Deloitte.

インシデントレスポンスの新潮流

能動的なダメージコントロールという考え方

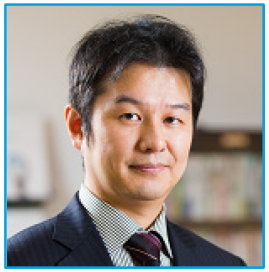
デロイト トーマツ リスクサービス株式会社
デロイト トーマツ サイバーセキュリティ先端研究所
公認会計士 森島 直人

2014年11月20日

トーマツ.

講演者紹介

名前	森島　直人
職位	マネジャー



略歴	通信会社等にて大規模システムの導入支援、構築運用などを実施すると共に、移動体通信環境に関する研究開発にも従事。その後、監査法人において内部統制監査、システム監査、会計監査等の監査業務等に多数従事。 有限責任監査法人トーマツに入社後は、ISMS認証取得支援、CSIRT構築支援を含む、情報セキュリティコンサルティング業務に多数従事。 Interop Tokyo 2001-2007,2014 NOCメンバーとして参加。 公認会計士、CISA、博士（工学）

アジェンダ

サイバー攻撃とリスプマップの変遷
サイバー攻撃に対する既存コントロールの限界

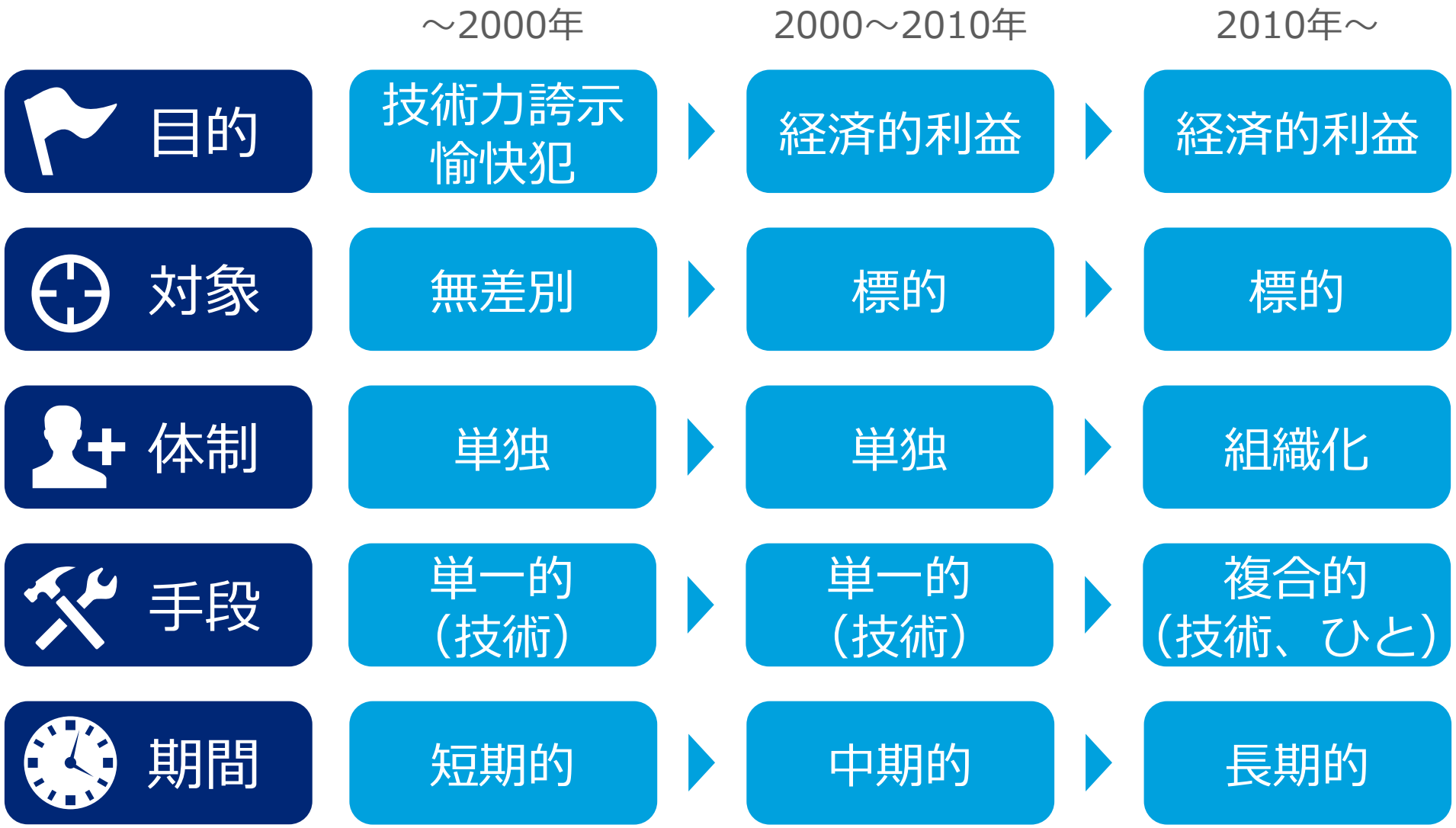
「サイバー攻撃による損害低減」に対する社会的要請の高まり
ダメージコントロールの考え方

