Vol.2022-CSEC-98 No.35
Vol.2022-SPT-48 No.35
2022/7/20

利用者教育・訓練から考える組織体制／セキュリティ文化の構築

内田勝也[†1]

概要：多くの利用者教育・訓練（Security Awareness）は，単に、セキュリティ・リテラシーの向上や標的型メール攻撃訓練でのクリックの低減が目的ではないはず。　組織的な業務であれば，明確な目標を策定し，それに向かうことではないだろうか？
　利用者への教育・訓練の成否は，ランサムウェアや大規模な個人情報漏えいをもたらし、組織の運営にも大きく影響を与える。
　サイバーセキュリティを経営課題の１つと考え，組織での『セキュリティ文化』の構築を目指す。CMMi 的なアプローチで、厳しいルールでなく、また、詳細な指導を必要とせず、組織としてあるべきセキュリティの維持向上に従業員が自然に行動することを目的とする

キーワード：セキュリティ文化，利用者教育・訓練，人的多重防御，標的型メール攻撃訓練

The proposal to establish of the cyber security organizational structure/the security culture based on the security awareness and the end point education.

Katuya UCHIDA[†1]

Keywords: セキュリティ文化，Security Awareness，標的型メール攻撃訓練，サイバー攻撃，人的多重防御

1. はじめに

1.1　サイバーセキュリティ環境の変化

従来，情報セキュリティ関連の教育・訓練では，コンピュータ関係者へのシステム技術の教育・訓練やコンピュータを利用する少数の人達を対象としたオペレーション教育や情報セキュリティのリテラシー教育を行えば良かった．

しかしながら，最近のコンピュータ化，ネットワーク化の進展に伴い，一企業内だけでなく，複数の企業を巻き込んだサプライチェーンも出現しており，企業の正規社員だけでなく，非正規社員など，多くの利用者が端末機器を使って，その役割を担うようになっている．

1.2　リスクの考え方

国内では，事件・事故等の発生は、「**想定内**」と言われ、『リスクゼロ』が当然であり，「100%安全だ」と言わないと納得しない管理者や経営者、マスコミが多い。

サイバーセキュリティでも、100%安全を確保できないから、何らかの対応を行い，リスクゼロの努力をする必要がある。図 1.1 に安全やリスクの考えを示したが、リスクがある程度、小さい場合、「安全」と考えているが，ここでは，リスクゼロを想定していない．このため、安全でも、何の対応もしなければ，事件・事故は起こる。

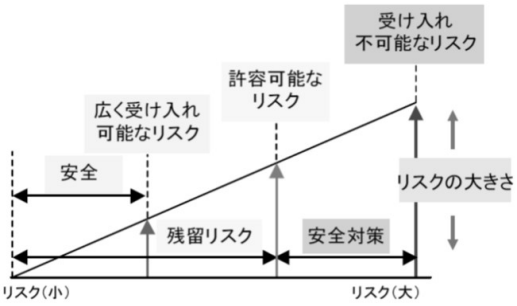

図 1.1 リスクの考え方

1.3　セキュリティレベル

セキュリティレベルは、セキュリティ対策の平均値と考えられる事もあるが、**図 1.2** を見れば明らかであろう。

図では、桶に水が入っており，水は桶の側面（**桶側**）の高さが一番低い所から溢れるのであり，桶側の高さの平均値ではない。桶側の高さが最も低い所が「**セキュリティレベル**」である．　サイバーセキュリティでも、最も弱い部分が攻撃対象になる可能性が高い。

図 1.2 セキュリティレベル

1.4　【サイバー攻撃】は，本当にサイバー攻撃なのか？

(1) サイバー攻撃とは？

サイバー攻撃とは、サーバーやパソコン、スマホなどの情報端末に対し、ネットワーク経由でシステムの破壊やデータの窃取、改ざんなどを行う行為と定義されているが，『サイバー攻撃』と言われるものは，

