。
	13:55	JCB へも同様に該当者リストを送信。
	23:19	三菱 UFJ ニコス、及び JCB へ、SH から配信予定の「お客様へのお知らせ」を送信。
4/1(火)	朝	カード会社、双方とも、すぐに対応できない、ということで SH と意見が対立、SH 代表と電話で直接会談。
	16:24	三菱 UFJ ニコスより SH から配信予定の、「お客様へのお知らせ」の加筆、校正文が戻ってくる。
	20:42	複数の JCB カードユーザーからメール及び電話で、「SH の顧客情報が漏洩したとカード会社から連絡があったがどうなっていますか?」と、問い合わせあり。カード会社の要請により、SH が情報発信を待機している間に、カード会社では先行して案内を開始している為、JCB に問い合わせ。 また、三菱 UFJ ニコス、JCB それぞれと電話協議。ニュースリリースの日取りについて調整。三菱 UFJ ニコスは、翌日水曜日、または木曜日配信なら準備ができると返事あり。JCB は 4 月 7 日、週明け月曜まで、どうしても待ってほしいと主張、譲らず。
4/2（水）	15:00	三菱 UFJ ニコスが VISA/Master Card の指定調査会社 2 社とともに来社。今後のクレジットカード利用再開に向けての説明を受ける。
	18:29	JCB より、「お客様へのお知らせ」の中で、「クレジットカード会社から、インターネット上でのクレジットカード不正使用の指摘があり･･･」という文言は、不正使用の不安感を増大させるため、削除してほしいと依頼あり。
	20:10	JCB より、4 月 7 日（月）の配信で良いかと念押しの連絡が入る。
	20:34	三菱 UFJ ニコス担当者と調整、JCB が月曜日でお願いしたい、ということで「お客様へのお知らせ」の送信を 4/7(月)の早朝より実行することで最終的に合意。
4/3(木)	朝	SH 掲示板等で、「なぜ情報流出によるクレジットカード不正使用について発表しないのか」、と書き込みと共に SH へ問い合わせが急増。三菱 UFJ ニコス担当者と相談の上、SH ホームページにメッセージを掲載することとなる。JCB に対してもお客様へのメール配信は週明けにて対応するので、WEB には掲載します、という内容のメールを送信。
	11:00	SH ホームページの TOP ページへお客様へのお知らせを掲載。
	13:12	三菱 UFJ ニコスより、月曜日配信予定の文面に掲載予定であった、パスワード云々の記述は、不安を感じさせてしまう懸念があるので削除

してもらいたい、と依頼あり。パスワード対策を含め、不正使用の対応については、クレジットカード会社側で会員様と個別に対応するとのこと。

16:55　ホームページ掲載文章、及び月曜日にカード保有者のみに送信予定のお客様へのお知らせ文章を三菱 UFJ ニコスへ送信。

17:03　JCB にも同内容で最終送信。校正を待つ。

4/4(金)　9:46　三菱 UFJ ニコスより、SH で作成した文面で問題ない旨連絡受ける。カード会社各社へ展開するとのこと

9:47　JCB に対して、お客様から「SH ホームページに掲載するだけで、なぜメールで連絡がないのか」、といった指摘をいただいているので、対象のお客様に対して、月曜日まで待たずにまず一報を送信したい、ということでその内容をメールにて通知。

10:01　三菱 UFJ ニコスにも同様に通知するとともに、クレジットカード会社に配信を止められている為と答えてよいか？と問い合わせ。

10:09　JCB に、あらためて本日配信する趣旨を説明。「なぜメールでお知らせを流さないのか？」といった問い合わせにはどう答えたら良いかをと確認。

4/4(金)　12:17　三菱 UFJ ニコスより、以下の校正がメールで入る。「その他、お客様への今後のアナウンスと致しましては、調査会社、及びクレジットカード会社各社と連携する業務の流れの中で、確実な情報のリリースとクレジットカード会社の迅速な対応が前提となっており、今週末にも追って情報をリリースすることができるかと思います。」を削除し、「現在、調査を継続しております。詳細分かり次第、ご連絡を致します。」という表記に変更。

13:00　JCB、三菱 UFJ ニコスへ SH 側で校正した文章の最終確認を送信。以下の文章を追加。

「お手数ではございますが、早急にクレジットカードのご利用明細を確認の上、内容に問題がないかご確認ください。また、弊社 WEB サイトへのログインパスワードと、クレジットカードのパスワードが同一のものを使用されていた場合、それらのパスワードの設定を変更して頂き、今後はそれぞれ異なるものをお使い頂くようお願い申し上げます。」

