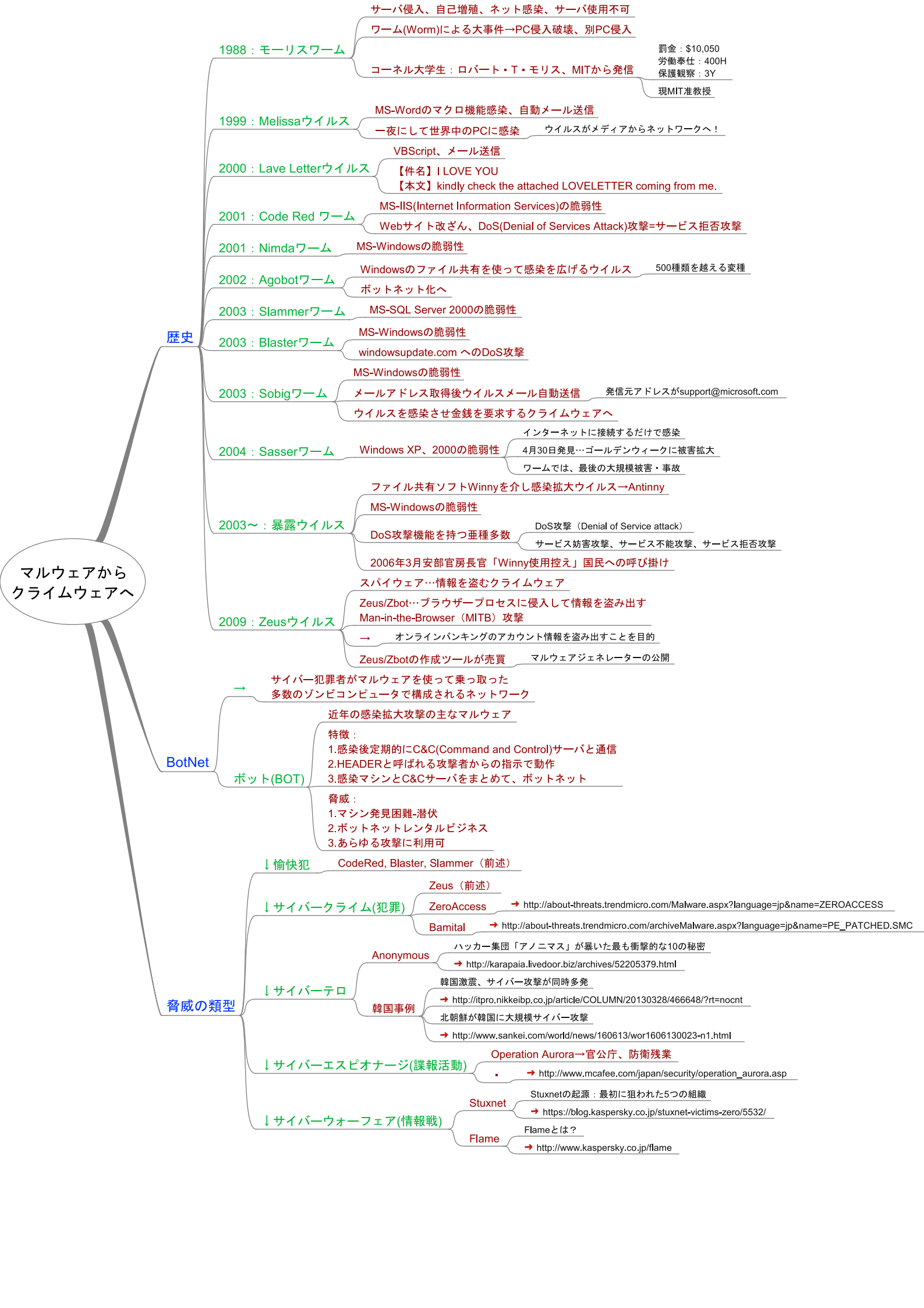
マルウェアから
クライムウェアへ
歴史
1988：モーリスワーム
サーバ侵入、自己増殖、ネット感染、サーバ使用不可
ワーム(Worm)による大事件→PC侵入破壊、別PC侵入
コーネル大学生：ロバート・T・モリス、MITから発信
罰金：$10,050
労働奉仕：400H
保護観察：3Y
現MIT准教授
1999：Melissaウイルス
MS-Wordのマクロ機能感染、自動メール送信
一夜にして世界中のPCに感染
ウイルスがメディアからネットワークへ！
2000：Lave Letterウイルス
VBScript、メール送信
【件名】I LOVE YOU
【本文】kindly check the attached LOVELETTER coming from me.
