SSRC-IR-201004-1

S.S.R.C.定期
インシデントレポート
Vol.4

株式会社　日立情報システムズ

サイバーセキュリティ対策センタ

初版　2010/04/01

S.S.R.C.インシデントレポート Vol.4
目次

1. はじめに

S.S.R.C. (SHIELD Security Research Center)は、株式会社日立情報システムズ サイバーセキュリティ対策センタが運営するセキュリティ情報公開サイトです。本サイトでは、サイバーセキュリティ対策センタによるリサーチ結果を随時配信する予定です。

本文書は、株式会社日立情報システムズ SHIELD セキュリティセンタで日々収集を行っているセキュリティ情報にもとづき、サイバーセキュリティ対策センタのセキュリティアナリストが、不正アクセスなどのセキュリティインシデントの傾向調査したレポートです。

次に示すご利用条件を十分にお読み頂き、ご了承頂いた上でご利用下さいます様、よろしくお願い致します。

2. ご利用条件

本文書内の画像等すべての情報の著作権は、特別の断りがない限り、株式会社日立情報システムズ（以下、「当社」）に帰属します。本文書をご利用いただく際には、非営利目的かつ利用者個人（または組織内部）での利用に限り、当社の著作物を複製することができます。但し、当該複製物には、当社の著作権表示を付して戴くことを条件と致します。

上記を除き、営利目的による複製・公衆送信等著作物の利用や、商標権・著作権・特許権等知的所有権に基づくいかなる権利も許諾するものではありません。なお、個々の著作物に利用条件が付されている場合は当該条件が優先されます。

また、当社は情報掲載にあたって細心の注意を払っておりますが、その内容に誤りや欠陥があった場合にも、いかなる保証もするものではありません。本文書をご利用いただいたことにより生じた損害につきましても、当社は一切責任を負いかねます。

本文書に掲載されている情報は、掲載した時点の情報です。掲載した時点以降に変更される場合もありますので、あらかじめご了承ください。

3． 概要

SHIELD セキュリティセンタでは、専属のセキュリティアナリストが全世界各地より各種セキュリティ情報の収集を行っております。本レポートでは、(株) 日立情報システムズ　SHIELD セキュリティセンタにて収集を行っているセキュリティ情報より、不正アクセスなどのセキュリティインシデントの傾向調査を行いましたのでご報告致します。

本レポートの対象は以下の通りとなっています。

対象期間	:	2010 年 01 月 01 日 ～ 2010 年 03 月 31 日
収集拠点	:	SHIELD　セキュリティセンタ
本レポートの対象装置	:	IDS　×　3 種

4. サマリレポート

本章では、SHIELD セキュリティセンタにて観測されたインシデントについて様々な観点から一次分析（単視点からの）を行いましたので報告します。

4.1. 地域傾向

SHIELD セキュリティセンタにて観測されたインシデントの内、対象期間中に観測されたユニーク IP 数、ユニーク地点数は以下の通りとなっています。

- ユニークIP　:約 300,899（1 月）
  :約 427,051（2 月）
  :約 424,668（3 月）
- ユニーク地点　:約 26,554（1 月）
  :約 28,648（2 月）
  :約 28,333（3 月）

前レポート期間と比較しますと、IP アドレスの範囲および地点は 2 月を境に増加していることがわかります。一時的な傾向である可能性もありますが、経過を見て判断します。

4.2. 攻撃元国別傾向

SHIELDセキュリティセンタにて観測された攻撃の、攻撃元国傾向についてご報告します。まず、攻撃元の国、上位 5 件について図 1、図 2、図 3に示します。ここでの値は、下記式をもとに算出しています。

値 ＝ 1 時間毎に観測される値 ÷ 先月分の 1 時間毎平均数

このため、先月の平均観測数との検知数が同じであれば、値＝1となり、増加した場合は、値＞1、減少した場合は、値＜1となります。また、本グラフにおけるタイムゾーンはGMT＋0 となっています。