13:18　三菱 UFJ ニコスより上記追加文章内の「クレジットカードのご利用明細を確認」という部分を削除してほしいとリクエストあり。即、校正し返答。

14:16　クレジットカード情報も含めた、個人情報の流出対象のお客様に対して、最初のメール配信を開始。

16:00　経済産業省の報告窓口である、独立行政法人情報処理推進機構セキュ

リティセンターの不正アクセス相談窓口へ電話にて確認の上、WEB ページの専用フォームより報告を送信

4/5(土)　11:25　SH ホームページに 2 回目のお知らせを掲載。

13:25　同内容を全てのサウンドハウス会員様にメール配信。

21:30　SH ホームページに 3 回目のお知らせを掲載。流出した内容、及びセキュリティ対策についての報告。

4/7(月)　5:47　3 回目のお知らせをメール配信。同内容を 6:00 に SH ホームページへ掲載。

11:13　JCB より、SH が提出した流出カード情報のリストに掲載されてない会員様より、SH からメールが届いたと連絡があったが、対象となるお客様のみに送信しているかどうか確認が入る。

11:52　JCB へ、お客様より問い合わせが増え始めたため、送信の段階で、SH 会員様全員へメール送信することになった旨返信。

上記メール返信直後、JCB より電話。当初、クレジットカード情報流出対象のみに送信という話が、全員に変更された為、問い合わせが殺到している。すぐに今回の流出の対象か、対象外か、また対象の中でも、クレジットカード情報の有無の違いなどについても、それぞれ告知内容を変えて送り直すようにとリクエストあり。配信途中のメールを一旦ストップし、条件ごとに計 6 通りの配信内容を作成し、それぞれの送信先アドレスを抽出し直し、配信準備にとりかかる。

13:34　三菱 UFJ ニコスよりメールで連絡あり。

「カード会社に連絡してください」という部分を訂正して欲しい、とリクエストあり。どのような文言がよいかと、電話で質問。メールにて以下の文章を受け取り、内容を差し替えリクエストに応じる。

「本日ご配信致しました情報流出に関するご案内の中に「クレジットカードの登録をされたお客様で、上記流出の対象となる場合は、お手数でもクレジットカード裏面に記載のある窓口へ連絡を取っていただき、カード会社の指示に従い、ご対応いただくようお願い致します。」と表記いたしましたが、クレジットカード会社側では、カードの不審な利用をモニタリングする等、不正使用を早期に発見できる体制を整えており、また、万が一、本件に起因してお客様のカード情報が不正に使用され被害が発生した場合には、お客様にご負担をおかけすることのないように対応することと聞いておりますので、お客様からクレジットカード会社へご連絡いただく必要はございません」

13:40　SH より、JCB、三菱 UFJ ニコスへ再送信予定のメール内容の校正を依頼。

15:57　JCB より「SH で作成した文面で問題ないので配信してください」との内容を受信。

各メールの配信数、及びメールの配信スケジュールの確認あり。

	16:19	JCB へ上記内容の回答送信。
	17:15	流出内容、及び対象か対象外か、既にメールを配信しているか、いないか、6 通りのメールを配信開始。
4/8(火)	8:16	JCB よりメールの配信対象の顧客データに間違いはなかったか、改めて確認あり。メールが届いたのでカードを交換し差し替えたが、その後対象外とメールが届いた人がいたということ。度重なるメールにて一部、混乱が生じた。
	11:40	経済産業省より電話あり。案件が大きいため、直接申請をお願いしたいとのこと。担当は情報通信機器課。
4/9(水)	12:52	JCB へリストに間違いはない旨連絡。
	13:21	お客様へのお詫びとお知らせを、会員にメール配信。
	13:30	同内容を SH ホームページへ掲載。
	夜	経済産業省へ申請書を発送。
4/15(火)	14:50	経済産業省より連絡あり。来週、ヒアリングに伺うとのこと。
	17:20	経済産業省へ送付する新フォーマットの申請書を作成。
4/16(水)	17:00	上記の申請書を発送。

3. 情報公開は速やかに行われたか

前述の「時系列情報」通り、不正使用の疑惑が生じた当初より、弊社では連日、カード会社と協議を重ねながら、できるだけ早く、しかもお客様にご迷惑がかからない最善の方法で、情報公開することを心掛けてまいりました。多くの不確定な情報が錯綜する中、一刻でも早く情報をお伝えしなければ、被害が拡大するのではないか、という判断から、情報公開は今すぐに実行したいという思いが募り、当初からカード会社と意見が対立することもありました。

しかし、今となって振り返ってみると、情報流出の詳細がまだ不確定で推測の域を出なかった3月22日に、もしニュースをリリースしたとするなら、それこそ大混乱に陥っていたことは明らかです。数万人のカード利用者が突然、一斉に問い合わせをしたら、どんなカード会社でも対応できず、少ない情報の中で数多くのお客様が混乱する結果となっていたことと思います。

3月30日夜には暫定のレポート内容がLACより提示されましたが、その時点では流出があったことは確定できても、未だその原因や詳細がわからないところがあり、引き続き調査が続いていました。しかし弊社としては、調査は継続しているものの、お客様にご一報するべき前提は整ったと考え、さっそく準備に入りました。そしてここからの数日間、リリースの準備をしている弊社、調査を継続する調査会社、そして顧客対応の受け皿となるカード会社の三者が足並みを揃える為に、連日協議しました。

