Information Security

Basic Approach

Approach Policy

Toppan controls information security and cyber security across the Group in the recognition that appropriate and safe management of information and systems necessary for business is a significant managerial challenge for the Group as Toppan grows as a leader in addressing global social agendas.

The threat of cyber-attacks has been mounting with the advancement of the IoT and rapid digital transformation. These attacks can result in the leakage of information assets, including personal information or confidential information, and endanger business continuity per se.

In keeping with the Toppan Group Basic Policy on Information Security, Toppan applies secure technologies and rigorous control in operations throughout the Group to drive digital transformation initiatives that enhance corporate value and reciprocate the trust of customers and society. The Group has been introducing various systems and tools to counter cyber-attacks and reinforcing safeguards across the tightly secured areas where personal information is handled throughout Japan.

More details on the Toppan Group Basic Policy on Information Security
https://www.toppan.com/en/about-us/our-corporate-approach/security-information.html ›

More details on the Personal Information Protection Policy
https://www.toppan.com/en/privacy.html ›

Toppan Group Basic Policy on Information Security

As a group of companies operating in the information communication industry, each of us at the Toppan Group carries out Groupwide information security management in the recognition that the management of information necessary for business is a significant managerial challenge for us as a means to reciprocate our customers' trust and promote the ongoing growth of the Toppan Group.

1. We manage information necessary for our business appropriately in observance of our in-house rules, the law, and the principles of social order.
2. We collect information for appropriate purposes using appropriate methods.
3. We safely manage the information entrusted to us by customers in order to reciprocate our customers' trust.
4. We are deeply aware of the risks to the information assets we handle, such as illegal access, loss, damage, falsification/manipulation, and leakage of information, and take necessary and reasonable safety measures against these risks. We deal with and rectify any problems that occur promptly and in an appropriate manner.
5. We establish, operate, maintain, and continuously improve information security management systems.

Established on April 1, 2001
Revised on June 27, 2019

Hideharu Maro
President & Representative Director
Toppan Inc.

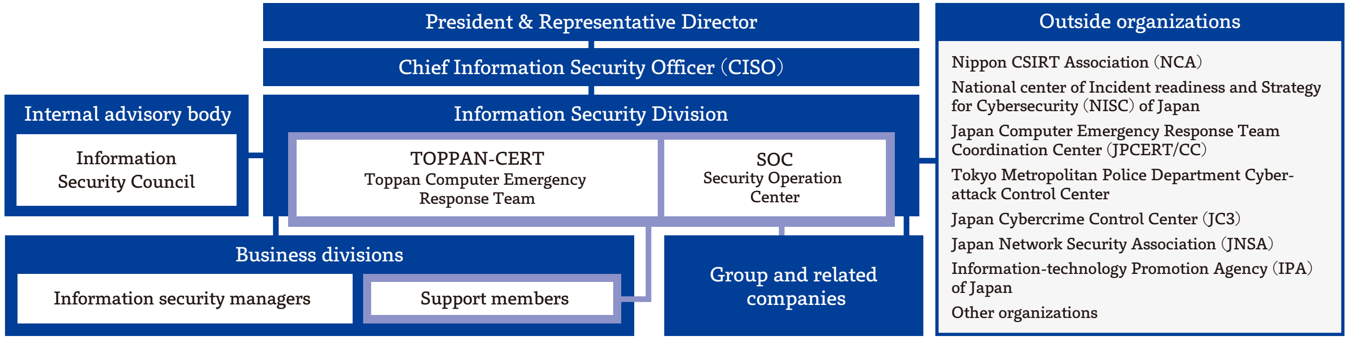
Promotion Framework

Promotion framework

Under the direction of the Chief Information Security Officer (CISO), the Information Security Division and specialist technical teams work together to manage information security at Toppan by overseeing business divisions and Group companies in cooperation with outside expert organizations.

In parallel, information security managers in the business divisions and Group companies work to ensure the safety of their organizations according to instructions issued by the head office.

