NRI 未来創発
Dream up the future.

ITソリューション フロンティア
IT Solutions Frontier

特集「情報セキュリティ対策の最新動向」

06 2012 Vol.29 No.6
（通巻342号）

www.nri.co.jp

野村総合研究所
Nomura Research Institute

Adobe Readerのメニューバーで「表示(V)→ページ表示(P)」にある「見開きページ(U)」と「見開きページモードで表紙をレイアウト(V)」の2か所にチェックすると紙面のイメージでご覧頂けます。また、両面プリンターをご使用の場合、印刷時に「ページの拡大/縮小(S)」で「小冊子の印刷」を選択すると紙面に近い状態を再現できます。

ITソリューション フロンティア
IT Solutions Frontier
06／2012

NRI Web Site

インターネットの隆盛と情報セキュリティ

総務省の2010年の調査によると、インターネットの利用者数（6歳以上で1年間に1回以上利用した人）は9,462万人で、人口普及率は78.2%に達している。年齢別では13歳以上、40歳代までのすべてで95%を超え、60〜64歳でも70%となっている（www.soumu.go.jp/johotsusintokei/statistics/data/110518_1.pdf）。NRIが2011年に首都圏（1都3県）で実施した「生活者1万人アンケート調査」でも、PCや携帯電話などを使ってほぼ毎日インターネットを利用している人の割合は、20歳代が80%、全体でも45%である。インターネットは今や日々の生活に溶け込んでいる。

インターネットの利用を加速しているのがスマートフォンである。その販売台数は急伸しており、2011年10月には携帯電話全体の販売台数の7割を超えたもようだ（bcnranking.jp/news/1111/111110_21373.html）。スマートフォンはホームページやソーシャルメディアの利用が手軽にできる便利さから、今後の端末の主流となることは間違いないだろう。

インターネットを介した消費も拡大している。大手のインターネットショッピング運営会社では、2011年の取扱高（出店している店舗の売上合計）が1兆円を超え、大手百貨店の売上高と肩を並べる規模となった。消費者向けのビジネスを行う会社では、インターネットを活用したサービスの良しあしが事業拡大の鍵となることは言うまでもない。

インターネットの利用形態も変わってきている。これまでは、“人”がインターネットにつながる形態が主だったが、今後は機械同士がインターネットによって通信するM2M（Machine to Machine）の時代がやってくる。自動販売機や建設機械の遠隔監視・制御、電気・ガスなどエネルギー消費状況のモニタリング、農業でのセンサー情報による温度・水などの管理、物流におけるRFID（無線個体識別）の利用などが例として挙げられる。省エネ型のインフラを備えるスマートコミュニティーの建設・整備など、今後の社会基盤の再構築に際して、インターネットはさらに重要な機能を果たすことになる。

インターネットは利便性が高い半面、誰でも自由に接続できるというオープンさゆえの弱点もある。全体を管理・統制する機能がない分散型のネットワークであるため、信頼性や性能の面で不安定であるほか、コンピュータウイルスへの感染、ホームページの改ざん、フィッシング詐欺などセキュリティ上のリスクがある。M2Mもウイルス感染などによって機械の誤作動や停止が引き起こされる不安がある。

2011年には機密情報をねらったサイバー攻撃の事件が多く報道され、情報セキュリティへの関心が高まっている。情報漏えいは、社会的信用の失墜、事業（売上）の不振、緊急対策費の計上、損害賠償など、企業に甚大な

野村総合研究所
理事
稲月　修（いなつきおさむ）

被害をもたらす。個人情報や機密情報を流出させないための情報セキュリティ対策は、システム部門の担当範囲を超えて経営的視点でとらえるべき重要な課題である。しかも、昨今の情報漏えいの事例を見れば、自社グループだけでなくバリューチェーンを形成する関連企業を含めた情報セキュリティの全体統制が必要なことは明らかである。

情報セキュリティとは、情報資産の機密性（漏えいの防止）、完全性（改ざんの防止）、可用性（データ破壊の防止）を確保することである。ISO（国際標準化機構）やJIS（日本工業規格）で規定されている情報セキュリティマネジメントシステムでは、事業活動のリスクマネジメントという視点から、情報セキュリティ上のリスクを分析・評価し対策を実施するPDCAサイクルを回すことが推奨されている。

セキュリティリスクは、対策が必要なリスクと受容するリスクに分類される。事業への影響の大きさを中期的視点で評価し、リスクに優先順位を付けて分類することになるが、受容するリスクの判断は経営者によってしかできない。また、事故が起きることを前提に、被害の最小化と迅速な対策のために、事故発生時の連絡体制や対処方法を準備しておくことも重要だ。

上場企業が金融商品取引法で提出を義務付けられている有価証券報告書には「事業等のリスク」という項目があり、情報セキュリティ面のリスクとそれに対する取り組みの概要を記述することになっている。その内容が、はたして実情に合わせて更新されているだろうか。情報セキュリテイ対策はPDCAサイクルを回して地道に改善するしかなく、リスクの認識と取り組み状況が有価証券報告書にも反映されるようにしてほしいものである。

情報セキュリティ対策の基本は“人”である。内閣官房情報セキュリティセンターはサイバー攻撃対策の一環として、2011年10月～12月に政府機関の職員約６万人を対象に、標的型攻撃への対応をテストした。対象者には事前に教育を実施し、標的型攻撃でよく使われるメールに似せた無害のメールを送信した。その結果、約10％の人が添付ファイルを開き、約３％の人がリンクをクリックしたという。（www.nisc.go.jp/press/pdf/torikumi_press.pdf）

外部からの攻撃以外にも、モバイル端末の盗難や紛失、USBメモリーでのデータの持ち出し、ソーシャルメディアなどへの不用意な書き込み、メールの誤送信など、情報漏えいにつながる要因は多い。これらのリスクへの対策の鍵はルール化と意識の向上である。守るべきルール（行動基準）を社内外のセキュリティリスクの実情に合わせて検討・策定し、継続的な啓発・教育活動を実施してルールの徹底を図ることが重要である。 ■

情報セキュリティ対策における課題
―2011年のセキュリティ事件を教訓に―

不正アクセス手法の高度化や多様化に伴い、情報セキュリティ対策の難しさも増している。ツールなどの技術的対策は着実に進んでいるが、情報をタイムリーに入手し、それに基づいて意思決定する人材の確保が多くの企業にとって課題となっている。本稿では、2011年に発生した情報キュリティ事件を取り上げ、進化する攻撃への対策のポイントについて解説する。

2011年の3大セキュリティ事件

近年、ニュースなどでよく耳にするように、ハッカーによる不正アクセスなどの情報セキュリティ事件が後を絶たない。2011年には以下のような事件が大きな話題になった。

(1) ネットワークサービスの個人情報漏えい

2011年4月、ソニー・コンピュータエンタテインメント（SCE）のネットワークサービス「PlayStation Network」とビデオオンデマンド・サービス「Qriocity」のサーバーが不正侵入を受けたという報道があった。アプリケーションサーバーの脆弱（ぜいじゃく）性（攻撃に利用される恐れのある仕様上の欠陥や問題点）を衝いた不正アクセスで、実に7,700万件の個人情報が漏えいした可能性があるという。