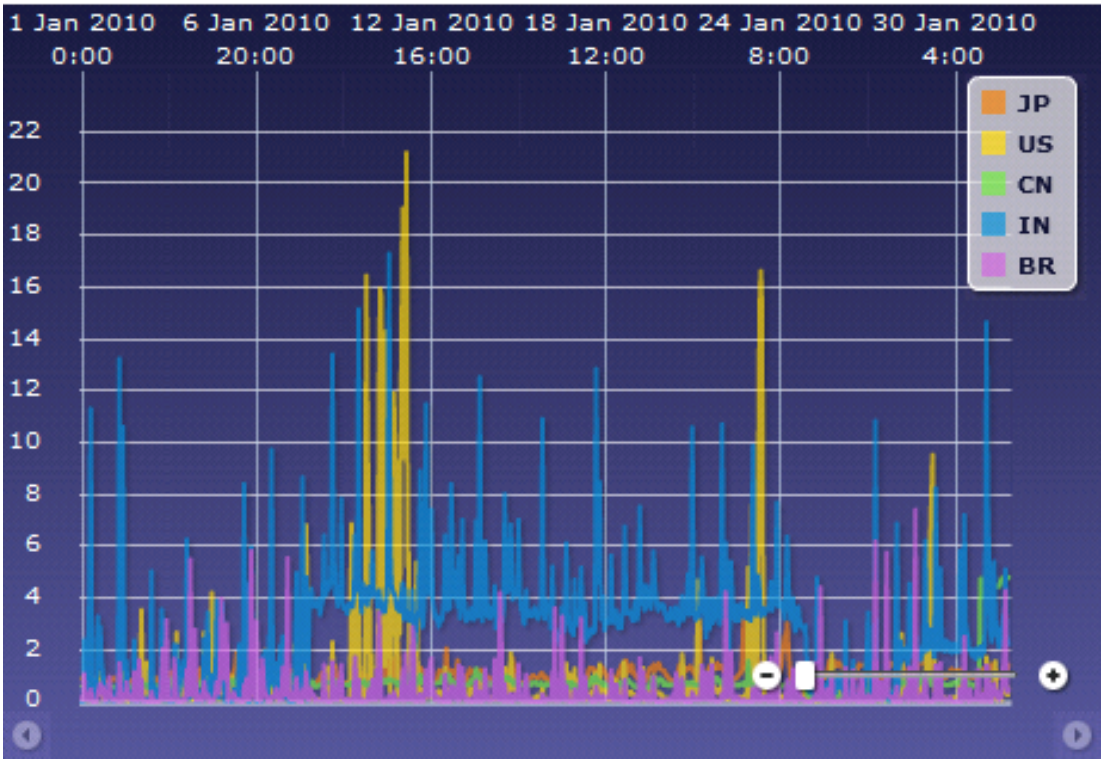


図 1 攻撃元国傾向(1 月)

