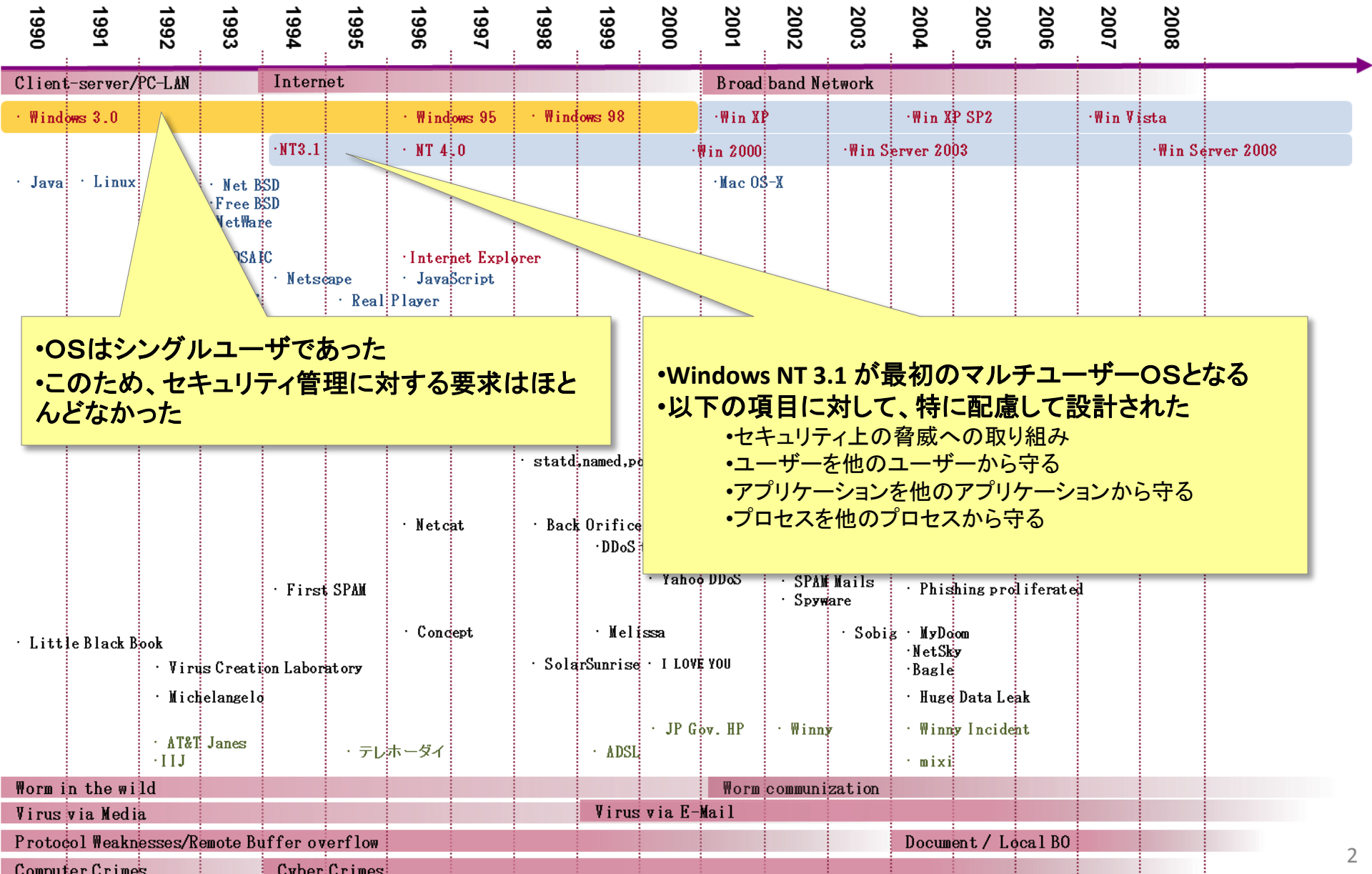
脆弱性への取組み―マイクロソフト社の事例 ～いかにしてSDLにたどり着いたのか～

