2020年
サイバーテロの可能性と経営としての監査役の役割

2020年1月29日（水）

丸山司郎

ねらい

SEからセキュリティ専門家を経て社長を経験した者として

サイバーテロへの対策と発生した場合の対応について

経営者に求められる責任を説明し

自社に準備に役立ていただく。

東京
オリンピック

2020年
　7月24日（金）～8月9日（日）

あと 177日

約 半年

混雑予想
8月7日
8:00~9:00

駅　朝ラッシュ時間帯（7:00~10:00）

- ● 普段の朝ラッシュよりも混雑（観客等の影響がかなりある）
- ● 普段の朝ラッシュよりも混雑（観客等の影響がある）

駅　朝ラッシュ以外の時間帯（5:00~7:00、10:00~24:00）

- ○ 普段の朝ラッシュ並みに混雑（観客等の影響がかなりある）
- ○ 普段の朝ラッシュ並みに混雑（観客等の影響がある）

路線

- かなり混雑（観客等の影響がある）
- かなり混雑（観客等の影響がほとんどない）
- やや混雑（観客等の影響がある）

大会輸送影響度マップ
https://2020tdm-tokyo.maps.arcgis.com/apps/opsdashboard/index.html#/634ef9f430514f0caebf27e0277c178a

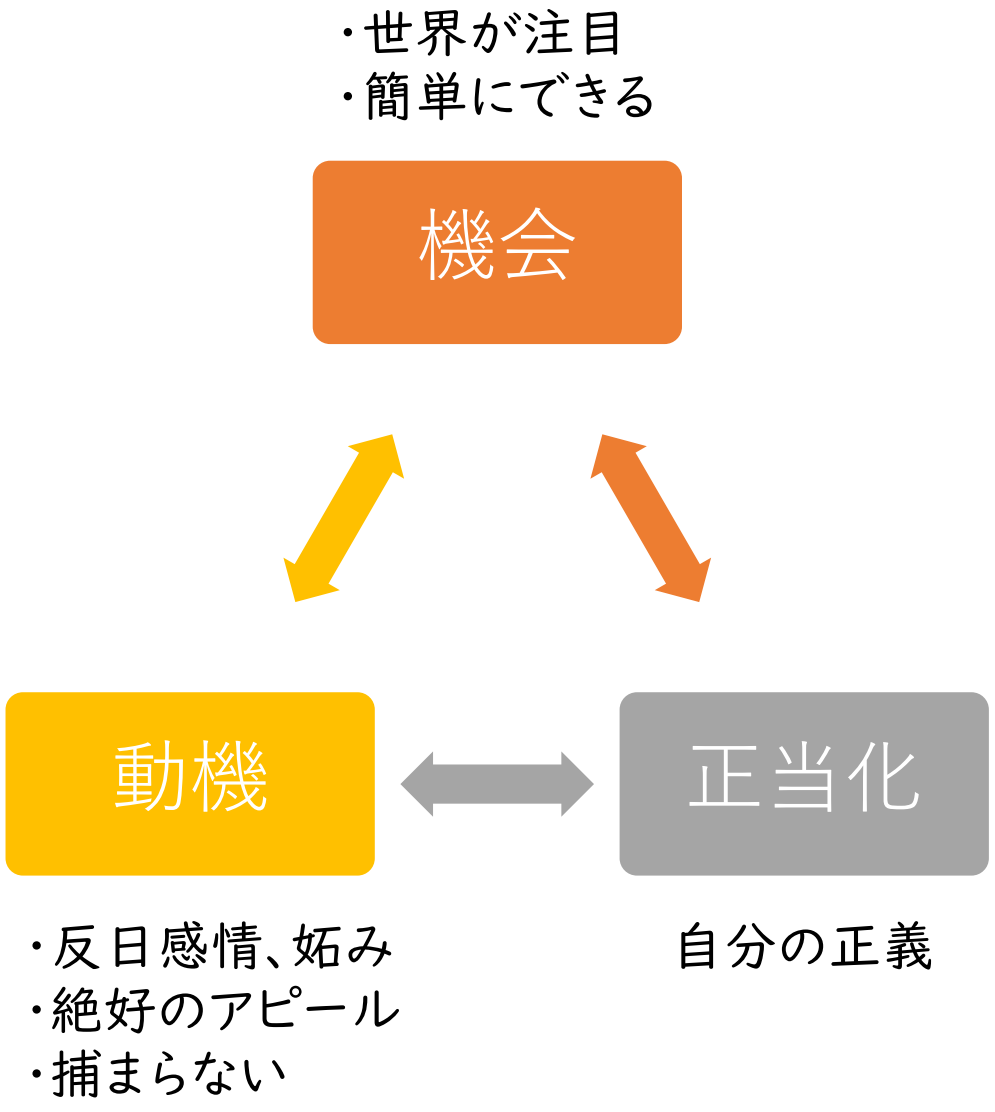
サイバー攻撃対策

Ｑ１：経営会議で毎月、対策会議を開催している。

Ｑ２：昨年よりサイバーセキュリティ予算がかなり増加している。

Ｑ３：昨年より情報セキュリティ部門の要員が増加している。

サイバーテロの可能性



	脅威	理由
1	好き嫌い 悪ふざけ	極端な好き嫌いや、悪ふざけが度を越すと、常識を超えた行動につながる。
2	貧困	インターネットが世界をつなげたことで、 つかまることのない犯罪が可能になった。
3	組織犯罪	アングラ経済は実在し、犯罪活動の道具としてインターネットを活用している。 カード詐欺、麻薬売買、武器、人身売買
4	貿易・経済行為	国境のないインターネット上で行われる貿易や経済行為に、各国の法制度が追い付けない。税制、為替、情報保護、産業スパイ
5	イデオロギー	宗教、民族、主義などが過激になると、テロ行為が正当化され英雄視される。アノニマス、など
6	戦争・紛争	インターネットは第5の戦場と呼ばれ、すでに国家間の戦争が行われているが、表面化しない。Wikileaksなどで暴露される


