SSRC-TR-2010-04

S.S.R.C.定期
トレンドレポート
Vol.3

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.トレンドトレポート Vol.3

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世界中のセキュリティトレンド情報にもとづき、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、月ごとでのセキュリティトレンドの動向をまとめたレポートです。

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頂きます様、よろしくお願い致します。

2． ご利用条件

本文書内の文章等すべての情報掲載に当たりまして、株式会社日立情報システムズ（以下、「当社」といいます。）と致しましても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、掲載した時点での情報です。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. トレンドレポート 2010 年第 1 四半期度版

該当期間の代表的なセキュリティ情報は以下の通りです。

対象期間:2010/01/01～2010/03/31

3.1. セキュリティトレンド情報

当期間確認された情報セキュリティに関する情報は以下の通りです。

1. 携帯ユーザを狙ったフィッシングサイトが出現

ニュースリリース	● 【注意喚起】 携帯サイトを装ったフィッシングサイトにご注意下さい（フィッシング対策協議会） http://www.antiphishing.jp/alert/alert1032.html#more
関連記事	● 携帯ユーザを狙ったフィッシングサイトが出現 ー 対策協議会が注意喚起（RBB TODAY） http://www.rbbtoday.com/article/2010/01/06/64762.html

2. Googleサイバー攻撃に中国政府関与か

関連記事	● 中国から Google ほか 30 社以上に攻撃：目的はソースコード（Wired Vision） http://wiredvision.jp/news/201001/2010011422.html ● Adobe もサイバー攻撃の標的に、ネットワークに組織的な攻撃か（IT media） http://www.itmedia.co.jp/enterprise/articles/1001/14/news020.html

3. ドイツ政府、脆弱性問題に懸念を抱き、IEブラウザの使用を控えるよう国民に勧告

関連記事	● ドイツ：政府が国民に対しＩＥ以外のブラウザを利用するように勧告（Cyber Law） http://cyberlaw.cocolog-nifty.com/blog/2010/01/post-6756.html

4. 警視庁、P2Pファイル共有ソフトを常時監視するシステム運用開始

関連記事	● シェアやウィニー、常時調査＝流通ファイルの実態把握－抽出の９割が違法・警察庁（時事ドットコム） http://www.jiji.com/jc/zc?k=201002/2010020400242

5. サイバーセキュリティ法案、米下院を通過

関連記事	● サイバーセキュリティ法案、米下院を通過（ZDNet Japan） http://japan.zdnet.com/news/sec/story/0,2000056194,20408117,00.htm

6. サイバーテロが物理攻撃よりも脅威になりうる　英国際戦略研調査

関連記事	● サイバー攻撃の脅威警告/「ミサイルよりも破壊力」/英国際戦略研（live door ニュース） http://news.livedoor.com/article/detail/4589092/

7. 「ファイル共有ソフトを悪用した著作権侵害への対応に関するガイドライン」の公表

関連記事	● 「ファイル共有ソフトを悪用した著作権侵害への対応に関するガイドライン」の公表について（ファイル共有ソフトを悪用した著作権侵害対策協議会） http://www.ccif-j.jp/news_20100208.html

8. 中国、世界最大のサイバー犯罪の温床に

関連記事	● 中国、世界最大のサイバー犯罪の温床に（japan.internet.com） http://japan.internet.com/webtech/20100210/11.html

9. オーストラリア政府関連サイトがDDoS被害に

関連記事	● オーストラリア：政府や議会のサイトが「Operation Titstorm」という名の DDoS 攻撃を受ける（Cyber Law） http://cyberlaw.cocolog-nifty.com/blog/2010/02/operation-titst.html

10. Web Application Firewall 読本公開

ニュースリリース	● Web Application Firewall 読本（IPA） http://www.ipa.go.jp/security/vuln/waf.html

11. 平成 21 年度における出会い系サイトに関連した事件検挙状況

ニュースリリース	● 平成 21 年中のいわゆる出会い系サイトに関係した事件の検挙状況について（警視庁） http://www.npa.go.jp/cyber/statics/h21/pdf52.pdf

12. 「2010 年版 10 大脅威 あぶり出される組織の弱点！」を公開

ニュースリリース	● 「2010 年版 10 大脅威 あぶり出される組織の弱点！」を公開 http://www.ipa.go.jp/security/vuln/10threats2010.html

13. 世界規模のハッカー攻撃の背後に東欧犯罪組織の影

関連記事	● 世界規模のハッカー攻撃の背後に東欧犯罪組織の影（ウォールストリートジャーナル） http://jp.wsj.com/IT/node_33954 ● 世界で 7 万 5000 台に感染のマルウェア、ログイン情報を大量窃盗（IT media） http://www.itmedia.co.jp/enterprise/articles/1002/19/news020.html

14. Googleへのサイバー攻撃、中国名門大学が発信源か―米紙

関連記事	● Google へのサイバー攻撃、中国名門大学が発信源か―米紙（レコードチャイナ） http://www.recordchina.co.jp/group.php?groupid=39878&type=1 ● Google 攻撃に使われたコード、作成した中国のセキュリティ専門家を特定か--英報道（CNET Japan） http://japan.cnet.com/news/sec/story/0,2000056024,20409082,00.htm