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

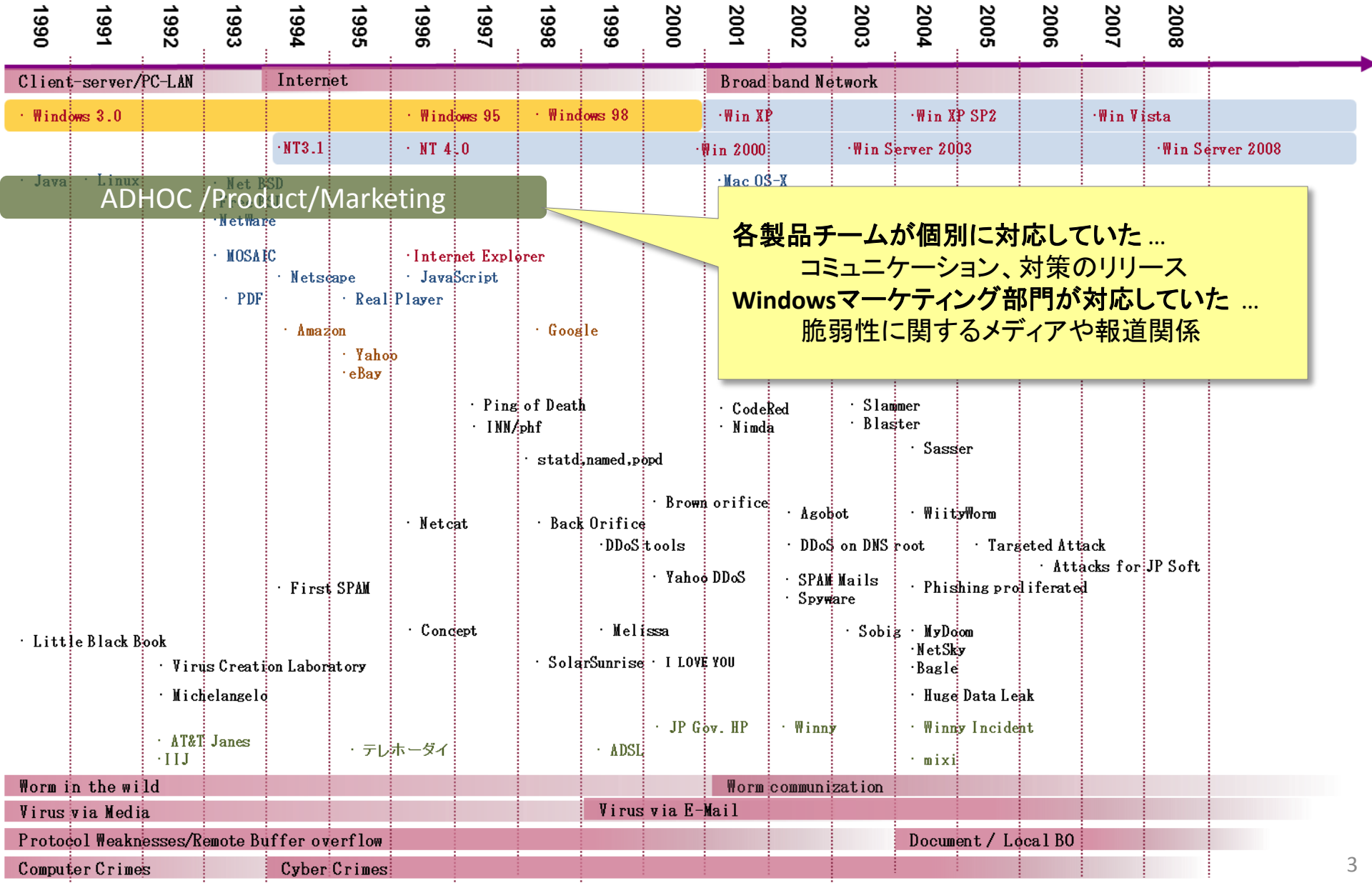
Windows Products and Security



- OSはシングルユーザであった
- このため、セキュリティ管理に対する要求はほとんどなかった

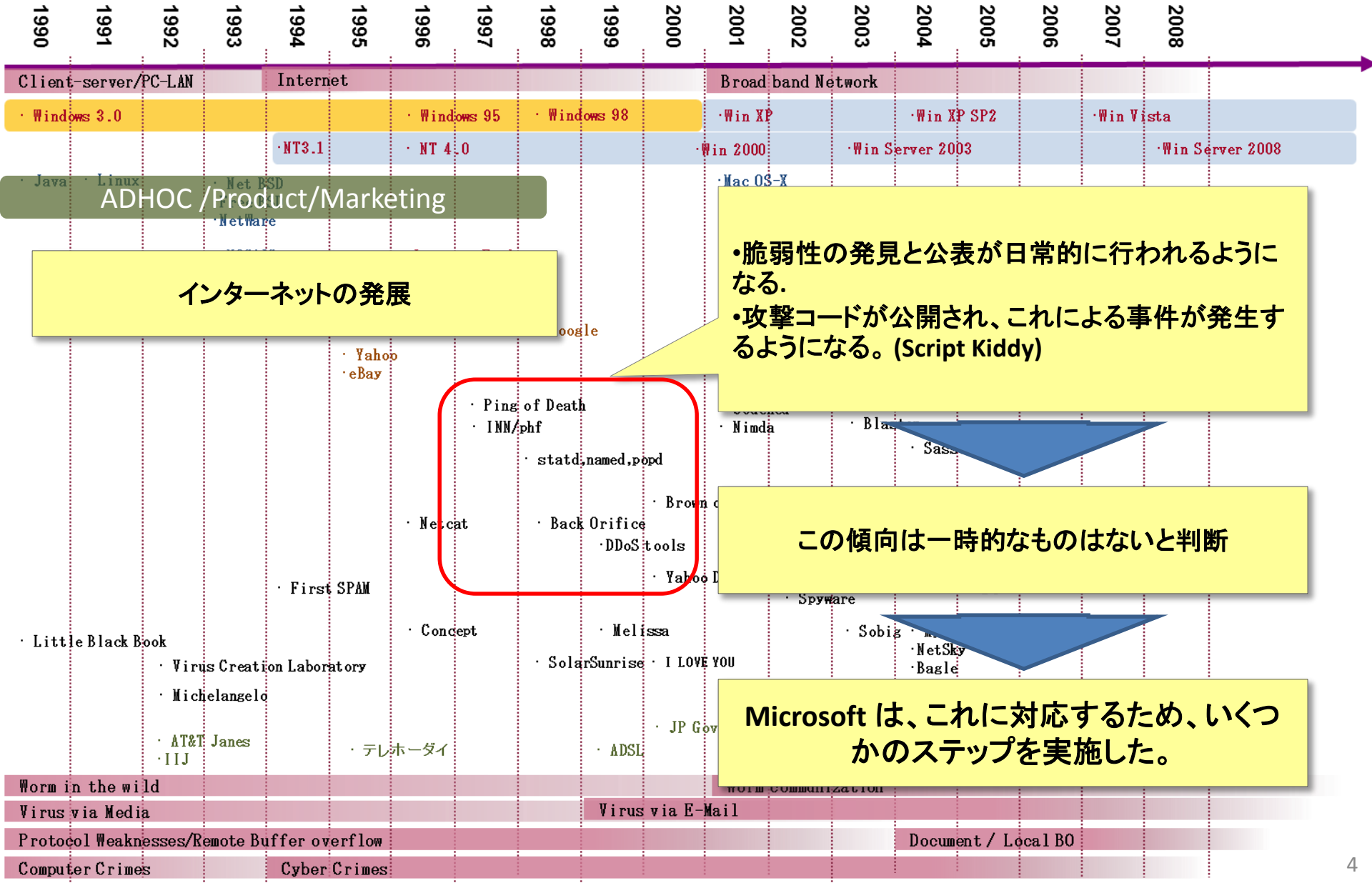
- Windows NT 3.1 が最初のマルチユーザーOSとなる
- 以下の項目に対して、特に配慮して設計された
  - セキュリティ上の脅威への取り組み
  - ユーザーを他のユーザーから守る
  - アプリケーションを他のアプリケーションから守る
  - プロセスを他のプロセスから守る