サーバーに最新のパッチ(修正プログラム)が適用されていなかったことが原因だが、大規模システムにおけるパッチマネジメントは想像以上に難しい。最新の脆弱性情報を収集する手間もさることながら、パッチ適用による不具合発生のリスクやコスト（大規模システムでは対象サーバーが数百台になることもある）を考慮した上で、パッチを適用するかどうかを総合的に判断しなければならないからである。

(2) ネットバンキングへの不正アクセス

2011年8月、全国の銀行がネットバンキングの不正利用に注意を促す文書をホームページに掲載した。6月下旬以降に不正アクセスが多発し金銭的被害も発生していることを受けての対応である。不正アクセスの多くは、ネットバンキング利用者のPCをマルウェア(コンピュータウイルスなど悪意ある不正なプログラム)に感染させてパスワードを盗み、利用者になりすましてログインするという手法によって行われていた。

近年では、不特定の企業から漏えいしたIDとパスワードのリストを用いてログインを試行しIDとパスワードの組を特定する、リスト型アカウントハッキングと呼ばれる攻撃も少なくない。こうした攻撃への対策として、同一IPアドレスからのログインの成功回数、失敗回数などをモニタリングし、不正アクセスの疑いがあるアクセスをタイムリーに遮断する運用が求められる。

(3) 防衛関連企業への標的型メール攻撃

2011年9月、三菱重工業が標的型メール攻撃を受けたことが報道された（後に社内情報

NRIセキュアテクノロジーズ
コンサルティング事業本部
上級セキュリティコンサルタント
鴨志田昭輝（かもしだあきてる）

専門は情報セキュリティに関わる調査・評価・コンサルティング・教育

NRIセキュアテクノロジーズ
コンサルティング事業本部
上級セキュリティコンサルタント
鈴木　伸（すずきしん）

専門は情報セキュリティに関するコンサルティング

が漏えいした可能性があると発表）。その後、川崎重工業やIHIなどの企業でも同様の攻撃を受けていたことが判明し、防衛関連企業が被害に遭ったことから大きな注目を浴びた。川崎重工業のケースでは、日本航空宇宙工業会（SJAC）の職員のPCがマルウェアに感染し、その職員が関連企業とやり取りしていたメールが盗まれ、それを悪用した標的型攻撃が行われたということである。

標的型攻撃は従来のセキュリティ対策で防ぐことは難しいため、マルウェア感染を検知して外部への通信を遮断する“出口対策”が重要となる。出口対策としては、セキュリティベンダーが次世代ファイアウォールと呼ぶ製品や、DLP（Data Loss PreventionまたはData Leak Prevention：データの機密性を識別してデータの流れを監視・制御するツール）と呼ばれる新しい情報漏えい対策ツールが注目されている。

セキュリティ対策は“運用”が課題

上記のような情報セキュリティ事件の発生を受けて、多くの企業でセキュリティ対策が見直されている。体制や仕組みの構築（情報セキュリティ製品の導入など）はもちろん必須だが、それに加えて適切な“運用”が重要な課題となる。運用とは、環境や脅威が変化しても重要情報を守れるように常に対策を施すことである。

しかし、その運用をどうするかに悩まされている企業が少なくない。常に最新の情報を収集して適切に対応することがいかに難しいことか、多くの企業はあらためて気が付いたといえるだろう。

中長期的な視点での対策が重要

適切な運用の基本は、脆弱性や攻撃のトレンドなどに関する一般的な情報の収集である。これらの情報は、独立行政法人情報処理推進機構（IPA）のホームページなどで収集することができるが、情報セキュリティへの脅威が深刻・複雑になるに従って、情報共有の場の必要性が増してきている。これを受けて2011年10月には、標的型攻撃などの情報共有を目的とした官民連携の「サイバー情報共有イニシアティブ」が発足している。

情報を収集したら、その情報を分析して対策の意思決定に役立てることが必要である。そのための人材確保が多くの企業で課題となっている。

2011年に発生した情報セキュリティ事件は、セキュリティ対策における運用の重要性をあらためて示した。適切な運用を行っていくために必要な情報の収集と、それを分析して意思決定する人材の確保は、多くの企業にとって共通の課題である。これらは簡単に解決できるものではない。セキュリティベンダーとの連携や人材育成などを含めて、中長期的な視点に立った情報セキュリティ対策がますます重要になっていくだろう。 ■

新たなサイバー攻撃への対抗策
―進化する標的型攻撃に備えるために―

2011年の夏、国内の防衛関連企業に対してサイバー攻撃が仕掛けられるという事件が起きた。海外でも、大手ネット企業やセキュリティ関連企業、さらに原子力発電所の制御システムまでもがサイバー攻撃を受けた。本稿では、このような特定の企業やシステムに的を絞ってシステムへの侵入や情報詐取を試みる新たなサイバー攻撃の手口と、最新の対策について解説する。

新たなサイバー攻撃の手口

特定の企業や個人の端末をマルウェア（コンピュータウイルスなど悪意のある不正なプログラム）に感染させ、重要情報を盗み出す新たな手口のサイバー攻撃は、標的型攻撃やAPT攻撃（Advanced Persistent Threat）などと呼ばれている。

攻撃者の目的は、標的企業が持つ知的財産などの重要情報の取得であることが多い。攻撃の特徴として、マルウェアが利用されること、事前に情報収集するなど手口が巧妙であること、攻撃が気付かれにくいため長期間にわたることが挙げられる。

このような攻撃は、一般に以下に示す段階を経て行われる（図1参照）。

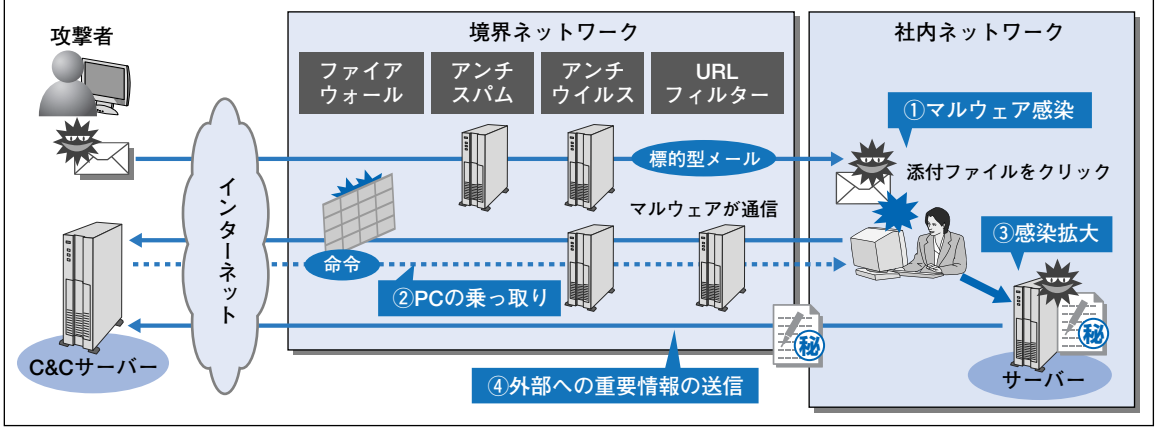
①マルウェア感染

攻撃者は、人事異動や打ち合わせ資料など、標的企業の受信者が興味を引く、または疑いを持ちにくい内容のメールを送付する。これにはウイルスを含むMicrosoft WordやExcelの文書ファイル、PDFファイルなどが添付されており、ファイルを開くと受信者のPCがマルウェアに感染する。

