KPMG

cutting through complexity

サイバーセキュリティへの進化

KPMGコンサルティング株式会社

田口　篤

2014年11月13日

1. サイバーセキュリティの定義は確立されていない

サイバーセキュリティ基本法案など

都道府県警察、警視庁ホームページなど

サイバー
セキュリティ

サイバー
犯罪

外部からの脅威
サイバー空間の話
高度なハッキング技術
明確な犯意　etc

なんとなくのイメージ

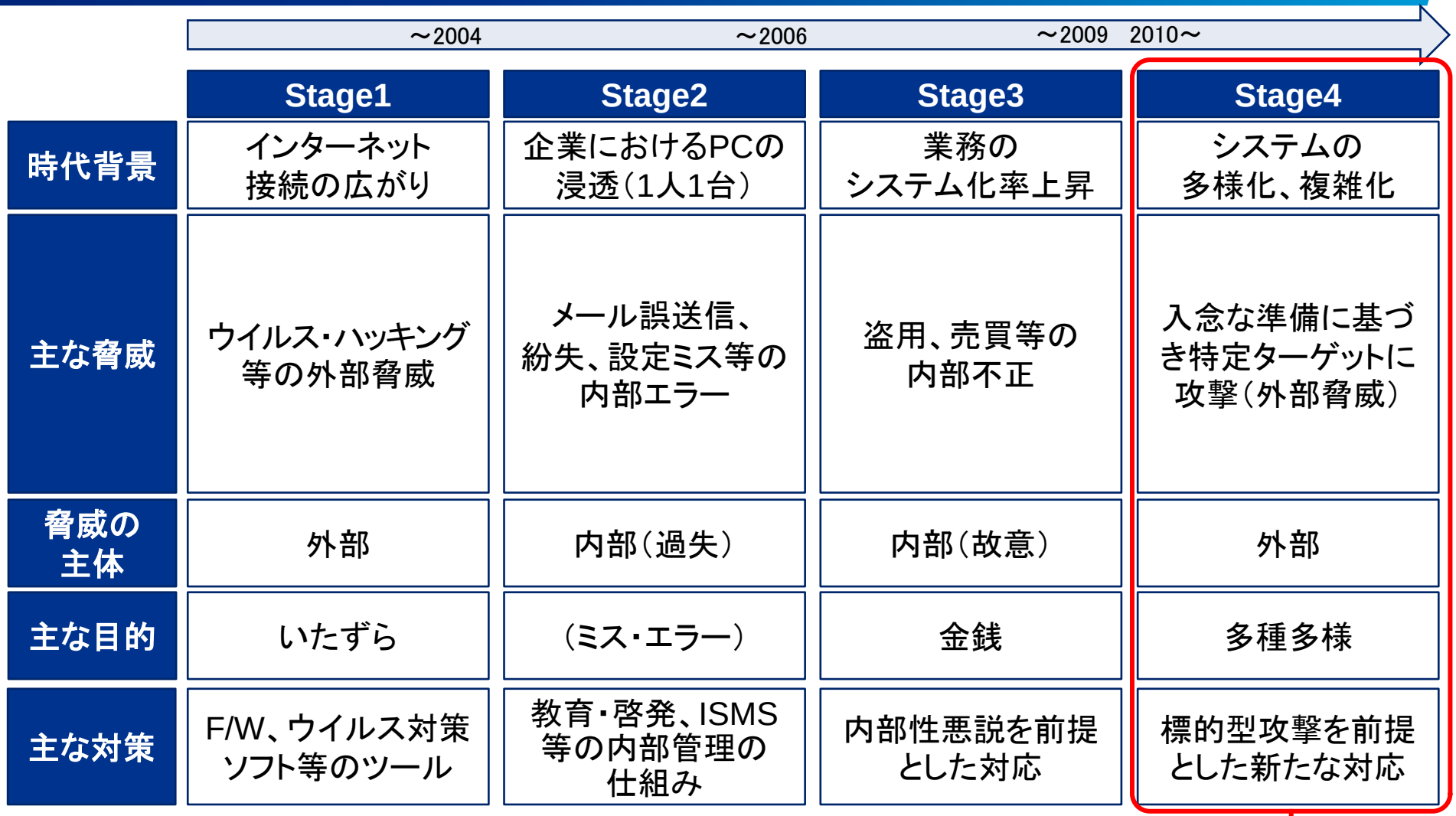
サイバー
攻撃

サイバー
テロ

防衛省ホームページなど

サイバーテロ対策協議会（警視庁）
情報通信ネットワーク安全・信頼性基準
（総務省）など

2. 情報セキュリティ上の脅威の変遷



Stage1との相違点：外部脅威のプロ化・多様化

3. 多様化する攻撃者と攻撃目的

サイバーセキュリティの本質は多様化する攻撃者と攻撃目的を理解し、自社に迫る脅威を的確に把握すること

Individual Hacker
- 技術スキルの誇示が目的
- Web改ざんなど

Stage1

Organized Crime
- 金銭的利益が目的
- フィッシング、詐取 など

Stage4

The Activist（Hacktivist）
- 業務妨害や評判へのダメージが目的
- サービス停止など

Nation States（Government）
- 地政学的、経済的優位性の獲得が目的
- スパイ、機密漏えいなど

Insider

Stage2 & 3

