— AUS（アルテミス・ユーザ・サポート）便り 2016/09/26号 —
http://www.artemis-jp.com

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。

●サイバー攻撃メールの81%は非公開アドレスに着弾…警察庁統計

http://www.itmedia.co.jp/enterprise/articles/1609/16/news057.html
https://www.npa.go.jp/kanbou/cybersecurity/H28_kami_jousei.pdf

このニュースをザックリ言うと･･･

- 9月15日（日本時間）、警察庁より、2016年上半期のサイバーセキュリティ脅威動向が発表されました。

- 警察が報告を受けたメール攻撃の件数は1951件で、前期（2015年下半期）の2356件から405件減となったとのことです。

- ただ、うち81%がネット上で公開していないメールアドレスに対して送信されたもので、攻撃者が攻撃対象の組織や職員について調査する等、周到な準備を行ったものと同庁では推測しています。

AUS便りからの所感等

- 非公開メールアドレスを使っている場合、SPAMメール等が来ないものと安心し、いざ第三者からの攻撃メールが来たときに油断して添付ファイル等を開けてしまうというシナリオが予想されます。

- アドレスの公開・非公開に拘らず、まずはUTM等によるメールチェック機能で攻撃メールを遮断する体制を整えること、また、それを回避して届いたメールに対しても不審な点がないかユーザが可能な限り注意を払うこと、さらには資料の添付や外部サイトへのアップロードについても一定のルールを設けると効果的でしょう。

- 発表ではこの他にも、インターネットとの接続点に設置したセンサーに対するアクセス件数が1日1IPアドレスあたり1119件（前期より346件増加）としており、ルータや監視カメラ等の探索ないしそれらを踏み台とした攻撃活動等が活発化していると結論付けています。

- こういったアクセスについても、機器の設定がセキュアなものか確認し、UTM等のファイアウォール機能によってアクセスを遮断するという多層防御が肝要です。

ITmedia エンタープライズ

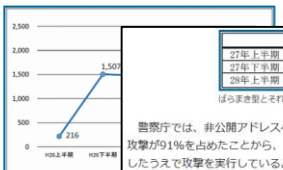
2016年09月16日 06時30分 更新

サイバー攻撃メールの81%は非公開アドレスに着弾――警察庁統計

2016年上半期のメール攻撃は1951件あり、「ばらまき型」以外の攻撃の占める割合が2倍近くに高まった。

[ITmedia]

警察庁は9月15日、2016年上半期のサイバーセキュリティ脅威動向を発表した。警察が報告を受けたメール攻撃は前期比で405件少ない1951件だったが、非公開アドレスに送り付けるものが81%を占めた。



メール攻撃の件数の推移（出典

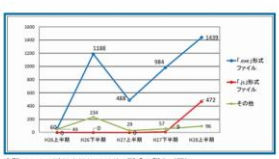
攻撃メールのうち、全体の85%（1667
特定の標的に送り付けたとみられる「ばら
前期、前々期の8%から2倍近くに増えてい

	ばらまき型	ばらまき型以外
27年上半期	92%（1,347件）	8%（ 125件）
27年下半期	92%（2,161件）	8%（ 195件）
28年上半期	85%（1,667件）	15%（ 284件）

ばらまき型とそれ以外のメール攻撃の割合（同）

警察庁では、非公開アドレスへの攻撃が81%を占め、送信アドレスを偽装したとみられる攻撃が91%を占めたことから、「攻撃者が対象の組織や職員について調査し、周到な準備をしたうえで攻撃を実行しているようだ」と指摘する。

攻撃メールに添付されるファイルは、圧縮されたものが99%を占めた。圧縮ファイルの中身は実行形式が最多だったものの、前期まではほとんどみられなかったJavaScriptが472ファイルと急増した。



攻撃メールに添付されたファイル形式の割合（同）

また、警察庁の監視センサーで検知された不審なアクセスは、1日・1IPアドレスあたり1119.1件の上り、前期から346.1件増加している。これらの多くは、Linux系OSを搭載したルータや監視カメラなど組み込み型機器への不正アクセスを探る通信とみられている。

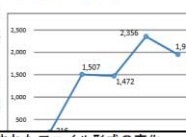
警察庁 National Police Agency

広　報　資　料
平成28年９月15日
警　　察　　庁

平成28年上半期におけるサイバー空間をめぐる脅威の情勢等について

1　サイバー攻撃の情勢等

○　警察が報告を受けた標的型メール攻撃は1,951件（前期比－405件）。
　このうち、これまでほとんど報告のなかった圧縮ファイルで送付された「.js」形式ファイルが472ファイルに急増。



○　攻撃ツールを用いて地方公共団体のサーバに対してDoS攻撃を行った少年を電子計算機損壊等業務妨害罪により検挙（５月、大阪）

○　伊勢志摩サミット等

重要インフラ事業者、

等と協力してサイバー

2　サイバー犯罪の情勢等

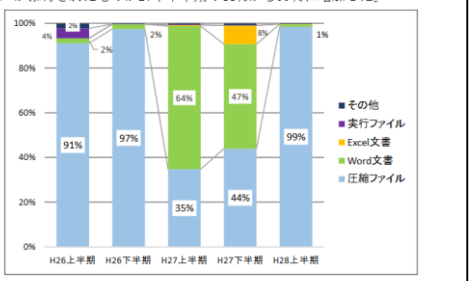
○　サイバー犯罪の検挙

○　金融機関等と連携し

犯による被害額は約９

○　違法中継サーバや海

○　標的型メールに添付されたファイル形式の変化
標的型メールに添付されたファイル形式の割合については、圧縮ファイルが添付されたものが27年下半期の44%から99%に増加した。



