マイクロソフトにおける
フィッシング対策への取り組み

マイクロソフト（株）
チーフセキュリティアドバイザー
高橋　正和

Microsoft

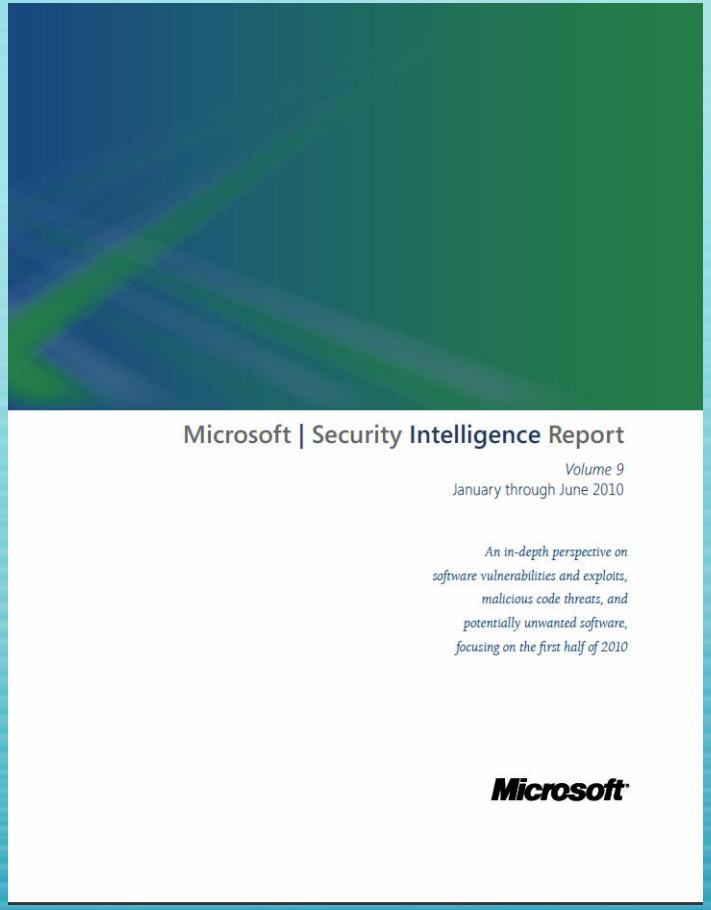
今日の傾向

- フィッシングの傾向について
- フィッシングの背景
- マイクロソフトのフィッシングへの取り組み
- 犯罪基盤としてのボットネット対策の事例
- 今後の取り組みの方向性

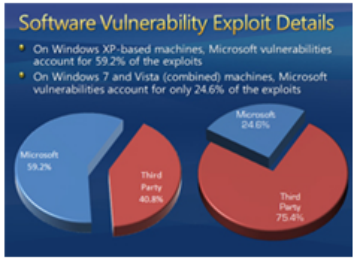
フィッシングの傾向について

Microsoft Security Intelligence Report Volume9
2010年 1月～6月

- マイクロソフトが半期に一度公表している分析レポート
  - 情報ソース（MMPC, MSEC, MSRC）
    - Forefrontなどのマイクロソフトのセキュリティ製品
    - MSRT, Defender, MSEなどの無償で提供しているセキュリティ製品



Microsoft Trustworthy Computing Security Center

Microsoft Malware Protection Center (MMPC)	Microsoft Security Engineering Center (MSEC)	Microsoft Security Response Center (MSRC)
Microsoft Malware Protection Center (MMPC) は、ウイルス、ワーム、スパイウェア、アドウェア、およびその他の悪意のあるソフトウェアおよび迷惑ソフトウェアの可能性のあるものなどの新たな脅威の研究、対応およびお客様の保護に取り組んでいる経験豊富な解析者とセキュリティ技術者のグローバルなチームです。	Microsoft Security Engineering Center (MSEC) は、マイクロソフトのお客様を保護するため、マイクロソフトの製品グループにセキュリティ ガイダンスを提供して、セキュリティ サイエンスおよびテクノロジーをマイクロソフトの開発文化に浸透させ、今後の製品開発に役立てています。	Microsoft Security Response Center (MSRC) は、セキュリティ リスク分析において中心を担っており、セキュリティ インシデントおよびマイクロソフトのソフトウェアの脆弱性の特定、監視、対応および解決のため 24 時間 365 日センターの管理を行っています。
		
SIR v8 では、MMPC は世界中のマルウェアや迷惑ソフトウェアの可能性のあるものについて の傾向について掘り下げ包括的な分析を提供しています。	本 SIR では、MSEC はブラウザー ベースのソフトウェアおよび Microsoft Office ドキュメントに対するエクスプロイトやドライブ バイ ダウンロード エクスプロイトの傾向についてレポートしています。	セキュリティの問題の継続的な警戒のため、MSRC はセキュリティのニュース グループを監視し、secure@microsoft.com に送信された電子メールの対応および全社的なセキュリティ更新プログラムの公開プロセスを管理しています。

http://www.microsoft.com/japan/security/contents/sir.mspx

Microsoft

フィッシングサイトの数とアクセス数

通常は、フィッシングサイトと、フィッシングサイトへのアクセス*は、安定した関係にある
しかし、2010年6月は、この傾向から大きく逸脱したアクセスが観測された。
マイクロソフトの調査では、特定のターゲットとの関連性はなかった。
このような動きは、必ずしも、珍しいケースではない。

* SmartScreenで、フィッシングサイトへのアクセスをブロックした回数

フィッシングのターゲット

FIGURE 57. Active phishing sites tracked each month from January to June 2010, by type of target

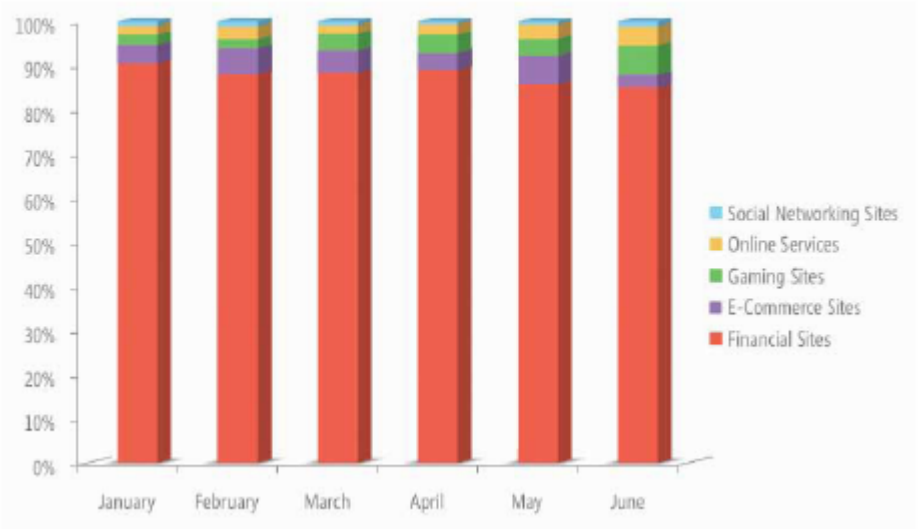
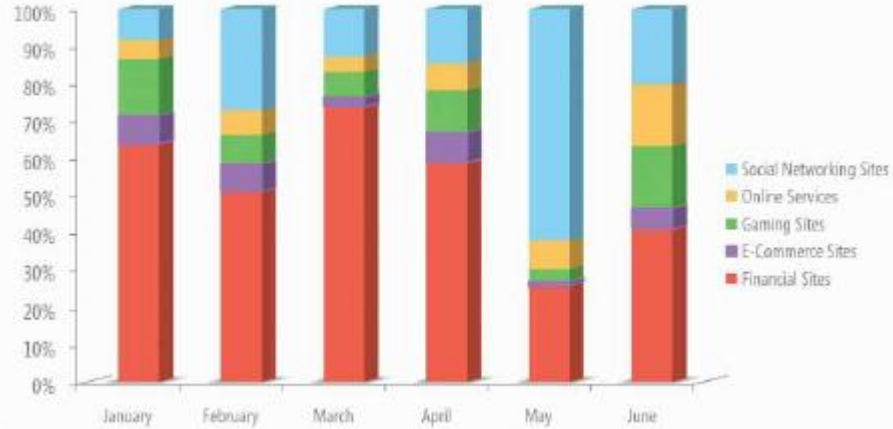