インシデントレスポンスの新潮流
副次的な損失を抑制する

本資料の意見に関する部分は私見であり、所属する法人の公式見解ではありません。

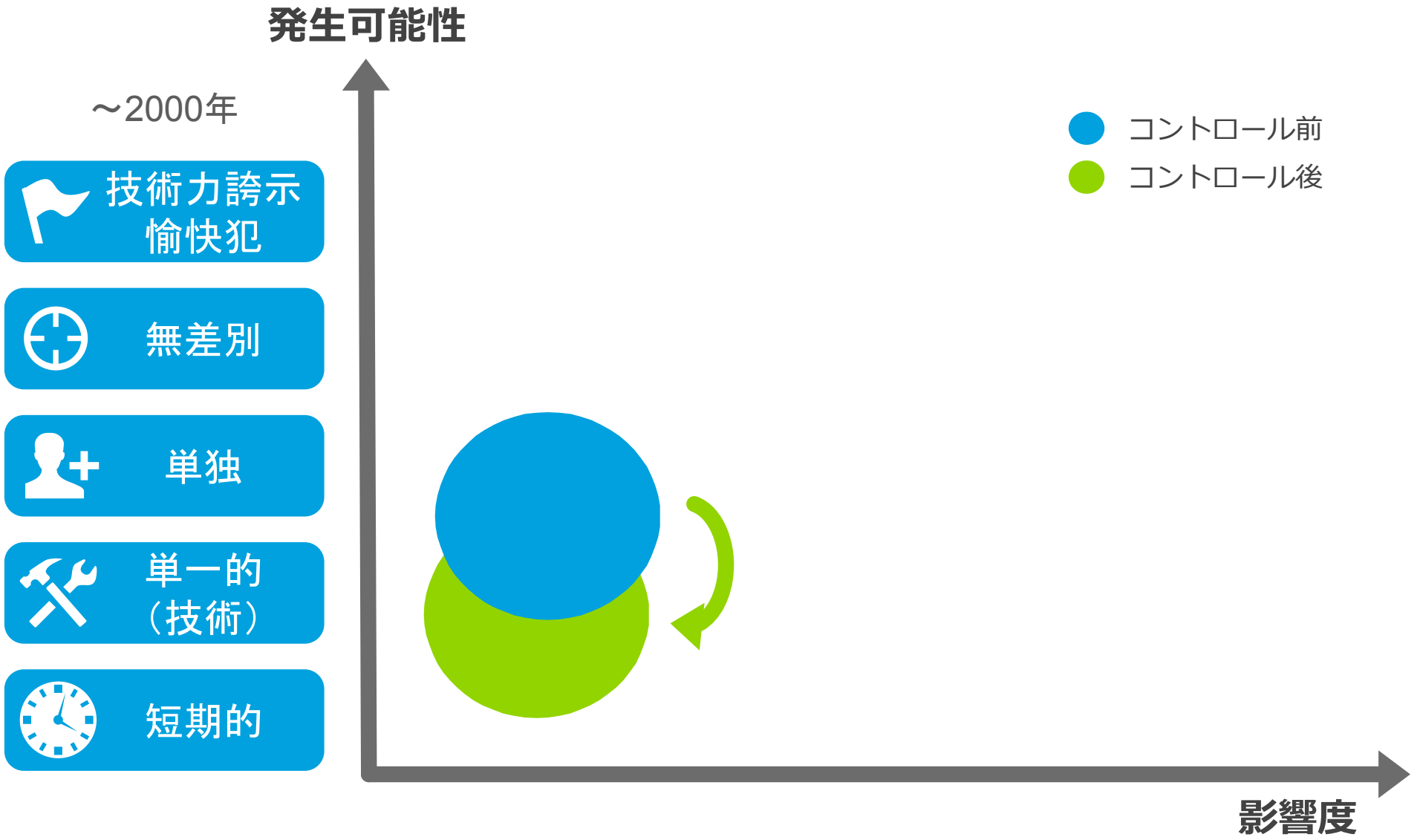
技術力誇示目的の単独犯から経済的利益目的の組織犯罪へ

サイバー攻撃の推移



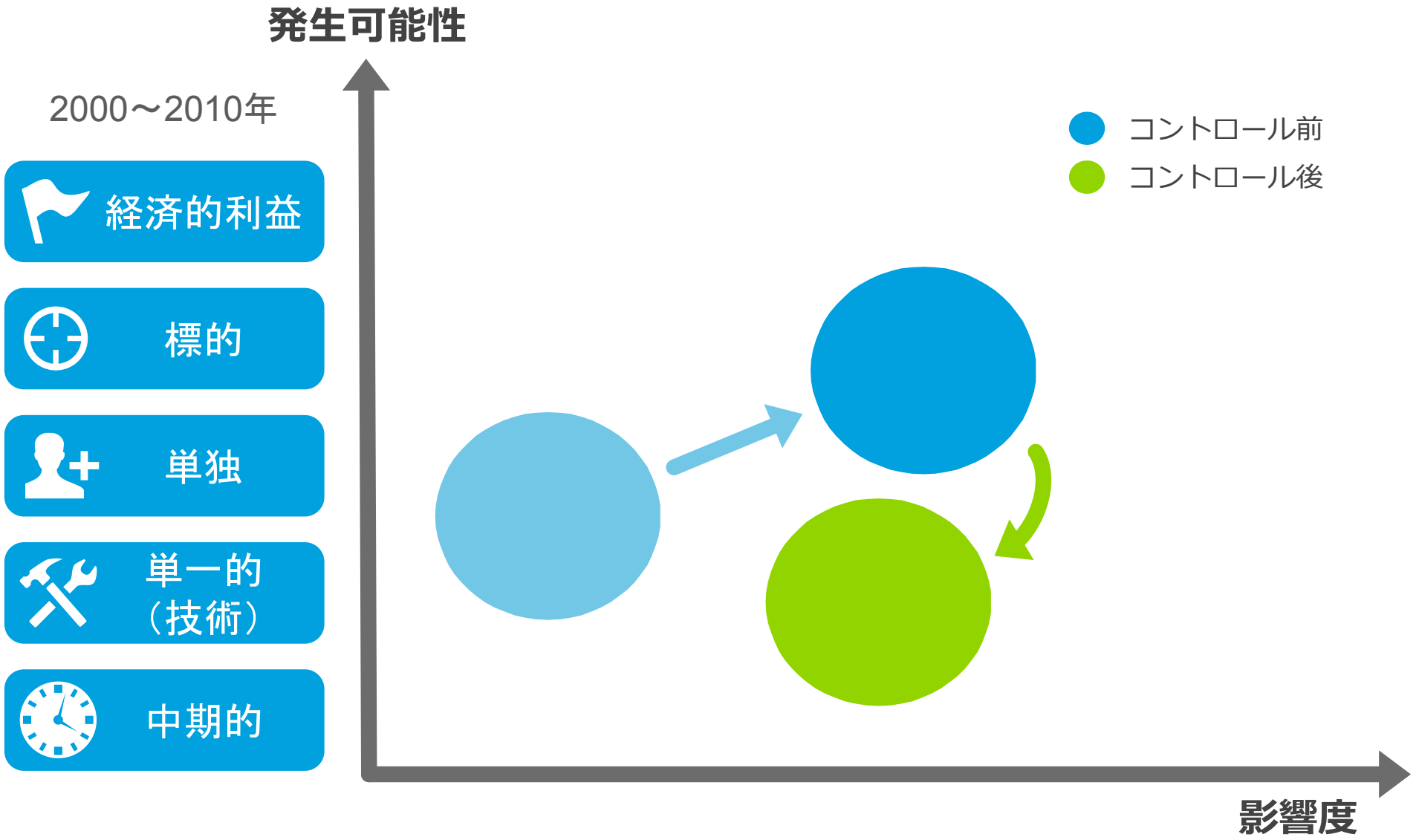
古き良き時代のリスクマップ

発生可能性と影響度の小ささから対応は限定的



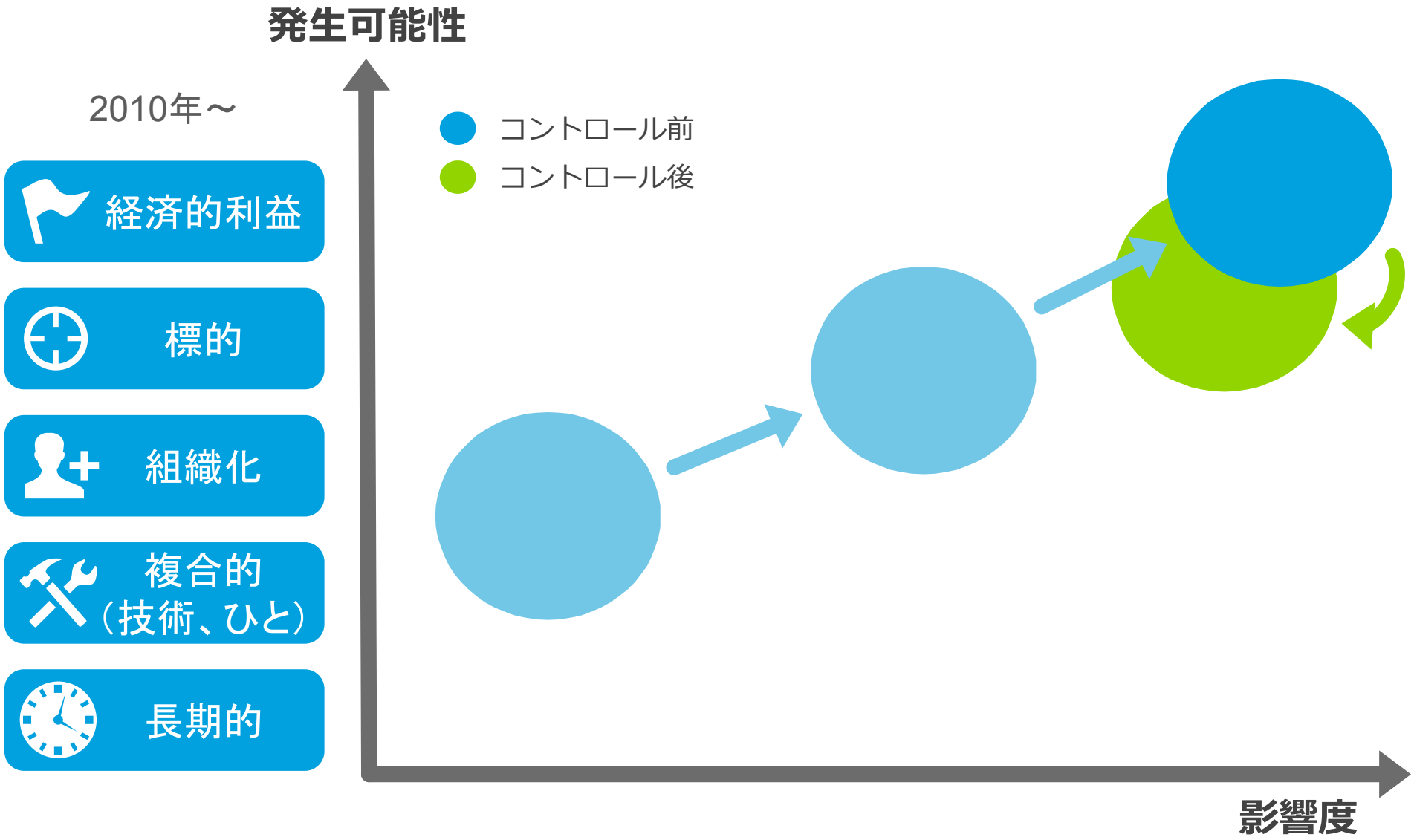
ビジネス化サイバー攻撃黎明期のリスクマップ

「防御優先」のアプローチ



標的型攻撃全盛期のリスクマップ（１）

「防御優先」アプローチの限界



「ひと」の脆弱性に劇的な改善は見込めない

防御技術の進歩で「ひと」が最も脆弱なポイントに

サイバー攻撃によって企業価値が毀損する時代へ

直接的、間接的な要因によって無視できない損害が発生するおそれ

一次被害

情報窃取はゼロサムゲーム

