資料2－2

symantec™

Confidence in a connected world.

最近のセキュリティ動向について

2007/12/5

株式会社シマンテック総合研究所

コンサルティング研究本部

山内　正

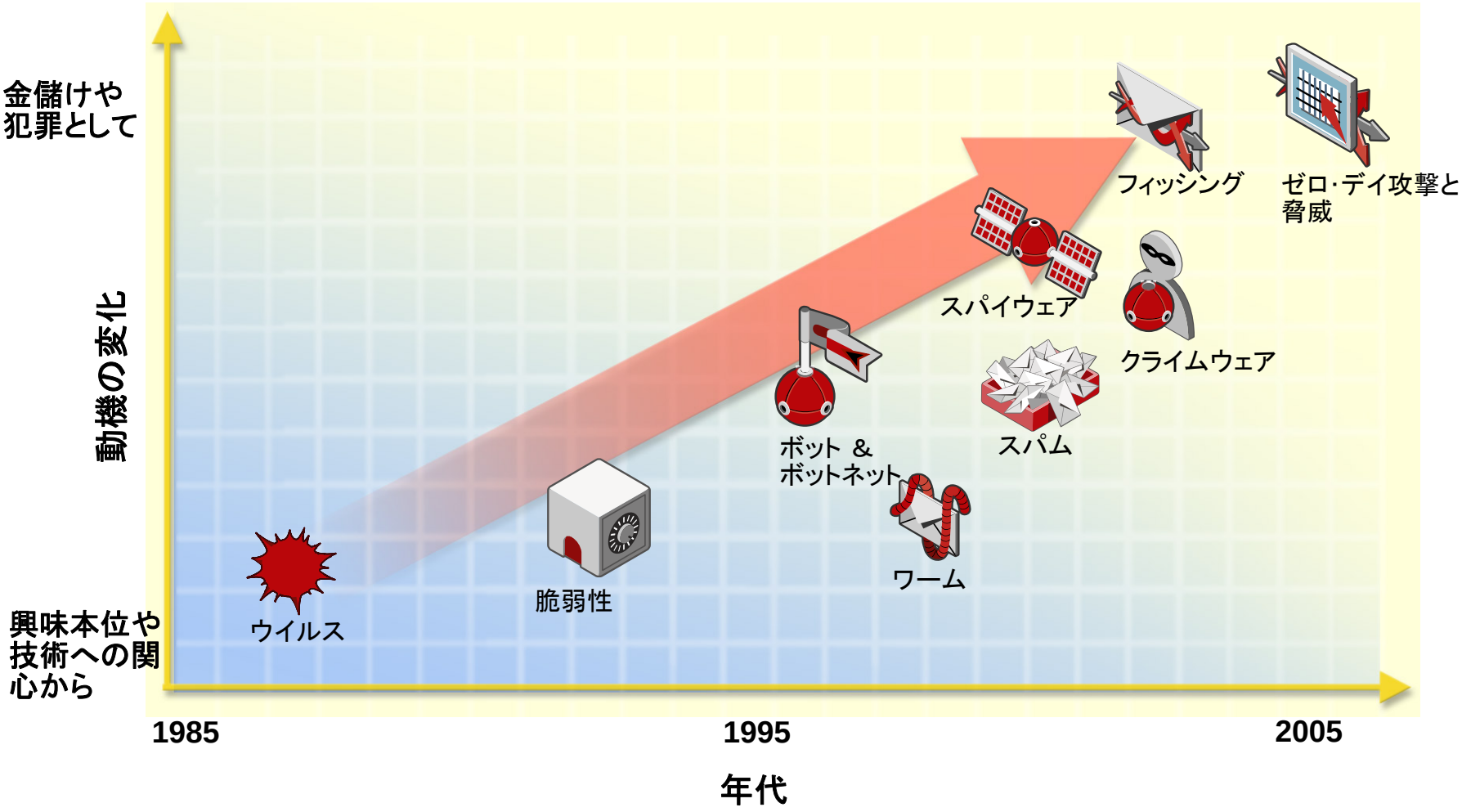
本日のご説明内容

1. これまでの脅威と対処の変遷
2. 現状注力している脅威
3. 必要な対応策、関連技術

本日のご説明内容

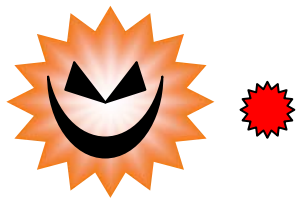
1. これまでの脅威と対処の変遷
2. 現状注力している脅威
3. 必要な対応策、関連技術

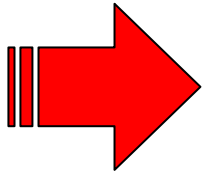
進化し続ける新たな脅威

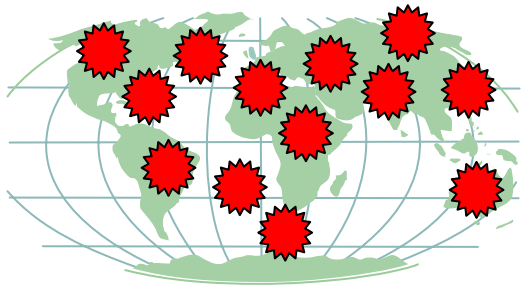


攻撃手法の変化（従来）

従来の攻撃手法







・CodeRed
・Blaster. Worm　等

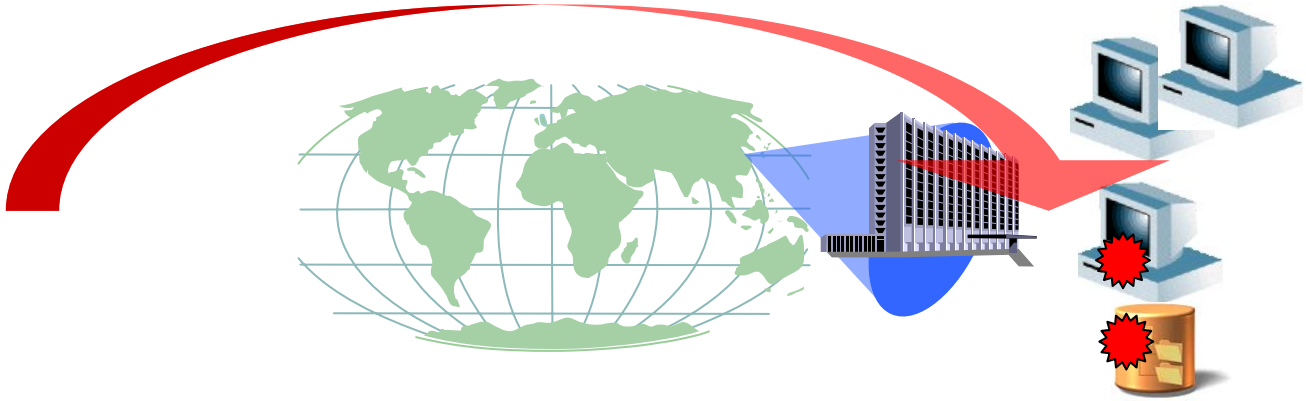
広範囲に及ぶネットワークベースの攻撃手法

・企業システムや、インターネット等のネットワーク自体を不能にする
・被害報告や報道に大きく取り上げられる

興味本位や自己技術の誇示、愉快犯的な発想による無差別的な攻撃

攻撃手法の変化（最近）

最近の攻撃手法



・Trojan. Horse
・Mydoom　等

広範囲から集中の攻撃手法へ

・ある特定企業、業種のシステムから情報を搾取することが目的
・価値のある情報を搾取し、それを金銭的な利益に結びつける

金銭的な利益の追求にシフトしている

（明確な目的がある）

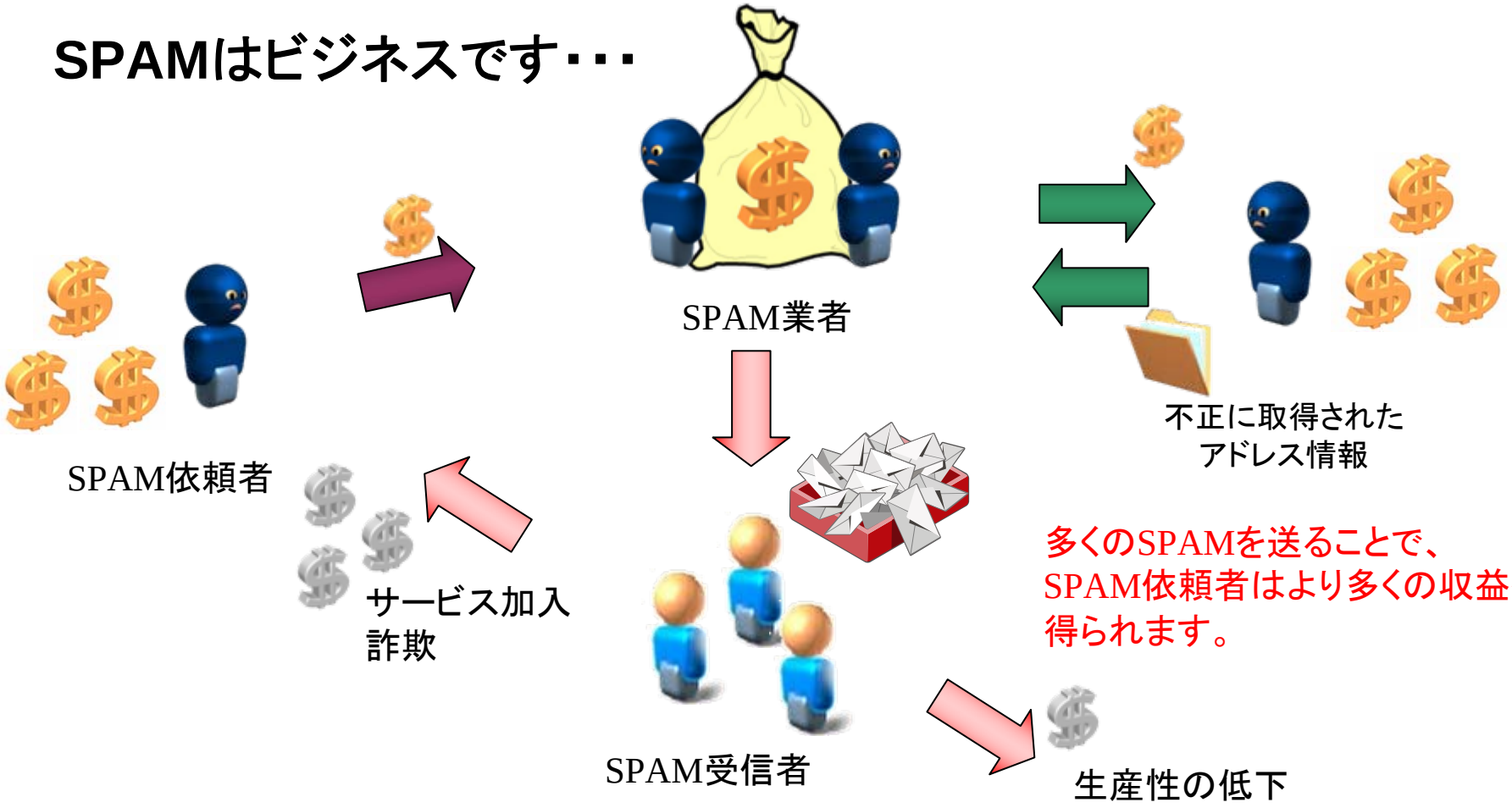
闇市場で売買される情報

- クレジットカード、ID、オンライン支払いサービス、銀行のアカウント、BOTや詐欺ツール等がアンダーグラウンド・エコノミーサーバ上で売り出し中
- クレジットカードが最も多く（22%）、続いて銀行のアカウント（21%）
- Emailのパスワードが銀行のアカウントとほぼ同額で販売

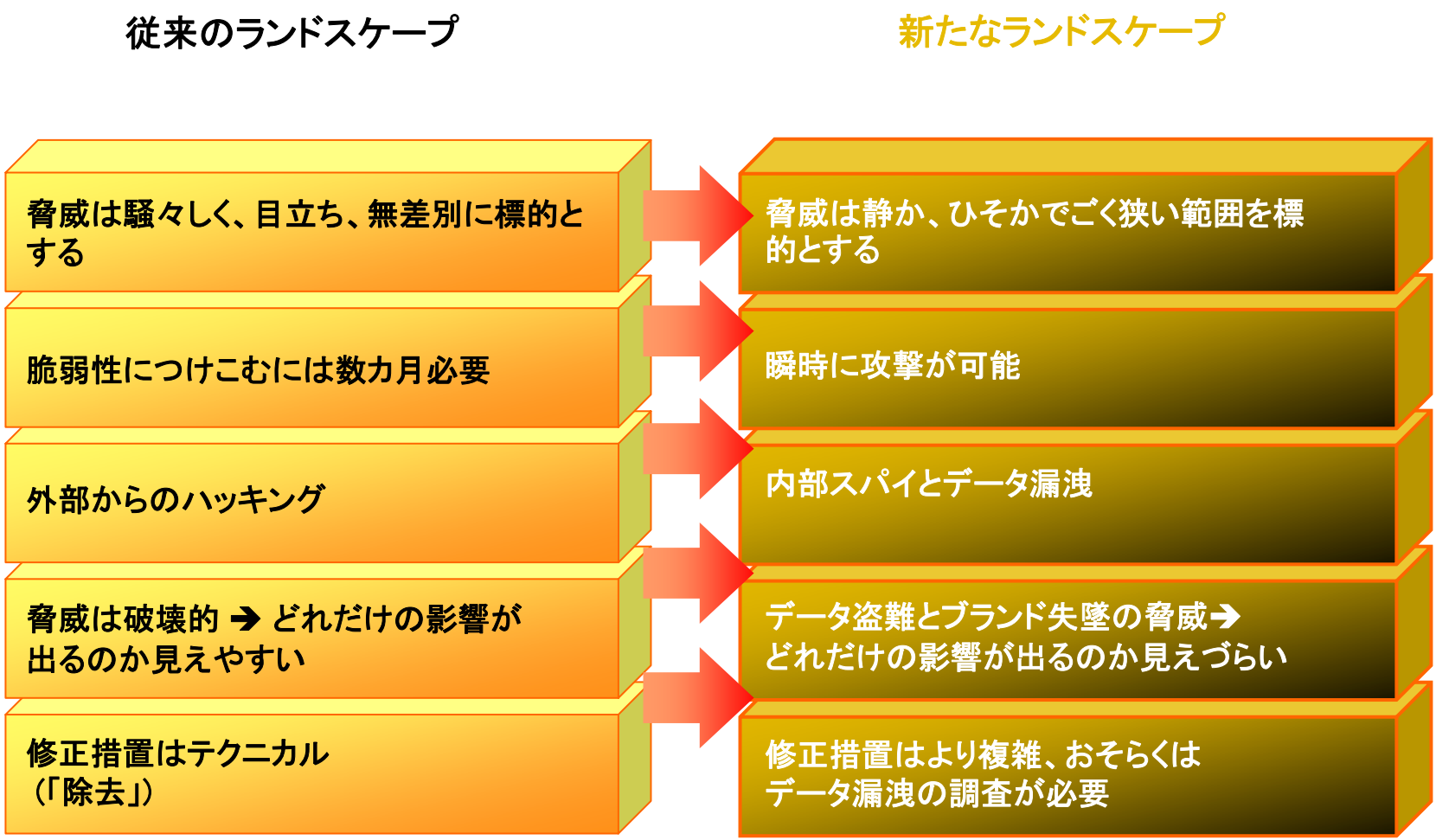
Rank	Item	Percentage	Range of Prices
1	Credit Cards	22%	$0.50–$5
2	Bank Accounts	21%	$30–$400
3	Email Passwords	8%	$1–$350
4	Mailers	8%	$8–$10
5	Email Addresses	6%	$2/MB–$4/MB
6	Proxies	6%	$0.50–$3
7	Full Identity	6%	$10–$150
8	Scams	6%	$10/week
9	Social Security Numbers	3%	$5–$7
10	Compromised Unix Shells	2%	$2–$10

