NPO ISEF
Not-for-Profit Organization of Information Security Forum

特定非営利活動法人
NPO情報セキュリティフォーラム

NPO-ISEF 情報セキュリティレポート：2011-No.02

韓国におけるサイバー侵害事故の動向と対策

株式会社イグルーセキュリティ日本支社
支社長　崔 正濬（Choi Jongjun）

【著者経歴】
1988年サムスングループ入社、日本駐在員。2002年、韓国のセキュリティベンダーの日本法人の取締役として再来日、以来韓国のオンラインゲーム会社日本法人のCEOを経て、現在、『統合セキュリティ・マネージメント・システム』（ESM：Enterprise　Security　Management）ソリューションでは韓国トップを誇る株式会社イグルーセキュリティ（IGLOO SECURITY Inc.)の日本支社長を務める。

1．韓国における情報セキュリティ

韓国は世界唯一の分断国家である。韓国と北朝鮮の対立状況は、国際法的に停戦状態であって終戦しているわけではない。このような背景のためなのか、韓国におけるセキュリティ問題は社会的にも敏感にならざるを得ない。

2012 年、韓国政府機関・市・道等の 294 機関の情報化事業の状況を調べてみると、計 5,012 件の事業があり、その規模は計 3 兆 6,158 億ウォン（約 2,676 億円）にも達している。そのうち、13.1%に当たる 1,055 件の事業は「安全な情報社会の実現」という予算に含まれている。

韓国の情報保護関連予算は、2010 年 2,384 億ウォン（約 176 億円）から 2012 年 2,837 億ウォン（約 210 億円）へと毎年増えている。これは 1)サイバー脅威への対応システム構築、2)個人情報漏えいへの対応システム構築など、情報保護に関連する事業の社会的必要性が益々高まっていることの表れなのである。

情報セキュリティは、韓国における 2012 年のホットトレンドキーワードである。その理由としては同年に行われる総選挙や大統領選挙、さらに個人情報保護法の本格的施行などの大きな案件が相次いでおり、それに伴うサイバー侵害事故の潜在的発生の危険性が高まっているからである。
今後、1)選挙関連サイバーテロ　2)DDoS※1 攻撃　3)個人情報関連の事故が浮上すると予測される。実例として、2011 年 KISA(韓国インターネット振興院)の DDoS 避難所を利用した企業がおよそ 133 社を超えており、被害は 53 件にものぼる。

2．韓国における最近のサイバー侵害事故

最近韓国内で話題になったサイバー侵害事故としては、3.4DDoS 攻撃、農協金融システムへの攻撃、現代キャピタルの 42 万人の個人情報漏えい事件、APT(Advance Persistent Threat)攻撃の増加などがある。

■ 3.4DDoS 攻撃

韓国では 2009 年 7 月 7 日(7.7DDoS)と 2011 年 3 月 4 日(3.4DDoS)に DDoS 攻撃が大規模に発生し、国全体のインターネットサービスが被害を受け、社会的混乱を引き起こした。また、2011 年にはソウル市長の選挙で有力候補のホームページが攻撃されるという事件もあった。

7.7DDoS と 3.4DDoS ともに大量の個人ユーザーの PC が DDoS 攻撃者として操られたが、個人ユーザーの PC を操るためのウイルスを配布するためにウェブハードサイト※2が悪用された。ウイルスに感染した個人ユーザーの PC（ゾンビ PC※3）は、外部サーバーからの命令を受けて攻撃を実施し、攻撃対象も似ていた。そして、いずれも最終的にゾンビ PC の HDD を破壊するために不正コードを実行させた上で攻撃が終了するものであった。 しかし、3.4DDoS は 7.7DDoS より攻撃の手口が巧妙かつ悪質になっていた。例えば、ゾンビ PC の OS が、すべての WindowsOS を対象として拡大され、攻撃のたびにファイルの構成が違っており、ホストファイルを改ざんして、アンチウイルスソフトのアップデートを妨害し、治療を妨げた。また、攻撃のシナリオを状況に応じて変えて流動的に攻撃をした。

