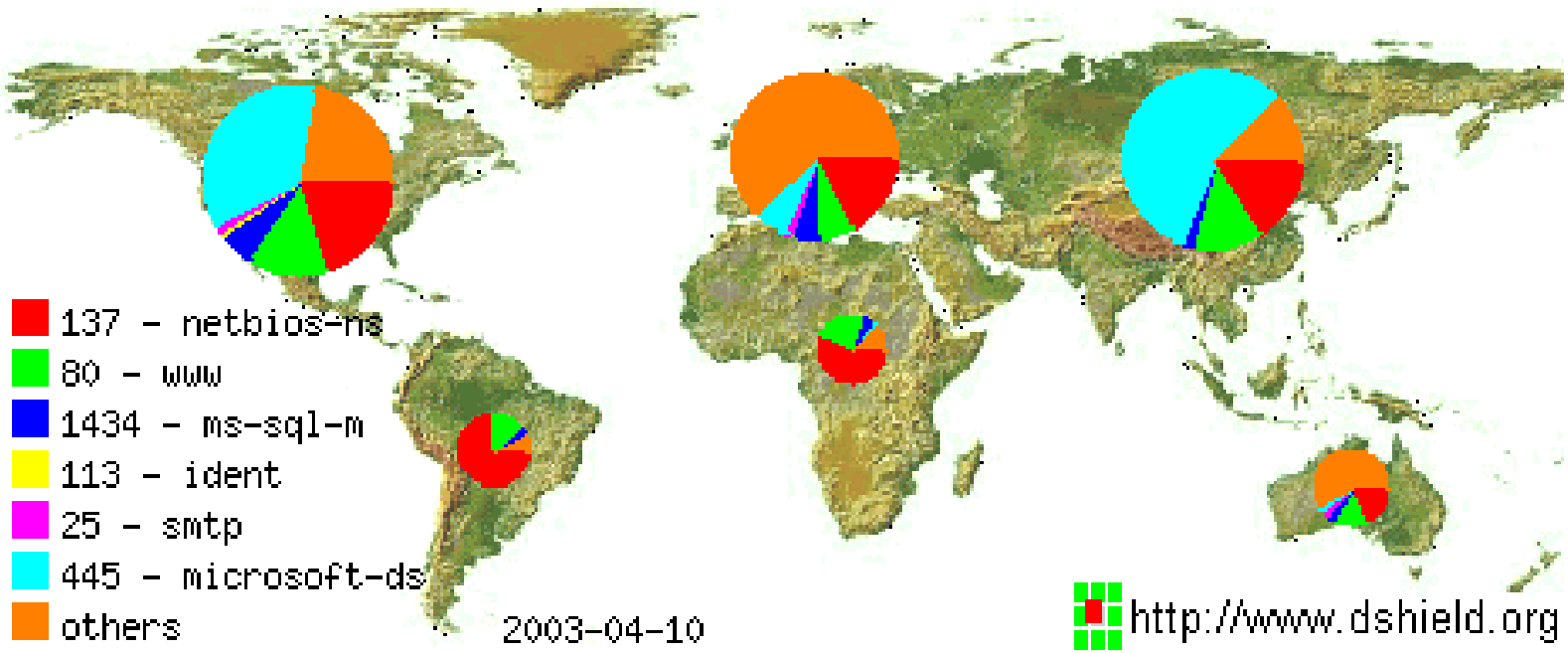
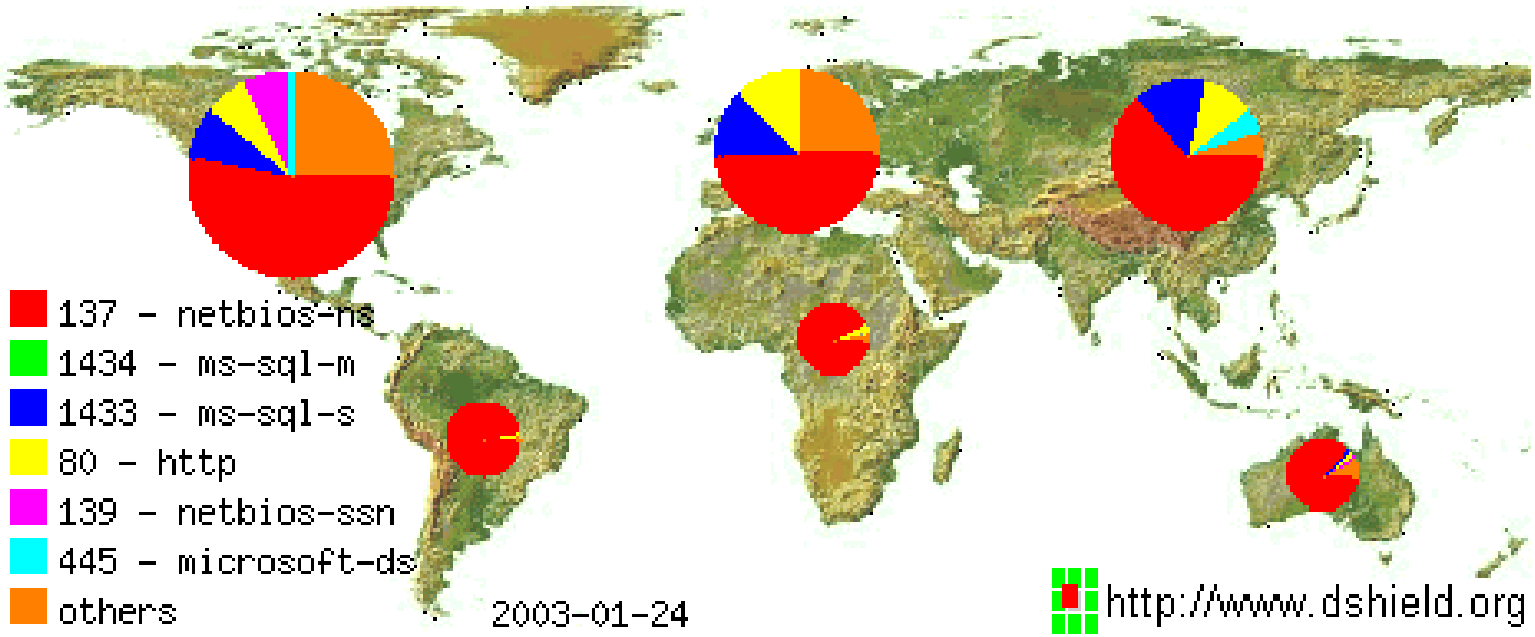
クライアント／サーバにおける次世代セキュリティテクノロジーのススメ