動機

ロシア
東京五輪参加禁止

- 11月28日、世界反ドーピング機関（ＷＡＤＡ）が、２０２０年東京五輪・パラリンピックを含む主要大会からロシア選手団を４年間排除する処分を決めた。
- 12月24日、ロシアは不服申し立て
- 1月9日、スポーツ仲裁裁判所に（ＣＡＳ）に仲裁を要請する手続き
- 最終的な判断は３月から４月ごろになるという見方

最悪の日韓関係

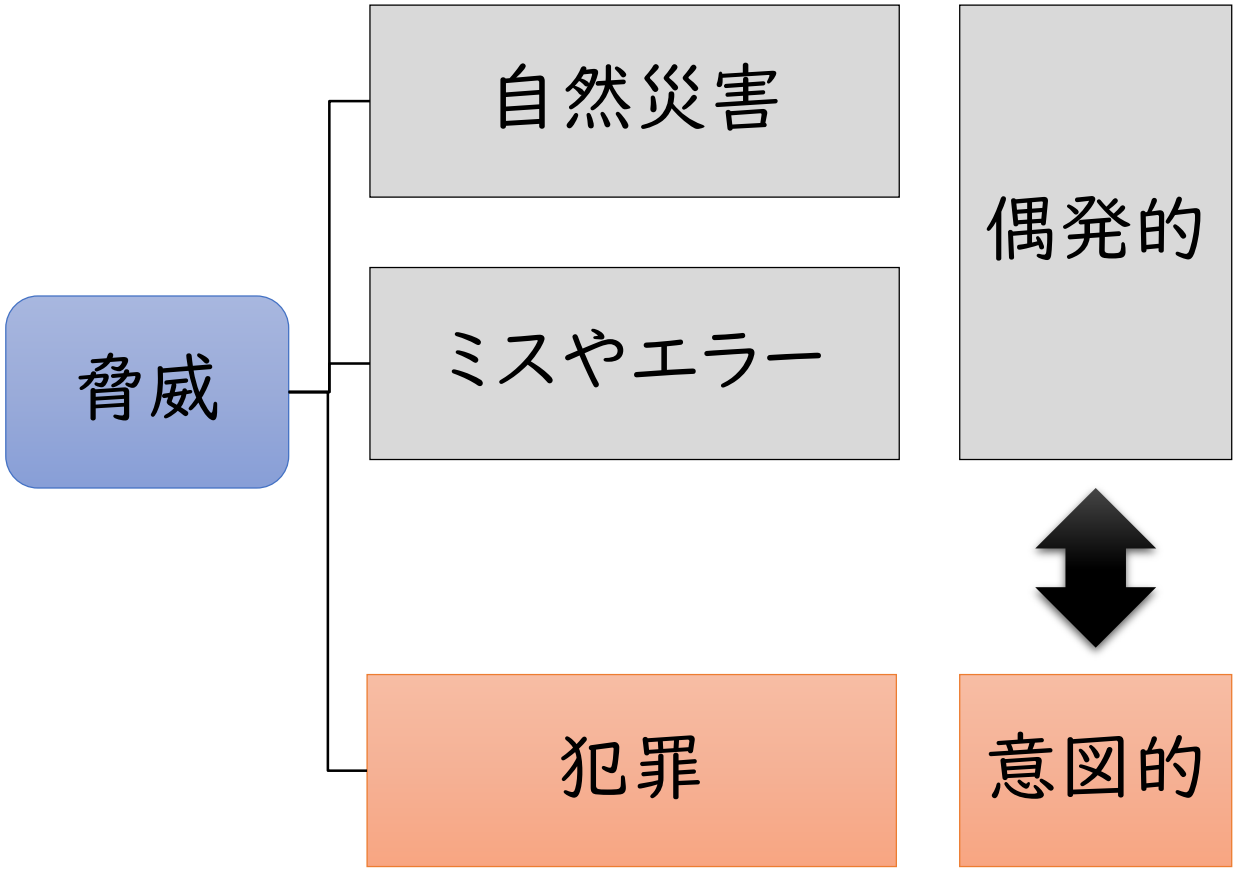
- 2018年、新日鐵住金を被告とした「徴用工」による損害賠償の判決
- 韓国政府、「日韓請求権協定」の外交的協議に応じることはなく、この問題を放置
- 8月2日、日本政府が一部半導体関連物品の輸出規制措置（いわゆる「ホワイト国除外」）
- 日本製品の不買運動と日本への旅行中止を呼びかける「NO JAPAN」運動
- 2020年に開かれる東京オリンピック・パラリンピックのボイコット論
- 8月22日、韓国政府が日韓両国間のGSOMIA（軍事情報包括保護協定）の破棄を通告することで安全保障分野にまで拡大
- 協定失効直前の11月22日、韓国政府が「破棄通告の効力を停止」を発表

トランプ大統領
イラン司令官の殺害指示

- 12月27日、武装勢力ヒズボラが、イラク軍基地をがロケット弾で攻撃。アメリカの民間人1人が死亡、アメリカ兵4人とイラク治安部隊2人が負傷
- 12月31日、シーア派成員、バグダード市内で数千人の抗議活動を展開。アメリカ大使館前に集結して放火、侵入を試みるなどして暴徒化
- 1月3日、イランのバグダード国際空港付近にて、ロケット弾3発による攻撃を受けヒズボラの最高指導者アブ・マフディ・ムハンディスとイランのソレイマニ司令官ら8名が死亡
- 1月3日、トランプ大統領は自らの指示でアメリカが攻撃を加えたことを発表
- 1月4日、米、イラク国内の緊張を受けて第82空挺師団の増派を決定
- 1月8日、イスラム革命防衛隊は報復として在イラク米軍基地を弾道ミサイルで攻撃
- 1月8日　イラン戦争間近？　twitterで＃WW3がトレンド入り