結果として当初、遅くとも週明け3月31日(月)には、第一回目の告知をする予定でしたが、数日遅れの4月3日にホームページ上で発表、及び4月4日(金）に初回のメール配信をすることになりました。カード会社側は、対応の準備をまずきちんと行い、お客様へのご迷惑を最小限に食い止める体制が整ってからの告知が不可欠な状況でした。また、カード会社にとっては、数日の対応準備期間というものは、実際には遅れではなく、「情報公開の即時告知」の範疇に入っていたのかもしれません。最終的にはカード利用者への対応がスムースに処理され、お客様が安心して再びカードをご利用になれることが、一番、大切なポイントです。

弊社におきましてはスタッフ一同、色々と議論を重ねながら、およそ10万人にも上るお客様との対応を考慮した上で、お客様及びカード会社が混乱しないよう、そしてお客様へ迷惑が及ばぬよう、カード会社との連携をとりながら、調査を継続して情報の収集に努め、全力対応してまいりました。お客様への告知前にこのような事情があったことをご理解ご了承頂ければ幸いです。

4. セキュリティ管理体制について

○現在のセキュリティ管理体制について

この度の事件を機に、お客様が安心して弊社のホームページをご利用して頂けるよう、セキュリティのアップグレードを図り、下記の作業を既に完了しております。

○対応策

１．24 時間体制の不正アクセス監視
IDS(侵入検知システム)を導入し、24 時間監視。

２．サーバーのセグメンテーション化
ファイヤーウォールを増設し、よりセキュアなネットワークセグメントを構築。

３．プログラムの見直し
SQL インジェクション対策を強化。

４．プログラムの除去
外部から挿入された疑いが高い不正プログラムの除去を実施。

５．データベースからカード情報を削除
カード情報を弊社サーバーに保持しないシステムに変更を完了。

６．パスワードの暗号化
DB に保存するパスワードを不可逆暗号化。

７．システム構成の見直し
システム構成を抜本的に改善、新サーバールームの構築（4 月中に移動予定)。

８．社内管理体制を見直し
セキュリティ管理・対策委員会を設置。また、情報セキュリティポリシーに基づいた社内内部規定を整備し、個人情報だけでなく、情報資産全般の取り扱いについて明確な方針を示し、全社員に継続的にセキュリティ教育、訓練を徹底。

これらの対策の結果、サウンドハウスでは、現在セキュリティ管理においても、安心してご利用頂ける環境が整っていると、確信しております。弊社もサイバーテロの被害にあったからこそ、新規に情報セキュリティ対策を構築できた部分も多々あり、設備も新しく、またより、堅固になったと自負しております。今後もセキュリティ対策を怠ることなく継続して参る所存ですので、どうかご安心の上、サイトをご利用下さい。

○これまでのセキュリティ管理体制について

お客様からは、「サウンドハウスの個人情報管理が甘かったのではないか」という管理責任を問う声を頂きました。当然ながら、流出が起きた時点で、どのような対策を講じていたかが問われます。それに対して弊社の率直な答えは、通常、企業が取るべき対策は取っており、完璧ではないが、落ち度があったと言えるレベルでもない、ということです。これは言い訳ではなく、ありのままの気持ちを述べております。以下にその根拠を述べます。

警察庁が平成 20 年 2 月に発表した平成 19 年度の報告文書によると、全国の企業（全国上場及び店頭公開企業、未上場企業)、教育機関（国公立、私立の大学等)、医療機関、行政機関（県・市町村等の地方自治体、特殊法人）に対して行ったアンケートの結果、不正アクセス等の検知対策を実施している機関は、まだ全体の 4 分の１しかなく、ファイアーウォールの導入は全体の 14.4%、不正侵入を自動検知する IDS に至っては全体の 12.1%し

か導入していないことがわかりました。国内全般にセキュリティ対策への関心がまだ、足りないことがデータで実証された例です。

弊社の WEB サイトは全て自社開発をしており、セキュリティ面に関しましては、24 時間体制のシステム管理者が、外部のアドバイス、指導を受けて構築してきております。そのシステムのセキュリティ対策として、早くからファイアーウォールを構築、2005 年 1 月には「WEB サイトの安全性を証明」、「世界標準」、という謳い文句で広告されているハッカーセーフを導入しました。

その後、2006 年 7 月には、カード会社側からの提案で、「導入すると、万が一不正使用があっても明確な責任区分ができ、その場合カード会社が責任を取るので弊社にとってメリットとなる」というお話から、３D セキュアも取り入れました。この３D セキュアの導入により、弊社の認識としては、セキュリティ対策は十分に行っているという安心感が社内に漂ってしまったようです。

この点が実は一番の問題であったと考えております。例をあげれば、その結果ファイアーウォールによるアクセス制限が甘くなり、弊社のシステム開発を行うスタッフとデータのやり取りを日々実行している内に、拠点のグローバル IP アドレスに対して、SQL サービスのアクセスがインターネットを介して可能な状態になっていました。この点につきましては、大変反省をしております。