株式会社　シマンテック
野々下　幸治

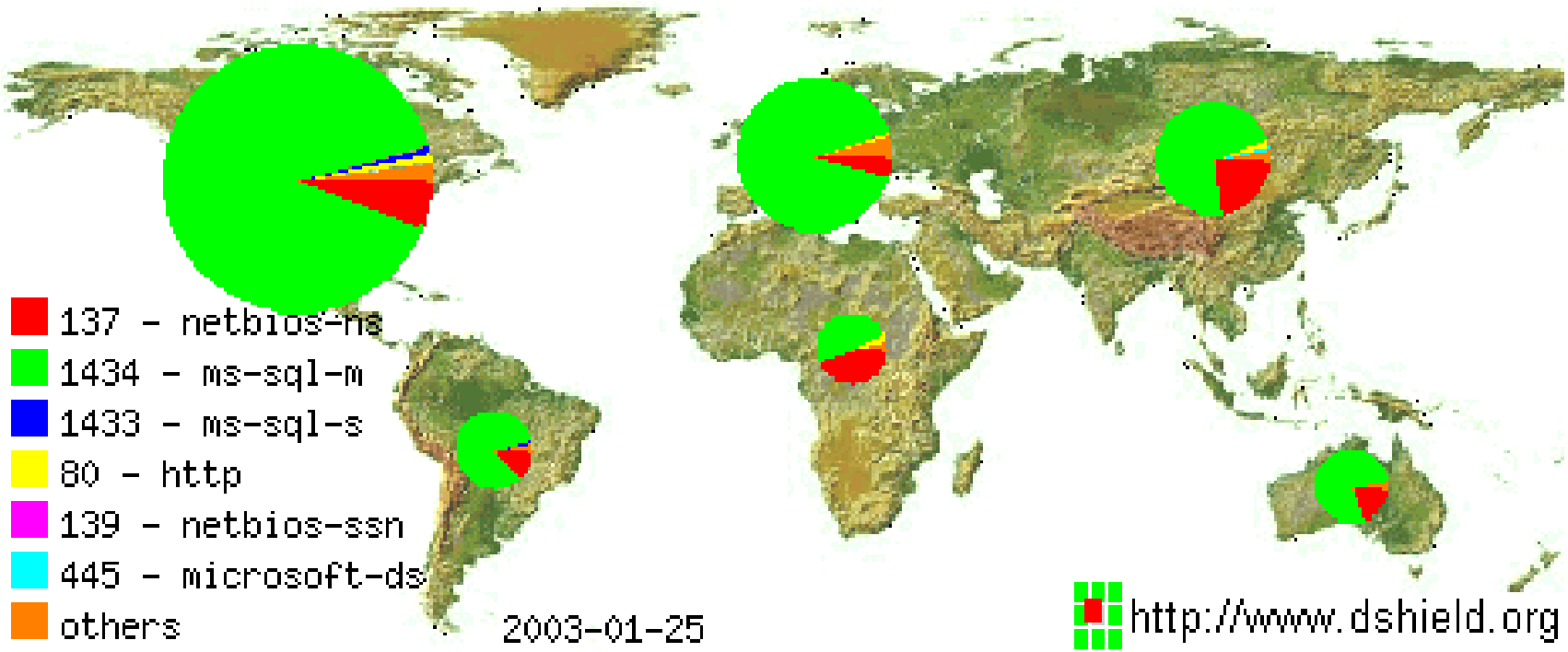
最近のInternetの攻撃パケットの状況



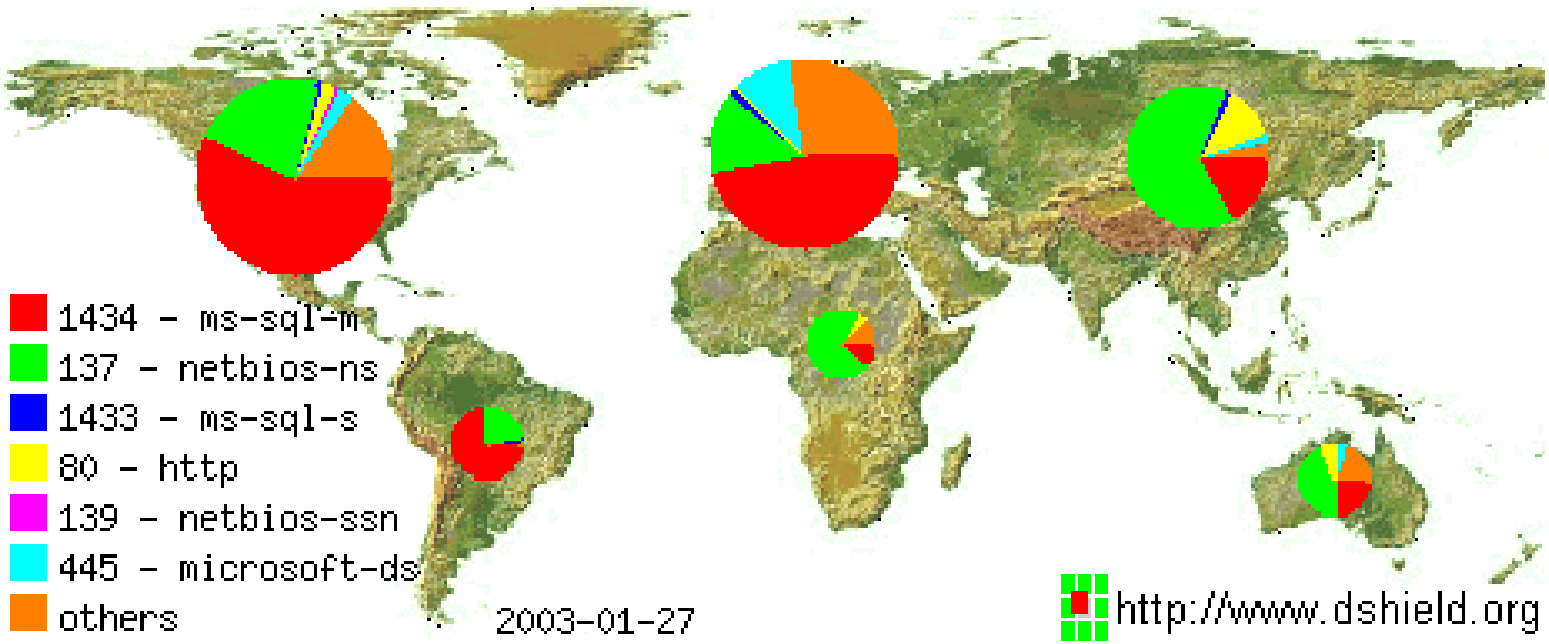
SQLワーム活動の前日のInternetの攻撃の状況



SQLワーム活動時のInternetの攻撃の状況



SQLのワームの活動鎮静時のInternetの活動



SecurityFocusにて捉えたSQLワームの状況

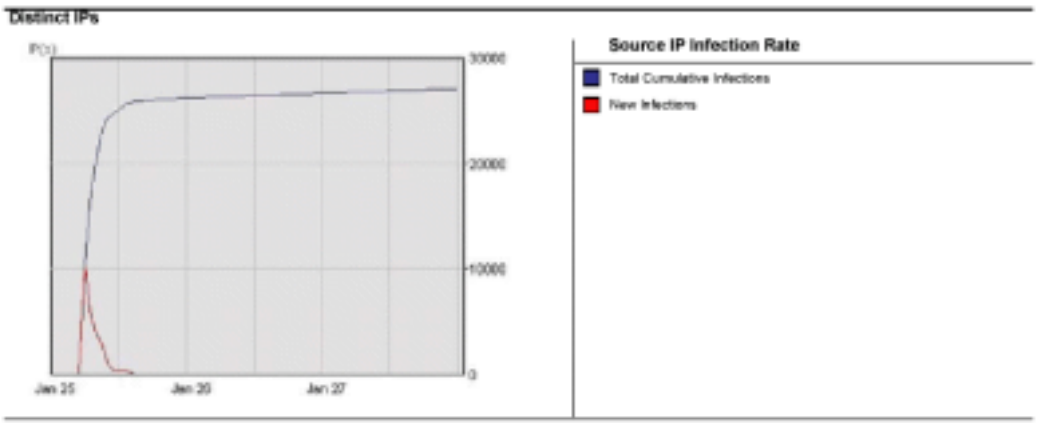


Figure 1. Hourly IP infection rate for UDP port 1434 for January 25 – 27, 2003

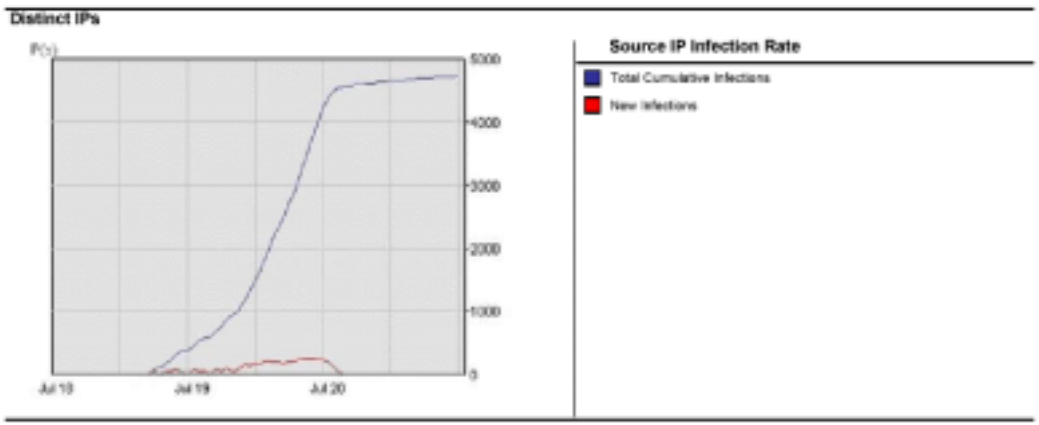
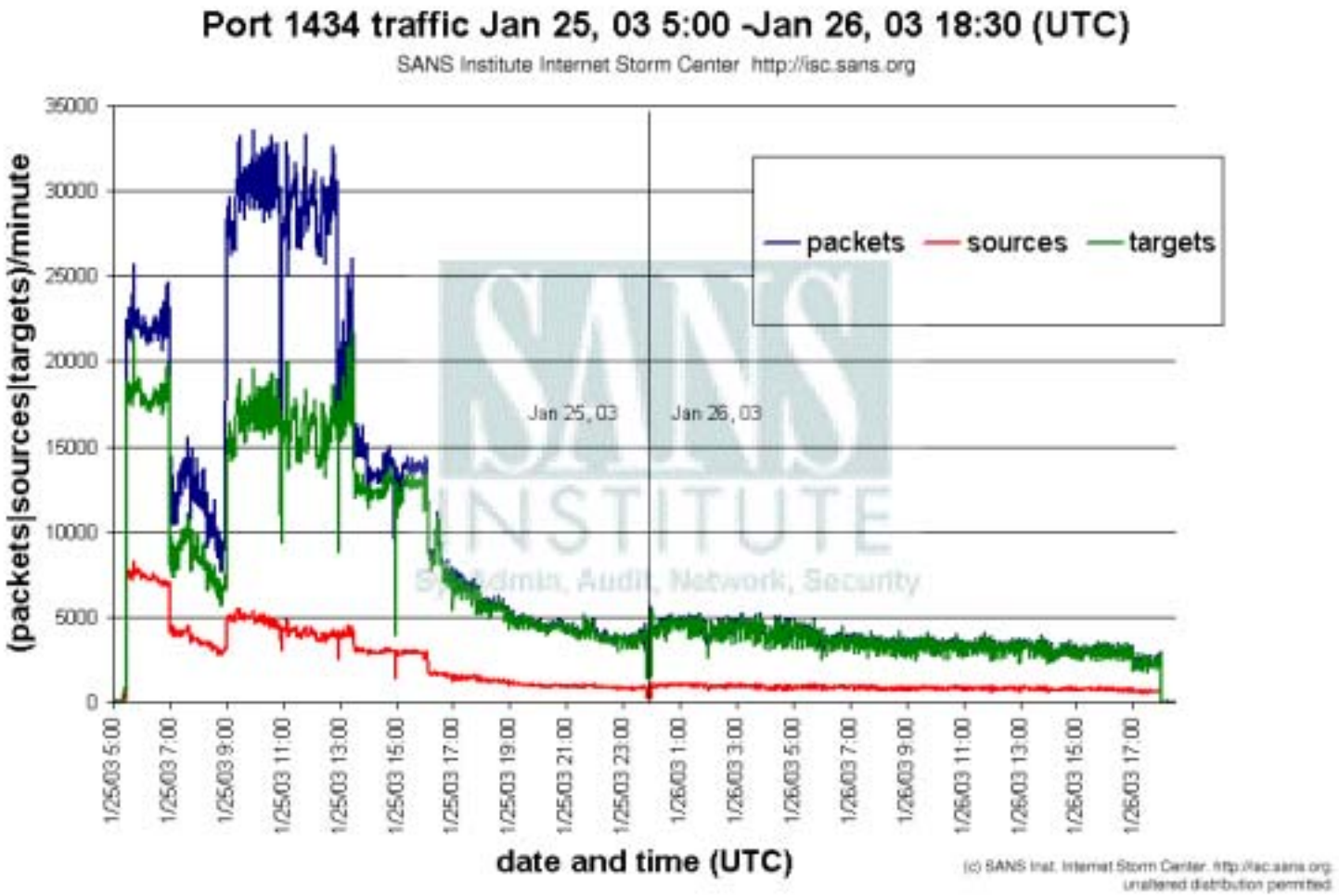
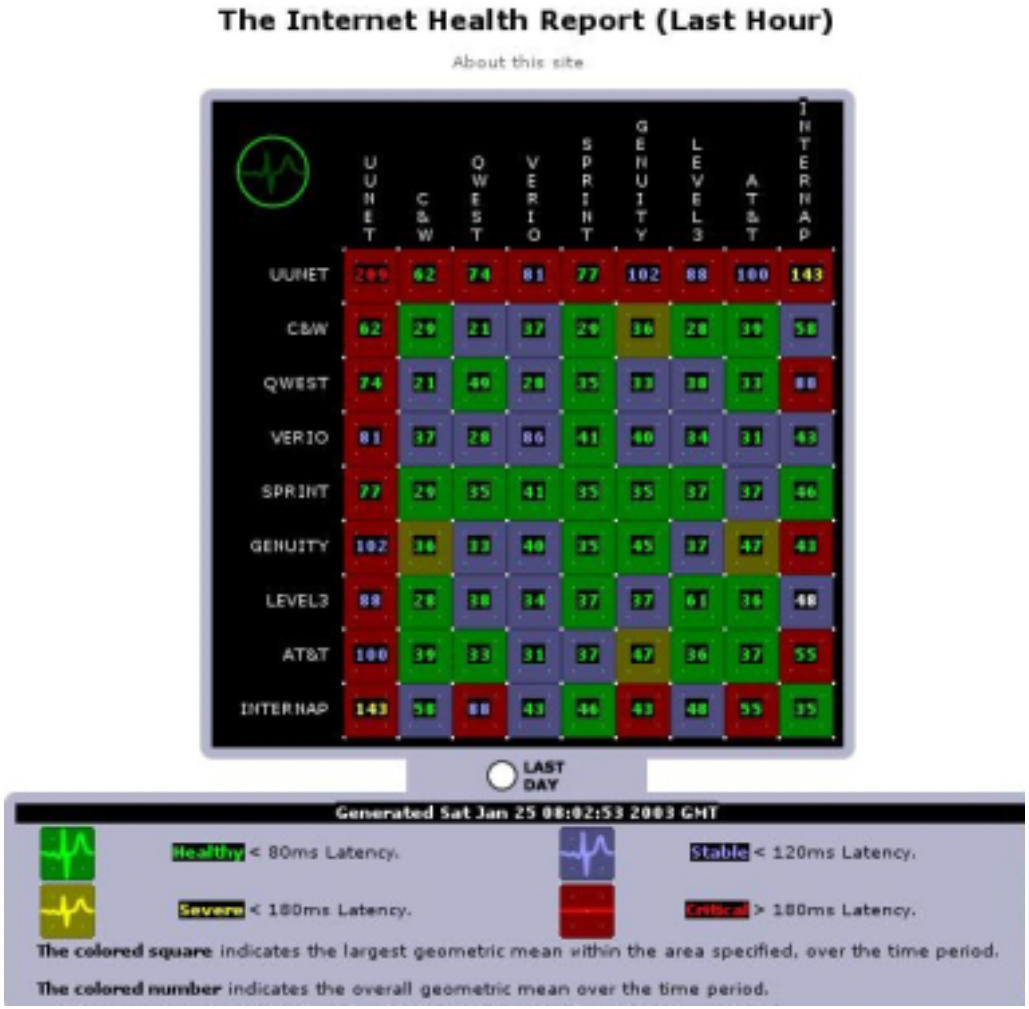