- イランは親日とはいわれれいるが、テロ組織の「ヒズボラ」や「ハマス」に資金や武器を与えている。
- DDoS流れ弾・便乗サイト改ざん

コンピュータ・セキュリティ
犯罪対策と災害対策　1981年

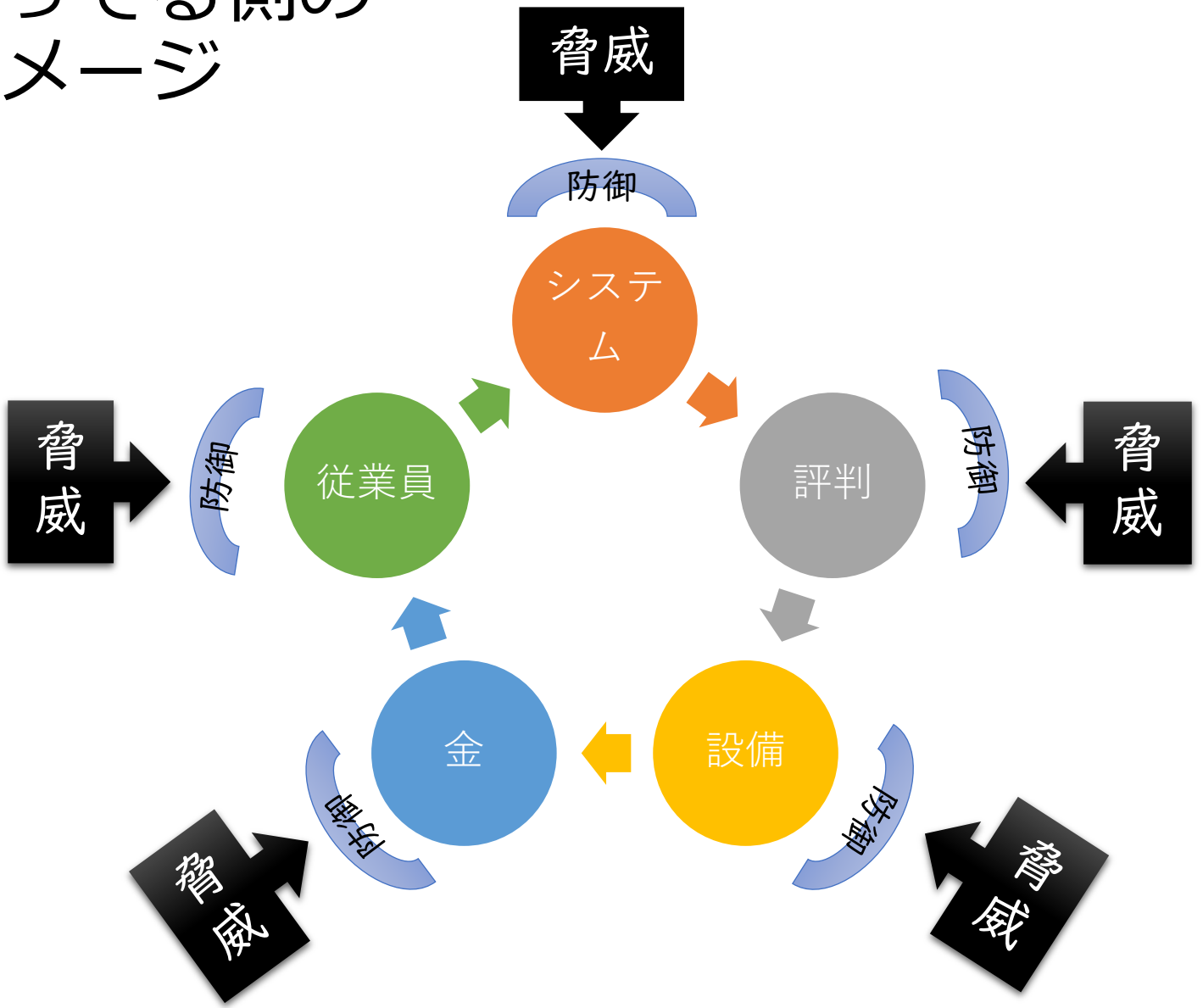


今までの経験則から
予測することができる。

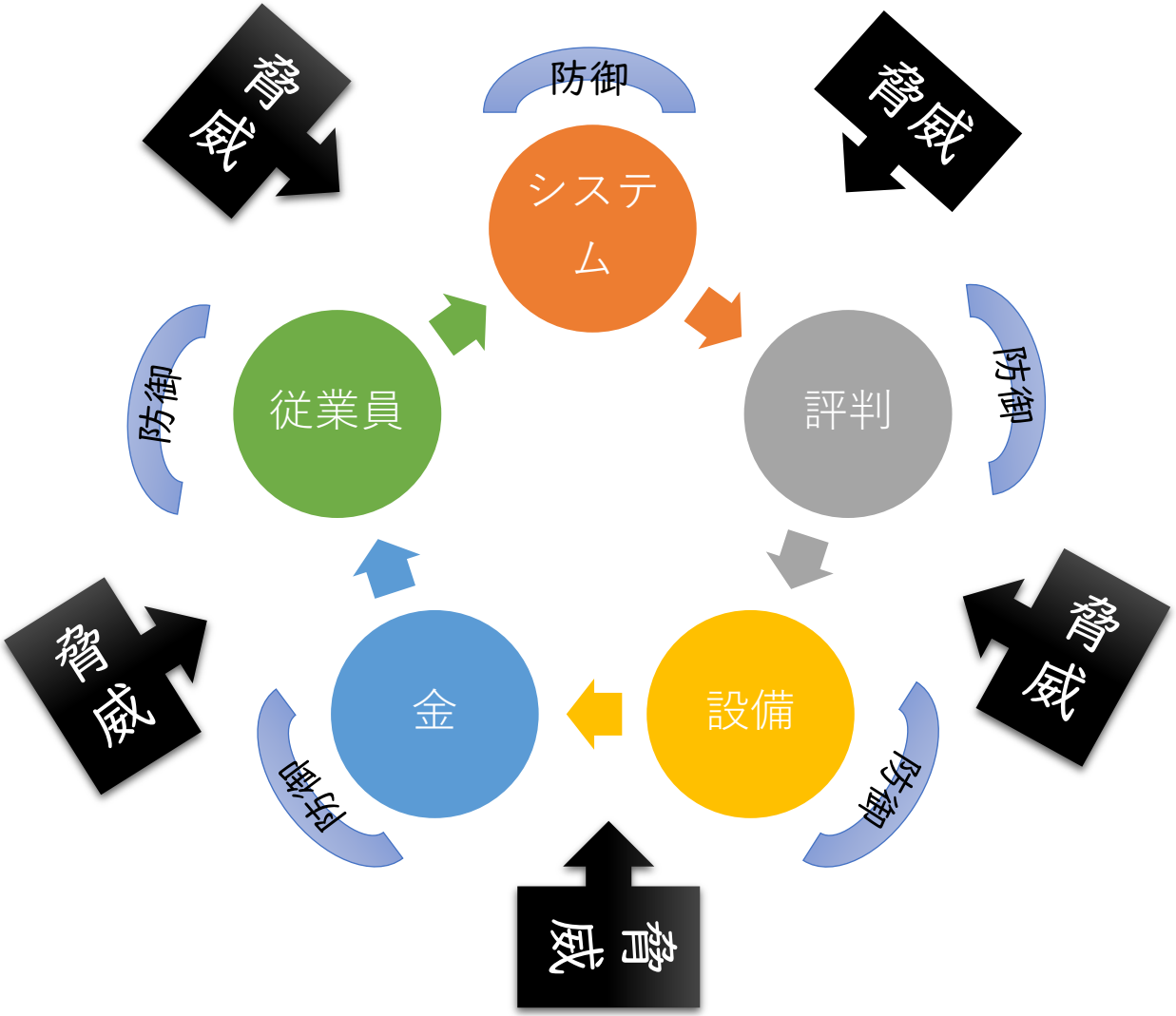
□ チェックリスト的対策

安全対策の裏をかこうと
するため、強化した場所
を避けて**防備の不充分
な所から攻撃**をしかける。

守ってる側のイメージ



現実



サイバー攻撃の実例

2019年ラグビーワールドカップ

2018年平昌オリンピック

ラグビー　ワールドカップ

【社会】

ラグビーW杯期間中、サイバー攻撃相次ぐ　五輪中継妨害への準備か

2019年12月17日 朝刊

ラグビー・ワールドカップ（W杯）の日本大会期間中に、テレビ放送システムを狙ったサイバー攻撃が相次いだことが、大会組織委員会への取材で分かった。政府関係者は「来年の東京五輪・パラリンピックのテレビ中継を妨害する準備が行われている」と警戒を強めている。

組織委によると、サイバー攻撃はシステムに大量のデータを送りつけて機能を停止させる「ＤＤｏＳ（ディードス）攻撃」。大会期間中に十二回あり、主に放送局が使う組織委のシステムが狙われたが、実害はなかった。

攻撃の多くに日本国内の機器が使われたが、実際の攻撃元は判明していない。情報セキュリティーの専門家は「多くの人が視聴するテレビ放送が止まれば影響は甚大だ」と懸念した。

ラグビーW杯では他に、偽メールを送って大会職員のパスワードを盗もうとする「フィッシング」や、大会職員が海外サイトを閲覧してウイルス感染する被害もあった。

平昌　オリンピック

【平昌五輪】

サイバー攻撃か？！　開会式のさなかにネットがダウン　国防省も巻き込んで原因調査中

　平昌五輪スタジアムで平昌冬季五輪の開会式が行われていた最中、五輪組織委員会がサイバー攻撃を受けていた可能性が浮上し、専門家が原因などの調査を進めていることが１０日、明らかになった。

　韓国メディアなどの報道によると、開会式が始まる４５分前の９日午後７時１５分ごろから、組織委内部のインターネットやＷｉ－Ｆｉ（ワイファイ）がダウンした。１０日正午の時点ではまだ完全復旧に至っていないと報じられた。

