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.05

サイバー攻撃の検知と分析

株式会社サイバーディフェンス研究所　情報分析部
部長／上級分析官　名和 利男（Nawa Toshio）

【著者経歴】

航空自衛隊において信務暗号・通信業務／在日米空軍との連絡調整業務／防空指揮システム等のセキュリティ担当（プログラム幹部）業務に従事。 その後、JPCERT/CC 早期警戒グループのリーダを経て、サイバーディフェンスに参加。 専門分野であるインシデントハンドリングの経験と実績を活かして CSIRT 構築及びサイバー演習の支援サービスを提供している。最近はサイバー攻撃のメカニズムの解明に力を入れている。デジタル・フォレンジック研究会 理事。

東日本大震災に乗じた標的型攻撃メール攻撃

1. 概要

2011 年 3 月 11 日、東北地方太平洋沖地震とそれに伴って発生した津波による大規模地震災害が発生した。そして、それを引き金とした東京電力福島第一原子力発電所の事故により、大量の放射性物質の漏洩を伴う重大な電子力事故に発展してしまった。これは、国内外で大きく報道され、特に、放射性物質の拡散に対する関心と不安が増大していった。

その直後、日本国内において、放射性物質に対する関心を寄せる「人の心理」を巧みに利用した標的型攻撃メール攻撃が発生した。特に、重要な情報を保有していると思われる人物或いはそのコミュニティをターゲットとし、かつ、その攻撃手法が巧妙かつ悪質なものがいくつか確認された。

同年 3 月、サイバーディフェンス研究所（CDI）が、特定のコミュニティに対して送付された「東日本大震災に乗じた標的型攻撃メール」を入手して分析を行ない、その結果を必要と思われる国内外の対応機関に情報提供を行った。

同年 9 月、独立行政法人 情報処理推進機構（IPA）が、全く同じ標的型攻撃メールに関する分析・調査報告の発表を行った。

> IPA 「東日本大震災に乗じた標的型攻撃メールによるサイバー攻撃の分析・調査報告書」の公開
> http://www.ipa.go.jp/about/press/20110929_2.html

本報告では、同年 4 月に行った分析結果に加え、この標的型攻撃メールを受信した方々へのヒアリングや多角的な観点での分析を行った結果を説明する。

2. 入手した標的型攻撃メール

2011 年３月 31 日、サイバーディフェンス研究所の CSIRT である CDI-CIRT[1] が、複数の特定のコミュニティから、次のような標的型攻撃メールの存在の報告を受け、すぐに、そのメールを入手した。

【基本情報】

2011/03/31 17:34

From: zhengri jin <zhngrjn@gmail.com>
Subject: ３月 30 日放射線量の状況
Body: <空白>
Attached file： ３月 30 日放射線量の状況.doc

CDI が入手した標的型攻撃メール

3. 標的型攻撃メールの一般情報に関する分析とコメント

受信日時について 2011/3/31

この標的型攻撃メールは、2011 年３月 31 日に送信されたものである。しかし、CDI の対応経験では、他の同様な標的型攻撃メールは、４月上旬頃から急激に目立ち始めていた。

したがって、この標的型攻撃メールの送信が震災が発生した月内だったところをみると、受信者が強い関心を抱いている時期を狙ったものなのか、或いは、月内に送信しなければならない何かしらの理由があったのかを想起させるようなタイミングであったといえる。

[1] CDI-CIRT：サイバーディフェンス研究所の CSIRT（Computer Security Incident Response Team）http://www.first.org/members/teams/cdi-cirt（海外）http://www.nca.gr.jp/member/cdi-cirt.html（国内）

送信者（From：）について　zhengri jin <zhngrjn@gmail.com>

送信者名を あえて〝zhengri jin〟としているが、これはハングルでは〝정일　김〟、中国語（漢字）では、〝正日　金〟となる。つまり、2011 年 12 月 17 日に死去した北朝鮮の最高指導者「金正日（キムジョンイル）」を騙ったものであると推定される。