Figure 2. Hourly IP infection rate for Microsoft Indexing Server/Indexing Services ISAPI Buffer Overflow for July 18 – 20, 2001

Internet Stormセンターによる SQLワームの状況



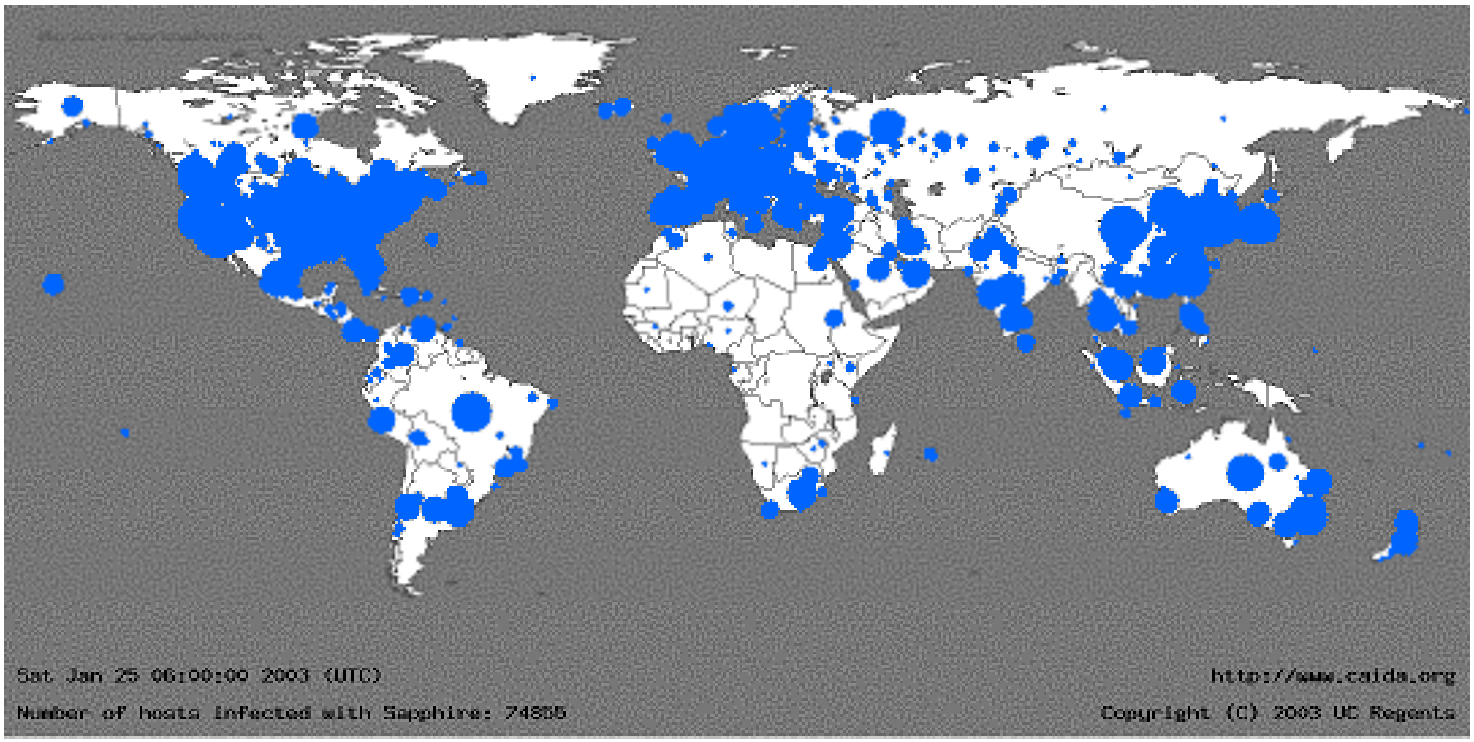
SQLワームにより受けたInternetのトラフィックの状況



SQL Slammerワームとシマンテックの対応

- 1月25日 5:30 GMT,Slammerの感染開始
  10分後には脆弱なシステムのほぼ90%に感染
- 6:00 GMT,Deepsight TMSのFirewallセンサーが大量の1434ポートへの接続を検知し、自動的にDeepSightの顧客へ警告が送信される。
- 7:00 GMT,Bagtraqへこの現象が投稿される
- 8:00 GMT,IDSのセンサーでワームの拡散活動を捉え,Deepsightの警告を2から3に上げる
- 10:00 GMT,Webに警告及びワームの詳細と対策方法を提供

SQL Slammerワーム:
Internetに放たれた後の30分後



- 8.5秒ごとに倍倍で感染
- CodeRedの100倍の速さで感染
- ピーク時には1秒間に5500万のホストがスキャンされた

Slammerワームの社会への影響

- バンク･オブ･アメリカの13000台のATMが止まった
- アトランタの新聞会社(The Atlanta Journal-Constitution)で日曜日の最初の新聞が印刷できなかった
- シアトル市の緊急通報システム（911）がダウン
- コンチネンタル航空のエレクトリック･チェックイン･システムがダウン
- 韓国では国内インターネットが大規模にダウン

2002年の攻撃のトレンド

- CERTによる攻撃のトレンドの概要
  - 自動化; 攻撃ツールのスピード
  - 攻撃ツールの高度化
  - より速くなった脆弱性の発見
  - ファイアウォールの通過可能性の増加
  - 非対称脅威の増加
  - インフラ攻撃による脅威の増加
    - ❖分散サービス不能攻撃 (DDoS)
    - ❖ワーム
    - ❖Internet DNSに対する攻撃
    - ❖ルータの悪用又はルータに対する攻撃

