サイバーセキュリティ 脅威の現状と対策の方向性

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

Microsoft

サイバー攻撃の現状
企業の9割は脅威が侵入済み

サイバー攻撃

- 日本の政府機関への不正アクセス 約**508万件***1
- 企業の**7割**はセキュリティ事故を経験 **9割**は未知の脅威が**侵入済み***2
- 米国納税者アカウント**10万人** 米政府職員**400万人**の情報流出*5
- 侵入から**発見**されるまで**242日**（中央値）*3

被害　推定総額 360兆円*3

- データ侵害に対する平均的なコスト　**4.2億円**
- クレジットカード会社への賠償金　**80億円+***6
- 不正送金被害　**29億円**（企業の被害が増加）
- **120万円**/情報流出した社員(総額**10億**以上)*7

セキュリティ問題
サーバールームから役員室へ

“ネットセキュリティはCEOレベルで対処すべき事項”*3

CEOの61%　ネット攻撃が増加することを心配 *4

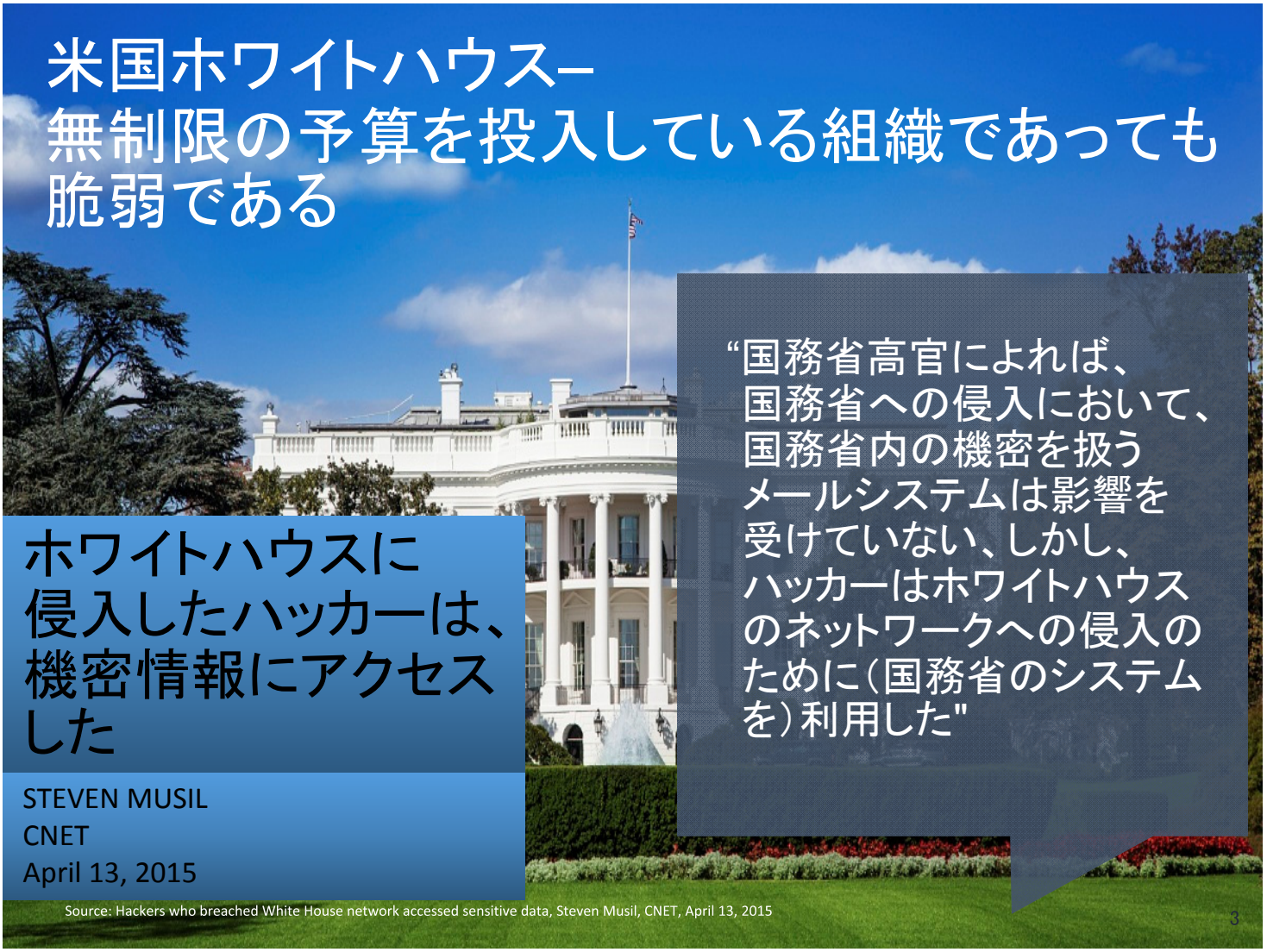
“CEOとCIOが退任” 適切なセキュリティ対策を実施していなかったとの株主からの圧力*6

APAC CIO 調査
新しいテクノロジ採用に際しての最大の障壁

- 予算 81%：新しいテクノロジに対する投資の不足
- 信頼 79%：新しいテクノロジに対するセキュリティ、プライバシーや コンプライアンスの懸念
- 採用に伴う影響 72%：ITに関する決定をする際に、多くの利害関係者が生まれ、意思決定が遅延

*1情報セキュリティ政策会議 2013年度データ
*2 トレンドマイクロ　IT Japan 2015 2015年07月
*3 McKinsey & Co. 高度ネットワーク社会で出来ることとそのリスク: 企業への示唆2014年1月
*4 PwC　グローバル CEO 調査 2015年1月
*5 米内国歳入庁（IRS）　2015年5月　人事管理局　2015年6月
*6 Bloomberg 2015/8/19 , computer weekl y 2015/5/06
*7 Reuters 2015/10/20

米国ホワイトハウス–
無制限の予算を投入している組織であっても脆弱である



ホワイトハウスに侵入したハッカーは、機密情報にアクセスした

STEVEN MUSIL
CNET
April 13, 2015

"国務省高官によれば、国務省への侵入において、国務省内の機密を扱うメールシステムは影響を受けていない、しかし、ハッカーはホワイトハウスのネットワークへの侵入のために(国務省のシステムを)利用した"

Source: Hackers who breached White House network accessed sensitive data, Steven Musil, CNET, April 13, 2015

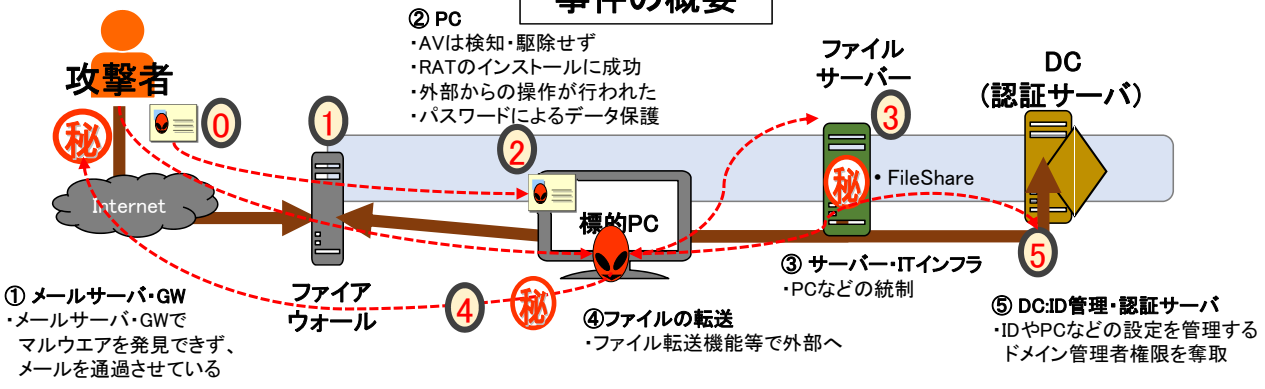
不正アクセスによる被害と事業への影響

動機	手法など	被害		事業への影響
• 愉快犯 • 金銭目的 • テロリズム • 情報(スパイ) • 紛争行為 • 不注意	• 内部犯行 • 標的型攻撃 • 水飲み場攻撃 • マルウエア感染 • ハッキング • 機器破壊	• 情報流出 • 機密情報流出 • データ破壊 • 踏み台 • 不正操作 • DDoS	機密性 Confidentiality 完全性 Integrity 可用性 Availability	• 売上/株価 • 対応/賠償費用 • 金銭的な損害 • 事業継続 • 不正競争被害 • ブランドイメージ

標的型攻撃により、銀行と放送局のPCがダウン。**銀行業務**や**放送業務**が**停止**	**標的型攻撃**により、多数の**偽造証明書**を発行。ルート証明書が無効化され**倒産**	**標的型攻撃**により、製品の**機密情報**が流出。製品の再配布などにより、**多額の費用**が発生	**企業のオンラインバンク**がマルウエアにより不正に操作され、**不正送金**が行われた	**ウィルス感染**により、工場のネットワークが停止し、**生産設備がダウン**
POSシステムへの侵入により、大量の**顧客情報**と**カード情報**が流出	**インターネット接続のない**制御装置を経由して、原子炉の遠心分離機が**破壊された**	上記**機密情報**により、軍事産業へVPN網への**不正アクセス**が行われた	**元社員**が、転職後にシステムを使って**得意先の情報**を転職先に持ち出した	**内部犯行**により、顧客情報が流出。1.5か月の**営業自粛**により、**150億円**の機会損失

典型的な事例としての日本年金機構事案に対する考察

事件の概要



必要とされる視点

①攻撃の検知・防御	②PCやサーバーの権限・設定	③適切な情報保護	④システム的な統制とモニタ(監視・監査)	⑤教育・啓発・訓練
ネットワーク:PC等に到達する攻撃を減少させる ホスト:最新の攻撃を検知しやすい環境 検出:ネットワークやログから攻撃を検知・検出する	マルウエアが動作しない、他のPCやサーバに侵入が困難なシステム・設定を実装する 特に、認証サーバーの設定には配慮する	ファイル(データ)を盗まれても、情報が漏れないような暗号を使った保護を、多段階で行う	PCやサーバ、ネットワーク接続を、一括して管理できる仕組みを構築する この仕組みに基づいたモニタを行い、監視や監査の元データとする	利用者への教育は不可欠、管理者に対する教育も忘れずに行う 事故を想定した訓練を定期的に実施することも重要

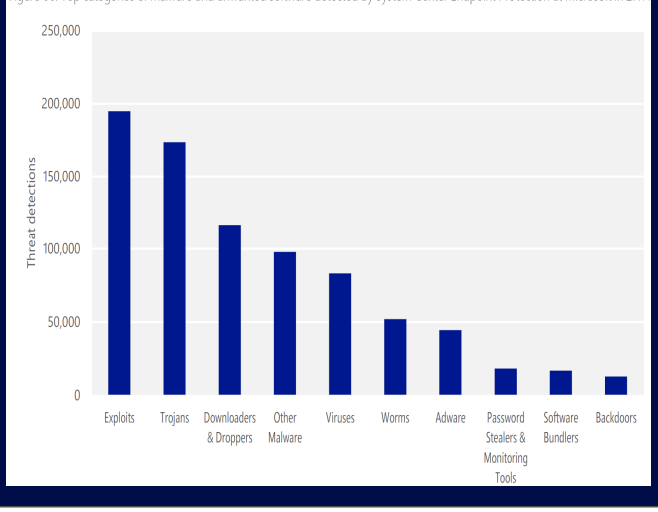
マイクロソフトにおけるマルウエア

マイクロソフトのIT環境

100カ国+ | **15万**人 | **60万**台+

AVの最新のリアルタイム検知適用率
99.85%

Figure 66. Top categories of malware and unwanted software detected by System Center Endpoint Protection at Microsoft in 2H14

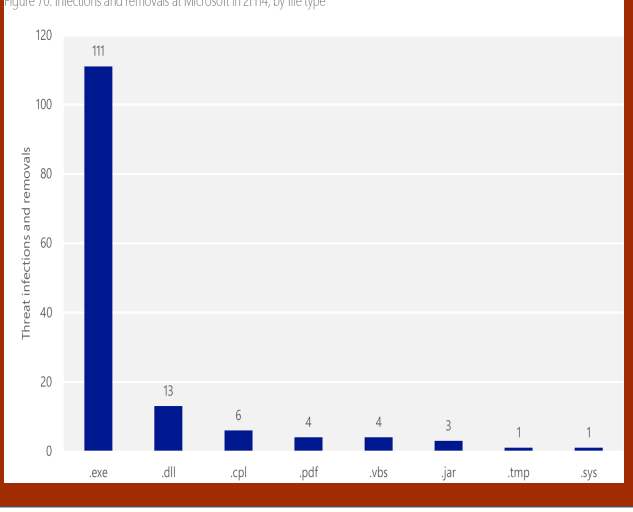


2014年7月-12月 (出典SIR18)

検出**80万**件 | 検出 **2.6** 回/年

感染 **143**件 | 感染 1/**2100**台/年

Figure 70. Infections and removals at Microsoft in 2H14, by file type



敵を知る：攻撃指令　#2015-02-20

ハッカー宣言

- 目的のためには手段を選ばない
- できるだけ楽な方法で攻撃する
- 時間をかけることを厭わない
- 成功するまで続ける
  （失敗を恐れない）

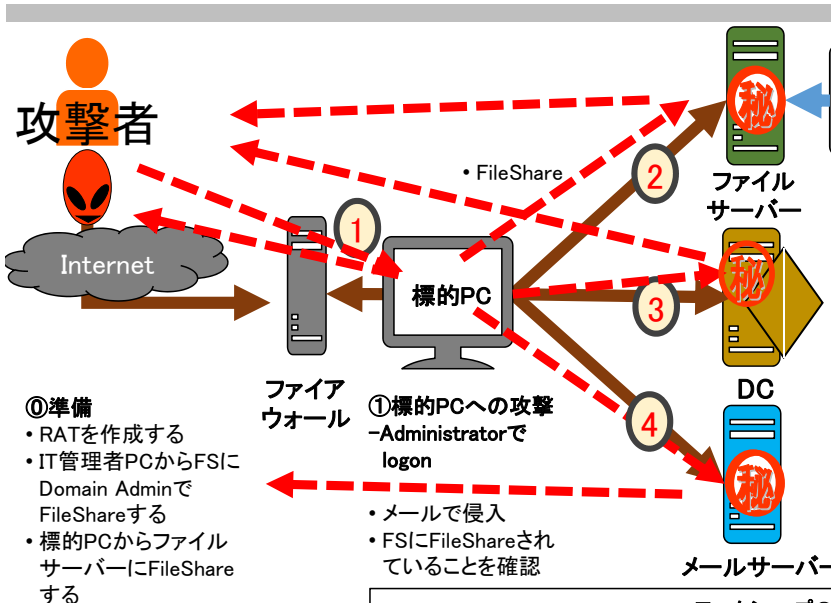
- CONTOSO社が、ID-SEC社を買収すると噂されている
- この買収が実現した場合、ID-SEC社の株価は間違いなく上昇する
- CONTOSO社に侵入し、買収金額と、発表の日程を盗み出せ
- 市場を混乱させるために、その情報を社長名義のメールでメディアにばらまけ

攻撃にあたっての初期情報

- CONTOSO社
  - ITソフトの大手企業
  - http://www.contoso.co.jp/
- ID-SEC社
  - 認証技術に特化したITセキュリティベンダー
  - ID-SEC者が販売する次世代認証技術は、市場を変えるといわれている
- ネットワーク
  - 外部から接続ができるのは、DMZのWebサーバーとメールだけである
  - 社内から社外に対する通信も、メールとWeb以外はすべてブロックされている
- 標的リスト
  - 社長　林　櫂　hkai@contoso.co.jp
  - 人事部長　渋谷　あきこ　sakiko@contoso.co.jp
  - 総務部長　大黒　俊英　otoshihide@contoso.co.jp
  - IT技術者　尾野　里佳子　orikako@contoso.co.jp
  - サポート窓口　support@contoso.co.jp
  - 広報窓口　pr@contoso.co.j
- メディア
  - 読売新聞　社会部　soc@yamn-shinbun.co.jp