　組織委の宋百裕報道官は報道陣に対し、「重要性が低いシステムのいくつかが影響を受ける事案があった。不便をかけたことを陳謝する」と述べたうえで、「開会式へは影響がなかった。選手や観客の安全にもまったく影響がなかった」と強調した。

　しかし、ロイター通信によると、開会式では予定していた小型無人機（ドローン）を飛ばすことができず、事前に録画した映像を使用した。システム障害との関連は明らかになっていないが、国際オリンピック委員会（ＩＯＣ）の広報担当者は「突然の計画変更でドローンを展開することができなかった」と、サイバー攻撃の影響を匂わせた。

https://www.sankei.com/pyeongchang2018/news/180210/pye1802100060-n1.html

産経ニュース

サイカル journal by NHK
SCIENCE & CULTURE

“オリンピックを破壊する”～サイバー攻撃、驚愕の実態～

<u>攻撃は、突然に始まった</u>

「リオ、ロンドンとは全く違う、オリンピックを妨害する明確な目的をもった攻撃だったと思う。ピョンチャンオリンピックが成功しないおそれもあっただろう」

https://www.nhk.or.jp/d-navi/sci_cul/2019/06/story/story_190613/

サイバー攻撃対応チームの総括責任者
「イグルーセキュリティ」チョ・チャンソブ副社長

「最初に異変についての情報がもたらされたのは、去年２月９日の午後７時頃、**開会式の１時間前**でした」

ＩＴサービス会社が運用する大会のシステムの一部に不具合が起きたが、「システム障害」との報告だったため、サイバー攻撃対応チームは出動しなかった。

しかし、開会式が始まった午後８時、会場の無線ＬＡＮが使えなくなったり、チケットの印刷が出来なくなったりするなど、トラブルが相次ぐ。

「多数のシステムが同時多発的に問題を起こし、**大会のサーバーの画面が青一色になって再起動も出来なくなった**。ウイルスによるサイバー攻撃と判断しました」

分析したところ、攻撃を受けたのは、観客の入退場から大会関係者のインターネット接続まで、あらゆる認証作業に必要な、大会の根幹を担うサーバーだと分かった。

開会式が終わるのは夜１０時。混乱を防ぐため、無線ＬＡＮや入退場システムなど、最低限の応急処置した上で、バックアップのサーバーを使って全体の復旧作業を急ぐことにした。