②PCの乗っ取り

PCに入り込んだマルウェアがインターネット経由で通信を始める。通信先はCommand & Control（C&C）サーバーと呼ばれる、攻撃者があらかじめ準備したサーバーである。攻撃者はC&Cサーバーを介してPCに命令を送

図1　標的型攻撃の代表的な手口



NRIセキュアテクノロジーズ
MSS事業二部
ITセキュリティアナリスト
木村尚亮（きむらたかあき）
専門はWebサイト、エンタープライズセキュリティ全般

表1　企業が実施している入口対策と標的型攻撃に対する有効性

入口対策	特徴
ファイアウォール	標的型攻撃メールは通常空いているSMTPポート（TCP25番）宛の通信なので遮断できない。マルウェアからC&Cサーバーへの通信は、通常のWebブラウジングと同じHTTP（HTTPS）ポートが利用されることが多く遮断できない。
スパムメール対策	広く出回っている広告目的などのスパム（迷惑）メールではなく、特定企業をターゲットにするために文面が考えられており、スパムメールと判定するのは困難。
ウイルス対策ソフト	特定企業をターゲットに作成されたマルウェアであるため、パターンマッチング型のウイルス対策ソフトでは検知が困難。攻撃者は事前に主要なウイルス対策ソフトで検知されないことを確認してからメールを送付してくることもある。
従業員教育	不審な添付ファイルやURLはクリックしないことなどについて従業員に注意を喚起し教育していても、攻撃者は事前に情報を収集してできるだけ不審に思われないようなメールを送付してくるため、警戒せずにクリックしてしまう恐れがある。
URLフィルター（HTTPプロキシ）	業務外利用や情報漏えい対策を目的とした製品であるため、マルウェア対策は範囲外であることが多い。対応する場合でも、マルウェアが通信するC&CサーバーのURLは短期間で変化し続けていくため、URLフィルターのデータベースに取り込むことは容易ではない。

ることができるようになり、PCは攻撃者に乗っ取られた状態となる。

③感染拡大

攻撃者は、PCに格納されている情報（受信メール、Webブラウザーのアクセス履歴、認証情報など）や通信を盗み見して得られた情報を使い、重要情報が格納されている企業のサーバーやドメインコントローラ（ユーザー情報の管理や認証を司るコンピュータ）へ侵入する。

④外部への重要情報の送信

FTP（ファイル転送プロトコル）やHTTP（Webサーバーとクライアント間のデータ転送プロトコル）など、企業から外部へ向けて許可されている通信を使い、企業の重要情報をC&Cサーバーに送信する。

防ぎにくい標的型攻撃

これまで企業ではマルウェアを社内に入れない、もしくはマルウェア感染を防ぐことを目的とした“入口対策”が重点的に実施されてきた。

表1は、現在多くの企業で実施されている対策と、標的型攻撃に対する有効性についてまとめたものである。これらの対策は、標的を定めない不特定多数をターゲットにした攻撃に対しては効果がある。しかし標的型攻撃では、攻撃者は事前に標的企業の内部情報を収集するなど周到な準備をしており、従来の対策では防ぐことが難しい。

現状では攻撃者側が優位であり、いったん標的にされてしまうと、情報セキュリティ対策を実施している企業でも被害に遭ってしまうのである。

入口対策の強化を

このように、従来型の入口対策では防ぐことが難しいため、標的型攻撃の対策としては

後述する“出口対策”に焦点が当たっている。しかし、マルウェア侵入を「やむを得ない」と諦めるわけにはいかないし、入口対策にはまだ改善の余地が残されている。

従来の対策のうち、多くの企業で十分ではないのがパッチ（修正プログラム）のマネジメントである。管理対象がMicrosoft社製品以外のソフトウェア（Adobe Systems社製品やJavaなど）にも広がってきたことや、脆弱（ぜいじゃく）性が発見される頻度が高くなっていることから、アップデート（パッチの適用）が追い付いていない企業が多い。

アップデートが追い付かない場合は、攻撃を受けた場合の影響を緩和する対策を検討すべきであろう。Adobe FlashやJavaに関しては、業務上必須でなければアンインストールすればよい。あるいは、通常利用するWebブラウザーでは無効化しておき、それが必要なWebサイトは別のWebブラウザーで有効化して利用するなどの使い分けが考えられる。Adobe Readerに関しては、攻撃で頻繁に利用されるJavaは無効化すべきである。あまり攻撃の対象とならない別のPDF閲覧ソフトを利用するという方法もある。

次に検討が必要なのは、アプリケーションの“ホワイトリスト”化である。実行を許可してよいアプリケーションを管理者がホワイトリストに登録し、許可されていないマルウェアのようなプログラムが実行されることを防ぐ対策である。

ホワイトリストができれば、Microsoft社から提供されている「ソフトウェア制限ポリシー」や「AppLocker」（Windows 7 UltimateとEnterprise、Windows Server 2008 R2で利用可能）などの機能を使ってアプリケーションの実行を制限することができるようになる。特に「AppLocker」では、実行ファイルの電子署名を判定条件に利用できるため、例えば「Adobe Flashアップデートのインストーラは実行を許可する」というポリシーを定義すれば、アップデートの都度ホワイトリストを更新する必要がない。

一方で、標的型攻撃の被害拡大を受け、新たなソリューションやサービスも出てきている。技術的対策で最も注目されているのが振る舞い検知型のマルウェア対策ソフトである。既存のマルウェア対策ソフトはパターンマッチング型が主流であるが、振る舞い検知型は、ファイルを仮想環境で実際に実行させてマルウェア固有の動作を行うかを検知するロジックを組み込んでおり、既知・未知に関係なくマルウェアを検出できる。

人的な対策では、標的型攻撃メールへの訓練が挙げられる。従業員に対して人事異動表などを装う訓練メールを送信し、本来自分に届くことが不自然なメールを受信させ、添付ファイルをクリックするかどうか判断することを実体験させるのである。従業員は訓練を通じて、標的型攻撃を身近な脅威として認識する。

訓練と併せて教育を実施することで、セキュリティ意識を向上させることも期待できる。また標的型攻撃のメールを受信した場合のエスカレーション（上司などへの報告）も併せて訓練することで、組織としての対策の実効性を向上させる効果も見込める。

