NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

中小企業のための Security by Design WG 活動紹介

NPO 日本ネットワークセキュリティ協会
西日本支部
株式会社インターネットイニシアティブ
大室 光正

Summary

WG 活動紹介

本日のセッション振り返り

Summary

WG 活動紹介

本日のセッション振り返り

WGの活動目的

中小企業のための Security by Design WG

「これまでの西日本支部の活動の成果物を元に、中小企業の情報システム部門が考えるべき導入、運用、廃止までのライフサイクルを考慮した情報セキュリティシステムの姿を検討する」

Security by Design?

情報セキュリティを企画/設計段階から確保するための方策

- 事後対応的というより事前予防的
- By design であって by security ではない

Security by Design?

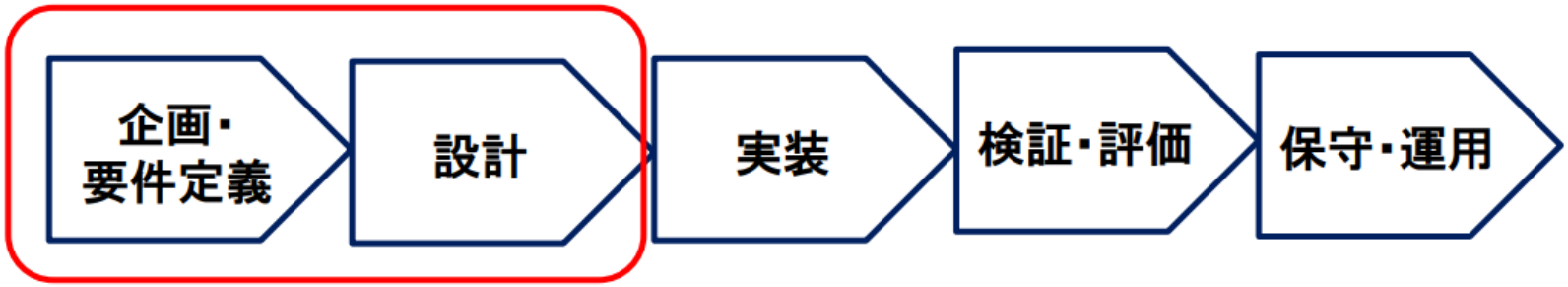
by IPA

JNSA

セキュリティ・バイ・デザインの定義(NISC)

SEC Software Reliability Enhancement Center

「情報セキュリティを企画・設計段階から確保するための方策」



”情報セキュリティ”でなく、”セキュリティ”とすればIoT製品やサービスにも適用できると考えられる。

IPA Software Reliability Enhancement Center

Security by Design?