Windows Products and Security: 1998年以前



各製品チームが個別に対応していた …
コミュニケーション、対策のリリース
Windowsマーケティング部門が対応していた …
脆弱性に関するメディアや報道関係

Windows Products and Security:1990年代中頃



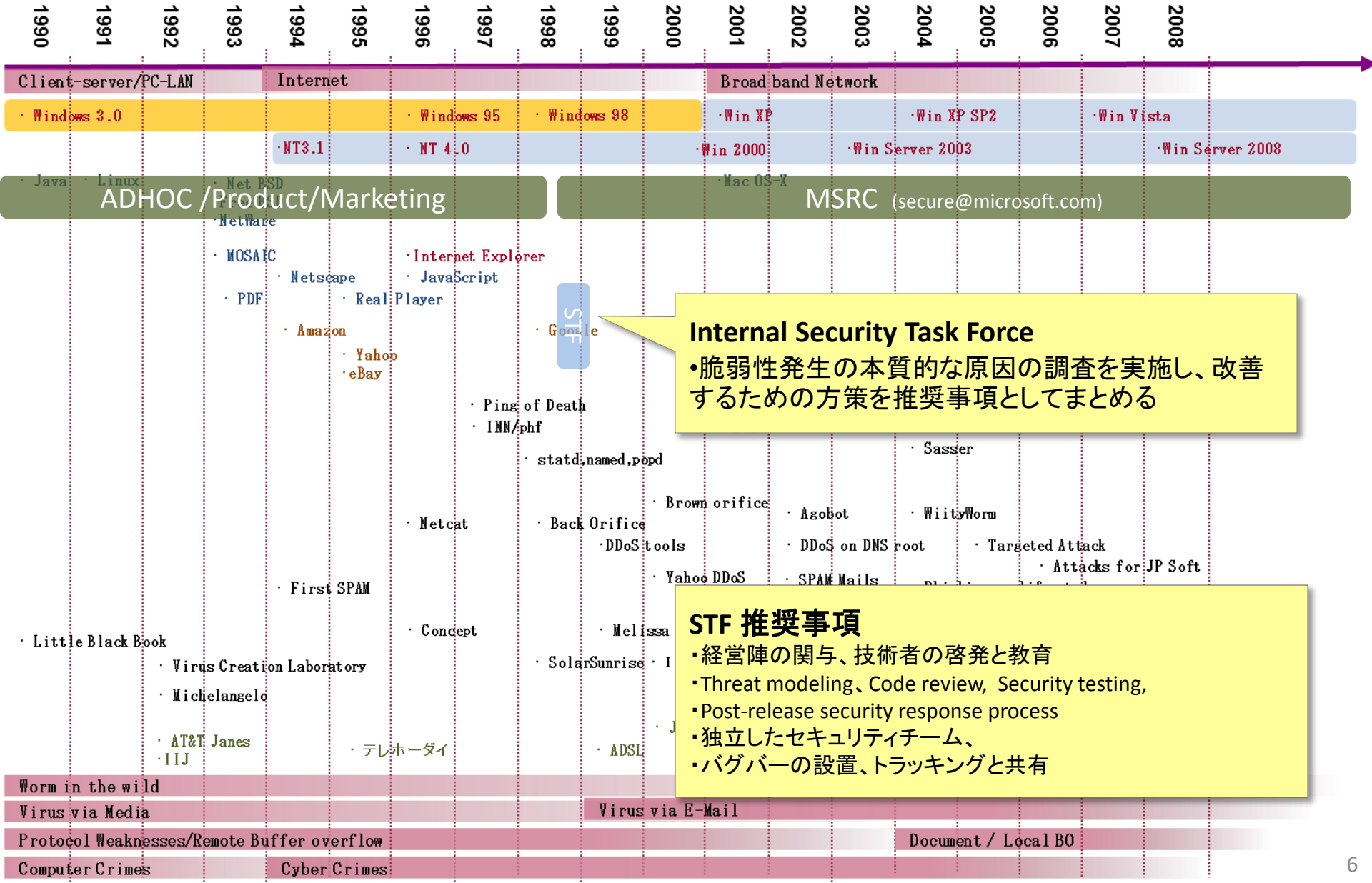
SANS: 最も重要なインターネット上の脅威

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