標的PC

敵を知る：標的型攻撃体験ワークショップ：シナリオ概要



⓪準備
- RATを作成する
- IT管理者PCからFSにDomain AdminでFileShareする
- 標的PCからファイルサーバーにFileShareする

①標的PCへの攻撃
-Administratorで logon
- メールで侵入
- FSにFileShareされていることを確認

②FSへの攻撃
-Administratorは同一パスワード
- FSを検索し機密情報を取得
- FileShareを使ってツールBをコピー
- コマンドラインから、ツールAを使って、FS上のツールBを実行し、Domain AdminのID/PWDハッシュを取得

③DCへ攻撃
- 取得したハッシュを使って、Domain AdminでDCにFileShare
- NTDSファイルを攻撃者PCにコピー
- ローカルでNTDSをクラックして、すべてのアカウントとパスワードを解析する。

④なりすましメールの送信
- 攻撃者PC上で、閲覧した情報をもとに、なりすましメールを作成。
- 人事部長PCにアップロード
- コマンドラインから、認証SMTPに接続し、メールを送信

ワークショップのポイント
Windows の最新版(8.1以降)をデフォルトで利用すると一連の攻撃は成功しません

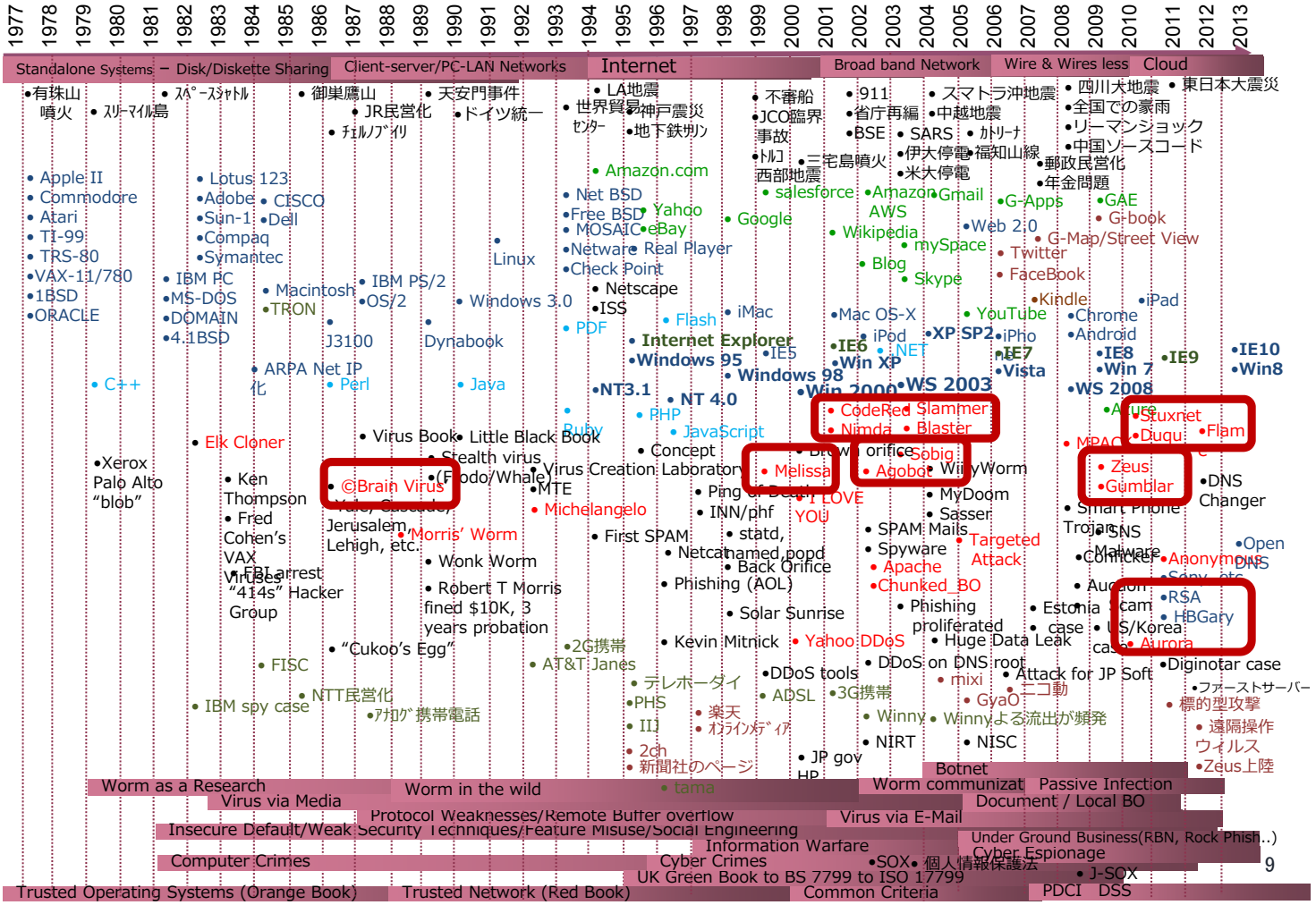
攻撃を成功させるための要因
管理者権限について
　ビルドインアドミニストレータ権限で利用
　UACを無効にする
　ローカルで共通の管理者のアカウントとパスワードが存在する（キッティング等）

メールについて
　実行ファイルが添付されたメールが端末まで届く

端末について
　Office 2003等古いOfficeを利用している
　（保護されたビューが実装されていない）
　最新のセキュリティソフトを利用しない
　最新のOSを利用しない（Windows 8.1, WS 2012R2以降）

Pass-The-Hash対策について
　ドメインアドミニストレーターで作業を行う場合がある
　ダイジェスト認証を有効になっている
　（可逆的にIDとパスワードを保存する必要がある）
　LM認証が有効になっている

30+ years of computing & insecurity

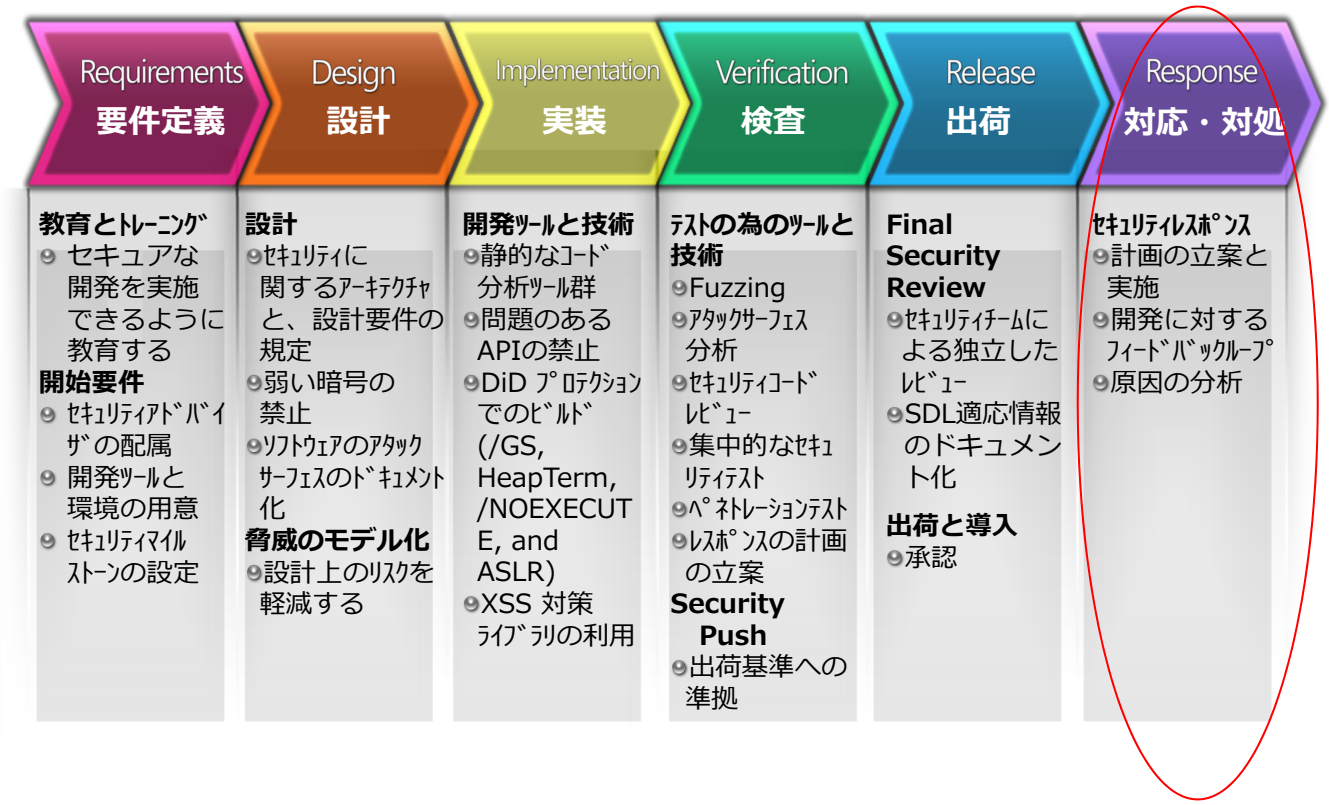


Security Development Lifecycleのコア要素

- **SD³+C：**SDLの基本コンセプト
  - Secure by Design，by Default and in Deployment.
  - Communications
- **脅威モデル（Threat modeling）**

  Threat modeling は、コードレビューでは見つけにくい、バグ以外の脅威を見つけるために有効.
  - アプリケーションの分解と、境界の明確化
  - 脅威の分析・定義と分類
    - **STRIDE** 分析
      - **Spoofing, Tampering, Repudiation, Information disclosure, Denial of service , Elevation of privilege**
  - 攻撃手法の特定
  - 脅威への対策

Security Development Lifecycle実施要素



SDLのISO/IEC 27034-1への適合宣言

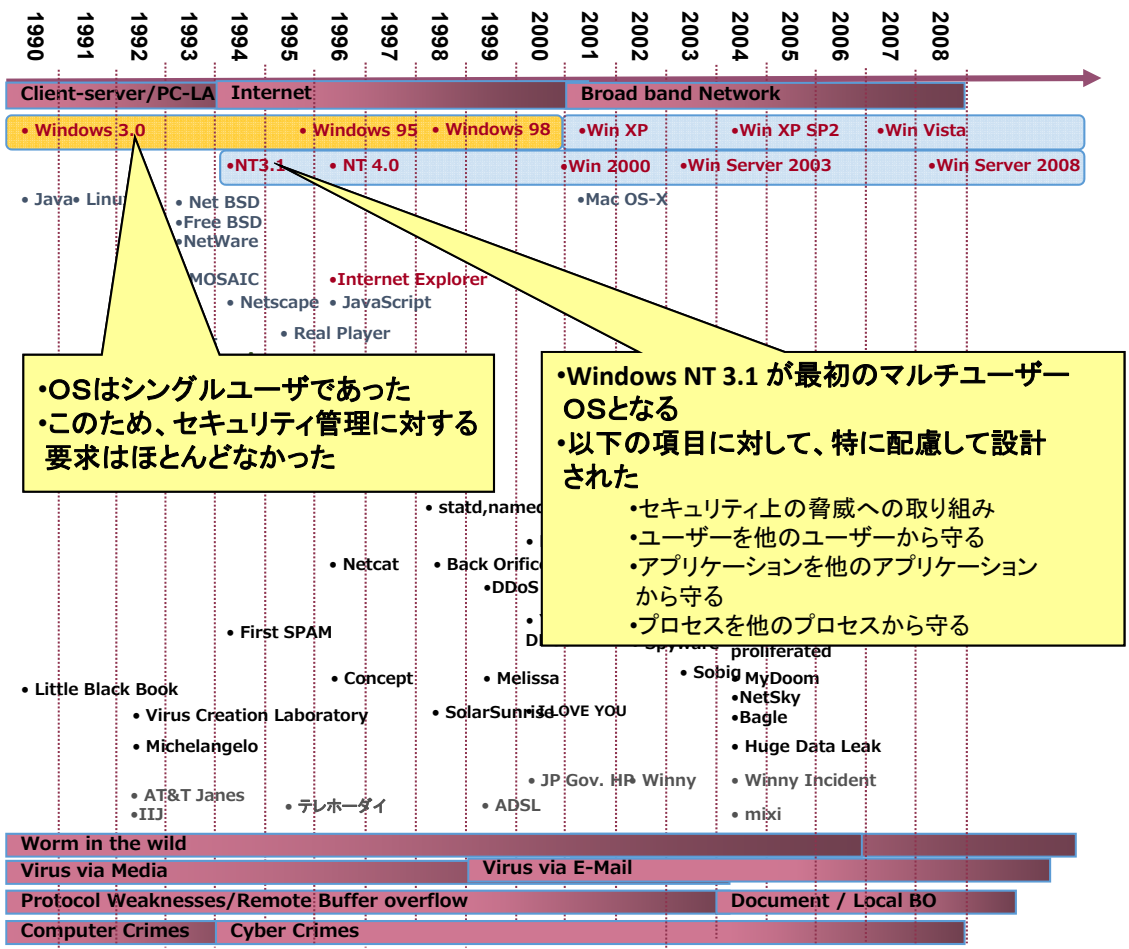
今がそのとき。すべての当事者の最優先事項とすべきセキュリティ開発

- 国際標準化機構 (ISO) と国際電気標準会議 (IEC) は、**セキュリティ開発プロセスに関する標準**が必要であると認識し、**ISO/IEC 27034-1を公開**しました。この新しい国際標準は、包括的なソフトウェア セキュリティ プログラムの構築に必要なプロセスとフレームワークに焦点を当てた初めての標準です。ISO/IEC 27034-1 は、セキュリティを正しい方向に向かわせる重要な一歩であり、組織に多くの可能性をもたらします。マイクロソフトはセキュリティ開発におけるこの重要なマイルストーンを認識し、本日、適合宣言を通じて、**マイクロソフトの SDL が ISO 27034-1 に適合していることを発表**しました。この標準に公に適合することによって、マイクロソフトが、セキュリティ開発に専心しようとする他の企業の見本となることを願っています。
  - **ソフトウェアを開発または販売する企業にとって**、この標準は、セキュリティ開発プラクティスの共通の評価言語を提供し、セキュリティ開発フレームワークを導入するための単純明快な概要を示し、市場で競争力を持つための差別化要因となります。
  - **ベンダーからソフトウェアやサービスを購入するお客様にとって**、この標準は、業界、プラットフォーム、地域全体でのセキュリティ開発を要求する購入者の単一の「言語」を提供します。