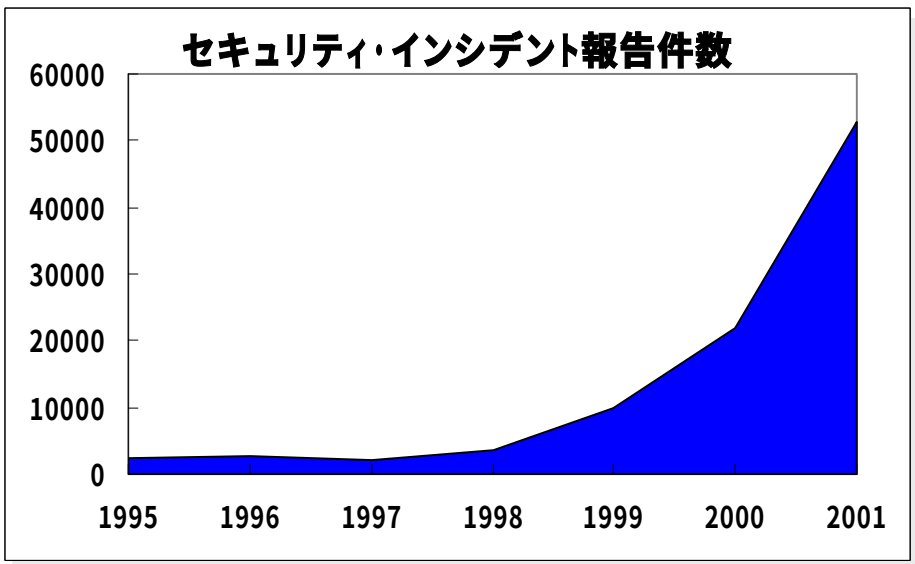
米CERT発信の文書より

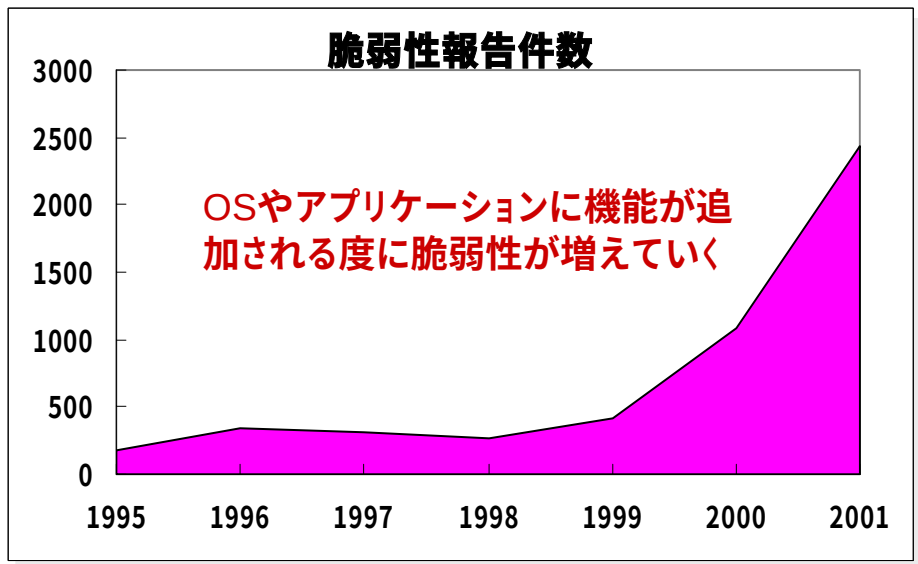
http://www.cert.org/archive/pdf/attack_trend.pdf

セキュリティ・インシデントと脆弱性の関係

1995年～2001年のインシデントと脆弱性の報告件数を比較すると、その増加傾向が非常に類似している

- ネット上に潜む脅威の大半が既知の脆弱性を狙った行為
- OSやアプリケーションの脆弱性対策を行うことで殆どの脅威に対応することが可能（99%の不正侵入は未然に防ぐことが可能：CERT）