参考：人名表（J）－ 维基百科，自由的百科全书
http://zh.wikipedia.org/wiki/%E4%BA%BA%E5%90%8D%E8%A1%A8_%28J%29

また、「金正日」の英語表記は、〝Kim Jong-il〟である。この送信者名の英語表記とは大きく異なる。〝Jin Zhengri〟は、中国語（北京語）で「金正日」の発音を尊重した英語表記であるためである。

ここで少し矛盾がみられる。最近の傾向は、添付ファイルを確実に開かせようとするために、創意工夫の一つとして、From：（送信元）に To：（受信者）と近い関係にある人物の名前或いはアドレスを入れることが多い。あまりにも有名な人物名を From：にした場合、受信者に警戒心を抱かせることになり、この標的型攻撃の目的が十分に達成されない可能性がある。

この標的型攻撃メールでは、国際的に有名な人物名を使っているため、その攻撃理由そのものが見えにくくなっていると言える。

受信者（To：）について　zhngrjn@gmail.com

通常の標的型攻撃メールは、To：（受信者）に明示的なターゲットを入れる傾向があるが、今回の標的型攻撃メールは、送信者自身のアドレスを入れている。これは、一斉通信をする時に見られる手法であり、使い回ししやすいメールであると言える。

本文について　〈空欄〉

本文が空欄であることは、不特定多数に対する送信という特徴という観点で、上述の受信者（To：）が個別でないことと符合する。或いは、緊急時対処をする業務領域において、電子メールをファイル送信ツールとして利用している人も存在しているため、添付ファイル名の名称と合わせて、受信する方によっては、ごく自然なメールと捉える人がいると考えられる。

添付ファイルについて　3 月 30 日放射線量の状況.doc

この送信時期が、福島第一原発事故による放射性物質の飛散が大きな問題となっていた時期であったため、「3 月 30 日放射線量の状況.doc」というファイル名は、多くの方が非常に興味を持つものであったということができる。

4. 標的型攻撃メールのメールヘッダに関する分析とコメント

```
From - Thu Mar 31 17:34:38 2011
X-Account-Key: account3
X-UIDL: 00011b8349b1d8f1
X-Mozilla-Status: 0001
X-Mozilla-Status2: 10000000
X-Mozilla-Keys:
Return-Path: <zhngrjn@gmail.com>
Delivered-To: xxxxxxxxxxxxxxxxxxxxx
Received: (qmail 1220 invoked by SAV 20110330.049 by uid 0); 31 Mar 2011 17:34:06 +0900
X-Spam-Scan: through
Received: from unknown (HELO mail-iy0-f171.google.com) (209.85.210.171)
  by xxxxxxxxx (xxx.xxx.xxx.xxx) with ESMTPS (RC4-SHA encrypted); 31 Mar 2011 17:34:06 +0900
Received-SPF: pass (xxxxxxxxx: SPF record at _spf.google.com designates 209.85.210.171 as
permitted sender)
Received: by iyi20 with SMTP id 20so2436051iyi.30
        for <xxxxxxxxxxxxxxxxxxxxx>; Thu, 31 Mar 2011 01:34:04 -0700 (PDT)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=gamma;
        h=domainkey-signature:mime-version:date:message-id:subject:from:to
         :content-type;
        bh=oPfJvcGPaGXmd6clJbY2H2/GMNyTdjcQo8w7B7otNKk=;
        b=LmeQL+QxP72oR6RikAtxiwgvK+xxkVRKoikF/TgyaZKMW1KKksfpfROtNeFT8wdcw+
         CFXarN7enDoWSQB2MQNe12ZVb5nV6dZ7p6onDc0cQ0jpiazYLe8U8bFoHwcgiNbV0OyL
         zx1IaZR7GAZivL1DPHKpr5VpgwcYB6rAi4om4=
DomainKey-Signature: a=rsa-sha1; c=nofws;
        d=gmail.com; s=gamma;
        h=bcc:mime-version:date:message-id:subject:from:to:content-type;
        b=fU8dTC9m3GltVbNnve/p63wZheSVCCbRAmjHEunw8lHTQtnwkMru1wzI+FtB8bm8Ab
         q8Ck4L6epCgtd27uct7XvxDjCvUscVDnO1WqoW21CDRb1xHtLvsQoshA/2nYjNv2MgQw
         qnrTUQUg5PJYyi9EGgvh7lKg9E6kUiBcVC1t0=
Bcc: xxxxxxxxxxxxxxxxxxxxx
MIME-Version: 1.0
Received: by 10.231.29.101 with SMTP id p37mr2534109ibc.3.1301560444611; Thu,
 31 Mar 2011 01:34:04 -0700 (PDT)
Received: by 10.231.183.142 with HTTP; Thu, 31 Mar 2011 01:34:04 -0700 (PDT)
Date: Thu, 31 Mar 2011 16:34:04 +0800
Message-ID: <AANLkTim8VtDiJtADMXsT8D+7DNyKTCNF5FoMb=VUo3Mv@mail.gmail.com>
Subject: =?GB2312?B?M9TCMzDI1bfFyeS+gMG/pM7XtJty?=
From: zhengri jin <zhngrjn@gmail.com>
To: zhngrjn@gmail.com
Content-Type: multipart/mixed; boundary=00151773e340f46eda049fc32752

--00151773e340f46eda049fc32752
Content-Type: multipart/alternative; boundary=00151773e340f46ed2049fc32750

--00151773e340f46ed2049fc32750
Content-Type: text/plain; charset=ISO-8859-1



--00151773e340f46ed2049fc32750
Content-Type: text/html; charset=ISO-8859-1



--00151773e340f46ed2049fc32750--
--00151773e340f46eda049fc32752
Content-Type: application/msword; name="=?GB2312?B?M9TCMzDI1bfFyeS+gMG/pM4=?=
          =?GB2312?B?17Sbci5kb2M=?="
Content-Disposition: attachment;
          filename="=?GB2312?B?M9TCMzDI1bfFyeS+gMG/pM7XtJtyLmRvYw==?="
Content-Transfer-Encoding: base64
X-Attachment-Id: f_glxfggvy0
```