その内、世間ではハッキングの事件が急増し、特に 2005 年以降は、SQL インジェクションによる被害も多々レポートされているにも関わらず、それらの情報を十分に得て、様々な他社の教訓から学ぶことがないまま、今回の事件に遭遇してしまいました。しかしこれは単に、一企業のみの責任ではなく、クレジットカードの被害状況を日々、把握、データ化しているにも関わらず、アラートを出して具体的な対策を示さないクレジットカード会社や、これらの被害情報をもっとタイムリーに収集して、世間に大々的に告知する為に能動的に動かない行政にも責任があるものと考えます。本来ならば、クレジットカードの取り扱いを開始するにあたって、インターネットセキュリティー構築のガイドラインがあってしかるべきであり、少なくとも最低限のセキュリティレベルが明示されているべきです。ところが、どこまでやれば十分か、という明確な基準が無いため、加盟店は、それぞれが独断で実行している部分があることを否めません。

セキュリティシステムは日々陳腐化しても、ハッカー技術は常に日々、新しい策を見つけて進化している訳ですから、100％安全なシステムなど、もはや存在しないのです。厳しい現実を直視して、ハッカー対策に取り組んでいかなければならないと、この度、認識を新たにしました。

5. LAC の調査報告概略

被害を拡大させないためにも、あえて記載させて頂くことにしました。

調査機関である LAC が行った WEB サーバーのログ解析により、今回の攻撃手法は「SQL インジェクションおよび以前からサーバー上に存在した悪性プログラムを利用した攻撃であることが確認できました」という報告を、3 月 30 日に受け取りました。SQL インジェクションとは、SQL に外部から別の SQL 文を挿入してデータベースを不正に操作する手法であり、その攻撃は数年前より激増しています。LAC がまとめた「侵入傾向分析レポート」によると、2006 年には、前年の 7 倍にあたる約 250 件の攻撃が確認されたとのことです。

特に注目すべきコメントは、攻撃対象が 2005 年を機に変わったことです。2004 年までは、一般に市販されているアプリケーションソフトが主に狙われていたのが、2005 年になると、企業が独自に作成したアプリケーションを狙った攻撃が激増し、全体のおよそ 7 割にまでなったのです。その理由は極めて簡単です。市販アプリケーションの場合には、複数のユーザーが存在するため、セキュリティ関連の問題も、早期に発覚する可能性が高く、その修正もメーカーが素早く対応します。ところが、自社開発のような独自のアプリケーションの場合、ユーザー企業が自分たちで調査をしなければならず、また、これらの独自開発を試みる企業は、多忙な成長企業が大半ですから、セキュリティ面まで神経が行き届かず、どうしても対策が後手に回りやすいのです。この盲点をついて、2005 年からはオリジナルのアプリケーションが集中的に狙われるようになりました。弊社もその一例であり、ハッカーのターゲットとなりました。

今回の攻撃手法は、「WEB サーバーに置かれた悪性プログラムを経由しての個人情報の抜き取り」です。ところがこの悪性プログラムの aa.asp が、WEB サーバーに挿入、作成された形跡が見当たらないのです。その為、この悪性プログラムを挿入したと思われるバックドアが以前から存在していたように見受けられます。これは推測の域を出ませんが、2006 年 6 月に SQL インジェクションを使用して、犯人はまず、外部からデータベースサーバーを直接操作するためのバックドアを作った可能性が考えられます。これは弊社 2006 年 6 月 29 日にサイトへの不正アクセス方法が中国のブログに載った内容に基づきます。

このバックドアを利用して、さらに社内の別のサーバーにバックドアを埋め込み、そのバックドアを使用して、asp1.asp というファイルを 2006 年 7 月 28 日に WEB サーバー上へ配置された可能性が高いのです。その内容が、2008 年 2 月 18 日に中国のホームページ改ざんサイトに登録されました。その為、不正アクセスが行われ、最終的に、既に存在していたバックドアを経由して悪性プログラムの aa.asp を生成したと推測されます。弊社では、2006 年 12 月にデーターベースサーバーをアップグレードした為、不用意なコマンドを SQL インジェクションでは実行できないようになりましたが、この時点ではすでに悪性プログラムはサーバー内に存在していたと考えられます。

そして 2008 年 3 月 11 日 21:00 頃から 3 月 22 日 24:00 頃の間に、顧客データが保存されているテーブルから 20 件ずつデータを抽出する悪性プログラムが×4875 回、起動されたのです。例えば 2008 年のデータ抽出に関しては、select*from○○○○where○○○○ like’%2008%’　という SQL クエリが送信された形跡が見つかり、2007 年分も合わせて最大、およそ 97,500 件にも昇る顧客データが流出した可能性があることがわかりました。尚、