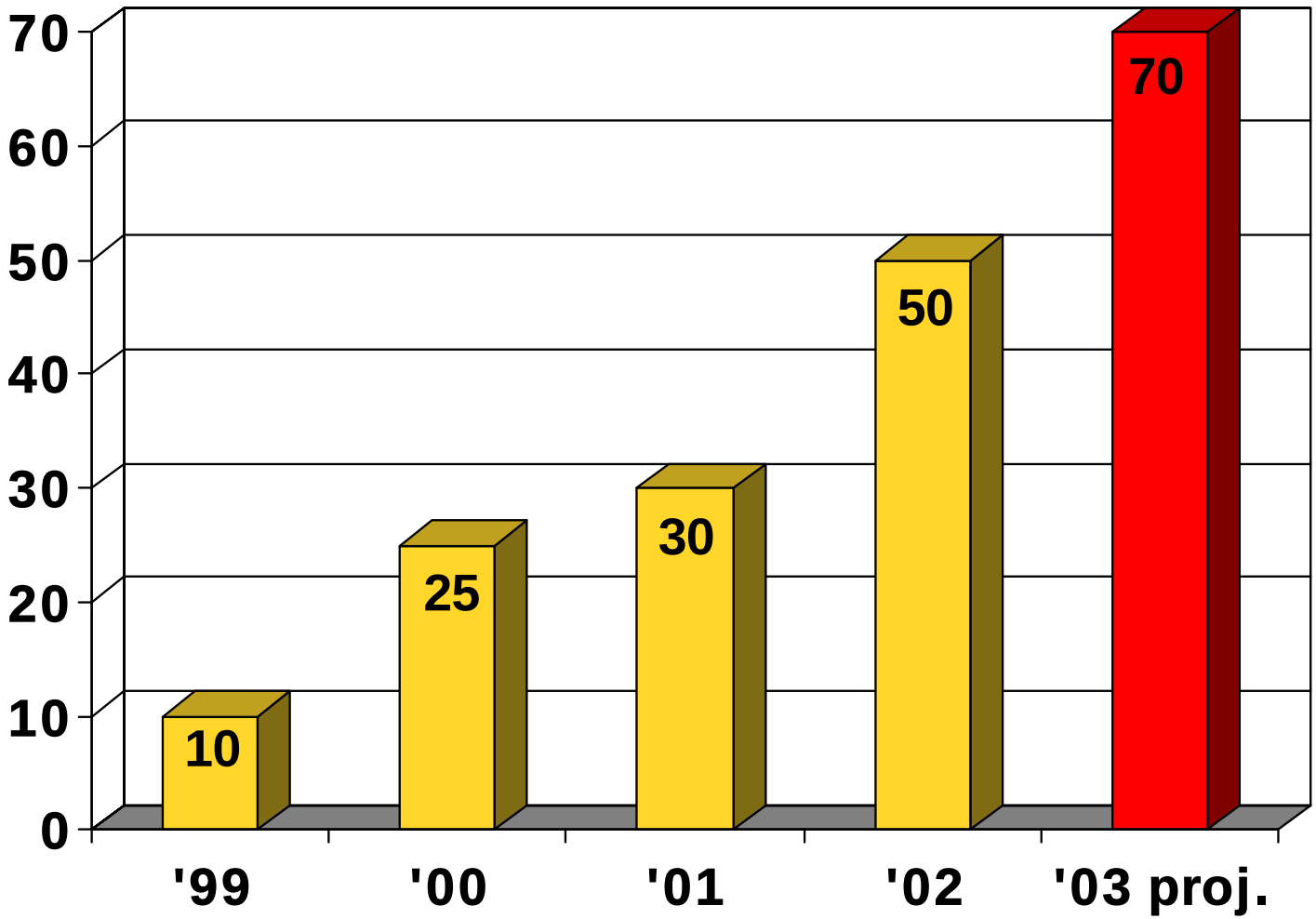




米CERT/CC発統計情報
http://www.cert.org/stats

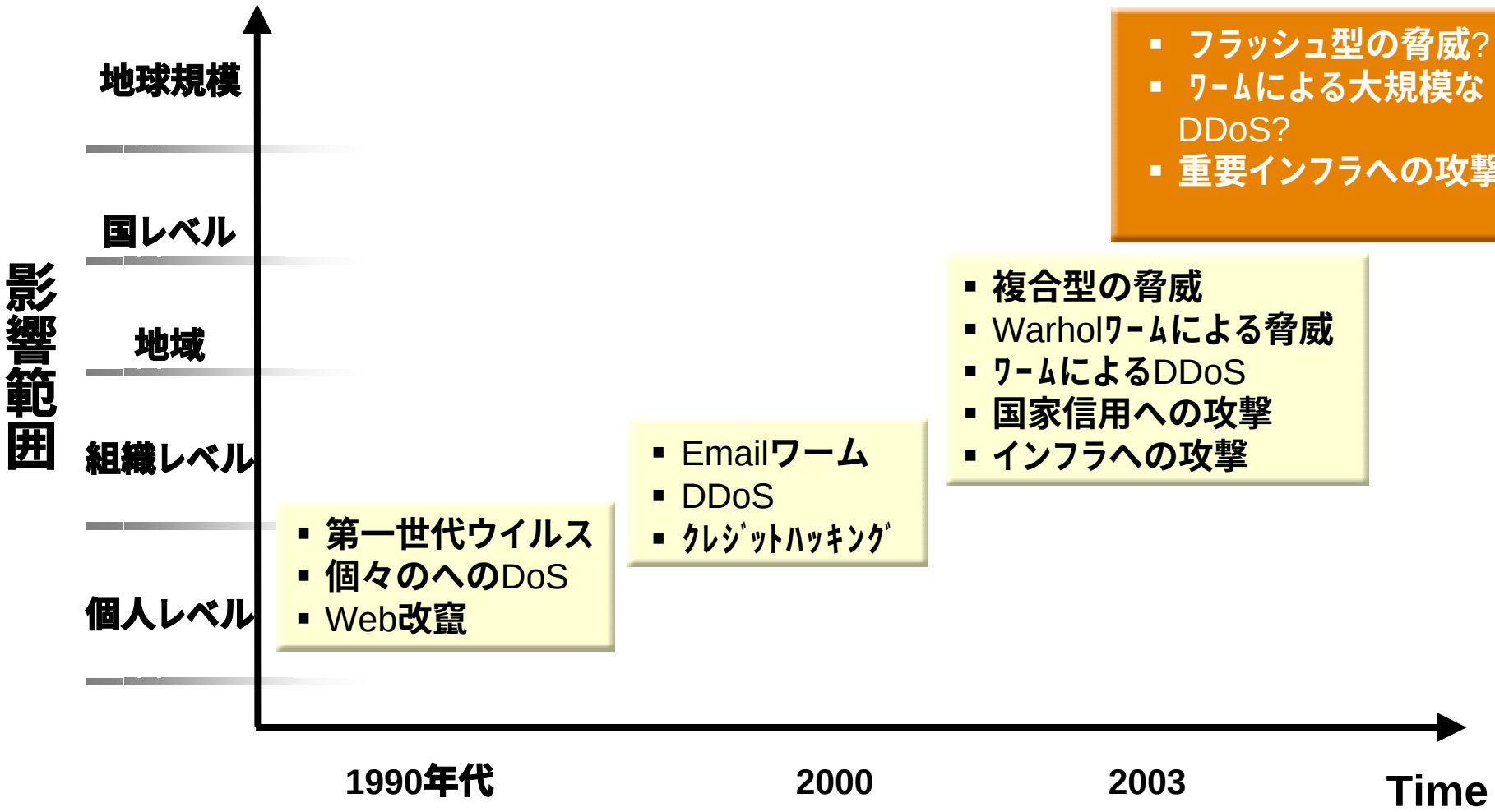
脆弱性の増加

1週間に発見される新しい脆弱性

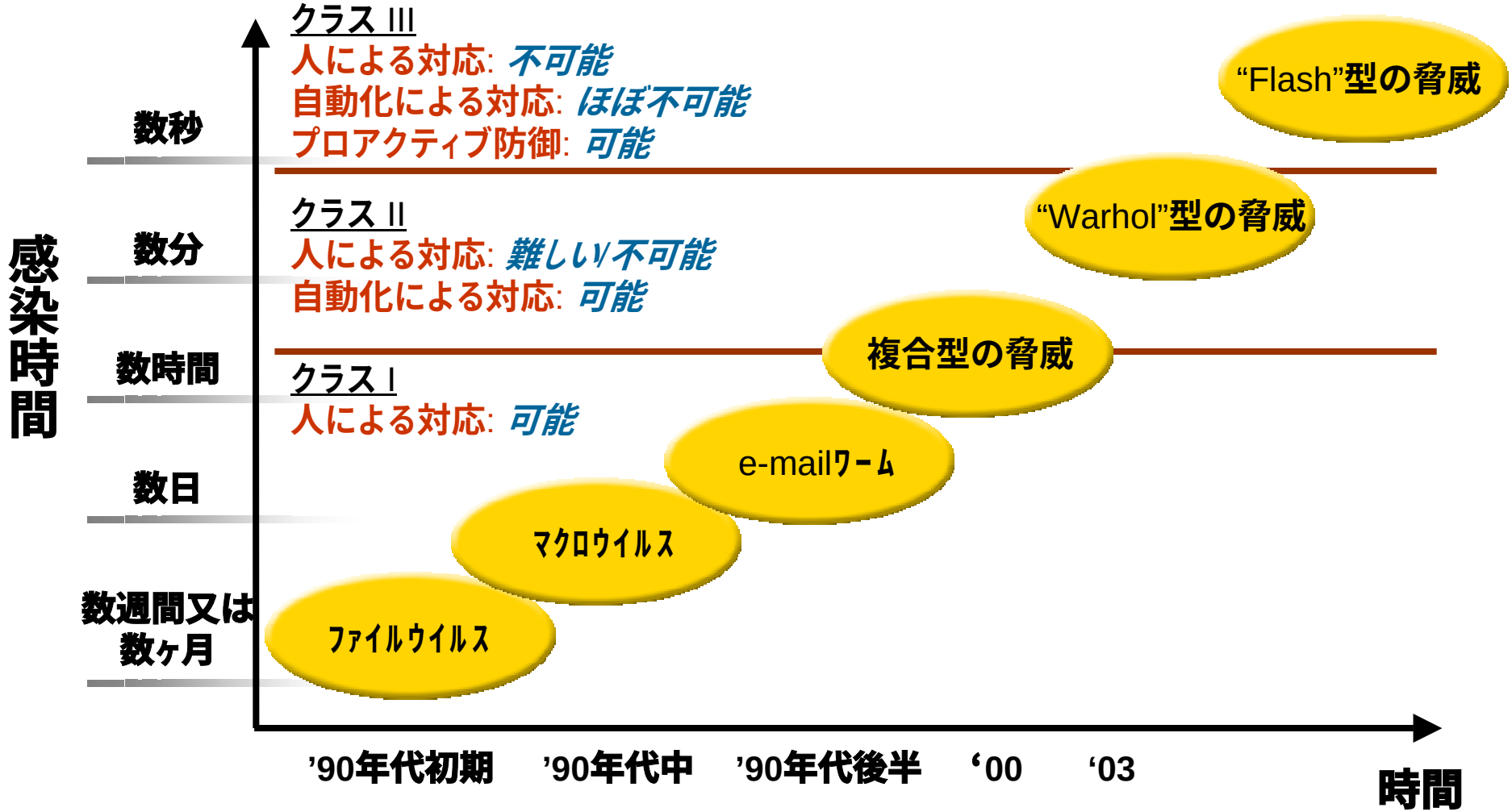


Source: Bugtraq

脅威の進化

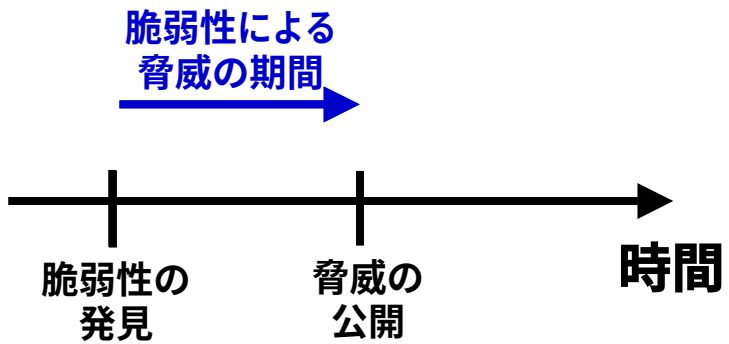

影響範囲
地球規模
国レベル
地域
組織レベル
個人レベル
▪ 第一世代ウイルス
▪ 個々へのDoS
▪ Web改竄
▪ Emailワーム
▪ DDoS
▪ ｸﾚｼﾞｯﾄﾊｯｷﾝｸﾞ
▪ 複合型の脅威
▪ Warholﾜｰﾑによる脅威
▪ ﾜｰﾑによるDDoS
▪ 国家信用への攻撃
▪ インフラへの攻撃
▪ フラッシュ型の脅威?
▪ ﾜｰﾑによる大規模なDDoS?
▪ 重要インフラへの攻撃?
1990年代
2000
2003
Time

脅威の進化: 悪意を持ったコード



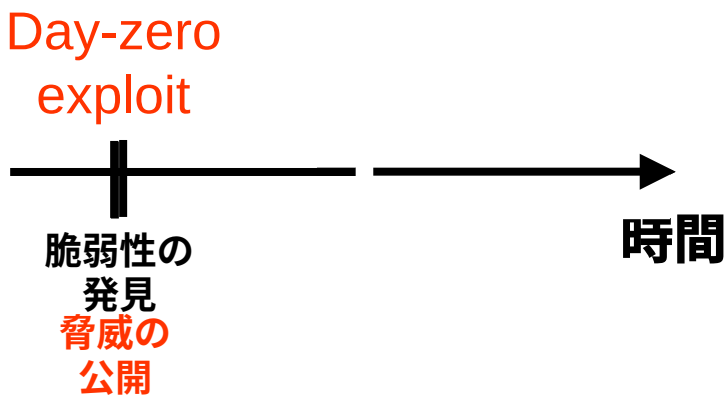
脅威の進化: Day-zeroの脅威

未知の脅威や脆弱性への対応が準備できる前に行なわれるのをDay-zero**の脅威 という**

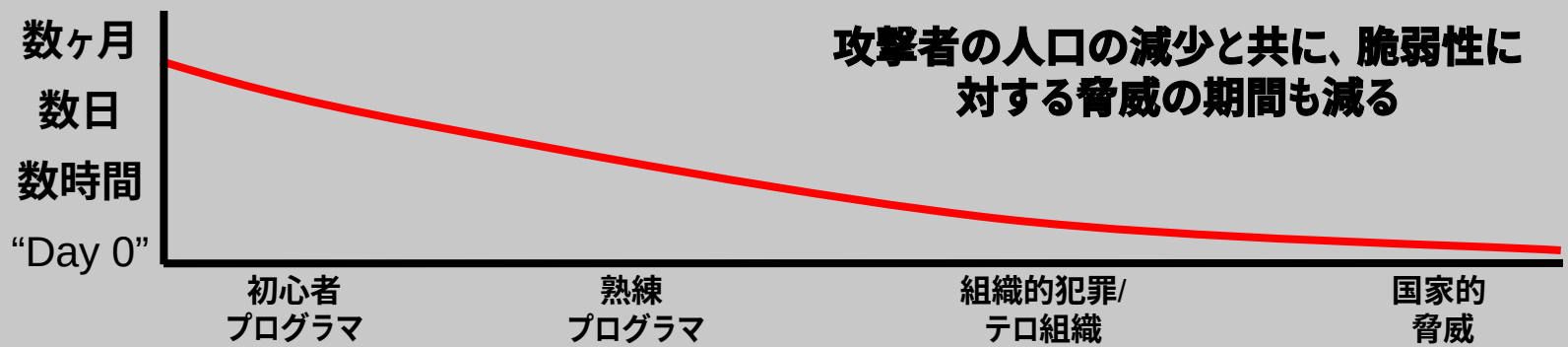


脅威の進化: Day-zeroの脅威

未知の脅威や脆弱性への対応が準備できる前に行なわれるのをDay-zero**の脅威 という**



脆弱性悪用までの時間



最近発見された脆弱性の報告までのプロセス

- Sendmailのバッファオーバーフローの脆弱性
  - 2002年12月1日 脆弱性の発見
  - 2002年5月2日 NIPCへ通知
  - 2003年1月13日 Sendmailへ通知
  - 2003年1月22日 Sendmailと最初のリリースの共同作業
  - 2003年2月7日 連邦政府と初期の共同作業
  - 2003年3月3日 アナウンス
  - 2003年3月4日 exploit codeがBugtraqに投稿
- Sambaのcall_trans2openのバッファオーバーフローの脆弱性
  - 2003年4月3日 security@samba.orgに通知
  - 2003年4月3日 elrond@**samba**-tng.orgに通知
  - 2003年4月3日 Sambaチームより脆弱性を確認したことが電話で連絡される
  - 2003年4月3日 Samba-TNGのElrondより同様に脆弱性の確認の回答が行なわれる
  - 2003年4月4日 Sambaチームがvendorsecメーリングリストに通知
  - 2003年4月7日 脆弱性の公開
  - 2003年4月7日 exploit codeも同時にリリース