サイバー攻撃のビジネス化
攻撃者：情報窃取により利益を獲得
被害者：情報漏洩により損失が発生

個人情報の漏洩

資産価値の毀損にとどまらない
- 漏洩情報の対象者に対する補償
- 訴訟対応の失敗による不利な和解

二次被害

企業ブランドの毀損

被害者であって被害者ではない
- セキュリティ対策への不安
- 遵法性への疑念
- 企業への信頼の失墜

レピュテーショナルリスク

利害関係者への情報開示のまずさ
- 適時適切な情報開示の重要性
- 「被害者」強調といった開示内容のまずさ

投資家もサイバー攻撃によって起こりうる損害に注目

財務報告に付随してサイバーセキュリティリスクの開示を要請する動き

米国
証券取引委員会
（SEC）

Registrants should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky. In determining whether risk factor disclosure is required, **we expect registrants to evaluate their cybersecurity risks** and take into account all available relevant information, including prior cyber incidents and the severity and frequency of those incidents.

出典：“CF Disclosure Guidance: Topic No. 2”（2011年10月13日）

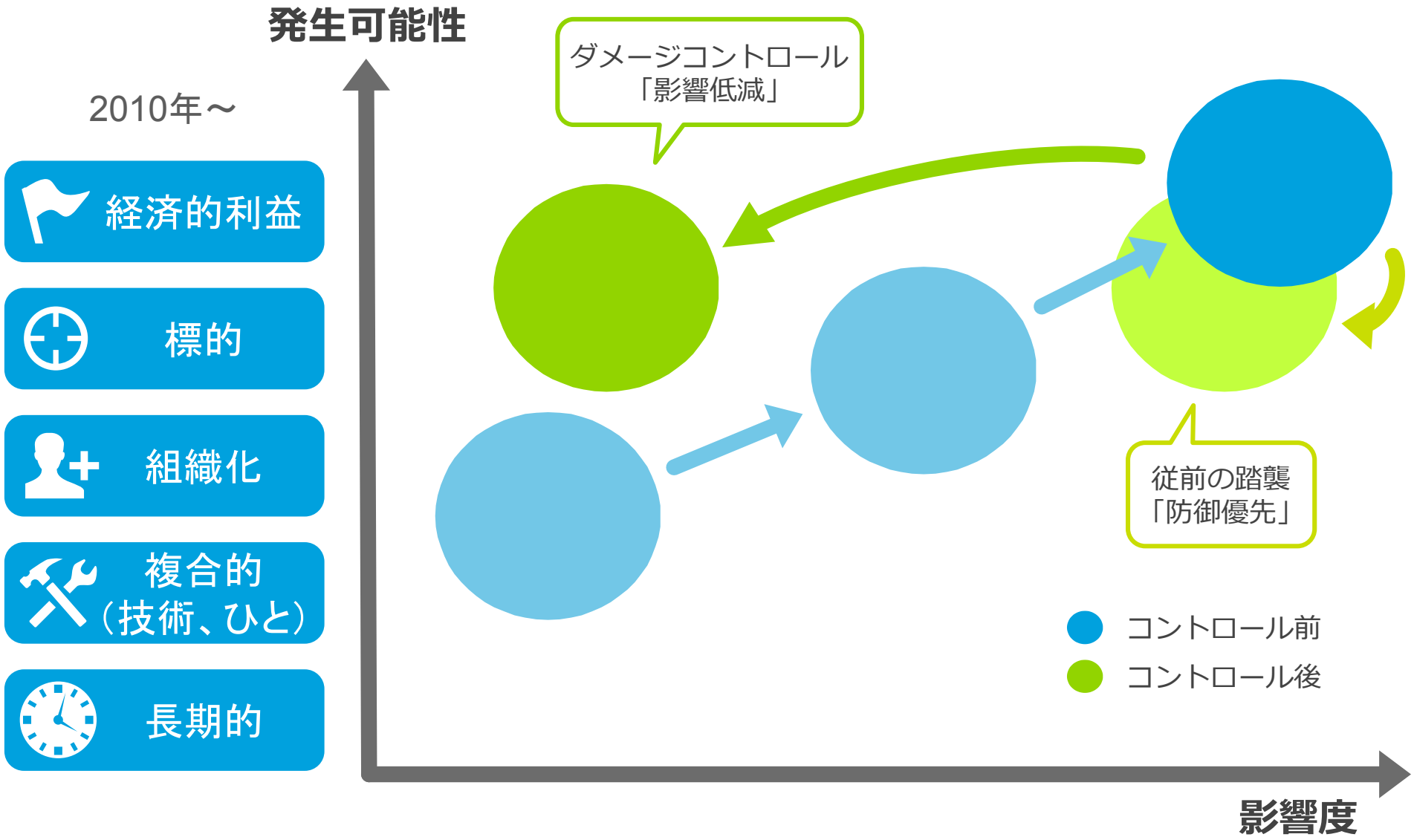
情報セキュリティ
政策会議

「金融庁において、**上場企業におけるサイバー攻撃によるインシデントの可能性等について、**米国の証券取引委員会（SEC）における取組等を参考にしつつ、**事業等のリスクとして投資家に開示することの可能性を検討**し、結論を得る。その際、関連情報の共有など開示するインセンティブを促すための仕組みの在り方についても併せて検討し、結論を得る。」

