

# 索引

## 記号・英数字

3.2.1 ルール.....	199
3389/tcp.....	47, 49, 104, 113, 250
443/tcp.....	124
445/tcp.....	47, 73, 108, 110, 122, 250
A41APT キャンペーン.....	95
Administrator.....	155
Affiliate.....	34, 41
AWS.....	49, 122
BlackCat.....	35, 39
Chrome.....	133
comsvcs.dll.....	70
CVE.....	129
CVE-2017-0145.....	25
CVE-2020-1472.....	72, 78
CVSS スコア.....	130
DDoS 攻撃.....	16
DLP.....	194
EDR.....	31, 177, 234
EPP.....	31, 217, 218
IAB.....	34, 42
IDS.....	217
IPS.....	217, 225
IRM.....	194
Lockbit.....	35, 42, 36, 81
LSA シークレット.....	63, 167
LSASS プロセス.....	62
MITRE ATT&CK.....	45
Monero.....	39
MS17-010.....	25, 26
NTDS データベース.....	67
Operator.....	34, 41
Pass the Hash 攻撃.....	71
Psexec.....	77, 88, 182, 187
RaaS.....	34
REG コマンド.....	70
RMM.....	58, 149

SaaS.....	59
SAM データベース.....	64
SIM カード.....	49
SMB.....	110, 122, 182, 187
SSL-VPN.....	108
UAC.....	185
ViewDNS.....	111
VPN.....	23, 28, 46, 108
WDAC.....	144
Web サーバ.....	127
Web 対策.....	130
Windows Defender.....	114
Windows Update.....	117
WMI.....	78
WMIC.....	191
WMI 通信.....	189

## あ・か行

アクセス権.....	194
悪用される拡張子.....	137
悪用されるツール.....	53
暗号化.....	82, 83, 86, 89, 196
安全宣言.....	251
イレギュラーな挙動.....	231
インシデント.....	86, 90, 238
ウイルス.....	15
永続化手法.....	58
カーネルモードドライバ.....	51
外部委託.....	233
監視.....	214, 251
感染経路.....	241
管理者アカウント.....	222
クラウド.....	122, 195
グローバル IP アドレス.....	50, 102
権限昇格.....	60, 100, 154, 204, 210
検出回避.....	51, 99, 203, 209
攻撃ステップ.....	44

攻撃の流れ.....	84, 88
コールバック.....	55, 100, 146, 211

## さ・た行

サイバー攻撃.....	14
サイバー保険.....	21
資格情報マネージャ.....	64
システム領域.....	224
社内外コミュニケーション.....	254
初期侵入.....	46, 99, 102, 202
スキャンング.....	85
スパム判定.....	138
正規ツールやコマンドを悪用.....	68
脆弱性.....	26, 72, 78
脆弱性バッチ.....	116
ダークウェブ.....	16
対策手法.....	98
タスクマネージャ.....	69
多要素認証.....	121
端末の隔離.....	241
注視すべき検出名.....	219
中小企業のセキュリティ対策.....	30
調査ツール.....	243
データ持ち出し.....	79, 101, 191, 213
特権アカウント.....	157
ドメインアカウントキャッシュ.....	65

## な・は行

内部探索.....	72, 100, 176, 205
二重脅迫.....	23, 89
二要素認証.....	23, 125
認証詐欺.....	100, 154, 204, 210
狙われやすいアカウント.....	61
パスワード.....	117, 118
パスワードハッシュ.....	71
パターン検出.....	174
パターンマッチング型.....	30
ハッキングツール.....	15, 67
ばらまき型攻撃.....	14

被害事例.....	22, 84, 201
被害の傾向.....	17
標的型攻撃.....	14
標的型ランサムウェア攻撃.....	17, 44, 94
封じ込め.....	248
復号.....	83
不審メール.....	28
不正プログラム.....	15
復旧にかかる費用・日数.....	19, 20
不要なローカル管理者アカウント.....	162
ブラウザ.....	66, 171
古いOS.....	26
プロキシ.....	148
ペネトレーションテストツール.....	56
ポート.....	104
ポート開放状況.....	111
ポートの制御.....	113
ホワイトリスト化.....	135

## ま・や・ら行

マクロ機能.....	140
マルウェア.....	15
身代金.....	21
身代金交渉人.....	40
無効化.....	89
メールアドレス.....	139
メール対策.....	136
メール添付.....	27
横展開.....	75, 78, 86, 88, 101, 205, 212
ランサムウェア.....	14, 16, 82, 86, 102
ランサムウェア実行.....	81, 207, 214
リモート管理ツール.....	58, 150
リモートデスクトップ.....	28, 75, 86, 104, 113, 159, 178
リンクURL.....	131, 138
ローカルセキュリティポリシー.....	119
ログ.....	218, 229
ロックアウト.....	120