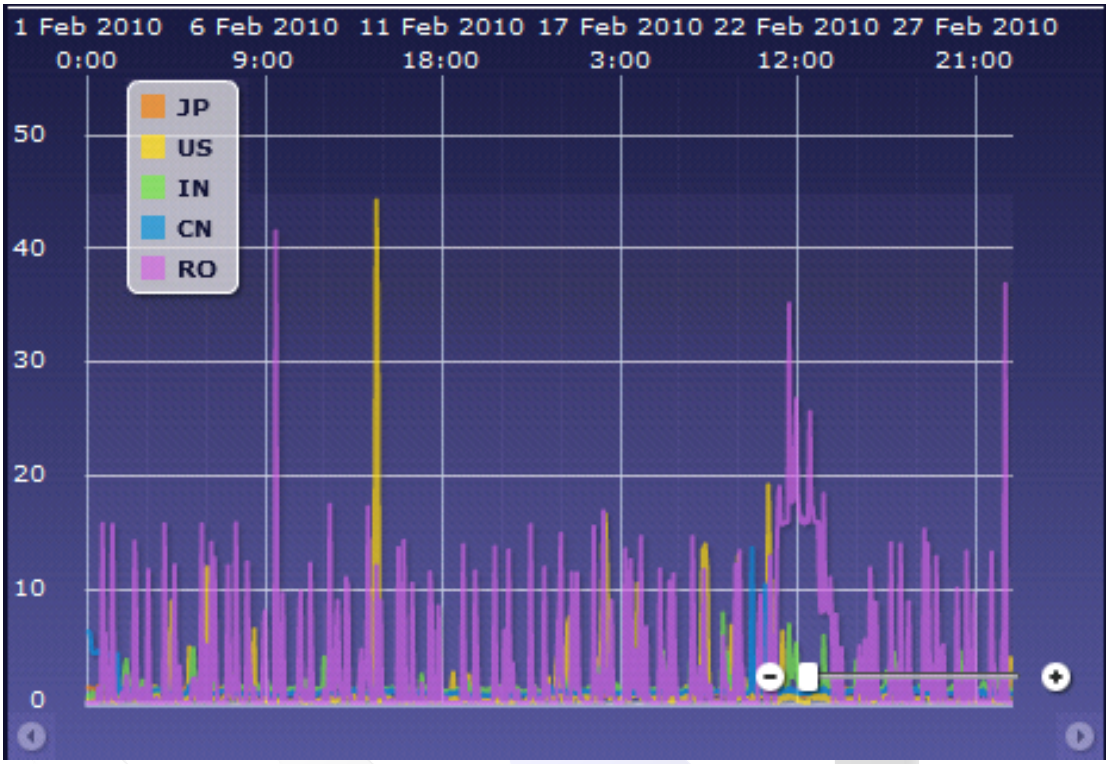


図 2 攻撃元国傾向(2 月)

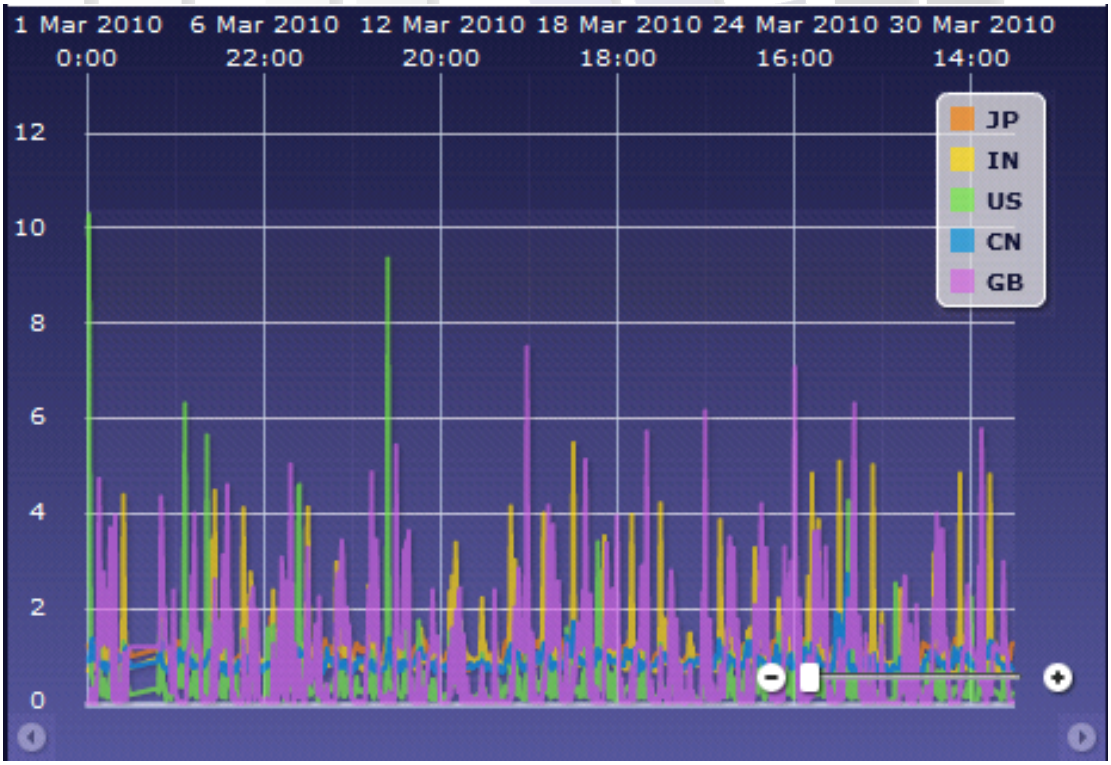


図 3 攻撃元国傾向(3 月)

