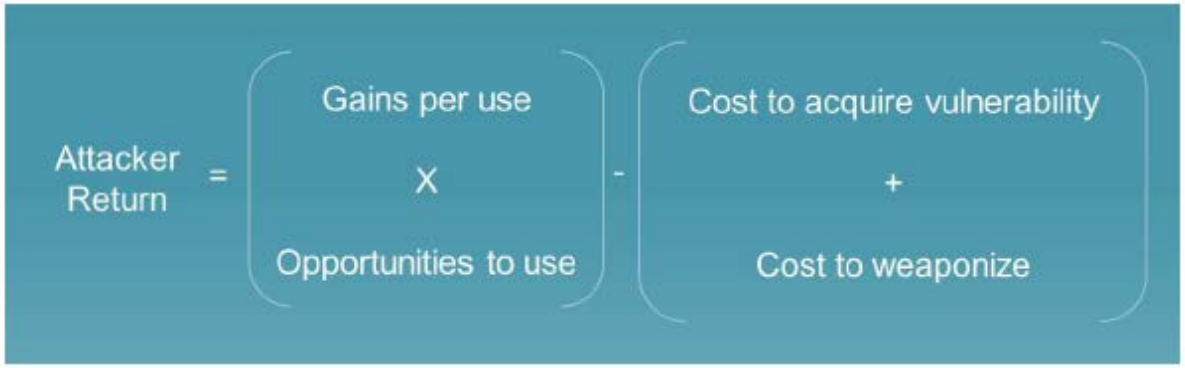
資料5

マイクロソフトにおける サイバー攻撃への対処

日本マイクロソフト株式会社
チーフセキュリティアドバイザー
高橋　正和

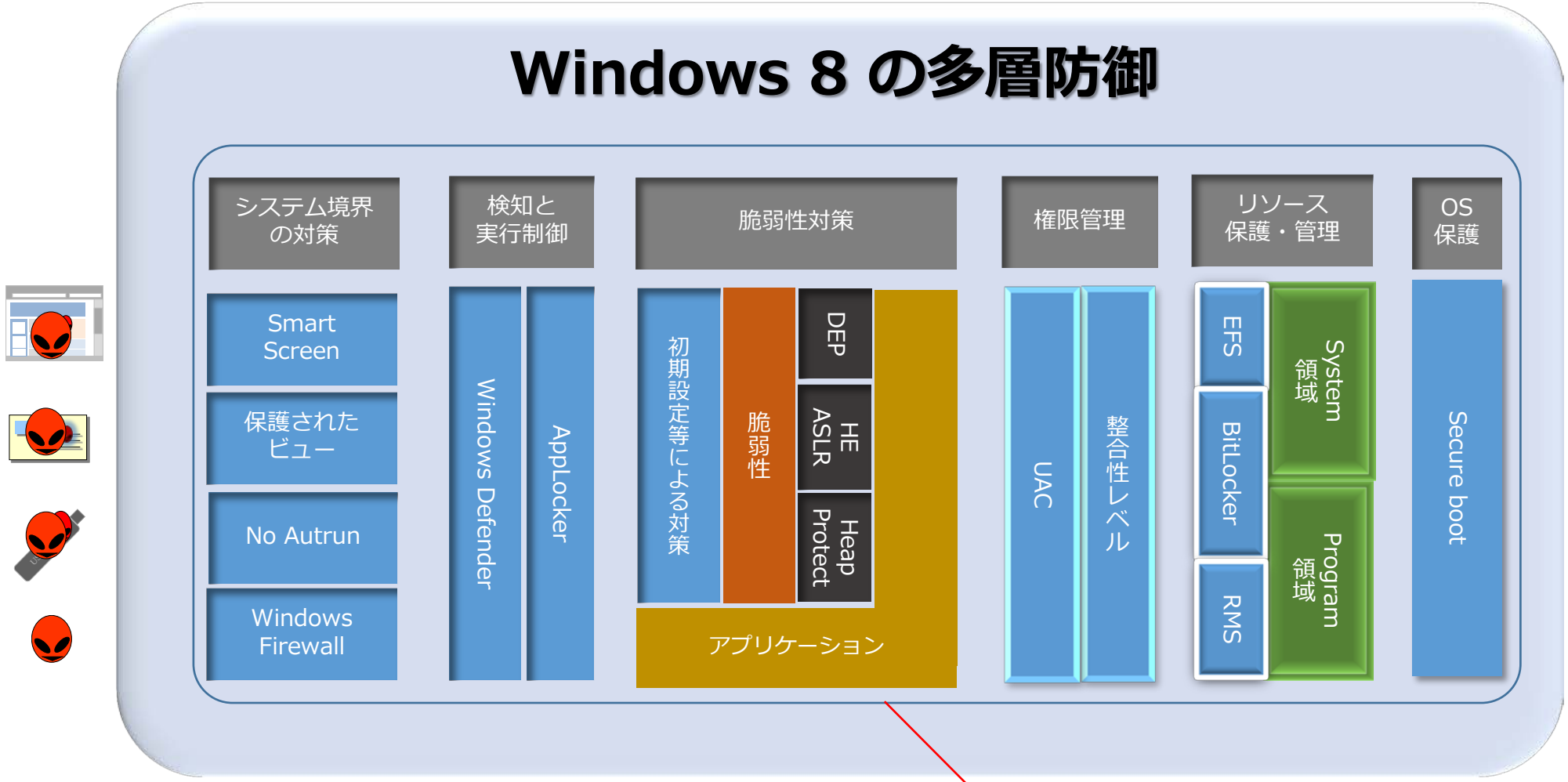
基本的な考え方



より安全な製品・サービスを提供する	サイバー犯罪等への取組み
脆弱性の適切な対応	ボットネット Takedown
より安全な製品の開発	PhotDNA
マルウエア対策 MTRS/Defender	CTIP