by NISC

JNSA

情報セキュリティを企画・設計段階から確保するための方策（SBD(Security by Design)）

NISC

問題認識： 行政情報システムの企画・設計段階から情報セキュリティ対策を考慮すべき

SBD検討会構成員
（座長）東工大 山岡准教授
（委員）大手ベンダー、システム関連事業者関連団体、府省庁CIO補佐官 等
（オブザーバ）関連府省庁 等

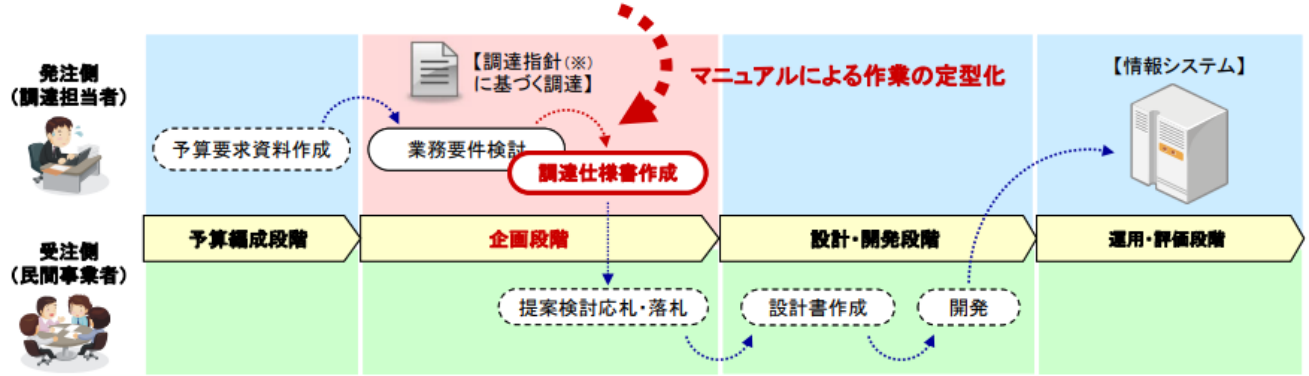
『情報セキュリティを企画・設計段階から確保するための方策に係る検討会（SBD検討会）』を設置

■ 検討課題
- ✓ 調達仕様書の「**情報セキュリティ要件の不明瞭さ**」から、調達者と供給者の合意形成に支障を来す。
- ✓ 結果として、「**不公平な調達**」、「**過度なセキュリティ対策**」、運用開始後の「**セキュリティ事故**」を招くおそれ。

■ 解決方針
- ✓ 調達担当者が調達仕様書作成時に「**情報セキュリティに係る仕様**」を適切に組み込める方法を確立する。

検討成果

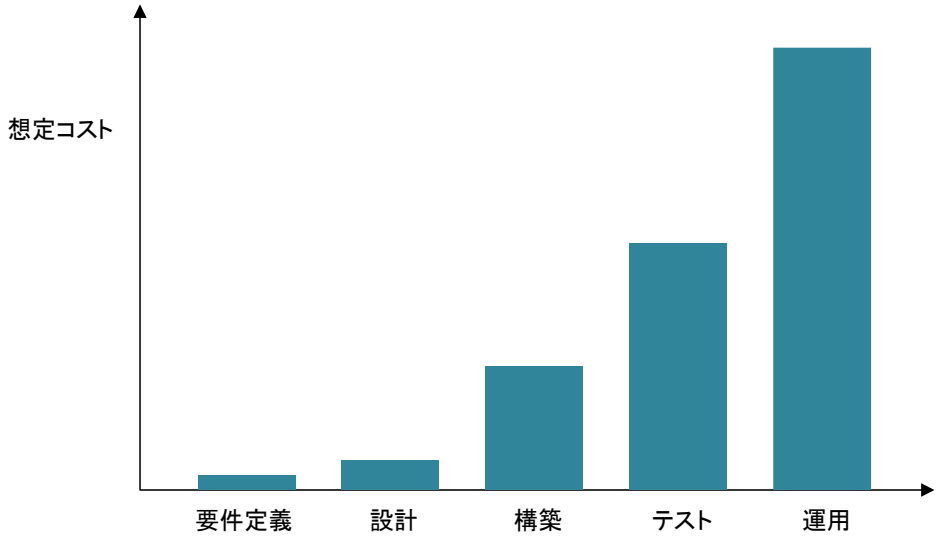
『情報システムに係る政府調達におけるセキュリティ要件策定マニュアル』
- 調達担当者がシステム特性に応じて「**調達仕様書にセキュリティ要件を記載する方法**」を解説
- 「**対策要件集**」及び「**対策要件選定作業の定型化**」等のツールによる調達担当者の支援



※ 調達指針：情報システムに係る政府調達の基本指針（H19.3.1 CIO 連絡会議決定）

Security by Design?