標的型攻撃の増加を受けて、内閣官房など12の政府機関が2011年10～12月に大規模な訓練を実施した。訓練は比較的短期間で実施できるため、標的型攻撃には即効性のある対策といえる。

出口対策のポイント

標的型攻撃に対する出口対策は、社内に入り込んだマルウェアや攻撃の兆候をいち早く発見し、標的型攻撃の後続ステップである「PCの乗っ取り」「感染の拡大」「外部への重要情報の送信」へと進ませないようにするための対策である。

出口対策では、認証付きProxy（Proxyサーバーを使ったWebアクセスの際に認証を必要とする仕組み）を導入してマルウェアが外部向けに通信する際のハードルを高くしたり、マルウェアの外部向け通信を各種セキュリティ機器のログ（履歴）を監視して検知したりする方法がある。

しかしこれで万全というわけではなく、ログ監視にも問題点がある。例えば従業員が自由にプログラムをインストールできるPCでは、ソフトウェアのアップデートのような正常の通信がログ監視によってアクセス違反として検知されてしまう。そのため、前述した「アプリケーションのホワイトリスト化」などの対策を併用することによって実行可能なプログラムを制限し、管理可能な正常状態をつくりあげることで、監視精度を高めることが必要である。

感染が疑われる動作のアラート（警告）を検知した際には、実際にマルウェアに感染しているのかを短時間で切り分ける必要がある。それにより感染が発覚した場合は、迅速かつ適切な一次対処が求められる。さらに、被害状況を把握するために、何をするマルウェアなのかを素早く解析する必要がある。これらの対応は、情報セキュリティ対策の中でも特に専門知識が要求される領域である。そのため、セキュリティログの監視を外部委託する場合には、上記のような対応が可能かどうかを確認する必要がある。

重要な“多層防御”の対策

情報セキュリティの基本は多層防御だといわれる。標的型攻撃には特効薬がなく、特に多層防御が重要となる。そのため、本稿で紹介した入口対策や出口対策を組み合わせた対策の検討が必要である。独立行政法人情報処理推進機構（IPA）から提供されている情報（www.ipa.go.jp/security/keihatsu/pr2012/general/02_targeted_attack.html）も併せて参照されることをお勧めしたい。 ■

スマートグリッドに必要なセキュリティ対策
―安全・便利な送電網の構築に向けて―

昨今、再生可能エネルギーの導入促進、電力の有効活用のニーズを背景にスマートグリッド（次世代送電網）が注目されているが、スマートグリッドはネットワークを利用した通信を行うため、情報セキュリティ対策が欠かせない。本稿では、欧米のスマートグリッドにおけるセキュリティ対策を紹介するとともに、日本で必要となる対策について提言する。

スマートグリッドの目的

スマートグリッドは、送電網に情報通信技術を組み込むことによって、効率的な電力の供給および制御を実現する仕組みのことである。簡略化して次世代送電網と呼ばれることも多い。

スマートグリッドを構築する目的には国によって違いがある。日本では、CO_2排出削減のほか原子力発電の代替としても注目される太陽光発電など再生可能エネルギーに対応することが目的の１つである。政府は2020年度までに太陽光発電を2,800万kWにすることを目標にしているが、太陽光発電は電力供給や電力品質の不安定化が想定される。そのため経済産業省では2010年より、NRIセキュアテクノロジーズも参加する「次世代送配電系統最適制御技術実証事業」や「次世代型双方向通信出力制御実証事業」などにより対応を検討している。

一方、米国では老朽化した既存の送配電網の更新や、自動検針、電力使用開始・停止の遠隔操作などを目的としている。欧州の場合は、米国と同様の目的に加え、省エネおよびエネルギー有効活用の観点から、家庭での電力使用量の可視化や家電製品の遠隔制御などが主な目的になっている。

スマートグリッドのセキュリティリスク

従来、電力網のような制御システムは独自仕様の製品で構成され、隔離されたネットワーク上に構築されているため、外部からの攻撃に対しては安全であるといわれてきた。しかし、近年、制御システムにおけるセキュリティ事件は世界的に増加している（表１参照）。その理由として、システムが独自仕様から汎用的な仕様に置き換わったことや、隔離されたネットワークでの運用から、他のネットワークと接続された形態へと移行したことが挙げられる。

スマートグリッドも、汎用的なITの活用や電力会社（系統）と家庭間での相互接続が必須であり、不正アクセスや盗聴などのセキュリティリスクが高まる。

例えば、遠隔制御を逆手に取って、制御情報が流れる通信ネットワークが盗聴され、制御情報が改ざんされて大規模停電が起こされる恐れがある。また、電力使用量の可視化のためにネットワークを通じて収集・蓄積される個人情報が、盗聴や不正侵入によって盗ま

NRIセキュアテクノロジーズ
セキュリティコンサルティング部
主任セキュリティコンサルタント
上田直哉（うえだなおや）

専門は情報セキュリティ全般に関するコンサルティング

NRIセキュアテクノロジーズ
テクニカルコンサルティング部
副主任セキュリティコンサルタント
野口大輔（のぐちだいすけ）

専門はセキュリティ診断、制御システムセキュリティ

表1　制御システムにおけるセキュリティ事件の事例

事故の内容	発生国・発生年	原因	事故の経緯
鉄道の信号システムがウイルスに感染し運行が大幅に遅延	米国 2003年	アクセス制御の不備	感染原因は解明されていないが、2003年に流行したSobig（Sobig自体は現在流行しているZeusやSpyeyeのようにメール添付で感染する）が原因との報道がある。ネットワークの隔離が十分でなかったと推測され、オペレーターの端末が感染した結果、システムが感染したと考えられている。
原子力発電所の制御システムがワームに感染	米国 2003年	アクセス制御の不備	社内のPCがSlammer（Microsoft SQLServerの脆弱（ぜいじゃく）性を突いて感染を広げるワーム）に感染。社内OA系ネットワークと制御系の間のアクセス制御が甘く制御系も感染。
鉄道の切り替え機を不正に操作されあわや列車同士の接触事故という状況に	ポーランド 2008年	アクセス制御の不備	無線LANから侵入。鉄道の切り替え機までの間でアクセス制御がなかった。 14歳の少年によるいたずら目的の犯行。テレビリモコン型のコントローラを作り、切り替え機の制御を奪った。
国内制御系のウイルス被害	日本 2008年～	ウイルスが保存された端末・USBメモリーの持ち込み	自動車工場で、製造ラインに組み込まれているコンピュータ約50台がウイルスに感染。別の自動車工場では設備系コンピュータ約10台が感染。石油化学プラントではウイルス感染でシステムが完全に使えなくなり一時操業停止に追い込まれた。

れることも考えられる。

これらは、制御システムや情報システムが直面しているセキュリティリスクと同じである。重要インフラとして位置付けられる電力網は、サイバーテロの標的ともなり得ることから、スマートグリッドのセキュリティ対策は最重要課題である。そこで、スマートグリッドの取り組みが進んでいる欧米のセキュリティ対策を見ることによって、日本のスマートグリッドに適用すべきセキュリティ対策について考えてみたい。