1．ハードウェア攻撃

[†1] 情報セキュリティ大学院大学
Institute of Information Security

ⓒ 2022 Information Processing Society of Japan

Vol.2022-CSEC-98 No.35
Vol.2022-SPT-48 No.35
2022/7/20

2. ソフトウェア攻撃
3. 人間への攻撃

の３つに分類され，更に，以下のように細分化できる．

1. ハードウェア攻撃
   ① 設計ミス
   ② ハードウェア改ざん，
   ③ サイドチャネル攻撃
   ④ 関連設備攻撃
2. ソフトウェア攻撃
   ① バグ
   ② 設定ミス／パッチ未適用
   ③ コバートチャネル
   ④ DoS／DDoS 攻撃
3. 人間への攻撃
   ① ソーシャルエンジニアリング
      ➢ 誘導質問術
      ➢ なりすまし
      ➢ サイト侵入
      ➢ 覗き見／Visual Hacking

国内ではあまり大きな報道がされなかったが，2018 年，米国ブルームバーグは，中国で製造されていた Super Micro Computer に米粒大のチップが組み込まれ，Amazon や Apple 等が被害を受けたと報道した[1].

(2) 調査からみるセキュリティ事件／事故

国内でも，サイバー攻撃が非常に多い感じを受けるが，表 1.1 に示した「セキュリティ調査」[2]を見る限り，サイバー攻撃は多くない．これは，一般的な事件・事故より，報道でのタイトルがサイバー攻撃となっていれば，人々の注目を集め，統計的な数字より大きいと思われる可能性がある．実際，この調査でサイバー攻撃と考えられるものは，2，4，8，9 だが，「**8 DoS／DDoS 攻撃**」を除き，多くは電子メールによる攻撃であり，全体の 30% 以上ある．実際，サイバー攻撃と言われるが，電子メールによる『**人間への攻撃**』であろう．

また，サイバー攻撃が国内でも数多くあるが，顕在化しない（調査時点での報告がない）と指摘もあるが，顕在化しないサイバー攻撃が数多くあり，情報資産（個人情報，知財など）に大きな被害があれば，表面化する可能性が高いのではないだろうか？

1 電子メール，FAX，郵便物の誤送信・誤配達	25.2%
2 標的型メール攻撃	14.9%
3 情報機器・記憶媒体の紛失･置き忘れ・毀損	14.5%
4 マルウェア感染	11.9%
5 社員証，書類等の紛失，置き忘れ・毀損	11.4%
6 システム設定ミス，誤操作	10.6%
7 情報機器，媒体などの盗難・紛失	9.0%
8 DoS／DDoS 攻撃	6.1%
9 ランサムウェアによる金銭等の要求	5.3%
10 退職者，転職者のよる在職時利用の情報の使用	4.0%

表 1.1 過去 1 年間に発生したセキュリティ事件／事故

2. 標的型攻撃訓練について

2.1 はじめに

利用者への教育・訓練では，「**標的型メール攻撃訓練**」が一般的で，2008 年頃から，一部の自治体などで始まったが，更に，2015 年に発覚した日本年金機構への攻撃が大きく報道され，企業等でも標的型メール攻撃訓練が行われるようになってきた．

更に，最近は，多くのセキュリティベンダーがサービスを提供している．

少し古い資料だが，国内での標的型メール攻撃訓練と米国での訓練結果を表 2.1[a]と表 2.2 に示す[b][3].

表 2.1 国内での標的型メール攻撃訓練結果

訓練概要	クリック率 %
1. 事前に情報を提供せず訓練実施	約 40.0
2. 事前に情報を提供し訓練実施	約 10.0
3. 訓練実施 2 年後、事前情報提供をせず再実施	約 12.5
4. 訓練実施 2 年後、事前情報を提供し再実施	約 6.3

表 2.2 米国での標的型メール攻撃訓練結果

訓練概要	クリック率 %
1. 4 半期毎に訓練を実施	約 19
2. 2ヶ月毎に訓練を実施	約 12
3. 毎月訓練実施	約 4
なお，初回訓練では，30～60%であった	

日米での訓練とも，クリック率は，40%程度で，繰返しの訓練をしていれば，クリック率は 1 桁になるが，ゼロにはならない．最近の状況でも，標的型メール攻撃訓練を行い，詳細な報告書を作成しているが，クリック率がゼロになることはない．

クリック率を一時的にゼロにできても，継続的にゼロにはなることはないであろう．

- 訓練でゼロになっても，実際の攻撃メールは，日々高度化しており，従来の標的型メールとは異なる考えのメールが送られてくれば，利用者は対応できない
- 特に，経営者や管理職は，業務繁忙期にメールの取り扱いが十分でなく，クリックしてしまうことが多い
- また，国内では，4 月に学卒の新人採用を行う傾向があり，標的型メールへの訓練ができていない利用者もおり，クリック率が変わる可能性がある