後工程での修正ほどコストは増加傾向



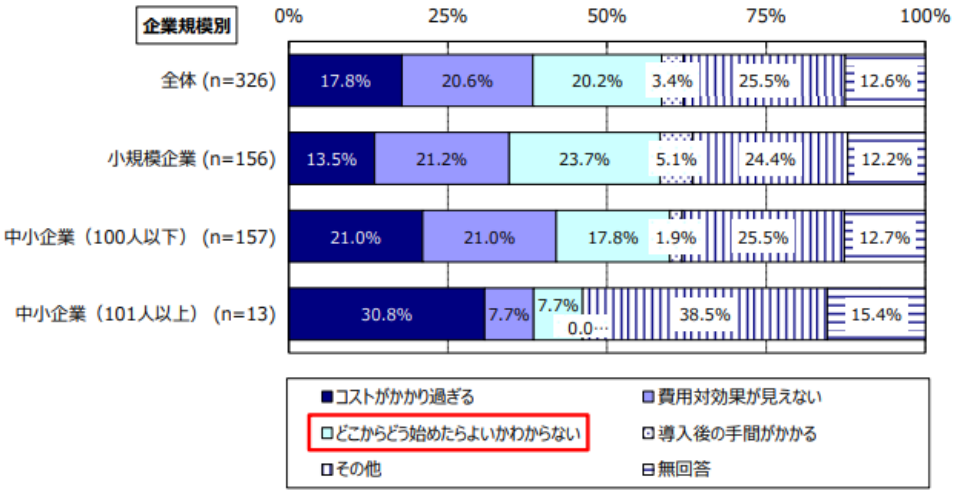
企画・設計段階からセキュリティを考慮した設計(=Security by Design) が推奨される

何から着手すればよいのか

3. 調査結果（アンケート調査）
IT投資の実態

- 情報セキュリティ対策投資がIT投資に含まれない理由として一番多いのは、小規模企業では「どこからどう始めたらよいかわからない」で23.7%
  - 「どこからどう始めたらよいかわからない」と回答した割合は、小規模企業で23.7%、100人以下の中小企業で17.8%、101人以上の中小企業で7.7%である。

Q5-4　情報セキュリティ対策に関する投資が含まれていない理由は何ですか。（○は1つ）
※回答者：Q5-2で「2.含まれていない 」と回答



13

何から着手すればよいのか

情報セキュリティ対策がIT投資に含まれない理由

TOP3

・コストがかかり過ぎる
・費用対効果が見えない
・どこから始めたらよいかわからない

絞り込みは難しい

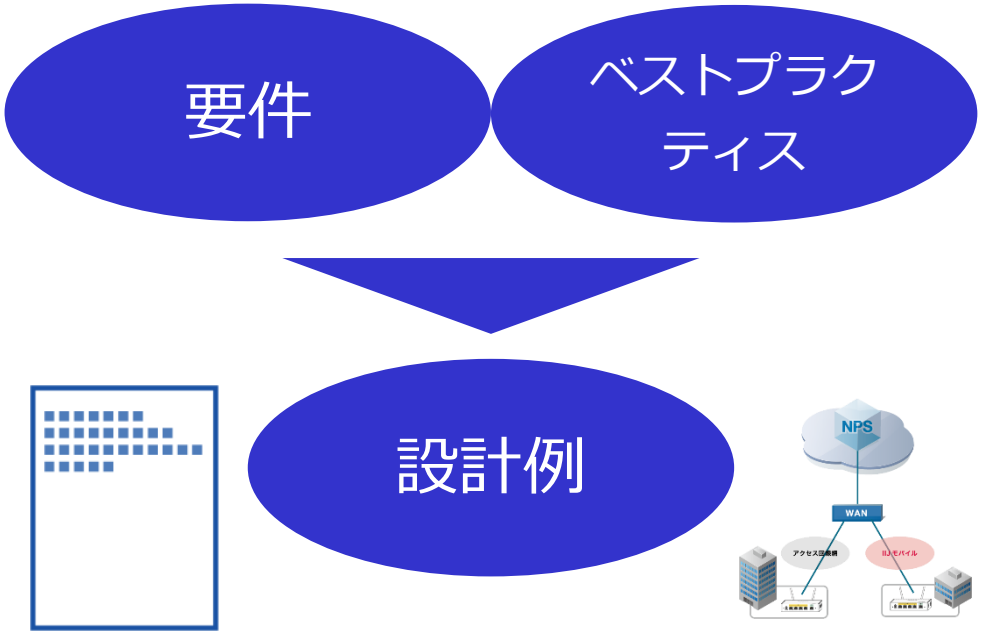
具体的な要件定義・設計の参考情報になると、
とたんに内容が複雑/膨大になってくる。