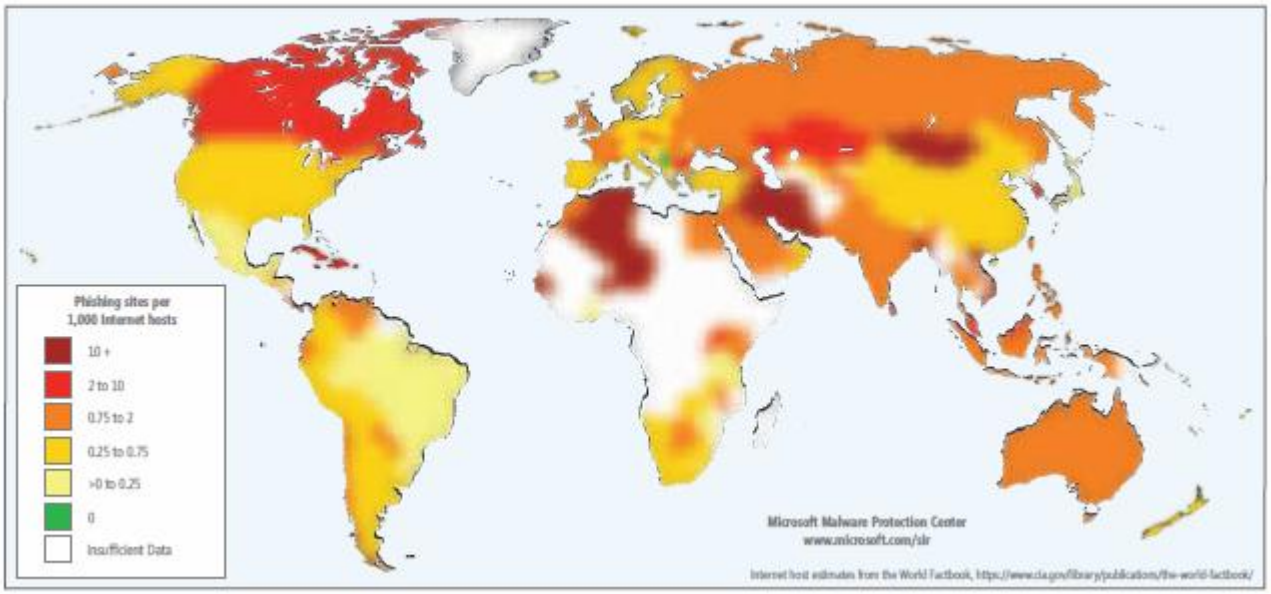
FIGURE 56. Impressions for each type of phishing site each month from January to June 2010



フィッシングサイトの大半は、金融機関をターゲットとしたものであるが、ソーシャルネットワークサイトへのアクセスが目立つ結果となっている。

フィッシングサイトの地域別分析

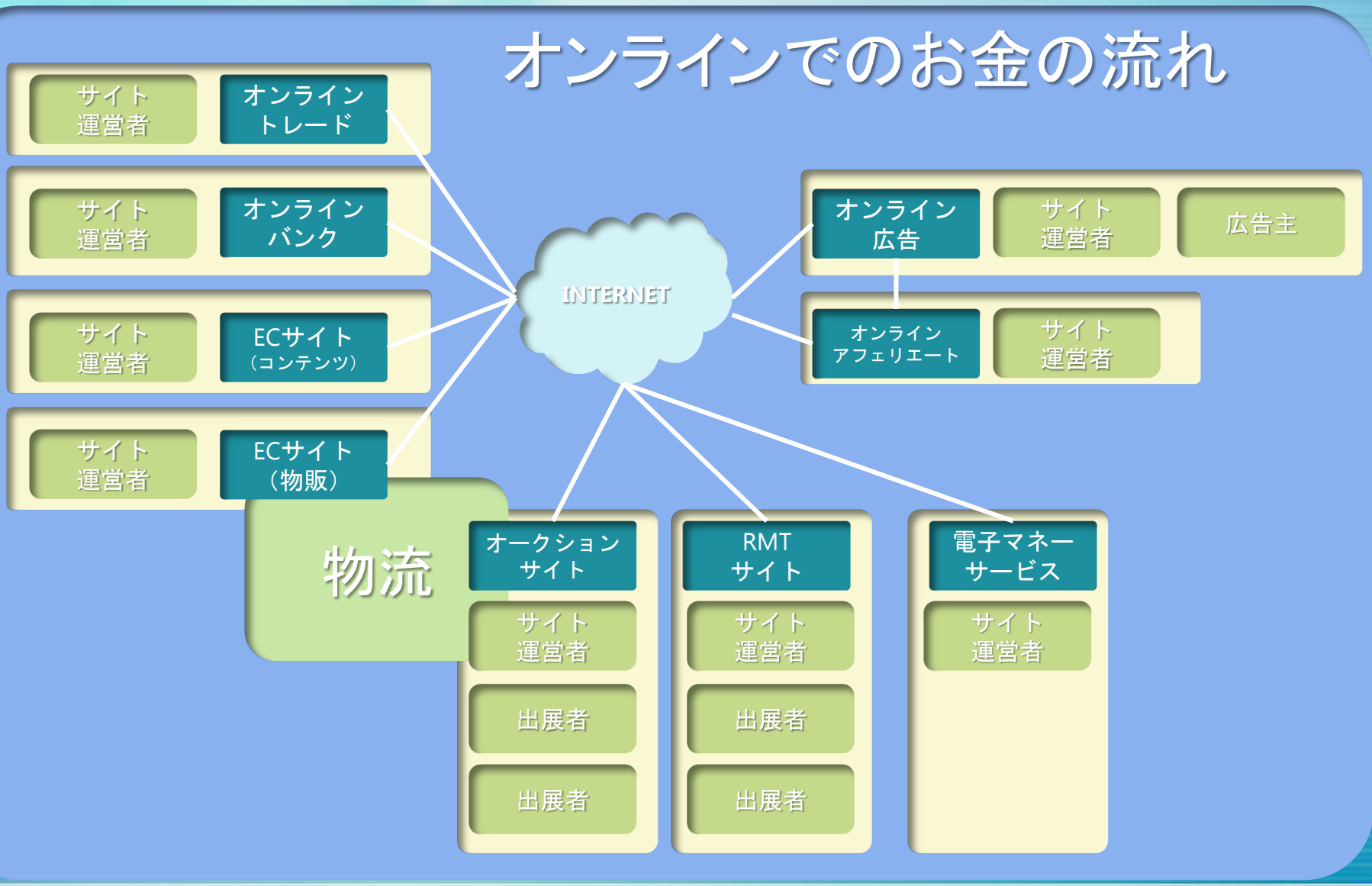
FIGURE 58. Phishing sites per 1,000 Internet hosts for locations around the world in 2Q10