15. ラトビア、ハッカーがハッキングした銀行や国営企業内部情報をテレビで暴露

関連記事	● ラトビア：ハッキングした銀行の取引情報及び国営企業の情報をハッカーがテレビで暴露（Cyber Law） http://cyberlaw.cocolog-nifty.com/blog/2010/02/post-7373.html

16. 米マイクロソフト、サイバー犯罪対策で新手法

関連記事	● 米マイクロソフト、サイバー犯罪対策で新手法（ウォールストリートジャーナル） http://jp.wsj.com/IT/node_36705 ● Microsoft、大規模ボットネット『Waledac』を粉砕（japan.internet.com） http://japan.internet.com/busnews/20100226/10.html ● Waledacよ安らかに？（エフセキュアブログ） http://blog.f-secure.jp/archives/50353680.html

17. 韓国からのF5 アタックにより２ちゃんねるサーバ陥落

関連記事	● ２ちゃんねるダウン、韓国と日本の歴史的関係が原因―欧米メディア（サーチナ） http://news.searchina.ne.jp/disp.cgi?y=2010&d=0303&f=national_0303_017.shtml ● 【韓フルタイム】日韓サイバー戦争、韓国が懲りずに 2 次攻撃を予定か！？（live door news） http://news.livedoor.com/article/detail/4636153/ ● 2 ちゃん攻撃問題で米企業が FBI に資料提出　攻撃表明のブログも（産経ニュース） http://sankei.jp.msn.com/economy/it/100305/its1003051845002-n1.htm

18. 警察庁、2009 年度のサイバー犯罪の検挙状況を発表

ニュースリリース	● 平成 21 年中のサイバー犯罪の検挙状況等について（警視庁） http://www.npa.go.jp/cyber/statics/h21/pdf54.pdf

19. サイバー犯罪者に悪用される可能性が高い公開映画トップ 10

ニュースリリース	● マカフィー、最も検索リスクの高いアカデミー賞ノミネート作品を発表（マカフィー） http://www.mcafee.com/japan/about/prelease/pr_10a.asp?pr=10/03/05-1

20. ＦＢＩ長官、サイバー攻撃による脅威拡大に警鐘

関連記事	● ＦＢＩ長官、サイバー攻撃による脅威拡大に警鐘（ロイター） http://jp.reuters.com/article/technologyNews/idJPJAPAN-14213620100306

21. 「サイバー攻撃に無防備、１９３自治体」

関連記事	● 「サイバー攻撃に無防備、１９３自治体」だそうです（まるちゃんの情報セキュリティ気まぐれ日記） http://maruyama-mitsuhiko.cocolog-nifty.com/security/2010/03/post-e68c.html

22. 活発に活動する 10 大ボットネット

関連記事	● スパムの元凶--活発に活動する 10 大ボットネット（ZDNet Japan） http://japan.zdnet.com/sp/feature/07tenthings/story/0,3800082984,20409761,00.htm

23. マカフィー、危険なオンライン上の脅威を個人ユーザに警告

ニュースリリース	● マカフィー、危険なオンライン上の脅威を個人ユーザに警告（マカフィー） http://www.mcafee.com/japan/about/prelease/pr_10a.asp?pr=10/03/09-2

24. 韓国で 2 千万人規模の個人情報漏洩の可能性

関連記事	● South Korea Dealing With Massive Data Breach（liquid matrix digest） http://www.liquidmatrix.org/blog/2010/03/13/south-korea-dealing-with-massive-data-breach/

25. インド：サイバー犯罪が増加

関連記事	● インド：サイバー犯罪が増加（Cyber Law） http://cyberlaw.cocolog-nifty.com/blog/2010/03/post-1204.html

26. 違法ＤＬで 120 万人失業、欧州で 2015 年までに

関連記事	● 違法ＤＬで 120 万人失業、欧州で 2015 年までに＝調査（ロイター） http://jp.reuters.com/article/oddlyEnoughNews/idJPJAPAN-14402720100318

27. ガンブラー：欧州サーバ感染源に

ニュースリリース	● 情報技術解析平成 21 年報（警視庁） http://www.npa.go.jp/cyberpolice/detect/pdf/H21_nempo.pdf

28. 欧州における情報セキュリティ関連動向調査報告書

ニュースリリース	● 欧州における情報セキュリティ関連動向調査報告書（IPA） http://www.ipa.go.jp/security/fy21/reports/fraunhofer/index.html

29. 米史上最大のコンピューター犯罪でハッカーに禁固 20 年

関連記事	● 米史上最大のコンピューター犯罪でハッカーに禁固 20 年（ウォールストリートジャーナル） http://jp.wsj.com/IT/node_45879

3.2. GUMBLAR(亜種)ウイルス被害サイト情報

当期間確認された Gumblar(亜種)ウイルスに感染されたサイトに関する情報は以下の通りです。

1. ローソンの採用サイトが改ざん被害に

ニュースリリース	● ローソンホームページ「採用」サイト改ざんについて（ローソン） http://www.lawson.co.jp/company/news/detail/detail_1748.html
関連記事	● ローソンの採用サイト改ざん　閲覧者に Gumblar ウイルス感染の恐れ（IT media） http://www.itmedia.co.jp/news/articles/1001/06/news083.html

