ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●10～12月のインシデント報告、ポートスキャンが倍増…JPCERT/CC

http://internet.watch.impress.co.jp/docs/news/1038586.html
https://www.jpcert.or.jp/pr/2017/IR_Report20170111.pdf

このニュースをザックリ言うと・・・

- 1月11日（日本時間）、セキュリティ専門機関である一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）より、2016年10月1日～2016年12月31日に報告を受けたインシデントの報告対応レポートが発表されました。

- 報告を受けたインシデントの数は4036件（7～9月期から29%増）、報告に対応して国内外のサイトとの調整を行った件数は2883件（同36%増）となっています。

- インシデントのうちポートスキャンは2177件（同98%増）で、スキャンされたポートの上位に挙げられているのは「22(SSH)」「25(SMTP･メール)」「80(HTTP･Web)」となっています。

AUS便りからの所感等

- ポートスキャンで、メールやWeb関係以上にターゲットとなったのはSSHであり、現代ではLinuxサーバ等へログインするためや、FTPに代わるファイルのアップロードのために用いられるようになっています。

- 他のサービスと異なり、SSHは不特定多数からのアクセスを受け付ける必要がないため、ポートを22番ポートから変更するだけでポートスキャンを回避し、攻撃者の感知をある程度避けられることが期待できます。

- ただし、スキルが高く執念深い攻撃者は、本来異なるポートであっても何らかのサービスがあることを探り出すことでしょうし、他のサービスも含め、同じIPアドレスからの頻繁なアタックを遮断する等の防御をサーバ自体の設定やUTMの設置により固めることを強く推奨します。

INTERNET Watch

ニュース

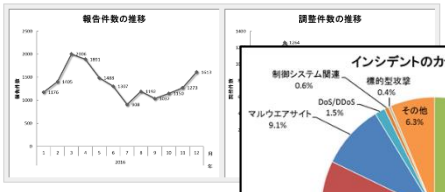
10～12月のインシデント報告、ポートスキャンが倍増、標的型攻撃は1.5倍に～JPCERT/CC

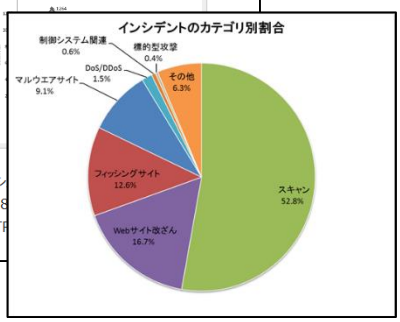
岩崎 宰守　2017年1月11日 19:05

ツイート リスト いいね！27 シェア B! 5 Pocket 17

一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）は11日、2016年10～12月に報告を受けたインシデントをまとめた「インシデント報告対応レポート」を公表した。

報告を受けたインシデントの数は4036件で、7～9月期から29%増加した。報告されたインシデントの総数は4122件。報告に対応してJPCERT/CCが国内外のサイトとの調整を行った件数は2883件で、36%増となった。





インシデントをカテゴリー別で見ると、シ
が2177件（52.8%）で、7～9月期からは98
となったポートは、SSH（22/TCP）、SMT
げられる。

JPCERT/CC

JPCERT-IR-2016-04
発行日: 2017-01-11

JPCERT/CC インシデント報告対応レポート
[2016 年 10 月 1 日 ～ 2016 年 12 月 31 日]

1. インシデント報告対応レポートについて

一般社団法人 JPCERT コーディネーションセンター（以下「JPCERT/CC」といいます。）では、国内外で発生するコンピュータセキュリティインシデント（以下「インシデント」といいます。）の報告を受け付けています(注1)。本レポートでは、2016 年 10 月 1 日から 2016 年 12 月 31 日までの間に受け付けたインシデント報告の統計および事例について紹介します。

（注 1）「コンピュータセキュリティインシデント」とは、本稿では、情報システムの運用におけるセキュリティ上の問題として捉えられる事象、コンピュータのセキュリティに関わる事件、できごとの全般をいいます。

JPCERT/CC
拡大の抑止に
トについて
を行ってい

［表 2 カテゴリ別インシデント件数］

インシデント	10 月	11 月	12 月	合計	前四半期合計
フィッシングサイト	139	185	197	521	467
Web サイト改ざん	180	314	194	688	554
マルウエアサイト	110	116	150	376	337
スキャン	709	679	789	2177	1098
DoS/DDoS	59	2	0	61	54
制御システム関連	3	13	8	24	5
標的型攻撃	8	4	3	15	10
その他	73	96	91	260	276

●セキュリティ啓発キャンペーンサイトが改ざんされる

http://securityblog.jp/news/20161221.html

このニュースをザックリ言うと・・・

- 1月15日（日本時間）、フィッシング対策協議会より、同協議会が運営するWebサイト「STOP. THINK. CONNECT.」が改ざんの被害を受けたと発表されました。

- 同サイトは、海外のフィッシング対策ワークグループ等のセキュリティ団体と共同で行っている、インターネットを安全に使うための消費者向けセキュリティ普及啓発キャンペーンの日本版サイトとのことです。