データセンターには、ネットワーク構築やサーバー管理など、各分野のプロおよそ２５０人が続々と駆けつけた。

ところが、作業開始後、さらに深刻な事態が判明した。**サーバーを１台復旧すると、ウイルスの変種が現れて別のサーバーに感染**していったのだ。

攻撃に使われたのは、「拡散型」と呼ばれる極めて悪質なウイルスだった。現場では驚きの声があがったという。

「攻撃は認証システムを通じて、ＩＤとパスワードを乗っ取った状態で始まりました。乗っ取ったアカウントから認証システムを破壊し、その認証システムがウイルスを連鎖的に伝播する攻撃となったのです」

被害は、認証用のサーバーを発信源に５０のサーバーに及び、大会に関わる５２のサービスが影響を受けた。

攻撃者の狙いは、単なる示威行為ではなく、**大会の破壊にある**ことは明らかだ。

このままでは、大会そのものに影響が出かねない。午前０時、これ以上の拡散を防ぐため、大会のインターネットを遮断した。

「これは時間との闘いだから、人員を追加投入して、変種のウイルスをひとつずつ見つけて治療する作業を繰り返しました。最終的に検出されたウイルスは、およそ４０種にのぼったのです」

復旧作業が終わったのは、競技開始が１時間後に迫った翌日の午前８時。徹夜で対応にあたった結果、競技の運営に支障が出る最悪の事態は避けられた。

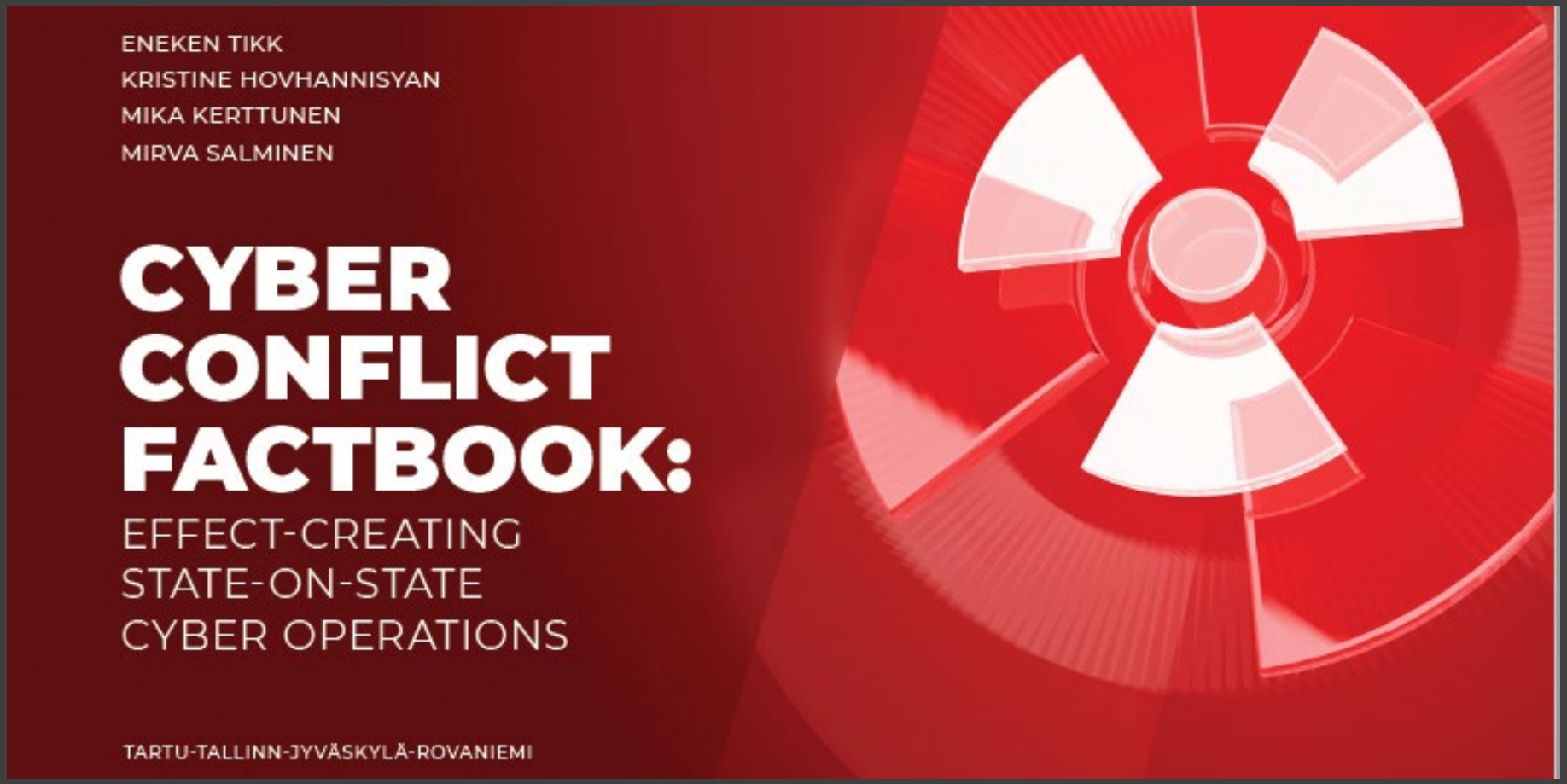
今回の攻撃を分析した結果、ウイルスの感染は、オリンピックの組織委員会の内部ではなく、大会に関連する**海外のＩＴサービス会社から始まっていた**。

