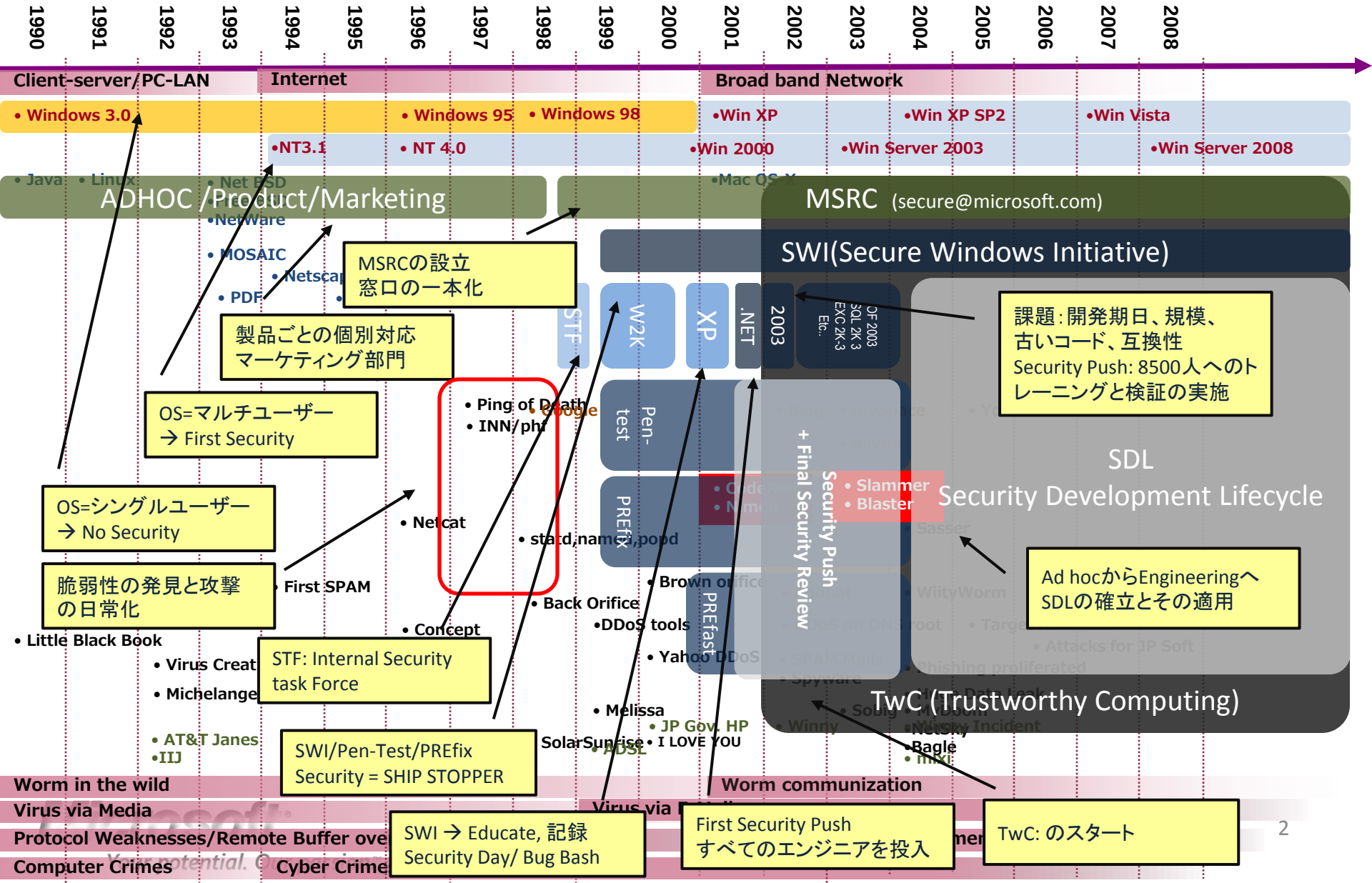
コンピュータセキュリティの歴史と Security Development Lifecycle

