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。

●仮想通貨取引所Coincheck、不正アクセスにより約580億円分の仮想通貨流出

http://nlab.itmedia.co.jp/nl/articles/1801/26/news136.html
https://japan.cnet.com/article/35114125/
https://www.buzzfeed.com/jp/ryosukekamba/coincheck

このニュースをザックリ言うと･･･

- 1月26日（日本時間）、コインチェック社より、同社が運営する仮想通貨取引サイト「Coincheck」が不正アクセスを受け、同サイトで保有されていた仮想通貨「NEM(XEM)」が不正に外部に送金されたと発表されました。

- 流出したNEMは5億2300万NEMで、流出時点の時価は日本円で約580億円に相当するとされています。

- 不正アクセスは同日00:02頃から発生、11:25頃に異常が検知され、同日中に入出金および売買停止等の措置がとられています。

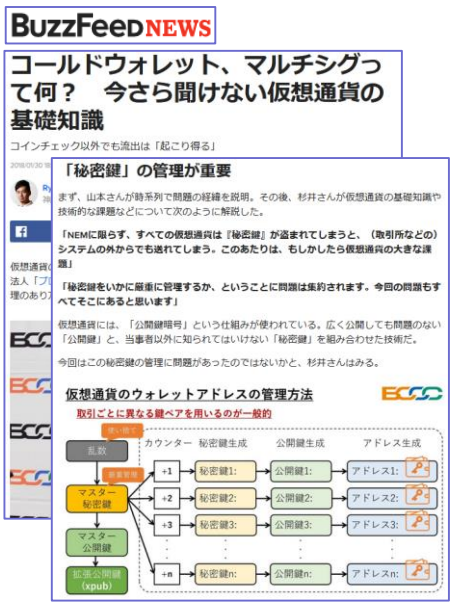
AUS便りからの所感等

- 仮想通貨の保管場所は専用デバイス等オフラインの「コールドウォレット」とオンラインの「ホットウォレット」とに大きく分類されますが、NEMはコールドウォレットの対応が遅れていたこともあり、主にホットウォレットで運用されていたことから標的にされたものとみられています。

- 加えて、Coincheckが仮想通貨の秘密鍵を分散管理する「マルチシグネチャ」を導入していなかったことも指摘されており、今回の不正アクセスはこの2つの要因が重なって発生したものと考えられます。

- 2014年に仮想通貨取引所「Mt.Gox」からのbitcoinの大量流出が発覚した際と同様、連日メディアで報道され、NEM以外の各種仮想通貨にも一時的な時価の値下がり等の影響が発生しています。

- このように、ある取引所でこういったセキュリティインシデントが発生することは、仮想通貨全体に大きなインパクトをもたらすものである一方、洗い出された問題点に対し他の取引所も含め対策が行われているかの見直しが着実に行われることに期待したいものです。



●設置1時間で覗き見…ウェブカメラ対策で警鐘

https://www3.nhk.or.jp/shutoken-news/20180126/0007039.html

このニュースをザックリ言うと・・・

- 1月26日（日本時間）、横浜国立大学の吉岡克成准教授らの研究グループより、WebカメラをはじめとするloT機器のセキュリティに関する実験結果が発表されています。

- 発表によれば、パスワードを設定していないカメラ4台と、パスワードは設定しているもののセキュリティ上の欠陥があるカメラ1台を設置し、アクセス状況を観察したところ、1ヶ月間で148の発信元からカメラへのアクセスによる映像の覗き見が行われ、うち33の発信元からカメラの向きを変えるなどの操作が行われたとのことです。

- こういったカメラの存在を自動的に探し出すプログラムにより、早ければ設置1時間後でアクセスされ、あるいはパスワードが破られたケースもあるとされています。

AUS便りからの所感等

- 2016年にWebカメラ等に感染しつつDDoS攻撃の為のネットワークを拡大していったマルウェアMirai等により、loT機器に対しても十分なセキュリティ保護を行う必要性が注目されています。

- Webカメラの他、複合機等についてインターネット上からアクセス可能な状態になっているものを探し出すサーチエンジンとして「SHODAN」「Censys」等が知られており、主に攻撃者がターゲットを探し出すために利用されていますが、一方で管理する側にとっても、外部からの不正アクセスの可能性がないか確認するための手段として有用です。