また、攻撃全体に対する国毎の割合を表 1に示します。

表 1 各月ごとの全体のインシデント中の国ごとの割合

ランキング	1 月 [%]		2 月[%]		3 月[%]	
1	日本	→ 67.5	日本	→ 57.4	日本	→ 63.5
2	アメリカ	↑ 9.3	アメリカ	→ 9.1	インド	↑ 6.3
3	中国	↓ 3.6	インド	→ 5.0	アメリカ	↑ 4.8
4	インド	→ 3.2	中国	→ 3.5	中国	↓ 3.3
5	ブラジル	↑ 1.7	ルーマニア	→ 2.1	イギリス	↑ 1.7
6	イギリス	↓ 0.9	イギリス	↑ 1.7	ベトナム	→ 1.5
7	韓国	→ 0.9	ブラジル	↓ 1.5	フィリピン	↑ 1.5
8	フィリピン	↓ 0.8	フィリピン	→ 1.3	ブラジル	↑ 1.3
9	ドイツ	↑ 0.8	ロシア	↑ 1.1	韓国	↓ 1.1
10	ルーマニア	↑ 0.8	ドイツ	↓ 1.1	ルーマニア	↑ 1.0
—	その他	11.0	その他	16.1	その他	13.9

今回の調査結果は、前回のご報告(10 月～12 月)[i]から比較しても上位国に大きな変化はありませんが、図 3からもわかりますように、2 月は一時的にルーマニアからのインシデントの増加が見受けられます。

4.3. サービス別

SHIELDセキュリティセンタにて観測された、主要サービス(smtp,pop3,domain,http,https)に対する攻撃をグラフ化したものを図 4、図 5、図 6に示します。ここでの値は、下記式をもとに算出しています。

値 ＝ 1時間毎に観測される値 ÷ 先月分の1時間毎平均数

このため、先月の平均観測数との検知数が同じであれば、値＝1となり、増加した場合は、値＞1、減少した場合は、値＜1となります。また、本グラフにおけるタイムゾーンはGMT＋0 となっています。

