

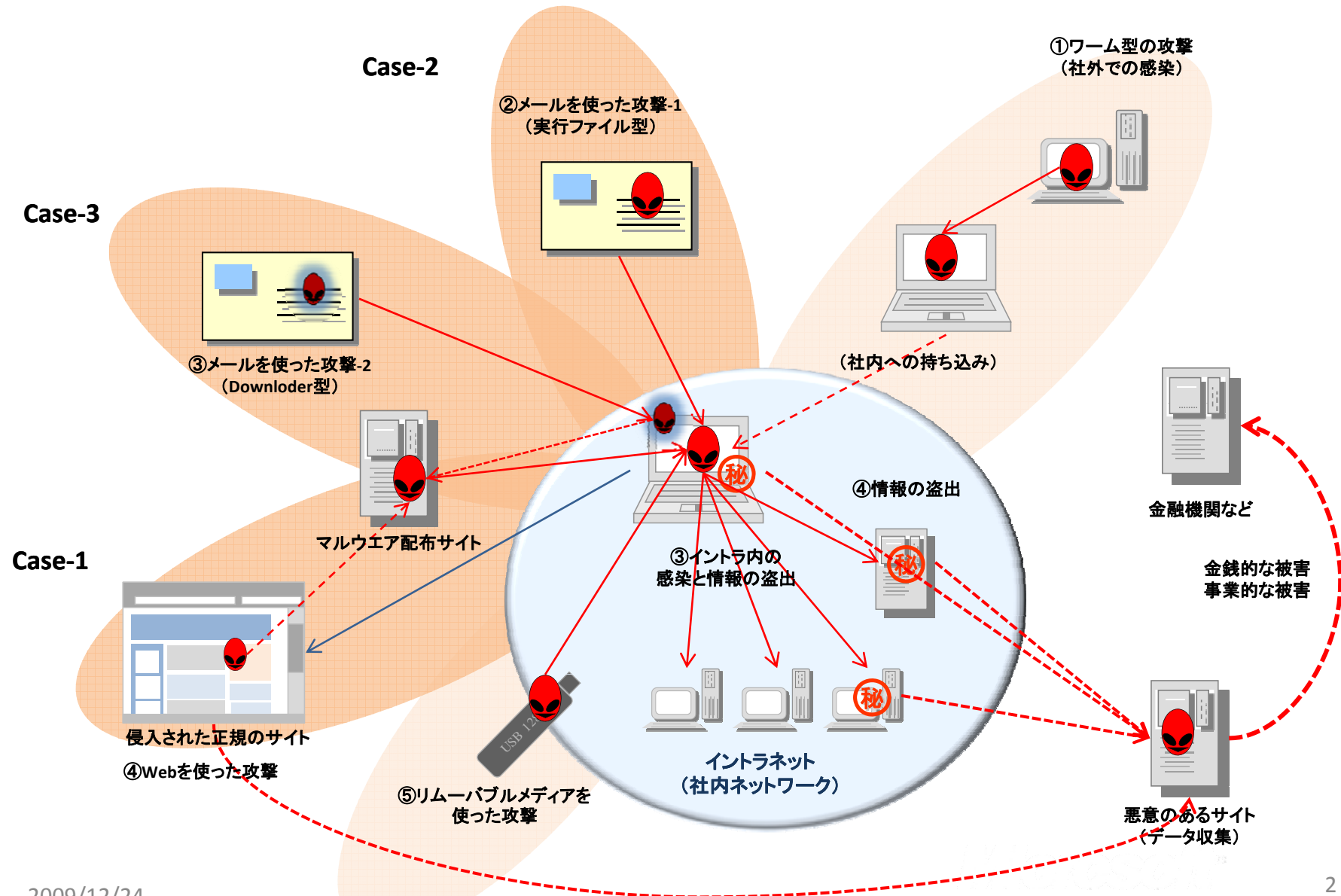
脅威のトレンド 2009

ソフトウェア、プロトコル、ウェブサイトをめぐる動向

