

11月中の主なセキュリティ関連ニュースをまとめたものをお届けします。

目次

脅威動向

- IoT機器を狙うボット「Reaper」、数百万台のネットワーク機器に感染
- Silence：ガンのように静かに広がる新たな標的型攻撃
- マルウェア「Mirai」の新型亜種が急増--日本でも感染被害か
- IoT機器を狙うウイルス感染 100倍に急増 先月から

トピックス

- 中小企業向けサイバーセキュリティの極意【注目】
- Twitter乗っ取りの有無を確認する方法と対策、今後の予防策
- 情報セキュリティ予算獲得の参考資料
- Androidの「パターンロック」認証は、のぞき見で簡単に破られることが判明
- 秘密の自撮り: iPhoneアプリはあなたが気づかない間に撮影可能
- スパイウェアが気になる方へ | 今すぐ有無を確認する方法と予防策
- 「ATMマルウェア」の実態とその攻撃手口に迫る
- サイバーセキュリティ経営ガイドラインの改定【注目】
- 「iPhone」を無線LANにつなぐだけでデータ流出の恐れ
- セキュリティを脅かす9つの「何となく」
- 「ファイルレス攻撃」が深刻化--ウイルス対策の見直しも
- 日本で流通する迷惑メール--4つのグループの特徴
- 「脆弱性体験学習ツール「AppGoat」を用いた集合教育実施の手引き」の公開
- サイバー犯罪者の狙いは「仮想通貨」に拡大、2017年第3四半期の脅威動向
- 社員のための抜け目ないショルダーハック対策と注意したい5つの事例

脅威動向 1

件名	IoT機器を狙うボット「Reaper」、数百万台のネットワーク機器に感染
出典	トレンドマイクロ
URL	http://blog.trendmicro.co.jp/archives/16282
内容	IoT機器を狙うボットが確認されています。報道では100万以上の法人ネットワークに感染し、更に感染を拡大しているとのことです。

件名	Silence：ガンのように静かに広がる新たな標的型攻撃
出典	カスペルスキー
URL	https://blog.kaspersky.co.jp/silence-financial-apt/18600/
内容	トロイの木馬を使って金融機関を狙う新たな標的型攻撃が発見されたとのことです。フィッシングメールで悪意のある添付ファイルが送られてくるようです。

件名	マルウェア「Mirai」の新型亜種が急増--日本でも感染被害か
出典	ZD Net Japan
URL	https://japan.zdnet.com/article/35110980/
内容	モノのインターネット（IoT）機器に感染するマルウェア「Mirai」の新たな亜種とみられる攻撃がセキュリティ企業「Qihoo 360」から報告されたとのことです。

件名	IoT機器を狙うウイルス感染 100倍に急増 先月から
出典	NHK
URL	http://www3.nhk.or.jp/news/html/20171126/k10011236191000.html
内容	日本国内でIoT機器を狙ったコンピューターウイルスの感染が100倍に急増しているとのことです。

トピックス 1

件名	中小企業向けサイバーセキュリティの極意【注目】
出典	東京都産業労働局
URL	http://www.sangyo-rodo.metro.tokyo.jp/chushou/shoko/cyber/iigyuu/guidebook/
内容	中小企業がサイバー攻撃について必ず行うべき対策や、事故が発生した場合の初期対応などをなるべく分かりやすく伝える内容のものです。

件名	Twitter乗っ取りの有無を確認する方法と対策、今後の予防策
出典	ノートン
URL	https://japan.norton.com/twitter-hacking-8709
内容	Twitter乗っ取りの手口や実態、乗っ取られていないかの確認方法、対策や予防策などについてまとめられています。

件名	情報セキュリティ予算獲得の参考資料
出典	カスペルスキー
URL	https://blog.kaspersky.co.jp/calculator-financial-report/17933/
内容	ビジネス上の意思決定者に対して情報セキュリティの重要性を客観的に説明するための資料などについてまとめられています。