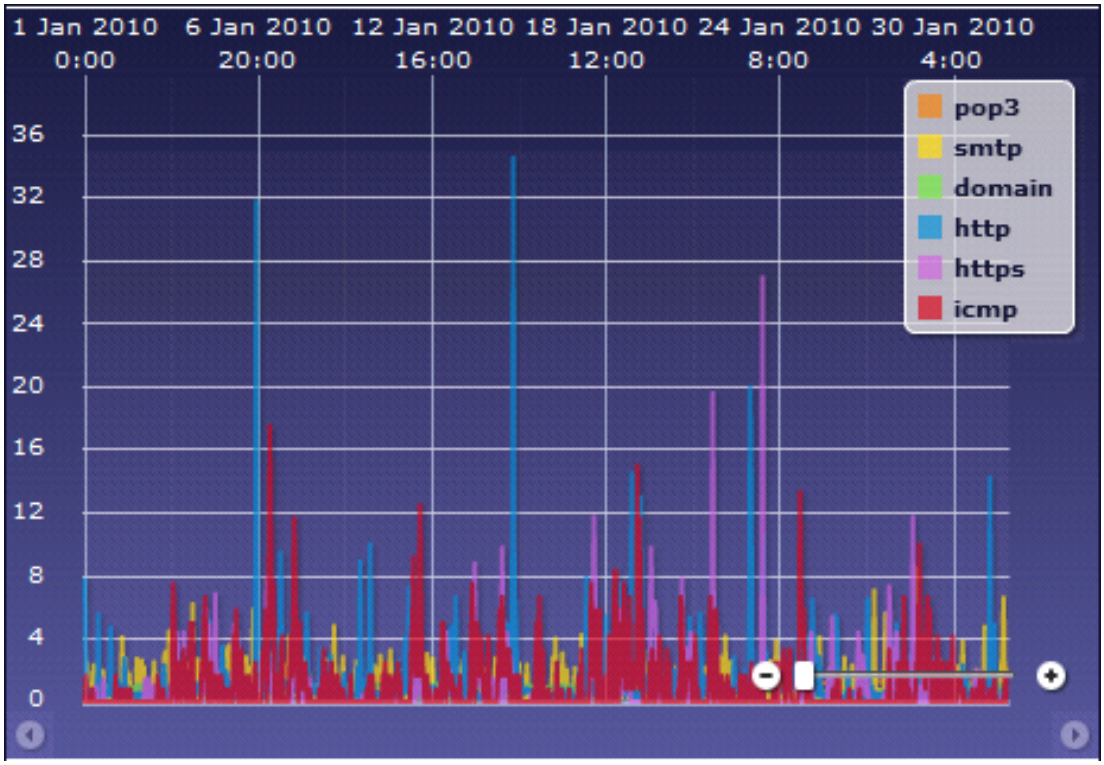


図 4 攻撃サービス傾向(1 月)

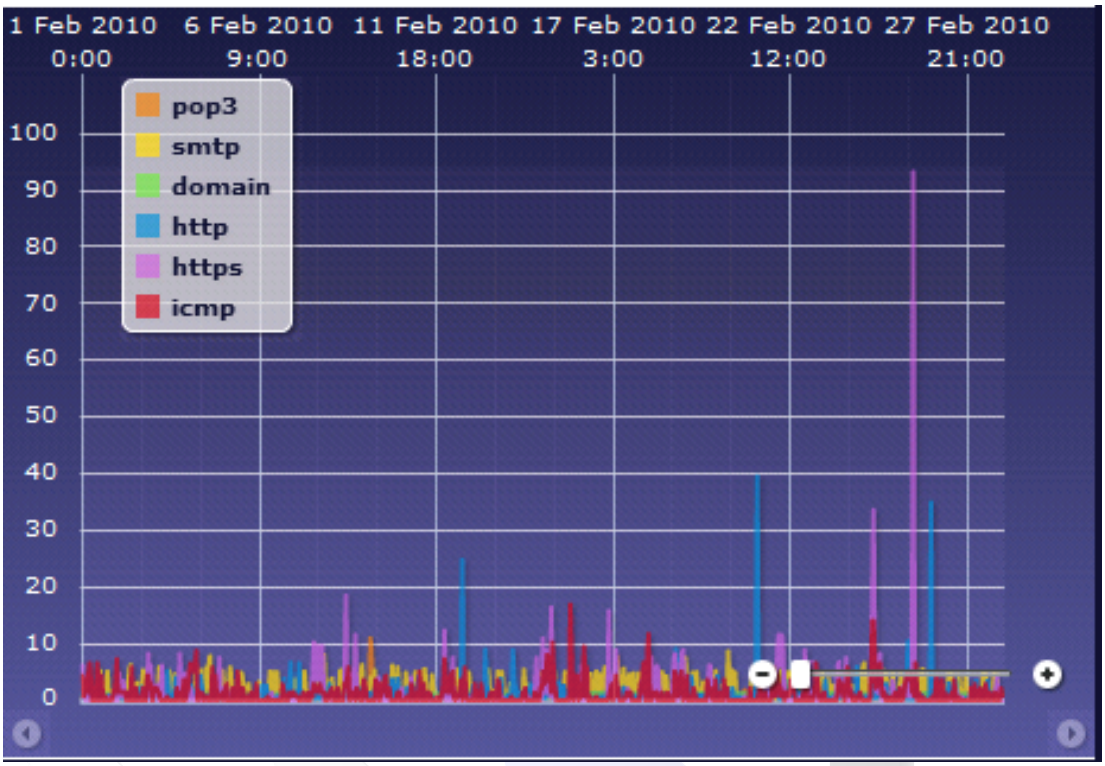


図 5 攻撃サービス傾向(2 月)

