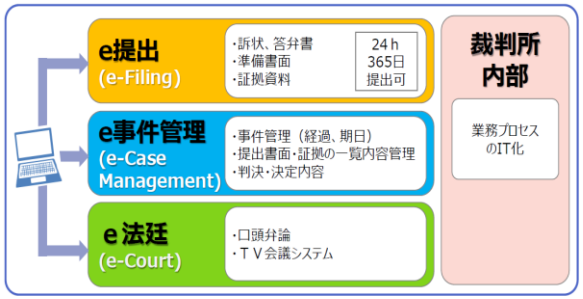
資料１

裁判手続等のIT化にともなうサイバーセキュリティについて

デロイト トーマツ リスクサービス株式会社
2018年2月22日

何を守るのか（情報の機密性は電子データか紙であるかを問わない）

情報のCIA（機密性・完全性・可用性）の観点から



保護対象を分類し、機密性の区分（高・中・低など）を明確にすることが重要
（例：政府機関の情報セキュリティ対策のための統一基準）

機密性3	行政事務で取り扱う情報のうち、秘密文書に相当する機密性を要する情報
機密性2	行政事務で取り扱う情報のうち、秘密文書に相当する機密性は要しないが、漏えいにより、国民の権利が侵害され又は行政事務の遂行に支障を及ぼすおそれがある情報
機密性1	公表済みの情報、公表しても差し支えない情報等、機密性2情報又は機密性3情報以外の情報

機密性
機密情報が漏えいしない

一連の裁判手続で取り扱われる機密性の高い情報（例）

- 高度の機密性が求められる裁判所が管理する文書（判決が出るまでの期間、特に機密性が高い裁判官のメモやドラフト等を含む）
- 訴訟記録の機密性のある情報

※必ずしも法令によりアクセス権が明確でない場合、詳細にポリシーを定める必要がある

完全性
情報が改ざんされない

裁判手続では「情報が正しい」ということは一般企業よりも重要

- 証拠等の関連情報に改ざんがあれば裁判手続の円滑な進行を妨げ、最悪のケースでは判決に影響があるかもしれない（紙を使った証拠調べの手続があるため、途中で改ざんが判明し回復することは可能と思われる）

可用性
情報が失われない

情報の喪失だけでなく、システム停止による業務停止のリスクがある

- システムが停止することによる裁判手続の停止ややり直しが起きる
- 情報が喪失することで裁判手続が滞る（おそらく原本は喪失しない）

何から(誰の、どんな攻撃から)守るのか

脅威を想定する

外部者によるサイバー攻撃

- 通常攻撃者は経済的利益や社会的思想、国家的利益などを目的(インセンティブ)としているが、裁判手続に関する情報を窃取するインセンティブと動機は攻撃者にとってあまり大きくない。

内部関係者による不正行為

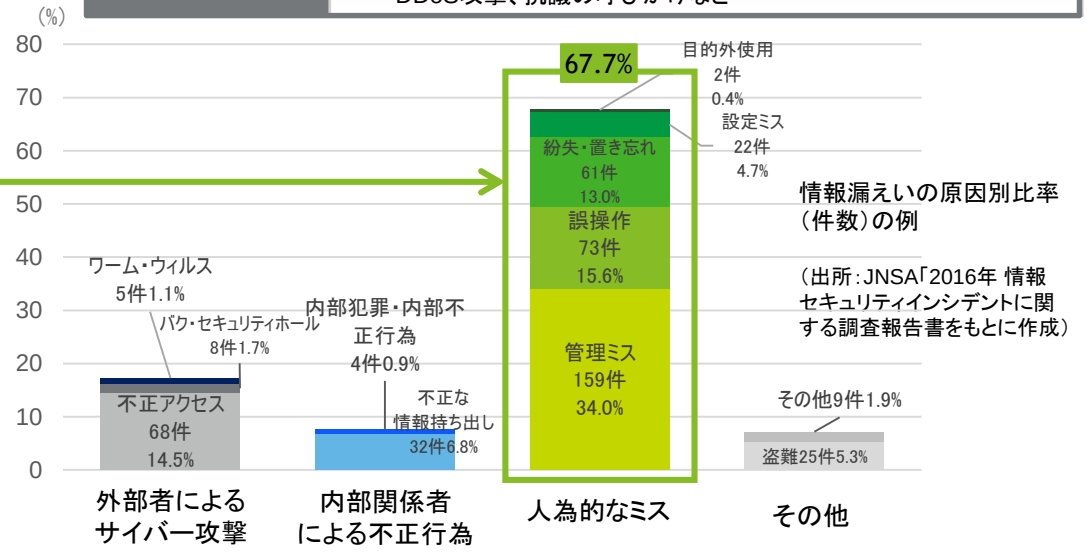
- 裁判所の内部関係者・原告・被告等(本人・企業関係者)・弁護士等・システム運用等の外注先企業などが考えられるが、 争っている相手方に対するなりすましによる不正アクセスなどはあまりインセンティブがない。

