TLP:GREEN

これからの経営層が担うべきセキュリティ統制力向上への役割について

～徹底的な現状認識に基づく事前準備と事後判断における重要ポイントとは？～

2019年 2月

名和 利男

アジェンダ

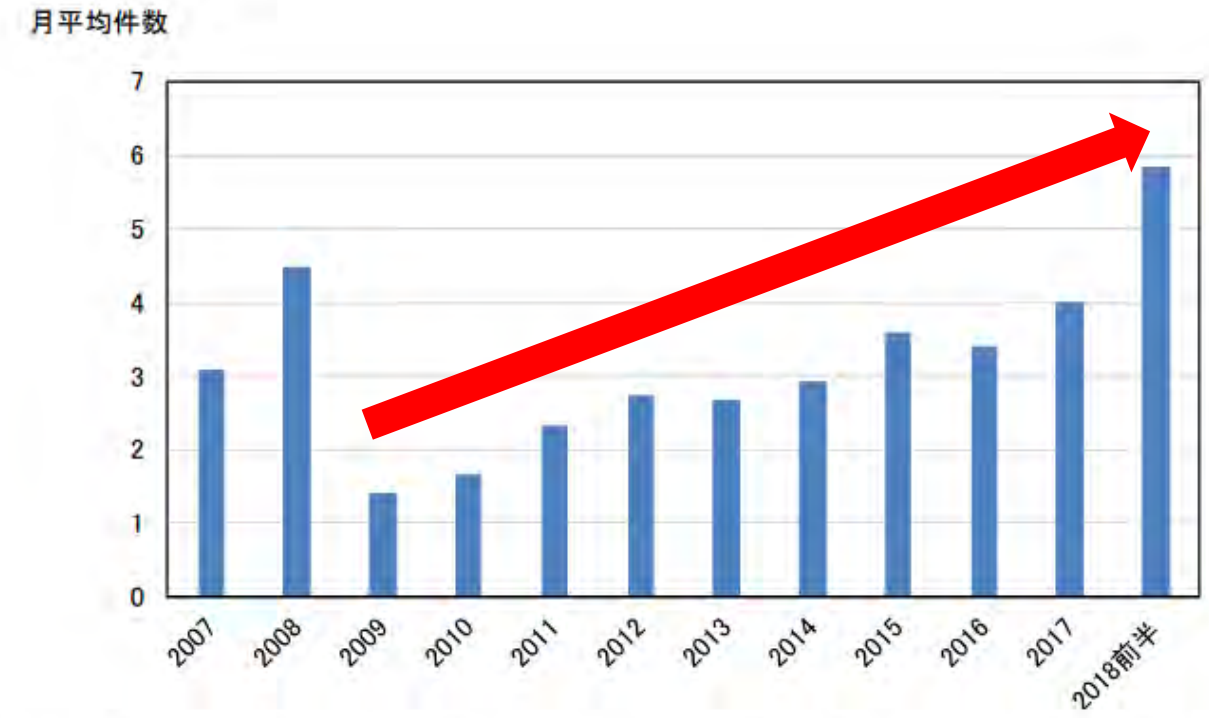
1. 「不具合・エラーによるシステム障害」と「サイバー攻撃による機能喪失」の違いついて
2. サイバー攻撃発生後の「組織内の混乱及び困難」への対処
3. 交通分野の経営層が(特に)認識すべき「2020年までのサイバー環境の変化」
4. 最悪のサイバー攻撃シナリオと「事案対処態勢」の構築

トピック 1

「不具合・エラーによるシステム障害」と「サイバー攻撃による機能喪失」の違いについて

システム障害発生の件数は増加傾向

2018 年の前半に報道された障害 35 件の概要は表 1 に示すとおりである。今期の発生件数は月平均 5.8 件と、かなり高い水準である（図 1）。なお、別表 1 は障害の影響範囲が特定の自治体に閉じ、広域にわたる影響はなかったものの、その地域にとっては影響が大きかった事例を取りまとめたものである。



発生件数	37	54	17	20	28	33	32	35	43	41	48	35

出典: IPA 情報システムの障害状況 2018 年前半データ https://www.ipa.go.jp/files/000070130.pdf

TLP:GREEN

(10年前から指摘されている)経営層によるシステム(障害)への積極的関与 (1)

連載　2012/10/29 08:00:00

システム障害はなぜ繰り返されるのか?

第1回

システム障害は経営者の責任だ!

重要情報を扱うITシステムを第三者に任せていいの?

ITシステムの開発や運用を子会社やITベンダーといった第三者に任せてしまう(アウトソーシング)企業があるが、本当にそれでよいのだろうか?