Organizational Structure for Information Security Management


President & Representative Director
Chief Information Security Officer (CISO)
Internal advisory body
Information Security Council
Information Security Division
TOPPAN-CERT
Toppan Computer Emergency Response Team
SOC
Security Operation Center
Business divisions
Information security managers
Support members
Group and related companies
Outside organizations
Nippon CSIRT Association (NCA)
National center of Incident readiness and Strategy for Cybersecurity (NISC) of Japan
Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)
Tokyo Metropolitan Police Department Cyber-attack Control Center
Japan Cybercrime Control Center (JC3)
Japan Network Security Association (JNSA)
Information-technology Promotion Agency (IPA) of Japan
Other organizations

Information Security Management Structure

Promotion framework

Information Security Management

Under the Chief Information Security Officer (CISO), the Information Security Division formulates a Groupwide information security plan, sets up rules and regulations, and disseminates and reviews them. The division convenes regular meetings with members from business divisions and related companies to share the details of information security polices and measures underway.

The Information Security Division also carries out regular audits of business divisions and related companies to check the quality of their security control and recommend corrective measures as necessary.

The results of these activities are regularly reported to the CISO. When a security incident arises, the division promptly initiates the Group's response and reports the present status to the CISO as required.

Arranging Remote Working Environments

Toppan has reviewed the Group's information security rules for remote working and formulated standards for the use of communication tools to ensure safe working environments outside of the office. A system has been introduced to enable Group employees to promptly report suspicious incoming emails and virus-infection incidents while working from remote locations.

Remote approaches have also been adopted for internal audits and audits of various other types to confirm information security management throughout the Group.

Revising Rules to Enhance Security Management

Toppan's rules and regulations on information security management have been established based on the ISO/IEC 27000 standard for information security management systems (ISMS) and comply with the JIS Q 15000 standard for personal information protection management systems (PMS). To sustain its ISMS and PMS, Toppan needs to ensure robust governance of information security throughout the entire Group, including overseas sites, and to better respond to emerging requirements in areas such as cyber security, the use of data, the IoT, and globalization. Toppan duly formulated a set of baseline standards for monitoring conformance with the Toppan Group Basic Rules on Information Security in fiscal 2021. The Group's control over information security has been reinforced through checks on conformance at Group companies.

Complying with Laws and Regulations

Activity results, performance data

The Toppan Group complies with the amended Act on the Protection of Personal Information of Japan, the EU General Data Protection Regulation, and other information-protection legislation around the world.

Japan's Amended Act on Personal Information Protection

The Toppan Group has revised its rules on information security management within Toppan Inc. and various other Group rules related to the handling of personal information to ensure compliance with the amended Act on the Protection of Personal Information enforced in Japan in April 2022. The Group has also set up procedures for handling personal information and anonymously processed information, notifying individuals when their information is provided to third parties outside of Japan, and submitting incident reports whenever necessary. The procedures are closely modeled after the guidelines announced by the Personal Information Protection Commission of Japan.

International Legislation on Personal Information Protection

To address globalized business operations, Toppan specifies the Group's global standards on personal information management in accordance with the core principles of the General Data Protection Regulation (GDPR) issued by the EU. Toppan seeks to handle personal information in conformance with the applicable legislation of every relevant country.

PrivacyMark Accreditation and ISMS Certification in Japan

Toppan's information security systems have received PrivacyMark accreditations and information security management system (ISMS) certification across Japan.

The Group is formulating in-house rules, building environments, and training personnel in charge to secure the handling of important information received from customers, personal or otherwise.

Japan's Individual Identification Number System

The Toppan Group has added new requirements for its security control measures under in-house standards for tightly secured areas, based on guidelines for the proper handling of specific personal information issued by the Japanese government's Personal Information Protection Commission. These security measures cover operations involving specific personal information, such as the handling of individual identification numbers under Japan's Social Security and Tax Number System and the collection of those numbers on behalf of Toppan's client companies.

Toppan has set up a room dedicated solely to the handling of these personal identification numbers, and a special team carries out accreditation audits on operations performed therein.