米国のスマートグリッドセキュリティ

米国では、エネルギー省傘下の連邦エネルギー規制委員会（FERC）の監督下で、国立標準技術研究所（NIST）がスマートグリッドに関するセキュリティガイドラインを整備している。電力各社はこのガイドラインに基づいて必要なセキュリティ対策を実施することになる。

ここでは、筆者らが現地調査に訪れたカリフォルニア州におけるスマートグリッドのセキュリティ対策を紹介する。カリフォルニア州のスマートグリッドに実装されている主なセキュリティ対策は以下の６つである。

①検針ネットワークと制御ネットワークとの分離

スマートメーターとアクセスポイントを結ぶ検針ネットワーク（家庭で消費した電力量情報（検針情報）を送信）から制御ネットワ

ーク（送配電の制御情報を送信する）への不正アクセスを防ぐため、両ネットワークを分離している。

②スマートメーターと宅内環境の非接続

家庭内からの不正アクセスを防ぐため、スマートメーターと家庭内機器は接続されていない。

③プライベートネットワークの利用

検針ネットワーク、制御ネットワークともに、インターネットを代表とする公衆回線を使用していない。制御ネットワークには従来からの電力網を利用し、検針ネットワークは新たにスマートグリッドのために敷設したメッシュネットワーク（端末同士が通信することにより形成される網目状のネットワーク）を利用している。

④通信内容の暗号化

検針ネットワークでは、スマートメーターからアクセスポイントへの無線通信を盗聴される恐れがあるため、通信内容をすべて暗号化している。

⑤通信機器に認証を導入

スマートメーター、アクセスポイントともに信頼できる通信機器間での通信であることを担保するため、機器を認証する仕組みを導入している。認証方法には、データセンター側に設置する認証局サーバーを利用するPKI（公開鍵基盤）方式を採用している。

⑥ネットワークの冗長化

前述のように検針ネットワークはメッシュ形式で接続されており、これは冗長化を考慮したものでもある。このため、アクセスポイントの盗難や、送られるはずの情報が送られてこないなどの異常が発生した場合、その通信機器のみを切り離して別ルートで接続可能となっている。

以上のように、米国では「制御ネットワークに対する不正アクセス」を最大の脅威ととらえ、ネットワークへのセキュリティ対策を重点的に採用している。

欧州のスマートグリッドセキュリティ

欧州のスマートグリッドの特徴は、家庭での電力消費量の可視化を積極的に推進していることである。

筆者らは英国とフランスの２つのスマートグリッドプロジェクトを現地調査した。英国のLCNF（Low Carbon Networks Fund）が補助するUK Power Networks社の「Flexible Plug and Playプロジェクト」と、ERDF（フランス配電会社）が推進する「Linkyプロジェクト」（Linkyはスマートメーターの名称）である。

両プロジェクトはともにスマートメーター導入プロジェクトであり、プライバシー保護を重視したセキュリティ対策を取り入れている点が共通の特徴であった。電力使用量からその家庭のライフスタイルを推測できるため、個人の住所、氏名などの情報と一緒に管理する場合は、電力使用量はプライバシーデータ

として扱われている。

両プロジェクトではともに以下のセキュリティ対策が検討されていた。

①通信の暗号化と通信機器の認証

具体的なセキュリティ対策は米国と同様である。特に「Flexible Plug and Playプロジェクト」では米国カリフォルニア州の事例と全く同じネットワーク構成を採用していた。

②プライバシーデータの暗号化

スマートメーターなどの通信機器にはプライバシーデータが保存されているため、機器が盗難に遭ってデータが漏えいすることを想定して、通信機器上でデータをすべて暗号化している。

以上のように、欧州では「プライバシーデータの漏えい」を大きなリスクととらえ、制御ネットワークへの不正アクセス対策に加えて、データそのものに対するセキュリティ対策を実施している。

日本が取り組むべきセキュリティ対策

日本では、制御ネットワークと家庭間で相互に通信が行われることが想定され、家庭のプライバシーデータ（電力使用量）を活用することも検討されている。そのため、米国で重視されている「制御ネットワークに対する不正アクセス」と、欧州で重視されている「プライバシーデータの漏えい」の両方のリスクを考慮することが求められる。従って、日本では欧米で導入または検討されているセキュリティ対策を併せて取り込んでいく必要がある。

しかし、欧米と同様のセキュリティ対策をそのまま導入すれば安全というわけではない。現地調査の結果では、電力会社のオペレーターなど内部の権限者による不正や過失を防止する対策が不足していると思われた。また、スマートグリッドは情報通信技術が広く活用されることから、一般の情報システムと同様に、採用した製品に脆弱（ぜいじゃく）性が発見される可能性が高い。その場合の対応についても、欧米では十分に考慮されているとはいい難い。

このように、欧米のセキュリティ対策も現時点では不備がある。セキュリティ事故はまさにこのような小さな穴から発生してしまう。日本が安全なスマートグリッドを構築するためには、スマートグリッドを構成する機器と、機器間の通信の１つ１つについて、機能、取り扱う情報、データ保存の有無、利用技術などを明確化し、それぞれに対する個別のセキュリティリスクを洗い出した上で対策を検討していく必要がある。

昨今、情報システムのセキュリティ事故が後を絶たず、事後対応に追われる状況が続いている。事故を未然に防ぐためには、スマートグリッドの計画段階である今、セキュリティ確保に向けて官民が連携して知恵を絞ることが求められている。 ■

クラウドサービスの利用は世界分散へ
―セキュリティ対策の見直しにより利便性を向上―

クラウドコンピューティング（以下、クラウド）は、ITにおける“持たざる経営”の本命施策といわれながらも、セキュリティへの懸念から企業への浸透は緩やかであった。しかし、事業継続計画（BCP）の見直しの動きが進むにつれ、徐々に利用が拡大しつつある。本稿では、企業がクラウドサービスを安心して利用するためのセキュリティサービスの動向を紹介する。

BCPとしてのクラウドの役割

企業は東日本大震災の発生を受けてBCPの策定・見直しを急いでいる。DR（Disaster Recovery：災害などによる致命的な障害からの復旧）サイトの拡充、外部のデータセンターの利用、社内のバックアップ設備の増強などに取り組む企業も増えている。

クラウドの利用をBCPの観点で検討する企業も増えてきた。しかし、クラウドを災害時の業務アプリケーションの稼働場所と考える企業は少数派で、クラウドはデータのバックアップ場所であると考える傾向が強い。