- 不特定多数から不正利用されないよう、推測されにくいパスワードの設定等の対策を行い、場合によっては外部からアクセスされる兆候がないか、第三者によるネットワーク診断を受けることも検討すべきでしょう。


NHK NEWS WEB

ウェブカメラ１時間でのぞき見も

01月26日　14時12分

自宅の様子などをインターネット経由で離れた場所から確認できる「ウェブカメラ」について、パスワードを設定しないなどの無防備な状態で設置すると、早いもので設置のわずか１時間後には何者かに映像をのぞき見られるとする実験結果がまとまり、研究グループはＩｏＴ機器のセキュリティ対策を入念に行うよう警鐘を鳴らしています。

ウェブカメラは、留守中の自宅や職場などを離れた場所から見ることが出来る便利さの一方、利用者がパスワードを設定しないなどセキュリティー対策を十分に行っていなかったり、セキュリティー上の欠陥がある製品もあったりするなどの課題が指摘されています。
このため、横浜国立大学の吉岡克成准教授らの研究グループは、パスワードを設定していないカメラ４台と、パスワードは設定しているもののセキュリティー上の欠陥があるカメラ１台を設置し、外部からの不審なアクセスを観察しました。
その結果、１か月あまりの間に１４８の発信元がカメラにアクセスして映像をのぞき見し、このうち３３の発信元はカメラの向きを変えるなどの操作まで行っていました。
さらに分析した結果、こうしたアクセスには無防備なカメラをインターネット上から自動で探し出すプログラムが使われ、早いものでは設置のわずか１時間後にのぞき見られたほか、別のカメラではパスワードを破る操作も自動で行われたおそれがあるということです。

●ソフトウェアの脆弱性情報、2017年は過去最多に…IPA集計

https://japan.zdnet.com/article/35113631/

このニュースをザックリ言うと・・・

- 1月24日（日本時間）、IPAより、同団体等が運営する脆弱性対策情報データベース「JVN iPedia」の登録状況について発表されました。

- 2017年に登録された情報の件数は13,792件で、2016年（6,524件）の2倍以上となり、2007年4月以降では過去最多だったとのことです。

- 同年第4四半期（10～12月）の件数は3,719件で、種類別で最も多かったのがバッファエラー（715件）、次いでクロスサイトスクリプティング（398件）、情報漏えい（371件）等となっています。

AUS便りからの所感等

- バッファエラーは、いわゆるバッファオーバーフローを含む、メモリの境界外への読み書きが可能になる脆弱性の総称で、悪用されるとサーバやPC上での悪意のあるコードの実行、データの盗聴あるいは改ざん等が行われる可能性があります。

- また、クロスサイトスクリプティング（XSS）はWebアプリケーションの脆弱性で、Webページの表示時に不正なスクリプトの実行などが行われ、表示あるいは入力された情報が外部に送信される等の可能性があります。

- 2017年における登録件数の急増は、個々の脆弱性につけられる世界標準の識別番号である「CVE」の登録に関するルールが改訂され、登録を行う機関が倍近くに増加したことが要因とされているものの、恐らくはプログラムミスによるセキュリティ上の問題が引き起こされるケースが依然として確認されている印象はあります。

- こういった脆弱性を突く攻撃はある程度パターンがあり、Webサーバ等の前面にIDS・IPSを設置することにより、事前に検知・遮断できるケースも少なくはありませんが、根本的に重要なのは、使用しているソフトウェアの脆弱性情報を定期的に調査し、常に最新バージョンに保つことです。


ZDNet Japan

ソフトウェアの脆弱性情報、2017年は過去最多に--IPA集計

ZDNet Japan Staff 2018年01月24日 15時05分

情報処理推進機構（IPA）は1月24日、同機構が運営するソフトウェアの脆弱性対策情報データベース「JVN iPedia」の登録状況を発表した。2017年の情報登録は前年比2倍以上の1万3792件に達し、2007年4月以降では過去最多だった。

2013年以降のJVN iPediaでの登録件数の推移（出典：IPA）