2.2 ゼロリスクからの脱却

上記のような理由から，全ての利用者のクリック率をゼロにできなければ，ゼロリスクを追い求める教育・訓練を見直すべきであろう．クリック率をゼロにできない前提での対応を考え，最終的に被害をゼロあるいは，最小限にすれば，目的を達成できる．

ハードウェアやソフトウェアの導入では，導入後，比較的短期間に効果を発揮するが，それらに関連する組織内人材の教育・訓練が不要にはならない．

a 各調査実施組織は以下の通り．
1. 横浜市，豊島区，藤沢市　2. NISC　3. & 4. 豊島区

b Lance Spitzner, RSA Conference 2014

ⓒ 2022 Information Processing Society of Japan

Vol.2022-CSEC-98 No.35
Vol.2022-SPT-48 No.35
2022/7/20

一朝一夕にできるセキュリティ対策を求めることが無理であれば，時間をかけて，安全を確保することが結果的には最良の方法であろう．

3. 標的型メール攻撃訓練

3.1 メール受信対応

(1) 連絡先の確立

通常，メール受信後の対応は，図 3.1 のように分類される．

ここで，④や⑥のように，クリックしたが，連絡をしなければ，マルウェアの被害が拡大し，組織全体に広がる可能性がある．

そのため，連絡先を明確にし，利用者全員が連絡できる仕組みの構築が必要になる

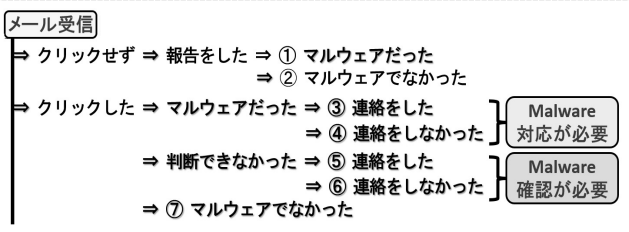

図 3.1 メール受信時の対応

(2) セキュリティ・リーダーの任命

連絡先が，セキュリティ部門／コールセンターの場合，電話での連絡に躊躇する，あるいは，メール連絡は，面倒で，連絡をやめてしまう管理職がいると言われる．一部のツールは，ワンクリックで当該担当部門にメールが送る仕組みがあるが，当該部門で端末機器の操作（リモートオペレーション）ができなければ，対応は個々の利用者がやらなければならない．

そこで，40 人程度の従業員で構成される部門を想定し，2 名程度のセキュリティ・リーダー[c]を任命し，気軽に連絡できる体制の構築を目指す．

受信したメールで，マルウェアが含まれている添付ファイルや埋込み URL をクリックした場合，セキュリティ・リーダーに声がけし，一緒に対応できる仕組みを考える．

クリック率は，多くの組織で，管理職，経営者，社員の順と言われており，気軽に対応を求めることができる仕組みを考える．

セキュリティ・リーダーは，入社 3～5 年程度の若手で構成し，リーダーの教育・訓練やリーダー間の情報交換も原則オンラインで行う体制を考える．

3.2 人的多重防御の考え方

(1) 人的多重防御とは？

多くの標的型攻撃訓練では，「クリック率」を下げ，データの分析を行うことがルーティン／目的になっている．

勿論，クリック率を下げるための工夫，クリックした従業員に対し，クリックしてはいけない理由などの解説等も訓練中には行われている．訓練は，複数の訓練メールでの実施から，期間を設定した訓練まであるが，いずれにしても，クリック率はゼロにならない．

そこで，クリック率をゼロにするのではなく，その後の対応・処理を考え，**被害をゼロ**あるいは，**最小限に**することを考え，結果として，必要な目的を達成できると考えている．

(2) 人的多重防御事例[d]

ある従業員のミス／エラーを他の従業員による発見や対応ができれば，被害の防止や被害を最小限に抑えることができ，それを想定した教育・訓練が重要になる．

その対応方法としては，事前対応と事後対応が考えられる．

- **事前対応**：自組織に関連する情報収集を行い，必要とする部門へ情報提供をすることで，被害を防ぐ

図 3.2 では，BEC (Business Email Compromise) の被害例だが，海外送金で，リース会社になりすまし，リース会社の送金確認メールの受信直後に，送金口座番号が変更されたという電子メールを送り，偽口座へ送金を依頼した．偽メールの送信時のタイミングや内容が適切であったため，海外送金担当者はだまされてしまった．