新しいサービスに対する脅威の影響

<table>
<tr><th>ターゲット
脅威</th><th>無線LANシステム</th><th>Webサービス</th><th>Internet
バックボーン/
ブロードバンド</th><th>物理インフラ/
SCADA</th></tr>
<tr><td>Flash又は
Day-Zero
型の脅威</td><td rowspan="2">複数のネットワークへの大規模な混乱</td><td rowspan="4">大規模なB2Bサービスの混乱による地域レベルへの影響</td><td rowspan="2">世界規模での
Internet
の混乱</td><td rowspan="3">多くのｲﾝﾌﾗに影響:
▪ 電力
▪ 通信
▪ 水
▪ プラント
▪ その他のｲﾝﾌﾗ</td></tr>
<tr><td>Warhol又は
Day-Zero
型の脅威</td></tr>
<tr><td>複合型の脅威</td><td rowspan="2">個別ネットワークの短期間の混乱</td><td rowspan="3">短期的/局所的な
Internet
の混乱</td></tr>
<tr><td>DDoS</td><td>Internetを利用した分散SCADA</td></tr>
<tr><td>狙った攻撃</td><td>ｱｶｳﾝﾄ情報の盗難/ 改竄, DoS</td><td>データの盗難/
改竄, DoS</td><td>ターゲット
となった
インフラの混乱</td></tr>
</table>

ソリューションの進化

	ホスト セキュリティ	ネットワーク/ゲートウェイ セキュリティ	アプリケーション セキュリティ	管理	警告と 対応
将来	適応型クライアントSec	ルータスロットリング	相関による アプリケーションIPS	適応型管理 と ロックダウン	包括的な 攻撃へ 防御
	クライアント適合チェック	統計的/PAD IPS			
	自動ロックダウン	Web サービス セキュリティ	ERP/CRM/ Database IPS	複数プロダクトの 相関	ハニーネット
	無線デバイス	無線ゲートウェイ			
				複数ベンダ	分散センサー
今日	ホスト侵入防御	アンチスパム			
		ネットワークIPS		複数製品, シングルベンダ	自動での 対応の実行
		7層でのFirewall	データベースの 脆弱性 スキャナ		
これまで	これまでの AV/HIDS	これまでの Firewall/IDS		単一製品の 管理性	人手による 対応の実行

悪意のあるコードの防御に対する戦略

脅威のｸﾗｽ	検知による防御	リアクティブ防御	プロアクティブ防御
ｸﾗｽIIIの脅威 (Flash型, Day-Zero型脅威)	分散センサー ネットワーク	以後に発生する 脅威の対してのみ 有効	攻撃への 包括的な防御
ｸﾗｽIIの脅威 (複合型の脅威, Warhol, Day-Zero)	プロトコル 違反検知 技術	自動での指紋の 作成 (より遅いｸﾗｽIIの 脅威へ有効)	ネットワーク型 侵入防止 ホスト型 侵入防止
ｸﾗｽIの脅威 (複合型の脅威, worms, viruses)	ﾙｰﾙと 統計による 相関	人手による 指紋 自動での 指紋の 生成	適応型 セキュリティ

未知の脅威に対する効果的セキュリティ対策

1. プロアクティブなセキュリティ対策
   - 定期的なシステム検査による健康なシステムづくり
   - 敵を知る、弱点を知る、防御策を知る → “知る”ことが大事
     (ポリシー監査／脆弱性検査／脅威管理システム)
2. 未知の脅威に対するリアルタイムなブロック
   - アプリケーションレベルでチェックするファイアウォール
   - 不正侵入防御ツール(IPS) – Anomaly検知、ホストベース
3. 包括的なセキュリティ対策
   - 各種セキュリティ製品のイベント／インシデント情報を統合

Internetの脅威の状況を知るための製品

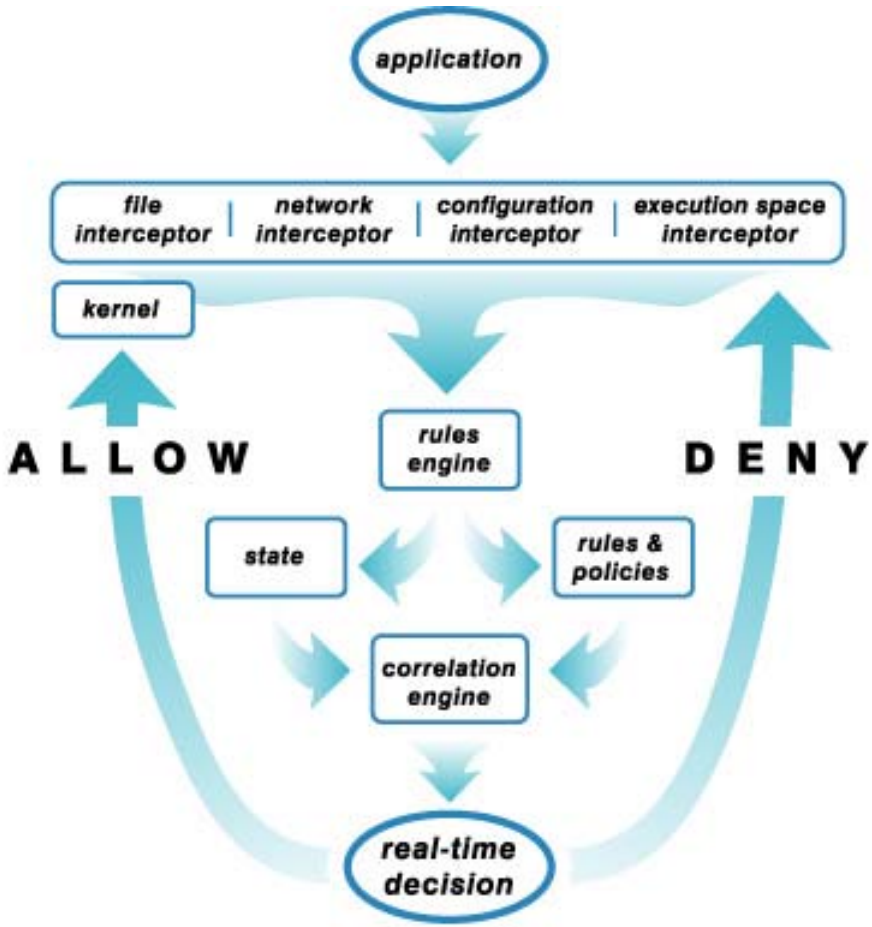
- Symantec DeepSight Threat Management
- ISS X-Force Threat Analysis Service
- TruSecure IntelliShield、Wormwatch.org
- SANS Internet Storm Center

サーバやクライアントをセキュリティを強化する方法

- アンチウイルスソフトの導入
- Sandboxでのアプリケーションの利用
- 脆弱性検査ツールで弱点の発見と対処
- ポリシーの強化及び遵守の定期的な検査
- ホストベースのファイアーウォール
- ホストベースのIDS
- ホストベースのIPS

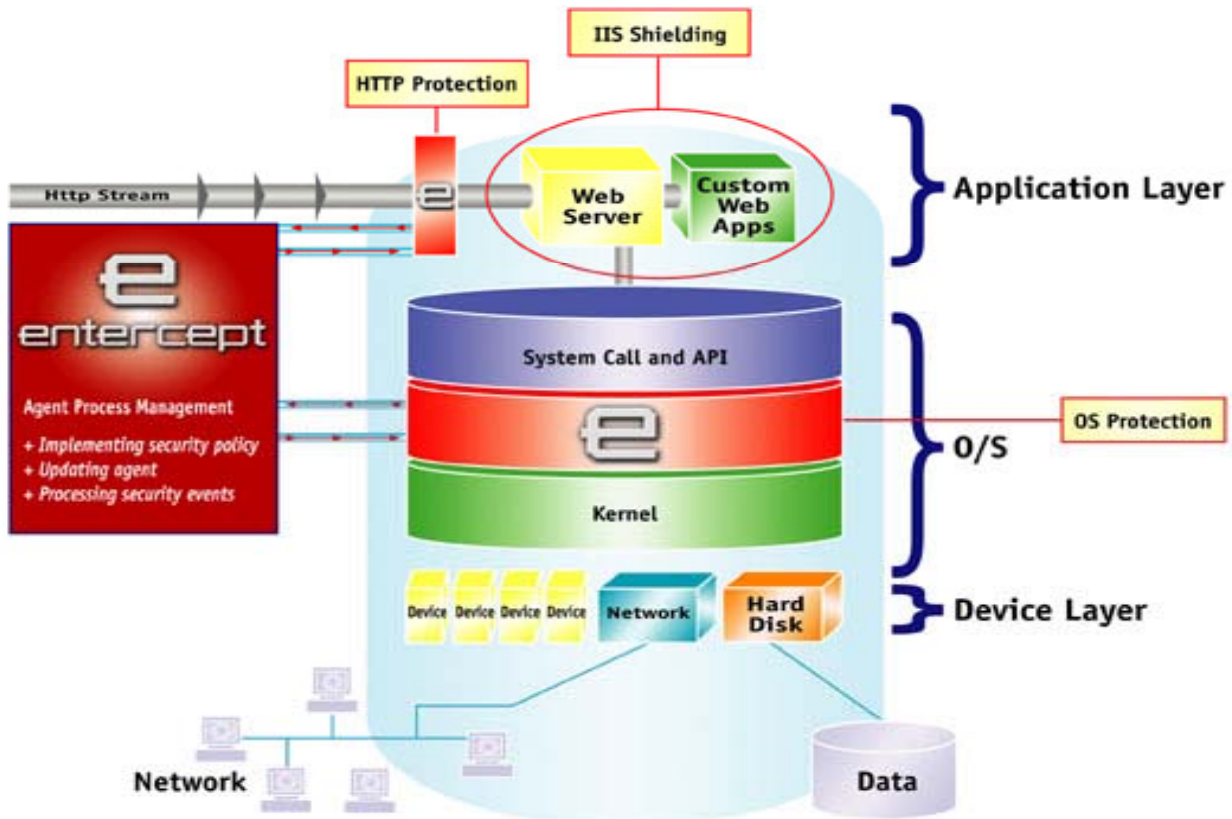
OKENA StormWatch アーキテクチャ

- StormWatchエージェントはアプリケーションのシステムコールの呼び出しを奪って、OkenaのINCOREアーキテクチャを通して許可/拒否を実行
- **INCORE**
  INtercept
  COrrelate
  Rules
  Engine
- “Zero Update”アーキテクチャ – シグネチュアを必要としないので、未知の攻撃へ対応



