2021 年　10 大トレンド投票候補

項目	
1　表題	**史上最悪の天災やパンデミックなどに対応できる IT－BCP へ**
内容	このところ毎年史上最大級の豪雨による大被害が発生している。環境省によれば、気候変動により今後さらなる大雨が予測され、災害が深刻化すると懸念されている。また、海溝型や直下型の地震は、ひとたび起きると甚大な被害をもたらすことになり、富士山噴火なども想定外においておくことはできない。さらに、今回の COVID-19 パンデミックでも、IT インフラの運用要員の確保などに多くの課題が露呈した。 デジタル化が進む中で、企業のみならず国民生活全般がサイバー空間に大きく依存するようになり、災害時においても IT インフラの機能確保が社会的要請になっている。企業や団体には、自組織の重要 IT インフラが利用できなくなるリスクの発生可能性と影響度を的確に把握できているか、そのようなリスクに対する対策や業務継続の実効性確保ができているかなど IT－BCP の見直しニーズがさらに高まる。
2　表題	**止まらない、安全なクラウドサービスへ広がる要求**
内容	クラウドサービスはこれまで様々な課題が指摘されている。一方、システム構築や運用上のメリットは大きく、クラウドを利活用する流れは加速している。我が国の政府もクラウドバイデフォルトを掲げ、クラウドのセキュリティ評価制度（ISMAP）を立ち上げた。企業、個人、国家などの膨大なデータがクラウドに集約されるということは、それだけ攻撃者にとっても価値が高く、クラウドに対する攻撃は、より狡猾にまた、激しさを増すと考えられる。クラウドに関連するシステムだけでなく、サプライチェーン、組織、個人も含めて、ありとあらゆる構成要素がターゲットとなる。安全性に疑義がないことを多面的に証明、維持していくことが重要となるだろう。
3　表題	**標的型攻撃の侵入パターンが多様化**
内容	今までの標的型メールによるシステムへの侵入から、VPN や管理ソフトウェアなどの脆弱性や、海外拠点の弱いネットワークから本体に侵入する標的型攻撃にシフトが移っている。そのため、攻撃されていることを見つけづらく、何かのきっかけで異常が発見されるまで侵害に気づかないことが多い。また、一般的なリモートデスクトップソフトなどを悪用し、普通の仕組みで浸透を継続することから、事案発覚後も侵害されつづけていることがある。
4　表題	**手法の高度化が進む金銭目的のサイバー攻撃**
内容	技術的なスキルが高いとされていた標的型攻撃の手法を取り込み、ランサムウェア・情報暴露・暗号通貨窃取・BEC を狙う攻撃者は、様々な手法によって組織を狙い、時には国家が背景にあると推定されるサイバー攻撃者グループよりも技術的に高度な手法を使ってくることも少なくない。すでに、標的型攻撃と金銭目的の攻撃の技術レベルは区別できず、より広汎で大量で高度な攻撃に組織はさらされることになる。

5　表題	**在宅勤務者から組織を狙うフィッシング詐欺の横行**
内容	リモートワークの増加や、ニューノーマルな働き方の一環による在宅増加に伴うウェブサービスの拡充により、ID/パスワードの利用シーンが増え、かつ、アクセスできるリソースや価値が増えたことから、相対的にアカウント情報を狙うフィッシングも増えている。さらに構築スピードと利便性を重視して乱立したサービスではセキュリティデザインもされておらず、被害範囲を拡大させる一因となっている。
6　表題	**DX ビジネスの進展により重要性を増すシフトレフト**
内容	世は DX の時代を迎えつつある。すでに多くのデジタルビジネスが生まれているが、これは萌芽に過ぎず今後ますます加速していくであろう。デジタルビジネスを語るキーワードとしては、大量データ、（複数組織での）情報活用、迅速・即応性、接続性、柔軟性、認証の連携などが挙がるが、いずれもセキュリティリスクを伴うキーワードである。こうしたビジネスにセキュリティが対応するためには、サービス提供の初期段階からセキュリティを意識する、いわゆるシフトレフトの考えが必要である。将来の変革を意識したセキュリティリスクの分析が初期段階に導入されているか、スレットインテリジェンスなどプロアクティブなセキュリティ運用が導入されているか、またビジネスを支えるシステムがサポート切れによりぜい弱性を増大させていないかなどの確認が必要である。
7　表題	**IoT により繋がるシステム、繋がらないセキュリティ**
内容	IoT 機器や工場の生産システムなど、ネットワークに接続するシステムが増大している。こうした機器や工場のシステムなどはぜい弱性が放置され、また管理されない野良機器として放置されることも多く、攻撃者に IoT として利用され、あるいは自社への入り口として利用されることがある。自社が提供側の組織の場合、製造する製品が安全な運用をできる設計となっているか、またそのための体制は十分か、利用側の組織の場合には安全に導入、運用する管理がなされているか、提供局面、利用局面双方において確認が必要である。IoT 機器は工場のセキュリティに関して各種ガイドラインも出されており、事故発生時に知らなかったではすまされない。
8　表題	**テレワークニーズに追いつかないセキュリティ対策**
内容	新型コロナウィルスの影響で、テレワークが急速に普及している。VPN 接続、クラウドサービスの利用、遠隔会議システムなどを十分なリスク分析を経ずして導入した組織も多い。一時的措置として、セキュリティポリシー違反となる施策を導入した組織もあるであろう。またコロナウィルスが収束したとしても、これらのシステムはニューノーマルの働き方として一定程度残ると考えられる。 急場しのぎで導入したシステムあるいはサービス利用が、組織の従来のセキュリティレベルを低下させていないか、インシデントハンドリングなどのセキュリティ運用業務がリモートでも行える準備ができているか、確認が必要である。