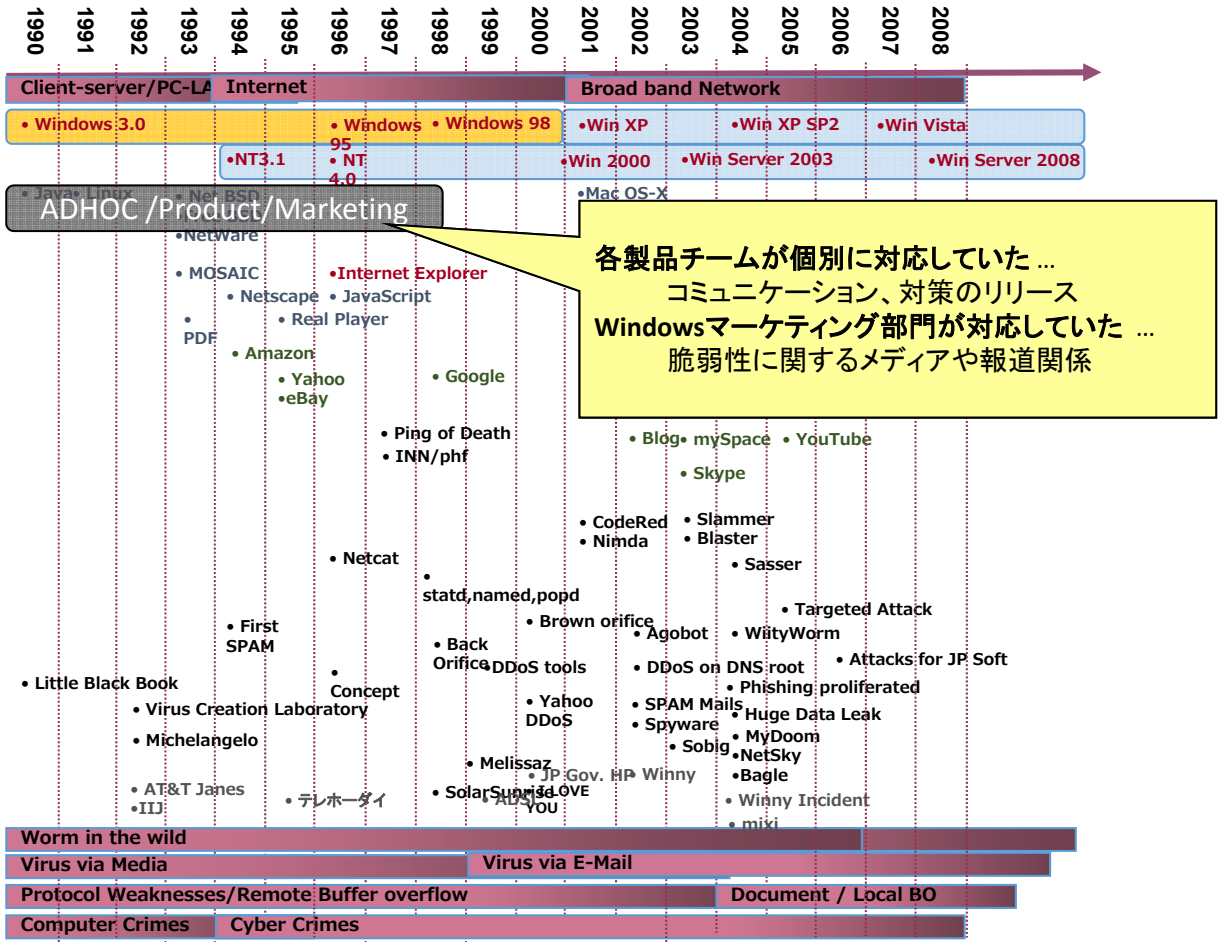
http://blogs.technet.com/b/jpsecurity/archive/2014/07/31/the-time-is-now-security-development-must-be-a-priority-for-everyone.aspx

いかにして
SDLにたどり着いたのか

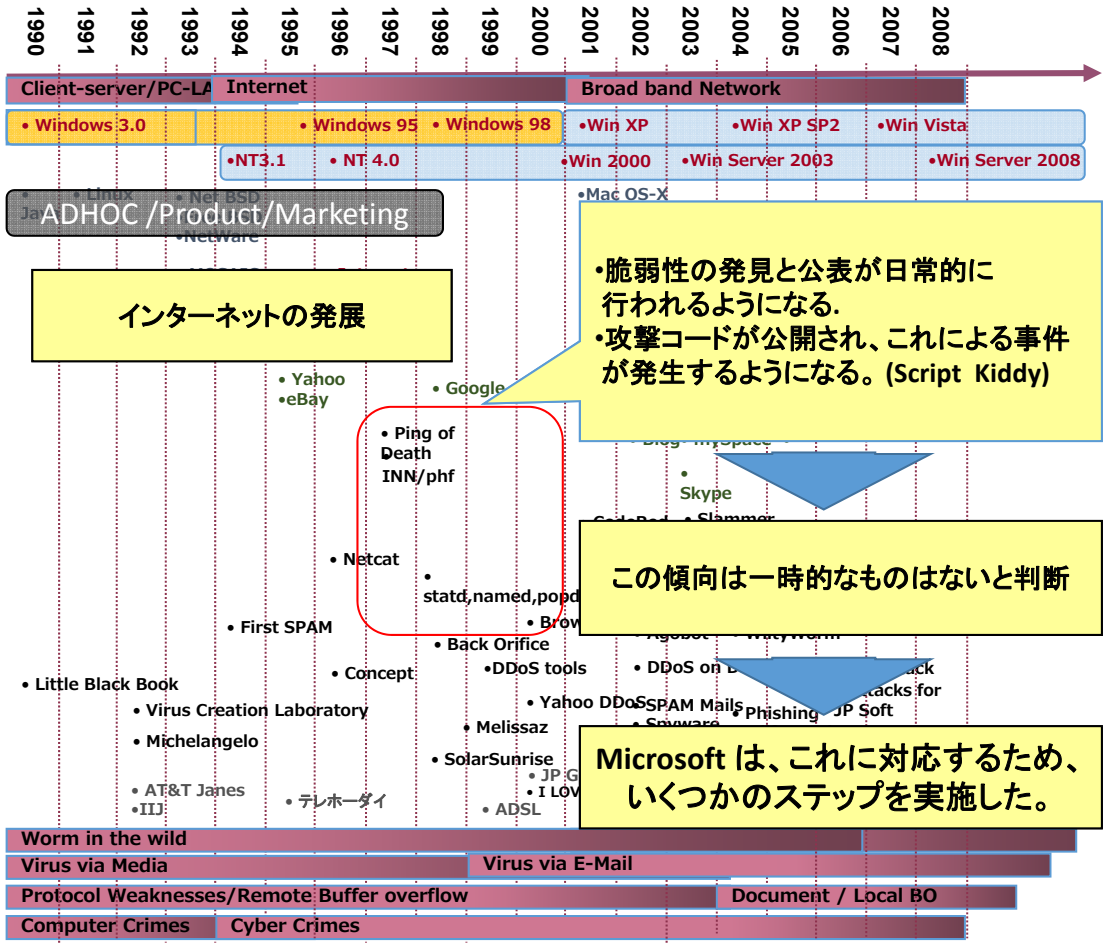
Windows Products and Security



Windows Products and Security: 1998年以前



Windows Products and Security:1990年代中頃



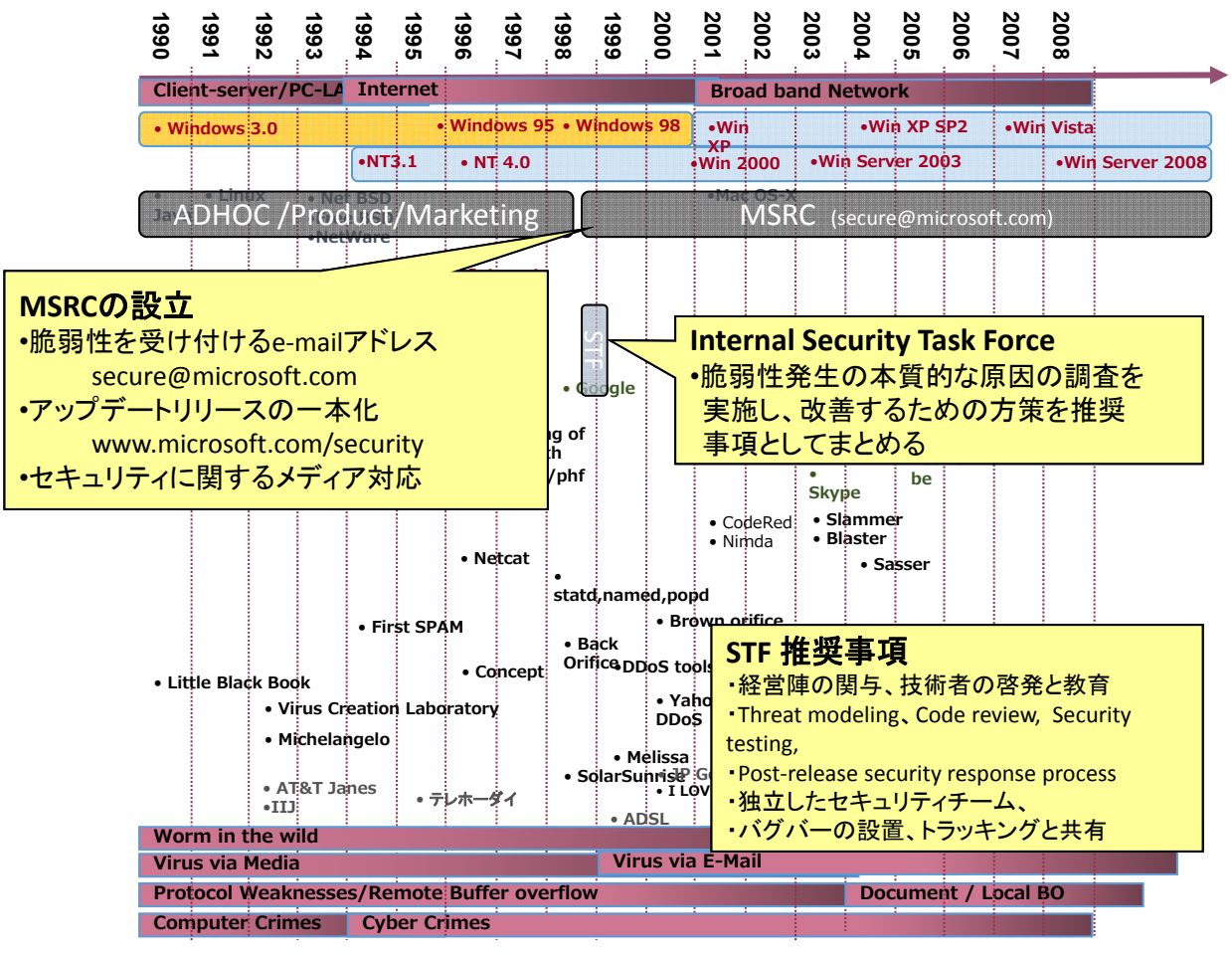
SANS: 最も重要なインターネット上の脅威

The Top 10 Most Critical Internet Security Threats (2000-2001)

1	BIND weaknesses: nxt, qinv and in.named allow immediate root compromise.
2	Vulnerable CGI programs and application extensions (e.g., ColdFusion) installed on web servers
3	Remote Procedure Call (RPC) weaknesses in rpc.ttdbserverd (ToolTalk), rpc.cmsd (Calendar Manager), and rpc.statd that allow immediate root compromise
4	RDS security hole in the Microsoft Internet Information Server (IIS)
5	Sendmail and MIME buffer overflows as well as pipe attacks that allow immediate root compromise
6	sadmind and mountd
7	Global file sharing and inappropriate information sharing via NetBIOS and Windows NT ports 135->139 (445 in Windows2000), or UNIX NFS exports on port 2049, or Macintosh Web sharing or AppleShare/IP on ports 80, 427, and 548
8	User IDs, especially root/administrator with no passwords or weak passwords
9	IMAP and POP buffer overflow vulnerabilities or incorrect configuration
10	Default SNMP community strings set to 'public' and 'private.'

http://www.sans.org/top20/2000/?portal=4f796007065f1ff4653df218233783ff

Windows Products and Security: 最初のステップ



過去のセキュリティ更新情報の検索

Bulletins 1-20 of 20 — Page 1 of 1

Date	Bulletin Number	KB Number	Title	Bulletin Rating
12/23/1998	MS98-020	167614	Patch Available for 'Frame Spoof' Vulnerability	Not Rated
12/21/1998	MS98-019	192296	Patch Av	
12/10/1998	MS98-018	196791	Patch Av	
11/19/1998	MS98-017	195733	Patch Av	
10/23/1998	MS98-016	168617	Update	
10/16/1998	MS98-015	169245	Update	
9/29/1998	MS98-014	193233	Update	
9/4/1998	MS98-013	168485	Fix available for Internet Explorer Cross Frame Navigate Vulnerability	Not Rated
8/18/1998	MS98-012		Updates available for Security Vulnerabilities in Microsoft PPTP	Not Rated
8/17/1998	MS98-011	191200	Update available for "Window.External" JScript Vulnerability in Microsoft Internet Explorer 4.0	Not Rated
8/4/1998	MS98-010		Information on the "Back Orifice" Program	Not Rated
7/27/1998	MS98-009	190288	Update Available for Windows NT Privilege Elevation Attack	Not Rated
7/27/1998	MS98-008		Update Available For Long file name Security Issue affecting Microsoft® Outlook 98 and Microsoft Outlook Express 4.x	Not Rated
7/24/1998	MS98-007	188341	Potential SMTP and NNTP Denial-of-Service Vulnerabilities in Microsoft Exchange Server	Not Rated
7/23/1998	MS98-006	189262	Potential Denial-of-Service in IIS FTP Server due to Passive Connections	Not Rated
7/17/1998	MS98-005		Unwanted Data Issue with Office 98 for the Macintosh	Not Rated
7/14/1998	MS98-004	184375	Unauthorized ODBC Data Access with RDS and IIS	Not Rated
7/2/1998	MS98-003	188806	File Access Issue with Windows NT Internet Information Server (IIS)	Not Rated
6/26/1998	MS98-002	148427	Updates Available for the "The Error Message Vulnerability" Against Secured Internet Servers	Not Rated
6/1/1998	MS98-001	169556	Disabling Creation of Local Groups on a Domain by Non-Administrative Users	Not Rated

Bulletins 1-20 of 20 — Page 1 of 1

7/2/1998	MS98-003	188806	File Access Issue with Windows NT Internet Information Server (IIS)	Not Rated
6/26/1998	MS98-002	148427	Updates Available for the "The Error Message Vulnerability" Against Secured Internet Servers	Not Rated
6/1/1998	MS98-001	169556	Disabling Creation of Local Groups on a Domain by Non-Administrative Users	Not Rated