分析などの手法で必要な防御策を絞り込むのも
多大な工数が発生する。

もっと簡単にできないか

小規模な組織でも脅威分析/要件抽出の手法を活用できるような簡略化ができないか。

たたき台を作り、検討してみたものの・・・



複雑化していく成果物

様々な脅威や手法を検討する毎に複雑化。

■分類した対象毎にセキュリティ要件を整理・収集する

利用者に関する質問				分類した利用者毎の回答				セキュリティ要件	
大項目	小項目	質問の説明	質問の選択肢					要件項目	優先度(A>B>C)
A. 利用者	A-1. 利用者属性	システムを利用するために実名登録は必要か。(匿名/非匿名) また利用に際して申請及び許可は必要か(特定/不特定)	特定 (許可された利用者のみ利用可能)					1.1.1 通信制御 1.1.2 ネットワーク分離 1.1.7 リモートアクセス 1.2.3 アクセス認証 1.2.4 アクセス認可	A B B A A
	A-2. 利用者数	利用者数はどの 想定されている							
	A-3. 一人当たり								

セキュリティ要件項目		要件例	要件の説明
1.1 攻撃侵入口の最小化(入口対策)	1.1.1 通信制御	① FW導入によるトラフィックフィルタリング	ネットワークを内部と外部に分離し、トラフィックを制御する。
		② UTM導入によるトラフィックフィルタリング	ネットワークを内部と外部に分離し、トラフィックを制御する。
		③ OS標準機能の利用（FW等）	ネットワーク内部のシステム毎に通信ポリシーを設定する。
	1.1.2 ネットワーク分離	① VLANによるNW分離	内部ネットワークを重要度や通信ポリシーに応じて分離する。
		② 外部からアクセスのあるシステムのクラウド移行	外部ネットワークを通信ポリシーに応じてアウトソースする。
	1.1.3 マルウェア検知	① WAF・UTMの利用	
		② リバースProxyサービスの利用	
		③ 外部からのアクセスのあるシステムのクラウド移行	
	1.1.4 侵入検知	① IDS/IPSの導入	
		② 外部からアクセスのあるシステムのクラウド移行	
	1.1.5 スパムフィルタ	① Anti-Spamソフトウェアの利用	
		② メールゲートウェイ等のクラウドサービスの利用	
	1.1.6 アンチウイルス	① Anti-Virusソフトウェアの利用	
		② メールゲートウェイ等のクラウドサービスの利用	
	1.1.7 リモートアクセス	① VPNの利用	許可された利用者のみシステムを利用できるようにし、盗聴を防止する。
		② 接続元の制限	許可された接続元のみシステムを利用できるようにする。
	1.1.8 外部媒体/不要ソフトウェアの利用制限	① デバイス制御ソフトウェアの利用	
	1.4.3 障害対応	① プロセス自動起動設定の利用	OS等に用意された自動復旧機能の利用を検討する。
		② サービス正常確認手順の準備	定義に従い、サービスが正常かどうかを確認できる手順を用意する。
		③ サービス停止時の復旧手順の準備	監視アラートに対応する復旧手順を用意する。
		④ インシデント発生時の対応フロー準備	インシデント発生時の体制、連絡方法及び各組織の対応を用意する。
		⑤ バックアップ/リカバリ手順の準備	バックアップからデータ/システムをリカバリする手順を用意する。