SPAMのビジネス化

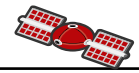
SPAMはビジネスです・・・



ITリスクはますます制御困難に

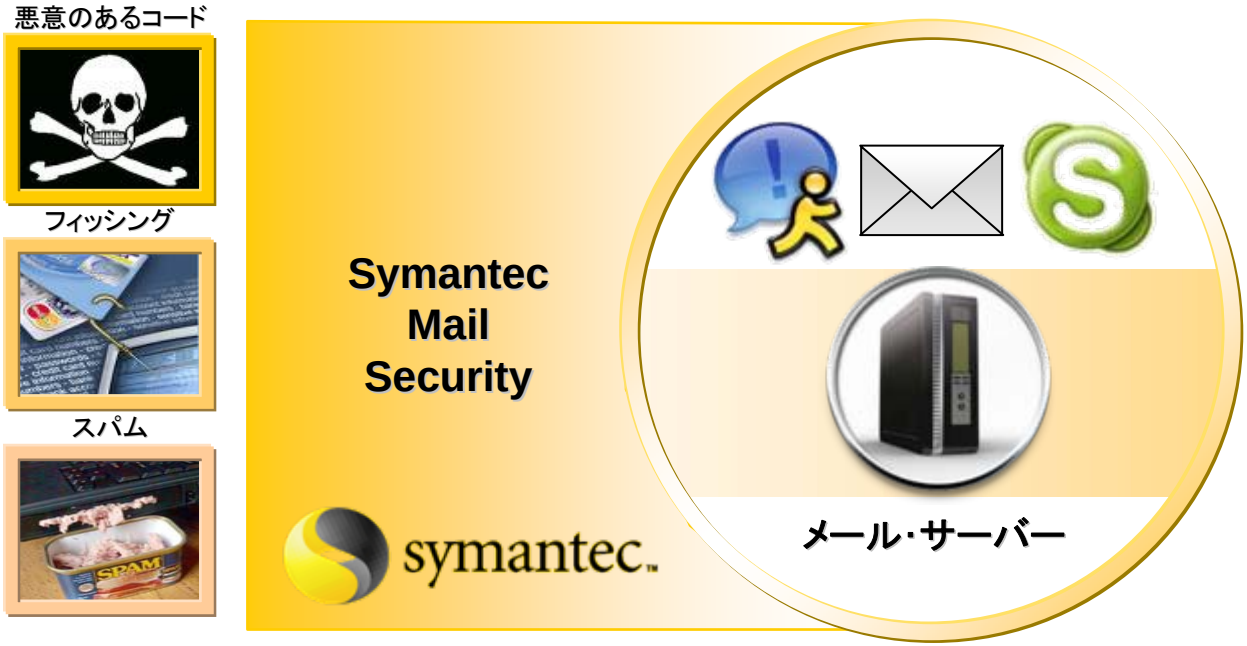


脅威対応の変遷

時　期	主な新機能	関連脅威
２００１年	広告ブロック	 クライムウェア
２００２年	スクリプト遮断	 ワーム
２００３年	ワーム遮断, スパム警告 インスタントメッセージ・スキャン	ニムダ  スパム
２００４年	スパイウェア検出, フィッシング	 スパイウェア
２００５年	インターネットワーム防止	ブラスター サッサー
２００６年	アドウェア，スパイウェアのリアルタイム検出	 フィッシング
２００７年	ルートキット検出, 悪質なトラッキングクッキー，オンラインフィッシング	
２００８年	FW, IDS, IPSの組み込み，ブラウザー脆弱性 リアルタイムボット検出	 ゼロ･デイ攻撃

悪いものは中に入れない

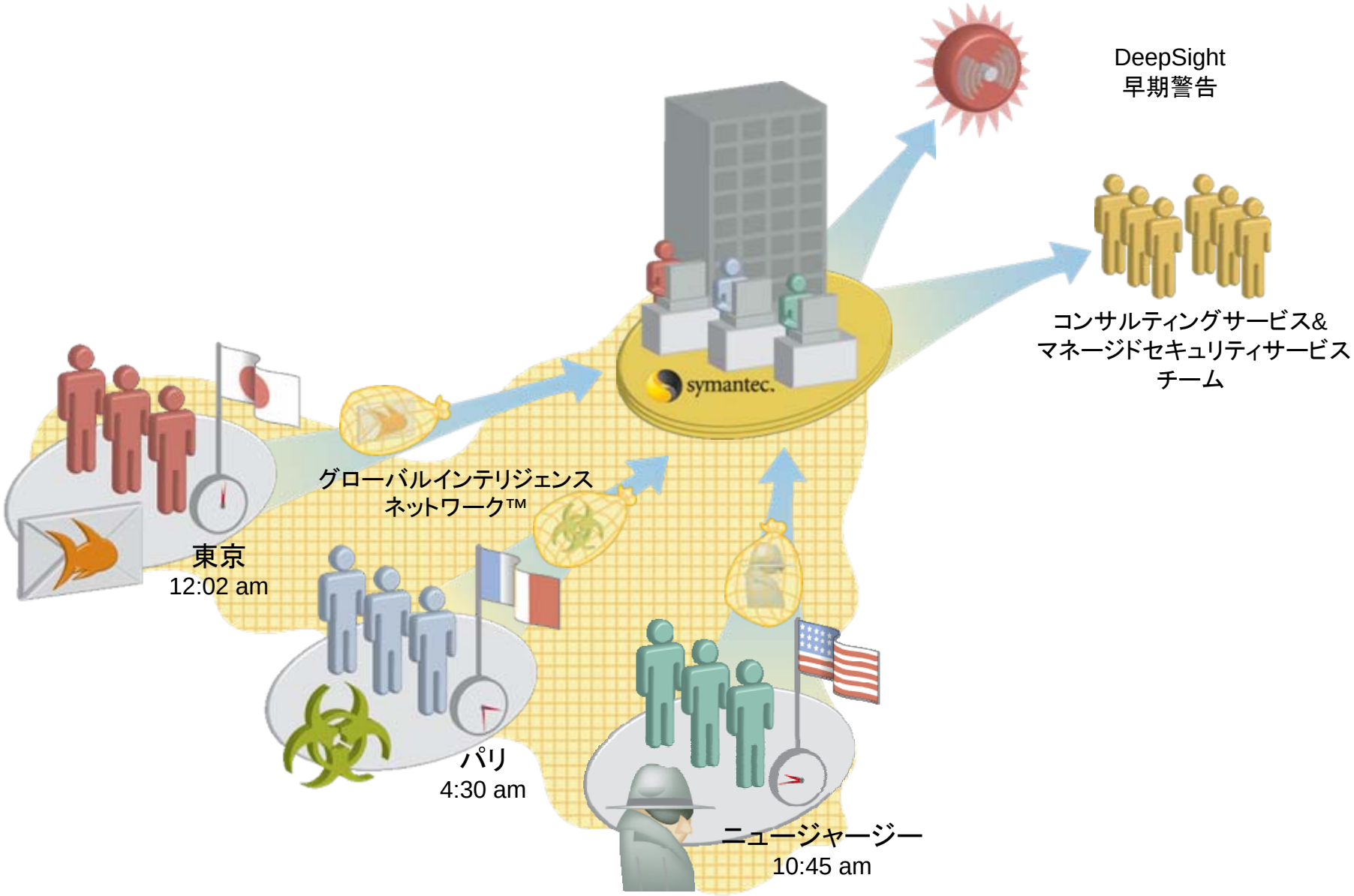
- スパム、フィッシング、ウイルス、ワーム
  - 最も高い発見率 (95%超), 最も低い間違い率 (0.0001%)
  - グローバル・インテリジェンス・ネットワーク上の膨大なセンサーから5-10分おきにアップデート