2. ハウス食品新卒採用サイトが改ざん被害に

ニュースリリース	● ハウス食品「採用ホームページ」に関するお詫びとお知らせ（ハウス食品） http://housefoods.jp/company/info/info2291.html
関連記事	● 「新卒採用ページ」が改ざん、閲覧者にウイルス感染のおそれ - ハウス食品（Security NEXT） http://www.security-next.com/011787.html

3. 大学図書館問題研究会サイトが改ざん被害に

ニュースリリース	● 大図研 HP 改竄被害について（大学図書館問題研究会） http://www.daitoken.com/
関連記事	● 大図研のサイトが改ざん被害 - 閲覧者にウイルス感染の可能性（Security NEXT） http://www.security-next.com/011786.html

4. 「Yahoo! 占い」一部サイトが改ざん被害に

ニュースリリース	● 「鏡リュウジの星に願いを」を閲覧されたお客様へご確認のお願い（Yahoo! JAPAN） http://fortune.yahoo.co.jp/information/announce/201001091617.html
関連記事	● Yahoo!が 2 カ月以上にわたり改ざん状態に - 「Gumblar」亜種原因で（Security NEXT） http://www.security-next.com/011803.html

5. 東京財団サイトが改ざん被害に

関連記事	● 東京財団のサイトが改ざん被害 - 閲覧者にウイルス感染のおそれ（Security NEXT） http://www.security-next.com/011794.html

6. 三栄コーポレーション「モッフル」サイトが改ざん被害に

ニュースリリース	● 「モッフル」ホームページの改ざんとウイルス被害に関する報告とお詫び（三栄コーポレーション） http://www.sanyeicorp.com/new/mofflevrsrpt.pdf
関連記事	● サイト改ざん(2)ハウス食品、民主党、ローソンなど被害サイト 23 の改ざん状況（So-net） http://www.so-net.ne.jp/security/news/library/2113.html

7. データリンクスサイトが改ざん被害に

ニュースリリース	● ホームページに関する報告とお詫び（データリンクス） http://www.haken.datalinks.co.jp/news/index.html?id=11
関連記事	● サイト改ざん(2)ハウス食品、民主党、ローソンなど被害サイト 23 の改ざん状況（So-net） http://www.so-net.ne.jp/security/news/library/2113.html

8. ビロングサイトが改ざん被害に

ニュースリリース	● 不正改ざんに関するお詫び（ビロング） http://illustshow.com/info_20100106.php
関連記事	● サイト改ざん(2)ハウス食品、民主党、ローソンなど被害サイト 23 の改ざん状況（So-net） http://www.so-net.ne.jp/security/news/library/2113.html

9. nccサイトが改ざん被害に

ニュースリリース	● ncc サイトに関する報告とお詫び（ncc） http://www.n-c-c.org/modules/info/index.php?id=19
関連記事	● サイト改ざん(2)ハウス食品、民主党、ローソンなど被害サイト 23 の改ざん状況（So-net） http://www.so-net.ne.jp/security/news/library/2113.html

10. モロゾフサイトが改ざん被害に

ニュースリリース	● ホームページに関する報告とお詫び　2010 年 01 月 05 日（モロゾフ） http://www.morozoff.co.jp/_cms_/news_item/detail/item00085.html
関連記事	● サイト改ざん(2)ハウス食品、民主党、ローソンなど被害サイト 23 の改ざん状況（So-net） http://www.so-net.ne.jp/security/news/library/2113.html

11. ブックオフ子会社サイトが改ざん被害に

ニュースリリース	● 当社子会社 HP に関する報告とお詫び（ブックオフ） http://www.bookoff.co.jp/news/index.php?action=news&news_id=496
関連記事	● ブックオフ子会社のサイトが改ざん被害 - ブックオフ本社サイトは影響なし（Security NEXT） http://www.security-next.com/011804.html

12. 野村ビルマネジメントサイトが改ざん被害に

ニュースリリース	● お詫び（ホームページ改ざんの件）（野村ビルマネジメント） http://www.nomura-bm.co.jp/data/pdf/NEWS091225.pdf
関連記事	● 改ざんでほぼ全ページが改ざん被害 - 野村ビルマネジメント（Security NEXT） http://www.security-next.com/011811.html

13. コープエイシスサイトが改ざん被害に

ニュースリリース	● ホームページに関する報告とお詫び　2010 年 01 月 07 日（コープエイシス） http://blog.coop-kobe.net/assis1/archives/2010/01/post_8.html
関連記事	● ウェブサイトが改ざんされ、閲覧でウイルス感染の可能性 - コープこうべ子会社（Security NEXT） http://www.security-next.com/011808.html

14. 三井住友カードサイトが改ざん被害に

ニュースリリース	● 弊社ホームページ上のリンクサイトの改ざんについて（三井住友カード） https://www.smbc-card.com/mem/cardinfo/cardinfo8090276.jsp
関連記事	● 外部へ運営を委託しているサイトが「Gumblar」で改ざん - 三井住友カード（Security NEXT） http://www.security-next.com/011823.html

15. 大学情報サイト「大学探し.com」が改ざん - 閲覧者にウイルス感染の可能性

関連記事	● 大学情報サイト「大学探し.com」が改ざん - 閲覧者にウイルス感染の可能性（Security NEXT） http://www.security-next.com/011815.html