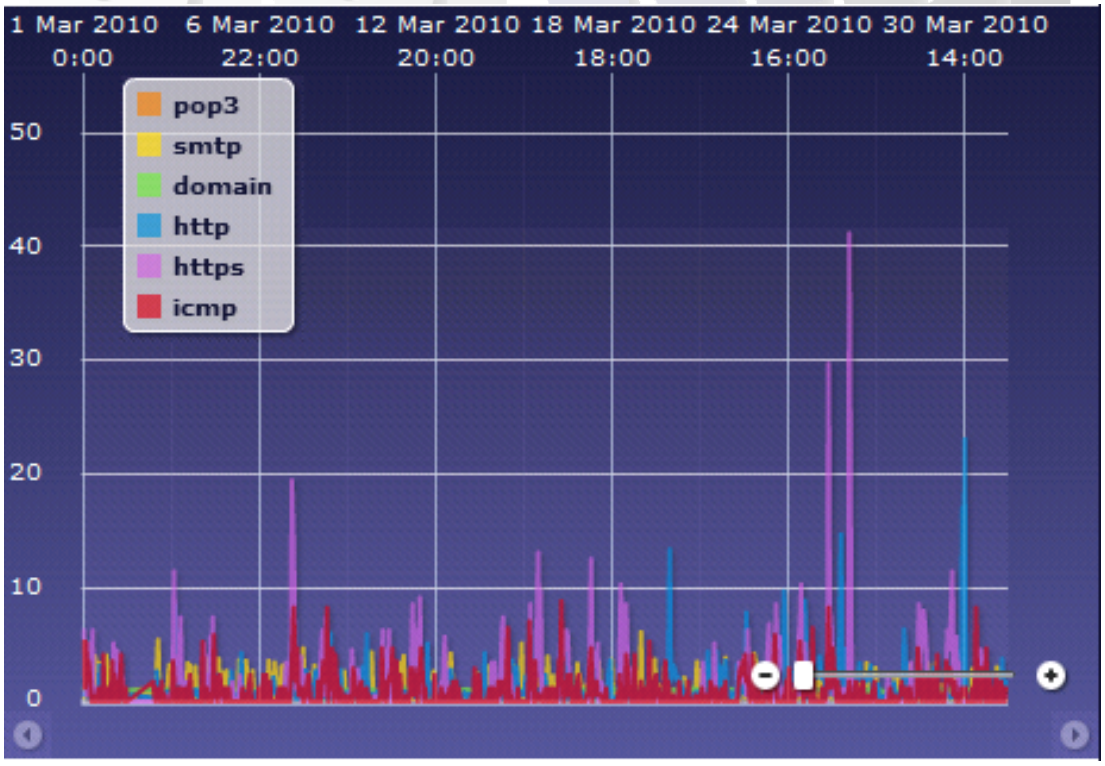


図 6 攻撃サービス傾向(3 月)

図 4にて観測されているHTTPへのインシデント、図 5、図 6にて観測されているHTTPSへのインシデントの増加は、ツールによる攻撃と考えられます。

5. 注目インシデントの現状

本章では現在注目する必要があるインシデントの現状についてご報告します。本レポートでは下記についてご報告します。

- Conficker ワームの現状

5.1. CONFICKER の現状

全号に続き、Confickerの現状について調査を行いましたのでご報告します。Confickerとは、Microsoft社から提供されている更新プログラム「MS08-067」[ii]を適用していないWindowsのUSBドライブやネットワーク共有などを使用して感染するワームです。