9　表題	**在宅勤務のセキュリティ対策に求められる説明責任**
内容	新型コロナの影響により、政府の推進していた働き方改革が加速する形でテレワークが実施される状況となった。各社テレワークを行う場合の自宅環境や実施ルールなどは一通り決められているものの、研修が十分に行われていなかったり、自宅兼仕事環境の物理的なセキュリティや通信環境など本当にセキュリティが保たれていることを実際に確認されてなかったりするケースも多い。 新しい働き方が定着し、2021 年に東京オリンピックが開催される場合は自宅のテレワーク環境への注目が高まってくる。この流れの中で、自宅環境の説明責任の向上のため、企業側に対しても従業員に丸投げにさせないための支援が急務となる。
10　表題	**新基準の導入により利用の見直しが迫られるクラウドサービスへの対応**
内容	今年春には政府機関が利用するクラウドサービスの安全性評価制度（ISMAP）の適合サービスリストが公開される。このリストは民間でもクラウドサービスを評価する場合の重要なベンチマークになると思われる。これまであまり真剣に検討されていない事項、例えば海外サーバの利用等についても厳しい評価が行われる可能性もある。利用中のサービスが不適合であった場合への対応が必要となる。
11　表題	**サプライチェーンがセキュリティ技術者の頭痛の種に**
内容	米中摩擦の結果、IT の重要な技術要素の利用が難しくなっている。自社で利用しているサービスなどが影響を受け、利用できなくなる可能性もある。また、従来から指摘されているように、汎用品に素性の怪しい部品があり、セキュリティホールが潜んでいる可能性もある。一方で米国政府等のサプライチェーン規制に求められる要件を満たさなければならない企業も増えると予想される。サプライチェーンがセキュリティ技術者の頭痛の種となりそうな予感。
12　表題	**ニューノーマルに対応した新たな情報セキュリティ監査**
内容	コロナ禍で監査に支障が生じている。三密の回避を理由に現場への立ち入りや担当者への質問ができないことがある。一方でリモートワーク中の社員たちへの監査は実質的に不可能である。これらの結果、監査手続きが不十分となり、脆弱性がとらえにくくなっている。このような状況が続くと情報セキュリティマネジメントが行き届かなくなり、情報セキュリティ事故につながりかねない。ニューノーマルに対応した情報セキュリティ監査のあり方が問われている。
13　表題	**頻発する大規模システム障害への対応**
内容	2020 年には 2 か月に 1 回程度の大規模システム障害が発生した。コンビニ決済、IC 乗車券、携帯電話ショップ、航空カウンター、そして証券取引システムなど、社会のインフラや人々の身近なサービスが長時間利用できなくなった。ネットワークが統合され、より便利になる一方で障害の影響も深刻化する。

14　表題	**RPA で作成されたロボットの管理不全による事故の発生**
内容	RPA ツールによってロボット作成が容易になり中核的な業務にも使われることが増加し、定着化してきている。その一方で、仕様が明確に文書化されていなかったり、存在自体が管理されてなかったりする場合、人事異動などを機に管理不全が事故を引き起こす可能性が高まっている。RPA は人間の業務を代替・自動化することから、事故防止のために「ヒト」に準じた管理を適用していくことが急務となる。
15　表題	**不完全なデータのライフサイクル管理が引き起こす情報漏洩事故の発生**
内容	2019 年末に廃棄ハードディスクの大規模な転売事案が起き、その原因から情報格納時のハードウェアレベルの暗号化の見直し、廃棄証明の確実な入手・確認、委託先管理全般のプロセスの見直しとモニタリング強化など、企業は自社のリスクに応じた様々な施策を実施している。一方で対策の十分性や有効性についての確認が不足している場合、情報流出リスクが残存したままになっており、情報のライフサイクル、機器のライフサイクル、委託先やサプライチェーン業務の管理サイクルのそれぞれにおいて「終える」時に確実なマネジメントがなされていないと、今後も似て非なる形での情報漏洩事故が続発することになる。
16　表題	**消費者のプライバシー保護意識と事業者への要求の高まり**
内容	2020 年 6 月に改正個人情報保護法が交付され、今後 1 年半以内に施行される。個人情報の利用停止、消去、第三者提供の停止を請求する要件が緩和されるなど個人の権利行使が容易になる一方、事業者によるオプトアウト規制の強化など事業者の責務を重くする改正内容となった。また、米国加州では消費者及び従業員の個人データ保護を定めた消費者プライバシー法が施行された。個人情報の漏えい事件が相次ぐ中で、消費者のプライバシー意識は確実に高まり、事業者に対するプライバシー保護の要求が高まることが予想される。
17　表題	**Easy なネットサービスの Easy な拡大がなりすましの温床に**
内容	ネットサービス、とりわけスマホによる決済サービス分野は顧客獲得競争が激化している。シェア拡大のため利便性を追求する一方でセキュリティが甘くなり、犯罪者によるなりすましと換金・送金手段も容易になった。また、行政も消費の活性化と官民キャッシュレス決済基盤の構築を目的にマイナポイント事業を展開し、マイナンバーカードの普及を促進している。リテラシーの低い消費者とサービス拡大路線を進む事業者、マイナンバーカードを普及させたい行政の三位一体が、深刻ななりすまし犯罪の温床になるおそれがある。
18　表題	**匿名性と高度で手軽な技術が生むネットの闇の拡大　―誹謗中傷、デマ、フェイク―**
内容	ネット上で誹謗中傷を受け自死に追い込まれる事件が後を絶たない。また、悪意のあるデマ、悪質で巧妙なアダルトディープフェイク動画の投稿など、ネットの匿名性、なりすましの容易さ、手軽で高度な AI 技術を悪用した犯罪が今後も増加することが予想される。