16. ゲームアーツサイトが改ざん被害に

関連記事	● Wii 向けゲームタイトルの公式サイトが改ざん - ゲームアーツ（Security NEXT） http://www.security-next.com/011829.html

17. FJネクストサイトが改ざん被害に

ニュースリリース	● 当社ホームページに関するお詫びと報告（FJ ネクスト） http://www.fjnext.com/info/
関連記事	● 年末から年始にかけてウェブサイトが改ざん - FJ ネクスト（Security NEXT） http://www.security-next.com/011828.html

18. 北海道生涯学習推進センタサイトが改ざん被害に

ニュースリリース	● 各道立青少年教育施設のホームページを閲覧されている皆様へのお知らせ（北海道立生涯学習推進センタ） http://manabi.pref.hokkaido.jp/center/kokuti.htm
関連記事	● 教育関連施設の複数ページが 1 カ月弱にわたり改ざん - 北海道立生涯学習推進センタ（Security NEXT） http://www.security-next.com/011833.html

19. 東京ガスの「硬式野球部サイト」が改ざん被害に

ニュースリリース	● 「東京ガス硬式野球部サイト」の改ざんに関するお詫びとお知らせについて（東京ガス） http://www.tokyo-gas.co.jp/important/20100115-01.html
関連記事	● 東京ガスの「硬式野球部サイト」が改ざん被害 - 閲覧でウイルス感染の可能性（Security NEXT） http://www.security-next.com/011845.html

20. 大阪のRMT事業者のダイアモンドギルのサイトが改ざん被害に

ニュースリリース	● 当サイトに関するお詫びとお知らせ [2010-01-08] （ダイアモンドギル） http://rmt.diamond-gil.jp/info_detail.php/info/414/
関連記事	● RMT 事業者のウェブサイトが改ざん - 閲覧でウイルス感染のおそれ（Security NEXT） http://www.security-next.com/011846.html

21. 中小企業向け情報サイト「パワーチャンネル」のサイトが改ざん被害に

ニュースリリース	● （お詫び）ホームページの再開について（パワーチャンネル） http://biz.sbr-inc.jp/info/owabi100108.shtml
関連記事	● 中小企業向け情報サイト「パワーチャンネル」がウイルスで改ざん（Security NEXT） http://www.security-next.com/011856.html

22. SAPジャパン・ユーザー・グループ（JSUG）のサイトが改ざん被害に

ニュースリリース	● コンピュータウィルス感染のご報告とウイルス撒布のお詫び（JSUG） http://www.jsug.org/news/2010/01/000254.html
関連記事	● JSUG のウェブサイトが「Gumblar」による改ざん被害（Security NEXT） http://www.security-next.com/011855.html

23. 環境共生住宅推進協議会のサイトが改ざん被害に

関連記事	● 環境共生住宅推進協議会のウェブサイトが改ざん、閲覧でウイルス感染のおそれ（Security NEXT） http://www.security-next.com/011851.html

24. テルモのショッピングサイトが改ざん被害に

ニュースリリース	● テルモホームページに関するお詫びとお知らせ（テルモ） http://www.terumo.co.jp/press/2010/notice.html
関連記事	● テルモのショッピングサイトが改ざん - 個人情報漏洩はなし（Security NEXT） http://www.security-next.com/011861.html

25. ファーストクレジットのサイトが改ざん被害に

ニュースリリース	● 当社ホームページに関するお知らせ（お詫び）（ファーストクレジット） http://www.firstcredit.co.jp/release/news100118.html
関連記事	● ファーストクレジットのサイトが改ざん被害 - 原因は「Gumblar」亜種（Security NEXT） http://www.security-next.com/011860.html

26. 札幌市公園緑化協会のサイトが改ざんに

ニュースリリース	● ウイルスの再発のお詫びとお願い（札幌市公園緑化協会） http://www.sapporo-park.or.jp/owabi.html
関連記事	● 札幌市公園緑化協会のサイトが改ざん - 全ページに不正スクリプト（Security NEXT） http://www.security-next.com/011865.html

27. NTTデータ先端技術の商品紹介サイトが改ざん被害に

ニュースリリース	● 「VOISTAGE サイト」の改ざんに関するご報告とお詫び（NTT データ先端技術株式会社） http://www.intellilink.co.jp/all/topics/2010/01/19/voistage.html
関連記事	● NTT データ先端技術の商品紹介サイト「VOISTAGE-ONLINE」が改ざん（Security NEXT） http://www.security-next.com/011863.html

28. 複数の FX 事業者サイトが改ざん被害に

ニュースリリース	● Klug クルーク「経済指標カレンダー」に関するお詫びとお知らせ（GCI キャピタル） http://www.gcic.jp/news_release/2010/20100119klug.pdf
関連記事	● 複数の FX 事業者サイトでウイルス感染のおそれ - 情報提供元サイトの改ざんが影響（Security NEXT） http://www.security-next.com/011869.html

29. 「東京芸術劇場チケットサービス」のサイトが再度改ざん被害に

ニュースリリース	● 東京芸術劇場ホームページの外部サイト「東京芸術劇場チケットサービス」の改ざんについて（東京都） http://www.metro.tokyo.jp/INET/OSHIRASE/2010/01/20k1l300.htm
関連記事	● 「東京芸術劇場チケットサービス」が改ざん - 1 月初旬に修正するも再発覚（Security NEXT） http://www.security-next.com/011883.html