人為的なミス

- 紙・電子データを問わず最も多い漏えいの原因は管理ミスや誤操作、紛失置き忘れなどの人為的なミスである。

参考:サイバー攻撃者の類型

ハッカー	■ 知識欲、自己顕示欲など個人的欲求に基づき活動 ■ 活動例として、不正アクセス、DDoS攻撃など
サイバー犯罪者	■ 金銭的利益を目的として活動 ■ 実際に攻撃を行う者、ツールを開発する者など分業化が進展 ■ 活動内容は広範で、大企業から個人まで幅広く標的
国攻撃グループ	■ 国家意志に基づき活動 ■ 活動例として、政府機関、インフラ事業者、先端産業に対するスパイ行為など
サイバーテロリスト	■ テロの実行や思想の普及を目的として活動 ■ 活動例として、Webサイト改ざん、DDoS攻撃のほか、テロの呼びかけなど
ハクティビスト	■ 思想上の目標達成のために活動 ■ 思想の代表例として、環境保護、動物愛護、言論の自由など ■ 活動例として、政府、大企業などを標的としたWebサイト改ざん、DDoS攻撃、抗議の呼びかけなど



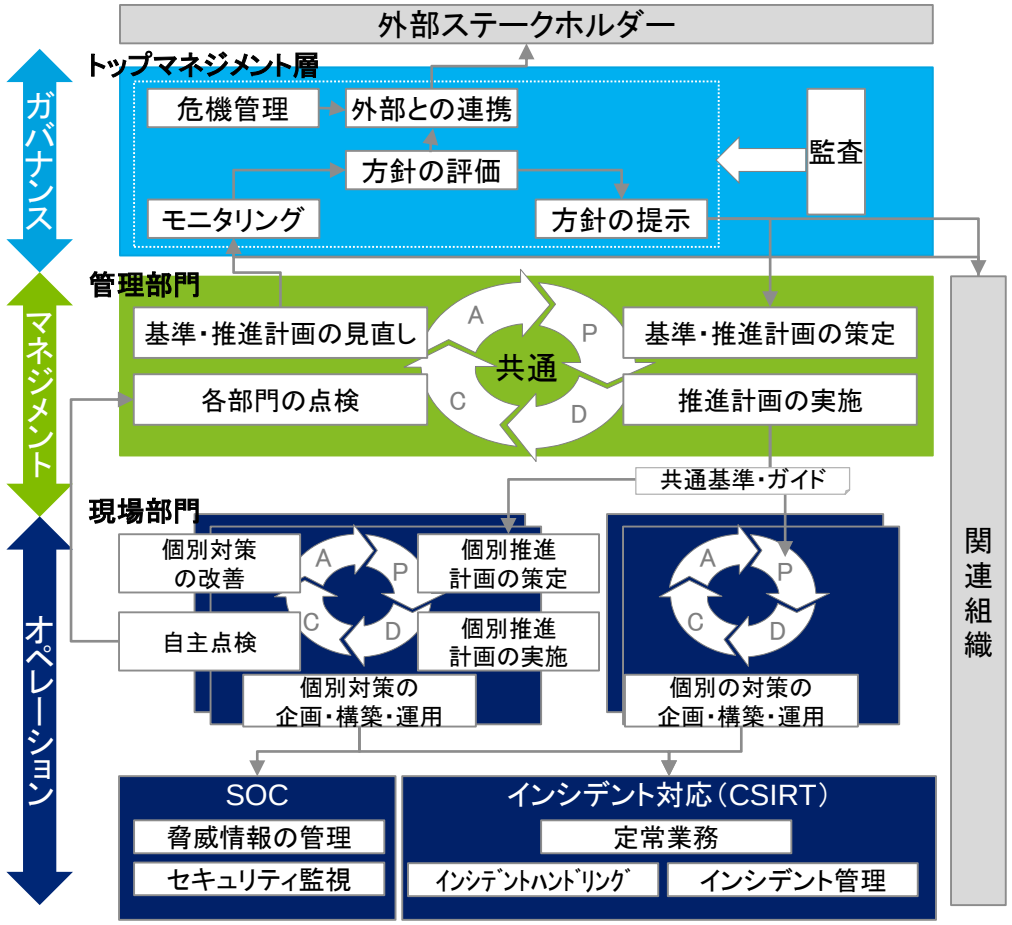
情報漏えいの原因別比率(件数)の例

(出所:JNSA「2016年 情報セキュリティインシデントに関する調査報告書をもとに作成)

どのように守るのか
セキュリティ対策を維持し運用できる体制が重要であり、技術的に守るだけではない

構築すべき情報セキュリティマネジメント体制の例（セキュリティ3層モデル*1）

あるべきセキュリティ管理体制の業務構造（例）



情報セキュリティマネジメントの要素

人的対策：
職員等への継続的な教育・研修や啓蒙等による現場レベルでのリテラシー向上等

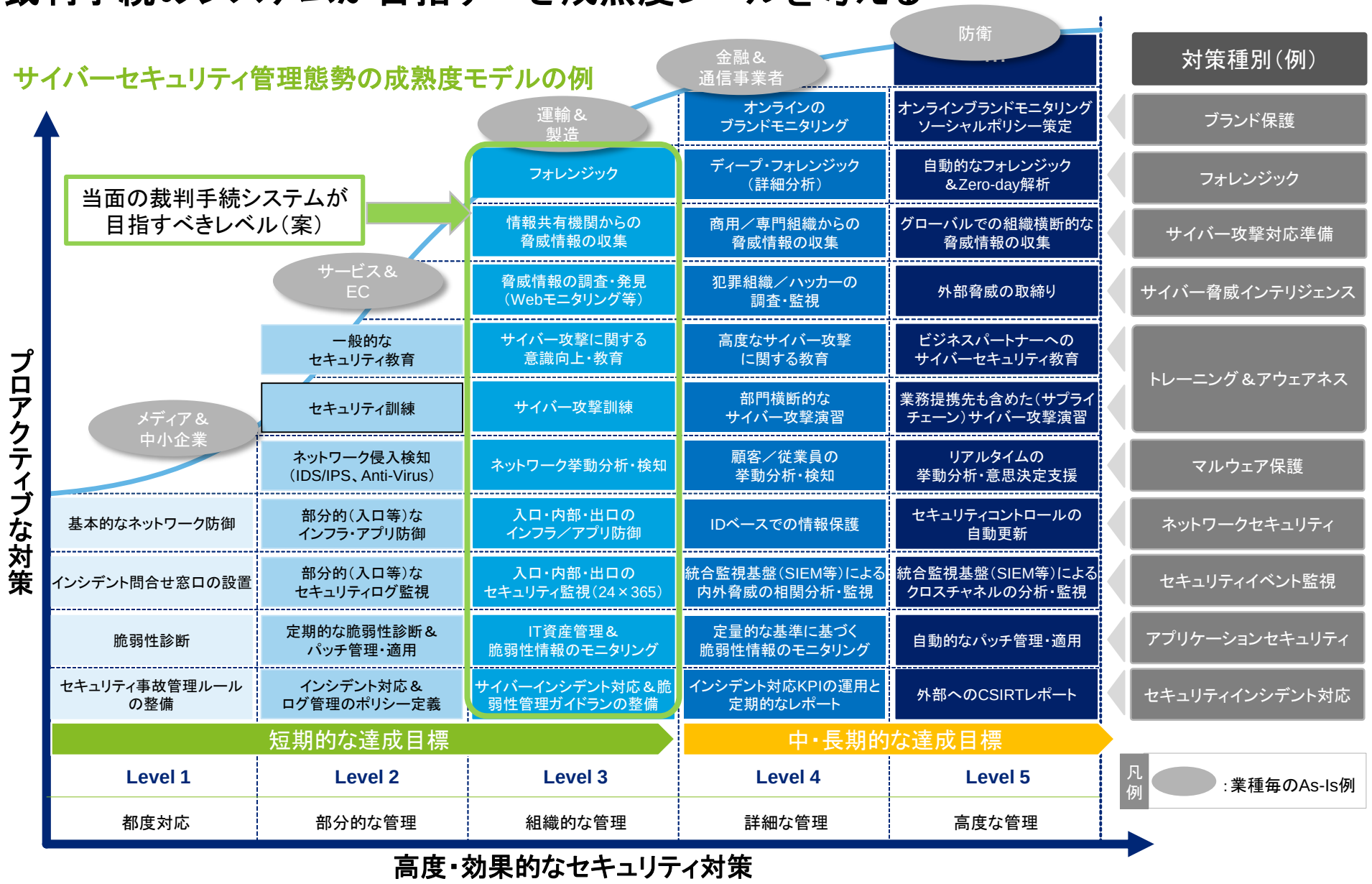
組織的対策：
組織におけるポリシー等のルール策定、情報セキュリティマネジメントのための組織づくり、運用に対する監査の実施等