標的型攻撃メールのソース

Date：について　Date: Thu, 31 Mar 2011 16:34:04 +0800

Date： に残される情報は、一般的には「送信者の時刻帯」で表記されることが多い。この標的型攻撃メールの Date の時刻表記 +0800 は、中国標準時（CST）であるため、中国を発信源としている可能性が高い。

参考：中国標準時

http://ja.wikipedia.org/wiki/%E4%B8%AD%E5%9B%BD%E6%A8%99%E6%BA%96%E6%99%82

一番下の Received： について　by 10.231.183.142 with HTTP; Thu, 31 Mar 2011 01:34:04 -0700 (PDT)

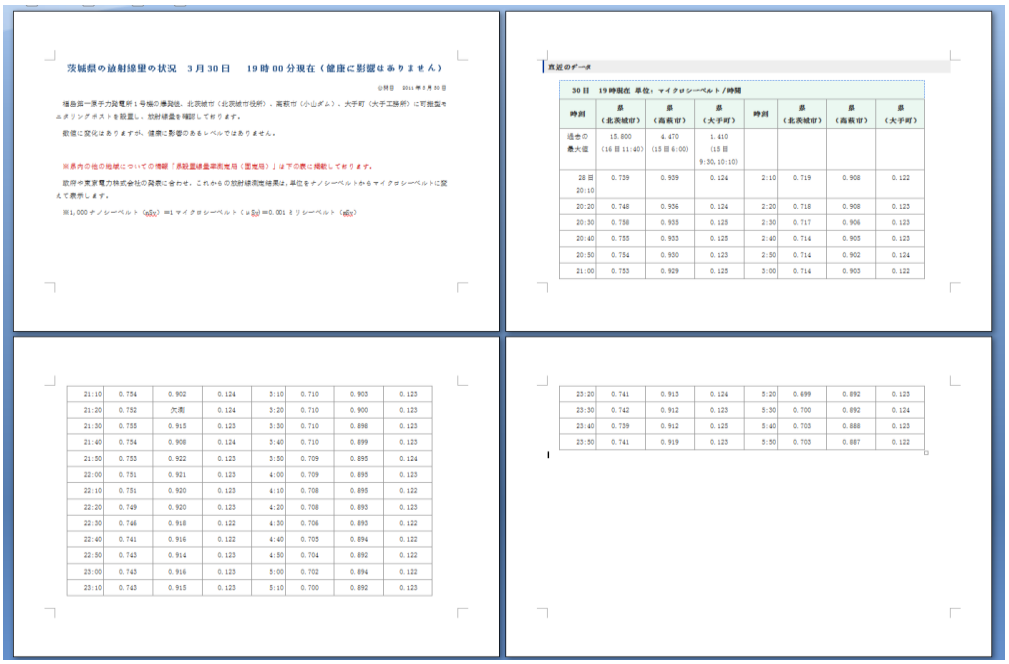
一番下の Received：は、最初の配送経路として記録される情報である。ここに残されている情報は、Web ブラウザによる Gmail でメール送信していることを示している。また、-0700（PDT）は、Gmail の配送経路の一つが所在する米国カルフォニア州の時刻帯である。