日本企業がシステム開発や運用をアウトソーシングしてしまう理由として、IT部門の人材不足を挙げることがよくある。実際、日本のIT部門の人員は少なく、役割はIT企画やプロジェクト管理、運用管理が多く、実際のプログラム開発やアーキテクチャの構築などは行わない。

米国企業はITシステムが経営を左右していることを十分理解しているため、他人に任せるようなことはしない。自分で運転する米国企業と、タクシーに乗って後部座席で行き先を指示している日本企業では大きな差となり、この差が企業競争力、企業価値の差を生んでいるとも言えるのではないだろうか?

https://news.mynavi.jp/article/sysfailure-1/

2009/10/22 00:00

すごい現場

[なぜ繰り返すのか?システム障害]経営陣がシステムに無関心

https://tech.nikkeibp.co.jp/it/article/COLUMN/20090323/327025/

TLP:GREEN

(10年前から指摘されている)経営層によるシステム(障害)への積極的関与 (2)

2017/09/19 05:00

木村岳史の極言暴論！

「システム障害は絶対に起こしてはならぬ」と叫ぶ馬鹿に付ける薬

「馬鹿に付ける薬はない」ということわざがある。思慮が足らず物事の道理が分からない人は救いようがないとの意味だが、「システム障害は絶対に起こしてはならぬ」と声高に叫ぶような“馬鹿”に付ける薬はないものだろうか。もしそうだとすると本当に困る。この手の主張は、言っている本人が救いようのないだけでは済まされない。こんな論がまかり通っていると、多くの人を不幸にし続けるので、ぜひとも完治させる薬が欲しい。

https://tech.nikkeibp.co.jp/it/atcl/column/14/463805/091400156/

2017.8.10

「経営者」が本気にならないプロジェクトが泥沼化する理由

「システムに欠陥が多すぎて使えない！」
「開発や保守・運用費用が高すぎる！」
「なぜか社員が協力してくれない……」
「経営者がシステムのことを全然わかってない……」

簡単に言えば、「ＩＴシステムの導入によってコスト削減や売上向上に成功し、**会社が利益を増やすことができたとき**」に、初めて成功と言えるわけです。

当然のことと思われるかもしれませんが、そもそもシステムの企画に誤りがあって、**導入しても効果のないシステムを導入したら、いくらＱＣＤを遵守したところで「成功」したことにはなりません。**

逆に、**大幅に納期が遅れたり、不具合のあるシステムだったとしても、経営に資するならプロジェクトは成功したと言える**のです。

しかし、こういうものの見方や判断、システム担当者レベルは難しいでしょう。

https://diamond.jp/articles/-/137866

TLP:GREEN

(10年前から指摘されている)経営層によるシステム(障害)への積極的関与 (3)

システム障害は、経営層と業務部門の責任

今やITシステムはビジネスの遂行に不可欠なもの。その要件をビジネスサイドの人間がしっかりと考えなければ、ビジネスに役立つシステムなど作れるわけがない。

2011年08月09日 12時00分 公開　　[@IT情報マネジメント編集部，@IT]

言ってみれば、ITシステムはビジネスそのものであり、テクノロジはビジネスを遂行するための手段に過ぎない。にもかかわらず、多くの場合、システムを使う側が考えるべきことを考えず、システム導入時には不毛な機能比較や価格比較に陥り、障害時には「開発した会社はどこか」といった犯人探しが始まる――本書を読めば、こうした丸投げ体質の異常さを客観的に理解できるのではないだろうか。

なお、本書では事例の分析を基に、「動かないコンピュータ撲滅のための十カ条」と題し、「経営トップが先頭に立ってシステム導入の指揮を執る」「自社のシステム構築に関する力を見極め、無理のない計画を立てる」など、あるべきシステム開発のポイントを詳細にまとめている。事例と合わせて読めば、ビジネスサイドの人、システム関係者、双方にさまざまな気付きをもたらしてくれるはずである。ぜひ手に取ってみてはいかがだろうか。