物理的対策：
建物、部屋、関連設備（電源・空調・消火設備・監視カメラ等）等、物理的なセキュリティ対策の実施

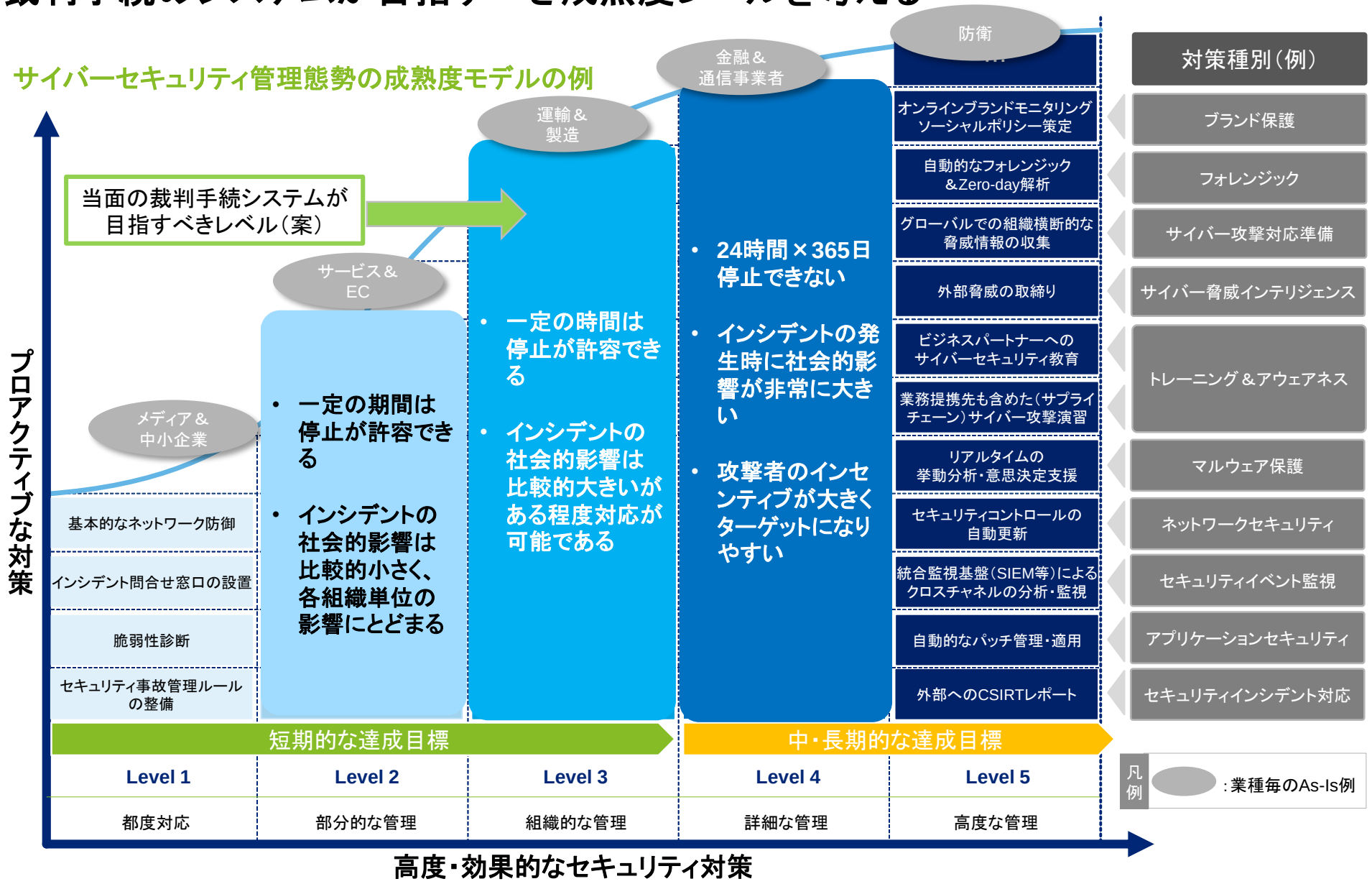
技術的対策：
各脅威に対する防御、発見、対応、復旧に関わる技術的対策の実施等（認証やアクセス制御、ファイア・ウォール等）

