

URL	タイトル
1 https://japan.zdnet.com/article/35136960/	マイクロソフト、5月の月例パッチでインテル製CPUの不具合などに対処
2 https://japan.zdnet.com/article/35136562/	クレデンシャルスタッフィング攻撃とは？--その具体的手法
3 https://japan.zdnet.com/article/35137389/	GDPR施行から1年、世界のプライバシーとデータ保護を巡る状況をどう変えたか
4 https://japan.zdnet.com/article/35136362/	第4回：シナリオベースで進めてしまいうインシデント調査の問題点
5 https://japan.zdnet.com/article/35126123/	iOS向けのウイルス対策アプリが存在しない理由--カスヘルスキーが見解
6 https://japan.zdnet.com/article/35137134/	「月に50億件の脅威を検知」--マイクロソフトが明らかに
7 https://japan.zdnet.com/article/35136962/	インテル製プロセッサに対する新たな「MDS」攻撃、ベンダー各社の対応状況は
8 https://japan.zdnet.com/article/35136193/	東京五輪後の日本のIT世界--リスクを感じられない日本企業
9 https://japan.zdnet.com/article/35136885/	スニコ製品に影響する「Thrangrycat」脆弱性--研究者が報告
10 https://japan.zdnet.com/article/35137171/	ハクティビストによる攻撃が大幅減少、その理由とは--IBM調査
11 https://japan.zdnet.com/article/35136407/	人体を通信媒体とした「安全」なネットワーク技術--埋め込み型医療機器を守る新手法に期待
12 https://japan.zdnet.com/article/35137216/	トレンドマイクロのデバッグ関連情報が流出--サイバー攻撃報道に見解
13 https://japan.zdnet.com/article/35137309/	グループ、「G Suite」の一部パスワードを暗号化せず14年間も保存していた
14 https://japan.zdnet.com/article/35136217/	解説「ゼロトラスト」シフト--脱「境界セキュリティ」への3つの技術
15 https://japan.zdnet.com/article/35137653/	依然として100万台弱のWindowsシステムに「BlueKeep」の脆弱性
16 https://japan.zdnet.com/article/35137375/	「Android」端末や「iOS」端末を追尾する新手法--センサーのキャリブレーション情報を利用
17 https://japan.zdnet.com/article/3513748/	インテル製チップに新たな脆弱性「SPOILER」--修正は困難との指摘も
18 https://japan.zdnet.com/article/35133776/	いたずらスクリプトのURL貼った女子中学生の補導、海外でも波紋
19 https://japan.zdnet.com/article/35136610/	グループ、「Chrome」でクッキー機能を制限へ--サイトによるユーザー追跡の抑制でプライバシー改善図る
20 https://japan.zdnet.com/article/35137157/	Stack Overflowがセキュリティ侵害を公表
21 https://japan.zdnet.com/article/35137577/	サイバーセキュリティ関連の求人が急増、高収入はIT監査人--英Indeed調べ
22 https://japan.zdnet.com/article/35136950/	インテルのチップに新たな脆弱性--「Microarchitectural Data Sampling (MDS)」
23 https://japan.zdnet.com/article/35123791/	Wi-Fiパスワードを破る新たな攻撃手法が見つかる--「WPA」「WPA2」を無効に
24 https://japan.zdnet.com/article/35137367/	マイクロソフト製品のゼロデイ脆弱性情報、新たに2件がGitHub上で公開
25 https://japan.zdnet.com/article/35136544/	NEC、口座開設時の本人確認業務を支援--LINE Payが先行採用
26 https://japan.zdnet.com/article/35137299/	「Docker Hub」ポータル、著名コンテナの20%に設定ミス
27 https://japan.zdnet.com/article/35136675/	管理者の約50%が標準型メール訓練によって業務生産性の低下を実感
28 https://japan.zdnet.com/article/35135993/	ネット接続から1分未満でサイバー攻撃の標的に--ソフォスのおとり調査
29 https://japan.zdnet.com/article/35137279/	生体認証データの収集に関する法規制の動き、その影響を探る
30 https://japan.zdnet.com/article/35137511/	NSAから流出のハッキングツール、米都市への攻撃に悪用の可能性
31 https://japan.zdnet.com/article/35136966/	セキュアワークス社長に廣川氏が就任--「日本に根ざしたセキュリティ企業」へ
32 https://japan.zdnet.com/article/35136188/	よく使われている弱いパスワードは？--英NCSCが分析
33 https://japan.zdnet.com/article/35137438/	米圏にもEUのようなプライバシー規制を--MSの法務幹部がGDPRから1年で提言
34 https://japan.zdnet.com/article/35053866/	「Googleドライブ」のセキュリティを高める5つの方法
35 https://japan.zdnet.com/article/35136582/	JBSが「Microsoft Cloud App Security」のマネージドサービスを提供開始
36 https://japan.zdnet.com/article/35137226/	ハッキング依頼サービスの多くは詐欺？--グループら調査
37 https://japan.zdnet.com/article/35137027/	ロシア政府の複数のウェブサイトから225万人分の個人情報流出か--政府高官らの情報も
38 https://japan.zdnet.com/article/35136748/	シマンテック、第4四半期決算を発表--CEO交代も明らかに
39 https://japan.zdnet.com/article/35135224/	Apacheウェブサーバに脆弱性、パッチが公開--共有ホスト環境の管理者権限奪取を誘発
40 https://japan.zdnet.com/article/35134329/	圧縮・解凍ソフト「WinRAR」の脆弱性、さまざまな攻撃キャンペーンで悪用
41 https://japan.zdnet.com/article/35136388/	マイクロソフト、パスワードの定期的な変更は無駄と認める
42 https://japan.zdnet.com/article/35095393/	NISTが警告、SMSでの二段階認証が危険な理由
43 https://japan.zdnet.com/article/20368582/	IAMのキホンを理解する--第1回：IAMとは
44 https://japan.zdnet.com/article/35137263/	ジェムアルト買収のタレス、クラウド向けセキュリティ事業を展開
45 https://japan.zdnet.com/article/35136496/	日本のエンタープライズセキュリティ市場に進出するイーセット
46 https://japan.zdnet.com/article/35133878/	NSAがリバースエンジニアリングツール「Ghidra」を公開
47 https://japan.zdnet.com/article/35132132/	総務省、脆弱なIoT機器のセキュリティ対策を促す「NOTICE」を開始
48 https://japan.zdnet.com/article/35135778/	東京五輪後の日本のIT世界--「令和3年不況」は発生するののか
49 https://japan.zdnet.com/article/35137431/	入選管理システムのセキュリティチェックリストを公開--IPA
50 https://japan.zdnet.com/article/35137100/	米警察が顔認識技術を使った捜査に不完全な画像を使用か