- 1月20日現在、同協議会はサイトが改ざんを受けた原因を調査中とのことで、同サイトで使われているURLへのアクセスは同協議会のサイトへ飛ぶよう設定が変更されている模様です。

AUS便りからの所感等

- セキュリティ普及のためのサイトが改ざんの被害を受けたというインパクトに気を取られがちですが、Webサイトの改ざんは、大企業や大手サイトだけでなく、中小零細企業等に至るまで無差別に発生し得る点に注意が必要です。

- 改ざんに至る経路は、サイトへの直接侵入、CMS（コンテンツマネジメントシステム）への攻撃、管理者アカウントの乗っ取り等様々で、少しでもそういった経路での攻撃を食い止められるよう、アンチウイルスやUTMの導入等による防御を固めることが重要です。


INTERNET Watch
ニュース
「STOP. THINK. CONNECT.」日本版サイト、第三者からの不正アクセスで改ざん
岩崎 宰守　2017年1月16日 12:15
ツイート　リスト　いいね！ 34　シェア　B! 13　Pocket 30
フィッシング対策協議会は15日、「STOP. THINK. CONNECT.」の日本版ウェブサイトが、第三者からの不正アクセスにより改ざんされたことを公表した。
現在、米国の「STOP. THINK. CONNECT.」と共同で調査が進められており、原因調査と対応が終了するまで、サイトへのアクセスを控えるよう呼び掛けている。16日正午現在、同サイトへアクセスを試みると、フィッシング対策協議会のウェブサイトへリダイレクトされる。
STOP. THINK. CONNECT.は、米国の世界的なフィッシング対策ワーキンググループ「Anti-Phishing Working Group（APWG）」と米国のNational CyberSecurity Alliance（NCSA）が共同で行っているインターネットを安全に使うための消費者向けセキュリティ普及啓発キャンペーン。オバマ大統領の声明により「National Cyber Security Awareness Campaign」として認められている。
日本版サイトでも、インターネットへアクセスする前に、その危険性について「立ち止まる 考える 楽しむ」意識を持つことをユーザーに呼び掛けるための情報を提供している。フィッシング対策協議会のほか、2016年1月時点で20の企業や組織が活動に参加している。

●「よく使われるパスワード」2016年の1位はまた「123456」

http://www.itmedia.co.jp/enterprise/articles/1701/17/news073.html

このニュースをザックリ言うと・・・

- 1月13日（現地時間）、パスワード管理ツールなどを提供する米Keeper Security社より、2016年に最もよく使われたパスワードのランキングが発表されました。

- 最も多いのが「123456」、次いで「123456789」「qwerty」「12345678」「111111」等と、ほとんどが数字の羅列やキーボード上の配列順に打っただけの推測されやすいパスワードとなっています。

- 発表された上位25個のうち11個がわずか6文字のパスワードとなっており、同社では、こういった短いパスワードは、ブルートフォースアタック（総当たり攻撃）により、ものの数秒で破られる恐れもあるとして警告しています。

AUS便りからの所感等

- 昨年も同様のランキングを同業他社が発表していますが、やはり1位は「123456」となっており、ここ何年かはこの傾向が変わらず続いているようです（AUS便り 2016/01/25号参照）。

- 上位に挙げられているパスワードを使っているユーザは、真っ先に攻撃者にこれらのパスワードを試され、不正ログインされることでしょうし、これと似ていたり、ちょっと変えただけのパスワードを使っている場合も、やはり格好のターゲットとなり得ます。

- とにかく根本は、他人から推測されにくい、ある程度以上複雑なパスワードを設定することが重要です。


ITmedia エンタープライズ
2017年01月17日 09時22分 更新
安易なパスワードの2016年版ランキング発表、ユーザー啓発はもう限界？
安易なパスワードの筆頭格「123456」は約17%ものユーザーが使っていたほか、「123456789」「qwerty」などのパスワードが依然として上位を独占している。
[鈴木聖子，ITmedia]
91　86　86　21　22　6
2016年の最もありがちなパスワー
掛けるKeeper Securityが1月13日の
し指摘されているにもかかわらず、こ
年も変わっていないといい、「ユーザ
いる。
同社は2016年に起きた情報流出事案で発覚した1000万のパスワードを分析してワーストランキングを作成した。
その結果、最も多かった「123456」は約17%ものユーザーが使っていたほか、「123456789」「qwerty」「12345678」「111111」などの安易なパスワードが依然として上位を独占。1000万件のパスワードのうち半数以上を、上位25件のパスワードが占めていた。
この数年、多数のユーザーがこうした安易なパスワードを使い続ける実態に変化はなく、「パスワードの弱さに起因する情報流出が後を絶たないにもかかわらず、これほど多くのWebサイト運営者が依然としてパスワードのベストプラクティスに従っていないことに当惑する」とKeeper Securityは述べている。
Top 25 Most Common Passwords of 2016

RANK	PASSWORD
1.	123456
2.	123456789
3.	qwerty
4.	12345678
5.	111111
6.	1234567890
7.	1234567
8.	password
9.	123123