Entercept アーキテクチャ

Host Sensor: How it Works



Sana Security Primary Response アーキテクチャ

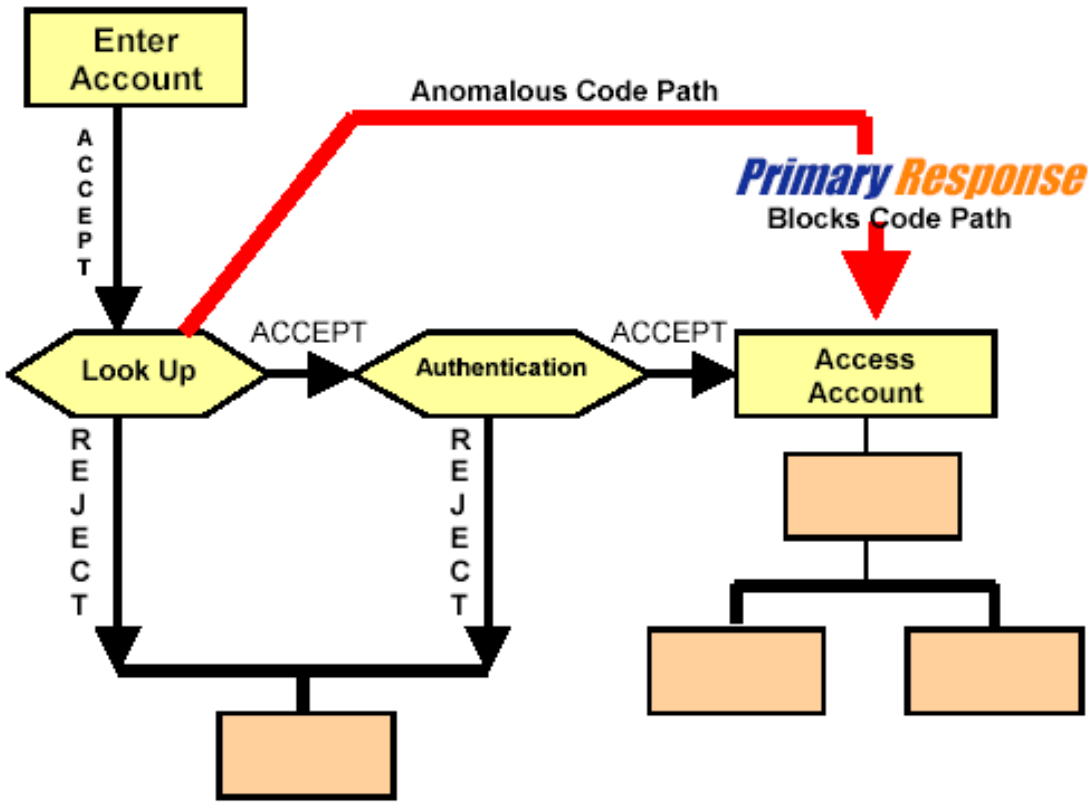
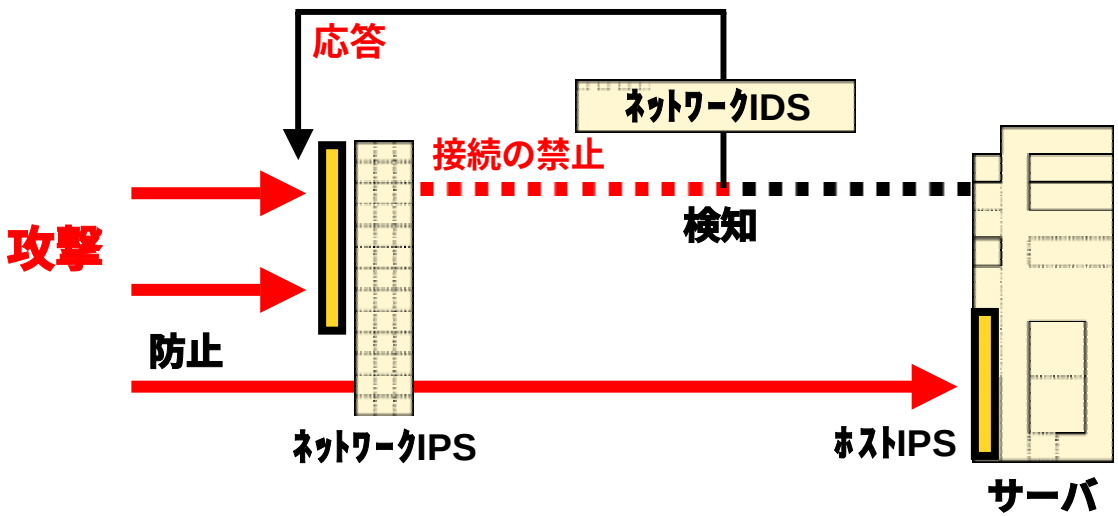


Figure 1. Monitoring and blocking code paths

侵入防止(IP)とビヘビアブロッキング

- 被害を受ける前に攻撃を防御する技術
- 2つのタイプの侵入防止技術: ネットワークとホスト



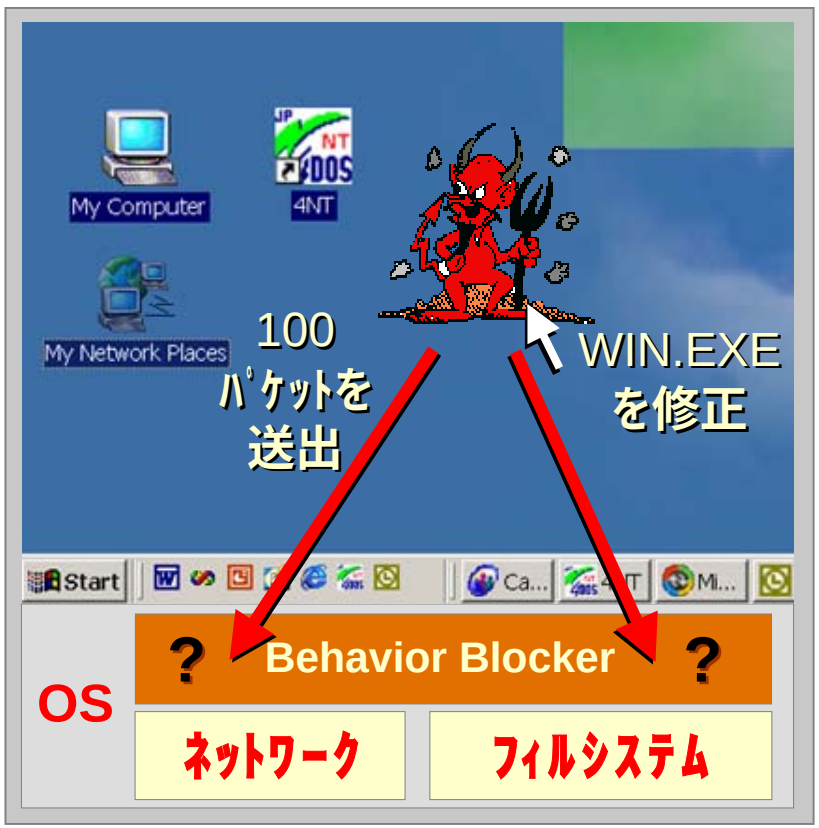
- 決して「検知の技術」は不要とはならない

侵入防止技術のチャレンジ

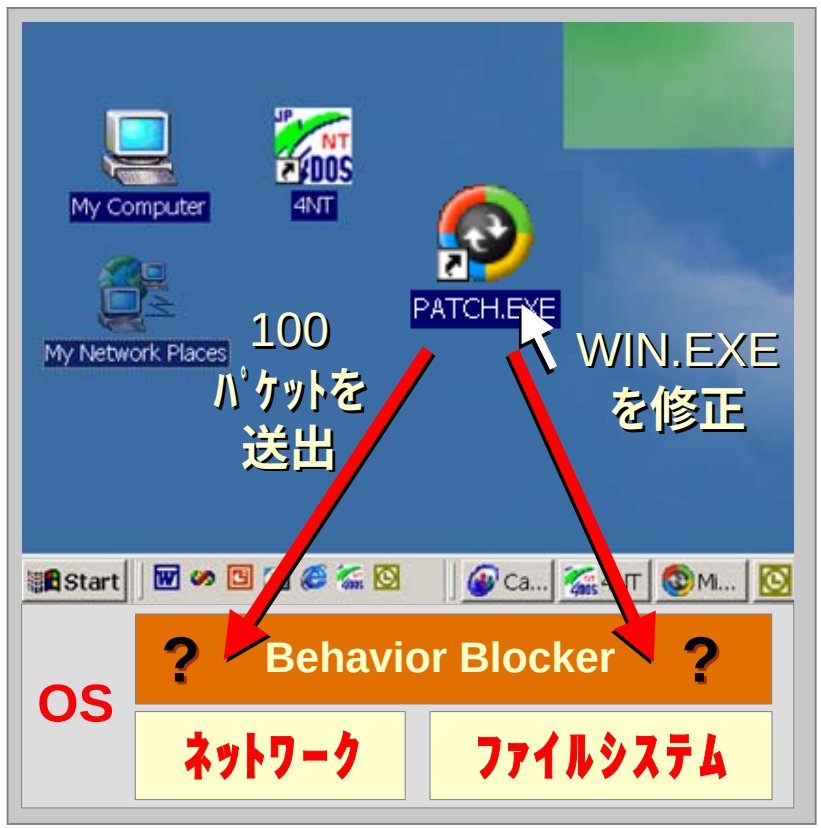
- 誤検知をいかに減らすか
- 複雑な侵入の特徴を捉えるための配置や管理上の問題
- より速く感染する新しい攻撃を未然に防御
- 特定のアプリケーションが正しいまたは違法な使用をすることを学習する方法の開発

IPSのチャレンジの例: ビヘビアブロッキング

悪いプログラム?