高橋　正和
日本マイクロソフト
チーフセキュリティアドバイザー

Microsoft
Your potential. Our passion.™

Windows Products and Security: never end story

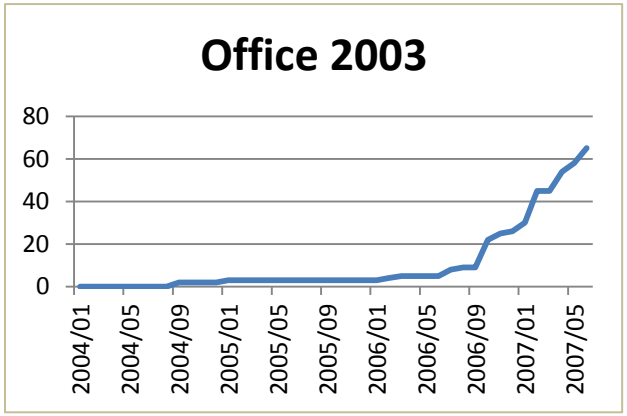


SDLに関して学んだこと

- **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。

最近思うこと #1

- Security ≠　Quality
  - 不具合は、Functionが機能しないこと（ある程度の検証が可能）
  - 脆弱性は、想定していない使い方をされた時の異常な動作の話
    - 意図（悪意）への着目



- 思い込みはないのだろうか？
  - 作り込みなので大丈夫、ネットワークは独立している等
    - 検証はされているのだろうか？
  - Fail Safeの機構と、その是非
    - そもそも汎用システムのFail Safeは成り立つのか？

最近思うこと #2

- 広域化と局所化の同時進行
  - 攻撃技術の広域的な共有
  - 攻撃対象の局所化

- 脆弱性対策以外のセキュリティ対策
  プログラムのホワイトリスト化等
  - Windows 7で導入された、AppLockerによる、動作プログラムのホワイトリスト化は、有効性の高い対策であることが確認されている。
  - 他にも、アプリケーションのサンドボックス化など、脆弱性対策以外のセキュリティ対策は多数存在する

SDL 関係の資料

- MSDNセキュリティデベロッパーセンター
  - http://www.microsoft.com/japan/msdn/security/
- 信頼できるコンピューティングのセキュリティ開発ライフサイクル
  - http://www.microsoft.com/japan/msdn/security/general/sdl.aspx
- Inside the Windows Security Push
  - http://www.princeton.edu/~echi/ele572/Howard%20-%20Windows%20security%20push.pdf
- Security Development Lifecycle (SDL) Banned Function Calls
  - http://msdn2.microsoft.com/en-us/library/bb288454.aspx
- Trustworthy Computing
  - http://www.microsoft.com/mscorp/twc/default.mspx （English）
  - http://www.microsoft.com/japan/mscorp/twc/security/default.mspx（日本語）
- Read the CNET report: MSセキュリティのこの10年：手痛い教訓をバネに
  - http://www.news.com/At-software-giant%2C-pain-gives-rise-to-progress/2009-7349_3-6220566.html?tag=st.nl (English)
  - http://japan.cnet.com/special/story/0,2000056049,20363043,00.htm（日本語）
- TechNet: 脆弱性の防御では、切り札である「プロセス」が「多くの目」に勝ります
  - http://www.microsoft.com/technet/community/columns/secmgmt/sm1007.mspx (English)
  - http://www.microsoft.com/japan/technet/community/columns/secmgmt/sm1007.mspx（日本語）
- “Windows Server 2003 by the Numbers: One of the Biggest Product Launches in Microsoft History
  - http://www.microsoft.com/japan/technet/community/columns/secmgmt/sm1007.mspx
- Windows Vista 1年間の脆弱性レポート
  - http://download.microsoft.com/download/c/d/c/cdcc38a5-50fa-4425-be75-9d165065d0c8/vista-one-year-vuln-report-ja.pdf
- Operating System Vulnerability Scorecard
  - http://blogs.technet.com/security/archive/2007/08/16/july-2007-operating-system-vulnerability-scorecard.aspx
- “Days-of-risk in 2006: Linux, Mac OS X, Solaris, and Windows”, CSO.com
  - http://blogs.csoonline.com/days_of_risk_in_2006
- Compare Security
  - http://www.microsoft.com/windowsserver/compare/linux/security.mspx

Microsoft®

Your potential. Our passion.™

The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.