■ 足元のセキュリティ動向は？パッチ当ては迅速に

この月は、比較的セキュリティを取り巻く状況としては落ち着いていたため、閲覧上位の記事については考察や情報収集に類するものが多くなった。

アクセストップは「**マイクロソフト、5月の月例パッチでインテル製CPUの不具合などに対処**」だが、既知の不具合に対する修正がメインだ。

「クレデンシャルスタッフィング攻撃とは？--その具体的手法」

この記事も読まれた。クレデンシャルスタッフィング攻撃は、ユーザー名とパスワードのリストを使い、様々なシステムやサービスへのログインを試行する攻撃手法だ。オンラインビジネスで現在、最も多く見かける脅威の1つでもある。エンドポイントのセキュリティは非常に重要であり、その対策は情報としてニーズが非常に高いのがわかる。

他にも、以下のように「セキュリティ戦略」に該当するような記事が読まれている。

- 「**GDPR施行から1年、世界のプライバシーとデータ保護を巡る状況をどう変えたか**」
- 「**第4回：シナリオベースで進めてしまいうインシデント調査の問題点**」

■ 脆弱性の情報は 引き続き多様なデバイス・システムに

とはいえ、多様なデバイス・システムにおいて、脆弱性は報告が続いている。記事は読まれているが、実際の国内企業のパッチ適用は海外に比べて遅いとの指摘があり、担当部署のパワー不足が懸念されるところだ。以下、MS・インテルの関連が この月はやや目立つ。

- 「**スニコ製品に影響する「Thrangrycat」脆弱性--研究者が報告**」
- 「**トレンドマイクロのデバッグ関連情報が流出--サイバー攻撃報道に見解**」
- 「**依然として100万台弱のWindowsシステムに「BlueKeep」の脆弱性**」
- 「**インテル製チップに新たな脆弱性「SPOILER」--修正は困難との指摘も**」
- 「**インテルのチップに新たな脆弱性--「Microarchitectural Data Sampling (MDS)」**」
- 「**マイクロソフト製品のゼロデイ脆弱性情報、新たに2件がGitHub上で公開**」

■ 中長期的な話題

2020年を節目として、今後のセキュリティをどうするといった記事は、国内・海外の情報 とともに読まれやすいようだ。

- 「**東京五輪後の日本のIT世界--リスクを感じられない日本企業**」
- 「**東京五輪後の日本のIT世界--「令和3年不況」は発生するののか**」
- 「**NISTが警告、SMSでの二段階認証が危険な理由**」
- 「**米圏にもEUのようなプライバシー規制を--MSの法務幹部がGDPRから1年で提言**」

■ ベンダ情報、事例関連記事

セキュリティベンダーの動向に関する記事は、この月は以下のようなところが読まれた。スマホ決済サービスで不正利用が多かったことが発覚したが、こうした動きに関する支援サービスが発表されている。素早く市場ニーズをつかむ動きも出ている。

- NEC、口座開設時の本人確認業務を支援--LINE Payが先行採用
- セキュアワークス社長に廣川氏が就任--「日本に根ざしたセキュリティ企業」へ
- JBSが「Microsoft Cloud App Security」のマネージドサービスを提供開始