BEC は，米国 FBI や国内セキュリティベンダーのブログ等で情報提供が行われており，適切な情報収集が行われ，担当部門に知らせていれば，被害を防げた可能性がある．

今回の例では，FBI の情報提供から被害発生まで，759 日，国内セキュリティベンダーのブログからでも，607 日あった．

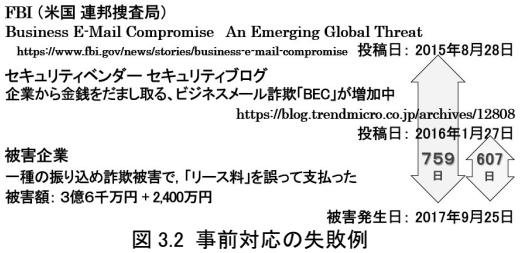

図 3.2 事前対応の失敗例

いわゆる，『**インテリジェンス**』と呼んでいるが，大規模な考えでは『**地政学 & インテリジェンス**』であるが，サイバーセキュリティでは，図 3.3 に示す「**インテリジェンス・サイクル**」が適切に機能すれば，多くの問題に対応ができる．

c 米国では，Lance Spitzner（SANS.org）が，Security Ambassador としており，ほぼ同じような考えがある

d マスコミ報道等を基に，調査分析であり，当該企業の対応を示したものではない

ⓒ 2022 Information Processing Society of Japan

Vol.2022-CSEC-98 No.35
Vol.2022-SPT-48 No.35
2022/7/20

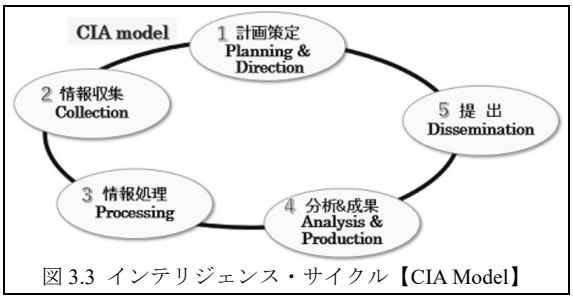

図 3.3 インテリジェンス・サイクル【CIA Model】

- 2013 年に発生した自治体での事件[4]では，自治体の複数部門への電話で個人情報の問い合わせであり，おかしいと感じた部門が関連部門への連絡をしたが，既に情報を窃取されていた．

➢ **事後対応**： クリック後の対応が良ければ，被害，即ち，情報窃取や情報の暗号化（ランサムウェア）を発生前に対応し，被害を防ぐ，あるいは，最小限の被害にするもの．

事後対応ができず，被害が発生した例．

- 『未達メール攻撃』がある．

① 顧客から添付ファイルの電子メールが送られてきたので，添付ファイルを開封したが、自社への内容でなかった、送付元へ 『弊社への情報ファイルではない』 と返信した

② 添付ファイルは、ウイルス感染目的で、クリックした時点で感染が始まったが、職員・組織とも、ウイルス感染プログラムとの認識がなかった

③ メールを返信したが，アドレスが顧客（送信元）にないメールアドレスで【未達メール】[e]が戻ってきたが，気づかなかった

事件の概要
④3 月 5 日（火）
添付ファイルを開き，顧客に返信したが，未達メールが返ってきた
⑤3 月 19 日（土）～24 日（木）
企業内情報漏えいが始まった

企業内の情報漏えいが始まった日より，4 日前に事件の前兆（未達メール）があり，この 4 日間に対応できていれば，事件を防ぐことができたと思われる．

当該企業では，標的型メール攻撃訓練を行っていたが，クリック率を下げることを目的にしており，セキュリティ部門（当時はなかったと言われている）で，利用者がおかしいと感じたことを報告する体制や各利用者などとの情報交換や攻撃の検討を行い，利用者が身近に相談できる体制が必要であったのではないだろうか？

e 送信元のメールサーバには，未達メールを返さない仕様のものもある

4. セキュリティ文化の構築

4.1 はじめに

標的型メール攻撃訓練に代表されるサイバーセキュリティ訓練の多くは，訓練時のリスクを減少（クリック率の低減）させるが，リスクはゼロにならず，リスクを残した形で教育・訓練が行われていないだろうか？