＜7.7DDoS 攻撃と 3.4DDoS 攻撃の比較＞

区分	2009 年　7.7 DDoS	2011 年　3.4 DDoS
攻撃対象	青瓦台（大統領官邸）及び国内主要サイト、米国の主要　サイト	青瓦台（大統領官邸）及び国内主要サイト、駐韓米軍の主要サイト
対象 OS	Windows 2000,XP,2003	すべての Windows OS
ファイル構成	同じファイル構成で攻撃	攻撃するたびに変更されたファイル構成で攻撃
命令変更	一貫された命令	対応状況に応じて命令を変更
治療妨害	なし	ホストファイルの改ざんでアンチウイルスのアップデートを妨害
ゾンビ PC 数	115,044 台	116,299 台
HDD 破壊	システムの日付を変更することで防止可能、7 月 10 日 24 時破壊開始	システムの日付の変更や感染時刻の記録ファイルを削除する場合にもディスクの破壊を実行 感染 4 日後に計画されていたが 5 日 21 時以降、すぐに破壊することに変更

※1　DoSは、Denial of Servicesの略。インターネット経由での攻撃の一つで、大量のデータや不正なデータを送りつけることにより相手のコンピュータやルータなどを使用不能に陥らせたり、ネットワークを流れるデータの量を増大させて相手のネットワーを麻痺させる攻撃。DDoSは、分散DoS攻撃とも呼ばれ、攻撃を行うコンピュータがネットワーク上に分散している攻撃を特に指す言葉である。

※2　ウェブハードとは、インターネット上でファイルの保存場所を貸すサービスのこと。オンラインストレージサービス。

■ 農協金融システムへの攻撃

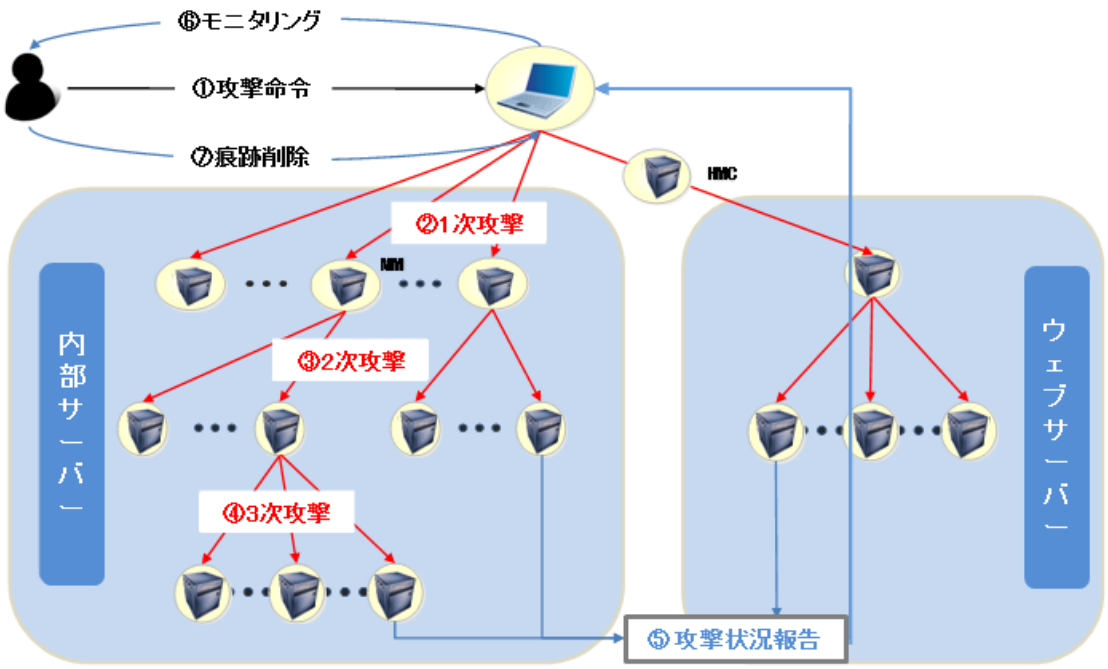
金融システムへの攻撃としては、2011 年４月に起きた農協(銀行)事件で、金融ネットワーク史上初の麻痺事態が発生した。農協の金融システムの攻撃に使用されたハッキングは、農協に出入りする協力会社社員のノートパソコンをまず最初にハッキングし、その後攻撃プログラムを内部で実行するという手口であった。