30. 保健指導関係者の情報交換SNSサイト「保健指導向上委員会」が改ざん被害に

ニュースリリース	● 「保健指導向上委員会」ホームページをご覧になった皆様へ （保険指導向上委員会） http://www.hokensidou.net/notice.html
関連記事	● 保健指導関係者の SNS サイトが改ざん - 利用者から指摘されるも対応遅れる（Security NEXT） http://www.security-next.com/011877.html

31. 鳥羽市のキャンペーンサイトが改ざん被害に

ニュースリリース	● 恋する鳥羽キャンペーンサイトに関するお詫びとお知らせ（コイトバ） http://www.koitoba.com/apology/
関連記事	● 鳥羽市のキャンペーンサイト改ざん被害 - 閲覧でウイルス感染の可能性（Security NEXT） http://www.security-next.com/011894.html

32. 電子情報技術産業協会サイトが改ざん被害に

ニュースリリース	● ホームページの再開について（JEITA） http://www.jeita.or.jp/cgi-bin/topics/detail.cgi?n=1754&ca=3
関連記事	● 改ざんされた電子情報技術産業協会のサイトが一部復旧（Security NEXT） http://www.security-next.com/011891.html

33. 東京・春・音楽祭サイトが改ざん被害に

ニュースリリース	● ホームページ改ざんに関する報告とお詫び（東京･春･音楽祭実行委員会） http://www.tokyo-harusai.com/news/news_450.html
関連記事	● 音楽祭のウェブサイトが「Gumblar」で改ざん状態に（Security NEXT） http://www.security-next.com/011896.html

34. 仙台国際交流協会サイトが改ざん被害に

ニュースリリース	● （財）仙台国際交流協会のホームページの改ざんについて（お詫び）（仙台国際交流協会） http://www.sira.or.jp/top_img/20100209_J.pdf
関連記事	● サイトが不正アクセスで改ざんされ、閉鎖 - 仙台国際交流協会（Security NEXT） http://www.security-next.com/011892.html

35. 東急不動産の関連サイトが改ざん被害に

ニュースリリース	● お詫び（弊社一部ホームページにおける改ざんの件）（東急不動産） http://sumai.tokyu-land.co.jp/help_notice.html
関連記事	● 東急不動産の関連サイトが改ざん - 複数の物件紹介ページが被害（Security NEXT） http://www.security-next.com/011887.html

36. トータルリラクゼーションスペース「宙 SORA」サイトが改ざん被害に

ニュースリリース	● 【「宙 ＳＯＲＡ」ホームページに関するお詫びとお知らせ】（宙 ＳＯＲＡ） http://blog.sora111.com/article/34871655.html
関連記事	● 新たに 20 件のサイト改ざんが明らかに～新規改ざんサイト一覧（So-net） http://www.so-net.ne.jp/security/news/library/2129.html

37. ミルブレインズLLCレンタルサーバサイトが改ざん被害に

ニュースリリース	● 1/20 Gamblar ウイルスにご注意下さい （ミルブレインズ LLC） http://gigasrv.jp/282.html ● 1/20 当社レンタルサーバを閲覧になったお客様へご確認のお願い （ミルブレインズ LLC） http://mbsrv.jp/532.html ● 1/20 当社レンタルサーバを閲覧になったお客様へご確認のお願い （ミルブレインズ LLC） http://99yen.jp/167.html
関連記事	● 新たに 20 件のサイト改ざんが明らかに～新規改ざんサイト一覧（So-net） http://www.so-net.ne.jp/security/news/library/2129.html

38. せいか幼稚園サイトが改ざん被害に

ニュースリリース	● せいか幼稚園ホームページをご覧の皆様へ（せいか幼稚園） http://www.seika-group.or.jp/blog_sukusuku/2010/01/post-213.html http://www.seika-group.or.jp/blog_nobinobi/2010/01/post-46.html
関連記事	● 新たに 20 件のサイト改ざんが明らかに～新規改ざんサイト一覧（So-net） http://www.so-net.ne.jp/security/news/library/2129.html

39. 東大大学院教育学研究科のサイトが改ざん被害に

関連記事	● 東大大学院教育学研究科のサイトが改ざん - 閲覧者にウイルス感染のおそれ（Security NEXT） http://www.security-next.com/011898.html

40. 中小企業基盤整備機構の関連サイトが改ざん被害に

ニュースリリース	● 中小機構インキュベーション施設の一部ホームページに関するご報告とお詫び（中小企業基盤整備機構） http://www.smrj.go.jp/kikou/news/051503.html
関連記事	● 中小企業基盤整備機構の関連サイトが改ざん - 複数施設の紹介ページが被害（Security NEXT） http://www.security-next.com/011899.html

41. 原子燃料リサイクル施設の研修施設サイトが改ざん被害に

ニュースリリース	● ウイルス感染へのお詫びおよび対処方法について（青森原燃テクノロジーセンター） http://www.agtcinc.co.jp/info2010.html
関連記事	● 原子燃料リサイクル施設の研修施設サイトが改ざん被害（Security NEXT） http://www.security-next.com/011921.html