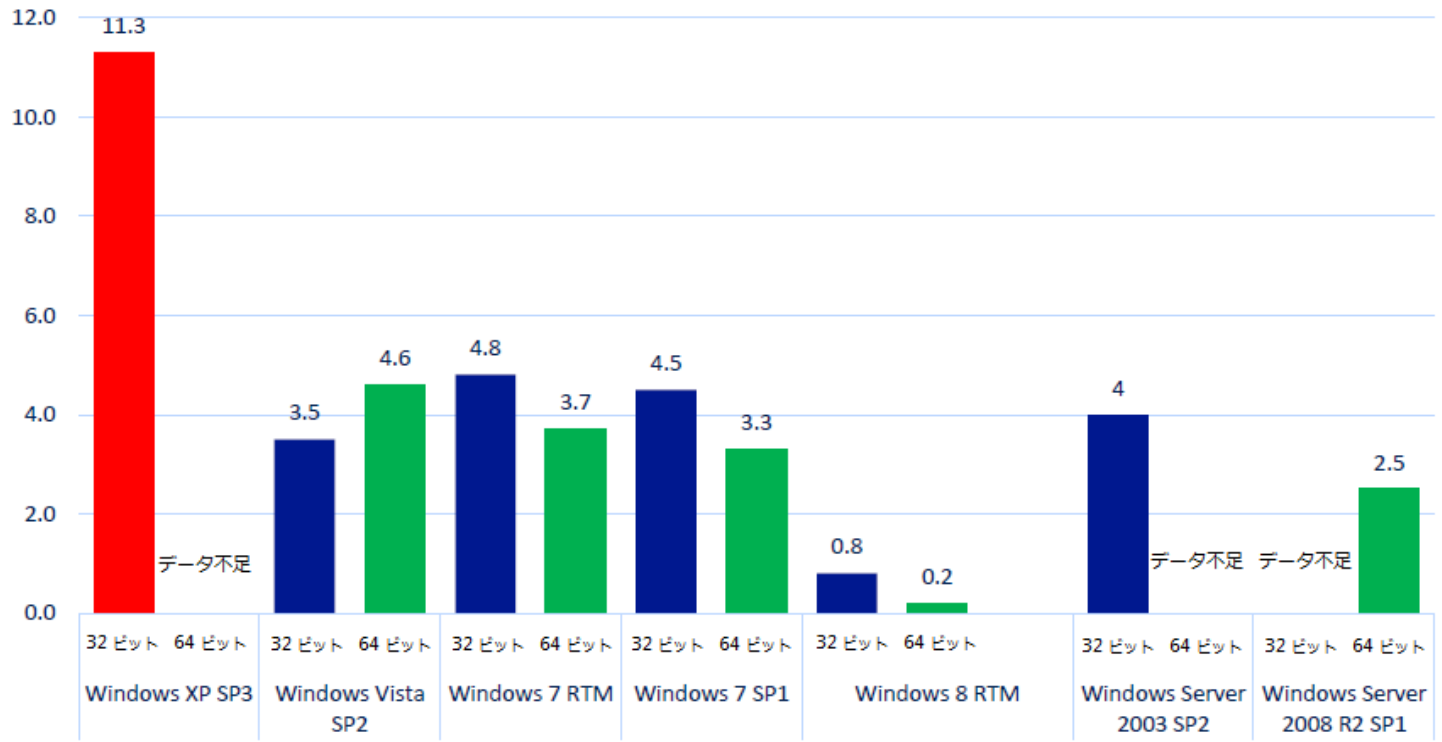
より安全な製品・サービスを提供する

最新システムの多層防御



IE8(XP)とIE10(Win-8)の比較

	Windows XP SP3 Internet Explorer 8	Windows 8 Internet Explorer 10
SEHOP	×	○
保護モード	×	○
拡張保護モード (EPM)	×	○
Virtual Table Guard	×	○
ASLR	限定的	広範
スタックのランダム化	×	○
ヒープのランダム化	×	○
イメージのランダム化	×	○
イメージのランダム化の強制	×	○
ボトムアップのランダム化	×	○
トップダウンのランダム化	×	○
高エントロピーのランダム化	×	○
PEB/TEB のランダム化	○	○
ヒープの強化	限定的	広範
ヘッダーのエンコード	×	○
破損時に終了	×	○
ガード ページ	×	○
割り当てのランダム化	×	○
安全なリンク解除	○	○
ヘッダー チェックサム	○	○
/GS	○	○
拡張 /GS	×	○
SafeSEH	○	○



BotnetのTakedown

日時	ボット名	推定台数	概要
2010/2/22	Waledac	数十万台	Operation b49 1日当たり15億通以上のスパム・メール送信に悪用
2010/10/25	Bredolab	3千万台	オランダ当局ハイテク犯罪チーム主導。ボットネットの停止の他、追加コマンドを送信し、コンピュータが感染していることを表示するプログラムをダウンロードさせてユーザーに通知
2011/4/11	Coreflood	2百万台	FBI 主導。感染したPCに対してマルウェアの停止コマンドを送信
2011/3/17	Rustock	2百万台	Operation b107 1日当たり300億通以上のスパム・メール送信に悪用。全スパム流通量の47.5%はRustock経由で送信
2011/9/27	Kelihos	4万台	Operation b79 スパムの大量送信、個人情報の窃盗、DDoS 攻撃など。Waledac との類似性から Waledac 2.0 とも呼ばれている。
2012/3/19	Zeus	800ドメイン 1300万	Operation B71 5億ドルに上る被害をもたらしている Zeus, SpyEye, Ice-IXをTakedown
2012/9/13	Nitol	7万ドメイン 500種	市場で販売されているコンピューターから検出されたNitolボットネットをTakedown
2013/2/6	Bamital		サーチハイジャック、$1M/年以上のクリック詐欺
2013/6/5	Citadel	500万台 1,462ドメイン	Operation b52 キーロガーを使い5億ドル以上を詐取
2013/12/5	ZeroAccess	200万台	$2.7M/月のオンライン広告のクリック詐欺

SPAM:Exchange Online のデータから

Figure 14. Messages blocked by Exchange Online Protection each half-year period, 2H09–1H13