この事件を契機に、外部からの攻撃に対するサイバー侵害事故の対応はさることながら、内部の従業員や協力会社による事故の発生に対しても十分な備えが必要だということが立証された。

〈農協事件日誌〉

日付	内容
2011 年４月 12 日	最初の障害及び金融ネットワークの中断現象発生
2011 年４月 13 日	銀行窓口の入出金業務一部再開
2011 年４月 14 日	ATM 機やインターネットバンキングサービスの再開
2011 年４月 18 日	金融監督院の調査開始
2011 年４月 19 日	ハッキングシナリオの分析
2011 年４月 30 日	クレジットカードサービスの完全復旧
2011 年５月３日	検察から公式捜査結果の発表

〈農協侵害事故の攻撃シナリオ〉



※３　ゾンビPCとは、ウイルスに感染したり、攻撃者に遠隔操作ソフトを仕掛けられたまま、利用者がそのことに気付かずに放置されているパソコンをさす。この事例では、ウェブハードの利用者のPCがボットと呼ばれるウイルスに感染させられ、これにより攻撃者からの遠隔操作が可能となり、DDoS攻撃を行うPCとして悪用された。

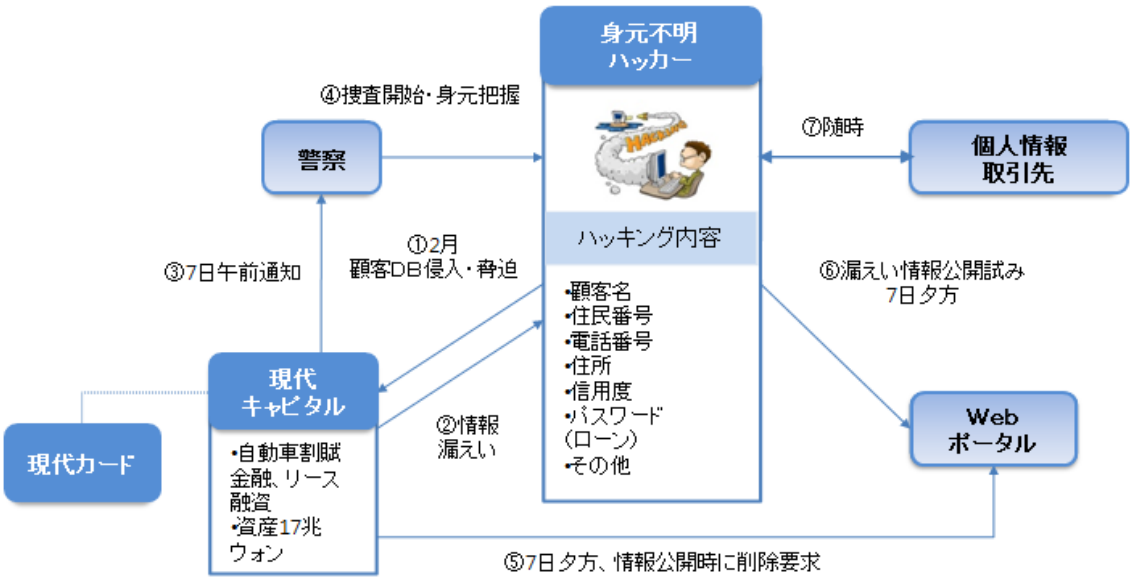
■ 現代キャピタルの個人情報漏えい事件

個人情報漏えい事件としては、2011 年４月にハッカーたちが金銭を目的とし、国内最大手の消費者金融業者である現代キャピタルの DB をハッキングして脅迫メールを送信した事件がある。この時に流出された個人情報件数は 42 万件にものぼる。

〈現代キャピタル事件日誌〉

日付	内容
2011 年２月	ホームページ関連のハッキングの試み
2011 年４月７日午前	ハッキング脅迫メール受信
2011 年４月７日午前	１次ハッキング被害規模の把握 犯罪の追跡に必要なお金を振込
2011 年４月７日午後	警察が犯罪の場所を急襲、不発に終わる
2011 年４月９日午前	ジョン・テヨン社長緊急帰国 犯罪に使われた追加 IP 確認
2011 年４月９日午後	追加ハッキング被害内容確認
2011 年４月 10 日午前	緊急記者懇談会