目指すべきセキュリティ対策のレベルを定義し、その成熟度を達成・維持できるようなマネジメント体制を確立する必要がある。その上で技術的な対策を実施するべきであるが、社会的な責任と問題発生時の影響度に鑑みて過剰投資ではないレベルを設定すべき。（当面、軍事・安全保障や警察、メガバンクのレベルまでを目指す必要はない）

どの程度守るのか①
裁判手続のシステムが目指すべき成熟度レベルを考える



どの程度守るのか②
裁判手続のシステムが目指すべき成熟度レベルを考える



どの程度守るのか③
リスクの大きさに応じた技術的対策が重要である

金融機関等におけるセキュリティ対策の例

■ 金融機関等では、各種の技術的対策で認証強度向上によるなりすましの防止を行っている。ただし裁判手続をIT化し、弁護士等の関係者にインターネットを経由したシステムへのアクセスを認める場合、厳密なID管理手続（ID・パスワード等を取得するための承認手続や、定期的な棚卸、不要になった際の迅速な削除等、一連の管理手続）及びそれを支援するシステムが必要となる。
■ 金融機関で採用されている認証強化策は相応のコストで賄われており、リスクの大きさとのバランスで選択する必要がある。

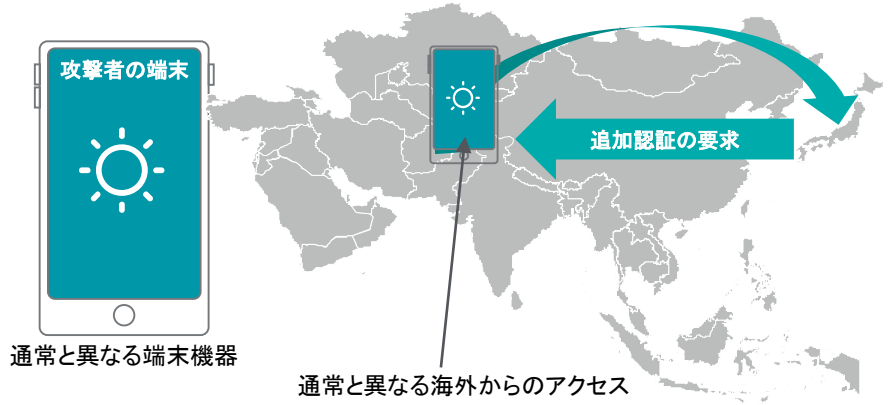
銀行における認証強化の例（多要素認証）

通常の残高や履歴の閲覧はID・パスワード（一定のパスワードポリシーを強制的に適用し、単純・推測可能なパスワードの利用を防止）を利用し、振り込み操作（未登録の振込先）の際は別途スマートフォンアプリに実装したワンタイムパスワードや、専用のパスワードカードを使って多要素認証を要求する。この操作により、なりすました第三者による任意の口座（攻撃者が現金を引き出す）への振り込みを防止している。