この、Conficker による攻撃の現状を図 7に示します。

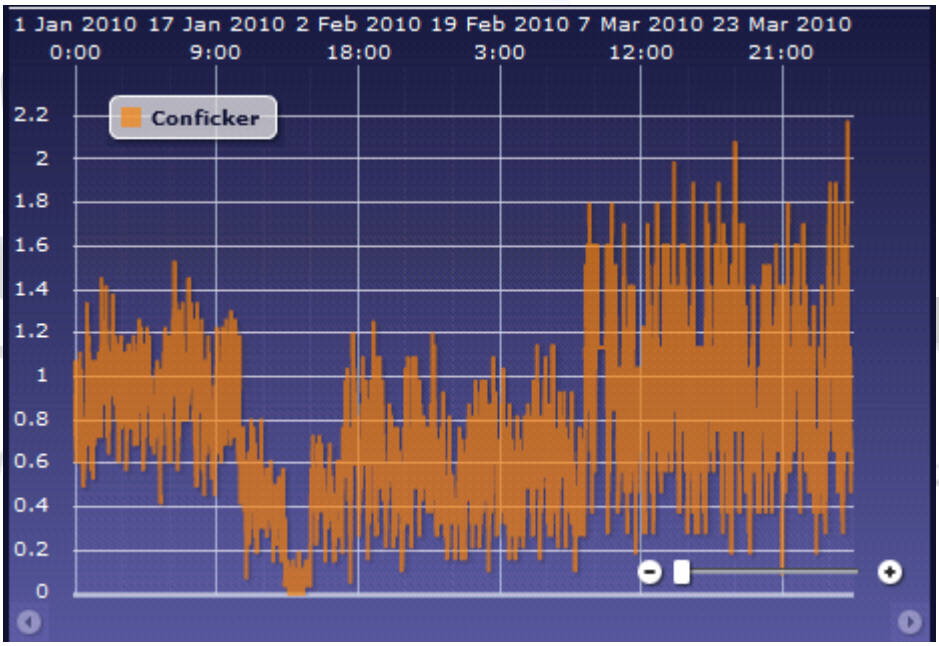


図 7 Confricker による攻撃の傾向

図 7から2010年1月～3月のConfickerは、大きな振れ幅もなく比較的安定しています。しかし、継続的に観測されていることから注意が必要です。

6. おわりに

1月 ～ 3月の期間中、SHIELDセキュリティセンタで観測された情報では大規模攻撃は発生していません。一方、全レポートから報告を続けております「Conficker」にやや減少傾向にあるものの、収束には至っていません。今後も、引き続き観測を続けて参ります。

一方で、「Gumblar」につきましては現在、幸運にもSHIELD セキュリティセンタでは観測されていません。しかし、「Gumblar」による被害は拡大を続けておりますので、引き続き注意が必要です。

7. 参考文献、参考資料、サイトなど

[i] S.S.R.C.セキュリティインシデントレポート Vol.3, 日立情報システムズ,
http://www.shield.ne.jp/ssrc/doc/SSRC-IR-201001.pdf
2010/04/26 確認

[ii] MS08-067 : Windows の重要な更新, Microsoft Corporation
http://www.microsoft.com/japan/security/bulletins/MS08-067e.mspx
2009/4/26 確認

8. 付録

- Web セキュリティ on-Demand「Web アプリケーションファイアウォール」のご案内

  - コンセプトは？

    Web アプリケーションの脆弱性を狙ったデータの不正取得や、Web サイトの改ざんなどの攻撃を検知し、ブロックします。

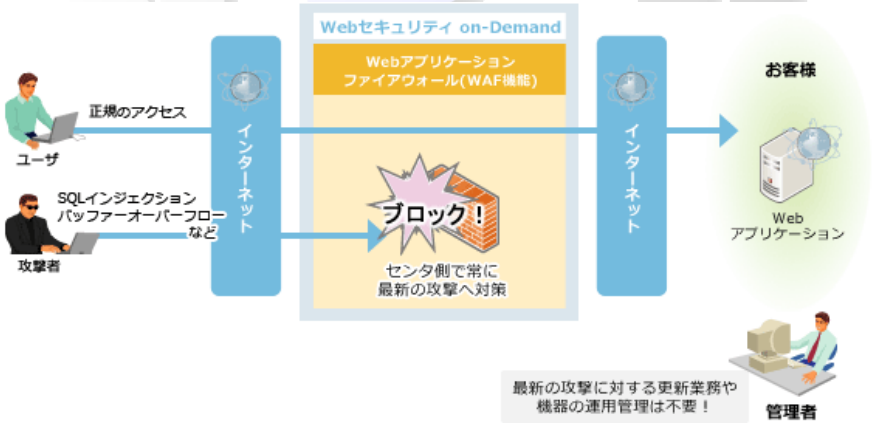
  - ソリューションメリットは？

    Web アプリケーションへの攻撃をブロックすることで、情報漏えいや Web サイトの停止などのリスクから守ります。また、Web アプリケーションへのセキュリティ対策を、短期間、低コストで実現できます。

  - このようなお客様におすすめです

    ＊Web アプリケーションの脆弱性対策をまだ行っていないお客様

    ＊Web アプリケーションの脆弱性対策を短期間で安価に実現したいお客様



詳細につきましては、下記、日立情報システムズHPからご確認ください。

http://www.hitachijoho.com/solution/shield/express/web/waf.html

株式会社　日立情報システムズ

〒141-8672 東京都品川区大崎 1-2-1

http://www.hitachijoho.com

http://www.shield.ne.jp/ssrc/