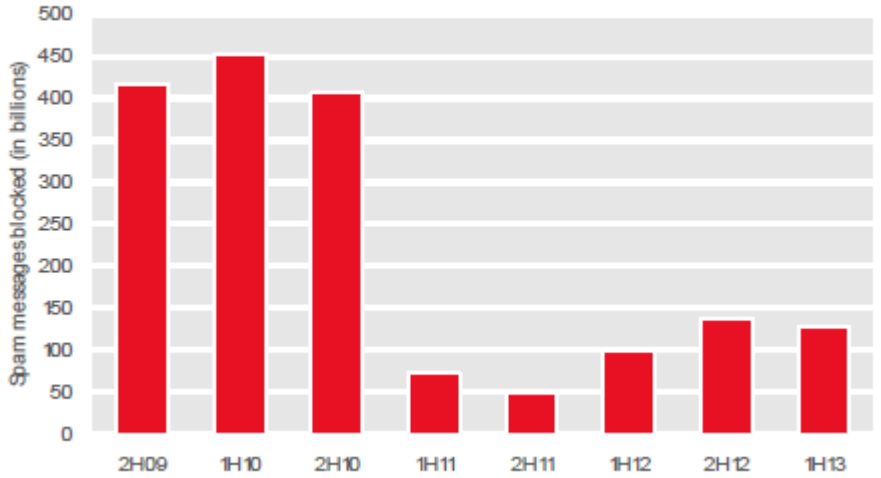
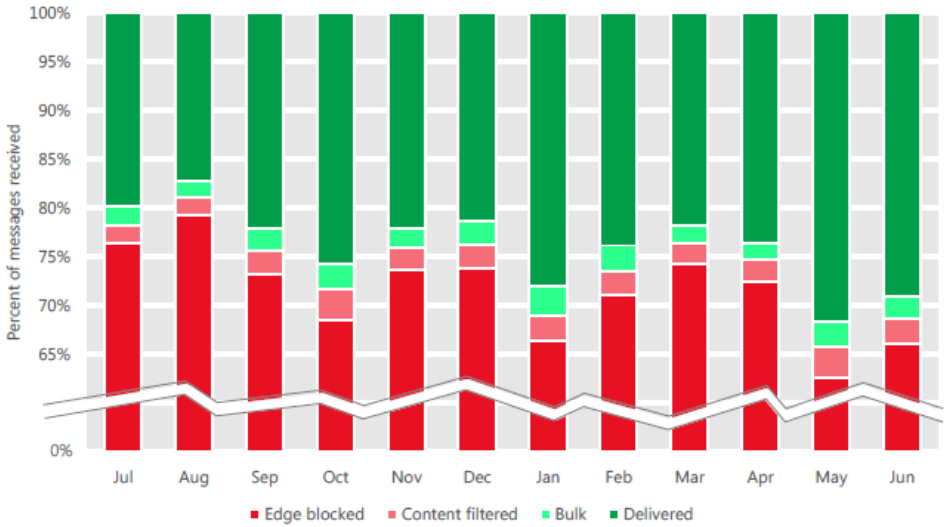
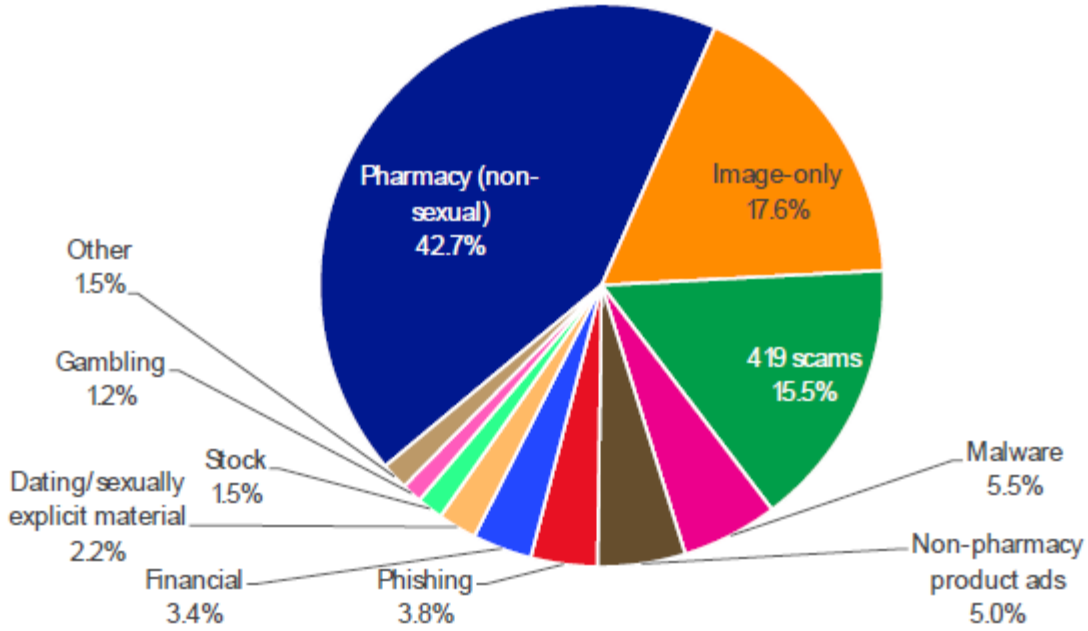


Figure 57. Percentages of incoming messages blocked, categorized as bulk email, and delivered, July 2012–June 2013



- Exchange Online Protectionのデータに見るSPAM
  - SPAMの送信量は、2010年に実施されたCutwailと RustockTakedownにより大きく減少し、2010年には1:33(SPAM)から、2013年上半期には1:4(SPAM)となっている
  - 62.7 - 74.2%のメールは、ネットワークエッジ（Reputation等）でブロック
  - 25.8 - 37.3%のメールだけが、よりリソースを必要とするコンテンツフィルタリングの対象となり、そのうちの7.6 -10.0%（全体の1.7 - 2.7%)がSPAMとしてフィルターされる。

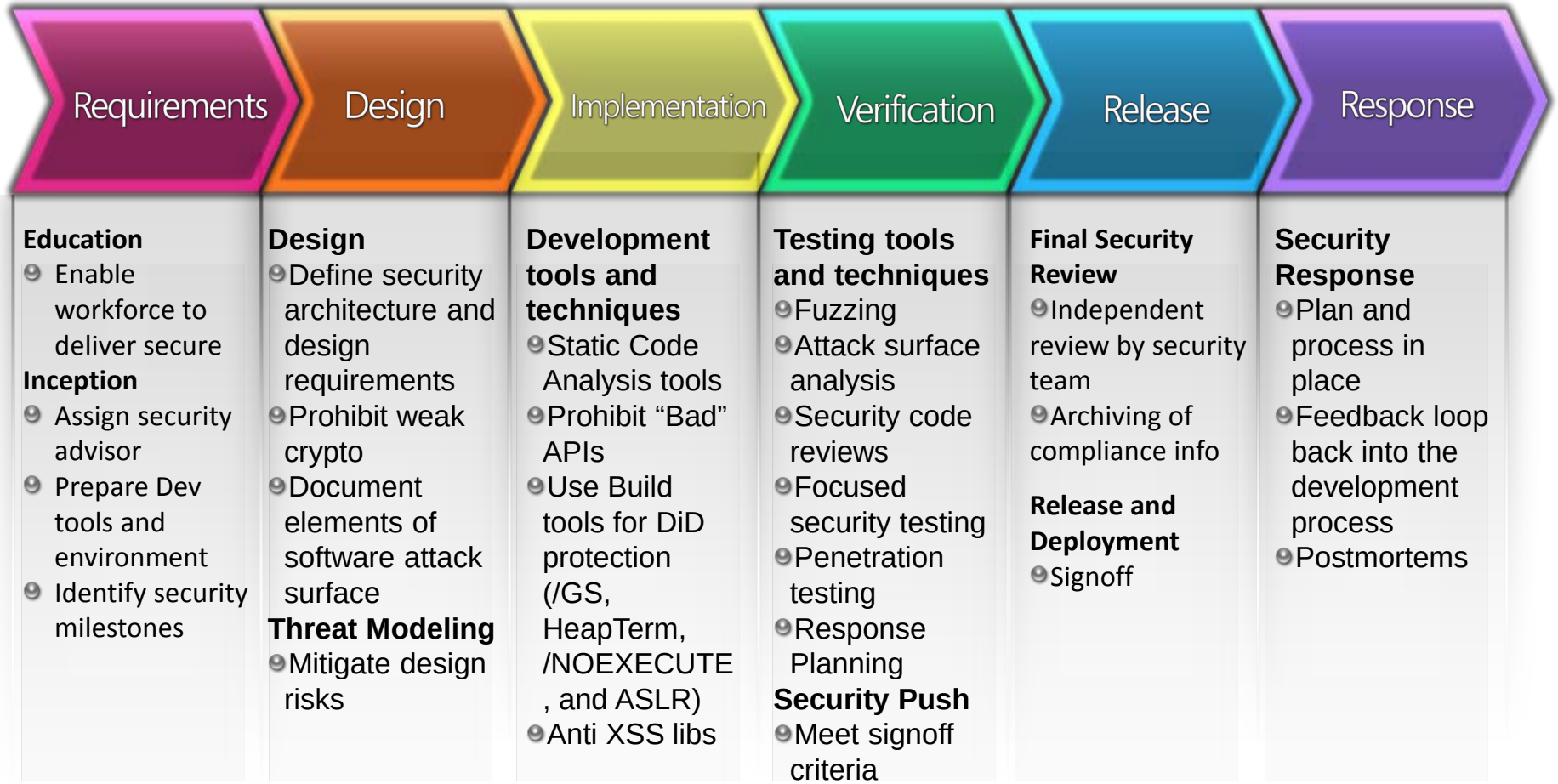
Figure 15. Inbound messages blocked by Exchange Online Protection filters in 1H13, by category