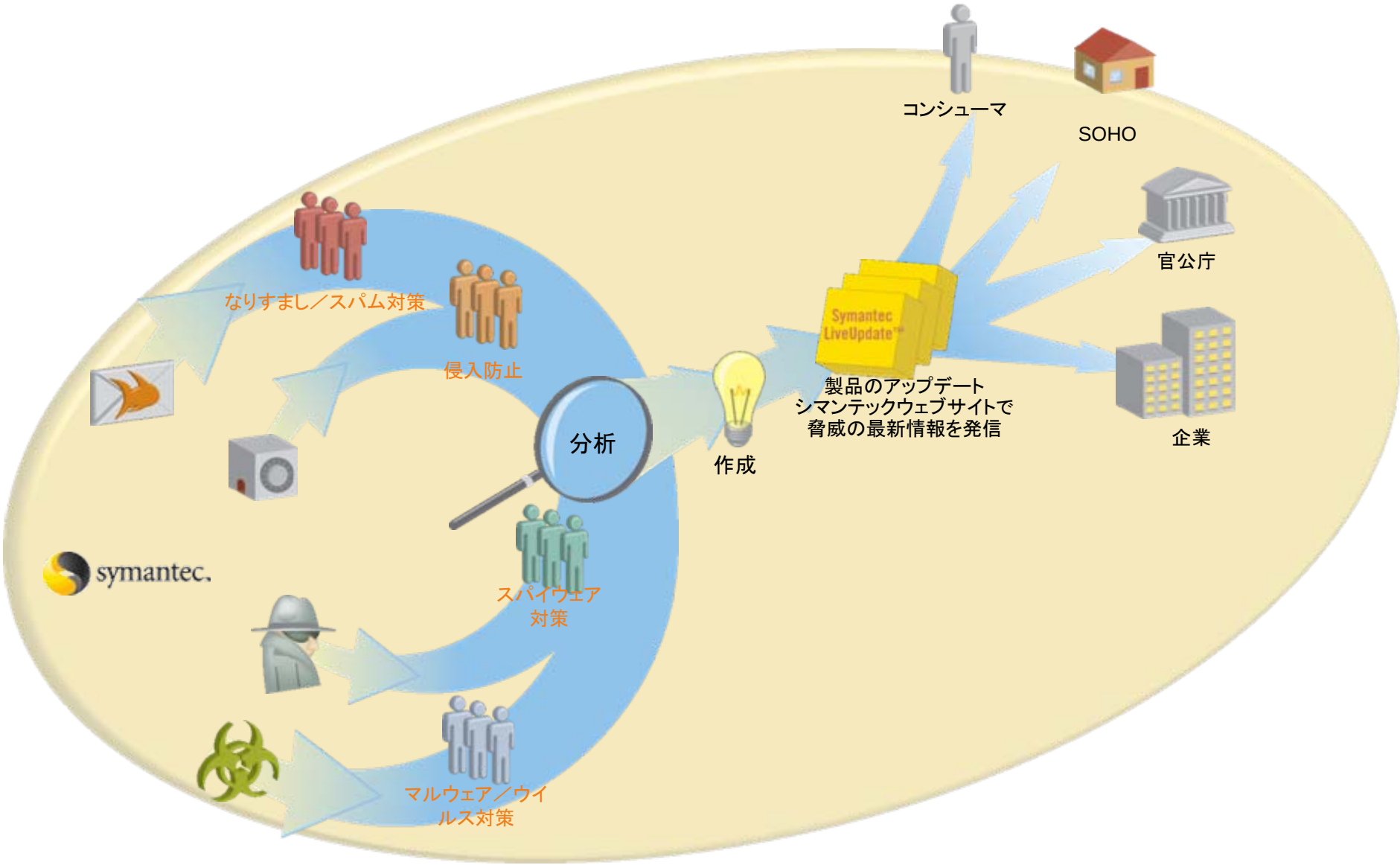
重要なものは外へ出さない

- クレジットカード番号、診療記録、従業員情報
  - 電子メールの本文や添付をスキャン

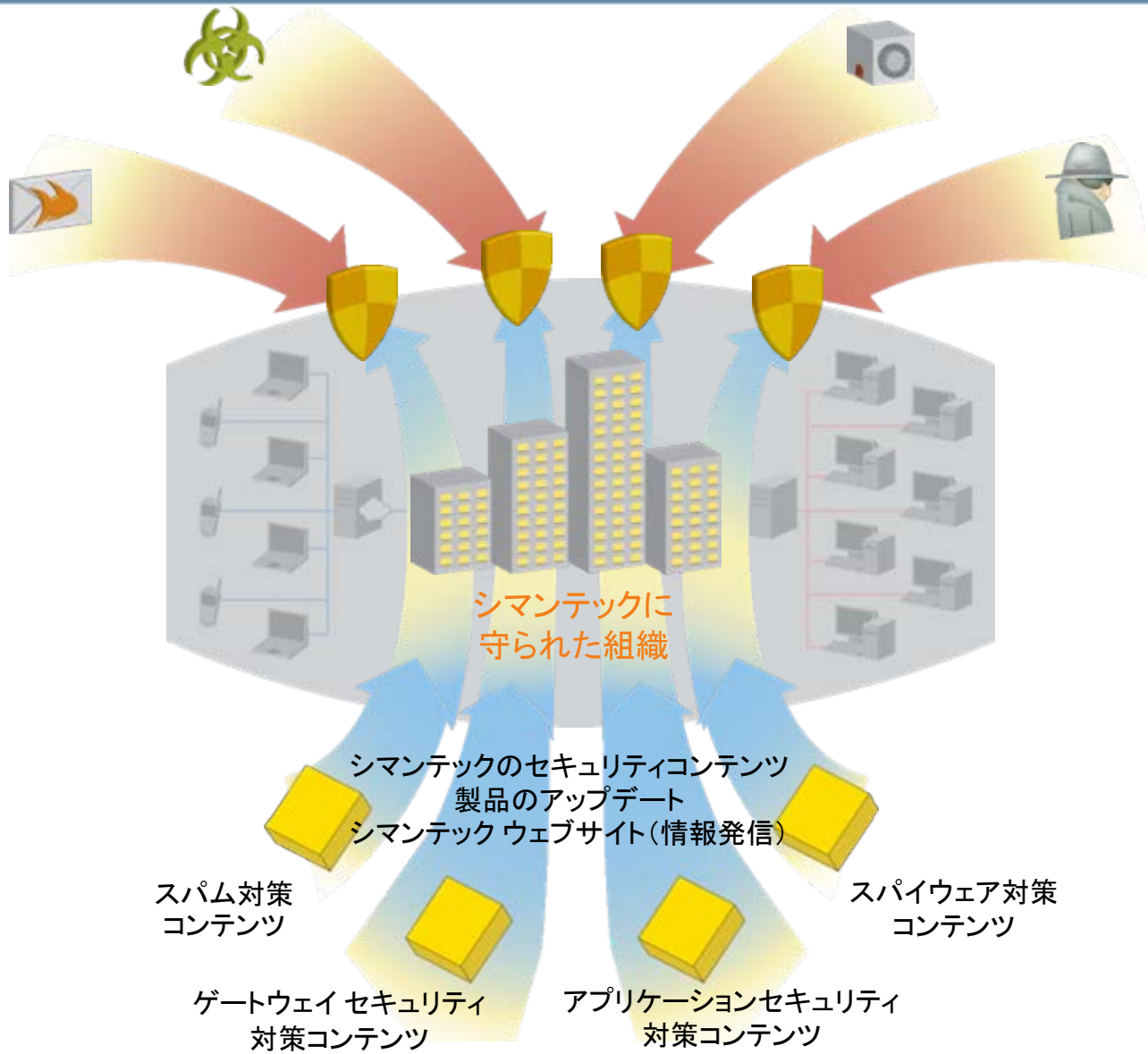
Security Responseの活動:
あらゆる場所で組織的に攻撃を収集



Security Responseの活動:
収集した脅威をセキュリティコンテンツに反映



Security Responseの活動:
セキュリティコンテンツがお客様を攻撃から守る



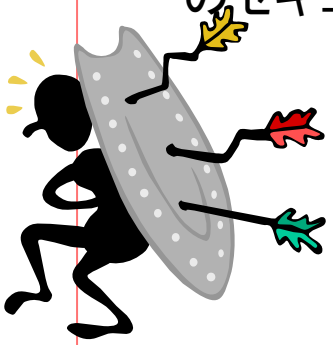
脅威への対策

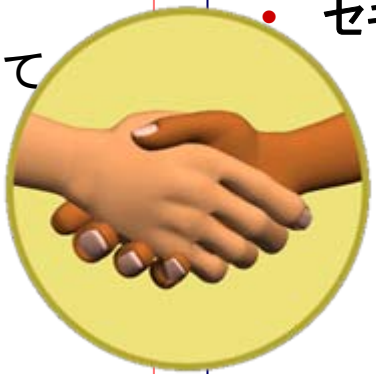
REACTIVE SECURITY

受動的セキュリティ

～脆弱性を攻撃から守る～

- アプリケーションファイアウォール
- パッチあて
- 最新の攻撃や脆弱性に対してのセキュリティ診断と対応





両方が必要！

PROACTIVE SECURITY

能動的セキュリティ

～脆弱性を作らない～

- セキュアアプリケーション開発
- セキュリティを考慮した変更管理
- セキュリティ教育

本日のご説明内容

1. これまでの脅威と対処の変遷
2. 現状注力している脅威
3. 必要な対応策、関連技術

インターネットセキュリティ脅威レポートとは…

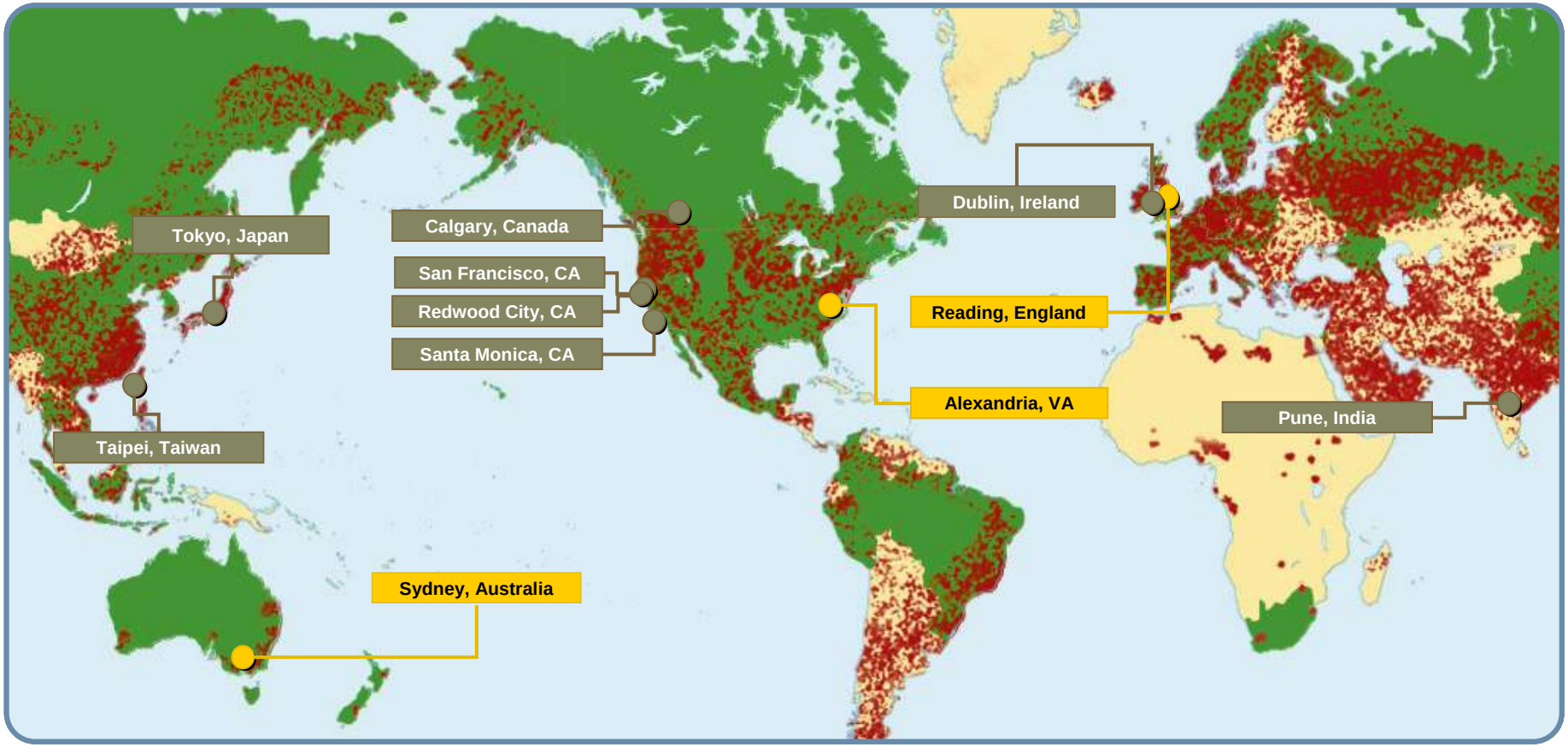
- 記載情報：
  - インターネットセキュリティ活動と動向について総合的な分析
  - 6か月毎に発刊
  - 今日のインターネットセキュリティ環境についての完全な概観
  - 攻撃者の手法や傾向の分析
  - 最新のトレンドと情報の詳細
    - インターネット攻撃
    - 発見／悪用された脆弱性
    - 悪意のあるコード
    - フィッシング
    - スパム
  - インターネットセキュリティの今後のトレンド予想

http://www.symantec.com/content/ja/jp/enterprise/white_papers/istr12_wp_200709.pdf

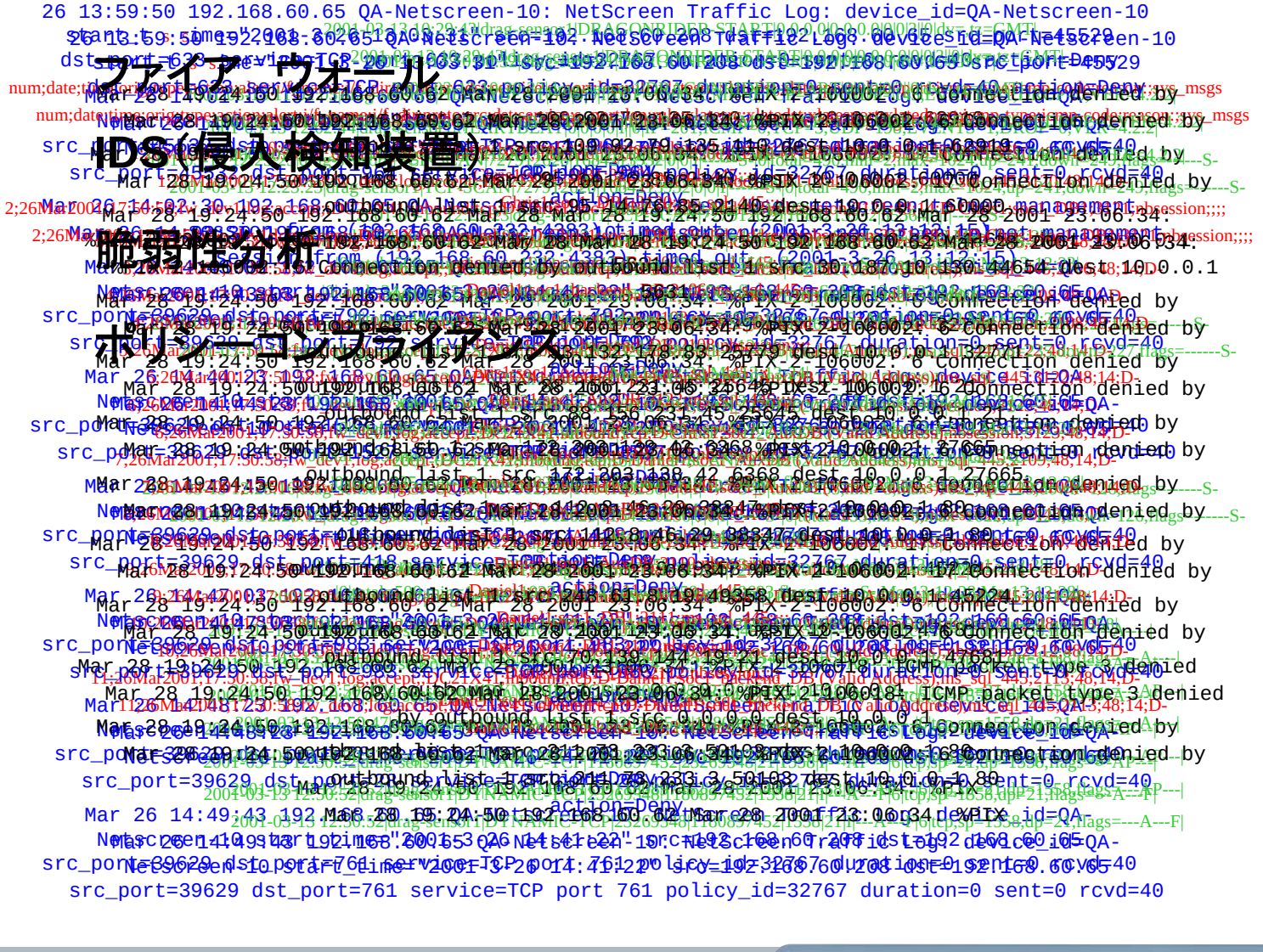
グローバル・インテリジェント・ネットワーク

3 Symantec SOCs + 74 Symantec Monitored Countries + 40,000+ Registered Sensors in 180+ Countries + 8 Symantec Security Response Centers