出典：「サイバーセキュリティ2014」（2014年7月10日）p.22

標的型攻撃全盛期のリスクマップ（２）

「影響低減」＝ダメージコントロールへのパラダイムシフト



被弾を前提とした被害局限のアプローチ

ダメージコントロール施策の例

軍事分野

- 開放型格納庫
- 可燃物の排除
- 士官室の設置位置

サイバーセキュリティ分野

- 出口対策
- MDM
リモートワイプ
- サイバー保険加入
- ストレージ暗号化
（HDD/SSD）
- クライシス
コミュニケーション
- eDiscovery対応

インシデントレスポンスの新潮流

「リアクティブ」から「プロアクティブ」へ意識の転換

インシデントの終息 → ダメージコントロール

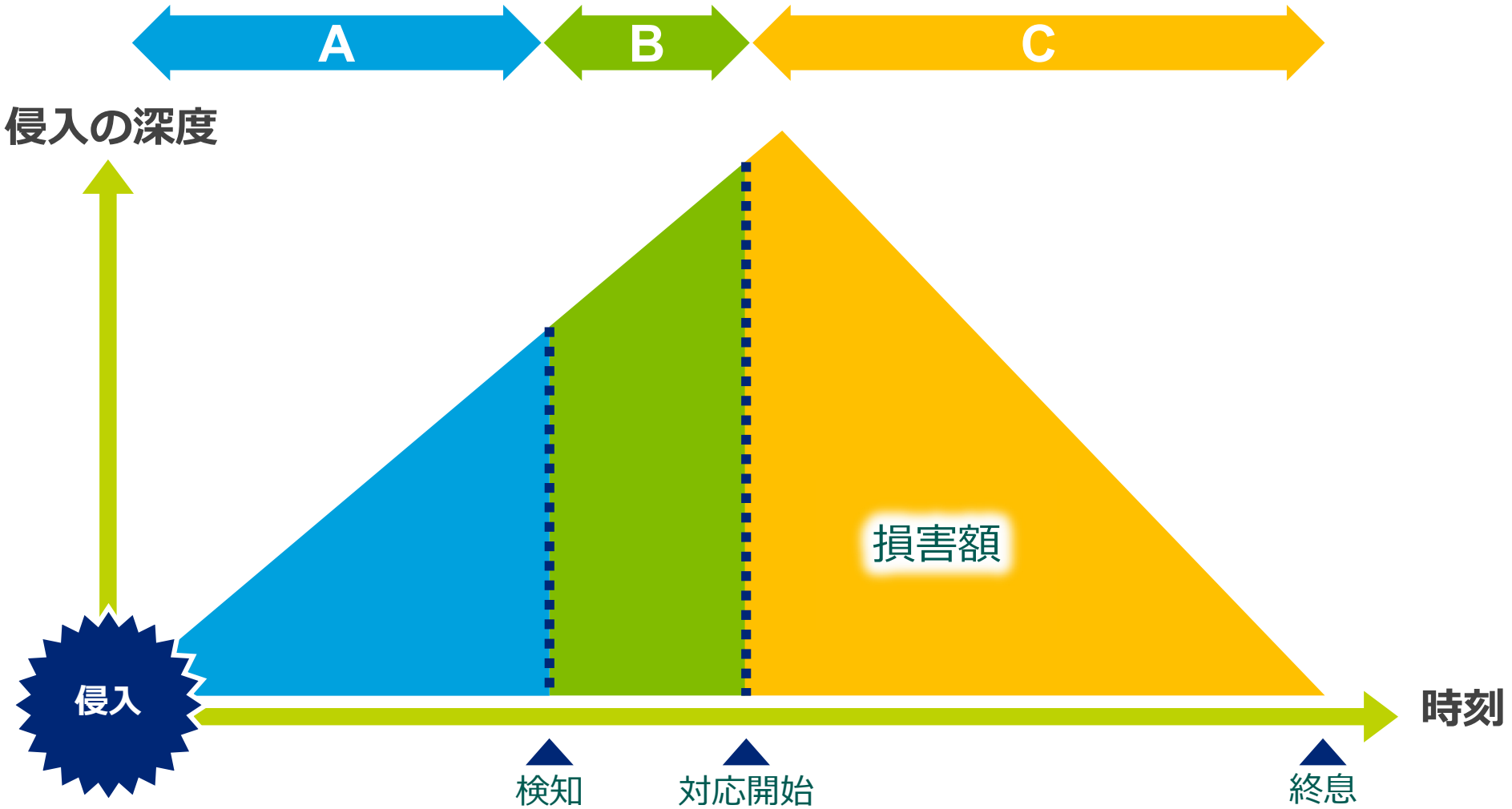
ダメージコントロール＝リスクマネジメントシステム

ダメコンの施策にベストプラクティスはない

1	リスク アセスメント	想定される脅威を洗い出しと分析を実施します。分析では、脅威の発生を前提とした被害拡大のシナリオ、許容できる被害水準の設定、被害を許容水準以下に収めるために優先的に守るべき資産や機能などを定義します。
2	リスク対応 計画の策定	リスクアセスメントの結果に基づき、脅威の具現化に伴う損害を軽減するための計画を策定します。インシデント発生時の対応に意識が向きがちですが、損害発生を遅らせる、対応の迅速化するといった日常的活動の施策が重要です。
3	態勢整備 計画の実施	ダメージコントロールに資する日常的活動を実施するための態勢を整備し、リスク対応計画を実行します。態勢整備には、インシデント対応組織、情報収集・状況確認の仕組み、報告連絡態勢などの整備が含まれます。
4	運用訓練	整備・実行した施策が十分に機能して損害を抑制できるかを検証するため、運用訓練を実施します。個別の施策ごとの検証だけではなく、インシデントの発生を想定したシナリオベースの訓練を実施することが望ましいと考えられます。