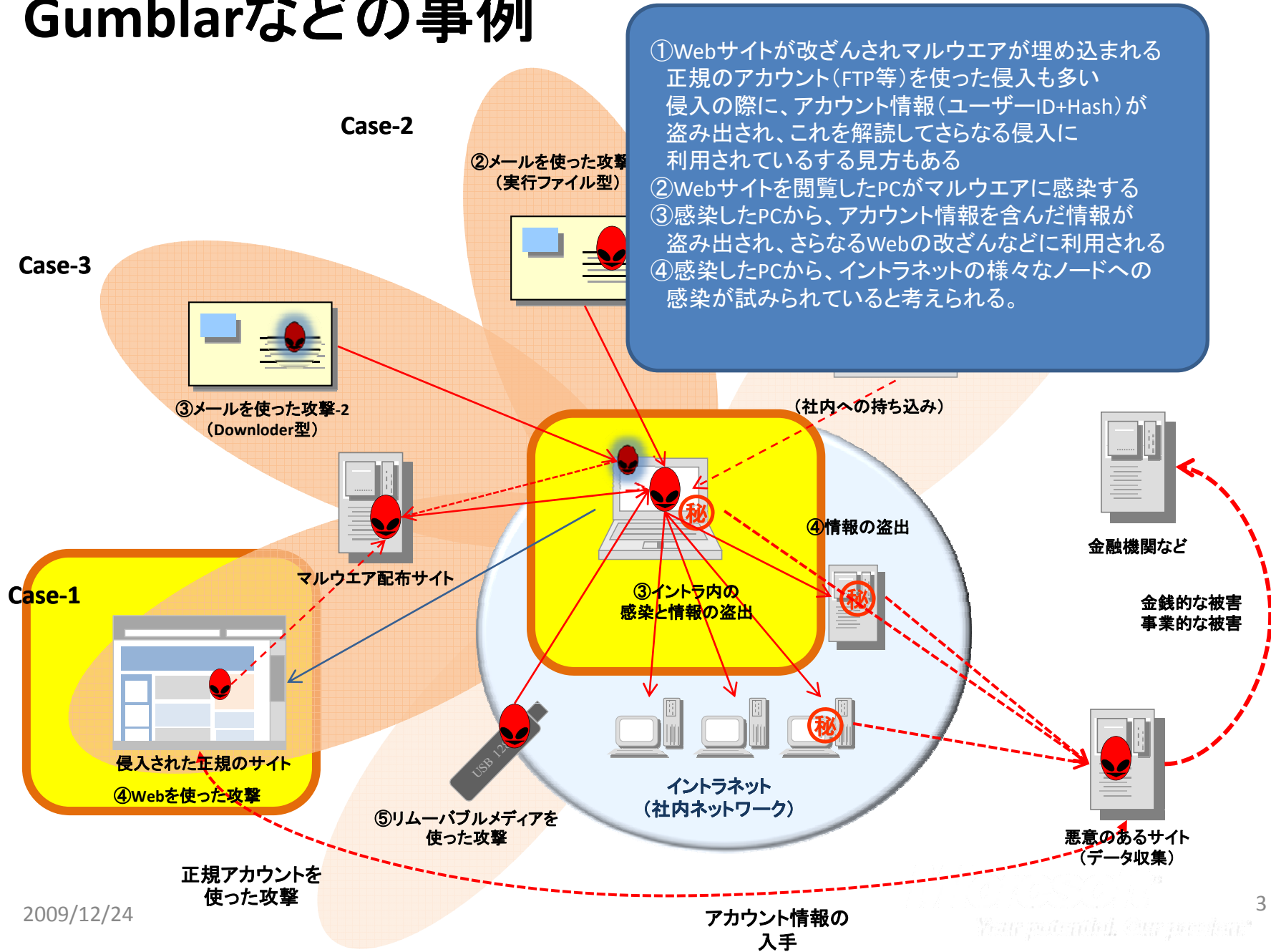
Masakazu Takahashi

Chief Security Advisor, Microsoft K.K.