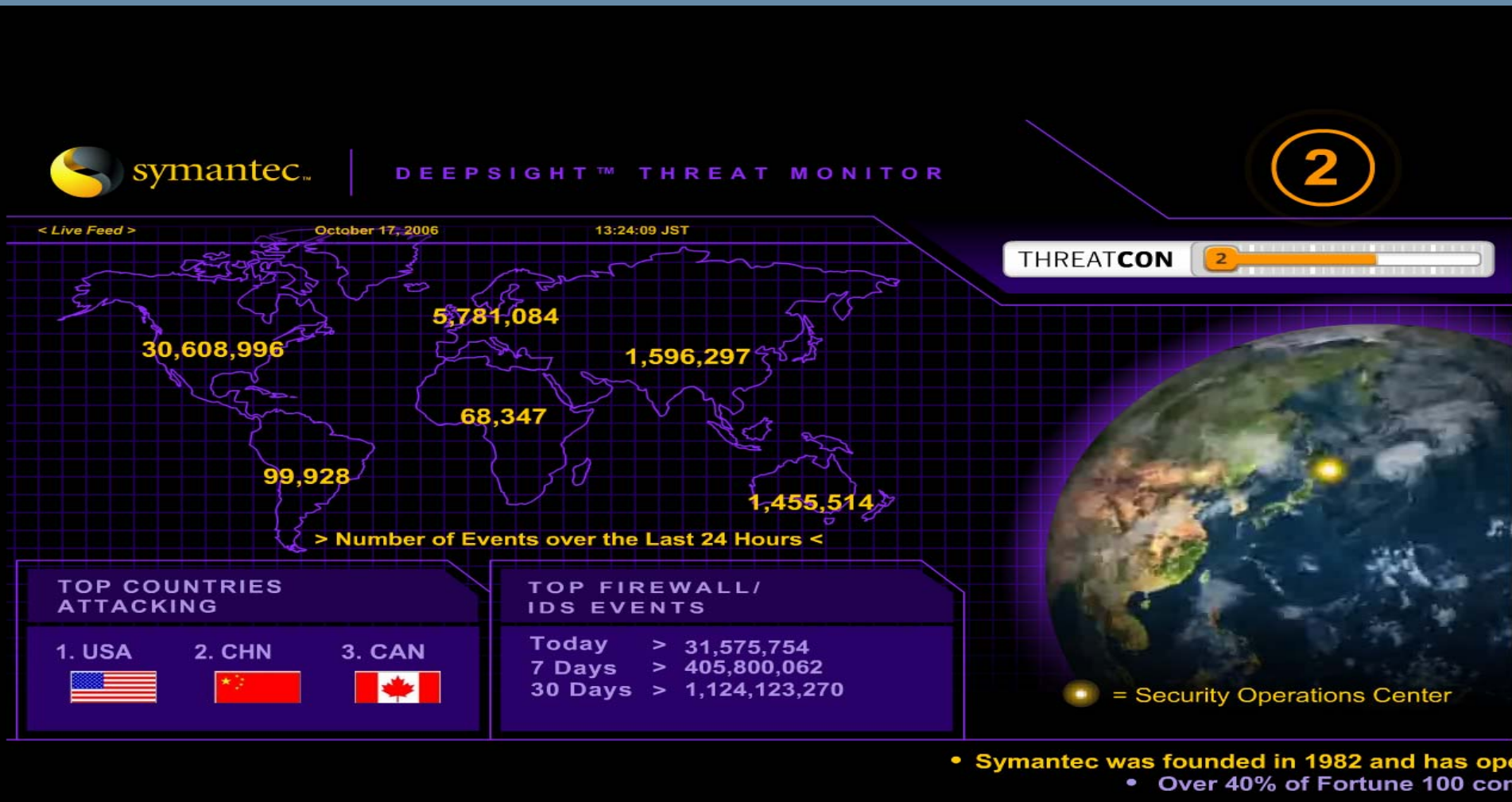
>6,200 Managed Security Devices + 120 Million Systems Worldwide + 30% of World's email Traffic + Advanced Honeypot Network



実際に攻撃として送付されてくる大量のデータ



脅威管理システム



攻撃の傾向

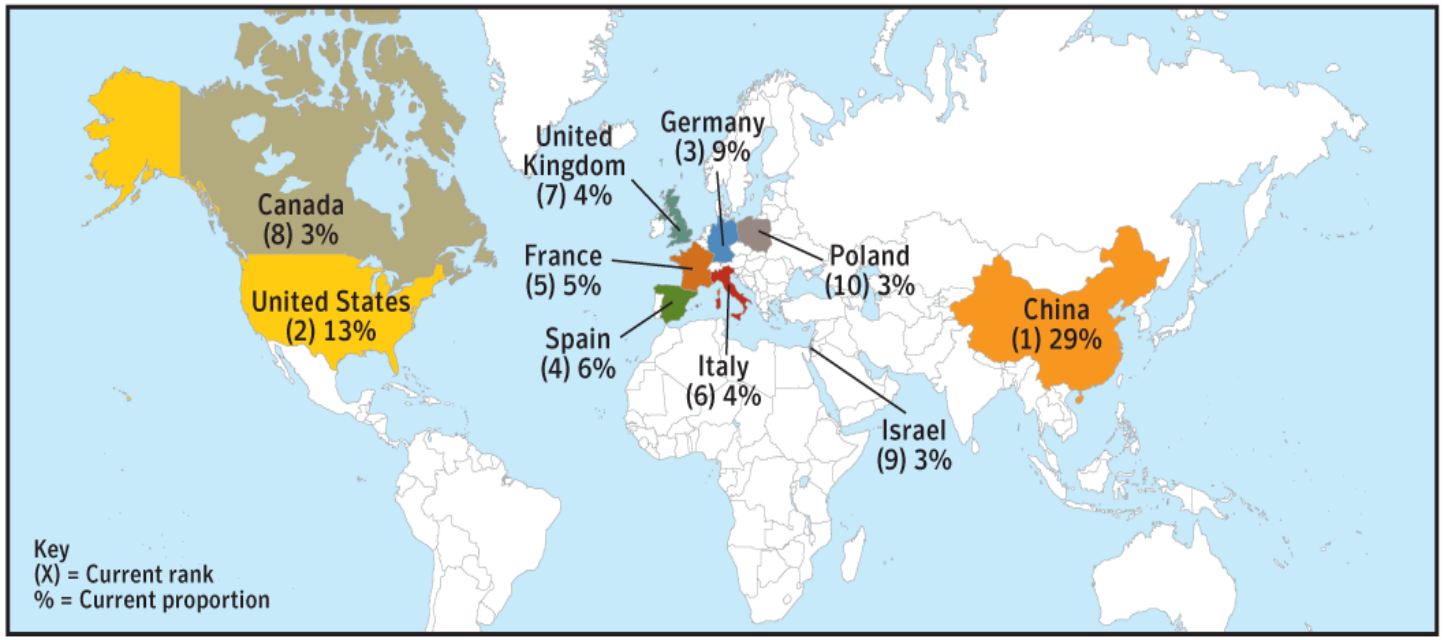
- 2007 年上半期には、国別では米国を標的としたサービス拒否（DoS）攻撃が最多となり、世界全体の 61% を占めた。
- 米国は 検出された世界全体での攻撃発信数の 25% を占め、国別で第 1 位にランク。
- インターネットユーザー 1 人あたりの国別マリシャスアクティビティ数はイスラエルが最多となり、カナダと米国がこれに続いている。
- マリシャスアクティビティ全体の 4% が、フォーチュン 100 社に含まれる企業の登録 IP スペースから発信されていた。
- 今期、1 日平均 52,771 台のアクティブなボット感染コンピュータを検出したが、これは前期の検出数に対して 17% の減少。
- 国別のボット感染コンピュータ数では、中国が全体の 29% を占めて最多となった。
- ボットのコマンドアンドコントロールサーバー数については、米国が世界全体の 43% を占めて国別で最多。
- ボット感染コンピュータの都市別台数については、北京が世界全体の 7% を占めて最多。
- 2007 年上半期におけるボット感染コンピュータの平均寿命は 4 日となり、2006 年下半期の 3 日よりも長くなっている。
- ホームユーザーを狙った標的特定型攻撃が 全体の 95% を占めて最多の攻撃対象カテゴリとなった。

攻撃の上位発信国

ランク	前期のランク	国名	全体に占める割合	前期での全体に占める割合	悪意のあるコードのランク	スパムゾンビのランク	コマンドアンドコントロールサーバーのランク	フィシングWebサイトのランク	ボットのランク	攻撃のランク
1	1	米国	30%	31%	1	1	1	1	2	1
2	2	中国	10%	10%	2	3	5	18	1	2
3	3	ドイツ	7%	7%	7	2	2	2	3	3
4	5	英国	4%	4%	3	15	6	3	7	5
5	4	フランス	4%	4%	9	7	12	6	5	4
6	7	カナダ	4%	3%	6	31	3	7	8	7
7	8	スペイン	3%	3%	10	10	22	13	4	6
8	10	イタリア	3%	3%	5	6	8	12	6	8
9	6	韓国	3%	4%	26	8	4	10	13	12
10	11	日本	2%	2%	4	20	13	8	16	10

ボットネットワーク

- 2007年上半期、一日平均52，771のアクティブなBOTを観測。これは2006年の前期から17%の減少。世界規模でのBOT感染コンピュータも5，029，309台となり昨年から17%の減少。
- コマンドコントロールサーバも今期は4622台となり3%の減少。米国が今期もコントロールサーバ比率43%と高く、前期よりも3%増加。
- 米国でのBOT感染数が減っている一方で中国では29%に上昇。しかし、昨年にくらべ中国でのBOT成長率も下がっている。



フィッシングサイトホスト国TOP10

- フィッシングサイトとして知られているサイトの59%が米国にホスティングしている。続いてドイツ（6%）、イギリス（3%）となっている
- 米国はウェブホスティングプロバイダが多いためNo1となっている。（特にフリーのプロバイダが多い）
- 今期のフィッシングサイトの増加の原因は北米でのTrojanの増加が原因と推測される

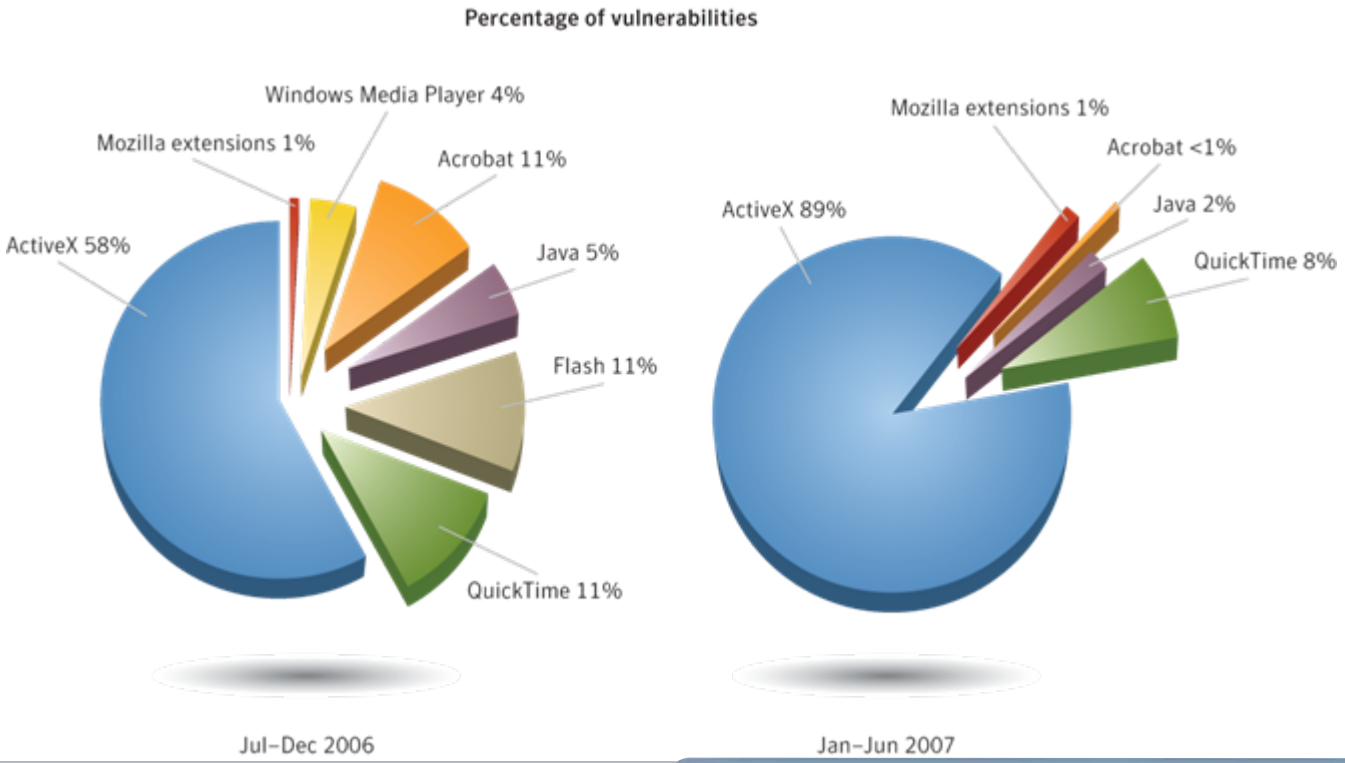
Rank	Previous Rank	Country	Current Period	Previous Period
1	1	United States	59%	46%
2	2	Germany	6%	11%
3	3	United Kingdom	3%	3%
4	10	Netherlands	2%	2%
5	11	Russia	2%	2%
6	4	France	2%	3%
7	7	Canada	2%	2%
8	5	Japan	2%	3%
9	8	China	1%	2%
10	6	Taiwan	1%	3%

脆弱性の傾向

- 2007 年上半期に記録した脆弱性の件数は 2,461 件となり、2006 年下半期との比較では 3% の減少となった。
- 今期中に公表された脆弱性について、全体の 9% を「高リスク」カテゴリ、51% を「中リスク」カテゴリ、40% を「低リスク」カテゴリに分類した。2006 年下半期には、新たに公表された脆弱性の 4% を「高リスク」カテゴリ、69% を「中リスク」カテゴリ、27% を「低リスク」カテゴリに分類している。
- 脆弱性の 61% が Web アプリケーションに影響を及ぼす脆弱性であったが、この割合は 2006 年下半期の 66% から低下している。
- 脆弱性の 72% が「エクスプロイト（悪用）が容易」な脆弱性であった。この割合は、前期の 79% から低下している。
- Hewlett Packard HP-UX® を除くすべてのオペレーティングシステムのパッチ開発平均期間が 2006 年下半期よりも短縮された。
- 企業ベンダーが脆弱性によって危険にさらされる平均期間は、55 日であった。これは、2006 年下半期の平均期間である 47 日よりも長くなっている。
- Apple Safari の「危険にさらされる平均期間」が 3 日となり、今期の調査対象となったブラウザの中で最短となった。2006 年下半期における Web ブラウザの「危険にさらされる平均期間」については、Mozilla が 2 日で最短であった。
- Web ブラウザのプラグインについて 237 件の脆弱性を記録した。これは、2006 年下半期の 74 件および 2006 年上半期の 34 件と比較すると、大幅な増加である。

脆弱性の傾向:ブラウザ・Plug-Inの脆弱性

- ウェブ・ブラウザのPlug-inにある脆弱性は悪意あるコードを含むソフトウェアをインストールするために悪用されることが多い。
- 前期にドキュメント化されたPlug-Inの脆弱性数は108だったが、今期は237に増加
- ブラウザ・Plug-Inの脆弱性の89%がIEのActiveXコンポーネントに関連するもので、前期の58%からかなり増加。