まずはダメージの構成要素を知る

3つの要素で構成



まずはダメージの構成要素を知る

3つの要素で構成

A

価値ある情報の在り処を探し当てるため、攻撃者は長期にわたって標的内に潜伏します。目立たないよう活動を続けるこの期間、徐々に損害が増加していきます。

B

インシデントを検知するだけでは、損害の拡大が収まるわけではありません。むしろ、検知したことが攻撃者に認識されると、損害が一気に加速する恐れもあります。

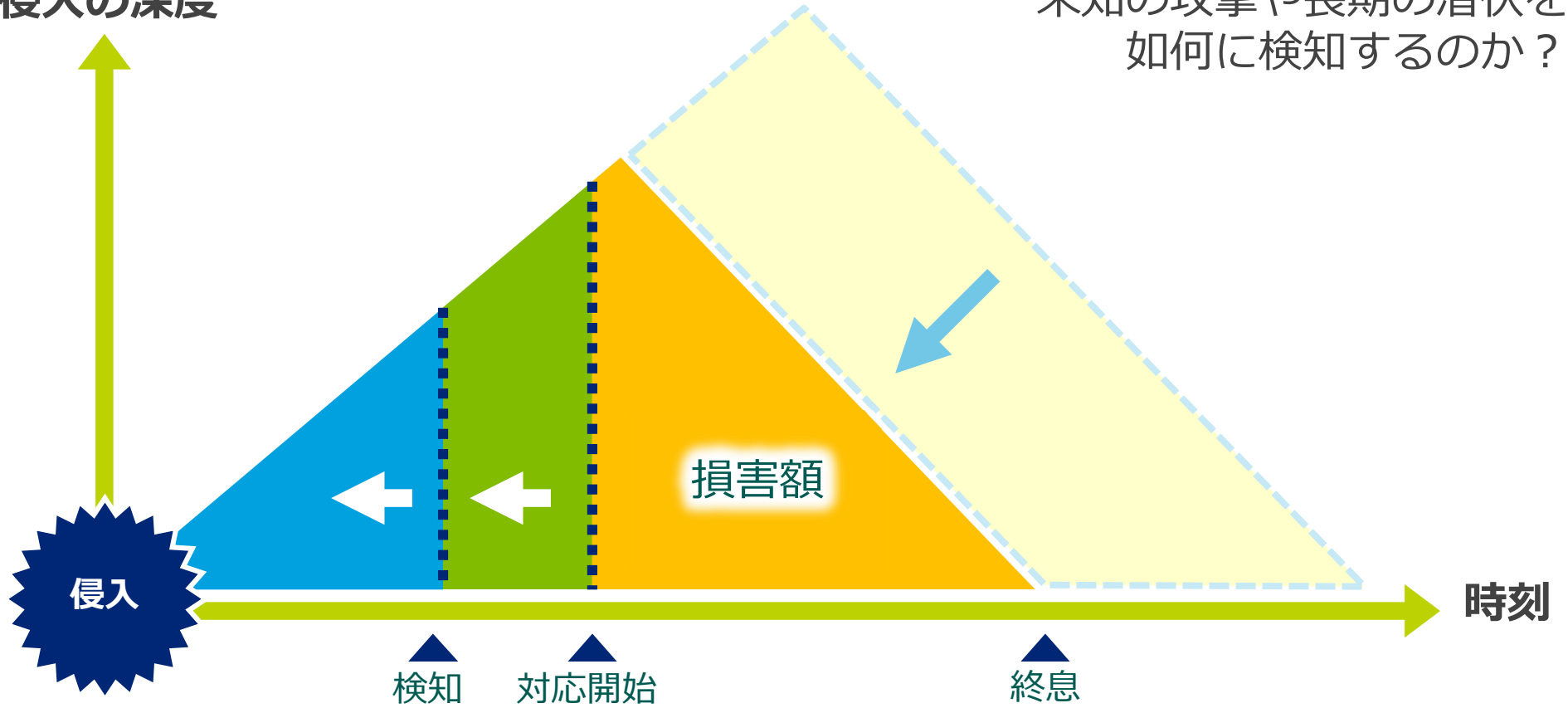
C

インシデント対応を開始によって損害の増加速度は逓減し、ついには終息してゼロになります。しかし、終息までの期間は継続して損害が発生しています。