http://www.itmedia.co.jp/im/articles/1108/09/news106.html

2017/11/30 05:00

システム開発トラブルに見舞われたら…

経営者の思い付きがシステム開発を迷走させる、完成後も問題が多発

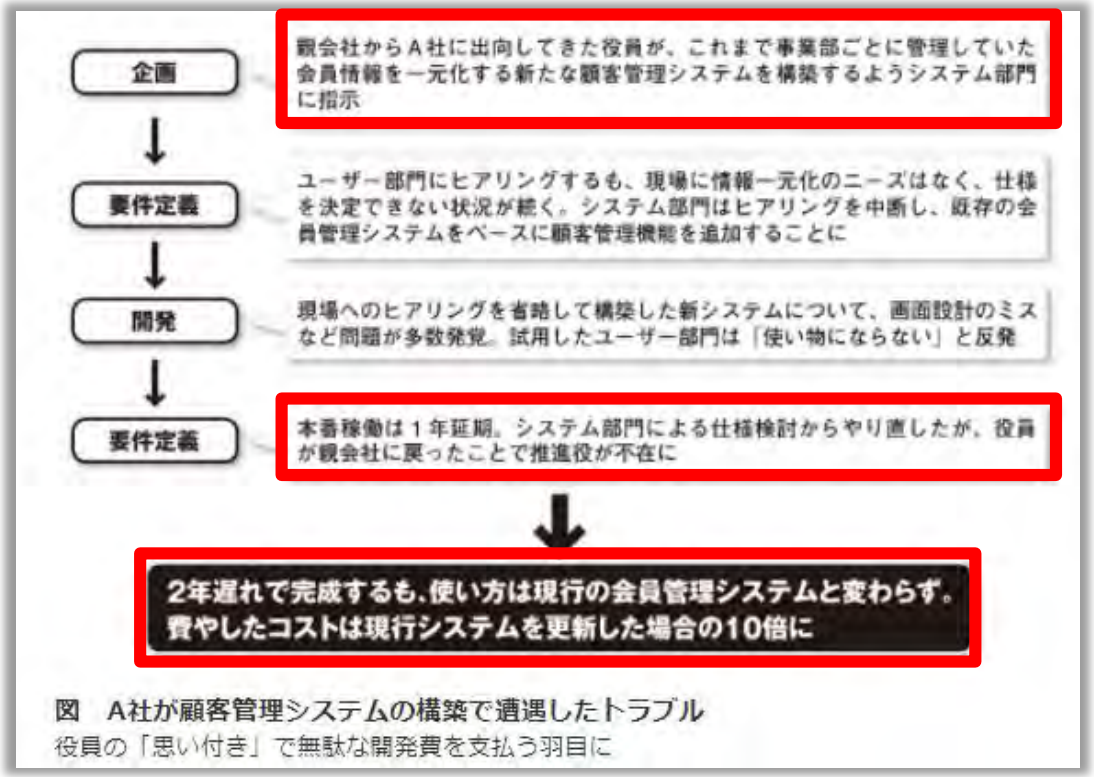


図　A社が顧客管理システムの構築で遭遇したトラブル
役員の「思い付き」で無駄な開発費を支払う羽目に

https://tech.nikkeibp.co.jp/it/atcl/column/17/110600484/110900008/

TLP:GREEN

最近の「サイバー攻撃による機能喪失」の例：
2018年5月 デンマークの鉄道会社DSBへのDDoS攻撃

- 2018年5月13日(日曜日)の夜、デンマークの鉄道会社DSB(Danske Statsbaner)がDDoS攻撃を受け、**DSBアプリ、Webサイト、チケット販売機、駅構内のセブンイレブンのキオスクで切符購入ができなくなった**。
  - Rejsekort トラベルカードを持っていた乗客は、列車内の乗務員から切符を購入できたが、約15,000の顧客が影響を受けたと推定。
  - これに対し、DSBの広報担当は、「本事案に関する専門家を迎え入れており、明日の朝までに、すべてのシステムを通常稼働にする」と伝えた。
- このDDoS攻撃の発生と同時に、**内部メールシステムと電話インフラが使用不能**になった。
  - そのため、顧客とコミュニケーションをとる方法は、ソーシャルメディアのみとなった。

https://twitter.com/omDSB/status/995711445454196737

現在、dsb.dkサイト、販売チャネル、交通情報、電話回線に関する技術的な問題が発生しています。私たちはこのエラーを解決するために取り組んでいます。

https://twitter.com/omDSB/status/995898708700123136

dsb.dkサイトへのアクセスエラーが継続して発生していることを認識しました。一部誤解されていますが、私たちはその問題に取り組んでいます。

TLP:GREEN

最近の「サイバー攻撃による機能喪失」の例：
【背景】デンマークにおけるデジタル化とサイバー脅威の高まり

- 2018年、**デンマークは国家戦略「デジタル化のフロントランナーになる」**を発表し、2025年までに約170億円を確保し、デジタル化を推進している。
  - デンマークは、3年連続EU内で最もデジタル化が進んでいる国として有名
- デンマークにおけるデジタル化の特徴
  - 小国(小さいところに多くの要素が集積しているため、アクションを取りやすい)、社会保障国家、民主主義国家であること
  - ビッグデータ(スマートフォンから得られる位置情報や、サーバー上のメール、カード会員情報など、ビジネスに役立てるための膨大で複雑な情報)が集積している
  - オープンイノベーション(自社だけでなく他社や大学、自治体など、外部のテクノロジーやアイデア、ノウハウ、データなどを組み合わせイノベーションを促進していくビジネスモデル)