扱う情報に関する質問

大項目	小項目	質問の説明	質問の選択肢
B. 情報	B-1. 外部公開の可否	関係者外秘の情報か。公開情報	公開
			非公開
	B-2. 情報へのアクセス権限	利用者がどの情報を読み取り/書き込みできるか。	
	B-3. 情報を送受信する方法	その情報はどのような方法で送受信されるか。	Web
			メール
			ファイル転送
			その他コマンドライン等
			物理媒体経由(USB等)
	B-3. 保存期間	その情報はどの程度の期間、システム内に保持する必要が	キャッシュのみ
			数カ月単位
			数年単位
	B-4. 記録媒体	その情報はシステムで利用される際、どこに保存されてい	ストレージ(HDD等)
			可搬媒体(USBメモリ等)
	B-5. 漏洩時の影響度	その情報が参照する権限の無	金銭被害大（数十万円以上）
			金銭被害小（数万円以下）
			金銭被害なし
			回復不能なプライバシー侵害
			回復可能なプライバシー侵害
			プライバシー侵害なし
			金銭被害大（数十万円以上）
			金銭被害小（数万円以下）
			金銭被害なし
			回復不能なプライバシー侵害
			回復可能なプライバシー侵害
			プライバシー侵害なし

様々な脅威や攻撃手法を検討する毎に
内容が増えていく
目的(簡略化)を見失っている

例：毎年発表される新しい脅威

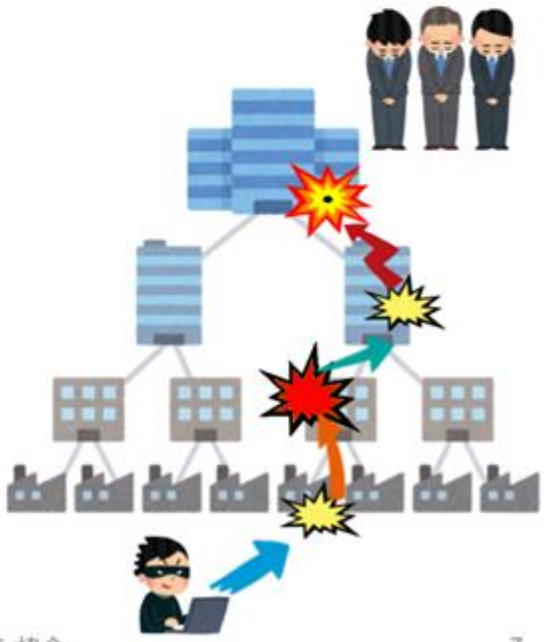
■IPA 情報セキュリティ10大脅威 2019

昨年順位	個人	順位	組織	昨年順位
1位	クレジットカード情報の不正利用	1位	標的型攻撃による被害	1位
1位	フィッシングによる個人情報等の詐取	2位	ビジネスメール詐欺による被害	3位
4位	不正アプリによるスマートフォン利用者の被害	3位	ランサムウェアによる被害	2位
NEW	メールやSNSを使った脅迫・詐欺の手口による金銭要求	4位	サプライチェーンの弱点を悪用した攻撃の高まり	NEW
3位	ネット上の誹謗・中傷・デマ	5位	内部不正による情報漏えい	8位
10位	偽警告によるインターネット詐欺	6位	サービス妨害攻撃によるサービスの停止	9位
1位	インターネットバンキングの不正利用	7位	インターネットサービスからの個人情報の窃取	6位
5位	インターネットサービスへの不正ログイン	8位	IoT機器の脆弱性の顕在化	7位
2位	ランサムウェアによる被害	9位	脆弱性対策情報の公開に伴う悪用増加	4位
9位	IoT 機器の不適切な管理	10位	不注意による情報漏えい	12位