42. 「なみはやスポーツネット」サイトが改ざん被害に

ニュースリリース	● 「なみはやスポーツネット」ガンブラーの感染について（大阪府） http://www.pref.osaka.jp/hodo/index.php?site=fumin&pageId=2847
関連記事	● サイト改ざん止まず(2) 改ざんサイト告知一覧（2010 年 1 月 14 日～1 月 28 日）（So-net） http://www.so-net.ne.jp/security/news/library/2139.html

43. まほろば・けいはんな 科学ネットワークサイトが改ざん被害に

ニュースリリース	● 【重要・要確認】ホームページ公開停止連絡（まほろば・けいはんな 科学ネットワーク） http://mk-kagaku.seesaa.net/article/139597723.html
関連記事	● サイト改ざん止まず(2) 改ざんサイト告知一覧（2010 年 1 月 14 日～1 月 28 日）（So-net） http://www.so-net.ne.jp/security/news/library/2139.html

44. 自民党衆議院議員・岸田文雄氏サイトが改ざん被害に

ニュースリリース	● お詫び（岸田文雄ホームページ） http://www.kishida.gr.jp/news.html
関連記事	● サイト改ざん止まず(2) 改ざんサイト告知一覧（2010 年 1 月 14 日～1 月 28 日）（So-net） http://www.so-net.ne.jp/security/news/library/2139.html

45. 公立学校共済組合奈良宿泊所「春日野荘」サイトが改ざん被害に

ニュースリリース	● 公立学校共済組合奈良宿泊所「春日野荘」ホームページに関する報告とお詫び（公立学校共済組合） http://www.kouritu.go.jp/topics/etc/kaizan/index.html
関連記事	● サイト改ざん止まず(2) 改ざんサイト告知一覧（2010 年 1 月 14 日～1 月 28 日）（So-net） http://www.so-net.ne.jp/security/news/library/2139.html

46. 東急ステイサービスサイトが改ざん被害に

関連記事	● 「Gumblar 亜種」による改ざんで約 4 週間にわたり危険な状態に - 東急ステイ（Security NEXT） http://www.security-next.com/011937.html

47. スタービューティーサイトが改ざん被害に

関連記事	● 美容ポータル「スタービューティー」が「Gumblar 亜種」による改ざん（Security NEXT） http://www.security-next.com/011959.html

48. リーダー電子サイトが改ざん被害に

ニュースリリース	● ホームページに関するお詫びとお願い（リーダー電子） http://www.leader.co.jp/company/t_100201.html
関連記事	● サイト改ざんで閲覧者にウイルス「Gumblar」感染の可能性 - 電子計測器メーカー（Security NEXT） http://www.security-next.com/011956.html

49. 「ゴーギャン展 2009」サイトが改ざん被害に

関連記事	● 東京国立近代美術館で開催された「ゴーギャン展 2009」のサイトが改ざん（Security NEXT） http://www.security-next.com/011976.html

50. オーク情報システムサイトが改ざん被害に

ニュースリリース	● Net Evidence サイトの改ざんに関するお詫びとお知らせについて（オーク情報システム） http://www.oakis.co.jp/topics/news/2010/01/netevidence.php
関連記事	● フォレンジック製品の紹介サイトが改ざん被害 - オーク情報システム（Security NEXT） http://www.security-next.com/011988.html

51. エヌイーホールディングスサイトが改ざん被害に

関連記事	● サイト改ざんで閲覧者にウイルス感染の可能性 - 愛知や三重で展開する進学塾（Security NEXT） http://www.security-next.com/011984.html

52. 遠鉄百貨店関連サイトが改ざん被害に

ニュースリリース	● 弊社ホームページに関するお詫びとお知らせ（遠鉄百貨店） http://www.endepa.com/osirase/osirase.html
関連記事	● 遠鉄百貨店サイト、12 月に発生した改ざんを公表 - 浜松市情報サイトも被害（Security NEXT） http://www.security-next.com/012016.html

53. エースデュースサイトが改ざん被害に

ニュースリリース	● 【お詫び】ホームページへの不正アクセスの発生について（エースデュース） http://www.acedeuce-ent.jp/topics.html
関連記事	● Gumblar 亜種でサイトが 3 カ月以上改ざん状態に - ウェッジ HD 子会社（Security NEXT） http://www.security-next.com/012030.html

54. 雇用・能力開発機構サイトが改ざん被害に

ニュースリリース	● 【当センターホームページ「仕事おためし訓練コース・概要」に関するお詫びとお知らせ】（雇用・能力開発機構大阪センタ） http://www.ehdo.go.jp/OSAKA/data/H22.01.29.pdf
関連記事	● 職業訓練の案内ページが改ざん、閲覧でウイルス感染のおそれ - 雇用・能力開発機構（Security NEXT） http://www.security-next.com/012033.html

55. ネッツトヨタ南国サイトが改ざん被害に

ニュースリリース	● ネッツトヨタ南国ホームページに関するお詫びとお知らせ（ネッツトヨタ南国） http://www.vistanet.co.jp/info.htm
関連記事	● トヨタ系ディーラーのサイトが改ざん - 閲覧でウイルス感染の可能性（Security NEXT） http://www.security-next.com/012058.html