オープンイノベーションが進展していくと同時に、
攻撃者は、重要インフラ分野で実装された(新しい)技術情報を得やすくなる。

「不具合・エラーによるシステム障害」vs「サイバー攻撃による機能喪失」

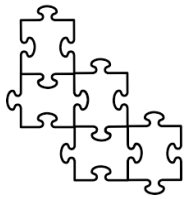
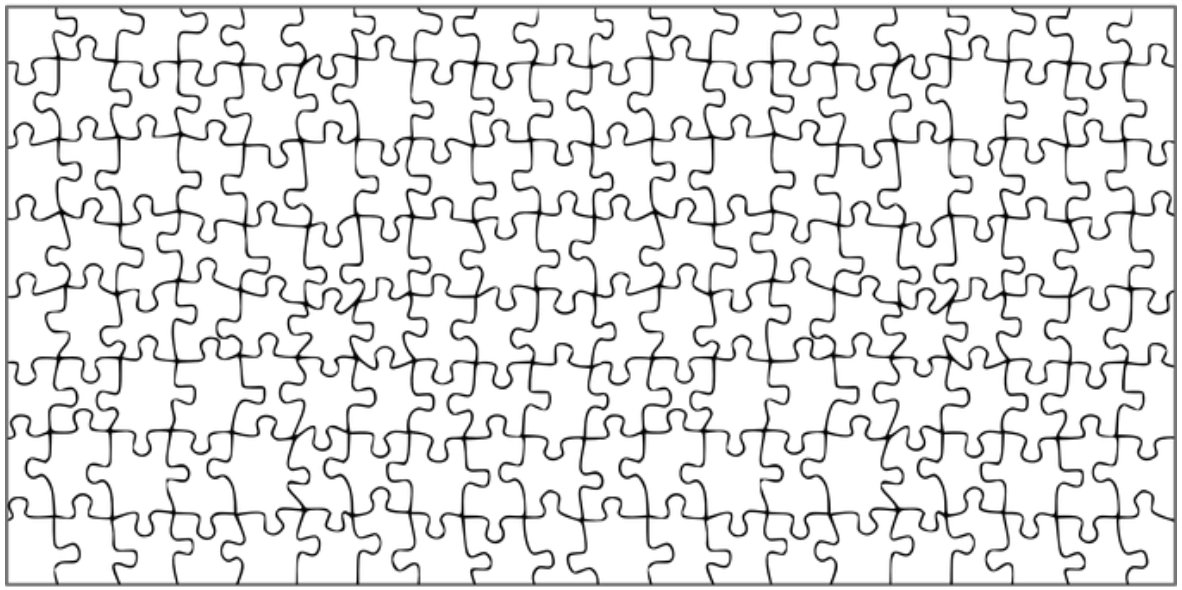
	「不具合・エラーによるシステム障害」	「サイバー攻撃による機能喪失」
経営層の指示	**原因究明、早期復旧、再発防止**	**原因究明、早期復旧、再発防止**
インシデントの**特性**	• メカニズムは固定的 • 偶発的に発生 • 原因は(以前から)システム内に存在	• メカニズムは**変動的(第三者が変化させる)** • **第三者の悪意のある活動**により発生 • 原因は**(第三者により)システム外で作られる**
現場に必要な**経験・能力**	• システム及びネットワーク構成に関する知識と設定状況の即時把握(ほぼ固定的) • システムが業務に与える影響(ほぼ固定的)	• システム及びネットワーク構成に関する知識と設定状況の即時把握(ほぼ固定的) • システムが業務に与える影響(ほぼ固定的) • **サイバー攻撃の知識(日々更新する)** • **フォレンジックの知識とリテラシー(日々更新する)** • **セキュリティ対策の知識とリテラシー(日々更新する)** • **説明力及びプレゼンテーション力(相手により変化)**
主な**再発防止策**	• 開発及び保守の体制・プロセスの厳格化	• 開発及び保守の体制・プロセスの厳格化 • **監視強化、サイバー能力構築、連携強化(訓練)等**

「不具合・エラーによるシステム障害」vs「サイバー攻撃による機能喪失」

	「不具合・エラーによるシステム障害」	「サイバー攻撃による機能喪失」
現場に(必然的に)求められる **スキル・能力**	• インターネットのアーキテクチャ、理念、将来像に関する知識 • ネットワークインフラのリテラシーと設計思想の理解 • ネットワークプロトコルの深い理解 • ネットワークアプリケーション、サービス、関連プロトコルの理解	• インターネットのアーキテクチャ、理念、将来像に関する知識 • ネットワークインフラのリテラシーと設計思想の理解 • ネットワークプロトコルの深い理解 • ネットワークアプリケーション、サービス、関連プロトコルの理解 **• セキュリティの基本原則** **• コンピュータ及びネットワークに対するリスクと脅威の理解** **• セキュリティの脆弱性及びそれを利用した攻撃の理解** **• ネットワーク及びネットワークのためのセキュリティ対策、及びそれらの問題に関する知識と理解** **• 暗号化技術、デジタル署名、ハッシュアルゴリズムの理解** **• プログラミング、ネットワークコンポーネント、基本ソフトウェアの理解と経験** **• コミュニケーション(対人)能力** **• 言語能力** **• 作業編成及びスタッフの統率に係る実務能力** **• 強い目的意識と不屈の精神**