Download Detailed Bulletin Information

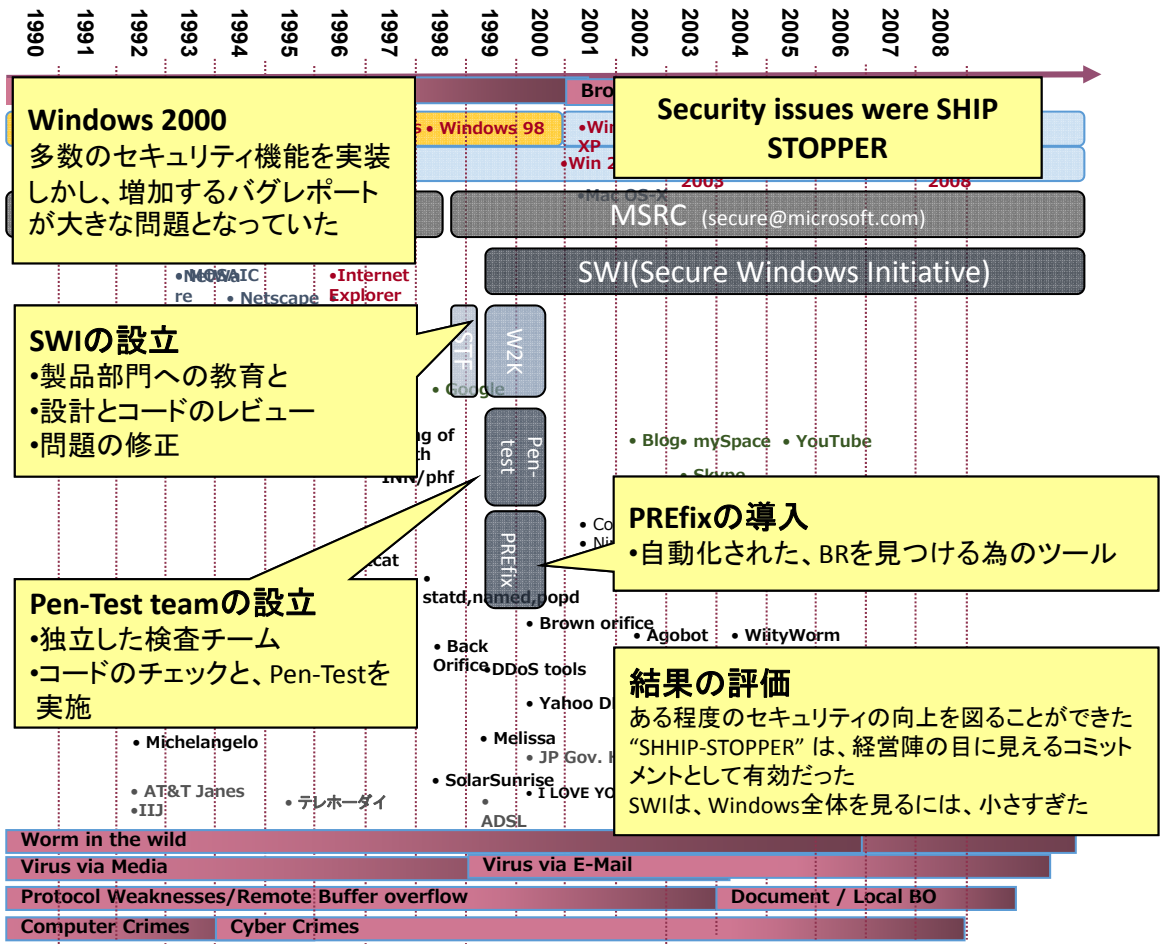
Download detailed information such as affected components, bulletin replacement, reboot requirements, and related CVEs in an Excel file. Additionally, bulletin information in the Common Vulnerability Reporting Framework (CVRF) format is available. Download

http://technet.microsoft.com/en-us/security/dn481339

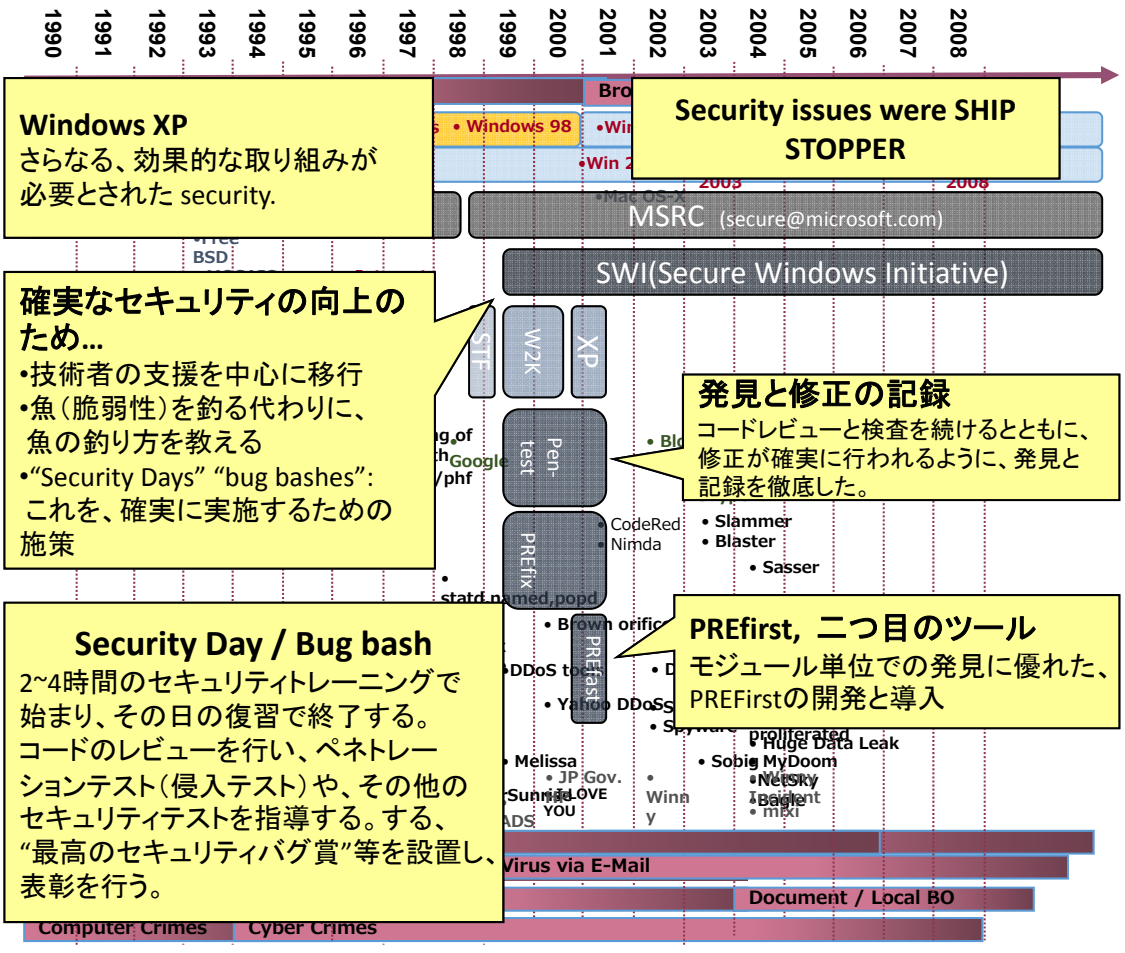
過去の全てのセキュリティ更新情報

	A	B	C	D	E	F	G	H	I	J
1	Date Posted	Bulletin ID	Bulletin KB	Severity	Impact	Title	Affected Product	Component KB	Affected Component	Impact
15235	1998/7/27	MS98-008		None	Remote Code Execution	Update Available For Long fi	Microsoft Windows 98		Microsoft Outlook Express 4	Remote Code Execution
15236	1998/7/27	MS98-008		None	Remote Code Execution	Update Available For Long fi	Microsoft Windows NT 4.0		Microsoft Outlook Express 4	Remote Code Execution
15237	1998/7/27	MS98-008		None	Remote Code Execution	Update Available For Long fi	Microsoft Outlook Express 4.01			Remote Code Execution
15238	1998/7/27	MS98-008		None	Remote Code Execution	Update Available For Long fi	Microsoft Outlook Express 4.01 for Mac			Remote Code Execution
15239	1998/7/24	MS98-007	188341	None	Denial of Service	Potential SMTP and NNTP D	Microsoft Exchange Server 5.0	188341		Denial of Service
15240	1998/7/24	MS98-007	188341	None	Denial of Service	Potential SMTP and NNTP D	Microsoft Exchange Server 5.0 Service Pack 1	188341		Denial of Service
15241	1998/7/24	MS98-007	188341	None	Denial of Service	Potential SMTP and NNTP D	Microsoft Exchange Server 5.0 Service Pack 2	188341		Denial of Service
15242	1998/7/24	MS98-007	188341	None	Denial of Service	Potential SMTP and NNTP D	Microsoft Exchange Server 5.5	188341		Denial of Service
15243	1998/7/23	MS98-006	189262	None	Denial of Service	Potential Denial-of-Service	Microsoft Windows NT Server 4.0	189262	Internet Information Server	Denial of Service
15244	1998/7/23	MS98-006	189262	None	Denial of Service	Potential Denial-of-Service	Microsoft Windows NT Server 4.0	189262	Internet Information Server	Denial of Service
15245	1998/7/23	MS98-006	189262	None	Denial of Service	Potential Denial-of-Service	Microsoft Windows NT Server 4.0	189262	Microsoft Internet Informati	Denial of Service
15246	1998/7/17	MS98-005		None	Information Disclosure	Unwanted Data Issue with C	Microsoft Office 98 for Mac			Information Disclosure
15247	1998/7/14	MS98-004	184375	None	Elevation of Privilege	Unauthorized ODBC Data Ac	Microsoft Windows NT Server 4.0	184375	Microsoft Internet Informati	Elevation of Privilege
15248	1998/7/14	MS98-004	184375	None	Elevation of Privilege	Unauthorized ODBC Data Ac	Microsoft Remote Data Services version 1.5	184375		Elevation of Privilege
15249	1998/7/14	MS98-004	184375	None	Elevation of Privilege	Unauthorized ODBC Data Ac	Microsoft Visual Studio 6.0	184375		Elevation of Privilege
15250	1998/7/2	MS98-003	188806	None	Information Disclosure	File Access Issue with Windo	Microsoft Windows NT Server 4.0	188806	Microsoft Internet Informati	Information Disclosure
15251	1998/7/2	MS98-003	188806	None	Information Disclosure	File Access Issue with Windo	Microsoft Windows NT Server 4.0	188806	Microsoft Internet Informati	Information Disclosure
15252	1998/7/2	MS98-003	188806	None	Information Disclosure	File Access Issue with Windo	Microsoft Windows NT Server 4.0	188806	Microsoft Internet Informati	Information Disclosure
15253	1998/7/2	MS98-003	188806	None	Information Disclosure	File Access Issue with Windo	Microsoft Windows NT Server 4.0	188806	Microsoft Internet Informati	Information Disclosure
15254	1998/7/2	MS98-003	188806	None	Information Disclosure	File Access Issue with Windo	Microsoft Windows NT Workstation 4.0	188806	Microsoft Personal Web Ser	Information Disclosure
15255	1998/7/2	MS98-003	188806	None	Information Disclosure	File Access Issue with Windo	Microsoft Peer Web Server versions 2.0	188806		Information Disclosure
15256	1998/7/2	MS98-003	188806	None	Information Disclosure	File Access Issue with Windo	Microsoft Peer Web Server versions 3.0	188806		Information Disclosure
15257	1998/6/26	MS98-002	148427	None	Information Disclosure	Updates Available for the "T	Microsoft Windows NT Server 4.0	148427	Internet Information Server	Information Disclosure
15258	1998/6/26	MS98-002	148427	None	Information Disclosure	Updates Available for the "T	Microsoft Windows NT Server 4.0	148427	Microsoft Internet Informati	Information Disclosure
15259	1998/6/26	MS98-002	148427	None	Information Disclosure	Updates Available for the "T	Microsoft Site Server 3.0 Commerce Edition	148427		Information Disclosure
15260	1998/6/26	MS98-002	148427	None	Information Disclosure	Updates Available for the "T	Microsoft Site Server 3.0 Enterprise Edition	148427		Information Disclosure
15261	1998/6/26	MS98-002	148427	None	Information Disclosure	Updates Available for the "T	Microsoft Exchange Server 5.0	148427		Information Disclosure
15262	1998/6/26	MS98-002	148427	None	Information Disclosure	Updates Available for the "T	Microsoft Exchange Server 5.5	148427		Information Disclosure
15263	1998/6/1	MS98-001	169556	None	Not a Vulnerability	Disabling Creation of Local G	Microsoft Windows NT Server 3.1	169556		Not a Vulnerability
15264	1998/6/1	MS98-001	169556	None	Not a Vulnerability	Disabling Creation of Local G	Microsoft Windows NT Server 3.5	169556		Not a Vulnerability
15265	1998/6/1	MS98-001	169556	None	Not a Vulnerability	Disabling Creation of Local G	Microsoft Windows NT Server 3.51	169556		Not a Vulnerability
15266	1998/6/1	MS98-001	169556	None	Not a Vulnerability	Disabling Creation of Local G	Microsoft Windows NT Server 4.0	169556		Not a Vulnerability

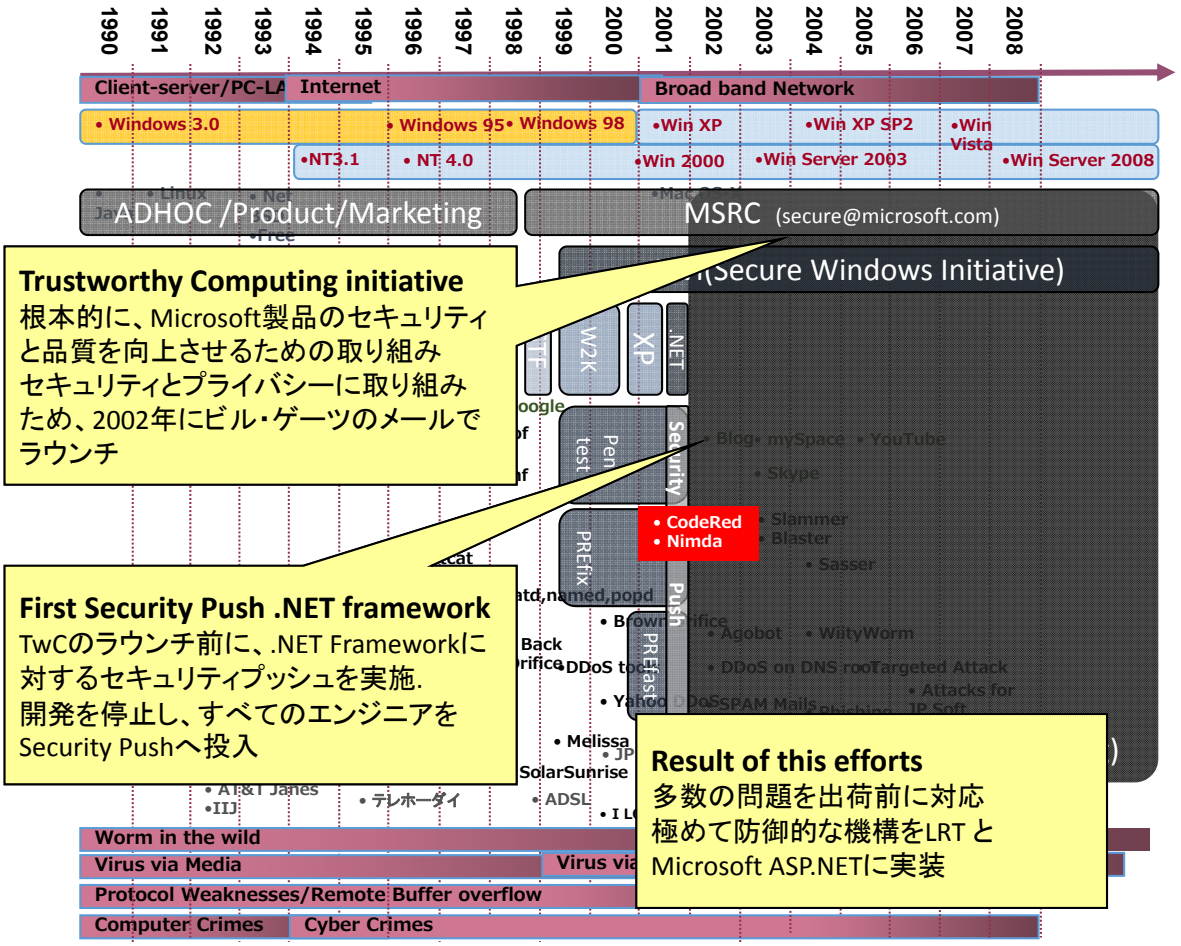
Windows Products and Security: Windows 2000