ウイルスは、ここの端末に保管されたＩＤやパスワードを盗み、組織委員会のサーバーへ移動していた。

こうした動きは、大会の**少なくとも３か月前から始まり、開会式に合わせてウイルスが作動する**ように仕組まれていたとみられている。

「いくら準備しても攻撃は必ずある。国家的行事では最悪のシナリオを想定して訓練すべきだ」

https://www.nhk.or.jp/d-navi/sci_cul/2019/06/story/story_190613/



サイバー紛争の真実

32件の現実に発生した、サイバーにおける紛争事例

https://drive.google.com/file/d/1wYaGNbrQXyJuDjrrOoRWIv99f9PX_N5C/view

The New York Times

U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say

By Julian E. Barnes

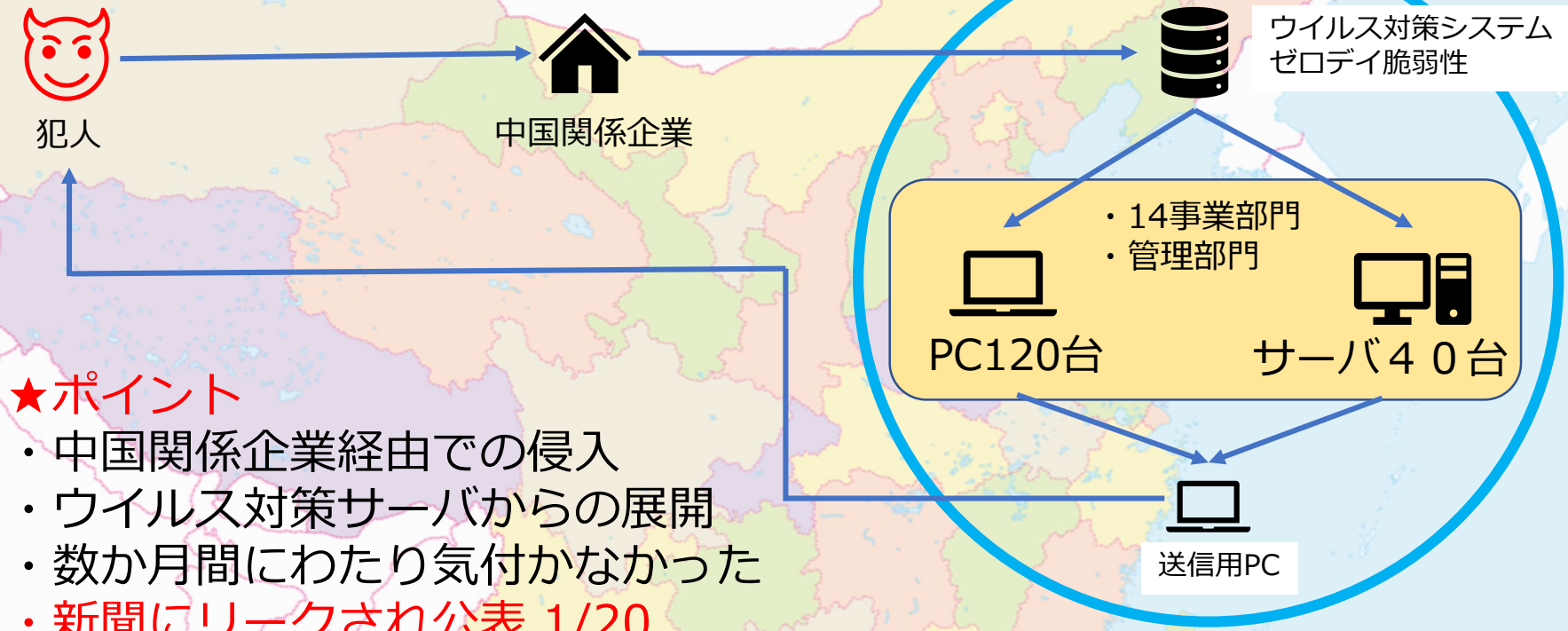
Aug. 28, 2019

WASHINGTON — A secret cyberattack against Iran in June **wiped out a critical database** used by Iran's paramilitary arm to plot attacks against oil tankers and degraded Tehran's ability to covertly target shipping traffic in the Persian Gulf, at least temporarily, according to senior American officials.

Iran is still trying to recover information destroyed in the June 20 attack and restart some of the computer systems — including military communications networks — taken offline, the officials said.

https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html

三菱電機への不正アクセス事件



★ポイント
- 中国関係企業経由での侵入
- ウイルス対策サーバからの展開
- 数か月間にわたり気付かなかった
- 新聞にリークされ公表 1/20
- 官房長官「機微情報の流出なし」1/21