Protecting Personal Information and Confidential Information

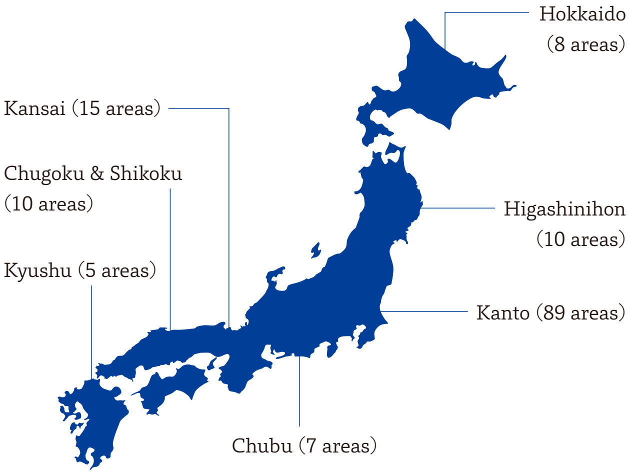
Activity results, performance data

Secured Areas for the Handling of Personal Information

Operations involving the use of confidential materials in the Toppan Group are conducted exclusively within a closed network environment and in tightly secured workplaces where the comings and goings of employees through entrances and exits are monitored to minimize the risk of fraudulent acts and other forms of misconduct inside of the Group and the risk of unauthorized access from outside of the Group. Strictly controlled operations include the handling of personal information (e.g., individual identification numbers under Japan's Social Security and Tax Number System) and the production and handling of security printing products with monetary value.

The Toppan Group found no instances of unauthorized information removal or other personal information-related incidents in fiscal 2021. Strict efforts to maintain a record of zero-incidents across the Group will be maintained.

Secured Areas for Handling Personal Information in Japan (As of March 31, 2022)



Controlling the Secured Areas

The Toppan Group seeks to ensure and upgrade security levels in the handling of personal information through regular internal audits and day-to-day operation checks based on operational management rules for the tightly secured areas within the Group.

Two key components of Toppan's security management regime are internal audits to inspect operational management and monitoring to detect fraudulent operations.

Operational management inspection through internal audits: Dedicated auditors regularly inspect the installation, management, and operation of tightly secured areas designated for the handling of personal information. Managers assess and accredit inspection results to maintain and further enhance operational management levels across the Toppan Group.

Detection of fraudulent operations: As a basic rule, Toppan prohibits Group employees from connecting any external memory media to the PCs used within the tightly secured areas. The Group's monitoring center carries out operational log analysis using log management systems. Whenever a potentially fraudulent log is detected, the center immediately notifies the relevant management personnel for verification.

Security Measures

Surveillance camera

Access control

Controlling Security across the Supply Chain

Toppan entrusts some of its operations involving the handling of personal information and confidential information to Group and partner companies. Toppan also relies on the cloud services of external companies in performing some of the Group's business operations.

Toppan strives to mitigate supply chain risks by checking the safety of cloud services and auditing subcontractors to confirm that their controls satisfy the Group's security standards. The levels of control required of subcontractors depend on the types of information and operations entrusted to them.

Countering Cyber-attacks

Activity results, performance data

Cyber-attacks pose especially significant security risks to Toppan. The Company has been implementing various measures to mitigate them.

Installing the EDR Application on PCs across the Group

In 2019 Toppan began installing Endpoint Detection and Response (EDR), an application that detects suspicious behaviors in PCs. The application is now installed in all PCs used for administrative work across the Group. The next step will be to install the EDR application on terminals used onsite in production settings, as well as on Apple computers and network servers. Toppan will continue to strengthen the system for detecting and countering sophisticated malware.

Using a CASB Service to Mitigate Cloud-usage Risks

The growing usage of cloud services is driving up the amount of important information handled by cloud-based applications. From fiscal 2020, Toppan began using a Cloud Access Security Broker (CASB) service that visualizes and controls computer usage in cloud environments. CASB enhances the safety of cloud-service usage by identifying risks associated with individual cloud services and detecting and restricting cloud usage subject to unduly high risk.

Implementing Threat Intelligence and OSINT Activities

Toppan continues to implement threat intelligence and Open Source Intelligence (OSINT) activities to uncover signs of cyber-attacks against the Group and detect vulnerabilities visible to outside parties early on. Toppan strives to mitigate cyber-attack risks by addressing weaknesses detected within the Group before attacks can occur.

Upgrading Website Vulnerability Assessments

Weaknesses in Toppan's web applications have been assessed to counter cyber-attacks targeting website vulnerabilities. An automatic vulnerability detection system is now installed to periodically diagnose the network and address vulnerabilities that become apparent from day to day. This system reinforces the Group's ability to provide customers with more tightly secured services.