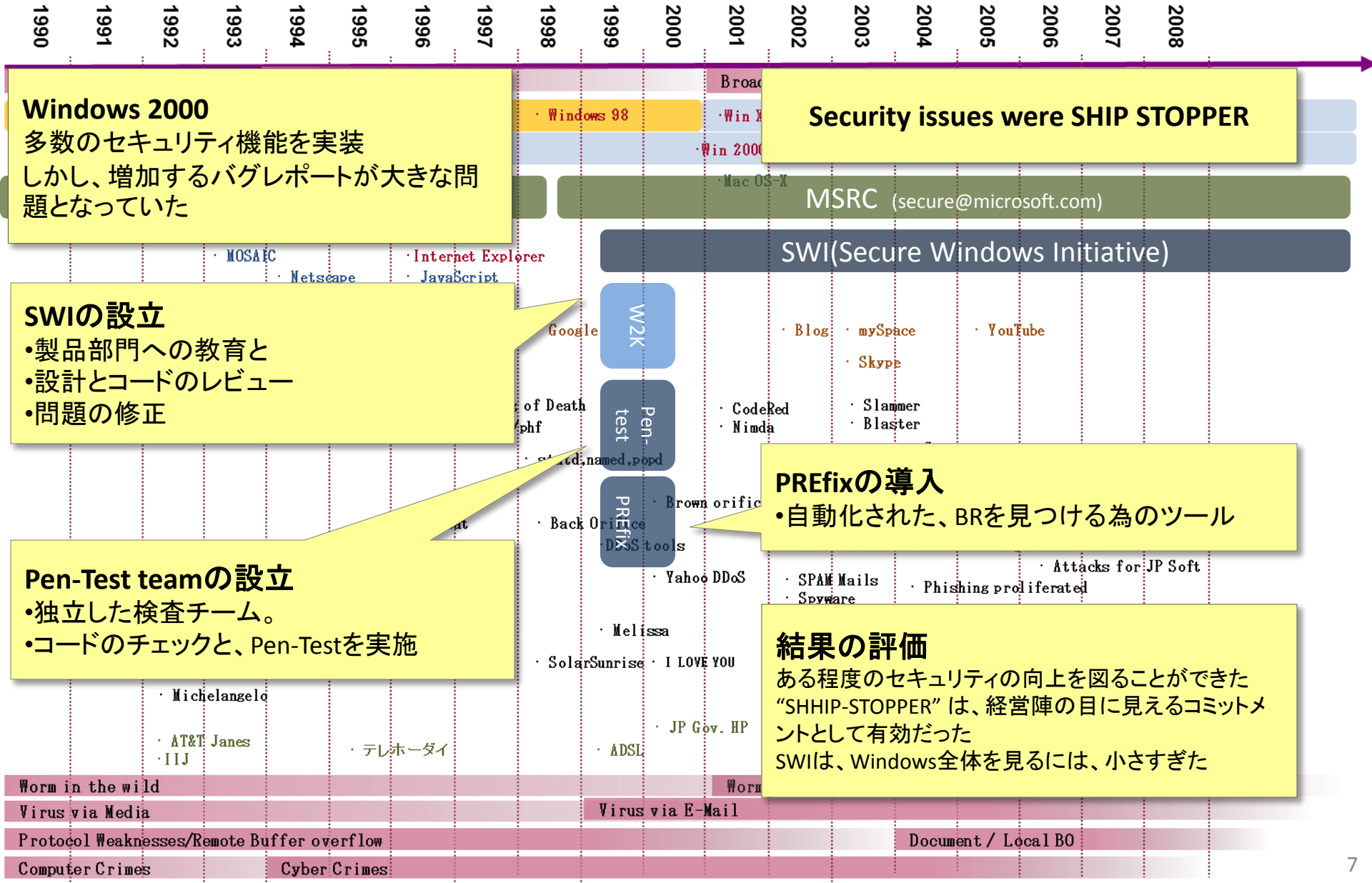
Internal Security Task Force

•脆弱性発生の本質的な原因の調査を実施し、改善するための方策を推奨事項としてまとめる

STF 推奨事項

・経営陣の関与、技術者の啓発と教育
・Threat modeling、Code review, Security testing,
・Post-release security response process
・独立したセキュリティチーム、
・バグバーの設置、トラッキングと共有