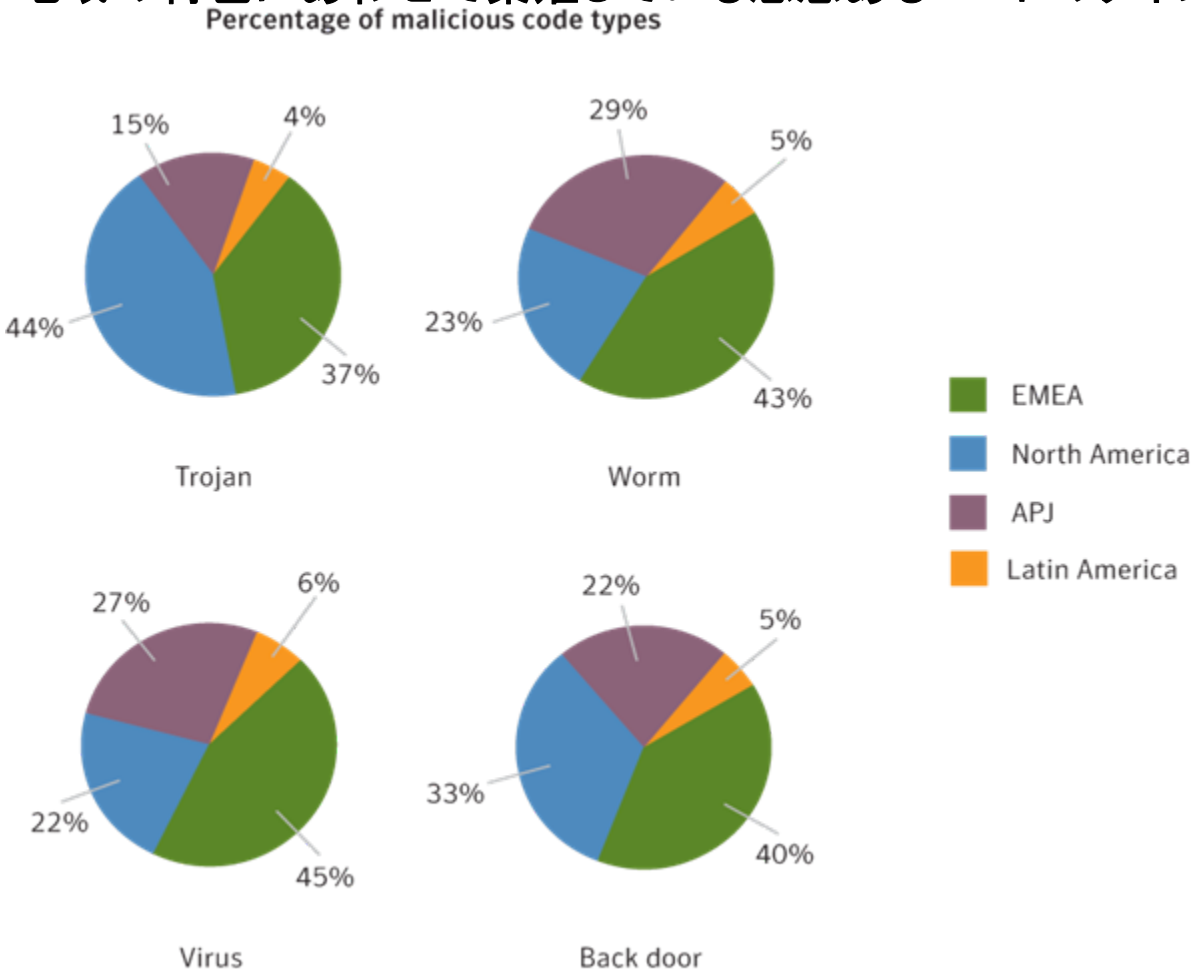


悪意のあるコードの傾向

- 2007 年上半期には、212,101 種の新たな悪意のあるコードの脅威がシマンテックに報告された。この数値は、2006 年下半期の数値に対して 185% の増加。
- 報告件数上位 50 種の悪意のあるコードの 54 % をトロイの木馬が占め、この割合は 2006 年下半期の 45% から増加。
- 推定感染数では、上位 50 種の悪意のあるコードサンプルの 73% をトロイの木馬が占め、この割合は前期の 60% から増加。
- ワーム感染の 43% がヨーロッパ、中東、およびアフリカ（EMEA）地域で報告された。
- トロイの木馬の報告件数全体の 44% を北米が占めた。
- キーストロークロギングの悪用による脅威は、機密情報に対する脅威の 88% を占め、バックドア設置などによるリモート操作などの脅威も、全体の 88% を占めている。
- 悪意のあるコードの 46% が SMTP を媒介として感染を拡大していたため、最も広く使用される感染拡大メカニズムが SMTP となった。
- 今期の上位 10 種の段階型ダウンローダの内訳は、8 種がトロイの木馬で 2 種がワームとなった。
- ダウンロードされた上位 10 種のコンポーネントの内訳は、7 種がトロイの木馬で 3 種がバックドアであった。
- オンラインゲームを標的とする悪意のあるコードは、推定感染数上位 50 種の悪意のあるコードサンプルの 5% を占めた。

脅威のローカリゼーション

- 脅威は特定の地域、国にあわせて作成されている
- その地域の特色にあわせて繁殖している悪意あるコードのタイプも変わる



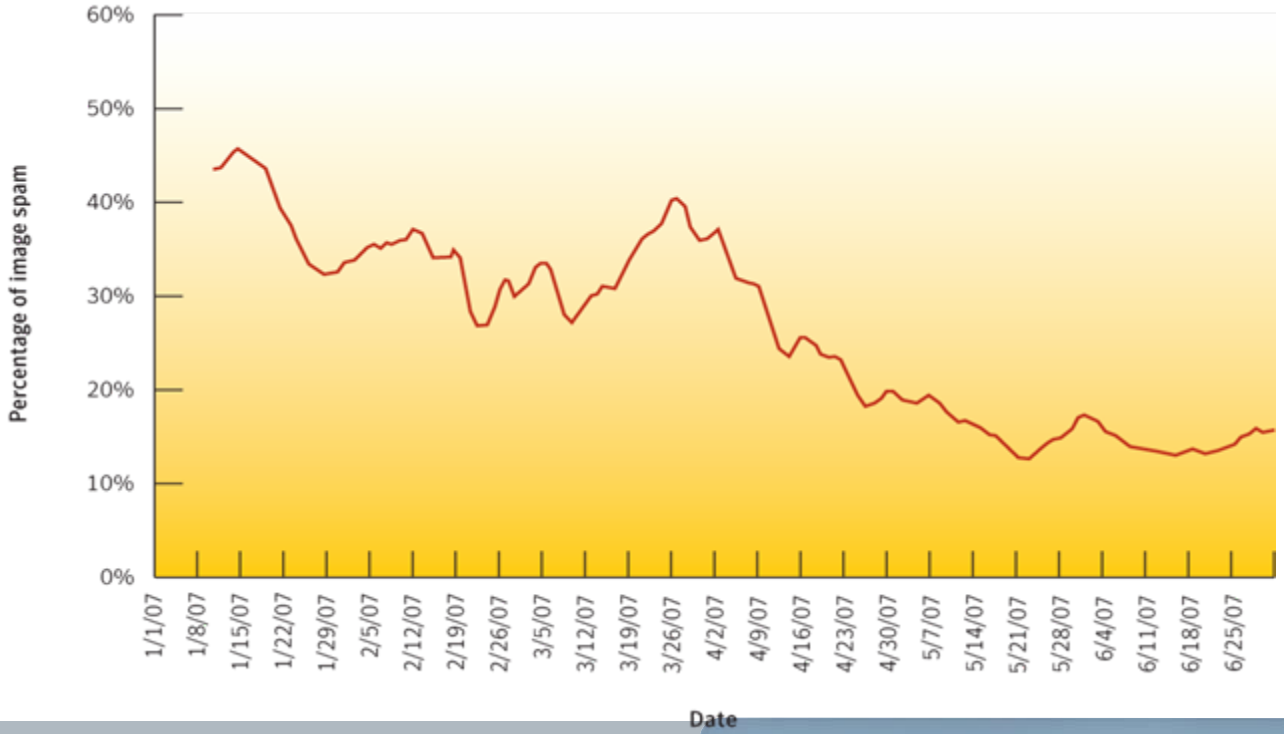
スパム発信国

- 全スパム中47%が米国を起源。この数は前期のレポートの44%から増加傾向にある。EU内の不特定国が7%と続き、さらに中国が4%。
- スパムの発信国はスパムゾンビ、または合法のEmailサーバからきているスパムを含む。スパムゾンビとはBOTやワーム、Trojanに感染した結果踏み台になったコンピューターで、スパムの発信元からスパムの拡大を手助けしている。
- スパムゾンビによる展開数の割合は、米国が10%、中国は9%、ドイツ9%となり、またスパムゾンビ国TOP10のうち5つがEMEA地域の国となっている

Top Ten Countries of Spam Origin	Jan–Jun 2007	Jul–Dec 2006
United States	47%	44%
Undetermined EU Countries	7%	7%
China	4%	6%
United Kingdom	4%	3%
Japan	4%	3%
South Korea	3%	3%
Taiwan	3%	1%
Poland	3%	3%
Germany	2%	2%
Switzerland	2%	1%

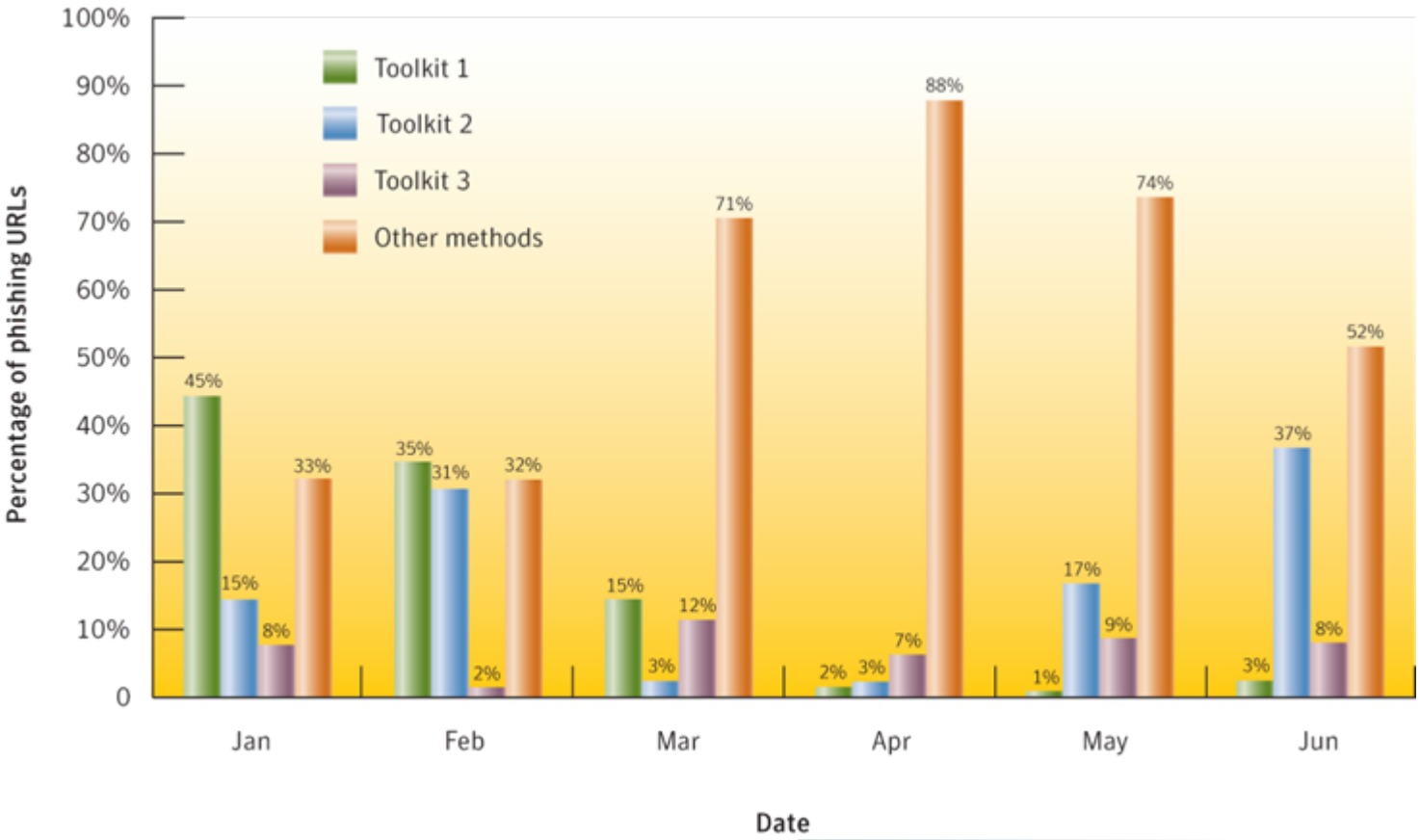
スパム：画像スパム

- 2007年上期においてブロックされたスパム中27%が画像スパム
- 今年の開始時点では全スパム中約50%を占めており、これはユーザーにイメージスパムメッセージを送信するPeacomm Trojanが関わっている可能性がある
- Spamalot作戦（株価操作スパムからの投資家保護作戦）が始まった後、4月始めころから徐々に数は減少している. そのため4月までの数は 株価操作スパムの詐欺に関連



攻撃手法のプロフェッショナル化

- 一般製品の開発サイクルにあわせ、アタッカー間でも攻撃手法のプロフェッショナル化、標準化が進んでいる。
- フィッシングツール、MPackの利用増加



今後の監視対象

1　バーチャルワールドにおける悪意のあるコード

- PVW（常駐仮想世界）におけるアバターを介した交流
- 仮想通貨を取引するための為替取引所
- ツールを用いたダウンロード時に悪意のあるコードもダウンロード
- オンラインゲームチャンネル経由のフィッシング、スパムメール

2　自動検出回避プロセスの高度化

- 検出回避テクニックの進化　＞亜種検出機能の向上
  - ポリモーフィック
    - 複製時に自らのバイトパターン変更
  - メタポリモーフィック
    - 複製時にコード自体を変更
- ウイルス配布サーバの秘匿、保護
  - サンプルウイルスの入手を遅らせることによる感染可能性拡大