〈現代キャピタル侵害事故の攻撃シナリオ〉



〈現代キャピタル侵害事故の内容〉

項目	内容
攻撃者	身元不明のプロのハッカーがフィリピンとブラジルにあるサーバーを利用して侵入
攻撃対象	現代キャピタルのプライムローンサイト、自動車金融リース情報管理サーバー
被害状況	42 万人の名前、住民番号、ローン商品のパスワード
攻撃方法	ウェブハッキング(ウェブページの脆弱性を分析、その後、ログファイルを利用して非公開ページに侵入)

■ APT 攻撃の増加

さらに、最近は APT(Advance Persistent Threat)という攻撃が問題とされているが、APT 攻撃とは、個人ハッカーによる攻撃ではなく、政府や特定機関の重要情報を取得、または政治的な意図で持続的に戦略的攻撃を多様なハッキング方式でハッキングを試みることをいう。

先に述べた農協の金融システム侵害事故も APT 攻撃の一例と言える。全世界的にこの APT 攻撃の被害が増えつつある。そのうち、いくつか代表的な事件を以下にあげる。

1）2011 年にエクソンモービル、BP などのグローバルエネルギー会社の 5 社がシステム侵害の被害を受けた。APT の攻撃により、ガスと石油分野の生産システム、石油探査に関連した財政ドキュメント、石油及びガスのリース契約、産業制御システムなどの情報が漏えいした事件である。
2）2011 年 3 月、アメリカセキュリティ会社の RSA の情報セキュリティ事業部がハッキングされ、OTP（ワンタイムパスワード）製品の機密情報が漏えいした事件である。個人情報やドキュメントの漏えいはなかったものの、OTP 製品の ID 情報が漏えいしたため、OTP 製品の信頼性が問われ、また第 2 次被害が憂慮されている状況であった。
OTP（ワンタイムパスワード）とは、金融システムやインターネットバンキングの利用の際、ユーザー認証のためのパスワードの生成システムで、「使い捨てパスワード」とも呼ばれる。韓国でもサムスン証券などが RSA の OTP 製品を採用していたため、すべてのお客様の OTP デバイス（ワンタイムパスワード生成器）を全面交換する羽目になった。
3）2011 年 4 月のアメリカのエネルギー省傘下の国立オークリッジ研究所の侵害事件があり、重要技術データのうち、約 1GB の規模が漏えいした。
4）2011 年 7 月に韓国のネイトというポータルサイトで 3500 万人の ID、パスワード、名前、住民番号、連絡先などの情報が漏えいした。

これらのサイバー侵害事故を通して察知できることは、ハッキング攻撃ツールによる攻撃ではなく、攻撃対象の企業を自由に出入りする従業員や協力会社の PC を優先的に支配した後、長期間にかけて攻撃対象の企業に侵入していく戦略的な攻撃が流行っているということである。

3．国での対応策

次第に知能化されつつあるサイバー侵害事故に対応するために、韓国では法律の改善を図っている。例えば 1）個人情報保護法の施行　2）セキュリティ監視専門会社の指定　3）ゾンビ PC 防止法の立法化の推進などである。

■ 個人情報保護法の施行

個人情報保護法は、1991 年 5 月国務総理大臣令で設けられた〝電算処理される個人情報保護のための管理指針〟を補完強化したもので、国家機関、地方自治団体、公共団体等が保有している個人情報を本来の目的以外に利用又は提供できないようにするために設けられた法律である。
違反した場合、3 年以下の懲役又は 1,000 万ウォン（約 74 万円）以下の罰金の処罰を受ける。同時に、個人情報を提供された側も 2 年以下の懲役又は 700 万ウォン（約 52 万円）以下の罰金の処罰を受ける。