Windows Products and Security: Windows 2000



Windows 2000
多数のセキュリティ機能を実装
しかし、増加するバグレポートが大きな問題となっていた

Security issues were SHIP STOPPER

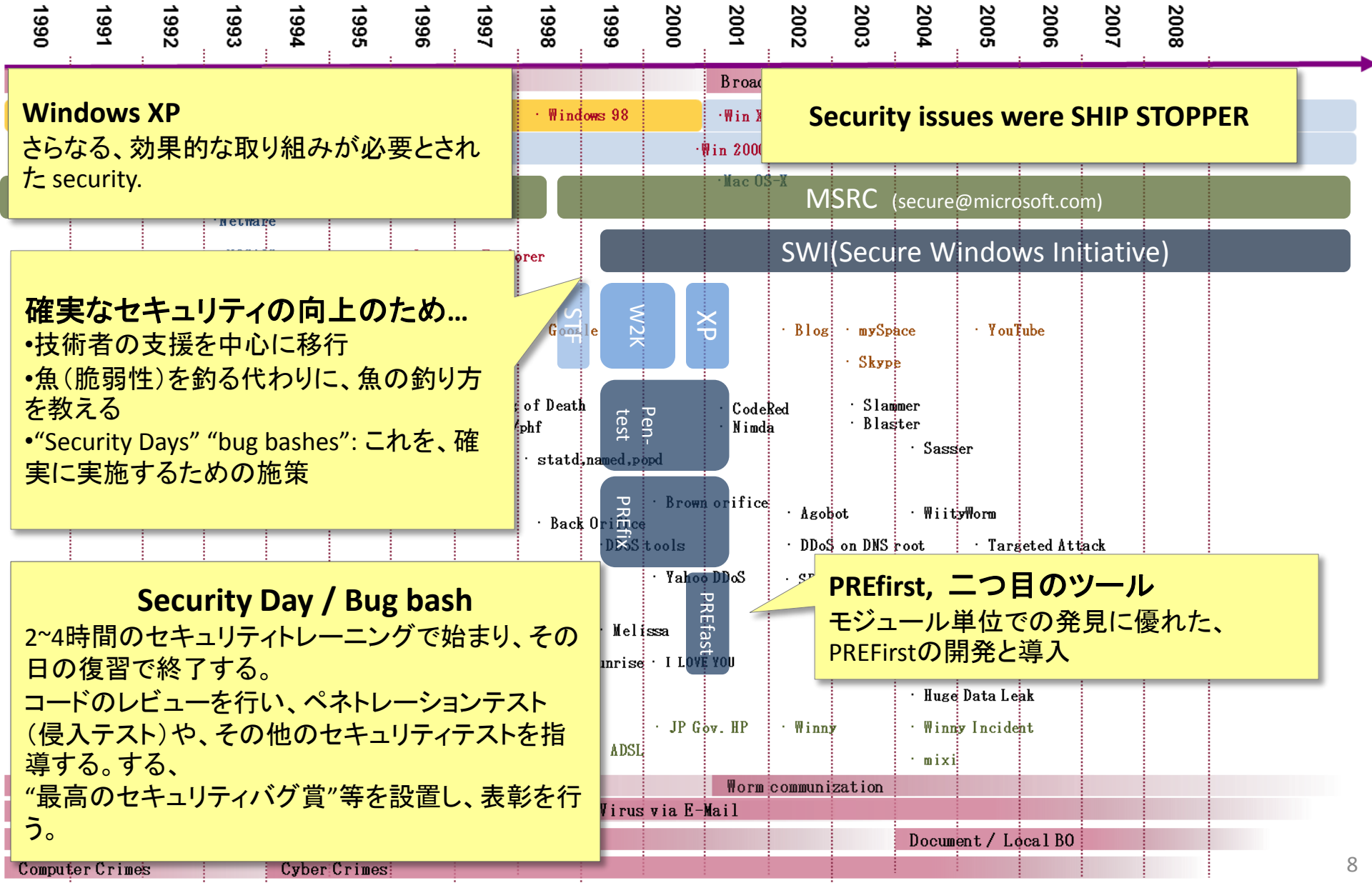
SWIの設立
- 製品部門への教育と
- 設計とコードのレビュー
- 問題の修正

PREfixの導入
- 自動化された、BRを見つける為のツール

Pen-Test teamの設立
- 独立した検査チーム。
- コードのチェックと、Pen-Testを実施

結果の評価
ある程度のセキュリティの向上を図ることができた
“SHHIP-STOPPER” は、経営陣の目に見えるコミットメントとして有効だった
SWIは、Windows全体を見るには、小さすぎた

Windows Products and Security: Windows XP



Windows XP
さらなる、効果的な取り組みが必要とされた security.