Countering Email Attacks

Cyber-threats continue to grow with the return of the malicious botnet Emotet and the rising frequency of fraudulent emails and business email compromise (BEC) crimes, where a cyber-criminal sends an email that appears to come from a familiar business acquaintance with the intent of stealing money or specific information. Starting from fiscal 2022, Toppan will be combatting these threats by launching an advanced service that uses AI analyses and machine learning to screen incoming emails. This service will mitigate targeted email attempts to steal money, exploit information, or compromise networks in other ways. Toppan will continue solidifying its systems to resist email attacks throughout the Group.

Acquiring Third-party Certification

Activity results, performance data

Toppan Inc. and Group companies have acquired ISO/IEC 27001 certification for information security management systems (ISMS), PrivacyMark accreditations under Japanese Industrial Standards (JIS) Q 15001:2017 for personal information protection management systems (PMS), and other third-party certifications.

ISMS Certification (ISO/IEC 27001) for Information Security Management Systems

Information & Communication Division (Toppan Inc.); Business Platform Department (Digital Innovation Division, Toppan Inc.); Technical Department (Integration Business Center, DX Design Division, Toppan Inc.); Toppan Communication Products Co., Ltd.; Toppan Graphic Communications Co., Ltd.; TGS Inc.; TB Next Communications Co., Ltd.	IC06J0151
Toppan Group Kansai Business Center (Toppan Forms Co., Ltd.)	JQA-IM0137
Toppan Infomedia Co., Ltd.	JUSE-IR-404
Asaka Plant and Shiga Plant (Toppan Inc.); Semiconductor photomask operations (Asaka Plant and Shiga Plant, Toppan Electronics Products Co., Ltd.); Design, development, commissioned manufacture, and management of products related to semiconductors (Toppan Technical Design Center Co., Ltd.)	IS 530416
ONE COMPATH Co., Ltd.	IS 533218
Kyushu, Chugoku & Shikoku Team and ISMS Promotion Committee (Information Security Management, Nishinihon Division, Toppan Inc.)	I308
Kansai Production Department (Toppan Graphic Communications Co., Ltd.)	IC13J0361
Higashinihon Division (Toppan Inc.)	IS 606897
Takino Plant (Toppan Communication Products Co., Ltd.); Takino Information & Communication Production Engineering Team (Kansai Technology, Kansai Subdivision, Toppan Inc.)	IC14J0376
Secure BPO Team (Chubu Division, Toppan Inc.); Chubu Production Department (Toppan Graphic Communications Co., Ltd.); Nagoya Plant (Toppan Communication Products Co., Ltd.)	IC17J0444
One undisclosed entity	

PrivacyMark Accreditations (JIS Q 15001:2017)

Toppan Inc.	10190891
Toppan Communication Products Co., Ltd.	24000216
Toppan Graphic Communications Co., Ltd.	10190298
Toppan Editorial Communications Co., Ltd.	24000308
Toppan Logistics Co., Ltd.	10450006
Toppan Travel Service Corp.	10450093
Toppan Forms Co., Ltd.	10190934
Toppan Forms Central Products Co., Ltd.	24000366
Toppan Forms Tokai Co., Ltd.	24000204
Toppan Forms Kansai Co., Ltd.	24000101
Toppan Forms Nishinihon Co., Ltd.	18860028
Toppan Forms Operation Co., Ltd.	10820089
Toppan Forms Logistics and Services Co., Ltd.	10450002
Toppan Forms (Hokkaido) Co., Ltd.	10190307
TOSCO Corp.	11820447
J-SCube Inc.	10860018
Tosho Printing Co., Ltd.	24000032
Tokyo Shoseki Co., Ltd.	10190966
Livretech Co., Ltd.	10190035
Tokyo Logistics Co., Ltd.	10860071
EduFront Learning Research Co., Ltd.	10861827
Froebel-Kan Co., Ltd.	24000369
BookLive Co., Ltd.	28000007
T.M.G. Challenged Plus Toppan Co., Ltd.	24000419
ONE COMPATH Co., Ltd.	24000445
Toppan Cosmo, Inc.	24000449
UNIWORX Co., Ltd.	21004696
Kirihara Shoten K.K.	24000459

Information Security Training

Training, education

Intensifying Training and Self-assessment

In fiscal 2021, regular group training was organized under the theme of "Staying ahead of change—Addressing risks as an advanced, reliable corporation." Participants learned about evolving information security risks, security risks to be recognized in the teleworking era, and the newly established Toppan Group Basic Policy on Information Security.