このクエリは実際には、上記のような形ではなく、難読化されたコマンドであり、解読することで判明しました。

6. ハッカー戦略と、その背景

ここ最近、北京オリンピックの聖火リレーで、数々の妨害が生じていることが話題となっています。既にヨーロッパでは、中国のチベットに対する権力の乱用に対して抗議が活発化しており、多くの国が開会式に不参加を表明しています。特にフランスの大統領は、あからさまに中国を非難し、開会式の不参加を明言したことはテレビでも放映されている通りです。その結果、数日前より中国では、反フランス運動がおきており、中国のネット社会の象徴とも言える携帯電話、及びインターネットの力を駆使して、フランス商品の不買運動が始まり、スーパーのカルフールなどがそのターゲットとして、被害を被り始めています。ちょうどこれは、2005 年 4 月、中国にて反日デモが激化した時の対応と良く似ています。

2005 年、中国において反日運動が広まりました。その当時、中国では携帯電話、及びインターネットが原動力となって、一般市民の反日感情が徐々に高まり、短時間で大きな社会運動にまで発展しました。中国では、ネット社会が影響力を持っている証とも言えます。その一連の流れとして、日本に対する中国からのハッカー攻撃が 2005 年を機に急増したと考えても、何ら不思議ではありません。実際、中国のブログ等でサイトの攻撃手法が堂々と公開されており、弊社サイトの攻撃マニュアルも 2006 年にブログで掲載されていたことがわかっています。

こうして SQL インジェクションによる日本の WEB サイトへの攻撃は 2006 年に向けて急増し、そのおよそ 75%は中国からの攻撃であることがわかっています。ところが、不思議なことに SQL インジェクションによる攻撃が 2005 年から 2006 年にかけて 4 倍、5 倍と急増したにも関わらず、JSOC のレポートによると、被害件数は殆ど増えることがなかったと報告されています。JSOC では、その理由を「JSOC よりお客様へ、SQL インジェクションを重要イベントとしてご連絡し、対象のウェブアプリケーションに存在する脆弱性の確認・修正が行われた結果」と記載されていますが、果たしてそうでしょうか。

そもそも平成 20 年、ハッカーの攻撃が発覚し、企業や個人に被害が生じたとしても、警察庁によるレポートにも記されている通り、日本企業の大半は、自らが解決できるならば、わざわざ行政に報告をすることはないでしょう。情報セキュリティに関する被害届けは、「届け出なかった」とする割合が過半数に昇ることが、平成 20 年 2 月の警察庁による調査報告書に明記されています。そして届出をしない理由の殆どが、「大した被害ではなかったので」、もしくは「社内で対応できたので」のどちらかを挙げています。被害がよほど膨大にでもならない限り、日本企業は自ら申し出て、告知することはあまり無いようです。また、相当数の攻撃が認知されないまま、密かに埋もれてしまったケースも少なくないはずです。更に考えられることは、SQL インジェクションによって悪性プログラムを埋め込んで、それを隠蔽したまま、長期間、周囲にわからないように悪用することをハッカーが目論んだ可能性があります。これら 3 つのポイントを総合的に考慮すると、被害件数が増加しなかった説明がつきます。

あくまでも推測の域を出ませんが、今回の SH に対する攻撃は、自社開発したアプリケーションに対して、SQL インジェクションを介して悪性プログラムを埋め込み、バックドアのアクセスを作っていくような手法が用いられた可能性が高いのです。簡単に言えば、相手

側に知られないように、データを少しずつ盗んで悪用する手法です。2006 年当時のことですから、企業のセキュリティ対策は当然ながら今よりも、更に脆弱なものであったことは明らかです。そして企業のオリジナル・アプリケーションを狙い、クレジットカード情報など、将来、換金できるデータを含んでいそうなサイトを攻撃し、侵入できたとしても、一斉に不正使用を試みるのではなく、日々、少しずつ、気がつかれないように悪用する訳です。こうすることにより、１）不正使用を長期化して、収入がとぎれないようにする、２）不要なアラートをたてて、相手国がセキュリティを強化し、侵入しづらくなることを避ける、という２つの目的を達成したのでしょう。

それを裏付けるかのごとく、2006 年、6 月 29 日、中国のブログにおいて何と、サウンドハウスが名指しで公開され、そのサイトに侵入することが成功した事例が解説されていたのです。そして今年の 2 月 18 日、同様に中国のサイトで弊社の名前が再度掲載され、それが引き金となって、3 月 11 日からの集中攻撃へと発展しました。

その後、攻撃に参加したハッカーらは、皆マニュアル通りに従って行動したのでしょうか、３Ｄセキュアを導入している Gungho 等のゲームサイトで、抽出したクレジットカード番号と、弊社サイトへのパスワードをマッチングさせて本人確認の認証を潜り抜け、金券、商品を購入し、その後、RMT （Real Money Trade）等のサイトで購入した商品を転売するという手段で、足がつかない形での換金を実行したのです。

不可解なことも多々ありますが、少なくとも今回の問題のルーツは 2006 年まで遡ることは、ほぼ間違いないようです。その為、近年になっていくら新しいセキュリティシステムを導入しても、2006 年に挿入された不正プログラムはその検閲に引っかかることなく、埋もれたままになっていたのです。その結果、3 月 11 日から攻撃を受け、ハッキングの被害に遭遇することになりました。