5. 標的型攻撃メールの添付ファイルの関する分析とコメント

このメールに添付されていたファイルは、次のとおり。

- Type of file: Microsoft Office Word 97 - 2003 Document (.doc)
- Size: 59.5KB（60,928bytes）
- Authors: ISA
- Last saved by: ISA
- Revision no.: 2
- Content created: 2011/03/30 20:39
- Date last saved: 2011/03/30 20:39
- Total edting time: 00:03:00
- Pages: 4
- Word count: 243
- Character count: 1386
- Line count: 11
- Paragraph count: 3

ファイルを開いた時のイメージは、次のとおり。



茨城県の放射線量の状況　3月30日　19時00分現在（健康に影響はありません）

公開日　2011年3月30日

福島第一原子力発電所1号機の爆発後、北茨城市（北茨城市役所）、高萩市（小山ダム）、大子町（大子工務所）に可搬型モニタリングポストを設置し、放射線量を確認しております。

数値に変化はありますが、健康に影響のあるレベルではありません。

※県内の他の地域についての情報「県設置線量率測定局（固定局）」は下の表に掲載しております。

政府や東京電力株式会社の発表に合わせ，これからの放射線測定結果は，単位をナノシーベルトからマイクロシーベルトに変えて表示します。

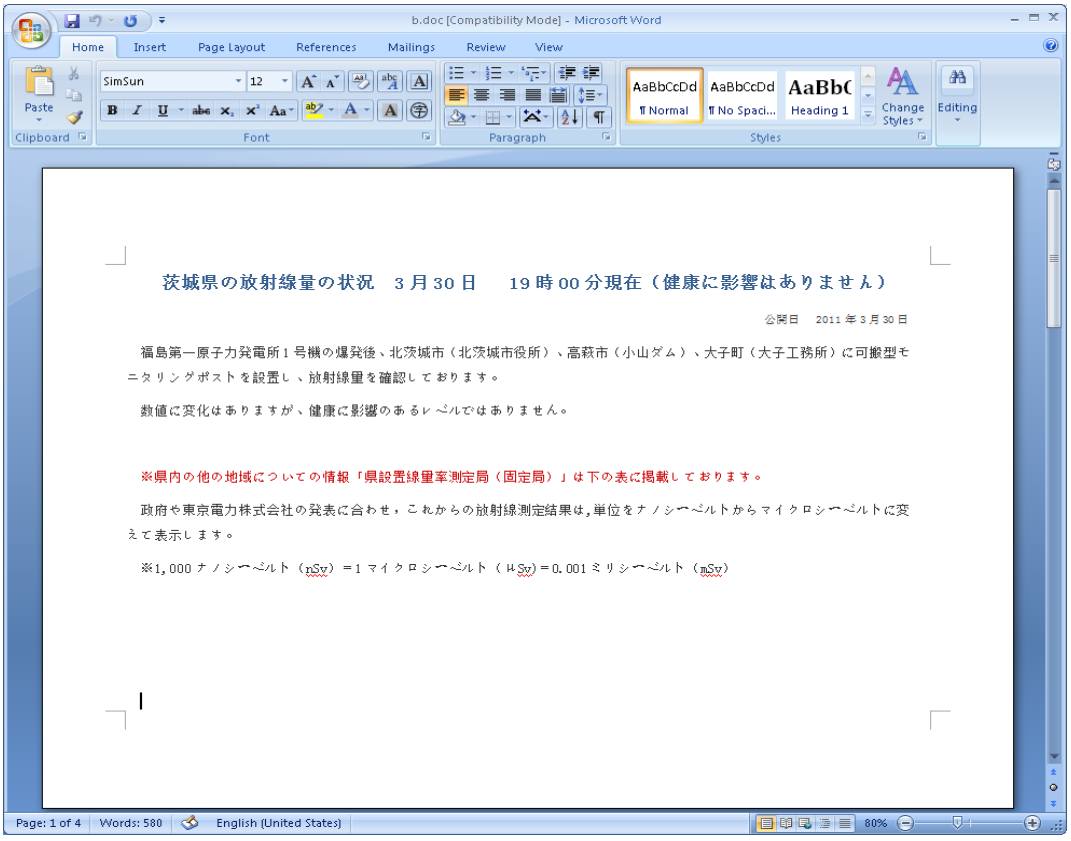
※1，000ナノシーベルト（nSv）＝1マイクロシーベルト（μSv）＝0.001ミリシーベルト（mSv）