検知はダメージコントロールの大前提

早期検知によるアプローチ – SOCの場合

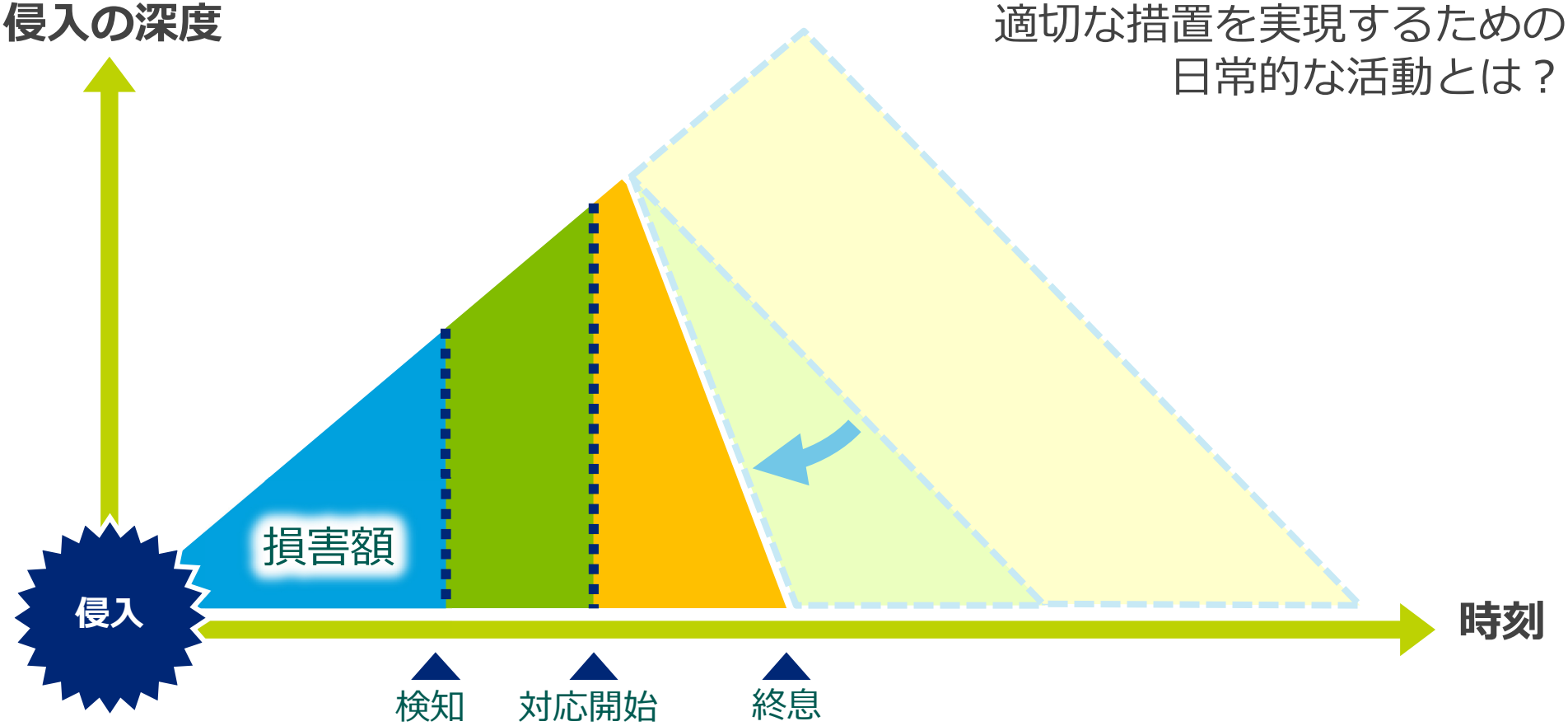
検知はインシデント対応の大前提。
未知の攻撃や長期の潜伏を
如何に検知するのか？



日頃の準備が被害の軽減に大きく寄与

早期終息によるアプローチ – CSIRTの場合

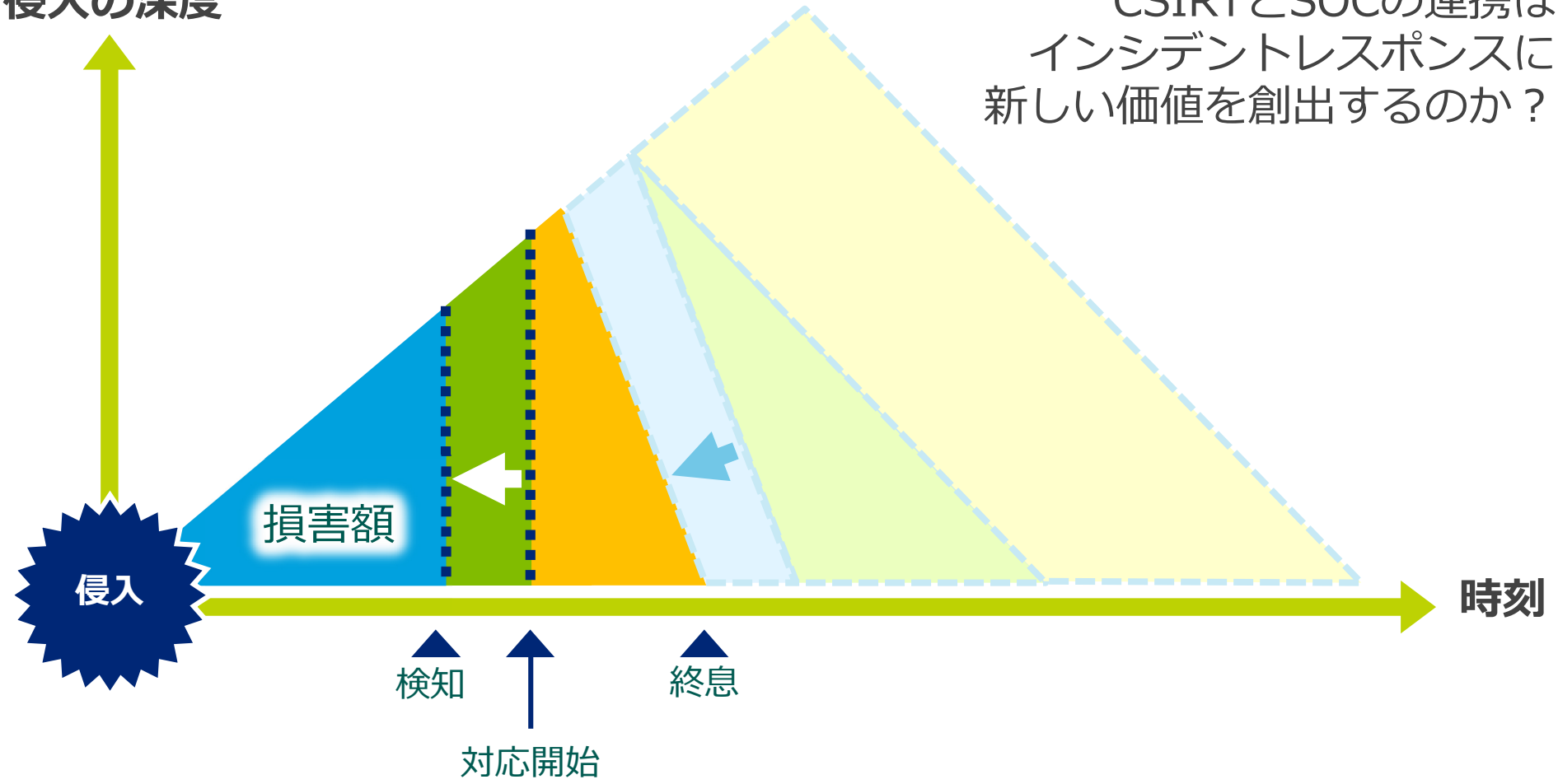
適切な対応なくしてインシデントは終息しない。
適切な措置を実現するための
日常的な活動とは？