7. サイバー社会への警告

今回の事件から、実に多くの教訓を得ることができました。特にサイバーテロの現実を目の当たりにし、SQL インジェクションの手法や、ハッカーグループの換金の手口まで検証することができました。しかし、サイバーテロは犯罪行為です。それ故、サイバー戦争の坩堝の中で、ハッカーより宣戦布告された現実を直視して、自らその戦いに負けぬよう、防御体制を整備しなければならないと、思いを新たにしています。

今回の流出に使われた手口は、2 年前に SQL インジェクションによって埋め込まれた悪性プログラムを活用するという、過去に殆ど例がないものでした。それは時限爆弾のように、いつ、不正使用をされても不思議ではない悪性プログラムです。その存在に全く気付かずに、この 2 年間、自分が会社を運営し、プログラムを動かしてきたかと思うと、ぞっとします。しかも弊社の場合、中国のブログ等で SH へのサイト攻撃の手法までが掲載されていたのです。その結果、一斉攻撃が 3 月 11 日から開始されましたが、それまでもおそらく、こちらに気づかれないように少しずつ、不正使用が繰り返されていた疑いを払拭できません。

おそらく弊社だけでなく、国内の他の企業も、2006 年前後の SQL インジェクション攻撃によって、同様の被害を受けている可能性があると考えられます。つまり、いつの間にか悪性プログラムを埋め込まれているかもしれないのです。もしそうならば、既に不正利用は始まっているはずであり、いつ集中攻撃が起きても不思議ではありません。

このままでは、いつまでたってもサイバー被害が続出するのが目に見えています。ではどうしたら、ハッカーの攻撃を未然に防ぐことができるのでしょうか？またどうやって、既に挿入された不正プログラムを見つけることができるのでしょうか？クレジットカードの不正利用についてもしかりです。どうしたら、個人データのセキュリティ管理がきちんと行われ、安全で強固なものとなるのでしょうか？如何にして市民をサイバーテロの被害から守ることができるのでしょうか？

正直に申しあげますと、サイバー社会の実態は一般市民が想像している以上に、既に汚染されていると考えております。つい数日前も、弊社のスタッフが利用している著名サイトにおいて、不正にログインされ、彼のパスワードが改ざんされていることが発覚しました。ログを検証してみると、国内外の IP アドレスからのアクセスが数秒ごとに頻繁に行われている形跡が残っていました。現実的には顧客データを持つ各社 WEB サイトにおいて覗かれたことがないデータベースというのは、あまり存在しないのではないでしょうか。そして昨今のトレンドの流れで、ハッカーの目的が「換金」に変わってきていますので、それが出来そうなデータをその中からあさっているのです。その結果、日本国内において、セキュリティの盲点をつかれた事故が絶えず生じており、抜本的なセキュリティ対策、及び改革を今、必要としているのです。

ところが、セキュリティの不備は中々解消されず、セキュリティの基準となるガイドラインさえ、殆ど見かけません。対策が進歩しない理由は明らかです。まず、エンジニアが不足していることです。本来ならば、プロのハッカーを雇用して、彼らの目から見た、美味しいと思えるホールを見つけて対処するようなハッキング対策がなされなければなりません。それ故、優秀なハッカーを見つけたら、むしろ国家の機密情報機関で雇用し、高額

な報酬を払ってでも、セキュリティ対策を講じるべきなのです。

2つ目の理由は、高コスト体質です。現在は普及率がまだ低いため、侵入検知システムは当然のことながら、コスト高となっています。しかし設置数が今の 10 倍、100 倍になったらどうでしょうか？いずれそのコストは現在の何分の１になるはずです。また、どうしてもコストダウンできないサービスがあれば、それこそ、国家が何らかの形で導入する為の支援策を提供するべきではないでしょうか。そのような前向きな行政対策を期待したいものです。

次の理由はその行政にあります。これだけ個人情報の流出が頻繁におきている昨今の現状を振り返れば、行政側も積極的に対応せざるを得ないはずです。世界的なトレンドをまず把握し、日本における地域的な特異性に留意した上で、民間企業、教育機関と協議を繰り返しながら、有効な対策案を打ち出していく必要があります。特に、セキュリティ対策に不可欠な監視装置の設置については、補助金や税の優遇措置等、積極的な支援策を打ち出していかなければ、普及に時間がかかりすぎて、手遅れになってしまいます。また情報の収集及び分析の開示に力をいれて、よりスピーディーな対策案を提示して頂きたいものです。

企業、金融・クレジットカード会社、そしてセキュリティ会社にも、それぞれ課題があるのではないでしょうか。まず企業はクレジット加盟店として、顧客のクレジットカードデータを処理し、保管する手前、その管理には細心の注意を払う義務があります。ところが現実問題として、セキュリティ管理についてはそのノウハウや、対策方法についての根本的な情報が不足しており、大半の企業はどういうセキュリティシステムを導入するか、どのくらいコストをかけるべきか、わからなくて困っているのが現状です。実際問題として、どこまで対策をとれば十分なのか、というガイドラインが無いため、予算を組むこともできないのです。また、一般論としてセキュリティ対策は、高価である、という既成概念があるため、どうしても後回しになってしまうようです。その結果、セキュリティ対策に進展が見られないまま、ハッカーの被害に遭うと、あわてて対策を講じるという流れになってしまっているようです。企業は、顧客データを預かる立場にありますから、サイバー社会のトレンドを把握し、どのようなセキュリティシステムを導入すれば、安全にデータを管理できるか、と自らリサーチして学び、日々知識の向上に努め、対策をとっていくことが不可欠です。