多様化する攻撃の手法

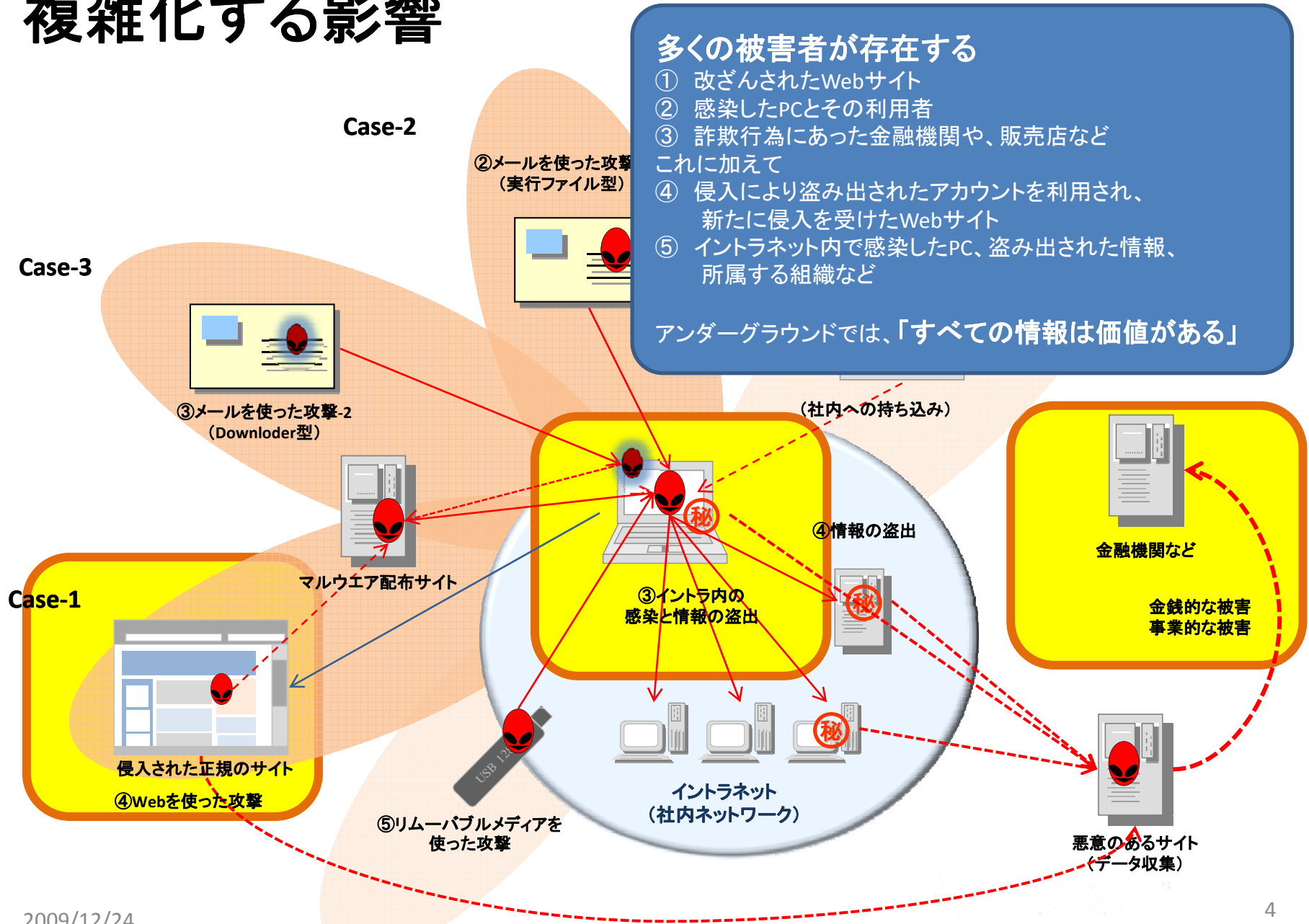


Gumblarなどの事例

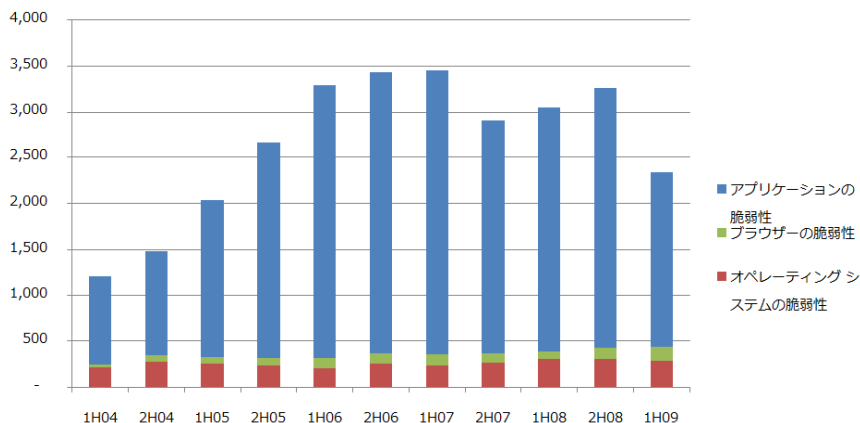


- ① Webサイトが改ざんされマルウェアが埋め込まれる
 正規のアカウント(FTP等)を使った侵入も多い
 侵入の際に、アカウント情報(ユーザーID+Hash)が盗み出され、これを解読してさらなる侵入に利用されているする見方もある
- ② Webサイトを閲覧したPCがマルウェアに感染する
- ③ 感染したPCから、アカウント情報を含んだ情報が盗み出され、さらなるWebの改ざんなどに利用される
- ④ 感染したPCから、イントラネットの様々なノードへの感染が試みられていると考えられる。

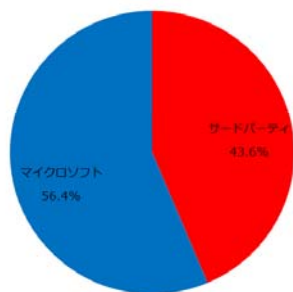
複雑化する影響



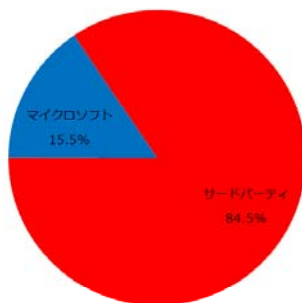
変化する脅威



業界全体のオペレーティングシステム、ブラウザおよびその他の脆弱性 (2004年上半期 - 2009年上半期)



Windows XP



Windows Vista

マイクロソフトおよびサードパーティのソフトウェアを標的としたブラウザベースの悪用 (2009年上半期)

- アプリケーションの脆弱性
 - 報告された脆弱性は、アプリケーションに関する脆弱性が大半を占めている
- 標的の拡大
 - 一般に、脆弱性の発見は、攻撃の増加と連動している
 - 攻撃の標的を調べてみると、XPでは43.6%、Vistaでは84.5%の攻撃が、マイクロソフト社以外のソフトウェアへの攻撃

ディスカッションポイント

- 今年の傾向と特徴
- IT管理者は、このトレンドにどう対処できるのか
- 来年はどうなっていくか？