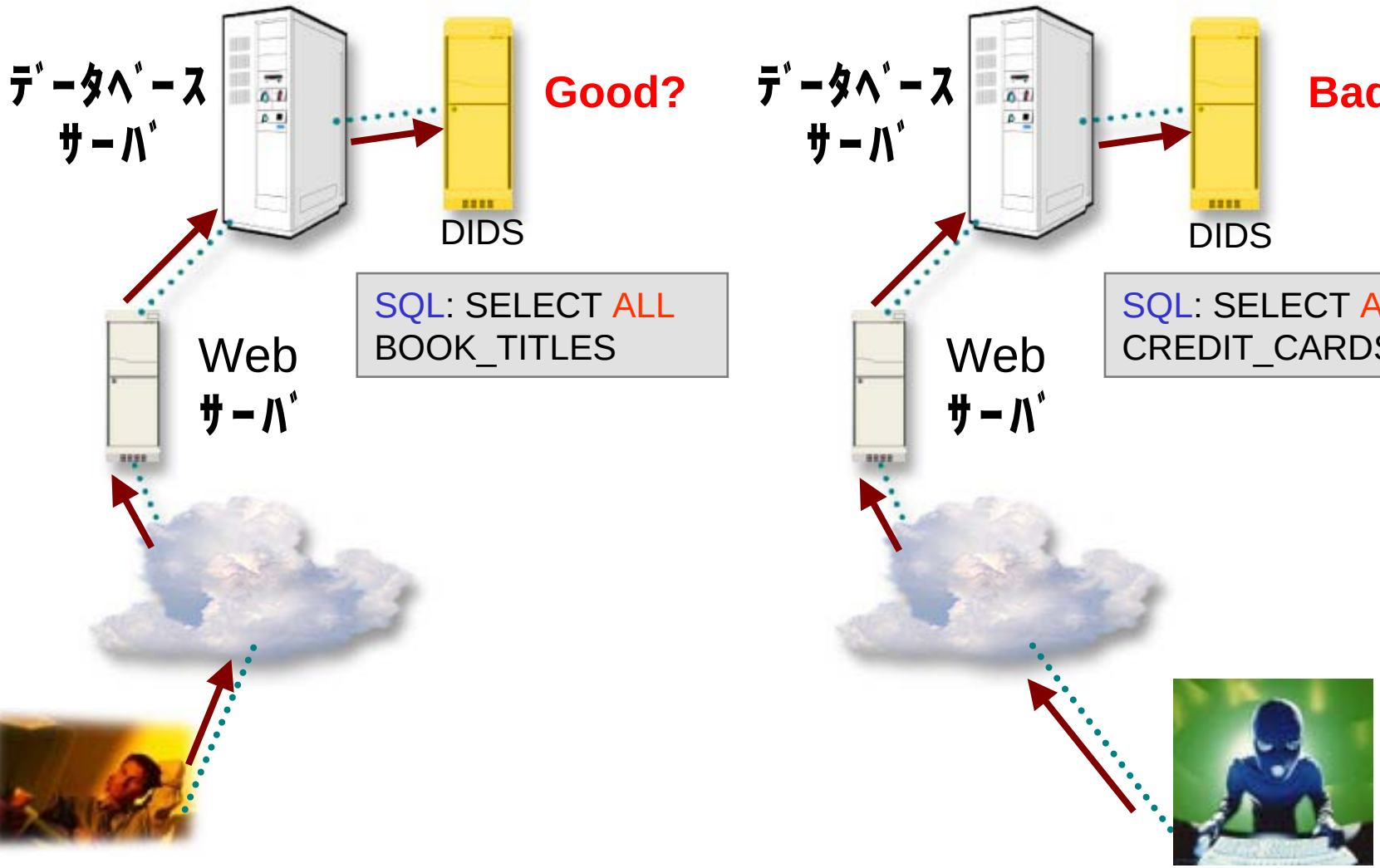
良いプログラム?



アプリケーションセキュリティに対するチャレンジ

- **動機**
  - 攻撃対象のビジネス資産の価値が高くなっている (例, クレジットカード)
  - ホストのセキュリティコンポーネントの分離
  - アプリケーション固有のセキュリティソリューションの不足
- **統合型のセキュリティ防御の必要性**
  - 制限されたサーバ上のCPUとメモリリソース
- **アプリケーション固有のセキュリティソリューション**
  - CRM, ERP, など.
  - データベース
  - e-Mail
  - Webアプリケーション
  - ストレージ

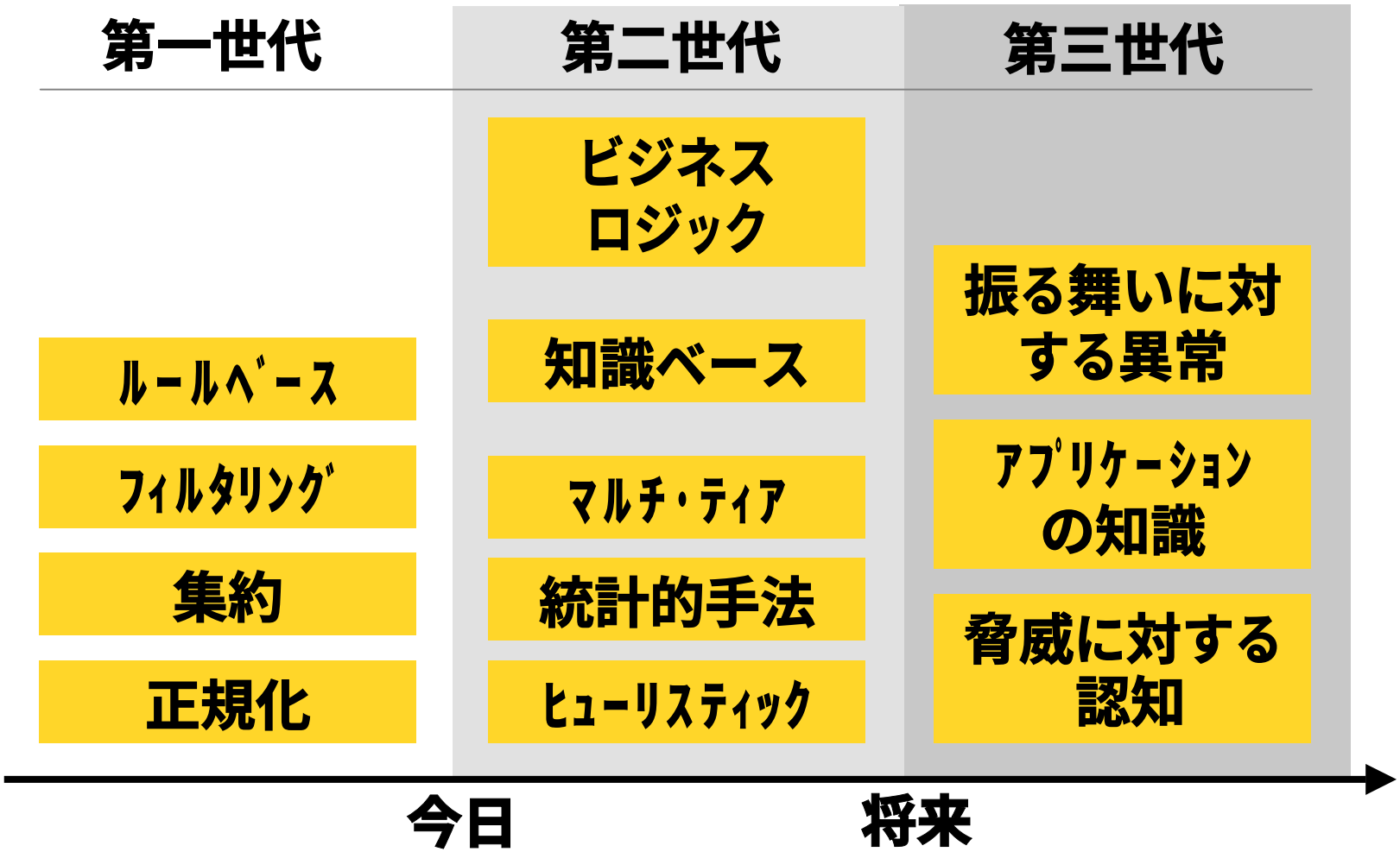
アプリケーションセキュリティの例: データベースIDS



セキュリティ管理に対するチャレンジ

- セキュリティの観点からITの統治をいかに容易にするか
- ユーザ管理とのリンク
- 自動的な修正やビヘイビアブロッキングへの方向
- ビジネスへの影響度の分析
- イベントの相関
  - 脆弱性や有名な脅威に関連した攻撃
  - 根本原因の分析 (例, 攻撃元の追跡)

相関分析の進化


第一世代
第二世代
第三世代
ビジネス
ロジック
振る舞いに対
する異常
ルールベース
知識ベース
フィルタリング
マルチ・ティア
アプリケーション
の知識
集約
統計的手法
脅威に対する
認知
正規化
ヒューリスティック
今日
将来

セキュリティコンテンツは将来ますます重要に

- セキュリティコンテンツはリアクティブまたはプロアクティブ･セキュリティの両方にとって鍵となる
  - アンチウイルス定義ファイル
  - 脆弱性評価のアップデート(例, 新しいパッチ)
  - 侵入検知、侵入防止のためのコンテンツのアップデート
  - 統合型セキュリティ製品のコンテンツのアップデート
  - インシデント管理の知識ルール
  - ポリシー準拠の為のコンテンツのアップデート
  - スパムルール
- Symantec社が持っているLiveUpdateやDeepSight、MSSの技術はこれらのコンテンツの更新のための基礎となる。

まとめ

- 早期警戒システムとセキュリティコンテンツ、自動対応が今後の鍵となる
- 将来の脅威を防御するためには予防的なソリューションが全ての層で重要
- 重要なビジネスプロセスを守るためにアプリケーションレベルのセキュリティが要求される
- セキュリティに対する全体的な視野とコントロールを与える為には包括的な統合的と管理および相関が必要