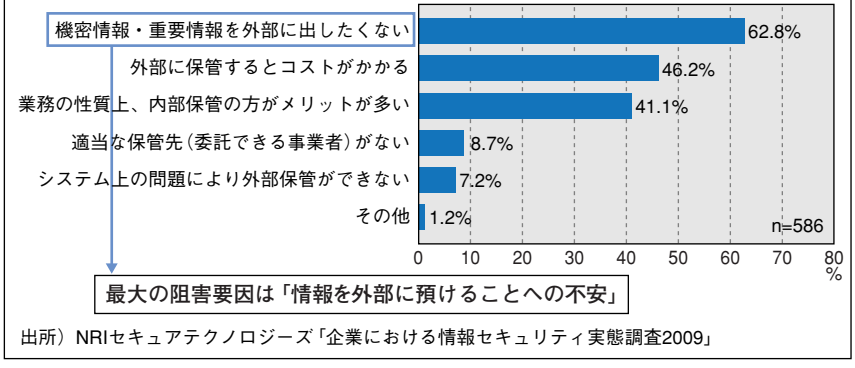
秘密分散技術でデータを安全に保管

2009年にNRIセキュアテクノロジーズが実施した調査で、情報を外部のデータセンターなどに保管しない理由を聞いたところ、「機密情報・重要情報を外部に出したくない」を挙げる企業が62.8％と最も多かった（図１参照）。クラウドの場合も、データを預ける際の安心感、信頼感は重要なポイントである。外部からの攻撃に対処可能か、外部監査が発生した場合にサービスの継続は可能か、クラウド事業者の内部犯行による情報漏えいは防げるのかなどを懸念する情報システムの担当者は多い。

しかし、以下のような発想の転換をすると、上記の懸念はほぼ解消できる。すなわち、機密情報をクラウド上に預けている間は“意味のない情報”にしてしまうのである。クラウド上から情報が盗まれても、元の情報に戻せなければ情報漏えいの恐れはなくなる。このような仕組みが秘密分散技術である。

秘密分散技術では、元のデータに乱数を掛け合わせて撹拌（かくはん）した上で複数の断片に分割する。１つの断片は元のデータの

図１　企業が情報を外部保管しない理由



出所）NRIセキュアテクノロジーズ「企業における情報セキュリティ実態調査2009」

野村総合研究所
NRIセキュアテクノロジーズ
SecretShare事業部
上級コンサルタント
森本伊知郎（もりもといちろう）
専門は事業戦略、サービス企画、アライアンス支援など

一部しか保持していないため、その断片からは情報の一部さえ類推できない。復元のためには断片を集める必要があり、この点が暗号化との大きな違いである。

データの断片を異なるクラウドサービスに分けて預ければ、第三者が複数の断片を集めることは困難である。仮に事業者の内部の人間が自社に置かれた断片を持ち出しても情報を復元できない。データを断片化する際にそれぞれ冗長データを付加しておき、一部のクラウドサービスが停止して断片がすべて集まらなくても、残りの断片から情報を復元できるようにする方法もある。

秘密分散技術の適用シーン

NRIセキュアテクノロジーズは、秘密分散技術を取り入れたクラウドサービス「Secure Cube / Secret Share」を提供している。ユーザーは、クラウドに預けたい情報を所定のフォルダーに入れるだけで、自動的に秘密分散に係る一連の処理がなされる。元の情報は分割され、3カ所または4カ所のクラウド事業者に預けられる。

このサービスは、もともと社外持ち出し用のノートPCを対象としたものであった。外出前に、必要なファイルを所定のフォルダーに入れてクラウドに預けておき、外出先でPCをネットワークに接続してファイルを復元する。ファイルの実体はPCの中には残らないため、PCが盗難に遭っても情報漏えいの心配がない。この機能を応用すれば、所定のフォルダーを共有設定しておき、社内のファイルサーバーとして利用することもできる。アクセス権も通常のファイルサーバーと同様に設定できる。ユーザーは、あたかも数TB（テラバイト）といった巨大なストレージ（外部記憶装置）を持つファイルサーバーにアクセスする感覚で、安全にクラウドサービスを利用することができる。

バックアップとしての用途にも対応している。バックアップを取りたいデータを所定のフォルダーに入れるだけでクラウド上に分散保管でき、ファイルサーバーと同様に巨大なストレージやメディアは不要となる。既存のバックアップツールの多くがそのまま利用できるというメリットもある。

企業間取引の安全なデータ交換に利用することもできる。取引先にデータ断片へのアクセス権を与えるだけで情報共有が可能になるためである。

データの世界的な分散保管も可能に

NRIセキュアテクノロジーズは、2011年11月に日本マイクロソフトと安全なクラウドサービスの提供に向けた協業に合意し、「世界分散ストレージサービス」の提供を始めた。これは、Microsoft社が提供するクラウドサービス「Windows Azure」を利用して、欧米・アジアの6カ所にデータの断片を保管するものである。■

震災を契機に浮上した事業継続の課題と対策
―電力不足が招く情報システム停止への対応―

東日本大震災を契機に、事業継続の実効性を高めるための事業継続計画（BCP）の見直しを進めている企業が多い。見直しの内容には、これから夏場を迎えるに当たって心配される電力供給不足への対応も含まれる。本稿では、BCP見直しのポイントを紹介するとともに、電力不足のリスクに対する事業継続の課題と対策について考察する。

企業が進めるBCPの見直し

東日本大震災以前にBCPを策定している企業は多かったが、震災後、“想定外”があったことと、“想定外”が起きた時の対応の仕組みがなかったことに対する反省が聞かれた。それらの企業では今、BCPの見直しを進めている。見直しのポイントは主に２つある。

(1) シナリオベースのBCPの改良

多くの企業が策定しているBCPは、特定の災害と被害の発生を想定したシナリオに基づくBCPである。

シナリオベースのBCPでは、実際の災害状況が想定シナリオと類似する場合は有効であるが、東日本大震災は被害規模が想定を超えて大きく、原子力発電所の事故のような“想定外”の事態も起きた。さらに計画停電によって情報通信手段の制限、鉄道の運行制限、業務の中断などが同時多発的に発生し、臨機応変な対応が求められた。

あらゆる事態を想定したシナリオを用意して“想定外”をなくすことは理論上は可能だが、現実的な対応とはいえない。そこで、BCPの再検討に当たっては“想定外”の要素には複数のシナリオベースのBCPを組み合わせて対応するというアプローチが有効である。具体的には、個々のシナリオの内容やシナリオの組み合わせパターン、意思決定のプロセスや判断基準などが検討のポイントとなる。

(2) 情報システムの復旧に依存しない事業継続

これまでのBCPでは、情報システムが比較的短期間で復旧することを前提にしていることが多かったが、その前提を見直す動きもある。データを完全二重化する遠隔地のバックアップシステムを用意している場合を除き、情報システムを復旧させるためには大まかに以下の手順を踏む必要があり、これには月単位の復旧期間を要する場合がある。

①情報システムが設置されている建物の安全確認
②電力・通信の復旧確認
③ハードウェアの修理・調達
④バックアップからのデータの復旧
⑤システム動作テスト

東日本大震災に際して、東北地方に設置された基幹系システムの完全復旧に数カ月を要したため、サプライチェーン上にある全国の拠点の業務に支障をきたして事業継続が妨げられた企業があった。一方で、情報システムの復旧を待たず、暫定的なシステムをクラウ