即ち，「訓練時点」でのリスクの最小化を目指していることに留まっている感じを受ける．

組織全体を考え，中長期的なセキュリティ教育・訓練を考えなければ，リスクをゼロに近づけることができないのではないだろうか？

勿論，最初から，組織全体のサイバーセキュリティを考えられないのであれば，**『セキュリティ ロードマップ』**を作成し，中長期のサイバーセキュリティ体制を構築すること，即ち，**『セキュリティ文化を構築』**することを目指し，高度で強固なセキュリティ組織の構築を考えることが望ましい．

4.2 ロードマップの作成

完璧なセキュリティ文化を最初から構築するのでなく，ロードマップを作成し，各段階に沿ってサイバーセキュリティ文化を構築する．

成熟度レベル	段階	概要
1	初期	プロセスは場当たり的で，秩序がない．レベル 1 の組織での成功は，実績のあるプロセルの使用によりもたらされる訳でなく，担当する人員の力量などに依存する
2	管理された	要件の管理，プロジェクトの計画，監視・精度測定などの基本的なプロジェクト管理が確実に行われる
3	定義された	プロセスは，標準，手順，ツール，手法を通して表現され，利用可能になっている．この標準プロセスは，各プロジェクト向けにテーラリング（手直し）して利用される
4	定量的に管理された	組織，プロジェクトは，品質とプロセス実績のデータを持ち，自分達の実施プロセスの実力を定量的に把握し，プロセス実施結果を予測する手法を持っている．この実力の理解を基に定量的目標を立て，プロセスを制御する
5	最適化している	レベル4での定量的理解を基に，今までにない新しい施策にも取り込める．また，改善のための根本的原因を探り，問題を未然に防止できる．更に，これらの施策の効果を定量的に評価でき，継続的な改善が実現される

図 4.1 CMMi の成熟度レベルと概要

組織がプロセス改善を行う能力の評価手法および指標で，ソフトウェア開発プロセスの成熟度である CMMi をモデルとし，利用者及び当該組織を対象とした成熟度モデル（Maturity Model）[3]を考え，ロードマップを作成し，推進を図る．図 4.1 は，CMMi の成熟度レベルとその概要で，図 4.2 は，CMMi をサイバーセキュリティにおける利用者とその組織での対応を考えた**『能力成熟度モデル統合』**である．

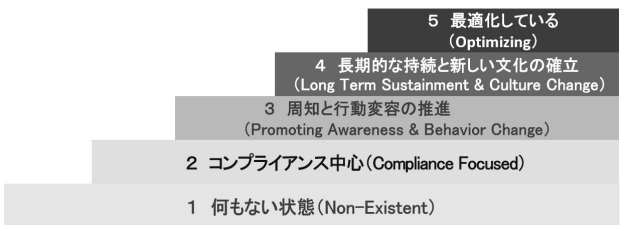

図 4.2 CMMi 能力成熟度モデル統合

このモデルを基に，各組織でのサイバーセキュリティ

ⓒ 2022 Information Processing Society of Japan

の成熟度レベルを考え，「レベル 5 最適化している」に達することが望まれる．

5. 終わりに

5.1 セキュリティ教育・訓練のめざす所

- 最近，サイバーセキュリティ分野でも，利用者への教育・訓練の必要性が言われるようになったが，「テストメール」をクリックした職員に，アラームを出し，次回はクリックしないように言葉を掛け，更に，各部門のクリック率や報告件数等を集計し，優秀部門には，賞品をだすこともあると聞いている．
- 心理学的考察をすれば，このような訓練は**キリスト教信者を発見するための『絵踏』**と同じで，発見が目的になっており，サイバーセキュリティの教育・訓練ではないと感じている．
- 組織内の全従業員が同じ方向を向き，セキュリティ文化の構築に進むことを考えるべきで，それは クリック率を下げることでなく，もっと広く，大きな観点から推進する必要があると感じていた．
  そのため，組織のセキュリティ文化の構築に結びつけることができれば，セキュリティ対応で大きな進展が望めるのではないかと思っている．