次にクレジット会社に関してのコメントです。弊社は、クレジットカード会社推奨の３Ｄセキュアを導入したことでクレジットカードの不正利用を防ぐことができるようになりましたが、今度はハッキングの被害に遭遇し、流出した顧客データを用いて他のサイトの 3D セキュアを使用した不正利用が発生しました。弊社は加盟店の立場として、こういう時こそカード会社が多少なりとも協力してくださり、お客様に迷惑がかからぬように、また早急にカード利用が復旧できるように手伝って下さると考えていたのですが、そうではありませんでした。

クレジットカードの再開にあたっては、協力してくださるどころか、驚くほど高額な調査費用のかかるサービスを、再開の条件として提示してきました。既に弊社では LAC の調査に多額の費用をつぎ込んでおり、同様の調査にさらに付加調査を加えたものをクレジッ

トカード会社が提案する２つの会社にお願いすることが､必須と言われてしまったのです。１つはサイバートラスト社によるフォレンジック調査であり、これは流出が生じたサーバーから不正行為の追跡を行い、証拠を見つける作業を意味します。もう一社は、NTT データセキュリティー社であり、PCIDSS と呼ばれるクレジットカード会社５社がクレジットカードの情報保護の為に策定した国際基準に準拠するための事前調査を行います。既に弊社はカードの利用を止め、営業に大きな打撃を受けているにもかかわらず、更に追い込みをかけるように多額な負担を要求してくるのには閉口してしまいました。

本来、クレジットカード会社は、被害に遭遇した加盟店に何を求めるべきでしょうか？まず､セキュリティ対策が十分に施され､クレジットカードの取り引きが今は安全である、ということを確認した上で、お客様へのカードサービスを復旧することが一番大事なことではないでしょうか。今回の流出を機に、弊社のセキュリティシステムは大幅にアップグレードされ、監視機能も付加されており、優れたセキュリティシステムを構築することができました。それ故、クレジットカード利用が再開できない理由が見当たりません。

もし本当にセキュリティ対策をクレジットカード会社を重視するならば、加盟店が当初、申請をする時点で、セキュリティ対策がしっかりとられているかどうか、一定の基準を設けてチェックし、それにパスした店舗のみを加盟店とするべきでしょう。ところが現実にはカード会社同士の営業競争があるのでしょうか、加盟店を安易に増やすことが優先され、問題が生じた時にのみ調査をするという、逆の順序になってしまっています。クレジットカード情報の流出、及び不正使用においても、クレジットカード会社はもっと情報を公開して、不正使用の予防に役立つようなデータを周囲に提供するべきでしょう。現実問題としては、クレジットカード会社は情報の公開を避ける傾向にあり、クレジットカード情報の流出や不正使用について、タイムリーに情報をリリースしていないように見受けられます。そしてセキュリティ対策よりもむしろ、クレジットカード契約者数を増やすことに熱心であるように見えるのは、気のせいでしょうか。もしそうだとすれば、理由があります。クレジットカード会社はその熾烈な業界内での競争の中で、各社とも会員数を増やしてマーケットシェアを上げるために必至です。また、優良加盟店も増やしてショップできる窓口を増やさなければ、カードからの手数料収入が増えません。その為、営業を優先する余り、恐怖心を煽るようなことは言えないのです。もしクレジットカードの不正使用の実態とその被害状況の実態を市民が知ったとするならば、多くの方々はきっと「クレジットカードはやっぱり怖い」と思って、手放す人もいるでしょう。また、新規加盟店に、一定基準の高いセキュリティレベルを求めてしまえば、中小企業の大半がそのコストを払うことができずに、取り扱いを諦めてしまうことになりかねません。つまり、問題点を開示しすぎても、取り扱いの条件を厳しくしすぎても、顧客離れが進み、クレジットカード会社自らにつけが返ってきます。クレジットカード会社も今や、情報公開のスタンスを踏まえ、企業、ユーザーと共に協力しながらクレジットカードの不正利用、犯罪に対して立ち向かわなければならない時がきていると言えます。

最後は、セキュリティ会社の在り方と、そのマーケティング手法です。セキュリティ会社も企業ですから、当然ながら利潤を追求しており、商品、サービスを販売して利益をあげることを目指します。それ故、どうしても一般ユーザーが安心してしまうような表現が