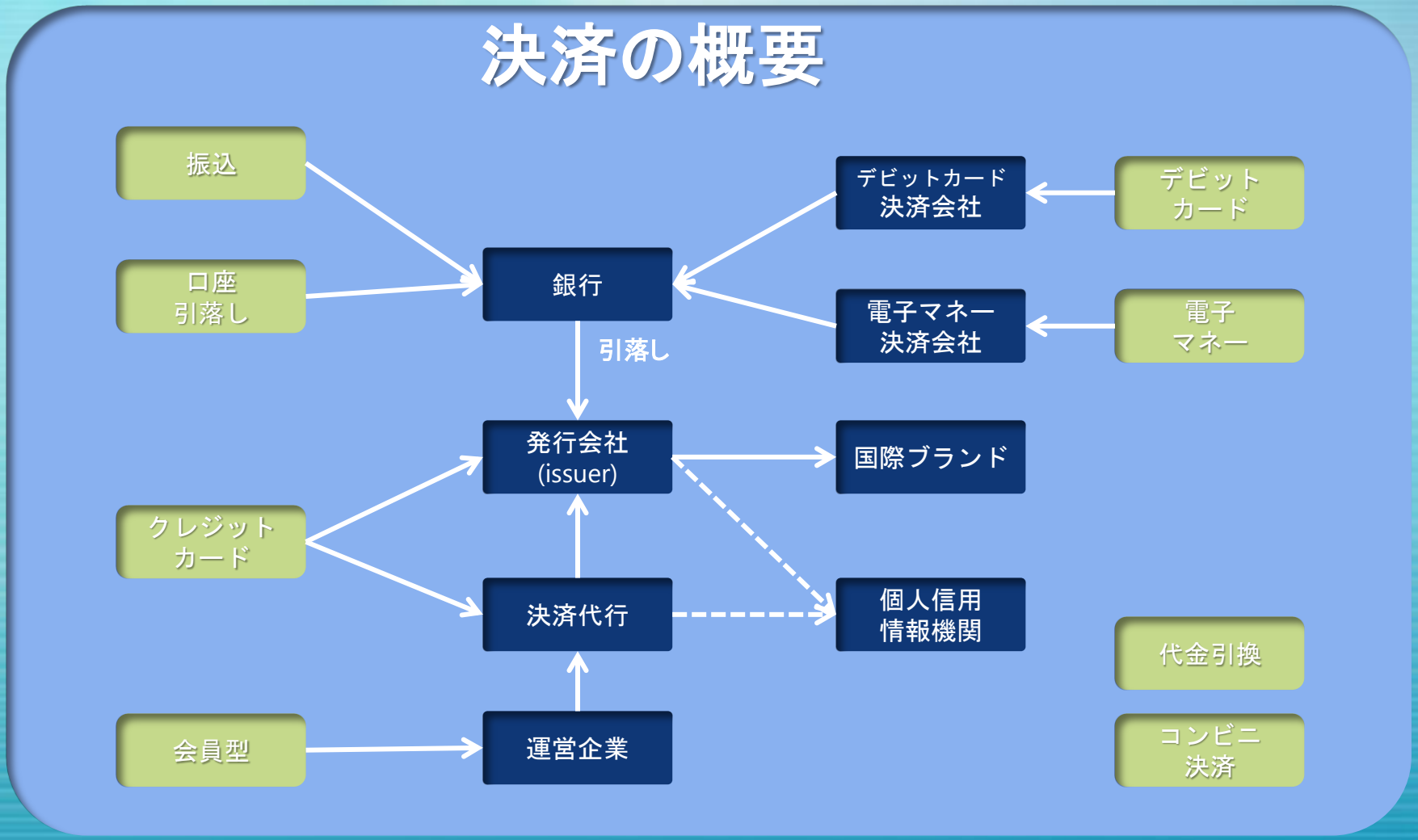
日本は、比較的フィッシングサイトの少ない国と分析している

フィッシングの背景
サイバー犯罪の経済化とは
どういうことか？

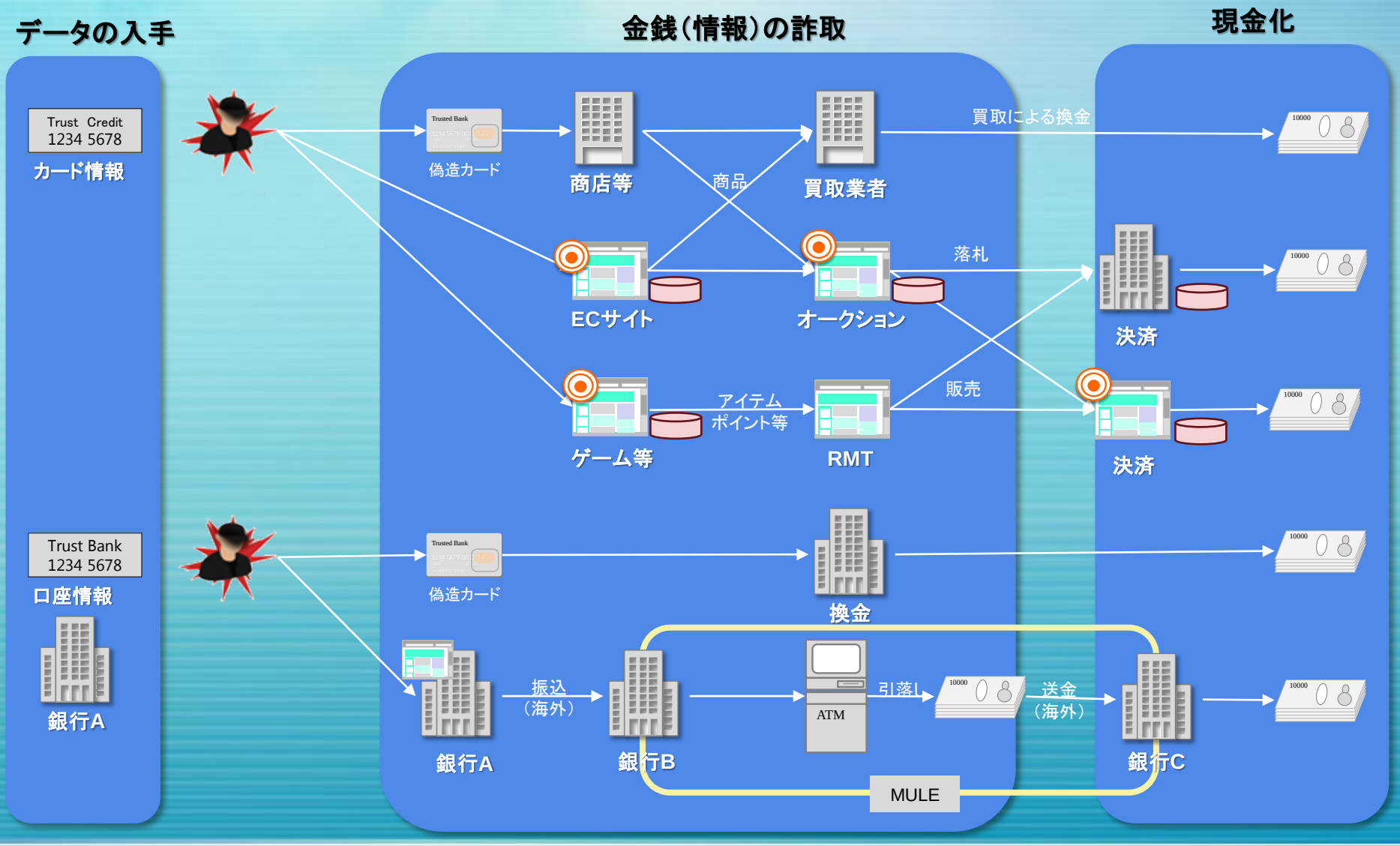
表のお金の流れはどうなっているのか？



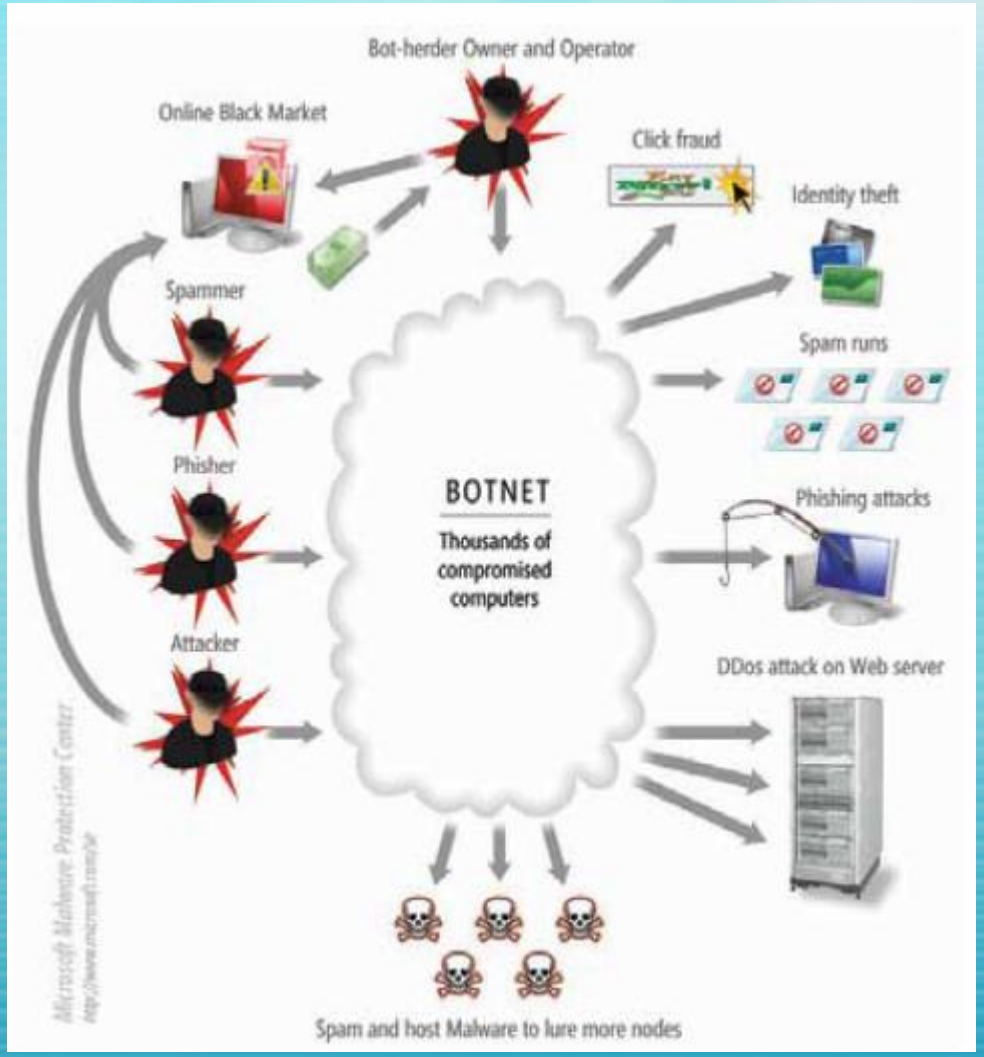
表のお金の流れはどうなっているのか？