プロ化・多様化
- 特定組織を明確な目的を持って攻撃
- 技術の高度化（Social+ Technical）

4. 企業が取り組むべき事項

これまでの情報セキュリティの取組みを
最新のサイバー攻撃に対応できるように進化させる

① Crown Jewelの特定

② リスクシナリオの検討

③ 突破されることを前提とした対策の導入

④ インテリジェンス機能の導入による継続的な学習

5. ①Crown Jewelの特定 ／②リスクシナリオの検討

自社にとってのCrown Jewelは何か

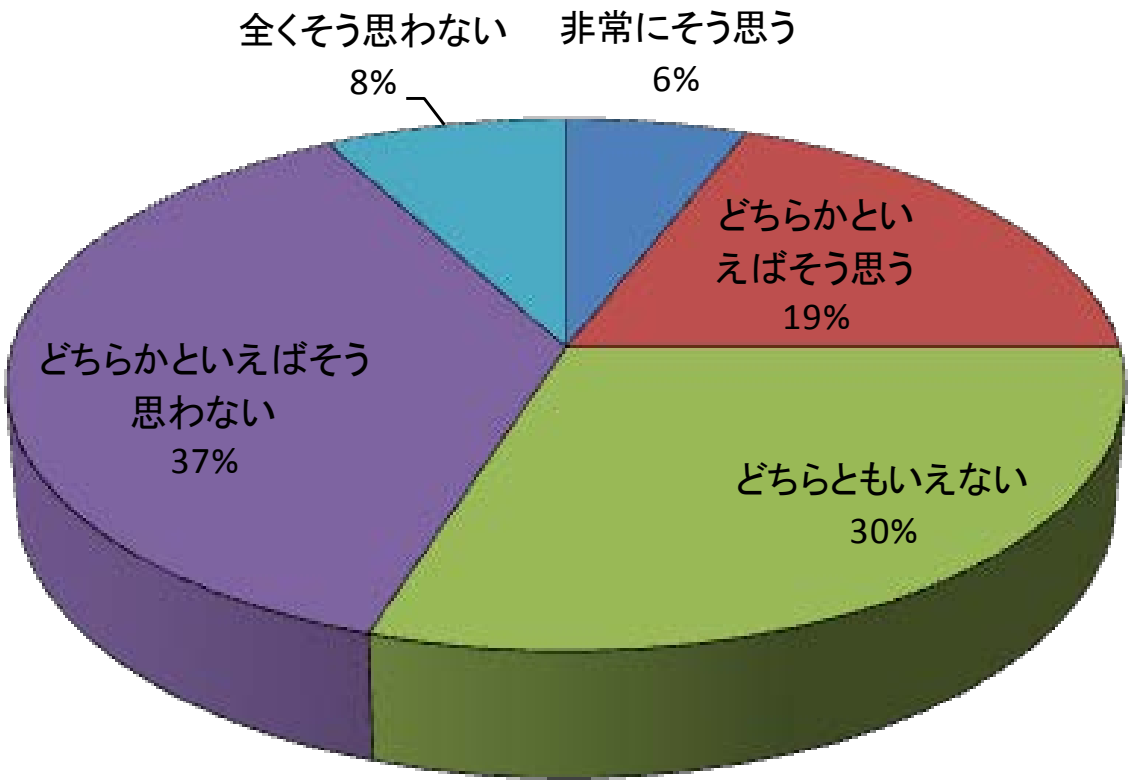
- 機密情報の範囲が広すぎる
- 管理側の都合で対象外にされているものがある（例：制御系システム、グループ会社）
- 外部から見たときに本当に魅力的なものは何か？

誰が、なぜ、何を、どうやって

- 誰から狙われているのか？
- なぜ狙われているのか？
- 何を狙われているのか？
- どうやって攻撃されるか？

会社によって狙われる理由は千差万別。自社固有のリスクシナリオが必要

6. 自社はサイバー攻撃のターゲットとして魅力的か？



KPMG「サイバーセキュリティサーベイ2013」より
上場企業、売上高500億円以上の未上場企業　308社回答

7. ③突破されることを前提とした対策の導入

100%完璧な防御はない。だから. . .
（これまで） セキュリティに過度のコストをかけるのはやめよう
（これから） Fail Safe思想の導入とDetect & Responseの充実