過去のデータ

30日　19時現在　単位：マイクロシーベルト/時間

時刻	県（北茨城市）	県（高萩市）	県（大子町）	時刻	県（北茨城市）	県（高萩市）	県（大子町）
過去の最大値	15.800（16日11:40）	6.470（15日6:00）	1.410（15日9:30,10:10）				
28日 20:10	0.739	0.939	0.124	2:10	0.719	0.908	0.122
20:20	0.748	0.936	0.124	2:20	0.718	0.908	0.123
20:30	0.738	0.935	0.125	2:30	0.717	0.906	0.123
20:40	0.735	0.933	0.125	2:40	0.714	0.905	0.123
20:50	0.754	0.930	0.123	2:50	0.714	0.902	0.124
21:00	0.753	0.929	0.125	3:00	0.714	0.903	0.122
21:10	0.754	0.902	0.124	3:10	0.710	0.903	0.123
21:20	0.752	欠測	0.124	3:20	0.710	0.900	0.123
21:30	0.755	0.915	0.123	3:30	0.710	0.898	0.123
21:40	0.754	0.908	0.124	3:40	0.710	0.899	0.123
21:50	0.753	0.922	0.123	3:50	0.709	0.895	0.124
22:00	0.751	0.921	0.123	4:00	0.709	0.895	0.123
22:10	0.751	0.920	0.123	4:10	0.708	0.895	0.122
22:20	0.749	0.920	0.123	4:20	0.708	0.893	0.123
22:30	0.746	0.918	0.122	4:30	0.706	0.893	0.122
22:40	0.741	0.916	0.122	4:40	0.705	0.894	0.122
22:50	0.743	0.914	0.123	4:50	0.704	0.892	0.122
23:00	0.743	0.916	0.123	5:00	0.702	0.894	0.122
23:10	0.743	0.915	0.123	5:10	0.700	0.892	0.123
23:20	0.741	0.913	0.124	5:20	0.699	0.892	0.123
23:30	0.742	0.912	0.123	5:30	0.700	0.892	0.124
23:40	0.739	0.912	0.125	5:40	0.703	0.888	0.123
23:50	0.741	0.919	0.125	5:50	0.703	0.887	0.122

標的型攻撃メールの添付ファイル（全ページ）



標的型攻撃メールの添付ファイル（1 ページのみ）

フォント（Font）について　　SimSun

SimSun とは、Windows OS で標準で入っている GB コード（中国の文字コードで、日本の JIS に相当）の中国語文字フォントで、中国語宋体字（明朝系）と呼ばれるものである。

