



Information security

Computers and the Internet are essential for today's corporate activities, but safely operating them is a heavy responsibility for companies. The EBARA Group sees information security as one of the important issues for management and is bringing various approaches forward.

Information security governance

The EBARA Group draws up information security-related regulations based on the "EBARA Group behavioral standard" and promotes the protection and usage of information assets. The EBARA Group sets up the EBARA Group IT strategy committee as a place to share the business strategy that the EBARA Group is trying to implement and the IT strategy. The committee plays a key role in activities to promote security. We also establish an IT strategy promotion section in each EBARA company. These sections draw up and implement the information strategy and coordinate information strategies of affiliate companies under the supervision of each company.

Approach to information security

For personnel and organizational measures, we enlighten people on the importance of information assets protection by preparing information security-related regulations and posting them on the Group's intranet. To deepen people's understanding, we issue the "EBARA Group IT newsletter" on a regular basis and deliver

information about the familiar information security. As for technological and physical measures, we consolidate connecting points to the external Internet into one point by building the EBARA Group's communication network "EC/NET." We introduce a firewall to protect hacking from the outside and make use of antivirus software and antispam software. We have sequentially taken measures such as limiting illegal access to our website, applying Web filtering technology. In addition, we provide the following information infrastructures shared by the group members and enhance the information security measures further.

- Computer virus measures for all PCs and servers in the entire group
- Integrated ID control system linked to the personnel management database and access control to the information assets
- Establishment of the data center and consolidation of servers considering business continuity when a disaster occurs

From now on, we will promote information security management based on the medium-term plan for the IT strategy and enhance personnel and organizational measures to make every single employee who handles important information be aware of compliance with rules.

第11号

2007年6月25日

【発行：IT戦略統括部 企画室／お問合せ先 02-704-8200 内々本線】

荏原グループITだより

第12号

2007年10月20日

【発行：IT戦略統括部 企画室／お問合せ先 02-704-8200 内々本線】

紹介

シリーズ：セキュリティ対策 第2回

— これだけは守って欲しい情報セキュリティのルール —

情報セキュリティ対策の基本は、社員各人が危機管理意識を持ち、会社の情報資産を守ろうとする気持ちで仕事をする事です。

重要な情報資産を守るために、次のプロセスを経て情報セキュリティ対策を行っています。

リスクアセスメント⇒規定の策定⇒ツールの導入⇒

広報・教育⇒運用

情報セキュリティ対策が効果を発揮できるのは、運用段階で各人^{*1}がルールを守るからです。

このルールを守らない為に、世の中でも、情報漏洩事件が後を絶ちません。

あんなところが！！と驚くばかりです。

マスメディアに登場した事件について、その原因

脅威のリスクと情報セキュリティ対策の導入

どんなにお金を掛けてセキュリティ対策してもリスク・ゼロにはできません。

受信レベル	リスク	情報セキュリティ対策の導入
リスク・ゼロ	リスク	残留リスク

残留リスクと脆弱性

資産(秘密情報)にアクセスするのは正理に権限を付与された各人であり、各人に資産保護の意識が低いと情報漏洩、データ改ざんなどのセキュリティ侵害が発生します。まさに各人が残留リスクであり、脆弱性を有しています。

セキュリティ対策システム

社員が遵守しなければならないルール

資産

を受け、4分科会（ネット）2007年度の活動がスター21社から延べ88名の皆様

）、事務局長

データ統合インフラ構築

Article of the "EBARA Group IT newsletter"

Society and EBARA Group

EBARA Group CSR Report 2008 33