TLP:GREEN

「不具合・エラーによるシステム障害」vs「サイバー攻撃による機能喪失」

	「不具合・エラーによるシステム障害」	「サイバー攻撃による機能喪失」
現場における 対処の**難易度** (イメージ)		

TLP:GREEN

「不具合・エラーによるシステム障害」vs「サイバー攻撃による機能喪失」

	「不具合・エラーによるシステム障害」	「サイバー攻撃による機能喪失」
現場が**立ち向かう対象**(イメージ)		

TLP:GREEN

「不具合・エラーによるシステム障害」vs「サイバー攻撃による機能喪失」

	「不具合・エラーによるシステム障害」	「サイバー攻撃による機能喪失」
インシデント対処に**巻き込まれる範囲**(イメージ)		

TLP:GREEN

トピック２

サイバー攻撃発生後の「組織内の混乱及び困難」への対処

経営層が持つべき「サイバー攻撃による機能喪失」に備えた心構え

- 企業内のそれぞれの部門は、**ICTへの依存や認識・理解の違い、所掌や責任範囲の割り当ての偏り**などが大きい。
  - サイバー攻撃発生時における迅速かつ円滑な対処を実現するには、部門間の相互理解を前提とした緊密連携(阿吽の呼吸)が必要になってくる。
- 「サイバー攻撃による機能喪失」の事態において、経営層(強い権限を持つリーダー)による陣頭指揮が不在である場合、**部門間のコンフリクトに起因した混乱や困難が発生**することが多い。
  - 深刻な被害を発生させたサイバー攻撃を経験した組織の経営層は、事前の心構え(態勢)やセキュリティ対策の不足よりも、インシデント発生直後の部門間の対処行動の不整合による(机上で見積もった計画)の遅延の繰り返しに苛立ちを感じる。
- 一般的に、経営層はサイバー攻撃に対してテクニカルな対処を主導することは難しいと言われている。しかし、対処活動を妨げるような**部門間のコンフリクトに起因した混乱や困難を解決する権限や能力を有している**。
  - リスクアセスメントで得られた脅威シナリオに基づいた訓練を、経営層を巻き込んで実施すべきである。

TLP:GREEN

トピック３

交通分野の経営層が(特に)認識すべき「2020年までのサイバー環境の変化」

今後の日本における**サイバー環境(Cyber Environment)**の変化

【テクノロジー】

- **USBグッズ**のオフィス利用
- ノートPCの**SSD**採用率の増加
- **ビジネスチャット**の利用拡大
- **RCS準拠**のメッセージングサービスの増加
- **キャッシュレス**取引の拡大
- **4K 8Kテレビ**放送の開始
- PSTNから**IP網への移行**
- 高速通信規格**5G**の導入
- 新たな**IoT用無線通信サービス**(LPWA等)
- 次世代無線規格 **Wi-Fi 6**

【Deep Web】

- **オンラインゲーム上のチャット**で闇取引
- オルトコイン情報の流通基盤(**Telegram**)

【対策】

- **CASB**(クラウドセキュリティ)
- EPP/**EDR**(エンドポイントセキュリティ)
- **カード決済のIC対応**(改正割賦販売法)
- **サプライチェーンリスク**の対策(SP800-171)
- **有給休暇**の義務化(働き方改革関連法)