スマホアプリの例　専用カードの例

銀行や大手SNSにおける認証強化の例（リスクベース認証）

通常本人が利用している端末ではない機器（PC・スマホ等）からアクセスした場合や、アクセス元の地域、ロケーションが通常と異なる場合等には「なりすましの可能性がある」と判定し、通常のID・パスワードに加えて、別のパスワード要求や、登録した携帯電話にSMSによるワンタイムパスワード送信を行う等、追加認証を行うことで第三者によるなりすまし操作を防止している。



通常と異なる端末機器　通常と異なる海外からのアクセス

どの程度守るのか④
リスクの大きさに応じた技術的対策が重要である②

インターネットを利用した会議システムの例

■ Skype、WebEX等の利用やインターネット経由でのアクセスについて、暗号化等の対策でネットワーク上での盗聴は相当程度防止することができる。このため、情報の機密性が高い場合や証人の保護が必要な場合であっても、e-法廷は既存のサービスを利用することも検討できる。

Skypeのセキュリティ:

マイクロソフトが「Private Conversations」と呼ばれる機能を通じて、「Signalプロトコル」を利用した通話、テキストメッセージ、マルチメディアメッセージでエンドツーエンドの暗号化を発表した。(現時点ではβ版であり、ビデオ通信には非対応)

(出所:https://answers.microsoft.com/en-us/skype/forum/skype_insiderms-skype_insnewsms/skype-insider-preview-private-conversations/01616ac9-2171-4151-b9a2-c77761c0fbf8?tm=1515686754397&auth=1)

WebEXのセキュリティ:

SSL 3.0 および 128 ビットまたは 256 ビット AES 暗号化を使用した安全な会議を提供しており、米国国防総省グレードの FIPS 140-2 Level 1 暗号化をサポートしている。またBYODやDMZとの兼ね合い、ポート 80(HTTP)とポート 443(SSL)でのシンプルなポート転送など企業向けの安全対策が行われている。

(出所:https://www.cisco.com/c/ja_jp/products/conferencing/webex-meetings-server/index.html)

暗号技術の実装例

AES(Advanced Encryption Standard)
NIST(米国立標準技術研究所)によって選定された暗号方式。
VPNやSSLの実装にも利用されている要素技術となっている。

VPN(Virtual Private Network):
データを安全に通信するために用いられるネットワーク技術のこと。インターネット上に「仮想の専用回線」を作ることによって、「パブリック」な公衆網であるインターネットをあたかも「プライベート」な専用線のように使うことができる。仮想的なトンネルを構築しデータの暗号化を行って通信することで、遠隔地との通信の安全性を高め、情報漏洩や改ざんリスクを軽減することができる。

SSL(Secure Sockets Layer)とTLS(Transport Layer Security):
インターネット上でデータを暗号化して送受信する仕組み(プロトコル)。公開鍵暗号と電子証明書を利用して、送信する情報を暗号化するために利用することで、送信される情報を悪意を持った第三者から守ると同時に、送信される情報が改ざんをされていないことを証明することができる。またこれにより否認の防止にも利用できる。

まとめ

情報の機密性、リスクに応じた対策が重要

1. サイバーセキュリティ対策は「何を」「何から」「どのように」守るのか、を適切に考えることが重要である
2. リスク（影響度）に応じた対策によって「どの程度」守るのか、目指すべき成熟度を検討・設定することが重要であり、過剰な対策で利便性を損ねるのは本末転倒
3. 裁判手続のIT化は防衛や金融、通信事業者のシステムに比べリーズナブルに実現できる可能性が高い

ご参考：サイバー脅威の主な類型（例）

サイバー脅威の全体像を整理した例（民間）

■ 裁判手続をIT化する場合、企業における社内システムまたはクラウド上のシステムを想定する