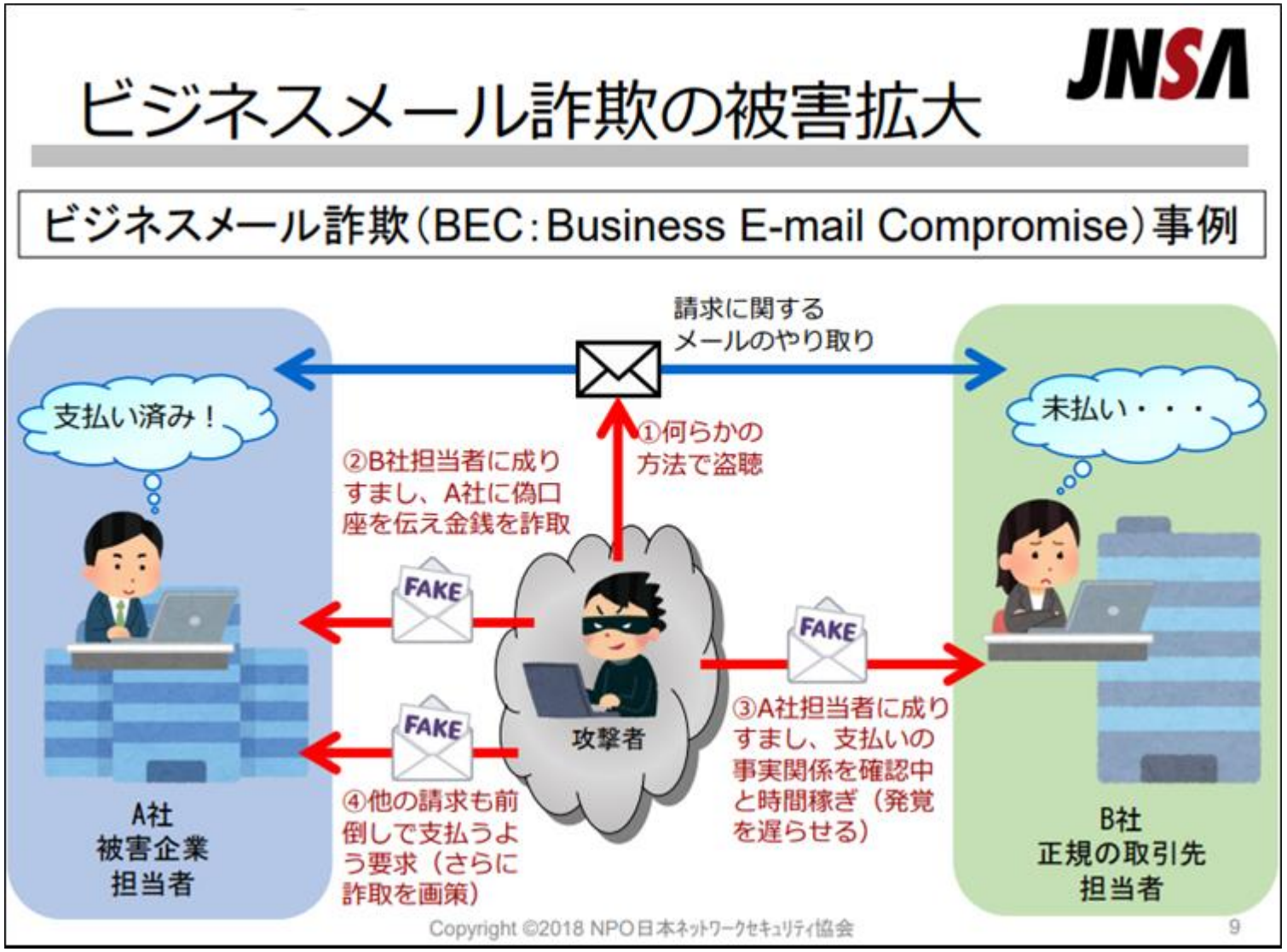
例：想定外の攻撃

サプライチェーン攻撃で鉄壁の守りも突破

- ビジネス活動の流れ(サプライチェーン)の途中を攻撃し、最終的にターゲットを攻撃する。
  - 大企業や政府組織などを攻撃するため、防御の手薄なビジネスパートナー等を“侵入口”として攻撃。そこからターゲットの組織へ潜入する。
  - 多くの組織が利用している製品・ソフトウェア等の開発元などに侵入し、密かにマルウェア等を混入し、それを利用している組織を攻撃する。