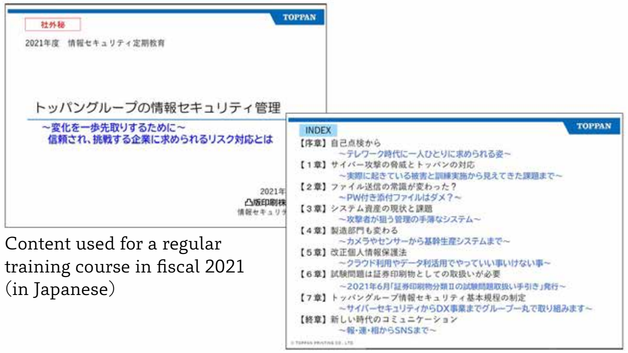
Personnel using Toppan email addresses continued to receive e-learning-based training attuned to their individual working styles.

For employees engaged in production, courses on specific risks on manufacturing premises are also arranged online in place of group training.

The Group also held division-specific training along with training sessions for persons handling individual identification numbers under Japan's Social Security and Tax Number System.

In parallel with training, Toppan works on a self-assessment initiative to ensure information security across the Group. This initiative aims to enhance individual awareness of everyday behaviors by visualizing security management at a level of detail not discernible by internal audits. Reviewing self-assessment reports sent in from different departments, the Group offers managerial staff suggestions for improvement and encourages them to take necessary actions at their workplaces.

A checklist item was added to the self-assessment sheet in fiscal 2021 to address a surge of cyber tricks triggered by virus-infected ZIP files delivered as email attachments with password prompts. This checklist item reminds Group employees of the need to use approved file transfer and storage services and to refrain from sending password-protected ZIP files as email attachments.



TOPPAN

社外秘

2021年度　情報セキュリティ定期教育

トッパングループの情報セキュリティ管理

～変化を一歩先取りするために～
信頼され、挑戦する企業に求められるリスク対応とは

2021年
凸版印刷株
情報セキュリテ

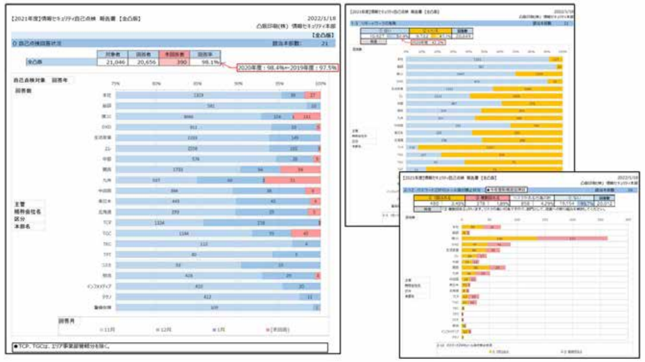
TOPPAN

INDEX

【序章】自己点検から
～テレワーク時代に一人ひとりに求められる姿～
【１章】サイバー攻撃の脅威とトッパンの対応
～実際に起きている被害と訓練実施から見えてきた課題まで～
【２章】ファイル送信の常識が変わった？
～PW付き添付ファイルはダメ？～
【３章】システム資産の現状と課題
～攻撃者が狙う管理の手薄なシステム～
【４章】製造部門も変わる
～カメラやセンサーから基幹生産システムまで～
【５章】改正個人情報保護法
～クラウド利用やデータ利活用でやっていい事いけない事～
【６章】試験問題は証券印刷物としての取扱いが必要
～2021年6月「証券印刷物分類Ⅱの試験問題取扱い手引き」発行～
【７章】トッパングループ情報セキュリティ基本規程の制定
～サイバーセキュリティからDX事業までグループ一丸で取り組みます～
【終章】新しい時代のコミュニケーション
～報・連・相からSNSまで～

© TOPPAN PRINTING CO., LTD.