※日本は、「JIS コード」或いは「Shift-JIS コード」という文字コードが使われているが、中国（特に、簡体字圏）は「GB コード」、中国・台湾（主に繁体字圏）は「Big5 コード」が使われている。中国語版の Windows OS が搭載された PC では、上述の SimSun のほかに、SimHei と呼ばれる中国語黒体字（ゴシック系）がよく使用されている。

ファイル内の情報について

このファイル内の情報は、次のサイトで公開されている本物の情報をコピーしたものである。

茨城県
IBARAKI Prefectural Government

Foreign Language　携帯用サイト　検索

サイトマップ　文字の大きさの変更について　文字の色　1　2

ホーム　創る　暮らす　楽しむ　学ぶ　知る

ホーム ＞ 重要事項 ＞ 平成23年東日本大震災 ＞ 茨城県の放射線量の状況　3月30日　19時00分現在（健康に影響はありません）【災害対策本部】

茨城県の放射線量の状況　3月30日　19時00分現在（健康に影響はありません）

公開日　2011年3月30日

福島第一原子力発電所1号機の爆発後、北茨城市（北茨城市役所）、高萩市（小山ダム）、大子町（大子工務所）に可搬型モニタリングポストを設置し、放射線量を確認しております。
数値に変化はありますが、健康に影響のあるレベルではありません。

東京電力福島第一原子力発電所の事故に伴う放射線の影響は心配ありません。【橋本 昌知事メッセージ】

※県内の他の地域についての情報「県設置線量率測定局（固定局）」は下の表に掲載しております。
政府や東京電力株式会社の発表に合わせ，これからの放射線測定結果は，単位をナノシーベルトからマイクロシーベルトに変えて表示します。
※1,000ナノシーベルト（nSv）＝1マイクロシーベルト（μSv）＝0.001ミリシーベルト（mSv）

直近のデータが見られます。
それ以前のデータはPDFファイルにしました。こちらはすべてのデータを見ることができます。

直近のデータ

30日　19時現在　単位：マイクロシーベルト／時間

時刻	県（北茨城市）	県（高萩市）	県（大子町）	時刻	県（北茨城市）	県（高萩市）	県（大子町）
過去の最大値	15.800（16日11:40）	4.470（15日6:00）	1.410（15日 9:30,10:10）				
28日 20:10	0.739	0.939	0.124	2:10	0.719	0.908	0.122
20:20	0.748	0.936	0.124	2:20	0.718	0.908	0.123

添付ファイル内の情報のコピー元

http://www.pref.ibaraki.jp/important2/20110311eq/20110330_18/

この時期、放射線量に関する情報が錯綜していたため、この添付ファイルの情報に不審を抱かなかった受信者がいたと考えられる。

また、Web ブラウザから MS Word にコピーするには、Firefox ではなく、Internet Explorer で閲覧した当該サイトをコピーして、MS Word（文字コードは SimSun）に貼りつけると、この標的型攻撃メールの添付ファイルとほぼ同じものを作成できることを確認した。