3×3のマスを埋める設計

	Prevention	Detection	Response
Management & Organization	管理体制（責任と権限）の整備	24時間365日体制の危機管理体制	フォレンジックスキルの活用
Process	シミュレーション 定期的な侵入テスト	インシデントの究明、追跡手続	インシデントレスポンスプラン
Technology	十分なデスクトップセキュリティ機能 ネットワークのセグメンテーション	重要なイベントのログ収集機能 セントラルモニタリング機能	攻撃下でのITサービス遮断機能

8. ④インテリジェンス機能の導入による継続的な学習

サイバーインテリジェンス機能とは

セキュリティに関するさまざまな情報を収集・分析し、自社への影響を評価することによって、サイバー攻撃の予兆を捉えプロアクティブに対応することを目的とした機能

【収集・分析対象となる情報の例】

- 日々、発見・報告されるシステムの脆弱性に関する情報
- 自社サイトの監視状況
- セキュリティに関する事件・事故情報
- 海外を含む同業種に対するサイバー攻撃の情報
- アンダーグラウンド情報
- 自社のインシデント情報 など

情報収集力と学習機能をもつことが最良の対応手段

9. サイバーセキュリティに関する誤解

- ITのテクニカルな話でユーザー部門には関係ない？
- 自社はハッカーには狙われない？
- セキュリティ認証をとっているので対策としては十分？

誤　解	実　際
最高クラスのITシステムに投資していればサイバーセキュリティは安全に保たれる	攻撃側は一番弱いところを狙ってくる 目的達成のためなら手段はオンラインに限定されない
サイバー攻撃から自社を守るためには、こちらも高度なスキルをもった専門家を雇わなければならない	サイバーセキュリティは特別なスキルを持った専門家集団だけで達成されるわけではない
サイバーセキュリティに関するさまざまなガイドラインに準拠していくことが最良の対応手段である	サイバーセキュリティのリスクは各社各様 標準的なルールセットだけでは対応しきれない

10. KPMGサイバーセキュリティサービス

KPMGでは昨今のサイバー攻撃の脅威の高まりに伴い、2013年より以下のサービスを提供しています。

サイバーアセスメントサービス

Prepare

サイバー攻撃の防御態勢に関する現状の問題点を明らかにし、サイバー攻撃防御態勢の改善ロードマップ立案をトータルに支援します。

【サービス項目の一例】

- サイバー攻撃防御態勢クイック診断
- サイバー侵入テスト
- モバイルセキュリティ診断
- 無線LANセキュリティ診断
- SNS利用のセキュリティ診断
- 顧客情報・営業秘密のセキュリティ診断
- 海外拠点のセキュリティ診断

サイバーマネジメントサービス

Protect

サイバー攻撃防御態勢の核となる体制、システム、ルール、PDCAの要素について、強化・改善するための活動をトータルに支援します。

【サービス項目の一例】

- サイバーセキュリティ組織の立上げ支援
- サイバーセキュリティポリシー立案支援
- モバイル・無線LANセキュリティ強化支援
- SNSセキュリティ強化支援
- サイバー攻撃防御態勢の高度化支援
- セキュリティ担当役員の補佐

サイバーインテグレーションサービス

Integrate

【サービス項目の一例】

- サイバー攻撃情報インテリジェンス支援
- GRC活動との統合支援
- 事業継続計画（BCP）との統合支援
- サイバー攻撃に関する教育・啓発支援
- グローバルな防御態勢への変革支援
- 制御システムの防御態勢への変革支援
- サイバー攻撃防御態勢の変革支援

時々刻々と進化していくサイバー攻撃に対して、防御態勢を有効に機能させ続けるために、既存の企業活動との統合、定着をトータルに支援します。

サイバーレスポンスサービス

Detect & Respond

【サービス項目の一例】

- 緊急対策本部の立上げ・運営支援
- 緊急時のクライシスマネジメント対応支援
- サイバー・フォレンジック
- 被害者への対応、賠償策の支援
- 再発防止策の策定・展開支援

サイバー攻撃が発生した際の広報・メディア対応、事実究明、再発防止策の立案・展開について、適切かつ迅速なアドバイスでトータルに支援します。

KPMG

cutting through complexity

お問合せ先

パートナー　田口　篤

KPMGコンサルティング株式会社

TEL：03-3548-5305（代表）

kpmg.com/jp/kc