例：様々な運用現場


ビジネスメール詐欺の被害拡大
ビジネスメール詐欺（BEC：Business E-mail Compromise）事例
請求に関する
メールのやり取り
支払い済み！
未払い・・・
①何らかの
方法で盗聴
②B社担当者に成り
すまし、A社に偽口
座を伝え金銭を詐取
FAKE
FAKE
FAKE
攻撃者
③A社担当者に成り
すまし、支払いの
事実関係を確認中
と時間稼ぎ（発覚
を遅らせる）
④他の請求も前
倒しで支払うよ
う要求（さらに
詐取を画策）
A社
被害企業
担当者
B社
正規の取引先
担当者
Copyright ©2018 NPO日本ネットワークセキュリティ協会
9

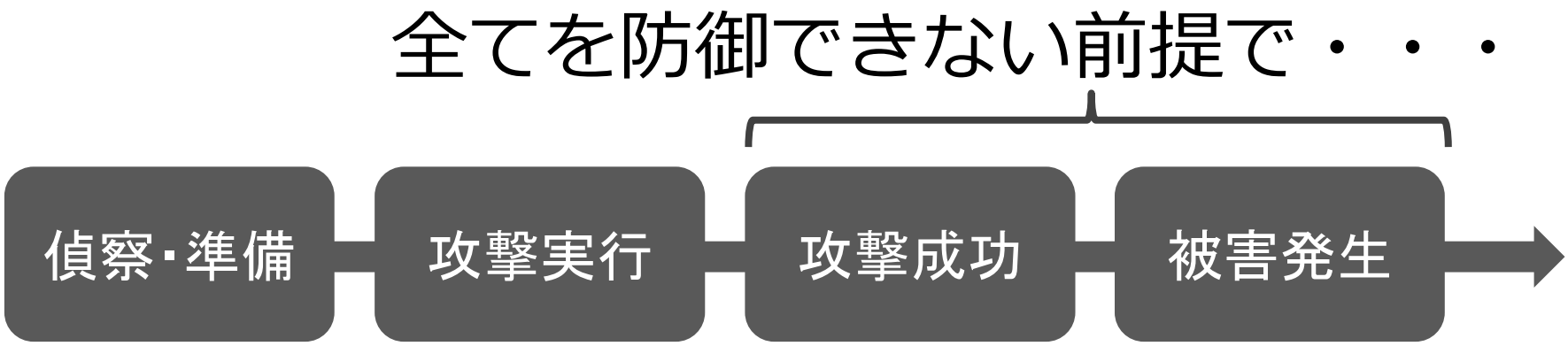
全てをカバーするのは難しい

脅威や防御策の網羅は困難。必要な対策の絞り込みをかけるのも大変な作業となる。