Content used for a regular training course in fiscal 2021 (in Japanese)

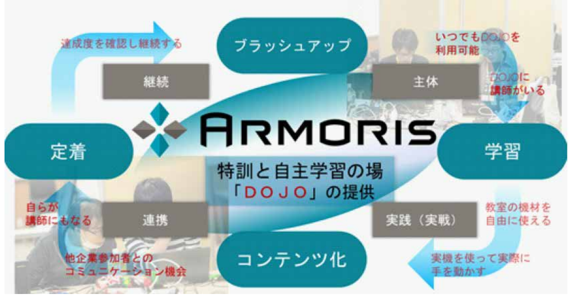


Self-assessment report on information security in fiscal 2021 (in Japanese)

Armoris DOJO Training for Cyber Security Specialists

In September 2019, the Toppan Group founded Armoris Co., Ltd., a company specialized in providing client companies and public-sector entities with programs to nurture cyber security specialists, as well as services geared to improving the security levels of their organizations. Armoris operates a series of practical personnel-training programs, including DOJO, DOJO Lite, DOJO Shot, and DOJO CORE.

Training programs at the DOJO are tailored to individual skills in an environment suited to long-term, continual practices. DOJO Lite and DOJO Shot, meanwhile, arrange case examples and case studies examining the latest cyber security themes. DOJO CORE provides practical simulation drills on responding to actual incidents. Armoris strives to enhance the security capabilities of individuals and organizations throughout Japan, including the Toppan Group, through the DOJO programs.



Overview of Armoris's DOJO service (in Japanese)

Sharing Information on Cyber Security Preparedness

Toppan continued to hold quarterly cyber-security information-sharing sessions for Group personnel involved in information security management in fiscal 2021. Toppan aims to heighten the understanding of cyber security preparedness within and outside of the Group.

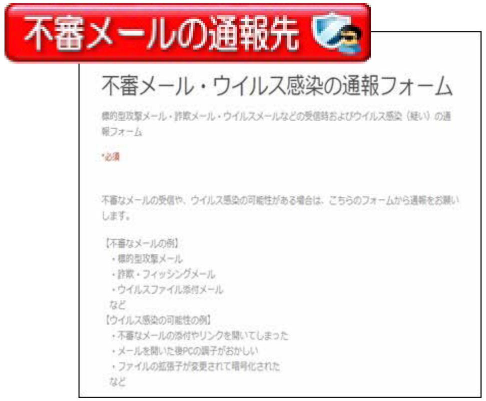
Staying on Alert for Cyber Incidents

Training, education

Organizing Drills to Address Virus-infected Emails

Toppan continues to hold suspicious email reporting drills twice a year. To prepare for the drills, all users of Toppan email addresses (about 23,000 users in total) are requested to add a shortcut link or icon that can be quickly clicked on their standing screens to report suspicious messages they have received or already opened. Starting from fiscal 2021, employees of overseas subsidiaries were asked to participate in the drills in parallel with employees from domestic subsidiaries and affiliated companies, expanding the coverage to about 39,000 persons in total.

The training held in fiscal 2021 was demanding. Toppan's cyber security team prepared a fraudulent email and sent it out to employees without pre-warning in a simulated cyber-attack. When the e-mail arrived in their inboxes, some employees went ahead and clicked a fraudulent URL link in the message and failed to recognize that the webpage launched was fake.



不審メール・ウイルス感染の通報フォーム

標的型攻撃メール・詐欺メール・ウイルスメールなどの受信時およびウイルス感染（疑い）の通報フォーム

*必須

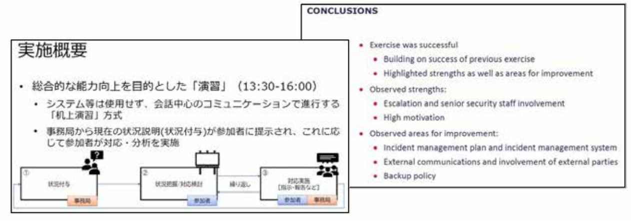
不審なメールの受信や、ウイルス感染の可能性がある場合は、こちらのフォームから通報をお願いします。

【不審なメールの例】
・標的型攻撃メール
・詐欺・フィッシングメール
・ウイルスファイル添付メール
など
【ウイルス感染の可能性の例】
・不審なメールの添付やリンクを開いてしまった
・メールを開いた後PCの調子がおかしい
・ファイルの拡張子が変更されて暗号化された
など

Screenshot of the suspicious-email report form on the Group's internal website (in Japanese)

Alerting Senior Management to Cyber Emergencies

Toppan Inc. conducts annual drills for senior management to rehearse the actions to take in the event of a cyber-attack. To fortify their safeguards, the drills better equip senior managers with leadership skills to control cyber emergencies. The drills also aim to identify any challenges they may face in their efforts to shore up the Group's risk management capabilities.