3　ボット使用方法の多様化

- 新しいコードや機能のダウンロード
- DOS攻撃、スパム、フィッシング
- スパイウェア、アドウェア、ミスリーディングアプリの配布

ボットネット

本日のご説明内容

1. これまでの脅威と対処の変遷
2. 現状注力している脅威
3. 必要な対応策、関連技術

エンドポイントセキュリティ

Endpoint Protection 11.0

Antivirus & Antispyware

- ウイルス
- スパイウェア
- ルートキット

の検出、ブロック、削除

Proactive Threat Protection

- ビヘイビアベースのマルウェア検出

ポリシーによる

- 外部デバイス接続制御
- アプリケーション制御

Network Threat Protection

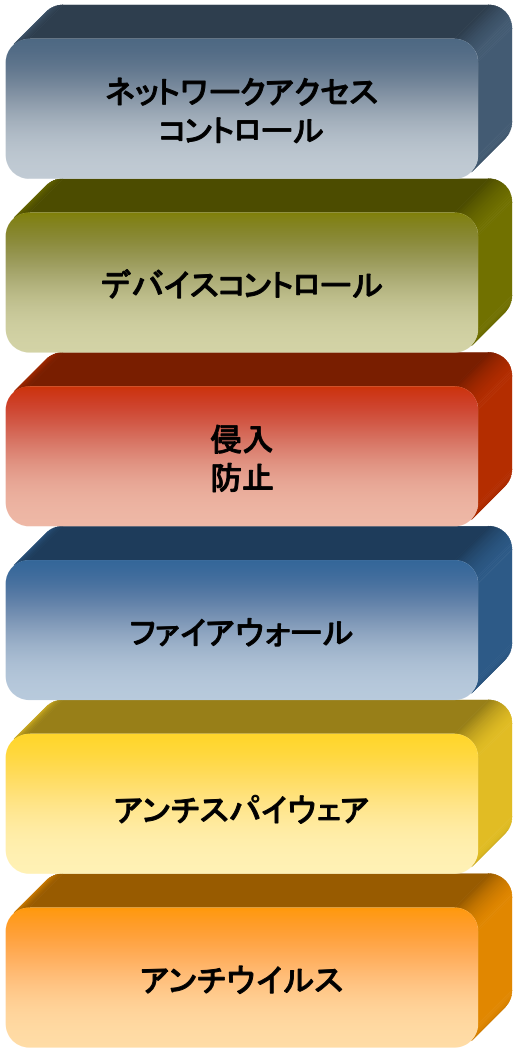
- ネットワーク型の脅威の検出とブロック
- クライアントファイアウォール
- 脆弱性ベースのIPS

Network Access Control

- 不正なエンドポイントの接続制御

Symantec Network Access Control 11.0

エンドポイントセキュリティ



- 単一のエージェントでNACにも対応可能
- エンドポイントプロテクションに加えて、エンドポイントコンプライアンスを実現

- エンドポイントでのデータ漏洩を防ぐ、デバイスコントロール（Sygate）
- MP3 プレーヤー、米国B スティックなどから保護

- ビヘイビアベースの侵入防止（Whole Security）
- ネットワークトラフィック検査により、脆弱性ベースの保護を追加

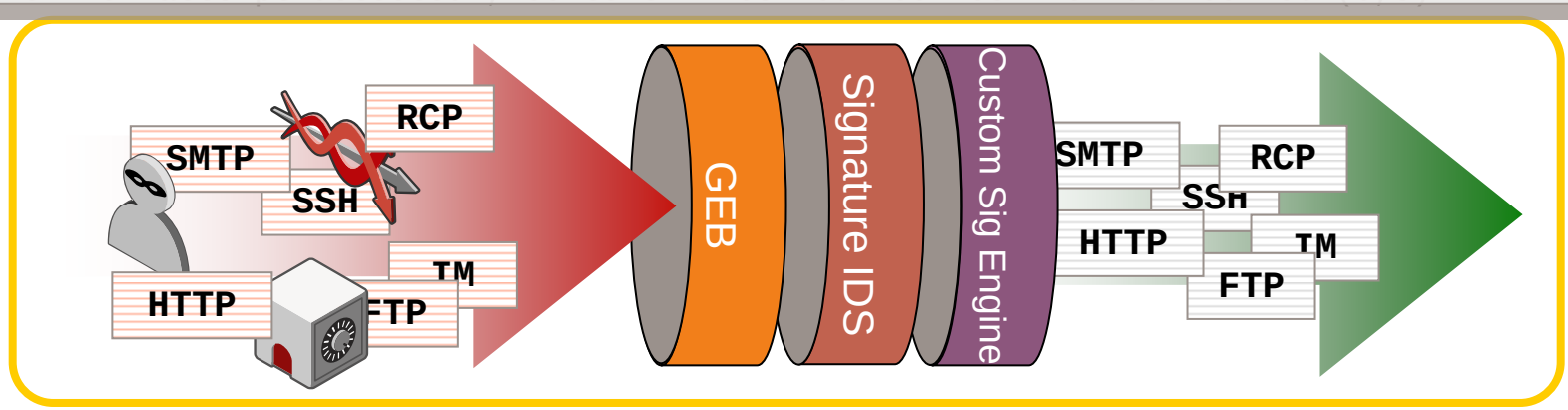
- 業界で最も優れたマネージドデスクトップファイアウォール[4]
- 適応ポリシーによって、他を凌駕する位置情報パックをリード
- Sygate 製品

- ルートキット検出／削除で他社を圧倒する、卓越したアンチスパイウェア[7]
- Raw Disk Scan スキャニングテクノロジー（Veritas）

- 世界をリードするアンチウイルスソリューション[1]
- どのベンダーよりも多く Vir米国 Bulletin の認証（30）を取得[8]

IPSポリシー

```
rule tcp, tcp_flag&ack, daddr=$LOCALHOST, msg="[182.1] RPC DCOM buffer
overflow attempt detected", content="¥x05¥x00¥x00¥x03¥x10¥x00¥x00¥x00"(0,8)
```



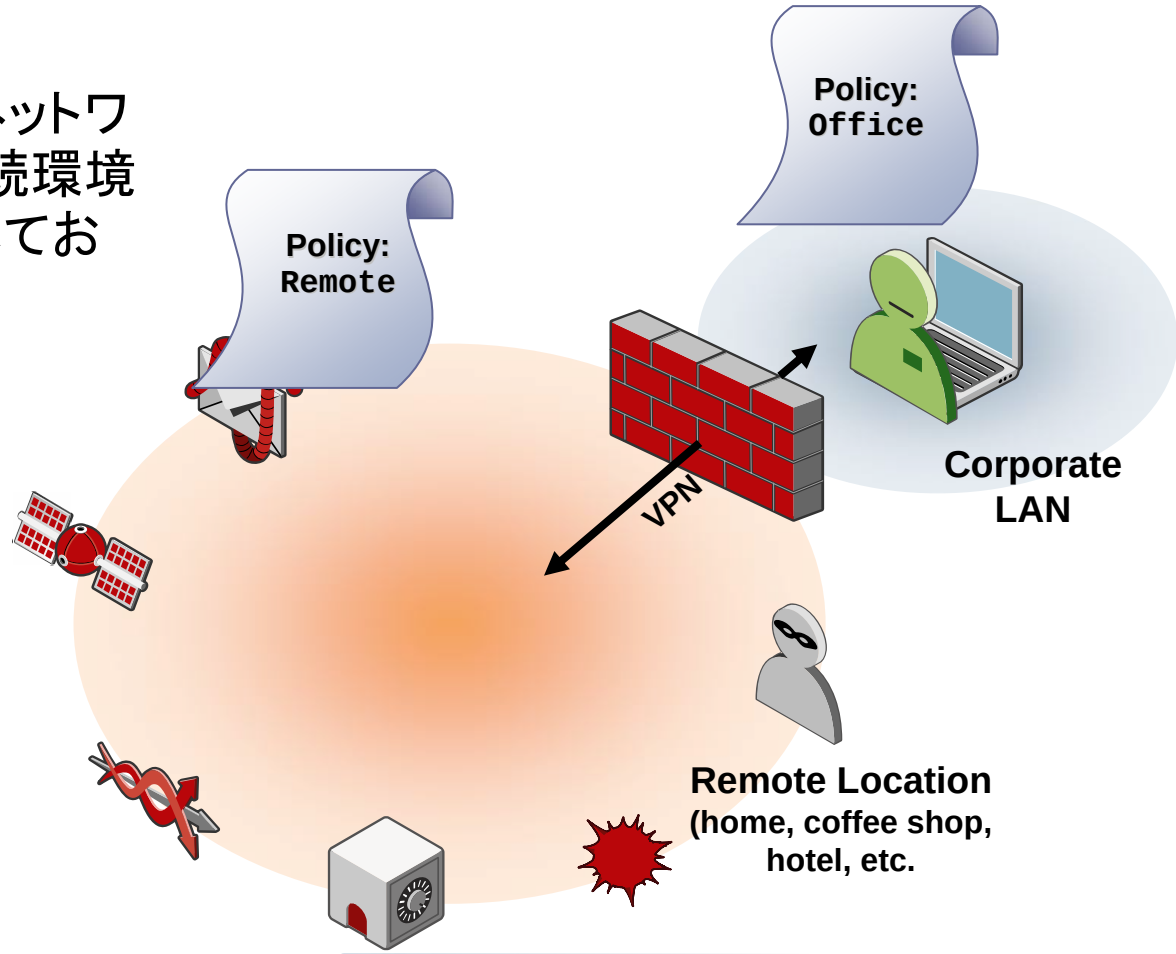
Intrusion Prevention Features

- Generic Exploit Blocking (GEB) を含む3種類のシグニチャによる
- 細かなパケット検査
- 管理者はカスタムシグネチャの作成が可能
  - SNORT™に近いシグネチャ
  - アプリケーションの脆弱性を狙った攻撃に対しユーザーの手によりいち早く防御

ポリシーの切換自動化

- ネットワーク接続環境ごとに異なるポリシーを作成することが可能

- 自動的にエンドポイントのネットワーク接続環境を識別し、接続環境に応じて、あらかじめ設定しておいたポリシーを適用



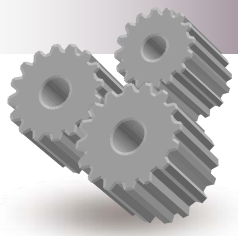
振る舞い検知エンジン

プロセス識別

Enumerate all processes & embedded components

プロセスの振る舞い分析

Assess behavior & characteristics of each process

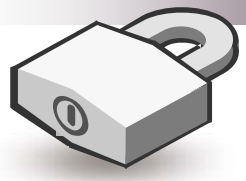


プロセス毎のスコアリング

Detection routines are weighted & processes are classified

自動防御

Malicious code is identified, reported & automatically mitigated



•2つのスコアリング（有効性スコアとマリシャススコア）

新しいプラットフォームでの新しいリスク：多様化するネットワーク

ネットワーク接続の多様化 → **感染経路・脅威の増加**

PDA：PCとの同期

携帯電話:ダイヤルアップ接続

融合

スマートフォン

-WiFi接続

-PCとの同期

-Bluetooth

-ショートメッセージ

感染経路が増加して脅威も増加

しかし

セキュリティは確保されていない！？

新しいプラットフォーム上の新しいリスク

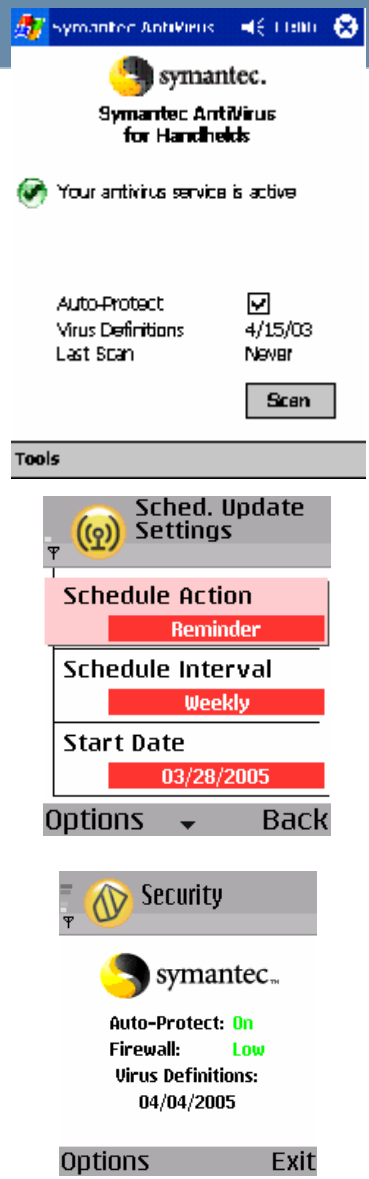
- 「人」がネットワーク外部との接続点：モバイルデバイスによって従業員と消費者が、ユーザとネットワークが融合する。
  - **常に携帯電話を持っている＝携帯電話が常にリスクになる。**
    - 70%のユーザが携帯電話をアラーム代わりに利用している。(source ICM Research)
  - **スヌープウェア**: モバイルのスパイウェアは電子メールだけでなく電話の機能を脅威にさらす
    - カレンダーを参照して盗聴に最適な時間を確認。
    - リモートからマイクを起動して会話を盗聴
    - 写真やムービー機能を使ったスパイ行為

      例: FlexiSpy, iCam など

スヌープウェアによって個人や会社の情報が危険に晒される!!