56. トヨタレンタリース東京サイトが改ざん被害に

ニュースリリース	● 株式会社トヨタレンタリース東京　ホームページに関する報告とお詫び（トヨタレンタリース東京） http://www.toyota-rl-tyo.co.jp/frameset/navi_news.html
関連記事	● トヨタレンタリース東京のサイトが改ざん - 委託先が「Gumblar 亜種」感染（Security NEXT） http://www.security-next.com/012067.html

57. 好学出版算数・数学思考力開発センタサイトが改ざん被害に

ニュースリリース	● お詫び　ホームページに関する報告とお詫び（好学出版算数・数学思考力開発センタ） http://www.iml-suken.com/owabi.html
関連記事	● 算数・数学思考力検定の資料請求ページなどが改ざん - 閲覧でウイルス感染のおそれ（Security NEXT） http://www.security-next.com/012071.html

58. 創都グループ校友会サイトが改ざん被害に

ニュースリリース	● ホームページに関するお詫びとお知らせ（校友会） http://www.souto-group.jp/news/20100215.html
関連記事	● サイト改ざんで閲覧者にウイルス感染の可能性 - 専門学校の同窓組織（Security NEXT） http://www.security-next.com/012135.html

59. 丸吉サイトが改ざん被害に

ニュースリリース	● 弊社ホームページ改ざんに関するお詫びとご報告（丸吉） http://www.askulnet.com/owabi.pdf
関連記事	● 1月に発生していたサイト改ざんを公表 - アスクル代理店（Security NEXT） http://www.security-next.com/012143.html

60. ダイナエアーサイトが改ざん被害に

ニュースリリース	● 弊社ホームページにおけるコンピューターウイルス・ガンブラー に対するお知らせ（ダイナエアー） http://www.dyna-air.jp/news100225.html

61. トップサイトが改ざん被害に

ニュースリリース	● 弊社 WEB サイトに関するお詫びとお知らせ（トップ） http://www.oa-top.co.jp/topics/2010/03/web.html
関連記事	● サイト改ざんで閲覧者にウイルス感染の可能性 - 名古屋の通信サービス会社（Security NEXT） http://www.security-next.com/012204.html

62. 神戸市に関連する複数サイトが改ざん被害に

ニュースリリース	● ホームページのウイルス感染（神戸市） http://www.city.kobe.lg.jp/information/press/2010/03/2010031206003.html
関連記事	● 複数の神戸市関連サイトが「Gumblar」により改ざん - 改ざん期間は調査中（Security NEXT） http://www.security-next.com/012234.html

63. インフォバーンサイトが改ざん被害に

ニュースリリース	● 弊社自社サイトに関するお詫びとお知らせ（インフォバーン） http://www.infobahn.co.jp/news/3073 http://www.infobahn.co.jp/news/3075
関連記事	● 改ざんで閲覧者にウイルス感染のおそれ - インフォバーン（Security NEXT） http://www.security-next.com/012329.html

3.3. 新種ウイルス情報

当期間確認された新種ウイルス情報は以下の通りです。

1. Googleなどを狙う攻撃コードが流出、McAfeeが警戒を呼びかけ

ニュースリリース	● McAfee Offers Guidance and Protection as China-Linked Google Cyberattack Continues to Unfold（McAfee） http://www.businesswire.com/portal/site/home/permalink/?ndmViewId=news_view&newsId=20100116005026&newsLang=en
関連記事	● Google などを狙う攻撃コードが流出、McAfee が警戒を呼びかけ（IT media） http://itpro.nikkeibp.co.jp/article/NEWS/20100118/343297/

2. 偽のMS通知でマルウェアに多重感染、欧米で被害拡大

ニュースリリース	● Thirteen Percent of Systems in US Infected by Flammable ZBot Malware Cocktail（bit defender） http://news.bitdefender.com/NW1294-en--Thirteen-Percent-of-Systems-in-US-Infected-by-Flammable-ZBot-Malware-Cocktail.html
関連記事	● 偽の MS 通知でマルウェアに多重感染、欧米で被害拡大（IT media） http://www.itmedia.co.jp/enterprise/articles/1001/20/news044.html

3. 高 IQ 集団「MENSA」の情報を騙るマルウェアスパム

関連記事	● 地獄か らの天使、というよりマルウェアの天使・・・（Panda Security Blog） http://pandajapanblogs.blogspot.com/2010/01/blog-post_28.html

3.4. 脆弱性情報

当期間確認された主な脆弱性情報は以下の通りです

1. 「PDFファイルに要注意」、ADOBE READERの脆弱性を突くウイルス出回る

ニュースリリース	● Security updates available for Adobe Reader and Acrobat（Adobe） http://www.adobe.com/support/security/bulletins/apsb10-02.html
関連記事	● Adobe Reader 及び Acrobat の脆弱性に関する注意喚起（JPCERT/CC） https://www.jpcert.or.jp/at/2010/at100003.txt ● Adobe Reader および Acrobat の脆弱性(APSB10-02)について（IPA） http://www.ipa.go.jp/security/ciadr/vul/20100113-adobe.html