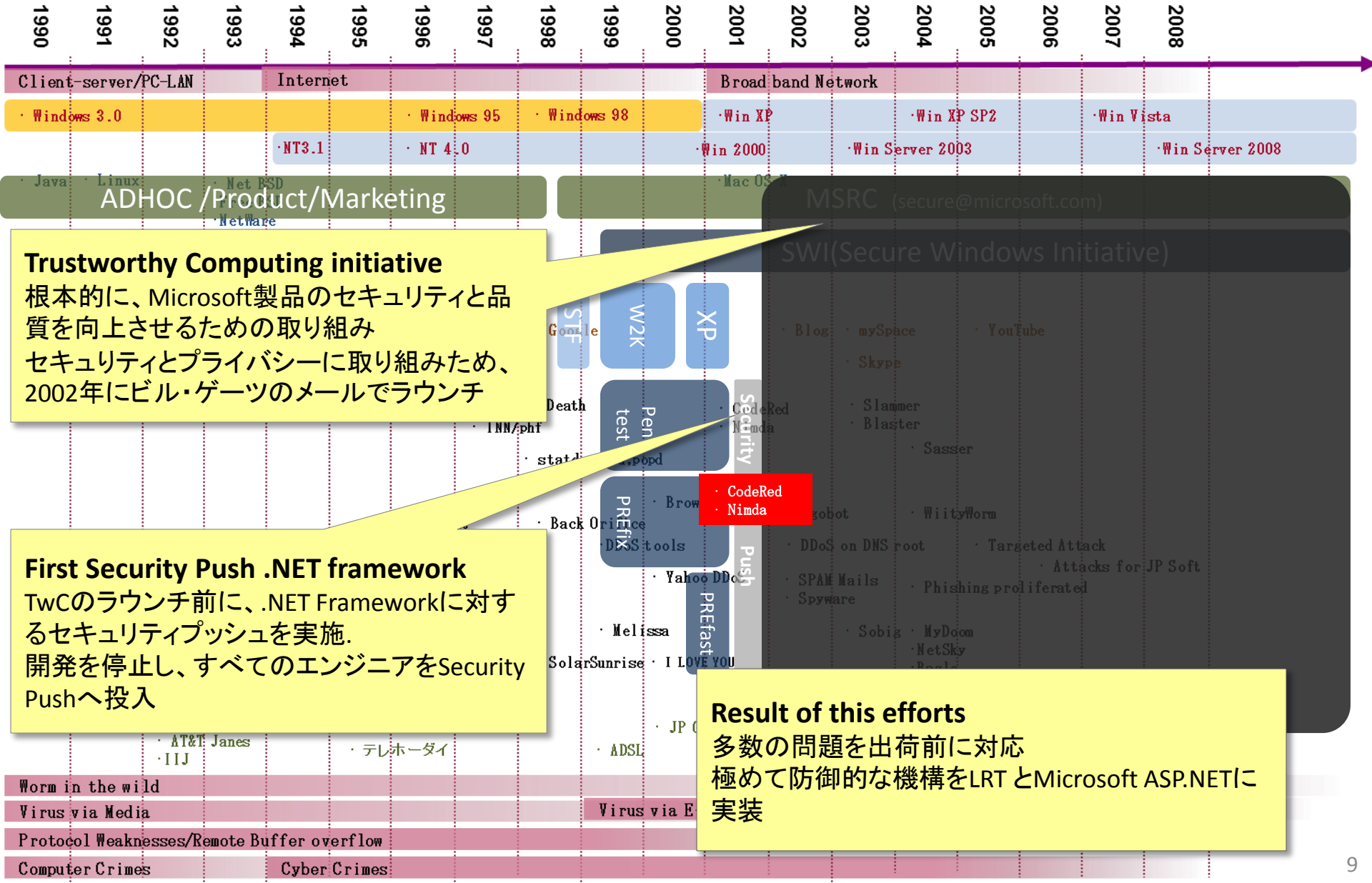
Security issues were SHIP STOPPER

確実なセキュリティの向上のため…
- 技術者の支援を中心に移行
- 魚（脆弱性）を釣る代わりに、魚の釣り方を教える
- “Security Days” “bug bashes”: これを、確実に実施するための施策

Security Day / Bug bash
2~4時間のセキュリティトレーニングで始まり、その日の復習で終了する。
コードのレビューを行い、ペネトレーションテスト（侵入テスト）や、その他のセキュリティテストを指導する。する、
“最高のセキュリティバグ賞”等を設置し、表彰を行う。