口座・クレジットカード情報を現金化



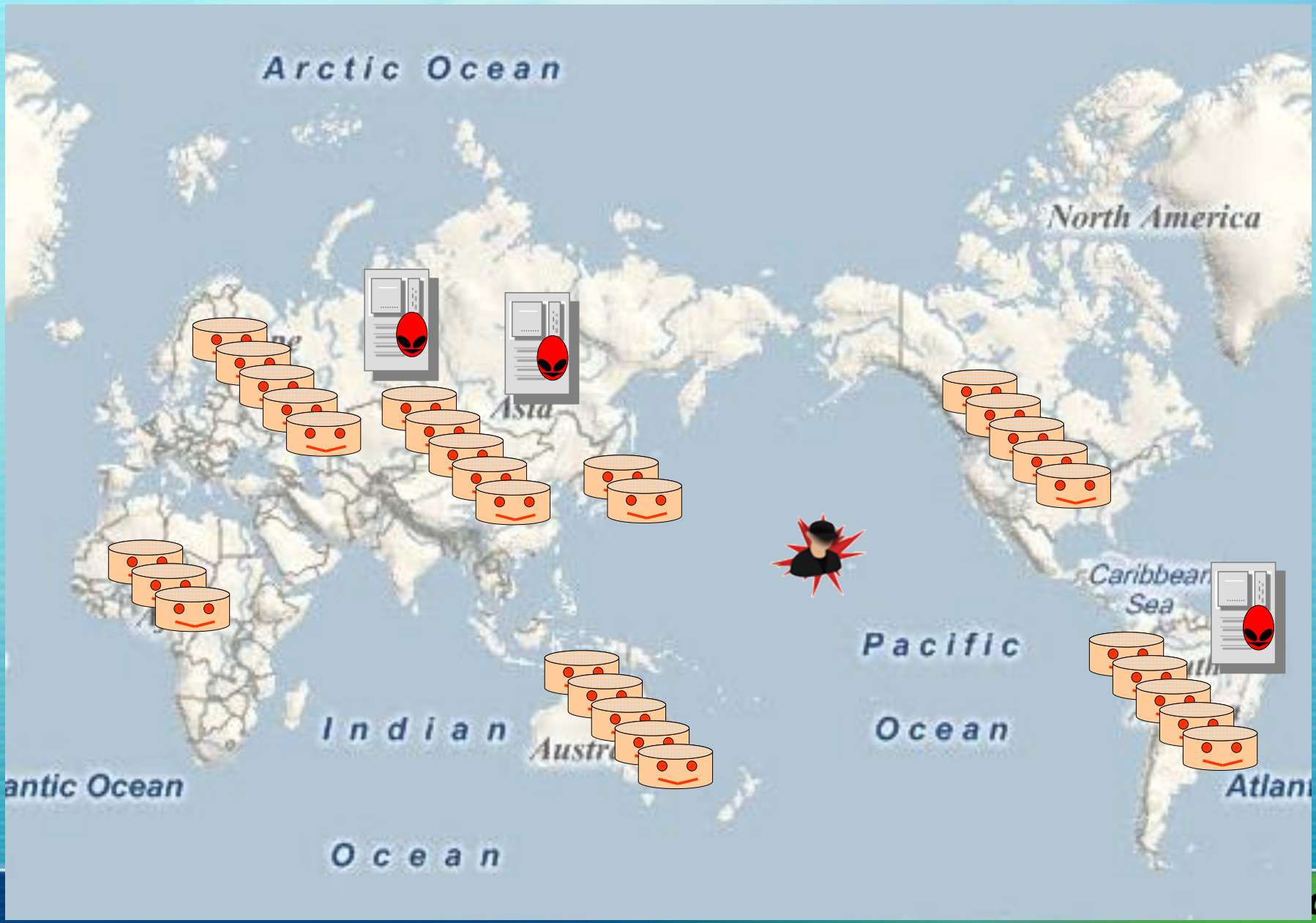
フィッシング等
サイバー犯罪の基盤としてのボットネット



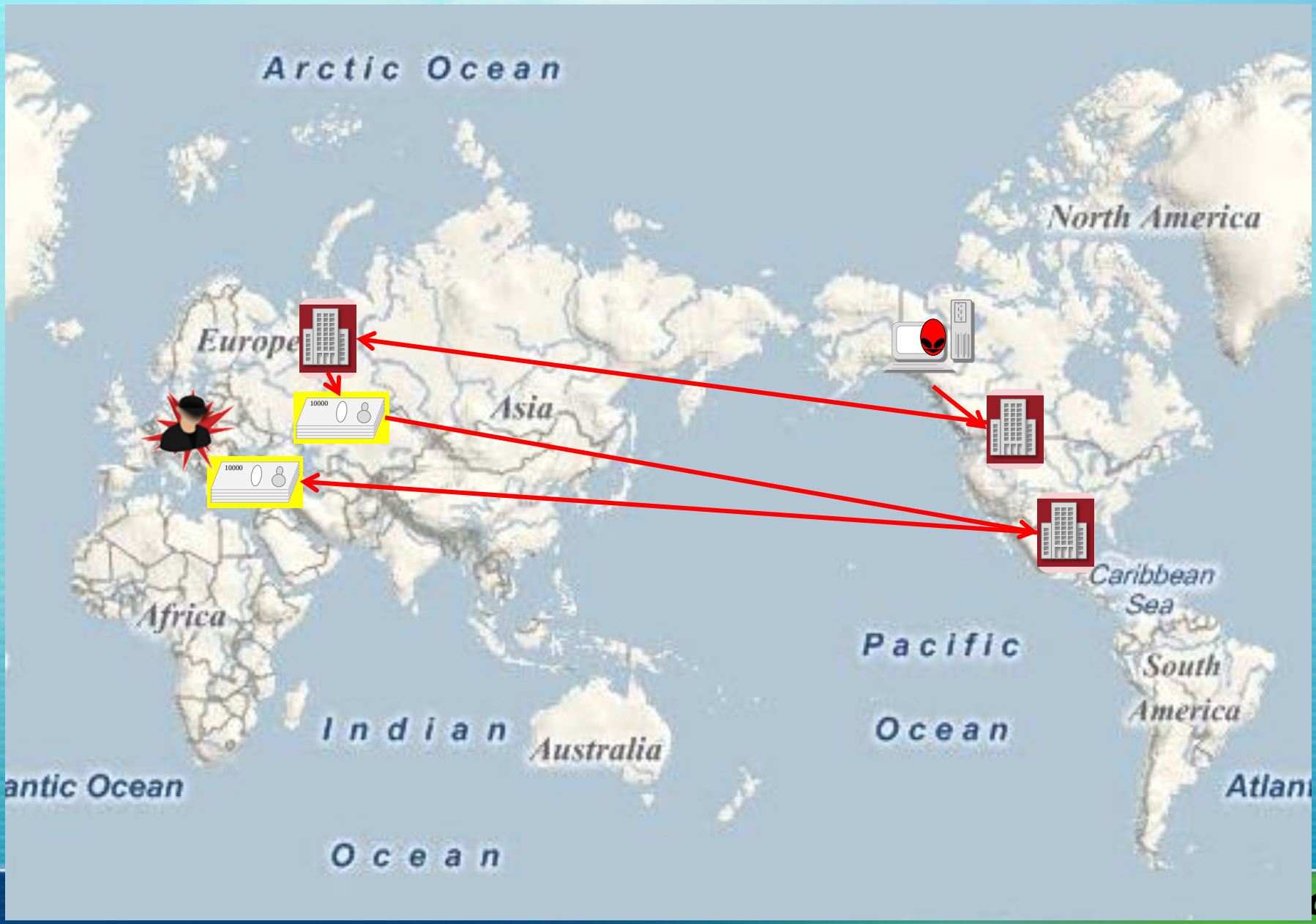
- **ボットネットの主な利用方法**
  - スパムメールの送信
  - フィッシング
  - 機密データの詐取
  - DDoS攻撃
  - マルウエアやPUSのインストール
  - マルウエアの配布
  - クリック詐欺

- **経済活動としてのボットネット**

ボットネットの世界的な展開



国際的な金銭の流れ

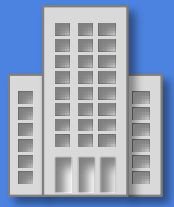

Arctic Ocean
North America
Europe
Asia
10000
10000
Africa
Caribbean Sea
Pacific
South America
Ocean
Indian
Australia
Ocean