Windows Products and Security: Windows XP



Windows Products and Security: Worms and TwC



毎週水曜更新へ 2002年5月

毎週火曜にまとめて公開

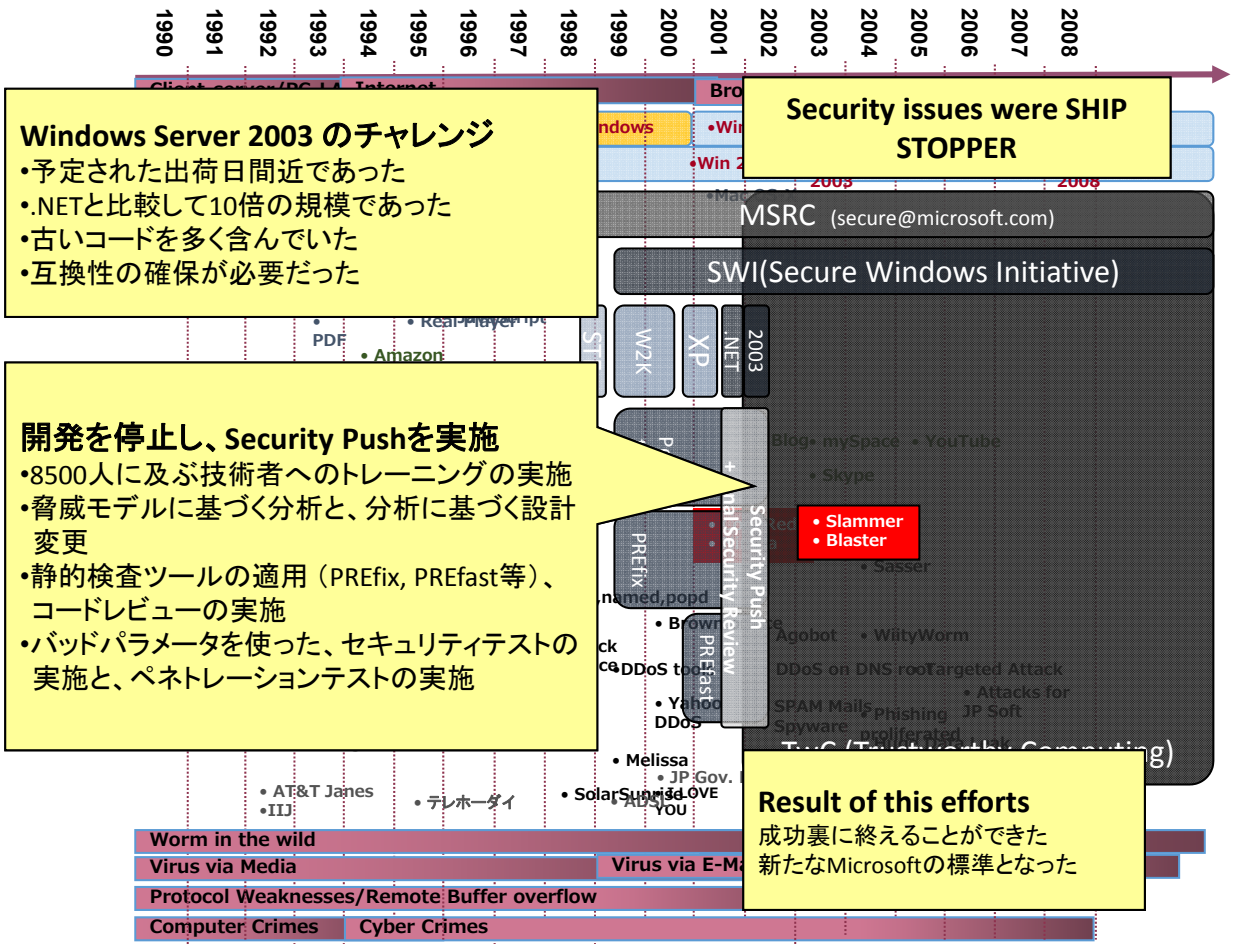
逐次公開

Bulletins 1-18 of 18 — Page 1 of 1

Date	Bulletin Number	KB Number	Title	Bulletin Rating
6/26/2002	MS02-033	322273	Unchecked Buffer in Profile Service Could Allow Code Execution in Commerce Server	Critical
6/26/2002	MS02-032	320920	26 June 2002 Cumulative Patch for Windows Media Player	Critical
6/19/2002	MS02-031	324458	Cumulative Patches for Excel and Word for Windows	Moderate
6/12/2002	MS02-030	321911	Unchecked Buffer in SQLXML Could Lead to Code Execution	Moderate
6/12/2002	MS02-029	318138	Unchecked Buffer in Remote Access Service Phonebook Could Lead to Code Execution	Critical
6/12/2002	MS02-028	321599	Heap Overrun in HTR Chunked Encoding Could Enable Web Server Compromise	Critical
6/11/2002	MS02-027	323889	Unchecked Buffer in Gopher Protocol Handler Can Run Code of Attacker's Choice	Critical
6/6/2002	MS02-026	322289	Unchecked Buffer in ASP.NET Worker Process	Moderate
5/29/2002	MS02-025	320436	Malformed Mail Attribute can Cause Exchange 2000 to Exhaust CPU Resources	Critical
5/22/2002	MS02-024	320206	Authentication Flaw in Windows Debugger can Lead to Elevated Privileges	Critical
5/15/2002	MS02-023	321232	15 May 2002 Cumulative Patch for Internet Explorer	Critical
5/8/2002	MS02-022	321661	Unchecked Buffer in MSN Chat Control Can Lead to Code Execution	Critical
4/25/2002	MS02-021	321804	E-mail Editor Flaw Could Lead to Script Execution on Reply or Forward	Moderate
4/17/2002	MS02-020	319507	SQL Extended Procedure Functions Contain Unchecked Buffers	Moderate
4/16/2002	MS02-019	321309	Unchecked Buffer in Internet Explorer and Office for Mac Can Cause Code to Execute	Critical
4/10/2002	MS02-018	319733	Cumulative Patch for Internet Information Services	Critical
4/4/2002	MS02-017	311967	Unchecked buffer in the Multiple UNC Provider Could Enable Code Execution	Moderate
4/4/2002	MS02-016	318593	Opening Group Policy Files for Exclusive Read Blocks Policy Application	Moderate

Bulletins 1-18 of 18 — Page 1 of 1

Windows Products and Security: Windows Server 2003



毎月第2火曜へ 2003年11月

第2火曜

緊急リリース

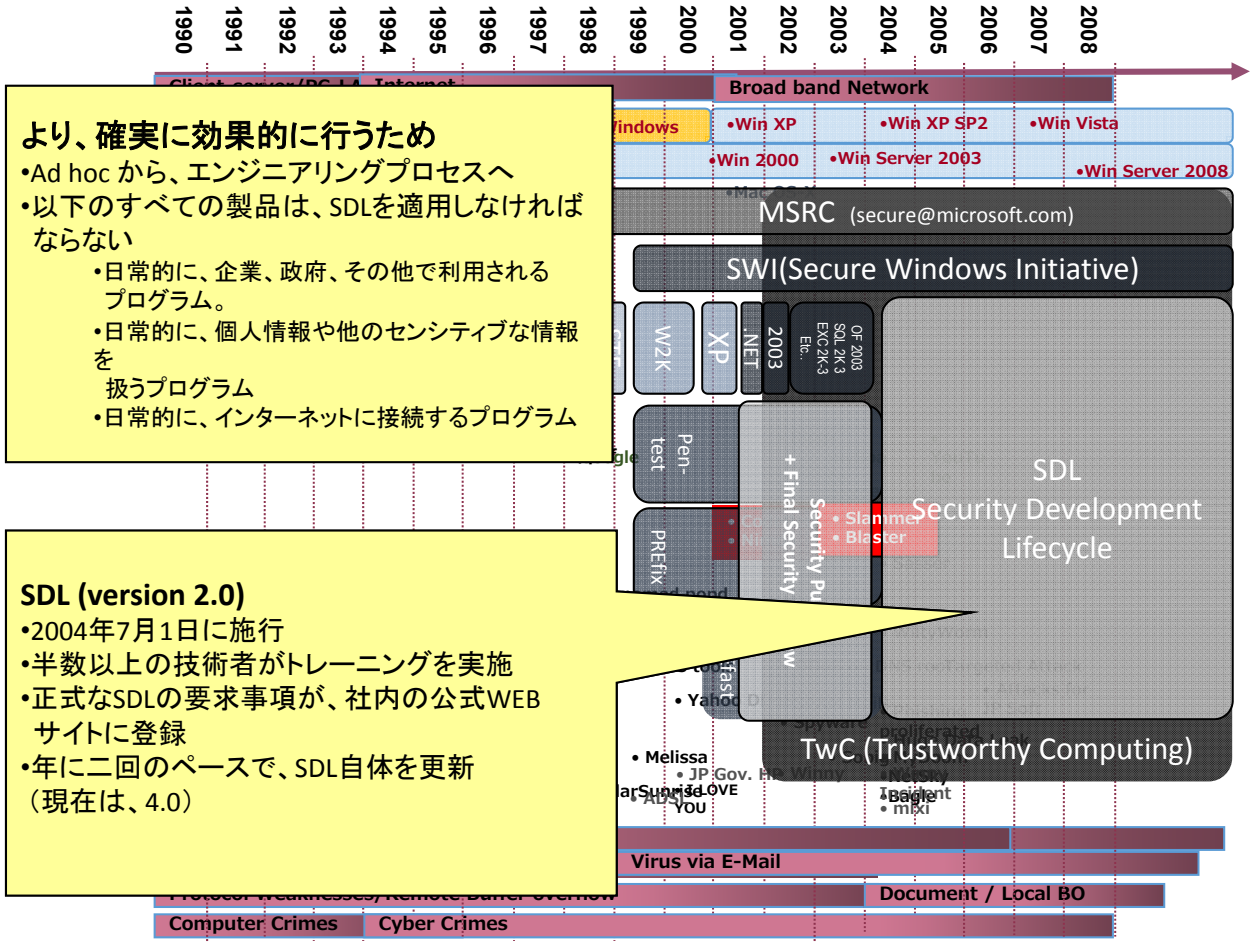
第2火曜

毎週水曜

2/10/2004	MS04-007	828028	ASN.1 Vulnerability Could Allow Code Execution	Critical
2/10/2004	MS04-006	830352	Vulnerability in the Windows Internet Naming Service (WINS) Could Allow Code Execution	Important
2/10/2004	MS04-005	835150	Vulnerability in Virtual PC for Mac Could Allow Privilege Elevation	Important
2/2/2004	MS04-004	832894	Cumulative Security Update for Internet Explorer	Critical
1/13/2004	MS04-003	832483	Buffer Overrun in MDAC Function Could Allow Code Execution	Important
1/13/2004	MS04-002	832759	Vulnerability in Exchange Server 2003 Could Lead to Privilege Escalation	Moderate
1/13/2004	MS04-001	816458	Vulnerability in Microsoft Internet Security and Acceleration Server 2000 H.323 Filter Could Allow Remote Code Execution	Critical
11/11/2003	MS03-051	813360	Buffer Overrun in Microsoft FrontPage Server Extensions Could Allow Code Execution	Critical
11/11/2003	MS03-050	831527	Vulnerability in Microsoft Word and Microsoft Excel Could Allow Arbitrary Code to Run	Important
11/11/2003	MS03-049	828749	Buffer Overrun in the Workstation Service Could Allow Code Execution	Critical
11/11/2003	MS03-048	824145	Cumulative Security Update for Internet Explorer	Critical
10/15/2003	MS03-047	828489	Vulnerability in Exchange Server 5.5 Outlook Web Access Could Allow Cross-Site Scripting Attack	Moderate
10/15/2003	MS03-046	829436	Vulnerability in Exchange Server Could Allow Arbitrary Code Execution	Critical
10/15/2003	MS03-045	824141	Buffer Overrun in the ListBox and in the ComboBox Control Could Allow Code Execution	Important
10/15/2003	MS03-044	825119	Buffer Overrun in Windows Help and Support Center Could Lead to System Compromise	Critical
10/15/2003	MS03-043	828035	Buffer Overrun in Messenger Service Could Allow Code Execution	Critical
10/15/2003	MS03-042	826232	Buffer Overflow in Windows Troubleshooter ActiveX Control Could Allow Code Execution	Critical
10/15/2003	MS03-041	823182	rability in Authenticode Verification Could Allow Remote Code Execution	Critical
10/3/2003	MS03-040	828750	Cumulative Patch for Internet Explorer	Critical
9/10/2003	MS03-039	824146	Buffer Overrun In RPCSS Service Could Allow Code Execution	Critical
9/3/2003	MS03-038	827104	Unchecked buffer in Microsoft Access Snapshot Viewer Could Allow Code Execution	Moderate
9/3/2003	MS03-037	822715	Flaw in Visual Basic for Applications Could Allow Arbitrary Code Execution	Critical

Bulletins 1-25 of 28 Page 1 of 2

Windows Products and Security: never end story



SDLに関して学んだこと

- **セキュリティテスト**は、重要な要素だが、十分ではない
- **セキュアコーディング**は、重要な要素だが、十分ではない
- **脅威分析**は、重要な要素だが、十分ではない
- **エンジニアの啓発とトレーニング**は、重要な要素だが、十分ではない
- **経営陣のコミットメント**は重要な要素だが、十分ではない
  - これらのすべては、個別に実施していたのでは効果的ではない
- 必要とされる要素を、効果的かつ安定したエンジニアリングとしてプロセスとする必要がある。
  - 具体的な手法については、最初のページ **“Security Development Lifecycle Overview”** を見てください

マイクロソフトの深刻度評価システム

セキュリティ情報の深刻度評価システム

価	定義
緊急 (Critical)	ユーザーの操作なしでコード実行の悪用が行われる可能性のある脆弱性です。これらのシナリオには、自己増殖性のマルウェア（例：ネットワーク ワーム）、もしくは、警告やプロンプトが表示されずにコード実行が起こる、避けることのできない一般的なシナリオなどが含まれます。Web ページを閲覧する、あるいは、メールを開ける可能性があるということを意味します。マイクロソフトは、お客様が緊急の更新プログラムを早急に適用することを推奨します。
重要 (Important)	この脆弱性が悪用された場合、ユーザー データの機密性、完全性または可用性が侵害される可能性があります。または、処理中のリソースの完全性または可用性が侵害される可能性があります。これらのシナリオには、クライアントが、プロンプトの出所、品質、あるいはユーザビリティに関わらず、表示された警告やプロンプトを受け入れるという一般的に使用されるシナリオが含まれます。プロンプト、もしくは警告を生成しない一連のユーザー アクションも網羅されています。マイクロソフトは、お客様が重要な更新プログラムをできる限り早く、適用することを推奨します。
警告 (Moderate)	脆弱性の影響は、認証要件、または、非デフォルト設定に対してのみ適用性があるなどの要素によって、大幅に緩和されます。マイクロソフトは、お客様がセキュリティ更新プログラムを適用することを検討することを推奨します。
注意 (Low)	脆弱性の影響は、影響を受けるコンポーネントの特性によって、包括的に緩和されます。マイクロソフトは、お客様が影響を受けるシステムに対してセキュリティ更新プログラムを適用するか否か判断することを推奨します。

セキュリティ情報の深刻度評価システム
http://technet.microsoft.com/ja-jp/security/gg309177.aspx

悪用可能性指標

Exploitability Indexの評価	簡単な定義
1	悪用コードの可能性*
2	悪用コードの作成困難**
3	悪用コードの可能性低***

* 以前の定義: 安定した悪用コードの可能性
** 以前の定義: 不安定な悪用コードの可能性
*** 以前の定義: 機能する見込みのない悪用コード

サービス拒否の悪用可能性の評価	定義
一時的	この脆弱性が悪用されると、攻撃が停止される、または想定外に停止して、自動的に回復するまでオペレーティング システムまたはアプリケーションが一時的に応答しなくなる可能性があります。攻撃が終了するとすぐに、標的の機能性が通常レベルに戻ります
永続的	この脆弱性が悪用されると、手動で再起動する、または自動的に回復せずに想定外に停止するまで、オペレーティング システムまたはアプリケーションが永続的に応答しなくなる可能性があります。

Microsoft Exploitability Index (悪用可能性指標)
http://technet.microsoft.com/ja-jp/security/cc998259