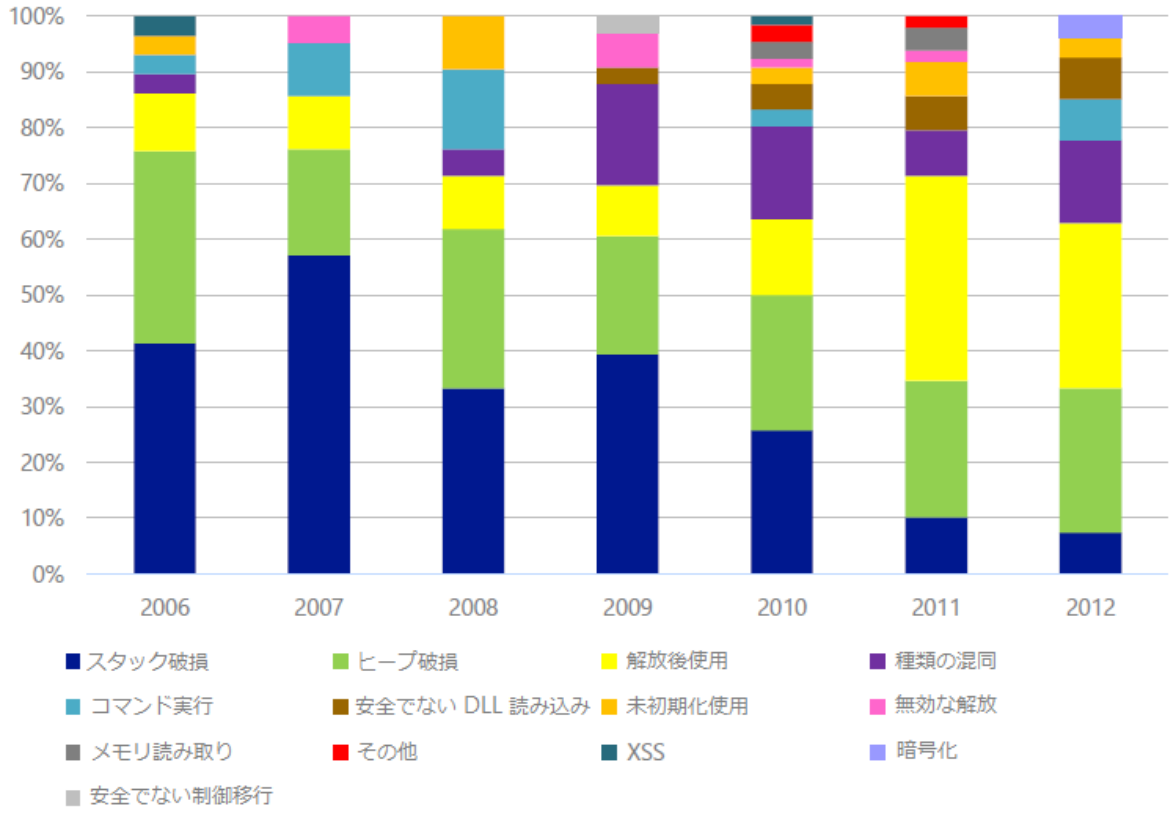
安全な製品への取組み

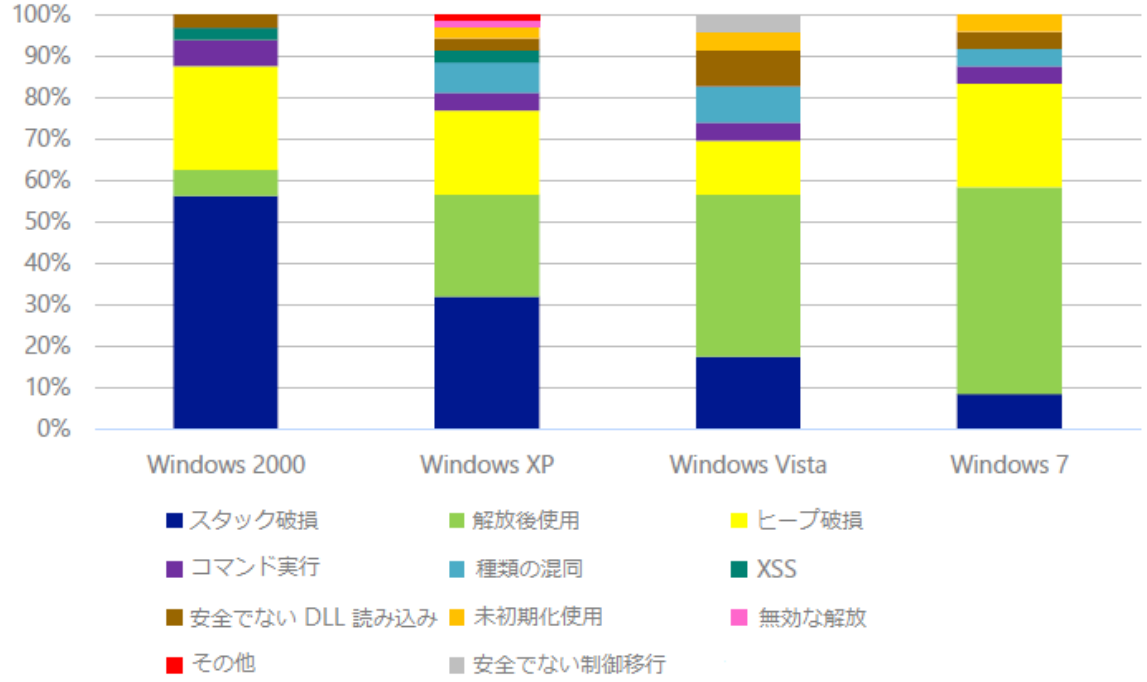
Security Development Lifecycle実施要素

- **Proven extensions of traditional methodologies with measurable results**
- **Holistic approach reducing chances of vulnerabilities entering into code**



悪用された脆弱性の推移





二つの顕著な傾向が確認できる。
ひとつは、スタック破壊が減少していることで、これは /GS, SafeSEH等の緩和策が普及した事と、スタック破壊の脆弱性を検出するための静的分析ツールの性能が向上したことが理由と考えられる。
もう一つは、メモリーの解放後使用に関する脆弱性の増加で、この傾向はクライアント側の脆弱性がターゲットなったことにある。特に、Webブラウザのようなアプリケーションにおいて、発生しやすい脆弱性である事が理由と考えられる。

オペレーティングシステムごとに悪用された脆弱性を分析すると、古いOSほどスタック破壊の脆弱性が悪用され、新しいOSほどメモリー解放後使用の脆弱性が悪用されている。Windows 7では、解放後使用とヒープ破壊が悪用された脆弱性の大半を占めており、スタック破損は主要な脆弱性ではなくなっている。

対策の例：OSとOffice/IEの攻撃緩和対策の一覧(XP SP2-Win7)