口座搾取対策とその対策

PCから口座情報を詐取

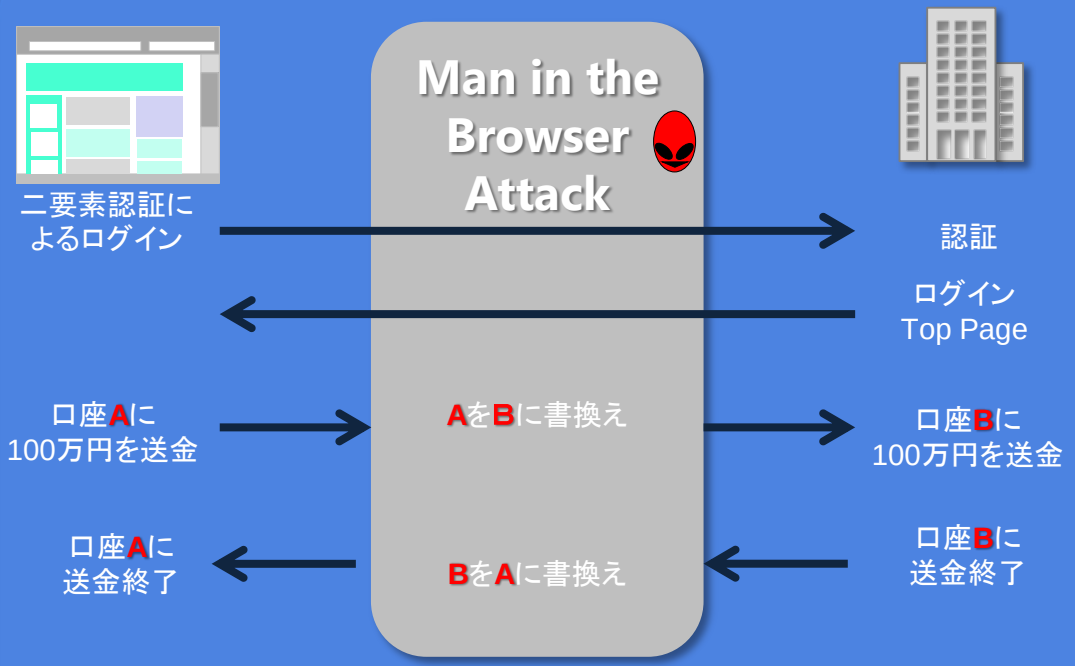
・ファイル等からの詐取
・Key loggerによる詐取

銀行などの
ID盗難の対策



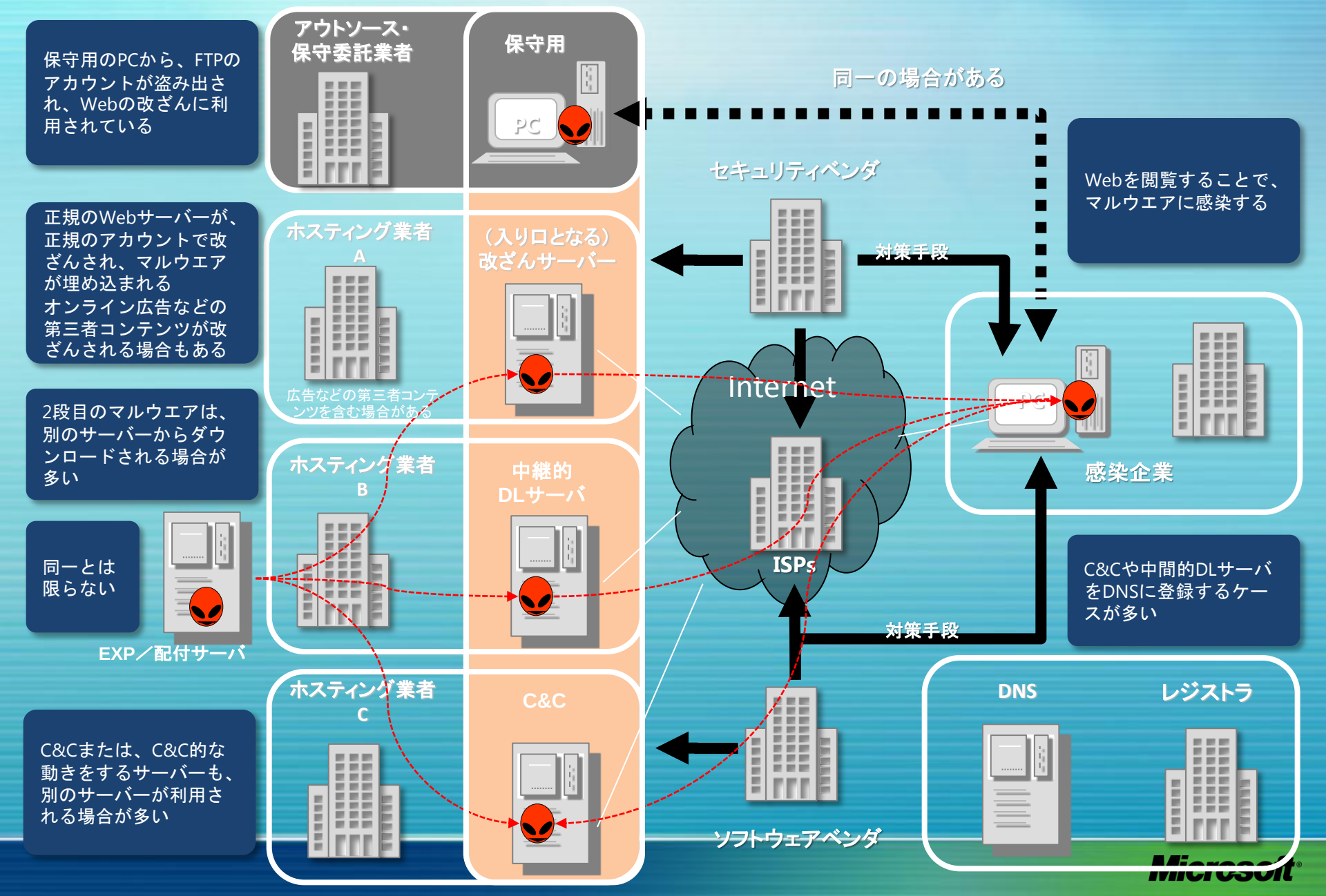
・二要素認証
乱数表
ワンタイムパスワード

二要素認証を使うオンラインバンクからの金銭を詐取



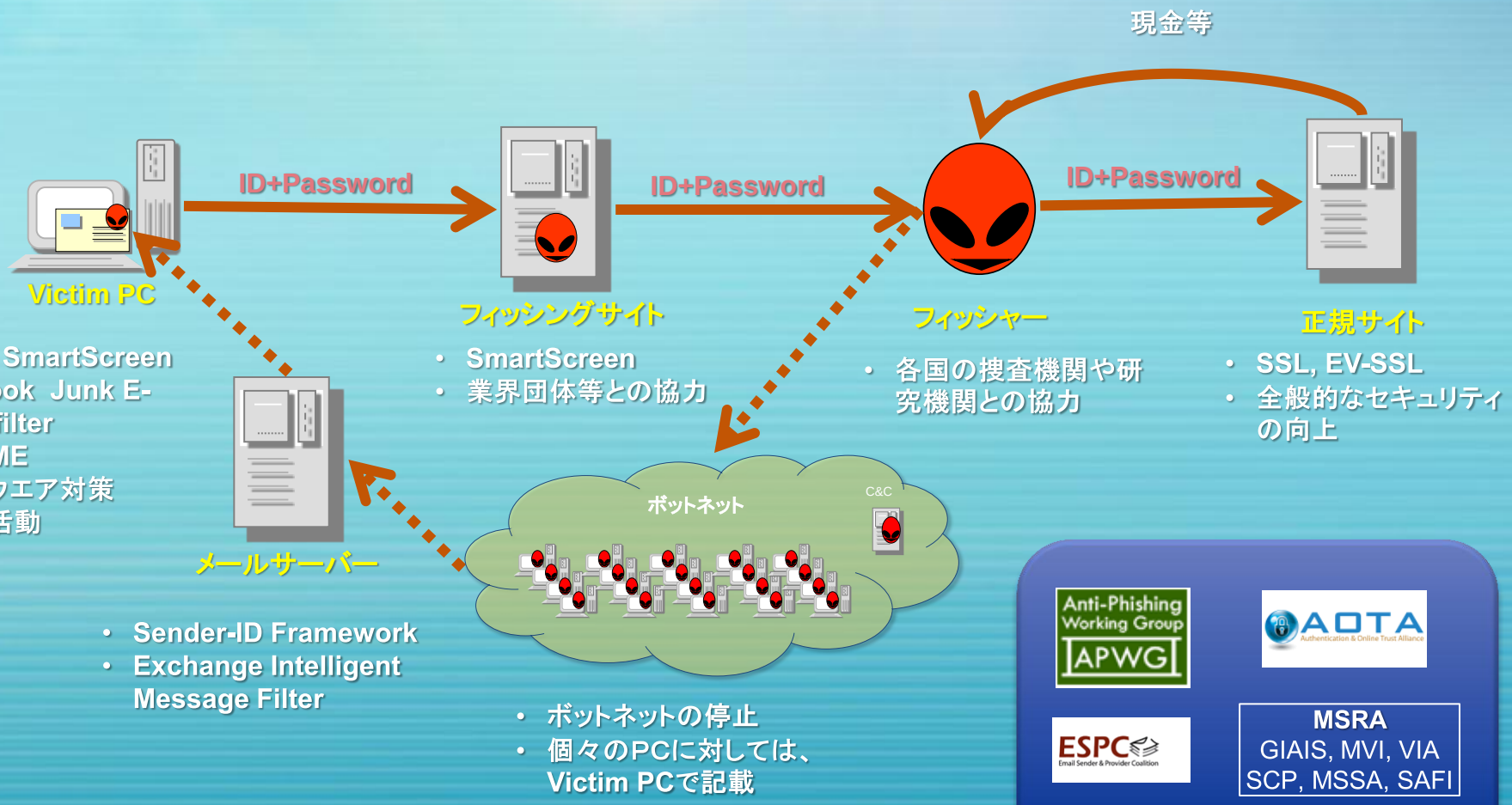
認証の確立したセッションを利用して、トランザクションを改ざんするため、二要素認証でも攻撃を防ぐことができない。また、銀行から表示されるデータも改ざんされているため、この行為に気づくことは困難。
一般に、送金先は、Money Muleと呼ばれる運び屋の口座が利用される。
Zeus/Zbot, URLZone/Bebloh 等

サーバーのアカウントも狙われている(Gumblar)



マイクロソフトの
フィッシングへの取り組み

マイクロソフトのフィッシングへの取り組み



- IE7/8 SmartScreen
- Outlook Junk E-mail filter
- S/MIME
- マルウエア対策
- 啓発活動

- SmartScreen
- 業界団体等との協力

- 各国の捜査機関や研究機関との協力

- SSL, EV-SSL
- 全般的な セキュリティの向上

- Sender-ID Framework
- Exchange Intelligent Message Filter

- ボットネットの停止
- 個々のPCに対しては、Victim PCで記載

Anti-Phishing Working Group APWG

AOTA Authentication & Online Trust Alliance

ESPC Email Sender & Provider Coalition

MSRA
GIAIS, MVI, VIA
SCP, MSSA, SAFI

Digital Crimes Consortium

MSRA: http://www.microsoft.com/japan/security/msra/default.mspx

Microsoft

レピュテーション、フィッシングフィルターのデータ提供元

Reputation Services and Phishing Filter Data Providers

Published: April 4, 2006 | Updated: July 19, 2007

Reputation Services

Reputation services play a critical role in e-mail authentication and identity verification. Microsoft works closely with several companies that provide such reputation services.