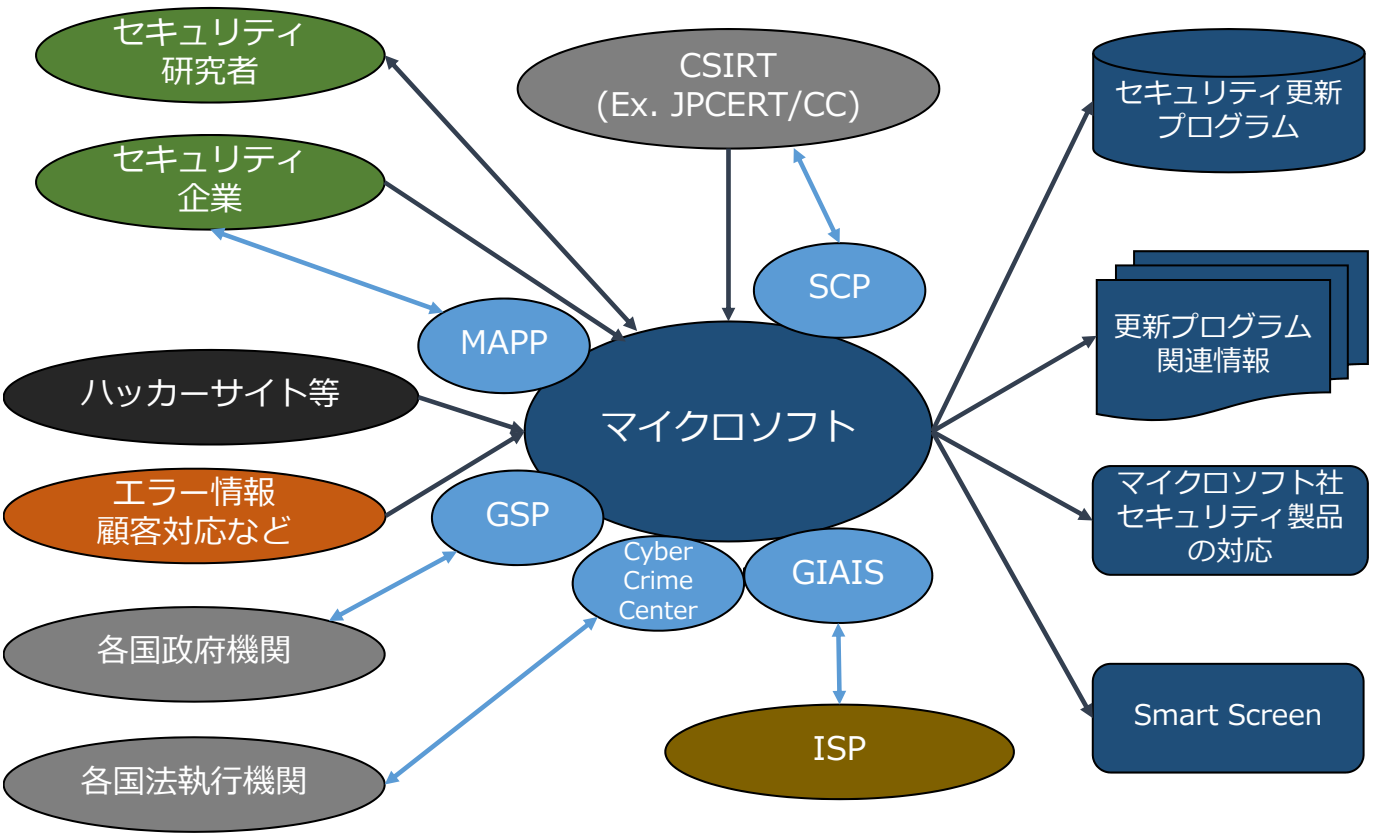
脆弱性対応プロセス

セキュリティ更新公開までの期間 - イメージ図

関連組織との連携

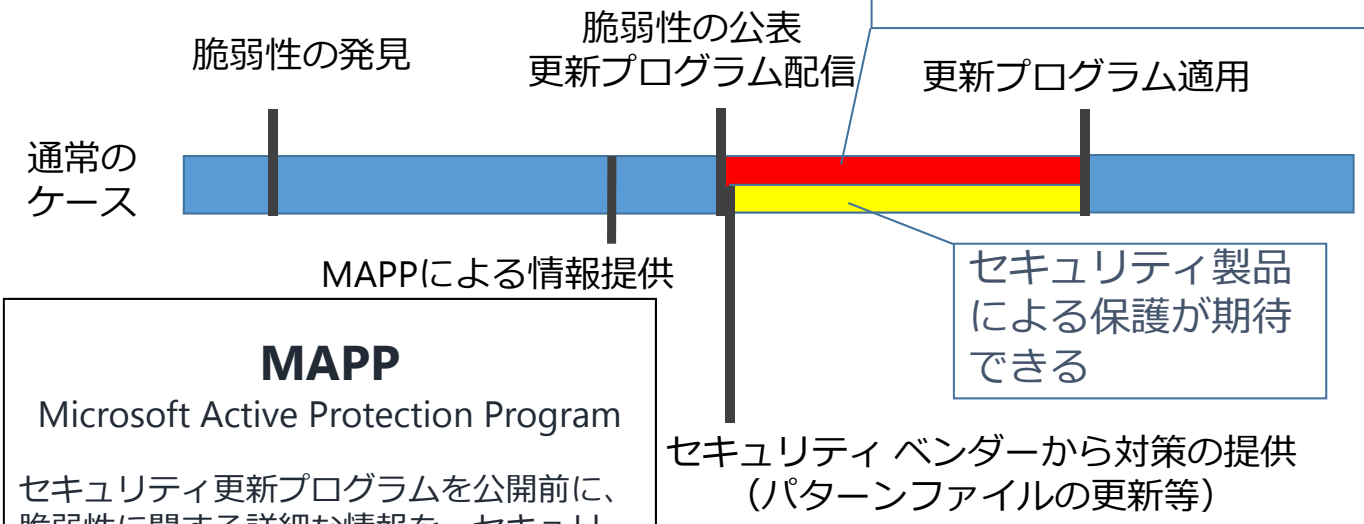
@マイクロソフト

- マルウエアの収集・解析（世界 5 箇所の MMPC ラボ）
  - 1 日当たり 15 万ウイルス検体
- 感染データなどに基づいた脅威観測および解析
  - 1 日当たり 1500 万テレメトリ観測



標準的な脆弱性への対応プロセス

公開情報を分析し、脆弱性を探し、**攻撃コードが開発**されるため、公表されたら、更新プログラム適用までの時間を、短くすることが重要



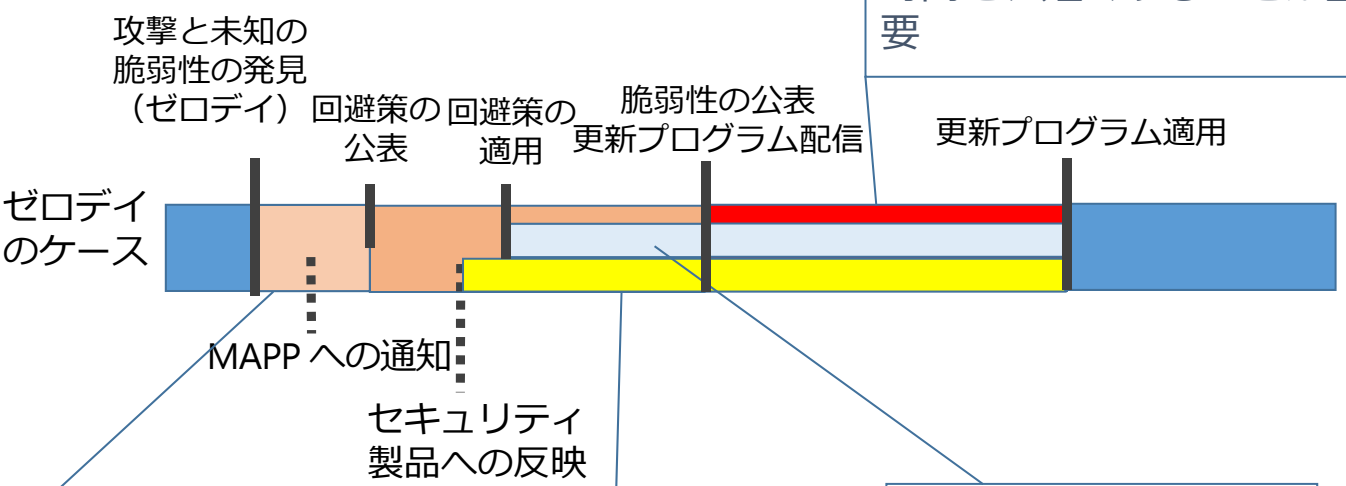
MAPP

Microsoft Active Protection Program

セキュリティ更新プログラムを公開前に、脆弱性に関する詳細な情報を、セキュリティ関連企業に通知することで、更新プログラム公開と同時に、セキュリティソフトによる利用者の保護を行うための取り組み

ゼロデイのケース

公開情報を分析し、脆弱性を探し、**攻撃コードが開発**されるため、公表されたら、更新プログラム適用までの時間を、短くすることが重要



攻撃の状況について、様々な手法でモニターをし、常に状況の把握に努める

セキュリティ製品による保護が期待できる

回避策により、攻撃を防ぐことができる

Microsoft Active Protections Program(MAPP)

- MAPP for Security Vendors
  - 現行のMAPPプログラムに、セキュリティ更新プログラムを事前に評価を提供するMAPP Validationを追加
  - 公表前日から３日前に情報を提供するように変更
    - MAPPに参加したばかりのベンダーは、これまで通り１日前に提供
- MAPP for Responders
  - 技術的な脅威情報（悪意のあるURL、ファイルハッシュ、検知ガイダンス）と、傾向などを含んだより一般的な情報を共有するメカニズム
- MAPP Scanner
  - Officeドキュメント、PDFファイル、URLに対するコンテンツベースの攻撃をスキャンするクラウドベースのサービス
  - 静的な解析に加えて、脆弱性の利用についての分析も行う
  - 新しい攻撃を早期に発見することにつながることを期待

MAPP Partners with Updated Protections

Microsoft Security Advisory (2963983)

Vulnerability in Internet Explorer Could Allow Remote Code Execution

MAPP Partners who have released protections within 48 hours of the release of the Microsoft Security Advisory

- Antiy Labs
- Avira GmbH
- Check Point Software
- Cisco
- Cyberoam Technologies Pvt. Ltd.
- Enterasys
- Eset
- Freescale
- Huawei
- McAfee
- Network-box
- NSFocus
- PaloAlto Networks
- SonicWALL
- Sophos
- Sourcefire
- symantec (messagelabs)
- Trend Micro
- Trustwave
- WinsTechNet (Nowcom)
- Zscaler

MAPP Partners who have released protections from 96 hours after the release of the Microsoft Security Advisory

- AdLAb (Venustech)
- Ahnlab
- Avast! Software
- Beijing Leadsec (Lenovo)
- Beijing Rising
- Emerging Threats Pro
- Estsoft
- Fortinet
- F-Secure
- Juniper
- Kaspersky
- K7Computing
- NETASQ
- Niksun
- Quickheal
- Sangfor
- Stonesoft

LNK脆弱性:ドキュメントの埋め込みショートカット

2010年07月21日 19:20

sean_sullivan
F-Secure Corporation
ヘルシンキ発 by:ショーン・サリバン

Microsoftが「セキュリティアドバイザリ 2286198(バージョン1.2)」をアップデートした。

Microsoftの人たちが、懸命にこの問題に取り組んでいることは非常に明白だ。我々の懸念は対処されており、同アドバイザリはもはやWindows 7 AutoPlayを緩和策とはしていない。

そして今度は悪いニュース。

同アドバイザリのバージョン1.2には、新しい重要な詳細が含まれている:

「エクスプロイトは、埋め込みショートカットをサポートする特定の文書タイプにも含まれる可能性がある。」

How could an attacker exploit the vulnerability?
An attacker could present a removable drive to the user with a malicious shortcut file, and an associated malicious binary. When the user opens this drive in Windows Explorer, or any other application that parses the icon of the shortcut, the malicious binary will execute code of the attacker's choice on the victim system.

An attacker could also set up a malicious Web site or a remote network share and place the malicious components on this remote location. When the user browses the Web site using a Web browser such as Internet Explorer or a file manager such as Windows Explorer, Windows will attempt to load the icon of the shortcut file, and the malicious binary will be invoked. In addition, an attacker could embed an exploit in a document that supports embedded shortcuts or a hosted browser control (such as but not limited to Microsoft Office documents).

文書 – Microsoft Office書類のような文書。

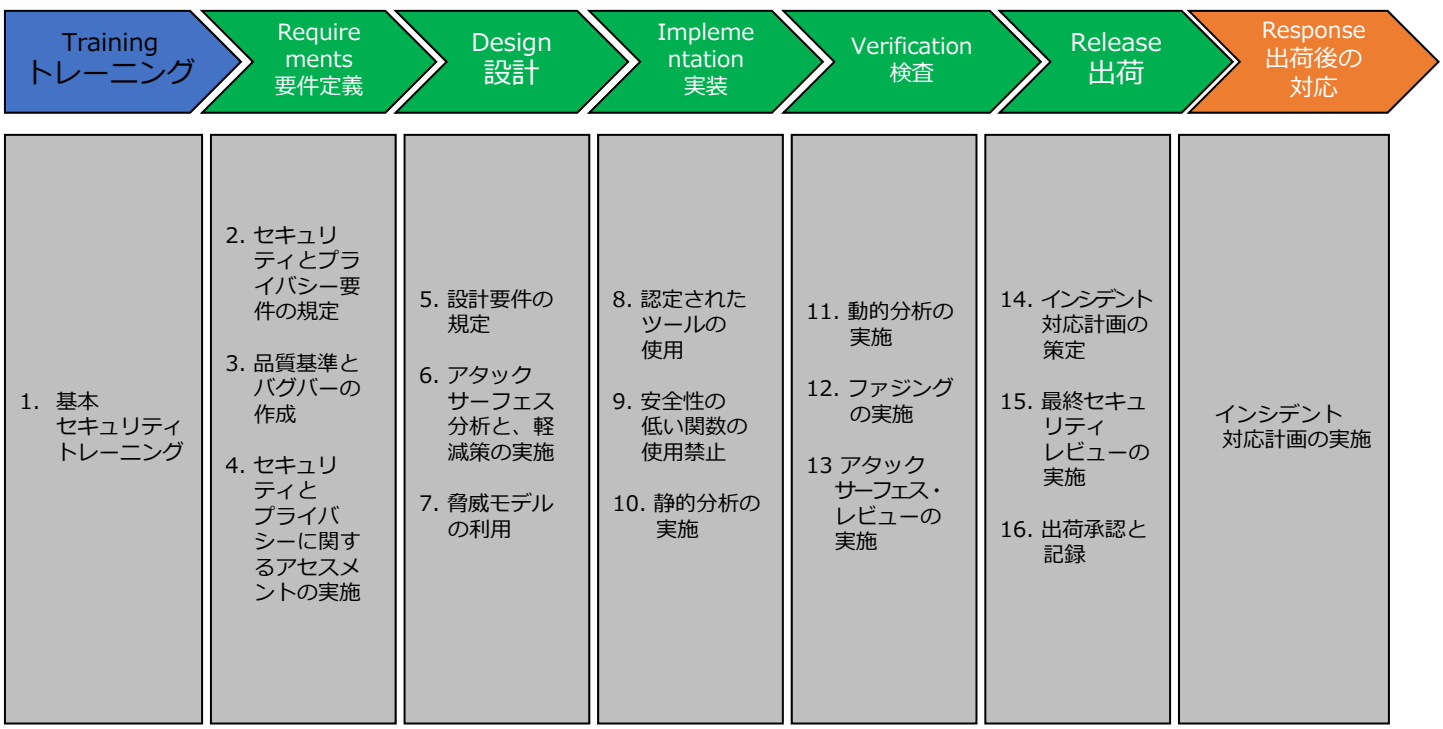
これはまさに、LNK脆弱性の潜在的な影響範囲を拡大するものだ。文書利用の容易さを考えると、我々はまもなく、電子メールメッセージを介した標的型攻撃添付ファイルをほぼ確実に見ることになるだろう。

幸いなことに、MicrosoftのActive Protections Program(MAPP)は優れた技術的詳細を提供しており、我々はWormLinkエクスプロイトに対するプロテクションをさらに改善した。我々の最新のシグネチャ:Exploit:W32/WormLink.BおよびCはより包括的であり、以前よりも効果的だ。Microsoftに賞賛を送りたい。

https://technet.microsoft.com/en-us/security/dn568129.aspx　http://blog.f-secure.jp/archives/50427829.html