	Internet Explorer 6	Internet Explorer 7	Internet Explorer 8	Internet Explorer 9
XP SP2	SEHOP Heap terminate DEP ASLR (image & stacks)	SEHOP Heap terminate DEP ASLR (image & stacks)	SEHOP Heap terminate DEP ASLR (image & stacks)	
XP SP3	SEHOP Heap terminate DEP ASLR (image & stacks)	SEHOP Heap terminate DEP ASLR (image & stacks)	SEHOP Heap terminate DEP ASLR (image & stacks)	
Vista RTM		SEHOP Heap terminate DEP ASLR (image & stacks)	SEHOP Heap terminate DEP ASLR (image & stacks)	
Vista SP1,SP2		SEHOP Heap terminate DEP ASLR (image & stacks)	SEHOP Heap terminate DEP ASLR (image & stacks)	SEHOP Heap terminate DEP ASLR (image & stacks)
Win 7			SEHOP Heap terminate DEP ASLR (image & stacks)	SEHOP Heap terminate DEP ASLR (image & stacks)

	Microsoft Office 2003	Microsoft Office 2007	Microsoft Office 2010
XP SP2	SEHOP DEP ASLR (image&stacks)	SEHOP DEP ASLR (image&stacks)	SEHOP DEP ASLR (image&stacks)
XP SP3	SEHOP DEP ASLR (image&stacks)	SEHOP DEP ASLR (image&stacks)	SEHOP DEP ASLR (image&stacks)
Vista RTM	SEHOP DEP ASLR (image&stacks)	SEHOP DEP ASLR (image&stacks)	SEHOP DEP ASLR (image&stacks)
Vista SP1,SP2	SEHOP DEP ASLR (image&stacks)	SEHOP DEP ASLR (image&stacks)	SEHOP DEP ASLR (image&stacks)
Win 7	SEHOP DEP ASLR (image&stacks	SEHOP DEP ASLR (image&stacks)	SEHOP DEP ASLR (image&stacks)

出典：Mitigating Software Vulnerabilities
http://www.microsoft.com/en-us/download/details.aspx?id=26788

OSごとの対応

	XP RTM, SP1	XP SP2	XP SP3	Vista RTM	Vista SP1, SP2	Win7 RTM, SP1
SEA						
safeSEH	n	y	y	y	y	y
SEHOP	n	n	n	n	OptIn	OptIn
SEHOP perprocess OptIn support	n	n	n	n	n	y
Heap						
Safe unlinking	n	y	y	y	y	y
block header cookies	n	y	y	y	y	y
lookaside/freelist removal	n	n	n	y	y	y
metadata encryption	n	n	n	y	y	y
terminate on corrution (320bit app)	n	n	n	OptIn	OptIn	OptIn
teminate on corrution (64-bit app)	n	n	n	OptIn	OptIn	OptIn
DEP						
NX support (i386)	n	OptIn	OptIn	OptIn	OptIn	OptIn
NX support (amd 64, 32-bit app)	n	OptIn	OptIn	OptIn	OptIn	OptIn
NX support (amd 64, 64-bit app)	n	Always On	Always On	Always On	Always On	Always On
ASLR						
randomization support						
images	n	n	n	OptIn	OptIn	OptIn
stacks	n	n	n	OptIn	OptIn	OptIn
heaps	n	n	n	y	y	y
PEBs/TEBs	n	n	n	y	y	y
entropy (bits)						
images	0	0	0	8	8	8
stacks	0	0	0	14	14	14
heaps	0	0	0	5	5	5
PEBs/TEBs	0	4	4	4	4	4
APIs						
set process DEP policy support	n	n	y	n	y	y

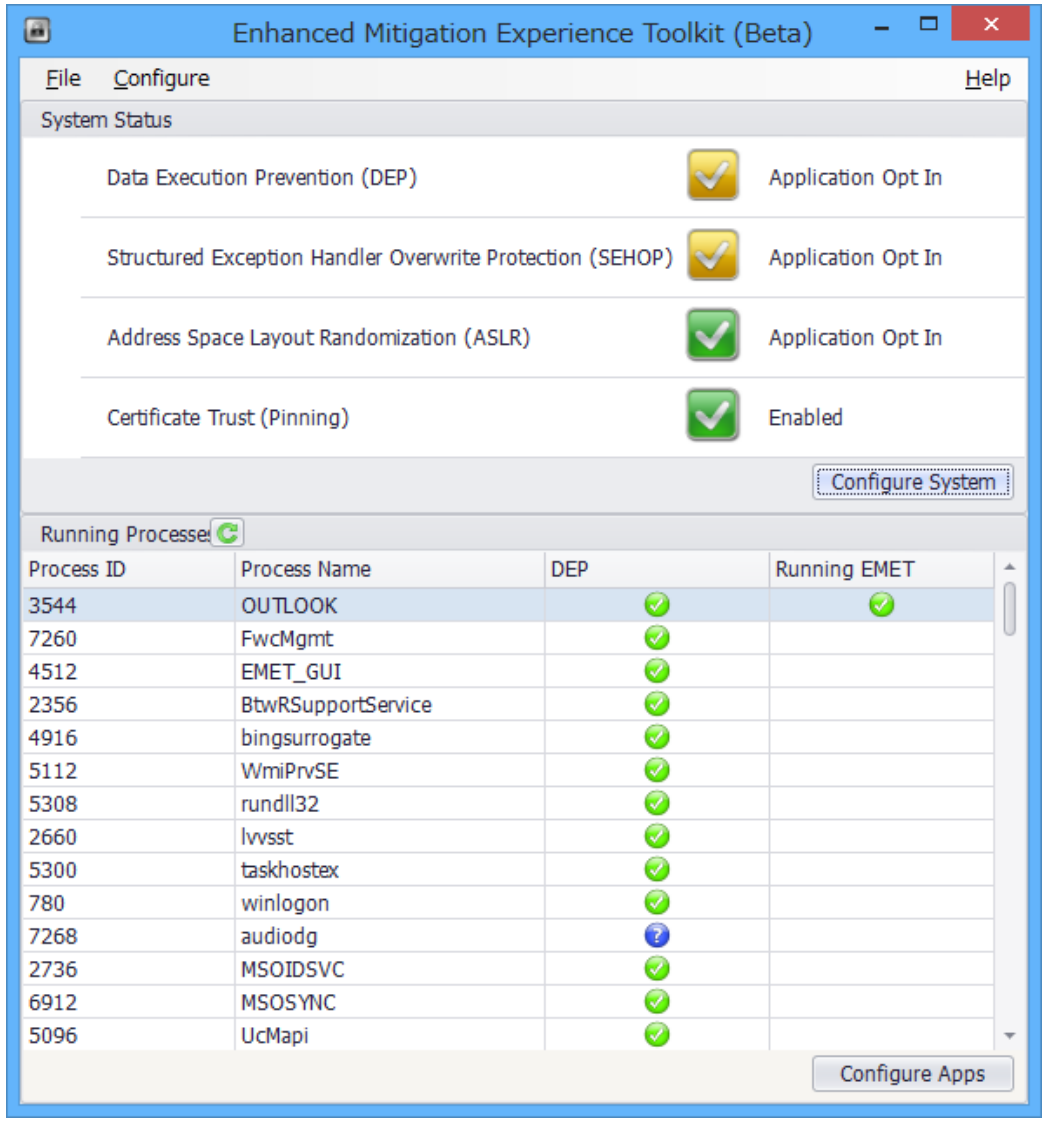
値	説明
n	機能はサポートされていない
y	機能はサポートされ有効になっている
OptIn	機能はサポートされているがデフォルトでは無効になっていない アプリケーションは、明示的に機能を有効にする必要がある
OptOut	機能はサポートされており、デフォルトで有効になっている。 アプリケーションこれを使用しない場合は、明示的に無効にする必要がある
AlwaysOn	機能はサポートされ、有効になっていて、無効にすることが出来ない