①
状況付与
事務局
②
状況把握/対応検討
参加者
繰り返し
③
対応実施
［指示・報告など］
参加者
事務局

実施概要

- 総合的な能力向上を目的とした「演習」（13:30-16:00）
  - システム等は使用せず、会話中心のコミュニケーションで進行する「机上演習」方式
  - 事務局から現在の状況説明(状況付与)が参加者に提示され、これに応じて参加者が対応・分析を実施

CONCLUSIONS

- Exercise was successful
  - Building on success of previous exercise
  - Highlighted strengths as well as areas for improvement
- Observed strengths:
  - Escalation and senior security staff involvement
  - High motivation
- Observed areas for improvement:
  - Incident management plan and incident management system
  - External communications and involvement of external parties
  - Backup policy

Operation guidance for the cyber security drill for senior management

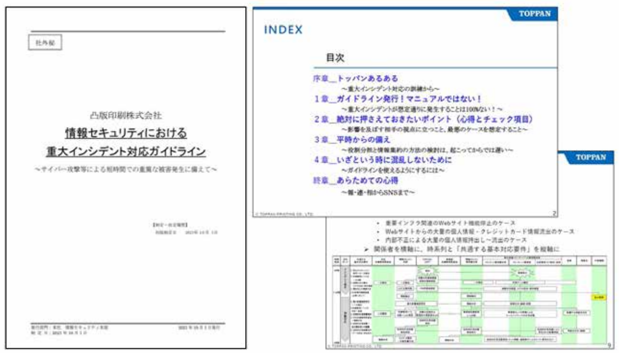
Formulating Guidelines to Address Cyber Emergencies

Cyber threats have been escalating across borders. Their unprecedented malice and technical cunning can result in instant and severe damage in all directions. In many instances, the conventional methods used against cyber-attacks are useless.

Toppan has formulated a set of guidelines that summarize the Group's basic approach, preparations, and action flows to address serious information security incidents caused by cyber-attacks and other destructive acts. The Group is strengthening its responsiveness to cyber emergencies on the assumption that unforeseen incidents can always happen.

Preparing for the Tokyo 2020 Games

As large-scale, international sporting events, the Olympic and Paralympic Games are easy targets for organized criminals. Toppan Inc., a Tokyo 2020 Official Partner, prepared for the games by gathering information on cyber threats through various channels, including an information-sharing system provided by the Cybersecurity Response Coordination Center of Japan. The Company also upgraded its emergency responsiveness by taking part in cross-sector anti-cyber-attack drills organized by the Nippon CSIRT Association and the National center of Incident readiness and Strategy for Cybersecurity (NISC) of Japan.



社外秘

凸版印刷株式会社
情報セキュリティにおける
重大インシデント対応ガイドライン
～サイバー攻撃等による短時間での重篤な被害発生に備えて～

INDEX

目次

序章＿トッパンあるある
～重大インシデント対応の訓練から～
１章＿ガイドライン発行！マニュアルではない！
～重大インシデントが想定通りに発生することは100%ない！～
２章＿絶対に押さえておきたいポイント（心得とチェック項目）
～影響を及ぼす相手の視点に立つこと、最悪のケースを想定すること～
３章＿平時からの備え
～役割分担と情報集約の方法の検討は、起こってからでは遅い～
４章＿いざという時に混乱しないために
～ガイドラインを使えるようにするには～
終章＿あらためての心得
～報・連・相からSNSまで～

- 重要インフラ関連のWebサイト機能停止のケース
- Webサイトからの大量の個人情報・クレジットカード情報流出のケース
- 内部不正による大量の個人情報持出し～流出のケース

➢ 関係者を横軸に、時系列と「共通する基本対応要件」を縦軸に

Guidelines for responding to serious information security incidents (in Japanese)