PREfirst，二つ目のツール
モジュール単位での発見に優れた、PREFirstの開発と導入

Windows Products and Security: Windows XP

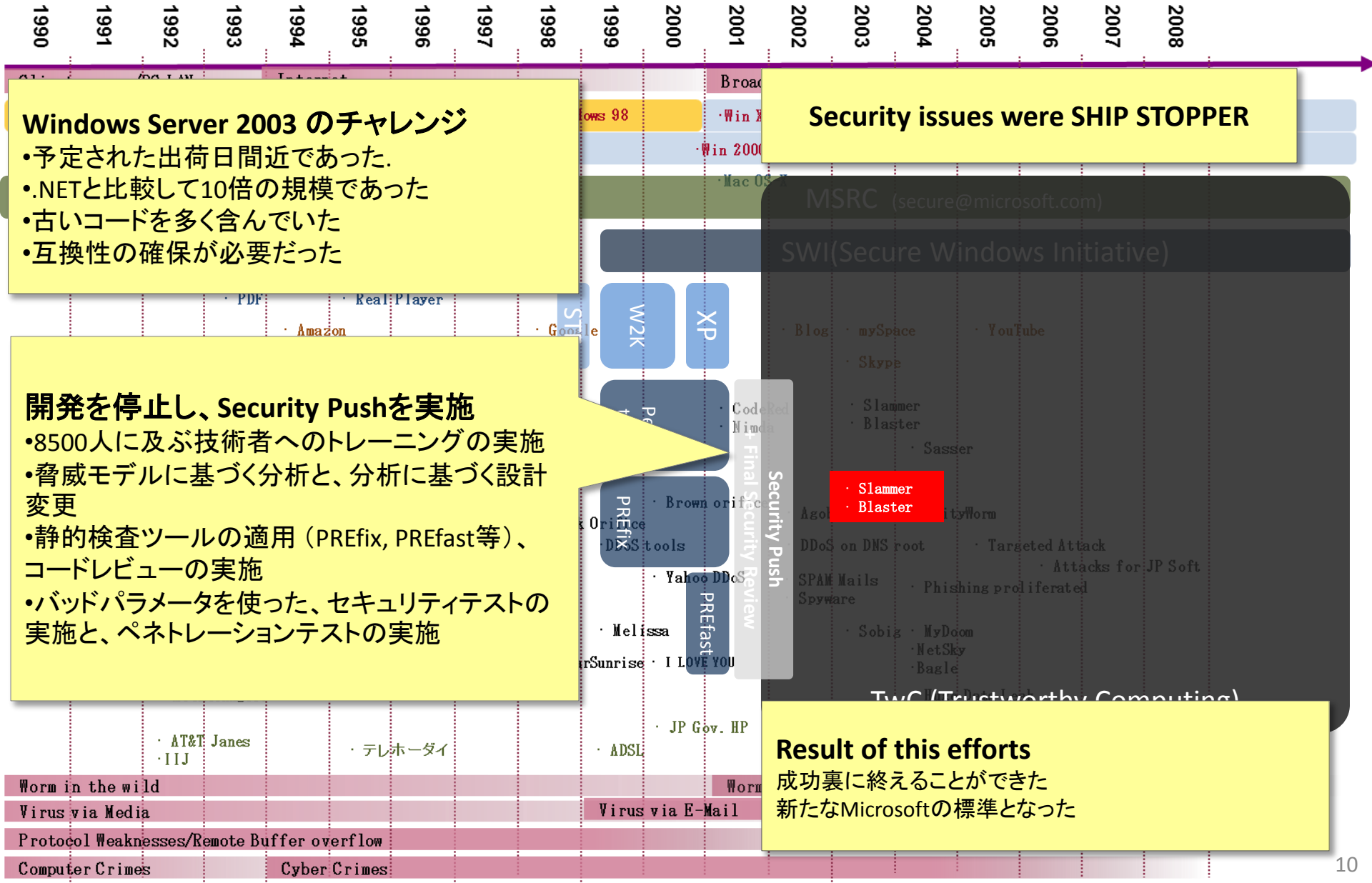


Trustworthy Computing initiative
根本的に、Microsoft製品のセキュリティと品質を向上させるための取り組み
セキュリティとプライバシーに取り組みため、2002年にビル・ゲーツのメールでラウンチ

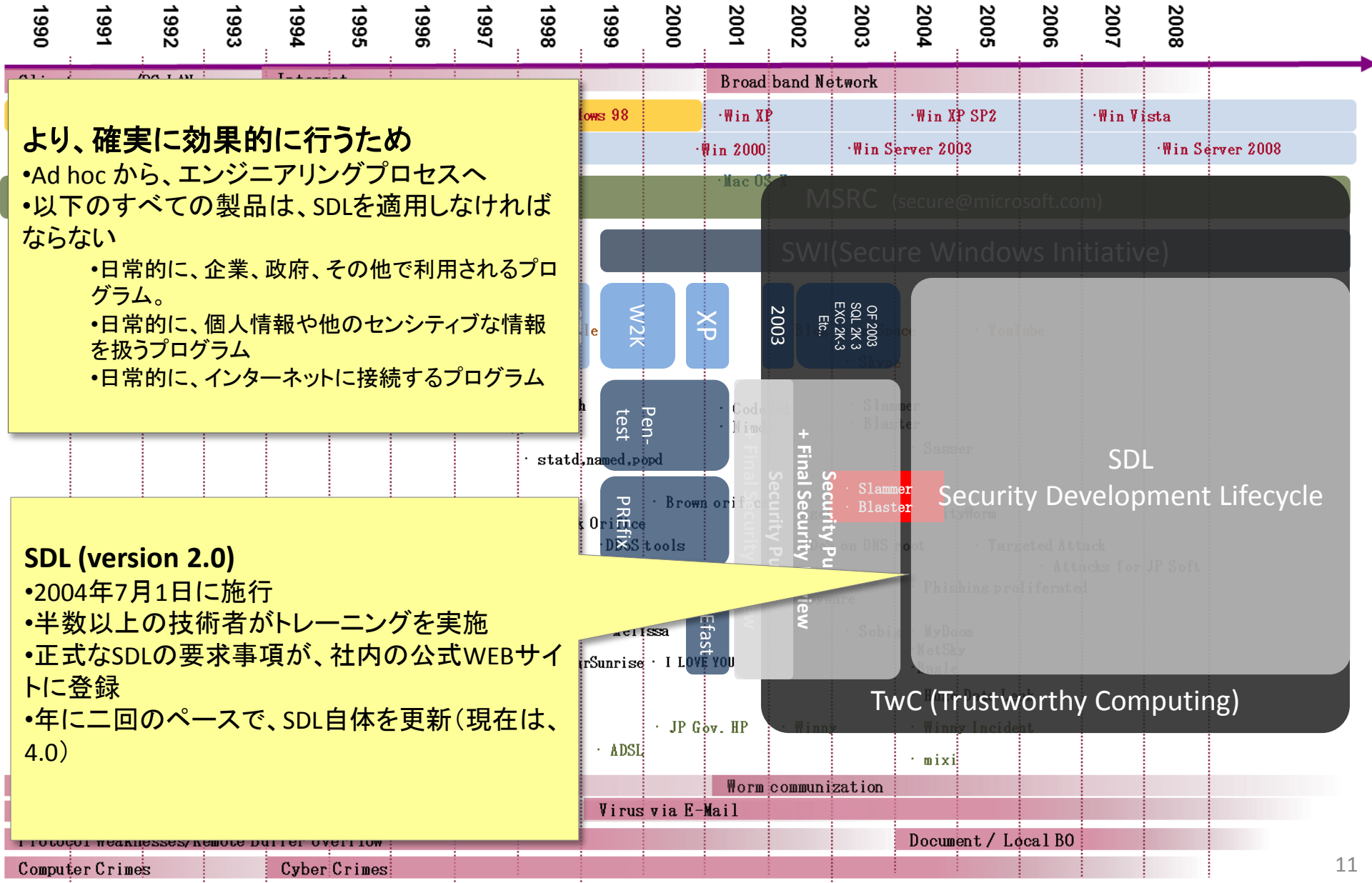
First Security Push .NET framework
TwCのラウンチ前に、.NET Frameworkに対するセキュリティプッシュを実施.
開発を停止し、すべてのエンジニアをSecurity Pushへ投入