コンパイラーにおける対応

Visual C++ Compiler Tools	VC6	VC7(VS2002)	VC7.1(VS2003)	VC8(VS2005)	VC8.1(VS2005 SP1)	VC10 (VS2010)
GS						
stack cookies	n	OptOut	OptOut	OptOut	OptOut	OptOut
String buffers	n	OptOut	OptOut	OptOut	OptOut	OptOut
strict_gs_check pragma	n	n	n	OptIn	OptIn	OptIn
non-pointer arrays	n	n	n	n	n	OptIn
structgs(pure data)	n	n	n	n	n	OptIn
variable reordering	n	n	OptOut	OptOut	OptOut	OptOut
shadow parameter copying	n	n	n	OptOut	OptOut	OptOut
operator new[] integer overflow check	n	n	n	Always On	Always On	Always On
Linker flags						
/DYNAMIC BASE	n	n	n	OptIn	OptIn	OptOut
/SAFESEH	n	n	OptOut	OptOut	OptOut	OptOut
/NXCOMPAT	n	OptIn	OptIn	OptIn	OptIn	OptOut

値	説明
n	機能はサポートされていない
y	機能はサポートされ有効になっている
OptIn	機能はサポートされているがデフォルトでは無効になっていない アプリケーションは、明示的に機能を有効にする必要がある
OptOut	機能はサポートされており、デフォルトで有効になっている。 アプリケーションこれを使用しない場合は、明示的に無効にする必要がある
AlwaysOn	機能はサポートされ、有効になっていて、無効にすることが出来ない

修正できないアプリケーションの対策
EMET: Enhanced Mitigation Experience Toolkit



EMET とは

- ソフトウェアの脆弱性が悪用されるのを防止する無償のセキュリティ ツール
  - 設定を行うことにより、脆弱性緩和技術が組み込まれていないアプリケーションでも、実行時に実装された状態となる
- システム全体、または任意のソフトウェアに対して設定が可能
  - サードパーティ アプリケーション、レガシ アプリケーション、ソースコードが利用不可のアプリケーションなど
- 緩和策
  - データ実行防止 (DEP), メモリ アドレスのランダム化 (ASLR) など
- 対応 OS
  - Windows XP SP3 以降のクライアント、サーバー OS
  - 日本語 OS 対応
- 企業向けの対応
  - Active Directory や System Center Configuration Manager による展開や管理
  - 企業向け マイクロソフト テクニカルサポートを提供 (正式版 EMET のみ)

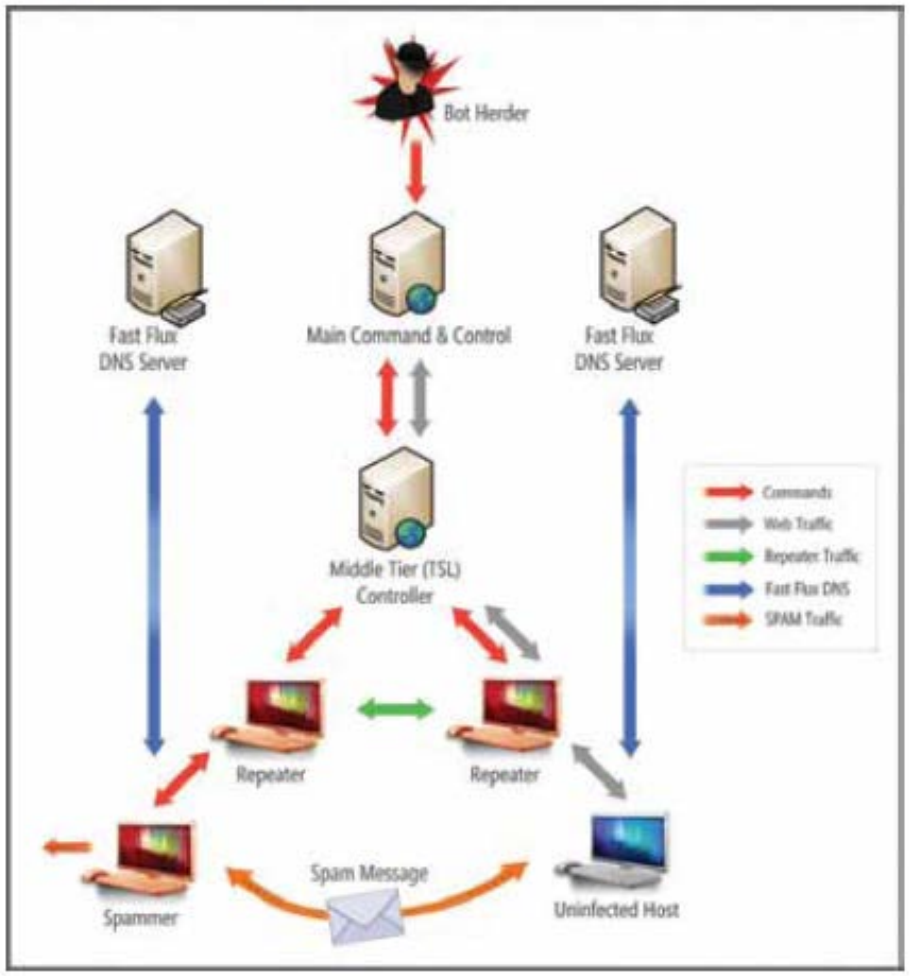
EMET 4.0 ポイント

- 既存の緩和策の強化、既知のバイパスをブロック
- 前バージョンの EMET で報告されていたアプリケーション互換性問題を解決
- 証明書信頼：疑わしい SSL/TLS 証明書を利用しようとする攻撃の検出
- 早期警告プログラム：攻撃や問題を自動でマイクロソフトへ報告
- 監査モード：緩和策のテストを行うための新たな動作オプション