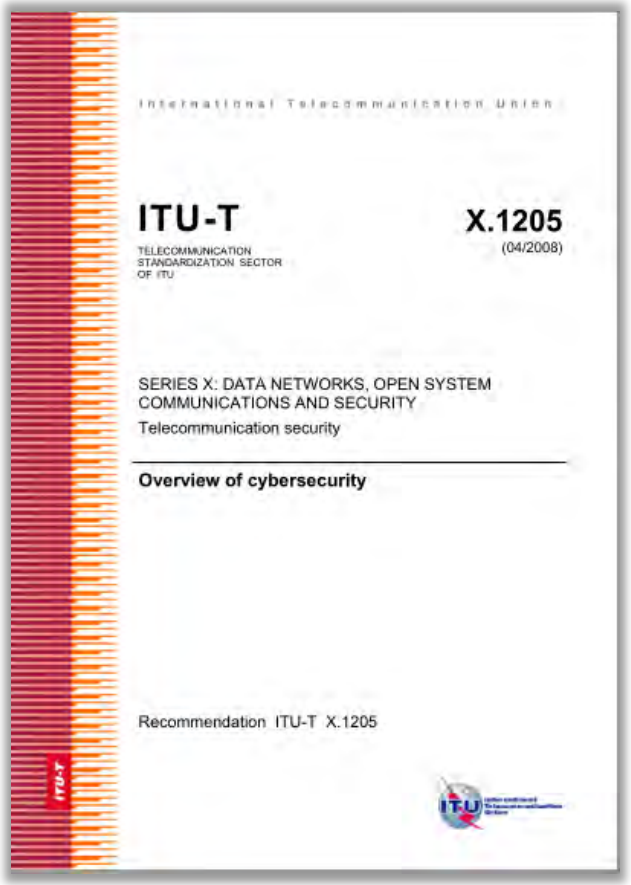
【ビジネス等】

- 少子高齢化に伴う**労働人口の急減**
- ERAB/**ネガワット取引**
- 「**全銀EDIシステム**」の稼働
- **OTT事業**(スポーツ等)の拡大
- 「**スポーツホスピタリティ**」の開始
- **外国人受け入れ**拡大(出入国管理法改正)
- **水道民営化**(水道法改正)

TLP:GREEN

【参考】サイバー環境(Cyber Environment)とは

- サイバー環境(Cyber Environment)には、次の構成要素があると定義されている。
  - ユーザー
  - ネットワーク
  - デバイス
  - 全てのソフトウェア
  - プロセス
  - ストレージ(記憶媒体)或いは経路上の情報
  - アプリーション(特定の作業や業務を目的として基本ソフトウェア上で動作するソフトウェア)
  - ネットワークに直接的及び間接的に接続されることのあるシステム



https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-E&type=items

TLP:GREEN

交通分野の経営層が(特に)認識すべき「2020年までのサイバー環境の変化」

【テクノロジー】

- USBグッズのオフィス利用
- ノートPCのSSD採用率の増加
- ビジネスチャットの利用拡大
- RCS準拠のメッセージングサービスの増加
- キャッシュレス取引の拡大
- 4K 8Kテレビ放送の開始
- PSTNからIP網への移行
- 高速通信規格5Gの導入
- 新たなIoT用無線通信サービス(LPWA等)
- 次世代無線規格 Wi-Fi 6

【Deep Web】

- オンラインゲーム上のチャットで闇取引
- オルトコイン情報の流通基盤(Telegram)

【対策】

- CASB(クラウドセキュリティ)
- EPP/EDR(エンドポイントセキュリティ)
- カード決済のIC対応(改正割賦販売法)
- サプライチェーンリスクの対策(SP800-171)
- 有給休暇の義務化(働き方改革関連法)

【ビジネス等】

- 少子高齢化に伴う労働人口の急減
- ERAB/ネガワット取引
- 「全銀EDIシステム」の稼働
- OTT事業(スポーツ等)の拡大
- 「スポーツホスピタリティ」の開始
- 外国人受け入れ拡大(出入国管理法改正)
- 水道民営化(水道法改正)

TLP:GREEN

トピック 4

最悪のサイバー攻撃シナリオと「事案対処態勢」の構築

最悪のサイバー攻撃(**事案**)シナリオの例

- 「**USBグッズ**のオフィス利用」
  - BadUSBによるデータ破壊を利用した誘導工作
- 「ノートPCの**SSD**採用率の増加」+「次世代無線規格 **Wi-Fi 6**」
  - 痕跡及びログの不足によるインシデントの原因究明の困難化
- 「少子高齢化に伴う**労働人口の急減**」+「**外国人受け入れ**拡大(出入国管理法改正)」
  - 不十分な個人信頼性確認のまま採用した経験の浅い技術者の早期退職による内部情報流出
  - メーカー技術者の常駐困難化により(徐々に)利用が始まる(セキュリティレベルの低い)リモート保守への攻撃
- 「**4K 8Kテレビ**放送の開始」
  - PTP(高精度時間プロトコル)の周波数ソースGPS/GNSSに対するタイムスプーフィング攻撃
- 「**サプライチェーンリスク**の対策(SP800-171)」
  - 制御システムの周辺システム(自動消火、警備、ビル管理、防災等)に対するソフトウェアサプライチェーン攻撃
- 「**水道民営化**(水道法改正)」
  - 浄水場の遠隔監視システムのアカウントハイジャックや中間者攻撃による毒物投入