2. Microsoft Internet Explorer の未修正の脆弱性に関する注意喚起

ニュースリリース	● マイクロソフト セキュリティ アドバイザリ (979352)（マイクロソフト） http://www.microsoft.com/japan/technet/security/advisory/979352.mspx ● マイクロソフト セキュリティ情報 MS10-002 - 緊急（マイクロソフト） http://www.microsoft.com/japan/technet/security/bulletin/ms10-002.mspx
関連記事	● Microsoft Internet Explorer の未修正の脆弱性に関する注意喚起（JPCERT/CC） https://www.jpcert.or.jp/at/2010/at100004.txt ● Internet Explorer の脆弱性(MS10-002)について（IPA） http://www.ipa.go.jp/security/ciadr/vul/20100122-ms10-002.html

3. マイクロソフト、Internet Explorerの新たな脆弱性で調査開始--情報流出の恐れ

ニュースリリース	● Microsoft Security Advisory (980088)（マイクロソフト） http://www.microsoft.com/technet/security/advisory/980088.mspx
関連記事	● マイクロソフト、Internet Explorer の新たな脆弱性で調査開始--情報流出の恐れ（CNET Japan） http://japan.cnet.com/news/sec/story/0,2000056024,20408013,00.htm

4. Windows XP/2000 のVBScriptに脆弱性、MSがアドバイザリを公開

ニュースリリース	● マイクロソフト セキュリティ アドバイザリ (981169)（マイクロソフト） http://www.microsoft.com/japan/technet/security/advisory/981169.mspx
関連記事	● Windows XP/2000 の VBScript に脆弱性、MS がアドバイザリを公開（INTERNET Watch） http://internet.watch.impress.co.jp/docs/news/20100302_352125.html

5. オープンソースのSNSソフト「OpenPNE」に「なりすまし」の脆弱性

ニュースリリース	● マイクロソフト セキュリティ アドバイザリ (981169)（マイクロソフト） http://www.microsoft.com/japan/technet/security/advisory/981169.mspx
関連記事	● オープンソースの SNS ソフト「OpenPNE」に「なりすまし」の脆弱性（Security NEXT） http://www.security-next.com/012180.html ● 「OpenPNE」におけるセキュリティ上の弱点（脆弱性）の注意喚起（IPA） http://www.ipa.go.jp/security/vuln/alert/201003_openpne.html

6. IE 7/6 に新たな脆弱性、既に標的型攻撃も

ニュースリリース	● マイクロソフト セキュリティ アドバイザリ (981374)（マイクロソフト） http://www.microsoft.com/japan/technet/security/advisory/981374.mspx
関連記事	● IE 7/6 に新たな脆弱性、既に標的型攻撃も（INTERNET Watch） http://internet.watch.impress.co.jp/docs/news/20100310_353760.html

4. 総括

前回のレポートより確認されている Gumblar（亜種）攻撃の被害が今期間一層増加しています。被害状況は様々で、攻撃感知が遅れ被害予想が増大とされる例も見受けられるようです。また、Gumblar 自体次々と感染方法を変えていますので、Web 管理者含めインターネットユーザには状況の迅速な把握や対策方法の共有等していただき、攻撃に備えておく事をお薦め致します。

感染方法が多岐に渡るGumblarは、Adobeのゼロデイ脆弱性やJavaの脆弱性まで悪用し感染範囲を広げようとしています。そもそもGumblar自体「Web感染型ウイルス」と呼ばれ、悪意のあるコードが埋め込まれたサイトを見ただけで感染してしまう恐れがあるウイルスです。これは、感染したユーザが別のWebサイトの管理者の場合、Webサイトを管理するためのIDやパスワードが搾取され、ウイルスを含みWebページへと改ざんされてしまいます。その結果、Webページを閲覧したユーザが新たにウイルスに感染してしまいます。この結果、例えばマイクロソフトから提供されているセキュリティパッチをインストールしていないPCやアンチウイルスソフトがインストールされていないPCはたちまち感染の危険性が飛躍的に高くなってしまいます。これは、ごく一般的なユーザが気づかないうちに感染被害に遭い感染を助長してしまう行為になりかねます。対岸の火事と捉えずにインターネットにアクセスする全てのPCのセキュリティ状況を再度チェックしてください。[1]

マイクロソフトから提供されているセキュリティパッチとは、ソフトウェアに悪意ある活動が可能となる「弱点」が確認された際に提供される修正プログラムで、月に一度の定例・緊急を要する際の定例外での提供がなされており、この提供パッチを所有 PC にインストールすることにより、弱点を取り除くというものです。このセキュリティパッチとは、マイクロソフトに限らず各ベンダより提供されています。現時点でセキュリティパッチを PC にインストールされてないユーザは、早急にインストールする必要があります。なぜなら、脆弱性情報は公開された時点で悪意ある犯罪者にもその詳細が知られる事になり、その弱点を悪用した攻撃である「ゼロデイ攻撃」の標的になりかねないからです。

[1] Gumblar 被害の対策は多岐に渡ります。詳しくは各ベンダやセキュリティ関連サイトをご参照下さい。

情報化社会が益々高度化していく中で、犯罪者も悪意のある活動で利益を得ようと躍起になっています。事実、悪意ある活動はビジネスとして成り立っており、様々な方法でユーザをウイルスに感染させ利益を得たり、感染した PC を使用して国家レベルでのサイバーテロを実施しています。より一層の安全なインターネットライフの為にも、こちらから歩み寄り、情報化社会の促進に繋げていく必要が望まれます。

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