5.2 セキュリティ文化の目指す所

- セキュリティ文化は、組織内の全ての人が，なすべきことと知っており、それが正しいと信じられるセキュリティ上の考え方や習慣である
- セキュリティ文化が醸成されることにより，ルールで厳しく縛ることなく、また、いちいち指導することなく、組織としてあるべきセキュリティの維持向上に従業員が自然に行動するようになる
- この状態が醸成されることにより、組織内部での悪意ある行為は抑制され、過失によるインシデントも相互扶助的な予防や早期発見ができ、セキュリティ管理投資を大幅に低減できる
- セキュリティ文化は、一朝一夕に構築できない．
  Lance Spitzner はレベル 5 に達するには，5〜10 年かかる[3]と言っている．
  経営者のリーダーシップが前提だが，国内組織の環境を考えれば、もう少し短期間でできる可能性はあると考えている．
- セキュリティ文化に関しては，2002 年 8 月，「OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security（情報システム及びネットワークのセキュリティのためのガイドライン：セキュリティ文化の普及に向けて）」[5]を発表しているが，国内では，注目度が高くない．
- 一方，海外では，コロナウイルスの影響により，テレワーク業務等により，従業員がフィッシング攻撃等で，パスワードを開示したりしており，この時期こそ，セキュリティを全社で考えるべきだとの議論[6] [7] [8]が行われている．
- セキュリティ文化の構築は，町内会の「お祭り」と考えられるのではないだろうか？ 組織内の全ての人が，セキュリティ構築のため，1 つの方向に進むことであろう．
  利用者教育・訓練では，Gamification を導入し，楽しみながら，セキュリティの推進を行い，効果を上げている組織もある．
  1980 年代の中頃に，横浜国立大学で行われていた暗号勉強会は『明るい明号研究会』と名付けられていたと聞き，1990 年代の初めに，情報セキュリティを『楽しいセキュリティ』とし，
  明るい明号，楽しいセキュリティ
  というキャッチフレーズを提案したが，採用されることはなかった．

5.3 今後の課題

- この様なセキュリティ文化の構築を目指している国内組織については，寡聞にして知らない．
- Lance Spitzner（SANS.ORG）が米国で「Security Ambassador」を任命し，対応する方法を提案しているが，2017 年に開催された教育・訓練[3]で話があったが，まだ，結果がでている段階ではないと思われる．
- 利用者向けキュリティ教育・訓練は，国内ではまだ途に就いたばかりであり，多くのセキュリティベンダーの方法も，優れたものがあるが，クリック率を下げる訓練が中心であり，目的を達成できるか疑問が残る．
- 現時点では，今回の報告を実施できる環境（組織での実施）がないため，今後は，その対応を目指したい．

謝辞 本報告書作成に以下の方々に貴重なご意見を頂き，厚くお礼を申し上げます．

- 日本心理学会・情報セキュリティ心理学研究会メンバー及びウェブへの参加の方々
- 前衆議院議員 福田峰之氏
- 九州大学 リカレント講座：SECKUN 推進者：小出洋教授，前推進者 藤岡福資郎氏

参考文献

[1] Businessweek, The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies, https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies
[2] NRI Secure，NRI Secure Insight 2021，https://www.nri-secure.co.jp/download/insight2021-report，pp22
[3] Lance Spitzner, Securing The Human: How to Build, Maintain and Measure a High-Impact Awa

ⓒ 2022 Information Processing Society of Japan

Vol.2022-CSEC-98 No.35
Vol.2022-SPT-48 No.35
2022/7/20

reness Program, MGT433, SANS.ORG
[4] 埼玉県吉川市，官公庁職員を名乗って市役所に電話で問い合わせ(平成 25 年 11 月 29 日発表)，入手先（http://www.city.yoshikawa.saitama.jp/sp/index.cfm/26,42250,181,942,html）（削除）
[5] OECD, Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, 2002 年 8 月
[6] Steve Thomas, How to build a culture of security, 2020.11 https://www.securitymagazine.com/articles/93980-how-to-build-a-culture-of-security
[7] International Civil Aviation Organization（ICAO）, Security Culture, https://www.icao.int/Security/Security-Culture/Pages/default.aspx
[8] Perry Carpenter, The Importance Of A Strong Security Culture And How To Build One, 2021.05, https://www.forbes.com/sites/forbesbusinesscouncil/2021/05/27/the-importance-of-a-strong-security-culture-and-how-to-build-one/?sh=618e7b356d49

ⓒ 2022 Information Processing Society of Japan