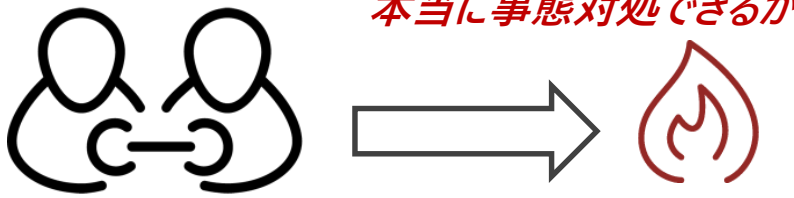
「情報セキュリティ体制」と「**事案**対処態勢」の違い

- 「情報セキュリティ体制」は管理策(Security Control)に基づいた各担当者の役割分担を重要視するが、**「事案対処態勢」は想定事案に相応する対処行動及びその能力維持を重要視**する。

❖ 「態勢」と「体制」は、***取るべき準備行動*** が大きく異なる。

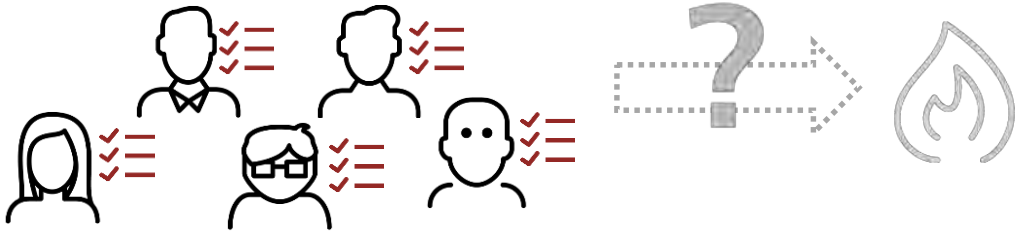
– 態勢: 事態に対処するための準備ができている状態のこと。（前もっての身構え）

本当に事態対処できるかどうかが重要



– 体制: 基本原理・方針によって秩序づけられている組織のこと。（政治支配の様式）

組織内の役割分担（責任所在）が重要



「**事案**対処態勢」の構築のための重要ポイント (1)

- 全ての関係者が、**徹底的な状況認識(Situation Awareness)**を行うこと。

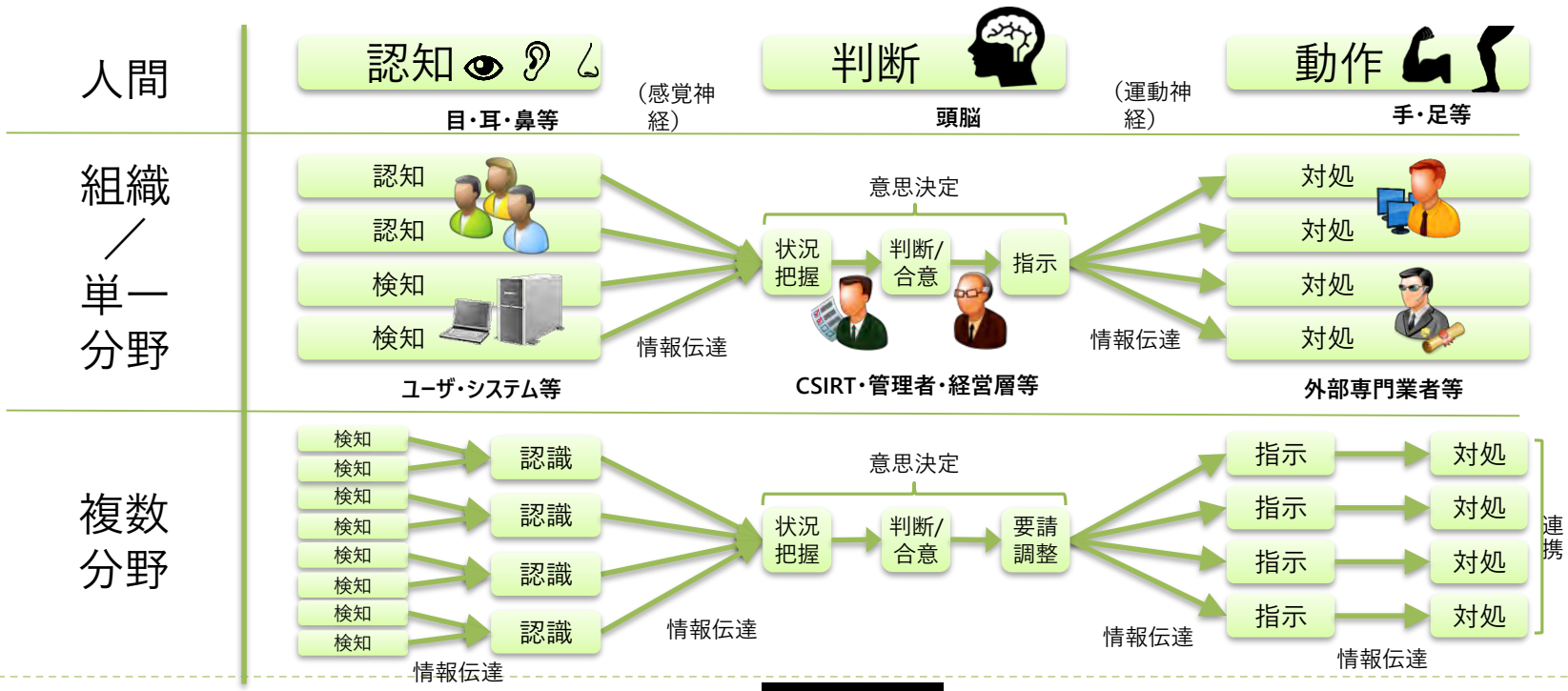
- インシデント発生時においてやり取りする**相手の顔**が見える
- やり取りにおいて必要となる**認識・教養の統一化**を図ることができる
- インシデントハンドリングの流れや**規定等の改善**を図ることができる
- **上層部の考え方**を把握することができる
- **発生した事例**を把握することができる