野村総合研究所
システムコンサルティング事業本部
金融ITコンサルティング部
主任システムコンサルタント
石原　武（いしはらたけし）
専門はITガバナンスに関する戦略立案・実行支援など

ドサービスを利用して短期間で構築し、迅速に業務を復旧させた企業もあった。

BCPの見直しに当たっては、まず情報システムの復旧にどれだけの時間がかかり、それが業務にどのような影響を与えるかを明らかにする。その上で、優先業務については、手作業や暫定システム構築など、情報システム復旧までの一時的な業務継続方法について検討する必要がある。

新たなリスクとしての電力不足

今、新たな事業継続上のリスクとして電力不足の問題が浮上している。2012年３月現在、定期点検中の原子力発電所は再稼働のめどが立っていない。日本エネルギー経済研究所の分析によると、仮にすべての原子力発電所の再稼働がない場合、長期停止火力発電所を除く電気事業者の総発電能力が需要を7.8％下回り、全国規模で電力不足になるという。そのため、需給調整契約を結んでいる工場などの大口需要家（契約電力500kw以上）は、需給が逼迫（ひっぱく）した場合に電力の供給制限を受ける可能性がある。企業は電力不足によるシステムの停止など事業継続面での影響について評価・点検を急ぐ必要がある。

電力不足に備えるBCPのポイント

電力不足は企業が単独で対応することが難しい課題ではあるが、計画停電、需給調整契約に基づく大口需要家への供給制限、政府からの節電要請、突発的な大規模停電の発生などを想定したBCPを策定する必要がある。その際、以下の項目を含め検討することが重要と考える。

①省エネ型データセンターの利用

情報システムを稼働させるために必要な電力の半分程度は、機器を冷却するための空調設備である。最新の省エネ型の空調設備を持ち、さらに自家発電装置を備えて燃料供給者との優先供給契約を結んでいるデータセンターは、計画停電が実施された場合も情報システムの連続稼働が可能である。このような最新鋭の設備を持つデータセンターを選ぶことによって、電力不足によるシステム停止というリスクは大幅に低減することができる。

②クラウドサービスの利用

クラウドサービスを利用して情報システムを分散配置すれば、局所的な電力不安に対する影響を小さくでき、代替システムの構築も短期間で行うことができる。

③リモート運用環境の導入

交通機関の停止などで情報システムの運用要員を確保できない場合も、遠隔監視・運用ができる仕組みがあれば業務を継続できる。

野村総合研究所（NRI）は、データセンターサービス、クラウドサービス、システム運営のコンサルティングやサービスの提供などを通じて、BCPの実効性を高める企業の取り組みを支援していく。 ■

米国におけるネット専業銀行の栄枯盛衰
―インターネットバンキング事業の成功要件とは―

米国で1990年代半ばに登場したネット専業銀行は、店舗網を持たない強みを生かした高金利預金で急拡大するとの見方があったが、大部分は行き詰まるか小規模にとどまるかの状態である。一方で、インターネットバンキングは伝統的銀行に欠かせないチャネルとして成長し続けている。本稿では、米国のネット専業銀行とインターネットバンキングの動向を紹介する。

成長が期待された米国のネット専業銀行

米国のネット専業銀行のさきがけは1995年に設立されたSecurity First Network Bank（SFNB）社である。同年には、Amazon.com社やeBay社など、今日の代表的なネット企業が相次いでネットショッピングなどのサービスを開始し、インターネット接続サービスのAOL社などが巨額の広告宣伝費を投入して利用者の拡大を図っていた。

ネット専業銀行の強みは、店舗網を持たず営業人員も少ないため低コストで運営ができ、高い預金金利や低い手数料を提供できることにあるとされた。SFNB社が社名を「安全第一」としたように、セキュリティ上の懸念さえ解消されれば、爆発的に増えるインターネット利用者の多くが伝統的銀行からネット専業銀行に預金をシフトさせるとの見方もあった。

こうした見方を背景にネット専業銀行の新規参入が相次いだほか、大手銀行や地方銀行でも別ブランドでネット専業銀行を立ち上げるところが出てきた。

1980～1990年代にかけて数百件もの買収で成長したBank One社は、1999年にネット専業銀行の別ブランドWingspan Bankを立ち上げ、2000年にはオランダを本拠とする金融サービスグループのING社が、ネット専業銀行のING Directとしては８カ国目となる米国でING Direct USAを設立した。同社は2010年までには800億ドルを超える預金を集め、米国のネット専業銀行最大手の地位を確立した。

節目を迎えたネット専業銀行

しかし米国銀行市場全体を見れば、一部の関係者が当初、期待したような伝統的銀行からの大規模な預金のシフトは起きなかった。図１に示すとおり、2011年６月末時点の米国の銀行の預金残高に占めるネット専業銀行の預金の比率は２％に届いていない。この数字は、直近の５年間でもほとんど変わらない。

それとともにネット専業銀行の撤退も相次いだ。SFNB社は銀行事業から撤退する一方、子会社のSecurity First Technologies社は社名をS1と変えて銀行・決済業者向けITベンダーとなった。

Bank One社が立ち上げたWingspan Bankは、高い預金金利の設定と１億6,000万ドルという巨額の広告宣伝費の投入にもかかわらず、設立からわずか２年後の2001年に撤退し、ネット預金口座は伝統的銀行事業チャネルに統

NRIアメリカ
金融サービス調査部門長
吉永高士（よしながたかし）

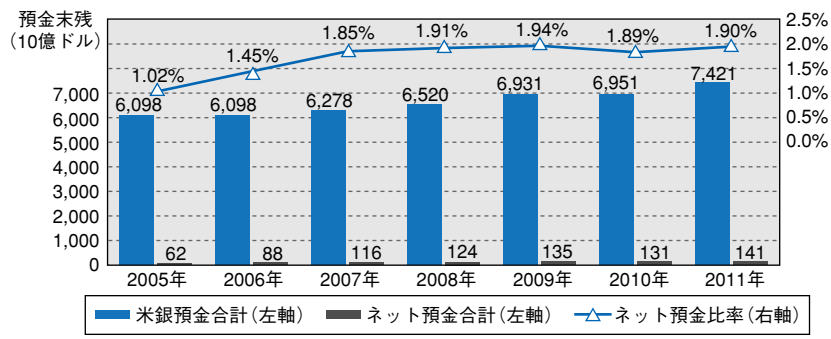
専門は米銀と米国証券会社の経営戦略・戦術、オペレーション、制度問題

合された。

ING Direct USA社も、2011年に大手クレジットカード・銀行兼営のCapital One社への売却を決定した。

ING Direct USA社は高い金利設定と巨額の広告宣伝費により、ROE（自己資本利益率）は創業以来一貫して米国の銀行全体の平均を10ポイント程度下回り続けていた。また預貸率（預金残高に対する貸出残高の比率）も平均の約半分の40%前後で推移するなかで、拡大に走った債券投資で巨額損失を計上した。同社が豊富な貸付機会を持つCapital One社へ売却されたのは、運用難というネット専業銀行の本質的な限界を示したものといえる。