ボットネット対策

ボットネットのTakdown対策

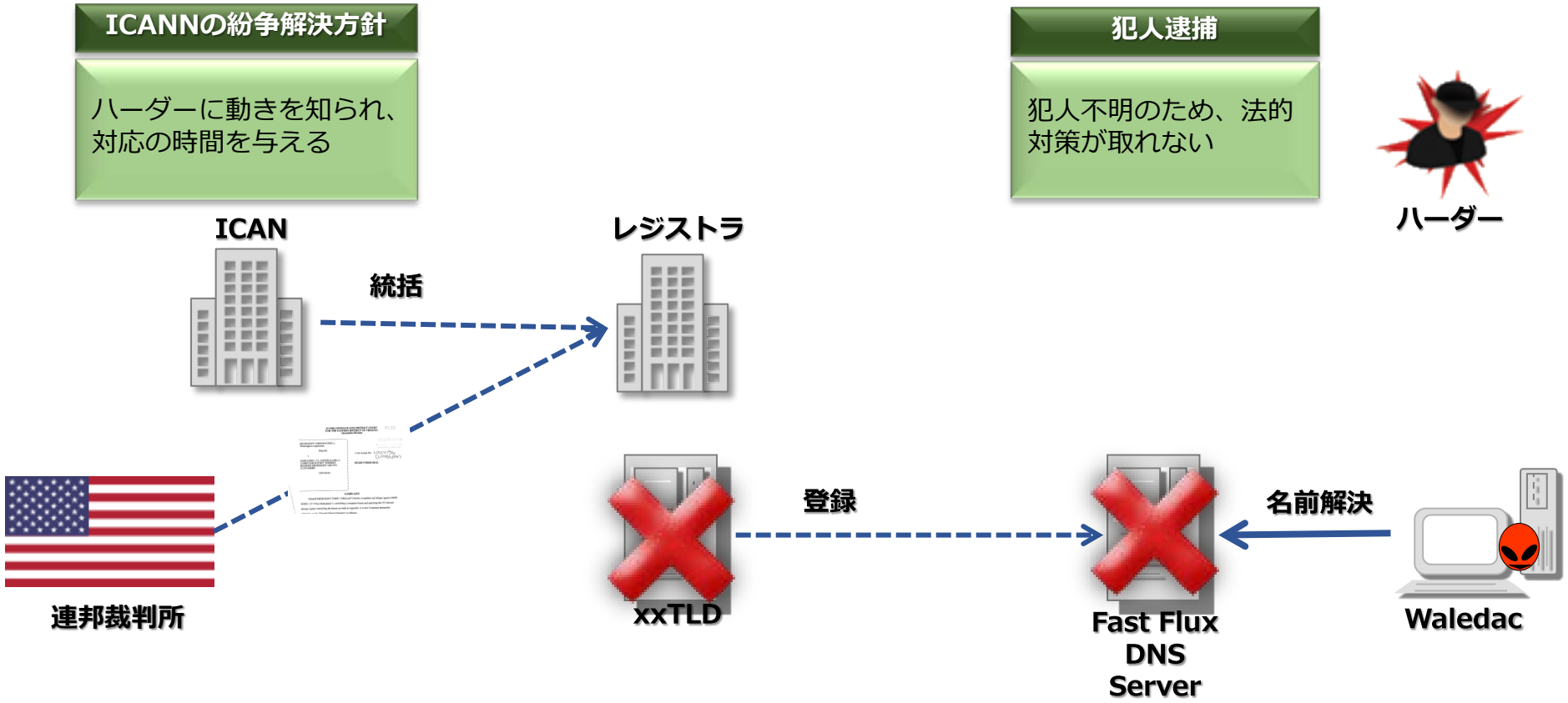
FIGURE 18. The Win32/Waledac tier infrastructure



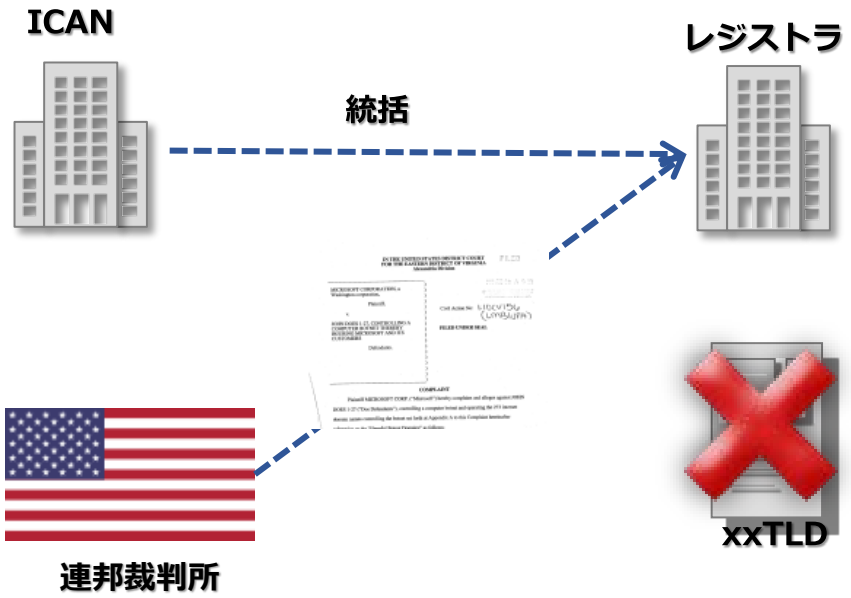
- Waledac等のボットネットは、C&Cサーバーをテイクダウンしても、すぐにボットネットを再構築できるような仕組みを持っている。
  - P2Pネットワークを使ったC&Cの構築
  - バックアップとしての、 Fast Flux DNSの利用

- Waledacの構図
  - スパマー・ノード
    - スパムを送信するためのノード
    - リピーター・ノードと接続し、指揮命令を受ける
  - リピーター・ノード
    - P2Pのアドレスリストを維持し、上位層からの指揮命令を受ける。
    - Fast Flux　DNSに登録される
  - 中間コントローラー
    - リピーター・ノードに対して、指揮命令を行うための中間コントローラー
  - メイン　コマンド・アンド・コントロールサーバー
    - ボットハーダーが、直截操作するC&C。
  - Fast Flux DNSサーバー
    - P2Pによるアドアレスが取得できない場合に問い合せ先を登録するDNSサーバー。

DNSの対策：ホスト名の削除



DNSの対策：ホスト名の削除



一方的な仮処分
(ex parte TRO)

紛争相手への事前通史なしに、一時的（14-28日間）な対処を行うための特別な救済策、証拠隠滅や回避策の実施を阻止するために適用される。
一般に”一方的なTRO“の発行は困難で、連邦原則ルール 65に基づき、**「これを行わない場合に即座に解決できない危害が継続すること」**、**「相手方への通知を行い、それができない場合にはその理由を明確にすること」**を求めている。

連邦裁判所に対する一方的なTRO発行の必要性の訴求

連邦裁判所は、通知を行った場合、訴訟を避け、不法行為を続ける機会があると判断し“一方的なTRO”を発行した。
（30年以上前に偽ブランド品に対して実施）

ドメインが乗っ取られているケースの対処

ドメイン登録者を被告とせず、27のドメイン登録者に対して被告人不詳として訴訟（John Does訴訟）。

中国のレジストラを通じて登録されたドメインの対処

起訴手続きの連邦原則、米国憲法、中国の法律を満たすことを確認し、ハーグ条約に基づいて、中国法務省に依頼

ドメイン登録者に通知

適法手続権利の維持を保証するため、ドメイン登録者に、訴状を送ると共に、電子メール、FAX、書簡による通知を行い、加えて、サイトを作成し、訴訟に関する書面をすべて掲載の上、これをメディアなどを通じて周知
www.noticeofpleadings.com