ファイルに含まれている悪意のあるコード

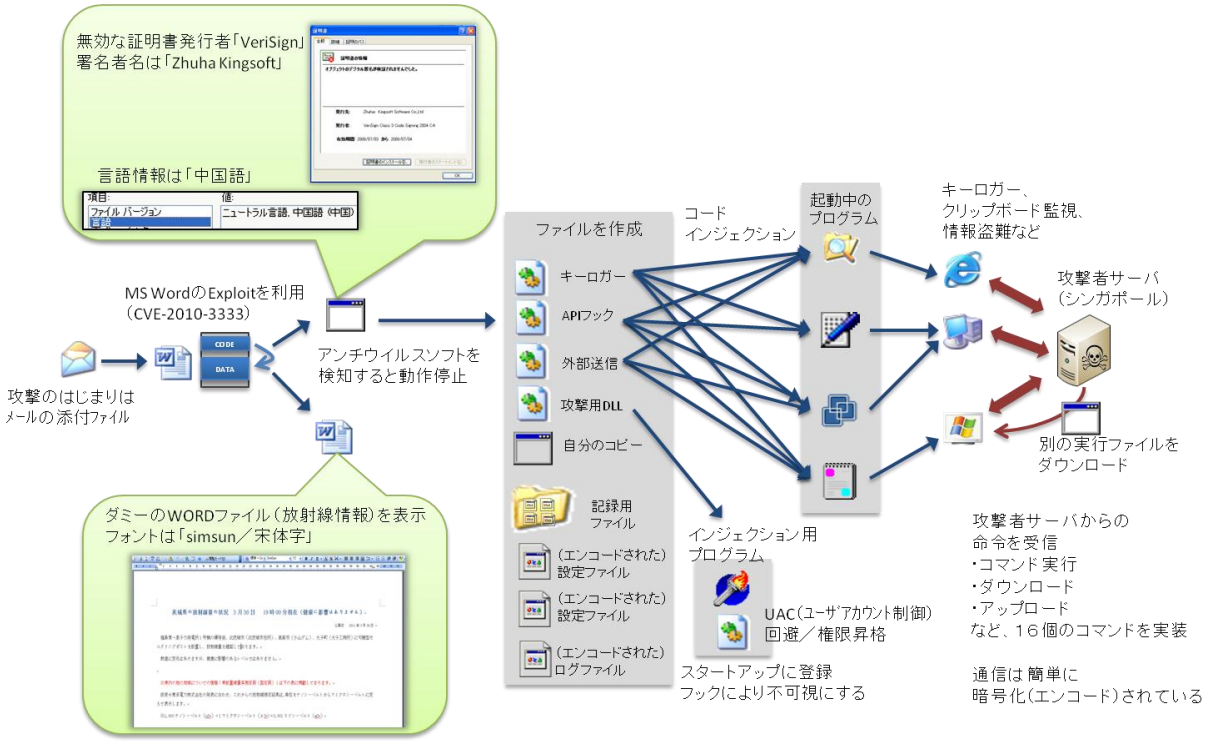
このファイルには、脆弱性 CVE-2010-3333 を利用した悪意のあるコードが含まれている。

※ CVE-2010-3333：RTF のスタック バッファ オーバーフローの脆弱性
Microsoft Office ソフトウェアが特別に細工されたリッチ テキスト形式（.rtf）のデータを分析する処理の方法に、リモートでコードが実行される脆弱性が存在する。攻撃者がこの脆弱性を悪用した場合、影響を受けるコンピューターを完全に制御する可能性がある。その後、攻撃者はプログラムのインストール、データの表示、変更、削除、または完全なユーザー権限を持つ新たなアカウントを作成する可能性がある。システムで、アカウントのユーザー権限を低く設定している場合、管理者ユーザー権限で実行しているユーザーよりもこの脆弱性の影響が少なくなると考えられる。
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3333

6. 添付ファイル中の悪性コードの分析

本報告では、詳細な分析過程を省略するが、添付ファイルに内在している悪性コードの挙動は、次のとおり。

- 添付ファイルを開くことにより、「悪性コードを含むファイル」と「本物の MS Word ファイル」が開く。
- 「悪性コードのファイル」は、アンチウィルスソフトが動作している環境では、それ以上の動作はしない。
- もし、アンチウィルスソフトが動作していない場合、「悪性コードを含むファイル」は、キーロガー、API フック、外部送信、攻撃用 DLL などのファイルを作成する。
- 作成されたファイルは、起動中のプログラム（Explorer、ワードパッド、VMware、ノートパッド）に対してコードインジェクションすることにより、（作成されたファイルの）それぞれの機能を動作させる。
- さらに、それらの機能は、Internet Explorer、Explorer、悪意のあるコードを含む DLL を通じて、外部と通信する。