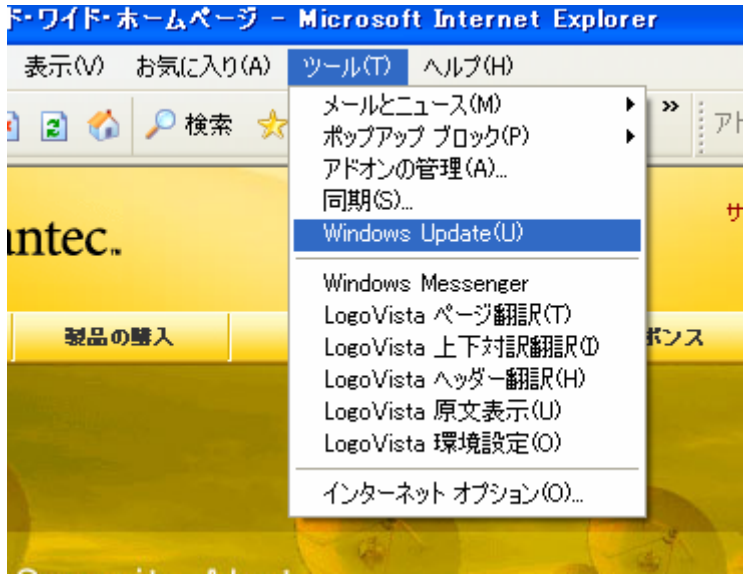
モバイル機器向けセキュリティ

- **Symbian, Windows, Palm 向けのアンチウィルス– 20以上のバージョン**
  - シンク後に拡張メモリーカードやデバイスをスキャン
  - Live Updateにより自動的に最新のウィルス定義ファイルを取得
- **ファイアウォール (Symbianのみ対応) による情報とappトランスミッションの保護）**
  - 事前設定された低・中・高のファイアウォール・ルール
  - プロトコルとポートのフィルタリング
  - デバイスに常駐し、コンスタントにバックグラウンドで動作。
- **OTA (Over the Air) Configuration Management**
  - IT管理者がリモート及びローカルでセキュリティポリシーを設定、ロック、エンフォース可能
  - ロック機能によりユーザが重要なセキュリティのセッティングを解除することを防止
- **Third Partyのモバイルデバイス管理システムを活用**
  - モバイルミドルウェアからデバイスへ、アプリケーションファイル、設定、アップデートをプッシュ配信
  - デバイスにすべてのイベントログが保存され、レポーティング可能



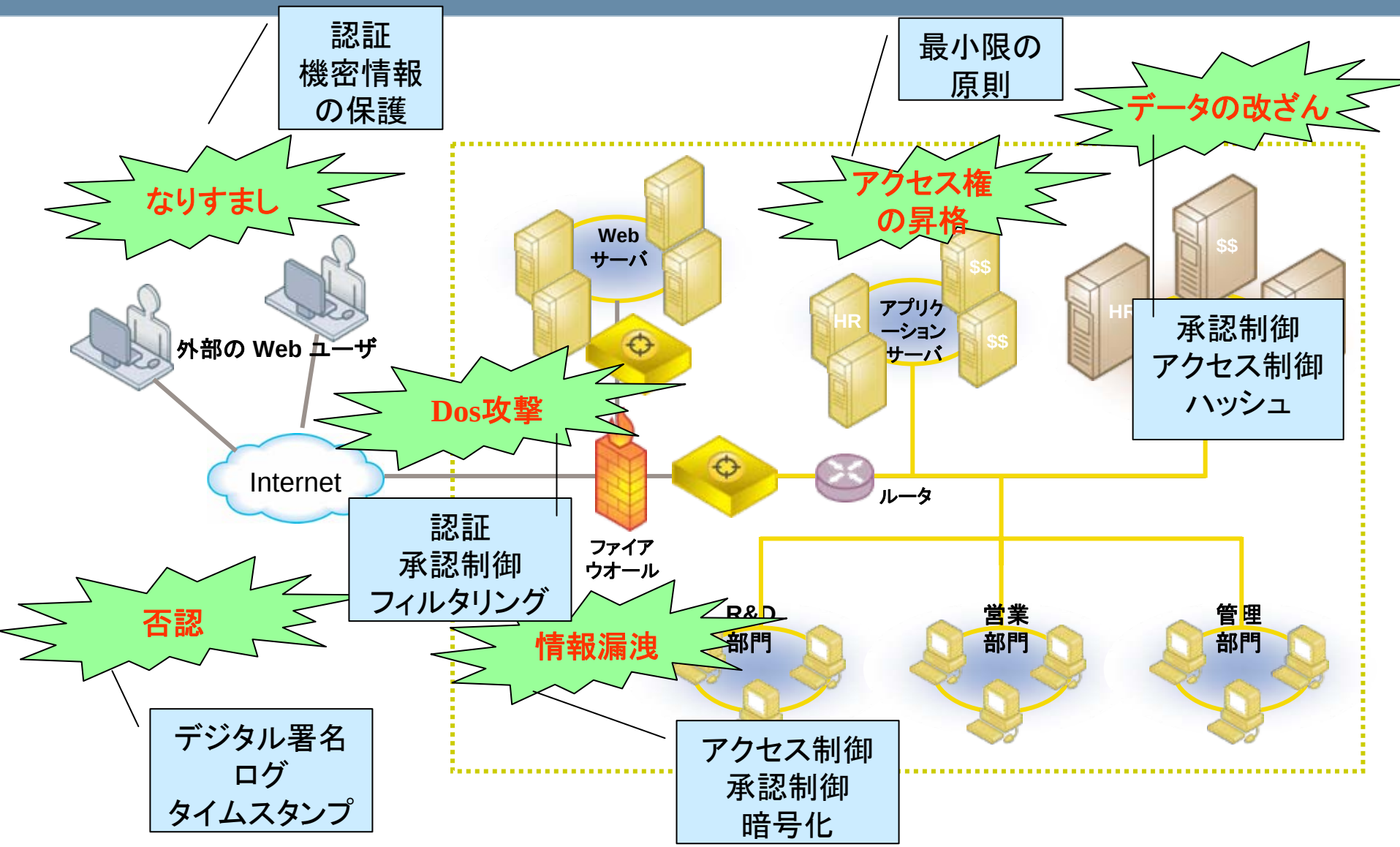
バグ（虫）はどこにでもいる

- OSやアプリケーションには必ず「バグ」がある
  - 完全無欠のものはなにひとつない
- 「バグ」は手当てすれば直る
  - セキュリティホールや脆弱性は「修正プログラム」や「修正パッチ」をインストールすれば直る
  - OSなどのバグは無料でダウンロードできる
- ハッカーは「バグ」を利用する
  - ハッカーはバグを利用して、ターゲットのコンピュータに被害を与えようとする



自分たちのアプリケーションのバグは誰が直す？

アプリケーションに対する脅威への対応策



アプリケーションセキュリティに対する要請

- 内閣官房情報セキュリティセンターより「**政府機関の情報セキュリティ対策のための統一基準**」に追加すべき項目（骨子） 平成17年10月17日

Ⅱ ソフトウェア開発 〈新規〉

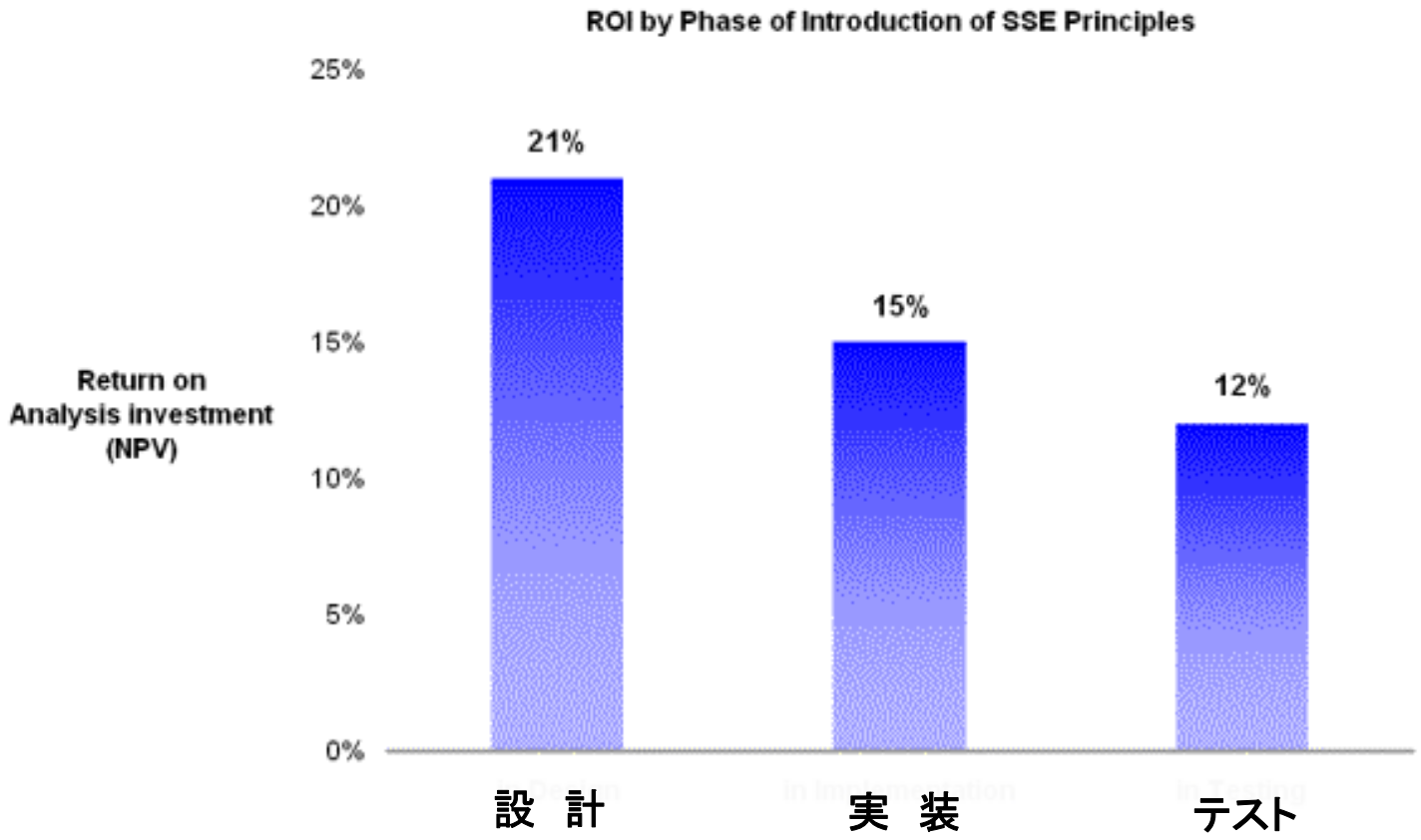
【 背 景 】

（1）ソフトウェアを開発する際には、当該ソフトウェアが運用される際に関連する情報資産に対して想定される脅威を分析し、その分析に基づいて脅威から情報資産を保護するためのセキュリティ機能及びその管理機能を適切にソフトウェアに組み込むことが

求められている。

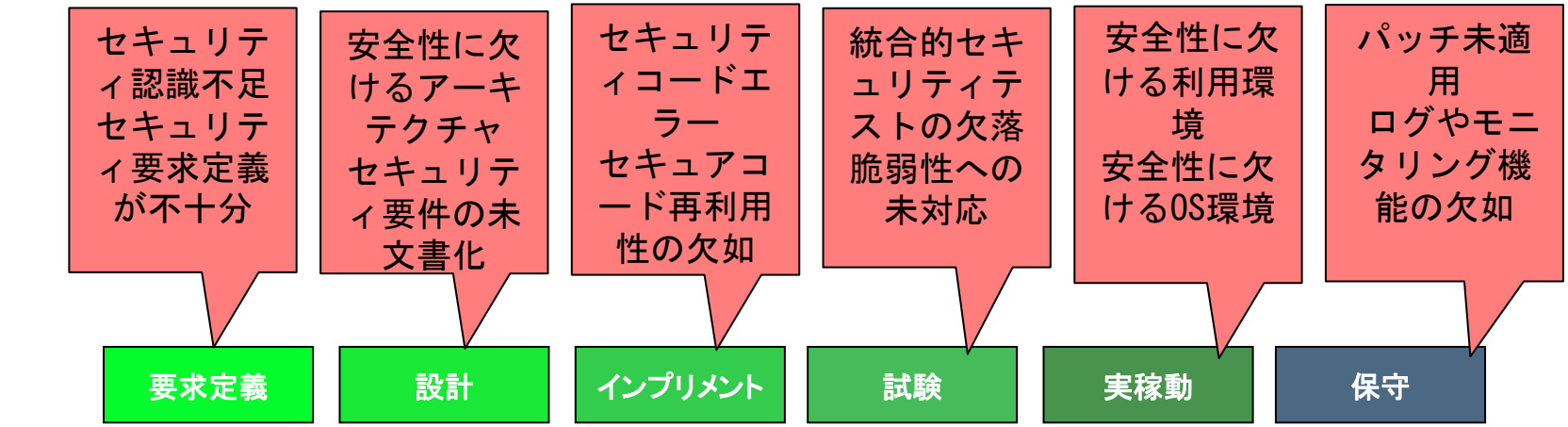
（2）加えて、開発するソフトウェアにセキュリティホールが混入しないための対策も必要となる。

アプリケーションセキュリティに対する早期の対応によるROIの改善



Analysis of 40 @stake Application Security Projects

アプリケーションセキュリティ　実現へのアプローチ



テンプレート提供
セキュリティ戦略
要求定義支援
セキュリティユースケース手法
コーディング規約構築
再利用可能なSモジュール提供
安全な利用環境構築
テストプログラム提供
パッチ管理環境構築
ログ管理のコンサルテーション

環境整備

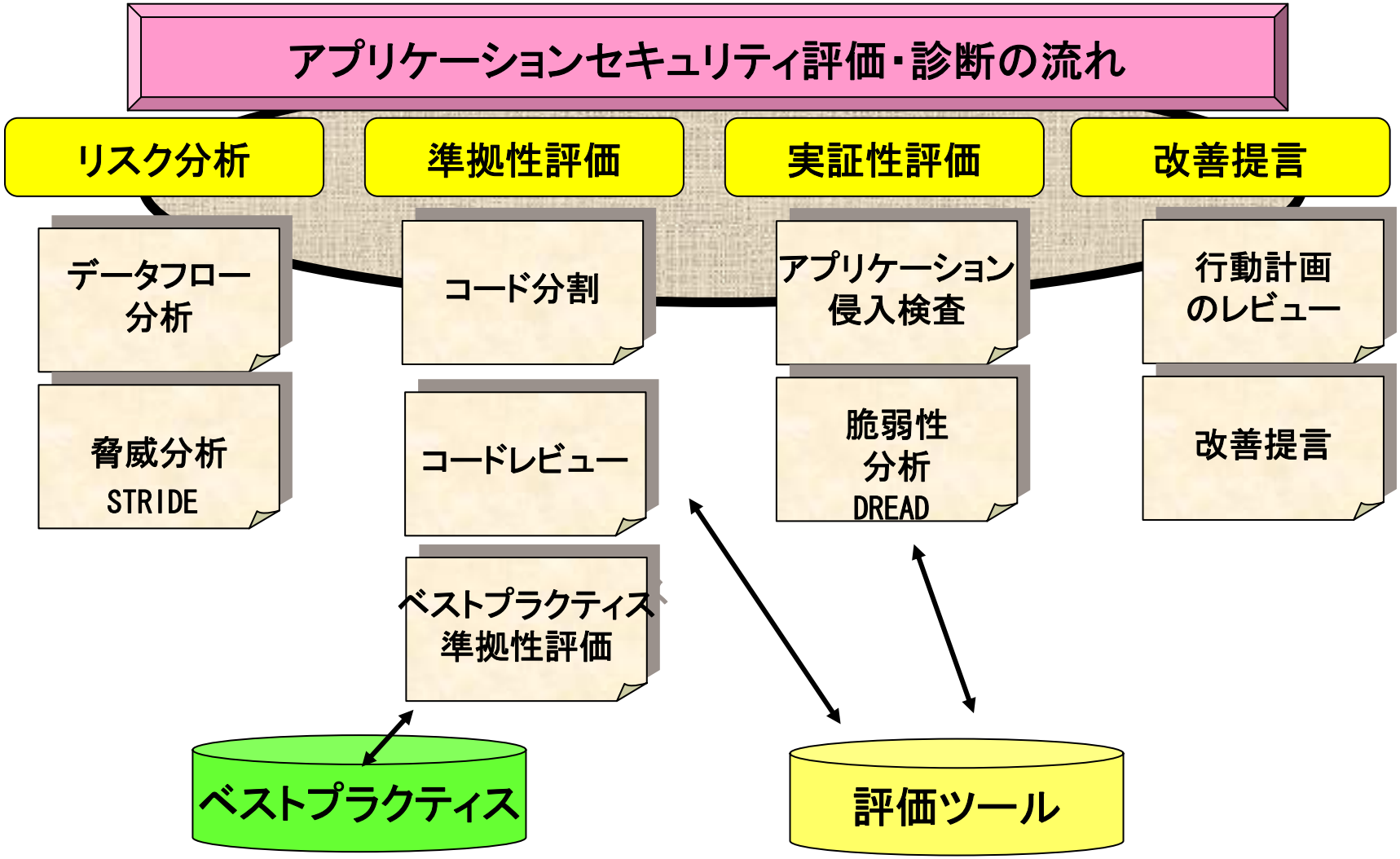
アプリケーションＡＡ
（アーキテクチャアセス）
脅威分析
コードレビュー
データ検証
侵入テスト
セキュリティバグ追跡
明瞭なセキュリティテスト
ネットワーク脆弱性評価
セキュアデザインレビュー