- 連絡先の**疎通確認**をすることができる(異動等による疎通不能の回避)
- サイバー脅威の**変動状況**に(ある程度)追いつくことができる
- メンバー間の**一体感**を感じることができる
- 潜在化した可能性のあるイベント(事象)を検知する**トリガー**となる
- **教養不足を補う**ことができる

TLP:GREEN

「事案対処態勢」の構築のための重要ポイント (2)

- 専任されたチームが、**検知(Detect)⇒トリアージ(Triage)⇒対処行動(Respond)**の各プロセスを確立及び実務能力の構築を行うこと。
  - 「人間の行動原理(認知⇒判断⇒動作)」をベースにして、「組織／単一分野」及び「複数分野」における**各フェーズ(認知検知⇒意思決定⇒対処)で実施される行動**を特定した上で、それを実現可能にする**能力スキルや情報・知見(ノウハウ)等**を見出し、実施可能な状況にしておくこと。



TLP:GREEN

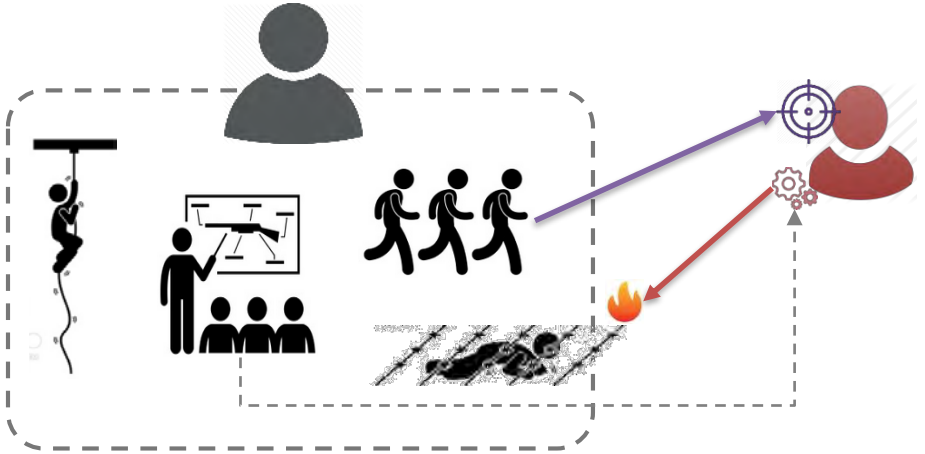
「事案対処態勢」の継続強化ためのアクションアイテム

- 状況認識(Situation Awareness)の共有や向上のために、サイバーセキュリティ事案への対処態勢関係者による定例会及び外部の専門家を招聘した**勉強会**を実施。

- 連絡体制の維持のために、定期的な**疎通確認訓練**(Communication Check Drill)或いは**電話会議**(Teleconference)を実施。

- 意思決定能力の向上及び最新の脅威動向の把握のために、脅威シナリオをベースにした**TTX**(Table Top Exercise; 机上演習)を実施。

- メンバー間の**関係性強化**を図ることができる
- 教養に加え、**(擬似)経験**を積み上げることができる
- メンバー間で流通する情報に対する**関心が向上**する
- インシデントハンドリングや規定等の**具体的な改善点**を見出せる
- 全般的なインシデント対応に係る**時間を短縮**できる



本資料に関する連絡先

名和 利男（Toshio NAWA）

SITE: https://www.nawa.to

PGP: 0xE38B4E01

TLP:GREEN