重要インフラ企業の経営者に求められる責任

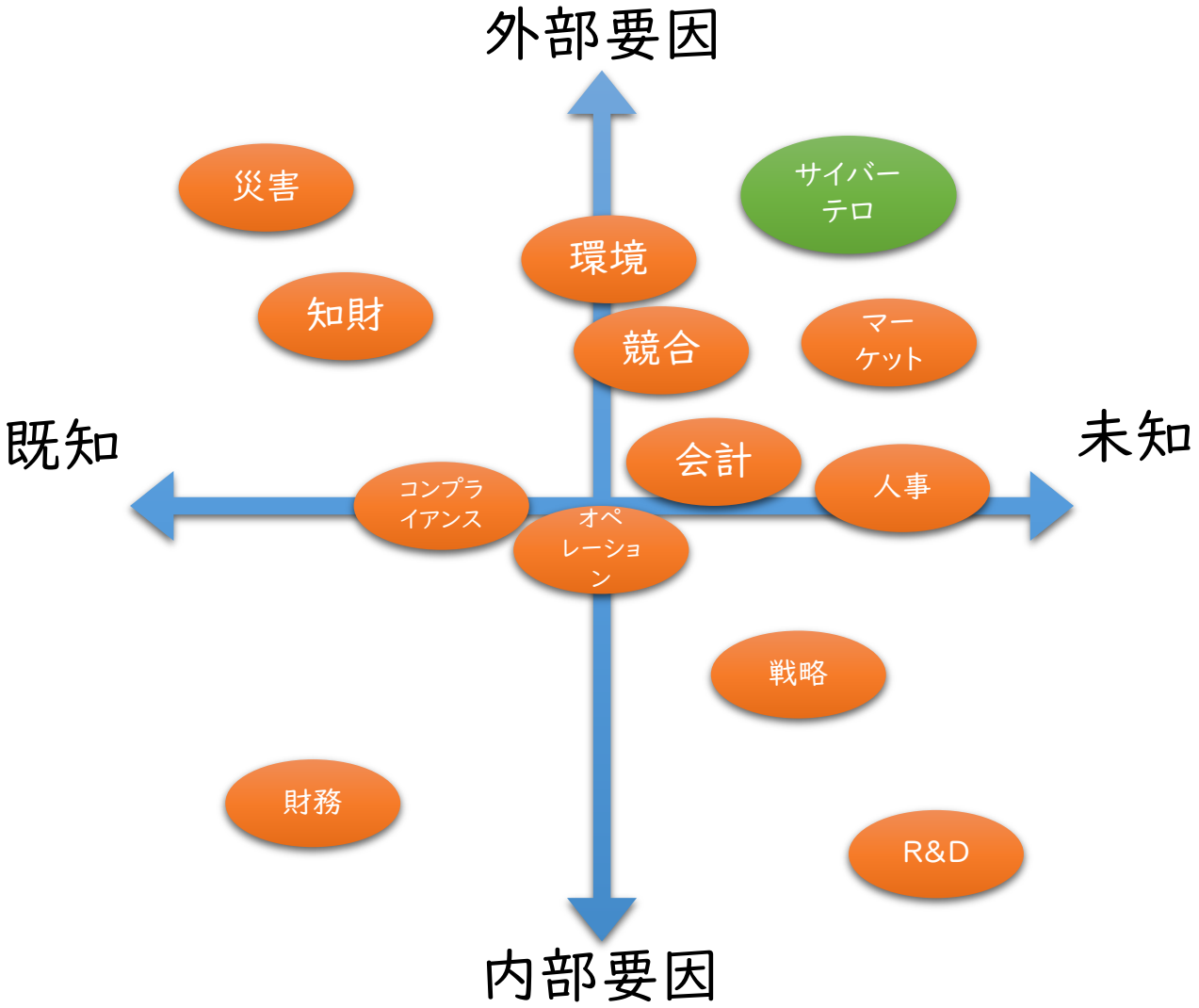
経営リスクに占める、サイバーテロの位置づけ

善管注意義務を果たしているか

ちゃんとやったと、説明できるか

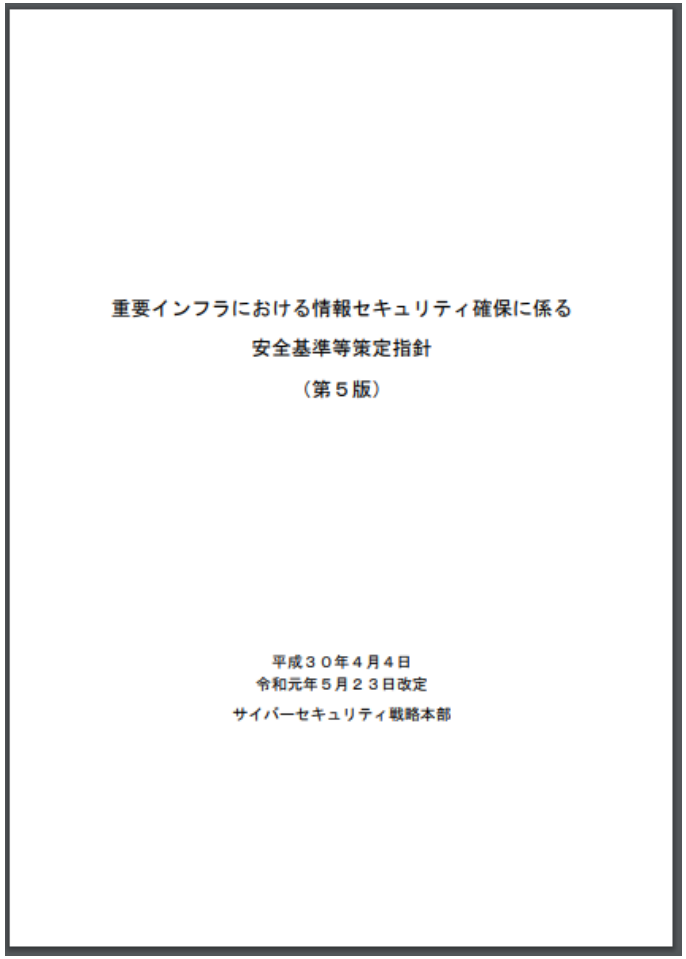
クライシスコミュニケーションの体制は

経営リスクに占める、サイバーテロの位置づけ



内閣官房　サイバーセキュリティ戦略本部

重要インフラにおける情報セキュリティ確保に係る安全基準策定指針（第5版）


重要インフラにおける情報セキュリティ確保に係る
安全基準等策定指針
（第５版）
平成３０年４月４日
令和元年５月２３日改定
サイバーセキュリティ戦略本部

● **経営層に求められる行動**

「情報セキュリティリスク」は「機能保証の考え方」を踏まえた事業運営を不確かにする影
響力があることを認識し、その対処の在り方を判断するために必要な情報セキュリティリス
クアセスメントの実施を指示すること。また、情報セキュリティ対策のＰＤＣＡサイクル推進に当たり、必要な資源（予算・体制・人材等）の継続的な確保及び適切な配分に努めること。
さらに、情報セキュリティリスクへの対応結果が事業に与えた効果と影響を定期的に検証し、情報セキュリティリスク対応戦略の見直しの必要性等について意思決定を行うこと。これらの取組に際して、「企業経営のためのサイバーセキュリティの考え方」、「**サイバーセキュリティ経営ガイドライン**」等を参照すること。