多く使われてしまうように見受けられます。例えばハッカーセーフには、「WEB サイトの安全証明」「365 日休まず WEB サイトを診断することでハッキングのリスクからサイトを守ります」と書かれているため、このサービスを導入することで、ユーザーが安心してしまうのではないでしょうか。実際に弊社もハッカーセーフを導入していましたが、今回の流出には全く功を奏しませんでした。これらのサービスは、他のセキュリティプランと併用して導入されなければ十分とは言えないのです。

もうひとつの大事なポイントは、せっかくセキュリティ調査会社が重要な資料やデータを持っているにも関わらず、そこで情報が止まりがちになってしまうことが懸念されます。彼らこそ、最前線で活躍している情報の宝庫であり、最新の情報を多数入手している訳ですから、そこで見聞きした重大メッセージが、行政を始めとし、企業や一般社会にもタイムリーに伝達されるようになると状況は一変するでしょう。

そのためにも、行政がもっと介入して、セキュリティ調査会社にインセンティブを与え、実際には行政の特殊部隊のような立場で仕事をこなして頂き、協力体制を密に保つことが不可欠といえます。その強い要望、アプローチが行政から無い限り、また、その為に十分な予算を組んで妥当なコストを支払うという条件が整わない限り、優秀な調査機関が苦労して得た情報をそう簡単には公開することはないでしょう。セキュリティ調査会社が活躍する場がもっとあるような気がしてなりません。

8. 総論

今回、この個人情報流出事件が弊社にて発覚したことを、私はサウンドハウスという会社の経営者として、色々な意味で大いに反省をすると共に、また、前向きな気持ちをもって受け止めております。サウンドハウスは今から 15 年前、何もないバラック小屋から創業し、いつしか音響業界においては価格破壊の雄として時代の波に乗り、今日では国内最大級の販売店のひとつと言われるまで成長を遂げました。何もない所から起業したからこそ、失うものも何もないと考えることができるのも、弊社の強みです。だからこそ、物怖じしないで皆様には包み隠さず、ありのままに事実関係を報告することが、弊社の使命だと思っています。

今回のプレスリリースにあたり、様々な反論が周囲からありましたが、お客様は勿論のこと、関係者各位、及び世間一般も含めて、単に事実関係の確認に留まらず、普段は語られることのない裏側の部分も含めて情報を公開し、自分の本音をそのままお伝えすることにより、少しでも参考になればと願いつつ、この数日間、心を込めて筆を執りました。歴史を遡らなければならないこともあり、またサイバー社会のことですから、不透明かつ、確定できないことも多々あります。しかし、これまでの経過、弊社がとった対策、及び今後の計画などを含め、その詳細を皆様に報告することにより、単に本件についての誤解を払拭するだけに留まらず、一連の検証から浮かび上がってきた事実を直視して、サイバー社会における問題と実態についての警告をより、リアルなものと受け止めて頂き、新たなる対策、方向性を見出すきっかけとなることができればと思います。

確かに今回の事件では、数多くのお客様にご迷惑をお掛けしており、できる限りの努力をもって大勢のスタッフと共に、何日も夜通しの作業を続けながら、お客様の対応を重視してまいりました。しかし冷静になって考えてみると、実は学ぶ事も多々あることに気付きました。

まず今回の流出事件に遭遇することによって、弊社のセキュリティ管理の在り方が抜本的に見直され、大幅に改善される結果になったことが、挙げられます。サイバーテロによる破壊の被害にもあいましたがその結果、サウンドハウスは今、およそ最強のセキュリティ管理体制を整えつつあります。

次に最先端のサイバーインフラについて、学ぶ機会が与えられたことです。この事件無くしては、インターネット関連のセキュリティについて私自身が積極的に学ぶことはなかったでしょう。ましてや、自社のサイトに侵入するマニュアルが中国のブログで出回っていることなど、想像もできないようなことが実際におきていることを知り、身が引き締まる思いです。学びなくしては進歩はありません。その学びの為に、今回大きな打撃を弊社は被り、それ以上にお客様にも大変なご迷惑をかけてしまい、申し訳ない気持ちで一杯ですが、それにめげることなく、新たなるステージに向かうことができるという思いを強く持っています。

この気持ちを持続して、真実をありのままに公開し、ひたすらお客様に対して一生懸命対応させて頂くことが、この度、色々とご迷惑をおかけしたお客様に対する恩返しと思っております。また、サイバーインフラに関わる企業、自治体、しいては国家に少しでも参考になるメッセージを発信することにより、サイバー社会を覆う闇の力や、邪悪なサイバ

一犯罪から一般市民を守る為の対策を、早急に協議するきっかけができるのではないかと考えております。

サウンドハウスは、人助けの為に創業した会社の歴史があり、今でもその想いは続いています。それ故、これを機に、今一度、原点に戻って、お客様からの信頼の回復、そして更なるサービスの向上を実現し、日本のサイバーインフラがより安全で、信頼できるものとなるため、あらゆる努力を惜しまず提供していきたいと願っております。

この度は、大変ご迷惑、ご心配をおかけ致しました。これからもサウンドハウスを宜しくお願い致します。

株式会社サウンドハウス

代表取締役社長　中島尚彦