2001：Code Red ワーム
MS-IIS(Internet Information Services)の脆弱性
Webサイト改ざん、DoS(Denial of Services Attack)攻撃=サービス拒否攻撃
2001：Nimdaワーム
MS-Windowsの脆弱性
2002：Agobotワーム
Windowsのファイル共有を使って感染を広げるウイルス
500種類を越える変種
ボットネット化へ
2003：Slammerワーム
MS-SQL Server 2000の脆弱性
2003：Blasterワーム
MS-Windowsの脆弱性
windowsupdate.com へのDoS攻撃
2003：Sobigワーム
MS-Windowsの脆弱性
メールアドレス取得後ウイルスメール自動送信
発信元アドレスがsupport@microsoft.com
ウイルスを感染させ金銭を要求するクライムウェアへ
2004：Sasserワーム
Windows XP、2000の脆弱性
インターネットに接続するだけで感染
4月30日発見…ゴールデンウィークに被害拡大
ワームでは、最後の大規模被害・事故
2003～：暴露ウイルス
ファイル共有ソフトWinnyを介し感染拡大ウイルス→Antinny
MS-Windowsの脆弱性
DoS攻撃機能を持つ亜種多数
DoS攻撃（Denial of Service attack）
サービス妨害攻撃、サービス不能攻撃、サービス拒否攻撃
2006年3月安部官房長官「Winny使用控え」国民への呼び掛け
2009：Zeusウイルス
スパイウェア…情報を盗むクライムウェア
Zeus/Zbot…ブラウザープロセスに侵入して情報を盗み出す
Man-in-the-Browser（MITB）攻撃
→
オンラインバンキングのアカウント情報を盗み出すことを目的
Zeus/Zbotの作成ツールが売買
マルウェアジェネレーターの公開
BotNet
→
サイバー犯罪者がマルウェアを使って乗っ取った
多数のゾンビコンピュータで構成されるネットワーク
ボット(BOT)
近年の感染拡大攻撃の主なマルウェア
特徴：
1.感染後定期的にC&C(Command and Control)サーバと通信
2.HEADERと呼ばれる攻撃者からの指示で動作
3.感染マシンとC&Cサーバをまとめて、ボットネット
脅威：
1.マシン発見困難-潜伏
2.ボットネットレンタルビジネス
3.あらゆる攻撃に利用可
脅威の類型
↓愉快犯
CodeRed, Blaster, Slammer（前述）
↓サイバークライム(犯罪)
Zeus（前述）
ZeroAccess
➜ http://about-threats.trendmicro.com/Malware.aspx?language=jp&name=ZEROACCESS
Bamital
➜ http://about-threats.trendmicro.com/archiveMalware.aspx?language=jp&name=PE_PATCHED.SMC
↓サイバーテロ
Anonymous
ハッカー集団「アノニマス」が暴いた最も衝撃的な10の秘密
➜ http://karapaia.livedoor.biz/archives/52205379.html
韓国事例
韓国激震、サイバー攻撃が同時多発
➜ http://itpro.nikkeibp.co.jp/article/COLUMN/20130328/466648/?rt=nocnt
北朝鮮が韓国に大規模サイバー攻撃
➜ http://www.sankei.com/world/news/160613/wor1606130023-n1.html
↓サイバーエスピオナージ(諜報活動)
Operation Aurora→官公庁、防衛残業
➜ http://www.mcafee.com/japan/security/operation_aurora.asp
↓サイバーウォーフェア(情報戦)
Stuxnet
Stuxnetの起源：最初に狙われた5つの組織
➜ https://blog.kaspersky.co.jp/stuxnet-victims-zero/5532/
Flame
Flameとは？
➜ http://www.kaspersky.co.jp/flame