次ページへ

機能保証の考え方

　重要インフラサービスは、それ自体が国民生活及び社会経済活動を支える基盤となっており、その提供に支障が生じると国民の安全・安心に直接的かつ深刻な負の影響が生じる可能性がある。このため、各関係主体は、重要インフラサービスを安全かつ持続的に提供するための取組（機能保証）が求められる。

　なお、本行動計画において、「機能保証」とは、各関係主体が重要インフラサービスの防護や機能維持を**確約することではなく**、各関係主体が重要インフラサービスの防護や機能維持のためのプロセスについて責任を持って請け合うことを意図している。すなわち、各関係主体が重要インフラ防護の目的を果たすために、情報セキュリティ対策に関する**必要な努力を適切に払うこと**を求める考え方である。

（「重要インフラの情報セキュリティ対策に係る第４次行動計画」からの抜粋）

サイバーセキュリティ経営ガイドライン

経営者が認識すべき3原則

1. 経営者は、サイバーセキュリティリスクを認識しリーダーシップによって対策を進めることが必要

特徴

2. 自社のみならず、ビジネスパートナーや委託先も含めたセキュリティ対策が必要

3. 平時及び緊急時のいずれにおいても、関係者との適切なコミュニケーションが必要

サイバーセキュリティ経営ガイドライン

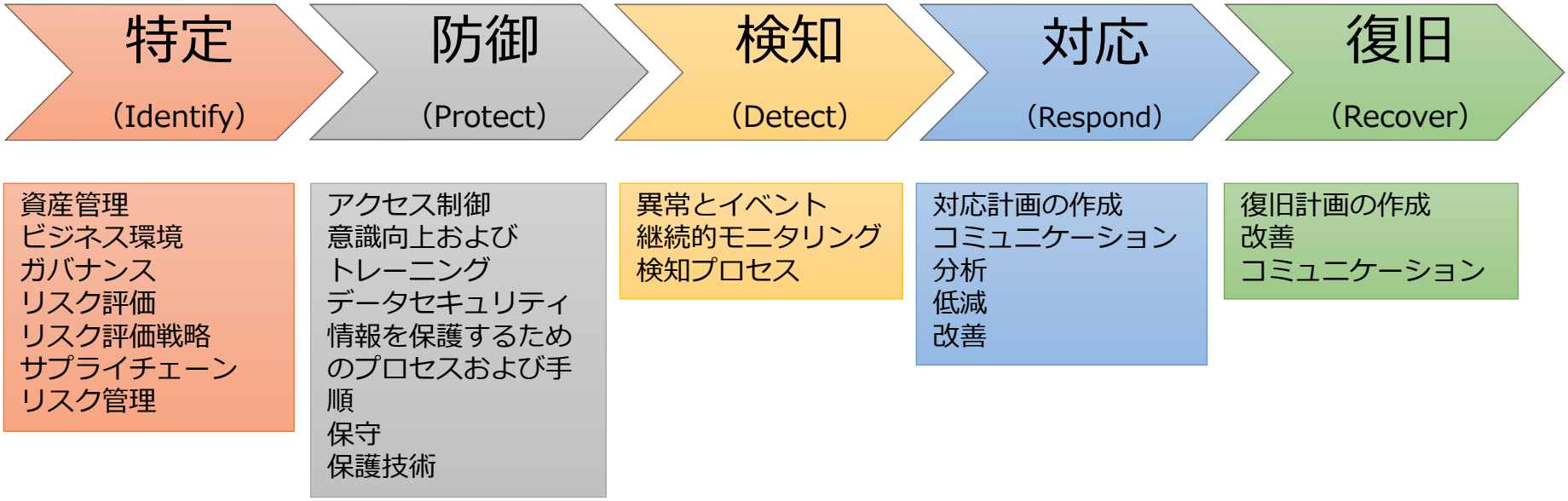
実質的な意味

1. サイバーセキュリティは経営者の責任であると**国が明言**した。

2. 炎上する事件が起きた場合に、経営者に対して**善管注意義務**を果たせと国が指導できる。

3. 将来、**裁判**が起きた場合に、2015年時点でこのようなガイドがあったと**判断材料**として経営者の責任が問われる。

NIST
サイバーセキュリティ・フレームワーク



サブカテゴリ
(108 のアクティビティ)

監査役

権限

- 取締役の職務執行を監査すること

役割

- 将来の不祥事につながると思われるリスクに対しては、監査を通じて、取締役をはじめ各事業部門に対して適時・適切に監査意見を述べたり注意喚起をすることにより、不祥事を防止する

義務

- 仮に、監査役が取締役の不正行為もしくは法令・定款違反の事実やそのおそれがあると認めたときには、取締役（会）に報告する

株主代表訴訟と監査役

１．株主が取締役の責任を追及する場合、**まず、監査役に対して**取締役の責任を追及するように書面により提訴請求する

２．監査役は、株主からの提訴請求に対して**60日間で調査し、結論**を出さなければならない。法務部門や内部監査部門に調査を依頼したり、結論を求めることはできない。

３．監査役が取締役の責任追及をしないと判断した場合、当該株主は裁判所に対して、取締役の責任追及の訴えを提起することができる。

４．仮に、監査役が調査した結果、提訴請求対象取締役に法的責任があり、会社の損害と違法行為との間に相当の因果関係が存在すると判断すれば、監査役が会社を代表して、当該取締役の責任追及の訴えの提起を裁判所に対して行う。

東京
オリンピック

あと 177日

・時間がない
・人が足りない
・専門家がいない

プラン B
大きなミスを避けて、無難にいきましょう作戦

ちゃんとやっているか、現場に確
認する。

サイバー保険に入る。

何かあった時の言い訳を考える。

プラン A
オリンピック後も役立つ節目作戦

経営者が直接セキュリティの現場に行って、
毎月（6回）話を聞く

経営者がインシデント事例3つ（DDoS、平昌、三菱）の
訓練をする

外部のプロに、穴を探してもらう。
（ペネトレーションテスト）

ありがとうございました。