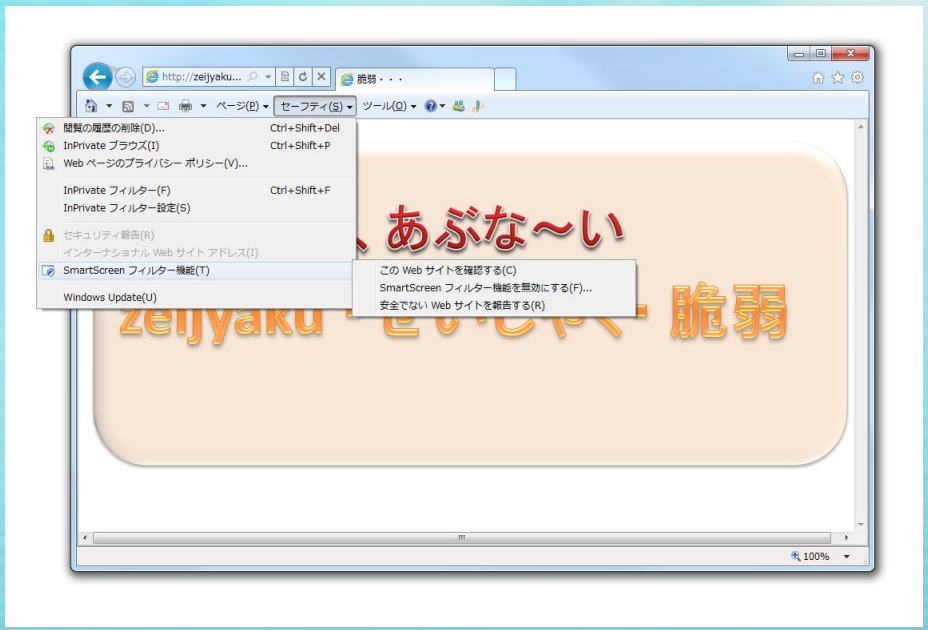
Provider	About their solutions
BONDED SENDER is now Sender Score Certified A service of Return Path	**Sender Score Certified** Microsoft and Windows Live Hotmail utilized the Sender Score Certified program from Return Path Inc. Sender Score Certified is one of the most widely accepted accreditation programs available today for legitimate e-mail senders. The program identifies legitimate senders of e-mail based on their past sending behavior and their adherence to strict program standards. Sender Score Certified gives e-mail recipients an objective way to help block unwanted e-mail messages and deliver legitimate ones.

Microsoft Phishing Filter Data Providers

To provide an unparalleled level of protection from phishing exploits, Microsoft has agreements with several commercial data providers to dynamically provide information to Microsoft on thousands of confirmed phishing Web sites. Microsoft has integrated this data into the Microsoft Phishing Filter technology, which is available for the MSN Search Toolbar and for Internet Explorer 7 for Windows Vista and Windows XP SP2. Today this data is helping improve online safety for millions of users worldwide.

Provider	About their solutions
brandprotect	**BrandProtect** BrandProtect, a leader in internet reputation management, empowers organizations to gain control over how they are represented online by uncovering and mitigating the issues that put their reputation at risk and erode customer trust. BrandProtect's Response Services help detect, uncover and mitigate brand and trademark infringement issues, phishing attacks, web traffic diversions, website integrity issues and defamatory discussions. BrandProtect has relationships with more than 3,500 Internet Service Providers globally.
Cyveillance® The World Leader in Cyber Intelligence™	**Cyveillance** Cyveillance, a world leader in cyber intelligence, provides an intelligence-led approach to security. Through continuous, comprehensive Internet monitoring and sophisticated intelligence analysis, Cyveillance proactively identifies and eliminates threats to information, infrastructure, individuals, and their interactions, thereby enabling its customers to preserve their reputation, revenues, and customer trust. Cyveillance serves the Global 2000 and OEM Data Partners, protecting the majority of the Fortune 50, regional financial institutions nationwide, and more than 30 million global consumers through its partnerships with security and Internet service providers.
InternetIdentity	**Internet Identity** Internet Identity is a leader in the area of Internet presence control, enabling financial services firms and e-commerce companies to help protect their customers against online fraud. Combining innovative technology with an extensive network of provider relationships, Internet Identity delivers highly effective fraud Web site deactivation and domain name control services.
MarkMonitor	**MarkMonitor** MarkMonitor, a global leader in enterprise brand protection, offers comprehensive solutions and services to safeguard brands, reputation, and revenue from online risks. With end-to-end solutions that address the growing threats of online fraud, brand abuse, and unauthorized channels, MarkMonitor makes the Internet safer for businesses and their customers. The company's exclusive access to data combined with its real-time detection, investigation, and response capabilities provide wide-ranging protection from the ever-changing online risks that brands face today.
NETCRAFT	**Netcraft** The Netcraft toolbar community is a giant neighborhood watch scheme, empowering the most alert members to defend the rest of the community against phishing frauds. To date it has blocked more than half a million phishing URLs aimed at customers of over 900 institutions. Netcraft provides a comprehensive set of security and antifraud services to financial institutions and Internet infrastructure companies.
RSA SECURITY	**RSA Security** RSA Security Inc. is an expert in protecting online identities and digital assets. The inventor of core security technologies for the Internet, RSA Security leads the way in strong authentication, encryption, and antifraud protection, bringing trust to millions of user identities and the transactions they perform. The RSA Security portfolio of award-winning solutions helps businesses to establish who's who, and what they can do, online.
S21sec	**S21sec** S21sec is a leading company in IT security services. Founded in 2000, S21sec offers holistic security services that focus on protecting the most valuable components of an organization: digital assets, information, and image. With offices in various countries, and a strong investment in research and development, S21sec helps businesses manage their security 24 hours a day, 7 days a week.