SDL詳細

SDLの具体的なフェーズと項目



SDL Process: http://www.microsoft.com/security/sdl/process/training.aspx

SDL Practice #1: (トレーニング)
基本セキュリティトレーニング

- 概要
  - SDLを実装するためには基本セキュリティトレーニングが不可欠で、セキュアな設計、脅威モデル、セキュア・コーディング、セキュリティテスト、プライバシーに関するベストプラクティスなどで構成される、より良いソフトウェアを開発するための基礎となります。
- 実施時期
  - ソフトウェア開発チーム（開発者、検査担当者、プログラムマネージャー）は、一年に一度は何らかのトレーニングクラスに参加する必要があります。
  - 各開発フェーズに対して推奨されるトレーニングは以下のリストを参照してください。

- SDLの導入トレーニング
  - マイクロソフト SDLの紹介
    - Introduction to Microsoft SDL
  - マイクロソフトSDLを実施するために必要なトレーニング
    - Essential Software Security Training for the Microsoft SDL

- 要求定義フェーズ
  - ソフトウェア開発におけるプライバシー
    - Privacy in Software Development
- 設計フェーズ
  - セキュア設な設計、開発、テストの基本
    - Basics of Secure Design, Development and Test
  - マイクロソフト脅威モデルの紹介
    - Introduction to Microsoft SDL Threat Modeling
  - SDLクイックセキュリティリファレンス
    - SDL Quick Security References
  - 開発者向けのSDLスターターキット
    - SDL Developer Starter Kit
- 実装フェーズ
  - セキュア設な設計、開発、テストの基本
    - Basics of Secure Design, Development and Test
  - SDLクイックセキュリティリファレンス
    - SDL Quick Security References
  - 開発者向けのSDLスターターキット
    - SDL Developer Starter Kit
- 検査フェーズ
  - セキュア設な設計、開発、テストの基本
    - Basics of Secure Design, Development and Test
  - SDLクイックセキュリティリファレンス
    - SDL Quick Security References
  - 開発者向けのSDLスターターキット
    - SDL Developer Starter Kit

SDL Practice #2: (要件定義)
セキュリティとプライバシー要件の規定

- 概要
  - 最初にセキュリティとプライバシーの許容最低レベルを定義することは、チームメンバーに対して、セキュリティに係るリスクの理解、開発段階での識別と修正、常に標準を遵守する上での助けとなります。
  - 合理的なバグバーの設定は、脆弱性に対する明示的な深刻度レベル（緊急、重要等）が必要です。ここで設定した基準は、後工程で下げない事が重要です。
- 実施時期
  - 伝統的なソフトウェア開発
    - 要求定義フェーズ
  - アジャイル開発
    - 一度（One Time）

- Reference
  - SDLプライバシー・バグバー　サンプル
    - SDL Privacy Bug Bar Sample
  - SDLセキュリティ：バグバー　サンプル
    - SDL Security Bug Bar Sample
- Downloads
  - Microsoft SDL の簡単な実装
    - Simplified Implementation of the Microsoft SDL
- Tools
  - Microsoft Team Foundation Server 2010 へのセキュリティバグバーの追加
    - Add a Security Bug Bar to Microsoft Team Foundation Server 2010
  - テンプレート：SDL除外申請
    - Template: SDL Exception Request
- Training
  - ソフトウェア開発におけるプライバシー
    - Privacy in Software Development

SDL Practice #3: (要件定義)
品質基準とバグバーの作成

- 概要
  - 最初にセキュリティとプライバシーの許容最低レベルを定義することは、チームメンバーに対して、セキュリティに係るリスクの理解、開発段階での識別と修正、常に標準を遵守する上での助けとなります。
  - 合理的なバグバーの設定は、脆弱性に対する明示的な深刻度レベル（緊急、重要等）が必要です。ここで設定した基準は、後工程で下げない事が重要です。
- 実施時期
  - 伝統的なソフトウェア開発
    - 要求定義フェーズ
  - アジャイル開発
    - 一度（One Time）

- Reference
  - SDLプライバシー・バグバー　サンプル
    - SDL Privacy Bug Bar Sample
  - SDLセキュリティ：バグバー　サンプル
    - SDL Security Bug Bar Sample
- Downloads
  - Microsoft SDL の簡単な実装
    - Simplified Implementation of the Microsoft SDL
- Tools
  - Microsoft Team Foundation Server 2010 へのセキュリティバグバーの追加
    - Add a Security Bug Bar to Microsoft Team Foundation Server 2010
  - テンプレート：SDL除外申請
    - Template: SDL Exception Request
- Training
  - ソフトウェア開発におけるプライバシー
    - Privacy in Software Development

SDL Practice #4: (要件定義)
セキュリティとプライバシーに関するアセスメントの実施

- 概要
  - ソフトウェア設計を、コストと規定の順守性に基づいて検討することは、出荷前に脅威分析とセキュリティ設計レビューを必要とするフェーズ、製品やサービスに対するプライバシーに関するインパクト評価を行う上で助けになります。
- 実施時期
  - 伝統的なソフトウェア開発
    - 要求定義フェーズ
  - アジャイル開発
    - 一度（One Time）

- Reference
  - SDLプライバシーアンケート サンプル
    - SDL Privacy Questionnaire Sample
- Downloads
  - Microsoft SDL の簡単な実装
    - Simplified Implementation of the Microsoft SDL
  - SDL最適化モデル　セルフアセスメントガイド
    - SDL Optimization Model Self-Assessment Guide
- Tools
  - セキュリティリスク評価
    - Security Risk Assessment
- Training
  - ソフトウェア開発におけるプライバシー
    - Privacy in Software Development

SDL Practice #5: (設計)
設計要件の規定

- 概要
  - 早期にセキュリティとプライバシーに関わる懸念事項に取り組むことは、スケジュールの混乱を最小限にし、プロジェクトのコストを減少させます。
  - 設計が機能要件に対して、正確で完全であることを検証し、暗号強度や各定義がレビューされていることも検証します。
- 実施時期
  - 伝統的なソフトウェア開発
    - 設計フェーズ
  - アジャイル開発
    - 一度（One Time）

- Reference
  - ファイアウォールルールと要件
    - Firewall Rules and Requirements
  - 暗号に関する柔軟性（Agility）
    - Cryptographic Agility
  - アプリケーションのセキュリティ保証の文書化と評価
    - Documenting And Evaluating The Security Guarantees Of Your Apps
- Downloads
  - セキュアな設計、開発、検査の基本
    - Basics of Secure Design, Development and Test
  - ソフトウェア開発におけるプライバシー
    - Privacy in Software Development
  - ソフトウェア製品とサービスのための プライバシーガイドライン
    - Privacy Guidelines for Developing Software Products and Services
- Tools
- Training
  - セキュアな設計、開発、検査の基本
    - Basics of Secure Design, Development and Test
  - マイクロソフト脅威分析の紹介
    - Introduction to Microsoft SDL Threat Modeling
  - SDL　セキュリティに関するクイックリファレンス
    - SDL Quick Security References
  - SDL　開発者向けスターターキット
    - SDL Developer Starter Kit

SDL Practice #6: (設計)
アタックサーフェス分析と、軽減策の実施

- 概要
  - 攻撃者が、潜在的な弱点や脆弱性を攻撃する機会を低下させるために、アタックサーフェス全般に対する完全な分析と、システムサービスへのアクセスを無効または限定すること、最小権限の原則を適用すること、多層防御を適用することが必要です。
- 実施時期
  - 伝統的なソフトウェア開発
    - 設計フェーズ
  - アジャイル開発
    - 一度（One Time）

- Reference
  - アタックサーフェスを減らすことにより将来の攻撃を避ける
    - Fending Off Future Attacks by Reducing Attack Surface
  - 信頼できない利用者が利用可能なコードを最小限にすることで、セキュリティリスクを軽減する
    - Mitigate Security Risks by Minimizing the Code You Expose to Untrusted Users
- Downloads
  - SDL開発者向けスターターキット セキュア設計基準
    - SDL Developer Starter Kit - Secure Design Principles
  - アタックサーフェスを減らすことにより将来の攻撃を避ける
    - Fending Off Future Attacks by Reducing Attack Surface
  - 信頼できない利用者が利用可能なコードを最小限にすることで、セキュリティリスクを軽減する
    - Mitigate Security Risks by Minimizing the Code You Expose to Untrusted Users
- Tools
- Training
  - セキュアな設計、開発、検査の基本
    - Basics of Secure Design, Development and Test
  - マイクロソフト脅威分析の紹介
    - Introduction to Microsoft SDL Threat Modeling
  - SDL　セキュリティに関するクイックリファレンス
    - SDL Quick Security References
  - SDL　開発者向けスターターキット
    - SDL Developer Starter Kit

SDL Practice #7: (設計)
脅威モデルの利用

- 概要
  - 設計時に脅威シナリオに対する構造的なアプローチを適用することは、チームがより効果的かつ容易に脆弱性を識別し、脅威によるリスクを判断し、適切な対策の実施を助けます。
- 実施時期
  - 伝統的なソフトウェア開発
    - 設計フェーズ
  - アジャイル開発
    - 全てのスプリント（ Every Sprint ）

- Reference
  - STRIDアプローチによるセキュリティ設計上の問題点の発見
    - Uncover Security Design Flaws Using the STRIDE Approach
- Downloads
  - SDL脅威モデルの紹介
    - Introduction to SDL Threat Modeling
  - SDL開発者向けスターターキット 脅威モデル規定と、脅威モデルツール規定
    - SDL Developer Starter Kit – Threat Modeling Principles, and Threat Modeling Tool Principles
- Tools
- Video
  - SDL　脅威モデル
    - SDL Threat Modeling
  - 脅威モデルツール　2014
    - Threat Modeling Tool 2014
- Training
  - セキュアな設計、開発、検査の基本
    - Basics of Secure Design, Development and Test
  - マイクロソフト脅威分析の紹介
    - Introduction to Microsoft SDL Threat Modeling
  - SDL　セキュリティに関するクイックリファレンス
    - SDL Quick Security References
  - SDL　開発者向けスターターキット
    - SDL Developer Starter Kit

SDL Practice #8: (実装)
認定されたツールの使用

- 概要
  - 許可されたツールと関連するセキュリティチェックを公開することは、セキュリティ規定（コンパイラ・リンカのオプションと警告など）を自動的かつ強制的に適用することを安価で容易にする。
  - リストを定期的に更新することは、最新のバージョンのツールを使用を意味し、新たなセキュリティ分析と防御を組み込むことを意味します。
- 実施時期
  - 伝統的なソフトウェア開発
    - 実装フェーズ
  - アジャイル開発
    - Bucket/Planning

- Reference
  - 推奨するコンパイラ・ツールとオプション
    - Recommended Compilers, Tools, and Options for All Platforms
    - Appendix E: Required and Recommended Compilers, Tools, and Options for All Platforms
    - http://msdn.microsoft.com/library/cc307395.aspx
- Downloads
  - SDL Tools
    - banned.h
    - Code Analysis for C/C++
    - SiteLock ATL Template
    - Anti-Cross Site Scripting (Anti-XSS) Library
    - FxCop
    - Microsoft Code Analysis Tool .NET (CAT.NET)
- Videos
- Tools
- Training

SDL Practice #9: (実装)
安全性の低い関数の使用禁止

- 概要
  - プロジェクトすべての関数とAPIを分析し、安全ではないと定義されたものの利用を禁止することは、わずかな費用で潜在的なセキュリティ上の問題を軽減する。
  - ヘッダーファイルの利用、新しいコンパイラや検査ツールを利用し、使用禁止リストに記載された関数を安全なものに変換する。
- 実施時期
  - 伝統的なソフトウェア開発
    - 実装フェーズ
  - アジャイル開発
    - 全てのスプリント（ Every Sprint ）

- Reference
  - Strsafe.h について
    - About Strsafe.h (with Visual Studio)
  - 安全なCRT
    - Safe CRT (with Visual Studio)
  - SDL禁止ファンクションコール
    - SDL Banned Function Calls
  - SDL開発者向けスターターキット 禁止API
    - SDL Developer Starter Kit – Banned APIs
- Downloads
  - Banned.h
  - セキュアな設計、開発、検査の基本
    - Basics of Secure Design, Development and Test
- Videos
  - Banned.h
- Tools
- Training
  - セキュアな設計、開発、検査の基本
    - Basics of Secure Design, Development and Test
  - SDL　セキュリティに関するクイックリファレンス
    - SDL Quick Security References
  - SDL　開発者向けスターターキット
    - SDL Developer Starter Kit

SDL Practice #10: (実装)
静的分析の実施

- 概要
  - コンパイル前にソースコードを分析することは、スケーラブルなセキュリティコードレビューを可能とし、セキュアコーディング規定に準じていることを確実にします。
- 実施時期
  - 伝統的なソフトウェア開発
    - 実装フェーズ
  - アジャイル開発
    - 全てのスプリント（ Every Sprint ）

- Reference
- Downloads
  - CAT.NET 32-bit/64-bit　Anti-XSS
  - FxCop　Code Analysis for C/C++
  - SDL Developer Starter Kit – Code Analysis
- Videos
  - CAT.NET 32-bit/64-bit　Anti-XSS
  - FxCop　Code Analysis for C/C++
- Webcast
  - CAT.NET 静的なコード分析を使用したソフトウェアセキュリティ
    - Software Security with Static Code Analysis Using CAT.NET (Level 200)
  - コード分析ツールを使用したセキュリティ問題の発見と対処
    - Detecting and Mitigating Security Issues Using the Code Analysis Tool .NET (Level 200)
- Tools
- Training
  - セキュアな設計、開発、検査の基本
    - Basics of Secure Design, Development and Test
  - SDL　セキュリティに関するクイックリファレンス
    - SDL Quick Security References
  - SDL　開発者向けスターターキット
    - SDL Developer Starter Kit

SDL Practice #11: (検査)
動的分析の実施

- 概要
  - ソフトウェアの実行時に検査によりアプリケーションの挙動をモニターし、メモリー破壊、ユーザー権限の問題など、重要なセキュリティ上の問題をチェックする
- 実施時期
  - 伝統的なソフトウェア開発
    - 検査フェーズ
  - アジャイル開発
    - Bucket検査（ Bucket Verification ）

- Reference
  - SDL開発者向けスターターキット バッファオーバーフロー、SQLインジェクション
    - SDL Developer Starter Kit – Buffer Overflows, SQL Injection
- Downloads
  - AppVerifier Download
  - BinScope Binary Analyzer Download
  - セキュアな設計、開発、検査の基本
    - Basics of Secure Design, Development and Test
  - セキュリティ検査基準
    - Secure Verification Principles
  - Cross-Site Scripting
- Videos
  - BinScope Binary Analyzer
- Tools
- Training
  - セキュアな設計、開発、検査の基本
    - Basics of Secure Design, Development and Test
  - SDL　セキュリティに関するクイックリファレンス
    - SDL Quick Security References
  - SDL　開発者向けスターターキット
    - SDL Developer Starter Kit

SDL Practice #12: (検査)
ファジングの実施

- 概要
  - 意図的に不正な形式やランダムなデータを扱うことで、プログラムエラーを引き起こすことは、ささやかなリソースの投資だけで、潜在的なセキュリティ上の問題を出荷前に明らかにすることを助ける。
- 実施時期
  - 伝統的なソフトウェア開発
    - 検査フェーズ
  - アジャイル開発
    - Bucket検査（ Bucket Verification ）

- Reference
  - ファジングテスト：Visual Studio Team System 向けのテストインタフェースプロバイダーの作成
    - Fuzz Testing: Create a Test Interface Provider for Visual Studio Team System
  - 正規表現DoSアタックと防御
    - Regular Expression Denial of Service Attacks and Defenses
  - ホワイトボックス・ファジングによる自動化されたペネトレーションテスト
    - Automated Penetration Testing with White-Box Fuzzing
- Downloads
  - セキュアな設計、開発、検査の基本
    - Basics of Secure Design, Development and Test
  - SDL　開発者向けスターターキット
    - SDL Developer Starter Kit
  - MiniFuzz File Fuzzer SDL Regex Fuzzer
- Videos
  - 楽しくて役に立つファジング
    - File Fuzzing for Fun and Profit (Level 300)
  - MiniFuzz File Fuzzer SDL Regex Fuzzer
- Tools
- Training
  - セキュアな設計、開発、検査の基本
    - Basics of Secure Design, Development and Test
  - SDL　セキュリティに関するクイックリファレンス
    - SDL Quick Security References
  - SDL　開発者向けスターターキット
    - SDL Developer Starter Kit