悪性コードの活動の流れ

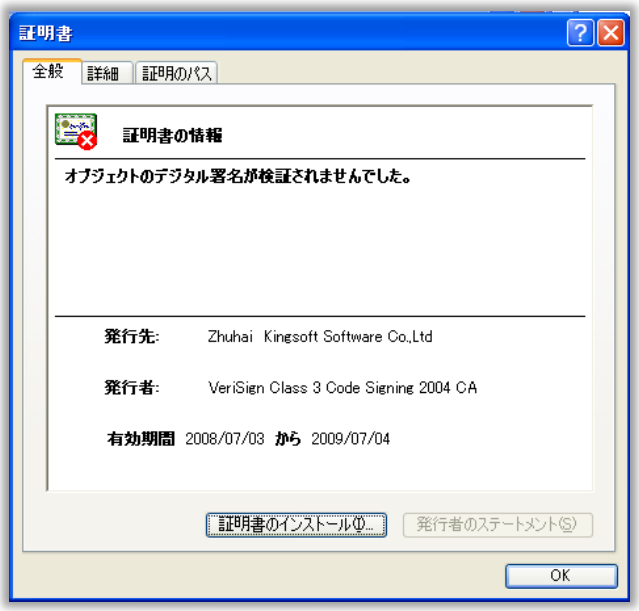
前述の分析及びコメントで示したもの以外に、これらの悪性コードの流れの中で、攻撃者の特性を示唆するものが、各所で確認できる。

悪性コードの言語情報

悪性コードの言語情報は、「ニュートラル言語」及び「中国語」となっている。「ニュートラル言語」と出た理由は、この悪性コードを分析した環境が、日本語、英語、中国語のみの言語のリソースしかなかったためと考えられる。つまり、悪性コードの中に「これら以外の言語」の情報が含まれていた可能性がある。

実行ファイルの証明書情報

実行ファイルに偽物の証明書がついており、デジタル署名の発行先に Zhuhai Kingsoft Software Co., Ltd という実在する事業者名を記していた。また、有効期間は 2009/07/04 に設定し、表示されているエラーを、期限が切れているように見せかけていた可能性がある。



興味深いことに、同月 2 日（米国時間）、米国シマンテック社が、このデジタル署名の発行先名と同じ名称を利用した不正行為を確認していた。

信頼済みのソフトウェアを悪用する不正行為 （Updated：04 Mar 2011）
http://www.symantec.com/connect/blogs-161

検知するアンチウィルスソフトの種類

悪性ファイルは、次のアンチウィルスソフトが動作しているかどうかを確認する。これらのリストには、国際的に有名なアンチウィルスソフトが入っていない代わりに、日本では馴染みのないものが入っている。

KSafe	?	Mcafee	
Kingsoft		GData	
Tencent		Filseclab	
Ahnlab		Kasperskylab	
Hauri		Nod32	
NProtect		Avg	
Dr_web		Rising	
New Technology Wave		QQ	
Avast		Jiangmin	
BitDefender		Avira	
Trendmicro		Micropoint	
Panda Security		Norton	

データ収集用サーバについて

キーロガーなどをよって搾取されたデータを送信する先のサーバは、次のような OS となっていた。

6. まとめ

以上のように、東日本大震災に乗じた標的型攻撃メール攻撃の分析結果の概要を説明したが、他のパートナーからの提供された同種のマルウェアを分析すると、次のような分析結果が出た。

- ２ヶ月ほど遅れて開発された形跡を確認した。
- 同じ不正コードを再利用していた。
- 情報収集用のサーバは、同じプロバイダであった。
- 異なるユーザがコンパイルした形跡を確認した。

さらに別の同種のマルウェアを分析及び調査すると、他所で 2011 年 10 月から「すでに」確認されていたことが分かった。東日本大震災に乗じた標的型攻撃メールで使用された不正コードは、南米を中心に感染を広げているものである。

Generic BackDoor!dqz!FF4778FCF9E3

http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=621218

このように、最近の標的型攻撃メールは、ターゲット毎に作成されているわけではなく、不正コードの部分は使い回しがされている。カスタマイズされているのは、メール本文や差出人の部分だけであり、その多くに、攻撃者の IT 環境や行動特性を示唆するような情報が見え隠れしている。

2012 年４月６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