評価・診断

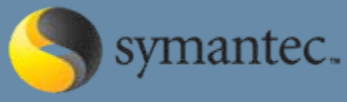
「セキュリティ基本」教育
「アプリケーションセキュリティ」教育
「サイバー攻撃と対応策」に関する教育

教　育

アプリケーションセキュリティ評価の枠組み



セキュリティ　実現のためのベストプラクティス



準拠性評価

モニタリング・ログ
監査証跡確保
ロギング保護
ログライフサイクル

開発プロセス
開発環境
メトリクス（評価基準）
セキュリティ要求仕様

データ完全性
入力データの検証
削除／アーカイブ保管
クライアント側検証

ベストプラクティス
安全なアプリケーションを構築するために実施すべき事項

認証
認証されたアクセス
パスワード機密性
資格情報の伝達

データベース
DBアクセス
DBパスワード
SQLインジェクション

アクセスコントロール
認可メカニズム
デフォルト全否定
最小限の権限原則

機密性
情報開示
エラーメッセージ
個人情報保護

暗号
データ暗号方式
通信路暗号化
記憶装置内暗号化

コードレビュー

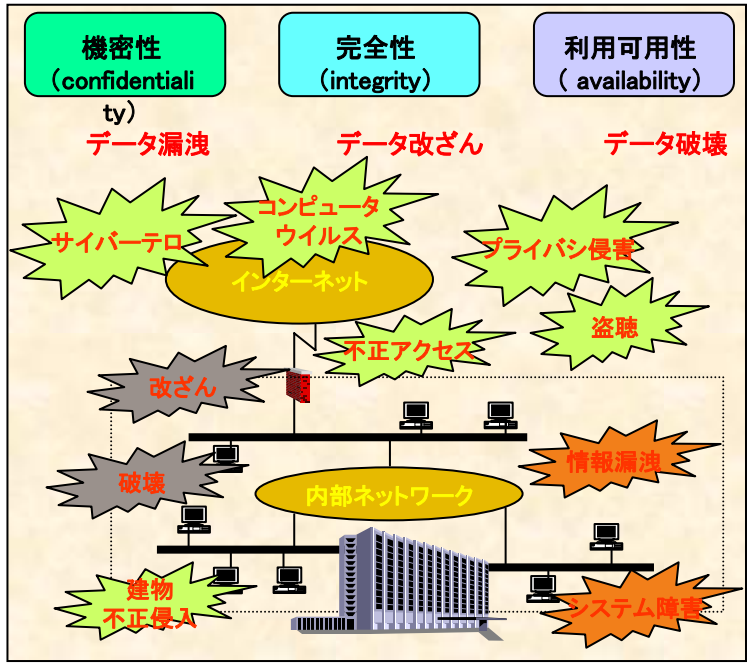
コード
レビュー

- コードレビューにより、アプリケーションソースコードの実装レベルでの問題点（脆弱性、有効資源の利用状況、問題の再現性）を明確化。

視点	レビュー内容
入力データの検証	入力データの内容をすべて検証しているか？ （クロスサイトスクリプティング）
暗号	暗号関連ルーチンが、アプリケーション内で適切にインプリメントされているか？
データベースとのやり取り	データベース用の動的なSQLクエリ使用が存在しないか？
機密性	機密性の高いデータが、ソースプログラム中に記述されたり、未暗号化のままで格納されていないか？
ロギングとモニタリング	法廷証拠確保のため、タイムスタンプ付で成功と失敗を含むイベントを規則的に記録しているか？
コード・メンテナンス	実行されない部分とデバックコード部分を取り除いた上で、適切にコメントされているか？
安全なプログラミング	フレームワークが提供しているセキュリティ上の機能をうまく活用しているか？(例：厳密名アセンブリ)

リスク分析

資産抽出

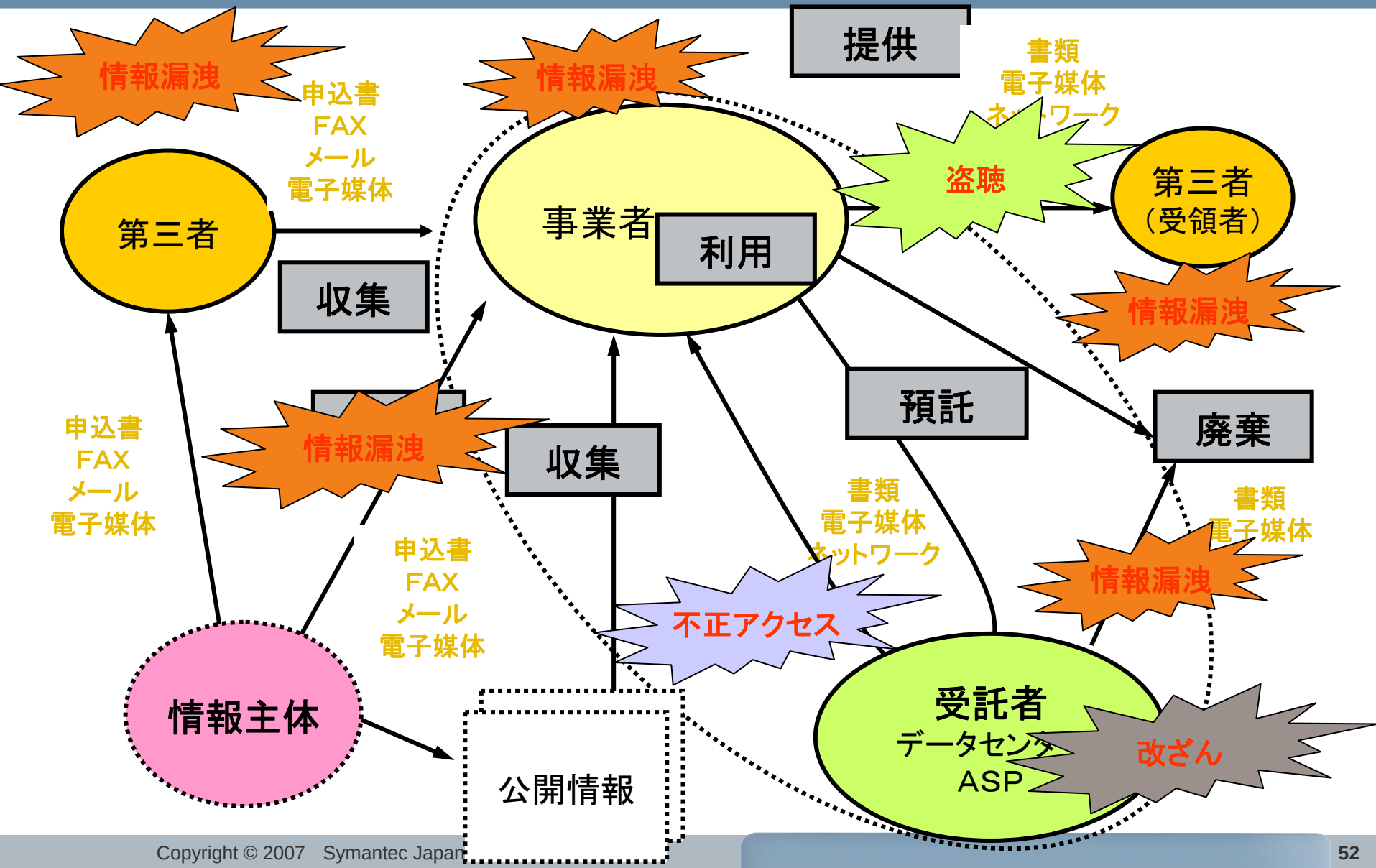


脅威識別

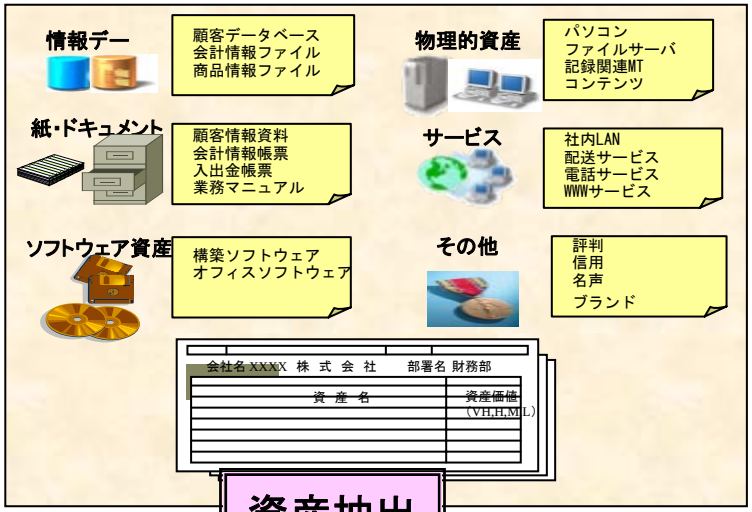
リスク ＝ Σ 発生頻度 × 損害額

リスク:負の期待値 影響度、重大性、脆弱性を考慮

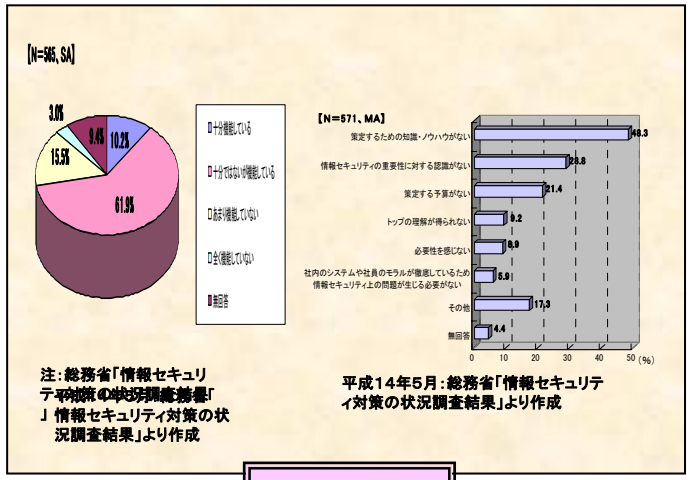
業務処理統制の重要性
（個人情報漏洩の可能性）



リスクに関する情報の掌握



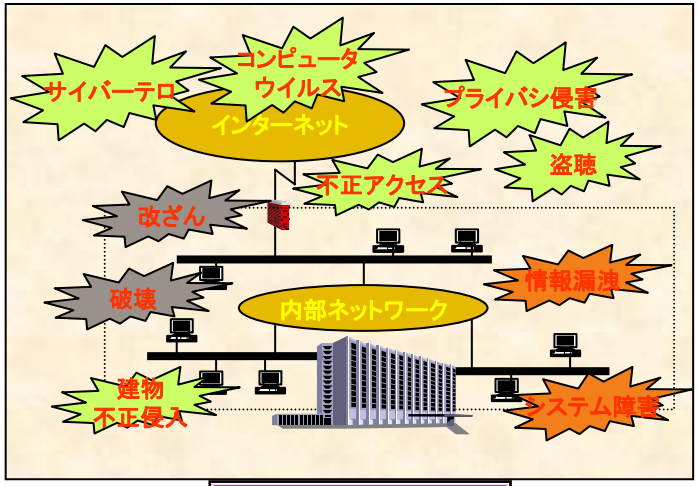
資産抽出



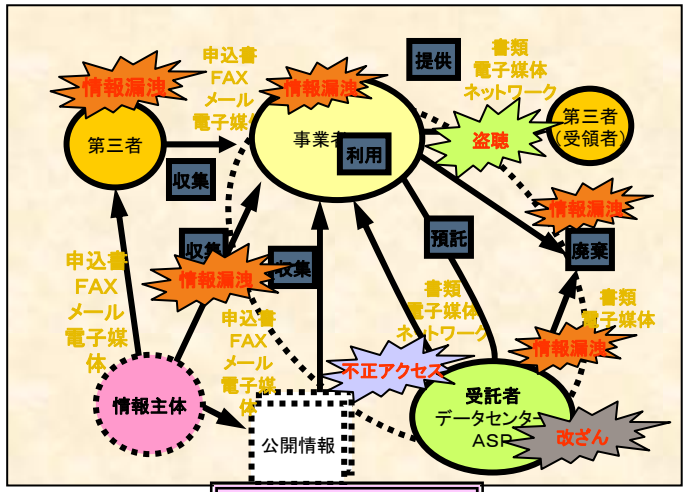
注：総務省「情報セキュリティ対策の状況調査結果」

平成14年5月：総務省「情報セキュリティ対策の状況調査結果」より作成

発生確率



システム基盤



業務プロセス

Confidence in a connected world.

御清聴ありがとうございます。

本資料のお問い合わせ先
山内　正
tadashi_yamanouchi@symantec.com