早期の対応開始はSOCとCSIRTの共同作業

早期対応開始 – SOCとCSIRT、それぞれの立場で考える

適時の対応開始、適切な対応の実現。
CSIRTとSOCの連携は
インシデントレスポンスに
新しい価値を創出するのか？



まとめ

1	「ひと」が情報管理に関して最も脆弱な点となる時代、 サイバー攻撃による被弾は不可避
2	インシデントレスポンスの新潮流 受動的な対応から能動的なダメージコントロールへの意識転換
3	ダメージコントロールの実現に向けて、 SOC/CSIRTは何をすべきで、どのように連携すべきか？

Deloitte. トーマツ.

トーマツグループは日本におけるデロイト トウシュ トーマツ リミテッド（英国の法令に基づく保証有限責任会社）のメンバーファームおよびそれらの関係会社（有限責任監査法人トーマツ、デロイト トーマツ コンサルティング株式会社、デロイト トーマツ ファイナンシャルアドバイザリー株式会社および税理士法人トーマツを含む）の総称です。トーマツグループは日本で最大級のビジネスプロフェッショナルグループのひとつであり、各社がそれぞれの適用法令に従い、監査、税務、コンサルティング、ファイナンシャルアドバイザリー等を提供しています。また、国内約40都市に約7,800名の専門家（公認会計士、税理士、コンサルタントなど）を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はトーマツグループWebサイト（www.deloitte.com/jp）をご覧ください。

Deloitte（デロイト）は監査、税務、コンサルティングおよびファイナンシャル アドバイザリーサービスをさまざまな業種にわたる上場・非上場クライアントに提供しています。全世界150を超える国・地域のメンバーファームのネットワークを通じ、デロイトは、高度に複合化されたビジネスに取り組むクライアントに向けて、深い洞察に基づき、世界最高水準の陣容をもって高品質なサービスを提供しています。デロイトの約200,000名を超える人材は、“standard of excellence”となることを目指しています。

Deloitte（デロイト）とは、英国の法令に基づく保証有限責任会社であるデロイト トウシュ トーマツ リミテッド（“DTTL”）ならびにそのネットワーク組織を構成するメンバーファームおよびその関係会社のひとつまたは複数を指します。DTTLおよび各メンバーファームはそれぞれ法的に独立した別個の組織体です。DTTL（または“Deloitte Global”）はクライアントへのサービス提供を行いません。DTTLおよびそのメンバーファームについての詳細は www.deloitte.com/jp/about をご覧ください。

本資料は、デロイト トウシュ トーマツ リミテッド、そのメンバーファームあるいはそれぞれの関連事業体（総称して“デロイトネットワーク”）の社員・職員のための、内部限の資料です。その趣旨に反して、本資料を利用して生じることのある損失等に対し、デロイトネットワークの社員・職員の責任に帰するものではありません。

有限責任監査法人トーマツ 東京事務所 エンタープライズ リスク サービスは、2006年2月8日、監査法人として初めて情報セキュリティマネジメントの国際規格であるISO/IEC27001の認証を取得しました。
2009年4月1日には、デロイト トーマツ リスク サービス株式会社をこの認証範囲に含めております。

IS 501214 / ISO (JIS Q) 27001

有限責任監査法人トーマツ 東京事務所におけるBCP/BCMサービス提供部門およびデロイト トーマツ リスクサービス株式会社は、2011年3月11日に事業継続マネジメントシステムの規格であるBS25999-2:2007の認証を取得し、2013年2月19日に国際規格であるISO22301:2012の認証を取得しました。

BCMS 568132 / ISO 22301

Member of
Deloitte Touche Tohmatsu Limited