フィッシングサイトの登録

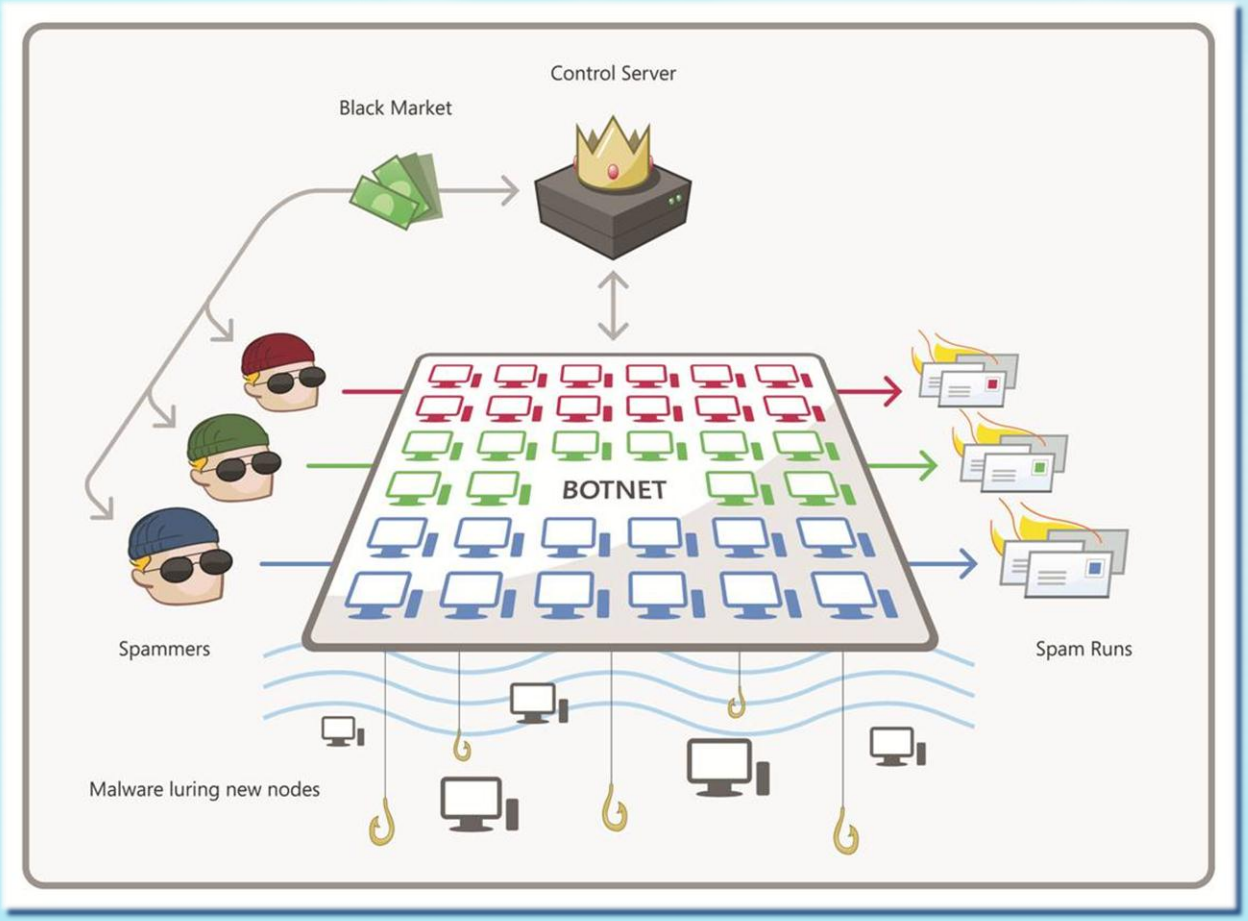


- IEのメニューから、フィッシングサイトの登録を行うことができる。

Microsoft

犯罪基盤としてのボットネットと対策の事例

ボットネット



未承諾電子メールの87%はボットネットが原因でおこる。

ボットネットに感染したコンピュータは380万台以上 – 米国のみで100万台

DDoS攻撃– 2008年中の攻撃190,000件

出典：Internet Security http://internet-security.suite101.com/article.cfm/botnets_guilty_for_87_of_2009_global_spam_mail#ixzz0eysy7BTj Namestnikov, Yuri. “The Economics of Botnets,” Kaspersky Lab. 2009年

Waledac：2009年7月～12月

Hotmailは18日間でマルウェア「Waledac」に感染したコンピュータからのトラフィック6億5,100万件を遮断

39カ国におけるボットネット上位10位

マイクロソフトは、 96,223台のマシンからWaledacを駆除した。

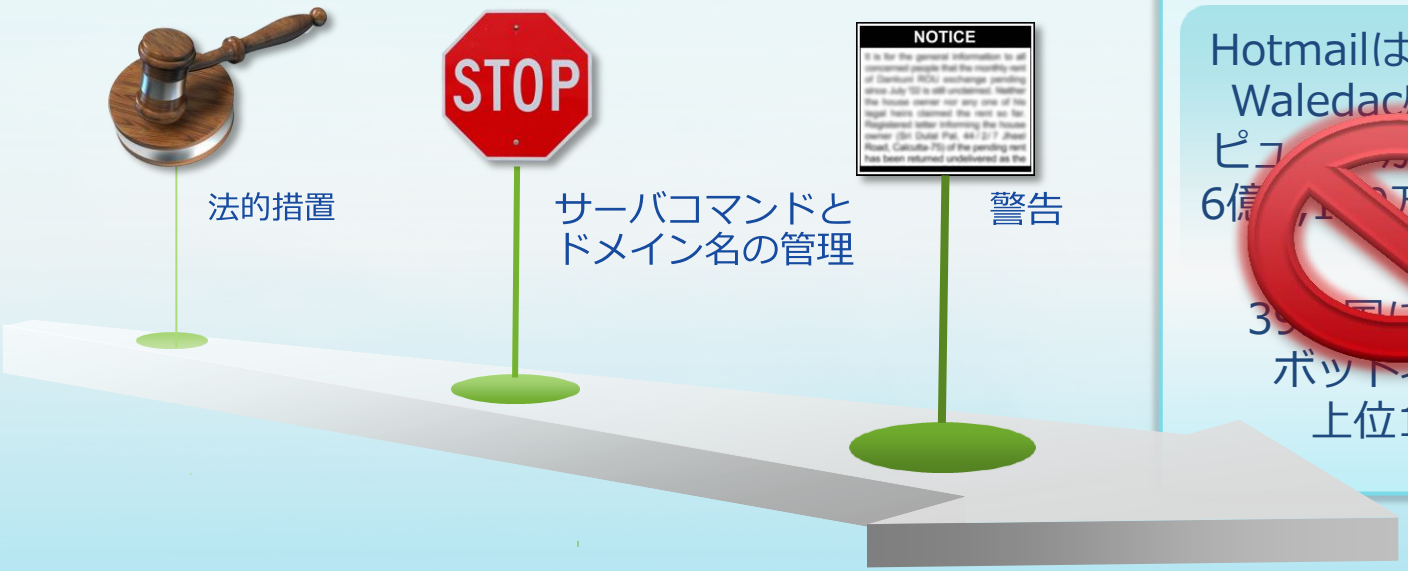
出典：マイクロソフトデジタル犯罪ユニット、
マイクロソフトマルウェアプロテクションセンター、2010年3月

Microsoft

ボットネット

WALEDACボットネット「遮断」アプローチ

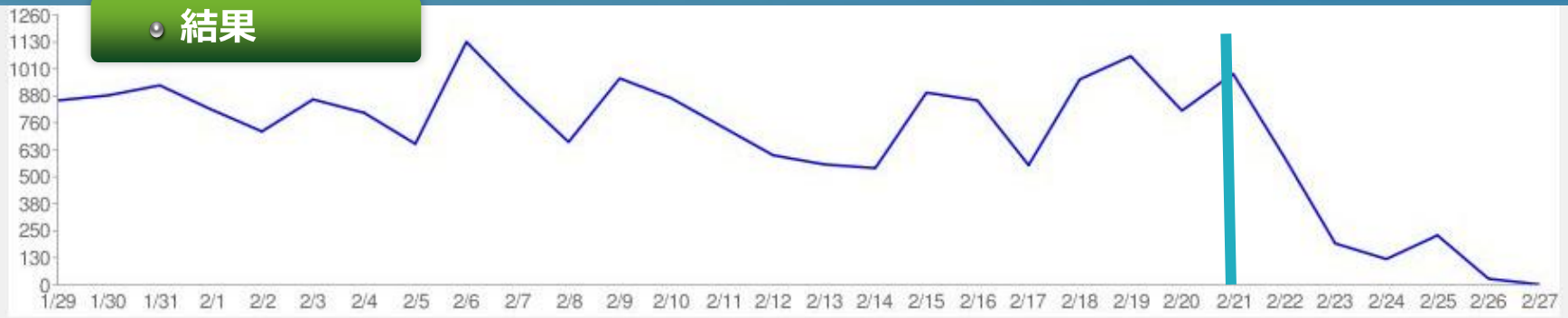
短期的 – 先例を作る



Hotmailは18日間で
Waledac感染コン
ピュ 接続
6億 万件を 遮断

3 る
ボットネット
上位10位

結果



Microsoft

今後の取り組みの方向性

End to End Trustの構築

ID認証
メタシステム

認証 | 権限付与 | アクセス制御

クレームベースのIDシステム

確実な身元確認

信頼できる
階層

管理
&
監査

政治的
法的要因

経済的
要因

セキュリティ／
プライバシーの
基礎

セキュリティ・デベロップメント
・ライフサイクルと
開発のためのプライバシー標準

多層防御

脅威の緩和

社会的要因

Microsoft®

Your potential. Our passion.™