【標的型メールに添付されたファイル形式の割合】

●NASに侵入、PCに感染して仮想通貨を発掘するマルウェア

http://gigazine.net/news/20160914-nas-malware-mint-monero/

このニュースをザックリ言うと・・・

- 9月8日（現地時間）、アンチウイルス等を提供する英Sophos社より、NASに侵入してPCに感染しようとするマルウェアの存在が発表されました。

- 発表によると、マルウェアはSeagate社製NASに含まれるアプリケーションの脆弱性を突いてNASの共有フォルダに自らをアップロードし、誤ってクリックしたユーザのPCに感染、PC上で密かに仮装通貨Moneroの発掘作業を行うというものです。

- マルウェアに感染した端末は、日本を含む世界中において既に3000台以上が確認されているとのことです。

AUS便りからの所感等

- マルウェアが行う活動は、NASの脆弱性を突いての侵入と、PCへの感染、そして仮装通貨の発掘のみとされており、現在のところ致命的な被害をもたらすものではありませんが、より過激な行動を起こす亜種がいつ発生するとも限りません。

- 外部からのデータ書き込みを有効にしている等、NASのセキュリティ対策をユーザが怠っていることにより、今回のマルウェア等のサイバー犯罪に悪用される可能性がSophos社により指摘されています。

- 認証されたユーザのみがファイルの書き込み（および読み込み）ができるよう強固な設定を行う、ファームウェア等を最新にアップデートする、そして可能であればNASをUTMの奥の隔離されたネットワークに配置する、といった各種セキュリティ対策をとることが重要です。


GIGAZINE
2016年09月14日 09時05分00秒
SeagateのNAS経由で感染してひそかに仮想通貨を発掘させるマルウェアが発見される
ハードディスク大手のSeagateが製造するNASの脆弱性を突いて感染し、接続するPCのマシンパワーをこっそり仮想通貨の発掘ソースとして利用するマルウェアが発見されました。すでに1時間で8万8000ドル(約900万円)以上の仮想通貨が発掘されたと推測されています。
感染端末は日本を含む世界中に広がっており、すでに3000台以上の端末での感染が確認されています。

●米Yahoo!、2014年に5億人の個人情報流出していた

http://www.nikkei.com/article/DGXLASGM23H2M_T20C16A9MM0000/

このニュースをザックリ言うと・・・

- 9月22日（現地時間）、米Yahoo!社より、2014年後半に同社ネットワークから「Yahoo!」ユーザ少なくとも5億人分の個人情報が流出していたことが発表されました。

- 流出した個人情報は、名前・メールアドレス・電話番号・生年月日・ハッシュ化されたパスワードおよび秘密の質問と答（一部ユーザ）とされており、ハッシュ化されていないパスワード・クレジットカード・銀行口座情報は含まれていないとのことです。

- 同社は、この流出を引き起こした攻撃について「特定の国家が関与した可能性」を示唆し、FBI等捜査当局と協力しながら調査を進めるとしており、また、該当するユーザに対し、パスワードや秘密の質問の変更、および二段階認証等の使用を呼び掛けています。

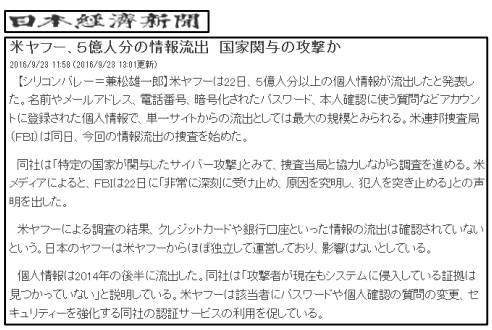
- なお、「Yahoo! JAPAN」については、日本のヤフー社により、影響はないと発表されています。

AUS便りからの所感等

- 大手ネットサービスからの大規模なアカウント情報流出については、5月にLinkedInから1億1700万人分、8月にもDropboxから6868万人分が流出していたことが発表されたばかりです（AUS便り 2016/09/12号参照）。

- 度々注意しているように、別のサービスでYahoo!と同じパスワードを使っている場合、連鎖的に不正ログインの被害を受ける可能性が高く、また、サービスを頻繁に利用せず、アカウントを作ったきり放置している場合、これもまた不正行為の温床となることでしょう。

- とにかく、アカウントを作成していたかどうか確認の上、速やかにパスワードを変更すること（もちろん、他のサービスでは使っていない、推測されにくいパスワードにすること）を推奨致します。


日本経済新聞
米ヤフー、5億人分の情報流出　国家関与の攻撃か
2016/9/23 11:58 (2016/9/23 13:01更新)
【シリコンバレー＝兼松雄一郎】米ヤフーは22日、5億人分以上の個人情報が流出したと発表した。名前やメールアドレス、電話番号、暗号化されたパスワード、本人確認に使う質問などアカウントに登録された個人情報で、単一サイトからの流出としては最大の規模とみられる。米連邦捜査局（FBI）は同日、今回の情報流出の捜査を始めた。
同社は「特定の国家が関与したサイバー攻撃」とみて、捜査当局と協力しながら調査を進める。米メディアによると、FBIは22日に「非常に深刻に受け止め、原因を究明し、犯人を突き止める」との声明を出した。
ヤフーによる調査の結果、クレジットカードや銀行口座といった情報の流出は確認されていないという。日本のヤフーは米ヤフーからほぼ独立して運営しており、影響はないとしている。
個人情報は2014年の後半に流出した。同社は「攻撃者が現在もシステムに侵入している証拠は見つかっていない」と説明している。米ヤフーは該当者にパスワードや個人確認の質問の変更、セキュリティーを強化する同社の認証サービスの利用を促している。