

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA256

各位

<<< 冬期の長期休暇を控えて 2010/12 >>>

JPCERT/CC

2010-12-16

冬期の長期休暇期間におけるコンピュータセキュリティインシデント発生の予防および緊急時の対応に関して、再確認していただきますようお願い致します。

#### I. Web サイトの閲覧や短縮 URL のアクセスに注意を

JPCERT/CC では、Web サイトや Web サイト内で利用される広告配信・アクセス解析サービスなどのサーバが改ざんされる事例に関するインシデント報告を受けています。

これらの攻撃では、日常利用される一般的な Web サイトが攻撃の入り口となっています。

また、12 月には Twitter などでも利用される短縮 URL を使った攻撃が確認されています。短縮 URL を使用した攻撃では、アクセス先のサイトがどのようなサイトかを事前に確認することが困難なため、不用意にアクセスしてしまうと、攻撃者が用意した攻撃用のサイトに誘導されてしまう危険性があります。

JPCERT/CC で確認したこれまでの攻撃の多くは既知の脆弱性が使用されていました。このため、業務で使用している PC はもちろんのこと、休暇期間中に自宅で使用する PC の OS やソフトウェアについても、最新の状態に更新することで、攻撃の影響を受ける可能性を低減することができます。また、PC で使用しているウイルス対策ソフトの定義ファイルが自動更新される設定になっていること、ウイルス対策ソフトの有効期限が切れていないことを併せて確認してください。

#### II. 休暇前の対応

長期休暇に入る前に、以下の点について改めて対策を確認してください。

##### [全般]

- 緊急時の連絡網が整備・周知されていることを確認する
- 休暇中に使用しない機器の電源を切る

##### [システム管理者向け]

- ベンダのサポートが切れている OS やソフトウェアを使用し続けていないか確認する
- 最新のセキュリティ更新プログラムが適用されていることを確認する
- 不要なサービスを無効にしているかどうか確認する
- 各種サービスへのアクセス権限を必要最低限に設定する
- 休暇時の業務遂行のために特別にシステムなどへのアクセス制御を変更する場合、通常の状態に戻す手順やスケジュール、およびそれに合わせた監視体制が整備されているか確認する

##### [一般社員、職員向け]

- 最新のセキュリティ更新プログラムが適用されていることを確認する
- 不要なプログラムがインストールされていないか確認する
  - ※ 一部メーカー製 PC では、初期状態で多数のソフトウェアがプリインストールされている場合がありますので、普段使用しないソフトウェアについてもこの機会にセキュリティ更新プログラムを適用してください。
- 名前や生年月日、電話番号、アカウントと同一のものなど、容易に推測できる脆弱なパスワードが設定されていないか確認する
- データを持ち出す際には、自組織のポリシーに従い、その取り扱いや情報漏えいに細心の注意を払う

※ 自宅の PC で P2P ファイル共有ソフトウェアを利用している場合、ウイルス感染によって自宅の PC から業務データなどの情報が漏えいする危険があることにご留意ください

例年、この時季にはクリスマスや年始の挨拶を装ったウイルス添付メールや攻撃用サイトに誘導する攻撃が発生します。JPCERT/CC では、これら攻撃の影響を低減するための電子メールソフトのセキュリティ設定に関する情報を公開しています。本情報を参考に、電子メールソフトの設定を今一度ご確認ください。

電子メールソフトのセキュリティ設定について

<https://www.jpcert.or.jp/magazine/security/mail/index.html>

### III. 休暇明けの対応

休暇明けは、以下の点について確認してください。

[システム管理者向け]

- 導入している機器やソフトウェアについて、休暇中にセキュリティ更新プログラムが公開されていないかどうか確認し、更新プログラムが公開されていた場合は、更新プログラムを適用する
- 一般社員、職員に対して、休暇中に持ち出していた PC を組織内のネットワークに接続する前に、ウイルスチェックするように周知する（確認用のネットワークを別途用意するなど）

[一般社員、職員向け]

- 休暇期間中に持ち出していた PC や USB メモリは、事前にウイルスチェックを行った上で使用する
- USB メモリは、自動実行機能を停止した上で PC に接続し、ウイルス対策ソフトで USB メモリ内のファイルをウイルスチェックする
- 社内ネットワーク経由でウイルス感染が拡大した場合を考慮し、入社後すぐにウイルス対策ソフトの定義ファイルを最新の状態に更新する

### IV. JPCERT/CC への報告のお願い

JPCERT/CC では、フィッシングサイトや改ざんされた Web サイト、不正なプログラムの配布サイトなどに対して、関係機関を通じて調整活動を行っています。もし、これらに関する情報をお持ちの場合は、以下の Web フォームまたは電子メールで、JPCERT/CC までご連絡ください。

Web フォーム: <https://form.jpcert.or.jp/>

電子メール: [info@jpcert.or.jp](mailto:info@jpcert.or.jp)

\* インシデントの報告についてはこちらをご参照ください

<https://www.jpcert.or.jp/form/>

### V. 参考情報:

インシデント報告対応四半期レポート

<https://www.jpcert.or.jp/ir/report.html>

Adobe Acrobat、Adobe Reader

Adobe.com – New downloads

<http://www.adobe.com/support/downloads/new.jsp>

Adobe Flash Player

以下の URL にて Flash Player のバージョンを確認してください。

Adobe Flash Player:Version Information

<http://www.adobe.com/jp/software/flash/about/>

Adobe Flash Player のインストール

<http://get.adobe.com/jp/flashplayer/>

Java/JRE

Java ソフトウェアのインストール状況の確認

<http://www.java.com/ja/download/installed.jsp>

全オペレーティングシステムの Java のダウンロード一覧

<http://java.com/ja/download/manual.jsp?locale=ja&host=java.com>

※ Java を最新に更新した場合、一部の Java 上で動作するアプリケーションが動作しなくなる可能性があります。利用するアプリケーションへの影響を考慮した上で、更新を適用してください。

Microsoft Windows / Office

Microsoft Update

<https://www.update.microsoft.com/>

Windows Update

<https://windowsupdate.microsoft.com/>

QuickTime

QuickTime - ダウンロード

<http://www.apple.com/jp/quicktime/>

RealPlayer

RealPlayer

<http://jp.real.com/?mode=rp>

以上

=====

一般社団法人 JPCERT コーディネーションセンター (JPCERT/CC)

MAIL: [info@jpcert.or.jp](mailto:info@jpcert.or.jp)

TEL: 03-3518-4600 FAX: 03-3518-4602

<https://www.jpcert.or.jp/>

-----BEGIN PGP SIGNATURE-----

iQEcBAEBCAAGBQJNCZLyAAoJEDF9I6Rp7OBIE2IH/2I/ITRP6Ihj2PzQpfs+KZkrAHy05KV834Y3QrxHTd  
PkruNb+NdZvAMnxJjn7UDdEIz7Q3ivfyUH31Mh8k2VbrJsV1sb3GjiRnqj+XaL/d/ENxyDS8NwD0wqjCKZi20  
p3p0agdkYxeW+YcAG8GzAAIXUZHINxQAR9QrqvVHFinoj3mHISUdPypGNHoskKrSYsvAF7DQqdr64IwWa  
peqkddUQ3yu6ndEFOEpP+k4z/WSZOdjiLltjz64sJ52vk0SGqk3Ya5cfJFov6nM+s9TpZHdtNHAtDrlww2VQyi  
L7+MRFMbsJeXWIC5TwEoVr99yuQ0k5t11B1EosJ+nzQWFJ2I==gNE8

-----END PGP SIGNATURE-----