Result of this efforts
多数の問題を出荷前に対応
極めて防御的な機構をLRT とMicrosoft ASP.NETに実装

Windows Products and Security: Windows XP



Windows Products and Security: Windows XP



より、確実に効果的に行うため

- Ad hoc から、エンジニアリングプロセスへ
- 以下のすべての製品は、SDLを適用しなければならない
  - 日常的に、企業、政府、その他で利用されるプログラム。
  - 日常的に、個人情報や他のセンシティブな情報を扱うプログラム
  - 日常的に、インターネットに接続するプログラム

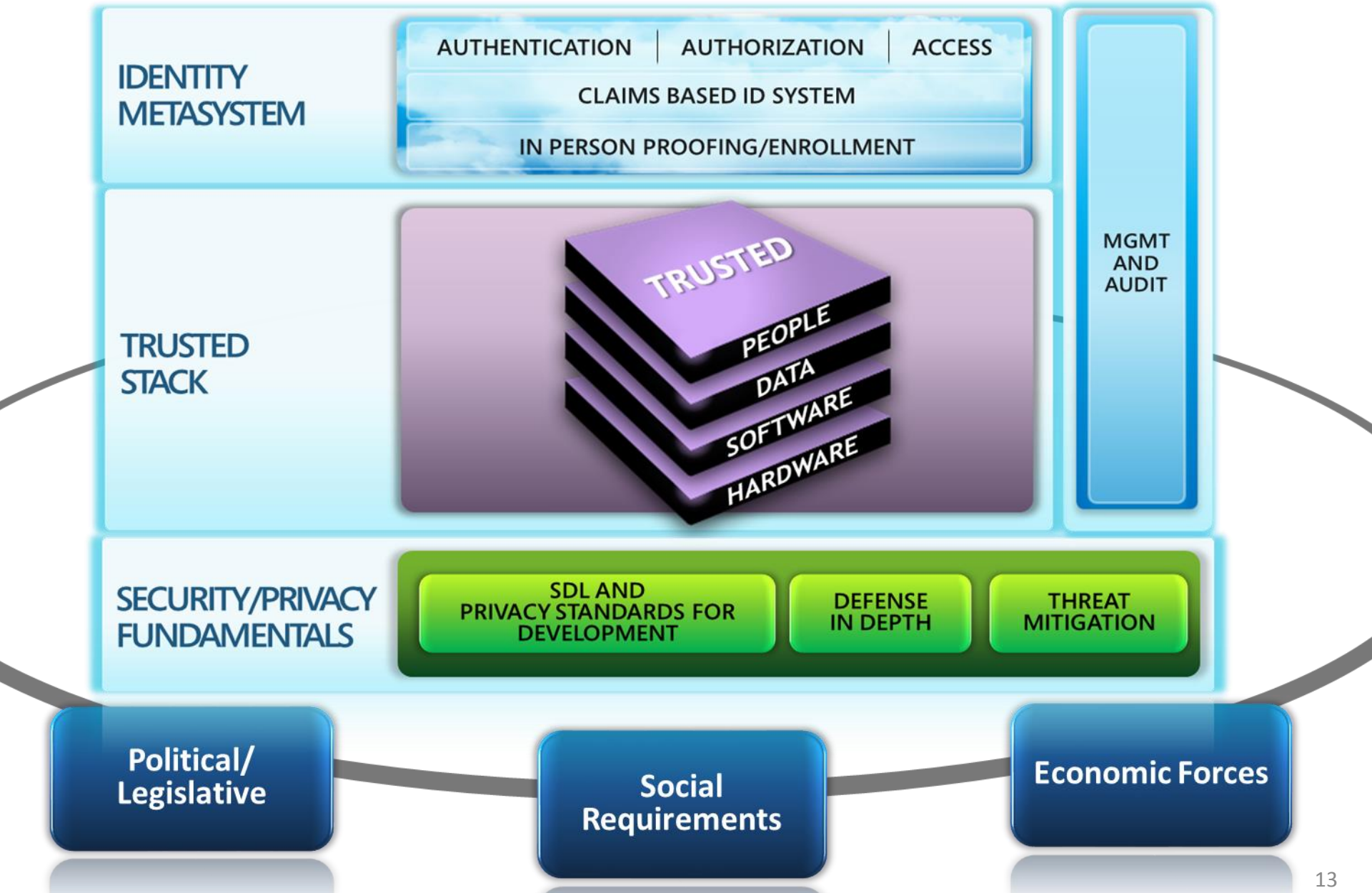
SDL (version 2.0)

- 2004年7月1日に施行
- 半数以上の技術者がトレーニングを実施
- 正式なSDLの要求事項が、社内の公式WEBサイトに登録
- 年に二回のペースで、SDL自体を更新（現在は、4.0）

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

End to End Trust : 新たなセキュリティモデル



最後に

- 思わぬ形で、ITが利用されている
  - ネットワークや端末、コントロールサーバーとして
    - もしかして、PCが端末になっていませんか？
    - もしかして、ブラウザで制御してませんか？
    - もしかして、TCP/IPとか使ってませんか？
      - ロボットのカタログを見ると、RJ45のインタフェースがついていることが多い
    - もしかして、、、、
- アンダーグラウンドビジネス
  - 絵空事だと思われるでしょうが。。。
    - 「すべてに価値がある」= 売買が可能である
      - クレジットカードなどの換金請負、ブランクカード、エンボスの販売
      - ロンダリング用のアカウントの提供者
      - 再配送サービス
      - 暗号解読サービス（4時間で38%が解読可能だったらしい）
  - 組み込み機器もハックされている
    - モチベーションの問題