件名	Androidの「パターンロック」認証は、のぞき見で簡単に破られることが判明
出典	WIRED
URL	https://wired.jp/2017/11/05/android-unlock-pattern-or-pin/
内容	スマホのロックなどで利用している方も多いパターンロックですが、6桁のパスワードに比べ、のぞき見による再現率が高く、破られやすいとのこと。

件名	秘密の自撮り: iPhoneアプリはあなたが気づかない間に撮影可能
出典	マカフィー
URL	http://blogs.mcafee.jp/secret-selfies-iphone-apps
内容	iPhoneには、携帯電話のカメラにアクセスできるアプリが前面で実行している時に、密かにユーザーの写真や動画を撮らせる機能があるとのこと。

トピックス 2

件名	スパイウェアが気になる方へ 今すぐ有無を確認する方法と予防策
出典	ノートン
URL	https://japan.norton.com/spyware-9127
内容	スパイウェアとは、どんな働きをするのか、スパイウェアが入っていないかどうか確認する方法、入り込まないための対策などについてまとめられています。

件名	「ATMマルウェア」の実態とその攻撃手口に迫る
出典	トレンドマイクロ
URL	http://blog.trendmicro.co.jp/archives/16318
内容	銀行のATMから現金を窃取するマルウェアに関する攻撃の手口や調査結果についてまとめられています。

件名	サイバーセキュリティ経営ガイドラインの改定 【注目】
出典	経済産業省
URL	http://www.meti.go.jp/press/2017/11/20171116003/20171116003.html
内容	サイバーセキュリティ経営ガイドラインが Ver2.0 に改訂されました。「事後対策」などが追加されています。

件名	「iPhone」を無線LANにつなぐだけでデータ流出の恐れ——脆弱性発見コンテストで判明
出典	TechTarget Japan
URL	http://techtarget.itmedia.co.jp/tt/news/1711/17/news06.html
内容	脆弱性発見コンテストの「Mobile Pwn2Own 2017」で、「iOS 11」の脆弱性を突いたハッキングが成功したとのこと。

件名	セキュリティを脅かす9つの「何となく」
出典	カスペルスキー
URL	https://blog.kaspersky.co.jp/nine-bad-online-habits/18730/
内容	日常の何気ない習慣の中ある、インターネットセキュリティにマイナスの影響を及ぼすものを紹介しています。

トピックス 3

件名	「ファイルレス攻撃」が深刻化--ウイルス対策の見直しも
出典	ZD Net Japan
URL	https://japan.zdnet.com/article/35110549/
内容	「ファイルレス攻撃」の脅威が問題化し、従来のセキュリティ対策を見直す動きが出始めているとのことです。

件名	日本で流通する迷惑メール--4つのグループの特徴
出典	ZD Net Japan
URL	https://japan.zdnet.com/article/35110995/
内容	国内で毎日大量に出回る迷惑メールは、送信元や手口などの特徴から4つのグループに大別できるとのことです。

件名	「脆弱性体験学習ツール「AppGoat」を用いた集合教育実施の手引き」の公開
出典	IPA
URL	https://www.ipa.go.jp/security/vuln/appgoat/
内容	社員教育などで活用できる脆弱性体験学習ツールの手引きが公開されています。

件名	サイバー犯罪者の狙いは「仮想通貨」に拡大、2017年第3四半期の脅威動向を分析
出典	トレンドマイクロ
URL	http://blog.trendmicro.co.jp/archives/16533
内容	仮想通貨発掘ツール（コインマイナー）のような比較的穏やかな金銭獲得手法も目立っているとのことです。

件名	社員のための抜け目ないショルダーハック対策と注意したい5つの事例
出典	マカフィー
URL	http://blogs.mcafee.jp/shoulder-surfing-protect
内容	重要な情報をのぞき見る「ショルダーハック」とその対策などがまとめられています。