停止命令が実施されない場合の対処

停止命令が実行され場合に、ドメインの所有権がマイクロソフトに移行するように申請し、認められる。

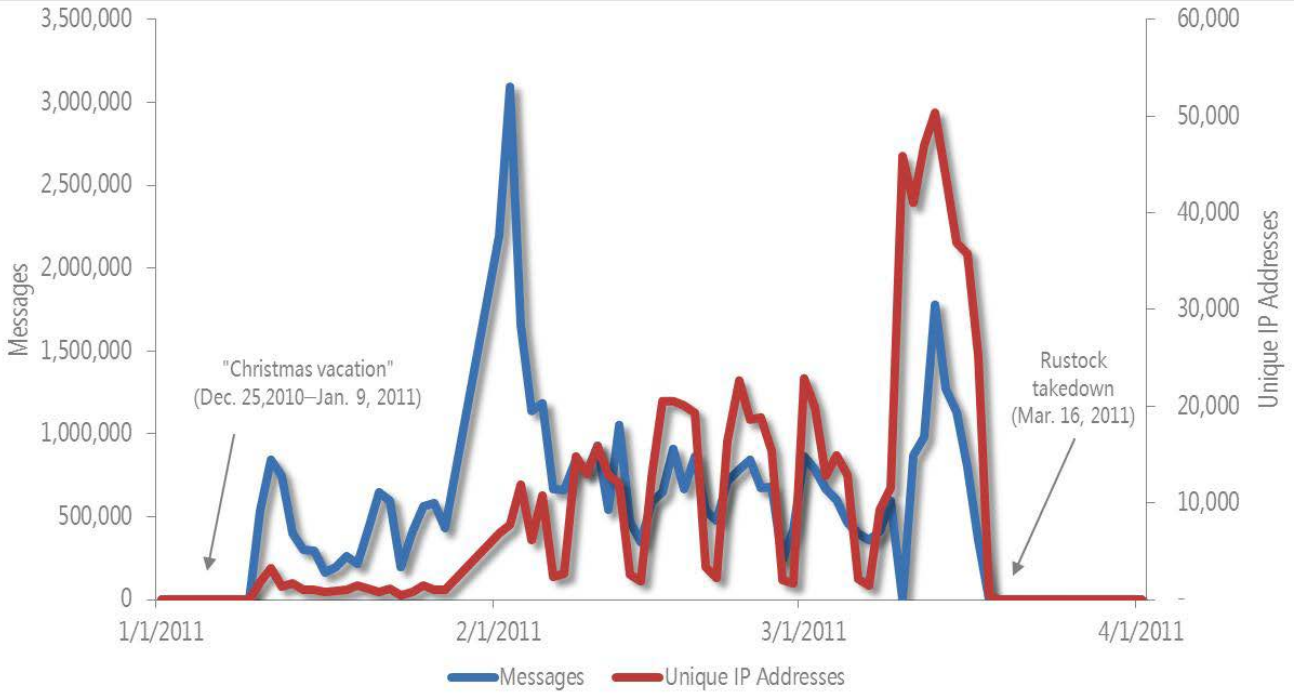
Operation b107:Rustock 解析結果

- 2011年3月16日、米国の7都市に拠点を置くホスティングプロバイダー5社からサーバーを押収
- プロバイダーの支援を受け、ボットネットを制御しているIPアドレスを分断

- ハードディスク20台の解析結果
  - スパムを送信するためのソフトウェアとデータ
    - 数千個の、メールアドレス、ID/パスワードの組み合わせを含んだテキストファイル
    - 42万個以上の電子メールアドレス
    - マイクロソフトや製薬会社の商標を不正に利用したテンプレート
  - ロシアのIPアドレスに対するサイバー攻撃に利用されていたことを示すデータ
  - 匿名インターネットアクセスを提供するノードとして使用
    - 電子メールテンプレート、商標、電子メールアドレスなどを保存する Rustockシステムへの匿名アクセスを提供するために使用したとみられる

- サーバーのホスティング契約を調査
  - オンライン決済サービスを利用
  - アカウントはモスクワ付近の住所が登録
  - C&Cサーバの多くは“Cosma2k”という個人によって設定
  - このニックネームは多数の異なる名前と関連
  - 法的な措置を取るために、これらの名前、電子メールアドレス、その他の証拠に対する調査を継続している

マイクロソフト製品によって検出された Rustock スパム活動



2011 年第 1 四半期に FOPE によって検出された Rustock ボットネットの活動 (受信したメッセージの数と使用された IP アドレスの数)

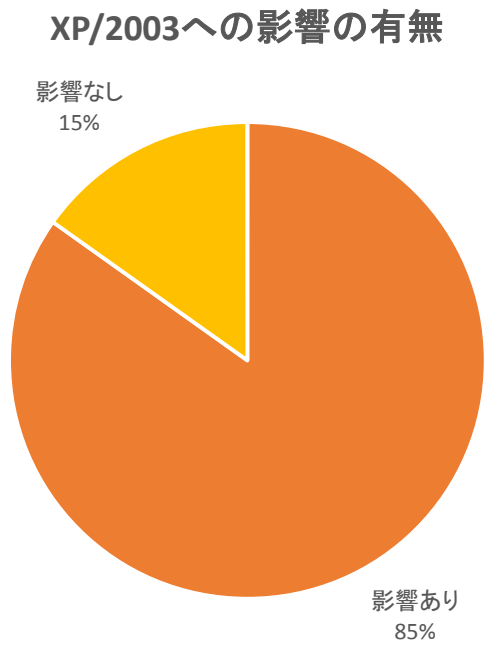
- Rustock から発信される大量のスパムは、Microsoft® Forefront® Online Protection for Exchange (FOPE) を使用して検出
- 2010年12月25日から2011年1月9日の間、Rustockボットネットは完全に非アクティブ
  - クリスマス休暇と、休息期間がぶつかったことの影響？
- 休暇期間後は、通常通りの活動を再開
- 2月初旬までは典型的な安定した活動パターン
- 遮断後の3月中旬には活動量が、ほぼゼロまで急減

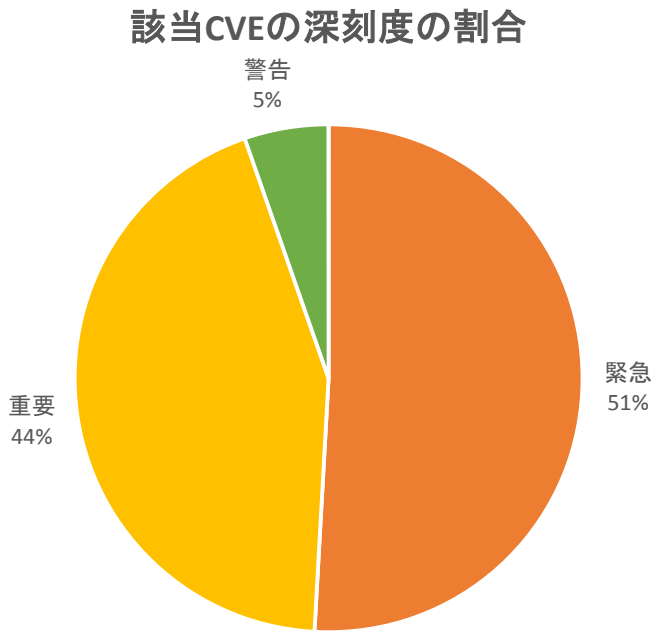
Windows XP に関するセキュリティ更新の分析

セキュリティ更新に関する統計情報 #1

Windows XP/Office 2003に関するCVEの分類　2013/1-8

	件数	緊急	重要	警告
Windows	20	11	35	2
Internet Explorer	9	43	3	1
.NET	5	2	7	1
Office	4	0	4	0
CSRSS	1	0	0	1
Server	1	0	0	1
Silverlight	1	1	0	0
AV	0	0	0	0
合計	**41**	**57**	**49**	**6**





セキュリティ更新に関する統計情報 #2