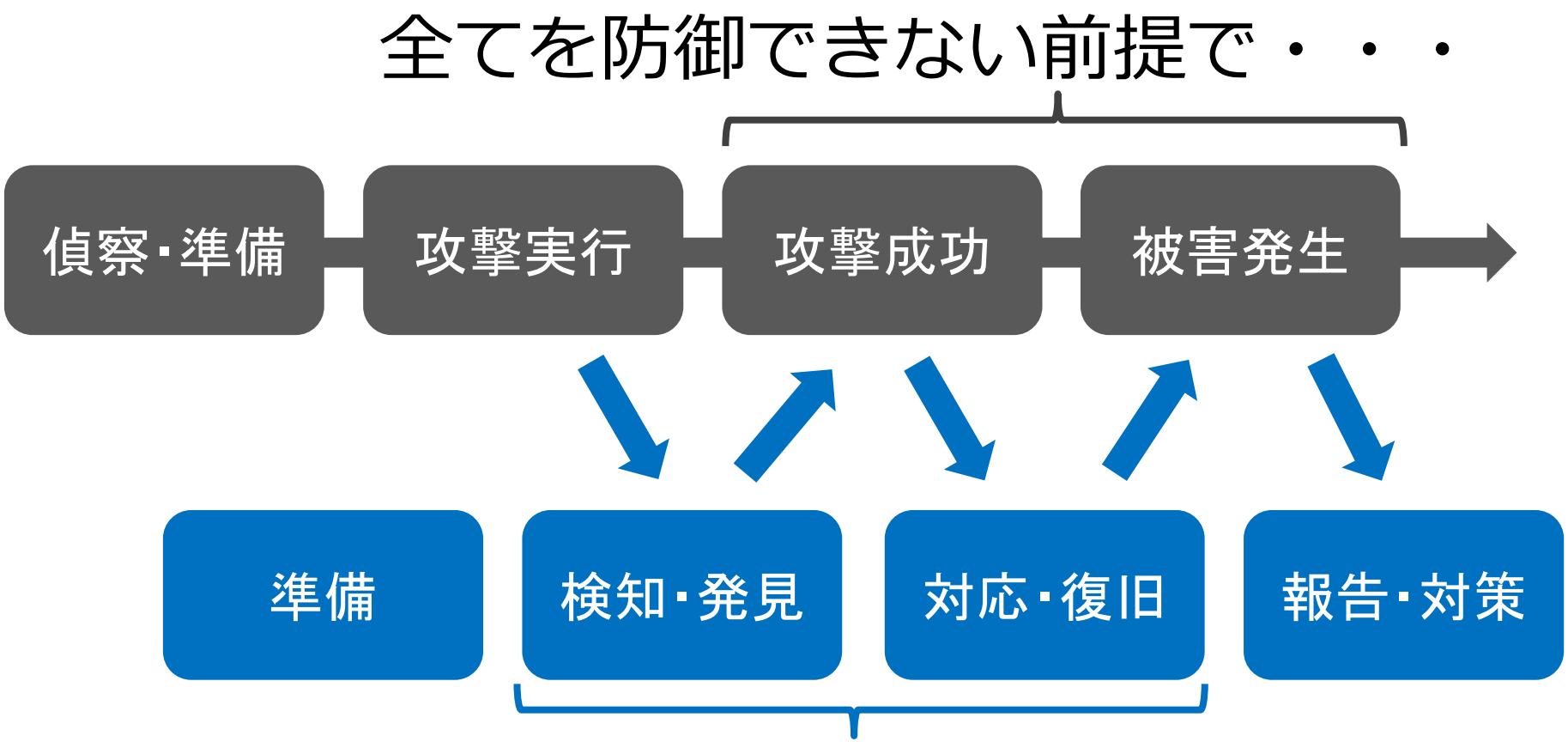
- 日々発見される新たな脆弱性
- 攻撃手法の高度化
- 対策の回避
- 様々な運用現場 etc..

参考：https://www.iij.ad.jp/dev/report/

全てを防御できない前提での対策



全てを防御できない前提での対策



運用での対処を用意しておく必要がある。

まとめ

様々なアプローチがある中、早期発見/早期対処をテーマにした情報セキュリティシステムの姿を検討し、設計着手ポイントを具体的に提示できないか。

現在、ＷＧで検討を行っています。

本日のセッション全体を振り返り、その中で意見交換できればと考えています。

Summary

WG 活動紹介

本日のセッション振り返り

本日のセッション振り返り