■ セキュリティ監視専門会社の指定

セキュリティ監視専門会社の指定とは、政府への DDoS などの新種/亜種のハッキング攻撃から国の重要情報を保護するために、公共機関のセキュリティ監視センターを専門的に運営する会社を指定するというものである。条件としては　1)人材(15 名以上)、2)財政(資本金 20 億ウォン（約 1.5 億円）以上)、3)監視経験(3 年間で 30 億ウォン（約 2.2 億円）以上の監視プロジェクト実行)などに制限されており、1)プロジェクトの実績　2)専門性　3)信頼度を点数で評価して 70 点/100 点以上の評価を受けた企業を「セキュリティ監視専門会社」として指定した。

これにより、政府の基幹システムや公共機関の専門的かつ体系的セキュリティ監視が可能となり、2012 年までに約 2,000 億ウォン（約 148 億円）規模のサービス市場と 1,200 人以上の雇用創出が展望されている。

■ ゾンビ PC 防止法の立法化

ゾンビ PC 防止法は、現在立法化を推進中の法案である。この法案は、たとえサーバー側の情報セキュリティの強化と監視サービスを実行したとしても、感染した PC の利用者が多くなってしまうと、潜在的な危険性が大きくなるため、個人 PC のセキュリティ製品のインストールを推奨するための法案であるが、個人のプライバシー侵害に当たる可能性があり、現在国会で協議が行われている最中である。

4．企業・個人での対策

政府の法的制度の改善に加え、韓国の一般的な企業や金融機関では、2012 年から主なサイバー侵害事故の原因となる内部の問題を根幹から防ぐために内部情報システムのセキュリティ監視センターの構築を本格的に開始する見込みである。

つまり、多様なサイバー侵害事故を防ぐためには、政府のサポートや法律化以外に、さらに企業や個人のセキュリティへの対応と管理システムの構築が必要であり、組織では、体系的なセキュリティポリシーの策定が切実に求められていると言えよう。

ただ単に、セキュリティソリューションの導入だけですべての侵害が防げるというわけではない。1)セキュリティ担当者による内部管理、2)従業員のセキュリティ教育、3)協力会社や外部入出者の物理的管理、4)中央集中管理と監視による情報の統合分析　5)セキュリティポリシーの樹立などが必要である。

政策的なアプローチによる組織の情報セキュリティシステムの強化が強く求められているだけに、韓国においても様々な方法論でセキュリティシステムを構築するためのコンサルティングサービスが、優秀な監視サービス会社によってお客様に提供されている。

5．今、求められるアジア諸国での連携・協力

最後に、ますます組織的かつグローバル化されているサイバー攻撃組織への対応のためには、アジア諸国とのサイバー侵害事故の情報交換や攻撃の予防と対応のための協力が必要不可欠であることを伝えたい。

これまで情報セキュリティは、あらゆる面でアメリカをはじめ欧米がリードしてきたことは否定できない。しかし、今後、韓国と日本さらにはアジアの各国は、欧米とは文化は勿論、ＩＴインフラも異なる状況下においてそれに相応する共同対応体制を設ける必要がある。

このために、韓国の KISIA（知識情報セキュリティ産業協会）は日本の JNSA と JASA との共同シンポジウムを開催するなど、両国間の交流協力を始め、台湾、シンガポール、マレーシア、フィリピンなどのアジア情報セキュリティ協会間の協力ネットワークの構築のために、積極的に取り組んできた。

＜KISIA の MOU（了解覚書）締結状況＞

期間	締結機関	国
2010 年	JNSA & JASA	日本
	CSM	マレーシア
2011 年	VNISA	ベトナム
	TISA	タイ
	ITAP	フィリピン
	MASTEL	インドネシア
	ISPA	マレーシア
	DCG	アラブ首長国連邦
2012 年	CISA	台湾
	SITF	シンガポール

このような努力を無駄にしないためにも、アジアの情報セキュリティ産業をリードしている韓国と日本が、今後アジア全体の安全なサイバー世界の構築のために手を取り合って先導していかなければならないと確信している。

2012年3月28日発行

特定非営利活動法人　NPO情報セキュリティフォーラム
〒221-0835
神奈川県横浜市神奈川区鶴屋町2-17　相鉄岩崎学園ビル
TEL(045)311-8777　　FAX(045)311-8747
E-Mail: isef@isef.or.jp　　URL: http://www.isef.or.jp