図1　米国の銀行における預金残高・ネット預金残高とネット預金比率の推移



※ネット預金：ネット専業銀行（店舗網を持つ伝統的銀行のネット専業部門を含む）の預金
※2011年のデータは6月末時点
出所）SNL Financial、FDIC（連邦預金保険公社）などの資料に基づきNRIアメリカ作成

存在感を増すマルチチャネルとしてのインターネットバンキング

米国でネット専業銀行が期待された成果を上げられない最大の要因は、大多数の米国民が高金利に飛び付かなかったことである。その一方で、伝統的銀行が提供するインターネットバンキングは順調に伸びている。

Bank of America社が2011年に実施した顧客調査では、「最も頻繁に利用したいチャネル」としてインターネットを挙げた人が46%と最多だった。「最も存在を重視するチャネル」として店舗を選んだ顧客は61%と大多数を占め、インターネットと電話がそれに続いた。大部分の米国民にとって、店舗網があることによる利便性は、いまだに高金利には替え難いことを示唆している。

ネット専業銀行の預金者数がここ数年、ほぼ横ばいであるのに対し、大手銀行や地方銀行ではそれぞれ500万～4,000万人規模の個人顧客の約9割が日常的にインターネットバンキングを利用し、利用者数も年3～5%のペースで増えている。過去四半世紀だけを見ても金利設定条件のあやで業態間での大幅な預貯金シフトを何度も経験している日本に、米国での教訓がそのまま当てはまるわけではない。しかし、こと米国のインターネットバンキングに関する限り、利用者数でも利用件数でも、地方銀行などを含む伝統的銀行のマルチチャネルモデルにおける不可欠な構成要素として存在感を発揮し続けるとの見方が、今なお支配的である。 ■

NRI Web Site

NRI公式ホームページ　www.nri.co.jp

会社情報

NRIグループのCSR活動	www.nri.co.jp/csr	IR情報	www.nri.co.jp/ir

事業・ソリューション別のポータルサイト

コンサルティング	www.nri.co.jp/products/consulting	日本における先駆者として社会や産業、企業の発展に貢献してきたコンサルティングサービスを紹介
未来創発センター	www.nri.co.jp/souhatsu	アジア・日本の新しい成長戦略に関わるNRIの取り組み、研究成果の情報発信、政策提言などを紹介
金融ITソリューション	www.nri.co.jp/products/kinyu	金融・資本市場でのビジネスを戦略的にサポートするITソリューションの実績、ビジョンを紹介
NRI Financial Solution	fis.nri.co.jp	金融・資本市場に関わるNRIの取り組みについての情報発信、政策提言、ITソリューションを紹介
産業ITソリューション	www.nri.co.jp/products/sangyo	流通業やサービス業、製造業などさまざまな産業分野のお客様に提供するソリューションを紹介
IT基盤サービス	www.nri.co.jp/products/kiban	産業分野や社会インフラを支えるシステム、システムを安全・確実に運用するためのソリューションを紹介
情報技術本部	www.nri-aitd.com	先端的な基盤技術への挑戦と知的資産創造、技術をベースにした新事業の創造の実践を紹介
BizMart	www.bizmart.jp	企業間業務や生・配・販を中心とするさまざまな業種の業務効率化を支援するソリューションを紹介
GranArch	granarch.nri.co.jp/main.html	システムインテグレーション事業において培った基盤構築のノウハウを結集させたソリューション群を紹介

サービス・ソリューション別のWebサイト

INSIGHT SIGNAL	www.is.nri.co.jp	マーケティング戦略の効果を科学的に“見える化”し、効果を最大化することを目的とした総合支援サービス
TrueNavi	truenavi.net	コンサルティング業務を通じて独自に開発したインターネットリサーチサービス
TRUE TELLER	www.trueteller.net	コールセンターからマーケティング部門までさまざまなビジネスシーンで活用可能なテキストマイニングツール
未来型携帯ナビ　全力案内!	www.z-an.com	独自に生成する道路交通情報を活用した携帯電話・スマートフォン総合ナビゲーションサービス
てぷらぱ	teplapa.nri.co.jp	テスト工程の効率化を実現するテスト自動実行支援ツール
OpenStandia	openstandia.jp	オープンソースソフトウェアにより高品質な業務システムを構築するワンストップサービス
Senju Family	senjufamily.nri.co.jp	ITサービスの品質向上とコスト最適化を実現するシステム運用管理ソフトウェア

グループ企業・関連団体のWebサイト

NRIネットコム	www.nri-net.com	インターネットシステムの企画・開発・設計・運用などのソリューションを提供
NRIセキュアテクノロジーズ	www.nri-secure.co.jp	情報セキュリティに関するコンサルティング、ソリューション導入、教育、運用などのワンストップサービスを提供
NRIサイバーパテント	www.patent.ne.jp	「NRIサイバーパテントデスク」など、特許の取得・活用のためのソリューションを提供
NRIデータiテック	www.n-itech.com	IT基盤の設計・構築・展開と稼働後のきめ細かな維持・管理サービスを提供
NRI社会情報システム	www.nri-social.co.jp	全国のシルバー人材センターの事業を支援する総合情報処理システム「エイジレス80」を提供
NRIシステムテクノ	www.ajitec.co.jp	味の素グループに情報システムの企画・開発・運用サービスを提供
野村マネジメント・スクール	www.nsam.or.jp	日本の経済社会の健全な発展および国民生活の向上のために重要な経営幹部の育成を支援する各種講座を開催

海外拠点のWebサイト

NRIアメリカ	www.nri.com	野村総合研究所(香港)有限公司	www.nrihk.com
野村総合研究所(北京)有限公司	www.nri.com.cn/beijing	NRIアジア・パシフィック	www.nrisg.com
上海支店	shanghai.nri.com.cn	NRIソウル支店	www.nri-seoul.co.kr
野村総合研究所(上海)有限公司	consulting.nri.com.cn	NRI台北支店	www.nri.com.tw

『ITソリューション フロンティア』について

本誌の各論文およびバックナンバーはNRI公式ホームページで閲覧できます。
本誌に関するご意見、ご要望などは、it-solution@nri.co.jp宛てにお送りください。

ITソリューションフロンティア

2012年 6 月号　Vol.29 No.6（通巻342号）
2012年 5 月20日　発行

発行人　嶋本　正
発行所　株式会社 野村総合研究所　コーポレートコミュニケーション部
〒100−0005　東京都千代田区丸の内1−6−5　丸の内北口ビル
ホームページ　www.nri.co.jp

発　送　NRIワークプレイスサービス株式会社 ビジネスサービスグループ
〒240−0005　横浜市保土ケ谷区神戸町134
電話（045）336−7331／直通　　Fax.（045）336−1408