SDL Practice #13: (Verification)
アタックサーフェス・レビューの実施

- 概要
  - コード完成と同時に、アタックサーフェス・レビューを行うことは、アプリケーションやシステムに対する設計や実装の変更が注意深く行われていることを確認し、修正の結果として新たなアタックベクターが作られた場合には、レビューを実施し、脅威モデルに反映する。
- 実施時期
  - 伝統的なソフトウェア開発
    - 検査フェーズ
  - アジャイル開発
    - Bucket検査（ Bucket Verification ）

- Reference
- Downloads
- Videos
- Tools
  - アタック・サーフェス・アナライザ
    - Attack Surface Analyzer
- Training

SDL Practice #14: (Release)
インシデント対応計画の策定

- 概要
  - インシデント対応計画の策定は、時間と共にあらわれる新たな脅威の対処を行う上で重要なものです。
  - 適切なセキュリティ上の緊急事態の連絡先、他の部門やサードパーティから引き継いだコードに対するセキュリティサービス計画も含みます。
- 実施時期
  - 伝統的なソフトウェア開発
    - リリースフェーズ
  - アジャイル開発
    - 一度（One Time）

- Reference
- Downloads
  - Microsoft SDL の簡単な実装
    - Simplified Implementation of the Microsoft SDL
  - SDLプライバシーアンケートのインシデント対応セクション
    - Incident Response section of SDL Privacy Questionnaire
  - SDLプライバシーエスカレーション対応フレームワークサンプル
    - SDL Privacy Escalation Response Framework Sample
- Videos
- Tools
- Training

SDL Practice #15: (Release)
. 最終セキュリティレビューの実施

- 概要
  - 実施されたすべてのセキュリティ活動を慎重にレビューすることは、ソフトウェアのリリースを確実にすることを助けます。
  - 通常、最終セキュリティレビューは、脅威モデル、ツールの出力、要求定義フェーズで策定した品質基準とバグバーに対する結果を含みます。
  - 最終セキュリティレビューに結果は、合格、除外項目を含んだ合格、エスカレーションの何れかとなります。
- 実施時期
  - 伝統的なソフトウェア開発
    - リリースフェーズ
  - アジャイル開発
    - Every Sprint

- Reference
  - SDL セキュリティ・バグバー　サンプル
    - SDL Security Bug Bar Sample
- Downloads
  - SDLプロセステンプレート
    - SDL Process Template
  - Agile+SDLプロセステンプレート
    - MSF-Agile+SDL Process Template
  - Microsoft SDL の簡単な実装
    - Simplified Implementation of the Microsoft SDL
- Videos
  - SDLプロセステンプレート
    - SDL Process Template
  - Agile + SDLプロセス
    - MSF- Agile + SDL Process
- Tools
- Training

SDL Practice #16: (Release)
出荷承認と記録

- 概要
  - 全ての関係するデータをアーカイブすることは、リリース後の活動を実施し、長期間にわたるソフトウエアの維持コストを削減するために重要です。
  - 全ての仕様書、ソースコード、バイナリ、プライベートシンボル、脅威モデル、ドキュメント、緊急対応プラン、サードパーティ製ソフトウェアのライセンスとサービスの条件をアーカイブする必要があります。
- 実施時期
  - 伝統的なソフトウェア開発
    - リリースフェーズ
  - アジャイル開発:
    - Every Sprint

- Reference
- Downloads
  - Microsoft SDL の簡単な実装
    - Simplified Implementation of the Microsoft SDL
  - SDL プロセステンプレート
    - SDL Process Template
  - Agile+SDL プロセステンプレート
    - MSF-Agile+SDL Process Template
- Videos
  - SDLプロセステンプレート
    - SDL Process Template
  - Agile + SDLプロセス
    - MSF- Agile + SDL Process
- Tools
- Training

SDL関連　リファレンス

リファレンス 1/3

About Strsafe.h (with Visual Studio)	http://msdn.microsoft.com/library/ms647466(VS.85).aspx
Add a Security Bug Bar to Microsoft Team Foundation Server 2010	http://msdn.microsoft.com/en-us/magazine/ee336031.aspx
Anti-XSS	http://go.microsoft.com/?linkid=9757780
Anti-XSS　(VIDEO)	http://www.microsoft.com/security/sdl/process/implementation.aspx#
AppVerifier Download	http://www.microsoft.com/downloads/en/details.aspx?FamilyID=c4a25ab9-649d-4a1b-b4a7-c9d8b095df18
AppVerifier Download	http://www.microsoft.com/downloads/en/details.aspx?FamilyID=c4a25ab9-649d-4a1b-b4a7-c9d8b095df18
Attack Surface Analyzer	http://go.microsoft.com/?linkid=9758398
Automated Penetration Testing with White-Box Fuzzing	http://msdn.microsoft.com/library/cc162782.aspx
Banned.h	http://www.microsoft.com/downloads/en/details.aspx?FamilyID=6aed14bd-4766-4d9d-9ee2-fa86aad1e3c9&displaylang=en
Banned.h (VIDEO)	http://www.microsoft.com/security/sdl/process/implementation.aspx#
Basics of Secure Design, Development and Test	http://download.microsoft.com/download/9/3/5/935520EC-D9E2-413E-BEA7-0B865A79B18C/Basics%20of%20Secure%20Design%20Development%20Test.ppsx
Basics of Secure Design, Development and Test	http://download.microsoft.com/download/9/3/5/935520EC-D9E2-413E-BEA7-0B865A79B18C/Basics%20of%20Secure%20Design%20Development%20Test.ppsx
Basics of Secure Design, Development and Test	http://download.microsoft.com/download/9/3/5/935520EC-D9E2-413E-BEA7-0B865A79B18C/Basics%20of%20Secure%20Design%20Development%20Test.ppsx
BinScope Binary Analyzer (VIDEO)	http://www.microsoft.com/security/sdl/process/verification.aspx#
BinScope Binary Analyzer Download	http://www.microsoft.com/download/en/details.aspx?id=11910
BinScope Binary Analyzer Download	http://www.microsoft.com/download/en/details.aspx?id=11910
CAT.NET 32-bit	http://www.microsoft.com/downloads/en/details.aspx?FamilyId=0178e2ef-9da8-445e-9348-c93f24cc9f9d&displaylang=en
CAT.NET 32-bit　(VIDEO)	http://www.microsoft.com/security/sdl/process/implementation.aspx#
CAT.NET 64-bit	http://www.microsoft.com/downloads/en/details.aspx?FamilyId=e0052bba-2d50-4214-b65b-37e5ef44f146&displaylang=en
CAT.NET 64-bit　(VIDEO)	http://www.microsoft.com/security/sdl/process/implementation.aspx#
Code Analysis for C/C++	http://msdn.microsoft.com/en-us/library/ms182025.aspx
Code Analysis for C/C++　(VIDEO)	http://www.microsoft.com/security/sdl/process/implementation.aspx#
Cross-Site Scripting	http://download.microsoft.com/download/F/B/D/FBDE7C61-3B58-4940-8653-FB375C1758DC/Cross-Site%20Scripting%20-%20Microsoft%20SDL%20-%20Developer%20Starter%20Kit.zip
Cross-Site Scripting	http://download.microsoft.com/download/F/B/D/FBDE7C61-3B58-4940-8653-FB375C1758DC/Cross-Site%20Scripting%20-%20Microsoft%20SDL%20-%20Developer%20Starter%20Kit.zip
Cryptographic Agility	http://msdn.microsoft.com/en-us/magazine/ee321570.aspx

リファレンス 2/3

Detecting and Mitigating Security Issues Using the Code Analysis Tool .NET (Level 200)	http://events.microsoft.com/Pages/Home.aspx?k=Detecting%20and%20Mitigating%20Security%20Issues%20Using%20the%20Code%20Analysis%20Tool%20.NET%20(Level%20200)&cs=This%20Site&u=https%3A%2F%2Fevents.microsoft.com#m=%3Br%3D0%3Bs%3D%3Byourrole%3D2%3Beventtype%3D2%3Blevel%3D2%3Btimelength%3D2%3Bv%3Dlist%3Bpi%3D%3Bmi%3D%3Bsi%3D%3Bai%3D
Documenting And Evaluating The Security Guarantees Of Your Apps	http://msdn.microsoft.com/en-us/magazine/cc163522.aspx
Essential Software Security Training for the Microsoft SDL	http://go.microsoft.com/?linkid=9786235
Firewall Rules and Requirements	http://msdn.microsoft.com/en-us/library/cc307394.aspx
Fuzz Testing: Create a Test Interface Provider for Visual Studio Team System	http://msdn.microsoft.com/magazine/cc163313.aspx
FxCop	http://www.microsoft.com/downloads/en/details.aspx?FamilyID=917023f6-d5b7-41bb-bbc0-411a7d66cf3c&displaylang=en
FxCop (VIDEO)	http://www.microsoft.com/security/sdl/process/implementation.aspx#
Incident Response section of SDL Privacy Questionnaire	http://msdn.microsoft.com/library/cc307393.aspx
Introduction to Microsoft SDL	http://download.microsoft.com/download/9/3/5/935520EC-D9E2-413E-BEA7-0B865A79B18C/Introduction%20to%20the%20Microsoft%20Security%20Development%20Lifecycle%20(SDL).ppsx
Introduction to Microsoft SDL Threat Modeling	http://download.microsoft.com/download/9/3/5/935520EC-D9E2-413E-BEA7-0B865A79B18C/Introduction_to_Threat_Modeling.ppsx
Introduction to Microsoft SDL Threat Modeling	http://download.microsoft.com/download/9/3/5/935520EC-D9E2-413E-BEA7-0B865A79B18C/Introduction_to_Threat_Modeling.ppsx
MiniFuzz File Fuzzer	http://www.microsoft.com/downloads/en/details.aspx?displaylang=en&FamilyID=b2307ca4-638f-4641-9946-dc0a5abe8513
MSF-Agile+SDL Process Template	http://www.microsoft.com/security/sdl/adopt/agile.aspx
Privacy Guidelines for Developing Software Products and Services	http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=16048
Privacy in Software Development	http://download.microsoft.com/download/9/3/5/935520EC-D9E2-413E-BEA7-0B865A79B18C/Privacy%20in%20Software%20Development.ppsx
Privacy in Software Development	http://download.microsoft.com/download/9/3/5/935520EC-D9E2-413E-BEA7-0B865A79B18C/Privacy%20in%20Software%20Development.ppsx
Recommended Compilers, Tools, and Options for All Platforms	http://msdn.microsoft.com/library/cc307395.aspx
Regular Expression Denial of Service Attacks and Defenses	http://msdn.microsoft.com/magazine/ff646973.aspx
Safe CRT (with Visual Studio)	http://msdn.microsoft.com/library/8ef0s5kh(VS.80).aspx
SDL Banned Function Calls	http://msdn.microsoft.com/library/bb288454.aspx
SDL Developer Starter Kit	http://www.microsoft.com/security/sdl/adopt/starterkit.aspx
SDL Developer Starter Kit	http://www.microsoft.com/security/sdl/adopt/starterkit.aspx
SDL Developer Starter Kit – Banned APIs	http://www.microsoft.com/security/sdl/adopt/starterkit.aspx
SDL Developer Starter Kit – Buffer Overflows, SQL Injection	http://www.microsoft.com/security/sdl/adopt/starterkit.aspx
SDL Developer Starter Kit – Buffer Overflows, SQL Injection	http://www.microsoft.com/security/sdl/adopt/starterkit.aspx

リファレンス 3/3

SDL Developer Starter Kit – Code Analysis	http://www.microsoft.com/security/sdl/adopt/starterkit.aspx
SDL Optimization Model Self-Assessment Guide	http://download.microsoft.com/download/2/c/4/2c414971-f61c-4679-8144-53a16adc844e/SDL%20Optimization%20Model%20-%20Self%20Assessment%20Guide.docx
SDL Privacy Bug Bar Sample	http://msdn.microsoft.com/en-us/library/cc307403.aspx
SDL Privacy Escalation Response Framework Sample	http://msdn.microsoft.com/library/cc307401.aspx
SDL Privacy Questionnaire Sample	http://msdn.microsoft.com/en-us/library/cc307393.aspx
SDL Process Template	http://go.microsoft.com/?linkid=9706652
SDL Quick Security References	http://www.microsoft.com/downloads/en/details.aspx?FamilyID=79042476-951f-48d0-8ebb-89f26cf8979d
SDL Regex Fuzzer	http://www.microsoft.com/downloads/en/details.aspx?FamilyID=8737519c-52d3-4291-9034-caa71855451f
SDL Security Bug Bar Sample	http://msdn.microsoft.com/en-us/library/cc307404.aspx
SDL Tools	http://www.microsoft.com/security/sdl/adopt/tools.aspx
Secure Code Review Guidance and Code Priority Definitions	http://download.microsoft.com/download/3/E/2/3E297035-2B7D-44F7-8EF6-08D4E9400EBE/Secure%20Code%20Review%20Guidance%20and%20Priority%20Definitions.docx
Secure Verification Principles	http://download.microsoft.com/download/F/B/D/FBDE7C61-3B58-4940-8653-FB375C1758DC/Secure%20Verification%20Principles%20-%20Microsoft%20SDL%20-%20Developer%20Starter%20Kit.zip
Secure Verification Principles	http://download.microsoft.com/download/F/B/D/FBDE7C61-3B58-4940-8653-FB375C1758DC/Secure%20Verification%20Principles%20-%20Microsoft%20SDL%20-%20Developer%20Starter%20Kit.zip
Security Definitions for Vulnerability Work Item Tracking	http://msdn.microsoft.com/library/cc307392.aspx
Security Requirements Questionnaire	http://download.microsoft.com/download/3/E/2/3E297035-2B7D-44F7-8EF6-08D4E9400EBE/Security%20Requirements%20Questionnaire.docx
Security Risk Assessment	http://download.microsoft.com/download/3/E/2/3E297035-2B7D-44F7-8EF6-08D4E9400EBE/Security%20Risk%20Assessment.docx
Simplified Implementation of the Microsoft SDL	http://go.microsoft.com/?linkid=9708425
Software Security with Static Code Analysis Using CAT.NET (Level 200)	https://msevents.microsoft.com/CUI/EventDetail.aspx?culture=en-US&EventID=1032402661&CountryCode=US
Template: SDL Exception Request	http://download.microsoft.com/download/3/E/2/3E297035-2B7D-44F7-8EF6-08D4E9400EBE/SDL%20Exception%20Request%20Template.docx

The SDL Developer Starter Kit

Design Phase	Secure Design Principles (.zip) Threat Modeling Principles (.zip) Threat Modeling Tool 2014 Principles (.zip) SQL Injection Vulnerabilities (.zip) Bonus! MSDN Virtual Lab Cross-Site Scripting Vulnerabilities (.zip) Bonus! MSDN Virtual Lab Buffer Overflows (.zip) Bonus! MSDN Virtual Lab
Implementation Phase	Secure Implementation Principles (.zip) Banned APIs (.zip) Code Analysis (.zip) Bonus! MSDN Virtual Lab Source Code Annotation Language (.zip) Bonus! MSDN Virtual Lab Compiler Defenses (.zip) Bonus! MSDN Virtual Lab SQL Injection Vulnerabilities (.zip) Bonus! MSDN Virtual Lab Cross-Site Scripting Vulnerabilities (.zip) Bonus! MSDN Virtual Lab Buffer Overflows (.zip) Bonus! MSDN Virtual Lab
Verification Phase	Secure Verification Principles (.zip) Security Code Review (.zip) Bonus! MSDN Virtual Lab Fuzz Testing (.zip) Bonus! MSDN Virtual Lab SQL Injection Vulnerabilities (.zip) Bonus! MSDN Virtual Lab Cross-Site Scripting Vulnerabilities (.zip) Bonus! MSDN Virtual Lab Buffer Overflows (.zip) Bonus! MSDN Virtual Lab